Commentationes Mathematicae Universitatis Carolinae

Jiří Tůma; Jiří Vábek

On the number of binary signed digit representations of a given weight

Commentationes Mathematicae Universitatis Carolinae, Vol. 56 (2015), No. 3, 287–306

Persistent URL: `http://dml.cz/dmlcz/144345`

On the number of binary signed digit representations of a given weight

Jiří Tůma, Jiří Vábek

Abstract. Binary signed digit representations (BSDR's) of integers have been studied since the 1950's. Their study was originally motivated by multiplication and division algorithms for integers and later by arithmetics on elliptic curves. Our paper is motivated by differential cryptanalysis of hash functions. We give an upper bound for the number of BSDR's of a given weight. Our result improves the upper bound on the number of BSDR's with minimal weight stated by Grabner and Heuberger in *On the number of optimal base* 2 *representations*, Des. Codes Cryptogr. **40** (2006), 25–39, and introduce a new recursive upper bound for the number of BSDR's of any given weight.

Keywords: binary signed digit representation; NAF; minimal weight

Classification: 11A63, 68R01

1. Introduction

Binary Signed Digit Representations (BSDR's) of integers were introduced in 1950's in connection with multiplication and division algorithms for integers, particularly by Booth in [1]. Later, BSDR's were studied by Reitwiesner in [2]. In particular, he proved that each integer has a special BSDR called *Non-Adjacent Form* (NAF) that is unique and minimal with respect to the number of non-zero digits in the representation.

BSDR's of minimal weight were also studied in connection with public-key cryptography based on elliptic curves. They helped to speed up algorithms for calculating products nP for a natural number n and a point P on an elliptic curve, see e.g. [3], [4], [5], [11], [17]. It also motivated a generalization of BSDR's of integers using different digits and bases, see e.g. [12], [20].

Other authors applied BSDR's to evaluate resistance of elliptic curve cryptosystems against differential power analysis. They gave upper bounds for the number of BSDR's of a given integer and designed algorithms to generate them, see e.g. [7], [8], [9], [16].

In 2004, Heuberger characterized BSDR's of minimal weight in [10] and in 2006, Grabner and Heuberger proved an upper bound for the number of BSDR's of minimal weight of any given integer z in [14]. In 2010, the upper bound was

DOI 10.14712/1213-7243.2015.129

The first author was supported by GACR 201/09/0816.

improved by Wu et al in [19], their upper bound depended on the length of NAF(z).

Our improved upper bound for the number of BSDR's of minimal weight of z depends on the number of non-zero digits of NAF(z). We further state a recursive formula for the number of BSDR's of any given (not only minimal) weight for any integer z.

Our research is motivated by Stevens' heuristic search algorithm for finding differential paths in the hash function MD5 as described in [15]. We applied the new upper bounds to optimize our implementation of Stevens' algorithm that found a new type of collisions for MD5, see [18].

2. Preliminaries

In this paper we study binary signed digit representations of integers. For us a *signed digit* is a number from the set $D = \{-1, 0, 1\}$.

Definition 2.1. A Binary Signed Digit Representation (BSDR) of an integer $z \in \mathbb{Z}$ is a string

$$\beta = b_{l-1} \ldots b_1 b_0$$

of elements of D such that

$$\sum_{i=0}^{l-1} b_i 2^i = z.$$

We will also use notation

$$(\beta)_2 = \sum_{i=0}^{l-1} b_i 2^i,$$

especially in the cases when concrete values of digits b_i are not important.

First some terminology. The set of strings of elements of D will be denoted by D^*, the empty string by ϵ. The *concatenation* of two strings $\beta, \gamma \in D^*$ will be denoted by $\beta\gamma$. For any string $\beta \in D^*$ and $k \geq 1$ we define $\beta^k = \beta\beta^{k-1}$, and set $\beta^0 = \epsilon$.

We define the *length* $l(\beta)$ of a string $\beta = b_{l-1} \ldots b_1 b_0 \in D^*$ as l.

The *weight* $w(\beta)$ is defined as the number of nonzero elements of β, i.e.

$$w(\beta) = \sum_{i=0}^{l-1} |b_i|.$$

Obviously $w(\beta\gamma) = w(\beta) + w(\gamma)$ for any $\beta, \gamma \in D^*$.

A string $\beta = b_{l-1} \ldots b_1 b_0 \in D^*$ is called *reduced* if $b_{l-1} \neq 0$. The empty string ϵ is reduced by definition.

A string $\beta = b_{l-1} \ldots b_1 b_0$ is called *Non-Adjacent Form* (NAF) if the product of integers $b_{i+1} b_i = 0$ for any $i = 0, \ldots, l-2$. Again ϵ is NAF by definition.

If β is a NAF of weight n, then it can be uniquely written in the form

$$\beta = 0^{l_n} c_n 0^{l_{n-1}} c_{n-1} \cdots c_2 0^{l_1} c_1 0^{l_0}, \tag{2.1}$$

where $c_i = \pm 1$ for each $i = 1, 2, \ldots, n$.

Reitwiesner [2] proved that a reduced NAF exists for every $z \in \mathbb{Z}$, is uniquely determined by z and with minimal weight among all BSDR's of z. In this paper we will denote it by NAF (z). He also gave an algorithm how to construct NAF (z) from the unique standard binary representation (i.e. using only digits 0,1) of z.

Any NAF of z possibly differs from NAF (z) by some leading zeroes and can be written as

$$0^m \,\mathrm{NAF}\,(z) \quad \text{for some} \quad m \geq 0. \tag{2.2}$$

In [13] Heuberger and Prodinger presented a transducer δ that transforms any BSDR of an integer into one of its NAF's.

We will use the following slightly modified version δ_0 of their transducer δ.

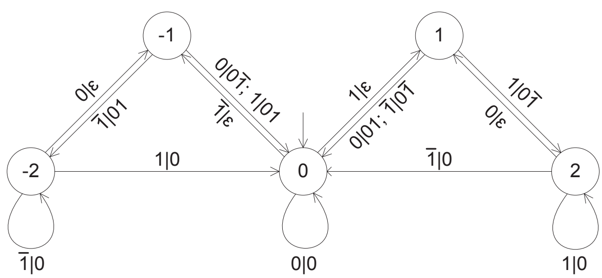

FIGURE 1. The transducer δ_0

Formally, the transducer δ_0 is a mapping

$$\delta_0 : Q \times D \to Q \times D^*,$$

where $Q = \{-2, -1, 0, 1, 2\}$ is the *set of states* of δ_0, the state 0 is the *initial state* of δ_0. Each particular instance of the mapping δ_0

$$\delta_0(q, \iota) = (s, \eta)$$

is called a *transition* of δ_0. In the picture, the transitions are depicted as arrows

$$q \xrightarrow{\iota|\eta} s,$$

$\iota \in D$ is the *input* of the transition and $\eta \in D^*$ is the *output* of it. We also use the usual convention that $\overline{1}$ denotes -1.

A state $q_0 \in Q$ and an input string $\beta = \beta_{l-1} \dots \beta_1 \beta_0$, determine a unique sequence of transitions, shortly called a *path*, in δ_0

$$q_0 \xrightarrow{\beta_0|\eta_0} q_1 \xrightarrow{\beta_1|\eta_1} \dots \xrightarrow{\beta_{l-2}|\eta_{l-2}} q_{l-1} \xrightarrow{\beta_{l-1}|\eta_{l-1}} q_l.$$

We will denote the path by $p(q_0, \beta)$ and call q_0 the *initial state* of the path and the state q_l the *terminal state* of the path. The string β is the *input* of the path $p(q_0, \beta)$ and the concatenation

$$\eta = \eta_{l-1}\eta_{l-2} \dots \eta_1 \eta_0$$

of the output of the individual transitions in the path is its *output*.

Since the terminal state q_l and the output η of the path $p(q_0, \beta)$ are uniquely determined by the initial state q_0 and the input β, we can extend the original mapping $\delta_0 : Q \times D \to Q \times D^*$ to a mapping

$$\delta_0^* : Q \times D^* \to Q \times D^*$$

by defining

$$\delta_0^*(q_0, \beta) = (q_l, \eta)$$

where q_l is the terminal vertex of the path $p(q_0, \beta)$ and η is its output.

Note that each nonzero digit in the output of any transition in δ_0 is immediately followed by the digit 0, so the output of any path in δ_0 is a NAF.

Again, we will sometimes simplify notation and write paths in δ_0 as

$$p = e_0 e_1 \cdots e_{l-1},$$

especially when the concrete form of transitions e_i are not important. We denote by $\mu(p)$ the initial state of p and by $\nu(p)$ the terminal state of p. We also denote $\iota(p)$ the input string of p and $\eta(p)$ the output of p.

We will also use the following straightforward lemma that is valid for any transducer, not just for δ_0.

Lemma 2.2. *If p_1 and p_2 are paths in δ_0 and $\nu(p_1) = \mu(p_2)$, then $p_1 p_2$ is also a path in δ_0 and its output $\eta(p_1 p_2) = \eta(p_2)\eta(p_1)$.*

If $\delta_0^*(q, \beta) = (r, \eta)$ and $\delta_0^*(r, \gamma) = (s, \xi)$, then $\delta_0^*(q, \gamma\beta) = (s, \xi\eta)$.

The following lemma was originally stated for the transducer δ in [13] and translates directly to the transducer δ_0.

Lemma 2.3. *If $\beta = b_{l-1} \dots b_0 \in D^*$ is a* BSDR *of z and $p = p(0, \beta)$ has terminal state $q = \nu(p)$ and output $\eta = \eta(p)$, then*

$$(\beta)_2 = 2^{l-1} q + (\eta)_2.$$

In particular, η is a NAF of z if and only if $q = 0$.

One can easily see that for any given NAF η and the initial and terminal states $q, r \in Q$, there are only finitely many input strings β such that

$$\delta_0^*(q, \beta) = (r, \eta)\,.$$

It follows for example from the fact that there are no two subsequent transitions with output ϵ in any path in δ_0. This can be seen by inspection of δ_0. Only transitions with an odd terminal state have output ϵ and there are no transitions with both initial and terminal states odd.

We are interested in the number of reduced BSDR's of an integer z with a given weight. Since $\mathrm{NAF}(z)$ has minimal weight among all BSDR's of z, any BSDR β of z has weight $w(\beta) = w(\mathrm{NAF}(z)) + j$ for some $j \in \mathbb{N}$.

Definition 2.4. For a BSDR β of z, the difference $j = w(\beta) - w(\mathrm{NAF}(z))$ is called the *overweight* of β and denoted by $\mathrm{ow}(\beta)$. The BSDR's β of z with overweight 0 are called *optimal* (BSDR's of z).

For any z and $j \in \mathbb{N}$ we denote

$$\mathcal{B}(z, j) = \{\, \beta \in D^*;\ \beta \text{ is a reduced BSDR of } z \ \text{ and } \ \mathrm{ow}(\beta) = j \,\}\,. \tag{2.3}$$

Our aim is to give an upper bound on the cardinality of the sets $\mathcal{B}(z, j)$.

3. Overweights

We want to use the transducer δ_0 to check if a given $\beta \in D^*$ is a BSDR of an integer z by checking if the output of $p(0, \beta)$ is a NAF of z. However, by Lemma 2.3 this happens if and only if the terminal state of $p(0, \beta)$ is 0, i.e. if and only if $\delta_0^*(0, \beta) = (0, \eta)$ for a NAF η of z.

So if necessary, we need to add to a $\beta \in \mathcal{B}(z, j)$ a number of leading zeroes to get an input $0^m\beta$ such that the path $p(0, 0^m\beta)$ has terminal state 0, or equivalently $\delta_0^*(0, 0^m\beta) = (0, \eta)$. This can be done in a straightforward minimal way by the following lemma.

Lemma 3.1. *For every state $q \in Q$, the terminal state of the path $p(q, 0^{|q|})$ is 0.*

If $\beta \in \mathcal{B}(z, j)$ and the path $p(0, \beta)$ has terminal state q, then the path $p(0, 0^{|q|}\beta)$ has terminal state 0 and outputs a NAF of z.

Proof: The first claim is directly checked from the definition of δ_0. Hence the terminal state of $p(0, 0^{|q|}\beta)$ is 0, by Lemma 2.2. By Lemma 2.3 we get that the value of the output of $p(0, 0^{|q|}\beta)$ is

$$(0^{|q|}\beta)_2 = (\beta)_2 = z.$$

Finally, the output of any path in δ_0 is a NAF. $\square$

In what follows we show that the overweight of a BSDR β of z can be calculated from the path $p(0, \beta)$.

Definition 3.2. We define the *weight of a transition* $e = q \xrightarrow{b|\eta} s$ as

$$w(e) = w(b) - w(\eta).$$

For a path $p = e_0 \dots e_{l-1}$ we define the *weight of the path* p as

$$w(p) = \sum_{i=0}^{l-1} w(e_i).$$

Lemma 3.3. *For a path $p = e_0 \dots e_{l-1}$ with the input string $\iota(p) = \beta$ and the output string $\eta(p) = \eta$,*

$$w(p) = w(\beta) - w(\eta).$$

Proof: We have

$$\begin{aligned} w(p) &= \sum_{i=0}^{l-1} w(e_i) = \sum_{i=0}^{l-1} (w(\iota(e_i)) - w(\eta(e_i))) \\ &= \sum_{i=0}^{l-1} w(\iota(e_i)) - \sum_{i=0}^{l-1} w(\eta(e_i)) = w(\beta) - w(\eta). \end{aligned}$$

□

Definition 3.4. For a state $q \in Q$ we define the *potential of the state* q as

$$\pi(q) = \min\{w(p);\ p \text{ a path in } \delta_0,\ \mu(p) = 0,\ \nu(p) = q\}.$$

The potential of a state q is the lowest weight among all paths from the initial state 0 to q.

Lemma 3.5. *In the transducer δ_0,*

$$\pi(0) = 0 \text{ and } \pi(1) = \pi(-1) = \pi(2) = \pi(-2) = 1.$$

Proof: Partition the states of δ_0 into two blocks $\{0\}$ and $\{1, -1, 2, -2\}$.

We directly check that $\pi(0) \le 0$ and $\pi(q) \le 1$ for $q \ne 0$. The only transitions with negative weight are

$$1 \xrightarrow{0|01} 0 \text{ and } -1 \xrightarrow{0|0\bar{1}} 0,$$

both with weight -1. All other transitions of δ_0 have non-negative weight. In particular the transitions $0 \xrightarrow{b|\epsilon} b$ with $b \ne 0$ have weight 1.

Thus whenever our path p leaves the block $\{0\}$, its weight increases by 1. It can only increase when we use transitions with both initial and terminal states in $\{1, -1, 2, -2\}$ and it decreases by at most one when it reaches the state 0 again. Thus the weight of any path from 0 to 0 is at least 0 and the weight of any path from 0 to a state of $\{1, -1, 2, -2\}$ is at least 1 as claimed. □

Definition 3.6. We define the *overweight of a transition* $e = q \xrightarrow{b|\eta} s$ by

$$\operatorname{ow}(e) = \pi(q) - \pi(s) + w(e).$$

We define the *overweight of a path* $p = e_0 \dots e_{l-1}$ as

$$\operatorname{ow}(p) = \sum_{i=0}^{l-1} \operatorname{ow}(e_i).$$

We directly check that each transition of δ_0 has non-negative overweight and that the set of transitions of δ_0 with positive overweight is

$$\Delta_{\mathrm{ow}} = \{1 \xrightarrow{\bar{1}|0\bar{1}} 0,\ -1 \xrightarrow{1|01} 0,\ 2 \xrightarrow{1|0} 2,\ 2 \xrightarrow{\bar{1}|0} 0,\ -2 \xrightarrow{1|0} 0,\ -2 \xrightarrow{\bar{1}|0} -2\}. \tag{3.1}$$

The transitions $2 \xrightarrow{\bar{1}|0} 0$, $-2 \xrightarrow{1|0} 0$ have overweight 2, the remaining four have overweight 1.

Lemma 3.7. *For a path $p = e_0 \dots e_{l-1}$, where $e_i = q_i \xrightarrow{b_i|\eta_i} q_{i+1}$ for $i = 0, 1, \dots, l-1$ with input string $\beta = b_{l-1} \dots b_1 b_0$ and output string $\eta = \eta_{l-1} \dots \eta_1 \eta_0$*

$$\operatorname{ow}(p) = \pi(q_0) - \pi(q_l) + w(p).$$

In particular, if $q_0 = q_l = 0$, then $\operatorname{ow}(p) = w(p) = w(\beta) - w(\eta) = \operatorname{ow}(\beta)$.

Proof: We have

$$\begin{aligned}
\operatorname{ow}(p) &= \sum_{i=0}^{l-1} \operatorname{ow}(e_i) = \sum_{i=0}^{l-1} (\pi(q_i) - \pi(q_{i+1}) + w(\iota(e_i)) - w(\eta(e_i))) \\
&= \pi(q_0) - \pi(q_l) + \sum_{i=0}^{l-1} w(\iota(e_i)) - \sum_{i=0}^{l-1} w(\eta(e_i)) \\
&= \pi(q_0) - \pi(q_l) + w(\beta) - w(\eta) = \pi(q_0) - \pi(q_l) + w(p).
\end{aligned}$$

By Lemma 3.5 and by the first claim we obtain $\operatorname{ow}(p) = w(p)$. By Lemma 3.3 we get $w(p) = w(\beta) - w(\eta)$. Since $(\beta)_2 = (\eta)_2 = z$ for an integer z by Lemma 2.3 and the fact that η is a NAF of z, we obtain $\operatorname{ow}(p) = w(\beta) - w(\eta) = \operatorname{ow}(\beta)$. $\square$

The second claim of previous lemma is the basis of our approach. For a NAF η, an integer $j \in \mathbb{Z}$ and states $q, s \in Q$ we consider the set

$$A_{q,s}(\eta, j) = \{p;\ p \text{ a path in } \delta_0,\ \mu(p) = q,\ \nu(p) = s,\ \ \eta(p) = \eta,\ \operatorname{ow}(p) = j\}.$$

We already know that the set $A_{q,s}(\eta, j)$ is always finite. Its cardinality will be denoted by

$$a_{q,s}(\eta, j) = |A_{q,s}(\eta, j)|.$$

Since each path has a non-negative overweight, the sets $A_{q,s}(\eta, j)$ are empty for $j < 0$, hence $a_{q,s}(\eta, j) = 0$ whenever $j < 0$.

There is a number of relations between the numbers $a_{q,s}(\eta, j)$. The following lemma contains a list of those that will be used later in the proof.

Lemma 3.8. *For each Non-Adjacent Form η and an integer $j \in \mathbb{Z}$, the following holds*

$$
\begin{array}{lrcl}
(3.2) & a_{0,0}(\eta 0, 0) & = & a_{0,0}(\eta, 0), \\
(3.3) & a_{\pm 1,0}(\eta 0, 0) & = & 0, \\
(3.4) & a_{0,0}(\eta 01, 0) & = & a_{1,0}(\eta 01, 0) + a_{-1,0}(\eta 01, 0), \\
(3.5) & a_{1,0}(\eta 01, 0) & = & a_{0,0}(\eta, 0), \\
(3.6) & a_{0,0}(\eta 0\overline{1}, 0) & = & a_{1,0}(\eta 0\overline{1}, 0) + a_{-1,0}(\eta 0\overline{1}, 0), \\
(3.7) & a_{1,0}(\eta 0\overline{1}, 0) & = & a_{2,0}(\eta, 0), \\
(3.8) & a_{2,0}(\eta, 0) & = & a_{1,0}(\eta, 0), \\
(3.9) & a_{-1,0}(\eta 01, 0) & = & a_{-2,0}(\eta, 0), \\
(3.10) & a_{-1,0}(\eta 0\overline{1}, 0) & = & a_{0,0}(\eta, 0), \\
(3.11) & a_{-2,0}(\eta, 0) & = & a_{-1,0}(\eta, 0), \\
(3.12) & a_{1,0}(\eta 0\overline{1}, 0) & = & a_{1,0}(\eta, 0), \\
(3.13) & a_{-1,0}(\eta 01, 0) & = & a_{-1,0}(\eta, 0), \\
(3.14) & a_{0,0}(\eta 01, 0) & = & a_{0,0}(\eta, 0) + a_{-1,0}(\eta, 0), \\
(3.15) & a_{0,0}(\eta 0\overline{1}, 0) & = & a_{0,0}(\eta, 0) + a_{1,0}(\eta, 0), \\
(3.16) & a_{0,-1}(\eta, 0) & = & a_{0,0}(0\overline{1}\eta, 0), \\
(3.17) & a_{0,1}(\eta, 0) & = & a_{0,0}(01\eta, 0), \\
(3.18) & a_{0,0}(\eta 01, j) & = & a_{0,0}(\eta, j) + a_{-2,0}(\eta, j) + a_{0,0}(\eta, j-1), \\
(3.19) & a_{0,0}(\eta 0\overline{1}, j) & = & a_{0,0}(\eta, j) + a_{2,0}(\eta, j) + a_{0,0}(\eta, j-1).
\end{array}
$$

PROOF: We prove only a few of the relations, the others can be proved in a similar way.

To prove (3.2), observe that for any path $p \in A_{0,0}(\eta 0, 0)$, the first transition of p must be $0 \xrightarrow{0|0} 0$. Hence

$$p' \mapsto (0 \xrightarrow{0|0} 0)\, p'$$

is a bijection between $A_{0,0}(\eta, 0)$ and $A_{0,0}(\eta 0, 0)$, which proves (3.2).

To prove (3.4), observe that for each path $p \in A_{0,0}(\eta 01, 0)$ the first transition of p is either $0 \xrightarrow{1|\epsilon} 1$ or $0 \xrightarrow{\overline{1}|\epsilon} -1$. The transition $0 \xrightarrow{1|\epsilon} 1$ is then followed by a path from 1 to 0 with output $\eta 01$, the transition $0 \xrightarrow{\overline{1}|\epsilon} -1$ is followed by a path from -1 to 0 with the same output $\eta 01$. Hence

$$|A_{0,0}(\eta 01, 0)| = |A_{1,0}(\eta 01, 0)| + |A_{-1,0}(\eta 01, 0)|,$$

thus proving (3.4).

To prove (3.3) it is enough to observe that there is no transition in δ with the initial state ± 1 and output 0.

Using (3.8) and (3.7) we get immediately (3.12), while (3.11) and (3.9) give (3.13).

Similarly, using (3.4), (3.5) and (3.13) we get (3.14) and symmetrically also (3.15).

To prove (3.16) (and symmetrically (3.17)) observe that for a path $p \in A_{0,0}(0\overline{1}\eta, 0)$ the last transition of p must be $-1 \xrightarrow{0|0\overline{1}} 0$. Hence

$$p' \mapsto p'\,(-1 \xrightarrow{0|0\overline{1}} 0)$$

is a bijection between $A_{0,-1}(\eta, 0)$ and $A_{0,0}(0\overline{1}\eta, 0)$, which proves (3.17).

To prove (3.18) we first observe that the proof of (3.4) also proves $a_{0,0}(\eta 01, j) = a_{1,0}(\eta 01, j) + a_{-1,0}(\eta 01, j)$. In any path of $A_{1,0}(\eta 01, j)$ the first transition $1 \xrightarrow{0|01} 0$ of overweight 0 is followed by a path from 0 to 0 with output η and overweight j, hence $a_{1,0}(\eta 01, j) = a_{0,0}(\eta, j)$. In any path of $A_{-1,0}(\eta 01, j)$, the first transition is either $-1 \xrightarrow{1|01} 0$ of overweight 1 followed by a path from $A_{0,0}(\eta, j-1)$ or $-1 \xrightarrow{\overline{1}|01} -2$ of overweight 0 followed by a path of $A_{2,0}(\eta, j)$. Hence

$$\begin{aligned} a_{0,0}(\eta 01, j) &= a_{1,0}(\eta 01, j) + a_{-1,0}(\eta 01, j) \\ &= a_{0,0}(\eta, j) + a_{0,0}(\eta, j-1) + a_{2,0}(\eta, j), \end{aligned}$$

thus proving (3.18). The equation (3.19) is proved symmetrically. □

4. A bound for the number of optimal BSDR's

In this section we give an upper bound for the number of optimal reduced BSDR's of any integer z. All paths considered in this section have overweight 0, so all transitions belong to the set

$$\delta_0 \setminus \Delta_{\mathrm{ow}}\,.$$

These transitions are shown in Figure 2.

To simplify notation, in this section we write $A_{q,s}(\eta)$ for $A_{q,s}(\eta, 0)$ and $a_{q,s}(\eta)$ for $a_{q,s}(\eta, 0)$.

The next theorem gives an upper bound for numbers $a_{0,0}(\eta)$ depending on the weight $w(\eta)$. The upper bound uses Fibonacci numbers defined by the recurrence

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n \quad \text{for} \quad n \geq 0\,.$$

Theorem 4.1. *For every Non-Adjacent Form η we have*

$$a_{0,0}(\eta) \leq F_{w(\eta)+1}\,.$$

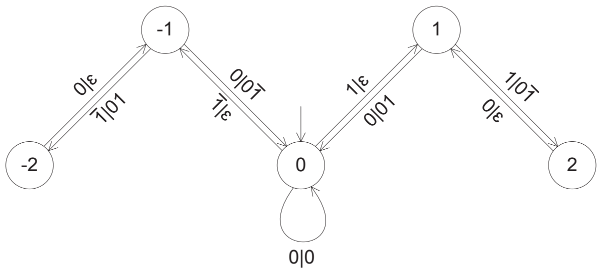

FIGURE 2. Transitions of δ_0 with overweight 0

The equality holds if and only if

$$l_n \geq 1 = l_{n-1} = \cdots = l_1 = 1, \text{ and } c_i c_{i+1} = -1 \text{ for each } i \neq n-2\,. \tag{4.1}$$

PROOF: First we prove the upper bound. We proceed by induction on $w(\eta)$ and prove not only that for every Non-Adjacent Form η

$$a_{0,0}(\eta) \leq F_{w(\eta)+1}, \quad \text{but also} \quad a_{\pm 1,0}(\eta) \leq F_{w(\eta)}\,.$$

If $w(\eta) = 0$, then $\eta = 0^{l_0}$ for some l_0. By repeated application of (3.2) we get $a_{0,0}(0^{l_0}) = a_{0,0}(\epsilon)$. Since the only path in $A_{0,0}(\epsilon)$ is the empty path, we get

$$a_{0,0}(0^{l_0}) = 1 = F_1 \quad \text{for any} \quad l_0 \in \mathbb{N}\,.$$

Moreover, by (3.3), $a_{\pm 1,0}(0^{l_0}) = 0 = F_0$.

Now suppose that $w(\eta) = n > 0$. The induction hypothesis is that $a_{0,0}(\eta') \leq F_{w(\eta')+1}$ and $a_{\pm 1,0}(\eta') \leq F_{w(\eta')}$ for any Non-Adjacent Form η' with $w(\eta') < n$.

To prove the induction step we deal with the case $w(\eta) = 1$ separately. In this case $\eta = 0^{l_1} c 0^{l_0}$ for some $l_0, l_1 \in \mathbb{N}$ and $c = \pm 1$. We consider only the case $c = 1$, the case $c = \overline{1}$ is symmetric.

Then by (3.2), (3.4), (3.13) and by (3.5),

$$\begin{aligned} a_{0,0}(0^{l_1} 1 0^{l_0}) &= a_{0,0}(0^{l_1} 1) = a_{-1,0}(0^{l_1} 1) + a_{1,0}(0^{l_1} 1) \\ &= \begin{cases} 0 + 0 < F_1, & \text{if } l_1 = 0\,, \\ a_{-1,0}(0^{l_1 - 1}) + a_{0,0}(0^{l_1 - 1}) = 0 + 1 = F_2, & \text{if } l_1 > 0\,. \end{cases} \end{aligned}$$

Moreover,

$$a_{1,0}(0^{l_1} 1 0^{l_0}) = \begin{cases} 0 < F_1, & \text{if } l_0 > 0 \text{ or } l_1 = 0\,, \\ a_{0,0}(0^{l_1 - 1}) = 1 = F_1, & \text{if } l_0 = 0 \text{ and } l_1 > 0\,, \end{cases}$$

and

$$a_{-1,0}(0^{l_1}10^{l_0}) = \begin{cases} 0 < F_1, & \text{if } \ l_0 > 0 \ \text{ or } \ l_1 = 0\,, \\ a_{-1,0}(0^{l_1-1}) = 0 < F_1, & \text{if } \ l_0 = 0 \ \text{ and } \ l_1 > 0\,. \end{cases}$$

Now suppose that $w(\eta) = n \geq 2$ and write $\eta = \eta' 0 c_1 0^{l_0}$. Again we consider only the case $c_1 = 1$. By (3.2) and (3.14) we get

$$a_{0,0}(\eta) = a_{0,0}(\eta' 010^{l_0}) = a_{0,0}(\eta' 01) = a_{0,0}(\eta') + a_{-1,0}(\eta')\,, \tag{4.2}$$

and by the induction hypothesis we obtain

$$a_{0,0}(\eta) = a_{0,0}(\eta') + a_{-1,0}(\eta') \leq F_n + F_{n-1} = F_{n+1}\,. \tag{4.3}$$

This verifies the induction step for the inequality $a_{0,0}(\eta) \leq F_{w(\eta)+1}$. Moreover, we also get

$$a_{0,0}(\eta) = F_{n+1} \ \text{ if and only if } \ a_{0,0}(\eta') = F_n \ \text{ and } \ a_{-1,0}(\eta') = F_{n-1}\,. \tag{4.4}$$

To complete the proof of upper bounds it remains to prove the induction step also for the inequalities $a_{\pm 1,0}(\eta) \leq F_{w(\eta)}$ in case $w(\eta) \geq 2$. We have

$$a_{1,0}(\eta) = a_{1,0}(\eta' 010^{l_0}) = \begin{cases} 0 < F_n, & \text{if } \ l_0 > 0 \ \text{ by (3.3)}\,, \\ a_{1,0}(\eta' 01) = a_{0,0}(\eta') \leq F_n, & \text{if } \ l_0 = 0 \ \text{ by (3.5)}\,, \end{cases}$$

by the induction hypothesis. We also obtain

$$a_{1,0}(\eta) = F_n \ \text{ if and only if } \ l_0 = 0 \ \text{ and } \ a_{0,0}(\eta') = F_n\,. \tag{4.5}$$

And finally, by another application of the induction hypothesis we get

$$a_{-1,0}(\eta) = a_{-1,0}(\eta' 010^{l_0}) = \begin{cases} 0 < F_n, & \text{if } l_0 > 0 \text{ by (3.3)}, \\ a_{-1,0}(\eta' 01) = a_{-1,0}(\eta') \leq F_{n-1}, & \text{if } l_0 = 0 \text{ by (3.13)}. \end{cases}$$

This completes the proof of the upper bound $a_{0,0}(\eta) \leq F_{w(\eta)+1}$. As for the equality, we obtain

$$a_{-1,0}(\eta) = F_n \ \text{ if and only if } \ l_0 = 0 \ \text{ and } \ a_{-1,0}(\eta') = F_{n-1} = F_n\,. \tag{4.6}$$

To characterize those η for which the equality $a_{0,0}(\eta) = F_{w(\eta)+1}$ holds, we again proceed by induction on $w(\eta)$ and prove also that for

$$\eta = 0^{l_n} c_n 0^{l_{n-1}} c_{n-1} \cdots c_2 0^{l_1} c_1 0^{l_0}$$

the equality $a_{1,0}(\eta) = F_{w(\eta)}$ holds if and only if either $w(\eta) = 0$, or $\eta = 0^{l_2}10\overline{1}$ with $l_2 > 0$, or η satisfies

$$l_n \geq l_{n-1} = \cdots = l_2 = 1, \quad l_0 = 0\,, \tag{4.7}$$

$$c_1 = 1, \quad \text{and} \quad c_i c_{i+1} = -1 \quad \text{for each} \quad i \neq 1, n-2\,. \tag{4.8}$$

And symmetrically, the equality $a_{-1,0}(\eta) = F_{w(\eta)}$ holds if and only if either $w(\eta) = 0$, or $\eta = 0^{l_2}\overline{1}01$ with $l_2 > 0$, or η satisfies

$$l_n \geq l_{n-1} = \cdots = l_2 = 1, \quad l_0 = 0\,, \tag{4.9}$$

$$c_1 = \overline{1}, \quad \text{and} \quad c_i c_{i+1} = -1 \quad \text{for each} \quad i \neq 1, n-2\,. \tag{4.10}$$

We have already checked the cases $w(\eta) \leq 1$ when proving the upper bounds.

Now suppose that $w(\eta) = n > 1$ and assume by induction that for any η' such that $w(\eta') < n$ the equalities $a_{0,0}(\eta') = F_{w(\eta')+1}$ and $a_{\pm 1,0}(\eta') = F_{w(\eta')}$ hold if and only if η' is in one of the corresponding lists of NAF's.

We write again $\eta = \eta' 0 c_1 0^{l_0}$ for some $l_0 \in \mathbb{N}$ and $c_1 = \pm 1$. Thus we have $\eta' = 0^{l_n} c_n 0^{l_{n-1}} c_{n-1} \cdots c_2 0^{l_1 - 1}$. Because of symmetry we consider only the case $c_1 = 1$.

By (4.4) we know that $a_{0,0}(\eta) = F_{n+1}$ if and only if $a_{0,0}(\eta') = F_n$ and $a_{-1,0}(\eta') = F_{n-1}$.

Using the induction hypothesis (and the fact that $w(\eta') = n - 1 > 0$) we get that $a_{0,0}(\eta') = F_n$ if and only if η' satisfies

$$l_n \geq l_{n-1} = \cdots = l_2 = 1 \quad \text{and} \quad c_i c_{i+1} = -1 \quad \text{for} \quad i \neq n-2\,.$$

And by induction hypothesis on $a_{-1,0}(\eta')$ we get moreover that $a_{-1,0}(\eta') = F_{n-1}$ if an only if either $\eta' = 0^{l_3}\overline{1}01$ or

$$l_n \geq l_{n-1} = \cdots = l_3 = 1, \; l_1 - 1 = 0, \; c_2 = \overline{1}, \; c_i c_{i+1} = -1 \quad \text{if} \quad i \neq 2, n-2\,.$$

Putting the last two lists of conditions together we obtain that $a_{0,0}(\eta) = F_{n+1}$ if and only if either $\eta = \eta' 010^{l_0} = 0^{l_3}\overline{1}01010^{l_0}$ or $\eta = \eta' 010^{l_0}$ satisfies

$$l_n \geq l_{n-1} = \cdots = l_1 = 1, \; c_2 = \overline{1}, \; c_i c_{i+1} = -1 \quad \text{if} \quad i \neq n-2\,,$$

which is equivalent to (4.1) if $c_1 = 1$.

It remains to prove the induction step also for the equalities $a_{\pm 1,0}(\eta) = F_{w(\eta)}$ in case $w(\eta) \geq 2$. Again we consider only the case $\eta = \eta' 010^{l_0}$.

By (4.5) we already know that $a_{1,0}(\eta) = a_{1,0}(\eta' 010^{l_0}) = F_n$ if and only if $l_0 = 0$ and $a_{0,0}(\eta') = F_n$. From the induction hypothesis on η' we obtain that this is true if and only if η' satisfies

$$l_n \geq l_{n-1} = \cdots = l_2 = 1, \quad \text{and} \quad c_i c_{i+1} = -1 \quad \text{if} \quad i \neq n-2\,,$$

thus $a_{1,0}(\eta) = a_{1,0}(\eta' 010^{l_0}) = F_n$ if and only if it satisfies conditions (4.7) and (4.8).

Finally by (4.6), $a_{-1,0}(\eta) = a_{-1,0}(\eta' 010^{l_0}) = F_n$ if and only if $l_0 = 0$ and $a_{-1,0}(\eta') \le F_{n-1} \le F_n$. However, $F_{n-1} = F_n$ if and only if $n = 2$ and by the induction hypothesis, $a_{-1}(\eta') = F_2 = 1$ if and only if $\eta' = 0^{l_2}\overline{1}$, hence $a_{-1,0}(\eta) = a_{-1,0}(\eta' 010^{l_0}) = F_n$ if and only if $\eta = 0^{l_2}\overline{1}01$, which is the only exceptional case not covered by (4.9) and (4.10).

It completes the inductive proof of the characterization of those η, for which $a_{0,0}(\eta) = F_{w(\eta)+1}$. □

Corollary 4.2. *For any integer z the number of optimal BSDR's of z is*

$$|\mathcal{B}(z,0)| \le F_{w(\mathrm{NAF}(z)+1)}$$

and the equality holds if and only if $\mathrm{NAF}(z) = c_n 0^{l_{n-1}} c_{n-1} \cdots c_2 0^{l_1} c_1 0^{l_0}$ *satisfies*

$$l_{n-1} = \cdots = l_2 = l_1 = 1, \quad \textit{and} \quad c_i c_{i+1} = -1 \quad \textit{for each} \quad i \ne n-2\,.$$

Proof: We prove that $|\mathcal{B}(z,0)| = a_{0,0}(0\,\mathrm{NAF}(z))$ by establishing a bijection F between $\mathcal{B}(z,0)$ and $A_{0,0}(0\,\mathrm{NAF}(z))$.

If $\beta \in \mathcal{B}(z,0)$ and the terminal state of $p(0,\beta)$ is q, then we define

$$F(\beta) = p(0, 0^{|q|}\beta)\,.$$

By Lemma 3.1, the path $p(0,0^{|q|}\beta)$ has terminal state 0. Since β is reduced, the last transition of $p(0,0^{|q|}\beta)$ is different from $0 \xrightarrow{0|0} 0$. Hence the output of $p(0,0^{|q|}\beta)$ has exactly one leading 0 and since it is a NAF of z by the same Lemma 3.1, it is equal to $0\,\mathrm{NAF}(z)$. It proves $F(\beta) \in A_{0,0}(0\,\mathrm{NAF}(z))$.

To prove that the mapping F is injective, take another $\beta \ne \gamma \in \mathcal{B}(z,0)$ and denote by r the terminal state of the path $p(0,\gamma)$. Then $F(\gamma) = p(0,0^{|r|}\gamma)$. If the length $l(\beta) = l(\gamma)$, then $0^{|q|}\beta \ne 0^{|r|}\gamma$, thus $p(0,0^{|q|}\beta) \ne p(0,0^{|r|}\gamma)$. And if, say, $l(\beta) > l(\gamma)$, then the leftmost non-zero bit in $0^{|q|}\beta$ is different from the corresponding bit with the same position in $0^{|r|}\gamma$, which is 0. Hence again $0^{|q|}\beta \ne 0^{|r|}\gamma$ thus proving $F(\beta) \ne F(\gamma)$ also in the case $l(\beta) > l(\gamma)$.

It remains to verify that F is onto $A_{0,0}(0\,\mathrm{NAF}(z))$. Let $p = e_0 e_1 \cdots e_l \in A_{0,0}(0\,\mathrm{NAF}(z))$ and denote by β the input of p. We write $\beta = 0^q\hat{\beta}$, where $\hat{\beta}$ is reduced. It means that q is the number of leading 0's in β.

Since the output of p is $0\,\mathrm{NAF}(z)$, the last transition e_l of p is different from $0 \xrightarrow{0|0} 0$. Thus either $e_l = -1 \xrightarrow{0|0\overline{1}} 0$ or $e_l = 1 \xrightarrow{0|01} 0$. We consider only the case $e_l = 1 \xrightarrow{0|01} 0$, the other one follows once again from symmetry. Then the transition e_{l-1} must have terminal state 1 and it again gives two possibilities. Either $e_{l-1} = 0 \xrightarrow{1|\epsilon} 1$ or $e_{l-1} = 2 \xrightarrow{0|\epsilon} 1$.

In the first case, the input β equals $0\hat{\beta}$, the path $p(0,\hat{\beta})$ has terminal state $q = 1$ and $F(\hat{\beta}) = p(0,0^q\hat{\beta}) = p(0,\beta) = p$.

In the case $e_{l-1} = 2 \xrightarrow{0|\epsilon} 1$, the transition e_{l-2} must have terminal state 2 and it leaves only one possibility e_{l-2}, namely $e_{l-2} = 1 \xrightarrow{1|0\overline{1}} 2$. Thus the input of

$e_0e_1\cdots e_{l-2}$ is reduced and the input of p is $0^2\hat{\beta}$. The path $p(0,\hat{\beta})$ has terminal state $q=2$ and also in this case $F(\hat{\beta}) = p(0, 0^q\hat{\beta}) = p(0,\beta) = p$. It completes the proof that F is a bijection.

By the first part of Theorem 4.1 we obtain that

$$|\mathcal{B}(z,0)| \leq a_{0,0}(0\,\mathrm{NAF}(z)) = F_{w(\mathrm{NAF}(z)+1)}\,.$$

The second part of corollary follows from the second part of the theorem. □

It is easy to check that the upper bound $F_{w(\mathrm{NAF}(z))+1}$ for the number of optimal BSDR's of an integer z improves the earlier upper bounds mentioned in the introduction. For a non-zero integer z the upper bound for the number of optimal BSDR's of z given in [14] is F_{t+3}, where $t = \lfloor \log_4 |z| \rfloor$, while the upper bound given in [19] is F_{m+1}, where $m = \left\lceil \frac{l(\mathrm{NAF}(z))}{2} \right\rceil$. Recall that $l(\eta)$ denotes the length of a BSDR η.

Since the Fibonacci sequence is non-decreasing, the following straightforward lemma establishes the relationship between the three upper bounds.

Lemma 4.3. *For any integer $z \neq 0$ the following holds:*

$$w(\mathrm{NAF}(z)) \leq \left\lceil \frac{l(\mathrm{NAF}(z))}{2} \right\rceil \leq \lfloor \log_4 |z| \rfloor + 2\,.$$

PROOF: We denote $n = w(\mathrm{NAF}(z))$. Since $\mathrm{NAF}(z)$ contains at least one digit 0 between any two non-zero digits, we immediately get $l(\mathrm{NAF}(z)) \geq 2n-1$, hence

$$w(\mathrm{NAF}(z)) = n = \frac{l(\mathrm{NAF}(z))}{2} - \frac{1}{2} \leq \left\lceil \frac{l(\mathrm{NAF}(z))}{2} \right\rceil\,.$$

To prove the other inequality, let $t = \log_4 |z|$. Then $|z| \in \langle 4^t, 4^{t+1}) = \langle 2^{2t}, 2^{2t+2})$. By the condition on the length $l(\mathrm{NAF}(z))$ (see e.g. [6]) we get $l(\mathrm{NAF}(z)) \leq 2t+3$, and

$$\frac{l(\mathrm{NAF}(z))}{2} \leq t + \frac{3}{2}\,,$$

which proves

$$\left\lceil \frac{l(\mathrm{NAF}(z))}{2} \right\rceil \leq t+2 = \lfloor \log_4 |z| \rfloor + 2\,.$$ □

5. Number of BSDR's with positive overweight

In this section we will estimate the number of BSDR's of $z \in \mathbb{Z}$ with positive overweight $j \in \mathbb{N}$. As in the previous section, first we estimate the cardinality of the set $A_{0,0}(\eta, j)$ of paths in δ_0 with a given output

$$\eta = \eta(p) = 0^{l_n}c_n0^{l_{n-1}}c_{n-1}\cdots c_2 0^{l_1}c_1 0^{l_0} \in D^*$$

and overweight $j \geq 1$.

For a path $p = e_0 \cdots e_{l-1} \in A_{0,0}(\eta, j)$ with overweight $\mathrm{ow}(p) \geq 1$ there exists a transition e_i with positive overweight $\mathrm{ow}(e_i)$ by Definition 3.6. Let $k \in \{0, 1, \ldots, l-1\}$ be the minimal index such that $\mathrm{ow}(e_k) > 0$. In this section we reserve the index k for the first transition e_k with positive overweight. In fact, $k \geq 1$ since all transitions of δ_0 with initial state 0 have overweight 0. Hence the path $e_0 e_1, \ldots, e_{k-1}$ is always non-empty and has overweight 0.

By (3.1), $e_k \in \Delta_{\mathrm{ow}}$. Another important parameter of the path $p = e_0 \cdots e_{l-1}$ is the weight i of the output $w(e_0 e_1 \cdots e_k)$. For $i = 1, 2, \ldots, n = w(\eta)$ we define

$$A^i_{0,0}(\eta, j) = \{p \in A_{0,0}(\eta, j) : w(\eta(e_0 \cdots e_k)) = i\}\,. \tag{5.1}$$

Since the output $\eta(e_0 \cdots e_k)$ has always positive weight $\leq n$, the set $A_{0,0}(\eta, j)$ is a disjoint union of the sets $A^i_{0,0}(\eta, j)$ for $i = 1, 2, \ldots, n$, and

$$a_{0,0}(\eta, j) = |A_{0,0}(\eta, j)| = \sum_{i=1}^{n} |A^i_{0,0}(\eta, j)|\,. \tag{5.2}$$

The following theorem gives a recursive upper bound for the number $a_{0,0}(\eta, j)$.

Theorem 5.1. *Let $j > 0$ and $\eta = 0^{l_n} c_n 0^{l_{n-1}} c_{n-1} \cdots c_2 0^{l_1} c_1 0^{l_0} \in D^*$ with weight $w(\eta) = n \geq 1$. For $i = 1, \ldots, n$ we write*

$$\eta = \beta_i 0 c_i \gamma_i$$

and denote

$$\xi_i = \begin{cases} \beta_i 0 c_i & \text{if } \ l_i = 1\,, \\ \beta_i c_i & \text{if } \ l_i > 1\,. \end{cases} \tag{5.3}$$

Then

$$a_{0,0}(\eta, j) \leq \sum_{i=1}^{n} a_{0,0}(0\overline{c}_i \gamma_i) \cdot a_{0,0}(\xi_i, j-1)\,. \tag{5.4}$$

Proof: Take any $p = e_0 \cdots e_{l-1} \in A_{0,0}(\eta, j)$. Then for $i = w(\eta(e_0 \cdots e_k))$ we have $p \in A^i_{0,0}(\eta, j)$. We split the path p into $p = p_i q_i$ depending on the transition e_k, the first one in p with positive overweight. Since e_k has positive overweight,

$$e_k \in \Delta_{\mathrm{ow}} = \{1 \xrightarrow{\overline{1}|0\overline{1}} 0,\ -1 \xrightarrow{1|01} 0,\ 2 \xrightarrow{1|0} 2,\ 2 \xrightarrow{\overline{1}|0} 0,\ -2 \xrightarrow{1|0} 0,\ -2 \xrightarrow{\overline{1}|0} -2\}\,.$$

We split Δ_{ow} into two subsets, one is $\{1 \xrightarrow{\overline{1}|0\overline{1}} 0,\ -1 \xrightarrow{1|01} 0\}$, the other is $\{2 \xrightarrow{1|0} 2,\ 2 \xrightarrow{\overline{1}|0} 0,\ -2 \xrightarrow{1|0} 0,\ -2 \xrightarrow{\overline{1}|0} -2\}$, and define

$$p_i = \begin{cases} e_0 e_1 \cdots e_{k-1} & \text{if } \ e_k \in \{1 \xrightarrow{\overline{1}|0\overline{1}} 0,\ -1 \xrightarrow{1|01} 0\}\,, \\ e_0 e_1 \cdots e_{k-2} & \text{otherwise}\,, \end{cases} \tag{5.5}$$

and also

$$q_i = \begin{cases} e_k e_{k+1} \cdots e_{l-1} & \text{if } \ e_k \in \{1 \xrightarrow{\overline{1}|0\overline{1}} 0,\ -1 \xrightarrow{1|01} 0\}\,, \\ e_{k-1} e_k \cdots e_{l-1} & \text{otherwise}\,. \end{cases} \tag{5.6}$$

We denote $c = c_i$. In case $e_k \in \{1 \xrightarrow{\overline{1}|0\overline{1}} 0,\ -1 \xrightarrow{1|01} 0\}$, the output $\eta(e_0 e_1 \cdots e_k)$ is $0c\gamma_i$, hence the output of the path $p_i = e_0 e_1 \cdots e_{k-1}$ is γ_i and its terminal state is $-c = -c_i$.

If $e_k \in \{2 \xrightarrow{1|0} 2,\ 2 \xrightarrow{\overline{1}|0} 0,\ -2 \xrightarrow{1|0} 0,\ -2 \xrightarrow{\overline{1}|0} -2\}$, then its initial state is ± 2. So the terminal state of the preceding transition e_{k-1} is also ± 2 and because the overweight of e_{k-1} is 0, it must be one of $\{1 \xrightarrow{1|0\overline{1}} 2, -1 \xrightarrow{\overline{1}|01} -2\}$. So we get four possibilities for the pair of transitions $e_{k-1}e_k$:

$$e_{k-1} e_k \in \{-c \xrightarrow{\overline{c}|0c} -2c \xrightarrow{\overline{c}|0} -2c,\quad -c \xrightarrow{\overline{c}|0c} -2c \xrightarrow{c|0} 0 : c = c_i = \pm 1\}\,. \tag{5.7}$$

Hence the output of the path $e_0 e_1 \cdots e_k$ is $00c\gamma_i$. So the output of $p_i = e_0 e_1 \cdots e_{k-2}$ is again γ_i and its terminal state is $-c = -c_i$.

So we proved

$$p_i \in A_{0,-c}(\gamma_i, 0), \quad \text{where} \ \ c = c_i \tag{5.8}$$

and also (since $p = p_i q_i$)

$$q_i \in A_{-c,0}(\beta_i 0c, j), \quad \text{where} \ \ c = c_i\,. \tag{5.9}$$

By (3.16) or (3.17) we get

$$|A_{0,-c}(\gamma_i, 0)| = a_{0,-c}(\gamma_i, 0) = a_{0,0}(0\overline{c}\gamma_i, 0)\,. \tag{5.10}$$

If $l_i = 1$, then by the discussion preceding (5.8) there is only one possibility for e_k, namely $e_k = -c \xrightarrow{c|0c} 0$. By (5.6), $q_i = e_k \cdots e_{l-1}$, and by (5.9), $q_i \in A_{-c,0}(\beta_i 0c, j)$. So we get that $e_{k+1} \cdots e_{l-1} \in A_{0,0}(\beta_i, j-1)$, because $\mathrm{ow}(e_k) = 1$. Thus the set of all possible q_i's (in the case $l_i = 1$) is

$$\{-c \xrightarrow{c|0c} 0\} \times A_{0,0}(\beta_i, j-1)$$

and therefore its cardinality is $a_{0,0}(\beta_i, j-1) \le a_{0,0}(\beta_i 0\overline{c}, j-1) = a_{0,0}(\xi_i, j-1)$, by (3.14) or by (3.15). Together with (5.8) and (5.10) we obtain that

$$|A^i_{0,0}(\eta, j)| \le a_{0,0}(0\overline{c}\gamma_i, 0) \cdot a_{0,0}(\xi_i, j-1), \quad \text{if} \ \ l_i = 1\,. \tag{5.11}$$

It is less straightforward to estimate the cardinality of the set of possible q_i's in the case $l_i > 1$. In this case

$$e_k \in \{-c \xrightarrow{c|0c} 0,\ -2c \xrightarrow{\overline{c}|0} -2c,\ -2c \xrightarrow{c|0} 0\}\,.$$

We write $\beta = \beta'0$. If $e_k = -c \xrightarrow{c|0c} 0$, then $e_{k+1} = 0 \xrightarrow{0|0} 0$, since $l_i \geq 2$. So in this case

$$q_i = e_k e_{k+1} \cdots e_{l-1} \in \{-c \xrightarrow{c|0c} 0 \xrightarrow{0|0} 0\} \times A_{0,0}(\beta', j-1)\,, \tag{5.12}$$

since $\mathrm{ow}(e_k) = 1$.

If $e_k = -2c \xrightarrow{\overline{c}|0} -2c$, then

$$q_i = e_{k-1} e_k \cdots e_{l-1} \in \{-c \xrightarrow{\overline{c}|0c} -2c \xrightarrow{\overline{c}|0} -2c\} \times A_{-2c,0}(\beta', j-1)\,, \tag{5.13}$$

since again $\mathrm{ow}(e_k) = 1$.

And if $e_k = -2c \xrightarrow{c|0} 0$, then

$$q_i = e_{k-1} e_k \cdots e_{l-1} \in \{-c \xrightarrow{\overline{c}|0c} -2c \xrightarrow{c|0} 0\} \times A_{0,0}(\beta', j-2)\,, \tag{5.14}$$

since this time $\mathrm{ow}(e_k) = 2$.

Putting together (5.12), (5.13) and (5.14) we get that the number of possible q_i's is at most

$$\begin{aligned} &|A_{0,0}(\beta', j-1)| + |A_{-2c,0}(\beta', j-1)| + |A_{0,0}(\beta', j-2)| \\ &= a_{0,0}(\beta', j-1) + a_{-2c,0}(\beta', j-1) + a_{0,0}(\beta', j-2) \\ &= a_{0,0}(\beta'0c, j-1) = a_{0,0}(\beta c, j-1) = a_{0,0}(\xi_i, j-1) \end{aligned} \tag{5.15}$$

by (3.18) or (3.19).

And since the number of possible p_i's is at most $a_{0,0}(0\overline{c}\gamma_i, 0)$ by (5.8) and (5.10), we get also in the case $l_i > 1$ that

$$|A^i_{0,0}(\eta, j)| \leq a_{0,0}(0\overline{c}\gamma_i, 0) \cdot a_{0,0}(\xi_i, j-1)\,.$$

So by (5.2) we finally obtain

$$a_{0,0}(\eta, j) = \sum_{i=1}^{n} |A^i_{0,0}(\eta, j)| \leq \sum_{i=1}^{n} a_{0,0}(0\overline{c}\gamma_i, 0) \cdot a_{0,0}(\xi_i, j-1)\,. \qquad \square$$

To establish the connection between the set $\mathcal{B}(z, j)$ of reduced BSDR's of z with overweight j and the set $A_{0,0}(\eta, j)$ for some η we prove the next lemma.

Lemma 5.2. *For every $j > 0$ and an integer $z \neq 0$, $|\mathcal{B}(z, j)| = a_{0,0}(0^j\,\mathrm{NAF}(z), j)$.*

Proof: We establish a bijection between $\mathcal{B}(z, j)$ and $A_{0,0}(0^j\,\mathrm{NAF}(z), j)$.

If $\beta \in \mathcal{B}(z, j)$, then we denote the terminal state of the path $p(0, \beta)$ by q. Then by Lemma 3.1, the terminal state of the path $p = p(0, 0^{|q|}\beta)$ is 0 and its output is $0^m\,\mathrm{NAF}(z)$ for some m. By Lemma 3.7, $\mathrm{ow}(p) = \mathrm{ow}(0^{|q|}\beta)) = \mathrm{ow}(\beta)$.

So if we set $F(\beta) = p(0, 0^{|q|}\beta)$, then $F(\beta) \in A_{0,0}(0^m\,\mathrm{NAF}(z), j)$ for some m. We prove that always $1 \leq m \leq j$.

Let $p = e_0 e_1 \cdots e_{l-1}$. Since every transition with terminal state 0 outputs one leading 0, there must be $m \geq 1$. Similarly as in the proof of Corollary 4.2, we observe that the last transition $e_{l-1} \neq (0 \xrightarrow{0|0} 0)$. If e_{l-1} has initial state ± 1, then the output of p has exactly one leading 0, i.e. $m = 1$. If the transition $e_{l-1} = 2c \xrightarrow{\overline{c}|0} 0$ for $c = \pm 1$, then the final part of p is

$$c \xrightarrow{c|0\overline{c}} \underbrace{2c \xrightarrow{c|0} 2c \cdots 2c \xrightarrow{c|0} 2c}_{n \text{ transitions}} \xrightarrow{\overline{c}|0} 0 \tag{5.16}$$

for some $n \geq 0$. Since the transition $2c \xrightarrow{c|0} 2c$ has overweight 1 and $2c \xrightarrow{\overline{c}|0} 0$ has overweight 2, we get $n + 2 \leq \mathrm{ow}(p) = j$, thus $n \leq j - 2$. The output of the final part (5.16) has exactly $n+2$ leading 0's, so also the output of p has exactly $n + 2 \leq j$ leading 0's. It completes the proof of $F(\beta) \in A_{0,0}(0^m \,\mathrm{NAF}(z), j)$.

We set

$$G(\beta) = p(0, 0^{j-m} 0^{|q|} \beta) \quad \text{if} \quad F(p) \in A_{0,0}(0^m \,\mathrm{NAF}(z), j)\,. \tag{5.17}$$

Thus $G(\beta)$ equals $F(\beta) = p(0, 0^{|q|}\beta)$ followed by $j - m$ transitions $0 \xrightarrow{0|0} 0$. It follows that $G(\beta)$ has exactly j leading 0's and therefore $G(\beta) \in A_{0,0}(0^j \,\mathrm{NAF}(z), j)$.

We easily observe that the mapping $G : \mathcal{B}(z, j) \to A_{0,0}(0^j \,\mathrm{NAF}(z), j)$ is injective and similarly as in the proof of Corollary 4.2 we prove that it is onto. □

From Lemma 5.2 and Theorem 5.1 we immediately obtain the following recursive relation.

Corollary 5.3. *For every $j > 0$ and any nonzero integer z with* $\mathrm{NAF}(z) = c_n 0^{l_{n-1}} c_{n-1} \cdots c_2 0^{l_1} c_1 0^{l_0} = \beta_i 0 c_i \gamma_i$, *and any $i = 1, 2, \ldots, w(\mathrm{NAF}(z))$ we denote $z_i' = (0\overline{c}_i\gamma_i)_2$ and $z_i'' = (\xi_i)_2$. Then*

$$|\mathcal{B}(z, j)| \leq \sum_{i=1}^{n} |\mathcal{B}(z_i', 0)| \cdot |\mathcal{B}(z_i'', j-1)|\,. \tag{5.18}$$

We can define recursively "generalized Fibonacci numbers" $F_{n\,,\,j}$ for $n, j \in \mathbb{N}$ as

$$\begin{aligned} F_{n\,,\,0} &= F_{n+1}\,, \\ F_{n\,,\,j} &= \sum_{i=1}^{n} F_i \cdot F_{n-i+1\,,\,j-1}\,, \quad \text{if} \quad j > 0\,. \end{aligned}$$

Then Corollary 5.3 states that for every non-zero integer z and every overweight $j \in \mathbb{N}$

$$|\mathcal{B}(z, j)| \leq F_{w(\mathrm{NAF}(z))\,,\,j}\,,$$

since $w(\mathrm{NAF}(z_i')) = i$ and $w(\mathrm{NAF}(z_i'')) = n - i + 1$.

Acknowledgment. The authors are indebted to the anonymous referee of an earlier manuscript by the second author for suggesting to use transducers to prove results on the number of optimal BSDR's of an integer.

References

[1] Booth A.D., *A signed binary multiplication technique*, Quart. J. Mech. Appl. Math. **4** (1951), 236–240.

[2] Reitwiesner G., *Binary arithmetic*, in Advances in Computers, 1, Academic Press, New York, 1960, pp. 231–308.

[3] Morain F., Olivos J., *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.

[4] Koyama K., Tsuruoka Y., *Speeding up elliptic cryptosystems by using a signed binary window method*, Advances in cryptology - CRYPTO' 92, Lecture Notes in Comput. Sci., 740, Springer, Berlin, 1993, pp. 345–357.

[5] Miyaji A., Ono T., Cohen H., *Efficient elliptic curve exponentiation*, Information and Communications Security, Lecture Notes in Comput. Sci., 1334, Springer, Berlin-Heidelberg, 1997, pp. 282–290.

[6] Solinas J., *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.

[7] Oswald E., Aigner M., *Randomized addition-subtraction chains as a countermeasure against power attacks*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., 2162, Springer, Berlin, 2001, pp. 39–50.

[8] Ha J., Moon S., *Randomized signed-scalar multiplication of ECC to resist power attacks*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., 2523, Springer, Berlin-Heidelberg, 2002, pp. 551–563.

[9] Ebeid N., Anwar Hasan M., *On randomized private keys to counteract DPA attacks*, in Matsui M., Zuccherato R. (ed.), SAC 2003, Lecture Notes in Comput. Sci., 3006, Springer, Berlin, 2004, pp. 58–72.

[10] Heuberger C., *Minimal expansions in redundant number systems: Fibonacci bases and greedy algorithm*, Period. Math. Hungar. **49** (2004), no. 2, 65–89.

[11] Xiaoyu R., Katti R., *Left-to-right optimal signed-binary representation of a pair of integers*, IEEE Trans. Comput. **54** (2005), 132–140.

[12] Muir J.A., Stinson D.R., *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. **75** (2006), no. 253, 369–384.

[13] Heuberger C., Prodinger H., *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248.

[14] Grabner P.J., Heuberger C., *On the number of optimal base* 2 *representations*, Des. Codes Cryptogr. **40** (2006), 25–39.

[15] Stevens M., Lenstra A., de Weger B., *Chosen-prefix collisions for MD*5 *and colliding X*.509 *certificates for different identities*, Advances in cryptology – EUROCRYPT 2007 (Moni Naor, ed.), Lecture Notes in Comput. Sci., 4515, Springer, Berlin, 2007, pp. 1–22.

[16] Kim T.H., Han D., Okeya K., Lim J.I., *Differential power analysis on countermeasures using binary signed digit representations*, ETRI Journal, vol. 29, no. 5, Oct. 2007, pp. 619–632.

[17] Bang-ju Wang, Huan-guo Zhang, Zhang-yi Wang, Yu-hua Wang, *Speeding up scalar multiplication using a new signed binary representation for integers*, Multimedia Content Analysis and Mining, Lecture Notes in Comput. Sci., 4577, Springer, Berlin-Heidelberg, 2007, pp. 277–285.

[18] Vábek J., Joščák D., Boháček M., Tůma J., *A new type of* 2*-block collisions in MD*5, in Chowdury, Rijmen, Das (ed.), Progress in cryptology – INDOCRYPT 2008, Lecture Notes in Comput. Sci., 5365, Springer, Berlin, 2008, pp. 78-90.

[19] Wu T., Zhang M., Du H., Wang R., *On optimal binary signed digit representation of integers*, Appl. Math. J. Chinese Univ. Ser.B **25** (2010), no. 3, 331–340.

[20] Avanzi R., Heuberger C., Prodinger H., *Redundant τ-adic expansions I: non-adjacent digit sets and their applications to scalar multiplication*, Des. Codes Cryptogr. **58** (2011), no. 2, 173–202.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: tuma@karlin.mff.cuni.cz
jiri.vabek@centrum.cz

(*Received* June 11, 2014, *revised* January 5, 2015)