# Autocorrelation Values of Generalized Cyclotomic Sequences of Order Two

Cunsheng Ding

***Abstract*—The generalized cyclotomic sequence of order two has several good randomness properties and behaves like the Legendre sequence in several aspects. In this correspondence we calculate the autocorrelation values of the generalized cyclotomic sequence of order two. Our result shows that this sequence could have very good autocorrelation property and pattern distributions of length two if the two primes are chosen properly.**

***Index Terms*—Autocorrelation, cyclotomy, sequences.**

## I. Introduction

Pseudorandom sequences have wide applications in simulation, software testing, global positioning systems, ranging systems, code-division multiple-access systems, radar systems, spread-spectrum communication systems, and stream ciphers.

Many applications require a set of sequences which have one or both of the following properties [6], [7].

- Each sequence in the set is easy to distinguish from a time-shifted version of itself (i.e., good autocorrelation).
- Each sequence in the set is easy to distinguish from (a possibly time-shifted version of) every other sequence in the set (i.e., good crosscorrelation).

The generalized cyclotomic sequence of order two has several good randomness properties [1]. This sequence has been proven to have also large linear span [2]. Although Whiteman [8] did not mention anything about the application of the generalized cyclotomy in sequences, the construction of the generalized cyclotomic sequence of order 2 is a natural application of this generalized cyclotomy. Whiteman studied the generalized cyclotomy of order 2 only for the purpose of searching for residue difference sets.

In this correspondence we calculate the exact autocorrelation values and pattern distributions of length two of this sequence. Then we discuss how to choose the parameters in order to ensure good autocorrelation property of this sequence.

## II. Generalized Cyclotomy and the Sequence

Let $p$ and $q$ be two distinct primes with $\gcd(p-1,\ q-1)=2$. By the Chinese Remainder Theorem there exists a common primitive root $g$ of both $p$ and $q$. Let $x$ be an integer satisfying the simultaneous congruences

$$x \equiv g \pmod{p} \qquad x \equiv 1 \pmod{q}.$$

The existence and uniqueness of $x$ modulo $pq$ are guaranteed by the Chinese Remainder Theorem and the Chinese Remainder Algorithm [3] gives the solution $x$.

Manuscript received February 10, 1997; revised January 8, 1998.

The author is with the Department of Information Systems and Computer Science, the National University of Singapore, Singapore 119260 (e-mail: dingcs@iscs.nus.edu.sg).

Publisher Item Identifier S 0018-9448(98)03482-8.

Define $N=pq$ and $e=(p-1)(q-1)/2$. Since $g$ is a primitive root of $p$ and $q$, by the Chinese Remainder Theorem again

$$\begin{aligned}\mathrm{ord}_N(g) &= \mathrm{lcm}\,(\mathrm{ord}_p(g),\ \mathrm{ord}_q(g))\\ &= \mathrm{lcm}\,(p-1,\ q-1)=e\end{aligned}$$

where $\mathrm{ord}_N(g)$ denotes the multiplicative order of $g$ modulo $N$.

Whiteman's generalized cyclotomic classes $D_0$ and $D_1$ of order two are defined by [8]

$$D_i=\{g^s x^i\colon s=0,\ 1,\ \cdots,\ e-1\}, \qquad i=0,\ 1$$

where the multiplication is that of $Z_N$, the residue ring modulo $N$. By the definition of $x$ it is easily seen that

$$Z_N^* = D_0 \cup D_1 \qquad D_0 \cap D_1 = \phi,$$

where $\phi$ denotes the empty set and $Z_N^*$ the multiplicative group of the ring $Z_N$.

The corresponding generalized cyclotomic numbers of order two are defined by

$$(i,\ j)=|(D_i+1)\cap D_j|, \qquad \text{for all } i=0,\ 1,\ j=0,\ 1.$$

Here and hereafter we define $A+a=\{x+a\colon x\in A\}$ and $aA=\{ax\colon x\in A\}$ for any subset $A$ of $Z_N$ and $a\in Z_N$.

Define

$$\begin{aligned}P &= \{p,\ 2p,\ \cdots,\ (q-1)p\}\\ Q &= \{q,\ 2q,\ \cdots,\ (p-1)q\}\\ R &= \{0\}\\ C_0 &= R\cup Q\cup D_0\\ C_1 &= P\cup D_1.\end{aligned}$$

Then

$$C_0\cup C_1 = Z_{pq} \qquad C_0\cap C_1=\phi.$$

The generalized cyclotomic sequence $s^\infty$ of order 2 with respect to the primes $p$ and $q$ is defined by

$$s_i=\left\{\begin{matrix}0, & \text{if } (i \bmod N)\in C_0;\\ 1, & \text{if } (i \bmod N)\in C_1\end{matrix}\right\}, \qquad \text{for all } i\ge 0$$

where $i \bmod N$ denotes the least nonnegative integer that is congruent to $i$ modulo $N$. It is easy to see that this sequence can be expressed as $s_i=F(i \bmod N)$ with

$$F(i)=\left\{\begin{matrix}0, & \text{if } i\in R\cup Q\\ 1, & \text{if } i\in P\\ \left(1-\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\right)/2, & \text{otherwise}\end{matrix}\right\} \tag{1}$$

for all $0\le i\le N-1$, where $(a/p)$ denotes the Legendre symbol.

## III. Autocorrelation Values

Let the symbols be the same as before. The periodic autocorrelation function of the binary sequence $s^\infty$ is defined by

$$\mathrm{C}_s(w)=\frac{1}{N}\sum_{i\in Z_N}(-1)^{s_{i+w}+s_i}$$

where $0\le w\le N-1$. Note that in the field $\mathrm{GF}(2)$ addition and subtraction are the same. So $s_{i+w}+s_i$ and $s_{i+w}-s_i$ are the same for binary sequences.

The main results of this correspondence are summarized in the following two theorems. The proofs will be given later.

*Theorem 1:* Let $(p-1)(q-1)/4$ be even. Then

$$\mathrm{C}_s(w)=\begin{cases}\dfrac{q-p-3}{pq}, & \text{if } w\in P\\ \dfrac{p+1-q}{pq}, & \text{if } w\in Q\\ \dfrac{-1}{pq}, & \text{if } w\in Z_N^*.\end{cases}$$

*Theorem 2:* Let $(p-1)(q-1)/4$ be odd. Then

$$\mathrm{C}_s(w)=\begin{cases}\dfrac{q-p-3}{pq}, & \text{if } w\in P\\ \dfrac{p+1-q}{pq}, & \text{if } w\in Q\\ \dfrac{-3}{pq}, & \text{if } w\in D_0\\ \dfrac{1}{pq}, & \text{if } w\in D_1.\end{cases}$$

By Theorems 1 and 2, the autocorrelation values of this generalized cyclotomic sequence of order two are quite flat when $|p-q|$ is very small.

The best case is when $q-p=2$, i.e., they are twin primes. In this case, if $(p-1)(q-1)/4$ is even, the $\mathrm{C}_s(w)$ is two-valued, i.e., the sequence has the best autocorrelation property. In this case, if $(p-1)(q-1)/4$ is odd, $\mathrm{C}_s(w)$ is four-valued.

Another interesting case is when $q-p=4$. In this case, $\mathrm{C}_s(w)$ is four-valued when $(p-1)(q-1)/4$ is even, and three-valued when $(p-1)(q-1)/4$ is odd. In the case $q-p=4$, this sequence has also good autocorrelation property.

To prove Theorems 1 and 2, we need the following nine lemmas. Define

$$d_s(i,\,j;\,w)=|C_i\cap(C_j+w)|,\qquad w\in Z_N,\ i,\,j=0,\,1.$$

*Lemma 1:* For each $a\not\equiv 0 \pmod N$

$$\mathrm{C}_s(a)=1-\frac{4d_s(1,\,0;\,a)}{N}.$$

*Proof:*

$$\begin{aligned}N\mathrm{C}_s(a)&=(|C_0\cap(C_0-a)|-|C_1\cap(C_0-a)|)\\&\quad+(|C_1\cap(C_1-a)|-|C_0\cap(C_1-a)|)\\&=(2|C_0\cap(C_0-a)|-|C_0|)\\&\quad+(|C_1|-2|C_0\cap(C_1-a)|)\\&=|C_1|-|C_0|+2|C_0|-4|C_0\cap(C_1-a)|\\&=N-4|C_1\cap(C_0+a)|\\&=N-4d_s(1,\,0;\,a).\end{aligned}$$

□

*Lemma 2:* For each $w\in Z_N^*$

$$|(D_0+w)\cap D_1|=\begin{cases}(0,\,1), & \text{if } w\in D_0\\ (1,\,0), & \text{if } w\in D_1.\end{cases}$$

*Proof:* By definition $aD_i=D_{i+j}$ if $a\in D_j$. Since $D_0$ is a group and $D_1=xD_0$, we have

$$\begin{aligned}|(D_0+w)\cap D_1|&=|(w^{-1}D_0+1)\cap w^{-1}D_1|\\&=\begin{cases}(0,\,1), & \text{if } w\in D_0\\ (1,\,0), & \text{if } w\in D_1.\end{cases}\end{aligned}$$

□

The proof of the following lemma can be found in [8, Lemma 2].

*Lemma 3:* For each $w\in P\cup Q$

$$|(D_0+w)\cap D_1|=\frac{(p-1)(q-1)}{4}.$$

*Lemma 4:*

$$|D_1\cap((Q\cup R)+w)|=\begin{cases}0, & \text{if } w\in Q\cup R\\ \dfrac{p-1}{2}, & \text{otherwise.}\end{cases}$$

*Proof:* The first part is clear. We now prove the second part. If $w\notin Q\cup R$, then an element $z=g^sx\in(Q\cup R)+w$ if and only if

$$g^sx-w\equiv 0 \pmod q. \tag{2}$$

Note that $x\equiv 1 \pmod q$. Let $v$ be the inverse of $w$ modulo $q$. Since $g$ is a primitive root of $q$, there must be an integer $t$ with $0\le t\le q-1$ such that $v\equiv g^t \pmod q$. Thus (2) is equivalent to

$$g^{s-t}\equiv 1 \pmod q$$

which is further equivalent to

$$s-t\equiv 0 \pmod{q-1}.$$

It follows that the number of solutions $s$ of (2) with $0\le s\le e-1$ is $e/(q-1)=(p-1)/2$. □

We need also the following Generalized Chinese Remainder Theorem [3].

*Lemma 5:* Let $m_1,\cdots,m_t$ be positive integers. For a set of integers $a_1,\cdots,a_t$, the system of congruences

$$y\equiv a_i \pmod{m_i},\qquad i=1,\cdots,t$$

has solutions if and only if

$$a_i\equiv a_j \pmod{\gcd(m_i,\,m_j)},\qquad i\ne j,\ 1\le i,\,j\le t. \tag{3}$$

If (3) is satisfied, the solution is unique modulo $\mathrm{lcm}\,(m_1,\cdots,m_t)$.

*Lemma 6:* $-1\in D_1$ if $|p-q|/2$ is odd, and $-1\in D_0$ if $|p-q|/2$ is even.

*Proof:* $-1\in D_0$ if and only if there is an integer $s$ with $0\le s\le e-1$ such that

$$g^s\equiv -1 \pmod{pq} \tag{4}$$

which is by the Chinese Remainder Theorem equivalent to

$$g^s\equiv -1 \pmod p \text{ and } g^s\equiv -1 \pmod q.$$

Since $g$ is a common primitive root of $p$ and $q$, we have

$$\begin{aligned}g^{(p-1)/2}&\equiv -1 \pmod p\\ g^{(q-1)/2}&\equiv -1 \pmod q.\end{aligned}$$

Thus (4) is further equivalent to

$$\begin{aligned}g^{s-(p-1)/2}&\equiv 1 \pmod p\\ g^{s-(q-1)/2}&\equiv 1 \pmod q\end{aligned}$$

which is equivalent to

$$\begin{aligned}s-(p-1)/2&\equiv 0 \pmod{p-1}\\ s-(q-1)/2&\equiv 0 \pmod{q-1}.\end{aligned}$$

By Lemma 5, (4) has a solution if and only if $|p-q/2|$ is even. □

*Lemma 7:*

$$|P\cap(D_0+w)|=\begin{cases}0, & \text{if } w\in P\\ \dfrac{q-1}{2}, & \text{if } w\in Q\\ \dfrac{q-1}{2}, & \text{if } w\in D_1 \text{ and } \dfrac{|p-q|}{2} \text{ even}\\ \dfrac{q-3}{2}, & \text{if } w\in D_1 \text{ and } \dfrac{|p-q|}{2} \text{ odd}\\ \dfrac{q-3}{2}, & \text{if } w\in D_0 \text{ and } \dfrac{|p-q|}{2} \text{ even}\\ \dfrac{q-1}{2}, & \text{if } w\in D_0 \text{ and } \dfrac{|p-q|}{2} \text{ odd.}\end{cases}$$

*Proof:* Similar to the proof of Lemma 4; we can prove that if $w \notin P \cup R$, then

$$|(P \cup R) \cap (D_0 + w)| = \frac{q-1}{2}.$$

By Lemma 6

$$|R \cap (D_0 + w)| = \begin{cases} 0, & \text{if } w \in Q \\ 0, & \text{if } w \in D_1 \text{ and } \dfrac{|p-q|}{2} \text{ even} \\ 1, & \text{if } w \in D_1 \text{ and } \dfrac{|p-q|}{2} \text{ odd} \\ 1, & \text{if } w \in D_0 \text{ and } \dfrac{|p-q|}{2} \text{ even} \\ 0, & \text{if } w \in D_0 \text{ and } \dfrac{|p-q|}{2} \text{ odd.} \end{cases}$$

The conclusion of this lemma then follows from

$$\begin{aligned} |P \cap (D_0 + w)| &= |(P \cup R) \cap (D_0 + w)| - |R \cap (D_0 + w)| \\ &= \frac{q-1}{2} - |R \cap (D_0 + w)|. \end{aligned}$$ □

*Lemma 8:*

$$|P \cap ((Q \cup R) + w)| = \begin{cases} 1, & \text{if } w \in P \\ 0, & \text{if } w \in Q \\ 1, & \text{if } w \in Z_N^*. \end{cases}$$

*Proof:* Note that

$$|P \cap ((Q \cup R) + w)| = |P \cap (Q + w)| + |P \cap \{w\}|.$$

The first two conclusions then follow easily.

Recall the definition of $P$ and $Q$. For any fixed $w \in Z_N^*$, consider now the following equation:

$$up - vq \equiv w \pmod{pq}$$

where $1 \le u \le q-1$ and $1 \le v \le p-1$. Suppose it has two solutions $(u_1, v_1)$ and $(u_2, v_2)$. Then

$$u_1 p - v_1 q \equiv u_2 p - v_2 q \pmod{pq}.$$

Hence

$$u_1 p \equiv u_2 p \pmod{q},\ v_1 q \equiv v_2 q \pmod{p}.$$

Note that

$$1 \le u_1,\ u_2 \le q-1,\ \ 1 \le v_1,\ v_2 \le p-1$$

and $\gcd(p, q) = 1$. We obtain that $(u_1, v_1) = (u_2, v_2)$.

Thus when $u$ ranges over $\{1, 2, \cdots, q-1\}$ and $v$ ranges over $\{1, 2, \cdots, p-1\}$, the function $up - vq$ takes on $(p-1)(q-1)$ different elements of $Z_N^*$, but $Z_N^*$ has exactly $(p-1)(q-1)$ elements. Therefore, $|P \cap (Q + w)| = 1$ for each $w \in Z_N^*$. □

A proof of the following lemma can be found in [8].

*Lemma 9:* If $(p-1)(q-1)/4$ is even, we have $(0, 0) = (1, 0) = (1, 1)$ and two different cyclotomic numbers

$$\begin{aligned} (0, 0) &= \frac{(p-2)(q-2)+1}{4} \\ (0, 1) &= \frac{(p-2)(q-2)-3}{4}. \end{aligned}$$

If $(p-1)(q-1)/4$ is odd, we have $(0, 1) = (1, 0) = (1, 1)$ and two different cyclotomic numbers

$$\begin{aligned} (0, 0) &= \frac{(p-2)(q-2)+3}{4} \\ (0, 1) &= \frac{(p-2)(q-2)-1}{4}. \end{aligned}$$

The following formula will be needed in the sequel:

$$\begin{aligned} d_s(1, 0; w) &= |C_1 \cap (C_0 + w)| \\ &= |(D_1 \cup P) \cap ((D_0 \cup Q \cup R) + w)| \\ &= |D_1 \cap (D_0 + w)| + |D_1 \cap ((Q \cup R) + w)| \\ &\quad + |P \cap (D_0 + w)| + |P \cap ((Q \cup R) + w)|. \end{aligned}$$

We are now ready to prove Theorems 1 and 2.

*Proof of Theorem 1:* By (5), Lemmas 2–4, 7, and 8, we obtain

$$\begin{aligned} &d_s(1, 0; w) \\ &= \begin{cases} \dfrac{(p-1)(q-1)}{4} + \dfrac{p-1}{2} + 0 + 1, & w \in P \\ \dfrac{(p-1)(q-1)}{4} + 0 + \dfrac{q-1}{2} + 0, & w \in Q \\ \dfrac{(p-2)(q-2)-3}{4} + \dfrac{p-1}{2} + \dfrac{q-1}{2} + 1, & w \in D_0 \\ \dfrac{(p-2)(q-2)+1}{4} + \dfrac{p-1}{2} + \dfrac{q-3}{2} + 1, & w \in D_1 \end{cases} \\ &= \begin{cases} \dfrac{pq+p-q+3}{4}, & w \in P \\ \dfrac{pq+q-p-1}{4}, & w \in Q \\ \dfrac{pq+1}{4}, & w \in D_0 \cup D_1. \end{cases} \end{aligned}$$

The conclusion of this theorem then follows from Lemma 1.

Similar to the proof of Theorem 1, we can prove Theorem 2.

## IV. Distributions of Patterns of Length 2

It is interesting to note that the parameter $d_s(i, j; -w)$ defined before is exactly the number of patterns

$$\underbrace{i * * \cdots * j}_{w}$$

appearing in one period of this sequence, where the $*$'s are arbitrary bits that could be different. Thus it measures exactly the pattern distributions of length two of a periodic sequence. We have already computed $d_s(1, 0; -w)$, the number of patterns

$$\underbrace{1 * * \cdots * 0}_{w}$$

in a period of this sequence. When $(p-1)(q-1)/4$ is even, we have

$$\begin{aligned} d_s(0, 0; w) &= |C_0 \cap (C_0 + w)| \\ &= |C_0| - |C_1 \cap (C_0 + w)| \\ &= \frac{(p-1)(q-1)}{2} + p - d_s(1, 0; w) \\ &= \begin{cases} \dfrac{pq+p-q-1}{4}, & \text{if } w \in P \\ \dfrac{pq+3p-3q+1}{4}, & \text{if } w \in Q \\ \dfrac{pq+2p-2q+1}{4}, & \text{if } w \in D_0 \cup D_1. \end{cases} \end{aligned}$$

Note that $|C_0| + q - p - 1 = |C_1|$, we have

$$\begin{aligned} d_s(1, 1; w) &= |C_1| - |C_1 \cap (C_0 + w)| \\ &= d_s(0, 0; w) + q - p - 1. \end{aligned}$$

It is easily seen that

$$d_s(0, 1; w) = d_s(1, 0; w).$$

Thus we have computed all $d_s(i, j; w)$ in the case that $(p-1) \cdot (q-1)/4$ is even. They can be easily written out with the help of Theorem 2 when $(p-1)(q-1)/4$ is odd.

These results show that the distribution of patterns of length two of this generalized cyclotomic sequence is quite good when $|q-p|$ is small enough.

## V. Concluding Remarks

It was proved in [2] that the linear span of this generalized cyclotomic sequence takes on one of $pq-1$, $(p-1)q$, and $(p-1)\cdot(q-1)$, depending on the values of $p \bmod 8$ and $q \bmod 8$. Thus it has large linear span.

For application we are concerned with the implementation of a generator that can produce the generalized cyclotomic sequences of order two. A hardware implementation of the generalized cyclotomic generator of order two that produces the sequences is described in [2], with the help of the Chinese Remainder Theorem. With dedicated chips for modular exponentiation, the performance of this generator is estimated to be 30 kbytes/s, when the two primes are about 48 bits [2]. In [2], this generator and its output sequences are suggested for military and diplomatic applications where security is the primary concern. For additive stream ciphering, the linear span of the keystream sequence must be large enough. So the generalized cyclotomic sequence of order 2 is ideal for this purpose, but $m$-sequences cannot be used as they have low linear span.

Finally, we mention that there are other cyclotomic sequences having good randomness properties. Among them are the Legendre sequences [4], the cyclotomic sequences of order $r$ [5], and others described in [1].

## Acknowledgment

The author wishes to thank the two anonymous referees for their detailed and very helpful comments and suggestions that much improved this correspondence.

## References

[1] C. Ding, "Binary cyclotomic generators," in *Fast Software Encryption* (Lecture Notes in Computer Science, vol. 1008, B. Preneel, Ed.) Berlin, Germany: Springer-Verlag, 1995, pp. 20–60.

[2] ——, "Linear complexity of the generalized cyclotomic sequence of order 2," *Finite Fields and Their Applications*, vol. 3, pp. 159–174, 1997.

[3] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996, ch. 2.

[4] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inform. Theory*, to be published.

[5] C. Ding and T. Helleseth, "On the cyclotomic generator of order $r$," *Inform. Processing Lett.*, to be published.

[6] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, Pless, Brualdi, and Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[7] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, May 1980.

[8] A. L. Whiteman, "A family of difference sets," *Illinois J. Math.*, vol. 6, pp. 107–121, 1962.

# Frequency and Symbol Rate Offset Compensating Algorithms for Simultaneous Estimation of Echo and Channel Responses

Weiping Li, Xixian Chen, *Member, IEEE*, Yi Wang, and Nobuhiro Miki, *Member, IEEE*

***Abstract*— This correspondence addresses two critical problems in designing new full-duplex fast training algorithms for simultaneously estimating echo and channel responses. Although algorithms of this type have been discussed and evaluated in previous work, the proposed algorithms concentrate on coping with the following two problems that were not solved in the previous approaches: 1) the symbol rate difference between the local transmitter and the remote transmitter, and 2) the frequency offsets in both far echo and far signal that are caused by the analog carrier network. The performance of the new methods is analyzed in terms of mean-square error. Simulation results are presented to confirm the analysis.**

***Index Terms*—Data transmission, digital communications, echo cancellation, equalization.**

## I. Introduction

The techniques of echo cancellation and channel equalization are widely used in high-speed two-wire full-duplex data modems to mitigate leakage of the locally transmitted signal (talker echo) and to cope with the intersymbol interference caused by channel distortion. Before the actual data are transmitted, the echo cancelers and channel equalizers of the modems have to be trained to mimic the characteristics of the echo and channel responses. Therefore, the efficiency of the overall system depends heavily on their initial setup time. A number of fast training algorithms [1]–[6] have been proposed to reduce this system initialization time. During the start-up period, these methods are operated in the half-duplex transmission mode. An exactly known periodic training sequence is alternately sent by each transmitter while the opposite end transmitter is intentionally silenced. The echo canceler and the equalizer at each end are then trained sequentially. After the coefficients of the echo cancelers and the equalizers at both ends converge to their optimum values, the system is switched to the full-duplex transmission mode, and starts transmitting the actual data signals.

In our recent publication [7], we proposed a full-duplex fast training procedure for simultaneously estimating echo and channel responses. Its novelty was that the echo cancelers and the channel equalizers at both ends can be trained simultaneously, rather than separately. The effects of channel noise and symbol rate offset between the local and remote transmitters were analyzed and simulated

Manuscript received March 13, 1996; revised January 8, 1998. The material in this correspondence was presented in part at the 1996 IEEE Global Telecommunication Conference, London, U.K., November 1996.

W. Li is with the Training Center, Beijing University of Posts and Telecommunications, Beijing 100088, China.

X. Chen was with the Department of Telecommunication Engineering, Beijing University of Posts and Telecommunications, Beijing 100088, China. He is now with Wireless Networks, Nortel (Northern Telecom), Ottawa ON, Canada K1A 4H7 (tel.: (613)763-3033 (O); fax: (613)765-6106; e-mail: xixianc@nortel.ca).

Y. Wang is with the Department of Computer Science, University of New Brunswick, Fredericton, BB, Canada (e-mail:yi.wang@unb.ca).

N. Miki is with the Department of Electronics and Information Engineering, Hokkaido University, Sapporo, 060 Japan (tel: +81–11–372-2505; e-mail: miki@cho2.hudk.hokudai.ac.jp).

Publisher Item Identifier S 0018-9448(98)03756-0.