Sporadic and Related Groups

Lecture 1

Classification of finite simple groups

Steiner Systems

Classification theorem (summary)

All finite simple groups are either

- Cyclic groups of prime order
- Alternating groups
- Various sorts of matrix groups over finite fields
- One of the 26 Sporadic groups.

Cyclic groups of prime order

- Not much to say about these . . .
- Addition modulo p for p a prime

- These are the *Abelian* or commutative simple groups.

- The rest are the *non-Abelian* simple groups.

Alternating groups

- The *Symmetric* group on n letters is the group of all permutations on a set of size n
- Written as a permutation matrix, the determinant may be +1 or -1.
- Those with determinant +1 form the *Alternating* group on n letters
- For n at least 5, the alternating group is simple.

A close look at A_5

- I will examine A_5 for a few minutes to set the scene . . .
- On 5 points, there are 5! = 120 permutations in the symmetric group.
- Half of these are *even* – the alternating group has order 60.
- This is the smallest non-Abelian simple group.

A_5 is simple

- If it had a normal subgroup N . . .

If N were intransitive, the transitivity sets would all be the same size since A_5 is transitive. This is impossible since 5 is prime.

If N were transitive, it would contain a Sylow-5 subgroup, so all Sylow-5 subgroups (N normal) so (12345).(32145) = (354) so its conjugate(243) and <(354),(243)> is A_4 of order 12. Hence N has order divisible by 60 so is all of A_5

Another proof of simplicity

- There is 1 identity element.
- There are 24 five cycles – e.g. (12345)
- There are 15 elements like (12)(34)
- There are 20 elements like (123)

- Any normal subgroup must consist of some, but not all, of these, and have order dividing 60. No way!

Proofs of simplicity

- Are usually fairly elementary.
- The general idea is to get your hands on an element that has to be in any normal subgroup, then generate the whole group with its conjugates.
- These proofs are often fairly tedious, and I will usually be omitting them.

$L_2(p)$

- For any prime p, the set of 2 x 2 matrices of determinant 1 form a group of order p.(p+1).(p-1).
- If p is odd, the scalar matrices of determinant 1 is a central subgroup of order 2.
- The quotient is a group $L_2(p)$ of order p.(p+1).(p-1)/2

$L_2(q)$

- This can be generalized a little by taking the 2 x 2 matrices over any field (of order $q=p^n$) and taking the quotient by the scalars.
- For q at least 4, $L_2(q)$ is a non-abelian simple group.
- $A_5 = L_2(4) = L_2(5)$ so we don't get anything new until $L_2(7)$.

$L_n(q)$

- Of course this can be generalized further by taking the set of all n x n matrices of determinant 1 of the finite field of order q, and then quotienting out by the scalars.
- This group is called $L_n(q)$
- It is simple except $L_2(2)$ and $L_2(3)$

The non-abelian simple groups of order up to ten thousand.

60	A_5	3420	$L_2(19)$
168	$L_2(7)$	4080	$L_2(16)$
360	A_6	5616	$L_3(3)$
504	$L_2(8)$	6048	$U_3(3)$
660	$L_2(11)$	6072	$L_2(23)$
1092	$L_2(13)$	7800	$L_2(25)$
2448	$L_2(17)$	7920	M_{11}
2520	A_7	9829	$L_2(27)$

$U_3(3)$

- The set of 3 x 3 matrices over the field of order 9, such that the transpose inverse is equal to the Galois Automorph σ.
- $M'^{-1}=M^{\sigma}$ is a group because
- $(AB)'^{-1}= A'^{-1}.B'^{-1}=A^{\sigma}B^{\sigma}=(AB)^{\sigma}$
- Quotiented out, as always, by the scalars.
- “Various sorts of matrix groups over finite fields”

M_{11}

- Is the smallest sporadic group.
- It is a permutation group on 11 points, so it really isn't very big at all.
- Its order is 7920 = 11.10.9.8
- It is 4-transitive, and only the identity fixes four points.
- It is the ONLY finite group with that property.

Mathieu Groups.

- All the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24} can be found by considering "Steiner Systems".

- So now we look at Steiner Systems

Steiner System S(k,s,n)

Here is a little example – S(2,3,7)

123, 145, 167, 246, 257, 347, 356

Every 2-element subset is in precisely one 3-element “special” subset from a set of size 7

S(2,3,7) is unique 1 of 2

Theorem. The S(2,3,7) is unique.

We will call the elements of our set 1,2,3,4,5,6,7.

Clearly 1 has to appear exactly once with each of the others

So we might as well have 123 145 167, renumbering the set if necessary.

S(2,3,7) is unique 2 of 2

123 145 167

24 has to appear somewhere, and it can't be with 1 or 3 (123) nor with 5 (145) so it must appear with 6 or 7. Swapping 6 and 7 if necessary, wlog we have 246

123 145 167 246

25? It can only appear with 7 [check]

123 145 167 246 257

34 must be in 347 35 must be in 356

What group do we get out of this?

- Define the automorphism group of a Steiner system (and more generally any collection of subsets) to be the permutations of the points that preserve the special subsets as a whole.
- 123 145 167 246 257 347 356

(1234567) is **not** an automorphism as 123 → 234 and 234 is not a special subset.

An automorphism of S(2,3,7)

123 145 167 246 257 347 356

(1243675) is an automorphism

123 145 167 246 257 347 356 $\rightarrow$
246 231 275 437 415 635 617

The automorohism group of S(2,3,7)

- Is a simple group of order 168 = 7.6.4.
- In a way, we actually showed the order while proving uniqueness.
- We chose 1 and 2 arbitrarily, then 3 was determined (the one appearing with 1 and 2). 4 we chose arbitrarily and the rest was then determined.

In retrospect it is $L_3(2)$

- We can use the seven non-zero vectors of a three space over GF(2)
- And define a special subset to be the three vectors of a two-space.
- In other words (a,b,c) if a+b+c=0
- This is clearly an S(2,3,7)
- And so must be the one we have, since it is unique.
- The automorphism group is therefore the set of invertible 3x3 matrices over GF(2).

Simplicity?

- One (hard) way is to find the conjugacy classes of elements.

1 element of order 1

21 conjugate elements of order 2

42 conjugate elements of order 4

56 conjugate elements of order 3

24 conjugate elements of order 7

24 other conjugate elements of order 7

No proper subset of these numbers including 1 adds up to a divisor of 168.

Simplicity using permutations

- A normal subgroup of a transitive group is either itself transitive, or the transitive blocks are all the same size.
- Since 7 is a prime, any normal subgroup is transitive . . .
- So contains a Sylow-7 subgroup
- So contains all Sylow-7 subgroups
- *Which generate the whole group – messy.*

What small Steiner Systems are there?

If there is an S(k,s,n), taking all the sets containing one of the points we get an S(k-1,s-1,n-1).

For example from

123 145 167 246 257 347 356, if we look at the special subsets containing 7 we get

16 25 34 – an S(1,2,6)

S(1,s,rs) and S(k,s,s) exist.

- For example there is the rather trivial Steiner system S(1,3,12)

(1,2,3) (4,5,6) (7,8,9) (10,11,12)

Similarly if we take the set of size s, every k-set is contained in just one set!

The number of sets must be an integer.

- So there cannot be an S(2,3,11) since there are 11.10/2 pairs of elements, and three pairs occur in each special subset, so there must be 11.10/2.3 = 55/3 special subsets!

Small Steiner Systems

S(2,3,7) – 7.6/2.3 = 7 sets

S(3,4,8) – 8.7.6/4.3.2 = 14 sets

S(2,3,9) – 9.8/2.3 = 12 sets

S(3,4,10) – 10.9.8/4.3.2 = 30 sets

S(4,5,11) – 11.10.9.8/5.4.3.2 = 66 sets

S(5,6,12) – 12.11.10.9.8/6.5.4.3.2 = 132 sets

The last two exist, and their automorphism groups are the sporadic groups M11 and M12

S(3,4,8)

We have the unique S(2,3,7), so we can start by sticking an 8 on the end of these

1238 1458 1678 2468 2578 3478 3568

The other 7 sets (there are 14 in all) must come from 1234567 and miss 8.

124? Cannot have 3,5,6 so must have 7, which is the exact complement of 356.

The same argument applies in every case

So S(3,4,8) is unique also

1238 1458 1678 2468 2578 3478 3568

4567 2367 2345 1357 1346 1256 1247

We can think of these as cosets of any 2^2 in a 2^3 showing that the automorphism group is at least $2^3L_3(2)$

In fact it is exactly this group.

S(2,3,9) 1 of 3

Without loss of generality, we have

123 145 167 189.

We need 9.8/2.3 = 12 sets. Four we have. There must be three more containing 2 and three more containing 3, and they must be all different.

There are therefore 12-4-3-3 = 2 sets without any of 1,2,3 and each of 4,5,6,7,8,9 must occur in one of them since they occur in at most three of the 10

Wlog these two sets are 468 and 579

S(2,3,9) 2 of 3

123 145 167 189 468 579

24 can’t appear with 1,2,3,4,5,6,8 so 7 or 9, but (68)(79) is an automorphism of what we have so far, so wlog 247

Now 28 can only appear with 5 and that leaves 269

S(2,3,9) 3 of 3

123 145 167 189 247 258 269 468 579

Now 34 can only go 9

35 can only go with 6 and that leaves 378

And we finally get

123 145 167 189 247 258 269 349 356 378 468 579

Which works!

Or we might make S(2,3,9) as

The set of elements in the group 3 x 3, and make a special set out of any three that add up to the identity.

A little thought will convince you that this is indeed an S(2,3,9)

And shows that the automorphism group is at least 3^2:GL(2,3) of order 432.

In fact it is exactly this group.

Sporadic and Related Groups

Lecture 2

M11 and M12

End of last lecture

There is a unique S(2,3,9), namely

123 145 167 189 247 258 269 349 356 378 468 579

Lemma. In S(2,3,9), if any two special sets are disjoint, the remaining points are also a special set.

Onwards to S(3,4,10)

I will take the ten points to be 123456789X, as “X” is more concise than “10”

We can start by sticking an X on the end of our S(2,3,9)

123X 145X 167X 189X 247X 258X 269X 349X 356X 378X 468X 579X

The lemma tells us

- If we have any two sets containing precisely one common point, that point and the three remaining points are a special set.
- But all the sets we have so far contain X, so the lemma can only give us sets containing X
- We need one more set

One more set

123X 145X 167X 189X 247X 258X
269X 349X 356X 378X 468X 579X

124? Can't have any of 123X 145X 247X so must have 6, 8 or 9.

But (1 2 4) (3 7 5) (6 8 9) is an automorphism of what we have so far

So wlog we have 1246

Now we are really cooking.

- 123X 145X 167X 189X 247X 258X 269X 349X 356X 378X 468X 579X 1246
- Now 1246 189X implies 1357 by the lemma.
- 1357 349X gives 2368
- And so on

S(3,4,10) is unique

- I could have done all the work and listed the 30 sets of size 4.

- An “exercise” for the student!

(8) Automorphisms of S(3,4,10)

Automorphism group is actually $S_6.2$ – the full automorphism group of S_6, which has an exceptional outer automorphism.

How do we see that S_6 has an outer automorphism . . . ?

One way is that S_5 has a subgroup of order 20, so index 6. So S_5 can act transitively on 6 points – by acting on the cosets of this group of order 20.

S_6 outer automorphism

- So S_6 contains a subgroup S_5 that is not the point stabilizer, and permuting the cosets of this, we get an action of S_6 on 6 points that we were not expecting.

- This automorphism swaps duads (12) with *synthemes* (12)(34)(56) and swaps three-cycles (123) with pairs of three cycles (123)(456).

Another proof

(12), (23), (34), (45), (56) is the normal way of generating S_6 with five elements of order 2, adjacent pairs having product order 3 and non-adjacent pairs having product order 2.

This is a **presentation** of S_6

One can get good at S6

A duad and syntheme are *incident* if the duad is one of the cycles of the syntheme

e.g. (12) is incident with (12)(34)(56)

Two duads [synthemes] commute if and only if they are incident to a single syntheme [duad]. Otherwise they have product of order three.

Explicit map

$$(12) \rightarrow (12)(34)(56)$$
$$(23) \rightarrow (15)(24)(36)$$
$$(34) \rightarrow (12)(35)(46)$$
$$(45) \rightarrow (13)(24)(56)$$
$$(56) \rightarrow (12)(36)(45)$$

What has this to do with S(3,4,10)?

Take a set of six points. To avoid confusion with the 10 points of S(3,4,10) I will take the six points to be a,b,c,d,e,f.

There are 6.5.4/2.3.2 = 10 ways of splitting the six points into two sets of size 3. These will be the ten points of our Steiner system.

Making S(3,4,10)

- Given a duad (ab) there are four splittings with these two points in the same part. We will take these as a special set.
- Given a syntheme (ab)(cd)(ef) there are four splittings where the bracketed pairs are always in opposite parts. We will take these as a special set also.
- This gives us 15 [duad) and 15 [syntheme] sets of four points. This is S(3,4,10).

Why is this a Steiner system

- Given any three splittings of a set of size six into two sets of size 3, there is always *either* a unique duad that always appears together, *or* a unique syntheme that always separates them.
- abc/def ade/bcf aef/bcd ? (bc)
  so other one is adf/bce
- abc/def ade/bcf abe/cdf ? (af)(bd)(ce)
  so other one is acd/bef

Suppose I should prove that

- Wlog first splitting is abc/def
- All nine other splitting are obtained by picking one point in each half and swapping them, so wlog second is abd/cef
- For the third one, we must either chose one same point and one different one, or two different points to swap.
- So the two cases on the previous slide is all there is!

(17) S(4,5,11)

The same sort of methods enable us to show that S(4,5,11) is unique. We take a new symbol E(leven) and stick it on the end of each of the 30 sets of size four from S(3,4,10).

We then pick four elements (not including E) that do not yet appear in a special set. We find that there are just two possibilities for the fifth, and that there is an automorphism of what we have that swaps them. Hence wlog we have a new special set.

The Lemma does the rest

- Our lemma now says that if we can find two sets with precisely two points in common, those two points and the remainder form a special set.

The result works.

- We get a collection of 66 sets of size 5, such that every four points is in exactly one of them.
- As everything was unique, the automorphism group must be transitive, and indeed if we are careful, we know that its order is 7920. This is our first sporadic group M_{11}.

Onwards do S(5,6,12)

- Looking at the (unique) S(4,5,11) we can see that no two special sets are totally disjoint. Therefore in any S(5,6,12) there cannot be two special sets sharing exactly one point. If we take any set of S(4,5,11) and take five of the points not in it, the set of size 6 containing them can only be in the complementary set.
- Hence we get every S(5,6,12) from S(4,5,11) merely by adding the complementary sets.

Mathieu groups are multiply transitive.

- In the 1860's and 1870's, Mathieu was looking for groups (other than Sn and An) that were multiply-transitive.
- (n-transitive means that the group is transitive on ordered n-tuples)
- For n as high as 4, there are only the Mathieu groups M_{11} M_{12} M_{23} M_{24}.
- This is only proved using classification.

M_{11} and M_{12} are ***sharply*** transtive.

In particular, M_{11} is transitive on ordered 4-tuples, but only the identity fixes any 4-tuple.

Jordan proved in 1872 that this is the only case of this apart from the trivial cases of S_4 S_5 and A_6

We will prove this now, assuming there are at least seven points to exclude the trivialities

Main idea of Jordan's theorem

- By bare hands, work out what the permutations must actually be
- By 4-transitivity, there is a permutation taking any four points chosen to any other (or indeed the same) four points in any order.
- But if two permutation act the same on 4 points, they must actually be the same.

(24) We first find a fourgroup

- Looking first at permutations on the first four points, we must have a four-group of given by the following permutations

a = (1)(2)(34)…

b = (12)(34)…

ab= (12)(3)(4)…

All involutions conjugate

Since there are at least 7 points, any element of order 2 must move at least 4 of them. There is a permutation bringing these four points to 1234, so any involution is conjugate in G to b.

Since a and b are conjugate, and a fixes at least 2 points, so does b ,but none can fix as many as four points. Since a and b commute, a must stabilize the set of points fixed by b, so wlog moves two of them. Hence we have . . .

Getting up to six points

a = (1)(2)(34)(56) …

b = (12)(34)(5)(6) …

ab=(12)(3)(4)(56) …

Except that there may be a point (call it 0) that is fixed by both a and b, no other point is fixed by any of a, b or ab as otherwise they would fix four or more points.

Hence we must have the permutations at the top of the next slide.

There cannot be more than 11 points

a = (0?) (1)(2)(34)(56) (ij)(kl) …

b = (0?) (12)(34)(5)(6) (ik)(jl) …

ab=(0?) (12)(3)(4)(56) (il)(jk) …

Now suppose that the ijkl part were repeated.

Then there would be a permutation x taking $i_1j_1k_1l_1$ to $i_2j_2k_2l_2$, and this would centralize a, b and ab. Since we already see all the points that a,b and ab can fix, x would have to fix or swap 1,2, fix or swap 3,4 and fix or swap 5,6. In each case at least 4 points are fixed by one of x, ax, bx and abx, which cannot be the identity since it moves i_1

On 7 or 10 points

If there are 7 points, the stabilizer of two points would be 5.4 and the setwise stabilizer have this as a normal subgroup of index 2. As 5.4 has no automorphisms, an element swapping the two points would have to fix the remaining 5.

If there were 10 points, the stabilizer of three points would have order 7 and the setwise stabilizer would be $7.S_3$. As S_3 does not act on a cyclic 7, the element of order 3 would have to centralize it and so fix seven points.

On 11 points

- With a little thought, one can show from sharp 4-transitivity alone, that the 3-point stabilizer is a quaternion group of order 8, that the two point stabilizer is (3 x 3).Q_8 that the 1-point stabilizer is A_6.2 and readily find another permutation that generates M_{11} and indeed another that generates M_{12}
- The theme is, as always, that the very existence if these groups is amazing, and therefore at every stage you have little choice but to do the right thing (or make a mistake!)

(30) Sharply 5-transitive groups

- The point stabilizer would have to be a sharply 4-transitive group, which must be on 11 points.
- In fact there is a sharply 5-transitive group on 12 points – M_{12}
- Order 12.11.10.9.8 = 95040

But does all this exist?

- All that I have shown so far is that if there is a sharply 4-transitive group it is M_{11} and that there is at most one S(4,5,11) and if there is, its automorphism group (more-or-less) has order 7920.

- I know of no really slick, easy way of showing that any of this actually works.

One way is to make S(4,5,11)

- There are only 66 blocks, each of size 5, so it is not too hard to write them all out.
- One must then show that every 4-set (of which there are 330, occurs in one of these blocks.
- This (along with some care in the uniqueness stages) shows that the automorphism group has order 7920

Or use permutations

- Again after listing the 66 blocks, one can check by hand that two particular permutations fix the system, then show that the permutations generate a 4-transitive group, hence one only has to check that one! 4-tuple is contained in a block.

How many pentads

Since the number of sets with various intersection sizes is determined by the fact that it is a Steiner system, the table below is a convenient summary.

66

30 36

12 18 18

4 8 **10** 8

1 3 5 5 3

1 0 3 2 3 0

The marked 10, for example, indicates that there are 10 pentads containing any point and avoiding two others

M_{12}

One readily sees that in S(4,5,11) no two sets are disjoint.

This does give us a slick way, once we have our S(4,5,11) and M_{11}, of showing that there is an S(5,6,12) and a group M_{12}

One can therefore see immediately that the S(4,5,11) with a “12” stuck on each, along with the 66 complementary sets forms an S(5,6,12), so M_{12} comes easily.

S(5,6,12)

Take the S(4,5,11), and take 132 sets – 66 of them the sets of the S(4,5,11) with “12” added, and the other 66 the complements of the sets of the S(4,5,11).

I claim this is an S(5,6,12).

Any five points including 12 are clearly in a (unique) set since S(4,5,11) is a Steiner System.

The sets of size 5 are either a special set or in a complement.

There are 11.10.9.8.7/120 = 462 sets of size 5 from 11. 66 of them are the special sets of S(4,5,11), leaving 396. The complement of a special set contains 6 such 5-sets, so this also gives a list of 396 sets of size 5, but if two complements had a 5 set in common, the two original sets would be made from the remaining six points, so would have four points in common. Thus the 5 sets are all different and our system is indeed an S(5,6,12)

Sporadic and Related Groups

Lecture 3

Introduction to M_{24}

M_{24}

- Probably the most “important” of the sporadic groups.
- Occurs in the Conway groups, the Fischer groups and the group J_4
- Is related in some way or other to 21 of the 26 sporadic groups.
- I will therefore take two lectures on it
- This first will just be a rather dry statement of facts.
- I will amplify some of the statements in the second lecture.

Whole vocabulary for M_{24}

Octad, dodecad, duum, sextet, octern, trio are all words that are used with precise technical meaning specifically in the context of this group.

The Mathieu group M_{24}

Take any matrix C with entries mod 2 (or indeed in any field).

Consider the set of pairs of matrices L_i and R_i such that $L_i.C.R_i = C$.

Given two such pairs, we can form their product $(L_i,R_i)\ (L_j,R_j) = (L_jL_i,R_iR_j)$ which is also a pair since $L_jL_i.C.R_iR_j = L_j.C.R_j = C$.

If we wish (and in this case we do wish) we may restrict R to be a permutation matrix.

We then call C a code and the (column) permutations R_i to be its automorphism group

Example – the Hamming code

C = 0001111 (1243675) = 1010101
0110011 0001111
1010101 1100110

The set of all permutations fixing the mod-2 span of these rows has order 168.

It is a bit easier to check that a permutation works, since you only have to check it on a basis.

The Hamming code (II)

The zeros of the seven non-zero rows occur in the places of the S(2,3,7)

r1	0001111	123
r2	0110011	145
r3	1010101	246
r1+r2	0111100	167
r1+r3	1011010	257
r2+r3	1100110	347
r1+r2+r3	1101001	356

Example – the hexacode

Take the field of order 4 to be {0,1,w,v}

C = 0 1 0 1 w v so has 4^3=64 vectors

1 0 1 0 w v

0 0 1 1 1 1

We allow monomial permutations – take a column to another column multiplied by a non-zero field element

The group is then 3.A6

(8) Further examples

- Include the tetracode and the Golay (3) code which are over the field of order 3 and can be used to construct M_{12}.

- It seems, however, that – in some sense – Steiner Systems and Codes both “run out of steam” somewhere around here, and are only genuinely useful for the Mathieu groups.

Take C to be the matrix

001010001100011010010000
000101000110001101001000
000010100011000110100100
000001010001100011010010
100000101000110001101000
010000010100011000110100
001000001010001100011010
100100000101000110001100
010010000010100011000110
101001000001010001100010
110100100000101000110000
111111111111111111111111

The permutations

a=(1,23,24) (2,3,22) (4,5,21) (6,19,20)
(7,11,18) (8,9,10) (12,16,17) (13,14,15)

b=(1,24) (2,23) (3) (4,22) (5) (6,21) (7,19) (9)
(8,11) (10) (12,18) (13,16) (14) (15) (17)
(20)

both fix the mod-2 span of C and in fact generate M_{24} of order 24.23.22.21.20.48

M_{24}

- It is not too hard to verify the following facts by hand, and though I did plan to show you some of them, they really are just a bit too long to do in this lecture.
- The first step is to notice that the product a.b of the two permutations given is (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17, 18,19,20,21,22,23) (24).

Experimental use of computer

- One could, of course, find the 12 x 12 matrices that pair with the two permutations given.
- Even if you use a computer to find them, you can still check by hand that they work.
- It is a moot point whether this is a computer-free proof of existence!
- Anyway – I decided that even this was too much like hard work.

M_{24} is 5-transitive

- M_{24} is clearly transitive, and the product ab fixes point 24 and rotates the remaining 23, so M_{24} is 2 transitive. A little further pratting about will produce a few more permutations that show that it is 2-, 3-, 4- and 5-transitive.
- It is not 6-transitive.

The (extended) Golay code

1 set of size 0

759 sets of size 8 - the special octads

2576 sets of size 12 – the dodecads

759 sets of size 16-complements of octads

1 set of size 24

====

$4096 = 2^{12}$

Steiner system

- The 759 octads form a Steiner System S(5,8,24)
- This is clear because M_{24} is 5-transitive, and one set of size 5 is contained in an octad, so they all are.
- Counting then shows they are contained in only one.
- M_{24} could be constructed via the Steiner System, but it is much easier to verify only 12 things rather than 759.

(16) The code is called the **Golay code**

- It was discovered by a communciations engineer called Golay
- He noticed that

  $1 + 23 + 23.22/2 + 23.22.21/6$

  $=1 + 23 + 253 + 1771 = 2048 = 2^{11}$

And wondered if it was possible to choose 2^{11} codewords of length 23 such that every string of 2^{23} 1s and 0s was distance at most 3 from one of the codewords

And of course it is possible

- The automorphism group is M_{23}
- The length 23 Golay code contains words of odd and even weight (number of 1s) and the minimum distance between codewords is 7.
- By simply adding a parity bit (the “extended” Golay code) the minimum distance is increased to 8.

Why was he interested

- Because if you transmit the codewords and only three (!) errors are made, you can still tell what codeword was sent.
- It is therefore a three-error-correcting code
- It was later used to transmit data from mars by the Mariner spacecraft.

Maximal subgroups of M_{24}

- Stabilizing one point – the sporadic group M_{23}.
- Stabilizing a set of size 2, the sporadic group M_{22} with an outer automorphism (the elements swapping the two points)
- Stabilizing a set of size 3 – the simple group $L_3(4)$ with an automorphism group of order 6 (S_3) permuting the three points,

Remaining maximal subgroups of M_{24}

- A group $2^6.3.S_6$ stabilizing a ***Sextet***
- A group $2^4.A_8$ stabilizing an ***Octad***
- A group $M_{12}.2$ stabilizing a ***Duum***
- A group $L_2(7)$ stabilizing an ***Octern***
- A group $2^6.(L_2(7)xS_3)$ stabilizing a ***Trio***
- A group $L_2(23)$

Sextet

- Modulo the Golay code, every set is either
- A set of size 0, 1, 2 or 3
- Or six disjoint sets of size 4, any two of which add up to a special octad.
- Called a sextet (6 lots of 4!)
- The stabiliser of the splitting of 24 points into 6 sets like this is a maximal subgroup of the form $2^6.3.S_6$

Octad

- The stabilizer of a Golay codeword of size 8 is a group of the form $2^4.A_8$. This demonstrates the isomorphism between A_8 (the way it acts on the 8 points of the octad) and $L_4(2)$ (the way it acts on the other 16 points).

Duum

- A Golay code set of size 12 is stabilized by a group M_{12}. The other 12 points are also a codeword, and the subgroup stabilizing the pair is $M_{12}.2$ - M_{12} with an outer automorphism.
- Just like in the case of S6 with S5, this results from the fact that M_{12} contains another subgroup M_{11} of index 12 besides the point stabiliser (of index 11).

(24) Trio

- Trio = Three disjoint Octads.
- If two octads are disjoint, the remaining 8 points are also an octad.
- The stabilizer of the splitting of 24 into three disjoint octads is a group of the form $2^6.(L_2(7)xS_3)$

$L_2(23)$ and Octern

- There are two subgroups of M_{24} that are not so clear from the Golay code, namely $L_2(23)$ and $L_2(7)$. Actually $L_2(23)$ can be used to construct the code and group in the first place, and many authors do this.
- The maximal subgroup $L_2(7)$ – the octern group – is actually the centralizer of a fixed-point-free permutation of order 3 (not in M_{24})

M_{24} is a truly sporadic group

- Once M_{24} has been shown to exist, its subgroups must all exist also, demonstrating all sorts of exceptional behaviour, including
- The sporadic subgroups M_{23} M_{22} M_{12} M_{11}
- The exceptional automorphism of S_6
- The exceptional triple-cover of A_6
- The isomorphism of A_8 and $L_4(2)$

MOG

- The best way to really get your hands dirty with M_{24} is to use the

  MOG = **M**iracle **O**ctad **G**enerator,

  invented by Rob Curtis.
- Works of J. H. Conway (including the ATLAS and “three lectures on exceptional groups”) describe this more effectively than I could in a lifetime

Preview of the Conway group

- In 24 dimensions with the usual quadratic form, take 24-tuples of integers $V=v_i$ such that they are all odd or all even and such that . . .
- If they are all even, the places where v_i is 2 (mod 4) is a Golay code word and their sum is divisible by 8.
- If they are all odd, the places where they are 1 mod 4 is a Golay code word and their sum is 4 (mod 8)
- This is the Leech Lattice, whose automorphism group is a sporadic Conway group $2.Co_1$.

The Monster

- Has a group of the form $2^{1+24}.Co_1$ from which it has been constructed.
- This huge group does not seem to be capable of easy understanding
- But apply to Richard Borcherds if you want a second (different) opinion!

Preview of F_{24}

- Fischer's sporadic groups are generated by "2-3 transpositions".
- A maximal commuting set of transpositions is called a "base".
- In F_{24} a base has 24 commuting transpositions identified with the points of M_{24}, generating a group of order 2^{12} where a product is the identity if and only if the corresponding set is a codeword.

Preview of J_4

- J_4 has a subgroup of the form $2^{11}.M_{24}$ which, although not appearing to explain or construct the group, does at least add some understanding to this impenetrable large sporadic group.

Sporadic and Related Groups

Lecture 4

Discovering M_{24}

Some properties of M_{24}

- Take a set of 24 “points”.
- M_{24} fixes (setwise) a collection of 4096 = 2^{12} subsets called the extended Golay code.
- These sets are closed under add mod 2 / symmetric difference / exclusive-or.
- The 4096 sets all have sizes 0[1], 8[759], 12[2576], 16[759],24[1]
- All sizes are 0 mod 4, Which is only possible for dimensions divisible by 8, though I know no elementary proof.
- So any two have even intersection.

So we take . . .

Our 24 points in a 4 x 6 array, and use little pictures to show things about them.

Of course we choose each brick to be an octad (there are three disjoint octads)

x x x x x x

x x x x x x

x x x x x x

x x x x x x

Curtis' MOG

- 4 x 2 array (the [first] "brick") and
- 4 x 4 array (the "square")

Making 24 points in all.

These 24 points have lots of structure.

Please take one.

Octad Generation property

- An “octad” is an 8 point set in the (extended) Golay code
- Or one of the special sets in the S(5,8,24)
- The MOG gives all the octads that meet the first brick in precisely four points.

The trio is shown

- The square can be divided into two further bricks, and the S3 of permutations bodily permuting them (without changing the positions of points within bricks) are in M_{24}

The three bricks of the trio

x x x x x x
x x x x x x
x x x x x x
x x x x x x

The octads

- Every pair of octads have even intersection.
- Any octad that isn’t actually one of the three bricks must meet one of the bricks in exactly four points.
- All octads for the first brick are shown
- The rest can be obtained by bodily permuting the bricks.

(8) Hence one can use the MOG to find octads

Example S(5,8,24) so every five points are in an octad. So which octad contains

```
_  *  _  _  *  _
_  _  _  _  _  *
*  _  _  _  _  _
_  _  *  _  _  _
```

Answer can be seen in the third picture.

```
*  *  _  _  *  _      Use the black in the brick
_  _  _  _  _  *      and the dots in the square
*  _  _  *  _  _
*  _  *  _  _  _
```

The Sextets

- A sextet is a partition of 24 points into six sets of 4 points, such that the union of any two is an octad.
- Given any four points, the sextet is determined.
- Thirty-five sextets are shown in the MOG.
- These are the thirty-five such that one of the sets of four lies in the brick (so another one does also!)

$L_2(23)$ numbering

- Is shown in the first “picture”.

- $z \to [az + b] / [cz + d] \pmod{23}$ (z in $\{\infty,0,1,2,\ldots,22\}$) are all in M_{24}
- For example $z \to z + 1$ is an element of order 23 that takes 0 to 1, so takes the top left of the brick to the top left of the square.

Hexacode

- For really serious M_{24} engineers, the best tool to use is the hexacode.
- This is a three-dimensional code over F_4 – the field of 4 elements – that can be used to construct the Golay code in its most convenient form.
- (A very subjective statement!)

Reference – this section follows closely from . . .

- Chapter 11
- “The Golay Codes and The Mathieu Groups”
- In “Sphere Packings, Lattices and Groups
- J.H.Conway and N.J.A.Sloane
- Springer-Verlag 1988

Field of order 4

I still haven't found a way of writing "omega-bar" in power point, so I will use the following (hideous) notation

0 Nought

1 One

w Omega

v Omega-bar

In case you don’t know the field of order 4

Addition

	0	**1**	**w**	**v**
0	0	1	w	v
1	1	0	v	w
w	w	v	0	1
v	v	w	1	0

Multiplication

	0	**1**	**w**	**v**
0	0	0	0	0
1	0	1	w	v
w	0	w	v	1
v	0	v	1	w

Hexacode Definition 1

The code spanned by

w v w v w v

w v v w v w

v w w v v w

v w v w w v

The sum of these four vectors is zero, but they span a three space.

(16) Hexacode Definition 2

The code has a word a b c d e f for each quadratic polynomial $p(x) = a.x^2 + b.x + c$ where d=p(1) e=p(w) and f=p(v).

Four checks of the form $p(x)= w.x^2 + v.x + w$,

then p(1)=v; p(w)=w.w.w+v.w+w=1+1+w=w

p(v)=w.v.v+v.v+w=v+w+w=v so w v w v w v from definition 1 is in this code also.

Symmetries of Hexacode

- Scalar multiplication by an element of F_4
- Swapping the two digits in exactly two of the couples.
- Bodily permuting the three couples.

Can get to one of

0101wv	wvwvwv	001111	00wwvv	000000
36	12	9	6	1

Since the first is more than half of the code, it is worth memorizing.

Oh-one-oh-one-omega-omegabar

Hexacode can be used for data sharing

Given a value (in F_4) on any three of the six positions, there is exactly one hexacode word taking those values there.

Hence if a file (divided up into chunks of six bits) is used to select hexacode words, six files (one column each) can be made, each 1/3 of the size of the original, such that any three of the files allow the original to be reconstituted.

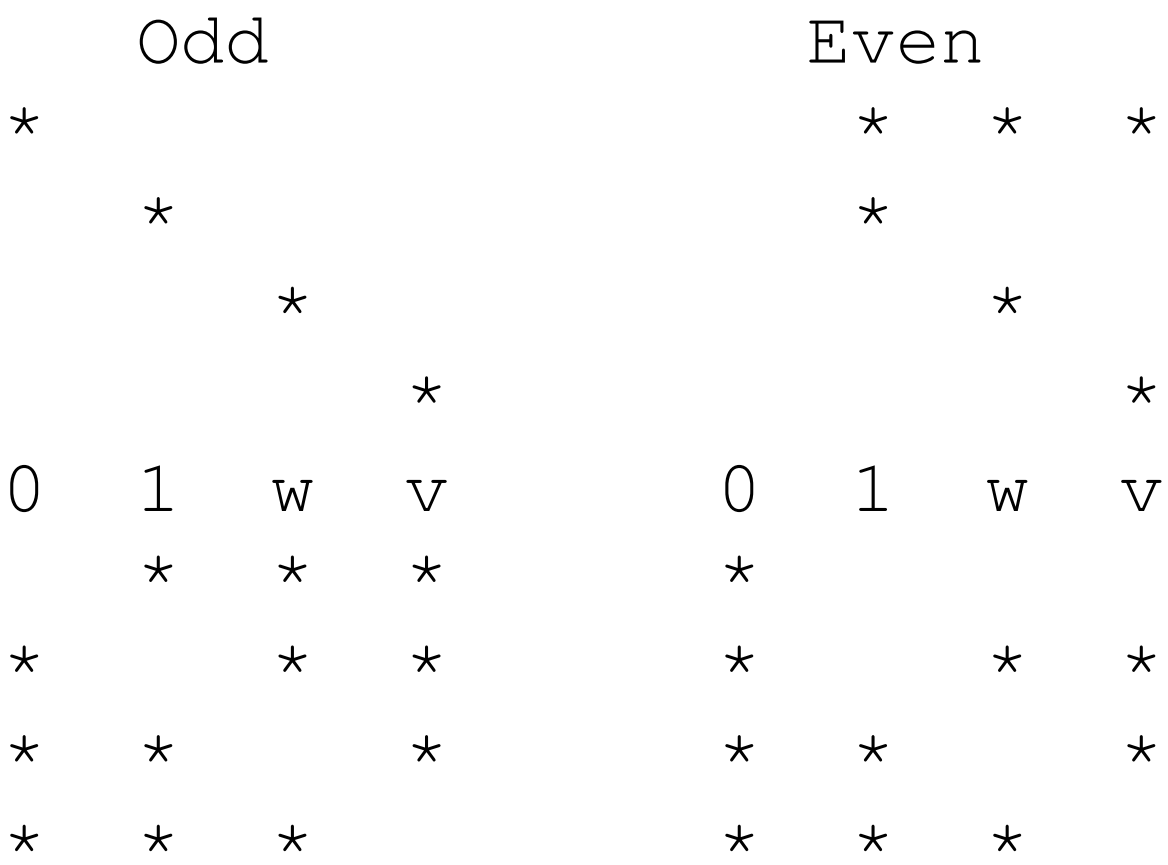
This is used for very strong secrets

- First encrypt your secret file (though you can publish the key!)
- This is just to make it useless to know some, but not all, bits of the file.
- Then divide it up into six files using the hexacode.
- Entrust six people with them
- Any three can reconstitute the secret, but no two can do so.

Actually this is not very sporadic

- The construction used in definition 2 can be used with many fields and polynomial degrees.
- The hexacode has more symmetry than you'd expect, though.

Back to M_{24}



E.g. octad from a hexacode word

```
Odd                Even
*                      *   *   *
    *                  *
        *                  *
            *                  *
0   1   w   v      0   1   w   v
    *   *   *      *
*       *   *      *       *   *
*   *       *      *   *       *
*   *   *          *   *   *
```

Golay code words must be hexacode words
Where either
every column has an odd interpretation
and the top row is odd
Or
every column has an even interpretation
and the top row is even

```
*   *   *
        *
    *       *
    *           *
0   1   0   1   w   v
```

This is the black squares from the first MOG picture

M_{24} engineers

1 Learn all the hexacode words (only 64 of them, and the symmetries make it very easy)

2 Learn the odd and even interpretations of the field of order 4

3 And you know all 2^{12} elements of the Golay code!

(24) $L_3(4)$

M_{24} contains the subgroup $L_3(4)$.

$L_3(4)$ acts on the projective plane of order 4 consisting of the triples of F_4 elements where scalar multiples are considered to be the same point.

There are 63/3 = 21 such points, and $L_3(4)$ is the stabilizer in M_{24} of three points acting on the 21 remaining points in this way.

$L_3(4)$ second slide

- Witt constructed M_{24} in this way, and Tits investigated the geometry in some detail.
- Some care is needed to handle the three fixed points correctly, involving the determinant of the 3 x 3 matrices.
- In the MOG the points are readily labelled to show the structure of this group, and the permutations of $L_3(4).S_3$ – the setwise stabilizer of 3 points – understood.

Trio group

- This construction starts with two versions of the extended Hamming code – a four-dimensional code on the 8 points of each of the three bricks.
- Turyn constructed M_{24} in this way.
- The Golay code consists of all words

X+t Y+t Z+t where X+Y+Z=0, X is in the first Hamming code and t is in the second.

Two Hamming codes

```
__   **   **   **   *_   *_   *_   *_   And their
__   **   __   __   *_   *_   _*   _*   complements
__   __   **   __   *_   _*   *_   _*   'linecode'
__   __   __   **   *_   _*   _*   *_

__   **   **   **   *_   *_   *_   *_   And their
__   __   _*   *_   _*   *_   **   __   complements
__   *_   __   _*   _*   __   *_   **   'pointcode'
__   _*   *_   __   _*   **   __   *_
```

- It is quite easy to learn the entire Golay code this waay also.
- To recognize an octad, add up the three bricks – better be in the point code – then add that to each brick and check two are in the line code.
- Not so easy for other purposes – e.g. octad completion.

Trio group shows . . .

- $2^6.(L_3(2) \times S3)$ are the “easy” automorphisms in this construction
- In fact the bricks can be seen in both $L_2(7)$ and $L_3(2)$ forms, giving an explicit isomorphism between these two groups.
- And in some ways this is the easiest construction

M_{23}

- Fixing a single point, the sporadic group M_{23} is obtained.
- This naturally gives the Steiner system S(4,7,23)
- And the (non-extended) Golay code is the original code found by Golay.
- Nevertheless there is very little about M_{23} that isn't just obtained by taking the same thing in M_{24} and fixing a point.

M_{12}

- The sets of size 12 in the extended Golay code are stabilized by the group M_{12} that permutes the points 5-transitively. The hexads are just the intersections of these 12 points with the octads that meet it in 12 points. The remaining two points of the octad are then an associated pair in the complementary dodecad.
- The stabilizer of this setup is the full automorphism group of S_6
- With a little care, this shows the existence of the S(5,6,12) and the group M_{12}.

The group M_{22}

- Fixing two points in M_{24} we get M_{22} which perhaps shows rather more individuality than M_{23} did.
- More specifically it has a twelve-fold cover! that does not extend to M_{23} or M_{24}.
- In particular the group $U_6(2)$ contains M_{22} and the 6 x 6 matrices represent the triple cover of M_{22}. This setup occurs in the smallest Fischer group F_{22}, but although in some ways the extension to M24 works, the M22 version is a lot simpler.

The 77 point graph

- Of course we get an S(3,6,22) from the S(5,8,24) of M_{24}.
- The 77 hexads of the S(3,6,22) form a "rank 3 graph" by joining two hexads when they are disjoint. The subgroup of M_{22} fixing a hexad is transitive on the 16 disjoint hexads, and also on the 60 hexads meeting our chosen one in two points.

This graph extends to the Higman Sims graph

- By taking 100 points as these 77 hexads, a single point “X” and the 22 points that M_{22} acts on
- and joining X to the 22 points, and each hexad to the six points in it
- We obtain the graph whose automorphism group is the sporadic group discovered by Higman and Sims.

Sporadic and Related Groups

Lecture 5

The Leech Lattice and the Conway Groups

The Conway Group

- Contains M_{24}, M_{23}, M_{22}, M_{12}, M_{11}
- Co_1, Co_2 and Co_3 which were new sporadic groups
- Also contains the Higman-Sims group, the second Janko group, the sporadic group of Suzuki and the McLaughlin group.
- So twelve sporadic groups are involved, and for seven of them Co_1 provides the “natural” setting.

Some History

- John Leech discovered the lattice in 24 dimensions.
- Studying the lattice we call Λ_0 he realized that not only did it have minimal norm 4 (32 in the scale we use here) but there is a particular point at distance 4 (32) from all points of the lattice, so you can put another copy of the lattice with origin there and still have the same minimal norm.

Automorphisms

- John McKay then pestered Conway to take a look at the lattice, and eventually Conway agreed to spend 12 noon to 12 midnight every Saturday until he had found the automorphism group.
- By midnight the first Saturday, he had shown, as McKay suspected, that the automorphism group was big and interesting.

Some terminology

We are working with a 24-point set which is called Ω in this lecture.

The extended Golay code is defined on Ω and a subset of Ω that is in this code is called a C-set. Hence a C-set has either 0, 8, 12, 16 or 24 elements of Ω in it.

Reference

- This lecture is following Conway quite closely
- Chapter 10 in Sphere Packings, Lattices and Groups.

Preliminaries.

- We start with a 24-dimensional space over the real numbers (actually rational is all we need).
- Equipped with its usual, positive definite quadratic form.
- An automorphism is required to preserve this quadratic form, so that the matrices are orthogonal.

(8) Definition of Leech Lattice

- Following Leech, we start off with a slightly different lattice Λ_0 consisting entirely of vectors with even coordinates, where the places where the vector is 2 (mod 4) are the places of a C-set, and where the coordinate sum is divisible by 8.
- The Leech lattice Λ is then "twice" as big. Every vector of Λ is either v or v + d where v is in Λ_0 and d is the particular vector
  d = –3,1,1,1,1,1,1,1, . . . 1

Some early properties

- Since -4 4 0 0 0 . . . 0 is in Λ_0 it follows that we could just as well take d' = 1,–3,1,1,1,1,1,1, . . . 1 or indeed any similar vector with the ,–3 in any postion.
- Hence the group M_{24} acts as automorphisms of both Λ_0 and Λ.

Sign changes.

If we negate all the coordinate vectors of any C-set, this clearly preserves Λ_0 since it does not change the places that are 2 (mod 4).

But also d = –3,1,,1,1, . . . 1,–1,–1, . . . ,–1 where -1 is on a C-set is obtained by subtracting twice that C-set, which is in Λ_0, and we can move the –3 before we do this if we want. Hence these sign changes are also automorphisms of the Leech lattice Λ.

The “easy” automorphisms

- We can therefore see a group of sign-changes and permutations, which a little thought will convince you is a group $2^{12}.M_{24}$.
- But this is not the whole automorphism group. I wouldn’t be talking about it if it were!

- We need one more automorphism ξ_T

ξ_T

- Take T to be any four points of Ω. Then this defines a sextet – a partition of Ω into 6 sets of size 4. Let S(j) be the subset containing j for j not in T.
- We define the action of ξ_T on the original 24 basis vectors (of the space, *not* the lattice) by taking
- x_i to $v_T/2 - x_i$ for i in T
- x_j to $x_j - v_{S(j)}/2$ for j in S(j).
- (Where v_U means the sum of the four vectors in the set U of size four).

ξ_T is an automorphism of Λ

- The Golay code is spanned by its octads, and so Λ_0 is spanned by the vectors 2,2,2,…2,0,0,0,0 with the 2's on the octads. It is sufficient to show, therefore, that ξ_T takes any octad and the single vector d to a vector of Λ
- Any octad hits T in 0,1,2,3 or 4 points, and there are about a dozen checks to be done.

Here are a few sample checks

- x_i to $v_T/2 - x_i$ for i in T x_j to $x_j - v_{S(j)}/2$ for j in S(j).

2 2 2 2 2 2 2 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 . ξ_T=
2 2 2 2 -2-2-2-2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

-3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 . ξ_T=
3-1-1-1 -1-1-1-1 -1-1-1-1 -1-1-1-1 -1-1-1-1 -1-1-1-1

2 2 2 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 . ξ_T=
1 1 1 3 1-1-1-1 1-1-1-1 1-1-1-1 1-1-1-1 1-1-1-1

4 0 0 0 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 . ξ_T=
-2 2 2 2 2-2-2-2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Actually we need ξ_T a bit more

- Although we have seen (when we finish the checks) that the automorphism group is bigger that the easy part, since it contains ξ_T as well, we need to prove transitivity on things now.
- Let's start by proving transitivity on the vectors of length 32

(16) Vectors of length 32

- A little thought should convince you that there are two sorts of vectors in Λ_0 and one in d+ Λ_0.
- (Can't be anything as big as 6 since that gives 36 already. 5 needs everything odd so gives at least 25+23. 4 leaves 16 which isn't enough to have 8 non-zero even entries so must be of shape 4 4. 3 we must have shape 3,1,1,1,…,1. 2 must be 22222222000000000000000, can't have all ones)

2^{12} .M_{24} has three orbits on length 32 vectors

4 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

2 2 2 2 2 2 2 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

-3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

And we have already seen ξ_T mixing them all up already.

Hence the automorphism group of the Leech Lattice (called .0 by Conway) is transitive on the vectors of length 32.

Divisibility of norms and inner products

- In Λ_0 it is fairly easy to see that all the norms of vectors are divisible by 16, and hence all inner products divisible by 8.
- Similarly the norm of d (-311111…1) is 32 and its inner product with anything in Λ_0 is divisible by 8 (as both 11111…1 and -400000 do)
- Hence all norms of Λ are divisible by 16 and all inner products divisible by 8.
- So it is natural to divide them by 8.
- From now on, “norm” means 1/8 of the sum of the squares of the coordinates.

Vectors mod 2

- Every vector of the Leech Lattice is congruent, modulo twice the lattice, to one of . . .
- The zero vector (i.e. is in the lattice)
- A vector of norm 4
- A vector of norm 6
- 24 mutually orthogonal pairs of vectors of norm 8
- This is shown by finding these vectors, demonstrating transitivity, and then noticing that we have already found 2^{24} vectors in the lattice mod twice the lattice, so have them all.

S-lattices

- Time and time again we need to find the stabilizer in Co_1 of some small dimensional sublattice L of the Leech lattice.
- If there is a vector of L congruent (mod 2) to a vector of norm 8, the stabilizer we seek stabilizes the set of 24 vectors of that congruence class
- Which are (up to automorphism) the basis that we used to construct the lattice.
- Hence all automorphisms are in the $2^{12}M_{24}$ group that we can see – the “easy” ones.

Otherwise we have an S-lattice

- Defined as a sublattice of the Leech lattice where no vector is congruent to a norm 8.
- There are 12, classified by Curtis (half the norm is called the "type" of a vector, given here.
- - $2Co_1$ — 333 3^5M_{11}
- 2 Co_2 — 2^53^2 $U_4(3)$
- 3 Co_3 — 2^33^4 $U_3(5)$
- 222 $U_6(2)$ — 2^93^6 3^4A_6
- 223 McL — 2^53^{10} $5^{1+2}.4$
- 233 HS — $2^{27}3^{36}$ $3^{1+4}.2$

Subgroups of Co_1

There are no vectors of norm 2.

Co_2 – stabilizing a vector of norm 4, such as 440000…0

Co_3 – stabilizing a vector of norm 6, such as 440000…0

When Conway discovered his group, these three groups were unknown.

Subgroups of Co_1

- Higman-Sims group – the stabilizer of two vectors of norms 6 with difference of norm 4.
- Such as a=5111…1 and b=1511…1
- We find all the vectors x of norm 2 such that x, x±a, x±b, x±a±b, can all be norm 2
- 44000…0 One such
- 11111-311111 22 such
- 2222222200000000 77 such

(24) Higman Sims group

- Joining two of these vectors when the difference is norm 6 gives exactly the graph of Higman-Sims, and provides an “easy” proof that the automorphism group of this graph is transitive.

McLaughlin group

- The stabilizer of two vectors of norm 4 with difference of norm 6
- Such as 2222222200000..0
- and -3111111..1
- The construction of a graph is not quite so straightforward, but it still works

Subgroups of Co_1

- Co_1 contains an element s of order three that fixes no vectors.
- Its centralizer is 3.Suz, a triple cover of the sporadic Suzuki group (Suzuki also discovered some groups that are not sporadic).
- s can be used to define a complex structure.
- A 12-dimensional lattice is defined using the integers of the cube root of 1 so s acts as a scalar (cube root of 1) and the automorphisms (as a unitary space) are the sporadic Suzuki group.

Subgroups of Co_1

- Co_1 also has an element of order 5 that fixes no vector. Its centralizer contains (the double cover of) the second Janko group J_2.
- This leads to a construction over the “icosians” – the quaternions over the square root of 5 – of a three dimensional “lattice” whose automorphisms are this group.
- It gets a bit messy when the underlying ring is not commutative.

Λ is an Even Unimodular lattice

- The result is an “even integral lattice”, which means all norms even and all inner products integral.
- The “determinant” of Λ (which can be defined as the density of points, or as the determinant of the quadratic form on a basis) is 1.
- There can only be even unimodular lattices if the dimension is divisible by 8.

Small even unimodular lattices

- In 8 dimensions, the unique even unimodular lattice is the E_8 lattice obtained by taking the integral vectors with even coordinate sum, and adjoining the vector ½ ½ ½ ½ ½ ½ ½ ½.
- In 16 dimensions, there are two unique even unimodular lattices. One is $E_8 + E_8$ and the other (called D_{16}^+) is the lattice obtained by taking the integral vectors with even coordinate sum, and adjoining the vector
  ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½.

Niemeier Lattices

- In 1973 Niemeier classified the 24-dimensional even unimodular lattices.
- There are 24 of them.

- A fascinating bunch that we shall meet again.

Sporadic and Related Groups

Lecture 6

Lorenzian lattices and the Conway Group

This is a “wow” lecture

- The Leech lattice is perhaps the most striking of the sporadic group structures.
- Nothing quite like it happens for the other sporadic groups.

- It is a big “Aladin’s Cave” subject. I can only hope to sketch it in one lecture.

26 dimensional Lorenz lattice

- The (unique) 26-dimensional even unimodular lattice has the Leech Lattice as its basic component.

- It may even be important in particle physics, where string theory picks out 26 and 10 dimensions as important.

First – a reminder of the Leech Lattice

- Following Leech, we start off with a slightly different lattice Λ_0 consisting entirely of vectors with even coordinates, where the places where the vector is 2 (mod 4) are the places of a C-set, and where the coordinate sum is divisible by 8.
- The Leech lattice Λ is then "twice" as big. Every vector of Λ is either v or v + d where v is in Λ_0 and d is the particular vector
  d = –3,1,1,1,1,1,1,1, . . . 1

Λ is an Even Unimodular lattice

- The result is an “even integral lattice”, which means all norms even and all inner products integral.
- The “determinant” of Λ (which can be defined as the density of points, or as the determinant of the quadratic form on a basis) is 1.
- There can only be even unimodular lattices if the dimension is divisible by 8.

Small even unimodular lattices

- In 8 dimensions, the unique even unimodular lattice is the E_8 lattice obtained by taking the integral vectors with even coordinate sum, and adjoining the vector ½ ½ ½ ½ ½ ½ ½ ½.
- In 16 dimensions, there are two even unimodular lattices. One is $E_8 + E_8$ and the other (called D_{16}^+) is the lattice obtained by taking the integral vectors with even coordinate sum, and adjoining the vector
  ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½ ½.

Niemeier Lattices

- In 1973 Niemeier classified the 24-dimensional even unimodular lattices.
- There are 24 of them.

- A fascinating bunch that we shall look at more closely soon.

What about 32 dimensions?

- I don’t think we will see a classification!
- There is a “mass-formula” which states that the sum of the reciprocals of the automorphism groups for the 32-dimensional even unimodular lattices comes to about 40,310,000. Since every lattice has -1 as an automorphism, that means there are at least 80 million distinct lattices.
- And the situation gets ever worse for yet higher dimensions.

So something special is going on at 24 dimensions.

- Basically up to 24 dimensions, lattices are fairly easy to understand.
- If you are determined enough you can do a bit in 25 dimensions, and a little bit in 26.
- But then all hell breaks loose. Things seem fundamentally different.

Niemeier lattices

- Apart from the Leech lattice (which has no vectors of norm 2), for the other 23 even unimodular lattices, in 24 dimensions, the entire space is spanned by the norm 2 vectors . . .
- But not (except $3.E_8$) the entire lattice.
- So let us start with the positive definite integral lattices (necessarily even) that are spanned by their norm 2 vectors.

You may have met them before

- There is A_n This is the set of integral vectors in n+1 dimensions with zero coordinate sum. Determinant n+1.
- Then there is D_n, which is the set of integral vectors in n dimensions with even coordinate sum. Determinant 4.
- Then E_6, E_7 and E_8 – three particular lattices in 6, 7 and 8 dimensions of determinant 3, 2 and 1 respectively.
- That's the lot.

Determinant is the dual quotient

- Given an integral lattice, the set of ***all*** points of space with integral inner product with the lattice points is call the dual lattice.
- It contains the original lattice
- But in general to finite index.
- This index is the determinant of the lattice.
- (Though with this definition it is an Abelian group, not just a number)

Can add “glue” points

- If a point of the dual lattice has norm that is an even integer, the lattice may be made larger by including this point also.
- The result is an even lattice, where the determinant has been divided by n^2, where n times the added vector was in the original lattice.
- These are called glue points.

Example – E_8 from D_8

- D_8 is the set of 8-dimensional vectors with even coordinate sum.
- So v =½ ½ ½ ½ ½ ½ ½ ½ has integral inner product with all of them (half an even integer) with 2.v already in D_8
- And its norm is 2 (eight times a quarter)
- So we can add it to the D_8 lattice (determinant 4) to get the E_8 lattice (determinant 1)

Niemeier lattice $6.D_4$

- Or we can take the direct sum of six copies of D_4
- (and pretend that the dual quotient – a fourgroup – has the structure of the field of order 4)
- And use a hexacode of glue!
- To make the Niemeier lattice $6.D_4$

The glued $6.D_4$ has determinant 1

- D_4 has determinant 4, so six of them has determinant $4^6 = 4096$.
- But then we add 64 glue-vectors so the determinant is divided by $64^2=4096$
- So the resulting lattice has determinant 1

Niemeier lattice $24.A_1$

- Or we can take the sum of 24 copies of the A_1 lattice – the 1 dimensional lattice spanned by a single vector of norm 2.
- Then use the Golay code to define the gluepoints – ½ on a Golay codeword and zero on the rest.
- Integral inner product? Yes.
- All norms even integers? Yes.

21 other ways.

- Each of them an amazing construction using lattices and codes that works particularly well in 24 dimensions.
- So making the 23 Niemeier Lattices.
- Philosophical question – why is there this striking pattern?

The 23 types of deep hole

- A “hole” in a lattice is a point of space that is a local maximum distance from all lattice points.
- A “deep hole” in the Leech Lattice is a hole at the (maximal) depth of sqrt(2)
- There are 23 distinct types, one for each Niemeier lattice.

Shallow holes

- Do not seem to be very important
- Just for the record, there are 284 types of them
- Classified by Richard Borcherds

One deep hole we can see easily

- If we take the point h=400000…0, the nearest lattice points are the origin, 8000…0 and the vectors 4±40000…0, making 48 points in all, each at distance norm=4 from h.
- The lattice spanned by these vectors is the orthogonal sum of 24 A_1 lattices at double the size (four times the norm).

“Holy” constructions

- Each of the 23 Niemeier lattices consists of a 24 dimensional lattice made up out of A_n, D_n and E_n.
- Along with the “code” that defines the glue vectors.
- Each of these also gives rise to a construction of the Leech Lattice
- Where a different group is “easy”

We saw the $24.A_1$ – Golay version

- But there are 22 others.
- Each giving rise to the Leech Lattice
- And if we knew that the Leech Lattice was unique, would (between them) give an easy proof that the automorphism group of the Leech Lattice is large.

Even Integral Lorenzian Lattices (EILLs)

- An EILL is a free Z-module equipped with an integral symmetric bilinear form that is Lorenzian – equivalent over the reals to 1 on all but one coordinate, and -1 on the last and for which the associated norm is even.
- This is just one of two essentially equivalent definitions of integral.
- “EILL” is my word. I invented it for this lecture.

Examples

- One can give just the bilinear form (which will have even numbers on the main diagonal)

$$\begin{matrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & -2 \end{matrix}$$

is an example of an EILL. It's determinant is (minus) six.

Automorphisms of an EILL.

- The set of integral matrices M such that M'.E.M = E.
- There is an algorithm for finding the generators and relations of any EILL.

Example – the EILL

2 0 0

0 0 1

0 1 0

has automorphism group

G = <A,B,C :

$A^2=B^2=C^2=(AB)^2=(AC)^3=1$>

This is a reflection group

- Given any vector such that all inner products are a multiple of half the norm
- The reflection in the perpendicular hyperplane is an automorphism of the lattice.
- In particular any vector of norm 2 (or -2) has that property.
- In the previous example, the reflections in the vectors of norm 2 generate the whole automorphism group.

Reflections and automorphisms.

2 0 0 $2x^2+2yz$ has automorphism group

0 0 1 $G = \langle A,B,C :$

0 1 0 $A^2=B^2=C^2=(AB)^2=(AC)^3=1\rangle$

- A = [0 1 1], B=[1 0 0], C=[-1 -1 0]

A and B have inner product zero, so are perpendicular, hence $(AB)^2=1$.

A and C have inner product -1, so are at 60°, hence $(AC)^3=1$

B and C have inner product outside the range -1, 0, 1 so there is no relation.

A whole bunch of lattices.

- Take any even positive definite lattice A and take B = A+H = the direct sum of A and
- $H = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$
- Then the automorphism group of B includes a reflection for each lattice point of A
- If every point of space in A is distance less than sqrt(2) from a lattice point (has covering radius less than sqrt(2))
- Then the quotient of the “lattice reflections” is just the automorphism group of A.

As the dimension rises, things gradually change . . .

- At higher dimensions, or – for the same dimension – at higher determinants, reflections account for less and less.
- First they give the whole group
- Then they are of finite index in the group
- There is then a boundary case, of which the Conway group is the most stunning.
- Then it goes bananas.

So what happens

The Leech lattice has covering radius exactly sqrt(2)

This is quite hard to prove

$H+\Lambda$ is the unique even 26-dimensional lattice of determinant 1

And the reflections generate a normal subgroup of $\mathrm{Aut}(H+\Lambda)$ with quotient group $Z^{24}.2.Co_1$

Let me just re-state that.

- Take ***the*** 26-dimensional even Lorenzian lattice, and take its automorphism group.
- Factor out the reflections in norm 2 vectors
- Then factor out the maximal normal abelian subgroup of that.
- And you get the sporadic Conway Group $2.Co_1$

One idea of what might be happening

- Given a group consisting of matrices of integers, one can, of course, take the set of matrices congruent to 1 mod N for some N.
- This is a normal subgroup with finite quotient.
- For which Lorenzian Lattices are there others?

My guess

- Only finitely many EILLs have non-congruence subgroups of finite index.
- Perhaps in dimension at least 4, or 5, or something . . .
- But really – I have no idea.

Lorenz Construction.

- Another unusual piece of arithmetic is that the sum of the squares of the first 24 integers comes to $4900 = 70^2$
- This gives rise to another construction whereby the 26-dimensional even unimodular lattice is taken as the usual integral (Lorenzian) quadratic form, except you require the coordinate sum to be even and add the all ½ vector.

- Then take w = 0,1,2,…,23,24 ; 70 where the last coordinate is the one whose square is subtracted.
- Then the norm of w is zero
- And the vectors with inner product zero with w, (modulo w, which satisfies this!) . . form a (non-linear) structure isometric to the Leech Lattice.

The magic goes on and on

- The study of the Leech Lattice has more amazing facts.
- Enough to fill a whole book
- “Sphere Packings, Lattices and Groups”

- I will be returning to planet earth for the next lecture.

Sporadic and Related Groups

Lecture 7

Matrix groups

and the Janko groups J_1 and J_3

Government Health Warning.

- This lecture is about the main bulk of the simple groups – not sporadic at all.
- And then about the two smallest of the six “pariah” groups.
- They appear to have no real “natural setting”
- One is led to wonder why they exist at all
- Whatever that means.

A little history

- Mathieu discovered his five sporadic groups in 1860-1880
- The various matrix groups were studied in the following 80 years
- Let's take a look at what they found

- The next sporadic was found in 1965 . . . I am coming to that.

Matrix groups

- Let me say at the outset that many of these matrix groups have some scalars – diagonal matrices where the exact number of them depends on the dimension and the field. We quotient them out.
- And also there is often the determinant function. We take the subgroup of determinant 1

Set of all matrices

- (of determinant 1, modulo scalars)
- These are all simple except for $L_2(2)$ and $L_2(3)$
- This gives the vast majority of simple groups, or at least would do if that meant anything.

Then you can take bilinear forms.

- Take a matrix F (the form) and consider the group of matrices such that M'.F.M=F
- Where M' means the transpose of M.
- This works best when the form is either symmetric or skew symmetric, since (transposing the above equation) we see that M fixes both F-F' and F+F'
- Characteristic 2 needs more careful treatment.

Symplectic groups

- If F is skew-symmetric (F' = –F) the set of matrices M with M'.F.M = F is called the symplectic group $S_{2n}(q)$. Only works in even dimensions.
- In dimension 2 this is no real condition, so we may as well take n at least 4.
- These are all simple except $S_4(2)$ which is S_6

Orthogonal groups

- Basically symmetric bilinear forms
- Actually to work in all characteristics, including 2, it is best to define a quadratic form as a function q(v) from a vector space to the field such that
- $q(v+w)=q(v)+q(w)+(v,w)$ where (v,w) is a bilinear form.
- And in even dimension there are two different quadratic forms . . .

Orthogonal groups

- So all in all we get the following orthogonal groups.
- $O_{2n}^{+}(q)$
- $O_{2n}^{-}(q)$
- $O_{2n+1}(q)$

Continuous groups

- If anyone has studied the continuous groups over the complex numbers, this list will sound very familiar.
- The classification of these using Dynkin diagrams is just over 100 years old.
- And in 1955, Chevalley showed that they all work over finite fields as well.
- So we get . . .

Straightforward Chevalley groups

$A_n(q)$	$L_{n+1}(q)$
$B_n(q)$	$Sp_{2n}(q)$
$C_n(q)$	$O_{2n+1}(q)$
$D_n(q)$	$O_{2n}^{+}(q)$
$E_n(q)$	(no classical analogue) n=6,7,8
$F_4(q)$	“
$G_2(q)$	“

Twisted versions

If the Dynkin diagram has a cyclic group of symmetries, you can extend the field and then require that the combination of the diagram symmetry and the field automorphism fixes your matrices.

Unitary is easiest.

A_n has a diagram symmetry of order 2

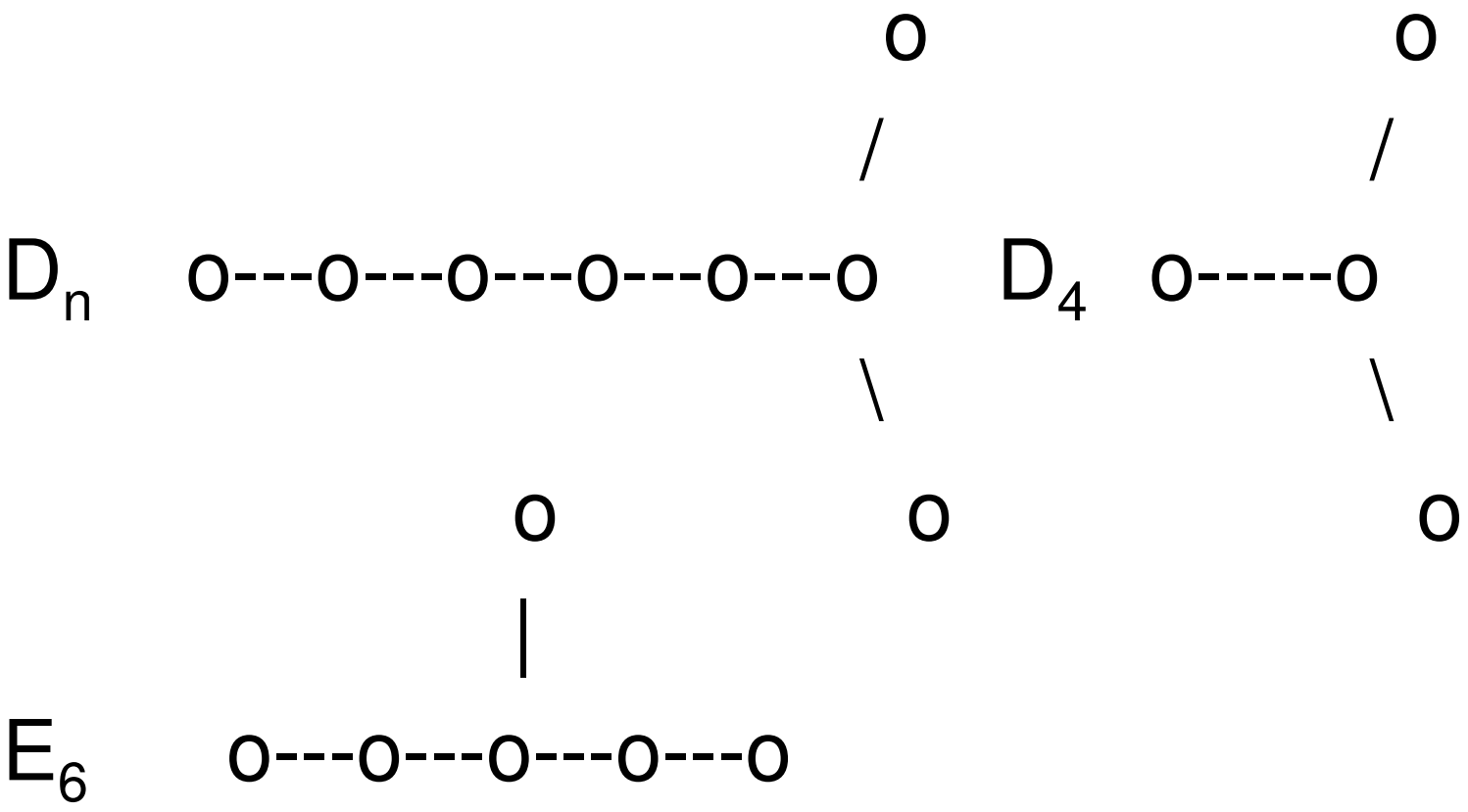
o---o---o---o---o---o---o---o

This corresponds to “transpose-inverse”.

So the twisted A_n requires transpose inverse to equal the field automorphism

This is called the unitary group

Other diagrams have symmetry also



These lead to further twised Chevalley groups

- ${}^2A_n(q)$ The unitary groups
- ${}^3D_4(q)$
- ${}^2D_n(q)$ The orthogonal groups $O_{2n}^-(q)$
- ${}^2E_6(q)$

Then there are some “Ree groups”

- These are symmetries with multiple bonds
- G_2 o≡ ≡ ≡ ≡o (a triple bond)
- F_4 o----o====o----o (with a double bond)
- B_2 o====o (with a double bond)

can all have twisted analogues if the field characteristic is 3 for G_2 and 2 for the other two

They seemed to go on and on

- (actually this turned out to be the end of the matrix groups)
- So Thompson and Janko looked at the Ree groups $G_2(q)$
- The centralizer of an involution (element of order 2) in these groups was $2 \times L_2(q)$
- And they were able to show conversely that if the centralizer of an involution was of this form, it was a Ree group . . .
- Except possibly $2 \times L_2(5)$

Janko's starting point.

- So, in an attempt to finish off their theorem, Janko tried to find all simple groups with involution centralizer $2 \times L_2(5)$

- There is a very general result that states that only finitely many simple groups can have any given centralizer of involution.

Janko's result

- He showed in turn that the 2^3 normalizer was $2^3.7.3$, that the 3 centralizer was 3×5.4, that the 5 centralizer was $5 \times S_3$, and eventually found the order (175560)
- The character table . . .

- But was there a group like that? It seemed pretty likely by now.

Modular characters

- He then applied Brauer's theory of modular characters, and found (from the character table) that there had to be a 7 dimensional representation of the group over the field of 11 elements.

- So he then proceeded to find 7 x 7 matrices and proved that there really is a group with involution centralizer 2 x $L_2(5)$

So in 1965

- Janko announced an new sporadic group of order 175560 that we now call J_1.
- It was a big shock

But what is this group ***for***?

- Well – I don't know.
- I have a sort-of faith that mathematics is an essentially infinite subject, and that there should be some setting in which J_1 is the central focus.
- But no-one seems to be able to find it.

Other small representations

Field	Smallest degree(s)
Complex	56
Rational	76
Mod 2	20
Mod 7	31,45,…
Mod 11	7,14,27,49,…
Mod 19	22,34,43
All others	56 or 76

One can “manufacture” an object with J_1 as its automorhism group

- If you take any of these representations, for example, and take their symmetric square (action of quadratic poynomials) there will usually be several invariant subspaces
- And one can therefore take the group as the automorphism group of that object.
- But it is not usually very enlightening.

Or look at permutations

- J_1 has seven classes of maximal subgroup including.

  $L_2(11)$ order 660 index 266. This gives

  rise to a graph on 266 points and rank

  5 (so $L_2(11)$ has 5 orbits on the points)

Again you can define the group as the automorphism group of this graph.

But the only real way to get the graph is to start with J_1 so that doesn't get anyone excited

The 7 x 7 matrices mod 11 might be good.

- J_1 is a subgroup of $G_2(11)$
- $G_2(11)$ is the automorphism group of the Octonions (or Cayley numbers) over the field of 11 elements.
- So it seems possible that something special happens with the octonions mod 11 that makes J_1 seem natural.
- Though I am not aware of anything. ☹

Or the 20 mod 2?

- We did look at that for quite a while, and couldn’t find anything. ☹

Or the 22 mod 19

- As far as I know, no-one has really looked at that in detail, but to be honest I don’t know what to look for . . . ☹

Perhaps . . .

- There is no natural setting for J_1
- Anyway, it does seem to be true that matrices and permutations do not expose the group as anything important in any way whatsoever.

Except that it exists.

- The discovery of J_1 set off a spate of investigations that led to the discovery, within about 10 years, of all (or almost all) of the sporadic groups.

- So its influence on group theory was quite big.

Another Janko group J_3

- This time the involution centralizer was $2^{1+4}.A_5$ so quite a bit bigger. This actually led to two sporadic groups, since J_2 has exactly the same involution centralizer.

- (J_2 arises as a 5-centralizer in the Conway group, so we have already met it once)

Again Janko got a long way

- But this time he had no 7 x 7 matrices to find, and was unable to show that this group existed. The order he knew – 50,232,960.
- It was eventually shown to exist by finding a permutation representation on 6156 points found using a computer.

Much later

- I found (with a computer) that $3.J_3$ has a 9-dimensional representation over the field of order 4.
- Actually I was so surprised I failed to notice it for many hours!
- Conway then studied if for quite a while, but although he was able to use this representation to prove existence, it still doesn't seem natural

How might this work . . .?

- Ideas anyone?
- We have a 9-dimensional representation (of $3.J_3$) over the field of 4 elements. The exterior square (action on quadratic polynomials without x^2 terms) has degree 9.8/2 = 36. This has an 18-dimensional invariant subspace for $3.J_3$ which Conway used to define the group, but how can one look for a purpose?

No other interesting representations

- And we now know all the degrees of the permutation representations and all the representations over all fields.
- So again – sadly – we seem to have to admit that J_3 is just one of those groups that exists, but is otherwise without purpose. ☹

How does one find a purpose?

- I have often heard depressed people say that the hardest thing to find in life is a purpose.
- True also in the case of the sporadic groups
- I feel that this is a fruitful direction to think.
- Big new ideas don't get you an academic job for ages. Sad but true. But find a big new idea that "explains" a sporadic group, and I reckon you will!

Pariahs

- There are six sporadic groups that seem "totally useless" in this way. If you find a use for any of them, you will have made a breakthrough.
- J_1 and J_3 we have met today
- J_4, Ruv, ONan, Ly are all much larger, and I will deal with them later.

- Warning . . . Lunacy coming!

One idea

- Take a binary product and call it *
- Now write down some rules. I'm thinking random rubbish here, but how about

$x*(y*x)=(x*y)*x = y$

$((((x*y)*y)*y)*y)*y = x$

- Call it a prongle-algebra to make it sound good.
- Now study things that satisfy your rules.
- Maybe there are very few finite prongle-algebras, and one of them has a pariah as its automorphism group.

Prongles are not totally silly

- They are designed to be likely to have A_5 in their automorphism group
- You define the free prongle on 2 generators p and q, then T takes (p,q) to (q,p) and S takes (p,q) to (q,p*q)
- The axioms now imply that $T^2=S^3=(ST)^5=1$
- Indeed that is where I got them from!
- Now what? Dunno.
- I haven't found a finite prongle yet.

Stupid Rings

- Or just take a random definition of + and * on some smallish finite set, and then see what you can find in the (huge) set of (say) 7 x 7 matrices over that.
- Maybe you can find some cases more general than fields but where you still get something like a group.
- Quaternions? Cayley numbers?

Or use a computer

- Try all stupid rings of order three, say, and look at the 4 x 4 matrices over that to see what single “matrices” you can find that do not generate loads of stuff.
- Anyway – better get back to some serious mathematics, I suppose.

- Next week.

Sporadic and Related Groups

Lecture 8

Fischer groups F_{22}, F_{23}, F_{24}

3-Transpositions.

- In any group, define D to be a set of 3-transpositions if
- D is a union of conjugacy classes
  $d \varepsilon D$ implies $x^{-1}.d.x \varepsilon D$ for any x in the group.
- If $d \varepsilon D$ then $d^2=1$
- If d_1 and d_2 are both in D, then the order of $d_1.d_2$ is 1, 2 or 3.

Symmetric groups

- Take D to be the class of “transpositions” (x,y) in the symmetric group – swapping two points and fixing all the others.
- Closed under conjugation and $d^2=1$
- Then (x,y).(x,y) = 1
- (x,y)(x,z) = (x,y,z) of order three and
- (x,y)(z,t) has order two.

Fischer's first idea

- Was to try to prove that the symmetric groups were the only examples.
- Roger Carter pointed out that this is not the case . . .
- But Fischer had got some way with his proof, and although his idea of the theorem was way out, the proof was still pretty good! ☺

Fischer's geometrical view.

- Take the set of transpositions in a 3-transposition group, and then make a "geometry" out of them by making a list of the triples that lie S_3 subgroups. Then the group (and the choice of set D) defines the geometry, and the geometry defines the conjugacy action of D on itself, so gives the group generated by D modulo the centre of that group.

A Fischer Geometry

- Take any old set D
- Define certain subsets of size 3 from D to be “special”.
- Wonder whether there is a group where D is a class of 3-transpositions where the product ab has order 2 unless a and b are in some special set, in which case the product has order 3 with aba=bab the other transposition in the S_3 generated.

If there is, you've got it!

- The geometry gives the conjugation action of D on itself (denote this by [a,b]), so the axioms needed are that this "works".

- [[[a,b],c],b] = [a,[c,b]]

- Which splits into several cases depending on whether various pairs are in a triple or not.

Fischer's theorem.

- If G is generated by a class of 3-transpositions, with trivial centre and derived group simple, then G is one of . . .
- S_n, $O_n^{\pm}(2)$, $O_n^{\pm}(3)$, $U_n(2)$ or
- F_{22}, F_{23}, F_{24}
- The last three are the sporadic Fischer groups, but we will look at them all.

Direct products work

- If two groups G_1 and G_2 are 3-transposition groups with transpositions D_1 and D_2, then G_1 x G_2 with transpositions the union of D_1 and D_2 is also a 3-transposition group.
- Conversely if we join two transpositions if their product has order 3, and the result is not connected, the resulting geometry is just the union of the connected components.

Disjoin cases

- One idea is just to disjoin cases as to what the product order might be, and then identify the group from its presentation.
- This gets us a long way.
- For this we usually use the graph – we join two transpositions if their product has order 3.
- (In Fischer's geometry we also need to say where the third one of the S_3 is if they are joined, but we won't always bother).

Familiarization.

- Suppose two transpositions are joined graph.
- Then their product has order 3, and they are two of the three involutions in that S_3.
- The third involution conjugates the first to the second.
- So two transpositions that are joined are conjugate

More generally

- If two transpositions are in the same connected component, they are conjugate in the group generated by the transpositions of the path.
- For in the path from one to the other, every step is done by conjugating by a transposition of the group.

First lemma

- If two distinct commuting transpositions a and b are in the same connected component of a Fischer graph, then there is a third transposition c with product order 3 with both.
- Proof. Take the shortest path in the graph from one to the other. It gives a presentation of S_n and S_n contains such a transposition.

Base

- In any 3-transposition group, define a “base” to be a maximal set of mutually commuting transpositions.
- Any two bases are conjugate.
- Proof . . . Take one Base and call it B.
- Take any other base and a transposition of it not in B. Cannot add it to B so there is a transposition of B with product order 3. Conjugate by the third transposition in the S3 they generate and you get a bigger intersection.

Rank.

- So we define the “rank” of a 3-transposition group to be the number of transpositions in a base.
- The centralizer of a transposition, modulo that transposition, is a 3-transposition group of one lower rank except in trivial cases, . . .
- So you can try to classify the 3-transposition groups inductively.

Frequent theme

- Given any configuration of transpositions, either it occurs in your group or it does not.
- If it does not occur, you can use that as an additional “axiom” in that part of the classification.
- If it does occur, you can start with that.

First example

- Take the configuration of three transpositions a,b,c where ab, ac, bc and abac all have order 3.
- Suppose first we look at groups which do not have this configuration.
- Then take four transpositions a,b,c,d where a,b and c all commute, and d has product order three with each of them
- Suppose we look at groups which do not have this configuration either.
- I call these “miniture transpositions”

A miniture classification problem

- We first wonder what three miniture transpositions a,b and c can generate. Clearly 2 x 2 x 2 and 2 x S_3
- Also S_4 works, generated by (12), (23) and (34).
- Er . . . That's the lot!

3 Miniture transpositions

- Consider the orders of ab ac and bc. If all are 2, it's 2 x 2 x 2. If one is 3 and two are 2, it is 2 x S_3. If two are 3 and one is 2, it's S_4. If all are three, abac cannot also be order 3 by assumption, so must be 2. This is also S_4 as it happens.

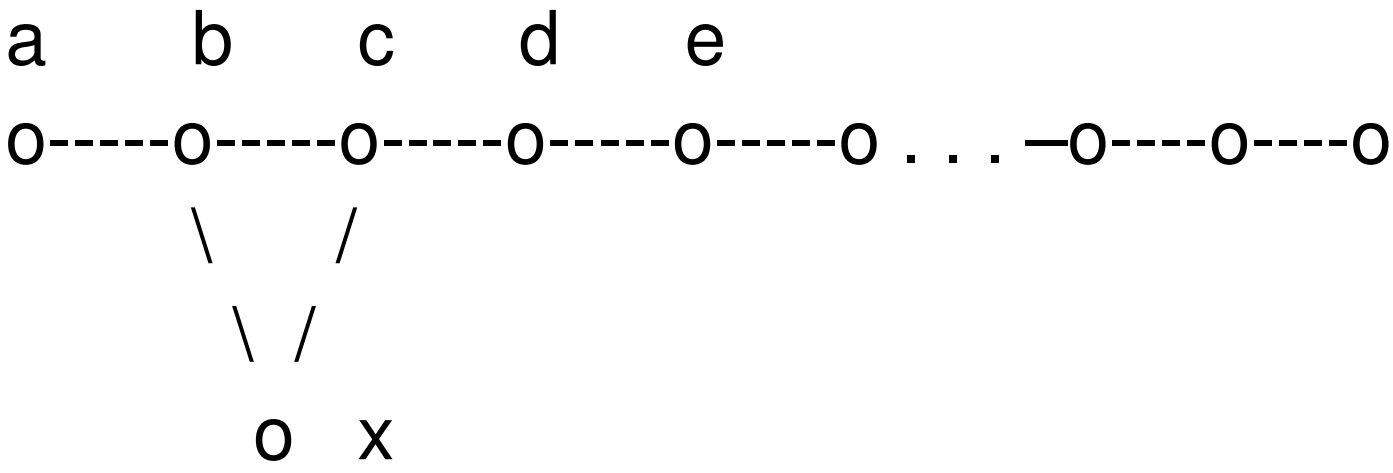
Main idea

- Induction on the number of generating transpositions.
- Add a new transposition. Since there are so many commuting transpositions on the diagram already, it cannot have many order 3 products without having three commuting ones.
- Hence you get a handful of diagrams to look at

Several miniture diagrams

- These diagrams need to be investigated in detail.
- In practice they all turn out to generate a symmetric group!
- Let me take an example

Example.



In the triangle, bxb.c must have order 2. We can rechoose x as bxb and it commutes with c and must have product order 3 with a. We can move the triangle along in this way until it reaches the end.

This does not generalize very well

- The nice presentation of the symmetric group is critical in the above miniture theorem. The general Fischer groups are not so simply presented.

- We need a better method.

A better method

- The main idea is therefore to ask which transposition group H centralizes one transposition x . . .
- And then which transpositions in H centralize also y where $(xy)^3=1$
- And then from this information we find all groups like that.

The major lemma.

- Except in “trivial” cases, the centralizer of a transposition x is transitive on transpositions y that commute with x, and on transpositions z that do not commute with x.
- Hence, given a transposition centralizer, there are only finitely many possibilities for what can happen at the next rank up.

The heart of Fischer's trick

- Given the centralizer of a transposition x, which elements in it are transpositions, and which subgroup of it also commutes with z (where xz has order 3 – all conjugate) you already have names for every element of D, so the problem is finite.

Fischer looked at the geometry

- If the group has a normal subgroup which is a 2-group (respectively a 3-group) the geometry can be “imprimitive” in that there is an equivalence relation on the transpositions such that equivalent transpositions have the same order product.
- We are therefore primarily interested in primitive cases.

Primitive cases

- Then we get a finite number of groups at each rank, and can proceed by manual induction!

- The four infinite series need to be dealt with, of course. We get, in turn

Small cases – I think this is right

- If the centralizer of a transposition is solvable, then the whole group is S_4, S_5, $U_4(2) = O_5(3)$.

- In what follows, I just assume that n is large enough. What that means is not explicitly sorted out.

1. S_n

- If the centralizer of a transposition is S_n, then the whole group is S_n, except . . .
- That it could be the Weyl group of E_6, which is $O_6^-(2)$ and $O_5(3)$

2. $O_n(2)$

- If the centralizer of a transposition is $O_n(2)$, then the whole group is of the form $O_m(2)$,

3. $O_n(3)$

- If the centralizer of a transposition is $O_n(3)$, then the whole group is of the form $O_m(3)$,

4. $U_n(2)$

- If the centralizer of a transposition is $U_n(2)$, then the whole group is of the form $U_m(2)$
- Except that it could also be F_{22}

Final bit.

- If the centralizer of a transposition is F_{22}
- then the whole group is F_{23}
- If the centralizer of a transposition is F_{23}
- then the whole group is F_{24}
- And the centralizer of a transposition can't be F_{24}

The base normalizer

- In F_{24}, the base has 24 mutually commuting transpositions, but a Golay codeword of them has product 1. Hence they only generate a group of order 2^{12} (not 2^{24}).
- But this does not extend to a code with 25 points, so F_{24} is the end of the line.

The Fischer groups are big.

- F_{24} is not a simple group, but has a simple subgroup F_{24}‘, of index 2. This subgroup has order just over 10^{24}. It has a permutation representation on the transpositions, of which there are 306,936.
- The base normalizer is $2^{12}.M_{24}$. This subgroup is *non-split* – there is no subgroup M_{24} in this group.

More on F_{24}

- There simple group F_{24}‘ has a triple cover 3 F_{24}, which has a 783-dimensional complex representation (actually it only needs the cube roots of 1).
- Basis vectors can be taken as points and octads of M_{24}.
- 24 + 759 = 783.
- There is a sort-of algebra in this space.

F_{23}

- For most purposes, F_{23} is best considered as a subgroup of F_{24}
- Perhaps the one interesting case is the there is a 253 dimensional representation over the field of order 3 which, although coming out of the 783 for F_{24}
- Is nevertheless of independent interest.

F_{22}

- Apart from its properties inherited from F_{24}, F_{22} has a triple cover which has a 27-dimensional representation in characteristic 2.
- Also the base normalizer $2^{10}.M_{22}$ is split in this case, making it much easier to work in than F_{24}