FINDING FINITE $B_2$-SEQUENCES FASTER

BERNT LINDSTRÖM

Abstract. A $B_2$-sequence is a sequence $a_1 < a_2 < \cdots < a_r$ of positive integers such that the sums $a_i + a_j$, $1 \leq i \leq j \leq r$, are different. When $q$ is a power of a prime and $\theta$ is a primitive element in $GF(q^2)$ then there are $B_2$-sequences $A(q, \theta)$ of size $q$ with $a_q < q^2$, which were discovered by R. C. Bose and S. Chowla.

In Theorem 2.1 I will give a faster alternative to the definition. In Theorem 2.2 I will prove that multiplying a sequence $A(q, \theta)$ by integers relatively prime to the modulus is equivalent to varying $\theta$. Theorem 3.1 is my main result. It contains a fast method to find primitive quadratic polynomials over $GF(p)$ when $p$ is an odd prime. For fields of characteristic 2 there is a similar, but different, criterion, which I will consider in “Primitive quadratics reflected in $B_2$-sequences”, to appear in Portugal. Math. (1999).

1. Introduction

A sequence of positive integers $a_1 < a_2 < \cdots < a_r$ is called a $B_2$-sequence (or Sidon sequence) if the sums $a_i + a_j$, $1 \leq i \leq j \leq r$, are different. Erdős and Turán proved in [4] that $r < n^{1/2} + O(n^{1/4})$. This was improved by the author in [5] to $r < n^{1/2} + n^{1/4} + 1$. Erdős asked in [3] if $r < n^{1/2} + C$ is true for a constant $C$.

$B_2$-sequences with $r > n^{1/2}$ are known to exist by a theorem of Bose and Chowla [1]. Let $q$ be a power of a prime and $\theta$ primitive in $GF(q^2)$; then

$$A(q, \theta) = \{a : 1 \leq a < q^2, \theta^a - \theta \in GF(q)\}$$

(1.1)

will give a $B_2$-sequence of size $q$. These Bose-Chowla $B_2$-sequences have the stronger property that the sums $a_i + a_j$, $1 \leq i \leq j \leq q$, are different modulo $q^2 - 1$. This has important consequences for the problem of Erdős, which Zhang noticed and used in [7].

By Lemma 3.3 in [7], if $\{a_i\}_1^r$ is a $B_2$-sequence (mod $m$), then $\{a_i + b\}_1^r$ will also be a $B_2$-sequence (mod $m$) for any integer $b$. Assume that $a_1 < a_2 < \cdots < a_r$ and define $a_{r+1} = a_1 + m$. Determine the largest interval $(a_i, a_{i+1})$ for $1 \leq i \leq r$. Let $b = m + 1 - a_{i+1}$. Then the largest number in the new sequence is, in general, smaller.

Another idea of Zhang was to generate a large number of $B_2$-sequences for each $q$ by varying the primitive element $\theta \in GF(q^2)$. There are $\varphi(q^2 - 1)$ primitive elements $\theta$, where $\varphi$ is Euler’s function. This number can be reduced to
There are integers \( \varphi(q^2 - 1)/4 \) due to symmetries of the \( B_2 \)-sequences. Then he determines one with largest possible interval giving a smallest possible upper bound by the previous idea. It is laborious to check each time that \( \theta \) is primitive. But it is only necessary to do this for one \( A(q, \theta) \). The other sequences can be found if we multiply the sequence by integers which are relatively prime to \( q^2 - 1 \) and reduce modulo \( q^2 - 1 \). This is contained in Theorem 2.2. In Theorem 2.1 I prove that \( A(q, \theta) \) can be determined \( q \) times faster than suggested by (1.1).

Zhang considered only the case when \( q = p \) is an odd prime. To check that \( \theta \) is primitive in \( GF(p^2) \) he used the following necessary and sufficient conditions: (i) \( \theta^{p+1} \) is primitive in \( GF(p) \); (ii) \( \theta, \theta^2, \ldots, \theta^p \notin GF(p) \) (Lemma 4.3 in [7]).

In Theorem 3.1 I give a new criterion for \( \theta \) to be primitive in \( GF(p^2) \). If \( \theta \) satisfies the quadratic equation \( \theta^2 = u\theta - v \) with \( u, v \in GF(p) \) my criterion poses conditions on \( u^2/v \) and \( v \).

2. Finding \( A(q, \theta) \) faster

In this section I will assume that \( q \) is a power of a prime. The following Lemma 2.2 generalizes Lemma 4.3 in [7].

**Lemma 2.1.** Let \( \theta \) be a root of an irreducible quadratic \( X^2 - uX + v \) with \( u, v \in GF(q) \). Then we have

\[
\theta^q + \theta = u, \quad \theta^{q+1} = v.
\]

*Proof.* There are two roots \( \theta \) and \( \theta^q \). The relations (2.1) follow since \( u \) is the sum and \( v \) is the product of the roots of the quadratic. \( \qed \)

**Lemma 2.2.** Let \( \theta \in GF(q^2) \) and write \( \theta^{q+1} = v \). Then \( \theta \) is a primitive element if and only if

(i) \( \theta^i \notin GF(q) \) for \( 1 \leq i \leq q \); and
(ii) \( \text{ord}(v) = q - 1 \).

*Proof.* Assume that \( \theta \) is primitive in \( GF(q^2) \). Then \( \text{ord}(\theta) = q^2 - 1 \). If \( \theta^i \in GF(q) \) for some \( i, 1 \leq i \leq q \), then \( \theta^i(q-1) = 1 \) gives a contradiction. Therefore (i) holds. If \( \text{ord}(v) = n < q - 1 \), then \( \theta^{(q+1)n} = 1 \) gives another contradiction since \((q + 1)n < q^2 - 1 \). Therefore (ii) holds.

Conversely, assume that (i) and (ii) are satisfied. Note that \( v \in GF(q) \) since \( v^{q-1} = \theta^{q-1} = 1 \). Let \( \text{ord}(\theta) = n = (q+1)k + r \), \( 0 \leq r \leq q \). Then \( \theta^n = 1 \) implies that \( \theta^r = v^{-k} \in GF(q) \) and \( r = 0 \) follows by (i). Then \( v^k = 1 \) and \( k = q - 1 \) follows by (ii). Hence \( n = q^2 - 1 \). \( \qed \)

Let \( \theta \) be primitive in \( GF(q^2) \). Define \( u_i \) and \( v_i \in GF(q) \) by

\[
(2.2) \quad \theta^i = u_i \theta - v_i.
\]

We have \( u_i \neq 0 \) for \( 1 \leq i \leq q \) by Lemma 2.2(i). Since \( v \) is primitive in \( GF(q) \) by (ii), there are integers \( t_i \) such that

\[
(2.3) \quad u_i = v^{t_i} = \theta^{(q+1)t_i}, \quad 1 \leq i \leq q.
\]

If we divide (2.2) by \( u_i \), then we find

\[
(2.4) \quad \theta^{i-(q+1)t_i} - \theta = -v_i u_i^{-1} \in GF(q)
\]

and since, by definition

\[
(2.5) \quad A(q, \theta) = \{ a : 1 \leq a < q^2, \theta^a - \theta \in GF(q) \},
\]
Proof. Let $\alpha$ be a primitive element in $GF(q^2)$ and define the integers $t_i$ for $1 \leq i \leq q$ by (2.3) and $A(q, \theta)$ by (2.5). Then we have

\begin{equation}
A(q, \theta) = \{i - (q + 1)t_i \mod q^2 - 1 : 1 \leq i \leq q\}.
\end{equation}

\begin{proof}
With regard to (2.6) it remains to prove that the elements are distinct modulo $q^2 - 1$. If $i - (q + 1)t_i \equiv j - (q + 1)t_j \mod q^2 - 1$, then $i \equiv j \mod (q + 1)$ and we have $i = j$ since $1 \leq i, j \leq q$.
\end{proof}

Example 2.1. Let $q = 7$ and $\theta^2 = \theta - 3$ (cf. Example 3.1 in [7]). We find $u_1 = u_2 = 1, u_3 = 5, u_4 = 2, u_5 = 1, u_6 = 2, u_7 = 3$ and, since $v = 3, t_1 = t_2 = 0, t_3 = 5, t_4 = 2, t_5 = 2, t_6 = 2, t_7 = 3$, which gives $A(7, \theta) = \{1, 2, 5, 11, 31, 36, 38\}$ after sorting.

If $c$ is relatively prime to $q^2 - 1$, then $M_c(x) = cx$ defines a one-one mapping of the integers modulo $q^2 - 1$. For any integer $t$ we define another one-one mapping $(mod q^2 - 1)$ by $T_t(x) = x - (q + 1)t$.

Theorem 2.2. Let $\theta$ and $\theta_1$ be primitive elements in $GF(q^2)$ and $\theta = \theta_1^{c} = u_0\theta_0 - v_c(u_c, v_c \in GF(q))$, $u_c = \theta_1^{c(q + 1)}t$. Then $A(q, \theta_1) = T_t M_c A(q, \theta)$.

\begin{proof}
Let $a \in A(q, \theta)$. Then we have $\theta^a - \theta \in GF(q)$ and $\theta_1^a - u_0\theta_0 \in GF(q)$. If we divide this by $u_c (\neq 0)$, we find that $ca -(q + 1)t \in A(q, \theta_1)$ and $T_t M_c A(q, \theta) = A(q, \theta_1)$ follows since both sets have $q$ elements.
\end{proof}

3. A CRITERION FOR PRIMITIVE QUADRATICS

I will prove a new criterion for a quadratic $X^2 - uX + v$ over $GF(p)$, $p$ an odd prime, to be primitive, i.e., with a root $\theta$, which is a primitive element in $GF(p^2)$. I am looking for a criterion which is suitable for computations and faster than the one in Lemma 2.2. There is a criterion by Bose, Chowla and Rao, Theorem 3A in [2], which depends on cyclotomic polynomials. I do not think it is what I am looking for, but I have use of the integral order of $\alpha \in GF(p^2)$. It is the least positive number $n$ for which $\alpha^n \in GF(p)$. I found this notion in [2].

I will need polynomials $Q_m(X)$ of degree $m \geq 0$ defined recursively by

\begin{equation}
Q_0(X) = 1, \quad Q_1(X) = X,
\end{equation}

\begin{equation}
Q_{m+1}(X) = XQ_m(X) - Q_{m-1}(X) \quad \text{when } m \geq 1.
\end{equation}

Lemma 3.1. Let $\alpha$ be a root of the irreducible quadratic $X^2 - uX + v$ over $GF(p)$ with $u, v \neq 0$. Write $u^2/v = w$ and let $n = 2(m + 1)$. Then $(\alpha^2/v)^n = 1$ if and only if $Q_m(w - 2) = 0$.

\begin{proof}
We have $(\alpha^2 + v)^2 = u^2\alpha^2$. Hence $\alpha^4 + v^2 = (u^2 - 2v)\alpha^2$ and

\begin{equation}
(\alpha^2/v) + (v/\alpha^2) = w - 2.
\end{equation}

Write $\alpha^2/v = \beta$ for brevity. Observe that $\beta \neq \pm 1$. Hence $\beta^2 - 1 \neq 0$.

Assume that $\beta^n - 1 = 0, n = 2(m + 1)$. If we divide $\beta^n - 1 = 0$ by $\beta^2 - 1 \neq 0$ we find $\beta^{2m} + \beta^{2m-2} + \cdots + 1 = 0$. Divide this by $\beta^m$. Now

\begin{equation}
\beta^m + \beta^{m-2} + \cdots + \beta^{-m} = 0.
\end{equation}

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The left-hand side of (3.4) can be written as a polynomial in $\beta + \beta^{-1}$. In fact, it is $Q_m(\beta + \beta^{-1})$. For obviously $Q_1(X) = X$, $Q_2(X) = X^2 - 2$ and (3.2) follows since $(\beta + \beta^{-1})Q_m(\beta + \beta^{-1}) = (Q_{m+1} + Q_{m-1})(\beta + \beta^{-1})$. Since $\beta + \beta^{-1} = w - 2$ by (3.3), we have $Q_m(w - 2) = 0$.

Conversely, assume that $Q_m(w - 2) = 0$. Then, working backward, we find that $\beta^n = 1$.

**Lemma 3.2.** If $\alpha^m \in GF(p)$ and $n$ is the integral order of $\alpha$, then $n|m$.

**Proof.** Write $m = kn + r$, $0 \leq r < n$. Then $\alpha^r = \alpha^m(\alpha^n)^{-k} \in GF(p)$ and $r = 0$ follows by the definition of $n$.

**Theorem 3.1.** Consider a quadratic $X^2 - uX + v$ with $u, v \in GF(p)$, $v \neq 0$ and $p$ an odd prime. Write $u^2/v = w$. The quadratic is primitive if and only if the following conditions are satisfied ((iv) or (iv'))

(i) $v$ is primitive (mod $p$),
(ii) $w \not\equiv 0$ is a quadratic nonresidue (mod $p$),
(iii) $w - 4$ is a quadratic residue (mod $p$),
(iv) $Q_m(w - 2) \not\equiv 0$ (mod $p$) when $m \leq \left(\frac{p + 1}{2}\right) - 1$.

(iv') For all odd primes $q$ dividing $p + 1$ $Q_{m(q)}(w - 2) \not\equiv 0$ (mod $p$), where $m(q) = \left(\frac{p + 1}{2q}\right) - 1$.

**Proof.** When we prove the necessity of one condition we may assume that the preceding ones are satisfied.

Condition (i) is necessary by Lemma 2.2(ii). Assume that (i) holds. Then $v$ is nonsquare in $GF(p)$. It follows that $w$ is nonsquare in $GF(p)$ ($u$ is impossible). This gives (ii). A primitive quadratic is irreducible. Then the discriminant $u^2 - 4v$ must be nonsquare in $GF(p)$. If we divide by nonsquare $v$ we will get a square by the rules. This is (iii).

Assume that the conditions (i)–(iii) are satisfied. The quadratic is then irreducible and we have $v = \theta^{p+1}$ by Lemma 2.1, where $\theta$ is a root.

Assume that $Q_m(w - 2) \equiv 0$ (mod $p$) for some $m \leq \left(\frac{p + 1}{2}\right) - 1$. By Lemma 3.1 we have $1 = (v/\theta^n)^m = \theta^{(p - 1)n} + 1$ with $n \leq \left(\frac{p + 1}{3}\right)$. This is impossible when $\theta$ is a primitive element in $GF(p^2)$. This gives (iv) and (iv').

Assume that (i)–(iii) and (iv') are satisfied. Let $n$ be the integral order of $\theta$. Since $\theta^{p+1} = v \in GF(p)$, $p + 1 = kn$ follows by Lemma 3.2.

Note that $v$ is nonsquare in $GF(p)$ and $v = \theta^{p+1} = (\theta^n)^k$, $\theta^n \in GF(p)$. It follows that $k$ is an odd integer. We claim that $k = 1$.

Assume that $k > 1$. Let $q$ be an odd prime divisor of $k$. Then $\bar{a} = (p+1)/q$ will be a multiple of $n = (p+1)/k$. Observe that $(v/\theta^n)^m = \theta^{n(p - 1)} + 1$ since $\theta^n \in GF(p)$. Then we have $(\theta^2/v)^b = 1$. By Lemma 3.1 it follows that $Q_{m(q)}(w - 2) \equiv 0$ (mod $p$), a contradiction to (iv'). Therefore $k = 1$ and $n = p + 1$.

We have proved that the integral order of $\theta$ is $p + 1$. I will prove that this implies that $\theta$ is primitive. If $N =$ order($\theta$), then $\theta^N = 1$ and we have $n \mid N$ by Lemma 3.2, i.e., $p + 1 \mid N$. Write $N = (p + 1)a$ and we find that $1 = \theta^N = v^a$. Since $v$ is primitive in $GF(p)$, it follows that $p - 1 \mid a$. Hence $N = p^2 - 1$, which was to be proved.

In calculations using a computer one could use (iv) and (3.1), (3.2). If the calculations are done by hand, then (iv') is better. In both cases start with a list L1 of all quadratic nonresidues (mod $p$). The length of this list is $(p - 1)/2$. Delete
from this list all integers $w$ for which $w - 4 \pmod{p}$ belongs to the list. Then we obtain a list $L_2$, which is about half as long (the length of $L_2$ is $(p + 1)/4$ when $-1$ is a quadratic nonresidue $(\mod{p})$ and $(p - 1)/4$ when $-1$ is a quadratic residue $(\mod{p})$). Then go to (iv) or (iv$'$) and check the numbers in $L_2$. Suppose we have found a number $w$, which satisfies all four conditions. Then find a primitive element $(\mod{p})$ from a table and determine $u$ such that $u^2 \equiv vw \pmod{p}$. Then we have the coefficients $u$ and $v$ of a primitive polynomial. If we apply (iv) or (iv$'$) to all numbers on the list $L_2$ we may determine all primitive quadratic polynomials.

It is easy to prove by induction over $m \geq 1$ that

$$Q_m(X) = \sum_{i=1}^{[m/2]} (-1)^i \binom{m - i}{i} X^{m-2i}.$$  

**Example 3.1.** Let $p = 29$. The odd primes dividing $p + 1$ are 3 and 5. We find that $m(3) = 4$ and $m(5) = 2$. We have $Q_3(X) = X^2 - 1$, $Q_4(X) = X^4 - 3X^2 + 1$. The list of quadratic nonresidues is $L_1 = \{2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27\}$. We delete all $w$ for which $w - 4$ belongs to the list and find $L_2 = \{3, 8, 10, 11, 17, 26, 27\}$. From $L_2$ we delete “3” since 3 is a root of $Q_2$ and we delete “8” and “26” because 6 and 24 are roots of $Q_4 \pmod{29}$. There remains: 10, 11, 17, 27, which satisfy conditions (ii), (iii) and (iv$'$). There are $\varphi(28) = 12$ primitive elements $v$ in $GF(29)$. Hence there are $4 \cdot 12 \cdot 2 = 96$ primitive polynomials (4 numbers $w$, 12 numbers $v$, and 2 numbers $u$ for each combination of $v$ and $w$). This gives 192 primitive elements in $GF(29^2)$ in agreement with $\varphi(29^2 - 1) = 192$. If we choose $w = 10$ and $v = 2$, we find $u = 7$ (or $-7$) and $X^2 - 7X + 2$ is a primitive polynomial $(\mod{29})$.

**Corollary.** If $p = 2^k - 1$ is a (Mersenne) prime or if $p = 2q - 1$ for an odd prime $q$, then the conditions (i)–(iii) are necessary and sufficient for the quadratic $X^2 - uX + v$ to be primitive.

**Proof.** In the first case (iv$'$) is vacuously satisfied. In the second case $m(q) = 0$ and $Q_0 = 1$. \hfill \Box

## 4. A very fast construction

There is a new construction of $B_2$-sequences by I. Z. Ruzsa in [6], Theorem 4.4, which gives $B_2$-sequences of the size $p - 1$ for each odd prime $p$. The computations are straightforward and therefore very fast. I have extended the construction by the introduction of a factor $f$, an integer in $1 \leq f < p - 1$, which is relatively prime to $p - 1$. Let $g$ be a primitive element $(\mod{p})$ and define

$$R(p, f) = \{pf{i} + (p - 1)g{i} \pmod{p(p - 1)}: 1 \leq i \leq p - 1\}.$$  

The integers of $R(p, f)$ are smaller than $p(p - 1)$.

**Theorem 4.1.** $R(p, f)$ is a $B_2$-sequence modulo $p(p - 1)$.

**Proof.** Let $pf(i + j) + (p - 1)(g{i} + g{j}) \equiv a \pmod{p(p - 1)}$ be the sum of two elements. Then we find

$$g{i} + g{j} \equiv -a \pmod{p}$$  

and $f(i + j) \equiv a \pmod{p - 1}$. Since $f$ is relatively prime to $p - 1$, there is an integer $h$ such that $fh \equiv 1 \pmod{p - 1}$. It follows that $i + j \equiv ah \pmod{p - 1}$ and we have
by Fermat’s little theorem

\begin{equation}
  g_i^j \equiv g^{ah} \pmod{p}.
\end{equation}

By (4.2) and (4.3) $g_i$ and $g_j$ are the roots of $X^2 + aX + g^{ah} = 0$ in $GF(p)$. Hence, $g_i$ and $g_j$ are unique and determine $\{i, j\}$ uniquely.

If we replace the primitive element $g$ by another primitive $g^b$ we will get $R(p, fd)$, where $bd \equiv 1 \pmod{p-1}$. If we multiply $R(p, f)$ by an integer $c$ relatively prime to $p(p-1)$ we get a translate of $R(p, fc)$. Thus we have essentially only $\varphi(p-1)$ $B_2$-sequences for each prime $p$. This “count” is much smaller than the count of the Bose-Chowla sequences $A(p, \theta)$. The estimates for $C$ using $R(p, f)$ are worse than those of $A(p, \theta)$.

References


Department of Mathematics, Royal Institute of Technology, S-100 44, Stockholm, Sweden

Current address: Turbingränd 18, S-17675 Järfälla, Sweden