Available online at www.sciencedirect.com

SCIENCE DIRECT®

ACADEMIC PRESS

Journal of Combinatorial Theory, Series A 104 (2003) 157–167

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Semidirect product constructions of directed strongly regular graphs ☆

Art M. Duval[a] and Dmitri Iourinski[b]

[a] *Department of Mathematical Sciences, University of Texas at El Paso, El Paso, TX 79968-0514, USA*

[b] *Department of Mathematics, Northeastern University, Boston, MA 02115, USA*

Received 23 May 2000

Communciated by Richard Wilson

Abstract

We construct a new infinite family of directed strongly regular graphs, as Cayley graphs of certain semidirect product groups. This generalizes an earlier construction of Klin, Munemasa, Muzychuk, and Zieschang on some dihedral groups.

Keywords: Directed strongly regular graph; Semidirect product; Cayley graph

1. Introduction

Strongly regular graphs have been extensively studied (see e.g. [3,10]), and were generalized to directed strongly regular graphs in [4]. Klin et al. [9] constructed an infinite family of directed strongly regular graphs as Cayley graphs of D_{2m}, the dihedral group of order $2m$, for odd m (see also [7,11]). Dihedral groups may be realized as semidirect products. We extend the construction of Klin et al. to a larger family of semidirect products that includes the dihedral groups D_{2m} (m odd), all metacyclic groups, and other groups as well. We thus find a new infinite family of directed strongly regular graphs.

This construction relies upon group automorphisms with a certain symmetry condition we call the "q-orbit condition" (see Section 3). Our first main result,

☆ An earlier version of this work appeared in the second author's M.S. Thesis, written under the direction of the first author, at the University of Texas at El Paso.

E-mail addresses: artduval@math.utep.edu (A.M. Duval), diourins@lynx.neu.edu (D. Iourinski).

0097-3165/$ - see front matter
doi:10.1016/S0097-3165(03)00141-9

Theorem 3.3, shows how to build a directed strongly regular graph whenever an automorphism with this condition exists. We follow that with general examples of such automorphisms, culminating in our second main result, Corollary 4.3, which gives the parameter sets of all the directed strongly regular graphs we can construct from these automorphisms. It seems likely that there are still other automorphisms with the q-orbit condition, which would therefore lead to new directed strongly regular graphs.

We start in Section 2 with a review of the definitions of directed strongly regular graphs and Cayley graphs, and of a condition that makes it easy to check whether a Cayley graph is directed strongly regular. Section 3 contains the statement and proof of our first main result (Theorem 3.3), including the definition of the q-orbit condition. In Section 4, we find automorphisms with this condition, and, in our second main result (Corollary 4.3), use them to construct directed strongly regular graphs. We also include in this section several specific examples of the construction. Section 5 briefly concludes with a list of the parameters of all the new directed strongly regular graphs we have constructed with at most 100 vertices.

2. Graphs

We begin by establishing the graph theory notation we use.

We say $G = (V, E)$ is a *directed graph* with vertices V if $E \subseteq V \times V - \{(v, v) : v \in V\}$. We call the elements of E the edges of G, and, when $(v, w) \in E$, we say there is an edge from v to w, and write $v \to w$. Note that we disallow loops $v \to v$, but we do allow a pair of vertices v, w to simultaneously satisfy $v \to w$ and $w \to v$, and we refer to such a pair of edges as a *bidirected edge*.

If v is a vertex of a directed graph then the *indegree* of v is the number of vertices w such that $w \to v$, and the *outdegree* is the number of vertices w such that $v \to w$. A directed graph is *regular* of degree k if every vertex has indegree and outdegree k.

The *length* of a directed path $v_0 \to v_1 \to \cdots \to v_m$ is m, the number of edges in the path.

Definition. A regular directed graph of degree k with n vertices is a *directed strongly regular graph* (*dsrg*) on the parameters (n, k, μ, λ, t) if the number of directed paths of length two from any vertex v to any vertex w is exactly λ if $v \to w$, exactly t if $v = w$ (this may be interpreted as the number of bidirected edges adjacent to any vertex), and exactly μ otherwise (i.e., when there is no edge from v to w, even though there may be an edge from w to v).

Directed strongly regular graphs are quite rare and there are numerous limitations on the possible sets of parameters (see [4] for these limitations and other details about dsrg's). For instance, there are only 127 possible parameter sets for a dsrg with 40 or fewer vertices (for the list of possible parameters, see [11]). For many of these parameter sets, it is not known if there is a dsrg with those parameters.

The directed strongly regular graphs we construct will be Cayley graphs.

Definition. Let S be a subset of a group G, such that $\langle S \rangle = G$. The *Cayley graph* of G, denoted $\mathscr{C}(G,S)$, is the directed graph with elements of G as its vertices, where $g \to h$ if and only if $g^{-1}h \in S$. (See e.g. [1, Section VIII.1].)

Hereafter, we will denote the identity element of a group G by e_G, or simply e if the group of which it is the identity is clear from context.

Definition. For any finite group G the *group ring* $\mathbf{Z}[G]$ is defined as the set of all formal sums of elements of G, with coefficients from $\mathbf{Z}$. The operations $+$ and $\cdot$ on $\mathbf{Z}[G]$ are given by

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g$$

and

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} (a_g b_h) gh.$$

The group ring $\mathbf{Z}[G]$ is a ring with multiplicative identity e. For any subset X of G, we use $\overline{X}$ to denote the element of $\mathbf{Z}[G]$ that is the sum of all elements of X, namely

$$\overline{X} = \sum_{x\in X} x.$$

Later, the following simple observation will be key:

Lemma 2.1. *If G is a finite group and $g \in G$, then*

$$g\overline{G} = \overline{G}.$$

Proof. Multiplying each of the elements of G by g simply permutes the elements of G (i.e., the map $\phi : G \to G$ given by $\phi : h \mapsto gh$ is a bijection). Thus $\{gh : h \in G\} = G$, and the lemma follows. $\square$

Proposition 2.3 below allows us to express necessary conditions for a Cayley graph to be directed strongly regular in terms of the group ring. This condition was first applied to dsrg's by Klin et al. [9] (but see [11] for a more detailed exposition); we sketch its proof for completeness. Most of the work is in the following lemma.

Lemma 2.2. *The number of paths of length 2 from g to h in $\mathscr{C}(G,S)$ equals the coefficient of $g^{-1}h$ in $\overline{S}^2$.*

Proof. The coefficient of $g^{-1}h$ in $\overline{S}^2$ is the number of ordered pairs $(s_1, s_2) \in S \times S$ such that $s_1 s_2 = g^{-1}h$. But there is a bijection between such pairs and paths $g \to v \to h$

in $\mathscr{C}(G,S)$, given by $s_1 = g^{-1}v$ and $s_2 = v^{-1}h$ in one direction, and $v = gs_1 = hs_2^{-1}$ in the other direction. $\square$

Proposition 2.3. *A Cayley graph $\mathscr{C}(G,S)$ is a directed strongly regular graph with parameters (n,k,μ,λ,t) if and only if $|G| = n$, $|S| = k$, and*

$$\overline{S}^2 = te + \lambda\overline{S} + \mu(\overline{G} - e - \overline{S}).$$

Proof. Suppose $\overline{S}^2 = te + \lambda\overline{S} + \mu(\overline{G} - e - \overline{S})$. By Lemma 2.2 then, the number of paths of length 2 from g to h is: t if $g^{-1}h = e$, i.e. if $h = g$; λ if $g^{-1}h \in S$, i.e. if $g \to h$; and μ otherwise. Since $\mathscr{C}(G,S)$ is clearly regular of degree $|S|$, we have that $\mathscr{C}(G,S)$ is a directed strongly regular graph.

The reverse direction is a direct consequence of Lemma 2.2, with $g = e$. $\square$

3. Semidirect products

In this section, we prove our first main result (Theorem 3.3), which shows how to construct directed strongly regular Cayley graphs whose groups are certain semidirect products.

Definition. Let $\theta : B \to \operatorname{Aut} A$ be an action of a group B on another group A. Let $A \times_\theta B$ be the direct product set of A and B, i.e., the set of pairs (a,b) of elements $a \in A$ and $b \in B$, with the following operation for the product of two elements

$$(a,b)(a',b') = (a[\theta(b)(a')], bb').$$

Then $A \times_\theta B$ forms a group of order $|A|\,|B|$ with identity element (e_A, e_B) and inverse $(a,b)^{-1} = (\theta(b^{-1})(a^{-1}), b^{-1})$. This group is called the *semidirect product* of A and B with respect to the action θ. (See e.g. [12, Section 1.8].)

As A is isomorphic to the subgroup $A \times e_B$ in $A \times_\theta B$, and B is isomorphic to $e_A \times B$, we will abuse notation and write $a = (a, e_B)$ for $a \in A$ and $b = (e_A, b)$ for $b \in B$. It is then easy to verify that $ab = (a,b)$ and

$$ba = (\theta(b)(a))b \tag{1}$$

for $a \in A,\ b \in B$.

Example 3.1. Let A be the cyclic group of order m, generated by element a, and let B be the two-element group with nontrivial element b. Let $\theta(b) : a \mapsto a^{-1}$, so $ba = a^{-1}b$. It is then easy to verify that $A \times_\theta B = D_{2m}$, the *dihedral group* of order $2m$, which was used by Klin et al. [9], when m is odd, and by Hobart and Shaw [7] and Shaw [11], when m is even, to generate new families of directed strongly regular graphs. Theorem 3.3 generalizes the construction of Klin et al. to other semidirect products (see Example 3.4).

Example 3.2. Let $C_p = \langle a \rangle$ and $C_q = \langle b \rangle$ be multiplicative cyclic groups of prime orders p and q respectively, such that $p > q$ and $q|(p-1)$. Let s be an integer such that $s \not\equiv 1 \pmod p$ and $s^q \equiv 1 \pmod p$, which implies $s \not\equiv 0 \pmod p$. (The proof of Lemma 4.1 will show how to find such an s.) The map $\beta \in \operatorname{Aut} C_p$ given by $\beta : a^i \mapsto a^{si}$ is thus an automorphism of order q, and the map $\theta : C_q \to \operatorname{Aut} C_p$ given by $\theta(b^r) = \beta^r$ is a homomorphism. Then

$$C_p \times_\theta C_q = \langle a, b : a^p = b^q = e,\ ba = a^s b \rangle$$

is a group of order pq, called the *metacyclic group*. (See e.g. [8, p. 99].) Theorem 3.3 applies to all metacyclic groups as a special case; see Corollary 4.4.

Definition. Recall that an *orbit* of an automorphism β of a group A is a set $\{\beta^r(a) : r \in \mathbf{Z}\}$, where a is any element of A. The orbits of β partition A.

Definition. We will say that a group automorphism β has the *q-orbit condition* if each of its orbits (other than the trivial orbit consisting only of the group identity) contains q elements.

It is easy to see that $\beta \in \operatorname{Aut} A$ satisfies this condition if and only if:

$$\beta^q(a) = a, \quad \text{for all } a \in A; \text{ and} \tag{2}$$

$$\beta^r(a) = a \quad \text{implies } q|r, \text{ for all } a \neq e_A. \tag{3}$$

Theorem 3.3. *Let A be a finite group of order m. If some $\beta \in \operatorname{Aut} A$ has the q-orbit condition, then we may construct a directed strongly regular graph with parameters*

$$(mq,\ m-1,\ (m-1)/q,\ ((m-1)/q)-1,\ (m-1)/q)$$

as follows:

Let B be the cyclic group of order q, generated by $b \in B$, and define $\theta : B \to \operatorname{Aut} A$ by $\theta(b^r) = \beta^r$. (It is easy to see that θ is a homomorphism, as $|b| = |\beta|$.) Let A' be a set of representatives of the nontrivial orbits of β (in other words, A' contains exactly one member of every orbit of β, except the orbit consisting only of the identity). Then the Cayley graph

$$\mathscr{C}(A \times_\theta B, A' \times B)$$

is a directed strongly regular graph with the parameters listed above.

Proof. Let $G = A \times_\theta B$ and $S = A' \times B$. Since $\mu = \lambda + 1 = t = (m-1)/q$ in this case, it suffices, by Proposition 2.3, to show that

$$\overline{S}^2 + \overline{S} = \mu \overline{G}, \tag{4}$$

$|G| = n = mq$, and $|S| = k = m - 1$.

In order to establish Eq. (4), first compute in the group ring $\mathbf{Z}[G]$

$$\begin{aligned}
\overline{B}\,\overline{A'}\,\overline{B} &= \left(\sum_{r=0}^{q-1} b^r\right)\left(\sum_{a\in A'} a\right)\overline{B} = \sum_{r=0}^{q-1}\sum_{a\in A'} b^r a\overline{B} \\
&= \sum_{r=0}^{q-1}\sum_{a\in A'} \beta^r(a) b^r \overline{B} \quad \text{by Eq. (1)} \\
&= \sum_{r=0}^{q-1}\sum_{a\in A'} \beta^r(a)\overline{B} \quad \text{by Lemma 2.1} \\
&= \left(\sum_{r=0}^{q-1}\sum_{a\in A'} \beta^r(a)\right)\overline{B} \\
&= (\overline{A} - e_A)\overline{B}.
\end{aligned}$$

(The last equality is because A' is a set of representatives of the nontrivial orbits of β, and β has the q-orbit condition.) We may simplify this further by noting that $e_A b = (e_A, b) = b$ for any $b \in B$, so $e_A\overline{B} = \overline{B}$. Thus

$$\overline{B}\,\overline{A'}\,\overline{B} = (\overline{A} - e_A)\overline{B} = \overline{A}\,\overline{B} - \overline{B}. \tag{5}$$

Then

$$\begin{aligned}
\overline{S}^2 + \overline{S} &= (\overline{A' \times B})^2 + (\overline{A' \times B}) = (\overline{A'}\,\overline{B})^2 + (\overline{A'}\,\overline{B}) \\
&= \overline{A'}\,\overline{B}\,\overline{A'}\,\overline{B} + \overline{A'}\,\overline{B} \\
&= \overline{A'}(\overline{A}\,\overline{B} - \overline{B}) + \overline{A'}\,\overline{B} \quad \text{by Eq. (5)} \\
&= (\overline{A'}\,\overline{A})\overline{B} \\
&= (\,|A'|\overline{A})\overline{B} \quad \text{by Lemma 2.1} \\
&= |A'|\overline{A \times_\theta B} \\
&= |A'|\overline{G}.
\end{aligned}$$

It now only remains to note that

$$|G| = |A \times_\theta B| = |A|\,|B| = mq,$$

$$|S| = |A' \times B| = |A - \{e_A\}| = m - 1, \quad \text{and}$$

$$|A'| = |S|/|B| = (m-1)/q.$$

(The above equality $|A' \times B| = |A - \{e_A\}|$ is again because A' is a set of representatives for the nontrivial orbits of β, and β has the q-orbit condition.) $\square$

Example 3.4. Let A, B, and θ be as defined in Example 3.1, and let $\beta = \theta(b)$. Note that $\beta : a^i \mapsto a^{-i} = a^{m-i}$. If m is odd, the nontrivial orbits of β are all pairs $\{a^i, a^{m-i}\}$ $(i = 1, \ldots, (m-1)/2)$, and so in this case, β has the 2-orbit condition. We may then choose $A' = \{a, a^2, \ldots, a^{(m-1)/2}\}$, so $S = A' \times B =$

$\{a, a^2, \ldots, a^{(m-1)/2}, ab, a^2b, \ldots, a^{(m-1)/2}b\}$. Theorem 3.3 then states that $\mathscr{C}(D_{2m}, S)$ is a dsrg with parameters $(2m, m-1, (m-1)/2, ((m-1)/2)-1, (m-1)/2)$.

This specific case of Theorem 3.3 was found previously by Klin et al. [9, Section 6]; Hobart and Shaw [7] and Shaw [11] have a more elementary description of this construction, as well as a similar construction of a directed strongly regular Cayley graph on D_{2m} for even m.

Example 3.5. We may generalize Example 3.4 as follows. Let A be any group with no nontrivial involutions (i.e., $a \neq a^{-1}$ for any $a \in A$, except the identity). Let B and θ be as defined in Examples 3.1 and 3.4, so, once again, $\beta : a \mapsto a^{-1}$ for all $a \in A$, and $ba = a^{-1}b$ in $A \times_\theta B$. To pick A', simply choose one element from each pair $\{a, a^{-1}\}$. The special case when $A = \{a^f : f \in F\}$, where F is a finite field of cardinality 3 mod 4, and A' is chosen to be $\{a^r : r \text{ is a quadratic residue in } F\}$, was found by Fiedler et al. [5, Subsection 3.2.2, graph Γ_4].

The rest of the paper is concerned with finding other examples of A and β satisfying the conditions of Theorem 3.3.

4. Applications

In this section, we find automorphisms with the q-orbit condition, and use them to construct directed strongly regular graphs. Our second main result, Corollary 4.3, summarizes the parameter sets of all dsrg's so constructed.

Lemma 4.1. *Let F be a finite field of order p^α. If $q|(p^\alpha - 1)$, then there is an $s \in F$ such that the automorphism β of the group $(F, +)$ given by $\beta : a \mapsto sa$ has the q-orbit condition.*

Proof. The multiplicative group of F is cyclic of order $p^\alpha - 1$ (see e.g. [8, Theorem V.5.3]), say with generator u. Let $s = u^{(p^\alpha - 1)/q}$, so s has multiplicative order q. Then $\beta^q(a) = s^q a = a$ for all $a \in F$, and thus β satisfies condition (2).

To show that β satisfies condition (3), assume $\beta^r(a) = a$ for some $a \in F$, $a \neq 0$. Then $s^r a = a$, so $s^r = 1$, and so $q|r$, as s has multiplicative order q. Therefore β satisfies condition (3). $\square$

Proposition 4.2. *If $\beta_j \in \operatorname{Aut} A_j$ has the q-orbit condition for $j = 1, \ldots, N$, then*

$$\beta = \prod_{j=1}^{N} \beta_j \in \operatorname{Aut}\left(\prod_{j=1}^{N} A_j \right)$$

also has the q-orbit condition.

Proof. First note that since each β_j has the q-orbit condition, it satisfies condition (2), so

$$\beta^q(a_1, \dots, a_N) = (\beta_1^q(a_1), \dots, \beta_N^q(a_N)) = (a_1, \dots, a_N).$$

Thus β satisfies (2) as well.

Next, to show that β satisfies condition (3), assume that $(a_1, \dots, a_N) \neq e$, i.e., there is some j such that $a_j \neq e_{A_j}$. Then if $\beta^r(a_1, \dots, a_N) = (a_1, \dots, a_N)$, it follows that $\beta_j^r(a_j) = a_j$, so $q|r$, as β_j satisfies condition (3). Therefore β also satisfies (3). $\square$

Example 4.7 demonstrates how to construct the orbits of a product, and so suggests a constructive proof of Proposition 4.2.

Corollary 4.3. *Let $m = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ be the factorization of an integer m into prime powers. If $q|(p_j^{\alpha_j} - 1)$ for each j, then there is a directed strongly regular graph with parameters*

$$(mq,\ m-1,\ (m-1)/q,\ ((m-1)/q) - 1,\ (m-1)/q).$$

Proof. For $j = 1, \dots, N$, let A_j be the additive group of the finite field of order $p_j^{\alpha_j}$, and let $A = \prod_{j=1}^N A_j$. Clearly $|A| = m$.

By Lemma 4.1, there is a $\beta_j \in \operatorname{Aut} A_j$ with the q-orbit condition, for every j. By Proposition 4.2, then $\beta = \prod_{j=1}^N \beta_j \in \operatorname{Aut} A$ has the q-orbit condition.

The corollary now follows directly from Theorem 3.3. $\square$

In the rest of this section, we offer several examples of dsrg's constructed using (the proof of) Corollary 4.3. To simplify their presentation, we introduce notation allowing us to easily switch from an additive group to an isomorphic multiplicative group in the obvious way. Given an additive group G, we will let a^G denote the group $\{a^g : g \in G\}$ with group operation $(a^g)(a^h) = a^{g+h}$; similarly, for $\phi \in \operatorname{Aut} G$, we will define $a^\phi \in \operatorname{Aut} a^G$ by $a^\phi : a^g \mapsto a^{\phi(g)}$.

We will also write $A \times_\beta \langle \beta \rangle$ for the group $A \times_\theta B$ constructed in Theorem 3.3 out of group A and automorphism β, since in this construction θ is defined by β, and B is naturally isomorphic to the cyclic subgroup of $\operatorname{Aut} A$ generated by β.

A special case of Corollary 4.3 concerns metacyclic groups, which were defined in Example 3.2.

Corollary 4.4. *Every metacyclic group $C_p \times_\theta C_q$ has a Cayley graph that is directed strongly regular with parameters $(pq, p-1, (p-1)/q, ((p-1)/q) - 1, (p-1)/q)$.*

Proof. Following the construction of Theorem 3.3, Lemma 4.1, and Corollary 4.3, let $\widetilde{A} = (\mathbf{Z}_p, +)$, and define $\widetilde{\beta} \in \operatorname{Aut} \widetilde{A}$ by $\widetilde{\beta} : i \mapsto si$, where $s^q \equiv 1 \pmod p$ and $s \not\equiv 1 \pmod p$. The proof of Lemma 4.1 guarantees the existence of such an s, as $\mathbf{Z}_p$ is a field, and also shows that $\widetilde{\beta}$ has the q-orbit condition. Now let $A = a^{\widetilde{A}}$ and

$\beta = a^{\widetilde{\beta}}$; thus $A = C_p$, and $\beta \in \operatorname{Aut} C_p$ is defined by $\beta : a^i \mapsto a^{si}$. Of course, β has the q-orbit condition since $\widetilde{\beta}$ has the q-orbit condition. It is easy to see that $A \times_\beta \langle \beta \rangle$ is the metacyclic group $C_p \times_\theta C_q$. $\square$

Example 4.5. Let $m = p = 7$ and $q = 3$. The multiplicative group of $\mathbf{Z}_7$ is generated by $u = 3$, so let $s = u^{(p-1)/q} = 3^2 \equiv 2 \pmod 7$. (Alternatively, simply note $2^3 \equiv 1 \pmod 7$, but $2, 2^2 \not\equiv 1 \pmod 7$.) Let $A = C_7$, and let $\beta \in \operatorname{Aut} C_7$ be given by $\beta : a^i \mapsto a^{2i}$; then $A \times_\beta \langle \beta \rangle$ is the metacyclic group

$$C_7 \times_\theta C_3 = \langle a, b : a^7 = b^3 = e,\ ba = a^2 b \rangle.$$

The nontrivial orbits of $\theta(b) = \beta$ are $\{a \mapsto a^2 \mapsto a^4 \mapsto a\}$ and $\{a^3 \mapsto a^6 \mapsto a^5 \mapsto a^3\}$, so we may let $A' = \{a, a^3\}$. Then $S = \{a, ab, ab^2, a^3, a^3b, a^3b^2\}$, and the Cayley graph $\mathscr{C}(C_7 \times_\theta C_3, S)$ is directed strongly regular with parameters $(21, 6, 2, 1, 2)$.

Example 4.6. Let $m = 9 = 3^2$ and $q = 4$. The finite field of order 9 is isomorphic to $F = \mathbf{Z}_3[x]/(x^2+1)$. Its multiplicative group is generated by $u = x+1$, so let $s = u^{(m-1)/q} = (x+1)^2 = -x$. Then let $\widetilde{A} = (F, +)$, and define $\widetilde{\beta} \in \operatorname{Aut} \widetilde{A}$ by $\widetilde{\beta} : f(x) \mapsto sf(x) = -xf(x)$. The nontrivial orbits of $\widetilde{\beta}$ are $\{1 \mapsto -x \mapsto -1 \mapsto x \mapsto 1\}$, and $\{x+1 \mapsto -x+1 \mapsto -x-1 \mapsto x-1 \mapsto x+1\}$.

Now let $A = a^{\widetilde{A}}$ and $\beta = a^{\widetilde{\beta}}$, so $G = A \times_\beta \langle \beta \rangle$ is the group generated by a (whose exponents are polynomials with integer coefficients) and b subject to the relations $a^3 = b^4 = a^{x^2+1} = e$, and $ba^{f(x)} = a^{-xf(x)}b$. The nontrivial orbits of $\theta(b) = \beta : a^{f(x)} \mapsto a^{-xf(x)}$ are $\{a \mapsto a^{-x} \mapsto a^{-1} \mapsto a^x \mapsto a\}$, and $\{a^{x+1} \mapsto a^{-x+1} \mapsto a^{-x-1} \mapsto a^{x-1} \mapsto a^{x+1}\}$, so we may let $A' = \{a, a^{x+1}\}$. Then $S = \{a, ab, ab^2, ab^3, a^{x+1}, a^{x+1}b, a^{x+1}b^2, a^{x+1}b^3\}$, and the Cayley graph $\mathscr{C}(G, S)$ is directed strongly regular with parameters $(36, 8, 2, 1, 2)$.

Example 4.7. Let $m = 91 = 7 \cdot 13$ and $q = 3$. Let $A_1 = C_7 = \langle a_1 \rangle$, $A_2 = C_{13} = \langle a_2 \rangle$, and $A = A_1 \times A_2 = C_7 \times C_{13}$.

In Example 4.5, we found $\beta_1 \in \operatorname{Aut} C_7$ with nontrivial orbits $\{a_1 \mapsto a_1^2 \mapsto a_1^4 \mapsto a_1\}$ and $\{a_1^3 \mapsto a_1^6 \mapsto a_1^5 \mapsto a_1^3\}$; similarly, $\beta_2 \in \operatorname{Aut} C_{13}$ given by $\beta_2 : a_2^j \mapsto a_2^{3j}$ has nontrivial orbits $\{a_2 \mapsto a_2^3 \mapsto a_2^9 \mapsto a_2\}$, $\{a_2^2 \mapsto a_2^6 \mapsto a_2^5 \mapsto a_2^2\}$, $\{a_2^4 \mapsto a_2^{12} \mapsto a_2^{10} \mapsto a_2^4\}$, and $\{a_2^7 \mapsto a_2^8 \mapsto a_2^{11} \mapsto a_2^7\}$. Since β_1 and β_2 have the 3-orbit condition, so does $\beta = \beta_1 \times \beta_2 \in \operatorname{Aut} C_7 \times C_{13}$. Then

$$\begin{aligned} A \times_\beta \langle \beta \rangle &= (C_7 \times C_{13}) \times_\theta C_3 \\ &= \langle a_1, a_2, b : a_1^7 = a_2^{13} = b^3 = e,\ a_1a_2 = a_2a_1, \\ &\qquad ba_1 = a_1^2 b,\ ba_2 = a_2^3 b \rangle. \end{aligned}$$

There are 30 nontrivial orbits of $\theta(b) = \beta : a_1^i a_2^j \mapsto a_1^{2i} a_2^{3j}$; rather than list them all, we will describe how to construct them. Every orbit is of the form $\{a_1^{i_1}a_2^{j_1} \mapsto a_1^{i_2}a_2^{j_2} \mapsto a_1^{i_3}a_2^{j_3} \mapsto a_1^{i_1}a_2^{j_1}\}$ where $O_1 = \{a_1^{i_1} \mapsto a_1^{i_2} \mapsto a_1^{i_3} \mapsto a_1^{i_1}\}$ and $O_2 = \{a_2^{j_1} \mapsto a_2^{j_2} \mapsto a_2^{j_3} \mapsto a_2^{j_1}\}$ are orbits of β_1 and β_2, respectively. Note that either (but not both) of O_1 and O_2 may be trivial, and that there are 6 such orbits of β where O_1 or O_2 is trivial, one for each of the nontrivial orbits of β_1 and β_2. If neither O_1 nor O_2 is trivial, then there are 3 different orbits of β that can be made from O_1 and O_2: $\{a_1^{i_1}a_2^{j_1} \mapsto a_1^{i_2}a_2^{j_2} \mapsto a_1^{i_3}a_2^{j_3} \mapsto a_1^{i_1}a_2^{j_1}\}$, $\{a_1^{i_1}a_2^{j_2} \mapsto a_1^{i_2}a_2^{j_3} \mapsto a_1^{i_3}a_2^{j_1} \mapsto a_1^{i_1}a_2^{j_2}\}$, and $\{a_1^{i_1}a_2^{j_3} \mapsto a_1^{i_2}a_2^{j_1} \mapsto a_1^{i_3}a_2^{j_2} \mapsto a_1^{i_1}a_2^{j_3}\}$. Thus the remaining 24 orbits of β, where O_1 and O_2 are nontrivial, may be chosen by picking one of the 2 nontrivial orbits of β_1 for O_1, one of the 4 nontrivial orbits of β_2 for O_2, and then picking one of the 3 possible orbits of β that can be made from O_1 and O_2.

We may pick the elements of A' in a particularly nice way. From orbits of β with nontrivial O_1 (including those with trivial O_2), pick $a_1^i a_2^j$ such that $a_1^i \in A_1'$; from the remaining 4 orbits, pick a_2^j such that $a_2^j \in A_2'$. (Here A_1' and A_2' stand for the set A' constructed when building dsrg's from A_1 and A_2, respectively.) Then it is not hard to see that $A' = A_1'A_2 \cup A_2' = \{a_1^i a_2^j : i = 1, 3;\ j = 0, \ldots, 12\} \cup \{a_2^j : j = 1, 2, 4, 7\}$. Finally, $S = A' \cup A'b \cup A'b^2$, and the Cayley graph $\mathscr{C}((C_7 \times C_{13}) \times_\theta C_3, S)$ is directed strongly regular with parameters $(273, 90, 30, 29, 30)$.

5. Parameters

Table 1 lists the parameters of all new directed strongly regular graphs with at most 100 vertices that can be constructed using Corollary 4.3. Two infinite families of dsrg's whose parameters fit the formula of Corollary 4.3 were already known, and are therefore excluded:

Table 1
Parameters of new dsrg's, $n \leqslant 100$

(n,k,μ,λ,t)	(m,q)
$(21,6,2,1,2)$	$(7,3)$
$(36,8,2,1,2)$	$(9,4)$
$(39,12,4,3,4)$	$(13,3)$
$(48,15,5,4,5)$	$(16,3)$
$(52,12,3,2,3)$	$(13,4)$
$(55,10,2,1,2)$	$(11,5)$
$(57,18,6,5,6)$	$(19,3)$
$(68,16,4,3,4)$	$(17,4)$
$(78,12,2,1,2)$	$(13,6)$
$(80,15,3,2,3)$	$(16,5)$
$(84,27,9,8,9)$	$(28,3)$
$(93,30,10,9,10)$	$(31,3)$
$(100,24,6,5,6)$	$(25,4)$

When $q = m - 1$, the parameters become $(m(m-1), m-1, 1, 0, 1)$, and the corollary only applies when m is the power of a prime. Dsrg's with these parameters for any value of m, not just powers of primes, were constructed in [4, Section 8]. It is a straightforward exercise to verify that the two constructions give isomorphic graphs.

When $q = 2$, the parameters become $(2m, m-1, (m-1)/2, ((m-1)/2) - 1, (m-1)/2)$, and m must be odd (otherwise, not only does the corollary not apply, but $(m-1)/2$ is not even an integer). These dsrg's were constructed by Klin et al. [9], as described in Example 3.4; when m is a prime power congruent to $3 \bmod 4$, they were also constructed by Fiedler et al., as described in Example 3.5. When m is a prime power congruent to $1 \bmod 4$, dsrg's with these parameters were constructed in [4, Section 5], but that construction yields different graphs than the ones here (for instance, if $m = 5$, then $t = 2$, and so the set of bidirected edges form a union of cycles, which in [4, Section 5] is always a pair of 5-cycles, but here, for any choice of A', is a union of even cycles).

After this paper was submitted for publication, Godsil et al. [6] announced on Brouwer's dsrg website [2, Section 2.12, Construction T12] a construction that generalizes ours, and which is purely combinatorial.

Acknowledgments

We are grateful for helpful suggestions from Piotr Wojciechowski, and an anonymous referee.

References

[1] B. Bollobás, Modern Graph Theory, Springer, New York, 1998.
[2] A.E. Brouwer, S.A. Hobart, Parameters of directed strongly regular graphs, http://homepages.cwi.nl/~aeb/math/dsrg/dsrg.html
[3] P.J. Cameron, Strongly regular graphs, in: L.W. Beineke, R.J. Wilson (Eds.), Selected Topics in Graph Theory, Academic Press, New York, 1978, pp. 337–360.
[4] A.M. Duval, A directed graph version of strongly regular graphs, J. Combin. Theory Ser. A 47 (1988) 71–100.
[5] F. Fiedler, M.H. Klin, M. Muzychuk, Small vertex-transitive directed strongly regular graphs, Discrete Math. 255 (2002) 87–115.
[6] C.D. Godsil, S.A. Hobart, W. Martin, in preparation.
[7] S.A. Hobart, T.J. Shaw, A note on a family of directed strongly regular graphs, European J. Combin. 20 (1999) 819–820.
[8] T.W. Hungerford, Algebra, Springer, New York, 1974.
[9] M. Klin, A. Munemasa, M. Muzychuk, P.-H. Zieschang, Directed strongly regular graphs via coherent (cellular) algebras, preprint, 1997.
[10] J.J. Seidel, Strongly regular graphs, in: B. Bollobas (Ed.), Surveys in Combinatorics: Proceedings of the Seventh British Combinatorial Conference, London Mathematical Society, Lecture Notes Series, Vol. 38, Cambridge University Press, Cambridge, 1979, pp. 157–180.
[11] T.J. Shaw, Directed Strongly Regular Graphs, Master's Thesis, University of Wyoming, 1998.
[12] M. Suzuki, Group Theory I, Springer, New York, 1982.