

## ORBITS OF BRAID GROUPS ON CACTI

GARETH A. JONES AND ALEXANDER ZVONKIN

**ABSTRACT.** One of the consequences of the classification of finite simple groups is the fact that non-rigid polynomials (those with more than two finite critical values), considered as branched coverings of the sphere, have exactly three exceptional monodromy groups (one in degree 7, one in degree 13 and one in degree 15). By exceptional here we mean primitive and not equal to  $S_n$  or  $A_n$ , where  $n$  is the degree. Motivated by the problem of the topological classification of polynomials, a problem that goes back to 19th century researchers, we discuss several techniques for investigating orbits of braid groups on “cacti” (ordered sets of monodromy permutations). Applying these techniques, we provide a complete topological classification for the three exceptional cases mentioned above.

2000 MATH. SUBJ. CLASS. Primary: 30C10; Secondary: 57M12, 05B25, 57M60, 20B15.

KEY WORDS AND PHRASES. Topological classification of polynomials, monodromy groups, Braid group actions.

### 1. PRELIMINARIES

**1.1. Introduction.** A polynomial  $p(z) \in \mathbb{C}[z]$  of degree  $\deg p = n$  may be regarded as an  $n$ -sheeted branched covering  $S^2 \rightarrow S^2$  of the Riemann sphere  $S^2 = \mathbb{C} \cup \{\infty\}$  by itself. If it has  $k$  finite critical values  $w_1, \dots, w_k \in \mathbb{C}$ , then a rotation of  $w = p(z)$  around  $w_i$  induces a permutation  $g_i$  of the  $n$  sheets  $z = p^{-1}(w)$ . These *monodromy permutations*  $g_1, \dots, g_k$  generate the monodromy group  $G$  of  $p$  (sometimes referred to as the monodromy group of  $p^{-1}$ ); this can be regarded as the subgroup of the symmetric group  $S_n$  consisting of the permutations of the sheets obtained by lifting closed paths in  $\mathbb{C} \setminus \{w_1, \dots, w_k\}$ . The product  $g_1 \cdots g_k$ , representing the branching of  $p$  at  $\infty$ , is an  $n$ -cycle, and by an appropriate labelling of the sheets with the integers mod  $(n)$  we may take this to be  $c = (0, 1, 2, \dots, n-1)$ . Certain properties of the permutation group  $G$  reflect those of the polynomial  $p$ : for instance, Ritt [Rit1] showed that  $G$  is imprimitive (preserves a nontrivial equivalence relation) if and only if  $p$  is a composition of polynomials of smaller degree; in this paper, we shall concentrate mainly on primitive monodromy groups.

---

Received April 10, 2001.

Second named author supported in part by the Project Alcophys and by the GDR Tresses.

The Riemann–Hurwitz formula states that an  $n$ -sheeted branched covering of  $S^2$  has genus

$$1 - n + \frac{B}{2},$$

where  $B$  is the total order of branching. In our case, each  $w_i$  contributes  $n - n_i$  to  $B$ , where  $n_i = |p^{-1}(w_i)|$  is the number of cycles of  $g_i$  (including any fixed-points), and the critical value  $\infty$  contributes  $n - 1$ ; so, by putting the genus equal to 0, we obtain the necessary *planarity condition*

$$\sum_{i=1}^k n_i = (k - 1)n + 1. \quad (1)$$

Conversely, if permutations  $g_1, \dots, g_k \in S_n$  satisfy (1), and  $g_1 \cdots g_k$  is an  $n$ -cycle, then the Riemann existence theorem (see for example [Völ, Section 4.2.3]) implies that there is a polynomial  $p$  of degree  $n$  with monodromy permutations  $g_i$  at its critical values  $w_i$ .

A *cactus* is an ordered  $k$ -tuple of elements  $g_1, \dots, g_k \in S_n$ , satisfying (1), such that  $g_1 \cdots g_k = c$ ; we shall denote it by  $C = [g_1, \dots, g_k]$ . Two cacti  $[g_1, \dots, g_k]$  and  $[h_1, \dots, h_k]$  are *isomorphic* if there is some  $f \in S_n$  such that  $h_i = g_i^f$  ( $:= f^{-1}g_i f$ ) for  $i = 1, \dots, k$ ; such an element  $f$  must satisfy  $c^f = (g_1 \cdots g_k)^f = g_1^f \cdots g_k^f = h_1 \cdots h_k = c$ , so it commutes with  $c$  and is therefore a power of  $c$ . The *unrooted cactus* corresponding to  $C$  is the class  $\mathcal{C} = [C]$  of cacti isomorphic to  $C$ . We define the *automorphism group*  $\text{Aut } C$  to be  $\{f \in S_n : C^f = C\}$ , a subgroup of  $\langle c \rangle$  of order  $n/|\mathcal{C}|$ . A cactus  $C$  is *symmetric* if  $|\text{Aut } C| > 1$ .

A *passport* is an ordered  $k$ -tuple  $\Pi = [\lambda^{(1)}, \dots, \lambda^{(k)}]$  of partitions  $\lambda^{(i)}$  of  $n$ . Each cactus  $[g_1, \dots, g_k]$  has a passport, in which  $\lambda^{(i)}$  corresponds to the cycle-structure of the permutation  $g_i$ ; isomorphic cacti have the same passport, so we can refer to the passport of an unrooted cactus. A passport  $\Pi$  is *valid* if it is the passport of some cactus; Thom [Tho] has shown that this happens if and only if  $\Pi$  satisfies the planarity condition (1), where  $n_i$  is the number of parts in  $\lambda^{(i)}$ .

The  $k$ -string braid group  $B_k$  of the euclidean plane is the fundamental group of the space of all unordered distinct  $k$ -tuples  $w_1, \dots, w_k$  in  $\mathbb{C}$ . This group has generators  $\sigma_1, \dots, \sigma_{k-1}$ , where  $\sigma_i$  has the effect of transposing  $w_i$  and  $w_{i+1}$ , while fixing the other  $k - 2$  points  $w_j$ ; the equations  $\sigma_i \sigma_j = \sigma_j \sigma_i$  where  $|i - j| > 1$  and  $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$  for  $i = 1, \dots, k - 2$  form a set of defining relations for  $B_k$  (see [Bir]). There is a natural action of this group on cacti, given by

$$\sigma_i : [g_1, \dots, g_{i-1}, g_i, g_{i+1}, g_{i+2}, \dots, g_k] \mapsto [g_1, \dots, g_{i-1}, g_{i+1}, g_i^{g_{i+1}}, g_{i+2}, \dots, g_k],$$

which induces an action of  $B_k$  on unrooted cacti. Since  $\sigma_i$  transposes the cycle-structures of  $g_i$  and  $g_{i+1}$ , and since the transpositions  $(i, i + 1)$  generate the symmetric group  $S_k$ , it follows that the passports of the cacti in an orbit of  $B_k$  represent all the possible permutations of a single passport  $\Pi$ .

Two polynomials  $p$  and  $q$  are *topologically equivalent* if  $q \circ h_1 = h_2 \circ p$  for some orientation-preserving self-homeomorphisms  $h_1$  and  $h_2$  of  $S^2$ . This is clearly an equivalence relation on  $\mathbb{C}[z]$ . The topological classification of polynomials, that is, the determination of the equivalence classes under this relation, is a major problem,

which can be traced back to the work of Clebsch [Cle], Hurwitz [Hur] and Lüroth [Lür] in the late 19th century. It has been solved in some special cases, for instance for polynomials of degree  $n \leq 11$  [Zvo], but the general problem remains open. A theorem of Zdravkovska [Zdr] asserts the following:

**Theorem 1.1.** *Two polynomials are topologically equivalent if and only if their unrooted cacti lie in the same orbit of  $B_k$ .*

In one direction, this result is in fact due to Hurwitz, while the converse depends on a theorem of Kneser [Kne] that the space of orientation-preserving self-homeomorphisms of the sphere is path-connected. It follows from Theorem 1.1 that the topological classification of polynomials is equivalent to the determination of the orbits of braid groups on unrooted cacti; this problem can be reduced to that of determining all the unrooted cacti with a given (unordered) passport, and then finding the orbits of the relevant braid group on this set. The latter problem is rather straightforward for  $k \leq 2$ , since  $B_1$  is the trivial group, while  $B_2$  is an infinite cyclic group with generator  $\sigma_1$  sending each cactus  $[g_1, g_2]$  to a cactus isomorphic to  $[g_2, g_1]$ ; in this paper we shall therefore concentrate mainly on the case  $k \geq 3$ .

Replacing the generators  $g_i$  and  $g_{i+1}$  with  $g_{i+1}$  and  $g_i^{g_{i+1}}$  preserves the monodromy group  $G$  of  $p$  (as a subgroup of  $S_n$ , not just as an abstract group), so the subgroup  $G$  is an invariant of each braid group orbit. In some cases, the splitting of cacti (with a given passport) into different orbits is explained by their having non-isomorphic monodromy groups, in others it is because their monodromy groups are isomorphic but distinct subgroups of  $S_n$ . However there are also cases where cacti in different orbits have the same monodromy group; indeed, one should expect this to happen rather frequently, since a randomly chosen set of permutations almost always generates either  $S_n$  or  $A_n$  [Dix], so ‘most’ polynomials of degree  $n$  have  $S_n$  or  $A_n$  as their monodromy group. (In fact, generic polynomials, meaning all except a subset of codimension 1, form a single equivalence class, with monodromy group  $G = S_n$  generated by  $k = n - 1$  transpositions  $g_i$ , see [Zdr, KZ].)

In this paper we shall show how to use methods from enumerative combinatorics, group theory and character theory to study the cacti with a given passport. In many cases, one can use computational techniques to split these cacti into braid group orbits. We shall give a number of examples of such splitting, and where possible we shall use monodromy groups to explain the different orbits. The principal motivation for our choice of examples is a theorem of Müller [Mül] (also found independently by Adrianov [Adr] in the case  $k = 2$ ) concerning primitive monodromy groups.

**1.2. Primitive monodromy groups.** Among the primitive permutation groups containing an  $n$ -cycle  $c$ , the simply transitive groups are easily described: theorems of Burnside [Bur, §252] and Schur [Sch] imply that the degree  $n$  is prime, another theorem of Burnside [Bur, §251] then implies that  $G$  is solvable, and finally it follows from work of Galois that  $G$  is a subgroup of the 1-dimensional affine group

$$\mathrm{AGL}_1(n) = \{z \mapsto az + b : a, b \in \mathbb{F}_n, a \neq 0\}$$

acting on the field  $\mathbb{F}_n$ . We therefore turn to the doubly transitive groups containing  $c$ : here a theorem of Ritt (see [Rit2] or [Hup, II, §3, Aufgabe 1]) implies that the only

solvable groups are  $\text{AGL}_1(n)$  where  $n$  is prime, and  $S_4$  acting naturally with degree  $n = 4$ , while Feit [Fei, Theorem 4.1] and Jones [Jon2] have used the classification of finite simple groups to determine the nonsolvable groups. Combining these results, we have the following:

**Theorem 1.2.** *A primitive permutation group  $G \leq S_n$  contains a regular  $n$ -cycle if and only if it satisfies one of the following conditions:*

- (a)  $G = A_n$  ( $n$  odd) or  $G = S_n$ , acting naturally;
- (b)  $C_n \leq G \leq \text{AGL}_1(n)$ , acting on  $\mathbb{F}_n$ , where  $n$  is prime;
- (c)  $\text{PGL}_d(q) \leq G \leq \text{P}\Gamma\text{L}_d(q)$ , acting on points or hyperplanes, with  $n = (q^d - 1)/(q - 1)$ ;
- (d)  $G = L_2(11) = \text{PSL}_2(11)$ , acting on the  $n = 11$  cosets of a subgroup  $A_5$ ;
- (e)  $G$  is a Mathieu group  $M_{11}$  or  $M_{23}$ , acting naturally with degree  $n = 11$  or  $23$ .

(This is essentially Feit's Theorem 4.1, except that in case (c) he simply refers to certain groups  $G$  satisfying  $\text{PSL}_d(q) \leq G \leq \text{P}\Gamma\text{L}_d(q)$ ; the above more precise statement of (c) is proved in [Jon2].)

In case (c), if  $d \geq 3$  then  $G$  has two transitive permutation representations of degree  $n$ , on the points and hyperplanes of the projective geometry  $\text{PG}_{d-1}(q)$ ; these two representations are equivalent under the outer automorphism of  $G$  induced by duality (the graph automorphism, in the terminology of groups of Lie type). There are also two representations in case (d), and in case (a) when  $G = S_6$ , transposed by  $\text{Aut}(G)$ ; in all other cases the representation of  $G$  is unique. In case (c) the cyclic regular subgroups are the Singer subgroups, except for  $G = \text{P}\Gamma\text{L}_2(8)$  which has one additional conjugacy class of such subgroups [Jon2].

If  $G$  is the monodromy group of a polynomial, then the planarity condition (1) imposes further restrictions on the generators  $g_i$  of  $G$ , and this allowed Müller [Mül] to prove the following:

**Theorem 1.3.** *Apart from  $A_n$  and  $S_n$ , the only primitive monodromy groups of polynomials with  $k \geq 3$  are the following (with their degrees  $n$  and passports  $\Pi$ ):*

- (A)  $G \cong L_3(2) = \text{PSL}_3(2) = \text{PGL}_3(2)$  with  $n = 7$  and  $\Pi = [2^2 1^3, 2^2 1^3, 2^2 1^3]$ ;
- (B)  $G \cong L_3(3) = \text{PSL}_3(3) = \text{PGL}_3(3)$  with  $n = 13$  and  $\Pi = [2^4 1^5, 2^4 1^5, 2^4 1^5]$ ;
- (C)  $G \cong L_4(2) = \text{PSL}_4(2) = \text{PGL}_4(2)$  with  $n = 15$  and  $\Pi = [2^6 1^3, 2^4 1^7, 2^4 1^7]$ .

All three of these groups are of type (c) in Theorem 1.2. Here  $L_3(2) (\cong L_2(7))$ ,  $L_3(3)$  and  $L_4(2) (\cong A_8)$  are simple groups of orders  $168 = 2^3 \cdot 3 \cdot 7$ ,  $5616 = 2^4 \cdot 3^3 \cdot 13$  and  $20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$ . For detailed information on these groups, see the *ATLAS of Finite Groups* [CCNPW]; in the notation used there, the generators  $g_i$  of  $L_3(2)$  and of  $L_3(3)$  lie in the conjugacy class  $2A$ , while the generators of  $L_4(2)$  lie in  $2B$ ,  $2A$  and  $2A$  respectively.

Let us denote the passports appearing in Theorem 1.3 by

$$\begin{aligned}\Pi_A &= [2^2 1^3, 2^2 1^3, 2^2 1^3], \\ \Pi_B &= [2^4 1^5, 2^4 1^5, 2^4 1^5], \\ \Pi_C &= [2^6 1^3, 2^4 1^7, 2^4 1^7].\end{aligned}$$

Our main goal in this paper is to provide detailed information on the classification of polynomials with these three passports. In doing this, we shall develop the ideas introduced in [EHZZ] by describing some general techniques for studying cacti, monodromy groups and braid group orbits. We shall illustrate these methods as we introduce them, firstly by applying them to the passport  $\Pi_A$ , and later by extending them to  $\Pi_B$  and  $\Pi_C$ .

**1.3. The Goulden–Jackson formula.** To state this formula, we first need some notation. Let  $\lambda$  be a partition of  $n$ , with  $m_j$  parts equal to  $j$  for each  $j = 1, \dots, n$ , so that  $\lambda$  has  $m = \sum_j m_j$  parts, and  $n = \sum_j jm_j$ ; then we define

$$N(\lambda) = \frac{1}{m} \binom{m}{m_1 m_2 \dots m_n} = \frac{(m-1)!}{m_1! m_2! \dots m_n!}.$$

The Goulden–Jackson formula [GJ] states that the number of cacti  $[g_1, \dots, g_k]$  of degree  $n$  with a valid passport  $\Pi = [\lambda^{(1)}, \dots, \lambda^{(k)}]$  is

$$n^{k-1} \prod_{i=1}^k N(\lambda^{(i)}).$$

Each cactus  $C$  lies in a class  $\mathcal{C} = [C]$  of size  $n/|\text{Aut } C|$ , so dividing by  $n$  we obtain the formula

$$\sum_{\mathcal{C}} \frac{1}{|\text{Aut } C|} = n^{k-2} \prod_{i=1}^k N(\lambda^{(i)}), \tag{2}$$

where the sum is over all unrooted cacti  $\mathcal{C}$  with passport  $\Pi$ . The number on the right-hand side of (2) is known as the *Goulden–Jackson number*  $N(\Pi)$  of  $\Pi$ ; if all cacti with passport  $\Pi$  are asymmetric (as is often the case), then this is the number of unrooted cacti with passport  $\Pi$ . In the symmetric case, Bóna, Bousquet, Labelle and Leroux [BBL] have provided a formula for the number of cacti with a given passport and order of symmetry.

**Example 1.4.** Let  $\Pi = \Pi_A = [2^2 1^3, 2^2 1^3, 2^2 1^3]$ , so that  $n = 7$  and the possible permutations  $g_i$  are the involutions in  $A_7$ . The Goulden–Jackson number is

$$N(\Pi_A) = 7 \cdot \left(\frac{4!}{2! 3!}\right)^3 = 56,$$

and all cacti with this passport are asymmetric since the degree  $n$  is prime, so we obtain 56 unrooted cacti. Since  $k = 3$  in this example, these cacti are permuted by the braid group  $B_3$ . Later we shall show that they split into four orbits, two of length 7 with monodromy group isomorphic to  $L_3(2)$ , and two of length 21 with monodromy group  $A_7$ .

## 2. FINDING BRAID GROUP ORBITS

**2.1. First example.** Given any cactus  $C = [g_1, \dots, g_k]$ , one can find the orbit  $\Omega$  of  $B_k$  containing  $C$  by starting with  $C$  and repeatedly applying the standard generators  $\sigma_1, \dots, \sigma_{k-1}$  of  $B_k$  until one has a set of cacti which is invariant under each  $\sigma_i$ . The same applies to orbits on unrooted cacti. This is a simple but tedious task, more suitable for computers than for human beings. In this way, one obtains

the permutation induced by each generator  $\sigma_i$  on  $\Omega$ , and from this it is often possible to identify the permutation group  $P$  induced by  $B_k$  on  $\Omega$  (possibly with the help of a system such as GAP).

For a given passport  $\Pi$ , one can repeat this process, starting with a new, unlisted cactus each time, until the number of cacti found is equal to that given by applying the Goulden–Jackson formula to  $\Pi$ . One then has the complete decomposition of these cacti into braid group orbits, together with the action of  $B_k$  on each orbit.

**Example 2.1.** Let  $\Pi = \Pi_A = [2^2 1^3, 2^2 1^3, 2^2 1^3]$ . Composing permutations from left to right (as we shall always do), we have

$$(0, 1)(2, 4) \cdot (0, 2)(5, 6) \cdot (0, 5)(3, 4) = (0, 1, 2, 3, 4, 5, 6),$$

so there is a cactus  $C_1 = [(0, 1)(2, 4), (0, 2)(5, 6), (0, 5)(3, 4)]$  with passport  $\Pi_A$ . If we apply the above process to  $C_1$  we eventually obtain an orbit  $\Omega_1$  of  $B_3$  consisting of seven unrooted cacti  $C_i = [C_i]$  ( $i = 1, \dots, 7$ ) where we can take

$$C_1 = [(0, 1)(2, 4), (0, 2)(5, 6), (0, 5)(3, 4)],$$

$$C_2 = [(0, 2)(5, 6), (0, 4)(1, 2), (0, 5)(3, 4)],$$

$$C_3 = [(0, 4)(1, 2), (1, 4)(5, 6), (0, 5)(3, 4)],$$

$$C_4 = [(1, 4)(5, 6), (0, 1)(2, 4), (0, 5)(3, 4)],$$

$$C_5 = [(0, 1)(2, 4), (0, 5)(3, 4), (0, 6)(2, 5)],$$

$$C_6 = [(0, 5)(3, 4), (1, 5)(2, 3), (0, 6)(2, 5)],$$

$$C_7 = [(1, 5)(2, 3), (0, 1)(2, 4), (0, 6)(2, 5)].$$

**2.2. Graphical representation of cacti.** A graphical representation of cacti was probably first used in [Zdr] (under the name of ‘pictures’), and later on in [GJ, EHZZ, BBLL] and in many other papers. In fact, this graphical image was the origin of the term ‘cactus’. Although very convenient for enumeration and for various other purposes, this representation is less convenient for computing braid group orbits. Here we use a *different* graphical representation, more convenient for this latter purpose, which has also been used by many authors and under different names (such as, e. g., ‘monodromy graphs’).

In Example 2.1, the cactus and its orbit are sufficiently small that it is feasible to find the orbit by hand. Since the permutations  $g_i$  all have order 2, we can represent each cactus  $C = [g_1, g_2, g_3]$  with passport  $\Pi_A$  as an undirected graph  $\Gamma$ : we place seven vertices, numbered 0, 1,  $\dots$ , 6, in cyclic order around a circle, and join vertices  $u$  and  $v$  by an unbroken, broken or dotted edge  $uv$  if  $(u, v)$  is a transposition in  $g_1, g_2$  or  $g_3$  respectively. For instance,  $C_1$  is represented by the graph shown in Figure 1.

The cacti isomorphic to  $C$  are those formed by rotating the graph  $\Gamma$ . The generator  $\sigma_1: [g_1, g_2, g_3] \mapsto [g_2, g_1^{g_2}, g_3]$  of  $B_3$  replaces each broken edge  $uv$  with an unbroken edge  $uv$ , and replaces each unbroken edge  $uv$  with a broken edge  $(uv)^{g_2}$ , obtained by applying  $g_2$  to  $u$  and  $v$ . Similarly,  $\sigma_2: [g_1, g_2, g_3] \mapsto [g_1, g_3, g_2^{g_3}]$  replaces each dotted edge  $uv$  with a broken edge  $uv$ , and replaces each broken edge  $uv$  with a dotted edge  $(uv)^{g_3}$ . In this way, the action of  $B_3$  on cacti is easily determined.

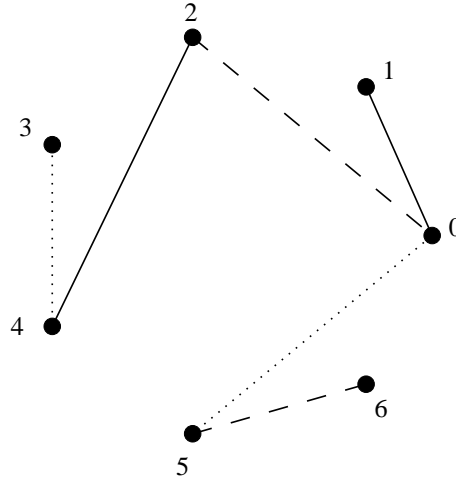


FIGURE 1. A graphical representation of a cactus

More generally, an arbitrary cactus  $C = [g_1, \dots, g_k]$  of degree  $n$  can be represented as a directed graph  $\Gamma$  on  $n$  vertices, with arcs  $uv$  assigned  $k$  colours corresponding to the actions  $g_i: u \mapsto v$  of the  $k$  permutations  $g_i$ . Thus  $\Gamma$  is simply a Schreier coset diagram for a point-stabilizer in the monodromy group  $G = \langle g_1, \dots, g_k \rangle$ , or equivalently for the subgroup  $p_*(\pi_1(p^{-1}(\mathbb{C} \setminus \{w_1, \dots, w_k\})))$  of the fundamental group  $\pi_1(\mathbb{C} \setminus \{w_1, \dots, w_k\})$  of the punctured plane, where  $p_*: \pi_1(p^{-1}(\mathbb{C} \setminus \{w_1, \dots, w_k\})) \rightarrow \pi_1(\mathbb{C} \setminus \{w_1, \dots, w_k\})$  is the inclusion induced by the covering  $p$ . The vertex-set of  $\Gamma$  can be identified with the fibre  $p^{-1}(w_0)$  above a base-point  $w_0 \in \mathbb{C} \setminus \{w_1, \dots, w_k\}$ , and the arcs are the lifts of mutually disjoint loops  $\gamma_i$  in  $\mathbb{C} \setminus \{w_1, \dots, w_k\}$ , one around each  $w_i$ , whose homotopy classes generate  $\pi_1(\mathbb{C} \setminus \{w_1, \dots, w_k\})$  and induce the permutations  $g_i$  of  $p^{-1}(w_0)$ . Being a lifting of the usual diagram of homotopy generators via a polynomial, the graph  $\Gamma$  is always planar. For visual simplicity it is often useful to omit loops, corresponding to fixed-points, and to replace mutually inverse pairs of arcs, corresponding to 2-cycles, with undirected edges, as in Figure 1. The effect of each generator  $\sigma_i$  of  $B_k$  on  $\Gamma$  is to transpose the colours of the arcs corresponding to  $g_i$  and  $g_{i+1}$ , while allowing  $g_{i+1}$  to act on those arcs corresponding to  $g_i$ .

**2.3. Continuation of Example 2.1.** Returning to Example 2.1, we find in this way (or by a computer calculation) that the generators of  $B_3$  act on the unrooted cacti  $[C_i]$  in the orbit  $\Omega_1$  by inducing the following permutations of their subscripts  $i$ :

$$\sigma_1 \mapsto (1, 2, 3, 4)(5, 6, 7), \quad \sigma_2 \mapsto (1, 5, 6, 2)(3, 4, 7).$$

The permutation group  $P$  induced by  $B_3$  on  $\Omega_1$  is transitive, and hence (since the degree 7 is prime)  $P$  is primitive; any primitive group containing a 3-cycle contains the alternating group [Wie, Theorem 13.3], and here  $\sigma_1^4$  induces a 3-cycle, so  $P \geq A_7$ ; since  $\sigma_1$  induces an odd permutation,  $P = S_7$ .

It is easy to see from its graph that the cactus

$$C'_1 = [(1, 3)(4, 5), (1, 6)(2, 3), (0, 1)(4, 6)]$$

is not isomorphic to one of those considered above, so a similar process, starting with  $C'_1$ , yields a second orbit  $\Omega_2$  consisting of seven unrooted cacti  $C'_i = [C'_i]$  where

$$\begin{aligned} C'_1 &= [(1, 3)(4, 5), (1, 6)(2, 3), (0, 1)(4, 6)], \\ C'_2 &= [(1, 6)(2, 3), (2, 6)(4, 5), (0, 1)(4, 6)], \\ C'_3 &= [(2, 6)(4, 5), (1, 2)(3, 6), (0, 1)(4, 6)], \\ C'_4 &= [(1, 2)(3, 6), (1, 3)(4, 5), (0, 1)(4, 6)], \\ C'_5 &= [(1, 3)(4, 5), (0, 1)(4, 6), (0, 4)(2, 3)], \\ C'_6 &= [(0, 1)(4, 6), (0, 3)(5, 6), (0, 4)(2, 3)], \\ C'_7 &= [(0, 3)(5, 6), (1, 3)(4, 5), (0, 4)(2, 3)]. \end{aligned}$$

Here  $\sigma_1$  and  $\sigma_2$  induce the same permutations of the subscripts as they do in  $\Omega_1$ , so  $B_3$  again acts as  $S_7$ . This suggests that there is a natural pairing between these two orbits, and we shall see later that this is indeed the case.

Continuing, we obtain two further orbits  $\Omega_3$  and  $\Omega_4$  of length 21, represented by cacti

$$D_1 = [(0, 6)(4, 5), (2, 6)(3, 4), (1, 2)(3, 6)]$$

and

$$E_1 = [(0, 6)(3, 4), (2, 6)(3, 5), (1, 2)(3, 6)].$$

With an appropriate numbering  $\mathcal{D}_1, \dots, \mathcal{D}_{21}$  of the unrooted cacti  $\mathcal{D}_i = [D_i] \in \Omega_3$ , one finds that the generators of  $B_3$  act as

$$\begin{aligned} \sigma_1 &\mapsto (1, 2, 3)(4, 16, 9, 6, 21, 19)(5, 13, 20, 12)(7, 10, 15)(8, 17, 14, 18, 11), \\ \sigma_2 &\mapsto (1, 4, 5, 6, 7)(2, 8, 9)(3, 10, 11, 12, 13, 14)(15, 16, 17)(18, 19, 20, 21). \end{aligned}$$

Similarly, with a suitable labelling of the unrooted cacti in  $\Omega_4$  as  $\mathcal{E}_a (= [E_1]), \dots, \mathcal{E}_u$ , the action on  $\Omega_4$  is

$$\begin{aligned} \sigma_1 &\mapsto (a, f, l)(m, p, e, h, d, u)(r, o, s, i, g)(b, q, k, t)(c, n, j), \\ \sigma_2 &\mapsto (a, b, c, d, e)(f, g, h, i, j, k)(l, m, n, o)(p, q, r)(s, t, u). \end{aligned}$$

It is easily seen that on each of  $\Omega_3$  and  $\Omega_4$ ,  $B_3$  induces a primitive group  $P \leq A_{21}$ ; since  $\sigma_1^{12}$  induces a 5-cycle, a theorem of Jordan [Wie, Theorem 13.9] implies that  $P = A_{21}$ . This fact, together with the equal cycle-structures of  $\sigma_i$  on  $\Omega_3$  and  $\Omega_4$ , suggests a natural pairing between these two orbits; however, we shall see later that this does not happen in this case.

Since  $7 + 7 + 21 + 21 = 56$ , we have now accounted for all the unrooted cacti with the passport  $\Pi_A$  (and therefore we may now affirm that there exist exactly four topological equivalence classes of polynomials with this passport). Later in this paper, we shall explain this splitting into orbits in terms of the monodromy groups of these cacti.



3. MORE ON BRAIDS AND PERMUTATION GROUPS

**3.1. The centre and automorphisms of the braid group.** In Example 2.1, if we take  $x = \sigma_1\sigma_2$  and  $y = \sigma_1\sigma_2\sigma_1$  as alternative generators of  $B_3$ , then the actions of  $B_3$  on  $\Omega_1$  and  $\Omega_2$  are given by

$$x \mapsto (1)(2, 4, 5)(3, 7, 6), \quad y \mapsto (1, 2)(3, 5)(4, 6)(7).$$

In the case of the longer orbits, we have

$$\begin{aligned} x &\mapsto (1, 8, 15)(2, 10, 16)(3, 4, 17)(5, 14, 19)(6, 18, 12)(7, 11, 9)(13, 21, 20), \\ y &\mapsto (1, 17)(2, 15)(3, 16)(4, 14)(5, 18)(6, 11)(7, 8)(9, 10)(12, 21)(13, 19)(20) \end{aligned}$$

on  $\Omega_3$  and

$$\begin{aligned} x &\mapsto (a, g, p)(b, r, l)(c, o, t)(d, s, j)(e, i, h)(f, m, q)(k, u, n), \\ y &\mapsto (a, r)(b, o)(c, s)(d, i)(e, g)(f, p)(h, j)(k, m)(l, q)(n, t) \end{aligned}$$

on  $\Omega_4$ . This shows that the element  $x^3 = y^2$ , which generates the centre  $Z(B_3)$  of  $B_3$ , is in the kernel of each of these actions of  $B_3$ , so we have induced actions of  $B_3/Z(B_3)$ , which is isomorphic to the modular group  $\text{PSL}_2(\mathbb{Z}) = \langle x, y : x^3 = y^2 = 1 \rangle$ .

This is, in fact, a general phenomenon. For any  $k$ , the centre  $Z(B_k)$  of  $B_k$  is an infinite cyclic group generated by the element  $z = (\sigma_1\sigma_2 \cdots \sigma_{k-1})^k$  [Bir]. We have:

**Theorem 3.1.** *The generator  $z$  of  $Z(B_k)$  acts on cacti  $[g_1, \dots, g_k]$  as conjugation by  $c$ , and acts trivially on unrooted cacti.*

*Proof.* The standard generators  $\sigma_1, \dots, \sigma_{k-1}$  of  $B_k$  act on cacti by

$$\sigma_i : [g_1, \dots, g_i, g_{i+1}, \dots, g_k] \mapsto [g_1, \dots, g_{i+1}, g_i^{g_i^{+1}}, \dots, g_k],$$

so

$$\begin{aligned} \sigma_1 \cdots \sigma_{k-1} : [g_1, g_2, \dots, g_{k-1}, g_k] &\mapsto [g_2, g_3, \dots, g_k, g_1^{g_2 \cdots g_k}] \\ &= [g_2, g_3, \dots, g_k, g_1^{g_1 g_2 \cdots g_k}] \\ &= [g_2, g_3, \dots, g_k, g_1^c], \end{aligned}$$

and hence

$$z = (\sigma_1 \cdots \sigma_{k-1})^k : [g_1, \dots, g_k] \mapsto [g_1^c, \dots, g_k^c].$$

Since  $[g_1, \dots, g_k]$  and  $[g_1^c, \dots, g_k^c]$  are isomorphic,  $z$  fixes every unrooted cactus.  $\square$

One can also give a simple visual proof of this result, based on the fact that the braid  $z$  corresponds to a rotation of the critical values of a polynomial through  $2\pi$ .

**Corollary 3.2.** *If  $\Omega$  is any orbit of  $B_k$  on unrooted cacti, then the cacti  $C$  such that  $[C] \in \Omega$  form an orbit of  $B_k$  on cacti.*

*Proof.* The cacti in a given unrooted cactus  $\mathcal{C}$  are all conjugates by  $c$  of a single cactus  $C$ , so they are equivalent to each other under powers of  $z$ . The result follows immediately.  $\square$

In the case  $k = 3$ , Theorem 3.1 implies that each orbit  $\Omega$  of  $B_3$  on unrooted cacti provides a transitive permutation representation of  $B_3/Z(B_3) \cong \text{PSL}_2(\mathbb{Z})$ . This action can therefore be described by an oriented trivalent map  $\mathcal{M} = \mathcal{M}(\Omega)$ , in which the darts (the “ends” of edges) correspond to the unrooted cacti in  $\Omega$ , while the vertices, edges and faces correspond to the cycles of  $x (= \sigma_1\sigma_2)$ ,  $y (= \sigma_1\sigma_2\sigma_1)$  and  $(xy)^{-1} = (\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1)^{-1}$  on  $\Omega$  (see [JS, Jon1] for connections between the modular group and maps; in the figures given below we write the label of a dart on the left side of this dart (if one moves along the edge away from the vertex): this rule ensures that the labels corresponding to a face are located inside the face). Then the actions of  $B_3$  on two orbits are equivalent if and only if the corresponding oriented maps are isomorphic.

**Example 3.3.** In Example 2.1, where  $\Pi = \Pi_A$ ,  $x$  and  $y$  act in the same way on  $\Omega_1$  and  $\Omega_2$ , giving equivalent actions of  $B_3$  (which we shall explain later) and isomorphic trivalent maps  $\mathcal{M}(\Omega_1) \cong \mathcal{M}(\Omega_2)$  (see Figure 2).

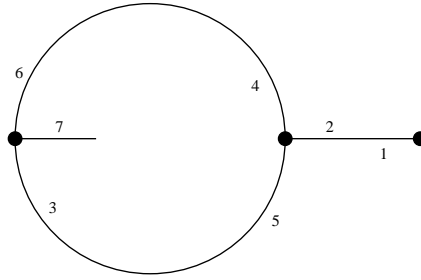


FIGURE 2. Trivalent map representing the orbits of size 7

However, this fails for the orbits  $\Omega_3$  and  $\Omega_4$ , despite their apparent similarity (same length, same cycle-structures for the generators of  $B_3$ ): for instance, in  $\Omega_3$  the unrooted cactus  $\mathcal{D}_{20}$  lies in cycles of  $\sigma_1$  and  $\sigma_2$  of length 4, whereas no cactus in  $\Omega_4$  has this property. Similarly by drawing the trivalent maps associated with these actions of  $x$  and  $y$  (see Figure 3) we see that  $\mathcal{M}(\Omega_3) \not\cong \mathcal{M}(\Omega_4)$ . For example, the ‘solitary’ dart 20 is adjacent to a face of degree 4, while the solitary dart  $h$  is adjacent to a face of degree 6. Moreover,  $\mathcal{M}(\Omega_3)$  is not isomorphic to the mirror image  $\overline{\mathcal{M}(\Omega_4)}$ , given by the actions of  $x^{-1}$  and  $y^{-1}$  on  $\Omega_4$ , so by the following result the actions of  $B_3$  on these two orbits are not equivalent under any automorphism of  $B_3$ . It therefore remains mysterious why  $B_3$  should have two orbits with such apparently similar properties.

**Theorem 3.4.** *The outer automorphism group  $\text{Out } B_3 = \text{Aut } B_3 / \text{Inn } B_3$  is a cyclic group of order 2, generated by  $\beta: \sigma_1 \mapsto \sigma_2^{-1}, \sigma_2 \mapsto \sigma_1^{-1}$  (which inverts  $x$  and  $y$ ), or equivalently by  $\gamma: \sigma_i \mapsto \sigma_i^{-1}$ .*

This is a special case of a theorem of Dyer and Grossman [DG], that  $\text{Out } B_k$  is cyclic of order 2, generated by  $\gamma: \sigma_i \mapsto \sigma_i^{-1}$ , for each  $k \geq 2$ . This is trivial for  $k = 2$ , and appears to have been ‘folk-lore’ for  $k = 3$ . We shall prove the latter case here for completeness.

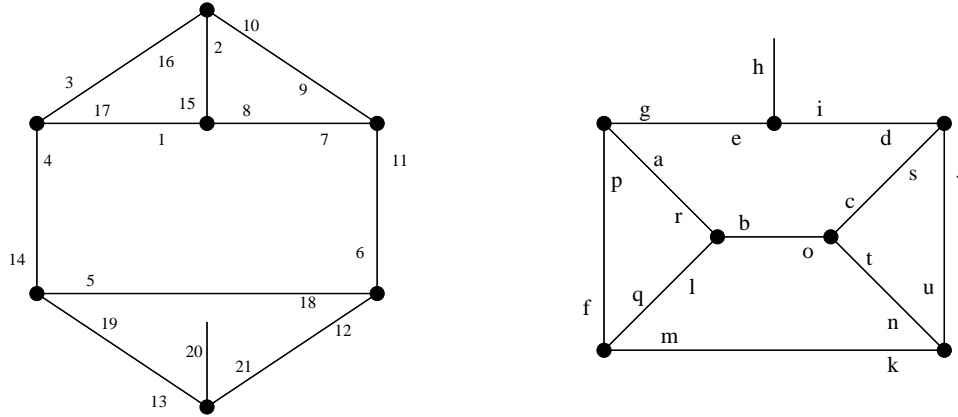


FIGURE 3. Trivalent maps representing the orbits of size 21

*Proof.* We have  $B_3 = \langle \sigma_1, \sigma_2 : \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle = \langle x, y : x^3 = y^2 \rangle$  where  $x = \sigma_1\sigma_2$  and  $y = \sigma_1\sigma_2\sigma_1$ , so  $\sigma_1 = x^{-1}y$  and  $\sigma_2 = yx^{-1}$ . Thus  $B_3$  is the free product of two infinite cyclic groups  $\langle x \rangle$  and  $\langle y \rangle$ , amalgamating the subgroups  $\langle x^3 \rangle$  and  $\langle y^2 \rangle$ . This common subgroup is the centre  $Z = \langle z \rangle$  of  $B_3$ , where  $z = x^3 = y^2$ , and the quotient  $B_3/Z$  is a free product  $C_3 * C_2$ .

Any  $\alpha \in \text{Aut } B_3$  leaves  $Z$  invariant, inducing an automorphism  $z \mapsto z^{\pm 1}$  of  $Z$ , so we have a homomorphism  $\text{Aut } B_3 \rightarrow \text{Aut } Z \cong C_2$ . This is an epimorphism, since  $\beta$  inverts  $x$  and  $y$  and hence inverts  $z$ , so  $\text{Aut } B_3$  has a subgroup  $\text{Aut}^+ B_3$  of index 2 fixing  $z$ . Clearly  $\text{Inn } B_3 \leq \text{Aut}^+ B_3$ .

To prove the reverse inclusion, let  $\alpha \in \text{Aut}^+ B_3$ . Then  $\alpha$  induces an automorphism  $\bar{\alpha}$  of the free product  $B_3/Z \cong C_3 * C_2$ . Now  $\text{Out}(C_3 * C_2) \cong C_2$ , generated by  $x \mapsto x^{-1}, y \mapsto y$ , so there is an element  $u \in B_3$  such that  $x\alpha = u^{-1}x^{\pm 1}uz^i$  and  $y\alpha = u^{-1}yuz^j$  for some  $i, j \in \mathbb{Z}$ . Then  $z = z\alpha = x^3\alpha = (x\alpha)^3 = (u^{-1}x^{\pm 1}uz^i)^3 = u^{-1}x^{\pm 3}uz^{3i} = z^{3i\pm 1}$ , so  $i = 0$  and  $x\alpha = u^{-1}xu$ . A similar calculation shows that  $j = 0$  and  $y\alpha = u^{-1}yu$ , so  $\alpha \in \text{Inn } B_3$ .

Hence  $\text{Inn } B_3 = \text{Aut}^+ B_3$ , so  $\text{Out } B_3 = \text{Aut } B_3 / \text{Aut}^+ B_3 \cong C_2$ , generated by  $\beta$ , or equivalently by  $\gamma$  since  $\beta\gamma$ , which transposes  $\sigma_1$  and  $\sigma_2$ , is conjugation by  $y^{-1}$ :  $\sigma_1 = x^{-1}y \mapsto yx^{-1} = \sigma_2, \sigma_2 = yx^{-1} \mapsto y^2x^{-1}y^{-1} = x^{-1}y = \sigma_1$ . This completes the proof.  $\square$

**3.2. The Frobenius character formula.** Whereas the Goulden–Jackson formula counts cacti (with a given passport) in  $S_n$ , the character formula, which is due to Frobenius, can be used to count cacti (again with a given passport) lying in any specific subgroup of  $S_n$ . This formula, proved in [Ser, Chapter 7], states that if  $K_1, \dots, K_k$  are conjugacy classes (not necessarily distinct) in some finite group  $G$ , then the number of solutions in  $G$  of the equation  $g_1 \cdots g_k = 1$ , with each  $g_i \in K_i$ , is

$$\frac{|K_1| \cdots |K_k|}{|G|} \sum_{\chi} \frac{\chi(g_1) \cdots \chi(g_k)}{\chi(1)^{k-2}},$$

where  $\chi$  ranges over the irreducible complex characters of  $G$ . Equivalently, if  $g$  is a fixed element of  $G$ , then the number of solutions of  $g_1 \cdots g_k = g$ , with each  $g_i \in K_i$ , is

$$\frac{|K_1| \cdots |K_k|}{|G|} \sum_{\chi} \frac{\chi(g_1) \cdots \chi(g_k) \overline{\chi(g)}}{\chi(1)^{k-1}}. \quad (3)$$

When counting cacti in a subgroup  $G \leq S_n$ , we can without loss of generality take  $g$  to be the standard  $n$ -cycle  $c$ , and we then take each  $K_i$  to be a conjugacy class in  $G$  of permutations with cycle-structure  $\lambda^{(i)}$ . If we are studying a particular braid group orbit, then we have to consider all possible orderings of the chosen classes  $K_i$ , since the effect of  $B_k$  is to permute them, inducing all possible permutations. Of course, formula (3) is invariant under such permutations, so we simply multiply it by the number of distinct orderings of  $K_1, \dots, K_k$ . If, on the other hand, we are interested in *all* the cacti in  $G$  with a given passport  $\Pi = [\lambda^{(1)}, \dots, \lambda^{(k)}]$ , then we apply the formula to every ordered  $k$ -tuple  $[K_1, \dots, K_k]$  of conjugacy classes in  $G$  with cycle-structures  $\lambda^{(1)}, \dots, \lambda^{(k)}$ , and add the results. (Note that the unordered set of conjugacy classes  $K_1, \dots, K_k$  is an obvious invariant of the braid group action.)

**Example 3.5.** If  $\Pi = \Pi_A$ , the permutations  $g_i$  are even involutions in  $S_7$ . We can therefore apply the character formula (3) to  $G = A_7$ , with  $K_1 = K_2 = K_3$  its unique conjugacy class  $2A$  of involutions (in ATLAS notation [CCNPW]); thus the choice of classes  $K_i$  is unique in this example, as is their ordering. We take  $g$  to be any fixed element from either of the mutually inverse classes  $7A$  or  $7B$  of elements of order 7, which we can assume to be  $c$ . We find (from the ATLAS) that the only irreducible characters of  $A_7$  not vanishing at either  $g_i \in 2A$  or at  $c$  are  $\chi_1, \chi_2, \chi_3, \chi_4$ , and  $\chi_7$ , with

$$\chi_1(1) = \chi_1(g_i) = \chi_1(c) = 1$$

and

$$\begin{aligned} \chi_2(1) &= 6, & \chi_2(g_i) &= 2, & \chi_2(c) &= -1, \\ \chi_3(1) &= 10, & \chi_3(g_i) &= -2, & \chi_3(c) &= (-1 + \sqrt{-7})/2, \\ \chi_4(1) &= 10, & \chi_4(g_i) &= -2, & \chi_4(c) &= (-1 - \sqrt{-7})/2, \\ \chi_7(1) &= 15, & \chi_7(g_i) &= -1, & \chi_7(c) &= 1. \end{aligned}$$

Since  $|A_7| = 7!/2$  and  $|2A| = 105$ , the character formula implies that the number of solutions in  $A_7$  of  $g_1 g_2 g_3 = c$ , with each  $g_i$  an involution, is

$$\frac{105^3}{\frac{1}{2} \cdot 7!} \left\{ 1 + \frac{2^3 \cdot (-1)}{6^2} + \frac{(-2)^3}{10^2} \left( \frac{-1 - \sqrt{-7}}{2} + \frac{-1 + \sqrt{-7}}{2} \right) + \frac{(-1)^3 \cdot 1}{15^2} \right\} = 392.$$

This is therefore the number of rooted cacti with passport  $\Pi$ , and dividing by  $n = 7$  we find that there are 56 unrooted cacti. This confirms our earlier result in Example 1.4, where the Goulden–Jackson formula showed that  $S_7$  contains 56 unrooted cacti with this passport.

We saw in Example 2.1 that these 56 cacti split into four orbits  $\Omega_1, \dots, \Omega_4$  under the action of  $B_3$ . In this example, as in many others, the splitting into orbits is explained (at least partially) by different orbits having different monodromy groups

$G = \langle g_1, \dots, g_k \rangle \leq S_n$ . To analyse this phenomenon, one needs to consider all the subgroups  $G \leq S_n$  which contain an  $n$ -cycle (such as  $c$ ) and which can be generated by permutations  $g_i$  with cycle-structures  $\lambda^{(i)}$  satisfying  $g_1 \cdots g_k = c$ . One way of doing this is to apply the character formula (3) to count solutions of this equation in every possible subgroup  $G$  containing  $c$ , and then use the inclusion-exclusion principle (or Möbius inversion within the lattice of subgroups) to find those  $G$  which are generated by such solutions.

**Example 3.6.** If  $\Pi = \Pi_A$ , then because the degree  $n = 7$  is prime, any subgroup  $G \leq S_7$  containing  $c$  must be primitive. It is easily seen from Theorem 1.2 that the only subgroups  $G \leq S_7$  which contain cacti with this passport are  $S_7$ ,  $A_7$  and subgroups  $G \cong L_3(2)$  ( $= PGL_3(2) = P\Gamma L_3(2)$ ). We have also seen that all 56 unrooted cacti lie in  $A_7$ , so we can ignore  $G = S_7$ . We now consider the case  $G \cong L_3(2)$ . The group  $L_3(2)$  has two inequivalent representations of degree  $n = 7$ , on the points and lines of the Fano plane  $\mathcal{F} = PG_2(2)$ , or equivalently on its two conjugacy classes of subgroups  $H \cong S_4$  (the stabilizers of points and lines). This gives rise to two conjugacy classes of subgroups  $G \cong L_3(2)$  in  $A_7$  (though they are conjugate in  $S_7$  since these two representations of  $L_3(2)$  differ only by an outer automorphism of  $L_3(2)$ , the point-line duality of  $\mathcal{F}$ ). If we apply the character formula (3) to a subgroup  $G \cong L_3(2)$  of  $S_7$ , we take  $K_1 = K_2 = K_3$  to be the unique class  $2A$  of 21 involutions in  $G$ . Using the character table for  $G$  in [CCNPW] we find that the number of solutions of  $g_1 g_2 g_3 = c$  with each  $g_i \in 2A$  is

$$\frac{21^3}{168} \left\{ 1 + \frac{(-1)^3}{3^2} \left( \frac{-1 - \sqrt{-7}}{2} + \frac{-1 + \sqrt{-7}}{2} \right) + \frac{2^3 \cdot (-1)}{6^2} \right\} = 49,$$

so there are 7 unrooted cacti in  $G$  with this passport. No proper subgroup of  $G$  contains elements of orders 2 and 7, so such a cactus must generate  $G$  and therefore has  $G$  as its monodromy group. Since monodromy groups are invariant under braid group actions, these 7 unrooted cacti form a union of orbits of  $B_3$ ; since the orbits have lengths 7, 7, 21 and 21, they form a single orbit of length 7. We shall show in Example 4.6 that the 7-cycle  $c$  lies in exactly two subgroups  $G \cong L_3(2)$ , one from each class in  $A_7$ , giving rise to the two braid group orbits  $\Omega_1$  and  $\Omega_2$  of length 7, so that the orbits  $\Omega_3$  and  $\Omega_4$  of length 21 both have monodromy group  $A_7$ . Before doing this, we need some general results on how a group (such as  $S_n$ ) permutes pairs of subgroups (such as monodromy groups  $G$  and cyclic regular subgroups  $C_n$ ) by conjugation; these are in turn deduced from even more general results about product actions.

#### 4. COUNTING MONODROMY GROUPS

**4.1. Counting lemma.** Suppose that  $\mathcal{G}$  is a conjugacy class of subgroups  $G \leq S_n$ , or equivalently an isomorphism class of finite permutation groups. Let  $\mathcal{C}$  denote the conjugacy class of cyclic regular subgroups  $C \cong C_n$  in  $S_n$ . Our aim is to enumerate the subgroups  $G \in \mathcal{G}$  containing a particular  $C \in \mathcal{C}$  (a global problem); we can do this by studying the subgroups  $C \in \mathcal{C}$  contained in a particular  $G \in \mathcal{G}$  (a local solution). The link between the global problem and the local solution is the action of  $S_n$  by conjugation on the set  $\mathcal{P}$  of pairs  $(G, C) \in \mathcal{G} \times \mathcal{C}$  such that  $G \geq C$ .

In particular, by double-counting  $\mathcal{P}$  we can find the number  $\nu$  of groups  $G \in \mathcal{G}$  containing a particular  $C \in \mathcal{C}$ . First we need a general result about groups acting on cartesian products; for background on permutation groups, see [DM].

**Lemma 4.1.** *Let  $S$  be a group acting transitively on sets  $\Gamma$  and  $\Delta$ , so there is a natural induced action of  $S$  on  $\Gamma \times \Delta$ , and let  $S_\alpha$  and  $S_\beta$  be the subgroups of  $S$  fixing elements  $\alpha \in \Gamma$  and  $\beta \in \Delta$ . Then there are bijections*

$$\phi: (\Gamma \times \Delta)/S \rightarrow \Gamma/S_\beta \quad \text{and} \quad \psi: (\Gamma \times \Delta)/S \rightarrow \Delta/S_\alpha$$

between orbit-spaces, given by

$$\phi: (\gamma, \delta)^S \mapsto (\gamma^s)^{S_\beta} \quad \text{and} \quad \psi: (\gamma, \delta)^S \mapsto (\delta^{s'})^{S_\alpha}$$

for all  $\gamma \in \Gamma$ ,  $\delta \in \Delta$ , where  $s, s' \in S$  satisfy  $\gamma^{s'} = \alpha$  and  $\delta^s = \beta$ . If  $\Gamma$  and  $\Delta$  are finite then  $\phi$  and  $\psi$  preserve proportional orbit-lengths, in the sense that

$$\frac{|\phi(\Omega)|}{|\Gamma|} = \frac{|\Omega|}{|\Gamma \times \Delta|} = \frac{|\psi(\Omega)|}{|\Delta|}$$

for each orbit  $\Omega$  of  $S$  on  $\Gamma \times \Delta$ .

*Proof.* To show that  $\phi$  is well defined, let  $(\gamma_1, \delta_1)^S = (\gamma_2, \delta_2)^S$ , so  $\gamma_2 = \gamma_1^t$  and  $\delta_2 = \delta_1^t$  for some  $t \in S$ ; if  $\delta_1^{s_1} = \beta = \delta_2^{s_2}$  then  $\gamma_2^{s_2} = \gamma_1^{ts_2} = (\gamma_1^{s_1})^{s_1^{-1}ts_2}$  with  $\beta^{s_1^{-1}ts_2} = \delta_1^{ts_2} = \delta_2^{s_2} = \beta$ , so  $(\gamma_1^{s_1})^{S_\beta} = (\gamma_2^{s_2})^{S_\beta}$ . To show that  $\phi$  is one-to-one, let  $(\gamma_1, \delta_1)^S$  and  $(\gamma_2, \delta_2)^S$  map to  $(\gamma_1^{s_1})^{S_\beta} = (\gamma_2^{s_2})^{S_\beta}$  where  $\delta_1^{s_1} = \beta = \delta_2^{s_2}$ ; then  $\gamma_2^{s_2} = (\gamma_1^{s_1})^t$  for some  $t \in S_\beta$ , so  $(\gamma_1, \delta_1)^{s_1ts_2^{-1}} = (\gamma_2, \delta_2)$  giving  $(\gamma_1, \delta_1)^S = (\gamma_2, \delta_2)^S$ . Since each orbit  $\gamma^{S_\beta}$  of  $S_\beta$  on  $\Gamma$  is the image of  $(\gamma, \beta)^S$ ,  $\phi$  is onto. To check that  $\phi$  preserves proportional orbit-lengths, note that

$$|(\gamma^s)^{S_\beta}| = |S_\beta : S_{\gamma^s, \beta}| = |S_\beta|/|S_{\gamma^s, \beta}| = |S_\beta|/|S_{\gamma, \delta}|$$

since  $(\gamma, \delta)^s = (\gamma^s, \beta)$ , so

$$\frac{|(\gamma^s)^{S_\beta}|}{|\Gamma|} = \frac{|S_\beta|}{|S_{\gamma, \delta}|} \cdot \frac{|S_\alpha|}{|S|} = \frac{|S|}{|S_{\gamma, \delta}|} \cdot \frac{|S_\alpha|}{|S|} \cdot \frac{|S_\beta|}{|S|} = \frac{|(\gamma, \delta)^S|}{|\Gamma| \cdot |\Delta|} = \frac{|(\gamma, \delta)^S|}{|\Gamma \times \Delta|}.$$

The symmetry between  $\Gamma$  and  $\Delta$  gives the corresponding results for  $\psi$ , thus completing the proof.  $\square$

In this Lemma, if we restrict  $\phi$  to some  $S$ -invariant subset (or relation)  $\Pi \subseteq \Gamma \times \Delta$ , then  $\phi(\Pi)$  is the set of the orbits of  $S_\beta$  on  $\Gamma$  consisting of those  $\gamma \in \Gamma$  such that  $(\gamma, \beta) \in \Pi$ , with a similar result for  $\psi$ . As before, these restrictions preserve proportional orbit-lengths.

In our applications, we shall generally by-pass  $\Gamma \times \Delta$ , and compose  $\phi$  with  $\psi^{-1}$  to obtain a bijection  $\Gamma/S_\beta \rightarrow \Delta/S_\alpha$ , again preserving proportional orbit-lengths and respecting any  $S$ -invariant relations.

We now take  $S$  to be a group acting by conjugation on conjugacy classes  $\Gamma = \mathcal{G}$  and  $\Delta = \mathcal{H}$  of subgroups  $G$  and  $H$  in  $S$ , with stabilizers  $\tilde{G} := S_G = N_S(G)$  (the normalizer of  $G$  in  $S$ ) and  $\tilde{H} := S_H = N_S(H)$ . The inclusion relation  $G \geq H$  on  $\mathcal{G} \times \mathcal{H}$  is invariant under  $S$ , so we can restrict the bijections and orbit-length equations in Lemma 4.1 to those orbits satisfying  $G \geq H$ . We deduce that for any fixed  $G \in \mathcal{G}$  and  $H \in \mathcal{H}$  there is a bijection between the set of orbits of  $\tilde{H}$  on

$\mathcal{G}_H := \{G \in \mathcal{G} : G \geq H\}$  and the set of orbits of  $\tilde{G}$  on  $\mathcal{H}_G := \{H \in \mathcal{H} : H \leq G\}$ . Both sets of orbits correspond bijectively to the set of orbits of  $S$  on  $\mathcal{P} = \{(G, H) \in \mathcal{G} \times \mathcal{H} : G \geq H\}$ , and these bijections all preserve proportional orbit-lengths.

If  $\mathcal{G}$  and  $\mathcal{H}$  are finite we can do some counting. Firstly, if  $G \in \mathcal{G}$  then  $|\mathcal{G}| = |S : \tilde{G}|$ . Now  $\tilde{G}$  acts by conjugation on  $\mathcal{H}_G = \{H \in \mathcal{H} : H \leq G\}$ . Suppose that  $\tilde{G}$  has  $t$  orbits  $\mathcal{H}_1, \dots, \mathcal{H}_t$  of lengths  $h_1, \dots, h_t$  on  $\mathcal{H}_G$ , with the groups  $H \in \mathcal{H}_i$  satisfying  $|N_{\tilde{G}}(H) : H| = m_i$  for each  $i$  (this is independent of the choices of  $G \in \mathcal{G}$  and of  $H \in \mathcal{H}_i$ ). Then  $h_i = |\tilde{G} : N_{\tilde{G}}(H)| = |\tilde{G} : H|/m_i$ , so

$$|\mathcal{H}_G| = \sum_{i=1}^t h_i = |\tilde{G} : H| \sum_{i=1}^t \frac{1}{m_i}$$

and hence

$$|\mathcal{P}| = |\mathcal{G}| \cdot |\mathcal{H}_G| = |S : \tilde{G}| \cdot |\tilde{G} : H| \sum_{i=1}^t \frac{1}{m_i} = |S : H| \sum_{i=1}^t \frac{1}{m_i}.$$

Secondly, if  $H \in \mathcal{H}$  then the stabilizer of  $H$  in  $S$  is its normalizer  $\tilde{H} = N_S(H)$ . Since each  $H \in \mathcal{H}$  is contained in the same number  $\nu := |\mathcal{G}_H|$  of groups  $G \in \mathcal{G}$ , we have

$$|\mathcal{P}| = |\mathcal{H}|\nu = |S : \tilde{H}|\nu.$$

Equating these two expressions for  $\mathcal{P}$  we obtain the following formula for  $\nu$ :

**Corollary 4.2.** *If  $\mathcal{G}$  and  $\mathcal{H}$  are finite conjugacy classes of subgroups of a group  $S$ , then the number  $\nu$  of groups  $G \in \mathcal{G}$  containing a particular  $H \in \mathcal{H}$  is given by*

$$\nu = |\tilde{H} : H| \sum_{i=1}^t \frac{1}{m_i};$$

here  $\tilde{H} = N_S(H)$ , and the subgroups  $H \in \mathcal{H}$  contained in  $G$  form  $t$  conjugacy classes under the action of  $\tilde{G} = N_S(G)$ , with the groups  $H$  in the  $i$ -th class satisfying  $|N_{\tilde{G}}(H) : H| = m_i$ .

Indeed, Lemma 4.1 implies that these  $\nu$  groups  $G \in \mathcal{G}_H$  form  $t$  orbits  $\mathcal{G}_1, \dots, \mathcal{G}_t$  of lengths  $|\tilde{H} : H|/m_i$  under the action of  $\tilde{H}$ . (Since  $H$  acts trivially on  $\mathcal{G}_H$ , we can regard this as an action of  $\tilde{H}/H$  on  $\mathcal{G}_H$ .) In particular, if all subgroups  $H \in \mathcal{H}_G$  are conjugate in  $\tilde{G}$ , then  $t = 1$  and  $\nu = |\tilde{H} : H|/m$  where  $m = m_1 = |N_{\tilde{G}}(H) : H|$ .

Now suppose that  $S$  is the symmetric group  $S_n$ ,  $\mathcal{H}$  is a conjugacy class of regular subgroups  $H$  of  $S_n$ , and  $\mathcal{G}$  is any conjugacy class of subgroups  $G \leq S_n$ . Then  $\tilde{H} = N_{S_n}(H)$  is the holomorph  $\text{Hol}(H)$ , a semidirect product of  $H$  by  $\text{Aut}(H)$ , so there are

$$\nu = \alpha \sum_{i=1}^t \frac{1}{m_i}$$

groups  $G \in \mathcal{G}$  containing  $H$ , where  $\alpha = |\text{Aut}(H)|$  and  $t$  and  $m_i$  are as in Corollary 4.2. These groups  $G$  form  $t$  orbits  $\mathcal{G}_1, \dots, \mathcal{G}_t$  of lengths  $\alpha/m_i$  under the action of  $\tilde{H}$ .

In particular, if we take  $\mathcal{H}$  to be the conjugacy class  $\mathcal{C}$  of cyclic regular subgroups  $C \cong C_n$  in  $S_n$ , then  $\text{Aut}(C) \cong U_n$ , the group of units mod  $(n)$ , and  $\alpha = \phi(n)$  (where  $\phi$  is Euler's function), so there are

$$\nu = \phi(n) \sum_{i=1}^t \frac{1}{m_i} \quad (4)$$

groups  $G \in \mathcal{G}$  containing each  $C$ , forming  $t$  orbits  $\mathcal{G}_i$  of length  $\phi(n)/m_i$  under  $\tilde{C}$ . Here  $t$  is the number of orbits of  $\tilde{G} = N_{S_n}(G)$  on the cyclic regular subgroups  $C \leq G$ , with the groups  $C$  in the  $i$ th orbit satisfying  $|N_{\tilde{C}}(C) : C| = m_i$ . There is an induced action of the abelian group  $\tilde{C}/C \cong U_n$  on  $\mathcal{G}_C$ , so for each orbit  $\mathcal{G}_i$  of  $\tilde{C}$  on  $\mathcal{G}_C$  all stabilizers of groups in  $\mathcal{G}_i$  are equal, and they coincide with the kernel  $K_i$  of  $\tilde{C}$  on  $\mathcal{G}_i$ . Thus, if  $G \in \mathcal{G}_i$  then  $K_i$  is the stabilizer  $N_{\tilde{C}}(G) = \tilde{C} \cap \tilde{G} = N_{\tilde{C}}(C)$  of  $G$  in  $\tilde{C}$ , so  $\tilde{C}$  acts on each orbit  $\mathcal{G}_i$  as the regular representation of the abelian group  $\tilde{C}/N_{\tilde{C}}(C)$  of order  $\phi(n)/m_i$ , which is a quotient of the group  $\tilde{C}/C \cong U_n$ .

**4.2. Examples of counting monodromy groups.** In Theorem 1.2 we listed the primitive groups  $G \leq S_n$  containing a cyclic regular subgroup. We shall now apply the results in Section 4.1 to them.

**Example 4.3.** In cases (a) and (b) of Theorem 1.2 we have  $G = S_n$  or  $A_n$ , or  $C_p \leq G \leq \text{AGL}_1(p)$ ; here it is fairly obvious that  $\nu = |\mathcal{G}_C| = 1$  for each conjugacy class  $\mathcal{G}$ , but nevertheless let us see how this follows from the preceding general results. If  $G = S_n$  or  $A_n$  we have  $\tilde{G} = S_n$ . All cyclic regular subgroups  $C$  are conjugate in  $S_n$ , so  $t = 1$ . We have  $m = m_1 = |N_{S_n}(C) : C| = \phi(n)$  and hence equation (4) gives  $\nu = \phi(n)/\phi(n) = 1$ . In the case  $C_p \leq G \leq \text{AGL}_1(p)$  there is one group  $G$ , of order  $pd$ , for each divisor  $d$  of  $p - 1$ . We have  $\tilde{G} = \text{AGL}_1(p)$ , so  $C = C_p$  is normal in  $\tilde{G}$ ; thus  $t = 1$ ,  $m = m_1 = |N_{\tilde{G}}(C) : C| = |\tilde{G} : C| = p - 1$ , and  $\nu = \phi(p)/(p - 1) = 1$ . The unique subgroup  $G \in \mathcal{G}_C$  is the unique subgroup of order  $pd$  in  $\tilde{C} = \text{AGL}_1(p)$ .

**Example 4.4.** In cases (d) and (e) of Theorem 1.2 we have  $G = \text{PSL}_2(11)$ ,  $M_{11}$  or  $M_{23}$ . The Mathieu groups  $M_{11}$  and  $M_{23}$  have no outer automorphisms, so they have normalizers  $\tilde{G} = G$ . Although  $G = \text{PSL}_2(11)$  has index 2 in  $\text{Aut}(G) = \text{PGL}_2(11)$ , its representation of degree 11 does not extend to  $\text{PGL}_2(11)$ , so in this case we also have  $\tilde{G} = G$ . In each of these three cases, the subgroups  $C \in \mathcal{C}_G$  are the Sylow  $p$ -subgroups of  $G$ , where  $p = n = 11$  or  $23$ , so they are all conjugate in  $G$  and hence  $t = 1$ . We have  $m = m_1 = |N_G(C) : C| = (p - 1)/2$ , so  $\nu = \phi(p)/m = 2$ , and the two groups  $G_1, G_2 \in \mathcal{G}_C$  form an orbit of length 2 under the action of  $\tilde{C} \cong \text{AGL}_1(p)$ . For each  $i$ ,  $N_{G_i}(C)$  is the unique subgroup  $\tilde{C} \cap A_p$  of order  $p(p - 1)/2$  in  $\tilde{C}$ ; when  $G = \text{PSL}_2(11)$  or  $M_{23}$  this is a maximal subgroup of  $G_i$ , so  $G_1 \cap G_2 = \tilde{C} \cap A_p$ . When  $G = M_{11}$  however,  $N_{G_i}(C)$  is not maximal in  $G_i$ : there is a unique subgroup  $H_i$  between it and  $G_i$ , namely a point-stabilizer  $H_i \cong \text{PSL}_2(11)$  in the representation of  $M_{11}$  of degree 12; as we have just seen,  $C$  is contained in exactly two subgroups of  $S_{11}$  isomorphic to  $\text{PSL}_2(11)$ , intersecting in  $\tilde{C} \cap A_{11}$ , so it follows that  $G_1 \cap G_2 = H_1 \cap H_2 = \tilde{C} \cap A_{11}$ .



**Example 4.5.** We now consider the most interesting case of Theorem 1.2, namely case (c), where  $\text{PGL}_d(q) \leq G \leq \text{P}\Gamma\text{L}_d(q)$  for some  $d \geq 2$ . For background on projective geometry, see [Hir, Tsu]. For notational convenience, we shall abbreviate  $\text{P}\Gamma\text{L}_d(q)$  to  $\text{P}\Gamma\text{L}$ , etc., whenever  $d$  and  $q$  are understood. If  $d > 2$  then the actions of  $\text{P}\Gamma\text{L}$  on the points and the hyperplanes of  $\text{PG}_{d-1}(q)$  are transposed by an outer automorphism of  $\text{P}\Gamma\text{L}$ ; in all cases we therefore have a single conjugacy class of subgroups isomorphic to  $\text{P}\Gamma\text{L}$  in  $S_n$ , and we can assume without loss of generality that the action is on points. We have  $\text{P}\Gamma\text{L}/\text{PGL} \cong \text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong C_e$  where  $q = p^e$  for some prime  $p$ , so there is one subgroup  $G = G_f$  satisfying  $\text{PGL} \leq G_f \leq \text{P}\Gamma\text{L}$  for each divisor  $f$  of  $e$ , with  $G_f/\text{PGL} \cong C_f$ . This means that there is one conjugacy class  $\mathcal{G} = \mathcal{G}_f$  of such subgroups  $G = G_f$  in  $S_n$  for each  $f$  dividing  $e$ . Each such  $G$  is normal in  $\text{P}\Gamma\text{L}$  (since  $\text{P}\Gamma\text{L}/\text{PGL}$  is abelian); indeed, since the normalizer  $\tilde{G} = N_{S_n}(G)$  of  $G$  also normalizes the subgroup  $\text{PSL} \leq G$ , and is therefore embedded in  $\text{Aut}(\text{PSL})$ , it follows that  $\tilde{G} = \text{Aut}(\text{PSL}) \cap S_n = \text{P}\Gamma\text{L}$ .

The Singer subgroups of  $\text{PGL}$  are cyclic regular subgroups  $C \leq G$ , induced by the multiplicative group  $\mathbb{F}_{q^d}^* \cong C_{q^d-1}$  of the field  $\mathbb{F}_{q^d} \supset \mathbb{F}_q$  acting linearly on  $\mathbb{F}_{q^d}$  (which is a  $d$ -dimensional vector space over  $\mathbb{F}_q$ ). These Singer subgroups are all conjugate in  $\text{PGL}$  (see [Hir]), and except the case  $G = \text{P}\Gamma\text{L}_2(8)$ , which we shall consider separately, they are the only cyclic regular subgroups of  $G$  (see [Jon2]). Thus, provided  $G \neq \text{P}\Gamma\text{L}_2(8)$  we have  $t = 1$ , and so the groups  $G \in \mathcal{G}_C$  are all conjugate under  $\tilde{C}$ . We have  $m = de$  since  $N_{\tilde{C}}(C)/C \cong \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_p) \cong C_{de}$  (generated by the Frobenius automorphism  $x \mapsto x^p$ ), so

$$\nu = \frac{\phi(n)}{de}. \tag{5}$$

The kernel  $K$  of this action of  $\tilde{C}$  is the stabilizer  $N_{\tilde{C}}(C)$  of  $G$ , so this action is the regular action of  $\tilde{C}/N_{\tilde{C}}(C) \cong U_n/\langle p \rangle$ , an abelian group of order  $\phi(n)/de$ .

(The subgroups  $G \in \mathcal{G}$  are in one-to-one correspondence with the different geometries, isomorphic to  $\text{PG}_{d-1}(q)$ , which can be imposed on an  $n$ -element set. There are

$$|\mathcal{G}| = |S_n : \text{P}\Gamma\text{L}| = n!(d, q-1)/e(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})$$

such geometries, and the  $\nu = \phi(n)/de$  groups  $G \in \mathcal{G}_C$  correspond to those geometries which are invariant under  $C$ .)

In the exceptional case  $G = \text{P}\Gamma\text{L}_2(8)$ , acting with degree  $n = 9$ , there is a second conjugacy class of cyclic regular subgroups  $C \leq G$ , in addition to the Singer subgroups: these extra subgroups are generated by elements of the class  $9D$  (in ATLAS notation), and are not contained in  $\text{PGL}_2(8) = \text{PSL}_2(8)$ , a simple subgroup of index 3 in  $G$ . In this case,  $\tilde{G} = G$  has  $t = 2$  orbits on the cyclic regular subgroups  $C \in \mathcal{C}_G$ . Both classes of subgroups  $C$  satisfy  $|N_{\tilde{G}}(C) : C| = 6$ , so

$$\nu = \phi(9) \left( \frac{1}{6} + \frac{1}{6} \right) = 2.$$

Thus, for each  $C \in \mathcal{C}$  there are two groups  $G_1, G_2 \in \mathcal{G}_C$ , with  $C$  a Singer subgroup of  $G_1$  and a non-Singer subgroup of  $G_2$ . Since  $\tilde{C}$  is contained in  $G_1$  and  $G_2$ , and

is maximal in  $G_1$  (it is a point-stabilizer in the doubly transitive representation of degree 28), we have  $G_1 \cap G_2 = \tilde{C}$ .

Note that the three groups  $G$  which appear in Theorem 1.3 as monodromy groups all satisfy  $\mathrm{PGL}_d(q) \leq G \leq \mathrm{P}\Gamma\mathrm{L}_d(q)$  for certain  $d$  and  $q$ , and they are not isomorphic to  $\mathrm{P}\Gamma\mathrm{L}_2(8)$ , so in each case equation (5) shows that there are  $\nu = \phi(n)/de$  groups  $G_i \cong G$  containing each cyclic regular subgroup  $C$ ; in particular, this applies to  $C = \langle c \rangle$ . We shall consider Case A of Theorem 1.3 here, and return to Cases B and C later.

**Example 4.6.** In Case A we have  $G = \mathrm{P}\Gamma\mathrm{L}_3(2) = \mathrm{PGL}_3(2) = \mathrm{L}_3(2)$  with  $n = 7$ . Here  $d = 3$  and  $e = 1$ , so  $\nu = \phi(7)/(3 \cdot 1) = 2$ , giving two groups  $G_1, G_2 \cong G$  containing each  $C$ . They are transposed by  $\tilde{C} = \mathrm{AGL}_1(7)$ , and the kernel  $K$  of this action of  $\tilde{C}$  is the unique subgroup  $\tilde{C} \cap \mathrm{A}_7$  of order  $7 \cdot 3 = 21$  in  $\tilde{C}$ . We have  $N_{G_i}(C) = K$  for each  $i$ , and  $G_1 \cap G_2 = K$  since  $K$  is a maximal subgroup of each  $G_i$ .

## 5. BACK TO BRAID GROUP ORBITS

**5.1. The geometry of Case A.** We now examine the geometric structures underlying Case A in more detail. We can find the two groups  $G_i \geq C$  explicitly by numbering the points and lines of the Fano plane  $\mathcal{F}$ . If we identify the set of points with  $\mathbb{Z}_7$ , we can take the set  $\mathcal{L}$  of lines to consist of the sets  $L_i = \{i+3, i+5, i+6\}$  where  $i \in \mathbb{Z}_7$ , the translates of the set  $L_0 = \{3, 5, 6\}$  of quadratic non-residues mod (7). It is straightforward to check that every two points lie in a unique line, and every two lines meet in a unique point, so we have a projective plane; in combinatorial language,  $L_0$  is a *difference set* in the abelian group  $\mathbb{Z}_7$  [LW, Chapter 27], [Sin], that is, the six differences of the elements  $L_0$  give each non-zero element of  $\mathbb{Z}_7$  the same number of times (exactly once in this case). The permutations of  $\mathbb{Z}_7$  which preserve  $\mathcal{L}$  form the automorphism group  $G = \mathrm{Aut} \mathcal{F} \cong \mathrm{L}_3(2)$ , which we can define to be  $G_1$ . Each automorphism  $g \in G$  permutes the set  $\mathcal{L}$  of lines, inducing a permutation  $g'$  of their subscripts  $i$ , and these permutations form a subgroup  $G'$  of  $\mathrm{S}_7$  isomorphic to  $G$ . For example, the permutations  $c = (0, 1, \dots, 6): i \mapsto i+1$  and  $b = (1, 2, 4)(3, 6, 5): i \mapsto 2i$  preserve  $\mathcal{L}$ , sending  $L_i$  to  $L_{i+1}$  and  $L_{2i}$  respectively, so they are automorphisms and satisfy  $b = b'$  and  $c = c'$ ; thus  $G \cap G'$  contains  $K = \langle b, c \rangle$ , a non-Abelian group of order 21, and the  $K$ -invariant bijection  $i \mapsto L_i$  is an isomorphism between the actions of  $K$  on points and lines. However,  $G \neq G'$ , since this bijection is not  $G$ -invariant: for example, the automorphism  $g = (1, 2)(3, 5)$  (acting on the points) induces the permutation  $g' = (2, 4)(5, 6)$  of the lines, so  $g' \in G'$ ; the permutation  $(2, 4)(5, 6)$  (of the points!) sends the line  $L_6 = \{2, 4, 5\}$  to the triple  $\{2, 4, 6\}$ , which is not a line, so  $g' \notin G$ . Indeed, since  $K$  is a maximal subgroup of  $G$  and  $G'$  we have  $G \cap G' = K$ . We therefore take the second subgroup  $G_2$  to be the group  $G'$ . As we saw in Example 3.6, the character formula shows that each of  $G_1$  and  $G_2$  is the monodromy group generated by a  $\mathrm{B}_3$ -orbit of 7 unrooted cacti  $C$  with passport  $\Pi$ .

As an example of a cactus in  $G_1$  with passport  $\Pi$ , let  $C_1 = [g_1, g_2, g_3]$  where

$$g_1 = (0, 1)(2, 4), \quad g_2 = (0, 2)(5, 6), \quad g_3 = (0, 5)(3, 4),$$

so that  $g_1g_2g_3 = (0, 1, 2, 3, 4, 5, 6) = c$  (see Example 2.1). It is straightforward to check that each  $g_i$  preserves  $\mathcal{L}$ , so that  $g_i \in \text{Aut } \mathcal{F} = G_1$ . In fact, these elements induce the permutations

$$g'_1 = (1, 3)(4, 5), \quad g'_2 = (1, 6)(2, 3), \quad g'_3 = (0, 1)(4, 6)$$

of the lines  $L_i$ . By assigning the following projective coordinates to the points,

$$\begin{aligned} 0 &= (0 : 1 : 1), & 1 &= (1 : 0 : 0), & 2 &= (0 : 1 : 0), & 3 &= (0 : 0 : 1), \\ 4 &= (1 : 0 : 1), & 5 &= (1 : 1 : 1), & 6 &= (1 : 1 : 0), \end{aligned}$$

we can represent  $g_1, g_2, g_3$  and  $c$  as the matrices

$$\begin{pmatrix} & 1 & 1 \\ 1 & & \\ & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \quad \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}.$$

(The matrices must act *on the right* on the ‘row-vectors’ if we want them to be multiplied in the same order as the corresponding permutations.) By the argument in Example 3.6,  $\langle g_1, g_2, g_3 \rangle = G_1$ , so  $C_1$  has monodromy group  $G_1$ . The remaining cacti isomorphic to  $C_1$  are obtained from  $C_1$  by cyclically permuting the symbols  $0, \dots, 6$  in the permutations  $g_i$ ; these seven cacti form an unrooted cactus  $\mathcal{C}_1 = [C_1]$ . The other unrooted cacti  $\mathcal{C}_2, \dots, \mathcal{C}_7$  in the orbit  $\Omega_1$ , given in Example 2.1, are found by applying the generators  $\sigma_1$  and  $\sigma_2$  of  $B_3$  to  $\mathcal{C}_1$ .

If  $C = [g_1, g_2, g_3]$  is any cactus with monodromy group  $G_1$ , then the even involutions  $g_1, g_2, g_3$  generate  $G_1$  and satisfy  $g_1g_2g_3 = c$ ; the corresponding permutations  $g'_1, g'_2, g'_3$  (of the lines) are even involutions which generate  $G'_1 = G_2$  and satisfy  $g'_1g'_2g'_3 = c' = c$ , so we have a second cactus  $C'$  with monodromy group  $G_2$ ; we shall call this the *geometric dual* of  $C$ . Since  $G_1 \neq G_2$ , the cacti  $C$  and  $C'$  must lie in different orbits of  $B_3$ . In fact, the cacti  $C_1, \dots, C_7$  listed earlier, which give rise to the orbit  $\Omega_1$ , have as their geometric duals the cacti  $C'_1, \dots, C'_7$  which give the orbit  $\Omega_2$  in Example 2.1.

The relationship between these two orbits is completely symmetric. If we start again by regarding the lines  $L_i$ , permuted by  $G_2$ , as new points, three of them forming a new line if they have an element of  $\mathbb{Z}_7$  in common, we obtain a new Fano geometry  $\mathcal{F}'$  in which the lines  $L'_i$  are the translates  $L'_0 + i$  of the set  $L'_0 = \{L_1, L_2, L_4\}$  of lines of  $\mathcal{F}$  containing 0. Thus  $\mathcal{F}'$  is defined by the quadratic residues 1, 2, 4 in  $\mathbb{Z}_7$ , just as  $\mathcal{F}$  is defined by the non-residues. (This duality may also be regarded as the multiplication by  $-1$ .) The automorphism group of  $\mathcal{F}'$  is  $G_2$ , and the permutation group induced by its action on the lines  $L'_i$  is  $G'_2 = G_1$ .

Geometric duality  $C \mapsto C'$  of cacti commutes with the action of  $B_3$ , since  $B_3$  acts initially on triples of elements of  $L_3(2)$ , which are then represented in two ways as triples  $[g_1, g_2, g_3]$  and  $[g'_1, g'_2, g'_3]$  in  $G$  and  $G'$  through their actions on points and lines of  $\mathcal{F}$ . This duality also commutes with the action of  $c$ , so it induces a duality  $[C] \mapsto [C]' = [C']$  of unrooted cacti.

**5.2. Algebraic duality of cacti.** We shall now describe a second type of duality of cacti. If  $C = [g_1, \dots, g_k]$  is any cactus, of any degree  $n$  and with any valid passport  $\Pi = [\lambda^{(1)}, \dots, \lambda^{(k)}]$ , then we can form another cactus  $\overline{C}$ , the *algebraic*

dual of  $C$ , as follows. Inverting the equation  $g_1 \cdots g_k = c$  gives  $g_k^{-1} \cdots g_1^{-1} = c^{-1}$ . Now  $c^{-1}$  is an  $n$ -cycle, so  $(c^{-1})^t = c$  for some  $t \in S_n$ . Then

$$(g_k^{-1})^t \cdots (g_1^{-1})^t = c,$$

so  $[(g_k^{-1})^t, \dots, (g_1^{-1})^t]$  is a cactus  $\overline{C}$  with passport  $\overline{\Pi} = [\lambda^{(k)}, \dots, \lambda^{(1)}]$ , the reverse of  $\Pi$ . Although this cactus depends on  $t$ , two choices of  $t$  differ by an element of the centralizer  $C_{S_n}(c) = \langle c \rangle$  of  $c$  in  $S_n$ , so the unrooted cactus  $\overline{C} = [\overline{C}]$  corresponding to  $\overline{C}$  is independent of the choice of  $t$ ; similarly, it is independent of the choice of  $C \in \mathcal{C} = [C]$ , so we obtain a duality  $\mathcal{C} \mapsto \overline{\mathcal{C}}$  of unrooted cacti. As the notation is intended to suggest, if  $\mathcal{C}$  corresponds to a topological equivalence class of polynomials  $p(z) = a_n z^n + \cdots + a_0$ , then  $\overline{\mathcal{C}}$  corresponds to the complex conjugate polynomials  $\overline{p}(z) = \overline{a}_n z^n + \cdots + \overline{a}_0$ . In particular, if one of the polynomials in the class has real coefficients then  $\mathcal{C} = \overline{\mathcal{C}}$ .

The actions of  $B_k$  on unrooted cacti  $\mathcal{C}$  and  $\overline{\mathcal{C}}$  differ by the automorphism  $\beta: \sigma_i \mapsto \sigma_{k-i}^{-1}$  of  $B_k$ , that is,  $\overline{\mathcal{C}}^\sigma = (\overline{\mathcal{C}})^{\sigma^\beta}$  for all  $\mathcal{C}$  and all  $\sigma \in B_k$ . To verify this, it is sufficient to note that  $\beta$  is an automorphism of  $B_k$  (since it sends the defining relations  $\sigma_i \sigma_j = \sigma_j \sigma_i$  and  $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$  to equivalent relations), and that  $\overline{\mathcal{C}}^{\sigma_i} = (\overline{\mathcal{C}})^{\sigma_i^\beta}$  for all  $\mathcal{C}$  and all generators  $\sigma_i$ . This implies that if  $\Omega$  is any orbit of  $B_k$  on unrooted cacti, then  $\overline{\Omega} = \{\overline{\mathcal{C}}: \mathcal{C} \in \Omega\}$  is also an orbit of  $B_k$ . By Corollary 3.2, this induces a duality between orbits of  $B_k$  on cacti  $\mathcal{C}$ , even though there is no canonically-defined duality of individual cacti  $C$ . We call this *algebraic* duality to distinguish it from the *geometric* duality which occurs only when the monodromy group preserves some geometry (or, more generally, some symmetric block design).

**Example 5.1.** If  $\Pi = \Pi_A$  we find that  $\overline{\Omega}_1 = \Omega_2$ , with  $\overline{\mathcal{C}}_1 = \mathcal{C}'_1$ ,  $\overline{\mathcal{C}}_2 = \mathcal{C}'_2$ ,  $\overline{\mathcal{C}}_3 = \mathcal{C}'_6$ ,  $\overline{\mathcal{C}}_4 = \mathcal{C}'_5$ ,  $\overline{\mathcal{C}}_5 = \mathcal{C}'_4$ ,  $\overline{\mathcal{C}}_6 = \mathcal{C}'_3$ ,  $\overline{\mathcal{C}}_7 = \mathcal{C}'_7$ . Applying  $\beta$ , we find that  $\sigma_1$  and  $\sigma_2$  permute the unrooted cacti  $\overline{\mathcal{C}}_i \in \Omega_2$  in the same way as  $\sigma_2^{-1}$  and  $\sigma_1^{-1}$  permute the unrooted cacti  $\mathcal{C}_i \in \Omega_1$ , that is, they act on subscripts by

$$\sigma_1 \mapsto (1, 2, 6, 5)(3, 7, 4), \quad \sigma_2 \mapsto (1, 4, 3, 2)(5, 7, 6),$$

so that

$$x \mapsto (1)(2, 5, 4)(3, 6, 7), \quad y \mapsto (1, 2)(3, 5)(4, 6)(7)$$

(the corresponding trivalent map is isomorphic to that of Figure 2). However, there is no such duality between  $\Omega_3$  and  $\Omega_4$ : these two orbits are algebraically self-dual, that is,  $\overline{\Omega}_i = \Omega_i$  for  $i = 3, 4$ , and similarly there is no underlying geometry with which to define a geometric duality between these two orbits.

Having used Case A of Theorem 1.3 to illustrate our techniques, we shall now apply them to Case B, and later to Case C.

**5.3. Case B of Theorem 1.3.** Let  $\Pi = \Pi_B = [2^4 1^5, 2^4 1^5, 2^4 1^5]$ , with  $n = 13$ . The Goulden–Jackson number is

$$N(\Pi_B) = 13 \cdot \left( \frac{8!}{4! 5!} \right)^3 = 35672.$$

Since 13 is prime, there are no symmetric cacti with this passport, so this is the number of unrooted cacti. By computer, we find a single orbit of  $B_3$  of length 35620, consisting of cacti with monodromy group  $A_{13}$ : a randomly-chosen cactus

with passport  $\Pi$  almost certainly lies in this orbit, and the other cacti in the orbit are then found by repeatedly applying  $\sigma_1$  and  $\sigma_2$ . The remaining 52 unrooted cacti with this passport are harder to find by random choice; instead, we shall use the methods developed earlier to show that they form four orbits of length 13, all with monodromy group isomorphic to  $L_3(3)$ . Thus, there are five topological equivalence classes of polynomials with this passport.

If we apply equation (5) to the group  $G = \text{PFL}_3(3) = \text{PGL}_3(3) = L_3(3)$  with  $n = 13$ , we find that there are  $\nu = \phi(13)/(3 \cdot 1) = 4$  groups  $G_1, \dots, G_4 \cong G$  containing  $C$ , permuted transitively by  $\tilde{C} = \text{AGL}_1(13)$ . The kernel  $K$  of this action is the unique subgroup of order  $13 \cdot 3 = 39$  in  $\tilde{C}$ , and  $\tilde{C}$  acts as  $\tilde{C}/K \cong C_4$  on these four groups. We have  $N_{G_i}(C) = K$  for each  $i$ , and  $G_i \cap G_j = K$  for each pair  $i \neq j$  since  $K$  is maximal in  $G_i$ .

The simple group  $G = L_3(3)$  of order  $5616 = 2^4 \cdot 3^3 \cdot 13$  has one conjugacy class of  $3^2 \cdot 13$  involutions, and four classes each of  $2^4 \cdot 3^3$  elements of order 13. If  $g$  is an element of order 13, then two powers of  $g$  are conjugate in  $G$  if and only if they are conjugate in  $N_G(\langle g \rangle)$ , a subgroup of order  $3 \cdot 13$  and of index 4 in  $N_{S_{13}}(\langle g \rangle) \cong \text{AGL}_1(13)$ ; a generator of  $N_G(\langle g \rangle)/\langle g \rangle$  acts on  $\langle g \rangle$  as  $g \mapsto g^3$ , so these four conjugacy classes meet  $\langle g \rangle$  in the subsets  $\{g, g^3, g^9\}$ ,  $\{g^2, g^5, g^6\}$ ,  $\{g^4, g^{10}, g^{12}\}$ , and  $\{g^7, g^8, g^{11}\}$ . In  $\text{Aut } G$ , a group of order  $2|G|$  consisting of  $G$  extended by the point-line duality, the first and third classes fuse together, as do the second and fourth.

Of the irreducible characters of  $G$ , only  $\chi_1$ ,  $\chi_2$ , and  $\chi_{11}$  (in ATLAS notation) are nonzero on elements of order 2 and 13, so the number of solutions in  $G$  of  $g_1 g_2 g_3 = g$ , where  $g_1, g_2$  and  $g_3$  are involutions and  $g$  is a fixed element of order 13, is

$$\frac{(3^2 \cdot 13)^3}{2^4 \cdot 3^3 \cdot 13} \left\{ 1 + \frac{4^3 \cdot (-1)}{12^2} + \frac{3^3 \cdot 1}{27^2} \right\} = 13^2.$$

No such solution can commute with  $g$ , since  $C_G(\langle g \rangle) = \langle g \rangle$ , so when  $g = c$  these solutions correspond to 13 unrooted cacti. Each solution generates  $G$  since no maximal subgroup of  $G$  has order divisible by 2 and 13 (see [CCNPW]), so each group  $G_i$  gives rise to 13 unrooted cacti with monodromy group  $G_i \cong L_3(3)$ .

Each of the four subgroups  $G \cong L_3(3)$  containing  $c$  is the automorphism group  $\text{Aut } \mathcal{P} \cong \text{PGL}_3(3) = L_3(3)$  of a projective plane  $\mathcal{P}$  with point-set  $\mathbb{Z}_{13}$  on which  $c : i \mapsto i + 1$  acts as a Singer cycle (an automorphism consisting of a single cycle [Sin]). These four geometries can be defined by taking the lines to be the translates under  $\langle c \rangle$  of the difference sets  $L_0 = \{0, 1, 4, 6\}$ ,  $-L_0 = \{0, 7, 9, 12\}$ ,  $M_0 = 5L_0 = \{0, 4, 5, 7\}$ , and  $-M_0 = \{0, 6, 8, 9\}$ . (The ATLAS uses the translates of  $\{0, 1, 3, 9\} = M_0 + 9$ , giving the third geometry.)

One of these unrooted cacti  $\mathcal{C}_1$ , associated with the first geometry  $\mathcal{L} = \{L_i = L_0 + i : i \in \mathbb{Z}_{13}\}$ , is represented by the cactus  $C_1$  consisting of

$$\begin{aligned} g_1 &= (0, 1)(2, 12)(3, 7)(8, 10), \\ g_2 &= (0, 2)(3, 11)(4, 5)(6, 7), \\ g_3 &= (3, 12)(4, 6)(8, 11)(9, 10). \end{aligned}$$

Indeed, we can assign projective coordinates to the points as follows:

$$\begin{aligned} 0 &= (0 : 0 : 1), & 1 &= (1 : 0 : 1), & 2 &= (2 : 2 : 1), & 3 &= (1 : 2 : 1), & 4 &= (2 : 0 : 1), \\ 5 &= (1 : 2 : 0), & 6 &= (1 : 0 : 0), & 7 &= (0 : 1 : 1), & 8 &= (0 : 2 : 1), & 9 &= (1 : 1 : 0), \\ 10 &= (1 : 1 : 1), & 11 &= (0 : 1 : 0), & 12 &= (2 : 1 : 1). \end{aligned}$$

Then we can represent  $g_1, g_2, g_3$ , and  $c$  as the matrices

$$\begin{pmatrix} 2 & & \\ & 2 & \\ 1 & & 1 \end{pmatrix}, \quad \begin{pmatrix} & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & & 1 \\ & 2 & 1 \\ & & 1 \end{pmatrix}, \quad \begin{pmatrix} & 1 & 1 \\ 2 & 1 & 1 \\ 1 & & 1 \end{pmatrix}.$$

By successively applying the generators  $\sigma_1$  and  $\sigma_2$  of  $B_3$  to  $C_1$ , one eventually obtains an orbit  $\Omega_1$  of 13 unrooted cacti  $C_1, \dots, C_{13}$ , on which the action of  $B_3$  is given by

$$\begin{aligned} \sigma_1 &\mapsto (1, 2, 3, 4)(5, 6, 7, 8, 9, 10)(11, 12, 13), \\ \sigma_2 &\mapsto (1, 4, 6, 7)(2, 3, 5, 12, 13, 8)(10, 11, 9), \end{aligned}$$

or equivalently

$$\begin{aligned} x &\mapsto (1, 3, 6)(2, 5, 7)(4)(8, 10, 12)(9, 11, 13), \\ y &\mapsto (1, 4)(2, 6)(3, 7)(5, 8)(9, 12)(10, 13)(11). \end{aligned}$$

These permutations are even, so they generate a subgroup  $P \leq A_{13}$ . Now  $P$  is transitive, and the only transitive proper subgroups of  $A_{13}$  are isomorphic to  $L_3(3)$  or to subgroups of  $AGL_1(13)$ . The cycle-structures of  $\sigma_1$  and  $\sigma_2$  exclude these possibilities, so  $P = A_{13}$ .

As in Case A,  $\text{Aut } \mathcal{P}$  can be identified with the group  $G$  of permutations of the points preserving the set of lines, and the action on lines induces a second subgroup  $G' \leq S_{13}$  which is isomorphic to  $G$  and which also contains  $c$ . Any cactus  $C = [g_1, g_2, g_3]$ , where the permutations  $g_i$  generate  $G$ , gives rise to a dual cactus  $C' = [g'_1, g'_2, g'_3]$ , where  $G'$  is generated by the permutations  $g'_i$  of the lines induced by  $g_i$ . For example, if  $C_1$  is the cactus given above, then  $C'_1$  is the cactus given by the following permutations of the subscripts of the lines  $L_i$ :

$$\begin{aligned} g'_1 &= (1, 12)(2, 6)(7, 10)(8, 9), \\ g'_2 &= (0, 1)(2, 7)(3, 5)(11, 12), \\ g'_3 &= (2, 11)(3, 6)(4, 5)(8, 10). \end{aligned}$$

If we regard these subscripts as the new points, then  $C'_1$  preserves the geometry  $\mathcal{L}' = \{-L_i\}$  on  $\mathbb{Z}_{13}$ . These cacti  $C_1$  and  $C'_1$  generate distinct subgroups  $G_1$  and  $G_2 = G'_1$  isomorphic to  $L_3(3)$  in  $S_{13}$ , so their corresponding unrooted cacti  $C_1$  and  $C'_1$  lie in distinct orbits  $\Omega_1$  and  $\Omega_2 = \Omega'_1$  of  $B_3$ , both of length 13. As in Case A, the geometric duality  $\mathcal{C} \mapsto \mathcal{C}'$  commutes with the actions of  $B_3$  on these two orbits, so  $\sigma_1$  and  $\sigma_2$  induce the same permutations of the subscripts, and  $B_3$  induces the same permutation group on  $\Omega_2$  as it does on  $\Omega_1$ , namely  $A_{13}$ . Similarly, the algebraic duality  $\mathcal{C} \mapsto \overline{\mathcal{C}}$  induces a bijection between  $\Omega_1$  and  $\overline{\Omega}_1 = \Omega_2$  which commutes with  $B_3$  modulo its outer automorphism  $\beta$ .

In exactly the same way, the remaining 26 unrooted cacti with monodromy group  $L_3(3)$  form two dual orbits  $\Omega_3$  and  $\Omega_4 = \Omega'_3 = \overline{\Omega}_3$ , in which the monodromy

groups  $G_3$  and  $G_4 = G'_3$  preserve the geometries  $\{-M_i\}$  and  $\{M_i\}$  on  $\mathbb{Z}_{13}$ . As a representative of  $\Omega_3$  we can take the unrooted cactus  $\mathcal{D}_1 = [D_1]$ , where  $D_1$  is given by

$$\begin{aligned} g_1 &= (0, 9)(3, 4)(5, 7)(10, 11), \\ g_2 &= (2, 9)(3, 8)(6, 7)(10, 12), \\ g_3 &= (0, 10)(1, 2)(3, 9)(5, 8); \end{aligned}$$

the dual orbit  $\Omega_4$  is represented by  $\mathcal{D}'_1 = [D'_1]$ , where  $D'_1$  is given by

$$\begin{aligned} g'_1 &= (1, 5)(3, 4)(7, 9)(10, 11), \\ g'_2 &= (0, 7)(1, 6)(2, 3)(10, 12), \\ g'_3 &= (0, 10)(1, 7)(2, 5)(8, 9). \end{aligned}$$

As in the case of  $\Omega_1$  and  $\Omega_2$ , geometric duality  $\Omega_3 \rightarrow \Omega_4$  commutes with the actions of  $B_3$ , while algebraic duality commutes with  $B_3$  modulo the outer automorphism  $\beta$ . The generators of  $B_3$  act on the subscripts of the unrooted cacti  $\mathcal{D}_i$  and  $\mathcal{D}'_i$  as follows:

$$\begin{aligned} \sigma_1 &\mapsto (1, 2, 3)(4, 5, 6, 7, 8, 9)(10, 11, 12, 13), \\ \sigma_2 &\mapsto (1, 4, 9, 3, 11, 13)(5, 8, 12)(6, 2, 7, 10), \end{aligned}$$

or equivalently

$$\begin{aligned} x &\mapsto (1, 7, 12)(2, 11, 5)(3, 4, 8)(6, 10, 13)(9), \\ y &\mapsto (1, 8)(2, 12)(3, 5)(4, 9)(6, 11)(7, 13)(10). \end{aligned}$$

As with  $\Omega_1$  and  $\Omega_2$ , their cycle-structures imply that these permutations generate  $A_{13}$ .

Although  $B_3$  acts in the same way on the pair  $\Omega_1$  and  $\Omega_2$ , and also in the same way on the pair  $\Omega_3$  and  $\Omega_4$ , it does *not* act on the same way on  $\Omega_3$  and  $\Omega_4$  as it does on  $\Omega_1$  and  $\Omega_2$ , even if we allow for an automorphism of  $B_3$ . This can be seen by comparing the trivalent maps  $\mathcal{M}$  representing the actions of  $B_3$  on these two pairs of orbits (see Figure 4): although they have the same vertex-, edge- and face-valencies, they are neither isomorphic nor mirror-images of each other. As in Case A, it is mysterious why  $B_3$  should have two actions which have so many features in common, and yet are not isomorphic.

For completeness, we give here a cactus representing the remaining orbit  $\Omega_0$  of 35620 unrooted cacti, with monodromy group  $A_{13}$ :

$$\begin{aligned} g_1 &= (0, 1)(2, 11)(3, 9)(4, 7), \\ g_2 &= (0, 12)(6, 7)(8, 9)(10, 11), \\ g_3 &= (2, 12)(3, 10)(4, 8)(5, 6). \end{aligned}$$

**5.4. Case C of Theorem 1.3.** In Case C of Theorem 1.3 we have  $\Pi = \Pi_C = [2^6 1^3, 2^4 1^7, 2^4 1^7]$ , with  $n = 15$ , so the Goulden–Jackson number is

$$N(\Pi_C) = 15 \cdot \left( \frac{8!}{6! 3!} \right) \cdot \left( \frac{10!}{4! 7!} \right)^2 = 126000.$$

Now there are no symmetric cacti with this passport: if there were, then either  $c^3$  or  $c^5$  would commute with  $g_2$  and would therefore have to permute its fixed

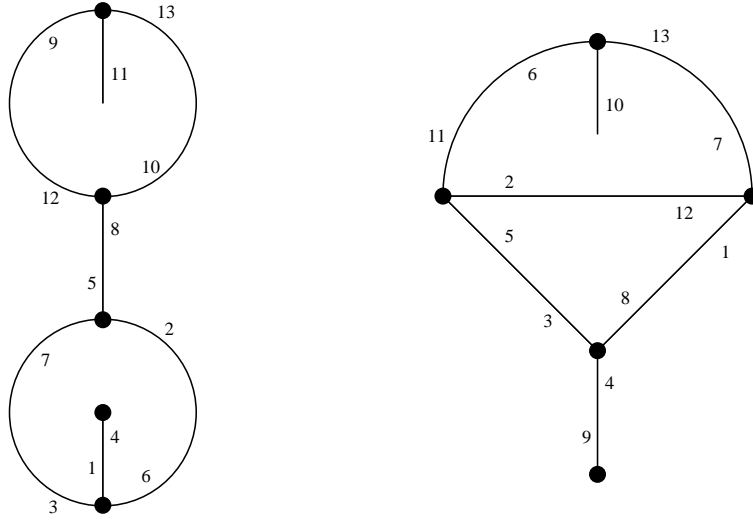


FIGURE 4. Each trivalent map represents two orbits of size 13

points; it would have to do so in cycles of length 5 or 3 respectively, which is impossible since  $g_2$  fixes 7 points. It follows that there are 126000 unrooted cacti with passport  $\Pi_C$ . The braid group  $B_3$  permutes the three different orderings of  $\Pi_C$ , so we need to consider the  $3 \cdot 126000 = 378000$  unrooted cacti associated with these three passports. By computer,  $B_3$  has a single orbit of length 377835, consisting of unrooted cacti with monodromy group  $A_{15}$ . We shall show that the remaining 165 unrooted cacti consist of a single  $B_3$ -orbit of length 135 with an imprimitive monodromy group  $(S_3 \wr S_5) \cap A_{15}$ , and two dual orbits of length 15 with monodromy group  $G \cong L_4(2) \cong A_8$ ; this is a simple group of order 20160 which acts on the 15 points and the 15 planes of the projective geometry  $PG_3(2)$ . Thus, there exist four topological equivalence classes of polynomials with this passport.

If we apply equation (5) to  $G = L_4(2)$ , with  $n = 15$ , we find that there are  $\nu = \phi(15)/(4 \cdot 1) = 2$  groups  $G_1, G_2 \cong G$  containing  $C$ . They are transposed by  $\tilde{C}$ , and the kernel of this action, of order  $15 \cdot 4 = 60$ , is  $K = N_{G_i}(C) \leq G_1 \cap G_2$ .

We shall now show that  $G_1 \cap G_2 = K$ , as in Cases A and B; this time, however, the proof is not so straightforward, the difference being that here  $K$  is not maximal in each  $G_i$ . In fact, it follows from the list of maximal subgroups of  $L_4(2)$  in [CCNPW] that there is a unique subgroup  $H_i$  of each  $G_i$  such that  $K < H_i < G_i$ : if we identify  $G_i$  with  $A_8$  then  $H_i$  corresponds to the subgroup  $(S_3 \times S_5) \cap A_8$  of index  $\binom{8}{3} = 56$  in  $A_8$  preserving a partition  $3 + 5$  of the eight symbols, given by the two orbits of  $C$  ( $\cong C_3 \times C_5$ ). Alternatively,  $H_i$  can be identified with a subgroup  $\Gamma L_2(4)$  of  $L_4(2)$ , acting on the  $4^2 - 1 = 15$  non-zero vectors of its 2-dimensional module over  $\mathbb{F}_4$ ; this group is a split extension of  $GL_2(4) = C_3 \times SL_2(4) \cong A_3 \times A_5$  by  $C_2$ , where the direct factor  $C_3$  consists of the scalar matrices and the complement  $C_2$  represents the action of the Galois group of  $\mathbb{F}_4$ . It follows that  $G_1 \cap G_2$  must be either  $K$ , of order 60, or a subgroup  $H_1 = H_2$  of order 360. If we let  $\mathcal{G}$  and  $\mathcal{H}$



denote the sets of subgroups of  $S = S_{15}$  conjugate to  $G_i$  and  $H_i$ , then these two possibilities are distinguished by the fact that each  $H \in \mathcal{H}$  is contained in  $\nu = 1$  or 2 groups  $G \in \mathcal{G}$  respectively. We shall use Corollary 4.2 to show that  $\nu = 1$ , so the first possibility occurs. In the notation of Section 4.1, we have already seen that  $\tilde{G} (:= N_S(G))$  coincides with  $G$ . In order to show that  $\tilde{H} = H$ , we need the elementary result that if  $P$  is any transitive permutation group, then its centralizer in the symmetric group is isomorphic to  $N_P(P_\alpha)/P_\alpha$ , where  $P_\alpha$  is the subgroup of  $P$  stabilising a point  $\alpha$ . Applying this to  $SL_2(4)$ , a transitive group of degree 15 with point-stabilizer  $V_4$  of index 3 in its normalizer  $A_4$ , we see that  $C_S(SL_2(4))$  is the group  $C_3$  of scalar matrices; this group is therefore also the centralizer of  $GL_2(4)$ , and since it does not commute with the Galois group  $C_2$ , it follows that  $C_S(H) = 1$ . Hence the normalizer  $\tilde{H} = N_S(H)$ , acting faithfully by conjugation on  $H$ , is isomorphic to a subgroup of  $\text{Aut}(H) \cong S_3 \times S_5$ ; it contains  $H$ , which has index 2 in  $\text{Aut}(H)$ , and we cannot have  $\tilde{H} \cong S_3 \times S_5$  since then the subgroup  $SL_2(4)$  of  $H$  would have centralizer  $S_3$ , so  $\tilde{H} = H$ . The subgroups  $H \in \mathcal{H}$  contained in  $G$  form a single conjugacy class in  $\tilde{G} (= G)$ , and they satisfy  $|N_{\tilde{G}}(H) : H| = 1$  since they are maximal and not normal in  $G$ , so in Corollary 4.2 we have  $t = 1$  and  $m_1 = 1$ ; thus  $\nu = 1$  and hence  $G_1 \cap G_2 = K$ .

Let  $C_1$  be the cactus given by

$$\begin{aligned} g_1 &= (0, 1)(2, 3)(5, 14)(7, 10)(8, 9)(11, 13), \\ g_2 &= (2, 5)(6, 11)(8, 10)(12, 13), \\ g_3 &= (0, 2)(4, 5)(6, 14)(7, 11). \end{aligned}$$

We aim to show that this has monodromy group  $G \cong L_4(2)$  by constructing a projective geometry  $\mathcal{P} \cong PG_3(2)$  on  $\mathbb{Z}_{15}$  with  $g_1, g_2, g_3 \in \text{Aut } \mathcal{P}$ . We define the planes to be the translates  $P_i = P_0 + i$  of the difference set  $P_0 = \{0, 1, 3, 4, 7, 9, 14\}$ . Then the generators  $g_i$  permute the 15 planes, inducing the following permutations of their subscripts

$$\begin{aligned} g'_1 &= (0, 1)(2, 14)(4, 10)(6, 7)(8, 9)(11, 13), \\ g'_2 &= (3, 4)(5, 10)(6, 8)(11, 14), \\ g'_3 &= (0, 2)(3, 11)(6, 10)(12, 13), \end{aligned}$$

so the set of planes is invariant under  $G = \langle g_1, g_2, g_3 \rangle$ . Using the invariance under  $c = g_1 g_2 g_3 : i \mapsto i + 1$ , it is straightforward to check that the pairs of distinct planes intersect in 35 triples, which we shall take as the lines of  $\mathcal{P}$ . These triples are the fifteen translates of  $P_0 \cap P_1 = \{0, 1, 4\}$ , the fifteen translates of  $P_0 \cap P_2 = \{0, 2, 8\}$ , and the five translates of  $P_0 \cap P_5 = \{0, 5, 10\}$ . One can check that each plane contains seven lines, forming a Fano geometry  $\mathcal{F}$ : by the transitivity of  $\langle c \rangle$  on planes, it is sufficient to verify this for a single plane, such as  $P_0 = \{0, 1, 3, 4, 7, 9, 14\}$ ; this plane contains the lines  $\{0, 1, 4\}$ ,  $\{0, 3, 14\}$ ,  $\{0, 7, 9\}$ ,  $\{1, 3, 9\}$ ,  $\{1, 7, 14\}$ ,  $\{3, 4, 7\}$ , and  $\{4, 9, 14\}$ , and it is clear that any two of these lines meet in a single point, and any two points in  $P_0$  lie on a single line. This shows that the geometry  $\mathcal{P}$  we have constructed is isomorphic to  $PG_3(2)$ , and indeed we can give an explicit

isomorphism by assigning projective coordinates to the points as follows:

$$\begin{aligned} 0 &= (1 : 0 : 1 : 0), & 1 &= (1 : 0 : 0 : 0), & 2 &= (0 : 1 : 0 : 1), & 3 &= (0 : 1 : 0 : 0), \\ 4 &= (0 : 0 : 1 : 0), & 5 &= (1 : 1 : 0 : 1), & 6 &= (0 : 0 : 0 : 1), & 7 &= (0 : 1 : 1 : 0), \\ 8 &= (1 : 1 : 1 : 1), & 9 &= (1 : 1 : 0 : 0), & 10 &= (0 : 1 : 1 : 1), & 11 &= (1 : 0 : 0 : 1), \\ 12 &= (0 : 0 : 1 : 1), & 13 &= (1 : 0 : 1 : 1), & 14 &= (1 : 1 : 1 : 0). \end{aligned}$$

Thus  $P_0$  is the ‘plane at infinity’  $x_4 = 0$ , and  $g_1, g_2, g_3$ , and  $c$  are represented by the matrices

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ 1 & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & & \\ & 1 & & \\ 1 & 1 & & 1 \\ 1 & 1 & 1 & \end{pmatrix}, \quad \begin{pmatrix} & 1 & & \\ & & 1 & \\ 1 & 1 & & 1 \\ & 1 & 1 & \end{pmatrix}.$$

Since  $G$  induces a group of automorphisms of this geometry, we have  $G \leq \text{Aut } \mathcal{P} \cong \text{L}_4(2)$ .

To show that  $G = \text{Aut } \mathcal{P}$ , note that

$$\begin{aligned} g_1 g_2 &= (0, 1)(2, 3, 5, 14)(4)(6, 11, 12, 13)(7, 8, 9, 10), \\ g_2 g_3 &= (0, 2, 4, 5)(1)(3)(6, 7, 11, 14)(8, 10)(9)(12, 13), \end{aligned}$$

so that

$$\begin{aligned} c^4 g_1 g_2 c^{-4} &= (0)(1, 10, 13, 14)(2, 7, 8, 9)(3, 4, 5, 6)(11, 12), \\ c^3 g_2 g_3 c^{-3} &= (0)(1, 2, 12, 14)(3, 4, 8, 11)(5, 7)(6)(9, 10)(13). \end{aligned}$$

These permutations both fix 0, so by comparing their cycles we see that the stabilizer in  $G$  of the point 0 is transitive on  $\{1, \dots, 14\}$ , and hence  $G$  is doubly transitive on the points. The only doubly transitive proper subgroups of  $\text{L}_4(2)$  are isomorphic to  $A_7$  (see [CCNPW]) and hence have a single conjugacy class of involutions; the involutions  $g_1$  and  $g_2$  in  $G$  have different cycle-structures, and hence lie in different conjugacy classes, so  $G = \text{Aut } \mathcal{P} \cong \text{L}_4(2)$ .

The cactus  $C_1 = [g_1, g_2, g_3]$  induces a dual cactus  $C'_1 = [g'_1, g'_2, g'_3]$ , where  $g'$  is the permutation of the subscripts of the fifteen planes induced by an element  $g \in G$ ; as in our earlier examples, the labelling of points and planes implies that  $g'_1 g'_2 g'_3 = c' = c$ , as can be verified from the cycle decompositions of the permutations  $g'_i$  given above. This cactus  $C'_1$  has monodromy group  $G' = \{g' : g \in G\} \leq \text{S}_{15}$ . The groups  $G$  and  $G'$  are conjugate in  $\text{S}_{15}$ , since they arise from permutation representations of  $\text{L}_4(2)$  which differ by an outer automorphism (the point-plane duality of  $\mathcal{P}$ ); however, these two groups are distinct, since the permutation  $g'_1 \in G'$  (acting on points) sends the line  $\{0, 1, 4\}$  of  $\mathcal{P}$  to the triple  $\{0, 1, 10\}$ , which is not a line, so  $g'_1 \notin G$ . Thus  $G$  and  $G'$  are the two subgroups isomorphic to  $\text{L}_4(2)$  and containing  $c$  which we enumerated earlier. Since  $G \neq G'$ , it follows that the unrooted cacti  $C_1 = [C_1]$  and  $C'_1 = [C'_1]$  lie in different orbits  $\Omega_1$  and  $\Omega_2 = \Omega'_1$  of  $\text{B}_3$ . As in Cases A and B, geometric duality  $\mathcal{C} \mapsto \mathcal{C}'$  commutes with the actions of  $\text{B}_3$ , while algebraic duality  $\mathcal{C} \mapsto \bar{\mathcal{C}}$  commutes with it modulo  $\beta$ .

With a suitable numbering, the generators of  $B_3$  induce the following permutations of the subscripts of the unrooted cacti in  $\Omega_1$  and  $\Omega_2$ :

$$\sigma_1 \mapsto (1, 2, 3, 4)(5, 6, 7, 8, 9, 10)(11, 12, 13, 14)(15),$$

$$\sigma_2 \mapsto (1, 3, 5, 7)(2, 11, 10, 15, 8, 14)(4, 12, 6, 13)(9),$$

or equivalently

$$x \mapsto (1, 11, 6)(2, 5, 13)(3, 12, 4)(7, 14, 10)(8, 9, 15),$$

$$y \mapsto (1, 12)(2, 6)(3, 13)(4)(5, 14)(7, 11)(8, 10)(9, 15).$$

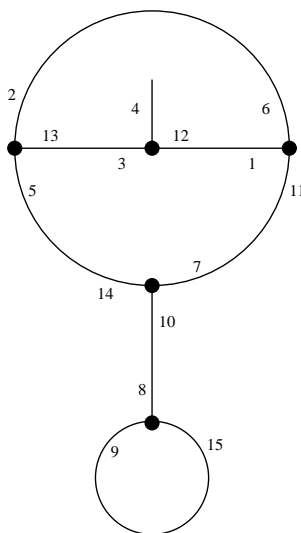


FIGURE 5. Trivalent map representing the orbits of size 15

These permutations generate an imprimitive permutation group  $P$ , with three blocks of size 5, so  $P$  is contained in the wreath product  $S_5 \wr S_3$ ; the blocks are the sets  $\{1, 3, 5, 7, 9\}$ ,  $\{2, 4, 6, 8, 10\}$ , and  $\{11, 12, 13, 14, 15\}$  corresponding to the cacti in which  $g_1, g_2$ , and  $g_3$  respectively have cycle-structure  $2^6 1^3$ . According to GAP,  $P$  has order  $5184000 = (5!)^3 \cdot 3!/2$ , so  $P$  has index 2 in  $S_5 \wr S_3$ . Now  $S_5 \wr S_3$  has three subgroups of index 2, namely the even subgroup  $(S_5 \wr S_3) \cap A_{15}$ , the subgroup  $S_5 \wr A_3$  which permutes the three blocks evenly, and the extension of the even subgroup  $(S_5)^3 \cap A_{15}$  of the base group  $(S_5)^3$  by  $S_3$ . Since the generators  $\sigma_i$  induce odd permutations, and also permute the three blocks as transpositions,  $P$  cannot be the first or second subgroup, so it must be the third. The trivalent map corresponding to these two orbits is shown in Figure 5.

This accounts for 30 of the ‘missing’ 165 unrooted cacti with passport  $\Pi_C$ . We shall now show that the remaining 135 all have an imprimitive monodromy group  $G = (S_3 \wr S_5) \cap A_{15}$ . We first consider the possibilities for an imprimitive monodromy group with passport  $\Pi_C$ .

Since the degree is  $15 = 3 \cdot 5$ , an imprimitive monodromy group  $G$  must have three blocks of size 5, or five of size 3. As shown by Ritt [Rit1], this corresponds to a decomposition  $p = q \circ r$  of the polynomial  $p$ , where  $q$  and  $r$  are polynomials of degrees 3 and 5 or vice versa. The first case is impossible: since  $g_2$  and  $g_3$  each fix seven points, they each fix set-wise at least two blocks, and hence they both permute the three blocks trivially, so  $g_1$  and  $c (= g_1 g_2 g_3)$  induce the same permutation of the blocks; this is impossible, since their cycle-structures imply that  $c$  must permute the blocks in a cycle of length 3, whereas  $g_1$  must fix a block. It follows that if  $G$  is imprimitive then it must have five blocks of size 3, so that  $G \leq S_3 \wr S_5$ . Since  $g_1, g_2$ , and  $g_3$  are all even permutations, we have  $G \leq (S_3 \wr S_5) \cap A_{15}$ . We now consider whether this can happen.

Let the blocks be  $\Phi_0, \dots, \Phi_4$ , and for each  $g \in G$  let  $\tilde{g} \in S_5$  denote the permutation of the labels of the blocks induced by  $g$ , so if  $C = [g_1, g_2, g_3]$  is an imprimitive cactus with passport  $\Pi_C$  then  $\tilde{C} = [\tilde{g}_1, \tilde{g}_2, \tilde{g}_3]$  is a cactus of degree 5, corresponding to the quintic polynomial  $q$  in the decomposition of  $p$ . Since each  $g_i$  is an involution, each  $\tilde{g}_i$  must have order 1 or 2. Now  $g_2$  and  $g_3$  fix seven points, so they fix set-wise at least three blocks, and hence they move at most two, that is,  $\tilde{g}_i$  is either a transposition or the identity for  $i = 2, 3$ . Since we require  $\tilde{G} = \langle \tilde{g}_1, \tilde{g}_2, \tilde{g}_3 \rangle$  to be a transitive subgroup of  $S_5$ , the only possibility is that  $\tilde{g}_2$  and  $\tilde{g}_3$  are mutually disjoint transpositions and  $\tilde{g}_1$  is a double transposition, that is,  $\tilde{C}$  has passport  $\tilde{\Pi} = [2^2 1, 2 1^3, 2 1^3]$ . The Goulden–Jackson number for this passport is

$$N(\tilde{\Pi}) = 5 \cdot \left( \frac{2!}{2!1!} \right) \cdot \left( \frac{3!}{1!3!} \right)^2 = 5,$$

corresponding to five unrooted cacti  $\tilde{C}_i$ , represented by

$$\begin{aligned} \tilde{C}_1 &= [(0, 4)(1, 3), (1, 4), (2, 3)], \\ \tilde{C}_2 &= [(0, 4)(1, 3), (2, 3), (1, 4)], \\ \tilde{C}_3 &= [(0, 1)(3, 4), (2, 3), (0, 2)], \\ \tilde{C}_4 &= [(0, 1)(3, 4), (0, 2), (0, 3)], \\ \tilde{C}_5 &= [(0, 1)(3, 4), (0, 3), (2, 3)]. \end{aligned}$$

It follows that there are  $3 \cdot 5 = 15$  unrooted cacti whose passports are permutations of  $\tilde{\Pi}$ . These all have monodromy group  $\tilde{G} = S_5$ , since a 5-cycle and a transposition generate  $S_5$ .

One can use a criterion of Khovanskii and Zdravkovska [KZ, Theorem 3] or verify directly by hand that these 15 unrooted cacti form a single orbit under  $B_3$ . If  $i$  denotes  $\tilde{C}_i$ , and  $i', i''$  denote the unrooted cacti formed from it by cyclic rotation of the partitions in  $\tilde{\Pi}$  (so that  $\tilde{g}_2$  and  $\tilde{g}_3$  are double transpositions in  $i'$  and  $i''$ ), then

$$\begin{aligned} \sigma_1 &\mapsto (1, 2', 5, 4')(2, 1', 4, 3', 3, 5')(1'', 2'')(3'', 4'', 5''), \\ \sigma_2 &\mapsto (1, 2)(3, 4, 5)(1', 2'', 5', 4'')(2', 1'', 4', 3'', 3', 5''), \end{aligned}$$

or equivalently

$$\begin{aligned} x &\mapsto (1, 1'', 5')(2, 2'', 4')(3, 4'', 2')(4, 5'', 3')(5, 3'', 1'), \\ y &\mapsto (1, 2'')(2, 1'')(3, 5'')(4, 3'')(5, 4'')(1', 4')(2', 5')(3'). \end{aligned}$$

This action is transitive but imprimitive, with three blocks  $\{1, \dots, 5\}$ ,  $\{1', \dots, 5'\}$ , and  $\{1'', \dots, 5''\}$  of size 5, so  $B_3$  induces a permutation group  $P \leq S_5 \wr S_3$  on this orbit. In fact, MAPLE shows that  $P$  has order 5184000, so  $P$  has index 2 in  $S_5 \wr S_3$ , and the argument we used in the case  $G \cong L_4(2)$  shows that  $P$  is the extension of  $B \cap A_{15}$  by  $S_3$ , where  $B$  is the base group  $(S_5)^3$  of  $S_5 \wr S_3$ . Thus  $P$  permutes the blocks as  $S_3$ ; the pure braid group  $P_3$  is the kernel of this action, since it has index 6 and its generators  $\sigma_1^2$ ,  $\sigma_2^2$ , and  $(\sigma_1^2)^{\sigma_2}$  act by

$$\begin{aligned} \sigma_1^2 &\mapsto (1, 5)(2, 4, 3)(1', 3', 5')(2', 4')(1'')(2'')(3'', 5'', 4''), \\ \sigma_2^2 &\mapsto (1)(2)(3, 5, 4)(1', 5')(2', 4', 3')(1'', 3'', 5'')(2'', 4''), \\ (\sigma_1^2)^{\sigma_2} &\mapsto (1, 5, 4)(2, 3)(1', 3', 2')(4')(5')(1'', 3'')(2'', 5'', 4''), \end{aligned}$$

leaving each block invariant.

We now consider how to construct an imprimitive cactus  $C$  of degree 15 as a triple covering of a cactus  $\tilde{C}$  of degree 5, or equivalently, how to construct the graph  $\Gamma$  corresponding to  $C$  as a triple covering of the graph  $\tilde{\Gamma}$  corresponding to  $\tilde{C}$  (see Figure 6 for  $\tilde{C} = \tilde{C}_1$ , and Section 2.2 for the general description of these graphs).

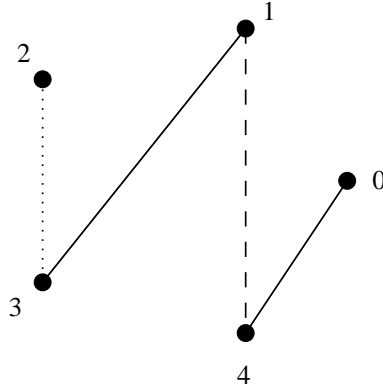


FIGURE 6. A cactus of degree 5

Since  $\tilde{g}_1$  is a double transposition in  $\tilde{C}$ , the four blocks it moves must support the six transpositions of  $g_1$ , and the remaining block must consist of the three fixed-points of  $g_1$ . Since  $\tilde{g}_i$  is a transposition for  $i = 2, 3$ , the two blocks it moves must support three of the four transpositions in  $g_i$ ; in each case, the remaining transposition must lie in one of the three blocks which are set-wise fixed by  $g_i$ . It follows that we can form  $\Gamma$  by taking three disjoint copies of  $\tilde{\Gamma}$ , the three copies of each vertex forming a block, and then, for  $i = 2, 3$ , adding a single broken or dotted edge (representing  $g_2$  or  $g_3$ ) joining a pair of vertices in one of the three blocks fixed by  $\tilde{g}_i$ ; provided these two extra edges do not connect the same two

copies of  $\tilde{\Gamma}$ , the resulting graph  $\Gamma$  will be a tree, representing a cactus  $C$ . There are five possibilities for  $\tilde{C} = [\tilde{C}]$ , and there are three choices each for the blocks fixed by  $g_2$  and  $g_3$ , giving  $5 \cdot 3 \cdot 3 = 45$  possible unrooted cacti  $C = [C]$  (or  $3 \cdot 45 = 135$  if we allow permutations of  $\Pi_C$ ).

We shall denote  $C$  by  $C_{ijk}$  if  $\Gamma$  is formed from three copies of the graph  $\tilde{\Gamma}_i$  corresponding to  $\tilde{C}_i$  by placing the extra edges corresponding to  $g_2$  and  $g_3$  in blocks  $\Phi_j$  and  $\Phi_k$ . For example, if  $i = 1$ , then  $j \in \{0, 2, 3\}$  and  $k \in \{0, 1, 4\}$  (see Figure 6). In Figure 7 two such imprimitive cacti are shown:  $C_{100}$  and  $C_{134}$ . The labels are put in such a way as to give  $c = (0, 1, 2, \dots, 14)$ . Note that, being projected from  $\mathbb{Z}_{15}$  to  $\mathbb{Z}_5$ , the labels in each copy of  $\tilde{\Gamma}_1$  become standard: 0, 1, 2, 3, 4.

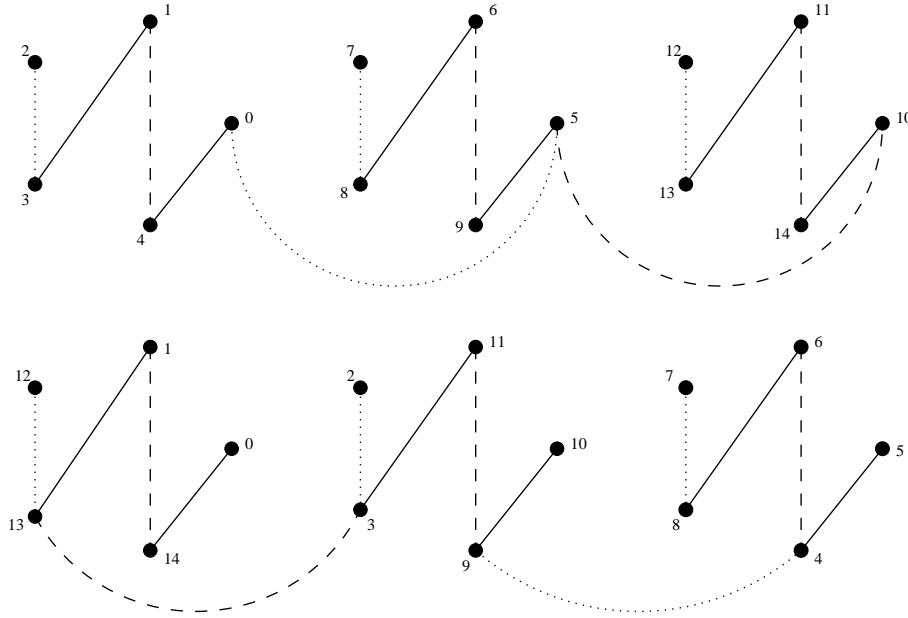


FIGURE 7. Two imprimitive cacti of degree 15

Let us now consider more closely the cactus  $C_{100}$  (see the upper part of Figure 7):

$$g_1 = (0, 4)(1, 3)(5, 9)(6, 8)(10, 14)(11, 13),$$

$$g_2 = (1, 4)(5, 10)(6, 9)(11, 14),$$

$$g_3 = (0, 5)(2, 3)(7, 8)(12, 13).$$

In this cactus,

$$g_2 g_3 = (0, 5, 10)(1, 4)(2, 3)(6, 9)(7, 8)(11, 14)(12, 13),$$

so  $(g_2 g_3)^2$  is the 3-cycle  $(0, 10, 5)$ , which lies in the factor  $S_3$  of the base group  $B = (S_3)^5$  of  $S_3 \wr S_5$  which permutes  $\Phi_0$ . Since  $G$  maps onto  $\tilde{G} = S_5$ , which permutes the factors of  $B$  transitively by conjugation, it follows that  $G$  contains a

3-cycle in every factor of  $B$ , so  $G$  contains the subgroup  $(A_3)^5$  of  $B$ . Similarly

$$g_1 g_3 = (0, 4, 5, 9)(1, 2, 3)(6, 7, 8)(10, 14)(11, 12, 13),$$

so  $(g_1 g_3)^6$  is the double transposition  $(0, 5)(4, 9)$ , which lies in the product of the factors of  $B$  which permute  $\Phi_0$  and  $\Phi_4$ . Since  $S_5$  permutes the factors of  $B$  doubly transitively, it follows that  $G$  contains a double transposition in the product of every pair of factors; conjugating these by suitable 3-cycles in the factors, we see that  $G$  contains every such double transposition, so  $G$  contains the even subgroup  $B \cap A_{15}$  which they generate. Thus  $G \cap B = B \cap A_{15}$ . Now  $G \cap B$  is the kernel of the epimorphism  $G \rightarrow \tilde{G} \cong S_5$  (the restriction to  $G$  of the natural epimorphism  $S_3 \wr S_5 \rightarrow (S_3 \wr S_5)/B \cong S_5$ ), so  $|G| = |G \cap B| \cdot |\tilde{G}| = \frac{1}{2}(3!)^5 \cdot 5! = |(S_3 \wr S_5) \cap A_{15}|$ . Since  $G \leq (S_3 \wr S_5) \cap A_{15}$ , it follows that  $G = (S_3 \wr S_5) \cap A_{15}$ .

By computer, these 135 unrooted cacti  $\mathcal{C}_{ijk} = [C_{ijk}]$  form a single orbit of  $B_3$ , so they all have the same monodromy group  $G$ . The corresponding polynomials form a single equivalence class, all of them having the form  $p = q \circ r$  where  $q$  and  $r$  are quintic and cubic polynomials.

For completeness, we give here a cactus representing the remaining orbit  $\Omega_0$  of 377835 unrooted cacti, with monodromy group  $A_{15}$ :

$$\begin{aligned} g_1 &= (0, 14)(4, 5)(6, 7)(8, 9)(10, 11)(12, 13), \\ g_2 &= (2, 14)(3, 12)(4, 10)(6, 8), \\ g_3 &= (1, 2)(3, 14)(4, 12)(6, 10). \end{aligned}$$

## 6. OBSERVATIONS

**1.** We have seen several instances where the braid group  $B_3$  has a pair of orbits  $\Omega$  and  $\Omega^*$  of the same length on unrooted cacti with the same passport, and the generators  $(\sigma_1$  and  $\sigma_2$ , or  $x$  and  $y$ ) of  $B_3$  have the same cycle-structures on these two orbits. In some cases, this is explained by a natural duality (algebraic or geometric) between  $\Omega$  and  $\Omega^*$ , which commutes with the actions of  $B_3$  (possibly modulo an outer automorphism). In other cases, we have shown (by determining  $\text{Aut } B_3$ ) that no such commuting duality  $\Omega \rightarrow \Omega^*$  can exist. Nevertheless, the numerical similarities between the actions on these pairs of orbits strongly suggest that there is some less obvious pairing, which is not respected by the braid group. It seems conceivable that the cacti in such orbits could correspond to polynomials defined over some subfield  $K$  of  $\mathbb{C}$ , and that an automorphism of  $K$ , applied to the coefficients, could induce such a pairing. This is by analogy with the case of algebraic duality  $\Omega \rightarrow \bar{\Omega}$ , which is induced by complex conjugation of  $K = \mathbb{C}$ ; being continuous, this automorphism respects the action of  $B_k$  modulo its outer automorphism induced by reflection of the plane. In other cases, an automorphism which is not continuous may not respect the action of  $B_k$ .

**2.** The geometric duality which we used in Cases A, B and C can be generalized. If  $\mathcal{B}$  is a block design, then any  $g \in \text{Aut } \mathcal{B}$ , regarded as a permutation of the points, induces a permutation  $g'$  of the blocks; if  $\mathcal{B}$  is symmetric (that is, the number of blocks is equal to the number  $n$  of points), then  $g'$  has the same cycle-structure as  $g$  [LW, Ch. 27]. In this case, if  $C = [g_1, \dots, g_k]$  is any cactus with monodromy group

$G \leq \text{Aut } \mathcal{B} \leq S_n$ , then by numbering the points and blocks so that  $c' = c$  we obtain a dual cactus  $C' = [g'_1, \dots, g'_k]$  with the same passport and with monodromy group  $G' \cong G$ . The arguments used earlier show that this geometric duality commutes with the actions of  $B_k$ , and induces a duality between unrooted cacti. As an example of a symmetric design one can take  $\mathcal{B}$  to consist of the points and hyperplanes of the projective geometry  $\text{PG}_{d-1}(q)$  over the field  $\mathbb{F}_q$  of order  $q$ , with  $n = (q^d - 1)/(q - 1)$ ; in this case the existence of an  $n$ -cycle  $c \in \text{Aut } \mathcal{B}$  was proved by Singer in [Sin]. Cases A, B and C provide particular examples of this.

**3.** It seems curious that, in the examples we have described here, the most ‘interesting’ braid group orbits on unrooted cacti have length equal to the degree  $n$  of the cacti concerned, while the other orbits have length divisible by  $n$ . In other similar situations we have examined (see Observation 4), the orbit-lengths are again multiples of  $n$ . This cannot be explained by the regular action of the cyclic subgroup  $\langle c \rangle$  of  $S_n$ , since by considering unrooted (rather than rooted) cacti we have already ‘factored out’ the action of this group. It is not at all clear what mechanism could explain such a phenomenon.

**4.** Much of this theory extends in a natural way to meromorphic functions  $p$  on compact Riemann surfaces  $X$ , regarded as branched coverings of the sphere. Instead of cacti, one must consider ordered sets of monodromy permutations, corresponding to the critical values  $w_i$  of  $p$ , but now the planarity condition (1) is replaced by the Riemann–Hurwitz formula, which gives the genus of  $X$  in terms of the branching data (including any branching at  $\infty$ ). As before, the topological equivalence classes correspond to the orbits of the appropriate braid group which moves the points  $w_i$  around the sphere. The monodromy group of  $p$  is a transitive permutation group of degree  $n$  equal to the order of  $p$  (the number of sheets of the covering); it is generated by the monodromy permutations, and is an invariant of the action of the braid group. If  $p$  has a single pole on  $X$ , or more generally if  $|p^{-1}(w_i)| = 1$  for some critical value  $w_i$ , then the corresponding generator is an  $n$ -cycle; in this situation, many of our results concerning permutations groups with cyclic regular subgroups can be applied, as we hope to show in a future paper.

**Acknowledgements.** G. J. is grateful to LaBRI (Université Bordeaux I) for its hospitality. A. Z. is grateful to Nikolai Adrianov, Askold Khovanskii and Smilka Zdravkovska for a number of extremely valuable discussions.

#### REFERENCES

- [Adr] N. M. Adrianov, *Classification of primitive edge rotation groups of plane trees*, *Fundam. Prikl. Mat.* **3** (1997), no. 4, 1069–1083 (Russian). MR 1 794 502
- [Bir] J. S. Birman, *Braids, links, and mapping class groups*, *Annals of Math. Studies*, 82, Princeton University Press, Princeton, N.J., 1974. MR 51 #11477
- [BBL] M. Bóna, M. Bousquet, G. Labelle, P. Leroux, *Enumeration of  $m$ -ary cacti*, *Adv. in Appl. Math.* **24** (2000), no. 1, 22–56. MR 2001c:05072
- [Bur] W. Burnside, *Theory of groups of finite order*, 2nd ed., Dover Publications Inc., New York, 1955. MR 16,1086c
- [Cle] A. Clebsch, *Zur Theorie der Riemann’schen Fläche*, *Math. Ann.* **6** (1873), 216–230.



- [CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. MR **88g**:20025
- [Dix] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205. MR **40** #4985
- [DM] J. D. Dixon, B. Mortimer, *Permutation groups*, Springer-Verlag, New York, 1996. MR **98m**:20003
- [DG] J. L. Dyer, E. K. Grossman, *The automorphism groups of the braid groups*, Amer. J. Math. **103** (1981), no. 6, 1151–1169. MR **82m**:20041
- [EHZZ] M. El Marraki, N. Hanusse, J. Zipperer, A. Zvonkin, *Cacti, braids and complex polynomials*, Sémin. Lothar. Combin. **37** (1996), Art. B37b, 36 pp. (electronic). MR **98j**:57003
- [Fei] W. Feit, *Some consequences of the classification of finite simple groups*, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., **37**, Amer. Math. Soc., Providence, R.I., 1980, pp. 175–181. MR **82c**:20019
- [GJ] I. P. Goulden, D. M. Jackson, *The combinatorial relationship between trees, cacti and certain connection coefficients for the symmetric group*, European J. Combin. **13** (1992), no. 5, 357–365. MR **93g**:05148
- [Hir] J. W. P. Hirschfeld, *Projective geometries over finite fields*, 2nd ed., Oxford Math. Monographs, The Clarendon Press, Oxford University Press, New York, 1998. MR **99b**:51006
- [Hup] B. Huppert, *Endliche Gruppen. I*, Springer-Verlag, Berlin, 1967. MR **37** #302
- [Hur] A. Hurwitz, *über Riemann'sche Fläche mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), 1–61.
- [Jon1] G. A. Jones, *Triangular maps and noncongruence subgroups of the modular group*, Bull. London Math. Soc. **11** (1979), no. 2, 117–123. MR **83a**:10039
- [Jon2] G. A. Jones, *Cyclic regular subgroups of primitive permutation groups*, submitted.
- [JS] G. A. Jones, D. Singerman, *Theory of maps on orientable surfaces*, Proc. London Math. Soc. (3) **37** (1978), no. 2, 273–307. MR **58** #21744
- [KZ] A. G. Khovanskii, S. Zdravkovska, *Branched covers of  $S^2$  and braid groups*, J. Knot Theory Ramifications **5** (1996), no. 1, 55–75. MR **97a**:57002
- [Kne] H. Kneser, *Die Deformationssätze der einfach zusammenhängenden Flächen*, Math. Z. **25** (1926), 362–372.
- [LW] J. H. van Lint, R. M. Wilson, *A course in combinatorics*, 2nd ed., Cambridge University Press, Cambridge, 2001. MR **1** 871 828
- [Lür] J. Lüroth, *Note über Verschweigungsschnitte und Querschnitte in einer Riemann'schen Fläche*, Math. Ann. **4** (1871), 181–184.
- [Mül] Peter Müller, *Primitive monodromy groups of polynomials*, Recent developments in the inverse Galois problem (Seattle, WA, 1993), Contemp. Math., **186**, Amer. Math. Soc., Providence, RI, 1995, pp. 385–401. MR **96m**:20004
- [Rit1] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), no. 1, 51–66. MR **1** 501 189
- [Rit2] J. F. Ritt, *On algebraic functions which can be expressed in terms of radicals*, Trans. Amer. Math. Soc. **24** (1923), no. 1, 21–30. MR **1** 501 211
- [Sch] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, S. B. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 598–623.
- [Ser] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett Publishers, Boston, MA, 1992. MR **94d**:12006
- [Sin] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385. MR **1** 501 951
- [Tho] R. Thom, *L'équivalence d'une fonction différentiable et d'un polynôme*, Topology **3** (1965), no. suppl. 2, 297–307. MR **32** #4702
- [Tsu] T. Tsuzuku, *Finite groups and finite geometries*, Cambridge Tracts in Math., **70**, Cambridge University Press, Cambridge, 1982. MR **83b**:20001
- [Völ] H. Völklein, *Groups as Galois groups*, Cambridge Studies in Adv. Math., **53**, Cambridge University Press, Cambridge, 1996. MR **98b**:12003

- [Wie] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964. MR 32 #1252
- [Zdr] S. Zdravkovska, *The topological classification of polynomial mappings*, Uspehi Mat. Nauk **25** (1970), no. 4, 179–180 (Russian). MR 46 #2684
- [Zvo] A. Zvonkin, *Towards topological classification of univariate complex polynomials*, Formal power series and algebraic combinatorics (Moscow, 2000), Springer, Berlin, 2000, pp. 76–87. MR **2001i**:14039

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHAMPTON, SOUTHAMPTON SO17 1BJ,  
UNITED KINGDOM

*E-mail address*: G.A.Jones@maths.soton.ac.uk

LABRI, UNIVERSITÉ BORDEAUX I, 351 COURS DE LA LIBÉRATION, F-33405 TALENCE CEDEX  
FRANCE

*E-mail address*: zvonkin@labri.u-bordeaux.fr