EXPLICIT CONSTRUCTION OF GRAPHS WITH AN ARBITRARY LARGE GIRTH AND OF LARGE SIZE [1]

Felix Lazebnik and Vasiliy A. Ustimenko

Dedicated to the memory of Professor Lev Arkad'evich Kalužnin.

Abstract: Let $k \geq 3$ be a positive odd integer and q be a power of a prime. In this paper we give an explicit construction of a q–regular bipartite graph on $v = 2q^k$ vertices with girth $g \geq k + 5$. The constructed graph is the incidence graph of a flag–transitive semiplane. For any positive integer t we also give an example of a $q = 2^t$–regular bipartite graph on $v = 2q^{k+1}$ vertices with girth $g \geq k + 5$ which is both vertex–transitive and edge–transitive .

Section 1. Introduction.

The missing definitions of graph–theoretical concepts which appear in this paper can be found in [6]. 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. $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. The *girth* of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G. Some examples of graphs with large girth which satisfy some additional conditions have been known to be hard to construct and they turned out to be useful in different problems in extremal graph theory, in studies of graphs with a high degree of symmetry, in the design of communication networks. There are many references on each of these topics. Here we mention just a few main books and survey papers which also contain extensive bibliographies. On extremal graph theory: [6,20]; on graphs with a high degree of symmetry: [8, 12,19]; on communication networks: [2,9].

In this paper we construct a new infinite series of regular bipartite graphs with edge–transitive automorphism group and large girth. More precisely, for any positive odd integer $k \geq 3$ and any prime power q, we build a q–regular bipartite graph $D(k, q)$ on $2q^k$ vertices with girth $g \geq k + 5$. Our construction generalizes the one of a graph isomorphic to $D(9, q)$ from [13]. Several reasons why we find these graphs interesting are described below.

[1] This research was partially supported by a grant DMS–9020485.

1. Let $\mathcal{F}$ be a family of graphs. By $ex(v, \mathcal{F})$ we denote the greatest number of edges in a graph on v vertices which contains no subgraph isomorphic to a graph from $\mathcal{F}$. Let C_n denote the cycle of length $n \geq 3$. It is known (see [6,7,10]) that all graphs of order v with more than $90kv^{1+\frac{1}{k}}$ edges contain a $2k$–cycle. Therefore $ex(v, \{C_3, C_4, \cdots, C_{2k}\}) \leq 90kv^{1+\frac{1}{k}}$. For a lower bound we know that $ex(v, \{C_3, C_4, \cdots, C_n\}) \geq c_n v^{1+\frac{1}{n-1}}$, for some positive constant c_n. This result follows from a theorem proved implicitly by Erdős (see [20]) and the proof is nonconstructive. As it was mentioned in [20], it is unlikely that this lower bound is sharp, and our construction supports this remark for arbitrary n. Graphs $D(k, q)$ show that for an infinite sequence of values of v, $ex(v, \{C_3, C_4, \cdots, C_{2s+1}\}) \geq d_s v^{1+\frac{1}{2s-3}}$, $s \geq 3$, and this is an improvement of the nonconstructive bound for large v. For large values of s and an infinite sequence of values of v, a better bound $ex(v, \{C_3, C_4, \cdots, C_{2s+1}\}) \geq f_s v^{1+\frac{4}{3}\frac{1}{2s+2}}$ is provided by the Ramanujan graphs (see below), and it appears to be the best asymptotic lower bound known. Comparing the exponents of v, we obtain that our bound is better for $3 \leq s \leq 8$ and large v. For $s = 9$ the bounds are equivalent. For all odd prime powers q or $q = 2^m$, m is a positive even integer, and all odd values of k, $3 \leq k \leq 17$, $k \neq 7$, graphs $D(k, q)$ are of the greatest known size among the graphs of given order and girth $\geq k + 5$. The same is correct if $q = 2^m$, m is odd, k is odd, $3 \leq k \leq 17$, $k \neq 7, 11$. Graphs $D(3, q)$ and $D(5, q)$ have asymptotically as many edges as the incidence 'point–line' graphs of a generalized quadrangle and a generalized hexagon respectively, and the greatest known edge density (the ratio $e/\binom{v}{2}$) among the graphs of the same order and girth (see Lazebnik, Ustimenko [13] for definitions and details). Extremal properties of incidence graphs of the generalized 4– and 6–gons were pointed out by Benson [1]. For prime q, a somewhat similar construction leading to graphs with the same order, edge density and girth as $D(3, q)$ and $D(5, q)$, was done by Wenger [24]. Graph $D(7, q)$ has girth ≥ 12 but asymptotically fewer edges, than the incidence graph of a generalized hexagon whose girth is 12. Graph $D(9, q)$ has girth at least 14 and shows that $ex(v, \{C_3, C_4, \cdots, C_{13}\}) \geq d_{13} v^{1+\frac{1}{9}}$. For $q = 2^m$, where m is an odd positive integer, this lower bound may not be the best due to a recent result of Ustimenko and Woldar[22], where an example of a q–regular graph of order $v = 2q^t$ and girth at least 16 is given, with t being an unknown integer satisfying the inequality $8 \leq t \leq 10$. Their result implies that $ex(v, \{C_3, C_4, \cdots, C_{15}\}) \geq d_{15} v^{1+\frac{1}{t}}$ for an infinite sequence of values of v and an integer t, $8 \leq t \leq 10$. (in fact, it was recently shown, [25], that $t \leq 9$.) This lower bound is certainly better than the one of magnitude $v^{1+\frac{1}{11}}$ provided by the graph $D(11, q)$.

2. Let $\{G_i\},\ i \geq 1$, be a family of graphs such that each G_i is a r–regular graph of order v_i and girth g_i. Following Biggs [3] we say that $\{G_i\}$ is a family of graphs with *large girth* if

$$g_i \geq \gamma \log_{r-1}(v_i)$$

for some constant γ. It is well known (e.g. see [6]) that $\gamma = 2$ would be the best possible constant, but no family has been found to achieve this bound. For many years the only significant results were the theorems of Erdős and Sachs and its improvements by Sauer, Walther, and others (see [6] pp. 107 for more details and references), who using nonconstructive methods proved the existence of infinite families with $\gamma = 1$. The first explicit examples of families with large girth were given by Margulis [15] with $\gamma \approx 0.44$ for some infinite families with arbitrary large valency, and $\gamma \approx 0.83$ 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 [11] was able to improve the result for an arbitrary large valency, $\gamma \approx 0.48$, and to produce a family of cubic graphs (valency 3) with $\gamma \approx 0.96$. In [5] 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 [23] proved the conjecture by showing that for the sextet graphs (or their double cover) $\gamma \geq 4/3$. Then independently Margulis [16–18] and Lubotzky, Phillips and Sarnak [14] came up with similar examples of graphs with $\gamma \geq 4/3$ and arbitrary large valency (they turned out to be so–called Ramanujan graphs). In [4], Biggs and Boshier showed that γ is exactly $4/3$ for graphs from [14]. The graphs are Cayley graphs of the group $PGL_2(Z_q)$ with respect to a set of $p+1$ generators (p, q are distinct primes congruent to 1 (mod 4)).

The family of graphs $D(k, q)$ presented in this paper gives an explicit example of graphs with an arbitrary large valency q and $\gamma \geq \log_q(q-1)$. Their definition and analysis are basically elementary. The construction was motivated by some results on embeddings of Chevalley group geometries in the corresponding Lie algebras, and the notion of a covering of a graph (in the sense of [21]) .

The authors are highly indebted to Professor W.M. Kantor who found a mistake in the computation of girth in a preliminary construction of a $D(5, q)$–like graph and made a number of useful remarks. We are also very grateful to Professors G.A. Margulis and M. Simonovits for consultations on some topics relative to this paper, and to Professor A.J. Woldar, Mr. A. Schliep and referees for their valuable comments.

Section 2. Construction of graphs $D(k,q)$.

The *incidence structure* (P,L,I) is a triple where P and L are two disjoint sets (a set of *points* and a set of *lines* respectively), and I is a symmetric binary relation on $P\cup L$ (*incidence relation*). As it is usually done, we impose the following restrictions on I : two points (lines) are incident if and only if they coincide. Let $B=B((P,L,I))$ be a bipartite graph such that $V(B)=P\cup L$ and $E(B)=\{\{p,l\}:pIl,p\in P,l\in L\}$. According to our definition B is a simple bipartite graph. We call B the *incidence* graph for the incidence structure (P,L,I).

Let q be a prime power. We define the infinite semiplane $\Gamma(q)$ as follows. Let P and L be two infinite–dimensional vector spaces over the finite field F_q. The vectors of P and L can be thought as infinite sequences of elements of F_q. P and L will be the set of points and the set of lines of the incidence structure $\Gamma(q)$. A vector $p\in P$ will be denoted by (p), and a vector $l\in L$ by $[l]$. The parentheses and brackets will allow us to distinguish vectors of different types (points and lines). It will be convenient for us to write the components of points and lines as

$$(p)=(p_1,p_{1,1},p_{1,2},p_{2,1},p_{2,2},p'_{2,2},p_{2,3},p_{3,2},p_{3,3},p'_{3,3},\ldots,p'_{i,i},p_{i,i+1},p_{i+1,i},p_{i+1,i+1},\ldots),$$

$$[l]=[l_1,l_{1,1},l_{1,2},l_{2,1},l_{2,2},l'_{2,2},l_{2,3},l_{3,2},l_{3,3},l'_{3,3},\ldots,l'_{i,i},l_{i,i+1},l_{i+1,i},l_{i+1,i+1},\ldots].$$

We also assume $p_{-1,0}=l_{0,-1}=p_{1,0}=l_{0,1}=0$, $p_{0,0}=l_{0,0}=-1$, $p'_{0,0}=l'_{0,0}=1$, $p_{0,1}=p_1$, $l_{1,0}=l_1$, $l'_{1,1}=l_{1,1}$, $p'_{1,1}=p_{1,1}$. We say that a point (p) is incident with a line $[l]$, and write it as $(p)I[l]$ if and only if the following conditions are satisfied:

$$\begin{cases} l_{i,i}-p_{i,i}=l_1p_{i-1,i} \\ l'_{i,i}-p'_{i,i}=p_1l_{i,i-1} \\ l_{i,i+1}-p_{i,i+1}=p_1l_{i,i} \\ l_{i+1,i}-p_{i+1,i}=l_1p'_{i,i} \\ \text{for}\quad i=1,2,\ldots \end{cases} \tag{2.1}$$

Notice that for $i=1$, the first two equations coincide and give $l_{1,1}-p_{1,1}=l_1p_1$.

Let $D(q)$ be the incidence graph of the incidence structure $\Gamma(q)=(P,I,L)$. For an integer $k\geq 2$, let $\Gamma(k,q)=(P(k),I(k),L(k))$ 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 $I(k)$ is defined by the first k equations of (2.1). (Actually we have $k-1$ distinct equations, since for $i=1$ the first two equation of the system (2.1) coincide.) Finally, let $D(k,q)$ be the incidence graph for $\Gamma(k,q)$.

Proposition 2.1. Let $k \geq 2$. The incidence system $\Gamma(k,q)$ is a semiplane and $D(k,q)$ is a q-regular bipartite graph on $2q^k$ vertices containing no 4–cycles.

Proof. It is clear that $|P(k)| = |L(k)| = q^k$, $|V(D(k,q))| = |P(k)| + |L(k)| = 2q^k$. It is also clear that $D(k,q)$ is bipartite. Let $(p) \in P(k)$. The degree of a point (p) is equal to the number of lines $[l] \in L(k)$ incident to it, i.e. the number of solutions of a system of the first k equations of (2.1). For a given (p), the solution is determined uniquely through the value assigned to l_1 , so there are q such solutions. Therefore the degree of any point in $D(k,q)$ is q. Similarly we get that the degree of any line in the graph is q, and the graph is q–regular. The same argument makes it clear that there is no more than one line incident to two distinct points and there is no more than one point incident to two distinct lines. This proves that $\Gamma(k,q)$ is a semiplane, and that $D(k,q)$ contains no 4–cycles. ■

Section 3. Main results.

Our goal now is to show that the girth $g(D(k,q)) \geq k+5$. This task will be greatly facilitated if we use some automorphisms of $D(k,q)$.

For every $x \in F_q$, let $t_1(x), t_2(x), t_{1,1}(x), t_{m,m+1}(x)$ and $t_{m+1,m}(x), m \geq 1$, $t_{m,m}(x)$ and $t'_{m,m}(x)$, $m \geq 2$, be maps of $P \to P$ and $L \to L$ defined by means of Table 1. An entry of the table shows the effect of the action of the corresponding map (top of the column) on the corresponding component of a line or a point (left end of the row). If the action of a map on the corresponding component of a point or a line is not defined by Table 1, it will mean that the component is fixed by the map. For example, the map $t_2(x)$ changes every component $l_{i,i+1}, i \geq 1$, of a line $[l]$ according to the rule : $l_{i,i+1} \to l_{i,i+1} + (l_{i,i} + l'_{i,i})x + l_{i,i-1}x^2$, and leaves every component $p_{i+1,i}, i \geq 1$, of a point (p) fixed; the map $t_{1,1}(x)$ changes every component $p_{i,i}, i \geq 1$, of a point (p) according to the rule $p_{i,i} \to p_{i,i} - p_{i-1,i-1}x$; the map $t_{5,6}(x)$ does not change components of any line $[l]$ (or any point (p)) which precede component $l_{5,6}$ (or $p_{5,6}$.)

$i \geq 0$	$t_1(x)$	$t_2(x)$	$t_{11}(x)$	$t_{m,m+1}(x)$ $m \geq 1$	$t_{m+1,m}(x)$ $m \geq 1$	$t_{m,m}(x)$ $m \geq 2$	$t'_{m,m}(x)$ $m \geq 2$
$l_{i,i}$		$+l_{i,i-1}x$	$-l_{i-1,i-1}x$	$+l_{r,r-1}x$, $r = i-m \geq 1$		$-l_{r,r}x$, $r = i-m \geq 0$	
$l_{i,i+1}$		$+(l_{i,i}+l'_{i,i})x+$ $+l_{i,i-1}x^2$	$-l_{i-1,i}x$	$+l'_{r,r}x$, $r = i-m \geq 0$		$-l_{r,r+1}x$, $r = i-m \geq 0$	
$l_{i+1,i}$	$+l_{i,i}x$		$+l_{i,i-1}x$		$-l_{r,r}x$, $r = i-m \geq 0$		$+l_{r+1,r}x$, $r = i-m \geq 0$
$l'_{i,i}$	$+l_{i-1,i}x$	$+l_{i,i-1}x$	$+l'_{i-1,i-1}x$		$-l_{r-1,r}x$, $r = i-m \geq 1$		$+l'_{r,r}x$, $r = i-m \geq 0$
$p_{i,i}$	$+p_{i-1,i}x$	$+p_{i,i-1}x$	$-p_{i-1,i-1}x$	$+p_{r,r-1}x$, $r = i-m \geq 1$		$-p_{r,r}x$, $r = i-m \geq 0$	
$p_{i,i+1}$		$+p'_{i,i}x$	$-p_{i,i-1}x$	$+p'_{r,r}x$, $r = i-m \geq 0$		$-p_{r,r+1}x$, $r = i-m \geq 0$	
$p_{i+1,i}$	$+(p_{i,i}+p'_{i,i})x+$ $+p_{i-1,i}x^2$		$+p_{i,i-1}x$		$-p_{r,r}x$, $r = i-m \geq 0$		$+p_{r+1,r}x$, $r = i-m \geq 0$
$p'_{i,i}$	$+p_{i-1,i}x$		$+p'_{i-1,i-1}x$		$-p_{r-1,r}x$, $r = i-m \geq 1$		$+p'_{r,r}x$, $r = i-m \geq 0$

$l_{0,0} = p_{0,0} = -1, l_{0,1} = p_{1,0} = 0; l_{1,0} = l_1; p_{0,1} = p_1; l'_{11} = l_{11}; p'_{11} = p_{11}; p'_{0,0} = l'_{0,0} = 1; p_{-1,0} = l_{0,-1} = p_{0,-1} = l_{-1,0} = 0$.

Table 1.

Proposition 3.1. For every $x \in F_q$, the maps $t_1(x), t_2(x), t_{1,1}(x); t_{m,m+1}(x)$ and $t_{m+1,m}(x), m \geq 1$; $t_{m,m}(x)$ and $t'_{m,m}(x), m \geq 2$, are automorphisms of $D(q)$, and their restrictions on $P(k) \cup L(k)$ are automorphisms of $D(k,q)$.

Proof. We shall prove the statement for $t_2(x)$ only. For other maps it can be done similarly. Obviously $t_2(-x) = t_2^{-1}(x)$. Let $(p)I[l]$ be an arbitrary pair of incident point and line of $D(q)$. In terms of components their incidence is given by system (2.1). The condition $(p)^{t_2(x)}I[l]^{t_2(x)}$ is

represented in terms of components by the following system:

$$\begin{cases} (l_{i,i} + l_{i,i-1}x) - (p_{i,i} + p_{i,i-1}x) = l_1(p_{i,i+1} + p'_{i-1,i-1}x) \\ (l'_{i,i} + l_{i,i-1}x) - p'_{i,i} = (p_1 + x)l_{i,i-1} \\ (l_{i,i+1} + (l_{i,i} + l'_{i,i})x + l_{i,i-1}x^2) - (p_{i,i+1} + p'_{i,i}x) = (p_1 + x)(l_{i,i} + l_{i,i-1}x) \\ l_{i+1,i} - p_{i+1,i} = l_1 p'_{i,i} \\ \text{for} \quad i = 1, 2, \dots \end{cases} \tag{3.1}$$

It is obvious that sytems (2.1) and (3.1) are equivalent for all $x \in F_q$, and therefore the map $t_2(x)$ is an automorphism of $D(q)$. Since the first k, $k \geq 2$, equations of (2.1) and (3.1) also form equivalent systems, the restriction of $t_2(x)$ on $P(k) \cup L(k)$ is an automorphism of $D(k, q)$. ■

Theorem 3.2. For all integers $k \geq 2$ and all prime powers q, graphs $D(q)$ and $D(k, q)$ are edge–transitive. For $q = 2^n, n \geq 1$, and any even integer $k \geq 2$, graphs $D(q)$ and $D(k, q)$ are vertex–transitive.

Proof. Let $(p)I[l]$ be an arbitrary pair of incident point and line in $D(q)$. We shall prove that for every $s \geq 1$, there exists an automorphism α_s of $D(q)$ such that both $(p)^{\alpha_s}$ and $[l]^{\alpha_s}$ have their first s components equal to zero .

The automorphism α_s will be constructed as a product of some automorphisms defined in Table 1. We start by applying $t_2(-p_1)$. Since $p_1 = p_{0,1}$ and $p'_{0,0} = 1$, $t_2(x)$ acts on the first component of (p) by the rule $p_1 \to p_1 + x$. Therefore $(p^1) = (p)^{t_2(-p_1)} = (0, p^1_{1,1}, p^1_{1,2}, \cdots)$. Let $[l^1] = [l]^{t_2(-p_1)}$. Consider the map $t_1(x)$. Since $l_1 = l_{1,0}$ and $l_{0,0} = -1$, $t_1(x)$ acts on the first component of $[l]$ by the rule $l_1 \to l_1 - x$, and at the same time it does not change the first component of any point. Therefore $(p^2) = (p^1)^{t_1(l_1)} = (0, p^2_{1,1}, p^2_{1,2}, \cdots)$ and $(l^2) = (l^1)^{t_1(l_1)} = (0, l^2_{1,1}, l^2_{1,2}, \cdots)$, and $\alpha_1 = t_2(-p_1)t_1(l_1)$. Consider the map $t_{1,1}(x)$. Since $p_{0,0} = l_{0,0} = -1$, and $p_{-1,0} = l_{-1,0} = 0$, $t_{1,1}(x)$ acts on the second component of any line $[l]$ by the rule $l_{1,1} \to l_{1,1} + x$, on the second component of any point (p) by the rule $p_{1,1} \to p_{1,1} + x$, and at the same time it does not change the first component or any point and any line. Therefore $(p^3) = (p^2)^{t_{1,1}(-p^2_{1,1})} = (0, 0, p^3_{1,2}, \cdots)$ and let $[l^3] = [l^2]^{t_{1,1}(-p^2_{1,1})}$. Since $(p^3)I[l^3]$, the first equation of (2.1) (for $i = 1$) gives $l^3_{1,1} - 0 = 0 \cdot 0$, so $l^3_{1,1} = 0$. Thus $\alpha_2 = \alpha_1 t_{1,1}(-p^2_{1,1})$. The last argument shows how one can continue by induction with respect to s. Suppose we have found the automorphism α_s, $s \geq 2$. Let $(p^{s+1}) = (p^s)^\beta$, where

$$\beta = \begin{cases} t_{a,a+1}(-p^s_{a,a+1}), & \text{if } s = 4a - 2; \\ t_{a+1,a}(-p^s_{a+1,a}), & \text{if } s = 4a - 1; \\ t_{a+1,a+1}(-p^s_{a+1,a+1}), & \text{if } s = 4a; \\ t'_{a+1,a+1}(-p'^s_{a+1,a+1}), & \text{if } s = 4a + 1. \end{cases}$$

Then β does not change the first s zero components of (p^s) and $[l^s]$, and makes the $(s+1)$–st component of (p^{s+1}) equal zero. Now (2.1) implies that the first $s+1$ components of $[l^{s+1}] = [l^s]^\beta$ are zeros. Set $\alpha_{s+1} = \alpha_s\beta$, and the proof of edge–transitivity of $D(k,q)$ is finished. The edge–transitivity of the infinite graph $D(q)$ follows from this, since any edge of $D(q)$ is an edge of $D(k,q)$ for some $k \geq 2$. The argument above also gives the transitivity of the automorphism group of $D(k,q)$ on each of the sets $P(k)$ and $L(k)$, and the transitivity of the automorphism group of $D(q)$ on each of the sets P and L. Consider a map $\phi: \quad V(D(q)) \to V(D(q))$, defined in the following way. For any point (p), $(p)^\phi = [l]$, where $l_{i,i+1} = p_{i+1,i},\ l_{i+1,i} = p_{i,i+1},\ l_{i+1,i+1} = p'_{i+1,i+1},\ l'_{i+1,i+1} = p_{i+1,i+1}$ for all $i = 0,1,2,\ldots$, and for any line $[l]$, $[l]^\phi = (p)$, where $p_{i,i+1} = l_{i+1,i},\ p_{i+1,i} = l_{i,i+1},\ p_{i+1,i+1} = l'_{i+1,i+1},\ p'_{i+1,i+1} = l_{i+1,i+1}$, for all $i = 0,1,2,\ldots$. It is a trivial verification , that if $char(F_q) = 2$, then ϕ is an automorphism of $D(q)$ which interchanges sets P and L and its restriction on the vertices of $D(2j,q)$ gives an automorphism of the latter graph which interchanges sets $P(2j)$ and $L(2j)$, $j \geq 1$. This fact together with transitivity of the automorphism group of $D(2j,q)$ on each of the sets $P(2j)$ and $L(2j)$ for all $j \geq 1$, proves the vertex–transitivity of these graphs. ■

Theorem 3.3. Let $k \geq 3$ be a positive odd integer, q be a positive prime power, and $g = g(D(k,q))$ be the girth of graph $D(k,q)$. Then $g \geq k+5$.

Proof. The idea of the proof is the following: for any distinct vertices x, y of $D(k,q)$ and any integer $m,\ 2 \leq m \leq (k+3)/2$, we show that there is no more than one simple path in $D(k,q)$ with the endpoints x and y of length m. When we say "simple path" we assume that all its vertices are distinct, and the length of a path is the number of its edges. This will imply that $g(D(k,q)) \geq k+5$, since $D(k,q)$ has no odd cycles. From now on let us denote $D(k,q)$ by G and its automorphism group by $Aut(G)$. We consider two different cases.

Case 1: $k = 4r-3,\ r \geq 2$. Let $[\tilde{l}^1]I(\tilde{p}^1)I[\tilde{l}^2]I\ldots I(\tilde{p}^r)I[\tilde{l}^{r+1}]$ be a simple path joining $[\tilde{l}^1]$ and $[\tilde{l}^{r+1}]$. By Theorem 3.2, $Aut(G)$ acts transitively on the set of lines. Therefore there exists $\alpha \in Aut(G)$ such that $[\tilde{l}^1]^\alpha = [0]$ – the line with all components equal to zero. Let the first component of $(\tilde{p}^1)^\alpha$ be z and $\beta = t_2(-z)$. Let $[l^i] = [\tilde{l}^i]^{\alpha\beta} = [l^i_1, l^i_{1,1}, \ldots, l^i_{r,r}], 1 \leq i \leq r+1$, and $(p^i) = (\tilde{p}^i)^{\alpha\beta} = (p^i_1, p^i_{1,1}, \ldots, p^i_{r,r}), 1 \leq i \leq r$. We have $[l^1] = [0]^\beta = [0], (p^1) = (0, p^1_{1,1}, \ldots, p^1_{r,r})$. Since $[l^1]I(p^1)$, incidence condition (2.1) implies that $(p^1) = (0)$. If two lines (points) are adjacent in

G to the same point (line), then they must coincide (this follows immediately from (2.1)). Therefore

$$l_1^i \neq l_1^{i+1}, i = 1, \ldots, r, \quad \text{and} \quad p_1^i \neq p_1^{i+1}, i = 1, \ldots, r-1. \tag{3.2}$$

In particular, $l_1^2 \neq 0$ and $p_1^2 \neq 0$.

Lemma 3.4. For all i, $2 \leq i \leq r$, $\quad l_{i-1,i-1}^i = l_{i-1,i}^i = l_{i,i-1}^i = l_{i,i}^i = p_{i,i}^i = p_{i-1,i}^i = p_{i,i}^{\prime i} = 0$.

Proof. To use induction, we introduce a linear order on the set of indices of components of points and lines in the following way. All components of a point (p^n) and a line $[l^n]$ will be written with the same superscript n. First we define a linear order $\prec$ on the set of four letters $\{p, p', l, l'\}$ as $l \prec l' \prec p \prec p'$. We encode indices of $p_{b,c}^a, p_{b,c}^{'a}, l_{b,c}^a, l_{b,c}^{'a}$ as ordered 4–tuples $(a, p, b, c), (a, p', b, c), (a, l, b, c), (a, l', b, c)$ respectively, where $a \in \{1, \ldots, r\}$; $b, c \in \{1, 2, \ldots, r\}, |b - c| \leq 1$. Indices of p_1^a, l_1^a are encoded as $(a, p, 0, 1), (a, l, 1, 0)$ respectively. From our set of 4–tuples we discard all 4–tuples of the form $(a, p', 1, 1)$ and $(a, l', 1, 1)$. Finally, assuming the usual ordering of integers, we define a linear order on the set of remaining 4–tuples lexicographically, and use for it the same notation $\prec$.

By using incidence condition (2.1) for the vertices of our path and the fact that $[l^1] = [0], (p^1) = (0)$, we obtain the following system:

$$\begin{aligned}
l_{i-1,i}^i &= p_{i-1,i}^{i-1} + p_1^{i-1} l_{i-1,i-1}^i \\
l_{i,i-1}^i &= p_{i,i-1}^{i-1} + l_1^i p_{i-1,i-1}^{'i-1} \\
l_{i,i}^i &= p_{i,i}^{i-1} + l_1^i p_{i-1,i}^{i-1} \\
l_{i,i}^{\prime i} &= p_{i-1,i-1}^{'i-1} + p_1^{i-1} l_{i-1,i-1}^i \\
p_{i-1,i}^i &= l_{i-1,i}^i - p_1^i l_{i-1,i-1}^i \\
p_{i,i}^i &= l_{i,i}^i - l_1^i p_{i-1,i}^i \\
p_{i,i}^{\prime i} &= l_{i,i}^{\prime i} - p_1^i l_{i,i-1}^i \ .
\end{aligned}$$

The equations of this system are ordered in such a way that for any choices of $l_1^i, p_1^i, i \geq 2$, the statement follows by a trivial induction on the set of indices ordered by $\prec$. ∎

Lemma 3.5. For all i, $2 \leq i \leq r$, $\quad l_{i,i-1}^{i+1} = (l_1^{i+1} - l_1^i)(p_1^{i-1} - p_1^i) l_{i-1,i-2}^i \neq 0$.

Proof. Using adjacency condition (2.1) and Lemma 3.4 we get: $l^{i+1}_{i,i-1} = p^i_{i,i-1} + l^{i+1}_1 p'^i_{i-1,i-1} = (l^i_{i,i-1} - l^i_1 p'^i_{i-1,i-1}) + l^{i+1}_1 p'^i_{i-1,i-1} = (0 - l^i_1 p'^i_{i-1,i-1}) + l^{i+1}_1 p'^i_{i-1,i-1} = (l^{i+1}_1 - l^i_1) p'^i_{i-1,i-1} = (l^{i+1}_1 - l^i_1)[l'^i_{i-1,i-1} - p^i_1 l^i_{i-1,i-2}] = (l^{i+1}_1 - l^i_1)[(0 + p^{i-1}_1 l^i_{i-1,i-2}) - p^i_1 l^i_{i-1,i-2}] = (l^{i+1}_1 - l^i_1)(p^{i-1}_1 - p^i_1) l^i_{i-1,i-2}$. Due to (3.2), $l^{i+1}_{i,i-1} \neq 0$ via trivial induction on i. ■

Now we are ready to finish the proof of the theorem in Case 1. We recall that $[l^{r+1}] = ([\tilde{l}^{r+1}]^\alpha)^\beta$, where $\beta = t_2(-z)$. If $[\tilde{l}^{r+1}]^\alpha = [a_1, a_{1,1}, \ldots, a_{r,r-1}, a_{r,r}]$, then $[l^{r+1}] = [a_1, a_{1,1} - a_1 z, \ldots, a_{r,r-1}, a_{r,r} - a_{r,r-1} z]$. Therefore $l^{r+1}_{r,r-1} = a_{r,r-1}$ and $l^{r+1}_{r,r} = a_{r,r} - l^{r+1}_{r,r-1} z$. Using $[l^{r+1}] I(p^r)$ and Lemma 3.4 we obtain $l^{r+1}_{r,r} - p^r_{r,r} = l^{r+1}_1 p^r_{r-1,r}$, or

$$a_{r,r} - l^{r+1}_{r,r-1} z = 0 \,. \tag{3.3}$$

According to Lemma 3.5, $l^{r+1}_{r,r-1} \neq 0$, and (3.3), considered as an equation with respect to z, has a unique solution. This means that $(\tilde{p}^1)^\alpha = (z, 0, 0, \ldots, 0)$ and point $(\tilde{p}^1)$ are determined uniquely by $a_{r,r-1}$ and $a_{r,r}$, and, therefore, by the endpoints $[\tilde{l}^1]$ and $[\tilde{l}^{r+1}]$ of the initial path. Therefore every simple path of length $2r$ between $[\tilde{l}^1]$ and $[\tilde{l}^{r+1}]$ passes through $(\tilde{p}^1)$, and no two simple paths of length $2r$ between any two given lines can have disjoint sets of interior vertices. This implies that G doesn't contain cycles of length $4r = k + 3$.

Case 2: $k = 4r - 1, r \geq 1$. The proof is very similar to the one in Case 1, and it is facilitated by the observation that for for an odd k, $k \geq 5$, the projection of a path in $D(k, q)$ on the first $k - 2$ components gives a path in $D(k - 2, q)$, and therefore $g(D(k, q)) \geq g(D(k - 2, q))$. We start with a simple path $[\tilde{l}^1] I(\tilde{p}^1) I[\tilde{l}^2] I \ldots I[\tilde{l}^{r+1}] I(\tilde{p}^{r+1})$ of length $2r + 1$ between a line $[\tilde{l}^1]$ and a point $(\tilde{p}^{r+1})$. Let $\alpha \in Aut(G)$ be such that $[\tilde{l}^1]^\alpha = [0], (\tilde{p}^1)^\alpha = (z, 0, 0, \ldots, 0),\ (\tilde{p}^{r+1})^\alpha = (b_1, b_{1,1}, \ldots, b'_{r,r}, b_{r,r+1})$, and $\beta = t_2(-z)$. Let $[\tilde{l}^i]^{\alpha\beta} = [l^i]$ and $(\tilde{p}^i)^{\alpha\beta} = (p^i), i = 1, \ldots, r + 1$. Then $[l^1] = [0],\ (p^1) = (0)$, and $l^i_1 \neq l^{i+1}_1, p^i_1 \neq p^{i+1}_1, i = 1, \ldots, r$.

Lemma 3.6. For $r \geq 1$, $l^{r+1}_{r,r} = 0$, and $p'^{r+1}_{r,r} = (p^r_1 - p^{r+1}_1) l^{r+1}_{r,r-1} \neq 0$.

Proof. $l^{r+1}_{r,r} = p^r_{r,r} + l^{r+1}_1 p^r_{r-1,r} = 0 + l^{r+1}_1 \cdot 0 = 0$ due Lemma 3.4. Then we consider $p'^{r+1}_{r,r} = l'^{r+1}_{r,r} - p^{r+1}_1 l^{r+1}_{r,r-1} = (p'^r_{r,r} + p^r_1 l^{r+1}_{r,r-1}) - p^{r+1}_1 l^{r+1}_{r,r-1} = p'^r_{r,r} + (p^r_1 - p^{r+1}_1) l^{r+1}_{r,r-1}$. Due to Lemma 3.4, $p'^r_{r,r} = 0$, and due to Lemma 3.5, $l^{r+1}_{r,r-1} \neq 0$. Since $p^r_1 \neq p^{r+1}_1$, the proof is completed. ■

We are ready to finish the proof of the theorem in Case 2. Since $(p^{r+1}) = (b_1 - z, \ldots, b'_{r,r}, b_{r,r+1} -$

$b'_{r,r}z$), and $b'_{r,r} = p'^{r+1}_{r,r}$, the incidence condition $[l^{r+1}]I(p^{r+1})$ gives $l^{r+1}_{r,r+1} - (b_{r,r+1} - p'^{r+1}_{r,r}z) = p_1^{r+1}l^{r+1}_{r,r}$. Using Lemma 3.6, we get

$$(l^{r+1}_{r,r+1} - b_{r,r+1}) + p'^{r+1}_{r,r}z = 0\ . \tag{3.4}$$

According to Lemma 3.6, $p'^{r+1}_{r,r} \neq 0$, and (3.4), considered as an equation with respect to z, has a unique solution. Like in Case 1, this implies that G has no cycles of length $4r+2$, and $g(G) \geq 4r+4 = k+5$. ■

References.

[1]. C.T. Benson, Minimal regular graphs of girths eight and twelve, *Canad. J. Math.* **18** (1966), pp. 1091–1094.

[2]. F. Bien, Constructions of telephone networks by group representations, *Notices Amer. Math. Soc.* **36**, 1989, pp. 5–22.

[3]. N.L. Biggs, Graphs with large girth, *Ars Combinatoria*, 25–C (1988) 73–80.

[4]. 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).

[5]. N.L. Biggs and M.J. Hoare, The sextet construction for cubic graphs, *Combinatorica* **3** (1983), 153–165.

[6]. B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[7]. J. A. Bondy and M. Simonovits, Cycles of even length in graphs, *J. Combinatorial Theory (B)*, **16** (1974), pp. 97–105.

[8]. A.E. Brouwer, A.M. Cohen, A. Neumaier, *Distance – Regular Graphs*. Springer–Verlag, Heidelberg–New York, 1989.

[9]. Fan K. Chung, Constructing random–like graphs. In "Probabilistic Combinatorics and its Applications." *Lecture Notes, A.M.S.*., San Francisco, 1991, pp. 1–24.

[10]. R.J. Faudree and M. Simonovits, On a class of degenerate extremal graph problems, *Combinatorica* **3 (1)** (1983), pp. 83–93.

[11]. W. Imrich, Explicit construction of graphs without small cycles, *Combinatorica* **2** (1984) 53–59.

[12]. W.M. Kantor, Generalized polygons, SCABs and GABs, In Buildings and the Geometry of Diagrams, Proceedings Como 1984, *Lecture Notes in Math.* **1181**, (L.A. Rosati, ed.), Springer Verlag, Berlin, 1986, pp. 79–158.

[13]. F. Lazebnik, V. Ustimenko , New examples of graphs without small cycles and of large size, to appear in *European Journal of Combinatorics*.

[14]. A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (3) (1988), pp. 261–277.

[15]. G.A. Margulis, Explicit construction of graphs without short cycles and low density codes, *Combinatorica*, **2**, 1982, pp. 71–78.

[16]. G.A. Margulis, Arithmetic groups and graphs without short cycles, *6th Internat. Symp. on Information Theory, Tashkent* 1984*, Abstracts, Vol. 1*, pp. 123–125 (in Russian).

[17]. G.A. Margulis, Some new constructions of low–density parity check codes. *3rd Internat. Seminar on Information Theory, convolution codes and multi–user communication, Sochi*, 1987, pp. 275–279 (in Russian).

[18]. G.A. Margulis, Explicit group–theoretical construction of combinatorial schemes and their application to the design of expanders and concentrators, *Journal of Problems of Information Transmission*, 1988, pp. 39–46 (translation from *Problemy Peredachi Informatsii*, vol. 24, No. 1, pp. 51–60, January–March 1988).

[19]. S. Payne and J.A. Thas, *Finite generalized quadrangles*, Pitman, New York, 1985.

[20]. M. Simonovits, Extremal 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.

[21]. V.A. Ustimenko, On some properties of geometries of the Chevalley groups and their generalizations, in *Studies in Algebraic Theory of Combinatorial Objects*, Moskow 1986, The English version will appear in Kluwer Publ., Dordresht, 1991, pp. 112–121.

[22]. V.A. Ustimenko and A. J. Woldar, An improvement on the Erdős bound for graphs of girth 16, submitted for publication.

[23]. A.I. Weiss, Girth of bipartite sextet graphs, *Combinatorica* **4**(2–3) (1984) pp. 241–245.

[24]. R.Wenger, Extremal graphs with no C^4, C^6,or C^{10}'s, *J. of Combinatorial Theory*, Series **B 52**, pp. 113-116 (1991)

[25]. A. J. Woldar, personal communication, 1992.

Felix Lazebnik
Department of Mathematical Sciences
University of Delaware
Newark, Delaware 19716, U.S.A.

Vasiliy A. Ustimenko
Department of Mathematics and Mechanics
Kiev State University
6 Glushkov Prospect, Kiev–252127, The Ukraine.