Subspace profiles, q-Whittaker functions and Krylov methods

Samrith Ram

IIIT Delhi

0. Notation

- $\mathbb{F}_q$: finite field of cardinality q.
- $\mathrm{M}_n(\mathbb{F}_q)$: $n \times n$ matrices over $\mathbb{F}_q$.
- μ, λ : Integer partitions.
- λ' : Partition conjugate to λ.
- $\ell(\lambda)$: Number of parts of λ.
- h_λ : Complete homogeneous symmetric function.
- p_λ : Power sum symmetric function.
- $P_\lambda(x; q, t)$: Macdonald symmetric function.
- $P_\lambda(x; t)$: Hall-Littlewood symmetric function.
- $W_\lambda(x; q)$: q-Whittaker symmetric function, $P_\lambda(x; q, 0)$.
- $\widetilde{W}_\lambda(x; q)$: Hall dual of q-Whittaker function.
- $\tilde{H}_\lambda(x; t)$: Modified Hall-Littlewood symmetric function.
- ω : Involution on symmetric functions satisfying $\omega s_\lambda = s_{\lambda'}$.
- $\langle f, g \rangle$: Hall scalar product of symmetric functions f and g.
- $f \circ g$: Plethystic substitution of g into f.
- Δ : A square matrix over $\mathbb{F}_q$.
- $F_\Delta(x)$: invariant flag generating function for $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$.
- $\begin{bmatrix} n \\ k \end{bmatrix}_q$: Number of k-dimensional subspaces of $\mathbb{F}_q^n$.

1. Main Problem

Definition: Given a matrix $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$, a subspace W of $\mathbb{F}_q^n$ has Δ-profile $\mu = (\mu_1, \mu_2, \ldots)$ if

$$\dim(W + \Delta W + \cdots + \Delta^{j-1} W) = \mu_1 + \mu_2 + \cdots + \mu_j \text{ for } j \geq 1.$$

Let $\sigma(\mu, \Delta)$ denote the number of subspaces with Δ-profile μ.

Theorem: If Δ is regular nilpotent (nilpotent with one-dimensional null space), then

$$\sigma(\mu, \Delta) = \prod_{i \geq 2} q^{\mu_i^2} \begin{bmatrix} \mu_{i-1} \\ \mu_i \end{bmatrix}_q .$$

Theorem: If Δ is simple (has irreducible characteristic polynomial),

$$\sigma(\mu, \Delta) = \frac{q^n - 1}{q^{\mu_1} - 1} \prod_{i \geq 2} q^{\mu_i^2 - \mu_i} \begin{bmatrix} \mu_{i-1} \\ \mu_i \end{bmatrix}_q .$$

Bender, Coley, Robbins and Rumsey [2, p. 2] proved the above theorems and posed the following problem in 1992.

Problem: Given μ and Δ, determine $\sigma(\mu, \Delta)$.

2. Invariant flag generating function

The action of Δ on $\mathbb{F}_q^n$ defines an $\mathbb{F}_q[t]$-module on $\mathbb{F}_q^n$ which is isomorphic to a direct sum

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\ell_i} \frac{\mathbb{F}_q[t]}{(g_i^{\lambda_{i,j}})},$$

where $g_i(t) \in \mathbb{F}_q[t]$ are distinct monic irreducible polynomials and the sequence $\lambda^i = (\lambda_{i,1}, \lambda_{i,2}, \ldots, \lambda_{i,\ell_i})$ is an integer partition for each $1 \leq i \leq k$. Let d_i denote the degree of g_i for $1 \leq i \leq k$.

Definition: The invariant flag generating function $F_\Delta(x)$ is a symmetric function in the variables $x = (x_1, x_2, \ldots)$ defined by

$$F_\Delta(x) := \prod_{i=1}^{k} \tilde{H}_{\lambda^i}(x_1^{d_i}, x_2^{d_i}, \ldots ; q^{d_i}) = \prod_{i=1}^{k} p_{d_i} \circ \tilde{H}_{\lambda^i}(x; q),$$

where $\tilde{H}_\lambda(x; t)$ denotes a modified Hall-Littlewood function.

3. General solution to main problem

Theorem (S. R. [3]): For each partition μ,

$$\sigma(\mu, \Delta) = (-1)^{\sum_{j \geq 2} \mu_j} q^{\sum_{j \geq 2} \binom{\mu_j}{2}} \langle F_\Delta(x), \widetilde{W}_\mu(x; q)\, h_{n-|\mu|} \rangle,$$

for each prime power q and each matrix $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$.
Here h_λ and $\widetilde{W}_\lambda$ denote the complete homogeneous symmetric function and dual (with respect to the Hall scalar product) q-Whittaker symmetric function.

Several symmetric functions such as the power sum symmetric functions, the complete homogeneous symmetric functions and products of modified Hall-Littlewood functions arise as $F_\Delta(x)$ for suitably chosen Δ. When μ is a partition of n, the theorem above entails new combinatorial interpretations of the coefficients in the q-Whittaker expansions of each of these symmetric functions.

4. Krylov Subspace Methods

Let $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$ and consider a subset $S = \{v_1, \ldots, v_k\} \subset \mathbb{F}_q^n$. The truncated Krylov subspace of order ℓ generated by S is defined by

$$\mathrm{Kry}(\Delta, S, \ell) := \left\{ \sum_{i=1}^{k} f_i(\Delta) v_i : f_i(x) \in \mathbb{F}_q[x] \text{ and } \deg f_i < \ell \right\}.$$

Let $\psi_{k,\ell}(\Delta)$ denote the probability of selecting a k-tuple of vectors uniformly at random from $\mathbb{F}_q^n$ such that $\mathrm{Kry}(\Delta, S, \ell) = \mathbb{F}_q^n$. Estimating $\psi_{k,\ell}(\Delta)$ is crucial for analyzing a class of algorithms called Krylov subspace methods. These can be traced back to work by Lagrange, Euler, Gauss, Hilbert and von Neumann, among others (Liesen and Strakoš [6, p. 8]). For instance, the Number Field Sieve [5] depends on Krylov subspace methods. Another example is Wiedemann's algorithm, used to determine the minimal polynomials of large matrices over finite fields.

Theorem (S. R. [3]): For each matrix $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$, we have $\psi_{k,\ell}(\Delta) = \langle F_\Delta(x), G(n, k, \ell) \rangle$, where

$$G(n, k, \ell) := q^{-nk} \sum_{\substack{\mu \vdash n \\ \ell(\mu) \leq \ell}} (-1)^{n-\mu_1} (q-1)^{\mu_1} q^{\sum_{j \geq 1} \binom{\mu_j}{2}} \begin{bmatrix} k \\ \mu_1 \end{bmatrix}_q [\mu_1]_q! \widetilde{W}_\mu(x; q).$$

5. Anti-invariant subspaces

Definition: Given $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$ and a positive integer k, a subspace W of $\mathbb{F}_q^n$ is k-fold Δ-anti-invariant if

$$\dim(W + \Delta W + \cdots + \Delta^k W) = (k+1) \cdot \dim W.$$

Anti-invariant subspaces were originally defined (for $k = 1$) by Barría and Halmos [1].

Theorem (S. R. [3]): For $\Delta \in \mathrm{M}_n(\mathbb{F}_q)$, the number of k-fold Δ-anti-invariant subspaces of dimension m equals

$$(-1)^{mk} q^{k\binom{m}{2}} \langle \omega F_\Delta(x), P_{((k+1)^m, 1^{n-m(k+1)})}(x; q) \rangle.$$

6. References

[1] J. Barría & P. R. Halmos, *Weakly Transitive Matrices*, Ill. J. Math. 28.3 (1984).

[2] E. A. Bender, R. Coley, D. P. Robbins & H. Rumsey Jr., *Enumeration of Subspaces by Dimension Sequence*, J. Combin. Theory Ser. A 59.1 (1992).

[3] S. Ram, *Subspace Profiles over Finite Fields and q-Whittaker Expansions of Symmetric Functions*, arXiv:2309.16607 [math.CO].

[4] J. A. Green, *The Characters of the Finite General Linear Groups*, Trans. Amer. Math. Soc. 80 (1955).

[5] A. K. Lenstra et al., *The Number Field Sieve*, Lecture Notes in Math. 1554 (1993).

[6] J. Liesen & Z. Strakoš, *Krylov Subspace Methods: Principles and Analysis*, SIAM 2013.

[7] S. Ram & M. J. Schlosser, *Diagonal Operators, q-Whittaker Functions and Rook Theory*, arXiv:2309.06401 [math.CO].