Algorithms For Integral Matrix Groups

Alexander Hulpke
Department of Mathematics
Colorado State University
Fort Collins, CO, 80523, USA
www.hulpke.com

Matrix Group Calculations

Matrix groups over commutative ring, given by (finite number) of generating matrices.

What can we say about such groups?

Computers crave finiteness !

Over finite fields: ***matrix group recognition***

Uses: Divide-and-conquer approach. Data structure ***composition tree***. Reduction to simple groups.

Effective Homomorphisms, recursion to kernel, image.

Hasse Principle

Instead of working (globally) over $\mathbb{Z}$, work (locally) modulo different coprime numbers, combine (Paradigm: Chinese Remainder Theorem)

The purpose of this talk is to show this principle applies to a certain class of integral matrix groups.

Matrix Groups Over $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

First consider $m = p^2$. ($m = p^a$ ditto.)

Reduction mod p gives hom. φ: $SL_n(\mathbb{Z}_m) \to SL_n(\mathbb{Z}_p)$.

Kernel $\{I + pA | A \in \mathbb{Z}_p{}^{n \times n}\}$. Note: $\det(I + pA) = 1 + p \cdot \mathrm{Tr}(A)$.

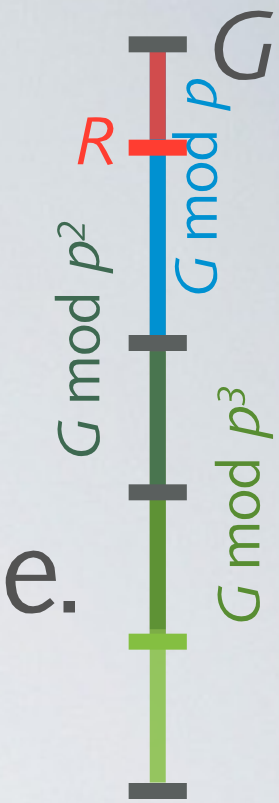
Multiplication:

$$(I+pA)(I+pB) = I + p(A+B) + p^2 \ldots \equiv I + p(A+B) \bmod m$$

is by addition of the the A-parts modulo p.

(Under map $A \mapsto I + pA$, $\ker\varphi$ is adjoint module in Lie-sense.)

Working With $G \leq GL_n(\mathbb{Z}_m)$



If $m=p^a$, first consider image H of G modulo p.

- Matrix group recognition on H. Get comp. tree. Split in radical factor and solvable radical.
- Presentation gives (module) generators of kernel. Consider p/p^2 layer as F_p-vector space. Basis with Spinning Algorithm.
- Combine to presentation of G mod p^2
- Iterate on p^2/p^3 kernel etc.

Multiple Primes

If m is product or multiple primes, G is a subdirect product of its images modulo prime powers.

To get standard solvable radical data structure:

- Consider images H_p modulo each prime.
- Combine radical factor homomorphisms ρ_p for different primes to direct product of images.
- Combine the PCGS for the radicals for different primes.
- Extend PCGS through the extra layers if there are higher prime powers in m. (Take new kernel generators each time, linear algebra on $1/p(I-x)$.)

Result: Data structure, in particular order, for $G \leq GL_n(\mathbb{Z}_m)$.

Multiple Primes

If m is product or multiple primes, G is a subdirect product of its images modulo prime powers.

To get standard solvable radical data structure:

- Consider images H_p modulo each prime.
- Combine radical factor homomorphisms ρ_p for different primes to direct product of images.
- Combine the PCGS for the radicals for different primes.
- Extend PCGS through the extra layers if there are higher

PCGS: polycyclic generating set — data structure for solvable group that combines bases for different vector space layers into object that can get coefficients.

Multiple Primes

Careful: This can still be subdirect.

ct or multiple primes, G is a subdirect product of o prime powers.

solvable radical data structure:

ges H_p modulo each prime.

ical factor homomorphisms ρ_p for different p direct product of images.

- Combine the PCGS for the radicals for different primes.
- Extend PCGS through the extra layers if there are higher prime powers in m. (Take new kernel generators each time, linear algebra on $1/p(I\text{-}x)$.)

Result: Data structure, in particular order, for $G \leq GL_n(\mathbb{Z}_m)$.

```
gap> LoadPackage("matgrp"); # available for GAP 4.8.3
   [...]
gap> g:=SL(3,Integers mod 1040);
SL(3,Z/1040Z)
gap> ff:=FittingFreeLiftSetup(g);;
gap> Size(g);
849852961151281790976000
gap> Collected(RelativeOrders(ff.pcgs));
[ [ 2, 24 ], [ 3, 1 ] ]
gap> m:=MaximalSubgroupClassReps(g);;time;
24631 #24 seconds
gap> List(m,x->Size(g)/Size(x));
[ 256, 7, 7, 8, 183, 183, 938119, 1476384, 3752476,
  123708, 123708, 123708, 31, 31, 3100, 3875, 4000 ]
```

Arithmetic Groups

Roughly: Discrete subgroup of Lie Group, defined by arithmetic properties on matrix entries(e.g. det=1, preserve form).

Definition: G linear algebraic group, over number field K. An *arithmetic group* is $\Gamma < G$, such that for integers $\mathcal{O} < K$ the intersection $\Gamma \cap G(\mathcal{O})$ has finite index in both intersectants.

Prototype: Subgroups of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$ of finite index.

Applications: Number Theory (Automorphic Forms), Topology, Expander Graphs, String theory, ...

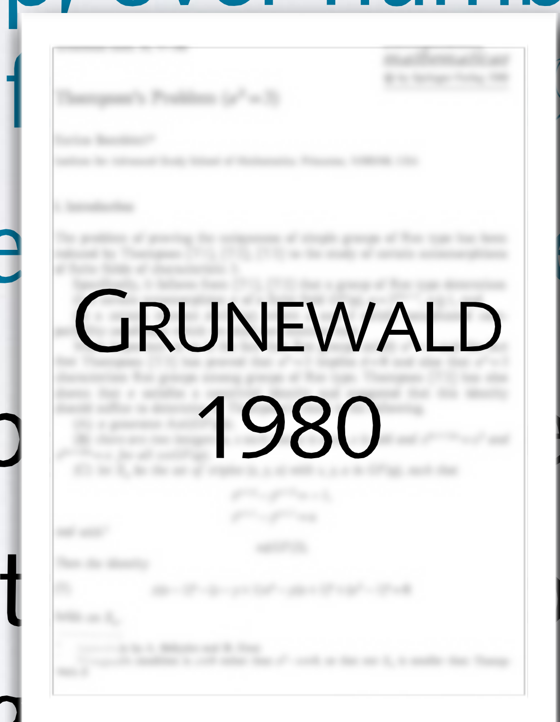
Theoretical algorithms for problems, such as conjugacy, known, but infeasible in practice.

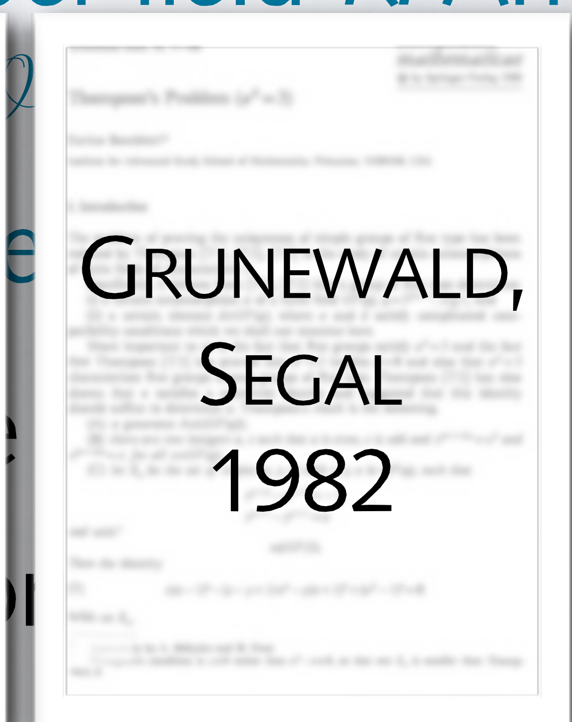
Arithmetic Groups

Roughly: Discrete subgroup of Lie Group, defined by arithmetic properties on matrix entries(e.g. det=1, preserve form).

Definition: G linear algebraic group, over number field K. An *arithmetic group* is $\Gamma < G$, such that f

intersection $\Gamma \cap G(\mathcal{O})$ has finite inde





Prototype: Subgroups of $SL_n(\mathbb{Z})$, Sp

Applications: Number Theory (Aut

Topology, Expander Graphs, String theory, ...

Theoretical algorithms for problems, such as conjugacy, known, but infeasible in practice.

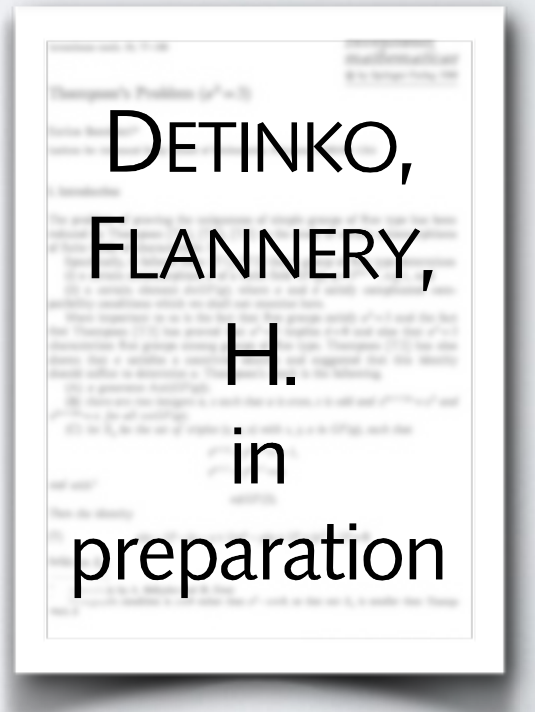
Subgroups Of $SL_n(\mathbb{Z})$, $Sp_{2n}(\mathbb{Z})$

Take subgroup $G < SL_n(\mathbb{Z})$ (or Sp_{2n}) given by finite set of generators. G is arithmetic if it has finite index.

- Can we determine whether G has finite index?
- If G has finite index, can we determine it?

Here: Only SL case.

Joint work with ALLA DETINKO, DANE FLANNERY (St. Andrews / NUI Galway).



Proving Finite Index

Consider $SL_n(\mathbb{Z})$ as finitely presented group.

Generators: Elementary matrices.

Relators (obvious ones: orders of products, commutators of generators) are known.

Write generators of G as words in these generators (Gaussian Elimination. Often better: Words in images mod m for sufficiently large m).

Enumerate cosets (Todd-Coxeter). If the index is finite this process will terminate, and give the correct index.

Proving Finite Index

Consider $SL_n(\mathbb{Z})$ as finitely presented group.

Generators: Elementary matrices.

Relators (obvious ones: orders of products,

Caveat: Coset enumeration is a *method*, not an *algorithm*: run-time cannot be bounded. If index is infinite the process does not terminate.

Enumerate cosets (Todd-Coxeter). If the index is finite this process will terminate, and give the correct index.

Second Caveat

The obstacles of coset enumeration are inherent to the problem.

$SL_n(\mathbb{Z})$ contains free subgroups if $n \geq 3$, and it is thus impossible to have an decision algorithm that is guaranteed to answer *whether* elements generate a subgroup of finite index.

Thus assume an *oracle* promises finite index (or hope to be lucky).

Second Caveat

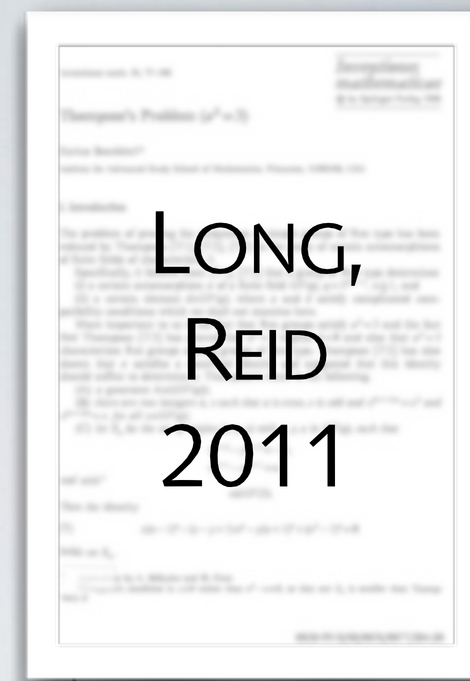
The obstacles of coset enume
the problem.

on Turing-machine
equivalent computer.
Entscheidungsproblem

$SL_n(\mathbb{Z})$ contains free subgroups if $n \geq 3$, and it is thus impossible to have an decision algorithm that is guaranteed to answer *whether* elements generate a subgroup of finite index.

Thus assume an *oracle* promises finite index (or hope to be lucky).

Easy Example



Let $SL_3(\mathbb{Z}) \geqq \beta_T =$

$$\left\langle \begin{pmatrix} -1+T^3 & -T & T^2 \\ 0 & -1 & 2T \\ -T & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -T^2 & 1 & -T \\ T & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & T^2 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle,$$

then $[SL_3(\mathbb{Z}): \beta_{-2}]=3670016.$ (Barely) doable.

But $[SL_3(\mathbb{Z}): \beta_7]=24193282798937316960$

$=2^5 3^4 5 \cdot 7^{10} 19 \cdot 347821 \sim 2^{64}.$ Hopeless.

Congruence Subgroups

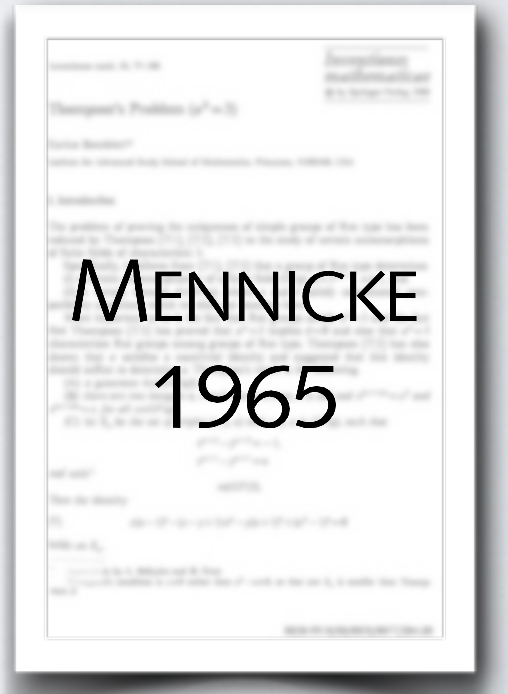
The *m*-th congruence subgroup $\Gamma_m \leq \mathrm{SL}_n(\mathbb{Z})$ is the kernel of the reduction φ_m modulo m. Image is $\mathrm{SL}_n(\mathbb{Z}_m)$.

If $G \leq \mathrm{SL}_n(\mathbb{Z})$ has finite index, there exists integer l such that $\Gamma_l \leq G$. The smallest such l is called the *level* of G.

Then $[\mathrm{SL}_n(\mathbb{Z}):G]=[\mathrm{SL}_n(\mathbb{Z}_l) : \varphi_l(G)]$.

Calculate this second index from generators of G modulo l.

Thus sufficient to find level to get index.



Strategy

Consider congruence images $\varphi_m(G) < SL_n(\mathbb{Z}_m)$ for increasing values of m to find level l of G.

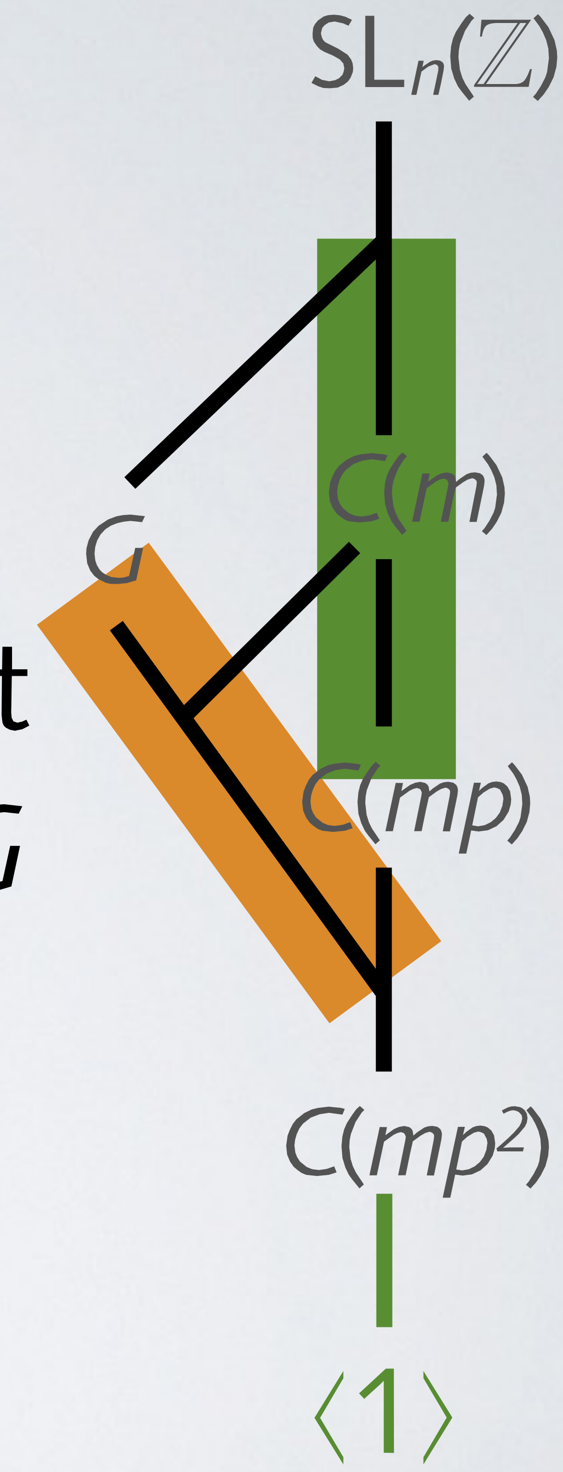
- Find the primes dividing l
- Find the prime powers dividing l
- Criterion on whether $I_m = [SL_n(\mathbb{Z}_m) : \varphi_m(G)]$ increases.

Same Index

Let $G \leq SL_n(\mathbb{Z})$ and $C(m) = \ker \varphi_m$.

If for a given m and prime p we have that $I_m = I_{mp}$ but $I_{mp} \neq I_{mp^2}$, then (modulo mp^2) G contains a supplement to $C(mp)$.

We show such supplements do not exist, thus a stable index remains stable.



Kernel Supplements

Let p be prime, $a \geq 2$, $m=p^a$ and $H=\mathrm{SL}(n,\mathbb{Z}_m)$ for $n \geq 2$ (or $H=\mathrm{Sp}(2n, \mathbb{Z}_m)$ for $n \geq 1$). Let $C(k) \triangleleft H$ kernel mod k.

Theorem: (D-F-H.) $C(p^{a+1})$ has no proper supplement in $C(p^a)$.

Theorem: (Beisiegel 1977, Weigel 1995, …,D-F-H.)

Let $a=2$. $C(p)$ has a supplement in H if and only if

(a) $H=\mathrm{SL}(2,\mathbb{Z}_4)$, $\mathrm{SL}(2,\mathbb{Z}_9)$, $\mathrm{SL}(3,\mathbb{Z}_4)$, or $\mathrm{SL}(4,\mathbb{Z}_4)$.

(b) $H=\mathrm{Sp}(2,\mathbb{Z}_4)$, $\mathrm{Sp}(2,\mathbb{Z}_9)$.

<u>Proof</u>: Small cases/counterexample by explicit calculation. Use nice elements to show supplement contains kernel.

Index Algorithm

Assume that G has (unknown) finite index and level l. Assume we know the set $\mathscr{P}$ of primes dividing l.

1. Set m=lcm(4,$\prod \mathscr{P}$).
2. While for any $p \in \mathscr{P}$ we have

   $[SL_n(\mathbb{Z}_m):\varphi_m(G)]<[SL_n(\mathbb{Z}_{pm}):\varphi_{pm}(G)]$, set $m:=pm$.
3. Repeat until index is stable, level divides m.

Show also that one can work prime-by-prime.

Index Algorithm

Assume that G has (unknown) finite index and level l. Assume we know the set $\mathscr{P}$ of primes dividing l.

1. Set m=lcm(4,∏ $\mathscr{P}$).
2. While for any $p \in \mathscr{P}$ we have $[SL_n(\mathbb{Z}_m):\varphi_m(G)]<[SL_n(\mathbb{Z}_{pm}):\varphi_{pm}(G)]$, set $m:=pm$.
3. Repeat until index is stable, level divides m.

Show also that one can wor because we start with 4

Index Algorithm

Assume that G has (unknown) finite index and level l. Assume we know the set $\mathscr{P}$ of primes dividing l.

1. Set m=lcm(4,$\prod \mathscr{P}$).

2. While for any $p \in \mathscr{P}$ we have

   $_m(G)$], set $m:=pm$.

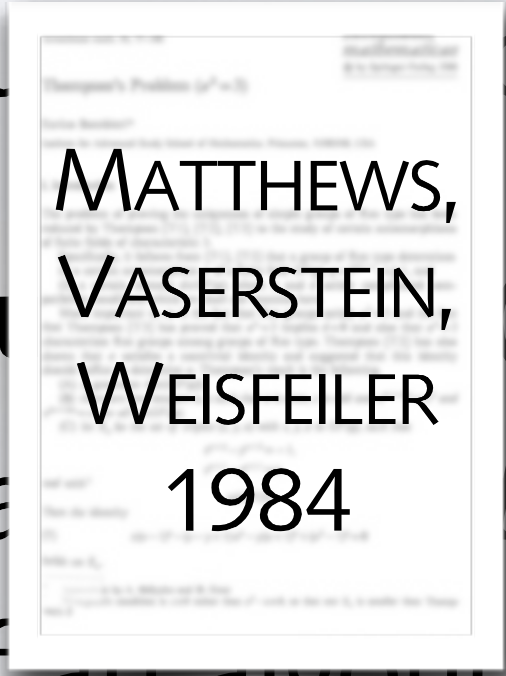
   A group projecting onto $\mathrm{PSL}_n(p)$ has only trivial subdirect products with subgroups of $\mathrm{PSL}_n(q)$

3. Repeat until index is stable, level divides m.

Show also that one can work prime-by-prime.

Strong Approximation

Theorem: Let $G \leq \mathrm{SL}_n(\mathbb{Z})$. If there is a prime $p > 2$ such that G mod p=$\mathrm{SL}_n(p)$, then this holds for almost all primes. Such a group is called *Zariski-dense* (which agrees with the usu … or



Caveat: There are dense subgrou … $(\mathbb{Z}$ do not have finite index. (They a … th goes back to the impossibility of an algorithm that determines whether G has finite index.

Strong Approximation

Theorem: Let $G \leq \mathrm{SL}_n(\mathbb{Z})$. If there is a prime $p > 2$ such that G mod p=$\mathrm{SL}_n(p)$, then this holds for almost all primes. Such a group is called *Zariski-dense* (which agrees with the usual definition).

Caveat: There are dense subgroups of $\mathrm{SL}_n(\mathbb{Z})$ that do not have finite index. (They are called *thin*.) This goes back to the impossibility of an algorithm that determines whether G has finite index.

Finding The Set Of Primes

Theorem: Let $n \geq 3$ and suppose G has finite index. The set $\mathscr{P}$ of primes dividing the level l consists of those primes p for which

1. $p>2$ and G mod $p \neq SL_n(p)$, or
2. $p=2$ and G mod 4 $\neq SL_n(\mathbb{Z}_4)$

Proof: If other primes divided the level, there would be a supplement modulo p^2 (or 8).

Representations

G group, F field.

A representation $\rho{:}G{\to}\mathrm{GL}_n(F)$ is *irreducible* if no proper subspace of F^n is invariant under $G\rho$.

It is *absolutely irreducible* if the same holds for subspaces of K^n for any algebraic extension K of F.

Theorem: ρ is absolutely irreducible, iff the matrices $G\rho$ span $F^{n\times n}$.

Irreducible modulo Prime

Let $\rho: G \rightarrow \mathrm{GL}_n(\mathbb{Z})$ a representation that is absolutely irreducible modulo one prime.

The $\mathbb{Z}$-lattice $L \leq \mathbb{Z}^{n\times n}$ spanned by $G\rho$ has rank n^2.

$G\rho$ is absolutely irreducible modulo each prime that does not divide discriminant of L (i.e. almost all).

To find these primes: Approximate L with (random) elements of $G\rho$ until full rank.

Transvections

Arithmeticity implies the existence of *transvections*, elements $t \in G$ with $\mathrm{rk}\,(t-1)=1$.

For such an element let $N = \langle t \rangle^G$ be the normal closure.

Let ρ be reduction modulo prime p with $G^\rho = SL_n(p)$. If $t^\rho - 1 \neq 0$, then t^ρ is transvection and N^ρ is absolutely irreducible. For odd n this implies it is SL.

Let L be the $\mathbb{Z}$-lattice spanned by (elements of) N.

Then $\mathscr{P}$ (primes with G mod $p \neq SL_n(p)$) consists of primes dividing lcm(disc.L, gcd of entries of $t-1$).

```
gap> g:=BetaT(7);
<matrix group with 3 generators>
gap> t:=b1beta(g); # transvection from Long/Reid paper
[ [-685,14,-98], [-16807,344,-2401], [2401,-49,344] ]
gap> RankMat(t-t^0);
1
gap> PrimesForDense(g,t,1);time;
[ 7, 1021 ]
60
gap> MaxPCSPrimes(g,[7,1021]);time;
Try 7 7
Try 49 7
Try 343 7
Try 343 1021
Try 350203 1021
[350203, 24193282798937316960 ] #Proven Index in SL
291395 # about 5 minutes
```

General Case

If we have no transvections but know index is finite:

Use other representations to identify primes.

Note: Representations of $SL_n(p)$ are given by polynomials on matrix entries, come from $SL_n(\mathbb{Z})$

Identify Subgroups

Take a set $\mathscr{R}$ of polynomial representations of $SL_n(\mathbb{Z})$, such that:

1. For every $\alpha \in \mathscr{R}$ the reduction α_p: $SL_n(p) \to \mathbb{Z}_p{}^{m \times m}$ modulo p is a well-defined representation.
2. For prime p sufficiently large (i.e. p>const(n)), α_p is absolutely irreducible.
3. For every maximal $M < SL_n(p)$, there exists $\alpha \in \mathscr{R}$, such that α_p is not abs. irreducible on M.

Existence: Steinberg representation.

Identify Subgroups

Take a set $\mathscr{R}$ of polynomial representations of $SL_n(\mathbb{Z})$, such that:

1. For every $\alpha \in \mathscr{R}$ the reduction α_p: $SL_n(p) \to \mathbb{Z}_p^{m \times m}$ modulo p is a well-defined representation.
2. For prime p sufficiently large (i.e. $p >$ const(n).) α_p is absolutely irreducible.
3. For every maximal $M < SL_n(p)$, there exist such that α_p is not abs. irreducible on M.

Existence: Steinberg representation.

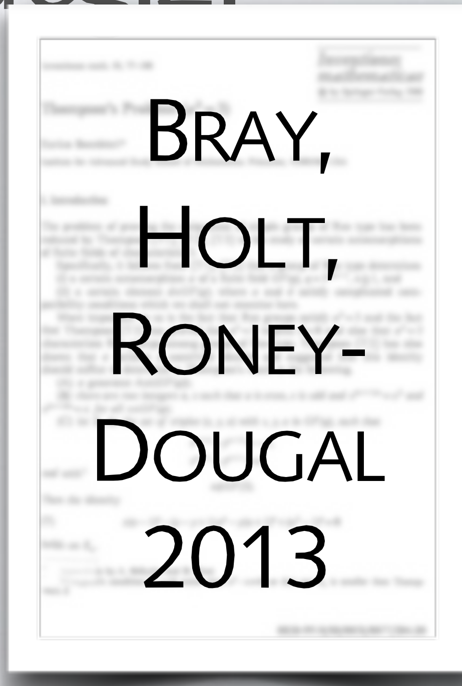
Small n

Let $\mathscr{R}$ be

1. Actions on homogeneous poly.^{s} of degree ≤ 4
2. Antisymmetric square of natural representation.
3. For n=3 (for 3.A_6) a 15-dimensional constituent of the symmetric square of polynomials deg.2.

Then the conjecture holds for $n \leqq 11$ if $p>4$.

Proof by inspection of lists of maximals.



Algorithm For Primes

For each polynomial representation $\rho \in \mathscr{R}$:

- Form (random) elements of G_ρ, span lattice L of full rank $\deg(\rho)^2$.
- Find primes dividing $\mathrm{disc}(L)$.

```
gap> g:=Group([[778,2679,665],[323,797,665],
>        [6674504920,-1557328,34062304949]],
>   [[-274290687,140904793,1960070592 ],[853,4560,294],
>        [151,930,209]]);;
gap> InterestingPrimes(g);   # about 12 hours
irrelevant prime 11
i=1 Pol1
i=2 Pol2 ->[ 53 ]
i=3 Pol3
i=4 rep15 ->[ 19 ]
[ 2, 3, 5, 19, 53 ]

gap> MaxPCSPrimes(g,[2,3,5,19,53]);
Try 1 2, Try 2 2, Try 2 3, Try 6 3, Try 6 5, Try 30 5
Try 30 19, Try 570 19, Try 570 53, Try 30210 53
Index is 5860826241898530299904=[ [ 2,13 ], [ 3,4 ],
 [ 13,3 ], [ 19,3 ], [ 31,1 ], [ 53,3 ], [ 127,1 ] ]
[ 30210, 5860826241898530299904 ]
```

Stronger Approximation, Again

As a corollary we easily get a proof of strong approximation, using our definition of Zariski dense:

Theorem: A subgroup of $SL_n(\mathbb{Z})$ is dense if and only if it surjects onto $SL_n(p)$ for at least one prime $p \geq 3$.

Proof: If G surjects onto $SL_n(p)$ for a prime, the lattice spanned by the Steinberg representation has full rank modulo p, thus full rank over $\mathbb{Z}$.

Open Questions, Directions

- Good set $\mathscr{R}$ of representations (small degree, easy construction)?
- Analog result for Sp or other classical groups? (are there polynomial representations)?
- Better arithmetic for matrices over $\mathbb{Z}_m$.
- Algorithm finds arithmetic closure for dense subgroups. Use this to *prove* finite index in certain cases more efficiently than coset enumeration?