THE UNIVERSITY OF WESTERN AUSTRALIA

Achieving International Excellence

Estimation Problems and Randomised Group Algorithms: Lecture 4

Cheryl E Praeger

Galway, April, 2011

p-Quokka Subset of group G

- Q closed under G-conjugation
- For g in G with p-Jordan decomposition g=us=su

  g in Q if and only if s in Q

Theorem on quokka subsets for groups of Lie type

$$\frac{|Q|}{|G^F|} = \sum_{C \in \mathcal{C}_Q} \frac{|C|}{|W|} \cdot \frac{|T_C^F \cap Q|}{|T_C^F|}.$$

In particular, for positive u_Q, ℓ_Q such that $\ell_Q \leq \frac{|T^F \cap Q|}{|T^F|} \leq u_Q$ for all Q-tori T, and if $\hat{\mathcal{C}}_Q = \bigcup_{C \in \mathcal{C}_Q} C$, then

$$\ell_Q \frac{|\hat{\mathcal{C}}_Q|}{|W|} \leq \frac{|Q|}{|G^F|} \leq u_Q \frac{|\hat{\mathcal{C}}_Q|}{|W|}.$$

Estimation techniques in Lie type groups II

- balanced involutions

  [work with Alice Niemeyer and Frank Luebeck]

- regular semisimple elements

  [work with Akos Seress]

- Lecture 5 will be given by Akos Seress

Finding involutions in classical groups in odd characteristic

- Charles Leedham-Green and Eamonn O'Brien Algorithm to recognise Class(n, q) constructively in natural representation, q odd
- Recursion via constructing involution $\sim \begin{pmatrix} -I_r & 0 \\ 0 & I_{n-r} \end{pmatrix}$ with $n/3 < r \leq 2n/3$
- Construct the centraliser etc.

Leedham-Green O'Brien strategy and bounds

Infeasible to find such involutions by random selection so ...

- by random selection seek an element h of classical H in
  - $\textsc{PreInv}(H) = \{h \in H \mid |h| \text{ even and } h^{|h|/2} \text{ suitable invol. }\}$.
  - Once found construct the involution $h^{|h|/2}$
- Leedham-Green/O'Brien lower bound for proportion:

$$\frac{|\textsc{PreInv}(H)|}{|H|} > \frac{c}{n}$$

where n is dimension, c an absolute constant

Consequences and issues

- With high probability find an element of PREINV(H) in $O(n)$ selections
- To Alice and me this seemed wrong 'order of magnitude'
- We hoped that an absolute constant number of elements might suffice (which turned out to be wrong!)

Worked with Frank Luebeck

- Quokka subset Q of preinvolutions for set I of all balanced involutions
- Why Q a quokka set?
- We gave up on getting upper bounds – focused on getting good lower bounds
- Some statistical evidence suggested we could not do much better

Lower bounds: choose special quokka tori

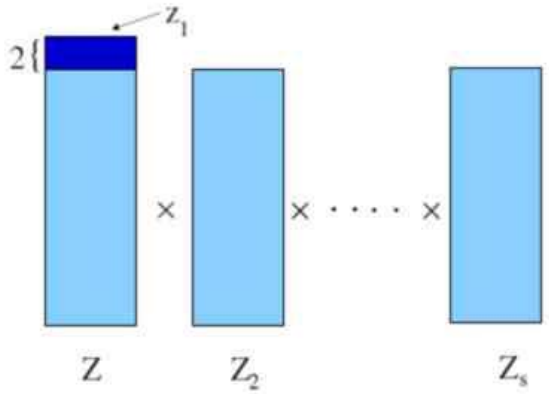
Tori: T^F has one cyclic factor Z, order $q^{2^a k} - 1$ with
$\frac{n}{3} < 2^a k \leq \frac{2n}{3}$, $a \geq 1$, and k odd
all other cyclic direct factors Z' have 2-part
$|Z'|_2 < |Z| = (q^{2^a k} - 1)_2$.

This means

- $|Z'| = q^{2^{a_0} k_0} - 1$ where $0 \leq a_0 < a$ for factors $Z' \neq Z$
- Also the involution $z \in Z$ lies in I

Proportion of quokka elements in these tori?

$$T^F = Z \times Z_2 \times \cdots \times Z_s$$



- Typical $t = (z_1, \ldots, z_s) \in T^F$
- If z_1 as shown then t powers to involution $t^{|t|/2} = (z, 1, \ldots, 1) \in Z$ and hence $t \in \textsc{PreInv}(G^F, I)$.
- Half the elements are like this, so $m_C = \frac{|T^F \cap \textsc{PreInv}(G^F; I)|}{|T^F|} \geq \frac{1}{2}$

Corresponding quokka classes C

All classes C: permutations with one cycle of length $2^a k$ with $\frac{n}{3} < 2^a k \leq \frac{2n}{3}$, $a \geq 1$, and k odd
and all other cycles of lengths not divisible by 2^a.

Union $\mathcal{C}(2^a, k)$ of W-conjugacy classes corresponding to fixed values of a, k has size

$$\frac{n!}{2^a k} \cdot \left\{ \begin{array}{l} \text{proportion of elements of } S_{n-2^a k} \text{ with} \\ \text{no cycles of length a multiple of } 2^a \end{array} \right\}$$

Applying theorem of Erdös and Turán (exact asymptotic form by BLNPS), this is at least

$$\frac{n!}{2^a k} \cdot \frac{1}{\Gamma(1-2^{-a})} \left(\frac{2^a}{n-2^a k} \right)^{1/2^a} \left(1 - \frac{1}{n-2^a k} \right).$$

Putting it together

$$\frac{|\textsc{PreInv}(G^F; I)|}{|G^F|} \geq \sum_{\text{these } c} m_C \cdot \frac{|C|}{n!} \geq$$

$$\sum_{a,k} \frac{\Gamma(1-2^{-a})^{-1}}{2^{a+1}k} \left(\frac{2^a}{n-2^a k}\right)^{1/2^a} \cdot \left(1 - \frac{1}{n-2^a k}\right)$$

$$> \frac{3}{4\sqrt{\pi}\, n} \left(1 - \frac{3}{n}\right) \cdot \sum_{a,k} \left(\frac{1}{n}\right)^{1/2^a}$$

$$> \frac{1}{24\sqrt{\pi}} \sum_{a} 2^{-a} n^{-1/2^a}$$

For the answer

$$\frac{|\textsc{PreInv}(G^F; I)|}{|G^F|} \geq \frac{1}{24\sqrt{\pi}} \sum_a 2^{-a} n^{-1/2^a}$$

- $a = 1$ gives contribution $O(n^{-1/2})$
- largest $a = O(\log_2 n)$ gives contribution $O(n^{-1})$
- Value of a giving largest contribution is (by calculus!) $a \sim \log_2(\log_2(n))$

From this single value of a we get

$$\frac{|\textsc{PreInv}(G^F; I)|}{|G^F|} \geq \frac{1}{624} \cdot \frac{1}{\log_2 n}.$$

So how good is the answer?

- For all finite classical groups G of rank ℓ we prove
$$\frac{|\text{PREINV}(G^F; I)|}{|G^F|} \geq \frac{1}{5000 \log_2 \ell}.$$
- Computationally we get exact answers for low Lie rank.
- Did "picking favourites" among the classes C give a less than optimal bound?
  - We believe that log is correct, only c could be improved.
  - Statistical tests[1], using package R, on random samples from $\mathrm{GL}_n(q)$ for growing n and various odd prime powers q.

Now we have a balanced invol z where to next?

- Construct the centraliser C(z)
- That's Akos's job Friday!

- But I have some more to say.
- Essential part of finding C(z) is to take random conjugates z^g to find a "nice" product y:= z.z^g
- Nice means "close to regular semisimple"
- Parker/Wilson: require O(n) random products to get a nice one -- our approach improves this to O(log n)

Akos and Cheryl: experiments in GL

For involution z and random conjugate z^g in

$$y := zz^g \sim \begin{pmatrix} I_r & 0 & 0 \\ 0 & y_0 & 0 \\ 0 & 0 & -I_s \end{pmatrix}$$

Question: What kind of matrix is y_0 'typically'?

Discovered: often y_0 is regular semisimple

That is, characteristic polynomial

$$c_{y_0}(t) = \text{product of distinct irreducibles}$$

Properties:

$$y := zz^g \sim \begin{pmatrix} I_r & 0 & 0 \\ 0 & y_0 & 0 \\ 0 & 0 & -I_s \end{pmatrix}$$

Moreover:

- $c_{y_0}(t)$ not divisible by $t \pm 1$
- $y^z = y^{-1}$ so $c_{y_0}(t) = c_{y_0^{-1}}(t) = c^*_{y_0}(t)$ is self-conjugate

  where $f^*(t) := f(0)^{-1} t^{\deg f} f(t^{-1})$ with $f(0) \neq 0$
- Parker–Wilson proofs of estimates recognised that regular semisimple y_0 prevalent

Now suppose y itself is regular semisimple

Assume

$$y \text{ regular semisimple in } \mathrm{GL}(n,q),\ q \text{ odd}$$
$$c_y(t) \text{ not divisible by } t \pm 1$$

- x an involution and $y^x = y^{-1}$ implies
  n even and $\mathrm{Fix}(x)$ dimension $\frac{n}{2}$
- So if x, x' involutions and $y = xx'$ then $y^x = y^{-1} = y^{x'}$
  so x, x' both have $\frac{n}{2}$-dimensional ± 1-eigenspaces
  so x, x' conjugate in $\mathrm{GL}(n,q)$

A helpful bijection

Let n even, q odd, and let $\mathcal{C}$ = conjugacy class of involutions in $\mathrm{GL}(n,q)$ with ± 1-eigenspaces both of dimension $\frac{n}{2}$

- Get bijection $(x', x) \mapsto (y, x)$ (where $y = x'x$) between

$$X = \left\{ (x', x) \in \mathcal{C} \times \mathcal{C} \mid \begin{array}{l} y := x'x \text{ regular semisimple} \\ \text{with } c_y(t) \text{ coprime to } t^2 - 1 \end{array} \right\}$$

$$\text{and} \quad Y = \left\{ (y, x) \mid \begin{array}{l} y, x \in \mathrm{GL}(n,q), |x| = 2, y^x = y^{-1} \\ y \text{ regular semisimple, and} \\ c_y(t) \text{ coprime to } t^2 - 1 \end{array} \right\}$$

- X relevant for algorithm; Y we could estimate

What we want for the algorithm

Given $x \in \mathcal{C}$ we want the proportion of $x' \in \mathcal{C}$ such that $(x, x') \in X$. This is

- $\frac{\#\, x' \in \mathcal{C} : (x,x') \in X}{|\mathcal{C}|} = \frac{|X|}{|\mathcal{C}|^2} = \frac{|Y|}{|\mathcal{C}|^2} = \frac{|\mathrm{GL}(n,q)|}{|\mathcal{C}|^2} \cdot \frac{|Y|}{|\mathrm{GL}(n,q)|}$
- $\frac{|\mathrm{GL}(n,q)|}{|\mathcal{C}|^2} = \frac{|\mathrm{GL}(n/2,q)|^4}{|\mathrm{GL}(n,q)|}$ bounded between $(1-q^{-1})^7$ and $(1-q^{-1})^2$
- So we care about $ss(n,q) := \frac{|Y|}{|\mathrm{GL}(n,q)|}$

What we proved

Theorem

For a fixed odd prime power q

- $ss(\infty, q) := \lim_{n\to\infty} ss(n, q)$ exists
- and is equal to $(1 - q^{-1})^2$
- Moreover $|ss(n, q) - (1 - q^{-1})^2| = o(q_0^{-n})$ for any q_0 such that $1 < q_0 < \sqrt{q}$

Consequence

Given $x \in \mathcal{C}$ the proportion of $x' \in \mathcal{C}$ such that $(x, x') \in X$ is bounded below by a positive absolute constant

How we proved it

Studied generating function for $ss(n,q) = \frac{|Y(n,q)|}{|\mathrm{GL}(n,q)|}$ where

$$Y(n,q) = \left\{ (y,x) \;\middle|\; \begin{array}{l} y, x \in \mathrm{GL}(n,q), |x| = 2, y^x = y^{-1} \\ y \text{ regular semisimple, and} \\ c_y(t) \text{ coprime to } t^2 - 1 \end{array} \right\}$$

Namely

$$S(u) = \sum_{d=0}^{\infty} ss(2d,q)u^d \quad \text{where} \quad ss(0,q) = 1$$

Working our centralisers (standard stuff)

$$S(u) = \sum_{d \geq 0} \sum_{f = f^*,\, \deg f = 2d} \frac{u^d}{\left(\prod_{i=1}^{r} (q^{\deg f_i} - 1)\right) \left(\prod_{j=1}^{s} (q^{\deg g_j} - 1)\right)}$$

where the inner summation over all self-conjugate monic polynomials $f(t)$ of degree $2d$ with a factorisation

$$f = \left(\prod_i f_i\right).\left(\prod_j (g_j g_j^*)\right)$$

with f_i, g_j monic irreducibles such that $f_i = f_i^*$, $g_j \neq g_j^*$

Staring hard at this ...

leads naturally to the following expression for $S(u)$:

$$\prod_{f=f^* \text{ irred.}} \left(1 + \frac{u^{\frac{\deg f}{2}}}{q^{\frac{\deg f}{2}} - 1}\right) \times \prod_{\{g,g^*\},\, g \neq g^* \text{ irred.}} \left(1 + \frac{u^{\deg g}}{q^{\deg g} - 1}\right)$$

Along comes serendipity!

Fulman, Neumann, Praeger (AMS Memoir 2005)

Somewhat similar generating function when studying separable matrices in finite unitary groups

We could analyse it!

Despite different function, different notion of conjugate poly f^*
A similar approach to the analysis worked!

Summary of our findings

- $S(u)$ analytic for $|u| < 1$ with simple pole at $u = 1$
- $S(u) = (1 - u)^{-1} H(u)$, with $H(u)$ analytic for $|u| < \sqrt{q}$

How this led to an improved algorithm analysis is part of the story Akos will tell !

☺ ☺