Yet Another Lecture on the Icosahedron‡

Arjeh M. Cohen*

1 Introduction

In the period 1984–1992, one of my research goals was to establish the existence of certain (non-abelian) finite subgroups of exceptional Lie groups. My main collaborators on this topic were R.L. Griess, Jr. and D.B. Wales.

Some of these embeddings could be done entirely by theoretic arguments and hand calculations. For the others, the best we could do was to reduce the problem to a form suitable for the computer to finish off the computations. I would like to sketch the nature of such computations using a few simple examples, thereby illustrating the improved possibilities of polynomial system solving.

Also, I will sketch roughly how, very recently, Serre has shown that the reduction techniques we developed can be pushed so far that at least the most spectacular of the existence proofs can also be done without recourse to a computer.

I will write about one more issue, as it represents some of the interactions between mathematics and computer science that Cor Baayen enjoys seeing. It is the use of rewriting techniques in group theory, in much the same way they are used in Buchberger's Gröbner basis approach to polynomials—the technique that lies at the heart of the present polynomial system solvers.

Before going into some of these details, I will present an elementary introduction into group representations. The quaternion group (of order 8) and the icosahedral group (of order 120) will be used to illustrate the ideas. The rotation group of the latter is the nonabelian finite simple group of smallest order. This may explain a bit why it is a gateway to understanding finite simple groups.

2 The quaternion group

Let G be a finite group. A classical group theoretic question is to determine all possible realisations of G as a group of matrices. To be more precise, one would like to know all possible morphisms $\rho : G \to GL(V)$ from G into the group $GL(V)$ of all linear transformations of a vector space V over a fixed field k.

*Written for Cor Baayen in gratitude for his rôle in my professional life.

‡Inspired by the 100 year old [K] and the introduction to [BCN].

Such a morphism is called a linear representation of G (over k). If $n = \dim V$, then ρ is said to be n-dimensional.

In fact, we are only interested in representations up to equivalence; we recall that a representation $\rho' : G \to GL(V')$ over k equivalent to ρ if there is a linear invertible map $A : V \to V'$ such that $\rho(g) = A^{-1}\rho'(g)A$ for all $g \in G$.

Another restriction we make here is the field: we shall only look at representations in characteristic 0 here. In fact, we shall take $k = \mathbf{C}$ for the time being, in which case we speak of complex representations. Consider representations of the quaternion group

$$Q = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$$

with multiplication determined by

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \quad \text{and} \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}$$

(and the fact that -1 is a central element of order 2).

It makes sense to restrict to irreducible representations, i.e., those that have no "subrepresentations" but for the zero-dimensional and the full vector space V. Every complex representation can be decomposed as a sum of irreducible representations.

There always is the trivial representation, sending every element to the 1×1 matrix (1). But Q can also be represented as a group of 1×1 matrices by the morphism

$$\pm 1 \mapsto 1, \quad \pm \mathbf{i} \mapsto 1, \quad \pm \mathbf{j} \mapsto -1, \quad \pm \mathbf{k} \mapsto -1.$$

The trivial representation and this one are not the only 1-dimensional representations. There are two more 1-dimensional representations. (one sending $\pm\mathbf{j}$ to 1, the other sending $\pm\mathbf{k}$ to 1, instead of $\pm\mathbf{i}$). None of these provides a faithful (that is, injective) representation. But the following 2-dimensional representation is faithful:

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm \mathbf{i} \mapsto \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$\pm \mathbf{j} \mapsto \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm \mathbf{k} \mapsto \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

How do we find such a representation? Suppose Q has a 2-dimensional faithful representation ρ. Then, from the fact that ρ must be irreducible (sums of 1-dimensional representations are not faithful!), we know that $\rho(1)$ is the identity matrix I_2, and, similarly, that $\rho(-1) = -I_2$. Furthermore, $\rho(\mathbf{j})$, being an element squaring to $-I_2$, can be chosen, up to conjugacy, to be

$$\rho(\mathbf{j}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Now all we need to find is $\rho(\mathbf{i})$, because the morphism law $\rho(xy) = \rho(x)\rho(y)$ will then determine the images of all remaining elements. Write

$$\rho(\mathbf{i}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

for certain $a, b, c, d \in \mathbf{C}$. Working out that $\rho(\mathbf{i})^2 = -I_2$ and that $(\rho(\mathbf{i})\rho(\mathbf{j}))^2 = -I_2$ yields a set of equations in these four variables. Solving these equations readily leads to the conclusion that, for any $a, b \in \mathbf{C}$ with $a^2 + b^2 = -1$, the morphism $\rho_{a,b}$ given by

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm \mathbf{i} \mapsto \pm \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

$$\pm \mathbf{j} \mapsto \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm \mathbf{k} \mapsto \pm \begin{pmatrix} -b & a \\ a & b \end{pmatrix}$$

is a 2-dimensional representation of Q.

The choice $a = i$, $b = 0$ gives the representation ρ mentioned before. Any representation $\rho_{a,b}$ is conjugate to ρ; if $b \neq 0$, then the matrix

$$A = \begin{pmatrix} i - t & -s \\ s & i - t \end{pmatrix},$$

where $t = i - s(a + i)/b$, conjugates ρ to $\rho_{a,b}$.

The four 1-dimensional representations and the 2-dimensional one are all we need to build up the full set of linear representations of Q over the field $\mathbf{C}$. Up to conjugacy, these are the only irreducible representations. The theory on which this assertion is based is known as character theory. A consequence of this beautiful theory is that the sum of all squares of the dimensions of the distinct (non-conjugate) irreducible representations equals the order of the group. Here, this amounts to

$$1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8.$$

It is of interest for the study of representations over finite fields to know minimal extension fields k over the rationals such that the represented group embeds in a version of $GL(V)$ defined over k. A look at ρ for the quaternion group shows that the 2-dimensional representation is realised over $\mathbf{Q}(i)$. But if we take $a = 3$, $b = 2\sqrt{-2}$, then $\rho_{a,b}(Q)$ is realised over the field $\mathbf{Q}(\sqrt{-2})$ and clearly no conjugate of ρ can be realised over $\mathbf{Q}$. This indicates that there is no minimal extension field of $\mathbf{Q}$ attached to the class of representations in $GL(V)$ containing ρ. Later we shall see that this seeming lack of a unique minimal "splitting field" for Q is due to the restricted notion of representation handled here.

3 The group of the icosahedron

The isometry group of the icosahedron (the usual Platonic solid in 3-dimensional Euclidean space) can be abstractly defined as the group W generated by the 3 elements x, y and z subject to the relations

$$x^2 = y^2 = z^2 = 1,$$

$$(xy)^3 = (yz)^5 = (xz)^2 = 1.$$

Such a definition by means of generators $X = \{x, y, z\}$ and relators $Y = \{x^2, y^2, z^2, (xy)^3, (yz)^5, (xz)^2\}$, often succinctly written as

$$W = \langle X \mid Y \rangle,$$

is called a presentation by generators and relations.

The abstract presentation of the icosahedral group can be understood by looking at the classical icosahedron. Cut the surface of the icosahedron into domains by means of the hyperplanes that are the mirrors of reflections preserving the icosahedron. By doing so, and selecting one of the 120 domains, we can identify the three generators x, y, z with the reflections whose mirror hyperplanes bound the selected domain of the icosahedron.

Surprisingly enough, we can go the other way around: by constructing the most general graph whose vertices are (transitively) permuted by the elements of the group W, we find the icosahedral graph. Let us perform this construction in some more detail. Start with a vertex, and label it with the trivial element of the group. We make three neighbours of 1, labeled x, y, z (the three generators of the group W). We also label the edges $\{1, x\}$, $\{1, y\}$, $\{1, z\}$ with the respective labels x, y, z. The graph under construction must allow for an action (on the left) of the generators as a group of automorphisms. It will be most convenient to think of the graph under construction as one whose edges are labeled with x, y, z.

Since the three generators are elements of order 2 (see the first line of relations for W), we can think of view each of them as a permutation interchanging the vertices of an edge on 1 whose label coincides with its name. The vertex of that edge distinct from 1 will then be labelled with that name as well. But the picture is still far from being complete: it has not yet been described to which node y maps the vertex x. Left multiplication by y, being an automorphism of the graph, must send the edge $\{1, x\}$ labeled x to the edge $\{y, yx\}$, labeled x. Thus, we find a new vertex yx, connected to y with an edge labeled x. Leaving alone z for a while, we continue this way, joining yxy to yx with and edge labeled y, joining $yxyx$ to yxy with an edge labeled x. Then we reach $yxyxy$, which is joined to $yxyx$ with an edge labeled y. The relation $(xy)^3 = 1$ (on the second line of relations for W) and the fact that x and y are their own inverses (being of order 2), tell us that the element $yxyxy$ coincides with x. Moreover, the edge $\{yxyxy, yxyx\}$ can be rewritten as $\{x, xy\}$. Thus, we have found a circuit of length 6, with nodes $1, y, yx, yxy = xyx, xy, x$ whose edges are alternatingly labeled y and x. This circuit is, all by itself, a graph on which the group with presentation $\langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle$ acts (regularly) as a group of automorphisms. Thus, we have found a realisation for this group. Apparently it has order 6 (the number of vertices) and is isomorphic to the symmetric group on 3 letters (which can be seen by verifying that the group is fully determined by its permutation behaviour on the three edges labeled x).

Returning to W, we can throw in z and continue in much the same way. Cor Baayen is encouraged to try this. If the edges labeled x, y, z are drawn as

dotted lines, ordinary lines, fattened lines, respectively, the result is as depicted in Figure 1.

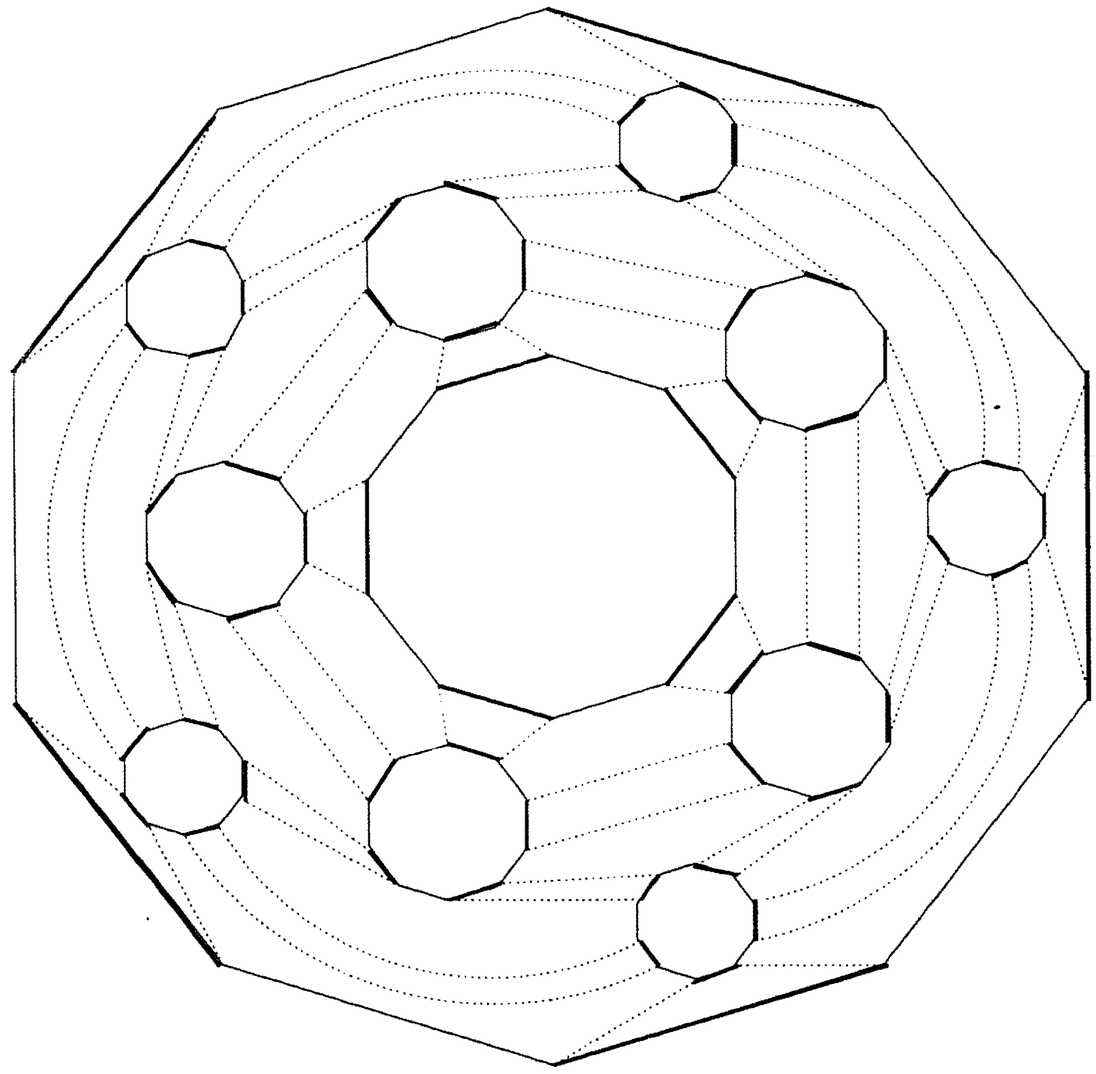

Figure 1. The Cayley graph of the icosahedral group

The number of vertices is 120, which is the order of the group W. In fact, the vertices of the graph can be identified with the elements of the group. In order to do so, select a vertex (which may be taken to be the starting point of the construction procedure that we just described) and identify it with the trivial element 1 of W. Next, associate any other vertex v with the element of W that can be found as follows: select a path from v to 1, and write down the consecutive labels of the edges of a path from 1 to v. This produces a word expressing v as a product of the generators x, y, z of W.

So far, we have obtained a very geometric description of the abstractly defined icosahedral group. The reader may wonder how much of a miracle just happened. In general, that is, for arbitrary presentations by generators and relations, the technique we have carried out a special "icosahedral" case of, is known as the Todd-Coxeter coset enumeration method. The construction of the graph will not always be as straightforward as in the above example. The reason is that collapses of a more drastic nature than the identification of $yxyxy$ with x above may occur. It usually happens that a whole collection of

new vertices has to be created before a collapse is found to occur. In fact, presentations by generators and relations of the trivial group are known which only produce the graph on a single vertex after an enormous intermediate growth of (temporary) vertices.

An even bigger problem is that, especially when nothing is known a priori about the presentation of the group, termination is not even guaranteed. The single positive (but very powerful) result regarding coset enumeration is that, due to a result of Mendelssohn, cf. [Suz], it terminates if the resulting group is finite. (There is no a priori indicator known though as to how long it might take before termination takes place.)

The more general coset enumeration takes as input not only a group specified by generators and relations, but also a subgroup. The resulting vertices of the graph will then correspond to the cosets of the subgroup. Once a coset enumeration has been completed, a permutation representation for the group results. The upshot, for finite groups G, is great in that many good algorithms exist for determination of the structure of a permutation group (certainly when compared to the algorithms available for groups presented by generators and relations).

4 How to find 3-dimensional representations

In this section, we show how using Gröbner basis methods, one can find 3-dimensional real (or complex) representations for the icosahedral group W. The construction will be similar to the one for the 2-dimensional quaternion group. Only this time the computations are done by use of a computer algebra package (for finding a Gröbner basis).

Thus, suppose $\phi : W \to GL(\mathbf{R}^3)$ is a 3-dimensional representation of W. We assume that x and z are mapped to distinct elements in $GL(\mathbf{R}^3)$. Observe that, without loss of generality, we are in one of the following cases:

$$\text{I. } \phi(x) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \phi(z) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}; \text{ or}$$

$$\text{II. } \phi(x) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \phi(z) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Since, for every representation ϕ, there is also a representation ψ of W with $\psi(u) = -\phi(u)$ for u equal to x, y and z, we only have to consider representations ϕ as in I. Let us do so. Then $\phi(u)$ is a reflection for u equal to x, y or z.

In order to extend ϕ we need to find a matrix $\phi(y) = (y_{i,j})_{1 \le i,j \le 3}$.

Since $\phi(y)$ is a reflection, its trace is 1. This gives us the following linear equation for the entries of y:

$$y_{1,1} + y_{2,2} + y_{3,3} = 1.$$

Similarly, as $\phi(xy)$ is a real element of order 3 (it cannot be of order 1 because $\phi(x)$ and $\phi(z)$ are distinct), its trace must be 1. This gives another linear equation for the entries of y, namely

$$-y_{1,1} + y_{2,2} + y_{3,3} = 0.$$

The following is a Maple programme that creates the equations for the coefficients of $\phi(y)$ that follow from the relations between the elements x, y and z of W:

```
with(linalg):

#The three matrices we start out with:

x := matrix(3,3,[[-1,0,0],[0,1,0],[0,0,1]]);
z := matrix(3,3,[[1,0,0],[0,1,0],[0,0,-1]]);
y := matrix(3,3,[[y11,y12,y13],[y21,y22,y23],[y31,y32,y33]]);


#putting the unknown in a list:

vars := [y11,y12,y21,y13,y31,y22,y23,y32,y33];
```

```
# Create the identity matrix of dimension n:

 idmat := proc(n)
 local ans,i,j;
 ans := matrix(n,n);
 for i to n do for j to n do ans[i,j] := 0;
 if i=j then ans[i,j] := 1 fi od od:
 evalm(ans)
 end;

#use it to construct the 3-dimensional identity matrix:

idm := idmat(3);


# Given a matrix, derive the equations
# for its coefficients to be zero.
```

```
mkeq := proc(a)
        local i,j,answ;
            answ := {};
```

```
for i to rowdim(a)
do
    for j to coldim(a)
    do
    answ := answ union {a[i,j]}
    od
    od;
    answ
end;
```

```
# The relations for x, y and z imply the following equations:

 y2 := evalm(evalm(y^2) - idm);
 eqy := mkeq(y2);

 xyx := evalm(  x  y  x);
 yxy:= evalm( y  x  y);
 eqxy := mkeq(evalm(xyx - yxy));

 yzyzy := evalm( y  z  y  z  y);
 zyzyz := evalm( z  y  z  y  z);
 eqyz := mkeq (evalm(yzyzy -zyzyz));
```

```
#loading the Groebner basis package:

with(grobner);


# the linear equations coming from the traces are

lineqs := {trace(evalm(y ) ) -1, trace(evalm(x  y ) )};


# We do the Groebner basis computation in 3 steps.
# After each step one can simplify the equations by hand!

gby  :=  gbasis(eqy  union lineqs           ,vars,plex);
gbxy  := gbasis(eqxy union convert(gby, set),vars,plex);
gbxyz := gbasis(eqyz union convert(gbxy,set),vars,plex);
```

The Gröbner basis found by the computer algebra package has the following form:

$$\{2y_{11}-1, y_{12}+4y_{32}y_{13}y_{33}+2y_{13}y_{32},$$
$$2y_{23}y_{31}+y_{21}+4y_{31}y_{23}y_{33}, 2y_{13}y_{31}+y_{33}-1,$$
$$2y_{22}+2y_{33}-1, 4y_{23}y_{32}-1, -1+4y_{33}^2-2y_{33}\}$$

From the "upper-triangular" structure of the Gröbner basis, the general shape of a solution up to algebraic conjugacy is readily seen to be

$$\phi(y)=\begin{bmatrix} \frac{1}{2} & \frac{-y_{32}}{2y_{31}} & -\frac{\sqrt{5}-3}{8y_{31}} \\ -\frac{y_{31}(\sqrt{5}+3)}{4y_{32}} & \frac{1-\sqrt{5}}{4} & \frac{1}{4y_{32}} \\ y_{31} & y_{32} & \frac{\sqrt{5}+1}{4} \end{bmatrix}.$$

with y_{31}, y_{32} both nonzero. In fact conjugation by suitable diagonal matrices shows that all solutions lead to equivalent representations (up to algebraic conjugacy, so in fact to two classes of representations).

By the way, using the same computer algebra package, checks can be easily carried out to verify that the solution $\phi(y)$ indeed gives a linear representation.

In a subsequent section, we shall show that a 3-dimensional representation can easily be written down directly by applying the theory of Coxeter groups to W.

5 Representations in algebraic groups

As we have seen, faithful representations for a finite group G are embeddings of G in a group of the form $GL(n,k)$. This point of view raises the question whether we can determine all embeddings of such a group G in other linear algebraic groups. Algebraic groups can be viewed as subgroups of $GL(n,k)$ stabilizing certain forms. For instance, the so-called symplectic groups are subgroups of even-dimensional linear groups stabilizing a non-degenerate bilinear alternating form. The crucial point is that such subgroups are algebraic subvarieties of $GL(n,k)$ as they are zeros of the polynomial equations obtained by writing out for the entries of a matrix in $GL(n,k)$ what it means to stabilize such a form (or more forms).

For the classical (infinite) series of algebraic groups, this viewpoint gives little news with respect to the usual representation theory, so naturally the attention is led to the exceptional types E_6, E_7, E_8, F_4, G_2. By use of the normal subgroup structure of a finite group, the problem can be reduced to three problems, the most salient of which concerns the study of embeddings of finite nonabelian simple groups in complex algebraic groups. Systematic searches for such embeddings received an impetus by *Kostant's conjecture*, formulated in 1983. It asserts that every simple complex algebraic group $G(\mathbf{C})$ with a Coxeter number h such that $2h+1$ is a prime power, has a subgroup isomorphic to $L(2,2h+1)$. Here, $L(2,q)$, for q a prime power, stands for

the group of functions (so-called fractional linear transformations) of the form $z \mapsto az + b/(cz + d)$ defined on the projective line of order q.

For $G(\mathbf{C})$ of classical type, Kostant's conjecture is readily checked using ordinary representation theory and the Frobenius-Schur index. For $G(\mathbf{C})$ of exceptional type the table below and the knowledge that $h = 6, 12, 12, 18, 30$ for the five respective exceptional types give an affirmative case-by-case answer.

A quick overview of the state of the art is supplied by Table 1.

Table 1.
Nonabelian simple groups L a central extension of which embeds in a complex Lie group of exceptional type X_n

X_n	L
G_2	Alt_5, Alt_6, $L(2,7)$, $L(2,8)$, $L(2,13)$, $U(3,3)$
F_4	Alt_7, Alt_8, Alt_9, $L(2,25)$, $L(2,27)$, $L(3,3)$, ${}^3D_4(2)$, $U(4,2)$, $O(7,2)$, $O^+(8,2)$
E_6	Alt_{10}, Alt_{11}, $L(2,11)$, $L(2,17)$, $L(2,19)$, $L(3,4)$, $U(4,3)$, ${}^2F_4(2)'$, M_{11}, J_2
E_7	Alt_{12}, Alt_{13}, $L(2,29)^?$, $L(2,37)$, $U(3,8)$, M_{12}
E_8	Alt_{14}, Alt_{15}, Alt_{16}, Alt_{17}, $L(2,16)$, $L(2,31)$, $L(2,41)^?$, $L(2,32)^?$, $L(2,49)^?$, $L(2,61)$, $L(3,5)$, $Sp(4,5)$, $G_2(3)$, $Sz(8)^?$

There are two meanings to be attached to this table:

Theorem. *Let L be a finite simple group and let G be a simple algebraic group of exceptional type X_n.*

(i) If L occurs on a line corresponding to X_n in Table 1, then a central extension of it embeds in $G(\mathbf{C})$, with a possible exception for the five groups marked with a "?".

(ii) If X_n is as in some line of Table 1 and L appears neither in the line corresponding to X_n nor in a line above it, then no central extension of L embeds in $G(\mathbf{C})$.

Here, to simplify the presentation,

a. we have deliberately neglected questions of conjugacy classes of embeddings, and

b. we have not specified the particular nonsplit central extensions of the simple groups involved.

During my years at CWI, I spent considerable time and effort realising some of the embeddings appearing in this table.

Ad a. An example where the conjugacy class question is more subtle than suggested by the table is provided by $L(2,13)$. By [CW93], it is isomorphic to

a subgroup of $F_4(\mathbf{C})$ whose normalizer is a finite maximal closed Lie subgroup of $F_4(\mathbf{C})$, whereas Table 1 only hints at the existence of embeddings via a closed Lie subgroup of $F_4(\mathbf{C})$ of type G_2.

Ad b. For instance, the simple group $L(2,37)$ listed embeds into a group of type E_7 but not in a group of type E_8 because each embedding in an adjoint group of type E_7 lifts to an embedding of $SL(2,37)$ into the universal covering group $2 \cdot E_7(\mathbf{C})$. Of course, the double cover $SL(2,37)$ of $L(2,37)$ embeds in the universal Lie group of type E_7, whence in a Lie group of type E_8.

Another warning concerning Table 1 is perhaps in order: The main theorems in [CW92] and [CoG] only concern subgroups not contained in closed Lie subgroups of positive dimension whereas Table 1 lists all finite simple subgroups (whether in a closed Lie subgroup of positive dimension or not).

i. The choice of central extensions of simple groups rather than just simple groups is important because they are the ones needed for the generalized Fitting subgroup.

ii. The table does not account for all groups that are involved in $E_8(\mathbf{C})$. For instance, no central extension of $L(5,2)$ is embeddable in $E_8(\mathbf{C})$, but a nonsplit extension $2^{\{5+10\}} \cdot L(5,2)$ does embed (cf. [A]).

iii. The group $L(2,29)$ appears in a Lie group of type B_7, whence in one of type E_8. So, if the question whether a central cover of $L(2,29)$ embeds in $E_7(\mathbf{C})$ has a negative answer, the group should appear at the bottom line of Table 1.

iv. Unlike the $GL(n,\cdot)$ case, knowledge of the classes of the individual elements of an embedded group L does not suffice to determine the conjugacy class of L in G. This has been observed by Borovik for the alternating group Alt_6 in $E_8(\mathbf{C})$. The problem of how many conjugacy classes of embeddings of L exist only has a partial solution. See [Gr] for the full solution concerning G_2.

v. The groups $L(2,41)$, $L(2,49)$ and $Sz(8)$ do not appear as possible subgroups of $E_8(\mathbf{C})$ in [CoG]; the arguments ruling them out given there are erroneous.

vi. Another error in [loc. cit.] concerns the character given for $L(2,31)$. The restriction of the adjoint character for $E_8(\mathbf{C})$ to the subgroup isomorphic to $L(2,31)$ constructed by Serre (see below) has a different character.

One of the more spectacular results is the embedding of $L(2,61)$ in $E_8(\mathbf{C})$, the biggest of all five exceptional Lie groups. Using more refined versions of the techniques described in §§2, 3, Griess, Lisser and I have been able to prove that the suggested embedding exists and is unique up to conjugacy. In this case, the algebraic group can be seen as the subgroup of $GL(248,\mathbf{C})$ stabilizing

a particular alternating trilinear form. Because our computations ran out of hand, we did all computations over a finite field ($\mathbf{Z}/1831$) and argued that, if G embeds in a modular form of E_8 over $\mathbf{Z}/1831$, it would also embed in $E_8(\mathbf{C})$. A key point in this argument was that G has order prime to 1831. This made it possible to deduce that any extension of G by a normal (profinite) subgroup of order a power of 1831, would split, that is, actually contain a subgroup isomorphic to G.

Very recently, Serre ([Se]) realised that this condition is not always needed. He started from a reasonable well-known embedding of $L(2,61)$ in $E_8(61)$. Then, the lifting technique gives a subgroup L of $E_8(\mathbf{C})$ that has a normal profinite 61-subgroup N with quotient isomorphic to $L(2,61)$. The important step is to show that, as an extension of $L(2,61)$ by N, the group L splits. For the $L(2,61)$ case, Serre needed a rather intricate argument; in the same sweep he also dealt with some other cases, like the embedding of $L(2,31)$ in $E_8(\mathbf{C})$, where the argument is rather succinct.

The algebraic group setting is also the right one for reconsidering the minimal splitting field question raised at the end of §3. Recall that, for the quaternion group, there is no unique minimal field realising an embedding in $GL(2,k)$. However, if we look at representations somewhat differently, it turns out that there does exist a minimal field for each conjugacy class of representations. To this end, we need to allow for all k-forms of $GL(V)$, that is all algebraic groups whose complex points form the group $GL(2,\mathbf{C})$.

In the above quaternion case, we have the following $\mathbf{Q}$-form of $GL(2,\mathbf{C})$:

$$H(k) = \{\alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \mid \alpha,\beta,\gamma,\delta \in k,\ \alpha^2+\beta^2+\gamma^2+\delta^2 \neq 0\}.$$

This set forms a group, the basis elements of which multiply as the elements in Q. In particular, Q is a subgroup of $H(\mathbf{Q})$. To see that it is a $\mathbf{Q}$-form of $GL(2,\mathbf{C})$, consider the injective morphism $H(\mathbf{Q}) \to GL(2,\mathbf{Q}(i))$:

$$\alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \mapsto \begin{pmatrix} \alpha+\beta i & \gamma+\delta i \\ -\gamma+\delta i & \alpha-\beta i \end{pmatrix}.$$

When extended to $\mathbf{Q}(i)$, and so certainly, when extended to $\mathbf{C}$, this maps becomes an isomorphism.

Thus, we have obtained a unique minimal field k, namely $\mathbf{Q}$, for which there exists a k-form of $GL(V)$ containing Q. This illustrates a result due to Springer [Spr] that for each group morphism $\rho : G \to H(\mathbf{C})$ from G to an algebraic group $H(\cdot)$, there is a minimal field extension k of $\mathbf{Q}$ such that G embeds into a k-form of H.

Coming back to this problem for the subgroup $L(2,61)$, the minimal splitting field is probably $Q(\sqrt{61})$; but, to the best of my knowledge, this has not yet been established. The next question is then, if k is the minimal splitting field, which k-form is it that the subgroup embeds in? The various $\mathbf{Q}(\sqrt{61})$-forms of $E_8(\mathbf{C})$ are known by Cernousov's work (there are 9).

Together with Tiep ([CT]), I have found the minimal splitting fields for some other remarkable subgroups of the exceptional algebraic groups, namely the Jordan subgroups.

6 The reflection representation

As promised earlier, we now come to another way of constructing a 3-dimensional representation for the icosahedral group W. Tits has shown that, for the so-called Coxeter groups, one can always find a faithful "reflection representation." The icosahedral group is a Coxeter group, whose reflection representation is equivalent to the one found above.

We shall describe the construction of the reflection representation of the icosahedral group, thereby following the general construction for Coxeter groups. Put $\sigma = \zeta^2 + \zeta^3$ and $\tau = \zeta + \zeta^4$, where $\zeta = e^{2\pi i/5}$.

Starting point is a 3-dimensional space V (one dimension for each generator of W), supplied with the symmetric bilinear form given by the following matrix:

$$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & \sigma \\ 0 & \sigma & 2 \end{pmatrix}.$$

Note that, if the rows and columns are labeled with x, y and z, respectively, the off-diagonal entries are $-2\cos(\pi/m)$, where m is the order of the product of the generators corresponding to row and to column. (This hints toward the general case for those who know what a Coxeter group is.) Denote the bilinear form by $(\cdot,\cdot)$. It is positive-definite, so the 3-dimensional space, supplied with this form is Euclidean. Now, for $\alpha \in V$ with $(\alpha,\alpha) = 2$, the reflection with "root" α is given by

$$s_\alpha : w \mapsto w - (w,\alpha)\alpha.$$

The reflection representation is determined by the images of x, y, z. These images will be the reflections s_α for α the standard basis vectors: $\alpha = e_1, e_2, e_3$. These roots are called the *fundamental roots* of W. Thus, we obtain the following matrices:

$$x = \begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$y = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -\sigma & 1 \end{pmatrix},$$

$$z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\sigma \\ 0 & 0 & -1 \end{pmatrix}.$$

By what we have seen above, this representation must be equivalent to one of the two (algebraically conjugate ones) constructed using Gröbner bases in §5.

Using the faithfulness of the reflection representation, it is easy to derive that the icosahedral group W is finite and to find a permutation representation. For instance, consider the set Φ of all roots of reflections in W. This set can be built up from the fundamental roots. Up to signs, they are:

$$\begin{array}{ccc}
(1,0,0) & (0,1,0) & (0,0,1) \\
(1,1,0) & (0,1,-\sigma) & (0,-\sigma,1) \\
(1,1,-\sigma) & (0,-\sigma,-\sigma) & (-\sigma,-\sigma,1) \\
(1,-\tau-2\sigma,-\sigma) & (-\sigma,-\sigma,-\sigma) & (1,-\tau-2\sigma,-\tau-2\sigma) \\
(-\sigma,-\tau-2\sigma,-\sigma) & (-\sigma,-\tau-2\sigma,-\tau-2\sigma) & (-\sigma,-2\sigma,-\tau-2\sigma)
\end{array}$$

Thus, we have a set Φ of $2 \times 15 = 30$ roots. Clearly, if $\alpha \in \Phi$, then also $-\alpha = s_\alpha \alpha \in \Phi$. If the 15 pairs $\pm\alpha$ are numbered according to their occurrence, the generators x, y and z induce the following permutations:

$$x = (2,4)(5,7)(6,9)(8,11)(10,13)(12,14),$$

$$y = (1,4)(3,6)(5,8)(7,10)(11,13)(14,15),$$

$$z = (2,5)(4,7)(6,8)(9,11)(10,12)(13,14).$$

The kernel of this permutation representation is readily seen to be $\{\pm I_2\}$. Since only a finite number of roots are being permuted, and the reflection representation of W is faithful, we see again that W is finite.

A remarkable property, true of arbitrary Coxeter groups, is that one of $\pm\alpha$ has all coefficients with respect to the fundamental root basis non-negative. These roots are called the positive roots. The set of all positive roots is denoted by Φ^+, so that $\Phi = \Phi^+ \cup \Phi^-$, where $\Phi^- = -\Phi^+$. In Figure 2 we have pictured Φ^+ and the way it is built up using the generators x, y, z, with the same conventions as for Figure 1 regarding the edges. The dashed line at the bottom indicates where the action of the generators crosses over to negative roots.

7 Presentation by generators and relations

We now go back to presentations of groups by means of generators and relations. For the icosahedral group W we have already given such a presentation: $W = \langle X \mid Y \rangle$, with $X = \{x, y, z\}$ and

$$Y = \{x^2, y^2, z^2, (xy)^3, (yz)^5, (xz)^2\}.$$

Of course, for a given group, such a presentation is far from unique.

Computations using the presentation of a group by generators and relations are based on the idea that it is easy to present a free group over a given alphabet X. Or maybe, even simpler, start with the free monoid X^* over X. This is the set of all strings (also called words) we can form with the symbols (also called letters) from X. Such a monoid has the great advantage that every element corresponds to a unique expression for it.

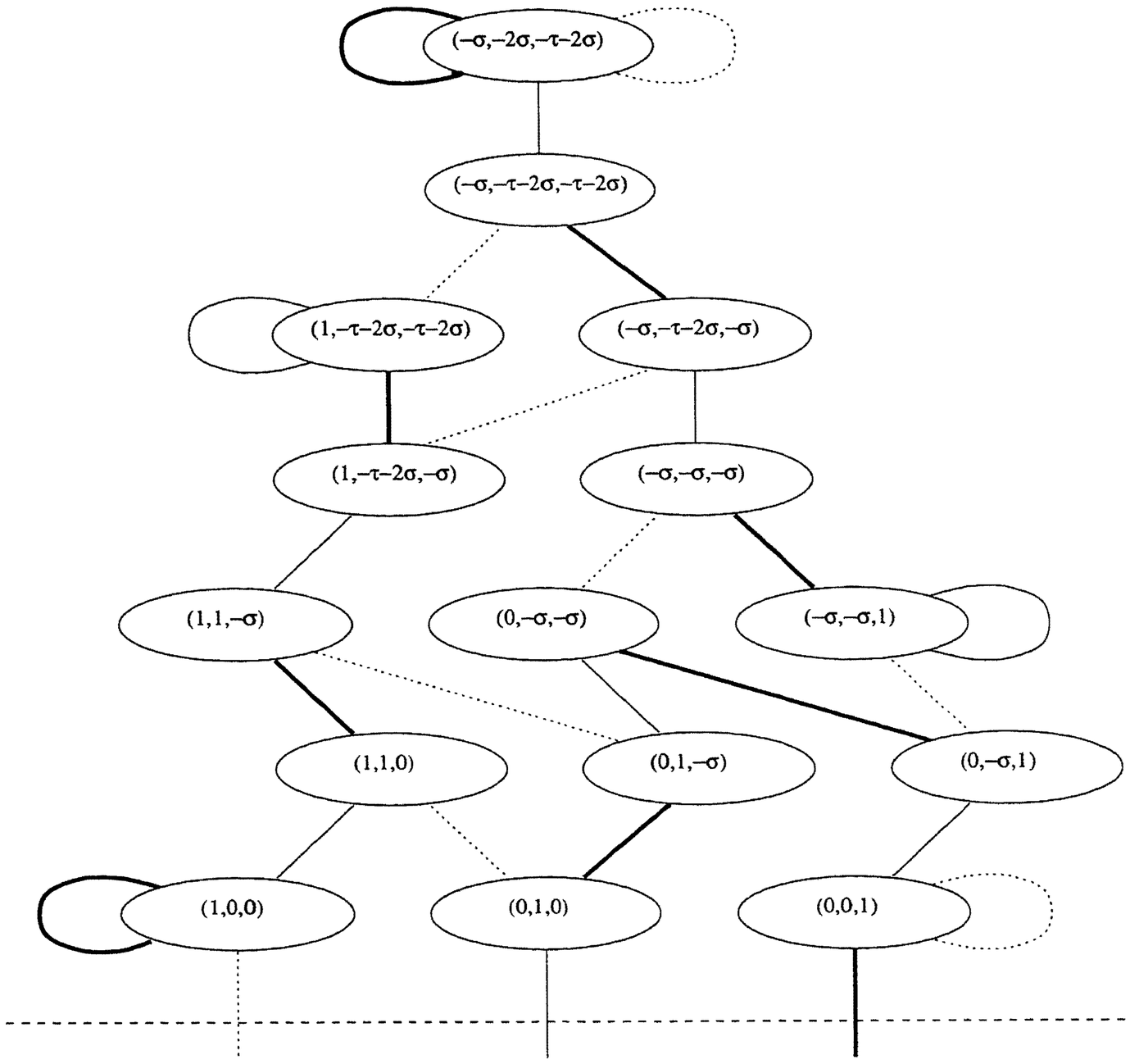

Figure 2. The positive roots with action of W

This phenomenon is no longer true of the free group on X. We can define it as a quotient of the free monoid on

$$A = X \cup X^{-1} = \{x, x^{-1}, y, y^{-1}, z, z^{-1}\}$$

with respect to the relations

$$xx^{-1} = x^{-1}x = 1$$

$$yy^{-1} = y^{-1}y = 1$$

$$zz^{-1} = z^{-1}z = 1.$$

Although now it is no longer true that every element of the free group on X corresponds to a unique word in A^*, we still have a very good way of handling this: the group elements correspond bijectively to the reduced words in the monoid, i.e., those with no occurrences of

$$xx^{-1}, x^{-1}x, yy^{-1}, y^{-1}y, zz^{-1}, z^{-1}z.$$

The icosahedral group W is obtained as a quotient by dividing out with respect to the normal subgroup generated by the relators

$$x^2, y^2, z^2, (xy)^3, (yz)^5, (xz)^2.$$

The question now arises how to find a set of words $\widetilde{W}$ in A^* such that every element of W corresponds to a unique element of $\widetilde{W}$. Another way of saying this is that we want to find a section σ of the natural map $\phi : A^* \to W$. The set $\widetilde{W}$ is then the image of σ. Yet another way of expressing the wish for unique representatives in A^* of elements of W is more algorithmic: for each element $w \in A^*$, we want to be able to find a "canonical" element in the fibre $\phi^{-1}(\phi(w))$.

A very successful approach is based on rewriting techniques. It uses a total well-ordering on A^*. More precisely, a well-founded total ordering $<$ is called a *reduction ordering* if

$$\forall\ l, r, m_1, m_2 \in A^*$$

$$m_1 < m_2 \ \Rightarrow\ lm_1r < lm_2r$$

and $1 = \min A^*$. We need a reduction ordering $<$ on A^*. There are plenty such orderings, but we will content ourselves with the total degree lexicographic one, that is the one where $v < w$ if either the length of v (as a string of symbols from A) is less than the length of w, or these lengths are equal and v comes prior to w in the usual lexicographic ordering (where $x < y < z < x^{-1} < y^{-1} < z^{-1}$). Thus,

$$1 < x < y < z < xx < xy < xz < yx < yy < \ldots$$

The canonical element for an arbitrary $m \in A^*$ can then be taken to be

$$\min \phi^{-1}\phi(m).$$

Now the purpose is to rewrite an arbitrary word $m \in A^*$ to the canonical word $\min \phi^{-1}\phi(m)$ by stepwise finding smaller representatives of $\phi(m)$. First of all, for involutions such as the generators in X for W, we may rid ourselves of inverses by use of the rewriting rules

$$x^{-1} \Rightarrow x,\ y^{-1} \Rightarrow y,\ z^{-1} \Rightarrow z.$$

For W with the above presentation, the obvious rewriting rules

$$xx \Rightarrow 1,\ yy \Rightarrow 1,\ zz \Rightarrow 1,$$

$$zx \Rightarrow xz,$$

$$yxy \Rightarrow xyx,$$

$$zyzyz \Rightarrow yzyzy.$$

do not suffice. For instance, $(xyz)^{10}$ cannot be reduced to the trivial element; but, for instance, writing out the permutation of the roots corresponding to xyz (by use of the permutations given for x, y and z in §6), we find cycles of length 5 only, so the fifth power is in the kernel of the permutation representation, whence $(xyz)^{10} = 1$.

8 A rewriting system for the icosahedral group

Recent techniques for Coxeter groups have given insight in how to produce a proper set of rewriting rules. By "proper" we mean what is usually called "confluent"; it has the effect that each input word can be successfully rewritten to the corresponding canonical word by use of the rewriting rules. Rather than presenting the rewriting rules explicitly, we give an algorithm for rewriting an input word $\mathbf{w} \in X^*$, where $X = \{x, y, z\}$ to the corresponding canonical element in $\widetilde{W}$. The present treatment comes from [BH], with a variation due to DuCloux and Casselman.

Consider the set Φ^+ of 15 positive roots of W again. The algorithm works with induction. Let us assume that, for $w = r_1 \cdots r_{k-1} r_k \cdots r_q$, where $r_i \in X$ for $i = 1, \ldots, q$, we have already established that $r_1 \cdots r_{k-1}$ is in canonical form.

Then, for $i = k-1, k-2, \ldots$ we consider the action of $r_i \cdots r_{k-1}$ on the fundamental root $\alpha \in \Pi = \{e_1, e_2, e_3\}$ corresponding to r_k. That is, we subsequently compute $r_{k-1}\alpha$, $r_{k-2}r_{k-1}\alpha$, and so on, until we reach a fundamental root again.

Say this happens the first time for $i \in \{1, \ldots, k-1\}$ and fundamental root β:

$$r_i r_{i+1} \cdots r_{k-1} \alpha = \beta.$$

Write $s = s_\beta$. Then, since $s_{g\gamma} = g s_\gamma g^{-1}$ for any $\gamma \in \Phi$ and $g \in GL(\mathbf{R}^3)$, we have

$$r_i r_{i+1} \cdots r_{k-1} r_k = s r_i r_{i+1} \cdots r_{k-1}.$$

If the right hand side represents a (lexicographically) smaller word, we substitute it for $r_i r_{i+1} \cdots r_{k-1} r_k$ and continue determining the canonical word for the first part $r_1 \cdots r_{i-1} s$ of $\mathbf{w}$. Otherwise, we leave things as they are ... except that we do not want to move to negative roots. This can only happen, if a fundamental root e_j occurs to which the corresponding reflection is applied (sending it to $-e_j$). This remarkable property is clearly visible from Figure 2, where only three edges make a root sink through the bottom line.

For further details, it is useful to write α_r for the positive root corresponding to a reflection r of W. Recall $\Pi = \{e_1, e_2, e_3\}$. Here is a full description of the canonical word algorithm:

At initialization: $\mathbf{w} = [r_1, \ldots, r_q] \in X^*$, representing $w = r_1 \cdots r_q \in W$; and an index $k := 1$.

At termination: $\mathbf{w}$ is the canonical word for w.

Invariants: $w \in W$ will be fixed throughout, and $\mathbf{w}$ will always be an expression for w. The first part of length $k-1$ of $\mathbf{w}$ is in canonical form.

while $k \leq \ell(\mathbf{w})$ **do**
  $i := k-1$; $\alpha := \alpha_{r_k}$;
  while $i > 0$ **do**
    $\alpha := r_i \alpha$;

case $\alpha \in \Phi^-$:
  $\mathbf{w} := [r_1, \ldots, r_{i-1}, r_{i+2}, \ldots, r_q]$;
  $k := k-1$; $i := i-1$;
case $\alpha \in \Pi$:
  if $[r_i, r_{i+1}, \ldots, r_k] > [s_\alpha, r_i, \ldots, r_{k-1}]$
  then $\mathbf{w} := [s_\alpha, r_j, \ldots, r_{k-1}]$;
    fi;
    $k := i$; $i := k-1$;
  otherwise: $i := i-1$;
 od;
 $k := k+1$;
od

For given i and k, the root $\alpha = r_i \cdots r_{k-1}\alpha_{r_k}$ is being considered. In case $\alpha \in \Phi^-$, we must have $i = k-1$; a fundamental root is reached by its corresponding reflection, we have $r_i = r_{i+1} = r_k$ and we can reduce length.

If a positive fundamental root $\alpha = r_i r_{i+1} \cdots r_{k-1}\alpha_{r_k}$ is hit, then we have seen above that the new expression generated by the algorithm represents the same element of W.

It may seem to be a computational difficulty that the root system is needed. But, in fact, the full action, in terms of images of roots under fundamental reflections, has already been stored in Figure 2. The roots there are pictured with respect to "depth": the number of fundamental reflections needed to turn them into negative roots: the fundamental roots have depth 1, the next layer up consists of $(1,1,0)$, $0,1,-\sigma)$ and $(0,-\sigma,1)$ (of depth 2), and so on, until we reach the unique one of depth 7: $(-\sigma, -2\sigma, -\tau-2\sigma)$.

A new rewriting rule that we obtain by applying the algorithm to the left hand side is $zyzyxz \Rightarrow yzyzyx$. Cor Baayen is encouraged to try and prove that $(xyz)^{10} = 1$ using the algorithm. (Hint: the rewriting rule $(yxz)^5 \Rightarrow (xzy)^5$ is crucial.)

We have seen that the positive root system, with its "depth" structure, and, above all, its W-action, is an excellent automaton for the "icosahedral" word problem. For a finite group like W, it may not be much of a surprise that we can find a solution to the word problem. The surprise however is that the technique described works for all Coxeter groups, including the infinite ones, once a little variation has been made that we shall now describe.

If we take W to be an arbitrary Coxeter group, the same algorithm may work again, but then the set of all positive roots may be infinite and so cannot be fully constructed in advance. The merit of Brink and Howlett is that they showed that in that case one can "truncate" the root system, and work with a finite part only. It runs as follows: define, for α and β positive roots, $\alpha \succ \beta$ if $(\alpha, \beta) \geq 1$ and $\alpha - \beta$ has non-negative coefficients (when written as a linear combination of fundamental roots). We then say that α dominates β. The domination relation is a partial ordering with (and this is the non-trivial result:) finitely many minimal roots. The "automaton" can then be restricted to the minimal roots, and a single additional element, denoted by $*$, replacing all non-minimal

elements. Whenever a minimal root is mapped onto a non-minimal root, the acceptance state $*$ is reached: this means that the word that is being rewritten is canonical (in the inner loop of the above algorithm), so that one can move up to the next value of k, without having to process the word any further to the left, lowering the parameter i).

9 Synthesis of Todd-Coxeter and Buchberger

It is well known that Buchberger's Gröbner basis algorithm can be seen as a particular case of the Knuth-Bendix procedure, in which confluent rewriting is guaranteed due to the successful completion in the context of polynomial algebras. More and more, I am convinced that the classical Todd-Coxeter coset enumeration procedure can also be seen as such. In particular, the success here is guaranteed by Mendelssohn's result described in §3. This is a line of research that I have only recently started to pursue, and I will only vaguely indicate what I have in mind.

Given a monoid M and a field k, we can define the monoid algebra $k\langle M\rangle$ (if M is a group, this comes down to the group algebra).

We study quotients of $k\langle M\rangle$ with repect to ideals I. Again a reduction ordering $<$ on M is useful. Not every monoid affords a reduction ordering, but the most important examples, the free monoid and the free abelian monoid (in which case M is a polynomial algebra!) on a finite alphabet do.

For

$$f = \sum_{m \in M} f_m m \in k\langle M\rangle,$$

with $f_m \in k$ (finitely many nonzero), we set

$$lt(f) = \max\{m \in M \mid f_m \neq 0\}.$$

Moreover, for any subset X of $k\langle M\rangle$, set:

$$M(X) = \{lt(f) \mid f \in X\} \quad \text{and} \quad O(X) = M \setminus M(X).$$

Theorem. *Let M be a monoid with a reduction ordering $<$, and suppose I is an ideal in $k\langle M\rangle$. Then the following statements hold.*

(i) $k\langle M\rangle = I \oplus k \cdot O(I)$.

(ii) $k\langle M\rangle / I \cong k \cdot O(I)$ *as vector spaces over* k.

(iii) $\forall\ f \in k\langle M\rangle\ \exists! g \in k \cdot O(I) : f - g \in I$.

In this setting, we write $g := Can(f, I)$, and refer to it as the canonical element corresponding to f. Observe that

$$Can(f, I) = Can(g, I) \Leftrightarrow f - g \in I;$$

A subset G of I is called a Gröbner basis if $(M(G)) = M(I)$, where (N), for a subset of M, denotes the semigroup ideal generated by N in M.

This approach can be found in [M].

Proposition. *Let M be finitely generated (Noetherian) and supplied with a reduction ordering. For each ideal I of $k\langle M\rangle$, there is a unique subset B of I satisfying:*

(i) $M(B)$ is a minimal generating set of $M(I)$;

(ii) the coefficient of $lt(b)$ in b is 1 for each $b \in B$;

(iii) $b = lt(b) - Can(lt(b), I)$ for each $b \in B$.

This set G is the so-called reduced Gröbner basis of I. The polynomial case occurs for $M = \mathbf{N}^n$. Then the already classical Buchberger algorithm finds a Gröbner basis for $M = \mathbf{N}^n$.

Thus, quotients of polynomial rings can be determined algorithmically. But this is inconceivable for the general case, since the word problem for groups is known to be unsolvable.

To see the connection with group presentations, start with a finitely presented group $G = \langle X \mid Y\rangle$. Take M to be the free monoid generated by $A = X \cup X^{-1}$ and total degree lexicographic ordering $<$ such that $x < y^{-1}$ for all $x, y \in X$. Now let I be the ideal of all $v - w \in k\langle M\rangle$ with $v, w \in M$ such that $vw^{-1} \in Y$. Here, we assume that xx^{-1} and $x^{-1}x$ are relators (i.e., belong to Y). Then $k\langle M\rangle/I$ is the group algebra of G over k. The set $O(I)$ of the above theorem coincides with the collection $\widetilde{G}$ of words in A^* which are minimal in the inverse image under $A^* \to G$ of an element in G.

It is a very useful fact that binomials are transformed into binomials under all operations involved in the Knuth-Bendix procedure, and also under the transformations obtained from a translation of the Todd-Coxeter enumeration to this setting. If a Gröbner basis is found for the ideal I, then, by the above proposition, and the "binomial invariance," a solution to the word problem for G has been found.

Let us return once more to the icosahedral group W. The algorithm of §8 uses only finitely many rewriting rules; they can be read off from Figure 2. A simple example is $[y, x, y] \Rightarrow [x, y, x]$, which corresponds to the element $yxy - xyx \in k\langle A\rangle$. The collection of all rules thus obtained, together with $x - x^{-1}$, $xx - 1$, $y - y^{-1}$, $yy - 1$, $z - z^{-1}$, $zz - 1$ will lead to a Gröbner basis for the ideal I, thus presenting a model to compute with the group algebra $k[W]$ in terms of $kO(I)$.

As remarked at the end of §8, such results are (at least theoretically) no surprise for finite groups like W (although the automaton is efficient). But, due to the results of Brink and Howlett, we have similar Gröbner bases for arbitrary (infinite) Coxeter groups.

10 Acknowledgments

I am grateful to Hans Sterk and Remko Riebeek for reading a preliminary version of this paper. I am greatly indebted to Hans Cuypers for making the figures.

Part of §4 is from joint preparations of a course with Hans Cuypers and Remko Riebeek. The bulk of §5 is from [CW94].

References

[A] A.V. Alekseevskii 1974, *Finite commutative Jordan subgroups of complex simple Lie groups*, Funct. Anal. and its Appl. 8 (1974), 277 – 279.

[BCN] A.E. Brouwer, A.M. Cohen, A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin, 1989.

[BH] B. Brink and R. Howlett, *A finiteness property and an automatic structure for Coxeter groups*, Math. Ann. 296 (1993), 179 – 190.

[CoG] A.M. Cohen and R.L. Griess, Jr., *On finite simple subgroups of the complex Lie group of type E_8*, Proc. Sympos. Pure Math. 47 (1987), Pt. 2, 367 – 405.

[CT] A.M. Cohen, P.H. Tiep, *Integral forms for Jordan subgroups*, preliminary preprint, Eindhoven, 1994.

[CW92] A. M. Cohen and D. B. Wales, *On finite subgroups of $E_6(C)$ and $F_4(C)$*, preprint, Eindhoven, 1992.

[CW93] A. M. Cohen and D. B. Wales, *Embedding of the group $L(2,13)$ in the groups of Lie type E_6*, Israel J. Math. 82 (1993), 45 – 86.

[CW94] A. M. Cohen and D. B. Wales, *Finite simple subgroups of semisimple complex Lie groups – a survey*, Como 1993 Proceedings.

[Gr] R.L. Griess, Jr., *Basic conjugacy theorems for G_2*, report, Ann Arbor, University of Michigan, 1994.

[K] F. Klein, *Vorlesungen über da Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig, 1884.

[M] T. Mora, *An introduction to commutative and non-commmutative Gröbner bases*, preprint, Genua, 1994.

[Se] J-P. Serre, *Les sous-groupes $PSL(2,p)$*, preliminary report, Paris, 1994.

[Spr] T.A. Springer, Private communication, Utrecht, 1994.

[Suz] M. Suzuki, *Group Theory I*, Chapter 2.5, Springer, Berlin, 1982.