ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 1, Pages 25–33
ISSN 1930-1235: (2009)

ALGEBRAIC GROUPS AND SMALL WORLD GRAPHS OF HIGH GIRTH

V. A. Ustimenko

University of Maria Curie-Sklodowska,
vasyl@golem.umcs.lublin.pl

Abstract. We apply term algebraic graphs for an infinite family of graphs for which the vertex set and the neighbourhood of each vertex are quasiprojective varieties over the commutative ring K. For each integral domain K with unity of characteristic $\neq 2$ and integral $m \geq 2$ we construct an edge transitive graph $\Gamma_m(K)$ of girth $\geq m$ and diameter bounded by the constant independent on K. In particular, for each m we have a family of algebraic small world graphs $\Gamma(m, F_{p^s})$, $s = 1, 2, \ldots$ over F_p, where p is prime, of girth $\geq m$.

1. Introduction

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [4]. All graphs (finite or infinite) we consider are simple, i.e. indirected without loops and multiple edges. Let $V(\Gamma)$ denotes the set of vertices of the graph Γ. A pass in Γ is called *simple* if all its vertices are distinct. When it is convenient, we shall identify Γ with the corresponding antireflexive symmetric binary relation on $V(\Gamma)$. The *length* of a pass is the number of its edges. The diameter of the graph is the maximal length of the shortest pass between two vertices. The *girth* of a graph Γ is the length of the shortest cycle in Γ.

We shall use term *the family of algebraic graphs* for the family of graphs $\Gamma(K)$, where K belongs to some infinite class F of commutative rings, such that the neighbourhood of each vertex of $\Gamma(K)$ and the vertex set itself are quasiprojective varieties over K of dimension ≥ 1 (see [1]).

Such a family can be treated as special Turing machine with the internal and external alphabet K.

Double cosets graphs corresponding to PwP', where P and P' are maximal parabolic subgroups of simple group $G(K)$ of Lie type defined over the field K are examples of algebraic edge-transitive graphs of finite diameter (see [1] or [6]). But the girth of them is bounded by 16 (case of generalised octagon defined over the field).

Theorem 1. *For each integer d, $d > 2$ there is an infinite family of edge-transitive algebraic graphs $\Gamma_d(K)$, where K is an integrity ring with unity of characteristic* $\neq$

Key words and phrases. infinite groups acting on graphs, algebraic graphs, graphs of large girth, small world graphs.

2, such that $g(\Gamma(K)) \geq d$ and diameter $\mathrm{diam}(\Gamma_d(K))$ is bounded by some constant, independent from K.

The statement proven by explicit construction of bipartite graphs $\Gamma_n(K)$ with point set and line set of kind K^n such that neighbourhood of each vertex is isomorphic to K.

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 it is known that the random k-regular graph has diameter close to this lower bound. In the case of family of small world graphs the diameter is $O(\log_{k-1}(v))$. The girth of the graph is the smallest length of it is cycle. Most known explicit constructions of infinite families of regular small world graphs are of girth 4 (see, for instance, [5]).

Corollary 2. *For each pair $(k \geq 3, g \geq 3)$ there is a regular small world graph of degree $\geq k$ and girth $\geq g$ with bounded diameter.*

The explicit construction construction of graph $\Gamma_d(K)$ are connected with studies of infinite families of graphs of large girth in the sense of N. Biggs [2] i.e. graphs G_i of degree l_i and unbounded girth g_i such that

$$g_i \geq \gamma \log_{l_i-1}(v_i) \tag{1.1}$$

As it follows from Even Circuit Theorem by Erdø s' $\gamma \leq 2$, but no family has been found for which $\gamma = 2$. Bigger γ's correspond to the larger girth.

The first explicit examples of families with large girth were given by Margulis [13], [14], [15] with for some infinite families with arbitrary large valency. The constructions were Cayley graphs $X^{p,q}$ of group $SL_2(Z_q)$ with respect to special sets of $q+1$ generators, p and q are primes congruent to 1 mod4. Then independently Margulis and Lubotsky, Phillips, and Sarnak [12] proved that for each p the constant γ for graphs $X^{p,q}$ with fixed p is $\geq 4/3$. In [3] Biggs and Boshier showed that this γ is asymptotically $4/3$.

The family of $X^{p,q}$ is not a family of algebraic graphs because the neighbourhood 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.

The fist family of connected algebraic graphs with over F_q of large girth and arbitrarily large degree had been constructed in [9]. These graphs $CD(k, q)$, k is an integer ≥ 2 and q is od prime power had been constructed as connected component of graphs $D(k, q)$ defined earlier (see [7], [8]). For each q graphs $CD(k, q)$, $k \geq 2$ form a family of large girth with $\gamma = 4/3\log_{q-1}q$.

Some new examples of algebraic graphs of large girth and arbitrary large degree the reader can find in [22].

Graphs $D(n, q)$ had been defined by diophantine equations, they have natural generalisations $D(n, K)$ defined over general commutative ring (see section 2 of the paper). In [22] the following statement had been proven.

Proposition 3. *For each integral domain K the girth of the graph $D(n, k)$ is $\geq n + 5$.*

We prove that for each commutative ring with unity of characteristic $\neq 2$ the connected components of $D(n, K)$ are isomorphic algebraic graphs over K. So the girth of the connected component is $g(D(n, K))$ We establish the upper bound for the diameter of the connected components of $D(n, K)$ independent on the ring K. It means that for each d we can chose the graph $\Gamma_d(K)$ among connected components of graphs $D(n, K)$, $n = 2, 3, \ldots$.

The description of the connected components $D(n, F_q)$, q is odd number had been obtained in [10], but the question on the evaluation of diameter was open.

The technique of studies the connected components of $CD(n, K)$ is group theoretical. In section 2 we define the automorphism group $U(n, K)$ acting edge transitive on the vertex set of graphs $D(n, K)$. We introduce imprimitivity blocks $CD(k, K) = C_t(K)$ of transformation group $(U(n, K), D(n, K))$ such that induced subgraph is an bipartite algebraic graph with partition sets isomorphic to K^t, where $t = [4/3n] + 1$ for $n = 0, 2, 3 \mod 4$ and $t = [3/4n] + 2$ for $n = 1 \mod 4$. We show that the graph $C_t(K)$ for the ring K with unity of odd characteristic is the connected component of $D(n, K)$. Let $D(K)$, $CD(K)$ and $U(K)$ are natural projective limits of graphs $D(n, K)$, $CD(n, K)$ and groups $U(n, K)$ when $n \to \infty$. As it was established in [22] for the case of integral domain K the girth of $D(n, K) \geq n+5$. It means that if K is an integral domain with unity of odd characteristic then CD(K) is a tree and $U(K)$ is isomorphic to the free product of two copies of additive group K^+ for the ring K.

In section 3 we establish the upper bound for the diameter of the graph $C_t(K)$, where K is the ring with unity of odd characteristic. As a corollary we get that the following statement

Proposition 4. *The family $C_t(K)$, where t is fixed and K belongs to the class of finite rings with unity of odd characteristic is the family of algebraic small world graphs of bounded diameter.*

The combination of small diameter and large girth makes graphs $C_t(K)$ useful in cryptographical applications (see [19], [20], [21], [22]).

2. Transformation groups of incidence structures defined over commutative rings

The *incidence structure* (P, L, I) (or *bipartite graph*) is a triple where P and L are two disjoint sets (set of *points* and set of lines, respectively) and I is symmetric binary relation on$P \cup L$ (*incidence relation*). As is usually done, we impose the following restrictions on I: two points (lines) are incident if and only if they coincide.

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 $\Gamma(G)_{G_1,G_2}$. Let $l(g)$ be the minimal length of representation of g in the form of products of elements from G_1 and G_2 The following statement had been formulated first by G. Glauberman.

Lemma 5. *Graph I is connected if and only if $< G_1, G_2 >= G$. The diameter of I is* max $l(g)$, $g \in G$.

Let $A =< a_1, \ldots, a_n | R_1(a_1, \ldots, a_n), \ldots, R_d(a_1, \ldots, a_n) >$ and
$B =< b_1, \ldots b_m | S_1(b_1, \ldots b_m), \ldots, S_t(b_1, \ldots, b_m) >$ are subgroups with generators a_i, $i = 1, \ldots, n$ and b_j, $j = 1, \ldots, m$ and generic relations R_i, $i = 1, \ldots, d$ and

S_j, $j = 1, \ldots, t$, respectively. Free product $F = A * B$ of A and B be the subgroup $< a_1, \ldots, a_n, b_1, \ldots, b_m | R_1, \ldots R_d, S_1, \ldots, S_t >$ (see [12]).

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 $H =< e >$, then $F_H = A*B$.

Theorem 6. *(see, for instance [12]) 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 7. *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.*

We define the family of graphs $D(k, K)$, where $k > 2$ is positive integer and K is a commutative ring, such graphs have been considered in [8] for the case $K = F_q$ (some examples are in [7]).

let P and L be two copies of Cartesian power K^N, where K is the commutative ring and 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 [15] for the case of general commutative ring 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 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:

$$\begin{aligned} l_{i,i} - p_{i,i} &= l_{1,0} p_{i-1,i} \\ l'_{i,i} - p'_{i,i} &= l_{i,i-1} p_{0,1} \\ l_{i,i+1} - p_{i,i+1} &= l_{i,i} p_{0,1} \\ l_{i+1,i} - p_{i+1,i} &= l_{1,0} p'_{i,i} \end{aligned} \tag{2.1}$$

(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 $D(K)$. We identify it with the bipartite *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 $(p)I[l]$.

For each positive integer $k \geq 2$ 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 with respect to the above order. The incidence I_k is then defined by imposing the first $k-1$ incidence equations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, K)$.

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 (2.1) 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 [16] (see [18]). Let us define the "root subgroups" U_α, where the "root" α belongs to the root system

$$\mathrm{Root} = \{(1,0),(0,1),(1,1),(1,2),(2,1),(2,2),(2,2)'\ldots,(i,i),(i,i)',(i,i+1),(i+1,i)\ldots\}.$$

The "root system above" contains all real and imaginary roots of the Kac-Moody Lie Algebra $\tilde{A}_1$ with the symmetric Cartan matrix. We just doubling imaginary roots (i,i) by introducing $(i,i)'$.

Group U_α generated by the following "root transformations" $t_\alpha(x)$, $x \in K$ of the $\mathrm{P} \cup \mathrm{L}$ given by rules $p_\beta = p_\beta + r_\beta(x)$, $l_\beta = l_\beta + s_\beta(x)$, where $\beta \in \mathrm{Root}$ and the functions $r_\beta(x)$, $s_\beta(x)$ are consist of summands defined by the following tables ($i \geq 0$, $m \geq 1$).

	$s_{0,1}(x)$	$s_{1,0}(x)$	$s_{m,m+1}(x)$	$s_{m+1,m}(x)$	$s_{m,m}(x)$	$s'_{m,m}(x)$
$l_{i,i}$		$-l_{i,i-1}x$	$+l_{r,r-1}x$, $r-m \geq 1$		$-l_{r,r}x$, $r-m \geq 0$	
$l_{i,i+1}$		$(l_{i,i}+l'_{i,i})x$ $+l_{i,i-1}x^2$	$+l'_{r,r}x$, $r=i-m \geq 0$		$-l_{r,r+1}x$, $r=i-m \geq 0$	
$l_{i+1,i}$	$+l_{i,i}x$			$-l_{r,r}x$, $r=i-m \geq 0$		$+l_{r+1,r}x$, $r=i-m \geq 0$
$l'_{i,i}$	$l_{i-1,i}x$	$l_{i,i-1}x$		$-l_{r-1,r-1}x$, $r=i-m \geq 1$		$+l'_{r,r}$, $r=i-m \geq 0$

TABLE 1

	$r_{0,1}(x)$	$r_{1,0}(x)$	$r_{m,m+1}(x)$	$r_{m+1,m}(x)$	$r_{m,m}(x)$	$r'_{m,m}(x)$
$p_{i,i}$	$+p_{i-1,i}x$	$p_{i,i-1}x$	$+p_{r,r-1}x$ $r=i-m \geq 1$		$-p_{r,r}x$ $r=i-m \geq 0$	
$p_{i,i+1}$		$+p'_{i,i}x$	$+p'_{r,r}x$ $r=i-m \geq 0$		$-p_{r,r+1}x$ $r=i-m \geq 0$	
$p_{i+1,i}$	$(p_{i,i}+p'_{i,i})x$ $+p_{i-1,i}x^2$			$-p_{r,r}x$, $r=i-m \geq 0$		$+p_{r+1,r}x$, $r=i-m \geq 0$
$p'_{i,i}$	$p_{i-1,i}x$			$-p_{r-1,r}x$, $r=i-m \geq 1$		$+p'_{r,r}$, $r=i-m \geq 0$

TABLE 2

Proposition 8. (i)*For each pair (α, x), $\alpha \in \mathrm{Root}$, $x \in K$ the transformation $t_\alpha(x)$ are automorphisms of $D(K)$. The projections of these maps onto the graph $D(n,K)$, $n \geq 2$ are elements of $\mathrm{Aut}(D(n,K))$.*

(ii) *Group $\mathrm{U}(K)$ acts edge regularly on the vertices of $\mathrm{D}(K)$.*

(iii) *Group $\mathrm{U}(n,K)$ generated by projections of $t_\alpha(x)$ onto the set of vertices V of $\mathrm{D}(n,K)$ 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 $[a,0,\ldots,0]$ 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 $D(K)$. This action is regular ((ii)) because the stabilizer of the edge $(0), [0]$ is trivial. Same arguments about the action of $U(n, K)$ justify (iii).

□

Remark For $K = F_q$ this statement had been formulated in [8].

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 $\mathrm{D}(k, K)$ ($\alpha \in \{(1,0),(0,1)\}$, 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 9. *(i) The classes of equivalence relation $\tau = \{(u, v)|a(u) = a(v)\}$ form the imprimitivity system of permutation groups* $\mathrm{U}(K)$ *and* $\mathrm{U}(n, K)$

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

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

(3i) The equivalence class C for the equivalence relation τ on the set $K^n \cup K^n$ is isomorphic to the affine variety $K^t \cup K^t$, $t = [4/3n] + 1$ 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 $\mathrm{D}(K)$ ($\mathrm{D}(n, K)$ then the induced subgraph, with the vertex set C is the union of several connected components of $\mathrm{D}(K)$ ($\mathrm{D}(n, K)$).

Without loss of generality we may assume that for the vertex v of $C(n, K)$ satisfying $a_2(v) = 0, \ldots a_t(v) = 0$. We can find the values of components $v'_{i,i)}$ from this system of equations and eliminate them. Thus we can identify P and L with elements of 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 $C(t, K)$ ($C(K)$) for the induced subgraph of $D(n, K)$ with the vertex set C.

Remark.

If $K = F_q$, q is odd, then the graph $C(t, k)$ coincides with the connected component $CD(n, q)$ of the graph $D(n, q)$ (see [10]), graph $C(F_q)$ is a q-regular tree. In other cases the question on the connectedness of $C(t, K)$ is open. It is clear that $g(C(t, F_q))$ is $\geq 2[2t/3] + 4$.

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

Proposition 10. (i) *The connected component $CD(n, K)$ of the graph $D(n, K)$ (or its induced subgraph $C(t, K)$) is isomorphic to $\Gamma({U_n}^C)_{U_{(0,1)}, U_{(1,0)}}$.*

(ii) Projective limit of graphs $D(n, K)$ (graphs $C(t, K)$, $CD(n, K)$) with respect to standard morphisms of $D(n+1, K)$ onto $D(n, K)$ (their restrictions on induced subgraphs) equals to $D(K)$ ($C(K)$, $CD(K) = {U^C}_{U_{(0,1)}, U_{(1,0)}}$, respectively).

If K is an integrity domain, then $D(K)$ and $CD(K)$ are forests. Let C be the connected component, i.e tree.

Group U^C acts regularly on $CD(K)$. So we can apply theorem on group acting regular on the tree and get the following statement.

Proposition 11. *If K is integrity domain then group $U^C(K)$ is isomorphic to the free product of two copies of K^+.*

3. Main statement

Theorem 12. *The diameter of the graph $C_m(K)$, $m \geq 2$, K is a commutative ring with unity of odd characteristic is bounded by function $f(m)$, defined by the following equations:*

$$f(m) = \begin{cases} (32/3)(4^{(m+1)/3} - 1) - m + 7, & \text{for } m = 2 \text{ (mod3)} \\ (32/3)(4^{(m-1)/3} - 1) + 4^{(m+5)/3} - m + 7 & \text{for } m = 1 \text{ (mod3)} \\ (32/3)(4^{m/3} - 1) + 32 \times 4^{(m-3)/3} - m + 7, & \text{for } m = 0 \text{ (mod3)} \end{cases}$$

Proof. Let $C = C_t(K)$ be the block of equivalence relation τ, containing zero point and zero line. Let us consider the stabiliser of this block. It is clear that group G generated by elements $t_{i,i+1}(x)$, $t_{i+1,i}(x)$, $i \geq 0$, $t_{1,1}(x)$ and $t_i(x) = t_{i,i}(x)t'_{i,i}(x)$, $i \geq 2$, $x \in K$ stabilises C and acts regularly on this set.

Let $l(g)$ be the minimal length of irreducible representation of $g \in G$ in the form

$$T_1(x_1)T_2(x_2)\dots T_d(x_d), x_i \in K, \quad (3.1)$$

where consecutive elements $T_i(x_i)$ and $T_{i+1}(x_{i+1})$ belong to different subgroups U_1 and U_2.

As it follows from the group theoretical interpretation of lemma 3 the diameter of group G is equal to the maximal length $l(g)$.

Let $G_{1,1}$ be the totality of all commutator elements $[t_{0,1}(x), t_{1,0}(y)] = t(x, y)$. Then applications of $T_{1,1}(y) = t(1, y)$ to zero point (0) (or line) do not change its first component. For the second component $u_{1,1}$ of (u) $= (0)^{T_{1,1}(y)}$ we have $u_{1,1} = y$. In fact, $(O)^{T_{1,1}(y)} = (O)^{t_{1,1}}(y)$ and $l(\text{u}) \leq 4$.

Let us consider the totality $G_{1,2}$ of the commutators $t(x, y) = [t_{0,1}(x), T_{1,1}(y)]$. Then its action of on zero line (point) does not change its first, second components. The third component will be $2xy$. Let us consider $T_{1,2}(y) = t(x/2, y)$. Let $u = [O]^{T_{1,2}(y)}$, then $u_{1,2} = y$. Similarly, we construct the totality $G_{2,1}$ of commutators $t(x, y)[t_{1,0}(x)T_{1,1}(y)]$ containing element $T = T_{2,1}(y)$, such that $O^T = O^{T_{2,1}(y)} = [0, 0, 0, y, \dots]$. We can write the irreducible presentation of $g \in G$ in the form (3.1) starting either with element from U_1 or U_2. It means that $l(g) \leq 8$ for $g \in G_{1,2} \cup G_{2,1}$

Let us define $G_{2,2}$ as totality of commutators $[t_{1,0}(x), T_{1,2}(y)]$ (or equivalently as set of elements of kind $[t_{0,1}(x), T_{2,1}(y)]$. Then for element $t \in G_{2,2}$ we have $O^t = O^{t_2(xy)} = (0, 0, 0, 0, xy, xy, \dots)$. We have $l(g) \leq 16$ for $g \in G_{2,2}$.

We can define recurrently $Gi, i+1$, $Gi+1, i$ and $G_{i+1,i+1}$, $i \geq 2$ as totalities of elements of kind $[t_{0,1}(x), T_{i,i}(y)]$, $[t_{1,0}(x), T_{i,i}(y)]$ and $[t_{0,1}(x), T_{i,i+1}(y)]$, respectively. The length of elements from $G_{i,i+1}$ and $G_{i+1,i}$ are bounded by 2^{2i+1} and $l(g) \leq 2^{2i+2}$ for $g \in G_{i+1,i+1)}$. Notice, that the element $g \in G_\alpha$ acting on element v (point or line) changing only components v_β , $\beta > \alpha$. We can find an element $g \in G_\alpha$, such that for $u = v^g$ the component u_α equals zero.

Let $u \in G$ be element such that $O^u = v$. Then by consecutive applications of appropriate transformations $g \in G_\alpha$ with respect to natural order on roots we can move v to O It means that each element $g \in G$ can be presented as product $g_{0,1}g_{1,0}g_{1,1}\dots g_\alpha \dots$, where $g_\alpha \in G_\alpha$. Let $d(\alpha)$ be the length of g_α. We can bound the length of g by the sum S of d_α. In case when α is not simple root we have a choice to write irreducible representation of g_α, is with the first character from U_1 or the one from U_2. It allows slightly improve the bound foe the diameter - get $S-m+1$ instead of S.

Let us count S for the case $m = 2\text{mod } 3$. If $m = 2$ then $S = 6$. In case of $m \geq 5$ each triple of roots $(i, i+1)$, $(i+1, i)$, $(i+1, i+1)$, $i \geq 1$ contributes summands 2^{2i+1}, 2^{2i+1} and 2^{2i+2}. So we can count S via the sum of the geometrical progression.

Let $m = 2\text{mod } 3$ then each triple as above contribute summand 2^{2i+3}. So we have the geometrical progression $2^{(2i+3)}$, $i = 1, \dots (m-2)/3$. The roots $(0,1)$, $(1,0)$ and $(1,1)$ contribute 6.

In case $m = 0\text{mod } 3$ we have a geometrical progression 2^{2i+3}, $i = 1, \dots, m/3-1$ and last root contributes $32 \times 4^{m/3-1}$.

In case $m = 1\text{mod}3$) we have a geometrical progression 2^{2i+3}, $i = 1, \dots, (m-4)/3$ and two last roots contributes $64 \times 4^{(m-4)/3}$

This way we are getting the formulae for the bound.

□

Remark. Theorem 1 follows directly from theorem 12 and Proposition 3.

References

[1] N. Biggs, *Algebraic Graph Theory* (2nd ed), Cambridge, University Press, 1993.
[2] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.
[3] 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).
[4] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.
[5] B. Bollobás, *Random Graphs*, Academic Press, London, 1985.
[6] A. Brouwer, A. Cohen and A. Niemaier *Distance Regular Graphs*, Springer Verlag (1987), 380 p.
[7] F. Lazebnik, V. A. Ustimenko, *New Examples of graphs without small cycles and of large size*, Europ. J. of Combinatorics, 14 (1993) 445-460.
[8] F. Lazebnik F. and V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.
[9] 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.
[10] Lazebnik, F., Ustimenko, V.A. and A.J. Woldar, *A characterisation of the components of the graph $D(k,q)$*, Discrete Mathematics, 157 (1996), 271-283.
[11] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.
[12] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory*, Interscience publ., 1966.
[13] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.
[14] 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.
[15] 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).
[16] V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukrainian Math. J. 43, Nos. 7,8 (1991), pp. 1055–1060 (in Russian).
[17] 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.

[18] V. A. Ustimenko, *On the varieties of parabolic subgroups, their generalizations and combinatorial applications*, Acta Applicandae Mathematicae, 52 (1998), 223-238.

[19] V. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.

[20] V. Ustimenko, *CRYPTIM: Graphs as tools for symmetric encryption*, In Lecture Notes in Comput. Sci., 2227, Springer, New York, 2001.

[21] V. Ustimenko, *Maximality of affine group and hidden graph cryptsystems*, Journal of Algebra and Discrete Mathematics, October, 2004, v.10, pp 51-65.

[22] V. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Zapiski Nauchnyh Seminarov POMI, vol. 326, "Representation Theory, Dynamical Systems. Combinatorial and Algorithmic Methods, 2005, 214-235.