RPS Energy

Centro-invertible Matrices

Roy S Wikramaratna, RPS Energy

WikramaratnaR@rpsgroup.com

Reading University (Conference in honour of Nancy Nichols' 70th birthday)

2-3 July 2012

RPS Energy References

- R.S. Wikramaratna, The centro-invertible matrix:a new type of matrix arising in pseudo-random number generation, *Linear Algebra and its Applications*, **434** (2011) pp144-151. [doi:10.1016/j.laa.2010.08.011].
- R.S. Wikramaratna, Theoretical and empirical convergence results for additive congruential random number generators, *J. Comput. Appl. Math.*, **233** (2010) 2302-2311. [doi: 10.1016/j.cam.2009.10.015].

RPS Energy Career Background

- Worked at Institute of Hydrology, 1977-1984
  - Groundwater modelling research and consultancy
  - P/t MSc at Reading 1980-82 (Numerical Solution of PDEs)
- Worked at Winfrith, Dorset since 1984
  - UKAEA (1984 – 1995), AEA Technology (1995 – 2002), ECL Technology (2002 – 2005) and RPS Energy (2005 onwards)
  - Oil reservoir engineering, porous medium flow simulation and simulator development
  - Consultancy to Oil Industry and to Government
- Personal research interests in development and application of numerical methods to solve engineering problems, and in mathematical and numerical analysis of those methods

RPS Energy Some definitions …

- **I** is the *k* by *k* identity matrix
- **J** is the *k* by *k* matrix with ones on anti-diagonal and zeroes elsewhere
  - Pre-multiplication by **J** turns a matrix 'upside down', reversing order of terms in each column
  - Post-multiplication by **J** reverses order of terms in each row

$$\mathbf{J} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \left(j_{pq}\right)$$

$$j_{pq} = 1 \text{ if } p+q = k+1$$

$$j_{pq} = 0 \text{ otherwise}$$

RPS Energy Outline of today's talk

- Definitions
  - Matrix centro-rotation operation
  - Centro-invertible matrix
- Theory
  - Properties
  - Examples
  - Relationship with involutory matrices
  - How common are centro-invertible matrices?

RPS Energy … more definitions …

- The matrix centro-rotation operation on a matrix **X** (to be denoted $\mathbf{X}^{\mathbf{R}}$) is defined as
  - A component-wise 180 degree rotation about centre of matrix
  - Equivalent to reversing order of both rows and columns

$$\mathbf{X}^{\mathbf{R}} = \mathbf{JXJ}$$

$$\mathbf{X}^{\mathbf{R}} = \begin{pmatrix} x_{44} & x_{43} & x_{42} & x_{41} \\ x_{34} & x_{33} & x_{32} & x_{31} \\ x_{24} & x_{23} & x_{22} & x_{21} \\ x_{14} & x_{13} & x_{12} & x_{11} \end{pmatrix} = \left(j_{(k+1-p)(k+1-q)}\right)$$

RPS Energy … yet more definitions

- A matrix **X** is defined to be centro-invertible if and only if $\mathbf{X}^{-1}=\mathbf{X}^{\mathbf{R}}$
- A matrix **X** with integer components is defined to be centro-invertible modulo *M* if and only if the equation $\mathbf{X}^{-1}=\mathbf{X}^{\mathbf{R}}$ holds true when working in modular arithmetic, modulo (a large integer) *M*

RPS Energy Simple examples

- The matrices **I**, **J** defined previously are centro-invertible, as are **–I** and **–J**
  - All of these matrices are also involutory matrices
  - All of these matrices are also centro-symmetric
  - Can show that any two of {centro-invertible, involutory, centro-symmetric} also imply the third

RPS Energy Observations …

- Centro-invertible matrices (modulo 2^k) arise naturally in a real application
  - Additive Congruential Random Number (ACORN) Generator
  - see reference in *JCAM*, 2010
- Choice of name is by analogy with centro-symmetric matrices (which are invariant under the centro-rotation operation)
  - It appears that centro-invertible matrices have not arisen or been described previously in the literature prior to the 2010 *JCAM* reference
  - The term centro-invertible was first used in the 2011 *LAA* reference

RPS Energy Non-trivial examples (modulo 16)

2 by 2 example, ACORN matrix, modulo 16

$$\begin{pmatrix} 15 & 2 \\ 14 & 3 \end{pmatrix}$$

3 by 3 example, ACORN matrix, modulo 16

$$\begin{pmatrix} 1 & 13 & 3 \\ 3 & 8 & 6 \\ 6 & 1 & 10 \end{pmatrix}$$

5 by 5 examples (*i*), ACORN matrix, modulo 16

$$\begin{pmatrix} 1 & 11 & 10 & 6 & 5 \\ 5 & 8 & 13 & 8 & 15 \\ 15 & 10 & 14 & 7 & 3 \\ 3 & 0 & 8 & 0 & 6 \\ 6 & 5 & 12 & 12 & 14 \end{pmatrix}$$

(*ii*), (-**I**) times ACORN matrix, modulo 16

$$\begin{pmatrix} 15 & 5 & 6 & 10 & 11 \\ 11 & 8 & 3 & 8 & 1 \\ 1 & 6 & 2 & 9 & 13 \\ 13 & 0 & 8 & 0 & 10 \\ 6 & 5 & 12 & 12 & 14 \end{pmatrix}$$

(*iii*), Block anti-diagonal with centro-invertible blocks

$$\begin{pmatrix} 0 & 0 & 0 & 15 & 2 \\ 0 & 0 & 0 & 14 & 3 \\ 1 & 13 & 3 & 0 & 0 \\ 3 & 8 & 6 & 0 & 0 \\ 6 & 1 & 10 & 0 & 0 \end{pmatrix}$$

(*iv*), Block anti-diagonal with centro-invertible blocks

$$\begin{pmatrix} 0 & 0 & 1 & 13 & 3 \\ 0 & 0 & 3 & 8 & 6 \\ 0 & 0 & 6 & 1 & 10 \\ 15 & 2 & 0 & 0 & 0 \\ 14 & 3 & 0 & 0 & 0 \end{pmatrix}$$

RPS Energy … more observations

- There is a key relationship that exists between centro-invertible matrices and involutory matrices (an involutory matrix **Y** is one for which $\mathbf{Y}^2=\mathbf{I}$)
  - Can define a one-one onto mapping between centro-invertible matrices and involutory matrices (in fact, there are several such mappings that are possible; in particular any centro invertible matrix is an upside down involutory matrix and vice-verca)
- Allows existing results concerning the number of *k* by *k* involutory matrices modulo *M* to be translated to give analogous results for centro-invertible matrices modulo *M*

RPS Energy Some properties of centro-invertible matrices

- The inverse of a centro-invertible matrix is itself centro-invertible
- If **X** is centro-invertible modulo *M*, then so is **X** raised to any integer power
- The determinant of a centro-invertible matrix is equal to +1 or -1 (for a centro-invertible matrix modulo *M* the determinant is 1 or *M*-1)
  - Note all ACORN matrices have determinant 1, so there are centro-invertible matrices that are not ACORN matrices
- Any block anti-diagonal matrix having centro-invertible sub-blocks on the anti-diagonal and zeroes elsewhere is itself centro-invertible
  - Note typographic error in *LAA*, 2011 – text says 'involutory' instead of 'centro-invertible' in this statement

Results …

- THEOREM
  - There exists a 1 to 1 correspondence between *k* by *k* centro-invertible matrices and *k* by *k* involutory matrices
- PROOF
  - Can show that **X** is centro-invertible if and only if **JX** is involutory
  - Note, also, **X** is centro-invertible if and only if **XJ** is involutory
- Corollary 1
  - Number of *k* by *k* centro-invertible matrices (modulo *M*) for any *k* is identical to the number of *k* by *k* involutory matrices (modulo *M*)

RPS Energy

Corollary 3 (modulus a power of 2)

- The number $T(k,2^n)$ of *k* by k centro-invertible matrices modulo 2^n is given by one of the following equations depending on the value of *n*, where as before g_0=1 and g_t is as in Corollary 2

$$T(k,2^1) = g_k \sum_{t=0}^{\lfloor k/2 \rfloor} \left(\frac{2^{-t(2k-3t)}}{g_t g_{k-2t}} \right)$$

$$T(k,2^2) = g_k \sum_{t=0}^{\lfloor k/2 \rfloor} \left(\frac{2^{k^2-4tk+5t^2}}{g_t g_{k-2t}} \right)$$

$$T(k,2^n) = 2^{k^2} g_k \sum_{t=0}^{k} 2^{2t(k-t)(n-3)} \sum_{r=0}^{\min(t,k-t)} \left(\frac{2^{r(3r-2k)}}{g_r g_{t-r} g_{k-t-r}} \right) \qquad n \geq 3$$

- PROOF
  - By analogy with Hodges (1958) and Levine and Korfhage (1964); making use of Corollary 1.
    [Note minor typo in L&K for the case *n*=2, corrected above].

RPS Energy

References for Corollaries 2, 3 and 4 (involutory matrices)

- J.H. Hodges, The matrix equation X^2-*I*=0 over a finite field, *Amer. Math. Monthly*, **65** (1958), pp. 518-520
- I. Reiner, The matrix congruence $X^2 \equiv I \pmod{p^a}$, *Amer. Math. Monthly*, **67** (1960), pp.773-775.
- J. Levine and R.R. Korfhage, Automorphisms of abelian groups induced by involutory matrices, general modulus, *Duke Math. J.*, **31** (1964), pp.631-653.

RPS Energy

Corollary 4 (general result, any modulus)

- Let $p_1, p_2, \ldots, p_r$ be distinct primes and let the prime power factorisation of *M* be

$$M = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$$

- Then the number of *k* by *k* centro-invertible matrices over the integers, modulo *M* is

$$T(k,M) = \prod_{j=1}^{r} T\left(k, p_j^{n_j}\right)$$

where $T(k,p_j^{n_j})$ is as defined in corollary 2 for odd values of p_j and corollary 3 if p_j is equal to 2

- PROOF
  - By analogy with Levine and Korfhage (1964); making use of Corollary 1.

RPS Energy

Corollary 2 (prime-power modulus, odd primes)

- For a *k* by *k* integer matrix **X**, the number of centro-invertible matrices modulo p^{a+1} for an odd prime *p* and a≥0 is given by

$$T(k, p^{a+1}) = \sum_{t=0}^{k} \left(\frac{g_k}{g_t g_{k-t}} \cdot p^{2t(k-t)a} \right)$$

where g_0=1 and g_t is given by

$$g_t = p^{t^2} \prod_{i=1}^{t} \left(1 - p^{-i}\right) = \prod_{i=0}^{t-1} \left(p^t - p^i\right) \qquad 0 < t \leq k$$

- PROOF
  - By analogy with Reiner (1960); making use of Corollary 1.

RPS Energy

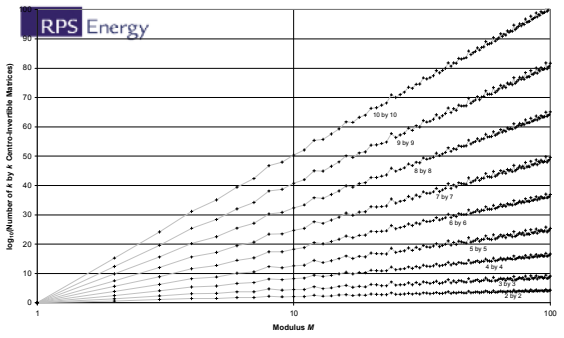

Figure 1: Number of *k* by *k* centro-invertible matrices (mod *M*), plotted against the modulus *M* on logarithmic scales, base 10

RPS Energy

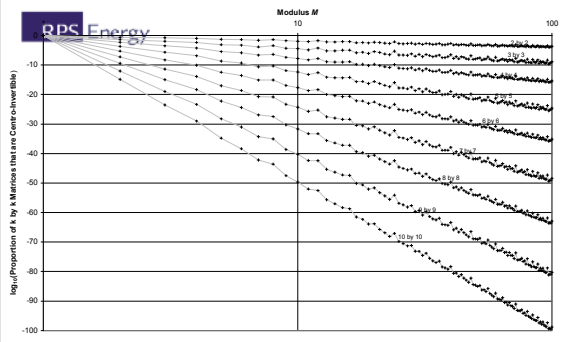

Figure 2: Proportion of k by k matrices (mod M) that are centro-invertible, plotted against modulus M on logarithmic scales, base 10

RPS Energy

Observations

- Results suggest an approximate relationship between the number of centro-invertible k by k matrices (or equivalently the number of k by k involutory matrices) that exist modulo M and the total number ($N=M^{(kxk)}$) of possible k by k matrices modulo M as follows
  - Number of centro-invertible matrices ~ $N^{0.5}=M^{(kxk)/2}$
  - Proportion that are centro-invertible ~ $N^{-0.5}=M^{-(kxk)/2}$
- *NOTE* Purely empirical relationship at present
- *QUESTION* Is it possible to infer these (or similar) expressions from Corollaries 2 – 4 based on theoretical analysis?

RPS Energy

… thank you for listening

RPS Energy