

Journal: PLMSOC

Article id: pdp061

The following queries have arisen while collating the corrections. Please check and advise us on the below queries.

1.	Please check the correction we carried out in line 898. Because it is unclear for us.	
----	---	--

# Regular embeddings of complete bipartite graphs: classification and enumeration

Gareth A. Jones

## ABSTRACT

The regular embeddings of complete bipartite graphs  $K_{n,n}$  in orientable surfaces are classified and enumerated, and their automorphism groups and combinatorial properties are determined. The method depends on earlier classifications in the cases where  $n$  is a prime power, obtained in collaboration with Du, Kwak, Nedela and Škoviera, together with results of Itô, Hall, Huppert and Wielandt on factorisable groups and on finite solvable groups.

5

## 1. Introduction

10

A major problem in topological graph theory is that of classifying the regular embeddings, in orientable or non-orientable surfaces, of particular classes of arc-transitive graphs. Extra motivation has been provided by Grothendieck's theory of *dessins d'enfants* [12], in which bipartite maps on orientable surfaces correspond to algebraic curves defined over the field  $\overline{\mathbf{Q}}$  of algebraic numbers. In recent years there has been particular interest in the regular embeddings of the complete bipartite graphs  $K_{n,n}$ . The non-orientable regular embeddings of these graphs have recently been classified by Kwak and Kwon [26], and our aim here is to present a similar result for the orientable regular embeddings. By these we mean the embeddings  $\mathcal{M}$  of  $K_{n,n}$  in orientable surfaces such that the orientation-preserving automorphism group  $\text{Aut}^+ \mathcal{M}$  acts transitively on the arcs (directed edges) of  $\mathcal{M}$ ; for conciseness, we refer to these simply as regular embeddings.

15

20

There is at least one such embedding of  $K_{n,n}$  for each positive integer  $n$ , namely the standard embedding  $\mathcal{S}(n)$ , introduced by Biggs and White [2, §5.6.7] as a Cayley map for the group  $\mathbf{Z}_{2n}$  with respect to the generators  $1, 3, \dots, 2n-1$  in that cyclic order. (By contrast, Biggs [1] showed that the complete graph  $K_n$  has regular embeddings, subsequently classified by James and the present author in [18], if and only if  $n$  is a prime power.) This embedding  $\mathcal{S}(n)$ , illustrated for  $n=3$  in Figure 1(a), has  $2n$ -gonal faces and has genus  $(n-1)(n-2)/2$ ; it also appears in the theory of *dessins d'enfants* as a map on the  $n$ th degree Fermat curve  $x^n + y^n = z^n$ , with the black and white vertices and the edges represented by the inverse images of the points  $0, 1$  and the interval  $[0, 1]$  under the function  $[x, y, z] \mapsto (x/z)^n$ ; see [19, 23] for details and [5, 22] for some generalisations.

25

30

The classification process was begun by Nedela, Škoviera and Zlatoš [27], who showed that if  $n$  is prime, then the standard embedding is the only regular embedding of  $K_{n,n}$ ; more generally, it was shown in [21], using group theory, that  $n$  has this uniqueness property if and only if  $n$  is coprime to  $\phi(n)$ , where  $\phi$  is Euler's function. (It follows from the results of Burnside [3] and Hölder [15] that these are also the integers  $n$  for which the cyclic group is the only group of order  $n$  (see [29, Exercise 575]); Erdős [10] has shown that the proportion of the natural

35

---

Received 3 October 2008.

2000 *Mathematics Subject Classification* 05C10 (primary), 05C25, 05C30, 20D10, 20F16 (secondary).

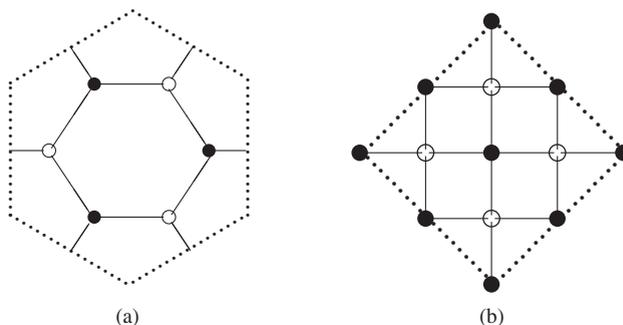


FIGURE 1. Embeddings  $\mathcal{S}(3)$  and  $\mathcal{N}(4;0,0)$ ; opposite sides of the outer hexagon and square are identified to form a torus.

numbers  $n \leq N$  with this property behaves asymptotically like

$$\frac{e^{-\gamma}}{\log \log \log N}$$

as  $N \rightarrow \infty$ , where  $\gamma$  is Euler's constant.) Using combinatorial methods based on permutations, Kwak and Kwon [24] have classified the regular embeddings in the case where  $n$  is a product of two primes, and also the reflexible embeddings (those regular embeddings with an orientation-reversing automorphism) for all  $n$  (see [25]). The classification problem has also been solved for prime powers  $n = p^e$ : the regular embeddings for  $p > 2$  are classified in [20] using properties of certain metacyclic  $p$ -groups; their direct analogues for  $p = 2$ , associated with metacyclic 2-groups, are dealt with in [8], and [9] describes the small number of exceptional embeddings  $\mathcal{N}(n; k, l)$ , defined in §3, which arise for each  $n = 2^e \geq 4$  (see Figure 1(b) for  $\mathcal{N}(4;0,0)$ ). These prime power classifications, which form an important ingredient in the present paper, are summarised in §3, and they have been used by Coste, Streit, Wolfart and the present author in [5, 23] to study the action of the absolute Galois group  $\text{Gal } \overline{\mathbf{Q}}/\mathbf{Q}$  on the corresponding algebraic curves.

Our aim here is to show that, for each  $n$ , the regular embeddings of  $K_{n,n}$  can be constructed from regular embeddings of  $K_{p^e, p^e}$  for various prime powers  $p^e$ , using two simple constructions described in §4. The first of these, introduced in [21], is the cartesian product, which produces a regular embedding  $\mathcal{S}$  of  $K_{s,s}$  from regular embeddings  $\mathcal{S}_i$  of  $K_{s_i, s_i}$  ( $i = 1, \dots, k$ ) for mutually coprime integers  $s_i$  with  $s = s_1 \dots s_k$ . The second construction produces a regular embedding  $\mathcal{M}$  of  $K_{n,n}$  as a  $t^2$ -sheeted regular abelian covering of a regular embedding  $\mathcal{S}$  of  $K_{s,s}$ , where  $n = st$  with  $s$  and  $t$  coprime. Our main result, formulated more precisely as Corollary 4.6 in §4, states that every regular embedding of  $K_{n,n}$  can be formed in this way as an abelian covering, where  $\mathcal{S}$  is the cartesian product of regular embeddings of  $K_{s_i, s_i}$  for various prime powers  $s_i$  appearing in the factorisation of  $n$ , and  $t$  is the product of the remaining prime powers. Since the prime power regular embeddings are all known, this completes the classification of regular embeddings of  $K_{n,n}$  for all  $n$ . The proof is given in §8, after some preliminary results in §§5–7. We consider the type and genus of these maps in §9, and their mirror images and Petrie duals in §10, while formulas for enumerating them are developed in §§11 and 12. There are comments on connections with directed graphs and the Erdős–Rényi random graph in §§13 and 14.

Our method is almost entirely group-theoretic, based on a study of the group  $\text{Aut}_0^+ \mathcal{M}$  of automorphisms of a regular embedding  $\mathcal{M}$  of  $K_{n,n}$ , preserving surface orientation and vertex colours. We use the fact, proved in [21] and briefly explained in §2, that a group  $G$  is isomorphic to  $\text{Aut}_0^+ \mathcal{M}$  for some regular embedding  $\mathcal{M}$  of  $K_{n,n}$  if and only if  $G$  is isobicyclic, that is, a

product of two disjoint cyclic groups of order  $n$ , with an automorphism of  $G$  transposing their generators. A result of Wielandt [30] on products of nilpotent groups shows that such a group  $G$  has a series

$$1 = N_0 < N_1 < \dots < N_{l-1} < N_l = G$$

of characteristic subgroups  $N_i$  in which the quotients  $N_i/N_{i-1}$  are isomorphic to the Sylow  $p$ -subgroups  $P$  of  $G$  for the distinct primes  $p$  dividing  $n$ . It follows that  $\mathcal{M}$  can be formed from a sequence of regular coverings, with the Sylow subgroups as the covering groups. These Sylow subgroups  $P$  are also isobicyclic, and hence they correspond to regular embeddings  $\mathcal{P}$  of  $K_{p^e, p^e}$ , where  $p^e$  ranges over the prime powers in the factorisation of  $n$ . The classification problem for prime powers having been solved, it is sufficient to consider how the groups  $P$  and maps  $\mathcal{P}$  corresponding to the prime powers dividing  $n$  may be combined to form  $G$  and  $\mathcal{M}$ . In particular, we need to determine how each Sylow  $q$ -subgroup  $Q$  of  $G$  can act by conjugation on the subgroups  $N_i$  to induce automorphisms of a Sylow  $p$ -subgroup  $P \cong N_i/N_{i-1}$ . Each possible pattern of actions can be represented as a directed graph  $\Gamma$ , in which the vertices are the primes  $p$  dividing  $n$ , and an arc from  $q$  to  $p$  represents a non-trivial action of  $Q$  on  $P$ . By determining the possible structures of such graphs  $\Gamma$ , and the ways in which regular embeddings  $\mathcal{P}$  and actions  $Q \rightarrow \text{Aut } P$  can be associated with their vertices and arcs, we obtain a classification of isobicyclic groups  $G$ ; this is stated as Theorem 4.5 in §4, and proved in §8. In particular, we find that the Sylow subgroups  $P$  corresponding to primes  $p$  which are terminal vertices of arcs of  $\Gamma$  generate a normal subgroup  $T \cong C_t \times C_t$  of  $G$ , while for the remaining primes dividing  $n$  one can choose Sylow subgroups  $S_i$  to generate their direct product  $S$ , which is a complement for  $T$  in  $G$ ; the action of  $S$  by conjugation on  $T$  can also be described explicitly, so that the structure of  $G$  is completely known. Corollary 4.6, which classifies the regular embeddings of  $K_{n,n}$ , is an immediate consequence of Theorem 4.5, using the correspondence between groups and maps explained in §2: the complement  $S = S_1 \times \dots \times S_k$  corresponds to the cartesian product  $\mathcal{S} = \mathcal{S}_1 \times \dots \times \mathcal{S}_k$  in the classification theorem, with the normal subgroup  $T$  yielding the abelian covering.

This method allows us to classify the reflexible embeddings of  $K_{n,n}$ , and those which are self-Petrie (isomorphic to their Petrie duals), thus confirming the enumerations of these two classes of maps recently obtained by Kwak and Kwon [25]. More generally, the method also yields an enumeration of all the regular embeddings of  $K_{n,n}$ . The general formula, which involves summation over all directed graphs  $\Gamma$  which may occur for a given  $n$ , is rather complicated, and this is particularly so when  $n$  is even because of the exceptional embeddings of  $K_{2^e, 2^e}$ ; however, in special cases, such as when  $n$  is divisible by at most two primes, the formula simplifies to something relatively straightforward. In particular, the formula agrees with the enumerations obtained earlier in the special cases mentioned above.

## 2. Regular embeddings and isobicyclic groups

There is a detailed treatment in [21] of the group-theoretic approach to regular embeddings of complete bipartite graphs, and hence we will simply outline it here. Throughout this paper,  $\mathcal{M}$  denotes a regular embedding of  $K_{n,n}$  in an orientable surface, and  $\text{Aut}^+ \mathcal{M}$  denotes its orientation-preserving automorphism group. The vertices can be coloured black or white so that each edge connects vertices of different colours; then  $\text{Aut}_0^+ \mathcal{M}$  denotes the subgroup of index 2 in  $\text{Aut}^+ \mathcal{M}$  preserving the vertex colours. It is shown in [21] that a group  $G$  is isomorphic to  $\text{Aut}_0^+ \mathcal{M}$  for some such  $\mathcal{M}$  if and only if  $G$  is  $n$ -isobicyclic, or simply isobicyclic; this means that  $G$  has cyclic subgroups  $X = \langle x \rangle$  and  $Y = \langle y \rangle$  of order  $n$  such that  $G = XY$  and  $X \cap Y = 1$  (hence  $|G| = n^2$ ), and there is an automorphism  $\alpha$  of  $G$  transposing  $x$  and  $y$ . We call  $(G, x, y)$  an  $n$ -isobicyclic triple, and we call  $x$  and  $y$  the canonical generators of  $G$ : these are

the orientation-preserving automorphisms of  $\mathcal{M}$  fixing a black vertex  $v$  and a white vertex  $w$ , and sending each neighbouring vertex to the next vertex by following the orientation around  $v$  or  $w$ ; the automorphism  $\alpha$  of  $G$  is induced by conjugation by the element of  $\text{Aut}^+\mathcal{M}$  which reverses the edge  $vw$ , so that  $\text{Aut}^+\mathcal{M}$  is a semidirect product  $G : \langle \alpha \rangle$  of  $G$  by  $C_2$ . Conversely, given an  $n$ -isobicyclic triple  $(G, x, y)$ , we can take the black and white vertices to be the cosets  $gX$  and  $gY$  of  $X = \langle x \rangle$  and  $Y = \langle y \rangle$  in  $G$ , and the edges to be the elements of  $G$ , with incidence given by inclusion; the successive powers of  $x$  and  $y$  give the rotation of edges around each vertex, thus defining the faces of a regular embedding  $\mathcal{M}$  of  $K_{n,n}$ .

We define two isobicyclic triples  $(G, x, y)$  and  $(G', x', y')$  to be *isomorphic* if there is an isomorphism  $G \rightarrow G'$  sending  $x$  to  $x'$  and  $y$  to  $y'$ . Two regular embeddings of  $K_{n,n}$  are isomorphic if and only if their corresponding isobicyclic triples are isomorphic, and thus we have the following result.

**THEOREM 2.1.** *The mapping  $\mathcal{M} \mapsto (G, x, y)$  induces a bijection between the set  $\mathcal{R}(n)$  of isomorphism classes of regular embeddings of  $K_{n,n}$  and the set  $\mathcal{I}(n)$  of isomorphism classes of  $n$ -isobicyclic triples. Here  $\text{Aut}_0^+\mathcal{M} \cong G$  and  $\text{Aut}^+\mathcal{M} \cong G : \langle \alpha \rangle$ .*

We denote the standard embedding of  $K_{n,n}$  by  $\mathcal{S}(n)$ ; this corresponds to the *standard triple*  $(G, x, y) \in \mathcal{I}(n)$ , with  $G = \langle x, y \mid x^n = y^n = [x, y] = 1 \rangle \cong C_n \times C_n$ . For any property of groups (such as being abelian), we say that a map  $\mathcal{M} \in \mathcal{R}(n)$  and its corresponding triple  $(G, x, y) \in \mathcal{I}(n)$  have this property if and only if  $G$  has this property. For instance, it is easily seen that  $\mathcal{S}(n)$  is the only abelian map in  $\mathcal{R}(n)$ .

### 3. The prime power embeddings

Here we briefly summarise the classifications in [8, 9] and [20] of what we call the *prime power embeddings* and triples, by which we mean the regular embeddings  $\mathcal{M}$  of  $K_{n,n}$  for prime powers  $n$  and the associated isobicyclic triples  $(G, x, y)$ . For our purposes, it is sufficient to describe the groups  $G = \text{Aut}_0^+\mathcal{M}$  and to give representatives of the orbits of  $\text{Aut} G$  on pairs of canonical generators  $x, y$ .

As shown in [20], if  $n = p^e$  for an odd prime  $p$ , then  $G$  is a metacyclic group

$$G_f = \langle g, h \mid g^n = h^n = 1, h^g = h^{1+p^f} \rangle, \quad (3.1)$$

where  $f = 1, \dots, e$ . This is a semidirect product  $C_n : C_n$  of a normal subgroup  $\langle h \rangle \cong C_n$  by a complement  $\langle g \rangle \cong C_n$ , and the action of  $\langle g \rangle$  by conjugation on  $\langle h \rangle$  is determined by the parameter  $f$ , which we sometimes denote by  $f_G$ . The canonical generators of  $G$  can be chosen to be  $x = g^u$  and  $y = g^u h$  for some  $u$  coprime to  $p$ ; we denote the corresponding regular embedding and isobicyclic triple by  $\mathcal{M}(n, f, u)$  and  $\mathcal{I}(n, f, u)$ , respectively. Then  $\mathcal{M}(n, f, u) \cong \mathcal{M}(n, f', u')$ , or equivalently  $\mathcal{I}(n, f, u) \cong \mathcal{I}(n, f', u')$ , if and only if  $f = f'$  and  $u \equiv u' \pmod{p^{e-f}}$ , and hence there are  $\phi(p^{e-f})$  isomorphism classes of regular embeddings  $\mathcal{M}(n, f, u)$  for each  $f$ , represented by taking  $u = 1, \dots, p^{e-f}$  coprime to  $p$ , and these give a total of  $\sum_{f=1}^e \phi(p^{e-f}) = p^{e-1}$  maps in  $\mathcal{R}(n)$  for each odd prime power  $n = p^e$ . They all have type  $\{2n, n\}$  and genus  $(n-1)(n-2)/2$ . Note that  $G_e \cong C_n \times C_n$ , and the unique map corresponding to  $G_e$  is the standard embedding  $\mathcal{S}(n) = \mathcal{M}(n, e, 1)$ .

It is shown in [8] that if  $n = 2^e$ , then the metacyclic maps  $\mathcal{M} \in \mathcal{R}(n)$  and triples  $(G, x, y) \in \mathcal{I}(n)$  are the direct analogues for  $p = 2$  of those defined in (3.1), but with the case  $f = 1$  excluded if  $e \geq 2$ ; this gives  $\sum_{f=2}^e \phi(2^{e-f}) = 2^{e-2}$  metacyclic maps and triples if  $n = 2^e \geq 4$ , and one if  $n = 2$ . In addition, it is shown in [9] that there is one non-metacyclic triple in  $\mathcal{I}(4)$ , and there are four in  $\mathcal{I}(n)$  for each  $n = 2^e \geq 8$ . To construct these, let  $G(n; k, l)$  be the group

defined by the presentation

$$G = G(n; k, l) = \langle x, y \mid x^n = y^n = 1, c := [y, x] = x^{2+k2^{e-1}} y^{-2-k2^{e-1}}, \\ c^x = c^{-1+l2^{e-2}} x^4, c^y = c^{-1-l2^{e-2}} y^{-4} \rangle,$$

where  $k, l \in \{0, 1\}$ . This is an extension of a normal subgroup  $\Phi(G) = \langle x^2, y^2 \rangle \cong C_{n/2} \times C_{n/2}$  (the Frattini subgroup of  $G$ ) by  $G/\Phi(G) \cong C_2 \times C_2$ ; the conjugation action is given by  $(y^2)^x = y^{-2}z^l$  and  $(x^2)^y = x^{-2}z^l$ , where  $z$  is the central involution  $x^{n/2}y^{n/2}$ . For each  $n = 2^e \geq 8$  the four choices for  $k$  and  $l$  give the four non-metacyclic triples  $(G, x, y)$  in  $\mathcal{I}(n)$ , and for  $n = 4$  the single non-metacyclic triple corresponds to the group  $G(4; 0, 0)$ . Let  $\mathcal{N}(n; k, l)$  denote the map in  $\mathcal{R}(n)$  corresponding to  $G(n; k, l)$ ; if  $k = l$  it has type  $\{4, n\}$  and genus  $(n - 2)^2/4$ , and if  $k \neq l$  it has type  $\{8, n\}$  and genus  $1 + n(3n - 8)/8$ . For instance, Figure 1(b) shows  $\mathcal{N}(4; 0, 0)$ , isomorphic to the torus map  $\{4, 4\}_{2,2}$  of Coxeter and Moser [6, Chapter 8]. The maps  $\mathcal{N}(n; 0, 0)$  are special cases for  $q = n/2 = 2^{e-1}$  of the maps  $\{4, 2q\}_4$ , the duals of the maps  $\{2q, 4\}_4$  in [6, Table 8]; they are also isomorphic to the maps  $\mathcal{O}_n$  in [8, Example 3], obtained by applying Wilson’s ‘opposite’ operation [31] to the torus maps  $\{4, 4\}_n = \{4, 4\}_{q,q}$  described in [6, Chapter 8]. All four maps  $\mathcal{N}(n; k, l)$  are 4-sheeted regular coverings of  $\mathcal{N}(n/2; 0, 0)$ , with the covering obtained by factoring out the central subgroup  $\langle x^{n/2}, y^{n/2} \rangle \cong C_2 \times C_2$  of  $G(n; k, l)$ . It will be useful in § 7 for us to define  $f_G = 1$  for each of these non-metacyclic 2-groups  $G = G(n; k, l)$ .

#### 4. Basic constructions

Here we describe two basic constructions of regular embeddings of complete bipartite graphs. Our eventual aim is to show that all such embeddings can be found by applying these constructions to the prime power embeddings described in § 3.

CONSTRUCTION 4.1. Let  $\mathcal{M}_i \in \mathcal{R}(s_i)$  for  $i = 1, \dots, k$ , where the integers  $s_1, \dots, s_k$  are mutually coprime. Each  $\mathcal{M}_i$  corresponds to a triple  $(G_i, x_i, y_i) \in \mathcal{I}(s_i)$ , and it is easy to check that if  $G = G_1 \times \dots \times G_k$ ,  $x = (x_1, \dots, x_k)$  and  $y = (y_1, \dots, y_k)$ , then  $(G, x, y) \in \mathcal{I}(s)$ , where  $s = s_1 \dots s_k$ . We call  $(G, x, y)$  the *cartesian product* of the triples  $(G_i, x_i, y_i)$ , and we call the corresponding regular embedding of  $K_{s,s}$  the *cartesian product*  $\mathcal{M}_1 \times \dots \times \mathcal{M}_k$  of the embeddings  $\mathcal{M}_i$ . For example, if  $s$  has prime power factorisation  $s = p_1^{e_1} \dots p_k^{e_k}$ , then

$$\mathcal{S}(s) \cong \mathcal{S}(p_1^{e_1}) \times \dots \times \mathcal{S}(p_k^{e_k}).$$

The above construction was introduced in [21]; the following construction is a generalisation of some simple examples also considered there.

CONSTRUCTION 4.2. Let  $\mathcal{S} \in \mathcal{R}(s)$  and let  $\mathcal{T} = \mathcal{S}(t)$ , respectively, corresponding to a triple  $(S, x_S, y_S) \in \mathcal{I}(s)$  and the standard triple  $(T, x_T, y_T) \in \mathcal{I}(t)$ . Since  $T \cong C_t \times C_t$ , we can use the basis  $x_T, y_T$  of the free  $\mathbf{Z}_t$ -module  $T$  to identify  $\text{Aut } T$  with the general linear group  $\text{GL}_2(\mathbf{Z}_t)$ . Suppose that  $s$  and  $t$  are coprime, and that there is a homomorphism  $\psi : S \rightarrow \text{GL}_2(\mathbf{Z}_t)$  such that

$$x_S \mapsto \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \quad \text{and} \quad y_S \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$$

for some  $\lambda$  in the group  $\mathbf{Z}_t^*$  of units in  $\mathbf{Z}_t$ ; we call this a *diagonal action* of  $S$  on  $T$ , with *eigenvalue*  $\lambda$ . Now let  $G$  be the semidirect product  $T :_{\psi} S$  of  $T$  by  $S$ , with  $\psi$  giving the action

of the complement  $S$  by conjugation on the normal subgroup  $T$ , so that

$$x_T^{xS} = x_T, \quad y_T^{xS} = y_T^\lambda, \quad x_T^{yS} = x_T^\lambda \quad \text{and} \quad y_T^{yS} = y_T.$$

If we define  $x = x_S x_T$  and  $y = y_S y_T$ , then these relations imply that  $(G, x, y)$  is an  $n$ -isobicyclic triple, where  $n = st$ . We call this triple a *semidirect product* of  $(T, x_T, y_T)$  by  $(S, x_S, y_S)$ , and we call the corresponding map  $\mathcal{M} \in \mathcal{R}(n)$  a *semidirect product*  $\mathcal{T} : \mathcal{S}$  of  $\mathcal{T}$  by  $\mathcal{S}$ , writing  $\mathcal{M} = \mathcal{T} :_\lambda \mathcal{S}$  if we need to specify the value of  $\lambda$ . The parameters  $t$  and  $\lambda$ , together with the isomorphism class of  $(S, x_S, y_S)$ , uniquely determine the isomorphism class of  $(G, x, y)$  and hence also that of  $\mathcal{M}$ . Any such map  $\mathcal{M} = \mathcal{T} : \mathcal{S}$  is a regular covering of  $\mathcal{S}$ , with  $\mathcal{T}$  as the covering group, such that  $\mathcal{M}/\mathcal{T} \cong \mathcal{S}$ ; we will therefore also refer to  $\mathcal{M}$  as an *abelian covering* of  $\mathcal{S}$ , and similarly for the triple  $(G, x, y)$ .

EXAMPLE 4.3. Construction 4.2 yields the cartesian product  $\mathcal{T} \times \mathcal{S}$  if and only if  $\lambda = 1$ .

EXAMPLE 4.4. Instances of non-trivial actions of  $S$  on  $T$  can be found by taking  $\mathcal{S}$  to be the standard embedding, so that  $S \cong C_s \times C_s$ , and choosing  $\lambda \in \mathbf{Z}_t^*$  such that  $\lambda^s = 1$ ; for example, see [21] for the case where  $t$  is prime, with  $s$  dividing  $t - 1$ .

The main results of this paper are that each  $n$ -isobicyclic triple, and hence each regular embedding of  $K_{n,n}$ , is an abelian covering of a cartesian product of prime power triples (or embeddings), as described in §3. More specifically, we will prove the following.

THEOREM 4.5. Each  $n$ -isobicyclic triple  $(G, x, y)$  is isomorphic to a semidirect product of a  $t$ -isobicyclic triple  $(T, x_T, y_T)$  by an  $s$ -isobicyclic triple  $(S, x_S, y_S)$ , where  $n = st$  with  $s$  and  $t$  coprime,  $(S, x_S, y_S)$  is a cartesian product of  $p_i^{e_i}$ -isobicyclic triples for  $i = 1, \dots, k$ , where  $s = p_1^{e_1} \dots p_k^{e_k}$  for distinct primes  $p_i$ , and  $(T, x_T, y_T)$  is the standard  $t$ -isobicyclic triple.

We will prove this result in §8. As an immediate consequence of Theorem 4.5, using the correspondence between maps and isobicyclic triples outlined in §2, we have the following corollary.

COROLLARY 4.6. Each regular orientable embedding of  $K_{n,n}$  has the form  $\mathcal{M} = \mathcal{T} : \mathcal{S}$ , where  $n = st$  with  $s$  and  $t$  coprime,  $\mathcal{S} = \mathcal{S}_1 \times \dots \times \mathcal{S}_k$  with each  $\mathcal{S}_i \in \mathcal{R}(p_i^{e_i})$ , where  $s = p_1^{e_1} \dots p_k^{e_k}$  for distinct primes  $p_i$ , and  $\mathcal{T}$  is the standard embedding of  $K_{t,t}$ .

In general, the decompositions in Theorem 4.5 and Corollary 4.6 are not unique: a Sylow subgroup which is an abelian direct factor of  $G$  could appear as a direct factor of either  $S$  or  $T$ , and there is a corresponding result for the decomposition of  $\mathcal{M}$ . However, this is the only way in which uniqueness can fail, and in each case there is a unique decomposition for which  $t$  is minimal; this is characterised by the property that  $T \cap Z(G) = 1$ , where  $Z(G)$  denotes the centre of  $G$ . We call this the *canonical decomposition* of  $(G, x, y)$  or of  $\mathcal{M}$ .

## 5. Hall subgroups and Sylow subgroups

If  $\mathcal{M}$  is a regular embedding of  $K_{n,n}$ , then the corresponding group  $G = \text{Aut}_0^+ \mathcal{M}$  is a product  $XY$  of abelian subgroups  $X$  and  $Y$ , and thus it follows from a theorem of Itô [17] that  $G$  is

metabelian, that is, an extension of one abelian group by another. Being solvable,  $G$  satisfies Hall's theorems, or the extended Sylow theorems, which we shall now explain.

If  $\pi$  is any set of prime numbers, then a  $\pi$ -number is a positive integer divisible only by primes in  $\pi$ , and a  $\pi$ -group is a group the order of which is a  $\pi$ -number. A Hall  $\pi$ -subgroup of a group  $G$  is a  $\pi$ -group  $H \leq G$  the index of which,  $|G : H|$ , is a  $\pi'$ -number, where  $\pi'$  denotes the set of primes not in  $\pi$ . A fundamental theorem of Hall [13] (see also [16, VI.1.8] or [29, 11.18]) states that, for each set  $\pi$  of primes, a finite solvable group has a single conjugacy class of Hall  $\pi$ -subgroups, and every  $\pi$ -subgroup is contained in a Hall  $\pi$ -subgroup. For instance, if  $\pi = \{p\}$  or  $\{p\}'$ , then the Hall  $\pi$ -subgroups of  $G$  are simply its Sylow  $p$ -subgroups or Sylow  $p$ -complements. 240

A finite nilpotent group has a unique Hall  $\pi$ -subgroup for each set  $\pi$  of primes, namely the direct product of its Sylow  $p$ -subgroups for the primes  $p \in \pi$ . In [16, Satz VI.4.8], Huppert has shown that if a solvable group  $G$  has the form  $G = XY$  for nilpotent subgroups  $X$  and  $Y$ , and  $X_\pi$  and  $Y_\pi$  are the Hall  $\pi$ -subgroups of  $X$  and  $Y$ , then  $X_\pi Y_\pi$  is a Hall  $\pi$ -subgroup of  $G$ . (In fact, one can omit the hypothesis that  $G$  is solvable, since this is true for any product of two nilpotent groups, by a theorem of Kegel and Wielandt [16, Satz VI.4.3].) This is a generalisation of results of Wielandt [30], who proved these properties for Sylow  $p$ -subgroups and their complements. 250

If  $G$  is  $n$ -isobicyclic, so that  $G = XY$  with  $X \cong Y \cong C_n$ , then these results apply to  $G$ . We call  $X_\pi Y_\pi$  the canonical Hall  $\pi$ -subgroup  $G_\pi$  of  $G$ . We have  $X = X_\pi \times X_{\pi'}$  and  $Y = Y_\pi \times Y_{\pi'}$ , and hence the canonical generators  $x$  and  $y$  of  $G$  have unique factorisations  $x = x_\pi x_{\pi'}$  and  $y = y_\pi y_{\pi'}$  with  $x_\pi, x_{\pi'}, y_\pi$  and  $y_{\pi'}$  elements of  $X_\pi, X_{\pi'}, Y_\pi$  and  $Y_{\pi'}$ , respectively. In fact, these four elements generate these subgroups, and hence we call them their canonical generators. In the particular case where  $\pi = \{p\}$  for some prime  $p$  dividing  $n$ , we write simply  $x_p, x_{p'}$  and so on. 255

Since  $X \cap Y = 1$  we have  $X_\pi \cap Y_\pi = 1$ . Moreover, the canonical automorphism  $\alpha$  of  $G$ , transposing  $x$  and  $y$ , must also transpose their powers  $x_\pi$  and  $y_\pi$ . Thus  $\alpha$  leaves  $G_\pi$  invariant and induces an automorphism  $\alpha_\pi$  of  $G_\pi$  transposing its canonical generators, and hence  $G_\pi$  is isobicyclic. We summarise this result as follows. 260

**PROPOSITION 5.1.** *If  $G = XY$  is  $n$ -isobicyclic, then, for each set  $\pi$  of primes dividing  $n$ , the group  $G_\pi = X_\pi Y_\pi$  is an isobicyclic Hall  $\pi$ -subgroup of  $G$ .*

**COROLLARY 5.2.** *If  $G$  is  $n$ -isobicyclic, then, for each prime  $p$  dividing  $n$ , the Sylow  $p$ -subgroups of  $G$  are isomorphic to one of the isobicyclic  $p$ -groups described in § 3.* 265

*Proof.* This follows from Proposition 5.1, the conjugacy of Sylow  $p$ -subgroups for a given  $p$ , and the prime-power classifications summarised in § 3. □

The next result gives us an important link between the Sylow subgroups and certain normal subgroups of  $G$ .

**PROPOSITION 5.3.** *If  $G$  is  $n$ -isobicyclic,  $p_1, \dots, p_l$  are the distinct primes dividing  $n$ , with  $p_1 > \dots > p_l$ , and  $P_i$  is a Sylow  $p_i$ -subgroup of  $G$  for each  $i$ , then  $N_i := P_1 \dots P_i$  is a normal subgroup of  $G$  for each  $i = 1, \dots, l$ .* 270

*Proof.* This is a special case of a result of Wielandt [30, Satz 3], which states that any finite group  $G$  which is a product of two cyclic groups has this property, where  $p_1, \dots, p_l$  are

280 the primes dividing  $|G|$ . In our case we have  $|G| = n^2$ , and hence these are also the primes dividing  $n$ .  $\square$

This result implies that  $G$  has an ascending series

$$1 = N_0 < N_1 < \dots < N_{l-1} < N_l = G \quad (5.1)$$

of normal (in fact, characteristic) subgroups  $N_i$  of  $G$  with  $N_i/N_{i-1} \cong P_i$  for each  $i = 1, \dots, l$ . We can (and will) without loss of generality take each  $P_i$  to be the canonical Sylow  $p_i$ -subgroup of  $G$ , so each  $N_i$  is the canonical Hall  $\pi$ -subgroup  $G_\pi$  of  $G$  for  $\pi = \{p_1, \dots, p_i\}$ . By Corollary 5.2, each of the quotients  $N_i/N_{i-1}$  in (5.1) is isomorphic to one of the isobicyclic  $p$ -groups described in §3, where  $p = p_i$ . More generally, if  $1 \leq i \leq j \leq l$ , then the natural epimorphism  $G \rightarrow G/N_{i-1}$  induces an isomorphism  $G_\pi \cong N_j/N_{i-1}$ , where  $\pi = \{p_i, \dots, p_j\}$ , so Proposition 5.1 implies that  $N_j/N_{i-1}$  is isobicyclic.

In order to determine the structure of  $G$ , and hence of  $\mathcal{M}$ , we need to know the canonical Sylow subgroups  $P_i$  of  $G$ , together with the action by conjugation of  $G/N_{i-1}$  on its normal subgroup  $N_i/N_{i-1} \cong P_i$  for each  $i$ . (Since the quotients  $N_i/N_{i-1}$  in (5.1) have mutually coprime orders, the Schur–Zassenhaus Theorem (see [16, I.18.1] or [29, 10.30]) ensures that all the relevant extensions split, so we do not have to consider cohomological problems associated with possibly non-split extensions.) In considering this action, by factoring out  $N_{i-1}$  if necessary, we can assume that  $i = 1$ , so that  $N_i/N_{i-1} = N_1$  is a normal Sylow  $p$ -subgroup  $P = P_1$  of  $G$  for the largest prime  $p = p_1$  dividing  $n$ . In this case, since  $G = P_1 \dots P_l$ , it is sufficient to determine how each canonical Sylow  $q$ -subgroup  $Q = P_j$  acts by conjugation on  $P$ , where  $q = p_j$  for some  $j > 1$ . We therefore assume for the next two sections that  $P$  is a normal Sylow  $p$ -subgroup of  $G$  for the largest prime  $p = p_1$  dividing  $n$ , and that  $Q$  is the canonical Sylow  $q$ -subgroup of  $G$  for a prime  $q = p_j$ , where  $j > 1$ . Even in the general case, when  $i > 1$  and  $P$  is not necessarily normalised by  $Q$ , we refer to the action of  $Q$  on  $P$ , meaning the action induced by the natural isomorphism of  $P$  with the corresponding quotient  $N_i/N_{i-1} \cong P$ .

305 An important aid to understanding this action is given by Hall’s corollary to the Burnside Basis Theorem. Let  $P$  be any finite  $p$ -group, and let  $\Phi(P)$  denote its Frattini subgroup, the intersection of its maximal subgroups, or equivalently the smallest normal subgroup of  $P$  with an elementary abelian quotient  $\tilde{P} = P/\Phi(P)$ . Since  $\Phi(P)$  is a characteristic subgroup of  $P$ , every automorphism of  $P$  induces an automorphism of  $\tilde{P}$ , giving a homomorphism  $\phi : \text{Aut } P \rightarrow \text{Aut } \tilde{P}$ . Hall [14] (see also [16, III.3.18] or [29, 11.13(i)]) showed that  $\ker \phi$  is a  $p$ -group, or equivalently the following proposition holds.

PROPOSITION 5.4. *If  $P$  is a finite  $p$ -group, then any  $p'$ -group  $A$  of automorphisms of  $P$  is represented faithfully on  $\tilde{P} := P/\Phi(P)$ .*

Indeed, one can regard  $\tilde{P}$  as a  $d$ -dimensional vector space over the field  $\mathbf{Z}_p$ , where  $d$  is the rank (minimum number of generators) of  $P$ , so that  $A$  acts linearly on  $\tilde{P}$  as a subgroup of  $\text{GL}_d(p)$ . In our situation, where  $P$  is a normal Sylow  $p$ -subgroup of an isobicyclic group  $G$ , we have  $d = 2$ ; any Sylow  $p$ -complement  $K$  in  $G$ , acting by conjugation, induces a  $p'$ -group  $\overline{K} = K/C_K(P)$  of automorphisms of  $P$ , where  $C_K(P)$  denotes the centraliser of  $P$  in  $K$ . We therefore have the following proposition.

320 PROPOSITION 5.5. *The group  $\overline{K}$  is represented faithfully on  $\tilde{P} \cong C_p \times C_p$  as a subgroup of  $\text{GL}_2(p)$ .*

In particular, if  $Q$  is a Sylow  $q$ -subgroup of  $G$  for any prime  $q \neq p$ , then  $\overline{Q} := Q/C_Q(P)$  is represented faithfully on  $\tilde{P}$  as a subgroup of  $\text{GL}_2(p)$ .

6. Non-abelian Sylow subgroups

In Construction 4.2, we chose  $\mathcal{T}$  to be a standard embedding. The next result explains why this is necessary if  $S$  is to act non-trivially on  $T$ . 325

**PROPOSITION 6.1.** *If  $G$  is isobicyclic, and  $P$  is a non-abelian normal Sylow  $p$ -subgroup of  $G$ , then  $P$  is a direct factor of  $G$ .*

Note that by Construction 4.2, an abelian normal Sylow  $p$ -subgroup need not be a direct factor. Returning to the series (5.1) for an isobicyclic group  $G$ , we can immediately deduce the following proposition. 330

**PROPOSITION 6.2.** *If  $P$  and  $Q$  are Sylow  $p$ - and  $q$ -subgroups of an isobicyclic group  $G$  for primes  $p \neq q$ , and  $P$  is non-abelian, then  $Q$  acts trivially on  $P$ .*

In order to prove Proposition 6.1, we first need the following technical result.

**LEMMA 6.3.** *Let  $P$  be a non-abelian isobicyclic  $p$ -group with canonical generators  $x$  and  $y$ , and canonical automorphism  $\alpha$ . If  $A = \langle \beta, \beta^\alpha \rangle \leq \text{Aut } P$ , where  $\beta$  is an automorphism fixing  $x$ , and  $A$  has order coprime to  $p$ , then  $A = 1$ .* 335

*Proof.* Since  $A$  has order coprime to  $p$ , it is represented faithfully on  $\tilde{P} := P/\Phi(P) \cong C_p \times C_p$  by Proposition 5.4, and thus it is sufficient to show that  $A$  acts trivially on  $\tilde{P}$ . If we use the basis of  $\tilde{P}$  formed by the images  $\tilde{x}$  and  $\tilde{y}$  of the canonical generators  $x$  and  $y$  of  $P$ , then  $A$  is identified with the subgroup of  $\text{Aut } \tilde{P} = \text{GL}_2(p)$  generated by two matrices of the form 340

$$M_\beta = \begin{pmatrix} 1 & 0 \\ \kappa & \lambda \end{pmatrix} \quad \text{and} \quad M_\gamma = \begin{pmatrix} \lambda & \kappa \\ 0 & 1 \end{pmatrix}$$

with  $\kappa, \lambda \in \mathbf{Z}_p$  and  $\lambda \neq 0$ . Here  $M_\beta$  represents the action of  $\beta$ , which fixes  $\tilde{x}$ , and  $M_\gamma$  represents that of  $\gamma := \beta^\alpha$ , which fixes  $\tilde{y}$ . If  $\lambda = 1$ , then such matrices have order  $p$  (against our hypotheses) or 1 (as required); thus we may assume that  $\lambda \neq 1$ , and hence  $p > 2$ . 345

In the proof of [20, Proposition 16] it is shown that if  $P$  is a non-abelian isobicyclic  $p$ -group, where  $p > 2$ , then every automorphism of  $P$  acts on  $\tilde{P}$  as a matrix in  $\text{GL}_2(p)$  of the form

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

with respect to the basis  $\tilde{g}, \tilde{h}$  for  $\tilde{P}$ , where  $g$  and  $h$  are as in (3.1). The group of all such matrices, isomorphic to the affine general linear group  $\text{AGL}_1(p)$ , acts faithfully on the projective line  $\text{PG}_1(p)$  formed by the 1-dimensional subspaces of  $\tilde{P}$ , fixing one element of  $\text{PG}_1(p)$  and acting sharply 2-transitively on the remaining  $p$  elements. Any subgroup of  $\text{AGL}_1(p)$  of order coprime to  $p$  is cyclic of order dividing  $p - 1$ , fixing two elements and acting semi-regularly on the other  $p - 1$ . In particular, this must apply to  $A$ ; however,  $M_\beta$  and  $M_\gamma$ , between them, have at least three fixed points on  $\text{PG}_1(p)$ , and thus  $A = 1$ , as required. 350

□ 355

*Proof of Proposition 6.1.* Being normal,  $P$  is the unique Sylow  $p$ -subgroup of  $G$ , and hence  $P$  is the canonical Sylow  $p$ -subgroup  $G_p = X_p Y_p$ . Let  $K$  be the canonical Sylow  $p$ -complement  $G_{p'} = X_{p'} Y_{p'}$  in  $G$ ; thus  $G$  is a semidirect product of  $P$  by  $K$ . Acting on  $P$  by conjugation,  $K$  induces a group  $\overline{K} \cong K/C_K(P)$  of automorphisms of  $P$ . This is generated by automorphisms  $\beta$  and  $\gamma = \beta^\alpha$  of  $P$ , induced by the canonical generators  $x_{p'}$  and  $y_{p'}$  of  $K$ . Since  $X_p$  and  $X_{p'}$  are contained in the abelian group  $X$ , it follows that  $\beta$  acts trivially on  $X_p$ , and similarly  $\gamma$  acts trivially on  $Y_p$ . Since  $P$  is a non-abelian isobicyclic  $p$ -group, and since  $\overline{K}$  has order coprime to  $p$ , Lemma 6.2 (with  $A = \overline{K}$ ) implies that  $\overline{K} = 1$ , and hence  $G = P \times K$ , as required.  $\square$

### 7. Abelian Sylow subgroups

We now assume that the normal Sylow  $p$ -subgroup  $P$  of  $G$  is abelian. Since  $P$  is isobicyclic, it follows that  $P \cong C_{p^d} \times C_{p^d}$  for some  $d \geq 1$ . In order to determine how  $G$  can act by conjugation on  $P$  we need the following lemma, an analogue of Lemma 6.3.

LEMMA 7.1. *Let  $P = C_{p^d} \times C_{p^d}$  and let  $A \leq \text{Aut } P = \text{GL}_2(\mathbf{Z}_{p^d})$  be a  $p'$ -group generated by the matrices*

$$M_x = \begin{pmatrix} 1 & 0 \\ \kappa & \lambda \end{pmatrix} \quad \text{and} \quad M_y = \begin{pmatrix} \lambda & \kappa \\ 0 & 1 \end{pmatrix}.$$

Then the following are equivalent:

- (a)  $A$  is abelian;
- (b)  $A$  consists of diagonal matrices;
- (c)  $\kappa = 0$ ;
- (d)  $\kappa \equiv 0 \pmod{p}$ .

*Proof.* It is clear that (b) and (c) are equivalent, that (b) implies (a), and that (c) implies (d). To show that (a) implies (c), we have

$$M_x M_y = \begin{pmatrix} \lambda & \kappa \\ \kappa \lambda & \kappa^2 + \lambda \end{pmatrix} \quad \text{and} \quad M_y M_x = \begin{pmatrix} \kappa^2 + \lambda & \kappa \lambda \\ \kappa & \lambda \end{pmatrix},$$

and hence  $M_x$  and  $M_y$  commute if and only if  $\kappa^2 = 0$  and  $\kappa(\lambda - 1) = 0$ . If  $\kappa \neq 0$  then this implies that  $\lambda \equiv 1 \pmod{p}$ . Since  $A$  is a  $p'$ -group, it is represented faithfully on  $\tilde{P} := P/\Phi(P) \cong C_p \times C_p$  as a subgroup of  $\text{GL}_2(p)$ ; however, since  $\lambda \equiv 1 \pmod{p}$  the images of  $M_x$  and  $M_y$  in  $\text{GL}_2(p)$  have order dividing  $p$ , and hence  $A = 1$ , contradicting  $\kappa \neq 0$ . To show that (d) implies (a), if  $\kappa \equiv 0 \pmod{p}$  then the images of  $M_x$  and  $M_y$  in  $\text{GL}_2(p)$  are diagonal matrices, and thus they commute; since  $A$  is represented faithfully in  $\text{GL}_2(p)$  it follows that  $M_x$  and  $M_y$  commute, and hence  $A$  is abelian.  $\square$

If  $A$  satisfies the equivalent conditions in Lemma 7.1, and hence

$$M_x = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \quad \text{and} \quad M_y = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$$

for some  $\lambda \in \mathbf{Z}_{p^d}$ , then we say that  $A$  acts diagonally on  $P$  with respect to the canonical basis of  $P$ , with eigenvalue  $\lambda$ . By Proposition 5.4 we must have  $\lambda^{p-1} = 1$ .

PROPOSITION 7.2. *If  $P$  is an abelian normal Sylow  $p$ -subgroup of an isobicyclic group  $G$ , then  $G$  acts diagonally on  $P$  with respect to its canonical basis.*

*Proof.* Since  $P$  is abelian, the action of  $G$  by conjugation on  $P$  is equivalent to that of  $G/P$ , and this in turn is equivalent to that of the Sylow  $p'$ -complement  $G_{p'}$  of  $G$ . Since  $G_{p'}$  is the product of the canonical Sylow  $q$ -subgroups  $Q = G_q$  of  $G$  for the primes  $q \neq p$  dividing  $n$ , it is sufficient to show that each such group  $Q$  acts diagonally on  $P$ . 395

Since  $|Q|$  is coprime to  $p$ , the subgroup  $\bar{Q} = Q/C_Q(P)$  of  $\text{Aut } P$  induced by  $Q$  on  $P$  is isomorphic to the subgroup  $\tilde{Q}$  of  $\text{GL}_2(p)$  induced by  $Q$  on  $\tilde{P} := P/\Phi(P)$ . Now  $\tilde{Q}$  is contained in a Sylow  $q$ -subgroup  $S$  of  $\text{GL}_2(p)$ . If  $q$  is odd, then  $S$  is abelian, conjugate to a subgroup of the diagonal group  $\text{GL}_1(p) \times \text{GL}_1(p)$  if  $q$  divides  $p - 1$ , or to a subgroup of a Singer group  $\text{GF}(p^2)^* \cong C_{p^2-1}$  if not. In either case,  $\tilde{Q}$  is abelian and hence so is  $\bar{Q}$ , so Lemma 7.1 implies that  $Q$  acts diagonally on  $P$ . 400

We may therefore assume that  $q = 2$ . The above argument does not apply in this case, since a Sylow 2-subgroup  $S$  of  $\text{GL}_2(p)$  is non-abelian for each prime  $p > 2$ . If  $p \equiv 1 \pmod{4}$ , then  $S$  is a wreath product  $C_{2^r} \wr C_2$ , where  $2^r \parallel p - 1$ : one can take the base group  $C_{2^r} \times C_{2^r}$  to consist of diagonal matrices, with the complement  $C_2$  generated by  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . If  $p \equiv -1 \pmod{4}$ , then  $S$  is a semidihedral group 405

$$\text{SD}_{2^{r+1}} = \langle c, d \mid c^{2^{r+1}} = d^2 = 1, c^d = c^{-1+2^r} \rangle,$$

where  $2^r \parallel p + 1$ : the normal subgroup  $\langle c \rangle \cong C_{2^{r+1}}$  is contained in a Singer group  $\text{GF}(p^2)^*$ , and the complement  $\langle d \rangle \cong C_2$  is induced by the Galois group of  $\text{GF}(p^2)$ . In either case,  $S$  has an abelian subgroup of index 2, and thus all squares in  $Q$  commute. 410

The canonical generators of  $Q$ , acting by conjugation on  $P$ , are represented by matrices of the form  $M_x, M_y \in \text{GL}_2(\mathbf{Z}_{p^d})$  in Lemma 7.1. Now

$$M_x^2 = \begin{pmatrix} 1 & 0 \\ \kappa(\lambda + 1) & \lambda^2 \end{pmatrix} \quad \text{and} \quad M_y^2 = \begin{pmatrix} \lambda^2 & \kappa(\lambda + 1) \\ 0 & 1 \end{pmatrix},$$

and hence

$$M_x^2 M_y^2 = \begin{pmatrix} \lambda^2 & \kappa(\lambda + 1) \\ \kappa\lambda^2(\lambda + 1) & \kappa^2(\lambda + 1)^2 + \lambda^2 \end{pmatrix} 415$$

and

$$M_y^2 M_x^2 = \begin{pmatrix} \kappa^2(\lambda + 1)^2 + \lambda^2 & \kappa\lambda^2(\lambda + 1) \\ \kappa(\lambda + 1) & \lambda^2 \end{pmatrix}.$$

This shows that  $M_x^2$  and  $M_y^2$  commute if and only if  $\kappa^2(\lambda + 1)^2 = 0$  and  $\kappa(\lambda + 1)(\lambda^2 - 1) = 0$  in  $\mathbf{Z}_{p^d}$ . Since they generate a  $p'$ -group, the matrices  $M_x^2$  and  $M_y^2$  commute if and only if their images in  $\text{GL}_2(p)$  commute, that is,  $\kappa^2(\lambda + 1)^2 \equiv \kappa(\lambda + 1)(\lambda^2 - 1) \equiv 0 \pmod{p}$ , or equivalently  $\kappa \equiv 0$  or  $\lambda \equiv -1 \pmod{p}$ . If  $\kappa \equiv 0 \pmod{p}$ , then Lemma 7.1 implies that  $Q$  acts diagonally, and thus we may assume that  $\lambda \equiv -1 \pmod{p}$ . Then  $M_x^2$  and  $M_y^2$  induce the identity on  $\tilde{P}$ , and hence they also induce the identity on  $P$ . Thus the images  $\bar{X}_q = \langle M_x \rangle$  and  $\bar{Y}_q = \langle M_y \rangle$  of  $X_q$  and  $Y_q$ , in  $\text{Aut } P$  each have order at most 2, and hence  $\bar{Q} = \bar{X}_q \bar{Y}_q$  has order at most 4. It follows that  $\bar{Q}$  is abelian, and thus Lemma 7.1 implies that  $Q$  acts diagonally on  $P$ . 425  $\square$

We can now deduce the analogue of Corollary 6.2 for abelian Sylow  $p$ -subgroups.

**COROLLARY 7.3.** *If  $P$  and  $Q$  are Sylow  $p$ - and  $q$ -subgroups, respectively, of an isobicyclic group  $G$  for primes  $p \neq q$ , and  $P$  is abelian, then  $Q$  acts diagonally on  $P$ . If  $q$  does not divide  $p - 1$ , then this action is trivial.*

430 *Proof.* The first statement follows immediately from Proposition 7.2. Proposition 5.5 then implies that  $\overline{Q}$  is represented faithfully on  $\tilde{P}$  as a subgroup of  $\mathrm{GL}_1(p) \times \mathrm{GL}_1(p) \cong C_{p-1} \times C_{p-1}$ , and thus if  $q$  does not divide  $p - 1$ , then  $\overline{Q} = 1$ , that is,  $Q$  acts trivially on  $P$ .  $\square$

It remains for us to determine how  $Q$  can act diagonally on  $P$  when  $q$  divides  $p - 1$ .

435 **LEMMA 7.4.** *Let  $p$  and  $q$  be primes, with  $q$  dividing  $p - 1$ . An isobicyclic  $q$ -group  $Q$  can act diagonally on  $P \cong C_{p^d} \times C_{p^d}$  with eigenvalue  $\lambda \in \mathbf{Z}_{p^d}$  if and only if  $\lambda^{q^m} = 1$ , where  $m = \min\{f_Q, r\}$  and  $q^r \parallel p - 1$ ; there are  $q^m$  such elements  $\lambda \in \mathbf{Z}_{p^d}$ .*

*Proof.* Since diagonal matrices commute, there is a diagonal action of  $Q$  on  $P$  with eigenvalue  $\lambda$  if and only if the mapping

$$x \mapsto M_x = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \quad \text{and} \quad y \mapsto M_y = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$$

440 of the canonical generators  $x$  and  $y$  of  $Q$  induces a homomorphism  $Q^{\mathrm{ab}} := Q/Q' \rightarrow \mathrm{GL}_2(\mathbf{Z}_{p^d})$ .

First suppose that  $Q$  is metacyclic. The results in [8, 20] (see §3) show that

$$Q = \langle g, h \mid g^{q^e} = h^{q^e} = 1, h^g = h^{1+q^f} \rangle,$$

where  $|Q| = q^{2e}$ , with  $f = f_Q$  taking a value  $1, \dots, e$  if  $q > 2$ , or  $2, \dots, e$  if  $q = 2$ , and hence

$$Q^{\mathrm{ab}} = \langle g, h \mid g^{q^e} = h^{q^f} = [g, h] = 1 \rangle.$$

445 The canonical generators of  $Q$  are  $x = g^u$  and  $y = g^u h$ , where  $u = 1, \dots, q^{e-f}$  is coprime to  $q$ , and thus we have an equivalent presentation as follows:

$$Q^{\mathrm{ab}} = \langle x, y \mid x^{q^e} = [x, y] = 1, x^{q^f} = y^{q^f} \rangle.$$

Since  $f \leq e$ , we see that  $M_x$  and  $M_y$  satisfy these relations, giving a diagonal action of  $Q$  with eigenvalue  $\lambda$ , if and only if  $\lambda^{q^f} = 1$ . Since  $q$  divides  $p - 1$ , we have  $p > 2$ , and hence 450 the multiplicative group  $\mathbf{Z}_{p^d}^*$  is cyclic, of order  $\phi(p^d) = (p - 1)p^{d-1}$ . The number of solutions of  $\lambda^{q^f} = 1$  in this group is therefore  $\mathrm{gcd}(q^f, \phi(p^d)) = \mathrm{gcd}(q^f, p - 1) = \mathrm{gcd}(q^f, q^r) = q^m$ , where  $q^r \parallel p - 1$  and  $m = \min\{f, r\}$ .

Now suppose that  $Q$  is not metacyclic; thus  $q = 2$ . As shown in [9] and explained in §3, we have

455 
$$Q = \langle x, y \mid x^{2^e} = y^{2^e} = 1, c := [y, x] = x^{2+k2^{e-1}} y^{-2-k2^{e-1}}, \\ c^x = c^{-1+l2^{e-2}} x^4, c^y = c^{-1-l2^{e-2}} y^{-4} \rangle,$$

where  $e \geq 2$  and  $k, l \in \{0, 1\}$ , with  $k = l = 0$  if  $e = 2$ . Thus

$$Q^{\mathrm{ab}} = \langle x, y \mid x^4 = y^4 = [x, y] = 1, x^{2+k2^{e-1}} = y^{2+k2^{e-1}} \rangle,$$

and hence we obtain a diagonal action of  $Q$  if and only if  $\lambda^2 = 1$ . Since  $p$  is odd, it follows 460 that  $Q$  has two diagonal actions on  $P$ , given by  $\lambda = \pm 1$ . Since we defined  $f_Q = 1$  for the non-metacyclic groups  $Q$ , giving  $m = 1$  and hence  $q^m = 2$ , this is consistent with the statement of the lemma.  $\square$

465 **PROPOSITION 7.5.** *Let  $P, Q$  and  $R$  be Sylow  $p$ -,  $q$ - and  $r$ -subgroups of an  $n$ -isobicyclic group  $G$ , for primes  $p, q$  and  $r$ , respectively, with  $p > q > r$ . If  $R$  acts non-trivially on  $Q$ , then  $Q$  acts trivially on  $P$ .*

*Proof.* Without loss of generality we can take  $P, Q$  and  $R$  to be the canonical Sylow subgroups  $G_p, G_q$  and  $G_r$  of  $G$ . Since  $R$  acts non-trivially on  $Q$ , it follows from Proposition 6.1 (applied to the action by conjugation on  $Q$ , rather than  $P$ ) that  $Q$  must be abelian, and hence  $Q \cong C_{q^e} \times C_{q^e}$ , where  $q^e \parallel n$ . It then follows from Proposition 7.2 (again applied to  $Q$  rather than  $P$ ) that  $R$  acts diagonally on  $Q$ , with an eigenvalue  $\lambda \neq 1$  in  $\mathbf{Z}_{q^e}$ . If  $x_q$  and  $y_q$  are the canonical generators of  $Q$ , and  $x_r$  and  $y_r$  are those of  $R$ , then  $x_q^{y_r} = x_q^\lambda$ , and thus  $[x_q, y_r] = x_q^{\lambda-1}$ , and similarly  $[y_q, x_r] = y_q^{\lambda-1}$ . Now  $\lambda \not\equiv 1 \pmod{q}$ , since the  $q'$ -group  $\langle \lambda \rangle \leq \mathbf{Z}_{q^e}^*$ , acting by multiplication on the additive  $q$ -group  $\mathbf{Z}_{q^e}$ , is represented faithfully on  $\mathbf{Z}_{q^e}/\Phi(\mathbf{Z}_{q^e}) = \mathbf{Z}_{q^e}/q\mathbf{Z}_{q^e} \cong \mathbf{Z}_q$ . It follows that  $x_q^{\lambda-1}$  and  $y_q^{\lambda-1}$  are generators of the groups  $\langle x_q \rangle = X_q$  and  $\langle y_q \rangle = Y_q$ , and hence the subgroup  $Q = X_q Y_q$ , generated by two commutators, is contained in the derived group  $G'$  of  $G$ . If  $P$  is abelian or non-abelian, then  $G$  acts diagonally or trivially on  $P$ , by Propositions 7.2 and 6.1, respectively. In either case,  $G$  induces an abelian group of automorphisms of  $P$ , and since  $Q \leq G'$  it follows that  $Q$  acts trivially on  $P$ .  $\square$

### 8. Isobicyclic groups and directed graphs

Using Corollary 7.3 and Lemma 7.5, we can describe the structure of an isobicyclic triple  $(G, x, y) \in \mathcal{I}(n)$  by means of a labelled directed graph. We will use this idea to give a proof of Theorem 4.5.

Let  $\Pi$  denote the set of all prime numbers, and let  $\rightarrow$  denote the binary relation on  $\Pi$  defined by  $q \rightarrow p$  if and only if  $q$  divides  $p - 1$ ; we can regard  $\Pi$  as a directed graph, with an arc from  $q$  to  $p$  whenever  $q \rightarrow p$ . For each integer  $n \geq 2$ , let  $\Pi_n$  denote the induced subgraph of  $\Pi$  the vertices of which are the prime factors  $p_1, \dots, p_l$  of  $n$ , formed by restricting the relation  $\rightarrow$  to these primes. We say that  $\rightarrow$  is a *short subrelation* of  $\rightarrow$  on  $\Pi_n$  if  $\rightarrow$  is a subrelation of  $\rightarrow$  on  $\Pi_n$  (that is,  $q \rightarrow p$  implies that  $q \rightarrow p$ ) and there is no triple  $p, q, r$  in  $\Pi_n$  with  $r \rightarrow q \rightarrow p$ ; equivalently,  $\rightarrow$  defines a directed subgraph  $\Gamma$  of  $\Pi_n$  which spans  $\Pi_n$  (that is, contains all the vertices of  $\Pi_n$ ), and contains no directed paths of length greater than 1. In these circumstances we call  $\Gamma$  a *short spanning subgraph* of  $\Pi_n$ , written as  $\Gamma \preceq \Pi_n$ .

The motivation for these definitions is that each short subrelation  $\rightarrow$  (equivalently each short spanning subgraph  $\Gamma$ ) represents a choice of which Sylow subgroups of an  $n$ -isobicyclic group  $G$  act non-trivially by conjugation on each other, with  $q \rightarrow p$  meaning that a Sylow  $q$ -subgroup  $Q$  acts non-trivially on a Sylow  $p$ -subgroup  $P$ . By Corollary 7.3, if  $q \rightarrow p$ , then  $q$  divides  $p - 1$ , and thus  $\rightarrow$  must be a subrelation of  $\rightarrow$ . Proposition 7.5 implies that there can be no directed paths  $r \rightarrow q \rightarrow p$  in  $\Gamma$ , and hence this subrelation must be short.

In order to specify an  $n$ -isobicyclic triple  $(G, x, y)$  completely, we need to describe the triples  $(P, x_p, y_p)$  corresponding to the Sylow subgroups  $P = G_p$  of  $G$ , together with the actions  $Q \rightarrow \text{Aut } P$  of these subgroups by conjugation on each other. We do this by attaching labels to the vertices and arcs of  $\Gamma$ , describing these triples and actions. First we define

$$T(\Gamma) = \{p \in \Pi_n \mid q \rightarrow p \text{ for some } q \in \Pi_n\},$$

the set of *terminal* vertices of  $\Gamma$ , and

$$N(\Gamma) = \{p \in \Pi_n \mid q \rightarrow p \text{ for no } q \in \Pi_n\},$$

the set of *non-terminal* vertices. An *isobicyclic labelling*  $\Lambda$  of  $\Gamma$  has two ingredients. First, each vertex  $p$  of  $\Gamma$  is labelled with a triple  $\Lambda(p) = (P, x_p, y_p) \in \mathcal{I}(p^d)$ , where  $p^d \parallel n$ , with the restriction that if  $p \in T(\Gamma)$ , then  $\Lambda(p)$  is the standard triple in  $\mathcal{I}(p^d)$ . Second, each arc  $q \rightarrow p$  in  $\Gamma$  is labelled with an element  $\lambda = \Lambda(q \rightarrow p) \in \mathbf{Z}_{p^d}$  satisfying  $\lambda^{q^m} = 1 \neq \lambda$ , where  $q$  is labelled with  $\Lambda(q) = (Q, x_q, y_q)$ ,  $q^r \parallel p - 1$  and  $m = \min\{f_Q, r\}$  (see § 3 for the definition of  $f_Q$ ).

Each  $n$ -isobicyclic triple  $(G, x, y)$  determines an isobicyclic labelling  $\Lambda = \Lambda(G, x, y)$  of a short spanning subgraph  $\Gamma = \Gamma(G, x, y) \preceq \Pi_n$ : the triple  $\Lambda(p) = (P, x_p, y_p)$  labelling a vertex  $p$  of  $\Pi_n$

represents the canonical Sylow  $p$ -subgroup of  $G$  and its canonical generators, with Corollary 5.2 implying that this triple is isobicyclic; an arc  $q \rightarrow p$  in  $\Gamma$  corresponds to a non-trivial action  $Q \rightarrow \text{Aut } P$  between Sylow subgroups of  $G$ , with Corollary 6.2 implying that  $P$  must then  
 515 be abelian, so that  $\Lambda(p)$  is the standard triple; these arcs define a short subgraph  $\Gamma \preceq \Pi_n$  by Proposition 7.5 and Corollary 7.3; if  $\Lambda(q) = (Q, x_q, y_q)$ , then the arc  $q \rightarrow p$  is labelled with the common non-identity eigenvalue  $\lambda$  of  $x_q$  and  $y_q$  in the diagonal action of  $Q$  on  $P$  (see Corollary 7.3), and this satisfies  $\lambda^{q^m} = 1 \neq \lambda$  by Lemma 7.4.

Let  $\mathcal{L}(n)$  denote the set of all pairs  $(\Gamma, \Lambda)$ , where  $\Lambda$  is an isobicyclic labelling of a short  
 520 spanning subgraph  $\Gamma$  of  $\Pi_n$ . We often refer to these simply as *isobicyclic labellings*. Let  $\mathcal{J}(n)$  denote the subset of  $\mathcal{I}(n)$  consisting of the triples  $(G, x, y)$  satisfying the conclusions of Theorem 4.5. Proving Theorem 4.5 then amounts to showing that  $\mathcal{J}(n) = \mathcal{I}(n)$ .

PROPOSITION 8.1. *Each isobicyclic labelling  $(\Gamma, \Lambda) \in \mathcal{L}(n)$  is induced by a unique triple  $(G, x, y) \in \mathcal{I}(n)$ ; this triple is in  $\mathcal{J}(n)$ .*

525 *Proof.* We first prove the existence of a suitable triple  $(G, x, y) \in \mathcal{J}(n)$  by induction on the number  $l = |\Pi_n|$  of primes dividing  $n$ . The case  $l = 1$  is trivial, with  $(G, x, y) = \Lambda(p) \in \mathcal{J}(n)$  for the unique prime  $p$  dividing  $n$ , and hence we may assume that  $l > 1$  and that existence has been proved for all integers divisible by  $l - 1$  primes.

Let  $p$  be the largest prime dividing  $n$ , so that there are no arcs  $p \rightarrow q$  in  $\Gamma$ , and let  $\Lambda(p) =$   
 530  $(P, x_P, y_P)$ . Let  $\Gamma^*$  be the directed graph formed from  $\Gamma$  by deleting the vertex  $p$  and any incident arcs  $q \rightarrow p$ , and let  $\Lambda^*$  be the restriction of the labelling  $\Lambda$  to  $\Gamma^*$ . Then  $(\Gamma^*, \Lambda^*) \in \mathcal{L}(n^*)$ , where  $n^* = n/p^d$  with  $p^d \parallel n$ , and thus by the induction hypothesis this labelling corresponds to a triple  $(G^*, x^*, y^*) = (T^*, x_{T^*}, y_{T^*}) : (S^*, x_{S^*}, y_{S^*}) \in \mathcal{J}(n^*)$ . Without loss of generality, we can assume that this is the canonical decomposition of this triple, and thus  $S^*$  and  $T^*$  are  
 535 the direct products of the Sylow  $q$ -subgroups  $Q$  of  $G^*$  corresponding to the non-terminal and terminal vertices  $q$  of  $\Gamma^*$ .

If  $P$  is non-abelian, then there are no arcs  $q \rightarrow p$  in  $\Gamma$ , and thus the triple  
 540  $(G, x, y) = (P, x_P, y_P) \times (G^*, x^*, y^*) \in \mathcal{I}(n)$  induces the labelling  $(\Gamma, \Lambda)$ . This triple has the form  $(T, x_T, y_T) : (S, x_S, y_S)$  with  $(T, x_T, y_T) = (T^*, x_{T^*}, y_{T^*})$  and  $(S, x_S, y_S) = (P, x_P, y_P) \times (S^*, x_{S^*}, y_{S^*})$ , and hence it is in  $\mathcal{J}(n)$ .

If  $P$  is abelian, then  $P \cong C_{p^d} \times C_{p^d}$ . We need to show that there is a diagonal action of  $G^*$   
 545 on  $P$  which is consistent with the labelling in  $\Lambda$  of the arcs  $q \rightarrow p$  of  $\Gamma$ . No terminal vertex  $q$  of  $\Gamma^*$  can be the source of an arc  $q \rightarrow p$ , since  $\Gamma$  is short, and thus  $T^*$  must be in the kernel of such an action. We therefore define the action  $G^* \rightarrow \text{Aut } P$  by composing the natural epimorphism  $G^* \rightarrow G^*/T^* \cong S^*$  with the unique extension to  $S^*$  of the actions  $Q \rightarrow \text{Aut } P$  for the Sylow  
 550  $q$ -subgroups  $Q$  of  $G^*$  corresponding to the non-terminal vertices  $q$  of  $\Gamma^*$ . This extension exists since the direct factors  $Q$  of  $S^*$  commute with each other and are represented by diagonal (and hence commuting) matrices on  $P$ ; it is unique since these subgroups  $Q$  generate  $S^*$ . (Indeed, the eigenvalue  $\lambda$  for this action of  $G^*$  is the product of the labels  $\Lambda(q \rightarrow p)$  on the arcs  
 550  $q \rightarrow p$  in  $\Gamma$ .) We now form the extension  $(G, x, y) = (P, x_P, y_P) :_\lambda (G^*, x^*, y^*)$  corresponding to this action. By its construction, this triple is in  $\mathcal{I}(n)$  and it induces the labelling  $(\Gamma, \Lambda)$ . To see that  $(G, x, y) \in \mathcal{J}(n)$ , note that the abelian normal groups  $P$  and  $T^*$  commute and have coprime orders, and thus they generate an abelian normal subgroup  $T = P \times T^*$  in  $G$ ; this is complemented by  $S^*$ , which acts diagonally on  $T$ , and hence  $(G, x, y) = (T, x_T, y_T) : (S, x_S, y_S)$   
 555 with  $(T, x_T, y_T) = (P, x_P, y_P) \times (T^*, x_{T^*}, y_{T^*})$  and  $(S, x_S, y_S) = (S^*, x_{S^*}, y_{S^*})$ .

The uniqueness of  $(G, x, y)$  is similarly proved by induction on  $l$ : any triple in  $\mathcal{I}(n)$  with labelling  $(\Gamma, \Lambda)$  must have the form  $(P, x_P, y_P) \times (G^*, x^*, y^*)$  or  $(P, x_P, y_P) :_\lambda (G^*, x^*, y^*)$  as above; such a product is determined up to isomorphism by the two factors (and, in the latter case, the eigenvalue  $\lambda$ ), and these in turn are uniquely determined by  $(\Gamma, \Lambda)$ .  $\square$

*Proof of Theorem 4.5.* Any  $(G, x, y) \in \mathcal{I}(n)$  induces an isobicyclic labelling  $(\Gamma, \Lambda) \in \mathcal{L}(n)$ . By Proposition 8.1 this is induced by a unique isobicyclic triple, which is in  $\mathcal{J}(n)$ . Thus  $(G, x, y)$  is in  $\mathcal{J}(n)$ , and hence it satisfies the conclusions of Theorem 4.5.  $\square$

Corollary 4.6, which gives a similar decomposition for the maps  $\mathcal{M} \in \mathcal{R}(n)$ , is an immediate consequence of Theorem 4.5.

As observed at the end of § 4, these decompositions of triples and maps are not in general unique. We shall now discuss this lack of uniqueness in terms of isobicyclic labellings; we do so mainly for triples, but the analogous comments apply in the obvious way to maps. Each triple  $(G, x, y) \in \mathcal{I}(n)$  corresponds to a labelling  $(\Gamma, \Lambda) \in \mathcal{L}(n)$ . This triple can be decomposed as a cartesian product of triples in  $\mathcal{I}(n')$  for various divisors  $n'$  of  $n$ , with the indecomposable direct factors corresponding to the connected components of  $\Gamma$ , each with its labelling induced by  $\Lambda$ . In particular, any isolated vertex  $p$  of  $\Gamma$  represents a Sylow  $p$ -subgroup  $P$  which is a direct factor of  $G$ , and if  $\Lambda(p)$  is a standard triple, then the abelian group  $P$  can be regarded as a subgroup of  $S$  or  $T$ . This shows that the decomposition in Theorem 4.5 is not generally unique. However, any terminal vertex  $p$  must correspond to a Sylow  $p$ -subgroup  $P \leq T$ , and hence if we use the canonical decomposition, with  $t$  minimal, then  $T$  is the Hall subgroup  $G_\pi$  for  $\pi = T(\Gamma)$ , the direct product of these Sylow subgroups  $P$  as in the proof of Proposition 8.1. We assume from now on that the canonical decomposition is always used, unless stated otherwise. Then  $\mathcal{M}$ , or equivalently  $(G, x, y)$ , uniquely determines  $t$  and the direct factors  $\mathcal{S}_i$  of  $\mathcal{S}$  in Corollary 4.6, up to a permutation of these factors. It also uniquely determines the eigenvalue  $\lambda$  for the diagonal action of  $S$  on  $T$ ; this is shown by the following result, which also establishes some properties of  $\lambda$  needed in the next section.

LEMMA 8.2. *In the canonical decompositions for  $\mathcal{M}$  and  $(G, x, y)$  we have the following.*

- (i) *The eigenvalue  $\lambda$  for  $S$  on  $T$  is the unique solution in  $\mathbf{Z}_t$  of the congruences  $\lambda \equiv \lambda_p \pmod{(p^d)}$  for each  $p \in \pi = T(\Gamma)$ , where  $p^d \parallel n$  and  $\lambda_p$  is the product in  $\mathbf{Z}_{p^d}^*$  of the labels  $\Lambda(q \rightarrow p)$  attached to the arcs  $q \rightarrow p$  in  $\Gamma$ .*
- (ii) *The multiplicative order  $|\lambda|$  of  $\lambda$  in  $\mathbf{Z}_t^*$  is  $\text{lcm}\{|\lambda_p| \mid p \in \pi\}$ , where the order  $|\lambda_p|$  of  $\lambda_p$  in  $\mathbf{Z}_{p^d}^*$  is the product of the orders of the labels  $\Lambda(q \rightarrow p) \in \mathbf{Z}_{p^d}^*$  on the arcs  $q \rightarrow p$  in  $\Gamma$ .*
- (iii) *If  $t > 1$ , then  $\lambda - 1$  is a unit in  $\mathbf{Z}_t$ .*

*Proof.* (i) The subgroup  $S$  acts diagonally on the Sylow  $p$ -subgroup  $P$  of  $T$  for each prime  $p \in \pi$ . Since  $x_S = x_{\pi'} = \prod_{q \in \pi'} x_q$ , and similarly for  $y_S$ , the eigenvalue  $\lambda_p$  for this action of  $S$  on  $P$  is the product of the eigenvalues for its Sylow  $q$ -subgroups, and this is the product of the labels  $\Lambda(q \rightarrow p)$  on the arcs  $q \rightarrow p$  in  $\Gamma$ . By the Chinese Remainder Theorem, there is a unique  $\lambda \in \mathbf{Z}_t^*$  such that  $\lambda \equiv \lambda_p \pmod{(p^d)}$  for each  $p \in \pi$ , and since  $T$  is the direct sum of its Sylow  $p$ -subgroups, this is the eigenvalue for  $S$  on  $T$ .

(ii) For a given  $p$ , the eigenvalues  $\Lambda(q \rightarrow p)$  have mutually coprime orders (since each is a power of  $q$  by Lemma 7.4), and hence the multiplicative order  $|\lambda_p|$  of  $\lambda_p$  in  $\mathbf{Z}_{p^d}^*$  is the product of the orders of these eigenvalues. Since  $\lambda$  is identified with  $(\lambda_p)$  under the natural isomorphism  $\mathbf{Z}_t^* \cong \prod_{p \in \pi} \mathbf{Z}_{p^d}^*$ , it has multiplicative order  $|\lambda| = \text{lcm}\{|\lambda_p| \mid p \in \pi\}$  in  $\mathbf{Z}_t^*$ .

(iii) By the minimality of  $t$ , each  $p \in \pi$  is a terminal vertex of  $\Gamma$ , and hence  $\lambda_p \neq 1$ . Then Proposition 5.4 implies that  $\lambda_p - 1$  is a unit in  $\mathbf{Z}_{p^d}$  for each  $p$ , and since  $\lambda \equiv \lambda_p \pmod{(p^d)}$  for each  $p$  it follows that  $\lambda - 1$  is a unit in  $\mathbf{Z}_t$ .  $\square$

Note that the exceptional case  $t = 1$  in (iii) corresponds to the situation where  $\mathcal{M} = \mathcal{S} = \mathcal{S}_1 \times \dots \times \mathcal{S}_k$  in Corollary 4.6, with  $\lambda = 1$ .

## 9. Type and genus

605 In the notation of [6], a regular map has type  $\{p, q\}$  if its faces are  $p$ -gons and its vertices have valency  $q$ . If  $\mathcal{M}$  is a regular embedding of  $K_{n,n}$ , corresponding to a triple  $(G, x, y) \in \mathcal{I}(n)$ , then the faces of  $\mathcal{M}$  are all  $2m$ -gons, and thus  $\mathcal{M}$  has type  $\{2m, n\}$ , where  $m = m_G$  is the order  $|xy|$  of  $xy$  in  $G$ . It follows that there are  $n^2/m$  faces, and thus  $\mathcal{M}$  has Euler characteristic

$$\chi = 2n - n^2 + \frac{n^2}{m}$$

610 and genus

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

For instance, it is shown in [8, 20] that if  $\mathcal{M}$  is a metacyclic prime power embedding, then  $m = n$  and thus  $\mathcal{M}$  has type  $\{2n, n\}$  and genus  $(n-1)(n-2)/2$ . However, [9, Equation (2.1)] states that, for  $n = 2^e$ , the non-metacyclic 2-groups  $G(n; k, l)$  described in §3 satisfy

615 
$$y^j x^i = x^{-i} y^{-j} z^{k+l(i+j)/2}$$

for all odd  $i$  and  $j$ , where  $z$  is the central involution  $x^{n/2} y^{n/2}$ , and thus  $(xy)^2 = z^{k+l}$ ; it follows that the non-metacyclic embeddings  $\mathcal{N}(n; 0, 0)$  and  $\mathcal{N}(n; 1, 1)$  have  $m = 2$ , and hence they have type  $\{4, n\}$  and genus  $(n-2)^2/4$ , while  $\mathcal{N}(n; 0, 1)$  and  $\mathcal{N}(n; 1, 0)$  have  $m = 4$ , and thus they have type  $\{8, n\}$  and genus  $1 + n(3n-8)/8$ .

620 LEMMA 9.1. *If  $S$  is as in the canonical decomposition of  $\mathcal{M}$ , then  $m_G = m_S$ .*

*Proof.* By Corollary 4.6 we have  $x = x_S x_T$  and  $y = y_S y_T$ , and thus

$$xy = x_S x_T y_S y_T = x_S y_S y_S^{-1} x_T y_S y_T = ab,$$

where

$$a = x_S y_S \in S \quad \text{and} \quad b = y_S^{-1} x_T y_S y_T \in T.$$

625 We can identify  $T$  with  $\mathbf{Z}_t^2$  so that  $x_T$  and  $y_T$  correspond to the basis elements  $(1, 0)$  and  $(0, 1)$ . Since  $y_S$  acts by conjugation as the matrix  $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$  with respect to this basis, we have  $y_S^{-1} x_T y_S = (\lambda, 0)$  and hence  $b = (\lambda, 1)$ . Since  $x_S$  acts as  $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ , the element  $a = x_S y_S$  acts as  $\lambda I$ . For any  $i \geq 1$  we have

$$(ab)^i = a^i \cdot b^{a^{i-1}} b^{a^{i-2}} \dots b^a b$$

630 with  $a^i \in S$  and each  $b^{a^j} \in T$ ; since  $S \cap T = 1$ , it follows that

$$(xy)^i = 1 \iff a^i = 1 \quad \text{and} \quad b^{a^{i-1}} b^{a^{i-2}} \dots b^a b = 1.$$

We have  $a^i = 1$  if and only if  $i$  is divisible by the order  $m_S$  of  $x_S y_S$  in  $S$ . Each  $b^{a^j}$  is identified with  $\lambda^j (\lambda, 1) = (\lambda^{j+1}, \lambda^j)$  in  $\mathbf{Z}_t^2$ , and hence

$$b^{a^{i-1}} b^{a^{i-2}} \dots b^a b = \sum_{j=0}^{i-1} (\lambda^{j+1}, \lambda^j) = (\lambda + \lambda^2 + \dots + \lambda^i, 1 + \lambda + \dots + \lambda^{i-1}).$$

635 Thus  $b^{a^{i-1}} b^{a^{i-2}} \dots b^a b = 1$  if and only if  $1 + \lambda + \dots + \lambda^{i-1} = 0$  in  $\mathbf{Z}_t$ , and since  $\lambda - 1$  is a unit by Lemma 8.2(iii), this is equivalent to  $\lambda^i = 1$ , that is, to  $i$  being divisible by the multiplicative order  $|\lambda|$  of  $\lambda$  in  $\mathbf{Z}_t^*$ . Since  $\lambda$  is an eigenvalue of  $x_S y_S$  on  $T$ , it follows that  $|\lambda|$  divides  $m_S$ , and hence  $(xy)^i = 1$  if and only if  $i$  is divisible by  $m_S$ . Thus  $xy$  has order  $m_S$ .  $\square$

640 Since  $S$  is the direct product of its Sylow  $q$ -subgroups  $Q$ , we have  $m_S = \prod_{q \in \pi'} m_Q$ , where  $m_Q$  is the order of  $x_q y_q$  in  $Q$  and  $\pi = T(\Gamma)$ . For example, if  $Q$  is metacyclic (as must happen

if  $q > 2$ ), then  $m_q = q^e$ , where  $q^e \parallel n$ ; it follows that  $m_S = s = n_{\pi'}$ , the maximal  $\pi'$ -number dividing  $n$ , unless  $S$  has a non-metacyclic Sylow 2-subgroup, in which case  $m_S = 2n_{\pi^*}$  or  $4n_{\pi^*}$ , where  $\pi^* = \pi' \setminus \{2\}$ . We therefore have the following proposition.

PROPOSITION 9.2. *Let  $\mathcal{M} \in \mathcal{R}(n)$ , corresponding to a pair  $(\Gamma, \Lambda) \in \mathcal{L}(n)$ , and let  $\pi$  be the set of primes which are terminal vertices of  $\Gamma$ .*

(i) *If  $n$  is odd, or if  $n$  is even and the Sylow 2-subgroup  $\Lambda(2)$  is metacyclic, then  $\mathcal{M}$  has type  $\{2n_{\pi'}, n\}$  and genus*

$$1 + \frac{n}{2}(n - n_{\pi} - 2).$$

(ii) *If  $n$  is even and  $\Lambda(2)$  is  $G(n; 0, 0)$  or  $G(n; 1, 1)$ , then  $\mathcal{M}$  has type  $\{4n_{\pi^*}, n\}$  and genus*

$$1 + \frac{n}{2}\left(n - \frac{n_{\pi^+}}{2} - 2\right),$$

where  $\pi^+ = \pi \cup \{2\}$ .

(iii) *If  $n$  is even and  $\Lambda(2)$  is  $G(n; 1, 0)$  or  $G(n; 0, 1)$ , then  $\mathcal{M}$  has type  $\{8n_{\pi^*}, n\}$  and genus*

$$1 + \frac{n}{2}\left(n - \frac{n_{\pi^+}}{4} - 2\right).$$

### 10. Operations on maps

Wilson's operations  $H_j$ , introduced in [31], act on maps  $\mathcal{M}$  by raising the rotation of edges around each vertex to its  $j$ th power, where  $j$  is coprime to the valencies; they preserve the embedded graph, the orientability and the automorphism group of  $\mathcal{M}$ . For instance,  $H_{-1}(\mathcal{M})$  is the mirror image  $\overline{\mathcal{M}}$  of  $\mathcal{M}$ . If a map  $\mathcal{M} \in \mathcal{R}(n)$  corresponds to an isobicyclic triple  $(G, x, y) \in \mathcal{I}(n)$ , and  $j$  is coprime to  $n$ , then  $H_j(\mathcal{M})$  is the map in  $\mathcal{R}(n)$  corresponding to the triple  $H_j(G, x, y) = (G, x^j, y^j) \in \mathcal{I}(n)$ . Similarly, if  $\mathcal{M}$  corresponds to a labelling  $(\Gamma, \Lambda) \in \mathcal{L}(n)$ , then  $H_j(\mathcal{M})$  corresponds to the labelling  $(\Gamma, \Lambda^j) \in \mathcal{L}(n)$  defined by  $\Lambda^j(p) = H_j(\Lambda(p))$  for each vertex  $p$  of  $\Gamma$  and  $\Lambda^j(q \rightarrow p) = \Lambda(q \rightarrow p)^j$  for each arc  $q \rightarrow p$ . This gives isomorphic actions of the multiplicative group  $\mathbf{Z}_n^*$  on the sets  $\mathcal{R}(n)$ ,  $\mathcal{I}(n)$  and  $\mathcal{L}(n)$ . For instance, if  $\Lambda(p)$  is a metacyclic triple  $(P, x_p, y_p)$ , corresponding to a map  $\mathcal{M}(p^e, f, u) \in \mathcal{R}(p^e)$  in the notation of §3, then  $\Lambda^j(p)$  corresponds to the map  $H_j(\mathcal{M}(p^e, f, u)) = \mathcal{M}(p^e, f, ju) \in \mathcal{R}(p^e)$ ; for a given pair  $p^e$  and  $f$  (equivalently, for a given  $p^e$ -isobicyclic group  $P = G_f$ ), these maps form a single orbit of  $\mathbf{Z}_n^*$ , as shown in [8, 20]. The non-metacyclic maps  $\mathcal{M} = \mathcal{N}(2^e; k, l)$  in  $\mathcal{R}(2^e)$  have mutually non-isomorphic orientation-preserving automorphism groups  $\text{Aut}^+ \mathcal{M}$ , and thus they are invariant under  $H_j$  for each odd  $j$ .

The operation  $H_{-1}$  is of particular interest. An orientably regular map  $\mathcal{M}$  is said to be reflexible if it has an automorphism reversing the orientation, or equivalently  $\mathcal{M}$  is isomorphic (as an oriented map) to its mirror image  $\overline{\mathcal{M}} = H_{-1}(\mathcal{M})$ ; otherwise  $\mathcal{M}$  and  $\overline{\mathcal{M}}$  form a chiral pair. If a map  $\mathcal{M} \in \mathcal{R}(n)$  corresponds to an isobicyclic triple  $(G, x, y) \in \mathcal{I}(n)$ , then  $\overline{\mathcal{M}}$  corresponds to the triple  $(G, x^{-1}, y^{-1})$ , and hence  $\mathcal{M}$  is reflexible if and only if  $G$  has an automorphism inverting  $x$  and  $y$ ; we then say that  $(G, x, y)$  is reflexible. Similarly, if  $\mathcal{M}$  corresponds to an isobicyclic labelling  $(\Gamma, \Lambda) \in \mathcal{L}(n)$ , then  $\overline{\mathcal{M}}$  corresponds to the labelling  $(\Gamma, \overline{\Lambda})$ , where  $\overline{\Lambda}(p) = (P, x_p^{-1}, y_p^{-1})$  if a vertex  $p$  has label  $\Lambda(p) = (P, x_p, y_p)$ , and  $\overline{\Lambda}(q \rightarrow p) = \Lambda(q \rightarrow p)^{-1}$  for each arc  $q \rightarrow p$ . It follows that  $\mathcal{M}$  is reflexible if and only if  $\Lambda(p)$  is reflexible for each vertex  $p$  of  $\Gamma$  and  $\Lambda(q \rightarrow p)^2 = 1$  for each arc  $q \rightarrow p$  of  $\Gamma$ . This allows us to classify and to count the reflexible embeddings by considering their corresponding labellings.

First we consider vertex labels  $\Lambda(p)$ . It is shown in [20] that, for an odd prime  $p$ , the only reflexible map in  $\mathcal{R}(p^e)$  is the standard embedding, corresponding to an abelian Sylow  $p$ -subgroup  $P \cong C_{p^e} \times C_{p^e}$  of  $G$ , and hence the only reflexible label  $\Lambda(p) \in \mathcal{I}(p^e)$  is the standard

triple  $(P, x_p, y_p)$ . In the case  $p = 2$ , however, there are extra possibilities. First, as shown in  
 685 [8], the reflexible metacyclic maps in  $\mathcal{R}(2^e)$  are the standard embedding  $\mathcal{S}(2^e) = \mathcal{M}(2^e, e, 1)$ ,  
 with  $P \cong C_{2^e} \times C_{2^e}$ , and also (provided  $e \geq 3$ ) the map  $\mathcal{M}(2^e, e - 1, 1)$ , corresponding to a  
 non-abelian group  $P$  with  $f = e - 1$ . In addition, the non-metacyclic maps  $\mathcal{N}(2^e; k, l)$  in  $\mathcal{R}(2^e)$   
 are all reflexible: there is one such map if  $e = 2$ , and there are four for each  $e \geq 3$ . Thus when  
 $n$  is even, the number of possibilities for a reflexible label  $\Lambda(2)$  is 1, 2 or 6 as  $2^e \parallel n$  with  $e = 1$ ,  
 690  $e = 2$  or  $e \geq 3$ , respectively.

We now consider which arc labels  $\lambda = \Lambda(q \rightarrow p)$  can satisfy  $\lambda^2 = 1$ . By Lemma 7.4 we have  
 $\lambda^{q^m} = 1$  for some  $m$ , and hence if  $q$  is odd, then the only solution is  $\lambda = 1$ ; this corresponds  
 to the trivial action of a Sylow  $q$ -subgroup  $Q$  on a Sylow  $p$ -subgroup  $P$ , and thus it cannot  
 be the label of an arc in  $\Gamma$ . It follows that if  $\mathcal{M}$  is reflexible, then any arc in  $\Gamma$  must have the  
 695 form  $2 \rightarrow p$ . In particular, if  $n$  is odd, then  $\Gamma$  must be the null graph; each vertex label  $\Lambda(p)$   
 is a standard triple, since  $p$  is odd, and hence in this case the standard embedding is the only  
 reflexible map in  $\mathcal{R}(n)$ . If  $n$  is even, then any arc  $2 \rightarrow p$  in  $\Gamma$  must be labelled with  $\lambda = -1$ ,  
 since this is the only solution of  $\lambda^2 = 1 \neq \lambda$  when  $p$  is odd, and conversely Lemma 7.4 shows  
 that each of the reflexible 2-subgroups  $Q$  listed above can act diagonally on  $P$  with eigenvalue  
 700  $\lambda = -1$ . It follows that if  $n$  is divisible by  $r$  odd primes  $p$ , then each of the  $2^r$  possible subgraphs  
 $\Gamma \preceq \Pi_n$  (one for each choice of a set of arcs  $2 \rightarrow p$ ) has a unique isobicyclic arc-labelling. Taking  
 account of the number of possible vertex-labellings, considered above, we see that the number  
 $\rho(n)$  of reflexible embeddings of  $K_{n,n}$  is given by

$$\rho(n) = \begin{cases} 1 & \text{if } e = 0, \\ 2^r & \text{if } e = 1, \\ 2^{r+1} & \text{if } e = 2, \\ 3 \cdot 2^{r+1} & \text{if } e \geq 3, \end{cases}$$

705 where

$$n = 2^e p_1^{e_1} \dots p_r^{e_r}$$

for distinct odd primes  $p_i$  and integers  $e_i \geq 1$ . This agrees with the enumeration recently  
 obtained by Kwak and Kwon [25], using a different method. The remaining maps in  $\mathcal{R}(n)$   
 occur in chiral pairs, and the number  $\chi(n)$  of such pairs can now be obtained from the formula

$$710 \quad \chi(n) = \frac{1}{2}(\nu(n) - \rho(n)),$$

where  $\nu(n)$  is the number  $|\mathcal{R}(n)|$  of regular embeddings of  $K_{n,n}$ , to be determined in the next  
 two sections.

The above argument also gives an explicit description of the reflexible embeddings  $\mathcal{M}$  of  
 $K_{n,n}$ . As we have seen, if  $n$  is odd, then  $\mathcal{M}$  is the standard embedding, and hence we may  
 715 assume that  $n$  is even. In the notation of Corollary 4.6, some direct factor of  $\mathcal{S}$ , which we can  
 take to be  $\mathcal{S}_1$ , is one of the reflexible maps in  $\mathcal{R}(2^e)$  described above, while  $\mathcal{S}_2, \dots, \mathcal{S}_k$ , which  
 are direct factors of  $\mathcal{M}$ , are all standard embeddings. In the canonical decomposition,  $\mathcal{S}$  acts  
 diagonally on  $T$  with eigenvalue  $-1$  (so that  $\mathcal{S}_2, \dots, \mathcal{S}_k$ , having odd orders, act trivially), and

$$\mathcal{M} \cong (\mathcal{T} : \mathcal{S}_1) \times \mathcal{S}_2 \times \dots \times \mathcal{S}_k \cong (\mathcal{T} : \mathcal{S}_1) \times \mathcal{S}(n/2^e t). \quad (10.1)$$

720 The Petrie dual  $P(\mathcal{M})$  of a map  $\mathcal{M}$ , also discussed in [31], has the same embedded graph  
 as  $\mathcal{M}$ , and has new faces, bounded by the Petrie polygons (closed zig-zag paths) of  $\mathcal{M}$ ; thus  
 $\text{Aut } \mathcal{M} = \text{Aut } P(\mathcal{M})$ . If  $\mathcal{M} \in \mathcal{R}(n)$ , then  $P(\mathcal{M})$  is an embedding of  $K_{n,n}$ , and is orientable  
 since this graph is bipartite, but it need not be regular; if it is, then  $\mathcal{M}$  must be reflexible,  
 since a half-turn reversing an edge of  $P(\mathcal{M})$  acts as a reflection reversing the same edge of  $\mathcal{M}$ .  
 725 We will therefore consider the effect of the Petrie duality operation  $P$  on the reflexible maps  
 $\mathcal{M} \in \mathcal{R}(n)$ .

If such a map  $\mathcal{M}$  corresponds to a triple  $(G, x, y) \in \mathcal{I}(n)$ , then  $P(\mathcal{M})$  corresponds to the triple  $(G, x, y^{-1})$ : this is in  $\mathcal{I}(n)$  since the automorphism of  $G$  transposing  $x$  and  $y$ , composed with the automorphism inverting them, gives an automorphism transposing  $x$  and  $y^{-1}$ . The Petrie polygons of  $\mathcal{M}$  are  $2m'$ -gons, and hence  $P(\mathcal{M})$  has type  $\{2m', n\}$ , where  $m'$  is the order of  $xy^{-1}$ . By arguments similar to those used in the case of the operation  $H_{-1}$ , if  $\mathcal{M}$  corresponds to a pair  $(\Gamma, \Lambda) \in \mathcal{L}(n)$ , then  $P(\mathcal{M})$  corresponds to the pair  $(\Gamma, P(\Lambda))$ , where the labelling  $P(\Lambda)$  is obtained from  $\Lambda$  by replacing each vertex label  $\Lambda(p) = (P, x_P, y_P)$  with  $(P, x_P, y_P^{-1})$ ; all the arc labels  $\lambda = \Lambda(q \rightarrow p)$  satisfy  $\lambda^{-1} = \lambda$ , and thus they are unchanged.

We say that a map  $\mathcal{M}$  is *self-Petrie* if  $\mathcal{M} \cong P(\mathcal{M})$ . A map  $\mathcal{M} \in \mathcal{R}(n)$  is self-Petrie if and only if  $G$  has an automorphism fixing  $x$  and inverting  $y$ , or equivalently the vertex labels  $\Lambda(p)$  are all self-Petrie. Since every standard embedding is self-Petrie, it follows that if  $\mathcal{M}$  is as in (10.1), then

$$P(\mathcal{M}) \cong (\mathcal{T} : P(\mathcal{S}_1)) \times \mathcal{S}_2 \times \dots \times \mathcal{S}_k \cong (\mathcal{T} : P(\mathcal{S}_1)) \times \mathcal{S}(n/2^e t).$$

Thus  $\mathcal{M}$  is self-Petrie if and only if  $\mathcal{S}_1$  is self-Petrie. Of the reflexible maps in  $\mathcal{R}(2^e)$  described above, all are self-Petrie with the exception of  $\mathcal{N}(2^e; 0, 1)$  and  $\mathcal{N}(2^e; 1, 1)$ , which are Petrie duals of each other for each  $e \geq 3$ . (Note that  $\text{Aut } \mathcal{N}(2^e; 0, 1) \cong \text{Aut } \mathcal{N}(2^e; 1, 1)$ , even though  $\text{Aut}^+ \mathcal{N}(2^e; 0, 1) \not\cong \text{Aut}^+ \mathcal{N}(2^e; 1, 1)$ .) It follows that a reflexible map  $\mathcal{M} \in \mathcal{R}(n)$  is self-Petrie if and only if  $\mathcal{S}_1$  is not one of these two maps, and hence the number  $\sigma(n)$  of self-Petrie maps in  $\mathcal{I}(n)$  is given by

$$\sigma(n) = \begin{cases} 1 & \text{if } e = 0, \\ 2^r & \text{if } e = 1, \\ 2^{r+1} & \text{if } e = 2, \\ 2^{r+2} & \text{if } e \geq 3, \end{cases}$$

where  $2^e \parallel n$  and  $n$  is divisible by  $r$  distinct odd primes. As in the case of reflexivity, this agrees with the enumeration obtained by Kwak and Kwon [25].

### 11. Enumeration: $n$ odd

Having used the bijections between  $\mathcal{R}(n)$ ,  $\mathcal{I}(n)$  and  $\mathcal{L}(n)$  to count the reflexible and self-Petrie embeddings of  $K_{n,n}$ , we can use the same method to count all its regular embeddings. By Theorem 2.1, the mapping  $\mathcal{M} \mapsto (G, x, y)$  induces a bijection  $\mathcal{R}(n) \rightarrow \mathcal{I}(n)$ , and thus the number

$$\nu(n) = |\mathcal{R}(n)|$$

of regular embeddings of  $K_{n,n}$  is equal to the number  $|\mathcal{I}(n)|$  of  $n$ -isobicyclic triples (up to isomorphism in each case). By Proposition 8.1 the mapping  $(G, x, y) \mapsto (\Gamma, \Lambda)$  is a bijection  $\mathcal{I}(n) = \mathcal{J}(n) \rightarrow \mathcal{L}(n)$ , and thus  $\nu(n)$  is also equal to the number  $|\mathcal{L}(n)|$  of isobicyclic labellings of short spanning subgraphs  $\Gamma \preceq \Pi_n$ . We can therefore enumerate maps by enumerating labellings. We do this first in the simplest case, when  $n$  is odd.

Given  $\Gamma$ , if  $q \in N(\Gamma)$  and  $q > 2$ , then by [20] there are  $\phi(q^{e_q - f})$  possible labels  $\Lambda(q) = (Q, x_q, y_q)$  for  $q$  for each  $f = 1, \dots, e_q$ , where  $q^{e_q} \parallel n$ ; given any  $p \in \Pi_n$  such that  $q \rightarrow p$ , Lemma 7.4 implies that there are  $q^{f_{q,p}}$  possible diagonal actions of  $Q$  on the abelian group  $P$ , where  $f_{q,p} = \min\{f, r(q, p)\}$  and we define  $r = r(q, p)$  by  $q^r \parallel p - 1$ . One of these is a trivial action, and hence there are  $q^{f_{q,p}} - 1$  non-trivial actions of  $Q$  on  $P$ . It follows that there are

$$\sum_{f=1}^{e_q} \left( \phi(q^{e_q - f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1) \right)$$

possible labels for  $q$  and its incident arcs  $q \rightarrow p$  in  $\Gamma$ . If  $q \in T(\Gamma)$ , then Lemma 7.5 implies that there is only one possibility for  $Q$  and its actions, namely that  $Q$  is abelian and that it acts trivially on all  $P$ . It follows that if  $n$  is odd, then there are

$$\prod_{q \in N(\Gamma)} \left( \sum_{f=1}^{e_q} (\phi(q^{e_q-f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1)) \right)$$

isobicyclic labellings  $\Lambda$  of each short spanning subgraph  $\Gamma \preceq \Pi_n$ . Using the bijection  $\mathcal{R}(n) \rightarrow \mathcal{L}(n)$  described above we therefore have the following.

**THEOREM 11.1.** *If  $n$  is odd, then*

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left( \prod_{q \in N(\Gamma)} \left( \sum_{f=1}^{e_q} (\phi(q^{e_q-f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1)) \right) \right).$$

For each  $\Gamma \preceq \Pi_n$ , the corresponding summand in this formula is non-negative, and thus it provides a lower bound for  $\nu(n)$ . Taking  $\Gamma$  to be the null graph, for which  $N(\Gamma) = \Pi_n$  and  $\prod_{q \rightarrow p} (q^{f_{q,p}} - 1)$  is the empty product, equal to 1 for all primes  $q$  dividing  $n$ , we see that

$$\nu(n) \geq \prod_{q|n} \left( \sum_{f=1}^{e_q} \phi(q^{e_q-f}) \right) = \prod_{q|n} q^{e_q-1} = n / \prod_{q|n} q.$$

This lower bound, first obtained in [20], represents the number of embeddings in  $\mathcal{R}(n)$  for which  $G$  is nilpotent. It is attained if and only if  $\Pi_n$  is itself a null graph, that is, no primes  $p$  and  $q$  dividing  $n$  satisfy  $p \equiv 1 \pmod{q}$ . In particular, an odd integer  $n$  satisfies  $\nu(n) = 1$  if and only if  $\Pi_n$  is null and  $e_q = 1$  for each prime  $q$  dividing  $n$ , or equivalently  $\gcd(n, \phi(n)) = 1$ , a result first obtained in [21].

The formula in Theorem 11.1 simplifies considerably when  $n$  is divisible by a small number of primes. In [20] it was shown that  $\nu(p^e) = p^{e-1}$  for each odd prime  $p$  (see also [24, 27] for the cases  $e = 1$  and  $e = 2$ ), and hence here we deal with the case where  $n$  is divisible by two odd primes. We considered the type and genus of the corresponding maps in Example 9.2.

**COROLLARY 11.2.** *Let  $n = p_1^d p_2^e$ , where  $p_1$  and  $p_2$  are odd primes, with  $d, e \geq 1$  and  $p_1 > p_2$ . Then*

$$\nu(n) = p_1^{d-1} p_2^{e-1} + \min\{e, r\} (p_2^e - p_2^{e-1}),$$

where  $p_2^r \parallel p_1 - 1$ .

*Proof.* In this case  $\Pi_n$  has two vertices  $p_1$  and  $p_2$ , with an arc  $p_2 \rightarrow p_1$  if and only if  $r \geq 1$ , and thus each  $\Gamma \preceq \Pi_n$  is either the null graph or equal to  $\Pi_n$ , the latter possible only if  $r \geq 1$ .

If  $\Gamma$  is the null graph, then  $q \in N(\Gamma)$  for both  $q = p_1$  and  $q = p_2$ , and in each case  $\prod_{q \rightarrow p} (q^{f_{q,p}} - 1)$  is the empty product, equal to 1; thus the number of embeddings corresponding to  $\Gamma$  is given by

$$\sum_{f=1}^d \phi(p_1^{d-f}) \sum_{f=1}^e \phi(p_2^{e-f}) = p_1^{d-1} p_2^{e-1}. \tag{11.1}$$

If  $r = 0$ , so that  $p_2$  does not divide  $p_1 - 1$ , these are the only embeddings, but if  $r \geq 1$ , then there are additional embeddings corresponding to  $\Gamma = \Pi_n$ . In this case  $N(\Gamma)$  consists of a single prime  $q = p_2$ , with  $q \rightarrow p$  if and only if  $p = p_1$ , and hence the number of embeddings

corresponding to  $\Gamma$  is given by

$$\sum_{f=1}^e \phi(p_2^{e-f})(p_2^{f p_2 \cdot p_1} - 1), \tag{11.2}$$

where  $f_{p_2, p_1} = \min\{f, r\}$  and  $p_2^r \parallel p_1 - 1$ . If  $r \geq e$  (equivalently  $p_2^e \mid p_1 - 1$ ) then  $f_{p_2, p_1} = f$  for each  $f = 1, \dots, e$ , and hence the number of embeddings obtained in (11.2) is given by

$$\begin{aligned} \sum_{f=1}^e \phi(p_2^{e-f})(p_2^f - 1) &= \sum_{f=1}^e \phi(p_2^{e-f})p_2^f - \sum_{f=1}^e \phi(p_2^{e-f}) \\ &= \sum_{f=1}^{e-1} (p_2^{e-f} - p_2^{e-f-1})p_2^f + p_2^e - p_2^{e-1} \\ &= (e-1)(p_2^e - p_2^{e-1}) + p_2^e - p_2^{e-1} \\ &= e(p_2^e - p_2^{e-1}). \end{aligned} \tag{11.3}$$

If  $r < e$ , then  $f_{p_2, p_1} = f$  for each  $f = 1, \dots, r$ , and  $f_{p_2, p_1} = r$  for each  $f = r, \dots, e$ ; for each  $f = r + 1, \dots, e$  we must therefore replace the summand  $\phi(p_2^{e-f})(p_2^f - 1)$  in the calculation (11.3) with  $\phi(p_2^{e-f})(p_2^r - 1)$ , thus subtracting

$$\begin{aligned} \sum_{f=r+1}^e \phi(p_2^{e-f})(p_2^f - p_2^r) &= \sum_{f=r+1}^{e-1} (p_2^{e-f} - p_2^{e-f-1})(p_2^f - p_2^r) + p_2^e - p_2^r \\ &= (e-1-r)(p_2^e - p_2^{e-1}) - \sum_{f=r+1}^{e-1} (p_2^{e-f+r} - p_2^{e-f-1+r}) + p_2^e - p_2^r \\ &= (e-1-r)(p_2^e - p_2^{e-1}) - (p_2^{e-1} - p_2^r) + p_2^e - p_2^r \\ &= (e-r)(p_2^e - p_2^{e-1}) \end{aligned}$$

from the final total, and hence in this case the number of embeddings obtained in (11.2) is given by

$$e(p_2^e - p_2^{e-1}) - (e-r)(p_2^e - p_2^{e-1}) = r(p_2^e - p_2^{e-1}). \tag{11.4}$$

Combining the two possibilities  $r \geq e$  and  $r < e$  covered by (11.3) and (11.4), we see that the number of embeddings corresponding to  $\Gamma = \Pi_n$  in (11.2) is given by

$$\min\{e, r\}(p_2^e - p_2^{e-1}).$$

Adding this to (11.1) we find that the total number of embeddings is given by

$$\nu(n) = p_1^{d-1}p_2^{e-1} + \min\{e, r\}(p_2^e - p_2^{e-1}). \quad \square$$

The embeddings enumerated by the first summand  $p_1^{d-1}p_2^{e-1}$ , corresponding to the null graph  $\Gamma$ , are simply the cartesian products of the maps in  $\mathcal{R}(p_1^d)$  and  $\mathcal{R}(p_2^e)$ . These embeddings have  $\pi = \emptyset$  in Proposition 9.2, and thus they have type  $\{2n, n\}$  and genus given by

$$g = \frac{(n-1)(n-2)}{2}.$$

If  $r \geq 1$ , then the embeddings enumerated by the second summand have  $\pi = \{p_1\}$ , and thus by Proposition 9.2 they have type  $\{2p_2^e, n\}$  and genus given by

$$g = 1 + \frac{n}{2} \left( n - p_1^d - 2 \right).$$

TABLE 1. Values of  $\nu(n) = |\mathcal{R}(n)|$  for  $1 \leq n \leq 120$ .

$n$	$\nu(n)$										
1	1	21	3	41	1	61	1	81	27	101	1
2	1	22	2	42	8	62	2	82	2	102	4
3	1	23	1	43	1	63	9	83	1	103	1
4	2	24	12	44	4	64	20	84	16	104	16
5	1	25	5	45	3	65	1	85	1	105	3
6	2	26	2	46	2	66	4	86	2	106	2
7	1	27	9	47	1	67	1	87	1	107	1
8	6	28	4	48	16	68	6	88	12	108	20
9	3	29	1	49	7	69	1	89	1	109	1
10	2	30	4	50	6	70	4	90	8	110	12
11	1	31	1	51	1	71	1	91	1	111	3
12	4	32	12	52	6	72	24	92	4	112	16
13	1	33	1	53	1	73	1	93	3	113	1
14	2	34	2	54	10	74	2	94	2	114	8
15	1	35	1	55	5	75	5	95	1	115	1
16	8	36	8	56	12	76	4	96	24	116	6
17	1	37	1	57	3	77	1	97	1	117	9
18	4	38	2	58	2	78	8	98	8	118	2
19	1	39	3	59	1	79	1	99	3	119	1
20	6	40	16	60	12	80	24	100	14	120	32

830 Corollary 11.2, together with the results for odd prime powers obtained in [20] (see §3), covers all odd  $n \leq 120$  with the exception of  $n = 105 = 3 \cdot 5 \cdot 7$ , where Theorem 11.1 is required; the corresponding values of  $\nu(n)$  are given in Table 1, together with those for even  $n$  to be considered in §12.

835 Kwak and Kwon [24] have developed a different method for studying the regular embeddings of  $K_{n,n}$ , based on describing them in terms of permutations in the symmetric group  $S_n$ . For instance, they deal with the case where  $n$  is a product of two primes, obtaining the enumeration in Corollary 11.2 in the case  $d = e = 1$ . They have used this method to carry out a computer analysis of the maps in  $\mathcal{R}(n)$  for all  $n \leq 20$ , and Fujisaki (private communication, via R. Nedela, April 2006) has extended their enumeration to  $n \leq 100$ . The values for  $\nu(n)$  given here agree with those of Fujisaki for all odd  $n$  in this range.

### 12. Enumeration: $n$ even

The method of enumeration used in §11 can also be used when  $n$  is even, so that  $2 \in N(\Gamma)$  for all  $\Gamma \preceq \Pi_n$ . Suppose that  $2^{e_2} \parallel n$ , with  $e_2 \geq 1$ . The following result shows that the formula in Theorem 11.1 for  $n$  odd is in fact valid for all  $n$  not divisible by 8.

845 THEOREM 12.1. *If  $1 \leq e_2 \leq 2$ , and thus  $2 \parallel n$  or  $2^2 \parallel n$ , then*

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left( \prod_{q \in N(\Gamma)} \left( \sum_{f=1}^{e_q} (\phi(q^{e_q-f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1)) \right) \right).$$

850 *Proof.* If  $e_2 = 1$ , then the label  $\Lambda(2)$  attached to the vertex  $q = 2$  of  $\Pi_n$  must be the standard triple in  $\mathcal{I}(2)$ , and the Sylow 2-subgroup  $Q \cong C_2 \times C_2$  of  $G$  has two possible actions on an abelian Sylow  $p$ -subgroup  $P$  for  $p > 2$ , with eigenvalues  $\pm 1$ . This is consistent with the formula in Theorem 11.1, with  $f = 1$  and the number of actions given by  $2^{f_{2,p}}$ .

If  $e_2 = 2$ , then there is one metacyclic Sylow 2-subgroup  $Q$  which can occur, namely  $C_4 \times C_4$ , corresponding to  $f = 2$ ; unlike in the odd prime power case, there is no metacyclic group for  $f = 1$ , but instead there is one non-metacyclic group  $Q = G(4; 0, 0)$  which can occur. The number of possible actions of  $C_4 \times C_4$  on  $P$  is  $2^{f_{2,p}}$ , and for  $G(4; 0, 0)$  it is 2, which is the value of  $2^{f_{2,p}}$  when  $f = 1$ . Thus the formula in Theorem 11.1 remains valid when  $e_2 = 2$ .  $\square$

855

Similar arguments show that Corollary 11.2 also applies when  $p_2 = 2$  and  $e = 1$  or 2. If  $e = 1$ , and thus  $n = 2p_1^d$  for an odd prime  $p_1$ , it gives  $\nu(n) = p_1^{d-1} + 1$ , and if  $e = 2$ , and thus  $n = 4p_1^d$ , it gives  $\nu(n) = 2p_1^{d-1} + 4$  or  $2p_1^{d-1} + 2$  as  $p_1 \equiv 1$  or  $-1 \pmod{4}$ .

The situation is more complicated when  $n$  is divisible by a higher power of 2.

**THEOREM 12.2.** *If  $n$  is divisible by 8, then*

860

$$\nu(n) = \sum_{\Gamma \preceq \Pi_n} \left( \left( \sum_{f=2}^{e_2} (\phi(2^{e_2-f}) \prod_{2 \rightarrow p} (2^{f_{2,p}} - 1)) + 4 \right) \prod_{2 \neq q \in N(\Gamma)} \left( \sum_{f=1}^{e_q} (\phi(q^{e_q-f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1)) \right) \right).$$

An equivalent version of this formula is as follows:

$$\begin{aligned} \nu(n) = & \sum_{\Gamma \preceq \Pi_n} \left( \prod_{q \in N(\Gamma)} \left( \sum_{f=1}^{e_q} (\phi(q^{e_q-f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1)) \right) \right) \\ & + (4 - 2^{e_2-2}) \sum_{\Gamma \preceq \Pi_n} \left( \prod_{2 \neq q \in N(\Gamma)} \left( \sum_{f=1}^{e_q} (\phi(q^{e_q-f}) \prod_{q \rightarrow p} (q^{f_{q,p}} - 1)) \right) \right). \end{aligned}$$

*Proof.* If  $e_2 \geq 3$ , then there are  $2^{e_2-2}$  metacyclic 2-groups  $Q$  which can occur, namely  $\phi(2^{e_2-f})$  for each  $f = 2, \dots, e_2$  (again,  $f = 1$  is excluded), and in addition there are four non-metacyclic groups. In the metacyclic case, the number of possible actions of  $Q$  on an abelian Sylow  $p$ -subgroup  $P$  is again  $2^{f_{2,p}}$ . In the non-metacyclic case, there are two actions for each  $Q$ , with eigenvalues  $\lambda = \pm 1$ . It follows that, for a given  $\Gamma \preceq \Pi_n$ , the number of possibilities for  $Q$  and its (non-trivial) actions on the Sylow  $p$ -subgroups such that  $2 \rightarrow p$  is given by

865

870

$$\sum_{f=2}^{e_2} \left( \phi(2^{e_2-f}) \prod_{2 \rightarrow p} (2^{f_{2,p}} - 1) \right) + 4.$$

When  $f = 1$  we have  $f_{2,p} = 1$  for all odd primes  $p$ , and thus the ‘missing’ summand for  $f = 1$  is given by

$$\phi(2^{e_2-1}) \prod_{2 \rightarrow p} (2^{f_{2,p}} - 1) = \phi(2^{e_2-1}) = 2^{e_2-2}$$

and hence we can write the number of possibilities for  $Q$  and its actions as follows:

875

$$\sum_{f=1}^{e_2} \left( \phi(2^{e_2-f}) \prod_{2 \rightarrow p} (2^{f_{2,p}} - 1) \right) - 2^{e_2-2} + 4.$$

The main sum here is given by putting  $q = 2$  in the corresponding formula for odd primes  $q$ , and we can regard  $-2^{e_2-2} + 4$  as a ‘correction term’ for  $e_2 \geq 3$ .  $\square$

This correction term is 0 if  $e_2 = 4$ , and hence the formulas in Theorem 11.1 and Corollary 11.2 are also valid in this case. Thus if  $n = 16p_1^d$  for an odd prime  $p_1$ , then Corollary 11.2 implies that  $\nu(n) = 8p_1^{d-1} + 8 \min\{4, r\}$ , where  $2^r \parallel p_1 - 1$ . More generally, the analogue of Corollary 11.2 for even  $n$  is as follows.

880

EXAMPLE 12.3. Let  $n = 2^e p_1^d$ , where  $p_1$  is an odd prime, let  $e \geq 3$  and let  $d \geq 1$ . As in Corollary 11.2, the first term takes the value

$$2^{e-1} p_1^{d-1} + \min\{e, r\}(2^e - 2^{e-1}) = 2^{e-1}(p_1^{d-1} + \min\{e, r\}),$$

where  $2^r \parallel p_1 - 1$ . In the second summation, if  $\Gamma = \Pi_n$ , then there is no odd  $q$  in  $N(\Gamma)$ , and thus the product is the empty product, with value 1. If  $\Gamma$  is the null subgraph, then  $N(\Gamma) = \{p_1\}$ , and there is no  $p$  such that  $p_1 \rightarrow p$ , and hence we have

$$\begin{aligned} \nu(n) &= 2^{e-1}(p_1^{d-1} + \min\{e, r\}) + (4 - 2^{e-2})(1 + p_1^{d-1}) \\ &= (2^{e-2} + 4)p_1^{d-1} + (2\min\{e, r\} - 1)2^{e-2} + 4. \end{aligned}$$

For instance, if  $e = 3$ , and thus  $n = 8p_1^d$ , then

$$\nu(n) = \begin{cases} 6p_1^{d-1} + 14 & \text{if } p_1 \equiv 1 \pmod{8}, \\ 6p_1^{d-1} + 10 & \text{if } p_1 \equiv 5 \pmod{8}, \\ 6p_1^{d-1} + 6 & \text{if } p_1 \equiv 3 \text{ or } 7 \pmod{8}. \end{cases}$$

Similarly, if  $e = 4$ , and thus  $n = 16p_1^d$ , then

$$\nu(n) = \begin{cases} 8p_1^{d-1} + 32 & \text{if } p_1 \equiv 1 \pmod{16}, \\ 8p_1^{d-1} + 24 & \text{if } p_1 \equiv 9 \pmod{16}, \\ 8p_1^{d-1} + 16 & \text{if } p_1 \equiv 5 \text{ or } 13 \pmod{16}, \\ 8p_1^{d-1} + 8 & \text{if } p_1 \equiv 3, 7, 11 \text{ or } 15 \pmod{16}. \end{cases}$$

These results, together with those for  $n = 2^e$  in [8, 9], account for most of the entries for even  $n \leq 120$  in Table 1; the remaining entries can be obtained from Theorem 12.1. For  $n \leq 20$  the resulting values of  $\nu(n)$  all agree with those in [24], and for  $n \leq 100$  as found by Fujisaki (private communication), except that the latter gives  $\nu(90) = 6$ . This may simply be a transcription error, as there are seven rather obvious embeddings for  $n = 90$  which decompose as cartesian products, together with one indecomposable embedding. This is the only integer  $n \leq 100$  for which our value for  $\nu(n)$  differs from that in Fujisaki.

### 13. The directed graphs $\Pi_n$

The vertices of the directed graph  $\Pi_n$  are the primes  $p$  dividing  $n$ , with an arc  $q \rightarrow p$  whenever  $q$  divides  $p - 1$ . We can label each such arc with the positive integer  $r = r(q, p)$  such that  $q^r \parallel p - 1$ . In view of the preceding enumerative results, it is interesting to know which labelled directed graphs can occur in this context. A directed graph is said to be *acyclic* if it contains no directed cycles. An *isomorphism* of labelled directed graphs is an isomorphism of directed graphs such that each arc has the same label as its image.

PROPOSITION 13.1. *Let  $\Delta$  be a finite directed graph the arcs of which are labelled with positive integers. Then  $\Delta$  is isomorphic as a labelled directed graph to  $\Pi_n$  for some  $n$  if and only if  $\Delta$  is acyclic.*

*Proof.* Each  $\Pi_n$  is acyclic, since if it has an arc  $q \rightarrow p$ , then  $q < p$ ; hence any directed graph isomorphic to  $\Pi_n$  is also acyclic.

For the converse, we use induction on the number  $l$  of vertices of  $\Delta$ . For technical reasons, we will prove that if  $\Delta$  is acyclic, then  $\Delta \cong \Pi_n$  for some odd  $n$ . This result is trivial if  $l = 1$ , and

hence we may suppose that  $l > 1$  and the result has been proved for all labelled directed graphs with  $l - 1$  vertices. Being finite and acyclic,  $\Delta$  has a vertex  $v$  which is not the source of any arc (for instance, the last vertex in a maximal directed path). Let  $\Delta'$  be the labelled directed graph formed from  $\Delta$  by removing  $v$  and any incident arcs  $u \rightarrow v$ . Then  $\Delta'$  is acyclic, and hence the induction hypothesis implies that there is an isomorphism of labelled directed graphs  $\theta : \Delta' \rightarrow \Pi_{n'}$  for some odd integer  $n'$ . Each vertex  $w$  of  $\Delta'$  corresponds to a prime  $\theta(w) = q > 2$  dividing  $n'$ . We extend  $\theta$  to an isomorphism  $\Delta \rightarrow \Pi_n$  by taking  $n = n'p$ , where  $p$  is a suitably chosen odd prime, and defining  $\theta(v) = p$ . Such an extension is an isomorphism if and only if  $q^{r_q} \parallel p - 1$  for each prime  $q$  dividing  $n'$ , where  $r_q = r$  if there is an arc  $w \rightarrow v$  in  $\Delta$  labelled  $r$ , and  $r_q = 0$  if there is no arc  $w \rightarrow v$ . These conditions are all satisfied if  $p \equiv q^{r_q} + 1 \pmod{(q^{r_q+1})}$  for each  $q$ . The Chinese Remainder Theorem implies that this set of congruences is equivalent to a single congruence of the form  $p \equiv a \pmod{(b)}$ , where  $b$  is the product of the prime powers  $q^{r_q+1}$ . Since  $q^{r_q} + 1$  is coprime to  $q^{r_q+1}$  for each  $q$ , it follows that  $a$  and  $b$  are coprime, and thus Dirichlet's Theorem on primes in arithmetic progressions implies that there is at least one odd prime  $p$  satisfying this congruence (in fact, there are infinitely many).  $\square$

A similar argument shows that the directed graphs corresponding to even integers  $n$  are those that are acyclic and have a vertex  $u$  (corresponding to the prime 2) with an arc from  $u$  to every other vertex.

**COROLLARY 13.2.** *Every finite graph is isomorphic to the underlying graph of some directed graph  $\Pi_n$ .*

*Proof.* If we number the vertices of a finite graph  $v_1, v_2, \dots$ , and regard any edge  $v_i v_j$  as an arc  $v_i \rightarrow v_j$  where  $i < j$ , then we obtain an acyclic directed graph, and hence the result follows from Proposition 13.1.  $\square$

#### 14. Connections with the random graph

The arguments used in the preceding section can be adapted to establish a link between the directed graph  $\Pi$  and the *random graph* or *universal graph*  $R$  studied by Erdős and Rényi [11] and constructed by Rado [28]. This graph has many remarkable properties, described in some detail in [4, § 5.1; 7, § 9.6]. For instance, given a countably infinite vertex set, if pairs of vertices are chosen randomly to be edges, each with probability  $\frac{1}{2}$ , then the resulting graph is isomorphic to  $R$  with probability 1.

In  $\Pi$  there is an arc from the vertex 2 to every other vertex. If we delete this vertex and all such incident arcs, and ignore the direction of each remaining arc, we obtain an undirected graph  $\Pi'$  the vertices of which are the odd primes, with an edge between  $p$  and  $q$  if and only if  $q$  divides  $p - 1$  or vice versa.

**PROPOSITION 14.1.** *The undirected graph  $\Pi'$  is isomorphic to  $R$ .*

*Proof.* The graph  $R$  is characterised (up to isomorphism) among countable graphs by the property that, for each disjoint pair  $U$  and  $V$  of finite sets of vertices, there is a vertex adjacent to every vertex in  $U$  and to no vertex in  $V$ . The fact that  $\Pi'$  has this property follows immediately from the Chinese Remainder Theorem and Dirichlet's Theorem on primes in arithmetic progressions: the simultaneous congruences  $p \equiv 1 \pmod{(u)}$  for all  $u \in U$  and  $p \equiv -1 \pmod{(v)}$  for all  $v \in V$  are equivalent to a single congruence modulo  $\prod u \cdot \prod v$ , and this

is satisfied by at least one odd prime  $p$  (by infinitely many, in fact). Then  $p - 1$  is divisible by each  $u \in U$  and by no  $v \in V$ , and  $p$  cannot divide any  $v - 1$  (for otherwise  $v = p + 1$  would be even). Hence  $\Pi' \cong R$ .  $\square$

960 Since every countable graph is isomorphic to an induced subgraph of  $R$ , this result gives an alternative proof of Corollary 13.2.

*Acknowledgements.* The author is grateful to Roman Nedela and Martin Škoviera for their advice and their continued encouragement to undertake this research, and to Jürgen Wolfart and the Mathematics Faculty at the J. W. Goethe University, Frankfurt-am-Main, for providing  
965 the ideal environment in which it could be carried out.

### 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 Mathematical Society Lecture Note Series 33 (Cambridge University Press, Cambridge, 1979).
- 970 3. W. BURNSIDE, ‘Notes on the theory of groups of finite order’, *Proc. London Math. Soc.* 26 (1895) 191–214, 559.
4. P. J. CAMERON, *Permutation groups*, London Mathematical Society Student Texts Series 45 (Cambridge University Press, Cambridge, 1999).
5. A. COSTE, G. A. JONES, M. STREIT and J. WOLFART, ‘Generalised Fermat hypermaps and Galois orbits’,  
975 *Glasgow Math. J.* 51 (2009) 289–299.
6. H. S. M. COXETER and W. O. J. MOSER, *Generators and relations for discrete groups*, 3rd edn (Springer, Berlin, 1972).
7. J. D. DIXON and B. MORTIMER, *Permutation groups*, Graduate Texts in Mathematics 163 (Springer, New York, 1996).
- 980 8. S.-F. DU, G. A. JONES, J. H. KWAK, R. NEDELA and M. ŠKOVIERA, ‘Regular embeddings of  $K_{n,n}$  where  $n$  is a power of 2. I: Metacyclic case’, *European J. Combin.* 28 (2007) 1595–1609.
9. S.-F. DU, G. A. JONES, J. H. KWAK, R. NEDELA and M. ŠKOVIERA, ‘Regular embeddings of  $K_{n,n}$  where  $n$  is a power of 2. II: Non-metacyclic case’, *European J. Combin.*, to appear.
10. P. ERDŐS, ‘Some asymptotic formulas in number theory’, *J. Indian Math. Soc.* 12 (1948) 75–78.
- 985 11. P. ERDŐS and A. RÉNYI, ‘Asymmetric graphs’, *Acta Math. Hungar.* 14 (1963) 295–315.
12. A. GROTHENDIECK, ‘Esquisse d’un Programme’, *Geometric Galois Actions I. Around Grothendieck’s Esquisse d’un Programme* (eds P. Lochak and L. Schneps), London Mathematical Society Lecture Note Series 242 (Cambridge University Press, Cambridge, 1997) 5–84.
13. P. HALL, ‘A note on soluble groups’, *J. London Math. Soc.* 3 (1928) 98–105.
- 990 14. P. HALL, ‘A contribution to the theory of groups of prime power orders’, *Proc. London Math. Soc.* 36 (1933) 29–95.
15. O. HÖLDER, ‘Die Gruppen mit quadratfreier Ordnungszahl’, *Nachr. Königl. Gesell. Wiss. Göttingen, Math.-Phys. Kl.* 1895 (1895) 211–229.
16. B. HUPPERT, *Endliche Gruppen I* (Springer, Berlin, 1967).
- 995 17. N. ITÔ, ‘Über das produkt von zwei abelschen Gruppen’, *Math. Z.* 62 (1955) 400–401.
18. L. D. JAMES and G. A. JONES, ‘Regular orientable imbeddings of complete graphs’, *J. Combin. Theory Ser. B* 39 (1985) 353–367.
19. G. A. JONES, ‘Maps on surfaces and Galois groups’, *Math. Slovaca* 47 (1997) 1–33.
20. G. A. JONES, R. NEDELA and M. ŠKOVIERA, ‘Regular embeddings of  $K_{n,n}$  where  $n$  is an odd prime power’,  
1000 *European J. Combin.* 28 (2007) 1863–1875.
21. G. A. JONES, R. NEDELA and M. ŠKOVIERA, ‘Complete bipartite graphs with a unique regular embedding’, *J. Combin. Theory Ser. B* 98 (2008) 241–248.
22. G. A. JONES and D. SINGERMAN, ‘Belyi functions, hypermaps and Galois groups’, *Bull. London Math. Soc.* 28 (1996) 561–590.
- 1005 23. G. A. JONES, M. STREIT and J. WOLFART, ‘Galois action on families of generalised Fermat curves’, *J. Algebra* 307 (2007) 829–840.
24. J. H. KWAK and Y. S. KWON, ‘Regular orientable embeddings of complete bipartite graphs’, *J. Graph Theory* 50 (2005) 105–122.
25. J. H. KWAK and Y. S. KWON, ‘Classification of reflexible regular embeddings and self-Petrie dual regular embeddings of complete bipartite graphs’, *Discrete Math.* 308 (2008) 2156–2166.
- 1010 26. J. H. KWAK and Y. S. KWON, ‘Classification of nonorientable regular embeddings of complete bipartite graphs’, Preprint, 2010, arXiv:1001.2936v1.
27. R. NEDELA, M. ŠKOVIERA and A. ZLATOŠ, ‘Regular embeddings of complete bipartite graphs’, *Discrete Math.* 258 (2002) 379–381.

28. R. RADO, 'Universal graphs and universal functions', *Acta Arith.* 9 (1964) 331–340. 1015
29. J. S. ROSE, *A course in group theory* (Cambridge University Press, Cambridge, 1978).
30. H. WIELANDT, 'Über das Produkt von paarweise vertauschbaren nilpotenten Gruppen', *Math. Z.* 55 (1951) 1–7.
31. S. E. WILSON, 'Operators over regular maps', *Pacific J. Math.* 81 (1979) 559–568.

*Gareth A. Jones*  
*School of Mathematics*  
*University of Southampton*  
*Southampton*  
*SO17 1BJ*  
*United Kingdom*

1020

G.A.Jones@maths.soton.ac.uk