On Two Applications of Polynomials $x^k - cx - d$ over Finite Fields and More

Canberk İrimağzı[1,2] and Ferruh Özbudak[1,2(✉)]

[1] Department of Mathematics, Middle East Technical University, Dumlupınar Bul., No:1, 06800 Ankara, Turkey
{canberk,ozbudak}@metu.edu.tr
[2] Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bul., No:1, 06800 Ankara, Turkey

Abstract. For integers $k \in [2, q-2]$ coprime to $q-1$, we first bound the number of zeroes of the family of polynomials $x^k - cx - d \in \mathbf{F}_q[x]$ where $q = 2^n$ such that $q-1$ is a prime or $q = 3^n$ such that $(q-1)/2$ is a prime. This gives us bounds on cross-correlation of a subfamily of Golomb Costas arrays.

Next, we show that the zero set of $x^k - cx - d$ over $\mathbf{F}_q$ is a planar almost difference set in $\mathbf{F}_q^*$ and hence for some set of pairs (c, d), they produce optical orthogonal codes with $\lambda = 1$.

More generally, we give an algorithm to produce optical orthogonal codes (OOCs) from $P(x) = x^{\ell_1} + c_{\ell_2} x^{\ell_2} + c_{\ell_2 - 1} x^{\ell_2 - 1} + \cdots + c_1 x \in \mathbf{F}_q[x]$ where interestingly $\ell_1 \gg \ell_2$. We focus on the case $\ell_2 \in \{2, 3\}$ and provide examples of $(q-1, w, \lambda)$-OOCs with $\lambda \in \{2, 3\}$.

Keywords: Golomb costas permutations · Planar cyclic almost difference sets · Almost difference families · Optical orthogonal codes · Radar · Sonar · Optical CDMA

1 Introduction

Costas arrays have applications in sonar and radar systems as they have optimal autocorrelation properties. Their study centres around two problems: searching for methods to create Costas arrays and studying cross-correlation of families of Costas arrays. The study of cross-correlation of Costas arrays boils down to finding a suitable family with good cross-correlation properties. One such family is considered by Gómez-Pérez and Winterhof in [8].

Optical orthogonal codes are primarily used in optical CDMA communication systems. It is important to construct such codes with good parameters and large size. There are constructions of optimal optical orthogonal codes with parameters (n, w, λ) in case $\lambda = 1$ in the literature ([2,11]), however either the number of such codes (even if optimal) is limited or these codes have low weight. In [4], Ding and Xing considers the next case where $\lambda = 2$.

Freedman and Levanon proved in [7] that any two distinct Costas arrays of the same size > 3 have cross-correlation of at least 2. In Subsect. 2.2, we

S. Mesnager and Z. Zhou (Eds.): WAIFI 2022, LNCS 13638, pp. 14–32, 2023.
https://doi.org/10.1007/978-3-031-22944-2_2

show that there are ℓ Golomb Costas arrays of size $q-2$ whose maximal cross-correlation achieves this lower bound where $q = 2^\ell$ and ℓ is a prime. More generally, let p be a prime, $n \geqslant 2$ a positive integer, and t denote the smallest prime divisor of n. We show that there is a collection of t distinct Golomb Costas arrays of size $q-2$ whose maximal cross-correlation is at most p where $q = p^n$.

The maximal cross-correlation $C(\mathcal{G}_q)$ of the set $\mathcal{G}_q = \{\pi_{g_1,g_2} \,|\, g_1 \in \mathbf{F}_q \text{ is a primitive element}\}$ (considered first by Gómez-Pérez and Winterhof in [8]) of Golomb Costas permutations where $g_2 \in \mathbf{F}_q$ is a fixed primitive element is expressed as follows:

$$\max_{\substack{2\leqslant k\leqslant q-2\\ \gcd(k,q-1)=1}} \max_{\substack{c,d\in\mathbf{F}_q\\ c\neq 0}} |\{x \in \mathbf{F}_q \setminus \{0,1\} \,|\, x^k - cx - d = 0\}|.$$

In [8], Gómez-Pérez and Winterhof showed that $C(\mathcal{G}_q)$ of the subfamily $\mathcal{G}_q$ of Golomb Costas permutations of size $q-2$ when $q-1 = 2^n - 1$ is a Mersenne prime is bounded above by $\lfloor (1-1/(q-1))(1+q^{1/2})\rfloor$. We call this Case I. They also show that in case q is an odd prime power and $(q-1)/2$ is prime, $C(\mathcal{G}_q)$ is bounded above by $1 + \lfloor (1-2/(q-1))q^{1/2}\rfloor$. We call this Case II, and it consists of two subcases when

(a) q is a power of 3 and $(q-1)/2$ is prime (see Lemma 1 in [6]), and
(b) q is a safe prime, that is, both q and $(q-1)/2$ are prime.

In Part I, we focus on Case I and Case II(a). Using a combinatorial argument, we obtain two new bounds for each case: conditional bound (on computing some values with the help of a computer) and unconditional bound. We prove that our unconditional bounds (at worst) recover Gómez-Pérez and Winterhof's bounds while the numerics suggest a mild improvement. In either case, numerics show that the conditional bounds (whenever computed) significantly improve the bounds given by Gómez-Pérez and Winterhof.

The combinatorial nature of zero-sets of polynomials $x^k - cx - d$ led us to produce optical orthogonal codes with $\lambda = 1$. In [4], Ding and Xing construct optical orthogonal codes with parameters $(2^m - 1, w, 2)$ where $w \in \{5, 9, 11, 13\}$ using cyclotomy (also, for odd primes $w \geqslant 11$ for which 2 is a primitive element in the prime field $\mathbf{F}_w$). Although these codes are non-optimal, they are of large size and thus very promising for applications. Motivated by their work, we provide the following examples:

(i) $(2^{21} - 1, 32, 2)$ optical orthogonal code with size $2^{16} - 1$, and
(ii) $(3^{13} - 1, 81, 3)$ optical orthogonal code with size $\frac{3^9-1}{2}$,
(iii) $(2^{14} - 1, 16, 2)$ optical orthogonal code with size $2 \cdot (2^{10} - 1)$,
(iv) $(3^7 - 1, 5, 2)$ optical orthogonal code with size 14329,
(v) $(2110, 5, 2)$ optical orthogonal code with size 13600.

The first three codes are members of some infinite classes and they arise from linearized polynomials while the last two arise from non-linearized polynomials. We provide a general algorithm to construct such codes in Part III.

The details of our results and the organization of the paper is as follows. Our main results in Part I are Theorem 3 and Theorem 4 from which we derive Corollary 1 and Corollary 2. The strength of the conditional bounds we obtain is illustrated in Table 1 and Table 2. Moreover, in the appendix (Sect. A), the unconditional bounds are proved to at worst recover the corresponding bounds given by Gómez-Pérez and Winterhof.

The elementary proof of Theorem 3 and Theorem 4 led us to investigate further to uncover the mathematical reason behind the picture and thus in Part II, we study the combinatorial nature of the zero sets of the polynomials $x^k - cx - d$. Our main results of Part II are Theorem 6 and Theorem 7. We discover that the zero sets of the polynomials $x^k - cx^{p^i} - d$ are planar almost difference sets in $\mathbf{F}_q^*$. Some collections of these zero sets in fact form almost difference families yielding optical orthogonal codes. Corollary 3 turns out to be a result of Moreno et al. [11]. We end this section by discussing the importance of computing the multiplicity distribution of low-degree monomials (see Remark 17).

Our efforts culminate in Part III and we present an algorithm to construct optical orthogonal codes from polynomials and provide examples.

2 Part I: Cross-Correlation of Golomb Costas Arrays

2.1 Golomb Costas Arrays

Let $q \geqslant 4$ be a prime power and $\mathbf{F}_q$ denote the finite field of q elements and with characteristic p. For an integer $m \geqslant 1$, let $[m]$ denote the set $\{1, 2, \ldots, m\}$.

Definition 1 *(Definition 3, [6]). Fix two primitive elements g_1, g_2 of the field $\mathbf{F}_q$. Define a permutation $\pi_{g_1,g_2} : [q-2] \to [q-2]$ by*

$$\pi_{g_1,g_2}(i) = j \text{ if and only if } g_1^i + g_2^j = 1.$$

Such a permutation is called Golomb Costas permutation. Note that $\pi_{g,h} = \pi_{g_1,g_2}$ if $g = \sigma(g_1)$ and $h = \sigma(g_2)$ where $\sigma \in Gal(\mathbf{F}_q/\mathbf{F}_p)$, so the cardinality of the set of all Golomb Costas permutations is $\varphi(q-1)^2/n$. Here, φ denotes Euler's phi function.

Definition 2 *(Definition 4, [6]). Let $f, g : [n] \to [n]$ be two maps. The cross-correlation between f and g at $(u, v) \in \mathbf{Z}^2$ is*

$$C_{f,g}(u, v) := |\{(i + u, f(i) + v) \,|\, i \in [n]\} \cap \{(i, g(i)) \,|\, i \in [n]\}|.$$

Note that $C_{f,g}(u, v) = 0$ for pairs (u, v) such that $|u|, |v| \geqslant n$. The maximal cross-correlation $C(\mathcal{F})$ of a family $\mathcal{F}$ of maps (of cardinality at least 2) is $\max_{\substack{f,g \in \mathcal{F} \\ f \neq g}} \max_{(u,v) \in \mathbf{Z}^2} C_{f,g}(u, v)$.

2.2 A Small Family of Golomb Costas Permutations with Low Cross-Correlation

Let n denote the degree of the extension field $\mathbf{F}_q$ over the prime field $\mathbf{F}_p$. Let t denote the smallest prime divisor of n.

Proposition 1. *Let us fix two primitive elements g_1, g_2 of the field $\mathbf{F}_q$ and $\sigma \in Gal(\mathbf{F}_q/\mathbf{F}_p)$ denote the Frobenius automorphism. Then, the maximal cross-correlation of the subfamily*

$$\mathcal{G} = \{\pi_{g,h} \,|\, g = \sigma^r(g_1), h = g_2 \text{ where } 0 \leqslant r < t\}$$

(where t is the smallest prime divisor of n) of Golomb Costas permutations is at most p.

Proof. Let $\pi_1 := \pi_{\sigma^{r_1}(g_1),g_2}$ and $\pi_2 := \pi_{\sigma^{r_2}(g_1),g_2}$ be distinct permutations in $\mathcal{G}$. Here, $r_1 \neq r_2$ and without loss of generality we may assume $r_1 > r_2$. Then, $C_{\pi_1,\pi_2}(u,v)$ is the number of solutions of the equation

$$g_2^v(1 - g_1^{p^{r_1}x}) = (1 - g_1^{p^{r_2}(x+u)})$$

where $x, x+u \in [q-2]$. This number is bounded above by the number of $\mathbf{F}_q$-solutions of the polynomial

$$b(1-y)^{p^{r_1}} = (1-ay)^{p^{r_2}},$$

or equivalently

$$b^{p^{-r_2}} y^{p^{r_1-r_2}} - ay + 1 - b^{p^{-r_2}} = 0.$$

If we denote one of its zeroes by c, then all of its zeroes are of the form $c+dz$ where $c, d \in \overline{\mathbf{F}_q}$ are fixed and $z \in \mathbf{F}_{p^k}$ where $k = r_1 - r_2$. Suppose it has three zeroes $c, c+dz_1, c+dz_2$ in $\mathbf{F}_q$, then $z_2/z_1 \in \mathbf{F}_q \cap \mathbf{F}_{p^k}^* = \mathbf{F}_p^*$ (note that $0 < k = r_1 - r_2 < t$ and $\gcd(k,n) = 1$.). This forces that there are at most p zeroes in $\mathbf{F}_q$ and this completes the proof.

Remark 1. Let $0 < d_1 < d_2$ be two consecutive divisors of n. One can more generally prove that the maximal cross-correlation of the subfamily

$$\mathcal{G} = \{\pi_{g,h} \,|\, g = \sigma^r(g_1), h = g_2 \text{ where } 0 \leqslant r < d_2\}$$

of Golomb Costas permutations is at most p^{d_1}.

2.3 Cross-Correlation of a Subfamily of Golomb Costas Arrays

Notations 1. For a fixed primitive element $g_2 \in \mathbf{F}_q$, let $\mathcal{G}_q$ denote the set

$$\{\pi_{g_1,g_2} \,|\, g_1 \text{ is a primitive element of } \mathbf{F}_q\}$$

of Golomb Costas permutations. The maximal cross-correlation of this subfamily is studied in [8].

Let $\pi_1 = \pi_{g_1^r, g_2}$ and $\pi_2 = \pi_{g_1^s, g_2}$ be two distinct Golomb Costas permutations where $1 \leqslant r, s \leqslant q-2$ coprime to $q-1$ and $r \neq s$. Then, $C_{\pi_1,\pi_2}(u,v)$ is the number of nonzero solutions to the equation

$$g_2^v(1 - g_1^{rx}) = (1 - g_1^{s(x+u)})$$

where $x, x+u \in [q-2]$ so that $\max\limits_{(u,v)\in\mathbf{Z}^2} C_{\pi_1,\pi_2}(u,v)$ is the number of $\mathbf{F}_q$-solutions other than 0 and 1 of the polynomial

$$b(1-y^r) = 1 - ay^s$$

where $a, b \in \mathbf{F}_q^*$ are arbitrary. Composing this polynomial with the permutation polynomial $x^{1/r}$ where $1/r$ denotes the multiplicative inverse of r modulo $q-1$, we get the polynomial

$$ay^{s/r} - by + b - 1.$$

Hence, $C(\mathcal{G}_q)$ is equal to

$$\max_{\substack{2\leqslant k\leqslant q-2\\ \gcd(k,q-1)=1}} \max_{\substack{c,d\in\mathbf{F}_q\\ c\neq 0}} |\{x \in \mathbf{F}_q \setminus \{0,1\} \mid x^k - cx - d = 0\}|. \qquad (\bigstar)$$

2.4 Golomb Costas Arrays of Size $q-2$ Where $q-1$ Is a Mersenne Prime

Throughout Sect. 2.4, let q denote a power of 2 such that $q-1$ is a prime, i.e., $q-1 = 2^n - 1$ is a Mersenne prime. In [8], Gómez-Pérez and Winterhof showed that the maximal cross-correlation $C(\mathcal{G}_q)$ of the subfamily $\mathcal{G}_q$ of Golomb Costas permutations of size $q-2$ when $q-1$ is a Mersenne prime is bounded above by $\lfloor (1 - 1/(q-1))(1 + q^{1/2}) \rfloor$.

Lemma 1. *Suppose $n > 2$ is a positive integer such that $q - 1 = 2^n - 1$ is a (Mersenne) prime. Then, we have*

$$C(\mathcal{G}_q) = \max_{2\leqslant k\leqslant q-2} \max_{\substack{c,d\in\mathbf{F}_q\\ c\neq 0}} |\{x \in \mathbf{F}_q \setminus \{0,1\} \mid x^k - cx - d = 0\}| = \max_{2\leqslant k\leqslant q-2} \max_{d\in\mathbf{F}_q^*} |\{x \in \mathbf{F}_q \mid x^k - x - d = 0\}|.$$

Proof. Note that the polynomials $x^k - cx - d$ and $(x/\alpha)^k - c/\alpha^{k-1}x/\alpha - d/\alpha^k$ have the same number of distinct zeroes where $\alpha \in \mathbf{F}_q^*$. Setting $\alpha = c^{\frac{1}{1-k}}$, we prove the statement. (Here, $\frac{1}{1-k}$ denotes the multiplicative inverse of $1-k$ modulo $q-1$.)

Remark 2. With the help of Lemma 1, we were able to compute that $C(\mathcal{G}_q) = 13$ for $n = 13$ using Magma [1] within two days.

Remark 3. For a Mersenne prime $q - 1 = 2^n - 1$, let $\alpha \in \mathbf{F}_q^*$ be a fixed element other than 1. Since the multiplicative group $\mathbf{F}_q^*$ is generated by any element other than 1, both α and $\alpha + 1$ are primitive elements. As α is primitive, we have $\alpha^k = \alpha + 1$ for some $2 \leqslant k \leqslant q-2$, i.e., α is a zero of the polynomial $x^k - x - 1 \in \mathbf{F}_p[x]$. As α is primitive, it has n distinct Galois conjugates over $\mathbf{F}_p$ so that $C(\mathcal{G}_q) \geqslant n$.

Definition 3 *(Definition 1.1, [10]). Let $f \in \mathbf{F}_q[x]$ be a nonzero polynomial. Throughout this definition, $\mathbf{F}_q$ denotes any finite field. Let $\nu_i(f)$ denote the cardinality of the set*

$$\{(c,d) \in \mathbf{F}_q^2 \mid \text{ the polynomial } f(x) - cx - d \text{ has } i \text{ distinct zeroes in } \mathbf{F}_q\}.$$

The sequence $(\nu_i(f))_{i=0}^q$ is called the intersection distribution of f.

For $c \in \mathbf{F}_q$, let $\mathcal{M}_i(f,c)$ denote the set $\{d \in \mathbf{F}_q \mid f(x) - cx - d$ has i solutions in $\mathbf{F}_q\}$ and $M_i(f,c)$ be its cardinality. The sequence $(M_i(f,c))_{i=0}^q$ is called the multiplicity distribution of f at c. We will use the multiplicity distribution in Part II.

Notations 2. Fix a polynomial $f \in \mathbf{F}_q[x]$. For $c, d \in \mathbf{F}_q$, let $S_{c,d}(f)$ denote the set $\{x \in \mathbf{F}_q \mid f(x) - cx - d = 0\}$. Note that for an automorphism $\sigma \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$, we have $|S_{c,d}(f)| = |S_{\sigma(c),\sigma(d)}(f)|$. If f is clear from the context, we will simply write $S_{c,d}$ in place of $S_{c,d}(f)$.

Theorem 3. *Suppose $n > 2$ is a positive integer such that $q - 1 = 2^n - 1$ is a (Mersenne) prime. Let $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ be defined by $f(x) = x^k$ where for some $2 \leqslant k \leqslant q-2$. Then, $\nu_i(f) = 0$ for $i > \max\left\{\left\lfloor \sqrt{\frac{q-2}{n} + \frac{1}{4}} + \frac{1}{2} \right\rfloor, \mathbf{S}_{1,1}\right\}$ where $\mathbf{S}_{1,1} = \max\limits_{2 \leqslant k \leqslant q-2} |S_{1,1}(x^k)|$.*

Proof. Consider the polynomial $f(x) - cx - d$. By Lemma 1, we may assume that $c = 1$ and $d \in \mathbf{F}_q^*$. Moreover, it suffices to show that the number of zeroes of $f(x) - x - d$ in $\mathbf{F}_q$ is bounded above by $\left\lfloor \sqrt{\frac{q-2}{n} + \frac{1}{4}} + \frac{1}{2} \right\rfloor$ whenever $d \neq 1$. In other words, we may assume that d is a primitive element.

Let $\beta, \beta + \alpha \in \mathbf{F}_{2^n}$ be two distinct zeroes of the polynomial $f(x) - x - d$ where $d \in \mathbf{F}_{2^n} \setminus \mathbf{F}_2$ (so, $\alpha \neq 0$). Then,

$$\begin{aligned} f(\beta) - \beta - d &= 0 \\ f(\beta + \alpha) - (\beta + \alpha) - d &= 0 \end{aligned}$$

This implies that β and $\beta + \alpha$ are solutions to the equation $f(x + \alpha) + f(x) = \alpha$. Dividing both sides by α^k, we observe that

$$D_1 f(\beta/\alpha) = \alpha^{1-k}$$

where $D_1 f(x) = (x+1)^k + x^k$ is the derivative of f at 1. In other words, α^{1-k} is in the image of $D_1 f(x)$ and β/α and $\beta/\alpha + 1$ are in the corresponding preimage set. Now, let us denote by Δ the set $\{(x_1, x_2) \in S_{1,d} \times S_{1,d} \mid x_1 = x_2\}$ and define a map Φ from the set

$$(S_{1,d} \times S_{1,d}) \setminus \Delta = \{(x_1, x_2) \in \mathbf{F}_q^2 \mid f(x_1) - x_1 - d = 0, f(x_2) - x_2 - d = 0 \text{ and } x_1 \neq x_2\}$$

to the graph

$$\{(y, z) \in \mathbf{F}_q^2 \mid D_1 f(y) = z, \text{ and } y \neq 0, 1\}$$

of the derivative of f at 1 by $(x_1, x_2) \mapsto (x_1/(x_1 - x_2), (x_1 - x_2)^{1-k})$. Note that this map is injective as $\gcd(1-k, q-1) = 1$. Let

$$(1, b) \sim (1, d)$$

if $b = \sigma^r(d)$ for some $0 \leqslant r < n$. If $x \in S_{1,d}$, then $x^{p^r} \in S_{1,\sigma^r(d)}$ and since $d \notin \mathbf{F}_2$, we have $S_{1,d} \cap S_{1,\sigma^r(d)} = \varnothing$ for any $r \neq 0$. Note that Φ injectively extends to the domain $\bigsqcup_{(1,b)\sim(1,d)} ((S_{1,b} \times S_{1,b}) \setminus \Delta)$. Here, $|S_{1,b}| = |S_{1,d}|$ for any $(1, b) \sim (1, d)$ and there are n such pairs $(1, b)$ as d is primitive. The target has cardinality $q - 2$ and the domain has $n\ell(\ell - 1)$ elements where ℓ is the number of distinct zeroes of the polynomial $f(x) - x - d$. This implies that

$$n\ell(\ell - 1) \leqslant q - 2$$

so that

$$\ell \leqslant \sqrt{\frac{q-2}{n} + \frac{1}{4}} + \frac{1}{2}.$$

and this finishes the proof.

Remark 4. Note that since $\mathbf{S}_{1,1}$ is divisible by n, the proof in fact shows that $\mathbf{S}_{1,1} \leqslant \left\lfloor \sqrt{q - 2 + \frac{1}{4}} + \frac{1}{2} \right\rfloor_n$ where $\lfloor x \rfloor_n$ denotes the largest integer divisible by n which is less than or equal to x.

Corollary 1. *Suppose $n > 2$ is a positive integer such that $q - 1 = 2^n - 1$ is a (Mersenne) prime. Then, we have*

$$\mathbf{S}_{1,1} \leqslant C(\mathcal{G}_q) \leqslant \max\left\{ \left\lfloor \sqrt{\frac{q-2}{n} + \frac{1}{4}} + \frac{1}{2} \right\rfloor, \mathbf{S}_{1,1} \right\}.$$

Moreover,

$$\mathbf{S}_{1,1} \leqslant \left\lfloor \sqrt{q - 2 + \frac{1}{4}} + \frac{1}{2} \right\rfloor_n.$$

Proof. It follows from Lemma 1, Theorem 3 and Remark 4.

Remark 5. We denote $\max\left\{ \left\lfloor \sqrt{\frac{q-2}{n} + \frac{1}{4}} + \frac{1}{2} \right\rfloor, \mathbf{S}_{1,1} \right\}$ by Bound A, and $\left\lfloor \sqrt{q - 2 + \frac{1}{4}} + \frac{1}{2} \right\rfloor_n$ by Bound B.

Remark 6. In the appendix, we prove that Bound B is at worst recovers Gómez-Pérez and Winterhof's bound. Numerics suggest that although Bound B is only slightly better than that of Gómez-Pérez and Winterhof, Bound A gives a significant improvement.

Remark 7. Computation of $C(\mathcal{G}_q)$ for $n \geqslant 17$ is beyond our reach even with the help of Lemma 1. It would be interesting to tackle the first instance (if any) of n for which $\mathbf{S}_{1,1} \neq C(\mathcal{G}_q)$.

Table 1. Comparison of our bounds and that of Gómez-Pérez and Winterhof's in Case I.

n	$\mathbf{S}_{1,1}$	$C(\mathcal{G}_q)$	Bound A	Bound B	Gómez-Pérez and Winterhof's bound
3	3	3	3	3	3
5	5	5	5	5	6
7	7	7	7	7	12
13	13	13	25	91	91
17	51	*	88	357	363
19	57	*	166	722	725

2.5 Golomb Costas Arrays of Size $3^n - 2$ Where $(3^n - 1)/2$ Is a Prime

Throughout Sect. 2.5, let q be a power of 3 such that $(q-1)/2 = (3^n-1)/2$ is a prime, i.e. q is a strict safe prime power as defined in [6]. Such n is necessarily an odd prime and first few values for it are $3, 7, 13, 71$. Recall that $C(\mathcal{G}_q)$ is equal to

$$\max_{\substack{2\leqslant k\leqslant q-2\\ \gcd(k,q-1)=1}} \max_{\substack{c,d\in\mathbf{F}_q\\ c\neq 0}} |\{x \in \mathbf{F}_q \setminus \{0,1\} \mid x^k - cx - d = 0\}|.$$

Lemma 2. *Suppose $n \geqslant 3$ is a positive integer such that $(q-1)/2 = (3^n-1)/2$ is a prime. Then, we have*

$$C(\mathcal{G}_q) = \max_{\substack{2\leqslant k\leqslant q-2\\ \gcd(k,q-1)=1}} \max_{\substack{c,d\in\mathbf{F}_q\\ c\neq 0}} |\{x \in \mathbf{F}_q \setminus \{0,1\} \mid x^k - cx - d = 0\}| = \max_{\substack{2\leqslant k\leqslant q-2\\ \gcd(k,q-1)=1}} \max_{\substack{d\in\mathbf{F}_q^*\\ c\in\{1,-1\}}} |\{x \in \mathbf{F}_q \mid x^k - cx - d = 0\}|.$$

Proof. Note that the polynomials $x^k - cx - d$ and $(x/\alpha)^k - c/\alpha^{k-1}x/\alpha - d/\alpha^k$ have the same number of distinct zeroes where $\alpha \in \mathbf{F}_q^*$. Either c or $-c$ is a square in $\mathbf{F}_q$ and $\gcd(k-1, q-1) = 2$ so that

$$\alpha^{k-1} = c \text{ or}$$

$$\alpha^{k-1} = -c$$

has a zero in $\mathbf{F}_q$. Therefore, we may assume that $c \in \{1, -1\}$.
Let us now argue why 0 and 1 can be excluded: First note that polynomials $x^k - cx$ can be excluded from the list as we already know that $C(\mathcal{G}_q) \geqslant n \geqslant 3$. Moreover, 0 is not a zero of any $x^k - cx - d$ where $d \in \mathbf{F}_q^*$. Clearly, $1 \notin S_{1,d}$ where $d \in \mathbf{F}_q^*$ and even if $1 \in S_{-1,-1}$, we have $S_{-1,-1} = S_{-1,1}$ and $1 \notin S_{-1,1}$.

Remark 8. With the help of Lemma 2, we were able to compute that $C(\mathcal{G}_q) = 14$ for $n = 7$ using Magma [1] within minutes.

Theorem 4. *Suppose $n \geqslant 3$ is a positive integer such that $(q-1)/2 = (3^n-1)/2$ is a prime. Let $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ be the (permutation) polynomial defined by*

$f(x) = x^k$ where for some $2 \leqslant k \leqslant q-2$ and $gcd(k, q-1) = 1$. Then, $\nu_i(f) = 0$ for

$$i > \max\left\{\sqrt{\frac{q-3}{n} + \frac{1}{4}} + \frac{1}{2}, \mathbf{S}_{1,1}, \mathbf{S}_{-1,1}\right\}$$

where $\mathbf{S}_{u,v} = \max_{\substack{2 \leqslant k \leqslant q-2 \\ gcd(k,q-1)=1}} |S_{u,v}(x^k)|$ *and* $u, v \in \{1, -1\}$.

Proof. Consider the polynomial $f(x) - cx - d$. Note that $\mathbf{S}_{1,1} = \mathbf{S}_{1,-1}$ and $\mathbf{S}_{-1,1} = \mathbf{S}_{-1,-1}$, so by Lemma 2 we may assume $c \in \{1, -1\}$ and $d \in \mathbf{F}_q \setminus \mathbf{F}_p$. Now, we imitate the proof of Theorem 3 by first considering the map Φ from the set $(S_{c,d} \times S_{c,d}) \setminus \Delta$ to the graph $\{(y, z) \in \mathbf{F}_q^2 \mid D_1 f(y) = z \text{ and } y \neq 0, 1\}$ defined by $(x_1, x_2) \mapsto (x_1/(x_1 - x_2), (x_1 - x_2)^{1-k})$ where $D_1 f(x) = f(x+1) - f(x)$. Note that now we have $\gcd(1-k, q-1) = 2$, so the injectivity of Φ requires a new argument: Suppose $\Phi(\beta_1, \beta_2) = \Phi(\beta_3, \beta_4)$. This implies that $(\beta_2 - \beta_1)^{1-k} = (\beta_4 - \beta_3)^{1-k}$, i.e.,

$$\beta_4 - \beta_3 = \xi(\beta_2 - \beta_1)$$

for some $\xi \in \mathbf{F}_q$ such that $\xi^{1-k} = 1$. Since $\gcd(k-1, q-1) = 2$, we must have $\xi = \pm 1$.
Note that $\Phi(\beta_1, \beta_2) = \Phi(\beta_3, \beta_4)$ also forces that $\beta_3 = \xi\beta_1$. However, we have

$$\beta_3^k - c\beta_3 - d = (\xi\beta_1)^k - c\xi\beta_1 - d = \xi(\beta_1^k - c\beta_1) - d = 0$$

as $\xi^{1-k} = 1$. This implies that $d = \xi d$, so we must have $\xi = 1$. This implies that $(\beta_1, \beta_2) = (\beta_3, \beta_4)$ proving the injectivity.

Next, we consider the equivalence relation defined in Theorem 3:

$$(1, b) \sim (1, d)$$

if $b = \sigma^r(d)$ for some $0 \leqslant r < n$ where σ denotes the Frobenius automorphism. Note that we have $|S_{1,b}| = |S_{1,d}|$ for any $(1, b) \sim (1, d)$ and moreover these $S_{1,b}$'s are all pairwise disjoint. Note that Φ injectively extends to the domain $\bigsqcup_{(1,b)\sim(1,d)} ((S_{1,b} \times S_{1,b}) \setminus \Delta)$ because $-d$ cannot be a Galois conjugate of d as the extension degree of $\mathbf{F}_q$ over $\mathbf{F}_p$ is necessarily an odd prime. There are n such pairs $(1, b)$ since $d \in \mathbf{F}_q \setminus \mathbf{F}_p$ and n is prime. The target has cardinality $q-2$ and the domain has $n\ell(\ell-1)$ elements where ℓ is the number of distinct zeroes of the polynomial $f(x) - cx - d$. This implies that $n\ell(\ell-1) \leqslant \lfloor q-2 \rfloor_n = q-3$ so that

$$\ell \leqslant \sqrt{\frac{q-3}{n} + \frac{1}{4}} + \frac{1}{2}$$

and this finishes the proof.

Remark 9. Note that since $\mathbf{S}_{-1,1} = 1 \pmod n$ and $\mathbf{S}_{1,1}$ is divisible by n, the proof shows that $\mathbf{S}_{1,1} \leqslant \left\lfloor \sqrt{q - 3 + \frac{1}{4}} + \frac{1}{2} \right\rfloor_n$ and $\mathbf{S}_{-1,1} \leqslant \left\lfloor \sqrt{q - 3 + \frac{1}{4}} + \frac{1}{2} \right\rfloor_{n,1}$.
Here, $\lfloor x \rfloor_{n,1}$ denotes the maximum of the two integers that are not exceeding x and equal to 0 or 1 modulo n.

Corollary 2. *Suppose $n \geqslant 3$ is a positive integer such that $(q-1)/2 = (3^n-1)/2$ is prime. Then, we have*

$$\max\{\mathbf{S}_{1,1}, \mathbf{S}_{-1,1}\} \leqslant C(\mathcal{G}_q) \leqslant \max\left\{\left\lfloor \sqrt{\frac{q-3}{n} + \frac{1}{4}} + \frac{1}{2} \right\rfloor, \mathbf{S}_{1,1}, \mathbf{S}_{-1,1}\right\}.$$

Moreover,

$$\max\{\mathbf{S}_{1,1}, \mathbf{S}_{-1,1}\} \leqslant \left\lfloor \sqrt{q-3+\frac{1}{4}} + \frac{1}{2} \right\rfloor_{n,1}.$$

Proof. Immediate.

Remark 10. We call the expression $\max\left\{\left\lfloor \sqrt{\frac{q-3}{n} + \frac{1}{4}} + \frac{1}{2} \right\rfloor, \mathbf{S}_{1,1}, \mathbf{S}_{-1,1}\right\}$ Bound A, and $\left\lfloor \sqrt{q-3+\frac{1}{4}} + \frac{1}{2} \right\rfloor_{n,1}$ is called Bound B.

Remark 11. We prove in the appendix that Bound B is at worst recovers Gómez-Pérez and Winterhof's bound.

Table 2. Comparison of our bounds and that of Gómez-Pérez and Winterhof's in Case II(a).

n	$\mathbf{S}_{1,1}$	$\mathbf{S}_{-1,1}$	$C(\mathcal{G}_q)$	Bound A	Bound B	Gómez-Pérez and Winterhof's bound
3	3	4	4	4	4	5
7	14	8	14	18	43	47
13	*	*	*	*	1262	1263

Remark 12. Computation of $C(\mathcal{G}_q)$ for $n \geqslant 13$ is beyond our reach even with the help of Lemma 2. It would be interesting to tackle the first instance (if any) of n for which $\max\{\mathbf{S}_{1,1}, \mathbf{S}_{-1,1}\} \neq C(\mathcal{G}_q)$.

Remark 13. Using the idea in Theorem 3 and Theorem 4, one can obtain an analogue of Bound B for the subfamily $\mathcal{G}_p$ of Golomb Costas permutations and the family $\mathcal{W}_p$ of Welch Costas permutations where p is a safe prime. However, there is no analogue of Bound A in these cases due to the lack of nontrivial automorphisms.

3 Part II: Almost Difference Families Arising from $x^k - cx - d$

3.1 Planar Almost Difference Sets Arising from the Polynomials $x^k - cx^{p^i} - d$

Definition 4 *([3]). Let $(A, +)$ be an abelian group of order n. A subset of $D \subset A$ of cardinality w is an (n, w, λ, t) almost difference set in A if, for t times, the*

difference function diff: $A \setminus \{0\} \to \mathbf{Z}^{\geqslant 0}$ *takes the value* λ *and, for* $n-1-t$ *times, it takes the value* $\lambda+1$ *where*

$$\mathit{diff}(\alpha) = |(D+\alpha) \cap D|.$$

Notations 5. Let $\mathbf{F}_q$ be a finite field where $q \geqslant 4$ and for fixed $c, d \in \mathbf{F}_q^*$ and $0 \leqslant i < n$, consider the set $S_{i,c,d}(k) = \{x \in \mathbf{F}_q \,|\, x^k - cx^{p^i} - d = 0\}$. Let $2 \leqslant k \leqslant q-2$ be an integer such that $\ell := |S_{i,c,d}(k)| \geqslant 2$. For brevity, we write $S_{i,c,d}$ in place of $S_{i,c,d}(k)$ if k is clear from the context. Moreover, if $i = 0$, we write $S_{c,d}$ in place of $S_{0,c,d}$ (see Notation 2).

Lemma 3. *The map* $G : (S_{i,c,d} \times S_{i,c,d}) \setminus \Delta \to \mathbf{F}_q$ *defined by* $G(\beta_1, \beta_2) = \dfrac{\beta_1}{\beta_2}$ *is injective.*

Proof. Let us first consider the map $\Phi : (S_{i,c,d} \times S_{i,c,d}) \setminus \Delta \to \mathbf{F}_q^2$ defined by

$$\Phi(x_1, x_2) = \left(\frac{x_1}{x_1 - x_2}, c(x_1 - x_2)^{p^i - k} \right).$$

This map is injective: For if $\Phi(\beta_1, \beta_2) = \Phi(\beta_3, \beta_4)$, then

$$c(\beta_1 - \beta_2)^{p^i - k} = c(\beta_3 - \beta_4)^{p^i - k}$$

implies that $\beta_1 - \beta_2 = \xi(\beta_3 - \beta_4)$ for some $\xi \in \mathbf{F}_q$ such that $\xi^{p^i - k} = 1$. This implies that $\beta_1 = \xi\beta_3$, but then

$$\beta_1^k - c\beta_1^{p^i} - d = (\xi\beta_3)^k - c\xi^{p^i}\beta_3^{p^i} - d = \xi^{p^i}(\beta_3 - c\beta_3^{p^i}) - d = 0$$

as $\xi^{p^i - k} = 1$. This implies that $d = \xi^{p^i} d$, so $\xi^{p^i} = 1$ and we conclude that $\xi = 1$. Hence, $(\beta_1, \beta_2) = (\beta_3, \beta_4)$. Moreover, the image of Φ is contained(!) in the graph $\{(x, y) \in \mathbf{F}_q^2 \,|\, y = (x+1)^k - x^k\}$ (see the proof of Theorem 3 for how we construct Φ) so that the map $F := \pi_1 \circ \Phi$ is also injective where $\pi_1 : \mathbf{F}_q^2 \to \mathbf{F}_q$ is the first projection. Note that $1 \notin \mathrm{Im}(F)$, so we may consider the composition $r \circ F$ where $r : \mathbf{F}_q \setminus \{1\} \to \mathbf{F}_q$ is the rational map $r(x) = \dfrac{x}{x-1}$. Observe that the map $r \circ F$ is the map G given in the statement above. The injectivity of r implies that G is injective, and we are done.

Theorem 6. $S_{i,c,d}(k)$ *is a* $(q-1, \ell, 0, q-2-\ell(\ell-1))$ *almost difference set in the group* $\mathbf{F}_q^*$.

Proof. For simplicity, we denote $S_{i,c,d}$ by D. Let $a \in \mathrm{Im}(G)$ (so, $a \neq 1$), then there exist distinct elements $\beta_1, \beta_2 \in D$ such that $a = \beta_1/\beta_2$. I.e. $\beta_1 \in aD \cap D$ so that $\mathrm{diff}(a) \geqslant 1$. Let us now show that in fact $\mathrm{diff}(a) = 1$ in this case. Let $\beta_1, \beta_1' \in aD \cap D$, then there exist $\beta_2, \beta_2' \in D$ such that

$$\begin{aligned} \beta_1 &= a\beta_2 \\ \beta_1' &= a\beta_2', \end{aligned}$$

i.e., $\frac{\beta_1}{\beta_2} = \frac{\beta_1'}{\beta_2'}$. This implies that $G(\beta_1, \beta_2) = G(\beta_1', \beta_2')$, so by the injectivity of G, we conclude that $\beta_1 = \beta_2$. Thus, $\mathrm{diff}(a) = 1$.

Now, suppose $a \notin \mathrm{Im}(G)$ and $a \neq 1$. We claim that $aD \cap D = \emptyset$, for if $\beta_1 \in aD \cap D$, then there would exist $\beta_2 \in D$ (with $\beta_2 \neq \beta_1$ as $a \neq 1$) such that $a\beta_2 = \beta_1$. This contradicts with our assumption that $a \notin \mathrm{Im}(G)$. Hence, D is a $(q-1, \ell, 0, q-2-\ell(\ell-1))$ almost difference set of the group $\mathbf{F}_q^*$.

3.2 Almost Difference Families Arising from the Polynomials $x^k - cx - d$

Definition 5 *([5]). Let $\mathcal{F} = \{D_1, D_2, \ldots, D_m\}$ be a family of w-subsets of a finite abelian group G of cardinality n. For $1 \leqslant j \leqslant m$, let ΔD_j denote the multiset*

$$\{a - b \,|\, a, b \in D_j,\ a \neq b\}.$$

Let $\Delta\mathcal{F}$ denote the formal sum of ΔD_j's. $\mathcal{F}$ is called an (n, w, λ, t) almost difference family of size m if some t nonzero elements of G occur in the multiset $\Delta\mathcal{F}$ with multiplicity λ, and the remaining $n-1-t$ nonzero elements of G occur in $\Delta\mathcal{F}$ with multiplicity $\lambda+1$.

The setup of the next theorem is as follows:

Let $\mathbf{F}_q$ be a finite field. Let $c \in \mathbf{F}_q^*$, $d \in \mathbf{F}_q$ and $2 \leqslant k \leqslant q-2$ be an integer. Let $r := \gcd(k-1, q-1)$ and we denote the subgroup of $\mathbf{F}_q^*$ consisting elements of order dividing r by H_r. Note that there is a (faithful) group action

$$\begin{aligned} H_r \times \mathcal{M}_s(x^k, c) \setminus \{0\} &\to \mathcal{M}_s(x^k, c) \setminus \{0\} \\ (h, x) &\mapsto hx \end{aligned}$$

where $s := |S_{c,d}|$ by multiplication (see Definition 3).

Theorem 7. *Let R be a set of representatives of the orbit space $(\mathcal{M}_s(x^k, c) \setminus \{0\})/H_r$. Then, $\{S_{c,d}(k) \,|\, d \in R\}$ is an $(q-1, s, 0)$ almost difference family in $\mathbf{F}_q^*$ of size $\left\lfloor \frac{M_s(x^k,c)}{r} \right\rfloor$.*

The proof of this theorem will be given after Remark 15.

Remark 14. Note that if $x^k - cx$ has s distinct zeroes in $\mathbf{F}_q$, then $\left\lfloor \frac{M_s(x^k,c)}{r} \right\rfloor = \frac{M_s(x^k,c)-1}{r}$, and otherwise $\left\lfloor \frac{M_s(x^k,c)}{r} \right\rfloor = \frac{M_s(x^k,c)}{r}$.

Note that $M_q(x^q, 1) = q^{n-1}$ ([10, Proposition B.1]) in $\mathbf{F}_{q^n}$ and this gives us the next immediate corollary known as the generalized Bose-Chowla construction of OOCs.

Corollary 3 *(Generalized Bose-Chowla construction, [11]). There is an almost difference family in* $\mathbf{F}_{q^n}^*$ *with parameters* $(q^n-1, q, 0)$ *of size* $\frac{q^{n-1}-1}{q-1}$.

Proof. It immediately follows from Theorem 7 and the remark above.

Remark 15. Note that after choosing an isomorphism $\mathbf{F}_{q^n}^* \simeq \mathbf{Z}_{q^n-1}$, associated to the family in the corollary above, there is an optimal optical orthogonal code (OOC for short) with parameters $(q^n-1, q, 1)$ for every prime power q and an integer $n \geqslant 2$ (see Definition 6 below). One may more generally consider the zero set of the polynomials $x^q - cx$ where c is a nonzero $(q-1)^{\text{th}}$ power, i.e. $c = \alpha^{q-1}$ for some $\alpha \in \mathbf{F}_{q^n}^*$. However, in the case, the two codewords (of weight q) associated to the zero sets of $x^q - x - d$ (where $d \in R$ is fixed) and $x^q - cx - \alpha^q d$ are cyclic shifts of each other. Hence, two relevant optical orthogonal codes would be related to each other by an already-known operation of replacing any codeword by a cyclic shift of itself (see Remark 18 below).

Proof (Proof of Theorem 7). Let us first consider the map

$$\Phi : \bigsqcup_{d \in R} ((S_{c,d} \times S_{c,d}) \setminus \Delta) \to \mathbf{F}_q^2$$

defined by

$$\Phi(x_1, x_2) = \left(\frac{x_1}{x_1 - x_2}, c(x_1 - x_2)^{1-k} \right).$$

This map is injective: For if $\Phi(\beta_1, \beta_2) = \Phi(\beta_3, \beta_4)$ where $\beta_1, \beta_2 \in S_{c,d_1}$ and $\beta_3, \beta_4 \in S_{c,d_2}$, then we have $\beta_3 - \beta_4 = \xi(\beta_1 - \beta_2)$ for some $\xi \in \mathbf{F}_q$ such that $\xi^{1-k} = 1$. This implies that $\beta_3 = \xi\beta_1$ but note that

$$\beta_3^k - c\beta_3 - d_2 = \xi(\beta_1^k - c\beta_1) - d_2 = 0.$$

Therefore, $\xi d_1 = d_2$ and this forces that $\xi = 1$ since $d_1, d_2 \in R$, proving the injectivity of Φ.

The rest is identical to the arguments given in Lemma 3 and Theorem 6.

Remark 16. For r as above, let $C_0^{(r,q)}$ is the set of $r-$th powers in $\mathbf{F}_q^*$ and $C_i^{(r,q)} = \{\alpha^i x \,|, C_0^{(r,q)}\}$ where $\alpha \in \mathbf{F}_q$ is a fixed primitive element and $0 \leqslant i \leqslant r-1$. Note that the almost difference family in Theorem 7 can in fact be extended to the union $\bigcup_{i=1}^{r-1} \{S_{c_i,d}(k) \,|\, d \in R_i\}$ where $c_i \in C_i^{(r,q)}$ are fixed elements and R_i's are fixed sets of representatives of the orbit spaces $(\mathcal{M}_s(x^k, c_i) \setminus \{0\})/H_r$. In this way, the size of the extended family increases to $\left\lfloor \frac{\sum_{i=0}^{r-1} M_s(x^k, c_i)}{r} \right\rfloor$.

Remark 17. In [9], Kyureghyan-Li-Pott computed the multiplicity distribution of x^3 over arbitrary finite fields. Using their result and Remark 16 above one can isolate the prime powers q such that there exist $(q-1, 3, 1)$ optimal optical orthogonal codes arising from the zero sets of polynomials $x^3 - cx - d$. Note

however that the existence problem of optimal OOCs of weight 3 is already settled (see Theorem 5, [2]).

If the multiplicity distribution of x^4 is studied, this might lead to a partial progress towards the open problem of existence of optimal OOCs of weight 4 and it might even be possible to formulate a conjecture about an exhaustive list of lengths for which such OOCs exist. We expect that such a task boils down to cyclotomy but we do not tackle this problem here.

4 Part III: An Algorithm to Produce OOCs

Definition 6. *An optical orthogonal code (OOC for short) $\mathcal{C}$ with parameters (n, w, λ) is a collection of sequences consisting 0s and 1s of length n and weight w such that*
(i) $\sum_{i=0}^{n-1} \mathbf{c}_i \mathbf{c}_{i+j} \leqslant \lambda$ *for any* $\mathbf{c} \in \mathcal{C}$ *and* $j \not\equiv 0 \, (mod n)$, *and*
(ii) $\sum_{i=0}^{n-1} \mathbf{c}_i \mathbf{d}_{i+j} \leqslant \lambda$ *for any distinct* $\mathbf{c}, \mathbf{d} \in \mathcal{C}$.

Remark 18. For a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, let $T(\mathbf{c})$ denote the cyclic shift $(c_n, c_1, c_2, \ldots, c_{n-1})$. Then, for an optical orthogonal codes $\mathcal{C}$, the collection $(\mathcal{C} \setminus \{\mathbf{c}\}) \cup \{T^m(\mathbf{c})\}$ is an OOC as well for any $0 \leqslant m \leqslant n$. That is, we can replace any codeword with some cyclic shift of itself.

This section is motivated by the work [4] of Ding-Xing (though we do not use cyclotomy). Here is our algorithm:

Step 1: Fix a polynomial of the form $P(x) = x^{\ell_1} + c_{\ell_2} x^{\ell_2} + c_{\ell_2 - 1} x^{\ell_2 - 1} + \cdots + c_1 x \in \mathbf{F}_q[x]$ where c_1 and c_2 are nonzero (or more generally, where c_i and c_j are nonzero for some $1 \leqslant i < j \leqslant \ell_2$ so that $\gcd(\ell_1 - i, \ell_1 - j) = 1$).

Step 2: Fix an extension $\mathbf{F}_{q^n}^*$ of $\mathbf{F}_q$ and element $d \in \mathbf{F}_{q^n}^*$ such that $P(x) - d$ has ℓ zeroes $\mathbf{F}_{q^n}^*$ where $\ell > \ell_2$. (Note that one can always let d be any nonzero element of $\mathbf{F}_q$ and set $\mathbf{F}_{q^n}$ as the splitting field of $P(x) - d$.)

Step 3: Find all elements $d \in \mathbf{F}_{q^n}$ such that $P(x) - d$ has ℓ non-zero zeroes in $\mathbf{F}_{q^n}$.

Output: Associated to the family

$$\{\{x \in \mathbf{F}_{q^n}^* \mid P(x) - d = 0\} \mid d \text{ is nonzero and } P(x) - d \text{ has } \ell \text{ zeroes in } \mathbf{F}_{q^n}^*\}$$

of sets (of cardinality ℓ), we have optical orthogonal codes with parameters $(q^n - 1, \ell, \ell_2)$ whose supports are obtained by taking discrete logarithm with respect to some primitive element of $\mathbf{F}_{q^n}$.

This algorithm will be extended in a way that the size of the code is as large as possible (yet likely still non-optimal) but we first provide some examples by considering linearized polynomials:

Proposition 2. *For any integer $f \geqslant 1$, there exists an $(2^{21f}-1, 32, 2)$ optical orthogonal code with size $2^{21f-5}-1$.*

Proof. It has been checked with Magma that the additive polynomial $L(x) = x^{32} - x^2 - x$ splits over $\mathbf{F}_{2^{21}}$. For nonzero elements $d_1, d_2 \in \mathbf{F}_{2^{21f}}$, denote by $D_i \subset \mathbf{F}^*_{2^{21f}}$ the zero set of $x^{32} - x^2 - x - d_i$ in $\mathbf{F}_{2^{21f}}$ for $i = 1, 2$. Note that for nonzero $\alpha \in \mathbf{F}_{2^{21f}}$,

$$\begin{aligned} |\alpha^{-1}D_1 \cap D_2| &= \deg \gcd(\alpha^{32}x^{32} - \alpha^2 x^2 - \alpha x - d_1, x^{32} - x^2 - x - d_2) \\ &= \deg \gcd((\alpha^{32} - \alpha^2)x^2 + (\alpha^{32} - \alpha)x + \alpha^{32}d_2 - d_1, x^{32} - x^2 - x - d_2) \\ &\leqslant 2 \end{aligned}$$

since $(\alpha^{32} - \alpha^2)x^2 + (\alpha^{32} - \alpha)x + \alpha^{32}d_2 - d_1$ is a nonzero polynomial (of degree at most 2) where $d_1 = d_2$ and $\alpha \neq 1$, or $d_1 \neq d_2$.

Then, associated to the set of 32-subsets

$$\{\{x \in \mathbf{F}^*_{2^{21f}} \mid x^{32} - x^2 - x - d = 0\} \mid d \text{ is nonzero and in the image of } L : \mathbf{F}_{2^{21f}} \to \mathbf{F}_{2^{21f}}\},$$

we have an OOC with the desired properties.

Proposition 3. *For any integer $f \geqslant 1$, there exists an $(3^{13f}-1, 81, 3)$ optical orthogonal code with size $\frac{3^{13f-4}-1}{2}$.*

Proof. It has been checked with Magma that the $\mathbf{F}_3$-linear polynomial $L(x) = x^{81} + x^3 + x$ splits over $\mathbf{F}_{3^{13}}$. As for a nonzero element $\alpha \in \mathbf{F}^*_{3^{13f}}$, that $\alpha^{81} = \alpha^3$ and $\alpha^{81} = \alpha$ implies $\alpha^2 = 1$, therefore associated to the set of 81-subsets

$$\{\{x \in \mathbf{F}^*_{3^{13f}} \mid x^{81} + x^3 + x - d = 0\} \mid d \text{ is a non-square element in the image of } L : \mathbf{F}_{3^{13f}} \to \mathbf{F}_{3^{13f}}\},$$

we have an OOC with the desired properties.

We will now give an example that will motivate the next subsection:

Proposition 4. *For an integer $f \geqslant 1$, there exists an $(2^{14f}-1, w(f), 2)$ optical orthogonal code with size*

$$\begin{cases} 2 \cdot \left(\frac{2^{14f}}{w(f)} - 1\right) & \text{if } f \text{ is not divisible by 5,} \\ \frac{2^{14f}}{w(f)} - 1 & \text{if } f \text{ is divisible by 5} \end{cases}$$

where

$$w(f) = \begin{cases} 16 & \text{if } f \text{ is odd} \\ 32 & \text{if } f \text{ is even but not divisible by 4,} \\ 64 & \text{if } f \text{ is divisible by 4.} \end{cases}$$

Proof. Let $\theta \in \mathbf{F}_{2^{14}}$ be a primitive third root of unity. It has been checked with Magma that the additive polynomial $L_\theta(x) = x^{64} - x^2 - \theta x$ factorizes over $\mathbf{F}_{2^{14}}$ as a product of 16 linear factors, 8 quadratic factors and 8 quartic factors (so does $L_{\theta^2}(x) = x^{64} - x^2 - \theta^2 x$).

If f is not divisible by 5, then 62 is coprime to $2^{14f} - 1$ and associated to the union of the set of $w(f)$-subsets

$$\{\{x \in \mathbf{F}^*_{2^{14f}} \mid x^{64} - x^2 - \theta x - d = 0\} \mid d \text{ is nonzero and in the image of } L_\theta : \mathbf{F}_{2^{14f}} \to \mathbf{F}_{2^{14f}}\}$$

with the set of $w(f)$-subsets

$$\{\{x \in \mathbf{F}^*_{2^{14f}} \mid x^{64} - x^2 - \theta^2 x - d = 0\} \mid d \text{ is nonzero and in the image of } L_{\theta^2} : \mathbf{F}_{2^{14f}} \to \mathbf{F}_{2^{14f}}\}$$

we have an OOC with the desired properties. In case f is divisible by 5, only one of these sets yields an OOC (and has the desired properties).

4.1 Algorithm Continued: How to Extend the Size of the OOC

Note that the algorithm in the previous section does not guarantee that the OOC produced will be optimal, so it is important to extend the algorithm in a way that we get as many codes as possible as an output. Here are the remaining steps of the algorithm:

Step 4: Set $S = \{P(x)\}$ and W be the complement of S in the set of polynomials in $\mathbf{F}_q$ which are of the form specified in Step 1.
Step 5: Let $Q(x) = x^{\ell_1} + c_{\ell_2} x^{\ell_2} + c_{\ell_2 - 1} x^{\ell_2 - 1} + \cdots + c_1 x$ be in W. If
(i) $Q(x) - e\mathbf{F}_{q^n}$ has ℓ zeroes in $\mathbf{F}^*_{q^n}$ for any $e \in \mathbf{F}^*_{q^n}$, and
(ii) $Q(x) \neq \alpha^{-\ell_1} P(\alpha x)$ for any $\alpha \in \mathbf{F}^*_{q^n}$ and any $P(x) \in S$,
then add $Q(x)$ to the list S.
Step 6: Remove $Q(x)$ from the set W and return Step 5 until S stabilizes.
Output: Associated to the family

$$\{\{x \in \mathbf{F}^*_{q^n} \mid P(x) - d = 0\} \mid P(x) \in S, d \text{ is nonzero and } P(x) - d \text{ has } \ell \text{ zeroes in } \mathbf{F}^*_{q^n}\}$$

of sets (of cardinality ℓ), we have optical orthogonal codes with parameters $(q^n - 1, \ell, \ell_2)$ whose supports are obtained by taking discrete logarithm with respect to some primitive element of $\mathbf{F}_{q^n}$.

The proofs of the propositions in previous subsection illustrate the idea behind our algorithm. Nevertheless, we provide an argument to show that the algorithm works:

(Proof of the validity of the algorithm:) Note that by Step 2 and Step 5, the family

$$\{\{x \in \mathbf{F}^*_{q^n} \mid P(x) - d = 0\} \mid P(x) \in S, d \text{ is nonzero and } P(x) - d \text{ has } \ell \text{ zeroes in } \mathbf{F}^*_{q^n}\}$$

contains only subsets of cardinality ℓ. Let $D_1 = \{x \in \mathbf{F}_{q^n}^* \mid P(x) - d_1 = 0\}$ and $D_2 = \{x \in \mathbf{F}_{q^n}^* \mid Q(x) - d_2 = 0\}$ and $\alpha \in \mathbf{F}_{q^n}^*$, then

$$\begin{aligned}|\alpha^{-1}D_1 \cap D_2| &= \deg \gcd(P(\alpha x) - d_1, Q(x) - d_2) \\ &= \deg \gcd(Q(x) - \alpha^{-\ell_1}P(\alpha x) + d_2 - \alpha^{-\ell_1}d_1, Q(x) - d_2)\end{aligned}$$

If $P(x) = Q(x)$ and $d_1 \neq d_2$, the polynomial $Q(x) - \alpha^{-\ell_1}P(\alpha x) + d_2 - \alpha^{-\ell_1}d_1$ is a nonzero polynomial of degree at most ℓ_2 by Step 1. If $P(x) \neq Q(x)$, then $Q(x) - \alpha^{-\ell_1}P(\alpha x) + d_2 - \alpha^{-\ell_1}d_1$ is a nonzero polynomial of degree at most ℓ_2 by Step 5.

We end by providing examples of OOCs arising from non-additive polynomials.

Example 1. Associated to the family

$$\{\{x \in \mathbf{F}_{3^7}^* \mid x^{59} - x^2 - cx - d = 0\} \mid d \text{ is nonzero and } x^{59} - x^2 - cx - d \text{ has at least 5 zeroes in } \mathbf{F}_{3^7}^*\},$$

we have a variable-weight OOC with parameters $(2186, \{5, 6, 7, 8, 9\}, 2)$ of size 17143 (14329 of them have weight 5). Note that the assumption in Step 5 of our algorithm is satisfied as $\gcd(57, 2186) = 1$.

Example 2. Associated to the family

$$\{\{x \in \mathbf{F}_{2^{111}}^* \mid x^{59} - x^2 - cx - d = 0\} \mid d \text{ is nonzero and } x^{59} - x^2 - cx - d \text{ has at least 5 zeroes in } \mathbf{F}_{2^{111}}^*\},$$

we have a variable-weight OOC with parameters $(2110, \{5, 6, 7, 8, 9\}, 2)$ of size 16263 (13600 of them have weight 5).

Acknowledgement. We would like to thank the anonymous referees for their valuable suggestions and comments.

A Appendix

Proposition 5. *Bound B recovers Gómez-Pérez and Winterhof's bound when $q = 2^n$ and $q - 1$ is a prime for $n \geqslant 3$.*

Proof. For $n = 3$, we have an equality (see Table 1), so may assume $n \geqslant 5$. Then, we have

$$\begin{aligned}\left(1 - \frac{1}{q-1}\right)(1 + \sqrt{q}) - \left(\frac{1}{2} + \sqrt{q - \frac{7}{4}}\right) &= \frac{1}{2} - \frac{1}{q-1} + \sqrt{q} - \frac{\sqrt{q}}{q-1} - \sqrt{q - \frac{7}{4}} \\ &\geqslant \frac{1}{2} - \frac{1}{q-1} - \frac{\sqrt{q}}{q-1}\end{aligned}$$

Note also that

$$\left(\frac{1}{2}-\frac{1}{q-1}\right)^2-\left(\frac{\sqrt{q}}{q-1}\right)^2 \geqslant \frac{1}{4}-\frac{1}{q-1}+\frac{1}{(q-1)^2}-\frac{q}{(q-1)^2}$$
$$\geqslant \frac{q^2-10q+9}{4(q-1)^2}.$$

As $q \geqslant 32$, we have $q^2-10q+9 \geqslant 0$. Hence, $\left\lfloor \frac{1}{2}+\sqrt{q-\frac{7}{4}} \right\rfloor_n \leqslant \left\lfloor \left(1-\frac{1}{q-1}\right)(1+\sqrt{q}) \right\rfloor$.

Proposition 6. *Bound B recovers Gómez-Pérez and Winterhof's bound when* $q=3^n$ *and* $(q-1)/2$ *is a prime.*

Proof. Assume the hypothesis on q. Then, we have

$$\begin{aligned}
&\left(1+\left(1-\frac{2}{q-1}\right)\sqrt{q}\right)^2-\left(\sqrt{q-3+\frac{1}{4}}+\frac{1}{2}\right)^2\\
&=\left(1+2\sqrt{q}\frac{q-3}{q-1}+\left(1-\frac{4}{q-1}+\frac{4}{(q-1)^2}\right)q\right)-\left(q-3+\frac{1}{4}+\sqrt{q-3+\frac{1}{4}}+\frac{1}{4}\right)\\
&=\left(1+q-\frac{4q}{q-1}+\frac{4q}{(q-1)^2}+2\sqrt{q}\frac{q-3}{q-1}\right)-\left(-\frac{5}{2}+q+\sqrt{q-\frac{11}{4}}\right)\\
&=-\frac{1}{2}+\frac{4}{q-1}+\frac{4q}{(q-1)^2}+\sqrt{q}\left(\frac{2(q-3)}{q-1}-\sqrt{1-\frac{11}{4q}}\right)\\
&\geqslant -\frac{1}{2}+\sqrt{q}\left(1-\frac{4}{q-1}\right)\\
&\geqslant -\frac{1}{2}+\frac{\sqrt{q}}{2}
\end{aligned}$$

Hence, $\left\lfloor \sqrt{q-3+\frac{1}{4}}+\frac{1}{2} \right\rfloor_{n,1} \leqslant \left\lfloor 1+\left(1-\frac{2}{q-1}\right)\sqrt{q} \right\rfloor = 1+\left\lfloor \left(1-\frac{2}{q-1}\right)\sqrt{q} \right\rfloor$.

References

1. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3-4), 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125, http://dx.doi.org/10.1006/jsco.1996.0125. computational algebra and number theory (London, 1993)
2. Chung, F., Salehi, J., Wei, V.: Optical orthogonal codes: design, analysis and applications. IEEE Trans. Inf. Theory **35**(3), 595–604 (1989). https://doi.org/10.1109/18.30982
3. Ding, C., Feng, T.: Codebooks from almost difference sets. Des. Codes Cryptogr. **46**(1), 113–126 (2008)
4. Ding, C., Xing, C.: Several classes of (2m–1, w, 2) optical orthogonal codes. Discret. Appl. Math. **128**, 103–120 (2003)

5. Ding, C., Yin, J.: Constructions of almost difference families. Discret. Math. **308**(21), 4941–4954 (2008). https://doi.org/10.1016/j.disc.2007.09.017, https://www.sciencedirect.com/science/article/pii/S0012365X07007418. chongqing 2004
6. Drakakis, K., Gow, R., Rickard, S., Sheekey, J., Taylor, K.: On the maximal cross-correlation of algebraically constructed costas arrays. IEEE Trans. Inf. Theory **57**, 4612–4621 (2011). https://doi.org/10.1109/TIT.2011.2145890
7. Freedman, A., Levanon, N.: Any two n × n costas signals must have at least one common ambiguity sidelobe if n gt; 3-a proof. Proc. IEEE **73**(10), 1530–1531 (1985). https://doi.org/10.1109/PROC.1985.13329
8. Gómez-Pérez, D., Winterhof, A.: A note on the cross-correlation of costas permutations. IEEE Trans. Inf. Theory **66**(12), 7724–7727 (2020). https://doi.org/10.1109/TIT.2020.3009880
9. Kyureghyan, G., Li, S., Pott, A.: On the intersection distribution of degree three polynomials and related topics (2020). https://doi.org/10.48550/ARXIV.2003.10040, https://arxiv.org/abs/2003.10040
10. Li, S., Pott, A.: Intersection distribution, non-hitting index and Kakeya sets in affine planes. Finite Fields Their Appl. **66**, 101691 (2020). https://doi.org/10.1016/j.ffa.2020.101691, https://doi.org/10.1016/j.ffa.2020.101691
11. Moreno, O., Omrani, R., Kumar, P.V., Lu, H.F.: A generalized bose-chowla family of optical orthogonal codes and distinct difference sets. IEEE Trans. Inf. Theory **53**(5), 1907–1910 (2007). https://doi.org/10.1109/TIT.2007.894658