Near-Optimal Partial Hadamard Codebook Construction Using Binary Sequences Obtained From Quadratic Residue Mapping

Seokbeom Hong, Hosung Park, Jong-Seon No, *Fellow, IEEE*, Tor Helleseth, *Fellow, IEEE*, and Young-Sik Kim, *Member, IEEE*

***Abstract*— In this paper, a new class of (N, K) near-optimal partial Hadamard codebooks is proposed. The construction of the proposed codebooks from Hadamard matrices is based on binary row selection sequences, which are generated by quadratic residue mapping of p-ary m-sequences. The proposed codebooks have parameters $N = p^n$ and $K = (p - 1/2p)(N + \sqrt{N}) + 1$ for an odd prime p and an even positive integer n. We prove that the maximum magnitude of inner products between the code vectors of the proposed codebooks asymptotically achieves the Welch bound equality for sufficiently large p and derive their inner product distribution.**

***Index Terms*— Codebook, Hadamard matrix, sequences, quadratic residue, Welch bound.**

I. Introduction

A N (N, K) codebook $\mathcal{C} = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}\}$ is a set of N unit-norm complex vectors $\mathbf{c}_i \in \mathbb{C}^K$. Let $I_{\max}(\mathcal{C})$ be the maximum magnitude of inner products between a pair of distinct code vectors in $\mathcal{C}$. The Welch bound [1], a well-known lower bound on $I_{\max}(\mathcal{C})$, is given as

$$I_{\max}(\mathcal{C}) = \max_{0 \le l \ne k \le N-1} |\mathbf{c}_l^H \mathbf{c}_k| \ge \sqrt{\frac{N-K}{K(N-1)}} \tag{1}$$

Manuscript received June 28, 2013; revised January 19, 2014; accepted March 10, 2014. Date of publication March 28, 2014; date of current version May 15, 2014. This work was supported by the National Research Foundation of Korea through the Korean Government under Grant NRF-2009-0081441.

S. Hong was with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea. He is now with Samsung Electronics, Company, Ltd., Gyeonggi-do 445-701, Korea (e-mail: fousbyus@ccl.snu.ac.kr).

H. Park was with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea. He is now with the Department of Electrical and Computer Engineering, University of California, San Diego, CA 92093 USA (e-mail: hpark1@snu.ac.kr).

J.-S. No is with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea (e-mail: jsno@snu.ac.kr).

T. Helleseth is with the Department of Informatics, Selmer Center, University of Bergen, Bergen N-5020, Norway (e-mail: tor.helleseth@ii.uib.no).

Y.-S. Kim is with the Department of Information and Communication Engineering, Chosun University, Gwangju 501-759, Korea (e-mail: iamyskim@Chosun.ac.kr).

Communicated by K. Yang, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2014.2314298

where $\mathbf{c}_l^H$ denotes the conjugate transpose of $\mathbf{c}_l$. The equality in (1) is satisfied if and only if

$$|\mathbf{c}_l^H \mathbf{c}_k| = \sqrt{\frac{N-K}{K(N-1)}}$$

for any pair (l, k) with $l \ne k$. If $I_{\max}(\mathcal{C})$ achieves the Welch bound with equality, then $\mathcal{C}$ is called a maximum-Welch-bound-equality (MWBE) codebook [2] or an equiangular tight frame [3]. MWBE codebooks have been widely used for various applications, for example, code-division multiple-access (CDMA) communication systems [4], packing [5], [6], compressed sensing [7], coding theory [8], [9], and quantum computing [10].

However, the construction of an MWBE codebook is known to be very hard in general [2]. The following codebooks are the known classes of MWBE codebooks except nearly trivial cases, i.e., partial Fourier and Hadamard codebooks with $K = N$ or $N - 1$.

1) (N, K) MWBE codebooks based on conference matrices [5], [6], where $N = 2K = 2^{d+1}$ for a positive integer d or $N = 2K = p^d + 1$ for a prime p and a positive integer d.
2) (N, K) MWBE codebooks based on (N, K, λ) cyclic difference sets (DS) [11], or (N, K, λ) DS in finite fields or Abelian groups [12], [13].
3) (N, K) MWBE codebooks or equiangular tight frames based on $(2, k, v)$-Steiner systems [14].

It is easy to see that the known classes of MWBE codebooks exist for very restrictive N and K. To provide the flexibility choosing the parameters N and K, many researches have been done instead to construct near-optimal codebooks, i.e., codebook $\mathcal{C}$ whose $I_{\max}(\mathcal{C})$ nearly achieves the Welch bound with equality. Several classes of near-optimal codebooks using error correcting codes and pseudo noise (PN) sequences are proposed in [2]. As an extension of the MWBE codebooks based on DS, various types of near-optimal codebooks based on almost (or relative) DS and/or cyclotomic classes are proposed [12], [15]–[19]. Also, near-optimal codebooks constructed from binary row selection sequences (e.g. binary Sidelnikov sequences) are proposed in [20]. In a recently published paper [21], near-optimal codebooks are proposed based on DS and the product of abelian groups.

In this paper, we propose a new class of (N, K) near-optimal partial Hadamard codebooks. For an odd prime p and an even positive integer n, the proposed codebooks are constructed by selecting K rows from $p^n \times p^n$ $(= N \times N)$ p-ary Hadamard matrices based on binary row selection sequences. The row selection sequences are generated by applying the quadratic residue (QR) mapping to the short period p-ary m-sequences. The resulting codebooks have parameters $N = p^n$ and $K = \frac{p-1}{2p}(N + \sqrt{N}) + 1$. We prove that $I_{\max}(\mathcal{C})$ of the proposed codebook $\mathcal{C}$ is bounded by $\sqrt{2}$ times the Welch bound equality for the worst case $(p = 3)$ and asymptotically achieves the Welch bound equality for sufficiently large p. In addition, we derive the whole distribution of their inner products.

This paper is organized as follows. Section II introduces Hadamard matrices, QR mapping, and the basic concept of character theory. In Section III, we propose a construction method of near-optimal partial Hadamard codebooks using the QR mapping and derive the ratio of the maximum inner product of the proposed codebooks to that of MWBE codebooks. We prove the main theorem on the maximum magnitude of inner products between the code vectors of the proposed codebooks in Section IV. Finally, the conclusions are provided in Section V.

II. Preliminaries

In order to introduce the proposed codebook construction, some notations and definitions are presented in this section. Let m and n be positive integers such that $n = 2m$. Let p denote an odd prime and $T = p^m + 1$. Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \backslash \{0\}$. Let ω be the complex p-th root of unity, i.e., $\omega = e^{j\frac{2\pi}{p}}$, where $j = \sqrt{-1}$. For two integers k and l with $l|k$, the trace function $\mathrm{Tr}_l^k : \mathbb{F}_{p^k} \to \mathbb{F}_{p^l}$ is defined as

$$\mathrm{Tr}_l^k(x) = \sum_{i=0}^{k/l-1} x^{p^{li}}$$

where $x \in \mathbb{F}_{p^k}$.

Let $s(t)$ be the p-ary m-sequence of period $p^n - 1$ defined as

$$s(t) = \mathrm{Tr}_1^n(\alpha^t)$$

where $t = 0, 1, \ldots, p^n - 2$ and α is a primitive element of $\mathbb{F}_{p^n}$.

The complex Hadamard matrix constructed by p-ary m-sequences is defined as follows.

Definition 1 (Hadamard matrix): Let $H = [h_{i,j}]$ be the $p^n \times p^n$ p-ary Hadamard matrix defined as

$$h_{i,j} = \begin{cases} 1, & i = 0 \text{ or } j = 0 \\ \omega^{\mathrm{Tr}_1^n(\alpha^{i+j-2})}, & \text{otherwise} \end{cases}$$

for $0 \le i, j \le p^n - 1$. ■

Let QR_p and $QNR_p \subset \mathbb{F}_p^*$ denote the sets of QR and quadratic nonresidue (QNR) on $\mathbb{F}_p$, respectively, i.e.,

$$QR_p = \{x | x = y^2 \text{ for } y \in \mathbb{F}_p^*\}$$
$$QNR_p = \{x | x \neq y^2 \text{ for all } y \in \mathbb{F}_p\}.$$

Definition 2 (QR mapping): The QR mapping $q : \mathbb{F}_p \to \mathbb{F}_2$ is defined as

$$q(x) = \begin{cases} 0, & x \in QR_p \text{ or } x = 0 \\ 1, & x \in QNR_p \end{cases}$$

where $x \in \mathbb{F}_p$. ■

We introduce a fundamental theory of characters and Gauss sums which will be used in the proof in Section IV. For more details, see Chapter 5 of [22]. The canonical additive character ψ_1 of $\mathbb{F}_p$ is defined as

$$\psi_1(x) = \omega^x, \text{ for all } x \in \mathbb{F}_p.$$

All additive characters of $\mathbb{F}_p$ can be expressed in terms of ψ_1. In other words, for $a \in \mathbb{F}_p$, the character ψ_a such that $\psi_a(x) = \psi_1(ax)$ for all $x \in \mathbb{F}_p$ is an additive character of $\mathbb{F}_p$.

The canonical lifted additive character $\psi^{(n)} (= \psi_1^{(n)})$ of $\mathbb{F}_{p^n}$ is defined as

$$\psi^{(n)}(x) = \omega^{\mathrm{Tr}_1^n(x)} \text{ for all } x \in \mathbb{F}_{p^n}.$$

Other additive characters of $\mathbb{F}_{p^n}$ are defined in a similar way as in $\mathbb{F}_p$, i.e., for $a \in \mathbb{F}_{p^n}$, the character $\psi_a^{(n)}$ such that $\psi_a^{(n)}(x) = \psi_1^{(n)}(ax)$ for all $x \in \mathbb{F}_{p^n}$. The character sum of an additive character over the whole field satisfies

$$\sum_{x \in \mathbb{F}_{p^n}} \psi_a^{(n)}(x) = \begin{cases} p^n, & a = 0 \\ 0, & a \in \mathbb{F}_{p^n}^*. \end{cases}$$

A multiplicative character χ_i of $\mathbb{F}_{p^n}$ for each $i = 0, 1, \ldots, p^n - 2$ is defined as

$$\chi_i(\alpha^k) = e^{j2\pi ik/(p^n-1)} \text{ for } k = 0, 1, \ldots, p^n - 2$$

where α is a primitive element of $\mathbb{F}_{p^n}$ (Set $\chi_i(0) = 0$ for convenience). The character sum of a multiplicative character over $\mathbb{F}_{p^n}$ satisfies

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_i(x) = \sum_{x \in \mathbb{F}_{p^n}^*} \chi_i(x) = \begin{cases} p^n - 1, & i = 0 \\ 0, & \text{otherwise.} \end{cases}$$

When $i = (p^n - 1)/2$, χ_i is called as a quadratic character. A quadratic character η becomes a real-valued function with $\eta(x) = 1$ if $x \in QR_{p^n}$ and $\eta(x) = -1$ if $x \in QNR_{p^n}$.

The Gauss sum $G(\chi, \psi)$ for a multiplicative character χ and an additive character ψ of $\mathbb{F}_{p^n}$ is defined as

$$G(\chi, \psi) = \sum_{x \in F_{p^n}^*} \chi(x)\psi(x).$$

Some of known properties of Gauss sums are listed in the following lemma.

Lemma 1 ([22]): Gauss sums for the finite field $\mathbb{F}_{p^n}$ satisfy the following properties:

1) *$G(\chi, \psi_{xy}) = \overline{\chi(x)} G(\chi, \psi_y)$ for $x \in \mathbb{F}_{p^n}^*$, $y \in \mathbb{F}_{p^n}$, where $\overline{\chi(x)}$ denotes the complex conjugate of $\chi(x)$;*
2) *$G(\chi, \psi)G(\overline{\chi}, \psi) = \chi(-1)p^n$ for $\psi \neq \psi_0$;*
3) *$\chi(x) = \frac{1}{p^n} \sum_{\psi} G(\chi, \overline{\psi})\psi(x)$ for $x \in \mathbb{F}_{p^n}^*$, where the summation is over all additive characters ψ of $\mathbb{F}_{p^n}$.* ■

Finally, we will introduce a lemma which connects the inner products of a partial Hadamard codebook to the Hadamard

transforms of a row selection sequence. The following lemma is a direct consequence of Theorem 3 in [20] so that the proof is omitted.

Lemma 2: Let $\mathbf{a} = \{a_0, a_1, \ldots, a_{N-1}\}$ *be a binary row selection sequence with support* $D = \{d_0, d_1, \ldots, d_{K-1}\}$. *Let* $\mathcal{C}_H(\mathbf{a}) = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}\}$ *be an* (N, K) *partial Hadamard codebook consisting of the columns of the submatrix obtained by selecting* K *rows corresponding to* D *from* $p^n \times p^n$ *Hadamard matrix* $H = [h_{i,j}]$. *Let* $I_{i,j}(\mathcal{C}_H(\mathbf{a})) = |\mathbf{c}_i^H \mathbf{c}_j|$ *for distinct integers* i, j *such that* $0 \le i, j \le N-1$ *denote the magnitude of inner product between* i*-th and* j*-th code vector of the codebook. Then, for any pair* (i, j), *there exists* l, $1 \le l \le N-1$, *such that*

$$I_{i,j}(\mathcal{C}_H(\mathbf{a})) = \frac{1}{2K}|\widehat{a_l}|$$

and the number of pairs corresponding to each l, $1 \le l \le N-1$, *is exactly* N, *where* $\widehat{a_l} = \sum_{k=0}^{N-1}(-1)^{a_k} h_{k,l}$ *is the* l*-th element of the Hadamard transform of the row selection sequence* $\mathbf{a}$. ■

III. The Proposed Codebook Construction

In this section, we will introduce the proposed construction of a partial Hadamard codebook and show its near-optimality.

A. Construction of the Proposed Codebooks

From the definitions in Section II, the row selection sequences for the codebook construction from $p^n \times p^n$ Hadamard matrices are defined as follows by applying QR mapping to p-ary m-sequences of period $p^m - 1$.

Construction 1 (Row selection sequences): The binary row selection sequence $\mathbf{r} = \{r_0, r_1, \ldots, r_{p^n-1}\}$ *is defined as*

$$r_l = \begin{cases} q(\mathrm{Tr}_1^m(\alpha^{T(l-1)})), & 1 \le l \le p^n - 1 \\ 1, & l = 0 \end{cases}$$

where $T = p^m + 1$ *and* $q(\cdot)$ *is the QR mapping from* $\mathbb{F}_p$ *to* $\mathbb{F}_2$ *defined in Definition 2*. ■

Then we will propose the construction method of a new class of near-optimal partial Hadamard codebooks using Construction 1.

Construction 2 (Partial Hadamard codebooks): Let $N = p^n$ *and* $K = \frac{p-1}{2p}(N + \sqrt{N}) + 1$. *Let* $H = [h_{ij}]$ *be an* $N \times N$ *p-ary Hadamard matrix defined in Definition 1. Let* $D = \{d_0, d_1, \ldots, d_{K-1}\}$ *be the support of the binary row selection sequence* $\mathbf{r}$. *Then* $\mathcal{C}_H(\mathbf{r}) = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1}\}$ *is an* (N, K) *partial Hadamard codebook, where*

$$\mathbf{c}_l = \frac{1}{\sqrt{K}}(h_{d_0,l}, h_{d_1,l}, \ldots, h_{d_{K-1},l})^T, \quad 0 \le l \le N-1. \quad ■$$

It is easy to see that the construction using any τ cyclic shifted (except the first padded element 1) row selection sequences $r^{(\tau)} = \{r_0, r_{\tau+1}, r_{\tau+2}, \ldots, r_\tau\}$ of the sequence $\mathbf{r}$ in Construction 1 is equivalent to the proposed construction. Since the first column of the Hadamard matrix in Definition 1 is the all-one column and the other columns are shifted (except the first padded element 1) versions of each other, the cyclic shift of the row selection sequence $\mathbf{r}$ corresponds to reordering by the cyclic shift of the columns of the Hadamard matrix, which does not affect the structure of the resulting codebooks.

The proposed construction is motivated by construction of binary partial Hadamard MWBE codebooks using bent functions. A binary partial Hadamard codebook $\mathcal{C}_{\mathrm{bin}}$ constructed by binary row selection sequences which are associated with a trace-type bent function [23] is a MWBE codebook [13], [20]. In this case, the (N, K) codebook $\mathcal{C}_{\mathrm{bin}}$ has parameter $K = \frac{N \pm \sqrt{N}}{2}$. Since the Hadamard transform of the binary trace-type bent function has constant magnitude $\sqrt{N}$, it can be easily shown by Lemma 2 that $\mathcal{C}_{\mathrm{bin}}$ is a MWBE codebook.

For the p-ary case with odd prime p, the Hadamard transform of the p-ary Kasami-type generalized bent function $\mathrm{Tr}_1^m(\alpha^{Tl})$ [23] also has a constant magnitude. However, it is impossible to generalize the result of binary case to p-ary case directly because the row selection sequences have to be binary. Thus, we generate the binary row selection sequences in Construction 1 by applying QR mapping to the p-ary sequences associated with p-ary Kasami-type generalized bent function. Therefore, the proposed construction can be viewed as an extension of the construction of the codebook $\mathcal{C}_{\mathrm{bin}}$ to p-ary case even though the resulting codebooks are not MWBE but near-optimal.

Remark 1: When $n = 2$ *and* $m = 1$, *the parameters of the proposed construction become* $N = p^2$ *and* $K = \frac{N+1}{2}$. *Let* $\mathcal{C}$ *denote the resulting codebook by the proposed construction. Let an* (N, K) *codebook* $\mathcal{C}'$ *with* $N = p^2$ *and* $K = \frac{N-1}{2}$ *be a partial Hadamard codebook constructed by complementary row selection sequence* $\mathbf{r}' = \{r'_0, r'_1, \ldots, r'_{p^n-1}\}$ *such that* $r'_l = 1 - r_l$ *for* $l = 0, 1, \ldots, p^n - 1$. *Then, it can be easily shown by Lemma 2 that* $\mathcal{C}'$ *has exactly the same inner product distribution as* $\mathcal{C}$ *before normalization by size of code vector* K. *Since* α^{p+1} *is a primitive element of* $\mathbb{F}_p$, $q(\mathrm{Tr}_1^m(\alpha^{Tl})) = q(\alpha^{(p+1)l})$ *is* 1 *if* l *is odd, and* 0, *otherwise. Thus, the support set of the row selection sequence* $\mathbf{r}$ *of codebook* $\mathcal{C}$ *consists of even-numbered (including* 0*) indices, i.e.,* $r_i = 1$ *for even* i *and* $r_i = 0$ *for odd* i. *In contrast, the support set of the sequence* $\mathbf{r}'$ *of codebook* $\mathcal{C}'$ *consists of odd-numbered indices. Then it is directly followed that the codebook* $\mathcal{C}'$ *is the same as the near-optimal codebook by Paley partial DS proposed in [12]. Thus, for* $n = 2$ *case, the proposed construction is equivalent to the near-optimal codebook construction using Paley partial DS in [12].*

However, for $n > 2$ *case, the proposed codebooks are not equivalent to the MWBE or near-optimal codebooks known in the literature. In Table I, we compare the values of* K *of the proposed codebooks with* $n > 2$ *and those of other conventional MWBE and near-optimal codebooks for the same* $N(= p^n)$. *It is easy to see that, at least for small* p *and* n, *the proposed construction results the codebooks with new parameters which cannot be constructed from the conventional construction methods for MWBE and near-optimal codebooks.*

B. Near-Optimality of the Proposed Codebooks

In this subsection, we derive the whole distribution of inner products of the proposed codebooks. In addition, we derive the ratio of $I_{\max}$ of the proposed codebooks to that of

TABLE I
PARAMETER K OF THE PROPOSED CODEBOOKS WITH $n > 2$ AND OTHER CODEBOOKS FOR THE SAME N

p	n	N	Values of K for the given N						
			Proposed	MWBE		Near-optimal ($l = 1, 2, 3, 4$)			
				[14]	[13]	[16]	[12],[20]	[21]	[17]
3	4	81	31	36	40	32	40	-	$10l$
3	6	729	253	351	364	338	364	364	$91l$
3	8	6561	2215	3240	3280	3200	3280	-	$820l$
5	4	625	261	300	-	288	312	-	$78l$
5	6	15625	6301	7750	-	7688	7812	-	$1953l$
7	4	2401	1051	1176	-	1152	1200	-	$300l$
11	4	14641	6711	7260	-	7200	7320	-	$1830l$

the MWBE codebooks and show that $I_{\max}$ of the proposed codebooks asymptotically achieves the Welch bound equality for sufficiently large p.

The following theorem gives the whole distribution of $I_{i,j}$ for the proposed codebooks $\mathcal{C}_H(\mathbf{r})$. The proof of Theorem 1 will be given in Section IV.

Theorem 1: The magnitude $I_{i,j}(\mathcal{C}_H(\mathbf{r}))$ of inner products between a pair of code vectors of the proposed codebooks for distinct i, j such that $0 \le i, j \le N-1$ has the following distribution

$$I_{i,j}(\mathcal{C}_H(\mathbf{r})) = \begin{cases} \frac{1}{K}\cdot\frac{p+1}{2p}\sqrt{N}, & \frac{p+1}{2p}N^2 - \frac{p-1}{2p}N^{3/2} - N \text{ times} \\ \frac{1}{K}\cdot\frac{p-1}{2p}\sqrt{N}, & \frac{p-1}{2p}(N^2 + N^{3/2}) \text{ times} \end{cases}$$

for $n = 2$, and

$$I_{i,j}(\mathcal{C}_H(\mathbf{r})) = \begin{cases} \frac{1}{K}\cdot\left(\frac{p+1}{2p}\sqrt{N} - 1\right), & \frac{p+1}{2p}N^2 - \frac{p-1}{2p}N^{3/2} - N \text{ times} \\ \frac{1}{K}\cdot\left(\frac{p-1}{2p}\sqrt{N} + 1\right), & \frac{p-1}{2p}(N^2 + N^{3/2}) \text{ times} \end{cases}$$

for $n > 2$. ■

The following corollary which is a direct consequence of Theorem 1 gives the upper bound of $I_{\max}$ for the proposed codebooks $\mathcal{C}_H(\mathbf{r})$.

Corollary 1: The maximum magnitude $I_{\max}(\mathcal{C}_H(\mathbf{r}))$ of inner products between a pair of code vectors of the proposed codebooks is upper bounded by

$$I_{\max}(\mathcal{C}_H(\mathbf{r})) \le \frac{1}{K}\cdot\frac{(p+1)\sqrt{N}}{2p}.$$ ■

Using Corollary 1, we can derive the ratio of $I_{\max}$ of the proposed codebooks to that of the MWBE codebooks and show the near-optimality of the proposed codebooks as in the following theorem.

Theorem 2: Let I_{Welch} be the magnitude of the optimal correlation, i.e., the Welch bound equality, for the given N, K in the proposed construction. Then,

$$1 \le \frac{I_{\max}(\mathcal{C}_H(\mathbf{r}))}{I_{\text{Welch}}} < \sqrt{\frac{p+1}{p-1}}.$$

Proof: It is easy to derive that

$$\begin{aligned} \frac{I_{\max}(\mathcal{C}_H(\mathbf{r}))}{I_{\text{Welch}}} &\le \sqrt{\frac{K(N-1)}{N-K}}\cdot\frac{1}{K}\cdot\frac{(p+1)\sqrt{N}}{2p} \\ &= \sqrt{\frac{p^{n-2}(p^n-1)(p+1)^2}{[(p-1)(p^{n-1}+p^{m-1})+2]}} \\ &\quad\cdot\sqrt{\frac{1}{[(p+1)p^{n-1}-(p-1)p^{m-1}-2]}} \\ &< \sqrt{\frac{p^{n-2}(p^n-1)(p+1)^2}{[(p-1)(p^{n-1}+p^{m-1})][(p+1)p^{n-1}-(p+1)p^{m-1}]}} \\ &= \sqrt{\frac{p^{n-2}(p^n-1)(p+1)^2}{(p-1)(p+1)p^{n-2}(p^m-1)(p^m+1)}} \\ &= \sqrt{\frac{p+1}{p-1}} \end{aligned} \tag{2}$$

where (2) follows by $(p+1)p^{m-1} = (p-1)p^{m-1} + 2p^{m-1} \ge (p-1)p^{m-1} + 2$. Clearly, we have $I_{\text{Welch}} \le I_{\max}(\mathcal{C}_H(\mathbf{r}))$. Thus we prove it. ■

From Theorem 2, it is easy to see that $I_{\max}$ of the proposed codebooks asymptotically achieves the Welch bound equality for sufficiently large p. For small p, $I_{\max}$ of the proposed codebooks has larger value than the Welch bound equality. However, $I_{\max}/I_{\text{Welch}}$ is smaller than $\sqrt{2} \approx 1.414$ for the worst case, i.e., $p = 3$, and the ratio of $I_{\max}$ of the proposed codebooks to that of the MWBE codebooks is rapidly decreasing with increasing p. For example, $I_{\max}/I_{\text{Welch}} < \sqrt{3/2} \approx 1.225$ for $p = 5$, $I_{\max}/I_{\text{Welch}} < \sqrt{4/3} \approx 1.155$ for $p = 7$, and $I_{\max}/I_{\text{Welch}} < \sqrt{6/5} \approx 1.095$ for $p = 11$, and so on.

Remark 2: It is shown by Theorem 2 that $I_{\max}$ of the proposed codebooks asymptotically achieves the Welch bound equality as p increases. However, unfortunately, near-optimality of the proposed construction is not always guaranteed only with sufficiently large order ($= p^n$) of the Hadamard matrix used in the construction. When n increases and p is fixed, it is easy to see that $I_{\max}$ of the proposed codebooks approaches to $\sqrt{\frac{p+1}{p-1}}$ times the Welch bound equality because the difference occurred from approximation in (2) becomes negligible with sufficiently large n. Comparison of $I_{\max}/I_{\text{Welch}}$ between the proposed codebooks and the other near-optimal codebooks in the literature for various p and n is listed in Table II. (It is hard to say that the comparison in Table II is fair because the value of K of the codebooks are different. The comparison is presented only for reference.) For small p and large n, the proposed codebooks is worse than the other near-optimal codebooks in terms of $I_{\max}/I_{\text{Welch}}$. However, when p increases, $I_{\max}/I_{\text{Welch}}$ of the proposed codebooks approaches to that of the other near-optimal codebooks.

IV. PROOF OF THE THEOREM 1

In this section, we will prove the upper bound on $I_{\max}$ of the proposed codebooks in Theorem 1. Let $\eta(x)$

TABLE II
COMPARISON OF $I_{\max}/I_{\text{Welch}}$ BETWEEN THE PROPOSED CODEBOOKS AND THE OTHER NEAR-OPTIMAL CODEBOOKS

p	n	N	Proposed		[16]		[12],[20]	
			K	$I_{\max}/I_{\text{Welch}}$	K	$I_{\max}/I_{\text{Welch}}$	K	$I_{\max}/I_{\text{Welch}}$
3	2	9	5	1.265	2	1.512	4	1.265
3	4	81	31	1.136	32	1.129	40	1.104
3	6	729	253	1.322	338	1.039	364	1.036
5	2	25	13	1.177	8	1.260	12	1.177
5	4	625	261	1.135	288	1.042	312	1.039
7	2	49	25	1.131	18	1.173	24	1.131
7	4	2401	1051	1.110	1152	1.021	1200	1.020
11	2	121	61	1.086	50	1.103	60	1.086

denote the quadratic character of $\mathbb{F}_p$ and let $\psi(x)$ denote the additive canonical character of $\mathbb{F}_p$. Let $\psi^{(n)}(x) = \omega^{\text{Tr}_1^n(x)}$ denote the lifted additive character of $\mathbb{F}_{p^n}$. Several following lemmas are needed for the proof of Theorem 1.

Lemma 3: Let $S_{a,b} = \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\text{Tr}_1^n(ax)+b\text{Tr}_1^m(x^T)}$ *where* $a \in \mathbb{F}_{p^n}$ *and* $b \in \mathbb{F}_p^*$. *Then, we have*

$$S_{a,b} = -p^m \omega^{-\text{Tr}_1^m\left(\frac{a^T}{b}\right)} - 1.$$

Proof: It holds that

$$\begin{aligned} S_{a,b} &= \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\text{Tr}_1^m(ax+a^{p^m}x^{p^m}+bx^T)} \\ &= \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\text{Tr}_1^m(b((x+\frac{a^{p^m}}{b})^T-\frac{a^T}{b^2}))}. \end{aligned} \tag{3}$$

Since

$$\sum_{x\in\mathbb{F}_{p^n}} \omega^{\text{Tr}_1^m(cx^T)} = 1 + T\sum_{z\in\mathbb{F}_{p^m}^*} \omega^{\text{Tr}_1^m(cz)} = 1 - p^m - 1 = -p^m$$

where $c \in \mathbb{F}_{p^m}^*$, (3) can be rewritten as

$$\begin{aligned} S_{a,b} &= \omega^{-\text{Tr}_1^m(\frac{a^T}{b})} \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\text{Tr}_1^m(b((x+\frac{a^{p^m}}{b})^T))} \\ &= \omega^{-\text{Tr}_1^m(\frac{a^T}{b})}(-p^m - \omega^{\text{Tr}_1^m(\frac{a^T}{b})}) \\ &= -p^m\omega^{-\text{Tr}_1^m(\frac{a^T}{b})} - 1. \end{aligned}$$ ■

The above lemma can also be proved by similar approaches used in [23] and [24].

Lemma 4: Let $U = \sum_{x\in\mathbb{F}_{p^n}^*} \psi^{(n)}(ax) I(\text{Tr}_1^m(x^T))$ *where* $a \in \mathbb{F}_{p^n}^*$ *and* $I(z) = 1$ *for* $z = 0$ *and* $I(z) = 0$, *otherwise.* Then we have

$$U = \begin{cases} -1 + p^{m-1}, & \text{if } \text{Tr}_1^m(a^T) \neq 0 \\ -1 - p^{m-1}(p-1), & \text{if } \text{Tr}_1^m(a^T) = 0. \end{cases}$$

Proof: It follows that

$$\begin{aligned} U &= \sum_{x\in\mathbb{F}_{p^n}^*, \text{Tr}_1^m(x^T)=0} \omega^{\text{Tr}_1^n(ax)} \\ &= \frac{1}{p}\sum_{b\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\text{Tr}_1^n(ax)+b\text{Tr}_1^m(x^T)} \\ &= \frac{1}{p}(-1 + \sum_{b\in\mathbb{F}_p^*}(-p^m\omega^{-\text{Tr}_1^m\left(\frac{a^T}{b}\right)} - 1)) \\ &= -1 - p^{m-1}\sum_{b\in\mathbb{F}_p^*} \omega^{-\text{Tr}_1^m\left(\frac{a^T}{b}\right)} \end{aligned} \tag{4}$$

where (4) is obtained from the fact that

$$\sum_{b\in\mathbb{F}_p} \omega^{b\text{Tr}_1^m(x^T)} = \begin{cases} p, & \text{if } \text{Tr}_1^m(x^T) = 0 \\ 0, & \text{otherwise.} \end{cases}$$

The result in the two cases now follows directly depending on the value of $\text{Tr}_1^m(\frac{a^T}{b})$. ■

Lemma 5: Let $R = \sum_{x\in\mathbb{F}_{p^n}^*} \eta(\text{Tr}_1^m(x^T))\psi^{(n)}(ax)$ *where* $a \in \mathbb{F}_{p^n}^*$. *Then we have*

$$R = \begin{cases} -p^m\eta(-\text{Tr}_1^m(a^T)), & \text{if } \text{Tr}_1^m(a^T) \neq 0 \\ 0, & \text{if } \text{Tr}_1^m(a^T) = 0. \end{cases}$$

Proof: R can be rewritten as

$$R = \frac{1}{p}\sum_{x\in\mathbb{F}_{p^n}^*}\sum_{b\in\mathbb{F}_p} G(\eta, \overline{\psi_b})\psi_b(\text{Tr}_1^m(x^T))\psi^{(n)}(ax) \tag{5}$$

$$\begin{aligned} &= \frac{1}{p}\sum_{b\in\mathbb{F}_p} G(\eta, \overline{\psi_b}) \sum_{x\in\mathbb{F}_{p^n}^*} \omega^{\text{Tr}_1^n(ax)+b\text{Tr}_1^m(x^T)} \\ &= \frac{1}{p}\sum_{b\in\mathbb{F}_p} G(\eta, \psi_{-b}) S_{a,b} \\ &= -p^{m-1}\sum_{b\in\mathbb{F}_p^*} G(\eta, \psi_{-b})\omega^{-\frac{1}{b}\text{Tr}_1^m(a^T)} - \frac{1}{p}\sum_{b\in\mathbb{F}_p^*} G(\eta, \psi_{-b}) \end{aligned} \tag{6}$$

$$= -p^{m-1}\sum_{b\in\mathbb{F}_p^*} G(\eta, \psi_{-b})\omega^{-\frac{1}{b}\text{Tr}_1^m(a^T)} \tag{7}$$

where (5) follows directly by 3) of Lemma 1, (6) follows because $G(\eta, \psi_0)S_{a,0} = 0$, and (7) can be derived from

$$\begin{aligned} \sum_{b\in\mathbb{F}_p^*} G(\eta, \psi_{-b}) &= \sum_{b\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_p^*} \eta(x)\psi(-bx) \\ &= \sum_{x\in\mathbb{F}_p^*} \eta(x)\sum_{b\in\mathbb{F}_p^*} \psi(-bx) = 0. \end{aligned}$$

Now we will consider two cases to compute the value of R.

Case 1) $\text{Tr}_1^m(a^T) = 0$;

Clearly, we have

$$R = -p^{m-1} \sum_{b \in \mathbb{F}_p^*} G(\eta, \psi_{-b}) = 0.$$

Case 2) $\mathrm{Tr}_1^m(a^T) \neq 0$;

Let $k = \mathrm{Tr}_1^m(a^T)$. Note that the quadratic character η of $\mathbb{F}_p$ is real-valued and $\eta(x) = \eta(\frac{1}{x})$ for $x \in \mathbb{F}_p^*$. Then we have

$$\begin{aligned} R &= -p^{m-1} \sum_{b \in \mathbb{F}_p^*} G(\eta, \psi_{-b}) \omega^{-\frac{1}{b}\mathrm{Tr}_1^m(a^T)} \\ &= -p^{m-1} \sum_{b \in \mathbb{F}_p^*} \eta(-b) G(\eta, \psi) \omega^{-\frac{k}{b}} \quad (8) \\ &= -p^{m-1} G(\eta, \psi) \sum_{b \in \mathbb{F}_p^*} \eta(-\frac{1}{b}) \psi(-\frac{k}{b}) \\ &= -p^{m-1} G(\eta, \psi) \eta(k) G(\eta, \psi) \quad (9) \\ &= -p^{m-1} \eta(k) \eta(-1) p \quad (10) \\ &= -p^m \eta(-\mathrm{Tr}_1^m(a^T)). \end{aligned}$$

Equations (8) and (10) follow by 1) and 2) of Lemma 1, respectively and (9) follows because

$$\sum_{b \in \mathbb{F}_p^*} \eta(-\frac{1}{b}) \psi(-\frac{k}{b}) = G(\eta, \psi_k) = \eta(k) G(\eta, \psi). \quad \blacksquare$$

Using Lemmas 4 and 5, we derive the cross-correlation distribution between the p-ary m-sequences and the binary sequences generated by applying QR mapping to short period p-ary m-sequences, $\mathrm{Tr}_1^m(\alpha^{Tt})$, in the following lemma.

Lemma 6: Let

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_1^n(\alpha^{t+\tau})} \cdot (-1)^{r_{t+1}} \\ &= \sum_{x \in \mathbb{F}_{p^n}^*} \psi^{(n)}(ax) \cdot (-1)^{q(\mathrm{Tr}_1^m(x^T))} \end{aligned}$$

for $\tau = 0, 1, \ldots, p^n - 2$, where $a \in \mathbb{F}_{p^n}^*$ and α is a primitive element of $\mathbb{F}_{p^n}$. Then, $C(\tau)$ has the following distribution

$$C(\tau) = \begin{cases} -p^m + p^{m-1} - 1, & \frac{p+1}{2p} p^n - \frac{p-1}{2p} p^m - 1 \text{ times} \\ p^m + p^{m-1} - 1, & \frac{p-1}{2p}(p^n + p^m) \text{ times.} \end{cases}$$

Proof: $C(\tau)$ can be rewritten as

$$\begin{aligned} C(\tau) &= \sum_{x \in \mathbb{F}_{p^n}^*} \psi^{(n)}(ax) \cdot (-1)^{q(\mathrm{Tr}_1^m(x^T))} \\ &= \sum_{x \in \mathbb{F}_{p^n}^*} \psi^{(n)}(ax)(\eta(\mathrm{Tr}_1^m(x^T)) + I(\mathrm{Tr}_1^m(x^T))) \quad (11) \\ &= R + U \quad (12) \end{aligned}$$

where (11) follows because $(-1)^{q(\mathrm{Tr}_1^m(x^T))} = \eta(\mathrm{Tr}_1^m(x^T)) + I(\mathrm{Tr}_1^m(x^T))$.

Case 1) $\mathrm{Tr}_1^m(a^T) = 0$;

By Lemmas 4 and 5, $R = 0$ and $U = -1 - p^{m-1}(p-1)$ in this case and therefore, we have

$$C(\tau) = -p^m + p^{m-1} - 1.$$

Case 2) $\mathrm{Tr}_1^m(a^T) \neq 0$;

By Lemmas 4 and 5, $R = -p^m \eta(-\mathrm{Tr}_1^m(a^T))$ and $U = -1 + p^{m-1}$ and therefore, we have

$$C(\tau) = -p^m \eta(-\mathrm{Tr}_1^m(a^T)) + p^{m-1} - 1.$$

Hence in this case, we have

$$C(\tau) = \begin{cases} -p^m + p^{m-1} - 1, & \text{if } \eta(-\mathrm{Tr}_1^m(a^T)) = 1 \\ p^m + p^{m-1} - 1, & \text{if } \eta(-\mathrm{Tr}_1^m(a^T)) = -1. \end{cases} \quad (13)$$

To find the distribution, we need to find how often each of the cases occurs. Case 1) occurs for any $a \in \mathbb{F}_{p^n}^*$ such that $\mathrm{Tr}_1^m(a^T) = 0$. This occurs $T(p^{m-1} - 1)$ times, because the number of different $z \in \mathbb{F}_{p^m}^*$ with trace zero is $p^{m-1} - 1$ and there are T different $a \in \mathbb{F}_{p^n}^*$ which satisfy $z = a^T$.

The two cases in (13) of Case 2) occur equally often $\frac{p-1}{2} p^{m-1} T = \frac{p-1}{2p}(p^n + p^m)$ times because the number of squares and nonsquares in $\mathbb{F}_p$ are the same as $\frac{p-1}{2}$. $\blacksquare$

Proof of Theorem 1: By Lemma 2, for each $l = 1, 2, \ldots, N-1$, there exist N distinct pairs of (i, j) which satisfy

$$\begin{aligned} I_{i,j}(\mathcal{C}_H(\mathbf{r})) &= \frac{1}{2K} |\widehat{r_l}| \\ &= \frac{1}{2K} \left| \sum_{i=0}^{p^n-1} (-1)^{r_i} h_{i,l} \right| \\ &= \frac{1}{2K} \left| -1 + \sum_{i=0}^{p^n-2} (-1)^{r_{i+1}} \omega^{\mathrm{Tr}_1^n(\alpha^{i+l-1})} \right| \\ &= \frac{1}{2K} \left| -1 + C(l-1) \right|. \quad (14) \end{aligned}$$

By Lemma 6, the distribution of $I_{i,j}$ becomes

$$I_{i,j}(\mathcal{C}_H(\mathbf{r})) = \begin{cases} \frac{1}{K} \cdot \frac{p+1}{2p} \sqrt{N}, & \frac{p+1}{2p} N^2 - \frac{p-1}{2p} N^{3/2} - N \text{ times} \\ \frac{1}{K} \cdot \frac{p-1}{2p} \sqrt{N}, & \frac{p-1}{2p}(N^2 + N^{3/2}) \text{ times} \end{cases}$$

for $n = 2$, and

$$I_{i,j}(\mathcal{C}_H(\mathbf{r})) = \begin{cases} \frac{1}{K} \cdot \left(\frac{p+1}{2p} \sqrt{N} - 1 \right), & \frac{p+1}{2p} N^2 - \frac{p-1}{2p} N^{3/2} - N \text{ times} \\ \frac{1}{K} \cdot \left(\frac{p-1}{2p} \sqrt{N} + 1 \right), & \frac{p-1}{2p}(N^2 + N^{3/2}) \text{ times} \end{cases}$$

for $n > 2$. $\blacksquare$

In Definition 2, the QR mapping is defined as $q(x) = 0$ for $x = 0$. Assume that QR mapping is alternatively defined as $q(x) = 1$ for $x = 0$. In this case, since $(-1)^{q(\mathrm{Tr}_1^m(x^T))} = \eta(\mathrm{Tr}_1^m(x^T)) - I(\mathrm{Tr}_1^m(x^T))$, (12) becomes $C(\tau) = R - U$. Then the distribution of $C(\tau)$ will be changed as

$$C(\tau) = \begin{cases} p^m - p^{m-1} + 1, & \frac{p+1}{2p} p^n - \frac{p-1}{2p} p^m - 1 \text{ times} \\ -p^m - p^{m-1} + 1, & \frac{p-1}{2p}(p^n + p^m) \text{ times.} \end{cases}$$

Above distribution is almost the same as the result of Lemma 6 except their sign change. However, the value of the maximal inner product before normalization by K becomes slightly

larger than the proposed codebooks for $n > 2$ because the maximal value of $|-1 + C(l-1)|$ in (14) for $l = 1, 2, \ldots, N-1$ is altered from $p^m + p^{m-1} - 2$ to $p^m + p^{m-1}$. Despite the increase in the maximal inner product, $I_{\max}$ of resulting codebooks constructed from modified QR mapping still satisfies Corollary 1 and Theorem 2, i.e., the resulting codebooks are still near-optimal codebooks.

In Construction 1, the row selection sequence $\mathbf{r}$ is defined as $r_l = 1$ for $l = 0$. Similarly, consider the case that the row selection sequence $\mathbf{r}$ is alternatively defined as $r_0 = 0$ rather than $r_0 = 1$. In this case, the distribution of $C(\tau)$ is the same as the result of Lemma 6. However, the term in (14) is changed as $|1 + C(l-1)|$ in this case. Thus, the maximal inner product before normalization by K of the resulting codebook becomes slightly larger than the proposed codebooks for $n > 2$, which is the same as the above case with modified QR mapping. The resulting codebooks in this case are also near-optimal codebooks whose $I_{\max}$ satisfies Corollary 1 and Theorem 2.

V. Concluding Remarks

In this paper, we proposed a new class of partial Hadamard codebooks using binary row selection sequences which are generated by QR mapping of p-ary m-sequences. Furthermore, we showed that the proposed construction results in codebooks which asymptotically achieve the Welch bound equality with sufficiently large alphabet size. To our best knowledge, the binary sequences constructed by QR mapping which have good cross-correlation properties with p-ary m-sequences are firstly proposed in this paper. We hope that this approach can be applied to further research for codebook construction and sequences.

References

[1] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.

[2] D. V. Sarwate, "Meeting the Welch bound with equality," in *Sequences and Their Applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. New York, NY, USA: Springer-Verlag, 1999, pp. 79–102.

[3] J. Kovacevic and A. Chebira, "An introduction to frames," *Found. Trends Signal Process.*, vol. 2, no. 1, pp. 1–94, 2008.

[4] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II: Methods in Communication, Security, and Computer Science*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds. New York, NY, USA: Springer-Verlag, 1993, pp. 63–78.

[5] J. H. Conway, R. H. Harding, and N. J. A. Sloane, "Packing lines, planes, etc.: Packings in Grassmannian spaces," *Exp. Math.*, vol. 5, no. 2, pp. 139–159, 1996.

[6] T. Strohmer and R. Heath, "Grassmannian frames with applications to coding and communication," *Appl. Comput. Harmon. Anal.*, vol. 14, no. 3, pp. 257–275, May 2003.

[7] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[8] P. Delsarte, J. M. Goethals, and J. J. Seidel, "Spherical codes and designs," *Geometriae Dedicate*, vol. 67, no. 3, pp. 363–388, 1977.

[9] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," *Proc. London Math. Soc.*, vol. 75, no. 3, pp. 436–480, 1997.

[10] J. M. Renes, R. Blume-Kohout, A. Scot, and C. Caves, "Symmetric informationally complete quantum measurements," *J. Math. Phys.*, vol. 45, no. 6, pp. 2171–2180, 2004.

[11] P. Xia, S. Zhou, and G. B. Giannakis, "Achieving the Welch bound with difference sets," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1900–1907, May 2005.

[12] C. Ding, "Complex codebooks from combinatorial designs," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 229–4235, Sep. 2006.

[13] C. Ding and T. Feng, "A generic construction of complex codebooks meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4245–4250, Nov. 2007.

[14] M. Fickus, D. G. Mixon, and J. C. Tremain, "Steiner equiangular tight frames," *Linear Algebra Appl.*, vol. 436, no. 5, pp. 1014–1027, 2012.

[15] C. Ding and T. Feng, "Codebooks from almost difference sets," *Des. Codes Cryptograph.*, vol. 46, pp. 113–126, Jan. 2008.

[16] A. Zhang and K. Feng, "Two classes of codebooks nearly meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2507–2511, Apr. 2012.

[17] A. Zhang and K. Feng, "Construction of cyclotomic codebooks nearly meeting the Welch bound," *Des. Codes Cryptograph.*, vol. 63, pp. 209–224, May 2012.

[18] N. Y. Yu, K. Feng, and A. Zhang, "A new class of near-optimal partial Fourier codebooks from an almost difference set," *Des. Codes Cryptogr.*, vol. 1, pp. 1–13, Sep. 2012.

[19] Z. Zhou and X. Tang, "New nearly optimal codebooks from relative difference sets," *Adv. Math. Commun.*, vol. 5, no. 3, pp. 521–527, Aug. 2011.

[20] N. Y. Yu, "A construction of codebooks associated with binary sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5522–5533, Aug. 2012.

[21] H. Hu and J. Wu, "New constructions of codebooks nearly meeting the Welch bound with equality," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1348–1355, Feb. 2014.

[22] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20. Reading, MA, USA: Addison-Wesley, 1983.

[23] T. Helleseth and A. Kholosha, "On generalized bent functions," in *Proc. Inf. Theory Appl. Workshop*, Feb. 2010, pp. 1–6.

[24] S.-C. Liu and J. J. Komo, "Nonbinary Kasami sequences over GF(p)," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1409–1412, Jul. 1992.

Seokbeom Hong received the B.S. and Ph.D. degrees in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2007 and 2013, respectively. He is currently a senior engineer at Samsung Electronics, Gyeonggi-do, Korea. His area of research interests includes compressed sensing, error-correcting codes, and communications theory.

Hosung Park received the B.S., M.S., and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 2007, 2009, and 2013, respectively. He was a postdoctoral researcher working with Prof. Jong-Seon No and Prof. Young-Han Kim at Institute of New Media and Communications in Seoul National University, Seoul, Korea, from March 2013 to August 2013. Since September 2013, he has worked with Prof. Young- Han Kim as a postdoctoral scholar in Department of Electrical and Computer Engineering, University of California, San Diego, USA. His research interests include low-density parity-check codes, coding theory, coding for memory, compressed sensing, network information theory, and network coding.

Jong-Seon No (S'80–M'88–SM'10–F'12) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, from September 1990 to July 1999. He joined the Faculty of the Department of Electrical and Computer Engineering, Seoul National University, in August 1999, where he is currently a Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.

Tor Helleseth (M'89–SM'96–F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973 to 1980, he was a Research Assistant with the Department of Mathematics, University of Bergen, Norway. From 1981 to 1984, he was with the Chief Headquarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics, University of Bergen. During the academic years 1977–1978 and 1992–1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979–1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology.

Prof. Helleseth served as an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1991 to 1993. He was Program Chairman for Eurocrypt93 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co- Chairman for SETA04, Seoul, Korea, and SETA06, Beijing, China. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Solstrand, Norway, in 2007. During 2007–2009, he served on the Board of Governors for the IEEE Information Theory Society. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography. In 2004, he was elected a member of Det Norske Videnskaps-Akademi.

Young-Sik Kim (M'09) received the B.S. and M.S., and Ph. D. degrees in electrical engineering and computer science from Seoul National University in 2001, 2003, and 2007, respectively. He joined Semiconductor Division, Samsung Electronics and carried out research and development for secure hardware IPs for various embedded systems, especially for smartcards until the end of August in 2010. He is an assistant professor at Chosun University, Gwangju, Korea. His research interests include cryptographic engineering and information theory including hardware security, embedded security, physical layer security, data hiding, channel coding, and signal design.