Reflection Groups and Polytopes over Finite Fields, I

B. Monson
University of New Brunswick
Fredericton, New Brunswick, Canada E3B 5A3

and

Egon Schulte
Northeastern University
Boston, Massachussetts, USA, 02115

With best wishes for our friend and colleague, Peter McMullen

Abstract

Any Coxeter group Γ, with string diagram, is the symmetry group of a (possibly infinite) regular polytope $\mathcal{P}$. When Γ is crystallographic, we may reduce its standard real representation modulo an odd prime p, thereby obtaining a finite representation in some orthogonal space over $\mathbb{Z}_p$. In many cases, the latter group will be the symmetry group of a finite regular polytope. In this paper, we investigate several such families of polytopes and the interplay between their geometric properties and the algebraic structure of the overlying finite orthogonal group.

Key Words: reflection groups, regular abstract polytopes

AMS Subject Classification (2000): Primary: 51M20. Secondary: 20F55.

1 Introduction

The regular polytopes have been objects of fascination for mathematicians since antiquity. In recent years, the algebraic and geometric theory of these and other symmetrical structures has been reinvigorated by the contributions of Coxeter, Grünbaum, Tits and many others. One particularly rich and satisfying branch of the subject concerns *abstract regular polytopes*. Here we investigate in considerable depth the interplay between these objects and the geometry of orthogonal spaces, usually over finite fields.

We begin in §2 with an overview of the basic theory of abstract regular polytopes, referring to [24] for details. Next, in §3, we discuss reflection groups, specifically linear representations of Coxeter groups, followed by a summary of the classification of finite irreducible reflection groups, as tailored to our geometrical needs.

In §4, we describe the modular reduction of crystallographic Coxeter groups. Then, in Theorems 4.1 and 4.2, we develop useful algebraic criteria which ensure that such linear groups are automorphism groups of regular polytopes. (The use of modular reduction to describe finite algebraic and geometric structures is, of course, quite natural: compare [13], [22], [26], [32], for example.) In §5 we catalog the modular polytopes of rank at most 3. We thereby obtain several new families of finite regular maps. In the final section we describe all the remaining spherical and Euclidean cases.

We must leave to a subsequent paper an investigation of the polytopes of higher rank obtained by our construction. The examples of rank 4 are particularly abundant and rich in structure, yet are accessible enough to be completely classified.

Finally, as a rather overdue birthday greeting, we wish to acknowledge once more the insight and help of our colleague Peter McMullen. Passing over his many deep contributions to convexity, one observes a continuing interest in symmetry, from the star-polytopes [19] and combinatorial regularity [18], continuing through several contributions to the theory of abstract polytopes, for instance [20, 21, 23], and culminating – for now – in the monograph [24]. We are confident that he will surprise us often again.

2 Abstract Regular Polytopes

An *(abstract) n-polytope* $\mathcal{P}$ is a partially ordered set with a strictly monotone rank function having range $\{-1, 0, \ldots, n\}$. An element $F \in \mathcal{P}$ with $\mathrm{rank}(F) = j$ is called a *j-face*; and faces of ranks 0, 1 and $n-1$ are called *vertices*, *edges* and *facets*, respectively. We also require that $\mathcal{P}$ have two improper faces: a unique least face F_{-1} and a unique greatest face F_n. Furthermore, each maximal chain or *flag* in $\mathcal{P}$ must contain $n+2$ faces, and $\mathcal{P}$ should be strongly flag–connected. Finally, $\mathcal{P}$ must have a homogeneity property: whenever $F < G$ with $\mathrm{rank}(F) = j-1$ and $\mathrm{rank}(G) = j+1$, there are exactly two j-faces H with $F < H < G$.

The symmetry of $\mathcal{P}$ is, of course, exhibited by its *automorphism group* $\Gamma(\mathcal{P})$. In particular, $\mathcal{P}$ is *regular* if $\Gamma(\mathcal{P})$ is transitive on flags, as will usually be the case here. Now fix a base flag $\Phi = \{F_{-1}, F_0, \ldots, F_{n-1}, F_n\}$, with rank $(F_j) = j$. For $0 \leq j \leq n-1$, there is a unique flag ${}^j\Phi$ differing from Φ in just the rank j face; let ρ_j be the (unique) automorphism with $\rho_j(\Phi) = {}^j\Phi$. In this case, $\Gamma(\mathcal{P})$ is generated by the involutions $\rho_0, \rho_1, \ldots, \rho_{n-1}$, which satisfy at least the relations

$$(\rho_i \rho_j)^{p_{ij}} = 1, \quad 0 \leq i, j \leq n-1, \tag{1}$$

where $p_{ii} = 1$ and $2 \leq p_{ij} \leq \infty$ for all $i \neq j$, and with the additonal restriction that

$$p_{ij} = 2 \ \text{ for } \ |i-j| \geq 2. \tag{2}$$

Finally, an *intersection condition* on standard subgroups holds:

$$\langle \rho_i \,|\, i \in I \rangle \cap \langle \rho_i \,|\, i \in J \rangle = \langle \rho_i \,|\, i \in I \cap J \rangle \tag{3}$$

for all $I, J \subseteq \{0, \ldots, n-1\}$. In short, $\Gamma(\mathcal{P})$ is a very particular quotient of a Coxeter group with string diagram. Conversely, given any group $\Gamma = \langle \rho_0, \ldots, \rho_{n-1} \rangle$ generated by involutions and satisfying (1), (2) and (3), one may construct a polytope $\mathcal{P}$ with $\Gamma(\mathcal{P}) = \Gamma$ (see [24, Theorem 2E11]). We shall say that $\Gamma(\mathcal{P})$ is a *string C-group.* The details of this construction identify $\mathcal{P}$ as a particular kind of *thin diagram geometry* (see [4, pp. 1165, 1187]).

A Coxeter group with *any* sort of diagram satisfies condition (3) [14, Th. 5.5(c)]. Thus, if a Coxeter group Γ has a string diagram, it certainly is a string C-group, although Γ and the corresponding polytope $\mathcal{P}$ may well be infinite. In particular, the automorphism group of the regular polygon $\{q\}$, $q \in \{2, 3, \ldots, \infty\}$, is the dihedral group of order $2q$.

Typically in the investigation of an interesting class of groups, the relations (1) and (2) are easily verified, whereas the intersection condition does not obviously hold. Thus, the following sufficient conditions are very helpful.

Proposition 2.1 *Suppose* $\Gamma = \langle \rho_0, \rho_1, \ldots, \rho_{n-1} \rangle$ *is a group generated by specified involutions satisfying relations (1) and (2), and suppose that the subgroup* $\Gamma_{n-1} := \langle \rho_0, \ldots, \rho_{n-2} \rangle$ *is a string C-group (with respect to the specified generators).*

(a) If $\Gamma_0 := \langle \rho_1, \ldots, \rho_{n-1} \rangle$ *is also a string C-group, and*

$$\Gamma_0 \cap \Gamma_{n-1} = \langle \rho_1, \ldots, \rho_{n-2} \rangle \ ,$$

then Γ *is a string C-group.*

(b) If Γ_0 *is also a string C-groups,* $\rho_{n-1} \notin \Gamma_{n-1}$*, and the subgroup* $\langle \rho_1, \ldots, \rho_{n-2} \rangle$ *is maximal in* Γ_0*, then* Γ *is a string C-group.*

Proof: [24, Prop. 2E16 and Lemma 11A10]. □

In order to prepare the way for our construction of several families of string C-groups (and the associated polytopes), we must first summarize some basic properties of groups generated by reflections.

3 Reflection Groups and Coxeter Groups

In order to sensibly discuss a detailed classification of finite irreducible reflection groups, we must first establish some terminology and describe several important classes of groups. Henceforth, V will denote a finite-dimensional vector space over a field $\mathbb{K}$ of characteristic $p \neq 2$; $\check{V}$ is its dual, and $e \in GL(V)$ is the identity mapping on V. For any subgroup $G \subseteq GL(V)$, we may define two G-invariant subspaces: the *fixed space* $V^G := \{x \in V \mid g(x) = x, \ \forall g \in G\}$, and the *direction space* V_G, spanned by $\{x - g(x) \mid g \in G, \ x \in V\}$. Similarly, V^g, V_g will denote the analogous subspaces for a particular element $g \in G$.

Usually below, G will be a subgroup of $O(V)$, the group of all *isometries* for some symmetric bilinear form $x \cdot y$ on V. Recall that $x \cdot y$ has *radical* (subspace)

$$\mathrm{rad} V := \{x \in V \mid x \cdot y = 0, \ \forall y \in V\} \ .$$

The *orthogonal space* V is *non-singular* if $\mathrm{rad}V = \{o\}$.

A mapping $r \in GL(V)$ is said to be *one-dimensional* (or a pseudo-reflection) if $\mathrm{rank}(r - e) = 1$. In other words, there should exist a vector $a \in V$, and a linear map $\varphi \in \check{V}$, both non-zero, so that

$$r(x) = x + \varphi(x)a, \quad \forall x \in V. \tag{4}$$

Since $\det(r) = 1 + \varphi(a)$, we have $\varphi(a) \neq -1$. Note that $V^r = \ker\varphi$ has codimension 1, and $V_r = \mathbb{K}a$. Thus $V_r \subseteq V^r$ if and only if $\varphi(a) = 0$, in which case r is a *transvection*, having period p, if $p > 2$, or period ∞, when $p = 0$. Otherwise, $V = V^r \oplus V_r$, and r acts as the scalar $1+\varphi(a)$ on V_r. Since $p \neq 2$, we conclude that r is involutory if and only if $\varphi(a) = -2$. Because r then acts as -1 on V_r, we call r a *reflection*. In this case, we say that a is a *root* for r. (More precisely, we could say that r is a *linear involutory hyperplane* reflection. Pseudo-reflections of period $q > 2$, such as occur in some of the unitary groups described in [9] or [5], will not concern us here.)

Let us extend the notation by setting $r_{\varphi,a}(x) = x + \varphi(x)a$, allowing $r_{0,a} = r_{\varphi,0} = e$. We record some useful and easily verified properties of these general one-dimensional mappings.

Lemma 3.1 (a) $r_{\varphi,ta} = r_{t\varphi,a}, \quad \forall t \in \mathbb{K}$.

(b) $g r_{\varphi,a} g^{-1} = r_{\varphi\circ g^{-1},\, g(a)}\ , \quad \forall g \in GL(V)$.

(c) $r_{\varphi,a}^{-1} = r_{\varphi,\, ta}$, where $t = -(1+\varphi(a))^{-1}$.

(d) Suppose $r_{\varphi,a} \neq e \neq r_{\psi,b}$, where a, b are independent; then $r_{\varphi,a}$ and $r_{\psi,b}$ commute if and only if $\varphi(b) = 0 = \psi(a)$.

(e) Suppose $r_{\varphi,a}$ is a one-dimensional isometry for the non-singular orthogonal space $(V, \cdot)$. Then $r_{\varphi,a}$ must be an orthogonal reflection, the root a must be non-isotropic and

$$r_{\varphi,a}(x) = x - 2\,\frac{x \cdot a}{a \cdot a}\,a, \quad \forall x \in V. \tag{5}$$

We often write $r_a := r_{\varphi,a}$ in this case.

(f) If $r_{\varphi,a},\ r_{\psi,b}$ are reflections, and $\varphi(b) = 0 \neq \psi(a)$, then the commutator

$$[r_{\varphi,a},\ r_{\psi,b}] = (r_{\varphi,a} r_{\psi,b})^2$$

is a non-trivial transvection.

(g) The product of two reflections with the same direction space (resp. fixed space) is a transvection with this direction space (resp. fixed space). The product, in any order, of a reflection and a transvection with the same direction space (resp. fixed space) is a reflection with this direction space (resp. fixed space).

(h) A subspace $U \subseteq V$ is invariant under the reflection $r_{\varphi,a}$ if and only if $U \subseteq \ker\varphi$ or $\mathbb{K}a \subseteq U$ (i.e. $a \in U$). Similarly, $f \in GL(V)$ commutes with $r_{\varphi,a}$ if and only if $\ker\varphi$ and $\mathbb{K}a$ are f-invariant.

(i) For transvections, one has

$$r_{\varphi,a} r_{\psi,a} = r_{\varphi+\psi,a} \quad \text{and} \quad r_{\varphi,a} r_{\varphi,b} = r_{\varphi,a+b}.$$

(Thus the transvections with common fixed space $\ker\varphi$ constitute an abelian subgroup of $GL(V)$ isomorphic to $(\ker\varphi, +)$.)

Proof. Part (f) appears in [30, Lemma 3.1], and part (h) in [2, chap.v, §2, prop.3]. □

In fact, we shall mainly be concerned with subgroups $G \subseteq GL(V)$ generated by reflections, typically

$$G = \langle r_j \,|\, j \in J \rangle,$$

for some finite index set J. Thus, we have $r_j(x) = x + \varphi_j(x)a_j$, with $\varphi_j(a_j) = -2$ for $j \in J$. Note then that

$$V^G = \bigcap_{j\in J} \ker\varphi_j, \quad V_G = \text{span}\{a_j \,|\, j \in J\}.$$

We shall say that the *reflection group* G, with the specified generators r_j, is *balanced* if $\varphi_j(a_k) = 0$ implies $\varphi_k(a_j) = 0$ for $j, k \in J$. For example, if G contains no transvections, then G must be balanced, in this sense, by Lemma 3.1(f). In particular, by Lemma 3.1(e), this is the case if G is a group of isometries for some non-singular orthogonal space V.

For a balanced reflection group we may define a graph $\Delta(G)$, with vertex set J, such that distinct $j, k \in J$ are adjacent whenever $\varphi_j(a_k) \neq 0$. To avoid confusion with the faces of polytopes, we speak of the *nodes* and *branches* of the *diagram* $\Delta(G)$. We shall soon see that Coxeter diagrams arise in this way, and numerous modifications of these can be seen below; but for now we attach no labels to the nodes or branches of $\Delta(G)$.

The matrix $N := [\varphi_i(a_j)]$ (indexed by $i, j \in J$) is called a *Cartan matrix* for G (with respect to the specified generating reflections). Since $\varphi_j(a_j) = t_j^{-1}\varphi_j(t_j a_j)$, for any $t_j \in \mathbb{K}^*$, N is not uniquely specified by the generators, but rather is determined only up to similarity by a diagonal matrix T with entries t_j. (See [17, §1] for implications in the real case.)

Lemma 3.2 *Let $\Delta(G)$ be the diagram for the balanced reflection group $G = \langle r_j \,|\, j \in J\rangle$ with Cartan matrix N. Then*

(a) G acts irreducibly if and only if $\det(N) \neq 0$ and $\Delta(G)$ is connected.

(b) If $\Delta(G)$ is connected, but $\det(N) = 0$, then every proper G-invariant subspace of V is either contained in V^G or contains V_G.

Proof. See [14, §6.1,6.3]; the key ideas in the real case generalize easily. □

An important class of balanced reflection groups is provided by the 'standard' real representation of a Coxeter group $\Gamma = \langle \rho_0, \ldots, \rho_{n-1}\rangle$ with presentation (1). On an n-dimensional *real* vector space V, with basis $a_0, \ldots, a_{n-1}$, we define a symmetric bilinear form $x \cdot y$ by setting

$$a_i \cdot a_j := -2\cos\frac{\pi}{p_{ij}}, \quad 0 \leq i, j \leq n-1, \tag{6}$$

where p_{ij} is the period of $\rho_i\rho_j$ indicated in (1). Note that each $a_j^2 := a_j \cdot a_j = 2$ and that $r_j(x) = x - (x \cdot a_j)a_j$ describes an isometric reflection on V. It is well known that the mapping $\rho_j \mapsto r_j$ induces a faithful representation

$$R : \Gamma \to G := \langle r_0, \ldots, r_{n-1} \rangle \tag{7}$$

of Γ in the orthogonal group $O(V)$ for the form $x \cdot y$ [14, §5.3-5.4]. Accordingly, we may put Γ aside and work instead with the *linear Coxeter group* G. (See [3, 16, 17] or [29] for further properties of more general linear Coxeter groups.)

From our earlier remarks, we observe that G is balanced and therefore has a diagram $\Delta(G)$, from which we obtain the familiar *Coxeter diagram* $\Delta_c(G)$ for G (and for Γ) as follows: whenever $p_{ij} \geq 3$ label the branch connecting nodes i, j by p_{ij}. (If $p_{ij} = 2$, nodes i, j are non-adjacent. The very common label 3 is often suppressed.)

Now let

$$m = 2\,\mathrm{lcm}\{p_{ij} \,|\, p_{ij} < \infty, \ \ 0 \leq i,\, j \leq n-1\}\ ,$$

and suppose ξ is a primitive m-th root of unity. It is easily seen that with respect to the basis $\{a_i\}$, the reflections r_j are represented by matrices in $GL_n(\mathbb{D})$, where $\mathbb{D} = \mathbb{Z}[\xi]$. (By [11, Th. 21.13], $\mathbb{D}$ is the ring of integers in the algebraic number field $\mathbb{Q}(\xi)$; and $\mathbb{D}$ has (finite) rank $\phi(m)$ as a $\mathbb{Z}$-module.) Since we may view G as a subgroup of $GL_n(\mathbb{D})$, it is possible to *reduce* G *mod* p, for any prime p, here allowing $p = 2$ [11, ch. XII]. Briefly, first suppose that $p\mathbb{D} \subseteq \mathbb{M} \subset \mathbb{D}$, for some maximal ideal $\mathbb{M}$. Then $\mathbb{K} := \mathbb{D}/\mathbb{M}$ is a finite field of characteristic p, and reduction mod p of G is achieved by applying the natural epimorphism $\mathbb{D} \to \mathbb{K}$ to the entries of $g \in G \subseteq GL_n(\mathbb{D})$. This defines a representation $\kappa : G \to GL_n(\mathbb{K})$. We let $G^p := \kappa(G)$ denote the image group. (This construction is essentially independent of the choice of $\mathbb{M}$.)

It is easy to prove that κ is faithful when $|G|$ is finite, but $p \nmid |G|$. In any case, $\ker\kappa$ is a p - subgroup of G. In fact, for the finite reflection groups G considered below, κ is usually faithful even when p divides $|G|$.

Recall that the linear Coxeter group G is finite precisely when $x \cdot y$ is positive definite ([14, Th. 6.4]). Each such G is therefore an *orthogonal group generated by reflections*. If G is irreducible, it is thus one of the well known finite Coxeter groups of type A_n $(n \geq 1)$, B_n $(n \geq 2)$, D_n $(n \geq 4)$, E_n $(n = 6, 7, 8)$, F_4, H_3, H_4, or $I_2(m)$ (dihedral of order $2m$). (It is convenient here to indicate the actual linear groups in this way. In the literature, A_n, for example, often refers to the corresponding diagram or root system.)

Clearly, a finite Coxeter group G will leave invariant the unit sphere $\mathbb{S}^{n-1}$ in V; in such cases, G (or Γ) is said to be of *spherical type*. Likewise, when $x \cdot y$ is positive semidefinite, with $\dim(\mathrm{rad}V) = 1$, the infinite Coxeter group G is of *Euclidean type* and acts naturally on Euclidean $(n-1)$-space $\mathbb{E}^{n-1}$ [14, ch. 4]. We shall also encounter several examples in which $x \cdot y$ is non-singular with signature $(+ + \ldots + -)$, so that G is of *hyperbolic type* and acts on hyperbolic $(n-1)$-space $\mathbb{H}^{n-1}$ [14, §6.8-6.9].

Also pertinent here are the finite *unitary groups generated by reflections*, first completely enumerated by Shephard and Todd ([27]). We need mention only the irreducible cases generated by involutory reflections in unitary space of dimension $n \geq 3$. These are (i) the *imprimitive* groups of type $D_n(m) = G(m, m, n)$, and type $B_n(m) = G(m, m/2, n)$ (for even $m \geq 2$); and (ii) the *primitive* groups $J_3(4)$, $J_3(5)$, N_4, EN_4, K_5 and K_6. (In the notation of [8] and [24, §9A], we have $J_3(4) = [1\,1\,1^4]^4$, $J_3(5) = [1\,1\,1^5]^4$, $N_4 = [1\,1\,2]^4$, $K_5 = [2\,1\,2]^3$ and $K_6 = [2\,1\,3]^3$; these groups require n generating reflections, whereas EN_4 requires $n+1(=5)$. We do not need a detailed description of the case $n = 2$, which is a little more involved; see [5], [8] or [9]).

Another important source of irreducible groups generated by reflections is the full orthogonal group $O(V)$ for some non-singular symmetric bilinear form $x \cdot y$ on V ([1, Th. 3.20]). The *discriminant* of this orthogonal space is $\mathrm{disc}(V) := \det[a_i \cdot a_j]$, where $\{a_i\}$ is some basis for V. Thus the image of $\mathrm{disc}(V)$ in $\mathbb{K}^*/(\mathbb{K}^*)^2$ is a true invariant, and we write $\mathrm{disc}(V) \sim t$ if $\mathrm{disc}(V) \in t(\mathbb{K}^*)^2$.

For the rest of this section we suppose that V has dimension $n \geq 1$ over $\mathbb{K} = GF(q)$, where $q = p^e,\ p \geq 3$. Thus, $\mathbb{K}^*/(\mathbb{K}^*)^2 \simeq C_2$ is cyclic of order 2. Let $\gamma \in \mathbb{K}^*$ be a fixed non-square. In any dimension, there are, up to similarity in $GL(V)$, just two distinct possibilities for the symmetric bilinear form $x \cdot y$. These may be distinguished by n and $\mathrm{disc}(V)$ ([1, III.6]).

When n is odd, one of these forms is merely γ times the other, so that the two groups are the same (up to similarity). Thus, the notation $O(n, q, 0)$ for $O(V)$ unambiguously describes the group. The possible discriminants are $(-1)^{(n-1)/2}$ and $(-1)^{(n-1)/2}\gamma \pmod{(\mathbb{K}^*)^2}$.

When n is even, the full orthogonal groups $O(n, q, \epsilon)$ for the two distinct geometries are now distinguished by the parameter $\epsilon = \pm 1$. For $\epsilon = 1$, the Witt index is $n/2$, $\mathrm{disc}(V) \sim (-1)^{n/2}$, and V is the orthogonal sum of $n/2$ hyperbolic planes. For $\epsilon = -1$, the Witt index is $(n/2) - 1$, $\mathrm{disc}(V) \sim (-1)^{n/2}\gamma$, and one of the $n/2$ hyperbolic planes is replaced by an anisotropic plane.

We also require the *spinor norm* on $O(V)$, i.e. the homomorphism

$$\begin{aligned} \theta : O(V) &\rightarrow \mathbb{K}^*/(\mathbb{K}^*)^2 \\ g &\longmapsto a_1^2 \ldots a_m^2 (\mathbb{K}^*)^2 \end{aligned}$$

which is well-defined on any factorization of $g = r_{a_1} \ldots r_{a_m}$ as the product of isometric reflections with roots $a_1, \ldots, a_m \in V$ ([1, V.5]). Note that we may assume each $a_j^2 \in \{1, \gamma\}$. Next define another homomorphism

$$\begin{aligned} \eta : O(V) &\rightarrow \{\pm 1\} \times \left(\mathbb{K}^*/(\mathbb{K}^*)^2\right) \simeq C_2 \times C_2 \\ g &\longmapsto (\det g,\ \theta(g)). \end{aligned}$$

By [1, Ths. 5.14, 5.17], $\ker \eta = \Omega(V)$, the *commutator subgroup* of $O(V)$. We must consider three other normal subgroups of $O(V)$:

$$\begin{aligned} SO(V) &:= \langle\, g \in O(V) \mid \det g = 1 \,\rangle \\ O_1(V) &:= \langle\, r_a \mid \ a^2 = 1 \,\rangle \\ O_2(V) &:= \langle\, r_a \mid \ a^2 = \gamma \,\rangle . \end{aligned}$$

In fact, $O_1(V)$, $O_2(V)$ are the subgroups generated by the two distinct conjugacy classes of reflections in $O(V)$.

Proposition 3.1 *Let $O(V)$ be the full orthogonal group for the non-singular space V of dimension $n \geq 3$, excluding the cases $O(3,3,0)$ and $O(4,3,+1)$. Then $\Omega(V) = O_1(V) \cap O_2(V)$; and $O_1(V), O_2(V), SO(V)$ correspond under the epimorphism η to the subgroups of $C_2 \times C_2$ generated by $(-1, (\mathbb{K}^*)^2)$, $(-1, \gamma(\mathbb{K}^*)^2)$ and $(1, \gamma(\mathbb{K}^*)^2)$, respectively.*

Proof. Since $\Omega(V)$ is generated by all commutators $[r_a, r_b] = (r_a r_b)^2$ of reflections, it suffices to show that all $(r_a r_b)^2 \in O_j(V)$ [1, p. 134]. But V is non-singular, so that a, b lie in a non-singular subspace W of dimension 3. (Use [1, Th. 3.8] to verify this when a, b themselves span a singular plane.) Now since W is clearly invariant under r_a and r_b, we may assume without loss of generality that $\dim V = 3$. Because V must contain isotropic vectors, it follows from [1, Th. 5.20] that $\Omega(V) \simeq PSL_2(q)$, which is simple when $q > 3$. But $O_j(V) \cap \Omega(V) \lhd \Omega(V)$. If the intersection were trivial, we would have $r_m r_n = r_n r_m$ for all roots m, n in one norm class. This is false for $q > 3$. Consequently, $O_j(V) \cap \Omega(V) = \Omega(V)$, so that $\Omega(V) \subseteq O_1(V) \cap O_2(V)$. Likewise, even if $q = 3$, we can similarly appeal to [1, Th. 5.21], so long as a, b always lie in a subspace W with $\dim(W) = 4$, $\mathrm{disc}(W) \sim \gamma$ (i.e. with Witt index 1). Again using [1, Th. 3.8], we find that this is the case whenever $n \geq 5$. Once more not all r_m, r_n commute, because W contains an anisotropic plane with non-abelian orthogonal group. Since $\Omega(V)$ has index 2 in $SO(V)$ [1, Th. 5.18], the rest of the theorem follows at once. Note that $C_2 \times C_2$ has three subgroups of index 2. □

Remarks. Actually, the proposition also holds when $n = 2$, by explicit calculation. The excluded cases for $n = 3, 4$ are genuine exceptions; see the remarks after Theorem 3.1.

Naturally, we denote the corresponding subgroups of $O(n, q, \epsilon)$ by $O_j(n, q, \epsilon)$, again with $\epsilon = 0$ when n is odd. For odd $n \geq 3$, the groups $O_1(n, q, 0)$ and $O_2(n, q, 0)$ are definitely non-isomorphic, since only one has non-trivial centre. To see this, note that the central isometry $-e$ must lie in exactly one of these two groups by Proposition 3.1. In fact, since $-e$ is the product of any n reflections with mutually orthogonal roots, we have $\theta(-e) = \mathrm{disc}(V)(\mathbb{K}^*)^2$. Consequently, $-e \in O_1(n, q, 0)$ if and only if $\mathrm{disc}(V) \sim 1$. Indeed, this condition almost always characterizes the cases in which $O_1(n, q, 0)$ has non-trivial centre. For suppose that z is a central isometry in $O_j(V)$, and consider the action of z on $M := \{m \in V \mid m \cdot m = \mu\}$, where $\mu = 1, \gamma$ for $j = 1, 2$ respectively. Since $r_{z(m)} = z r_m z^{-1} = r_m$, we have $z(m) = \epsilon_m m$ where $\epsilon_m \in \{1, -1\}$, for all $m \in M$. If $m_1, m_2 \in M$ are independent, they span a plane containing at least one $m_3 \in M$ such that m_1, m_2, m_3 are pairwise independent. (As in the proof of Proposition 3.1, we must again assume here that $q > 3$ when $n = 3$.) Since at least two of $m_1 \cdot m_2$, $m_1 \cdot m_3$, $m_2 \cdot m_3$ are non-zero, we have $\epsilon_{m_1} = \epsilon_{m_2} = \epsilon_{m_3}$. Since M spans V, we conclude that $z = \pm e$. Thus for odd $n \geq 3$, $O_1(V)$ and $O_2(V)$ are non-isomorphic. (For $O_j(3, 3, 0)$, see the remarks after Theorem 3.1.)

For even $n \geq 2$ it is possible to show in all cases that $O_1(n, q, \epsilon)$ and $O_2(n, q, \epsilon)$ are isomorphic, in fact conjugate in $GL(V)$. Therefore, we shall usually need to consider just one of the two groups, typically $O_1(n, q, \epsilon)$. (The key here is to investigate what happens when $n = 2$. It is also useful to note that $O(2, q, \epsilon)$ is dihedral.)

The notations $O(n, q, \epsilon)$ and $O_j(n, q, \epsilon)$, where $\epsilon \in \{0, +1, -1\}$ and $\epsilon = 0$ if and only if n is odd, are precise enough to cover all groups of 'orthogonal type' considered here.

We are now able to describe the classification of the finite, irreducible reflection groups. This problem has a long history, culminating in a difficult paper by Zalesskiĭ and Serežkin,

[34]. (A more geometrical proof for the corresponding projective linear groups was given by Wagner in [30, 31].)

Suppose then that G is a finite, irreducible reflection group in $GL(V)$, where V has dimension $n \geq 3$ over $\mathbb{K}$; and let $\mathbb{L}$ be an algebraic closure for $\mathbb{K}$. Also suppose that G contains no non-trivial transvection. The key theorem in [34, p. 478] states that, up to conjugacy in $GL(V_{\mathbb{L}})$ (i.e. allowing extension of scalars), G must be

1. a group of orthogonal type $O(n, q, \epsilon)$ or $O_j(n, q, \epsilon)$; or
2. the reduction mod p of a finite, irreducible orthogonal or unitary group generated by reflections in characteristic 0; or
3. one of two special groups of unitary type over finite fields, namely $[EJ_3(5)]^5$ ($n = 3$, over $GF(5^2)$), or $[J_4(4)]^3$ ($n = 4$, over $GF(3^2)$); or
4. $[\widehat{A}_n]^p \simeq S_{n+2}$, when $p \mid (n+2)$.

Concerning the last case, recall that the usual permutation action of S_{m+1} on $\mathbb{K}^{m+1}$ leaves invariant a subspace V of dimension m, in which S_{m+1} is usually represented faithfully and irreducibly as the group A_m. However, if $p \mid (m+1)$, V itself has a 1-dimensional invariant subspace, and from the resulting quotient we obtain the irreducible and faithful representation $[\widehat{A}_{m-1}]^p$ of degree $m-1$ for S_{m+1}. For similar reasons, $[E_6]^3$ is not irreducible, and so we obtain a faithful representation $[\widehat{E}_5]^3$ of degree 5 for the group E_6. (Note that the subscripts in these examples do correctly indicate the degree of an irreducible representation.)

An indication of the depth of this classification can be seen in many examples in §4. If G is an infinite, irreducible linear Coxeter group (Lemma 3.2), then G^p can take no 'middle ground': it must either (rarely) be some finite Coxeter group, or (usually) must jump in size to some orthogonal group $O(n, q, \epsilon)$ or $O_j(n, q, \epsilon)$. This is remarkable, given the relatively small number of generators.

For our purposes below, we may restrict our considerations to a more manageable subclass of these groups described in the next theorem; see also the remarks that follow.

Theorem 3.1 *Suppose $G \subseteq GL(V)$ is a finite irreducible group generated by reflections $r_0, \ldots, r_{n-1}$, where V has dimension $n \geq 3$ over the finite field $\mathbb{K} = GL(q)$, of characteristic $p > 2$. Also suppose that G leaves invariant some non-zero bilinear form. Then, up to conjugacy in $GL(V_{\mathbb{L}})$, the group G is either*

(a) an orthogonal group $O(n, q, \epsilon)$ or $O_j(n, q, \epsilon)$, excluding the cases $O_1(3, 3, 0)$, $O_2(3, 5, 0)$, $O_2(5, 3, 0)$ (assuming for these three that disc$(V) \sim 1$), and also excluding the case $O_j(4, 3, -1)$; or

(b) the reduction mod p of one of the finite linear Coxeter groups generated by reflections in characteristic 0, namely the groups of type A_n, B_n, D_n, E_6 ($p \neq 3$), E_7, E_8, F_4, H_3 or H_4.

Proof. Since G is an irreducible reflection group, any non-zero invariant bilinear form $x \cdot y$ is necessarily symmetric and non-singular [2, chap.v, §2, prop.1]. Thus, by Lemma 3.1(e), G contains no non-trivial transvection, so that we may apply the main classification theorem.

First of all, our insistence that G be generated by $n = \dim(V)$ reflections immediately rules out the cases $G = [\widehat{A}_n]^p$ (when $p \mid (n+2)$), $O_j(4,3,-1) \simeq [\widehat{A}_4]^3$, $O_2(3,5,0) \simeq [\widehat{A}_3]^5$ and $O_2(5,3,0) \simeq [\widehat{E}_5]^3$. In each of these cases, $n+1$ reflections are required to generate the group ([34, 0.8]). Also, $O_1(3,3,0)$ is not irreducible.

It remains to rule out certain groups of unitary type. The group $G = J_3(5)$ $(= [1\,1\,1^5]^4)$ of order 2160 and acting on unitary space $\mathbb{C}^3$ is typical. Following [5, p. 406] or [24, p. 331, Table 9D1], we recall that G is generated by reflections r_0, r_1, r_2 whose roots are the standard basis vectors e_0, e_1, e_2, for which the underlying Hermitian form has Gram matrix

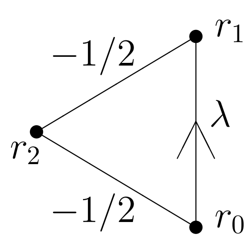
$$B = [b_{ij}] = \begin{bmatrix} 1 & \lambda & -1/2 \\ \bar{\lambda} & 1 & -1/2 \\ -1/2 & -1/2 & 1 \end{bmatrix}$$

where

$$\lambda = -\cos(\frac{\pi}{5})\, e^{2\pi i/3} = \frac{-\tau\omega}{2} \ ,$$

with $\tau = (1+\sqrt{5})/2$ and $\omega = (-1+i\sqrt{3})/2$.

Following [5, §4], we next encode this data in the *root diagram*



Now let us reduce $G \bmod p$, and suppose that G^p leaves invariant a symmetric bilinear form $x \cdot y$. Since, of course, G also leaves B invariant, we find, for all i, j, k that

$$e_i \cdot e_j = r_k(e_i) \cdot r_k(e_j) = (e_i - 2b_{ki}e_k) \cdot (e_j - 2b_{kj}e_k) \ .$$

Thus, since 2 is invertible, we have

$$b_{ki}e_k \cdot e_j + b_{kj}e_i \cdot e_k = b_{ki}b_{kj}e_k \cdot e_k \ .$$

Using this condition and the fact that the diagram has a spanning tree with real, invertible labels, we eventually find that either $x \cdot y$ is identically 0, or $\lambda \equiv \bar{\lambda} \pmod{p}$ (even allowing extension of scalars). In the first case, G^p is excluded by hypothesis, whereas in the second case, we must have $p = 3$. Indeed, when $p = 3$, B reduces to a symmetric matrix and G^3 preserves both a symmetric and Hermitian form. In fact, $[J_3(5)]^3 \simeq O_1(3, 3^2, 0)$, of order $2160/3 = 720$. (Since $e_j^2 = 1$, each r_j has square spinor norm.) Similar considerations apply to the groups $B_n(2k)$ $(k \geq 2)$, $D_n(k)$ $(k \geq 3)$, $J_3(4)$, N_4, EN_4, K_5, and K_6, as well as to

$[EJ_3(5)]^5$, which has $[J_3(5)]^5$ as a subgroup for $p = 5$ only, and to $[J_4(4)]^3$, which for $p = 3$ extends $[J_3(4)]^3$ in a natural way. □

Remarks on Theorem 3.1 and Table 1.

We summarize some useful data for the various cases in Table 1. For certain groups G, there are restrictions on the characteristic p or on the (minimal) order q of the ground field $\mathbb{K}$. We also indicate the order $|Z(G)|$ of the centre; $d(G)$, the maximum order $|rr'|$ of a product of two reflections $r, r' \in G$; and $k(G)$, the number of conjugacy classes of reflections in G (see [34, pp. 478-481]). In describing the orders of the groups of orthogonal type, we employ

$$\Phi(n, q, 0) := q^{(n-1)^2/4} \prod_{j=1}^{(n-1)/2} (q^{2j} - 1), \quad \text{for odd } n$$

$$\Phi(n, q, \epsilon) := q^{n(n-2)/4} (q^{n/2} - \epsilon) \prod_{j=1}^{(n-2)/2} (q^{2j} - 1), \quad \text{for even } n$$

([1, III. 6] and Proposition 3.1).

Finally, note some coincidences and exclusions in the tables:

1. $O(3, 3, 0) \simeq [B_3]^3$, the symmetry group of the ordinary cube, and $|\Omega(3, 3, 0)| = 12$. Assuming $\mathrm{disc}(V) \sim 1$, we have $O_2(3, 3, 0) \simeq [A_3]^3 \simeq S_4$, whereas $O_1(3, 3, 0) \simeq C_2 \times C_2 \times C_2$ is not irreducible.
2. Assuming $\mathrm{disc}(V) \sim 1$, we find that $O_1(3, 5, 0) \simeq [H_3]^5$, whereas $O_2(3, 5, 0) \simeq [\widehat{A}_3]^5 \simeq S_5$. Likewise, $O_2(5, 3, 0) \simeq [\widehat{E}_5]^3$. Complementary exclusions hold when $\mathrm{disc}(V) \sim \gamma$.
3. $O_1(4, 3, -1) \simeq O_2(4, 3, -1) \simeq [\widehat{A}_4]^3 \simeq S_6$.
4. In the full orthogonal group $O(4, 3, +1) \simeq [F_4]^3$, the subgroups

   $$O_1(4, 3, +1) \simeq O_2(4, 3, +1) \simeq [D_4]^3$$

   have index 6.
5. $O_1(4, 5, +1) \simeq [H_4]^5$.

G	$\lvert G\rvert$	$\lvert Z(G)\rvert$	$d(G)$	$k(G)$
$(n \geq 3)$				
$O(n,q,0),\ n$ odd	$2\Phi(n,q,0)$	2	$q+1$	2
$O_1(n,q,0),\ n$ odd (see remarks)	$\Phi(n,q,0)$	1 *or* 2	see [34, p.480]	1
$O_2(n,q,0),\ n$ odd (see remarks)	$\Phi(n,q,0)$	2 *or* 1	see [34, p.480]	1
$O(n,q,\epsilon),\ n$ even, $\epsilon = \pm 1$	$2\Phi(n,q,\epsilon)$	2	$q+1$	2
$O_j(n,q,\epsilon),\ n$ even, $\epsilon = \pm 1$ (assume $q > 3$ for $n = 4$)	$\Phi(n,q,\epsilon)$	1 or 2	see [34, p.480]	1
$[A_n]^p,\ p \nmid (n+1)$	$(n+1)!$	1	3	1
$[B_n]^p$	$2^n n!$	2	4	2
$[D_n]^p$	$2^{n-1} n!$	$\gcd(n,2)$	3	1
$[E_6]^p,\ n=6,\ p \neq 3$	51840	1	3	1
$[E_7]^p,\ n=7$	$2^{10}\, 3^4\, 5\, 7$	2	3	1
$[E_8]^p,\ n=8$	$2^{14}\, 3^5\, 5^2\, 7$	2	3	1
$[F_4]^p,\ n=4$	1152	2	4	2
$[H_3]^p,\ n=3$	120	2	5	1
$[H_4]^p,\ n=4$	14400	2	5	1

Table 1: The Finite, Irreducible Reflection Groups in Theorem 3.1.

4 Crystallographic Coxeter Groups and Their Modular Reductions

We return now to the standard representation R of the Coxeter group Γ in the real vector space V, with basis $a_0, \ldots, a_{n-1}$ and equipped with the symmetric bilinear form $x \cdot y$ defined in (6). We shall say that Γ is *crystallographic* (with respect to the standard representation) if the corresponding linear Coxeter group $G := R(\Gamma)$ leaves invariant some *lattice* Λ in V. (By 'lattice' we mean here the $\mathbb{Z}$-module spanned by some basis of V.) Naturally, G is also said to be crystallographic.

Now let G once more be any Coxeter group. Following [17, §1] we say that a set $\beta = \{t_i a_i\}$ of positive multiples of the a_i is a *basic system* for G if

$$m_{ij} := -t_i^{-1}(a_i \cdot a_j)t_j \in \mathbb{Z}, \quad 0 \leq i,j \leq n-1. \tag{8}$$

Notice that $M := [m_{ij}]$ is a Cartan matrix for G, with respect to the new basis β. In particular, $m_{ii} = -2$ and $m_{ij}t_i^2 = m_{ji}t_j^2$ for all i,j; and $m_{ij} = 0$, if $p_{ij} = 2$. Furthermore, for the rescaled roots $b_i := t_i a_i$, we immediately see that

$$r_i(b_j) = b_j + m_{ij} b_i \tag{9}$$

so that the corresponding *root lattice* $Q(\beta) := \oplus_j \mathbb{Z} b_j$ actually is G-invariant. In fact, the converse holds and the crystallographic condition can even be described purely in terms of the presentation (1).

Proposition 4.1 *The following are equivalent for the standard linear Coxeter group G.*

(a) G is crystallographic.

(b) There exists a basic system β for G.

(c) For all $i \neq j$, $p_{ij} \in \{2, 3, 4, 6, \infty\}$; and in every circuit in the Coxeter diagram $\Delta_c(G)$, the number of branches marked 4 and the number marked 6 are even.

Proof. See [17, §1] and [2, chap.v, §4, exer.6] or [25, pp. 104-105]. In fact, we shall verify part of (b) $\Rightarrow$ (c) below. □

Remarks: G may admit many essentially distinct invariant lattices. However, when the form $x \cdot y$ on V is non-singular, and in particular when G is finite, all G–invariant lattices can be classified in a natural way ([3, 16, 17]).

Suppose now that β is a basic system for the crystallographic Coxeter group G, and for any $i \neq j$, consider the dihedral subgroup $\langle r_i, r_j \rangle$. By (8) and (6), we conclude that

$$4 \cos^2 \frac{\pi}{p_{ij}} = m_{ij} m_{ji}$$

is an integer, namely $0, 1, 2, 3$ or 4, so that $p_{ij} = 2, 3, 4, 6$ or ∞, respectively. Define the ratio $k_{ij} := t_j^2 / t_i^2$. If $p_{ij} = 2$, then $m_{ij} = m_{ji} = 0$ and k_{ij} is indeterminate. Otherwise, we may suppose that $m_{ij} \geq m_{ji} \geq 1$, whence $1 \leq m_{ij}, m_{ji} \leq 4$, so that $k_{ij} = m_{ij}/m_{ji} = 1, 2, 3, 4(\text{ or } 1)$ for $p_{ij} = 3, 4, 6$ or ∞, respectively.

Following [7, p. 415], we shall conveniently represent the various possible basic systems $\{t_i a_i\}$ for a given crystallographic group G by a new diagram $\Delta(G)$ (a variant of the Coxeter diagram): for $0 \leq i, j \leq n-1$, node i is labelled $2t_i^2$; and distinct nodes $i \neq j$ are joined by

$$\lambda_{ij} := \min\{m_{ij}, m_{ji}\}$$

unlabelled branches. (Note that $\lambda_{ij} = \lambda_{ji} = 0, 1$ or 2. Thus the underlying graph is essentially that of $\Delta_c(G)$, except that a mark $p_{ij} = \infty$ is indicated by a *doubled* branch in the case that $m_{ij} = m_{ji} = 2$.) In Table 2 we display the possible subdiagrams corresponding to the dihedral subgroups $\langle r_i, r_j \rangle$. For simplicity we have replaced the node labels $2t_i^2, 2t_j^2$ by s, t or s, ks, $(k = 1, 2, 3, 4)$ as appropriate. We also list the associated binary quadratic forms, as described below.

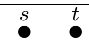
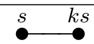
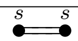
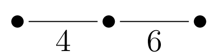
Nodes i, j	Parameters	λ_{ij}	The binary quadratic form
	$p_{ij} = 2$	0	$sx_i^2 + tx_j^2$
	$p_{ij} = 3, 4, 6, \infty$ $(k = 1, 2, 3, 4)$	1	$s(x_i^2 - kx_ix_j + kx_j^2)$
	$p_{ij} = \infty$ $(k = 1)$	2	$s(x_i - x_j)^2$

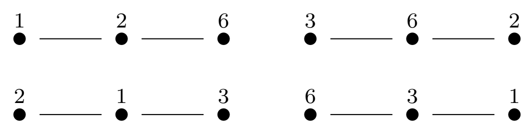
Table 2: Basic Systems for the Dihedral Groups $\langle r_i, r_j\rangle$.

Clearly it is the *ratio* of labels on adjacent nodes that matters here; and given any acceptable choice for such ratios, the node labels are determined *up to scale* on each connected component of $\Delta(G)$. In fact, we may take the labels on any particular connected component to be a set of relatively prime positive integers. Consequently, if $\Delta_c(G)$ is connected, there are, up to similarity, only finitely many different basic systems for G.

For example, the group G with Coxeter diagram



is crystallographic and acts naturally on $\mathbb{H}^2$. Now $k_{01} = 2^{\pm 1}$ and $k_{12} = 3^{\pm 1}$, so that by suitably adjusting the t_i, any basic system for G is described (up to scale) by one of the following diagrams:



Notice that the Gram matrix $B = [b_{ij}] := [b_i \cdot b_j]$ is easily computed from the diagram, since $b_{ii} = 2t_i^2$ is simply the label attached to node i, and

$$b_{ij} = \frac{-\lambda_{ij}}{2} \max\{b_{ii}, b_{jj}\} \quad (i \neq j). \tag{10}$$

(It is useful to note also that $b_{ij} = -m_{ij}t_i^2 = -m_{ji}t_j^2$, so that $m_{ij} = -2b_{ij}/b_{ii}$.)

The diagram just as well describes the associated quadratic form $f(x) := x \cdot x$. Indeed, computing with respect to the basis β we obtain

$$\begin{aligned} f(x) &= (x_0b_0 + \cdots + x_{n-1}b_{n-1})^2 \\ &= \sum_i b_{ii}x_i^2 - \sum_{i<j} \lambda_{ij} \max\{b_{ii}, b_{jj}\} x_ix_j \ . \end{aligned} \tag{11}$$

Thus, if all $b_{ii} \in \mathbb{Z}$, as we can always assume here, we conclude that f is an *integral quadratic form*. (Such forms are of particular interest in the cases that G acts on $\mathbb{E}^{n-1}$, $\mathbb{S}^{n-1}$ or $\mathbb{H}^{n-1}$, in such a way that the fundamental region is a simplex of finite volume; see [7] and [25], where the full *unit groups* of such forms are determined.) Next to each diagram in Table 2 we have for convenience also indicated the corresponding *binary quadratic form*

$$(x_ib_i + x_jb_j)^2 \ .$$

The computation of disc$(V) = \det(B)$ is simplified if $\Delta(G)$ has a univalent node j, say adjacent to node k. If $B_{[j]}$ (resp. $B_{[j,k]}$) denotes the submatrix of B obtained by deleting row and column j (resp. j, k), then

$$\det(B) = b_{jj} \det(B_{[j]}) - b_{jk}^2 \det(B_{[j,k]}). \tag{12}$$

(Expand along row j [7, p.426].)

For example, the diagram $\overset{6}{\bullet} — \overset{3}{\bullet} — \overset{1}{\bullet}$ from above has Gram matrix

$$B = \begin{bmatrix} 6 & -3 & 0 \\ -3 & 3 & -3/2 \\ 0 & -3/2 & 1 \end{bmatrix}$$

and associated quadratic form

$$f = 6x_0^2 - 6x_0x_1 + 3x_1^2 - 3x_1x_2 + x_2^2 \ .$$

Taking $j = 0, k = 1$, we note that $\det(B_{[0]}) = 3(1) - (-\frac{3}{2})^2 = \frac{3}{4}$, so that

$$\det(B) = 6(\frac{3}{4}) - (-3)^2(1) = -\frac{9}{2} \ . \tag{13}$$

We now focus our investigations by henceforth assuming that Γ is a crystallographic Coxeter group for which the diagram $\Delta_c(\Gamma)$ is a string with branch labels

$$p_j := p_{j-1,j} \in \{3, 4, 6, \infty\} \ .$$

Furthermore, we may now unambiguously denote Γ by $[p_1, \ldots, p_{n-1}]$, a reminder that Γ is the automorphism group of the universal regular polytope $\mathcal{P} = \{p_1, \ldots, p_{n-1}\}$ (see [24, §3D]).

Since $\Delta_c(\Gamma)$ is connected, the corresponding geometric group $G \simeq \Gamma$ has to scale only finitely many basic systems β. Any such system, as well as the corresponding Gram matrix B, is represented by an essentially unique diagram $\Delta(G)$, in which node labels form a set of relatively prime positive integers (cf. the group $G = [4, 6]$ described above).

Since the group G is crystallographic, it is represented by *integral* matrices with respect to the root basis β. In particular, using (10) we have

$$\begin{aligned} r_i(b_i) &= -b_i \\ r_i(b_j) &= b_j + \lambda_{ij} \max\{1, b_{jj}/b_{ii}\} b_i \ , \quad (i \neq j) \end{aligned} \tag{14}$$

and so easily obtain the matrix for r_i from the diagram.

Before proceeding, we first consider how G might depend on the choice between two basic systems β, β'. By our earlier observations, we can convert from $\Delta(G)$ to $\Delta'(G)$ by consecutively inverting the ratios of the labels on various pairs of adjacent nodes. If nodes i, j are joined by a single branch, then the effect on the corresponding roots may be described by

$$b_i' = k^{\epsilon} b_i \ , \quad b_j' = b_j$$

for a suitable choice of $\epsilon = \pm 1$, and where $k = 1, 2, 3, 4$ for $p_{ij} = 3, 4, 6, \infty$, respectively (cf. Table 2). Likewise, when $p_{ij} = \infty$, a similar transformation, with $k = 2$, effectively doubles a single branch connecting the corresponding nodes (and balances their labels), or converts a double branch into a single branch (with ratio 4). Following these adjustments on pairs of nodes, we may finally have to rescale the entire set of labels. In the end, however, we conclude that the new Gram matrix

$$B' = \delta(DBD)$$

for some diagonal matrix D whose diagonal entries, like the scale factor δ, are rational numbers of the form $2^x 3^y$, for $x, y \in \mathbb{Z}$.

Now fix an odd prime p. As described in §3, we may reduce $G \bmod p$. The natural epimorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ induces a homomorphism of G onto a subgroup G^p of $GL_n(\mathbb{Z}_p)$, the group of invertible $n \times n$ matrices over $\mathbb{Z}_p$. Notice that the homomorphic image of r_i is still a reflection, since $p \neq 2$; in fact, r_i has a 1-dimensional direction space and is involutory. We shall conveniently abuse notation by letting r_i, $B = [b_{ij}]$, f refer as well to their modular images. Similarly, $\{b_i\}$ will denote the usual basis for $\mathbb{Z}_p^n$, the space of column vectors over $\mathbb{Z}_p$. Thus, from this point of view,

$$G^p = \langle r_0, \ldots, r_{n-1} \rangle$$

is a subgroup of the orthogonal group $O(\mathbb{Z}_p^n)$ of isometries for the symmetric bilinear form $x \cdot y$, defined on $\mathbb{Z}_p^n$ by means of the Gram matrix B. (It may be that $x \cdot y$ is singular.)

We note that when $p \geq 5$, a change in the underlying basic system has the effect of merely conjugating G^p inside $GL_n(\mathbb{Z}_p)$ (by a diagonal matrix D). In fact, the matrices representing the elements of G^p in the two bases are similar (under D). Likewise, the corresponding quadratic form f can change in only an inessential way (cf. [1, p. 144]). The same conclusions hold when $p = 3$, so long as no branch of $\Delta_c(\Gamma)$ is labelled '6' (no factor 3^y occurs in this case). However, we will find that the remaining cases are less predictable.

Remark. The above observations hold for a crystallographic Coxeter group with any sort of connected diagram.

Our goal now is to assess when G^p is a string C-group, so that we must determine when the intersection condition (3) is inherited from G by G^p. We begin with some observations about the geometric action of the standard subgroups of G or G^p. For any $J \subseteq \{0, \ldots, n-1\}$, we let $G_J := \langle r_j \,|\, j \notin J \rangle$; in particular, for $k, l \in \{0, \ldots n-1\}$ we let $G_k := \langle r_j \,|\, j \neq k \rangle$ and $G_{k,l} := \langle r_j \,|\, j \neq k, l \rangle$. Similarly, $G_J^p, G_k^p, G_{k,l}^p$ will denote the images in G^p of these subgroups of G. We also let V_J be the subspace of $\mathbb{Z}_p^n$ spanned by $\{b_j \,:\, j \notin J\}$, and similarly for $V_k, V_{k,l}$.

For $g \in G_J^p$ and $0 \leq k \leq n-1$, it follows at once from (14) that

$$g(b_k) = b_k + \sum_{j \notin J} x_j b_j \; . \tag{15}$$

From this observation we easily obtain

Lemma 4.1 *Let $J \subseteq \{0, \ldots, n-1\}$. Then*

(a) V_J is a G^p_J – invariant subspace of dimension $n - |J|$ in $\mathbb{Z}_p^n$; and the action of G^p_J on this subspace can be reconstructed from the subdiagram of $\Delta(G)$ induced on the node set complementary to J.

(b) $r_k \in G^p_J$ implies $k \notin J$.

It is worth noting here that it is quite possible for a subspace V_J, which is non-singular in characteristic 0, to become singular under reduction mod p. At one extreme, we may have $\mathrm{disc}(V) \equiv 0 \pmod p$. At the other, it may happen that certain b_j become isotropic. Actually, in our setup, the latter degeneracy occurs only when $p = 3$ and some $r_{j-1}r_j$ has period 6; and in all such cases it must be that $\mathrm{disc}(V) \equiv 0 \pmod 3$.

Although the situation for higher ranks is complicated, we can now say a few general things about the intersection condition.

Theorem 4.1 *Let $G = \langle r_0, \ldots, r_{n-1} \rangle$ be a crystallographic linear Coxeter group with string diagram, and suppose the prime $p \geq 3$. Suppose that G^p_0 and G^p_{n-1} are string C-groups, and that the subspace $V_{0,n-1}$ is non-singular (i.e. $\det(B_{[0,n-1]}) \not\equiv 0 \bmod p$). Then if $G^p_{0,n-1}$ is the full orthogonal group $O(n-2, p, \epsilon)$ on $V_{0,n-1}$, G^p must be a string C-group.*

Proof. Let $g \in G^p_0 \cap G^p_{n-1}$. By Lemma 4.1(a), g induces an isometry on the non-singular subspace $V_{0,n-1}$. By hypothesis, the subgroup $G^p_{0,n-1}$ of G^p_0 (or G^p_{n-1}) is large enough that there must exist $\tilde{g} \in G^p_{0,n-1}$ such that $g, \tilde{g}$ have the same action on $V_{0,n-1}$. Thus, since our goal is to show that $G^p_0 \cap G^p_{n-1} \subseteq G^p_{0,n-1}$, we may assume without loss of generality that g acts as the identity e on $V_{0,n-1}$. But by (15), $g(b_0) = b_0 + u$, $g(b_{n-1}) = b_{n-1} + v$, for $u, v \in V_{0,n-1}$. For arbitrary $w \in V_{0,n-1}$ we now have

$$b_0 \cdot w = g(b_0) \cdot g(w) = (b_0 + u) \cdot w = b_0 \cdot w + u \cdot w \ ,$$

so that $u \cdot w = 0$, and so $u = o$. Thus $g(b_0) = b_0$; similarly $g(b_{n-1}) = b_{n-1}$. Hence $g = e$, and $G^p_0 \cap G^p_{n-1} = G^p_{0,n-1}$. □

The proof of the next result is greatly simplified by exploiting the contragredient action of G on the dual space $\check{V}$, working for now in characteristic 0. Thus, if $\{\mu_i\}$ is the basis of $\check{V}$ dual to $\{b_i\}$, then from (9) we find that

$$r_i(\mu_j) = \mu_j, \quad \text{if } i \neq j, \tag{16}$$

$$r_i(\mu_i) = m_{i,i-1}\mu_{i-1} - \mu_i + m_{i,i+1}\mu_{i+1} \ ,$$

(taking $m_{0,-1} = m_{n-1,n} = 0$). Note that the dual lattice $\oplus_j \mathbb{Z}\mu_j$ is G-invariant. Moreover, it is well known [14, Th. 5.13(a)] that

$$\mathrm{Stab}_G(\mu_0) = G_0 \ . \tag{17}$$

Thus, when G is of spherical type and is therefore some finite Coxeter group $[p_1, \ldots, p_{n-1}]$, the G-orbit of μ_0 has size $[G : G_0]$. Furthermore, in this case the Euclidean space V is naturally isomorphic to $\check{V}$, so that we may identify μ_0 with a point $w \in V$ satisfying $w \cdot b_j = 0$, for $1 \leq j \leq n-1$. We may thus view μ_0 (or w) as the base vertex in the universal regular polytope $\{p_1, \ldots, p_{n-1}\}$, as realized by Wythoff's construction; see [24, 3D6, 3D7].

Clearly, the essentials of this description survive reduction mod p, and again we may abuse notation in an obvious way. In particular, we may think of $\{\mu_j\}$ as the usual basis for the space $\check{\mathbb{Z}}_p^n$ of row vectors over $\mathbb{Z}_p$. Each r_i, being an involution, is represented by the same matrix as before, now acting on $\check{\mathbb{Z}}_p^n$ by right multiplication.

Theorem 4.2 *Let $G = \langle r_0, \ldots, r_{n-1}\rangle$ be a crystallographic linear Coxeter group with string diagram, and suppose the prime $p \geq 3$. If G_{n-1} is of spherical type and G_0^p is a string C-group, or (dually) if G_0 is of spherical type and G_{n-1}^p is a string C-group, then G^p is a string C-group.*

Proof. We need only consider the case that G_{n-1} is of spherical type. In fact, it is then true that $G_{n-1}^p \simeq G_{n-1}$ (see Theorem 5.1 and the discussion in §6). Thus, by Proposition 2.1(a), it suffices to show that $G_0^p \cap G_{n-1}^p = G_{0,n-1}^p$. Next observe that

$$G_{0,n-1} \simeq G_{0,n-1}^p \subseteq G_0^p \cap G_{n-1}^p \subseteq G_{n-1}^p \simeq G_{n-1} .$$

Since $G_0^p \cap G_{n-1}^p$ stabilizes μ_0 by (16), we are done if we can show that the orbit of μ_0 under the action of G_{n-1}^p has the same size in characteristic p as in characteristic 0. But this straightforward calculation with row vectors is easy for groups (of spherical type) having rank $n \leq 3$ (cf. the proof of Theorem 5.1(a)), and for $n \geq 4$ is briefly described in §6. (A subtle concern in this argument is the distinction between G_{n-1}, a linear group of degree n, and the (isomorphic) linear group of degree $n-1$, defined directly from the subdiagram on nodes $\{0, \ldots, n-2\}$ in $\Delta(G)$; but this worry may be handled much as in the proof of [14, Th. 5.5].) □

Remark. The conditions in Theorems 4.1 and 4.2 can often be quickly established with the help of the diagram $\Delta(G)$, in tandem with Theorem 3.1. In part II of this work, we use several refinements of the above ideas to tackle large classes of examples of higher rank.

5 Modular Polytopes of Low Rank

In this section, we completely describe the groups G^p with rank $n \leq 3$. We maintain our standing assumption that G is isomorphic to the crystallographic Coxeter group Γ, whose diagram $\Delta_c(\Gamma)$ is a string with branch labels $3, 4, 6$ or ∞.

Theorem 5.1 *Suppose $p \geq 3$, and let $G = \langle r_0, \ldots, r_{n-1}\rangle$ be a crystallographic linear Coxeter group with string diagram.*

(a) Any group G^p of rank $n = 1, 2$ or 3 is a string C-group.

(b) In any group G^p of rank $n \geq 2$, each subgroup $\langle r_i, r_j\rangle$ with $i \neq j$ is dihedral of order $4, 6, 8, 12$ or $2p$.

Proof. We have already verified the case $n = 1$ with our earlier observation that each r_i has period 2 in G^p. For any two generating reflections r_i, r_j, with $i \neq j$, we conclude from Lemma 4.1(b) that $\langle r_i, r_j \rangle$ is indeed a dihedral group, and hence a string C-group, and that the period of $r_i r_j$ divides p_{ij} $(= 2, 3, 4, 6$ or $\infty)$. Since the plane spanned by $\{b_i, b_j\}$ is $\langle r_i, r_j \rangle$–invariant, a simple calculation with 2×2 matrices suffices to show that $r_i r_j$ retains the period p_{ij} in G^p, if $p_{ij} < \infty$. If $p_{ij} = \infty$, it is almost as easy to check that $r_i r_j$ has period p in G^p.

Suppose now that $n = 3$. If $p > 3$, the subspace $V_{0,2}$ spanned by b_1 in $\mathbb{Z}_p^3$ is non-singular, so that the intersection property follows directly from Theorem 4.1. Even when $p = 3$, there can be doubt only in cases with $p_{01} = 6$ or $p_{12} = 6$. But all such groups are covered by Theorem 4.2. □

Whenever G^p is, in fact, a string C-group, we shall call the corresponding polytope $\mathcal{P} = \mathcal{P}(G^p)$ a *modular polytope*. (The *dual* polytope $\mathcal{P}^*$ results from listing the specified generators of G^p in reverse order.) When $n = 1$ we obtain, of course, the unique rank 1 polytope $\{\ \}$, which is realized as a line segment; and when $n = 2$, G^p is the dihedral symmetry group of the polygon $\{q\}$, where in our cases we have $q \in \{2, 3, 4, 6, p\}$.

Let us now consider the rank 3 cases in some detail. If some branch of the underlying Coxeter diagram is labelled 6 or is labelled ∞, when $p > 5$, then the maximum rotation order $d(G^p) \geq 6$ (by Theorem 5.1(b)). Thus, if $V = \mathbb{Z}_p^3$ is non-singular and $\Delta(G)$ is a (connected!) string, then G^p is irreducible by Lemma 3.2; and it follows from Theorem 3.1 and Table 1 that G^p must be a full group of orthogonal type $O(3, p, 0)$ or $O_j(3, p, 0)$. Using Proposition 3.1, it is then an easy matter to determine the precise group from the quadratic character of the node labels.

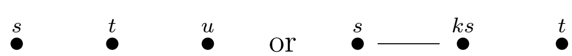
All remaining cases, in particular those in which $\text{disc}(V) \equiv 0 \pmod{p}$, are handled easily enough by inspection. For completeness, we include the rank 3 polytopes arising from disconnected diagrams.

It is useful to recall that each rank 3 Coxeter group Γ can be viewed as a 'triangle group', with a natural action on $\mathbb{S}^2$, $\mathbb{E}^2$ or $\mathbb{H}^2$. (See [25] for a description of the various cases, along with their analogues of higher rank.) The polyhedron $\mathcal{P}$ is then considered to be a regular map on some compact surface; in fact, this surface must be orientable, since $G^p = \Gamma(\mathcal{P})$ has a rotation subgroup of index 2 [10, §8.1].

A. Groups in which Γ has Spherical Type

When the Coxeter group Γ is itself finite, Γ acts naturally on the 2-sphere. It is easy to check in each case that the reduction mod p is faithful, for any prime $p \geq 3$.

5.1 The groups with diagrams



$(k = 1, 2, 3)$

For each $p \geq 3$, the group G^p is a direct product $I_2(q) \times C_2$, where $q = 2, 3, 4$ or 6. The corresponding 3-polytope, or regular map $\mathcal{P}$, is the *dihedron* $\{q, 2\}$.

5.2 The groups with diagram

$$\overset{1}{\bullet} \text{———} \overset{1}{\bullet} \text{———} \overset{1}{\bullet}$$

For $p \geq 3$, $G^p \simeq [A_3]^p \simeq S_4$ is the automorphism group for the regular tetrahedron $\mathcal{P} = \{3, 3\}$.

5.3 The groups with diagram

$$\overset{2}{\bullet} \text{———} \overset{1}{\bullet} \text{———} \overset{1}{\bullet}$$

For $p \geq 3$, $G^p \simeq [B_3]^p \simeq S_4 \times C_2$ is the automorphism group for the ordinary cube $\mathcal{P} = \{4, 3\}$.

B. Groups in which Γ has Euclidean Type

We turn to the cases in which Γ acts naturally on the Euclidean plane, so that $\mathrm{disc}(V) = 0$ [14, Ch.4].

5.4 The groups with diagram

$$\overset{s}{\bullet} \text{———} \overset{4s}{\bullet} \qquad \overset{t}{\bullet}$$

Using Theorem 5.1(b), we easily see that for any $p \geq 3$, G^p is the direct product $I_2(p) \times C_2$, the group of the dihedron $\mathcal{P} = \{p, 2\}$.

5.5 The groups with diagram

$$\overset{1}{\bullet} \text{———} \overset{2}{\bullet} \text{———} \overset{1}{\bullet}$$

For $p \geq 3$, the 'translation' $x = r_0 r_1 r_2 r_1$ has odd period p. It follows that G^p has order $8p^2$ and must be the automorphism group of the toroidal map $\mathcal{P} = \{4, 4\}_{(p,0)}$ (see [10, §8.3]).

5.6 The groups with diagram

$$\overset{3}{\bullet} \text{———} \overset{3}{\bullet} \text{———} \overset{1}{\bullet}$$

For $p \geq 3$, the 'translation' $x = r_0 r_1 r_2 r_1 r_2 r_1$ has period p. In all cases, G^p has order $12p^2$ and is the automorphism group of the toroidal map $\mathcal{P} = \{3, 6\}_{(p,0)}$.

The diagram $\overset{1}{\bullet} \text{—} \overset{1}{\bullet} \text{—} \overset{3}{\bullet}$ yields an isomorphic group for $p \geq 5$. However, when $p = 3$, we obtain instead the automorphism group of order 36 for the toroidal map $\mathcal{P} = \{3, 6\}_{(1,1)}$.

C. Groups in which Γ has Hyperbolic Type

Up to similarity in $GL_3(\mathbb{Z}_p)$, the remaining cases are as follows. Here we note that $\Omega(3, p, 0) \simeq PSL_2(\mathbb{Z}_p)$ if V is non-singular (see [1, Th. 5.20]). Furthermore, if $p > 3$, then

$$O_1(3, p, 0) \simeq PSL_2(\mathbb{Z}_p) \rtimes C_2 \ ,$$

with a direct product occuring if and only if $\mathrm{disc}(V) \sim 1$. Moreover, $SO(3,p,0) \simeq PGL_2(\mathbb{Z}_p)$, if V is non-singular (see [1, p. 200]), so that

$$O(3,p,0) \simeq PGL_2(\mathbb{Z}_p) \rtimes C_2 \quad .$$

Note that since $PSL_2(\mathbb{Z}_p)$ is simple for $p > 3$, we cannot generally expect that the regular polyhedra constructed below have interesting (regular) proper quotients.

5.7 The groups with diagram

$$\overset{1}{\bullet} \text{——} \overset{1}{\bullet} \text{——} \overset{4}{\bullet} \qquad (\mathrm{disc}(V) = -1)$$

Here G^p is the automorphism group of a regular map of type $\{3,p\}$. For $p = 3$ we once again obtain $G^p \simeq [A_3]^p \simeq S_4$ for the polyhedron $\{3,3\}$. Since $1, 4$ are squares, we find for $p \geq 5$ that $G^p = O_1(3,p,0)$ of order $p(p^2-1)$. From our comments in §3 we conclude that the centre of G^p is non-trivial if and only if $p \equiv 1 \pmod 4$. Keeping in mind that the rotation group of $O_1(3,p,0)$ is (usually) $\Omega(3,p,0) \simeq PSL_2(\mathbb{Z}_p)$, it is easy to see that we have redescribed here the family of regular maps discussed in [21] or [22]. In particular, when $p = 5$, $G^5 = O_1(3,5,0) \simeq [H_3]^5$ is the automorphism group for the regular icosahedron $\{3,5\}$. Likewise, G^7 is the group for the Klein polyhedron $\{3,7\}_8$.

5.8 The groups with diagram

$$\overset{2}{\bullet} \text{——} \overset{1}{\bullet} \text{——} \overset{3}{\bullet} \qquad (\mathrm{disc}(V) = -3/2)$$

In this case, we obtain a mostly new family of finite regular maps of type $\{4,6\}$. For $p \geq 5$, V is non-singular, so that

$$G^p = \begin{cases} O_1(3,p,0)\ , & \text{if } p \equiv \pm 1 \pmod{24} \\ O(3,p,0)\ , & \text{otherwise.} \end{cases}$$

(Note that $2, 3$ are both squares (mod p) just when $p \equiv \pm 1 \pmod{24}$.) Thus, if either 2 or 3 is quadratic non-residue, then G^p is the full orthogonal group of order $2p(p^2-1)$, and the corresponding map has Euler characteristic $-p(p^2-1)/12$.

For $p = 5$, we have $G^5 = O(3,5,0) \simeq S_5 \times C_2$. We thus obtain in a new way the Coxeter-Petrie polyhedron $\{4,6\,|\,3\}$ [10, §8.5]. From $p = 7$ we obtain the map R15.4 of genus 15 in [6].

When $p = 3$, V is singular and G^3 is the group of $\{4,6\}_4$, the dual of the Petrial of the toroidal map $\{4,4\}_{(3,3)}$. In fact, the same group arises in another way as the reduction (mod 3) of

$$\overset{6}{\bullet} \text{——} \overset{3}{\bullet} \text{——} \overset{1}{\bullet} \qquad (\mathrm{disc}(V) = -9/2).$$

5.9 The groups with diagram

$$\overset{2}{\bullet} \text{——} \overset{1}{\bullet} \text{——} \overset{4}{\bullet} \qquad (\mathrm{disc}(V) = -4)$$

Again, this family of regular maps of type $\{4,p\}$ is mainly new. For $p \geq 3$, we have

$$G^p = \begin{cases} O_1(3,p,0)\ , & \text{if } p \equiv \pm 1 \pmod 8 \\ O(3,p,0)\ , & \text{otherwise.} \end{cases}$$

In particular, $G^3 = O(3,3,0) \simeq [B_3]^3$ is the group of the cube $\{4,3\}$; and $G^5 = O(3,5,0) \simeq S_5 \times C_2$ appears anew as the group of Gordon's map $\{4,5\}_6$ of genus 4 (see [12]). For this diagram, $p = 7$ gives the map R10.9 of [6].

5.10 The groups with diagram

$$\overset{1}{\bullet} — \overset{3}{\bullet} — \overset{1}{\bullet} \quad (\mathrm{disc}(V) = -3/2)$$

We obtain a family of regular maps of type $\{6,6\}$. For $p \geq 5$ we find that

$$G^p = \begin{cases} O_1(3,p,0)\ , & \text{if } p \equiv \pm 1 \pmod{12} \\ O(3,p,0)\ , & \text{otherwise.} \end{cases}$$

Taking $p = 5$ we obtain the map R11.5 of [6].

When $p = 3$, we find that G^3, of order 72, is the group for the Petrie dual of Sherk's map $\{6,6\}_{(1,1)}$ [28]. We obtain the same polytope from $\overset{3}{\bullet} — \overset{1}{\bullet} — \overset{3}{\bullet}$. However, $\overset{1}{\bullet} — \overset{3}{\bullet} — \overset{9}{\bullet}$ yields the automorphism group of order 216 for the Petrie dual of Sherk's map $\{6,6\}_{(3,0)}$.

5.11 The groups with diagram

$$\overset{3}{\bullet} — \overset{1}{\bullet} — \overset{4}{\bullet} \quad (\mathrm{disc}(V) = -9)$$

The maps in this case have type $\{6,p\}$. For $p \geq 5$ we again have

$$G^p = \begin{cases} O_1(3,p,0)\ , & \text{if } p \equiv \pm 1 \pmod{12} \\ O(3,p,0)\ , & \text{otherwise.} \end{cases}$$

In particular, $G^5 = O(3,5,0) \simeq S_5 \times C_2$ is now the group for the map $\{6,5\}_4$, the Petrial of $\{4,5\}_6$.

When $p = 3$ we find that G^3, of order 36, is the automorphism group for the toroidal map $\{6,3\}_{(1,1)}$. Similarly, when $p = 3$, $\overset{1}{\bullet} — \overset{3}{\bullet} — \overset{12}{\bullet}$ yields the group of order 108 for $\{6,3\}_{(3,0)}$.

5.12 The groups with diagram

$$\overset{1}{\bullet} — \overset{4}{\bullet} — \overset{1}{\bullet} \quad (\mathrm{disc}(V) = -4)$$

Finally, we have in this last case, an interesting family of self-dual maps of type $\{p,p\}$. When $p = 3$, we once more obtain $G^3 = [A_3]^3 \simeq S_4$.

For $p \geq 5$, $G^p = O_1(3,p,0)$ has order $p(p^2-1)$. In particular, G^5 now appears as the group for the map $\{5,5\,|\,3\}$, which can be metrically realized in Euclidean space as either the great dodecahedron $\{5,5/2\}$, or as its dual, the small stellated dodecahedron $\{5/2,5\}$.

6 Modular Polytopes of Spherical or Euclidean Type

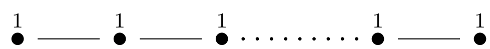
In this section, we briefly discuss the modular polytopes associated with the crystallographic string Coxeter groups G of spherical or Euclidean type. Since the groups of rank at most 3 have already been treated, we now are primarily interested in the case $n \geq 4$. We begin with the spherical groups.

A. Groups of Spherical Type

Here there are three kinds of string diagrams with $n \geq 3$ (up to duality), namely A_n, B_n and F_4. From general results we already know that $G^p \simeq G$ if $p \nmid |G|$, but we shall see that indeed this is true for all $p \geq 3$.

The corresponding modular polytopes $\mathcal{P}(G^p)$ are isomorphic to the n-simplex, n-cube or 24-cell, respectively. Moreover, we obtain a "modular representation" of $\mathcal{P}(G^p)$ in $\check{V} = \check{\mathbb{Z}}_p^n$ by applying Wythoff's construction to G^p, with the point μ_0 as initial vertex (see (16) and [24, Sect. 5A]). In particular this completes the proof of Theorem 4.2, which requires us to verify that the orbit of this point μ_0 in $\check{V}$ has the same size as in characteristic 0. When V is non-singular and hence is naturally isomorphic to $\check{V}$, we obtain an isomorphic modular representation of $\mathcal{P}(G^p)$ in V itself. Recall that the base vertex w is then determined (to scale) by the equations $w \cdot b_j = 0$ $(j = 1, \ldots, n-1)$.

6.1 The group A_n^p with diagram



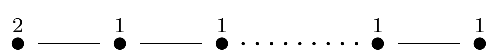
Now $G^p \simeq G \simeq S_{n+1}$, for each $n \geq 1$ and each $p \geq 3$. In fact, observe that G^p is a quotient of S_{n+1} with the same Coxeter diagram (see Theorem 5.1b), and that S_{n+1} does not have any non-trivial normal subgroups other than the alternating group if $n \geq 4$ (the case $n \leq 3$ was settled before). It follows that $\mathcal{P}(G^p)$ is isomorphic to $\{3^{n-1}\}$, the regular n-simplex. Note that $\mathrm{disc}(V) = (n+1)\, 2^{-n}$, so that V is non-singular if and only if $p \nmid (n+1)$.

For any characteristic p, the orbit of the base vertex μ_0 under G^p consists of the $n+1$ distinct points

$$\nu_k := \mu_k - \mu_{k-1} \quad (k = 0, \ldots, n),$$

taking $\mu_{-1} = \mu_n = o$, the origin in V. Then $\nu_0, \ldots, \nu_n$ are the vertices of a modular representation of the regular n-simplex in $\check{\mathbb{Z}}_p^n$.

6.2 The group B_n^p with diagram



Now $G^p \simeq G \simeq C_2^n \rtimes S_n$, for each $n \geq 2$ and each $p \geq 3$, where the semi-direct product in G^p is determined by $G_0^p \simeq S_n$ and $N_0 := \langle g r_0 g^{-1} \mid g \in G_0^p \rangle \simeq C_2^n$. The latter subgroup of G^p is generated by the reflections in V whose roots are the vectors (of squared length 2) in the orthogonal basis

$$c_0 := b_0,\ c_1 := r_1(b_0),\ c_2 := r_2 r_1(b_0),\ \ldots\ldots,\ c_{n-1} := r_{n-1} r_{n-2} \cdots r_1(b_0).$$

Note that

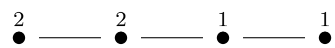
$$c_j = b_0 + 2(b_1 + b_2 + \ldots + b_j) \qquad (j = 0, \ldots, n-1).$$

In particular, G_0^p permutes the vectors $c_0, \ldots, c_{n-1}$ like an S_n, whereas N_0 takes each c_j to $\pm c_j$. The corresponding polytope $\mathcal{P}(G^p)$ is isomorphic to the n-cube $\{4, 3^{n-2}\}$.

Then the initial point, being invariant under G_0^p, is given by $w := c_0 + c_1 + \ldots + c_{n-1}$. Its orbit consists of the 2^n vertices $\pm c_0 \pm c_1 \pm \ldots \pm c_{n-1}$ of a modular representation of the n-cube in (the non-singular space) $\mathbb{Z}_p^n$. Similarly, by switching to the base vertex c_{n-1}, we obtain a modular representation of the (dual) crosspolytope, whose $2n$ vertices are the points $\pm c_j$, $(0 \leq j \leq n-1)$. We do not actually need to work in the space $\check{V}$ here, and merely note that the basis $\{\nu_j\}$ dual to $\{c_j\}$ is given by

$$\begin{aligned}
\nu_0 &= \mu_0 - \frac{1}{2}\mu_1 \\
\nu_j &= \frac{1}{2}(\mu_j - \mu_{j+1}), \quad (1 \leq j \leq n-2) \\
\nu_{n-1} &= \frac{1}{2}\mu_{n-1} \, .
\end{aligned}$$

6.3 The group F_4^p with diagram



Now we have $F_4^p \simeq F_4$, for each $p \geq 3$. In fact, consider the subgroup B of $G^p = \langle r_0, \ldots, r_3 \rangle$ generated by the reflections

$$s_0 := r_1, \; s_1 := r_2, \; s_2 := r_3, \; s_3 := r_0 r_1 r_2 r_1 r_0$$

with roots

$$a_0 := b_1, \; a_1 := b_2, \; a_2 := b_3, \; a_3 := r_0 r_1 (b_2) = b_0 + b_1 + b_2,$$

respectively. Then B is a reflection group of type $B_4^p \simeq B_4$ (with a diagram as in 6.2, with $n = 4$). Let $c_0, \ldots, c_3$ be the orthogonal basis associated with B. In characteristic 0, the corresponding subgroup has index 3 in F_4, so it suffices to check that this is also true mod p. But $r_0 \notin B$ (the lines spanned by $c_0, \ldots, c_3$ are not permuted by r_0), so B must indeed be a proper subgroup. Hence, $G^p \simeq F_4$ and the polytope $\mathcal{P}(G^p)$ is isomorphic to the 24-cell $\{3, 4, 3\}$.

The initial vertex, being invariant under $G_0^p = \langle r_1, r_2, r_3 \rangle = \langle s_0, s_1, s_2 \rangle$, now corresponds to the "center" of the base facet of the 4-cube associated with B in $\mathbb{Z}_p^4$ and thus is given by

$$w := c_3 = a_0 + 2(a_1 + a_2 + a_3) = 2b_0 + 3b_1 + 4b_2 + 2b_3.$$

The orbit of w then consists of the 24 vertices

$$\pm c_0, \; \pm c_1, \; \pm c_2, \; \pm c_3, \; \tfrac{1}{2}(\pm c_0 \pm c_1 \pm c_2 \pm c_3)$$

of a modular representation of the 24-cell in (the non-singular space) $\mathbb{Z}_p^4$. Note that $r_0(c_3) = \frac{1}{2}(c_0 + c_1 + c_2 + c_3)$.

Once again we observe without further checking that the G^p orbit of μ_0 in $\check{V}$ has size 24, for any $p \geq 3$.

B. Groups of Euclidean Type

The Euclidean groups of ranks 2 or 3 were already discussed in the previous section, so it remains to investigate the Coxeter groups $G = [4, 3^{n-3}, 4]$ or $[3, 4, 3, 3]$ associated with the regular tessellations $\{4, 3^{n-3}, 4\}$ or $\{3, 4, 3, 3\}$ in $\mathbb{E}^{n-1}$ or $\mathbb{E}^4$, respectively. Now V is singular, for each p, with a radical of dimension 1. The resulting modular polytopes $\mathcal{P}(G^p)$ are regular toroids of ranks n or 5, respectively (see [24, Sect. 6D,6E]).

6.4 The group $[4, 3^{n-3}, 4]^p$ with diagram

We allow $n \geq 3$. The subgroups G_0^p and G_{n-1}^p of G^p are isomorphic to the finite reflection groups associated with the corresponding subdiagrams and thus are of type B_{n-1}^p. The intersection property of G^p follows from Theorem 4.2. (For a direct proof in all cases, recall that $G_{n-1}^p \simeq N_0 \rtimes G_{0,n-1}^p$, where $N_0 = \langle g r_0 g^{-1} \mid g \in G_{0,n-1}^p \rangle$ is the group associated with the orthogonal basis $c_0, \ldots, c_{n-2}$ for B_{n-1}^p. Now, if $h \in G_0^p \cap G_{n-1}^p$, then, by changing h modulo $G_{0,n-1}^p$, we may assume that $h \in N_0$. We need to prove that $h = e$, the identity mapping. Using the fact that h must leave $V_{0,n-1}$ invariant, we then further conclude that h is $\pm e$ on V_0 and thus on V. But $-e = (r_0 r_1 \cdots r_{n-2})^{n-1}$ in B_{n-1}^p, so the case $h = -e$ can also be ruled out by verifying that the latter element does not map b_{n-1} to $-b_{n-1}$.)

Now $\mathcal{P}(G^p) = \{4, 3^{n-3}, 4\}_{(p,0,\ldots,0)}$ (with $n-2$ entries 0 in the subscript) is the regular toroid of rank n with automorphism group $G^p \simeq C_p^{n-1} \rtimes B_{n-1}$. Its p^n facets are cubes, and the vertex-figures at its p^n vertices are crosspolytopes. For the isomorphism with the toroid, note that, since p is a prime, it suffices to verify the relation

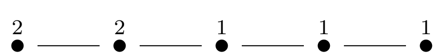
$$(r_0 r_1 r_2 \cdots r_{n-2} r_{n-1} r_{n-2} \cdots r_2 r_1)^p = e$$

(see [24, Thm. 6D4]). Here, the reflection $r := r_1 r_2 \cdots r_{n-2} r_{n-1} r_{n-2} \cdots r_2 r_1$ is conjugate to r_{n-1} and its root is given by

$$b \;:=\; r_1 r_2 \cdots r_{n-2}(b_{n-1}) \;=\; b_{n-1} + 2(b_{n-2} + \ldots + b_1)$$

(this is the last vector in the orthogonal basis associated with the vertex figure group G_0^p). The plane spanned by the roots b_0 of r_0 and b of r is easily seen to be singular (it contains the radical of V, spanned by $b + b_0$), so that the product $r_0 r$ does indeed have period p.

6.5 The group $[3, 4, 3, 3]^p$ with diagram



Now we have $G_0^p \simeq B_4^p \simeq B_4$ and $G_{n-1}^p \simeq F_4^p \simeq F_4$. The intersection property of G^p follows directly from Theorem 4.2, for all p. The corresponding polytope is the toroid $\mathcal{P}(G^p) = \{3, 4, 3, 3\}_{(p,0,0,0)}$ of rank 5, whose automorphism group is $G^p \simeq C_p^4 \rtimes F_4$. Its p^4 facets are 24-cells, and the vertex-figures at its $3p^n$ vertices are 4-cubes. For the isomorphism with the toroid we now need to verify the relation

$$(r_4 s\, t\, s)^p = e,$$

with $s := r_3r_2r_1r_2r_3$ and $t := r_0r_1r_2r_1r_0$ (see [24, Thm. 6E6]). The reflection $r := s\,t\,s$ is conjugate to r_2 and has root

$$b \;:=\; s\,r_0r_1(b_2) \;=\; b_0 + 2b_1 + 3b_2 + 2b_3.$$

The plane spanned by the roots b_4 of r_4 and b of r is again singular (it contains the radical of V, now spanned by $b + b_4$), so the product r_4r indeed has period p.

References

[1] E. Artin, Geometric Algebra, Interscience, New York (1957).

[2] N. Bourbaki, Groupes et algèbres de Lie, ch. iv-vi, Hermann, Paris (1968).

[3] N. Broderick and G.Maxwell, The crystallography of Coxeter groups II, J. Algebra **44** (1977), pp. 290–318.

[4] F. Buekenhout and A. Pasini, Finite diagram geometries extending buildings. In Handbook of Incidence Geometry (ed. F. Buekenhout), Elsevier Publishers, Amsterdam (1995), pp. 1143–1254.

[5] A.M. Cohen, Finite Complex Reflection Groups, Ann. Sci. École Norm. Sup. (4) **9** (1976), pp. 379–436.

[6] M. Conder and P. Dobcsányi, Determination of all regular maps of small genus, J. Combin. Theory Ser. B **81** (2001), pp. 224–242.

[7] H.S.M. Coxeter, Extreme Forms, Canadian J. Math. , **3** (1951), pp.391–441.

[8] H.S.M. Coxeter, Groups Generated by Unitary Reflections of Period Two, Canadian J. Math. **9** (1957), pp. 243–272.

[9] H.S.M. Coxeter, Regular Complex Polytopes, 2nd Ed., Cambridge University Press, Cambridge (1991).

[10] H.S.M. Coxeter and W.O.J. Moser, Generators and Relations for Discrete Groups, 3rd Ed., Springer, New York (1972).

[11] C.W.Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley-Interscience, New York (1962).

[12] D. Garbe, Über die regulären Zerlegungen geschlossener orientierbarer Flächen, J. Reine. Angew. Math. **237** (1969), pp. 39–55.

[13] R. L. Griess, Quotients of infinite reflection groups, Math. Ann. **263** (1983), pp. 267–278.

[14] J. E. Humphries, Reflection Groups and Coxeter Groups, Cambridge University Press, Cambridge, 1990.

[15] W. Kantor, Generation of linear groups, The geometric vein - the Coxeter Festschrift, Springer, New York-Berlin, 1981, pp. 497–509.

[16] G.Maxwell, The crystallography of Coxeter groups, J. Algebra **35** (1975), pp. 159–177.

[17] G.Maxwell, On the crystallography of infinite Coxeter groups, Math. Proc. Cambridge Philos. Soc. **82** (1977), pp. 13–24.

[18] P. McMullen, Combinatorially regular polytopes, Mathematika **14** (1967), pp. 142-150.

[19] P. McMullen, Regular star-polytopes, and a theorem of Hess, Proc. London Math. Soc. **18** (1968), pp. 577–596.

[20] P. McMullen, Realizations of Regular Polytopes, Aequationes Math. **37** (1989), pp. 38-56.

[21] P. McMullen, Regular polyhedra related to projective linear groups, Discrete Mathematics. **91** (1991), pp. 161-170.

[22] P. McMullen, B. R. Monson and A. I. Weiss, Regular maps constructed from linear groups, European J. Combin. **14** (1993), pp. 541–552.

[23] P. McMullen and E. Schulte, Regular polytopes in ordinary space, Discrete and Comput. Geom. **17** (1997), pp. 449–478.

[24] P. McMullen and E. Schulte, Abstract Regular Polytopes, Encyclopedia of Mathematics and its Applications, **92**, Cambridge University Press, Cambridge, 2002.

[25] B. Monson, Simplicial Quadratic Forms, Canad. J. Math. **35** (1983), pp.101–116.

[26] E. Schulte and A. I. Weiss, Chirality and projective linear groups, Discrete. Math. **131** (1994), pp. 221–261.

[27] G.C. Shephard and J.A. Todd, Finite Unitary Reflection Groups, Canad. J. Math. **6** (1954), pp.274 – 304.

[28] F.A. Sherk, A Family of Regular Maps of Type $\{6,6\}$, Canad. Math. Bull. **5** (1962), pp.13 – 20.

[29] E.B. Vinberg, Discrete linear groups generated by reflections, Izv. Akad. Nauk. SSSR Ser. Mat. **35** (1971), pp. 1072–1112 (= Math. USSR-Izv. **5** (1971), pp. 1083–1119).

[30] A.Wagner, Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two. I, Geom. Dedicata **9** (1980), pp. 239–253.

[31] A.Wagner, Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two. II, III, Geom. Dedicata **10** (1981), pp. 191–203, 475–523.

[32] S.E.Wilson, Applications and refinements of Vince's construction, Geom. Dedicata **48** (1993), pp. 231–242.

[33] A.E. Zalesskiĭ and V.N. Serežkin, Linear groups generated by transvections. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), pp. 26–49. (English translation in Math. USSR Izvestija **10** (1976), pp. 25–46.)

[34] A.E. Zalesskiĭ and V.N. Serežkin, Finite linear groups generated by reflections. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), pp. 1279–1307, 38. (English translation in Math. USSR Izvestija **17** (1981), pp. 477–503.)