Trace representation of Binary Jacobi Sequences

2003 IEEE ISIT
June 29 - July 4, 2003

Zongduo Dai
State Key Laboratory of Information Security,
Chinese Academy of Sciences, Beijing, China

Guang Gong
Dept. Electrical and Computer Engineering,
University of Waterloo, Waterloo, ON, Canada

Hong-Yeop Song
School of Electrical and Electronics Engineering,
Yonsei University, Seoul, Korea
hy.song@coding.yonsei.ac.kr

I. Binary Jacobi Sequences

◇ **Definition** Let p, q be two distinct odd primes. We define a binary sequence $\mathbf{J}_{p,q} = \{J_{p,q}(t) | t \geq 0\}$ of period pq as

$$J_{p,q}(t) = \begin{cases} 0 & t \equiv 0 \pmod{pq} \\ 1 & t \equiv 0 \pmod{p}, \quad t \not\equiv 0 \pmod{q} \\ 0 & t \not\equiv 0 \pmod{p}, \quad t \equiv 0 \pmod{q} \\ \sigma\left((\frac{t}{p})(\frac{t}{q}) \right) & (t, pq) = 1, \end{cases} \tag{1}$$

where $\sigma(1) = 0$ and $\sigma(-1) = 1$, and $\left(\frac{t}{p}\right)$ is the legendre symbol of the integer t mod p, taking the value $+1$ or -1 according to whether t is a quadratic residue mod p or not. It is clear that

$$\sigma\left((\frac{t}{p})(\frac{t}{q}) \right) = \sigma\left(\frac{t}{p}\right) + \sigma\left(\frac{t}{q}\right).$$

◇ **Example** Jacobi sequence $\mathbf{J}_{3,7} = \{J_{3,7}(t) | t \geq 0\}$ of period 21 is defined as

$$J_{3,7}(t) = \begin{cases} 0 & t \equiv 0 \pmod{21} \\ 1 & t \equiv 0 \pmod{3}, \quad t \not\equiv 0 \pmod{7} \\ 0 & t \not\equiv 0 \pmod{3}, \quad t \equiv 0 \pmod{7} \\ \sigma\left(\left(\frac{t}{3}\right)\left(\frac{t}{7}\right)\right) & (t, 21) = 1. \end{cases}$$

This can be viewed as follows:

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\sigma\left(\left(\frac{t}{3}\right)\right)$		0	1		0	1		0	1		0	1		0	1		0	1		0	1
$\sigma\left(\left(\frac{t}{7}\right)\right)$		0	0	1	0	1	1		0	0	1	0	1	1		0	0	1	0	1	1
$\sigma\left(\left(\frac{t}{3}\right)\left(\frac{t}{7}\right)\right)$		0	1		0	0			1		1	1		1			0	0		1	0
$J_{3,7}(t)$	0	0	1	1	0	0	1	0	1	1	1	1	1	1	0	1	0	0	1	1	0

◇ Relation with Cyclic Hadamard Difference Sets

When $q = p + 2$ so that p and $p + 2$ are both prime (twin prime), the binary jacobi sequence of period $p(p + 2)$ is the characteristic sequence of a cyclic Hadamard difference set with parameter $v = p(p + 2)$, $k = (v - 1)/2$, and $\lambda = (v - 3)/4$, and has the ideal autocorrelation:

$$\phi(\tau) \triangleq \sum_{0 \le t < p(p+2)} (-1)^{J_{p,p+2}(t) + J_{p,p+2}(t+\tau)}$$

$$= \begin{cases} p(p+2), & \tau \equiv 0 \pmod{p(p+2)} \\ -1, & \text{otherwise} \end{cases}$$

Preparation

- Let $\mathbf{s} = \{s(t)|t \geq 0\}$ be a binary sequence of period N that divides $2^n - 1$ for some n.
  $\Longrightarrow$ There exists a primitive N-th root γ of unity and a polynomial $g(x) = \sum_{0 \leq i < N} \rho(i) x^i \pmod{x^N - 1}$ such that

$$s(t) = g(\gamma^t) \qquad t = 0, 1, 2, \ldots$$

- We call the pair $(g(x), \gamma)$ a *defining pair* of the sequence $\mathbf{s}$.
- We will consider only the case where N is either an odd prime or a product of two distinct odd primes.
- The relation between the sequence $\mathbf{s} = \{s(t)|t \geq 0\}$ and its spectral counterpart $\{\rho(i)|i \geq 0\}$ is given as

$$s(t) = \sum_{0 \leq i < N} \rho(i) \gamma^{it} \quad \Longleftrightarrow \quad \rho(i) = \sum_{0 \leq t < N} s(t) \gamma^{-it}.$$

Quadratic Residue Cyclic Difference Sets mod p

- Let p be an odd prime, and F_p be the finite field with p elements. We denote by F_p^* the cyclic multiplicative group $F_p \backslash \{0\}$.
- F_p^* is a disjoint union of $A_0 \triangleq \{x^2 | x \in F_p^*\}$ and $A_1 \triangleq F_p^* \backslash A_0$ of equal size $(p-1)/2$.
- A_0 is a (quadratic residue) cyclic difference set with parameters $(v = p, k = (p-1)/2, \lambda = (p-3)/4)$.
- We let $A_0(x) = \sum_{t \in A_0} x^t \pmod{x^p - 1}$, and $A_1(x) = \sum_{t \in A_1} x^t \pmod{x^p - 1}$, which are called the *generating polynomials* of A_0 and A_1, respectively.
- Let $A(x) = \frac{p-1}{2} + a_0 A_0(x) + a_1 A_1(x) \quad \pmod{x^p - 1}$, where

$$(a_0, a_1) = \begin{cases} (1,0) & \text{if } p \equiv \pm 1 \pmod 8 \\ (\omega, \omega^2) & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

and $\omega \in F_4 \backslash F_2$ is a chosen primitive 3-rd root of unity.

- It is known [Dai-Gong-Song 2002] that one can always find a primitive p-th root α of unity such that

$$A_0(\alpha) = \begin{cases} 1 & p \equiv +1 \pmod 8 \\ 0 & p \equiv -1 \pmod 8 \\ \omega^2 & p \equiv +3 \pmod 8 \\ \omega & p \equiv -3 \pmod 8. \end{cases} \quad (2)$$

- It is also known that if a primitive p-th root α of unity does not satisfies the above condition, then α^u must satisfy the above condition, where u is an arbitrary generator of F_p.
- For this choice of α, it is also known that $A_1(\alpha) = 0, 1, \omega, \omega^2$ for $p \equiv +1, -1, +3, -3 \pmod 8$, respectively.
- With $A(x)$ and α defined above, we have the following basic lemma.

Lemma 1 (Basic Lemma (Dai-Gong-Song 2002)) *Let p be an odd prime, α be chosen by above, and $A(x)$ be as given above. Let $\mathbf{b}_p = \{b_p(t) | t \geq 0\}$ be the sequence of period p defined as*

$$b_p(t) = \begin{cases} 1 & t \in A_0, \\ 0 & t \in F_p \backslash A_0. \end{cases}$$

Then, $(A(x), \alpha)$ is a defining pair of the sequence $\mathbf{b}_p$.

- For the sake of convenience, for any other odd prime q, we let

$$B(x) = \frac{q-1}{2} + b_0 B_0(x) + b_1 B_1(x) \pmod{x^q - 1},$$

where $B_i(x)$ is the generating polynomial of the set B_i for $i = 0, 1$, B_0 is the set of quadratic residues mod q, B_1 is the set of quadratic non-residues mod q, and

$$(b_0, b_1) = \begin{cases} (1, 0) & \text{if } q \equiv \pm 1 \pmod 8 \\ (\omega, \omega^2) & \text{if } q \equiv \pm 3 \pmod 8. \end{cases}$$

- Let $\mathbf{b}_q = \{b_q(t) | t \geq 0\}$ be the sequence of period q defined as

$$b_q(t) = \begin{cases} 1 & t \in B_0, \\ 0 & t \in F_p \backslash B_0. \end{cases}$$

- Then, from Lemma 1, one can find a primitive q-th root β of unity such that $(B(x), \beta)$ is a defining pair of $\mathbf{b}_q$. It is the choice that gives

$$B_0(\alpha) = \begin{cases} 1 & p \equiv +1 \pmod 8 \\ 0 & p \equiv -1 \pmod 8 \\ \omega^2 & p \equiv +3 \pmod 8 \\ \omega & p \equiv -3 \pmod 8). \end{cases} \tag{3}$$

Main Result

- In the remaining of this paper, we keep the notations $A_i(x)$, $B_i(x)$, $A(x)$, $B(x)$, and the choice ω, α and β.
- Also in the remaining, we let e_p and e_q be integers mod pq such that

$$e_p = \begin{cases} 1 & \pmod{p} \\ 0 & \pmod{q}, \end{cases} \quad \text{and} \quad e_q = \begin{cases} 1 & \pmod{q} \\ 0 & \pmod{p}. \end{cases}$$

  Note that e_p and e_q are unique mod pq due to the Chinese Remainder Theorem.
- We let $Tr_1^n(x) = \sum_{0 \le i < n} x^{2^i}$ be the trace of x from F_{2^n} to F_2.
- Modulo 8, the odd primes p and q have 4 difference values, and there are 16 different cases for the pair (p, q). In the following, we group 8 of them together, and distinguish only two cases as follows:

  CASE 1: $(p,q) \in \{(+1,+1),(+1,-1),(-1,+1),(-1,-1),$
  $(+3,+3),(+3,-3),(-3,+3),(-3,-3)\}$; and

  CASE 2: $(p,q) \in \{(+1,+3),(+1,-3),(-1,+3),(-1,-3),$
  $(+3,+1),(+3,-1),(-3,+1),(-3,-1)\}$.

Theorem 1 (Main Theorem) *For any two distinct odd primes p and q, there exist α, β and ω which satisfy the conditions* (2) *and* (3)*, respectively, where α is a p-th primitive root of unity, β is a q-th primitive root of unity and ω is a 3-th primitive root of unity. And recall the choice of all the notations discussed so far. Define a polynomial $J(x) \pmod{x^{pq}-1}$ as follows:*

$$J(x) = \frac{q-1}{2} \sum_{1 \le i < p} x^{e_p i} + \frac{p+1}{2} \sum_{1 \le j < q} x^{e_q j}$$

$$+ \begin{cases} \sum_{i=0,1} A_i(x^{e_p}) B_i(x^{e_q}) & \text{for CASE 1, and} \\ \omega \sum_{i=0,1} A_i(x^{e_p}) B_i(x^{e_q}) + \omega^2 \sum_{i=0,1} A_i(x^{e_p}) B_{i+1}(x^{e_q}) & \text{for CASE 2,} \end{cases}$$

where $B_2(x) = B_0(x)$. Then,

(i) *the Jacobi sequence $\mathbf{J}_{p,q} = \{J_{p,q}(t) | t \ge 0\}$ has a defining pair $(J(x), \alpha\beta)$, and*

(ii) *it has a trace representation as follows:*

$$J_{p,q}(t) = \frac{q-1}{2} \sum_{0 \le i < c_p} \mathsf{Tr}_1^m(\alpha^{u^i t}) + \frac{p+1}{2} \sum_{0 \le j < c_q} \mathsf{Tr}_1^n(\beta^{v^j t})$$

$$+ \begin{cases} \displaystyle\sum_{\substack{0 \le i < c_p \\ 0 \le j < c_q d \\ i \equiv j \pmod 2}} \mathsf{Tr}_1^M\Big((\alpha^{u^i}\beta^{v^j})^t\Big) & \text{for CASE 1, and} \\ \displaystyle\sum_{\substack{0 \le i < c_p \\ 0 \le j < c_q d \\ i \equiv j \pmod 2}} \mathsf{Tr}_1^M\Big(\omega(\alpha^{u^i}\beta^{v^j})^t\Big) + \sum_{\substack{0 \le i < c_p \\ 0 \le j < c_q d \\ i \not\equiv j \pmod 2}} \mathsf{Tr}_1^M\Big(\omega^2(\alpha^{u^i}\beta^{v^j})^t\Big) & \text{for CASE 2,} \end{cases}$$

where m *and* n *are orders of* 2 *mod* p *and* q*, respectively,* $c_p = \frac{p-1}{m}$, $c_q = \frac{q-1}{n}$, $d = (m, n)$ *is the gcd of* m *and* n, $M = mn/d$*, and finally,* u *and* v *are any given generators of* F_p^* *and* F_q^**, respectively.*

Remark 1 The linear complexity $LS(\mathbf{J}_{p,q})$ of $\mathbf{J}_{p,q}$ is given by:

$$LS(\mathbf{J}_{p,q}) = (p-1)\epsilon(\frac{q-1}{2}) + (q-1)\epsilon(\frac{p+1}{2}) + \begin{cases} (p-1)(q-1)/2 & \text{CASE 1,} \\ (p-1)(q-1) & \text{CASE 2,} \end{cases}$$

where $\epsilon(a) = 1, 0$ for $a \equiv 1, 0 \pmod 2$, respectively. ■

Now, we begin the proof of the main theorem.

◇ **Definition** Let T be an odd integer. A δ-sequence of period T, which will be denoted by $\delta_T = \{\delta_T(t) | t \geq 0\}$, is defined as

$$\delta_T(t) = \begin{cases} 1 & t \equiv 0 \pmod T \\ 0 & \text{otherwise.} \end{cases}$$

We also define

$$\Delta_T(x) = \sum_{0 \leq i < T} x^i.$$

It is clear that $(\Delta_T(x), \gamma)$ is a defining pair of the δ-sequence δ_T, where γ is any given T-th primitive root of unity.

◇ **Definition** Given a sequence $\mathbf{s} = \{s(t) | t \geq 0\}$, the λ-jump sequence of $\mathbf{s}$, which will be denoted by $\mathbf{s}^{[\lambda]} = \{s^{[\lambda]}(t) | t \geq 0\}$, is defined as

$$s^{[\lambda]}(t) = \begin{cases} s(t) & t \equiv 0 \pmod{\lambda} \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that the λ-jump sequence of $\mathbf{s}$ is obtained by multiplying $\mathbf{s}$ by δ_λ term-by-term. That is,

$$s^{[\lambda]}(t) = s(t)\delta_\lambda(t), \quad \forall t. \tag{4}$$

Lemma 2

$$\mathbf{J}_{p,q} = \mathbf{b}_p + \mathbf{b}_q + \mathbf{b}_p^{[q]} + \mathbf{b}_q^{[p]} + \delta_p + \delta_{pq}.$$

Proof: Obvious. See the following:

sequences	$t \equiv 0(pq)$	$t \equiv 0(p)$ $t \not\equiv 0(q)$	$t \not\equiv 0(p)$ $t \equiv 0(q)$	$(t, pq) = 1$
$\mathbf{b}_p$	0	0	$\sigma\left(\left(\frac{t}{p}\right)\right)$	$\sigma\left(\left(\frac{t}{p}\right)\right)$
$\mathbf{b}_q$	0	$\sigma\left(\left(\frac{t}{q}\right)\right)$	0	$\sigma\left(\left(\frac{t}{q}\right)\right)$
$\mathbf{b}_p^{[q]}$	0	0	$\sigma\left(\left(\frac{t}{p}\right)\right)$	0
$\mathbf{b}_q^{[p]}$	0	$\sigma\left(\left(\frac{t}{q}\right)\right)$	0	0
δ_p	1	1	0	0
δ_{pq}	1	0	0	0
SUM $= \mathbf{J}_{p,q}$	0	1	0	$\sigma\left(\left(\frac{t}{p}\right)\left(\frac{t}{q}\right)\right)$

Lemma 3 *Defining pairs of six component sequences of* $\mathbf{J}_{p,q}$ *in* Lemma 2 *are given as follows:*

sequences	*defining pair*
$\mathbf{b}_p$	$(A(x^{e_p}), \alpha\beta)$
$\mathbf{b}_q$	$(B(x^{e_q}), \alpha\beta)$
$\mathbf{b}_p^{[q]}$	$(A(x^{e_p})\Delta_q(x^{e_q}), \alpha\beta)$
$\mathbf{b}_q^{[p]}$	$(B(x^{e_q})\Delta_p(x^{e_p}), \alpha\beta)$
δ_p	$(\Delta_p(x^{e_p}), \alpha\beta)$
δ_{pq}	$(\Delta_{pq}(x), \alpha\beta)$

Proof: Obvious.

Lemma 4 *If* $f(x) \equiv g(x) \pmod{x^p - 1}$ *then*

$$f(x^{e_p}) \equiv g(x^{e_p}) \pmod{x^{pq} - 1}.$$

Lemma 5 *The three identities in the following are true:*

(i) $$\Delta_{pq}(x) = 1 + \sum_{1 \le i < p} x^{e_p i} + \sum_{1 \le j < q} x^{e_q j} + \sum_{\substack{1 \le i < p \\ 1 \le j < q}} x^{e_p i + e_q j} \pmod{x^{pq} - 1},$$

(ii) $$\sum_{1 \le i < p} x^{e_p i} = A_0(x^{e_p}) + A_1(x^{e_p}) \pmod{x^{pq} - 1},$$

(iii) $$\sum_{\substack{1 \le i < p \\ 1 \le j < q}} x^{e_q j + e_p i} = \sum_{\substack{i = 0,1 \\ j = 0,1}} A_i(x^{e_p}) B_j(x^{e_q}) \pmod{x^{pq} - 1}.$$

Lemma 6 *Let*

$$J_{p,q}(x) = \frac{q-1}{2} \sum_{1 \le i < p} x^{e_p i} + \frac{p+1}{2} \sum_{1 \le j < q} x^{e_q j} + \sum_{\substack{i=0,1 \\ j=0,1}} (a_i + b_j + 1) A_i(x^{e_p}) B_j(x^{e_q}) \pmod{x^{pq} - 1},$$

where $a_i, b_j, A_i(x), B_j(x)$ *are defined for* $\mathbf{b}_p$ *and* $\mathbf{b}_q$ *in the previous section. Then,* $(J_{p,q}(x), \alpha\beta)$ *is a defining pair of* $\mathbf{J}_{p,q}$*.*

Lemma 7 *A complete set* S *of representatives of conjugacy classes of the* $(p-1)(q-1)$ *primitive* pq*-th roots of unity over* F_2 *is given as:*

$$S = \{ \alpha^{u^i} \beta^{v^j} \mid 0 \le i < c_p,\ 0 \le j < c_q d \}.$$

Finally, using the above and more, we were able to prove the main theorem. Please see the full-version paper (currently on review at some Journal).

Concluding Remarks

- The characteristic sequences of $(v, (v-1)/2, (v-3)/4)$-cyclic Hadamard difference sets are known to have the ideal two-level autocorrelation function, and they have been studied in the community of communications engineering and cryptography.
- Every *known* cyclic Hadamard difference set has the value v which is either (i) a prime congruent to $3 \pmod 4$, (ii) a product of twin primes, or (iii) of the form $2^m - 1$ for some integer m.
- Family (iii) have been intensively studied for long time and their linear complexity and trace representations are now well understood except possibly for the newly discovered hyperoval constructions.
- Recently, in a series of publications, trace representations for the family (i) have been completed.
- This paper determined a trace representation for the family (ii).