GRAPHS OF PRESCRIBED GIRTH AND BI–DEGREE[1]

Z. FÜREDI

Department of Mathematics

University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

F. LAZEBNIK

Department of Mathematical Sciences

University of Delaware, Newark, DE 19716, USA

Á. SERESS

Department of Mathematics

The Ohio State University, Columbus, OH 43210, USA

V. A. USTIMENKO

Department of Mathematics and Mechanics

University of Kiev, Kiev 252127, Ukraine

and

A. J. WOLDAR[2]

School of Mathematics

Institute for Advanced Study, Princeton, NJ 08540, USA

Abstract

We say that a bipartite graph $\Gamma(V_1 \cup V_2, E)$ has bi-degree r, s if every vertex from V_1 has degree r and every vertex from V_2 has degree s. Γ is called an (r, s, t)–graph if, additionally, the girth of Γ is $2t$. For $t > 3$, very few examples of (r, s, t)–graphs were previously known. In this paper we give a recursive construction of (r, s, t)–graphs for all $r, s, t \geq 2$, as well as an algebraic construction of such graphs for all $r, s \geq t \geq 3$.

1. Introduction

All graphs in this paper are assumed to be simple and bipartite. A bipartite graph $\Gamma(V_1 \cup V_2, E)$ is said to be *biregular* if there exist integers r, s such that deg(x)=r for all $x \in V_1$ and deg(y)=s for all $y \in V_2$. In this case, the pair r, s is called the *bi-degree* of Γ.

[1] This research was partially supported by NSF grants DMS–9115473, DMS–9304580, CCR–9201303, and NSA Grant MDA904-92-H-3046.

[2] On leave from Villanova University.

By an (r, s, t)–*graph* we shall mean any biregular graph with bi-degree r, s and girth (i.e. length of smallest cycle) exactly $2t$.

Trivially, $(r, s, 2)$–graphs exist for all $r, s \geq 2$ (e.g. complete bipartite graphs). For all $r, t \geq 2$, Erdős and Sachs (see [3],[10]) constructed r-regular graphs with girth t; from such graphs Γ, $(r, 2, t)$–graphs can be obtained by inserting a new vertex on each edge of Γ. For $r, s, t \geq 3$, the problem of existence of (r, s, t)–graphs was motivated by a question in [11] regarding semi–Moore graphs. These are (r, s, t)–graphs for which $r > s \geq 3$ and $t \geq 3$. Biregular graphs with girth at least 6 were studied extensively in the last 150 years, in the context of geometric configurations (see, e.g., a survey [2]). Calling the two classes of vertices of the graph points and lines, respectively, we obtain an incidence structure of a geometry with each line containing s points and each point contained in r lines. The girth condition means that no two points lie on two common lines. Steiner systems are a special case. From the known constructions, it can be deduced that $(r, s, 3)$ graphs exist for all $r, s \geq 3$. However, apart from certain isolated examples such as even cycles, generalized polygons, and cages, very little is known for $t > 3$.

The purpose of this paper is to show that (r, s, t)–graphs exist in abundance. In fact, we prove:

Theorem A. *There exist* (r, s, t)*–graphs for all* $r, s, t \geq 2$.

We give two constructions: an *algebraic* one and a *recursive* one. Using the algebraic method, we can prove only that (r, s, t)–graphs exist in the case $r, s \geq t$; however, the graphs obtained by this method have nicer structure. For example, we prove the following result, which shows that an (r, s, t)–graph can be chosen to possess the following interesting property.

Theorem B. *Let* $t \geq 3$ *and* $r, s \geq t$. *Then there exists an* (r, s, t)*–graph* Γ *such that for all* $r \geq r_1 \geq t$ *and* $s \geq s_1 \geq t$, Γ *contains an induced* (r_1, s_1, t)*–subgraph.*

From a geometric point of view, (r, s, t)–graphs are most interesting if the number of vertices is relatively small. A trivial lower bound on the number of vertices is $N(r, s, t) := [(r-1)(s-1)]^{(t-1)/2}$; the number of vertices in (r, s, t)–graphs constructed by the algebraic method is at most $(cr)^{ct}$ ($r \geq s \geq t$, c is an absolute constant). The recursive method gives (r, s, t)–graphs of much larger order. However, we shall describe a procedure which, given any (r, s, t)–graph, constructs an (r, s, t)–graph with the number of vertices bounded by a polynomial of $N(r, s, t)$.

The paper is organized as follows. In Section 2 we introduce the graphs $D(k, q)$ which are the central objects of our algebraic construction. A method of producing girth cycles (of size $k+5$, k odd) is described in Section 3, and the algebraic construction and proof of Theorem B are given in Section 4. In Section 5 we give explicit examples of girth cycles constructed by the method of Section 3, and state some conjectures. Finally, in Section 6, we describe the recursive construction (proving Theorem A) and explain in detail the procedure for reducing the number of vertices as discussed in the previous paragraph.

2. The family $D(k,q)$

The graphs $D(k,q)$ which we define below were introduced in [6] in the context of extremal graph theory. Their relevance in that paper stems from the fact that they have girth at least $k+5$ when k is odd and satisfy $e = \Omega(v^{1+1/k}),\ v \to \infty$, where v is number of vertices and e is number of edges. Later in [8], it was shown that for $k \geq 6$ graphs $D(k,q)$ are disconnected, and, for an infinite sequence of values of v, each of its component has size $e = \Omega(v^{1+\frac{4}{3k+3+2\epsilon}})$, where $\epsilon = 0$ if $\frac{k+3}{2}$ is odd, and $\epsilon = 1$ if $\frac{k+3}{2}$ is even. To our knowledge, this is the best known asymptotic lower bound for the size of a graph of order v containing no $(k+3)$–cycle for all odd k, $k \geq 19$. (In fact, it is known that $e = O(v^{1+\frac{2}{k+3}}),\ v \to \infty$, for any family of $(k+3)$–cycle free graphs [1], [4].)

From our current perspective, what makes the graphs $D(k,q)$ so critically important is their increasing girth and the ease with which one can obtain biregular graphs with prescribed bi–degree as induced subgraphs. This latter property was explored in an earlier paper with the graphs $B(q)$ (see [7]), whose definition, like that of $D(k,q)$, was motivated by certain properties of affine root systems (see [12]).

The main obstacle which confronts us in the pursuit of the algebraically constructed (r,s,t)–graphs is that of determining the exact girth of $D(k,q)$. As this girth was shown to be at least $k+5$ for k odd (see [6]), we now assume the task of constructing, whenever possible, a $(k+5)$–cycle in $D(k,q)$. Although we conjecture that such cycles exist for all k odd and q at least 5, our methods are amenable only to the case $k = 2t-5$, $t \geq 3$, and q any prime power of the form $1+mt$, $m \geq 1$.

We now give the definition of graphs $D(k,q)$. The reader is referred to [6] for additional information on these graphs, although only the definition is required for our development.

Let q be a prime power, and let P and L be two copies of the countably infinite dimensional vector space V over $GF(q)$. Elements of P will be called *points* and those of L *lines*. In order to distinguish points from lines we introduce the use of 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 coordinates of points and lines introduced in [6]:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots),$$

$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots).$$

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

$$\begin{aligned}
&l_{11} - p_{11} = l_1 p_1 \\
&l_{12} - p_{12} = l_{11} p_1 \\
&l_{21} - p_{21} = l_1 p_{11} \\
&l_{ii} - p_{ii} = l_1 p_{i-1,i} \\
&l'_{ii} - p'_{ii} = l_{i,i-1} p_1 \\
&l_{i,i+1} - p_{i,i+1} = l_{ii} p_1 \\
&l_{i+1,i} - p_{i+1,i} = l_1 p'_{ii}
\end{aligned}$$

(The last four relations are defined for $i \geq 2$.) These relations, which we call the *incidence relations* of (P, L, I), actually become adjacency relations for a related bipartite graph. We speak now of the *incidence graph* of (P, L, I), which has 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. Incidence I_k is then defined by imposing the first $k-1$ incidence relations and ignoring all others. The incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, q)$. Finally, we define $D(1, q)$ to coincide with $D(2, q)$ as this will allow us to state the results of Section 3 in a unified manner.

3. Girth cycles in $D(k,q)$

The main purpose of this section is to prove the following result.

Theorem C. Let k be odd, $k \geq 1$, and let q be any prime power in the arithmetic progression $\{1+n(\frac{k+5}{2})\}_{n\geq 1}$. Then the girth of $D(k,q)$ is $k+5$.

The proof will be based on the existence of a special automorphism of $D(k,q)$, where k and q are related as in the theorem statement. Before proceeding, we make several observations which will help to clarify our methods.

Suppose u and v are adjacent vertices of a graph Γ, and σ is an automorphism of Γ of order m. Then the edge $\{u,v\}$ is mapped by σ to the edge $\{u^\sigma, v^\sigma\}$, which in turn is mapped to $\{u^{\sigma^2}, v^{\sigma^2}\}$, and so on. Clearly, $\{u^{\sigma^m}, v^{\sigma^m}\} = \{u,v\}$, though this equality may hold for smaller powers of σ. Assume now that that Γ is bipartite with bipartition $V_1 \cup V_2$, that each of V_1 and V_2 is σ–invariant, that vertex v is adjacent to u^σ and that $u \neq u^\sigma$, $v \neq v^\sigma$. Then we claim that girth of Γ is at most $2m$, Indeed, as v and u^σ are adjacent, so are v^{σ^i} and $u^{\sigma^{i+1}}$ for all i; similarly u^{σ^i} is adjacent to v^{σ^i}. But then

$$\pi = uvu^\sigma v^\sigma u^{\sigma^2} v^{\sigma^2} \ldots u^{\sigma^{m-1}} v^{\sigma^{m-1}} uv$$

must contain a $2j$–cycle for some j, $2 \leq j \leq m$. (Indeed, the assumption that $u \neq u^\sigma$ and $v \neq v^\sigma$ precludes the possibility that any edge of π be transversed twice in succession.) This proves that the girth is at most $2j$, so at most $2m$ as claimed.

Applying this reasoning to the graphs $D(k,q)$, we seek point $(p) \in P_k$, line $[l] \in L_k$, and automorphism σ, such that

(1) σ has order $\frac{k+5}{2}$,

(2) σ preserves points and lines (i.e., each of the sets P_k and L_k are σ–invariant),

(3) $(p) \neq (p)^\sigma$ and $[l] \neq [l]^\sigma$,

(4) $[l]$ is adjacent to each of (p) and $(p)^\sigma$.

By the argument above, this will establish that the girth of $D(k,q)$ is at most $k+5$. As this girth is known to be at least $k+5$ (for $k \geq 3$ see [6]; case $k = 1$ is left to the reader), the theorem will follow.

Note. We could not see from the incidence relations how to construct a graph automorphism whose order depends only on k, the number of coordinates of the vertices. In contrast, it is easy to construct automorphisms whose order (as well as many other important properties) depends on the underlying field $GF(q)$. This explains the somewhat unusual dependence between k and q which appears in the statement of the theorem.

Proof of Theorem C. Let k and q be as in the statement of the theorem, with $q = 1+mt$, $t = \frac{k+5}{2}$. Let α be a primitive element of $GF(q)$, i.e. a generator of the multiplicative group $GF(q)^*$. Set $\beta = \alpha^m$. Assuming $k \equiv 1 \pmod 4$ (the argument is similar for $k \equiv 3 \pmod 4$), define the mapping σ on points and lines as follows:

$$(p)^\sigma = (\beta p_1, \beta^2 p_{11}, \beta^3 p_{12}, \beta^3 p_{21}, \beta^4 p_{22}, \beta^4 p'_{22}, \beta^5 p_{23}, \dots, \beta^{2j} p_{jj})$$

$$[l]^\sigma = (\beta l_1, \beta^2 l_{11}, \beta^3 l_{12}, \beta^3 l_{21}, \beta^4 l_{22}, \beta^4 l'_{22}, \beta^5 l_{23}, \dots, \beta^{2j} l_{jj})$$

where $j = \frac{k+3}{4}$. It is immediate from the incidence relations that σ is an automorphism of $D(k,q)$. It has order t because this is the order of β in $GF(q)^*$. Thus we have found σ which satisfies (1) and (2).

Note. There is an easy way to remember the definition of σ by its action on point and line coordinates. Namely, the effect of σ on any coordinate is to multiply the entry of that coordinate by β^h, where h is the sum of subscripts which identify that coordinate position.

We now seek (p) and $[l]$ which satisfy (3) and (4). Since $\beta \neq 1$, (3) is trivially ensured if we insist that both of p_1 and l_1 is nonzero. For convenience, we set $p_1 = 1$ and $l_1 = 1$, although any choice of nonzero values will work.

As $[l]$ is to be adjacent to both (p) and $(p)^\sigma$, we get two sets of equations which must be simultaneously satisfied, namely,

$$\begin{aligned}
l_{11} - p_{11} &= 1 & \qquad l_{11} - \beta^2 p_{11} &= \beta \\
l_{12} - p_{12} &= l_{11} & l_{12} - \beta^3 p_{12} &= \beta l_{11} \\
l_{21} - p_{21} &= p_{11} & l_{21} - \beta^3 p_{21} &= \beta^2 p_{11} \\
l_{ii} - p_{ii} &= p_{i-1,i} & l_{ii} - \beta^{2i} p_{ii} &= \beta^{2i-1} p_{i-1,i} \\
l'_{ii} - p'_{ii} &= l_{i,i-1} & l'_{ii} - \beta^{2i} p'_{ii} &= \beta l_{i,i-1} \\
l_{i,i+1} - p_{i,i+1} &= l_{ii} & l_{i,i+1} - \beta^{2i+1} p_{i,i+1} &= \beta l_{ii} \\
l_{i+1,i} - p_{i+1,i} &= p'_{ii} & l_{i+1,i} - \beta^{2i+1} p_{i+1,i} &= \beta^{2i} p'_{ii}
\end{aligned}$$

Solving, we obtain

$$
\begin{array}{ll}
p_{11} = \frac{\beta-1}{1-\beta^2} & l_{11} = 1 + \frac{\beta-1}{1-\beta^2} \\
p_{12} = \left(\frac{\beta-1}{1-\beta^3}\right) l_{11} & l_{12} = \left(1 + \frac{\beta-1}{1-\beta^3}\right) l_{11} \\
p_{21} = \left(\frac{\beta^2-1}{1-\beta^3}\right) p_{11} & l_{21} = \left(1 + \frac{\beta^2-1}{1-\beta^3}\right) p_{11} \\
p_{ii} = \left(\frac{\beta^{2i-1}-1}{1-\beta^{2i}}\right) p_{i-1,i} & l_{ii} = \left(1 + \frac{\beta^{2i-1}-1}{1-\beta^{2i}}\right) p_{i-1,i} \\
p'_{ii} = \left(\frac{\beta-1}{1-\beta^{2i}}\right) l_{i,i-1} & l'_{ii} = \left(1 + \frac{\beta-1}{1-\beta^{2i}}\right) l_{i,i-1} \\
p_{i,i+1} = \left(\frac{\beta-1}{1-\beta^{2i+1}}\right) l_{ii} & l_{i,i+1} = \left(1 + \frac{\beta-1}{1-\beta^{2i+1}}\right) l_{ii} \\
p_{i+1,i} = \left(\frac{\beta^{2i}-1}{1-\beta^{2i+1}}\right) p'_{ii} & l_{i+1,i} = \left(1 + \frac{\beta^{2i}-1}{1-\beta^{2i+1}}\right) p'_{ii}
\end{array}
$$

(Note that all denominators are nonzero since $\beta^s \neq 1$ for all $1 \leq s < t$.) The resulting point (p) and line $[l]$ satisfy (3) and (4). Thus (p), $[l]$ and σ satisfy (1)–(4), and the girth of $D(k,q)$ is $k+5$. ■

4. The algebraic construction and proof of Theorem B

We are now ready to describe our first construction, which provides (r,s,t)–graphs for $r, s \geq t$.

Let $t \geq 3$ and $r, s \geq t$. We choose a prime q such that $q \geq r, s$ and q is of the form $1 + mt$, for some $m \geq 1$. The existence of q follows from the well known result of Dirichlet asserting the existence of infinitely many primes in arithmetic progressions. Moreover, the smallest such q is $O((r+s)^c)$, for any constant $c > 5.5$ (see [5], [9]).

Set $k = 2t - 5$. Let C be a cycle of length $2t$ in $D(k,q)$, constructed by the method of the previous section. The first coordinates of points (respectively, lines) on C comprise a t–element subset T_p (respectively, T_l) of $GF(q)^*$; let $R \subseteq GF(q)$ (respectively, $S \subseteq GF(q)$) be an r–element subset containing T_p (respectively, an s–element subset containing T_l). The vertex set $V_R \cup V_S$ of our (r,s,t)–graph $D(k,R,S)$ is defined as

$$
V_R = \{(p) \in P_k | p_1 \in R\},
$$
$$
V_S = \{[l] \in L_k | l_1 \in S\}.
$$

Note that $|V_R \cup V_S| = O((r+s)^{2ct})$. Finally, let $D(k,R,S)$ be the subgraph of $D(k,q)$ induced on $V_R \cup V_S$. $D(k,R,S)$ contains C, so the girth of $D(k,R,S)$ is $2t$.

It remains to show that $D(k,R,S)$ has bi-degree s, r. For fixed $(p) \in V_R$, and arbitrary $x \in S$, there exists a unique neighbor $[l]$ of (p) in $D(k,R,S)$ whose first coordinate l_1 equals to x. Since there are precisely s choices for x, the degree of (p) in $D(k,R,S)$ is s. Similarly, one shows that the degree of any $[l] \in V_S$ in $D(k,R,S)$ is r. ■

Proof of Theorem B. Given $t \geq 3$ and $r, s \geq t$, let the (r, s, t)–graph $D(k, R, S)$ be defined as above. For any r_1, s_1 with $r \geq r_1 \geq t$, $s \geq s_1 \geq t$, choose sets $R_1 \subseteq R$, $S_1 \subseteq S$, $|R_1| = r_1$, $|S_1| = s_1$ such that R_1, S_1 contain the first coordinates of points and lines of C (i.e. the sets T_p and T_l), respectively. Then $D(k, R_1, S_1)$ is an (r_1, s_1, t)–graph which is an induced subgraph of $D(k, R, S)$. ∎

5. Examples of girth cycles in $D(k, q)$

In this section we construct girth cycles for the graphs $D(k, q_0)$, $k = 1, 3, 5$, where q_0 is the smallest prime power of the form $1 + (\frac{k+5}{2})m$. We use the procedure which is implicit in the proof of Theorem C (with $p_1 = l_1 = 1$).

Example. $k = 1$: Here $q_0 = 4$ and $m = 1$ (so $\beta = \alpha$). We choose α to be a primitive element of $GF(4)$, i.e. α is a root of x^2+x+1 over $GF(2)$. The resulting 6–cycle is

$$(1, \alpha)\,[1, \alpha{+}1]\,(\alpha, 1)\,[\alpha, \alpha]\,(\alpha{+}1, \alpha{+}1)\,[\alpha{+}1, 1]\,(1, \alpha)$$

Example. $k = 3$: Here $q_0 = 5$ and $m = 1$ (so $\beta = \alpha$). We choose $\alpha = 2$ as primitive element of $GF(5)$. The resulting 8–cycle is

$$(1, 3, 3)\,[1, 4, 2]\,(2, 2, 4)\,[2, 1, 1]\,(4, 3, 2)\,[4, 4, 3]\,(3, 2, 1)\,[3, 1, 4]\,(1, 3, 3)$$

Example. $k = 5$: Here $q_0 = 11$ and $m = 2$. We choose $\alpha = 2$ as primitive element of $GF(11)$, so that $\beta = \alpha^2 = 4$. The resulting 10–cycle is

$$(1, 2, 3, 10, 10)\,[1, 3, 6, 1, 2]\,(4, 10, 5, 2, 8)\,[4, 4, 10, 9, 6]\,(5, 6, 1, 7, 2)\,[5, 9, 2, 4, 7]$$
$$(9, 8, 9, 8, 6)\,[9, 1, 7, 3, 10]\,(3, 7, 4, 6, 7)\,[3, 5, 8, 5, 8]\,(1, 2, 3, 10, 10)$$

Naturally, we would like to remove the restriction $r, s \geq t$ in the algebraic construction and in Theorem B. We conjecture the following.

Conjecture 1. *For all $r, s \geq 2$ and $t \geq 3$, an (r, s, t)–graph can be obtained as a subgraph of a graph $D(k, q)$, with k, q chosen appropriately.*

Almost all cases of Conjecture 1, namely those for which $r, s \geq 5$, would follow immediately from a proof of

Conjecture 2. *$D(k, q)$ has girth $k{+}5$ for all odd k and all $q \geq 5$.*

Remark. The graphs $D(k,3)$ appear to have girth greater than $k+5$ for small values of k. For example, $D(5,3)$ has girth 12.

6. The recursive construction

Our first goal in this section is to prove Theorem A. We prove the existence of (r,s,t)–graphs by induction. The base cases are the existence of $(r,s,2)$, $(r,2,t)$, and $(2,s,t)$–graphs; as mentioned in the introduction, such graphs exist.

Let $\Gamma_1(A_1 \cup B_1, E_1)$ and $\Gamma_2(A_2 \cup B_2, E_2)$ be $(r-1,s,t)$ and $(r,s-1,t)$–graphs, respectively, $|A_1| = a$, $|B_2| = b$. Moreover, let $\Gamma_3(U \cup V, E_3)$ be an $(a,b,t-1)$–graph. Then we can construct an (r,s,t)–graph Γ the following way.

The graph Γ consists of $|U|$ copies of Γ_1 and $|V|$ copies of Γ_2 (all $|U|+|V|$ copies are pairwise disjoint), with some additional edges. So far, Γ has $|U||B_1|$ vertices of degree s, $|V||A_2|$ vertices of degree r, $|U|a$ vertices of degree $r-1$, and $|V|b$ vertices of degree $s-1$. Let us denote the set of vertices of degree $r-1$ by $A = \{a_{i,j} : 1 \le i \le |U|, 1 \le j \le a\}$. The vertices $a_{i,1}, a_{i,2}, ..., a_{i,a}$ belong to the ith copy of Γ_1. Similarly, let $B = \{b_{i,j} : 1 \le i \le |V|, 1 \le j \le b\}$ be the set of vertices of degree $s-1$. Note that $|A| = |B|$. We shall add a matching M between A and B to Γ, resulting in a biregular graph with bi-degree r, s.

We now describe how the edges in the matching M are defined. Let $U = \{u_1, u_2, ..., u_{|U|}\}$ and $V = \{v_1, v_2, ..., v_{|V|}\}$ be the two classes of Γ_3. For each $u_i \in U$, we list in a sequence $(v_{i_1}, v_{i_2}, ..., v_{i_a})$ all the neighbors of u_i in Γ_3; similarly, for $v_i \in V$, we list in a sequence $(u_{i_1}, ..., u_{i_b})$ all the neighbors of v_i. For $a_{i,j} \in A$ and $b_{k,l} \in B$, let $\{a_{i,j}, b_{k,l}\} \in M$ if and only if $\{u_i, v_k\} \in E_3$, v_k is the jth neighbor of u_i, and u_i is the lth neighbor of v_j. It is clear that M is a matching, covering the sets A, B; note that for any copies of Γ_1, Γ_2 in Γ, there is at most one edge of M connecting them. Moreover, contracting each copy of Γ_1, Γ_2, only the edges of M remain and we obtain a graph isomorphic to Γ_3.

Finally, we have to check that the girth of Γ is $2t$. Γ contains copies of Γ_1, so the girth is at most $2t$. Let C be an arbitrary cycle in Γ. If C contains no edges from M, then $|C| \ge 2t$. If C contains edges of M, then at the contraction of all copies of Γ_1, Γ_2, the image of C is isomorphic to a cycle in Γ_3. Hence C contains at least $2t-2$ edges from M. Between two consecutive edges from M, C must contain at least two edges from a copy of Γ_1 or Γ_2; hence $|C| \ge 3(2t-2) > 2t$. ■

In (r,s,t)–graphs constructed by the recursive method, the number of vertices is not bounded by a polynomial of the trivial lower bound $N(r,s,t)$ (we defined $N(r,s,t)$ in the introduction). Our final goal is to construct (r,s,t)–graphs with order bounded by a polynomial of $N(r,s,t)$.

Lemma D. *Let $\Gamma(U\cup V,E)$ be a biregular graph with bi-degree r,s and girth at least $2t$, $t\geq 3$. Suppose that there exist $x\in U$, $y\in V$ with distance $2t+3$ in Γ. Then there exists a biregular graph on $|U|+|V|-(r+s)$ vertices with bi-degree r,s and girth at least $2t$.*

Proof: Let $N(x):=\{v_1,...,v_r\}$ be the set of neighbors of x and $N(y):=\{u_1,...,u_s\}$ be the set of neighbors of y in Γ. Let Γ' be the graph obtained from Γ by deleting $x,v_2,v_3,...,v_r,y,u_2,u_3,...,u_s$. Since the girth of Γ is at least 6 and the Γ–distance $d_\Gamma(x,y)\geq 9$, there are no vertices in Γ' which were adjacent to two deleted vertices in Γ. Hence the degrees in Γ' are $r-1,s-1,r$, and s.

There are exactly $1+(r-1)(s-1)$ vertices of degree $r-1$ in Γ': namely, u_1 and the Γ–neighbors of $v_2,v_3,...,v_r$. Let A denote the set of these vertices. Similarly, there are $1+(r-1)(s-1)$ vertices of degree $s-1$ and we denote their set by B. For any $a\in A\setminus\{u_1\}$ and $b\in B\setminus\{v_1\}$, the Γ'–distance $d_{\Gamma'}(a,b)\geq 2t-1$, since adding four edges of Γ, any Γ'–path between a,b can be augmented to a Γ–path between x and y. For the same reason, $d_{\Gamma'}(a,u_1)\geq 2t$, $d_{\Gamma'}(b,v_1)\geq 2t$, and $d_{\Gamma'}(u_1,v_1)\geq 2t+1$. Also, for any $a,a'\in A\setminus\{u_1\}$, $d_{\Gamma'}(a,a')\geq 2t-4$ since adding at most four edges of Γ, any Γ'–path between a,a' can be augmented to a cycle in Γ. Similarly, $d_{\Gamma'}(a,v_1)\geq 2t-3$ and, for all $b,b'\in B\setminus\{v_1\}$, $d_{\Gamma'}(b,b')\geq 2t-4$, $d_{\Gamma'}(b,u_1)\geq 2t-3$.

Let Γ'' be the graph obtained by adding the edge (u_1,v_1) and a matching between $A\setminus\{u_1\}$ and $B\setminus\{v_1\}$ to Γ'. Clearly, Γ'' has bi-degree r,s and we also claim that the girth of Γ'' is at least $2t$.

Let C be an arbitrary cycle of Γ''. If C has no edges from $\Gamma''\setminus\Gamma'$, then $|C|\geq 2t$. If C contains exactly one edge of $\Gamma''\setminus\Gamma'$, then, checking the Γ'–distances listed above, we see that $|C|\geq 1+(2t-1)=2t$. Finally, if C contains at least two edges from $\Gamma''\setminus\Gamma'$ then $|C|\geq 2+2(2t-4)\geq 2t$. ■

Theorem E. *Let $r,s,t\geq 3$ and let Γ be an (r,s,t)–graph of minimum order. Then the number of vertices in Γ is bounded by a polynomial of $N(r,s,t)$.*

Proof: Let C be a cycle of length $2t$ in $\Gamma(V,E)$. Then the distance of any $x\in V$ from C is at most $2t+4$. Indeed, otherwise we can choose $x\in V$ of distance $2t+5$ from C, and y of distance $2t+3$ from x. Then none of the neighbors of x,y belong to C, and, since $d_\Gamma(x,y)=2t+3$ is an odd integer, x and y belong to distinct partitions of Γ. Applying the procedure described in the proof of Lemma D for such x,y, we obtain an (r,s,t)–graph, since the cycle C is contained in the new graph. However, this contradicts the minimality of Γ. Therefore, counting the greatest possible number of distinct vertices of Γ of distance $\leq 2t+4$ from C, we get

$$|V| \leq 2t+t(r-2)+t(s-2)+t(r-2)(s-1)+t(s-2)(r-1)+\cdots+t(r-2)(r-1)^{t+1}(s-1)^{t+2}+$$
$$t(s-2)(s-1)^{t+1}(r-1)^{t+2}.$$

Clearly, the right-hand-side is bounded from above by a polynomial of $N(r,s,t) = [(r-1)(s-1)]^{(t-1)/2}$. ■

Acknowledgment

We are grateful to Mr. Alexander Schliep, who designed computer programs which improved our understanding of the graphs $D(k,q)$, and to Professor Carl Pomerance for helpful discussions and for providing reference [5].

References

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

2. A.E. Brouwer and J.H. van Lint, Strongly regular graphs and partial geometries. In Enumeration and Design. Ed. by D.M. Jackson and S.A. Vanstone. Academic Press, Toronto, 1984, 85–122.

3. P. Erdős and H. Sachs, Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl, *Wiss. Z. Univ. Halle Martin Luther Univ. Halle–Wittenberg Math.–Natur.Reihe* **12** (1963), 251–257.

4. R. Faudree, M. Simonovits, On a class of degenerate extremal problems II, *Combinatorica* **3** (1) (1983), 83–93.

5. D.R. Heath–Brown, Zero–free regions for Dirichlet L–functions, and the least prime in an arithmetic progression, *Proc. London Math. Soc.* **64** (1992), 265–338.

6. F. Lazebnik and V.A. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, to appear in *Discrete Applied Math.*

7. F. Lazebnik, V.A. Ustimenko, and A.J. Woldar, New Constructions of Bipartite Graphs on m, n vertices, with many edges, and without small cycles; *Journal of Combinatorial Theory* Ser. B, **61** (1) (1994), pp. 111–117.

8. F. Lazebnik, V.A. Ustimenko, and A.J. Woldar, A New Series of Dense Graphs of High Girth, to appear in *Bulletin of the AMS.*

9. Y.V. Linnik, On the least prime in an arithmetic progression, I. The basic theorem, *Matematicheskii Sbornik* **15** (57) (1944), 139–178; II. The Deuring–Heilbronn's phenomenon, *Matematicheskii Sbornik* **15** (57) (1944), 347–368.

10. H. Sachs, Regular graphs with given girth and restricted circuits, *J. London Math. Society* **38** (1963), 423–429.

11. C.P. Teo and K.M. Koh, The number of Shortest Cycles and the Chromatic Uniqueness of a Graph, *Journal of Graph Theory* **16** (1) (1992), 7–15.

12. V.A. Ustimenko, A linear interpretation of the flag geometries of Chevalley groups. Kiev University. Translated from *Ukrainskii Matematicheskii Zhurnal*, Vol. 42, No. 3, pp. 383–387, March, 1990.