GAP Computations with $O_8^+(5).S_3$ and $O_8^+(2).S_3$

THOMAS BREUER

Lehrstuhl D für Mathematik RWTH, 52056 Aachen, Germany

October 08th, 2006

Abstract

This note shows how to construct a representation of the automorphic extension G of the simple group $S = O_8^+(5)$ by a symmetric group on three points, together with an embedding of the normalizer H of an $O_8^+(2)$ type subgroup of $O_8^+(5)$.

As an application, it is shown that the permutation representation of G on the cosets of H has a base of length two. This question arose in [BGS11].

Contents

1	Overview	2
2	Constructing Representations of $M.2$ and $S.2$	2
	2.1 A Matrix Representation of the Weyl Group of Type E_8	2
	2.2 Embedding the Weyl group of Type E_8 into $\mathrm{GO}^+(8,5)$	3
	2.3 Compatible Generators of $M, M.2, S$, and $S.2 \dots \dots \dots \dots \dots \dots \dots$	3
3	Constructing Representations of $M.3$ and $S.3$	4
	3.1 The Action of $M.3$ on M	4
	3.2 The Action of S .3 on S	6
4	Constructing Compatible Generators of ${\cal H}$ and ${\cal G}$	7
5	Application: Regular Orbits of H on G/H	7
6	Appendix: The Permutation Character $(1_H^G)_H$	8
7	Appendix: The Data File	11
\mathbf{R}	eferences	11

1 Overview

Let S denote the simple group $O_8^+(5) \cong P\Omega^+(8,5)$, that is, the nonabelian simple group that occurs as a composition factor of the general orthogonal group $GO^+(8,5)$ of 8×8 matrices over the field with five elements.

The outer automorphism group of S is isomorphic to the symmetric group on four points. Let G be an automorphic extension of S by the symmetric group on three points. By [Kle87], the group S contains a maximal subgroup M of the type $O_8^+(2)$ such that the normalizer H, say, of M in G is an automorphic extension of M by a symmetric group on three points. (In fact, H is isomorphic to the full automorphism group of $O_8^+(2)$.)

Let S.2 and S.3 denote intermediate subgroups between S and G, in which S has the indices 2 and 3, respectively. Analogously, let $M.2 = H \cap S.2$ and $M.3 = H \cap S.3$.

In Section 2, we use the following approach to construct representations of M.2 and S.2. By [CCN⁺85, p. 85], the Weyl group W of type E_8 is a double cover of M.2, and the reduction of its rational 8-dimensional representation modulo 5 embeds into the general orthogonal group $\mathrm{GO}^+(8,5)$, which has the structure $2.O_8^+(5).2^2$. Then the actions of $\mathrm{GO}^+(8,5)$ and an isomorphic image of W in $\mathrm{GO}^+(8,5)$ on 1-spaces in the natural module of $\mathrm{GO}^+(8,5)$ yield M.2 as a subgroup of (a supergroup of) S.2, where both groups are represented as permutation groups on N=19656 points.

In Section 3, first we use GAP to compute the automorphism group of M. Then we take an outer automorphism α of M, of order three, and extend α to an automorphism of S. Concretely, we compute the images of generating sets of S and M under α and α^2 . This yields permutation representations of S.3 and its subgroup M.3 on $3N = 58\,968$ points.

In Section 4, we put the above information together, in order to construct permutation representations of G and M, on 3N points.

As an application, it is shown in Section 5 that the permutation representation of G on the cosets of H has a base of length two; this question arose in [BGS11].

In two appendices, it is discussed how to derive a part of this result from the permutation character $(1_H^G)_H$ (see Section 6), and a file containing the data used in the earlier sections is described (see Section 7).

2 Constructing Representations of M.2 and S.2

2.1 A Matrix Representation of the Weyl Group of Type E_8

Following the recipe listed in [CCN⁺85, p. 85, Section Weyl], we can generate the Weyl group W of type E_8 as a group of rational 8×8 matrices generated by the reflections in the vectors

$$(\pm 1/2, \pm 1/2, 0, 0, 0, 0, 0, 0)$$

plus the vectors obtained from these by permuting the coordinates, plus those those vectors of the form

$$(\pm 1/2, \pm 1/2)$$

that have an even number of negative signs. (Clearly it is sufficient to consider only one vector form a pair $\pm v$.)

```
gap> rootvectors:= [];;
gap> for i in Combinations( [ 1 .. 8 ], 2 ) do
>     v:= 0 * [ 1 .. 8 ];
>     v{i}:= [ 1, 1 ];
>     Add( rootvectors, v );
>     v:= 0 * [ 1 .. 8 ];
```

```
> v{i}:= [ 1, -1 ];
> Add( rootvectors, v );
> od;
gap> Append( rootvectors,
> 1/2 * Filtered( Tuples( [ -1, 1 ], 8 ),
> x -> x[1] = 1 and Number( x, y -> y = 1 ) mod 2 = 0 ) );
gap> we8:= Group( List( rootvectors, ReflectionMat ) );
<matrix group with 120 generators>
```

2.2 Embedding the Weyl group of Type E_8 into $GO^+(8,5)$

The elements in the group constructed above respect the symmetric bilinear form that is given by the identity matrix.

```
gap> I:= IdentityMat( 8 );;
gap> ForAll( GeneratorsOfGroup( we8 ), x -> x * TransposedMat(x) = I );
true
```

So the reduction of the matrices modulo 5 yields a group W^* of orthogonal matrices w. r. t. the identity matrix. The group $\mathrm{GO}^+(8,5)$ returned by the GAP function GO leaves a different bilinear form invariant.

In order to conjugate W^* into this group, we need a 2×2 matrix T over the field with five elements with the property that TT^{tr} is half of the upper left 2×2 matrix in the above matrix.

```
gap> T:= [ [ 1, 2 ], [ 4, 2 ] ] * One( GF(5) );;
gap> Display( 2 * T * TransposedMat( T ) );
    . 1
    1 .
gap> I:= IdentityMat( 8, GF(5) );;
gap> I{ [ 1, 2 ] }{ [ 1, 2 ] }:= T;;
gap> conj:= List( GeneratorsOfGroup( we8 ), x -> I * x * I^-1 );;
gap> IsSubset( largegroup, conj );
true
```

2.3 Compatible Generators of M, M.2, S, and S.2

For the next computations, we switch from the natural matrix representation of $GO^+(8,5)$ to a permutation representation of $PGO^+(8,5)$, of degree $N=19\,656$, which is given by the action of $GO^+(8,5)$ on the smallest orbit of 1-spaces in its natural module.

```
gap> orbs:= OrbitsDomain( largegroup, NormedRowVectors( GF(5)^8 ), OnLines );;
gap> List( orbs, Length );
[ 39000, 39000, 19656 ]
gap> N:= Length( orbs[3] );
19656
gap> orbN:= SortedList( orbs[3] );;
gap> largepermgroup:= Action( largegroup, orbN, OnLines );;
```

In the same way, permutation representations of the subgroup $M.2 \cong SO^+(8,2)$ and of its derived subgroup M are obtained. But first we compute a smaller generating set of the simple group M, using a permutation representation on 120 points.

```
gap> orbwe8:= SortedList( Orbit( we8, rootvectors[1], OnLines ) );;
gap> Length( orbwe8 );
120
gap> we8_to_m2:= ActionHomomorphism( we8, orbwe8, OnLines );;
gap> m2_120:= Image( we8_to_m2 );;
gap> m_120:= DerivedSubgroup( m2_120 );;
gap> sm1:= SmallGeneratingSet( m_120 );; Length( sml );
2
gap> gens_m:= List( sml, x -> PreImagesRepresentative( we8_to_m2, x ) );;
```

Now we compute the actions of M and M.2 on the above orbit of length N. For generating M.2, we choose an element $b_N \in M.2 \setminus M$, which is obtained from the action of a matrix $b \in 2.M.2 \setminus 2.M$.

(Note that M.2 is not contained in PSO⁺(8,5), since the determinant of b is -1 in the field with five elements.)

The group S is the derived subgroup of PSO⁺(8,5), and S.2 is generated by S together with b_N .

```
gap> s_N:= DerivedSubgroup( largepermgroup );;
gap> s2_N:= ClosureGroup( s_N, b_N );;
```

3 Constructing Representations of M.3 and S.3

3.1 The Action of M.3 on M

Let α be an automorphism of M, of order three. Then a representation of the semidirect product M.3 of M by $\langle \alpha \rangle$ can be constructed as follows.

If M is given by a matrix representation then we map $g \in M$ to the block diagonal matrix

$$\left[\begin{array}{cc}g&&\\&g^{\alpha}&\\&&g^{(\alpha^2)}\end{array}\right],$$

and we represent α by the block permutation matrix

$$\left[\begin{array}{cc} & & I \\ I & & \\ & I & \end{array}\right],$$

where I is the identity element in M.

So what we need is the action of α on M. More precisely, we need images of the chosen generators of M under α and α^2 .

The group M is small enough for asking GAP to compute its automorphism group, which is isomorphic with $O_8^+(2).S_3$; for that, we use the permutation representation of degree 120 that was constructed in Section 2.3.

```
gap> aut_m:= AutomorphismGroup( m_120 );;
```

We pick an outer automorphism α of order three.

```
gap> nice_aut_m:= NiceMonomorphism( aut_m );;
gap> der:= DerivedSubgroup( Image( nice_aut_m ) );;
gap> der2:= DerivedSubgroup( der );;
gap> repeat x:= Random( der );
>         ord:= Order( x );
>         until ord mod 3 = 0 and ord mod 9 <> 0 and not x in der2;
gap> x:= x^( ord / 3 );;
gap> alpha_120:= PreImagesRepresentative( nice_aut_m, x );;
```

Next we compute the images of the generators sml under α and α^2 , and the corresponding elements in the action of M on N points.

Finally, we use the construction described in the beginning of this section, and obtain a permutation representation of M.3 on $3N = 58\,968$ points.

3.2 The Action of S.3 on S

Our approach is to extend the automorphism α of M to S; we can do this because in the full automorphism group of S, any $O_8^+(2)$ type subgroup extends to a group of the type $O_8^+(2).3$, and this extension lies in a subgroup of the type $O_8^+(5).3$ (see [Kle87]).

The group M is maximal in S, so S is generated by M together with any element $s \in S \setminus M$. Having fixed such an element s, what we have to is to find the images of s under the automorphisms that extend α and α^2 .

For that, we first choose $x \in M$ such that $C_S(x)$ is a small group that is not contained in M. Then we choose $s \in C_S(x) \setminus M$, and using that s^{α} must lie in $C_S(C_M(s)^{\alpha})$, we then check which elements of this small subgroup can be the desired image.

Each element x of order nine in M has a root s of order 63 in S, and $C_S(x)$ has order 189. For suitable such x, exactly one element $y \in C_S(C_M(s)^{\alpha})$ has order 63 and satisfies the necessary conditions that the orders of the products of s and the generators of M are equal to the orders of the product of y and the images of these generators under α . In other words, we have $s^{\alpha} = y$.

```
gap> alpha:= GroupHomomorphismByImagesNC( m_N, m_N,
                 gens_m_N, gens_m_N_alpha );;
gap> CheapTestForHomomorphism:= function( gens, genimages, x, cand )
         return Order(x) = Order(cand) and
                ForAll([1 .. Length(gens)],
>
             i -> Order( gens[i] * x ) = Order( genimages[i] * cand ) );
> end;;
gap> repeat
      repeat
         x:= Random( m_N );
       until Order(x) = 9;
       c_s:= Centralizer( s_N, x );
      repeat
         s:= Random( c_s );
       until Order( s ) = 63;
      c_m_alpha:= Images( alpha, Centralizer( m_N, s ) );
      good:= Filtered( Elements( Centralizer( s_N, c_m_alpha ) ),
         x \rightarrow CheapTestForHomomorphism(gens_m_N, gens_m_N_alpha, s, x));
    until Length( good ) = 1;
gap> s_alpha:= good[1];;
gap> c_m_alpha_2:= Images( alpha, c_m_alpha );;
gap> good:= Filtered( Elements( Centralizer( s_N, c_m_alpha_2 ) ),
       x -> CheapTestForHomomorphism( gens_m_N_alpha, gens_m_N_alpha_2,
                                      s_alpha, x ) );;
gap> s_alpha_2:= good[1];;
```

Using the notation of the previous section, this means that the permutation representation of M.3 on 3N points can be extended to S.3 by choosing the permutation corresponding to the block diagonal matrix

$$\left[\begin{array}{cc} s & & \\ & s^{\alpha} & \\ & & s^{(\alpha^2)} \end{array}\right],$$

as an additional generator.

```
gap> outer:= s * ( s_alpha^alpha_3N ) * ( s_alpha_2^(alpha_3N^2) );;
gap> s3_3N:= ClosureGroup( m3_3N, outer );;
```

(And of course we have $S = \langle M, s \rangle$, which yields generators for S that are compatible with those of M.)

```
gap> s_3N:= ClosureGroup( m_3N, outer );;
```

4 Constructing Compatible Generators of H and G

After having constructed compatible representations of M.2 and G.2 on N points (see Section 2.3) and of M.3 and S.3 on 3N points (see Section 3.2), the last construction step is to find a permutation on 3N points with the following properties:

- The induced automorphism β of M extends to M.3 such that the automorphism α of M is inverted, modulo inner automorphisms of M.
- The action on the first N points coicides with that of the element $b_N \in M.2 \setminus M$ that was constructed in Section 2.3.

Using the notation of the previous sections, we represent β by a block diagonal matrix

$$\left[\begin{array}{cc} b & & \\ & & bd \\ & bg \end{array}\right],$$

where b describes the action of β on M (on N points), g describes the inner automorphism γ of M that is defined by the condition $\beta\alpha = \alpha^2\beta\gamma$, and d describes $\gamma\gamma^{\alpha}$.

So we compute an element in M that induces the conjugation automorphism γ , and its image under α . We do this in the representation of M on 120 points, and carry over the result to the representation on N points, via the rational matrix representation; this approach had been used already in Section 2.3.

So we have constructed compatible generators for H and G.

```
gap> h:= ClosureGroup( m3_3N, inv );;
gap> g:= ClosureGroup( s3_3N, inv );;
```

5 Application: Regular Orbits of H on G/H

We want to show that H has regular orbits on the right cosets G/H. The stabilizer in H of the coset Hg is $H \cap H^g$, so we compute that there are elements $s \in S$ with the property $|H \cap H^s| = 1$.

(Of course this implies that also in the permutation representations of the subgroups S, S.2, and S.3 of G on the cosets of the intersection with H, the point stabilizers have regular orbits.)

```
gap> repeat
> conj:= Random( s_3N );
> inter:= Intersection( h, h^conj );
> until Size( inter ) = 1;
```

Eventually GAP will return from this loop, so there are elements c with the required property.

(Computing one such intersection takes about six minutes on a 2.5 GHz Pentium 4, so one may have to be a bit patient.)

6 Appendix: The Permutation Character $(1_H^G)_H$

As an alternative to the computation of $|H \cap H^s|$ for suitable $s \in S$, we can try to derive information from the permutation character $(1_H^G)_H$. Unfortunately, there seems to be no easy way to prove the existence of regular H-orbits on G/H (cf. Section 5) only by means of this character.

However, it is not difficult to show that regular orbits of M, M.2, and M.3 exist. For that, we compute $(1_H^G)_{H}$, by computing class representatives of H, their centralizer orders in G, and the class fusion of H-classes in G.

We want to compute the class representatives in a small permutation representation of H; this could be done using the degree 360 representation that was implicitly constructed above, but it is technically easier to use a degree 405 representation that is obtained from the degree 58 968 representation by the action of H on blocks in an orbit of length 22 680. (One could get this also using the GAP function SmallerDegreePermutationRepresentation.)

Then we carry back class representatives to the degree $58\,968$ representation, and compute the class fusion and the centralizer orders in G.

```
> od;
> if not found then
> Add( fusreps, reps[i] );
> Add( fusion, Length( fusreps ) );
> Add( centralizers, cen );
> fi;
> od:
```

Next we compute the permutation character values, using the formula

$$(1_H)^G(g) = (|C_G(g)| \sum_h |h^H|)/|H|,$$

where the summation runs over class representatives $h \in H$ that are G-conjugate to g.

In order to write the permutation character w.r.t. the ordering of classes in the GAP character table, we use the GAP function CompatibleConjugacyClasses.

```
gap> tblh:= CharacterTable( "08+(2).S3" );;
gap> map:= CompatibleConjugacyClasses( Image( acthom ), ccl, tblh );;
gap> pi:= pi{ map };
[ 51162109375, 69375, 1259375, 69375, 568750, 1750, 4000, 375, 135, 975, 135, 625, 150, 650, 30, 72, 80, 72, 27, 27, 3, 7, 25, 30, 6, 12, 25, 484375, 1750, 375, 375, 30, 40, 15, 15, 15, 6, 6, 3, 3, 3, 157421875, 121875, 4875, 475, 75, 3875, 475, 13000, 1750, 300, 400, 30, 60, 15, 15, 15, 125, 10, 30, 4, 8, 6, 9, 7, 5, 6, 5 ]
```

Now we consider the restrictions of this permutation character to M, M.2, and M.3. Note that $(1_H^G)_M = (1_M^S)_M$, $(1_H^G)_{M.2} = (1_{M.2}^{S.2})_{M.2}$, and $(1_H^G)_{M.3} = (1_{M.3}^{S.3})_{M.3}$.

```
gap> tblm2:= CharacterTable( "08+(2).2" );;
gap> tblm3:= CharacterTable( "08+(2).3" );;
gap> tblm:= CharacterTable( "08+(2)" );;
gap> pi_m2:= pi{ GetFusionMap( tblm2, tblh ) };;
gap> pi_m3:= pi{ GetFusionMap( tblm3, tblh ) };;
gap> pi_m:= pi_m3{ GetFusionMap( tblm, tblm3 ) };;
```

The permutation character $(1_M^S)_M$ decomposes into 483 transitive permutation characters, and regular M-orbits on S/M correspond to regular constituents in this decomposition. If there is no regular transitive constituent in $(1_M^S)_M$ then the largest degree of a transitive constituent is |M|/2; but then the degree of 1_M^S is less than 483|M|/2, which is smaller than [S:M].

```
gap> n:= ScalarProduct( tblm, pi_m, TrivialCharacter( tblm ) );
483
gap> n * Size( tblm ) / 2;
42065049600
gap> pi[1];
51162109375
```

For the case of M.2 < S.2, this argument turns out to be not sufficient. So we first compute a lower bound on the number of regular M-orbits on S/M. For involutions $g \in M$, the number of transitive constituents $1_{\langle g \rangle}^M$ in $(1_M^S)_M$ is at most the integral part of $1_M^S(g)/1_{\langle g \rangle}^M(g) = 2 \cdot 1_M^S(g)/|C_M(g)|$; from this we compute that there are at most 208 such constituents.

As a consequence, M has at least 148 regular orbits on S/M.

Now we consider the action of M.2 on S.2/M.2. If M.2 has no regular orbit then the 148 regular orbits of M must arise from the restriction of transitive constituents $1_U^{M.2}$ to M with |U| = 2 and such that U is not contained in M. (This follows from the fact that the restriction of a transitive constituent of $(1_{M.2}^{S.2})_{M.2}$ to M is either itself a transitive constituent of $(1_M^S)_M$ or the sum of two such constituents; the latter case occurs if and only if the point stabilizer is contained in M.) However, the number of these constituents is at most 134.

Finally, we consider the action of M.3 on S.3/M.3. We compute that $(1_{M.3}^{S.3})_{M.3}$ has 205 transitive constituents, and at most 69 of them can be induced from subgroups of order two. This is already sufficient to show that there must be regular constituents.

7 Appendix: The Data File

The file o8p2s3_o8p5s3.g that can be found at

http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib/data/o8p2s3_o8p5s3.g

contains the relevant data used in the above computations. This covers the representations for the groups and the permutation character of $O_8^+(2).S_3$ computed in Section 6.

Reading the file into GAP will define a global variable $\mathsf{o8p2s3_o8p5s3_data}$, a record with the following components.

pi the list of values of the permutation character of $G = O_8^+(5).S_3$ on the cosets of its subgroup $H = O_8^+(2).S_3$, restricted to H, corresponding to the ordering of classes in the character table of H in the GAP Character Table Library (this table has the Identifier value "08+(2).3.2"),

dim8Q a record with generators for 2.M and 2.M.2, matrices of dimension eight over the Rationals, deg120 a record with generators for M and M.2, permutations of degree 120,

deg360 a record with generators for M, M.2, M.3, and <math>H, permutations of degree 360,

dim8f5 a record with generators for 2.M, 2.M.2, 2.S, and 2.S.2, matrices of dimension eight over the field with five elements.

deg19656 a record with generators for M, M.2, S, and S.2, permutations of degree 19656,

deg58968 a record with generators for M, M.2, M.3, H, S, S.2, S.3, and G, permutations of degree 58968,

 $\mathtt{seed405}$ a block whose H-orbit in the representation on 58 968 points, w.r.t. the action \mathtt{OnSets} , yields a representation of H on 405 points.

For each of the permutation representations, we have (where applicable)

```
M
                         \langle a_1, a_2 \rangle,
M.2
               \cong
                         \langle a_1, a_2, b \rangle,
M.3
              \cong
                         \langle a_1, a_2, t \rangle,
H
                         \langle a_1, a_2, t, b \rangle,
S
               \cong
                         \langle a_1, a_2, c \rangle,
S.2
               \cong
                         \langle a_1, a_2, c, b \rangle,
S.3
               \cong
                         \langle a_1, a_2, c, t \rangle,
G
               \cong
                         \langle a_1, a_2, c, t, b \rangle,
```

where a_1, a_2, b, t, c are the values of the record components a1, a2, b, t, and c.

Analogously, for the matrix representations, we have (where applicable)

```
2.M \cong \langle a_1, a_2 \rangle,
2.M.2 \cong \langle a_1, a_2, b \rangle,
2.S \cong \langle a_1, a_2, c \rangle,
2.S.2 \cong \langle a_1, a_2, c, b \rangle,
```

Additional components are used for deriving the representations from initial data, as in the constructions in the previous sections.

For example, most of the permutations needed arise as the induced actions of matrices on orbits of vectors; these orbits are computed when the file is read, and are then stored in the components orb120 and orb19656.

The file o8p2s3_o8p5s3.g does not contain the generators explicitly, but it is self-contained in the sense that only a few GAP functions are actually needed to produce the data; for example, it should not be difficult to translate the contents of the file into the language of other computer algebra systems.

Advantages of this way to store the data are that the relations between the representations become explicit, and also that only very little space is needed to describe the representations—the size of the file is less than 10 kB, whereas storing (explicitly) one of the permutations on 58 968 points requires already about 350 kB.

References

- [BGS11] T. C. Burness, R. M. Guralnick, and J. Saxl, On base sizes for symmetric groups, Bull. Lond. Math. Soc. 43 (2011), no. 2, 386–391. MR 2781219 (2012d:20003)
- [CCN⁺85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, Atlas of finite groups, Oxford University Press, Eynsham, 1985, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. MR 827219 (88g:20025)
- [Kle87] P. B. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups, J. Algebra **110** (1987), no. 1, 173–242. MR 904187 (88i:20070)