A Note on Set Families and Codes

Jingfeng Xu†, Jian Liu‡
†China Institute for Actuarial Science, Central University of Finance and Economics, Beijing 100081, P. R. China
‡School of Banking and Finance, University of International Business and Economics, Beijing 100029, P. R. China
Email: jingfeng.caida@gmail.com, liujian8210@gmail.com

Abstract

We give two Frankl-like results of set systems with restrictions on set difference sizes and set symmetric difference sizes modulo prime powers. Based on the similar method, we also give a bound on codes satisfying the properties of Hamming distance modulo prime powers.

Keywords: difference, symmetric difference, Hamming distance, separating polynomial

AMS Classification: 05D05

1 Introduction

Let X be a set with n elements, say $X = \{1, 2, \ldots, n\}$ and let $\mathcal{F}$ denote a family of subsets of X. We call a family $\mathcal{F}$ of subsets of X an *antichain* or a *Sperner family* if no member of $\mathcal{F}$ properly contains any other. Throughout the paper let p be a prime and $q = p^\alpha$ be a prime power.

In 1973, Delsarte [4] presented a classical result which is about the families with given symmetric difference sizes between subsets.

Theorem 1.1. *Suppose for any distinct two members F, F' of $\mathcal{F}$, the size of symmetric difference $|F \triangle F'|$ belongs to a set comprising s distinct positive integers. Then $|\mathcal{F}| \leq \sum_{0 \leq i \leq s} \binom{n}{i}$.*

Subsequently, Blokhuis [3] and Frankl [6] proved a "modular version" of Delsarte's theorem respectively.

Theorem 1.2. *Let $\mathcal{F} \subseteq 2^X$ and p be a prime. Suppose for any distinct two members F, F' of $\mathcal{F}$, $p \nmid |F \triangle F'|$, and the number of distinct sizes of symmetric difference $|F \triangle F'| \pmod p$ does not exceed s. Then $\mathcal{F} \leq \sum_{i=0}^{s} \binom{n}{i}$.*

In addition, Frankl [6] obtained the similar result for set systems with given difference sizes between subsets in his same paper.

Theorem 1.3. *Let $\mathcal{F}$ be a Sperner family. Suppose for any two distinct members F, $F' \in \mathcal{F}$, $|F \backslash F'| \pmod p$ is equal to at most s nonzero residues of modulo p. Then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$.*

Let $Z = \{0, 1, \ldots, z-1\}$. The *Hamming distance* $d(\mathbf{a}, \mathbf{b})$ between two words $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ in Z^n is the number of coordinates i, $1 \leq i \leq n$ with $a_i \neq b_i$. The *weight* of a word $\mathbf{a} = (a_1, \ldots, a_n)$ is its Hamming distance from $\mathbf{0} = (0, \ldots, 0)$, i.e., the number of nonzero coordinates. A z-ary code of length n is a subset $C \subseteq Z^n$. Actually the Hamming distance or simply the distance between two sets A and B is $d(A, B) = |A \triangle B|$. Accordingly a 2-ary code of length n corresponds to a family of subsets of X.

The following result on codes is a classical inequality of Delsarte in [4, 5].

Theorem 1.4. *Let C be a z-ary code of length n. If the set of Hamming distances $d(\mathbf{a}, \mathbf{b})$ that occur between distinct codewords $\mathbf{a}$, $\mathbf{b}$ in C has cardinality s, then $|C| \leq \sum_{i=0}^{s} (z-1)^i \binom{n}{i}$.*

Twelve years later Frankl [7] gave the modular generalization of Delsarte's inequality, which was further strengthened by Babai *et al.* [2] in 1995. Moreover, Babai *et al.* proved the result of codes modulo prime powers at the same time.

Theorem 1.5. *Let C be a z-ary code of length n. Suppose that the Hamming distance between any two distinct members of C is never divisible by a prime power q. Then $|C| \leq \sum_{i=0}^{q-1} (z-1)^i \binom{n}{i}$.*

In this paper we will first give a result about set systems with restrictions on the set difference sizes modulo prime powers. Actually for the family with given set symmetric difference sizes between sets, we can give an uniform bound.

Theorem 1.6. *Let $\mathcal{L} = \{1, 2, \ldots, s\}$, where $1, 2, \ldots, s$ are in the residual class of modulo $q (s < q)$. Suppose $\mathcal{F}$ is a family of subsets of X such that $|F \setminus F'| \in \mathcal{L} \pmod q$ for any two distinct members F, F' of $\mathcal{F}$. Then*

$$|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}.$$

Analogously we consider codes and strengthen Theorem 1.5 with special Hamming distances.

Theorem 1.7. *Let C be a z-ary code of length n and $\mathcal{L} = \{1, 2, \ldots, s\}$ be a subset of residue class modulo $q (s < q)$. Suppose that the Hamming*

distance modulo q between any two distinct words of C belongs to $\mathcal{L}$. Then

$$|C| \leq \sum_{i=0}^{s} (z-1)^i \binom{n}{i}.$$

2 Proof of Theorems 1.6

We begin with some helpful definitions and notations, which are also introduced in [1].

The (p-adic) valuation $\mathrm{val}(t)$ of an integer t is defined to be the exponent j such that p^j divides t, but p^{j+1} does not. There are some useful properties of the valuation:

(i) $\mathrm{val}(t) \leq \infty$ and $\mathrm{val}(t) = \infty$ iff $t = 0$;
(ii) $\mathrm{val}(tu) = \mathrm{val}(t) + \mathrm{val}(u)$;
(iii) $\mathrm{val}(t+u) \geq \min\{\mathrm{val}(t), \mathrm{val}(u)\}$ (ultrametric inequality);
(iv) If $\mathrm{val}(t) < \mathrm{val}(u)$ then $\mathrm{val}(t+u) = \mathrm{val}(t)$ (a consequence of the ultrametric inequality);
(v) $\mathrm{val}(p) = 1$.

Definition 2.1. *A polynomial f with integer coefficients separates a set $A \subset \mathbb{Z}$ from a set $B \subset \mathbb{Z}$ if*

$$\max_{x \in A} \mathrm{val}(f(x)) < \min_{x \in B} \mathrm{val}(f(x)).$$

If $A = \{\mu\}$, we say that f separates μ from B.

Note that the above definition is not symmetric in A and B.

We call a polynomial $f(x)$ in variables x_i, $1 \leq i \leq n$, *multilinear* if the power of each variable x_i in each term is at most one. Clearly, if each variable x_i takes only the value 0 or 1, then any polynomial in variables x_i, $1 \leq i \leq n$, can be regarded as a multilinear polynomial since any positive power of a variable x_i may be replaced by one. Throughout this section we use $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ to denote a vector of n variables with each variable x_i only taking values 0 or 1, and we define *the characteristic vector* of subset F of X to be the vector $\mathbf{v}_F = (v_{F_1}, v_{F_2}, \ldots, v_{F_n}) \in R^n$ with $v_{F_i} = 1$ if $i \in F$ and $v_{F_i} = 0$ otherwise. For $x, y \in R^n$, let $x \cdot y = \sum_{i=1}^{n} x_i y_i$ denote their standard inner product.

Proof of Theorem 1.6. Consider the polynomial $g(x) = \prod_{l \in \mathcal{L}} (x - l)$, the coefficients of which are integers obviously.

For each $F \in \mathcal{F}$, let $\mathbf{v}_F$ denote its corresponding characteristic vector. Let $f_F(\mathbf{x})$ be the multilinear polynomial in n variables defined by $f_F(\mathbf{x}) = g(\mathbf{v}_{X \setminus F} \cdot \mathbf{x})$. Note that $f_F(\mathbf{v}_{F'}) = g(|F' \setminus F|)$.

First of all we show that $g(x)$ is a polynomial which separates 0 from $\mathcal{L}+q\mathbb{Z}$ under the condition $\mathcal{L}=\{1,2,\ldots,s\}$. Since $g(|F\setminus F|)=g(0)=(-1)^s s!$, we have $\mathrm{val}(g(|F\setminus F|))=\mathrm{val}(s!)$. For $F\neq F'$, $|F\setminus F'|=ap^\alpha+t$, $1\leq t\leq s$, where a is a nonnegative integer, consider the set $\{ap^\alpha+t-1, ap^\alpha+t-2,\ldots,ap^\alpha+t-s\}$. For each $j>0$, the number of multiples of p^j in this set is at least $\lfloor s/p^j\rfloor$. Specially the number of multiples of p^α is 1, while $\lfloor s/p^\alpha\rfloor=0$. Therefore we have $\mathrm{val}(g(|F\setminus F'|))>\mathrm{val}(s!)$. This implies $\mathrm{val}(g(|F\setminus F|))<\mathrm{val}(g(|F\setminus F'|))$ for any $F\neq F'$. By the definition of the separating polynomial, it is obvious to see that the polynomial $g(x)$ separates 0 from $\mathcal{L}+q\mathbb{Z}$.

There is a claim that the polynomials $f_F(\mathbf{x})$, $F\in\mathcal{F}$, are linearly independent over $\mathbb{Q}$. Note that since the degree of $g(x)$ is s, the degree of $f_F(\mathbf{x})$ is at most s. As we all know, the dimension of the space of multilinear polynomials of degree at most s in n variables is $\sum_{i=0}^{s}\binom{n}{i}$, which can infer $|\mathcal{F}|\leq\sum_{i=0}^{s}\binom{n}{i}$.

Suppose, to the contrary, there exists a nontrivial linear combination

$$\sum_{F\in\mathcal{F}}\beta_F f_F(\mathbf{x})=0$$

with $\beta_F\in\mathbb{Q}$, where not all β_F, $F\in\mathcal{F}$, are zero. Actually we may assume that all coefficients β_F in the above equality are integers, and there exists some non-zero $\beta_{F'}$ which is not divisible by p. By taking $\mathbf{x}=\mathbf{v}_{F'}$ we can rewrite the above equality as

$$\beta_{F'}g(|F'\setminus F'|)=-\sum_{F\neq F'}\beta_F g(|F'\setminus F|).$$

Using property (iii) of the valuation (that is, ultrametric inequality), we obtain the following inequality,

$$\mathrm{val}(\beta_{F'}g(|F'\setminus F'|))\geq\min_{F\neq F'}\{\mathrm{val}(\beta_F g(|F'\setminus F|))\}. \tag{2.1}$$

As we have proved $g(x)$ is a polynomial which separates 0 from $\mathcal{L}+q\mathbb{Z}$, here we have $\mathrm{val}(g(|F'\setminus F|))>\mathrm{val}(g(|F'\setminus F'|))=\mathrm{val}(s!)$ for any $F\neq F'$. Therefore, the right hand side of inequality (2.1) is greater than $\mathrm{val}(s!)$. For the left hand side of inequality (2.1), it is easy to see that

$$\mathrm{val}(\beta_{F'}g(|F'\setminus F'|))>\mathrm{val}(s!). \tag{2.2}$$

Based on property (ii) of the valuation, we have $\mathrm{val}(\beta_{F'}g(|F'\setminus F'|))=\mathrm{val}(\beta_{F'})+\mathrm{val}(g(|F'\setminus F'|))=\mathrm{val}(\beta_{F'})+\mathrm{val}(s!)$, implying $\mathrm{val}(\beta_{F'})>0$. But $\mathrm{val}(\beta_{F'})=0$ since $p\nmid\beta_{F'}$, a contradiction. This concludes our proof. ∎

3 Proof of Theorem 1.7

In this section, we are concerned with codes and give the proof of Theorem 1.7.

Proof of Theorem 1.7. As Babai *et al.* [2], at first we define the following two polynomials which are crucial for our proof.

For a fixed integer $a \in Z$, let $\varepsilon(a, x)$ be the polynomial in the variable x with rational coefficients such that for each $b \in Z$

$$\varepsilon(a,b) = \begin{cases} 0, & \text{if } b = a, \\ 1, & \text{if } b \neq a. \end{cases}$$

For every $\mathbf{a} = (a_1, \ldots, a_n) \in C$, let us define the polynomial $f_{\mathbf{a}}(\mathbf{x})$ of n variables $x_1, \ldots, x_n$:

$$f_{\mathbf{a}}(\mathbf{x}) = \prod_{l \in \mathcal{L}} \left(\sum_{i=0}^{n} \varepsilon(a_i, x_i) - l \right),$$

clearly the coefficients of which are integers.

Note that, for any two distinct words $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n) \in C$, the representation $\sum_{i=0}^{n} \varepsilon(a_i, b_i)$ computes the Hamming distance of $\mathbf{a}$ and $\mathbf{b}$. For $\mathbf{a} = \mathbf{b}$, $f_{\mathbf{a}}(\mathbf{a}) = (-1)^s s!$, so $\mathrm{val}(f_{\mathbf{a}}(\mathbf{a})) = \mathrm{val}(s!)$. For $\mathbf{a} \neq \mathbf{b}$, we may assume $\sum_{i=0}^{n} \varepsilon(a_i, b_i) = rp^\alpha + t$, where r is a non-negative integer and $1 \leq t \leq s$. Then for every $j > 0$, the number of multiples of p^j in the set $\{rp^\alpha + t - 1, \ldots, rp^\alpha + t - s\}$ is at least $\lfloor s/p^j \rfloor$, specially the number of multiples of p^α is 1 in this set while $\lfloor s/p^\alpha \rfloor = 0$. Accordingly, $\mathrm{val}(f_{\mathbf{a}}(\mathbf{b})) > \mathrm{val}(s!)$ for and distinct pair $\mathbf{a}$, $\mathbf{b}$. By the argumentation in previous section, it is not difficult to see polynomials $f_{\mathbf{a}}$, $\mathbf{a} \in C$, separate 0 from $\mathcal{L} + q\mathbb{Z}$.

We claim that these polynomials $f_{\mathbf{a}}$, $\mathbf{a} \in C$, are linearly independent over $\mathbb{Q}$. Consider a nontrivial linear combination

$$\sum_{\mathbf{a} \in C} \lambda_{\mathbf{a}} f_{\mathbf{a}}(x) = 0,$$

and discuss as in the proof of Theorems 1.6, then we can obtain all $\lambda_{\mathbf{a}}$, $\mathbf{a} \in C$, equal to zero. This concludes our claim.

Note that all our discussions are over the domain where $x_i(x_i - 1) \cdots (x_i - z + 1) = 0$ for every variable x_i, $1 \leq i \leq n$. Consequently we can assume that each variable x_i has exponent at most $z - 1$ in polynomials $f_{\mathbf{a}}$, $\mathbf{a} \in C$. Otherwise we can reduce it modulo $x_i(x_i - 1) \cdots (x_i - z + 1)$ for all x_i.

In addition, each term of $f_{\mathbf{a}}$ is a monomial with at most s variables. The space of such monomials has dimension $\sum_{i=0}^{s}(z-1)^i\binom{n}{i}$. Before this, we have found $|C|$ linearly independent polynomials in this space, implying our desired bound. ∎

Remark. As a corollary, a similar result of Theorem 1.6, which is about the family with given symmetric difference sizes between sets, is derived directly from the above theorem when $z = 2$.

Corollary 3.1. *Let $\mathcal{L} = \{1, 2, \ldots, s\}$, where $1, 2, \ldots, s$ are in the residual class of modulo q. Suppose $\mathcal{F}$ is a family of subsets of X such that $|F \triangle F'| \in \mathcal{L} \pmod q$ for any two distinct members F, F' of $\mathcal{F}$. Then*

$$|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}.$$

Acknowledgments. Authors are very grateful to the referee for detailed comments and suggestions which helped to improve the presentation of the manuscript.

References

[1] L. Babai, P. Frankl, S. Kutin and D. Štefankovič, Set systems with restricted intersections modulo prime powers, J. Combinatorial Theory Ser. A 95 (2001) 39–73.

[2] L. Babai, H. Snevily and R. M. Wilson, A new proof of several inequalities on codes and sets, J. Combinatorial Theory Ser. A 71 (1995) 146–153.

[3] A. Blokhuis, Few-distance sets, 1983. (This is his Ph. D. Thesis. Publication: http://repository.tue.nl/53747)

[4] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Repts. Suppl. 10 (1973), Centrex Publ. Co., Eindhoven, Netherlands, 1973.

[5] P. Delsarte, The association schemes of coding theory, *in* "Combinatorics; Proceedings of the NATO Advanced Study Institute, Breukelen, 1974, Part 1: Theory of Designs, Finite Geometry and Coding Theory," pp. 139–157, Math. Center Tracts, No. 55, Math. Centrum, Amsterdam, 1974.

[6] P. Frankl, Bounding the size of a family knowing the cardinality of differences, Studia Sci. Math. Hungar. 20 (1985), no. 1–4, 33–36.

[7] P. Frankl, Orthogonal vectors in the n-dimensional cube and codes with missing distances, Combinatorica 6 (1986) 279–285.

SMALL COMPLETE CAPS IN GALOIS SPACES

GIORGIO FAINA, FABIO PASTICCI, AND LORENZO SCHMIDT

ABSTRACT. Some new families of complete caps in Galois affine spaces $AG(N,q)$ of dimension $N \equiv 0 \pmod 4$ and odd order $q \leq 127$ are constructed. No smaller complete caps appear to be known.

1. INTRODUCTION

A k-cap in an (affine or projective) Galois space over the finite field with q elements $\mathbb{F}_q$, is a set of k points no three of which are collinear. A k-cap is said to be complete if it is not contained in a $(k+1)$-cap. A plane k-cap is also called a k-arc.

The central problem on caps is determining the maximal and minimal sizes of complete caps in a given space, see the survey papers [14],[1] and the references therein. For the size of the smallest complete cap in the affine space $AG(N,q)$ of dimension N over $\mathbb{F}_q$, the trivial lower bound is $\sqrt{2}q^{\frac{N-1}{2}}$. Complete caps of size about $q^{N/2}$ are known to exist for q even, see [16, 10, 8, 12]; the same holds for q odd, provided that N is even [7]. In this paper, the case q odd, $N \equiv 0 \pmod 4$ will be dealt with. Under these assumptions, complete caps of size $k \leq \frac{1}{2}q^{\frac{N}{2}}$ were obtained by Giulietti, provided that $q \geq 76^2$ [7]. For $25 < q < 76^2$, the smallest known complete caps appear to have size $q^{N/2}$. The aim of this paper is to construct smaller complete caps for q in this range.

Our main result is the following.

Theorem 1.1. *Assume that* $N \equiv 0 \pmod 4$. *Then there exists a complete cap in* $AG(N,q)$ *of size* $n_q q^{\frac{N-2}{2}}$, *with* (q, n_q) *as follows:*

q	27	29	53	67	73	81	83	89
n_q	23	25	35	42	45	49	50	54
q	97	101	103	107	109	113	121	127
n_q	55	61	60	63	65	66	71	74

2000 *Math. Subj. Class.*: 51E22.
Keywords: Affine space, Complete cap, Complete arc.