J Algebr Comb (2011) 33: 215–238
DOI 10.1007/s10801-010-0242-8

Classification of regular embeddings of n-dimensional cubes

Domenico A. Catalano · Marston D.E. Conder · Shao Fei Du · Young Soo Kwon · Roman Nedela · Steve Wilson

Received: 25 October 2009 / Accepted: 14 June 2010 / Published online: 9 July 2010

Abstract An orientably-regular map is a 2-cell embedding of a connected graph or multigraph into an orientable surface, such that the group of all orientation-preserving automorphisms of the embedding has a single orbit on the set of all arcs (incident vertex-edge pairs). Such embeddings of the n-dimensional cubes Q_n were classified for all odd n by Du, Kwak and Nedela in 2005, and in 2007, Jing Xu proved that for $n = 2m$ where m is odd, they are precisely the embeddings constructed by Kwon in 2004. Here, we give a classification of orientably-regular embeddings of Q_n for all n. In particular, we show that for all even n $(= 2m)$, these embeddings are in one-to-one correspondence with elements σ of order 1 or 2 in the symmetric group S_n such that σ fixes n, preserves the set of all pairs $B_i = \{i, i + m\}$ for $1 \le i \le m$, and induces

D.A. Catalano
Departamento de Matemática, Universidade de Aveiro, 3810-193 Aveiro, Portugal
e-mail: domenico@ua.pt

M.D.E. Conder (✉)
Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand
e-mail: m.conder@auckland.ac.nz

S.F. Du
School of Mathematical Sciences, Capital Normal University, Beijing 100048, China
e-mail: dushf@mail.cnu.edu.cn

Y.S. Kwon
Department of Mathematics, Yeungnam University, Kyongsan 712-749, Republic of Korea
e-mail: ysookwon@ynu.ac.kr

R. Nedela
Mathematical Institute, Slovak Academy of Sciences, 975 49 Banská Bystrica, Slovakia
e-mail: nedela@savbb.sk

S. Wilson
Department of Mathematics and Statistics, Northern Arizona University, Flagstaff, AZ 86011, USA
e-mail: Stephen.Wilson@nau.edu

the same permutation on this set as the permutation $B_i \mapsto B_{f(i)}$ for some additive bijection $f : \mathbb{Z}_m \to \mathbb{Z}_m$. We also give formulae for the numbers of embeddings that are reflexible and chiral, respectively, showing that the ratio of reflexible to chiral embeddings tends to zero for large even n.

Keywords Hypercubes · Cubes · Regular maps · Regular embeddings · Chiral

1 Introduction

A (topological) *map* is a cellular decomposition of a closed surface. A common way to describe such a map is to view it as a 2-cell embedding of a connected graph or multigraph X into the surface S. The components of the complement $S \setminus X$ are simply-connected regions called the *faces* of the map (or the embedding).

An *automorphism* of a map $M = (X, S)$ is an automorphism of the underlying (multi)graph X which extends to a self-homeomorphism of the supporting surface S. It is well known that the automorphism group of a map acts semi-regularly on the set of all incident vertex-edge-face triples (sometimes called the *flags* of M); in other words, every automorphism is uniquely determined by its effect on a given flag.

If for any given flag (v, e, f) the automorphism group contains two automorphisms that induce (respectively) a single cycle on the edges incident with v and a single cycle on the edges incident with f, then the map M is called *rotary*. In the orientable case, this condition implies that the group of all orientation-preserving automorphisms of M acts regularly on the set of all incident vertex-edge pairs (or *arcs*) of M, and we call M an *orientably-regular* map. Such maps fall into two classes: those that admit also orientation-reversing automorphisms, which are called *reflexible*, and those that do not, which are *chiral*. In the non-orientable case (and in the reflexible case), the automorphism group acts regularly on flags, while in the chiral case, there are two orbits on flags, such that the two flags associated with each arc lie in different orbits.

A *regular embedding* (or more technically, a *rotary embedding*) of a graph X is then a 2-cell embedding of X as a rotary map on some closed surface.

Classification of rotary maps by their underlying graphs is one of the central problems in topological graph theory. An abstract characterization of graphs having regular embeddings was given by Gardiner et al. in [12]. The classification problem has been solved only for few families of graphs, including the complete graphs [1, 13, 14], their canonical double covers [23], and complete multipartite graphs $K_{p,p,\dots,p}$ for prime p [8, 10]. Particular contributions towards the classification of regular embeddings of complete bipartite graphs $K_{n,n}$ can be found in papers [6, 7, 16, 17, 19, 20, 26], and this classification was recently completed by Gareth Jones [15]. In this paper we focus on the classification of regular embeddings of n-dimensional cubes Q_n.

The existence of at least two different regular embeddings of Q_n for each $n > 2$ has been known for some time: in [24], Nedela and Škoviera constructed a regular embedding of Q_n for every solution e of the congruence $e^2 \equiv 1 \bmod n$, with different solutions giving rise to non-isomorphic maps. Later, Du, Kwak and Nedela [9] proved that there are no other regular embeddings of Q_n into orientable surfaces when n is odd. In contrast, Kwon [21] constructed new regular embeddings for all even $n \geqslant 6$, by applying a 'switch' operator (as defined in [25]); he thereby also derived an exponential lower bound in terms of n for the number of non-isomorphic regular embeddings of Q_n.

Recently, Jing Xu [28] proved that the embeddings constructed by Kwon cover all regular embeddings of Q_n into orientable surfaces, when $n = 2m$ for odd m. In [22], Kwon and Nedela proved that there are no regular embeddings of Q_n into *non-orientable* surfaces, for all $n > 2$. Also recently, the first and fifth authors of this paper gave a characterization of all orientably-regular embeddings of Q_n (in terms of certain 'quadrilateral identities'), and a construction for new regular embeddings of Q_n for all n divisible by 16, not covered by the family of embeddings found by Kwon; see [3].

The aim of the present paper is to classify the regular embeddings of Q_n for all n. By [22], these are orientable for $n > 2$, and by [9] they are known for all odd n, so we concentrate on the case where n is even, say $n = 2m$.

In our main theorem (Theorem 5.1), we will show that when $n = 2m$ the orientably-regular embeddings are in one-to-one correspondence with elements σ of order 1 or 2 in the symmetric group S_n such that σ fixes n, preserves the set of all pairs $B_i = \{i, i+m\}$ for $1 \le i \le m$, and induces the same permutation on this set as the permutation $B_i \mapsto B_{f(i)}$ for some additive bijection $f : \mathbb{Z}_m \to \mathbb{Z}_m$. (Note: by *additive*, we mean that $f(i+j) \equiv f(i) + f(j) \bmod m$ for all $i, j \in \mathbb{Z}_m$; and since σ^2 is trivial, this is equivalent to f being given by $f : i \mapsto ei$ for some square root e of 1 in $\mathbb{Z}_m$ (namely $e = f(1)$).) In particular, it follows that every regular embedding of Q_n belongs to one of the families constructed by Kwon [21] and Catalano and Nedela [3]. This also gives rise to formulae for the numbers of embeddings that are reflexible and chiral, respectively, which show that the ratio of reflexible to chiral embeddings tends to zero for large even n.

Before proving our main theorem in Sect. 5, we give some further background in Sects. 2 and 3, and introduce a reduction process in Sect. 4. Reflexibility and the enumeration formulae are then considered in Sect. 6, and the genera and other properties of the resulting maps are dealt with in Sect. 7.

2 Further background

Let M be an orientably-regular map, and let $G = \mathrm{Aut}^{\mathrm{o}}(M)$ be the group of all orientation-preserving automorphisms of M. Then G acts transitively on vertices, on edges, and on faces of M; in particular, every face has the same size k, say, and every vertex has the same degree (valency) m, say. The pair $\{k, m\}$ is then called the *type* of the map M.

Moreover, for any given flag (v, e, f) of M, there exists an automorphism R in G inducing a single-step rotation of the edges incident with f, and an automorphism S in G inducing a single-step rotation of the edges incident with v, with product RS an involutory automorphism that reverses the edge e. By connectedness, R and S generate G, which is therefore a quotient of the ordinary $(k, m, 2)$ *triangle group*

$\Delta^{o}(k,m,2) = \langle x, y \mid x^k = y^m = (xy)^2 = 1\rangle$ (under an epimorphism taking x to R and y to S). The map M is reflexible if and only if the group G admits an automorphism of order 2 taking R to R^{-1} and S to S^{-1}, or equivalently (by conjugation), an automorphism of order 2 taking S to S^{-1} and RS to $S^{-1}R^{-1} = (RS)^{-1} = RS$.

Conversely, given any epimorphism θ from $\Delta^{o}(k,m,2)$ to a finite group G with torsion-free kernel, a map M can be constructed using (right) cosets of the images of $\langle x\rangle$, $\langle y\rangle$ and $\langle xy\rangle$ as vertices, faces and edges, with incidence given by non-empty intersection, and then G acts regularly on the arcs of M by (right) multiplication. From this point of view the study of regular maps is simply the study of smooth finite quotients of triangle groups, with 'smooth' here meaning that the orders of the elements x, y and xy are preserved.

An isomorphism between maps is an isomorphism between their underlying graphs that preserves oriented faces. Isomorphic regular maps have the same type, and therefore come from the same triangle group; in fact, two orientably-regular maps of the same type $\{k,m\}$ are isomorphic if and only if they are obtainable from the same torsion-free normal subgroup of $\Delta^{o}(k,m,2)$.

Rotary maps can be classified according to the genus or the Euler characteristic of the supporting surface, or by the underlying graph, or by the automorphism group of the map. Deep connections exist between maps and other branches of mathematics, which go far beyond group theory, and include hyperbolic geometry, Riemann surfaces and, rather surprisingly, number fields and Galois theory, based on observations made by Belyĭ and Grothendieck; see [18] for example.

The correspondence between rotary maps and normal subgroups of finite index in triangle groups has been exploited to develop the theory of such maps and produce or classify many families of examples. In particular, it was used by Conder and Dobcsányi in [5] to determine all rotary maps of Euler characteristic -1 to -28 inclusive, and subsequently extended by Conder in [4] for characteristic -1 to -200.

Now we turn to the cube graphs Q_n. For each integer $n > 1$, the *n-dimensional cube* graph Q_n is the graph on vertex-set $V = \mathbb{Z}_2{}^n$, with two vertices $u, v \in V$ adjacent if and only if the Hamming distance $d(u,v)$ between them is 1 (that is, if and only if u and v differ in exactly one coordinate position).

The automorphism group of Q_n is well known to be the wreath product $\mathbb{Z}_2 \wr S_n$, which is a semi-direct product $\mathbb{Z}_2{}^n \rtimes S_n$ of $V = \mathbb{Z}_2{}^n$ by the symmetric group S_n. In particular, we may view any element of $\mathrm{Aut}(Q_n)$ as a product of some $v \in V$ with a permutation $\pi \in S_n$, and multiplication follows from the rule $v\pi = \pi v^{\pi}$ where v^{π} denotes the vector in V obtained from v by applying the permutation π to the coordinates of v.

In any orientably-regular embedding of Q_n, we may choose the rotation S about the vertex $v = 0$ to be the n-cycle $\rho = (1,2,3,\dots,n)$ in S_n, and then choose the rotation R about a face f incident with v so that RS is the involution $e_n\sigma$, where $e_n = (0,0,\dots,0,1)$ is the nth standard basis vector for V, and σ is a permutation of order 1 or 2 in S_n fixing n. This is explained further in [21], where e_0 is used in place of e_n for the purposes of consistency with taking residues modulo n.

For any such permutation σ (of order 1 or 2 and fixing n) in S_n, let $G(\sigma) = \langle \rho, e_n\sigma\rangle$. By [21, Lemma 3.1], this subgroup of $\mathrm{Aut}(Q_n)$ acts transitively on the arcs of Q_n. Next, if $G(\sigma)$ acts regularly on the arcs of Q_n, so that $|G(\sigma)| = n2^n$, then we call the permutation σ an *admissible involution* (allowing an 'involution' to have order 1), and we denote the corresponding regular embedding by $\mathcal{M}(\sigma)$. In particular, the identity permutation ι is an admissible involution in S_n, giving the *standard embedding* $\mathcal{M}(\iota)$.

We can now state the following theorem.

Theorem 2.1 (Kwon [21, Theorem 3.1]) *Every regular embedding of Q_n is isomorphic to $\mathcal{M}(\sigma)$ for some admissible involution $\sigma \in S_n$. Moreover, for any admissible involutions $\sigma_1, \sigma_2 \in S_n$, the maps $\mathcal{M}(\sigma_1)$ and $\mathcal{M}(\sigma_2)$ are isomorphic if and only if $\sigma_1 = \sigma_2$.*

Hence the classification of regular embeddings of Q_n is equivalent to the classification of admissible involutions σ in S_n. We remark that for $n = 2$ the standard embedding is the only regular orientable embedding of Q_2, and so from now on, we suppose $n > 2$.

For some time it has been known (see [24], for example) that for every square root e of 1 in $\mathbb{Z}_n$, the mapping $\tau_e : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\tau_e : i \mapsto ei$ (multiplication by e) gives rise to an admissible involution in S_n (when we think of 0 as n).

The classification of regular embeddings of Q_n for n odd was achieved by proving the following:

Theorem 2.2 (Du, Kwak & Nedela [9]) *If n is odd and $\sigma \in S_n$ is an admissible involution, then $\sigma = \tau_e$ for some e satisfying $e^2 \equiv 1 \bmod n$.*

In this paper we focus attention on the even-dimensional case. In this case, the following partial results are known:

Theorem 2.3 (Kwon [21, Theorems 4.1 & 5.2)] *For $n = 2m$ (even), let e be a square root of 1 in $\mathbb{Z}_n$, and let χ_A be the characteristic function of a subset $A \subseteq \mathbb{Z}_n \setminus \{0\}$ preserved by $\langle \tau_e, \rho^m \rangle$, where $\rho = (1, 2, \dots, n)$. Then the mapping $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ given by*

$$\sigma : i \mapsto ei + m\chi_A(i) \tag{K}$$

gives an admissible involution in S_n.

Theorem 2.4 (Catalano & Nedela [3, Theorem 5.3]) *For $n = 2m$ where m is divisible by 8, let e be a square root of $m + 1$ in $\mathbb{Z}_n$, and let χ_A be the characteristic function of a subset $A \subseteq \mathbb{Z}_n \setminus \{0\}$ such that $\chi_A(i + m) = \chi_A(i)$ and $\chi_A(ei) \equiv \chi_A(i) + i \bmod 2$ for all $i \in \mathbb{Z}_n$. Then the mapping $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ given by*

$$\sigma : i \mapsto ei + m\chi_A(i) \tag{CN}$$

is an admissible involution.

Admissible involutions defined by (K) and (CN) may be called *K-involutions* and *CN-involutions*, respectively. Jing Xu extended the classification for n odd to the case $n = 2m$ where m is odd, by proving the following:

Theorem 2.5 (Xu [28]) *Let $n = 2m$ where m is odd. Then an involution σ in S_n fixing n is admissible if and only if it is a K-involution.*

One may observe that any K- or CN-involution commutes with ρ^m, when $n = 2m$. In fact, this holds for any admissible involution:

Proposition 2.6 *Let H be a permutation group of even degree $2m$ containing a regular element y (acting as a $2m$-cycle), such that the stabilizer of each point is a 2-group. Then y^m is central in H, so the m orbits of $\langle y^m\rangle$ form a system of imprimitivity for H.*

Proof We prove this by induction on m. If $m = 1$ then the result is trivial. Now suppose $m > 1$. The lengths of orbits of a point-stabilizer H_α are powers of 2, so the fixed point set P of H_α must have even size. If $|P| = 2m$, then $H = \langle y\rangle$ and the result is immediate. If not, then P is a block of imprimitivity for H, and the action of the setwise stabilizer $H_{\{P\}}$ on P satisfies the hypotheses, with $y^{2m/|P|}$ acting regularly, so that by induction, we may assume that y^m is central in $H_{\{P\}}$ and that the orbits of $\langle y^m\rangle$ on P form a system of imprimitivity for $H_{\{P\}}$. It then follows that the translates of those orbits form a system of imprimitivity for H. As y^m induces a 2-cycle on each such block, y^m is central in H. □

Corollary 2.7 *If σ is any admissible involution in S_{2m}, then σ commutes with ρ^m, and the orbits $\{i, i+m\}$ of $\langle\rho^m\rangle$ form a system of imprimitivity for $\langle\rho, \sigma\rangle$.*

3 Some technical observations

Let $\{e_1, e_2, \dots, e_n\}$ be the standard orthonormal basis for $V = \mathbb{Z}_2{}^n$, and for any subset J of $\{1, 2, \dots, n\}$, let e_J be the characteristic vector of J (so that $e_{\{i\}} = e_i$ for all i). Then multiplication in $\mathbb{Z}_2 \wr S_n \cong V \rtimes S_n$ is given by

$$(e_J\pi)(e_K\mu) = e_L\pi\mu \quad \text{for } J, K \subseteq \{1, 2, \dots, n\} \text{ and } \pi, \mu \in S_n,$$

where L is the symmetric difference of J and $K^{\pi^{-1}}$.

Now suppose σ is an admissible involution in S_n, so $G(\sigma) = \langle\rho, e_n\sigma\rangle$ has order $n2^n$. For $1 \le i \le n$, conjugating $e_n\sigma$ by powers of ρ gives $\rho^{-i}(e_n\sigma)\rho^i = e_i(\rho^{-i}\sigma\rho^i)$ as an element of $G(\sigma)$, and the above multiplication then gives elements in $G(\sigma)$ of the form $e_L\theta$ for every subset L of $\{1, 2, \dots, n\}$. Furthermore, post-multiplication by powers of ρ gives at least n possibilities for the element θ in S_n, for each subset L. In fact since $|G(\sigma)| = n2^n$, we have the following:

Lemma 3.1 *If σ is an admissible involution in S_n, then for each $L \subseteq \{1, 2, \dots, n\}$, the set of all elements of $G(\sigma)$ of the form $e_L\pi$ for $\pi \in S_n$ is a left coset of $\langle\rho\rangle$, of size n.*

In particular, for each $i \in \{1, 2, \dots, n\}$ there is a unique permutation $\gamma_i \in S_n$ fixing n such that $e_i\gamma_i \in G(\sigma)$. Clearly $\gamma_n = \sigma$, and more generally, since $G(\sigma)$ contains $\rho^{-i}(e_n\sigma)\rho^i = e_i(\rho^{-i}\sigma\rho^i)$, we find that $\gamma_i = \rho^{-i}\sigma\rho^{-(-i)^\sigma}$ for $1 \le i \le n$.

This leads to an alternative proof of the *quadrilateral identities* given in [3], involving the permutation τ in S_n induced by multiplication by -1 in $\mathbb{Z}_n$:

Proposition 3.2 *If σ is an admissible involution in S_n, then*

$$\sigma\rho^j\sigma\rho^{j^{\sigma\tau}}\sigma\rho^{j^{(\sigma\tau)^2}}\sigma\rho^{j^{(\sigma\tau)^3}} = 1 \quad \textit{for all } j \in \mathbb{Z}_n. \tag{$*$}$$

Proof First note that if $i \in \{1, 2, \dots, n\}$ and $i^{\gamma_n} = i^\sigma = \ell$ then

$$(e_i\gamma_i)(e_n\gamma_n) = e_ie_n\gamma_i\gamma_n \quad \text{while } (e_n\gamma_n)(e_\ell\gamma_\ell) = e_ne_i\gamma_n\gamma_\ell.$$

But $e_ie_n = e_ne_i$ since V is Abelian, and $\gamma_i\gamma_n$ and $\gamma_n\gamma_\ell$ both fix n, so we deduce that

$$\gamma_i\gamma_n = \gamma_n\gamma_\ell \quad \text{whenever } \ell = i^\sigma.$$

Now $\gamma_i\gamma_n = \rho^{-i}\sigma\rho^{-(-i)^\sigma}\sigma$ while $\gamma_n\gamma_\ell = \sigma\rho^{-\ell}\sigma\rho^{-(-\ell)^\sigma} = \sigma\rho^{-i^\sigma}\sigma\rho^{-(-i^\sigma)^\sigma}$, and hence

$$1 = (\gamma_i\gamma_n)^{-1}\gamma_n\gamma_\ell = \big(\sigma\rho^{(-i)^\sigma}\sigma\rho^i\big)\big(\sigma\rho^{-i^\sigma}\sigma\rho^{-(-i^\sigma)^\sigma}\big) = \sigma\rho^{i^{\tau\sigma}}\sigma\rho^i\sigma\rho^{i^{\sigma\tau}}\sigma\rho^{i^{(\sigma\tau)^2}}.$$

Taking $i = j^{\sigma\tau}$ (or, equivalently, $j = i^{\tau\sigma}$) gives the required identity. □

Corollary 3.3 *If σ is an admissible involution in S_n, then $(\sigma\tau)^4 = 1$.*

Proof Take $j = k^{\sigma\tau}$ in the above identity, to obtain $\sigma\rho^{k^{\sigma\tau}}\sigma\rho^{k^{(\sigma\tau)^2}}\sigma\rho^{k^{(\sigma\tau)^3}}\sigma\rho^{k^{(\sigma\tau)^4}} = 1$, and put this together with $\sigma\rho^k\sigma\rho^{k^{\sigma\tau}}\sigma\rho^{k^{(\sigma\tau)^2}}\sigma\rho^{k^{(\sigma\tau)^3}} = 1$, to give $\rho^{k^{(\sigma\tau)^4}} = \rho^k$ for all k. □

The converse of Proposition 3.2 holds as well. This was shown in [3], but again we give an alternative proof (below).

Proposition 3.4 *If σ is an involution in S_n that fixes n and satisfies the quadrilateral identities* ($*$), *then σ is admissible.*

Proof We prove that $G(\sigma) = \langle\rho, e_n\sigma\rangle$ has order $n2^n$, by showing it contains a unique left coset of the form $e_L\gamma_L\langle\rho\rangle$ with $\gamma_L \in S_n$ fixing n, for every $L \subseteq \{1, 2, \dots, n\}$.

Define $\gamma_i = \rho^{-i}\sigma\rho^{-(-i)^\sigma}$ for $1 \le i \le n$, as previously. Then each γ_i is an element of S_n fixing n such that $e_i\gamma_i = \rho^{-i}(e_n\sigma)\rho^i\rho^{-(-i)^\sigma-i}$ lies in $G(\sigma)$. Moreover, since $G(\sigma) = \langle\rho, e_n\sigma\rangle$, every element w of $G(\sigma)$ can be expressed as a product of conjugates of $e_n\sigma$ by powers of ρ, followed by some power of ρ, and hence has the form $w = e_{i_1}\gamma_{i_1}e_{i_2}\gamma_{i_2}\cdots e_{i_r}\gamma_{i_r}\rho^s$ for some $i_1, i_2, \dots, i_r$ and s. The multiplication rule

$$(e_a\gamma_a)(e_b\gamma_b) = (e_ae_c)\gamma_a\gamma_b \quad \text{whenever } b = c^{\gamma_a}$$

can then be used to rewrite w in the form $w = e_L\gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_r}\rho^s$ for some $L \subseteq \{1, 2, \dots, n\}$.

The quadrilateral identities $(*)$ imply that for given L, the element $\gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_r}$ is uniquely determined.

To see this, note that if $b = c^{\gamma_a}$ and $d = a^{\gamma_c}$, then the above multiplication rule gives $(e_a\gamma_a)(e_b\gamma_b) = (e_a e_c)\gamma_a\gamma_b$ while $(e_c\gamma_c)(e_d\gamma_d) = (e_c e_a)\gamma_c\gamma_d$. Since $e_a e_c = e_c e_a$, all we have to do is to prove that $\gamma_a\gamma_b = \gamma_c\gamma_d$ whenever $b = c^{\gamma_a} = c^{\rho^{-a}\sigma\rho^{-(-a)^\sigma}} = (c-a)^\sigma - (-a)^\sigma$ and $d = a^{\gamma_c} = a^{\rho^{-c}\sigma\rho^{-(-c)^\sigma}} = (a-c)^\sigma - (-c)^\sigma$. The quadrilateral identity for $j = (a-c)^\sigma$ is

$$1 = \sigma\rho^{(a-c)^\sigma}\sigma\rho^{c-a}\sigma\rho^{(c-a)^{\sigma\tau}}\sigma\rho^{(c-a)^{(\sigma\tau)^2}},$$

which can be rewritten as $1 = \sigma\rho^{d+(-c)^\sigma}\sigma\rho^{c-a}\sigma\rho^{-(-a)^\sigma-b}\sigma\rho^{(c-a)^{(\sigma\tau)^2}}$. Upon conjugation this becomes

$$1 = \rho^{-a}\sigma\rho^{-(-a)^\sigma-b}\sigma\rho^{(c-a)^{(\sigma\tau)^2}}\sigma\rho^{d+(-c)^\sigma}\sigma\rho^{c},$$

which can be rewritten as $1 = \gamma_a\gamma_b\rho^u\gamma_d^{-1}\gamma_c^{-1}$ where $u = (-b)^\sigma + (c-a)^{(\sigma\tau)^2} - (-d)^\sigma$. Thus $(\gamma_a\gamma_b)^{-1}\gamma_c\gamma_d = \rho^u$, and as the left-hand side of this identity fixes n, we find $\rho^u = 1$, so $(\gamma_a\gamma_b)^{-1}\gamma_c\gamma_d = 1$ and therefore $\gamma_a\gamma_b = \gamma_c\gamma_d$, as required. □

Corollary 3.5 *Let σ be any involution in S_{2m} such that σ fixes $n = 2m$, preserves the set of all pairs $B_i = \{i, i+m\}$ for $1 \le i \le m$, and induces the same permutation on this set as the permutation $B_i \mapsto B_{f(i)}$ for some additive bijection $f : \mathbb{Z}_m \to \mathbb{Z}_m$. Then σ is admissible.*

Proof It is an easy exercise to verify that σ satisfies the quadrilateral identities $(*)$. □

Note that the condition that σ preserves the set $\{B_i : 1 \le i \le m\}$ is equivalent to σ commuting with $\rho^m = (1, m+1)(2, m+2)\cdots(m, 2m)$.

4 Reduction

In this section we describe a reduction from the case of Q_n to the case of Q_m when $n = 2m$ (even). This can be used to provide an alternative proof of Theorem 2.5, as well as assist with the proof of our main theorem in the next section. To do this, we consider the natural action of the wreath product $\mathbb{Z}_2 \wr S_n$ on the set $\{1, 2, \ldots, 2n\}$, with block-set $\{\{i, i+n\} : 1 \le i \le n\}$ preserved by $V = {\mathbb{Z}_2}^n$ and permuted by S_n. Indeed let e_i induce the transposition $(i, i+n)$ for $1 \le i \le n$, and let ρ induce the permutation $(1, 2, \ldots, n)(n+1, n+2, \ldots, 2n)$.

Lemma 4.1 *Suppose $n = 2m$, and σ is an admissible involution in S_n. Let K be the subgroup of $\mathbb{Z}_2 \wr S_n$ generated by ρ^m and $e_i e_{i+m}$ for $1 \le i \le m$. Then K is an Abelian subgroup of $G(\sigma)$, of order 2^{m+1}. Moreover, K is a normal subgroup of $G(\sigma)$, and consists of all elements that preserve each of the sets $P_i = \{\{i, i+m\}, \{i+2m, i+3m\}\}$ (and each of the sets $Q_i = \{\{i, i+3m\}, \{i+2m, i+m\}\}$), for $1 \le i \le m$.*

Proof First, let $G = G(\sigma)$, and let $\gamma_j = \rho^{-j}\sigma\rho^{-(-j)^\sigma}$ be the elements defined in Sect. 3. By Corollary 2.7, we know that σ permutes the sets $B_i = \{i, i+m\}$ among themselves, and hence that $(i+m)^\sigma = i^\sigma + m \pmod n$ for all i. Then since ρ^m commutes with σ, we find that

$$\begin{aligned}\gamma_{i+m} &= \rho^{-(i+m)}\sigma\rho^{-(-(i+m))^\sigma} = \rho^{-i}\rho^{-m}\sigma\rho^m\rho^{-(-i)^\sigma}\\ &= \rho^{-i}\sigma\rho^{-(-i)^\sigma} = \gamma_i \quad \text{for } 1 \le i \le m.\end{aligned}$$

In particular, as G contains $e_i\gamma_i$ and $e_{i+m}\gamma_{i+m} = e_{i+m}\gamma_i$, it follows that G contains $(e_i\gamma_i)(e_{i+m}\gamma_i)^{-1} = e_ie_{i+m}$ for all i, so K is a subgroup of G. Also the generators of K are commuting involutions, so K is Abelian, of order 2^{m+1}.

Observe that both ρ and σ centralize ρ^m and conjugate the e_ie_{i+m} among themselves, while e_n centralizes all the e_ie_{i+m} and conjugates ρ^m to $e_me_{2m}\rho^m$. It follows that K is normalized by each of ρ, σ and e_n, and in particular, K is normal in $\langle \rho, e_n\sigma\rangle = G$.

Next, let H be the stabilizer in G of the two points m and $2m$ (or equivalently, of the four points $m, 2m, 3m$ and $4m$). Since the stabilizer in G of m fixes $3m$ and has $\{2m, 4m\}$ as one of its orbits, and has index $2n = 4m$ in G, this subgroup H has index $4n$ in G, so has order 2^{n-2}. Now consider the subgroup HK. The intersection $H \cap K$ contains all the e_ie_{i+m} for $i \ne m, 2m$, but does not contain e_me_{2m}, ρ^m or $e_me_{2m}\rho^m$ (which take m to $3m, 2m$ and $4m$ respectively), so $H \cap K$ has index 4 in K and therefore has order 2^{m-1}. Thus $|HK| = |H||K|/|H \cap K| = 2^{n-2+m+1}/2^{m-1} = 2^n$, so the index of HK in G is $n = 2m$. It follows that HK is the stabilizer in G of the set $P_m = \{\{m, 2m\}, \{3m, 4m\}\}$, the images of which under other elements of G are the sets P_i and Q_i given in the statement of this Lemma. Moreover, the core of H in G is trivial (being the stabilizer of all points), so the core of HK in G is K. This completes the proof. □

The above lemma gives a quotient $G(\sigma)/K$ that acts transitively on a set of size $2m$, namely the set of all P_i and Q_i. The permutation induced by ρ is a pair of m-cycles, namely $(P_1, P_2, \dots, P_m)$ and $(Q_1, Q_2, \dots, Q_m)$. But also the generators e_i of $V = \mathbb{Z}_2{}^n$ and the involution σ induce permutations of this set, with each e_i interchanging the points P_i and Q_i while fixing all others, and σ inducing effectively the same permutation on the Q_i as it does on the P_i. In particular, since σ commutes with ρ^m, the orbits $\{P_i, P_{i+m}\}$ and $\{Q_i, Q_{i+m}\}$ of $\langle \rho^m\rangle$ form a system of imprimitivity for $G(\sigma)/K$, which accordingly can be viewed as a subgroup of the wreath product $\mathbb{Z}_2 \wr S_m$. Furthermore, we may note that σ fixes Q_m (and P_m), and hence that $e_n\sigma$ interchanges P_m and Q_m while otherwise acting to preserve the sets $\{P_1, P_2, \dots, P_{m-1}\}$ and $\{Q_1, Q_2, \dots, Q_{m-1}\}$.

In other words, K is the kernel of a reduction, from $G(\sigma)$ as a subgroup of $\mathbb{Z}_2 \wr S_n$, to $G(\sigma)/K$ which is a subgroup of $\mathbb{Z}_2 \wr S_m$ in its natural action on the P_i and Q_i (with $\{P_i, Q_i\}$ as the 'base pairs'). In particular, G/K has order $2^m m$, and is the group of orientation-preserving automorphisms of a regular embedding of Q_m.

In fact this permutation induced by σ is effectively the same as the one induced by σ on the blocks $B_i = \{i, i+m\}$ of the natural action of $\langle \rho, \sigma\rangle$ on $\{1, 2, \dots, n\}$. This gives another way of defining the reduction. As explained in [3], we may directly define the *projections* $\overline{\rho}$ and $\overline{\sigma}$ of ρ and σ in S_m by letting $i^{\overline{\rho}}$ and $i^{\overline{\sigma}}$ be the residues mod m of i^ρ and i^σ respectively, for $1 \le i \le m$. Then $\overline{\sigma}$ obviously satisfies the quadrilateral identities, and is therefore an admissible involution in S_m. Reciprocally, we may call σ an *admissible lift* of $\overline{\sigma}$. By the above remarks, we now have the following:

Proposition 4.2 *Every admissible involution $\sigma \in S_{2m}$ is an admissible lift of some admissible involution in S_m.*

Note that every K-involution and every CN-involution in S_{2m} is an admissible lift of the involution $\tau_e : \mathbb{Z}_m \to \mathbb{Z}_m$ given by multiplication by some square root e of 1 in $\mathbb{Z}_m$. This was observed in [3], where it was also proved that every admissible lift of such an involution τ_e in S_m is a K-involution or CN-involution in S_{2m}; see [3, Theorem 5.3].

We also now have the following:

Alternative proof of Theorem 2.5 For $n = 2m$ where m is odd, let σ be an admissible involution in S_n. By the above reduction, $\overline{\sigma}$ is an admissible involution in S_m, so by Theorem 2.2, we know that $\overline{\sigma} = \tau_e$ for some square root e of 1 in $\mathbb{Z}_m$. Now replace e by $e + m$ if e is even. Then $e^2 \equiv 1$ mod 2 and mod m, so $e^2 \equiv 1$ mod n. Taking $A = \{i \in \mathbb{Z}_n : i^\sigma \ne ei \pmod n\} = \{i \in \mathbb{Z}_n : i^\sigma = ei + m \pmod n\}$, we see that $0 \notin A$ and that A is preserved by both ρ^m and multiplication by e mod n, so σ is a K-involution. $\square$

5 Classification theorem

In this section, we give a characterization of all admissible involutions in S_{2m}, for every positive integer m. When taken together with Theorem 2.2, this gives a complete classification of all regular embeddings of hypercubes Q_n.

Theorem 5.1 *Let $n = 2m$ be an even positive integer, and let $\rho = (1, 2, 3, \ldots, n)$ in S_n. Then every regular embedding of Q_n is isomorphic to the embedding $\mathcal{M}(\sigma)$ for some permutation σ of order* 1 *or* 2 *in S_n and fixing n, such that*:

(1) *σ commutes with ρ^m, so that the sets $B_i = \{i, i+m\}$ (for $1 \le i \le m$) form a system of imprimitivity for $\langle \rho, \sigma \rangle$ on $\{1, 2, \ldots, n\}$, and*
(2) *σ permutes the blocks B_i in the same way as the permutation $B_i \mapsto B_{f(i)}$ for some additive bijection $f : \mathbb{Z}_m \to \mathbb{Z}_m$.*

Moreover, every such σ gives a regular embedding of Q_n, and distinct σ give non-isomorphic embeddings.

Part (1) follows from Corollary 2.7, and we will prove part (2) by induction on m. We have already seen that when m is odd, this follows from Theorem 2.5, so we suppose that m is even, say $m = 2k$, and let σ be any admissible involution in S_{2m}. By the reduction described in Sect. 4, we know that the action of σ on the blocks B_i is the same as that of an admissible involution $\overline{\sigma}$ in S_m, and now by induction, we may assume that the projection of $\overline{\sigma}$ in S_k is an additive bijection from $\mathbb{Z}_k$ to $\mathbb{Z}_k$.

Let $e = 1^\sigma$ if this is odd, or otherwise let $e = 1^\sigma + k$ (which will be odd, since k is odd when 1^σ is even). Then by additivity of the projection of $\overline{\sigma}$ in S_k, we can prove by induction that $i^\sigma \equiv ei \bmod k$ for all $i \in \mathbb{Z}_n$. Hence we may define a function $\psi : \mathbb{Z}_n \to \mathbb{Z}_4$ satisfying

$$i^\sigma = ei + k\psi(i) \quad \text{for all } i \in \mathbb{Z}_n.$$

The remainder of our proof will depend heavily on properties of this function ψ and related objects.

Lemma 5.2 *If $e \in \mathbb{Z}_n$ and $\psi : \mathbb{Z}_n \to \mathbb{Z}_4$ are defined as above, then*:

(a) $\psi(0) = \psi(m) = 0$, *and* $\psi(k)$ *and* $\psi(3k)$ *are both even*;
(b) $e^2 \equiv \delta k + 1 \bmod n$ *for some* $\delta \in \mathbb{Z}_4$;
(c) $\delta i + e\psi(i) + \psi(i^\sigma) \equiv 0 \bmod 4$, *for all* $i \in \mathbb{Z}_n$;
(d) $\psi(i + m) = \psi(i)$ *for all* $i \in \mathbb{Z}_n$;
(e) $\psi(i + k) \equiv \psi(i) \bmod 2$ *for all* $i \in \mathbb{Z}_n$.

Proof Parts (a) and (b) are obvious from the definitions. For part (c), observe that

$$i = \left(i^\sigma\right)^\sigma = ei^\sigma + k\psi\left(i^\sigma\right) = e\left(ei + k\psi(i)\right) + k\psi\left(i^\sigma\right) = i + k\left(\delta i + e\psi(i) + \psi\left(i^\sigma\right)\right)$$

in $\mathbb{Z}_n$, since $e^2 = 1 + k\delta$ by part (b). Part (d) is a consequence of the fact that σ commutes with ρ^m:

$$\begin{aligned} 0 &= (i+m)^\sigma - \left(i^\sigma + m\right) = em + k\left(\psi(i+m) - \psi(i)\right) - m \\ &= k\left(\psi(i+m) - \psi(i)\right). \end{aligned}$$

Similarly, $(i + k)^\sigma - i^\sigma = ek + k(\psi(i + k) - \psi(i)) = k(e + \psi(i + k) - \psi(i))$, and since the left-hand side is either k or $3k (\mathrm{mod}\ n)$, and e is odd, we obtain part (e). □

We wish to prove that σ is additive when reduced modulo m. Now since

$$\begin{aligned} (i+j)^\sigma - i^\sigma - j^\sigma &= e(i+j) + k\psi(i+j) - ei - k\psi(i) - ej - k\psi(j) \\ &= k\left(\psi(i+j) - \psi(i) - \psi(j)\right) \end{aligned}$$

we can define

$$\psi(i, j) = \psi(i + j) - \psi(i) - \psi(j) \quad \text{in } \mathbb{Z}_4,$$

and then it suffices to prove that $\psi(i, j)$ is even for all $i, j \in \mathbb{Z}_n$.

We will call a pair (i, j) *good* if $\psi(i, j)$ is even, and *bad* otherwise. In a sequence of further observations (Lemma 5.3 to Proposition 5.18) we will prove that there are no bad pairs, and hence σ is an admissible lift of its additive projection $\overline{\sigma}$. Note here that $-i^\sigma$ stands for $-(i^\sigma)$, rather than $(-i)^\sigma$ (which can differ from $-(i^\sigma)$).

Lemma 5.3 $\psi(i^\sigma, -i^\sigma) \equiv \psi(ei, -ei) \equiv \psi(i, -i) \bmod 2$ *for all* $i \in \mathbb{Z}_n$.

Proof Since $i^\sigma = ei + k\psi(i)$, we have $\psi(i^\sigma) \equiv \psi(ei)$ mod 2 by Lemma 5.2(e), and similarly, $\psi(-i^\sigma) \equiv \psi(-ei)$ mod 2. Then by Lemma 5.2(c) and since e is odd we find that $\psi(ei) \equiv \psi(i^\sigma) \equiv -\delta i - e\psi(i) \equiv -\delta i - \psi(i)$ mod 2, and replacing i by $-i$ gives also $\psi(-ei) \equiv \delta i - \psi(-i)$. Adding these last two congruences gives

$$\psi\big(i^\sigma\big) + \psi\big(-i^\sigma\big) \equiv \psi(ei) + \psi(-ei) \equiv -\psi(i) - \psi(-i) \equiv \psi(i) + \psi(-i) \bmod 2,$$

and the rest follows since $\psi(t,-t) = \psi(0) - \psi(t) - \psi(-t) = -(\psi(t) + \psi(-t))$ for all t. □

Corollary 5.4 $i^{(\sigma\tau)^2} \equiv i + k\psi(i,-i)$ mod m *for all* $i \in \mathbb{Z}_n$.

Proof

$$\begin{aligned}
i^{(\sigma\tau)^2} &= -\big(-i^\sigma\big)^\sigma = ei^\sigma - k\psi\big(-i^\sigma\big) = e\big(ei + k\psi(i)\big) - k\psi\big(-i^\sigma\big) \\
&= i + k\big(\delta i + e\psi(i) - \psi\big(-i^\sigma\big)\big) \quad \text{by Lemma 5.2(b)} \\
&= i + k\big(-\psi\big(i^\sigma\big) - \psi\big(-i^\sigma\big)\big) \quad \text{by Lemma 5.2(c)} \\
&= i + k\psi\big(i^\sigma, -i^\sigma\big),
\end{aligned}$$

and thus $i^{(\sigma\tau)^2} \equiv i + k\psi(i,-i)$ mod m, by Lemma 5.3. □

Lemma 5.5 $\psi(i,j) + \psi(i + k\psi(i,-i), j + k\psi(i,j)) \equiv 0$ mod 4 *for all* $i, j \in \mathbb{Z}_n$.

Proof First we observe that for every $t, i \in \mathbb{Z}_n$, Lemma 5.2 gives

$$\begin{aligned}
t^{\sigma\rho^i\sigma\rho^{i^{\sigma\tau}}} &= \big(i + t^\sigma\big)^\sigma - i^\sigma \\
&= et^\sigma + k\big(\psi\big(i + t^\sigma\big) - \psi(i)\big) \\
&= e\big(et + k\psi(t)\big) + k\big(\psi\big(i + t^\sigma\big) - \psi(i)\big) \\
&= t + k\big(\delta t + e\psi(t) + \psi\big(i + t^\sigma\big) - \psi(i)\big) \quad \text{by Lemma 5.2(b)} \\
&= t + k\big(-\psi\big(t^\sigma\big) + \psi\big(i + t^\sigma\big) - \psi(i)\big) \quad \text{by Lemma 5.2(c)} \\
&= t + k\psi\big(i, t^\sigma\big).
\end{aligned}$$

Replacing t by $t^{\sigma\rho^i\sigma\rho^{i^{\sigma\tau}}}$ and i by $i^{(\sigma\tau)^2}$ here, and applying the quadrilateral identity $(*)$ for t then gives

$$\begin{aligned}
t &= t^{\sigma\rho^i\sigma\rho^{i^{\sigma\tau}}} + k\psi\big(i^{(\sigma\tau)^2}, t^{\sigma\rho^i\sigma\rho^{i^{\sigma\tau}}}\sigma\big) \\
&= t + k\big(\psi\big(i, t^\sigma\big) + \psi\big(i^{(\sigma\tau)^2}, t^{\sigma\rho^i\sigma\rho^{i^{\sigma\tau}}}\sigma\big)\big) \\
&= t + k\big(\psi\big(i, t^\sigma\big) + \psi\big(i^{(\sigma\tau)^2}, \big(t + k\psi\big(i, t^\sigma\big)\big)^\sigma\big)\big) \quad \text{by the above.}
\end{aligned}$$

Letting $t = j^\sigma$ (so that also $j = t^\sigma$), we find that

$$\psi(i,j) + \psi\big(i^{(\sigma\tau)^2}, \big(j^\sigma + k\psi(i,j)\big)^\sigma\big) \equiv 0 \bmod 4.$$

Further application of Lemma 5.2 gives

$$
\begin{aligned}
&\big(j^\sigma + k\psi(i,j)\big)^\sigma \\
&\quad = e\big(j^\sigma + k\psi(i,j)\big) + k\psi\big(j^\sigma + k\psi(i,j)\big) \\
&\quad = e\big(ej + k\psi(j) + k\psi(i,j)\big) + k\psi\big(j^\sigma + k\psi(i,j)\big) \\
&\quad = j + k\big(\delta j + e\psi(j) + e\psi(i,j) + \psi\big(j^\sigma + k\psi(i,j)\big)\big) && \text{by Lemma 5.2(b)} \\
&\quad = j + k\big(-\psi\big(j^\sigma\big) + \psi\big(j^\sigma + k\psi(i,j)\big) + e\psi(i,j)\big) && \text{by Lemma 5.2(c)} \\
&\quad \equiv j + ke\psi(i,j) \bmod m && \text{by Lemma 5.2(e)} \\
&\quad \equiv j + k\psi(i,j) \bmod m && \text{since } e \text{ is odd,}
\end{aligned}
$$

and inserting this into the previous equation (and using Lemma 5.2(d)) we obtain

$$\psi(i,j) + \psi\big(i^{(\sigma\tau)^2}, j + k\psi(i,j)\big) \equiv 0 \bmod 4.$$

On the other hand, by Lemma 5.4 we have $i^{(\sigma\tau)^2} \equiv i + k\psi(i,-i) \bmod m$, and so the required congruence follows from Lemma 5.2(d). □

Next, by Lemma 5.2(e), we may define another function $c : \mathbb{Z}_n \to \mathbb{Z}_2$

$$\psi(t+k) = \psi(t) + 2c(t) \quad \text{for all } t \in \mathbb{Z}_n.$$

It is easy to see that $c(0) = c(m) = 0$, and that $\psi(t+kd) = \psi(t) + 2dc(t)$ for all d, again by parts (d) and (e) of Lemma 5.2. We use this function and the previous lemma to prove the following:

Lemma 5.6 *$\psi(i,-i)$ is even, for all $i \in \mathbb{Z}_n$.*

Proof Assume the contrary, so that $\psi(i,-i)$ is odd for some i. By Lemma 5.5 and the definition of c, for all $i, j \in \mathbb{Z}_n$ we have

$$
\begin{aligned}
0 &\equiv \psi(i,j) + \psi\big(i + k\psi(i,-i), j + k\psi(i,j)\big) \\
&\equiv \psi(i,j) + \psi\big(i + j + k\big(\psi(i,-i) + \psi(i,j)\big)\big) \\
&\qquad - \psi\big(i + k\psi(i,-i)\big) - \psi\big(j + k\psi(i,j)\big) \\
&\equiv 2\psi(i,j) + 2\big(\psi(i,-i) + \psi(i,j)\big)c(i+j) \\
&\qquad - 2\psi(i,-i)c(i) - 2\psi(i,j)c(j) \bmod 4,
\end{aligned}
$$

and hence (from the assumption that $\psi(i,-i)$ is odd), we have

$$\psi(i,j) + \big(1 + \psi(i,j)\big)c(i+j) - c(i) - \psi(i,j)c(j) \equiv 0 \bmod 2,$$

or equivalently,

$$\big(1 + \psi(i,j)\big)c(i+j) \equiv c(i) + \psi(i,j)\big(c(j) - 1\big) \bmod 2.$$

This can be used to prove by induction that $c(t) = c(i)$ whenever t is a multiple of i in $\mathbb{Z}_n$. For if that is true for $t = j$, then $\psi(i, j)$ must be even (or otherwise $(1 + \psi(i, j))c(i + j)$ would be even while $c(i) + \psi(i, j)(c(j) - 1) \equiv 2c(i) - 1 \equiv 1 \bmod 2$); and it then follows easily that $c(i+j) \equiv (1+\psi(i, j))c(i+j) \equiv c(i) \bmod 2$, so it is true also for $t = i + j$.

But on the other hand, since $c(0) = 0$ and $\psi(i, -i)$ is odd, taking $j = -i$ in the last displayed congruence above gives

$$0 \equiv c(i) + c(-i) - 1 \bmod 2,$$

so $c(-i) \neq c(i)$, a contradiction. This completes the proof. □

Corollary 5.7 *$(\sigma\tau)^2$ acts trivially modulo m; that is, $i^{(\sigma\tau)^2} \equiv i \bmod m$ for all $i \in \mathbb{Z}_n$.*

Proof We know $i^{(\sigma\tau)^2} \equiv i + k\psi(i, -i) \bmod m$, by Corollary 5.4, and the rest follows from Lemma 5.6. □

Also Lemma 5.6 can be used to provide a simpler version of Lemma 5.5:

Corollary 5.8 *$\psi(i, j)((1 + c(i + j) - c(j)) \equiv 0 \bmod 2$ for all $i, j \in \mathbb{Z}_n$.*

Proof First Lemma 5.5 gives this congruence mod 4:

$$\begin{aligned}
0 &\equiv \psi(i, j) + \psi\big(i + k\psi(i, -i), j + k\psi(i, j)\big) \\
&\equiv \psi(i, j) + \psi\big(i + j + k\big(\psi(i, -i) + \psi(i, j)\big)\big) \\
&\quad - \psi\big(i + k\psi(i, -i)\big) - \psi\big(j + k\psi(i, j)\big).
\end{aligned}$$

Since $\psi(i, -i)$ is even, it follows that

$$\begin{aligned}
0 &\equiv \psi(i, j) + \psi\big(i + j + k\psi(i, j)\big) \\
&\quad - \psi(i) - \psi\big(j + k\psi(i, j)\big) && \text{by Lemma 5.2(d)} \\
&\equiv 2\psi(i, j) + 2\psi(i, j)c(i + j) - 2\psi(i, j)c(j) && \text{by the definition of } c \\
&\equiv 2\psi(i, j)\big(1 + c(i + j) - c(j)\big) \bmod 4,
\end{aligned}$$

and the result follows. □

Lemma 5.9 *$c(i + k) = c(i)$ and $c(ei) = c(i)$ for all $i \in \mathbb{Z}_n$.*

Proof The first of these is an easy consequence of the following:

$$\begin{aligned}
\psi(i) = \psi(i + m) = \psi(i + k + k) &= \psi(i + k) + 2c(i + k) \\
&= \psi(i) + 2c(i) + 2c(i + k).
\end{aligned}$$

For the second, note that by Lemma 5.2(c) and the definitions of ψ and c, we have

$$0 \equiv i\delta + e\psi(i) + \psi(ei) + 2c(ei)\psi(i) \bmod 4.$$

Replacing i by $i+k$, we have also

$$0 \equiv (i+k)\delta + e\psi(i+k) + \psi(ei+ek) + 2c(ei+ek)\psi(i+k) \bmod 4.$$

But now $\psi(ei+ek) = \psi(ei) + 2ec(ei)$, and by what we proved above, $c(ei+ek) = c(ei)$, so the latter congruence can be rewritten as

$$0 \equiv (i+k)\delta + e\psi(i+k) + \psi(ei) + 2ec(ei) + 2c(ei)\psi(i+k) \bmod 4.$$

Subtracting the earlier congruence (namely the one for i) from this one (for $i+k$), and again using $\psi(i+k) = \psi(i) + 2c(i)$, we find that

$$0 \equiv k\delta + 2ec(i) + 2ec(ei) + 4c(ei)c(i) \equiv k\delta + 2e\big(c(i) + c(ei)\big) \bmod 4.$$

Finally, since e is odd and n is divisible by 4, we know that $k\delta + 1 \equiv e^2 \equiv 1 \bmod 4$, and so $c(i) + c(ei)$ must be even. □

Corollary 5.10 $i\delta + (e + 2c(i))\psi(i) + \psi(ei) \equiv 0 \bmod 4$ *for all* $i \in \mathbb{Z}_n$.

Proof We observed that $0 \equiv i\delta + e\psi(i) + \psi(ei) + 2c(ei)\psi(i) \bmod 4$ in the proof of Lemma 5.9. Since $c(ei) = c(i)$, the result follows. □

Next, recall that a pair (i, j) is *good* if $\psi(i, j) = \psi(i+j) - \psi(i) - \psi(j)$ is even, or equivalently, if $(i+j)^\sigma \equiv i^\sigma + j^\sigma \bmod m$, and *bad* otherwise. Clearly $(i, 0)$ and $(0, j)$ are good for all i and j. Moreover, since $(i+m)^\sigma = i^\sigma + m = i^\sigma + m^\sigma$, we know that (i, m) is good, for all $i \in \mathbb{Z}_n$, and it follows that (i, mj) is good for all j. We also have the following:

Lemma 5.11 *If* (i, j) *is a bad pair, then the pairs* (j, i), (i^σ, j^σ), (j^σ, i^σ), $(-i, -j)$, $(-j, -i)$ *and* $(-i, i+j)$ *are all bad.*

Proof The first of these six follows from the definition, the second one from $\sigma^2 = 1$, and the third is a combination of the first two. The fourth and fifth follow from Corollary 5.7. For the last one, note that $j^\sigma \not\equiv (-i)^\sigma + (i+j)^\sigma \equiv -(i^\sigma) + (i+j)^\sigma \bmod m$. □

Lemma 5.12 *If* (i, j) *is a bad pair, then*

$$c(i) = c(j) = c\big(-(i+j)\big) \neq c(-i) = c(-j) = c(i+j).$$

Equivalently, if $c(u)$ *and* $c(v)$ *have opposite parities, then the pair* (u, v) *must be good.*

Proof By Lemma 5.8, we know that $\psi(i, j)((1 + c(i+j) - c(j)) \equiv 0 \bmod 2$ for every pair (i, j), whether good or bad. Now if (i, j) is bad, then $\psi(i, j)$ is odd, and therefore $1 + c(i+j) - c(j)$ is even, so $c(j)$ and $c(i+j)$ have opposite parities. The rest follows from Lemma 5.11. □

Lemma 5.13 *If (i, j) is a bad pair and (u, v) a good pair, with $i + j \equiv u + v \bmod m$, then exactly one of $(i, -u)$ and $(v, -j)$ is bad, and exactly one of $(i, -v)$ and $(u, -j)$ is bad.*

Proof First $i^\sigma + j^\sigma \not\equiv (i + j)^\sigma \equiv (u + v)^\sigma \equiv u^\sigma + v^\sigma \bmod m$, so by Corollary 5.7, we find $i^\sigma + (-u)^\sigma \equiv i^\sigma - u^\sigma \not\equiv v^\sigma - j^\sigma \equiv v^\sigma + (-j)^\sigma \bmod m$. On the other hand, $i + (-u) = v + (-j) \bmod m$ (since $i + j = u + v \bmod m$), so $(i + (-u))^\sigma \equiv (v + (-j))^\sigma \bmod m$. It follows that $(i + (-u))^\sigma \not\equiv i^\sigma + (-u)^\sigma$ or $(v + (-j))^\sigma \not\equiv v^\sigma + (-j)^\sigma \bmod m$. Just one of these holds, since $i^\sigma + (-u)^\sigma \equiv (i - u)^\sigma \equiv (v - j)^\sigma \equiv v^\sigma + (-j)^\sigma \bmod k$, by our assumption that σ is additive modulo k. Hence exactly one of $(i, -u)$ and $(v, -j)$ is bad. Similarly, exactly one of $(i, -v)$ and $(u, -j)$ is bad. □

Lemma 5.14 *If (i, j) is bad, then for every positive integer a, there exists some $v \in \mathbb{Z}_n$ such that the pair $(2^a i, v)$ is bad.*

Proof By Lemma 5.12, we know $c(i) \neq c(i + j)$ and hence the pair $(i, i + j)$ is good. Also $(-i, 2i + j)$ must be good, for otherwise $(i, i + j)$ would be bad, by Lemma 5.11. Now since (i, j) is bad and $(-i, 2i + j)$ is good, Lemma 5.13 shows that exactly one of (i, i) and $(2i + j, -j)$ is bad. In the former case, both $(-i, 2i)$ and $(2i, -i)$ are bad (by Lemma 5.11), while in the latter case, both $(-(2i + j), 2i)$ and $(2i, -(2i + j))$ are bad. In each case, we find that $(2i, t)$ is bad for some t (namely $-i$ or $-(2i + j)$, respectively). But now the same argument applied to $(2i, t)$ shows that $(4i, u)$ is bad for some u, and so on, and hence by induction, we get the result claimed. □

Now let q be the largest odd divisor of k, so that $n = 2m = 4k = 2^s q$ for some $s \geq 2$, and let $d = \gcd(e - 1, q)$.

Lemma 5.15 *With $d = \gcd(e - 1, q)$ defined as above*:

(a) *the pair (aq, b) is good for all $a, b \in \mathbb{Z}_n$*;
(b) *if (i, j) is a bad pair, then so is $(i + aq, j + bq)$ for all $a, b \in \mathbb{Z}_n$*;
(c) *the pair $(a(e - 1), b)$ is good for all $a, b \in \mathbb{Z}_{2m}$*;
(d) *if (i, j) is a bad pair, then so is $(i + a(e - 1), j + b(e - 1))$ for all $a, b \in \mathbb{Z}_n$*;
(e) *if (i, j) is a bad pair, then so is $(i + ad, j + bd)$ for all $a, b \in \mathbb{Z}_n$*;
(f) *for all $a, b \in \mathbb{Z}_{2m}$, the pair (ad, b) is good.*

Proof For part (a), note that if (aq, b) is bad, then by Lemma 5.14, the pair $(2^s aq, v)$ is bad for some v. But $2^s aq = an = 0$ in $\mathbb{Z}_n$, so this says $(0, v)$ is bad, contradiction. Next, if (i, j) is bad, then by Lemma 5.11 the pair $(i + j, -j)$ is bad, and by (a), we know that $(-aq, i + aq)$ is good. Hence by Lemma 5.13, we find that exactly one of $(i + j, aq)$ and $(i + aq, j)$ is bad. But $(i + j, aq)$ is good, so $(i + aq, j)$ must be bad. A similar argument then shows that $(i + aq, j + bq)$ is bad, which proves (b).

For part (c), let $v = a(e - 1)$. Then

$$ve = a(e - 1)e = a\big(e^2 - e\big) \equiv a(1 + k\delta - e) \equiv a(1 - e) = -v \bmod k,$$

so $c(v) = c(ev) = c(-v)$ by Lemma 5.9, and it follows from Lemma 5.12 that no pair (v, b) is bad. Hence $(a(e-1), b)$ is good for all b, proving part (c).

By Lemma 5.11, also $(-a(e-1), u)$ is good for all u. In particular, if (i, j) is bad, then we can take $u = i + j + a(e-1)$, which gives a pair with the same sum as (i, j), and by Lemma 5.13, we find that exactly one of $(i, a(e-1))$ and $(u, -j)$ is bad. But $(i, a(e-1))$ is good by part (c), so $(u, -j)$ must be bad, and therefore $(i + a(e-1), j) = (u - j, j)$ is bad. A similar argument then shows that $(i + a(e-1), j + b(e-1))$ is bad, which proves (d).

By Bézout's identity, $d = \gcd(e-1, q) = u(e-1) + vq$ for some integers u and v, and thus $ad = au(e-1) + avq \equiv au(e-1) \bmod q$ and similarly $bd \equiv bu(e-1) \bmod q$, for given $a, b \in \mathbb{Z}_n$. Hence if (i, j) is bad, then $(i + ad, j + bd) \equiv (i + au(e-1), j + bu(e-1)) \bmod q$, so $(i + ad, j + bd)$ is bad by parts (b) and (d). This proves (e).

Finally, for part (f), if (ad, b) is bad, then by part (e), so is $(ad - ad, b) = (0, b)$, a contradiction. □

Lemma 5.16 *For every integer i, there exists an integer a such that $(e-1)(i + ad)$ is divisible by m.*

Proof First, write $q = du$ and $e - 1 = d2^r v$, where u and v are odd integers (and r is a non-negative integer), and $\gcd(u, 2^r v) = \gcd(q/d, (e-1)/d) = 1$. Then since $(e-1)(e+1) = e^2 - 1 \equiv 0 \bmod k (= 2^{s-2}q)$, we know that $du = q$ divides $(e-1)(e+1)$, and as d divides $e-1$ but u is coprime to $2^r v = (e-1)/d$, we deduce that u divides $e+1$. It follows that $\gcd(d, u)$ divides $\gcd(e-1, e+1) = 2$, and since both d and u are odd, we must have $\gcd(d, u) = 1$. But also u and v are coprime (since $\gcd(u, 2^r v) = 1$), therefore also $\gcd(dv, u) = 1$. Thus $\gcd(e-1, m/d) = \gcd(d2^r v, 2^{s-1}q/d) = \gcd(d2^r v, 2^{s-1}u)$ is a power of 2, say $\gcd(e-1, m/d) = 2^w$.

Now $e - 1$ is divisible by both $2^w (= \gcd(e-1, m/d))$ and $d (= \gcd(q, e-1))$, which is odd, so $e - 1 = 2^w dt$ for some t. Also, by Bézout's identity, there exist integers A and B such that $2^w = (e-1)A + (m/d)B$, and therefore $e - 1 = 2^w dt = (e-1)Adt + mBt$.

For any given i, it follows that $(e-1)i = (e-1)Adti + mBti$, and hence that $(e-1)(i - (Ati)d) = mBti$. Taking $a = -(Ati)$, we have $(e-1)(i + ad) \equiv 0 \bmod m$. □

Corollary 5.17 *For every integer i, there exists an integer t such that $t \equiv i \bmod d$ and $et \equiv t \bmod m$.*

Proof By Lemma 5.16, there exists some a for which $(e-1)(i + ad)$ is divisible by m. Let $t = i + ad$. Then $t \equiv i \bmod d$, and $et - t = (e-1)t = 0 \bmod m$. □

Proposition 5.18 *There are no bad pairs.*

Proof Suppose there exists a bad pair (i, j). By Lemma 5.15(e), we can replace i by any integer t congruent to i mod d, and so by Corollary 5.17, we may assume that $ei \equiv i \bmod m$. Similarly, we may assume that $ej \equiv j \bmod m$. Then by Lemma 5.2(d), we find that $\psi(ei) = \psi(i)$ and $\psi(ej) = \psi(j)$.

Next, since $\psi(i,j)=\psi(i+j)-\psi(i)-\psi(j)$ is odd, we know that at least one of $\psi(i)$, $\psi(j)$ and $\psi(i+j)$ is odd, and without loss of generality (replacing (i,j) by (j,i) or $(i+j,-i)$ if necessary), we may assume that $\psi(i)$ is odd. We also know that $c(i)\neq c(-i)$, by Lemma 5.12, so that $c(-i)\equiv c(i)+1 \bmod 2$.

Now by Corollary 5.10 and the fact that $\psi(ei)=\psi(i)$, we find that

$$0\equiv i\delta+\big(e+2c(i)\big)\psi(i)+\psi(ei)\equiv i\delta+\big(e+2c(i)+1\big)\psi(i) \bmod 4.$$

Similarly, replacing i by $-i$ (and using $c(-i)\equiv c(i)+1 \bmod 2$), we have

$$0\equiv -i\delta+\big(e+2c(-i)\big)\psi(-i)+\psi(-ei)\equiv -i\delta+\big(e+2c(i)+3\big)\psi(-i) \bmod 4.$$

Adding these two congruences gives

$$0=\big(e+2c(i)+3\big)\big(\psi(i)+\psi(-i)\big)-2\psi(i) \bmod 4.$$

Since both $e+3+2c(i)$ and $\psi(i)+\psi(-i)=\psi(i,-i)$ are even, their product is divisible by 4. Thus $2\psi(i)$ is divisible by 4, which is a contradiction. □

This completes the proof of Theorem 5.1.

6 Reflexibility and enumeration

In this section, we consider reflexibility of the orientably-regular embeddings $\mathcal{M}(\sigma)$ of Q_n, and then derive formulae for the total number of non-isomorphic embeddings as well as for those that are reflexible and chiral, respectively.

We begin with the following:

Proposition 6.1 *Let σ be an admissible involution in S_n. Then the embedding $\mathcal{M}(\sigma)$ is reflexible if and only if $(\sigma\tau)^2=1$, where τ is the permutation S_n induced by multiplication by -1 in $\mathbb{Z}_n$.*

Proof By the background theory of regular maps given in Sect. 2, we know $\mathcal{M}(\sigma)$ is reflexible if and only if there exists an involutory automorphism θ of $G(\sigma)=\langle\rho,e_n\sigma\rangle$ that inverts ρ and fixes $e_n\sigma$. This reflecting automorphism must induce an automorphism of the underlying graph Q_n, and hence can be assumed to be an element of $\mathbb{Z}_2\wr S_n$, say $\theta=v\pi$ for some $v\in V={\mathbb{Z}_2}^n$ and $\pi\in S_n$. Now

$$\rho^{-1}=\rho^\theta=\rho^{v\pi}=(v\rho v)^\pi=\big(v\big(\rho v\rho^{-1}\big)\big)^\pi\rho^\pi,$$

which implies that $\rho v\rho^{-1}=v$ and $\rho^\pi=\rho^{-1}$. The latter implies $\pi=\tau\rho^i$ for some i, and the former implies that v is either trivial (zero) or the product $e_1e_2\cdots e_n$. Since $e_1e_2\cdots e_n$ is central in $\mathbb{Z}_2\wr S_n$, we may assume without loss of generality that v is trivial, so $\theta=\tau\rho^i$ for some i. If $i\neq 0 \pmod n$, however, then ${e_n}^\theta={e_n}^{\tau\rho^i}={e_n}^{\rho^i}=e_i$, so $(e_n\sigma)^\theta=e_i\sigma^\theta$, so θ does not centralize $e_n\sigma$. Thus $\theta=\tau$, which centralizes e_n, and then since $e_n\sigma=(e_n\sigma)^\tau=e_n\sigma^\tau$, the reflexibility condition reduces to requiring $\sigma^\tau=\sigma$, or equivalently, $(\sigma\tau)^2=1$. □

Next, we consider the total number of non-isomorphic regular embeddings of Q_n, or equivalently, the number of admissible involutions in S_n. We also determine how many of these embeddings are reflexible.

To do this, it helps to define $\mathrm{Inv}(n) = \{e \in \mathbb{Z}_n \mid e^2 = 1 \bmod n\}$ (the set of all square roots of 1 in $\mathbb{Z}_n$) for each positive integer n. Note also that when n is an odd prime-power, there are just two such roots, viz. 1 and $n-1$, since the group of units in $\mathbb{Z}_n$ is cyclic in that case.

Now for odd n, by Theorem 2.2 (taken from [9]) the total number of embeddings is simply the number of square roots of 1 in $\mathbb{Z}_n$. If $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ is the prime-power decomposition of n (with $p_1, p_2, \ldots, p_t$ distinct odd primes and $a_1, a_2, \ldots, a_t$ positive integers), this number is 2^t (by the Chinese Remainder Theorem). Moreover, every admissible involution τ_e commutes with τ, so every regular embedding is reflexible in this case. In other words, none of the regular embeddings of Q_n is chiral when n is odd.

For even n, by Theorem 5.1 the total number of regular embeddings is equal to the number of permutations σ of order 1 or 2 in S_n that fix n and reduce modulo m to multiplication by some square root e of 1 in $\mathbb{Z}_m$. In this case, we have the following counting theorem.

Theorem 6.2 *For $n = 2m$ (even), the total number of regular embeddings of Q_n is*

$$\sum_{e\in \mathrm{Inv}(m)} 2^{\frac{1}{2}(m+\gcd(e-1,m)-2)}.$$

Proof Let $\sigma \in S_n$ be an admissible involution that reduces to τ_e modulo m.

If τ_e fixes $i \in \mathbb{Z}_m \setminus \{0\}$, then σ either fixes or interchanges the two points i and $i+m$. Similarly, if τ_e moves $i \in \mathbb{Z}_m$, then σ induces either $(i, ei)(i+m, ei+m)$ or $(i, ei+m)(i+m, ei)$ on the 4-point set $\{i, ei, i+m, ei+m\}$ (considered mod n).

Hence the number of admissible $\sigma \in S_n$ that reduce to τ_e modulo m is 2^d, where d is the number of cycles of the permutation τ_e on $\mathbb{Z}_m \setminus \{0\}$.

Now $i \in \mathbb{Z}_m$ is fixed by τ_e if and only if $(e-1)i = ei - i \equiv 0 \bmod m$, which occurs if and only if i is divisible by $m/\gcd(e-1, m)$, so the number of $i \in \mathbb{Z}_m$ fixed by τ_e is exactly $\gcd(e-1, m)$. Hence the number of cycles of τ_e on $\mathbb{Z}_m$ is

$$d + 1 = \gcd(e-1, m) + \frac{1}{2}\big(m - \gcd(e-1, m)\big) = \frac{1}{2}\big(m + \gcd(e-1, m)\big),$$

and the result follows. □

By Lemma 6.1, the reflexible embeddings come from the admissible involutions that commute with τ, and for these we have the following:

Theorem 6.3 *For $n = 2m$ (even), the number of reflexible regular embeddings of Q_n is*

$$\begin{cases} \sum_{e\in \mathrm{Inv}(m)} 2^{\frac{1}{4}(m+\gcd(e-1,m)+\gcd(e+1,m)-3)} & \text{if } m \text{ is odd} \\ \sum_{e\in \mathrm{Inv}(m)} 2^{\frac{1}{4}(m+\gcd(e-1,m)+\gcd(e+1,m)-2)} & \text{if } m \text{ is even.} \end{cases}$$

Proof Let $\sigma \in S_n$ be an admissible involution that reduces to τ_e modulo m, and commutes with τ (so that $(-i)^\sigma = -(i^\sigma)$ for every $i \in \mathbb{Z}_n$). Note that σ fixes m and n.

If m is even, then τ_e fixes $\frac{m}{2}$, and σ either fixes or interchanges the points $\frac{m}{2}$ and $\frac{3m}{2}$.

If τ_e fixes $i \in \mathbb{Z}_m \setminus \{0, \frac{m}{2}, m, \frac{3m}{2}\}$, then σ induces either the identity permutation or $(i, i+m)(m-i, n-i)$ on the 4-point set $\{i, i+m, m-i, n-i\}$ (considered mod n). Similarly, if τ_e takes $i \in \mathbb{Z}_m \setminus \{0, \frac{m}{2}, m, \frac{3m}{2}\}$ to $m-i$ (mod m), then σ induces either $(i, m-i)(i+m, n-i)$ or $(i, n-i)(i+m, m-i)$ on the 4-point set $\{i, m-i, i+m, n-i\}$ (considered mod n).

For any other $i \in \mathbb{Z}_n$ (neither fixed by τ_e nor taken to $m-i$ by τ_e), it is easy to see that σ induces either $(i, ei)(i+m, ei+m)(m-i, m-ei)(n-i, n-ei)$ or $(i, ei+m)(i+m, ei)(m-i, n-ei)(n-i, m-ei)$ on the set $\{i, ei, i+m, ei+m, m-i, m-ei, n-i, n-ei\}$ (considered mod n).

Since the number of fixed points of τ_e on $\mathbb{Z}_m$ is $\gcd(e-1, m)$ while (similarly) the number of $i \in \mathbb{Z}_m$ satisfying $ei = m-i \bmod \gcd(e+1, m)$, we find the total number of possibilities for σ is 2^d, where

$$\begin{aligned}
d &= \frac{1}{2}\big(\gcd(e-1,m) + \gcd(e+1,m) - 2\big) \\
&\quad + \frac{1}{4}\big(m - \gcd(e-1,m) - \gcd(e+1,m) + 1\big) \\
&= \frac{1}{4}\big(m + \gcd(e-1,m) + \gcd(e+1,m) - 3\big) \quad \text{if } m \text{ is odd, while} \\
d &= \frac{1}{2}\big(\gcd(e-1,m) + \gcd(e+1,m) - 4\big) \\
&\quad + \frac{1}{4}\big(m - \gcd(e-1,m) - \gcd(e+1,m) + 2\big) + 1 \\
&= \frac{1}{4}\big(m + \gcd(e-1,m) + \gcd(e+1,m) - 2\big) \quad \text{if } m \text{ is even,}
\end{aligned}$$

and the result follows. □

Corollary 6.4 *For $n = 2m$ (even), the number of (orientably) regular embeddings of Q_n that are chiral is*

$$\begin{cases} \sum_{e\in\mathrm{Inv}(m)} \big(2^{\frac{1}{2}(m+\gcd(e-1,m)-2)} - 2^{\frac{1}{4}(m+\gcd(e-1,m)+\gcd(e+1,m)-3)}\big) & \textit{if } m \textit{ is odd} \\ \sum_{e\in\mathrm{Inv}(m)} \big(2^{\frac{1}{2}(m+\gcd(e-1,m)-2)} - 2^{\frac{1}{4}(m+\gcd(e-1,m)-2-\gcd(e+1,m)-2)}\big) & \textit{if } m \textit{ is even.} \end{cases}$$

Since the term $2^{\frac{1}{2}(m+\gcd(e-1,m)-2)} - 2^{\frac{1}{4}(m+\gcd(e-1,m)+\gcd(e+1,m)-c)}$ in the formula for chiral embeddings clearly outweighs the corresponding term $2^{\frac{1}{4}(m+\gcd(e-1,m)+\gcd(e+1,m)-c)}$ in the formula for reflexible embeddings (with $c = 3$ or 2), this shows that the ratio of reflexible to chiral embeddings tends to zero for large even n.

The numbers of regular embeddings of Q_n for small values of n (from 3 to 36) are given in Table 1.

Table 1 Table of numbers of regular embeddings of Q_n for small n

n	Reflexible	Chiral	Total
3	2	0	2
4	2	0	2
5	2	0	2
6	4	2	6
7	2	0	2
8	8	4	12
9	2	0	2
10	8	12	20
11	2	0	2
12	16	24	40
13	2	0	2
14	16	56	72
15	4	0	4
16	48	144	192
17	2	0	2
18	32	240	272
19	2	0	2
20	64	480	544
21	4	0	4
22	64	992	1056
23	2	0	2
24	192	2304	2496
25	2	0	2
26	128	4032	4160
27	2	0	2
28	256	8064	8320
29	2	0	2
30	320	16960	17280
31	2	0	2
32	640	34688	35328
33	4	0	4
34	512	65280	65792
35	4	0	4
36	1024	130560	131584

7 Genera and other properties

To determine the genus of any regular embedding of Q_n, all we need to calculate is the face-size, which is the order of the product $e_n\sigma\rho$ of the two generators of $G(\sigma) = \langle \rho, e_n\sigma \rangle$. If this face-size is s, say, then the genus g and Euler characteristic χ of the map $\mathcal{M}(\sigma)$ are given by the Euler–Poincaré formula

$$2 - 2g = \chi = |V| - |E| + |F| = 2^n - n2^{n-1} + n2^n/s.$$

Now let t be the order of $\sigma\rho$ in S_n, and let O be the orbit of the point n under the subgroup of S_n generated by $\sigma\rho$. Then an easy calculation gives

$$(e_n\sigma\rho)^t = \frac{t}{|O|}\sum_{i\in O} e_i,$$

and so the order s of $e_n\sigma\rho$ is given by $s = t$ if $\frac{t}{|O|}$ is even, or $s = 2t$ if $\frac{t}{|O|}$ is odd.

When n is odd, we know that $\sigma = \tau_e$ (multiplication by e mod n) for some square root e of 1 in $\mathbb{Z}_n$, and since ρ is addition by 1 mod n, it is a straightforward exercise to show that

$$s = 2t = 2|O| = \begin{cases} 2n & \text{when } e = 1, \\ 4 & \text{when } e = -1, \text{ and} \\ \frac{4n}{\gcd(e+1,n)} & \text{when } 1 < e < n-1 \end{cases}$$

so that the genus $g = g(\mathcal{M}(\sigma))$ of the map $\mathcal{M}(\sigma)$ is given by

$$g\big(\mathcal{M}(\sigma)\big) = \begin{cases} 2^{n-2}(n-3)+1 & \text{when } e = 1, \\ 2^{n-3}(n-4)+1 & \text{when } e = -1, \text{ and} \\ 2^{n-3}(2n-4-\gcd(e+1,n))+1 & \text{when } 1 < e < n-1. \end{cases}$$

Note that this corrects an error in calculation of both the face-size and the genus in the first concluding remark of [9, Sect. 4] for cases where $1 < e < n-1$.

When n is even, the situation is more complicated. Here we let $e = 1^\sigma$ if this is odd, or $e = 1^\sigma + n/2$ if 1^σ is even (and $n/2$ is odd). Then letting f denote multiplication by e mod m, we know that σ induces the permutation $B_i \mapsto B_{f(i)}$ on the m blocks $B_i = \{i, i+m\}$. It is now a straightforward (but longer) exercise to verify that

$$s = 2|O| = \begin{cases} 2n & \text{when } e \equiv 1 \bmod m \text{ and the permutation } \sigma \text{ is even}, \\ n & \text{when } e \equiv 1 \bmod m \text{ and the permutation } \sigma \text{ is odd}, \\ 8 & \text{when } e \equiv -1 \bmod m \text{ and } 1^\sigma = m-1, \\ 4 & \text{when } e \equiv -1 \bmod m \text{ and } 1^\sigma = n-1, \\ \frac{4n}{\gcd(e+1,m)} & \text{when } e \not\equiv \pm 1 \bmod m \text{ and } m^{(\sigma\rho)^i} = n \text{ for some } i, \text{ and} \\ \frac{2n}{\gcd(e+1,m)} & \text{when } e \not\equiv \pm 1 \bmod m \text{ and } m^{(\sigma\rho)^i} \neq n \text{ for any } i. \end{cases}$$

Hence for $n = 2m$, the genus $g = g(\mathcal{M}(\sigma))$ of the map $\mathcal{M}(\sigma)$ is given by

$$\begin{cases} 2^{n-2}(n-3)+1 & \text{when } e \equiv 1 \bmod m \text{ and } \sigma \text{ is even}, \\ 2^{n-2}(n-4)+1 & \text{when } e \equiv 1 \bmod m \text{ and } \sigma \text{ is odd}, \\ 2^{n-4}(3n-8)+1 & \text{when } e \equiv -1 \bmod m \text{ and } 1^\sigma = m-1, \\ 2^{n-3}(n-4)+1 & \text{when } e \equiv -1 \bmod m \text{ and } 1^\sigma = n-1, \\ 2^{n-3}(2n-4-\gcd(e+1,m))+1 & \\ \quad \text{when } e \not\equiv \pm 1 \bmod m \text{ and } m^{(\sigma\rho)^i} = n \text{ for some } i, & \\ 2^{n-2}(n-2-\gcd(e+1,m))+1 & \\ \quad \text{when } e \not\equiv \pm 1 \bmod m \text{ and } m^{(\sigma\rho)^i} \neq n \text{ for all } i. & \end{cases}$$

It follows that whether n is even or odd, the maximum genus of all orientably-regular embeddings of Q_n is $2^{n-2}(n-3)+1$ (attained in some cases when $e=1$), while the minimum genus is $2^{n-3}(n-4)+1$ (attained in some cases when $e=-1$).

Another observation we can make is that if the map $\mathcal{M}(\sigma)$ is reflexible, then $\tau\sigma$ is not just an involution, but an admissible involution; indeed the map $\mathcal{M}(\tau\sigma)$ is the Petrie dual of $\mathcal{M}(\sigma)$. On the other hand, if $\mathcal{M}(\sigma)$ is chiral, then $\tau\sigma\tau$ is an admissible involution, and $\mathcal{M}(\tau\sigma\tau)$ is the mirror image of $\mathcal{M}(\sigma)$. Thus orientably-regular embeddings of Q_n always come in mated pairs, with each map being the Petrie dual or mirror image of its mate. More generally, we may consider the effect of the 'hole operators' considered in [27]. For each j coprime to n, applying the operator H_j to an n-valent map M gives a map $H_j(M)$ with the same underlying graph as M. Here $H_j(\mathcal{M}(\sigma))$ is $\mathcal{M}(\tau_j\sigma\tau_j^{-1})$, given by the admissible involution $\tau_j\sigma\tau_j^{-1}$ (where τ_j is multiplication by j mod n).

Finally, we add the following:

Theorem 7.1 *All the maps obtained from orientably-regular embeddings of Q_n are* regular Cayley maps, *in the sense that the automorphism group of the map contains a subgroup that acts regularly on vertices.*

Proof The group of all orientation-preserving automorphisms of the map is the subgroup $G=\langle e_n\sigma,\rho\rangle$ of the wreath product $\mathbb{Z}_2 \wr S_n$, and so has a natural transitive but imprimitive action on the set $\{1,2,\dots,2n\}$, with n blocks $B_i=\{i,i+n\}$ of size 2. The cyclic subgroup Y generated by ρ, which permutes these n blocks in a cycle, is the stabilizer in G of a vertex of the map $\mathcal{M}(\sigma)$. Now if H is the stabilizer in G of any block, say $B_n=\{n,2n\}$, then H is complementary to Y in G (that is, $G=HY$ with $H\cap Y=1$), and so H acts regularly on the vertices of $\mathcal{M}(\sigma)$, which is therefore a regular Cayley map for H. □

Acknowledgements The authors acknowledge the use of GAP [11] and MAGMA [2] in analyzing small examples and testing conjectures in the preparation of this paper.

The first author's work was supported by the UI&D Matemática e Aplicações of the University of Aveiro, through the Programa Operacional Ciência, Tecnologia, Inovaçao (POCTI) of the Fundação para a Ciência e a Tecnologia (FCT), and co-financed by the European Community fund FEDER. The second author's work was supported by the Marsden Fund of New Zealand, project number UOA-721. The third author's work was supported by the research grants NNSF(10971144) and BNSF(1092010) in China. The fourth author's work was supported by a Korea Research Foundation grant, funded by the Korean Government (MOEHRD, Basic Research Promotion Fund), number KRF-2008-331-C00049. The fifth author's work was supported by grant VEGA 1/0722/08 of the Slovak Republic's Ministry of Education.

References

1. Biggs, N.L.: Classification of complete maps on orientable surfaces. Rend. Mat. **4**(6), 132–138 (1971)
2. Bosma, W., Cannon, J., Playoust, C.: The MAGMA algebra system I: the user language. J. Symb. Comput. **24**, 235–265 (1997)
3. Catalano, D.A., Nedela, R.: A characterization of regular embeddings of n-dimensional cubes. Discrete Math. (2010, to appear). doi:10.1016/j.disc.2010.05.010
4. Conder, M.D.E.: Regular maps and hypermaps of Euler characteristic −1 to −200. J. Comb. Theory Ser. B **99**, 455–459 (2009). With associated lists of computational data available at the website http://www.math.auckland.ac.nz/~conder/hypermaps.html

5. Conder, M.D.E., Dobcsányi, P.: Determination of all regular maps of small genus. J. Comb. Theory Ser. B **81**, 224–242 (2001)
6. Du, S.F., Jones, G.A., Kwak, J.H., Nedela, R., Škoviera, M.: Regular embeddings of $K_{n,n}$ where n is a power of 2. I: Metacyclic case. Eur. J. Comb. **28**, 1595–1609 (2007)
7. Du, S.F., Jones, G.A., Kwak, J.H., Nedela, R., Škoviera, M.: Regular embeddings of $K_{n,n}$ where n is a power of 2. II: Non-metacyclic case. Eur. J. Comb. (2010, to appear). doi:10.1016/j.ejc.2010.01.009
8. Du, S.F., Kwak, J.H., Nedela, R.: Regular maps with pq vertices. J. Algebraic Comb. **19**, 123–141 (2004)
9. Du, S.F., Kwak, J.H., Nedela, R.: Classification of regular embeddings of hypercubes of odd dimension. Discrete Math. **307**, 119–124 (2007)
10. Du, S.F., Kwak, J.H., Nedela, R.: Regular embeddings of complete multipartite graphs. Eur. J. Comb. **26**, 505–519 (2005)
11. The GAP Group: GAP—Groups Algorithms and Programming, Version 4.3 (2002). http://www.gap-system.org
12. Gardiner, A., Nedela, R., Širáň, J., Škoviera, M.: Characterization of graphs which underlie regular maps on closed surfaces. J. Lond. Math. Soc. **59**, 100–108 (1999)
13. Heffter, L.: Über metacyclic Gruppen und Nachbarconfigurationen. Math. Ann. **50**, 261–268 (1898)
14. James, L.D., Jones, G.A.: Regular orientable imbeddings of complete graphs. J. Comb. Theory Ser. B **39**, 353–367 (1985)
15. Jones, G.A.: Regular embeddings of complete bipartite graphs: classification and enumeration. Proc. Lond. Math. Soc. (to appear). doi:10.1112/plms/pdp061
16. Jones, G.A., Nedela, R., Škoviera, M.: Regular embeddings of $K_{n,n}$ where n is an odd prime power. Eur. J. Comb. **28**, 1863–1875 (2007)
17. Jones, G.A., Nedela, R., Škoviera, M.: Complete bipartite graphs with a unique regular embedding. J. Comb. Theory Ser. B **98**, 241–248 (2008)
18. Jones, G.A., Singerman, D.: Belyi functions, hypermaps, and Galois groups. Bull. Lond. Math. Soc. **28**, 561–590 (1996)
19. Kwak, J.H., Kwon, Y.S.: Regular orientable embeddings of complete bipartite graphs. J. Graph Theory **50**, 105–122 (2005)
20. Kwak, J.H., Kwon, Y.S.: Classification of reflexible regular embeddings and self-Petrie dual regular embeddings of complete bipartite graphs. Discrete Math. **308**, 2156–2166 (2008)
21. Kwon, Y.S.: New regular embeddings of n-cubes Q_n. J. Graph Theory **46**, 297–312 (2004)
22. Kwon, Y.S., Nedela, R.: Non-existence of nonorientable regular embeddings of n-dimensional cubes. Discrete Math. **307**, 511–516 (2007)
23. Nedela, R., Škoviera, M.: Regular maps of canonical double coverings of graphs. J. Comb. Theory Ser. B **67**, 249–277 (1996)
24. Nedela, R., Škoviera, M.: Regular maps from voltage assignments and exponent groups. Eur. J. Comb. **18**, 807–823 (1997)
25. Nedela, R., Škoviera, M., Zlatoš, A.: Bipartite maps, Petrie duality and exponent groups. Atti Semin. Mat. Fis. Univ. Modena **49** (Suppl.), 109–133 (2001). Dedicated to the memory of Professor M. Pezzana (in Italian)
26. Nedela, R., Škoviera, M., Zlatoš, A.: Regular embeddings of complete bipartite graphs. Discrete Math. **258**, 379–381 (2002)
27. Wilson, S.E.: Operators over regular maps. Pac. J. Math. **81**, 559–568 (1979)
28. Xu, J.: A classification of regular embeddings of hypercubes Q_{2m} with m odd. Sci. China Ser. A, Math. **50**, 1673–1679 (2007)