New Families of Optimal Variable-Weight Optical Orthogonal Codes With High Weights

Jin-Ho Chung, *Member, IEEE*, and Kyeongcheol Yang, *Senior Member, IEEE*

***Abstract*— The optical orthogonal codes (OOCs) have been widely used as spreading codes in communication systems employing the unipolar transmission. They are classified into constant-weight OOCs (CW-OOCs) and variable-weight OOCs (VW-OOCs) according to the number of distinct Hamming weights which their codewords have. In this paper, we present a new generic construction of VW-OOCs of length $(q-1)N$ from a CW-OOC of length N, where q is a prime power and $\gcd(q-1, N) = 1$. As a result, three new families of optimal VW-OOCs with a maximum correlation value 1 are obtained. In particular, these families can have the codewords of high weights, while most of the previously known optimal VW-OOCs have only codewords of weight less than 8.**

***Index Terms*— Correlation, optical fiber networks, optical orthogonal codes (OOCs), unipolar transmission, variable-weight OOCs.**

I. Introduction

OPTICAL orthogonal codes (OOCs) have been widely used as spreading codes in communication systems employing unipolar transmission, including optical fiber networks. A codeword of an OOC is a $\{0, 1\}$-sequence such that 1 means signal 'on' and 0 signal 'off' [1]–[3]. Length, weight, size, and correlation values are the important parameters of an OOC. The ratio between the weight and the length of a codeword is closely related to its detectability, while correlation values are concerned with the multiple-access interference. Moreover, the size of an OOC is desired to be as large as possible in order to accommodate as many simultaneous users as possible. Roughly speaking, design of a good OOC is a different problem from that of a $\{0, 1\}$-sequence family for bipolar transmission. See [4]–[7] for a survey of sequence families for bipolar transmission.

OOCs are classified into constant-weight OOCs (CW-OOCs) and variable-weight OOCs (VW-OOCs) according to the number of distinct Hamming weights which their codewords have. The former supports a single quality-of-service (QoS), while the latter may support multiple QoSs. Chung *et al.* [3] set up a guideline for design of OOCs, and presented some optimal CW-OOCs. Since then, several constructions for optimal CW-OOCs with respect to the Johnson bound [8] have been reported in the literature [9]–[24]. Later, Yang [25] introduced the concept of VW-OOCs and presented a bound on their sizes by generalizing the Johnson bound. Since then, a number of optimal VW-OOCs with a finite set of small weights have been reported [26]–[31]. However, there is no known systematic construction for VW-OOCs with a set of weights larger than 7, except for the construction by Yang in [25]. Therefore, it is challenging to design a VW-OOC with high weights. Furthermore, it is known that the ratio between the weight and the maximum cross-correlation of an OOC is the performance figure of merit [11].

In this paper, we present a new generic construction of VW-OOCs of length $(q-1)N$ from a CW-OOC of length N, where q is a prime power and $\gcd(q-1, N) = 1$. The new construction can be applied to any CW-OOCs with maximum correlation value 1. As a result, three new families of optimal VW-OOCs with maximum correlation value 1 are obtained. In particular, these families can have codewords of high weights, while most of the previously known optimal VW-OOCs have only codewords of weight less than 8, as shown in Table I. For example, optimal VW-OOCs with codewords of weights u and $u-1$ are constructed for any prime power u. The new VW-OOCs can be applied to much more general cases in a practical situation.

The outline of the paper is as follows. In Section II, we give some preliminaries to OOCs. In Section III, we present a new generic construction for VW-OOCs of length $(q-1)N$, by which three new families of optimal VW-OOCs are obtained. Finally, we give some concluding remarks in Section IV.

II. Preliminaries

Throughout the paper, the following notation is employed.

- $\langle x \rangle_y$: the least nonnegative residue of x modulo y for an integer x and a positive integer y,
- $\lfloor z \rfloor$: the largest integer less than or equal to z,
- $I(x)$: the function defined as $I(x) = 1$ if x is true, and 0 otherwise,
- $\mathbb{Z}_n$: the ring of integers modulo n for a positive integer n.

Let $\mathcal{X} \triangleq \{X_0, \ldots, X_{L-1}\}$ be a set of $\{0, 1\}$-sequences of length N, where $X_a \triangleq \{X_a(t)\}_{t=0}^{N-1}$ for $0 \le a \le L-1$.

Manuscript received December 2, 2014; revised April 8, 2015; accepted May 28, 2015. Date of publication June 4, 2015; date of current version July 10, 2015. This work was supported in part by the 2014 Research Fund (1.140053.01) of UNIST (Ulsan National Institute of Science and Technology), in part by the ICE R&D Program (Development of Service and Transmission Technology for Convergent Realistic Broadcast, R0101-15-294) funded by the the Ministry of Science, ICT and Future Planning (MSIP) of the Korean Government, and in part by the National Research Foundation (NRF) of Korea under Grant 2011-0017396 funded by the MSIP. This paper was presented in part at the 2015 IEEE International Symposium on Information Theory.

J.-H. Chung is with the School of Electrical and Computer Engineering, Ulsan National Institute of Science and Technology, Ulsan 689-798, Korea (e-mail: jinho@unist.ac.kr).

K. Yang is with the Department of Electrical Engineering, Pohang University of Science and Technology, Pohang, Gyungbuk 790-784, Korea (e-mail: kcyang@postech.ac.kr).

Communicated by S. Mesnager, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2015.2441695

TABLE I
PARAMETERS OF OPTIMAL VARIABLE-WEIGHT OPTICAL ORTHOGONAL CODES WITH $\lambda = 1$

Reference	(N, W, λ, R)	Constraints
[25]	$\left(p, \{w, w+1\}, 1, \left\{\frac{r_0}{r_0+r_1}, \frac{r_1}{r_0+r_1}\right\}\right)$	$p = w(w+1)r_0 + w(w-1)r_1 + 1$, p: a prime, $2 \nmid w$
[27]	$(lv, \{3,4\}, 1, \{\frac{1}{2}, \frac{1}{2}\})$	$l \in \{3, 12\}$ (each prime factor of v) $\equiv 1 \bmod 6$
	$(6v, \{3,4\}, 1, \{\frac{1}{2}, \frac{1}{2}\})$	(each prime factor of v) $\equiv 7 \bmod 12$
	$(6v, \{3,6\}, 1, \{\frac{1}{2}, \frac{1}{2}\})$	(each prime factor of v) $\equiv 7, 31 \bmod 36$
[28]	$(v, \{3,4\}, 1, \{\frac{1}{2}, \frac{1}{2}\})$	$u \equiv 9, 45 \bmod 54$
	$(v, \{4,5\}, 1, \{\frac{1}{2}, \frac{1}{2}\})$	$u \equiv 16, 80 \bmod 96$
[29]	$(63v, \{3,4,5,6\}, 1, \{\frac{1}{19}, \frac{6}{19}, \frac{6}{19}, \frac{6}{19}\})$	$\gcd(v, 63) = 1$, (each prime factor of v) $\equiv 1 \bmod 6$
	$(105v, \{3,4,5,6,7\}, 1, \{\frac{1}{25}, \frac{6}{25}, \frac{6}{25}, \frac{6}{25}, \frac{6}{25}\})$	$\gcd(v, 105) = 1$, (each prime factor of v) $\equiv 1 \bmod 6$
[30]	$(19v, \{3,4,5\}, 1, \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\})$, $(22v, \{3,4,5\}, 1, \{\frac{1}{2}, \frac{1}{4}, \frac{1}{4}\})$, $(25v, \{3,4,5\}, 1, \{\frac{3}{5}, \frac{1}{5}, \frac{1}{5}\})$, $(28v, \{3,4,5\}, 1, \{\frac{2}{5}, \frac{2}{5}, \frac{1}{5}\})$	$\gcd(v, 6) = 1$
	$(24v, \{3,4,6\}, 1, \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\})$, $(28v, \{3,5,6\}, 1, \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\})$, $(34v, \{3,4,5,6\}, 1, \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\})$	$\gcd(v, 30) = 1$
Corollary 8	$\left((q-1)p, \{w-1, w\}, 1, \left\{\frac{w}{q+1}, \frac{q+1-w}{q+1}\right\}\right)$	p: a prime with $p = w(w-1)L + 1$, q: a prime power with $q \geq w$, $\gcd(p, q-1) = 1$, there exists an optimal $(p, w, 1, 1)$ CW-OOC.
Corollary 9	$\left((q-1)(u^2+u+1)^k, \{u, u+1\}, 1, \left\{\frac{u+1}{q+1}, \frac{q-u}{q+1}\right\}\right)$	u: an odd prime power, $k \geq 1$, q: a prime power with $q > u$, $\gcd(u^2+u+1, q-1) = 1$.
Corollary 10	$\left((q-1)(u^k-1), \{u-1, u\}, 1, \left\{\frac{u}{q+1}, \frac{q+1-u}{q+1}\right\}\right)$	u: a prime power, $k \geq 2$, q: a prime power with $q \geq u$, $\gcd(u^k-1, q-1) = 1$.

The support of X_a is defined by $\mathrm{supp}(X_a) \triangleq \{t \mid X_a(t) = 1, 0 \leq t \leq N-1\}$. Conversely, any subset S of $\mathbb{Z}_N$ induces its incidence sequence $X = \{X(t)\}_{t=0}^{N-1}$ given by $X(t) = I(t \in S)$. The *cross-correlation* $\Lambda_{a,b}(\tau)$ between X_a and X_b in $\mathcal{X}$ is defined as

$$\Lambda_{a,b}(\tau) = \sum_{t=0}^{N-1} X_a(t) X_b(\langle t+\tau \rangle_N) \tag{1}$$

where $0 \leq a, b \leq L-1$. Equivalently, $\Lambda_{a,b}(\tau)$ can be represented as

$$\Lambda_{a,b}(\tau) = |(\mathrm{supp}(X_a) + \tau) \cap \mathrm{supp}(X_b)|. \tag{2}$$

If $a = b$, it is called the *autocorrelation* of X_a. Note that the correlation property of $\mathcal{X}$ is closely related to the combinatorial structure *difference family* or its generalized versions. See [9], [14], [30], [32] for more details.

A. Constant-Weight OOC

Let $\mathcal{C} \triangleq \{C_a \mid 0 \leq a \leq L-1\}$ be a set of L $\{0, 1\}$-sequences such that $C_a \triangleq \{C_a(t)\}_{t=0}^{N-1}$ has support size w for $0 \leq a \leq L-1$. That is, $\mathcal{C}$ has size L and its codewords have weight w. Let $\Lambda_{a,b}(\tau)$ be the cross-correlation between C_a and C_b. If $\mathcal{C}$ has

$$\max_{\substack{0 \leq a \leq L-1, \\ 1 \leq \tau \leq N-1}} \{\Lambda_{a,a}(\tau)\} = \lambda_{\mathrm{a}}$$

and

$$\max_{\substack{0 \leq a \neq b \leq L-1, \\ 0 \leq \tau \leq N-1}} \{\Lambda_{a,b}(\tau)\} = \lambda_{\mathrm{c}}$$

for some positive integers λ_{a} and λ_{c}, it is called an $(N, w, \lambda_{\mathrm{a}}, \lambda_{\mathrm{c}})$ CW-OOC. Conventionally, the maximum correlation λ of $\mathcal{C}$ is defined as

$$\lambda = \max\{\lambda_{\mathrm{a}}, \lambda_{\mathrm{c}}\}.$$

Johnson [8] derived a bound illustrating a trade-off among the parameters of a CW-OOC.

Theorem 1 (Johnson Bound [8]): An $(N, w, \lambda_{\mathrm{a}}, \lambda_{\mathrm{c}})$ CW-OOC of size L satisfies

$$L \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{N-1}{w-1} \left\lfloor \frac{N-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{N-\lambda}{w-\lambda} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor$$

where $\lambda = \max\{\lambda_{\mathrm{a}}, \lambda_{\mathrm{c}}\}$.

If an $(N, w, \lambda_a, \lambda_c)$ CW-OOC $\mathcal{C}$ of size L satisfies the Johnson bound with equality, it is called an *optimal CW-OOC*.

B. Variable-Weight OOC

Let $\mathcal{V} = \{V_a \mid 0 \le a \le K-1\}$ be a set of K $\{0, 1\}$-sequences of length N, where $V_a \triangleq \{V_a(t)\}_{t=0}^{N-1}$. It is called an $(N, W, \Lambda, \lambda_c, R)$ VW-OOC with $W = \{w_1, \ldots, w_m\}$, $\Lambda = \{\lambda_a(1), \ldots, \lambda_a(m)\}$, and $R = \{r_1, \ldots, r_m\}$ if the following three conditions are satisfied:

i) there are exactly $r_i K$ codewords with weight w_i for $1 \le i \le m$, where $r_1 + \cdots + r_m = 1$ and $r_j \ge 0$ for $1 \le j \le m$;

ii) the autocorrelation of V_a with weight w_i in $\mathcal{V}$ is upper bounded by

$$\Lambda_{a,a}(\tau) \le \lambda_a(i), \quad \langle \tau \rangle_N \ne 0$$

for some positive integer $\lambda_a(i)$; and

iii) the cross-correlation between V_a and V_b with $a \ne b$ in $\mathcal{V}$ is upper bounded by

$$\Lambda_{a,b}(\tau) \le \lambda_c$$

for some positive integer λ_c.

In the particular case that $\lambda_a(1) = \cdots = \lambda_a(m) = \lambda_c = \lambda$, it will be referred to as an (N, W, λ, R) VW-OOC for short notation. Note that if $m = 1$, an $(N, W, \Lambda, \lambda_c, R)$ VW-OOC becomes an $(N, w, \lambda_a, \lambda_c)$ CW-OOC with $w = w_1$ and $\lambda_a = \lambda_a(1)$.

Yang [25] established an upper bound on the size of an $(N, W, \Lambda, \lambda_c, R)$ VW-OOC by generalizing the Johnson bound.

Theorem 2 ([25]): The size K of an $(N, W, \Lambda, \lambda_c, R)$ VW-OOC $\mathcal{V}$ satisfying $\lambda_a(i) \ge \lambda_c$ for any $1 \le i \le m$ is upper bounded by

$$K \le \left\lfloor \frac{(N-1)(N-2)\cdots(N-\lambda_c)}{\sum_{i=1}^{m} r_i w_i (w_i - 1)\cdots(w_i - \lambda_c)/\lambda_a(i)} \right\rfloor. \quad (3)$$

Later, Wu *et al.* [28] presented an improved bound which is tighter than (3) in some cases.

Theorem 3 ([28]): The size K of an $(N, W, \Lambda, \lambda_c, R)$ VW-OOC $\mathcal{V}$ satisfying $\lambda_a(i) \ge \lambda_c$ for any $1 \le i \le m$ is upper bounded by

$$K \le \min_{i:\, 1 \le i \le m} \left\lfloor \frac{1}{r_i} \left\lfloor r_i \left\lfloor \frac{(N-1)(N-2)\cdots(N-\lambda_c)}{\sum_{i=1}^{m} r_i w_i (w_i - 1)\cdots(w_i - \lambda_c)/\lambda_a(i)} \right\rfloor \right\rfloor \right\rfloor. \quad (4)$$

If $\mathcal{V}$ satisfies (3) or (4) with equality, it is called an *optimal VW-OOC*. The bound (4) can be further simplified for an $(N, W, 1, R)$ VW-OOC as follows:

$$K \le \min_{i:\, 1 \le i \le m} \left\lfloor \frac{1}{r_i} \left\lfloor r_i \left\lfloor \frac{N-1}{\sum_{i=1}^{m} r_i w_i (w_i - 1)} \right\rfloor \right\rfloor \right\rfloor. \quad (5)$$

Remark: In communication systems based on bipolar transmission, $\{0, 1\}$-sequences are transformed into $\{+1, -1\}$-sequences by the map $f(x) = (-1)^x$. In this case, the cross-correlation $\theta_{S_a, S_b}(\tau)$ between two $\{0, 1\}$-sequences $S_a = \{S_a(t)\}_{t=0}^{N-1}$ and $S_b = \{S_b(t)\}_{t=0}^{N-1}$ is given by

$$\theta_{S_a, S_b}(\tau) = \sum_{t=0}^{N-1} (-1)^{S_a(t) + S_b(\langle t+\tau \rangle_N)} \quad (6)$$

for $0 \le \tau \le N-1$. Binary sequences with low correlation in this sense have been extensively studied. For a survey, see [4]–[7]. Note that a sequence family with low correlation in bipolar transmission does not necessarily have small λ when it is converted to an OOC. Similarly, an OOC with small λ does not always have low correlation when it is used in bipolar transmission. The main reason is that the two correlations in (1) and (6) have quite distinct attributes. Therefore, design of an OOC with small λ is another challenging task.

III. New Optimal Variable-Weight OOCs of Length $(q-1)N$

Let $\mathcal{X} = \{X_0, X_1, \ldots, X_{L-1}\}$ be an $(N, w, 1, 1)$ CW-OOC, where X_a is defined as

$$\mathrm{supp}(X_a) = \{x_a[0], x_a[1], \ldots, x_a[w-1]\}$$

for $0 \le a \le L-1$, where $x_a[i]$ is the position of the ith nonzero value of X_a, and $0 \le x_a[0] < x_a[1] < \cdots < x_a[w-1] \le N-1$. Let q be a prime power satisfying $q \ge w$ and α a primitive element of $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of q elements. Note that every nonzero element $\beta \in \mathbb{F}_q$ can be expressed as a power of α, that is, $\beta = \alpha^l$ for some l with $0 \le l \le q-2$. In this expression, the exponent l is denoted by $l = \log_\alpha \beta$. For simplicity, we will use $\log \beta$ instead of $\log_\alpha \beta$ throughout the paper.

Let M and N be two positive integers with $\gcd(M, N) = 1$. By the Chinese Remainder Theorem (CRT) [33], any integer t with $0 \le t \le MN-1$ can be uniquely represented as

$$t = (t_0, t_1)$$

where $t_0 = \langle t \rangle_M$ and $t_1 = \langle t \rangle_N$.

Construction A: Let $\mathcal{X} = \{X_0, X_1, \ldots, X_{L-1}\}$ be an $(N, w, 1, 1)$ CW-OOC. Assume that q is a prime power with $q \ge w$ and $\gcd(q-1, N) = 1$. For a primitive element α of $\mathbb{F}_q$, let

$$U \triangleq \{\alpha^0, \alpha^1, \ldots, \alpha^{w-1}\}.$$

For $0 \le a \le L-1$ and $s \in \mathbb{F}_q \cup \{\infty\}$, we define $Y_{a,s} = \{Y_{a,s}(t)\}_{t=0}^{(q-1)N-1}$ as the $\{0, 1\}$-sequence of length $(q-1)N$, given by

$$Y_{a,s}(t) = \begin{cases} 1, & \text{if } \alpha^{t_0} + s \in U \text{ and } t_1 = x_a\left[\log(\alpha^{t_0} + s)\right] \\ 0, & \text{otherwise} \end{cases}$$

for $s \in \mathbb{F}_q$, and

$$Y_{a,\infty}(t) = \begin{cases} 1, & \text{if } t_0 = 0 \text{ and } t_1 \in \mathrm{supp}(X_a) \\ 0, & \text{otherwise} \end{cases}$$

where $t_0 = \langle t \rangle_{q-1}$ and $t_1 = \langle t \rangle_N$. The VW-OOC $\mathcal{Y}_A$ is defined as

$$\mathcal{Y}_A \triangleq \{Y_{a,s} \mid 0 \le a \le L-1,\ s \in \mathbb{F}_q \cup \{\infty\}\}.$$

Note that the support of each codeword in $\mathcal{Y}_A$ can be equivalently represented as a subset of $\mathbb{Z}_{q-1} \times \mathbb{Z}_N$ by the CRT. That is,

$$\begin{aligned}\mathrm{supp}(Y_{a,s}) = &\left\{\left(\log(g-s), x_a\left[\log g\right]\right) | g \in U \setminus \{s\}\right\} \\ &\subset \mathbb{Z}_{q-1} \times \mathbb{Z}_N. \end{aligned} \tag{7}$$

for $s \in \mathbb{F}_q$, and

$$\mathrm{supp}(Y_{a,\infty}) = \{(0, x_a[\log g]) \mid g \in U\} \subset \mathbb{Z}_{q-1} \times \mathbb{Z}_N.$$

In order to calculate the correlation values of $\mathcal{Y}_A$, we divide the problem into three cases. The following three lemmas will be very useful in demonstrating the correlation property of $\mathcal{Y}_A$.

Lemma 4: For $0 \le a_1, a_2 \le L-1$ and $s_1, s_2 \in \mathbb{F}_q$, the correlation $\Lambda_{(a_1,s_1),(a_2,s_2)}(\tau)$ between Y_{a_1,s_1} and Y_{a_2,s_2} in Construction A satisfies

$$\Lambda_{(a_1,s_1),(a_2,s_2)}(\tau) \le 1$$

if $(a_1, s_1) \ne (a_2, s_2)$ or $\tau \ne 0$.

Proof: For $0 \le \tau \le (q-1)N - 1$, let $\tau_0 = \langle \tau \rangle_{q-1}$ and $\tau_1 = \langle \tau \rangle_N$. For a simple proof, we will denote $\Lambda_{(a_1,s_1),(a_2,s_2)}(\tau)$ by $\Lambda(\tau)$. We have

$$\begin{aligned}&\Lambda(\tau) \\ &= \Lambda(\tau_0, \tau_1) \\ &= \left|\left(\mathrm{supp}(Y_{a_1,s_1}) + (\tau_0, \tau_1)\right) \cap \mathrm{supp}(Y_{a_2,s_2})\right| \\ &= \left|\left\{\left(\log(g-s_1) + \tau_0, x_{a_1}[\log g] + \tau_1\right) | g \in U \setminus \{s_1\}\right\}\right. \\ &\quad \left. \cap \left\{\left(\log(g'-s_2), x_{a_2}[\log g]\right) | g' \in U \setminus \{s_2\}\right\}\right| \\ &= \sum_{\substack{g \in U\setminus\{s_1\}, \\ g' \in U\setminus\{s_2\}}} I\left(\tau_0 = \left\langle \log(g'-s_2) - \log(g-s_1)\right\rangle_{q-1}\right) \\ &\quad \cdot I\left(\tau_1 = \left\langle x_{a_2}[\log g'] - x_{a_1}[\log g]\right\rangle_N\right)\end{aligned}$$

where the last equality comes from (7). Calculation of $\Lambda(\tau)$ can be divided into three cases according to a_1, a_2 and τ_1.

Case i) $a_1 = a_2$ and $\tau_1 = 0$. Note that $0 = x_{a_1}[\log g'] - x_{a_1}[\log g]$ implies $g' = g$ when $g \in U \setminus \{s_1\}$ and $g' \in U \setminus \{s_2\}$. Thus,

$$\begin{aligned}\Lambda(\tau_0, \tau_1) = &\sum_{\substack{g \in U\setminus\{s_1\}, \\ g' \in U\setminus\{s_2\}}} I\left(\tau_0 = \left\langle \log(g'-s_2) - \log(g-s_1)\right\rangle_{q-1}\right) \\ &\cdot I(g' = g).\end{aligned}$$

If $s_1 = s_2$,

$$\begin{aligned}&\Lambda(\tau_0, \tau_1) \\ &= \sum_{g, g' \in U\setminus\{s_1\}} I(\tau_0 = 0) \cdot I(g' = g) \\ &= \sum_{g \in U\setminus\{s_1\}} I(\tau_0 = 0) \\ &= \begin{cases} w, & \text{if } \tau = 0 \text{ and } s_1 \in \mathbb{F}_q \setminus U \\ w-1, & \text{if } \tau = 0 \text{ and } s_1 \in U \\ 0, & \text{otherwise.} \end{cases}\end{aligned}$$

If $s_1 \ne s_2$,

$$\begin{aligned}\Lambda(\tau_0, \tau_1) &= \sum_{\substack{g \in U\setminus\{s_1\}, \\ g' \in U\setminus\{s_2\}}} I\left(\tau_0 = \log\frac{g'-s_2}{g-s_1}\right) \cdot I(g' = g) \\ &= \sum_{g \in U\setminus\{s_1,s_2\}} I\left(\tau_0 = \log\frac{g-s_2}{g-s_1}\right) \\ &\le 1\end{aligned}$$

where the last inequality comes from the fact that $\frac{x-s_2}{x-s_1} \ne \frac{y-s_2}{y-s_1}$ for any $x, y \in \mathbb{F}_q \setminus \{s_1, s_2\}$ with $x \ne y$.

Case ii) $a_1 = a_2$ and $\tau_1 \ne 0$. We have

$$\begin{aligned}\Lambda(\tau_0, \tau_1) &\le \sum_{\substack{g \in U\setminus\{s_1\}, \\ g' \in U\setminus\{s_2\}}} I\left(\tau_1 = \left\langle x_{a_1}[\log g'] - x_{a_1}[\log g]\right\rangle_N\right) \\ &\le \sum_{g, g' \in U} I\left(\tau_1 = \left\langle x_{a_1}[\log g'] - x_{a_1}[\log g]\right\rangle_N\right) \\ &= \Lambda_{X_{a_1}, X_{a_1}}(\tau_1) \\ &\le 1\end{aligned}$$

where $\Lambda_{X_{a_1}, X_{a_1}}(\tau_1)$ is the autocorrelation of $X_{a_1} \in \mathcal{X}$.

Case iii) $a_1 \ne a_2$. In a similar way to the proof of Case ii),

$$\begin{aligned}\Lambda(\tau_0, \tau_1) &\le \Lambda_{X_{a_1}, X_{a_2}}(\tau_1) \\ &\le 1\end{aligned}$$

where $\Lambda_{X_{a_1}, X_{a_2}}(\tau_1)$ is the cross-correlation between X_{a_1} and X_{a_2} in $\mathcal{X}$.

By summarizing the results of Cases i), ii), and iii), we can conclude that

$$\Lambda(\tau) \le 1$$

if $(a_1, s_1) \ne (a_2, s_2)$ or $\tau \ne 0$. □

Lemma 5: For $0 \le a_1, a_2 \le L-1$ and $s_1 \in \mathbb{F}_q$, the correlation $\Lambda_{(a_1,s_1),(a_2,\infty)}(\tau)$ between Y_{a_1,s_1} and $Y_{a_2,\infty}$ in Construction A satisfies

$$\Lambda_{(a_1,s_1),(a_2,\infty)}(\tau) \le 1.$$

Proof: In a similar way to the Proof of Lemma 4, we have

$$\begin{aligned}\Lambda(\tau_0, \tau_1) &\le \sum_{\substack{g \in U\setminus\{s_1\}, \\ g' \in U}} I\left(\tau_0 = \langle -\log(g-s_1)\rangle_{q-1}\right) \\ &\quad \cdot I\left(\tau_1 = \left\langle x_{a_2}[\log g'] - x_{a_1}[\log g]\right\rangle_N\right) \\ &= \sum_{g \in U\setminus\{s_1\}} I\left(\tau_0 = \langle -\log(g-s_1)\rangle_{q-1}\right) \\ &\quad \cdot \sum_{g' \in U} I\left(\tau_1 = \left\langle x_{a_2}[\log g'] - x_{a_1}[\log g]\right\rangle_N\right) \\ &\le \sum_{g \in U\setminus\{s_1\}} I\left(\tau_0 = \langle -\log(g-s_1)\rangle_{q-1}\right) \\ &\le 1.\end{aligned}$$

□

Lemma 6: For $0 \le a_1, a_2 \le L-1$, the correlation $\Lambda_{(a_1,\infty),(a_2,\infty)}(\tau)$ between $Y_{a_1,\infty}$ and $Y_{a_2,\infty}$ in Construction A satisfies

$$\Lambda_{(a_1,\infty),(a_2,\infty)}(\tau) \le 1$$

if $a_1 \ne a_2$ or $\tau \ne 0$.

Proof: We have

$$\Lambda(\tau_0,\tau_1) = \sum_{g,g'\in U} I\left(\tau_0 = 0\right)\cdot I\left(\tau_1 = \left\langle x_{a_2}[\log g'] - x_{a_1}[\log g]\right\rangle_N\right).$$

If $\tau_0 = 0$,

$$\begin{aligned}\Lambda(\tau_0,\tau_1) &= \sum_{g,g'\in U} I(\tau_1 = \left\langle x_{a_2}[\log g'] - x_{a_1}[\log g]\right\rangle_N)\\ &= \Lambda_{X_{a_1},X_{a_2}}(\tau_1)\\ &\le \begin{cases} w, & \text{if } \tau_1 = 0 \text{ and } a_1 = a_2\\ 1, & \text{otherwise.}\end{cases}\end{aligned}$$

If $\tau_0 \neq 0$, it is clear that $\Lambda(\tau_0,\tau_1) = 0$. □

Lemmas 4–6 tell us that the maximum correlation between any two sequences in $\mathcal{Y}_A$ is 1.

Theorem 7: Given an $(N, w, 1, 1)$ CW-OOC $\mathcal{X}$ of size L, the set $\mathcal{Y}_A$ in Construction A is a

$$\left((q-1)N, \{w-1, w\}, 1, \left\{\frac{w}{q+1}, \frac{q+1-w}{q+1}\right\}\right)$$

VW-OOC of size $(q+1)L$, where q is a prime power such that $q \ge w$ and $\gcd(q-1, N) = 1$.

Proof: Note that the number of t_0, $0 \le t_0 \le q-2$, satisfying $\alpha^{t_0}+s \in U$ is $|U|-1$ if $s \in U$, and $|U|$ if $s \in \mathbb{F}_q \backslash U$. This implies that the weight of $Y_{a,s}$ is $w-1$ if $s \in U$, and w if $s \in \mathbb{F}_q \backslash U$, where $0 \le a \le L-1$. Moreover, the weight of $Y_{a,\infty}$ is equal to the weight w of X_a for all $0 \le a \le L-1$. Hence, $W = \{w-1, w\}$, $R = \left\{\frac{w}{q+1}, \frac{q+1-w}{q+1}\right\}$, and $|\mathcal{Y}_A| = (q+1)L$. Clearly, $\lambda = 1$ by Lemmas 4–6. □

It is possible to obtain three new classes of optimal VW-OOCs by applying Construction A to some known optimal CW-OOCs. The first one is from the optimal $(p, w, 1, 1)$ CW-OOCs of size L_1 in [9], [10], and [12], where p is a prime such that $p = w(w-1)L_1 + 1$.

Corollary 8: Let $p = w(w-1)L_1 + 1$ be an odd prime such that there exists an optimal $(p, w, 1, 1)$ CW-OOC $\mathcal{X}_1$ of size L_1. Let q be a prime power satisfying $\gcd(q-1, p) = 1$ and $q \ge w$. Then, the set $\mathcal{Y}_1$ obtained from $\mathcal{X}_1$ by Construction A is an optimal $\left((q-1)p, \{w-1, w\}, 1, \left\{\frac{w}{q+1}, \frac{q+1-w}{q+1}\right\}\right)$ VW-OOC of size $(q+1)L_1$.

Proof: The parameters of $\mathcal{Y}_1$ are clear from Theorem 7. It is enough to prove the optimality. By (5), we get

$$\begin{aligned}&|\mathcal{Y}_1|\\ &\le \left\lfloor \frac{q+1}{w} \left\lfloor \frac{w}{q+1} \left\lfloor \frac{(q-1)w(w-1)L_1 + q - 2}{\frac{w}{q+1}\cdot(w-1)(w-2) + \frac{q+1-w}{q+1}\cdot w(w-1)} \right\rfloor \right\rfloor \right\rfloor\\ &\le \left\lfloor \frac{q+1}{w} \left\lfloor \frac{w}{q+1} \left((q+1)L_1 + \frac{(q+1)(q-2)}{w(w-1)(q-1)}\right) \right\rfloor \right\rfloor\\ &= \left\lfloor \frac{q+1}{w} \left(wL_1 + \left\lfloor \frac{q-2}{(w-1)(q-1)} \right\rfloor\right) \right\rfloor\\ &= (q+1)L_1.\end{aligned}$$

Therefore, $\mathcal{Y}_1$ is an optimal VW-OOC. □

The second new optimal class of VW-OOCs comes from the optimal $\left((u^2+u+1)^k, u+1, 1, 1\right)$ CW-OOC of size $\frac{(u^2+u+1)^k-1}{u(u+1)}$ in [20], where u is a prime power and $k \ge 1$.

Corollary 9: Let u be an odd prime power, and $\mathcal{X}_2$ an optimal $\left((u^2+u+1)^k, u+1, 1, 1\right)$ CW-OOC of size $L_2 \triangleq \frac{(u^2+u+1)^k-1}{u(u+1)}$. Let q be a prime power satisfying $\gcd(q-1, u^2+u+1) = 1$ and $q \ge u+1$. Then, the set $\mathcal{Y}_2$ obtained from $\mathcal{X}_2$ by Construction A is an optimal

$$\left((q-1)(u^2+u+1)^k, \{u, u+1\}, 1, \left\{\frac{u+1}{q+1}, \frac{q-u}{q+1}\right\}\right)$$

VW-OOC of size $(q+1)L_2$ for any $k \ge 1$.

Proof: In a similar way to the Proof of Corollary 8, we have

$$\begin{aligned}&|\mathcal{Y}_2|\\ &\le \left\lfloor \frac{q+1}{u+1} \left\lfloor \frac{u+1}{q+1} \left\lfloor \frac{(q-1)(u^2+u+1)^k - 1}{\frac{u+1}{q+1}\cdot u(u-1) + \frac{q-u}{q+1}\cdot(u+1)u} \right\rfloor \right\rfloor \right\rfloor\\ &\le \left\lfloor \frac{q+1}{u+1} \left\lfloor \frac{u+1}{q+1} \left((q+1)L_2 + \frac{(q+1)(q-2)}{(q-1)u(u+1)}\right) \right\rfloor \right\rfloor\\ &= \left\lfloor \frac{q+1}{u+1} \left((u+1)L_2 + \left\lfloor \frac{q-2}{(q-1)u} \right\rfloor\right) \right\rfloor.\\ &= (q+1)L_2.\end{aligned}$$

Therefore, $\mathcal{Y}_2$ is an optimal VW-OOC. □

Another new optimal class of VW-OOCs can be constructed from the optimal $\left(u^k-1, u, 1, 1\right)$ CW-OOC of size $u^{k-2} + u^{k-3} + \cdots + 1$ in [23], where u is a prime power and $k \ge 2$.

Corollary 10: Let u be a prime, and $\mathcal{X}_3$ an optimal $\left(u^k-1, u, 1, 1\right)$ CW-OOC of size $L_3 \triangleq u^{k-2} + u^{k-3} + \cdots + 1$, where $k \ge 2$. Let q be a prime power satisfying $\gcd(q-1, u^k-1) = 1$ and $q \ge u$. Then the set $\mathcal{Y}_3$ obtained from $\mathcal{X}_3$ by Construction A is an optimal $\left((q-1)(u^k-1), \{u-1, u\}, 1, \left\{\frac{u}{q+1}, \frac{q+1-u}{q+1}\right\}\right)$ VW-OOC of size $(q+1)L_3$ for any $k \ge 2$.

Proof: Note that

$$\begin{aligned}&\left\lfloor \frac{u}{q+1} \left\lfloor \frac{(q-1)(u^k-1) - 1}{\frac{u}{q+1}\cdot(u-1)(u-2) + \frac{q+1-u}{q+1}\cdot u(u-1)} \right\rfloor \right\rfloor\\ &= \left\lfloor \frac{u}{q+1} \left\lfloor (q+1)L_3 + \frac{q+1}{u} - \frac{q+1}{(q-1)u(u-1)} \right\rfloor \right\rfloor\\ &\le \left\lfloor \frac{u}{q+1} \left((q+1)L_3 + \frac{q+1}{u} - \frac{q+1}{(q-1)u(u-1)}\right) \right\rfloor\\ &= \left\lfloor uL_3 + 1 - \frac{1}{(q-1)(u-1)} \right\rfloor\\ &= uL_3.\end{aligned}$$

Hence, we have

$$\begin{aligned}
&|\mathcal{Y}_3| \\
&\le \left\lfloor \frac{q+1}{u} \left\lfloor \frac{u}{q+1} \right. \right. \\
&\quad \left. \left. \left\lfloor \frac{(q-1)(u^k-1)-1}{\frac{u}{q+1}\cdot(u-1)(u-2)+\frac{q+1-u}{q+1}\cdot u(u-1)} \right\rfloor \right\rfloor \right\rfloor \\
&\le \left\lfloor \frac{q+1}{u} \cdot uL_3 \right\rfloor \\
&= (q+1)L_3.
\end{aligned}$$

Therefore, $\mathcal{Y}_3$ is an optimal VW-OOC. □

In Corollaries 8–10, it is clear that there are infinitely many choices of q for a given optimal CW-OOC. Therefore, an infinite family of new optimal VW-OOCs can be generated from an optimal CW-OOC.

Example 11: Let $N = p = 61$, $w = 5$, $L = 3$, $q = 7$, and $\alpha = 3$ in Construction A. Let $\mathcal{X}_1 \triangleq \{X_1, X_2, X_3\}$ be the optimal $(61, 5, 1, 1)$ CW-OOC presented in [9], where the support of $X_a = \{X_a(t)\}_{t=0}^{60}$ for $0 \le a \le 2$ is given by

$$\begin{aligned}
\mathrm{supp}(X_0) &= \{1, 9, 20, 34, 58\}, \\
\mathrm{supp}(X_1) &= \{4, 14, 19, 36, 40\}, \\
\mathrm{supp}(X_2) &= \{13, 15, 16, 22, 56\}.
\end{aligned}$$

Let $\mathcal{Y}_1 \triangleq \{Y_{a,s} \mid 0 \le a \le 2,\ s \in \mathbb{F}_7 \cup \{\infty\}\}$ be the VW-OOC obtained by applying Construction A to $\mathcal{X}_1$. Then, the support of $Y_{a,s} \triangleq \{Y_{a,s}(t)\}_{t=0}^{365}$ is given by

$$\begin{aligned}
\mathrm{supp}(Y_{0,0}) &= \{(0,1), (1,9), (2,20), (3,34), (4,58)\}; \\
\mathrm{supp}(Y_{0,\alpha^0}) &= \{(0,20), (1,58), (2,9), (5,34)\}; \\
\mathrm{supp}(Y_{0,\alpha^1}) &= \{(0,58), (1,34), (3,20), (5,1)\}; \\
&\vdots \\
\mathrm{supp}(Y_{0,\alpha^5}) &= \{(0,34), (1,1), (3,58), (4,20), (5,9)\}; \\
\mathrm{supp}(Y_{0,\infty}) &= \{(0,1), (0,9), (0,20), (0,34), (0,58)\}; \\
\mathrm{supp}(Y_{1,0}) &= \{(0,4), (1,14), (2,19), (3,36), (4,49)\}; \\
&\vdots \\
\mathrm{supp}(Y_{2,\infty}) &= \{(0,13), (0,15), (0,16), (0,22), (0,56)\}
\end{aligned}$$

where (t_0, t_1) denotes t via $t_0 = \langle t \rangle_6$ and $t_1 = \langle t \rangle_{61}$. It is easily checked that $\mathcal{Y}_1$ is a $\left(366, \{4,5\}, 1, \left\{\frac{5}{8}, \frac{3}{8}\right\}\right)$ VW-OOC of size 24. Furthermore, it is optimal with respect to the bound (5) since

$$\left\lfloor \frac{8}{3} \left\lfloor \frac{3}{8} \left\lfloor \frac{366-1}{\frac{5}{8}\cdot 4\cdot 3+\frac{3}{8}\cdot 5\cdot 4} \right\rfloor \right\rfloor \right\rfloor = 24.$$

In a similar way, an infinite family of optimal VW-OOCs can be obtained from $\mathcal{X}_1$, including an optimal $\left(427, \{4,5\}, 1, \left\{\frac{5}{9}, \frac{4}{9}\right\}\right)$ VW-OOC of size 27 by choosing $q = 8$, an optimal $\left(488, \{4,5\}, 1, \left\{\frac{1}{2}, \frac{1}{2}\right\}\right)$ VW-OOC of size 30 by choosing $q = 9$, and so on. ■

IV. Concluding Remarks

We presented a new generic construction for VW-OOCs of length $(q-1)N$. As a result, we obtained three new families of optimal VW-OOCs. For practical applications, this construction can provide optimal VW-OOCs with high weights, while the previously known constructions except for the construction by Yang in [25] cover only weights less than or equal to 7.

Acknowledgment

The authors would like to thank anonymous reviewers and Associate Editor, Prof. Sihem Mesnager for their valuable comments that helped to improve the presentation of the paper.

References

[1] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks. I. Fundamental principles," *IEEE Trans. Commun.*, vol. 37, no. 8, pp. 824–833, Aug. 1989.
[2] J. A. Salehi and C. A. Brackett, "Code division multiple-access techniques in optical fiber networks. II. Systems performance analysis," *IEEE Trans. Commun.*, vol. 37, no. 8, pp. 834–850, Aug. 1989.
[3] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis and applications," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 595–604, May 1989.
[4] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA, USA: Aegean Park, 1982.
[5] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. London, U.K.: Research Studies Press, 1996.
[6] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. Huffman, Eds. Amsterdam, The Netherlands: North Holland, 1998, ch. 21, pp. 1765–1853.
[7] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[8] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inf. Theory*, vol. 8, no. 3, pp. 203–207, Apr. 1962.
[9] R. M. Wilson, "Cyclotomy and difference families in elementary abeilan groups," *J. Number Theory*, vol. 4, no. 1, pp. 17–47, Jan. 1972.
[10] H. Chung and P. V. Kumar, "Optical orthogonal codes-new bounds and an optimal construction," *IEEE Trans. Inf. Theory*, vol. 36, no. 4, pp. 866–873, Jul. 1990.
[11] G.-C. Yang and T. E. Fuja, "Optical orthogonal codes with unequal auto- and cross-correlation constraints," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 96–106, Jan. 1995.
[12] G.-C. Yang, "Some new families of optical orthogonal codes for code-division multiple-access fibre-optic networks," *IEE Proc.-Commun.*, vol. 142, no. 6, pp. 363–368, Dec. 1995.
[13] O. Moreno, Z. Zhang, P. V. Kumar, and V. Zinoviev, "New constructions of optimal cyclically permutable constant weight codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 448–455, Mar. 1995.
[14] M. Buratti, "From a $(G, k, 1)$ to a $(C_k \oplus G, k, 1)$ difference family," *Design, Codes Cryptogr.*, vol. 11, pp. 5–9, Apr. 1997.
[15] J. Yin, "Some combinatorial constructions for optical orthogonal codes," *Discrete Math.*, vol. 185, pp. 201–219, Apr. 1998.
[16] R. Fuji-Hara and Y. Miao, "Optical orthogonal codes: Their bounds and new optimal constructions," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2396–2406, Nov. 2000.
[17] G. Ge and J. Yin, "Constructions for optimal $(v, 4, 1)$ optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2998–3004, Nov. 2001.
[18] M. Buratti, "Cyclic designs with block size 4 and related optimal optical orthogonal codes," *Designs, Codes Cryptogr.*, vol. 26, pp. 111–125, Jun. 2002.
[19] Y. Chang, R. Fuji-Hara, and Y. Miao, "Combinatorial constructions of optimal optical orthogonal codes with weight 4," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1283–1292, May 2003.
[20] W. Chu and S. W. Golomb, "A new recursive construction for optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3072–3076, Nov. 2003.

[21] S. Ma and Y. Chang, "A new class of optimal optical orthogonal codes with weight five," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1848–1850, Aug. 2004.
[22] S. Ma and Y. Chang, "Constructions of optimal optical orthogonal codes with weight five," *J. Combinat. Designs*, vol. 13, no. 1, pp. 54–69, Jan. 2005.
[23] O. Moreno, R. Omrani, P. V. Kumar, and H.-F. Lu, "A generalized Bose–Chowla family of optical orthogonal codes and distinct difference sets," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1907–1910, May 2007.
[24] J.-H. Chung and K. Yang, "Asymptotically optimal optical orthogonal codes with new parameters," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3999–4005, Jun. 2013.
[25] G.-C. Yang, "Variable-weight optical orthogonal codes for CDMA networks with multiple performance requirements," *IEEE Trans. Commun.*, vol. 44, no. 1, pp. 47–55, Jan. 1996.
[26] D. Wu, P. Fan, H. Li, and U. Parampalli, "Optimal variable-weight optical orthogonal codes via cyclic difference families," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seoul, Korea, Jun./Jul. 2009, pp. 448–452.
[27] H. Zhao, D. Wu, and P. Fan, "Consturctions of optimal variable-weight optical orthogonal codes," *J. Comb. Des.*, vol. 18, no. 4, pp. 274–291, Jul. 2010.
[28] D. Wu, H. Zhao, P. Fan, and S. Shinohara, "Optimal variable-weight optical orthogonal codes via difference packings," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4053–4060, Aug. 2010.
[29] J. Jiang, D. Wu, and P. Fan, "General constructions of optimal variable-weight optical orthogonal codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4488–4496, Jul. 2011.
[30] M. Buratti, Y. Wei, D. Wu, P. Fan, and M. Cheng, "Relative difference families with variable block sizes and their related OOCs," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7489–7497, Nov. 2011.
[31] D. Wu, P. Fan, X. Wang, and M. Cheng, "New classes of optimal variable-weight optical orthogonal codes based on cyclic difference families," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 93-A, no. 11, pp. 2232–2238, Nov. 2010.
[32] R. J. R. Abel and M. Buratti, "Difference families," in *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., 2nd ed. London, U.K.: Chapman & Hall, 2006, ch. VI-16, pp. 392–410.
[33] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996.

Jin-Ho Chung (M'13) received the B.S., M.S. and Ph.D. degrees in electronics and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 2005, 2007, and 2011, respectively.

He was a postdoctoral researcher in Communications and Signal Design Laboratory, Department of Electrical Engineering, POSTECH from March 2011 to February 2013. He joined the faculty of the Ulsan National Institute of Science and Technology (UNIST) in February 2013, where he is currently an Assistant Professor in the School of Electrical and Computer Engineering. From April 2013 to February 2014, he was a visiting assistant professor at the University of Waterloo. His current research interests include sequences, coding theory, and wireless communication systems.

Kyeongcheol Yang (S'87–M'93–SM'12) received the B.S. and M.S. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1986 and 1988, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, in 1992.

During the summer of 1990, he was with Bellcore, Morristown, NJ, as an intern. From March 1993 to January 1999, he was an Assistant Professor in the Department of Electronic Communication Engineering, Hanyang University, Seoul, Korea. He joined the faculty of the Pohang University of Science and Technology (POSTECH) in February 1999, where he is currently a Professor in the Department of Electrical Engineering. During his sabbatical year in 2006, he was a technical consultant at Telecommunication R&D Center, Samsung Electronics Co., Suwon, Korea. His research interests include coding theory, signal design, iterative information processing, and communication systems.

Dr. Yang was Program Co-Chair at the International Conference on Sequences and Their applications (SETA'01), and Program Co-Chair at the Fifth International Workshop on Signal Design and Its Applications in Communications (IWSDA'11). He is currently an Associate Editor of IEEE TRANSACTIONS ON INFORMATION THEORY, and an Associate Editor of *Cryptography and Communications*.