*Biometrical Letters*
*Vol. 46 (2009), No. 2, 89-102*

# Optimal Optical Orthogonal Signature Pattern Codes of Weight 3

**Masanori Sawa**[1], **Sanpei Kageyama**[2]

[1]Nagoya University, Graduate School of Information Science, Nagoya 464-8601, Japan,
e-mail: sawa@is.nagoya-u.ac.jp
[2]Hiroshima Institute of Technology, Department of Environmental Design,
Hiroshima 731-5193, Japan, e-mail: s.kageyama.4b@it-hiroshima.ac.jp

Dedicated to Professor Tadeusz Caliński for his 80th birthday

## Summary

The purpose of this paper is to investigate the existence of optical orthogonal signature pattern codes (OOSPCs) of weight 3 and cross-correlation constraint 1 and to discuss what is optimal for such OOSPCs. First we focus on OOSPCs of auto-correlation constraint 1, where the optimality is decided by the classical upper bound for the number of codewords in an OOSPC, as presented by Kitayama (1994). We provide two constructions – one is a direct construction using certain combinatorial objects, called Skolem sequences, and the other is a recursive construction. Using these constructions, for any odd integers $m, n$ such that either $m$ or $n$ is not congruent to 5 modulo 6, we obtain an optimal OOSPC of size $m \times n$ which attains the Kitayama bound. Next we focus on OOSPCs of auto-correlation constraint 2. We prove that the number of codewords in such an OOSPC of size $m \times n$ is bounded above by $mn/4$ or $\lfloor (mn-1)/4 \rfloor$ OOSPs, according as $mn$ is divisible by 4 or not. This new bound represents a significant improvement on the Kitayama bound. Finally we construct many optimal OOSPCs which attain the new bound, by presenting two new algebraic constructions.

**Key words:** optical orthogonal signature pattern code (OOSPC), packing design, Kitayama bound (Kwong-Yang bound).

## 1. Introduction

Kitayama (1994) proposed a novel type of optical code-division multiple-access (CDMA), called a space CDMA, for the parallel transmission of 2-dimensional images through multicore fibers. In a space CDMA each pixel in a 2-dimensional image is encoded into a signature address, called an optical orthogonal signature pattern (OOSP). All the encoded images are multiplexed and broadcast to all receivers. Then each receiver regenerates the intended data from the multiplexed signals using its own OOSP. We refer the reader to Hassan et al. (1995), Hui (1985), Kwong and Yang (2001) and Park et al. (1992) for more information about spatial optical CDMA networks using multicore fibers.

Let $m, n, k, \lambda_a, \lambda_c$ be positive integers with $mn > k > \lambda_a \geqslant \lambda_c$. An *optical orthogonal signature pattern code*, denoted by an $(m, n, k, \lambda_a, \lambda_c)$-OOSPC, is a family $\mathcal{C}$ of binary $(0, 1)$-matrices $(x_{i,j})$ of size $m \times n$ which satisfies the following correlation properties:

(i) (auto-correlation property)

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} x_{i \oplus p, j \hat{\oplus} q} \begin{cases} = k & \text{if } p = q = 0, \\ \leqslant \lambda_a & \text{otherwise} \end{cases}$$

for any matrix $(x_{i,j}) \in \mathcal{C}$;

(ii) (cross-correlation property)

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} y_{i \oplus p, j \hat{\oplus} q} \leqslant \lambda_c$$

for any distinct matrices $(x_{i,j}), (y_{i,j}) \in \mathcal{C}$,

where the additions $\oplus, \hat{\oplus}$ are reduced modulo $m, n$ respectively. The value $k$ is called a *weight* and $\lambda_a, \lambda_c$ are respectively called *auto-* and *cross-correlation constraints*. The OOSPCs form a special class of 2-dimensional optical orthogonal codes; see Omrani and Kumer (2006).

Throughout this paper we restrict our attention to the case where $\lambda_c = 1$, from a practical point of view. A challenging problem is to determine the largest possible cardinality $\phi(m, n, k, \lambda_a, 1)$ of an $(m, n, k, \lambda_a, 1)$-OOSPC for given $m, n, k, \lambda_a$. An $(m, n, k, \lambda_a, 1)$-OOSPC is said to be *optimal*

if $\phi(m,n,k,\lambda_a,1)$ is attained. The following upper bound for $\phi(m,n,k,\lambda_a,1)$ was given independently by Kitayama (1994) and Kwong and Yang (1996).

$$\phi(m,n,k,\lambda_a,1) \leqslant \left\lfloor \frac{\lambda_a(mn-1)}{k(k-1)} \right\rfloor =: J(m,n,k,\lambda_a,1). \tag{1}$$

An improvement of (1) was also derived by Kwong and Yang (2001).

When $m$ and $n$ are relatively prime, the existence of an optimal $(m,n,k,\lambda_a,1)$-OOSPC is just equivalent to that of an optimal $(mn,k,\lambda_a,1)$ optical orthogonal codes (OOCs); see Construction I of Kwong and Yang (1996). Thus in this case we can obtain a large number of optimal OOSPCs, in conjunction with the known results on optimal OOCs; for example, see Chung and Kumer (1990), Chung et al. (1989), Fuji-Hara and Miao (2000), Fuji-Hara et al. (2001) and Moreno et al. (1995). However, when $m$ and $n$ are not relatively prime, the problem of finding OOSPCs cannot be reduced to that of finding OOCs. In this case some families of optimal OOSPCs have been found for prime numbers $m\ (=n)$; see Kwong and Yang (1996). To the authors' knowledge, little is known regarding the existence or the construction of optimal OOSPCs for values of $m$ and $n$ in general, even for the case where $k=3$, being the minimal nontrivial case on $k$. Note that an $(m,n,2,1,1)$-OOSPC which attains (1) can be constructed in a trivial manner.

The purpose of this paper is to investigate the existence of OOSPCs of weight 3 and to discuss what is optimal for such OOSPCs, by observing a relationship between OOSPCs and combinatorial designs. The relationship is shown in Section 2. Essentially there are two cases to be considered, that is, $\lambda_a=\lambda_c=1$, or $\lambda_a=2$ and $\lambda_c=1$. Section 3 is devoted to the former case, where (1) is used to decide the optimality of OOSPCs. We present two constructions of optimal $(m,n,3,1,1)$-OOSPCs; one is a direct construction using Skolem sequences, and the other is a recursive construction. By combining these constructions, for any odd integers $m,n$ such that $m \not\equiv 5 \pmod 6$ or $n \not\equiv 5 \pmod 6$, an optimal $(m,n,3,1,1)$-OOSPC can be obtained. Section 4 is devoted to the case where $\lambda_a=2$ and $\lambda_c=1$. We show that the cardinality of an $(m,n,3,2,1)$-OOSPC is bounded from above by $mn/4$ or $\lfloor (mn-1)/4 \rfloor$, according as $mn$ is divisible by 4 or not. This new bound represents a significant improvement on the Kitayama bound (or the Kwong-Yang bound) and hence it may be seen that the Kitayama bound cannot be used in determining the optimality of OOSPCs of $\lambda_a=2$, unlike in the case where $\lambda_a=1$. Recall that there

exist many optimal OOSPCs of $\lambda_a = 1$ which attain (1). Finally we show the validity of the new bound by constructing many $(m, n, 3, 2, 1)$-OOSPCs optimal with respect to the bound through two new algebraic constructions.

## 2. OOSPCs and combinatorial designs

In this section we will mention a relationship between OOSPCs and combinatorial designs.

Let $k, v$ be positive integers such that $2 < k < v$. A 2-$(v, k, 1)$ *packing design* is a system $\mathcal{D}$ of $v$ points $V$ and those $k$-subsets $\mathcal{B}$, called blocks, such that every pair of points occurs in at most one block. In particular $\mathcal{D}$ is called a *balanced incomplete block* (BIB) *design* if "at most" in the packing design definition is replaced by "exactly". In fact, Yates (1936) first proposed the use of BIB designs in agricultural experiments. Since then, many researchers in statistics as well as in combinatorics have studied packing designs and more general combinatorial designs. The theory of combinatorial designs has been recently applied to many fields such as quantum mechanics (see Beth et al., 2003), optics (see Harwit and Sloane, 1979), and bioinformatics (see Mutoh et al., 2003).

We explain some notations and terminologies from design theory; see Beth et al. (1993). Let $\binom{A}{k}$ be a set of all $k$-subsets of an abelian group $A$. Let $B = \{b_0, \cdots, b_{k-1}\} \in \binom{A}{k}$. The *stabilizer of* $B$ *under* $A$ is a subgroup of $A$ consisting of all elements $a \in A$ such that $B+a = B$, where $B+a = \{b_0+a, \cdots, b_{k-1}+a\}$. The $A$-*orbit of* $B$ is the set $\mathrm{Orb}_A(B) = \{B + a \mid a \in A\}$. An *automorphism of* $\mathcal{D}$ is a permutation $\xi$ on $V$ such that $B^\xi \in \mathcal{B}$ for each $B \in \mathcal{B}$. A system $\mathcal{D}$ is said to be $A$-*invariant* if it admits $A$ as a point-regular automorphism group. In particular a $\mathbb{Z}_v$-invariant packing design is called *cyclic*. $\mathcal{D}$ is further said to be *strictly* $A$-*invariant* if it is $A$-invariant and the stabilizer of any block in $\mathcal{D}$ under $A$ equals the identity.

Now, observe that a set of all ordered pairs of subscripts $(i, j)$ in an OOSP $(x_{i,j})$ forms the group $\mathbb{Z}_m \times \mathbb{Z}_n$, where $\mathbb{Z}_l$ is a set of residue classes modulo $l$. There is a natural one-to-one correspondence between an OOSP $(x_{i,j})$ and a subset $X$ of $\mathbb{Z}_m \times \mathbb{Z}_n$;

$$x_{i,j} = \begin{cases} 1 & \text{if } (i, j) \in X, \\ 0 & \text{otherwise.} \end{cases}$$

Thus an $(m, n, k, \lambda_a, \lambda_c)$-OOSPC can be identified with a family $\mathcal{C}$ of $k$-subsets of $Z_m \times \mathbb{Z}_n$ which satisfies the conditions:

(i) (auto-correlation property)

$$|X \cap (X + (i,j))| \begin{cases} = k & \text{if } (i,j) = (0,0), \\ \leqslant \lambda_a & \text{otherwise} \end{cases} \tag{2}$$

for any $X \in \mathcal{C}$, and

(ii) (cross-correlation property)

$$|X \cap (Y + (i,j))| \leqslant \lambda_c \tag{3}$$

for any distinct $X, Y \in \mathcal{C}$.

Hereafter let $A = \mathbb{Z}_m \times \mathbb{Z}_n$ and $X \in \binom{A}{k}$. Let $\Delta X$ be the multiset defined by

$$\Delta X = \{a - b \mid a, b \in X,\ a \neq b\}$$

and $m_a(\Delta X)$ be the multiplicity of $a$ in $\Delta X$. Then it is obvious that

$$\max_{a \in A \setminus \{0\}} |X \cap (X + a)| = \max_{a \in \Delta X} m_a(\Delta X). \tag{4}$$

**Proposition 2.1.** An $(m, n, k, \lambda_a, 1)$-OOSPC is a subset $\mathcal{C}$ of $\binom{\mathbb{Z}_m \times \mathbb{Z}_n}{k}$ such that

(i) $\max_{a \in \Delta X} m_a(\Delta X) \leqslant \lambda_a$ for any $X \in \mathcal{C}$,

(ii) $\Delta X \cap \Delta Y = \emptyset$ for any distinct $X, Y \in \mathcal{C}$.

In particular an $(m, n, k, 1, 1)$-OOSPC is itself a strictly $(\mathbb{Z}_m \times \mathbb{Z}_n)$-invariant 2-$(mn, k, 1)$ packing design.

**Proof.** (i) follows from (2) and (4), whereas (ii) follows from (3), since $\lambda_c = 1$. □

## 3. Correlation $\lambda_a = \lambda_c = 1$

In this section the following theorem will be proved.

**Theorem 3.1.** Let $m, n$ be odd integers such that $m \not\equiv 5 \pmod 6$ or $n \not\equiv 5 \pmod 6$. Then there exists an optimal $(m, n, 3, 1, 1)$-OOSPC which attains (1).

In order to show Theorem 3.1, we need some observations. The *Skolem sequence of order* $f$ is a sequence $S = (s_1, \cdots, s_{2f})$ of $2f$ integers which satisfies the conditions that

(i) for every $k = 1, \cdots, f$, there exist exactly two elements $s_i, s_j \in S$ such that $s_i = s_j = k$, and

(ii) if $s_i = s_j = k$ with $i < j$, then $j - i = k$.

A *hooked Skolem sequence of order* $f$ is a sequence $S = (s_1, \cdots, s_{2f+1})$ of $2f+1$ integers satisfying the above conditions (i) and (ii), and the additional condition that

(iii) there exists exactly one $s_i \in S$ such that $s_i = 0$.

It is well known (see O'Keefe, 1961, Skolem, 1957) that the Skolem sequence of order $n$ exists if and only if $n \equiv 0, 1 \pmod 4$, and a hooked Skolem sequence of order $n$ exists if and only if $n \equiv 2, 3 \pmod 4$.

**Lemma 3.1.** For any positive integer $n$, there exists an optimal $(3, n, 3, 1, 1)$-OOSPC which attains (1).

**Proof.** The proof will be made by considering three cases:

Case 1 $n \equiv 1 \pmod 2$:

This case is well known; see for example Anderson (1997).

Case 2 $n \equiv 2, 4 \pmod 8$:

Let $S = (s_1, \cdots, s_{n-2})$ be the Skolem sequence of order $(n-2)/2$. We identify $S$ with a collection of ordered pairs $\tilde{S} = \{(a_i, b_i) \mid b_i - a_i = i,\ i = 1, \cdots, (n-2)/2\}$ with $\bigcup_{i=1}^{(n-2)/2} \{a_i, b_i\} = \{1, \cdots, n-2\}$. Then Proposition 2.1 can be used to show that the set

$$\{\{(0,0), (1,a_i), (1,b_i)\} \mid (a_i, b_i) \in \tilde{S}\}$$

is a $(3, n, 3, 1, 1)$-OOSPC. Hence the cardinality of the OOSPC equals $(n-2)/2 = J(3, n, 3, 1, 1)$.

Case 3 $n \equiv 0, 6 \pmod 8$:

In the proof of Case 2, replace "Skolem sequence of order $(n-2)/2$" by "hooked Skolem sequence of order $(n-2)/2$".

Thus we obtain the result. □

**Example 3.1.** (i) Since $(1, 1, 3, 4, 2, 3, 2, 4)$ is the Skolem sequence of order 4, Lemma 3.1 yields the following optimal $(3, 8, 3, 1, 1)$-OOSPC which attains (1):

$$\{(0,0), (1,1), (1,2)\},\ \{(0,0), (1,5), (1,7)\},$$
$$\{(0,0), (1,3), (1,6)\},\ \{(0,0), (1,4), (1,8)\}.$$

(ii) Since $(3,1,1,3,2,0,2)$ is a hooked Skolem sequence of order 3, Lemma 3.1 yields the following optimal $(3,7,3,1,1)$-OOSPC which attains (1):

$$\{(0,0),(1,2),(1,3)\},\ \{(0,0),(1,5),(1,7)\},\ \{(0,0),(1,1),(1,4)\}.$$

**Remark 3.1.** In the case that $n$ is divisible by 3, the optimal $(3,n,3,1,1)$-OOSPC constructed by Lemma 3.1 cannot be obtained through Construction I of Kwong and Yang (1996).

For a divisor $m'$ of $m$, we denote by $(\frac{m}{m'})\mathbb{Z}_m$ the subgroup of $\mathbb{Z}_m$ of order $m'$. An $(m,n,k,1,1)$-OOSPC, say $\mathcal{C}$, is said to be $((\frac{m}{m'})\mathbb{Z}_m \times \mathbb{Z}_n)$-*regular* if it satisfies the condition

$$\bigcup_{X\in\mathcal{C}} \Delta X = (\mathbb{Z}_m \times \mathbb{Z}_n) \setminus \left(\left(\frac{m}{m'}\right)\mathbb{Z}_m \times \mathbb{Z}_n\right).$$

A $k \times n$ matrix $D = (d_{ij})$ with entries from $\mathbb{Z}_n$ is called an $(n,k)$-*cyclic difference matrix* (CDM) if, for distinct $i, j = 0, \cdots, k-1$, the set

$$\{d_{i\ell} - d_{j\ell} \mid \ell = 0, \cdots, n-1\}$$

contains every element of $\mathbb{Z}_n$ exactly once; see Colbourn and Dinitz (2007).

**Lemma 3.2.** Let $m, n$ be positive integers and $m'$ be a divisor of $m$. Assume that there exist an $(m',n,k,1,1)$-OOSPC with $l$ OOSPs, an $((\frac{m}{m'})\mathbb{Z}_m \times \mathbb{Z}_1)$-regular $(m,1,k,1,1)$-OOSPC and an $(n,k)$-CDM. Then there exists an $(m,n,k,1,1)$-OOSPC with $n\lfloor\frac{m-m'}{k(k-1)}\rfloor + l$ OOSPs, where $\lfloor\cdot\rfloor$ denotes the Gauss symbol.

**Proof.** Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be an $((\frac{m}{m'})\mathbb{Z}_m \times \mathbb{Z}_1)$-regular $(m,1,k,1,1)$-OOSPC and an $(m',n,k,1,1)$-OOSPC, respectively. Let $D = (d_{ij})$ be an $(n,k)$-CDM. For each $B = \{(b_0,0), \cdots, (b_{k-1},0)\} \in \mathcal{C}_1$, take a collection $\mathcal{C}(B)$ of elements of $\binom{\mathbb{Z}_m \times \mathbb{Z}_n}{k}$ such that

$$\mathcal{C}(B) = \{\{(b_0,d_{0,j}), \cdots, (b_{k-1},d_{k-1,j})\} \mid j = 0, \cdots, n-1\}.$$

Then by Proposition 2.1, the set

$$\mathcal{C} = \bigcup_{B\in\mathcal{C}_1} \mathcal{C}(B)$$

forms an $(m,n,k,1,1)$-OOSPC such that

$$\Delta\mathcal{C} \cap \left(\left(\frac{m}{m'}\right)\mathbb{Z}_m \times \mathbb{Z}_n\right) = \emptyset. \tag{5}$$

Thus, by embedding each $m' \times n$ OOSP in $\mathcal{C}_2$ into an $m \times n$ OOSPC as its $m' \times n$ sub-OOSP with $(\frac{m}{m'})$th, $(\frac{2m}{m'})$th, $\cdots$, $m$th rows of the $m \times n$ OOSPC, we can take $\mathcal{C} \cup \mathcal{C}_2$ as an $(m, n, k, 1, 1)$-OOSPC. It remains to compute the cardinality of the resulting OOSPC. Evidently, an $(n, k)$-CDM consists of $n$ columns and an $((\frac{m}{m'})\mathbb{Z}_m \times \mathbb{Z}_1)$-regular $(m, 1, k, 1, 1)$-OOSPC consists of $\lfloor \frac{m-m'}{k(k-1)} \rfloor$ OOSPs. Hence it follows from (5) that

$$|\mathcal{C} \cup \mathcal{C}_2| = |\mathcal{C}| + |\mathcal{C}_2| = n \left\lfloor \frac{m - m'}{k(k-1)} \right\rfloor + l. \qquad \square$$

We are now in a position to prove Theorem 3.1.

**Proof of Theorem 3.1.** Let $D = (d_{ij})$ be a $3 \times n$ matrix with entries from $\mathbb{Z}_n$ defined by $d_{ij} = ij$. Then $D$ is a $(3, n)$-CDM, since 2 is an invertible element in $\mathbb{Z}_n$. Hence the result follows from Lemmas 3.1 and 3.2. $\square$

It is well known that for any odd prime power $p^n \equiv 1 \pmod 6$, there exists a $\mathbb{Z}_p^n$-invariant 2-$(p^n, 3, 1)$ packing design which attains (1); for example, see Colbourn and Dinitz (2007). In particular this fact shows the existence of an optimal $(p, p, 3, 1, 1)$-OOSPC attaining (1) for $p \equiv 5 \pmod 6$. It remains unsolved whether or not Theorem 3.1 is valid for $m, n$ being congruent to 5 modulo 6 in general. We conclude this section by proposing a general open problem.

**Problem 3.1.** Does there exist an optimal $(m, n, 3, 1, 1)$-OOSPC which attains (1) for all positive integers $m, n$?

## 4. Correlation $\lambda_a = 2$ and $\lambda_c = 1$

As was revealed in Section 3, there are many optimal $(m, n, 3, 1, 1)$-OOSPCs attaining the classical bound of Kitayama (1994). Thus in the case that $\lambda_a = 1$, the Kitayama bound can be used in deciding the optimality of OOSPCs. Next, what criteria should be used in deciding whether or not given OOSPCs of $\lambda_a = 2$ are optimal? In this section we will give an answer by deriving a new upper bound for the cardinality of OOSPCs and in fact by finding many OOSPCs which attain the new bound.

Throughout this section we let $A = \mathbb{Z}_m \times \mathbb{Z}_n$ and use the same notations as those introduced in Sections 1 and 2. For distinct nonzero elements $a_1, \ldots, a_t \in A$, we abbreviate $\mathrm{Orb}_A(\{0, a_1, \ldots, a_t\})$ as $[a_1, \ldots, a_t]$. Let

$$\Omega(A) = \{a \in A \mid 2a = 0\}.$$

Since $\Omega(A)$ is an elementary abelian 2-group, $\Omega(A)$ can be regarded as a vector space over the finite field $\mathbb{F}_2$ of two elements. Let

$$\mathcal{T}_1 = \{[a, -a] \mid a \in A \setminus \Omega(A)\},$$
$$\mathcal{T}_2 = \{[a, h] \mid a \in A \setminus \{0\},\ h \in \Omega(A) \setminus \{0, a\}\}.$$

It is possible to understand $\mathcal{T}_1$ and $\mathcal{T}_2$ geometrically when $A$ is cyclic. That is, when $m = 1$ (or $n = 1$), under a natural one-to-one correspondence between $x \in A$ and $e^{\frac{2\pi xi}{m}} \in \mathbb{C}$ (or $e^{\frac{2\pi xi}{n}} \in \mathbb{C}$), the elements of $\mathcal{T}_1(A)$ or $\mathcal{T}_2(A)$ can be viewed as isoceles or rectangles respectively; see Beth et al. (1993) for the detail.

The following lemma will play a key role in deriving our new bound. It focuses on the underlying elements in $\Delta X$, denoted by $\mathrm{supp}(\Delta X)$, where $X$ is a subset of $A$.

**Lemma 4.1.** Let $X = \{0, a, b\} \in \binom{A}{3}$. Then it holds that

$$|\mathrm{supp}(\Delta X)| = \begin{cases} 2 & \text{if } \langle a, b\rangle \simeq \mathbb{Z}_3, \\ 3 & \text{if } \langle a, b\rangle \simeq \mathbb{Z}_4 \text{ or } \mathbb{Z}_2^2, \\ 4 & \text{if } [a, b] \in \mathcal{T}_1, \\ 5 & \text{if } [a, b] \in \mathcal{T}_2, \\ 6 & \text{otherwise,} \end{cases}$$

where $\langle a, b\rangle$ denotes the subgroup of $A$ generated by $a$ and $b$.

**Proof.** For $X = \{0, a, b\} \in \binom{A}{3}$, we have $\Delta X = \{\pm a, \pm b, \pm(b - a)\}$.
Case 1 $|\Delta X \cap \Omega(A)| \geqslant 2$:

Without loss of generality we may let $a = h, b = h'$ for some $h, h' \in \Omega(A)$ with $h \neq h'$, or equivalently, $\langle a, b\rangle \simeq \mathbb{Z}_2^2$.
Case 2 $|\Delta X \cap \Omega(A)| = 1$:

If $b - a = h$ for some $h \in \Omega(A)$, we have $X = \{0, a, a+h\} = \{0, -a, h\}+a$. Thus it suffices to consider the case where $a = h$ for some $h \in \Omega(A)$. It is obvious that $|\mathrm{supp}(\Delta X)| = 3$ if and only if $b = -b + h$. This implies that $\langle a, b\rangle$ is a cyclic subgroup of $A$ generated by $b$.
Case 3 $|\Delta X \cap \Omega(A)| = 0$:

Observe that $\{0, a, 2a\} = \{0, a, -a\} + a$. Hence if $|\mathrm{supp}(\Delta X)| = 2$ or 4, we may let $a = -b$. In particular, $|\mathrm{supp}(\Delta X)| = 2$ if and only if $3a = 0$.
Thus we get the result. □

**Lemma 4.2.** Let $X \in \binom{A}{3}$. Then it holds that

$$\max_{a \in A \setminus \{0\}} |X \cap (X+a)| = \begin{cases} 3 & \text{if } |\mathrm{supp}(\Delta X)| = 2, \\ 2 & \text{if } |\mathrm{supp}(\Delta X)| = 3,4,5, \\ 1 & \text{otherwise.} \end{cases}$$

**Proof.** The result immediately follows from (4) and Lemma 4.1. □

**Lemma 4.3.** Let $m, n$ be odd integers. Then,

(i) $\mathbb{Z}_{2m} \times \mathbb{Z}_{4n}$ contains exactly two cyclic subgroups of order 4 which share an element of order 2, and

(ii) $\mathbb{Z}_{4m} \times \mathbb{Z}_{4n}$ contains exactly six cyclic subgroups of order 4. Given a cyclic subgroup $H_1$ of order 4, there exist two cyclic subgroups $H_2, H_3$ of order 4 such that for any $X \in \binom{H_i}{3}, Y \in \binom{H_j}{3}$ with $i, j = 1, 2, 3$, $\Delta X \cap \Delta Y = \emptyset$. Moreover, given four cyclic subgroups $H_1, H_2, H_3, H_4$, we can choose some $H_i, H_j$ such that for any $X \in \binom{H_i}{3}, Y \in \binom{H_j}{3}$, $\Delta X \cap \Delta Y \neq \emptyset$.

**Proof.** Straightforward from a standard argument in group theory. □

**Theorem 4.1.**

$$\phi(m,n,3,2,1) \leqslant \begin{cases} \dfrac{mn}{4} & \text{if } mn \equiv 0 \pmod 4, \\ \left\lfloor \dfrac{mn-1}{4} \right\rfloor & \text{otherwise.} \end{cases} \tag{6}$$

**Proof.** The proof consists of two cases.
Case 1 $mn \equiv 0 \pmod 4$:

In the case where the Sylow 2-subgroup of $A$ contains $\mathbb{Z}_4^2$, it follows from Lemmas 4.1, 4.2 and 4.3 (ii) that

$$\phi(m,n,3,2,1) \leqslant \left\lfloor \frac{(mn-1)-3\cdot 3}{4} \right\rfloor + 3 = \frac{mn}{4}.$$

Similarly, in the case where the Sylow 2-subgroup of $A$ is $\mathbb{Z}_2 \times \mathbb{Z}_4$, it follows from Lemmas 4.1, 4.2 and 4.3 (i) that

$$\phi(m,n,3,2,1) \leqslant \left\lfloor \frac{(mn-1)-3\cdot 1}{4} \right\rfloor + 1 = \frac{mn}{4}.$$

In the case where the Sylow 2-subgroup of $A$ is $\mathbb{Z}_2^2$, it follows from Lemmas 4.1 and 4.2 that

$$\phi(m,n,3,2,1) \leqslant \left\lfloor \frac{(mn-1)-3\cdot 1}{4} \right\rfloor + 1 = \frac{mn}{4}.$$

Case 2 $mn \not\equiv 0 \pmod 4$:

In this case $A$ contains no subgroups of order 4. Hence Lemmas 4.1 and 4.2 yield

$$\phi(m,n,3,2,1) \leqslant \left\lfloor \frac{mn-1}{4} \right\rfloor.$$

Thus we obtain the result. □

**Remark 4.1.** The bound (6) represents an improvement on the Kitayama bound (or the Kwong-Yang bound), since $J(m,n,3,2,1) = \lfloor (mn-1)/3 \rfloor$.

By Remark 4.1, the optimality of OOSPCs of $\lambda_a = 2$ cannot be evaluated by the Kitayama bound. In the following we will discuss the existence of optimal $(m,n,3,2,1)$-OOSPCs which attain the new bound (6).

**Theorem 4.2.** Let $m,n$ be positive integers such that $mn \equiv 2 \pmod 4$. Then there exists an optimal $(m,n,3,2,1)$-OOSPC which attains (6).

**Proof.** Let $\sigma$ be an automorphism of $A$ defined by $a^\sigma = 2a$. Since $mn \equiv 2 \pmod 4$, $A$ contains the unique element $h$ of order 2. Let $\tilde{A}$ be a subset of $A$ such that

$$A \setminus A^\sigma = \tilde{A} \cup (-\tilde{A}) \cup \{h\} \quad \text{and} \quad \tilde{A} \cap (-\tilde{A}) = \emptyset.$$

First we will claim that for $a \in \tilde{A}$,

$$m_a(\Delta(\{0,a,-a\})) \leqslant 2. \tag{7}$$

Suppose the contrary. Then there are two possibilities that $a = -2a$ or $a = -a$. The former case cannot occur since $-2a \in A^\sigma$ and $\tilde{A} \cap A^\sigma = \emptyset$. Thus we have $a = -a$, or equivalently, $a \in \Omega(A)$, which contradicts the uniqueness of $h$. Second we will claim that for distinct $a, b \in \tilde{A}$,

$$\Delta(\{0,a,-a\}) \cap \Delta(\{0,b,-b\}) = \emptyset. \tag{8}$$

Suppose the contrary. Then there are three possibilities, that is, $a = \pm 2b$, $b = \pm 2a$, $a = -b$. Since $\{2a, 2b\} \subset A^\sigma$, an argument made in the proof of (7) excludes the first two possibilities. The third case cannot also occur

either, since $\tilde{A} \cap (-\tilde{A}) = \emptyset$. Hence Proposition 2.1, together with (7) and (8), shows that the set

$$\{\{0, a, -a\} \mid a \in \tilde{A}\}$$

is an $(m, n, 3, 2, 1)$-OOSPC. Evidently the resulting OOSPC consists of $(mn-2)/4$ OOSPs and hence it is optimal with respect to (6). □

**Remark 4.3.** If $m$ or $n$ equals 1, the statement of Theorem 4.2 is equivalent to that of Theorem 3 in Levenshtein (2007).

**Theorem 4.4.** Let $m$ be a prime number with $m \equiv 1 \pmod 4$, and 2 be a primitive root modulo $m$. Then there exists an optimal $(m, m, 3, 2, 1)$-OOSPC which attains (6).

**Proof.** First, note that there exists a subset $P$ of $A$ which intersects each cyclic subgroup of $A$ in exactly one nonzero element, since $A$ contains $m+1$ pairwise disjoint cyclic subgroups of order $m$ (that is, any two of these subgroups should intersect in the zero element only). With the same symbol $\sigma$ as in Theorem 4.2, for each $p \in P$, let $\mathcal{C}_p$ be the set defined by

$$\mathcal{C}_p = \{p^{\sigma^{2i}} \mid i = 1, \cdots, (m-1)/4\}.$$

It is obvious that for distinct $p, p' \in P$, $\mathcal{C}_p \cap \mathcal{C}_{p'} = \emptyset$. Moreover by the assumption, $(m-1)/2$ is the smallest positive integer $r$ such that

$$2^r + 1 \equiv 0 \pmod m \quad \text{or} \quad 2^r - 1 \equiv 0 \pmod m.$$

This implies that for distinct $a, a' \in \mathcal{C}_p$,

$$\Delta(\{0, a, -a\}) \cap \Delta(\{0, a', -a'\}) = \emptyset.$$

Thus by Proposition 2.1, the set

$$\mathcal{C} = \{\{0, a, -a\} \mid a \in \mathcal{C}_p,\ p \in P\}$$

yields an $(m, m, 3, 2, 1)$-OOSPC. The OOSPC consists of $(m+1)(m-1)/4 = (m^2-1)/4$ OOSPs, which is seen to be optimal with respect to (6). □

**Remark 4.5.**

(i) Using Theorems 4.2 and 4.4, we have found many optimal OOSPCs attaining (6), which seems to confirm the validity of using the new bound in deciding whether or not given OOSPCs of $\lambda_a = 2$ are optimal.

(ii) The construction of optimal OOSPCs developed in Theorem 4.4 can be similarly modified for $m$ being a prime number congruent to 3 modulo 4, though the resulting OOSPCs are not optimal with respect to (6).

(iii) Theorem 4.4 is also valid for some nonprime odd integers $m$. For example, in the case that $m = 65$, we choose a cyclic subgroup of $\mathbb{Z}_{65}^2$ of order 65 and identify it with $\mathbb{Z}_{65}$. Then all the nonzero elements of $\mathbb{Z}_{65}$ appear among the differences arising from the following triples

$$\begin{array}{lll} \{0,1,2\}, & \{0,4,8\}, & \{0,16,32\}. \\ \{0,3,6\}, & \{0,12,24\}, & \{0,17,34\}. \\ \{0,5,10\}, & \{0,20,40\}, & \{0,15,30\}. \\ \{0,7,14\}, & \{0,28,56\}, & \{0,18,36\}. \\ \{0,11,22\}, & \{0,21,42\}, & \{0,19,38\}. \\ \{0,13,26\}. & & \end{array}$$

Since any cyclic subgroup of $\mathbb{Z}_{65}^2$ is isomorphic to one of $\mathbb{Z}_5$, $\mathbb{Z}_{13}$ and $\mathbb{Z}_{65}$, there exists an optimal $(65, 65, 3, 2, 1)$-OOSPC which attains (6).

We conclude this section by summarizing two open problems.

**Problem 4.1.** (i) Extend Theorem 4.4 for nonprime odd integers. (ii) In the case that $mn \equiv 0 \pmod 4$, find the construction of optimal $(m, n, 3, 2, 1)$-OOSPCs which attain (6).

## References

Anderson I. (1997): Combinatorial Designs and Tournaments. Clarendon Press, Oxford.

Beth T., Charnes C., Grassl M., Alber G., Delgado A., Mussinger M. (2003): A new class of designs which protect against quantum jumps. Des. Codes, Cryptogr. 29: 51–70.

Beth T., Jungnickel D., Lenz H. (1993): Design Theory – Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge. 69 (2nd ed.).

Colbourn C. J., Dinitz J. H. (eds.) (2007): Handbook of Combinatorial Designs (2nd ed.). Chapman and Hall/CRC, Boca Raton.

Chung H., Kumar P. V. (1990): Optical orthogonal codes – New bounds and an optimal construction. IEEE Trans. Inf. Theory. 36: 866–873.

Chung F. R. K., Salehi J. A., Wei V. K. (1989): Optical orthogonal codes: Design, analysis, and applications. IEEE Trans. Inf. Theory. 35: 595–604.

Fuji-Hara R., Miao Y. (2000): Optical orthogonal codes: Their bounds and new optimal constructions. IEEE Trans. Inf. Theory. 46: 2396–2406.

Fuji-Hara R., Miao Y., Yin J. (2001): Optimal $(9v, 4, 1)$ optical orthogonal codes. SIAM J. Discrete Math. 14: 256–266.

Harwit M., Sloane N. J. A. (1979): Hadamard Transform Optics. Academic Press, New York.

Hassan A. A., Hershey J. E., Riza N. A. (1995): Spatial optical CDMA. IEEE J. Sel. Areas Commun. 13: 609–613.

Hui J. Y. (1985): Pattern code modulation and optical decoding – A novel code-division multiplexing technique for multifiber networks. IEEE J. Sel. Areas Commun. 3: 919–927.

Kitayama K. (1994): Novel spatial spread spectrum based fiber optic CDMA networks for image transmission. IEEE J. Sel. Areas Commun. 12: 762–772.

Kwong W. C., Yang G. C. (1996): Two-dimensional spatial signature patterns. IEEE Trans. Commun. 44: 184–191.

Kwong W. C., Yang G. C. (2001): Double-weight signature pattern codes for multicore-fiber code-division multiple-access networks. IEEE Commun. Lett. 5: 203–205.

Levenshtein V. I. (2007): Conflict-avoiding codes and cyclic triple systems. Probl. Inf. Transm. 43: 199–212.

Moreno O., Zhang Z., Kumar P. V., Zinoviev V. A. (1995): New constructions of optimal cyclically permutable constant weight codes. IEEE Trans. Inf. Theory 41: 448–455.

Mutoh Y., Morihara T., Jimbo M., Fu H. L. (2003): The existence of $2 \times 4$ grid-block designs and their applications. SIAM J. Discrete Math. 16: 173–178.

Omrani R., Kumer P. V. (2006): Codes for optical CDMA. Lecture Notes in Computer Science, Springer, 4088: 34–46.

O'keefe E. S. (1961): Verification of a conjecture of T. Skolem. Math. Scand. 9: 80–82.

Park E., Mendez A. J., Garmire E. M. (1992): Temporal/spatial optical CDMA networks – Design, demonstration, and comparison with temporal networks. IEEE Photonics Technol. Lett. 4: 1160–1163.

Schönheim J. (1966): On maximal systems of $k$-tuples. Syudia Sci. Math. Hungar. 1: 363–368.

Skolem T. (1957): On certain distributions of integers in pairs with given differences. Math. Scand. 5: 57–58.

Yang G. C., Kwong W. C. (1997): Performance comparison of multiwavelength CDMA and WDMA+CDMA for fiber-optic networks. IEEE Trans. Commun. 45: 1426–1434.

Yates F. (1936): Incomplete randomized blocks. Ann. Eugen. 7: 121–140.