Loop matrices, loop determinants and S-rings on loops

Ken Johnson
Penn State Abington College

Outline

- 1) Group matrices and group determinant, Loop matrices and loop determinants (latin square determinants)
- 2) Some properties of group matrices .
- 3) The group matrix modulo p
- 4) The loop matrix mod p
- 5) the k-S-ring of a group and a corresponding "ring" for a loop
- 6) The connection with harmonic analysis
- 7) Fusion for loop classes
- 8) Fission for loop classes
- 9) Further ideas

Group matrices

Let G be a finite group of order n with a listing of elements $\{g_1 = e, g_2, ..., g_n\}$ and let $\{x_{g_1}, x_{g_2}, ..., x_{g_n}\}$ be a set of independent commuting variables indexed by the elements of G.

Definition

The (full) *group matrix* X_G is the matrix whose rows and columns are indexed by the elements of G and whose $(g, h)^{\text{th}}$ entry is $x_{gh^{-1}}$.

The group matrix is a patterned matrix: it is determined by its first row (or column)

Example

The group matrix of C_3 is (abbreviating x_{g_i} by i) the circulant

$$C(1, 2, 3) = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

Further example

Example

The group matrix of S_3 is the matrix

$$\begin{bmatrix} 1 & 3 & 2 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \\ 3 & 2 & 1 & 5 & 6 & 4 \\ 4 & 6 & 5 & 1 & 2 & 3 \\ 5 & 4 & 6 & 3 & 1 & 2 \\ 6 & 5 & 4 & 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} C(1,2,3) & C(4,6,5) \\ C(4,5,6) & C(1,3,2) \end{bmatrix}$$

The loop matrix

The loop matrix: Q is a loop of order n
variables $\{x_{q_i}\}_{q_i \in Q}$ are taken.
X_Q is the matrix with $(i,j)^{th}$ element x_{q_i/q_j}.
Most of the time think of this as $x_{q_i q_j^{-1}}$
This is the latin square matrix of the parastrophe.
The loop determinant...

group matrices obtained from the cosets of an arbitrary subgroup

If $|G| = kr$ and H is any cyclic subgroup of order k then the elements of G can be listed such that X_G is a block matrix of the form

$$\begin{bmatrix} B_{11} & B_{12} & \ldots & B_{1r} \\ B_{21} & B_{22} & \ldots & B_{2r} \\ \ldots & .. & \ldots & .. \\ B_{r1} & B_{r2} & \ldots & B_{rr} \end{bmatrix},$$

where each B_{ij} is a circulant of size $k \times k$. A corresponding result holds for any subgroup H. (Dickson 1907) If in the above H is arbitrary, X_G is as above, but the blocks are now all of the form $X_H(g_{i_1}, g_{i_2} \ldots g_{i_k})$. Here elements in the vector $(g_{i_1}, g_{i_2} \ldots g_{i_k})$ are elements in G, and not necessarily arising from any specific coset of H.

Dickson's results on the mod p case

The group determinant mod p of a p-group.

Lemma

Let H be any p-group of order $r = p^s$. Let P be the upper triangular matrix of the form

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ & 1 & 2 & 3 & & r-1 \\ & & 1 & 3 & & (r-1)(r-2)/2 \\ & & & 1 & & \dots \\ & & & & \dots & r-1 \\ & & & & & 1 \end{bmatrix}.$$

Then a suitable ordering of H exists such that, modulo p, PX_HP^{-1} is a lower triangular matrix with identical diagonal entries of the form $\alpha = \sum_{i=1}^{r} x_{h_i}$.

The group determinant Θ_H modulo p is thus α^r.

Example

$G = C_5$. Then $P =$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ & 1 & 2 & 3 & 4 \\ & & 1 & 3 & 6 \\ & & & 1 & 4 \\ & & & & 1 \end{bmatrix}$$

and modulo 5

$$PX_G P^{-1} = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 \\ \beta & \alpha & 0 & 0 & 0 \\ \gamma & \beta & \alpha & 0 & 0 \\ \delta & \gamma & \beta & \alpha & 0 \\ \mu & \delta & \gamma & \beta & \alpha \end{bmatrix}$$

where $\alpha = \sum_{i=1}^{5} x_{g_i}$, $\beta = 4x_2 + 3x_3 + 2x_4 + x_5$, $\gamma = x_2 + 3x_3 + x_4$, $\delta = 4x_2 + x_3$ and $\mu = x_2$.

Question: does this have any relevance to the FFT?

Lemma

Let G be a group of order n divisible by p and H be a Sylow-p subgroup of index k and order r. Then, an ordering of G exists such that, modulo p, X_G is similar to a matrix which has a block diagonal part of the form

$$diag(B, B, ..., B) \text{ (r occurences of B)}$$

with the upper triangular part above the diagonal 0. Moreover B encodes the permutation representation of G on the cosets of H.

This is proved by acting on the X_G obtained by ordering G by the left cosets of H and acting by $diag(P, P, ..., P)$ and rearranging. Thus it follows that, modulo p, $\Theta_G = \det(B)^r$.
Question: is there an explanation of all this using the standard techniques of modular representation theory?

(a) M_{12} (smallest non-associative Moufang loop)
With a suitable ordering of the loop, the loop matrix is of the form (abbreviating x_i by i)

$$\begin{bmatrix} C(1,3,2) & C(4,5,6) & C(7,8,9) & C(10,11,12) \\ C(4,6,5) & C(1,2,3) & R(10,11,12) & R(7,8,9) \\ C(7,9,8) & R(10,11,12) & C(1,2,3) & R(4,5,6) \\ C(10,12,11) & R(4,5,6) & R(7,8,9) & C(1,2,3) \end{bmatrix}.$$

Now, if P_3 is the 3×3 Pascal matrix,

$$PC(a,b,c)P^{-1} \equiv \begin{bmatrix} \alpha & 0 & 0 \\ \beta & \alpha & 0 \\ \gamma & \beta & \alpha \end{bmatrix}, \quad PR(a,b,c)P^{-1} = \begin{bmatrix} \alpha & 0 & 0 \\ \beta & -\alpha & 0 \\ \gamma & \delta & \alpha \end{bmatrix}$$

$\mathbb{O}_{16}$ (the Octonion loop) The loop matrix can be put in the form

$$\begin{bmatrix} C_{(1,2,3,4)} & C_{(7,6,5,8)} & C_{(11,10,9,12)} & C_{(15,14,13,16)} \\ C_{(5,6,7,8)} & C_{(1,4,3,2)} & R_{(13,16,15,14)} & R_{(11,10,9,12)} \\ C_{(9,10,11,12)} & R_{(15,14,13,16)} & C_{(1,4,3,2)} & R_{(5,8,7,6)} \\ C_{(13,14,15,16)} & R_{(9,12,11,10)} & R_{(7,6,5,8)} & C_{(1,4,3,2)} \end{bmatrix}.$$

Now, if $P = P_4$ is the 4×4 Pascal matrix,

$$PC(a,b,c,d)P^{-1} \equiv \begin{bmatrix} \alpha & 0 & 0 & 0 \\ \beta & \alpha & 0 & 0 \\ \gamma & \beta & \alpha & 0 \\ \delta & \gamma & \beta & \alpha \end{bmatrix} \text{ (modulo 2)},$$

$$PR(a,b,c,d)P^{-1} = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ * & \alpha & 0 & 0 \\ * & * & \alpha & 0 \\ * & * & * & \alpha \end{bmatrix} \text{(modulo 2)}$$

Then, after conjugating by $\mathrm{diag}(P, P, P, P)$, rearranging and conjugating again, the loop matrix of $\mathbb{O}_{16}$ is transformed, mod 2, to a lower triangular matrix with diagonal entry $\sum_{i=1}^{16} x_i$. Thus the determinant of $\mathbb{O}_{16}$ mod 2 is exactly the same as that of any group of order 16.

Questions: (1) When do loops of order a power of p loops Q which are of the form

$$D \to Q \to C_p.$$

behave similarly?

(2) Is there a characterisation of loops whose loop matrix can be written as a block matrix of circulants and reverse circulants with respect to a cyclic subgroup? (they probably need to be power associative). (3) Commutative automorphic loops mod 2?

The k-class algebra

Let Q be a loop with inner mapping group IQ. The **k-class algebra** of Q is defined as follows. Consider the orbits $\{\Delta_i\}$ of $IQ \times S_k$ acting on $Q^{(k)}$ by

$$\sigma(q_1, ..., q_k) = (\sigma q_1, ..., \sigma q_k), \ \sigma \in IQ$$

and

$$\tau(q_1, ..., q_k) = (q_{\tau(1)}, ..., q_{\tau(k)}).$$

Let $\overline{\Delta_i}$ be the element of $\mathbb{C}(Q^{(k)})$ which is the sum of the elements of Δ_i.These sums generate the k-class algebra of Q. Call this A_k. If Q is a group, then the k-class algebra is an S-ring over $Q^{(k)}$. It contains interesting information.
If Q is a loop, the 1-class algebra is commutative and associative (and is an S-ring over Q).

Questions: (1) for an arbitrary loop, when is A_k an S-ring over $Q^{(k)}$?
If Q is an A-loop- yes.

(2) For which loops is A_k commutative?
(3) For which loops is A_k associative?

Harmonic analysis

Suppose that a random walk on a loop Q proceeds as follows. There is given a probability p on Q, i.e. p is a function $Q \to \mathbb{R}^{\succeq 0}$ such that $\sum_{q \in Q} p(q) = 1$. If the walk is at element q_1 at the r^{th} stage, it moves to the element $q_1 s$ with probability $p(s)$. This is a Markov chain with transition matrix $X_Q(p)$ with (i, j) entry $p(q_i^{-1} q_j)$ (from the loop matrix under left division). If Q is a group this case has been the subject of a lot of analysis, and especially important is that $(X_Q(p))^2 = X_Q(p * p)$, where $p * p$ denotes convolution. If Q is nonassociative then it is not so easy to describe $(X_Q(p))^2$ but the analysis of the walk involves the calculation of $(X_Q(p))^r$ for arbitrary r.

It is easiest if $X_Q(p)$ is similar to a diagonal matrix, and this is always the case if p is constant on conjugacy classes. It might be an interesting project to analyse a random walk on Chein loops constructed from, say, families of simple groups.

Fusion

Fusion of the character table of a loop to that of another loop was discussed in papers (CFQI...)of JDH Smith and KWJ beginning in the 1980's as part of the project to construct a character theory of quasigroups. Often a character table of a loop is most easily obtained by fusing that of a group. More recently work of Humphries and KWJ discussed the class of groups whose character table fuses from a cyclic group, the methods used being mainly those of S-rings. The results with Smith in a special case were rediscovered in a paper by Diaconis and Isaacs (Supercharacters) and then applied to the problem of random walks on $U_n(q)$. The calculation of the conjugacy classes of $U_n(q)$ is wild, but if the classes are fused in a certain way the new classes, the superclasses, can be described. More recently it was shown that the superclasses form a Hopf algebra which is isomorphic to the Hopf algebra of non-commutative symmetric functions.

The talk of Michael Munywoki indicated how a loop can be constructed on $U_n(q)$ in such a way that the classes of the loop are almost equal to the superclasses.
Questions:
(1) Is it possible to change the multiplication of the loop such that the classes are exactly the same as the superclasses?
(2) Is there a natural Hopf algebra on the conjugacy classes of the loops constructed on $U_n(q)$?
(3) Which loops have character tables which fuse fom those of groups?
(4) Which loops have character tables which fuse fom those of abelian groups?

Fission

Consider the loop Q of order 6 whose group matrix is

$$\begin{bmatrix} C(1,3,2) & C(4,5,6) \\ C(4,6,5) & C(1,3,2) \end{bmatrix}.$$

It has classes $\{1\}, \{2,3\}, \{4,5,6\}$, and a random walk with probability p on the loop has diagonalisable $X_Q(p)$ if p is constant on these classes. However, either of the following "fissions" of classes are used, then $X_Q(p)$ remains diagonalisable.

(a) $\{1\}, \{2\}, \{3\}, \{4,5,6\}$, (b) $\{1\}, \{2,3\}, \{4\}, \{5,6\}$.

Question: what is the maximum number of classes in a fission of Q for which $X_Q(p)$ is diagonalisable whenever p is constant on these classes?

Answer for groups (Humphries). The maximum number is $\tau(G) = \sum_{\chi \in Irr(Q)} \deg(\chi)$.

(This may not be attained, but is attained for all groups of orders < 54).

Answer for loops-no idea.

Strange fact: the Jucy's Murphy elements in the group ring of the symmetric group produce a commutative subring of the group ring of dimension $\tau(G)$, but this is not an S-ring

Latin squares

Suppose we take a collection $\{L_i\}_{i=1}^{r}$ of orthogonal latin squares on $\{1,..,n\}$. Consider the array A whose $\{i,j,k\}^{th}$ element is $L_k(i,j)$. Then consider the array obtained by replacing each i by a variable x_i.

There is a wonderful book by Gelfand, Kapranov, Zelevinsky: Hyperdeterminants, resultants...

(see Bull AMS for a review). They go back to papers of Cayley.

Questions:

(1) What are the properties of the hyperdeterminant of A?

(2) Special case: suppose $\{L_i\}_{i=1}^{n}$ is a collection of orthogonal latin squares arising from a projective plane. But: Beware of ET!!!