Dimensionality restrictions on sums over $\mathbb{Z}_p^d$

Ioannis Koutis

January 2007
CMU-CS-07-103

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

Let A be an arbitrary multi-set of vectors from $\mathbb{Z}_p^d$, where p is any prime, and $|A| \geq p(d+2)$. For any fixed j, $0 \leq j \leq p-1$, we show that the numbers (modulo p) of zero-sum A-subsets of cardinality $kp+j$ for $k \geq d+2$, can be determined from the numbers (modulo p) of zero-sum A-subsets of cardinality $kp+j$, for $0 \leq k \leq d+1$. For $p = 2$, we show that the (necessarily odd when $|A| \geq d$) number of zero-sum A-subsets is at most one less than the (necessarily even when $|A| \geq d$) number of subsets summing up to any other vector. We also show a similar result for odd primes. Our main tool is the representation theory for the corresponding groups.

Keywords: additive number theory, zero-sum, group representations

1 Introduction

Throughout the paper, p denotes an odd prime, unless explicitly stated that $p = 2$. $\mathbb{Z}_p$ denotes the group of numbers with addition modulo p, and $\mathbb{Z}_p^d$ denotes the group of d-dimensional vectors with entry-wise addition over $\mathbb{Z}_p$. We study sums over $\mathbb{Z}_p^d$. We say that a set $B \subseteq \mathbb{Z}_p^d$ is α-sum, or that α attracts B, if $\sum_{b \in B} = \alpha$, and that it is an A-subset if $B \subseteq A$.

In a classical paper ([2]), Erdős, Ginzburg and Ziv showed that any set of $2n - 1$ integers contains at least one subsequence of n numbers summing up to zero $mod\ n$. Their result spurred the interest of several authors. Most notably, researchers have considered related questions for sequences of elements taken from finite abelian groups, with respect to different sizes of subsequences (e.g. [1, 3, 6, 8, 7]), or the related problem of the number of subsequences with given sum, taken from sequences of small size (see for example [4, 5] and the references therein).

In this paper we take a different direction and consider the numbers of given sum subsets taken from arbitrary multi-sets $A \subseteq \mathbb{Z}_p^d$. We show that when the size of A exceeds $p(d + 2)$ (roughly the logarithm of the size of $\mathbb{Z}_p^d$), we get strong relationships among the numbers (modulo powers of p) of α-sum subsets of different cardinalities. The result holds for all $\alpha \in \mathbb{Z}_p^d$. We also show that the zero vector behaves differently than any other vector in $\mathbb{Z}_p^d$, with respect to the number of A-subsets that it attracts.

2 A review of basic representation theory

The main tool in our approach will be the representation theory for $\mathbb{Z}_p^d$. We review some standard notions, omitting the proofs. A complete exposition can for example be found in [9].

We will use the fact that there is a set R of permutation matrices of dimension p^d, with $|R| = p^d$, and a bijection $\rho : \mathbb{Z}_p^d \to R$, such that, for any $\alpha, \beta \in \mathbb{Z}_p^d$, we have $\rho(\alpha + \beta) = \rho(\alpha)\rho(\beta) = \rho(\beta)\rho(\alpha)$. That is, the set R with respect to matrix multiplication is a group isomorphic to $\mathbb{Z}_p^d$.

The matrices in R are simultaneously diagonalizable. The Fourier transform that diagonalizes R can be described exactly, but here we will only make use of the following theorem.

Theorem 2.1. *For any α, $\rho(\alpha)$ can be written as*

$$\rho(a) = \frac{1}{p^d} V \Lambda(\alpha) V^H$$

V is independent from α and its entries are powers of the p^{th} primitive root of unity ω, and $V^H V = p^d I$. $\Lambda(\alpha)$ is a diagonal matrix containing the eigenvalues of $\rho(\alpha)$ which are all powers of ω.

3 A representation theory approach

Let A be an arbitrary subset of $\mathbb{Z}_p^d$. Define

$$H = \prod_{\alpha \in A} (I + x\rho(a)) \tag{1}$$

Using the closure of R under multiplication, H can be rewritten as

$$H = \sum_{a \in \mathbb{Z}_p^d} p_a(x)\rho(a) \tag{2}$$

where $p_a(x)$ is a polynomial in x. We take a closer look at $p_a(x)$. Observe that, for any α-sum set $B \subseteq A$, we have

$$\prod_{b \in B} x\rho(b) = x^{|B|}\rho\left(\sum_{b \in B} b\right) = x^{|B|}\rho(\alpha)$$

This term is multiplied by I in Eq. 1, and so, any α-sum A-subset of cardinality k, contributes one x^k term in $p_\alpha(x)$. This means that the coefficient of x^k in $p_\alpha(x)$ is equal to the number of α-sum subsets of A that contain k elements. This observation will allow us to study the problem by considering the coefficients in the polynomials in Eq. 2. Before we proceed, let us illustrate the concept with a small example.

Example. Let $p = 2$, $d = 2$. Then

$$\rho\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \rho\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \rho\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

and

$$H = \prod_{a \in \{Z_2^2 - 0\}} (I + x\rho(a)) = \begin{bmatrix} 1+x^3 & x+x^2 & x+x^2 & x+x^2 \\ x+x^2 & 1+x^3 & x+x^2 & x+x^2 \\ x+x^2 & x+x^2 & 1+x^3 & x+x^2 \\ x+x^2 & x+x^2 & x+x^2 & 1+x^3 \end{bmatrix}$$

Observe for instance that the sum of the three vectors in $\{Z_2^2 - 0\}$ is zero, and this accounts for the coefficient of x^3 in the polynomial appearing in the diagonal of H.

4 Preparatory Lemmas

Let ω be the p^{th} primitive root of unity. We will say that an expression of the form

$$P(\omega) = \sum_{j=0}^{p-1} a_j \omega^j$$

is an integral polynomial in ω if the coefficients a_j are integers. If furthermore $a_j = 0 \; mod \; m$ for all j, we will say that P is $0 \; mod \; m$ and we will write $P = 0 \; mod \; m$. We will naturally use the same terminology for multivariate polynomials, or polynomials in one variable with coefficients that are integral polynomials in ω.

Lemma 4.1. *Let $P = 1 + x\sum_{k=1}^{p} c_k\omega^k$, where $\sum_k c_k = 0$, and c_k are integers. Then P can be rewritten as*

$$P = (1 + x\omega - x\omega^2)Q(\omega) + 1 - Q(\omega)$$

where Q is an integral polynomial.

Proof. It is easy to see that the polynomial $\hat{P}(z) = \sum_{k=1}^{p} c_k z^k$ is divisible by $z - z^2$, and thus there is a polynomial $Q(z)$ such that $\hat{P} = (z - z^2)Q$. Furthermore, Q is an integral polynomial because $\hat{P}$ is an integral polynomial. Then it is easy to verify that

$$P = 1 + x\hat{P}(\omega) = (1 + x\omega - x\omega^2)Q(\omega) + 1 - Q(\omega)$$

□

Lemma 4.2. *Let $t = kp + j$, for $j \in [1, p-1]$. The coefficient of x^m, $m \geq pd$ in*

$$(1 + x\omega - x\omega^2)^t$$

is a $0 \; mod \; p^d$ integral polynomial in ω.

Proof. By Fermat's identity

$$(1 + x\omega - x\omega^2)^p = 1^p + (x\omega)^p + (-x\omega^2)^p + T(x,\omega) = 1 + T(x,\omega)$$

where $T(x,\omega) = 0 \; mod \; p$. The degree of x in $T(x,\omega)$ is p. We have

$$\begin{aligned} (1 + x\omega - x\omega^2)^t &= (1 + x\omega - x\omega^2)^j(1 + x\omega - x\omega^2)^{pk} \\ &= (1 + x\omega - x\omega^2)^j(1 + T(x,\omega))^k \\ &= (1 + x\omega - x\omega^2)^j \sum_{i=0}^{d-1} \binom{k}{i} T^i(x,\omega) + \\ & \quad (1 + x\omega - x\omega^2)^j \sum_{i=d}^{k} \binom{k}{i} T^i(x,\omega) \end{aligned}$$

For $i \leq d-1$, the degree of x in $(1 + x\omega - x\omega^2)^j T^i(x,\omega)$ is less than pd. Thus, any term x^m with $m \geq pd$, necessarily comes as the product of terms from $(1 + x\omega - x\omega^2)^j$ and $T^i(x,\omega)$ for $i \geq d$. The proof follows from the fact that for $i \geq d$, $T^i(x,\omega)$ is $0 \; mod \; p^d$. □

Lemma 4.3. *For $j = 1, \ldots, t$, let $P_j = 1 + x\sum_{k=1}^{p} c_{kj}\omega^k$, where $\sum_{k=1}^{p} c_{kj} = 0$, and c_{kj} are integers. Then for $m \geq pd$, the coefficient of x^m in $\prod_{j=1}^{t} P_j$ is a $0 \; mod \; p^d$ integral polynomial in ω.*

Proof. Each P_j satisfies the conditions of Lemma 4.1 and so it can be rewritten as

$$P_j = (1 + x\omega - x\omega^2)Q_j(\omega) + 1 - Q_j(\omega)$$

where Q_j is an integral polynomial. Using these expressions for P_j, we can write

$$\prod_{j=1}^{t} P_j = \sum_{j=0}^{t} a_j(1 + x\omega - x\omega^2)^j$$

where a_j, $j = 0, \ldots p$, are integral polynomials in ω. The terms contributing to x^m for $m \geq pd$ are $a_j(1 + x\omega - x\omega^2)^j$ for $j \geq pd$. By Lemma 4.2 the coefficient of x^m, $m \geq pd$ in each of these terms is a $0 \ mod \ p^d$ integral polynomial in ω. $\square$

We will also need the following lemma.

Lemma 4.4. *Let $t \geq pd$, where d is any integer. Let $P_j = 1 - \omega^{k_j}$, $j = 1, \ldots, t$. Then, $\prod_{j=1}^{t} P_j$ is a $0 \ mod \ p^d$ integral polynomial in ω.*

Proof. Observe that either P_j is 0 if $k_j = 0 \ mod \ p$, or it is a multiple of $1 - \omega$. Thus $\prod_{j=1}^{t} P_j$ is a multiple of $(1 - \omega)^{pd}$. The lemma follows from the fact that $(1 - \omega)^p$ is $0 \ mod \ p$. $\square$

5 Main results

Theorem 5.1. *Let $A \subset \mathbb{Z}_p^d$, with $|A| \geq p(d + 2)$. For $0 \leq j \leq p - 1$, define $N_\alpha(j, k)$ as the number of α-sum A-subsets of cardinality $kp + j$. Then, for fixed j, the numbers $N_\alpha(j, k) \ mod \ p$, $k \geq 0$ are fully determined from any $d + 2$ of them, $N_\alpha(j, k_1), \ldots, N_\alpha(j, k_{d+2}) \ mod \ p$.*

Proof. We use the approach presented in Section 3. Let $\rho(\alpha)$ denote the matrix representation of α. Define

$$H = \prod_{a \in A}(I + x\rho(a))$$

Now, consider A as a subset of $\mathbb{Z}_p^{d+1}$, by adding a common zero coordinate to all the vectors in A. Let $v \in \mathbb{Z}_p^{d+1}$ be the vector with zeros in the non-zero coordinates of A, and an one in the zero coordinate of A. Consider the product

$$H' = \prod_{\alpha \in A}(I + x\rho(\alpha) - x\rho(v)) = \sum_{a \in \mathbb{Z}_p^{d+1}} p_a(x)\rho(a)$$

By Theorem 2.1, for any α, we have

$$I + x\rho(\alpha) - x\rho(v) = \frac{1}{p^{d+1}} V\Lambda(\alpha)V^H$$

where V contains only powers of the p^{th} primitive root of unity ω, $VV^H = p^{d+1}I$, and $\Lambda(a)$ is a diagonal matrix with all its entries in the form $1 + x\omega^i - x\omega^j$. It follows that H' is of the form

$$H' = \frac{1}{p^{d+1}} V \Lambda_1 V^H$$

where Λ_1 is a diagonal matrix, with each entry being a product of $|A|$ factors of the form $1 + x\omega^i - x\omega^j$. Note that the matrix $V^H \Lambda_1 V$ must have entries which are integral polynomials. Since V consists only of powers of ω, by applying Lemma 4.3 to the entries of Λ_1, it follows that for $m \geq p(d+2)$ the coefficient of x^m, in any entry of $V^H \Lambda_1 V$ must be equal to $0 \; mod \; p^{d+2}$. Thus, the coefficient of x^m in any entry of H' must be equal to $0 \; mod \; p$.

Now we take a closer look at H'. Observe that $(\rho(v))^i = I$ only for $i = 0 \; mod \; p$. Every monomial $x^{(k-i)p+j}$ corresponding to an α-sum A-subset in H, can be padded with ip copies of $-x\rho(v)$ to give a x^{kp+j} term in $p_\alpha(x)$ in H'. On the other hand, any monomial corresponding to an α-sum A-subset in H, padded with $ip + j'$ ($j' \neq 0$) copies of $-x\rho(v)$, gives a monomial that gets added to $p_{\alpha'}(x)$, where α' is non-zero in the $(d+1)^{th}$ coordinate.

Thus, for all α that are zero in the $(d+1)^{th}$ coordinate, every monomial x^{kp+j} in $p_\alpha(x)$ is generated as a product of a term $x^{(k-i)p+j}$ corresponding to an α-sum A-subset of size $(k-i)p+j$, and ip copies of $-xv$. By definition, there are $N_\alpha(j, k-i)$ ways of choosing an α-sum A-subset of size $(k-i)p+j$. Each of these can be completed in $\binom{|A|-((k-i)p+j)}{ip}$ ways with ip copies of $-xv$ to form a x^{kp+j} term. Recall that for $k \geq d+2$, the coefficient of x^{kp+j} is equal to $0 \; mod \; p$. So, for each $k \geq d+2$, we have

$$\sum_{i=0}^{k} N_\alpha(j, k-i)(-1)^i \binom{|A| - ((k-i)p+j)}{ip} = 0 \; mod \; p$$

where $N_\alpha(0,0) = 1$. Each value of k defines a linear equation. Thus, we have obtained a system of linear equations on $N_\alpha(j,k)$. In the k^{th} equation ($k \geq d+2$), the coefficient of $N_\alpha(j,k)$ is 1, and the coefficients of $N_\alpha(j, k' > k)$ are 0. Hence, the equations are linearly independent and the theorem follows. $\square$

Actually, a more general theorem can be proved along the lines of Theorem 5.1. It roughly states that for large enough sets A, decreasing the number of linear relationships between the numbers $N_\alpha(j,k)$ by one, the modulo for which they hold increases by a factor of p. Formally, we have

Theorem 5.2. *Let $A \subset \mathbb{Z}_p^d$, with $|A| \geq p(d+t)$, where $t \geq 2$ is any integer. For $0 \leq j \leq p-1$, define $N_\alpha(j,k)$ as the number of α-sum A-subsets of cardinality $kp+j$. Then, for fixed j, the numbers $N_\alpha(j,k) \; mod \; p^{t-1}$, $k \geq 0$ are fully determined from any $d+t$ of them, $N_\alpha(j,k_1), \ldots, N_\alpha(j, k_{d+t}) \; mod \; p^{t-1}$.*

Proof. Repeat the proof of Theorem 5.1, with the observation that in any entry of H', the coefficient of x^m, for $m \geq p(d+t)$ is $0 \; mod \; p^{t-1}$ $\square$

It is interesting to observe that the the zero vector behaves differently than all other vectors of $\mathbb{Z}_p^d$ with respect to the number of A-subsets that it attracts. This is formalized in the following theorems.

Theorem 5.3. *Let A be an arbitrary multi-set of $\mathbb{Z}_p^d$, with $|A| \geq kp$, $k \geq d+1$. For $\alpha \neq 0$, α attracts an equal (modulo p^{k-d}) number of odd and even cardinality A-subsets. The even cardinality A-subsets attracted by the zero vector is one less (modulo p^{k-d}) than the odd cardinality A-subsets.*

Proof. Let $Z_{1,\alpha}$ be the number of odd cardinality α-sum A-subsets, and $Z_{0,\alpha}$ the number of even cardinality α-sum A-subsets. Let

$$Z_\alpha = \sum_{\substack{B \subseteq A \\ \sum_{b\in B} b = \alpha}} (-1)^{|B|} = Z_{0,\alpha} - Z_{1,\alpha}$$

Let $\rho(\alpha)$ be the representation of α and define

$$H = \prod_{\alpha \in A} (I - \rho(a))$$

By the reasoning developed in Section 3 it can be seen that the diagonal entry of H is equal to $1 + Z_0$ and each other entry is equal to Z_α for some $\alpha \neq 0$. Applying Theorem 2.1 we can rewrite

$$H = \frac{1}{p^d} V \Lambda V^H$$

where each entry of Λ is a product of $|A|$ factors of the form $1 - \omega^j$. By applying Lemma 4.4 to Λ, and using the fact that V contains only powers of ω, we get that each entry of H is $0 \; mod \; p^{k-d}$. The theorem follows. $\square$

In the case $p = 2$ we can similarly prove the following slightly stronger result.

Theorem 5.4. *Let $\alpha \in \mathbb{Z}_2^d$ and $|A| \geq k$, $k \geq d+1$. Let Z_α be the number of α-sum $|A|$-subsets. Then $Z_0 = -1 \; mod \; 2^{d-k}$ and for all $\alpha \neq 1$, $Z_\alpha = 0 \; mod \; 2^{d-k}$.*

Note that the example in Section 3 provides an illustration of this theorem.

Finally, when $p = 2$ we show that the zero vector "attracts" at least one less A-subsets than any other vector a.

Theorem 5.5. *Let Z_α be the number of α-sum A-subsets. Then, $Z_0 + 1 \geq Z_\alpha$, for all $\alpha \in \mathbb{Z}_2^d$.*

Proof. Let $H = \prod_{\alpha \in A}(I + \rho(\alpha))$. The trace of H is equal to $2^d(1 + Z_0)$, and it is also equal to the sum of the eigenvalues of H. By Theorem 2.1 for $\mathbb{Z}_2^d$, it can be seen that the eigenvalues of H are all positive. For any other α, $2^d Z_\alpha$ is a weighted, by the entries of the diagonalizing matrix V, sum of the eigenvalues. The theorem follows from the fact that the entries of V are $1, -1$. $\square$

6 Acknowledgments

I wish to thank Gary L. Miller for helpful discussions.

References

[1] N. Alon and M. Dubiner. Zero-sum sets of presribed size. *Combinatorics*, Paul Erdős is Eighty:33–50, 1993.

[2] P. Erdős, A. Ginzburg, and A. Ziv. Theorem in the additive number theory. *Bull. Research Council Israel*, 10:41–43, 1961.

[3] W. D. Gao. On zero-sum subsequences of restricted size. *J. Number Theory*, 61:97–102, 1996.

[4] W. D. Gao. On the number of zero sum subsequences. *Discrete Math.*, 163:267–273, 1997.

[5] W. D. Gao. On the number of subsequences with given sum. *Discrete Math.*, 195:127–138, 1999.

[6] W. D. Gao. On zero-sum subsequences of restricted size, iii. *Ars. Combin.*, 61:65–72, 2001.

[7] H. Harboth. Ein extremalproblem fur gitterpunkte. *J. Reine Angew. Math.*, 262:356–360, 1973.

[8] Z. W. Sun. Unification of zero-sum problems, subset sums and covers of z. *Electron. Res. Announc. Amer. Math. Soc.*, 9:51–60, 2003.

[9] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University, 1999.