A Generalization of the Family of p-ary Decimated Sequences With Low Correlation

Dae San Kim, *Member, IEEE*, Hi-Joon Chae, and Hong-Yeop Song, *Senior Member, IEEE*

***Abstract*—Let p be a prime and n a positive integer. Let $e|p^n - 1$ and $N = \frac{p^n-1}{e}$. In this paper, we construct a family S of e^2N p-ary sequences, each member of S has period N and the magnitudes of correlations of members of S are upper bounded by $2\sqrt{p^n} = 2\sqrt{eN+1}$.**

***Index Terms*—CDMA signature sequences, correlation bound, linear complexity, m-sequences, Weil bound on Kloosterman sum.**

I. Introduction

In the wireless communication systems employing code-division multiple-access (CDMA) scheme, a signature sequence is used for each user in order to distinguish the intended signal from others. [5], [24] In the design of a family S of such sequences, some of the important properties that should be considered are known to be (1) how big $|S|$ is, (2) how long the period of each sequence in S is, (3) how small the maximum of nontrivial auto-correlation and cross-correlation of sequences in S is, and sometimes (4) how big the linear complexity of each member of S is. [5], [11], [24]

In 1969, Sidelnikov showed that two types of certain character sequences (nonbinary) have "good" auto-correlation property. [22] These sequences are now almost fully studied and expanded to families of sequences with "good" cross-correlation properties. [7], [10], [11] Some results on the distribution of cross-correlation and size of p-ary sequence family are given in [1], [2], [4], [9], [18], [19], [26], [28] for $p = 2$ and in [6], [8], [13], [14], [16], [17], [20], [23], [25] for p odd prime. Recently, Kim *et al.* presented a family of p-ary decimated sequences with low correlation [12], and this paper is a further generalization of their results.

Let p be a prime (even or odd) and n a positive integer. Let $e|p^n-1$ and $N = \frac{p^n-1}{e}$. In this paper, we construct a family S of size e^2N, each member of S has period N and the magnitudes of correlations of members of S are upper bounded by $2\sqrt{p^n} = 2\sqrt{eN+1}$ with some reasonable condition on e.

Manuscript received February 16, 2011; revised May 24, 2011; accepted June 07, 2011. Date of current version November 11, 2011. This work was supported in part by the National Foundation (NRF) of Korea Grant funded by the Korean Government (2009-0072514) and in part by the Basic Science Research Program through the National Research Foundation (NRF) of Korea funded by the Ministry of Education, Science and Technology (2009-0083888).

D. S. Kim is with the Department of Mathematics, Sogang University, Seoul, South Korea (e-mail: dskim@sogang.ac.kr).

H.-J. Chae is with the Department of Mathematics Education, Hongik University, Seoul, South Korea (e-mail: hchae@hongik.ac.kr).

H.-Y. Song is with the School of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea (e-mail: hysong@yonsei.ac.kr).

Communicated by N. Y. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2159576

II. Family S

We fix the notations in this paper as follows:

- p is a prime and n is a positive integer.
- $\mathbf{F}_{p^n}$ is the finite field of size p^n. [15]
- $\mathbf{F}_{p^n}^* = \mathbf{F}_{p^n}\backslash\{0\}$.
- $N = \frac{p^n-1}{e}$ where e is a positive divisor of $p^n - 1$. We will use e-decimation of an m-sequence of period $p^n - 1$ so that the result has period N.
- $\omega = e^{2\pi\sqrt{-1}/p}$ is a complex primitive pth root of unity.
- $\mathrm{Tr}_1^n(\cdot) : \mathbf{F}_{p^n} \to \mathbf{F}_p$ is a trace function from $\mathbf{F}_{p^n}$ to $\mathbf{F}_p$, namely, $\mathrm{Tr}_1^n(x) = \sum_{j=0}^{n-1} x^{p^j}$ for $x \in \mathbf{F}_{p^n}$.
- $\lambda(x) = \omega^{\mathrm{Tr}_1^n(x)}$, the canonical additive character of $\mathbf{F}_{p^n}$. Note that $\lambda(x) = \lambda(x^p)$ for $x \in \mathbf{F}_{p^n}$.
- $\alpha \in \mathbf{F}_{p^n}$ is a primitive element.
- $d = N - p^{n-1}$.

For any p-ary sequence $s_1(t)$, $0 \le t < N$, of period N, its nontrivial auto-correlation is given by, for $0 < \tau < N$

$$R_1(\tau) = \sum_{t=0}^{N-1} \omega^{s_1(t+\tau)-s_1(t)}. \tag{1}$$

When $s_2(t)$, $0 \le t < N$, is any other p-ary sequence of period N, then the cross-correlation of the two is given by, for $0 \le \tau < N$

$$R_{1,2}(\tau) = \sum_{t=0}^{N-1} \omega^{s_1(t+\tau)-s_2(t)}. \tag{2}$$

We say $s_1(t)$ and $s_2(t)$ are cyclically equivalent if there exists an integer τ such that $s_1(t+\tau) = s_2(t)$ for all t. Otherwise, they are said to be cyclically distinct.

Let $s(t) = \mathrm{Tr}_1^n(\alpha^t)$ for $0 \le t < p^n - 1$ be a p-ary m-sequence of period $p^n - 1$. Since $gcd(N, d) = 1$, the decimated sequences $s(et)$ and $s(edt)$ have the period $N = (p^n - 1)/e$. We define a family S of e^2N sequences each of period N to contain the sequence $\{s_{k,i,u}(t) | 0 \le t < N\}$ for each of $k = 0, 1, \ldots, e-1$, $u = 0, 1, \ldots, e-1$, and $i = 0, 1, \ldots, N-1$, where

$$s_{k,i,u}(t) = s(et+k) + s(ed(t+i)+u). \tag{3}$$

Theorem 1 (Main): Let S be the family of sequences whose members are given in (3). Then, (i) the magnitude of nontrivial auto-correlation and cross-correlation of members in S is upper bounded by $2\sqrt{p^n}$, and (ii) no two members in S are cyclically equivalent, and hence, $|S| = e^2N$, provided that

$$e < \frac{\sqrt{p^n} - 1/\sqrt{p^n}}{2}.$$

III. Proof of the Main Theorem

We will follow initially the method in [12]. The major differences are (1) p can be even and (2) e can be bigger than 2.

To calculate the correlation of sequences in S, we consider two sequences $s_1(t) = s_{k,i,u}(t)$ and $s_2(t) = s_{l,j,v}(t)$ in S, and calculate (2). It is an auto-correlation when $k = l$, $i = j$, and $u = v$, and it is a cross-correlation of two distinct members of S otherwise. It will be the trivial auto-correlation when $k = l$, $i = j$, $u = v$, and $\tau = 0$.

Letting $a = \alpha^{e\tau+k} - \alpha^l$, $b' = \alpha^{ed(\tau+i)+u} - \alpha^{edj+v}$, $b = (b')^p$, and following some similar steps in [12], we arrive easily at the following:

$$R_{1,2}(\tau) = \sum_{t=0}^{N-1} \lambda(a\alpha^{et} + b\alpha^{-et}) = \frac{1}{e} \sum_{x\in\mathbf{F}_{p^n}^*} \lambda(ax^e + bx^{-e}). \tag{4}$$

Note that if $a = \alpha^{e\tau+k} - \alpha^l = 0$, then

$$e\tau \equiv l - k \pmod{p^n - 1}.$$

Observe that both l and k are integers less than e. Since $p^n - 1$ is a multiple of e and so is the LHS, the above congruence implies that $k = l$, and hence, $\tau \equiv 0 \pmod N$. If, furthermore, $b = 0$, then $b' = \alpha^{edi+u} - \alpha^{edj+v} = 0$ and this implies that $ed(i - j) \equiv v - u \pmod{p^n - 1}$. Then, similarly, we have $u = v$ and $i = j$. Therefore, if $a = 0 = b$, then (4) becomes trivial.

Now, we need the following two results, which are true whether p is even or odd. The first one is Theorem 4 of [3]:

Theorem 2 (Weil Bound for all p): Let χ be any multiplicative character of $\mathbf{F}_{p^n}$ and let $a, b \in \mathbf{F}_{p^n}^*$. Define the generalized Kloosterman sum $K(\lambda, \chi; a)$ as follows:

$$K(\lambda, \chi; a, b) = \sum_{x\in\mathbf{F}_{p^n}^*} \chi(x)\lambda(ax + b/x).$$

Then

$$|K(\lambda, \chi; a, b)| \le 2\sqrt{p^n}.$$

Note that the (twisted) Kloosterman sum in Theorem 4 of [3] or in [27] is usually defined as $\sum_{x\in\mathbf{F}_{p^n}^*} \chi(x)\lambda(x + c/x)$ for $c \in \mathbf{F}_{p^n}^*$, and the one in the above theorem is $\sum_{x\in\mathbf{F}_{p^n}^*} \chi(x)\lambda(x + ab/x)$ when both a and b are not zero. Note also that the bound does not depend on the value of a or b. Following bound for any prime p (even or odd) is also given by Weil [27]:

Theorem 3 (Weil): Let $f(x)$ be a polynomial of degree $m \ge 1$ over $\mathbf{F}_{p^n}$ with $gcd(m, p^n) = 1$. Then

$$\left| \sum_{x\in\mathbf{F}_{p^n}} \lambda(f(x)) \right| \le (m - 1)\sqrt{p^n}.$$

Now, we continue the calculation given in (4). For this, we let, for $a, b \in \mathbf{F}_{p^n}$

$$\Lambda_e = \sum_{x\in\mathbf{F}_{p^n}^*} \lambda(ax^e + bx^{-e}).$$

Then

$$R_{1,2}(\tau) = \frac{1}{e}\Lambda_e.$$

Assume $a \ne 0$ and $b = 0$. From Theorem 3, by letting $f(x) = ax^e$ and since $gcd(e, p^n) = 1$, we have

$$|\Lambda_e| \le (e - 1)\sqrt{p^n} + 1 < e\sqrt{p^n}.$$

Similarly, we have the same when $a = 0$ and $b \ne 0$.

Assume $a \ne 0$ and $b \ne 0$, and observe that

$$\frac{1}{e}\sum_{\chi^e=1} \chi(x) = \begin{cases} 1, & \text{if } x = y^e \text{ for } y \in \mathbf{F}_{p^n}^* \\ 0, & \text{otherwise.} \end{cases}$$

Here, the sum is extended over all the multiplicative characters over $\mathbf{F}_{p^n}$ of order dividing e. Therefore

$$\begin{aligned} \Lambda_e &= e \sum_{x=e\text{-th power } \in\mathbf{F}_{p^n}^*} \lambda(ax + b/x) \\ &= e \sum_{x\in\mathbf{F}_{p^n}^*} \frac{1}{e} \sum_{\chi^e=1} \chi(x)\lambda(ax + b/x) \\ &= \sum_{\chi^e=1} \sum_{x\in\mathbf{F}_{p^n}^*} \chi(x)\lambda(ax + b/x) \\ &= \sum_{\chi^e=1} K(\lambda, \chi; a, b). \end{aligned}$$

Thus

$$|R_{1,2}(\tau)| = \left|\frac{1}{e}\Lambda_e\right| \le 2\sqrt{p^n}.$$

This proves the upper bound (i) on the magnitudes of the correlation.

For (ii), we assume that $e < \frac{\sqrt{p^n} - 1/\sqrt{p^n}}{2}$ and suppose that $s_1(t)$ and $s_2(t)$ in the beginning of this section are cyclically equivalent. Then, there exist τ_0 such that $s_1(t + \tau_0) = s_2(t)$ for all t, and hence, $s_1(t)$ and $s_2(t)$ have a trivial correlation value

$$N = R_{1,2}(\tau_0) = \frac{1}{e}\Lambda_e.$$

This implies that

$$p^n - 1 = \Lambda_e = |\Lambda_e| \le 2e\sqrt{p^n} < p^n - 1$$

under our restrictions on e. Thus, we proved that all the members of S are cyclically distinct with each other. Therefore, $|S| = e^2 N$ and the theorem follows.

IV. Examples and Conclusion

We consider two examples here. The first one is for $p = 3$, $n = 4$, $e = 4$ so that $p^n - 1 = 80$ and $N = 20$. Note that $e = 4 < (\sqrt{81} - 1/\sqrt{81})/2 \approx 4.444$. In this case, $|S| = 320$ and the max correlation magnitude is upper bounded by 18 by Theorem 1. It turned out that, using the irreducible polynomial $x^4 + x + 2$, the true max is 14.00, which is achieved by two member sequences with cases $(k, i, u) = (0, 0, 2)$ and $(0, 1, 1)$, which correspond to two sequences $s_1 = (11221221202211211210)$ and $s_2 = (21211210011212212002)$, respectively. It turned out that

TABLE I
COMPARISON OF WELL-KNOWN p-ARY SEQUENCE FAMILIES ($p = 2$ OR AN ODD PRIME)

Reference	Period N	Alphabet	C_{max}	Family size
Gold [4]	p^n-1, n odd	$p=2$	$1+\sqrt{2(N+1)}$	$N+2$
Kasami (Small Set) [9]	p^n-1, n even	$p=2$	$1+\sqrt{N+1}$	$\sqrt{N+1}$
Kasami (Large Set) [9]	p^n-1, n even	$p=2$	$1+2\sqrt{N+1}$	$(N+2)\sqrt{N+1}-1$ or $(N+2)\sqrt{N+1}$
Bent [18]	p^n-1, n even	$p=2$	$1+\sqrt{N+1}$	$\sqrt{N+1}$
Boztas and Kumar [1]	p^n-1, n odd	$p=2$	$1+\sqrt{2(N+1)}$	$N+2$
Udaya [26]	p^n-1, n even	$p=2$	$1+2\sqrt{N+1}$	$N+2$
Chang *et al.* [2]	p^n-1, n odd	$p=2$	$1+2\sqrt{2(N+1)}$	$(N+1)^2$
Rothaus [19]	p^n-1, n odd	$p=2$	$1+2\sqrt{2(N+1)}$	N^2+3N+3
Yu and Gong ($S_o(2)$) [28]	p^n-1, n odd	$p=2$	$1+2\sqrt{2(N+1)}$	$(N+1)^2$
Yu and Gong ($S_e(2)$) [28]	p^n-1, n even	$p=2$	$1+4\sqrt{N+1}$	$(N+1)^2$
Trachtenberg [25]	p^n-1, n odd	p odd	$1+\sqrt{p(N+1)}$	$N+2$
Helleseth [8]	p^n-1, n even, $p^{n/2}\not\equiv 2 \pmod 3$	p odd	$1+2\sqrt{(N+1)}$	$N+2$
Sidelnikov [23]	p^n-1	p odd	$1+\sqrt{(N+1)}$	$N+1$
Kumar [13]	p^n-1, n even	p odd	$1+\sqrt{(N+1)}$	$\sqrt{N+1}$
Kumar and Moreno [14]	p^n-1	p odd	$1+\sqrt{(N+1)}$	$N+1$
Gong [6]	$(p^n-1)^2$	p odd	$3+2\sqrt{N}$	$\sqrt{N}$
Kim *et.al.* [12]	$(p^n-1)/2$, n odd	p odd	$2\sqrt{(N+1/2)}$	$4N$
This paper	$(p^n-1)/e$, $e<\frac{\sqrt{p^n}-1/\sqrt{p^n}}{2}$	$p=2$ or p odd	$2\sqrt{eN+1}$	e^2N

TABLE II
MAXIMUM INTEGER VALUE OF e FOR SOME SMALL p AND n

$n \setminus p$	2	3	5	7	11	13	17	19	23
3	1	2	4	9	14	18	16	27	22
4	1	4	12	24	60	84	144	180	264
5	1	2	22	6	50	12	16	453	22
6	3	13	62	171	665	1098	2456	3429	6083
7	1	2	4	174	430	12	16	12618	638
8	5	40	312	1200	7320	14280	41760	65160	139920

the cross-correlation values of the two are all real and its profile is given as

$$R_{1,2}(\tau) = \begin{cases} -1, & 3 \text{ times} \\ 2, & 3 \text{ times} \\ -4, & 3 \text{ times} \\ 5, & 4 \text{ times} \\ -7, & 3 \text{ times} \\ 8, & 3 \text{ times} \\ 14, & 1 \text{ time.} \end{cases}$$

The second one is for $p=2, n=6, e=3$ so that $p^n-1=63$ and $N=21$. Note that $e=3<(\sqrt{64}-1/\sqrt{64})/2=3.9375$. In this case, $|S|=189$ and the max correlation magnitude is upper bounded by 16 by Theorem 1. It turned out that, using the irreducible polynomial x^6+x+1, the true max is 13.00, which is achieved by two member sequences with cases $(k,i,u)=(0,0,0)$ and $(0,0,1)$, which correspond to two sequences $s_1=(011011001011010011011)$ and $s_2=(011010100010110111110)$, respectively. It turned out that the cross-correlation values of the two are all real and its profile is given as

$$R_{1,2}(\tau) = \begin{cases} 1, & 4 \text{ times} \\ -3, & 3 \text{ times} \\ 5, & 5 \text{ times} \\ -7, & 6 \text{ times} \\ 9, & 2 \text{ times} \\ 13, & 1 \text{ time.} \end{cases}$$

Finally, we remark that each member of S has the linear complexity $2n$ since both $s(et)$ and $s(edt)$ have the linear complexity n.

For the purpose of comparison, we show various parameters of p-ary sequence families in Table I. Table II shows the maximum integer value of e for some small p and n. Note that e must be a divisor of p^n-1 and no larger than $\frac{\sqrt{p^n}-1/\sqrt{p^n}}{2}$.

ACKNOWLEDGMENT

The authors are grateful for the helpful suggestions from anonymous referees on the initially submitted version of this manuscript.

REFERENCES

[1] S. Boztas and P. V. Kumar, "Binary sequences with Gold-like correlation but larger linear span," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 532–537, Mar. 1994.

[2] A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth, and P. V. Kumar, "On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 680–687, Mar. 2000.

[3] K. Conrad, "On Weil's proof of the bound for Kloosterman sums," *J. Num. Theory*, vol. 97, pp. 439–446, 2002.

[4] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.

[5] S. W. Golomb and G. Gong, *Sequence Design for Good Correlation*. New York: Cambridge Univ. Press, 2005.

[6] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2847–2867, Nov. 2002.

[7] Y. K. Han and K. Yang, "On the crosscorrelation distributions of M-ary multiplicative character sequences," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2384–2391, May 2009.

[8] T. Helleseth, "Some result about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209–232, 1976.

[9] T. Kasami, "Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes," *Inf. Control*, vol. 18, pp. 369–394, 1971.

[10] Y.-J. Kim, H.-Y. Song, G. Gong, and H. Chung, "Cross correlation of q-ary power residue sequences of period p," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 311–315.

[11] Y.-J. Kim and H.-Y. Song, "Crosscorrelation of Sidel'nikov sequences and their constant multiples," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1220–1224, May 2007.

[12] J.-Y. Kim, S.-T. Choi, J.-S. No, and H. Chung, "A new family of p-ary decimated sequences with low correlation," presented at the IEEE Int. Symp. Information Theory, Austin, TX, Jun. 13–18, 2010.

[13] P. V. Kumar, "On Bent Sequences and Generalized Bent Functions," Ph.D. dissertation, Univ. Southern California, Los Angeles, 1983.

[14] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 603–616, May 1991.

[15] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983, vol. 20, Encyclopedia of Mathematics and Its Applications.

[16] E. N. Muller, "On the crosscorrelation of sequences over $GF(p)$ with short periods," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 289–295, Jan. 1999.

[17] G. J. Ness, T. Helleseth, and A. Kholosha, "On the correlation distribution of the Coulter-Matthews decimation," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2241–2247, May 2006.

[18] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 6, pp. 858–864, Nov. 1982.

[19] O. S. Rothaus, "Modified Gold codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 654–656, Mar. 1993.

[20] E. Y. Seo, Y. S. Kim, J. S. No, and D. J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3140–3149, Jul. 2008.

[21] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, "Improved binary codes and sequence families from Z_4-linear codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 5, pp. 1582–1587, Sep. 1996.

[22] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equi-distance codes," *Probl. Pered. Inf.*, vol. 5, pp. 16–22, 1969.

[23] V. M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, no. 1, pp. 197–201, 1971.

[24] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. Rockville, MD: Computer Science Press, 1985.

[25] H. M. Trachtenberg, "On the Cross-Correlation Function of Maximal Linear Sequences," Ph.D. dissertation, Univ. Southern California, Los Angeles, 1970.

[26] P. Udaya, "Polyphase and Frequency Hopping Sequences Obtained From Finite Rings," Ph.D. dissertation, Dept. Elect. Eng., Indian Inst. Technol., Kanpur, India, 1992.

[27] A. Weil, "On some exponential sums," in *Proc. Natl. Acad. Sci.*, 1948, vol. 34.

[28] N. Y. Yu and G. Gong, "A new binary sequence family with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1624–1636, Apr. 2006.

Dae San Kim (M'05) received his B.S. and M.S. degrees in mathematics from Seoul National University, Seoul, Korea, in 1978 and 1980, respectively, and the Ph.D. degree in mathematics from University of Minnesota, Minneapolis, MN, in 1989. He is a professor in the Department of Mathematics at Sogang University, Seoul, Korea. He has been there since 1997, following a position at Seoul Women's University. His research interests include number theory (exponential sums, modular forms, zeta functions) and coding theory.

Hi-Joon Chae received the B.S. degree in mathematics from Korea Advanced Institute of Science and Technology, Dae-jeon, Korea, in 1990 and the Ph.D. degree in mathematics from Massachusetts Institute of Technology, Cambridge, MA, in 1994. He is a professor in the Department of Mathematics Education at Hongik University, Seoul, Korea. He has been there since 2000 following a position at Korea Advanced Institute of Science and Technology. His research interests include representation theory (of p-adic groups), algebraic geometry (of varieties over finite fields) and number theory (exponential sums).

Hong-Yeop Song (S'85–M'92–SM'07) received his B.S. degree in Electronic Engineering from Yonsei University in 1984, M.S.E.E. and Ph.D. degrees from the University of Southern California, Los Angeles, in 1986 and 1991, respectively. He spent 2 years as a research associate at USC and then 2 years as a senior engineer at the standard team of Qualcomm, Inc., San Diego, CA. Since September 1995, he has been with Department of electrical and electronic engineering, Yonsei University, Seoul, Korea, and he is currently serving as the department Chair for two years beginning March 2010. His area of research interest includes digital communications and channel coding. He is a member of the IEEE, MAA (Mathematical Association of America), IEEK, KICS, KIISC, and KMS.