Binary Signed-Digit Integers and the Stern Polynomial

Laura Monroe

Ultrascale Systems Research Center, Los Alamos National Laboratory, Los Alamos, NM 87501
lmonroe@lanl.gov

Abstract

The binary signed-digit representation of integers is used for efficient computation in various settings. The Stern polynomial is a polynomial extension of the well-studied Stern diatomic sequence, and has itself been investigated in some depth. In this paper, we show previously unknown connections between BSD representations and the Stern polynomial.

We derive a weight-distribution theorem for \( i \)-bit BSD representations of an integer \( n \) in terms of the coefficients and degrees of the terms of the Stern polynomial of \( 2^i - n \).

We then show new recursions on Stern polynomials, and from these and the weight-distribution theorem obtain similar BSD recursions and a fast \( O(n) \) algorithm that calculates the number and number of 0s of the optimal BSD representations of all of the integers of NAF-bitslength \( \log(n) \) at once, which then may be compared.

Keywords: Binary signed-digit representations; hyperbinary representations; non-adjacent form, Stern polynomial.

Mathematics Subject Classification (2010): 11A63 · 11B83 · 68R01

1 Introduction

Integers may be represented in binary signed-digit (BSD) representation, in which each integer is represented in terms of sums or differences of distinct powers of 2 [17, 2, 16]. BSD representations of an integer are not unique; there are an infinite number of such
representations for any integer using an arbitrary number of bits, and of course, a finite number for a fixed number of bits.

The number of such representations of an integer is of interest, as is the number of representations having a maximal number of 0s, as these optimal representations may be used for efficient calculation [17, 2, 1], and in many other applications [10, 4, 8]. At times, it can be useful to have a choice of integers of a given length, each having many optimal representations, or optimal representations with many 0s, or both.

In [9], a correspondence was shown between the number of BSD representations of an integer and Stern’s diatomic sequence. We extend that work here, and examine the relationship of the related Stern polynomial [7] to the number of integer BSD representations, and in particular to optimal representations.

The first result of this paper is a weight-distribution theorem identifying the number of \(i\)-bit BSD representations of an integer \(n\) having weight \(i - \ell\) with the coefficient of the \(\ell^{th}\) term of the Stern polynomial of \(2^i - n\). This refines the result in [9], and is the basis for the rest of the paper.

As a consequence of this theorem, the number of \(i\)-bit optimal BSD representations of an integer \(n\) is the same as the leading coefficient of the Stern polynomial \(B_{2^i-n}\), and the number of 0s in an optimal representation of \(n\) is the degree of \(B_{2^i-n}\).

In an effort to express these Stern parameters more directly, we derive a simple recursion on the leading coefficients and degrees of Stern polynomials of integers. This recursion depends on a partition of \(I_k\), the interval of integers having non-adjacent form (NAF) of bitlength \(k\). \(I_k\) is partitioned into three subintervals \(A_k\), \(B_k\) and \(C_k\), as shown in Fig. 1. The leading coefficients and degrees of the Stern polynomials of integers in \(A_k\) and \(C_k\) are expressed in terms of those of \(I_{k-2}\) and those of \(B_k\) are expressed in terms of those of \(I_{k-1}\), in forward and reverse order. This is the second result of the paper.

The weight-distribution theorem is then applied to the recursion on Stern polynomials, and similar recursive formulas based on the partition are established for the number of optimal BSD representations of integers and for the weights of these optimal representations. This is the third result of the paper.

Finally, the simplicity of the recursions is illustrated with algorithms that calculate the number and number of 0s of the optimal BSD representations of all integers in \(I_k\). These algorithms are \(O(n)\), where \(n\) is the maximum integer calculated. Their advantage is that they permit comparison between all integers of a given NAF-length that have weights and number of optimal representations appropriate to the application in question.

2 The Stern polynomial

The Stern polynomial of \(n\), \(B_n(t)\), was introduced by Klavžar et al. in [7]. This polynomial is closely related to the Stern diatomic sequence. Among other things, Klavžar et al. show that \(B_n(1) = c(n)\), where \(c(n)\) is the \(n^{th}\) entry in the Stern sequence, and \(B_n(2) = n\).

Definition 1 (Stern polynomial). [7] Let \(n \in \mathbb{N}_0\). The Stern polynomial \(B_n(t)\) is defined
as follows:

\[ B_n(t) = \begin{cases} 
0 & \text{if } n = 0, \\
1 & \text{if } n = 1, \\
t \cdot B_m(t) & \text{if } n = 2m, \\
B_m(t) + B_{m+1}(t) & \text{if } n = 2m + 1. 
\end{cases} \]

For ease of notation, throughout the rest of this paper we will refer to \( B_n(t) \) simply as \( B_n \). We refer to the leading coefficient of \( B_n \) as \( \ell c(B_n) \), and to the degree of \( B_n \) as \( \deg(B_n) \).

Many papers have addressed aspects of the Stern polynomial. Ulas and Ulas discuss some of its arithmetic properties in [20] and Ulas continues this investigation in [19]. Schinzel investigates the factors of Stern polynomials in [14], and presents a formula for the leading coefficient of \( B_n(t) \) in terms of the binary representation of \( n \) in [15]. Dilcher and Tomkins continue the investigation into divisibility of Stern polynomials in [3].

The Stern polynomial and its associated properties are extremely useful in the study of BSD representations of integers. We discuss these applications throughout the rest of this paper.

\section{The weight distribution of the BSD representations of an integer}

As our first result, we derive a weight distribution of \( i \)-bit BSD representations of \( n \), in terms of the Stern polynomials \( B_{2^i - n}(t) \). This permits the application of the many prior results on the Stern polynomial to the study of BSD representations of integers.

The result given here is exact, so improves upon the upper bound given in [18] by Túma and Vábek for the number of \( i \)-bit BSD representations of an integer \( n \) of a given weight.

This derivation depends on a transform between the \( i \)-bit BSD representations of \( n \) and the \( i \)-bit hyperbinary representations of \( (2^i - 1 - n) \).

\textbf{Definition 2} (BSD representation of an integer). An integer \( n \) is in BSD representation when

\[ n = \sum_{j=0}^{i-1} b_j 2^j, \text{ where } b_j \in \{1, 0, -1\}. \]

\textbf{Definition 3} (Hyperbinary representation of an integer). [12] An integer \( n \) is in hyperbinary representation when

\[ n = \sum_{j=0}^{i-1} h_j 2^j, \text{ where } h_j \in \{0, 1, 2\}. \]

In [9], Monroe noted a correspondence between the BSD representations of \( n \) and the hyperbinary representations of \( 2^i - 1 - n \). This correspondence is restated here in Theorem 4.
Theorem 4. [9] \((b_{i-1} \cdots b_0)\) is an \(i\)-bit BSD representation of a non-negative integer \(n\) if and only if \(((1 - b_{i-1}) \cdots (1 - b_0))\) is an \(i\)-bit hyperbinary representation of \(2^i - 1 - n\).

As noted in [9], Theorem 4 gives the following transform between the digits of a BSD representation \((b_{i-1} \cdots b_0)\) of an integer \(n\) and the digits of the corresponding hyperbinary representation, \((h_{i-1} \cdots h_0)\) of \(2^i - 1 - n\).

\[
\begin{align*}
1 & \leftrightarrow 0, \\
0 & \leftrightarrow 1, \\
-1 & \leftrightarrow 2.
\end{align*}
\]  

(1)

Klavžar et al. [7] relate the coefficients of Stern polynomials to hyperbinary representations in the following theorem.

Theorem 5. [7] Let \(h_1(n, \ell)\) be the number of hyperbinary representations of \(n \in \mathbb{N}\) that have exactly \(\ell\) 1s. Then

\[
B_n = \sum_{\ell \geq 0} h_1(n - 1, \ell) \cdot t^\ell.
\]

Using Klavžar’s Theorem 5 and the transform in Equation (1), we obtain a weight distribution of the \(i\)-bit BSD representations of an integer \(n\) in terms of the Stern polynomial of \(2^i - n\).

Theorem 6. Let \(b_0(n, i, \ell)\) be the number of \(i\)-bit BSD representations of \(n \in \mathbb{N}\) that have exactly \(\ell\) 0s (and thus have weight \(i - \ell\)). Then

\[
B_{2^i - n} = \sum_{\ell \geq 0} b_0(n, i, \ell) \cdot t^\ell.
\]

Proof. By Theorem 5,

\[
B_{2^i - n} = \sum_{\ell \geq 0} h_1(2^i - n - 1, \ell) \cdot t^\ell.
\]

By Equation (1), there is a one-to-one correspondence between the \(i\)-bit hyperbinary representations of \(2^i - 1 - n\) having exactly \(\ell\) 1s and the \(i\)-bit BSD representations of \(n\) having exactly \(\ell\) 0s. So \(h_1(2^i - n - 1, \ell) = b_0(n, i, \ell)\).

Corollary 7. Let \(n \in I_k\). Then the number of 0s in the reduced NAF of \(n\) is \(\deg(B_{2^k - n})\), and its weight is \(k - \deg(B_{2^k - n})\).

Proof. This follows immediately from the weight distribution result in Theorem 6, and the fact that the NAF of \(n\) has minimum weight.
4 Non-adjacent form and the NAF-interval $I_k$

Reitweisner introduced the non-adjacent form (NAF) of an integer in [11]. The NAF-interval $I_k$ turns out to be very useful in the derivation of several properties of Stern polynomials, and therefore of BSD representations.

Using the definitions in this section, we will calculate degrees and leading coefficients of Stern polynomials recursively across NAF-intervals. The weight-distribution Theorem 6 then allows us to extend that result to count the number of optimal BSD representations of integers along with their weights.

Definition 8 (Non-adjacent form). [11] The $k$-bit non-adjacent form (NAF) of an integer $n$ is a BSD representation $(b_{k-1} \cdots b_0)$ of $n$, with the property that for all $0 \leq i < k - 1$, either $b_i$ or $b_{i+1}$ must be 0. An NAF is said to be reduced if $b_{k-1} \neq 0$.

Every integer $n$ has exactly one reduced NAF. The NAF of $n$ has the most 0s of any BSD representation of $n$ of the same length, so the smallest weight, thus making the NAF good for fast arithmetic. However, the NAF of $n$ may not be the only BSD representation of its length having minimal weight.

Definition 9 (NAF-bitlength). The NAF-bitlength of $n$ is the bitlength of the reduced NAF of $n$.

Definition 10 (NAF-interval). The NAF-interval of bitlength $k$ is the interval of positive integers having NAF-bitlength $k$. We denote this as $I_k$.

The following simple lemma shows a symmetry on the NAF-interval $I_k$: all integers in $I_k$ come in pairs $(n, 2^k - n)$, except for $2^{k-1}$, which is the midpoint of $I_k$ and is paired with itself.

Lemma 11. An integer $n \in I_k$ if and only if $2^k - n \in I_k$.

Proof. Let $n$ be positive and let $\bar{n}_i = -n_i$. The NAF of $n$ is $(1 \ 0 \ n_{k-3} \ldots n_1 \ n_0)$ if and only if the NAF of $2^k - n$ is $(1 \ 0 \ \bar{n}_{k-3} \ldots \bar{n}_1 \ \bar{n}_0)$. Both of these have NAF-bitlength $k$. \qed

Definition 12 (Sibling integers). Let $n \in I_k$. The sibling of $n$ is $2^k - n$.

Siblings appear throughout this paper, and have already appeared in Theorem 6, giving the weight distribution of the BSD representations of $n$ in terms of the Stern polynomial of its sibling $2^k - n$.

5 A partition on the NAF-interval $I_k$

The following partition of $I_k$ is the basis for the recursions shown in subsequent sections. We will draw correspondences between $A_k$, $C_k$ and $I_{k-2}$, and between $B_k$ and the first half
of $I_{k-1}$, and use these to establish recursions for Stern polynomials and BSDs of integers in $I_k$. The partition is illustrated in Fig. 1.

The interval is partitioned into three disjoint subintervals, so $I_k = A_k \cup B_k \cup C_k$. The integers $a_k$, $b_k$, and $c_k$ are the lower bounds of the intervals $A_k$, $B_k$, and $C_k$. The first and third of these subintervals, $A_k$ and $C_k$, have the same length as $I_{k-2}$. The middle subinterval, $B_k$, has the same length as $I_{k-1}$.

**Figure 1:** Partition of $I_k$, the interval of integers having NAF-bitlength $k \geq 3$. The values above the brackets indicate the length of the subintervals. The integers $a_k$, $b_k$, and $c_k$ are the lower bounds of the intervals $A_k$, $B_k$, and $C_k$, respectively. $2^{k-1}$ is the midpoint of $I_k$.

**Lemma 13.** The interval of integers $I_k$ is

$$[a_k, a_{k+1}) = \left[\left\lfloor \frac{2^k}{3} \right\rfloor, \left\lceil \frac{2^{k+1}}{3} \right\rceil\right].$$

**Proof.** This proof rests on the fact that $2^k = 1 \mod 3$, if $k$ is even, and $2^k = 2 \mod 3$, if $k$ is odd. Let $n_k$ be the the greatest integer having NAF-bitlength $k$. Then $n_k = (1010 \ldots 10)$ if $k$ is even, and $n_k = (1010 \ldots 01)$ if $k$ is odd. In either case, $n_k = \left\lfloor \frac{2^{k+1}}{3} \right\rfloor$. So $a_{k+1} = n_k + 1 = \left\lceil \frac{2^{k+1}}{3} \right\rceil$, and $a_k = n_{k-1} + 1 = \left\lfloor \frac{2^k}{3} \right\rfloor$. \hfill \Box

The remainder of this section is comprised of a few lemmas on the length of $I_k$ and on the values of the lower endpoints $a_k, b_k, c_k$ of the partitions, to be used in the recursions in Section 6 and 7. These lemmas follow from Lemma 13, the partition definition and some arithmetic. We do not include the routine proofs of Lemmas 14 through 16 here, in the interest of brevity of exposition.

**Lemma 14.** The length of $I_k$, with $k \geq 1$, is

$$|I_k| = |I_{k-1}| + 2 \cdot |I_{k-2}| = \begin{cases} \left\lceil \frac{2^k}{3} \right\rceil = a_k - 1, & \text{if } k \text{ is even,} \\ \left\lfloor \frac{2^k}{3} \right\rfloor = a_k, & \text{if } k \text{ is odd.} \end{cases}$$

**Lemma 15.** Let $I_k$ be partitioned as in Fig. 1, where $k \geq 3$. Then

$$a_k = 2^{k-2} + a_{k-2}, \quad c_k = 2^{k-1} + a_{k-2}.$$
Lemma 16. Let $I_k$ be partitioned as in Fig. 1, where $k \geq 3$. Then

$$b_k = \begin{cases} 2^{k-1} - |I_{k-2}| & \text{if } k \text{ is even}, \\ 2^{k-1} - (|I_{k-2}| - 1) & \text{if } k \text{ is odd}. \end{cases}$$

$$c_k = \begin{cases} 2^{k-1} + (|I_{k-2}| + 1) & \text{if } k \text{ is even}, \\ 2^{k-1} + |I_{k-2}| & \text{if } k \text{ is odd}. \end{cases}$$

The following lemma gives a relationship between siblings in $I_{k-2}$ and siblings in $I_k$ from $A_k$ and $C_k$.

Lemma 17. Let $0 \leq v < |I_{k-2}|$. Then

$$2^{k-2} - (a_{k-2} + v) = a_{k-2} + x \text{ if and only if } 2^k - (a_k + v) = c_k + x.$$  

In other words, $a_{k-2} + v$ is the sibling of $a_{k-2} + x$ in $I_{k-2}$ if and only if $a_k + v$ is the sibling of $c_k + x$ in $I_k$.

Proof. Let $2^{k-2} - (a_{k-2} + v) = a_{k-2} + x$. Then

$$2^k - (a_k + v) = 2^k - (2^{k-2} + a_{k-2} + v) \quad \text{by Lemma 15}$$

$$= 2^{k-1} + (2^{k-2} - (a_{k-2} + v)) \quad \text{by Lemma 15}$$

$$= 2^{k-1} + (a_{k-2} + x) \quad \text{by the assumption}$$

Conversely, let $2^k - (a_k + v) = c_k + x$. This implies $2^{k-1} - (a_k + v) = c_k - 2^{k-1} + x$. So

$$2^{k-2} - (a_{k-2} + v) = 2^{k-1} - 2^{k-2} - a_{k-2} - v \quad \text{by Lemma 15}$$

$$= 2^{k-1} - a_k - v \quad \text{by the assumption}$$

$$= c_k - 2^{k-1} + x \quad \text{by the assumption}$$

$$= a_{k-2} + x. \quad \text{by Lemma 15}$$

\[ \square \]

6 Degrees and leading coefficients of Stern polynomials on $I_k$

In this section, we give a recursion expressing the degrees and leading coefficients of Stern polynomials of integers in $I_k$ in terms of the degrees and leading coefficients of Stern polynomials of integers in $I_{k-2}$ and $I_{k-1}$.

The idea in this section is to express the Stern polynomial of $n \in I_k$ as a sum involving Stern polynomials of $2^a - r$ and $r$ so that $2^a - r$ (and perhaps $r$) are in $I_{k-1}$ or $I_{k-2}$. We then
compare the degrees of these polynomials, which allows us to deduce the leading coefficient and degree of the sum.

We make use of a lemma by Schinzel [14], extended by Dilcher and Tomkins in [3], to obtain the needed expression.

Lemma 18. [14, 3] Let $a, m, \text{ and } r$ be integers such that $0 \leq r \leq 2^a$. Then

\[ B_{2^a m + r} = B_{2^a - r} B_m + B_r B_{m+1}, \text{ and } \]
\[ B_{2^a m - r} = B_{2^a - r} B_m + B_r B_{m-1}. \]

By applying Lemma 18 with $m = 1$ or $m = 2$ (which forces the values of $a$ and $r$), a Stern polynomial may be expressed as a combination of the Stern polynomials $B_{2^a - r}$ and $B_r$, each multiplied by 1, $t$, or ($t + 1$). Lemma 19 then allows us to compare the degrees of $B_{2^a - r}$ and $B_r$, and from that, obtain the degree and leading coefficient of the sums derived from Lemma 18.

Lemma 19. Let $a \geq 1$, and let $0 \leq s < a$. Let $r \in I_{a-s}$. Then

\[ \deg(B_{2^a-r}) = s + \deg(B_r). \]

Proof. $2^a$ has NAF-bitlength $a + 1$ and $r$ has NAF-bitlength $a - s$.

If $s = 0$, $2^a - r$ may be expressed as

\[
\begin{array}{cccccccc}
1 & 0 & 0 & 0 & \cdots & 0 \\
-1 & 0 & r_{a-s-2} & \cdots & r_0 \\
1 & 0 & \overline{r}_{a-s-2} & \cdots & \overline{r}_0
\end{array}
\]

with $r$ in non-adjacent form, and with $\overline{x} = -x$. By Theorem 6, the number of 0s in $r$ is $\deg(B_r)$. The result is in reduced non-adjacent form, and has the same number of 0s as $r$. So again by Theorem 6, $\deg(B_{2^a-r}) = \deg(B_r)$.

If $s > 0$, $2^a - r$ may be expressed as

\[
\begin{array}{cccccccc}
1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\
-1 & 0 & r_{a-s-2} & \cdots & r_0 \\
1 & 0 & \cdots & 0 & \overline{1} & 0 & \overline{r}_{a-s-2} & \cdots & \overline{r}_0
\end{array}
\]

with $r$ in non-adjacent form. By Theorem 6, the number of 0s in $r$ is $\deg(r)$. The result is in reduced non-adjacent form, and has $(a + 1) - (a - s) - 1 = s$ more 0s than $r$. So again by Theorem 6, $\deg(B_{2^a-r}) = s + \deg(B_r)$. \qed

Lemma 19 has as a corollary the symmetry of degrees of Stern polynomials in $I_k$. In other words, siblings in $I_k$ have Stern polynomials of equal degree.
Corollary 20. Let $k \geq 1$ and let $n \in I_k$. Then

\[ \deg(B_{2^k-n}) = \deg(B_n). \]

Lemma 19 requires consideration of integers in terms of their NAF-bitlengths. We have not found a similar relationship in terms of binary bitlengths. The partition $I_k = A_k \cup B_k \cup C_k$ comes into play in the recursion, since $2^n - r$ and $r$ fall into different prior NAF-intervals, for $n$ in $A_k$, $B_k$ and $C_k$.

6.1 Degrees and leading coefficients of the Stern polynomial in $A_k$ and $C_k$

The Stern polynomials for the integers in both $A_k$ and $C_k$ may be expressed as a combination of Stern polynomials of siblings in $I_k - 2$. This follows by application of Schinzel’s Lemma 18 and the symmetricity of degrees of siblings.

Proposition 21. Let $k \geq 3$, and let $0 \leq v < |I_{k-2}|$. Then

\[ \deg(B_{a_k+v}) = \deg(B_{a_{k-2}+v}) + 1, \text{ and} \]
\[ \ell c(B_{a_k+v}) = \ell c(B_{a_{k-2}+v}). \]

Proof. Setting $a = 2^{k-2}$, $m = 1$, and $r = a_{k-2} + v$, we apply Lemma 18:

\[ B_{a_k+v} = B_{(2^{k-2}+a_{k-2})+v} \]
\[ = B_{2^{k-2}-(a_{k-2}+v)} + t \cdot B_{a_{k-2}+v}. \]

Because of the symmetry of degrees of siblings in $I_k$ shown in Corollary 20, $B_{a_{k-2}+v}$ and $B_{2^{k-2}-(a_{k-2}+v)}$ have the same degree. The theorem follows.

Proposition 22. Let $k \geq 3$, and let $0 \leq v < |I_{k-2}|$. Then

\[ \deg(B_{c_k+v}) = \deg(B_{2^{k-2}-(a_{k-2}+v)}) + 1, \text{ and} \]
\[ \ell c(B_{c_k+v}) = \ell c(B_{2^{k-2}-(a_{k-2}+v)}) + \ell c(B_{a_{k-2}+v}). \]

Proof. Setting $a = 2^{k-2}$, $m = 2$, and $r = a_{k-2} + v$, we apply Lemma 18:

\[ B_{c_k+v} = B_{(2^{k-1}+a_{k-2})+v} \]
\[ = t \cdot B_{2^{k-2}-(a_{k-2}+v)} + (t+1) \cdot B_{a_{k-2}+v}. \]

Because of the symmetry of degrees of siblings in $I_k$ shown in Corollary 20, $B_{a_{k-2}+v}$ and $B_{2^{k-2}-(a_{k-2}+v)}$ have the same degree. The theorem follows.
6.2 Degrees and leading coefficients of the Stern polynomial in $B_k$

The Stern polynomials of the integers in $B_k$ may be expressed as a combination of Stern polynomials of integers in $I_{k-1}$ and integers in $I_d$ with $d < k - 1$. This follows by application of Schinzel’s Lemma 18 and the lemma comparing degrees of $B_{2^n-r}$ and $B_r$.

Lemma 23 is a translation lemma that allows us to express elements in $B_k$ in the form of $2^{k-1} \pm w$, thus permitting easy application of Lemma 18.

**Lemma 23.** Let $0 \leq u \leq 2^{k-1} - b_k$, and let $w = a_{k-2} - 1 - u$. Then $w \in I_m$, with $m < k - 2$, and

\[
\begin{align*}
a_{k-1} + u &= 2^{k-2} - w, \\
b_k + u &= 2^{k-1} - w, \text{ and} \\
2^k - (b_k + u) &= 2^{k-1} + w.
\end{align*}
\]

**Proof.** We have that $w \in I_m$, for $m < k - 2$, since $w < a_{k-2}$.

By the definition of siblings in $I_k$, $a_{k-2}$ and $a_{k-1} - 1$ are siblings, so

\[
a_{k-1} - 1 = 2^{k-2} - a_{k-2}, \quad \text{by Lemma 11} \quad (2)
\]

Likewise, $b_k$ and $c_k - 1$ are siblings, so

\[
\begin{align*}
b_k &= 2^k - (c_k - 1) \\
&= 2^k - (2^{k-1} + a_{k-2} - 1) \quad \text{by Lemma 15} \\
&= 2^{k-1} - a_{k-2} + 1. \quad (3)
\end{align*}
\]

The results follow from these equations and the definition of $w$.

\[
\begin{align*}
a_{k-1} + u &= a_{k-1} + a_{k-2} - 1 - w \\
&= (2^{k-2} - a_{k-2} + 1) + a_{k-2} - 1 - w \quad \text{by Equation (2)} \\
&= 2^{k-2} - w.
\end{align*}
\]

\[
\begin{align*}
b_k + u &= b_k + a_{k-2} - 1 - w \\
&= 2^{k-1} - w. \quad \text{by the definition of } w
\end{align*}
\]

\[
\begin{align*}
2^k - (b_k + u) &= 2^k - b_k - u \\
&= 2^k - b_k - a_{k-2} + 1 + w \quad \text{by the definition of } w \\
&= 2^k - (2^{k-1} + 1) + 1 + w \quad \text{by Equation (3)} \\
&= 2^{k-1} + w.
\end{align*}
\]
Proposition 24. Let \( k \geq 3 \) and let \( 0 \leq u \leq 2^{k-1} - b_k \). Then
\[
\deg(B_{b_k+u}) = \deg(B_{a_k-1+u}) + 1, \quad \text{and} \\
\deg(B_{2^k-(b_k+u)}) = \deg(B_{a_k-1+u}) + 1.
\]

Proof. Let \( w \) be as in Lemma 23. By applying Lemma 18, with \( a = 2^{k-2}, m = 2, \) and \( r = w \),
\[
\deg(b_k + u) = \deg(B_{2^k-1-w}) \quad \text{by Lemma 23} \\
= \deg(t \cdot B_{2^k-2-w} + B_w) \quad \text{by Lemma 18} \\
= \deg(B_{2^k-2-w}) + 1 \quad \text{by Lemma 19}
\]
\( 2^k - (b_k + u) \) is the sibling of \( b_k + u \), so by Corollary 20,
\[
\deg(B_{2^k-(b_k+u)}) = \deg(B_{a_k-1+u}) + 1.
\]

\( \square \)

Proposition 25. Let \( k \geq 3 \) and let \( 0 \leq u \leq 2^{k-1} - b_k \). Then
\[
\ellc(B_{b_k+u}) = \ellc(B_{a_k-1+u}), \quad \text{and} \\
\ellc(B_{2^k-(b_k+u)}) = \ellc(B_{a_k-1+u}).
\]

Proof. Let \( w \) be as in Lemma 23. By applying Lemma 18, with \( a = 2^{k-2}, m = 2, \) and \( r = w \):
\[
B_{b_k+u} = B_{2^k-1-w} \quad \text{by Lemma 23} \\
= t \cdot B_{2^k-2-w} + B_w \quad \text{by Lemma 18} \\
\deg(t \cdot B_{2^k-2-w}) > \deg(B_w) \quad \text{by Lemma 19}
\]
So by the above and Lemma 23,
\[
\ellc(B_{b_k+u}) = \ellc(B_{2^k-2-w}) = \ellc(B_{a_k-1+u}).
\]
Again applying Lemma 18, with \( a = 2^{k-2}, m = 2, \) and \( r = w \):
\[
B_{2^k-(b_k+u)} = B_{2^k-1+w} \quad \text{by Lemma 23} \\
= t \cdot B_{2^k-2-w} + (t + 1) \cdot B_w \quad \text{by Lemma 18} \\
\deg(t \cdot B_{2^k-2-w}) > \deg((t + 1) \cdot B_w) \quad \text{by Lemma 19}
\]
So by the above and Lemma 23,
\[
\ellc(B_{2^k-(b_k+u)}) = \ellc(B_{2^k-2-w}) = \ellc(B_{a_k-1+u}).
\]

\( \square \)
6.3 Recursions on leading coefficients and degrees of Stern polynomials

In this section, the recursions on the degrees and on the leading coefficients of $I_k$ are brought together.

**Theorem 26.** Let $k \geq 3$, and let $n \in I_k$. Let $0 \leq v < |I_{k-2}|$, and let $0 \leq u \leq 2^{k-1} - b_k$. Then

\[
\deg(B_{a_k+v}) = \deg(B_{a_k-2+v}) + 1,
\]

\[
\deg(B_{b_k+u}) = \deg(B_{a_{k-1}+u}) + 1,
\]

\[
\deg(B_{2^k-(b_k+u)}) = \deg(B_{a_{k-1}+u}) + 1,
\]

\[
\deg(B_{c_k+v}) = \deg(B_{2^{k-2}-(a_{k-2}+v)}) + 1.
\]

**Proof.** The results on the integers in $A_k$ and $C_k$ follow from Propositions 21 and 22. The result on the integers in $B_k$ follows from Proposition 24. \qed

**Theorem 27.** Let $k \geq 3$, and let $n \in I_k$. Let $0 \leq v < |I_{k-2}|$, and let $0 \leq u \leq 2^{k-1} - b_k$. Then

\[
\ellc(B_{a_k+v}) = \ellc(B_{a_k-2+v}),
\]

\[
\ellc(B_{b_k+u}) = \ellc(B_{a_{k-1}+u}),
\]

\[
\ellc(B_{2^k-(b_k+u)}) = \ellc(B_{a_{k-1}+u}),
\]

\[
\ellc(B_{c_k+v}) = \ellc(B_{2^{k-2}-(a_{k-2}+v)}) + \ellc(B_{a_{k-2}+v}).
\]

**Proof.** The results on the integers in $A_k$ and $C_k$ follow from Propositions 21 and 22. The result on the integers in $B_k$ follows from Proposition 25. \qed

In [15], Schinzel proved a theorem expressing the leading coefficients of the Stern polynomial of a single integer $n$ in terms of its binary representation. The recursion above, however, may be applied en masse to the Stern polynomials of all the integers in $I_k$, facilitating comparison between them.

7 Optimal BSD representations of integers in $I_k$

We can now apply the weight-distribution theorem to the recursions on Stern polynomials, and derive the number of optimal BSD representations of an integer $n$, along with their Hamming weight.

**Definition 28** (Optimal BSD representations). A BSD representation of $n$ is called optimal if it has same Hamming weight as the reduced NAF representation of $n$. We refer to the number of optimal representations of $n$ as $M(n)$, and to the number of 0s in an optimal representation as $Z(n)$. 

12
Theorem 29. Let \( k \geq 3 \), and let \( n \in I_k \). Let \( 0 \leq v < |I_{k-2}| \), and let \( 0 \leq u \leq 2^{k-1} - b_k \). Then

\[
Z(a_k + v) = Z(a_{k-2} + v) + 1, \\
Z(b_k + u) = Z(a_{k-1} + u) + 1, \\
Z(2^k - (b_k + u)) = Z(a_{k-1} + u) + 1, \\
Z(c_k + v) = Z(2^{k-2} - (a_{k-2} + v)) + 1.
\]

Proof. By Theorem 6, the number of 0s in the NAF-representation of \( n \) is the same as \( \deg(B_{2^k-n}) \). By Lemma 19, \( \deg(B_{2^k-n}) = \deg(B_n) \). The theorem follows by application of these results to Theorem 26, the result on the degree of a Stern polynomial. \( \square \)

Theorem 30. Let \( k \geq 3 \), and let \( n \in I_k \). Let \( 0 \leq v < |I_{k-2}| \), and let \( 0 \leq u \leq 2^{k-1} - b_k \). Then

\[
M(a_k + v) = M(2^{k-2} - (a_{k-2} + v)) + M(a_{k-2} + v), \\
M(b_k + u) = M(2^{k-1} - (a_{k-1} + u)), \\
M(2^k - (b_k + u)) = M(2^{k-1} - (a_{k-1} + u)), \\
M(c_k + v) = M(a_{k-2} + v).
\]

Proof. For the \( M(a_k + v) \) and \( M(c_k + v) \) cases, let \( x \) be as in Lemma 17.

\[
M(a_k + v) = \ell c(B_{2^k-(a_k+v)}) \\
= \ell c(B_{a_k+x}) \\
= \ell c(B_{a_{k-2}+x} + c(B_{2^k-(a_{k-2}+x)})) \\
= \ell c(B_{2^k-(a_{k-2}+v)}) + \ell c(B_{a_{k-2}+v}) \\
= M(a_{k-2} + v) + M(2^{k-2} - (a_{k-2} + v)).
\]

\[
M(c_k + v) = \ell c(B_{2^k-(c_{k}+v)}) \\
= \ell c(B_{a_k+x}) \\
= \ell c(B_{a_{k-2}+x}) \\
= \ell c(B_{2^k-(a_{k-2}+v)}) \\
= M(a_{k-2} + v).
\]
The $M(b_k + u)$ and $M(2^k - (b_k + u))$ cases follow from Theorems 6 and 27.

\[
M(b_k + u) = \ell c(B_{2^k - (b_k + u)}) \\
= \ell c(B_{a_{k-1} + u}) \\
= M(2^{k-1} - (a_{k-1} + u)).
\]

by Theorem 6

\[
M(2^k - (b_k + u)) = \ell c(B_{2^k - (2^k - (b_k + u))}) \\
= \ell c(B_{b_k + u}) \\
= \ell c(B_{a_{k-1} + u}) \\
= M(2^{k-1} - (a_{k-1} + u)).
\]

by Theorem 6

Fig. 2 shows three examples of distributions of the number of optimal representations of integers in $I_k$, for $k = 14, 15$ and 16. Fig. 3 shows the number of 0s in the optimal representations of integers in $I_{16}$. Here in the text, we will discuss Fig. 2, and provide Fig. 3 for comparison.

(a) The number of optimal representations of integers in $I_{15}$. (b) The number of optimal representations of integers in $I_{14}$.

(c) The number of optimal representations of integers in $I_{16}$. The distribution for $I_{14}$ from (b) can be seen to be exactly that of $C_{16}$ here, and the distribution in the second half of $I_{15}$ from (a) can be seen to be exactly that of the second half of $B_{16}$ here.

Figure 2: The number of optimal representations of integers in $I_{14}$, $I_{15}$, and $I_{16}$. 
The $x$-axes represent the integers in $I_k$. These axes are delineated at $a_k$, $b_k$ and $c_k$ and $2^{k} - 1$. In Fig. 2, the $y$ axes represent the number of representations of a given integer $n \in I_k$. The tick marks on the $y$-axes are the Fibonacci numbers, which are the maxima within a NAF-interval. The maxima have value $F_{\lceil \frac{k}{2} \rceil + 1}$ and are reached in $A_k$, as discussed in [5, 6, 13, 18]. Relative maxima can also be seen within subintervals, and these are also Fibonacci numbers.

In general, the distributions of the number of optimal representations in $I_k$ for odd $k$ have similar shapes, as do the distributions for even $k$. One of the differences between odd and even NAF-bitlengths $k$ is that the relative maxima in $B_k$ are $F_{\frac{k}{2}}$ for $k$ even, but are only $F_{\frac{k}{2} - 1}$ for $k$ odd.

The symmetries within $A_k$ and $B_k$ are evident. The $C_k$ are not symmetric, but instead have the same values as $A_{k-2}$, giving a fractal structure in the $C_i$.

The distributions of the leading coefficients of the Stern polynomials $n \in I_k$ are easily obtained from the distributions of the number of optimal representations: by Theorem 6, the Stern polynomial distributions are those of the number of optimal representations, but reflected about the $I_k$-midpoint $x = 2^{k-1}$.

![Figure 3: The number of 0s in the optimal representations of integers in $I_{16}$.](image)

8 Algorithms

We present in this section two algorithms counting the number of $k$-bit optimal BSD representations of integers in $I_k$, and giving the number of 0s in such representations. They calculate for all the integers in $I_k$ recursively, depending on previously calculated values for the integers in $I_{k-1}$ and $I_{k-2}$.

They are quite simple. Algorithm 1 does a copy and an increment for each $n$. Algorithm 2 does only a single copy for three-quarters of the integers in $I_k$ and a two-term sum for the rest of $I_k$. Algorithm 2 is illustrated in Fig 4.

These algorithms are $O(n)$, with $n \in I_k$. They are $O(1)$ on average per integer, but must calculate for all $m < n$. They are embarrassingly parallel within a NAF-interval $I_k$; however, the $i$-loop that calculates each NAF-interval must be performed sequentially, because of the NAF-interval dependency.
The advantage of these algorithms is that they permit comparison between all integers in \( I_k \), since all values for \( I_k \) are calculated in one loop iteration. It is often advantageous to work with integers of a given NAF-bitlength having a relatively large number of optimal representations, or else having optimal representations of relatively small weight. These algorithms allow one to choose between many integers having lengths, weights and optimal representations suited to the needs at hand.

In [6], Grabner and Heuberger gave relations that count the number of optimal representations of an integer \( n \) using transducers. In [15], Schinzel gave a method for calculating the leading coefficients of the Stern polynomial of an integer \( n \), in terms of its binary decomposition. From this, the number of optimal representations of \( n \) may be calculated from application of the weight-distribution Theorem 6.

Both of these are \( O(\log(n)) \) and would be algorithms of choice if one wanted the result for only one \( n \). However, calculating for all \( n \in I_k \), both would be \( O(n \log(n)) \). So if comparison is desired, the \( O(n) \) Algorithm 2 presented below is preferable.

**Algorithm 1** Number of 0s in optimal BSD representations

1: function Zeros-Opt-BSD\((k, Z)\)
2: \( Z[0] \leftarrow 0, Z[1] \leftarrow 0, Z[2] \leftarrow 1, a_{i-2} \leftarrow 0, a_{i-1} \leftarrow 1, a_i \leftarrow 2 \)
3: for \( i \leftarrow 3, k \) do
4: \( a_{i-2} \leftarrow a_{i-1}, a_{i-1} \leftarrow a_i, a_i \leftarrow 2^{i-2} + a_{i-2} \) \hspace{1cm} \( \triangleright \) By Lemma 15
5: \( \text{loop_length} \leftarrow 2^{i-1} - a_i \)
6: \( Z[2^{i-1}] \leftarrow i - 1 \) \hspace{1cm} \( \triangleright \) By Theorem 29
7: for \( j \leftarrow 0, \text{loop_length} - 1 \) do
8: \( Z[a_i + j] \leftarrow Z[a_{i-2} + j] + 1 \)
9: \( Z[2^i - (a_i + j)] \leftarrow Z[a_{i-2} + j] + 1 \)
10: end for
11: end for
12: end function
Algorithm 2 Number of optimal BSD representations

1: function Num-Opt(k, M)
2: \[
M[0] \leftarrow 0, \ M[1] \leftarrow 1, \ M[2] \leftarrow 1, \ a_0 \leftarrow 0, \ a_1 \leftarrow 1, \ a_2 \leftarrow 2
\]
3: for \( i \leftarrow 3, k \) do
4: \[
a_{i-2} \leftarrow a_{i-1}, \ a_{i-1} \leftarrow a_i, \ a_i \leftarrow 2^{i-2} + a_{i-2}
\]
5: if \( i \) is even then
6: \[
ac\_loop\_length \leftarrow a_{i-2} - 1
\]
7: \[
b\_loop\_length \leftarrow a_{i-2}
\]
8: else
9: \[
ac\_loop\_length \leftarrow a_{i-2}
\]
10: \[
b\_loop\_length \leftarrow a_{i-2} - 1
\]
11: end if
12: \[
b_i \leftarrow a_i + ac\_loop\_length
\]
13: \[
c_i \leftarrow 2^{i-1} + a_{i-2}
\]
14: for \( h \leftarrow 0, ac\_loop\_length - 1 \) do
15: \[
M[a_i + h] \leftarrow M[a_{i-2} + h] + M[2^{i-2} - (a_{i-2} + h)]
\]
16: \[
M[c_i + h] \leftarrow M[a_{i-2} + h]
\]
17: end for
18: \[
M[2^{i-1}] \leftarrow 1
\]
19: for \( j \leftarrow 0, b\_loop\_length - 1 \) do
20: \[
M[b_i + j] \leftarrow M[2^{i-1} - (a_{i-1} + j)]
\]
21: \[
M[2^i - (b_i + j)] \leftarrow M[2^{i-1} - (a_{i-1} + j)]
\]
22: end for
23: end for
24: end function
(a) The number of optimal representations of integers in $A_5$ and $C_5$ are calculated in the $h$ loop. In general, the entries from $I_{k-2}$ in order are added to the entries of $I_{k-2}$ in reverse order, and the result is entered into $A_k$. The entries of $I_{k-2}$ are entered into $C_k$ in order.

(b) The number of optimal representations of integers in $B_5$ are calculated in the $j$ loop. In general, the entries from $I_{k-1}$ are entered into the first half of $B_k$ in reverse order, and into the last half of $B_k$ in order. (The reverse ordering is not evident in this small example, because the relevant entries of $I_4$ are palindromic.) The entry for $2^4$ is 1.

Figure 4: An illustration of the $h$ and $j$ loops inside of the $i$ loop in Algorithm 2, showing the calculation of the number of optimal BSD representations of $n \in I_5$. The calculation inside of the $i$ loop is embarrassingly parallel. Every calculation is a copy from $I_3$, or the sum of two entries from $I_3$, or a copy from $I_4$.

9 Acknowledgements

The author wishes to thank the anonymous reviewers of a previous paper for helpful reference suggestions, and Andrew Alexander, Matthew Broussard, Vanessa Job and Nathan Kodama for much discussion.

References

[1] Avizienis, A.: Signed-digit number representations for fast parallel arithmetic. IRE Trans. Comput. **EC-10**(3), 389–400 (1961)
[2] Booth, A.D.: A Signed Binary Multiplication Technique. Quart. J. Mech. Appl. Math. 4(2), 236–240 (1951). DOI 10.1093/qjmam/4.2.236. URL https://doi.org/10.1093/qjmam/4.2.236

[3] Dilcher, K., Tomkins, H.: Square classes and divisibility properties of Stern polynomials. Integers 18 (2018)

[4] Eğecioğlu, Ö., Koç, Ç.K.: Fast modular exponentiation. Proceedings of 1990 Bilkent International Conference on New Trends in Communication, Control, and Signal Processing 1, 188–194 (1990)

[5] Ganesan, P., Manku, G.S.: Optimal routing in Chord. In: ACM SIAM Symposium on Discrete Algorithms (SODA 2004) (2004). URL http://ilpubs.stanford.edu:8090/640/

[6] Grabner, P., Heuberger, C.: On the number of optimal base 2 representations of integers. Des. Codes Cryptogr. 40, 25–39 (2006). DOI 10.1007/s10623-005-6158-y

[7] Klavžar, S., Milutinović, U., Petr, C.: Stern polynomials. Adv. in Appl. Math. 39(1), 86 – 95 (2007). DOI https://doi.org/10.1016/j.aam.2006.01.003. URL http://www.sciencedirect.com/science/article/pii/S0196885806000807

[8] Koblitz, N.: CM-curves with good cryptographic properties. In: Advances in Cryptology—CRYPTO ’91 (Santa Barbara, CA, 1991), Lecture Notes in Comput. Sci., vol. 576, pp. 279–287. Springer, Berlin (1992). DOI 10.1007/3-540-46766-1_22. URL https://doi.org/10.1007/3-540-46766-1_22

[9] Monroe, L.: Binary signed-digit integers and the Stern diatomic sequence. https://arxiv.org/abs/2108.11495 (to appear in Designs, Codes and Cryptography)

[10] Morain, F., Olivos, J.: Speeding up the computations on an elliptic curve using addition-subtraction chains. RAIRO Theor. Inform. Appl. 24, 531–544 (1990). DOI 10.1051/ita/1990240605311

[11] Reitwiesner, G.W.: Binary Arithmetic, Advances in Computers, vol. 1, pp. 231 – 308. Elsevier (1960). DOI https://doi.org/10.1016/S0065-2458(08)60610-5. URL http://www.sciencedirect.com/science/article/pii/S0065245808606105

[12] Reznick, B.: Some binary partition functions. In: Analytic Number Theory, Progress in Mathematics, vol. 85, pp. 451–477. Birkhauer Boston (1990). DOI 10.1007/978-1-4612-3464-7_29. URL http://dx.doi.org/10.1007/978-1-4612-3464-7_29

[13] Sawada, J.: A simple Gray code to list all minimal signed binary representations. SIAM J. Discrete Math. 21(1), 16–25 (2007). DOI 10.1137/050641405. URL https://doi.org/10.1137/050641405
[14] Schinzel, A.: On the factors of Stern polynomials: Remarks on the preceding paper of M. Ulas. Publicationes Mathematicae 79 (2011). DOI 10.5486/PMD.2011.5110

[15] Schinzel, A.: The leading coefficients of Stern polynomials. In: From Arithmetic to Zeta-Functions: Number Theory in Memory of Wolfgang Schwarz, pp. 427–434. Springer International Publishing (2016). DOI 10.1007/978-3-319-28203-9_25. URL https://doi.org/10.1007/978-3-319-28203-9_25

[16] Shallit, J.: A primer on balanced binary representations. http://cs.uwaterloo.ca/~shallit/Papers/bbr.pdf (1992)

[17] Shannon, C.E.: A symmetrical notation for numbers. Amer. Math. Monthly 57(2), pp. 90–93 (1950). URL http://www.jstor.org/stable/2304993

[18] Tůma, J., Vábek, J.: On the number of binary signed digit representations of a given weight. Commentationes Mathematicae Universitatis Carolinae 56(3), 287–306 (2015). DOI 10.14712/1213-7243.2015.129

[19] Ulas, M.: Arithmetic properties of the sequence of degrees of Stern polynomials and related results. Int. J. Number Theory 8, 669–687 (2012). DOI 10.1142/S1793042112500388

[20] Ulas, M., Ulas, O.: On certain arithmetic properties of Stern polynomials. Publ. Math. Debrecen 79(1-2), 55–81 (2011)