二值自相关的二元周期序列

曹海涛

南京师范大学

第十届海峡两岸图论与组合学研讨会,台湾,8月18-23, 2019

Outline:

- **Introduction**
- $n \equiv 1 \pmod 4$
- $n \equiv 2 \pmod 4$
- $n \equiv 3 \pmod 4$
- $n \equiv 0 \pmod 4$

Introduction

Definition

For a binary periodical sequence $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}, \ldots)$ with period n and $a_j \in \{-1, 1\}$, $j \geq 0$, the **autocorrelation values** of **a** are defined by

$$C_{\mathbf{a}}(t) = \sum_{i=0}^{n-1} a_i a_{i+t}, \quad t = 0, 1, \ldots, n-1.$$

It is obvious that $C_{\mathbf{a}}(0) = n$, and it is called **trivial** autocorrelation value. These $C_{\mathbf{a}}(t)$, $1 \leq t \leq n-1$, are called **nontrivial** autocorrelation values.

A simple necessary condition for the existence of a binary sequence is

$$C_{\mathbf{a}}(t) \equiv n \pmod 4 \tag{1}$$

for $0 \leq t \leq n-1$.

Binary sequences with 2-level autocorrelation values： all nontrivial autocorrelation values are equal to some constant d ($C_{\mathbf{a}}(t) = d$ for $1 \leq t \leq n-1$).

A binary sequence with 2-level autocorrelation values is called **perfect** if the nontrivial autocorrelation value d is as small as possible in absolute value.

Definition

Let G be an additive group of order n. A k-subset D of G is an (n, k, λ)-**difference set** (briefly (n, k, λ)-DS) if any nonzero element $g \in G$, $d - d_0 = g$ has exactly λ solutions (d, d_0) with $d, d_0 \in D$. The difference set D is **cyclic** (briefly (n, k, λ)-CDS), if the group G has the property.

Example

Let $G = \mathbb{Z}_7$ and $D = \{0, 1, 3\}$. Then D is a $(7, 3, 1)$-CDS.

$$1 - 0 = 1, \quad 3 - 1 = 2, \quad 3 - 0 = 3,$$
$$0 - 3 = 4, \quad 1 - 3 = 5, \quad 0 - 1 = 6.$$

Theorem (Jungnickel and Pott, 1999)

A binary sequence with 2-level autocorrelation values (with all nontrivial autocorrelation values equal to d) is equivalent to an (n, k, λ)-CDS, where $d = n - 4(k - \lambda)$.

Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}, \ldots)$ be a binary periodical sequence and $G = \mathbb{Z}_n$. Let $D = \{0 \le i \le n-1 : a_i = -1\}$.

$C_{\mathbf{a}}(t) = d$, $0 < t \le n-1 \iff D$ is an (n, k, λ)-CDS, where $d = n - 4(k - \lambda)$.

Example

$\mathbf{a} = (-1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, \ldots)$ $(d = 1)$.

Let $G = \mathbb{Z}_{13}$ and $D = \{0, 1, 3, 9\}$. Then D is a $(13, 4, 1)$-CDS.

Let **a** be a binary sequence with $C_{\mathbf{a}}(t) = d$, $0 < t \leq n-1$. By above theorem, **a** corresponds to an (n, k, λ)-CDS. Since $k(k-1) = (n-1)\lambda$, we have

$$(n, k, \lambda) = \left(n, \frac{n - \sqrt{dn + n - d}}{2}, \frac{n + d - 2\sqrt{dn + n - d}}{4}\right). \quad (2)$$

So $dn + n - d \geq 0$ is a perfect square number. Then $d > -2$ when $n > 2$ and $d = -2$ when $n = 2$. For the later case there exists a perfect binary sequence with $(n, d) = (2, 2)$, for example, $(-1, 1, -1, 1, \ldots)$.

$n \equiv 1 \pmod 4$ and $d = 1$

A perfect binary sequence with $d = 1$ corresponds to an $(n, \frac{1}{2}(n - \sqrt{2n-1}), \frac{1}{4}(n + 1 - 2\sqrt{2n-1}))$-CDS, by (2). $n = 5$ and $n = 13$ are the only known perfect binary sequences since there exist (5, 1,0)-CDS and (13,4,1)-CDS.

Theorem

1. There are no perfect binary sequences for $13 < n < 266$. (Turyn, 1965)
2. There are no perfect binary sequences for $13 < n < 20605$, except $n = 181, 4901, 5101, 13613$. (Eliahou, Kervaire, 1992)
3. There are no perfect binary sequences for $13 < n < 20605$. (Broughton, 1994)

Conjecture (Schmidt, 2016)

There are no perfect binary sequences with $n > 13$ and $d = 1$.

If a and b are integers, we say that a is **semiprimitive** modulo b if there exists an integer c such that $a^c \equiv -1 \pmod{b}$.

Let p be a prime. For any nonzero integer m, $v_p(m) = l$ if and only if $p^l | m$ and $p^{l+1} \nmid m$.

Theorem (Lander, 1983)

Suppose that there exists an (n, k, λ)-CDS. Let $e \geq 2$ be a divisor of n, and p be a prime number, and p be semiprimitive modulo e. Then $v_p(k - \lambda)$ is even.

An $(n, \frac{1}{2}(n-\sqrt{2n-1}), \frac{1}{4}(n+1-2\sqrt{2n-1}))$-CDS is a $(\frac{1}{2}(u^2+1), \frac{1}{4}(u-1)^2, \frac{1}{8}(u-1)(u-3))$-CDS if $2n-1=u^2$.

Theorem

Let $u \equiv 3, 7 \pmod{10}$. There does not exist a $(\frac{1}{2}(u^2+1), \frac{1}{4}(u-1)^2, \frac{1}{8}(u-1)(u-3))$-CDS if one of the following two conditions is satisfied:

1. $v_2(u^2-1)$ is even.
2. There exists a prime $p \equiv 2, 3, 4 \pmod{5}$ such that $v_p(u+1)$ or $v_p(u-1)$ is odd.

Equivalently there do not exist perfect binary sequences with $(n, d) = (\frac{1}{2}(u^2+1), 1)$.

Example

1. Let $u \equiv \pm 7, \pm 23 \pmod{80}$ or $u \equiv \pm 33, \pm 97 \pmod{320}$. There do not exist perfect binary sequences with $(n, d) = (\frac{u^2+1}{2}, 1)$. $(p = 2)$

2. Let $u \equiv \pm 13, \pm 23, \pm 43, \pm 83 \pmod{90}$. There do not exist perfect binary sequences with $(n, d) = (\frac{u^2+1}{2}, 1)$. $(p = 3)$

Theorem

Let e be a prime with $e \equiv 1 \pmod 4$. If there exists an integer u satisfying the following two conditions:

1. $2 \nmid u$ *and* $u^2 \equiv -1 \pmod e$.

2. $u \equiv 2^l \cdot c^2 r \pm 1 \pmod{2^{l+1} \cdot c^2 e}$, *where* $c > 0$, $l \geq 0$, $2 | (2^l \cdot c)$, $2 \nmid r$ *and* r *is a nonsquared elements.*

Then there do not exist perfect binary sequences with $(n, d) = (\frac{u^2+1}{2}, 1)$.

Example

1. Let $u \equiv \pm 7 \pmod{20}$ or $u \equiv \pm 55 \pmod{180}$. Then there do not exist perfect binary sequences with $(n, d) = (\frac{u^2+1}{2}, 1)$. $(e = 5)$

2. Let $u \equiv \pm 21 \pmod{52}$. Then there do not exist perfect binary sequences with $(n, d) = (\frac{u^2+1}{2}, 1)$. $(e = 13)$

$n \equiv 2 \pmod 4$ and $d = 2$

A perfect binary sequence with $d = 2$ corresponds to a $(2u, \frac{1}{2}(2u - \sqrt{6u-2}), \frac{1}{2}(u + 1 - \sqrt{6u-2}))$-CDS, by (2).

Theorem (Jungnickel and Pott, 1999)

There are no perfect binary sequences with $d = 2$ for $6 < n < 10^9$ except $n = 12546$, $n = 174726$, $n = 2433602$ and $n = 33895686$.

We use the algebraic number theory to obtain a necessary condition of $(2u, \frac{1}{2}(2u - \sqrt{6u-2}), \frac{1}{2}(u + 1 - \sqrt{6u-2}))$-CDS.

Lemma

If there exists a $(2u, \frac{1}{2}(2u - \sqrt{6u-2}), \frac{1}{2}(u + 1 - \sqrt{6u-2}))$-CDS with odd integer $u \geq 3$, then $u = 2B_i^2 + 1$, where $\varepsilon = 2 + \sqrt{3}$ and $\varepsilon^i = A_i + \sqrt{3}B_i$ for $i \geq 1$.

Lemma

There are no perfect binary sequences with $d = 2$ for $n = 12546$, 174726, 2433602.

$n \equiv 3 \pmod 4$ and $d = 3$

By (2), a binary sequence with $n \equiv 3 \pmod 4$ and $d = 3$ corresponds to $(n, \frac{1}{2}(n - \sqrt{4n-3}), \frac{1}{4}(n + 3 - 2\sqrt{4n-3}))$-CDS. Let $u = \sqrt{4n-3}$. Since $n \equiv 3 \pmod 4$, we have $4n - 3 = u^2$, $u \equiv \pm 3 \pmod 8), u \geq 5$ and $(n, k - \lambda) = (\frac{1}{4}(u^2+3), \frac{1}{16}(u^2-9))$.

Theorem

Let $u \equiv \pm 3 \pmod{24}$. If there exists a prime $p \equiv 2 \pmod 3$ such that $v_p(u^2 - 9)$ is odd, then there does not exist a binary sequence with $(n, d) = (\frac{1}{4}(u^2+3), 3)$.

Example

Let $u \equiv 27, 45, 51, 69 \pmod{72}$. There does not exist a binary sequences with $(n, d) = (\frac{u^2+3}{4}, 3)$.

Theorem

Let e and p be two prime numbers such that $e \equiv 1 \pmod 6$ and p is semiprimitive modulo e. Let $u \equiv \pm 3 \pmod 8$ such that the following two conditions are satisfied:

1. $u^2 \equiv -3 \pmod e$.
2. one of the following three conditions is satisfied:

(i) $p = 2$ and $v_2(u^2 - 9)$ is odd.

(ii) $p = 3$, $v_3(u' - 1)$ or $v_3(u' + 1)$ is odd, where $u = 3u'$.

(iii) $p \geq 5$ and $v_p(u+3)$ or $v_p(u-3)$ is odd.

Then there does not exist a binary sequence with $(n, d) = (\frac{1}{4}(u^2+3), 3)$.

Example

1. There does not exist a binary sequence with $(n, d) = (\frac{u^2+3}{4}, 3)$ for $u \equiv 75, 93 \pmod{1512}$.

2. There does not exist a binary sequence with $(n, d) = (\frac{u^2+3}{4}, 3)$ for $u \in \{37, 59, 85\}$.

Table 1 **Cyclic difference sets for** $n \equiv 3 \pmod 4$, $n = \frac{u^2+3}{4}$ **and** $u \leq 100$

$u \equiv 3 \pmod 8$	11	19	27	35	43	51	59	67	75	83	91	99
n	31	91	183	307	463	651	871	1123	1407	1723	2071	2451
k	10	36	78	136	210	300	406	528	666	820	990	1176
λ	3	14	33	60	95	138	189	248	315	390	473	564
$k-\lambda$	7	22	45	76	115	162	217	280	351	430	517	612
Existence	×	×	×	?	×	×	×	×	×	×	×	×
$u \equiv -3 \pmod 8$	5	13	21	29	37	45	53	61	69	77	85	93
n	7	43	111	211	343	507	703	931	1191	1483	1807	2163
k	1	15	45	91	153	231	325	435	561	703	861	1035
λ	0	5	18	39	68	105	150	203	264	333	410	495
$k-\lambda$	1	10	27	52	85	126	175	232	297	370	451	540
Existence	√	×	×	×	×	×	?	×	×	×	×	×

Question

the nonexistence of binary sequence with $d = 3$ and $n \in \{307, 703\}$.

$n \equiv 0 \pmod 4$ and $d = 4$

By (2), a binary sequence is equivalent to an $(n, \frac{1}{2}(n - \sqrt{5n-4}), \frac{1}{4}(n + 4 - 2\sqrt{5n-4}))$-CDS.

We obtain two binary sequences with $d = 4$ and $n \in \{8, 40\}$ from $(8, 1, 0)$-CDS and $(40, 13, 4)$-CDS. Since $n \equiv 0 \pmod 4$, we may assume that $n = 4u$. Then we have

$(n, k, \lambda) = (4u, 2u - \sqrt{5u-1}, u + 1 - \sqrt{5u-1})$.

Lemma

If there exists a $(4u, 2u - \sqrt{5u-1}, u + 1 - \sqrt{5u-1})$-CDS, then $u = B_i^2 + 1$, where $\varepsilon = \frac{3+\sqrt{5}}{2}$ and $\varepsilon^i = \frac{A_i + \sqrt{5}B_i}{2}$ for $i \geq 1$.

Theorem

There do not exist binary sequences with $n \neq 8, 40$ and $d = 4$.

References

- L. D. Baumert. Cyclic difference sets. Springer-Verlag, Berlin, 1971.
- W.J. Broughton. A note on Table I of : Barker sequences and difference sets. Enseign. Math. 2 40 (1994) 105-107.
- S. Eliahou and M. Kervaire. Barker sequences and difference sets. Enseign. Math. 2 38 (1992) 345-382.
- L. Hua. Introduction to number theory. Springer-Verlag, New York, Pacific Grove, CA, USA, 1982.
- D. Jungnickel and A. Pott. Perfect and almost perfect sequences. Discrete Appl. Math. 95 (1999), 331-359.

- E. S. Lander. Symmetric designs: an algebraic approach. Cambridge University Press, Cambridge, 1983.
- H. Liu and K. Feng. New results on nonexistence of perfect *p*-ary sequences and almost perfect *p*-ary sequences. Acta Math. Sin. 32 (2016), 2-10.
- K. U. Schmidt. Sequences with small correlation. Des. Codes Cryptogr. 78 (2016), 237-267.
- R. J. Turyn. Character sums and difference sets. Pac. J. Math. 15 (1965), 319-346.

Thank you!