Homology of Mathieu groups

Mathieu Dutour Sikirić
Institut Rudjer Bošković

Ellis Graham
NUI Galway

April 27, 2012

I. Homology

Polytopal complex

- A polytopal complex $\mathcal{PC}$ is a family of cells:
  - It contains $\emptyset$ and P such that for every face F one has $\emptyset \subset F \subset P$.
  - If F is a face and

$$\emptyset = F_0 \subset F_1 \subset \cdots \subset F_p = F$$

    is a chain, which cannot be further refined, then dim $F = p$.
  - We set $dim\ \mathcal{PC} = dim\ P - 1$
  - If F_{p-1} and F_{p+1} are two cells of dimension $p-1$ and $p+1$ then there exist exactly two cells G, G' such that

$$F_{p-1} \subset G, G' \subset F_{p+1}$$

  - The faces F are equivalent to polytopes.
- Example:
  - Any plane graph, any map on a surface.
  - Any polyhedral subdivision

Boundary operator

- Let $\mathcal{PC}$ be a polytopal complex and for any $0 \leq p \leq dim\,\mathcal{PC}$ denote by $C_p(\mathcal{PC})$ the $\mathbb{Z}$-module, whose basis is the p-dimensional faces of $\mathcal{PC}$.
- We denote by d_p the boundary operator:

$$d_p : C_p(\mathcal{PC}) \to C_{p-1}(\mathcal{PC})$$

  Note that $d_0 : C_0 \to \{0\}$.
- Note that $d_p(F)$ is not defined uniquely, we can replace $d_p(F)$ by its opposite with no damage.
- But if one imposes the relation $d_p(d_{p-1}) = 0$ then this is the only freedom, which is available.
- If $e = \{v, v'\}$ is an edge then we will have $d(e) = v - v'$ or $v' - v$.

Polytopal homology

- Take $\mathcal{PC}$ a polytopal complex of dimension n and define

$$B_p(\mathcal{PC}) = \mathrm{Im}\, d_{p+1} \text{ and } Z_p(\mathcal{PC}) = \text{Ker } d_p$$

- From the relation $d_p d_{p-1} = 0$ we have $B_p \subset Z_p$ and we define

$$H_p(\mathcal{PC}) = Z_p / B_p$$

- If the tessellation of the space is by simplices, then we speak of "simplicial homology".
- $H_0(\mathcal{PC}) = \mathbb{Z}^p$ with p the number of connected components.
- H_i is a sum of $\mathbb{Z}$ and $\mathbb{Z}/a\mathbb{Z}$ groups.

Topological invariance

- If $\mathcal{M}$ is a manifold and $\mathcal{PC}_1$ and $\mathcal{PC}_2$ are two polytopal subdivision modelled on it, then

$$H_p(\mathcal{PC}_1) = H_p(\mathcal{PC}_2)$$

- A space X is called contractible if it can be continuously deformed to a point x. For a contractible space, one has

$$H_0(X) = \mathbb{Z} \text{ and } H_p(X) = \{0\} \text{ for } p > 0$$

II. Group homology

Covering space

- If X, Y are two topological spaces, then a mapping $\phi : X \to Y$ is called a covering map if
  - For any $y \in Y$, there exist a neighborhood N_y of y
  - such that for any $x \in \phi^{-1}(y)$ there exist a neighborhood N_x with
    - $N_y \subset \phi(N_x)$,
    - $N_x \cap N_{x'} = \emptyset$ if $x \neq x'$,
    - $\phi : N_x \to \phi(N_x)$ is bijective.
- As a consequence $|\phi^{-1}(y)|$ is independent of y and ϕ is surjective.
- There exist a group G of homeomorphisms of X such that for any $x, x' \in X$, there is a $g \in G$ such that $g(x) = x$.
- We then write $X/_G = Y$.

Group homology

- Take G a group, suppose that:
  - X is a contractible space.
  - G act fixed point free on X.

  Then we define $H_p(G) = H_p(X/G)$.
- The space X is then a classifying space.
- Every group has a classifying space but finding them can be difficult.
- For example if $G = \mathbb{Z}^2$, then $X = \mathbb{R}^2$, $Y = X/G$ is a 2-dimensional torus and one has
  - $H_0(G) = \mathbb{Z}$,
  - $H_1(G) = \mathbb{Z}^2$,
  - $H_2(G) = \mathbb{Z}$,
  - $H_i(G) = 0$ for $i > 2$.

III. Orbit polytope

Orbit polytope

- Suppose a group G has a linear representation in $\mathbb{R}^n$ and v is a vertex. The orbit polytope is then

$$conv(v.G)$$

- The interest of the orbit polytope is that it is an approximation of a classifying space:
  - If v is chosen randomly, the vertices have trivial stabilizers.
  - Then edges have stabilizer of size 1 or 2.
  - 2-faces have cyclic or dihedral stabilizers.
  - 3-faces stabilizers are also classified.
- See for more details:
  - G. Ellis; J. Harris, E. Sköldberg, *Polytopal resolutions for finite groups*. J. Reine Angew. Math. **598** (2006), 131–137

Polyhedral algorithm

- If G is an "interesting group" then it is big and the orbit polytope $conv(v.G)$ has too many vertices to be stored in memory. The facets are also too big.
- The technique is store the set S of vertices adjacent to v, say, $S = \{v_1, \dots, v_m\} = v.\{g_1, \dots, g_m\}$.
- Use an iteration
  - Determine an initial set S with (g_i) generating G.
  - By the group action, we know the vertices adjacent to S.
  - We check if those vertices are adjacent to S.
    - If yes, we update the set S.
    - If no, we return the set S as the reply.
- Several problem:
  - The algorithm can iterate forever to get the correct S, choosing a good initial set S is a good idea.
  - To find the adjacencies, one can compute the facets of the cone at v determined by S or linear programming.

Coxeter group case

Take G a finite Coxeter group acting on $\mathbb{R}^n$ by its natural representation.

- Denote by $\mathcal{S}$ a fundamental simplex of the group G.
- The stabilizer of $v \in \mathcal{S}$ is the group generated by the reflections on the facets of $\mathcal{S}$ containing v.
- If v is inside of $\mathcal{S}$ then we obtain the permutahedron; and we have $S = v.\{s_1, \dots, s_n\}$.
- If v is contained in some facets of $\mathcal{S}$ then we can describe the set of faces of $conv(v.G)$. One possible reference:
  - M. Deza, M. Dutour and S. Shpectorov, *Isometric embeddings of Archimedean Wythoff polytopes into hypercubes and half-cubes*, MHF Lecture Notes Series, Kyushu University, proceedings of COE workshop on sphere packings (2004) 55–70.
- For non-Coxeter groups, there is few hopes of a simple way to describe the face lattice.

IV. Resolutions

G-modules

- We use the GAP notation for group action, on the right.
- A G-module M is a $\mathbb{Z}$-module with an action

$$\begin{array}{ccc} M \times G & \rightarrow & M \\ (m, g) & \mapsto & m.g \end{array}$$

- The group ring $\mathbb{Z}G$ formed by all finite sums

$$\sum_{g \in G} \alpha_g g \text{ with } \alpha_g \in \mathbb{Z}$$

  is a G-module.
- If the orbit of a point v under a group G is $\{v_1, \dots, v_m\}$, then the set of sums

$$\sum_{i=1}^{m} \alpha_i v_i \text{ with } \alpha_i \in \mathbb{Z}$$

  is a G-module.
- We can define the notion of generating set, free set, basis of a G-module. But not every finitely generated G-module admits a basis.

Free G-modules

- A G-module is free if it admits a basis $e_1, \ldots, e_k$.
- For free G-modules, we can work in much the same way as for vector space, i.e., with matrices.
- Let $\phi : M \to M'$ be a G-linear homomorphism between two free G-modules and (e_i), (e'_i) two basis of M, M'.
- We can write $\phi(e_i) = \sum_j f_j a_{ij}$ with $a_{ij} \in \mathbb{Z}G$
- but then we have with $g_i \in \mathbb{Z}G$

$$\begin{array}{rcl} \phi(\sum_i e_i g_i) & = & \sum_i \phi(e_i g_i) \\ & = & \sum_i \phi(e_i) g_i \\ & = & \sum_j f_j (\sum_i a_{ij} g_i) \end{array}$$

- More generally the "right" matrix product is $AB = C$ with $c_{ij} = \sum_k b_{kj} a_{ik}$.

Resolutions

Take G a group.

- A resolution of a group G is a sequence of G-modules $(M_i)_{i\geq 0}$:

$$\mathbb{Z} \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \leftarrow \dots$$

  together with a collection of G-linear operators $d_i : M_i \to M_{i-1}$ such that $\text{Ker } d_i = \mathrm{Im}\, d_{i-1}$
- What is useful to homology computations are free resolutions with all M_i being free G-modules.
- The homology is then obtained by killing off the G-action of a free resolution, i.e replacing the G-modules $(\mathbb{Z}G)^k$ by $\mathbb{Z}^k$, replacing accordingly the d_i by $\tilde{d}_i$ and getting

$$H_i(G) = \text{Ker } \tilde{d}_i / \mathrm{Im}\, \tilde{d}_{i-1}$$

How to get resolutions

- HAP can produce resolutions (with left actions) for finite groups, such that $M_0 = \mathbb{Z}G$ and

$$\mathrm{Im}\ d_1 = \{x = \sum_{g \in G} \alpha_g g \in \mathbb{Z}G \text{ such that } \sum \alpha_g = 0\}$$

- To get resolutions on the right we use the antiisomorphism

$$\begin{array}{rcl} inv : \mathbb{Z}G & \rightarrow & \mathbb{Z}G \\ \sum \alpha_g g & \mapsto & \sum \alpha_g g^{-1} \end{array}$$

- The CTC wall lemma can be used to sum things and get resolutions:
  - Suppose we have a resolution,

    $$\mathbb{Z} \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \leftarrow \dots$$

    which is not free, then we can lift the M_i to free modules $R_{i,0}$

    $$\mathbb{Z} \leftarrow R_{0,0} \leftarrow R_{1,0} \leftarrow R_{2,0} \leftarrow \dots$$

    but we no longer have the relation $d_i d_{i-1} = 0$
  - CTC wall gives a method to get a free resolution.

CTC Wall lemma

- We denote d_1 the operator of the $R_{i,0} \to R_{i-1,0}$.
- We can find free resolutions of the $R_{i,0}$ G-modules by G-modules
$$R_{i,0} \leftarrow R_{i,1} \leftarrow R_{i,2} \leftarrow \dots$$
with the boundary operators being named d_0.
- Then we search for operators $d_k : R_{i,j} \to R_{i-k,j-1+k}$ such that
$$D = \sum_{i=0}^{\infty} d_i$$
realize a free resolutions of G-modules $\sum_{i+j=k} R_{i,j}$.
- It suffices to solve the equations
$$\sum_{h=0}^{k} d_h d_{k-h} = 0$$

CTC Wall lemma

- One way is to have the expression

$$d_k = -h_0(\sum_{h=1}^{k} d_h d_{k-h})$$

  with h_0 a contracting homotopy for the d_0 operator, i.e. an operator $h_0 : R_{i,j} \to R_{i,j+1}$ such that $d_0(h_0(x)) = x$ if x belongs to the image of d_0.
- This gives a recursive method for computing first d_1 from the relations

$$d_1 d_0 + d_0 d_1 = 0$$

- Then d_2, d_3, ...
- CTC Wall also gives a contracting homotopy for the obtained resolution.

V. Homology of Mathieu groups

Mathieu groups

- A permutation group G acting on $\{1, \dots, n\}$ is called k-transitive if it is transitive on k-uples $(x_1, \dots, x_k)$.
- The residual stabilizer $Res_k(G)$ of a k-transitive group is the stabilizer of $(x_1, \dots, x_k)$.
- The Mathieu groups were discovered by Émil Mathieu:

Group	simple	sporadic	$\lvert G\rvert$	k	$\lvert Res_k(G)\rvert$
M_9	no	-	72	2	1
M_{10}	no	-	720	3	1
M_{11}	yes	yes	7920	4	1
M_{12}	yes	yes	95040	5	1
M_{21}	yes	$= PSL(3,4)$	20160	2	48
M_{22}	yes	yes	443520	3	48
M_{23}	yes	yes	10200960	4	48
M_{24}	yes	yes	244823040	5	48

- Note that the 2-transitive groups are classified.

Orbit polytope for Mathieu groups

- If G is a k-transitive group acting on n points, then we take the vector

$$v = (1, 2, 3, \dots, k, 0^{n-k}) \text{ and } G.v = \mathrm{Sym}(n).v$$

- The fact that $\mathrm{Sym}(n)$ is a Coxeter group means that we can describe the face-lattice of $\mathrm{Sym}(n).v$ simply.
- In fact for the vectors v chosen, the orbit polytope $\mathrm{Sym}(n).v$ is simple, i.e. every vertex is adjacent to $n-1$ vertices.
- The vertex stabilizer has size 48, but this is manageable.

CTC wall in practice: right cosets

- Take $R_{k,0}$, which is sum of orbits O_i of faces of dimension k.
- We compute resolutions $\tilde{R}_{k,i,l}$ of Stab f_l with f_l representative of O_l.

$$R_{k,i} = \oplus_{l=1}^{r} \tilde{R}_{k,i,l}$$

- The matrix of the operator $d_0 : R_{k,i} \to R_{k,i-1}$ is then a block matrix of the $\tilde{d}_0 : \tilde{R}_{k,i,l} \to \tilde{R}_{k,i-1,l}$
- For the contracting homotopy of a vector $v \in R_{k,i}$:
  - Decompose v into components $v_l \in \tilde{R}_{k,i,l} \otimes \mathbb{Z}G$
  - Decompose v_l into right cosets

$$v_l = \sum_s v_{s,l} g_s$$

    with $g_s \in G$ distinct right Stab f_l-cosets and $v_{s,l} \in \tilde{R}_{k,i,l}$.
  - Apply the contracting homotopy h_0 of the resolution $\tilde{R}_{k,i,l}$ to $v_{s,l}$ and sum

$$h_0(v_l) = \sum_s h_0(v_{s,l}) g_s$$

CTC wall in practice: signature

- Take e an edge and s an element of the stabilizer inverting e.
- The element $e - e.s$ belong to the image of d_0, say $d_0(w) = e - e.s$
- If $d_1(e) = v - v.g$ then we have

$$\begin{array}{rcl} d_1(d_0(w)) & = & d_1(e - e.s) \\ & = & (v - v.g) - (v - v.g).s \\ & = & v.(Id + g.s) - v.(Id + s.g^{-1}).g, \end{array}$$

  which do not belong to $\mathrm{Im} d_0$!
- What is needed is for every element $s \in \mathrm{Stab}\, f$ a signature $\det_f(s) = \pm 1$, i.e., the determinant of s acting on the linear space of f.
- ϵ defines to a $\mathbb{Z}\,\mathrm{Stab}\, f$ isomorphism:

$$\epsilon(\sum \alpha_g g) = \sum \alpha_g \det_f(g) g$$

- The matrix d_0 coming from the resolution are replaced by $\epsilon(d_0)$.

Some examples

- M_{24} (51 minutes, 250M) dimensions 1, 9, 50, 203, 635:

$$H_0(M_{24}) = \mathbb{Z},\ H_1(M_{24}) = 0,$$
$$H_2(M_{24}) = 0,\ \text{and}\ H_3(M_{24}) = \mathbb{Z}/12\mathbb{Z}.$$

- M_{23} (20 minutes, 140M) dimensions 1, 8, 41, 155, 457:

$$H_0(M_{23}) = \mathbb{Z},\ H_1(M_{23}) = 0,$$
$$H_2(M_{23}) = 0,\ \text{and}\ H_3(M_{23}) = 0.$$

What's next?

- Recursive use of CTC Wall?
  - This requires computing contracting homotopy at the polyhedral level
  - CTC Wall lemma also provides a recursive method of computation.
- Banking system?
  - Since most of computing time is taken by contracting homotopy, the gain is not obvious.
- Other groups?
  - The key ingredient of success of the method is that Mathieu groups are k-transitive for high k, and so we can use a polytope coming from Coxeter groups.
  - For other groups, there is no reason to expect things to be simple.

THANK

YOU