

Regular embeddings of $K_{n,n}$ where n is a power of 2. I: Metacyclic case

SHAO-FEI DU

Department of Mathematics, Capital
Normal University
Beijing 100037, People's Republic of
China

GARETH JONES

School of Mathematics, University of Southampton
Southampton S017 1BJ, United Kingdom

JIN HO KWAK

Combinatorial and
Computational Mathematics Center
Pohang University of
Science and Technology, Pohang 790-784,
Korea

ROMAN NEDELA

Institute of Mathematics, Slovak Academy of Sciences
Severná 5, 975 49 Banská Bystrica, Slovakia

MARTIN ŠKOVIERA

Faculty of Mathematics, Physics and Informatics, Comenius University
842 48 Bratislava, Slovakia

A 2-cell embedding of a graph in an orientable closed surface is called regular if its automorphism group acts regularly on arcs of the embedded graph. The aim of this and of the associated consecutive paper is to give a classification of regular embeddings of complete bipartite graphs $K_{n,n}$, where $n = 2^e$. The method involves groups G which factorise as a product XY of two cyclic groups of order n so that the two cyclic factors are transposed by an involutory automorphism. In particular, we give a classification of such groups G . Employing the classification we investigate automorphisms of these groups, resulting in a classification of regular embeddings of $K_{n,n}$ based on that for G . We prove that given $n = 2^e$, $e \geq 3$ there are, up to map isomorphism, exactly $2^{e-2} + 4$ regular embeddings of $K_{n,n}$. Our analysis splits naturally into two cases depending on whether the group G is metacyclic or not.

1 Introduction

One of the central problems in topological graph theory is to classify all the regular embeddings in orientable surfaces of a given class of graphs. Here we are studying orientably regular embeddings of graphs, by which we mean 2-cell embeddings in oriented surfaces such that the orientation-preserving automorphism group of the resulting map acts transitively on the directed edges. The classification problem was treated in a general setting in [10]. However, for particular classes of graphs, it has been solved in only a few cases. Most notably, all regular embeddings of complete graphs K_n have been determined by James and Jones [15], showing that the regular embeddings are precisely those discovered by Biggs [1]. This classification has been extended to the ‘cocktail party’ graphs $K_n \otimes K_2$ by Nedela and Škovič [25]. More recently, the classification has been achieved for n -dimensional cubes, n odd, in [9], for complete multipartite graphs $K_n[\bar{K}_p]$, p prime, in [7], and for merged Johnson graphs in [18].

The aim of this paper is to consider a similar problem for the complete bipartite graphs $K_{n,n}$. It is well known that for each integer n , the graph $K_{n,n}$ has at least one regular embedding in an orientable surface, namely the standard embedding, described by Biggs and White [2, §5.6.7] as a Cayley map for the group \mathbb{Z}_{2n} . Nedela, Škovič and Zlatoš [28] showed that there is exactly one regular embedding of $K_{p,p}$ when p is a prime. This result was generalised by Jones et al. [19], who proved that there is a unique regular embedding of $K_{n,n}$ if and only if $\gcd(n, \phi(n)) = 1$. Note that the set of all integers n for which $K_{n,n}$ admits a unique regular embedding coincides with the set of all integers n for which there exists exactly one group of order n [19]. A different generalisation of [28] has been proved in [20], where regular embeddings of $K_{n,n}$ are classified in the case where n is odd and no primes p and q dividing n satisfy $p \equiv q \pmod{n}$. In particular, there are exactly p^{e-1} regular embeddings of K_{p^e, p^e} , where p is an odd prime. Most of these results were obtained by using a purely group-theoretical interpretation of the problem, which will also be used in the present paper. A more combinatorial approach has been taken by Kwak and Kwon in [22, 23], where they have determined all the reflexible regular embeddings of $K_{n,n}$. These embeddings had been constructed earlier by Líšková et al. in [24]. In particular, for n odd the standard embedding is the only reflexible regular embedding of $K_{n,n}$.

Our method uses the fact, proved in [19], that if \mathcal{M} is a regular orientable embedding of $K_{n,n}$ for any n , then the group $G = \text{Aut}_0^+ \mathcal{M}$ of automorphisms of \mathcal{M} , preserving orientation and vertex-colours, factorises as a product of two disjoint cyclic groups of order n . When n is an odd prime power, a result of Huppert [11] implies that such a group G must be metacyclic, and this fact was used in

[20] to classify the possibilities for G , and hence for \mathcal{M} . When n is a power of 2, however, Huppert's result does not apply, and indeed for each $e \geq 2$ there are regular embeddings of $K_{n,n}$ ($n = 2^e$) for which G is not metacyclic, so these are not direct analogues of the maps arising when p is odd. Nevertheless, the techniques used in the odd case can also be applied for $n = 2^e$ provided that one restricts to those embeddings for which G is metacyclic. The purpose of the present paper is to give a classification of regular embeddings of $K_{n,n}$ for $n = 2^e$ in the metacyclic case. The complementary non-metacyclic case will be treated in a second paper [8], using different techniques.

It is well known that the automorphism group $A = \text{Aut}(\mathcal{M})$ of a regular map is generated by a generator r of the stabiliser of a vertex v (which is necessarily cyclic) and by an involution ℓ inverting an edge incident with v , see [10]. Moreover, the embedding is determined by the group A and the choice of the generators $\langle r, \ell \rangle$ [27, 6]. A regular map given by $A = \langle r, \ell \rangle$, $\ell^2 = 1$, is called an *algebraic map* $\mathcal{M}(A; r, \ell)$. Two algebraic maps $\mathcal{M}(A; r, \ell)$ and $\mathcal{M}(A; r', \ell')$ are isomorphic if there is a group automorphism in $\text{Aut}(A)$ taking $r \rightarrow r'$ and $\ell \rightarrow \ell'$. In the particular case where the underlying graph of $\mathcal{M}(A; r, \ell)$ is $K_{n,n}$, the automorphism group $A = \text{Aut}(\mathcal{M})$ contains a subgroup of index 2 which is a product $\langle r \rangle \langle r^\ell \rangle$ of two cyclic groups. Indeed, any $y \in \langle r \rangle \cap \langle r^\ell \rangle$ fixes two adjacent vertices. Since $K_{n,n}$ is a simple graph, regularity of the action on darts gives $y = 1$, so $|G| = |\langle r, r^\ell \rangle| \geq |r||r^\ell| = n^2$. By regularity of the action $|G| = n^2$, so $G = \langle r \rangle \langle r^\ell \rangle$. Conversely, given a product of cyclic groups $G = \langle a \rangle \langle b \rangle$ admitting $\alpha \in \text{Aut}(G)$, $\alpha^2 = 1$, $a^\alpha = b$, a regular embedding of $K_{n,n}$, $n = |a| = |b|$, can be defined via the algebraic map $(A; a, \alpha)$, where A is the semidirect product $A = G \rtimes \langle \alpha \rangle$.

Thus the problem of determining the isomorphism classes of regular embeddings of complete bipartite graphs $K_{n,n}$ can be solved in two steps:

1. First we determine the products $G = \langle a \rangle \langle b \rangle$ of two cyclic groups of order n interchanged by an involutory automorphism taking a to b ;
2. Given G of the above form we consider its extension $A = \langle G, x \rangle$, where $b = a^x$, $x^2 = 1$. For each such A we determine all the generating pairs r, ℓ (up to the action of $\text{Aut}(A)$) such that $G = \langle r \rangle \langle r^\ell \rangle$, $|r| = n$, $\ell^2 = 1$.

It follows that the problem of classifying regular embeddings of $K_{n,n}$ is closely related to the problem of classifying products of cyclic groups. In the 1950s this problem attracted group theorists. Fundamental results were obtained by Wielandt in [29], by Huppert in [11], by Itô in [13, 14]. However, the classification is not yet complete. The particular case when the two cyclic factors are interchanged by an involutory group automorphism has been considered by Jones, Nedela and Škovič

[20]. The groups have been determined in the case where the order of the cyclic factors is $n = p^e$, p an odd prime, and also for many others values of n . In all cases where the solution has been achieved the groups G are metacyclic. In fact, the main obstacle to describing the groups which are products of cyclic groups is a lack of understanding of the structure of the groups in the non-metacyclic case.

The following two theorems present the main results of this and the following paper [8]. Theorem 1.4 solves the classification problem for products of cyclic groups in the case when $n = 2^e$ and the two cyclic factors are interchanged by an involutory automorphism. Theorem 1.2 describes the associated regular embeddings of $K_{n,n}$ up to isomorphism.

Theorem 1.1. *Suppose that $G = \langle a \rangle \langle b \rangle$, where $|a| = |b| = 2^e$, $\langle a \rangle \cap \langle b \rangle = 1$, and $a^\alpha = b$ for some involution α in $\text{Aut}(G)$. Then one of the following cases holds:*

(1) G is metacyclic and G has a presentation

$$G = G_1(e, f) = \langle h, g \mid h^{2^e} = g^{2^e} = 1, h^g = h^{1+2^f} \rangle$$

where $f = 2, \dots, e$, and we may set $a = g^u$ and $b = g^u h$, where u is odd and $1 \leq u \leq 2^{e-f}$;

(2) G is not metacyclic, $|G'| = 2$, and G has a presentation

$$G = G_2 = \langle a, b \mid a^4 = b^4 = 1, [b, a] = a^2 b^2, [a^2, b] = [b^2, a] = 1 \rangle;$$

(3) G is not metacyclic, $|G'| > 2$, and G has presentation

$$G = G_3(e, k, l) = \langle a, b \mid a^{2^e} = b^{2^e} = 1, c = [b, a] = a^{2+k2^{e-1}} b^{-2-k2^{e-1}}, \\ c^a = c^{-1+l2^{e-2}} a^4, c^b = c^{-1-l2^{e-2}} b^{-4} \rangle,$$

where $e \geq 3$ and $k, l \in \{0, 1\}$. Moreover, $G_3(e, 0, 1) \cong G_3(e, 1, 1)$.

The presentation in case (1) shows that the group $G = \text{Aut}_0^+ \mathcal{M}$ is a split extension of a normal subgroup $\langle h \rangle \cong C_n$ by a complement $\langle g \rangle \cong C_n$; it is a direct product of these subgroups if and only if $f = e$ (which is equivalent to taking $f = 0$), in which case $\text{Aut}^+ \mathcal{M}$ is the wreath product $C_n \wr C_2$.

Corresponding to the groups $G = G_1(e, f)$, G_2 and $G_3(e, k, l)$ in Theorem 1.4, we use $A_1(e, f, m)$, A_2 and $A_3(e, k, l)$ respectively to denote the extension of G by α , where $\alpha^2 = 1$ and $a^\alpha = b$, noting that $A_3(e, 0, 1) \not\cong A_3(e, 1, 1)$. Moreover, $A_1(e, f_1, m_1) \cong A_1(e, f_2, m_2)$ if and only if $(f_1, m_1) = (f_2, m_2)$. Now we are ready to state the second main theorem.

Theorem 1.2. *Let \mathcal{M} be a regular map whose underlying graph is the complete bipartite graph $K_{2^e, 2^e}$, $e \geq 2$.*

- (1) *If $e = 2$ then \mathcal{M} is isomorphic to $\mathcal{M}(A_1(2, 2, 1); a, \alpha)$ or $\mathcal{M}(A_2; a, \alpha)$.*
- (2) *If $e \geq 3$ then either \mathcal{M} is isomorphic to $\mathcal{M}(A_1(e, f, u); a, \alpha)$, where u is odd, $1 \leq u \leq 2^{e-f}$ and $f = 2, \dots, e$, or \mathcal{M} is isomorphic to $\mathcal{M}(A_3(e, k, l); a, \alpha)$, where $k, l \in \{0, 1\}$.*

Corollary 1.3. *The number of regular embeddings of $K_{2^e, 2^e}$ is $2^{e-2} + 4$ for each $e \geq 3$.*

It follows that for any given $e \geq 3$ there are exactly four regular embeddings of $K_{n,n}$, $n = 2^e$, with non-metacyclic groups $G \leq \text{Aut}(\mathcal{M})$; the remaining 2^{e-2} regular embeddings of $K_{n,n}$ come from metacyclic groups G . The proofs of our main results are given in two consecutive papers. In the present paper we deal with the case where G is metacyclic. The main result proved in this paper is as follows:

Theorem 1.4. *Let \mathcal{M} be a regular map whose underlying graph is the complete bipartite graph $K_{2^e, 2^e}$, $e \geq 2$. Let the colour-preserving subgroup $G \leq \text{Aut}(\mathcal{M})$ be metacyclic. Then*

- (1) *G has a presentation*

$$G = G_1(e, f) = \langle h, g \mid h^{2^e} = g^{2^e} = 1, h^g = h^{1+2^f} \rangle$$

where $f = 2, \dots, e$; moreover, $G = \langle a \rangle \langle b \rangle$, where $a = g^u$, $b = g^u h$ for some odd u such that $1 \leq u \leq 2^{e-f}$, and the assignment $a \mapsto b$ extends to an involutory group automorphism α .

- (2) *\mathcal{M} is isomorphic to $\mathcal{M}(A_1(e, f, u); a, \alpha)$, where $a = g^u$, $b = g^u h$ for some odd u such that $1 \leq u \leq 2^{e-f}$; moreover, different choices of the parameters f and u give rise to non-isomorphic maps.*

2 Preliminaries

We will assume, without further comment, that all maps we consider are orientable. If \mathcal{M} is such an embedding of $K_{n,n}$, let $\text{Aut}^+ \mathcal{M}$ be its orientation-preserving automorphism group, and let $\text{Aut}_0^+ \mathcal{M}$ be the subgroup of $\text{Aut}^+ \mathcal{M}$ preserving the two parts (regarded as sets of black and white vertices). Our method uses the following result:

Proposition 2.1. *If G is a finite group, then the following are equivalent:*

- (a) $G \cong \text{Aut}_0^+ \mathcal{M}$ for some regular orientable embedding \mathcal{M} of $K_{n,n}$;
- (b) G has cyclic subgroups $X = \langle x \rangle$ and $Y = \langle y \rangle$ of order n such that $G = XY$ and $X \cap Y = 1$, and there is an automorphism α of G transposing x and y .

Given such a group G , two maps \mathcal{M} and \mathcal{M}' corresponding to pairs (x, y) and (x', y') are isomorphic if and only if there is an automorphism of G given by $x \mapsto x'$, $y \mapsto y'$.

In these circumstances, we will say that the group G or the triple (G, x, y) is n -isobicyclic, or simply *isobicyclic* if n is understood. This result transforms our classification problem into a group-theoretic problem: given n , find all the n -isobicyclic triples (G, x, y) , and in each case find the orbits of $\text{Aut } G$ on the corresponding pairs (x, y) .

Proposition 2.1 is proved in [19], and outlined in [20], so here we will simply explain that the elements x and y of $G = \text{Aut}_0^+ \mathcal{M}$ are the orientation-preserving automorphisms of \mathcal{M} fixing a black vertex v and a white vertex w , and sending each of their neighbours to the next neighbour by following the orientation around v or w ; the automorphism α of G is induced by conjugation by the automorphism of \mathcal{M} which rotates the edge vw about its midpoint, transposing v and w .

The map \mathcal{M} in Proposition 2.1 has type $\{2m, n\}$, where m is the order of xy in G . It has $2n$ vertices, n^2 edges and n^2/m faces, so it has characteristic $2n - n^2 + n^2/m$ and genus

$$g = 1 + \frac{n}{2} \left(n - \frac{n}{m} - 2 \right) \quad (2.1)$$

Wilson's operation H_j [30] acts on regular maps by raising the rotations of edges around vertices to their j -th powers, where j is coprime to the valency. Here it acts on the maps \mathcal{M} corresponding to G by replacing the pair (x, y) with (x^j, y^j) where $\text{gcd}(j, n) = 1$. In particular, the mirror-image $\overline{\mathcal{M}} = H_{-1}(\mathcal{M})$ of \mathcal{M} corresponds to the pair (x^{-1}, y^{-1}) , so \mathcal{M} is reflexible (has an orientation-reversing automorphism) if and only if G has an automorphism inverting x and y .

Example 1. For each $n \geq 1$ the group

$$G = \langle x, y \mid x^n = y^n = [x, y] = 1 \rangle = X \times Y \cong C_n \times C_n. \quad (2.2)$$

is n -isobicyclic. Here the pair (x, y) is unique up to automorphisms of G , so this group gives rise to a unique regular embedding of $K_{n,n}$. This is the *standard embedding* $\mathcal{S}_{n,n}$ of $K_{n,n}$, in which the two sets of n vertices can be labelled with the elements of \mathbb{Z}_n so that the orientation of the surface around each vertex induces the cyclic permutation $(0, 1, \dots, n-1)$ of the labels of its neighbours. (The original

construction of this embedding, due to Biggs and White [2, §5.6.7], was as a Cayley map for the additive group \mathbb{Z}_{2n} with respect to the generators $1, 3, \dots, 2n - 1$ in that cyclic order.) We have $\text{Aut}^+ \mathcal{S}_{n,n} \cong C_n \wr C_2$, the wreath product of C_n by C_2 , that is, a split extension of a normal subgroup G by a complement $\langle \alpha \rangle \cong C_2$ which transposes X and Y . Since xy has order n , $\mathcal{S}_{n,n}$ has type $\{2n, n\}$ and genus $(n - 1)(n - 2)/2$; it is invariant under Wilson's operations H_j , where $\gcd(j, n) = 1$, and in particular it is reflexible.

The group G in Example 1 is clearly metacyclic, and Theorem 1.2 gives further regular embeddings with this property. The next two examples demonstrate the existence of regular embeddings for which G is not metacyclic; Example 2 is a single instance, which is extended in Example 3 to an infinite family.

In order to construct these examples, let \mathcal{T} denote the square tessellation $\{4, 4\}$ of the complex plane, with the Gaussian integers $a + bi \in \mathbb{Z}[i]$ as vertices. For each even integer $n = 2q \geq 2$, let \mathcal{T}_n be the reflexible torus map $\{4, 4\}_n$ obtained from \mathcal{T} by identifying points n steps apart along its Petrie paths [3, §8.6]. Equivalently, \mathcal{T}_n is the quotient $\{4, 4\}_{q,q}$ of \mathcal{T} by the group T_n of automorphisms of \mathcal{T} generated by the translations $z \mapsto z + q(1 \pm i)$ [3, §8.3]. We can take the square in \mathbb{C} with corners $\pm q, \pm qi$ as a fundamental region for T_n , and by identifying opposite sides we obtain \mathcal{T}_n as an orientable map of type $\{4, 4\}$ with $2q^2$ vertices, $4q^2$ edges and $2q^2$ faces. Its automorphism group is an extension of an abelian normal subgroup group of order $2q^2$, induced by the translations of \mathcal{T} and acting regularly on the vertices, by a dihedral group of order 8 fixing a vertex. The underlying graph is bipartite, with the vertex $a + bi$ coloured black or white as a and b have equal or opposite parity.

Example 2. When $n = 4$ the graph underlying \mathcal{T}_n is $K_{4,4}$, so \mathcal{T}_4 is a regular embedding of $K_{4,4}$, of type $\{4, 4\}$ and genus 1; it cannot be the standard embedding, since this has type $\{8, 4\}$ and genus 3. We can take x and y to be the automorphisms of \mathcal{T}_2 induced by the rotations $z \mapsto iz$ and $z \mapsto i(z - 1) + 1$ of \mathcal{T} around the vertices 0 and 1, so that $\text{Aut}_0^+ \mathcal{T}_4$ has the form

$$G = \langle x, y \mid x^4 = y^4 = [x^2, y] = [x, y^2] = 1, [x, y] = x^2 y^2 \rangle, \quad (2.3)$$

an extension of its centre $Z(G) = \langle x^2, y^2 \rangle \cong C_2 \times C_2$ by $G/Z(G) \cong C_2 \times C_2$; then $\text{Aut}^+ \mathcal{T}_4$ is an extension of G by a complement $\langle \alpha \rangle$ transposing x and y , induced by the rotation $z \mapsto 1 - z$ of \mathcal{T} around the point $1/2$. Since G has order 16 and exponent 4, if it is metacyclic then it must be an extension of C_4 by C_4 ; by mapping G onto C_4 we see from (2.3) that the only normal subgroups with quotient C_4 are the normal closures of xy and of xy^{-1} , and these are not isomorphic to C_4 since xy and xy^{-1} have order 2. Thus G is not metacyclic.

Example 3. For each even $n = 2q \geq 2$, let \mathcal{O}_n be the map obtained by applying Wilson's opposite operation [21, 30] to the torus map $\mathcal{T}_n = \{4, 4\}_n$ described above: thus we cut \mathcal{T}_n along all its edges and then rejoin adjacent pairs of faces along these edges but with the opposite orientation, so that edges and faces are preserved while vertices and Petrie polygons are interchanged. Like \mathcal{T}_n , the resulting map \mathcal{O}_n is reflexible, with the same automorphism group, and it is orientable since \mathcal{T}_n is face-bipartite. Now \mathcal{T}_n has two parallel sets of n Petrie polygons, each polygon having no edges in common with the other polygons in its own set, and one edge in common with each polygon in the other set; it follows that the vertices and edges of \mathcal{O}_n have the same incidence properties, that is, the underlying graph of \mathcal{O}_n is $K_{n,n}$. By construction, \mathcal{O}_n is a reflexible map of type $\{4, n\}$; in fact, since $\mathcal{T}_n = \{4, 4\}_n$ it follows that \mathcal{O}_n is the map $\{4, n\}_4 = \{4, 2q\}_4$ of genus $(q-1)^2 = (n-2)^2/4$, the dual of the map $\{2q, 4\}_4$ in Table 8 of [3]. Since its faces are 4-gons, \mathcal{O}_n is a minimum-genus embedding of $K_{n,n}$.

The automorphisms x and y of \mathcal{O}_n correspond to the automorphisms of \mathcal{T}_n induced by the glide-reflections $z \mapsto \pm i\bar{z} + 1$ of \mathcal{T} , moving \mathcal{T}_n one step along an orthogonal pair of Petrie polygons. It follows that

$$G = \langle x, y \mid x^n = y^n = 1, (x^2)^y = x^{-2}, (y^2)^x = y^{-2}, (xy)^2 = 1 \rangle.$$

The last relation can be written as $[x, y] = (y^{-2})^x x^{-2}$, so an equivalent presentation is

$$G = \langle x, y \mid x^n = y^n = 1, (x^2)^y = x^{-2}, (y^2)^x = y^{-2}, [x, y] = x^{-2}y^2 \rangle. \quad (2.4)$$

Thus G has a normal subgroup $N = \langle x^2, y^2 \rangle \cong C_q \times C_q$, with $G/N \cong C_2 \times C_2$, so that \mathcal{O}_n is a q^2 -sheeted covering of the spherical map $\mathcal{O}_n/N \cong \mathcal{O}_2 \cong \mathcal{S}_{2,2}$, branched over its four vertices. Now $[x, y] = x^{-2}y^2$, $[x, y]^x = x^{-2}y^{-2}$ and $[x, y]^y = x^2y^2$, so the commutator subgroup G' is the subgroup $\langle x^2y^2, x^{-2}y^2 \rangle$ of index $\gcd(2, q)$ in N . If $n > 4$ then G' is not cyclic, so G cannot be metacyclic; this is also true when $n = 4$ since \mathcal{O}_4 is isomorphic to the map \mathcal{T}_4 in Example 2. In particular, for each $n = 2^e \geq 4$ we obtain a regular embedding of $K_{n,n}$ for which G is not metacyclic.

3 Normal subgroups

We now start the proof of Theorem 1.4. Suppose that G is n -isobicyclic for some $n \geq 1$. For each m dividing n , let X_m and Y_m denote the unique subgroups of order m in X and Y . Let X^* denote the core $\bigcap_{g \in G} X^g$ of X in G , the kernel of the

action of G on the black vertices. By a result of Douglas [5] and Itô [14] (see also [12, VI.10.1(a)]), this normal subgroup of G is non-trivial, and the same applies to the core $Y^* = (X^*)^\alpha$ of Y in G . Since the commutator of two normal subgroups is contained in their intersection, we have $[X^*, Y^*] \leq X^* \cap Y^* \leq X \cap Y = 1$; thus X^* and Y^* commute and therefore generate $X^* \times Y^*$, which is a normal subgroup of $\text{Aut}^+ \mathcal{M}$.

Suppose from now on that $n = 2^e$ for some integer $e \geq 2$, so $|G| = n^2 = 2^{2e}$. Since X^* and Y^* are non-trivial cyclic 2-groups, they have unique subgroups X_2 and Y_2 of order 2; these are central subgroups of G and generate a subgroup $Z_1 = X_2 \times Y_2$ which is central in G and normal in $\text{Aut}^+ \mathcal{M}$. Now G/Z_1 is \bar{n} -isobicyclic where $\bar{n} = n/2$, so factoring out Z_1 and iterating this argument, we obtain a central series $1 = Z_0 < Z_1 < Z_2 < \dots < Z_e = G$ of subgroups $Z_i = X_{2^i} Y_{2^i}$ of order 2^{2i} in G , where ‘central’ means that $Z_{i+1}/Z_i \leq Z(G/Z_i)$ for all i . (Note that for $i > 1$, Z_i need not be the direct product of X_{2^i} and Y_{2^i} : see Example 2, for instance, with $i = 2$.)

There is an alternative description of these subgroups Z_i . Since G is a 2-generator 2-group, its Frattini subgroup $\Phi = \Phi(G)$ (the intersection of its maximal subgroups) has quotient $G/\Phi \cong C_2 \times C_2$ [12, III.3.14, III.3.15]. Now $\Phi = G'G^2$, where G' is the commutator subgroup and G^2 is generated by the squares [12, III.3.14], so Φ contains $X^2 Y^2 = X_{2^{e-1}} Y_{2^{e-1}} = Z_{e-1}$; since $|\Phi| = 2^{2(e-1)} = |Z_{e-1}|$ we have $\Phi = Z_{e-1}$. Indeed, since $X^2 Y^2 \leq G^2 \leq \Phi$ we also have $Z_{e-1} = G^2$. One can apply the same argument to Φ , which is $n/2$ -isobicyclic; iterating, we see that $Z_{i-1} = \Phi(Z_i) = Z_i^2$ for all i , so each Z_i is the subgroup $G^{2^{e-i}}$ of G generated by the 2^{e-i} -th powers. In particular, all n -th powers are equal to 1, so G has exponent dividing n ; since x has order n , the exponent is equal to n . To summarise, we have proved:

Lemma 3.1. *G has a central series $1 = Z_0 < Z_1 < Z_2 < \dots < Z_e = G$ of subgroups $Z_i = X_{2^i} Y_{2^i} = G^{2^{e-i}}$ of order 2^{2i} , with $Z_{i-1} = \Phi(Z_i) = Z_i^2$ and $Z_i/Z_{i-1} \cong C_2 \times C_2$ for each $i = 1, \dots, e$. □*

Corollary 3.2. *G has exponent n . □*

4 The structure of G

From now on we will assume that G is metacyclic.

Proposition 4.1. *G has a presentation*

$$G = \langle g, h \mid g^n = h^n = 1, h^g = h^r \rangle \quad (4.1)$$

with r odd.

Proof. Proposition 2.1 implies that $|G| = |X| \cdot |Y| = n^2 = 2^{2e}$, so G is a 2-group. By our hypothesis, G is metacyclic. The general form for a metacyclic p -group is given in [12, III.11.2], so putting $p = 2$ we find that G has a presentation

$$\langle g, h \mid h^{2^i} = 1, g^{2^j} = h^{2^k}, h^g = h^r \rangle \quad (4.2)$$

where $0 \leq k \leq i$, $r^{2^j} \equiv 1 \pmod{2^i}$ and $2^k(r-1) \equiv 0 \pmod{2^i}$, so G has a normal subgroup $H = \langle h \rangle \cong C_{2^i}$ with $G/H \cong C_{2^j}$, and $|G| = 2^{i+j}$. In our case we have $|G| = n^2 = 2^{2e}$, so $i+j = 2e$. We showed in Corollary 3.2 that G has exponent n , and since h has order 2^i it follows that $i \leq e$, so $i \leq j$. Similarly, since g has order 2^{i+j-k} we have $i+j-k \leq e$, so $k \geq (i+j)/2 \geq i$; however, $k \leq i$, so $k = i$ and hence $(i+j)/2 = i$ giving $i = j = e$. Thus G has the presentation given in (4.1). Since $r^{2^e} \equiv 1 \pmod{2^e}$, r is odd. \square

This result shows that G is a split extension of $H = \langle h \rangle$ by $\langle g \rangle$, both of them cyclic groups of order n . In order to find a canonical presentation for G , and to study its structure more deeply, we need to know the multiplicative orders of certain units in \mathbb{Z}_n . Let the notation $2^k \parallel m$ indicate that 2^k is the highest power of 2 dividing an integer m .

Lemma 4.2. *If $2^k \parallel u \pm 1$ where $k \geq 2$ then $2^{k+i} \parallel u^{2^i} - 1$ for all $i \geq 1$.*

Proof. We can write $u = \pm 1 + s2^k$ with s odd and $k \geq 2$. Then $u^2 - 1 = s2^{k+1}(\pm 1 + s^2 2^{k-1})$, so $2^{k+1} \parallel u^2 - 1$. Iterating this argument gives $2^{k+i} \parallel u^{2^i} - 1$ for all $i \geq 1$. \square

Corollary 4.3. *If $2^f \parallel u - 1$ where $2 \leq f \leq e$, or if $2^f \parallel u + 1$ where $2 \leq f < e$, then u has multiplicative order 2^{e-f} in \mathbb{Z}_{2^e} .*

Proof. Putting $k = f$ in Lemma 4.2 gives $2^{f+i} \parallel u^{2^i} - 1$ for all $i \geq 1$, so if $f < e$ then $u^{2^{e-f}} \equiv 1 \pmod{2^e}$; thus the order of u divides 2^{e-f} , and is equal to 2^{e-f} since Lemma 4.2 also gives $u^{2^{e-f-1}} \not\equiv 1 \pmod{2^e}$. The case where $2^f \parallel u - 1$ with $f = e$ is trivial. \square

Proposition 4.4. *Either*

$$G = G_f := \langle g, h \mid g^n = h^n = 1, h^g = h^{1+2^f} \rangle \quad (4.3)$$

or

$$G = H_f := \langle g, h \mid g^n = h^n = 1, h^g = h^{-1+2^f} \rangle \quad (4.4)$$

for some $f = 2, \dots, e$.

Proof. If replace g in presentation (4.1) with another generator $g' = g^i$ of $\langle g \rangle$, where i is odd, we obtain the same presentation for G , except that in the final relation r is replaced with $r' = r^i$. Two units $r, r' \in \mathbb{Z}_n$ satisfy $r' = r^i$ (where i is odd) if and only if they generate the same subgroup of the multiplicative group U_n of units mod (n) . Since $n = 2^e$ we have $U_n = \langle -1 \rangle \times V_n$, with $V_n = \langle 5 \rangle \cong C_{2^{e-2}}$ consisting of the units congruent to 1 mod (4) [16, Theorem 6.10]. Writing $r = \delta v$ and $r' = \delta' v'$, with $\delta, \delta' \in \langle -1 \rangle$ and $v, v' \in V_n$, we see that $\langle r' \rangle = \langle r \rangle$ if and only if $\delta' = \delta$ and $\langle v' \rangle = \langle v \rangle$. Since V_n is cyclic, this last condition is equivalent to v' and v having the same multiplicative order, and since they are both congruent to 1 mod (4) , Corollary 4.3 implies that this is equivalent to $v' - 1$ and $v - 1$ being divisible by the same power of 2. By a suitable choice of i we may therefore replace r with $q := \pm 1 + 2^f$ for some $f = 2, \dots, e$, so that (renaming the generators) we have $h^g = h^q$ and $G = G_f$ or H_f as in (4.3) or (4.4). \square

These groups are all non-abelian, apart from $G_e \cong C_n \times C_n$. Note also that G_f is the group denoted by $G_1(e, f)$ in Theorems 1.1 and 1.4; for convenience we will retain the notation G_f from now on. For similar reasons we write H_f instead of $H_1(e, f)$.

If $G = G_f$ then $[h, g] = h^{2^f}$, which generates a normal subgroup of order 2^{e-f} ; since $G = \langle g, h \rangle$, G' is the normal closure of $[h, g]$, which therefore coincides with this subgroup. This shows that for a given $n = 2^e$, the different groups G_f can be distinguished from each other by the fact that $|G'_f| = 2^{e-f}$. The groups H_f are of less interest here since, as we shall eventually prove in Corollary 5.5, they are not isobicyclic, so they do not arise from regular embeddings of $K_{n,n}$.

For each $i = 0, 1, \dots$, the subgroup $\langle g^{2^i}, h^{2^i} \rangle$ of G is a semidirect product of $\langle h^{2^i} \rangle$ by $\langle g^{2^i} \rangle$, both cyclic of order 2^{e-i} , so it has index 2^{2i} in G . Being generated by 2^i -th powers, it is contained in G^{2^i} ; but we saw in Lemma 4.2 that G^{2^i} also has index 2^{2i} , so

$$\langle g^{2^i}, h^{2^i} \rangle = G^{2^i} = Z_{e-i}.$$

Each element of G can be written uniquely in the standard form $g^i h^j$ where $i, j \in \mathbb{Z}_n$. Multiplication of standard forms is given by

$$g^i h^j \cdot g^k h^l = g^{i+k} (h^j)^{g^k} h^l = g^{i+k} h^{jq^k+l}, \quad (4.5)$$

since $(h^j)^{g^k} = (h^{g^k})^j = h^{jq^k}$.

An element $g^i h^j$ is central in G if and only if g^i commutes with h and h^j commutes with g . Since $h^{g^i} = h^{q^i}$ and $(h^j)^g = h^{jq}$ this happens if and only if

$q^i \equiv 1$ and $jq \equiv j \pmod{n}$. If $G = G_f$, this is equivalent to $2^{e-f} \mid i$ (by Lemma 4.2) and $2^{e-f} \mid j$, so G_f has centre

$$Z(G_f) = \langle g^{2^{e-f}}, h^{2^{e-f}} \rangle = Z_f \cong C_{2^f} \times C_{2^f}. \quad (4.6)$$

Powers in G are given by

$$\begin{aligned} (g^i h^j)^m &= g^{im} (h^j)^{g^{i(m-1)}} (h^j)^{g^{i(m-2)}} \dots (h^j)^{g^i} h^j \\ &= g^{im} h^{j(q^{i(m-1)} + q^{i(m-2)} + \dots + q^i + 1)} = g^{im} h^{j(q^{im} - 1)/(q^i - 1)}. \end{aligned} \quad (4.7)$$

5 Generating pairs for G

Let \mathcal{P} denote the set of all pairs $(x, y) \in G \times G$ such that the subgroups $X = \langle x \rangle$ and $Y = \langle y \rangle$ satisfy $G = XY$ and $X \cap Y = 1$, and let \mathcal{B} be the subset consisting of those pairs where x and y are transposed by an automorphism of G . By Proposition 2.1, the regular embeddings of $K_{n,n}$ associated with G correspond to the orbits of $\text{Aut } G$ on \mathcal{B} . Our strategy is first to find \mathcal{P} , then by finding the automorphisms of G to determine \mathcal{B} , and finally to find the orbits of $\text{Aut } G$ on \mathcal{B} . The following technical result enables us to determine \mathcal{P} .

Proposition 5.1. *Let $m := 2^{e-1}$. Then*

$$(g^i h^j)^m = \begin{cases} g^{im} h^{jm} & \text{if } G = G_f \text{ or } i \text{ is even,} \\ g^{im} & \text{if } G = H_f \text{ and } i \text{ is odd.} \end{cases}$$

Proof. By equation (4.7) we have

$$(g^i h^j)^m = g^{im} h^{j(q^{im} - 1)/(q^i - 1)}.$$

Suppose first that $q^i \equiv 1 \pmod{4}$, that is, either $q = 1 + 2^f$, or $q = -1 + 2^f$ and i is even. Then $2^k \parallel q^i - 1$ for some $k \geq 2$, so Lemma 4.2 gives $2^{k+e-1} \parallel q^{im} - 1$, and hence $2^{e-1} \parallel (q^{im} - 1)/(q^i - 1)$; thus the exponent of h in $(g^i h^j)^m$ is 0 or m as j is even or odd, so $(g^i h^j)^m = g^{im} h^{jm}$. Now suppose that $q^i \equiv -1 \pmod{4}$, that is, $q = -1 + 2^f$ and i is odd. Then Lemma 4.2 shows that $2^{e+1} \mid q^{im} - 1$, so $2^e \mid (q^{im} - 1)/(q^i - 1)$ and the exponent of h in $(g^i h^j)^m$ is 0. \square

Corollary 5.2. *The elements of order n in G are those in $G \setminus \Phi$.*

Proof. Since G has exponent $n = 2^e$, the elements of order n are those with non-identity m -th powers. The result therefore follows immediately from Proposition 5.1.

□

In fact, Proposition 5.1 shows that if $G = G_f$ then taking m -th powers induces an isomorphism $\mu : G/\Phi \rightarrow Z_1 = \langle g^m, h^m \rangle$ given by $g^i h^j \Phi \mapsto (g^i h^j)^m = g^{im} h^{jm}$; however, μ is not a homomorphism if $G = H_f$. Corollary 5.2 fails if we do not assume that G is metacyclic, as shown by Example 2, where the element $xy \in G \setminus \Phi$ has order 2, not 4.

We now consider when the cyclic subgroups generated by two elements of order n have trivial intersection (or are *disjoint* in the rather imprecise group-theoretic terminology).

Corollary 5.3. *Elements a and b of order n in G generate disjoint subgroups if and only if their images form a basis for G/Φ , and in addition $\{a\Phi, b\Phi\} \neq \{g\Phi, gh\Phi\}$ when $G = H_f$.*

Proof. The cyclic subgroups $A = \langle a \rangle$ and $B = \langle b \rangle$ are disjoint if and only if their subgroups $A_2 = A^m$ and $B_2 = B^m$ of order 2, contained in Z_1 , are disjoint. If $G = G_f$ then $\mu : G/\Phi \rightarrow Z_1$ is an isomorphism, so this is equivalent to A and B having disjoint images in G/Φ , that is, to $a\Phi$ and $b\Phi$ generating G/Φ . If $G = H_f$ the result follows from Corollary 5.2. □

Recall that a *characteristic* subgroup of a group G is one which is invariant under all automorphisms of G .

Proposition 5.4. *If G is non-abelian then $H\Phi$ is a characteristic subgroup of G .*

Proof. Any $\theta \in \text{Aut } G$ must preserve Φ and must send the normal subgroup $H = \langle h \rangle$ to a cyclic normal subgroup J of order n . If $J\Phi \neq H\Phi$ then Corollary 5.3 implies that H and J are disjoint subgroups of G , so $|HJ| = |H||J|/|H \cap J| = n^2 = |G|$ and hence $G = HJ$. Since H and J are normal subgroups of G we have $[H, J] \leq H \cap J = 1$ and hence $G = H \times J$. Thus G is abelian, against our assumption, so $J\Phi = H\Phi$ as required. □

Corollary 5.5. *The groups H_f are not isobicyclic.*

Proof. If H_f is isobicyclic then some pair $(x, y) \in \mathcal{P}$ must be transposed by an automorphism α of H_f . By Corollary 5.3, exactly one of the cosets $x\Phi$ and $y\Phi$ coincides with $h\Phi$. However, $h\Phi$ is invariant under α by Proposition 5.4, since H_f is non-abelian, so α cannot transpose x and y . □

Having excluded the groups H_f , we may assume from now on that $G = G_f$ for some $f = 2, \dots, e$, so $q = 1 + 2^f$.

Proposition 5.6. *We have*

$$\mathcal{P} = \{(x, y) \in G \times G \mid G/\Phi = \langle x\Phi, y\Phi \rangle\} = \{(g^i h^j, g^k h^l) \in G \times G \mid il - jk \not\equiv 0 \pmod{2}\}.$$

Proof. By Corollary 5.2, the cyclic subgroups X and Y of order n in G are those generated by elements $x, y \in G \setminus \Phi$. By Corollary 5.3, such subgroups are disjoint if and only if $x\Phi$ and $y\Phi$ generate G/Φ , or equivalently $x = g^i h^j$ and $y = g^k h^l$ with $il - jk \not\equiv 0 \pmod{2}$. For each such pair x, y we have $|XY| = |X||Y|/|X \cap Y| = n^2 = |G|$, so $G = XY$. Thus \mathcal{P} consists of all such pairs (x, y) . \square

Corollary 5.7. $|\mathcal{P}| = 3 \cdot 2^{4e-3}$.

Proof. We use Proposition 5.6 to count the pairs $(x, y) \in \mathcal{P}$: there are $|G \setminus \Phi| = 2^{2e} - 2^{2e-2} = 3 \cdot 2^{2e-2}$ choices for x , and each is paired with $|G \setminus X\Phi| = 2^{2e} - 2^{2e-1} = 2^{2e-1}$ elements y , so $|\mathcal{P}| = 3 \cdot 2^{4e-3}$. \square

6 Automorphisms of G

Recall that \mathcal{B} consists of those pairs $(x, y) \in \mathcal{P}$ where x and y are transposed by an automorphism of G , and that the regular embeddings of $K_{n,n}$ associated with G correspond to the orbits of $\text{Aut } G$ on \mathcal{B} . Since $G = \langle x, y \rangle$ for each pair $(x, y) \in \mathcal{P}$, $\text{Aut } G$ acts semiregularly on \mathcal{P} , and hence on \mathcal{B} , with orbits of length $|\text{Aut } G|$. First we deal with the case $f = e$.

Proposition 6.1. *The group $G = G_e$ corresponds to a single regular embedding of $K_{n,n}$, namely the standard embedding $\mathcal{S}_{n,n}$.*

Proof. If $G = G_e \cong C_n \times C_n$ then $\text{Aut } G \cong GL_2(\mathbb{Z}_n)$, of order $3 \cdot 2^{4e-3} = |\mathcal{P}|$, so $\text{Aut } G$ acts transitively on \mathcal{P} ; all pairs $(x, y) \in \mathcal{P}$ are transposed by an automorphism (since one pair (g, h) is), so $\mathcal{B} = \mathcal{P}$ and G corresponds to a unique regular embedding. Since $\mathcal{M} = \mathcal{S}_{n,n}$ has $\text{Aut}_0^+ \mathcal{M} \cong C_n \times C_n$, this is the corresponding map. \square

By Proposition 6.1, we may assume for the rest of this section that $f \neq e$, so $G = G_f$ for some $f = 2, \dots, e-1$. Thus G is non-abelian, and $H\Phi = \langle g^2, h \rangle$ is a characteristic subgroup of G by Proposition 5.4.

We will consider the automorphisms of G through their induced actions as linear transformations of G/Φ , regarded as a 2-dimensional vector space over \mathbb{Z}_2 . Each $\theta \in \text{Aut } G$ sends g, h to some pair $g' = g^i h^j, h' = g^k h^l$, so it is represented on G/Φ as the matrix $A = \begin{pmatrix} i & j \\ k & l \end{pmatrix} \in GL_2(\mathbb{Z}_2)$ with respect to the basis $\{g\Phi, h\Phi\}$. (Here we abuse the notation by identifying the exponents $i, j, k, l \in \mathbb{Z}_n$ with their images in \mathbb{Z}_2 .) Since A is invertible, $il - jk \not\equiv 0 \pmod{2}$. Since G is non-abelian, Proposition 5.4 implies that the 1-dimensional subspace $H\Phi/\Phi$ is invariant under $\text{Aut } G$, so $k \equiv 0 \pmod{2}$ and hence $i, l \not\equiv 0 \pmod{2}$.

Proposition 6.2. *The automorphisms of G are the mappings given by $g \mapsto g^i h^j, h \mapsto g^k h^l$ where $i, j, k, l \in \mathbb{Z}_n$ with $i \equiv 1 \pmod{2^{e-f}}, k \equiv 0 \pmod{2^{e-f}}$, and $l \not\equiv 0 \pmod{2}$.*

Proof. Any automorphism θ of G sends g and h to $g' = g^i h^j$ and $h' = g^k h^l$, where $i \not\equiv 0 \pmod{2}$ and $k \equiv 0 \not\equiv l \pmod{2}$ by Propositions 5.4 and 5.6. Any such pair g', h' generate G by the Burnside Basis Theorem [12, III.3.15], since their images generate G/Φ ; they both have order n by Corollary 5.2, so the mapping $g \mapsto g', h \mapsto h'$ determines an automorphism of G if and only if $(h')^{g'} = (h')^q$, corresponding to the final relation in (4.3). Now

$$(h')^{g'} = (g^k h^l)^{g^i h^j} = (g^k)^{g^i h^j} (h^l)^{g^i h^j} = (g^k)^{h^l} (h^l)^{g^i} \in g^k H,$$

and

$$(h')^q = (g^k h^l)^q \in g^{kq} H,$$

so if θ is an automorphism then $kq \equiv k \pmod{2^e}$; since $q = 1 + 2^f$ this is equivalent to $k \equiv 0 \pmod{2^{e-f}}$, that is, $g^k \in Z(G)$ by (4.6). In this case

$$(h')^{g'} = g^k (h^l)^{g^i} = g^k h^{lq^i} \quad \text{and} \quad (h')^q = g^{kq} h^{lq} = g^k h^{lq},$$

so θ is an automorphism if and only if $lq \equiv lq^i \pmod{2^e}$, that is, $q^{i-1} \equiv 1 \pmod{2^e}$ since l is odd, or equivalently $i \equiv 1 \pmod{2^{e-f}}$ by Corollary 4.3. \square

Corollary 6.3. $|\text{Aut } G| = 2^{2e+2f-1}$.

Proof. In Proposition 6.2, the number of choices for each of i, j, k and l is $2^f, 2^e, 2^f$ and 2^{e-1} respectively, and multiplying these gives the number of automorphisms. \square

Not every involution in $\text{Aut } G$ transposes a pair $(x, y) \in \mathcal{P}$: for instance, the inner automorphisms act trivially on G/Φ , since $G' \leq \Phi$, and these include involutions since G is a non-abelian 2-group. For those involutions which do transpose such a pair, we have:

Corollary 6.4. *Any involution $\alpha \in \text{Aut } G$ which transposes a pair $(x, y) \in \mathcal{P}$ is represented on G/Φ as the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_2)$ with respect to the basis $\{g\Phi, h\Phi\}$.*

Proof. Since $x\Phi$ and $y\Phi$ generate G/Φ , α induces an automorphism of order 2 on G/Φ . By Proposition 5.4, α leaves $H\Phi/\Phi$ invariant, so the result follows. \square

7 Proof of the classification theorems, the metacyclic case

We will first count the regular embeddings of $K_{n,n}$ corresponding to $G = G_f$ for each f . By Proposition 2.1, this is equivalent to counting the orbits of $\text{Aut } G$ on \mathcal{B} . First let $f < e$. By Proposition 6.2, the automorphisms θ of G are given by $g \mapsto g^i h^j$, $h \mapsto g^k h^l$, where $i \equiv 1$, $k \equiv 0 \pmod{2^{e-f}}$ and $l \not\equiv 0 \pmod{2}$; thus $g^{i-1}, g^k \in Z = Z(G)$ by (4.6), and hence θ sends an arbitrary element $x = g^u h^v$ of G to

$$g^{u'} h^{v'} = (g^i h^j)^u (g^k h^l)^v = g^{(i-1)u+kv} (gh^j)^u h^{lv} = g^{iu+kv} h^{j(q^{u-1}+\dots+q+1)+lv} \quad (7.1)$$

by (4.7). If $(x, y) \in \mathcal{B}$ for some $y \in G$ then $x \notin H\Phi$ by Proposition 5.4 and Corollary 6.4, or equivalently $u \not\equiv 0 \pmod{2}$. Since $q \equiv 1 \pmod{2}$ we have $q^{u-1} + \dots + q + 1 \equiv u \pmod{2}$, so if $x \notin H\Phi$ then $q^{u-1} + \dots + q + 1$ is a unit mod (n) . For any such x , by choosing a suitable value of j we can therefore find some $\theta \in \text{Aut } G$ so that v' takes any given value in \mathbb{Z}_n ; similarly, with suitable i and k we can also have any $u' \equiv u \pmod{2^{e-f}}$, so the orbit of x under $\text{Aut } G$ is the coset xHZ of $HZ = \langle g^{2^{e-f}}, h \rangle$, of size $|HZ| = 2^{e+f}$.

Let $\mathcal{B}(x) = \{y \in G \mid (x, y) \in \mathcal{B}\}$ and $\mathcal{P}(x) = \{y \in G \mid (x, y) \in \mathcal{P}\}$, so $\mathcal{B}(x) \subseteq \mathcal{P}(x)$. By definition of \mathcal{B} , each $y \in \mathcal{B}(x)$ is an image of x under $\text{Aut } G$, so $\mathcal{B}(x) \subseteq xHZ \cap \mathcal{P}(x)$. Now xHZ consists of the elements $y = g^{u'} h^{v'}$ with $u' \equiv u \pmod{2^{e-f}}$; by Proposition 5.6, $(x, y) \in \mathcal{P}$ if and only if $uv' - vu' \not\equiv 0 \pmod{2}$, or equivalently $v' \not\equiv v \pmod{2}$, since $u' \equiv u \not\equiv 0 \pmod{2}$, so

$$xHZ \cap \mathcal{P}(x) = \{g^{u'} h^{v'} \mid u' \equiv u \pmod{2^{e-f}}, v' \not\equiv v \pmod{2}\}. \quad (7.2)$$

Counting values of u' and v' we have $|xHZ \cap \mathcal{P}(x)| = 2^f(2^e - 2^{e-1}) = 2^{e+f-1}$. Now $\text{Aut } G$ has order $2^{2e+2f-1}$ by Corollary 6.3, and its orbit xHZ containing x has length 2^{e+f} , so the stabiliser $(\text{Aut } G)_x$ of x in $\text{Aut } G$ has order 2^{e+f-1} ; this subgroup acts semi-regularly on $\mathcal{P}(x)$, and preserves the coset xHZ , so by comparing orders we see that it acts regularly on $xHZ \cap \mathcal{P}(x)$.

As a representative of the orbit xHZ of $\text{Aut } G$ we can choose $x = g^u$ for some unique odd $u = 1, \dots, 2^f$ (so $v = 0$); then the element $y = g^u h$ is in $xHZ \cap \mathcal{P}(x)$

by (7.2). By Proposition 6.1, putting $i = 1$, $j(q^{u-1} + \cdots + q + 1) = 1$, $k = 0$ and $l = -1$ in \mathbb{Z}_n gives an automorphism $\alpha : g \mapsto gh^j$, $h \mapsto h^{-1}$ of G , this choice of j being possible since $q^{u-1} + \cdots + q + 1$ is a unit mod (n) . Then (7.1) gives $x\alpha = y$ and $y\alpha = x$, so α is an involution since $G = \langle x, y \rangle$. Thus $(x, y) \in \mathcal{B}$, so $\mathcal{B}(x)$ is non-empty. Now $\mathcal{B}(x)$ is a subset of $xHZ \cap \mathcal{P}(x)$, invariant under $(\text{Aut } G)_x$, and $(\text{Aut } G)_x$ acts transitively on $xHZ \cap \mathcal{P}(x)$, so $\mathcal{B}(x) = xHZ \cap \mathcal{P}(x)$. Since this equation is satisfied by one element $x = g^u$ of the orbit xHZ of $\text{Aut } G$, it is satisfied by every element x of this orbit. This is true for all odd u , so

$$\mathcal{B} = \{(g^u h^v, g^{u'} h^{v'}) \mid u \not\equiv 0 \pmod{2}, u' \equiv u \pmod{2^{e-f}} \text{ and } v' \not\equiv v \pmod{2}\}. \quad (7.3)$$

Moreover, this argument shows that two pairs $(x, y) \in \mathcal{B}$ are in the same orbit of $\text{Aut } G$ if and only if their corresponding values of u are congruent mod (2^{e-f}) , and that we can take the pairs $(g^u, g^u h)$ with odd $u = 1, \dots, 2^{e-f}$ as representatives of these orbits. It follows that there are $\phi(2^{e-f})$ orbits of $\text{Aut } G$ on \mathcal{B} , so by Proposition 2.1 this is the number of regular embeddings of $K_{n,n}$ associated with $G = G_f$ for each $f = 2, \dots, e-1$. This is also valid for $f = e$ by Proposition 6.1, since $\phi(1) = 1$. Summing over all f , we have a total of

$$\sum_{f=2}^e \phi(2^{e-f}) = 2^{e-3} + 2^{e-4} + \cdots + 2 + 1 + 1 = 2^{e-2}$$

regular embeddings of $K_{n,n}$.

Since xy has order n (being an element of $G \setminus \Phi$), these maps \mathcal{M} all have type $\{2n, n\}$ and hence have genus $(n-1)(n-2)/2$. In each case, $\text{Aut}^+ \mathcal{M}$ is a split extension of a normal subgroup $G = \text{Aut}_0^+ \mathcal{M}$ by a complement $\langle \alpha \rangle \cong C_2$, where the automorphism α of \mathcal{M} reverses the edge joining the vertices fixed by x and y ; thus α acts by conjugation on G as the automorphism $\alpha \in \text{Aut } G$ transposing $x = g^u$ and $y = g^u h$, so we obtain the presentation for $\text{Aut}^+ \mathcal{M}$ in Theorem 1.4(1). Since $(\text{Aut } G)_x$ acts transitively on $\mathcal{B}(x)$, there is a single conjugacy class of involutions in $\text{Aut } G$ transposing pairs $(x, y) \in \mathcal{B}$, so the groups $\text{Aut}^+ \mathcal{M}$ corresponding to the 2^{e-f-1} maps \mathcal{M} associated with each G_f are all isomorphic.

Wilson's operations H_j ($j \in U_n$) permute the regular embeddings of $K_{n,n}$, preserving G and replacing (x, y) with (x^j, y^j) . For each f , if we let \mathcal{M}_u denote the regular embedding associated with the pair $(g^u, g^u h)$ then H_j sends \mathcal{M}_u to \mathcal{M}_{ju} , where we regard these subscripts as units mod (2^{e-f}) . For a given f these $\phi(2^{e-f})$ maps \mathcal{M}_u therefore form a single orbit under the operations H_j , which confirms that their groups $\text{Aut}^+ \mathcal{M}_u$ are all isomorphic. A map \mathcal{M}_u is reflexible if and only if it is isomorphic to $H_{-1}(\mathcal{M}_u) = \mathcal{M}_{-u}$, or equivalently $u \equiv -u \pmod{2^{e-f}}$; this happens

only if $f = e$, corresponding to $\mathcal{M}_u = \mathcal{S}_{n,n}$, or $f = e - 1$, whereas for $f < e - 1$ the maps \mathcal{M}_u are all chiral. \square

8 Comments on the classification

The involution α centralises and inverts the elements $r = xy$ and $x^{-1}y$ of order n , giving cyclic and dihedral subgroups $R = \langle \alpha, r \rangle$ of order $2n$ in $\text{Aut}^+ \mathcal{M}$. Corollary 5.3 implies that each R is disjoint from X , so it has an orbit of length $|R : R \cap X| = 2n$ on the vertices and thus permutes them regularly. Each \mathcal{M}_u is therefore a Cayley map for both the cyclic and dihedral groups R of order $2n$ with respect to the generating sets $R \setminus \langle r \rangle$.

The normal subgroup $H = \langle x^{-1}y \rangle$ of $\text{Aut} \mathcal{M}$ acts semi-regularly on the vertices and edges of \mathcal{M} , and has two orbits of length $n/2$ on the faces, so \mathcal{M}/H has two vertices, n edges and two faces. This map is the regular embedding $M(n, 1)$ of a dipole D_n in the notation of [25, 26]. The regular covering $\mathcal{M} \rightarrow \mathcal{M}/H$ is branched over its two face-centres, and is unbranched elsewhere.

The group $\text{Ex} \mathcal{M}$ of exponents of a map \mathcal{M} of valency n consists of those $j \in U_n$ such that $H_j(\mathcal{M}) \cong \mathcal{M}$ [27]. Here, writing $\mathcal{M} = \mathcal{M}_u$ we see that $j \in \text{Ex} \mathcal{M}$ if and only if $ju \equiv u \pmod{(2^{e-f})}$, or equivalently $j \equiv 1 \pmod{(2^{e-f})}$. If $f = e$ or $e - 1$ then $\text{Ex} \mathcal{M} = U_n$, whereas if $2 \leq f \leq e - 2$ then $\text{Ex} \mathcal{M}$ is a proper subgroup of index 2^{e-1-f} and order 2^f in U_n . Thus if $e \geq 3$ then $K_{n,n}$ has $e - 2$ non-isomorphic exponent groups for its regular embeddings; as in the odd prime-power case [20] this solves Problem 3 of [27], which asks whether the exponent group for a given graph is unique.

The *Petrie dual* $P(\mathcal{M})$ of a map \mathcal{M} has the same underlying graph, but its faces are bounded by the Petrie polygons of \mathcal{M} [3, 21, 30]. Here, the operation P corresponds to replacing $(x, y) \in \mathcal{B}$ with (x, y^{-1}) . If $f = e$ or $e - 1$ then it follows from (7.3) that $(x, y^{-1}) \in \mathcal{B}$, so $P(\mathcal{M})$ is a regular embedding of $K_{n,n}$, isomorphic to \mathcal{M} by the uniqueness of \mathcal{M} for these values of f . If $f < e - 1$, however, $P(\mathcal{M})$ is not a regular map since $(x, y^{-1}) \notin \mathcal{B}$ by (7.3), though it is an edge-transitive orientable embedding of $K_{n,n}$.

If, instead of regular embeddings of $K_{n,n}$, we look for those for which the group $G = \text{Aut}_0^+ \mathcal{M}$ acts transitively (and thus regularly) on the edges, then a simple modification of Proposition 2.1 (omitting the automorphism α) shows that the maps \mathcal{M} associated with G correspond to the orbits of $\text{Aut} G$ on \mathcal{P} . Moreover, the analysis

in Sections 3 and 4 shows that the only metacyclic groups G which can occur are the groups G_f and H_f defined in Proposition 4.4 for $f = 2, \dots, e$: the existence of α is used only to eliminate the groups H_f in the regular case (Corollary 5.5). It follows from Corollaries 5.7 and 6.3 that if $f < e$ then G_f contributes

$$\frac{3 \cdot 2^{4e-3}}{2^{2e+2f-1}} = 3 \cdot 2^{2(e-f-1)}$$

orbits; of these, 2^{e-f-1} are in \mathcal{B} , each corresponding to a single regular embedding, while the remaining $(3 \cdot 2^{e-f-1} - 1)2^{e-f-1}$ orbits in $\mathcal{P} \setminus \mathcal{B}$ correspond in pairs (transposed by reversing the vertex-colours) to $(3 \cdot 2^{e-f-1} - 1)2^{e-f-2}$ non-regular embeddings, giving a total of $(3 \cdot 2^{e-f-1} + 1)2^{e-f-2}$ embeddings. The proof of Proposition 6.1 shows that G_e contributes just one orbit, corresponding to the standard embedding. In the case of H_f , it follows from Corollaries 5.2 and 5.3 that $|\mathcal{P}| = 2^{4e-2}$, while an argument similar to that in Proposition 6.2 and Corollary 6.3 (but with $q = -1 + 2^f$) shows that $|\text{Aut } G| = 2^{2e+f}$ or 2^{3e-1} as $f < e$ or $f = e$; thus H_f contributes 2^{2e-f-2} or 2^{e-1} orbits respectively, corresponding in pairs to 2^{2e-f-3} or 2^{e-2} non-regular embeddings. Summing over $f = 2, \dots, e$ we see that the groups G_f and H_f respectively contribute

$$1 + 3 \left(\frac{1}{2} + 2 + 8 + \dots + 2^{2e-7} \right) + \left(\frac{1}{2} + 1 + 2 + \dots + 2^{e-4} \right) = 2^{e-3}(2^{e-2} + 1)$$

and

$$2^{e-2} + (2^{e-2} + 2^{e-1} + \dots + 2^{2e-5}) = 2^{2e-4}$$

embeddings, so the total number with metacyclic groups G is $2^{e-3}(2^{e-1} + 2^{e-2} + 1)$. For instance, if $e = 2$ then there are two embeddings: $G_2 = C_4 \times C_4$ contributes the standard embedding, while

$$H_2 = \langle g, h \mid g^4 = h^4 = 1, h^g = h^{-1} \rangle$$

contributes a second embedding of type $\{8, 4\}$ and genus 3, which is not regular; this can be formed by labelling the black and white vertices 1, 2, 3, 4, and letting the rotation of neighbours about vertices of one colour be (1, 2, 3, 4), but alternately (1, 2, 3, 4) and its inverse around successive vertices of the other colour.

9 Acknowledgement

The fourth author's research was partially supported by the Slovak grant agency APVT, Grant No. 51-012502.

References

- [1] N.L. Biggs, Automorphisms of imbedded graphs, *J. Combin. Theory Ser. B* **11** (1971), 132–138.
- [2] N.L. Biggs and A.T. White, *Permutation Groups and Combinatorial Structures*, London Math. Soc. Lecture Note Ser. **33**, Cambridge University Press, Cambridge (1979).
- [3] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Finite Groups*, 3rd ed., Springer, Berlin (1972).
- [4] M.D.E. Conder and I.M. Isaacs, Derived subgroups of an abelian and a cyclic subgroup, a manuscript.
- [5] J. Douglas, On the supersolvability of bicyclic groups, *Proc. Nat. Acad. Sci. US* **49** (1961), 1493–1495.
- [6] S.F. Du, J.H. Kwak, R. Nedela, Regular maps with pq vertices, *J. Algebraic Combinatorics* **19**, 2004, 123–141.
- [7] S.F. Du, J.H. Kwak and R. Nedela, Regular embeddings of complete multipartite graphs, *European J. Combin.* **26** (2005), 505–519.
- [8] S.F. Du, G.A. Jones, J.H. Kwak, R. Nedela, M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2. II: Nonmetacyclic case, Submitted.
- [9] S.F. Du, J.H. Kwak and R. Nedela, Classification of Regular Embeddings of Hypercubes of odd dimension, Submitted.
- [10] A. Gardiner, R. Nedela, J. Širáň, M. Škoviera, Characterization of graphs which underlie regular maps on closed surfaces. *J. London Math. Soc.* **59** (1), 1999, 100–108.
- [11] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Zeitschriften* **58** (1953), 243–264.
- [12] B. Huppert, *Endliche Gruppen I*, Springer, Berlin (1979).
- [13] N. Itô, Über das Produkt von zwei abelschen Gruppen, *Math. Zeit.*, **62** (1955), 400–401.
- [14] N. Itô, Über das Produkt von zwei zyklischen 2-Gruppen, *Publ. Math. Debrecen*, **4** (1956), 517–520.

- [15] L.D. James and G.A. Jones, Regular orientable imbeddings of complete graphs, *J. Combin. Theory Ser. B* **39** (1985), 353–367.
- [16] G.A. Jones and J.M. Jones, *Elementary Number Theory*, Springer, London (1998).
- [17] G.A. Jones and D. Singerman, Theory of maps on orientable surfaces, *Proceedings of London Math. Soc.* **37** (3) (1978), 273–307.
- [18] G.A. Jones, Automorphisms and regular embeddings of merged Johnson graphs, *European J. Combin.* **26**, (2005), 417–435.
- [19] G.A. Jones, R. Nedela and M. Škoviera, Complete bipartite graphs with unique regular embeddings, submitted.
- [20] G.A. Jones, R. Nedela and M. Škoviera, Regular Embeddings of $K_{n,n}$ where n is an odd prime power, a manuscript.
- [21] G.A. Jones and J.S. Thornton, Operations on maps, and outer automorphisms, *J. Combinatorial Theory, Ser. B*, **35** (1983), 93–103.
- [22] J.H. Kwak and Y.S. Kwon, Regular orientable embeddings of complete bipartite graphs, in print.
- [23] J. H. Kwak and Y. S. Kwon, Classification of reflexible regular embeddings and self-Petrie dual regular embeddings of complete bipartite graphs, Submitted.
- [24] L. Líšková, M. Mačaj, and M. Škoviera, Regular maps from Cayley graphs III: t-Balanced Cayley maps, *Discrete Math.*, accepted.
- [25] R. Nedela and M. Škoviera, Regular embeddings of canonical double coverings of graphs, *J. Combinatorial Theory, Ser. B* **67** (1996), 249–277.
- [26] R. Nedela and M. Škoviera, Regular maps from voltage assignments and exponent groups, *European J. Combinatorics* **18** (1997), 807–823.
- [27] R. Nedela and M. Škoviera, Exponents of orientable maps, *Proc. London Math. Soc.* (3) **75** (1997), 1–31.
- [28] R. Nedela, M. Škoviera and A. Zlatoš, Regular embeddings of complete bipartite graphs, *Discrete Math.*, **258** (1-3), 2002, p. 379–381.
- [29] H. Wielandt, Über das Produkt von paarweise vertauschbaren nilpotenten Gruppen, *Math. Z.* **55** (1951), 1–7.

- [30] S. E. Wilson, Operators over regular maps, *Pacific J. Math.* **81** (1979), 559–568.