SUBDIVISION SCHEMES WITH NONNEGATIVE MASKS

XINLONG ZHOU

Abstract. The conjecture concerning the characterization of a convergent univariate subdivision algorithm with nonnegative finite mask is confirmed.

1. Introduction

Let $\mathbb{Z}$ denote the integer lattice. A univariate subdivision algorithm with a finitely supported mask $a = \{a_j\}_{j \in \mathbb{Z}}$ is given as follows: beginning with an initial sequence of data $v^0 = \{v_0^k\}$, we set recursively new sequences of values $v^k$, by applying the rule

$$v_i^k = \sum_{j \in \mathbb{Z}} a_{i-2j}i_j^{k-1}.$$ 

This algorithm is said to converge if for each finite $v^0 = \{v_0^0\}$ there exists a continuous function $f_v$ such that $f_v \neq 0$ for at least one $v^0$ and

$$\lim_{k \to \infty} \sup_{i \in \mathbb{Z}} |f_v(i/2^k) - v_k^i| = 0.$$ (1.1)

Obviously, the subdivision algorithm with mask $a = \{a_j\}_{j \in \mathbb{Z}}$ converges if and only if the polygon $f_k$ defined by the control points $(i/2^k, v_k^i)$ converges uniformly to $f_v$. One can easily check

$$f_k(x) = \sum_i v_0^i \sum_j a_j^k h(2^k(x - i) - j),$$

where $h$ is the hat function and $a_j^k = \sum_{j} a_j^{k-1} a_{i-2j}$ with $a_j^1 = a_j$. Thus (1.1) for all such $v^0$ is equivalent to the uniform convergence of

$$\sum_j a_j^k h(2^k x - j).$$

On the other hand, define $S$ to be the operator given by

$$Sf(x) = \sum_j a_j f(2x - j).$$

One gets

$$S^k f(x) = \sum_j a_j^k f(2^k x - j), \quad k = 1, 2, \ldots.$$
The convergence of (1.1) is therefore equivalent to the uniform convergence of \( S^k h \), which leads to the following cascade algorithm: let \( g_0(x) = h(x) \); one defines recursively \( g_k(x) \) by

\[
g_k(x) = \sum_j a_j g_{k-1}(2x - j).
\]

The limit \( g = \lim_{k \to \infty} g_k = \lim_{k \to \infty} S^k h \) satisfies \( Sg = g \), i.e.,

\[
g(x) = \sum_j a_j g(2x - j).
\]

This so-called two-scale dilation equation and the above presented algorithms play an important role in wavelet analysis as well as in computer aided geometry design. A comprehensive discussion of this subject can be found in [2, 5, 10]. In order to characterize the convergence of the above algorithms, one uses the concept of joint spectral radius (see [11]). The joint spectral radius for two square matrices \( A_0 \) and \( A_1 \) is defined by

\[
\rho(A_0, A_1) = \lim_{n \to \infty} \sup_{k \leq n} \| A_{i_1} \cdots A_{i_k} \|^{\frac{1}{k}},
\]

where \( \| \cdot \| \) is a given matrix-norm and \( \epsilon_i \in \{0, 1\} \). Thus, write \( a(z) = \sum_j a_j z^j \) and \( a(z) = (1 + z)b(z) \) if \( a(-1) = 0 \). The subdivision algorithm with finite mask \( a = \{a_j\}_{j \in \mathbb{Z}} \) converges if and only if (see [2, 5, 10])

(i) \( a(1) = 2 \) and \( a(-1) = 0 \),
(ii) \( \rho(B_0, B_1) < 1 \) where \( B_0 = [b_{2j-i}]_{i,j}, B_1 = [b_{2j-i+1}]_{i,j} \) and \( \{b_1\} \) is the coefficients of \( b \).

Unfortunately, the determination of the joint spectral radius is generally NP-hard by a result of Tsitsiklis and Blondel (see [13]). Thus, it seems difficult to determine whether the considered spectral radius is less than one. Some partial results concerning the calculation of the joint spectral radius can be found in [1, 4, 7, 10] and the papers cited therein.

In this paper we focus on subdivision algorithms with nonnegative finite masks, a property possessed by many applications in geometric modelling (see, e.g., [3, 12]). A remarkable fact of this class is that the convergence does not depend on the actual values of the mask but rather on the support of the mask \( I = \{i : a_i > 0\} \) (see [11, 8]). Consequently the question was raised in [2] (see p. 55 of [2]) of identifying those \( I \) such that given any nonnegative mask supported on \( I \), the corresponding subdivision algorithm converges. By applying a suitable translation, we may always assume in the following discussion that a nonnegative mask \( a = \{a_j\} \) has the form \( a = \{a_0, \ldots, a_N\} \) with \( a_0, a_N > 0 \). We believe that the answer to this question is (see [9]):

**Conjecture.** The subdivision algorithm associated with the nonnegative mask \( a = \{a_0, \ldots, a_N\} \) converges if and only if the following both hold:

(i) \( a(1) = 2 \), \( a(-1) = 0 \) and \( 0 < a_0, a_N < 1 \),
(ii) the greatest common divisor of \( \{j : a_j > 0\} \) is 1.

This conjecture is still not verified. On the other hand, it has been shown that the conditions are necessary (see [2, 10, 14]). There are various partial results which support this conjecture. Denote \( S(a) = \{j : a_j > 0\} \). Thus, Micchelli and Prautzsch (see [10]) prove that if (ii) is replaced by \( S(a) = \{0, 1, \ldots, N\} \), convergence follows.
Gonsor (see [5]) shows that $S(a) = \{0,1,\ldots,N\}$ can be weakened by $\{0,1,N-1,N\} \subseteq S(a)$, while Melkman (see [9]), among others, proves that if instead of (ii) it holds that $S(a) \supseteq \{0,p,q,p+q\}$ for $\gcd(p,q) = 1$ or that $S(a)$ contains two successive integers, then convergence follows. Recently, Wang proves this conjecture for a class of masks. One of the main results in [15] is the following

**Theorem 1.1.** The subdivision algorithm with the nonnegative mask $a = \{a_j\}$ converges if instead of (ii) it holds that $\{r,p,q\} \subseteq S(a)$ such that $\gcd(p-r,q-r) = 1$ and $q-r$ is even.

Improving the technique introduced in [15], we can now confirm this conjecture. In next section we first collect some lemmas from [15] and prove the conjecture by using a lemma (see Lemma 2.4), which will be verified in Section 3. The proof of Lemma 2.4 is the kernel of this paper.

## 2. Proof of the Conjecture

Let us collect some results from [15]. For this goal we should denote the vector $x$ in $\mathbb{R}^N$ by $x = (x_0,\ldots,x_{N-1})^T$. For any $T \subseteq \mathbb{Z}_N$, where $\mathbb{Z}_N = \{0,1,\ldots,N-1\}$, we define $I_T$ to be the vector $(x_0,x_1,\ldots,x_{N-1})^T$ with $x_i = 1$ if $i \in T$ and $x_i = 0$ otherwise. For any nonnegative $N \times N$ row stochastic matrix $B$, i.e., the sum for each row is one, we define a map $F_B$ such that

$$F_B(T) = \{j \in \mathbb{Z}_N : (BI_T)_j = 1\}.$$

Let $A_0$ and $A_1$ be $N \times N$ matrices deduced by the mask $a$:

$$A_0 = [a_{2j-i}]_{0 \leq i,j \leq N-1} \quad \text{and} \quad A_1 = [a_{2j-i+1}]_{0 \leq i,j \leq N-1}.$$

Clearly, $A_0$ and $A_1$ are row stochastic matrices if $a(1) = 2$ and $a(-1) = 0$. We should write simply $F_0 = F_{A_0}$ and $F_1 = F_{A_1}$. For convenience we should also use the following standard notation for algebraic sums of sets: let $T$ be a set of integers; then for any integers $\alpha$ and $\beta$ the set $\alpha T + \beta$ is given by

$$\alpha T + \beta := \{\alpha x + \beta : x \in T\}.$$

We have (see [15])

**Lemma 2.1.** Let $B$ be a $N \times N$ nonnegative row stochastic matrix. Then $F_B(T_1)$ and $F_B(T_2)$ are disjoint if $T_1,T_2 \subseteq \mathbb{Z}_N$ are. Let $C$ be an $N \times N$ nonnegative row stochastic matrix. Then $F_B = F_B \circ F_C$. Furthermore, the subdivision algorithm with nonnegative mask $a$, which satisfies $a(1) = 2$ and $a(-1) = 0$, diverges if and only if there exist disjoint nonempty subsets $T$ and $T'$ of $\mathbb{Z}_N$ and a sequence $(d_1,d_2,\ldots,d_m) \in \{0,1\}^m$ for some $m \geq 1$ such that

$$T = F_{d_1} \circ \cdots \circ F_{d_1}(T) \quad \text{and} \quad T' = F_{d_1} \circ \cdots \circ F_{d_1}(T').$$

Denote for $S(a)$ the sets $S_0 = S(a) \cap (2\mathbb{Z})$ and $S_1 = S(a) \cap (2\mathbb{Z} + 1)$. The map $\Psi$ for $T \subseteq \mathbb{Z}$ is defined by

$$\Psi(T) = \left\{\bigcap_{q \in S_0} (2T - q)\right\} \cup \left\{\bigcap_{q \in S_1} (2T - q)\right\}.$$

The following relationship between $\Psi$ and $F_i$ is proved in [15].
**Lemma 2.2.** Let \( a \) be a nonnegative mask satisfying \( a(1) = 2 \) and \( a(-1) = 0 \). Then for any \( T \subset \mathbb{Z}_N \), we have
\[
F_0(T) = \Psi(T) \cap \mathbb{Z}_N, \quad F_1(T) = (\Psi(T) + 1) \cap \mathbb{Z}_N.
\]
Furthermore, for any \((d_1, \ldots, d_m) \in \{0, 1\}^m\) we have
\[
F_{d_1} \circ \cdots \circ F_{d_m}(T) = (\Psi^m(T) + k) \cap \mathbb{Z}_N,
\]
where \( k = \sum_{j=1}^m d_j 2^{j-1} \).

We may write \( S(a) = \{0, p_1, \ldots, p_k\} \) with \( p_k = N \). Generalizing Wang’s lemma (see [13]), we have

**Lemma 2.3.** Let \( T \) be a subset of \( \mathbb{Z} \) and let \( y \not\in T \). Let \( \epsilon_{i, j} \in \{0, 1\} \) such that
\[
\sum_{j=1}^k \epsilon_{i, j} \leq 1, \quad \forall \quad i = 1, 2, \ldots, m.
\]
Then it holds that
\[
2^m y - \sum_{j=1}^k \sum_{i=1}^m 2^{m-i} \epsilon_{i, j} p_j \not\in \Psi^m(T).
\]

**Proof.** For \( m = 1 \) the assertion is clear since \( 2y - xp_l \not\in \Psi(T) \) for all \( x = 0, 1 \) and \( l = 1, 2, \ldots, k \). On the other hand, \( \epsilon_{1, 1} + \cdots + \epsilon_{1, k} \leq 1 \) implies either \( \epsilon_{1, j} = 0 \) for \( j = 1, \ldots, k \) or else \( \epsilon_{1, j} = 0 \) for \( j \neq j' \) and \( \epsilon_{1, j'} = 1 \). Thus
\[
2y - \epsilon_{1, 1} p_1 - \epsilon_{1, 2} p_2 - \cdots - \epsilon_{1, k} p_k \not\in \Psi(T).
\]

The general case follows from induction on \( m \).

Let \( \varphi(n) \) be the Euler function of the number of elements in \( \mathbb{Z}_n \) that are co-prime with \( n \). It is known that if \( \gcd(k, n) = 1 \), then
\[
k^{\varphi(n)} \equiv 1 \pmod{n}.
\]
In particular, for any odd integer \( n \) one has
\[
2^{\varphi(n)} \equiv 1 \pmod{n}.
\]

Now we are in the position to prove the conjecture.

**Proof of Conjecture.** The necessity of the conditions is proved in [9]. To show the sufficiency, we denote \( S(a) = \{0, p_1, \ldots, p_k\} \) with \( p_k = N \) and \( |S(a)| \) for the number of \( S(a) \). The first assumption of the conjecture implies that \( |S(a)| \geq 3 \) and there exists an odd \( p \) in \( S(a) \) such that \( p = p_{j_0} < p_k \) no matter if \( p_k \) is odd or even. Hence, for \( |S(a)| = 3 \) one has \( S(a) = \{0, p, N\} \) with even \( N \). Wang’s result for \( |S(a)| = 3 \) (see [15]) may be read as: the subdivision algorithm converges if \( \gcd(p, N) = 1 \). We assume in the following that \( |S(a)| \geq 3 \). Let us observe that if the subdivision algorithms with the mask \( a = \{a_j\} \) diverges, then by Lemma 2.1 there are a sequence \((d_1, \ldots, d_m')\) and disjoint nonempty sets \( T, T' \subset \mathbb{Z}_N \) so that
\[
F_{d_1} \circ \cdots \circ F_{d_m'}(T) = T \quad \text{and} \quad F_{d_1} \circ \cdots \circ F_{d_m'}(T') = T'.
\]
It follows from Lemma 2.2 (see (2.3)) that
\[
T = (\Psi^m(T) + k') \cap \mathbb{Z}_N \quad \text{and} \quad T' = (\Psi^m(T') + k') \cap \mathbb{Z}_N,
\]
where \( k' = \sum_{l=1}^{m'} d_l 2^{l-1} \). Write \( F = F_{d_1} \circ \cdots \circ F_{d_m} \). Then \( F^\eta(T) = T \) and \( F^\eta(T') = T' \) for any \( \eta \geq 1 \). Therefore, with
\[
k'_\eta = \left( \sum_{l=1}^{m'} d_l 2^{l-1} \right) + \left( \sum_{l=1}^{m'} d_l 2^{l-1} \right) 2^m + \cdots + \left( \sum_{l=1}^{m'} d_l 2^{l-1} \right) 2^{(\eta-1)m'}
\]
\[
= k' \sum_{i=0}^{\eta-1} 2^{im'}
\]
we get for any \( \eta \geq 1 \)
\[
T = (\Psi^{m'\eta}(T) + k_\eta) \cap \mathbb{Z}_N \quad \text{and} \quad T' = (\Psi^{m'\eta}(T') + k_\eta) \cap \mathbb{Z}_N.
\]
We should choose \( \eta \) in connection with \( S(a) \). For our goal we define \( \eta \) to be
\[
(2.7) \quad \eta = t \prod_{j=1}^{p_k} \{ j \varphi(j) \}
\]
with some positive integer \( t \), which will be given later. Denote \( m = m'\eta \). We have \( 2^m \equiv 1 \pmod{x} \) for odd number \( x \) from \( \{1, \ldots, p_k\} \). Indeed, \( \eta \) has a factor \( x\varphi(x) \), so for some integer \( n' \) one has \( \eta = n'x\varphi(x) \). Since \( x \) is odd, we obtain by Euler’s formula (2.4)
\[
(2.8) \quad 2^m = 2^{m'n'x\varphi(x)} \equiv 1 \pmod{x}.
\]
Similarly, we have
\[
(2.9) \quad k_\eta \equiv 0 \pmod{x}.
\]
To see this, one gets by the expression of \( k_\eta \)
\[
k_\eta = k' \sum_{l=0}^{n'x-1} \varphi(x)(l+1)-1 \sum_{j=\varphi(x)l} 2^{jm'}
\]
\[
= k' \left( \sum_{l=0}^{n'x-1} \varphi(x)-1 \right) \sum_{j=0}^{2^{jm'} \varphi(x)lm'}
\]
\[
= k' \left( \sum_{l=0}^{n'x-1} \varphi(x)-1 \right) \sum_{j=0}^{2^{jm'} \varphi(x)lm'}
\]
\[
\equiv k'n'x \sum_{j=0}^{\varphi(x)-1} 2^{jm'} \quad (\text{mod} \ x)
\]
\[
\equiv 0 \quad (\text{mod} \ x),
\]
which yields (2.9). Moreover,
\[
k_\eta = 0 \iff d_1 = \cdots = d_{m'} = 0
\]
and
\[
k_\eta = 2^m - 1 \iff d_1 = \cdots = d_{m'} = 1.
\]
For all other \( d_j \) we can thus choose \( t \) large enough such that for some \( 0 < \delta < 1 \)
\[
(2.10) \quad p_k < k_\eta = k' \frac{2^{m'} - 1}{2^{m'} - 1} \leq (1 - \delta) 2^m
\]
Additionally, in view of (2.5) we may without loss of the generality assume that $k_\eta$ is even if $k_\eta \neq 2^m - 1$. In the following discussion we should always denote $m$ and $k_\eta$ to be any nonnegative integers, which satisfy the above properties, i.e., $0 \leq k_\eta \leq 2^m$; if $k_\eta \neq 0, 2^m - 1$, then $k_\eta$ is even, $m$ and $k_\eta$ satisfy (2.8)–(2.11). We know that the divergence of the subdivision algorithm implies that there are two disjoint nonempty sets $T, T' \subset \mathbb{Z}_N$ for (2.5). We may therefore assume $x \notin T$ and $x \in \mathbb{Z}_N$. So from Lemma 2.3 it holds that

$$2^m x - \sum_{j=1}^k \sum_{i=0}^{m-1} 2^i \epsilon_{i,j} p_j \notin \Psi^m(T)$$

for all $\epsilon_{i,j} \in \{0, 1\}$ such that $\sum_{j=1}^k \epsilon_{i,j} \leq 1$. By (2.6) we obtain

$$2^m x + k_\eta - \sum_{j=1}^k \sum_{i=0}^{m-1} 2^i \epsilon_{i,j} p_j \notin T$$

(2.12) for all those $\epsilon_{i,j}$. Denote $B_0 = \{x\}$ with $x \in \mathbb{Z}_N$ and for $l = 0, 1, \ldots,$

$$B_{l+1} = \{2^m y + k_\eta - \sum_{j=1}^k \sum_{i=0}^{m-1} 2^i \epsilon_{i,j} p_j \in \mathbb{Z}_N \mid y \in B_l, \epsilon_{i,j} \in \{0, 1\}, \sum_{j=1}^k \epsilon_{i,j} \leq 1\}.$$

Thus, (2.12) tells us that $x \notin T$ implies $B_l \cap T = \emptyset$ for all $l \geq 0$. In the next section we will prove the following

**Lemma 2.4.** Let the mask $a = \{a_j\}$ satisfy the conditions of the conjecture and $S(a) = \{0, p_1, \ldots, p_k\}$. Then there is an $0 \leq x < p_k$ such that with $B_0 = \{x\}$ one has

$$\bigcup_{l \geq 0} B_l = \mathbb{Z}_{p_k}.$$

This lemma, together with the above consideration, implies that the set $T$ or $T'$ must be empty. This contradiction proves the conjecture. □

The proof of Lemma 2.4 is much more involved and, in fact, is the kernel of this paper. We prove this lemma in the next section.

### 3. Proof of Lemma 2.4

The notation such as $B_j$, $k_\eta$ and $m$ have the same mean and properties as in Sections 1 and 2. Let us begin with the observation of the first condition of the conjecture. We need the following

**Definition.** A set of integers $I = \{0, q_1, \ldots, q_k\}$ with $0 < q_j < q_{j+1}$ has property P if either $q_k$ is even and $I$ contains at least one odd integer or else $I$ contains at least two odd and two even integers (including 0).

Obviously, if $a = \{a_j\}$ satisfies the first condition of the conjecture, the set $S(a)$ has property P. Conversely, if a set $\{0, q_1, \ldots, q_k\}$ has property P, then one can construct a mask $a = \{a_j\}$ satisfying the first condition of the conjecture and
Lemma 2.4. If $S(a) = \{0, p_1, \ldots, p_k\}$ has property P and $\gcd(p_1, \ldots, p_k) = 1$, then there is an $x \in \mathbb{Z}_{p_k}$ such that with $B_0 = \{x\}$

\[
(3.1) \quad \bigcup_{l \geq 0} B_l = \mathbb{Z}_{p_k}.
\]

To prove Lemma 2.4 or Lemma 2.4', we remember that $\{\epsilon_{i,j}\} \in \{0,1\}$ for $i = 0, 1, \ldots, m-1$, $j = 1, \ldots, k$ and

\[
\sum_{j=1}^{k} \epsilon_{i,j} \leq 1, \quad i = 0, 1, \ldots, m-1.
\]

Let $\delta_{i,j} = \epsilon_{i,j}$ for $i = 0, 1, \ldots, m-1$, $j = 1, \ldots, k-1$ and

\[
\delta_{i,k} = 1 - \sum_{j=1}^{k-1} \epsilon_{i,j}.
\]

Hence, $\{\delta_{i,j}\}$ satisfies our conditions. We obtain

\[
(3.2) \quad 2^m x + k_\eta - \sum_{j=1}^{k} \sum_{i=0}^{m-1} \delta_{i,j} 2^i p_j = (p_k - 1) \quad \text{for} \quad \sum_{j=1}^{k} \epsilon_{i,j} 2^i p_j = (p_k - 1)
\]

We notice that $2^m - 1 - k_\eta$ is between 0 and $2^m - 1$. Formulas (2.8) and (2.9) imply that (2.9) also holds for $k_\eta' = 2^m - 1 - k_\eta$ instead of $k_\eta$. Let $\hat{B}_j = p_k - 1 - B_j$. Then $\hat{B}_j$ is defined by $\{0, p_k - p_k - 1, \ldots, p_k - p_1, p_k\}$ and $k_\eta'$. Since $\gcd(p_1, \ldots, p_k) = \gcd(p_k - p_k - 1, \ldots, p_k - p_1, p_k)$, the symmetric relation (3.2) tells us that

\[
v \in \bigcup_{l \geq 0} B_l \iff p_k - 1 - v \in \bigcup_{l \geq 0} \hat{B}_l.
\]

Moreover, if $\{0, p_1, \ldots, p_k\}$ has property P, then $\{0, p_k - p_k - 1, \ldots, p_k - p_1, p_k\}$ does also. Thus, it is enough to show Lemma 2.4' either for $\{0, p_1, \ldots, p_k\}$ or for $\{0, p_k - p_k - 1, \ldots, p_k - p_1, p_k\}$. For simplicity we define

\[
\mathcal{B}(x) = \bigcup_{l \geq 0} B_l
\]

with $B_0 = \{x\} \subset \mathbb{Z}_{p_k}$.

The following assertions will be used frequently and are based on some special choices of $\{\epsilon_{i,j}\}$. We formulate them as four lemmas.

Lemma 3.1. Let $y \in \mathcal{B}(x)$ and $0 \leq y \leq p_1$, for some odd $p_1 \in S(a)$. If $0 < (2^m - 1)y + k_\eta \leq (2^m - 1)p_1$, then $y + j p_1 \in \mathcal{B}(x)$ for $j$ such that $y + j p_1 \in \mathbb{Z}_{p_k}$.

Proof. We choose $\epsilon_{i,j} = 0$ for $j \neq l_1$. By the definition of $\epsilon_{i,j}$ the number $l = \sum_{i=0}^{m-1} \epsilon_{i,l_1} 2^i$ can be any number between 0 and $2^m - 1$. On the other hand, in view
of (2.8) and (2.9) we have \((2^m - 1)y + k_\eta = \alpha p_{i_1}\). Hence,

\[
y + (2^m - 1)y + k_\eta - \sum_{i=0}^{m-1} \epsilon_{i,j} p_j 2^i = y + (\alpha - l)p_{i_1}.
\]

The choice of \(\eta\) (see (2.7)) implies \(k_\eta > p_k\) and \(2^m - k_\eta > 2p_k\) if \(k_\eta \neq 0\) and \(2^m - 1\), while for \(k_\eta = 0\), the inequality \((2^m - 1)y > 0\) yields \(y \geq 1\). Moreover, if \(k_\eta = 2^m - 1\), then the condition implies \(y < p_{i_1}\). Hence \(\alpha - l\) can be any number between \(-p_k\) and \(p_k\). In particular, for \(l\) such that \(y + (\alpha - l)p_{i_1} \in \mathbb{Z}_{p_k}\) we have \(y + (\alpha - l)p_{i_1} \in \mathcal{B}(x)\). \(\square\)

**Lemma 3.2.** Let \(y \in \mathcal{B}(x)\) and \(p_{i_1} \in S(a)\) be even. Assume \(p_{i_1}/2 \leq y\) and \((2^m - 1)(y - p_{i_1}/2) + k_\eta \leq (2^{m-1} - 1)p_{i_1}\) for some odd \(p_{i_2} \in S(a)\). Then \(y - p_{i_1}/2 \in \mathcal{B}(x)\).

**Proof.** We choose \(\epsilon_{m-1,i_1} = 1\) and \(\epsilon_{i,j} = 0\) if \(i \neq m-1\). For other \(j \neq l_2\) let \(\epsilon_{i,j} = 0\). To meet the condition on \(\epsilon_{i,j}\), we have to choose \(\epsilon_{m-1,i_2} = 0\). Now \(\sum_{i=0}^{m-2} \epsilon_{i,j} 2^i\) can be any number between \(0\) and \(2^{m-1} - 1\). From (2.8), (2.9) and our restriction on \(y\) we conclude \((2^m - 1)(y - p_{i_1}/2) + k_\eta = \alpha p_{i_2}\) for some \(0 \leq \alpha \leq 2^{m-1} - 1\). Hence, we can choose \(\epsilon_{i,j}\) for \(i = 0, 1, \ldots, m - 2\) to obtain \(\sum_{i=0}^{m-2} \epsilon_{i,j} 2^i = \alpha\). With this choice of \(\epsilon_{i,j}\) we get

\[
2^m y + k_\eta - \sum_{j=1}^{m-1} \sum_{i=0}^{m-1} \epsilon_{i,j} p_j 2^i = y - p_{i_1}/2.
\]

Thus, \(y - p_{i_1}/2 \in \mathcal{B}(x)\). \(\square\)

**Lemma 3.3.** Let \(y \in \mathcal{B}(x)\). If there is some odd \(p_{i_1} \in S(a)\) such that \((2^m - 1)y + k_\eta < (2^m - 1)p_{i_1}\), then for any \(p_j \in S(a)\) one has

(i) \(y + (2l + 1)p_{i_1} - p_j \in \mathcal{B}(x)\) whenever \(y + (2l + 1)p_{i_1} - p_j \in \mathbb{Z}_{p_k}\) and \((2^m - 1)y + k_\eta\) is odd;

(ii) \(y + 2l p_{i_1} - p_j \in \mathcal{B}(x)\) whenever \(y + 2l p_{i_1} - p_j \in \mathbb{Z}_{p_k}\) and \((2^m - 1)y + k_\eta\) is even.

**Proof.** Clearly \((2^m - 1)y + k_\eta = \alpha p_{i_1}\) for some \(0 \leq \alpha < 2^m - 1\). If \(\alpha\) is odd, we choose \(\epsilon_{i,1}\) such that \(\alpha - \sum_{i=0}^{m-1} \epsilon_{i,1} 2^i = 2l + 1\). Obviously, \(\epsilon_{0,1}\) must be zero. Hence, we can choose \(\epsilon_{0,j} = 1\) or 0 to obtain

\[
2^m y + k_\eta - \sum_{j=1}^{k-1} \sum_{i=0}^{m-1} \epsilon_{i,j} p_j 2^i = y + (2l + 1)p_{i_1} - \epsilon_{0,j} p_j.
\]

Since \(y \in \mathcal{B}(x)\), the set \(\mathcal{B}(x)\) contains \(y + (2l + 1)p_{i_1} - \epsilon_{0,j} p_j\) whenever \(y + (2l + 1)p_{i_1} - \epsilon_{0,j} p_j \in \mathbb{Z}_{p_k}\). Similarly, we have the second assertion. \(\square\)

**Lemma 3.4.** Let \(y \in \mathcal{B}(x)\) and \(p_{i_2} - p_{i_1} > 0\) be odd for some \(p_{i_1}, p_{i_2} \in S(a)\). Assume \(0 < (2^m - 1)(y - p_{i_1}) + k_\eta < (2^m - 1)(p_{i_2} - p_{i_1})\). Then, \(y + j(p_{i_2} - p_{i_1}) \in \mathcal{B}(x)\) for \(j \in \mathbb{Z}\) such that \(y + j(p_{i_2} - p_{i_1}) \in \mathbb{Z}_{p_k}\).

**Proof.** Let \(\epsilon_{i,1} = 1 - \epsilon_{i,2}\) and \(\epsilon_{i,j} = 0\) for \(j \neq l_1, l_2\). We obtain

\[
2^m y + k_\eta - \sum_{j=1}^{k-1} \sum_{i=0}^{m-1} \epsilon_{i,j} p_j 2^i = y + (2^m - 1)(y - p_{i_1}) + k_\eta - \sum_{i=0}^{m-1} \epsilon_{i,l_2} (p_{i_2} - p_{i_1}) 2^i
\]

\[
= y + (2^m - 1)(y - p_{i_1}) + k_\eta - l(p_{i_2} - p_{i_1}),
\]
where $l$ can be any integer between 0 and $2^m - 1$. On the other hand, our condition, (2.8) and (2.9) imply

$$p_k \leq (2^m - 1)(y - p_k) + k_\eta = \alpha(p_{l_2} - p_k) < (2^m - 1)(p_{l_2} - p_{l_1}).$$

Hence, for any nonnegative integer $j$ such that $y + j(p_{l_2} - p_k) \in \mathbb{Z}_{p_k}$ we can choose $l \in [0, 2^m - 1]$ so that $\alpha - l = j$, i.e., $y + j(p_{l_2} - p_k) \in \mathcal{B}(x)$. On the other hand, the condition implies that $y + 1 \leq p_{l_1}$ if $k_\eta \neq 2^m - 1$ and $y + 2 \leq p_{l_2}$ if $k_\eta = 2^m - 1$. Thus, for any negative integer $j$ such that $y + j(p_{l_2} - p_k) \in \mathbb{Z}_{p_k}$ we can choose $l \in [0, 2^m - 1]$ so that $\alpha - l = j$, i.e., $y + j(p_{l_2} - p_k) \in \mathcal{B}(x)$. 

We are now ready to verify Lemma 2.4'. We prove this lemma using induction on $|S(a)|$. The assertion (3.1) for $|S(a)| = 3$ is essentially given by Wang in [15] (see the proof of Theorem 1.1 in [15]).

**Proof of Lemma 2.4'**. The idea behind the proof is that first we prove the assertion for a small $p$ instead of $p_k$, i.e.,

$$\{0, \ldots, p - 1\} \subseteq \mathcal{B}(x).$$

If $p$ is odd and belongs to $S(a)$, we can then extend this to all of $\{0, 1, \ldots, p - 1\}$ by using Lemma 3.1. In order to obtain the result for all of $\{0, 1, \ldots, p - 1\}$, we choose carefully an $x$ in this set and apply Lemmas 3.1–3.4 to get another number, which is greater than $p$. Using Lemma 3.2 or Lemma 3.4, we may reduce the number so that the new number is again contained in $\{0, \ldots, p - 1\}$ but is different from $x$. Recursively, we obtain several numbers. One of our tasks is to show that those numbers are all different. A careful choice of $x$ is necessary. Otherwise the following calculation leads to $\mathcal{B}(x) = \{0\}$. In fact, if $k_\eta = 0$, then for $x = 0$ and $B_0 = \{0\}$ one gets $B_1 = \{0\}$ for all $l = 1, 2, \ldots$. Thus, in our choice of $x$ it may be understood that we avoid zero if $k_\eta = 0$ or $p_k - 1$ if $k_\eta = 2^m - 1$ during the calculation of new numbers. In other words, we should choose such an $x$ that zero or $p_k - 1$ occurs at the last step of our calculation.

Next let us observe the set $S(a)$ with $|S(a)| \geq 5$. It is easy to check that for some nonzero $p \in S(a)$ the set $S(a) \setminus \{p\}$ also has property P. However, for sets with $|S(a)| = 4$ we may not have this $p$. The only set that does not have this $p$ is $\{0, p_1, p_2, p_3\}$ with even $p_1$ and odd $p_2, p_3$. We already know that $|S(a)| \geq 3$. Since the assertion for $|S(a)| = 3$ is essentially given in [15], we should omit the proof for this case. Our approach, therefore, has two steps; namely, the proof for the special case of $|S(a)| = 4$ and for $|S(a)| \geq 4$. Let us begin with the special case.

**Step 1.** $S(a) = \{0, p_1, p_2, p_3\}$ with even $p_1$ and odd $p_2, p_3$. We divide the proof into three cases according to the different position of $p_1, p_2$ and $p_3$.

**Case 1.** Let us prove (3.1) for $2p_2 < p_3$. Assume $k_\eta \neq 2^m - 1$. Denote $\gcd(p_1, p_2) = d$ and $p = p_1/2$. The $0 \leq x < p$ is given as follows:

$$\begin{cases} 
  x + p_3 \equiv 0 \pmod{d}, & d \neq 1, \\
  x - p_2 \equiv 0 \pmod{p}, & d = 1.
\end{cases}$$

With this $x$ we have

$$\{x + dv : 0 \leq x + dv \leq p\} \subseteq \mathcal{B}(x).$$

To see this, we apply Lemma 3.1 to get $x + p_2 \in \mathcal{B}(x)$. Using Lemma 3.2 for $p_1 = p_3$ and $p_2 = p_3$, we conclude $x + p_2 - p \in \mathcal{B}(x)$. Repeatedly we get $x + p_2 - \alpha_1 p \in \mathcal{B}(x)$ whenever $0 \leq x + p_2 - \alpha_1 p < p$. We notice that $x + p_2 - \alpha_1 p$ satisfies the above restriction. Thus, recursively, i.e., replacing $x$ by $x + p_2 - \alpha_1 p$, we conclude
Moreover, it follows from \( \gcd(p_2, p) = d \) that \( x + sp_2 - \alpha_s p \neq x + s'p_2 - \alpha_{s'} p \) if \( 0 \leq s < s' \leq p/d - 1 \). Therefore,

\[
\{ x + sp_2 - \alpha_s p : \ s = 0, 1, \ldots, p/d - 1 \} = \{ x + dv : 0 \leq x + dv < p \} \subseteq \mathcal{B}(x).
\]

Examining the way we calculate the number \( x + sp_2 - \alpha_s p \) for \( s = p - 1 \) and \( d = 1 \), we obtain additionally \( p \in \mathcal{B}(x) \), proving (3.3).

Having (3.3), we will replace \( p \) in (3.3) by \( p_2 \). We use the same procedure as above. Let \( x + dv \) be any nonzero element from \( \{ x + dv : 0 \leq x + dv \leq p \} \). Lemma 3.1 leads to \( x + dv + p_2 \in \mathcal{B}(x) \) while Lemma 3.2 implies \( x + dv + p_2 - lp \in \mathcal{B}(x) \) for \( l \geq 0 \) such that \( x + dv + p_2 - lp \in \mathbb{Z}_{p_2} \). Clearly, there are \( l' \) and \( \nu \) such that \( p_2/d = l'p/d + \nu \) or \( p_2 = l'p + \nu d \). Hence, for \( p < x + dv' \leq p_2 \) we get \( x + dv' = x + d(v' - \nu) + p_2 - l'p \). Now, if \( 0 < x + d(v' - \nu) \leq p \), then \( x + dv' \in \mathcal{B}(x) \). If \( x + d(v' - \nu) \leq 0 \), there exists \( l'' \) such that \( 0 < x + d(v' - \nu) + l''p \leq p \). Hence, \( x + dv' = x + d(v' - \nu + l''p) + l''p \). We still have \( x + dv' \in \mathcal{B}(x) \).

Finally, if \( p < x + d(v' - \nu) \), one has \( l''' \) such that \( 0 < x + d(v' - \nu - l'''p) \leq p \). Thus, \( x + dv' = x + d(v' - \nu - l'''p) + p_2 - (l' + l'''p) \). We conclude in particular that

\[
\{ x + dv : 0 \leq x + dv \leq p_2 \} \subseteq \mathcal{B}(x).
\]

In order to replace \( p_2 \) in (3.4) by \( p_3 - 1 \), we again use Lemma 3.1. Examining the conditions of Lemma 3.1, we know that if \( d \neq 1 \), then for each \( 0 \leq x + dv \leq p_2 \) one gets \( x + dv + lp_2 \in \mathcal{B}(x) \) whenever \( x + dv + lp_2 \in \mathbb{Z}_{p_3} \). Hence,

\[
\{ x + dv : 0 \leq x + dv < p_3 \} \subseteq \mathcal{B}(x).
\]

However, if \( d = 1 \), the above calculation may not be true. We should modify this as follows: for \( k_\eta \neq 0 \) let \( 0 \leq x + v < p_2 \). Again we have (3.5). If \( k_\eta = 0 \), let \( 0 < x + v \leq p_2 \). We obtain \( x + v + lp_2 \in \mathcal{B}(x) \). Hence, (3.5) is still valid. Clearly, (3.5) implies (3.1) if \( d = 1 \).

To show (3.1) for \( d \neq 1 \), we observe elements from (3.5) satisfying \( p_3 - p_1 \leq x + dv < p_3 - p \). Obviously we can apply Lemma 3.4 for \( y = x + dv, p_1 = p_1 \) and \( p_2 = p_3 \) to obtain \( x + dv - (p_3 - p_1) \in \mathcal{B}(x) \). Noticing \( 2p_2 < p_3 \) and \( 0 \leq x + dv - (p_3 - p_1) < p_3 \), we get from Lemma 3.1 that \( x + dv - (p_3 - p_1) + 2p_2 \in \mathcal{B}(x) \) if \( k_\eta = 0 \) or \( x - p_3 \neq 0 \mod d \). Under this restriction, Lemma 3.2 tells us that \( x + dv - (p_3 - p_1) + lp_2 \in \mathcal{B}(x) \) whenever \( x + dv - (p_3 - p_1) + p_2 - pl \in \mathbb{Z}_{p_3} \). Recursively, we conclude that if \( k_\eta = 0 \) or \( x - p_3 \neq 0 \mod d \), then \( x + dv - (p_3 - p_1) + np_2 - lp \in \mathcal{B}(x) \) whenever \( x + dv - (p_3 - p_1) + np_2 - lp \in \mathbb{Z}_{p_3} \). Let \( 0 \leq x + dv - (p_3 - p_1) < p_3 \). Then due to \( \gcd(p_2, p) = d \), there are \( j \geq 0, l \geq 0 \) and \( 0 \leq x + dv - (p_3 - p_1) < p_3 \) such that

\[
x + dv - (p_3 - p_1) = x + dv - (p_3 - p_1) + jp_2 - lp.
\]

Therefore, if \( k_\eta = 0 \) or \( x - p_3 \neq 0 \mod d \),

\[
\{ x + dv - (p_3 - p_1) : 0 \leq x + dv - (p_3 - p_1) < p_3 \} \subseteq \mathcal{B}(x).
\]
This observation leads to the following assertion: Let $A_j = \{ x + dv - j(p_3 - p_1) : 0 \leq x + dv - j(p_3 - p_1) < p_3 \}$. Then under the assumption $k_\eta \neq 0$ or $x - (i + 1)p_3 \neq 0$ (mod $d$) we have that $A_i \subseteq B(x)$ implies $A_{i+1} \subseteq B(x)$. We already know $A_0 \cup A_1 \subseteq B(x)$. Thus, we use the above procedure with $p_3 - p_1 \leq x + dv - i(p_3 - p_1) < p_3 - p$ instead of $p_3 - p_1 \leq x + dv - (i - 1)(p_3 - p_1) < p_3 - p$ to obtain $A_{i+1} \subseteq B(x)$. We remember $x + p_3 \equiv 0$ (mod $d$). Hence, $x - jp_3 \neq 0$ (mod $d$) for $j = 0, 1, \ldots, d - 2$. We conclude

$$\sum_{j=0}^{d-2} A_j \subseteq B(x).$$

Moreover, in the case of $k_\eta \neq 0$

$$\sum_{j=0}^{d-1} A_j \subseteq B(x).$$

To have (3.1) for $k_\eta \neq 0$, we notice $\gcd(d, p_3) = 1$. Hence, for any $v'$ such that $0 \leq x + v' < p_3$ there is $0 \leq j \leq d - 1$ with $v' + j(p_3 - p_1) \equiv 0$ (mod $d$), which gives $v' = dv - j(p_3 - p_1)$ for some $v$. We conclude that $x + v' = x + dv - j(p_3 - p_1) \in A_j$ or

$$Z_{p_3} = \{ v : 0 \leq v < p_3 \} \subseteq B(x).$$

It remains to show (3.1) for $k_\eta = 0$. We already have (3.6). But what is the corresponding $A_{d-1}$ for this case? We know that the first step in our procedure is to find an element in $A_{d-2}$ which satisfies

$$p_3 - p_1 \leq x + dv - (d - 2)(p_3 - p_1) < p_3 - p.$$  

If $x + dv - (d - 2)(p_3 - p_1) \neq p_3 - p_1$, we can use our procedure to obtain $x + dv - (d - 2)(p_3 - p_1) + jp_2 - lp \in B(x)$. If however $x + dv - (d - 2)(p_3 - p_1) = p_3 - p_1$, we get formally from the above procedure a set

$$A' = \{ jp_2 - lp : 0 \leq lp_2 - lp < p_3 \}.$$  

But, because $k_\eta = 0$, we cannot use this approach for $x + dv - (d - 1)(p_3 - p_1)$ (≡ 0). Thus, instead of $A_{d-1}$ we have only $A_{d-1} \setminus A' \subseteq B(x)$. Hence, combining this with (3.6), we obtain $(\bigcup_{i=0}^{d-1} A_i) \setminus A' \subseteq B(x)$, which implies

$$\{ v : 0 \leq v < p_3 \} \setminus A' \subseteq B(x).$$

To show $A' \subseteq B(x)$, we have to modify (3.7). We remember that $\gcd(d, p) = d$ and $x - (d - 1)p_3 \equiv 0$ (mod $d$). Hence, there is a $v$ such that

$$p_3 - p_1 < x + dv' - (d - 2)(p_3 - p_1) = p_3 - p,$$

which implies that $x + dv' - (d - 1)(p_3 - p_1)$ (≡ $p$) is contained in $B(x)$ due to Lemma 3.4. Now we can apply our procedure for $p$ to obtain $jp_2 - lp \in B(x)$ or $A' \subseteq B(x)$. Consequently,

$$Z_{p_3} = \{ v : 0 \leq v < p_3 \} \subseteq B(x).$$

For $k_\eta = 2^m - 1$ we replace $x + p_3 \equiv 0$ (mod $d$) by $x + 1 + p_3 \equiv 0$ (mod $d$) and $p_i(x - p_2)$ by $p_i(x + 1 - p_2)$, respectively.

Case 2. Now if $p_3 < 2p_1$, we use the symmetric relation to obtain (3.1), since $(0, p_3 - p_2, p_3 - p_1, p_3)$ has property P and $2(p_3 - p_1) < p_3$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Case 3. Since $p_3$ is odd, it remains to show (3.1) for $2p_1 < p_3 < 2p_2$. Without loss of generality we may suppose $p_3 \geq p_2 + p_1$. Now, $p_1$ is even, so $p_1 = 2p$ for some $p$.

Let $p$ be odd. Denote $\gcd(p_1, p_3) = d$. We have $\gcd(p, p_3) = d$. We verify for some $0 \leq x < p$ that

$$v : 0 \leq v < p_1 \setminus \{p\} \subseteq \mathcal{B}(x).$$

To this end we choose $0 \leq x \leq p$ in the following way: if $0 \leq k_\eta < 2^m - 1$, then $x \neq 0$ and

$$\begin{cases} x - p_2 \equiv 0 \pmod{d}, & \text{if } d \neq 1, \\ x + p_3 \equiv 0 \pmod{d}, & \text{if } d = 1; \end{cases}$$

if $k_\eta = 2^m - 1$, then $x \neq p$ and

$$\begin{cases} x + 1 - p_2 \equiv 0 \pmod{d}, & \text{if } d \neq 1, \\ x + 1 \equiv 0 \pmod{d}, & \text{if } d = 1. \end{cases}$$

In the following we deal only with the case $0 \leq k_\eta < 2^m - 1$. The corresponding assertion for $k_\eta = 2^m - 1$ can be treated in the same way.

To begin with we note $p|(2^m - 1)$ and $p|k_\eta$ (see (2.8) and (2.9)). Hence, for some $k$ we get $2^m x + k_\eta = x + kp$. Since $k_\eta < (1 - \delta)2^m$ for some $0 < \delta < 1$ (see (2.10)), the number $k$ satisfies $2p_3 < k < (2 - \delta)2^m$. Write $k = 2\mu + \beta$ with $\beta \in \{0, 1\}$, so $p_3 < \mu < (1 - \delta/2)2^m$. Let $\epsilon_{i,j} = 0$ for $j = 2, 3$. We get

$$2^m x + k_\eta - \sum_{i=0}^{m-1} \sum_{j=1}^3 \epsilon_{i,j} p_j 2^i = 2^m x + k_\eta - lp_1$$

$$= x + kp - lp_1$$

$$= x + \mu p_1 - lp_1 + \beta p$$

$$= x + \alpha p_1 + \beta p.$$

We can choose $l$ satisfying $p_3 - p_1 \leq x + \alpha p_1 + \beta p < p_3$. Thus, $x + \alpha p_1 + \beta p \in \mathcal{B}(x)$ by the definition of $\mathcal{B}(x)$. Now the fact $p_1 < p_3 - p_1$ and Lemma 3.4 imply further

$$0 \leq x + \alpha p_1 + \beta p - p_3 + p_1 < p_1 \quad \text{and} \quad x + \alpha p_1 + \beta p - p_3 + p_1 \in \mathcal{B}(x).$$

Lemma 3.2 tells us that we can substitute $p$ if the above number is not less than $p$. We obtain in this way $x - p_3 + l_1 p = x + \alpha p_1 + \beta p - p_3 + p_1 - p \in \mathcal{B}(x)$ and $0 \leq x - p_3 + l_1 p < p$. As in Case 1 we conclude recursively that $0 \leq x - sp_3 + l_1 p + p \leq x + dv + \alpha p_1 + \beta p < p_3 - p_2$. Now, since $d \neq 1$, we deduce $p_3 - p_1 - p_2 \neq 0$. Hence, $0 < x + dv + \alpha p_1 + \beta p < p_3 - p_2 < p_2$. We can therefore apply Lemma 3.1 for

$$\{0, 1, \ldots, p - 1\} \subseteq \mathcal{B}(x).$$
Let \( l \) be odd and let it satisfy \( 0 \leq l < p_3 \). Then Lemma 3.1 shows that \( 2^m l \) is odd and \( 2^m l \leq 2^m p_3 \leq p_3 \). Hence, we can again substitute \( \alpha p_1 \) and \( \beta p_3 \) with \( \alpha p_3 \) and \( \beta p_3 \). The above approach tells us that we need only to have \( 2^m l + \alpha p_1 + \beta p_3 < p_3 \). For this goal let us observe that \( \alpha p_1 + \beta p_3 \) is odd and \( 2^m l + \alpha p_1 + \beta p_3 < p_3 \). We conclude from the last relation that

\[
\{ l : 0 < l \leq p_3 \text{, } l \text{ is odd} \} \subseteq \mathcal{B}(x).
\]

(3.13)

Assertion (3.1) follows from (3.12) and (3.13).

Next we prove (3.1) for \( k_{m} = 0 \) via (3.8). The above approach tells us that we need only to have (3.12). For this goal let us observe \( \mathcal{B}(p_1) \). By the definition of \( \mathcal{B}(p_1) \) we certainly have \( \{ l p_1 : 0 \leq l \leq l' \} \subseteq \mathcal{B}(p_1) \), where \( l' \) satisfies \( l' p_1 \leq p_3 \leq (l' + 1) p_3 \). Lemma 3.2 implies \( p \in \mathcal{B}(p_1) \). On the other hand, there is a choice of \( \epsilon_{i,j} \) such that

\[
2^m p_1 - \sum_{i=0}^{m-1} \sum_{j=1}^{3} \epsilon_{i,j} 2^{j} p_j = (2^m - 1) p_1 - \sum_{i=1}^{m-1} \epsilon_{i,3} 2^{i} p_3 = 0.
\]

Thus,

\[
\{ l p_1 : 0 \leq l \leq l' \} \cup \{ p \} \subseteq \mathcal{B}(p_1).
\]
Let \( p_3 - p_1 \leq lp_1 < p_3 \). It follows from Lemma 3.4 that \((l + 1)p_1 - p_3 \in \mathcal{B}(p_1)\). Thus, by Lemma 3.2 there exists a \( j \) such that \( 0 < jlp - p_3 \leq p \) and \( jlp - p_3 \in \mathcal{B}(p_1) \). Similarly, let \( p_3 - p_2 - p_1 < lp_1 \leq p_3 - p_2 \). We conclude for some \( j \) that \( jlp - p_3 + p_2 \in \mathcal{B}(p_1) \) and \( 0 < jlp - p_3 + p_2 \leq p \). Now we can choose \( x \) as follows:

\[
\begin{cases}
x = jlp - p_3 + p_2 \text{ and } 0 < jlp - p_3 + p_2 \leq p, & \text{if } d \neq 1, \\
x = jlp - p_3 \text{ and } 0 < jlp - p_3 \leq p, & \text{if } d = 1.
\end{cases}
\]

Clearly, \( x \) satisfies (3.9) and \( x \in \mathcal{B}(p_1) \). Consequently, (3.8) holds with this \( x \) and \( \mathcal{B}(x) \subseteq \mathcal{B}(p_1) \). We obtain by (3.8) the desired relation, i.e.,

\[
\{0, 1, \ldots, p_1 - 1, p_1, 2p_1, \ldots, l'p_1\} \subseteq \mathcal{B}(p_1).
\]

Now let \( p = p_1/2 \) be even. Denote \( \gcd(p_3 - p_2, p) = d \). So \( d \) is even. We verify for some \( 0 \leq x < p \) that

\[
(x + dv: 0 \leq x + dv < p) \subseteq \mathcal{B}(x).
\]

To this end we choose \( 0 \leq x < p \) as follows:

\[
\begin{cases}
x - p_2 = 0 \pmod{d}, & \text{if } 0 \leq k_\eta < 2^m - 1, \\
x + 1 - p_2 = 0 \pmod{d}, & \text{if } k_\eta = 2^m - 1.
\end{cases}
\]

Clearly, \( x \) is not unique. But \( x \) is odd if \( 0 \leq k_\eta < 2^m - 1 \) and even when \( k_\eta = 2^m - 1 \). Moreover, any \( 0 \leq x + dv < p \) satisfies (3.15). To verify (3.14), we remember that \( k_\eta \) is even when \( 0 \leq k_\eta < 2^m - 1 \). So in any case \((2^m - 1)x + k_\eta \) is odd. We also remember \( p_3|\!(2^m - 1) \) and \( p_3|\!k_\eta \) since \( p_3 \) is odd. Now by Lemma 3.3 we obtain \( x + p_3 - p_2 \in \mathcal{B}(x) \). On the other hand, since \( x - p \leq -1 \) and \( p_3 - p_2 \leq (p_3 - 1)/2 \), we have

\[
(2^m - 1)(x + p_3 - p_2 - p) + k_\eta < (2^{m-1} - 1)p_3.
\]

Thus, the condition of Lemma 3.2 is satisfied. We obtain by Lemma 3.2 with \( y = x + p_3 - p_2, p_1 = p_1 \) and \( p_2 = p_3 \) that \( x + p_3 - p_2 - p \in \mathcal{B}(x) \). Recursively, \( x + p_3 - p_2 - \alpha_1p \in \mathcal{B}(x) \) for some \( \alpha_1 \) such that \( 0 \leq x + p_3 - p_2 - \alpha_1p < p \). Clearly, this new number also satisfies (3.15). We can therefore apply this procedure for this new number to obtain another number that satisfies (3.15) and is contained in \( \mathcal{B}(x) \). Repeatedly, we obtain for \( s = 0, 1, \ldots, p/d - 1 \) that

\[
x + sx(p_3 - p_2) - \alpha_sp \in \mathcal{B}(x) \quad \text{and} \quad 0 \leq x + s(p_3 - p_2) - \alpha_sp < p,
\]

where \( \alpha_0 = 0 \). Since \( \gcd(p_3 - p_2, p) = d \), they are all different and have the form \( x + dv \). This shows (3.14).

Next we verify

\[
(3.16) \quad \{0, \ldots, p - 1\} \subseteq \mathcal{B}(x).
\]

To show (3.16), let \( 0 \leq x + dv < p \). Since \((2^m - 1)(x + dv) + k_\eta \) is odd, it follows from (i) of Lemma 3.3 with \( p' = p_1 \) and \( p_1 = p_2 \) that \( x + dv + p_1 - p_1 \in \mathcal{B}(x) \). Now \( (2^m - 1)(x + dv + p_2 - p_1) + k_\eta \) is even. We apply (ii) of Lemma 3.3 with \( p_1 = p_2 \) and, if necessary, Lemma 3.3 with \( p_1 = p_1 \) to obtain \( 0 \leq x + dv + p_2 - l_1p < p \) and

\[
x + dv + p_2 - l_1p = x + dv + p_2 - l_1p - l_1p \in \mathcal{B}(x).
\]

For this new number \((2^m - 1)(x + dv + p_2 - l_1p) + k_\eta \) is even. Clearly, we can again use (ii) of Lemma 3.3 to obtain \( x + dv + p_2 - l_1p + 2p_2 - p_3 \in \mathcal{B}(x) \). Write

\[
x + dv + p_2 - l_1p + 2p_2 - p_3 = x + dv + 2p_2 - l_1p - (p_3 - p_2).
\]
For this number \((2^m - 1)(x + dv + 2p_2 - l_1p - (p_3 - p_2)) + k_{\eta}\) is odd. We get by (i) of Lemma 3.3 and, if necessary, Lemma 3.2 that \(0 \leq x + dv + 2p_2 - l_2p - l'(p_3 - p_2) < p\) and

\[
x + dv + 2p_2 - l_1p - l'(p_3 - p_2) - lp = x + dv + 2p_2 - l_2p - l'(p_3 - p_2) \in \mathcal{B}(x).
\]

Repeatedly, we conclude for \(s = 0, 1, \ldots, d - 1\) that

\[
0 \leq x + dv + sp_2 - l_3p - l'_s(p_3 - p_2) < p \quad \text{and} \quad x + dv + sp_2 - l_3p - l'_s(p_3 - p_2) \in \mathcal{B}(x).
\]

By our construction it is easy to see that if \((v, s) \neq (v', s')\), then the corresponding numbers are different. There are \(p/d\) different \(v\) and \(d\) different \(s\). Therefore, \(\mathcal{B}(x)\) contains \(d \times p/d\) numbers in \(\{0, \ldots, p - 1\}\). In other words, (3.16) holds.

We have to show that \(p\) in (3.16) can be replaced by \(p_3\). We first prove this for \(k_{\eta} \neq 2^m - 1\). Let \(0 < l < p_3\) be odd. So \((2^m - 1)l + k_{\eta}\) is odd. As before we use Lemmas 3.3 and 3.2 to obtain \(l + p_3 - p_2 - \alpha p \in \mathcal{B}(x)\) for \(\alpha \geq 0\) satisfying \(0 \leq l + p_3 - p_2 - \alpha p < p_3\). Since \(l + p_3 - p_2 - \alpha p = l'\) is again odd, we obtain in particular that all odd numbers in \(\{0, \ldots, p_3 - p_2 - 1\}\) belong to \(\mathcal{B}(x)\). Applying Lemma 3.3 for each odd number \(l'\) from the last set, we conclude \(l' + l(p_3 - p_2) \in \mathcal{B}(x)\) whenever \(0 \leq x + dv + l(p_3 - p_2) < p_3\) and \(l \geq 0\). Thus, \(\mathcal{B}(x)\) contains all odd \(0 < l' < p_3\), i.e.,

\[
(3.17) \quad \{l: \ 0 \leq l < p_3, \ l \ is \ odd\} \subseteq \mathcal{B}(x).
\]

Let \(l\) be odd and \(0 < l < p_3 - p_2\). Since \(p_3 - p_2 < p_2\), we have by Lemma 3.1 with \(p_2\) that \(l + p_2 \in \mathcal{B}(x)\). Consequently,

\[
(3.18) \quad \{l: \ p_2 \leq l < p_3\} \subseteq \mathcal{B}(x).
\]

Furthermore, let \(l\) be even and \(p_2 \leq l < p_3\). So \((2^m - 1)l + k_{\eta}\) is even. We conclude from Lemma 3.3 that \(\mathcal{B}(x)\) contains \(l - \mu p_1\) whenever \(\mu \geq 0\) and \(0 \leq l - \mu p_1 < p_3\). It follows from the fact that \(p_3 \geq p_2 + p_1\) and \(p_1\) is even that

\[
(3.19) \quad \{l: \ 0 \leq l < p_2, \ l \ is \ even\} \subseteq \mathcal{B}(x).
\]

The desired assertion follows from (3.16)-(3.19).

The proof for \(k_{\eta} = 2^m - 1\) is the same. We omit the details here.

**Step 2.** Let (3.1) be true for \(|S(a)| \leq k\) with \(k \geq 3\). We verify (3.1) for \(|S(a)| = k + 1\). Write \(S(a) = \{0, p_1, \ldots, p_k\}\) and \(\hat{S}(a) = \{0, p_k - p_{k-1}, \ldots, p_3 - p_1, p_1\}\). Therefore, we need to prove (3.1) either for \(S(a)\) or for \(\hat{S}(a)\). The special case of \(|S(a)| = 4\), which we dealt with in Step 1, allows us to suppose that there is \(0 < p \in S(a)\) such that \(S(a) \setminus \{p\}\) has property P. Denote \(\gcd(p^\prime: p^\prime \in S(a) \setminus \{p\}) = d\) and

\[S'(a) = \{q: dq \in S(a) \setminus \{p\}\} = \{0, q_1, \ldots, q_{k-1}\}.
\]

\(S'(a)\) has property P. Moreover, \(\gcd(q_1, \ldots, q_{k-1}) = 1\) and \(|S'(a)| = k\). Let us also remark that in general \(m\) and \(k_{\eta}\) depend on \(S(a)\). Hence, for different \(S(a)\) the numbers \(m\) and \(k_{\eta}\) are generally different. On the other hand, it is clear that if \(m\) and \(k_{\eta}\) are numbers for \(S(a)\), they are also suitable for \(S(a) \setminus \{p\}\). Furthermore, \(m\) and \(k_{\eta}/d\) are numbers for \(S'(a)\). With this in mind it is now clear that the hypothesis of the induction implies for some \(0 \leq x' < q_{k-1}\) that

\[
\{0, \ldots, q_{k-1} - 1\} = B'(x'),
\]
where $\mathcal{B}'(x')$ is the corresponding set $\mathcal{B}(x)$ defined by $S'(a)$, $m$ and $k_n/d$. By Lemma 3.1 and the definition of $\mathcal{B}(dx')$ we obtain

$$\{ld : 0 \leq ld < p_k\} \subseteq \mathcal{B}(dx').$$

Indeed, if $dq_{k-1} = p_k$, (3.20) follows directly from the definition of $\mathcal{B}(dx')$. If however $dq_{k-1} \neq p_k$, then $p = p_k$ and $dq_{k-1} = p_{k-1}$. So

$$\{ld : 0 \leq ld < p_{k-1}\} \subseteq \mathcal{B}(dx').$$

But there is an odd number in $S(a) \setminus \{p_k, p_{k-1}\}$. Using Lemma 3.1 with this number, we can still replace $p_{k-1}$ by $p_k$. Clearly, (3.20) is (3.1) if $d = 1$. So in the following discussion we should always assume $d \neq 1$. In what follows we should use (3.20) to prove (3.1) for $S(a)$. The proof will be divided into four cases according to different $p$ and $p_k$.

**Case 1.** $p_k$ is even and there are at least two odd numbers in $S(a)$. Without loss of generality let two odd numbers be $p_1$ and $p_2$. Let $\gcd(p_1, p_3, \ldots, p_k) = d$ and

$$S'(a) = \{q_i : dq_i \in S(a) \setminus \{p_2\}\} = \{0, q_1, \ldots, q_{k-1}\}.$$

We obtain (3.20) with $p = p_2$. To verify (3.1) for $S(a)$ from (3.20), let $2p_2 \leq p_k$. We choose $l' \geq 0$ such that $p_k - p_2 + ld \leq l'd + ld < p_k - p_2 + (l + 1)d$ for $l = 0, \ldots, p_1/d - 1$. Clearly, $l'd + ld \in \mathcal{B}(dx')$. Moreover, by Lemma 3.4 the set $\mathcal{B}(dx')$ contains $l'd + ld - p_k + p_2$ and

$$ld \leq l'd + ld - p_k + p_2 < (l + 1)d \leq p_1.$$ 

Denote $y = l'd - p_k + p_2$. We have $y - p_2 \equiv 0 \pmod{d}$ and $y \neq 0$. Using Lemma 3.1, we conclude that for some $\alpha_{l,1} > 0$ and $l = 0, \ldots, p_1/d - 1$ the numbers $y + ld + \alpha_{l,1}p_1$ are in $\mathcal{B}(dx')$ as well as in $[p_k - p_2, p_k - p_2 + p_1]$. Again by Lemma 3.4 we obtain for $l = 0, 1, \ldots, p_1/d - 1$ that

$$0 < y + ld + \alpha_{l,1}p_1 - (p_k - p_2) < p_1 \quad \text{and} \quad y + ld + \alpha_{l,1}p_1 - (p_k - p_2) \in \mathcal{B}(dx').$$

We note that the choice of $y$ ensures $y - s(p_k - p_2) \equiv 0 \pmod{d}$ if and only if $s + 1 \equiv 0 \pmod{d}$. Thus, write $\alpha_{l,0} = 0$. We conclude repeatedly that $\mathcal{B}(dx')$ contains $y + ld + \alpha_{l,s}p_1 - s(p_k - p_2)$ and

$$0 \leq y + ld + \alpha_{l,s}p_1 - s(p_k - p_2) < p_1, \quad \forall s = 0, \ldots, d - 1, \quad l = 0, 1, \ldots, p_1/d - 1.$$ 

It is easy to see that all these numbers are different. Consequently, $\{0, \ldots, p_1 - 1\} \subseteq \mathcal{B}(dx')$. Since $d[p_1, we get by (3.20) that

$$\{0, \ldots, p_1\} \cap \{ld : 0 \leq ld < p_k\} \subseteq \mathcal{B}(dx').$$

The desired assertion follows from this relation and Lemma 3.1, since any $p_1 < z < p_k$ can be written as $z = z' + np_1$ with $0 \leq z' < p_1$.

Let $2p_1 \geq p_k$. Then $2(p_k - p_{k-2}) \leq p_k$. Hence, the above proof is valid for $\tilde{S}(a)$. We again get (3.1) by the symmetric relation (3.2).

Finally, let $2p_1 < p_k < 2p_2$. Equation (3.2) allows us to suppose $p_1 + p_2 \leq p_k$. The approach is the same as for the case $2p_2 \leq p_k$. First we choose $l' \geq 0$ such that

$$p_k - p_2 - p_1 + ld \leq l'd + ld < p_k - p_2 - p_1 + (l + 1)d, \quad \forall \ l = 0, \ldots, p_1/d - 1.$$ 

Hence, by Lemma 3.1 and (3.20) the number $l'd + p_2$ is contained in $\mathcal{B}(dx')$, while Lemma 3.4 implies that $y = l'd + p_2 + p_1 - p_k$ is in $\mathcal{B}(dx')$. Moreover, for the same reason

$$y + ld \in \mathcal{B}(dx') \quad \text{and} \quad ld \leq y + ld < (l + 1)d, \quad \forall \ l = 0, \ldots, p_1/d - 1.$$
Clearly, $y + sp_2 \equiv 0 \pmod{d}$ if and only if $s + 1 \equiv 0 \pmod{d}$. Therefore, using the same approach as for $2p_2 \leq p_k$, we conclude that $B(dx')$ contains $y + dl + \alpha l, p_1 - s(p_2 - p_2 - p_1)$ for $s = 0, 1, \ldots, d - 1$ and $l = 0, \ldots, p_1/p_2 - 1$. These numbers are different and are in $[0, p_1)$. Consequently, $\{0, \ldots, p_1\} \cup \{ld : 0 \leq ld < p_k\} \subseteq B(dx')$ and thus we get the desired assertion.

Case 2. $p_k$ is even and there is only one odd number $p$ in $S(a)$. Let $p \neq p_1, p_{k-1}$. We may assume $2p \leq p_k$. Otherwise, we consider $S(a)$ and $q = p_k - p$. Write gcd$(p_1, p_2, \ldots, p_{k-1}) = d$. So with $S'(a) = \{0, p_1/d, \ldots, p_{k-1}/d\}$ we obtain for some $0 \leq x' < p_k - 1/d$ the relation (3.20). Having (3.20), we choose $l'$ such that
\[
p_k - p + ld \leq dl' + ld < p_k - p + (l + 1)d, \quad \forall \ l = 0, \ldots, p/d - 1.
\]
Next we apply Lemma 3.4 to get $y + ld = dl' + ld - p_k + p \in B(dx')$. Now it is clear that
\[
0 \leq y + dl < p, \quad \forall \ l = 0, \ldots, p/d - 1.
\]
Moreover, $y - sp_k \equiv 0 \pmod{d}$ if and only if $s + 1 = 0 \pmod{d}$. The same approach as in Case 1 (with $p$ instead of $p_1$) yields
\[
\{0, \ldots, p\} \cup \{ld : 0 \leq ld < p_k\} \subseteq B(dx').
\]

We know now how to get (3.1) from this relation.

To show (3.1) for $p = p_1$ or $p_{k-1}$, we should modify the above proof. Without loss of generality we may assume $p = p_1$ and $2p_1 > p_k$. So the $p_j, j = 2, \ldots, k$, are even. Denote gcd$(p_1, p_2, \ldots, p_{k-2}, p_k) = d_1$. With $S'(a) = \{0, p_1/d_1, \ldots, p_{k-2}/d_1, p_k/d_1\}$ we obtain (3.20). To verify (3.1), let $q = p_k - p_1, q' = p_k - 1/2$. So gcd$(d_1, q') = 1$. We already know that $ld_1 + dx'_1 \in B(d_1x')$ for all $l = 0, 1, \ldots, q'/d_1 - 1$. Now, since $q < p_1$, it follows from Lemma 3.1 that $ld_1 + d_1 + p_1 \in B(d_1x')$ while Lemma 3.4 with $p_1 = p_1$ and $p_2 = p_k$ implies $ld_1 + d_1 + p_1 - q \in B(d_1x')$ for some $q' \leq q_1 + d_1 + p_1 - q_1' < q + q'$. Lemma 3.2 with $p_{k-1}$ leads to $ld_1 + x_1 + (p_1 - q_1') - q_1 \in B(d_1x')$ and $0 \leq ld_1 + d_1 + (p_1 - q') - q_1 < q$. Now, let $y = d_1 + (p_1 - q') - q_1$. Then $y \in B(d_1x')$ and $0 < y < q$. Recursively, we obtain from the above procedure that $0 \leq y + ld_1 + t_1d_1 - sq' < 2$ and $0 + ld_1 + t_1d_1 - sq' < q$. Combining this with (3.21) leads to (3.1).

Case 3. $p_k$ is odd. $S(a) \setminus \{p_k\}$ does not have property $P$. Thus, $S(a)$ contains an odd $p \neq p_k$ and an even $q \neq 0$. It is easy to see that $p_1, \ldots, p_{k-2}$ are even and $p_{k-1}$ is odd. Suppose $p_k \geq 2p_{k-2}$, so $2p_j < p_k$ for $j = 1, 2, \ldots, k - 2$. Clearly $S(a) \{p_2\} = \{0, p_1, p_3, \ldots, p_k\}$ has property $P$. Denote gcd$(p_1, p_3, \ldots, p_k) = d_1$ and $S'(a) = \{0, p_1/d_1, p_3/d_1, \ldots, p_k/d_1\}$. We obtain (3.20) with some $0 \leq x' < p_k$, i.e.,
\[
\{ld_1 : 0 \leq ld_1 < p_k\} \subseteq B(d_1x').
\]
Let \( l' \) satisfy
\[
p_k - p_2 + ld_1 \leq l'd_1 + ld_1 < p_k - p_2 + (l + 1)d_1 \quad \forall \ l = 0, \ldots, p_1/d_1 - 1.
\]
Clearly, for each such \( l \) it holds that
\[
(2^m - 1)(l'd_1 + ld_1 - p_2) + k_\eta < (2^m - 1)(p_k - p_2).
\]
Hence, by Lemma 3.4 we conclude that
\[
ld_1 \leq l'd_1 + ld_1 - (p_k - p_2) < (l + 1)d_1 \quad \text{and} \quad l'd_1 + ld_1 - (p_k - p_2) \in \mathcal{B}(d_1x').
\]
Write \( y = l'd_1 - (p_k - p_2) \). We obtain \( y + sp_2 \equiv 0 \pmod{d_1} \) if and only if \( s + 1 \equiv 0 \pmod{d_1} \). We know that \( p_1 = 2^\mu g_i \), where \( g \) is odd. Also, \( d_1 \neq 1 \) implies \( g \neq 1 \). For each \( y + ld_1 \) we choose \( \epsilon_{i,j} = 0 \) for \( j > 1 \) to obtain
\[
2^m(y + ld_1) + k_\eta - \sum_{i=0}^{m-1} \sum_{j=1}^{k} \epsilon_{i,j} 2^jp_j = 2^m(y + ld_1) + k_\eta - \sum_{i=0}^{m-1} \epsilon_{i,1} 2^ip_1
\]
\[
= y + ld_1 + (2^m - 1)(y + ld_1) + k_\eta - \gamma p_1
\]
\[
= y + ld_1 + (2^m - 1)(y + ld_1) + k_\eta - \gamma 2^\mu g,
\]
where \( \gamma \) can be any integer between 0 and \( 2^m - 1 \). By the definition of \( \mathcal{B}(d_1x') \) we conclude that \( y + ld_1 + (2^m - 1)(y + ld_1) + k_\eta - \gamma 2^\mu g \in \mathcal{B}(x) \) whenever \( y + ld_1 + (2^m - 1)(y + ld_1) + k_\eta - \gamma 2^\mu g \in \mathbb{Z}_{p_k} \). Thus, we can choose \( \gamma \) to obtain
\[
y + ld_1 + (2^m - 1)(y + ld_1) + k_\eta - \gamma 2^\mu g = y + ld_1 + rp_1 + \beta g
\]
with some \( r \) and \( 0 \leq \beta \leq 2^\mu - 1 \) such that \( p_k - p_2 \leq y + ld_1 + rp_1 + \beta g < p_k \). It follows from Lemma 3.4 that \( 0 \leq y + ld_1 + rp_1 + \beta g - (p_k - p_2) < p_2 \) is contained in \( \mathcal{B}(d_1x') \). Furthermore, with \( p_{i_1} = p_1 \) and \( p_{i_2} = p_k \) we get by Lemma 3.2 for some \( \alpha \geq 0 \) that
\[
0 \leq y + ld_1 + rp_1 + \beta g - (p_k - p_2) - \alpha g < p_1
\]
and
\[
y + ld_1 + rp_1 + \beta g - (p_k - p_2) - \alpha g \in \mathcal{B}(d_1x')
\]
We may write with some \( \alpha_{i,1} \)
\[
y + ld_1 + rp_1 + \beta g - (p_k - p_2) - \alpha g = y + ld_1 + \alpha_{i,1} d_1 - (p_k - p_2).
\]
Clearly, these new numbers are different from \( y + ld_1 \). Therefore with \( \alpha_{i,0} = 0 \) we conclude recursively for \( s = 0, 1, \ldots, d_1 - 1, l = 0, \ldots, p_1/d_1 - 1 \) that
\[
0 \leq y + ld_1 + \alpha_{i,s} d_1 - s(p_k - p_2) < p_1 \quad \text{and} \quad y + ld_1 + \alpha_{i,s} d_1 - s(p_k - p_2) \in \mathcal{B}(d_1x').
\]
The choice of \( y \) ensures that these numbers are all different. Hence, together with (3.20) we get
\[
\{0, 1, \ldots, p_1\} \cup \{ld_1 : 0 \leq ld_1 < p_k\} \subseteq \mathcal{B}(d_1x').
\]
To finish our proof for the case \( p_k \geq 2p_k - 2 \), we have to verify \( \{p_1 + 1, \ldots, p_k - 1\} \subseteq \mathcal{B}(d_1x') \). For this goal we assume first \( k_\eta \neq 2^m - 1 \). Thus, \( k_\eta \) is even. We apply (i) of Lemma 3.3 with \( p_{i_1} = p_k \) and \( p_{i_2} = p_k - 1 \) for each odd number from \( \{0, \ldots, p_1\} \) to obtain
\[
\{x : 0 \leq x \leq p_1 + p_k - p_1, \ x \ \text{is odd}\} \cap \mathbb{Z}_{p_k} \subseteq \mathcal{B}(d_1x').
\]
Recursively, we conclude
\[
\{x : 0 \leq x < p_k, \ x \ \text{is odd}\} \subseteq \mathcal{B}(d_1x').
\]
Next, we use Lemma 3.1 with \( p_{k-1} \) for each number from \( \{1, \ldots, p_1\} \) to get
\[
\{x : p_{k-1} < x \leq \min\{p_{k-1} + p_1, p_k - 1\}\} \subseteq B(d_1x').
\]
Now for each even number \( x \) between \( p_{k-1} \) and \( \min\{p_{k-1} + p_1, p_k - 1\} \) we apply (ii) of Lemma 3.3 with \( p_i = p_k \) and \( p_j' = p_1 \). So, recursively, we obtain
\[
\{x : p_1 \leq x \leq p_{k-1}, \; x \text{ is even}\} \subseteq B(d_1x').
\]
Combining this with (3.22) and (3.23), we get
\[
\{0, \ldots, p_{k-1}\} \subseteq B(d_1x').
\]
The desired assertion follows from Lemma 3.1 with \( p_{k-1} \) and the last relation. Similarly, we have (3.1) for \( k = 2^m - 1 \).

It remains to show (3.1) for \( 2p_{k-2} \geq p_k \). Thus \( 2(p_k - p_{k-2}) \leq p_k \). The symmetric relation (3.2) tells us that in this case we need only to verify (3.1) for the set \( S(a) \) with even \( p_1 \) and odd \( p_2, \ldots, p_k \), which satisfies \( 2p_1 \leq p_k \). Clearly \( \{0, p_1, \ldots, p_{k-1}\} \) has property \( P \). Denote gcd\( (p_1, \ldots, p_{k-1}) = d_2 \). We have as before
\[
\{ld_2 : 0 \leq ld_2 < p_k\} \subseteq B(d_2x').
\]
Next, for \( l = 0, \ldots, p_1/d_2 - 1 \) let \( l' \) be such that
\[
p_k - p_1 + ld_2 \leq l'd_2 + ld_2 < p_k - p_1 + (l + 1)d_2.
\]
Write \( y = l'd_2 - (p_k - p_1) \). Lemma 3.4 tells us that \( y + ld_2 \in B(d_2x') \) for \( l = 0, \ldots, p_1/d_2 - 1 \). We now know how to use Lemmas 3.1, 3.2 and 3.4 from these numbers to obtain, for \( s = 0, \ldots, d_2 - 1 \) and \( l = 0, \ldots, p_1/d_2 - 1 \),
\[
y + ld_2 + \alpha_{s,l}d_2 - s(p_k - p_1) < p_1 \quad \text{and} \quad y + ld_2 + \alpha_{s,l}d_2 - s(p_k - p_1) \in B(d_2x'),
\]
which in turn implies \( \{0, \ldots, p_1 - 1\} \subseteq B(d_2x') \). Hence,
\[
\{0, \ldots, p_1\} \cup \{ld_2 : 0 \leq ld_2 < p_k\} \subseteq B(d_2x').
\]
The assertion follows from Lemmas 3.1, 3.3 and this relation.

Case 4. \( p_k \) is odd. \( S(a) \setminus \{p_k\} \) has property \( P \) and \( S(a) \setminus \{p_k\} \) contains an odd \( p \) and an even \( q \neq 0 \). Denote gcd\( (p_1, \ldots, p_{k-1}) = d \). Thus, we obtain (3.20), i.e.,
\[
\{ld : 0 \leq ld < p_k\} \subseteq B(dx').
\]
For \( q \leq p_k - q \) the proof is the same as in the last situation of Case 3. We omit the details here.

Let \( q \geq p_k - q \). We may assume that \( q \) is minimal among all nonzero even numbers in \( S(a) \) and that \( p \) satisfies \( 2p < p_k \). Otherwise we consider \( S(a) \), for which we have already the desired assertion. For the same reason we can also assume \( p + q \leq p_k \). To this end, first let \( 2p \geq q \). Denote \( q' = q/2 \). Furthermore, let \( q \leq l'd + ld < p_k \) for some \( l' \) and \( l = 0, \ldots, q'/d - 1 \). By Lemma 3.4 we get \( 2q - p_k \leq l'd + ld - (p_k - q) \leq q \). We may use Lemma 3.2 to subtract \( q' \) from \( l'd + ld - (p_k - q) \) such that \( 0 \leq l'd + ld - (p_k - q) - \alpha_lq' < q' \). Now write
\[
y_l = l'd + ld - (p_k - q) - \alpha_lq'.
\]
Thus,
\[
y_l \in B(dx') \quad \text{and} \quad y_l \neq 0, \: \forall \: l = 0, \ldots, q'/d - 1.
\]
Furthermore, they are all different and \( y_l - sp_k \equiv 0 \pmod{d} \) if and only if \( s + 1 \equiv 0 \pmod{d} \). Now we obtain recursively by applying Lemma 3.1 with \( p \), Lemma 3.4 with \( q \) and \( p_k \) and finally Lemma 3.2 with \( q \) that
\[
y_l + \alpha_{l,s}d + s(p_k - q) \in B(dx') \quad \text{and} \quad 0 \leq y_l + \alpha_{l,s}d + s(p_k - q) < q'.
\]
for \( l = 0, \ldots, q'/d-1 \) and \( s = 0, \ldots, d-1 \). Hence, together with (3.20) we conclude

\[
\{0, \ldots, q'\} \cup \{ld : 0 \leq ld < p_k\} \subseteq \mathcal{B}(dx').
\]

We verify that \( q' \) in the above relation can be replaced by \( p \). If \( q' \geq p \), we have nothing more to do. If \( q' < p \), we use Lemma 3.1 with \( p \) to obtain

\[
\{0, \ldots, q'\} \cup \{p, \ldots, p + q'\} \subseteq \mathcal{B}(dx').
\]

For each number of \( \{p, \ldots, p + q' - 1\} \) we apply Lemma 3.2 with \( q \) to obtain \( \{p - q', \ldots, p - 1\} \subseteq \mathcal{B}(dx') \). Thus,

\[
\{p - q', \ldots, p + q'\} \subseteq \mathcal{B}(dx').
\]

Again using Lemma 3.2 with \( q \) for each element from \( \{p - q', \ldots, p + q' - 1\} \), we obtain \( \{p - 2q', \ldots, p + q'\} \subseteq \mathcal{B}(dx') \). Recursively, \( \{0, \ldots, p + q'\} \subseteq \mathcal{B}(dx') \). Thus,

\[
(3.24) \quad \{0, \ldots, p\} \cup \{ld : 0 \leq ld < p_k\} \subseteq \mathcal{B}(dx').
\]

Since \( p \) is odd, (3.1) follows from Lemma 3.1 with \( p \) and the last relation.

It remains to verify (3.1) for \( 2p \leq q \). We should modify the procedure for \( 2p \geq q \) as follows: let \( p_k - p \leq l'd + ld < p_k \) for some \( l' \) and \( l = 0, \ldots, p/d - 1 \). By Lemma 3.4 with \( p_k \) and \( q \) we get \( q - p \leq l'd + ld - (p_k - q) < q \). Again using Lemma 3.4 with \( p \) and \( q \), we conclude that \( 0 \leq l'd + ld - (p_k - p) < p \). Now write \( y_l = l'd + ld - (p_k - p) \). Thus,

\[
y_l \in \mathcal{B}(dx') \quad \text{and} \quad y_l \neq 0, \quad \forall \ l = 0, \ldots, p/d - 1.
\]

We obtain in the same way that

\[
y_l + \alpha_{l,s}p + s(p_k - p) \in \mathcal{B}(dx') \quad \text{and} \quad 0 \leq y_l + \alpha_{l,s}p + s(p_k - p) < p
\]

for \( l = 0, \ldots, p/d - 1 \) and \( s = 0, \ldots, d-1 \). Hence, together with (3.20) we conclude (3.24). From (3.24) we know how to get (3.1).

\[\square\]

ACKNOWLEDGMENT

The author is indebted to the referee for various helpful comments on his paper.

REFERENCES


Department of Mathematics, China Jiliang University, Hangzhou, China; Institute of Mathematics, University of Duisburg-Essen, D-47057 Duisburg, Germany

E-mail address: zhou@math.uni-duisburg.de