HYPERPLANE ARRANGEMENTS OVER THE RING OF INTEGERS MODULO n

E. Obeahon
Faculty Advisors: S. Chebolu, P. Sissokho
Illinois State University Math Department

Abstract

We study the structure of hyperplane arrangements over the ring of integers modulo n. The specific problem we are interested in is the problem of counting the number of points in the complement of the Threshold arrangement over a finite field, and the Complete (Resonance) arrangement over a ring.

Introduction

Given positive integers $d \ and \ n$, an odd prime p and a finite field $\mathbb{Z}_p \ with \ characteristic \ p$, an affine hyperplane (or simply hyperplane) in a vector space $\mathbb{Z}_p^d$ is the set of all solutions to an equation of the form $\sum_{i=1}^{d} a_i x_i = b$, where $a_i, b \in \mathbb{Z}_p$, and not all a_i equal to zero. A finite collection of hyperplanes in $\mathbb{Z}_p^d$ is called a hyperplane arrangement (or arrangement). An arrangement H in $\mathbb{Z}_p^d$ is called the Threshold arrangement if $H = \{x_i + x_j = 0 : 1 \leq i < j \leq d\}$. An arrangement L in $\mathbb{Z}_n^d$ is called complete if L is the collection $\{\sum_{x_i \in S} a_i x_i = 0 : S \ is \ nonempty \ and \ S \subseteq \{x_i : 1 \leq i < j \leq d\}\}$. As mentioned in the abstract, we are interested in the cardinality of the sets $\mathbb{Z}_p^d \setminus H$ and $\mathbb{Z}_n^d \setminus L$. We denote $\alpha_p^d(threshold) = |\mathbb{Z}_p^d \setminus H|$, $\alpha_n^d = |\mathbb{Z}_p^d \setminus L|$.

Result

Theorem 1.1. Let d be a positive integer, then there exists a monic polynomials $f_d(x)$, $h_d(x)$ of degree d with integer coefficients such that for any sufficiently large prime p, $\alpha_p^d(threshold) = f_d(p)$, $\alpha_p^d = h_d(p)$.

$Sketch \ of \ Proof$. Consider the $\binom{d}{2}$ hyperplanes defined by the equations $x_i + x_j = 0 : 1 \leq i < j \leq d$; that is, the threshold arrangement on $\mathbb{Z}_n^d$. For every non-empty subset P_i of these hyperplanes, let A_i be a matrix whose rows are the coefficients of hyperplanes contained in P_i. Then A_i defines the linear map:

$$A_i : F_p^d \rightarrow F_p^{m_i}$$

Where $m_i = \# \ of \ hyperplanes \ in \ P_i$. Then $Null(A_i)$ is the intersection of the hyperplanes in P_i. Therefore, we have

$$\alpha_p^d(threshold) = p^d - |the \ set \ of \ all \ points \ in \ the \ union \ of \ the \ \binom{d}{2} \ hyperplanes \ in \ H|$$

Using the exclusion-inclusion principle, we have

$$\alpha_p^d(threshold) = p^d - \sum_{A_i \subseteq S} \pm Null(A_i)$$

Therefore,

$$\alpha_p^d(threshold) = p^d - \sum_{A_i \subseteq S} \pm p^{d-rank(A_i)}$$

We know that $rank(A_i)$ is equal to the maximum order of a non-zero minor of A_i. But the set of all minors of A_i is finite. Therefore, if v_d is the maximum prime divisor of one of these minors of A_i, then for every $p > v_d$, we have rank (A_i) independent of p. Also, rank$(A_i) \geq 1$ because the entries of A_i are not all zeros. Therefore,

$$\alpha_p^d(threshold) = O(p^d).$$

QED.

Theorem 1.2 (R.P. Stanley). Let p be an odd prime, then the exponential generating function of $\alpha_p^d(threshold)$ is given by

$$\sum_{d \geq 0} \alpha_p^d(threshold) \frac{x^d}{d!} = (1+x)(2e^x - 1)^{\frac{p-1}{2}}$$

Let $[x^n]f(x)$ denote the coefficient of x^n in $f(x)$, then from theorem 1.2, we see that

Result

$$\alpha_p^d(threshold) = \left[\frac{x^d}{d!}\right](1+x)(2e^x - 1)^{\frac{p-1}{2}}$$

$$= \sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r r^d \binom{\frac{p-1}{2}}{r} + \sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r d \, r^{d-1} \binom{\frac{p-1}{2}}{r}$$

$$= \sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r r^{d-1} \binom{\frac{p-1}{2}}{r} (r + d)$$

The last equation is a polynomial in p of degree d.

Special Cases.

For $d = 3$: (1,6,4), we have

Let $(f(x))^{(k)} = \frac{d^k}{dx^k} f(x)$, $[f(x)]_{x=k} = f(k)$, then

$$\alpha_p^3(threshold) = \sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r \binom{\frac{p-1}{2}}{r} \left[(x^r)^{(3)} + 6(x^r)^{(2)} + 4(x^r)^{(1)}\right]_{x=1}$$
$$= (p-1)(p-3)(p-5) + 6(p-1)(p-3) + 4(p-1)$$
$$= (p-1)^3$$

For $d = 4$: (1,10,19,5), we have

$$\alpha_p^4(threshold) = \sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r \binom{\frac{p-1}{2}}{r} \left[(x^r)^{(4)} + 10(x^r)^{(3)} + 19(x^r)^{(2)} + 5(x^r)^{(1)}\right]_{x=1}$$
$$= (p-1)(p-3)(p-5)(p-7) + 10(p-1)(p-3)(p-5) + 19(p-1)(p-3) + 5(p-1)$$
$$= p^4 - 6p^3 + 15p^2 - 17p + 7$$

Theorem 1.3. Let the finite sequence $\{\alpha_k\}_{k=0}^{d-1}$ be such that $r^d + dr^{d-1} = \left[\sum_{k=0}^{d-1} \alpha_k (x^r)^{(d-k)}\right]_{x=1}$, then

$$\alpha_p^d(threshold) = \sum_{k=0}^{d-1} \alpha_k \prod_{r=1}^{d-k} (p - (2r - 1))$$

$Proof.$ $\alpha_p^d(threshold) =$

$$\sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r r^{d-1} \binom{\frac{p-1}{2}}{r} (r + d)$$

$$\sum_{r \geq 0} (-1)^{\frac{p-1}{2} - r} 2^r \binom{\frac{p-1}{2}}{r} \left[\sum_{k=0}^{d-1} \alpha_k (x^r)^{(d-k)}\right]_{x=1}$$

$$= \sum_{k=0}^{d-1} \alpha_k 2^{d-k} \frac{p-1}{2} . \frac{p-3}{2} \ldots \frac{p - 2d + 2k + 1}{2}$$

$$= \sum_{k=0}^{d-1} \alpha_k \prod_{r=1}^{d-k} (p - (2r - 1)) \qquad \text{QED.}$$

Therefore, computing α_p^d for all odd prime p is a problem reduced to computing the finite sequence α_k which are the coefficients of $(x^r)^{(d-k)}$ such that $r^d + dr^{d-1} = \left[\sum_{k=0}^{d-1} \alpha_k (x^r)^{(d-k)}\right]_{x=1}$. In general, for $d = d$, let $\alpha_{m,d}$ be such that $r^d + dr^{d-1} = \left[\sum_{m=0}^{d-1} \alpha_{m,d} (x^r)^{(d-m)}\right]_{x=1}$ then

Result

$$[r^k]\left[\sum_{m=0}^{d-1} \alpha_{m,d} (x^r)^{(d-m)}\right]_{x=1}, \qquad 0 \leq k \leq d - m$$

$$= \sum_{m=0}^{d-k} \alpha_{m,d} (-1)^{d-m-k} S_{d-m-k, d-m-1}$$

Where

$$S_{p,q} = \sum_{0 \leq a_1 < a_2 < \ldots < a_p \leq q} a_1 a_2 \ldots a_p$$

$$= \sum_{1 \leq a_1 < a_2 < \ldots < a_p \leq q} a_1 a_2 \ldots a_p \ ; \ S_{0,q} = 1$$

In particular, we have

$$\alpha_{0,d} = 1, \alpha_{1,d} = d + S_{1,d-1} = d + \frac{d(d-1)}{2} = \frac{d(d+1)}{2} = S_{1,d}$$

Also, for $k = 0,1,2,\ldots,d-2$, we have the following recurrence relation

$$\sum_{m=0}^{d-k} \alpha_{m,d} (-1)^{d-m-k} S_{d-m-k, d-m-1} = 0$$

$$\alpha_{k,d} = -\sum_{m=0}^{k-1} \alpha_{m,d} (-1)^{k-m} S_{k-m, d-m-1} \ ; \ 2 \leq k \leq d.$$

For $d = 5$, we have

$$\alpha_{0,5} = 1; \alpha_{1,5} = 15; \alpha_{2,5} = -(\alpha_{0,5} S_{2,3} - \alpha_{1,5} S_{1,3}) = 55;$$

$$\alpha_{3,5}(threshold) = -(-\alpha_{0,5} S_{3,4} + \alpha_{1,5} S_{2,3} - \alpha_{2,5} S_{1,2}) = 50;$$

$$\alpha_{4,5} = -(\alpha_{0,5} S_{4,4} - \alpha_{1,5} S_{3,3} + \alpha_{2,5} S_{2,2} - \alpha_{3,5} S_{1,1}) = 6$$

$$\Longrightarrow \ \alpha_p^5(threshold)$$
$$= (p-1)(p-3)(p-5)(p-7)(p-9) + 15(p-1)(p-3)(p-5)(p-7) + 55(p-1)(p-3)(p-5) + 50(p-1)(p-3) + 6(p-1)$$

The Complete Arrangement

Action of $Aut(\mathbb{Z}_n)$ on $\mathbb{Z}_n^d \setminus L$

Let $Aut(\mathbb{Z}_n)$ denote the automorphism group of $\mathbb{Z}_n$, and L, the complete hyperplane arrangement on $\mathbb{Z}_n^d$ where $\mathbb{Z}_n$ is the ring of integers modulo n. Then $Aut(\mathbb{Z}_n)$ acts naturally on $\mathbb{Z}_n^d \setminus L$ component-wise. Here, we will identify $Aut(\mathbb{Z}_n)$ with the set $\{k : 1 \leq k \leq n - 1 \ and \ gcd(k,n) = 1\}$. An element $\boldsymbol{x} \in \mathbb{Z}_n^d \setminus L$ is called irreducible if $gcd(\boldsymbol{x}, n) = 1$, otherwise x is called reducible. Let $\mathcal{R}_n^d (resp. I_n^d)$ denote the sets of reducible (resp. irreducible) elements of $\mathbb{Z}_n^d \setminus L$. Then,

$$\mathbb{Z}_n^d \setminus L = \mathcal{R}_n^d \sqcup I_n^d$$

The following theorem shows that computing $\alpha_n^d = |\mathbb{Z}_n^d \setminus L|$ is equivalent to computing $\beta_n^d = |I_n^d|$.

Result

Theorem 2.1 ([1]). Let $n \geq 3 \ and \ 1 \leq d < n$ and consider the action of $Aut(\mathbb{Z}_n)$ on $\mathbb{Z}_n^d \setminus L$.

(a) For any $k \in Aut(\mathbb{Z}_n) \ and \ any \ \boldsymbol{x} \in \mathbb{Z}_n^d \setminus L, we \ have \ k \in Stab(\boldsymbol{x}) \ if and \ only \ if \ \frac{n}{gcd(k-1,n)}$ divides $gcd(\boldsymbol{x}, n)$. In particular, if $gcd(\boldsymbol{x}, n) = 1$, then $Stab(\boldsymbol{x}) = 1 \ for \ any \ \boldsymbol{x} \in \mathbb{Z}_n^d \setminus L$.

(b) The number of orbits of the restricted action of $Aut(\mathbb{Z}_n)$ on I_n^d is equal to $\frac{\beta_n^d}{\phi(n)}$. Thus $\phi(n) \ divides \ \beta_n^d$.

(c) $\alpha_n^d = \sum_{m|n, m \geq n} \beta_m^d \ and \ \beta_n^d = \sum_{m|n, m \geq n} \alpha_n^d \, \mu\left(\frac{n}{m}\right)$

(d) If $d \geq max\{m : 1 \leq m < n \ and \ m|n\}$, then $\alpha_n^d = \beta_n^d$ and $\phi(n) \ divides \ \alpha_n^d$. Moreover, the conclusion of this statement holds if $d \geq \frac{n}{2}$.

Determining $\boldsymbol{\alpha_n^d}$ for $\boldsymbol{d > \frac{n}{2}}$ or $\boldsymbol{d \leq 3}$.

We first determine α_n^d for $d > \frac{n}{2}$. We will use the following important theorem based on Savchev and Chen.

Theorem 2.2 ([2]). Every element $\boldsymbol{x} \in \mathbb{Z}_n^d \setminus L$ of length $d > \frac{n}{2}$ can be uniquely represented as $(x_1 k, x_2 k, \ldots, x_d k)$ where k generates $\mathbb{Z}_n$ and $x_1, x_2, \ldots, x_d$ are positive integers whose sum is less than n.

Theorem 2.3. Let $n \geq 3 \ and \ d > {}^n/_2$. Then, $\alpha_n^d = \phi(n)\binom{n-1}{d}$

Sketch of $Proof$. We consider the action of $Aut(\mathbb{Z}_n) \ on \ \mathbb{Z}_n^d \setminus L$. Since $d > {}^n/_2$ it follows from theorem 2.1(d) that $\alpha_n^d = \phi(n) N$, where N is the number of orbits under the action of $Aut(\mathbb{Z}_n)$. So, it suffices to determine N. Thus, N is the number of ordered tuples $(x_1, x_2, \ldots, x_d)$ that satisfy $\sum_{i=1}^{n} x_i < n$. Thus,

$$N = \sum_{j=1}^{n-1} \binom{j-1}{d-1} = \binom{n-1}{d}$$

Therefore, $\alpha_n^d = \phi(n)\binom{n-1}{d}$. QED.

Corollary 1 For any positive integer k, we have $\alpha_n^{n-k} = \phi(n)\binom{n-1}{k-1}$ for all large enough value of n. Moreover,

$$\liminf_n \frac{\phi(n+1)}{\phi(n)} = 0, and \ \limsup_n \frac{\phi(n+1)}{\phi(n)} = \infty$$

References

[1] Sunil K. Chebolu and Papa A. Sissokho, Zero-sum free tuples and hyperplane arrangement, arXiv:2201.01714 ***[math.NT].*** (2022).
[2] S. Savchev and F. Chen, Long zero-free sequences in finite cyclic groups, *Discrete Math*. **307** (2007), 2671 − 2679.
[3] Y. Caro, Zero-sum problems — a survey, *Discrete Math*. **152** (1993), 93−113.
[4] W. Gao and A. Geroldinger, On the structure of zero free sequences, *Combinatorica*. **18** (no. 4) (1998), 519 − 527.
[5] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University press, 5th edition, 1980.[6] T. M. Apostol, Introduction to Analytic Number Theory, Springer Verlag, New York, 1976.
[7] V. Ponomarenko, Minimal zero sequences of finite cyclic groups, *Integers* **4** (2004), #A24.
[8] R.P. Stanley, An introduction to hyperplane arrangement, *in Geometric Combinatorics* (E. Miller, V. Reiner, and B. Sturmfels, eds), IAS/Park City Mathematics Series, vol.13, Amer. Math. Soc., Providence, 2007, 389 − 496.