Finite geometries, LDPC codes and cryptography

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UMCS

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt „Programowa i strukturalna reforma systemu kształcenia na Wydziale Mat-Fiz-Inf”.
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Człowiek-najlepsza inwestycja

Maria Curie-Skłodowska University
Faculty of Mathematics, Physics and Computer Science
Institute of Computer Science

Finite geometries, LDPC codes and cryptography

Vasyl Ustimenko
Urszula Romańczuk

Lublin 2012

Institute of Computer Science UMCS
Lublin 2012

Vasyl Ustimenko
Urszula Romańczuk

Finite geometries, LDPC codes and cryptography

Reviewer: Nadiya Gubareni

Technical Editor: Marcin Denkowski
Cover Designer: Agnieszka Kuśmierska

Praca współfinansowana ze środków Unii Europejskiej w ramach
Europejskiego Funduszu Społecznego

A free online edition of this book is available at informatyka.umcs.lublin.pl.

Publisher
Maria Curie-Skłodowska University
Institute of Computer Science
pl. Marii Curie-Skłodowskiej 1, 20-031 Lublin
Series Editor: prof. dr hab. Paweł Mikołajczak
www: informatyka.umcs.lublin.pl
email: dyrii@hektor.umcs.lublin.pl

ISBN: 978-83-62773-39-8

Contents

Preface

Finite geometries are intensively used in the Computer Networking because geometries with fixed Coxeter diagram form a family of small world graphs. Such families have many remarkable applications in economics, natural sciences, computer sciences and even in sociology.

From modern view Geometry is a special graph with the large group of symmetries. Geometrical studies are very important part of Modern Mathematics, for resent contribution in Geometry theory J.Tits (Paris) was awarded by Abel Prize in 2008.

Finite geometries are traditionally used in Classical Coding Theory (problems of error detection, error correction, fight with the noise). Foundations of this theory are based on the concept of finite distance - transitive or distance-regular metrics (distance regular and distance transitive graphs in other terminology). Great deal of known families of distance transitive graphs are constructed in terms of finite incidence geometry (geometries of Lie type and Coxeter geometries). Linear codes are just elements of projective geometry and all applications of Incidence Geometries are hard to observe . Notice that some nonclassical areas like LDPC codes and turbocodes use objects constructed finite geometries:for the first constructions of such codes.Tanner used finite geometries of rank 2. The infinite family of graphs of large girth (minimal length of the cycle) and its modifications have been applied to constructions of LDPC codes.

Quite resent development gives an application of linear codes and their lattices to cryptography. Incidence geometries were used for the development of cryptographical algorithms. The handbook is introduction to theory of finite geometries and its applications to Coding Theory and Cryptography. It can be used by students with specialization in Informatics and Applied Mathematics as a support for special or monographical courses within the above area. Chapter 1 is devoted to computation in geometries of Coxeter groups and geometries of simple groups of Lie type. We indicate the connections of finite geometries theory with classical Coding Theory. Famous Hamming and Johnson metrics correspond to families of orbital of Coxeter groups B_n and A_n on elements of their geometries. Similarly

Grassman metric corresponds to action of group $A_n(q)$ (projective special linear $PSL_n(q)$) on elements of its geometry of chosen type (subspaces of the $n+1$-dimensional vector space of chosen dimension m). We introduce a geometrically defined functions such as number of small Schubert cells (in case of grassmanian and general variety of elements of Lie geometry), Gaussian binomial coefficient and its generalization). We present light introduction to the theory of Shevalley groups (Simple Lie groups of normal type) Lie type and their geometries. We consider efficient for computations interpretation of Lie geometries obtained via embedding of such incidence system into the Borel subalgebra of corresponding Lie algebra. The efficient computation in the geometry of Weyl group defined by generalized Cartan matrix can be done via natural embedding of this geometry into Cartan subalgebra of corresponding Lie algebra.

Chapter 2 is devoted to connections of theory of Tits geometries with the construction of distance regular but not distance regular graphs. Various constructions of small world graphs are introduced via generalisations of geometries of Chevalley groups. Famous example of Ramanujan Cayley graphs are given with the discussions of their properties (diameter, girth, second largest eigenvalue). New family of expanding small graphs is introduced.

In chapter 3 is introduced nonlinear equations for the description of regular tree. The infinite simple graphs with irreversible walks are given by nonlinear equations over the commutative ring. Subgroups of Cremona groups with elements of bounded polynomial degree and large order are introduced.

Chapter 4 is devoted to examples of LDPC codes. In chapter 5 we investigate infinite directed graphs with irreversible walks and their applications to construction of stable subgroups of Cremona group. Last section is devoted to applications of Algebraic Graph Theory and Extremal Graph Theory to multivariate cryptography.

ACKNOLEGEMENTS.

I would like to express my deep gratitude to my graduate students Monika Polak for her advice on technical aspects of Coding Theory, Urszula Romańczuk, who is a coauthor, active research collaborator and technical advisor, Aneta Wróblewska for the useful feed back and constant support. Special thanks to my wife who is always on my side.

Vasyl Ustimenko

First and foremost I would like to thank my advisor Prof. Vasyl Ustimenko without whose aid and advise, guidance and co-operation this research work would not have been possible. I wish to thank his wonderful wife for her kindness and advices. I also want to acknowledge and thank my dear friends Aneta Wróblewska and Monika Polak for their friendship and significant contributions to the development of this research.

I am forever grateful to Prof. Wojciech Szapiel (1948- 2010) who was a supervisor of my master thesis in The Catholic University in Lublin. His professional conduct and unflagging support of me and my work has provided an excellent model for me to follow in my career. From The Catholic University in Lublin, I extend thanks and appreciation to Dr. Armen Grigoryan and Prof. Dariusz Partyka. I am also greatly indebted to Prof. Jerzy Kozicki, Prof. Maria Nowak, Prof. Stanisaw Prus and Prof. Zdzisaw Rychlik of Maria Curie-Skłodowska University in Lublin for their guidance and support.

Special thanks to my high school teacher Mikołaj Babulewicz. I have been very fortunate to have the love and support of my family. Especially I would like to thank my mother and sister for their never-ending belief in my ability. Finally I would like to thank my fiancé, for all his love, support and encouragement. Without you I could not have made it.

Urszula Romańczuk

Chapter 1

Incidence systems and geometries over diagrams

1.1. Graphs and incidence structures

The missing definitions of graph-theoretical concepts which appearin this paper can be found in [10] or [131]. All graphs we consider are *simple* , i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write $v\, G\, u$ for the adjacent vertices u and v (or neighbors). We assume that $V(G)$ is a finite or infinite set. The majority of examples will be *locally finite graphs* G, i.e. each vertex v has finite number of neighbours ($x \in V(G)$, such that $x\, G\, v$).

The sequence of distinct vertices $v_0, v_1, \dots, v_t$, such that $v_i\, G\, v_{i+1}$ for $i = 1, \dots, t-1$ is the *path* in the graph. A path in G is called *simple* if all its vertices are distinct. The graph is *connected* if each two its vertices are joined by some path. The length of a path is a number of its edges. The *distance* between two vertices u and v of the graph, denoted by $\mathrm{dist}(u, v)$, is the length of the shortest path between them. The *diameter* of the graph, denoted by $\mathrm{diam}(G)$, is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m, i.e. the sequence of distinct vertices $v_0, \dots, v_m$ such that $v_i G v_{i+1}$, $i = 1, \dots, m-1$ and $v_m G v_1$. The *girth* of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G.

The *incidence structure* is the set V with partition sets P (*points*) and L (*lines*) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another one is a line. We shall identify I with the simple graph of this incidence relation (*bipartite graph*). If number of neighbours of each element is finite and depends only on its type (point or line), then the incidence structure is a *tactical configuration in the sense of Moore* (see [100]). An incidence structure is a *semiplane* if two distinct lines are intersecting at most at one point and two distinct points are incident at most at one line. As it follows from the definition, graphs of the semiplane have no cycles C_3 and C_4.

The graph is *k-regular* if each of its vertices has degree k, where k is a constant.

Example 1.1.1. Let us consider an example of a locally finite incidence structure with point set P and line set L, which are two copies of n-dimensional vector space over the finite field $\mathbb{F}_q$. It will be convenient for us to denote vectors from P as

$$\mathrm{x} = (x) = (x_1, x_2, x_3, \dots x_i, \dots)$$

and vectors from L as

$$\mathrm{y} = [y] = [y_1, y_2, y_3, \ldots, y_i, \ldots]$$

We say that point (x) is incident with the line $[y]$ and we write it $\mathrm{x\,I\,y}$ or $(x)\,\mathrm{I}\,[y]$ if and only if the following conditions are satisfied:

$$y_i - x_i = y_{i-1}x_1$$

where $i = 2, 3, \ldots$.

It is easy to see that $W(q)$ is an infinite q-regular graph. Really, there is the unique neighhbour $\mathrm{y} = [y]$ of the given vertex $\mathrm{a} = (a)$ with the chosen first coordinate y_1 from $\mathbb{F}_q$. Other coordinates $y_2, y_3, \ldots$ can be consecutively computed from the above written equations. The neighbourhood of the line $\mathrm{b} = [b]$ can be observed in a similar way.

Let $\mathrm{W}(q)$ be the incidence graph of the structure $\Gamma(\mathbb{F}_q) = (P, L, I)$. For each integer $n \geq 2$ let $\Gamma(n, \mathbb{F}_q) = (P_n, L_n, I_n)$ be the incidence system, where P_n and L_n are the images of P and L under the projection of these spaces on the first n-coordinates and binary relation I_n is defined by the first $n-1$ equations. Finally, let $\mathrm{W(n, q)}$ be the incidence graph for $\Gamma(n, \mathbb{F}_q)$. This is exactly the graph, which has been defined by Wenger [183] and used in various problems in Computer Science [178]. Graph $\mathrm{W}(q)$ is a projective limit of $\mathrm{W}(n, q)$ when n goes to infinity.

Example 1.1.2. Let P_m be the incidence graph of the incidence structure of points (vertices) and lines (edges) of the ordinary m-gon. We can identify P with the set of singletons $\{i\}$, $i = 1, 2, \ldots, m$ and L with the collection of subsets $\{1, 2\}$, $\{2, 3\}$, $\ldots$, $\{m-1, m\}$, $\{m, 1\}$. It is easy to see that the girth of P_m is $2m$ and the diameter is m.

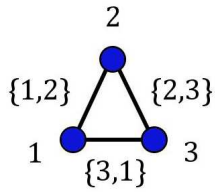


Figure 1.1. Graph P_3

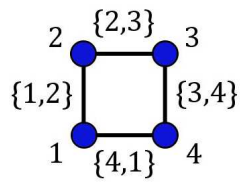


Figure 1.2. Graph P_4

According to F. Harary, who is a well known author of didactic books, Graph Studies consist of Beautiful Graph Theory dealing with graphs, which are easy to draw and imagine, and Theory of Ugly Graphs, which investigates large graphs, such that the methods of computer drawing are impossible to apply. Obviously, graphs P_m and $W(n, q)$ are objects of the

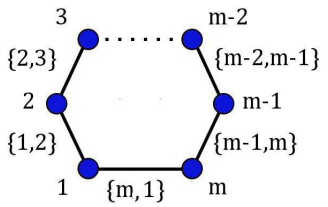


Figure 1.3. Graph P_m

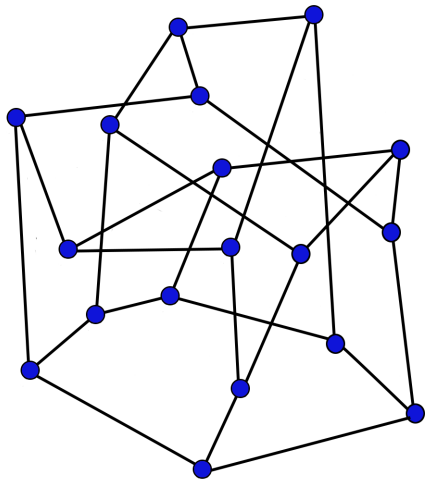


Figure 1.4. W(2,3)=A(2,3)

mentioned above different areas. Anyway, in a case of small n and q we can draw some ugly graphs (look at the pictures below).

Recall, that a *tree* is a connected graph without cycles, each finite tree on v vertices contains $v-1$ edges. It always has a leaf (vertex of degree 1). So, the tree with degrees ≥ 2 is always a locally finite graph. Vertices on the even distance from given vertex a form the set of points, the line set is a collection of vertices on an odd distance from a. There is a unique up to isomorphism *infinite biregular tree* $T_{r,s}$, which is a tactical configuration with degrees r, $r \geq 2$ and s, $s \geq 2$.

We have to mention, that many authors use term bipartite biregular graph with bidegrees rand s instead of tactical configurations with degrees r and s. In this book both terms will be used. The tree $T_{q,q}$ where q is an odd prime power can be described in the terms of equations over finite field $\mathbb{F}_q$ in the following way.

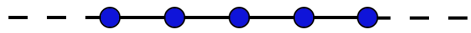


Figure 1.5. Tree $T_{2,2}$

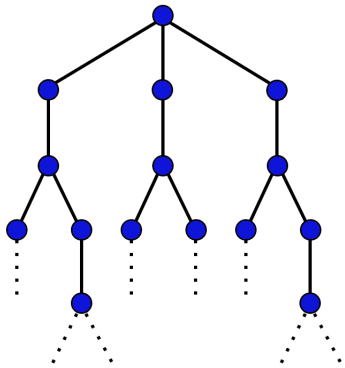


Figure 1.6. Tree $T_{3,2}$

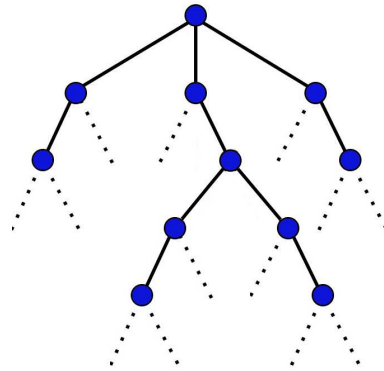


Figure 1.7. Tree $T_{3,3}$

Example 1.1.3. Let us consider the following bipartite finite graph $A(n,q)$ (*alternating graph*). The partition sets P_n and L_n are two copies of the n-dimensional vector space $\mathbb{F}_q^n$ (point set and line set, respectively). Brackets and parentheses allow us to distinguish point $(p) = (p_1, p_2, \ldots, p_n) \in P_n$ and line $[l] = [l_1, l_2, \ldots, l_n] \in L_n$. Point (p) is incident to line $[l]$ if and only if the following equations hold:

$$l_i - p_i = l_1 p_{i-1}$$
$$l_{i+1} - p_{i+1} = p_1 l_i$$

where $i = 2,\ 3, \ldots, 2\left\lfloor \frac{n}{2} \right\rfloor$, but when n is even we have to ignore the last equation. Similarly to the case of Wenger graphs we can check that graph $A(n,q)$ is the a q-regular bipartite graph (each vertex has q neighbours). Clearly, that $A(n,q)$ has $2q^n$ vertices and q^{n+1} edges.

The naturally defined projective limit of graphs $A(n,q)$ equals $T_{q,q}$.

Different description of $T_{q,q}$ in terms of equations over finite field $\mathbb{F}_q$ the reader can find [152].

Graphs $W(n,q)$ and $A(n,q)$ are examples of semiplanes. Further properties of $A(n,q)$ the reader can find in [175], [176].

Example 1.1.4. The complete bipartite graph $K_{m,n}$ is biregular graph with the sets of points P, $|P| = m$ and lines L,$|L| = n$, such that each point is

incident with each line. So, the order of $K_{m,n}$ is $m+n$ (number of vertices), the size is mn (number of edges) and bidegrees m, and n.

1.2. Incidence systems and geometries

An *incidence system* over a set Δ of types is a triple (Γ, I, t), where Γ is the set of objects of the system, I is a symmetric reflexive incidence relation over Γ and t is a mapping of Γ onto Δ, $|\Delta| \geq 2$. Sometimes we will write Γ instead of (Γ, I, t). We assume that xIy implies $t(x) \neq t(y)$. So the incidence system with $|\Delta| = 2$ is an incidence structure.

A *flag* $\mathcal{F}$ of an incidence system is a set of its objects which are pairwise incident. We assume that

$$t(\mathcal{F}) = \{t(x) | x \in \mathcal{F}\}.$$

The *residue of a flag* $\mathcal{F}$ in Γ, denoted by Res $\mathcal{F}$, is the set of objects from $t^{-1}(\Delta - t(\mathcal{F}))$ which are incident to each element of the flag, with the restrictions of I and t on this set.

A *morphism of incidence systems* Γ and Γ' over the same set of types is a mapping of Γ onto Γ' which preserves the incidence and the type of objects.

An automorphism group G of an incidence system Γ is said to *act flag-transitively* on Γ if its action on the flags of a fixed type is transitive.

The *rank of an incidence system* (of a flag $\mathcal{F}$) is the cardinality of Δ (the cardinality of $t(\mathcal{F})$). The *corank of a flag* $\mathcal{F}$ is defined as the cardinality of $\Delta - t(\mathcal{F})$. The incidence system (Γ, I, t) is said to be *connected* if the graph with the vertex set Γ and the edge set I is connected.

An incidence system (Γ, I, t) over Δ is called *geometry* if the restriction of t on each maximal flag $\mathcal{F}$ of Γ is a bijection of $\mathcal{F}$ onto Δ.

It is easy to see that if $\mathcal{F}$ is a flag of a geometry Γ then the residue Res $\mathcal{F}$ is a geometry over the set of types $\Delta - t(\mathcal{F})$.

A *diagram* over Δ is a mapping D defined on the totality of the 2-element subsets A of Δ such that $D(A)$ is an element from the certain class of geometries of rank 2 over the set of types A. A geometry Γ is said to be a *geometry over diagram* D if for each flag $\mathcal{F}$ of corank 2 Res $\mathcal{F}$ is contained in $D(\Delta - t(\mathcal{F}))$.

The most important class of rank 2 geometries is the class of so called generalized m-gons, (see [139], [186]).

Generalized m-gons defined by J. Tits in 1959 (see [139], [140], [141], [142], [143]) as a tactical configurations of bidegrees $s+1$ and $t+1$ of girth $2m$ and diameter m. The pair (s, t) is known as *order* of generalized m-gon.

It is clear that ordinary m-gon P_m is a generalised m-gon of order $(1,1)$. A connected generalised ∞-gon is a bipartite tree $T_{r,s}$ of order $(r-1,s-1)$.

The following statement is known as Feit-Higman theorem (see [16]).

Theorem 1.2.1. *For a finite generalized m-gon of order (s,t) with $s>1$ and $t>1$ parameter m is an element of the set $\{3,4,6,8\}$.*

The known examples of flag transitive generalized m-gons of bidegrees ≥ 3 are incidence graphs of geometries of finite simple groups of Lie type with rank 2. The regular incidence graphs are m=3 (group $A_2(q)$), $m=4$ (group $B_2(q)$ or $C_2(q)$), $m=6$ (group $G_2(q)$), in all cases $s=t=q$, where q is prime power.

The biregular but not regular generalized n-gons have parameters $s=q^\alpha$ and $t=q^\beta$, where q is some prime power. The list of such objects is below:
(i) $n=4$: $s=q, t=q^2$ and q is arbitrary prime power or $s=q^2, t=q^3$ and q is arbitrary prime power;
(ii) $n=6$: $s=q^2$, $t=q^3$ and $q=3^{2k+1}$, $k>1$;
(iii) $n=8$: $s=q$, $t=q^2$ and $q=2^{2k+1}$.

The known generalised octagon corresponds to finite simple group of twisted type ${}^2F_4(q)$, $q=2^{2k+1}$ (see [21]).

The genelalised triangle corresponding to $A_2(q)$ is *classical projective plane*, i.e. it is the following incidence structure. Let $V=\mathbb{F}_q^3$ be a vector space of dimension 3. Let us assume that the set of points

$$P=\{W<V|\dim(W)=1\}$$

is the totality of one dimensional subspaces of V (projective points) and the set of lines is

$$L=\{W<V|\dim(W)=2\}.$$

We will use brackets (p) and parenthesis $[l]$ to distinguish point $(p)\in P$ from the line $[l]\in L$.

Point (p) is incident to line $[l]$ exactly if and only if (p) is a subspace of two dimensional space $[l]$.

Cycles of arbitrary incidence structure have even length. The cycle of length 4 is $K_{2,2}$ graph which contains two points (p_1) and (p_2) and two lines $[l_1]$ and $[l_2]$. But the intersection of $[l_1]\cap[l_2]$ is uniquely defined point. So, we get a contradiction and the proof of nonexistence of cycles of length 4. We can form a cycle of length 6 from the standard basis e_1, e_2, e_3 of the vector space V as the following sequence of subspaces $\langle e_1\rangle$, $\langle e_1,e_2\rangle$, $\langle e_2\rangle$, $\langle e_2,e_3\rangle$, $\langle e_3\rangle$, $\langle e_3,e_1\rangle$.

The unique chain between two lines $[l_1]$ and $[l_2]$ (points (p_1) and (p_2)) is a sequence $[l_1]\ I\ ([l_1]\cap[l_2])\ I\ [l_2]$ $((p_1)\ I\ [\langle(p_1),(p_2)\rangle]\ I\ (p_2)$, respectively), so the length is two. The maximal length will be between point (p) and line

$[l]$, which are not connected by an edge, the corresponding chain is of kind $(p)\ I\ [l']\ I\ (p')\ I\ [l]$, where $[l']$ is a line trough the point (p) and (p') is the point on a line $[l]$. So, the diameter of our incidence structure is 3. Let us compute the degree of each vertex. Every two dimensional subspace over $\mathbb{F}_q$ contains q^2-1 nonzero vectors, $q-1$ proportional vectors and zero vector form one dimensional subspace. So, we have $(q^2-1)/(q-1) = q+1$ points through chosen line. The change of two dimensional subspace in the written above computation for the space of dimension 3 will allow us to compute number of all points, which is $(q^3-1)/(q-1) = 1+q+q^2$. The general equation of the line is

$$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 0,$$

where the point with nonzero vector $(\alpha_1, \alpha_2, \alpha_3)$ gives full information about the line. It means that we have $1+q+q^2$ lines in our incidence structure. So, the order of our bipartite graph is $2(1+q+q^2)$. We can get the size (number of edges) as a product of number of points $1+q+q^2$ with the degree $q+1$. So, the size e equals $(q^3-1)/(q+1)$. We compute the degree of line simply by division of e on number of lines $(1+q+q^2)$. So, incidence graph is regular of degree $q+1$. Let use the notation $PG_2(q)$ for the classical projective plane introduced above.

The connected geometries over diagrams D such that $D(A)$ is the class of generalized m-gons for some m together with the family of complete bibartite graphs are called the *Tits geometries*. If $A = \{i, j\}$ and $D(A)$ is generalised m-gon, then we shall draw the edge between nodes i and j with the weight $m-2$. If $D(A)$ is a biregular tree we put the weight ∞. Absence of the edge between nodes i and j means that $D(A)$ is a bipartite complete graph $K_{n,m}$.

We refer to Tits geometry as *thin incidence system* if all generalised m-gons of kind $D(A)$ have order $(1,1)$, i.e. $D(A)$ is an ordinary m-gon P_m, tree $T_{2,2}$ or complite bipartite graph.

In opposite case when all generalised m-gons of Tits geometry are of order (r,s), $r \geq 2$ and $s \geq 2$, we will use term *thick incidence system*. As it follows from the definitions and Feit Higman theorem the diagram of finite thick Tits geometry has weights $1, 2, 4$ or 6.

1.2.1. Flag transitive thin geometry over diagram A_n

Let us consider the example of flag transitive thin geometry over diagram A_n:

Let $N = \{1, 2, \ldots, n, n+1\}$ be the set of cardinality $n+1$. We will define the incidence structure (Γ, I, t) on the set Γ of all proper nonempty subsets of N. Γ is a disjoint union of Γ_i consisting of subsets of cardinality

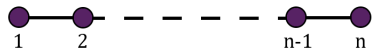


Figure 1.8. Diagram A_n

i, $i = 1, 2, \ldots, n$. We assume $A\,I\,B$ if $A \neq B$ and A is a subset of B or B is a subset of A. Type function is introduced by $t(A) = |A|$.

Let us consider the flag $\mathcal{F}$ of corank 2, which consist of $\{1\}$, $\{1,2\}$, $\ldots$, $\{1,2,\ldots,n-2\}$. The incidence structure $\mathrm{Res}(\mathcal{F})$ corresponds to nodes $n-1$ and n. Clearly,

$$\Gamma_{n-1} \cap \mathrm{Res}(\mathcal{F}) = \{A \cup \{n-1\}, A \cup \{n\}, A \cup \{n+1\}\}$$

and

$$\Gamma_n \cap \mathrm{Res}(F) = \{A \cup \{n-1, n\}, A \cup \{n, n+1\}, A \cup \{n+1, n-1\}\},$$

where $A = \{1, 2, \ldots, n-2\}$. So, $\mathrm{Res}(\mathcal{F})$ is isomorphic to ordinary triangle P_3 and nodes $n-1$ and n are connected by edge with weight 1. Let $\mathcal{E}$ be the maximal flag, which consist of $\{1\}$, $\{1,2\}$, $\ldots$, $\{1,2,\ldots,n-1\}$, $\{1,2,\ldots,n\}$ and $\mathcal{E}_{i,j}$ is obtained by deleting of subsets of cardinalities i and j. It is easy to see that $\mathrm{Res}(\mathcal{E}_{i,j})$, $j = i+1$ is isomorphic to triangle P_3. Let us investing are $\mathrm{Res}(\mathcal{E}_{1,3})$ corresponding to flag $\{1,2\}$, $\{1,2,3,4\}$, $\{1,2,3,4,5\}$, $\ldots$, $\{1,2,\ldots,n\}$. It contains singletons $\{1\}$ and $\{2\}$ together with subsets $\{1,2,3\}$ and $\{1,2,4\}$. It means that $\mathrm{Res}(\mathcal{E}_{1,3})$ is isomorphic to complete graph $K_{2,2}$ and nodes 1 and 3 are not connected by edge. In similar way we proof the absence of edge between i and j, such that $|i-j| \geq 2$. We refer to this Tits geometry as *Boolean geometry* A_n.

The symmetric group S_{n+1} of all permutations on the set

$$N = \{1, 2, \ldots, n, n+1\}$$

of order $(n+1)!$ naturally acts on Γ: permutation π sends $\{i_1, i_2, \ldots, i_m\}$ to $\{\pi(i_1), \pi(i_2), \ldots, \pi(i_m)\}$. It is easy to see that $A\,I\,B$ implies $\pi(A)\,I\,\pi(B)$, $t(A) = t(\pi(A))$. So, each permutation π is an automorphism of (Γ, I, t). The maximal flag $\mathcal{F}$ is a collection of $\{i_1\}$, $\{i_1, i_2\}, \ldots, \{i_1, i_2, \ldots, i_n\}$, there is a uniquely defined $i_{n+1} \in N \setminus \{i_1, i_2, \ldots, i_n\}$. So, flag $\mathcal{F}$ corresponds to permutation $i_1, i_2, \ldots, i_n, i_{n+1}$ and there are exactly $(n+1)!$ maximal flags. The symmetric group S_{n+1} acts transitively on the set of maximal flags, i.e. for each pair of maximal flags $\mathcal{F}$ and $\mathcal{F}'$ there is a permutation $\pi \in S_{n+1}$ which sends $\mathcal{F}$ into $\mathcal{F}'$. This action is regular, the permutation π sending $\mathcal{F}$ in $\mathcal{F}'$ is uniquely determined. Notice, that the map $c : A \to N \setminus A$, $A \in \Gamma$ is an automorphism of the incidence graph, which does not preserve the type

functions, $t(c(A))$ can be different from $t(A)$. Anyway $t(A) = t(B)$ implies $t(c(A)) = t(c(B))$.

Group S_{n+1} appears as the automorphism group of thin Tits geometry Γ. Vise versa we can reconstruct the geometry from symmetric group. Recall, that each permutation from the group S_{n+1} is a product of transpositions (i, j), $i, j \in N$. So, the symmetric group is generated by all transpositions. The number of generators is $(n + 1)(n + 2)/2$. In fact we may use only transpositions from the smaller set

$$\{s_1 = (1, 2),\ s_2 = (2, 3), \ldots,\ s_{n-1} = (n - 1, n),\ s_n = (n, n + 1)\}$$

of cardinality n. Really

$$\begin{aligned}(23)(12)(23) &= (13),\\ (34)(13)(34) &= (14),\\ (45)(14)(45) &= (1, 5),\\ &\ldots\\ (n, n + 1)(1, n)(n, n + 1) &= (1, n + 1).\end{aligned}$$

So, we have all transpositions with the symbol 1. We can conjugate them with (12) and get all transpositions with symbol 2: $(1, 2)$ and $(2, 3)$ are already on our list

$$(12)(1i)(12) = (2i), \quad i = 4, 5, \ldots, n + 1.$$

We may consider consequtively

$$\begin{aligned}(23)(2i)(23) &= (3i), \quad i = 4, 5, \ldots, n + 1,\\ (34)(3i)(34) &= (4i), \quad i = 5, 6, \ldots, n + 1,\\ &\ldots\\ (n, n + 1)(n - 1, n)(n, n + 1) &= (n - 1, n + 1).\end{aligned}$$

Let W_i be a subgroup of S_{n+1} generated by s_j, $j \neq i$. Then W_1 and W_n are isomorphic to S_n, $W_i = S_i \times S_{n+1-i}$ (direct product of two symmetric groups).

Let Γ' be the totality of left cosets of kind gW_i, $g \in S_{n+1}$, $i = 1, 2, \ldots, n$. We set $t'(gW_i) = i$ and $\alpha\ I'\ \beta$ for α and β from Γ' if and only if $\alpha \neq \beta$ and set theoretical intersections of α and β is a nonempty set.

Proposition 1.2.2. *The incidence system* (Γ', I', t) *is isomorphic to Boolean geometry* A_n.

Proof. The symmetric group S_{n+1} acts transitively on the set Γ'_i of elements of the type i from Γ'. The set Γ'_i contains all left cosets of group S_{n+1} by subgroup W_i, which is isomorphic to $S_i \times S_{i+1}$. So

$$|\Gamma'_i| = \frac{(n+1)!}{i!(n+1-i)!} = C^i_{n+1}.$$

So, actions of S_{n+1} on sets Γ_i and Γ'_i are similar. Let d_i be the bijection of Γ_i onto Γ'_i, which send $\{g(1), g(2), \ldots, g(i)\}$ to gW_i. Then the map d of Γ onto Γ' such that $d(x) = d_i(x)$ for $x \in \Gamma_i$ induces the similarity of intransitive permutation groups (S_{n+1}, Γ) and (S_{n+1}, Γ') and isomorphism of incidence structures Γ and Γ'. □

Recall that *commutator* of S_{n+1}, i.e. group generated by elements of kind $aba^{-1}b^{-1}$, $a, b \in S_{n+1}$ is alternating group A_n consisting of all even permutations. A_n, $n \geq 5$ is finite nonabelian simple group, i. e. it does not contain normal subgroups (subgroups H, such that $gHg^{-1} = H$ for all $g \in A_n$). Group A_3 is a cyclic group of order 3. Group A_4 contains normal subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$. The smallest finite nonabelian group A_5 was discovered by Galois.

1.2.2. Flag transitive thick geometry over diagram A_n

Now let us consider the example of flag transitive thick geometry over diagram A_n, $n \geq 2$.

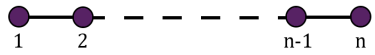


Figure 1.9. Diagram A_n

Let $\mathbb{F}_q$ be a finite field and $V = \mathbb{F}_q^{n+1}$ is the vector space of dimension $n+1$. We will define the incidence structure (Γ, I, t) on the set Γ of all proper nonzero subspaces of V. Γ is a disjoint union of Γ_i consisting of subspaces of dimension i, $i = 1, 2, \ldots, n$. We assume that $A\, I\, B$ if $A \neq B$ and A is a subspace of B or B is a subspace of A. Type function is introduced by $t(A) = \dim(A)$.

Let $e_1, e_2, \ldots, e_{n+1}$ be the standard basis of V. Let us consider the flag $\mathcal{F}$ of corank 2, which consists of $\langle e_1 \rangle$, $\langle e_1, e_2 \rangle$, $\ldots$, $\langle e_1, e_2, \ldots, e_{n-2} \rangle$. The incidence structure $\mathrm{Res}(\mathcal{F})$ corresponds to nodes $n-1$ and n. Clearly,

$$\Gamma_{n-1} \cap \mathrm{Res}(\mathcal{F}) = \{W \,|\, \langle e_1, e_2, \ldots, e_{n-2} \rangle < W < V,\ \dim(W) = n-1\}$$

and

$$\Gamma_n \cap \mathrm{Res}(\mathcal{F}) = \{\langle e_1, e_2, \ldots, e_{n-2}\rangle < W < V,\ \dim(W) = n\}.$$

So, $\mathrm{Res}(\mathcal{F})$ is isomorphic to projective plane $PG_2(q)$ corresponding to group $A_2(q)$ (*thick generalised triangle*) and nodes $n-1$ and n are connected by edge with weight 1. Let $\mathcal{E}$ be the maximal flag, which consists of $\langle e_1\rangle$, $\langle e_1, e_2\rangle, \ldots, \langle e_1, e_2, \ldots, e_{n-1}\rangle$, $\langle e_1, e_2, \ldots, e_n\rangle$ and $\mathcal{E}_{i,j}$ is obtained by deleting of subspaces of dimensions i and j. It is easy to see that $\mathrm{Res}(\mathcal{E}_{i,j})$, $j = i+1$ is isomorphic to thick generalised triangle $PG_2(q)$.

Let us investigate $\mathrm{Res}(\mathcal{E}_{1,3})$ corresponding to flag $\langle e_1, e_2\rangle$, $\langle e_1, e_2, e_3, e_4\rangle$, $\langle e_1, e_2, e_3, e_4, e_5\rangle$, $\ldots$, $\langle e_1, e_2, \ldots, e_n\rangle$. It contains $q+1$ one dimensional subspaces of $\langle e_1, e_2\rangle$ together with collection of 3 dimensional subspaces of $\langle e_1, e_2, e_3, e_4\rangle$, which contains $\langle e_1, e_2\rangle$ (there are $q+1$ of them). Every one dimensional subspace is incident to every subspace of dimension 3. It means, that $\mathrm{Res}(\mathcal{E}_{1,3})$ is isomorphic to complete graph $K_{q+1,q+1}$ and nodes 1 and 3 are not connected by an edge. In similar way we prove the absence of edge between i and j such that $|i-j| \geq 2$. The described incidence system $PG_n(q)$ is a *classical projective geometry of rank* n.

Let us consider the *general linear group* $GL_{n+1}(q)$ of all nonsingular matrices $A = (a_{i,j})$ over the finite field $\mathbb{F}_q$, i.e. matrices of order $(n+1) \times (n+1)$ with entries from finite field $\mathbb{F}_q$ and nonzero determinant.

Let us count the order of this finite group. We can choose arbitrary nonzero vector a_1 to form the first row of the matrix. Number of options to make this step is $q^{n+1} - 1$. For the right choice of the second row we have to use nonproportional to a_1 vectors. So, we have to subtract q (number of bad vectors) from the number q^{n+1} of all vectors from $\mathbb{F}_q^{n+1}$ on the second step of forming second row a_2. For the third row we have to avoid linear combinations of a_1 and a_2. So, the total number of right options is $q^{n+1} - q^2$. We have to continue the design of a matrix. Last row can be chosen in $q^{n+1} - q^n$ right ways. The number of options for each step of the described above process does not depend on previous steps. So, we have to apply multiplication rule for the counting of order for the group $GL_n(q)$. It means that

$$|GL_n(q)| = (q^{n+1} - 1)(q^{n+1} - q)(q^{n+1} - q^2)\ldots(q^{n+1} - q^n).$$

Group $GL_n(q)$ acts on the vectors (rows) from $V = \mathbb{F}_q^{n+1}$ by the rule: matrix A sends $\mathrm{x} \in V$ into $\mathrm{x}A$. The action of this group on the set V induces the action on $PG_n(q)$. Matrix $A \in GL_n(q)$ moves subspace W into subspace $W' = \{\mathrm{x}A | x \in W\}$. The induced action is not faithful, totality $S(q)$ of scalar matrices form the kernel. The factor group $PGL_n(q) = GL_{n+1}(q)/S(q)$ (*projective linear group*) is the automorphism group of $PG_n(q)$.

The maximal flag $\mathcal{F}$ is a collection of subspaces W_i, $i = 1, 2, \ldots, n$, such that $W_1 < W_2 < \cdots < W_n$ and $\dim(W_i) = i$, $i = 1, 2, \ldots, n$.

The group $PGL_n(q)$ acts transitively on the set of maximal flags of projective geometry $PGL_n(q)$. The commutator of group $PGL_n(q)$ is a group $PSL_n(q) = SL_n(q)/S(q)$, where $SL_n(q)$ is a totality of all matrices from $GL_n(q)$ with determinant 1. Groups $PSL_n(q)$, $q > 2$ or $A_n(q)$ in notations of theory of simple group of Lie type form a family of finite nonabelian simple groups.

1.3. Distance transitive graphs

1.3.1. Johnson graph

Let us consider some applied object connected with the introduced geometries.

Recall that group S_{n+1} acts transitively on the set Γ_i of elements A_n of type i, $1 < i < n$. Let us consider *orbitals* of S_{n+1}, i.e. classes of equivalence on the Cartezian product $\Gamma_i \times \Gamma_i$: $(a, b) \Longleftrightarrow (a', b')$ if and only if there exists π, such that $\pi(a) = a'$ and $\pi(b) = b'$. Each class ϕ_j is a binary relation (graph). In partition of $\Gamma_i \times \Gamma_i$ into ϕ_i can be described explicitely in the following way:

$$\phi_j = \{(A, B) |\ |A \cap B| = j\}, \quad j = 1, 2, \ldots, i.$$

Each ϕ_j is a symmetric relation and ϕ_i is equality relation.

We may introduce the function

$$J(A, B) = i - |A \cap B|.$$

Obviously, elements (A, B) and (A', B') are taken from the same orbital if and only if

$$J(A, B) = J(A', B').$$

It is easy to see that symmetric function $J(A, B)$ is a metric on the finite set Γ_j, i.e. $J(A, B) \geq 0$, $J(A, B) = 0$ implies $A = B$ and the triangle inequality holds $J(A, B) \leq J(A, C) + J(C, B)$.

Recall, that function d is a *distance transitive metric* d if $d(A, B) = d(A', B')$, then there exists a metric automorphism π (i.e. $d(x, y) = t$ implies $\pi(x) = \pi(y)$), such that $\pi(A) = A'$ and $\pi(B) = B'$.

The classical Coding Theory studies examples of finite distance transitive metrics d on the set X and maximal subsets Y of X such that $d(x, y) \geq t$, where t is fixed parameter ≥ 1, and x, y are arbitrary pair of distinct

elements on X. Notice, that in the case of distance transitive metric d can be given by the family of symmetric binary relations

$$\psi_j = \{(a,b) \in X^2 | d(a,b) = j\}, \quad j = 0,1,2,\ldots,i.$$

It is clear that ψ_0 is identity relation and we can identify ψ_j, $j = 1,2,\ldots,i$ with corresponding simple graph. It is easy to check that $(a,b) \in \psi_j$ if and only if the shortest path between vertices a and b in the graph ψ_1 has length j.

Graph of the symmetric binary relation ψ_1 is called *distance transitive graph*.

The function $J(A,B)$ is well known *Johnson metric* of Coding Theory, graph

$$J_1 = \{(A,B) \in \Gamma^2 | J(a,b) = 1\}$$

is known as *Johnson graph*. This is an example of finite distance transitive graph.

The k-regular tree $T_{k,k}$ is an example of infinite, but locally finite distance transitive graph (see [126], [127]).

Notice, that Γ_j can be generated as a totality of strings $(x_1, x_2, \ldots, x_{n+1})$, $x_s \in \{0,1\}$, $s = 1,2,\ldots,n,n+1$ such that

$$x_1 + x_2 + \cdots + x_{n+1} = j.$$

Dijkstra algorithm will provide us with the distance between A and B for $O(C_n^j \ln(C_n^j))$ elementary steps via computation of the shortest path in J_1. But we can compute this distance $J(A,B)$ as $i - |A \cap B|$, where $A \cap B$ is obtained by computation of scalar product for vectors $(x_1, x_2, \ldots, x_{n+1})$ and $(y_1, y_2, \ldots, y_{n+1})$ corresponding to subsets A and B ($O(n)$ elementary steps).

Fast computation of the distance is common feature of all known families of distance transitive graphs. This is one of the reason for their importance in Computer Science (Networking, Parallel computations, Coding and etc).

The Johnson metric is connected with the thin Tits geometry with the diagram A_n.

1.3.2. Hamming graph

Let us consider the totality B_{n+1} of pairs (A,f), where A is a nonempty subset of $\{1,2,\ldots,n,n+1\}$ of cardinality $|A| \leq n+1$ and f is a map from A into $\{0,1\}$. It is easy to count B_{n+1} as

$$2C_{n+1}^1 + 2^2 C_{n+1}^2 + \cdots + 2^{n+1} C_{n+1}^{n+1} = 3^{n+1} - 1.$$

We consider B_{n+1} as incidence system with the incidence relation I: $(A, f)\ I\ (B, g)$ if and only if $A \neq B$, A is a subset of B or B is a subset of A, $x \in A \cap B$ implies $f(x) = g(x)$.

Let us consider the maximal flag $\mathcal{F}$, which contains $(\{1\}, f_1)$, $(\{1, 2\}, f_2)$, $\ldots$, $(\{1, 2, \ldots, n\}, f_n)$, $(\{1, 2, \ldots, n, n+1\}, f_{n+1})$, where $f_{n+1}(x) = 0$ for all $x \in \{1, 2, \ldots, n, n+1\}$

Let $\mathcal{F}_{i,j}$, $i < j$ be the flag of corank 2 which is obtained by deleting of elements of type i and j from the maximal flag $\mathcal{F}$. Similarly to thin flag-transitive geometry A_{n+1} we can show that if $|i - j| \geq 2$ then $\mathrm{Res}(\mathcal{F}_{i,j})$ is complete graph, if $|i - j| = 1$ and $j \neq n + 1$ then $\mathrm{Res}(\mathcal{F}_{i,j})$ is isomorphic to thin triangle P_3. The incidence structure $\mathrm{Res}(\mathcal{F}_{n,n+1})$ consist on two elements of kind $(\{1, 2, \ldots, n\}, f_n)$, such that $f_n(i) = 0$ for $i = 1, 2, \ldots, n-1$ ($f_n(n)$ can be chosen as 0 or 1) and two elements of kind ($\{1, 2, \ldots, n, n+1\}$,f_{n+1}), such that $f_{n+1}(i) = 0$ for $i = 1, 2, \ldots, n$ ($f_{n+1}(n+1)$ can be chosen as 0 or 1). The restriction of our incidence relation I on $\mathrm{Res}(\mathcal{F}_{n,n+1})$ is isomorphic to ordinary quadrangle P_4. This way we computed the diagram of the incidence structure and prove that the object is thin Tits geometry with the diagram B_{n+1}.

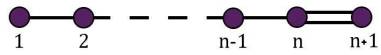


Figure 1.10. Diagram B_{n+1}

The maximal flag of our geometry is an element of kind

$$
\begin{aligned}
&(\{i_1\}, f_1),\\
&(\{i_1, i_2, \}f_2),\\
&\qquad\vdots\\
&(\{i_1, i_2, \ldots, i_n\}, f_n),\\
&(\{i_1, i_2, \ldots, i_n, i_{n+1}\}, f_{n+1}),
\end{aligned}
$$

where $f_{n+1}(i) = b_i$, $i = 1, 2, \ldots, n, n+1$ for some vector b $= (b_1, b_2, \ldots, b_{n+1})$ belonging to $\mathbb{F}_2^{n+1}$.

Let us consider the totality of pairs and (π, c), where $\pi \in S_{n+1}$ and $\mathrm{c} \in \mathbb{F}_2^{n+1}$. Each pair (π, c) moves written above flag into

$$\begin{aligned}
&(\{\pi(\{i_1\})\}, f'_1),\\
&(\pi(\{i_1, i_2\}), f'_2),\\
&\qquad\vdots\\
&(\pi(\{i_1, i_2, \ldots, i_n\}), f'_n),\\
&(\pi(\{i_1, i_2, \ldots, i_n, i_{n+1}\}), f'_{n+1}),
\end{aligned}$$

where $f'_{n+1}(\pi(i)) = b_i + c_i$. It is easy to see that the transformation group on the set of maximal flags is isomorphic to the group of bijections $\mathrm{x} \to \mathrm{x}A + \mathrm{c}$ on the set of row vectors from $\mathbb{F}_2^{n+1}$, where A is permutational matrix and $\mathrm{c} \in \mathbb{F}_2^{n+1}$. Recall, that the entries of permutational matrix are taken from $\{0, 1\}$ and each row or column contains exactly one symbol 1. We refer to this group as *hypercubical group* and denote it via HC_{n+1}. Obviously $|HC_{n+1}| = 2^{n+1}(n+1)!$. This group acts naturally on the set of elements of our incidence systems. This action allow us treat each element of HC_{n+1} as an automorphism of our thin Tits geometry with the diagram A_{n+1}. Notice that HC_{n+1} *acts regularly on the set of maximal flags*, i.e. for each pair of flags $\mathcal{F}_1$, $\mathcal{F}_2$ there exist unique group element, which moves $\mathcal{F}_1$ into $\mathcal{F}_2$.

Notice, that the group HC_{n+1} acts on the set of elements corresponding to the node $n+1$ similarly to $(HC_{n+1}, \mathbb{F}_2^{n+1})$. Two pairs of functions $(f,\, g)$ and $(f',\, g')$ from $\{1, 2, \ldots, n, n+1\}$ into $\mathbb{F}_2$ are in the same group orbital if and only if sets $A = \{x | f(x) = g(x)\}$ and $A' = \{x | f'(x) = g'(x)\}$ have the same cardinality k.

We can introduce distance regular metric

$$H(f, g) = n + 1 - |\{x | f(x) = g(x)\}|$$

and write the condition (f, g) and (f', g') are from the same orbital as $d(f, g) = d(f', g')$. The symmetric function $d(f, g)$ is, in fact, famous *Hamming metric*, which has various applications in Computer Science. Let us consider distance transitive *Hamming graph*

$$H_1 = \{(f, g) | H(f, g) = 1\}.$$

In case of dimension 2, 3 graphs H_1 are isomorphic to of P_4 and 3 dimensional cube, for which HC_2 and HC_3 are full automorphism groups, respectively.

1.3.3. Grassman graph

Recall that group $PSL_{n+1}(q)$ acts transitively on the set Γ_i of elements of geometry $A_n(q)$ of type i, $1 < i < n$ Let us consider *orbitals* of S_{n+1}, i.e.

classes of equivalence on the Cartezian product $\Gamma_i \times \Gamma_i$: $(a,b) \Longleftrightarrow (a',b')$ if and only if there exist π, such that $\pi(a) = a'$ and $\pi(b) = b'$. Each class ϕ_j is a binary relation (graph). In partition of $\Gamma_i \times \Gamma_i$ into ϕ_i can be described explicitely in the following way:

$$\phi_j = \{(W_1, W_2) | \dim(W_1 \cap W_2) = |W_1 \cap W_2| = j\}, \quad j = 1, 2, \ldots, i.$$

Each ϕ_j is a symmetric relation and ϕ_i is equality relation.

We may introduce the function

$$G(W_1, W_2) = i - |\mathrm{W}_1 \cap \mathrm{W}_2|.$$

Obviously elements (W_1, W_2) and (W_1', W_2') are taken from the same orbital if and only if $G(W_1, W_2) = G(W_1', W_2')$. it is easy to see that symmetric function $G(A, B)$ is a metric function on the finite set Γ_j. The function is an other example of distance transitive metric known as *Grassman metric*.

If $G(W_1, W_2) = G(W_1', W_1')$, then there exists a metric automorphism $g \in PSL_n(q)$, such that $g(W_1) = W_1'$ and $g(W_2) = W_2'$. The classical Coding Theory studies examples of maximal subsets Y of Γ_i such that $d(W_1, W_2) \geq t$, where t is fixed parameter ≥ 1, and W_1, W_2 are arbitrary pair of distinct elements on Γ_j.

Information on the Grassman metric G can be given by the family of symmetric binary relations

$$G_j = \{(W_1, W_2) \in {\Gamma_i}^2 | G(W_1, W_2) = j\}, \quad j = 0, 1, 2, \ldots, i.$$

It is clear that ϕ_0 is identity relation and we can identify ϕ_j, $j = 1, 2, \ldots, i$ with corresponding simple graph. It is easy to check that $(W_1, W_2) \in G_j$ if and only if the shortest path between vertices W_1 and W_2 in the graph G_1 has length j.

Graph of the symmetric binary relation G_1 is called *Grassman graph*. It is an example of distance transitive graph.

1.4. Some connections between thick geometry $A_n(q)$ and thin Tits geometry A_n.

Let us consider some connections between thick geometry $A_n(q)$ and thin Tits geometry A_n. Let $e_1, e_2, \ldots, e_n, e_{n+1}$ be the *standard basis* of the vector space $\mathbb{F}_q^{n+1}$. The *simplex* $\mathrm{Sim}(n+1)$ is formed by subspaces of kind $\langle e_{i_1}, e_{i_2}, \ldots, e_{i_s} \rangle$, $1 \leq s \leq n$. It is easy to see that it contains exactly $2^{n+1} - 2$ subspaces and the restrictions of the incidence relation I of geometry $A_n(q)$ and type functions on $\mathrm{Sim}(n+1)$ introduce incidence system isomorphic to A_n.

We can treat the totality of *unitriangle group* $U(n+1,q)$ consisting on matrices with entries $a_{i,j}$ such that $(i<j)$ implies $a_{i,j}=0$ and $a_{i,i}=0$, as a subgroup of $PSL_n(q)$. Let us investigate the orbits of this group on the variety of elements of geometry $A_n(q)$. Let $E(A)=\langle e_{i_1},e_{i_2},\dots,e_{e_s}\rangle$, where $i_1<i_2<\dots<i_s$ and $A=\{i_1,i_2,\dots,i_s\}$ be a subspace from Sim$(n+1)$. An element g, $g\in U(n+1,q)$ will send $E(A)$ to $g(W)$ with the basic elements

$$\begin{aligned}
e'_{i_1} &= e_{i_1}+a_{1,i_1}e_1+a_{2,i_2}e_2+a_{i_1-1,i_1}e_{i_1-1},\\
e'_{i_2} &= e_{i_2}+a_{1,i_2}e_1+a_{2,i_2}e_2+a_{i_2-1,i_2}e_{i_2-1},\\
&\vdots\\
e'_{i_s} &= e_{i_s}+a_{1,i_s}e_1+a_{2,i_s}e_2+a_{i_s-1,i_s}e_{i_s-1}.
\end{aligned}$$

We can make zero instead a_{i_l,i_l} by subtraction of uniquely determined linear combination of previous vectors e'_{i_k}, $k<l$. So without loss of generality we assume $a_{i_l,i_t}=0$ for $i_l<i_t$.

We refer to written above basis as *canonical basis* of $g(W)$. In fact we described all $q^{i_1+i_2+\dots+i_s}/q^{s(s+1)/2}$ elements of the orbit. We will write $W\iff W'$ if and only if W and W' are elements of the same orbit of $U(n+1,q)$.

Notice that group $U(n+1,q)$ acts regularly but not faithfully on each orbit. Let $\mathcal{R}et$ be the map from geometry $A_n(q)$ which maps subspace W into uniquely determined representative $E(A)$ of the simplex in the orbit. It is easy to see that $\mathcal{R}et$ is homomorphism of $A_n(q)$ onto thin geometry A_n.

Let $\mathcal{F}=\{\langle e_1\rangle,\langle e_1,e_2\rangle,\dots,\langle e_1,e_2,\dots e_n\rangle\}$ be the standard maximal flag of $A_n(q)$. The relation $W_1\overset{C}{\iff}W_2$ holds if and if $\dim(W_1\cap W)=\dim(W_2\cap W)$ for each subspace W from the standard maximal flag. Notice that we have exactly n options. Classes of the above equivalence relation are known as *large Schubert cells*.

We can investigate another equivalence relation $W_1\overset{c}{\iff}W_2$ if and only if $\dim(W_1\cap W)=\dim(W_2\cap W)$ for each subspace W from the simplex Sim(n+1). In this definition subspace W can be chosen in $2^{n+1}-2$ distinct ways. The classes of equivalence relation $\overset{c}{\iff}$ are known as *small Schubert cells*. studies of such cells have various applications - theory hypergeometrical functions, coding theory and etc (see [48]).

Obviously, we can change finite field $\mathbb{F}_q$ for general field $\mathbb{F}$ in the written above definition and study projective geometry $PG_n(\mathbb{F})$ and its partition into small Schubert cells. In the case of algebraically closed field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F})=0$ there is a following nice topological definition of small cell.

Let us consider the action of group $T=T(n,\mathbb{F})$ of triangular matrices on the set $PG(n,\mathbb{F})$. The description of T orbits, i.e. classes of equivalence

relation $x\hat{O}y$ if and only if there exist g in T such that $g(x) = y$ is "*wild*" algebraic problem (see [47] and further references for the definition of algebraic wilderness). The description of classes as above heavily depends on the choice of field $\mathbb{F}$. We can consider the algebraic closure of this partition in Zarisski topology. Instead of orbit we can take the minimal topologically closed subset in $PG_n(\mathbb{F})$. D. Hilbert defined small Schubert sets as a collection of such subsets (see [55]).

Recall, that *algebraically closed sets in Zarisski topology* are simply sets of solutions of algebraic system of algebraic equations. It is interesting that the number of small $\mathrm{sch}(n)$ does not depend on the choice of $\mathbb{F}$ if parameter n is "sufficiently large". Function $\mathrm{cch}(n)$ is an important example of function which is hard to compute.

The number $g^m_{n+1}(q)$ of m-dimensional subspaces of $\mathbb{F}^m_q$ is known as *Gaussian binomial coefficient*. Group $GL_{n+1}(q)$ of order

$$(q^{n+1} - 1)(q^{n+1} - q) \dots (q^{n+1} - q^n)$$

acts transitively on subspaces of dimension m. The stabiliser of $\langle e_1, e_2, \dots e_m \rangle$ has order $|GL_m(q)| \cdot |GL_{n+1-m}(q)| q^{m(n+1-m)}$. It means that Gaussian binomial coefficient can be computed as

$$\frac{|GL_{n+1}(q)|}{|GL_m(q)| \cdot |GL_{n+1-m}(q)| q^{m(n+1-m)}}.$$

So the number $g^m_{n+1}(q)$ equals

$$\frac{(q^{n+1} - 1)(q^n - 1)(q^{n-1} - 1) \dots (q - 1)}{[(q^m - 1)(q^{m-1} - 1) \dots (q - 1)] \cdot [(q^{n+1-m} - 1)(q^{n+m} - 1) \dots (q - 1)]}.$$

We can assume that parameter q in the expression for Gaussian binomial equations can be any positive integer ≥ 2.

Lemma 1.4.1. $g^m_{n+1}(q) = C^m_{n+1} \bmod (q - 1)$

Proof. We can compute the number of m-dimensional subspaces as sum of Schubert cells orders of kind $q^{i_1+i_2+\dots+i_m-m/(m-1)/2}$. So we have C^m_{n+1} expressions equals to 1 mod $q - 1$.

□

Let us introduce *Schubert projective geometry*. We consider "*largest large*" *Schubert cells*, i.e. Schubert cells of maximal dimension as algebraic varieties. The list is the following, cell of size q^n containing $\langle e_n + 1 \rangle$, cell of size $q^{2(n-1)}$ with the representative $\langle e_n, e_{n+1} \rangle$, cell of size $q^{3(n-2)}$ with an element $\langle e_{n-1}, e_n, e_{n+1} \rangle$ from the simplex, ..., cell of size q^n with the hyperplane $\langle e_2, e_3, \dots, e_n \rangle$. The disjoint union of our cells with the restriction of I and t on it is a Schubert projective geometry $SPG(n, q)$.

1.5. Groups and Tits geometries

1.5.1. Group incidence system

An important example of the incidence system as above is the so-called *group incidence system* $\Gamma(G, G_s)_{s\in S}$. Here G is the abstract group and G_s, $s \in S$ is the family of distinct subgroups of G. The objects of $\Gamma(G, G_s)_{s\in S}$ are the left cosets of G_s in G for all possible $s \in S$. Cosets α and β are incident precisely when $\alpha \cap \beta \neq \emptyset$. The type function is defined by $t(\alpha) = s$, where $\alpha = gG_s$ for some $s \in S$.

One of the important direction in studies of groups is so called Combinatorial Group Theory which uses language of generators and generic relations.

Let $S = \{s_1, s_2, \ldots, s_n\}$ be a *finite alphabet*. We consider the totality $Fs(S)$ of all words in S. Let $w = s_{i_1}s_{i_2}\ldots s_{i_l}$ be the *word of length* $l = l(w)$ in our alphabet. The *empty word* e of length 0 will be also an element $Fs(S)$. We introduce the product (operation of concatenation) of $w^1 = s_{i_1}s_{i_2}\ldots s_{i_l}$ and $w^2 = s_{j_1}s_{j_2}\ldots s_{j_s}$ as word $w = s_{i_1}s_{i_2}\ldots s_{i_l}s_{j_1}s_{j_2}\ldots s_{j_s}$ of length $l + s$. It is easy to see that written above rule introduces a semigroup $Fs(S)$ with unity e i.e. $ew = we$ for each $w \in Fs(S)$. The semigroup $Fs(S)$ is known as *free semigroup*.

Obviously, in the case of nonempty word w the equation $wx = e$ does not have a solution.It means that nonempty word is not an invertible element of $Fs(S)$.

We may expand set $Fs(S)$ and introduce a *free group* $Fg(S)$ in the following way. Let S^{-1} be the collection of symbols s_1^{-1}, s_2^{-1}, ..., s_n^{-1}. We introduce a *cutting rules* as $s_i{s_i}^{-1} = e$ and ${s_i}^{-1}s_i = e$, $i = 1, 2\ldots, n$, and declare that the word $s'_{i_1}s'_{i_2}\ldots s'_{i_l}$, where $s'_{i_k} \in S \cup S^{-1}$, $k = 1, 2, \ldots, l$, is *irreducible* in case of absence $s'_{j_i}s'_{j_{i+1}} \neq e$ for $i = 1, 2, \ldots, n-1$ (cutting rules are not applicable).

We assume that ${s_i}^{-1} = s_i$ for each $i = 1, 2, \ldots, n$. The *inverse word* for $s'_{i_1}s'_{i_2}\ldots s'_{i_l}$ can be written as $s'^{-1}_{i_l}s'^{-1}_{i_{l-1}}\ldots s'^{-1}_{i_1}$. It is easy to see that $Fg(S)$ is group containing all elements of $Fs(S)$ as irreducible words. $Fg(S)$ is known as *free group*.

We may introduce additional cutting rules of kind $s'_{i_1}s'_{i_2}\ldots s'_{i_l} = e$ (*generic relations*) and consider new group of irreducible words. Combinatorial Group Theory contains a theorem, that any group can be obtained via list of generic relations.

Let G be the group with generators $g_1, g_2, \ldots g_n$, i.e. each $g \in G$ can be obtained as a product of several g_i. The rules $\phi(s_i) = g_i$, $i = 1, 2, \ldots, n$ define the *homomorphism* ϕ of free group $Fg(S)$ onto group G.

1.5.2. Coxeter systems and their geometries

Let (W, S) be a *Coxeter system*, i.e. W is a group with set of distinguished generators given by $S = \{s_1, s_2, \ldots, s_m\}$ and generic relation

$$(s_i \times s_j)^{m_{i,j}} = e.$$

Here $M = (m_{i,j})$ is a symmetrical $m \times m$ matrix with $m_{i,i} = 1$ and off-diagonal entries satisfying $m_{i,j} \geq 2$ (allowing $m_{i,j} = \infty$ as a possibility, in which case the relation $(s_i \times s_j)^{m_{i,j}} = e$ is omitted).

We obtain the diagram D on the set of nodes $1, 2, \ldots, m$ by putting edge between nodes i and j with *weight* equal to $m_{i,j} - 2$. As usually absence of edge corresponds to $m_{i,j} = 2$, weight is zero. Absence of weight at the edge between i and j means that $m_{i,j} = 3$ (weight is 1).

We saw that symmetric group S_{m+1} corresponds to the Coxeter system with diagram A_m. We may identify s_1 with the transposition $s_1 = (1, 2)$, $s_2 = (2, 3)$, $\ldots$, $s_m = (m, m + 1)$ and check that the image homomorphism ϕ of free group $Fg(S)$ given by rules $\phi(s_i) = (i, i + 1)$ is a Coxeter system (W, S) with diagram A_l and W is isomorphic to S_{l+1}.

Letting $W_i = \langle S - \{s_i\}\rangle$, $1 \leq i \leq m$ in the case of general Coxeter system we obtain a group incidence system $\Gamma_W = \Gamma(W, W_i)_{1 \leq i \leq m}$ called the *Coxeter geometry* of W. The W_i are referred to as the *maximal standard subgroups* of W (see [15]).

We saw that in the case of diagram A_l groups W_i are isomorphic to direct products of S_i and S_{m-i+1}, corresponding geometry is thin Tits geometry with diagram A_m. This fact holds in the general case (see, for instance [21], [56]).

Theorem 1.5.1. *Let (W, S) be the Coxeter system with the diagram D. Then the corresponding Coxeter geometry is thin flag transitive Tits geometry over diagram D.*

Example 1.5.2. (*Infinite Coxeter group with the diagram $\tilde{A}_1$*) Notice, that the group W and its geometry can be infinite objects. Obvious example is a geometry with the following diagram (Fig. 1.11).

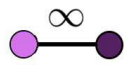


Figure 1.11. Diagram $\tilde{A}_1$

So generic relations are given by the list: $s_1^2 = e$ and $s_2^2 = e$. Irreducible words are $s_1 s_2 s_1 s_2 \ldots s_1 s_2$, $s_2 s_1 \ldots s_2 s_1$ in case of even length and

$s_1s_2s_1s_2 \dots s_2s_1$, $s_2s_1 \dots s_1s_2$ in case of odd length. The length of the product of two words w_1 and w_2 will be the sum of lengthes if the last character of w_1 differs from the first character of w_2, otherwise the length is the difference of lengthes. This Coxeter geometry is isomorphic to $T_{2,2}$.

Group and geometry can be infinite in the case of finite diagram. You can play with the case of $D = P_3$ (*ordinary triangle*) and produce infinitely many irreducible words.

1.5.3. Case of finite Coxeter groups

The following statement brings us the list of finite Coxeter groups.

Theorem 1.5.3. *Coxeter system (W, S) is finite ($|V| < \infty$) if and only if its digram belongs to the list diagrams in Table 1.1.*

Let us consider the description of all infinite families of Coxeter groups.

Figure 1.12. Diagram I_{m-2}

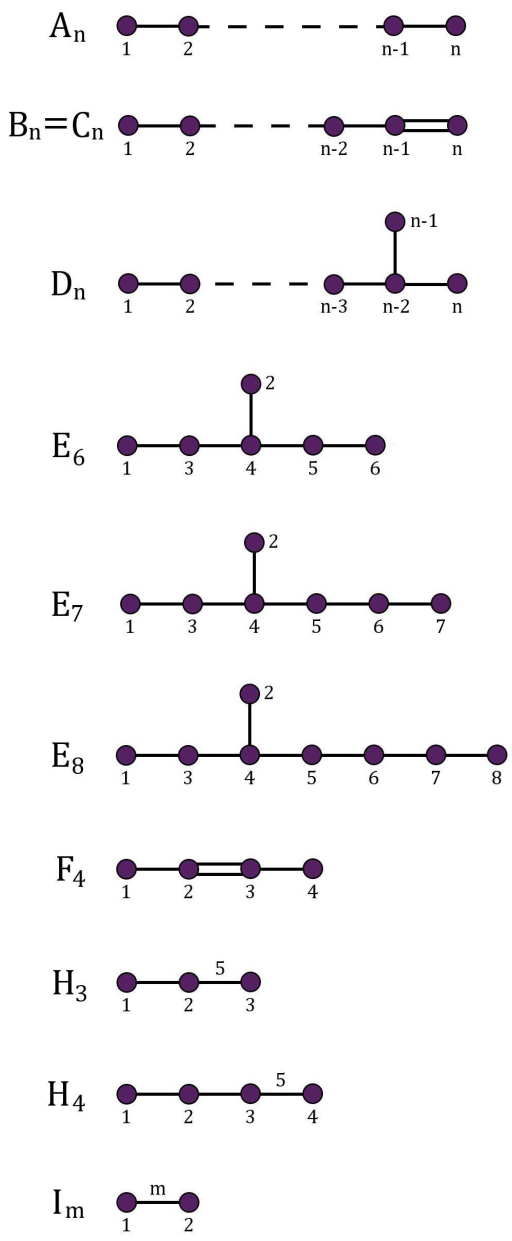
Example 1.5.4. (*Finite Coxeter group with the diagram I_{m-2}*) In case of diagram (Fig. 1.12) the geometry is orginary m-gon P_m. We have to generators s_1 and s_2 and unique generic relation $(s_1s_2)^m = e$.

The list of irreducible words contains $2m$ irreducible words e, s_1, s_2, s_1s_2, s_2s_1, ..., the maximal length of the word is m. We may identify s_1 and s_2 with mirror symmetries of P_m, which fix the line $[1, 2]$ together with incident points (1) and (2), so s_1s_2 is a rotation of regular polygon P_m corresponding to the angle $2\pi/m$.

We already discuss the case of Coxeter diagram B_n and corresponding group of transformations $x \to xA + \mathrm{b}$ of vector space $\mathbb{F}_2^n$, where $\mathrm{b} \in \mathbb{F}_2^n$ and A permutational matrix. We may identify set S of generators with permutational matrices corresponding to transpositions (12), (23), ..., $(n-1, n)$ and translation τ adding $1 \in \mathbb{F}_2$ to the last coordinate of vector x. It is easy to check that $\tau(n-1, n)$ has order 4. So τ corresponds to extremal right node of the diagram. The action of group $W = B_n$ on the left cosets by $W_n = \langle (12), (23), \dots, (n-1, n) \rangle$ is similar to natural action of B_n onto vector space $\mathbb{F}_2^n$. Hamming metrics corresponds to this action.

Let us change τ for τ' adding 1 to the last two coordinates of vector x. It is easy to see that τ commutes with linear transformation $(n-1, n)$ and generic relations between (12), (23), ..., $(n-1, n)$, τ' are "encoded"

Table 1.1. Diagrams of irreducible finite Coxeter systems



by diagram D_n. Group D_n can be identified with the subgroup of B_n which consist on map $\mathrm{x} \to \mathrm{x}A + \mathrm{b}$, where A is permutational matrix and coordinates $\mathrm{b} = (b_1, b_2, \ldots, b_m)$, satisfy to relation $b_1 + b_2 + \cdots + b_n = 0$. Action D_n on left cosets by $W_n = \langle (12), (23), \ldots, (n-1, n) \rangle$ is similar to natural action on vectors from hyperplane H given by equation

$$x_1 + x_2 + \cdots + x_n = 0.$$

This action corresponds to distance transitive metric for D_n which is the restriction of Hamming metrics onto the set of vectors from H.

Various descriptions and interpretations of "sporadic" thin flag transitive Tits geometries the redear can find in [15], [16], [43], [44].

1.5.4. On locally finite Coxeter geometries

Let us consider *locally finite Coxeter geometry* $\Gamma(W)$, where (W, S) is Coxeter system with $S = \{s_1, s_2, \ldots, s_m\}$. The length $l(w)$ of minimal irreducible representation of the word w is the minimal length of the irreducible word $s'_1 s'_2 \ldots s'_k$, $s'_i \in S$ which is equal to w. We introduce the set T of reflexions of W as the totality of elements of kind $g^{-1} s_i g$, $s_i \in S$, $g \in W$. The information on the element gW_i of type i can be given by word

$$w = s'^{-1} \in gW_i$$

with minimal length $l(w)$. We set $l(\beta) = l(w)$ for $\beta = gW_i$, $1 \le i \le m$.

We can introduce a triple $T^+(\beta)$, $T^0(\beta)$ and $T^+(\beta)$, where

$$T^+(\beta) = \{r \in T | l(r\beta) < l(\beta)\},$$
$$T^0(\beta) = \{r \in T | l(r\beta) = l(\beta)\},$$
$$T^+(\beta) = \{r \in T | l(r\beta) > l(\beta)\}.$$

In fact $T^+(\beta)$ is a collection

$$\{s'_1, s'_1 s'_2 s'_1, s'_1 s'_2 s'_3 s'_2 s'_1, \ldots, s'_1 s'_2 \ldots s'_n s'_{n-1} \ldots s'_1\}.$$

Let us treat string

$$\beta, T^+(\beta), T^0(\beta), T^-(\beta), i$$

as a code of an element $\beta \in \Gamma_i(W)$. As it was proven in [169] the condition of incidence of β', $T^+(\beta')$, $T^0(\beta)$, $T^-(\beta)$, i is the following relation:

$$|T^+(\beta) \cap T^-(\beta')| = |T^-(\beta) \cap T^+(\beta')| = 0.$$

We can rewrite this condition in the form: $T^+(\beta')$ is a subset $T^+(\beta) \cup T^0(\beta)$ and $T^+(\beta)$ is a subset $T^+(\beta') \cup T^0(\beta)$.

So we can investigate an adjacency matrix of induced subgraph I_k for the graph I with the vertex set

$$\{\beta \in \Gamma(W) | l(\beta) \leq k\}$$

by the following algorithm
1. Create $T_{2k-1} = \{r \in T | l(r) \leq 2k-1\}$
2. Encode β via string $T^+(\beta), T^0(\beta), T^-(\beta)$
3. check the written above condition of incidence of β and β' for time $O(|T_{2k-1}|)$.

In case of finite Coxeter system we have to change T_{2k+1} for T [169]. Elements of T are in one to one correspondence with positive roots. The implementation of the above algorithm can be done with in GAP software. In the Appendix we put the description of root systems for finite Weyl groups.

1.6. Cartan matrices and Coxeter groups

Let $A = (a_{i,j})$, $i, j \in M$, $|M| = m$ is a matrix with the integer entries, such that $a_{i,i} = 2$ for $i \in M$, and $(a_{i,j} = 0) \Rightarrow a_{j,i} = 0$. We refer to A as *Cartan matrix*.

Let us consider the *integer lattice*, denoted by $\mathcal{L}at(A)$ spanned by formal elements $\alpha_1, \alpha_2, \ldots \alpha_m$ (*simple roots*) and introduce the transformations r_i acting on the lattice according to rule:

$$r_j(\alpha_i) = \alpha_i - a_{i,j}\alpha_j.$$

We refer to the group $W(A)$ generated by r_j, $j \in M$ as *Weyl group* of matrix A.

Lemma 1.6.1. *Group $W(A)$ is a Coxeter system with the diagram for which nodes i and j are joint by the edge with the weight $n_{i,j}$, where $a_{i,j}a_{j,i} = 0$, 1, 2, 3 implies $n_{i,j} = 0$, 1, 2, 4, respectively, and $(a_{i,j}a_{j,i} \geq 4)$ implies $n_{i,j} = \infty$.*

The group is finite if and only if A is nonsingular matrix. Each crystallographic Coxeter group (case of weights $1, 2, 4, \infty$ on the edges of diagram) can be obtained as $W(A)$.

We refer to the set Δ of all elements of kind $g(\alpha)$, $i \in M$ from the lattice $\mathcal{L}at(A)$ as set of *real roots*. We can prove the set Δ is partited into subsets Δ^+ of *positive roots* (linear combinations of simple roots with nonpositive coefficients) and Δ^- of *negative roots* (combinations of simple roots with nonnegative coefficients). For each simple root α_i, $i = 1, 2, \ldots$ we

introduce the *dual element* ${\alpha_i}^*$, which is a linear function $l(x)$ from $\mathcal{L}at(A)$ into Z, such that $l(\alpha_i) = 1$ and $l(\alpha_j) = 0$ for $j \neq i$. Notice, that group $W(A)$ acts naturally on linear functions $l(x)$ from dual lattice for $\mathcal{L}at(A)$: $g(l(x)) = l(g(x))$.

Let $H_i = H_i(A)$ be the orbit of group $W(A)$, which contains ${\alpha_i}^*$. We consider an incidence structure defined on the set $H(A) = H_1 \cup H_2 \cup \cdots \cup H_m$ with the type function $t(h(x)) = i \iff x \in H_i$ and incidence relation $hIh' \iff h(x)h'(x) \geq 0$ for all $x \in \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$

The following statement the reader can find in [151], [153].

Proposition 1.6.2. *The incidence system $H(A)$ is isomorphic to Coxeter geometry $W(A)$.*

The information on element h in $H(A)$ can be given by string

$$(h(\alpha_1), h(\alpha_2), \ldots, h(\alpha_m), i),$$

where i is the type of elements. So we can check the incidence of elements for time $O(m)$.

If Γ is a finite subset of $H(A)$ of cardinality k, then adjacency matrix of Γ can be computed for time $O(k^2 m)$.

In the case of finite group $W(A)$ linear functions ${\alpha_i}^*$ corresponds to fundamental weights f_i. Linear function α_i^* can be given as a map

$$x \to (f_i, x),$$

where scalar product $(\cdot, \cdot)$ is defined by *Killing form* (see [43], [44]).

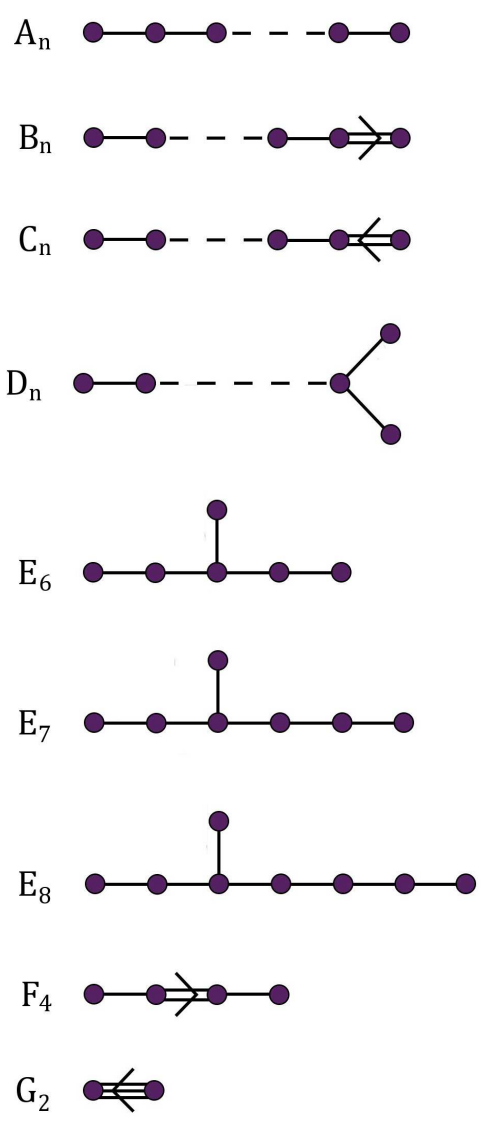
We assume that Cartan matrices A_1 and A_2 are equivalent if corresponding Weyl groups $W(A_1)$ and $W(A_2)$ act similarly on lattices $\mathcal{L}at(A_1)$ and $\mathcal{L}at(A_2)$. If the Coxeter diagram $W(A)$ is different from B_l, then class of equivalent matrices is uniquely defined by diagram: $A_1 \iff A_2$ if and only if diagrams for $W(A_1)$ and $W(A_2)$ coincide. There are exactly two classes of equivalent Cartan matrices in the case of diagram B_n, $n \geq 3$. Each claa is denoted by the directed graph which can be obtained by putting the double arrow instead of the underected edge with weight 2. This way we obtained two "Coxeter-Dynkin" diagrams B_n and C_n. In case of Weyl groups we will use term *Coxeter-Dynkin diagrams*. We are not discussing here the symbolic meaning, of the directions (from left to right or opposite). We simply will put the list of positive roots in both cases B_n and C_n in the Appendix (last pages of manuscript).

Theorem 1.6.3. *The list of finite Weyl groups is given by the list of diagrams in table 1.2.*

In case of rank $(A) = m - 1$ we use term *affine Coxeter-Dynkin diagram*.

Theorem 1.6.4. *The affine Coxeter matrix uniquely defined up to equivalence by its Coxeter-Dynkin diagrams from the list given in Table 1.3.*

Table 1.2. Coxeter-Dynkin diagrams



1.7. On general constructions of thick flag transitive Tits geometries

1.7.1. On the axioms of BN-pairs and Schubert geometries

Let G be a group, B and N subgroups of G, and S a collection of cosets of $B \cap N$ in N. We call (G, B, N, S) a *Tits system* (or we say that G *has a* BN*-pair*) if

$(BN1)$ $G = \langle B, N\rangle$ and $B \cap N$ is normal in N,
$(BN2)$ S is a set of involutions which generate $W = N/(B \cap N)$,
$(BN3)$ sBw is a subset in $BuB \cup BswB$ for any $s \in S$ and $w \in W$,
$(BN4)$ $sBs \neq B$ for all $s \in S$.

Properties $(BN1)$-$(BN4)$ imply that (W, S), $S = \{s_1, s_2, \ldots, s_m\}$, is a Coxeter system (see [15], [142]). Whenever (G, B, N, S) is a Tits system, we call the group W the *Weyl group of the system*, or more usually the *Weyl group* of G. The subgroups P_i of G defined by BW_iB are called the *standard maximal parabolic subgroups* of G, where $W_i = \langle S - \{s_i\}\rangle$, $1 \leq i \leq m$. The group incidence system $\Gamma_G = \Gamma(G, P_i)_{1 \leq ilel}$ is commonly referred to as the *Lie geometry* of G (see [15]).

Note that the Lie geometry of G and the Coxeter geometry of the corresponding Weyl group have the same rank. In fact there is a type preserving morphism from Γ_G onto Γ_W given by $gP_i \to wW_i$, where w is determined from the equality $BgP_i = BwP_i$. This morphism is called a *retraction* (see [16]).

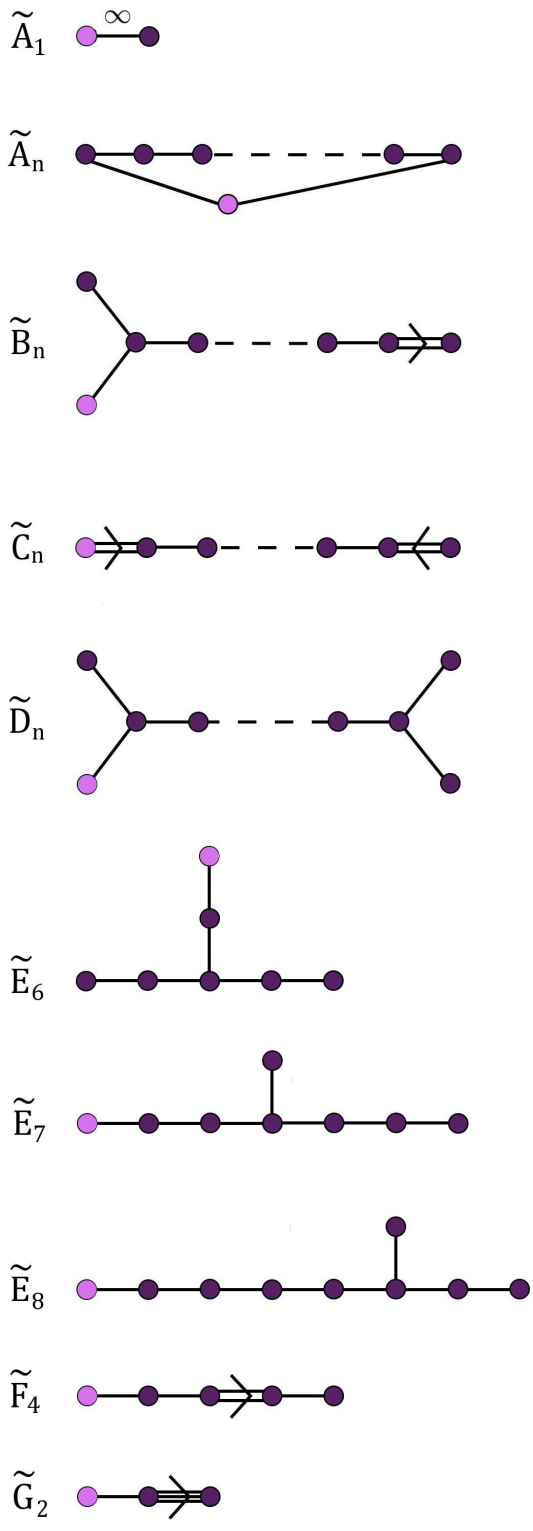
Let G be a group with a BN-pair (a Tits system (G, B, N, S) in the sense of [15]) and (W, S) be the corresponding Coxeter system. The maximal subgroups of the group G containing B (the maximal standard parabolic subgroups) have the form $P_i = BW_iB$, $1 \leq i \leq m$. It can be shown that the incidence system $\Gamma(G, G_s)$ is a Tits geometry. This geometry is called the *geometry of the* BN*-pair* or the geometry of G.

Written above text means that we can get thick Tits geometry if finite BN pair is exist. At the moment we move from system of axioms on combinatorial level (definitions of geometry over the diagram and Tits geometry) to the system of axioms in the language of group theory.

Example 1.7.1. (*BN-pairs for the projective geometry*) We start with the explicit description of BN- pair related to the Group $GL_{n+1}(q)$ to show that some BN-pairs are really exist.

The unitriangular subgroup $U(n+1, q)$, which consist of all matrices $(a_{i,j})$, such that $j > i \Rightarrow a_{i,j} = 0$ and for each i entry $a_{i,i} = 0$, maximal torus $T = T_{n+1}(q)$, which contains all elements of kind $\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_{n+1})$ and group of permutational matrices S_{n+1} are subgroups of $GL_{n+1}(q)$. We

Table 1.3. Affine Coxeter-Dynkin diagrams



may check that that group $B_{n+1}(q)$ of triangular matrices which is minimal subgroups, which contains $T_{n+1}(q)$ and $U_{n+1}(q)$, together with the group $N = N_{n+1}(q)$ of monomial matrices for which exactly one entry of each row differs from zero, form BN-pair.

The *maximal standard parabolic subgroup*, i.e group X, such that $B_{n+1}(q) < X < GL_{n+1}(q)$ is a totality of matrices P_i

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix},$$

where A is $i \times i$ matrix with $\det(A) \neq 0$, and $\det(B) \neq 0$.

The standard parabolic subgroup P_i, $i = 1, 2, \ldots, n$ is a stabiliser of subspace $\langle e_1, e_2, \ldots, e_i \rangle$. It means that cosets of kind gP_i are in natural one to one correspondence with i-dimensional subsets of $\mathbb{F}_q^{n+1}$. The reader can use this correspondence to show the existence of isomorphism between incidence system of left cosets by P_i and projective geometry $PG(n, q)$.

We can check that subgroups $SL_{n+1}(q) \cap N_{n+1}(q)$ and $SL_{n+1}(q) \cap B_{n+1}(q)$ form a BN-pair for $SL_{n+1}(q)$. Factorization of $SL_{n+1}(q) \cap N_{n+1}(q)$ and $SL_{n+1}(q) \cap B_{n+1}(q)$ by subgroup $S = S_{n+1}(q)$, which is a the totality of scalar matrices, will provide simple group $PSL_n(q)$ with the structure of BN-pair.

Let us consider the action of group B onto left cosets of kind gP_i.

We refer to the orbits of this action as *large Schubert cells* for $\Gamma(G)$ they are in one to one correspondence with the double cosets of kind BgP_i. It can be prowen that there is unique represantative $w \in W_i$ of the shortest length such then $BgP_i = wW_i$. Let $\mathcal{R}etr$ be the map from $\Gamma(G)$ such that $\mathcal{R}etr(gP_i) = wW_i$ if an only if BgP_i. The map $\mathcal{R}etr$ is a homomorphism of $\Gamma(G)$ onto $\Gamma(W)$ (*retration map*).

Let us consider groups of kind $w^{-1}Bw$, $w \in W$ and equivalence relation $gP_i \iff g'P_i$ if and only if there exist $w \in W$ such that cosets gP_i and $g'P_i$ are in the same orbit of $w^{-1}Bw$. We refer to classes of this equivalence relation as *small Schubert cells of Tits geometry* $\Gamma(G)$.

Let G be a split finite BN-pair with cooresponding geometry $\Gamma(G)$. Let us consider the largest orbits of Borel subgroup B acting on $\Gamma(G)$, i.e. orbits corresponding to double coset GwP_i with maximal $l(wW_i)$ for each $i = 1, 2, \ldots, n$. As it follows directly from definition disjoint union $[\Gamma]$ ("integer part" of Tits geometry) with the restriction of incidence I and type function t on this set is a flag transitive incidence system. In fact, Borel subgroup B acts transitively on the totality of maximal flags (cosets of kind gB, $g \in G$. We refer to this incidence system as *Schubert geometry* and use notation $\mathrm{Sch}(\Gamma(G))$.

Let us consider class of finite BN-pairs of rank 2. For each thick m-gon from this class $m \in \{3, 4, 6, 8\}$ we consider biregular incidence structure $\mathrm{Sch}(\Gamma(G))$. Tis incidence structure $a(m) = a_{q^r,q^s}(m)$ is uniquely determined by the triple m, q^r, q^s, where last two parameters stands for the bidegrees of corresponding incidence graph. We refer to $a(m)$ as affine part of generalised m-gon (see [156]). We associate with the general Schubert geometry $\mathrm{Sch}(\Gamma(G))$ the diagram obtained from diagram of $\Gamma(G)$ simply by the change of weight $m-2$ of the edge for symbol $a(m)$. It is easy to see that Schubert geometry $\mathrm{Sch}(\Gamma(G))$ is a diagram geometry over new diagram.

The idea of diagram geometry allows easily expand the class of geometry. For instant adding some new incidence structures to the list of generalised polygons brings famous class of Buekenhout-Tits geometries, which contains geometries of finite nonabelian sporadic groups together with the geometries of BN-pairs (see [18], [19]).

1.7.2. On Lie algebras, Schevalley groups and their geometries

In this section we associate Tits system of kind (G, B, N, S) with each Chevalley group G. Recall, that C. Shevalley for each pair $(X_l, \mathbb{F})$, where $\mathbb{F}$ is general field and X_l is a Coxeter - Dynkin diagram for the Weyl group associated with the Cartan matrix A of dimension l, $\det(A) \neq 0$, constructed simple group $G = X_l(\mathbb{F})$ to signify that G is the *Chevalley group* over the field $\mathbb{F}$, with associated Dynkin diagram X_l. We are most interested in the case when $\mathbb{F}$ is finite, and we shall write $X_l(q)$ instead of $X_l(\mathbb{F}_q)$ in that case.

Let, fixe Chevalley group $G = X_l(\mathbb{F})$ with Weyl group defined by Coxeter Dynkin diagram. As in the previous section Γ_W and Γ_G are associated with G thin and thick Tits geometries, respectively.

The axioms of BN-pairs are very convenient for the investigations Of geometrical properties. We may easily generalise the concepts of large and small Schubert cells and retraction map for the geometry of general BN-pair.

Simple Lie group of normal type (*Shevalley groups* in other terminology) had been obtaines as groups of internal automorphism of simple groups. We introduce briefly the method by C. Shevalley (see [132], [135]) with the usage of some ideas from Kac-Moody Algebras Theory ([63], [64], [65]). Let us assume for a while that $\mathbb{F}$ is general algebraic field. Lie algebra $\mathcal{L}$ is a vector space over $\mathbb{F}$ with the bilinear product $[x, y]$, for which the relations

$$[x, y] + [y, x] = 0$$

and

$$[x, [y, z]] + [y, [z, x]] + [z[x, y]] = 0$$

hold for all vectors x, y, z from $\mathcal{L}$.

For each $x \in \mathcal{L}$ we can consider the linear transformation $a \to [a, x]$, $a \in \mathcal{L}$. The standard notation for this map is $\mathrm{ad}(x)$. For $x, y \in \mathcal{L}$ we consider the bilinear symmetric form

$$(x, y) = Tr(\mathrm{ad}(x)\mathrm{ad}(y)),$$

where operator Tr is a trace of linear map.

Let $A = (a_{i,j})$, $i, j \in M$ be an arbitrary finite Cartan matrix.

Let us denote as $\mathcal{L}(A)$ special Lie algebra over the general field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = 0$ with distinguished generators e_i, f_i, h_i, $i \in M$, which satisfy to following conditions

$$\begin{aligned}
&[e_i, f_j] = \sigma_{i,j},\\
&[h_i, h_j] = 0,\\
&[h_i, e_j] = a_{i,j}e_j,\\
&[h_i, f_j] = -a_{i,j}f_i,\\
&(\mathrm{ad}(e_i))^{1-a_{i,j}}(e_j) = (\mathrm{ad}(f_i))^{1-a_{i,j}}(f_j) = 0,\ i \neq j.
\end{aligned}$$

This Lie algebra is known a *Kac-Moody algebra*.

It is easy to check that in case $\det(A) = 0$ the dimension of algebra $\mathcal{L}(A)$ is infinity, we can obtain infinite BN- pairs corresponding to $\mathcal{L}(A)$. In this section we are concentrated on finite dimensional objects. So, we assume that $\det(A) = 0$. Elements $h_1, h_2, \ldots, h_n$ form a basis of Cartan subalgebra $\mathcal{L}_0$. It is abelian subalgebra $[h, h'] = 0$ for $h, h' \in \mathcal{L}_0$.

We define the simple roots α_i, $i = 1, 2, \ldots, m$ in dual space $\mathcal{L}_0^*$ for the Cartan subalgebra via relations $h_i(\alpha_j) = a_{i,j}$, $i, j \in M$. As it follows from condition $\det(A) \neq 0$ roots α_i are linearly independent. Let $\mathcal{L}_\alpha$ denote the totality of $\mathrm{x} \in H^*$, such that

$$[h, x] = h(\alpha)$$

for arbitrary $\alpha \in \mathcal{L}^*$. We refer to α as a *root* if $\dim(\mathcal{L}_\alpha) \neq 0$. The totality of such elements α form so called root system Δ for Cartan matrix A. It agrees with the previous definition of real roots. In case nonsingular matrix A all roots are real and $\dim(\mathcal{L}_\alpha) = 1$ for each root α. Lie algebra $\mathcal{L}$ can be treated as directed sum

$$\mathcal{L}(A) = \mathcal{L}_0 + \sum_{\alpha \in \Delta} \mathcal{L}_\alpha.$$

We can choose basis of simple roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ and partite all roots in the set of positive roots and Δ^+ (totality of linear combinations of basic roots with nonnegative coefficients) and Δ^- consisting on negative roots.

Basis of lie algebra consisting on e_i, h_i, f_i can be expanded to the basis of the entire vector space $h_i \in \mathcal{L}_0$, $e_\alpha \in \mathcal{L}_\alpha$ such that Lie product of each two basic elements is a linear combinations of basic elements with integer coefficients. The existence of such basis was great break through by C. Chevalley. It allows to define our object $L(A)$ over arbitrary field. We are particularly interested in the case of $\mathbb{F}_q$. Notice, that

$$[e_\alpha, e_\beta] = 0$$

if $\alpha + \beta$ is not a root, and

$$[e_\alpha, e_\beta] = r_{\alpha+\beta} e_{\alpha+\beta}$$

in opposite case.

Let us consider BN-pairs corresponding to algebra $\mathcal{L}(A)$ over various fields $\mathbb{F}$. Let $(\mathcal{L}(A), \mathrm{ad})$ be adjoint representation of $\mathcal{L}(A)$. As it follows from the definitions transformations

$$\exp(\mathrm{ad}(\lambda e_i))(v) = \sum_{n\geq 0} (1/n!)\lambda^n (\mathrm{ad}(e_i))^n (v),$$
$$\exp(\mathrm{ad}(\lambda f_i))(v) = \sum_{n\geq 0} (1/n!)\lambda^n (\mathrm{ad}(f_i))^n (v),$$

are well defined automorphisms for arbitrary $t \in \mathbb{F}_q$.

In case of $\mathrm{char}\, \mathbb{F} = 0$ we may assume that $\mathcal{L}at(A)$ with basic elements ${\alpha_i}^*$ is a collection of vectors from the Cartan algebra $\mathcal{L}_0$. The orbits

$$H_i = \{w({\alpha_1}^*) | w \in W(A)\}$$

of Weyl group and their union H are also subsets of $\mathcal{L}_0$. Recall that we treat the set H as an incidence system. Linear functionals $l_1(x)$ and $l_2(x)$ are incident if and only if products $l_1(\alpha) l_2(\alpha) \geq 0$ for all roots α corresponding to Cartan matrix A. The *type function* t is defined by $t(l(x)) = i$ where $l(x) \in H_i$. We already discussed the isomorphism of (H, I, t) and Coxeter geometry $\Gamma(W)$. In fact there is a unique isomorphism of Γ_W with (H, I, t), which sends W_i to α_i, $1 \leq i \leq m$.

We now consider an analogous embedding of the Lie geometry Γ_G into the Borel subalgebra $\mathcal{B} = \mathcal{L}_0 + \mathcal{L}^+$ of $\mathcal{L}$. Let $d = {\alpha_1}^* + {\alpha_2}^* + \cdots + {\alpha_m}^*$. Than we can take

$$\Delta^+ = \{\alpha \in \Delta | d(\alpha) \geq 0\}$$

to be our set of positive roots in Δ. For any $l(x) \in \mathcal{L}at(\mathcal{L})$ define

$$\Delta^-(l) = \{\alpha \in \Delta^+ | l(\alpha) < 0\}.$$

Let $\mathcal{L}_\alpha$ be the root space corresponding to positive root α. For each $h \in H$ from $\mathcal{L}at(A)$ we define the subalgebra $\mathcal{L}_h$ as the sum of $\mathcal{L}_\alpha$, $\alpha \in \delta^-(h)$. Let

$$\mathcal{B}_i = \{(h, v) | h \in H_i, v \in L_h\}$$

and $\mathcal{B}(A)$ is a disjoint union of $\mathcal{B}_i$.

Let us introduce h' for $h \in \mathcal{L}at(A)$, where

$$h = x_1\alpha_1^* + x_2\alpha_2^* + \cdots + x_m\alpha_m^*,$$

simply as linear combination of kind

$$[x_1(\mathrm{mod}\, p)]\alpha_1^* + [x_2(\mathrm{mod}\, p)]\alpha_2^* + \cdots + [x_m(\mathrm{mod}\, p)]\alpha_m^*$$

if $\mathrm{char}\, \mathbb{F} = p$ and in case of $\mathrm{char}\mathbb{F} = 0$ we set

$$h' = h.$$

We can check that values of $l(\alpha)$, where $l(x) \in \mathcal{L}at$ and α in $\mathcal{L}_0$ are < 5 . So, the embedding of H into $\mathcal{L}_0$ is still working for a field $\mathbb{F}$ of characteristic ≥ 5 . So we may use it in the case of finite field.

We give $\mathcal{B} = \mathcal{B}(A, \mathbb{F})$ the structure of an incident system as follows. Elements (h_1, v_1) and (h_2, v_2) are incident if and only if each of the following hold:

(i) $h_1(\alpha)h_2(\alpha) \geq 0$ for all $\alpha \in \Delta$, i.e. it means that h_1 and h_2 are incident in (H, I, t).

(ii) $[h_1' + v_1, h_2' + v_2] = 0$

Element (h, v) has type i if $h + v \in U_i$.

In [151] it is shown that this newly defined incident system is isomorphic to the Lie geometry Γ_G, provided that the characteristic of K is zero or sufficiently large to ensure the isomorphism at the level of the subgeometries (H, I, t) and Γ_W. Then analogous to the Weyl case, there exists a unique isomorphism $\mathcal{R}etr$ of $\Gamma(G)$ into $(\mathcal{B}, I, t)$ which sends P_i to α_i, $1 \leq i \leq l$. The following statement

Theorem 1.7.2. *Let $\Gamma(A, q) = \Gamma(G)$ be the Tits geometry of finite group $G = X_n(q)$ corresponding to Cartan matrix A,* $\mathrm{char}(\mathbb{F}_q) \geq 5$. *Then Γ is isomorphic to the incidence system $(\mathcal{B}(A, \mathbb{F}_q), I, T)$*

$\Gamma(A, q)$ in $O(|\Gamma|)$ elementary steps and check whether or not two elements of Γ are incident for time $O(N^2)$, where N is the number of positive roots.

Corollary 1.7.3. *Geometry $\Gamma(A, q)$ o can be generated in computer memory in time $O(|\Gamma|)$. The check whether or not two elements of Γ are incident can be $O(m^2)$, where m is the number of diagram nodes.*

Interpretation of the geometry of group G with BN-pair in the form of $U(A, \mathbb{F})$ is convenient for studies of small Schubert cells. Rather fast general algorithms for check whether or not two elements from $\Gamma_i(G)$ are from the Small Schubert cell is introduced in [173].

From the mentioned above constructions we can get the following description if Schubert geometry $\mathrm{Sch}(\Gamma(G))$. We have to take elements $(-\alpha_i^*, v_i)$, $v_i \in \mathcal{L}_h$, $h = -\alpha_i^*$ and consider the incidence of $(-\alpha_i^*, v_i)$ and $(-\alpha_j^*, v)$, $i \neq j$ defined by the relation:

$$[-\alpha_i^* + v_i, -\alpha_j^* + v_j] = 0.$$

Remark 1.7.4. The change of subalgebra $\mathcal{L}_h$, which is a direct sum of $\mathcal{L}_\alpha$, such that $h(\alpha) > 0$ for $\mathcal{L}'_h$ which is direct sum of $\mathcal{L}_\alpha$, $h(\alpha) \leq 0$ will lead to isomorphic incidence system. It follows from the fact that elements α_i^* and $-\alpha_i^*$ both are elements of the same orbit of transformation group $(W(A), \mathcal{L}at(A))$

In fact we can consider similar incidence systems in the case of affine Coxeter-Dynkin diagram (see [166] , [170], [171]). Families of subalgebras $\mathcal{L}_h$ and $\mathcal{L}'_h$ in this case lead to distinct geometrical objects. The list of diagrams related to the case when the rank of Cartan matrix is $m - 1$ is above.

The theory of root system in the case of rank A differs seriously from the case of nonsingular matrix. We have to use so called "imaginary" roots together ith real roots (conjugates of basic roots in the Weyl group).

In the example of diagram $\tilde{A}_1$ the imaginary roots are of kind $c(\alpha_1 + \alpha_2)$, where c can be arbitrary nonzero integer. Totality Of real consist on elements of kind $k\alpha_1 + (k+1)\alpha_2$ or $(k+1)\alpha_1 + k\alpha_2$, where k is arbitrary integer.

In this book we introduce only Schubert geometry defined for the case of general Cartan matrix A in the following way.

We have to take subalgebra $\mathcal{L}^+(A)$ over the field $\mathbb{F}$, which is a direct sum of subspaces $\mathcal{L}_\beta$, where β is positive root (real or imaginary) from the root system corresponding to Cartan matrix A. It is easy to see that in case of singular matrix Borel subalgebra is infinitedimensional vector space.

Foe each $i \in M$ we consider the subalgebra L_i, which is a direct sum of root spaces $\mathcal{L}_\beta$, such that β is positive and $\alpha_i^*(\beta) \neq 0$. The incidence system consist on elements (α_i^*, v_i), $v_i \in L_i$, incidence of (α_i^*, v_i) and (α_j^*, v_j), $i \neq j$ is defined by the relation: $[\alpha_i^* + v_i, \alpha_j^* + v_j] = 0$. The type function is defined simply by relation $t(\alpha_i^*, v_i) = i$.

To avoid problems in case of small characteristic we can work with "deformated" Lie product $[\alpha_i^*, \beta] = \beta$ if $\alpha_i^*(\beta) \neq 0$. It means that $[\beta, \alpha_i^*] = -\beta$. We set $[e_{\beta_1}, e_{\beta_2}] = e_{\beta_1+\beta_2}$, if $\beta_1 + \beta_2$ is also a positive root and $\beta_1 > \beta_2$

according to natural lexicographical order on positive roots. Notice, that if $\beta_2 > \beta_1$ we need to write $-e_{\beta_1+\beta_2}$ in the right hand side.

We refer to the above incidence system as *Schubert geometry* $\mathrm{Sch}(A, \mathbb{F})$ with Cartan matrix A over the field $\mathbb{F}$.

Remark 1.7.5. If $\det A \neq 0$ then incidence system $\mathrm{Sch}(A, \mathbb{F})$ coincides with the Schubert geometry of some BN-pair.

Remark 1.7.6. An interesting new incidence systems can be obtained from $\mathrm{Sch}(A, \mathbb{F})$ via the deformation rules. For instance rule $[e_{\beta_1}, e_{\beta_2}] = e_{\beta_1+\beta_2}$, if $\beta_1 + \beta_2$ is also a positive root and one of the roots β_1, β_2 is simple.

Natural approximations of infinite graph $\mathrm{Sch}(A, \mathbb{F})$ can be obtained in the following way.

Let us take the set Δ_n of n first positive roots β_1, β_2, $\ldots$, β_n according to lexicographical order and consider subspace $\mathcal{L}_n = \mathcal{L}^+(A, \mathbb{F}, n)$, which is directed sum of $\mathcal{L}_{\beta_i}$, $i = 1, 2, \ldots, n$. We can consider bilinear product such that $[e_{\beta_i}, e_{\beta_j}] = e_{\beta_i+\beta_j}$ if $\beta_i + \beta_j \in \Delta_n$ and $[e_{\beta_i}, e_{\beta_j}] = 0$ if $\beta_i + \beta_j$ does not belong to Δ_n.

We define an incidence system $\mathrm{Sch}(A, \mathbb{F}, n)$ simply by the change of $\mathcal{L}^+(A)$ for finite dimensional space $\mathcal{L}_n$.

Proposition 1.7.7. *Let A be a singular Cartan matrix. Then natural projective limit of incidence systems* $\mathrm{Sch}(A, \mathbb{F}, n)$ *coincides with* $\mathrm{Sch}(A, \mathbb{F})$.

Chapter 2

Distance regular graphs, small world graphs and generalisations of Tits geometries

2.1. On Tits geometries, association schemes and distance regular graphs

Theory of association schemes is one of the important directions of Algebraic Combinatorics.

Association scheme Ω consist of finite set X and a collection of binary relations R_0, R_1, ..., R_d, such that

1. $R_0 = \{(x,x)|x \in X\}$
2. for each i, $i = 1, 2, \ldots, d$ the inverse relation

$$R_i^{-1} = \{(x,y)|(y,x) \in R_i\}$$

coincides with some R_j from the collection.

3. for $i, j, k \in \{0, 1, 2, \ldots, d\}$ the number

$$p_{i,j}^k = p_{i,j}^k(a,b) = |\{x \in X|(a,x) \in R_i, (x,b) \in R_j\}|$$

does not dependend on the choice of the pair $(a,b) \in R_k$

Let (G,X) be the transitive permutation group acting on the set X. *Orbitals* of (G,X), i.e. orbits of natural action of G on the set $X \times X$, are binary relations (subsets of Cartezian product of X with itself). Let $a \in X$ and

$$H = \{g \in G|g(a) = a\},$$

then orbitals of (G,X) are in one to one correspondence with double cosets HgH, $g \in G$.

For each directed graph R_i of associative scheme we consider its adjacency matrix A_i of size $|X| \times |X|$ with entries $a_{x,y}^i \in \{0,1\}$ such that $a_{x,y}^i = 1$ if and only if $(x,y) \in R_i$. As it follows from definition matrix product of A_i and A_j is $\sum p_{i,j}^k A_k$.

So the vector subspace $A(\Omega) = \langle A_0, A_1, A_2, \ldots, A_d\rangle$ in $M_n(\mathbb{C})$, $n = |X|$ (matrix algebra over the field $\mathbb{C}$ of complex numbers) is closed under matrix multiplication. Such algebras appeared in different areas of mathematics under different names such as *Bose-Messner algebra*, *cellular algebras*, *V-Shur rings* (see [2], [18], [29], [47]). We will use term *Bose Messner algebra* in this book. In the case of association schemes of orbitals for permutation group (G,X) we will use term *Hecke algebra* (see [15]) instead of Bose Messner algebra. Hecke algebra $\mathcal{H} = \mathcal{H}(G,X)$ can be identified with the centralizator of the totality of all permutations from (G,X):

$$\mathcal{H} = \{M \in M_n(\mathbb{C})|A_\pi M = M A_\pi \text{ for all } \pi \in G\}$$

A_π here is a permutational $n \times n$ matrix corresponding to permutation π.

We can consider also the totality HG of formal linear combinations of formal symbols a_0, a_1, ..., a_d such that relations

$$a_i \times a_j = \sum z_{i,j}^k a_k$$

give us definition of associative algebra with unity a_0. This object is known in Functional Analisis as *hypergroup* (see [53], [54]). Notice that hypergroup is an abstract algebra with fixed basis a_0, a_1, ..., a_d and integer structure constants $p_{i,j}^k \geq 0$.

We will refer to nonisomorphic matrix Bose-Messner algebras with the same hypergroups as *hyperequivalent BM algebras*.

Let us consider the concept of fusion hypergroup. With the equivalence relation τ on the set $\{1, 2, \ldots, d\}$ formed by classes T_1, T_2, ..., T_r we can associate algebraic elements

$$\begin{aligned} a(T_1) &= \sum_{i \in T_1} a_i, \\ a(T_2) &= \sum_{i \in T_2} a_i, \\ &\ldots \\ a(T_r) &= \sum_{i \in T_r} a_i. \end{aligned}$$

In case, when $a(T_1)$, $a(T_2)$, ..., $a(T_r)$ form a basis of subalgebra HG_τ in HG we refer to a new hypergroup as *fusion hypergroup* of HG and refer to τ as *fusion equivalence*. Let Ω be association scheme, we use notations $BM(\Omega)$ and $HG(\Omega)$ for corresponding Bose-Messner algebra and hypergroup, respectively.

Notice, that the existence of fusion hypergroup $HG_\tau(\Omega)$ in the hypergroup of association scheme Ω means that the binary relation R_0 and $R'_j = \bigcup R_i$, $i \in T_j$, $j = 1, 2, \ldots, r$ form new association scheme $\Omega' = \Omega_\tau$ and $BM(\Omega') = BM_\tau(\Omega)$ is a subalgebra in $BM(\Omega)$, $HG(\Omega') = HG_\tau(\Omega)$.

Let us assume that association schemes Ω^1 and Ω^2 are hyperequivalent and τ is a fusion in $HG(\Omega^1)$. As it follows from definitions $HG_\tau(\Omega^1) = HG_\tau(\Omega^2)$, but Bose Messner algebras $BM_\tau(\Omega^1)$ and $BM_\tau(\Omega^2)$ can be nonisomorphic and association schemes Ω^1_τ and Ω^2_τ can be different up to isomorphism.

Recall, that *metric* on the set X is the symmetric integer function $\rho(x, y)$ in two variables such that $(\rho(x, y) \geq 0,\ \rho(x, y) = 0) \Rightarrow (x = y)$ and triangle inequalities holds $\rho(x, y) \leq \rho(x, z) + \rho(z, y)$.

Let us assume that for the association scheme R_0, R_1, ..., R_d there is a metric ρ such $(x, y) \in R_d$ if and only if $\rho(x, y) = d$. In case of such scheme

we refer to the graph R_1 as *distance regular graph*. The adjacency matrix A_1 of R_1 is special: for each matrix A_i there is a polynomial $f_i(x) \in \mathbb{Z}[x]$ (polynomial with integer coefficients) such that $A_i = f_i(x)$.

We already notice that orbital schemes of Coxeter groups A_n, acting on elements of corresponding geometry of type i, $1 < i < n$ and groups B_n, acting on elements of geometry of type n, form Johnson and Hamming schemes of Coding theory. From other side orbital scheme of simple group $A_n(q)$ corresponds to Grassman metrics, which has some similarity with Johnson group. Let us consider finite BN-pair $G(q)$ defined over finite field $\mathbb{F}_q$ with the Weyl group W.

We can consider the decomposition of G into double cosets by Borel subgroup B:

$$G = \bigcup_{g \in G} BgB.$$

The well known Bruhat lemma each double class BgB has unique representative $w \in W$. So there is natural one to one correspondence η between double classes by Borel subgroup and elements of Weyl group:

$$\eta(BwB) = w.$$

Let us change Borel subgroup for maximal standard parabolic P_i i.e.

$$P_i = BW_iB.$$

Then

$$G = P_igP_i$$

contains uniquely defined element w from the Weyl group of the shortest length from W_iwW_i. So we have natural η one to one correspondence between orbitals of G, acting on cosets gP_i, and orbitals of permutation group $(W, W : W_i)$. The following statement was formulated in [66].

Proposition 2.1.1. *Orbital scheme of group $(G, G : P_i)$ is metric associative scheme if and only if orbital scheme of its Weyl group $(W, W : W_i)$ is a metric one.*

It means that orbitals $R_i, i = 0, 1, 2, \ldots, d$ and $R'_i, i = 0, 1, 2, \ldots, d$ of transformation groups $(B_n(q), B_n(q) : P_n)$ and $(C_n(q), C_n(q) : P_n)$, respectively, for which $\eta(R_i)$ and $\eta(R'_i)$ are same orbitals of Hamming scheme, form metric association schemes

The following fact had been formulated in [149].

Proposition 2.1.2. *Let $B_n(q)$ and $C_n(q)$, $n \geq 2$ are simple groups acting on the totalities of left cosets by maximal parabolic subgroup P_n corresponding to extreme right point of Coxeter diagram. Then their Hecke algebras $\mathcal{H}(B_n(q))$ and $\mathcal{H}(C_n(q))$ are hyperequivalent.*

It means that structure constant of $\mathcal{H}(B_n(q))$ and $\mathcal{H}(C_n(q))$ are equal and there is a natural one to one correspondence between fusions of $\mathcal{H}(B_n(q))$ and $\mathcal{H}(C_n(q))$. Notice that groups $B_2(q)$ and $C_2(q)$ are isomorphic. So, $\mathcal{H}(B_2(q)) = \mathcal{H}(C_2(q))$.

Let (G, X) be a permutation group. We refer to

$$N(G) = \{\pi \in S(X) | \pi^{-1} G \pi = G\}$$

as *permutational normalizer* of G.

The group of automorphism of distance transitive metric corresponding to the action of $B_n(q)$ on $B_n(q) : P_n$ ($C_n(q)$ on $C_n(q) : P_n$) coincides with $N(B_n(q))$ ($N(C_n(q))$), respectively. In fact $N(B_n(q))$ and $N(C_n(q))$ are simply extensions of $B_n(q)$ and $C_n(q)$ by automorphisms of finite field $\mathbb{F}_q$ (see [31]). So $N(B_n(q))$ and $N(C_n(q))$ are different quasisimple finite group. So, we prove the following statement.

Proposition 2.1.3. *Hyperequivalent Hecke algebras $\mathcal{H}(B_n(q))$ and $\mathcal{H}(C_n(q))$ are not isomorphic.*

In paper [173] the following problem had been investigated. Let G be a finite BN pair acting on $G : P_i$. Describe over groups X of $(G, G : P_i)$, i.e. subgroups Z of symmetric group $S(G : P_i)$ such that $Z > G$. The proof of this results use some corollaries from the classification theorem of finite simple groups (t.f.s.g.). The compact solution independent from for the (t.f.s.g.) for the case of classical BN pairs, i.e. simple groups with diagrams A_n, B_n, C_n and D_n, was obtained in [188], [189]. In particular, the following statement was proven.

Theorem 2.1.4. *(i) Let Z be over group of $(C_n(q), C_n(q) : P_n)$, $n \geq 2$ then Z is subgroup of permutational normalizer $N(C_n(q))$.*

(ii) Let Z be over group of $(B_n(q), B_n(q) : P_n)$, which is not a subgroup $N(B_n(q))$. Then

$$D_{n+1}(q) < Z < N(D_{n+1}(q))$$

The nature of the embedding of $B_n(q)$ into $D_{n+1}(q)$ was investigated in [104]. Orbitals of $D_{n+1}(q) : P_n$ on $B_n(q) : P_n$ obviously form distance transitive orbital scheme corresponding to Hecke algebra $\mathcal{H}(D_{n+1}(q))$ but the image $\Omega_n(q)$ of $\mathcal{H}(D_{n+1}(q))$ under the hyperequivalence $\eta\eta'$ sending R_i to R'_i is *distance regular but not distance transitive map.* The distance regular graph of $\Omega_n(q)$ is called "*Ustimenko graph*" according to subject index of [16]. J. Hemmeter used the existence of $\Omega_n(q)$ for the prove of existence of other family of distance regular but not distance transitive graphs of unbounded diameter (see Hemmeter graphs in the subject index in [16]).

We may consider an interesting family of hypergroups associated with $A_n(q)$, $B_n(q)$, and $D_{n+1}(q)$. The structure constant $p^k_{i,j}(q)$ are polynomial expression in variable q. We can change q for positive integer parameter t which is not a prime power and get a new hypergroups $HG(A_n(t))$, $HG(B_n(t))$ and $HG(D_n(t))$.

Notice that $HG(A_n(1))$, $HG(B_n(1))$ and $HG(D_n(1))$ are hyperequivalent to Hecke algebras of Weyl groups A_n, B_n and D_n acting on elements of their Coxeter geometry of type corresponding to right extreme node of diagram.

Recall, that the most important task of Coding Theory is search for large subsets Y on finite metric space (X, ρ), such that for each pair y, y' of distinct elements from Y the distance $\rho(y, y') \geq t$, where t is fixed nonzero parameter. If $t = 1$ then vertices from Y form a clique of distance regular graph of relation $\{(x, y)|\rho(x, y) = 1\}$. In case of distance transitive metrics related to $G \in \{B_n(q), C_n(q), D_n(q)\}$ we can take an element $v \in \Gamma_{n-1}$ and form a maximal clique $\{x \in \Gamma_n(G)|xIv\}$ (see [16] and further references). This method is not working for the case of distance regular but not distance transitive metrics $\Omega_n(q)$. The description of the maximal cliques for the distance regular graph in $\Omega_n(q)$ the reader can find in [60].

Let us discuss the automorphism of graphs $\Phi_J = \{(x, y)|\rho(x, y) \in J\}$, where J is a proper subset of $\{1, 2, \ldots, n\}$ for the above mentioned metrics. For the cases of metrics related to $\Gamma_n(G)$, where G is one of groups $C_n(q)$, $D_n(q)$, we have $\mathrm{Aut}(\Phi_j) = N(G)$. In case of association scheme $\Omega_n(q)$ we have $\mathrm{Aut}(\Phi_J) = N(C_n(q))$. Case of the action of $B_n(q)$ onto $B_n(q) : P_n$ is an interesting one: if J correspond to union of orbitals for $B_n(q)$, which is not a union of orbitals of $D_{n+1}(q)$, then $\mathrm{Aut}(\Phi_J) = N(B_n(q))$, in the opposite case of union orbitals of larger group we have $\mathrm{Aut}(\Phi_J) = N(D_{n+1}(q))$.

The structure constants for Bose-Messner algebas corresponding to metric spaces of classical simple groups of Lie type were computed in [190].

2.2. On the parallelotopic graphs

Definition 2.2.1. Let Γ be a bipartite graph with partition sets P_i, $i = 1, 2$. Suppose that C be a disjoint union of finite sets C_1 and C_2. We say that Γ is a *bipartite parallelotopic graph* over (C_1, C_2) if

(i) there exists a function $\pi : V(\Gamma) \to M$ such that if $p \in P_i$, then $\pi(p) \in C_i$,

(ii) for every pair (p, j), $p \in P_i$, $j \in C_i$, there is a unique neighbour u with given $\pi(u) = j$.

It is clear that the bipartite parallelotopic graph Γ is a biregular graph with bidegrees $r = |C_1|$ and $s = |C_2|$.

We refer also to the function π in the definition of bipartite parallelotopic graph as a *labelling*. We will often omit the term "bipartite", because all our simple graphs are bipartite.

It is clear that a parallelotopic graph is biregular graph with bidegrees r and s. The neighbourhood of each vertex is "rainbow like" set - collection of elements of different colour.

Walks in the parallelotopic graph are in one to one correspondence with chains of colours ($c_1 \in C_1$, $c_2 \in C_2$, $c_3 \in C_1$, ...). Let $N_c(v)$ be the operator of taking the neighbour of v with the colour c.

Linguistic graph is a parallelotopic graph as above such that C_1, C_2, P and L are Cartesian powers of the alphabet M .

Example 2.2.2. *Planary Linguitic Graphs* Let us consider the bipartite graph L (incidence structure) with the points set D^n and the line set D^m such that the point $(x_1, \ldots, x_n)$ is incident with line $[y_1, \ldots, y_m]$ if and only if the following k equalities ($k \leq m$, $k \leq n$) hold

$$
\begin{aligned}
x_1 \times_1 y_1 &= f_1(x_{k+1}, \ldots, x_n, y_{k+1}, \ldots, y_n) \\
x_2 \times_2 y_2 &= f_2(x_1, y_1, x_{k+1}, \ldots, x_n, y_{k+1}, \ldots, y_n) \\
&\ldots \\
x_k \times_k y_k &= f_k(x_1, \ldots, x_{k-1}, y_1, \ldots, y_{k-1}, x_{k+1}, \ldots, x_n, y_{k+1}, \ldots, y_m),
\end{aligned}
$$

where $\times_j$ are quasigroups (latin squares) on D, F_j are chosen functions with the codomain D (*governing functions*).

Let us define structure of the parallelotopic graphs via the following colouring functions

$$
\begin{aligned}
\rho_1((x_1, \ldots, x_n)) &= (x_{k+1}, \ldots, x_n), \\
\rho_2([y_1, \ldots, y_n]) &= (y_{k+1}, \ldots, y_m).
\end{aligned}
$$

Thus $C_1 = D^{n-k}$ and $C_2 = D^{m-k}$ are colour sets.

Example 2.2.3. Linguistic polynomial graphs over the commutative ring $(\mathbb{K}, +, \times)$ We shall use the term as above in case of planary linguistic graphs for which D is the ring $\mathbb{K}$ and

$$x_i \times_i y_i = \lambda_i x_i + \mu_i y_i,$$

and each polynomial expression f_i from $\mathbb{K}[x]$.

Example 2.2.4. This is generalisaion of the planary linguistic graphs obtained by rewriting the equations (i) in the form $x_i = f_i(y_i, x_1, \ldots, y_m)$. We require that for each i, $i = 1, \ldots, k$ equation (i) has unique solution in variable y_i, when other variables are specialised. We have the same colouring functions as in the Example 2.2.2. The important particular case here is $f_i(y_1, \ldots, y_m) = y_1$ (*straight linguistic graph*).

Example 2.2.5. *Graded graphs* We may generalise the previous example via consideration of Cartesian products of $D_1, \ldots, D_n$ and $D_1, \ldots, D_m$ as partition sets and assuming that the domain of each variable x_i (or y_i) is D_i .

Example 2.2.6. *Group parallelotopic graph.* Let G be a group with the proper subgroups G_1 and G_2 such that $\langle G_1, G_2\rangle = G$. Let us consider the incidence structure $\Gamma(G) = \Gamma(G)_{G_1,G_2}$ with a set of points $P = (G : G_1)$ and set of lines $L = (G : G_2)$. The group G is a subgroup of the automorphism group of $\Gamma(G)$, the action of G on the set of edges being equivalent to its action on $(G : G_1 \cap G_2)$ by right shifting.

The following elementary statement is well known.

Lemma 2.2.7. *The incidence graph for $\Gamma = \Gamma(G)_{G_1,G_2}$ is connected if and only if the subgroups G_1 and G_2 generate G. Every connected component of Γ is isomorphic to $\Gamma(G')_{G_1,G_2}$ where $G' = \langle G_1, G_2\rangle$.*

We will say that a bipartite parallelotopic graph is a *group parallelotopic graph* if it is isomorphic to the incidence graph of an incidence structure $\Gamma(G)_{G_1,G_2}$, where G is a group with subgroups G_1 and G_2.

We will consider further the case of a *unipotent-like factorisation*, i.e. a factorisation of a group U into 3 subgroups U_1, U_2 and U_3 such that $U_1 \cap U_2 = 1$, $U_1 \cap U_3 = 1$, $U_2 \cap U_3 = 1$, and U_3 contains $[U_1, U_2]$. Thus, there are unique decompositions $u \in U$ of the kinds $u = u_1u_2u_3$ and $u = u_2u1u'_3$ where $u_1 \in U_1$, $u_2 \in U_2$ and $u_3, u'_3 \in U_3$.

Let us consider the incidence structure $\Gamma = \Gamma(U)_{U_1,U_2}$. Directly from definitions we obtain:

1. For every coset U_1u there is a canonical representative u_2u_3, $u_2 \in U_2$, $u_3 \in U_3$. Let us call $u_2 = \pi(U_1u)$ the colour of the coset U_1u.
2. For every coset U_2u' there is a canonical representative $u_1u'_3$, $u_1 \in U_1$, $u'_3 \in U_3$. Let us call $u_1 = \pi(U_2u')$ the colour of the coset U_2u'.

Lemma 2.2.8 (16)**.** *Let $U = U_1U_2U_3$ be a unipotent-like factorisation of the group U. Then the incidence graph of $\Gamma(U) = \Gamma(U)_{U_1,U_2}$ is a group parallelotopic graph with color set $U_1 \cup U_2$ and with parallelotopic colouring π.*

Remark 2.2.9. Graph $\Gamma(U)_{U_1,U_2}$ is a biregular with bidegrees $a = |U_1|$ and $b = |U_2|$ and $r = |U_3|$.

2.3. On the linguistic graph

Let P and L be copies of $n + r$-dimensional free module $\mathbb{K}^{n+r}$ and $n + s$-dimensional free module $\mathbb{K}^{n+s}$ over the finite commutative ring $\mathbb{K}$,

respectively. Elements of P will be called *points* and those of L *lines*. To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to choose two fixed bases and write:

$$(p) = (p_1, \ldots, p_n, c_1, c_2, \ldots, c_r)$$
$$[l] = [l_1, \ldots, l_n, t_1, t_2, \ldots, t_s]$$

We now define an incidence structure (P, L, I) as follows. We say the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$\begin{aligned}
a_1 l_1 - b_1 p_1 &= f_1(c_1, \ldots c_r, t_1, \ldots, t_s) \\
&\ldots \\
a_i l_i - b_i p_i &= f_i(c_1, \ldots c_r, t_1, \ldots, t_s, l_1, \ldots, l_{i-1}, p_1, \ldots, l_{i-1}) \\
&\ldots \\
a_n l_n - b_n p_n &= f_n(c_1, \ldots c_r, t_1, \ldots, t_s, l_1, \ldots l_{n-1}, p_1, \ldots, p_{n-1})
\end{aligned} \tag{2.3.1}$$

where f_i, $i = 2, \ldots, n$ can be any polynomial expressions in variables $c_1, \ldots, c_r$, $t_1, \ldots, t_s$, $l_1, \ldots, l_{i-1}$, $p_1, \ldots, p_{i-1}$ over $\mathbb{K}$, a_i, b_i can be any nonzero elements from $\mathbb{K}$.

It is easy to see that the above graph is a parallelotopic graph such that tuples $c_1, \ldots c_r$ and $t_1, \ldots, t_s$ be the "colours" of (p) and $[l]$, respectively. Let $C(P) = \mathbb{K}^r$ and $C(L) = \mathbb{K}^s$ are sets of colours for points and lines.

Let us refer to the graph $I = I(n, r, s)$ defined by above equations as *linguistic graphs of triangular type over* $\mathbb{K}$ of type (r, s, n). We assume that one of the expressions f_i, $i = 1, 2, \ldots, n$ has degree ≥ 2.

The *colour function* π for such a graph is just a projection of tuples $(p) \in P$ and $[l] \in L$ onto r and s last components, respectively. We assume that $N_c(v)$ is the operator of taking the neighbour of v of colour c in our linguistic graph.

The linguistic graphs naturally appear as induced subgraphs of Incidence Geometries of Finite Simple Groups of Lie type. They play an important role in studies of Large Schubert cell related to the geometry ([151], [153]. The following examples are induced subgraphs of incidence geometries of rank 2. The theory of incidence geometries corresponding to finite simple groups of Lie type the reader can find in [19], [145]. Special dynamical systems related to linguistic graphs will be discussed in next chapter.

Example 2.3.1. Let $P = \{(x_1, x_2) | x_i \in GF(q)\}$, $L = \{[y_1, y_2] | y_i \in GF(q)\}$. Let us define an incidence relation I_1 as: $(a, b)I_1[x, y]$ if and only if

$$y - b = xa \quad .$$

Let us consider the function $\pi : P \cup L \to GF(q)$, such that

$$\pi((x_1, x_2)) = x_1, \text{ and } \pi([y_1, y_2]) = y_1.$$

It is easy to check that π is a labelling for the graph I_1. It is a linguistic graph of type $(1, 1, 1)$ over $GF(q)$. This is the induced subgraph of the incidence graph of the geometry for simple group $A_2(q)$ (classical Desargues projective plane).

Example 2.3.2. Let $P = \{(x_1, x_2, x_3)|x_i \in GF(q)\}$ be the set of points and $L = \{[y_1, y_2, y_3]|y_i \in GF(q)\}$. be the set of lines. Let us define an incidence relation I_2 as: $(a, b, c)I_2[x, y, z]$ if and only if

$$y - b = xa \text{ and } z - c = xb.$$

Let us assume that $\pi((x_1, x_2, x_3)) = x_1$ and $\pi([y_1, y_2, y_3]) = y_1$. It is clear, that I_2 defines a family of linguistic graphs over $GF(q)$ with parameters (1, 1, 2). This is the induced subgraph of the incidence graph of the geometry for simple group $B_2(q)$ (classical regular generalised quadragon). So the girth of I_2 (length of minimal cycle) is at least 8.

Example 2.3.3. Let $P = \{(x_1, x_2, x_3, x_4, x_5)|x_i \in GF(q)\}$ be the set of points and $L = \{[y_1, y_2, y_3, y_4, y_5]|y_i \in GF(q)\}$ be the set of lines. Let us define an incidence relation I_3 as: $(a, b, c, d, e)I_3[x, y, z, u, v]$ if and only if

$$\begin{aligned} y - b &= xa \\ z - 2c &= -2xb \\ u - 3d &= -3xc \\ 2v - 3e &= 3zb - 3yc - ua \end{aligned}$$

From the equations above, it follows that $\pi : \pi((x_1, x_2, x_3, x_4, x_5)) = x_1$ and $\pi([y_1, y_2, y_3, y_4, y_5]) = y_1$ is a labelling for I_3.

This is the induced subgraph of the geometry of group $G_2(q)$ (*generalised gexagon*).

If char$GF(q) > 3$ then the girth of this graph is at least 12. Directly from the equations above we can get that I_3 is the linguistic graph with parameters (1, 1, 4) over $GF(q)$.

Example 2.3.4. Let $GF(q^2)$ be the quadratic extension of $GF(q)$ and $x \to x^q$ be the Frobenius automorphism of $GF(q^2)$. Let

$$\begin{aligned} P &= \{(x_1, x_2, x_3)|x_1 \in GF(q), x_2 \in GF(q^2), x_3 \in GF(q)\}, \\ L &= \{[y_1, y_2, y_3]|y_1 \in GF(q^2), y_2 \in GF(q^2), y_3 \in GF(q)\}. \end{aligned}$$

Let us define the incidence relation I_4 as: $(a, b, c)I_4[x, y, z]$ if and only if

$$\begin{aligned} y - b &= xa \\ z - c &= ay + ay^q. \end{aligned}$$

It is clear that rules $\pi((x_1, x_2, x_3)) = x_1$ and $\pi([y_1, y_2, y_3]) = y_1$ define the parallelotopic graph over $GF(q^2)$, It is a linguistic graph over $\mathbb{F}_q$ of the type it's parameters are $(1, 2, 3)$.

Example 2.3.5. Let us consider the following bipartite algebraic graph $A(n, \mathbb{K})$ (*alternating graph*) defined over commutative ring $\mathbb{K}$ by the following rules.

Partition sets P_n and L_n are two copies of the free module $\mathbb{K}^n$. Brackets and paranthesis allow us to distinguish point $\mathrm{p} = (p_1, p_2, \ldots, p_n)$ and line $\mathrm{l} = [l_1, l_2, \ldots, l_n]$. We say the point p is incident to line l if and only if the following equations hold:

(1) $l_{2s} - p_{2s} = l_1 p_{2s-1}$ for $s = 1, 2, \ldots, t$,

(2) $l_{2s+1} - p_{2s+1} = p_1 l_{2s}$ for $s = 1, 2, 3, \ldots, d$,

where $d = t - 1$ for even n ($n = 2t$) and $d = t$ if n is odd ($n = 2t + 1$). The graph is a linguistic graphs of triangular type over $\mathbb{K}$ of type $(1, 1, n - 1)$.

2.4. On small world graphs obtained by blow up operation

The term graphs with memory used for an infinite family of finite graphs $\Gamma_i(K)$ with the vertices and which are tuples over the alphabet K and the choice of neighbour described by disjoint union of several Cartesian powers of K.

The family of graphs with memory can be treated as special models of Turing machina with the internal and external alphabet K and few special symbols.

Definition 2.4.1. We define, that family of k-regular graphs Γ_i (or graph with the average degree k) and increasing order v_i is a *family of graphs of small world* if

$$\mathrm{diam}(\Gamma_i) \leq c\log_{\mathrm{k}}(v_i)$$

for some independent constant c, $c > 0$, where $\mathrm{diam}(\Gamma_i)$ is diameter of graph Γ_i.

The chapter is devoted to explicit constructions of new families of small world tactical configurations with memory. They form wide class of graphs containing incidence graphs of geometries of finite simple groups of Lie type. The examples can be partited into three following categories - cases of graphs with bounded diameter, unbounded diameter, and the case of bounded degree.

For the defined class of graphs the natural parametrisation of walks (computations in the corresponding Turing machine) will be given. It is allow to introduce analogs of small Schubert sells on the set of vertices.

It is well known that the diameter of a k-regular graph (or graph with the average degree k) of order v is at least $\log_{k-1}(v)$ and that the random k-regular graph has diameter close to this lower bound (see [3, X]). Only several explicit constructions of families of k-regular graphs with diameter close to $\log_{k-1}(v)$ are known(see [11], X, sec.1) and further references or geometrical construction .

In case of irregular graph with the list of valencies $k_1, k_2, \ldots, k_t$, we shall use the term small world graph for the graph with the diameter bounded by $c_i \log_{k_i}(v)$ for each $i = 1, \ldots, t$ for appropriate constant c_i.

In case of that family of irregular graphs Γ_i of degree k_i and increasing order v_i, we shall use also the term *family of graphs of small world* if

$$\mathrm{diam}(\Gamma_i) \leq c_i \log_{k_i}(v_i)$$

for some independent constant c_i, $c_i > 0$, where $\mathrm{diam}(\Gamma_i)$ is diameter of graph Γ_i.

The problem of constructing infinite families of small world graphs with given degrees and certain additional properties is far from trivial. This problem has many remarkable applications in economics, natural sciences, computer sciences and even in sociology. For instance, the "small world graph" of binary relation "two person shake their hands" on the set of people in the world, has small diameter.

The restriction of this problem on the class of bipartite graphs has additional motivations because such problem for random graphs has been studied by Klee, Larman and Wright, Harary and Robinson, Bollobas and others (see the survey in [11], chapter 10, section 5). The purpose of the paper is to define explicitly wide class of small world graphs which contains graphs [171], [174] and incidence graphs of finite Lie geometries, in particular (see [158]).

2.4.1. On blowing of incidence systems in term of linear algebra

Let $(A, +)$ be an abelian group and $\sum$ be an arbitrary set. Let u denote a certain subgroup of the abelian group consisting of all functions from $\sum$ to A. For $\sum_0 \subseteq \sum$ let $u(\sum_0)$ denote the subgroup of the functions from u which vanish outside $\sum_0$ and for $f \in u(\sum_0)$ let $f|_{\sum_0}$ be the function which coincides with f inside $\sum_0$ and vanishes outside $\sum_0$. We will assume that on u a distributive operation $*$ is defined:

$$(f + g) * h = f * h + g * h,$$

$$h * (f + g) = h * f + h * g.$$

Definition 2.4.2. Let Φ a binary relation on a set N and η be a mapping of N into $2^{\sum}$. Let $\tilde{\Phi} = \tilde{\Phi}(\sum, u, *, \eta)$ be the relation on

$$\tilde{N} = \{(\alpha, f) | \alpha \in N, f \in u(\eta(\alpha))\}$$

defined as follows: $((\alpha, f), (\beta, g)) \in \tilde{\Phi}$ if and only if $(\alpha, \beta) \in \Phi$ and

$$f - g|_{\eta(\alpha)\cap\eta(\beta)} = f * g|_{\eta(\alpha)\cap\eta(\beta)}.$$

Then $\tilde{\Phi}$ is called a *blowing of the relation* Φ.

If u coincides with the set of all functions from $\sum$ to A (with all functions having a finite support) then a blowing is said to be *cartesian* (*direct*).

If A is a module over a ring $\mathbb{K}$, u is a submodule of $A^{\sum}$ and $*$ is a bilinear operation on u then the blowing $\tilde{\Phi}$ is said to be *linear* over $\mathbb{K}$.

If the relation Φ is symmetric and the operation $*$ is alternating (i.e. $x * y = -y * x$) then the relation $\tilde{\Phi}$ is symmetric. In particular if (Γ, I, t) is an incidence system over a set of types Δ, then for an alternating operation $*$ the covering $(\tilde{\Gamma}, \tilde{I}, \tilde{t})$, where $\tilde{t}(\alpha, f) = t(\alpha)$, is an incidence system over Δ and the mapping $(\alpha, g) \to \alpha$ is a morphism. Such a morphism will be called *retract*. The system $(\tilde{\Gamma}, \tilde{I}, \tilde{t})$ will be referred as a *blowing of the system* (Γ, I, t).

Example 2.4.3. Let N be the set of all subsets of a finite set $\Omega = \{1, \ldots, n\}$ and Φ be the symmetric inclusion relation on N. Put

$$\sum = \{(i, j) \in \Omega^2, i > j\}.$$

For $\alpha \in N$, let us consider

$$\Delta(\alpha) = \{(i, j) \in L, i \in \alpha, j \neq \alpha\}.$$

Let $\mathbb{F}$ be an arbitrary skew field. In the vector space $V = \mathbb{F}^{\sum} = \{f : \sum \to \mathbb{F}\}$, let us fix the basis elements v_{ij} such that

$$v_{ij}(x) = \begin{cases} 1, & x = (i, j) \\ 0, & x \neq (i, j) \end{cases}$$

and let us define an alternating bilinear multiplication $\circ$ by the following rule:

$$v_{ij} \circ v_{kl} = \begin{cases} v_{il}, & j = k \\ -v_{jk}, & l = i \\ 0, & \text{otherwise.} \end{cases}$$

Let us consider the relation $\tilde{\Phi} = \tilde{\Phi}(\sum, \mathbb{F}^{\sum}, \circ, \Delta)$ and let $\Gamma(N, \mathbb{F})$ be the incidence system $(\tilde{N}, \tilde{\Phi}, \tilde{t})$, where $\tilde{t}(\alpha, f) = |\alpha| = t(\alpha)$. It is clear that $\tilde{\Phi}$ is a linear blowing of Φ.

Let us show that the incidence system $\Gamma(N, \mathbb{F})$ is isomorphic to the projective geometry $PG_{n-l}(\mathbb{F})$. The latter is the set of all proper subspaces of the space $V_n(\mathbb{F})$ with the incidence relation

$$(u, w) \in I \Longleftrightarrow [(u > w) \vee (w > u)]$$

and the type function dim.

Let us fix a basis in $V_n(\mathbb{F})$. With an arbitrary collection $\bar{h}_1, \bar{h}_2, \ldots, \bar{h}_t$ of vectors from $V_n(\mathbb{F})$ let us associate the number

$$l(\{\bar{h}_1, \ldots, \bar{h}_t\}) = \max\{i | h_{s,i} \neq 0 \text{ for some } \bar{h}_s = (h_{s,1}, h_{s,2}, \ldots, h_{s,n})\}$$

i.e., the maximum of the largest number of nonzero components of the vectors $\bar{h_s}$ in the chosen basis.

Let W be a subspace of $V_n(\mathbb{F})$, dim $W = m$. Then

$$W = \langle \bar{b}_1, \bar{b}_2, \ldots, \bar{b}_m \rangle$$

for some vectors

$$\bar{b}_i = (b_{i,1}, \ldots, b_{i,n}), \quad i = 1, 2, \ldots, m.$$

Let us transform the basis $\bar{b}_i$ into another basis by the following algorithm:
Step 1 Let

$$l_m = l(\{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_m\})$$

and $\bar{b}_s$ be a vector such that $b_{s,l_m} \neq 0$. Let us fix a vector

$$\bar{\Gamma}^{(1)}_{l_m} = (b_{sl_m})^{-1} \times \bar{b}_s$$

and consider the new basis

$$\bar{b}^{(1)}_1, \ldots, \bar{b}^{(1)}_{s-1}, \bar{b}^{(1)}_{s+1}, \ldots, \bar{b}^{(1)}_m, \bar{\Gamma}^{(1)}_{l_m}, \text{ where } \bar{b}^{(1)}_i = \bar{b}_i - b_{il_m} \times \bar{\Gamma}^{(1)}_{l_m}.$$

Suppose that in the new basis

$$\bar{b}^{(1)}_i = (b^{(1)}_{i,1}, b^{(1)}_{i,2}, \ldots, b^{(1)}_{i,n}), \quad \bar{\Gamma}^{(1)}_{l_m} = (g^{(1)}_{l_m,1}, g^{(1)}_{l_m,2}, \ldots, g^{(1)}_{l_m,n}).$$

Step 2 Put $l_{m-1} = l(\{\bar{b}^{(1)}_1, \bar{b}^{(1)}_2, \ldots, \bar{b}^{(1)}_m\})$. Let us consider the vector $b^{(1)}_{s'}$ such that $b^{(1)}_{s',l_{m-1}} \neq 0$. Put

$$\bar{\Gamma}^{(2)}_{l_{m-1}} = (b^{(1)}_{s',l_{m-1}})^{-1} \times \bar{b}^{(1)}_{s'} \quad .$$

Let us consider also

$$\bar{\Gamma}^{(2)}_{l_m} = \bar{\Gamma}^{(1)}_{l_m} - g^{(1)}_{l_m,l_{m-1}} \times \bar{\Gamma}^{(2)}_{m-1}$$

and come to the system of vectors

$$\bar{b}^{(2)}_i = \bar{b}^{(1)}_i - b^{(1)}_{i,l_{m-1}} \times \bar{\Gamma}^{(2)}_{l_{m-1}}.$$

We will use the notation

$$\bar{b}^{(2)}_i = (\bar{b}^{(2)}_{i,1}, \bar{b}^{(2)}_{i,2}, \ldots, \bar{b}^{(2)}_{i,n}), \ i \neq s,$$
$$\bar{\Gamma}^{(2)}_{l_m} = (\bar{g}^{(2)}_{l_m,1}, \ldots, \bar{g}^{(2)}_{l_m,n}),$$
$$\bar{\Gamma}^{(2)}_{l_{m-1}} = (\bar{g}^{(2)}_{l_{m-1},1}, \ldots, \bar{g}^{(2)}_{l_{m-1}.n}).$$

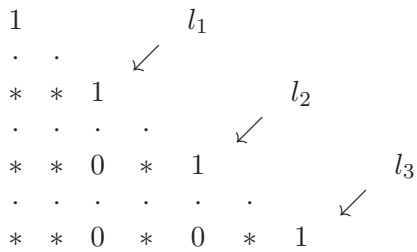


Figure 2.1.

Let us continue this process and consider the step m. The system $\{\bar{b}_1^{m-1}, \bar{b}_2^{m-2}, \ldots, \bar{b}_m^{m-1}\}$ contains the unique vector $\bar{b}_l^{m-1}$ such that all its components having number $> l_1$ are equal to 0, where

$$l_1 = l(\{\bar{b}_1^{m-1}, \ldots, \bar{b}_m^{m-1}\}).$$

Put

$$\bar{\Gamma}_{l_1} = \bar{\Gamma}_{l_1}^{(m)} = (b_{l,l_1}^{m-1})^{-1} \times \bar{b}_l^{m-1}$$

and exchange the vectors $\bar{\Gamma}_{l_2}^{(m-1)}$, $\bar{\Gamma}_{l_3}^{(m-1)}$, $\ldots$, $\bar{\Gamma}_{l_m}^{(m-1)}$ by

$$\bar{\Gamma}_{l_i} = \bar{\Gamma}_{l_i}^{(m-1)} - g_{l_i,l_1} \cdot \bar{\Gamma}_{l_1}^{(m-1)}.$$

It can be shown that the result of application of the presented-variation of the Gauss method does not depend on the choice of the basis $\bar{b}_1$, $\bar{b}_2$, $\ldots$, $\bar{b}_n$ and on the choice of the vector $\bar{b}_s^{k-1}$ with the property that $b_{s,l_{k-1}} \neq 0$ on the step number k of the algorithm.

Lemma 2.4.4. *The system $\bar{\Gamma}_{l_1}$, $\bar{\Gamma}_{l_2}$, $\ldots$, $\bar{\Gamma}_{l_m}$ of vectors is uniquely determined by the subspace W.*

It is convenient to present the vectors $\bar{\Gamma}_{l_1}$, $\bar{\Gamma}_{l_2}$, $\ldots$, $\bar{\Gamma}_{l_m}$ as rows with numbers $l_1, l_2, \ldots, l_m$ in an $n \times n$ matrix $\Gamma(W)$. In this case the component g_i, $i < l_s$ of the vector $\bar{\Gamma}_{l_s}$will be in the (l_s, i)-item of the matrix. If we put the vector e_j, $j \neq l_s$ as the j-th rows of the matrix, we obtain a triangular matrix of a special type (the Gaussian matrix in the sense of [149], see Fig. 2.1).

Let us consider the algorithm which associate with a subspace W the subset $\{l_1, l_2, \ldots, l_m\}$ of Ω and the triangular matrix $\Gamma(W) = (g_{ij})$ such that $g_{ij} = 0$ if $(i,j) \in \Delta(\{l_1, l_2, \ldots, l_m\})$. It is clear that the matrix $\Gamma(W)$ is uniquely determined by the function $g(W)$ from $\sum$ to K such that $g(W)((i,j)) = g_{ij}$. So the algorithm associates with W the element $\rho(W) = (\{l_1, l_2, \ldots, l_m\}, g_{ij})$ of the set $\tilde{N}$ of the incidence system $\Gamma(N, \mathbb{F})$

and determing mapping $\rho : PG_{n-1}(\mathbb{F}) \to \tilde{N}$. Notice that it is convenient to identify $\sum$ either with the set of transpositions of the group S_n (the Weil group A_{n-1} of the general linear group $PG_n(\mathbb{F})$) or with the positive roots of the system A_{n-1} (i.e. with the vectors $e_i - e_j$). Here e_i is the orthonormal basis vectors of the Euclidean space of dimension n.

Proposition 2.4.5. *The mapping ρ is an isomorphism of the geometries $PG_{n-1}(\mathbb{F})$ and $\Gamma(N, \mathbb{F})$.*

Proof. If U and W are distinct subspaces then $\rho(U)$ and $\rho(W)$ are distinct elements of $\tilde{N}$. In fact, the equality $\rho(U) = \rho(W)$ implies the equality of the Gaussian basises $\bar{\Gamma}_{l_1}, \bar{\Gamma}_{l_2}, \ldots, \bar{\Gamma}_{l_m}$ a $\bar{\Gamma}'_{l_1}, \bar{\Gamma}'_{l_2}, \ldots, \bar{\Gamma}'_{l_m}$ of the subspaces U and W, respectively. In this case

$$U = \langle \bar{\Gamma}_{l_1}, \bar{\Gamma}_{l_2}, \ldots, \bar{\Gamma}_{l_m} \rangle = \langle \bar{\Gamma}'_{l_1}, \bar{\Gamma}'_{l_2}, \ldots, \bar{\Gamma}'_{l_m} \rangle = W.$$

On the other hand the image of an element (B, f) is nonempty. It contains the subspace $\langle \bar{\Gamma}_{l_1}, \bar{\Gamma}_{l_2}, \ldots, \bar{\Gamma}_{l_m} \rangle$ where $\{l_1, l_2, \ldots, l_m\} = B$ and $\bar{\Gamma}_{l_1}, \bar{\Gamma}_{l_2}, \ldots, \bar{\Gamma}_{l_m}$ is the Gaussian basis determined by the function f. Thus the mapping ρ is a bijection.

Let U be a subspace of W and $\rho(U) = (B, f)$, $\rho(W) = (A, g)$. Let us show that $B \subset A$. Suppose to the contrary that $i \in B$ & $i \notin A$. The vector $\bar{\Gamma}_i$ of the Gaussian basis of U is a linear combination of the vectors $\bar{\Gamma}'_j$of the Gaussian basis of W. Moreover the coefficients behind the vectors having number $j > i$ should be equal to zero:

$$\bar{\Gamma}_i = \sum_{j<i} \lambda_j \bar{\Gamma}'_j. \tag{2.4.1}$$

But the i-th component of the vector on the right is zero while this component of the vector on the left is 1, a contradiction. Notice that if $i \in B$ then

$$\bar{\Gamma}_i - \bar{\Gamma}'_i = \sum_{j<i} \lambda_j \bar{\Gamma}'_j. \tag{2.4.2}$$

Finally let us show that

$$g - f|_{\Delta(A)\cap\Delta(B)} = g \circ f.$$

Notice that the vectors from $\mathbb{F}^{\Delta(A)} = \{f | f(x) = 0 \text{ for } x \notin \Delta(A)\}$ form an abelian subalgebra (since $x \circ y = 0$ for all $x, y \in \mathbb{F}^{\Delta(A)}$). This is due to the fact that if the elements of $\Delta(A)$ are considered as the roots $e_i - e_j$ of the system A_{n-1} then the sum of two roots from $\Delta(A)$ is not a root. So

$$g \circ f = g|_{\Delta(A)\setminus\Delta(A)\cap\Delta(B)} \circ f|_{\Delta(B)\setminus\Delta(A)\cap\Delta(B)}$$

An element $e_i - e_j$ from $\Delta(A) \cap \Delta(B)$ has $i - j - 1$ presentations as sum of two roots: $e_i - e_j = (e_i - e_k) + (e_k - e_j)$, $i < k < j$. Hence

$$g \circ f(e_i - e_j) = \sum_{k \in A \ \& \ i > k > j} g(e_i - e_k) f(e_i - e_j).$$

The right side of the above equality is just the j-th component of the right side of (2.4.2).

Definition 2.4.6. Let $(\tilde{\Gamma}, \tilde{I}, \tilde{t})$ be a blowing of an incidence system (Γ, I, t) with the set of types Δ. For an element $y \in U$ let us define a transformation $\hat{y}$ of the set $\tilde{\Gamma}_i$ by the following rule:

$$\hat{y} : (\alpha, x) \to (\alpha, x + (y + x * y)|_{\eta(\alpha)}),$$

where $(\alpha, x) \in \tilde{\Gamma}_i$. The incidence system $(\tilde{\Gamma}, \tilde{I}, \tilde{t})$ will be called a *smooth blowing of an incidence system* (Γ, I, t) if there is an element $i \in \Delta$ (the distinguished type) such that

(a) an element $a \in \Gamma$ is uniquely determined by the set O_a of elements from $\tilde{\Gamma}_i$ which are incident to a;

(b) for arbitrary y and a the transformation $\hat{y}$ maps O_a into the set O_b for some b;

(c) the action of $\hat{y}$ on $\tilde{\Gamma}$ defined by the rule:

$$a^{\hat{y}} = b \Longleftrightarrow (O_a)^{\hat{y}} = O_b$$

is an automorphism of $\tilde{\Gamma}$.

The incidence system $(\tilde{N}, \tilde{\Phi}, \tilde{t})$ considered in Example 2.4.3 is a smooth blowing of the system (N, Φ, t). For the distinguished type one can take 1 or $n - 1$ (remind that $t(A) = |A|$ for $A \in N$).

Example 2.4.7. *Geometry of the Weyl groups of classical groups.*

The relation Φ on the set N considered in the previous example can be identified with the incidence relation of the geometry of the Coxeter group A_{n-1} (i.e. of the symmetric group $S(\Omega)$ with the set of generating transpositions $(1, 2), \ldots, (n - 1, n)$).

Let us consider the geometry of the Coxeter group B_n. 1ts elements can be interpreted as the partially defined functions on the set n taking values in the field $\mathbb{F}_2$. So

$$\Gamma(B_n) = \{(B, f) | B \subset \Omega \text{ and } f \in \mathbb{F}_2^B\}.$$

Put $(B, f) \prec (C, g)$ if and only if $C \subset B$ and the restrictions of the functions f and g on the set B coincide. The incidence relation Φ' of the geometry

is the symmetrization of the relation $\prec$. The type is of a partial function (A, f) is by definition $|A|$.

The incidence relation of the geometry $\Gamma(B_n)$ can be considered as a direct blowing of $\Gamma(A_n)$. In fact, let us consider the directed blowing $\tilde{\Phi} = \tilde{\Phi}(\Omega, \mathbb{F}_2^\Omega, \circ, e)$, where e is the identity mapping of $N = 2^\Omega$ onto itself, $x \circ y = 0$ for all $x, y \in \mathbb{F}_2^\Omega$. Then it is easy to see that $\Phi' = \tilde{\Phi}$ and that $\tilde{\Phi}$ is a smooth blowing of Φ.

The geometry $\Gamma(D_n)$ is a subset Γ' of the partially defined functions from $\Gamma(B_n)$ with the incidence relation and the type function restrict Γ'. The set Γ' consists of all functions which either are defined everywhere or have an even number of values 1.

Example 2.4.8. Let us consider the segment $[0, 1]$ of the real line. Let D be the set of intervals $[a, b]$, where $0 \leq a < b \leq 1$. Let Φ be the symmetrization of the inclusion relation, on D. For $[a, b] \in D$ put $t([a, b]) = b - a$. So (D, Φ, t) is a incidence system. Let $\sum = \{(x, y) \in [0, 1] \times [0, 1] | x > y\}$, $\eta([a, b]) = \{(x, y) \in \sum | a \leq x \leq b,\ 0 \leq y \leq a\}$. The subgroup U in $R^{\sum}$ and the bilinear multiplication will be defined as follows.

Let us consider a partially continuous bounded function f which is defined on $[0, 1] \times [0, 1]$. This means that $[0, 1] \times [0, 1]$ is divided into a finite number of domains with continuous boundaries and the restriction of f on either of these domains is a continuous function. The space L of all these functions will be considered as a linear algebra with the mu1tiplication

$$f(x, y) * g(x, y) = \int_0^1 f(x, y)g(z, y)dz - \int_0^1 g(x, z)f(x, y)dz.$$

Let us consider the subalgebra U in η consisting of all functions which are zero outside $\sum$. A direct check shows that $\tilde{\Phi}(\sum, U, *, \eta)$ is a blowing of the incidence system (D, Φ, t).

2.4.2. Blow-up of the graph

Definition 2.4.9. Let Γ be the simple graph with the vertex set $V = V(\Gamma)$, $E = E(\Gamma)$. For each $v, u \in V$ we chose the set U_v the set U_v, and for each edge $e = \{v, u\} \in E$ we chose the parallelotopic graph G_e with partition sets U_v and U_u and the colour sets $C_v(e)$ and $C_u(e)$.

We define the *parallelotopic blow of* Γ as the graph $\tilde{\Gamma}$ with the vertex set $V(\tilde{\Gamma}) = \{(v, x) | v \in V(\Gamma), x \in U_v\}$ such that $(v, x)\tilde{\Gamma}(u, y)$ if and only if $e = (v, u) \in E(\Gamma)$ and $(x, y) \in E(G_e)$.

Definition 2.4.10. We refer to the paralelotopic blow up as *distributed blow up* if we have the map $\Delta : V(\Gamma) \to 2^Y$ and chosen weights $m_y \geq 1$ for each $y \in Y$ such that $|U_v|$ is the product of m_y, $y \in \Delta(v)$ and sets

of colours for the parallelotopic graph G_e , $e = (v, u)$ are $C_v(e)$ is the product of m_y, $y \in \Delta(v)\backslash\Delta(v) \cap \Delta(u)$ and $C_u(e)$ is the product of m_y, $y \in \Delta(u)\backslash\Delta(u) \cap \Delta(v)$.

Definition 2.4.11. (*Graded blow up*). Let Γ be the simple graph with the vertex set $V = V(\Gamma)$, $E = E(\Gamma)$. The distributed blow up as above such that there is a family of finite sets M_y, $y \in Y$ such that for each edge $e = (u, v)$ in $E(\Gamma)$ we have the parallelotopic graph G_e with the point set P_e which is the product of M_y, $y \in \Delta(v)$, the line set L_e is the product of M_y, $y \in \Delta(u)$ and the colourings $\rho : P_e \to M^{\Delta(v)\backslash\Delta(v)\cap\Delta(u)}$ and $\rho_2 : L_e \to M^{\Delta(u)\backslash\Delta(v)\cap\Delta(u)}$.

To the parallelotopic blow up as above we refer as *graded blow up* of Γ.

Properties:

1. The order of $\tilde{\Gamma}$ is the sum of cardinalities of U_v, $v \in V(\Gamma)$.
2. Let $\{w_1, w_2, \ldots, w_m\}$ be the list of neighbours of the vertex v an $e_i = \{v, w_i\}$, $i = 1, \ldots, m$, then $\deg(v)$ is the sum of $|C_{w_i}(e_i)|$, $i = 1, \ldots, m$.
3. Let v be the vertex of $\tilde{\Gamma}$ with $|U_v| = 1$ then

$$\mathrm{diam}(\Gamma) \leq \mathrm{diam}(\tilde{\Gamma}) \leq 2\mathrm{diam}(\Gamma).$$

We can write more precise bound

$$\mathrm{diam}(\tilde{\Gamma}) \leq 2 \max_{u \in \Gamma}(d(v, u)).$$

We refer to the homomorphism map $\mathcal{R}etr : \tilde{\Gamma} \to \Gamma$ as *retraction map.*

2.4.3. Blow diagram and Schubert cells

Let Γ be the simple graph. For each edge $e = \{u, v\} \in E(\Gamma)$ we chose sets of colours $C_e(u)$ and $C_e(v)$. We assume that for each $c \in C_e(u)$ ($C_e(v)$) there is the arrow directed from v to u (from u to v, respectively) labeled by c. We refer to this multigraph as *blow diagram* $D(\Gamma)$.

We refer to the paralletopic blow up with the sets of colours as *representation of the blow diagram.*

Let $v' = (v, x)$, $v \in \Gamma$ be chosen vertex from $\tilde{\Gamma}$ (initial state). The totality of walks from v' are in one to one correspondence with walks from the blow diagram $D(\Gamma)$ starting from initial state v. Really, the walk (or computation) in our automaton is the object defined by the walk $v\Gamma u_1\Gamma u_2\Gamma \ldots \Gamma u_k$ in Γ and sequence of colours (or arrows): $\beta_1 \in C_{e_1}(u_1)$, $e_1 = (v, u_1)$, $\ldots$, $\beta_k \in C_{e_k}(u_k)$, $e_k = (u_{k-1}, u_k)$. The last element of computation (walk) c with the initial state (v, x) we write as $c(v, x)$. We say that computations c_1 and c_2 are equivalent if the images of retraction map of states from c_1 and c_2 form same walk in Γ. We refer to the totality S_v of all elements (v, x), $x \in U_v$ as *Schubert cell.*

In the case of linguistic blow up we say that element 0 of the alphabet is neutral if the induced graph on the set Γ' of elements of kind (v, x), $v \in \Gamma$, $x = 0, 0, \ldots 0$, is isomorphic to the Γ. We refer to Γ' as *standard camera* with respect to chosen neutral element. Two elements (v, x) and (u, y) we call *computationally equivalent* if $v = u$ and for each computation c_1 with the starting element v, x and last element from the Γ' there is equivalent computation c_2 with the starting point (u, y) such that $c_1(x) = c_2(y)$.

We refer to the class of computational equivalence as *computational cell*. The Grassmanian over the field $\mathbb{F}$ is the linguistic blow up of the geometry of Coxeter group A_n and the computational cells are small Schubert cells in this case (see [169]).

2.4.4. Coxeter groups and Schubert cells

Let W be the finite Coxeter group, $S = \{s_1, \ldots, s_n\}$ be the set of standard generators, i.e. (W, S) be the *Coxeter system*. Let T be the totality of reflections, i.e. elements of kind $z = gsg^{-1}$, $g \in W$, $s \in S$, $|S| = n$. The *geometry of the group geometry of the group*W, denote by $\Gamma(W)$, is the disjoint union of $(W : W_i)$ i.e. collections of the right cosets of the group W by standard maximal subgroups $W_i = \langle S \backslash \{s_i\} \rangle$, $i = 1, \ldots, n$ with the type function $t(\alpha) = i$ for $\alpha \in (W : W_i)$ and the incidence relation I such that $\alpha I \beta$ if and only if $\alpha \cap \beta = \emptyset$.

We consider the *flag systems* $GF(W)$ as disjoint union of the sets $(W : W_J)$, where J is a proper subset of S, and $W_J = \langle S \backslash J \rangle$. We assume $t(gW_J) = J$ and $\alpha I \beta$ if and only if $\alpha \cap \beta$ is not the empty set and $t(\alpha) \cap t(\beta)$ is empty. Let $l(g)$ be the minimal length of irreducible decomposition of g with respect to S, we assume

$$l(\alpha) = \min_{g \in \alpha} l(g), \quad \alpha \in GF(W).$$

The elements of T partited onto at most 2 classes of conjugate elements. Let $c(\alpha) = |\Delta(\alpha)|$ for the $\alpha \in GF(W)$. Let T_1 and T_2 be two classes of conjugate reflections. We assume that

$$a(\alpha) = |\Delta(\alpha) \cap T_1|$$

and

$$b(\alpha) = |\Delta(\alpha) \cap T_2|.$$

Let us consider the polynomial expressions g_J which is the sum of monomial terms $z^c(\alpha)$, $t(\alpha) = J$ and G_J which is the sum of monomial terms $x^{a(\alpha)} y^{b(\alpha)}$, $t(\alpha) = J$.

For each ordered edge (α, β), $\alpha I \beta$ in $GF(W)$ such that $t(\alpha) = J_1$ and $t(\beta) = J_2$ we consider set

$$C(\alpha, \beta) = \Delta(\alpha) \backslash \Delta(\alpha) \cap \Delta(\beta).$$

Let $c(\alpha, \beta) = |C(\alpha, \beta)|$ and $r_{J_1,J_2}(\alpha)$ which is the sum of monomial terms $x^{c(\alpha,\beta)}$, $\beta I \alpha$ and $t(\beta) = J_2$.

If T is not a collection of conjugate elements we consider

$$a(\alpha, \beta) = |T_1 \cap C(\alpha, \beta)|, \quad b(\alpha, \beta) = |T_2 \cap C(\alpha, \beta)|.$$

Let $s_{J_1,J_2}(\alpha)$ be the sum of monomial expressions $x^{a(\alpha,\beta)} y^{b(\alpha,\beta)}$, such that $\alpha I \beta$ and $t(\beta) = J_2$.

Proposition 2.4.12. *Let W be the finite Coxeter group with the standard set of generators S, then polynomial expressions $r_{J_1,J_2}(\alpha)(x) = r_{J_1,J_2}$ does not depend on α. If not all elements are conjugate, then polynomials $s_{J_1,J_2}(\alpha)$ does not depend on α.*

Theorem 2.4.13. *Let us consider a distributed blow up $\tilde{\Gamma}(W)(a)$ of the geometry $\Gamma(W)$ $(GF(W))$ such that $Y = T$, $m(x) = m(y)$ if x and y are conjugate and*

$$\Delta(\alpha) = \{w \in T | l(\alpha w) < l(\alpha)\}.$$

Let $a = m(x)$ for each x if all elements of T are conjugate (conjugate case), and a and a^t , $t \geq 1$ are weight of elements from different conjugate classes of T in the case of existence of two conjugate classes. Then $\tilde{\Gamma}(W)$ is geometrical incidence structure, $GF(\tilde{\Gamma}(W)_{J_1,J_2}(a))$ $(GF'(W)_{J_1,J_2}$, respectively) $a = 2, 3, \ldots$ are small world tactical configurations with bidegrees $r_{J_1,J_2}(a)$ and $r_{J_2,J_1}(a)$ in conjugate or $s_{J_1,J_2}(a, a^t)$ and $s_{J_2,J_1}(a, a^t)$ otherwise.

Let us refer to the blow up for $\Gamma(W)$ as *balanced blow up*.

Let us consider the retraction map $r : \tilde{\Gamma} \to \Gamma(W)$ such that $r(v, x) = v$ which is graph homomorphism.

We refer to reimage $\mathrm{Sch}(v)$ of the element $v \in \Gamma$ under the retraction map as *Schubert cell*. Let $\mathrm{Sch}(\tilde{\Gamma})$ be the disjoint union of the Schubert cells $\mathrm{Sch}(v)$ where cosets v contain the Coxeter element i.e. element with the maximal length of the irreducible decomposition relatively to the standard set of generators S.

The complete list of finite Coxeter groups contains several sequences A_n, B_n, D_n, I_m (groups of symmetries for incidence graphs of m-gons) and the following "sporadic groups": F_4, E_6, E_7, E_8, H_3, H_4 (see [15]). The properties of graphs Γ_{J_1,J_2}, $J_1 \cap J_2 = \emptyset$ such as bidegrees and diameters the reader can find in [16]] (look at "incidence Coxeter graphs" in the subject index).

Theorem 2.4.14. *Let (W, S) be the finite Coxeter System, $GF(W)$ be the totality of cosets by $\langle S \backslash J_2 \rangle$, where J_2 is a proper nonempty subset of S, GF_{J_1,J_2} be the tactical configuration corresponding to the incidence relation on $GF(W)$ restricted on $GF_{J_1} \cup GF_{J_2}$. Let $\tilde{GF}_{J_1,J_2}(a)$ ($\tilde{GF}(W)(s)$) be the graded linguistic blow up of the graph $GF_{I,J}(a)$ ($GF(W)$, respectively), $a \geq 1$ over the reflection set T with the basic data $M_r = A^{am_r}$, $r \in T$, $m_r \geq 1$ are constant, A is the finite set (alphabet).*

(i) The family $\tilde{GF}_{J_1,J_2}(a)$ is a small world graph with memory over the alphabet A.

(ii) If $c_r = c$ for each $r \in T$ or W contains two classes of conjugates T_1 and T_2 and $c_r = a_i$ for each $r \in T_i$, $i = 1, 2$, then $GF_{J_1,J_2}(sa)$ be the family of tactical configurations.

(iii) If J_1 and J_2 are conjugated under the automorphism graph related to involutive symmetry of the diagram (case of A_n, D_n, G_n, F_4, E_6) then GF_{J_1,J_2} is a family of regular graphs.

Remark 2.4.15. In case of basic data for the $\tilde{GF}(W)$ formed by infinite sets M_i the blow up of each GF_{J_1,J_2} is an infinite bipartite graph with infinite valencies.

Let $\tilde{GF}_{J_1,J_2}$ be the finite o infinite blow up with the basic data M_r, $r \in T$. Let us consider the union $\tilde{\mathrm{Sch}}_{J_1,J_2}$ of Schubert cells Sch_v such that v contains the Coxeter element, i.e. uniquely determined element $w \in W$ with the maximal length of irreducible decomposition $l(w)$, with the restriction of the incidence relation on it. There is precisely one Schubert cell Sch_v and Sch_u for each type (J_1 or J_2). The graph $\tilde{\mathrm{Sch}}_{J_1,J_2}$ is the graded parallelotopic graph. In finite case it is tactical configuration with bidegrees which are products of $|M_r|$, $r \in \Delta(v) \backslash \Delta(v) \cap \Delta(u)$ and products of $|M_r|$, $r \in \Delta(u) \backslash \Delta(v) \cap \Delta(u)$, respectively.

2.4.5. Blowing of Coxeter geometries and Lie geometries

Let G be the finite simple group of Lie type of rank n defined over the field $\mathbb{K}$ with the Borel subgroup B and Weyl group W. Let $B = U\lambda T$ be the decomposition of B into semidirect product of unipotent subgroup U and the maximal torus T . The Coxeter group W is the Weyl group of certain root system R. Let r_i, $i = 1, \ldots, n$ be the system of fundamental roots (base) for R, R^+ and R^- are sets of positive and negative roots relatively to the chosen base. Let U_r, $r \in R$ be the root subgroup of the unipotent subgroup U, which admit the factorisation U into the product of U_r with respect to Bruhat's order on R^+. Each parabolic subgroup, i.e. proper subgroup of G containing the Borel subgroup of G containing the Borel subgroup B, is a subgroup of kind BW_JB, where J is a proper subset of standard set S

of generators formed by reflactions corresponding to r_i, $i = 1, \ldots, n$. It is known that (see [6])

$$\begin{aligned}
&\operatorname{diam}(GF(G)) = \operatorname{diam}(GF(W)),\\
&\operatorname{diam}(GF_{J_1,J_2}(G)) = \operatorname{diam}(GF_{J_1,J_2}(W)\\
&\operatorname{diam}(\Gamma(G)) = \operatorname{diam}(\Gamma(W)).
\end{aligned}$$

We can reformulate results of the previous section on the interpretations of Lie geometries in the following form.

Theorem 2.4.16. *Let G be the simple group of Lie type over the finite field $\mathbb{F}_q$, $q = p^m$ with the Weyl group W with the set S, $|S| = n$ of standard generators. Then*

(i) the incidence systems $GF(G)$, GF_{J_1,J_2}, $\Gamma(W)$, where J_1 and J_2 are subsets of S such that $J_1 \cap J_2 = \emptyset$, $\Gamma(G)$ are unipotent balanced blow up of $GF(W)$, $GF_{J_1,J_2}(W)$ and $\Gamma(W)$ over $\mathbb{F}_q$.

(ii) if G is a group of normal type then it is a linguistic blow up over $\mathbb{F}_q$ with the generic functions which are bilinear forms over this field.

(iii) if G is twisted group then it is a linguistic blow up with the bilinear form generic functions over the invariant subfield $\mathbb{F}_q$ for the field automorphism of same order with the corresponding symmetry of Coxeter-Dynkin diagram.

Let p be the prime number and $m = 1, 2, \ldots$ (m greater then the order of diagram symmetry in the twisted case). Then $\Gamma_{J_1,J_2}(G(p^m))$ as in the statement above form edge transitive family of small world graphs with memory. Graphs $\Gamma(G(p^m))$ and $GF(G(p^m))$ are also small world graphs with memory.

Remark 2.4.17. Let us consider the *orbitals of transformation group* $(G, GF(G(p^m)))$ $((W, GF(W))$, respectively) i.e. binary relations of orbits for the transformation group $(G, GF(G) \times GF(G))$ $((W, GF(W) \times GF(W))$, respectively). Their disjoint unions form a coherent configuration $C(G)$ generated by the incidence relation I . There is a natural one to one correspondence η_{p^m} between elements of $C(W)$ and $C(G(p^m)$ induced by Bruhats decomposition. Let ϕ be of the symmetric connected relation from $C(W)$ then $\eta_{p^m}(\phi)$, $m = 1, 2, \ldots$ form a family of small world graphs with memory over the alphabet $\mathbb{F}_p$. In fact neighbours of the vertex v in such graph can be given via list of types for walks with initial state v.

2.4.6. Regular small world graphs with unbounded diameter

In previous chapter we consider the examples of families of small world graphs with bounded diameter and $\log_{k_i}(v)$. This unit is devoted to some

construction of families of small world graphs with increasing diameter. In particular we consider several families of such graphs of bounded degree.

Theorem 2.4.18. *Let W be the Coxeter group corresponding to the Coxeter diagram A_n, ρ the diagram symmetry, j_1 and j_2 are of distinct nodes such that $\rho(j_1) = j_2$ and difference $|i - j|$ is numerical constants, which does not depend on n. Let us chose balanced blow up graph $G(a, n) = \tilde{GF}_{j_1,j_2}(a)(n)$ with the weight a for, each $n = 2, 3, \dots$. Then $G(a, n)$ with $n = 2, \dots$ form the family small world graphs with increasing diameter for each $a \geq 2$.*

Theorem 2.4.19. *Let W be the Coxeter group corresponding to the Coxeter diagram D_n . Let $n - 1$ and n be nodes of the diagram $\rho(n - 1) = n$ for the involutive diagram symmetry ρ. Let us chose balanced blow up $G_a(n) = \tilde{GF}_{n,n-1}(a)$ with the weight a for each $n = 4, 5, \dots$. Then the graphs $G_a(n)$, $n = 4, \dots$ form the family of small world graphs for each integer $a \geq 2$.*

Theorem 2.4.20. *Let W be the Coxeter group corresponding to the Coxeter diagram I_m with two nodes. Let us choose the balanced blow up*

$$P(a, 2k + 1) = \Gamma(\tilde{W})(a)$$

for each pair $(a, 2k + 1)$ with weight a, $k \geq 0$ and $P(a, 2k)$, $k \geq 2$ with both weights equal to a. Then graphs $P(a, n)$, $n = 1, 2, \dots$ form an infinite family of small world graphs of fixed valency $a + 1$ and diameter d, $n \leq d \leq 2n$.

Remark 2.4.21. In fact, families $G(a, n)$, $G_a(n)$, and $P(a, n)$ are families of small world graphs depending from two parameters a and n.

Remark 2.4.22. If a is prime degrees then for the proper choice of linguistic blow up $P(a, n)$ will be the graph without cycles C_4 (see examples in [9] and [17]. In this case graph $P^2(a, n)$, $n = 1, 2, \dots$ binary relation: two points of $P(2, n)$ are incident to common line, form an infinite family of small world graphs of diameter D, $n/2 \leq D \leq n$ with fixed degree $(a + 1)^2 - 1$.

Let us remove all edges between elements from the "largest Schubert cells" in $P(a, m)$ i.e. elements of kind (α, x), where $l(\alpha) = m - 1$. After the completion of this operation we shall get the graph $ST_m(a)$.

Lemma 2.4.23. *$ST_m(a)$ is a spanning tree for the graph $P(a, m)$.*

Proof. Let us consider the process of walking from one of the vertices $(\langle a \rangle, 0)$ or $(\langle b \rangle, 0)$ which does not contain the edge between these two verices. This branching processes produce rooting trees $T_{\langle a \rangle}$ and $T_{\langle b \rangle}$. They do not contain common vertices. So adding extra edge between $(\langle a \rangle, 0)$ and $(\langle b \rangle, 0)$ leads to the tree $ST_m(q)$, which contains all vertices of $PC_m(q)$. □

2.5. Small word expanding graphs of large girth or large cycle indicator

2.5.1. On the expansion properties of special graphs

Many applications of tree approximations use expansion properties of graphs (Coding Theory, Cryptography, parallel computations and some other area of Computer Science (see [57] and further references).

The *families of graphs of large girth*, i.e. infinite families of simple regular graphs Γ_i of degree k_i and order v_i such that

$$g(\Gamma_i) \geq \gamma \log_{k_i} v_i,$$

where c is the independent of i constant (see [7], [8]). Erdős proved the existence of such a family with arbitrary large but bounded degree $k_i = k$ with $\gamma = 1/4$ by his famous probabilistic method.

Just two explicit families of graphs of large girth with unbounded girth and arbitrarily large k are known: the family of Cayley graphs had been defined by G. Margulis (see next unit) and investigated further by several authors and the family of algebraic graphs $CD(n, q)$ (see Chapter 3).

The first explicit examples of families with large girth were mention above given by Margulis [93], [94], [95] with $\gamma = 0.44$ for some infinite families with arbitrary large valency, and $\gamma = 0.83$ for an infinite family of graphs of valency 4. The constructions were Cayley graphs of $SL_2(Z_p)$ with respect to special sets of generators. Imrich [59] was able to improve the result for an arbitrary large valency, $\gamma = 0.48$, and to produce a family of cubic graphs (valency 3) with $\gamma = 0.96$. A family of geometrically defined cubic graphs, so called sextet graphs, was introduced by Biggs and Hoare. They conjectured that these graphs have large girth. Weiss proved the conjecture by showing that for the sextet graphs (or their double cover) $\gamma \geq 4/3$. Then independently Margulis (see [93], [94] , [95]) and Lubotsky, Phillips, and Sarnak [87] came up with similar examples of graphs (graphs $X(p, q)$) with $\gamma \geq 4/3$ and arbitrary large valency (they turned out to be, additionally, so-called Ramanujan graphs). In [9] Biggs and Boshier showed that that γ is asymptotically $4/3$ for graphs from [93], [94], [95].

Let us consider these facts in more details. Recall, that *adjacency matrix* T for k-regular graph X on the vertex set $\{1, 2, \ldots, m\}$ is $m \times m$ matrix $(t_{i,j})$ such that $t_{i,j} = 1$ if nodes i and j are connected by an edge, if i and j do not form an edge in X, then $t_{i,j} = 0$. The matrix T of simple graph is symmetrical, so all its eigenvalues (eigenvalues of the graph) are real numbers. It is easy to see that k is the largest eigenvalue of the graph. Let $\lambda_1(X)$ be the second largest eigenvalue.

Let A be a set of vertices of simple graph X. We define ∂A to be the set of all elements $b \in X - A$ such that b is adjacent to some $a \in A$.

We say that *k-regular graph with n vertices has an expansion constant c* if there exists a constant $c > 0$, such that each set $A \subset X$ with $|A| \leq n/2$, that $|\partial A| \geq c|A|$.

One says that the infinite family of graph X_i is a *family of expanders*, if there exists a constant c which is an expansion constant for each graph X_i.

An explicit construction of infinite families of t-regular expanders (k-fixed) turns out to be difficult. It can be shown that if $\lambda_1(X)$ is the second largest eigenvalue of the adjacency matrix of the graph X, then $c \geq (k - \lambda_1)/2k$. Thus, if λ_1 is small, the expansion constant is large.

So, the family X_i of t-regular graphs will be a family of expanders, if the upper bound for the limit $\lambda_1(X_n)$, $n \to \infty$ is bounded away from t. A well-known result of Alon and Bopanna says, that if X_n is an infinite family of k-regular graphs (k fixed), then $\lim \lambda_1(X_n) \geq 2\sqrt{k-1}$. This statement was the motivation of Ramanujan graphs as special objects among k-regular graphs. A finite t-regular graph Y is called *Ramanujan*, if for every eigenvalue λ of Y, either $|\lambda| = k$ or $|\lambda| \leq 2\sqrt{k-1}$. So, Ramanujan graphs are, in some sense, the best expanders. There is an interest to families of the Ramanujan graph of unbounded degree too.

Gregory Margulis constructed the first family of expanders via studies of Cayley graphs of large girth. He uses representation theory of semisimple groups.

Lubotzky, Phillips and Sarnak [87] proved that defined below Cayley graphs introduced by G. Margulis [93] are Ramanujan graphs of degree $p + 1$ for all primes p.

2.5.2. On small world Ramanujan graphs

In this section we describe *Ramanujan graphs* and discuss their use for the generation of matrices with large order. We give a brief outline of the explicit construction of a class of Cayley graphs called *the Ramanujan Graph* $X(p, q)$ due to Lubotzky, Phillips and Sarnak [87].

Let p and q be primes, $p \equiv q \equiv 1 (\mathrm{mod}\ 4)$. Suppose that i is an integer so that $i^2 \equiv -1 (\mathrm{mod}\ q)$. By a classical formula of Jacobi, we know that there are $8(p + 1)$ solutions $\alpha = (a_0, a_1, a_2, a_3)$ such that $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. Among these, there are exactly $p+1$ with $a_0 > 0$ and a_0 odd and a_j even for $j \in \{1,\ 2,\ 3\}$, as is easily shown. To each such α we associate the matrix

$$\tilde{\alpha} = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}$$

which gives us $p+1$ matrices in $\mathrm{PGL}_2(\mathbb{F}_q)$. We let S be the set of generators of these matrices $\tilde{\alpha}$ and take $\mathrm{PGL}_2(\mathbb{F}_q)$. In [6], it is shown that the Cayley graphs $X(p,q)$ will be a $(p+1)$-regular graph, namely the Cayley graph of $\mathrm{PSL}_2(\mathbb{F}_q)$ if $\left(\frac{p}{q}\right) = 1$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ if $\left(\frac{p}{q}\right) = -1$, (where $\left(\frac{p}{q}\right)$ is the Legendre symbol). As we vary q, we get an infinite family of such graphs, all $p+1$-regular.

Moreover, in papers written by Lubotzky, Phillips and Sarnak [6], an explicit formula for the girth $g(X(p,q))$ of $X(p,q)$ was found.

Corollary 2.5.1. [87] *The following cases draw ahead:*

(1) *If* $\left(\frac{p}{q}\right) = -1$ *then* $X(p,q)$ *is bipartite of order* $n = |X(p,q)| = q(q^2-1)$ *and*

$$g(X(p,q)) \geq 4\log_p q - \log_p 4$$

(2) *If* $\left(\frac{p}{q}\right) = 1$ *then* $X(p,q)$ *is not bipartite,* $n = |X(p,q)| = q(q^2-1)/2$ *and*

$$g(X(p,q)) \geq 4\log_p q.$$

Corollary 1 above shows that the Ramanujan graph $X(p,q)$ of order v asymptotically satisfies $g(X(p,q)) \geq 4\log_p v/3$ [87].

Theorem 2.5.2. *Graphs* $X(p,q)$, $q \to \infty$ *form a family of* $(p+1)$ *regular small world Ramanujhan graphs of large girth with the diameter bounded by* $2\log_p(v) + 2$ *and the girth* $g(X(p,q)) \approx 4\frac{4}{3}\log_p(v)$.

Here we can use the Ramanujan graphs to generate matrices with large order. The algorithm is:

Algorithm 2.5.3. *Let* $X(p,q)$ *be the Ramanujan graph. Then*

(1) *Take the product*

$$g = s_{i_1}s_{i_2}\dots s_{i_k}, \qquad (k - small, \quad s_{i_j} \in S, j = 1,\dots,k)$$

and $s_{i_1} \neq s_{i_k}^{-1}$. *(We can chose the sequence* $s_{i_1}s_{i_2}\dots s_{i_k}$ *in a way that* g *is not similar to a diagonal matrix or matrix of the kind* $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$*)*

(2) *The order* $|g|$ *of* g *is such that* $|g| \geq \frac{g(X(p,q))}{k}$, *where* ($g\,(X\,(p,q))$*-girth of the Ramanujan graph* $X\,(p,q)$*).*

Example 2.5.4. We now construct the sequence of the Ramanujan graphs $X(p,q)$, where $p = 5$ and q is prime. For the equation $a_0^2 + a_1^2 + a_2^2 + a_3^2 = 5$ there are $8(p+1) = 48$ solutions, with 6 of them having the property that $a_0 > 0$ and a_0 is odd and a_1, a_2, a_3 are even. To each of these solutions

$\alpha_k = (a_{k,0}, a_{k,1}, a_{k,2}, a_{k,3})$, $k = 1, 2, \ldots, 6$ we associate a matrix $\tilde{\alpha_k}$ in $PGL(5, q)$ as follows:

$$s_k = \tilde{\alpha_k} = \begin{pmatrix} a_{k,0} + ia_{k,1} & a_{k,2} + ia_{k,3} \\ -a_{k,2} + ia_{k,3} & a_{k,0} - ia_{k,1} \end{pmatrix}$$

where $i^2 \equiv -1 (\mathrm{mod}\ q)$.

We have $\alpha_1 = (1, 0, 0, -2)$, $\alpha_2 = (1, 0, -2, 0)$, $\alpha_3 = (1, -2, 0, 0)$, $\alpha_4 = (1, 0, 0, 2)$, $\alpha_5 = (1, 0, 2, 0)$, $\alpha_6 = (1, 2, 0, 0)$. For example, if $q = 17$, then

$$s_1 = \begin{pmatrix} 1 & 9 \\ 9 & 1 \end{pmatrix} s_2 = \begin{pmatrix} 1 & 15 \\ 2 & 1 \end{pmatrix} s_3 = \begin{pmatrix} 10 & 0 \\ 0 & 9 \end{pmatrix}$$

$$s_4 = \begin{pmatrix} 1 & 8 \\ 8 & 1 \end{pmatrix} s_5 = \begin{pmatrix} 1 & 2 \\ 15 & 1 \end{pmatrix} s_6 = \begin{pmatrix} 9 & 0 \\ 0 & 10 \end{pmatrix}$$

2.5.3. On small world graph with large cycle indicator and their expansion properties

We generalize the concept of family of large girth in the following way Let $g_x = g_x(\Gamma)$ be the length of the minimal cycle through the vertex x from the set $V(\Gamma)$ of vertices in graph Γ. We refer to

$$\mathrm{Cind}(\Gamma) = \max\{g_x,\ x \in V(\Gamma)\}$$

as *cycle indicator* of the graph Γ.

We refer to the graph Γ as *cycle irregular graph* if

$$\mathrm{Cind}(\Gamma) \neq g(\Gamma).$$

We refer to the family of regular simple graphs Γ_i of degree k_i and order v_i as *family of graphs of large cycle indicator*, if

$$\mathrm{Cind}(\Gamma_i) \geq c\log_{\mathrm{k_i}}(v_i)$$

for some independent constant c, $c > 0$. We refer to the maximal value of c satisfying the above inequality as *speed of growth* of the cycle indicator for family of graphs Γ_i.

We refer to such a family as a *family of cyclically irregular graphs of large cycle indicator* if almost all graph from the family are cycle irregular graphs.

We got the algebraic construction of the family of cyclically irregular graphs of large cycle indicator. The pseudorandom nature of graphs can be used for the development of algorithms for Post-Quantum Cryptography.

The size of constructed sequence of graphs $A(n,q)$, $n = 2,3,\ldots$ with the given degree of kind $q = p^s$, where p is arbitrary odd prime and s is arbitrary positive integer, belongs to the upper bound of previous theorem. Irregularity of cycle indicator insure that graphs are not vertex transitive. The description of this extremal graphs is below.

Let $\mathbb{F}_q$ be a finite field of order q. Recall, that a bipartite graph $A(n,q) = A(n,\mathbb{F}_q)$ with the set of points $P = \mathbb{F}_q^n$ and set of lines $L = \mathbb{F}_q^n$ via incidence relation I: xIy for $x = (x_1, x_2, \ldots, x_n) \in P$ and $y = [y_1, y_2, \ldots, y_n] \in L$ if and only if, when conditions $y_2 - x_2 = y_1x_1$, $y_3 - x_3 = x_1y_2$, $y_4 - x_4 = y_1x_3$, $y_5 - x_5 = x_1y_4$, ... with the last equation $y_n - x_n = y_1x_{n-1}$ in the case of n even or the last equation $y_n - x_n = x_1y_{n-1}$ in the case of n odd. Brackets and parenthesis will allow us to distinguish points and lines again.

Theorem 2.5.5. *Graphs $A(n,q)$ form a family of graphs of small word graphs which is a family of cyclically irregular graphs of large cycle indicator.*

The computer simulations are supporting the following assumption.

Conjecture 1. *Graphs $A(n,q)$, $n = 2,3,\ldots$ form a family of graphs of large girth.*

Theorem 2.5.6. *The second largest eigenvalue of $A(n,q)$ is bounded by $2\sqrt{q}$.*

So they are very good expanders which close to Ramanujan graphs [176]. In fact , q-regular Wegner graphs $W(n,q)$ and graphs $CD(n,q)$ have the second largest eigenvalue $\leq 2\sqrt{q}$ also. Graphs $W(n,q)$ form a family of small world graphs. There is a conjecture that $CD(n,q)$ is an other family of small world graphs (see [178] for further details).

Chapter 3

On regular trees and simple graphs given by nonlinear equations

3.1. On biregular trees and free products of finite simple groups

We need the following well known results on groups acting on graphs.

Let G be a group with proper distinct subgroups G_1 and G_2. Let us consider the incidence structure with the point set $P = (G : G_1)$ and the line set $(G : G_2)$ and incidence relation $I : \alpha I \beta$ if and only if the set theoretical intersection of cosets α and β is nonempty set. We shall not distinguish the incidence relation and corresponding graph $\Gamma(G)_{G_1,G_2}$.

Lemma 3.1.1. *Graph I is connected if and only if $G = \langle G_1, G_2 \rangle$.*

Let

$$A = \langle a_1, \dots, a_n | R_1(a_1, \dots, a_n), \dots, R_d(a_1, \dots, a_n) \rangle ,$$
$$B = \langle b_1, \dots b_m | S_1(b_1, \dots b_m), \dots, S_t(b_1, \dots, b_m) \rangle$$

are subgroups with generators a_i, $i = 1, \dots, n$ and b_j, $j = 1, \dots, m$ and generic relations R_i, $i = 1, \dots, d$ and S_j, $j = 1, \dots, t$, respectively. Free product $F = A * B$ of A and B (see [19]) is the following group

$$\langle a_1, \dots, a_n, b_1, \dots, b_m | R_1, \dots R_d, S_1, \dots, S_t \rangle .$$

The definition of an operation of free product F_H of groups A and B amalgamated at common subgroup H can be found in [20]. If $H = \langle e \rangle$, then $F_H = A * B$.

Theorem 3.1.2. *(see, for instance [19]) Let G acts edge transitively but not vertex transitively on a tree T. Then G is the free product of the stabilizers G_a and G_b of adjacent vertices a and b amalgamated at their intersection.*

Corollary 3.1.3. *Let G acts edge regularly on the tree T, i.e. $|G_a \cap G_b| = 1$. Then G is the free product $G_a * G_b$ of groups G_a and G_b.*

Corollary 3.1.4. *Let A and B be a finite groups and $G = A * B$ is their free product. Then $\Gamma_{A,B}(G)$ is an infinite biregular tree $T_{r,s}$ with bidegrees $r = |A|$ and $s = |B|$.*

3.2. On infinite family of simple graphs $D(n, \mathbb{K})$ defined by nonlinear algebraic equations

We define the family of graphs $D(n, \mathbb{K})$, where $n > 2$ is positive integer and $\mathbb{K}$ is a commutative ring, such graphs have been considered in [81] for the case $\mathbb{K} = \mathbb{F}_q$ (some examples are in [78]).

Let P and L be two copies of Cartesian power $\mathbb{K}^{\mathbb{N}}$, where $\mathbb{K}$ is the commutative ring and $\mathbb{N}$ is the set of positive integer numbers. Elements of P will be called *points* and those of L *lines*.

To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to adopt the notation for co-ordinates of points and lines introduced in [79] for the case of general commutative ring $\mathbb{K}$:

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \ldots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \ldots),$$
$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \ldots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \ldots].$$

The elements of P and L can be thought as infinite ordered tuples of elements from $\mathbb{K}$, such that only finite number of components are different from zero.

We now define an incidence structure (P, L, I) as follows. We say the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their co-ordinates hold:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1}p_{0,1} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1} \\ l_{i+1,i} - p_{i+1,i} &= l_{1,0}p'_{i,i} \end{aligned}$$

(This four relations are defined for $i \geq 1$, $p'_{1,1} = p_{1,1}, l'_{1,1} = l_{1,1}$. This incidence structure (P, L, I) we denote as $D(\mathbb{K})$. We speak now of the incidence graph of (P, L, I), which has the vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

Theorem 3.2.1. *If $\mathbb{K}$ is the finite field $\mathbb{F}_q$ then $D(\mathbb{F}_q) = D(q)$ is a infinite forest.*

For each positive integer $n \geq 2$ we obtain an incidence structure (P_n, L_n, I_n) as follows. First, P_n and L_n are obtained from P and L, respectively, by simply projecting each vector onto its n initial coordinates. The incidence I_n is then defined by imposing the first $n-1$ incidence relations and ignoring all others. The incidence graph corresponding to the structure (P_n, L_n, I_n) is denoted by $D(n, \mathbb{K})$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = -1$, and to assume that (6) are defined for $i \geq 0$.

Notice that for $i = 0$, the four conditions (6) are satisfied by every point and line, and, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0}p_{0,1}$.

The incidence relation motivated by the linear interpretation of Lie geometries in terms their Lie algebras [39] (see [151]). [153]). Let us define the "root subgroups" U_α, where the "root" α belongs to the root system $\mathrm{Root} = \{(10),(01),(11),(12),(21),(22),(22)',\dots,(i,i),(ii)',(i,i+1),(i+1,i)\dots\}$. Group U_α generated by the following "root transformations" $t_\alpha(x)$, $x \in \mathbb{K}$ of the $\mathrm{P} \cup \mathrm{L}$:

1. The transformations $t_{1,0}(x)$, acts on the coordinates of l and p by the following rules.

$$\begin{aligned}
\mathrm{l}^{t_{1,0}(x)} =&[l_{1,0}+x, l_{1,1}, l_{2,1}-l_{1,1}x, l_{1,2}, l_{2,2}, \dots, l'_{s,s}+l_{s-1,s}x, l_{s+1,s}+l_{s,s}x,\\
&l_{s,s+1}, l_{s+1,s+1}, \dots];\\
\mathrm{p}^{t_{1,0}(x)} =&(p_{0,1}, p_{1,1}-p_{0,1}x, p_{2,1}-2p_{1,1}+p_{0,1}x^2, p_{1,2}, p_{2,2}+p_{1,2}x, \dots,\\
&p_{s+1,s}-(p_{s,s}+p'_{s,s})x+p_{s-1,s}x^2, p_{s,s+1}, p_{s+1,s+1}-p_{s,s+1}x, \dots)
\end{aligned}$$

2. The transformations $t_{0,1}(x)$, acts on the coordinates of l and p by the following rules.

$$\begin{aligned}
[\mathrm{l}]^{t_{0,1}(x)} =&[l_{1,0}, l_{1,1}+l_{1,0}x, l_{1,2}+2l_{1,1}x+l_{1,0}x^2, l_{2,1}, l_{2,2}+l_{2,1}x, \dots,\\
&l'_{s,s}+l_{s,s-1}x, l_{s,s+1}+(l_{s,s}+l'_{s,s})x+l_{s,s-1}x^2, l_{s+1,s}, l_{s,s}+l_{s,s-1}x, \dots]\\
(\mathrm{p})^{t_{0,1}(x)} =&(p_{0,1}+x, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \dots)
\end{aligned}$$

3. The transformations $t_{1,1}(x)$, acts on the coordinates of l and p by the following rules.

$$\begin{aligned}
\mathrm{l}^{t_{1,1}(x)} =&[l_{1,0}, l_{1,1}+x, l_{1,2}, l_{2,1}+l_{1,0}x, l_{2,2}-l_{1,1}x, l'_{2,2}+l_{1,1}x, \dots,\\
&l_{s,s}-l_{s-1,s-1}x, l'_{s,s}+l_{s-1,s-1}x, l_{s,s+1}-l_{s-1,s}x, l_{s+1,s}+l_{s,s-1}x, \dots]\\
\mathrm{p}^{t_{1,1}(x)} =&(p_{0,1}, p_{1,1}+x, p_{1,2}-p_{0,1}x, p_{2,1}, p_{2,2}-p_{2,1}x, \dots,\\
&p_{s,s}-p_{s-1,s-1}x, p'_{s,s}-p'_{s-1,s-1}x, p_{s,s+1}-p_{s-1,s}, p_{s+1,s}+p_{s,s-1}x, \dots)
\end{aligned}$$

4. The transformations $t_{m+1,m}(x)$, $m \geq 1$ acts on the coordinates of l and p by the following rules.

$$\begin{aligned}
&l_{m+1,m} \to l_{m,m+1}+x, && p_{m,m+1} \to p_{m,m+1}+x,\\
&l'_{m+1,m+1} \to l'_{m+1,m+1}, && p'_{m+1,m+1} \to p'_{m+1,m+1}+p_{0,1}x,\\
&l'_{m+r,m+r} \to l'_{m+r,m+r}-l_{r-1,r}x, && p'_{m+r,m+r} \to p'_{m+r,m+r}-p_{r-1,r}x,\ r \geq 2,\\
&l_{m+r+1,m+r} \to l_{m+r+1,m+r}-l_{r,r}x, && p_{m+r+1,m+r} \to p_{m+r+1,m+r}-p_{r,r}x,\ r \geq 2.
\end{aligned}$$

All other components are unchanged.

5. The transformation $t_{m,m+1}(x)$, $m \geq 1$ is defined by following rules.

$$l_{m,m+1} \to l_{m,m+1} + x, \qquad p_{m_m+1} \to p_{m,m+1} + x,$$
$$l_{m+1,m+2} \to l_{m+1,m+2} + l_{1,1}x, \qquad p_{m+1,m+2} \to p_{m+1,m+2} + p_{1,1}x,$$
$$l_{m+1,m+1} \to l_{m+1,m+1} + l_{1,0}x$$
$$l_{m+r,m+r+1} \to l_{m+r,m+r+1} + l'_{r,r}x, r \geq 2.$$

   All other components are unchanged.
6. The transformation $t'_{m,m}(x)$ acts on vertices of $D(\mathbb{K})$ by the following rules.

$$l'_{m,m} \to l'_{m,m} + x, \qquad p'_{m,m} \to p'_{m,m} + x,$$
$$l_{m+1,m} \to l_{m+1,m} + l_{1,0}x, \qquad p_{m+1,m+1} \to l_{m+1,m+1} + p_{1,1}x,$$
$$l_{m+1,m+1} \to l_{m+1,m+1} + l_{1,1}x, \qquad p_{m+r,m+r} \to p_{m+r,m+r} + p'_{r,r}x, r \geq 2,$$
$$l_{m+r,m+r} \to l_{m+r,m+r} + l'_{r,r}x, \qquad p_{m+r+1,m+r} \to p_{m+r+1,m+r} + p_{r+1,r}x,\ r \geq 2.$$
$$l_{m+r+1,m+r} \to l_{m+r+1,m+r} + l_{r+1,r}x,$$

   All other components are unchanged.
7. The transformation $t_{m,m}(x), m \geq 1$ act on coordinates of vertices by the following rules.

$$l_{m,m} \to l_{m,m} + x, \qquad p_{m,m} \to p_{m,m} + x,$$
$$l_{m+r,m+r} \to l_{m+r,m+r} - l_{r,r}x, \qquad p_{m,m+1} \to p_{m,m+1} - p_{0,1}x,$$
$$p_{m+r,m+r} \to p_{m+r,m+r} - p_{r,r}x,\ r \geq 1.$$

   All other components are unchanged.

Note that action of each transformation above on the n-s component of a vertex from $P \cup L$ depends only from this component itself and previous components. Thus we can define a natural projection of this transformation onto the graph $\mathrm{D}(n, \mathbb{K})$.

Proposition 3.2.2. (i) *For each pair* (α, x), $\alpha \in \mathrm{Root}$, $x \in \mathbb{K}$ *the transformation* $t_\alpha(x)$ *are automorphisms of* $D(\mathbb{K})$. *The projections of these maps onto the graph* $D(n, \mathbb{K})$, $n \geq 2$ *are elements of* $Aut(D(n, \mathbb{K}))$.
(ii) *Group* $\mathrm{U}(\mathbb{K})$ *acts edge regularly on the vertices of* $\mathrm{D}(\mathbb{K})$.
(iii) *Group* $\mathrm{U}(n, \mathbb{K})$ *generated by projections of* $t_\alpha(x)$ *onto the set of vertices* V *of* $\mathrm{D}(n, \mathbb{K})$ *acts edge regularly on* V.

Proof. Statement (i) follows directly from the definitions of incidence and closed formulas of root transformations $t_\alpha(x)$. Let $<$ be the natural lexicographical linear order on roots of kind (i, j), where $|i - j| \leq 1$. Let us assume additionally that $(i, i) < (i, i)' < (i, i + 1)$. Then by application of

transformations $t_\alpha(x_\alpha)$, $\alpha \neq (0,1)$ to a point (p) consecutively with respect to the above order, where parameter x_α is chosen to make α component of the image equals zero, we are moving point (p) to zero point (0). A neighbour $[a,0,\dots,0]$ of the zero point can be shifted to the line $[0]$ by the transformation $t_{(1,0)}(-a)$. Thus each pair of incident elements can be shifted to $((0),[0])$ and group U acts edge regularly on vertices of $D(\mathbb{K})$. This action is regular $((ii))$ because the stabilizer of the edge $(0),[0]$ is trivial. Same arguments about the action of $U(n,\mathbb{K})$ justify (iii).

□

Lemma 3.2.3. *Let ϕ_a be a binary relation : "difference of colours of the same type is a". Then group U ($U(n,\mathbb{K})$) preserves ϕ_a.*

Proof. Transformations t_α, $\alpha \neq (0,1),(1,0)$ preserves colours of vertices. Maps $t_{(0,1)}(x)$ and $t_{(1,0)}(x)$ preserve the binary relation ϕ_a for each $a \in \mathbb{K}$.

□

Let $k \geq 6$, $t = [(k+2)/4]$, and let $u = (u_\alpha, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $\mathrm{D}(k,\mathbb{K})$ ($\alpha \in \{(1,0),(0,1)\}$, it does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$$a_r = a_r(u) = \sum_{i=0,r} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1}),$$

and

$$a = a(u) = (a_2, a_3, \cdots, a_t).$$

Proposition 3.2.4. (i) *The classes of equivalence relation*

$$\tau = \{(u,v) | a(u) = a(v)\}$$

form the imprimitivity system of permutation groups $\mathrm{U}(\mathbb{K})$ *and* $\mathrm{U}(n,\mathbb{K})$.

(ii) *For any $t-1$ ring elements $x_i \in \mathbb{K}$, $2 \leq t \leq [(k+2)/4]$, there exists a vertex v of* $\mathrm{D}(k,\mathbb{K})$ *for which*

$$a(v) = (x_2, \dots, x_t) = (x).$$

(iii) *The equivalence class C for the equivalence relation τ on the set $\mathbb{K}^n \cup \mathbb{K}^n$ is isomorphic to the affine variety $\mathbb{K}^t \cup \mathbb{K}^t$, $t = [4/3n] + 1$ for $n = 0,2,3 \bmod 4$, $t = [4/3n] + 2$ for $n = 1 \bmod 4$.*

Proof. Let C be the equivalence class on τ on the vertex set $\mathrm{D}(\mathbb{K})$ ($\mathrm{D}(n,\mathbb{K})$ then the induced subgraph, with the vertex set C is the union of several connected components of $\mathrm{D}(\mathbb{K})$ ($\mathrm{D}(n,\mathbb{K})$).

Without loss of generality we may assume that for the vertex v of $C(n,\mathbb{K})$ satisfying $a_2(v) = 0, \dots a_t(v) = 0$. We can find the values components $v'_{i,i}$

from this system of equations and eliminate them. Thus we can identify P and L with elements of $\mathbb{K}^t$, where $t = [3/4n] + 1$ for $n = 0, 2, 3 \bmod 4$, and $t = [3/4n] + 2$ for $n = 1 \bmod 4$.

□

We shall use notation $C(t, \mathbb{K})$ ($C(\mathbb{K})$) for the induced subgraph of $D(n, \mathbb{K})$ with the vertex set C.

Remark 3.2.5. If $\mathbb{K} = \mathbb{F}_q$, q is odd, then the graph $C(t, k)$ coincides with the connected component $CD(n, q)$ of the graph $D(n, q)$ (see [164]), graph $C(\mathbb{F}_q)$ is a q-regular tree. In other cases the question on the connectedness of $C(t, \mathbb{K})$ is open. It is clear that $g(C(t, \mathbb{F}_q))$ is $\geq 2[2t/3] + 4$.

We define an incidence structure with point set P' and line set L'. It will be convenient for us to denote vectors from P' as

$$\mathrm{x} = (\mathrm{x}) = (x_{0,1}, x_{1,1}, x_{1,2}, x_{2,2}, \dots x_{i,i}, x_{i,i+1} \dots,)$$

and vectors from L' as

$$\mathrm{y} = [\mathrm{y}] = [y_{1,0}, y_{1,1}, y_{1,2}, y_{2,2}, \dots, y_{i,i}, y_{i,i+1}, \dots].$$

We say that point (x) is incident with the line [y] and we write it xJy or (x)J[y] if and only if the following condition are satisfied:

$$y_{i,i} - x_{ii} = x_{i-1,i} y_{1,0}$$
$$y_{i,i+1} - x_{i,i+1} = x_{0,1} y_{i,i}$$

where $i = 1, 2, \dots$.

Let $\mathrm{E}(\mathbb{K})$ be the incidence graph of the incidence graph of the incidence structure $\Gamma(\mathbb{K}) = (P', L', J')$. For each integer $k \geq 2$ let $\Gamma(k, q) = (P'_k, L'_k, J_k)$ be the incidence system, where P_k and L_k are images of P and L under the projection of these spaces on the first k -coordinates and binary relation $J(k)$ is defined by the first k equations. Finally, let $\mathrm{E}(k, \mathbb{K})$ be the incidence graph for $\Gamma(k, \mathbb{K})$.

Similarly we can define an incidence structure $E'(\mathbb{K})$ with points of kind

$$(\mathrm{x}) = (x_{0,1}, x_{1,1}, x_{2,1}, \dots, x'_{i,i}, x_{i+1,i}, \dots),\ i \geq 2,$$

lines of kind

$$[\mathrm{y}] = [y_{1,0}, y_{1,1}, y_{2,1}, \dots y'_{i,i}, y_{i+1,i}, \dots]$$

and the incidence relation given by equations

$$y'_{i,i} - x'_{i,i} = y_{i,i-1} x_{0,1},$$
$$y_{i+1,i} - x_{i+1,i} = y_{1,0} x'_{i,i}.$$

By projections of the point space and the line space on the first k components we get the quotient graph $E'(n, \mathbb{K})$. It is easy to see that graphs $E(\mathbb{K})$ and $E'(\mathbb{K})$ ($E(n, \mathbb{K})$ and $E'(n, \mathbb{K})$) are isomorphic.

Let us recall some information from graph theory. Let G be the graph with the colouring $\rho : V(G) \to C$ of the set of vertices $V(G)$ into colours from C such that the *neighbourhood of each vertex looks like rainbow*, i.e. consists of $|C|$ vertices of different colours. In case of pair (G, ρ), we shall refer to G as *parallelotopic graph* with the local projection ρ.

It is obvious that parallelotopic graphs are k-regular with $k = |C|$. Linguistic graphs are just bipartite parallelotopic graphs of order $2q^t$ and degree $q = p^s$ where p is a prime number.

If C' is a subset of C, then induced subgraph $G^{C'}$ of G which consists of all vertices with colours from C' is also a parallelotopic graph. It is clear that connected component of the parallelotopic graph is also a parallelotopic graph.

The *arc* of the graph G is a sequence of vertices $v_1, \dots, v_k$ such that $v_i I v_{i+1}$ for $i = 1, \dots, k-1$ and $v_i \neq v_{i+2}$ for $i = 1, \dots, k-2$. If $v_1, \dots, v_k$ is an arc of the parallelotopic graph (G, ρ) then $\rho(v_i) \neq \rho(v_{i+2})$ for $i = 1, \dots, k-2$.

The *trail* of the graph G is the sequence of vertices $v_1, \dots, v_k$, such that $v_i \neq v_{i+1}$, $i = 1, \dots, k-1$ and $v_1 = v_k$.

If (G_1, ρ_1) and (G_2, ρ_2) be two parallelotopic graphs over the same set of colours. We say that graph homomorphism $\phi : G_1 \to G_2$ is a parallelotopic morphism if $\rho_1(v) = \rho_2(\phi(v))$ for each vertex v of the graph G_1.

Parallelotopic morphism moves arc of the graph G_1 into the arc of graph G_2.

Example 3.2.6. Let $\Gamma = \Gamma_k(\mathbb{K})$ be one graph among the graphs $D(k, \mathbb{K})$, $CD(k, \mathbb{K})$ and $E(k, \mathbb{K})$. Γ with the colouring $\rho([\mathrm{x}]) = x_1$, $\rho((\mathrm{x})) = x_1$ is a parallelotopic graph. If $\mathbb{K} = \mathbb{F}_q$, then it is q-regular bipartite graph with $2q^k$ vertices. The map η_s of deleting the s last components of the tuple-vertex (point or line) of $\Gamma_{k+s}(q)$ is a parallelotopic morphism onto $\Gamma_k(q)$.

Example 3.2.7. Let ϕ be a map of deleting of coordinates with indices $(i, i+1)$, $(i, i)'$ for vertices of $D(\mathbb{K})$ (or $CD((\mathbb{K}))$. Then ϕ is a parallelotopic morphism onto the graph $E(\mathbb{K})$. It is preserves not only colours but all components $x_\alpha, \alpha \in \mathrm{Root}'$, where Root' contains exactly $(1, 0)$, $(0, 1)$, (i, i), $(i, i+1)$, $i = 1, 2, \dots$.

Example 3.2.8. We can consider the map ϕ_n (ϕ'_n)on the set of vertices of the graph $D(n, \mathbb{K})$. The image of this parallelotopic morphism belongs to the family $E(k, \mathbb{K})$ ($E'(k, \mathbb{K})$, respectively).

Let $U_\alpha = \langle t_\alpha(x) | x \in \mathbb{K} \rangle$ be a subgroup of $U(\mathbb{K})$. It is isomorphic to the additive group $\mathbb{K}^+$ of the ring $\mathbb{K}$. Let U^C be subgroup generated by $t_\alpha(x)$, $x \in \mathbb{K}$, $\alpha \in \{(0, 1, (1, 0), \dots, (i, i), (i, i+1), \dots\}$. Let ${U_n}^C$ be the subgroup generated by transformations $t_\alpha(x)$ from U^C onto the graph $D(n, \mathbb{K})$ (or $C(t, \mathbb{K})$).

Proposition 3.2.9. (i) *The connected component* $CD(n,\mathbb{K})$ *of the graph* $D(n,\mathbb{K})$ *(or its induced subgraph* $C(t,\mathbb{K})$*) is isomorphic to* $\Gamma({U_n}^C)_{U_{(0,1)},U_{(1,0)}}$.
(ii) *Projective limit of graphs* $D(n,\mathbb{K})$ *(graphs* $C(t,\mathbb{K})$, $CD(n,\mathbb{K})$ *) with respect to paralletopic morphisms of* $D(n+1,\mathbb{K})$ *onto* $D(n,\mathbb{K})$ *(their restrictions on induced subgraphs) equals to* $D(\mathbb{K})$ ($C(\mathbb{K})$, $CD(\mathbb{K}) = {U^C}_{U_{(0,1)},U_{(1,0)}}$, *respectively).*

Remark 3.2.10. Let $v_1, v_2, \dots v_k$ be the pass in the parallelotopic graph G, then it is uniquely determined by the starting point v_1 of the colour c_1 and the sequence of colours $c_2, \dots c_k$ of colours of vertices $v_2, \dots, v_k$, respectively. We have $c_i \neq c_{i+2}$, for $i = 1, \dots, k-2$.

The following statement can be proven by straightforward induction on n.

Lemma 3.2.11. *(two numbers lemma)*
Let $[\mathrm{y}_1]I(\mathrm{y}_2)I \dots I\mathrm{y}_n$ *be the path in the graph* $E(n,\mathbb{K})$, $n \geq 4$ *starting from the zero point* ($\mathrm{y}_1 = 0$) *defined by the sequence of colours* 0, x_1, x_2, $\dots$, x_{n-1}. *Then two last components of the vertex* y_n *are*

$$\alpha = x_1x_2(x_1 - x_3)\dots(x_{n-3} - x_{n-1}) \quad \textit{and} \quad \beta = -x_{n-2}\alpha.$$

3.3. On polarity graphs of incidence structures

Let P and L be disjoint sets, the elements of which we call points and lines, respectively. A subset I of $P \times L$ is called an incidence relation on the pair (P, L). The *incidence graph* Γ of geometry (P, L, I) is defined to be the bipartite graph with vertex set $P \cup L$ and edge set $\{\{p, l\} | p \in P, l \in L, (p, l) \in L\}$.

Let $\pi : P \cup L \to P \cup L$ be a bijection for which the following hold

(i) $P^\pi = L$ and $L^\pi = P$,
(ii) for all $p \in P$, $l \in L$ $(l^\pi, p^\pi) \in I$ if and only if $(p, l) \in I$,
(iii) $\pi^2 = 1$.

We call such π a polarity of the incidence structure (P, L, I). Note that π induces an order two automorphism of the incidence graph Γ which interchanges the bipartition sets P and L. We shall use the term "polarity" and the notation "π" for the graph automorphism as well.

We now define the *polarity graph* Γ^π of the structure (P, L, I) with respect to polarity π. It is the graph with the vertex set $V(\Gamma^\pi) = P$ and edge set $E(\Gamma^\pi) = \{\{p_1, p_2\}\} | p_1, p_2 \in P, p_1 \neq p_2, (p_1, {p_2}^\pi) \in I\}$.

Finally, we call point $p \in P$ an *absolute point of the polarity* π provided (p, p^π) in I.

Let N_π denote the number of absolute points of π.

Proposition 3.3.1. *(see, for instance* [85]*)*

Let π be be a polarity of the finite incidence structure (P, L, I) and let Γ and Γ^π be the correspondent incidence and polarity graphs.

(a) $\deg_{\Gamma^\pi} = \deg_{\Gamma^\pi} - 1$ *if p is an absolute point of π, and* $\deg_{\Gamma\pi} = \deg_\Gamma$ *otherwise.*

(b) $|V(\Gamma)^\pi| = 1/2|V(\Gamma)|$, $|E(\Gamma^\pi)| = |E(\Gamma)| - N_\pi$,

(c) *If Γ^π contains a $(2k+1)$-cycle then Γ contains a $(4k+2)$ cycle.*

(d) *If Γ^π contains a $2k$-cycle then Γ contains two vertex disjoint $2k$ cycles C and C' such that $C^\pi = C'$. Consequently, if Γ is $2k$-cycle-free then so is Γ^π.*

(e) *The girth of the two graphs are related by $g(\Gamma^\pi) \geq 1/2g(\Gamma)$.*

It is clear that statements (c), (d) and (e) are valid for an infinite incidence structure with polarities.

Let us consider the case of the incidence structure with paralleloopic graph (Γ, ρ) with the polarity π which is the parallelotopic morphism. We call such π a *parallelotopic polarity.* In that case we can define the *regular folding graph*

$$\mathrm{R}\Gamma = \mathrm{R}(\Gamma^\pi) = \{(p, p')|\rho(p) \neq \rho(p'), (p, p') \in E(\Gamma^\pi)\}.$$

Let us consider the case when the set B of colours of the absolute points is a proper subset of the set of all colours C. In that case we can define an *induced subgraph* $\mathrm{I}\Gamma = \mathrm{I}\Gamma^\pi$ with the set of vertices

$$\{v \in \Gamma^\pi | \rho(v) \in C - B\}.$$

Directly from the definitions and above proposition we are getting the following statement.

Lemma 3.3.2. *Let P, L, I be the incidence structure with the k-regular parallelotopic incidence graph Γ and parallelotopic polarity $\pi : \Gamma \to C$. Then $\mathrm{R}(\Gamma^\pi)$ is $k-1$-regular graph of girth $g(\mathrm{R}(\Gamma^\pi))$, where*

$$g(\mathrm{R}(\Gamma^\pi)) \geq g(\Gamma^\pi) \geq g(\Gamma).$$

If the set B of colours for absolute points of π is different from C, then $\mathrm{I}\Gamma$ is $|C - B|$-regular graph and

$$g(\mathrm{I}\Gamma)) \geq g(\Gamma^\pi) \geq g(\Gamma)$$

Remark 3.3.3. Graph $\mathrm{I}\Gamma$ is a parallelotopic graph. Let S be a finite proper subset of $C - B$ of cardinality s. Then the graph $\mathrm{I}\Gamma^S$ has valency s and

$$g(\mathrm{I}\Gamma^S) \geq g(\mathrm{I}\Gamma).$$

Remark 3.3.4. Graph $R\Gamma$ is not a parallelotopic graph because of sets of colours from tne neighbourhoods differs from vertex to vertex. Let S, $|S| = s$ be a subset of the colour set C of the parallelotopic graph Γ. Then parallelotopic polarity π induces a parallelotopic polarity π of $R\Gamma^S$. The graph $\mathrm{R}\Gamma^S$ shall be a graph of valency $s-1$ and

$$g(\mathrm{R}\Gamma^S) \geq g(\Gamma^S) \geq g(\Gamma).$$

Proposition 3.3.5. *The map π given by the close formula*

$$\mathrm{p}^\pi = [p_{0,1}, -p_{1,1}, p_{2,1}, p_{1,2}, -p'_{2,2}, -p_{2,2}, \dots, -p'_{i,i}, -p_{i,i}, p_{i+1,i}, p_{i,i+1}, \dots],$$
$$\mathrm{l}^\pi = (l_{1,0}, -l_{1,1}, l_{2,1}, l_{1,2}, -l'_{2,2}, -l_{2,2}, \dots, -l'_{i,i}, -l_{i,i}, l_{i+1,i}, l_{i,i+1}, \cdots)$$

is a parallelotopic polarity of $D(n, \mathbb{K})$. It preserves blocks of the equivalence relation τ. It is restriction on $V(\mathrm{CD}(n, \mathbb{K}))$ is a parallelotopic polarity of $\mathrm{CD}(n, \mathbb{K})$.

Let $L(n, \mathbb{K})$ be regular folding graph corresponding to the parallelotopic polarity π induced on the vertices of the graph $C(n, \mathbb{K})$. In case of $\mathrm{char}\mathbb{K} = 2$ the colours of absolute points of the polarity graph of $C(n, \mathbb{K})$ corresponding to the polarity π form the set $B = \{x | x^2 = 0\}$. Thus colours of the vertices of $B(n, \mathbb{K})$ are elements of $\mathbb{K} - B$.

Directly from the fact $g(D(n, \mathbb{F}_q)) \geq 2[(n+5)/2]$ from above we are getting

Proposition 3.3.6. (i) *The girth of the graph $L(n, \mathbb{F}_q) = L(n, q)$ and $B(n, \mathbb{F}_q) = B(n, q)$, q is even is, at least $2[(n+5)/2]$. They are regular graphs of degrees $q-1$ and q^t with q^t and $(q-1)q^{t-1}$ vertices, respectively.*

(ii) *For each q they form a families of graphs of large girth with the $\gamma = 2/3\log_{q-1}(q)$.*

(iii) *Let S be a subset of nonzero elements of $\mathbb{F}_q$, $|S| = s$ then $L(n, \mathbb{F}_q)^S$ and $B(n, \mathbb{F}_q)^S$ (q is even) are graphs of the order sq^{t-1}, girth is greater than or equal to $2[(n+5)/2]$ and degrees $s-1$ and s, respectively.*

3.4. On algebraic dynamical systems and irreversible walks on simple graphs

This section is devoted to studies of linguistic dynamical system of dimension $n \geq 2$ over arbitrary commutative ring $\mathbb{K}$, i.e. family $\mathfrak{F}$ of nonlinear polynomial maps $f_\alpha : \mathbb{K}^n \to \mathbb{K}^n$ *depending on "time"* $\alpha \in \mathbb{K} - \{0\}$ such that ${f_\alpha}^{-1} = f_{-\alpha}$ and $f_{\alpha_1}(x) = f_{\alpha_2}(x)$ for some $x \in \mathbb{K}^n$ implies $\alpha_1 = \alpha_2$, each map f_α has no invariant points.

The neighbourhood $\{f_\alpha(v)|\alpha \in \mathbb{K} - \{0\}\}$ of element v defines the graph Γ of a *dynamical system* $F_\Gamma(n, \mathbb{K})$ on the vertex set $\mathbb{K}^n$.

We refer to a string $\alpha_1, \alpha_2, \ldots, \alpha_r$ of elements from $\mathbb{K}$ such that

$$(\alpha_1 + \alpha_2)(\alpha_2 + \alpha_3)\ldots(\alpha_{r-1}\alpha_r) \neq 0$$

as *accepting string*. Let $AS_r = AS_r(\mathbb{K})$ be the totality of all accepting string of length r.

We refer to a subset M of $\mathbb{K}$ as *multiplicative set of ring* $\mathbb{K}$ if M is closed under multiplication ($x, y \in M$ implies $xy \in M$) and M does not contain zero. We will use term *M-regular string* for an accepting string $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that $\alpha_i + \alpha_{i+1}$, $i = 1, 2, \ldots, r-1$ are elements of multiplicative set M in commutative ring $\mathbb{K}$ The reader may keep in mind the following simple examples:

(1) Obvious example of multiplicative set is the multiplicative group $\mathbb{F}_q^*$ of finite field $\mathbb{F}_q$, where q is a prime power.

(2) Let us consider the ring $\mathbb{Z}_m$ corresponding to arithmetic modulo m, $\mathrm{a} \in \mathbb{Z}_m$ is some residue modulo m. The totality of elements $\mathrm{b} \in \mathbb{Z}_m$, which are mutually prime with a, form a multiplicative set Q_a of the ring.

(3) The Cartesian power $\mathbb{F}_2^m$ of the finite field $\mathbb{F}_2$ with two elements is a Boolean ring B_m containing all functions f from the finite set $M = \{1, 2, \ldots, m\}$ into $\mathbb{F}_2$. Recall, that

$$\begin{aligned}(x_1, x_2, \ldots, x_m) + (y_1, y_2, \ldots, y_m) &= (x_1 + y_1, x_2 + y_2, \ldots, x_m + y_m)\\ (x_1, x_2, \ldots, x_m) \cdot (y_1, y_2, \ldots, y_m) &= (x_1y_1, x_2y_2, \ldots, x_my_m).\end{aligned}$$

We can identify ring B_m with the totality of subsets of $\{1, 2, \ldots, m\}$ with operation of symmetric difference of subsets and intersection. The totality $Q_i = \{\mathrm{y} \in B_m | y_i = 1\}$ is an example of multiplicative subset in B_m.

(4) If $\mathbb{K}$ is a general commutative ring with unity, I is some ideal of $\mathbb{K}$, then the totality of all invertible elements modulo I is a multiplicative set. Symbol $\mathrm{Reg}(\mathbb{K})$ stands for the totality of regular elements of $\mathbb{K}$, i.e. nonzero divisors. Free module $\mathbb{K}^n$ is a Cartesian product of n copies of $\mathbb{K}$.

(5) Symbol $\mathrm{Reg}(\mathbb{K})$ stands for the totality of regular elements of $\mathbb{K}$, i. e. non zero divisors. Set $\mathrm{Reg}(\mathbb{K})$ is a multiplicative set for each commutative ring $\mathbb{K}$.

We shall refer to $\mathcal{F}$ as *symmetric linguistic dynamical system of rank d*, $d \geq 1$, denote also by $SF^d(n, \mathbb{K})$, if for each accepting string $\mathrm{a} = (\alpha_1, \ldots, \alpha_s)$, $s \leq d$ vertices v and $v_\mathrm{a} = f_{\alpha_1} \times \cdots \times f_{\alpha_s}(v)$ in the graph are connected by a unique path.

For each commutative ring $\mathbb{K}$ and even integer number $n \neq 0 \bmod 3$ there is family of symmetric linguistic dynamical systems $SF_L(\mathbb{K})$ of rank $d \geq 1/3n$. Let $L(n, \mathbb{K})$ be the graph of a dynamical system $SF_L(n, \mathbb{K})$. If $\mathbb{K} = \mathbb{F}_q$ graphs $L(n, \mathbb{F}_q)$ form a new family of graphs of large girth. The projective limit $L(\mathbb{K})$ of $L(n, \mathbb{K})$, $n \to \infty$ is well defined for each commutative ring $\mathbb{K}$, in case of integral domain $\mathbb{K}$ graph $L(\mathbb{K})$ is a forest, if $\mathbb{K}$ has zero divisors the girth of $\mathbb{K}$ is dropping to 4.

It is well known that a continuous bijection of the interval $[a, b]$ has a fixed point. In case of open variety $\mathbb{K}^n$, where $\mathbb{K}$ is commutative ring situation is different. For each pair $(\mathbb{K}, n)$, $n \geq 3$ and each $t \in \mathbb{K} - \{0\}$ we shall construct a *symmetric linguistic dynamical system*, $SF(n, \mathbb{K})$ i.e family $\mathfrak{F} = \mathfrak{F}_n(\mathbb{K})$ contains invertible nonlinear polynomial maps $f_t : \mathbb{K}^n \to \mathbb{K}^n$ without fixed points ($f_t(x) \neq x$ for each $x \in \mathbb{K}^n$), such that ${f_t}^{-1} = f_{-t}$ and $t_1 \neq t_2$ implies $f_{t_1}(x) \neq f_{t_2}(x)$ for each x. For each sting $\mathrm{a} = (a_1, a_2 \dots a_s)$ we consider the composition

$$F_{\mathrm{a},n} = f_{a_1,n} \circ f_{a_2,n} \circ \cdots \circ f_{a_s,n}$$

of transformations $f_{a_i,n}$, $i = 1, 2, \dots, s$.

The *level* of symmetric linguistic dynamical system $SF(n, \mathbb{K})$, denoted by $d = d(SF(n, \mathbb{K}))$, $d \geq 1$, is the maximal number s such that for each $\mathrm{a} \in AS_s(\mathbb{K})$ condition $F_{\mathrm{a},n}(x) = F_{\mathrm{b},n}(x)$, $\mathrm{b} \in (\mathbb{K} - \{0\})^s$ for some $x \in \mathbb{K}^n$ implies $\mathrm{a} = \mathrm{b}$.

The *rank* of symmetric linguistic dynamical system $SF(n, \mathbb{K})$, denoted by $r = \mathrm{rank}(SF(n, \mathbb{K}))$, $r \geq 1$, is the maximal number s, such that for each $\mathrm{a} \in AS_s(\mathbb{K})$ the condition $F_{\mathrm{a}}(x) = F_{\mathrm{b}}(x)$, $b \in (\mathbb{K} - \{0\})^l$, $l \leq s$ implies $\mathrm{a} = \mathrm{b}$.

Let us consider simple graph $\Gamma(n, \mathbb{K}) = \Gamma(F(n, \mathbb{K}))$ of the dynamical system $F(\mathbb{K})$ with the vertex set $V = \mathbb{K}^n$ such that $u \in V$ and $v \in V$ are connected by edge if and only $f_{t,n}(u) = v$ for some $t \in \mathbb{K}$.

The property $d(F) \geq s$ means that for each vertex x and "regular" string $\mathrm{a} = (\mathrm{a}_1, \dots, \mathrm{a}_s)$, $s \leq d$ as above x and $F_{\mathrm{a},n}(x) = f_{a_1,n} \circ \dots \circ f_{a_s,n}(x)$ are not included together in a cycle of even length $\leq 2d$ in the graph $\Gamma(F(n, \mathbb{K}))$.

The property $\mathrm{rank}(F(n, \mathbb{K})) \geq s$ means that for each vertex x and $\mathrm{a} \in AS_s(\mathbb{K})$ vertices x and $F_{\mathrm{a},n}(x)$ are connected by the unique path of length $\leq s$ in graph $\Gamma(n, \mathbb{K})$.

We consider the definition of *symmetric arithmetical dynamical system* $SAF(Q, \mathbb{K}) = \{f_\alpha | \alpha \in Q\}$ simply via consideration of quasi projective manyfold M of $\mathbb{K}^n$ instead of $\mathbb{K}^n$ and requirement $f_{\alpha,n} \in SAF(Q, \mathbb{K})$ instead of ${f_{\alpha,n}}^{-1} = f_{-\alpha,n}$,where Q is just a subset of $\mathbb{K}$. Major justification of *arithmetical graphs* related to such dynamical systems is that they are examples of graphs with memory (see [164]) because we can not only consider such a graph as finite automaton where states v and $f_{\alpha,n}(v)$ are connected by the

arrow with the label α, but each state v is a string of characters from the alphabet $\mathbb{K}$.

We consider explicit construction of symmetric arithmetic dynamical systems $SF_D(n,\mathbb{K})$ and $SF_C(n,\mathbb{K})$ on $\mathbb{K}^n \cup \mathbb{K}^n$ related to permutational representations of infinite group $U_D(\mathbb{K})$ and $U_C(\mathbb{K})$ defined over arbitrary commutative ring, if $\mathbb{K}$ is an integral domain than $U_C(\mathbb{K})$ is a free product $\mathbb{K}^+ * \mathbb{K}^+$, where $\mathbb{K}^+$ is an additive group of the ring, well defined projective limit of graphs $\Gamma(SF_C(n\mathbb{K}))$ is an infinite tree. If $\mathbb{K}$ has zero divisors, then the girth of each graph $\Gamma(SF_C(n,\mathbb{K}))$ and their projective limit is dropping to 4 (see section 4).

The following statement is the generalisation of statement in [164].

Theorem 3.4.1. *Let $N_{D,x,n}(\mathrm{v})$ be the operator of taking the neighbour of the vertex $\mathrm{v} = (v_1, v_2, \ldots, v_s)$ of the colour $v_1 + x$ in the graph $D(n,\mathbb{K})$.*

Then operator it defines symmetric arithmetical dynamic system $SAF_D(n,\mathbb{K})$ on $\mathbb{K}^n \cup \mathbb{K}^n$ of level $d = [(n+5)/2] - 1$.

Proof. Let us consider the action of operator

$$F_d = F_{D,t_1,\ldots,t_d,n} = N_{D,t_1,n} N_{D,t_2,n} \ldots N_{D,t_d,n},$$

where $t_1, t_2, \ldots, t_d$ is accepting string, on the vertex u.

Consecutive applications of $N_{D,t_i,n}$ produce the walk

$$\mathrm{u}_0 = \mathrm{u}, \mathrm{u}_1 = N_{D,t_1,n}(u_0), \ldots, \mathrm{u}_d = N_{D,t_d,n}(\mathrm{u}_{\mathrm{d}-1}),$$

where the difference of colours for elements u_i and u_{i+2} is $t_i + t_{i+1}$. The group $U_D(n,\mathbb{K})$ acts transitively on the vertex set of $D(n,\mathbb{K})$ and preserves difference of colours for elements of same type. Thus without loss of generality we may assume that u is zero point.

We can apply map ϕ_n (or ${\phi'}_n$) to u_d and compute the common for u_d and its image component α via two numbers lemma. It is product of M-regular elements and one nonzero element. Thus it differs from zero. Let us assume that

$$F'_s(\mathrm{u}) = F_{D,t'_1,\ldots,t'_s,n}(\mathrm{u}) = N_{D,t'_1,n} \ldots N_{D,t'_s,n}(\mathrm{u}) = F_d(\mathrm{u}).$$

Without loss of generality we may assume that $t'_i \neq t'_{i+1}$, $i = 1, \ldots,$ s-1. If $s \leq d$, the component with number α for $F'(\mathrm{u}) = 0$ according to the 2 numbers lemma and we are getting a contradiction. So $s = d$ and consecutive execution of transformation $N_{D,t'_i,n}, (i = 1, \ldots, d)$ produces the walk $\mathrm{u}'_1, \ldots \mathrm{u}'_d$. Let $t_1 \neq t'_1$. Then we can apply operator $t_{0,1}(-t')$ to each element u_i, u'_i, $i = 1, \ldots, d$ and get elements v_i, v'_i, $i = 1, \ldots, d$, respectively. Conditions $\mathrm{u}_d = \mathrm{u}'_d$ and $\mathrm{v}_d = \mathrm{v}'_d$ are equivalent.

According to two numbers lemma component α of v'_d equals zero but same component of v_d is not a product of regular and nonzero elements.

Thus $t_1 = t'_1$. Application of same argument to the sequence $\mathrm{u}_i, \dots \mathrm{u}_d$, $i = 1, \dots, d-1$ gives us $t_i = t'_i$ for $i = 2, \dots d$.

□

Operator $N_{D,x,n}$ preserves connected components of $D(n, \mathbb{K})$ and blocks of equivalence relation τ.

Corollary 3.4.2. *Let $N_{C,x,t}(v)$, $t \in \mathbb{K}$ be the operator of taking the neighbour of the vertex* v *of the colour $v_1 + x$ in the graph $C(t, \mathbb{K})$, which is the restriction of operator $N_{C,x,t}(v)$ on the equivalence class C. Then it defines symmetric arithmetical dynamic system $SF_C(t, \mathbb{K})$ on $\mathbb{K}^t \cup \mathbb{K}^t$ over $Q = \mathbb{K}$ of rank $d = [2/3t] + 1$.*

Theorem 3.4.3. (i) *Let $N_{\mathrm{R}C,x,t}(v)$, $x \in \mathbb{K} - \{0\}$ be the operator of taking the neighbour of the vertex $v \in V(\mathrm{R}C(t, \mathbb{K})) = \mathbb{K}^t$, of colour $v_{1,0} + x$, then it defines the linguistic dynamical system $F_{\mathrm{R}C}(t, \mathbb{K})$ on $\mathbb{K}^t$, $t \geq 2$ of level $d = [2/3t] + 1$ and rank $r \geq [1/3t]$*

(ii) *Let* char$\mathbb{K} = 2$, *B is the set of roots for the equation $x^2 = 0$, $N_{\mathrm{I}C,x,t}(v)$, $x + \rho(v) \neq y$, $y \in B$ be the operator of taking the neighbour of $v \in V(\mathrm{I}C(t, \mathbb{K})) = (\mathbb{K} - B) \times \mathbb{K}^{t-1}$ of the colour $v_{1,0} + x$, then it defines an arithmetical dynamic system $AF_{\mathrm{I}C}(t, \mathbb{K})$ of level $d = [2/3t] + 1$ and rank $r = [1/3t] + 1$.*

Proof. Let $F_\Gamma(\mathbb{K})$ be one of the systems $F_{\mathrm{R}C}(t, \mathbb{K})$, $AF_{\mathrm{I}C}(t, \mathbb{K})$. Let us consider the action of operator $F_d = N_{t_1} N_{t_2} \dots N_{t_d}$, where $t_i + t_{i+2}$ are elements of multiplicative subset M of ring $\mathbb{K}$, on the vertex u.

Consecutive applications of $N_{\Gamma,t_i,t}$ produce the walk

$\mathrm{u} = \mathrm{u}_0, \mathrm{u}_1 = N_{\Gamma,t_1,t}(\mathrm{u}_0), \dots, \mathrm{u}_d = N_{\Gamma,t_d,t}(\mathrm{u}_{d-1})$, where the difference of colours for elements u_i and u_{i+2} is $t_i + t_{i+1}$. Let us consider the -dynamic equation- $F'_s(\mathrm{u}) = F_d(\mathrm{u})$, where

$F_s(\mathrm{u}) = N_{\Gamma,t'_1,t} \dots N_{\Gamma,t'_s,t}(\mathrm{u}) = F_d(\mathrm{u})$. Without loss of generality we may assume that $t'_i \neq t'_{i+1}$, $i = 1, \dots, s-1$.

Consecutive execution of transformation $N_{\Gamma,t'_i,t}$, $i = 1, \dots, s$ produces the walk $\mathrm{u}'_1, \dots, \mathrm{u}'_s$.

So, we are getting -the dynamical trail-: $u_0, \dots u_d, u'_{s-1}, \dots, u'_1$, where u'_1 is adjacent to u_0. We can consider elements of the trail as points in $D(n, \mathbb{K})$. Then $u_0, \pi(u_1), u_2, \pi(u_3), \dots$ is a dynamical trail in $D(n, \mathbb{K})$ corresponding to the same dynamical equation. But the only trail in $D(n, \mathbb{K})$ can be related to the sequence of colours x, $x + t_1$, $x + t_1 + t_2$, $\dots$, $x + t_1 + \dots + t_d$, $x + t_1 + \dots t_{d-1}, \dots$, $x + t_1$, x where x is the colour of u. Thus $s = d$, tuple $(t_1, \dots, t_d)^* = (t'_1, \dots t'_d)$ and $G(\mathbb{K})$ is an invertible dynamical system of level d.

Let us investigate possible odd cycles in the graph. If $N_{\Gamma,t_s,t} \dots N_{\Gamma,t_1,t}(x) = x$ and $p_l = N_{\Gamma,t_{l-1},t}$, $l = 2, \dots, 2k{+}1$. Then $p_1, (p_2)^\pi, \dots, p_{2k+1}, (p_1)^\pi \dots (p_{2k+1})^\pi$

are consecutive verices of a $(4k+2)$-cycle in the bipartite graph. Half of this cycle has colours from the regular string.

□

3.5. Stable cubical polynomial maps corresponding to dynamiacal systems $B_D(n, \mathbb{K})$

We are going to evaluate degrees of transformations

$$F_{D,\alpha_{1,\alpha_2,\ldots,\alpha_k},n} = N_{D,\alpha_1,n} N_{D,\alpha_2,n} \ldots N_{D,\alpha_k,n}$$

from bipartite dynamical systems $BF_D(n, \mathbb{K})$ given by graphs $D(n, \mathbb{K})$ (see [175], [176]), where $\alpha_i \in \mathbb{K}$, $i = 1, 2, \ldots, k$. We will assume that the point set $\mathbb{K}^n$ is the domain of our map. The codomain will be the set of points in the case of even k, and the set of lines for odd parameter k.

The following computations the reader can find in [184] and [120]

3.5.1. Transformation $F_{D,\alpha_1,n}$

Our research we start with studying transformation $F_{D,\alpha_1,n} = N_{D,\alpha_1,n}$. Hence we have:

$$\begin{aligned}
&l_{1,0} = p_{0,1} + \alpha_1 \qquad \deg l_1 = 1\\
&l_{1,1} = p_{1,1} + l_{1,0}p_{0,1} = p_{1,1} + \alpha_1 p_{0,1} + p_{0,1}^2\\
&l_{1,2} = p_{1,2} + p_{0,1}l_{1,1} = p_{1,2} + p_{0,1}p_{1,1} + \alpha_1 p_{0,1}^2 + p_1^3\\
&l_{i,i} = p_{i,i} + l_{1,0}p_{i-1,i} = p_{i,i} + \alpha_1 p_{i-1,i} + p_{0,1}p_{i-1,i}\\
&l_{i,i+1} = p_{i,i+1} + p_{0,1}l_{i,i} = p_{i,i+1} + \alpha_1 p_{0,1}p_{i-1,i} + p_{0,1}p_{i,i} + p_{0,1}^2 p_{i-1,i}.
\end{aligned}$$

Similarly we are receiving:

$$\begin{aligned}
&l_{i+1,i} = p_{i+1,i} + l_{1,0}p'_{i,i} = p_{i+1,i} + \alpha_1 p'_{i,i} + p_{0,1}p'_{i,i}\\
&l'_{i,i} = p'_{i,i} + p_{0,1}l_{i,i-1} = p'_{i,i} + \alpha_1 p_{0,1}p'_{i-1,i-1} + p_{0,1}p_{i,i-1} + p_{0,1}^2 p_{i-1,i-1}.
\end{aligned}$$

So if we take the plane data (p) as $(p_1, p_2, \ldots, p_n)$ after this transformation we get the line vertex $f_1(p_1), f_2(p_1, p_2), \ldots, f_n(p_1, p_2, \ldots, p_n)$,

$$\deg f_n(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1,\\ 2, & n = 2,\\ 2, & n = 4k, 4k+1,\\ 3, & n = 4k+2, 4k-1 \quad \text{where} \quad k = 1, 2, 3 \ldots \end{cases}$$

3.5.2. Transformation $F_{D,\alpha_1,\alpha_2,n}$

Using the previous part of the calculation (transformation $F_{D,\alpha_1,n}$) we can calculate the composition with transformation $N_{D,\alpha_2,n}$.

$$p_{0,1}^{(2)} = p_{0,1} + \alpha_1 + \alpha_2$$
$$p_{1,1} = l_{1,1} - l_{1,0}p_{0,1}^{(2)} = -(\alpha_1 + \alpha_2)(\alpha_1 + p_{0,1})$$
$$p_{1,2}^{(2)} = l_{1,2} - p_{0,1}^{(2)}l_{1,1} = p_{1,2} - (\alpha_1 + \alpha_2)p_{1,1} - \alpha_1(\alpha_1 + \alpha_2)p_{0,1} - (\alpha_1 + \alpha_2)p_{0,1}^2$$
$$p_{i,i+1}^{(2)} = l_{i,i+1} - p_{0,1}^{(2)}l_{i,i} = p_{i,i+1} - (\alpha_1 + \alpha_2)(p_{i,i} + \alpha_1 p_{i-1,i} + p_{0,1}p_{i-1,i})$$
$$p_{i,i}^{(2)} = l_{i,i} - l_{1,0}p_{i-1,i}^{(2)} = p_{i,i} + (\alpha_1 + p_{0,1})(\alpha_1 + \alpha_2)(p_{i-1,i-1} + \alpha_1 p_{i-2,i-1} + p_{0,1}p_{i-2,i-1})$$

Similarly we are receiving:

$$p_{i,i}^{\prime(2)} = l_{i,i}^{\prime} - p_1^{(2)}l_{i,i-1} = p_{i,i}^{'} - (\alpha_1 + \alpha_2)(p_{i,i-1} + \alpha_1 p_{i-1,i-1} + p_1 p_{i-1,i-1}^{\prime})$$
$$p_{i+1,i}^{(2)} = l_{i+1,i} - l_{1,0}p_{i,i}^{\prime(2)} = p_{i+1,i} + (\alpha_1 + p_1)(\alpha_1 + \alpha_2)(p_{i-1,i-1} + \alpha_1 p_{i-1,i-1}^{\prime} + p_1 p_{i-1,i-1}^{\prime})$$

Hence we got vertex point from codomain in the form

$$(p) = (g_1(p_1), g_2(p_1, p_2), \ldots, g_n(p_1, p_2, \ldots, p_n))$$

and degrees of each component are following:

$$\deg g_n(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 1, & n = 2, \\ 2, & n = 4k-1, 4k+2, \\ 3, & n = 4k, 4k+1 \quad \text{where} \quad k = 1, 2, 3 \ldots \end{cases}$$

3.5.3. Transformation $F_{D,\alpha_1,\alpha_2,\ldots,\alpha_m,n}$

Degrees of elements of vertex point and vertex line after transformation

$$F_{D,\alpha_1,\alpha_2,\ldots,\alpha_{m-1},n} = N_{D,\alpha_1,n}N_{D,\alpha_2,n}\ldots N_{D,\alpha_{m-1},n}$$

and

$$F_{D,\alpha_1,\alpha_2,\ldots,\alpha_m,n} = N_{D,\alpha_1,n}N_{D,\alpha_2,n}\ldots N_{D,\alpha_m,n},$$

respectively, we will calculate using induction, imposing m-even.

Assume transformation $F_{D,\alpha_1,\alpha_2,\ldots,\alpha_{m-3},n} = N_{\alpha_1}N_{\alpha_2}\ldots N_{\alpha_{m-3},n}$ gave us vertex point:

$$(p)^{(m-3)} = (g_1^{(m-3)}(p_1), g_2^{(m-3)}(p_1, p_2), \ldots, g_n^{(m-3)}(p_1, p_2, \ldots, p_n))$$

with degree

$$\deg g_n^{(m-3)}(p_1,p_2,\ldots,p_n)=\begin{cases}1, & n=1,\\ 1, & n=2,\\ 2, & n=4k-1,4k+2,\\ 3, & n=4k,4k+1 \quad \text{where} \quad k=1,2,3,\ldots\end{cases}$$

and vertex line after transformation $F_{D,\alpha_1,\alpha_2,\ldots,\alpha_{m-2},n}$:

$$[l]^{(m-2)}=(f_1^{(m-2)}(p_1),f_2^{(m-2)}(p_1,p_2),\ldots,f_n^{(m-2)}(p_1,p_2,\ldots,p_n))$$

with degree

$$\deg f_n^{(m-2)}(p_1,p_2,\ldots,p_n)=\begin{cases}1, & n=1,\\ 2, & n=2,\\ 2, & n=4k,4k+1,\\ 3, & n=4k+2,4k-1 \quad \text{where} \quad k=1,2,3,\ldots\end{cases}$$

Now we have to check the degree of polynomial $g_n^{(m-1)}$.

$$\begin{aligned}p_1^{(m-1)} &= p_1+\alpha_1+\alpha_2+\ldots+\alpha_{m-3}+\alpha_{m-2}+\alpha_{m-1}\\ &= p_1^{(m-3)}+\alpha_{m-2}+\alpha_{m-1}\\ p_{i,i+1}^{(m-1)} &= l_{i,i+1}^{(m-2)}-p_1^{(m-1)}l_{i,i}^{(m-2)}\\ &= p_{i,i+1}^{(m-3)}+p_1^{(m-3)}l_{i,i}^{(m-2)}-p_1^{(m-3)}l_{i,i}^{(m-2)}-(\alpha_{m-2}+\alpha_{m-1})l_{i,i}^{(m-2)}\\ &= p_{i,i+1}^{(m-3)}-(\alpha_{m-2}+\alpha_{m-1})l_{i,i}^{(m-2)}.\end{aligned}$$

Since $p_{i,i+1}^{(m-3)}$ is independent from α_{m-2} and α_{m-1} and both $p_{i,i+1}^{(m-3)}$ and $l_{i,i}^{(m-2)}$ have degree equal 2, we get that $p_{i,i+1}^{(m-1)}$ has degree 2.

By similar reasoning we obtain that $p_{i,i}^{(m-1)}$ has degree 3, $p_{i,i}^{\prime(m-1)}$ degree 2, $p_{i+1,i}^{(m-1)}$ degree 3.

Hence by means of transformation $F_{D,\alpha_1,\alpha_2,\ldots,\alpha_{m-1},n}$ we encoded plain text $(p_1,p_2,\ldots,p_n)$ on ciphertext

$$(p)^{(m-1)}=(g_1^{(m-1)}(p_1),g_2^{(m-1)}(p_1,p_2),\ldots,g_n^{(m-1)}(p_1,p_2,\ldots,p_n))$$

with degree

$$\deg g_n^{(m-1)}(p_1,p_2,\ldots,p_n)=\begin{cases}1, & n=1,\\ 1, & n=2,\\ 2, & n=4k-1,4k+2,\\ 3, & n=4k,4k+1 \quad \text{where} \quad k=1,2,3,\ldots\end{cases}$$

In the same way using second part of inductive assumption we get the ciphertext

$$[l]^{(m)} = (f_1^{(m)}(p_1), f_2^{(m)}(p_1, p_2), \ldots, f_n^{(m)}(p_1, p_2, \ldots, p_n))$$

after transformation $F_{D,\alpha_1,\alpha_2,\ldots,\alpha_m,n}$ with

$$\deg f_n^{(m)}(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 2, & n = 2, \\ 2, & n = 4k, 4k+1, \\ 3, & n = 4k+2, 4k-1 \quad \text{where} \quad k = 1, 2, 3, \ldots \end{cases}$$

We refer to the string $\alpha_1, \alpha_2, \ldots, \alpha_m$ as *antinilpotent sequence* if each power of the product of $\alpha_1 + \alpha_2$, $\alpha_2 + \alpha_2$, $\ldots$, $\alpha_{m-1} + \alpha_m$ and $\alpha_1 + \alpha_m$ is different from zero.

It is easy to see that antinilpotent sequence is an accepting string.

Theorem 3.5.1. *Let $G_D(n, \mathbb{K})$ be the group of cubical transformations of free module $\mathbb{K}^n \cup \mathbb{K}^n$ over finite commutative ring, generated by $F_{D,t,n} = N_{D,t,n}$, $t \in \mathbb{K}$ and $G_D(\mathbb{K})$ is the projective limit of $G_D(n, \mathbb{K})$, $n \to \infty$.*

Each element $F_{D,\alpha_1,\ldots,\alpha_m,n} = N_{D,\alpha_1,n} N_{D,\alpha_2,n} \ldots N_{D,\alpha_m,n} \in G_D(n, \mathbb{K})$, where $\alpha_1, \alpha_2, \ldots, \alpha_m$ is accepting string of length $m < n + 5$, has no fixed points over $\mathbb{K}$. If $\alpha_1, \alpha_2, \ldots, \alpha_m$ is antinilpotent sequence then the order of

$$F_{D,\alpha_1,\ldots,\alpha_m} = N_{D,\alpha_1} N_{D,\alpha_2} \ldots N_{D,\alpha_m} \in G_D(\mathbb{K})$$

is infinity.

Corollary 3.5.2. *The order of transformation $N_{D,\mathrm{t},n} \in G_D(n, \mathbb{K})$, where $\mathrm{t} = (t_1, t_2, \ldots, t_m)$ is antinilpotent string is growing to infinity with the growth of n.*

Remark 3.5.3. The commutator $CG_D(n, \mathbb{K})$ generated by $F_{D,t_1,t_2,n}$, $t_1, t_2 \in \mathbb{K}$ acts faithfully on the set of points P (or set of lines L).

3.6. On symmetric bipartite dynamical systems of large cycle indicator corresponding to graphs $A(n, \mathbb{K})$

We will define graph $A(n, \mathbb{K})$ with the vertex set $\mathbb{K}^n \cup \mathbb{K}^n$, where $\mathbb{K}$ is general commutative ring.

Let $\mathbb{K}$ be a arbitrary commutative ring. We define a infinte bipartite graph $A(\mathbb{K})$ (*alternating graph*) with the set of points $P = \mathbb{K}^{\mathbb{N}}$ and set of

lines $L = \mathbb{K}^{\mathbb{N}}$ are two copies of infinite dimensional free module via incidence relation I. Let us denote point (p) from P by

$$(x) = (x_1, x_2, \dots, x_i, x_{i+1}, \dots)$$

and line $[y]$ form L by

$$[y] = [y_1, y_2, \dots, y_i, y_{i+1}, \dots].$$

We say that point (x) is incident with the line $[y]$ if and only if the following conditions are satisfied

$$y_i - x_i = y_1 x_{i-1}$$
$$y_{i+1} - x_{i+1} = x_1 y_i,$$

where $i = 2, 3, \dots$. Brackets and parenthesis will allow us to distinguish points and lines again.

This incidence structure (P, L, I) we denote as $A(\mathbb{K})$. We identify it with the bipartite *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and the edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

For each positive integer $n \geq 2$ we obtain an incidence structure (P_n, L_n, I_n) as follows. First, P_n and L_n are obtained from P and L respectively by simply projecting each vector onto its n initial coordinates with respect to the above order. The incidence I_n is then defined by imposing the first $n-1$ incidence equations and ignoring all others. The incidence graph corresponding to the structure (P_n, L_n, I_n) is denoted by $A(n, \mathbb{K})$.

Natural canonical homomorphism of $A(n, \mathbb{K})$ onto $A(n-1, \mathbb{K})$ given by procedure to delete last coordinate of the vertex (point or line) allow us to consider well define projective limit $A(\mathbb{K})$ of $A(n, \mathbb{K})$ $n \to \infty$. It is very interesting that $A(n, \mathbb{K})$, which is not an edge transitive incidence structure which aproximaates infinite graphs $A(\mathbb{K}) = \lim_{n\to\infty} A(n, \mathbb{K})$ with edge-transitive automorphism group.

Similarly to the case of $D(n, \mathbb{K})$ we assume that the colour of the vertex v is the first coordinates of this vector (point or line). So colours are elements of $\mathbb{K}$. Each vertex v of graph $A(n, \mathbb{K})$ has unique neighbour of given colour. Let $N_{A,t,n}$ be the map on the vertex set of graph $A(n, \mathbb{K})$, which transform point $x = (x_1, x_2, \dots, x_n)$ to its neighbour of colour $x_1 + t$, $t \in \mathbb{K}$ and transform line $y = [y_1, y_2, \dots, y_n]$ into its neighbour of colour $y_1 + t$.

We define in this chapter the incidence structure $\mathrm{E}(\mathbb{K})$ with point set P' and line set L'. It will be convenient for us to denote vectors from P' as

$$\mathrm{x} = (x) = (x_{0,1}, x_{1,1}, x_{1,2}, x_{2,2}, \dots x_{i,i}, x_{i,i+1} \dots,)$$

and vectors from L' as

$$\mathrm{y} = [y_{1,0}, y_{1,1}, y_{1,2}, y_{2,2}, \dots, y_{i,i}, y_{i,i+1}, \dots].$$

We say that point (x) is incident with the line $[y]$ and we write it xJy or (x)J$[y]$ if and only if the following condition are satisfied:

$$y_{i,i} - x_{ii} = x_{i-1,i}y_{1,0},$$
$$y_{i,i+1} - x_{i,i+1} = x_{0,1}y_{i,i}$$

where $i = 1, 2, \ldots$.

The simplification of notations by the following change of indices:

$$\begin{array}{llll} x_{0,1} = x_1, & x_{1,1} = x_2, & y_{1,0} = y_1, & y_{1,1} = y_2, \\ x_{1,2} = x_3, & x_{2,2} = x_4, & y_{1,2} = y_3, & y_{2,2} = y_4, \\ \ldots & \ldots & \ldots & \ldots \\ x_{i,i} = x_{i+1}, & x_{i,i+1} = x_{i+2} & y_{i,i} = y_{i+1}, & y_{i,i+1} = y_{i+2} \\ \ldots & \ldots & \ldots & \ldots \end{array}$$

allows us to establish isomorphism of E$(\mathbb{K})$ and A$(\mathbb{K})$.

It means that linear operator η of deleting coordinates with indices of kind $(i+1, i)$ and $(i, i)'$ for points and lines $D(\mathbb{K})$ defines the homomorphism of this incidence structure onto $A(\mathbb{K})$. Notice that for the computations of coordinates (i, i), $(i, i+1)$ of vector $N_{D,t}(x)$ or $N_{D,t}(y)$ we need only coordinate x and y with indices $(1, 0), (0, 1)$, (i, i) and $(i, i+1)$. So, we prove the following proposition.

Proposition 3.6.1. *Let $F_{A,t_1,\ldots,t_m,n}$ be the composition of maps $N_{A,t_1,n}$, $N_{A,t_2,n}$, $\ldots$, $N_{A,t_m,n}$. Then cubical map $F_{A,t_1,\ldots,t_m,n}$ can be computed as a composition of linear projection η of cubical map $F_{A,t_1,t_2,\ldots,t_m}$.*

As we mention before the polynomial equations $y_i = f_i(x_1, x_2, \ldots, x_n)$, which are made public, have the degree 3. Notice, that we computed degrees of components of $F_{A,t_1,t_2,\ldots,t_m,n}$ in previous unit of the section.

Now we define as special class of linguistic bipartite dynamical system on the variety $\mathbb{K}^n \cup \mathbb{K}^n$ dimension $n \geq 2$ over arbitrary commutative ring $\mathbb{K}$.

Theorem 3.6.2. *Let $N_{A,t,n}$ be the operator of taking the neighbour in the graph $A(n, \mathbb{K})$, where $\mathbb{K}$ is a commutative ring. For each accepting string $\mathrm{t} = (t_1, t_2, \ldots, t_s)$, $s \leq n$ there exists a vertex v of the graph such that v and $F_{A,t_1,t_2,\ldots,t_s,n}(v)$ are connected by unique path in the graph $A(n, \mathbb{K})$.*

Corollary 3.6.3. *Polynomial maps of kind $N_{A,\mathrm{t},n}$ and $N_{A,\mathrm{t}',n}$ corresponding to different strings accepting strings of length $\leq n$ are different.*

Polynomial maps $N_{A,t,n}$, $n = 2, 3, \ldots$ form a family of symmetric bipartite dynamical systems $SB_A(n, \mathbb{K})$ with large cycle indicator defined in [175], [176]

Theorem 3.6.4. *Let $G_A(n,\mathbb{K})$ be the group of cubical transformations of $\mathbb{K}^n \cup \mathbb{K}^n$ over finite commutative ring, generated by $N_{A,t,n}$, $t \in \mathbb{K}$ and $G_A(\mathbb{K})$ is a projective limit of $G_A(n,\mathbb{K})$, $n \to \infty$.*

Then order of transformation $F_{A,\mathrm{t}} \in G_A(\mathbb{K})$, where $\mathrm{t} = (t_1, t_2, \ldots, t_m)$, where is an antinilpotent string, is infinity.

Corollary 3.6.5. *The order of transformation $F_{A,\mathrm{t},n} \in G_A(n,\mathbb{K})$, where $\mathrm{t} = (t_1, t_2, \ldots, t_m)$ is antinilpotent string is growing to infinity with the growth of n.*

Remark 3.6.6. The commutator $CG_A(n,\mathbb{K})$ generated by

$$F_{A,t_1,t_2,n} = N_{A,t_1,n} \circ N_{A,t_2,n}, \quad t_1, t_2 \in \mathbb{K}$$

acts faithfully on the set of points P_n (or set of lines L_n).

Chapter 4

On some LDPC codes corresponding to algebraic graphs

4.1. LDPC codes and Schubert incidence structure

Families of simple graphs of high girth had been used for the development of algorithms in Cryptography and Turbocoding. Recent results in that directions show the interest of applied researchers to "families of directed graphs of high girth" as possible source of applied ideas, In this chapter we discussed some explicit construction of simple and directed graphs which can be applicable to Theory of LDPC codes Turbocoding.

Various applications of graph theory to Coding Theory are hard to observe. We just mention that the code is just subset in finite metric space defined via distance regular graph (see [8], [29] , [2]) and expanding graphs (superconcentrators, magnifyers) had been used for the design of important codes (see [57], [87]).

Similar situation is in Cryptography: each computation can be defined in terms of finite automaton, roughly directed graph with labels on arrows, various applications of automata theory to cryptography are very hrd to observe. We just mention [38](see also further references in this survey).

In this chapter we briefly observe some traditional applications of families of simple graphs of large girth to construction of LDPC and Turbo Codes (see [115], last chapter of[64], [137], [138], , [107], [51], [50]).

Low-density parity-check (LDPC) codes were originally introduced in his doctoral thesis by Gallager in 1961 [45]. Since the discovery of Turbo codes in 1993 by Berrou, Glavieux, and Thitimajshima [5], and the rediscovery of LDPC codes by Mackay and Neal in 1995 [90], there has been renewed interest in Turbo codes and LDPC codes, because their error rate performance approaches asymptotically the Shannon limit. Much research is devoted to characterizing the performance of LDPC codes and designing codes that have good performance. Commonly, a graph, the Tanner graph (see [61] and further references), is associated with the code and an important parameter affecting the performance of the code is the girth of its Tanner graph. In [93], [50], [51] authors consider the design of structured regular LDPC codes based on Tanner graphs of large girth. The regularity and structure of LDPC codes utilize memory more efficiently and simplify the implementation of LDPC coders. The Tanner graph is a special type of graph, a bipartite graph, where the nodes divide into two disjoint classes with edges only between nodes in the two different classes.

Large girth speeds the convergence of iterative decoding and improves the performance of LDPC codes, at least in the high SNR range, by slowing down the onsetting of the error floor. Large size of such graphs implies fast convergence.

On the web page of Professor Moura (see also [101]) one can find the following text: "Commonly, a graph, the Tanner graph, is associated with

the code and an important parameter affecting the performance of the code is the girth of its Tanner graph. In our work, we consider the design of structured regular LDPC codes whose Tanner graphs have large girth. The regularity and structure of LDPC codes utilize memory more efficiently and simplify the implementation of LDPC coders. The Tanner graph is a special type of graph, a bipartite graph, where the nodes divide into two disjoint classes with edges only between nodes in the two different classes. The problem we have been considering is a generic problem in graph theory, namely, that of designing bipartite graphs with large girth. We actually have studied a more special class of this generic problem, in particular, the design of undirected regular bipartite graphs with large girth".

So here we can see clearly two ideas:

(i) new families of bipartite simple graphs of large girth can be used as families of Tanner's graphs

(ii) for the constructions of LDPC codes and turbo codes we can use directed graphs which are analogs of bipartite graphs of large girth.

4.2. Explicit constructions of Tanner graphs

The induced biregular bipartite subraphs of graphs $D(n, q)$ of order $2q^n$, degree q and girth $\geq n + 4$ or their connected components $CD(d, q)$ had been used by Guinnand and Lodge for the construction of turbocodes. The description of the class of biregular subgraphs of the above graphas the reader can find in previous chapter. The parameters of related codes are very close to the Shannon bound.

We notice that the family of graphs $D(n, q)$ depending on two parameters n and $q = p^m$, where p is prime, is not the unique known family of graphs of unbounded degree and arbitrarily large girth. For "sufficiently large p" the exact girth is computed in [129].

Recall, that the first explicit examples of families of simple graphs with large girth of arbitrary large degree were given by Margulis. The constructions were Cayley graphs $X(p, q)$ of group $SL_2(\mathbb{Z}_q)$ with respect to special sets of $q+1$ generators, p and q are primes congruent to 1 mod 4. The family of $X(p, q)$ is not a family of algebraic graphs because the neighborhood of each vertex is not an algebraic variety over F_q. For each p, graphs $X(p, q)$, where q is running via appropriate primes, form a family of small world graph of unbounded diameter (see Chapter 2).

Of course Cayley graph corresponding to finite group G and symmetrical set of generators S ($s \in S$ leads to $s^{-1} \in S$) is not a bipartite graph. But we can take it bipartite analog - the graph of incidence structure $I = I(G, S)$ for which the point set P and line set L are two distinct copies of G and

$p \in P$ is incident to $l \in L$ if and only if $ps = l$ in group G for some generator $s \in S$.

Let R be arbitrary subset of S containing at least 3 elements, G_R be the group generated by $R \cup R^{-1}$ and $G_R < H < G$.

We can consider the bipartite graph $I' = I(H, R)$ with the partition sets $P' = P \cap H$ and $L' = L \cap H$ such that $p \in P'$ and $l \in L'$ are incident ($pI'l$ or $lI'p$) if and only if $ps = l$ for some $s \in R$. Notice, that last condition is equivalent to $ls = p$ for some $s \in R^{-1}$.

We set the Cayley graph corresponding to G, S is $X^{p,q}$. then $g(I(H, R))$ is larger than the girth of $X(p, q)$. So $I(H, R)$ can be used as Tanner graph.

4.3. On the comparrison of some LDPC codes

Recent results show that very good codes can be obtained from families of simple, bipartitee graphs of high girth. There is only a few known infinite families suitable for this purpose: Ramanujan expander graps, generalised polygons, construction based on finite geometries (graphs $D(n, \mathbb{K})$, $\widetilde{D}(n, \mathbb{K})$ and $A(n, \mathbb{K})$). Graphs $D(n, q)$ and them compact parts $CD(n, q)$ were use to create LDPC by Guinand and Lodge [50], [51]. This codes are use by NASA and have very good error correcting properties. Families based on similar algebraic constructions $\widetilde{D}(n, \mathbb{K})$ and $A(n, \mathbb{K})$ give codes witch even beter properties which was show in [117]. Codes obtained using affine generalized polygons allow you to get the codes with good properties [116]. Other algebraic constructiong based on graphs: Margulis and Ramanujan-Margulius give interesting codes but in 2003 D. MacKay and M. Postol shown the weaknesses of this two constructions in [91]. They reported that the Margulis construction gives code with near-codewords, which cause problems for the sum-pruduct decoder. The Ramanujan-Margulis construction gives a code with low-weight codeword which contributes to the effect of error-floor. Since 1997, when $D(n, q)$ and $CD(n, q)$ was first use to construct LDPC there has been no information about the weaknesses of codes based on such construction. For this reason, the codes with similar designs are good.

4.4. On basics of LDPC codes theory

Information is always transmitted through the communication channels with interferences, which can be an air, a telephone line, a beam of light or a cable. An interference could cause errors in the transmited messages. It is very important for the recipient to receive exactly the same message as it was sent, in order to minimize the number of errors in the transmission we can use error correcting codes.

All information in a computer is represented as zeros-ones sequences. Coding of information using linear error correcting codes means adding to the sequences of k elements some extra bits in a certain way. Such codes are called redundant codes, extra bits don't carry any information and are used for error detection and correction. We denote by $[N, k]$ the code, which has a length of code words N and k information bits. Error correcting code is $A \subset \mathbb{F}_2^N$, where $\mathbb{F}_2 = \{0, 1\}$ and codewords are in classical Hamming metric:

$$d(x, y) = |\{i : x_i \neq y_i\}|.$$

In that code we have $r = N - k$ parity checks. The ratio r/N is called *code rate* and is denoted by R_C. It is interesting to look for codes with the best correction properties at the lowest code rate for economic reasons. In 1948 Claude Shannon in his works defined the concept of capacity and proved that there exists code allowing the transfering of information from any small error probability if the rate of information transmission is below the capacity. Let T be the time of transmition of a single bit. Then *the rate of information transmission* is

$$R_t = \frac{k}{NT}.$$

Unfortunately, he didn't show a way of constructing such codes. The most known classes of error correcting codes are Turbocodes and Low Density Parity Check Codes (LDPC codes). In this article we are only interested in LDPC codes. They were introduced in 1963 by Robert G. Gallanger. These codes have a high possibility of selection of parameters N and r, making it possible to create codes with a large block size and excellent correction properties. Their advantage is the existence of efficient decoding algorithms of linear complexity of the block length N.

LDPC codes can be obtained by few methods but a very good codes can be obtained from families of graphs with certain specific properties. The ability to use graphs to construct error correcting codes was first discussed by Tanner [137], [138]. This is the area where we can work because only specified graphs are suitable for creating a good code. Usually for this purpose, *simple graphs* are used, which means graphs undirected and containing no graph loops or multiple edges. The graph should be bipartite, sparse, without small cycles and biregular or regular with the possibility to obtain biregularity.

There are three ways to represent linear error correcting code allowing us to obtain LDPC codes: generator matrix G, parity checks matrix H or Tanner graph $\Gamma(V, E)$. *Parity checks matrix* for $[N, k]$ code is $r \times N$ matrix which words are zeros or ones. Rows of this matrix correspond to the parity

checks and the column to codeword bits. If a bit number j in codeword is checked by a parity check number i then the number on a position (i, j) in matrix H is one, otherwise the number is zero. Each bit is checked by a unique set of control equations. In regular LDPC code every row has the same constant weight r and every column has the same constant weight s. Switching columns doesn't change code properties and gives an equivalent code. We assume that every codeword is from set

$$\mathcal{C} = \{y \in \mathbb{F}_2^N |\ Hy^T = 0\}.$$

Generator matrix G for $[N, k]$ code is $k \times N$ zeros-ones matrix, which rows create code base. G creates a codeword y for information vector x of length k: $y = x \cdot G$. Each information vector corresponds to exactly one codeword. Parity checks matrix and generator matrix are dependent. It is known that if $G = [I_k|A]$ is generator matrix in standard form for the $[N, k]$ code $\mathcal{C}$ then $H = [-A^T|I_{N-k}]$ is a parity check matrix for $\mathcal{C}$.

Bipartite graph we call graph $\Gamma(V, E)$, in which a set of nodes V can be divided into two subsets $V = V_1 \cup V_2$ in such a way that no two vertices from each set V_i, $i = 1, 2$ are connect by an edge. The only connection is an edge from V_1 to V_2.

Tanner graph we call bipartite graph in which one subset V_1 corresponds to codeword bits and the second subset V_2 corresponds to the parity checks. Vertex from the subset V_1 is connected to a vertex from the subset V_2 if and only if a bit corresponding to vertex from V_1 is controled by the parity check corresponding to vertex from V_2. There is a standard way to create LDPC codes depending on adjacency matrix of bipartite, biregular Tanner graph. Parity check matrix H is a part of the adjacency matrix for a graph used to create a code. Adjacency matrix has the form:

$$\begin{pmatrix} 0 & H \\ H^T & 0 \end{pmatrix}.$$

Determination of the matrix H is equivalent code designation.

Codes which have sparse parity checks matrices H we call *Low Density Parity Checks Codes* (LDPC). Matrix is called a *sparse* matrix if the ratio of ones to the number of zeros in each row and column is small comparing to the length of the rows and columns. Code has a sparse matrix H if and only if when it has a representation as sparse Tanner graph. Sparse graph has a small number of edges in comparison to the number of vertices. A simple relationship describing the density of the graph $\Gamma(V, E)$ is

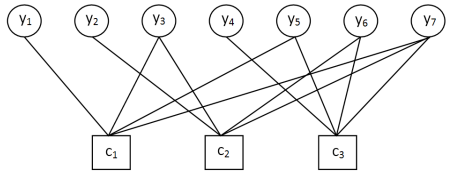
$$g = \frac{2|E|}{|V|(|V| - 1)},$$

where $|E|$ is the number of edges of graph Γ and $|V|$ is the number of verteces. The parameter g can take values from the interval $[0, 1]$. If $g = 1$, then the graph is totally connected.

Example 4.4.1. A very primary example of LDPC code is $[7, 4]$ Hamming code with $R_C = \frac{3}{7}$ and density $g = 4/15$. Parity check matrix for this code has the form:

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and Tanner graph of the code have the following structure:



To encode information vector x it is sufficient to determine the values of control bits. The remaining positions in codeword y contain all the bits of information vector x. $H[7, 4]$ has codewords of length 7 and information vectors of length 4:

$$x = [x_1, x_2, x_3, x_4]$$
$$y = [y_1, y_2, x_1, y_3, x_2, x_3, x_4]$$

To encode information vector $[1, 1, 0, 0]$ we must designate coordinates y_1, y_2, y_3 in codeword $y = [y_1, y_2, 1, y_3, 1, 0, 0]$. The parity check equations have the form:

$$\begin{cases} y_1 + x_1 + x_2 + x_4 = 0 \\ y_2 + x_1 + x_3 + x_4 = 0 \\ y_4 + x_2 + x_3 + x_4 = 0 \end{cases}$$

We substitute values x_i, $i = 1, 2, 3, 4$ and solve equations:

$$\begin{cases} y_1 + 1 + 1 + 0 = 0 \\ y_2 + 1 + 0 + 0 = 0 \\ y_4 + 1 + 0 + 0 = 0 \end{cases}$$

All calculations must be performed in the field $\mathbb{F}_2$.

4.5. Codes based on families of graphs $D(n,\mathbb{K})$, $\widetilde{D}(n,\mathbb{K})$ and $A(n,\mathbb{K})$

4.5.1. Description of graphs

Described families consist of simple, bipartite graphs of high girth (girth bigger or equal 6 for any parameters so there is no short cycles) . It is good for codes because short cycles decrease the speed of decoding algorithms. Girth in graphs from described families increasing with growing n. In fact adverse influence of short cycles decreases with increasing length of the codewords N, but they also contribute to the formation of the error-floor.

Family of graphs $\widetilde{D}(n,\mathbb{K})$ described below come from Cartan matrix

$$\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}.$$

Let us to use the analogical notions for points and lines in graph $\widetilde{D}(n,\mathbb{K})$:

$$\begin{aligned}(p) &= (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p_{2,3}, \dots, p_{i,i}, p_{i,i+1}, p_{i+1,1}, \dots),\\ [l] &= [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{2,3}, \dots, l_{i,i}, l_{i,i+1}, l_{i+1,1}, \dots].\end{aligned}$$

Infinite incidence structure $(\widetilde{P}, \widetilde{L}, \widetilde{I})$ is defined in a following way. We say that the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$\begin{aligned}&l_{1,1} - p_{1,1} = l_{1,0}p_{1,0}\\ &l_{1,2} - p_{1,2} = l_{1,1}p_{1,0}\\ &l_{2,1} - p_{2,1} = l_{0,1}p_{1,1}\\ &l_{i,i} - p_{i,i} = l_{0,1}p_{i-1,i} - l_{i,i-1}p_{1,0}\\ &l_{i,i+1} - p_{i,i+1} = l_{i,i-1}p_{1,0}\\ &l_{i+1,i} - p_{i+1,i} = l_{0,1}p_{i,i}\end{aligned} \tag{4.5.1}$$

where $i \geq 2$. The graph corresponding to the finite incidence structure $(\widetilde{P}_n, \widetilde{L}_n, \widetilde{I}_n)$ obtained by the way described above is denoted by $\widetilde{D}(n,\mathbb{K})$.

For graph $A(n,\mathbb{K})$ let us use the notion for points and lines :

$$\begin{aligned}(p) &= (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,2}, p_{2,3}, \dots, p_{i,i}, p_{i,i+1}, \dots),\\ [l] &= [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,2}, l_{2,3}, \dots, l_{i,i}, l_{i,i+1}, \dots].\end{aligned}$$

For this graph we define an incidence structure $(P, L, I)_A$ as follows. We say that the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations hold:

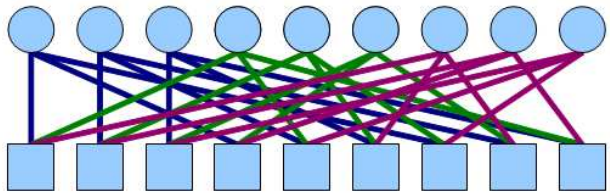


Figure 4.1. Graph $D(2,3) = \widetilde{D}(2,3) = A(2,3) = W(2,3)$

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0}p_{i-1,i} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i}p_{0,1} \end{aligned} \tag{4.5.2}$$

Denote this infinite incidence structure $(P,L,I)_A$ as $A(\mathbb{K})$ and it can be identify with the bipartite incidence graph of $(P,L,I)_A$. $A(\mathbb{K})$ is an infinite tree. For each positive integer $n > 2$ we obtain an finite incidence structure $(P_n, L_n, I_n)_A$ as above. The incidence graph corresponding to the structure $(P_n, L_n, I_n)_A$ is denoted by $A(n,\mathbb{K})$.

In case $\mathbb{K} = \mathbb{F}_q$, where q is prime power we denote $D(n,\mathbb{F}_q)$, $\widetilde{D}(n,\mathbb{F}_q)$ and $A(n,\mathbb{F}_q)$ simply as $D(n,q)$, $\widetilde{D}(n,q)$, $A(n,q)$ accordingly.

$D(n,\mathbb{K})$ and $\widetilde{D}(n,\mathbb{K})$ have the same structure for $n < 6$. For $n \leq 3$ graphs $D(n,q)$, $\widetilde{D}(n,q)$ and $A(n,q)$ are isomorphic. For $n \geq 4$ $A(n,q)$ has different structure than: $D(n,q)$, $\widetilde{D}(n,q)$ and lead as to different codes. For example, graphs $D(n,q)$ are disconnected for $k \geq 6$ when $A(n,q)$, $q \neq 2$ are connected.

For all n they are $|\mathbb{K}|$-regular but have a structure that allows us to remove points and lines in such a way that we can obtain arbitrary bidegree (a,b) for $1 \leq a,b \leq |\mathbb{K}|$. We can make it as was shown in [59]. When L is a set of all lines and P is a set of all points to obtain the desired bidegree (a,b) we must put restriction on coordinates. Let $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$ be an a-element and b-element subsets respectively and let V_P and V_L be sets of points and lines in new bipartite graph. They are the following sets:

$$\begin{aligned} V_P &= \{(p) \in P | c_p \in A\} \\ V_L &= \{[l] \in L | c_l \in B\}, \end{aligned}$$

where c_p is fixed coordinate of points and c_l is fixed coordinate of lines. Usually restriction are imposed on first coordinates.

4.5.2. Codes construction

To create LDPC code with codeword of length N we use $\widetilde{D}(n,\mathbb{K})$ ($D(n,\mathbb{K})$, $A(n,\mathbb{K})$), where $n^{|\mathbb{K}|} > N$. Each of these graphs is already bipartite. To obtain biregularity we can use method described above. Let denote the number of parity checks by d and it should be at least 2. We reduce the bidegree to $(d,|\mathbb{K}|)$ by the method shown above. We can also reduce the bidegree to (d,e), where $d,e \leq |\mathbb{K}|$ by taking smaller subsets A, B of $\mathbb{F}_q$. We can impose restrictions on the value of chosen coordinate of lines or points. Bidegree reduction can only increase the girth so there is no risk that short cycles will appear. After bidegree reduction the graph can become disconnected and divided into several components. Choose one vertex and take the component containing this selected vertex (point or line)and find all other vertices for which there is a path to the chosen one. We use this component to create a parity check matrix. If $|V_P| > |V_L|$ then points correspond to code words bits and lines to parity checks, if not then lines correspond to code words bits and points to parity checks. We decide to put one or zero on position (i,j) in parity check matrix H by checking if relations on coordinates of point number j and line number i hold (for example when we create code based on graph $A(n,\mathbb{K})$ we check if relations 4.5.2 hold).

4.5.3. Example codes and them properties

Transmission quality depends mainly on code, decoding algorithm and the level of noise in a communication channel. Properties of error-correcting codes are tested by determining the relationship between noise level and bit error rate. *Bit error rate* (BER) is the ratio of number of error bits to the total number of transferred bits. Simulation usually is carried out for Gaussian Channel where disruptions are modeled by White Gaussian Noise. Our simulations were done using BPSK modulation over AWGN channel and simple MAP decoder implementation with 10 iteration. Let y be the received codeword. MAP decoder works according to the rule which returns an output value $\hat{x}$ of a code word x for which the *a posterior* probability $P = (x|y,H)$ is maximized.

Traditionally d_v means the number of ones per column in the matrix H and d_c number of ones per row. In general it is assumed that $d_v < d_c$ in case the number of bits of information will not be greater than the number of control bits for economic reasons. In 1948 Claude Shannon [133], [134] in his works proved that there exists code allowing the transferring of information from any small error probability if the rate of information transmission is below the capacity. Parameter related to the error correction properties of the code is the minimum distance d_{min} between codewords measured

in Hamming metric. Correction properties are better for codes that have a higher minimum distance or a very small amount of codewords which are on the minimum distance from each other. A study of asymptotic performance [191] shows the future for degree distribution: $d_v \geq 2$ is enough. Every bit in codeword should be checked by unique set of control equations. If $d_v = 2$ then every bit is checked by 2 equations and the condition:

$$\binom{r}{2} > N$$

is necessary. It is easy to see that for every code in this section $r^2 > 2N$. If $d_v \geq 3$ then d_{min} for code is growing linear with increasing N, so error probability decreases exponentially with increasing length of the block. 4.2, 4.3, 4.4 show that presented codes give good results for $d_v = 2$. The codes considered in this section have $d_v = \min(a, b)$. 4.1, 4.2, 4.3, 4.4 and 4.5 show properties of sample described codes.

4.2, 4.3, 4.4 show BER for codes obtained from graphs described in 4.1, 4.2, 4.3 accordingly. With increasing parameter n graphs for the same field produce codes with better correcting properties (4.2, 4.3, 4.4) and bigger block length N. In order to compare 4.8 shows codes based on some representatives of family $A(n, q)$ and 4.9 of family $D(n, q)$ with the same paremeter accordingly. We see that codes based on representatives of family $A(n, q)$ have better error correcting properties. This fact is supported by a dozen other simulations conducted.

The most consistent structure have graphs $A(n, q)$, so that they give codes with the best correcting properties. For example, graph $A(8, 5)$ after the reduction of bidegrees to $(2, 5)$ splits into 125 components and $D(8, 5)$ into 625, $A(10, 3)$ after the reduction of bidegrees to $(2, 3)$ splits into 81 components and $D(10, 3)$ into 243. The worst results in the case of the considered families of graphs give codes obtained from graphs $D(n, q)$. The structure of $A(n, q)$ after biregularity reduction allows us to obtain codes with bigger block size than for codes obtained from $D(n, q)$. When we use bigger field we obtain better code rate. Reducting bidegrees to $(2, q)$ gives code rate $\frac{2}{q}$. Obviously, in a case of each code we can reduce the bidegrees of a graph. After the reduction the code rate can increase. A good example is a case of bidegrees 3 and q.

Use bidegree (a, b), where $a \geq 3$ makes the desired codes much better (4.6) and of bigger block size. For this two presented codes $d_v = 3$. In case of codes which come from presented families, reducing bidegrees to (a, b) gives code rate $R_C = \frac{a}{b}$. Codes described in 4.1, 4.2, 4.3 (4.2, 4.3, 4.4) have code rate 0.4. When we use bigger field $\mathbb{F}_q$ we can obtain different and often better (more economic) code rate (For example see 4.4) and usually code correcting properties don't change much. However, we must be carefull

because used much bigger field and reduced biregularity to $(2, q)$ or $(3, q)$ can give R_C close to zero, but error correcting properties can be much worse.

Presented codes have a high possibility to choose the code rate R_C. In many well known constructions the code rate is strictly determined, for example is equal to 1/2. David MacKay considerd [107], [90] very good, randomly generated codes with code rate 1/2 and 1/4. Codes arising from graphs with symmetric adjacency matrix, which was considered in [145] have code rate 1/2 and 1. 4.6 shows codes: $[75, 150]$ (blue), $[500, 1000]$ (green), $[1875, 3750]$ (purple), $[250, 500]$ (black) obtained from random construction based on Radford M. Neal's programs available from [102]. Radfold M. Neal and David MacKay reinvented LDPC codes in the mid-1990' (see [107]). 4.7 shows codes based on presented graphs with accordingly to randomly generated codes with the same number of information bits k. It is easy to see that codes (blue, green and purple) based on graphs (4.7) with the same number of information bits as random codes (4.6) have better error correcting properties and less code rate (4.5).

Table 4.1. Properties of graphs $\widetilde{D}(n, 5)$ after receiving bidegree $(2, 5)$ used for presented sample codes

Based graph	$\lvert P\rvert = \lvert L\rvert$	Size of desired H	Block length
$\widetilde{D}(2, 5)$	25	10×25	25
$\widetilde{D}(3, 5)$	125	10×25	25
$\widetilde{D}(4, 5)$	625	50×125	125
$\widetilde{D}(5, 5)$	3125	50×125	125
$\widetilde{D}(6, 5)$	15625	50×125	125
$\widetilde{D}(7, 5)$	78125	1250×3125	3125
$\widetilde{D}(8, 5)$	390625	1250×3125	3125
$\widetilde{D}(9, 5)$	1953125	1250×3125	3125
$\widetilde{D}(10, 5)$	9765625	6250×15625	15625

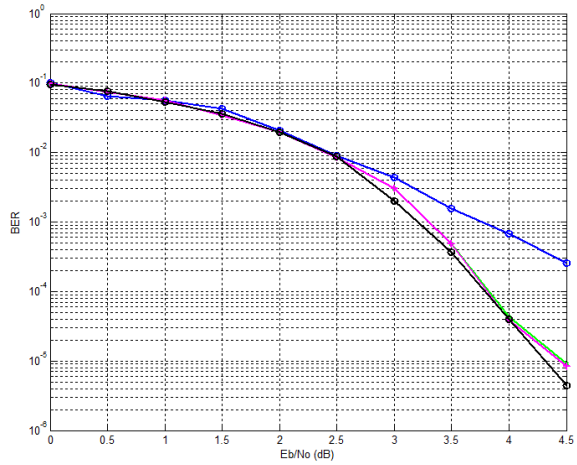


Figure 4.2. Bit error rate for $[50, 125]$ code (blue) based on $\widetilde{D}(6, 5)$, $[1250, 3125]$ code (red) based on $\widetilde{D}(7, 5)$, $[1250, 3125]$ code (purple) based on $\widetilde{D}(8, 5)$ and $[1250, 3125]$ code (black) based on $\widetilde{D}(10, 5)$

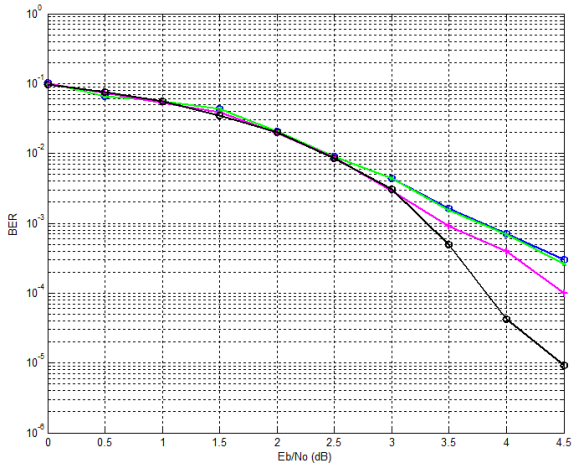


Figure 4.3. Bit error rate for $[50, 125]$ code (green) based on $D(6, 5)$, $[50, 125]$ code (blue) based on $D(7, 5)$, $[250, 625]$ code (purple) based on $D(8, 5)$ and $[1250, 3125]$ code (black) based on $D(9, 5)$

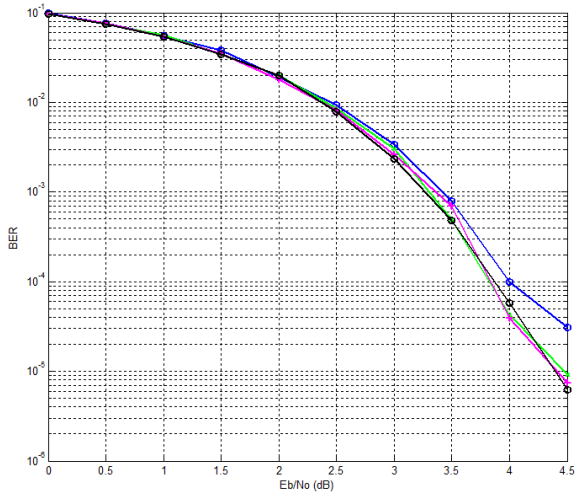


Figure 4.4. Bit error rate for $[250, 625]$ code (blue) based on $A(6, 5)$, $[1250, 3125]$ code (green) based on $A(7, 5)$, $[1250, 3125]$ code (purple) based on $A(8, 5)$ and $[1250, 3125]$ code (black) based on $A(9, 5)$

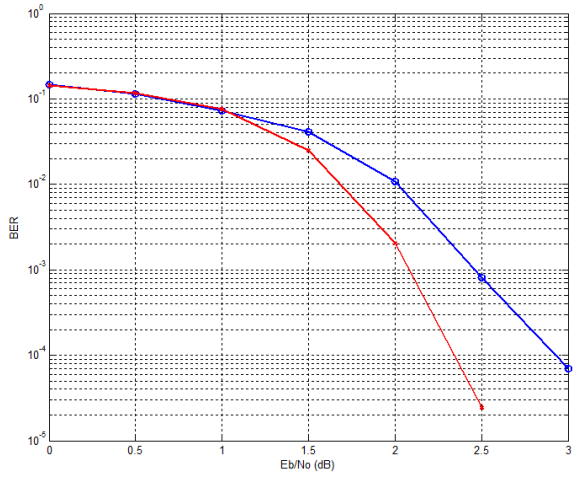


Figure 4.5. Bit error rate for $[1875, 3125]$ code (red) based on $\widetilde{D}(6, 5)$ and $[375, 625]$ code (blue) based on $\widetilde{D}(5, 5)$ after reducing bidegree to $(3, 5)$

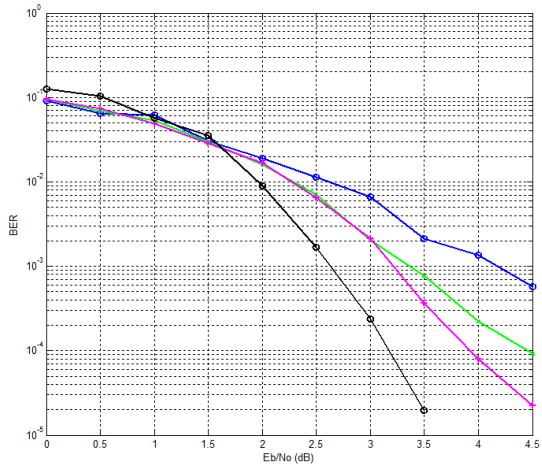


Figure 4.6. Bit error rate for $[75, 150]$ code (blue), $[500, 1000]$ code (green), $[1875, 3750]$ code (purple) and $[250, 500]$ code (black), all based on Radford M. Neal random constructions [27] with code rate $R_C = 1/2$.

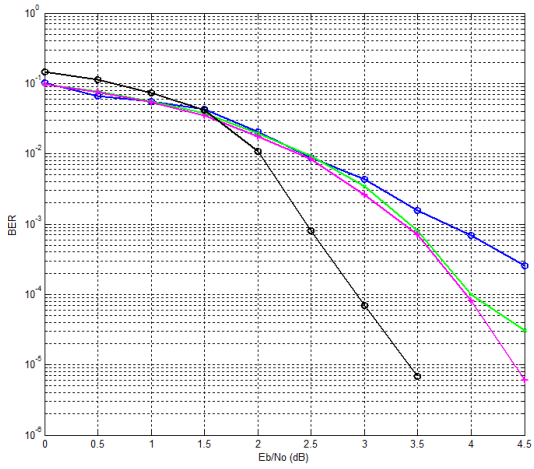


Figure 4.7. Bit error rate for $[50, 125]$ code (blue) based on $\widetilde{D}(6, 5)$, $[250, 625]$ code (green) based on $A(6, 5)$, $[1250, 3125]$ code (purple) based on $A(9, 5)$ and $[375, 625]$ code (black) based on $\widetilde{D}(5, 5)$

4.5.4. Remarks

Instead of using $\mathbb{F}_q$ as $\mathbb{K}$ we can use ring $\mathbb{Z}_n$ and modulo operations. Modified codes where rings are used, based on subgraph of $A(n, \mathbb{Z}_m)$ give better code than those based on subgraph of $D(n, \mathbb{Z}_m)$ (4.10 shows results for fixed parameters).

In [51] authors as coordinates used elements from $\mathbb{F}_q$ where q is the first

Table 4.2. Properties of graphs $D(n, 5)$ after receiving bidegree $(2, 5)$ used for presented sample codes

Based graph	$\lvert P\rvert = \lvert L\rvert$	Size of desired H	Block length
$D(2, 5)$	25	10×25	25
$D(3, 5)$	125	10×25	25
$D(4, 5)$	625	50×125	125
$D(5, 5)$	3125	50×125	125
$D(6, 5)$	15625	50×125	125
$D(7, 5)$	78125	50×125	125
$D(8, 5)$	390625	250×625	625
$D(9, 5)$	1953125	1250×3125	3125
$D(10, 5)$	9765625	1250×3125	3125

Table 4.3. Properties of graphs $A(n, 5)$ after receiving bidegree $(2, 5)$ used for presented sample codes

Based graph	$\lvert P\rvert = \lvert L\rvert$	Size of desired H	Block length
$A(2, 5)$	25	10×25	25
$A(3, 5)$	125	10×25	25
$A(4, 5)$	625	50×125	125
$A(5, 5)$	3125	50×125	125
$A(6, 5)$	15625	250×625	625
$A(7, 5)$	78125	1250×3125	3125
$A(8, 5)$	390625	1250×3125	3125
$A(9, 5)$	1953125	1250×3125	3125
$A(10, 5)$	9765625	6250×15625	15625

Table 4.4. Properties of graphs $\widetilde{D}(5, q)$, $D(5, q)$ and $A(5, q)$ after receiving bidegree to $(2, 5)$ and $(2, q)$used for presented sample codes

Based graph	$\lvert P\rvert = \lvert L\rvert$	Biregularity	Size of desired H	Block length	R_C
$\widetilde{D}(5, 5)$, $D(5, 5)$, $A(5, 5)$	3125	(2,5)	50×125	125	0.4
$\widetilde{D}(5, 7)$, $D(5, 7)$, $A(5, 7)$	16807	(2,5)	98×245	245	0.4
$\widetilde{D}(5, 11)$, $D(5, 11)$, $A(5, 11)$	161051	(2,5)	242×605	605	0.4
$\widetilde{D}(5, 7)$, $D(5, 7)$, $A(5, 7)$	16807	(2,7)	98×343	343	0.28
$\widetilde{D}(5, 11)$, $D(5, 11)$, $A(5, 11)$	161051	(2,11)	242×1331	1331	0.18

prime greater than n. We take q which is first prime power greater than n. 4.11 shows that for the code based on $D(3,16)$ we obtain as good results as for $D(3,17)$. $D(3,16)$ gives $[256,32]$ code with slightly better code rate than code $[255,34]$ arising from $D(3,17)$.

4.6. Codes based on generalised polygons

4.6.1. Description of generalised polygons

The missing definitions on theory of simple graphs the reader can find in [16].

The distance between vertices v_1 and v_2 of the graph is the length of minimal pass from v_1 and v_2. The graph is connected if for arbitrary pair

Table 4.5. Properties of graphs after receiving bidegree $(2,s)$ used for presented sample codes

Initial graph	Biregularity	Number of lines in fixed component	Number of points in fixed component	Code rate
$A(6,6)$	$(2,6)$	648	216	0.(3)
$A(6,7)$	$(2,7)$	2401	686	≈ 0.286
$A(8,5)$	$(2,5)$	3125	1250	0.4
$A(10,3)$	$(2,3)$	729	486	0.(6)
$D(6,6)$	$(2,6)$	216	72	0.(3)
$D(6,7)$	$(2,7)$	2401	686	≈ 0.286
$D(8,5)$	$(2,5)$	625	250	0.4
$D(10,3)$	$(2,3)$	243	162	0.(6)

Table 4.6. Comparison between presented codes and other effective LDPC

Code	Number of information bits	Block length	R_C	Number of ones per column
random $[75,150]$	75	150	0.5	2
random $[500,1000]$	500	1000	0.5	2
random $[1875,3750]$	1875	3750	0.5	2
random $[250,500]$	250	500	0.5	3
$[50,125]$ based on $\widetilde{D}(6,5)$	75	125	0.4	2
$[250,625]$ based on $A(6,5)$	500	1250×3125	0.4	2
$[1250,3125]$ based on $A(9,5)$	1875	1250×3125	0.4	2
$[375,625]$ based on $\widetilde{D}(5,5)$	250	625	0.6	3

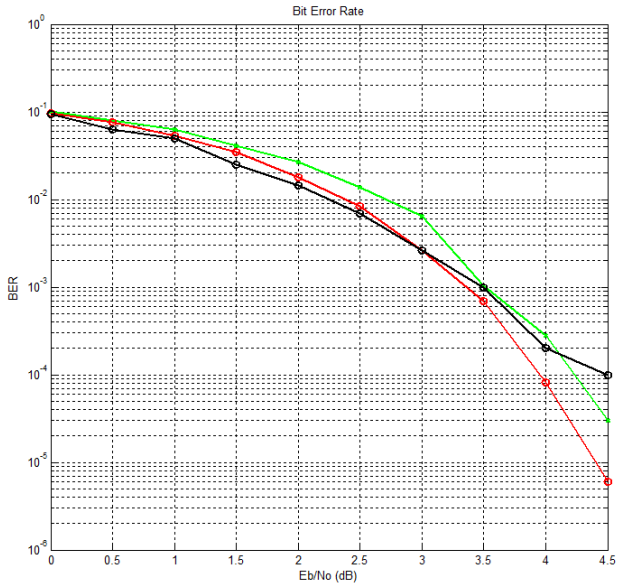


Figure 4.8. Bit error rate for $[2401, 686]$ code (green) based on $A(6, 7)$, $[3125, 1250]$ code (red) based on $A(8, 5)$ and $[729, 486]$ code (black) based on $A(10, 3)$

of vertices v_1, v_2 there is a pass from v_1 to v_2. The diameter of connected simple graph is the maximum od distances between vertices of the graph.

We refer to bipartite graph $\Gamma(V, E)$ with partition sets V_i, $i = 1, 2$, $V = V_1 \cup V_2$ as *biregular one* if the number of neighbors for representatives of each partition sets are constants $r + 1$ and $s + 1$ (bidegrees). We call the *regular graph* in case $r = s$.

Generalized m-gons are connected biregular bipartite graphs with girth $2m$ and diameter m. Traditionally, in case of generalised m-gon $\Gamma(V_1 \cup V_2, E)$ one partition set of $V_1 = P$ is called set of point and other $V_2 = L$ is called the set of lines. Vertex corresponds to point can be connected be edges only with some vertex from L and vertex corresponds to line can be connect only with vertex from set P.

When two vertices point (p) and line $[l]$ are connected by edge we call this incidence pair (p, l) *flag*. We define the distance from flag (p, l) to vertex $v \in V$ as the sum of distances from p to v and l to v.

Affine generalized m-gon can be obtained by the following way. Let us chose flag (p, l) and remove all points and lines except these with are on maximal distance from the flag. By this method we obtain biregular graph with bidegrees r and s. It is clear that affine generalized m-gons have girth

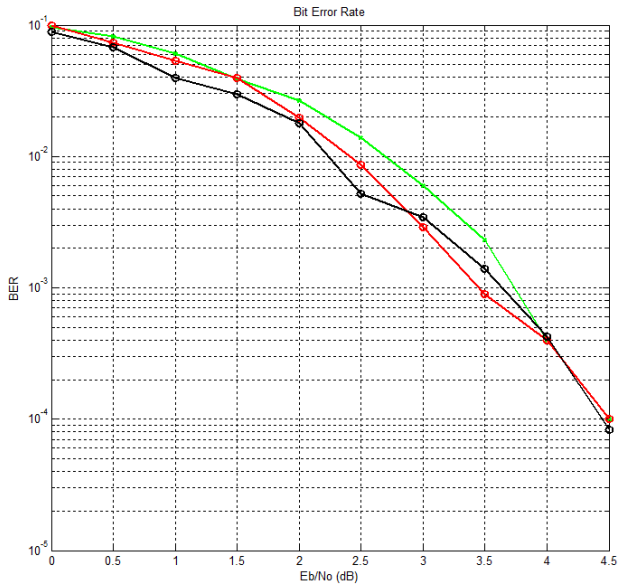


Figure 4.9. Bit error rate for $[2401, 686]$ code (green) based on $D(6, 7)$, $[625, 250]$ code (red) based on $D(8, 5)$ and $[243, 162]$ code (black) based on $D(10, 3)$

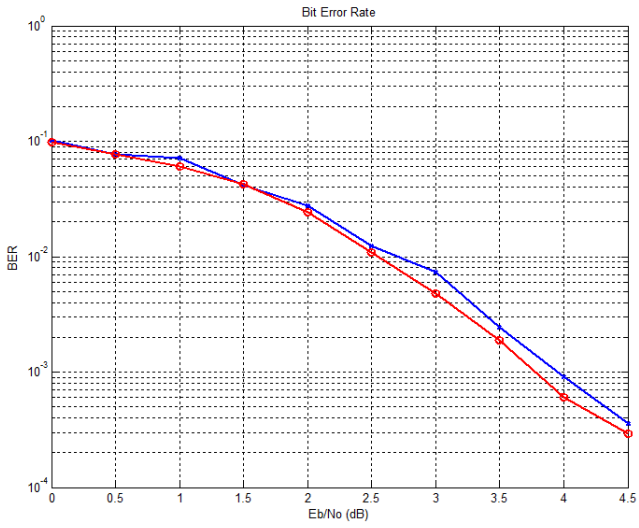


Figure 4.10. Bit error rate for $[648, 216]$ code (red) based on $A(6, \mathbb{Z}_6)$, $[625, 250]$ code (blue) based on $D(6, \mathbb{Z}_6)$

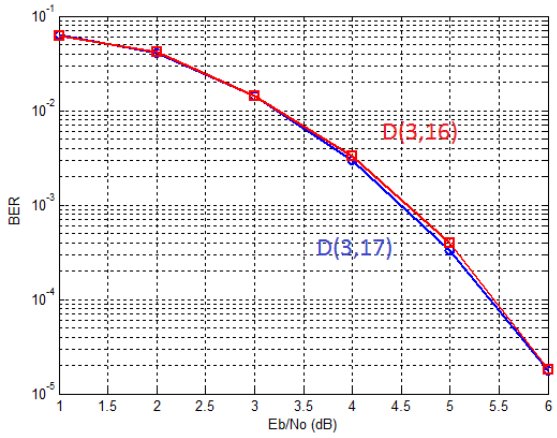


Figure 4.11. Bit error rate for $[256, 32]$ code (square) based on $D(3, 16)$ and $[255, 34]$ code (circle) based on $D(3, 17)$

$\geq 2m$. If the generalised m-gon is edge transitive then the construction of generalised m-gon does not depend on the choice of flag. In case $m = 6$ there is only one known family of regular generalised m-gons. Ii is bidegree is $r + 1 = s + 1$, where $r = q = p^m$, p is prime, $m \geq 1$. Each representative of this family is an edge transitive graph.

When $m = 6$ we denote generalized m-gon as $GH(q, q)$ and affine generalized m-gon as $AH(q, q)$, where q is a prime power. For more details about the structure we refer to [16]. Notice that $q + 1$-regular graph $GH(q, q)$ has $1 + q + q^2 + q^3 + q^4 + q^5$ points and the same number of lines. The order of q regular $AH(q, q)$ is $2q$.

The following interpretation of $AH(q, q)$ the reader can find in [156]. Let $\mathbb{F}_q$ be the finite field containing q elements. Each point can be identified with $(p) = (x, y, z, u, w) \in$ and each line with $[l] = [a, b, c, d, f]$. Brackets and parenthesis allow us to distinguish points and lines. We say point (p) is incident to line $[l]$, and we write $(p)I[l]$, if following relations on their coordinates hold:

$$\begin{aligned} y - b &= xa \\ 2c - z &= 2xb \\ u - 3d &= -3xc \\ 2w - 3f &= 3zb - 3yc + ua \end{aligned} \tag{4.6.1}$$

where all coordinates are elements of $\mathbb{F}_q$. Any bipartite graph $\Gamma(P \cup L, E)$ has *bidegree* (r, s) if every vertex from P has degree r and every vertex from L has degree s. $AH(q, q)$ has a structure that allows us to remove points and lines in such a way that we can obtain arbitrary bidegree. We can make it exactly the same as it was done with $D(n, q)$ and $A(n, k)$ in previous

section. Let L be set of all lines and P set of all points. To obtain the desired bidegree (r, s) we must put restriction on coordinates. Let $R \subset \mathbb{F}_q$ and $S \subset \mathbb{F}_q$ be an r-element and s-element subsets respectively and let V_P and V_L be sets of points and lines in new bipartite graph. They are the following sets:

$$V_P = \{(p) \in P | x \in R\}$$
$$V_L = \{[l] \in L | a \in S\}.$$

If set of points is bigger than set of lines then points correspond to codeword bits and lines correspond to parity checks. Otherwise, lines correspond to codeword bits and points correspond to parity checks. The ratio of total number of bits in codeword to number of parity bits is called code rate and is denoted as R_C. The lower the code rate is the more economic the code is. Thus, the most wanted codes are those with low code rate and the best error correcting properties.

4.6.2. Code construction

To create LDPC code of dimension d containing (N, k) Hamming code as component codes we must use $AH(q, q)$, where q is the first prime which is greater than N. Then we reduce the bidegree to (d, N). Bidegree reduction can only increase the girth. After reduction the bidegree graph can be disconnected. When we put restriction on coordinates x of point the graph will be divided into several components, but when we put restriction on first coordinates a of lines graph remains connected. This is due to lack of symmetry $AH(q, q)$. Next we take one component containing a chosen vertex (point or line) and find all other vertices for which there is a path to the chosen vertex. We use this component to create a parity checks matrix. If $|V_P| > |V_L|$ then points correspond to code words bits and lines to parity checks if not then lines correspond to code words bits and points to parity checks. We decide to put one or zero in parity check matrix by checking if relations 4.6.1 on their coordinates holds. Every bit from codeword is checked by d parity checks. In the case of graphs $D(n, q)$ resulting graphs are always disconnected.

4.6.3. Example codes and them properties

It is interesting that the properties of codes obtained from $D(5, q)$ and $AH(q, q)$ through the restriction on points coordinates are similar as seen in 4.12 and 4.13. 4.7 contains the data about resulting graphs.

Graphs $D(5, 7)$ and $AH(7, 7)$ with $x \in R$ after reduction bidegree to $(2, 7)$ split into 49 components and $D(4, 7)$ splits into 7 ones. They all

give equivalent codes os there is no different which component we choose. Graphs $AH(17,17)$ with restriction on points coordinate $x \in R$, $|R| = 2$ and $D(5,17)$ after reduction bidegree to $(2,15)$ split into 289 components. When we use bigger field we obtain better code rate, for example taking $\mathbb{F}_7$ for codes based on these graphs code rate is $R_C \approx 0.286$ but taking $\mathbb{F}_{17}$ we have $R_C = 0.1(3)$. Obviously in each code we can reduce the bidegree of graphs to $(3,7)$ or $(3,15)$ depending on a field and a graph. But then code rate increases.

In $D(n,q)$ there is no differences if we put restriction on points or lines. When we take lines from smaller partition set in a reduced $AH(q,q)$, we obtain better code but with exactly the same code rate $R_C \approx 0.286$ as if we take points from R, $|R| = 2$. 4.14 shows results.

Remark 4.6.1. It is also possibility to construct LDPC codes based on graphs $AO(q,q^2)$, $q = 2^{2k+1}$ arising from generalized 8-gons, which girth is 16, so it seems that this kind of codes have better error correcting properties. Graph $AO(q,q^2)$ has bidegree (q,q^2). It also has structure which allows easily to remove points and lines to obtain arbitrary bidegree exactly as it was done with $D(k,q)$ and $AH(q,q)$.

Table 4.7. Graphs property after receiving bidegree $(2,7)$ and $(2,15)$ respectively

Initial graph	Girth	Restriction on coordinates	Number of lines in fixed component	Number of points in fixed component	Code rate
$AH(17,17)$	12	$a \in S$, $\|S\| = 2$ $x \in R$, $\|R\| = 15$	167042	1252815	0.1(3)
$AH(17,17)$	12	$x \in R$, $\|R\| = 2$ $a \in S$, $\|S\| = 15$	4335	578	0.1(3)
$D(5,17)$	10	$x \in R$, $\|R\| = 2$ $a \in S$, $\|S\| = 15$	4335	578	0.1(3)
$D(5,17)$	10	$a \in S$, $\|S\| = 2$ $x \in R$, $\|R\| = 15$	578	4335	0.1(3)
$AH(7,7)$	12	$a \in S$, $\|S\| = 2$	4802	16807	≈ 0.286
$AH(7,7)$	12	$x \in R$, $\|R\| = 2$	343	98	≈ 0.286
$D(5,7)$	10	$x \in R$, $\|R\| = 2$	343	98	≈ 0.286
$D(5,7)$	10	$a \in S$, $\|S\| = 2$	98	343	≈ 0.286
$D(4,7)$	8	$x \in R$, $\|R\| = 2$	98	343	≈ 0.286
$D(4,7)$	8	$a \in S$, $\|S\| = 2$	343	98	≈ 0.286

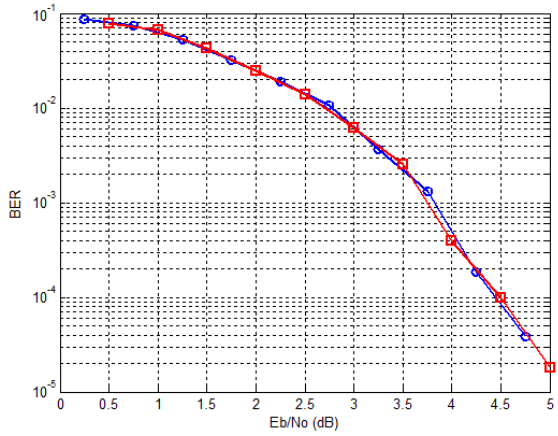


Figure 4.12. Bit error rate for $[343, 98]$ code (circle) based on $AH(7, 7)$ and $[343, 98]$ code (square) based on $D(5, 7)$, both with $x \in \{0, 1\}$

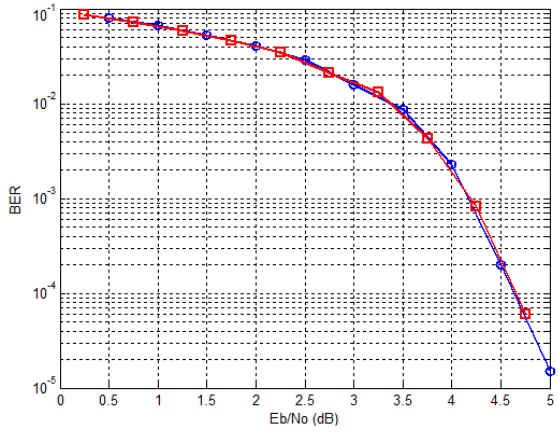


Figure 4.13. Bit error rate for $[4335, 578]$ code (circle) based on $AH(17, 17)$ and $[4335, 578]$ code (square) based on $D(5, 17)$, both with $x \in \{0, 1\}$ and $a \in \{0, 14\}$

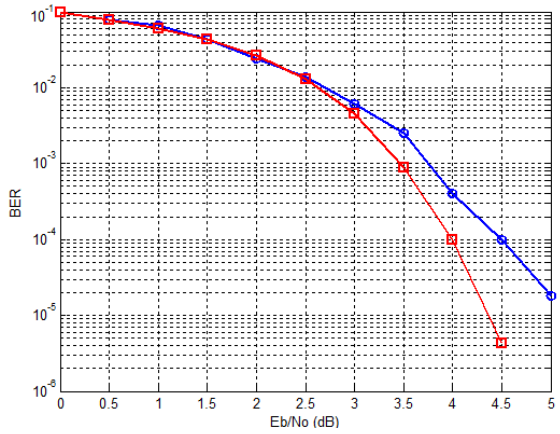


Figure 4.14. Bit error rate for $[16807, 4802]$ code (square) with $a \in \{0, 1\}$ and chosen vertex $[l] = [0, 0, 0, 0, 0]$ and $[343, 98]$ code (circle) with $x \in \{0, 1\}$ and chosen vertex $(p) = (0, 0, 0, 0, 0)$, both based on $AH(7, 7)$

Chapter 5

Directed graphs of high girth and large diagram indicator

5.1. On directed graphs of binary relations

It is known that rooted tree is a directed graph. The concept of a tree which allows consideration of simple and directed trees as members of one class of graphs the reader can find in [127].

The missing theoretical definitions on directed graphs the reader can find in [105]. Let Φ be an *irreflexive binary relation* over the set V, i.e., $\Phi \in V \times V$ and for each v the pair (v, v) is not the element of Φ. We refer to the graph of Φ as *directed graph* (shortly *digraph*).

We say that u is the *neighbour of vertex* v and write $v \to u$ if $(v, u) \in \Phi$. We use the term *balanced binary relation graph* for the graph Γ of irreflexive binary relation ϕ over a finite set V such that for each $v \in V$ the sets $\{x|(x, v) \in \phi\}$ and $\{x|(v, x) \in \phi\}$ have the same cardinality. It is a directed graph without loops and multiple edges. We say that a *balanced graph* Γ is k-regular if for each vertex $v \in \Gamma$ the cardinality of $\{x|(v, x) \in \phi\}$ is k.

Let Γ be the graph of binary relation. The *path* between vertices a and b is the sequence $a = x_0 \to x_1 \to \cdots \to x_s = b$ of length s, where x_i, $i = 0, 1, \ldots s$ are distinct vertices.

We say that the pair of paths $a = x_0 \to x_1 \to \cdots \to x_s = b$, $s \geq 1$ and $a = y_0 \to y_1 \to \cdots \to y_t = b$, $t \geq 1$ form an (s, t)-*commutative diagram* $O_{s,t}$ if $x_i \neq y_j$ for $0 < i < s$, $0 < j < t$. Without loss of generality we assume that $s \geq t$.

We refer to the number $\max(s, t)$ as the *rank of commutative diagram* $O_{s,t}$. It is ≥ 2, because the graph does not contain multiple edges.

Notice that the graph of antireflexive binary relation may have a *directed cycle* $O_s = O_{s,0}$: $v_0 \to v_1 \to \cdots \to v_{s-1} \to v_0$, where v_i, $i = 0, 1, \ldots, s-1$, $s \geq 2$ are distinct vertices.

We will count directed cycles as *commutative diagrams*.

Let $dirg(G)$ be a *directed girth of the graph* G, i.e., the minimal length of a directed cycle in the graph.

For the investigation of commutative diagrams we introduce *diagram indicator* of a directed graph Γ, denoted by $\mathrm{Dind}(\Gamma)$, which is the minimal value for $\max(s, t)$ for parameters s, t of a commutative diagram $O_{s,t}$, $s+t \geq 3$. The minimum is taken over all pairs of vertices (a, b) in the directed graph. Notice that two vertices v and u at distance $< \mathrm{Dind}(\Gamma)$ are connected by the unique path from u to v of length $< \mathrm{Dind}(\Gamma)$.

We assume that the *girth* $g(\Gamma)$ of a directed graph Γ with the girth indicator $d + 1$ is $2d + 1$ if it contains a commutative diagram $O_{d+1,d}$. If there are no such diagrams we assume that $g(\Gamma)$ is $2d + 2$.

In case of a symmetric binary relation $\mathrm{Dind}(\Gamma) = d$ implies that the girth of the graph is $2d$ or $2d - 1$. It does not contain an even cycle $2d - 2$. In general case $\mathrm{Dind}(\Gamma) = d$ implies that $g(\Gamma) \geq d + 1$. So in the case

of the family of graphs with unbounded girth indicator, the girth is also unbounded. We also have

$$\mathrm{Dind}(\Gamma) \geq g(\Gamma)/2.$$

In the case of symmetric irreflexive relations the above mentioned general definition of the girth agrees with the standard definition of the *girth* of simple graph, i.e., the length of its minimal cycle.

We will use the term *the family of directed graphs of large girth indicator* for the family of balanced directed regular graphs Γ_i of degree k_i and order v_i such that

$$\mathrm{Dind}(\Gamma_i) \geq c \log_{k_i} v_i,$$

where c is a constant independent of i.

As it follows from the definition $g(\Gamma_i) \geq c' \log_{k_i}(v_i)$ for an appropriate constant c'. So, it agrees with the well known definition for the case of simple graphs.

The *directed diameter* of the strongly connected digraph Γ, denoted by $\mathrm{dirdim}(\Gamma)$ is minimal number d such that every pair of vertices is connected by a directed path of length at most d (see [105]). We denote directed path of length d between two vertices a and b by $a = x_0 \to x_1 \to x_2 \cdots \to x_d = b$. Recall that a digraph is *k-regular*, if each vertex of G has exactly k outputs.

Let $\mathfrak{F}$ be the infinite family of k_i regular directed graphs Γ_i of order v_i, $i = 1, 2, \ldots$. We say, that $\mathfrak{F}$ is a *family of small world directed graphs* if

$$\mathrm{dirdiam}(\Gamma_i) \leq C \log_{k_i}(v_i),$$

for some constant C independent on i.

The definition of small world simple graphs and related explicit constructions the reader can find in [11]. For the studies of small world simple graphs without small cycles see [9], [178].

5.2. On the directed algebraic graphs over commutative rings

Let $\mathbb{K}$ be a commutative ring. A *directed algebraic graph* ϕ over $\mathbb{K}$ consists of two things, such as the *vertex set* Q being a quasiprojective variety over $\mathbb{K}$ of nonzero dimension and the *edge set* being a quasiprojective variety ϕ in $Q \times Q$. We assume that ($x\phi y$ means $(x, y) \in \phi$).

The graph ϕ is *balanced* if for each vertex $v \in Q$ the sets

$$\mathrm{Im}(v) = \{x \mid v\phi x\} \text{ and } \mathrm{Out}(v) = \{x \mid x\phi v\}$$

are quasiprojective varieties over $\mathbb{K}$ of the same dimension.

The graph ϕ is *homogeneous* (or (r,s)-homogeneous) if for each vertex $v \in Q$ the sets

$$\mathrm{Im}(v) = \{x | v\phi x\} \text{ and } \mathrm{Out}(v) = \{x | x\phi v\}$$

are quasiprojective varieties over $\mathbb{K}$ of fixed nonzero dimensions r and s, respectively.

In the case of balanced homogeneous algebraic graphs for which $r = s$ we will use the term *r-homogeneous* graph. Finally, *regular algebraic graph* is a balanced homogeneous algebraic graph over the ring $\mathbb{K}$ if each pair of vertices v_1 and v_2 is a pair of isomorphic algebraic varieties.

Let $M(\mathbb{K})$ be the totality of nonzero ring elements from $\mathbb{K}$, such that for each x and $y \in \mathbb{K}$ the product xy is also an element of $M(\mathbb{K})$. We refer to $M(\mathbb{K})$ as a *multiplicative set*. We assume that the $M(\mathbb{K})$ contains at least 3 elements. We assume here that $\mathbb{K}$ is finite, thus the vertex set and the edge set are finite and we get a usual finite directed graph.

We apply the term *affine graph* for the regular algebraic graph such that its vertex set is an affine variety in Zarisski topology.

Let G be r-regular affine graph with the vertex $V(G)$, such that Out v, $v \in V(G)$ is isomorphic to the variety $\mathfrak{R}(\mathbb{K})$. Let the variety $E(G)$ be its arrow set (a binary relation in $V(G) \times V(G)$). We use the standard term *perfect algebraic colouring of edges* for the polynomial map ρ from $E(G)$ onto the set $\mathfrak{R}(\mathbb{K})$ (the set of colours) if for each vertex v different output arrows $e_1 \in \mathrm{Out}(v)$ and $e_2 \in \mathrm{Out}(v)$ have distinct colours $\rho(e_1)$ and $\rho(e_2)$ and the operator $N_{G,\alpha}(v)$ of taking the neighbour u of vertex v ($v \to u$) is a polynomial map of the variety $V(G)$ into itself.

We will use the term *rainbow-like colouring* in the case when the perfect algebraic colouring is a bijection.

Studies of infinite families of directed affine algebraic digraphs over commutative rings $\mathbb{K}$ of large girth with the rainbow-like colouring is a nice and a difficult mathematical problem. Good news is that such families do exist. In the next section we consider the example of such a family for each commutative ring with more than 2 regular elements.

5.3. On the concept of dooble directed graphs for tactical configuration

E. Moore used term *tactical configuration* of order (s,t) for biregular bipartite simple graphs with bidegrees $s+1$ and $r+1$. It corresponds to the incidence structure with the point set P, the line set L and the symmetric incidence relation I. Its size can be computed as $|P|(s+1)$ or $|L|(t+1)$.

Let (P, L, I) be the incidence structure corresponding to regular tactical configuration of order t. Let

$\mathcal{F}_1 = \{(l,p)|l \in L, p \in P, lIp\}$ and $\mathcal{F}_2 = \{[l,p]|l \in L, p \in P, lIp\}$ be two copies of the totality of flags for (P, L, I). Brackets and parenthesis allow us to distinguish elements from $\mathcal{F}_1$ and $\mathcal{F}_2$. Let $D\mathcal{F}(I)$ be the *directed graph* (*double directed flag graph*) on the disjoint union of $\mathcal{F}_1$ with $\mathcal{F}_2$ defined by the following rules

$(l_1, p_1) \to [l_2, p_2]$ if and only if $p_1 = p_2$ and $l_1 \neq l_2$,
$[l_2, p_2] \to (l_1, p_1)$ if and only if $l_1 = l_2$ and $p_1 \neq p_2$.

We already consider the family of graphs $D(n, \mathbb{K})$, where $n > 5$ is a positive integer and $\mathbb{K}$ is a commutative ring. Let $DD(n, \mathbb{K})$ ($DD(n, \mathbb{K})$) be the double directed graph of the bipartite graph $D(n, \mathbb{K})$ ($D(\mathbb{K})$, respectively).

Remember, that we have the arc e of kind

$$(l^1, p^1) \to [l^2, p^2]$$

if and only if $p^1 = p^2$ and $l^1 \neq l^2$. Let us assume that the colour $\rho(e)$ of the arc e is $l^1_{1,0} - l^2_{1,0}$.

Recall, that we have the arc e' of kind

$$[l^2, p^2] \to (l^1, p^1)$$

if and only if $l^1 = l^2$ and $p^1 \neq p^2$. Let us assume that the colour $\rho(e')$ of arc e' is $p^1_{0,1} - p^2_{0,1}$.

It is easy to see that ρ is a perfect algebraic colouring. If $\mathbb{K}$ is finite, then the cardinality of the colour set is $(|\mathbb{K}| - 1)$.

Let M be the multiplicative set of the ring $\mathbb{K}$. It means that $x \in M$ and $y \in \mathbb{K}$ imply $xy \in \mathbb{K}$, and 0 does not belong to M. Let us delete all arrows with colour, which is not an element M. We will show that a new graph $DD(n, M, \mathbb{K})$ ($DD(M, \mathbb{K})$) with the induced colouring into colours from the alphabet M is vertex transitive. Really, according to theorem of previous chapter graph $D(n, \mathbb{K})$ is an edge transitive. This fact had been established via the description of regular on the edge set subgroup $U_D(n, \mathbb{K})$ of the automorphisms group $Aut(D(n, \mathbb{K}))$. The vertex set for the graph $DD(n, \mathbb{K})$ consists of two copies $\mathcal{F}_1$ and $\mathcal{F}_2$ of the edge set for $D(n, \mathbb{K})$.

If $\mathbb{K}$ is finite, then the cardinality of the colour set is $|M|$. We can show that a new affine graph $DD(n, M, \mathbb{K})$ with the induced colouring into colours from the alphabet $M(\mathbb{K})$ is vertex transitive (see previous chapter). We can change graphd $D(n, \mathbb{K})$ for graphs $CD(n, \mathbb{K})$ consider double directed graphs $DCD(n, \mathbb{K})$ for $CD(n, \mathbb{K})$. Let ψ_n be canonical homomorphism of graph $D(n, \mathbb{K})$ onto $CD(n, \mathbb{K})$, which send point $(p_{01}, p_{11}, \dots)$ and line $[l_{1,0}, l_{1,1}, \dots]$ to the vectors without coordinates with indexes of kind (i, i).

We may mark vertices of $DCD(n, \mathbb{K})$ by colours from $\mathbb{K} - \{0\}$ of their preimages for ψ_n, choose multiplicative subset M of commutative ring $\mathbb{K}$ and delete all arrows of colours from $\mathbb{K} - M$ and obtain family $DCD(n, M, \mathbb{K})$

Theorem 5.3.1. *Let $\mathbb{K}$ be finite ring and M, $|M| \geq 2$ be a multiplicative set of $\mathbb{K}$. Then families $DD(n, M, \mathbb{K})$ and $DCD(n, M, \mathbb{K})$, $n = 1, 2, \ldots$ are families of directed graphs of large girth indicator.*

Let us consider the map δ_n of deleting components of points and lines of $D(n, \mathbb{K})$ with coordinates of kind (i, i) and $(i, i + 1)$. It is easy to see that δ_n is a homomorphism of graph $D(n, \mathbb{K})$ onto graph $A(n, \mathbb{K})$. We assume that colours of $v \in V(D(n, \mathbb{K}))$ and $\delta_n(v)$ are the same. It is clear, that the map δ_n induces homomorphism of $DD(n, \mathbb{K})$ onto the double directed graph $DA(n, \mathbb{K})$ for the simple graph $A(n, \mathbb{K})$. We will use the same symbol δ_n for the induced homomorphism. Let us denote by $DA(n, M, \mathbb{K})$ the homomorphic image of $DA(M, \mathbb{K})$ under the map δ_n.

Theorem 5.3.2. *Let $\mathbb{K}$ be a finite commutative ring and M, $|M|$ be the multiplicative subset, then graphs $DCD(n, M, \mathbb{K})$ of $DD(n, M, \mathbb{K})$ form families of directed graphs of large girth. Well defined projective limits of this graphs are infinite directed trees $DCD(M, \mathbb{K})$.*

5.4. Directed graphs of generalised polygons

Let $\mathcal{F} = \{(p, l)|p \in P, l \in L, pIl\}$ be the totality of flags for the tactical configuration with partition sets P (point set) and L (line set) and incidence relation I. We define the following irreflexive binary relation ϕ on the set $\mathcal{F}$:

$$((l_1, p_1), (l_2, p_2)) \in \phi \text{ if and only if } p_1 I l_2,\ p_1 \neq p_2 \text{ and} l_1 \neq l_2.$$

Let $\mathcal{F}(I)$ be the binary relation graph corresponding to ϕ. The order of $\mathcal{F}(I)$ is $|P|(s + 1)$ (or $|L|(t + 1)$ We refer to it as *directed flag graph* of I.

Lemma 5.4.1. *Let (P, L, I) be a tactical configuration with bidegrees $s + 1$ and $t + 1$ of girth $g \geq 4k$. Then the girth indicator of directed graph $\mathcal{F}(I)$ with the output and input degree st is $> k$.*

Proof. The absence of even cycles C_{2s}, $2 < s < 2k - 2$ in the graph I insure the absence of commutative diagrams $O_{r,s}$, $1 \leq s \leq r \leq k$ in the directed graph $\mathcal{F}(I)$. □

Let (P, L, I) be the incidence structure corresponding to regular tactical configuration of order t.

Let $\mathcal{F}_1 = \{(l, p)|l \in L, p \in P, lIp\}$ and $\mathcal{F}_2 = \{[l, p]|l \in L, p \in P, lIp\}$ be two copies of the totality of flags for (P, L, I). Brackets and parenthesis allow us to distinguish elements from $\mathcal{F}_1$ and $\mathcal{F}_2$. Let $D\mathcal{F}(I)$ be the *directed graph* (*double directed flag graph*) on the disjoint union of $\mathcal{F}_1$ with $\mathcal{F}_2$ defined by the following rules

$(l_1, p_1) \to [l_2, p_2]$ if and only if $p_1 = p_2$ and $l_1 \neq l_2$,
$[l_2, p_2] \to (l_1, p_1)$ if and only if $l_1 = l_2$ and $p_1 \neq p_2$.

Lemma 5.4.2. *Let (P, L, I) be a regular tactical configuration of order s with the girth $g \geq 2m$. Then the girth indicator of double directed graph $D\mathcal{F}(I)$ with the output and input degree s is $> m$.*

Proof. The absence of even cycles C_{2s}, $2 < s < m-1$ in the bipartite graph I insure the absence of commutative diagrams $O_{r,s}$, $1 \leq s \leq r \leq m$ in the double directed graph $D\mathcal{F}(I)$.

□

Generalized m-gons $GP_m(r, s)$ of order (r, s) were defined by J. Tits in 1959 (see [140], [141]and survey [139]) as tactical configurations of order (s, t) of girth $2m$ and diameter m.

According to well known Feit-Higman theorem a finite generalized m-gon of order (s, t) has $m \in \{3, 4, 6, 8, 12\}$ unless $s = t = 1$.

The known examples of generalized m-gons of bidegrees ≥ 3 and $m \in \{3, 4, 6, 8\}$ include rank 2 incidence graphs of finite simple groups of Lie type (see [21]). The regular incidence structures are

(i) $I_{1,1}(3, q)$ for $m = 3$ (groups $A_2(q)$),
(ii) $I_{1,1}(4, q)$, $m = 4$ (groups $B_2(q)$),
(iii) $I_{1,1}(6, q)$, $m = 6$ (group $G_2(q)$).

In all such cases $s = t = q$, where q is prime power.

The biregular but not regular generalized m-gons have parameters $s = q^\alpha$, $t = q^\beta$, where q is a prime power. The list is below:

(i) $I_{2,1}(4, q)$, $s = q^2, t = q$, q is arbitrary large prime power for $m = 4$;
(ii) $I_{3,2}(6, q)$, $s = q^3, t = q^2$, where $q = 3^{2k+1}$, $k > 1$ for $m = 6$;
(iii) $I_{2,1}(8, q)$, $s = q^2, t = q$, $q = 2^{2k+1}$ for $m = 8$.

For each triple of parameters (m, s, t) listed above there is an edge transitive generalized m-gon of order (s, t) related to certain finite rank 2 simple group of Lie type. In the cases of $m = 3$ (*projective planes*) and $m = 4$ (*generalized quadrangles*) some infinite families of graphs without edge transitive automorphism group are known.

The following 2 lemmas can be obtained immediately from the axioms of generalized polygon.

Lemma 5.4.3. *Let (P, L, I) be the generalized $2k$-gon of order (r, s). Then*

$$|P| = \sum_{t=0,k-1} (r^t s^t + r^{t+1} s^t),$$
$$|L| = \sum_{t=0,k-1} (s^t r^t + s^{t+1} r^s).$$

Lemma 5.4.4. *Let (P, L, I) be regular generalized m-gon of degree $q+1$. Then*

$$|P| = |L| = 1 + q + \cdots + q^{m-1}.$$

Corollary 5.4.5. *For each $m = 3, 4, 6$ and prime p the family $F_m(q)$, $q = p^n$, $n = 1, \ldots$ of edge transitive polygons is an algebraic family over F_p of cages of girth $2m$ of degree $q+1$ with the order on the Tutte's lower bound.*

Let (P, L, I) be generalized m-gon of order (s, t), $s \geq 2$, $t \geq 2$ and $e = \{p, l\}$, ($p \in P$, $l \in L$, pIl) be chosen edge of this simple graph.

Let $\mathrm{S}_e = \mathrm{Sch}_e(I)$ be the restriction of incidence relation I onto $P' \cup L'$ where P' (L') is the totality of points (lines) at maximal distance from p (l, respectively). It can be shown that (P', L', S_e) is a tactical configuration of degree $(s-1, t-1)$. Let us refer to (P', L', S_e) as *Schubert graph*. If the generalized polygon is edge-transitive its Schubert graph is unique up to isomorphism. In this case Schubert graph corresponds to the restriction of incidence relation onto the union of two of the largest "large Schubert cells", i.e. orbits of standard Borel subgroups of the highest dimension.

The following statement immediately follows from the definitions of graphs $S_m(q)$.

Proposition 5.4.6. *For each $S_m(p)$ $m = 3, 4, 6$ and prime p the family of Schubert graphs $S_m(p)$ of regular generalized m-gons $F_m(q)$ is algebraic over F_p family of asymptotical cages of even girth with the order $2q^{m-1}$ and degree q.*

The extremal properties of finite generalized polygons, their Schubert graphs and some of their induced subgraphs have been considered in [167].

Remark 5.4.7. The girth of $S_m(q)$ is $2m$ for "sufficiently large" parameter q.

Let (P, L, I) be a regular tactical configuration of order (t, t). The *double configuration* $I' = DT(I)$ is the incidence graph of the following incidence structure (P', L', I') : $P' = \mathcal{F}(I) = \{(p, l) | p \in P, l \in L, pIl\}$, $L' = P \cup L$, $f = (p, l)Ix$, $x \in L'$ if $p = x$ or $l = x$. It is clear that the order of tactical configuration I' is $(1, t)$.

If (P, L, I) is a generalized m-gon, then (P', L', I') is a generalized $2m$-gon.

Proposition 5.4.8.

(i) *If the girth of regular tactical configuration (P, L, I) of degree $s+1$ is $2t$, then the girth of $DT(I)$ is $4t$. The order of $DT(I)$ is $(s, 1)$.*

(ii) *Let (P, L, I) be regular generalized m-gon, then $DT(I)$ is generalized $2m$-gon.*

Proof. It is clear that cycle C_l of length $2l$ in the simple graph $DT(I)$ corresponds to the cycle C_l of original tactical configuration. Notice that bipartite graphs does not contain odd cycles. So equality $g(I) = 2t$ implies $g(DT(I)) = 4t$.

Let I be generalised m-gon. Then the girth and diameter of m-gon are $g(I) = 2m$ and $d(I) = m$ respectively. As it follows from the definition the diameter of $DT(I)$ is twice large than $d(I)$. So the girth and diameter of $DT(I)$ are $4m$ and $2m$, respectively.

□

Corollary 5.4.9. *The configurations $DT(I) = I^2(m, q)$ for known regular m-gons, $m = 3, 4, 6$ of degree $q + 1$, q is a prime power, are generalized $2m$-gons of order $(1, q)$.*

Theorem 5.4.10. (i) *Let $I_{s,t}(m, q)$, $m \geq 4$ be the incidence relation of one of the known edge transitive m-gons defined over the field F_q, $q = p^n$, where p is a prime number. Then for each tuple (m, s, t, p) the family of directed flag-graphs $F^n = F^n(m, s, t, p)$, $n = 1, \dots$ for generalized m-gon of order (q^s, q^t) is an algebraic over F_p family of asymptotic cages of odd girth. The girth indicator of each graph from the family is $m/2 + 1$ and the girth is $m + 1$ $(5, 7, 9)$.*

(ii) *Let $S_{s,t}(m, q)$, $m \geq 4$ be the Schubert graph of the incidence relation $I_{s.t}(m, q)$ of one of the known edge transitive m-gons defined over the field F_q, $q = p^n$, where p is a prime number. Then for each tuple (m, s, t, p) the family of directed flag-graphs $SF^n(m, s, t, p)$ for $S_{s.t}(m, q)$ is an algebraic family of asymptotic cages of odd girth defined over F_p. The girth indicator of graph from the family is $m/2 + 1$ and the girth is $m + 1$ if parameter q is sufficiently large.*

(iii) *Let $I_{1,1}(m, q)$ be the incidence relation of one of the known edge transitive regular m-gons defined over the field F_q, $q = p^n$, where p is a prime number. Then for each pair (m, p) the family $DF(m, p)$ of double flag graphs $DF(m, i) = DF(I_{1,1}(m, p^i))$, $i = 1, \dots$ is an algebraic over family of directed asymptotic cages of even girth defined over $\mathbb{F}_p$. The girth indicator of each $DF(m, i)$ is $m + 1$ and the girth is $2m + 2$ (possible values are $(8, 10.14)$). Double flag graphs of Schubert subgraphs for $I_{1,1}(m, p^n)$, $n = 1, \dots$ form the family of asymptotical directed cages as well.*

(iv) *Let $I^2(m, q)$, $m \geq 3$ be the incidence relation of double tactical configuration of regular generalized m-gon defined over $\mathbb{F}_q$, $q = p^n$, where p is a prime. Then for each pair (m, p) the family $F(m, p)$ of directed flag-graphs $F^n(m, p)$ of $I^2(m, p^n)$, $n = 1, \dots$ is an algebraic family of directed graphs of large girth over $\mathbb{F}_p$. The girth indicator of each graph is $m + 1$ and girth is $2m + 1$ (possible values are 7, 9, 13).*

Proof. As it follows from lemma 11 the girth indicator of each directed graph F^n is $> m/2$. The existence of cycles C_{2m} in the corresponding generalised m-gon leads to the existence of commutative diagrams $O_{m/2+1,m}$. So the girth indicator of each graph is $m/2+1$ and the girth is $2(m/2)+1$.

The order of each directed graph F^n coinsides with the cardinality of the flag set of the correspondent generalised m-gon or its size and can be given by polynomial expession $f(q)$ in single variable q (see lemmas 13 and 14 for the close formulae for the order). The degree of the balanced graph F^n is q^{s+t}. The highest term for the polynomial $F(q)$ is $q^{(s+t)m/2}$.

So for each prime p the family F^n is the family of asymptotical cages of odd girth and we proved statement (i) of the theorem.

The Schubert subgraphs SF^n is the induced subgraps of F^n. So for the the girth indicator and the girth of the Schubert subgraph we have $\mathrm{Dind}(SF^n) \geq \mathrm{Dind}(F^n) \geq m/2+1$ and $g(SF^n) \geq g(F^n) \geq m+1$. Notice that the order of SF^n is exactly $q^{(s+t)m/2}$. The assumption that $\mathrm{Dind}(SF^n) > \mathrm{Dind}(F^n) \geq m/2+1$ for sufficiently large q contrudict to previously proven statement (i) (or established upper bound for directed cages). So graphs (SF^n), $n = 1, \ldots$ form the family of asymptotical cages and we proved (ii).

The graphs $DF(m,i)$. $i = 1, \ldots$ are graphs of order $2f(q)$ where $f(q)$ is the order of corresponding directed flag graph F^i. As it follows from lemma 12 the girth indicator of each double directed graph $DF(m,i)$ is $> m$. The bipartite structure of the graph corresponding to the partition which formed by 2 copies of $F(I)$ insures the absence of commutative diagrams $O_{m+1,m}$ The existence of cycles C_{2m} in the corresponding generalised m-gon leads to the existence of commutative diagrams $O_{m+1,m+1}$. So the girth indicator of each graph is $m+1$ and the girth is $2m+2$. The highest term of polyniomial expression $2f(q)$ is $2q^m$. So the graphs form the family of asymptotical directed cages. Double flag graphs of Schubert subgraphs for $I_{1.1}(m,p^n)$, $n = 1, \ldots$ have order $2q^m$, $q = p^n$. So if n is sufficiently the girth indicator and girth of such graph is $m+1$ and $2m+2$, respectively. Thus we show that they form the family of asymptotical cages as well. So we proved point (iii).

Acording to proposition 17 the double tactical configuration $I^2(m,q)$, $q = p^n$, p is prime is generalised $2m$-gon. Similarly to part (i) of the proof we can show that the girth indicator of directed flag graph of $I^2(m,q)$ is $m+1$ and its girth is $2m+1$ (7, 9, 13). The order $v = v^n(m,p)$ of the graph $F^n(m,p)$ can be computed as the size of generalised $2m$-gon of order $(q,1)$. It is polynomial expression in variable q of degree m. So these graphs form the family of graphs of large girth.

□

5.5. Construction of groups of cubical transformations from special directed graphs

Let $\mathbb{K}$ be a commutative ring,$\mathbb{K}^n$ is n-dimensional module.

Cremona group $C(\mathbb{K}^n)$ is a totality of all bijective polynomial maps f of $\mathbb{K}^n$ onto itself such that the inverse map f^{-1} is also a polynomial transformation, We introduce *infinite-dimensional Cremona group* denoted by $C(\mathbb{K}^\infty$ as natural projective limit $C(\mathbb{K}^n)$, where n is going to infinity .

Let us consider double directed graph $DD(n,\mathbb{K})$ for the bipartite graph $D(n,\mathbb{K})$ and infinite double directed flag graph $DD(\mathbb{K})$ for $D(\mathbb{K})$ defined over the commutative ring $\mathbb{K}$.

Let $N_{DD,\alpha,\beta,n+1}(v)$ ($N_{DD,\alpha,\beta}(v)$), be the operator of taking the neighbor alongside the output arrows of colours $\alpha,\beta \in \mathbb{K}-\{0\}$ of vertex $v \in \mathcal{F}_1 \cup \mathcal{F}_2$ in graph $DD(n,\mathbb{K})$ ($DD(\mathbb{K})$),respectively, by the following rule
(i) if $v = \langle (p),[l]\rangle \in F_1$ then

$$N_{DD,\alpha,\beta,n}(v) = v' = [[l],(p')] \in \mathcal{F}_2 \ (N_{DD,\alpha,\beta}(v) = v' = [[l],(p')] \in \mathcal{F}_2),$$

where the colour of v' is $\alpha = p'_{1,0} - p_{1,0}$.
(ii) if $v = [[l],(p)] \in \mathcal{F}_2$ then

$$N_{DD,\alpha,\beta,n+1}(v) = v' = \left\langle (p),[l']\right\rangle \in \mathcal{F}_1 \ (N_{DD,\alpha,\beta}(v) = v' = \left\langle (p),[l']\right\rangle \in \mathcal{F}_1),$$

where the colour of v' is $\beta = l'_{1,0} - l_{1,0}$.
Let us consider the elements

$$Z_{DD,\alpha,\beta,n+1} = N_{DD,\alpha,0,n+1}N_{DD,0,\beta,n+1} \ \ (Z_{DD,\alpha,\beta} = N_{DD,\alpha,0}N_{DD,0,\beta}).$$

It moves $v \in \mathcal{F}_1$ into $v' \in \mathcal{F}_1$ at distance two from v and fixes each $u \in \mathcal{F}_2$. Notice that $Z_{DD,\alpha,\beta,n+1}Z_{DD,-\alpha,-\beta,n+1}$ ($Z_{DD,\alpha,\beta}Z_{DD,-\alpha,-\beta}$) is an identity map.

We consider the group $G_{DD}(n,\mathbb{K})$ ($G_{DD}(\mathbb{K})$), generated by all transformations $Z_{DD,\alpha,\beta,n+1}$ ($Z_{DD,\alpha,\beta}$) for nonzero $\alpha,\beta \in \mathbb{K}$ acting on the variety $\mathcal{F}_1 = \mathbb{K}^{n+1}$ ($\mathbb{K}^\infty$), respectively.

Theorem 5.5.1. *Each element subgroups $G_{DD}(n,\mathbb{K})$ of Cremona group $C(\mathbb{K}^{n+1})$ is a cubical multivariable map from $\mathbb{K}^{n+1}$ to $\mathbb{K}^{n+1}$.*

Proof. In the first step we connect point with line to get two sets of vertices of new graph:

$$\mathcal{F} = \{\langle (p),[l]\rangle \mid (p)I[l]\} \quad \cong \mathbb{K}^{n+1}$$
$$\mathcal{F}' = \{\{[l],(p)\} \mid [l]I(p)\} \quad \cong \mathbb{K}^{n+1}.$$

Now we define the following relation between vertices of the new graph:

$$\langle (p),[l]\rangle R\{[l'],(p')\} \ \Leftrightarrow \ [l] = [l'] \ \ \& \ \ p_1 - p'_1 \in \mathbb{K}$$

$$\{[l^{'}],(p^{'})\}R\langle(p),[l]\rangle \quad \Leftrightarrow \quad (p^{'})=(p) \ \ \& \ \ l_1^{'}-l_1\in\mathbb{K}$$

Our key will be $\alpha_1,\alpha_2,\ldots,\alpha_n$, such that $\alpha_i\in Reg\mathbb{K}$.

As a first vertex we take

$$\{[l],(p)\}=(l_1,l_{1,1},l_{1,2},\ldots,l_{i,j},p_1)$$

(our variables) . Using the above relation we get get next vertex:

$$\langle(p)^{(1)},[l]^{(2)}\rangle=(p_1,p_{1,1}^{(1)},\ldots,p_{i,j}^{(1)},l_1+\alpha_1)$$

with coefficients of degree 2 or 3, where

$$\begin{array}{ll}
p_{1,1}^{(1)}=l_{1,1}-l_1p_1, & deg=2\\
p_{1,2}^{(1)}=l_{1,2}-l_{1,1}p_1 & deg=2\\
p_{2,1}^{(1)}=l_{2,1}-l_1(l_{1,1}-l_1p_1) & deg=3\\
p_{i,i}^{'(1)}=l_{i,i}^{'}-p_1l_{i,i-1} & deg=2\\
p_{i,i+1}^{(1)}=l_{i,i+1}-p_1l_{i,i} & deg=2\\
p_{i,i}^{(1)}=l_{i,i}-l_1(l_{i-1,i}-p_1l_{i-1,i-1}) & deg=3\\
p_{i+1,i}^{(1)}=l_{i+1,i}-l_1(l_{i,i}^{'}-p_1l_{i,i-1}) & deg=3
\end{array}$$

Similarly we get third vertex:

$$\{[l]^{(2)},(p)^{(3)}\}=(l_1+\alpha_1,l_{1,1},\ldots,l_{i,j},p_1+\alpha_2)$$

also with coefficients of degree 2 or 3, where

$$\begin{array}{ll}
l_{1,1}^{(2)}=l_{1,1}-l_1p_1, & deg=2\\
l_{1,2}^{(2)}=l_{1,2}-l_{1,1}p_1 & deg=2\\
l_{2,1}^{(2)}=l_{2,1}-l_1(l_{1,1}-l_1p_1) & deg=2\\
l_{i,i}^{(2)}=l_{i,i}+\alpha_1p_{i-1,i}^{(1)} & deg=2\\
l_{i+1,i}^{(2)}=l_{i+1,i}+\alpha_1p_{i,i}^{'(1)} & deg=2\\
l_{i,i}^{'(2)}=l_{i,i}^{'}+\alpha_1p_1p_{i-1,i-1}^{'(1)} & deg=3\\
l_{i,i+1}^{(2)}=l_{i,i+1}+\alpha_1p_1p_{i-1,i}^{(1)} & deg=3
\end{array}$$

Let us represent:

$$p_1^{(2k-1)}=p_1+\alpha_2+\alpha_4+\ldots+\alpha_{(2k-2)}=p_1^{(2k-3)}+\alpha_{(2k-2)}$$

$$l_1^{(2k)}=l_1+\alpha_1+\alpha_3+\ldots+\alpha_{(2k-1)}=l_1^{(2k-2)}+\alpha_{(2k-1)}$$

Assume that the following vertices:

$$\langle(p)^{(2k-1)},[l]^{(2k)}\rangle=(p_1^{(2k-1)},p_{1,1}^{(2k-1)},\ldots,p_{i,j}^{(2k-1)},l_1^{(2k)})$$

$$\{[l]^{(2k)},(p)^{(2k+1)}\}=(l_1^{(2k)},l_{1,1}^{(2k)},\dots,l_{i,j}^{(2k)},p_1^{(2k+1)})$$

have degrees:

$$\deg p_{i,j}^{(2k-1)}(l_1,l_2,\dots,l_k,p_1)=\begin{cases}2, & (i,j)=(i,i)^{'}\ \text{ or }\ (i,j)=(i,i+1),\\ 3, & (i,j)=(i,i)\ \text{ or }\ (i,j)=(i+1,i)\end{cases}$$

$$\deg l_{i,j}^{(2k)}(l_1,l_2,\dots,l_k,p_1)=\begin{cases}3, & (i,j)=(i,i)^{'}\ \text{ or }\ (i,j)=(i,i+1),\\ 2, & (i,j)=(i,i)\ \text{ or }\ (i,j)=(i+1,i)\end{cases}$$

Now we would like to find out degrees of polynomials of the vertices $\langle(p)^{(2k+1)},[l]^{(2k+2)}\rangle$ and $\{[l]^{(2k+2)},(p)^{(2k+3)}\}$.

We have the components of the vertices with corresponding degrees: :

$$\begin{array}{ll}
p_{i,i}^{'(2k+1)}=p_{i,i}^{'(2k-1)}-\alpha_{2k}l_{i,i-1}^{(2k)} & deg=2\\
p_{i,i+1}^{(2k+1)}=p_{i,i+1}^{(2k-1)}-\alpha_{2k}l_{i,i}^{(2k)} & deg=2\\
p_{i,i}^{(2k+1)}=p_{i,i}^{(2k-1)}+\alpha_{2k}l_1^{(2k)}l_{i-1,i-1})^{(2k)} & deg=3\\
p_{i+1,i}^{(2k+1)}=p_{i+1,i}^{(2k-1)}+\alpha_{2k}l_1^{(2k)}l_{i,i-1}^{(2k)} & deg=3
\end{array}$$

and

$$\begin{array}{ll}
l_{i,i}^{(2k+2)}=l_{i,i}^{(2k)}+\alpha_{2k+1}p_{i-1,i}^{(2k+1)} & deg=2\\
l_{i+1,i}^{(2+2)}=l_{i+1,i}^{(2k)}+\alpha_{2k+1}p_{i,i}^{'(2k+1)} & deg=2\\
l_{i,i}^{'(2+2)}=l_{i,i}^{'(2k)}+\alpha_{2k+1}p_1^{(2k+1)}p_{i-1,i-1}^{'(2k+1)} & deg=3\\
l_{i,i+1}^{(2+2)}=l_{i,i+1}^{(2k)}+\alpha_{2k+1}p_1^{(2k+1)}p_{i-1,i}^{(2k+1)} & deg=3
\end{array}$$

Hence using the induction we got:

$$\deg p_{i,j}^{(2k+1)}(l_1,l_2,\dots,l_k,p_1)=\begin{cases}2, & (i,j)=(i,i)^{'}\ \text{ or }\ (i,j)=(i,i+1),\\ 3, & (i,j)=(i,i)\ \text{ or }\ (i,j)=(i+1,i)\end{cases}$$

$$\deg l_{i,j}^{(2k+2)}(l_1,l_2,\dots,l_k,p_1)=\begin{cases}3, & (i,j)=(i,i)^{'}\ \text{ or }\ (i,j)=(i,i+1),\\ 2, & (i,j)=(i,i)\ \text{ or }\ (i,j)=(i+1,i)\end{cases}$$

□

Remark 5.5.2. We may change the group $G_{DD}(n,\mathbb{K})$ for its conjugation $\tau^{-1}G_{DD}(n,\mathbb{K})\tau$, where τ is an affine invertible transformation of $\mathbb{K}^{n+1}$.

Let $\alpha_1,\alpha_2,\dots,\alpha_{2m}$ is a string of nonzero ring elements. We define the map $F_{DD,\alpha_1,\alpha_2,\dots,\alpha_{2m},n+1}$ as the composition of transformations $Z_{DD,\alpha_1,\alpha_2,n+1}$, $Z_{DD,\alpha_3,\alpha_4,n+1}$, …, $Z_{DD,\alpha_{2m-1},\alpha_{2m},n+1}$ acting on the free module $\mathbb{K}^{n+1}$. Symbol $F_{DD,\alpha_1,\alpha_2,\dots,\alpha_{2m}}$ as the composition of transformations Z_{DD,α_1,α_2}, Z_{DD,α_3,α_4}, …, $Z_{DD,\alpha_{2m-1},\alpha_{2m}}$ from the group $G_{DD}(\mathbb{K})$.

We refer to sequence $\alpha_1, \alpha_2, \ldots, \alpha_{2m}$ as *multipicative string* if product $d = \alpha_1\alpha_2 \ldots \alpha_{2m}$ is nonzero ring element.

We will use term *irreversible string* if d is antinilpotent ring element, i. e. $d^x \neq 0$ for each positive integer x.

Theorem 5.5.3. (i) *Let $\alpha_1, \alpha_2, \ldots, \alpha_{2m}$ is irreversible string then the order of $F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m}}$ is infinity.*

(ii) *Let $2m < n+5$, then transformation $F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m},n+1}$ corresponding to multiplicative string $\alpha_1, \alpha_2, \ldots, \alpha_{2m}$ does not have fixed points on $\mathbb{K}^{n+1}$.*

(iii) *Let $4m < n+5$ and $\alpha_1, \alpha_2, \ldots, \alpha_{2m}$ is multiplicative string, then for each $x \in \mathbb{K}^{n+1}$ the inequality*

$$F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m},n+1}(x) \neq F_{DD,\beta_1,\beta_2,\ldots,\beta_{2m},n+1}(x)$$

holds for each string $\beta_1, \beta_2, \ldots, \beta_{2m}$ from $(\mathbb{K} - \{0\})^{2m}$.

Remark 5.5.4. Properties (i)- (iii) formulated in previous statements hold for the conjugates

$$H^{-1}F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m}}H, \;\; H \in C(\mathbb{K}^\infty)$$

and

$$H_{n+1}^{-1}F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m},n+1}H_{n+1}, \quad H_{n+1} \in C(\mathbb{K}^{n+1}),$$

of transformations $F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m}}$ and $F_{DD,\alpha_1,\alpha_2,\ldots,\alpha_{2m},n+1}$, respectively.

Chapter 6

On multivariate cryptography, algebraic groups and graphs

6.1. Some historical remarks on multivariate cryptography

Multivariate cryptography in the narrow sense is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over finite fields. In certain cases these polynomials could be defined over both a ground and an extension field. If the polynomials have the degree two, we talk about multivariate quadratics. Solving systems of multivariate polynomial equations is proven to be NP-Hard or NP-Complete. That is why these schemes are often considered to be good candidates for post-quantum cryptography, once quantum computers can break the current schemes based on difficult problems of Number Theory.

We are given a shorter version of historical survey given in [113]. Multivariate cryptography is quite popular nowadays because it can be a possible option applicable to both conventional and quantum computers (see [35]). In multivariate cryptography the public key cryptosystems are based on the problem of solving system of nonlinear equations which complexity we discuss above. Imai and Matsumoto (1988, see [96]) have been proposed, the first cryptosystem (MIC) based on the map from Cremona group over the finite field of characteristic 2. The MIC* cryptosystem was based on the idea of hiding a monomial $x^{2^l}+1$ by left and right shifts by two invertible affine transformations (see [75]). This cryptosystem was rather efficient for implementations. Unfortunately this cryptosystem was broken by Patarin (see [124], 1995). Next year [108] J. Patarin proposed a generalization of MIC cryptosystem called HFE. In attempt to improve security level of HFE the proposed secret key computation was more sophisticated in comparison with MIC cryptosystem. Unfortunately the efficient cryptanalisis for the primitive instance of HFE was broken in 1999 (see [68]). The attack uses a simple fact that every homogeneous quadratic multivariate polynomial has a matrix representation. Using this representation a highly over defined system of equations can be obtained which can be solved by a new technique called relinearization [68]. Other efficient attacks on the HFE scheme can be found in [26], [41], [28]. J. Patarin [109] investigated whether it is possible to repair MIC with the same kind of easy secret key computations. He designed some cryptosystems known as Dragons with multivariate polynomials of total degree 3 or 4 in public key (instead of 2) with enhanced security and with efficiency comparable to MIC. In Dragon cryptosystems the public key was of mixed type of total degree 3 which is quadratic in plaintext variables and linear in ciphertext variables. However Patarin found [109] that Dragon scheme with one hidden monomial is insecure. A public key scheme based on the composition of tame transformation methods (TTM) was proposed in 1999 (see [97]). Next year this scheme has been broken (see [27], where the cryptanalysis is reduced to an instance of the Min-Rank problem that can

be solved within a reasonable time. In 2004 Ding [34] proposed a perturbed variant of MIC* cryptosystem called PMI. The PMI system attempts to increase the complexity of the secret key computations in order to increase security, using a system of r arbitrary quadratic equations over $\mathbb{F}_q$ with the assumption that $r << n$, where n is the bitsize. The PMI Cryptosystem was broken by Fouque, Granboulan and Stern [42]. The trick of the attack on PMI is to use differential cryptanalysis to reduce the PMI system to the MIC* system. A cryptosystem called Medium Field Equation [86] was proposed in 2006 but it also was broken one year later of appearance (Ding, [36] using high order linearization equation attack.

Despite mention above sequence of unsuccessful attempts to construct secure and efficient multivariable cryptosystems public key development based on symbolic computation became a popular area of research [35]. Rather informative introduction to hidden monomial cryptosystems can be found in reference [75]. An example of cryptosystem which are still under the investigation of cryptoanalitics is given in [113].

6.2. On multivariate cryptography over commutative rings

We define *multivariable cryptography* as studies of cryptosystems based on special regular automorphism f of algebraic variety $M_n(\mathbb{K})$ of dimension n in a sense of Zarisski topology over finite commutative ring $\mathbb{K}$. An example of algebraic variety is a free module $\mathbb{K}^n$ which is simply a Cartesian product of n copies of $\mathbb{K}^n$ into iself. Regular automorphism is a bijective polynomial map of $M_n(\mathbb{K})$ onto itself such that f^{-1} is also a polynomial map.

Elements of $\mathbb{K}^n$ can be identified with strings $(x_1, x_2, \ldots, x_n)$ in *alphabet* $\mathbb{K}$, nonlinear map f of restricted degree d can be used as a *public rule* if the key holder (Alice) knows the secret decomposition of f into composition of special maps $f_1, f_2, \ldots, f_s$ with known inverse maps ${f_i}^{-1}$. So she can decrypt by consecutive application of ${f_s}^{-1}, f_{s-1}^{-1}, \ldots, {f_1}^{-1}$. Of course $\mathbb{K}^n$ can be changed for the family of varieties $M_n(\mathbb{K})$, $n = 1, 2, \ldots$, the commutative ring can be treated as an alphabet, element $v \in M_n(\mathbb{K})$ as a *"potentially infinite" plaintext*, parameter n (dimension) as a *measurement of size* of v.

The complexity of the best general algorithms for the solution of nonlinear system of equation of kind $f(x) = y$, $x, y \in \mathbb{K}^n$ equals $d^{0(n)}$ (see recent paper [20]). One can use Gröbner basis, Gauss elimination method or alternative options for the investigation of the system. Of course, one can write simple nonlinear equations which are easy to solve. So the system of nonlinear equations has to be tested on "pseudorandomness" and the map f has to be of large order. Notice, that one of the first attempts to create workable multivariate cryptosystem was proposed by Imai and Matsumoto.

They used finite field of characteristic 2 and its extension, f has a decomposition $f_1 f_2 f_3$, where f_1 and f_2 are affine maps (of degree 1) and f_2 is a Frobenius automorphism. Cryptanalysis for the scheme the reader can find in [76]. We have to notice that the failure of this cryptosystem is not a surprise for specialists in algebra. Despite its formal quadratic appearance Frobenius automorphism is quite close to linear maps (in his famous book [31] J. Dieudonne uses term 3/2 linear map for such automorphism). One of the new directions in multivariate cryptography is the use of tools outside commutative algebra such as dynamical systems or algebraic automata theory for the creation of nonlinear maps of pseudorandom nature.

The goal of the chapter is a discussion of new cryptosystems in the area of Multivariate Cryptography, which have some potential to be used in the era of Postquantum Informatics. The Quantum Computer is a special random computational machine. The cryptographical algorithm have to produce a ciphertext which is "a seeming chaos". So The Theory of Continuous Dynamical Chaos and its discrete approximation can be used in multivariate cryptography.

6.3. On the discrete logarithm problem in Cremona group

Group theoretical discrete logarithm problem (DLP is a generalisation of classical DLP known in a Number Theory used in a well known Diffe-Hellman protocol ([32], [74]), ElGamal method and other cryptosystems (see [75]).

In the case of subgroups of Cremona group DLP is closely connected to the following classical difficult mathematical problems:

(1) solving the system of nonlinear polynomial equations over finite fields and rings
(2) problem of finding the inverse map of bijective polynomial multivariable map.

Any finite abstract group can be considered as a subgroup of certain Cremona group. It means that complexity of DLP depends heavily on the choice of a base. Generation of a good "pseudorandom" base guarantees the high complexity of (1) and (2) and security of related proposed cryptographical security tools.

Let us discuss the known results on the oldest classical problem (1) of investigation of the system of nonlinear equations

$$g(x) = b.$$

This problem is investigated for centuries and modern research on this topic is very interesting but in principal the complexity of the best known

algorithm is practically same with those given by the famous Gauss elimination method. If the degree of g is d then the best known general algorithm has complexity $d^{O(n^2)}$. In the case of some special restrictions on g solution can be found for $d^{O(n)}$. It is clear, that if g^{-1} is known, then $x = g^{-1}b$. So the problem (2) of finding the inverse map of bijective polynomial multivariable map is more sophisticated. In fact it is much harder algebraic problem in comparison with the solving of non linear equation. Traditionally specialists use $d^{O(n)}$ as a lower bound for the complexity of both problems.

The efficient general algorithm of finding g^{-1} is known only in the case when g is linear map. There is an amassing gap between linearity and nonlinearity, which can be used to guarantee the security of cryptographical tools. Of course specialists have to use g which is close to pseudorandom map.

The old problem DLP for the group $\mathbb{F}_p^*$, where prime p is "sufficienly large", has been used in a well known Diffie-Hellman algorithms for the key exchange and several public-key cryptosystems, including the ElGamal system and DSS. Recall that multiplicative group $\mathbb{F}_p^*$ is isomorphic to additive group $\mathbb{Z}_{p-1}$, for which DLP is equivalent to the finding the solution of linear equation. This fact demonstrates that group theoretical DLP, in fact, depends not only on chosen abstract finite group, but also on the ways of its representations. Both groups $\mathbb{F}_p^*$ and $\mathbb{Z}_{p-1}$ are isomorphic subgroups of symmetric group S_p of order p!. They are isomorphic but not similar (groups are not conjugated by some permutation from S_p). So they are distinct transformation groups.

DLP problem can be considered formally for any finite transformation group. In fact even the case of group $\mathbb{Z}_n^*$, where n is a composite number, is not investigated properly. We can consider the following natural generalisations of DLP for $\mathbb{F}_p^*$.

It is well known that each permutation from S_p can be written in the form of polynomial transformation $x \to f(x)$. We can identify $\mathbb{F}_p^*$ with totality of maps $x \to ax$ of degree 1, where $a \neq 0$.

The simplest generalisation DLP can be obtained by the change of the pair $\mathbb{F}_p^*$, S_p on the pair of groups $GL_n(\mathbb{F}_p)$ (general linear group over $\mathbb{F}_p$) and symmetric group S_{p^n}. Recall that $GL_n(\mathbb{F}_p)$ consists of all bijective linear transformations $x \to xA$ of the vector space $\mathbb{F}_p^n$, where A is non singular quadratic matrix with entries from $\mathbb{F}_p$. Notice, that each permutation from S_{p^n} can be written in the form $x \to F(x)$, where F is a bijective polynomial map from the vector space $\mathbb{F}_p^n$ onto itself. Similarly to the case $n = 1$ we can identify $GL_n(\mathbb{F}_p)$ with totality of invertible polynomial maps $x \to xA$ of degree 1. It is clear that $GL_1(\mathbb{F}_p) = \mathbb{F}_p^*$ and we have natural generalisation of classical DLP.

The natural second step of generalisation DLP is the change of the field

$\mathbb{F}_p$ on the general finite commutative ring $\mathbb{K}$, vector space $\mathbb{F}_p^n$ onto free module $\mathbb{K}^n$, symmetric group S_{p^n} onto Cremona group $C(\mathbb{K}^n)$ of all bijective polynomial maps F of $\mathbb{K}^n$ onto $\mathbb{K}^n$ such that the inverse map F^{-1} is also a polynomial one.

The DLP problem for the cyclic group generated by nonlinear transformation g of order t from Cremona group $C(\mathbb{K}^n)$, i.e. problem of solving $g^k = h$ is more difficult than the problem of finding h^{-1}. If x is known together with t, then our equation can be written in the form $g^{t-k} = h^{-1}$ and we are computing the inverse map for b, last computation generally requires $d^{O(n^2)}$ operations, where d is the degree of polynomial map g.

Cremona group $C(\mathbb{K}^n)$ is an important object of algebraic geometry. There are many open questions connected with cryptographical aspects about this group. For instance, let $AGL_n(\mathbb{K})$ be the totality of all invertible affine maps of $\mathbb{K}^n$ onto itself, i.e. maps $x \to xA + \mathrm{b}$, where x and b are row vectors from V and A is invertible square matrix with entries from $\mathbb{K}$. Describe subgroups $\mathbb{X}$ of $C(\mathbb{K}^n)$ containing $AGL_n(\mathbb{K})$ as a subgroup. This problem is still open.

In the next section we consider new problem of construction families of polynomial maps $g = g_n \in C(\mathbb{K}^n)$ of large order (order of g_n is going to infinity with the growth of n) and small degree (bounded by small constant) for all powers g^k of g (iteration of g with itself). Such maps can be used as bases for DLP.

6.4. On the idea of key exchange with a subgroups of Cremona group

We can choose the base of $\mathbb{K}^n$ and write each transformation $g \in C(\mathbb{K}^n)$ as a "public rule" in this base:

$$\begin{aligned} x_1 &\to g_1(x_1, x_2, \ldots, x_n), \\ x_2 &\to g_2(x_1, x_2, \ldots, x_n), \\ &\ldots \\ x_n &\to g_n(x_1, x_2, \ldots, x_n). \end{aligned}$$

Let $g^k \in C(\mathbb{K}^n)$ be the new public rule obtained via iteration of g.

We consider Diffie-Hellman algorithm for the key exchange in the case of group $C(\mathbb{K}^n)$. Correspondents Alice and Bob establish $g \in S_{p^n}$ via open communication channel, they choose positive integers n_A and n_B, respectively. They exchange public rules $h_A = g^{n_A}$ and $h_B = g^{n_B}$ via open channel. Finally, Alice and Bob compute common transformation T as $h_B^{n_A}$ and $h_A^{n_B}$, respectively.

In practice they can establish common vector $v = (v_1, v_2, \ldots, v_n)$, $v_i \in \mathbb{K}$ via open channel and use the collision vector $T(v)$ as a password for their private key encryption algorithm. Other option is usage of ordered array of the coefficients of collision map. In the case of DLP with "pseudorandom" family g_n of growing order we can use the term *hidden symbolic* discrete logarithm problem, word *hidden* is used because the order t of cyclic group usually is impossible to compute for the adversary.

This scheme of "symbolic Diffie - Hellman algorithm" can be secure, if the order of g is "sufficiently large" and adversary is not able to compute number n_A (or n_B) as functions from degrees for g and h_A. Obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case n_A is just a ratio of degh_A and deg$g$.

To avoid such trouble one can look at family of subgroups G_n of $C(\mathbb{K}^n)$, $n \to \infty$ such that maximal degree of its elements equal c, where c is small independent constant (*groups of degree c* or *groups of stable degree*). This chapter is devoted to some explicit constructions of such families.

We refer to a sequence of elements $g_n \in G_n$ such that all its nonidentical powers are of degree c as *element of stable degree*. This is equivalent to stability of families of cyclic groups generated by g_n. Of course, cyclic groups are important for the Diffie-Hellman type protocols.

It is clear that affine groups $AGL_n(\mathbb{K})$ of all invertible affine transformations, $n \to \infty$ form a family of subgroups of stable degree for $c = 1$ and all nonidentical affine transformations are of stable degree. Notice that if g is a linear diagonalisable element of $AGL_n(\mathbb{F}_p)$, then discrete logarithm problem for base g is equivalent to the classical number theoretical problem. Obviously, in this case we are loosing the flavor of symbolic computations and multivariate cryptography.

One can take a subgroup H of $AGL_n(\mathbb{K})$ and consider its conjugation with nonlinear bijective polynomial map f. Of course the group

$$H' = f^{-1}Hf$$

will be also a stable group, but for "most pairs" f and H group H' will be of degree degf $\times$ deg$f^{-1} \geq 4$ because of nonlinearity f and f^{-1}.

So the problem of construction an infinite families of subgroups G_n in $C(\mathbb{K}^n)$ of degree 2 and 3 may attract special attention.

6.5. On the projective limits of stable subgroups and corresponding multivariate cryptosystems

General problem of construction an infinite families of stable subgroups G_n of $C(\mathbb{K}^n)$ of degree c satisfying some additional conditions (unbounded

growth of order of "pseudo random" nonidentical group elements, existence of well defined projective limit, etc) can be also interesting because of possible applications in cryptography.

Notice, that even we conjugate nonlinear map F with invertible linear transformation $\tau \in AGL_n(\mathbb{K})$, some of important cryptographical parameters of F and $F' = \tau^{-1}F\tau$ can be different. Of course conjugate generators F and F' have the same number of fixed points, same cyclic structure as permutations, but counting of equal coordinates for pairs $(x,\ F(x))$ and $(x, F'(x))$ may bring very different results.

So two conjugate families of stable degree are not quite equivalent because corresponding cryptoanalytical problems may have different complexity.

Let $G_n = G_n(\mathbb{K})$, $n \geq 3$, $n \to \infty$ be a sequence of subgroups of $C(\mathbb{K}^n)$. We say that G_n is a *family of groups of stable degree* (or *subgroup of degree* c) if the maximal degree of representative $g \in G_n$ is some independent constant c. Recall, that cases of degree 2 and 3 are especially important.

Now, let us assume that there is a well defined projective limit G of G_n, $n \to \infty$ and G is the group of infinite order, it contains elements of infinite order. In case of finite commutative ring we assume that G is finitely generated group with the set of generaters $S = \{g_1, g_2, \ldots, g_r\}$. We assume that $G_n = \langle g_{1,n}, g_{2,n}, \ldots, g_{r,n}\rangle$ and g_i is a natural limit of $g_{i,n}$ when number of variables n growth to infinity.

We will refer to sequence $i_1, i_2, \ldots i_s$ as *irreversible string* if the order of $g_{i_1}g_{i_2}\ldots g_{i_s}$ is infinity and use the following multivariate cryptosystem.

Private-key algorithms.
We assume that two users Alice and Bob share a common password for the simple graph based encryption which is the irreversible string $i_1, i_2, \ldots i_s$, and two affine transformations τ_1, τ_2 from the affine group $AGL(n, \mathbb{K})$

Then, they encrypt the plaintext m and obtain ciphertext c as follows:

$$c = \tau_1 F_n \tau_2(m)$$

where $F_n = F_{i_1,i_2,\ldots,i_s,n} = g_{i_1,n}g_{i_2,n}\ldots g_{i_s,n}$. Decryption process is as follows:

$$m = \tau_2^{-1}F_n^{-1}\tau_1^{-1}(c),$$

where

$$F_n^{-1} = g_{i_s,n}^{-1}g_{i_{s-1},n}^{-1}\cdots g_{i_1,n}^{-1}.$$

Public-key algorithm
We assume that password as a string $i_1, i_2, \ldots, i_s$. Alice pick up parameter n.

She takes invertible affine transformations τ_1, τ_2 of the free module $\mathbb{K}^n$ also, She stores this secret information in secure way and computes the element

$$F_n = F_{i_1,i_2,\ldots,i_k,n} = g_{i_1,n}g_{i_2,n}\ldots g_{i_s,n}$$

and the map

$$f_A = \tau_1 F_n \tau_2$$

in symbolic way (she can use packages "Maple" , "Mathematica" or tools of Computer Algebra for specialists). She gets a public rule, which is a map of bounded degree c:

$$\begin{gathered} x_1 \to f_1(x_1, x_2, \ldots, x_n), \\ x_2 \to f_2(x_1, x_2, \ldots, x_n), \\ \ldots, \\ x_n \to f_n(x_1, x_2, \ldots, x_n), \end{gathered}$$

where f_i are multivariate polynomials from $\mathbb{K}[x_1, x_2, \ldots, x_n]$. If she uses the irreversible string $i_1, i_2, \ldots, i_s$ and affine maps τ_1, τ_2, such that $\tau_2 = \tau_1^{-1}$, then the order of transformation F_n of bounded polynomial degree is growing with the growth of n.

Alice can decrypt with the consequtive applications of maps τ_2^{-1}, $g_{i_s,n}^{-1}$, $g_{i_{s-1},n}^{-1}$, $\ldots$, $g_{i_1,n}^{-1}$ and τ_1^{-1}.

She can use numerical computations for the private key. We refer to scheme as multivariate cryptosystem with fast decryption if Alice can decrypt for $O(n)$. The computation of the ciphertext for public user will take time $O(n^{c+1})$.

Notice that general algorithm for the solution of nonlinear system of polynomial equations over finite field takes $c^{O(n)}$ (see, for example [20]).

Symbolic Diffie-Hellman algorithm

Suppose Alice and Bob want to agree on a key K_{AB}.

1. Alice use the information on the family of groups G_n and set of generators. She picks up the irreversible string $i_1, i_2, \ldots, i_s$ and parameter n. She chooses the invertible affine transformation τ of the free module $\mathbb{K}^n$. The first step Alice computes symbolically

$$F = \tau F_{i_1,i_2,\ldots,t_s,n} \tau^{-1}.$$

She sends the cubical symbolic map F to Bob. The next step is for Alice to pick a secret integer n_A that she does not reveal to anyone, while at the same time Bob picks an integer n_B that he keeps secret.

2. Alice and Bob use their secret integers (n_A and n_B, respectively) to compute $A = F^{n_A}$ and $B = F^{n_B}$ in Cremona group, respectively. Recall, that they use composition of multivariable map f with itself. After

that they exchange these computed cubical transformations.

3. Finally, Alice and Bob again use their secret integers to compute $K_{AB} = B^{n_A} = (f^{n_B})^{n_A} = f^{n_A n_B}$, and $K_{AB} = A^{n_B} = (f^{n_A})^{n_B} = f^{n_A n_B}$, respectively.

Recall, that, g is *cubical map* if has a form

$$g = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)),$$

where $f_i(x_1, \ldots, x_n)$ are polynomials of n variables written as the linear combination of monomials of kind

$$x_{i_1}^{n_1} x_{i_2}^{n_2} x_{i_3}^{n_3},$$

for $i_1, i_2, i_3 \in 1, 2, \ldots, n$; $n_1,\ n_2,\ n_3 \in \{0, 1, 2, 3\}$, $n_1 + n_2 + n_3 \leq 3$ with the coefficients from $\mathbb{K}$.

Security of the cryptographic algorithms usage based on the complexity of hard discrete logarithm problem for the group generated by polynomial transformations of degree $\leq c$ from the subgroup G_n of Cremona group $C(\mathbb{K}^n)$.

6.6. On constructive examples

Example 6.6.1. Let us consider family of graphs $D(n, \mathbb{K})$ over finite commutative ring $\mathbb{K}$. Let $N_{D,t,n}$ be the operator of taking the neighbour of the vertex from $\mathbb{K}^n \cup \mathbb{K}^n$. Let $G_D(n, \mathbb{K})$ be the group of cubical transformations from $C(\mathbb{K}^n)$ generated by $N_{D,t_1,n} N_{D,t_2,n}$, $t_1, t_2 \in \mathbb{K}$. The projective limit $G_D(\mathbb{K})$ is well defined and we can use described above cryptosystem. The string $t_1, t_2, \ldots t_{2s}$ of ring elements produce irreversible string $N_{D,t_1,n} N_{D,t_2,n}, \ldots, N_{D,t_{2s-1},n} N_{D,t_{2s},n}$ if the product d of $t_i + t_{i+1}$, $i = 1, 2, \ldots, 2s-1$ is antinilpotent ring element, i.e. $d^x \neq 0$ for each positive integer x.

Example 6.6.2. Let us consider family of graphs $A(n, \mathbb{K})$ over finite commutative ring $\mathbb{K}$. Let $N_{A,t,n}$ be the operator of taking the neighbour of the vertex from $\mathbb{K}^n \cup \mathbb{K}^n$ Let $G_A(n, \mathbb{K})$ be the group of cubical transformations from $C(\mathbb{K}^n)$ generated by $N_{A,t_1,n} N_{A,t_2,n}$, $t_1, t_2 \in \mathbb{K}$. The projective limit $G_A(\mathbb{K})$ is well defined and we can use described above cryptosystem. The string $t_1, t_2, \ldots t_{2s}$ of ring elements produce irreversible string $N_{A,t_1,n} N_{A,t_2,n}, \ldots, N_{A,t_{2s-1},n} N_{A,t_{2s},n}$ if the product d of $t_i + t_{i+1}$, $i = 1, 2, \ldots, 2s-1$ is antinilpotent ring element.

Example 6.6.3. Let us consider family of graphs $DD(n, \mathbb{K})$ over finite commutative ring $\mathbb{K}$. Let $N_{DD,t,n+1}$ be the operator of taking the neighbour of the vertex from $\mathbb{K}^{n+1} \cup \mathbb{K}^{n+1}$ Let $G_D D(n, \mathbb{K})$ be the group of cubical transformations from $C(\mathbb{K}^n)$ generated by $N_{DD,t_1,n+1}N_{DD,t_2,n+1}$, $t_1, t_2 \in \mathbb{K}$. The projective limit $G_{DD}(\mathbb{K})$ is well defined and we can use described above cryptosystem. The string $t_1, t_2, \dots t_{2s}$ of ring elements produce irreversible string $N_{DD,t_1,n+1}N_{DD,t_2,n+1}$, $\dots$, $N_{DD,t_{2s-1},n+1}N_{DD,t_{2s},n+1}$ if the product d of t_i, $i = 1, 2, \dots, 2s$ is antinilpotent ring element, i.e. $d^x \neq 0$ for each positive integer x.

Some other examples of such multivariate cryptosystem the reader can find in [175], [176]. The first example of quadratic stable maps the reader can find in [182].

Multivariate cryptosystem corresponding to group $D(n, \mathbb{K})$ were introduced in [157] [159]. The theorem on stability of group $G_D(n, \mathbb{K})$ was proven in [184]. Private key algorithm for this system was introduced earlier [152], [154]. Properties of corresponding stream ciphers over special rings and fields and technicalities of the implementations the reader can find in [76], [146], [147], [163] see also [168] for earlier implementations.

Cryptoalgorithms corresponding graphs $A(n, \mathbb{K})$ were introduced in [119], [121], some properties are investigated [77] , [122] and implementations [69].

Multivariate cryptosystem corresponding to directed graphs $DD(n, \mathbb{K})$ were introduced in [162], [165].

The implementations of this multivariate cryptosystem were described in [70], [72], [73], [162].

In all three examples (1) - (3) the stable groups are formed by cubical maps. So, the complexity of ciphertext computation is $O(n^4)$. In case of strings $t_1, t_2, \dots, t_{2s}$ of finite length s and sparse affine transformations τ_1 and τ_2 for which exactly $O(n)$ entries are distinct from zero, the decryption takes time $O(n)$.

6.7. On Multivariate Cryptography with stable groups and Extremal Graph Theory

The goal of Multivariate Cryptography, which have some potential to be used in the era of Postquantum Cryptography. The Quantum Computer is a special random computational machine. Recall that computation in Turing machine can be formalised with the concept of finite automaton as a walk in the graph with arrows labelled by special symbols. "Random computation" can be defined as a random walk in the random graph. So we are looking for the deterministic approximation of random graphs by extremal algebraic

graphs. It is known that the explicit solutions for an optimization graphs have properties similar to random graphs.

The probability of having rather short cycle in the walking process on random graph is zero. So the special direction of Extremal Graph Theory of studies of graphs of order v (the variable) without short cycles of maximal size (number of edges) can lead to the discovery of good approximation for random graphs. On can use dual problem of finding k-regular graphs of minimal order v without cycles of given length $3, 4, \ldots, d$ during the search for good pseudorandom graphs. We can try to use similar idea for directed graphs, which are important for automata theory. In that case we have to prohibit commutative diagrams instead cycles. So we will look for optimal algebraic graphs. Recall that in case of algebraic graph, its vertex set and edge set (arrow set for directed graph) are algebraic varieties over special finite ring $\mathbb{K}$. Of course for the purposes of Multivariate Cryptography we need a strong additional condition that walk of the graph produce bijective polynomial nonlinear automorphism of the vertex set of restricted polynomial degree.

In the case of simple graphs we concentrate mainly on the investigation of maximal size
$ex(C_3, C_4, \ldots, C_{2m}, v)$ of the graph on v vertices without cycles of length $3, 4, \ldots, 2m$ i.e. graphs of girth $> 2m$. Recall that the girth is the length of minimal cycle in the simple graph. As it follows from famous Even Circuit Theorem by P. Erdős we have inequality

$$ex(C_3, C_4, \ldots, C_{2m}, v) \leq cv^{1+1/m},$$

where c is a certain constant. The bound is known to be sharp only for $m = 4, 6, 10$.

The first general lower bounds of kind

$$ex(v, C_3, C_4, \ldots C_n) = \Omega(v^{1+c/n}) \tag{6.7.1}$$

The best known lower bound for $d \neq 2, 3, 5$ had been obtained in [82]:

$$ex(v, C_3, C_4, \ldots, C_{2d}) = c(v^{1+2/(3d-3+e)}) \tag{6.7.2}$$

where $e = 0$ if d is odd, and $e = 1$ if d is even. This results is based on studies of graphs $CD(n, q)$. Let Γ_i be a family of regular simple graphs of order v_i of increasing girth g_i. We refer to Γ_i as a optimal family of large graphs if there is a constant d such that v_i^d is on the upper bound of Erdos Even Circuit Theorem.

Graphs $CD(n, q)$ and $X(p, q)$ are examples of optimal graphs of large girth with $d = 3/2$. The first family of nonlinear algebraic graphs is connected with cubical stable group of previous section.

Recall that we refer to minimal length of a cycle, through the vertex of given vertex of the simple graph as *cycle indicator of this vertex*. The *cycle indicator of the graph* will be defined as maximal cycle indicator of its vertices. We refer to the simple graph as *cycle irregular graph* if this indicator differs from the girth (the length of minimal cycle). The solution of the optimization problem of computation of maximal size $e = e(v)$ of the graph of order v with the cycle indicator greater than d, $d > 2$ has been found very recently (see [175], [176]).

Theorem 6.7.1. *Let $e(v, d)$ be the maximal size of the simple graph on v with the cycle indicator at least $d + 1$, $d \geq 2$. Then*

$$e(v, d) \Leftrightarrow O(v^{1+[2/d]}).$$

Let Γ_i be a family of regular simple graphs of order v_i with the increasing cycle indicator g_i. We refer to Γ_i as a optimal family of graphs with large girth indicator if there is a constant d such that v_i^d is on the written above upper bound. Graphs $A(n, q)$ form a family of optimal graphs with large cycle indicator with best possible constant $d = 1$. This family of nonlinear algebraic graphs is used for the generation of cubical stable groups (example 2 of previous section).

Theorem 6.7.2. *Finally, let* $\mathrm{Ex}(v, d)$ *be the maximal size of balanced directed graph on v vertices with the girth indicator $> d$. Then*

$$\mathrm{Ex}(v, d) \Leftrightarrow O(v^{1+1/d}).$$

Let Γ_i be a family of directed balanced graphs of order v_i with the increasing cycle indicator d_i. We refer to Γ_i as a optimal family of directed graphs with large girth indicator if there is a constant d such that ${v_i}^d$ is on the written above upper bound. Graphs $DD(n, M, \mathbb{K})$ form a family of optimal directed graphs with large cycle indicator for some constant $d = d(M, \mathbb{K})$. This family of nonlinear algebraic graphs over rings is used for the generation of cubical stable groups (example 3 of previous section).

Behaviour of optimal graphs from mentioned above classes (large girth, large cycle indicator, large girth indicator) are similar to random graphs.

6.8. On the minimal graphs of given degree and girth

Graphs of large girth have not only cryptographical applications, they used in Networking, Theory of parallel computations, Error correction, Image Processing and etc. Quite often solutions for the minimization problem of the order of k-regular graph with prescribed girth can be used.

Let $k \geq 3$ and $g \geq 3$ be in integers. A (k, g)-graph is a k-regular graph with girth exactly g. A $(k, g) -$ cage is a (k, g)-graph of minimal order. The problem of determining the $v(k, g)$ of a (k, g)-cage is unsolved for most pairs (k, g) and is extremely hard in general case. By counting the number of vertices in the breadth-first-search tree of a (k, g)-graph, one easily establishes the following lower bounds for $v(k, g)$:

$v(k, g) \geq k(k-1)^{(g-1)/2}/(k-2)$ for g odd, $k \geq 4$

$v(k, g) \geq 2(k-1)^{g/2-2}/(k-2)$ for g even, $k \geq 4$

The problem of determining $v(k, g)$ was posed in 1959 by F. Kartesi who observed that $v(3, 5) = 10$ was realized by the Petersen graph (see [164]). The above lower bound had been established by Tutte [148].

Let us consider the family of graphs G_i of degree l_i and unbounded girth g_i such that

$$g_i \geq \gamma \log_{l_i - 1}(v_i)$$

The last formula means that G_i, $i = 1, \ldots$ form an infinite *family of graphs of large girth* in the sense of N. Biggs [7], [8].

The order of graphs from such a family is close to the lower bound on $v(k, g)$, this bound shows that $\gamma \leq 2$ but no family has been found for which $\gamma = 2$. Bigger γ's correspond to the larger girth.

For many years the only significant result were the theorems of Erdø"s' and Sachs [37], and its improvement by Sauer [127], Walther and others (see [10], [11] for more details and references), who using nonconstructive methods proved the existence of infinite families with $\gamma = 1$.

The problem of estimation of order of cages is dual to problem on the maximal size of graphs on girth g.

Let $v(k, C_{2n})$ be the minimal order of k-regular graph without cycles of the length $2n$. The problem to evaluate $v(k, C_{2n})$ is dual to famous problem on the maximal size of the graph on v vertices without even cycles C_{2n} by Erdø"s' (see [38]). As it follows from definitions

$$v(k, C_{2n}) \leq v(k, 2n+1),$$
$$v(k, C_{2n}) \leq v(k, 2n+2).$$

The construction of graphs $L(n, q)$ and $B(n, q)$ implies the following result (the best known upper bounds on $v(k, C_{4n})$ (see [84]).

Theorem 6.8.1. *Let $k \geq 2$ and $g \geq 5$ be integers, and let q denote the smallest prime power for which $k < q$, let b be the smallest power of 2 for which $k \leq q$.*

Then the following upper bounds hold

$$v(k, C_{4n}) \leq (k+1)q^{(3/4)^{n-2}} \tag{6.8.1}$$

$$v(k, C_{4n}) \leq kb^{(3/4)^{n-2}} \tag{6.8.2}$$

It is clear, that for some very special k the bound 6.8.2 is better then 6.8.

By Chebyshev's Theorem for a fixed integer $k \geq 3$ there is always a prime between k and $2k-2$. For any $e \geq 0$ and $k > k_0(e)$, this interval can be narrowed to $[k, k + k^{2/3+e}]$.

The best known bound for $v(k, 2n)$, n is odd, follows from the bound on $v(k, 2n)$:

Let $k \geq 2$ and $g \geq 5$ be integers, and let q denote the smallest odd prime power for which $k \leq q$. Then

$$v(k, g) \leq 2kq^{(3/4)^{g-\alpha}} \tag{6.8.3}$$

where $\alpha = 4, 11/4, 7/2, 13/4$ for $g = 0, 1, 2, 3 \bmod 4$, respectively. It is clear that bound on $v(k, C_{4n})$ is always better then .

Appendix A

Cartan matrices and Root Systems

PLATE I

SYSTEM OF TYPE A_n $(n \geq 1)$

I V is the hyperplane of $E = \mathbb{R}^{n+1}$ consisting of the points the sum of whose coordinates is zero.
Roots: $e_i - e_j$ $(i \neq j,\ 1 \leq i \leq n+1,\ 1 \leq j \leq n+1)$.
Number of roots: $N = n(n+1)$

II Basis: $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3$, $\ldots$, $\alpha_n = e_n - e_{n+1}$
Positive roots:

$$e_i - e_j = \sum_{i \leq k < j} \alpha_k \quad (1 \leq i < j \leq n+1),$$

(more details reader can find in [15]).

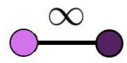
III Coxeter number: $h = n + 1$.

IV Coxeter diagram:

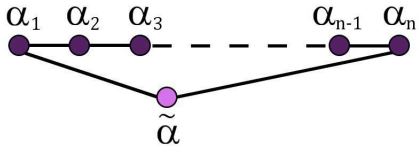
V Highest root: $\tilde{\alpha} = e_1 - e_{n+1} = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

VI Completed Coxeter-Dynkin diagram:

for $n = 1$:



for $n \geq 2$:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & -1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 & 0 \\ 0 & 0 & -1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & 2 \end{pmatrix}$$

PLATE II

SYSTEM OF TYPE B_n $(n \geq 2\ )$

I $V = E = \mathbb{R}^n$.
Roots: $\pm e_i$ $(1 \leq i \leq n)$, $\pm e_i \pm e_j$ $(1 \leq i < j \leq n)$.
Number of roots: $N = 2n^2$

II Basis: $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3$, $\ldots$, $\alpha_{n-1} = e_{n-1} - e_n$, $\alpha_n = e_n$.
Positive roots:

$$e_i = \sum_{i \leq k \leq n} \alpha_k \quad (1 \leq i \leq n),$$

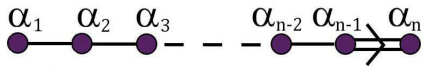
$$e_i - e_j = \sum_{i \leq k < j} \alpha_k \quad (1 \leq i < j \leq n)$$

$$e_i + e_j = \sum_{i \leq k < j} \alpha_k + 2 \sum_{j \leq k \leq n} \alpha_k \quad (1 \leq i < j \leq n),$$

(more details reader can find in [15]).

III Coxeter number: $h = 2n$.

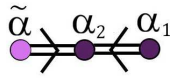
IV Coxeter diagram:



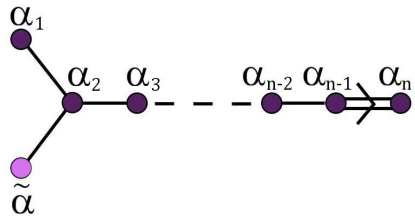
V Highest root: $\tilde{\alpha} = e_1 + e_2 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_n$.

VI Completed Coxeter-Dynkin diagram:

for $n = 2$:



for $n \geq 3$:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & -1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 & 0 \\ 0 & 0 & -1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 2 & -2 \\ 0 & 0 & 0 & 0 & \dots & -1 & 2 \end{pmatrix}$$

PLATE III

SYSTEM OF TYPE C_n $(n \geq 2\ )$

I $V = E = \mathbb{R}^n$.
Roots: $\pm 2e_i$ $(1 \leq i \leq n)$, $\pm e_i \pm e_j$ $(1 \leq i < j \leq n)$.
Number of roots: $N = 2n^2$.

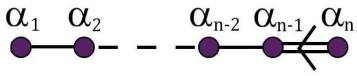
II Basis: $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3$, $\ldots$, $\alpha_{n-1} = e_{n-1} - e_n$, $\alpha_n = 2e_n$.
Positive roots:

$$e_i - e_j = \sum_{i \leq k < j} \alpha_k \quad (1 \leq i < j \leq n)$$
$$e_i + e_j = \sum_{i \leq k < j} \alpha_k + 2 \sum_{j \leq k < n} \alpha_k + \alpha_n \ (1 \leq i < j \leq n),$$
$$2e_i = \sum_{i \leq k < n} \alpha_k + \alpha_n \quad (1 \leq i \leq n)$$

(more details reader can find in [15]).

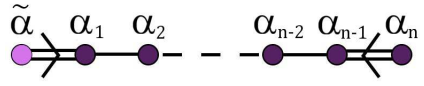
III Coxeter number: $h = 2n$

IV Coxeter diagram:



V Highest root: $\tilde{\alpha} = 2e_1 = 2\alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_{n-1} + \alpha_n$.

VI Completed Coxeter-Dynkin diagram:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & -1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 2 & -1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 2 & -1 & \dots & 0 & 0 \\ 0 & 0 & -1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 & -1 \\ 0 & 0 & 0 & 0 & \dots & -2 & 2 \end{pmatrix}$$

PLATE IV

SYSTEM OF TYPE D_n $(n \geq 1)$

I $V = E = \mathbb{R}^n$
Roots: $\pm e_i \pm e_j$ $(1 \leq i < j \leq n)$; (e_i) the canonical basis of $\mathbb{R}^n$.
Number of roots: $N = 2n(n-1)$

II Basis: $\alpha_1 = e_1 - e_2$, $\alpha_2 = e_2 - e_3$, $\ldots$, $\alpha_{n-1} = e_{n-1} - e_n$, $\alpha_n = e_{n-1} + e_n$.
Positive roots:

$$e_i - e_j = \sum_{i<k<j} \alpha_k \quad (1 \leq i < j \leq n),$$

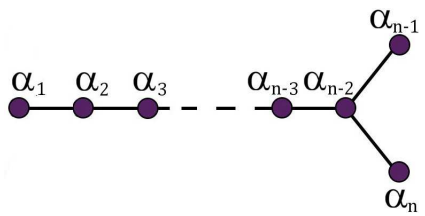
$$e_i + e_n = \sum_{i \leq k \leq n-2} \alpha_k + \alpha_n \quad (1 \leq i < n),$$

$$e_i + e_j = \sum_{i \leq k < j} \alpha_k + 2 \sum_{j \leq k < n-1} \alpha_k + \alpha_{n-1} + \alpha_n \ (1 \leq i < j < n),$$

(more details reader can find in [15]).

III Coxeter number: $h = 2n - 2$.

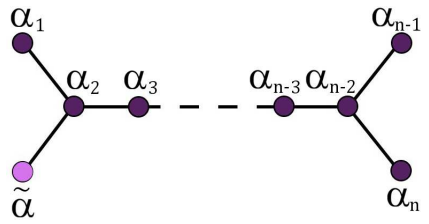
IV Coxeter diagram:



V Highest root:

$$\tilde{\alpha} = e_1 + e_2 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_{n-2} + \alpha_{n-1} + \alpha_n.$$

VI Completed Coxeter-Dynkin diagram ($n \geq 4$):



VII Cartan matrix ($n \times n$)

$$\begin{pmatrix} 2 & -1 & \dots & 0 & 0 & 0 & 0 \\ -1 & 2 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 2 & -1 & 0 & 0 \\ 0 & 0 & \dots & -1 & 2 & -1 & -1 \\ 0 & 0 & \dots & 0 & -1 & 2 & 0 \\ 0 & 0 & \dots & 0 & -1 & 0 & 2 \end{pmatrix}$$

PLATE V

SYSTEM OF TYPE E_6

I V is the subspace of $E = \mathbb{R}^8$ consisting of the points whose coordinates (x_i) are such that $x_6 = x_7 = -x_8$.
Roots: $\pm e_i \pm e_j$ $(1 \le i < j \le 5)$,

$$\pm\frac{1}{2}(e_8 - e_7 - e_6 + \sum_{i=1}^{5}(-1)^{\nu(i)}e_i) \quad \text{with} \quad \sum_{i=1}^{5}\nu(i) \text{ even}$$

Number of roots: $N = 72$.

II Basis: $\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + e_4 + e_5 + e_6 + e_7)$, $\alpha_2 = e_1 + e_2$, $\alpha_3 = e_2 - e_1$, $\alpha_4 = e_3 - e_2$, $\alpha_5 = e_4 - e_3$, $\alpha_6 = e_5 - e_4$.
Positive roots: $\pm e_i + e_j$ $(1 \le i < j \le 5)$,

$$\frac{1}{2}(e_8 - e_7 - e_6 + \sum_{i=1}^{5}(-1)^{\nu(i)}e_i) \quad \text{with} \quad \sum_{i=1}^{5}\nu(i) \text{ even}$$

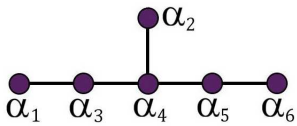
Positive roots with at least one coefficient ≥ 2 we denote the root $a\alpha_1 + b\alpha_2 + c\alpha_3 + d\alpha_4 + e\alpha_5 + f\alpha_6$ by $\begin{smallmatrix} a\,c\,d\,e\,f \\ \quad b \end{smallmatrix}$

$$\begin{array}{ccccccccccc} 0\,1\,2\,1\,0 & & 1\,1\,2\,1\,0 & & 0\,1\,2\,1\,1 & & 1\,2\,2\,1\,0 & & 1\,1\,2\,1\,1 & & 0\,1\,2\,2\,1 \\ & 1 & & 1 & & 1 & & 1 & & 1 & \\ 1\,2\,2\,1\,1 & & 1\,1\,2\,2\,1 & & 1\,2\,2\,2\,1 & & 1\,2\,3\,2\,1 & & 1\,2\,3\,2\,1 & & \\ & 2 & & 1 & & 1 & & 1 & & 2 & \end{array}$$

(more details reader can find in [15])

III Coxeter number: $h = 12$.

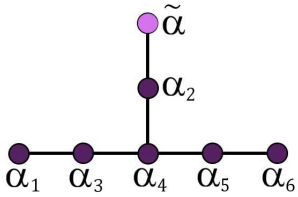
IV Coxeter diagram:



V Highest root:

$$\begin{aligned}\tilde{\alpha} &= \frac{1}{2}(e_1 + e_2 + e_3 + e_4 + e_5 - e_6 - e_7 + e_8) \\ &= \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6.\end{aligned}$$

VI Completed Coxeter-Dynkin diagram:



VII Cartan matrix (6×6)

$$\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

PLATE VI

SYSTEM OF TYPE E_7

I V is hyperplane in $E = \mathbb{R}^8$ ortogonal to $e_7 + e_8$.
Roots: $\pm e_i \pm e_j$ $(1 \le i \le j \le 6)$, $\pm(e_7 - e_8)$.

$$\pm\frac{1}{2}(e_7 - e_8 + \sum_{i=1}^{6}(-1)^{\nu(i)}e_i) \quad \text{with} \quad \sum_{i=1}^{6}\nu(i) \text{ odd}$$

Number of roots: $N = 126$.

II Basis: $\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + e_4 + e_5 + e_6 + e_7)$, $\alpha_2 = e_1 + e_2$, $\alpha_3 = e_2 - e_1$, $\alpha_4 = e_3 - e_2$, $\alpha_5 = e_4 - e_3$, $\alpha_6 = e_5 - e_4$, $\alpha_7 = e_6 - e_5$.
Positive roots:

$$\pm e_i + e_j (1 \le i < j \le 6), \quad -e_7 + e_8,$$

$$\frac{1}{2}(-e_7 + e_8 + \sum_{i=1}^{6}(-1)^{\nu(i)}e_i) \quad \text{with} \quad \sum_{i=1}^{6}\nu(i) \text{ odd}$$

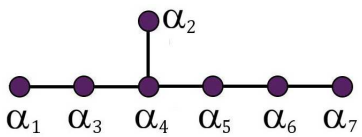
Positive roots containing α_7 and having at least one coefficient ≥ 2, we denote the root $a\alpha_1 + b\alpha_2 + c\alpha_3 + d\alpha_4 + e\alpha_5 + f\alpha_6 + g\alpha_7$ by $\begin{smallmatrix} a & c & d & e & f & g \\ & & b & & & \end{smallmatrix}$

0 1 2 1 1 1	1 1 2 1 1 1	0 1 2 2 1 1	1 2 2 1 1 1	1 1 2 2 1 1
1	1	1	1	1
0 1 2 2 2 1	1 2 2 2 1 1	1 1 2 2 2 1	1 2 2 2 2 1	1 2 3 2 1 1
1	1	1	1	1
1 2 3 2 2 1	1 2 3 2 1 1	1 2 3 3 2 1	1 2 3 2 2 1	1 2 3 3 2 1
1	2	1	2	2
	1 2 4 3 2 1	1 3 4 3 2 1	2 3 4 3 2 1	
	2	2	2	

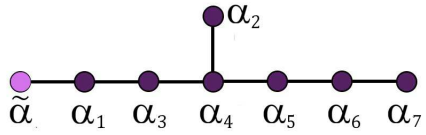
(more details reader can find in [15])

III Coxeter number: $h = 18$.

IV Coxeter diagram:



V Highest root: $\tilde{\alpha} = e_8 - e_7 = 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7$.
VI Completed Coxeter-Dynkin diagram:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

PLATE VII

SYSTEM OF TYPE E_8

I $V = E = \mathbb{R}^8$.
Roots: $\pm e_i \pm e_j$ $(i < j)$,

$$\frac{1}{2}\sum_{i=1}^{8}(-1)^{\nu(i)}e_i \quad \text{with} \quad \sum_{i=1}^{8}\nu(i) \text{ even}.$$

Number of roots: 240.

II Basis: $\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + e_4 + e_5 + e_6 + e_7)$, $\alpha_2 = e_1 + e_2$, $\alpha_3 = e_2 - e_1$, $\alpha_4 = e_3 - e_2$, $\alpha_5 = e_4 - e_3$, $\alpha_6 = e_5 - e_4$, $\alpha_7 = e_6 - e_5$, $\alpha_8 = e_7 - e_6$.
Positive roots: $\pm e_i + e_j$ $(i < j)$,

$$\frac{1}{2}(e_8 + \sum_{i=1}^{7}(-1)^{\nu(i)}e_i) \quad \text{with} \quad \sum_{i=1}^{7}\nu(i) \text{ even}$$

Positive roots containing α_8 and having at least one coefficient ≥ 2, we denote the root $a\alpha_1 + b\alpha_2 + c\alpha_3 + d\alpha_4 + e\alpha_5 + f\alpha_6 + g\alpha_7 + h\alpha_8$ by $\begin{smallmatrix} a & c & d & e & f & g & h \\ & b & & & & & \end{smallmatrix}$

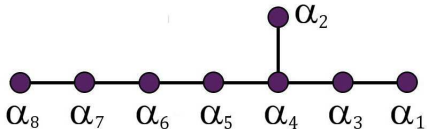
0 1 2 1 1 1 1	0 1 2 2 1 1 1	1 1 2 1 1 1 1	0 1 2 2 2 1 1	1 2 2 1 1 1 1
1	1	1	1	1
1 1 2 2 1 1 1	1 2 2 2 1 1 1	1 1 2 2 2 1 1	0 1 2 2 2 2 1	1 2 3 2 1 1 1
1	1	1	1	1
1 2 2 2 2 1 1	1 1 2 2 2 2 1	1 2 3 2 1 1 1	1 2 3 2 2 1 1	1 2 2 2 2 2 1
1	1	2	1	1
1 2 3 2 2 1 1	1 2 3 3 2 1 1	1 2 3 2 2 2 1	1 2 3 3 2 1 1	1 2 3 2 2 2 1
2	1	1	2	2
1 2 3 3 2 2 1	1 2 4 3 2 1 1	1 2 3 3 2 2 1	1 2 3 3 3 2 1	1 3 4 3 2 1 1
1	2	2	1	2
1 2 4 3 2 2 1	1 2 3 3 3 2 1	2 3 4 3 2 1 1	1 3 4 3 2 2 1	1 2 4 3 3 2 1
2	2	2	2	2
2 3 4 3 2 2 1	1 3 4 3 3 2 1	1 2 4 4 3 2 1	2 3 4 3 3 2 1	1 3 4 4 3 2 1
2	2	2	2	2
1 3 5 4 3 2 1	2 3 4 4 3 2 1	1 3 5 4 3 2 1	2 3 5 4 3 2 1	2 3 5 4 3 2 1
2	2	3	2	3

$$\begin{array}{ccccccccc} 2\,4\,5\,4\,3\,2\,1 & & 2\,4\,5\,4\,3\,2\,1 & & 2\,4\,6\,4\,3\,2\,1 & & 2\,4\,6\,5\,3\,2\,1 & & 2\,4\,6\,5\,4\,2\,1 \\ 2 & & 3 & & 3 & & 3 & & 3 \\ & & & 2\,4\,6\,5\,4\,3\,1 & & 2\,4\,6\,5\,4\,3\,2 & & & \\ & & & 3 & & 3 & & & \end{array}$$

(more details reader can find in [15]).

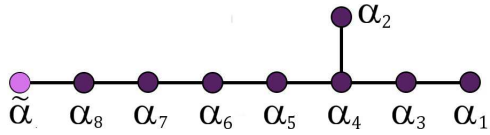
III Coxeter number: $h = 30$.

IV Coxeter diagram:



V Highest root: $\tilde{\alpha} = e_7 + e_8 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8$.

VI Completed Coxeter-Dynkin diagram:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

PLATE VIII

SYSTEM OF TYPE F_4

I $V = E = \mathbb{R}^4$.
Roots:

$$\pm e_i,\ (1 \le i \le 4), \quad \pm e_i \pm e_j\ (1 \le i < j \le 4),$$

$$\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4).$$

Number of roots: $N = 48$.

II Basis: $\alpha_1 = e_2 - e_3$, $\alpha_2 = e_3 - e_4$, $\alpha_3 = e_4$, $\alpha_4 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4)$.
Positive roots:

$$e_i\ (1 \le i \le 4),\ e_i \pm e_j\ (1 \le i < j \le 4),\ \frac{1}{2}(e_1 \pm e_2 \pm e_3 \pm e_4).$$

Positive roots with at least one coefficient ≥ 2, we denote the root $a\alpha_1 + b\alpha_2 + c\alpha_3 + d\alpha_4$

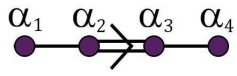
0120 1120 0121 1220 1121 0122 1221

1122 1231 1222 1232 1242 1342 2342

(more details reader can find in [15]).

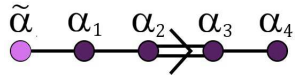
III Coxeter number: $h = 12$.

IV Coxeter diagram:



V Highest root: $\tilde{\alpha} = e_1 + e_2 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4$.

VI Completed Coxeter-Dynkin diagram:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

PLATE IX

SYSTEM OF TYPE G_2

I V is hyperplane in $E = \mathbb{R}^3$ with equation $x_1 + x_2 + x_3 = 0$.
Roots:

$$\pm(e_1 - e_2),\ \pm(e_1 - e_3),\ \pm(e_2 - e_3),\ \pm(2e_1 - e_2 - e_3),$$

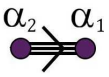
$$\pm(2e_2 - e_1 - e_3),\ \pm(2e_3 - e_1 - e_2).$$

Number of roots: $N = 12$.

II Basis: $\alpha_1 = e_1 - e_2$, $\alpha_2 = -2e_1 + e_2 + e_3$.
Positive roots: α_1, α_2, $\alpha_1 + \alpha_2$, $2\alpha_1 + \alpha_2$, $3\alpha_1 + \alpha_2$, $3\alpha_1 + 2\alpha_2$,
(more details reader can find in [15]).

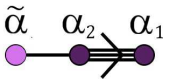
III Coxeter number: $h = 6$.

IV Coxeter diagram:



V Highest root: $\tilde{\alpha} = -e_1 - e_2 + 2e_3 = 3\alpha_1 + 2\alpha_2$.

VI Completed Coxeter-Dynkin diagram:



VII Cartan matrix $(n \times n)$

$$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

Bibliography

[1] E. Artin, *Galois Theory*, Lectures Delivered at the University of Notre Dame Notre Dame Mathematical Lectures, Number 2 Notre Dame, Indiana : University of Notre Dame, 1971. 2nd edition 82 pp.

[2] E. Bannai, N. Ito, *Algebraic Combinatorics*.

[3] A. Beutelspachera, *Enciphered Geometry*. Some Applications of Geometry To Cryptography, Annals of Discrete Mathematics, V.37, 1988, 59-68.

[4] C.T. Benson, *Minimal regular graphs of girth eight and twelve*, Canadien Journal of Mathematics, (18):1091- 1094, 1966.

[5] C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: turbo-codes*, ICC 1993, Geneva, Switzerland, pp. 1064-1070, May 1993.

[6] F. Bien, *Constructions of telephone networks by group representations*, Notices Amer. Mah. Soc., 36 (1989), 5-22.

[7] N. Biggs, *Algebraic Graph Theory* (2nd ed), Cambridge, University Press, 1993.

[8] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.

[9] N.L. Biggs and A.G. Boshier, *Note on the Girth of Ramanujan Graphs*, Journal of Combinatorial Theory, Series **B 49**, pp. 190–194 (1990).

[10] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[11] B. Bollobás, *Random Graphs*, Academic Press, London, 1985.

[12] J.A. Bondy and M.Simonovits, *Cycles of even length in graphs*, J. Combin.Theory, Ser. B, 16 (1974) 87-105.

[13] A. Borovik, *Matroids and Coxeter groups*, In: Survey in Combinatorics 2003, London Math Soc. Lect. Notes Ser., vol 307, Cambridge University Press, 2003, 79-114.

[14] A. Borovik, I. Gelfand, N. White, *Combinatorial flag varieties*, J. Comb. Theory (A), 2000, v. 91, 111-136.

[15] N. Bourbaki, *Lie Groups and Lie Algebras*, Chapters 1 - 9, Springer, 1998-2008.

[16] A. Brower, A. Cohen, A. Nuemaier, *Distance regular graphs*, Springer, Berlin, 1989.

[17] A. A. Bruen D. L. Wehlau, *Error-Correcting Codes, Finite Geometries and Cryptography*, AMS, 2010.

[18] F. Buekenhout, *Diagrams for geometries and groups*, J. Comb. Theory, Ser. A., 27,1979, pp 261-285.

[19] F. Buekenhout (Editor), *Handbook on Incidence Geometry*, North Holland, Amsterdam, 1995.

[20] A.L.Chistov, *An improvement of the complexity bound for solving systems of polynomial equations*, Zapisky nauchnych seminarov POMI, vol. 390, 2011, 2999-306.
[21] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York (1972).
[22] P. J. Cameron and J.H. van Lint, *Graphs, Codes and Designs*, London. Math. Soc. Lecture Notes, 43, Cambridge (1980).
[23] W. Chow, *On the geometry of algebraic homogeneous spaces*, Ann. Math.,2, 1950, pp 93 - 99.
[24] A. Cohen, *A synopsis of known distance regular graphs with large diameters*, Math Centr. Afd. Zuiv. Wisk.- N168, 1981, 38p.
[25] A. Cossidente, M. J. de Ressmine, *Remarks on Singer Cycle Groups and Their Normalizers*, Desighns, Codes and Cryptography, 32, 97-102, 2004.
[26] N.T. Courtois, *The sequrity of Hidden Field equations (HFE)*, in CT-RSA01, 2001, LNCS, vol. 2020 pp. 266-281.
[27] N. T. Courtois, L. Goubin, *Cryptanalysis of the TTM cryptosystem* in Adv. Cryptol. ASIACRYPT00, 2000 LNCS, vol. 1976, pp. 44-57.
[28] N.T. Courtois, A. Klimov, J. Patarin, A. Shamir, *Efficient Algorithm for Solving Overdefined System of Multivariate Polynomial Equations*, EUROCRYPT 2000, LNCS Vol. 1807, pp. 392-407. 16
[29] P. Delsart, *Algebraic approach to association schemes of coding theory*, Philips Res. Rep. Suppl. 10 (1973).
[30] L. Dickson, *Linear groups with an exposition of the Galois field theory*, New York, Dower Publ. Inn, 1958, 398p.
[31] J. Dieudonne, *La geometrie des groupes classiques*, Springer-Verlag, 1955.
[32] W. Diffie and M. E. Hellman *New directions in cryptography*, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, 644-654.
[33] E. Dijkstra, *A note on two problems in connection with graphs*, Num. Math., 1 (1959), 269-271.
[34] J. Ding, *A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation*, in PKC04, LNCS Vol. 2947, pp. 305-318, 2004.
[35] J. Ding, J. E. Gower, D. S. Schmidt, *Multivariate Public Key Cryptosystems*, Springer, 2006
[36] J. Ding, Lei Hu, Xuyun Nie, Jianyu Li, John Wagner, *High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems*, PKC 2007 LNCS, vol. 4450, pp. 233-248, Springer, 2007.
[37] P. Erdös', A. R'enyi and V. T. S'oc, *On a problem of graph theory*, Studia. Sci. Math. Hungar. 1 (1966), 215-235.
[38] P. Erdös', M. Simonovits, *Compactness results in extremal graph theory*, Combinatorica 2 (3), 1982, 275-288.
[39] I. Faradjev, A. Ivanov, M. Klin, A. Woldar, *Investigations in Algebraic Theory of Combinatorial Objects*, Kluwer, Dordrecht, 1992.
[40] W. Feit, D. Higman *The nonexistence of certain generalised polygons*, J. of Algebra 1 (1964), 114-131.
[41] Jean-Charles Faugere, A. Joux A, *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Grobner Basis*, in CRYPTO 2003, LNCS Vol. 2729, pp. 44-60, 2003.
[42] Pierre-Alain Fouque, L. Granboulan, J. Sterm, *Differential Cryptanalysis for*

Multivariate Schemes, in EUROCRYPT 2005, LNCS Vol. 3494, pp. 341-353, 2005.

[43] H. Freudental,*Octaven Ausnahmegruppen und Octavengeometrie*, Utrecht: Math. Inst. der Rijksuniv.-1951, 1956.

[44] H. Freudental, H. de Vries, *Linear groups*, New York, Acad. Press, 1969, 547 p.

[45] R.G. Gallager, *Low-Density Parity-Checks Codes*, IRE Trans of Info Thy 8 (Jan 1962):21–28.

[46] M. Gari, D. Johnson, *Computers and Intractability, A Guide to the Theory of NP-Completeness*, Freeman, 1979.

[47] I. Gelfand, R. MacPherson, *Geometry in Grassmanians and generalisation of the dilogarithm*, Adv. in Math., 44 (1982), 279-312.

[48] I. Gelfand, V. Serganova, *Combinatorial geometries, and tor stratification on homogeneous compact varieties*, Uspehi Mat. Nauk, 1987, v.42. part 2, pp 108-138.

[49] D. Gorenstein, *Finite Simple Groups: an introduction to their classification*, Plenum Press, 1982, 333 pp.

[50] P. Guinand, J. Lodge, *Graph theoretic construction of generalized product codes*, IEEE International Symposium on Information Theory ISIT'97 Ulm, Germany (June 29-July 4 1997):111–.

[51] P. Guinand, J. Lodge, *Tanner type codes arising from large girth graphs*, Canadian Workshop on Information Theory CWIT '97, Toronto, Ontario, Canada (June 3-6 1997):5–7.

[52] J. Hemmeter, *Distance regular graphs and halved graphs*, Europ. J. Comb, 1986, P. 119-130.

[53] E. Hewitt, K.Ross, *Abstract harmonic analysis*, vol.2. Structure and analysis for compact groups. Analysis on locally compact abelian groups , Springer, 1970, 392 p.

[54] E. Hewitt, K. Ross, *Abstract Harmonic Analysis: Volume 1*: Structure of Topological Groups. Integration Theory. Group Representations, Springer, 1994, 540 p.

[55] D. Hilbert, *The Foundations of Geometry* ,translation by E. Townsend, University of Illinoie, 1950

[56] H. Hiller, *Geometry of Coxeter groups*, Research Notes in MATH., Pitman, New York, 1982.

[57] S. Hoory, N. Linial, and A.Wigderson, *Expander graphs and their applications*, Bulletin (New Series) of AMS, volume 43, N4, 439-461,

[58] W. C. Huffman, V. Pless, *Fundamentals of error correcting codes*, first edition, Cambridge University Press, Cambridge, 2003.

[59] W. Imrich, *Explicit construction of graphs without small cycles*, Combinatorica 2 (1984) 53–59.

[60] A. Ivanov, M. Muzichuk, V. Ustimenko, *On a new family of (P and Q)-polynomial schemes*, European J. Comb., 10, 1989, p. 337 -345.

[61] Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles* , Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.

[62] K. Jordan, *Traite des substitutions et des equations algebraiques* (1870), Paris, Gauthier Villars, 1961.
[63] V. Kac. *Infinite dimensional Lie algebras*, Birkhauser, Boston, 1983.
[64] V. Kac, *Fourteen Lectures on Infinite Dimensional Lie algebras*, Boston, Birkhauser, 1988, 412 pp.
[65] V. Kac, *Infinite root systems*, representations of graphs and invariant theory, Inv. Math., 56, 1980, P. 57-92.
[66] L. Kaluznin, V. Suschansky, V. Ustimenko, *On the use of Computers in permutation group theory and its applications*, Cybernetics, 1982, N6, pp. 93-94.
[67] W. Kantor, *Linear groups containing a Singer cycle"*, J. of Algebra 62, 1982, 232-234.
[68] A. Kipnis, A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, CRYPTO 99, LNCS Vol. 1666, pp. 19-30, 1999.
[69] M. Klisowski, U. Romańczuk, V. Ustimenko, *On the implementation of cubic public keys based on new family of algebraic graphs*, Annales UMCS Informatica AI XI, 2 (2011) p. 127-141;
[70] M. Klisowski, V. Ustimenko, *On the public keys based on the extremal graphs and digraphs*, International Multiconference on Computer Science and Informational Technology, October 2010, Wisla, Poland, CANA Proceedings.
[71] M. Klisowski, V. Ustimenko, *On the cubical multivariate cryptosystem over the boolean ring*, (to apper)
[72] M. Klisowski, V. Ustymenko, *On the implementation of cubic public keys based on algebraic graphs over the finite commutative rings and their symmetries*, Albanian Journal of Mathematics, Vol 5, No 3 (2011), 139-149
[73] M. Klisowski, V. Ustimenko, *On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator*, Mathematics in Computer Science, 2012, Volume 6, Number 2, Pages 181-198
[74] N. Koblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.
[75] N.Koblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.
[76] J. Kotorowicz, V. A. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condenced Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimerz Dolny, Poland, 2006, 11 (no. 2(54)) (2008) 347–360.
[77] J. S. Kotorowicz, V. Ustimenko, U. Romaúczk, *On the implementation of stream ciphers based on a new family of algebraic graphs*, IEEE Computer Society Press, Proceedings of the Conference CANA, FedSCIS, 2011 , pp. 485-490.
[78] F. Lazebnik, V. A. Ustimenko, *New Examples of graphs without small cycles and of large size*, Europ. J. of Combinatorics, 14 (1993) 445-460.
[79] F. Lazebnik, V. Ustimenko, *Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science, V. 10 (1993), 75-93.
[80] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *Properties of certain fam-*

ilies of $2k$*-cycle free graphs*, J. Combin. Theory, ser B, 60, No. 2 (1994), 293-298.

[81] F. Lazebnik, V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.

[82] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[83] F. Lazebnik, V.A. Ustimenko, A.J. Woldar, *A characterisation of the components of the graph* $D(k, q)$, Discrete Mathematics, 157 (1996), 271-283.

[84] F. Lazebnik,V.A. Ustimenko, A.J. Woldar, *New upper bounds on the order of cages*, Electronic J. Combin. 14 R13 (1997), 1–11.

[85] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *Polarities and* $2k$*-cycle-free graphs*, Discrete Mathematics, 197/198, (1999), 503–513.

[86] Lih-Chung Wang, Bo-yin Yang, Yuh-Hua Hu, Feipei Lai, *A Medium- Field Multivariate Public key Encryption Scheme*, CT-RSA 2006: The Cryptographers Track at the RSA Conference 2006, LNCS 3860, 132- 149, Springer, 2006

[87] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[88] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi and D. A. Spielman, *Improved Low-Density Parity-Check Codes Using Irregular Graphs and Belief Propagation*, in ISIT 98-IEEE International Symposium of Information Theory, p 171, Cambridge, USA,1998.

[89] D. J. C. MacKay, R. M. Neal, *Good Codes Based on Very Sparse Matrices*, in Cryptography and Coding 5th IMA Conference, pp. 100-111, Berlin, 1995.

[90] D. J. C. MacKay, *Good error correcting codes based on very sparse matrices*, IEEE Trans. Information Theory, pp. 399-431, March 1999.

[91] D. MacKay and M. Postol, *Weakness of Margulis and Ramanujan Margulis Low Dencity Parity Check Codes*, Electronic Notes in Theoretical Computer Science, 74 (2003), 8pp.

[92] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory*, Interscience publ., 1966.

[93] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.

[94] G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatsii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.

[95] M. Margulis, *Arithmetic groups and graphs without short cycles*, 6th Intern. Symp. on Information Theory, Tashkent, abstracts, vol. 1, 1984, pp. 123-125 (in Russion).

[96] T. Matsumoto, H. Imai H, *Public quadratic polynomial-tuples for efficient signatureverification and message-encryption*, Eurocrypt 88, Springer-Verlag (1988), pp. 419-453.

[97] T. Moh, *A public key system with signature and master key functions*, Commun. Algebra, vol. 27, no. 5, pp. 2207-2222, 1999.

[98] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Springer Verlag, New York, 1971.

[99] B. Mortimer, *Permutation groups containing affine of the same degree*, J. London Math. Soc., 1971, 15, N3, 445-455.
[100] E. H. Moore, *Tactical Memoranda*, Amer. J. Math., v.18, 1886, 264-303.
[101] Jose M. F. Moura, Jin Lu, and Haotian Zhang, *Structured LDPC Codes with Large Girth*, IEEE Signal Processing Magazine, vol. 21:1, pp.42-55, January 2004. Included in Special Issue on Iterative Signal Processing for Communications.
[102] R. M. Neal, *Software for Low Density Parity Check (LDPC) codes*, available form: `http://www.cs.utoronto.ca/ radford/ldpc.software.html`, 2012.
[103] H. Niederreiter, Chaoping Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton University Press, 2009.
[104] A. Oniscik, *Parabolic factorization of semisimple algebraic graphs*, Math. Nachr, 104, 1981, p. 315-329.
[105] R. Ore, *Graph theory*, Wiley, London, 1971
[106] J. Patarin, *Cryptoanalysis of the Matsumoto and Imai public key scheme of the Eurocrypt '88*, Advances in Cryptology, Eurocrypt '96, Springer Verlag, 43-56.
[107] J. Patarin, *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88*, Advances in Cryptology-Crypto 95, Springer-Verlag, 248-261.
[108] J. Patarin, *Hidden Field equations (HFE) and isomorphism of polynomials (IP): two new families of asymetric algorithms*, Advances in cryptology-Eurocrypt 96, Springer-Verlag, pp. 33-48.
[109] J. Patarin, *Asymmetric cryptography with a hidden monomial*, Advances in Cryptology- Crypto 96, Springer-Verlag, pp. 4560.
[110] J. Patarin, N.T. Courtois, L. Goubin, *FLASH, a fast multivariate signature algorithm*, in CT-RSA01, 2001, LNCS Vol. 2020, pp. 298-307.
[111] D. Petersen, V. Kac, *Infinite flag varieties and conjugancy theorems*, Proc. Math. Acad. Sci, Usa, V. 80, p. 1778-1782.
[112] S. Payne and J. Thas, *Finite generalised quadrangles*, Pitman, New York, 1985, 456 p.
[113] P. Rajesh, B. Singh, K. Sarma, A. Saiki, *Public key cryptography using Permutation P-Polynomials over Finite Fields*, IACR Cryptology ePrint Archive, Vol. 2009 (2009), p. 208.
[114] P. Ribenboim, *The new book of prime number records*, 3rd edition, Springer-Verlag, New York, NY, 1995, 541 p.
[115] T. Richardson, R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.
[116] M. Polak, V. Ustimenko, *On LDPC Codes corresponding to affine parts of generalized polygons*, Annales UMCS Informatica AI X1, 2 (2011), 143-150.
[117] M. Polak , V. Ustimenko, *LDPC Codes Based on Algebraic Graphs* , Annales UMCS Informatica AI (to appear).
[118] M. Polak, V. Ustimenko, *On LDPC Codes Corresponding to Infinite Family of Graphs A(k,K)*, Proceedings of the Federated Conference on Computer Science and Information System (FedCSIS), CANA 2012 (to appear).
[119] U. Romańczuk, V. Ustimenko, *On the key exchange with new cubical maps*

based on graphs, Annales UMCS Informatica AI, Volume 11, Number 4 , 2011.

[120] U. Romańczuk, V. Ustimenko, *On Families of Graphs of Large Cycle Indicator, Matrices of Large Order and Key Exchange Protocols With Nonlinear Polynomial Maps of Small Degrees*, Mathematics in Computer Science, 2012, Volume 6, Number 2, Pages 167-180.

[121] U. Romańczuk, V. Ustimenko, *On the key exchange with new cubical maps based on graphs*, Annales UMCS Informatica AI XI, 4 (2011) p. 11-19.

[122] U. Romańczuk, V. Ustimenko, *On the family of cubical multivariate cryptosystems based on algebraic graph over finite fields of characteristic 2*, Annales UMCS Informatica AI (to appear).

[123] H. Sachs, Regular graphs with given girth and restricted circuits, J. London. Math. Soc. 38 (1963), 423-429.

[124] N. Sauer. *Extermaleigenschaften regularer Graphen gegebener Taillenweite*, 1, 2, Osterreich. Acad. Wiss. Math. Natur. Kl. S. -B 2, 176 (1967), 9-25, 27-43.

[125] C. Shevalley, *On some simple groups*, Matematika, 2;1 (translation in Russion), p. 3-57. Computer Security, Prentice Hall 1989, 379 p.

[126] J. P. Serre, *Lie Algebras and Lie groups*, N. Y., Lectures in Math., Springer, Berlin, 1974.

[127] J. P. Serre, *Trees*, Springer, 2003.

[128] T. Shaska , W C Huffman, D. Joyner, V Ustimenko (Editors), *Advances in Coding Theory and Crytography* (Series on Coding Theory and Cryptology) World Scientific Publishing Company, 2007.

[129] T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra and its Applications Article, Volume 430, Issue 7, 1 April 2009, Special Issue in Honor of Thomas J. Laffey.

[130] T. Shaska and V. Ustimenko, *On some applications of graph theory to cryptography and turbocoding*, Special issue of Albanian Journal of Mathematics:Proceedings of the NATO Advanced Studies Institute "New challenges in digital communications", May 2008, University of Vlora, 2008, v.2, issue 3, 249-255.

[131] M. Simonovitz, *Extermal Graph Theory* , In "Selected Topics in Graph Theory", 2, edited by L. W. Beineke and R. J. Wilson, Academic Press, London, 1983, pp. 161-200.

[132] R. Steinberg, *Lectures on Shevalley groups*, Yale University, 1967, 554 pp.

[133] C.E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal Vol. 27 (1948):379–423, 623–656.

[134] C. E. Shannon, W. Warren, *The Mathematical Theory of Communication*, Univ Of Illinois Pr 1963.

[135] A. Shokrollahi, *LDPC Codes: An Introduction*, Digital Fountain Inc, Fremont (2002), available from: `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.1008`.

[136] M. Sipser, D. A. Spielman, *Expander codes*, IEEE Trans on Info Theory, 42, No. 6, pp. 1710-1722, November 1996.

[137] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.

[138] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.

[139] J. A. Thas, *Generalised polygons*, in F. Buekenhout (ed), Handbook in Incidence Geometry, Ch. 9, North Holland, Amsterdam, 1995.

[140] J. Tits, *Sur la trialite at certains groupes qui s'en deduicent*, Publ. Math. I.H.E.S. 2 (1959), 15-20.

[141] J. Tits, *Les groupes simples de Suzuki et de Ree*, Seminaire Bourbaki 13 (210), 1960/1961, 1-18.

[142] J. Tits, *Buildings of spherical type and Finite BN-pairs*, Lecture Notes in Math, Springer Verlag, 1074.

[143] J. Tits, *Buildings and Buekenhout geometries*, Finite Simple Group 2, Symp. Durham, July-August, 1978, Proc. London Math. Soc., 1980,p. 309-320.

[144] A. Touzene, V. Ustimenko, *Graph Based Private Key Crypto System*, International Journal on Computer Research, Nova Science Publisher, volume 13 (2006), issue 4, 12p.

[145] V. D. Tonchev, *Error-correcting codes from graphs*, Discrete Math. 257 (2002), 549-557.

[146] A. Touzene, V. Ustimenko,*Private and Public Key Systems Using Graphs of High Girth*, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008, pp.205-216

[147] A. Touzene, V. Ustimenko, Marwa AlRaissi, Imene Boudelioua, *Performance of algebraic graphs based stream-ciphers using large finite fields*, Annales UMCS, Informatica IssueVolume 11, Number 2 / 2011, 81-93

[148] W. Tutte, *A family of cubical graphs*, Proc. Cambridge Philos. Soc. 43 (1945).

[149] V. A. Ustimenko, *On some properties of Chevalley groups and their generalisations*, In: Investigations in Algebraic Theory of Combinatorial objects, Moskow, Institute of System Studies, 1985, 134 - 138 (in Russian), Engl.trans.: Kluwer, Dordrecht, 1992, pp. 112-119

[150] V. A. Ustimenko, *Geometries of twisted simple groups of Lie type as objects of linear algebra*, in Questions of Group Theory and Homological Algebra, University of Jaroslavl, Jaroslavl, 1990, 33-56 (in Russian).

[151] V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukraine Math. J. 43, Nos. 7,8 (1991), pp. 1055–1060 (in Russian).

[152] V. A. Ustimenko, *Coordinatisation of regular tree and its quotients*, in "Voronoi's impact on modern science", eds P. Engel and H. Syta, book 2, National Acad. of Sci, Institute of Matematics, 1998, 228p.

[153] V. A. Ustimenko, *On the Varieties of Parabolic Subgroups, their Generalizations and Combinatorial Applications*, Acta Applicandae Mathematicae 52 (1998): pp. 223–238.

[154] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, 2001, v. 2227, 278-287.

[155] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.

[156] V. Ustimenko, A. Woldar, *Extremal properties of regular and affine generalised polygons of tactical configurations*, European Journal of Combinatorics, 24 (2003) 99–111.

[157] V. Ustimenko, *Maximality of affine group and hidden graph cryptsystems*,

Journal of Algebra and Discrete Mathematics, October, 2004, v.10, pp. 51-65.

[158] V. Ustimenko, *Small world graphs with memory and Coxeter groups*, technical report 110/05 of the Centre of Mathematical Sciences, Madeira University, Portugal, July, 2005, 12 p.

[159] V. A. Ustimenko, *On the graph based cryptography and symbolic computations*, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).

[160] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

[161] V. A. Ustimenko, *On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography*, Albanian. J. of Mathematics, Special Issue "Algebra and Computational Algebraic Geometry", vol. 1, N4, 387-400, 2007

[162] V. A. Ustimenko, *On the hidden discrete logarithm for some polynomial stream ciphers*, International Multiconference on Computer Science and Informational Technology, 20-22 October 2008, Wisla, Poland, CANA Proceedings.

[163] V. A. Ustimenko, J. Kotorowicz, *On the properties of Stream Ciphers Based on Extremal Directed graphs*, In "Cryptography Research Perspectives", Nova Publishers, Ronald E. Chen (the editor), 2008.

[164] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.

[165] V. A. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, in Algebraic Aspects of Digital Communications, IOS Press (Lectures of Advanced NATO Institute, NATO Science for Peace and Security Series - D: Information and Communication Security, Volume 24, July 2009, 296 pp.

[166] V. Ustimenko, *On the embeddings of some geometries and flag systems in Lie algebras and superalgebras*, in "Root systems, representations and geometries", Kiev, IM AN UkrSSR, pp. 3–16, 1990.

[167] V. Ustimenko, *Small Schubert cells as subsets in Lie algebras*, Functional Analysis and Applications, v. 25, no. 4, 1991, pp. 81–83.

[168] V. Ustimenko,*Geometries of twisted groups of Lie type as objects of linear algebra*, Voprosi teorii grupp i gomologicheskoi algebry, 1990, pp. 33–56.

[169] V. Ustimenko, *Calculations in Coxeter groups and corresponding geometrical objects*, Ukr. Math. J., v.43, no. 7–8, 1991, pp. 1055–1060.

[170] V. Ustimenko, *Affine system of roots and Tits geometries*, Voprosy teorii grupp i gomologicheskoy algebry, Yaroslavl, 1989, pp.155-157 (in Russian).

[171] V. Ustimenko, *Groups, quasigroups and Tits geometries, in Questions of Algebra*, 4, Minsk, 1989, 21 p. (Procedings of the 10-th All Union symposium on group theory, Gomel, 1986), Minsk. (in Russian).

[172] V. Ustimenko, *On the maximality of finite Chevalley groups acting on conjugacy classes of parabolic subgroups*, DAN USSR, v.275, 4, 1984, pp. 809-813 (in Russian).

[173] V. Ustimenko, *Maximality of the group $PGL_n(q)$ acting on subspaces of dimension m*, DAN USSR, vol. 240, no. 6, 1978, pp. 769–772.

[174] V, Ustimenko,*Division algebras and Tits geometries*, DAN USSR, v. 296, no. 5, 1987, pp.1061-1065 (in Russian).

[175] V. Ustimenko, U. Romańczuk, *On Dynamical Systems of Large Girth or Cycle Indicator and their applications to Multivariate Cryptography*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Volume 427, Springer, 2013, p. 231-256.

[176] V. Ustimenko, U. Romańczuk, *On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, 2013, Volume 427, p. 257-285.

[177] V. Ustimenko, *Extremal Graph Theory and Symbolic Computations*, Dopovidi of Nath. Acad of Sci. of Ukraine (to appear)

[178] V. Ustimenko *Algebraic graphs and security of digital communications*, Institute of Computer Science, University of Maria Curie Sklodowska in Lublin, 2011, 151 p (oppen access book supported by European Social Foundation), available at the UMCS web.http : //informatyka.umcs.lublin.pl/files/ustimenko.pdf.

[179] V. Ustimenko, A. Wróblewska, *On the key exchange with nonlinear polynomial maps of degree 4*, Albanian Journal of Mathematics, Special Issue, Applications of Computer Algebra 2010, Vol 4, No 4 (2010), December 2010.

[180] V. Ustimenko, A. Wróblewska, *On the key expansion of D(n;K)-based cryptographical algorithm*, Annales UMCS Informatica AI XI, 2 (2011), 95-111.

[181] V. Ustimenko, A. Wóblewska, *Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography*, Annales UMCS Informatica AI (to appear)

[182] V. Ustimenko, A. Wróblewska, *On the key exchange with nonlinear polynomial maps of stable degree*, (to appear)

[183] R. Wenger, *Extremal graphs with no C^4, C^6 and C^{10}s*, 1991, J. Comb. Theory, Ser B, 52, 113-116.

[184] A. Wróblewska, *On some properties of graph based public keys* , Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234p.

[185] H. Wielandt, *Finite permutation groups*, Acad. Press, New York, 1964, 312p.

[186] R. Weiss, *Distance transitive graphs and generalised polygons*, Arch. Math, 45, 1985, pp.186-192.

[187] Zhengya Zhang, Pamela Lee, Venkat Anantharam, Borivoje Nikolic, Martin Wainwright, Lara Dolecek, *Predicting error floors of structured LDPC codes: deterministic bounds and estimates*, Journal IEEE Journal on Selected Areas in Communications - Special issue on capaciyy approaching codes archive Volume 27 Issue 6, August 2009, Pages 908-917.

[188] V. Zdan-Pushkin, V. Ustimenko, *Maximality of finite classical groups acting on totally isotropic subspaces*, Selecta Mathematica Sovietica, 9, N4, 1990, p.339-354.

[189] V. Zdan-Pushkin, V. Ustimenko, *On the maximality of some classical trans-*

formation groups, Voprosy teorii grupp i gomologicheskoj algebry, Jaroslavl, 1985, pp. 125-139.

[190] V. Zdan-Poushkin, V. Ustimenko, *Classical groups and metrical association schemes*, Cybernetics, N6, 1986, pp. 83-94.

[191] Yuming Zhu, Chaitali Chakrabarti, *Architecture-aware LDPC code design for multiprocessor software defined radio systems*, Journal IEEE Transactions on Signal Processing archive Volume 57 Issue 9, September 2009 Pages 3679-3692.

Index