PORTUGALIAE MATHEMATICA
Vol. 56 Fasc. 3 – 1999

PRIMITIVE QUADRATICS REFLECTED IN B_2-SEQUENCES

B. Lindström

Abstract: A B_2-sequence of positive integers $a_1, a_2, ..., a_r$ has the property that the sums $a_i + a_j$, $1 \le i \le j \le r$, are different. R.C. Bose and S. Chowla have proved the existence of B_2-sequences of size $r = q$, a power of a prime p, such that the sums $a_i + a_j$, $1 \le i \le j \le r$, are different modulo $q^2 - 1$. If $\theta \in GF(q^2)$ is a primitive element, then $A(q, \theta) = \{a\colon 1 \le a < q^2 - 1, \, \theta^a - \theta \in GF(q)\}$ gives a Bose–Chowla sequence.

The main result of this paper is a characterization of primitive quadratics over $GF(2^k)$ in terms of coefficients (Theorem 2). This characterization depends on polynomials over $GF(2)$ defined by a recursion. In Theorem 1 we give a shortcut to the computation of these polynomials.

O. Moreno has proved the existence of primitive quadratics $X^2 + X + v$ over $GF(2^k)$. It is unknown how many there are. In Theorem 3 we prove that the number of Moreno quadratics, divided by 2, equals the number of elements $a \in A(2^k, \theta)$ with $\gcd(a, 2^{2k} - 1) = 1$, when θ is a root of any Moreno quadratic.

1 – Introduction

A quadratic polynomial $X^2 + uX + v$ over $GF(2^k)$ is *primitive* when the powers of a root give all non-zero elements of $GF(2^{2k})$. A simple example of a primitive polynomial is $X^2 + X + \alpha$ over $GF(4) = \{0, 1, \alpha, \alpha^2\}$. On the other hand, the quadric $X^2 + \alpha X + 1$ is irreducible but not primitive: if θ is a root then $\theta^5 = 1$.

I will give a criterion for quadric over $GF(2^k)$ to be primitive. I am interested in primitive quadrics because they can be used in the construction of B_2-sequences. A *B_2-sequence* is a sequence of positive integers $a_1, a_2, ..., a_r$ such that the sums $a_i + a_j$, $1 \le i \le j \le r$, are distinct. These are sometimes called Sidon sequences because S. Sidon [6] came up with them in a question on Fourier

Received: July 20, 1997.
1991 Mathematics Subject Classification: 11B50, 11B83, 11T06.

series. *Golomb rulers* is another name. These are sequences on non-negative integers such that all non-zero differences of them are different. Golomb rulers may be applied in coding theory, circuit layout and radio astronomy.

For an elementary introduction to Golomb rulers see [2]. B_h-sequences, a generalization of B_2-sequences, are discussed in Chapter 2 of the monograph [3] of H. Halberstam and K.F. Roth.

I will now mention briefly how B_2-sequences can be determined from primitive quadratics. Bose and Chowla proved [1] that

$$A = \Big\{a\colon\ 1 \le a < q^2-1,\ \theta^a-\theta \in GF(q)\Big\} \tag{1.1}$$

gives a B_2-sequence when θ is primitive in $GF(q^2)$. If θ is a root of a primitive quadratic $X^2 - uX + v$ over $GF(q)$ and we define $u_i, v_i \in GF(q)$ for $i \ge 1$ by

$$\theta^i = u_i\,\theta - v_i \tag{1.2}$$

and u_i can be computed recursively by

$$u_1 = 1\,, \quad u_2 = u \quad \text{and} \quad u_{i+1} = u\,u_i - v\,u_{i-1},\ \ i \ge 2\ . \tag{1.3}$$

The i for which $u_i = 1$ belong to the B_2-sequence A. This algorithm is due to Z. Zhang [7], Lemma 4.6. The algorithm was improved by me in [4], which also contains a criterion for primitive quadratic over fields of *odd* characteristic [4], Theorem 3.1. We are concerned with a criterion for *even* characteristic.

2 – A sequence of polynomials

Our criterion for primitive quadratics, Theorem 2, depends on certain polynomials $P_n(X)$ over $GF(2)$, which are defined recursively by

$$P_0(X) = 1,\ \ P_1(X) = 1 + X,\ \ P_{n+1}(X) = X P_n(X) + P_{n-1}(X)\ , \tag{2.1}$$

where all coefficients are 0 or 1 (mod 2). Here are the first few polynomials, except P_0 and P_1

$$\begin{aligned}
P_2(X) &= X^2 + X + 1\\
P_3(X) &= X^3 + X^2 + 1\\
P_4(X) &= X^4 + X^3 + X^2 + 1\\
P_5(X) &= X^5 + X^4 + X^2 + X + 1\\
P_6(X) &= X^6 + X^5 + X^4 + X + 1\ .
\end{aligned}$$

It is tedious to compute the polynomials using (2.1) when n is large, but we need them. For example, to find a quadratic over $GF(2^7)$ we need $P_{21}(X)$ and to find one over $GF(2^9)$ we need $P_{85}(X)$. But Theorem 1 below gives a short cut. By this theorem we have

$$X^2\,P_{21}(X) = P_3(X)\,P_5^4(X) + P_4^4(X)\ ,$$
$$X^8\,P_{85}(X) = P_{13}(X)\,P_5^{16}(X) + P_2(X)\,P_4^{16}(X)$$

(let $r=2$, $c=5$, $s=1$, resp. $r=4$, $c=5$, $s=5$).

Theorem 1. *Let r, c, s be integers, $r, c \geq 1$, $R = 2^r$ and $-R/2 \leq s < R/2$. Then we have*

$$X^{R/2}\,P_{Rc+s}(X) = P_{R/2+s}(X)\,P_c^R(X) + P_{R/2-s-1}(X)\,P_{c-1}^R(X)\ . \tag{2.2}$$

Proof: We have, by induction over $n \geq 1$

$$P_n(w+w^{-1}) = w^n + w^{n-1} + \cdots + w^{-n}\ . \tag{2.3}$$

The following relations follow easily if $X = w + w^{-1}$

$$\begin{aligned}(w^a + w^{-a})\,P_b(X) &= P_{a+b}(X) + P_{b-a}(X)\,, \qquad 0 < a \leq b\\ &= P_{a+b}(X) + P_{a-b-1}(X)\,, \qquad a > b\ .\end{aligned} \tag{2.4}$$

The theorem is proved by induction over $c \geq 1$ when $X = w + w^{-1}$. Note that $x^{R/2} = w^{R/2} + w^{-R/2}$ since R is a power of 2, the characteristic.

We consider first the case $c = 1$. Let $a = R/2$ and $b = R + s$ in (2.4). We find that

$$X^{R/2}\,P_{R+s}(X) = P_{3R/2+s}(X) + P_{R/2+s}(X)\ . \tag{2.5}$$

Then let $a = R$ and $b = R/2 + s$ in (2.4). This gives

$$X^R\,P_{R/2+s}(X) = P_{3R/2+s}(X) + P_{R/2-s-1}(X)\ . \tag{2.6}$$

The relation (2.2) for $c = 1$ follows by (2.5) and (2.6) since $P_1^R(X) = 1 + X^R$ and $P_0^R(X) = 1$.

The case $c = 2$ of (2.2) can be verified similarly. We leave this for the reader.

Let $a = R$ and $b = Rc + 1$ in (2.4). Then we find that

$$X^R\,P_{Rc+s}(X) + P_{R(c-1)+s}(X) = P_{R(c+1)+s}(X)\ . \tag{2.7}$$

By (2.1) we have since R is a power of 2,

$$X^R P_c^R(X) + P_{c-1}^R(X) = P_{c+1}^R(X) \ . \tag{2.8}$$

Assume that (2.2) holds for c and $c-1$. Consider the linear combination with coefficients X^R and 1 and apply (2.7) and (2.8). Then (2.2) follows for $c+1$. ∎

3 – Primitive quadratics

For $y \in GF(2^k)$ define the trace $\mathrm{Tr}(y)$ by

$$\mathrm{Tr}(y) = y + y^2 + y^4 + \cdots + y^{2^{k-1}} \ . \tag{3.1}$$

Note that $\mathrm{Tr}(y)^2 = \mathrm{Tr}(y)$ since $y^{2^k} = y$, and we have

$$\mathrm{Tr}(y) = 0 \quad \text{or} \quad 1 \ . \tag{3.2}$$

Lemma 3.1. *The quadric $X^2 + uX + v$ over $GF(2^k)$ is irreducible if and only if $u \neq 0$ and $\mathrm{Tr}(v/u^2) = 1$. A root θ of the irreducible quadric satisfies $\theta^{2^k+1} = v$.*

Proof: Assume that $u \neq 0$. Then we have $(\theta/u)^2 + (\theta/u) = v/u^2$ when θ is a root. Repeated squarings of this relation gives

$$(\theta/u)2^{i+1} + (\theta/u)^{2^i} = (v/u^2)^{2^i} \qquad \text{for} \ \ i \geq 0 \ .$$

The sum of these relations when $i = 0, ..., k-1$ gives

$$\mathrm{Tr}(v/u^2) = (\theta^{2^k} + \theta)/u \ . \tag{3.3}$$

If the quadric is irreducible, then θ and θ^{2^k} are distinct roots and we have $u = \theta + \theta^{2^k} \neq 0$ and $v = \theta^{2^k+1}$ by the relation between roots and coefficients in a quadric. Hence, $\mathrm{Tr}(v/u^2) = 1$ by (3.3).

Conversely, if $u \neq 0$ and $\mathrm{Tr}(v/u^2) = 1$, then $\theta^{2^k} \neq \theta$ by (3.3) and $\theta \notin GF(2^k)$, i.e. the quadratic is irreducible. ∎

Lemma 3.2. *If the quadric $X^2 + uX + v$ over $GF(2^k)$ is primitive, then v is primitive in $GF(2^k)$.*

Proof: Let θ be a root of the quadric. By Lemma 3.1 we have $v = \theta^{2^k+1}$. It follows that the order of v is $2^k - 1$. ∎

Lemma 3.3. *Assume that the quadric X^2+uX+v over $GF(2^k)$ is irreducible and v primitive in $GF(2^k)$. If θ is a root, we have order$(\theta) = a(2^k-1)$, where a is a divisor of 2^k+1, and $P_{(a-1)/2}(u^2/v) = 0$. If $P_n(u^2/v) = 0$, then order$(\theta) \leq (2n+1)\,(2^k-1)$.*

Proof: Since $0 \neq \theta \in GF(2^{2k})$, the order of θ divides $2^{2k}-1$. We may write order$(\theta) = a\,b$, where $a \mid 2^k+1$ and $b \mid 2^k-1$, since 2^k+1 and 2^k-1 are relatively prime. From $\theta^{ab} = 1$, we get $\theta^{(2^k+1)b} = 1$ and $v^b = 1$ by Lemma 3.1. Hence, $b = 2^k-1$, for v is primitive in $GF(2^k)$ by assumption. Now we have order$(\theta) = a(2^k-1)$ and $\theta^{a(2^k-1)} = 1$. If we multiply this relation by θ^{2a}, we find that $\theta^{2a} = v^a$ and we have

$$w^a = 1, \qquad \text{with } \ w = \theta^2/v \ . \tag{3.4}$$

Note that $w \neq 1$ since $u \neq 0$ by Lemma 3.1. If we expand $(w^a-1)/(w-1)$ we find

$$w^{a-1} + w^{a-2} + \cdots + 1 = 0 \ . \tag{3.5}$$

We may write $a = 2c+1$ since a is odd $(a \mid 2^k+1)$. When we divide (3.5) by w^c, we find that

$$w^c + w^{c-1} + \cdots + w^{-c} = 0 \ . \tag{3.6}$$

By (2.3) we may write this

$$P_c(w + w^{-1}) = 0 \ . \tag{3.7}$$

If we square the relation $\theta^2 + v = u\,\theta$ and divide by $\theta^2\,v$, we find that

$$w + w^{-1} = u^2/v \ . \tag{3.8}$$

Recall that $a = 2c+1$. By (3.7) and (3.8) we have

$$P_{(a-1)/2}(u^2/v) = 0 \ . \tag{3.9}$$

If $P_n(u^2/v) = 0$, we have $P_n(w+w^{-1}) = 0$ by (3.8). Working backwards from (3.7), with n in place of c, we find that $\theta^{(2n+1)(2^k-1)} = 1$ and order$(\theta) \leq (2n+1)\,(2^k-1)$ follows. ∎

Theorem 2. *The quadratic X^2+uX+v over $GF(2^k)$ is primitive if and only if the following conditions are satisfied* (**a**) *$u \neq 0$ and $\mathrm{Tr}(v/u^2) = 1$,*

(**b**) *v is a primitive element in $GF(2^k)$,*

(**c**) *$P_{(a-1)/2}(u^2/v) \neq 0$ when a is a proper divisor of 2^k+1 (alt. for all proper prime divisors p of 2^k+1 and $a = (2^k+1)/p$).*

Proof: Assume that the quadratic is primitive. The necessity of (a), (b) and (c) then follows by Lemma 3.1, 3.2 and 3.3.

Assume that (a), (b) and (c) are satisfied. The quadric is then irreducible by Lemma 3.1. If $P_{(a-1)/2}(u^2/v) \neq 0$ when a is a proper divisor of 2^k+1, we conclude by Lemma 3.3 that $\mathrm{order}(\theta) = 2^{2k}-1$, i.e. θ is primitive in $GF(2^{2k})$.

If $P_{(a-1)/2}(u^2/v) \neq 0$ when $a = (2^k+1)/p$ and p is any proper prime divisor, then $w^a \neq 1$, and $w^b \neq 1$ for any proper divisor $b \mid 2^k+1$. hence, θ is primitive. ∎

Example. Suppose we want a primitive X^2+X+v with $v \in GF(2^7)$. Since $2^7+1 = 3 \cdot 43$ we need a primitive v in $GF(2^7)$ with $\mathrm{Tr}(v) = 1$ and $P_1(v^{-1}) \neq 0$ and $P_{21}(v^{-1}) \neq 0$. Only the last inequality is a serious restriction. In fact, $P_{21}(X)$ is the product of 3 primitive polynomials of degree 7 over $GF(2)$:

$$X^7+X+1\,, \quad X^7+X^6+X^5+X^4+X^2+X+1\,, \quad X^7+X^5+X^4+X^3+X^2+X+1\,.$$

The coefficients of the X-term is 1 in all three implying that the inverse of any root has trace 1. Hence, 21 primitive v of trace 1 are excluded. But there are 63 primitive elements of trace 1 in $GF(2^7)$ and there remains 42 that can be used in a quadratic X^2+X+v. One of them is $v = \alpha^{-3}$ if α satisfies $\alpha^7+\alpha+1 = 0$. If θ is a root of $X^2+X+\alpha^{-3}$ we find the B_2-sequence $A(2^7,\theta) = (1)_{14} \cup (147)_{14} \cup (227)_{14} \cup (491)_{14} \cup (741)_{14} \cup (859)_{14} \cup (1944)_{14} \cup (2653)_{14} \cup (3059)_{14} \cup (5461)_2$, where $(a)_s = \{a, 2a, 2^2a, ..., 2^{s-1}a\}$ and $2^s a \equiv a \pmod{2^{14}-1}$. Observe that 6 generators (1, 227, 491, 859, 2653, 3059) are relatively prime to $2^{14}-1$, which gives 84 elements with this property.

O. Moreno proved the existence of primitive quadratics X^2-X+v "of trace 1" over $GF(q)$ in [5]. It is unknown how many there are. In the previous example the number is half as large as the number of elements in $A(2^7,\theta)$ relatively prime to $2^{14}-1$. This is no accident. It is a special case of the following result.

Theorem 3. *The number of primitive quadratics X^2+X+v over $GF(2^k)$ is half as large as the number of $a \in A(2^k,\theta)$ which are relatively prime to $2^{2k}-1$, when θ is a root of any of these quadratics.*

Proof: Let

$$A = A(2^k, \theta) = \left\{a\colon\, 1 \le a < 2^{2k} - 1,\; \theta^a + \theta \in GF(2^k)\right\} , \tag{3.10}$$

where θ is a root of a (Moreno) primitive quadratic

$$X^2 + X + v\,, \qquad v \in GF(2^k)\ . \tag{3.11}$$

Observe that

$$a \in A \quad \text{implies} \;\; 2a \in A \;(\mathrm{mod}\, 2^{2k} - 1)\ . \tag{3.12}$$

For $\theta^a + \theta \in GF(2^k)$ gives $\theta^{2a} + \theta = (\theta^a + \theta)^2 + v \in GF(2^k)$.

Assume that $a \in A$ is relatively prime to $2^{2k} - 1$. Then θ^a is a primitive element in $GF(2^{2k})$. We have $\theta^a = \theta + z$ with $z \in GF(2^k)$. It follows that $(\theta^a)^2 + \theta^a = \theta^2 + \theta + z^2 + z = v + z^2 + z\ (= w) \in GF(2^k)$ and θ^a is root of a primitive quadratic $X^2 + X + w$. The second root is θ^{a2^k} with $a2^k \in A$ by (3.12). Hence, for each pair $\{a,\, a2^k\}$ of elements in A there is a Moreno quadratic.

Conversely, let $X^2 + X + w$ be a primitive quadratic over $GF(2^k)$ and θ_1 one root. Then we have $\theta_1 = x\,\theta + y$, where $x, y \in GF(2^k)$. We find that $w = \theta_1^2 + \theta_1 = (x^2 + x)\,\theta + x^2 v + y^2 + y$. This implies that $x^2 + x = 0$ and $x = 0$ or 1. But $x = 0$ is impossible since $\theta_1 \notin GF(2^k)$. Therefore $x = 1$ and $\theta_1 = \theta + y$. We conclude then that $\theta_1 = \theta^a$, $a \in A$, where a is relatively prime to $2^{2k} - 1$ since θ_1 is primitive. A second root is $\theta_1^{2^k} = \theta^{a2^k}$.

Therefore there is a one-one correspondence between pairs $\{a,\, a2^k\}$ of elements in A with $\gcd(a, 2^{2k} - 1) = 1$ and Moreno quadratics over $GF(2^k)$, and the theorem follows. ∎

REFERENCES

[**1**] Bose, R.C. and Chowla, S. – Theorems in the additive theory of numbers, *Comment. Math. Helv.,* 37 (1962–63), 141–147.

[**2**] Dewdney, A.K. – *The Armchair Universe*, Freeman & Co., New York, 1988.

[**3**] Halberstam, H. and Roth, K.F. – *Sequences*, Oxford University Press, 1966.

[**4**] Lindström, B. – Finding finite B_2-sequences faster, *Math. of Computation,* 67 (1988), 1173–1178.

[**5**] Moreno, O. – On the existence of a primitive quadratic of trace 1 over $GF(p^m)$, *J. Comb. Theory A* 51 (1989), 104–110.

[**6**] Sidon, S. – Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier–Reihen, *Math. Ann.,* 106 (1932), 536–539.

[**7**] Zhang, Z. – Finding finite B_2-sequences with larger $m - a_m^{1/2}$, *Math. of Computation,* 63 (1994), 403–414.

Bernt Lindström,
Department of Mathematics, Royal Institute of Technology,
S-100 44 Stockholm – SWEDEN