TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 366, Number 7, July 2014, Pages 3585–3609
S 0002-9947(2014)05933-3
Article electronically published on March 3, 2014

REGULAR CAYLEY MAPS FOR CYCLIC GROUPS

MARSTON D.E. CONDER AND THOMAS W. TUCKER

ABSTRACT. An orientably-regular map M is a 2-cell embedding of a connected graph in a closed, orientable surface, with the property that the group $\mathrm{Aut}^{\mathrm{o}}M$ of all orientation-preserving automorphisms acts transitively on the arcs of M. If $\mathrm{Aut}^{\mathrm{o}}M$ contains a subgroup A that acts regularly on the vertex set, then M is called a regular Cayley map for A. In this paper, we answer a question of recent interest by providing a complete classification of the regular Cayley maps for the cyclic group C_n, for every possible order n. This is the first such classification for any infinite family of groups. The approach used is entirely algebraic and does not involve skew morphisms (but leads to a classification of all skew morphisms which have an orbit that is closed under inverses and generates the group). A key step is the use of a generalisation by Conder and Isaacs (2004) of Ito's theorem on group factorisations, to help determine the isomorphism type of $\mathrm{Aut}^{\mathrm{o}}M$. This group is shown to be a cyclic extension of a cyclic or dihedral group, dependent on n and a single parameter r, which is a unit modulo n that satisfies technical number-theoretic conditions. For each n, we enumerate all such r, and then in terms of r, we find the valence and covalence of the map, and determine whether or not the map is reflexible, and whether it has a representation as a balanced, anti-balanced or t-balanced regular Cayley map.

1. INTRODUCTION

Regular maps are generalisations of the Platonic solids (viewed as embeddings of their 1-skeletons into the sphere) to symmetrical embeddings of graphs on surfaces of arbitrary genus. Formally, a *regular map* M on an orientable surface is a 2-cell embedding of a connected graph or multigraph into that surface, such that the group $\mathrm{Aut}^{\mathrm{o}}M$ of all orientation-preserving automorphisms of the embedding has a single orbit on the set of all arcs (incident vertex-edge pairs) of M. Transitivity on the arcs ensures that every face has the same size, say t, and that every vertex has the same valency, say s. The resulting pair $\{t, s\}$ is called the *type* of M. The regular map M is called *reflexible* if there is an orientation-reversing automorphism of the embedding, and *chiral* otherwise.

The study of such maps dates back over 100 years, to observations made by Dyck, Klein and Heffter among others, and later developed by Brahana, but many questions about them have remained open until recently. The last decade has seen a burgeoning of interest in regular maps (and the related topic of dessins d'enfants), partly motivated by observations made by Grothendieck and Belyĭ about the action of the absolute Galois group on maps.

Received by the editors March 2, 2011 and, in revised form, August 9, 2012.
2010 *Mathematics Subject Classification.* Primary 05E18; Secondary 05C10, 20B25, 57M15.

Regular maps are now viewed from three main perspectives: by the genus of the carrier surface (see [3,4]), by the underlying graph of the map (see [2,15,16]) or by the automorphism group (see [9]). See also the recent survey paper [25].

A *Cayley graph* for the group A with generating set X, denoted by $C(A,X)$, is the graph with vertex set A and with edges of the form $\{a, ax\}$ for all $a \in A$ and $x \in X$. It is usually assumed that X is closed under inverses but does not contain the identity, so that $C(A,X)$ is undirected and simple — with no loops or multiple edges. Left multiplication by any element of A gives an automorphism of the Cayley graph $C(A,X)$, and the resulting action of A on $C(A,X)$ is regular on vertices — that is, transitive with trivial vertex stabilisers. Conversely, if a graph has a group A of automorphisms acting regularly on its vertices, then the graph is a Cayley graph $C(A,X)$ for some generating set X. In fact, if one specifies which vertex is labelled by the identity, then the group action by A identifies the neighbours of that vertex with the generating set X; see [11] for details.

Just as a Cayley graph can be viewed as a graph which admits a regular group action on its vertices, a *Cayley map* is a map M whose automorphism group has a subgroup acting regularly on the vertex set. In particular, the action of any such subgroup A makes the underlying graph of M a Cayley graph $C(A,X)$. A *regular Cayley map* for the group A is a regular map that is also a Cayley map for A.

In [6] the authors and Jajcay initiated a substantial investigation of regular Cayley maps for abelian groups, and this was taken further by the first author with Kwon and Širáň in [8], producing a curious theorem about the reflexibility of a regular Cayley map for a cyclic group C_n. At the time the latter theorem was written up for publication, we noted that a proof would be much easier if the generating set X could be assumed to contain an element of order n; that, however, is not obviously true, and this paper grew out of our (successful) attempt to show it is true.

In fact, we can now provide a complete classification of all regular Cayley maps for finite cyclic groups C_n. In this paper, we show there is a one-to-one correspondence between such maps and certain presentations for their automorphism groups, each of which is a cyclic extension of either C_n or the dihedral group $D_{n/2}$ (of order n). The classification splits into two classes, according to whether n is odd or even, using the 'BCD' structure of the automorphism group (as considered in [6]).

Specifically, we prove the following. For odd n, regular Cayley maps for C_n are in one-to-one correspondence with roots of -1 mod n, and for any such root r of (even) multiplicative order s, the orientation-preserving automorphism group of the map is the metacyclic group $G(n,r) = \langle\, v, y \,|\, v^n = y^s = 1,\, yvy^{-1} = v^r \,\rangle$ of order ns. On the other hand, for (even) $n = 2m$, regular Cayley maps for C_n are in one-to-one correspondence with units r mod n having the property that if b is the largest divisor of m coprime to $r-1$, then either $b = 1$, or r is a unit mod b of multiplicative order $2k$ where k is coprime to m/b. In each such case, the orientation-preserving automorphism group is a semi-direct product of D_m by C_s, with presentation $H(m,r) = \langle\, x, v, y \,|\, x^2 = v^m = y^s = 1,\, xvx = v^{-1},\, yvy^{-1} = v^r,\, yxy^{-1} = xv \,\rangle$, where s is the order of the automorphism of $\langle x, v\rangle \cong D_m$ taking x to xv and v to v^r.

In addition to this classification, we give enumeration formulae for the number of regular Cayley maps for C_n for any given n, and describe exactly which of these maps are reflexible, and determine their types. We also consider how each such map can be represented as a regular Cayley map for C_n in different ways, and determine exactly which representations are balanced, anti-balanced or t-balanced for some t (see [7]).

We believe this is the first complete classification of all regular Cayley maps for an infinite family of groups. Partial classifications have been achieved by others for various kinds of regular Cayley maps for cyclic, dicyclic, dihedral, semi-dihedral and generalised quaternion groups; see [18–21, 24, 26] for example. We also remark that the underlying graphs of regular Cayley maps for cyclic groups are arc-transitive circulants, which were classified (independently) by Kovács [17] and Li [22], but we do not need to use that classification here.

2. Preliminaries

We begin with some further background on regular maps. Details can be found in [4] or [10], for example.

Let M be a regular map on an orientable surface, with orientation-preserving automorphism group $G = \mathrm{Aut}^{\mathrm{o}}M$. Then G acts transitively on the arcs of M, and hence also transitively on the vertices, edges and faces of M. As noted earlier, this implies that every face has the same size, say t, and that every vertex has the same valency, say s, and then the pair $\{t, s\}$ is called the *type* of the regular map M.

Next, if (v, e, f) is any vertex-edge-face incident triple, then there exist automorphisms R and S in G that induce single-step rotations (of orders t and s) about the face f and vertex v respectively, such that RS is an automorphism of order 2 that acts like a half-turn around the midpoint of the edge e. By connectedness (and the fact that every automorphism is uniquely determined by its effect on any any vertex-edge-face incident triple), these two automorphisms generate the group $G = \mathrm{Aut}^{\mathrm{o}}M$. We will take the alternative generators $x = RS$ and $y = S^{-1}$, and call (x, y) a *canonical generating pair* for the map M. These two elements satisfy the relations $x^2 = y^s = (xy)^t = 1$, which are defining relations for the $(2, s, t)$ *triangle group.*

The vertices, edges and faces of M can be labelled with left cosets of the cyclic subgroups generated by y, x and xy respectively, in such a way that the group G acts by left multiplication, and incidence is given by non-empty intersection. This allows us to reconstruct a regular map from its automorphism group alone. Indeed *we can view a regular map as nothing more than a generating pair (x, y) for a finite group G, such that x is an involution.* For any two such pairs (x, y) and (x', y'), the corresponding regular maps are isomorphic if and only if there is an isomorphism from $G = \langle x, y\rangle$ to $G' = \langle x', y'\rangle$ taking x to x' and y to y'. Note that for a given group G, altering x may change the order of xy and hence the face size t, while altering y may change the orders of both y and xy and hence both the valence s and the face size t, but the number of edges (viz. $|G|/2$) remains unchanged.

[For fixed t and s, regular maps of type $\{t, s\}$ are in one-to-one correspondence with normal subgroups of finite index in the $(2, s, t)$ triangle group $\Delta = \Delta(2, s, t)$ that are torsion-free, since these are precisely the ones that contain no non-trivial powers of the canonical generators of orders 2, s and t, and in each case the factor group Δ/N is the orientation-preserving automorphism group of the map.]

The oppositely oriented regular map for M (or 'mirror image' of M) has the same type as M, and the same orientation-preserving automorphism group G, but with generating pair (x^{-1}, y^{-1}). It follows that *the regular map M is reflexible if and only if there is an automorphism of the group G taking x to x $(= x^{-1})$ and y to y^{-1}.*

In this paper, because we are dealing with Cayley graphs, we assume there are no multiple edges. The relationship of this assumption to the group structure of $G = \langle x, y\rangle$ is easily explained. The edges incident to the vertex $\langle y\rangle$ are those labelled with cosets $y^i\langle x\rangle$, while the vertices adjacent to $\langle y\rangle$ are those labelled with cosets $y^i x\langle y\rangle$. If there are multiple edges, then by arc-transitivity there must be at least two edges between the vertices labelled $\langle y\rangle$ and $x\langle y\rangle$, in which case some edge coset $y^i\langle x\rangle$ with $0 < i < s$ has non-empty intersection with $x\langle y\rangle$, or equivalently, $y^i x = xy^j$ for some j. In that case $x^{-1}y^i x = y^j$, which happens if and only if some non-trivial subgroup of $\langle y\rangle$ is normalised by x and is therefore normal in $\langle x, y\rangle = G$. Thus *to have a simple underlying graph, we require that $\langle y\rangle$ contains no non-trivial normal subgroup*; that is, the vertex-stabiliser $Y = \langle y\rangle$ must be *core-free* in G.

The Euler characteristic χ and the genus g of the carrier surface (and hence of the map M) are then given by the Euler-Poincaré formula

$$2 - 2g = \chi = V - E + F = |G|/s - |G|/2 + |G|/t = |G|(2t - ts + 2s)/2ts.$$

The (geometric) *dual* of the regular map M is also regular, with type $\{s, t\}$, and has the same genus and characteristic as M. For this reason, the face-size of M is often called the *co-valence* of M. On the other hand, if M is a regular Cayley map for the group A, then the dual of M might not be a regular Cayley map for A, since the action of A could have non-trivial face stabilisers.

Next, we give some more background on regular Cayley maps.

Suppose M is a regular Cayley map for the group A. Let $G = \mathrm{Aut}^{\mathrm{o}}M$, and let (x, y) be a canonical generating pair, with y stabilising a vertex v, and x stabilising an incident edge e. Since A acts regularly on the vertices of M, we know that $G = AY$ with $A \cap Y = \{1\}$; that is, A is *complementary* to Y in G. Conversely, if $G = \langle x, y\rangle$, where x is an involution and G has a subgroup A complementary to $Y = \langle y\rangle$, then G is the orientation-preserving automorphism group of a regular Cayley map for A with canonical generating pair (x, y).

The underlying graph of M is a Cayley graph $C(A, X)$ for some generating set X for A. By vertex-transitivity, we may label the vertex v with the identity element of A, and then the neighbours of v are the vertices labelled with the elements of X, say $x_1, x_2, \ldots, x_s$ in anti-clockwise order. The embedding of $C(A, X)$ in the surface defines a cyclic rotation on those neighbours, so that $yx_i \in x_{i+1}Y$ for all i (mod s). This extends to a mapping $\varphi\colon A \to A$ with the property that for each $a \in A$,

$$ya = \varphi(a)y^{\pi(a)} \quad \text{for some } \pi(a) \in \mathbb{Z}_s.$$

The function $\varphi : A \to A$ is called a *skew morphism* of A, with associated *power function* $\pi : A \to \mathbb{Z}_s$ (see [14]). This skew morphism has the special property that one of its orbits, namely $X = \{x_1, x_2, \ldots, x_s\}$, is closed under inverses and generates A. We call any such orbit a *good* orbit of φ. Also with X and φ so defined, we may denote the labelled regular Cayley map M by $\mathrm{Cay}(A, X, \varphi)$.

Note that there may be other subgroups of G isomorphic to A that are complementary to Y, so *there may be many different ways to label the vertices by the elements of A to represent M as a Cayley map for A.* We will take this observation further in Section 7. Note also that there may be more than one good orbit X for the skew morphism φ, and the regular Cayley maps associated with these might or might not be isomorphic. From our algebraic viewpoint of a regular Cayley map as a generating pair (x, y) for a group G with complementary factorisation AY, the cyclically ordered generating set X that prescribes the embedding is determined by the choice of x: since the vertices are cosets of $Y = \langle y \rangle$, the ith element x_i of X is the unique element of A such that $x_i \in y^i xY$. Hence in particular, *if there is an automorphism of the group $G = AY$ taking (x, y) to (x', y), then there is an automorphism of A taking the cyclically oriented generating set X for x to the corresponding one for x'.*

The regular Cayley map $\mathrm{Cay}(A, X, \varphi)$ is *balanced* if either all elements of X are involutions, or all of them are non-involutions and the cyclic ordering of the elements of X around the identity vertex has the form $(x_1, x_2, \ldots, x_{s/2}, x_1^{-1}, x_2^{-1}, \ldots, x_{s/2}^{-1})$. Equivalently, $\mathrm{Cay}(A, X, \varphi)$ is balanced if the skew morphism φ has the property that $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in X$. In that case, the skew morphism φ is actually an automorphism of A, so A is a normal subgroup of G; see [6, Proposition 2.3]. Also in that case, $\varphi^{s/2}$ inverts every element of X, and the power function takes value $\pi(x) = 1$ at every $x \in X$. Conversely, if A is normal in G, then the φ-ordering $(x, \varphi(x), \varphi^2(x), \ldots, \varphi^{s-1}(x))$ of the elements of X gives a balanced map. Note also that *Y may have many complements in G that are isomorphic to A, and it can happen that the same regular Cayley map M is balanced for one such complement but not balanced for another.*

Similarly, if the ordering of X has the form $(x_1, x_2, \ldots, x_{s/2}, x_{s/2}^{-1}, \ldots, x_2^{-1}, x_1^{-1})$ when s is even or $(x_1, x_2, \ldots, x_{(s-1)/2}, x_{s/2}, x_{(s-1)/2}^{-1}, \ldots, x_2^{-1}, x_1^{-1})$ when s is odd, then $\mathrm{Cay}(A, X, \varphi)$ is *anti-balanced*. Equivalently, $\mathrm{Cay}(A, X, \varphi)$ is anti-balanced if φ has the property that $\varphi(x^{-1}) = (\varphi^{-1}(x))^{-1}$ for all $x \in X$. In that case, the power function takes value $\pi(x) = -1$ (in $\mathbb{Z}_s$) at every $x \in X$.

More generally, if the power function π takes constant value j on X for some $j \in \mathbb{Z}_s$, then the map M is said to be *j-balanced*. Regular j-balanced Cayley maps were investigated in detail in [7]. In this case, the skew morphism φ induces an automorphism on the subgroup $K = \{a \in A : \pi(a) = 1\}$, which is called the *kernel* of φ. The kernel K has index 1 or 2 in A, depending on whether $j = 1$ or $j \neq 1$. Hence in particular, *if $|A|$ is odd, then A has no j-balanced regular Cayley maps for* $j \neq 1$ (modulo the valence).

3. The classification of regular Cayley maps for a given cyclic group

We now give the major part of our classification of regular Cayley maps for cyclic groups. Although we make connections with the skew-morphism viewpoint, our approach is almost entirely group-theoretic, and made possible by the following corollary of a theorem of Conder and Isaacs given in [6]:

Theorem 3.1. *If $G = AY$ is the automorphism group of a regular Cayley map for the finite abelian group A, and G' is the commutator subgroup of G, then $G'/(G' \cap A)$ is cyclic and G' is isomorphic to a subgroup of A.*

This is an extension of a theorem of Ito [12], which says that the commutator subgroup of any group expressible as a product AB of two abelian subgroups is abelian. While the proof of Ito's theorem is elegant but elementary, we know of no easy proof of the above, even in the case where A and B are both cyclic, and so we refer the reader to the paper [5] by Conder and Isaacs for its proof.

In particular, when A is cyclic, it follows that G' is cyclic. All of the rest of the structure of G that we need when A is cyclic holds also when A is abelian, and was exploited at considerable length in [6]. We can summarise it as follows:

Theorem 3.2. *Let $A = C_n$ be the cyclic group of order n, and let G be the orientation-preserving automorphism group of a regular Cayley map for A with canonical generating pair (x, y). Let $Y = \langle y\rangle$ be the vertex-stabiliser, of order s and core-free in G, let $C = G'$ be the commutator subgroup of G, and let D be the normal closure of the subgroup $\langle x\rangle$ in G.*

(a) *If n is odd, then $G = CY$ with $C \cap Y = \{1\}$, and $C \cong A = C_n$. In particular, if v is a generator of C, then the group G has defining presentation*

$$G(n, r) = \langle\, v, y \mid v^n = y^s = 1,\ yvy^{-1} = v^r\,\rangle,$$

where r is a root of -1 mod n, of multiplicative order s. Moreover, there is an automorphism of G taking (x, y) to $(vy^{s/2}, y)$.

(b) *If n is even, say $n = 2m$, then $G = DY$ with $D \cap Y = \{1\}$, and D is isomorphic to the dihedral group D_m, with C as its index two cyclic subgroup. In particular, if v is a generator of C, then $D = \langle x, v\rangle$, and the group G has defining presentation*

$$H(m, r) = \langle\, x, v, y \mid v^m = x^2 = y^s = 1,\ xvx = v^{-1},\ yvy^{-1} = v^r,\ yxy^{-1} = xv\,\rangle,$$

where r is a unit mod m, and s is the order of the automorphism of $D = \langle x, v\rangle$ induced by conjugation by y.

Proof. First, note that G/D is cyclic, generated by the coset Dy, and therefore D contains the commutator subgroup C, and $G = DY$. Moreover, since G/D can be obtained from the abelianisation G/C of G by making trivial the coset containing x, we know that C has index at most 2 in D. Next, since C is cyclic (by Theorem 3.1), every subgroup of C is characteristic in C and therefore normal in G, and then since Y is core-free in G, it follows that $C \cap Y = \{1\}$.

Now suppose $G = CY$. Then $|G| = |C||Y|$ and therefore $|C| = |G|/|Y| = |A| = n$. In particular, C is isomorphic to C_n. Taking v as a generator for C gives $yvy^{-1} = v^r$ for some unit r mod n, and $G = CY = \langle v, y\rangle$. The multiplicative order of r must be s, for otherwise some non-trivial subgroup of $Y = \langle y\rangle$ centralises v and is then normal in $\langle v, y\rangle = G$, which is impossible since Y is core-free in G. Also n must be odd, for if n were even, then the unit r would have to be odd, in which case all conjugates of commutators $vy^iv^{-1}y^{-i} = v^{1-r^i}$ would lie in the proper subgroup $\langle v^2\rangle$ of C.

The involution x must be expressible in the form v^iy^j for some i, j, and then since

$$1 = x^2 = (v^iy^j)^2 = v^{i(1+r^j)}y^{2j},$$

we have $i(1 + r^j) \equiv 0 \bmod n$ and $2j \equiv 0 \bmod s$. On the other hand,

$$\langle v, y\rangle = G = \langle x, y\rangle = \langle v^iy^j, y\rangle = \langle v^i, y\rangle,$$

with $\langle v^i\rangle$ being normal in G, so i must be a unit mod n, and thus $1+r^j \equiv 0 \bmod n$. In particular, r is a root of -1 mod n, and s must be even. It follows that $j = s/2$. Finally, the relations $v^n = y^s = 1$ and $yvy^{-1} = v^r$ are preserved when v is replaced by v^i, so there exists an automorphism of G taking $x = v^iy^{s/2}$ to $vy^{s/2}$.

Next, suppose instead that $G \neq CY$. Then $C \neq D$, so C has index 2 in D. Moreover, since C is generated by the commutators xy^ixy^{-i}, each of which is inverted by conjugation by the involution x, we find that conjugation by x inverts all elements of C, and therefore D is a dihedral group, with C a cyclic subgroup of index 2. Also $|G| > |CY| = |C||Y|$ (since $C \cap Y = \{1\}$), so $|C| < |G|/|Y| = |A|$, while on the other hand, $2|C| = |D| \geq |DY|/|Y| = |G|/|Y| = |A|$, so $2|C| = |D| = |A| = n$. In particular, n is even, say $n = 2m$, and $C \cong C_m$ while $D \cong D_m$.

Taking v as a generator for C gives $yvy^{-1} = v^r$ for some unit r mod m, and $xvx^{-1} = v^{-1}$ (by the observations above about commutators). Also $xyxy^{-1} \in C$ and hence $xyxy^{-1} = v^i$ for some i, which gives $yxy^{-1} = xv^i$, and it then follows easily that all conjugates of x by powers of y lie in the subgroup generated by x and v^i. Thus $\langle x, v\rangle = D = \langle x, v^i\rangle$, and so i is a unit mod m. In particular, we can replace v by v^i if necessary, giving $yxy^{-1} = xv$ (and preserving the relations $xvx^{-1} = v^{-1}$ and $yvy^{-1} = v^r$). Hence we have the presentation in case (b). Finally, s is the order of the automorphism of D induced by conjugation by y, since Y is core-free in G. □

Corollary 3.3. *If M is a regular Cayley map for the cyclic group C_n, then M is a balanced regular Cayley map for C_n when n is odd, and a balanced regular Cayley map for $D_{n/2}$ when n is even.*

In Theorem 3.2, we began with a regular Cayley map and found information about its automorphism group G. To complete our classification, we start with the group A and then want to construct all possibilities for the map. There are two potential problems with this approach.

In the first case, where n is odd, the group presentation mentions nothing about the involution x, yet we need to be sure that there is such an involution, which together with y generates G. The condition in Theorem 3.2 that r is a root of -1 mod n does the trick: it lets us choose $x = vy^{s/2}$, because $vy^{s/2}vy^{s/2} = vv^{r^{s/2}}y^s = vv^{-1} = 1$. Moreover, once we have this x, all other choices for x define the same map, since we know there is always an automorphism of G taking (x, y) to $(vy^{s/2}, y)$. Also the map is a regular Cayley map for the subgroup generated by v, which is cyclic of order n.

In the second case, where n is even, the involution x is given as a generator in the presentation for G. Also x and y generate G since $yxy^{-1} = xv$. The problem here is that if we start with the given presentation for G, it is not easy to see a complementary factorisation $G = AY$ for G with $A \cong C_n$; in other words, we do not have an obvious element a of order n with the property that $\langle a\rangle \cap \langle y\rangle = \{1\}$, and in fact there might not be one! Once we know there is one, however, the same regular Cayley map will result, whichever elements we choose as the generators.

Definition 3.4. Call the group $G(n, r)$ *admissible* if r is a root of -1 mod n, and similarly, call the group $H(m, r)$ *admissible* if it has an element a of order $2m$ such that $\langle a\rangle \cap \langle y\rangle = \{1\}$. Then also call the pair (n, r) *admissible* if either n is odd and the group $G(n, r)$ is admissible, or $n = 2m$ and the group $H(m, r)$ is admissible.

Theorem 3.5. *Two regular Cayley maps for C_n are isomorphic if and only if their orientation-preserving automorphism groups are isomorphic. Moreover, the regular Cayley maps for C_n are in one-to-one correspondence with admissible pairs (n, r).*

Proof. Clearly if the maps are isomorphic, then so are their groups. Conversely, we observe that different values for the parameter r give different groups, since the value of r tells us how G/G' acts by conjugation on the commutator subgroup G', and this is uniquely determined by the isomorphism class of the group. The rest follows from Theorem 3.2 and the comments immediately after Corollary 3.3. □

Because of the above, it makes sense to introduce the following:

Definition 3.6. For any admissible pair (n, r), let $M(n, r)$ be the regular Cayley map given by Theorem 3.2.

Theorem 3.5 now tells us that every regular Cayley map for a cyclic group is isomorphic to one (and only one) such map $M(n, r)$. Also $\mathrm{Aut}^{\mathrm{o}}M(n, r) = G(n, r)$ when n is odd, while $\mathrm{Aut}^{\mathrm{o}}M(n, r) = H(m, r)$ when $n = 2m$.

We will develop more precise criteria for admissibility and other properties in subsequent sections. What will become clear is that Theorem 3.2 allows us to reduce many important questions about regular Cayley maps to elementary number theory. As the first instance of this, we give the following characterisation of reflexibility.

Theorem 3.7. *For odd n, the only reflexible regular Cayley map $M(n, r)$ is the equatorial map on the sphere with n vertices of valence 2. For even $n = 2m$, the regular Cayley map $M(n, r)$ is reflexible if and only if $r^2 \equiv 1$ mod m.*

Proof. Let $M = M(n, r)$, and let (x, y) be a canonical generating pair for $G = \mathrm{Aut}^{\mathrm{o}}M$. We know that M is reflexible if and only if there is an automorphism θ of G fixing x and taking y to y^{-1}.

For odd n, we have $G = G(n, r) = \langle v, y\rangle$ for some r, and the required automorphism θ would fix the involution $y^{s/2}$, and hence also fix $v = xy^{s/2}$. But then θ would have to take $v = y^{-1}v^r y$ to $yv^r y^{-1} = v^{r^2}$, in which case $r^2 \equiv 1$ mod n. This forces $s = 2$ and $r \equiv -1$ mod n, giving the valence 2 map on the sphere.

Similarly, for (even) $n = 2m$ we have $G = H(m, r) = \langle x, v, y\rangle$ for some r, and the automorphism θ must preserve the commutator subgroup $C = \langle v\rangle$, so θ takes v to v^j for some j coprime to m. In this case, applying θ to the relation $yvy^{-1} = v^r$ gives $y^{-1}v^j y = v^{jr}$ and therefore $v^j = yv^{jr}y^{-1} = v^{jr^2}$, so that $v^{j(r^2-1)} = 1$, which in turn gives $r^2 \equiv 1$ mod m. Conversely, if $r^2 \equiv 1$ mod m, then the defining relations for $H(m, r)$ are preserved by replacing (x, v, y) by (x, v^{-r}, y^{-1}), and so there exists an automorphism θ of G taking (x, y) to (x, y^{-1}). For example, the relation $yxy^{-1} = xv$ is equivalent to $y^{-1}xvy = x$ and hence is taken under this replacement to $yxv^{-r}y^{-1} = x$, which holds as a relation since $yxy^{-1} = xv$ and $yv^{-r}y^{-1} = v^{-r^2} = v^{-1}$. □

There is an interesting phenomenon when $r^2 \equiv 1$ mod m as in Theorem 3.7. In that case, let b be the largest divisor of m coprime to $r - 1$. Then since $b(m/b) = m$ divides $r^2 - 1 = (r + 1)(r - 1)$, we find that $r \equiv -1$ mod b, while $r = 1$ mod p for all primes p dividing m/b. Note that b is necessarily odd, since if m were even, then r would be odd, in which case $r - 1$ is even, but coprime to b. It could be tempting to think that also $r = 1$ mod m/b, but that does not always hold; for example, when 8 divides m, there are at least four square roots of 1 mod m, but not all are congruent to 1 mod 8, let alone congruent to 1 mod m/b. We will generalise this in the next two sections, where we derive a number-theoretic condition for the group $H(m, r)$ to be admissible, and determine the types of the regular Cayley maps $M(n, r)$.

4. Orders of elements in metacyclic groups

Before proceeding much further, we need some number theory that enables calculation of the orders of certain elements in our groups $G(n, r)$ and $H(m, r)$.

The following notation will ease the exposition considerably: for given positive integers t and k, define t_k to be the sum $1+t+t^2+\cdots+t^{k-1}$. With this notation, it is an easy algebraic exercise to see that $(t-1)t_k = t^k - 1$ for all k, and also that $t_{jk} = t_j(t^j)_k = t_k(t^k)_j$ for all j and k.

Lemma 4.1. *Let m, d and t be positive integers for which $t^d \equiv 1 \bmod m$. Then in the semi-direct product $C_m \rtimes_t C_d$, with presentation $\langle\, u, w \mid u^m = w^d = 1,\ wuw^{-1} = u^t \,\rangle$, the following hold:*

(a) $(uw)^k = u^{t_k} w^k$ *for all k.*
(b) *The order of uw is equal to d times the additive order of t_d in Z_m, that is, $dm/\gcd(t_d, m)$.*
(c) *In particular, uw has order m if and only if d divides m and the additive order of t_d in Z_m is m/d, or equivalently, if and only if $\gcd(t_d, m) = d$.*
(d) *The subgroups $\langle uw\rangle$ and $\langle w\rangle$ have trivial intersection if and only if every positive integer k for which $t_k \equiv 0 \bmod m$ is a multiple of d.*

Proof. (a) $(uw)^k = u(wuw^{-1})(w^2uw^{-2})\ldots(w^{k-1}uw^{-(k-1)})w^k = u^{1+t+t^2+\cdots+t^{k-1}}w^k = u^{t_k}w^k$.

(b) If $1 = (uw)^k = u^{t_k}w^k$, then $w^k = 1$ because $\langle u\rangle \cap \langle w\rangle = \{1\}$, and so k must be a multiple of d (the order of w). Then since $(uw)^d = u^{t_d}$, it follows that the order of uw is d times the additive order of t_d in $\mathbb{Z}_m$, viz. $m/\gcd(t_d, m)$.

(c) By (b), the order of uw is m if and only if $\gcd(t_d, m) = d$, which occurs if and only if d divides m and $m/d = m/\gcd(t_d, m)$.

(d) Let k be any integer for which $(uw)^k$ lies in the intersection $J = \langle uw\rangle \cap \langle w\rangle$. Then $u^{t_k} = (uw)^{-1}w^k$ lies in $\langle w\rangle$, so must be trivial (since $\langle u\rangle \cap \langle w\rangle = \{1\}$), and therefore $t_k \equiv 0 \bmod m$. On the other hand, if $t_k \equiv 0 \bmod m$, then $(uw)^k = u^{t_k}w^k = w^k$ and therefore w^k lies in J. The rest follows easily from this. □

The next piece of number theory helps us deal with prime-powers:

Lemma 4.2. *For any prime-power p^e, let t be a positive integer of the form $t = 1 + cp^f$, where c is coprime to p and $0 < f \le e$.*

(a) *If p is odd, then the order of t as a unit mod p^e is p^{e-f}, and moreover, if $t^d \equiv 1 \bmod p^e$, then $t_d \equiv d \bmod p^e$, and so $\gcd(t_d, p^e) = \gcd(d, p^e)$.*
(b) *If $p = 2$, and $e = 1$ or $f > 1$, then the order of t as a unit mod 2^e is 2^{e-f}; moreover, if $t^d \equiv 1 \bmod 2^e$, then $t_d \equiv d \bmod 2^e$ when $e = 1$, while $t_d \equiv d \bmod 2^{e-1}$ when $f > 1$, and in both cases, $\gcd(t_d, 2^e) = \gcd(d, 2^e)$.*
(c) *If $p = 2$, $e > 1$ and $f = 1$, then the order of t as a unit mod 2^e divides 2^{e-2} if $e > 2$, or is 2 if $e = 2$, and if $t^d \equiv 1 \bmod 2^e$, then $t_d \equiv (1+t)(d/2) \bmod 2^e$.*

In particular, in all cases the order of t as a unit mod p^e divides p^{e-1}.

Proof. First suppose p is odd. Then using the binomial theorem, it is easy to see that $t^{p^i} = 1 + c'p^{i+f}$ where $c' \equiv c \bmod p$, for all $i > 0$, and it follows that the order of t as a unit mod p^e is p^{e-f}. In particular, if $t^d \equiv 1 \bmod p^e$ then p^{e-f} divides d. Also again by the binomial theorem, we have

$$t_d = \frac{t^d - 1}{t - 1} = \frac{\sum_{k=1}^{d} \binom{d}{k} c^k p^{kf}}{cp^f} = d + \sum_{k=2}^{d} \binom{d}{k} c^{k-1} p^{(k-1)f},$$

and since d is divisible by p^{e-f}, it follows by induction on k that $\binom{d}{k}p^{(k-1)f}$ is divisible by p^e for all $k > 1$. (Note: the number of occurrences of p in the prime factorisation of the denominator $k!$ of $\binom{d}{k}$ grows more slowly than $(k-1)f$, as a function of k.) Thus $t_d \equiv d \bmod p^e$, and this proves (a).

Next, suppose $p = 2$, so $t = 1 + c2^f$. If $e = 1$, then $f = 1$ (because $0 < f \leq e$) and so $p^e = 2$ and $t = 1 + 2c \equiv 1 \bmod 2^e$, and the conclusions are trivial.

If $p = 2$ and $f > 1$, then just as in the previous case, the order of t as a unit mod 2^e is 2^{e-f}, and so d is divisible by 2^{e-f} whenever $t^d \equiv 1 \bmod 2^e$. To verify that $t_d \equiv d \bmod 2^{e-1}$, we proceed as in case (a), but we note that the term for $k = 2$ in the final sum is $\binom{d}{2}c\,2^f$, and that this term is divisible by 2^{e-1}, but not necessarily by 2^e. All of the higher terms are divisible by 2^e for the same reason as in case (a), namely that the number of occurrences of 2 in the prime factorisation of the denominator $k!$ of $\binom{d}{k}$ is no more than $(k-1)f$, when $f > 1$. In particular, since $t_d \equiv d \bmod 2^{e-1}$ with $e > 1$, we have $\gcd(t_d, 2^e) = \gcd(d, 2^e)$, proving (b).

Finally, suppose $p = 2$ and $f = 1 < e$. Then $t = 1 + 2c$ where c is odd, so $t^2 = 1 + 4c(1+c) = 1 + c'2^j$ where c' is odd and $j \geq 3$. If $e = 2$, then $t \equiv 3 \bmod 2^e$, so $t^2 \equiv 1 \bmod 2^e$ and t has order 2 as a unit mod 2^e, while if $e > 2$, then by case (b), the order of t^2 as a unit mod 2^e divides 2^{e-3}, so the order of t as a unit mod 2^e divides 2^{e-2}. In both cases, if $t^d \equiv 1 \bmod 2^e$, then d is even and $t_d \equiv t_2(t^2)_{d/2} \equiv (1+t)(t^2)_{d/2}$, and then since $t+1$ is even and $t_{d/2} \equiv d/2$ or $d/2 + 2^{e-1} \bmod 2^e$, it follows that $t_d \equiv (1+t)(d/2) \bmod 2^e$, proving (c). □

We can apply this to obtain the following:

Lemma 4.3. *Let m, d and t be positive integers for which $t^d \equiv 1$ mod m, and let u and w be generators of the semi-direct product $C_m \rtimes_t C_d$, satisfying the relations $u^m = w^d = 1$ and $wuw^{-1} = u^t$, as in Lemma 4.1.*

(a) *If b is the largest divisor of m that is coprime to $t-1$, then b is odd. Moreover, if $m \not\equiv 0$ mod 4 or $r \equiv 1$ mod 4, then $\gcd(t_d, m/b) = \gcd(d, m/b)$, so the additive order of t_d in $\mathbb{Z}_{m/b}$ is equal to $(m/b)/\gcd(d, m/b)$.*

(b) *If uw has order m, then d divides m, and $t \equiv 1$ mod m/d. Moreover, if uw has order m and every positive integer k such that $t_k \equiv 0$ mod m is a multiple of d, then $t \equiv 1$ mod p for every prime p that divides m.*

Proof. (a) If m is odd, then b is odd, while if m is even, then t is odd and so $t-1$ is even, which again implies that b is odd. Hence in particular, any power of 2 dividing m will also divide m/b. Now let p^e be any maximal prime-power divisor of m/b. Then $t \equiv 1 \bmod p$, by definition of b. If p is odd, then $\gcd(t_d, p^e) = \gcd(d, p^e)$, by case (a) of Lemma 4.2. On the other hand, if $p = 2$ and $t = 1 + c2^f$ where c is odd, then our assumption that $m \not\equiv 0 \bmod 4$ or $r \equiv 1 \bmod 4$ gives $e = 1$ or $f > 1$, and we can apply case (b) of Lemma 4.2. It follows that $\gcd(t_d, p^e) = \gcd(d, p^e)$ for all such p^e, so $\gcd(t_d, m/b) = \gcd(d, m/b)$, and the additive order of t_d in $\mathbb{Z}_{m/b}$ is $(m/b)/\gcd(d, m/b)$.

(b) Suppose uw has order m. Then by Lemma 4.1(c), d divides m and the additive order of t_d in $\mathbb{Z}_m$ is m/d. On the other hand, $(t-1)t_d \equiv t^d - 1 \equiv 0 \bmod m$, so this implies that $t-1$ is a multiple of m/d, and hence $t \equiv 1 \bmod m/d$.

Next, suppose that every positive integer k for which $t_k \equiv 0 \bmod m$ is a multiple of d. Then by Lemma 4.1(d), the subgroups $\langle uw \rangle$ and $\langle w \rangle$ have trivial intersection.

Let p be any prime divisor of m, but suppose that $t \not\equiv 1 \bmod p$. Also let k be the multiplicative order of t (as a unit) mod p. Then $k \leq p-1$, and k divides d, which divides m. Moreover, $(t-1)t_k = t^k - 1 \equiv 0 \bmod p$, but we have assumed that $t-1 \not\equiv 0 \bmod p$, and it follows that $t_k \equiv 0 \bmod p$. Thus p divides both t_k and m, and in particular, $p \leq \gcd(t_k, m)$. On the other hand, consider the subgroup $K = \langle u^{t_k}, w^k \rangle$. Since $K \cong \langle u^{t_k} \rangle \rtimes \langle w^k \rangle$, the order of K is $m/\gcd(t_k, m)$ times d/k. But also $(uw)^k = u^{t_k} w^k$, from which it follows that $K = \langle (uw)^k, w^k \rangle$, and since $\langle uw \rangle \cap \langle w \rangle = \{1\}$ this shows that the order of K is at least $(m/k)(d/k)$. Comparing these two gives $\gcd(t_k, m) \leq k$, which is impossible since $k < p \leq \gcd(t_k, m)$.

Thus $t \equiv 1 \bmod p$ for every prime p dividing m. □

5. Admissibility and type

In this section, we derive a purely number-theoretic condition for a pair $(2m, r)$ to be admissible, and find the type of the regular Cayley map $M(n, r)$ for every admissible pair (n, r). To do this, we consider two kinds of pairs (m, r), associated with the cases of Lemma 4.2. We call a pair (m, r) *nice* if either $m \not\equiv 0 \bmod 4$ or $r \equiv 1 \bmod 4$.

Theorem 5.1. *Let m be any positive integer, and let r be any unit modulo m. Define b to be the largest divisor of m that is coprime to $r-1$. Then the pair $(2m, r)$ is admissible if and only if either $b = 1$, or r is a root of -1 mod b of multiplicative order $2k$ where k is coprime to m/b. Furthermore, if this holds, then in the group $H(m, r)$, the element $a = xv^i y^j$ generates a cyclic group of order $2m$ complementary to $\langle y \rangle$ if and only if j is coprime to m/b and $r^j \equiv -1$ mod p for every prime divisor p of b (with no restriction on i).*

Proof. We first prove necessity. Suppose that $a = xv^i y^j$ generates a cyclic group of order $2m$ intersecting $Y = \langle y \rangle$ trivially. We will show that j is coprime to m/b and that $r^j \equiv -1 \bmod p$ for every prime p dividing b, and then show that either $b = 1$, or r is a root of -1 mod b of multiplicative order $2k$ where k is coprime to m/b.

Consider xv^i, which is an involution in the dihedral subgroup $\langle x, v \rangle \cong D_m$. Since $a = (xv^i)y^j$, we have $\langle xv^i, y \rangle = \langle a, y \rangle = H(m, r)$, and therefore (x', y) is a canonical generating pair for some regular Cayley map for C_{2m} with orientation-preserving automorphism group $H(m, r)$. By Theorems 3.2 and 3.5, all such pairs for $H(m, r)$ are equivalent, and hence we can assume without loss of generality that $xv^i = x$, which means we can take $i = 0$ and $a = xy^j$.

Now $a^2 = v^{r_j} y^{2j}$ lies in $\langle v, y \rangle$, which has order ms. On the other hand, $\langle a^2, y \rangle$ has order at least ms (since a has order $2m$), so $\langle v^{r_j}, y \rangle = \langle v^{r_j} y^{2j}, y \rangle = \langle a^2, y \rangle = \langle v, y \rangle$, and it follows that v^{r_j} has order m. In particular, r_j is coprime to m.

For the moment, let $r' = r^{2j}$, and let $v' = v^{r_j}$ and $y' = y^{2j}$, and choose $x' = xv^k$ (for some k) so that the elements x', v' and y' satisfy the presentation for $H(m, r')$, with s' being the order of the automorphism of $\langle x', v' \rangle \cong D_m$ that takes x' to $x'v'$ and v' to $(v')^{r'}$. Then since $v'y' = v^{r_j} y^{2j}$ $(= a^2)$ has order m, we find by Lemma 4.3(b) that $r^{2j} \equiv 1 \bmod p$ for every prime p dividing m. In particular, every such prime p divides $r^{2j} - 1 = (r^j - 1)(r^j + 1)$, and hence divides $r^j - 1$ or $r^j + 1$.

If p divides m/b, then p divides $r - 1$ and hence divides $(r-1)r_j = r^j - 1$. Also since $r \equiv 1 \bmod p$ in this case, we have $r_j \equiv 1 + 1^1 + \cdots + 1^{j-1} \equiv j \bmod p$, and therefore j is coprime to p. It follows that j is coprime to m/b.

On the other hand, if p divides b, then p is coprime to $r-1$ (by definition of b), and hence also to $(r-1)r_j = r^j - 1$, from which it follows that p divides r^j+1. Thus $r^j \equiv -1 \bmod p$, as required.

Also b is odd, by Lemma 4.3(a), and so p is odd. Hence by Lemma 4.2(a), if p^e is the largest power of p dividing b, then the order of r^{2j} as a unit mod p^e divides p^{e-1}, and therefore divides b. It follows that $r^{bj} \equiv -1 \bmod p^e$ for all such p, and therefore $r^{bj} \equiv -1 \bmod m$. In particular, r is a root of $-1 \bmod b$.

Finally, let k be the smallest positive integer such that $r^k \equiv -1 \bmod b$. If $b > 1$, then r has order $2k$ as a unit mod b. Furthermore, since $r^{bj} \equiv -1 \bmod m$, we find that k divides bj, and then since both b and j are coprime to m/b, it follows that also k is coprime to m/b.

Next, we prove sufficiency. Suppose that r is a root of $-1 \bmod b$, and k is the smallest positive integer such that $r^k \equiv -1 \bmod b$, and k is coprime to m/b. Note that by the definition of b, we have $r \equiv 1 \bmod p$ for every prime p dividing m/b.

Take $a = xy^j$ for any integer j coprime to m/b such that $r^j \equiv -1 \bmod p$ for every prime p dividing b. (For example, we can take $j = k$, hence such a j always exists.) We need to show that the cyclic subgroup A generated by a is complementary to $Y = \langle y \rangle$. Since $a^2 = v^{r_j} y^{2j}$ lies in $\langle v, y \rangle$, which does not contain x and therefore does not contain $xv^j = a$, we know that a^2 generates a proper subgroup of A, and hence we need to show that $a^2 = v^{r_j} y^{2j}$ has order m.

For every prime p dividing b, we have $(r-1)r_j = r^j - 1 \equiv -1-1 \equiv -2 \bmod p$, so r_j is not divisible by p. On the other hand, for every prime p dividing m/b, we have $r_j \equiv 1 + 1^1 + \cdots + 1^{j-1} \equiv j \bmod p$, and since $\gcd(j, m/b) = 1$, again we find that r_j is not divisible by p. Thus $\gcd(r_j, m) = 1$, and in particular, v^{r_j} has order m.

Now let $t = r^{2j}$, and let d be the order of y^{2j}. Then $t^d \equiv (r^{2j})^d \equiv 1 \bmod m$. Also conjugation by y^{2j} takes v^{r_j} to $(v^{r_j})^t$, and hence by Lemma 4.1(c), we know that $v^{r_j} y^{2j}$ has order m if and only if $\gcd(t_d, m) = d$. In turn, since b and m/b are coprime, this is equivalent to having $\gcd(t_d, b) = \gcd(d, b)$ and $\gcd(t_d, m/b) = \gcd(d, m/b)$.

For the former, note that for every maximal prime-power p^e dividing b we have $t \equiv (r^j)^2 \equiv (-1)^2 \equiv 1 \bmod p$, and as p is odd, Lemma 4.2(a) gives $t_d \equiv d \bmod p^e$. Thus $t_d \equiv d \bmod b$, and it follows that $\gcd(t_d, b) = \gcd(d, b)$. For the latter, the same argument applies to maximal prime-power divisors of m/b, noting that if m/b is even, then r (and hence also r^j) is odd, which gives $t \equiv (r^j)^2 \equiv 1 \bmod 4$. Hence by Lemma 4.2 we have $\gcd(t_d, p^e) = \gcd(d, p^e)$ for every such prime-power p^e, which implies that $\gcd(t_d, m/b) = \gcd(d, m/b)$. Thus a has order $2m$.

Finally, we note that the group $H(m, r)$ is generated by x and y and hence also by $a = xy^j$ and y, so every element of the intersection $\langle a \rangle \cap \langle y \rangle$ is central in $H(m, r)$. On the other hand, no non-trivial element of $Y = \langle y \rangle$ centralises $\langle x, v \rangle \cong D_m$, so the intersection $\langle a \rangle \cap \langle y \rangle$ must be trivial. Thus $A = \langle a \rangle$ is complementary to $Y = \langle y \rangle$. ☐

Putting together Theorems 3.2, 3.5 and 5.1, we have the following:

Corollary 5.2. *For odd n, every regular Cayley map for C_n is isomorphic to the map $M(n, r)$ for some root r of -1 in $\mathbb{Z}_n$. For even $n = 2m$, every regular Cayley map for C_n is isomorphic to the map $M(n, r)$ for some unit r in $\mathbb{Z}_m$ with the properties that if b is the largest divisor of m coprime to $r-1$, then either $b = 1$,* *or r is a root of -1 mod b of multiplicative order $2k$ where k is coprime to m/b. Furthermore, in all cases, r is unique.*

Observe that the pair $(2m, 1)$ is admissible for all m, with $b = 1$. In this case y centralises v and conjugates x to xv, so $s = m$. Moreover, we can take $j = 1$ in Theorem 5.1, and find that xy has order $2m$, so the map $M(2m, 1)$ has type $\{2m, m\}$. As we will see later, these maps are anti-balanced. Similarly, the pair $(2m, -1)$ is admissible for all m, with b being the odd part of m, and $k = 1$; in this case y has order 2, and again xy has order $2m$, so the map $M(2m, -1)$ has type $\{2m, 2\}$. These are 2-valent balanced maps on the sphere.

In some sense the two special cases above are extremes, with $b = 1$ in the former case and b as large as possible in the latter. We now determine the types of all of the regular Cayley maps $M(n, r)$ defined in Section 3.

Theorem 5.3. *For odd n, the valence s of the map $M(n, r)$ is the multiplicative order of r as a unit mod m, and $s = 2k$ for some integer k. Furthermore, if k is even, then $M(n, r)$ has type $\{2k, 2k\}$, while if k is odd, then $M(n, r)$ has type $\{\operatorname{lcm}(k, n/c), 2k\}$ where c is the largest divisor of n that is coprime to $r + 1$. In particular, if k is odd and $r + 1$ is coprime to n, then the type of the map $M(n, r)$ is $\{k, 2k\}$.*

Proof. Admissibility requires r to be a root of -1 mod n, so its order s (as a unit mod n) is even, say $s = 2k$. The co-valence is the order of $xy = vy^k y = vy^{k+1}$ in the group $G(n, r)$. Note that y^{k+1} conjugates v to $v^{r^{k+1}} = v^{-r}$, since $r^k \equiv -1$ mod n. Hence if d denotes the order of y^{k+1}, then by Lemma 4.1(b), the order of vy^{k+1} is d times the additive order of $(-r)_d$ in $\mathbb{Z}_n$.

When k is even, $k+1$ is odd and hence coprime to $2k$, so y^{k+1} has order $2k = s$. Also $((-r) - 1)(-r)_s \equiv (-r)^s - 1 \equiv r^s - 1 \equiv 1 - 1 \equiv 0$ mod n, but similarly, we have $((-r) - 1)(-r)_k \equiv (-r)^k - 1 \equiv r^k - 1 \equiv -1 - 1 \equiv -2$ mod n, which shows that $(-r) - 1$ is coprime to n, and it follows that $(-r)_s \equiv 0$ mod n. Hence in this case, the order of vy^{k+1} is $2k = s$.

When k is odd, $k + 1$ is even and hence coprime to k but not to $2k$, so y^{k+1} has order $k = s/2$. In this case, let c be the largest divisor of n coprime to $r + 1$. Then since $((-r)-1)(-r)_k \equiv (-r)^k-1 \equiv -r^k-1 \equiv 1-1 \equiv 0$ mod n, the additive order of $(-r)_k$ in $\mathbb{Z}_n$ is $(n/c)/\gcd(k, n/c)$, by Lemma 4.3(a), which applies here with $m = n$ because n is odd. Hence in this case, the order of vy^{k+1} is $k(n/c)/\gcd(k, n/c)$, which is $\operatorname{lcm}(k, n/c)$. The rest follows easily. □

For the even order case, we first compute the valence, and then the co-valence.

Theorem 5.4. *For the admissible map $H(m, r)$, let b and k be as in Theorem 5.1, and let q be the multiplicative order of r as a unit mod m.*

(a) *Suppose the pair (m, r) is nice. Then the valence s is $\operatorname{lcm}(q, m/b)$. In particular, if $b = 1$, then $s = m$, while if $b > 1$, then $s = 2km/b$ if m is odd, and $s = km/b$ if m is even.*

(b) *Suppose the pair (m, r) is not nice. Then $s = k(m/b)/2^{f-1}$, where 2^f is the largest power of 2 dividing m for which $r \equiv -1$ mod 2^f.*

In particular, s is divisible by $2k$ except when m is odd and $b = 1$ (in which case $s = m$). Moreover, in all cases, s divides $(r - 1)q$, and s/k divides $2m/b$.

Proof. The valence s is the order of the automorphism of $\langle x, v\rangle \cong D_m$ given by conjugation by y. This is a multiple of q (the order of r as a unit mod m), and hence also a multiple of k (because k divides the order of r as a unit mod b). Next, since conjugation by y^q centralises v and takes x to xv^{r_q}, we find that s is q times the additive order of r_q in $\mathbb{Z}_m$. The latter divides $r-1$, since $0 \equiv r^q - 1 \equiv (r-1)r_q \bmod m$, and therefore s divides $(r-1)q$.

Now suppose that (m,r) is nice. Then by Lemma 4.3(a), the additive order of r_q in $\mathbb{Z}_m$ is $(m/b)/\gcd(q,m/b)$, and therefore $s = q(m/b)/\gcd(q,m/b) = \mathrm{lcm}(q,m/b)$.

If $b=1$, then for any maximal prime-power divisor p^e of m, by the definition of b we must have $r \equiv 1 \bmod p$, so the order of r as a unit mod p^e divides p^e. Hence q divides m, or equivalently, $\gcd(q,m) = q$. It follows that in this case, we have $s = q(m/b)/\gcd(q,m/b) = qm/\gcd(q,m) = m$.

If $b > 1$, then the order of r as a unit mod b is $2k$, while on the other hand, the order of r as a unit mod m/b divides m/b, by the same argument as in the previous paragraph. Hence $2k$ divides q, and q divides $\gcd(2k, m/b)$, which is $2km/b$ if m is odd, or km/b if m is even. Also if m is odd, then m/b is odd, and hence is coprime to $2k$, but m/b divisible by $q/(2k)$, so $\gcd(q,m/b) = \gcd(q/(2k), m/b) = q/(2k)$, and we find that $s = q(m/b)/\gcd(q,m/b) = 2k(m/b)$. Similarly, if m is even, then m/b is coprime to k and divisible by q/k, and therefore $\gcd(q,m/b) = \gcd(q/k, m/b) = q/k$, which gives $s = q(m/b)/\gcd(q,m/b) = k(m/b)$.

Next, suppose that (m,r) is not nice, so that $m \equiv 0 \bmod 4$ and $r \equiv 3 \bmod 4$. Then in particular, q is even. Also let 2^e and m' be the 2-power part and odd part of m, and let f be the largest integer such that $2 \le f \le e$ and $r \equiv -1 \bmod 2^f$.

If $f = e$, then $r \equiv -1 \bmod 2^e$, so $r_q \equiv 1 + (-1) + \cdots + 1 + (-1) \equiv 0 \bmod 2^e$, and therefore the additive order of r_q in $\mathbb{Z}_m$ is equal to the additive order of r_q in $\mathbb{Z}_{m'}$. In this case r has order 2 as a unit mod 2^e, so the order of r as a unit mod m' is still q, which is divisible by $2k$ but now divides $\gcd(2k, 2m'/b) = 2km'/b$, so we have $\gcd(q, m'/b) = \gcd(q/(2k), m'/b) = q/(2k)$. Hence the additive order of r_q in $\mathbb{Z}_{m'}$ is $(m'/b)/\gcd(q,m'/b) = 2k(m'/b)/q$, which gives $s = 2k(m'/b) = k(m/b)/2^{e-1}$.

If $f < e$, then $r \equiv -1 + c2^f \bmod 2^e$, where c is odd. Now the order of r as a unit mod b is $2k$, where k is odd (since k is coprime to m/b, which is even). On the other hand, $r^2 = 1 - 2c2^f + c^2 2^{2f} = 1 + c' 2^{f+1}$ where $c' = -c + c^2 2^{f-1}$ is odd, so the order of r^2 as a unit mod 2^e is 2^{e-f-1}, and hence the order of r as a unit mod 2^e is 2^{e-f}. Also the order of r as a unit mod m'/b divides m'/b, by the same argument as given previously. It follows that the 2-power part of q is 2^{e-f}. Next, Lemma 4.2(c) tells us that $r_q \equiv (r+1)q/2 \equiv cq2^{f-1} \bmod 2^e$, and since the 2-power part of $cq2^{f-1}$ is $2^{e-f}2^{f-1} = 2^{e-1}$, we find that the additive order of r_q in $\mathbb{Z}_{2^e}$ is 2. Also $\gcd(q, m'/b) = \gcd(q/(2^{e-f}k), m'/b) = q/(2^{e-f}k)$, so the additive order of r_q in $\mathbb{Z}_{m'}$ is $(m'/b)/\gcd(q,m'/b) = 2^{e-f}k(m'/b)/q$, which is odd. Hence the additive order of r_q in $\mathbb{Z}_m$ is $2^{e-f+1}k(m'/b)/q$, and we have $s = 2^{e-f+1}k(m'/b) = k(m/b)/(2^{f-1})$.

Finally, it is easy to check the above to verify that s is divisible by $2k$ except when m is odd and $b=1$, and that s/k divides $2m/b$ in all cases. □

Theorem 5.5. *Let s be the valence of the regular Cayley map $M(2m,r)$. If s is odd, then $s = m$ and the co-valence of the map is $2m$, while if s is even, then the co-valence is $2\,\mathrm{lcm}(s/2, m/c)$, where c is the largest divisor of m coprime to r^2-1.*

Proof. In all cases, the co-valence of $M(2m,r)$ is the order of xy in the group $H(m,r)$.

First suppose that s is odd. Then $b = 1$ (since otherwise s is divisible by $2k$), and we can take $j = 1$ in Theorem 5.1, and find that xy has order $2m$. Also (m, r) is nice, for otherwise Theorem 5.4(b) gives $s = m/2^{f-1}$ where 2^f divides m, but that would make s even. Hence $s = m$, by Theorem 5.4(a), and so the type of the map $M(2m, r)$ is $\{2m, m\}$ in this case.

Suppose instead that s is even. Since $(xy)^2 = vy^2$ and $(vy^2)^i = v^{(r^2)_i}y^{2i}$, which is trivial only if $2i$ is a multiple of s, we see that the order of xy is divisible by s, and indeed since $(xy)^s = (vy^2)^{s/2} = v^{(r^2)_{s/2}}$, the order of xy is s times the additive order of $(r^2)_{s/2}$ in $\mathbb{Z}_m$. Now let c be the largest divisor of m coprime to $r^2 - 1$. Then since $(r^2 - 1)(r^2)_{s/2} \equiv (r^2)^{s/2} - 1 \equiv r^s - 1 \equiv 0 \bmod m$ but $r^2 - 1$ is coprime to c, we have $(r^2)_{s/2} \equiv 0 \bmod c$. On the other hand, the pair (m, r^2) is nice (since if $m \equiv 0 \bmod 4$, then r is odd and so $r^2 \equiv 1 \bmod 4$), and hence by Lemma 4.3(a), the additive order of $(r^2)_{s/2}$ in $\mathbb{Z}_{m/c}$ is $(m/c)/\gcd(s/2, m/c)$. Since $(r^2)_{s/2} \equiv 0 \bmod c$, this is also the the additive order of $(r^2)_{s/2}$ in $\mathbb{Z}_m$, and therefore the order of xy (and co-valence of $M(2m, r)$) is $s(m/c)/\gcd(s/2, m/c) = 2\,\mathrm{lcm}(s/2, m/c)$. □

6. Enumeration

In this section, we give a specific formula for the number of regular Cayley maps for C_n in each of the two cases (n odd and n even).

For odd n, this is simply a formula for the number of roots of -1 in the group of units modulo n. To obtain it, we need some notation. For any positive integer k, let $O_2(k)$ and $O_{2'}(k)$ be the 2-power part and the odd part of k given by its prime factorisation, so $k = O_2(k)O_{2'}(k)$. For example, $O_2(120) = 8$ while $O_{2'}(120) = 15$.

Theorem 6.1. *For every odd $n > 2$, the number of non-isomorphic regular Cayley maps for the cyclic group C_n is*

$$O_{2'}(\phi(n))(t^{\omega(n)} - 1)/(2^{\omega(n)} - 1),$$

where ϕ is Euler's function, $\omega(n)$ is the number of distinct prime divisors of n, and t is the minimum of the 2-powers $O_2(p-1)$ over all primes p dividing n.

Proof. First consider the case where $n = p^e$ for some odd prime p. Here the number of units of n is $\phi(p^e) = p^{e-1}(p-1)$, and these are well known to form a cyclic group. (In fact our Lemma 4.2(a) gives a unit of multiplicative order p^{e-1}.) Now the units of odd order mod p^e are precisely those of the form $ap + b$ where $a \in \mathbb{Z}_{p^{e-1}}$ and b is a unit of odd order in $\mathbb{Z}_p$, so the number of these is $p^{e-1}O_{2'}(p-1)$. Hence the number of units of odd order in $\mathbb{Z}_{p^e}$ is $p^{e-1}(p-1) - p^{e-1}O_{2'}(p-1)$, which can be rewritten as $(O_2(p-1) - 1)p^{e-1}O_{2'}(p-1)$.

Next, more generally, consider n as a product of such prime-powers. If r is a root of $-1 \bmod n$, then the 2-power parts of the orders of r modulo q must be the same for all maximal prime-powers $q = p^e$ dividing n, and hence must all be at most t (the minimum of the 2-power parts of $p-1$ for all p). Now suppose $2^i \le t$. Then for all such q the number of roots of $-1 \bmod q$ having order divisible by 2^i but not 2^{i+1} is

$$2^ip^{e-1}O_{2'}(p-1) - 2^{i-1}p^{e-1}O_{2'}(p-1) = (2^i - 2^{i-1})p^{e-1}O_{2'}(p-1) = 2^{i-1}p^{e-1}O_{2'}(p-1).$$

By the Chinese Remainder Theorem, the number of roots of -1 mod n having order divisible by 2^i but not 2^{i+1} is the product of these (over all primes p dividing n). The product of the odd parts $p^{e-1}O_{2'}(p-1)$ is

$$\prod_{p|n}(p^{e-1}O_{2'}(p-1)) = O_{2'}(\prod_{p|n}(p^{e-1}(p-1))) = O_{2'}(\prod_{p|n}\phi(p^e)) = O_{2'}(\phi(n)),$$

while the product of the 2-power parts 2^{i-1} is

$$\prod_{p|n}2^{i-1} = 2^{\sum_{p|n}(i-1)} = 2^{(i-1)\omega(n)}.$$

Hence the total number of roots of -1 mod n is

$$\begin{aligned}\sum_{1\le 2^i\le t} 2^{(i-1)\omega(n)}O_{2'}(\phi(n)) &= O_{2'}(\phi(n))\sum_{1\le 2^i\le t} 2^{(i-1)\omega(n)}\\ &= O_{2'}(\phi(n))(t^{\omega(n)}-1)/(2^{\omega(n)}-1),\end{aligned}$$

as required. □

Thus, for example, the number of regular Cayley maps for C_{11}, C_{27}, C_{49} and C_{65} are $O_{2'}(11) = 5$, $(O_2(2)-1)\cdot 9 = 9$, $7\cdot O_{2'}(6) = 21$ and $O_{2'}(48)\cdot(4^2-1)/(2^2-1) = 15$, respectively. We have confirmed that the given formula is correct for many such small cases, using Magma [1].

Corollary 6.2. *If n is a Fermat prime $p = 2^e+1$, then the number of non-isomorphic regular Cayley maps for the cyclic group C_n is $\phi(n)-1 = n-2$. On the other hand, if n is a product of distinct Fermat primes one of which is 3, then there is just one regular Cayley map for C_n (of valency 2 and genus 0). In all other cases for odd n, the number of such maps is strictly between 1 and $\phi(n)-1$.*

Obtaining a specific formula for the number of regular Cayley maps for cyclic groups of even order is a little more challenging. To do this, we use the following:

Lemma 6.3. *If the pair $(2m, r)$ is admissible, then so is $(2m', r')$ for any positive integer m' with exactly the same prime divisors as m, and any $r' \in \mathbb{Z}_{m'}$ with the property that $r' \equiv r$ mod p for every prime p dividing m.*

Proof. Let b' be the largest divisor of m' coprime to $r'-1$. Then b' has exactly the same prime divisors as b, and m'/b' has exactly the same prime divisors as m/b, by the given property of r'. If $b' = 1$, then admissibility is trivial, so suppose that $b' > 1$, in which case $b > 1$ as well.

Now let d be the smallest positive integer such that $r^d \equiv -1$ mod p for every prime p dividing b. Then d divides k, and $(r')^d \equiv -1$ mod p for all such p, and in fact d is the smallest positive integer for which this happens, by the hypothesis on r'. Hence by Lemma 4.2, the order of r' as a unit mod b' is $2d\ell$ for some ℓ dividing b'. In particular, $(r')^{d\ell}$ has order 2 as a unit mod b', and $(r')^{d\ell} \equiv (-1)^\ell \equiv -1$ mod p for all primes p dividing b', and it follows that $(r')^{d\ell} \equiv -1$ mod b'. Therefore r' is a root of -1 mod b'. Also the smallest positive integer k' for which $(r')^{k'} \equiv -1$ mod b' must divide $d\ell$, which in turn divides kb', and is therefore coprime to m/b, and hence also to m'/b'. Thus the pair $(2m', r')$ is admissible. □

The above lemma allows a reduction which gives us our enumeration formula for the case $n = 2m$:

Theorem 6.4. *For all $m > 1$, let q be the product of the odd prime divisors of m. Then the number of non-isomorphic regular Cayley maps for the cyclic group C_{2m} is equal to*

$$\begin{cases} \dfrac{m}{2q} \displaystyle\sum_{b\,|\,q} \prod_{p\,|\,b} \delta(p-1, 2q/b) & \text{if } m \text{ is even,} \\ \dfrac{m}{q} \displaystyle\sum_{b\,|\,q} (1 + 2^{\omega(b)} + \cdots + 2^{\omega(b)(t(b)-1)}) \prod_{p\,|\,b} \delta(p-1, 2q/b) & \text{if } m \text{ is odd,} \end{cases}$$

where the product is over all primes p dividing b in each case, $\omega(b)$ is the total number of prime divisors of b, and $\delta(p-1, 2q/b)$ is the largest (odd) divisor of $p-1$ coprime to $2q/b$, while $2^{t(b)}$ is the greatest common divisor of the 2-power parts of $p-1$ for all primes p dividing b.

Proof. By Theorem 3.5, the number of regular Cayley maps for C_{2m} is equal to the number of units r in $\mathbb{Z}_m$ for which the pair (m, r) is admissible. Any such r determines a unique odd divisor b of m with the properties given in Theorem 5.1.

Now let m' be the largest square-free divisor of m, namely the product of all prime divisors of m. Then by Lemma 6.3, the number of units r mod m for which (m, r) is admissible is equal to m/m' times the number of units r' mod m' for which (m', r') is admissible. Thus we can reduce to the case where m is square-free.

In that case, write $m = 2q$ when m is even, or $m = q$ when m is odd. Then we find the total number of regular Cayley maps by counting for each divisor b of q the number of $r \in \mathbb{Z}_m$ for which r is a kth root of -1 mod b for some k coprime to q/b, while $r \equiv 1$ mod p for every prime p dividing q/b. If $b = 1$, then there is just one possibility, namely $r = 1$, and also this case contributes 1 to the summation given in the statement of the theorem, as required. If $b > 1$, we proceed as follows.

If m is even, then m/b is even, and k must be odd and coprime to $m/b = 2q/b$. In particular, for every prime divisor p of b, the order of r as a unit mod p must be twice a divisor of $\delta(p-1, 2q/b)$. Conversely, if the order of r as a unit mod p is twice a divisor of $\delta(p-1, 2q/b)$ for all such p, then -1 is a kth root of -1 mod b for some odd k (equal to the least common multiple of those divisors). Since the group of units of each $\mathbb{Z}_p$ is cyclic (of even order $p-1$), it now follows from the Chinese Remainder Theorem that the number of possibilities for r is the product of the terms $\delta(p-1, 2q/b)$ for all primes p dividing b.

If m is odd, then k can be even, but is coprime to $m/b = q/b$. Let $2^{t(b)}$ be the greatest common divisor of the 2-power parts of $p-1$ for all the primes p dividing b. Then the 2-power part of k must be 2^i for some i in the range $0 \le i < t(b)$, and the order of r as a unit mod p must be an odd multiple of 2^{i+1}. For any such i and p, the number of such units mod p is $2^i\,\delta(p-1, 2q/b)$, and hence (again by the Chinese Remainder Theorem) the number of possibilities for r is the product of these, which is $2^{\omega(b)i}$ times the product of the terms $\delta(p-1, 2q/b)$ over the primes p dividing$b$. □

Corollary 6.5. *For $m > 2$, the total number of non-isomorphic regular Cayley maps for the cyclic group C_{2m} is equal to $\phi(m)$ whenever m is*

(a) *a power of 2, or*
(b) *a power of an odd Fermat prime $p = 2^e + 1$, or*
(c) *a positive integer of the form $2^e 3^f$ where $e > 0$ and $f > 0$.*

On the other hand, the number of such maps is 2 when m is 3 or 4 or twice an odd Fermat prime. In all other cases, the number is strictly between 2 and $\phi(m)$.

Proof. In case (a), if $m = 2^e$ then Theorem 6.4 gives the number of maps as $\frac{m}{2} = \phi(m)$. (Indeed, more directly: for any unit r mod m we can take $b = 1$ and find that the pair (m, r) is admissible, and so gives a regular Cayley map.) In case (b), if $m = p^f$ where $p = 2^e + 1 > 2$, the number of maps is $\frac{m}{p}(1 + (2^e - 1)) = p^{f-1}2^e = p^{f-1}(p-1) = \phi(m)$. Similarly, in case (c), where $m = 2^e 3^f$, the number of maps is $\frac{m}{6}(1+1) = \frac{m}{3} = \phi(m)$.

In particular, the number of maps is 2 when $m = 3$ or 4. Also if $m = 2p$ where p is an odd Fermat prime, then the number of maps is $\frac{m}{2p}(1+1) = \frac{m}{p} = 2$.

For all other values of m, it is easy to show that there exists at least one unit $r \not\equiv \pm 1$ mod m such that the pair (m, r) is admissible, and at least one unit r mod m for which (m, r) is not admissible.

For example, suppose m is divisible by some non-Fermat odd prime, say p. Then $\phi(m)$ is divisible by some odd prime $\ell < p$. Take any $r \in \mathbb{Z}_m$ with the property that r has order ℓ when considered as a unit mod p^e, the highest power of p dividing m, and $r \equiv 1$ mod q for every other maximal prime-power q dividing m. Then r has (odd) order $\ell > 1$ as a unit mod m, so the pair (m, r) is not admissible. On the other hand, if m is a power of p, then we can choose r as a unit of order $p - 1$ in $\mathbb{Z}_m$, or otherwise choose r (using the Chinese Remainder Theorem) such that $r \equiv -1$ mod p but $r \equiv 1$ mod q for every other prime divisor q of m, and find that (m, r) is admissible.

The remaining possibilities are left as an exercise for the reader. □

7. Representing maps in different ways

In this final section we investigate how a regular Cayley map $M = \mathrm{Cay}(A, X, \varphi)$ for a cyclic group A can take different forms with respect to the given group A, depending on the choice of the generating orbit X.

For odd n, we first characterise all elements of $G(n, r)$ that generate a cyclic group acting regular on vertices of $M(n, r)$:

Theorem 7.1. *In the group $G(n, r)$, the element $a = vy^j$ generates a cyclic subgroup complementary to $Y = \langle y \rangle$ if and only if $s/\gcd(s, j)$ divides n and $r^j \equiv 1$ mod p for every prime p dividing n.*

Proof. Let $t = r^j$, and let d be the order of t as a unit mod n, which is $s/\gcd(s, j)$.

Now suppose that $a = vy^j$ has order n and $\langle a \rangle \cap \langle y \rangle = \{1\}$. Then taking $m = n$ and $u = v$ and $w = y^j$, we find by Lemma 4.1(d) that every positive integer k for which $t_k \equiv 0$ mod n is a multiple of d, and hence by Lemma 4.3(b) that d divides n and $t \equiv 1$ mod p for every prime p that divides n.

Conversely, suppose d divides n and $r^j \equiv 1$ mod p for every prime p dividing n. Then since n is odd, Lemma 4.2(a) gives $t_d \equiv d$ mod p^e for every prime-power p^e dividing n, and so $t_d \equiv d$ mod n. This gives $\gcd(t_d, n) = \gcd(d, n) = d$, and hence by Lemma 4.1(c), we find that vy^j has order n. Also $G(n,r)$ is generated by v and y and hence also by $a = vy^j$ and y, so every element of $\langle a\rangle \cap \langle y\rangle$ is central in $G(n,r)$. But no non-trivial element of $\langle y\rangle$ centralises $\langle v\rangle$, so the intersection $\langle a\rangle \cap \langle y\rangle$ must be trivial. Thus $A = \langle a\rangle$ is complementary to $Y = \langle y\rangle$. □

This leads to the following:

Theorem 7.2. *For odd $n > 2$, every regular Cayley map $M(n,r)$ has a balanced representation. On the other hand, in the group $G(n,r)$, the subgroup $\langle v\rangle$ is the only normal subgroup complementary to $Y = \langle y\rangle$. As a consequence, the cyclic group C_n has a regular Cayley map with a non-balanced representation if and only if n is not square-free.*

Proof. For the first assertion, see Corollary 3.3 and earlier observations. For the second, note that if A is any normal subgroup of G complementary to $Y = \langle y\rangle$, then $G/A \cong Y \cong C_s$ (where s is the order of y); in particular, G/A is abelian so A contains the commutator subgroup $\langle v\rangle$, and then a comparison of orders gives $A = \langle v\rangle$.

Now suppose n is square-free, and let $M(n,r)$ be any regular Cayley map for C_n. Also let j be any integer such that $a = vy^j$ generates a subgroup A complementary to Y in $G(n,r)$. Then by Theorem 7.1, $r^j \equiv 1 \bmod p$ for every prime p dividing n, and since n is square-free, this implies that $r^j \equiv 1 \bmod n$. Therefore y^j is trivial, so $j \equiv 0 \bmod s$, and $a = v$. Hence every representation of $M(n,r)$ as a regular Cayley map for C_n is balanced.

Conversely, suppose that n is not square-free. Then n is divisible by p^2 for some prime p. Let p^e be the largest power of p dividing n, and let r be any positive integer for which $r \equiv p^{e-1} - 1 \bmod p^e$ while $r \equiv -1 \bmod n/p^e$. (Such an integer exists by the Chinese Remainder Theorem.) Then r is a unit mod p^e of order $2p$ and also a unit mod n/p^e of order 2, so r is a unit mod n, with $r^p \equiv -1 \bmod n$. Hence the pair (n,r) is admissible. In particular, $s = 2p$ for this choice of r. Also we can take $j = 2$ in Theorem 7.1, since $\gcd(s,2) = 2$ and $s/2 = p$ which divides n, and $r^2 \equiv 1 \bmod t$ for every prime t dividing n. Hence $a = vy^2$ generates a cyclic subgroup of $G(n,r)$ that is complementary to Y, but is not normal in $G(n,r)$. Thus $M(n,r)$ has a non-balanced representation. □

Note that the smallest non-balanced representations in the odd order case occur for $n = 9$; these are obtainable by taking $r = 2$ and letting $a = vy^2$ or $a = vy^4$.

There are no anti-balanced regular Cayley maps for C_n when n is odd. In fact, as noted earlier, there are no t-balanced regular Cayley maps for C_n for any $t \neq 1$ (modulo the valence), since C_n has no subgroup of index 2.

For cyclic groups of even order, the situation is different — it can happen that $M(2m,r)$ has no balanced representation at all:

Theorem 7.3. *For $m > 2$, the regular Cayley map $M(2m,r)$ has a balanced representation if and only if r is a root of -1 mod m. In all such cases, $m = 2^e b$ for some e, with $r \equiv -1$ mod 2^e, and $s = 2k$, which is the order of r as a unit mod m.*

Proof. Suppose $M(2m,r)$ has a balanced representation as a regular Cayley map for C_{2m}. Then $G = H(m,r)$ contains a cyclic normal subgroup A complementary to $Y = \langle y\rangle$. In particular, $G/A \cong Y$ which is cyclic, so A contains $G' = \langle v\rangle$, and therefore A is generated by some element a such that $a^2 = v$. Moreover, conjugation by y takes a to a^t, and since the balanced property requires $y^{s/2}$ to invert every element of a generating set for A, we find that t is a root of -1 mod $2m$, and hence also a root of -1 mod m. But now $yvy^{-1} = ya^2y^{-1} = a^{2t} = v^t$ and so $t \equiv r$ mod m, and it follows that r is root of -1 mod m.

Conversely, suppose r is a root of -1 mod m (and the pair (m, r) is admissible). Then $r \not\equiv 1$ mod p for any odd prime p dividing m, so b is the odd part of m, and $m = 2^e b$, say. But also if $e > 0$ (so that m is even), then r must be -1 itself mod 2^e (since the order of any unit mod 2^e is a power of 2, and the square of any such unit is 1 mod 4), and hence r has order 1 or 2 as a unit mod 2^e. It follows that the order of r as a unit mod m is equal to $2k$, and therefore $r^k \equiv -1$ mod m. We could now use Theorem 5.4 to prove that $s = 2k$, but it is easy to do this directly: first, y^{2k} centralises v, because $r^{2k} \equiv 1$ mod m, but also $y^{2k}xy^{-2k} = xv^{r_{2k}}$ where $r_{2k} = r_k(1 + r^k) \equiv r_k(1 - 1) \equiv 0$ mod m, and so y^{2k} centralises x as well; thus y has order $2k$. Next, we can take $a = xy^k$ in Theorem 5.1 and find that $M(2m, r)$ is a regular Cayley map for $\langle a \rangle$. For this choice of a we have $x^{-1}ax = y^k x = y^{-k}x = a^{-1}$, and $yay^{-1} = yxy^{k-1} = xvy^k = v^{-1}xy^k = v^{-1}a$, which lies in $A = \langle a \rangle$ because $a^2 = v^{r_k}$ generates $\langle v \rangle$. Thus A is normal in $\langle x, y \rangle = \langle x, v, y \rangle = G$, and so the map $M(2m, r)$ is balanced with respect to $A \cong C_{2m}$. □

Note that in the special case where $r = -1$, we have $k = 1$ and valence $s = 2$, giving us the balanced maps of genus 0 mentioned after Corollary 5.2.

On the other hand, it is easy to use Theorem 7.3 to construct regular Cayley maps for cyclic groups of even order that have no balanced representation: for example, just take $r = 1$ for any $m > 2$, or for any m divisible by two distinct primes, take a maximal odd prime-power divisor b of m and choose r such that $r \equiv -1$ mod b while $r \equiv 1$ mod m/b.

Similarly, when $M(2m, r)$ does have a balanced representation, it can sometimes also have a non-balanced representation. For suppose m is odd and has an odd maximal prime-power divisor p^e with $e > 1$. Take r such that $r \equiv -1+p^{e-1}$ mod p^e while $r \equiv -1$ mod m/p^e, in which case $r^p \equiv -1$ mod m, and $b = m$ (and $k = p$). Then $H(m, r)$ has a balanced representation using $a = xy^p$. On the other hand, taking $a = xy$ also gives a cyclic group complementary to Y, by Theorem 5.1, since $r \equiv -1$ for all p dividing b, but in this case $a^2 = vy^2 \notin \langle v \rangle$, so this representation of the map is not balanced.

Finally, we consider which maps $M(2m, r)$ have t-balanced representations for some t. Together with the balanced maps for cyclic groups of odd order, this gives a complete classification of t-balanced regular Cayley maps for cyclic groups. A similar classification has been achieved independently by Young Soo Kwon [21].

Theorem 7.4. *The regular Cayley map $M(2m, r)$ can be represented as a t-balanced regular Cayley map for C_{2m} for some t if and only if $r^2 \equiv 1$ mod m/b. Moreover, if $r \equiv 1$ mod m, then the map is anti-balanced* (*with $t = -1$*)*, while if $r \equiv -1$ mod m, then the map is balanced* (*with $t = 1$*)*. In all other cases, the order of r as a unit mod m is equal to $2k$* (*where $k = 1$ if $b = 1$*)*, and r_k is a unit mod m, and then $t \equiv 1 - 2k\ell$ mod s, where ℓ is the multiplicative inverse of r_k in $\mathbb{Z}_m$.*

Proof. First we consider the special cases $r \equiv \pm 1$ mod m, which were described briefly after Corollary 5.2.

When $r \equiv 1$ mod m we have $s = m$, since y centralises v and conjugates x to xv. Also $b = 1$, and we can take $a = xy^j$ for any j coprime to m. Since $r \equiv 1$ mod m we have $r_j \equiv j$ mod m, and so $a^2 = v^{r_j}y^{2j} = v^j y^{2j}$. Letting ℓ be the multiplicative inverse of j mod m, we find that $a^{2\ell} = (v^j y^{2j})^\ell = v^{j\ell} y^{2j\ell} = vy^2$, and it follows that $ya = yxy^j = xvy^{j+1} = xy^j vy = avy = avy^2 y^{-1} = a^{2\ell+1} y^{-1}$. Hence the map is anti-balanced, for every choice of a. [In fact $M(2m, r)$ is a regular Cayley map for C_{2m} of class (i) or (ii) as described in [7, §7], depending on whether m is odd or even.]

On the other hand, when $r \equiv -1$ mod m we have $s = 2$, since y^2 centralises v and $r_2 \equiv 1 + (-1) \equiv 0$ mod m. Because $s = 2$ we must take $j = 1$, giving $a = xy$, and then $a^2 = vy^2 = v$. It follows that $ya = yxy = y^{-1}xy = a^{-1}y$, which means we have a 1-balanced map (of type $\{2m, 2\}$ on the sphere).

So from now on let us suppose that $r \not\equiv \pm 1$ mod m. Also let q be the multiplicative order of r as a unit mod m.

Suppose that $M(2m, r)$ can be represented as a t-balanced regular Cayley map for $A \cong C_{2m}$ by taking $a = xy^j$ as the generator for A.

Let K be the kernel of the skew morphism of A given by conjugation by y. Then since we have a t-balanced map representation, K has index 1 or 2 in A, and hence $K = \langle a \rangle$ or $\langle a^2 \rangle$. In either case, $\langle a^2 \rangle$ is normalised by y (by [7, Lemma 5.1]), and hence is normal in $\langle a, y \rangle = G$. The centraliser $C_G(K)$ of K contains a, so the quotient $G/C_G(K)$ is cyclic, generated by the image of y, and so $C_G(K)$ also contains $G' = \langle v \rangle$. Thus a^2 commutes with v. Then since $a^2 = v^{r_j} y^{2j}$, we find that y^{2j} commutes with v, and so $2j$ is a multiple of q.

Also by Theorem 5.1 we know that j is coprime to m/b, and hence $q/2$ is coprime to m/b. On the other hand, since $r - 1$ is divisible by every prime divisor of m/b, we know that the order of r as a unit mod m/b divides m/b (by Lemma 4.2), and hence the order of r as a unit mod m/b divides $\gcd(q, m/b)$, which is at most 2. Thus $r^2 \equiv 1$ mod m/b.

Conversely, suppose that $r^2 \equiv 1$ mod m/b. If $b > 1$, then since also $r^{2k} \equiv (-1)^2 \equiv 1$ mod b, we have $r^{2k} \equiv 1$ mod m, and so y^{2k} centralises v and q divides $2k$. Moreover, since $2k$ is the order of r as a unit mod b, it follows that $q = 2k$. Similarly, if $b = 1$, then $r^2 \equiv 1$ mod m and so $q = 2$, and in this case we take $k = 1$ in what follows.

By Theorem 5.1 we can take $a = xy^k$ and obtain $M(2m, r)$ as a regular Cayley map for $A = \langle a \rangle$. In particular, by the observation we made in the second paragraph of Theorem 5.1, we know that r_k is a unit mod m.

Note that $a^2 = v^{r_k} y^{2k} = v^{r_k} y^q$. We claim that the subgroup generated by a^2 is normal in $H(m, r)$. Since $H(m, r)$ is generated by a and y, we need to show that $\langle a^2 \rangle$ is normalised by y, and then since

$$ya^2 y^{-1} = y(v^{r_k} y^q) y^{-1} = v^{r_k r} y^q = v^{r_k (r-1)} v^{r_k} y^q = v^{r_k (r-1)} a^2,$$

it suffices to show that $v^{r_k(r-1)} \in \langle a^2 \rangle$. To do this, note that s is divisible by $q = 2k$, and by Theorem 5.4 that s divides $(r-1)q$. Now let $w = a^{s/k} = (a^2)^{s/q} = (v^{r_k} y^q)^{s/q}$, which equals $v^{r_k s/q}$ because y^q commutes with v and $y^s = 1$. It now follows that $v^{r_k(r-1)} = w^{(r-1)q/s} = a^{(r-1)q/k} = a^{2(r-1)}$, which lies in $\langle a^2 \rangle$.

Finally, let $c = r^k = r^{q/2}$. Then $c^2 \equiv r^q \equiv 1$ mod m, and since y^{2k} centralises v, we have $y^{-k} v y^k = y^k v y^{-k} = v^c$, and so $ya = yxy^k = xvy^{k+1} = xy^k v^c y = av^c y$. On the other hand, since s divides $(r-1)q$, we know that $qr \equiv q$ mod s, and then an easy induction gives $qc \equiv qr^k \equiv q$ mod s, and therefore $y^{qc} = y^q$. Hence if ℓ is the multiplicative inverse of r_k in $\mathbb{Z}_m$, we have

$$(a^2)^{\ell c} = (v^{r_k} y^q)^{\ell c} = v^{r_k \ell c} y^{qc\ell} = v^c y^{q\ell} = (v^c y) y^{q\ell - 1},$$

and thus $ya = av^c y = a(a^2)^{\ell c}(y^{q\ell-1})^{-1} = a^{2\ell c+1}y^{1-q\ell}$. This shows that the map is t-balanced, where $t \equiv 1 - q\ell \equiv 1 - 2k\ell \bmod s$. □

Note that for balanced representations (where $t = 1$), the last condition implies that $2k\ell \equiv 0 \bmod s$, and hence that $y^{2k\ell}$ is trivial. But the order of $y^{2k} = y^q$ is s/q, which divides m (by Theorem 5.4), and ℓ is a unit mod m, so this implies that y^{2k} is trivial, and therefore $s = q = 2k$. Also for a balanced representation we need conjugation of $A = \langle a \rangle$ by $y^{s/2}$ to be the inversion automorphism, so we find that $r^k \equiv -1 \bmod m$, which is precisely the requirement of Theorem 7.3.

Similarly we have the following, which also follows from the fact that a regular Cayley map for a cyclic group is reflexible if and only if it is anti-balanced (see [8]):

Corollary 7.5. *For $m > 1$, the regular Cayley map $M(2m, r)$ has a representation as an anti-balanced regular Cayley map for C_{2m} if and only if $r^2 \equiv 1 \bmod m$.*

Proof. If such a representation occurs, then $1 - 2k\ell \equiv -1 \bmod s$, so $k\ell \equiv -1 \bmod s/2$, and in particular, k is a unit mod $s/2$. On the other hand, $q = 2k$ divides s, so this forces $k = 1$ and $q = 2$, and so $r^2 \equiv 1 \bmod m$. Conversely, if $r^2 \equiv 1 \bmod m$, then $k = 1$ and $r_k = 1$, so $\ell = 1$ and $1 - 2k\ell \equiv 1 - 2 \equiv -1 \bmod s$. □

Some small examples of regular Cayley maps for cyclic groups of even order that have a t-balanced representation for some $t \neq \pm 1$ are as follows:

- $M(30, 7)$ is 5-balanced, of type $\{12, 12\}$,
- $M(56, 5)$ is 7-balanced, of type $\{24, 12\}$,
- $M(90, 28)$ is 17-balanced, of type $\{36, 36\}$,
- $M(110, 12)$ is 21-balanced, of type $\{44, 44\}$,
- $M(112, 5)$ is 7-balanced, of type $\{48, 24\}$,
- $M(210, 43)$ is 41-balanced, of type $\{84, 84\}$,
- $M(264, 85)$ is 11-balanced, of type $\{120, 60\}$,
- $M(280, 61)$ is 19-balanced, of type $\{120, 60\}$.

Some small examples of regular Cayley maps for cyclic groups of even order that have no t-balanced representation for any t are as follows, with the 'power function values' indicating the values of the power function of any skew morphism associated with a regular Cayley map representation:

- $M(18, 4)$, of type $\{18, 9\}$, with power function values $\{2, 5, 8\}$,
- $M(32, 3)$, of type $\{32, 8\}$, with power function values $\{3, 7\}$,
- $M(32, 5)$, of type $\{32, 16\}$, with power function values $\{7, 15\}$,
- $M(36, 7)$, of type $\{36, 18\}$, with power function values $\{5, 11, 17\}$,
- $M(50, 6)$, of type $\{50, 25\}$, with power function values $\{4, 9, 14, 19, 24\}$,
- $M(54, 10)$, of type $\{54, 27\}$, with power function values $\{8, 17, 26\}$,
- $M(64, 3)$, of type $\{64, 32\}$, with power function values $\{3, 7\}$ or $\{11, 15\}$.

8. Summary

To complete this paper, and to make reference easier for the reader, we bring together most of the main facts about our two families of regular Cayley maps for cyclic groups.

Every regular Cayley map for C_n is isomorphic to exactly one of the maps $M(n,r)$ we have defined here. For odd n, the regular Cayley map $M(n,r)$:

- is defined for every unit r mod n that is a root of -1 in $\mathbb{Z}_n$,
- has automorphism group $G(n,r) = \langle\, v, y \,|\, v^n = y^s = 1,\, yvy^{-1} = v^r \,\rangle$, where s is the order of r as a unit mod n,
- has valence s (which is even), and co-valence s if $s/2$ is even, or $\mathrm{lcm}(s/2, n/c)$ where c is the largest divisor of n coprime to $r+1$, if $s/2$ is odd,
- is reflexible if and only if $r \equiv -1$ mod n (and $s = 2$),
- is a regular Cayley map for $A = \langle vy^j \rangle$ if and only if $s/\gcd(s,j)$ divides n and $r^j \equiv 1$ mod p for every prime p dividing n,
- always has a balanced representation,
- has a non-balanced representation if and only if n is divisible by the square of some prime,
- has no anti-balanced representation, and indeed has no t-balanced representation for any $t \neq 1$.

For even $n = 2m$, the regular Cayley map $M(2m, r)$:

- is defined for every unit r mod m such that if b is the largest divisor of m that is coprime to $r-1$, then either $b = 1$, or r is a root of -1 mod b of multiplicative order $2k$ where k is coprime to m/b,
- has automorphism group$H(m,r) = \langle\, x, v, y \,|\, x^2 = v^m = y^s = 1,\, xvx = v^{-1},\, yvy^{-1} = v^r,\, yxy^{-1} = xv \,\rangle$, where s is the order of the automorphism of $\langle x, v\rangle \cong D_m$ taking (x,v) to (xv, v^r),
- has valence s, which is $\mathrm{lcm}(q, m/b)$ where q is the order of r as a unit mod m, if $m \not\equiv 0$ mod 4 or $r \equiv 1$ mod 4, or $k(m/b)/2^{f-1}$ where 2^f is the largest 2-power dividing m such that $r \equiv -1$ mod 2^f, if $m \equiv 0$ mod 4 and $r \equiv 3$ mod 4,
- has co-valence $2m$ if s is odd (in which case $s = m$), or $2\,\mathrm{lcm}(s/2, m/c)$ where c is the largest divisor of m coprime to $r^2 - 1$, if s is even,
- is reflexible if and only if $r^2 \equiv 1$ mod m,
- is a regular Cayley map for $A = \langle xv^i y^j \rangle$ if and only if j is coprime to m/b and $r^j \equiv -1$ mod p for every prime divisor p of b (with no restriction on i),
- has a balanced representation if and only if r is a root of -1 mod m,
- has a t-balanced representation for some t if and only if $r^2 \equiv 1$ mod m/b,
- has an anti-balanced representation if and only if $r^2 \equiv 1$ mod m.

Formulae for the numbers of such maps for C_n for given n were provided in Section 6.

Acknowledgments

The authors acknowledge the use of the Magma computational package [1], which not only led to the main result of [8], but also showed the way to many of the results given in this paper by helping the authors to construct, analyse and enumerate sufficiently many small examples that the authors were able to see patterns in their distribution. Also the first author is grateful for support from the N.Z. Marsden Fund (grant no. UOA1015).

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] Domenico A. Catalano, Marston D. E. Conder, Shao Fei Du, Young Soo Kwon, Roman Nedela, and Steve Wilson, *Classification of regular embeddings of n-dimensional cubes*, J. Algebraic Combin. **33** (2011), no. 2, 215–238, DOI 10.1007/s10801-010-0242-8. MR2765323 (2012b:57005)

[3] Marston D. E. Conder, *Regular maps and hypermaps of Euler characteristic* -1 *to* -200, J. Combin. Theory Ser. B **99** (2009), no. 2, 455–459, DOI 10.1016/j.jctb.2008.09.003. MR2482963 (2010b:05084)

[4] Marston Conder and Peter Dobcsányi, *Determination of all regular maps of small genus*, J. Combin. Theory Ser. B **81** (2001), no. 2, 224–242, DOI 10.1006/jctb.2000.2008. MR1814906 (2002f:05088)

[5] M. D. E. Conder and I. M. Isaacs, *Derived subgroups of products of an abelian and a cyclic subgroup*, J. London Math. Soc. (2) **69** (2004), no. 2, 333–348, DOI 10.1112/S0024610703005027. MR2040608 (2005e:20030)

[6] Marston Conder, Robert Jajcay, and Thomas Tucker, *Regular Cayley maps for finite abelian groups*, J. Algebraic Combin. **25** (2007), no. 3, 259–283, DOI 10.1007/s10801-006-0037-0. MR2317333 (2008d:05069)

[7] Marston Conder, Robert Jajcay, and Tom Tucker, *Regular t-balanced Cayley maps*, J. Combin. Theory Ser. B **97** (2007), no. 3, 453–473, DOI 10.1016/j.jctb.2006.07.008. MR2305898 (2007k:05086)

[8] Marston D. E. Conder, Young Soo Kwon, and Jozef Širáň, *Reflexibility of regular Cayley maps for abelian groups*, J. Combin. Theory Ser. B **99** (2009), no. 1, 254–260, DOI 10.1016/j.jctb.2008.07.002. MR2467830 (2009k:05192)

[9] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular hypermaps over projective linear groups*, J. Aust. Math. Soc. **85** (2008), no. 2, 155–175, DOI 10.1017/S1446788708000827. MR2470535 (2010f:57005)

[10] Marston D. E. Conder, Jozef Širáň, and Thomas W. Tucker, *The genera, reflexibility and simplicity of regular maps*, J. Eur. Math. Soc. (JEMS) **12** (2010), no. 2, 343–364, DOI 10.4171/JEMS/200. MR2608943 (2011i:05092)

[11] Jonathan L. Gross and Thomas W. Tucker, *Topological graph theory*, Dover Publications Inc., Mineola, NY, 2001. Reprint of the 1987 original [Wiley, New York; MR0898434 (88h:05034)] with a new preface and supplementary bibliography. MR1855951

[12] Noboru Itô, *Über das Produkt von zwei abelschen Gruppen* (German), Math. Z. **62** (1955), 400–401. MR0071426 (17,125b)

[13] Robert Jajcay, *Characterization and construction of Cayley graphs admitting regular Cayley maps*, Discrete Math. **158** (1996), no. 1-3, 151–160, DOI 10.1016/0012-365X(95)00076-9. MR1411114 (97d:05141)

[14] Robert Jajcay and Jozef Širáň, *Skew-morphisms of regular Cayley maps*, Discrete Math. **244** (2002), no. 1-3, 167–179, DOI 10.1016/S0012-365X(01)00081-4. Algebraic and topological methods in graph theory (Lake Bled, 1999). MR1844030 (2003b:05079)

[15] Lynne D. James and Gareth A. Jones, *Regular orientable imbeddings of complete graphs*, J. Combin. Theory Ser. B **39** (1985), no. 3, 353–367, DOI 10.1016/0095-8956(85)90060-7. MR815402 (87a:05060)

[16] Gareth A. Jones, *Regular embeddings of complete bipartite graphs: classification and enumeration*, Proc. Lond. Math. Soc. (3) **101** (2010), no. 2, 427–453, DOI 10.1112/plms/pdp061. MR2679697 (2011g:05072)

[17] István Kovács, *Classifying arc-transitive circulants*, J. Algebraic Combin. **20** (2004), no. 3, 353–358, DOI 10.1023/B:JACO.0000048519.27295.3b. MR2106966 (2005g:05068)

[18] I. Kovács, D. Marušič and M. Muzychuk, Regular Cayley maps for dihedral groups of twice odd order, preprint.

[19] Jin Ho Kwak, Young Soo Kwon, and Rongquan Feng, *A classification of regular t-balanced Cayley maps on dihedral groups*, European J. Combin. **27** (2006), no. 3, 382–393, DOI 10.1016/j.ejc.2004.12.002. MR2206474 (2007a:05058)

[20] Jin Ho Kwak and Ju-Mok Oh, *A classification of regular t-balanced Cayley maps on dicyclic groups*, European J. Combin. **29** (2008), no. 5, 1151–1159, DOI 10.1016/j.ejc.2007.06.023. MR2419219 (2009f:05122)

[21] Young Soo Kwon, *A classification of regular t-balanced Cayley maps for cyclic groups*, Discrete Math. **313** (2013), no. 5, 656–664, DOI 10.1016/j.disc.2012.12.012. MR3009432

[22] Cai Heng Li, *Permutation groups with a cyclic regular subgroup and arc transitive circulants*, J. Algebraic Combin. **21** (2005), no. 2, 131–136, DOI 10.1007/s10801-005-6903-3. MR2142403 (2006b:20002)

[23] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, 5th ed., John Wiley & Sons Inc., New York, 1991. MR1083765 (91i:11001)

[24] Ju-Mok Oh, *Regular t-balanced Cayley maps on semi-dihedral groups*, J. Combin. Theory Ser. B **99** (2009), no. 2, 480–493, DOI 10.1016/j.jctb.2008.09.006. MR2482966 (2010d:05074)

[25] Jozef Širáň and Thomas W. Tucker, *Symmetric maps*, Topics in topological graph theory, Encyclopedia Math. Appl., vol. 128, Cambridge Univ. Press, Cambridge, 2009, pp. 199–224. MR2581547

[26] Yan Wang and Rong Quan Feng, *Regular balanced Cayley maps for cyclic, dihedral and generalized quaternion groups*, Acta Math. Sin. (Engl. Ser.) **21** (2005), no. 4, 773–778, DOI 10.1007/s10114-004-0455-7. MR2156952 (2006c:05075)

Department of Mathematics, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

Department of Mathematics, Colgate University, Hamilton, New York 13346