

Estimation Problems in Finite Classical Groups

Cheryl E. Praeger

University of Western Australia

Joint work with Alice C. Niemeyer and Tomasz Popiel (UWA)

Outline

- 1 What and how to estimate?
 - Estimation: algorithms and theorems
 - Involutions in finite classical groups
- 2 Geometrical methods
 - Good tori and RSS elements
- 3 Lie methods: Quokka sets
 - Preinvolution sets as Quokka sets
 - Niemeyer, Popiel, Praeger results
- 4 Summary

Estimation: algorithms and theorems

- A randomised algorithm often involves inferences made after random sampling from group – seeking an element with a certain property
- **Estimation problem:** find proportion of elements with property
- Estimate both justifies correctness, and describes algorithm performance

Estimation: algorithms and theorems

- A randomised algorithm often involves inferences made after random sampling from group – seeking an element with a certain property
- **Estimation problem:** find proportion of elements with property
- Estimate both justifies correctness, and describes algorithm performance

Monte Carlo algorithms

Typical component: find an element of certain type by random selection

To control error: Need good lower bound on proportion of such elements.

To really understand the performance characteristics: estimate should be close to real proportion

Best case: exact determination of proportion;

Next best: fairly close upper and lower bounds;

Often: just a lower bound, hoping it is good enough

General estimation questions for finite groups

- What proportions should we estimate?
- In what groups?
- Using what kinds of methods?
- (for the algorithm) how good an estimate is good enough?
- (the mathematician) how good an estimate can we get?

Involutions in finite classical groups

Focus on constructing involutions in $G = \text{Class}(n, q)$ with q odd.

Problem: Find an involution x in subset \mathcal{I} of G where

$$\mathcal{I} = \begin{cases} \text{particular conjugacy class of } G & \text{or} \\ \text{union of "desirable" conjugacy classes} \end{cases}$$

Groups G : $S \leq G \leq X$ where $S = \text{SL}, \text{Sp}, \text{SU}, \Omega^\epsilon$
or $\text{PSL}, \text{PSp}, \text{PSU}, \text{P}\Omega^\epsilon$, and $X = \text{GL}, \text{PGL}$, etc.

In lecture discuss for $G = \text{GL}(n, q)$ or $\text{SL}(n, q)$, q odd

Basic approach and estimation methods

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

- by random selection seek an element g of classical G in
 - $\text{PREINV}(G; \mathcal{I}) = \{g \in G \mid |g| \text{ even and } g^{|g|/2} \in \mathcal{I}\}$.
- Once found construct the involution $g^{|g|/2}$ in \mathcal{I}
- Approach of Parker/Wilson and Leedham-Green/O'Brien
- For $G = \text{SL}(n, q)$ or $\text{GL}(n, q)$ take \mathcal{I} to be
 - $\mathcal{I}_r :=$ class of invols with -1 eigenspace dimension r , or
 - $\hat{\mathcal{I}} :=$ union of \mathcal{I}_r over $\frac{n}{3} \leq r < \frac{2n}{3}$
- **Methods:** Geometrical + Centralisers, or Lie/Quokka theory

Basic approach and estimation methods

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

- by random selection seek an element g of classical G in
 - $\text{PREINV}(G; \mathcal{I}) = \{g \in G \mid |g| \text{ even and } g^{|g|/2} \in \mathcal{I}\}$.
- Once found construct the involution $g^{|g|/2}$ in \mathcal{I}
- Approach of Parker/Wilson and Leedham-Green/O'Brien
- For $G = \text{SL}(n, q)$ or $\text{GL}(n, q)$ take \mathcal{I} to be
 - $\mathcal{I}_r :=$ class of invols with -1 eigenspace dimension r , or
 - $\hat{\mathcal{I}} :=$ union of \mathcal{I}_r over $\frac{n}{3} \leq r < \frac{2n}{3}$
- **Methods:** Geometrical + Centralisers, or Lie/Quokka theory

Basic approach and estimation methods

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

- by random selection seek an element g of classical G in
 - $\text{PREINV}(G; \mathcal{I}) = \{g \in G \mid |g| \text{ even and } g^{|g|/2} \in \mathcal{I}\}$.
- Once found construct the involution $g^{|g|/2}$ in \mathcal{I}
- Approach of Parker/Wilson and Leedham-Green/O'Brien
- For $G = \text{SL}(n, q)$ or $\text{GL}(n, q)$ take \mathcal{I} to be
 - $\mathcal{I}_r :=$ class of invols with -1 eigenspace dimension r , or
 - $\hat{\mathcal{I}} :=$ union of \mathcal{I}_r over $\frac{n}{3} \leq r < \frac{2n}{3}$
- **Methods:** Geometrical + Centralisers, or Lie/Quokka theory

Parker–Wilson geometrical methods

Class \mathcal{I} : essentially $\mathcal{I}_r \cup \mathcal{I}_{n-r}$ (work in PSL)

Seek lower bound for: $\frac{|\text{PREINV}(G; \mathcal{I})|}{|G|}$

Chris and Rob's idea 1. Restrict to **regular semisimple** elements in $\text{PREINV}(G; \mathcal{I})$ that is, elements lying in a unique maximal torus T (Maximal abelian subgroup)

Avoids overcounting:

$$|\text{PREINV}(G; \mathcal{I})| \geq \#\text{conjugates of } T \times |\text{PREINV}(T; \mathcal{I}) \cap \text{RSS}|$$

Chris and Rob's idea 2. Choose “good tori” T

Parker–Wilson geometrical methods II

Recall $\mathcal{I}_r \cup \mathcal{I}_{n-r}$ (essentially working in PSL)

Consider ‘nice’ case: r even (so $\mathcal{I} \subset \mathrm{SL}(n, q)$) and
2-part r_2 greater than 2-part $(n-r)_2$

- **Good tori:** $T = R_1 \times R_2 < \mathrm{GL}(n, q)$ with
 $R_1 \cong \mathrm{Z}_{q^r-1}$ and $R_2 \cong \mathrm{Z}_{q^{n-r}-1}$
- **Properties:** x_1 RSS in $\mathrm{GL}(r, q)$ and x_2 RSS in $\mathrm{GL}(n-r, q)$
 $\implies x_1 x_2$ RSS in T , and ‘good proportion’ from R_i are RSS
- **And** at least half RSS $x_1 \in R_1$ have $|x_1|_2 = (q^r - 1)_2$
Note: such $|x_1|_2$ is greater than 2-part $|x_2|_2$ for any $x_2 \in R_2$
so $x_1 x_2 \in \mathrm{PREINV}(T; \mathcal{I}) \cap \mathrm{RSS}$

Parker–Wilson geometrical methods II

Recall $\mathcal{I}_r \cup \mathcal{I}_{n-r}$ (essentially working in PSL)

Consider ‘nice’ case: r even (so $\mathcal{I} \subset \mathrm{SL}(n, q)$) and
2-part r_2 greater than 2-part $(n-r)_2$

- **Good tori:** $T = R_1 \times R_2 < \mathrm{GL}(n, q)$ with
 $R_1 \cong Z_{q^r-1}$ and $R_2 \cong Z_{q^{n-r}-1}$
- **Properties:** x_1 RSS in $\mathrm{GL}(r, q)$ and x_2 RSS in $\mathrm{GL}(n-r, q)$
 $\implies x_1 x_2$ RSS in T , and ‘good proportion’ from R_i are RSS
- **And** at least half RSS $x_1 \in R_1$ have $|x_1|_2 = (q^r - 1)_2$
Note: such $|x_1|_2$ is greater than 2-part $|x_2|_2$ for any $x_2 \in R_2$
so $x_1 x_2 \in \mathrm{PREINV}(T; \mathcal{I}) \cap \mathrm{RSS}$

Parker–Wilson geometrical methods II

Recall $\mathcal{I}_r \cup \mathcal{I}_{n-r}$ (essentially working in PSL)

Consider ‘nice’ case: r even (so $\mathcal{I} \subset \mathrm{SL}(n, q)$) and
2-part r_2 greater than 2-part $(n-r)_2$

- **Good tori:** $T = R_1 \times R_2 < \mathrm{GL}(n, q)$ with
 $R_1 \cong Z_{q^r-1}$ and $R_2 \cong Z_{q^{n-r}-1}$
- **Properties:** x_1 RSS in $\mathrm{GL}(r, q)$ and x_2 RSS in $\mathrm{GL}(n-r, q)$
 $\implies x_1 x_2$ RSS in T , and ‘good proportion’ from R_i are RSS
- **And** at least half RSS $x_1 \in R_1$ have $|x_1|_2 = (q^r - 1)_2$
Note: such $|x_1|_2$ is greater than 2-part $|x_2|_2$ for any $x_2 \in R_2$
so $x_1 x_2 \in \mathrm{PREINV}(T; \mathcal{I}) \cap \mathrm{RSS}$

Parker–Wilson geometrical methods III

Conjugates of $T = \frac{|G|}{|N_G(T)|} = \frac{|G|}{r(n-r)|T|}$

RSS in T at least $c|T|$ with c absolute constant,

Gives $|\text{PREINV}(G; \mathcal{I})| \geq \frac{|G|}{r(n-r)|T|} \times c|T|$ so

$$\frac{|\text{PREINV}(G; \mathcal{I})|}{|G|} \geq \frac{c}{r(n-r)} \geq \frac{4c}{n^2}$$

Other cases: sometimes $c = c(q)$, worst case $c = c_0/n$, and

$$\frac{|\text{PREINV}(G; \mathcal{I})|}{|G|} \geq \frac{c'}{n^3} \text{ for some constant } c'$$

Leedham-Green geometrical methods

Involution set $\hat{\mathcal{I}} = \cup_{r=n/3}^{2n/3} \mathcal{I}_r$ adding over even r geom. methods give

$$\frac{|\text{PREINV}(G; \hat{\mathcal{I}})|}{|G|} \geq \sum_r \frac{c_0}{r(n-r)} > \frac{c_0}{2n}$$

So how does Quokka theory help?

Suggested Benefit 1. avoids need to address RSS elements explicitly (simplifies arguments; gives smaller constants)

Suggested Benefit 2. enables consideration of larger range of tori related to $\text{PREINV}(G; \mathcal{I})$ (improves asymptotic estimates)

Lübeck, Niemeyer, Praeger Results

Using the Quokka theory methods

(before they were completely written down as a theory)

Lübeck, Niemeyer, Praeger: improve, for $\hat{\mathcal{I}} = \cup_{r=n/3}^{2n/3} \mathcal{I}_r$ to

$$\frac{|\text{PREINV}(G; \hat{\mathcal{I}})|}{|G|} \geq \frac{c}{\log n}$$

for an explicit constant c . I will compare the approaches for the Parker–Wilson problem

PREINV($G; \mathcal{I}$) is a Quokka subset of G

Set $Q := \text{PREINV}(G; \mathcal{I})$

Recall Quokka Subset: A non-empty subset $Q \subseteq G$ such that

(i) For $g \in G$ with Jordan decomposition $g = su = us$,

$g \in Q$ if and only if $s \in Q$

Since $|u|$ is odd this holds for $Q = \text{PREINV}(G; \mathcal{I})$

(ii) and Q is a union of G -conjugacy classes.

Clearly this holds, so $Q = \text{PREINV}(G; \mathcal{I})$ is Quokka set.

Niemeyer, Popiel, Praeger results

Involution set $\mathcal{I} = \mathcal{I}_r$ single conjugacy class (because G linear)

and take $G = \text{GL}(n, q)$ for discussion and comparison

Quokka Theory gives $\frac{|\text{PREINV}(G; \mathcal{I})|}{|G|} = \sum_C \frac{|C|}{|W|} \cdot m_C$ Where

sum is over all conjugacy classes C of Weyl group $W \cong S_n$.

Also $m_C = \frac{|T_C \cap Q|}{|T_C|}$ where T_C is representative maximal torus corresponding to C

Niemeyer, Popiel, Praeger results II

We also make careful choices of C, T_C (but use many more of them) so $\frac{|\text{PREINV}(G; \mathcal{I})|}{|G|} \geq \sum_{\text{such } C} \frac{|C|}{|W|} \cdot m_C$

Nicest case: take r even, $s = (s_1, \dots, s_k)$ with all s_i odd and $r + \sum_i s_i = n$

Corresponding tori: $T_C = R_1 \times R_2$ with $R_1 \cong Z_{q^{r-1}}$ and $R_2 = \prod_{i=1}^k Z_{q^{s_i-1}}$

And Weyl group class C : all permutations in S_n with cycle lengths r, s_1, \dots, s_k

Niemeyer, Popiel, Praeger results III

Torus proportion in $T_C = R_1 \times R_2$ $m_C = \frac{|T_C \cap Q|}{|T_C|} \geq \frac{1}{2}$

(take $x_1 x_2 \in T_C$ with $|x_1|_2$ maximal)

Weyl group proportion: $\sum_{\text{such } c} \frac{|C|}{|W|} =$ proportion of these
 permutations $\geq (2r\sqrt{\pi(n-r)})^{-1} \geq \frac{1}{4\sqrt{\pi}(n/3)^{3/2}}$

Yields lower bound

$$\frac{|\text{PREINV}(G; \mathcal{I})|}{|G|} \geq \frac{1}{8\sqrt{\pi}(n/3)^{3/2}}$$

For r even same result: case U for \mathcal{I}_r , Sp for \mathcal{I}_{2r} , and O for \mathcal{I}_{2r}^+
 Compare with $O(n^{-2})$ for this case of Parker–Wilson.

Niemeyer, Popiel, Praeger results IV

General comments for r odd: Use tori $T_C = R_1 \times R_2$ with

$$R_1 = \begin{cases} Z_{q^r-1} & \text{case SL} \\ Z_{q^r+1} & \text{case U} \\ Z_{q^r-1} \text{ or } Z_{q^r+1} & \text{case Sp or O for } \mathcal{I}_{2r} \end{cases}$$

$R_2 = \prod_{i=1}^k Z_{q^{s_i} \pm 1}$ where 2-part of each $q^{s_i} \pm 1$ **at most** $|R_1|_2$

Example case SL: Corresponding Weyl conjugacy class C

permutations with cycles of lengths r, s_1, \dots, s_k

Proportion $m_C = \frac{|\text{PREINV}(T_C; \mathcal{I})|}{|T_C|}$ at least $\frac{1}{2^{k+1}}$ so **take k small**

Niemeyer, Popiel, Praeger results V

Continue example with n even, r odd: $k = 3$, s_1, s_2, s_3 odd, $s_1 = 1$, s_2, s_3 arbitrary; then $m_C \geq \frac{1}{16}$ (Parker–Wilson: $k = 1$)

Weyl group estimate: $\sum_{\text{such } c} \frac{|C|}{|W|}$ proportion in S_n with 4 odd cycles, including lengths 1 and r . We prove: at least $\frac{\log_2(n-r)}{12r(n-r)}$

Apply quokka theory: $\frac{|\text{PREINV}(G; \mathcal{I}_r)|}{|G|} \geq \frac{\log_2(n-r)}{192r(n-r)}$

Overall result, all cases: $c(q)$ absolute constant for SL, U, Sp

$$\frac{|\text{PREINV}(G; \mathcal{I}_r)|}{|G|} \geq \frac{c(q) \log_2(n)}{n^2}$$

Summary

- Better estimates give greater understanding of algorithms
- Quokka theory separates into Torus and Weyl problems
- Torus problem sometimes simpler than geometric methods (e.g. RSS unnecessary; overcounting problems disappear)
- Can also deal with all $su = us$ in quokka set, not only s
- Weyl group estimation problems easier to state/solve
- Enables larger range of tori in estimates
- Gain in asymptotics: bounds for PREINV rise from $O(n^{-3})$ to $O(n^{-2} \log n)$

Summary

- Better estimates give greater understanding of algorithms
- Quokka theory separates into Torus and Weyl problems
- Torus problem sometimes simpler than geometric methods (e.g. RSS unnecessary; overcounting problems disappear)
- Can also deal with all $su = us$ in quokka set, not only s
- Weyl group estimation problems easier to state/solve
- Enables larger range of tori in estimates
- Gain in asymptotics: bounds for PREINV rise from $O(n^{-3})$ to $O(n^{-2} \log n)$

Summary

- Better estimates give greater understanding of algorithms
- Quokka theory separates into Torus and Weyl problems
- Torus problem sometimes simpler than geometric methods (e.g. RSS unnecessary; overcounting problems disappear)
- Can also deal with all $su = us$ in quokka set, not only s
- Weyl group estimation problems easier to state/solve
- Enables larger range of tori in estimates
- Gain in asymptotics: bounds for PREINV rise from $O(n^{-3})$ to $O(n^{-2} \log n)$

Summary

- Better estimates give greater understanding of algorithms
- Quokka theory separates into Torus and Weyl problems
- Torus problem sometimes simpler than geometric methods (e.g. RSS unnecessary; overcounting problems disappear)
- Can also deal with all $su = us$ in quokka set, not only s
- Weyl group estimation problems easier to state/solve
- Enables larger range of tori in estimates
- Gain in asymptotics: bounds for PREINV rise from $O(n^{-3})$ to $O(n^{-2} \log n)$