AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **34** (2006), Pages 3–15

Cayley maps with given exponents and distribution of inverses

Ľubica Líšková

Department of Mathematics
Faculty of Civil Engineering
Slovak University of Technology
Radlinského 11, 813 68 Bratislava
Slovak Republic
ls@math.sk

Abstract

A Cayley map is a Cayley graph embedded in an oriented surface in such a way that the cyclic order of generators is the same at each vertex. The distribution of inverses of a Cayley map is the involution indicating the position of mutually inverse generators in the cyclic order at a vertex. In a regular Cayley map, the orientation-preserving map automorphism group acts regularly on darts. An exponent of a regular Cayley map is a number e with the property that (roughly speaking) the Cayley map is isomorphic to its 'e-fold rotational image'.

In this paper we prove that there exist regular Cayley maps of a given valence with any given exponents and any given distribution of inverses.

1 Introduction

Maps with a large number of symmetries have been one of the central topics of investigation in algebraic and topological graph theory. The most symmetrical maps are regular maps. The question of when a Cayley map is regular was studied in [2], [13] and [12] for balanced and antibalanced maps and in [6] and [11] for arbitrary Cayley maps.

In [9] the authors introduced the concept of an exponent of a map as a tool for classification of regular maps with a given underlying graph. As a number of important regular maps turn out to be Cayley maps, it is natural to consider exponents of Cayley maps in more detail.

While it is not hard to construct regular Cayley maps of a given valence with any given exponent, or with any given distribution of inverses, it is not at all obvious if the two requirements can be combined. The aim of this contribution is to present a construction of regular Cayley maps with given exponents and with a given distribution of mutually inverse elements in the cyclic order of generators.

1.1 Cayley graphs

Graphs in this paper are finite or countably infinite and locally finite. In our graphs we allow multiple edges, loops and semiedges. An edge endowed with one of the two possible orientations is a *dart*. A semiedge admits just one orientation and gives rise to a unique dart.

Let G be a finite group with unit element 1_G and let $\Omega = x_0, x_1, \ldots, x_{n-1}$ be a finite sequence of elements of G together with an involutory permutation τ of the set $[n] = \{0, 1, \ldots, n-1\}$, such that $x_i^{-1} = x_{i\tau}$ for each $i \in [n]$; the permutation τ is called the *distribution of inverses*. Moreover, let the collection of elements of Ω generate the group G. The *Cayley graph* $C(G, \Omega, \tau)$ for G, Ω and τ is an undirected graph with vertex-set G, where for each $g \in G$ and each $i \in [n]$ there is a dart (g, i) with initial vertex g. The dart (g, i) is a semiedge if $x_i = 1_G$ and $i = i\tau$, a directed loop at g if $x_i = 1_G$ and $i \neq i\tau$, and a directed edge incident with two distinct vertices if $x_i \neq 1_G$. In the last two cases the terminal vertex of the dart (g, i) is the vertex gx_i, and the *reverse* of (g, i) the dart $(gx_i, i\tau)$. A pair of mutually reverse darts forms an undirected edge in $C(G, \Omega, \tau)$.

An *automorphism* of a Cayley graph is a permutation of its dart set which preserves the incidence between darts and vertices. Observe that for each $a \in G$ the left translation that sends a dart (g, i) onto the dart (ag, i) is an automorphism of the Cayley graph $C(G, \Omega, \tau)$. The set of all such translations forms a subgroup of the automorphism group $\mathrm{Aut}(C(G, \Omega, \tau))$; this subgroup is isomorphic to G and acts transitively on vertices. Hence every Cayley graph is vertex-transitive. Conversely, if the group $\mathrm{Aut}(K)$ of a graph K contains a subgroup that acts regularly on the vertex set of K, then the graph K is a Cayley graph [10].

1.2 Cayley maps

Let $\Omega = (x_0, \ldots, x_{n-1})$ be a cyclic sequence of generators of a group G. We will assume throughout that the set of elements appearing in Ω is a generating set for G. A *Cayley map* $CM(G, \Omega, \tau)$ is a cellular embedding of a Cayley graph $C(G, \Omega, \tau)$ on a closed oriented surface S such that for each $i \in [n]$ the dart $(g, i+1)$ immediately follows the dart (g, i) in the orientation of S; here the second coordinate is taken modulo n.

In general, there are numerous ways a Cayley graph $C(G, \Omega, \tau)$ can be embedded in an orientable surface. For example, one can take another cyclic permutation of the generating sequence. The most natural way to do this is to use a power θ^e of the mapping $\theta : i \mapsto i+1$, $i \in [n]$, such that $\gcd(e, n) = 1$. This way we obtain an embedding of $C(G, \Omega, \tau)$ on some orientable surface in which the dart $(g, i+e)$ immediately follows the dart (g, i) in the orientation of the surface. We may now rearrange the sequence Ω in the form $\Omega^e = (y_0, y_1, \ldots, y_{n-1})$ where $y_i = x_{ei}$. This gives a new distribution of inverses τ_e associated with Ω^e; the new and old distributions are related, for each $i \in [n]$, by

$$e(i\tau_e) = (ei)\tau. \tag{1}$$

In order to identify face boundary walks in a Cayley map $CM(G,\Omega,\tau)$ we may proceed as follows. For auxiliary reasons we will assume that all faces carry orientation opposite to the orientation of S. Define a permutation α on $[n]$ by $i\alpha = i\tau+1$. Then, the dart $(gx_i, i\alpha)$ immediately follows the dart (g,i) in the boundary walk of the face incident with (g,i) such that the orientation of the face agrees with the dart (g,i). It follows that the entire boundary walk of the face has the form (g,i), $(gx_i, i\alpha)$, $(gx_i x_{i\alpha}, i\alpha^2), \ldots,$ $(gx_i x_{i\alpha} \ldots x_{i\alpha^{j-1}}, i\alpha^j), \ldots$ The length of the boundary walk is the smallest positive j such that $i\alpha^j = i$ and $x_i x_{i\alpha} \ldots x_{i\alpha^{j-1}} = 1_G$; in particular, the length is a multiple of the size of the orbit of α containing i.

A map isomorphism $f : M_1 \to M_2$ is any bijection from the dart set of M_1 onto the dart set of M_2 which preserves the cell structure of the maps and induces an orientation preserving homeomorphism between the supporting surfaces of the two maps. If $M_1 = M_2 = M$, then f is a map automorphism of M. Clearly, each map automorphism is also an automorphism of the underlying graph. It can be shown that for any pair of darts of M there exists at most one map automorphism taking one dart onto the other [7]. Thus the order of $\mathrm{Aut}(M)$, the automorphism group of M, is bounded above by the number of darts. If $|\mathrm{Aut}(M)|$ is equal to the number of darts of M, the map M is called *regular*. Similarly, if $\mathrm{Aut}(M)$ acts transitively on vertices of M, the map is called vertex-transitive.

In general, a Cayley map $CM(G,\Omega,\tau)$ need not be regular. However, since the translation automorphisms of the underlying Cayley graph are, in fact, map automorphisms of $CM(G,\Omega,\tau)$, every Cayley map is vertex-transitive.

1.3 Exponents

Let $M = CM(G,\Omega,\tau)$ be a Cayley map of valence $|\Omega| = n$ and let e be an integer such that $\gcd(e,n) = 1$. Let Ω^e be the e-th power of the cyclic sequence Ω as introduced in subsection 1.2 and let τ_e be as in (1). We say that e is an *exponent* of M if the Cayley maps M and $M^e = CM(G,\Omega^e,\tau_e)$ are isomorphic. Note that having exponent -1 means that M is isomorphic to its 'mirror image' M^{-1}.

If an integer e is an exponent of a map M with valence n and $f \equiv e \pmod n$, then the maps M^e and M^f are identical, and hence f is also an exponent of M. Therefore we will make no distinction in notation between an exponent of M and its residue class $(\mathrm{mod}\ n)$. Further, let ψ: $M \to M^e$ and μ: $M \to M^f$ be isomorphisms corresponding to exponents e and f, respectively. Then $\mu\psi$ is an isomorphism associated with ef. Thus ef is an exponent of M. It follows that the residue classes (modulo the valence of M) of exponents of the map M form a multiplicative group $\mathrm{Ex}(M)$, the exponent group of M. Clearly, $\mathrm{Ex}(M)$ is a subgroup of $\mathbb{Z}_n^*$, the multiplicative group of invertible elements of the ring $\mathbb{Z}_n$.

2 Exponents and distributions of inverses

We indicated in the Introduction that regular Cayley maps with a given distribution of inverses, or with a given exponent, may be constructed with no difficulty. However, simultaneous requirement of the two instances leads to a much harder problem. In what follows we will discuss this in detail.

First, it is easy to construct regular Cayley maps with a given distribution of inverses. We begin with one-vertex maps, that is, Cayley maps for the trivial group temporarily abandoning the regularity requirement. Let τ be an involution on $[n]$, let $s = |\{i = i\tau, i \in [n]\}|$, and let $\langle 1_G \rangle$ be the trivial group presented in the form $\langle 1_G \rangle = \langle x_0, \ldots, x_{n-1} | x_0 = x_1 = \cdots = x_{n-1} = 1_G \rangle$; note that we trivially have $x_i x_{i\tau} = 1_G$. The Cayley map $\mathcal{M} = CM(\langle 1_G \rangle, (x_0, \ldots, x_{n-1}), \tau)$ has one vertex, namely 1_G, s semiedges and $(n-s)/2$ loops. For any i such that $i \neq i\tau$, the pair of mutually reverse darts $(1_G, x_i)$ and $(1_G, x_{i\tau})$ form one loop. Clearly, the distribution of inverses of $\mathcal{M}$ is τ.

In order to construct less trivial examples we just invoke Theorem 7.3 of [11] which implies that if a map M' regularly covers a one-vertex Cayley map $CM(\langle 1_G \rangle, \Omega, \tau)$ with no branch point at the single vertex, then M' is a Cayley map with the same distribution of inverses τ. Any number of such maps can be obtained from one-vertex maps by voltage assignments, cf. [4] and [11]. The existence of infinitely many finite regular Cayley maps with a given distribution of inverses then follows from Theorem 7.3 of [11].

In the case of Cayley maps of valence n with a given exponent e such that $\gcd(e, n) = 1$, one-vertex maps help again. Namely, the one-vertex Cayley map $\mathcal{M}$ with $\tau = id$, that is, $x_i^2 = 1_G$ for all $i \in [n]$, has the exponent group $\mathrm{Ex}(\mathcal{M}) = \mathbb{Z}_n^*$. This is a regular Cayley map formed by an n-semistar embedded in a sphere. If each of the semiedges is given a voltage in the group $(\mathbb{Z}_2)^n$ in any $1-1$ fashion, the lift will be a regular Cayley map for the group $(\mathbb{Z}_2)^n$ whose exponent group will remain $\mathbb{Z}_n^*$. In general, however, it is not true that exponent groups lift onto covering spaces. For example, the classical regular embedding of K_7 in a torus does not have exponent -1 while it can be obtained as a lift of a one-vertex, three-loop regular toroidal map which admits -1 as an exponent.

It is not true that every one-vertex Cayley map has the full exponent group. The following result from [8] gives an answer to the question when an integer e is an exponent of $\mathcal{M}$.

Proposition 2.1. *A one-vertex Cayley map $\mathcal{M} = CM(G, \Omega, \tau)$ of valence n has an exponent e if and only if there exists $z \in \mathbb{Z}_n$ such that $(z + ei)\tau = z + (i\tau)e \pmod{n}$.*

What happens if one wants to construct a regular Cayley map in which both a distribution of inverses τ and an exponent e are prescribed in advance? Observe that for some pairs of τ, e it is possible to begin with one-vertex map $\mathcal{M}$ whose existence follows from Proposition 2.1 and then try to construct voltage assignments on the underlying graph of $\mathcal{M}$ such that the isomorphism $\mathcal{M} \to \mathcal{M}^e$ lifts onto the corresponding covering space [1]. We will not pursue this direction here because of its limited applicability. Instead, we will base our approach on the following result of [8] which is a special case of a general Cayley map isomorphism result of [11].

Theorem 2.2. *Let $M = CM(G, \Omega, \tau)$ be a Cayley map. Then an integer e such that* $\gcd(e, n) = 1$ *is an exponent of M if and only if there exist two mappings $\eta : G \to \mathbb{Z}_n$, $\omega : G \to G$ and an integer k such that, for each $a \in G$ and $x_i \in \Omega$,*

(*i*) $\omega(1_G) = 1_G$ *and* $\omega(ax_i) = \omega(a)x_{\eta(a)+ei}$
(*ii*) $\eta(1_G) = ek$ *and* $\eta(ax_i) = (\eta(a) + ei)\tau - e(i\tau)$.

An isomorphism ψ from M onto M^e can then be defined by $\psi(a, t) = (\omega(a), \eta(a) + et)$ for an arbitrary dart of M. It may be useful to observe that ω maps vertices to vertices and η determines the images of neighbours of a vertex. Accordingly, we will refer to ω and η as to the *global* and *local* part of the isomorphism ψ, respectively.

To be able to state our main result we need to introduce appropriate notation. Let τ be an involution on $[n]$ and let $p, q \in \mathcal{E}$ where $\mathcal{E}$ is any given subgroup of $\mathbb{Z}_n^*$. Let τ_p be the involution given by (1). Then, $p(qi)\tau_p = (pqi)\tau = pq(i\tau_{pq})$ for $i \in [n] = \mathbb{Z}_n$ and we have

$$q(i\tau_{pq}) = (qi)\tau_p. \tag{2}$$

For each $p \in \mathcal{E}$ we now define a one-vertex Cayley map

$$\mathcal{M}^p = CM(\langle 1_G \rangle, (x_0, \ldots, x_{n-1}), \tau_p).$$

Also, let $\alpha_p : \mathbb{Z}_n \to \mathbb{Z}_n$ be a mapping such that $i\alpha_p = i\tau_p + 1$. Consider an orbit $(i, i\alpha_p, i\alpha_p^2, \ldots,$
$i\alpha_p^v = i)$ of the element i under α_p. Let l be the least common multiple of all orbit lengths of α_p for every $p \in \mathcal{E}$. Further, for each $i \in [n]$ and $p \in \mathcal{E}$ let

$$r_{i,p} = x_{pi} x_{p(i\alpha_p)} \ldots x_{p(i\alpha_p^{(l-1)})}. \tag{3}$$

Finally, for any $p \in \mathcal{E}$, $f \in \mathbb{Z}_n^*$ and $i \in [n]$ we set

$$i\alpha_{p,f} = i\tau_p + f, \tag{4}$$

with the identification $\alpha_{p,1} \equiv \alpha_p$.

The main result of this paper is:

Theorem 2.3. *Let τ be an involution on $[n]$ and let $\mathcal{E}$ be a subgroup of $\mathbb{Z}_n^*$. Let $r_{i,p}$ be given by (3) and G be the group given by $G = \langle x_0, x_1, \ldots, x_{n-1} | x_i x_{i\tau} = 1_G, r_{i,p}^d = 1_G \rangle$ where d is a fixed positive integer, and let $\Omega = (x_0, x_1, \ldots, x_{n-1})$. Then, the map $M = CM(G, \Omega, \tau)$ is a regular Cayley map with exponent group $Ex(M) \geq \mathcal{E}$.*

The proof will be based on establishing an isomorphism ψ from $M = CM(G, \Omega, \tau)$ onto M^e as in Theorem 2.2. The local part η and the global part ω of the isomorphism are constructed in the next subsection.

2.1 The local and global part of the isomorphism

Let $F = \langle x_i, i \in [n] | \varnothing \rangle$ be the free group of rank n and let $\eta : F \to [n]$ be the mapping defined recursively by $\eta(1_G) = 1$ and by

$$\eta(ax_i) = [\eta(a) + hi]\tau - h(i\tau),$$

$$\eta(ax_i^{-1}) = [\eta(a) + h(i\tau)]\tau - hi$$

where $h \in \mathbb{Z}_n^*$ and $a \in F$. To show that the mapping $\eta : F \to [n]$ is well defined it is sufficient to prove that the above recursions imply $\eta(ax_ix_i^{-1}b) = \eta(ax_i^{-1}x_ib) = \eta(ab)$. This follows immediately from our next lemma.

Lemma 2.4. *Let $a, b, x_i \in F$. Then*

(i) $\eta(a) = \eta(b)$ *implies* $\eta(ax_i) = \eta(bx_i)$ *and* $\eta(ax_i^{-1}) = \eta(bx_i^{-1})$
(ii) $\eta(ax_ix_i^{-1}) = \eta(ax_i^{-1}x_i) = \eta(a)$
(iii) $\eta(a) = \eta(b)$ *implies* $\eta(ac) = \eta(bc)$ *for any* $c \in F$.

Proof. (i) Assume first that $\eta(a) = \eta(b)$ for some $a, b \in F$. Using the definition of η only, for each $x_i \in F$, we have:

$$\eta(ax_i) = (\eta(a) + hi)\tau - h(i\tau) = (\eta(b) + hi)\tau - h(i\tau) = \eta(bx_i),$$

which gives the first part of (i). For $\eta(ax_i^{-1})$ the argument is similar.
(ii) As in the previous part we just prove that $\eta(ax_ix_i^{-1}) = \eta(a)$, which is a consequence of the computation below:

$$\begin{aligned}\eta(ax_ix_i^{-1}) &= (\eta(ax_i) + h(i\tau))\tau - h(i\tau)\tau = ((\eta(a) + hi)\tau - h(i\tau) + h(i\tau))\tau - hi \\ &= ((\eta(a) + hi)\tau)\tau - hi = \eta(a) + hi - hi = \eta(a).\end{aligned}$$

The part (iii) is obtained by induction on the length of the word c from (i). □

Corollary 2.5. *For any $w_1, w_2 \in F$, if $\eta(w_1) = \eta(1_G)$, then $\eta(w_1w_2) = \eta(w_2)$.*

Let η be the well defined mapping from the beginning of the subsection. Let ω be recursively defined on F by $\omega(1_G) = 1_G$ and

$$\omega(ax_i) = \omega(a)x_{\eta(a)+hi};$$

$$\omega(ax_i^{-1}) = \omega(a)x_{\eta(a)+h(i\tau)}.$$

We shall again prove that $\omega : F \to F$ is a well defined mapping.

Lemma 2.6. *Let $a, b, x_i, x_{i\tau} \in F$. Then:*

(i) $\omega(a) = \omega(b)$ *and* $\eta(a) = \eta(b)$ *imply* $\omega(ax_i) = \omega(bx_i)$ *and* $\omega(ax_i^{-1}) = \omega(bx_i^{-1})$
(ii) $\omega(ax_ix_i^{-1}) = \omega(a) = \omega(ax_i^{-1}x_i)$

(iii) $\omega(a) = \omega(b)$ *and* $\eta(a) = \eta(b)$*, then* $\omega(ac) = \omega(bc)$*.*

Proof. The proof is similar to the proof of Lemma 2.4. For illustration we only show that $\omega(ax_i x_i^{-1}) = \omega(a)$. First we use twice the definition of ω, then the definition of η and finally the relation $x_i x_{i\tau} = 1_G$:

$$\begin{aligned}\omega(ax_i x_{i\tau}) &= \omega(ax_i)x_{\eta(ax_i)+h(i\tau)} = \omega(a)x_{\eta(a)+hi}x_{\eta(ax_i)+h(i\tau)}\\ &= \omega(a)x_{\eta(a)+hi}x_{(\eta(a)+hi)\tau} = \omega(a).\end{aligned}$$

□

Lemma 2.6 implies that $\omega(ax_i x_i^{-1}b) = \omega(ab) = \omega(ax_i^{-1}x_i b)$, and hence the mapping $\omega : F \to F$ is well defined.

Corollary 2.7. *If* $\omega(w_1) = \omega(1_G)$ *and* $\eta(w_1) = \eta(1_G)$*, then* $\omega(w_1 w_2) = \omega(w_2)$ *for* $w_1, w_2 \in F$*.*

Our aim is to show that the mappings $\eta : F \to [n]$ and $\omega : F \to F$ project down onto the quotient group $G = F/N$ where N is the normal subgroup of F generated by the elements $x_i x_{i\tau}$ and $r_{i,p}$ where $i \in [n]$ and $p \in \mathcal{E}$. This will be achieved if we prove that $\eta(a) = 1$ and $\omega(a) = 1_G$ for any $a \in N$. Indeed, if this is satisfied, we may define $\eta(Nb) = \eta(b)$ and $\omega(Nb) = \omega(b)$; the correctness of such a definition follows from Corollary 2.5 and Corollary 2.7. To this end we prove a series of auxiliary results. In order not to be repetitious we will be using throughout the notation introduced before the formulation of Theorem 2.3.

Lemma 2.8. *Let* $p \in \mathcal{E}$*,* $f \in \mathbb{Z}_n^*$ *and* $k_p = (fp)^{-1}\eta(g)$*. Then, for each* $z \geq 0$ *we have*

(i) $\eta(gx_{pi}x_{p(i\alpha_p)} \dots x_{p(i\alpha_p^z)}) = p[((fk_p + fi)\alpha_{p,f}^z)\tau_p - f((i\alpha_p^z)\tau_p)]$

(ii) $\omega(gx_{pi}x_{p(i\alpha_p)} \dots x_{p(i\alpha_p^z)}) = \omega(g)x_{p(fk_p+fi)}x_{p(fk_p+fi)\alpha_{p,f}} \dots x_{p(fk_p+fi)\alpha_{p,f}^z}$*.*

Proof. (i) We use induction on z. Since $\gcd(p, n) = 1$ and $\gcd(f, n) = 1$, we may assume that

$$\eta(g) = fpk_p \tag{5}$$

where $k_p = (fp)^{-1}\eta(g)$. In the first step we use just the definition of η for an exponent f, in combination with (5) and (2).

$$\eta(gx_{pi}) = (\eta(g) + fpi)\tau - f((pi)\tau) = p(fk_p + fi)\tau_p - fp(i\tau_p).$$

Now, let $\eta(gx_{pi}x_{p(i\alpha_p)} \dots x_{p(i\alpha_p^z)}) = p[((fk_p + fi)\alpha_{p,f}^z)\tau_p - f(i\alpha_p^z)\tau_p]$. With the help of the definition of η, (2) and the induction hypothesis we successively obtain:

$$\begin{aligned}
&\eta(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^{z+1})})\\
&\quad = [\eta(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^{z})}) + fp(i\alpha_p^{z+1})]\tau - fp(i\alpha_p^{z+1})\tau_p\\
&\quad = [p[((fk_p + fi)\alpha_{p,f}^z)\tau_p - f(i\alpha_p^z)\tau_p] + fp(i\alpha_p^{z+1})]\tau - fp(i\alpha_p^{z+1})\tau_p\\
&\qquad\qquad \text{using (2)}\\
&\quad = p[((fk_p + fi)\alpha_{p,f}^z)\tau_p - f(i\alpha_p^z)\tau_p + f(i\alpha_p^{z+1})]\tau_p - fp(i\alpha_p^{z+1})\tau_p\\
&\qquad\qquad \text{routine computation and (4)}\\
&\quad = p[((fk_p + fi)\alpha_{p,f}^z)\tau_p - f(i\alpha_p^z)\tau_p + f((i\alpha_p^z)\tau_p + 1)]\tau_p - fp(i\alpha_p^{z+1})\tau_p\\
&\quad = p[((fk_p + fi)\alpha_{p,f}^z)\tau_p + f]\tau_p - fp(i\alpha_p^{z+1})\tau_p\\
&\quad = p[((fk_p + fi)\alpha_{p,f}^{z+1})\tau_p - f(i\alpha_p^{z+1})\tau_p].
\end{aligned}$$

(ii) The proof is similar to (i). □

Lemma 2.9. *Let $p \in \mathcal{E}$, $f \in \mathbb{Z}_n^*$ and $k_p = (fp)^{-1}\eta(g)$. Then, $(fi)\alpha_{p,f}^z = f(i\alpha_{pf}^z)$ for each $z \geq 0$.*

Proof. By an alternate use of (4) and (2) we obtain:

$$(fi)\alpha_{p,f} = (fi)\tau_p + f = f[i\tau_{pf} + 1] = f(i\alpha_{pf}).$$

Let $(fi)\alpha_{p,f}^z = f(i\alpha_{pf}^z)$. Using (4), the induction hypothesis and (2) we obtain:

$$(fi)\alpha_{p,f}^{z+1} = ((fi)\alpha_{p,f}^z)\tau_p + f = (f(i\alpha_{pf}^z))\tau_p + f = f(i\alpha_{pf}^z)\tau_{pf} + f = f(i\alpha_{pf}^{z+1}).$$

□

Proposition 2.10. *Let $r_{i,p}$ be a relator. Then, for each $g \in F$,*

(i) $\eta(gr_{i,p}) = \eta(g)$
(ii) $\omega(gr_{i,p}) = \omega(g)$.

Proof. (i) Using Lemma 2.8, Lemma 2.9 and (2) we have:

$$\begin{aligned}
\eta(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^z)}) &= p[((fk_p + fi)\alpha_{p,f}^z)\tau_p - f(i\alpha_p^z)\tau_p]\\
&= p[(f(k_p + i)\alpha_{pf}^z)\tau_p - f(i\alpha_p^z)\tau_p]\\
&= p[f((k_p + i)\alpha_{pf}^z)\tau_{pf} - f(i\alpha_p^z)\tau_p]\\
&= fp[((k_p + i)\alpha_{pf}^z)\tau_{pf} - (i\alpha_p^z)\tau_p].
\end{aligned}$$

Moreover if $z = l - 1$ and $f \in \mathcal{E}$, from $i\tau_p = i\alpha_p - 1$ and $i\alpha_p^l = i$ (if $p, f \in \mathcal{E}$, then $i\alpha_{pf}^l = i$) we have:

$$\begin{aligned}
\eta(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^{l-1})}) &= fp[((k_p + i)\alpha_{pf}^{l-1})\tau_{pf} - ((i\alpha_p^{l-1})\tau_p)]\\
&= fp[k_p + i - 1 - (i - 1)] = \eta(g).
\end{aligned}$$

Similarly, Lemma 2.8 for $f = 1$ and $z = l-1$ gives:

$$\begin{aligned}\eta(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^{l-1})}) &= p[((k_p+i)\alpha_{p,1}^{l-1})\tau_p - (i\alpha_p^{l-1})\tau_p]\\ &= p[((k_p+i)\alpha_p^{l-1})\tau_p - (i\alpha_p^{l-1})\tau_p]\\ &= p[k_p+i-1-(i-1)] = \eta(g).\end{aligned}$$

(ii) Setting $z = l-1$ in the part (ii) of Lemma 2.8 and applying Lemma 2.9 for $f \in \mathcal{E}$ we obtain:

$$\begin{aligned}\omega(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^{l-1})}) &= \omega(g)x_{p(fk_p+fi)}x_{p(fk_p+fi)\alpha_{p,f}}\dots x_{p(fk_p+fi)\alpha_{p,f}^{(l-1)}}\\ &= \omega(g)x_{fp(k_p+i)}x_{fp(k_p+i)\alpha_{pf}}\dots x_{fp(k_p+i)\alpha_{pf}^{(l-1)}}\\ &= \omega(g)r_{k_p+i,pf} = \omega(g)1_G = \omega(g).\end{aligned}$$

Similarly, for $f = 1$ and $z = l-1$ the part (ii) of Lemma 2.8 implies:

$$\begin{aligned}\omega(gx_{pi}x_{p(i\alpha_p)}\dots x_{p(i\alpha_p^{l-1})}) &= \omega(g)x_{p(k_p+i)}x_{p(k_p+i)\alpha_p}\dots x_{p(k_p+i)\alpha_p^{(l-1)}}\\ &= \omega(g)r_{k_p+i,p} = \omega(g)1_G = \omega(g).\end{aligned}$$

□

We are now ready to show that η and ω are equal to 1 on N.

Proposition 2.11. *For each $g \in N$ we have $\eta(g) = 1$ and $\omega(g) = 1_G$.*

Proof. By the computation in the proof of Lemma 2.4 we know that $\eta(gx_ix_{i\tau}) = \eta(gx_{i\tau}x_i) = \eta(g)$. Also, Proposition 2.10 says that $\eta(gr_{i,p}) = \eta(g)$ for each relator $r_{i,p}$.

Next we prove that $\eta(gw^{-1}rw) = \eta(g)$ where $g \in N$, w is an arbitrary word over F and r is any relator of the form $r_{i,p}$ or $x_ix_{i\tau}$. The facts mentioned in the above paragraph imply that

$$\eta(gw^{-1}r) = \eta(gw^{-1})$$

for each relator r.

The third and second part of Lemma 2.4 imply that

$$\eta(gw^{-1}rw) = \eta(gw^{-1}w) = \eta(g).$$

We now complete the proof by induction on the length of the word $g \in F$. If $g = 1_G$ then clearly $\eta(g) = 1$. Assume that $g' = gw^{-1}rw$ where $g \in N$, r is a relator, and $w \in F$. By the induction hypothesis we have $\eta(g) = 1$, and by the above computation, $\eta(g') = \eta(gw^{-1}rw) = \eta(g) = 1$. The proof for ω is almost identical — it suffices to replace η by ω. □

This allows us to project our mappings $\eta : F \to [n]$ and $\omega : F \to F$ onto the quotient group $G = F/N$ by letting $\eta(Ng) = \eta(g)$ and $\omega(Ng) = \omega(g)$, respectively. We have thus accomplished the first step of our plan, that is, to establish the correctness of the definition of the local and global part of the isomorphism $\psi : M \to M^e$ to be constructed.

2.2 Conclusion of the proof and examples

At this point we have just proved that the Cayley maps from Theorem 2.3 have exponents from $\mathcal{E}$. In order to prove their regularity we use the following approach. It is obvious that a Cayley map $M = CM(G, \Omega, \tau)$ is regular if and only if there is an automorphism ψ of M such that $\psi(1_G, 0) = (1_G, 1)$. This requirement, however, exactly corresponds to the conditions in Theorem 2.2 when the map has exponent 1 (which is always the case) and when $\eta(1_G) = 1$. We therefore have:

Theorem 2.12. *A Cayley map $CM(G, \Omega, \tau)$ is regular if and only if there exist two mappings $\eta_r : G \to \mathbb{Z}_n$ and $\omega_r : G \to G$ such that:*

(i) $\omega_r(1_G) = 1_G$ *and* $\omega_r(ax_i) = \omega_r(a)x_{\eta_r(a)+i}$
(ii) $\eta_r(1_G) = 1$ *and* $\eta_r(ax_i) = (\eta_r(a) + i)\tau - (i\tau)$

for each $a \in G$ and $x_i \in \Omega$.

The arguments in subsection 2.1 actually show that a pair of functions η_r and ω_r as in Theorem 2.12 exist. Indeed, it suffices to prove that the mappings ω_r and η_r from Theorem 2.12 are well defined. Lemma 2.4 clearly holds for $e = 1$, and hence $\eta_r(ax_ix_{i\tau}b) = \eta_r(ab)$. Proposition 2.10 for $f = 1$ implies that $\eta_r(gr_{i,p}) = \eta_r(g)$ for all $g \in F$. As in the previous subsection one can prove that η_r is well defined, and the same is valid for ω_r. Therefore the Cayley maps constructed in Theorem 2.3 are regular. This completes the proof of Theorem 2.3.

Example 2.1. Let us illustrate the above approach by constructing a Cayley map with the distribution of inverses $\tau = (0)(12)(34)$ and with the exponent $e = 2$ (or equivalently with $\mathcal{E} = \mathbb{Z}_5^*$). This is the smallest non-trivial example, i.e. $e \neq \pm 1$ and the corresponding one-vertex map has not e as its exponent. The generating set is $\Omega = (x_0, \ldots, x_{n-1})$. Trivially, we have the equations $x_0^2 = x_1x_2 = x_3x_4 = 1_G$. Now we have to construct the relators $r_{i,p}$ for $0 \le i \le 4$ and $1 \le j \le 4$. By (4) or from tracing the faces of the corresponding one-vertex maps (see Figure 1) we obtain:

$$\begin{array}{llll}
r_{0,1} = (x_0x_1x_3)^5 & r_{0,2} = (x_0x_2x_3x_1x_4)^3 & r_{0,4} = (x_0x_4x_2)^5 & r_{0,3} = (x_0x_3x_2x_4x_1)^3 \\
r_{1,1} = (x_1x_3x_0)^5 & r_{1,2} = (x_2x_3x_1x_4x_0)^3 & r_{1,4} = (x_4x_2x_0)^5 & r_{1,3} = (x_3x_2x_4x_1x_0)^3 \\
r_{2,1} = x_2^{15} & r_{2,2} = (x_4x_0x_2x_3x_1)^3 & r_{2,4} = x_3^{15} & r_{2,3} = (x_1x_0x_3x_2x_4)^3 \\
r_{3,1} = (x_3x_0x_1)^5 & r_{3,2} = (x_1x_4x_0x_2x_3)^3 & r_{3,4} = (x_2x_0x_4)^3 & r_{3,3} = (x_4x_1x_0x_3x_2)^3 \\
r_{4,1} = x_4^{15} & r_{4,2} = (x_3x_1x_4x_0x_2)^3 & r_{4,4} = x_1^{15} & r_{4,3} = (x_2x_4x_1x_0x_3)^3
\end{array}$$

It follows that $l = 15$ and the corresponding Cayley group has a presentation of the form $G = \langle x_0, \ldots, x_4 | x_0^2 = x_1x_2 = x_3x_4 = x_1^{15d} = x_3^{15d} = (x_0x_1x_3)^{5d} = (x_0x_2x_3x_1x_4)^{3d} = 1_G \rangle$, where d is any fixed positive integer.

Example 2.2. For the distribution of inverses $\tau = (0)(14)(23)$ and the exponent $e = -1$, i.e. $\mathcal{E} = \{1, -1\}$, we obtain the group $G = \langle x_0, x_1, \ldots, x_4 | x_0^2 = 1_G, x_0 = x_1 = x_2 = x_3 = x_4 \rangle$ and the Cayley map M is in Figure 2. Observe that $\mathrm{Ex}(M) = \mathbb{Z}_5^* \neq \mathcal{E}$, hence we cannot claim that $\mathrm{Ex}(M) = \mathcal{E}$ in Theorem 2.3.

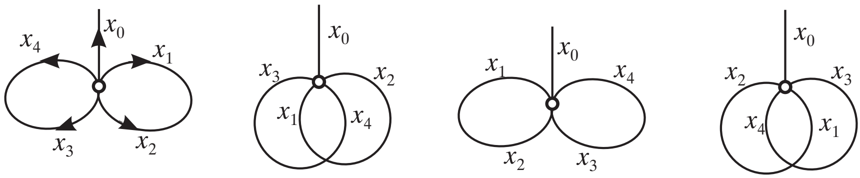

Figure 1: Cayley maps $\mathcal{M}(5,(0)(12)(34))$, $\mathcal{M}^2$, $\mathcal{M}^{-1}$ and $\mathcal{M}^3$.

Figure 2: Distribution of inverses $\tau = (0)(14)(23)$ and the corresponding map M for $d = 1$.

3 The size of the constructed Cayley maps

The maps constructed in the previous section are infinite in many cases. We will prove this by showing that the group G has often an infinite quotient group. We will assume that $n \geq 3$ and divide the analysis in three cases depending on τ.

(i) First, let $\tau = id$. Then the group from Theorem 2.3 has a presentation of the form $G = \langle x_0, \ldots, x_{n-1} | x_i^2 = (x_0 \ldots x_{n-1})^d = (x_0 x_e \ldots x_{e(n-1)})^d = (x_0 x_{e^2} \ldots x_{e^2(n-1)})^d = \cdots = 1_G \rangle$. We set $x_i = 1_G$ for $i \geq 3$. Then we have a quotient group H of G with presentation:

$$H = \langle x_0, x_1, x_2 | x_i^2 = (x_0 x_1 x_2)^d = 1_G \rangle.$$

By [3], the group H is infinite for any $d \geq 2$.

(ii) Second, assume that τ has at least one fixed point and $\tau \neq id$. Without loss of generality we can assume that $0\tau = 0$ and $1\tau = 2$. Setting $x_i = 1_G$ for $i \geq 3$ we obtain a quotient group of the form

$$H = \langle x_0, x_1, x_2 | x_0^2 = x_1 x_2 = x_1^u = (x_0 x_1)^v = (x_1 x_0 x_2)^t = 1_G \rangle.$$

If t is odd then H reduces to a cyclic group $\langle x_1 \rangle$. However, if t is even then the last relator is redundant and H is isomorphic to the triangle group $T(2, u, v)$. These groups are infinite if $1/u + 1/v \leq 1/2$ [3].

To illustrate this we revisit Example 2.1. Setting there $x_3 = x_4 = 1_G$ we obtain the quotient group

$$H = \langle x_0, x_1, x_2 | x_0^2 = x_1 x_2 = (x_0 x_1)^{5d} = x_1^{15d} = (x_1 x_0 x_2)^{3d} = 1_G \rangle.$$

If d is even then $H \cong T(2, 15d, 5d)$ which is infinite for any even d, because $1/15d + 1/5d \leq 1/2$.

(iii) Finally, let τ have no fixed point. Without loss of generality we may assume that $\tau(0) = 2$ and $\tau(1) = 3$ (the situation when, say, $\tau(0) = 1$ and $\tau(2) = 3$ is analogous). Setting $x_i = 1_G$ for $i \geq 4$ we have a quotient group the most general form of which is

$$H = \langle x_0, x_1, x_2, x_3 | x_0x_2 = x_1x_3 = x_0^u = x_1^v = (x_0x_1)^p = (x_0x_3)^s = (x_0x_1x_2x_3)^q = 1_G \rangle.$$

If there is no relation of type $(x_0x_3)^s$ we have a Coxeter group which is infinite for $u = 2$, $v = 3$, $p \geq 14$ and $q \geq 12$, see [5].

The problem of deciding (in)finiteness of the group remains open when all the relations above are present. Another open problem is to find a construction (or to prove existence) of finite maps with given exponent (group) and given distribution of inverses.

Acknowledgement

I would like to thank Jozef Širáň for many helpful comments and suggestions.

Partial support from the APVT grant No. 023302 and VEGA grant 1/9176/02 is acknowledged as well.

References

[1] D. Archdeacon, R.B. Richter, J. Širáň and M. Škoviera, *Branched coverings of maps and lifts of map homomorphisms*, Australas. J. Combin. 91 (1994) 109–121.

[2] N. Biggs and A.T. White, *Permutation Groups and Combinatorial Structures*, London Math. Soc. Lec. Notes 33 (Cambridge Univ. Press, Cambridge, 1979).

[3] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups*, Springer, Berlin, 1965.

[4] J.L. Gross and T.W. Tucker, *Topological Graph Theory*, Wiley, New York, 1987.

[5] J. Howie and R.M. Thomas, *The Groups $(2, 3, p; q)$; Asphericity and a Conjecture of Coxeter*, J. Algebra 154 (1993) 289–309.

[6] R. Jajcay and J. Širáň, *Skew-morphisms of regular Cayley maps*, Discrete Math. 244 (2002) 167–179.

[7] G.A. Jones and D. Singerman, *Theory of maps on orientable surfaces*, Proc. London Math. Soc. (3) 31 (1978), 211–256.

[8] Ľ. Lísková, *Exponents of Cayley maps*, J. Electrical Engineering, Vol. 53, No. 12/s (2002) 97–99.

[9] R. Nedela and M. Škoviera, *Exponents of Orientable Maps*, Proc. London Math. Soc. (3) 75 (1997) 1–31.

[10] G. Sabidussi, *On a class of fixed-point free graphs*, Proc. Amer. Math. Soc. 9 (1958) 800–804.

[11] R.B. Richter, J. Širáň, R. Jajcay, T.W. Tucker and M.E. Watkins, *Cayley maps*, to appear in J. Combin. Theory Ser. B.

[12] J. Širáň and M. Škoviera, *Regular maps from Cayley graphs II: Antibalanced Cayley maps*, Discrete Math. 124 (1994) 179–191.

[13] M. Škoviera and J. Širáň, *Regular maps from Cayley graphs I: Balanced Cayley maps*, Discrete Math. 109 (1992) 265–276.

(Received 1 Mar 2004; revised 23 Feb 2005)