TABLE I
(I) < G_1 < G_2 < G_3 < G_4 < G_5 < G_6

<table>
<thead>
<tr>
<th>Channel</th>
<th>Message Words</th>
<th>Minimum Distance Squared</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F = 1.1</td>
<td>F = 2</td>
</tr>
<tr>
<td>1</td>
<td>46080</td>
<td>0.0225</td>
</tr>
<tr>
<td>2</td>
<td>23040</td>
<td>0.0247</td>
</tr>
<tr>
<td>3</td>
<td>7680</td>
<td>0.0252</td>
</tr>
<tr>
<td>4</td>
<td>1920</td>
<td>0.0257</td>
</tr>
<tr>
<td>5</td>
<td>384</td>
<td>0.0262</td>
</tr>
<tr>
<td>6</td>
<td>64</td>
<td>0.0267</td>
</tr>
</tbody>
</table>

TABLE II
(I) < S_1 < S_2 < S_3 < S_4 < S_5 < S_6

<table>
<thead>
<tr>
<th>Channel</th>
<th>Message Words</th>
<th>Minimum Distance Squared</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F = 1.1</td>
<td>F = 2</td>
</tr>
<tr>
<td>1</td>
<td>46080</td>
<td>0.0243</td>
</tr>
<tr>
<td>2</td>
<td>23040</td>
<td>0.0247</td>
</tr>
<tr>
<td>3</td>
<td>5760</td>
<td>0.0252</td>
</tr>
<tr>
<td>4</td>
<td>960</td>
<td>0.0263</td>
</tr>
<tr>
<td>5</td>
<td>120</td>
<td>0.0262</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
<td>0.0267</td>
</tr>
</tbody>
</table>

We list below achievable minimum distances and number of message words for certain ratios of minimum distance. The value $F$ is the ratio of the square of the minimum distance of the first channel to that of the last. The minimum distance squared is also given for the optimal single receiver code with the given number of message words which may be generated by $G_6$. Each of these is an upper bound for the minimum distance squared for the corresponding channel.

REFERENCES

Ternary Sequences with Perfect Periodic Autocorrelation
TOM HØHOLDT AND JØRN JUSTESEN

Abstract—We construct 0, ±1 sequences of length $q^{2s+1} - 1$/$q - 1$ with out-of-phase periodic autocorrelation 0, and in-phase correlation $q^{2s}$ such that the peak factor of radiation is $(q^{2s+1} - 1)/(q^{2s+1} - q^{2s})$, which is close to 1 as $q$ becomes large.

In several applications, including estimation of impulse responses and detection of reflected waves, it is important to have periodic sequences $(x_i)$ of period $N$, with periodic autocorrelation function

$$
\sum_{i=1}^{N} x_i x_{i+k} = \begin{cases} M, & \text{if } k \equiv 0 \pmod{N}; \\ 0, & \text{if } k \not\equiv 0 \pmod{N}. 
\end{cases}
$$

We shall say that such sequences have perfect autocorrelation. Further it is desirable that the peak factor $M/N$ be as large as possible when the amplitudes are restricted to $|x_i| \leq 1$. It is well-known that binary maximum length shift register sequences which have $|x_i| = 1$ achieve a small out-of-phase correlation, but it is not exactly 0. However, by allowing $x_i \in \{0, 1, -1\}$, it is possible to obtain sequences with perfect autocorrelation and a large peak factor.

A large class of such ternary sequences was constructed by Ipatov [1], [2] using shift register sequences over GF$(q')$ for $q$ odd. These sequences have length $(q^{2s+1} - 1)/(q - 1)$, but the construction depends heavily on the fact that $q$ is odd. Moharir [3] has given necessary conditions for the existence of perfect ternary sequences and has observed that a construction based on difference sets is sometimes possible. Shedd and Sarwate [4] have constructed perfect ternary sequences of length $2^{s+1}$, based on earlier work of Kasami, Gold, and Helleseth [5], using cross correlation of binary maximum length sequences. Sarwate and Pursley [6] have written an excellent survey on the subject.

In this correspondence we combine ideas of [3] and [4] and use some facts on quadrics in PG$(2s, 2)$, the projective geometry of dimension $2s$ over GF$(2^s)$, to construct perfect ternary sequences of length

$$
\frac{(2^s)^{2s+1} - 1}{2^s - 1},
$$

with peak factor

$$
\frac{(2^s)^{2s+1} - 1}{(2^s)^{2s+1} - (2^s)^{2s}}.
$$

The details of our construction are more difficult than those of [1], but the sequences may be generated more simply. The calculation of the correlation between a received signal and the ternary sequence is also facilitated by the use of a binary ground field.

In Section II we present the construction of ternary sequences with perfect autocorrelation. The proofs of certain properties of projective geometries over GF$(2^s)$ are postponed to Section III. In Section IV we present examples of the most important sequences and details of their construction.

II. THE CONSTRUCTION

For basic facts on difference sets, the reader is referred to [7], let $D = \{i_1, i_2, \ldots, i_v\}$ be a Singer difference set with parameters

$$
n = q^{2s+1} - 1, \quad k = \frac{q^{2s} - 1}{q - 1}, \quad \lambda = \frac{q^{2s-1} - 1}{q - 1},
$$

where $q$ is a prime power. Let $x_D$ denote the characteristic vector of $D$, that is

$$
x_D = (x_1, x_2, \ldots, x_v), \quad x_i = \begin{cases} 1, & i \in D; \\ 0, & i \not\in D. 
\end{cases}
$$

It is well-known that the periodic autocorrelation

$$
R(j) = \sum_{i=1}^{v} x_{i+j} x_i,
$$

satisfies

$$
R(j) = \begin{cases} k, & j \equiv 0 \pmod{v}; \\ \lambda, & j \not\equiv 0 \pmod{v}. 
\end{cases}
$$

0018-9448/83/0700-0597$01.00 ©1983 IEEE
Let \( \hat{D} \) denote another Singer difference-set, with the same parameters as \( D \), and let \( \theta \) denote the sequence obtained by cross correlation of \( x_D \) and \( x_{\hat{D}} \). The periodic autocorrelation of \( \theta \) is then
\[
R_{\theta}(j) = \begin{cases} 
2k^2 + (v - \lambda)k^2, & j \equiv 0 \pmod{v} \\
2k\lambda + (v - \lambda)k^2, & j \not\equiv 0 \pmod{v}.
\end{cases}
\]

The fact that makes our construction work is the following theorem.

**Theorem 1:** Let \( D \) be a Singer difference set with parameters
\[
v = \frac{q^{2l+1} - 1}{q - 1}, \quad k = \frac{q^{2l-1} - 1}{q - 1}, \quad \lambda = \frac{q^{2l-1} - 1}{q - 1}, \quad q = 2^s.
\]
then there exists another Singer difference set \( \hat{D} \) with the same parameters, such that if \( \theta \) denotes the sequence obtained by cross correlating the characteristic vectors \( x_D \) and \( x_{\hat{D}} \), \( \theta \) takes on only three values, namely,
\[
\begin{align*}
g'(q' - 1), & \quad \text{which appears } q'(q' - 1) \text{ times}, \\
g^{2l-1} - 1, & \quad \text{which appears } q^{2l-1} \text{ times}, \\
q^{2l-1} - 1, & \quad \text{which appears } q^{2l-1} \text{ times}.
\end{align*}
\]

The proof of this theorem is given in Section III. Since
\[
(q' + 1)(q' - 1) \quad \text{and} \quad q^{2l-1} - 1,
\]
we obtain, by subtracting \((q^{2l-1} - 1)/(q - 1)\) from each element of \( \theta \), and then dividing all the elements by \( q' \), a sequence \( \hat{\theta} \) with elements \( 0 \) and \( \pm 1 \).

Moreover the periodic autocorrelation of \( \hat{\theta} \) is
\[
R_{\hat{\theta}}(j) = \begin{cases} 
g^{2l}, & j \equiv 0 \pmod{v}; \\
0, & j \not\equiv 0 \pmod{v}.
\end{cases}
\]

This follows from
\[
R_{\hat{\theta}}(j) = R_{\theta}(j) + a^2v - 2a(A(a - x) + Ba + C(a + x)) / x^2,
\]
where
\[
a = q^{2l-1} / q - 1, \quad x = q^{-1}, \\
A = q'(q' - 1) / 2, \quad B = q^{2l-1} / q - 1, \quad C = q'(q' + 1) / 2.
\]

and a straightforward calculation.

Theorem 1 contains an existence statement, but the proof is by construction of the desired \( \hat{D} \). Some examples are given in Section IV.

**III. Proof of Theorem 1**

The proof of Theorem 1 consists of two parts, which are formulated as follows.

**Theorem 2:** Let \( D = (i_1, i_2, \ldots, i_k) \) be a Singer difference set with parameters
\[
v = \frac{q^{2l+1} - 1}{q - 1}, \quad k = \frac{q^{2l-1} - 1}{q - 1}, \quad \lambda = \frac{q^{2l-1} - 1}{q - 1}, \quad q = 2^s,
\]
then there exists \( r \in (1, 2, \ldots, v) \) such that if we construct the hyperplanes of \( PG(2l, q) \) by cyclic shifts of \( D \), the points corresponding to \( rD \) constitute a nondegenerate quadric in \( PG(2l, q) \).

**Theorem 3:** Let \( Q \) be a nondegenerate quadric of \( PG(2l, q) \), \( q = 2^s \). The hyperplanes of \( PG(2l, q) \) is then divided into 3 classes; namely \( q'(q' - 1)/2 \) which have \((q' + 1)(q' - 1)/(q - 1)\) points in common with \( Q \), \( (q^{2l-1} - 1)/(q - 1) \) which have \( (q^{2l-1} - 1)/(q - 1) \) points in common with \( Q \), \( q'(q' + 1)/2 \) which have \((q' - 1)(q' + 1)/(q - 1)\) points in common with \( Q \).

**Proof of Theorem 3:** Let \( Q \) be a nondegenerate quadric of \( PG(2l, q) \), \( q = 2^s \). Following Dickson [8], we can choose coordinates such that \( Q \) has the equation \( x_1^2 + x_2x_3 + \cdots + x_{2l-1}x_{2l} = 0 \), and the equation of a hyperplane is
\[
a_0x_0 + a_1x_1 + \cdots + a_{2l}x_{2l} = 0, \quad a_i \in GF(q), \quad a_0 \neq 0.
\]

Now we consider two cases.

**Case 1:** \( a_0 = 0 \), of course there are \( (q^{2l-1} - 1)/(q - 1) \) of these. We can without loss of generality assume that the hyperplane is
\[
x_0 = a_2x_2 + \cdots + a_{2l}x_{2l}.
\]

Now if \( l = 1 \) we shall find the number of common points of \( x_1 + x_2x_3 = 0 \) and \( x_2 = ax_3 \), and it is easy to see that only \((qa, a, 1)\) satisfies both equations. If \( l > 1 \) we shall count the number of points in the set
\[
\{(x_0, x_1, \ldots, x_{2l}) | x_1 = a_2x_2 + \cdots + a_{2l}x_{2l}, \quad a_0x_0 + a_1x_1 + \cdots + a_{2l}x_{2l} = 0\},
\]

but for each point on the hyperplane \( x_1 = a_2x_2 + \cdots + a_{2l}x_{2l} \), the last equation has exactly one solution \( x_0 \), so the number of points in the set is \((q^{2l-1} - 1)/(q - 1)\).

**Case 2:** \( a_0 \neq 0 \). We can assume that the hyperplane has the equation \( x_0 = a_1x_1 + \cdots + a_{2l}x_{2l} \), so we shall count the number of points in the set
\[
\{(x_0, x_1, \ldots, x_{2l}) | x_0 = a_1x_1 + \cdots + a_{2l}x_{2l}, \quad a_0x_0 + a_1x_1 + \cdots + a_{2l}x_{2l} = 0\},
\]

and \( (a_1x_1 + \cdots + a_{2l}x_{2l})^2 + x_1x_2 + \cdots + x_{2l-1}x_{2l} = 0 \).

Here the last equation is the equation of a nondegenerate quadric \( \hat{Q} \) in \( PG(2l - 1, q) \) and obviously the number of points in the set is equal to the number of points on \( \hat{Q} \). Now in the odd-dimensional projective space there are two kinds of quadrics, namely, the elliptic ones which contain \((q' + 1)(q' - 1)/(q - 1)\) points and hyperbolic ones which contain \((q' - 1)(q' + 1)/(q - 1)\) points. These numbers are due to Primrose [9].

To finish the proof of the theorem we only need to count the number of elliptic (or hyperbolic) quadrics of the form
\[
b_1x_1^2 + \cdots + b_{2l}x_{2l}^2 + x_1x_2 + \cdots + x_{2l-1}x_{2l} = 0.
\]

If \( l = 1 \) this is \( b_1x_1^2 + b_2x_2^2 + x_1x_2 = 0 \), which has a solution for \( q(q + 1)/2 \) choices of \((b_1, b_2)\), this follows for instance from [10,
If \( l > 1 \) the quadric is given by

\[
\begin{pmatrix}
  b_1 & 0 & & & & & x_1 \\
  b_2 & 0 & & & & x_2 \\
  & & \ddots & & & \vdots \\
  0 & & & b_{2l} & & x_{2l-1}
\end{pmatrix}
\begin{pmatrix}
  x_1 \\
  x_2 \\
  \vdots \\
  x_{2l-1}
\end{pmatrix}
+ \begin{pmatrix}
  x_2x_4 & \cdots & x_{2l-1}
\end{pmatrix}
\begin{pmatrix}
  b_2 & & & & & x_4 \\
  & & \ddots & & & \vdots \\
  & & & b_{2l} & & x_{2l}
\end{pmatrix}
= 0
\]

so there is a one-to-one correspondence between those quadrics in PG(2l - 1, q) and the quadric \( y_1y_2^2 + y_2y_3^2 + y_3y_4^2 \) in PG(1, q^2), so by the above result the number of hyperbolic quadrics is \( q'(q^2 + 1)/2 \). This completes the proof of Theorem 3. \( \square \)

**Proof of the Theorem 2:** The Singer difference set \( D \) can be described by choosing a primitive element \( a \) of \( GF(q^{2l+1}) \) and a fixed linear mapping \( L : GF(q^{2l+1}) \to GF(q) \), then \( D = \{ \alpha \} \) for \( \alpha \in (0, 1, \cdots, q - 1) \).

Now define \( f(x, y) : [GF(q^{2l+1})]^2 \to GF(q) \) by \( f(x, y) = L(x^ay^b) \), where \( a, b \) are chosen such that

\[
a \equiv (2^l)^m \pmod{q^{2l+1} - 1},
\]

\[
b \equiv (2^l)^n \pmod{q^{2l+1} - 1},
\]

for some \( m \) and \( n \),

\[
a \neq b,
\]

and such that

\[
r = (a + b)^{-1} \text{ is not congruent to a power of } 2 \pmod{v}.
\]

Then it is easy to see that the mapping \( f(x, y) \) is bilinear and that \( \langle f(x, x) = 0 \rangle \) constitutes a nonsingular quadric in PG(2l, q) consisting of the points corresponding to \( rD \).

The bilinearity is ensured by (5) and that the quadric is nonsingular is ensured by (6) since \( r \) by definition then is a nonmultiplier \( [7, p. 118] \).

Moreover it is a straightforward matter to verify that there indeed are choices of \( a \) and \( b \) which satisfy (5) and (6). This completes the proof of Theorem 2. \( \square \)

Theorem 1 is now easily obtained. The Singer difference set \( D \) can be arbitrary, and we can then, according to Theorem 2 find a number \( r \) such that \( D = rD \) is a quadric of PG(2l, q). Using Theorem 3 we then see that the sequence \( \theta \), obtained by cross correlating the sequences corresponding to \( D \) and \( D \), has the properties claimed in the theorem.

**IV. EXAMPLES**

If \( s - 1 \), that is \( q = 2 \), our construction gives sequences of length \( 2^{2l+1} - 1 \). It is worth noting that the construction here coincides with that of \([4]\), and that the choices of \( D \) and \( rD \) corresponds to choosing words of the first and second order Reed–Muller codes, respectively.

The first interesting new sequences are obtained by setting \( l = 1 \). We will now construct two examples in detail for this special case.

When \( l = 1 \) we are considering lines and quadrics in a projective plane over \( GF(q^2) \); in this case, it is easy to see [7] that as the nonmultiplier \( r \) of the construction we can choose \( r = -1 \), so that the quadric corresponds to \( -D \), where \( D \) is the difference set that gives the lines of the geometry. More specifically if \( s = 2 \), we can as \( D \) use the \((21, 5, 1)\)-Singer difference set \([3, 6, 7, 12, 14] \), \(-D \) is then \([7, 9, 14, 15, 18] \).

The description is facilitated by introducing the cyclotomic classes \( (mod 21) \) that is \( C(j) = \{ j \cdot 2 \pmod{21}, j = 0, 1, \cdots \} \) and it is seen that \( D = C(3) \cup C(7) \) and \(-D \) is \( C(7) \cup C(9) \).

If we crosscorrelate the sequences corresponding to \( D \) and \(-D \) it can be seen that \( |D \cap (-D)| \) is constant when \( t \) belongs to a given cyclotomic class. Moreover \(|D \cap (-D)| = 1 \) if \( t \in -D \), so since \( C(0) \) has size 1, \( C(3) \) has size 3 and \( C(1) \) and \( C(5) \) have size 6, and since we know that the cross correlation takes on the value 0 six times, the value 1 five times, and the value 2 ten times, it is an easy matter to decide whether \( C(1) \) or \( C(5) \) corresponds to the value 2. One gets

\[
|D + t \cap (-D)| = 0,
\]

if \( t \in C(5) = \{ 5, 10, 13, 17, 19, 20 \} \)

\[
|D + t \cap (-D)| = 1,
\]

if \( t \in C(7) \cup C(9) = \{ 7, 9, 14, 15, 18 \} \)

\[
|D + t \cap (-D)| = 2,
\]

if \( t \in C(0) \cup C(1) \cup C(3) = \{ 0, 1, 2, 3, 4, 6, 8, 11, 12, 16 \} \)

so the perfect ternary sequence is

\[
+ + + + + + + + + + + + + + + + + + + + + + + + + + +.
\]

If \( s = 3 \) we can, as \( D \), use \((9, 18, 36, 41, 57, 65, 69, 71, 72) \), and \(-D \) becomes \((1, 2, 4, 8, 16, 32, 37, 55, 64) \).

In this case all the cyclotomic classes except \( C(0) \) have size 9, and again we have \(|D \cap (-D)| = 1 \) if \( t \in -D \). Since the cross correlation will have the value 0 in 28 cases then for \( t = 0 \):

\[
|D + t \cap (-D)| = 0, \quad \text{which is also immediately seen above.}
\]

What remains is to find the three cyclotomic classes, where the cross correlation is 0. One finds that this is the case for \( C(11), C(25), C(13) \), so we get

\[
|D + t \cap (-D)| = 0, \quad \text{for } t = 0, 1, 11, 22, 44, 15, 30, 60, 47, 21, 42, 25, 50, 27, 54, 35, 70, 67, 61, 49, 13, 26, 52, 31, 62, 51, 29, 58, 43
\]

and

\[
|D + t \cap (-D)| = 1, \quad \text{for } t = 1, 2, 4, 8, 16, 32, 37, 55, 64.
\]

The perfect ternary sequence is therefore

\[
-00 + + + + + + + + + + + + + + + + + + + + + + + + + + +.
\]

As a concluding remark, we mention that the correlation of a received signal with the ternary sequences we have constructed can be obtained by correlating the received signal with the binary sequences given by \( D \) and \(-D \), subtracting them, and then scaling the result.

**REFERENCES**


On the Characterization of PN Sequences

UNJENG CHENG, MEMBER, IEEE, AND SOLOMON W. GOLOMB, FELLOW, IEEE

Abstract—Balanced binary sequences of period $2^m - 1$ with the run property and the two-level autocorrelation property are not necessarily PN sequences.

In [1] a hierarchy of classes of binary sequences of period $2^m - 1$ was presented, and several conjectures about the intersections of these classes were offered. The hierarchy is summarized in Fig. 1, where $U$ is the class of all binary sequences of period $2^m - 1$, and PN is the class of maximum-length shift register sequences of period $2^m - 1$. The intermediate classes are $R$ (the “run property”), $M$ (the “multiplicity property”), and $C$ (the two-level correlation property). The intermediate classes are $R \cap C = \text{PN}$. Explicitly, the sequence is

\[
\begin{align*}
\text{U} & \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quan...