THE UNIVERSITY OF WESTERN AUSTRALIA

*Achieving International Excellence*

# Estimation Problems and Randomised Group Algorithms: Lecture 3

Cheryl E Praeger

Galway, April, 2011

# Estimation techniques in Lie type groups

- One of my favourite results
- An estimation problem in Lie type groups – new idea
- quokka sets and applications
- p-abundant elements

- Alice will give some of this lecture

# One of my favourite results

**Theorem: Isaacs, Kantor, Spaltenstein, 1995**

$G$ any permutation group on $n$ points, prime $p$ dividing $|G|$, implies at least 1 chance in $n$ that a random permutation in $G$ has order a multiple of $p$. [Best possible in some cases.]

# Sounds elementary?

- Only known proof relies on simple group classification
- Proof strategy: elementary reduction to G simple
- Not too difficult for An and sporadics
- Magic introduced for Lie type groups!
- Alice and I set about trying to understand it

# After false lead [nonexistent reference!] ...

- Pointers from Klaus Lux
- Help from Frank Lubeck
- Discovered some beautiful theory which had been used
  - in representation theory by Gus Lehrer – first in print
  - For Lie algebra computations by Arjeh Cohen and Scott Murray
- We wanted to develop this as a method for solving estimation problems

# p-Jordan decomposition of group elements

- p prime, g in finite group G

Let $|g| = p^a b$ where $p \not| b$ and $a \geq 0$

Find integers $r, t$ such that $rp^a + tb = 1$

Set $u = g^{tb}$ and $s = g^{rp^a}$ so $g = us = su$

This is called the $p$-Jordan decomposition of $g$

Exercise: $u, s$ independent of choices of $r, t$

# Two conditions on a subset Q 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

Call Q with these two properties

a p-Quokka subset.

This is a quokka ☺ ->>

# Example of a p-Quokka subset

- G = GL(n,q)  e >n/2
- Q:= set of all ppd(n,q;e) elements of G
  - Q conjugation closed (conjugates have same order)
  - For g=us=su, and ppd r of q^e-1

    r divides |g|  if and only if  r divides |s|

    so g in Q  if and only if  s in Q

# Real Power from Lie Theory

- Over to Alice

then me again

# Ppd quokka subset Q in G = GL(n,q)

- Q:= set of all ppd(n,q;e) elements of G, with e >n/2
- Weyl group W = S_n
- Quokka torus T_C = Z_{q^e-1} x others
- Proportion of T_C in Q between 1-1/(e+1) and 1
- Quokka class C – elements of W containing an e-cycle
- Proportion of W in quokka classes 1/e
- Quokka thm: Prop in Q between 1/(e+1) and 1/e

# p-abundant elements

- G=GL(n,q)  prime p dividing q^b-1 dividing |G|
- Wanted to understand  IKS (hidden) O(1/b) lower bound for proportion of p-singular elements (ie p divides |g|)
- Alice's computer experiments suggested
- Special kind of p-singular elements occur at least as frequently as the IKS lower bound

We called them p-abundant

# p-abundant elements g of G=GL(n,q)

Setup:

- p primitive prime divisor of q^b-1 p odd
- p divides |g|
- g-invariant irreducible subspace U of V(n,q) with dim(U) >n/2
- Note: dim(U)=bm for some m
- Slightly different definition for elements of Sp, U, O

# Comments on p-abundant elements

p ppd of q^b-1 and p divides |g|

- irreducible action on g-module U has order coprime to q [algorithmically easy to detect]
- so if g=us=su is the Jordan decomposition then s is also p-abundant!
- So set of p-abundant elements is a quokka set!
- If b>n/2 then same argument as for the ppd quokka subset gives that the p-abundant proportion is between 1/(b+1) and 1/b ☺

# Quokka set of p-abundant elements

Quokka torus: $T_C = Z_{q^{bm}-1} \times$ other factors

$\frac{|T_C \cap Q|}{|T_C|} \sim 1 - \frac{1}{P_m}$ where $P_m$ is $p$-part of $q^{bm} - 1$

$P_m$ depends on $p$-part $m'$ of $m$.

Let $P = p-$part of $q^b - 1$, then $P_m = P \times m'$
Corresponding Quokka classes: elements have a cycle length divisible by $bm'$

# Quokka set of p-abundant elements

We considered separately the exponents $bm$

with a given $p$-part $m'$ of $m$
And obtained precise leading term:

**Theorem ($p$-abundant)**

Prop($p-$ abundant elements in $G$
$= (1 - \frac{1}{P})\frac{\ln 2}{b} + \Theta(\frac{1}{n})$