Girth 5 graphs from relative difference sets
Jørgensen, Leif Kjær

Publication date: 2005

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

? Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
? You may not further distribute the material or use it for any profit-making activity or commercial gain
? You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: oktober 18, 2018
Girth 5 graphs from relative difference sets

by

Leif Kjær Jørgensen
Girth 5 graphs from relative difference sets.

Leif K. Jørgensen
Department of Mathematical Sciences, Aalborg University
F. Bajers Vej 7, DK-9220 Aalborg Ø, Denmark

Abstract

We consider the problem of construction of graphs with given degree \( k \) and girth 5 and as few vertices as possible. We give a construction of a family of girth 5 graphs based on relative difference sets. This family contains the smallest known graph of degree 8 and girth 5 which was constructed by G. Royle, four of the known cages including the Hoffman-Singleton graph, some graphs constructed by G. Exoo and some new smallest known graphs.

Keywords: Cage, girth, Cayley graph, relative difference set.

A \((k, g)\) graph is a \(k\) regular graph with girth \(g\). Sachs [13] proved that for every \(k \geq 3\) and \(g \geq 5\) there exists a \((k, g)\) graph. The number of vertices in the smallest \((k, g)\) graph is denoted by \(f(k, g)\). A \((k, g)\) graph with \(f(k, g)\) vertices is called a \((k, g)\) cage. It is well-known that \(f(k, g) \geq n(k, g)\) where \(n(k, g)\) is the Moore bound

\[
n(k, g) = \begin{cases} 
\frac{k(k-1)\frac{g-1}{2} - 2}{k-2} & \text{if } g \text{ is odd} \\
\frac{2(k-1)^{\frac{g}{2}} - 2}{k-2} & \text{if } g \text{ is even}
\end{cases}
\]

In this paper we consider the case \(g = 5\). Then the Moore bound is \(n(k, 5) = k^2 + 1\). For \(k \leq 7\), the exact value of \(f(k, 5)\) is known, but for \(k \geq 8\) the difference between the upper and lower bound on \(f(k, 5)\) is large. In particular, for \(k = 8\) the Moore bound is \(n(8, 5) = 65\) but the smallest known \((8, 5)\) graph is a Cayley graph of order 80 constructed by Royle [12].

For a table of smallest known \((k, g)\) graphs we refer to Royle [12].

The unique cage of degree 7 is the graph constructed by Hoffman and Singleton [7]. It was observed by de Resmini and Jungnickel [6, Ex. 4.5]
(see Example 7 below) that the Hoffman-Singleton graph can be constructed from a relative difference set in a group of order 25 acting semiregularly on the graph.

Exoo [5] gave a construction of some new smallest \((k, 5)\) graphs for \(k = 8, 10, 11, 12, 13, 14\). This construction was also based on relative difference sets (or sets which are nearly relative difference sets) in a cyclic group acting semiregularly on the graph with two orbits of equal size.

Royle’s Cayley graph on 80 vertices can be constructed in a similar way from a non-abelian group.

In this paper we give a general construction of graphs with girth 5 from relative difference sets and from subgraphs of Cayley graphs.

We will first give a short introduction to the concepts used in the construction.

Let \(G\) be any finite group and let \(S \subseteq G\) be a subset not containing the group identity and with the property that \(g \in S \implies g^{-1} \in S\). Then the Cayley graph of \(G\) with connection set \(S\) is the graph Cay\((G, S)\) with vertex set \(G\) and edge set \(\{\{x, y\} \mid x, y \in G, xy^{-1} \in S\}\), where \(\{x, y\}\) denotes an edge joining the vertices \(x\) and \(y\).

A \((v, \kappa, \lambda)\) difference set in a group \(G\) of order \(v\) is a set \(S \subseteq G\) with \(|S| = \kappa\) such that for every non-identity element \(g \in G\) there exists exactly \(\lambda\) pairs \((s, t) \in S \times S\), where \(g = ts^{-1}\).

A \((v, \kappa, \lambda)\) difference set in a group \(G\) of order \(v\) is a set \(S \subseteq G\) with \(|S| = \kappa\) such that for every non-identity element \(g \in G\) there exists exactly \(\lambda\) pairs \((s, t) \in S \times S\) so that \(g = st^{-1}\).

The following well known theorem of Singer [14] gives an important class of difference sets.

**Theorem 1** Let \(q\) be a prime power. Then there exists a \((\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^d-1}{q-1})\) difference set in the cyclic group. In particular \((d = 2)\), there exists a \((q^2 + q + 1, q + 1, 1)\) difference set in the cyclic group.

It is also well known that for a prime power \(q\) and a \((q^2 + q + 1, q + 1, 1)\) difference set \(S \subset \mathbb{Z}_{q^2+q+1}\), the graph with vertex set \(\mathbb{Z}_{q^2+q+1} \times \{1, 2\}\) and edge set \(\{((a, 1), (a + s, 2)) \mid a \in \mathbb{Z}_{q^2+q+1}, s \in S\}\) is a \((q + 1, 6)\) cage.

**Definition 2** Let \(G\) be a group of order \(nm\) and let \(N \triangleleft G\) be a normal subgroup of order \(n\). A subset \(S \subseteq G\) is said to be a relative \((m, n, \kappa, \lambda)\) difference set with forbidden subgroup \(N\) if \(|S| = \kappa\) and for every non-identity element \(g \in G\) the number of pairs \((t, s) \in S \times S\) where \(g = ts^{-1}\) is exactly \(\lambda\) if \(g \notin N\) and 0 if \(g \in N\).
We refer to Pott [10] for basic theory of relative difference sets.

We can now state our main theorem. We note that in the application of relative difference sets in the construction of \((k,5)\) graphs we could replace exactly \(\lambda\) by at most \(\lambda\) in the above definition.

**Theorem 3** Let \(G\) be a group of order \(nm\) and let \(N \triangleleft G\) be a normal subgroup of order \(n\). Let \(Na_1, \ldots, Na_m\) be the cosets of \(N\). Suppose that \(S\) is a relative \((m, n, \kappa, 1)\) difference set in \(G\) with forbidden subgroup \(N\). Let \(\Delta\) be a Cayley graph of \(N\) and let \(H_1\) and \(H_2\) be \(\ell\)-regular graphs with vertex set \(N\) and with girth at least 5, such that \(H_1\) is a subgraph of \(\Delta\) and \(H_2\) is a subgraph of the complement of \(\Delta\).

Let \(\Gamma\) denote the graph with vertex set \(G \times \{1, 2\}\) and edges of the following types

**Type I** \(\{(g, 1), (gs, 2)\}\) for \(g \in G\) and \(s \in S\),

**Type II.1** \(\{(ga_i, 1), (ha_i, 1)\}\) for \(\{g, h\} \in H_1\) and \(i \in \{1, \ldots, m\}\),

**Type II.2** \(\{(ga_i, 2), (ha_i, 2)\}\) for \(\{g, h\} \in H_2\) and \(i \in \{1, \ldots, m\}\).

Then \(\Gamma\) has girth at least 5 and is regular of degree \(\kappa + \ell\).

**Proof** Since each vertex is incident with \(\kappa\) edges of type I and \(\ell\) edges of type II, \(\Gamma\) is \(\kappa + \ell\) regular.

Suppose that \(C\) is a cycle in \(\Gamma\) of length at most 4.

Since the subgraphs spanned by \(G \times \{1\}\) and \(G \times \{2\}\) consist of disjoint copies of \(H_1\) and \(H_2\), respectively, and both \(H_1\) and \(H_2\) have girth at least 5, \(C\) contains at least two edges of type I.

Suppose that \(\{(g, 1), (x, 2)\}\) and \(\{(h, 1), (x, 2)\}\), \(h \neq g\), are edges in \(\Gamma\). Then \(g\) and \(h\) are in different cosets of \(N\). This follows from the fact that there exists \(s, t \in S\) so that \(x = gs = ht\) and so \(h^{-1}g = ts^{-1} \notin N\).

If \((y, 2) \neq (x, 2)\) was another vertex adjacent to both \((g, 1)\) and \((h, 1)\) then \(y = gs_1 = ht_1\) for some \(s_1, t_1 \in S\) and \(h^{-1}g = ts^{-1} = t_1s_1^{-1}\). Since this contradicts \(\lambda = 1\) for the relative difference set \(S\), \(C\) contains at least one edge of type II.

If \(\{(g, 1), (gs, 2)\}\) and \(\{(g, 1), (gt, 2)\}\), \(s \neq t\), are edges in \(\Gamma\), i.e. \(s, t \in S\) then, since \(ts^{-1} \notin N\) and \(N\) is normal, \((gt)(gs)^{-1} = gts^{-1}g^{-1} \notin N\) and so \(gt\) and \(gs\) are in different cosets of \(N\).

It follows that if \((g, i)\) and \((h, i)\) have a common neighbour in \(G \times \{3 - i\}\) then \((g, i)\) and \((h, i)\) are in different connected component of the graph spanned by \(G \times \{i\}\).
Thus the only possible cycles of length at most 4 have vertices in the following cyclic order
\[(g_1, 1), (g_2, 1), (g_2 s, 2), (g_1 t, 2)\]
where \(s, t \in S\). Since \((g_1, 1)\) and \((g_2, 1)\) are adjacent, \(g_1\) and \(g_2\) are in the same coset, say \(N a_i\), and we can write \(g_1 = h_1 a_i, g_2 = h_2 a_i\) for some \(h_1, h_2 \in N\).

Since \((g_1 t, 2)\) and \((g_2 s, 2)\) are adjacent, \(g_1 t = h_1 a_i t\) and \(g_2 s = h_2 a_i s\) are in the same coset of \(N\). Thus
\[(h_1 a_i t)(h_2 a_i s)^{-1} = h_1 a_i t s^{-1} a_i^{-1} h_2^{-1} \in N\]
and so \(a_i t s^{-1} a_i^{-1} \in N\) and since \(N < G\), \(ts^{-1} \in N\). Since \(N\) is the forbidden subgroup, it follows that \(s = t\).

By the construction of type II edges, \(\{h_1, h_2\}\) is an edge in \(H_1\), and if we write \(a_i s = h a_j\) where \(h \in N\) then \(g_1 t = h a_i s = h h a_j\) and \(g_2 s = h_2 h a_j\) and so \(\{h_1 h, h_2 h\}\) is an edge in \(H_2\). Since \(H_1 \subseteq \Delta\), \(\{h_1, h_2\}\) is an edge in \(\Delta\) and so \(h_1 h_2^{-1}\) is in the connection set of \(\Delta\). Similarly, \(\{h_1 h, h_2 h\}\) is not an edge in \(\Delta\) and so the connection set of \(\Delta\) does not contain \((h_1 h)(h_2 h)^{-1} = h_1 h h^{-1} h_2^{-1} = h_1 h_2^{-1}\).

This contradiction proves that \(\Gamma\) does not contain any cycle of length at most 4. \(\square\)

The smallest value of \(\ell\) for which the construction in this theorem is interesting is \(\ell = 2\). In this case we need the following lemma. In the applications of the lemma, the group \(N\) is either cyclic or isomorphic to \(S_3\).

**Lemma 4** Let \(N\) be a group of order \(n \geq 5\). Then there exists graphs \(\Delta, H_1, H_2\) as in Theorem 3 with \(\ell = 2\), except if \(N\) is the quaternion group of order 8.

**Proof** We want to find \(\Delta\) so that the complement of \(\Delta\) has degree at least \(\frac{n}{2}\). Then, by a theorem of Dirac [4], we can take \(H_2\) to be a Hamiltonian cycle in the complement of \(\Delta\).

Suppose that \(N\) has an element \(g\) of order at least 5. Then we can take \(H_1 = \Delta = \text{Cay}(N, \{g, g^{-1}\})\). Thus we may assume that \(N\) does not have any element of order at least 5 and so, by Sylow’s theorems, \(n = 2^i 3^j\), for some \(i, j\).

Suppose that \(j \geq 2\). Then \(N\) has a subgroup \(H\) of order 9. Since \(N\) does not have any element of order at least 5, \(H\) is the non-cyclic group of order 9, \(H \simeq \mathbb{Z}_3 \times \mathbb{Z}_3\).
Since \( S = \{(1, 0), (2, 0), (0, 1), (0, 2)\} \subset H \) has the property that \( \text{Cay}(H, S) \) is a self-complementary 4 regular Hamiltonian graph, we choose \( \Delta = \text{Cay}(N, S) \). So we assume that \( j \in \{0, 1\} \).

Suppose first that \( i \leq 2 \). Then \( n = 6 \) or \( n = 12 \). If \( n = 6 \) and every element has order at most 4 then \( N = S_3 \). In this case we take \( H_1 = \Delta = \text{Cay}(S_3, \{(1 2), (1 3)\}) \). For \( n = 12 \) the lemma is true if \( N \) has a subgroup of order 6. If \( N \) does not have a subgroup of order 6 then \( N = A_4 \). In this case we choose \( \Delta = \text{Cay}(A_4, \{(1 2 3), (1 3 2), (1 2)(3 4)\}) \) and \( H_1 \) is a Hamilton cycle in \( \Delta \).

Suppose now that \( i \geq 3 \). Then \( N \) has a (non-cyclic) subgroup \( H \) of order 8. If \( H \) is not the quaternion group then there exists \( S \subset H \) so that \( \text{Cay}(H, S) \) is the cube graph and then we can take \( \Delta = \text{Cay}(N, S) \). Thus we may assume that every subgroup of order 8 is isomorphic to the quaternion group.

Since every group of order 16 has a subgroup of order 8 not isomorphic to the quaternion group, the lemma is true if 16 divides \( n \).

Since every group of order 24 has a subgroup of order 6, the lemma is true for \( n = 24 \). \( \Box \)

We can now start constructing graphs with girth 5.

**Example 5** \( \{0\} \subset \mathbb{Z}_5 \) is trivially a relative \((1, 5, 1, 1)\) difference set. The construction in Theorem 3 combined with Lemma 4 gives the Petersen graph.

One general construction of relative difference sets was found by Dembowsk and Ostrom [2].

**Theorem 6** Let \( q \) be an odd prime power and let \( G \) be the additive group of \( GF(q) \). Then \( \{(x, x^2) \mid x \in GF(q)\} \subset G \times G \) is a relative \((q, q, q, 1)\) difference set with forbidden subgroup \( \{0\} \times G \).

**Example 7** For \( q = 5 \), we find that \( \{(0, 0), (1, 1), (2, 4), (3, 4), (4, 1)\} \subset \mathbb{Z}_5 \times \mathbb{Z}_5 \) is a relative difference set. The construction in Theorem 3 combined with Lemma 4 gives a 7 regular graph with girth 5 and 50 vertices, i.e. the Hoffman Singleton graph.

For other values of \( q \) we get smaller graphs from the following construction of relative difference sets. This construction was found by Bose [1] and Elliot and Butson [3].
Theorem 8 For every prime power $q$ and every positive integer $d$ there exists a relative

\[
\left(\frac{q^d-1}{q-1}, q-1, q^{d-1}, q^{d-2}\right)
\]

difference set in the cyclic group of order $q^d - 1$. In particular, (for $d = 2$) there exists a cyclic relative $(q+1, q-1, q, 1)$ difference set.

Combining Theorem 3, Theorem 8 and Lemma 4 we get the following result which is essentially one of two constructions in Exoo [5]

Corollary 9 For every prime power $q \geq 7$, there exists a $q+2$ regular graph of girth 5 with $2(q^2-1)$ vertices.

In order to get other values of the degree, we may consider subgraphs of the graph constructed in Theorem 3.

Theorem 10 Let $q \geq 7$ be a prime power and let $k \leq q+2$. Then there exists a $k$ regular graph with girth 5 and with $2(k-1)(q-1)$ vertices.

Proof Let $G$ be the cyclic group of order $(q+1)(q-1)$ and let $N$ be the subgroup of order $q-1$. Let $S \subset G$ be a relative $(q+1, q-1, q, 1)$ difference set with forbidden subgroup $N$. Let $\Gamma$ be the graph constructed in Theorem 3 with $\ell = 2$.

Since elements in $N$ do not occur as the difference of two elements in $S$, $S$ contains at most one element from each coset of $N$.

Since the parameters of the relative difference set satisfy $m - \kappa = 1$ there is a unique coset of $N$ containing no elements of $S$. Thus, for each coset $Na_i$ there is a unique coset $Na_{i'}$ so that $\Gamma$ has no edges from $Na_i \times \{1\}$ to $Na_{i'} \times \{2\}$.

Then the subgraph of $\Gamma$ spanned by

\[
\bigcup_{i=1}^{k-1} Na_i \times \{1\} \cup \bigcup_{i=1}^{k-1} Na_{i'} \times \{2\}
\]

has the required properties. \qed

Similarly, we obtain the following result from Theorem 6.

Theorem 11 Let $q \geq 5$ be a prime power and let $k \leq q+2$. Then there exists a $k$ regular graph with girth 5 and with $2q(k-2)$ vertices. \qed
With $k = 6$ and $q = 5$ we get a graph with 40 vertices. O’Keefe and Wong [9] and Wong [16] proved that this is the unique $(6, 5)$-cage. With $k = q = 5$ we get a graph with 30 vertices. This is one of four $(5, 5)$-cages, see Wegner [15], Yang and Zhang [17] and Meringer [8]. The Petersen graph can also be obtained from Theorem 11 with $k = 3$ and $q = 5$. The unique $(4, 5)$ cage has 19 vertices and was constructed by Robertson [11].

The smallest number of vertices in a $k$ regular graph of girth 5 is not known for any $k \geq 8$. For $8 \leq k \leq 16$, the following table lists the smallest number $n$ of vertices in a $k$ regular graph with girth 5 constructed in this paper. For $k = 10$ and $k = 13$ these graphs are exactly the graphs constructed by Exoo [5] and for $k = 8$ the graph was constructed by Royle [12].

<table>
<thead>
<tr>
<th>$k$</th>
<th>$n$</th>
<th>Construction</th>
<th>First constructed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>80</td>
<td>Ex. 13</td>
<td>Royle</td>
</tr>
<tr>
<td>9</td>
<td>96</td>
<td>Cor. 9</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>126</td>
<td>Cor. 9</td>
<td>Exoo</td>
</tr>
<tr>
<td>11</td>
<td>156</td>
<td>Ex. 12</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>216</td>
<td>Ex. 14</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>240</td>
<td>Cor. 9</td>
<td>Exoo</td>
</tr>
<tr>
<td>14</td>
<td>288</td>
<td>Thm. 17, $q = 13$</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>312</td>
<td>Thm. 17, $q = 13$</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>336</td>
<td>Thm. 17, $q = 13$</td>
<td></td>
</tr>
</tbody>
</table>

**Example 12** In the group $\mathbb{Z}_{13} \times S_3$ of order 78 the set
$$\{(1, I), (10, I), (11, I), (0, (12)), (5, (12)), (2, (23)), (8, (23)), (7, (13)), (9, (13))\}$$
where $I$ is the identity permutation, is a $(13, 6, 9, 1)$ relative difference set with forbidden subgroup $\{0\} \times S_3$, see Pott [10]. The construction in Theorem 3 gives an 11 regular graph with girth 5 and 156 vertices.

**Example 13** In the group $G = \langle x, y \mid x^8 = y^5 = 1, yx = xy^2 \rangle$ of order 40 with normal subgroup $N = \langle y \rangle$ the set $S = \{1, x, x^3, x^5y^4, x^5y, x^7y^3\}$ has the property that no non-identity element in $N$ can be written as $st^{-1}$ where $s, t \in S$ and all other elements in $G$ can be written as $st^{-1}$ for at most one pair $s, t \in S$. Using the construction in Theorem 3 we get an 8 regular graph with 80 vertices and girth 5. This graph was first constructed by Royle [12]. The graph is vertex transitive with automorphism group of order 160. It is a Cayley graph of two groups of order 80.
Example 14 In the group $G = \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ of order 108 with normal subgroup $N = \langle (2,1,0,0) \rangle$ the set $S = \{(0,0,0,0), (0,0,0,2), (0,0,1,0), (0,1,1,0), (1,0,1,2), (1,1,0,2), (1,1,2,1), (1,2,0,2), (2,1,2,0), (3,1,2,2)\}$ has the property that no non-identity element in $N$ can be written as $s - t$ where $s, t \in S$ and all other elements in $G$ can be written as $s - t$ for at most one pair $s, t \in S$. Using the construction in Theorem 3 we get a 12 regular graph with 216 vertices and girth 5.

We next consider the case $\ell = 3$ in Theorem 3. In this case $n$ must be even and $n \geq f(3,5) = 10$. It can be shown that $n = 10$ is not possible. Thus $n = 12$ is the first case where it is possible to have $\ell = 3$ in Theorem 3. In the next example we show that it is possible to have $\ell = 3$ if $n = 12$, except maybe if $N = A_4$.

Example 15 Let $\Delta = \text{Cay}(\mathbb{Z}_{12}, \{\pm 2, \pm 3, 6\})$. There are two cubic graphs with girth 5 and 12 vertices. In Figure 1, one these is shown as a subgraph of $\Delta$ and the other is shown as a subgraph of the complement of $\Delta$. Thus we can take the graphs in Figure 1 to be $H_1$ and $H_2$ in Theorem 3.

$\Delta$ is a Cayley of every group of order 12, except $A_4$.

Theorem 16 Let $N$ be a cyclic or dihedral group of order $n \geq 12$, $n$ even. Then there exists graphs $\Delta, H_1, H_2$ as in Theorem 3 with $\ell = 3$. 

8
Proof The case $n = 12$ was considered in Example 15. Thus we may assume that $n \geq 14$. Let $m = \frac{n}{2} \geq 7$. Then all differences of distinct elements in \{0, 1, 3\} are different in $\mathbb{Z}_m$. Thus the graph $H_1$ with vertex set $\mathbb{Z}_m \times \{1, 2\}$ and edges $\{(i, 1), (i + s, 2)\}$ where $i \in \mathbb{Z}_m$ and $s \in \{0, 1, 3\}$ has girth 6. The similar graph $H_2$ with $s \in \{2, 4, 5\}$ also has girth 6.

$H_1$ and $H_2$ are edge-disjoint Cayley graphs of the dihedral group.

Now denote the vertex $(i, j)$ by $x_{2i - j + 1}$. Then $H_1$ is a subgraph of $\Delta = \text{Cay}(\mathbb{Z}_n, \{\pm 1, \pm 5\})$ and $H_2$ is a subgraph of $\text{Cay}(\mathbb{Z}_n, \{\pm 3, \pm 7, \pm 9\})$. If $n \geq 16$ these graphs are disjoint.

If $n = 14$ then let $p = (1, 3, 4, 2)(5, 12, 11, 13, 8, 10, 9, 6)$ and redefine $H_2$ to be the graph with vertex set $\{x_i \mid i \in \mathbb{Z}_{14}\}$ and edge set $\{(x_{p(i)}, x_{p(j)}) \mid x_i, x_j \in H_1\}$.

As in Theorem 10 we get the following.

**Theorem 17** Let $q \geq 13$ be an odd prime power and let $k \leq q + 3$. Then there exists a $k$ regular graph with girth 5 and with $2(q^2 - 1)$ vertices.

For large values of $k$ we can get better results with $\ell > 3$.

**Theorem 18** Let $\ell \geq 4$ and let $n \geq 16\ell^2$ be even. Let $N$ be a cyclic group of order $n$. Then there exists graphs $\Delta, H_1, H_2$ as in Theorem 3.

Proof By Chebyshev’s Theorem, there exists a prime $p$, so that $\ell - 1 \leq p < 2(\ell - 1)$. By Singer’s theorem there exists numbers $t_1, \ldots, t_{p+1}$ that form a difference set with $\lambda = 1$ modulo $p^2 + p + 1$. We may assume $-2\ell^2 < t_1 < \ldots < t_\ell < 2\ell^2$. Let $r = \frac{p}{2}$. Then the differences $t_i - t_j$, $1 \leq i, j \leq \ell, i \neq j$ are all different modulo $r$. Thus the graph $H_1$ with vertex set $\mathbb{Z}_r \times \{1, 2\}$ and edges $\{(a, 1), (a + t_i, 2)\}$, for $a \in \mathbb{Z}_r, 1 \leq i \leq \ell$ has girth at least 6.

Now denote the vertex $(i, j)$ in $H_1$ by $x_{2i - j + 1}$. Then $x_{2a}$ is adjacent to $x_{2(a+i-1)}$, for $a \in \mathbb{Z}_n, 1 \leq i \leq \ell$. Thus $H_1$ is a subgraph of $\Delta = \text{Cay}(\mathbb{Z}_n, \{\pm (2i - 1) \mid 1 \leq i \leq \ell\}) \subseteq \text{Cay}(\mathbb{Z}_n, \{i \mid -4\ell^2 < i \leq 4\ell^2\})$.

Similarly, the graph $H_2$ with vertex set $\mathbb{Z}_r \times \{1, 2\}$ and edges $\{(a, 1), (a + t_i + 4\ell^2, 2)\}$, for $a \in \mathbb{Z}_r, 1 \leq i \leq \ell$ has girth at least 6 and is a subgraph of the complement of $\Delta$. \hfill \Box

Combining the Theorems 3, 8 and 18, we get the following.

**Corollary 19** Let $q$ be an odd prime power. Then there exists a $q + \lfloor \frac{\sqrt{q-1}}{4} \rfloor$ regular graph of girth 5 and with $2(q^2 - 1)$ vertices.
References


