# Practical computation of Hecke operators

Mathieu Dutour Sikirić

Institute Rudjer Bošković, Croatia

October 30, 2014

# I. Modular forms

# Modular forms for $\mathrm{SL}(2,\mathbb{Z})$

- We call $\mathbb{H} = \{z \in \mathbb{C} \text{ s.t. } Im(z) > 0\}$ the upper half-plane.
- A function $f : \mathbb{H} \to \mathbb{C}$ is called a modular form of weight $k$ for $\mathrm{SL}(2,\mathbb{Z})$ if:
  - $f$ is holomorphic
  - For any matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

  - $f$ is holomorphic at the cusps.
- Modular forms are of primary importance in number theory.
- Let us call $M_k$ the space of modular forms of weight $k$. We have the Shimura-Eichler isomorphism:

$$M_k \simeq H_1(\mathrm{SL}_2(\mathbb{Z}), R_{k-2})$$

with $R_k$ the space of homogeneous polynomials of degree 2.

# The general case and Hecke operators

- We want to find modular forms for some finite index subgroups $\Gamma$ of $\mathrm{SL}(n,\mathbb{Z})$ with $n > 2$ (and other groups as well).
- What is known is that the spaces of modular forms are isomorphic to the space

$$H_k(\Gamma,\mathbb{Q})$$

- But in order to understand the operators we need more than just the dimension and the solution to that is to consider the Hecke operators.
- This is the only way we know of extracting the arithmetic informations.
- The perfect domain method that we will present works for $\mathrm{GL}_n(\mathbb{Z})$, $\mathrm{GL}_n(R)$ and $\mathrm{Sp}(4,\mathbb{Z})$.
- In the following the pictures/examples will be for $\mathrm{SL}_2(\mathbb{Z})$ and applications for $\mathrm{Sp}(4,\mathbb{Z})$.

# II. Perfect domain complex

# Arithmetic minimum of positive definite matrices

- Denote by $S^n$ the vector space of real symmetric $n \times n$ matrices, $S^n_{>0}$ the convex cone of real symmetric positive definite $n \times n$ matrices and $S^n_{\geq 0}$ the convex cone of real symmetric positive semidefinite $n \times n$ matrices.
- The arithmetic minimum of $A \in S^n_{>0}$ is

$$\min(A) = \min_{x \in \mathbb{Z}^n - \{0\}} A[x] \text{ with } A[x] = x^T A x$$

- The minimal vector set of $A \in S^n_{>0}$ is

$$\mathrm{Min}(A) = \{x \in \mathbb{Z}^n \mid A[x] = \min(A)\}$$

- The matrix $A_{hex} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ has

$$\mathrm{Min}(A_{hex}) = \{\pm(1,0), \pm(0,1), \pm(1,-1)\}.$$

# Perfect forms and domains

- A matrix $A \in S^n_{>0}$ is perfect (Korkine & Zolotarev) if the equation

$$B \in S^n \quad \text{and} \quad x^T B x = \min(A) \text{ for all } x \in \text{Min}(A)$$

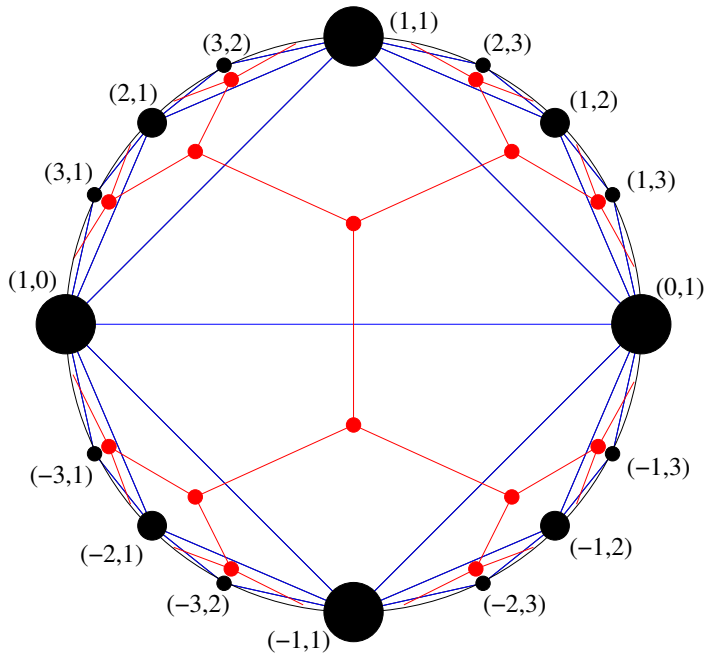
  implies $B = A$.
- If $v \in \mathbb{Z}^n$ then the corresponding rank 1 form is $p(v) = vv^T$.
- If $A$ is a perfect form, its perfect domain is

$$\text{Dom}(A) = \sum_{v \in \text{Min}(A)} \mathbb{R}_+ p(v)$$

- If $A$ has $m$ shortest vectors then $\text{Dom}(A)$ has $\frac{m}{2}$ extreme rays.
- Together they define the perfect domain complex
- So actually, the perfect domains realize a tessellation not of $S^n_{>0}$, nor $S^n_{\geq 0}$ but of the rational closure $S^n_{rat,\geq 0}$.

# Well rounded forms and retract

- A form $Q$ is said to be well rounded if it admits vectors $v_1$, ..., $v_n$ such that
  - $(v_1, \ldots, v_n)$ form a $\mathbb{R}$-basis of $\mathbb{R}^n$ (not necessarily a $\mathbb{Z}$-basis)
  - $v_1, \ldots, v_n$ are shortest vectors of $Q$.
- The set of well rounded forms defines the Well rounded retract $WR_n$ of dimension $\frac{n(n-1)}{2}$.
- Every positive definite form can be continuously deformed to a well rounded form.
- Every face of $WR_n$ has finite stabilizer.



# Topological applications

- The fact that we have finite stabilizers for all faces means that we can compute rational homology of $\mathrm{GL}_n(\mathbb{Z})$ efficiently.
- This has been done for $n \leq 7$
  - P. Elbaz-Vincent, H. Gangl, C. Soulé, *Perfect forms, K-theory and the cohomology of modular groups*, Adv. Math 245 (2013) 587–624.
- As an application, we can compute $K_n(\mathbb{Z})$ for $n \leq 8$.
- By using perfect domains, we can compute the action of Hecke operators on the cohomology.
- This has been done for $n \leq 4$:
  - A. Ash, M. McConnells, *Experimental indications of three-dimensional Galois representations from the Cohomology of* $\mathrm{SL}_3(\mathbb{Z})$, Experimental Mathematics 1-3 (1992) 209–223.
  - P.E. Gunnells, *Computing Hecke Eigenvalues Below the Cohomological Dimension*, Experimental Mathematics 9-3 (2000) 351–367.

# Linear Reduction theories for $S^n_{rat,\geq 0}$

Some $\mathrm{GL}_n(\mathbb{Z})$ invariant tessellations of $S^n_{rat,\geq 0}$:

- The perfect form theory (Voronoi I) for lattice packings (full face lattice known for $n \leq 7$, perfect domains known for $n \leq 8$)
- The central cone compactification (Igusa & Namikawa) (Known for $n \leq 6$)
- The $L$-type reduction theory (Voronoi II) for Delaunay tessellations (Known for $n \leq 5$)
- The $C$-type reduction theory (Ryshkov & Baranovski) for edges of Delaunay tessellations (Known for $n \leq 5$)
- The Minkowski reduction theory (Minkowski) it uses the successive minima of a lattice to reduce it (Known for $n \leq 7$) not face-to-face
- Venkov's reduction theory also known as Igusa's fundamental cone (finiteness proved by Crisalli and Venkov)

# The case of $\mathrm{Sp}(4,\mathbb{Z})$

- For the symplectic group $\mathrm{Sp}(2n,\mathbb{Z})$, we do not know a CW complex that is preserved by the action. The only known exception is for $\mathrm{Sp}(4,\mathbb{Z})$:
  - R. MacPherson and M. McConnel, *Explicit reduction theory for Siegel modular threefolds*, Invent. Math. **111** (1993) 575–625.
- The idea is to take the space of symplectic Gram matrices, i.e.

$$S^n_{Sp} = \left\{A \in S^n_{>0} : AJA^t = J\right\}$$

  with $J$ the matrix defining the symplectic form.
- With this one gets a description in terms of combinatorial object which correspond to some cones of the perfect domain complex.
- The top dimensional cells have finite stabilizers but the lowest dimensional cells correspond to rank 1 forms and have infinite stabilizers.

# III. $G$-modules and 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

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

- 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 $\{v_1, \ldots, v_m\}$, 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, independent set, basis of a $G$-module. But not every finitely generated $G$-module admits a basis.

# Polyhedral complex and $G$-module

Let us take a $n$-dimensional polyhedral complex and a group $G$ acting on it.

- Denote $n_k$ the number of orbits of faces of dimension $k$.
- For each dimension $k$ we need to select a number of orbit representatives $G_1^k, \ldots, G_{n_k}^k$.
- The differentials of a $k$-dimensional face $F$ is

$$\begin{aligned} d_k F &= \sum_{i=1}^{N} \alpha_i F_i \quad \text{(no group action)} \\ &= \sum_{i=1}^{N} \alpha_i G_{p(i)}^{k-1} g_i \quad g_i \in \Gamma \\ &= \sum_{i=1}^{n_{k-1}} G_i^{k-1} \left\{ \sum_{j=1}^{m_i} \alpha_{i,j} g_{i,j} \right\} \quad \text{(grouping terms)} \end{aligned}$$

- So, we can express the differencial $d_k$ as a $G$-module $n_k \times n_{k-1}$ matrix.
- The terms $g_i$ are not defined uniquely because the stabilizer may not be trivial.

# 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 Ker $d_i = \operatorname{Im} d_{i-1}$
- What is useful to homology computations are free resolutions with all $M_i$ being free $G$-modules, i.e. $(\mathbb{Z}G)^d$ for some $d$.
- The resolution from a polyhedral complex is free if and only if the stabilizers are all trivial.
- In terms of homology if an element $s$ stabilizes a face $F$ then we have

  $$F.s = \epsilon_F(s)F \text{ with } \epsilon_F(s) = \pm 1$$

  whether $s$ preserves the orientation of $F$ or not.

# Using resolutions for computing group homology

- The method is to take a free-resolution of a group $G$.
- 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

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

- The big problem is to get free resolutions. It is not an easy task.
- Two alternatives:
  - Compute free resolutions for the stabilizers and put it all together with the CTC Wall lemma. KeyWord: Spectral sequence
  - Compute a resolution with only finite stabilizers: Kill the faces with orientation reversing stabilizers. Kill the $G$-action. Then compute the quotient. It is the rational homology.

# IV. Hecke operators on homology

# Definitions

We take $\Gamma$ a finite index subgoup of $\mathrm{SL}(n, \mathbb{Z})$.

- We consider elements $g \in \mathrm{GL}(n, \mathbb{Q})$ such that $\Gamma \cap g^{-1}\Gamma g$ has finite index in $\Gamma$.
- We want to consider the action of $g$ on the homology classes. The problem is that the homology are obtained after killing the $\Gamma$ action, so we need to consider more than just $g$.
- The idea is to split the double coset

$$\Gamma g \Gamma = g_1\Gamma \cup g_2\Gamma \cup \cdots \cup g_m\Gamma$$

  into right cosets.
- The splitting can be done by a very simple iterative algorithm if we have:
  - A generating set for $\Gamma$.
  - An oracle function $\phi$ for testing membership in $\Gamma$
- The perfect domain complex gives a generating set and $\Gamma$ is usually defined by some congruence relations.

# Actions on the perfect domain complex

- A $k$-dimensional face $F$ of the perfect domain complex is defined as a family of vectors $v_1, \ldots, v_m$ with $v_i \in \mathbb{Z}^n$.
- The image $F.g$ is defined by the vectors $v_1 g, \ldots, v_m g$.
- In dimension $k = 1$ all is ok:
  - They are spanned by just one vector. So the image $F.g$ is spanned by $v_1 g$.
  - $v_1 g$ is not necessarily integral, but it is a multiple of an integral vector.
  - So, we can define the action in dimension 1.
- For higher dimensions we want to do recursively. That is if:

$$d_k F = \sum_i \alpha_i F_i h_i \text{ with } h_i \in \Gamma$$

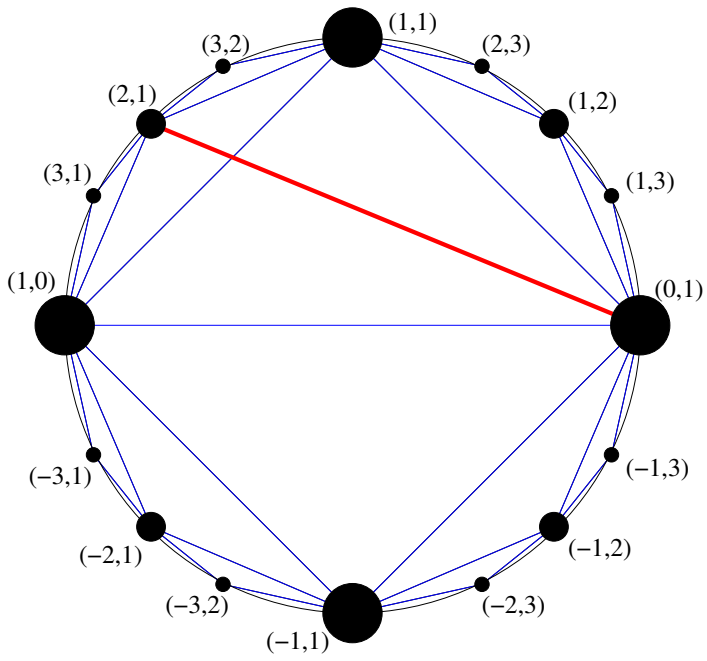
then

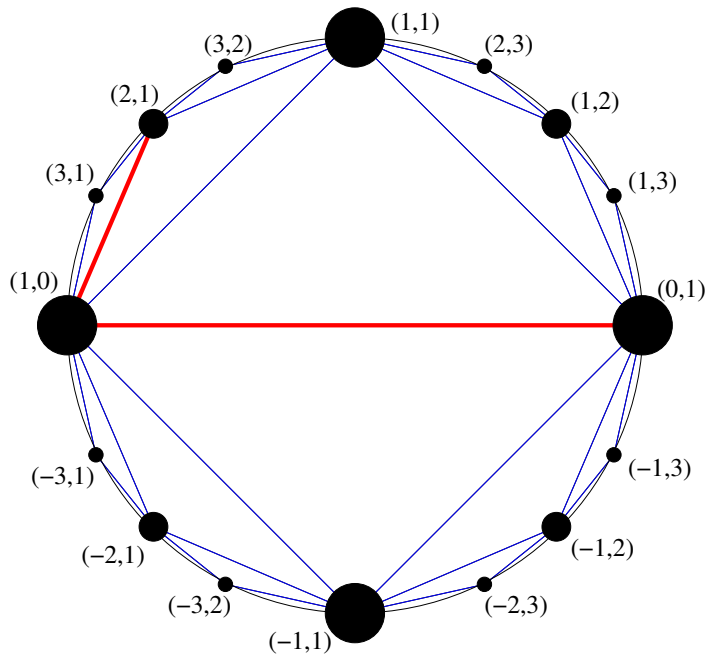
$$\begin{aligned} d_k(F.g) = b &= \textstyle\sum_i \alpha_i F_i h_i g \\ &= \textstyle\sum_i \alpha_i F_i g_i k_i \text{ with } k_i \in \Gamma \end{aligned}$$

So, we need to compute on all cosets. We must have $d_{k-1} b = 0$.

# Two dimensional example

- Let us take the face $F = \{(1,0),(0,1)\}$ and $g = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$.
- We then have




- So we set

$$F.g = F.\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} + F$$

# Computing on the perfect domain complex: Groups

- We need to compute stabilizers of cells (possibly infinite) and checking equivalence.
- What we can do is for a face $F = \{v_1, \ldots, v_m\}$ with $\text{rank}\{v_1, \ldots, v_m\} = k < n$ is to:
  - Find a subspace $W \subset \mathbb{Z}^n$ of rank $k$ with $v_i \in F$ and $W = (W \otimes \mathbb{R}) \cap \mathbb{Z}^n$.
  - Compute the finite group of automorphism of $F$ in $W$.
  - Determine directly the group preserving $W$ pointwise.

  This requires doing the number theory which is ok for $\mathbb{Z}^n$ but harder in other cases.
- An alternative is for a face $F$ to consider all full dimensional cells $G$ with $F \subset G$. We then:
  - have a finite set of such pairs $(F, G)$ up to equivalence.
  - We can enumerate all of them by using the full-dimensional cells.

  This is harder computationally but much simpler and general.

# The invariance problem I

We set $F.g = x = \sum_i \alpha_i F_i g_i$.

- In order for the operator to be consistent we need that for every $s$ stabilizing $F$ we have

$$F.sg = F.g\epsilon_F(s)$$

- If $sg = g'v$ with $g'\Gamma \neq g\Gamma$ then we simply write

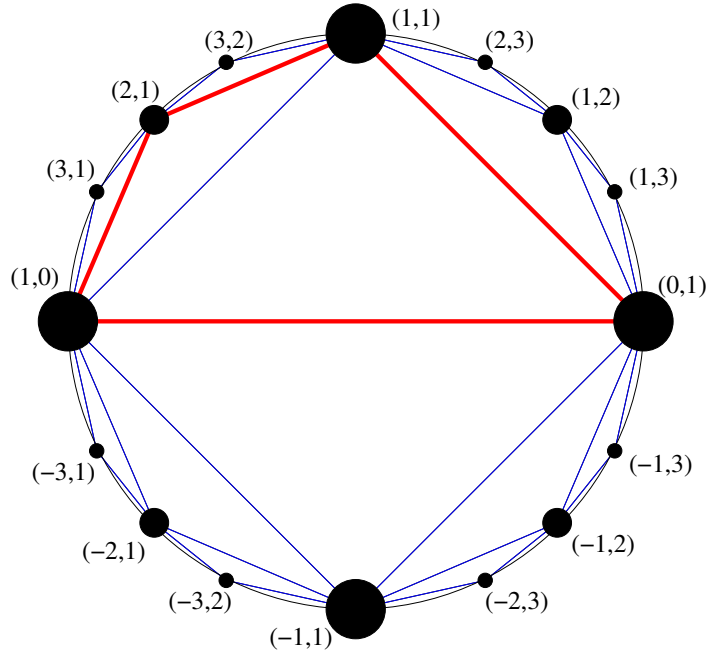
$$F.g' = (F.g)v^{-1}\epsilon_F(s)$$

- However if $sg = gv$ with $v \in \Gamma$ then we face a consistency problem because we could have $d_{k-1}b \neq 0$.
- Let us call $\mathrm{Stab}(x)$ the corresponding stabilizer (maybe infinite).
- Let us call $O(x)$ the orbit of the solution $x$ under $\mathrm{Stab}(x)$.
- The following is invariant:

$$\frac{1}{|O(x)|} \sum_{u \in O(x), u.g = x} \epsilon_F(g)u$$

# The invariance problem II

- For our example this gives




- In order to have $O(x)$ finite we impose that the solution $x$ has the same singularities as $F.g$.
- If the solutions are not consistent then we cannot solve the system.
- By taking the average we forfeit the integral solution and so we can only compute the action on rational homology.

# Computing on the perfect domain complex: Equations I

- In order to build the Hecke operators, we need to be able to solve

$$d_k x = b$$

  for $x$ a $k$-dimensional chain and $b$ a $k-1$ dimensional chain.
- A necessary and sufficient condition for $x$ to exist is $d_{k-1} b = 0$.
- In other words we have an infinite integral linear system.
- The chosen solution is to take a family $C_1, \ldots C_r$ of top-dimensional cells such that
  - Any face occuring in $b$ is contained in at least one $C_i$.
  - The graph defined by all $C_i$ with adjacency relation is connected.
- If the system has no solution then we iterate by adding all cells neighboring to the $C_i$.

# Computing on the perfect domain complex: Equations II

- We are thus led to trying to find solutions of equations

$$Ax = b$$

  with $A$ a very large matrix.
- We want to find sparse solutions because they are expected to be the nicest and simplest.
- When searching for sparse solutions, a good heuristic is to solve the linear program

$$\min \|x\|_1 \text{ with } Ax = b$$

- We found reasonably fast solutions with `GLPK` and slow ones with `CDD` and `LP_SOLVE`.
- Critical aspect of the computation is how to find sparse solutions of overdetermined linear systems.

# Computing on the perfect domain complex: Equations III

- There is a whole field of science devoted to that: Compressed Sensing, it has many applications to Photography, Facial recognition, Magnetic Resonance Imaging, Network Tomography, etc.
- Our problem is then named "basis pursuit" and two classes of methods have been found to be good: First order linear programming, and Approximate Message Passing.
- First order linear programming relies on small steps in order to obtain an approximate feasible solution without having to solve a linear system. See TFOCS: Templates for First-Order Conic Solvers, `http://cvxr.com/tfocs/`
- Approximate Message Passing relies on ideas of Belief Propagation, Statistical Mechanics, Modern Coding Theory, in order to solve systems, `http://gampmatlab.wikia.com`
- Unfortunately those codes are in `Matlab`. We will have to translate them in `C++`.

# The action on homology

- Say, the group $H_k(\Gamma, \mathbb{Q})$ has dimension $p$.
- It has a basis of cycles

$$c_i = \sum_{j=1}^{n_k} \alpha_{i,j} F_i$$

  with $\alpha_{i,j} \in \mathbb{Z}$ and $F_i$ representatives of orbits of $k$-dimensional faces of the perfect domain complex.
- The Hecke operator on a cycle $c$ is defined as

$$T_g(c) = \sum_i c g_i$$

- Theorem: The operator $T_g$ preserves $H_k$.
- The characteristic polynomial of $T_g$ is the important arithmetic information.

# Results

- The procedure has been implemented successfully for the symplectic group $\mathrm{Sp}(4,\mathbb{Z})$. We take the element

$$g = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$ and the finite index subgroups

$$\Gamma_p = \left\{ P \in \mathrm{Sp}(4,\mathbb{Z}) : P \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix} \pmod{p} \right\}$$

- For example for $p = 7$ the homology groups are of dimension 1, 0, 0, 11, 2, 0. The non-characteristic polynomials of the Hecke action are:
  - $x - 15$
  - $x^{11} - 52x^{10} + 1108x^9 - 14309x^8 + 157475x^7 - 1532582x^6 + 9739638x^5 - 30872097x^4 + 42989994x^3 - 77001840x^2 + 236925000x - 246402000$
  - $x^2 - 20x + 75$

THANK

YOU