Linear Algebra and its Applications 430 (2009) 1826–1837

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

On the homogeneous algebraic graphs of large girth and their applications

T. Shaska [a], V. Ustimenko [b,*]

[a] *Department of Computer Science and Electrical Engineering, University of Vlora, Vlora, Albania*

[b] *Institute of Mathematics, The University of Maria Curie, Sklodowska, Lublin, Poland*

ARTICLE INFO

Article history:
Received 4 February 2008
Accepted 15 August 2008
Available online 5 October 2008

Submitted by V. Mehrmann

Dedicated to Thomas Laffey on the occasion of his 65th birthday.

AMS classification:
15A63
14Q15
05d99

Keywords:
Extremal graphs
Algebraic varieties
Coding theory
Cryptography

ABSTRACT

Families of finite graphs of large girth were introduced in classical extremal graph theory. One important theoretical result here is the upper bound on the maximal size of the graph with girth $\geqslant 2d$ established in even circuit theorem by Erdös. We consider some results on such algebraic graphs over any field. The upper bound on the dimension of variety of edges for algebraic graphs of girth $\geqslant 2d$ is established. Getting the lower bound, we use the family of bipartite graphs $D(n,K)$ with $n \geqslant 2$ over a field K, whose partition sets are two copies of the vector space K^n. We consider the problem of constructing homogeneous algebraic graphs with a prescribed girth and formulate some problems motivated by classical extremal graph theory. Finally, we present a very short survey on applications of finite homogeneous algebraic graphs to coding theory and cryptography.

1. Introduction: two optimisation problems

We study extremal graphs and their applications to coding theory, cryptography, and quantum computations. The main object of consideration is a homogeneous algebraic graph defined in terms of algebraic geometry in the following way.

Let F be a field. Recall that a *projective space* over F is a set of elements constructed from a vector space over F such that a distinct element of the projective space consists of all non-zero vectors which

* Corresponding author.
E-mail addresses: shaska@univlora.edu.al (T. Shaska), vasyl@hektor.umcs.lublin.pl (V. Ustimenko).

0024-3795/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2008.08.023

are equal up to a multiplication by a non-zero scalar. Its subset is called a *quasiprojective variety* if it is the set of all solutions of some system of homogeneous polynomial equations and inequalities.

An *algebraic graph* ϕ over F consists of two things: the *vertex set* Q being a quasiprojective variety over F of nonzero dimension, and the *edge set* being a quasiprojective variety ϕ in $Q \times Q$ such that $(x,x) \notin \phi$ for each $x \in Q$ and $x\phi y$ implies $y\phi x$ ($x\phi y$ means $(x,y) \in \phi$). The graph ϕ is *homogeneous* (or *M-homogeneous*) if for each vertex $v \in Q$ the set $\{x \mid v\phi x\}$ is isomorphic to some quasiprojective variety M over F of nonzero dimension. The reader can find the general conception of algebraic graphs [4].

We assume that the field F contains at least 5 elements. If F is finite then the vertex set and the edge set are finite and we get a usual finite graph.

The *cycle* C_t in ϕ is a sequence $x_1, x_2, \ldots, x_t$ of distinct elements of Q such that $x_1\phi x_2$, $x_2\phi x_3$, $\ldots$, $x_{t-1}\phi x_t$, $x_1\phi x_t$ are edges of the graph.

We define the girth $g = g(\phi)$ of a graph ϕ as the length of its minimal cycle. If ϕ is without cycles then $g(\phi) = \infty$.

The paper is devoted to the following two optimization problems:

(A) Let Q be a M-homogeneous graph such that $\dim M = k$ over F and its girth is a finite number g. What is the minimal possible dimension $v_a(k,g)$ for the variety of vertices?

(B) Let ϕ be a homogeneous graph of girth $g \geqslant t$ and $\dim M = k$. What is the maximal possible dimension of ϕ?

Problems (A) and (B) are related to each other, in case of finite field we can change the dimension of Q and ϕ on their cardinalities and get classical problems on minimal order of regular simple graph of given degree and given girth (analogue of A) and maximal size (number of edges) of the graph with girth $\geqslant t$ (analogue of B).

So (A) and (B) are motivated by the branch of extremal graph theory which studies order of cages, related bounds, cages itself, bounds on maximal number of edges of the graph of given order and girth, and families of graphs of large girth (see Section 2).

In Section 3 we consider an analogue of Tutte's bound and variants of Erdös' even circuit theory for homogeneous graphs, and define the family of algebraic graphs of large girth over an arbitrary field. Examples of extremal algebraic graphs of bounded dimension are presented. We formulate some open problems for general homogeneous graphs motivated by classical extremal graph theory.

In Section 4 we consider examples of families of algebraic graphs of large girth over fields and establish the upper bound on the minimal dimension of the vertex set for the graph of prescribed girth g.

In Section 5 we consider properties of some homogeneous algebraic graphs of prescribed girth in detail, from the algebraic geometry point of view. We are applying the "Mathematica" package for investigation of variety of all vertices or variety of vertices at certain distance from the chosen point.

In Section 6 we discuss applications of finite regular algebraic graphs in Coding theory and Cryptography. We hope that the construction of homogeneous algebraic graphs over $\mathbb{C}$ and over the ring of Gaussian numbers can be used in quantum coding theory [1] and quantum cryptography [53].

2. Dense finite graphs of large girth and of large size

All graphs that 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 a finite graph G, respectively. The number of vertices $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When it is convenient, we identify G with the corresponding symmetric antireflexive binary relation Φ on $V(G)$, i.e. Φ is a subset of $V(G) \times V(G)$. The *length* of a path is the number of its edges.

The *girth* of a graph G, denoted by $g = g(G)$, is the length of a shortest cycle in G. Let $k \geqslant 3$ and $g \geqslant 3$ be 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 $v(k,g)$ 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, Tutte [9] established the following classical lower bounds for $v(k,g)$:

$$v(k,g) \geqslant k(k-1)^{(g-1)/2}/(k-2) \quad \text{for } g \text{ odd}, \quad k \geqslant 4,$$

$$v(k,g) \geqslant 2(k-1)^{g/2-2}/(k-2) \quad \text{for } g \text{ even}, \quad k \geqslant 4.$$

The graphs of odd girth for which equality holds are called *Moore graphs*. Each Moore graph with valency $k = 2$ is a polygon and each $(2d+1)$-gon is a Moore graph. Damerell proved that Moore graph with valency $k \geqslant 3$ has a diameter 2 and $k \in \{3, 7, 57\}$. There are unique examples for $k = 3$ (the Petersen graph) and $k = 7$ (Hoffman-Singleton graph). No example with $k = 57$ is known, see [9].

The problem of determining $v(k,g)$ was posed in 1959 by Kartesi who observed that $v(3,5) = 10$ was realized by the Petersen graph (see [9]). The classical extremal graph theory studies extremal properties of simple graphs. Let F be family of graphs none of which is isomorphic to a subgraph of the graph Γ. In this case we say that Γ is F-free. Let P be certain graph theoretical property. By $\mathrm{ex}_P(v,F)$ we denote the greatest number of edges of F-free graph on v-vertices that satisfies property P. If P is just a property to be simple graph we omit index P and write $\mathrm{ex}(v,F)$. The reader can find the missing definitions in extremal graph theory in [7,10], or [33].

This theory contains several important results on $\mathrm{ex}(v,F)$, where F is a finite collection of cycles of different length. The following statement had been formulated by Erdös: let C_n denote the cycle of length n, then

$$\mathrm{ex}(v, C_{2k}) \leqslant Cv^{1+1/k},$$

where C is an independent positive constant.

For the proof of this result and its generalizations see [8,13]. In [12] the upper bound

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2k}, C_{2k+1}) \leqslant (1/2)^{1+1/k} v^{1+1/k} + \mathrm{O}(v) \tag{1}$$

was established for all integers $k \geqslant 1$. Both bounds are known to be sharp for $k = 2, 3, 5$; in other cases the question on the sharpness is open (see [7,33] and further references).

Let us consider the family of graphs G_i of degree l_i and unbounded girth g_i such that

$$g_i \geqslant \gamma \log_{l_i - 1}(v_i).$$

The last formula means that G_i, $i = 1, 2, \ldots$, form an infinite *family of graphs of large girth* in the sense of Biggs [3]. The order of graphs from such a family is close to the lower bound on $v(k,g)$, but their size is close to 1. The last bound shows that $\gamma \leqslant 2$ but no family has been found for which $\gamma = 2$. Bigger γ corresponds to the larger girth.

For many years the only significant results were the theorems of Erdös and Sachs [11,30] and their improvements by Sauer [31], Walther [54,55], and others (see [7] for more details and references), who proved the existence of infinite families with $\gamma = 1$ by using nonconstructive methods. The reader can find the essential improvement of the upper bound in [22]. The first explicit examples of families with large girth were given by Margulis [27,28] with $\gamma = 0.44$ for some infinite families with an arbitrary large valency, and $\gamma = 0.83$ for an infinite family of graphs of valency 4. The constructions were Cayley graphs of $\mathrm{SL}_2(Z_p)$ with respect to special sets of generators. Imrich [20] improved the result for an arbitrary large valency, $\gamma = 0.48$, and constructed 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 [6]. They conjectured that these graphs have large girth. Weiss [56] proved the conjecture by showing that $\gamma \geqslant 4/3$ for the sextet graphs or their double covers. Then independently Margulis and Lubotsky, Phillips, and Sarnak [25] came up with similar examples of the graphs $X^{p,q}$ with $\gamma \geqslant 4/3$ and an arbitrary large valency (they turned out to be so-called Ramanujan graphs, additionally). Biggs and Boshier [5] showed that γ is asymptotically 4/3 for such graphs. The graphs $X^{p,q}$ are Cayley graphs of the group $\mathrm{PSL}_2(Z_q)$ with respect to a set of $p+1$ generators (p and q are special primes congruent to 1 mod 4).

The first family of connected algebraic graphs over F_q of a large girth and arbitrarily large degree had been constructed in [23]. These graphs are $CD(k,q)$ as above, where k is growing integer $\geqslant 2$ and odd prime power q is fixed. They had been constructed as connected components of graphs $D(k,q)$ defined earlier in [21], see also [24]. For each q, the graphs $CD(k,q)$, $k \geqslant 2$ form a family of large girth with $\gamma = 4/3 log_{q-1} q$ of degree q. The reader can find in [51] some new examples of simple algebraic graphs with memory of large girth and arbitrary large degree.

Notice that the graphs $X^{p,q}$ are not algebraic because the neighbourhood of a vertex is not an algebraic variety over F_q of dimension $\geqslant 1$. The problem of estimation of order of cages is dual to problem on the maximal size of graphs of the given girth g.

3. Algebraic analogue of Erdös' even-circut theorem

Let G be a quasi homogeneous graph defined on manifold $V(F)$, where F is a field (see Section 1). We say that G is a *homogeneous algebraic graph* if the neighbourhood of each vertex v from $V(F)$ is isomorphic to the algebraic variety $N(F)$. Furthermore, we always consider graphs with more than 2 neighbours for each vertex.

Theorem 3.1. *Let G be quasi homogeneous algebraic graph over a field F of girth g such that the dimension of neighbourhood for each vertex is N, $N \geqslant 1$. Then*

$$[(g-1)/2] \leqslant \dim(V)/N.$$

Proof. Assume that $[(g-1)/2] = k > \frac{\dim V}{\dim N(F)}$. Let v be a vertex and M be the variety of elements at distance k from v. The absence of cycles C_s, $1 \leqslant s \leqslant 2k$, means that each element from M is connected with v by the unique pass. Elements of M are in one to one correspondence with such passes. Let $N_v(F)$ be a neighbourhood of v. A *pass* is a sequence $v, u_1, u_2, \ldots, u_k$, where $u_1 \in N_v(F), u_2 \in N_{u_1}(F) - \{u_1\}, \ldots, u_k \in N_{u_{k-1}}(F) - \{u_{k-1}\}$. So the dimension of M is $N \times k$. But $N \times k > \dim V$ by our assumption, so we get a contradiction. □

We can rewrite the above statement in the form similar to Tutte's inequalities as follows.

Corollary 3.2. *Let G be an algebraic (k,g)-graph, i.e. a homogeneous algebraic graph over a field F of girth g such that the neighbourhood of each vertex is isomorphic to variety $N(F)$ of dimension k. Then* $\dim V(G) \geqslant [(g-1)/2]k$.

The following form of Theorem 2 is an analogue of inequality 1.

Corollary 3.3. *Let G be a homogeneous graph over a field F and $E(G)$ be the variety of its edges. Then* $\dim(E(G)) \leqslant \dim V(G)(1 + [(g-1)/2]^{-1})$.

Indeed, $\dim(E(G)) = \dim(V) \times \dim(N(F))$. From the previous inequality we have $\dim(N(F)) \leqslant \dim V(G)[2/(g-1)/2]$. So $\dim(E(G)) \leqslant \dim(V) \times \dim V(G)[(g-1)/2] = \dim V(G)((1 + [(g-1)/2]^{-1})$.

Let $v(k,g,F)$ be the minimal dimension of the variety of vertices for algebraic (k,g)-graph defined over F. Let $v_a(k,g)$ be the minimal dimension of the variety of vertices for algebraic (k,g)-graph defined over some field F. We have

$$v_a(k,g) \geqslant [(g-1)/2]k. \tag{2}$$

The bi-homogeneous incident structure is a bipartite graph with partition sets P and L containing points and lines, respectively, such that there is a field F such that $P \cup L$ is an algebraic variety over F and neighbourhoods of each pair of points (lines) are isomorphic algebraic varieties over F as well. Tits [37] defined generalized m-gon as a graph of diameter m and girth $2m$, see also [36,38,46].

We use the term *bi-homogeneous generalized polygon* for a bi-homogeneous incident structure which is a generalized polygon.

Theorem 3.4. *The equalities $v_a(n,6) = 2n$, $v_a(n,8) = 3n$ and $v_a(n,12) = 5n$, $n \geqslant 1$ hold.*

Proof. From the previous theorem we have $v_a(n,6) \leqslant 2n$, $v_a(n,8) \leqslant 3n$ and $v_a(n,12) \leqslant 5n$. Let G be Shevalley group of rank 2 defined over a field F which is an n-dimensional extension of field K. In particular, we can take $K = \mathbb{Q}$ or consider finite field $K = \mathbb{F}_p$, where p is prime, and define the exten-

sion via an irreducible polynomial of degree n. Let B be the standard Borel subgroup of G, P_1 and P_2 are standard parabolic subgroups of G, i.e. proper subgroups containing B. The geometry of G is the incidence structure with the point set $(G : P_1)$ and the line set $(G : P_2)$ consisting of left cosets gP_i, $i = 1, 2$. A point $p \in (G : P_1)$ and a line $l \in (G : P_2)$ are *incident* (pIl) if and only if the set theoretical intersection of cosets p and l is not empty. The simple graph of binary relation I is a homogeneous algebraic graph over $F = K^n$, the neighbourhood of each vertex is isomorphic to projective line over F. So the dimension of neighbourhood over K is n. It is well known that graph I is an algebraic generalized m-gon. For each field F we have the following options:

(i) $G = A_2(F)$ (classical linear group $PSL_2(F)$), $m = 3$.
(2i) $G = B_2(F)$ (classical projective symplectic group $PSp_4(F)$), $m = 4$.
(3i) $G = G_2(F)$ (well known Dixon group over F), $m = 6$.

The projective variety $(G : P_1) \cup (G : P_2)$ has dimension $m - 1$ over the field F. So for each $m \in \{3, 4, 6\}$ we have an example of algebraic (n, g)-graph of dimension $n(m - 1)$. So $v_a(n, 2m) = n(m - 1)$ for $m \in \{3, 4, 6\}$. □

Let $e(g, n)$ be the maximal dimension of the variety of edges of homogeneous algebraic graph of girth g with the n-dimensional variety of vertices. The following equalities are dual to equalities of the above theorem.

Corollary 3.5. *The following equalities hold:* $e(6, n) = n + n/2$ *for even* n, $n \geqslant 2$, $e(8, n) = n + n/3$ *for* $n = 3s$, $s = 1, 2, \ldots$, *and* $e(12, n) = n + n/5$ *for* $n = 5s$, $s = 1, 2, \ldots$

The following open problems are interesting:
(i) Find all values of girth g for which the lower bound (2) is sharp.
(ii) Find all values m for which there exist homogeneous algebraic generalized polygons. The word 'algebraic' is strict here, the polygon has to be a homogeneous algebraic graph in a sense of the above definition, i.e. neighbourhoods of each two vertices are isomorphic.

From the existence of homogeneous generalized m-gon follows that the bound (2) is sharp in case of girth $2m$.

As follows from [14], finite bi-homogeneous generalized m-gons are exist if $m \in \{3, 4, 6, 8\}$ (see [9]). Recall the assumption that each vertex of the graph contains at least three neighbours. Tits and Weiss [38] classified all bi-homogeneous generalized m-gons with Moufang property.

Conjecture 3.6. *Equality* $v_a(k, g) = [(g - 1)/2]k$ *implies* $g \in \{6, 8, 12\}$.

We define the family of algebraic graphs of large girth G_i, $i = 1, 2, \ldots$ over the field F if the $\dim V(G_i)$ is growing and the girth of $G_i \geqslant c \cdot \frac{\dim V(G_i)}{\dim N(G_i)}$, where $c > 0$ is a constant independent of i. From Theorem 1 we get $c \leqslant 2$.

In the next section we prove the following upper bound on $v_a(k, 2s)$.

Theorem 3.7. *For each even* g, $g \geqslant 6$, *we have* $v_a(k, g) \leqslant k((3/4)g - \alpha)$, *where* $\alpha = 3, 5/2$ *for* $g = 0, 2 \bmod 4$, *respectively.*

The problem of finding the good upper bound for $v_a(k, 2s + 1)$ is very interesting. Algebraic $(k, 2s + 1)$-graphs such that the dimension of variety of vertices is $v_a(k, 2s + 1)$ are analogues of well known Moore graphs or cages with odd girth.

4. Explicit construction of algebraic graphs over general fields

Let K be any field, N be the totality of positive integers. Let us consider the subset $\Omega = \{(i, j) || i - j| \leqslant 1\}$ of the Cartezian product $Z^+ \times Z^+$. The elements of this set are in one-to-one correspondence with

the positive roots of the root system for the Kac–Moody algebra $\widetilde{A_1}$ over some field. If $|i-j|=1$ we may identify the pair (i,j) with the real root of $\widetilde{A_1}$. The pairs $(1,0)$ and $(0,1)$ corresponds to simple (or fundamental) roots. The set $\{(i,i)|i \geqslant 0\}$ can be identified with the totality of positive imaginary roots for $\widetilde{A_1}$.

Let us introduce the double $(i,i)'$ for each imaginary root (i,i) with $i \geqslant 1$. Let us denote the totality of all doubles as Ω', and consider the set $\text{Root} = \Omega \cup \Omega'$.

Let $A = K^{\text{Root}}$ be the totality of all functions from Root to the field K with the finite support. Each function can be written as formal linear combination of $\alpha_i \in \text{Root}$, $i = 1, \ldots, n$ with coefficients $x_i \in K$. We may identify elements α from K with the elements of the standard base for the vector space L. Let us define the linear algebra on A via alternating bilinear product $[,]$ (alternating property: $[x,y] = -[y,x]$) such that $[(1,0),(i,i)] = (i+1,i), [(0,1),(i,i)] = (i,i+1)', [(1,0),(i-1,i)] = (i,i), [(0,1),(i,i-1)] = (i,i)'$. The algebra $L, [,]$ is a Lie algebra, $P = A \cap K^{\text{Root}-\{(1,0)\}}$ and $L = A \cap K^{\text{Root}-\{(0,1)\}}$ are Abelian subalgebras. We introduce the incidence structure I with the point set P, line set L and incidence relation: point (p) is incident to line $[l]$ if the standard projection of vector $(p) - [l]$ onto $P \cup L$ is the Lie product $[p,l]$. 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 $[x] \in L$. Let p_α and l_α be the components of vectors (p) and $[l]$ in the standard basis of the free module K^{Root}:

$$(p) = (p_{0,1}, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots),$$
$$[l] = [l_{1,0}, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots).$$

It is easy to see that the point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$\begin{aligned}
&l_{11} - p_{11} = l_{1,0}p_{0,1},\\
&l_{12} - p_{12} = l_{11}p_{0,1},\\
&l_{21} - p_{21} = l_{1,0}p_{11},\\
&l_{ii} - p_{ii} = l_{1,0}p_{i-1,i},\\
&l'_{ii} - p'_{ii} = l_{i,i-1}p_{0,1},\\
&l_{i,i+1} - p_{i,i+1} = l_{ii}p_{1,0},\\
&l_{i+1,i} - p_{i+1,i} = l_{1,0}p'_{ii}.
\end{aligned} \tag{3}$$

The last four relations are defined for $i \geqslant 2$. This incidence structure (P, L, I) we denote as $D(K)$. 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 $(p)I[l]$. We can generalize the definition of $D(K)$ on the general commutative ring K by the definition of incidence of (p) and $[l]$ in the form of Eq. (3).

For each positive integer $k \geqslant 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. First, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all others. For fixed q, the incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k,K)$ (see [21,41]).

Let $\rho((p)) = p_{1,0} \in K$ and $\rho([l]) = l_{0,1} \in K$ be the colours of a point and a line, respectively. We can see that there is a unique neighbour of point (line) with the chosen colour a, and its components can be computed from the triangular system of linear equations. So if K is a finite set of cardinality b, the graphs $D(K)$ and $D(n,K)$ are b-regular.

Proposition 4.1 [21,41]. *Let K be an integral domain, and $k \geqslant 2$. Then for odd k, $g(D(k,K)) \geqslant k+5$.*

The reader can find in [51] the simplest proof of this statement. The following statement is proved in [15].

Theorem 4.2. *Let k be odd, and q be any prime power in the arithmetic progression $\{1 + n(k+5)/2\}$, $n = 1, 2, \ldots$ Then the girth of $D(k, F_q)$ is $k+5$.*

Let us consider some graph invariants for $D(k,K)$. To facilitate notation in future results, it is convenient to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0, p_{0,0} = l_{0,0} = -1, p'_{0,0} = l'_{0,0} = 1, l'_{1,1} = l_{1,1}, p'_{1,1} = p_{1,1}$, and to rewrite the system of Eq. (3) as follows:

$$
\begin{aligned}
&l_{ii} - p_{ii} = l_1 p_{i-1,i},\\
&l'_{ii} - p'_{ii} = l_{i,i-1} p_{0,1},\\
&l_{i,i+1} - p_{i,i+1} = l_{ii} p_{0,1},\\
&l_{i+1,i} - p_{i+1,i} = l_{1,0} p'_{ii}
\end{aligned}
$$

for $i = 0, 1, 2, \ldots$ Note that for $i = 0$, the four conditions as above are satisfied by every point and line, and for $i = 1$ the first two equations coincide and give $l_{1,1} - p_{1,1} = l_{1,0} p_{0,1}$.

Let $k \geqslant 6$, $t = [(k+2)/4]$, and let $u = (u_i, u_{11}, \ldots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \ldots)$ be a vertex of $D(k,K)$. We assume that $u_1 = u_{0,1}$ ($u_{1,0}$) if u be a point (a line, respectively). It does not matter whether u is a point or a line. For every r, $2 \leqslant r \leqslant t$, let

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

and $a = a(u) = (a_2, a_3, \ldots, a_t)$. The following statement was proved in [22,23] for the case $K = F_q$. Its generalization on arbitrary commutative rings is straightforward, see [51].

Proposition 4.3. *Let K be a commutative ring with unity and u and v be vertices from the same connected component of $D(k,K)$. Then $a(u) = a(v)$. Moreover, for any $t-1$ ring elements $x_i \in K$, $2 \leqslant t \leqslant [(k+2)/4]$, there exists a vertex v of $D(k,K)$ for which $a(v) = (x_2, \ldots, x_t) = (x)$.*

So the classes of equivalence for the relation $\tau = \{(u,v) \mid a(u) = a(v)\}$ on the vertices of the graph $D(n,K)$ are unions of connected components.

Theorem 4.4 [51]. *For each commutative ring with unity, the graph $D(k,K)$ is edge transitive.*

So all connected components of $D(n,K)$ are isomorphic to the same variety C over the ring K of dimension t. Let $C(t,K)$ be the induced subgraph whose vertex set is a class for τ. Then the girthes of $C(t,K)$ and $D(n,K)$ are equal.

Proposition 4.5 [51]. *The vertex set of $C = C(t,K)$ for t on the set $K^n \cup K^n$ is isomorphic to the affine variety $K^t \cup K^t$, where $t = [3/4n] + 1$ for $n = 0, 2, 3 \bmod 4$ and $t = [3/4n] + 2$ for $n = 1 \bmod 4$.*

Theorem 4.6. *Let k be odd, and P be the arithmetic progression $P = \{1 + n(k+5)/2\}$, $n = 1, 2, \ldots$ Then*

(i) *for each integrity ring F of prime characteristic $p \in P$ or 0 the girth of the graph $D(k,F)$ is $k+5$;*
(ii) *there is an integer function $n(k)$ such that for each commutative ring K with unity such that* $\mathrm{char}(K) \geqslant n(k)$ *the girth is at most $k+5$.*

Proof. We chose the prime p of the form $1 + mt$ for some $m = (k+5)/2$. The existence of p follows from the well known result of Dirichlet asserting the existence of infinitely many primes in arithmetic progressions. Then we get the existence of a cycle of length $k+5$ in $D(k,p)$. Let F be the integrity ring of characteristic p. Then F contains the prime field $\mathbb{F}_p$, so $D(k,p)$ can be considered as an induced subgraph of the graph $D(k,F)$. It means that $D(k,F)$ contains a cycle of length $k+5$ as well. This means that $g(D(k,F) \geqslant k+5$. It means that the girth of the graph $D(k,F)$ is exactly $k+5$.

The graph $D(k,Z)$ is edge transitive. So without loss of generality we may assume that a cycle contains the edge $(0)I[0]$. Let us consider the cycle of the length $k+5$ starting and ending at zero point (0) such that the colours of other consecutive elements are 0 (zero line), $x_1, x_1 + x_2, \ldots, x_1 + x_2 + \cdots + x_{k+4}$. The incidence of the last line of the colour $x_1 + x_2 + \cdots + x_{k+4}$ to point (0) can be written by the system of $k-1$ algebraic equations in variables $x_1, \ldots, x_{k+4}$:

$$f_1(x_1,\dots,x_{k+4}) = 0,\dots, f_{k-1}(x_1,\dots,x_{k+4}) = 0 \tag{4}$$

The incidence conditions imply that the absolute values of coefficients in the system are bounded by some function $t(k)$ depending on k only. Let us take a prime p in our arithmetic progression such that $p > 2t(k)$. The graph $D(k,\mathbb{F}_p)$ is edge transitive. So equations of its cycle of length $k+5$ can be written in the form

$$f_1(x_1,\dots,x_{k+4}) = 0 \bmod p,\dots, f_{k-1}(x_1,\dots,x_{k+4}) = 0 \bmod p.$$

For infinitely many primes from our arithmetical progression, the system above has a solution $x_1 = a_1 \neq 0$, $x_2 = a_2 \neq 0,\dots, x_{k+4} = a_{k+4} \neq 0$. From well known principle of arithmetics, we get that system (4) has such a solution as well. It means that graph $D(k,Z)$ contains a cycle of length $k+5$.

Let F be integrity ring of characteristic zero. We can view $D(k,Z)$ as the induced subgraph of $D(k,F)$. So the girth of $D(k,F)$ is bounded above by $k+5$. □

Theorem 3.4 follows directly from Proposition 4.5 and statement (i) of above theorem.

Note that the lower bound was obtained via explicit construction (graphs $C(t,K)$ introduced in [51]). By [52], the graphs $C(t,K)$ with char$K \neq 2$ are connected. The class of graphs $C(t,K)$, in which char$K \neq 2$, t is fixed, and K is running through the set of finite rings, is a family of small world graphs.

5. Examples of algebraic graphs of bounded girth via their investigation by computational algebra

5.1. The graph $D(14,K)$

It is convenient to write points (p) and lines $[l]$ as follows:

$$\begin{aligned}(p) &= (p_1,p_{11},p_{12},p_{21},p_{22},p'_{22},p_{23},p_{32},p_{33},p'_{33},p_{34},p_{43},p_{44},p''_{44}),\\ [l] &= [l_1,l_{11},l_{12},l_{21},l_{22},l'_{22},l_{23},l_{32},l_{33},l'_{33},l_{34},l_{43},l_{44},l'_{44}].\end{aligned} \tag{5}$$

The coordinates $p_{0,1} = p_1$ and $l_{1,0} = l_1$ are colours of a point (p) and a line $[l]$, respectively. The girth of $D(14,K)$ is at least 19.

The graph $D(14,K)$ is defined by the first 13 equations of (3). The operators $N_{l_1}(p)$ and $N_{p_1}([l])$ of taking the neighbour of point (p) with the colour l_1 and neighbour of line $[l]$ with the colour p_1, respectively, are well defined and can be written in the form

$$\begin{aligned}N_{l_1}((p)) = [l] = [&l_1, p_1 + l_1p_1, p_{12} + p_1l_{11}, p_{21} + l_1p_{11}, p_{22} + l_1p_{12}, p'_{22}\\ &+ p_1l_{21}, p_{23} + p_1l_{22}, p_{32} + l_1p'_{22}, p_{33} + l_1p_{23}, p'_{33} + p_1l_32, p_{34}\\ &+ p_1l_{33}, p_{43} + l_1p'_{33}, p_{44} + l_1p_{34}, p'_{44} + p_1l_{43}]\\ N_{p_1}([l]) = (p) = (&p_1, p_{11} - l_1p_1, p_{12} - l_1p_{11}, p_{21} - l_1p_{11}, p_{22} - l_1p_{12}, p'_{22}\\ &- l_{21}p_1, p_{23} - p1l_{22}, p_{32} - l_1p'_{22}, p_{33} - l_1p_{23}, p'_{33} - p_1l_{32}, p_{34}\\ &- p_1l_{22}p_{43} - l_1p'_{33}, p_{44} - l_1p_{34}, p'_{44} - p_1l_{43})\end{aligned}$$

We have to compute coordinates of the (p) and $[l]$ in natural order by iterative process. The following invariants $a_2(u), a_3(u), a_4(u)$ of the tuple $u = \langle u_1, u_{11},\dots,u'_{44}\rangle$ (point or line) depend only on the connected component of $D(k,K)$ containing u

$$\begin{aligned}a_2(u) &= ((u'_{22} - u_{21}u_{01}) + (u_{11}u'_{11} - u_{12}u_{10}) - u_{22},\\ a_3(u) &= ((u'_{33} - u_{01}u_{32}) + (u_{11}u'_{22} - u_{12}u_{21}) + (u_{22} - u'_{11} - u_{23}u_{10}) - u_{33}),\\ a_4(u) &= (u'_{44} - u_{01}u_{43}) + (u_{11}u'_{33} - u_{12}u_{32}) + (u_{22}u'_{22} - u_{23}u_{21})\\ &\quad + (u_{33}u'_{11} - u_{34}u_{10}) - u_{44}).\end{aligned}$$

5.2. Algebraic graph of girth 10 defined over a field of characteristic zero

Take the graph $CD(6,F)$, char$F=0$. We can rewrite the equations in the following form:

$$\begin{cases} y_2 - x_2 = y_1x_1, \\ y_3 - x_3 = y_1x_2, \\ y_4 - x_4 = y_2x_1, \\ y_5 - x_5 = y_3x_1, \\ y_6 - x_6 = y_1x_4, \\ x_6 - x_3x_1 + x_2^2 - x_4x_1 = x_5, \\ y_6 - y_3y_1 + y_2^2 - y_4y_1 = y_5; \end{cases}$$

$$y_1 = \frac{(y_6 - x_3x_1 + x_2^2 - x_4x_1 - x_5)}{x_4},$$

$$y_2 = \frac{(x_2x_4 + y_6x_1 - x_1^2x_3 + x_1x_2^2 - x_1^2x_4 - x_5x_1)}{x_4},$$

$$y_3 = \frac{(x_3x_4 + x_2y_6 - x_2x_1x_3 + x_2^3 - x_2x_1x_4 - x_2x_5)}{x_4},$$

$$y_4 = \frac{(x_4^2 + x_2x_1x_4 + y_6x_1^2 - x_1^3x_3 + x_1^2x_2^2 - x_1^3x_4 - x_1^2x_5)}{x_4},$$

$$y_5 = \frac{(x_5x_4 + x_3x_1x_4 + x_2x_1y_6 - x_2x_1^2x_3 + x_2^3x_1 - x_2x_1^2x_4 - x_2x_1x_5)}{x_4},$$

$$x_6 = x_3x_1 - x_2^2 + x_4x_1 + x_5.$$

Moreover, y_6 is given by the quadratic equation

$$\begin{aligned} &x_2y_6^2 + (-2x_2x_5 - 2x_2x_1x_3 - 2x_2x_1x_4 + 2x_2^3 + x_3x_4)y_6 - x_3^2x_1x_4 - x_4^2x_1x_3 \\ &\quad + x_2x_1^2x_4^2 - x_5x_3x_4 + x_3^2x_1^2x_2 + 2x_2x_1^2x_3x_4 + 2x_2x_1x_5x_4 + x_2x_5^2 - x_4^3x_1 \\ &\quad + x_2^5 + 2x_3x_1x_2x_5 + x_2^2x_3x_4 - 2x_2^3x_1x_4 - 2x_3x_1x_2^3 - 2x_2^3x_5 = 0 \end{aligned}$$

The discriminant of the above quadratic equation is 0 when

$$x_4^2(x_3^2 + 4x_2x_1x_4) = 0.$$

The graph $CD(6,F)$ is isomorphic to $CD(5,F) = D(5,F)$, which can be obtained by deleting the last components of points and lines of $CD(6,F)$ and omitting the last equation.

Let X be graph $CD(5,F)$. We define two transformations f and g of F^5. The first transformation f is given by

$$\begin{aligned} y_1 &= x_1 + a_1, \\ y_2 &= x_2 - x_1^2 - x_1a_1, \\ y_3 &= x_3 - x_2x_1 + x_1^3 + x_1^2a_1, \\ y_4 &= x_4 - x_2x_1 - x_2a_1, \\ y_5 &= x_5 - x_1x_4 + x_2x_1^2 + x_1x_2a_1 \end{aligned}$$

and the second g is given by

$$\begin{aligned} z_1 &= y_1 + a_2, \\ z_2 &= y_2 + y_1^2 + y_1a_2, \end{aligned}$$

$$z_3 = y_3 + y_2y_1 + y_2a_2,$$
$$z_4 = y_4 + y_1y_3 + y_2y_1^2 + y_1y_2a_2,$$
$$z_5 = y_5 + y_4y_1 + y_4a_2.$$

We define the algebraic variety V_k as follows:

$$V_k = \begin{cases} f_{\alpha_1}g_{\alpha_2}\dots f_{\alpha_{k-1}}g_{\alpha_k}(x_1,\dots,x_5) = (\lambda_1,\dots,\lambda_5), \text{ if } k \text{ is even,} \\ f_{\alpha_1}g_{\alpha_2}\dots f_{\alpha_k}(x_1,\dots,x_5) = (\lambda_1,\dots,\lambda_5), \text{ if } k \text{ is odd.} \end{cases}$$

Consider V_d as an algebraic variety defined over $k(x_1,\dots,x_5,\lambda_1,\dots,\lambda_5)$. The following lemma can be obtained similarly, using computational algebra tools.

Lemma 5.1. *Let V_d be defined as above. Then $k(V_d)$ is a subfield of $k(x_1,\dots,x_5,\lambda_1,\dots,\lambda_5)$ such that*

(i) *V_2 and V_3 are rational varieties;*
(ii) *V_4 is a 0-dimensional variety and has a unique point;*
(iii) *V_5 is a 0-dimensional variety and has 6 different points;*
(iv) *If $2 \leqslant d \leqslant 4$ the equation in variables a_i in the definition of V_d has not more than one solution for each (x_1,x_2,x_3,x_4,x_5) and $(\lambda_1,\dots,\lambda_5)$.*

Proof. We can eliminate a_i's and y_i's from the above system. The result is the variety V_d over k. The fact that V_2 and V_3 are rational varieties is an easy computational exercise. Similarly for V_4 and V_6. Part (iv) follows directly from (i), (ii), and (iii). □

Theorem 5.2. *The graph $CD(6,F)$ has girth 10.*

Proof. The graph $D(5,F)$ is bipartite. So it does not contain cycles of odd length. The expression $f_{\alpha_1}(x_1,x_2,x_3,x_4,x_5)$ is the neighbour of colour $x_1+\alpha_1$ (line) of the point (x_1,x_2,x_3,x_4,x_5) in the graph. Similarly, $g_{\alpha_1}(x_1,x_2,x_3,x_4,x_5)$ is a neighbour of colour $x_1+\alpha_1$ (point) of the line $[x_1,x_2,x_3,x_4,x_5]$. So equations in the definition of V_d are algebraic interpretation of the walk starting from point (x_1,x_2,x_3,x_4,x_5) and with the final vertex $(\lambda_1,\dots,\lambda_5)$ (point or line). Such a walk is a pass if and only if $\alpha_{i+1} \neq -\alpha_i$, $i = 1,\dots,d-1$. So the property (iv) implies the absence of cycles C_4, C_6, and C_8, but (iii) implies the existence of C_{10}. □

Remark 5.3. Similarly can be established that the girth of $D(9,F)$ is 14.

6. On the applications of graphs with high girth to coding theory and cryptography

The following directions of applied data security are motivations of studies of extremal properties of balanced graphs of large girth.

6.1. LDPS and turbo codes and graphs of large girth

Low-density parity-check (LDPC) codes were originally introduced in doctoral thesis by Gallager [16] in 1961. The discovery of Turbo codes by Berrou, Glavieux, and Thitimajshima [2] in 1993, and the rediscovery of LDPC codes by Mackay and Neal [26] in 1995 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, the Tanner graph (see [32,34,35] and further references), is associated with the code and an important parameter affecting the performance of the code is the girth of corresponding Tanner graph. The design of structured regular LDPC codes whose Tanner graphs have large girth is considered

in [17,18,29]. The regularity and structure of LDPC codes utilize memory more efficiently and simplify the implementation of LDPC coders. The Tanner graph is a bipartite graph, in which the set of nodes is divided into two disjoint classes with edges only between nodes in the two different classes. The impotence of the studies of undirected regular bipartite graphs with large girth for the design of turbo codes is discussed in [29].

Large girth speeds the convergence of iterative decoding and improves the performance of LDPC codes, at least in the high SNR range. Large size of such graphs implies fast convergence.

6.2. Cryptography

The cryptographical properties of infinite families of simple graphs of large girth with the special colouring of vertices are studied during the last 10 years; see [40,41,44,45,50]) and further references. Such families can be used for the development of cryptographical algorithms (on symmetric or public key modes). Only few families of simple graphs of large unbounded girth and arbitrarily large degree are known.

Papers [48,49] are devoted to a more general theory of directed graphs of large girth and their cryptographical applications. It contains new explicit algebraic constructions of infinite families of such graphs. It is shown that they can be used for the implementation of secure and very fast symmetric encryption algorithms. The symbolic computations technique allow us to create a public key mode for the encryption scheme based on algebraic graphs. The information on the implementations of such algorithms can be found in [39,42,43,47] (case of simple graphs) and [48,49,19] (for directed graphs). The paper [19] compares the speed of the graph based algorithms with the speed of RC4 and DES.

References

[1] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, Umesh Vazirani, Dense quantum coding and quantum finite automata, J. ACM (JACM), 49 (4) (2002) 496–511.
[2] C. Berrou, A. Glavieux, P. Thitimajshima, Near Shannon limit error-correcting coding and decoding: turbo-codes, ICC 1993, Geneva, Switzerland, 1993, pp. 1064–1070.
[3] N.L. Biggs, Graphs with large girth, Ars Combin. 25C (1988) 73–80.
[4] N. Biggs, Algebraic Graph Theory, second ed., Cambridge, University Press, 1993.
[5] N.L. Biggs, A.G. Boshier, Note on the girth of Ramanujan graphs, J. Combin. Theory, Ser. B 49 (1990) 190–194.
[6] N.L. Biggs, M.J. Hoare, The sextet construction for cubic graphs, Combinatorica 3 (1983) 153–165.
[7] B. Bollobás, Extremal Graph Theory, London Math. Soc. Monograph, Academic Press, 1978.
[8] J.A. Bondy, M. Simonovits, Cycles of even length in graphs, J. Combin. Theory, Ser. B 16 (1974) 87–105.
[9] A. Brower, A. Cohen, A. Nuemaier, Distance Regular Graphs, Springer, Berlin, 1989.
[10] P. Erdös, A. Renyi, V.T. Soc, On a problem of graph theory, Studia Math. Hungar. 1 (1966) 215–235.
[11] P. Erdös, H. Sachs, Regulare Graphen gegebener Taillenweite mit minimaler Krotenzahl, Wiss. Z. Univ. Halle Martin Luther, Univ. Halle–Wittenberg, Math. Natur. Reine 12 (1963) 251–257.
[12] P. Erdös, M. Simonovits, Compactness results in extremal graph theory, Combinatorica 2 (3) (1982) 275–288.
[13] W. Faudree, M. Simonovits, On a class of degenerate extremal graph problems, Combinatorica 3 (1) (1983) 83–93.
[14] W. Feit, D. Higman, The nonexistence of certain generalised polygons, J. Algebra 1 (1964) 114–131.
[15] Z. Füredi, F. Lazebnik, A. Seress, V.A. Ustimenko, A.J. Woldar, Graphs of prescribed Girth and Bi-Degree, J. Combin. Theory, Ser. B 64 (2) (1995) 228–239.
[16] R.G. Gallager, Low-density parity-check codes, IRE Trans. Inform. Theory IT-8 (1962) 21–28.
[17] P. Guinand, J. Lodge, Tanner type codes arising from large girth graphs, in: Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT '97), Toronto, Ontario, Canada, 1997, pp. 5–7.
[18] P. Guinand, J. Lodge, Graph theoretic construction of generalized product codes, in: Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT '97), Ulm, Germany, 1997, pp. 111–112.
[19] J. Kotorowicz, V.A. Ustimenko, On the implementation of cryptoalgorithms based on agebraic graphs over some commutative rings, in: Condenced Matters Physics, Special Issue: Proceedings of the International Conferences "Infinite particle systems, Complex systems theory and its application, Kazimerz Dolny, Poland, 2006, 11 (2(54)), 2008, pp. 347–360.
[20] W. Imrich, Explicit construction of graphs without small cycles, Combinatorica 2 (1984) 53–59.
[21] F. Lazebnik, V. Ustimenko, Some algebraic constructions of dense graphs of large girth and of large size, DIMACS Series Discrete Math. Theoret. Comput. Sci. 10 (1993) 75–93.
[22] F. Lazebnik, V.A. Ustimenko, A.J. Woldar, New upper bounds on the order of cages, Electron. J. Combin. 14 (R13) (1997) 1–11.
[23] F. Lazebnik, V.A. Ustimenko, A.J. Woldar, A new series of dense graphs of high girth, Bull. (New Series) AMS 32 (1) (1995) 73–79.
[24] F. Lazebnik, V.A. Ustimenko, A.J. Woldar, A characterization of the components of the graphs $D(k,q)$, Discrete Math. 157 (1996) 271–283.
[25] A. Lubotsky, R. Philips, P. Sarnak, Ramanujan graphs, J. Combin. Theory 115 (2) (1989) 62–89.

[26] D.J.C. MacKay, R.N. Neal, Good Codes based on very sparse matrices, in: "Cryptography and Coding, 5th IMA Conference, Lecture Notes in Computer Science 1025, 1995, pp. 110–111.
[27] G. Margulis, Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators, Probl. Peredachi Informatsii 24 (1) 51–60. English translation: J. Prob. Inform. Trans., 1988, pp. 39–46.
[28] M. Margulis, Arithmetic groups and graphs without short cycles, in: 6th Int. Symp. on Information Theory, Tashkent, Abstracts 1, 1984, pp. 123–125 (in Russian).
[29] Jose M.F. Moura, Jin Lu, Haotian Zhang, Structured LDPC Codes with Large Girth, IEEE Signal Process. Mag. 21 (1) (2004) 42–55.
[30] H. Sachs, Regular graphs with given girth and restricted circuits, J. London. Math. Soc 38 (1963) 423–429.
[31] N. Sauer, Extermaleigenschaften regularer Graphen gegebener Taillenweite 1, 2, Osterreich. Acad. Wiss. Math. Natur. Kl. S.-B 2, 176 (1967) 9–25, 27–43.
[32] T. Shaska, W.C. Huffman, D. Joyner, V. Ustimenko (Eds.), Advances in Coding Theory and Cryptography, Series on Coding Theory and Cryptology, vol. 3, World Scientific, 2007.
[33] M. Simonovits, Extremal graph theory, in: L.W. Beineke, R.J. Wilson (Eds.), Selected Topics in Graph Theory 2, Academic Press, London, 1983, pp. 161–200.
[34] R.M. Tanner, A transform theory for a class of group-invariant codes, IEEE Trans. Inform. Theory 34 (4) (1988) 725–775.
[35] R. Michiel Tanner, A recursive approach to low density codes, IEEE Trans. Info Th. IT 27 (5) (1984) 533–547.
[36] J.A. Thas, Generalised polygons, in: F. Buekenhout (Ed.), Handbook in Incidence Geometry, North-Holland, Amsterdam, 1995 (Chapter 9).
[37] J. Tits, Sur la trialite et certains groupes qui s'en deduisent, Publ. Math. I.H.E.S 2 (1959) 15–20.
[38] J. Tits, R. Weiss, Moufang Polygons, Springer-Verlag, 2002.
[39] A. Touzene, V. Ustimenko, Graph based private key crypto-system, Int. J. Comput. Res. 13 (3) (2005) 275–282.
[40] V.A. Ustimenko, Random walks on special graphs and Cryptography, Amer. Math. Soc. Meeting, Loisville, March, 1998.
[41] V.A. Ustimenko, Coordinatization of regular tree and its quotients, in "Voronoi's Impact in Modern Science", Proceedings of Memorial Voronoi Conference, Kiev, 1998, Kiev, Institute of Mathematics, 1998, pp. 125–152.
[42] V. Ustimenko, D. Sharma, Special Graphs in Cryptography, in: Proceedings of 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC 2000), Melbourne, 2000.
[43] V. Ustimenko, D. Sharma, CRYPTIM: the system to encrypt text and image data, in: Proceedings of International ICSC congress on Intelligent Systems and Applications, 2000, University of Wollongong, 2001, 14pp.
[44] V. Ustimenko, CRYPTIM: Graphs as tools for symmetric encryption, in: Lecture Notes in Computer Science, Proceedings of AAECC-14 Symposium on Applied Algebra, Algebraic Algorithms and Error Correction Codes, November 2001, vol. 2237, Springer, 2001, pp. 278–287.
[45] V. Ustimenko, Graphs with special arcs and cryptography, Acta Appl. Math. 74 (2) (2003) 117–153.
[46] V. Ustimenko, A. Woldar, Extremal properties of regular and affine generalised polygons of tactical configurations, Eur. J. Combin. 24 (2003) 99–111.
[47] V. Ustimenko, Yu. Khmelevsky, Walks on graphs as symmetric and assymetric tools for encryption, South Pacific J. Nat. Stud. 20 (2002) 23–41.
[48] V. Ustimenko, On the extremal graph theory for directed graphs and its cryptographical applications, Series on Coding Theory and Cryptology, vol. 3, World Scientific, 2007, pp. 181–200.
[49] V. Ustimenko, On the graph based cryptography and symbolic computations, Serdica J. Comput., Proceedings of International Conference on Application of Computer Algebra 2006, Varna 1, 2007, pp. 131–186.
[50] V. Ustimenko, On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography, Albanian. J. Math. (5) (2007) (Special Issue "Algebra and Computational Algebraic Geometry" 1).
[51] V. Ustimenko, On linguistic dynamical systems, graphs of large girth and cryptography, J. Math. Sci. 140 (3) (2007) 412–434.
[52] V. Ustimenko, Algebraic small world graphs of large girth and related groups, Condenced Matters Physics, in: Proceedings of the International Conferences "Infinite particle systems", Complex systems theory and its application, Kazimerz Dolny, Poland, 2008, in press.
[53] Gilles Van Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge University Press, 2006.
[54] H. Walther, Eigenschaften von regularen Graphen gegebener Taillenweite und Minimaler Knotzenzahl, Wiss. Z. Illmenau 11 (1965) 167–168.
[55] H. Walther, Uber regulare Graphen gegebener Taillenweite und inimaler Knotenzahl, Wiss. Z. Techn Hochsch. Ilmenau 11 (1965) 93–96.
[56] A.L. Weiss, Girth of bipartite sextet graphs, Combinatorika 4 (2–3) (1984) 241–245.