Sequences with ideal autocorrelation and Difference sets

T. Helleseth and H. M. Martinsen

Department of Informatics, University of Bergen
Høyteknologisenteret, N-5020 Bergen, Norway.
Email: {torh, halvard}@ii.uib.no

Abstract. We consider ternary sequences and their relation to difference sets. A new infinite family of difference sets with Singer parameters will be presented, constructed from ternary sequences. The paper also presents a new conjectured family of difference sets explaining one of the three unexplained $(121, 40, 13)$ difference sets given by Hall in 1956.

1 Introduction

Let D be a subset of an abelian group G under addition, with $|G| = v$ and $|D| = k$. D is called a (v, k, λ) difference set if

$$x - y = a$$

has exactly λ solutions $(x, y) \in D \times D$ for any $a \neq 0$. Two difference sets D_1 and D_2 with parameters (v, k, λ) are said to be equivalent if there exists a t, $(t, v) = 1$ and a $r \in G$ such that

$$D_1 = \{t \cdot d + r \,|\, d \in D_2\}.$$

Singer [11] discovered a large class of difference sets which are related to finite projective geometry, called Singer difference sets. These difference sets have parameters

$$v = \frac{q^n - 1}{q - 1}, \;\; k = \frac{q^{n-1} - 1}{q - 1}, \;\; \lambda = \frac{q^{n-2} - 1}{q - 1},$$

where $n \geq 3$. The construction of Singer difference sets is as follows. Let F_{q^n} be the finite field of q^n elements and let $Tr_{q^n/q}$ be the trace from F_{q^n} to F_q and let α be a primitive element in F_{q^n}. Let $s(t) = Tr_{q^n/q}(\alpha^t)$ be the m-sequence over F_q. Let

$$D = \{t \,|\, s(t) = 0, \, 0 \leq t \leq (q^n - 1)/q - 1\},$$

or equivalently,

$$D = \{\alpha^t \,|\, Tr_{q^n/q}(\alpha^t) = 0, \, 0 \leq t \leq (q^n - 1)/q - 1\}.$$

Then D is a Singer Difference set.

Recently there has been great progress in finding inequivalent difference sets with Singer parameters, especially in the case of $q = 2$. Construction of such difference sets is highly related to two-level autocorrelation sequences.

Let $s(t)$ be a sequence over F_p, p prime, of length $p^n - 1$. We will call the sequence p-balanced if the number occurrences of $1, 2, \ldots, p-1$ in $s(t)$ is p^{n-1} and the number of zeros in $s(t)$ is $p^{n-1} - 1$. The autocorrelation of the sequence at shift τ is defined by

$$a(\tau) = \sum_{t=0}^{p^n-1} \omega^{s(t+\tau)-s(t)},$$

where ω is a primitive p-th root of unity. An important problem in sequence designs is to find sequences with two-level ideal autocorrelation, i.e., where $a(\tau) = -1$ for any $\tau \neq 0$.

A binary sequence $s(t)$ with ideal autocorrelation gives rise to a difference set with Singer parameters. Let α be a primitive element in F_{2^n}. Let $D \subset F_{2^n}$ be a difference set and let

$$s(t) = \begin{cases} 0 & \text{if } \alpha^t \in D \\ 1 & \text{if } \alpha^t \notin D, \end{cases}$$

then $s(t)$ has ideal autocorrelation.

If $s(t)$ is the binary m-sequence, then D is called the Singer difference set. For recent work on binary sequences with two-level ideal autocorrelation function the reader is referred to [1–3, 7, 9] and [10].

Recently, Helleseth et. al [5], found a new family of ternary sequences $s(t) = Tr_{3^n/3}(\alpha^t + \alpha^{dt})$, $n = 3k$ and $d = 3^{2k} - 3^k + 1$, with ideal autocorrelation. This and the m sequences are the only known infinite families of ternary sequences with ideal autocorrelation. Lin [6] has conjectured that the family of ternary sequences $s(t) = Tr_{3^n/3}(\alpha^t + \alpha^{dt})$, $n = 2m + 1$ and $d = 2 \cdot 3^m + 1$, has ideal autocorrelation.

It is natural to ask if these sequences gives difference sets. The m-sequence is of course by definition the Singer difference set. In the non-binary case, it is to our knowledge unknown if a sequence over $s(t)$ with ideal autocorrelation gives a difference set. We will prove a weaker result on ternary sequences in the next section.

2 Difference sets from a Ternary sequence

In this section let $s(t)$ be a 3-balanced ternary sequence with ideal autocorrelation of period $3^n - 1$. The sequence also satisfies

$$s(t + \frac{3^n - 1}{2}) = -s(t),$$

for all $t \geq 0$. The last criteria only states that the second half of the sequences is the negative of the first half. We have the following result, which we have been unable to find in the literature.

Theorem 1. *Let $s(t)$ be given as above, and let $D = \{t \,|\, s(t) = 0, 0 \leq t < \frac{3^n-1}{2}\}$. Then D is a $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$ difference set.*

Proof: Since $s(t + \frac{3^n-1}{2}) = -s(t)$, we need not reduce t modulo $\frac{3^n-1}{2}$, but calculate modulo $3^n - 1$.

If we can express each residue $\tau \neq 0$ modulo $\frac{3^n-1}{2}$ as $d_i - d_j$ for $d_i, d_j \in D$ in λ different ways, then D is a difference set. That is, if for each $\tau \neq 0$, the numbers of pairs $(t+\tau, t) \in D \times D$ is constant then D is a difference set. If we compare $s(t+\tau)$ and $s(t)$, this is equivalent to show that the number of times $s(t+\tau) = 0$ and $s(t) = 0$ is constant for all τ, $0 < \tau < \frac{3^n-1}{2}$.

We will compare $s(t+\tau)$ and $s(t)$ for all τ, $0 < \tau < \frac{3^n-1}{2}$. Let $a_{i,j}$ be the number of times we compare (i,j). Since the sequences are balanced, $s(t)$ has $3^{n-1} - 1$ zeros, 3^{n-1} ones and 3^{n-1} twos. Since $a_{i,j} = a_{2\cdot i, 2\cdot j}$, we have the following situation,

$s(t)$	1	1	1	2	2	2	0	0	0
$s(t+\tau)$	0	1	2	0	1	2	0	1	2
Times occurring	α	β	γ	α	γ	β	$a_{0,0}$	δ	δ

where $\alpha = a_{1,0} = a_{2,0}$, $\beta = a_{1,1} = a_{2,2}$, $\gamma = a_{1,2} = a_{2,1}$ and $\delta = a_{0,1} = a_{0,2}$. Since $s(t)$ is balanced, we have the following equations.

$$
\begin{aligned}
a_{0,0} + 2\delta &= 3^{n-1} - 1 \\
\alpha + \beta + \gamma &= 3^{n-1} \\
\alpha + \beta + \gamma &= 3^{n-1}.
\end{aligned}
$$

$s(t+\tau)$ is of course also balanced, such that

$$
\begin{aligned}
a_{0,0} + 2\alpha &= 3^{n-1} - 1 \\
\beta + \gamma + \delta &= 3^{n-1} \\
\delta + \beta + \gamma &= 3^{n-1}.
\end{aligned}
$$

Since $s(t)$ has ideal autocorrelation,

$$-1 = (a_{0,0} + a_{1,1} + a_{2,2}) + (a_{1,0} + a_{2,1} + a_{0,2})\omega + (a_{2,0} + a_{0,1} + a_{1,2})\omega^2,$$

and hence,

$$
\begin{aligned}
a_{0,0} + 2\beta &= 3^{n-1} - 1 \\
\alpha + \gamma + \delta &= 3^{n-1} \\
\alpha + \delta + \gamma &= 3^{n-1}.
\end{aligned}
$$

Evaluating these 9 equations we get that $\alpha = \beta = \delta$ and that

$$
\begin{aligned}
\gamma &= a_{0,0} + 1 \\
2\alpha + \gamma &= 3^{n-1}
\end{aligned}
$$

The above comparison was for $1 \leq \tau \leq \frac{3^n-3}{2}$. Compare the two sequences $s(t)$ and $s(t + \tau + \frac{3^n-3}{2})$. Then we will have the following situation.

$s(t)$	1	1	1	2	2	2	0	0	0
$s(t+\tau+\frac{3^n-1}{2})$	0	1	2	0	1	2	0	1	2
Times occurring	α	γ	α	α	α	γ	$a_{0,0}$	α	α

Since $a(\tau) = -1$,

$$\begin{aligned} -1 &= (a_{0,0} + a_{1,1} + a_{2,2}) + (a_{1,0} + a_{2,1} + a_{0,2})\omega + (a_{2,0} + a_{0,1} + a_{1,2})\omega^2 \\ &= (a_{0,0} + 2\gamma) + 3\alpha\omega + 3\alpha\omega^2. \end{aligned}$$

Hence, $3\alpha = 3^{n-1}$, such that $\gamma = 3^{n-2}$. Since $a_{0,0} = \gamma - 1$, we have shown that $a_{0,0}$ is constant for all τ, $1 \leq \tau \leq \frac{3^n-3}{2}$. □

Note that $a_{0,0} = 3^{n-2} - 1 = 2\lambda$ since we counted for all t, $0 \leq t \leq 3^n - 2$.

The result could probably be generalized to any p. We will in the general case assume that $s(t)$ is p-balanced, ideal autocorrelation and that is satisfies the block property. By the block property we mean that the sequence is divided into $p-1$ blocks, such that each block is a unique nonzero scalar multiplication of the first block.

3 Infinite families of Difference sets

The following result follows directly by Theorem 1, if $s(t)$ is 3-balanced.

Theorem 2. *Let $s(t) = Tr_{3^n/3}(\alpha^t + \alpha^{dt})$, $n = 3k$ and $d = 3^{2k} - 3^k + 1$. Let $D = \{t \,|\, s(t) = 0,\, 0 \leq t \leq \frac{3^n-3}{2}\}$, then D is a $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$ difference set.*

Proof: Since $s(t)$ has ideal autocorrelation and obvious satisfies the block property, the only thing left to show, before using Theorem 1, is that it is 3-balanced. This can easily be shown.

Name this difference set as the ternary Kasami difference set.

Given that A. Lin's [6] conjecture is true, which we highly believe, and that $s(t)$ is 3-balanced, then

Theorem 3. *Let $s(t) = Tr_{3^n/3}(\alpha^t + \alpha^{dt})$, $n = 2m+1$ and $d = 2 \cdot 3^m + 1$. Let $D = \{t \,|\, s(t) = 0,\, 0 \leq t \leq \frac{3^n-3}{2}\}$, then D is a $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$ difference set.*

By computer this has been verified up to $n = 11$.

In 1956, Hall [4] described 4 inequivalent $(121, 40, 13)$ difference sets, which have Singer parameters. The first one, see p. 985 in [4] is the Singer Difference set as pointed out in the same paper. Xiang [12] also pointed out that the last three difference sets were unexplained. What is interesting is that difference set number 4 in [4] is equivalent to the difference set constructed by the Lin sequence.

In the construction above, we started with a ternary sequence which had ideal autocorrelation, was 3-balanced and satisfied the block property. We got interested in the two unexplained difference sets given in [4], and named them

B and C. We thought that these difference sets were constructed similarly. That is, the difference sets B and C gave in each case the zero positions in the first block. Then there were 81 positions left. We also assumed that the sequence was constant on cylotomic cosets. We tried all possible combinations of 1 and 2 in these 81 positions, and in each case we scalar multiplied to get the second block. None of the sequences gave ideal autocorrelation. Hence, the difference sets must have another construction.

4 3-ranks of the difference sets

The p-ranks of difference sets have been studied extensively for a couple of reasons. First, if D_1 and D_2 are two equivalent (v, k, λ) difference sets in an Abelian group, then the p-ranks of D_1 and D_2 are the same. Therefore, the p-ranks can help us to distinguish two inequivalent difference sets. Second, let D be a cyclic (v, k, λ) difference set in Z_v, and let $s(t)$ be the characteristic sequence of D, that is

$$s(t) = \begin{cases} 0 & \text{if } t \in D \\ 1 & \text{if } t \notin D. \end{cases}$$

Then $s(t)$ has two-level autocorrelation. and the p-rank is the smallest linear shift register over F_p which generates $s(t)$. Therefore, the study of cyclic difference sets is important for communication and cryptographic applications. The p-rank of the characteristic sequence of the Singer difference sets is known and can be found in [8]. We state the result here.

Theorem 4. *Let D be the $(\frac{p^n-1}{p-1}, \frac{p^{n-1}-1}{p-1}, \frac{p^{n-2}-1}{p-1})$ Singer difference set. Then the p-rank of D is*

$$\binom{p+n-2}{n-1} + 1.$$

We next state conjectures about the 3-rank of the characteristic sequences of the Kasami and the Lin difference sets.

Conjecture 1. Let $n \geq 6$ and let $s(t)$ be the characteristic sequence of the $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$ Kasami difference set. Then the 3-rank of $s(t)$ is given by

$$2n^2 - 2n + 1.$$

Conjecture 2. Let $n \geq 5$ and let $s(t)$ be the characteristic sequence of the $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$ Lin difference set. Then the 3-rank of $s(t)$ is given by

$$2n^2 - 2n + 1.$$

We would assume that the Kasami and the Lin difference sets are equivalent. The first common extension degree n in which they construct a difference set is $n = 9$. By computer we found that in this case, the two difference sets were inequivalent. That brings us to our next conjecture.

Conjecture 3. Let $(\frac{3^n-1}{2}, \frac{3^{n-1}-1}{2}, \frac{3^{n-2}-1}{2})$ be the parameters to the Kasami and the Lin difference set where $n = 3k = 2m + 1$. Then the two difference sets are inequivalent.

References

1. J. Dillon, "Multiplicative difference sets via additive characters", submitted for publication.
2. J. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters", submitted for publication.
3. R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang, "Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets", submitted for publication.
4. M. Hall, Jr., "A survey of difference sets", Proc. Amer. Math. Soc. **7**, 975-986, 1956.
5. T. Helleseth, P. V. Kumar and H. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation function", submitted to Codes, Design and Crytography, 1999.
6. A. Lin, "title unknown", Ph. D. Thesis, University of Southern California, Los Angeles, 1998.
7. A. Maschietti, "Difference sets and hyperovals", *Designs, Codes and Cryptography*, Vol. 14, (1998) pp. 89-98.
8. J. MacWilliams and H. B. Mann, "On the p-rank of the design matrix of a difference set", Inform. Control, Vol. 12, (1968), pp. 474-488.
9. J.S. No, H. Chung and M.S. Yun, "Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation generated by the polynomial $z^d+(z+1)^d$", *IEEE Trans. Inform. Theory*, Vol. 44, (1998) pp. 1278-1282.
10. J.S. No, S.W. Golomb, G. Gong, H.K. Lee and P. Gaal, "Binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation", *IEEE Trans. Inform. Theory*, Vol. 44, (1998) pp. 814-817.
11. J. Singer, "A theorem in finite projective geometry and some applications to number theory", Trans. AMS **43**, 377-385, 1938.
12. Q. Xiang,"Recent results on difference sets with classical parameters", preprint, NATO, 1998.