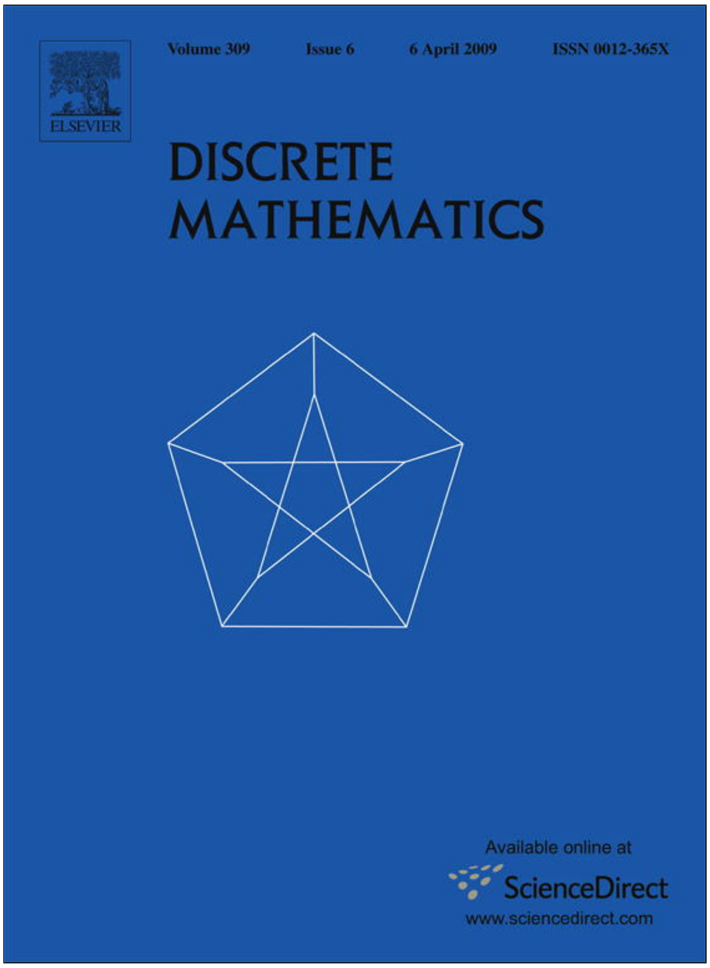
Volume 309
Issue 6
6 April 2009
ISSN 0012-365X
ELSEVIER
DISCRETE
MATHEMATICS
Available online at
ScienceDirect
www.sciencedirect.com

Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Discrete Mathematics 309 (2009) 1517–1527
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

A trace representation of binary Jacobi sequences[☆]

Zongduo Dai[a], Guang Gong[b], Hong-Yeop Song[c,*]

[a] *State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, 100039, Beijing, China*
[b] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada*
[c] *School of Electrical and Electronics Engineering, Yonsei University, Seoul, Republic of Korea*

Received 1 February 2004; received in revised form 19 February 2008; accepted 19 February 2008
Available online 1 April 2008

Abstract

We determine the trace function representation, or equivalently, the Fourier spectral sequences of binary Jacobi sequences of period pq, where p and q are two distinct odd primes. This includes the twin-prime sequences of period $p(p+2)$ whenever both p and $p+2$ are primes, corresponding to cyclic Hadamard difference sets.

Keywords: Cyclic difference sets; Twin-prime cyclic difference sets; Trace representations; (discrete) Fourier spectral sequence; Defining pairs; Binary sequences with two-level autocorrelation; Binary Hadamard sequences

1. Introduction

We will begin by the following definition of Jacobi sequences of period pq for two distinct odd primes p and q:

Definition 1. 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

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

where $\sigma(1) = 0$ and $\sigma(-1) = 1$, and $(\frac{t}{p})$ 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

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

To study the characteristic sequence of cyclic difference sets mod $p(p+2)$ (which has been called "twin-prime cyclic Hadamard difference sets" [21,9]) whenever both p and $p+2$ are prime, Kim and Song [13] have generalized the definition of the characteristic sequences into the cases with sequences of period pq where both p and q are

☆ Part of this paper has been presented in 2003 IEEE International Symposium on Information Theory, Yokohama, Japan.
* Corresponding author.
E-mail addresses: yangdai@public.bta.net.cn (Z. Dai), ggong@calliope.uwaterloo.ca (G. Gong), hysong@yonsei.ac.kr (H.-Y. Song).

0012-365X/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.02.024

two odd primes. The minimal polynomial of these sequences was obtained in [5]. From the well-known result, the trace representation of a Jacobi sequence can be given by $\sum_i \mathrm{Tr}(\rho(i)x^i)$ where $\rho(i) \in F_{2^n}$ (n will be defined later), i is a coset leader modulo $N = pq$, and summution is taken over a set consisting of coset leaders modulo N for which $\rho(i) \neq 0$ (see [17], Exercise 8.41). The trace representation can be computed by applying the (discrete) Fourier transform [2]. $\{\rho(i)\}$ is referred to as a *(Fourier) spectral sequence*. In general, from the minimal polynomial of a sequence, it is not easy to determine the spectral sequence $\{\rho(i)\}$. In this paper, we will determine the trace representation of Jacobi sequences of period pq, i.e., the spectral sequence $\{\rho(i)\}$. As an easy consequence, we determine the linear complexity of the sequence which was obtained earlier [5,13]. The result in this paper makes use of the results in both [14,4].

Section 2 reviews the trace representation of quadratic residue sequences of period p. Section 3 gives the main result with a proof. Section 4 concludes this paper.

2. Preparation

Let $\mathbf{s} = \{s(t)|t \geq 0\}$ be a binary sequence of period N that divides $2^n - 1$ for some n. Then, it is known [17,2,10] that 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

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

We call the pair $(g(x), \gamma)$ a *defining pair* of the sequence $\mathbf{s}$ [4]. In the remainder of this paper, 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

$$s(t) = \sum_{0\leq i<N} \rho(i)\gamma^{it} \quad \Longleftrightarrow \quad \rho(i) = \sum_{0\leq t<N} s(t)\gamma^{-it}. \tag{2}$$

The RHS of (2) is referred to as the *(discrete) Fourier transform of* $\mathbf{s}$, and the LHS of (2), its inverse formula. The main result of this paper is to determine the spectral sequence$\{\rho(i)\}$, or equivalently the defining pair $(g(x), \gamma)$, when $\mathbf{s}$ is a Jacobi sequence.

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 $F_p \setminus \{0\}$. It is well known that F_p^* is a disjoint union of $A_0 \triangleq \{x^2|x \in F_p^*\}$ and $A_1 \triangleq F_p^* \setminus A_0$ of equal size $(p-1)/2$. It is also well known that A_0 is a cyclic difference set with parameters $(v = p, k = (p-1)/2, \lambda = (p-3)/4)$ [1,4,9,11,12,14]. In the remainder of this paper, we let

$$A_0(x) = \sum_{t\in A_0} x^t \pmod{x^p - 1},$$

and

$$A_1(x) = \sum_{t\in A_1} x^t = \sum_{t\in F_p^*\setminus A_0} x^t \pmod{x^p - 1},$$

which are called the *generating polynomials* of A_0 and A_1, respectively. Let

$$A(x) = \frac{p-1}{2} + a_0A_0(x) + a_1A_1(x) \pmod{x^p - 1}, \tag{3}$$

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 $\omega \in F_4 \setminus F_2$ is a chosen primitive 3-rd root of unity. It is known [4] that one can always find a primitive p-th root α of unity such that

$$A_0(\alpha) = \begin{cases} 1 & p \equiv +1 \pmod 8 \\ 0 & p \equiv -1 \pmod 8 \\ \omega^2 & p \equiv +3 \pmod 8 \\ \omega & p \equiv -3 \pmod 8. \end{cases} \tag{4}$$

For this choice of α, we have that $A_1(\alpha) = 0, 1, \omega, \omega^2$ for $p \equiv +1, -1, +3, -3 \pmod 8$, respectively [4]. With $A(x)$ in (3) and α defined above, we have the following basic lemma.

Lemma 2 (*Basic Lemma [4]*). *Let p be an odd prime, α be chosen by (4), and $A(x)$ be as given in (3). Let $\mathbf{b}_p = \{b_p(t) | t \geq 0\}$ be the sequence of period p defined as*

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

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

$$B(x) = \frac{q-1}{2} + b_0 B_0(x) + b_1 B_1(x) \pmod{x^q - 1}, \tag{5}$$

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

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

Then, from Lemma 2, 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

$$B_0(\alpha) = \begin{cases} 1 & p \equiv +1 \pmod 8) \\ 0 & p \equiv -1 \pmod 8) \\ \omega^2 & p \equiv +3 \pmod 8) \\ \omega & p \equiv -3 \pmod 8). \end{cases} \tag{6}$$

In the remainder of this paper, we keep the notations $A_i(x)$, $B_i(x)$, $A(x)$, $B(x)$, which can be regarded as polynomials over some extension of F_2, and the choice ω, α and β. Also in the following, 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 [6].

3. Main result

We let $\mathrm{Tr}_1^n(x) = \sum_{0 \leq i < n} x^{2^i}$ be the trace [17] 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: $(p, q) \in \{(+1, +3), (+1, -3), (-1, +3), (-1, -3), (+3, +1), (+3, -1), (-3, +1), (-3, -1)\}$.

This section is entirely devoted to the proof of the main theorem given as follows:

Theorem 3 (*Main Theorem*). *For any two distinct odd primes p and q, there exist α, β and ω which satisfy the conditions (4) and (6), 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-rd primitive root of unity. Recall the choice of all the notations discussed so far. Define a polynomial $J(x)(\bmod\ x^{pq}-1)$ 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 $\mathbf{J}_{p,q} = \{J_{p,q}(t)|t \ge 0\}$ in Definition 1 has a defining pair $(J(x), \alpha\beta)$, and **(ii)** it has a trace representation as follows:*

$$J_{p,q}(t) = \frac{q-1}{2}\sum_{0\le i<c_p} \mathrm{Tr}_1^m(\alpha^{u^i t}) + \frac{p+1}{2}\sum_{0\le j<c_q} \mathrm{Tr}_1^n(\beta^{v^j t}) + \begin{cases} \sum_{\substack{0\le i<c_p\\ 0\le j<c_q d\\ i\equiv j (\bmod\ 2)}} \mathrm{Tr}_1^M\left((\alpha^{u^i}\beta^{v^j})^t\right) & \text{for CASE 1, and} \\ \sum_{\substack{0\le i<c_p\\ 0\le j<c_q d\\ i\equiv j (\bmod\ 2)}} \mathrm{Tr}_1^M\left(\omega(\alpha^{u^i}\beta^{v^j})^t\right) + \sum_{\substack{0\le i<c_p\\ 0\le j<c_q d\\ i\not\equiv j (\bmod\ 2)}} \mathrm{Tr}_1^M\left(\omega^2(\alpha^{u^i}\beta^{v^j})^t\right) & \text{for CASE 2,} \end{cases}$$

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.

Before we start the proof of the main theorem, we observe the following (see [5,13]):

Remark 4. The linear complexity $LS(\mathbf{J}_{p,q})$ of $\mathbf{J}_{p,q}$ is given from the main theorem as follows:

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

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

Now, we begin the proof of the main theorem.

Definition 5. Let T be an odd integer. A δ-sequence of period T, which will be denoted by $\delta_T = \{\delta_T(t)|t \ge 0\}$, is defined as

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

We also define

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

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

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

Table 1
Proof of Lemma 7

Sequences	$t \equiv 0(pq)$	$t \equiv 0(p)$ $t \not\equiv 0(p)$	$t \not\equiv 0(q)$ $t \equiv 0(q)$	$(t, pq) = 1$
$\mathbf{b}_p$	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	$\sigma\left(\left(\frac{t}{p}\right)\left(\frac{t}{q}\right)\right)$

Table 2
Defining pair of each component sequence in Lemma 8

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}	$(\Delta_{pq}(x), \alpha\beta)$

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,

$$s^{[\lambda]}(t) = s(t)\delta_\lambda(t), \quad \forall t. \tag{7}$$

Lemma 7.

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

Proof. It is straightforward to check. See Table 1. ■

Lemma 8. *The defining pairs of six component sequences of $\mathbf{J}_{p,q}$ in Lemma 7 are given in Table 2.*

Proof. Note that

$$(\alpha\beta)^{e_p} = \alpha, (\alpha\beta)^{e_q} = \beta.$$

Now, it is straightforward to check the following:

$$\begin{aligned}
A((\alpha\beta)^{e_p t}) &= A(\alpha^t) = b_p(t), \quad \forall t. \\
B((\alpha\beta)^{e_q t}) &= B(\beta^t) = b_q(t), \quad \forall t. \\
A((\alpha\beta)^{e_p t})\Delta_q((\alpha\beta)^{e_q t}) &= A(\alpha^t)\Delta_q(\beta^t) = b_p(t)\delta_q(t) = b_p^{[q]}(t), \quad \forall t, \\
B((\alpha\beta)^{e_q t})\Delta_p((\alpha\beta)^{e_p t}) &= B(\beta^t)\Delta_p(\alpha^t) = b_q(t)\delta_p(t) = b_q^{[p]}(t), \quad \forall t,
\end{aligned}$$

where, we use the relation in (7). The remaining two cases can be done similarly. ■

Lemma 9. *If $f(x) \equiv g(x)(\text{mod } x^p - 1)$ then*

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

Proof.

$$\begin{aligned}
&f(x) \equiv g(x) (\text{mod } x^p - 1)\\
&\Rightarrow f(x) - g(x) = (x^p - 1)h(x) \quad \text{for some } h(x)\\
&\Rightarrow f(x^{e_p}) - g(x^{e_p}) = (x^{pe_p} - 1)h(x^{e_p}).
\end{aligned}$$

Since $pe_p \equiv 0 (\text{mod } pq)$, we get $f(x^{e_p}) - g(x^{e_p}) \equiv 0 (\text{mod } x^{pq} - 1)$. ∎

Lemma 10. *The three identities in the following are true:*

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

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

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

Proof. The identity (i) comes from the following:

$$\begin{aligned}
&\{i (\text{mod } pq) \mid 0 \le i < pq\}\\
&\quad = \{e_p i + e_q j (\text{mod } pq) \mid 0 \le i < p, 0 \le j < q\}\\
&\quad = \{0\} \cup \{e_p i (\text{mod } pq) \mid 1 \le i < p\} \cup \{e_q j (\text{mod } pq) \mid 1 \le j < q\}\\
&\qquad \cup \{e_p i + e_q j (\text{mod } pq) \mid 1 \le i < p, 1 \le j < q\}.
\end{aligned}$$

Note that

$$\sum_{1 \le i < p} x^i = \sum_{i \in F_p^*} x^i = \sum_{i \in A_0 \cup A_1} x^i = A_0(x) + A_1(x) (\text{mod } x^p - 1).$$

Now, the assertion (ii) follows from Lemma 9. For (iii), observe the following:

$$\begin{aligned}
\sum_{\substack{1 \le i < p\\ 1 \le j < q}} x^{e_p i + e_q j} &= \left(\sum_{1 \le i < p} x^{e_p i} \right) \left(\sum_{1 \le j < q} x^{e_q j} \right)\\
&= \sum_{i=0,1} A_i(x^{e_p}) \sum_{j=0,1} B_j(x^{e_q})\\
&= \sum_{\substack{i=0,1\\ j=0,1}} A_i(x^{e_p}) B_j(x^{e_q}) (\text{mod } x^{pq} - 1),
\end{aligned}$$

where we use the above identity (ii) in the second equality. ∎

Lemma 11. *Let*

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

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 $\mathbf{J}_{p,q}$.

Proof. Lemmas 7 and 8 imply that $\mathbf{J}_{p,q}$ has a defining pair $(g(x), \alpha\beta)$, where

$$g(x) = A(x^{e_p}) + B(x^{e_q}) + A(x^{e_p}) \Delta_q(x^{e_q}) + B(x^{e_q}) \Delta_p(x^{e_p}) + \Delta_p(x^{e_p}) + \Delta_{pq}(x) (\text{mod } x^{pq} - 1).$$

Therefore, Lemma 10 implies that

$$g(x) = A(x^{e_p})(1+\Delta_q(x^{e_q})) + B(x^{e_q})(1+\Delta_p(x^{e_p})) + \Delta_p(x^{e_p}) + \Delta_{pq}(x)$$
$$= \left(\frac{p-1}{2} + \sum_{i=0,1} a_i A_i(x^{e_p})\right) \sum_{1\le j<q} x^{e_q j} + \left(\frac{q-1}{2} + \sum_{j=0,1} b_i B_i(x^{e_q})\right) \sum_{1\le i<p} x^{e_p i} + 1 + \sum_{1\le i<p} x^{e_p i}$$
$$+ 1 + \sum_{1\le i<p} x^{e_p i} + \sum_{1\le j<q} x^{e_q j} + \sum_{\substack{i=0,1\\ j=0,1}} A_i(x^{e_p}) B_j(x^{e_q}) (\text{mod } x^{pq}-1),$$

which can be re-organized to equal to $J_{p,q}(x) (\text{mod } x^{pq}-1)$. ■

Now, consider the proof of the item (i) of the main theorem. We have shown that $J_{p,q}(x)$ in Lemma 11 and $\alpha\beta$ form a defining pair of the Jacobi sequence. Therefore, we need to show that the last term of $J_{p,q}(x)$ in Lemma 11 is the same as the last term of $J(x)$ in the main theorem. This can easily be done by recalling the definition of a_i, b_j in the previous section. That is, when $(p, q) = (\pm 1, \pm 1) (\text{mod } 8)$, for example, $(a_0, a_1) = (b_0, b_1) = (1, 0)$ and hence, the last term of $J_{p,q}(x)$ in Lemma 11 becomes $A_0(x^{e_p})B_0(x^{e_q}) + A_1(x^{e_p})B_1(x^{e_q})$. The remaining cases can similarly be checked.

For the item (ii) of the main theorem, we consider the set of all the primitive pq-th roots of unity. It is well-known that there are $(p-1)(q-1)$ primitive pq-th roots of unity in the algebraic closure of F_2, all of them are sitting in F_{2^M}, and it is also known that they are partitioned into $(p-1)(q-1)/M$ conjugacy classes over F_2, where $M = mn/d$, $d = (m, n)$. We need the following lemma which gives a complete set S of representatives of these conjugacy classes.

Lemma 12. *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:*

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

Proof. Note that $|S| = c_p c_q d = (p-1)(q-1)/M$. Therefore, it is enough to show that any two elements in S are not conjugate of each other.

Suppose there are two elements in S which are conjugate of each other. Then, there exist $(i, j) \ne (k, l)$ with $0 \le i, k < c_p$ and $0 \le j, l < c_q d$ such that $\alpha^{u^i}\beta^{v^j} \in S$, $\alpha^{u^k}\beta^{v^l} \in S$, and

$$(\alpha^{u^i}\beta^{v^j})^{2^t} = \alpha^{u^k}\beta^{v^l}.$$

This implies

$$\alpha^{u^i 2^t - u^k} = \beta^{v^l - v^j 2^t} \in \langle\alpha\rangle \cap \langle\beta\rangle = \langle 1\rangle,$$

where $\langle\alpha\rangle$ is the cyclic subgroup generated by α. Therefore, we have

$$\begin{cases} u^i 2^t \equiv u^k & (\text{mod } p) \\ v^l \equiv v^j 2^t & (\text{mod } q). \end{cases} \tag{8}$$

Note that $\langle u^{c_p}\rangle = \langle 2\rangle$ is a subgroup of F_p^*, and that $\langle v^{c_q}\rangle = \langle 2\rangle$ is a subgroup of F_q^*. Therefore,

$\exists\lambda$ s.t. $(\lambda, m) = 1$ and $u^{c_p\lambda} \equiv 2 \ (\text{mod } p)$,
$\exists\mu$ s.t. $(\mu, n) = 1$ and $v^{c_q\mu} \equiv 2 \ (\text{mod } q)$.

Therefore,

$$(8) \Rightarrow \begin{cases} u^{c_p\lambda t} \equiv u^{k-i} & (\text{mod } p) \\ v^{c_q\mu t} \equiv v^{l-j} & (\text{mod } q) \end{cases}$$
$$\Rightarrow \begin{cases} c_p\lambda t \equiv k-i & (\text{mod } p-1) \\ c_q\mu t \equiv l-j & (\text{mod } q-1) \end{cases} \tag{9}$$

$$\Rightarrow \begin{cases} c_p | k - i \\ c_q | l - j \end{cases} \tag{10}$$

$$\Rightarrow \begin{cases} k - i = c_p z_p & \text{for some } z_p \\ l - j = c_q z_q & \text{for some } z_q. \end{cases} \tag{11}$$

Note that we have assumed

$$0 \le k < c_p \quad \text{and} \quad 0 \le i < c_p.$$

Therefore, (10) implies

$$k = i. \tag{12}$$

Therefore,

$$\begin{aligned} (9) &\Rightarrow c_p \lambda t \equiv 0 \ (\text{mod } p - 1) \\ &\Rightarrow \lambda t \equiv 0 \ (\text{mod } m) \quad \text{since } c_p = (p-1)/m, \\ &\Rightarrow t \equiv 0 \ (\text{mod } m) \quad \text{since } (\lambda, m) = 1. \end{aligned}$$

Assume that, for some τ,

$$t = m\tau. \tag{13}$$

Then,

$$\begin{aligned} (9) \text{ and } (11) &\Rightarrow c_q \mu t \equiv l - j \equiv c_q z_q (\text{mod } q - 1) \\ &\Rightarrow \mu t \equiv z_q (\text{mod } n) \\ &\Rightarrow \mu m \tau \equiv z_q (\text{mod } n) \\ &\Rightarrow d = (m, n) | z_q \\ &\Rightarrow c_q d | c_q z_q = l - j. \end{aligned}$$

Note that we have assumed

$$0 \le l < c_q d \quad \text{and} \quad 0 \le j < c_q d.$$

Therefore, the above $c_q d | l - j$ implies

$$j = l.$$

Therefore $(i, j) = (k, l)$, which is a contradiction. ■

Now, we are ready for the item (ii) of the main theorem. For the first term in the trace representation, note that $\langle u^{c_p} \rangle = \langle 2 \rangle$ is a subgroup of F_p^*, and hence,

$$F_p^* = \bigcup_{0 \le i < c_p} u^i \langle u^{c_p} \rangle = \bigcup_{0 \le i < c_p} u^i \langle 2 \rangle.$$

Therefore,

$$\begin{aligned} \sum_{1 \le i < p} x^i &= \sum_{j \in F_p^*} x^j = \sum_{j \in \bigcup_{i=0}^{c_p - 1} u^i \langle 2 \rangle} x^j = \sum_{i=0}^{c_p - 1} \sum_{k=0}^{m-1} x^{u^i 2^k} \\ &= \sum_{0 \le i < c_p} \mathrm{Tr}_1^m \left(x^{u^i} \right) (\text{mod } x^p - 1). \end{aligned}$$

Lemma 9 now implies that

$$\sum_{1 \le i < p} x^{e_p i} = \sum_{0 \le i < c_p} \mathrm{Tr}_1^m \left(x^{e_p u^i} \right) (\text{mod } x^{pq} - 1).$$

Substituting $x = (\alpha\beta)^t$ into the above gives

$$\sum_{1\le i<p} x^{e_p i}\bigg|_{x=(\alpha\beta)^t} = \sum_{0\le i<c_p} \mathrm{Tr}_1^m\left(\alpha^{u^i t}\right). \tag{14}$$

Similarly, using the fact that $\langle v^{c_q}\rangle = \langle 2\rangle$ is a subgroup of F_q^*, we get the second term as

$$\sum_{1\le j<q} x^{e_q j}\bigg|_{x=(\alpha\beta)^t} = \sum_{0\le j<c_q} \mathrm{Tr}_1^n\left(\beta^{v^j t}\right). \tag{15}$$

For the third term, recall the notation of A_i, B_j and their generating polynomials $A_i(x)$, $B_j(x)$, respectively.

$$\begin{aligned}
\sum_{\substack{i=0,1\\ j=0,1}} (a_i+b_j+1)A_i(x^{e_p})B_j(x^{e_q}) &= \sum_{\substack{i=0,1\\ j=0,1}} (a_i+b_j+1)\sum_{t\in A_i} x^{e_p t}\sum_{s\in B_j} x^{e_q s}\\
&= \sum_{\substack{i=0,1\\ j=0,1}} (a_i+b_j+1)\sum_{\substack{t\in A_i\\ s\in B_j}} x^{e_p t+e_q s}\\
&= \sum_{\substack{i=0,1\\ j=0,1}} (a_i+b_j+1)\sum_{\substack{0\le t_1<(p-1)/2\\ 0\le s_1<(q-1)/2}} x^{e_p u^{i+2t_1}+e_q v^{j+2s_1}}\\
&= \sum_{\substack{i=0,1\\ j=0,1\\ 0\le t_1<(p-1)/2\\ 0\le s_1<(q-1)/2}} (a_i+b_j+1)x^{e_p u^{i+2t_1}+e_q v^{j+2s_1}}\\
&= \sum_{\substack{0\le i<p-1\\ 0\le j<q-1}} \rho_{i,j} x^{e_p u^i+e_q v^j} \triangleq \zeta(x) \pmod{x^{pq}-1},
\end{aligned}$$

where we use the notation

$$\rho_{i,j} \triangleq a_j + b_j + 1,$$

where the subscripts i and j are understood mod 2. Recall that $(a_0, a_1) = (1, 0)$ or (ω, ω^2) if $p \equiv \pm 1$ or ± 3, respectively, and similarly for (b_0, b_1). Therefore, when $(p, q) = (\pm 1, \pm 1)$ or $(\pm 3, \pm 3)$, i.e., in CASE 1, we have

$$\rho_{i,j} = \begin{cases} 1 & i \equiv j \pmod 2\\ 0 & i \not\equiv j \pmod 2.\end{cases}$$

For CASE 2, on the other hand, we have

$$\rho_{i,j} = \begin{cases} \omega & i \equiv j \pmod 2\\ \omega^2 & i \not\equiv j \pmod 2.\end{cases}$$

Now, consider CASE 1, first. Then,

$$\zeta(x) = \sum_{\substack{0\le i<p-1\\ 0\le j<q-1\\ i\equiv j \pmod 2}} x^{e_p u^i+e_q v^j} \pmod{x^{pq}-1}.$$

Substituting $x = (\alpha\beta)^t$ into $\zeta(x)$ gives the following:

$$\begin{aligned}
\zeta((\alpha\beta)^t) &= \sum_{\substack{0\le i<p-1\\ 0\le j<q-1\\ i\equiv j \pmod 2}} (\alpha\beta)^{t(e_p u^i+e_q v^j)} = \sum_{\substack{0\le i<p-1\\ 0\le j<q-1\\ i\equiv j \pmod 2}} (\alpha^{u^i}\beta^{v^j})^t\\
&= \sum_{\substack{0\le i<c_p\\ 0\le j<c_q d\\ i\equiv j \pmod 2}} \mathrm{Tr}_1^M\left((\alpha^{u^i}\beta^{v^j})^t\right),
\end{aligned} \tag{16}$$

where the last equality comes from Lemma 12. For CASE 2,

$$\zeta(x) = \sum_{\substack{0\le i<p-1\\0\le j<q-1\\ i\equiv j \pmod 2}} \omega x^{e_p u^i+e_q v^j} + \sum_{\substack{0\le i<p-1\\0\le j<q-1\\ i\not\equiv j \pmod 2}} \omega^2 x^{e_p u^i+e_q v^j} \pmod{x^{pq}-1}.$$

Similarly, substituting $x = (\alpha\beta)^t$ into $\zeta(x)$ and using Lemma 12 gives the following:

$$\zeta((\alpha\beta)^t) = \sum_{\substack{0\le i<c_p\\0\le j<c_q d\\ i\equiv j \pmod 2}} \mathrm{Tr}_1^M\left(\omega(\alpha^{u^i}\beta^{v^j})^t\right) + \sum_{\substack{0\le i<c_p\\0\le j<c_q d\\ i\not\equiv j \pmod 2}} \mathrm{Tr}_1^M\left(\omega^2(\alpha^{u^i}\beta^{v^j})^t\right). \tag{17}$$

The item (ii) of the main theorem now follows from (14)–(17), and this finishes the proof of the main theorem.

Example 13. The smallest example would be $(p, q) = (3, 5)$, and this turns out to be the same as the binary m-sequence of period 15. The next is $(p, q) = (3, 7)$, but this case does not correspond to any cyclic difference set. Therefore, we consider the case $(p, q) = (5, 7)$ which gives a binary sequence $\mathbf{J}_{p,q} = \{s(t)\}_{t\ge 0}$ of period 35 with the ideal two-level autocorrelation. Now we consider $\mathbf{J}_{5,7} = \{s(t)\}_{t\ge 0}$. Keeping the notations in the Main Theorem, it is clear that $(p, q) = (5, 7)$ belongs to the CASE 2, and that

$$A_0 = \{1, 4\}, A_1 = \{2, 3\}, m = 4, c_5 = 1, e_5 = 21,$$
$$B_0 = \{1, 2, 4\}, B_1 = \{3, 5, 6\}, n = 3, c_7 = 2, e_7 = 15,$$

$d = 1$, $M = 12$, and that

$$A_0(x) = x + x^4$$
$$A_1(x) = x^2 + x^3$$
$$B_0(x) = x + x^2 + x^4$$
$$B_1(x) = x^3 + x^5 + x^6.$$

According to the Main Theorem, we may take $u = 2$ and $v = 3$, since 2 and 3 are generators of F_5 and F_7, respectively. Note that $5 = -3 \pmod 8$, $7 = -1 \pmod 8$, it belongs to the CASE 2. It is known that there exists a 5-th primitive root α of unity such that $A_0(\alpha) = \omega$, where ω is a 3-rd primitive root of unity, and there exists a 7-th primitive root of unity β such that $B_0(\alpha) = 0$. With such choices of α, ω and β, based on Main Theorem we get the following:

Fact: Keep the notations in the Main Theorem. Let α be a 5-th primitive root α of unity such that $A_0(\alpha) = \omega$, where ω is a 3-rd primitive root of unity, and let β be a 7-th primitive root of unity β such that $B_0(\alpha) = 0$. Then the Jacobi sequence $\mathbf{J}_{5,7}$ has a defining pair $(J(x), \alpha\beta)$ with

$$J(x) = \sum_{1\le i<5} x^{21i} + \sum_{1\le j<7} x^{15j} + \omega\sum_{i=0,1} A_i(x^{21})B_i(x^{15}) + \omega^2\sum_{i=0,1} A_i(x^{21})B_{i+1}(x^{15}),$$

and a trace representation as

$$s(t) = \mathrm{Tr}_1^4\left(\alpha^t\right) + \mathrm{Tr}_1^3\left(\beta^t + \beta^{3t}\right) + \mathrm{Tr}_1^{12}\left(\omega(\alpha\beta)^t + \omega^2(\alpha\beta^3)^t\right), \forall t.$$

Next we show how to get the right elements α, ω and β. In order to choose the right α and ω, we start from a 5-th primitive root θ of unity, which must be a root of the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$ over F_2, hence, $Tr_1^4(\theta) = 1$. Let $\delta = A_0(\theta)$, it is clear that $\delta = A_0(\theta) = \theta + \theta^4 = Tr_2^4(\theta)$, and then that $1 = Tr_1^4(\theta) = Tr_1^2(Tr_2^4(\theta)) = Tr_1^2(\delta)$, which leads to the fact that $\delta \in F_{2^2} \setminus F_2$, hence, δ is a 3-rd primitive root of unity. Thus, $\omega = \delta$ and $\alpha = \theta$ are the right choices. Similarly, in order to choose a right β, we start from a 7-th primitive root θ of unity, say, θ is a root of the primitive polynomial $x^3 + x + 1$ of degree 3 over F_2. It is clear that $B_0(\theta) = \theta + \theta^2 + \theta^4 = \theta + \theta^2 + \theta(1 + \theta) = 0$. Thus, $\beta = \theta$ is a right choice.

4. Concluding remarks

The characteristic sequences of $(v, (v-1)/2, (v-3)/4)$-cyclic Hadamard difference sets [1,9,10,12,20,4] 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(mod 4), (ii) a product of twin primes, or (iii) of the form $2^m - 1$ for some integer m [1,8,12,20]. Family (iii) have been intensively studied for a long time and their linear complexity and trace representations are now well understood except possibly for the newly discovered hyperoval constructions [16,3,7]. Recently, in a series of publications, trace representations for the family (i) have been completed [18,19,14,15,4]. This paper determined a trace representation for the family (ii).

Acknowledgements

Zongduo Dai and Hong-Yeop Song wish to acknowledge Prof. Guang Gong of University of Waterloo who invited them to visit University of Waterloo from July 1 to August 30, 2002, and from Jan. 17 to Feb. 7, 2004, respectively. Zongduo Dai's work was supported by National Natural Science Foundation of CHINA (Grant No. 60173016), and the National 973 Project (Grant No. 1999035804), Guang Gong's work is supported by NSERC, CANADA, and Hong-Yeop Song's work was supported by the grant (R01-2003-000-10330-0) from the Basic Research Program of the Korea Science & Engineering Foundation, KOREA.

References

[1] L.D. Baumert, Cyclic Difference Sets, in: Lecture Notes in Mathematics, vol. 182, Springer-Verlag, New York, 1971.
[2] R.E. Blahut, Theory and Practice of Error Control Codes, Addison-Wesley, Reading MA, 1983.
[3] A. Chang, S.W. Golomb, G. Gong, P.V. Kumar, On ideal autocorrelation sequences arising from hyperovals, in: C. Ding, T. Helleseth, H. Niederreiter (Eds.), Sequences and Their Applications, Proceedings of SETA98, Springer, New York, 1999, pp. 17–38.
[4] Z. Dai, G. Gong, H.-Y. Song, Trace representation and linear complexity of binary e-th residue sequences, WCC 2003, in: International Workshop on Coding and Cryptography, Versailles, France, March 24–28, 2003.
[5] C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, Finite Fields Appl. 3 (2) (1997) 159–174.
[6] C. Ding, D. Pei, A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Coding and Cryptography, World Scientific, Singapore, 1996.
[7] R. Evans, H. Hollmann, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, J. Combin. Theory, Ser. A 87 (1999) 74–119.
[8] S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, CA, 1967, Revised edition, Aegean Park Press, Laguna Hills, CA, 1982.
[9] S.W. Golomb, Construction of signals with favourable correlation properties, in: A.D. Keedwell (Ed.), Survey in Combinatorics, in: LMS Lecture Note Series, vol. 166, Cambridge University Press, 1991, pp. 1–40.
[10] S.W. Golomb, G. Gong, Signal Designs with Good Correlation: For Wireless Communications, Cryptography and Radar Applications, Cambridge University Press, 2005.
[11] D. Jungnickel, Difference sets, in: J.H. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory, John Wiley & Sons, Inc, New York, 1992, pp. 241–324.
[12] J.-H. Kim, H.-Y. Song, Existence of cyclic hadamard difference sets and its relation to binary sequences with ideal autocorrelation, J. Commun. Networks 1 (1) (1999) 14–18.
[13] J.-H. Kim, M. Shin, H.-Y. Song, Linear complexity of Jacobi sequences, pre-print, 1999.
[14] J.-H. Kim, H.-Y. Song, Trace representation of legendre sequences, Des. Codes Cryptogr. 24 (3) (2001) 343–348.
[15] J.-H. Kim, H.-Y. Song, G. Gong, Trace Function Representation of Hall's Sextic Residue Sequences of Period $p \equiv 7 (\mathrm{mod}\ 8)$, in: J.-S. No, H.-Y. Song, T. Helleseth, V. Kumar (Eds.), Mathematical Properties of Sequences and Other Combinatorial Structures, Kluwer Academic Publishing, New York, 2003.
[16] A. Maschietti, Difference sets and hyperovals, Des. Codes Cryptogr. 14 (1998) 157–166.
[17] R. Lidl, H. Niederreiter, Finite Fields, in: Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, 1983 (Chapter 8) (Revised version, Cambridge University Press, 1997).
[18] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, K. Yang, Trace representation of legendre sequences of Mersenne prime period, IEEE Trans. Inform. Theory 42 (6) (1996) 2254–2255.
[19] H.-K. Lee, J.-S. No, H. Chung, K. Yang, J.-H. Kim, H.-Y. Song, Trace function representation of Hall's sextic residue sequences and some new sequences with ideal autocorrelation, in: Proceedings of APCC'97, APCC, Dec. 1997, pp. 536–540.
[20] H.-Y. Song, S.W. Golomb, On the existence of cyclic Hadamard difference sets, IEEE Trans. Inform. Theory 40 (4) (1994) 1266–1268.
[21] R.G. Stanton, D.A. Sprott, A family of difference sets, Canad. Jour. Math. 10 (1958) 73–77.