Alternative Digit Sets for Nonadjacent Representations*

James A. Muir[1]** and Douglas R. Stinson[2]***

[1] Department of Combinatorics and Optimization

[2] School of Computer Science

University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
{jamuir,dstinson}@uwaterloo.ca

Abstract. It is known that every positive integer n can be represented as a finite sum of the form $n = \sum a_i 2^i$, where $a_i \in \{0, 1, -1\}$ for all i, and no two consecutive a_i's are non-zero. Such sums are called *nonadjacent representations*. Nonadjacent representations are useful in efficiently implementing elliptic curve arithmetic for cryptographic applications.
In this paper, we investigate if other digit sets of the form $\{0, 1, x\}$, where x is an integer, provide each positive integer with a nonadjacent representation. If a digit set has this property we call it a *nonadjacent digit set* (NADS). We present an algorithm to determine if $\{0, 1, x\}$ is a NADS; and if it is, we present an algorithm to efficiently determine the nonadjacent representation of any positive integer. We also present some necessary and sufficient conditions for $\{0, 1, x\}$ to be a NADS. These conditions are used to exhibit infinite families of integers x such that $\{0, 1, x\}$ is a NADS, as well as infinite families of x such that $\{0, 1, x\}$ is not a NADS.

1 Introduction and History

In a base 2 (or *radix* 2) positional number system, representations of integers are converted into integers via the rule

$$(\ldots a_3 a_2 a_1 a_0)_2 = \cdots + a_3 2^3 + a_2 2^2 + a_1 2^1 + a_0 \ .$$

Each of the a_i's is called a *digit*. In the usual radix 2 positional number system the digits have the property that $a_i \in \{0, 1\}$, for all i. If we let $D = \{0, 1\}$ then we say that D is the *digit set* for this number system.

* *Date: 18 November 2003.* This paper is extended version which supersedes the paper appearing in the Proceedings of SAC 2003 (Lecture Notes in Computer Science, Vol. 3006, 2004) and the CACR technical report (CACR 2003-04).
** Supported in part by an NSERC Postgraduate Scholarship.
*** Supported by NSERC grant RGPIN 203114-02.

It is often advantageous to employ alternate digit sets. The digit set $D = \{0, 1, \overline{1}\}$, where $\overline{1}$ stands for -1, was studied as early as 1951 by Booth. In [1], Booth presents a technique whereby a binary computer can calculate a representation of the product of two integers without any extra steps to correct for its sign. His method is implicitly based on replacing one of the operands in the multiplication with a $\{0, 1, \overline{1}\}$ radix 2 representation. Later, in 1960, through his investigations on how to reduce the number of additions and subtractions used in binary multiplication and division, Reitwiesner [7] gave a constructive proof that every integer has a canonical $\{0, 1, \overline{1}\}$ radix 2 representation with a *minimal* number of nonzero digits.

Reitwiesner's canonical representations have a simple description. A $\{0, 1, \overline{1}\}$ radix 2 representation of an integer is in Reitwiesner's canonical form if and only if it satisfies the following property:

NA-1 *Of any two adjacent digits, at least one is zero.*

Said another way, for such representations, nonzero digits are nonadjacent. These representations have come to be called *nonadjacent forms* (NAFs).

Cryptographers came to be interested in NAFs through a study of exponentiation. Jedwab and Mitchell [3] noticed that it is possible to reduce the number of multiplications used in the square-and-multiply algorithm for exponentiation if a $\{0, 1, \overline{1}\}$ radix 2 representation of the exponent is used. This led them to an independent discovery of the NAF. However, in multiplicative groups, like those used for RSA and DSA, using the digit $\overline{1}$ requires the computation of an inverse which is more costly than a multiplication.

In elliptic curve groups this is not a problem since inverses can be computed essentially for free. Morain and Olivos [6] observed that in these groups the operation analogous to exponentiation could be made more efficient using $\{0, 1, \overline{1}\}$ representations. They give two algorithms for performing scalar-multiplication using addition and subtraction. The $\{0, 1, \overline{1}\}$ radix 2 representations upon which their algorithms are based are in fact the same ones that Booth and Reitwiesner studied. In the quest for efficient implementations of elliptic curve cryptosystems, NAFs and representations like them have become an important device; Gordon [2] and Solinas [9, 10] make this point quite convincingly.

If a finite length radix 2 representation has digit set D and satisfies **NA-1**, we call it a *D-nonadjacent form* (D-NAF). In this paper, we consider the question of which sets D provide nonadjacent forms for *every positive* integer. If D is such a digit set then we call it a *nonadjacent digit set* (NADS). After a preliminary version of this paper was completed it was discovered that a related question has been studied by Matula. In [4], Matula defines and investigates *basic* digit sets. A set of digits containing 0 is called *basic* if it provides every integer, positive and negative, with a unique radix-r representation without the use of a separate sign. If a digit set is basic, Matula shows that $r \neq 2$; in this paper we are concerned only with radix 2 representations. Another difference between our work and Matula's is that he imposes no relation on the digits of a representation while we are interested only in nonadjacent representations.

We examine digit sets of the form $\{0, 1, x\}$ with $x \in \mathbb{Z}$. It is known that letting $x = \overline{1}$ gives a NADS, but it is somewhat surprising that there are many values of x with this property; for example, $x = \overline{5},\ \overline{13},\ \overline{1145}$ (note $\overline{5}$ means -5, etc.). We give infinite families of x's for which $\{0, 1, x\}$ is a NADS, and we also give infinite families of x's for which $\{0, 1, x\}$ is not a NADS. We also give some results on the necessary conditions D must satisfy in order to be a NADS. The algorithms we present and analyze for computing D-NAFs might be of some interest as well.

2 Preliminaries

We start by introducing some definitions and notation which will facilitate our discussions.

If n is an integer and we write $n = (\ldots a_2 a_1 a_0)_2$ then we are expressing n as the sum of an *infinite* series. If there is some ℓ such that $a_i = 0$ for all $i \geq \ell$ then n is the sum of a *finite* series and we indicate this by writing $n = (a_{\ell-1} \ldots a_2 a_1 a_0)_2$. If, in addition, $a_{\ell-1} \neq 0$ we say this representation has *length* ℓ.

Definition 1. *The* length *of a representation* $(\ldots a_2 a_1 a_0)_2$ *is the largest integer* ℓ *such that* $a_{\ell-1} \neq 0$ *but* $a_i = 0$ *for all* $i \geq \ell$*. The length of the all zero representation is defined to be zero.*

We will always use D to denote a digit set. The set of all *strings* of digits from D is denoted by D^*. The empty string is in D^* and is denoted by ϵ. Now, if D is the digit set for $(a_{\ell-1} \ldots a_1 a_0)_2$, then $a_{\ell-1} \ldots a_1 a_0$ is a string in D^*. Conversely, any string $\alpha \in D^*$ corresponds to a radix 2 representation with digit set D, namely $(\alpha)_2$. If $\alpha, \beta \in D^*$ then we denote their *concatenation* by $\alpha \| \beta$.

We apply some of our terminology for representations to strings. If $0 \in D$ and a finite string $\alpha \in D^*$ satisfies the property **NA-1**, then we call α a D-NAF. If in addition, $(\alpha)_2 = n$ we say α is a D-NAF for n. Notice that if α is a D-NAF for n then α with any leading zeros removed is also a D-NAF for n. We denote the string formed by deleting the leading zeros from α by $\widehat{\alpha}$.

Given a digit set D and an integer n, we define a map

$$R_D(n) := \begin{cases} \widehat{\alpha} & \text{where } \alpha \in D^* \text{ is a } D\text{-NAF for } n, \text{ if one exists} \\ \perp & \text{otherwise.} \end{cases}$$

Here, $\perp$ is just some symbol not in D. If $R_D(n)$ evaluates to a D-NAF for n, then by definition that string has no leading zeros. For example, if $D = \{0, 1, \overline{9}\}$ then $R_D(7)$ might evaluate to $1000\overline{9}$ since $1000\overline{9}$ is a D-NAF, has no leading zeros, and $(1000\overline{9})_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + \overline{9} \cdot 2^0 = 7$. If there is more than one string in D which is a D-NAF for n and has no leading zeros then $R_D(n)$ might evaluate to any one of these strings. Later on we will prove that 3 does not have a D-NAF, hence $R_D(3) = \perp$.

We are interested in determining which integers have D-NAFs, so we define the set

$$\mathrm{NAF}(D) := \{n \in \mathbb{Z} : R_D(n) \neq \perp\} .$$

From our example with $D = \{0, 1, \overline{9}\}$ we see $7 \in \mathrm{NAF}(D)$ but $3 \notin \mathrm{NAF}(D)$. Using this notation, our definition of a nonadjacent digit set is as follows:

Definition 2. *D is a* nonadjacent digit set *if* $\mathbb{Z}^+ \subseteq \mathrm{NAF}(D)$.

3 Necessary Conditions for $\{0, 1, x\}$ to be a NADS

If we suppose $D = \{0, 1, x\}$ is a nonadjacent digit set then we can deduce necessary conditions on x.

Theorem 3. *Let $D = \{0, 1, x\}$. If there exists $n \in \mathrm{NAF}(D)$ with $n \equiv 3 \pmod 4$, then $x \equiv 3 \pmod 4$.*

Proof. Take $n \in \mathrm{NAF}(D)$ with $n \equiv 3 \pmod 4$. For some particular D-NAF, say $(\ldots a_2 a_1 a_0)_2$, we have

$$\begin{aligned} (\ldots a_2 a_1 a_0)_2 &= n \\ &\implies a_0 \equiv 1 \pmod 2 \\ &\implies a_0 \neq 0 \ . \end{aligned}$$

Since a_0 is nonzero and the representation is nonadjacent we have $a_1 = 0$. Thus

$$\begin{aligned} (\ldots a_2 0 a_0)_2 &= n \\ &\implies a_0 \equiv 3 \pmod 4 \\ &\implies a_0 \neq 1 \\ &\implies a_0 = x \ . \end{aligned}$$

So $x = a_0 \equiv 3 \pmod 4$. ∎

If $D = \{0, 1, x\}$ is a NADS then $3 \in \mathrm{NAF}(D)$, and by the previous result $x \equiv 3 \pmod 4$. So, if we are trying to find a value of x that makes $\{0, 1, x\}$ a NADS we need only consider those values congruent to 3 modulo 4.

3.1 The case $x > 0$

If we restrict x to be a positive integer, then we can give a complete characterization of all values which make $D = \{0, 1, x\}$ a NADS. It is well known that $x = 3$ is such a value, and this is remarked by Solinas [8]. We give a proof of this fact and then show that no other positive value of x makes $\{0, 1, x\}$ a NADS.

Theorem 4. *The only NADS of the form $\{0, 1, x\}$ with $x > 0$ is $\{0, 1, 3\}$.*

Proof. Let n be any positive integer. We want to show that n has a $\{0, 1, 3\}$-NAF. Let $(\ldots a_2 a_1 a_0)_2$ be the usual $\{0, 1\}$-radix 2 representation of n. If this representation satisfies **NA-1** there is nothing to prove, so suppose it does not. Let i be the smallest integer for which $a_{i+1} = a_i = 1$. Replace digits a_{i+1} and a_i

by 0 and 3, respectively. Since $2^{i+1} + 2^i = 0 \cdot 2^{i+1} + 3 \cdot 2^i$, the resulting representation stands for the same integer. By working from right to left, repeating this substitution as necessary, we transform $(\ldots a_2 a_1 a_0)_2$ into a $\{0, 1, 3\}$-NAF. This proves that $\{0, 1, 3\}$ is a NADS.

Now consider x with $x > 3$. We show $n = 3$ does not have a $\{0, 1, x\}$-NAF. Suppose to the contrary that for some $\{0, 1, x\}$-NAF we have $(\ldots a_2 a_1 a_0)_2 = 3$. Since 3 is odd, $a_0 \neq 0$ and so $a_1 = 0$. Now $a_0 \equiv 3 \pmod 4$ so it must be that $a_0 = x$. However, since each of the digits in $\{0, 1, x\}$ is nonnegative we have

$$3 = (\ldots a_2 0 x)_2 = \cdots + a_2 2^2 + 0 \cdot 2^1 + x \geq x > 3 \ ,$$

which is a contradiction. So, 3 does not have a $\{0, 1, x\}$-NAF when $x > 3$. ■

An example helps illustrate the construction used in the above proof. Suppose $n = 237$. To find a $\{0, 1, 3\}$-NAF for 237 we start with its usual binary representation and then, working from right to left, replace any occurrences of the digits 11 with 03:

$$237 = (11101101)_2 = (10300301)_2 \ .$$

A natural question to ask is if this is the only $\{0, 1, 3\}$-NAF for 237. We give the answer in the next section.

3.2 Uniqueness

We show that every integer, not only just the positive ones, has at most one $\{0, 1, x\}$-NAF where $x \equiv 3 \pmod 4$.

Theorem 5. *If $x \equiv 3 \pmod 4$, then any integer has at most one finite length $\{0, 1, x\}$-nonadjacent form.*

Proof. Let $D = \{0, 1, x\}$ and suppose the result is false. Then it must be that

$$(a_{\ell-1} \ldots a_2 a_1 a_0)_2 = (b_{\ell'-1} \ldots b_2 b_1 b_0)_2$$

where $(a_{\ell-1} \ldots a_2 a_1 a_0)_2$ and $(b_{\ell'-1} \ldots b_2 b_1 b_0)_2$ are two different D-NAFs with lengths ℓ and ℓ' respectively. These representations stand for the same integer, call it n. We can assume that ℓ is as small as possible.

If $a_0 = b_0$, then

$$(a_{\ell-1} \ldots a_2 a_1)_2 = (b_{\ell'-1} \ldots b_2 b_1)_2 \ ,$$

and so we have two different, and shorter, D-NAFs which stand for the same integer, contrary to the minimality of ℓ. So it must be that $a_0 \neq b_0$.

If one of a_0 or b_0 is 0, then n is even, and so both a_0 and b_0 are 0. But a_0 and b_0 are different so it must be that a_0 is equal to 1 or x. Without loss of generality, we can assume the representations have the form

$$(a_{\ell-1} \ldots a_2 0 x)_2 = (b_{\ell'-1} \ldots b_2 01)_2 \ .$$

This implies $x \equiv 1 \pmod 4$, contrary to our hypothesis that $x \equiv 3 \pmod 4$. Thus every integer has at most one D-NAF. ■

4 Recognizing NADS of the form $\{0, 1, x\}$

From now on we fix $D = \{0, 1, x\}$ with $x \equiv 3 \pmod 4$. In this section we work towards a method of deciding if $\{0, 1, x\}$ is a NADS. By Theorem 4, this is easy when $x > 0$, so we will assume $x < 0$.

Recall that $R_D(n)$ either evaluates to the symbol $\perp$ or a finite string, with no leading zeros, that is a D-NAF for n. Theorem 5 tells us that any n has at most one D-NAF, so in the second case, the string returned by $R_D(n)$ is unique. Thus, $R_D(n)$ is well defined (i.e., for every input n there is exactly one output.).

The ability to evaluate $R_D(n)$ can be useful in deciding if D is a NADS. If we can find $n \in \mathbb{Z}^+$ such that $R_D(n) = \perp$ then we know that D is not a NADS. Also, if we have an algorithmic description of $R_D(n)$, we might be able to analyze this algorithm and show that for any $n \in \mathbb{Z}^+$, $R_D(n) \neq \perp$, thus proving that D is a NADS.

We show that $R_D(n)$ can be computed recursively and give an algorithm which evaluates $R_D(n)$ in this manner. We begin with some lemmas:

Lemma 6. *If $n \equiv 0 \pmod 4$ then $n \in \mathrm{NAF}(D)$ if and only if $n/4 \in \mathrm{NAF}(D)$. Further, if $n \in \mathrm{NAF}(D)$ then $R_D(n) = R_D(n/4)\|00$.*

Proof. Since $n \equiv 0 \pmod 4$, the definition of the digit set D implies that any D-NAF for n is of the form $(a_{\ell-1} \dots a_3 a_2 00)_2$, where $a_{\ell-1} \neq 0$. Now,

$$\begin{aligned} n \in \mathrm{NAF}(D) &\iff n \text{ has a } D\text{-NAF of the form } (a_{\ell-1} \dots a_3 a_2 00)_2 \\ &\iff n/4 \text{ has a } D\text{-NAF of the form } (a_{\ell-1} \dots a_3 a_2)_2 \\ &\iff n/4 \in \mathrm{NAF}(D) \ , \end{aligned}$$

which proves the first part of the lemma. If $n \in \mathrm{NAF}(D)$ then

$$R_D(n) = a_{\ell-1} \dots a_3 a_2 00 = a_{\ell-1} \dots a_3 a_2 \| 00 = R_D(n/4)\|00 \ ,$$

which proves the second part of the lemma. ■

We omit the proofs of the next three lemmas since they can be established by making only minor changes to the proof of Lemma 6.

Lemma 7. *If $n \equiv 1 \pmod 4$ then $n \in \mathrm{NAF}(D)$ if and only if $(n-1)/4 \in \mathrm{NAF}(D)$. Further, if $n \in \mathrm{NAF}(D)$ then $R_D(n) = R_D(\frac{n-1}{4})\|01$.*

Lemma 8. *If $n \equiv 2 \pmod 4$ then $n \in \mathrm{NAF}(D)$ if and only if $n/2 \in \mathrm{NAF}(D)$. Further, if $n \in \mathrm{NAF}(D)$ then $R_D(n) = R_D(n/2)\|0$.*

Lemma 9. *If $n \equiv 3 \pmod 4$ then $n \in \mathrm{NAF}(D)$ if and only if $(n-x)/4 \in \mathrm{NAF}(D)$. Further, if $n \in \mathrm{NAF}(D)$ then $R_D(n) = R_D(\frac{n-x}{4})\|0x$.*

Given an integer n, if we somehow know that $n \in \mathrm{NAF}(D)$ then Lemmas 6–9 suggest a recursive procedure that we can use to evaluate $R_D(n)$. To illustrate

suppose $D = \{0, 1, \overline{9}\}$. It was shown in an earlier example that $7 \in \mathrm{NAF}(D)$. Using these lemmas, we have:

$$R_D(7) = R_D(4)\|0\overline{9} = R_D(1)\|00\|0\overline{9} = 1\|00\|0\overline{9} = 1000\overline{9} \ .$$

To describe the general procedure for computing $R_D(n)$, given that $n \in \mathrm{NAF}(D)$, we use the following two functions:

$$f_D(n) := \begin{cases} n/4 & \text{if } n \equiv 0 \pmod 4 \\ (n-1)/4 & \text{if } n \equiv 1 \pmod 4 \\ n/2 & \text{if } n \equiv 2 \pmod 4 \\ (n-x)/4 & \text{if } n \equiv 3 \pmod 4 \ , \end{cases} \tag{1}$$

$$g_D(n) := \begin{cases} 00 & \text{if } n \equiv 0 \pmod 4 \\ 01 & \text{if } n \equiv 1 \pmod 4 \\ 0 & \text{if } n \equiv 2 \pmod 4 \\ 0x & \text{if } n \equiv 3 \pmod 4 \ . \end{cases} \tag{2}$$

Note that f_D returns an integer, and g_D returns a string. Here is the procedure described in pseudocode:

Procedure 10: EVAL_α-$R_D(n)$

$\alpha \leftarrow \epsilon$
while $n \neq 0$
  do $\begin{cases} \alpha \leftarrow g_D(n) \parallel \alpha \\ n \leftarrow f_D(n) \end{cases}$
return $\widehat{\alpha}$

Procedure 10 terminates on input n if and only if ${f_D}^i(n) = 0$ for some positive integer i. An easy calculation shows that, for $D = \{0, 1, \overline{9}\}$, ${f_D}^3(7) = 0$, and so the procedure terminates on input $n = 7$. However, $f_D(3) = 3$ and so ${f_D}^i(3) = 3 \neq 0$ for all i, thus the procedure does not terminate on input $n = 3$.

Using the previous lemmas, we can show Procedure 10 terminates on input n if and only if $n \in \mathrm{NAF}(D)$. Instead of making use of the lemmas individually, it is more convenient to summarize them as follows:

Lemma 11. *For all $n \in \mathbb{Z}$, $n \in \mathrm{NAF}(D)$ if and only if $f_D(n) \in \mathrm{NAF}(D)$. Further, if $n \in \mathrm{NAF}(D)$ then $R_D(n) = R_D(f_D(n))\|g_D(n)$.*

Now, suppose $n \in \mathrm{NAF}(D)$. Then the finite string $R_D(n)$ can be computed with a finite number of recursive steps. This implies that there is some positive integer i such that ${f_D}^i(n) = 0$, which in turn implies that the procedure terminates. Conversely, suppose the procedure terminates. Then ${f_D}^i(n) = 0$ for some i, and clearly $0 \in \mathrm{NAF}(D)$. Thus, ${f_D}^i(n) \in \mathrm{NAF}(D)$, and by the lemma $n \in \mathrm{NAF}(D)$.

Procedure 10 is named EVAL$_\alpha$-$R_D(n)$. We justify this name by noting that if the procedure terminates, it returns a string with no leading zeros (i.e., $\widehat{\alpha}$) equal to $R_D(n)$. We are not able to evaluate $R_D(n)$ for all values of n using this procedure because we have not yet described a way to recognize when $R_D(n) = \perp$. We proceed to do this now.

To decide if $D = \{0, 1, x\}$ is a NADS, it suffices to determine if there are any $n \in \mathbb{Z}^+$ for which Procedure 10 fails to terminate. We can determine if the procedure will terminate by examining the iterates of f_D.

Let n be a positive integer. Observe that, for $n \not\equiv 3 \pmod 4$, we have that

$$n > f_D(n) \geq 0 \ , \tag{3}$$

and, for $n \equiv 3 \pmod 4$, that

$$n > f_D(n) \iff n > \frac{-x}{3} \tag{4}$$

$$f_D(n) \geq 0 \iff n \geq x \ . \tag{5}$$

Since x is negative, we see that any iterate of the function f_D, on input n, always results in a nonnegative integer. Consider the graph G_n having directed edges

$$n \to f_D(n) \to {f_D}^2(n) \to {f_D}^3(n) \to \cdots \quad .$$

The vertices of G_n are nonnegative integers. Inequalities (3) and (4) tell us that there must be some vertex of G_n that is less than $\frac{-x}{3}$. Suppose ${f_D}^i(n) < \frac{-x}{3}$. We claim ${f_D}^{i+1}(n) < \frac{-x}{3}$ as well. This is clearly true if ${f_D}^i(n) \equiv 0, 1, 2 \pmod 4$. If ${f_D}^i(n) \equiv 3 \pmod 4$ then

$$\begin{aligned} {f_D}^i(n) < \frac{-x}{3} &\implies \frac{{f_D}^i(n) - x}{4} < \frac{\frac{-x}{3} - x}{4} \\ &\implies {f_D}^{i+1}(n) < \frac{-x - 3x}{12} = \frac{-x}{3} \ , \end{aligned}$$

and so the claim is true. The claim also tells us that if ${f_D}^i(n) < \frac{-x}{3}$, then any subsequent iterate of f_D must be less than $\frac{-x}{3}$.

From the preceding discussion it is clear that for a positive integer n, either:

1. G_n is a path terminating at 0, or
2. G_n contains a directed cycle of integers in the interval $\{1, 2, \ldots, \lfloor \frac{-x}{3} \rfloor\}$.

If we can detect a directed cycle in G_n then we can determine whether or not Procedure 10 will terminate on input n. To do this we need to compute and store some of the vertices of G_n. However, as Procedure 10 executes, it computes all the vertices of G_n, so we might as well modify the procedure to detect a directed cycle in G_n on its own. This modification is described as Algorithm 12.

Algorithm 12: EVAL-$R_D(n)$

$\alpha \leftarrow \epsilon$
while $n > \frac{-x}{3}$
  do $\begin{cases} \alpha \leftarrow g_D(n) \parallel \alpha \\ n \leftarrow f_D(n) \end{cases}$
$\mathcal{S} \leftarrow \varnothing$
while $n \neq 0$
  do $\begin{cases} \textbf{if } n \in \mathcal{S} \\ \quad \textbf{then return } \perp \\ \mathcal{S} \leftarrow \mathcal{S} \cup \{n\} \\ \alpha \leftarrow g_D(n) \parallel \alpha \\ n \leftarrow f_D(n) \end{cases}$
return $\widehat{\alpha}$

Now we can use the title "Algorithm" rather than "Procedure", because EVAL-$R_D(n)$ terminates for every $n \in \mathbb{Z}^+$. (For some positive integers, it was shown that EVAL$_\alpha$-$R_D(n)$ fails to terminate, which is why it cannot technically be called an algorithm.) As its name suggests, Algorithm 12 evaluates $R_D(n)$ for any $n \in \mathbb{Z}^+$. It is possible to show that the running time of EVAL-$R_D(n)$ is $O(\lg n + |x|)$.

Returning to our main task of recognizing when $\{0, 1, x\}$ is a NADS, Algorithm 12 and the preceding analysis are very helpful since they lead us to the following result:

Theorem 13. *Suppose x is a negative integer and $x \equiv 3 \pmod 4$. If every element in the set $\{n \in \mathbb{Z}^+ : n \leq \lfloor -x/3 \rfloor\}$ has a $\{0, 1, x\}$-NAF, then $\{0, 1, x\}$ is a NADS.*

Proof. From inspection of Algorithm 12 this result is almost immediate, however we can give a formal argument using the graph G_n.

Suppose the hypothesis is true. We must argue that $\{0, 1, x\}$ is a NADS. Take any $n \in \mathbb{Z}^+$ and consider the graph G_n. Suppose G_n contains a directed cycle. Let n_0 be a vertex in this cycle. Then $1 \leq n_0 \leq \lfloor -x/3 \rfloor$, and G_{n_0} must contain the same directed cycle. This implies that n_0 does not have a $\{0, 1, x\}$-NAF, contrary to our hypothesis. So, G_n is a path terminating at 0, and thus n has a $\{0, 1, x\}$-NAF. ∎

Theorem 13 suggests a computational method of determining if $\{0, 1, x\}$ is a NADS. For each $n \in \mathbb{Z}^+, n \leq \lfloor -x/3 \rfloor$, compute EVAL-$R_D(n)$. If all of these values have $\{0, 1, x\}$-NAFs then $\{0, 1, x\}$ is a NADS; otherwise, we find a value which does not have a $\{0, 1, x\}$-NAF which proves that $\{0, 1, x\}$ is not a NADS. To recognize a NADS, this method requires $\lfloor -x/3 \rfloor$ calls to EVAL-$R_D(n)$. However, we can decrease this number, as the next result shows.

Corollary 14. *Suppose x is a negative integer and $x \equiv 3 \pmod 4$. If every element in the set $\{n \in \mathbb{Z}^+ : n \leq \lfloor -x/3 \rfloor, n \equiv 3 \pmod 4\}$ has a $\{0, 1, x\}$-NAF, then $\{0, 1, x\}$ is a NADS.*

Proof. If $\{0, 1, x\}$ is not a NADS then choose the smallest integer $n_0 \in \mathbb{Z}^+$ such that G_{n_0} contains a directed cycle. By Theorem 13 it must be that $n_0 \leq \lfloor -x/3 \rfloor$. Let $n_1 = f_D(n_0)$, then (n_0, n_1) is an arc of G_n. If $n_0 \not\equiv 3 \pmod 4$ then $n_1 < n_0$ and G_{n_1} contains the same directed cycle, contrary to the choice of n_0. Thus, it must be that $n_0 \equiv 3 \pmod 4$. So, if the hypothesis is true, there can be no smallest positive integer which does not have a $\{0, 1, x\}$-NAF. Hence $\{0, 1, x\}$ is a NADS. ■

Now we can detect a NADS of the form $\{0, 1, x\}$ with about $\lfloor -x/12 \rfloor$ calls to EVAL-$R_D(n)$. An optimized version of an algorithm which utilizes this method is described in Algorithm 15. We have used this algorithm to find all the values of x greater than -10^6 such that $\{0, 1, x\}$ is a NADS; some of these values are listed in the Appendix.

Algorithm 15: IS-NADS(x)

$N \leftarrow 3$
$\mathcal{T} \leftarrow \varnothing$
while $N \leq \frac{-x}{3}$
do
  $n \leftarrow N$
  $\mathcal{S} \leftarrow \varnothing$
  while $n \neq 0$ **and** $n \notin \mathcal{T}$
  do
    if $n \in \mathcal{S}$
      then return "no"
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{n\}$
    $n \leftarrow f_D(n)$
  $N \leftarrow N + 4$
  $\mathcal{T} \leftarrow \mathcal{T} \cup \mathcal{S}$
return "yes"

5 Directed Graphs and NADS

For small values of x, a convenient way to demonstrate that $\{0, 1, x\}$ is a NADS is to draw a number of directed graphs. From the previous section, we know that $\{0, 1, x\}$ is a NADS if and only if each directed graph, G_n, $n \in \{1, 2, \ldots, \lfloor \frac{-x}{3} \rfloor\}$, is a path terminating at zero. If we define

$$G(x) := \bigcup_{n=1}^{\lfloor \frac{-x}{3} \rfloor} G_n \ ,$$

then we have that $\{0, 1, x\}$ is a NADS if and only if $G(x)$ is a directed tree rooted at zero. If $\{0, 1, x\}$ is not a NADS then $G(x)$ must contain a directed cycle. In this section we discuss some of the properties of $G(x)$; in particular, we

give a correspondence between strings in $\{00, 01, 0, 0x\}^*$ which represent nonzero multiples of Mersenne numbers and directed cycles of $G(x)$.

We start with an example. Let $x = -61$. Since $\lfloor \frac{-x}{3} \rfloor = 20$, $G(x)$ is the union of $G_1, G_2, \ldots G_{20}$. A drawing of $G(x)$ is given in Figure 1. In the appendix, it is

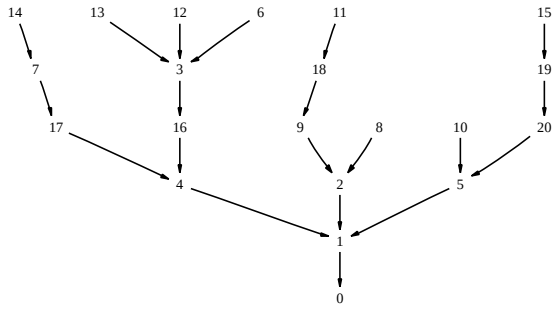

Fig. 1. $G(-61)$

noted that $\{0, 1, -61\}$ is a NADS and from Figure 1 we see that is indeed the case since $G(x)$ contains no directed cycle.

The function g_D, which was defined in (2), can be used to label the arcs of each of $G_1, G_2, \ldots G_{20}$ as follows:

$$n \xrightarrow{g_D(n)} f_D(n) \xrightarrow{g_D(f_D(n))} {f_D}^2(n) \xrightarrow{g_D({f_D}^2(n))} {f_D}^3(n) \xrightarrow{g_D({f_D}^3(n))} \cdots \quad .$$

Recall that g_D returns a string from the set $\{00, 01, 0, 0x\}$. These arc labels can be applied to $G(x)$, as shown in Figure 2.

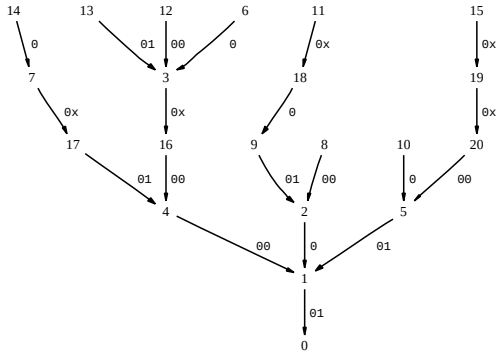

Fig. 2. $G(-61)$ with arc labels.

The arc labels on this drawing of $G(x)$ allow us to easily determine the D-NAF of any node of $G(x)$. If n is a node then, since $G(x)$ is a tree, there is a unique directed path from n to the root node (i.e., G_n). The sequence of arc labels on the reverse of this path identifies the $\{0, 1, x\}$-NAF for n. For example, if we let $n = 14$, then from Figure 2 the directed path from 14 to 0 is

$$14 \xrightarrow{0} 7 \xrightarrow{0x} 17 \xrightarrow{01} 4 \xrightarrow{00} 1 \xrightarrow{01} 0 \ .$$

If we read the sequence of arc labels above from right to left and concatenate them we get the string $01\|00\|01\|0x\|0$. It is easily verified that $14 = (0100010x0)_2$.

To see why this is true in general, suppose the path from n to 0 has length t and consider the label $g_D(n)$ on the arc $(n, f_D(n))$. From the definition of f_D and g_D we have

$$\begin{aligned} f_D(n) &= \frac{n - (g_D(n))_2}{2^{|g_D(n)|}} \\ \Longrightarrow \qquad n &= 2^{|g_D(n)|} f_D(n) + (g_D(n))_2 \ , \end{aligned} \tag{6}$$

where $|g_D(n)|$ denotes the length of the string $g_D(n)$. Replacing n by $f_D(n)$ in (6) we have

$$f_D(n) = 2^{|g_D(f_D(n))|} {f_D}^2(n) + (g_D(f_D(n)))_2 \ . \tag{7}$$

Substituting (7) into (6) we find

$$\begin{aligned} n &= 2^{|g_D(f_D(n))|+|g_D(n)|} {f_D}^2(n) + 2^{|g_D(n)|}(g_D(f_D(n)))_2 + (g_D(n))_2 \\ \Longrightarrow \ n &= 2^{|g_D(f_D(n))\|g_D(n)|} {f_D}^2(n) + (g_D(f_D(n))\|g_D(n))_2 \ . \end{aligned}$$

This method of substitution can be applied again. In (6), n can be replaced by ${f_D}^2(n)$ and then we can use this new equation to substitute for ${f_D}^2(n)$ above, and so on.

Let α be the string formed by concatenating the arc labels along the reverse of the path from n to 0. Then we have:

$$\alpha = g_D({f_D}^{t-1}(n))\| \cdots \|g_D({f_D}^2(n))\|g_D(f_D(n))\|g_D(n) \ .$$

From (6), it follows that

$$n = 2^{|\alpha|} {f_D}^t(n) + (\alpha)_2. \tag{8}$$

Since the length of the path from n to 0 is t, ${f_D}^t(n) = 0$, and thus

$$n = (\alpha)_2 \ ,$$

that is, α is a D-NAF for n.

The main result of this section concerns directed cycles in $G(x)$, so let us consider an example that contains a directed cycle. Let $x = -41$. This value of x is not listed in the appendix, so we expect that $\{0, 1, -41\}$ is not a NADS,

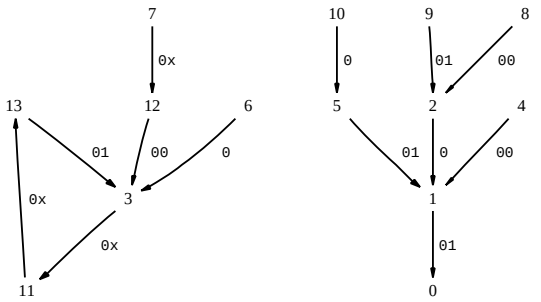

Fig. 3. $G(-41)$ with arc labels.

and the drawing of $G(x)$ in Figure 3 establishes this. Note, $G(x)$ consists of two components. Any node in the component of $G(x)$ which does not contain 0 does not have a D-NAF since there is no directed path from that node to 0.

Consider the directed cycle of $G(x)$. This cycle can be considered as a directed path from 3 to itself:

$$3 \xrightarrow{0x} 11 \xrightarrow{0x} 13 \xrightarrow{01} 3 \ .$$

Reading the sequence of arc labels above from right to left and concatenating them we get the string $01\|0x\|0x$. This string has length 6 and because of this we claim that $2^6 - 1$ must divide $(010x0x)_2$. Since $x = -41$, $(010x0x)_2 = -189$ and it is easy to check that this claim is valid. The following result provides an explanation.

Theorem 16. *Suppose x is a negative integer and $x \equiv 3 \pmod 4$. Then, $G(x)$ has a directed cycle if and only if $\exists \alpha \in \{00, 01, 0, 0x\}^*$ such that $(\alpha)_2 \neq 0$ and $2^{|\alpha|} - 1 \mid (\alpha)_2$.*

Proof. Suppose $G(x)$ has a directed cycle. Choose a node n in some directed cycle of $G(x)$ and let t be the length of this cycle. Then we have

$$n \xrightarrow{g_D(n)} f_D(n) \xrightarrow{g_D(f_D(n))} {f_D}^2(n) \to \cdots \to {f_D}^{t-1}(n) \xrightarrow{g_D({f_D}^{t-1}(n))} n \ .$$

Some node in this cycle must be congruent to 3 modulo 4. If not, then the iterates of f_D are strictly decreasing on this cycle and we get

$$n > f_D(n) > {f_D}^2(n) > \cdots > {f_D}^{t-1}(n) > n \ ,$$

which is a contradiction. A consequence of this fact is that one of the arcs in the cycle is labeled $0x$. As before, let

$$\alpha = g_D({f_D}^{t-1}(n))\| \cdots \|g_D({f_D}^2(n))\|g_D(f_D(n))\|g_D(n) \ .$$

Note, $(\alpha)_2 \neq 0$ because α contains the substring $0x$. Equation (8) gives us

$$n = 2^{|\alpha|} {f_D}^t(n) + (\alpha)_2 \ .$$

Since ${f_D}^t(n) = n$, we have

$$\begin{aligned} n &= 2^{|\alpha|}n + (\alpha)_2 \\ \implies -n(2^{|\alpha|} - 1) &= (\alpha)_2 \ . \end{aligned}$$

Thus, $(\alpha)_2 \neq 0$ and $2^{|\alpha|} - 1 \mid (\alpha)_2$, as required.

Suppose $\alpha \in \{00, 01, 0, 0x\}^*$ has the property that $(\alpha)_2 \neq 0$ and $2^{|\alpha|} - 1 \mid (\alpha)_2$. The string $0x$ must be a substring of α; otherwise, $0 < (\alpha)_2 < 2^{|\alpha|} - 1$, and this contradicts our hypothesis that $2^{|\alpha|} - 1 \mid (\alpha)_2$. We claim that we can assume $(\alpha)_2$ is odd. To see why, let α' be any left cyclic shift of α. For some $u \in \mathbb{Z}^+$, we have

$$\begin{aligned} (\alpha')_2 &\equiv 2^u(\alpha)_2 \pmod{2^{|\alpha|} - 1} \\ \implies (\alpha')_2 &\equiv 0 \pmod{2^{|\alpha|} - 1} \ , \end{aligned}$$

and since $|\alpha| = |\alpha'|$, this gives us that $2^{|\alpha'|} - 1 \mid (\alpha')_2$. Also, $(\alpha')_2 \neq 0$ because $(\alpha)_2 \neq 0$. Now, α contains the substring $0x$, so it must have some left cyclic shift that ends in 1 or x; that is, for some α', $(\alpha')_2$ is odd. Thus, if $(\alpha)_2$ is not odd, we can replace α by α' where $(\alpha')_2$ is odd.

Let $n = -\frac{(\alpha)_2}{2^{|\alpha|}-1}$. We will show n is in a directed cycle of $G(x)$. Since α contains the substring $0x$, $|\alpha| \geq 2$, and so we have the following:

$$\begin{aligned} & -n(2^{|\alpha|} - 1) = (\alpha)_2 \\ \implies \quad & n = 2^{|\alpha|}n + (\alpha)_2 \qquad (9) \\ \implies \quad & n \equiv (\alpha)_2 \pmod 4 \\ \implies \quad & \alpha = \alpha_1 \| g_D(n), \text{ where } \alpha_1 \in \{00, 01, 0, 0x\}^* \ . \end{aligned}$$

Using these implications, we can compute $f_D(n)$ as follows:

$$\begin{aligned} f_D(n) &= \frac{n - (g_D(n))_2}{2^{|g_D(n)|}} \\ &= \frac{2^{|\alpha|}n + (\alpha)_2 - (g_D(n))_2}{2^{|g_D(n)|}} \\ &= \frac{2^{|\alpha|}n + (\alpha_1 \| g_D(n))_2 - (g_D(n))_2}{2^{|g_D(n)|}} \\ &= 2^{|\alpha| - |g_D(n)|}n + (\alpha_1)_2 \\ &= 2^{|\alpha_1|}n + (\alpha_1)_2 \ . \qquad (10) \end{aligned}$$

Equation (10) is similar to equation (9). If $|\alpha_1| \geq 2$, the preceding arguments can be reapplied to compute ${f_D}^2(n)$. In doing so, we find

$${f_D}^2(n) = 2^{|\alpha_2|}n + (\alpha_2)_2 \ ,$$

where $\alpha_1 = \alpha_2 \| g_D(f_D(n))$ and $\alpha_2 \in \{00, 01, 0, 0x\}^*$. We can continue computing iterates of f_D in this manner until, for some $t \geq 1$, we obtain

$${f_D}^t(n) = 2^{|\alpha_t|}n + (\alpha_t)_2 \ ,$$

where $\alpha_{t-1} = \alpha_t \| g_D({f_D}^{t-1}(n))$, $\alpha_t \in \{00, 01, 0, 0x\}^*$ and $|\alpha_t| < 2$.

There are two cases to consider. If $|\alpha_t| = 0$ then it must be that $\alpha_t = \epsilon$, and thus

$$ {f_D}^t(n) = 2^0 n + (\epsilon)_2 = n \ . $$

Thus, n is in a directed cycle (of length t) in $G(x)$. If $|\alpha_t| = 1$ then it must be that $\alpha_t = 0$, and thus

$$ {f_D}^t(n) = 2^1 n + (0)_2 = 2n \ . $$

Recall that $(\alpha)_2$ is odd. Since $n = 2^{|\alpha|} n + (\alpha)_2$ and $|\alpha| \geq 2$, n is also odd. Thus, $2n \equiv 2 \pmod 4$ and so

$$ {f_D}^{t+1}(n) = \frac{2n}{2} = n \ . $$

Thus, n is in a directed cycle (of length $t+1$) in $G(x)$. ■

Theorem 16 gives a complete characterization of NADS, however, it is unclear if this characterization is helpful in finding values of x which make $\{0, 1, x\}$ a NADS. On the other hand, Theorem 16 is very useful for finding values of x for which $\{0, 1, x\}$ is not a NADS. We give some examples of this in the next section.

The remainder of this paper reads as follows. In Section 6, we give some infinite families of values for x for which D is *not* a NADS. In Section 7, we give some infinite families of values for x for which D is a NADS. We conclude by mentioning some additional problems related to NADS in Section 8.

6 Infinite Families of non-NADS

Consider the list of x values which appears in the Appendix. If we examine the first few entries of this list we find no multiples of 3. In fact, this is true of the whole list, and the same can be said of multiples of 7 and 31. These observations are a consequence of the following result:

Corollary 17. *Let x be a negative integer with $x \equiv 3 \pmod 4$. If $(2^s - 1) | x$ for any $s \geq 2$, then $\{0, 1, x\}$ is not a NADS.*

Proof. This result follows from Theorem 16, however it is just as easy to give a direct proof. Let $n = -x/(2^s - 1)$. We show G_n contains a directed cycle. We have

$$ \begin{aligned} & n(2^s - 1) \equiv -x \pmod 4 \\ \Longrightarrow\ & n(0 - 1) \equiv -3 \pmod 4 \\ \Longrightarrow\ & n \equiv 3 \pmod 4 \ . \end{aligned} $$

Note that,

$$ n - x = \frac{-x}{2^s - 1} - x = \frac{-x - x(2^s - 1)}{2^s - 1} = 2^s \frac{-x}{2^s - 1} = 2^s n \ . $$

Now,

$$f_D(n) = \frac{n-x}{4} = 2^{s-2}n$$

Subsequent iterates of f_D will cancel out the factor 2^{s-2}. Thus, for some i, ${f_D}^i(n) = n$ and so G_n contains a directed cycle. ■

Corollary 17 says that many sets $\{0, 1, x\}$ are not NADS. In particular, it rules out sets where x is divisible by 3, 7, 31, etc. Besides numbers of the form $2^s - 1, s \geq 2$, there are many other *non-allowable factors* of x. For example, if any of the integers

$$73, 85, 89, 337, 451, 1103, 1205, 1285, 2089$$

divides x then it is possible to show that, for a carefully chosen value of n, G_n contains a directed cycle. This technique of proof is not fully satisfying since it does little to elucidate why one integer is a non-allowable factor and another is not. A better approach is presented in the following corollary to Theorem 16.

Corollary 18. *Suppose x_0 is an integer. If $\exists \beta \in \{00, 0, 0x_0\}^*$ such that $(\beta)_2 \neq 0$ and $2^{|\beta|} - 1 \mid (\beta)_2$ then x_0 is a non-allowable factor.*

Proof. Notice there are no restrictions put on the integer x_0. Let x be a negative integer with $x \equiv 3 \pmod 4$ and $x_0 | x$. We must show $\{0, 1, x\}$ is not a NADS. Let α be the string formed by changing every occurrence of x_0 in β to x. It is easy to see that $(\alpha)_2 = \frac{x}{x_0}(\beta)_2$, $\alpha \in \{00, 0, 0x\}^*$ and $|\alpha| = |\beta|$. Now,

$$\begin{aligned} & 2^{|\beta|} - 1 \mid (\beta)_2 \\ \Longrightarrow\ & 2^{|\beta|} - 1 \mid \frac{x}{x_0}(\beta)_2 \\ \Longrightarrow\ & 2^{|\beta|} - 1 \mid (\alpha)_2 \\ \Longrightarrow\ & 2^{|\alpha|} - 1 \mid (\alpha)_2 \end{aligned}$$

Since $\alpha \in \{00, 01, 0, 0x\}^*$ and $(\alpha)_2 \neq 0$, by Theorem 16 we have that $\{0, 1, x\}$ is not a NADS. ■

We can use this result to generate non-allowable factors. All we need to do is find an integer x_0 and a string $\beta \in \{00, 0, 0x_0\}^*$, where β is not an all-zero string, such that $2^{|\beta|} - 1 \mid (\beta)_2$. To do this we first choose a string $\beta' \in \{00, 0, 01\}^*$ that is not an all-zero string. Now, we find an integer x_0 such that $2^{|\beta'|} - 1 \mid x_0(\beta')_2$. The smallest positive value of x_0 that satisfies this relation is

$$\frac{2^{|\beta'|} - 1}{\gcd(2^{|\beta'|} - 1, (\beta')_2)} .$$

We assign x_0 this value. If we change each occurrence of 1 in the string β' to x_0 we get a string $\beta \in \{00, 0, 0x_0\}^*$ such that $(\beta)_2 \neq 0$ and $2^{|\beta|} - 1 \mid (\beta)_2$.

So, by the corollary, x_0 is a non-allowable factor. Here is a short example. Let $\beta' = 000010101$. Then $|\beta'| = 9$, $(\beta')_2 = 21$, and so

$$x_0 = \frac{2^9 - 1}{\gcd(2^9 - 1, 21)} = 73 \ .$$

Thus, 73 is a non-allowable factor.

More generally, Theorem 16 be can used to generate infinite families of non-NADS which do not necessarily involve non-allowable factors. We know $\{0, 1, x\}$ is not an NADS if we can find a string $\alpha \in \{00, 01, 0, 0x\}^*$ such that $-n(2^{|\alpha|} - 1) = (\alpha)_2$. If we fix α and solve the resulting integer equation for x this will give us an infinite family of non-NADS. For example, suppose we fix $\alpha = 01010x0x$, then

$$\begin{aligned} & -n(2^{|\alpha|} - 1) = (01010x0x)_2 \\ \iff & -n(2^8 - 1) = (01010000)_2 + x(00000101)_2 \\ \iff & -255n = 80 + 5x \\ \iff & -51n = 16 + x \ . \end{aligned}$$

Thus, if $x \equiv -16 \pmod{51}$ then $\{0, 1, x\}$ cannot be a NADS.

Some of our first results on infinite families of non-NADS, which were discovered empirically, are unified as corollaries of Theorem 16. The following two results demonstrate this.

Corollary 19. *If* $\frac{3-x}{4} = 11 \cdot 2^i$*, where* $i \geq 0$*, then* $\{0, 1, x\}$ *is not a NADS.*

Proof. We have,

$$\begin{aligned} & \frac{3 - x}{4} = 11 \cdot 2^i \\ \implies & 3 - x = 11 \cdot 2^{i+2} \\ \implies & 11 - x = 11 \cdot 2^{i+2} + 8 \\ \implies & -11(2^{i+2} - 1) = 8 + x \\ \implies & -11(2^{i+2} - 1) = (0100x)_2 \ . \end{aligned}$$

The length of the string $0100x$ is 5. If $i + 2 \geq 5$ we can prepend zeros to $0100x$ and build a string α such that $|\alpha| = i + 2$; thus, by Theorem 16 we are done. If $i + 2 < 5$, it must be that $i = 0, 1, 2$.

When $i = 0$, $x = -41$ and from the drawing in Figure 3 we see $G(-41)$ has a directed cycle. When $i = 1$, $x = -85$ and then G_3 is a directed cycle:

$$3 \to 22 \to 11 \to 24 \to 6 \to 3 \ .$$

When $i = 2$, $x = -173$ and G_3 is also a directed cycle:

$$3 \to 44 \to 11 \to 46 \to 23 \to 49 \to 12 \to 3 \ .$$

In any case, $\{0, 1, x\}$ is not an NADS, as required. ■

Corollary 20. *Let* $\frac{3-x}{4} = 7 \cdot 2^i$*, where* $i \geq 0$*. Then* $\{0, 1, x\}$ *is an NADS if and only if* $i \in \{0, 1\}$*.*

Proof. We have,

$$\begin{aligned} & \frac{3-x}{4} = 7 \cdot 2^i \\ \Longrightarrow\ & 3 - x = 7 \cdot 2^{i+2} \\ \Longrightarrow\ & 7 - x = 7 \cdot 2^{i+2} + 4 \\ \Longrightarrow\ & -7(2^{i+2} - 1) = 4 + x \\ \Longrightarrow\ & -7(2^{i+2} - 1) = (010x)_2\ . \end{aligned}$$

Arguing as in the previous corollary, if $i + 2 \geq 4$ then by Theorem 16, $\{0, 1, x\}$ is not a NADS. If $i + 2 < 4$, it must be that $i = 0, 1$.

When $i = 0$, $x = -25$ and when $i = 1$, $x = -53$. By drawing the graphs $G(-25)$ and $G(-53)$, it is easy to verify that both of these values give NADSs (this is confirmed in the Appendix). ■

Not all infinite families of non-NADS are derived from Theorem 16. Consider the set of integers $\mathrm{NAF}(\{0, 1\})$. If this set is ordered, from smallest to largest, we sometimes notice large gaps between consecutive elements. One type of gap is described as follows. For $i \geq 0$, let

$$m_i := \begin{cases} 2 \cdot \frac{2^i - 1}{3} & \text{for } i \text{ even}, \\ \frac{2^{i+1} - 1}{3} & \text{for } i \text{ odd}. \end{cases}$$

Computing the first few values of m_i, we have

i	m_i
0	0
1	$1 = (1)_2$
2	$2 = (10)_2$
3	$5 = (101)_2$
4	$10 = (1010)_2$
5	$21 = (10101)_2$
6	$42 = (101010)_2$
7	$85 = (1010101)_2$
⋮	⋮

It is easy to see that if $a \in \mathrm{NAF}(\{0, 1\})$ then it is never true that $m_i < a < 2^i$. This observation gives us another infinite family.

Theorem 21. *Let* x *be an integer such that* $4m_i - 1 < -x < 3 \cdot 2^i$ *for some* $i \geq 0$*. If there exists* $n \in \{1, 2, \ldots \lfloor -x/3 \rfloor\}$ *with* $n \equiv 3 \pmod 4$ *then* $\{0, 1, x\}$ *is not a NADS.*

Proof. We can assume $x \equiv 3 \pmod 4$, since otherwise $\{0, 1, x\}$ cannot be a NADS. Suppose to the contrary that $\{0, 1, x\}$ is a NADS. Then, in the graph $G(x)$, there must be a directed path from n to 0. Let n_0 be the integer on this path that is *closest* to 0 and is congruent to 3 modulo 4. The arc labels on the path from n_0 to 0 give the $\{0, 1, x\}$-NAF for n_0. It must be that $n_0 = (\alpha \| 0x)_2$ with $\alpha \in \{00, 01, 0\}^*$ (if α contained the substring $0x$ this would contradict our choice of n_0).

Now,

$$\begin{aligned} & 1 \le n_0 \le -x/3 \\ \Longrightarrow\ & 1 \le (\alpha \| 0x)_2 \le -x/3 \\ \Longrightarrow\ & 1 \le 4(\alpha)_2 + x \le -x/3 \\ \Longrightarrow\ & \frac{1-x}{4} \le (\alpha)_2 \le \frac{-x/3 - x}{4} \\ \Longrightarrow\ & \frac{1-x}{4} \le (\alpha)_2 \le -x/3\ . \end{aligned}$$

By hypothesis, we have

$$\begin{aligned} & 4m_i - 1 < -x \quad \text{and} \quad -x < 3 \cdot 2^i \\ \Longrightarrow\ & m_i < \frac{1-x}{4} \quad \text{and} \quad \frac{-x}{3} < 2^i \end{aligned}$$

Thus, for some $i \ge 0$, we have

$$m_i < (\alpha)_2 < 2^i$$

which is a contradiction. Thus, $\{0, 1, x\}$ is not a NADS. ■

For example, if $i = 5$ then $-(4m_5 - 1) = -83$ and $-3 \cdot 2^5 = -96$. Theorem 21 tells us that no value of x with $-83 < x < -96$ can give a NADS. In addition, the proof of Theorem 21 also gives us some information about the graphs $G(x)$ for such values of x. For each of these graphs, in the component that contains 0 there can be no integer congruent to 3 modulo 4 (or equivalently, no arc label in this component can be $0x$). This property can be observed in $G(-85)$ which is drawn in Figure 4.

7 Infinite Families of NADS

If n is a nonnegative integer, $w(n)$ denotes the number of ones in the usual $\{0, 1\}$-radix 2 representation of n (i.e., the Hamming weight of n). We use the function $w(n)$ to describe two infinite families.

Theorem 22. *Let x be a negative integer with $x \equiv 3 \pmod 4$. If $w\left(\frac{3-x}{4}\right) = 1$, then $\{0, 1, x\}$ is a NADS.*

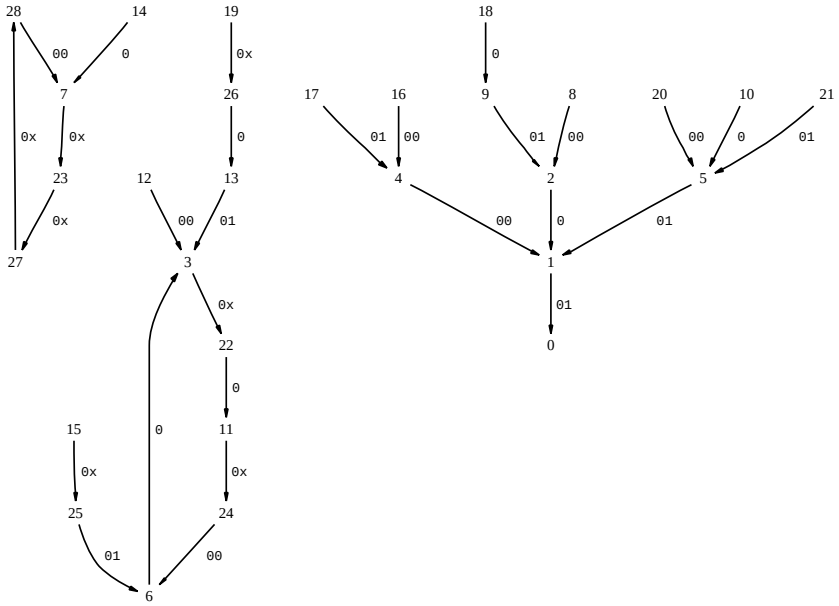

Fig. 4. $G(-85)$ with arc labels.

Proof. Suppose $\{0, 1, x\}$ is not a NADS. Then there is some $n \in \mathbb{Z}^+$ for which the graph G_n contains a directed cycle. We can assume n is a vertex of this cycle. Let t be the number of vertices in the cycle, then

$$n \to f_D(n) \to {f_D}^2(n) \to \cdots \to {f_D}^{t-1}(n) \to n \ .$$

Let $n' = f_D(n)$. We want to relate $w(n')$ to $w(n)$. There are four possible residues of n modulo 4, and for the residues $0, 1, 2$ we can determine $w(n')$ exactly:

$n \mod 4$	n'	$w(n')$
0	$\frac{n}{4}$	$w(n)$
1	$\frac{n-1}{4}$	$w(n)-1$
2	$\frac{n}{2}$	$w(n)$

If $n \equiv 3 \pmod 4$, we have

$$n' = \frac{n-x}{4} = \frac{n-3}{4} + \frac{3-x}{4} \ .$$

By hypothesis $w\left(\frac{3-x}{4}\right) = 1$, and so

$$\begin{aligned} w(n') &= w\left(\frac{n-3}{4} + \frac{3-x}{4}\right) \\ &\leq w\left(\frac{n-3}{4}\right) + w\left(\frac{3-x}{4}\right) \\ &= w(n) - 2 + 1 \\ &= w(n) - 1 \ . \end{aligned}$$

So, in any case, $w(n') \leq w(n)$, but if n is odd then we have the strict inequality $w(n') < w(n)$. Applying this inequality to the integers in the cycle of G_n we see

$$w(n) \geq w(f_D(n)) \geq w({f_D}^2(n)) \geq \cdots \geq w({f_D}^{t-1}(n)) \geq w(n) \ .$$

However, some vertex in this cycle must be congruent to 3 modulo 4. If not, then the iterates of f_D are strictly decreasing on this cycle and we get

$$n > f_D(n) > {f_D}^2(n) > \cdots > {f_D}^{t-1}(n) > n \ ,$$

which is a contradiction. So, there is some odd vertex in the cycle which means one of the inequalities relating the Hamming weights of adjacent vertices is strict. This implies that $w(n) > w(n)$, which is a contradiction.

So, G_n cannot contain a directed cycle, and hence $\{0, 1, x\}$ is a NADS. ■

When x is negative, $w(\frac{3-x}{4}) = 1$ if and only if $\frac{3-x}{4} = 2^t$, $t \geq 0$. Letting $t = 0, 1, 2, 3, 4, \ldots$ we see that Theorem 22 asserts that $x = \overline{1}, \overline{5}, \overline{13}, \overline{29}, \overline{61}, \ldots$ all yield NADS. Our next result also describes an infinite family using the function $w(n)$. However, when compared to the previous result, proving that $\{0, 1, x\}$ is a NADS for each x in this second infinite family seems to be more difficult.

Theorem 23. *Let x be a negative integer with $x \equiv 3 \pmod 4$. If $w\left(\frac{3-x}{4}\right) = 2$ and $2^s - 1$ does not divide x for any $s \in \mathbb{Z}^+$, $s \geq 2$, then $\{0, 1, x\}$ is a NADS.*

To prove this result we suppose x is a negative integer with $x \equiv 3 \pmod 4$ and $w\left(\frac{3-x}{4}\right) = 2$. We will argue that if $\{0, 1, x\}$ is not a NADS then it must be that $2^s - 1$ divides x for some $s \in \mathbb{Z}^+$, $s \geq 2$.

We begin our argument following the proof of Theorem 22. Suppose $\{0, 1, x\}$ is not a NADS. Then there is some $n \in \mathbb{Z}^+$ for which the graph G_n contains a directed cycle. We can assume n is a vertex of this cycle and, as described in Section 5, we can label the arcs of this cycle using the function g_D. Let t be the number of vertices in the cycle, then

$$n \xrightarrow{g_D(n)} f_D(n) \xrightarrow{g_D(f_D(n))} {f_D}^2(n) \to \cdots \to {f_D}^{t-1}(n) \xrightarrow{g_D({f_D}^{t-1}(n))} n \ .$$

Let $n' = f_D(n)$. We want to relate $w(n')$ to $w(n)$. There are four possible residues of n modulo 4, and for the residues $0, 1, 2$ we can determine $w(n')$ exactly:

$n \mod 4$	n'	$w(n')$
0	$\frac{n}{4}$	$w(n)$
1	$\frac{n-1}{4}$	$w(n) - 1$
2	$\frac{n}{2}$	$w(n)$

If $n \equiv 3 \pmod 4$, we have

$$n' = \frac{n-x}{4} = \frac{n-3}{4} + \frac{3-x}{4} \ .$$

By hypothesis $w\left(\frac{3-x}{4}\right) = 2$, and so

$$\begin{aligned} w(n') &= w\left(\frac{n-3}{4} + \frac{3-x}{4}\right) \\ &\leq w\left(\frac{n-3}{4}\right) + w\left(\frac{3-x}{4}\right) \\ &= w(n) - 2 + 2 \\ &= w(n) \ . \end{aligned}$$

So, in any case, $w(n') \leq w(n)$, but if $n \equiv 1 \pmod 4$ then we have the strict inequality $w(n') < w(n)$. Applying this inequality to the integers in the cycle of G_n we see

$$w(n) \geq w(f_D(n)) \geq w({f_D}^2(n)) \geq \cdots \geq w({f_D}^{t-1}(n)) \geq w(n) \ .$$

No vertex in this cycle can be congruent to 1 modulo 4; otherwise, one of the inequalities above would be strict and this would imply $w(n) > w(n)$, which is a contradiction. Also, at least one vertex in this cycle is congruent to 3 modulo 4; otherwise, by definition of f_D, the vertices would form a strictly decreasing integer sequence which would imply $n > n$, which is a contradiction.

Let α be the string formed by concatenating of the all the arc labels from the cycle:

$$\alpha = g_D({f_D}^{t-1}(n)) \| \cdots \| g_D({f_D}^2(n)) \| g_D(f_D(n)) \| g_D(n) \ .$$

Since α is a concatenation of strings from the set $\{00, 0, 0x\}$ it is nonadjacent, and further, for the same reason, every cyclic shift of α is also nonadjacent (i.e., α is *cyclically nonadjacent*). Equation (8) from Section 5 tells us

$$n = 2^{|\alpha|} {f_D}^t(n) + (\alpha)_2 \ .$$

Since ${f_D}^t(n) = n$, we have

$$n = 2^{|\alpha|} n + (\alpha)_2 \ . \tag{11}$$

The integer $(\alpha)_2$ is divisible by x. Let

$$A = \frac{(\alpha)_2}{x}, \quad \text{and} \quad a = |\alpha| \ .$$

From (11) we have

$$-xA \equiv 0 \pmod{2^a - 1} \ . \tag{12}$$

Since $w\left(\frac{3-x}{4}\right) = 2$, for some $u, v \in \mathbb{Z}$ we have

$$-x = 2^u + 2^v - 3, \quad u > v \geq 2 \ ,$$

and now (12) implies

$$(2^u + 2^v - 3)A \equiv 0 \pmod{2^a - 1}, \text{ where } u > v \geq 2 \ . \tag{13}$$

To finish the proof we need a lemma. Before we can introduce the lemma, we need a definition.

Definition 24. *An integer $B \in \mathbb{Z}$ is* length-ℓ cyclically nonadjacent *if $B \neq 0$ and there is a cyclically nonadjacent string $\beta \in \{0,1\}^\ell$ such that $(\beta)_2 = B$.*

Note that in this definition, the string β may have leading zeros. For example, 21 is length-6 cyclically nonadjacent (6-CNA, for short) since the string $010101 \in \{0,1\}^6$ is cyclically nonadjacent and $(010101)_2 = 21$. However, 21 is not 5-CNA because the only string in $\{0,1\}^5$ which gives a representation of 21 is 10101, but the cyclic shift 01011 of this string is not nonadjacent. Now we are ready for the lemma.

Lemma 25. *If B is length-ℓ cyclically nonadjacent and the congruence*

$$(2^u + 2^v - 3)B \equiv 0 \pmod{2^\ell - 1}$$

holds for some $u, v \in \mathbb{Z}$, $u > v \geq 2$, then either

$$\gcd(u, v-1) > 1 \quad \textit{or} \quad \gcd(u-1, v) > 1 \ .$$

Assuming, for the moment, the truth of Lemma 25, our proof of Theorem 23 continues as follows. The string α is cyclically nonadjacent, therefore so is the string formed by changing each occurrence of x in α to 1. This establishes that A is length-a cyclically nonadjacent, because $A = \frac{(\alpha)_2}{x}$. Now we can apply Lemma 25 to (13) and deduce, without loss of generality, that $\gcd(u, v-1) > 1$. Let $s = \gcd(u, v-1)$. Note that

$$-x = 2^u + 2^v - 3 = (2^u - 1) + 2(2^{v-1} - 1) \ .$$

Since $\gcd(2^u - 1, 2^{v-1} - 1) = 2^{\gcd(u,v-1)} - 1 = 2^s - 1$ we have that $2^s - 1 \mid x$, where $s \in \mathbb{Z}^+$ and $s \geq 2$, which is exactly what we wanted to show. (If x was chosen so as to satisfy all the conditions of Theorem 23, $2^s - 1$ cannot divide x, thus it must be that $\{0, 1, x\}$ is a NADS.) This concludes our proof of Theorem 23 , however we still have to deal with Lemma 25.

In proving Lemma 25, we will make use of the following easy result:

Lemma 26. *For any two nonempty subsets $S, T \subseteq \{0, 1, \ldots, \ell - 1\}$,*

$$\sum_{s \in S} 2^s \equiv \sum_{t \in T} 2^t \pmod{2^\ell - 1}$$

if and only if $S = T$.

Proof. We have $0 < \sum_{s\in S} 2^s \leq 2^\ell - 1$, and similarly for $\sum_{t\in T} 2^t$. Thus,

$$\begin{aligned} & \sum_{s\in S} 2^s \equiv \sum_{t\in T} 2^t \pmod{2^\ell - 1} \\ \iff & \sum_{s\in S} 2^s = \sum_{t\in T} 2^t \\ \iff & S = T \ . \end{aligned}$$

■

Proof (of Lemma 25). We fix some notation that will help describe our proof of Lemma 25. From now on, we let B be an integer which satisfies the hypothesis of Lemma 25. B is ℓ-CNA and we let $\beta = b_{\ell-1}\ldots b_1 b_0$ be the string in $\{0,1\}^\ell$ which establishes this. Further, let $S = \{i : b_i = 1\}$. For $k \in \mathbb{Z}$, define

$$S + k = \{(s + k) \mod \ell : s \in S\} \ .$$

The set $S + k$ is called a *translate* of S modulo ℓ. Using this notation, we have

$$\begin{aligned} & (2^u + 2^v - 3)B \equiv 0 \pmod{2^\ell - 1} \\ \iff & (2^u + 2^v)B \equiv 3B \pmod{2^\ell - 1} \\ \iff & (S + u) \cup (S + v) = (S + 1) \cup S \ , \end{aligned} \tag{14}$$

where the last equivalence follows from the fact that B is ℓ-CNA and Lemma 22. Because B is ℓ-CNA, the union on the right-hand side of (14), and hence also the left-hand side, is disjoint. We will establish Lemma 25 by analyzing this set equality.

We need one more concept. The *cyclic order* of B is the smallest positive integer k such that

$$2^k B \equiv B \pmod{2^\ell - 1} \ .$$

We denote this integer by $\overset{\hookrightarrow}{\mathrm{ord}}(B)$. Such an integer always exists since

$$2^\ell B \equiv B \pmod{2^\ell - 1} \ .$$

Using the quotient-remainder theorem, it is easy to show for any $m \in \mathbb{Z}^+$ that

$$2^m B \equiv B \pmod{2^\ell - 1} \iff \overset{\hookrightarrow}{\mathrm{ord}}(B) | m \ .$$

Applying this result, we see that $\overset{\hookrightarrow}{\mathrm{ord}}(B) | \ell$. (An equivalent definition of $\overset{\hookrightarrow}{\mathrm{ord}}(B)$ can be made by considering the string β. The smallest number of left cyclic shifts that, when applied to β, results in the string β is exactly $\overset{\hookrightarrow}{\mathrm{ord}}(B)$.)

We claim that we can assume $\overset{\hookrightarrow}{\mathrm{ord}}(B) = \ell$ in the hypotheses of Lemma 25. We justify this claim as follows. Let $k = \overset{\hookrightarrow}{\mathrm{ord}}(B)$ and suppose $k < \ell$. Since $k | \ell$ we can write $km = \ell$ for some positive integer m. Since B is ℓ-CNA we have

$$B = (2^{(m-1)k} + \cdots + 2^{2k} + 2^k + 1)B' = \frac{2^\ell - 1}{2^k - 1} B'$$

where $B' = (b_{k-1} \dots b_1 b_0)_2$, and B' is k-CNA. Now, for any positive integer j, we have

$$\begin{aligned} & 2^j B \equiv B \pmod{2^\ell - 1} \\ \iff & 2^j \frac{2^\ell - 1}{2^k - 1} B' \equiv \frac{2^\ell - 1}{2^k - 1} B' \pmod{\frac{2^\ell - 1}{2^k - 1}\, 2^k - 1} \\ \iff & 2^j B' \equiv B' \pmod{2^k - 1} \ , \end{aligned}$$

and so it must be that $\overset{\hookrightarrow}{\mathrm{ord}}(B') = k$ (i.e., $\overset{\hookrightarrow}{\mathrm{ord}}(B')$ is as large as possible). Also, we have

$$\begin{aligned} & (2^u + 2^v - 3)B \equiv 0 \pmod{2^\ell - 1} \\ \iff & (2^u + 2^v - 3)\, \frac{2^\ell - 1}{2^k - 1}\, B' \equiv 0 \pmod{\frac{2^\ell - 1}{2^k - 1}\, 2^k - 1} \\ \iff & (2^u + 2^v - 3)B' \equiv 0 \pmod{2^k - 1} \ . \end{aligned}$$

So if we can prove Lemma 25 for all B with $\overset{\hookrightarrow}{\mathrm{ord}}(B)$ as large as possible, then by the above arguments, it is true for all B.

Returning to the set equality described in (14), recall $S \subseteq \{0, 1, \dots, \ell - 1\}$. Since S is a subset of integers its elements can be ordered from smallest to largest. From S we define a sequence, $d(S)$, of differences modulo ℓ:

$$d(S) := (s_1 - s_0, s_2 - s_1, \dots, s_{p-1} - s_{p-2}, s_0 - s_{p-1})$$

where

$$S = \{s_0, s_1, \dots, s_{p-1}\} \quad \text{with} \quad s_0 < s_1 < \cdots < s_{p-1} \ .$$

Because B is ℓ-CNA, each of the differences in the sequence $d(S)$ must be at least 2. The definition of $d(S)$ can be extended to the translates of S. For any $k \in \mathbb{Z}$, $S + k$ can be considered as a subset of $\{0, 1, \dots, \ell - 1\}$ and hence it can also be ordered from smallest to largest. Thus, $d(S + k)$ can be defined in the same way as $d(S)$. It is easy to show that $d(S + k)$ is a cyclic shift of $d(S)$. Because of this property there are at most p different sequences of the form $d(S + k)$ where $p = |S|$. In fact, we can show there are exactly p such sequences.

Let

$$t_i := \ell - s_i \ , \quad \text{for} \ \ 0 \le i \le p - 1 \ .$$

The smallest element in each of the translates $S + t_0, S + t_1, \dots, S + t_{p-1}$ is equal to 0. Thus, for $i, j \in \{0, 1, \dots, p - 1\}$, we have

$$d(S + t_i) = d(S + t_j) \iff S + t_i = S + t_j \ .$$

Let $i \geq j$. Then we have

$$\begin{aligned} & S + t_i = S + t_j \\ \iff \quad & 2^{t_i} B \equiv 2^{t_j} B \pmod{2^\ell - 1} \\ \iff \quad & 2^{t_i - t_j} B \equiv B \pmod{2^\ell - 1} \\ \iff \quad & \overleftrightarrow{\text{ord}}(B) \mid (t_i - t_j) \\ \iff \quad & \ell \mid (t_i - t_j) \\ \iff \quad & t_i = t_j \ . \end{aligned}$$

So, each of the sequences $d(S + t_0), d(S + t_1), \ldots, d(S + t_{p-1})$ is distinct and hence there are exactly p different sequences of the form $d(S + k)$ where $k \in \mathbb{Z}$.

By applying a lexicographical ordering to the sequences $d(S + t_0), d(S + t_1), \ldots, d(S + t_{p-1})$ we can identify a *unique* smallest sequence. Let t^* be the value of t_i which corresponds to this smallest sequence. Note that

$$\begin{aligned} & (S + u) \cup (S + v) = (S + 1) \cup S \\ \iff \quad & \big((S + u) \cup (S + v)\big) + t^* = \big((S + 1) \cup S\big) + t^* \\ \iff \quad & (S + u + t^*) \cup (S + v + t^*) = (S + 1 + t^*) \cup (S + t^*) \ . \end{aligned} \tag{15}$$

We have $0 \in S + t^*$, so either $0 \in S + u + t^*$ or $0 \in S + v + t^*$. Without loss of generality we can assume $0 \in S + v + t^*$. We will show $S + v + t^* = S + t^*$.

Let

$$d(S + t^*) = (d_0, d_1, d_2, \ldots, d_{p-1}) \ ,$$

and note that

$$S + t^* = \{0, d_0, d_1 + d_0, d_2 + d_1 + d_0, \ldots\} \ .$$

Also, let

$$\begin{aligned} d(S + u + t^*) &= (u_0, u_1, u_2, \ldots, u_{p-1}) \\ d(S + v + t^*) &= (v_0, v_1, v_2, \ldots, v_{p-1}) \ . \end{aligned}$$

Since $d(S + t^*)$ is a lexicographically smallest sequence of the form $d(S + k)$ where $k \in \mathbb{Z}$, we have

$$d(S + t^*) \leq d(S + u + t^*) \quad \text{and} \quad d(S + t^*) \leq d(S + v + t^*) \ .$$

Recall $0 \in S + t^*$ and $0 \in S + v + t^*$. Since $0 \in S + t^*$, we have $1 \in S + 1 + t^*$. By (15), either $1 \in S + u + t^*$ or $1 \in S + v + t^*$. Suppose $1 \in S + v + t^*$. Then both 0 and 1 are elements of $S + v + t^*$. No two elements in any translate of S can have a difference of 1; otherwise, this contradicts the fact that B is ℓ-CNA. So, it must be that $1 \in S + u + t^*$.

We now know the smallest elements in each of the sets $S + u + t^*$, $S + v + t^*$, $S + 1 + t^*$, $S + t^*$. The next smallest element of $S + t^*$ is d_0. Again, by (15), either $d_0 \in S + u + t^*$ or $d_0 \in S + v + t^*$. Suppose $d_0 \in S + u + t^*$.

Then, since both 1 and d_0 are in $S+u+t^*$ and 1 is the smallest element of this set, we have

$$u_0 \le d_0 - 1 < d_0 \ .$$

However, $d(S+t^*) \le d(S+u+t^*)$ implies that $d_0 \le u_0$ which gives a contradiction. So, it must be that $d_0 \in S+v+t^*$, and hence, $d_0+1 \in S+u+t^*$.

From our lexicographical ordering we have $d_0 \le v_0$. Since the smallest element of $S+v+t^*$ is 0 and d_0 is also in this set, we have

$$v_0 \le d_0 - 0 = d_0 \ .$$

Hence, $v_0 = d_0$. Similarly,

$$d_0 \le u_0 \quad \text{and} \quad u_0 \le (d_0+1) - 1 = d_0 \ ,$$

and so $u_0 = d_0$. From these two equalities, we have that d_0 and d_0+1 are the second smallest elements of the sets $S+v+t^*$ and $S+u+t^*$, respectively. Further, our lexicographical ordering now implies that $d_1 \le v_1$ and $d_1 \le u_1$.

The next smallest element of $S+t^*$ is d_1+d_0. Either $d_1+d_0 \in S+u+t^*$ or $d_1+d_0 \in S+v+t^*$. Suppose $d_1+d_0 \in S+u+t^*$. This implies that

$$u_1 \le (d_1+d_0) - (d_0+1) = d_1 - 1 < d_1 \ ,$$

which is a contradiction. So, $d_1+d_0 \in S+v+t^*$, and hence, $d_1+d_0+1 \in S+u+t^*$.

We now have

$$d_1 \le v_1 \quad \text{and} \quad v_1 \le (d_1+d_0+1) - (d_0+1) = d_1 \ ,$$

so $v_1 = d_1$. Also

$$d_1 \le u_1 \quad \text{and} \quad u_1 \le (d_1+d_0) - d_0 = d_1 \ ,$$

and so $u_1 = d_1$. Thus we can identify the third smallest elements of the sets $S+v+t^*$ and $S+u+t^*$. Further, we have that $d_2 \le v_2$ and $d_2 \le u_2$.

By repeating the previous arguments, we can show that each element of $S+t^*$, from smallest to largest, must also be an element of $S+v+t^*$. Thus, $S+v+t^* = S+t^*$ and so $S+v = S$. In (14), the union operations are both disjoint, hence $S+v=S$ implies $S+u = S+1$. Now,

$$\begin{aligned} & S+v = S \\ \Longrightarrow \quad & 2^v B \equiv B \pmod{2^\ell - 1} \\ \Longrightarrow \quad & \overset{\hookrightarrow}{\mathrm{ord}}(B) \mid v \\ \Longrightarrow \quad & \ell \mid v \ . \end{aligned}$$

And similarly, $\ell \mid (u-1)$. Thus $\gcd(u-1, v) \ge \ell > 1$. This proves the lemma. ■

Looking at an example can help us connect the different steps in the proof of Theorem 23. Suppose $x = 3-(2^u+2^v)$ with $u > v \ge 2$. If $\{0, 1, x\}$ is not a NADS

then $\exists \alpha \in \{00, 01, 0, 0x\}^*$ such that $(\alpha)_2 \equiv 0 \pmod{2^{|\alpha|} - 1}$. By the definition of x, it must be that $\alpha \in \{00, 0, 0x\}^*$. We will suppose $\alpha = 0x0x000x0x0x000x$, and so $|\alpha| = 16$. Now,

$$\begin{aligned}
(0x0x000x0x0x000x)_2 &\equiv 0 \pmod{2^{16} - 1} \\
\implies x(01010001 \| 01010001)_2 &\equiv 0 \pmod{2^{16} - 1} \\
\implies (2^u + 2^v - 3)(2^8 + 1)(01010001)_2 &\equiv 0 \pmod{2^{16} - 1} \\
\implies (2^u + 2^v - 3)(01010001)_2 &\equiv 0 \pmod{2^8 - 1} \\
\implies (2^u + 2^v) \cdot 81 &\equiv (2^1 + 2^0) \cdot 81 \pmod{2^8 - 1} .
\end{aligned}$$

Note that $(01010001)_2 = 81$ is 8-CNA, and $\overleftrightarrow{\text{ord}}(81) = 8$. Let $S = \{0, 4, 6\}$, then $d(S) = (4, 2, 2)$ and $d(S + 4) = (2, 2, 4)$ which is the lexicographically smallest cyclic shift of $d(S)$. Continuing from our last implication,

$$\begin{aligned}
\implies (S + u) \cup (S + v) &= (S + 1) \cup S \\
\implies (S + u + 4) \cup (S + v + 4) &= (S + 5) \cup (S + 4) \\
\implies (S + u + 4) \cup (S + v + 4) &= \{1, 3, 5\} \cup \{0, 2, 4\} .
\end{aligned}$$

We can assume that $0 \in S + v + 4$, and then it must be that $1 \in S + u + 4$. If $2 \in S+u+4$, this would contradict the fact that $(2, 2, 4)$ is the smallest difference sequence of all translates of S. Thus, $2 \in S + v + 4$ and then $3 \in S + u + 4$. Similarly, $4 \in S + v + 4$ and $5 \in S + u + 4$. Thus,

$$\begin{aligned}
S + u + 4 = S + 5 \quad &\text{and} \quad S + v + 4 = S + 4 \\
\implies u \equiv 1 \pmod 8 \quad &\text{and} \quad v \equiv 0 \pmod 8 .
\end{aligned}$$

Now, $-x = 2^u + 2^v - 3 = 2(2^{u-1} - 1) + (2^v - 1)$. Since $2^8 - 1 | 2^{u-1} - 1$ and $2^8 - 1 | 2^v - 1$, we have $2^8 - 1 | x$. So, if $\{0, 1, x\}$ is not a NADS, then it must be that x is divisible by a Mersenne number.

If we take $u, v \in \{2, 3, 4, 5, 6, 7, 8\}$ with $u \neq v$ and set $x = 3 - (2^u + 2^u)$ then, after eliminating multiples of Mersenne numbers, Theorem 23 tells us that each of the values $-17, -37, -65, -157, -257, -269, -317$ makes $\{0, 1, x\}$ a NADS.

Looking at Theorems 22 and 23, a natural question to ask is if there is an infinite family of NADS with the property that $w(\frac{3-x}{4}) = 3$. One of our results gives a partial answer to this question. If $\frac{3-x}{4} = 11 \cdot 2^i$ with $i \geq 0$, then $w(\frac{3-x}{4}) = 3$, however Corollary 19 tells us that such a value of x will never give a NADS.

8 Further Work and Comments

It is possible to show that for $n \in \mathbb{Z}^+$ with $n \leq \lfloor -x/3 \rfloor$, the running time of EVAL-$R_D(n)$, as described in Algorithm 12, is $O(|x|/3) = O(|x|)$. Thus, to compute EVAL-$R_D(n)$ for all positive integers in this range takes time $O(|x|^2)$. So, we can decide if $\{0, 1, x\}$ is a NADS in $O(|x|^2)$ time. The running time can be

reduced to $O(|x|)$ if more memory is used, and this is the approach taken in Algorithm 15. However, since the size of the input to this algorithm is $\lg |x|$, the running time is exponential. It would be interesting to determine if there is a polynomial-time algorithm for deciding if $\{0, 1, x\}$ is a NADS.

Of the non-allowable factors of x that we discussed, perhaps the more interesting variety of these integers are those for which none of their proper divisors are non-allowable factors. We call a non-allowable factor *simple* if it has this property. It would be interesting to know if there are an infinite number of simple non-allowable factors. Also, it would be interesting to determine if all non-allowable factors can be discovered via Corollary 18.

Some of our results on NADS appear to have analogs in Matula's theory on basic digit sets (see [4]). In particular, our Theorem 13 corresponds to Matula's Lemma 6, and our Theorem 16 corresponds to Matula's Theorem 5. It would be interesting to find other connections between the two works. It might be that our Theorems 22 and 23, which do not appear to have analogs in [4], could lead to some new results in the theory of basic digit sets.

References

1. A. D. Booth. A Signed Binary Multiplication Technique, *Quarterly Journal of Mechanics and Applied Mathematics* **4** (1951), 236–240.
2. D. M. Gordon. A Survey of Fast Exponentiation Methods, *Journal of Algorithms* **27** (1998), 129–146.
3. J. Jedwab and C. J. Mitchell. Minimum Weight Modified Signed-Digit Representations and Fast Exponentiation, *Electronic Letters* **25** (1989), 1171–1172.
4. D. W. Matula. Basic Digit Sets for Radix Representation, *Journal of the Association for Computing Machinery*, **29** (1982), 1131–1143.
5. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1996.
6. F. Morain and J. Olivos. Speeding up the Computations on an Elliptic Curve using Addition-Subtraction Chains, *RAIRO Theoretical Informatics and Applications* **24** (1990), 531–543.
7. G. W. Reitwiesner. Binary Arithmetic, In *Advances in Computers, Vol. 1*, Academic Press, 1960, pp. 231–308.
8. J. A. Solinas. Low-Weight Binary Representations for Pairs of Integers. Technical Report CORR 2001-41, Centre for Applied Cryptographic Research. Available from `http://www.cacr.math.uwaterloo.ca/techreports/-2001/corr2001-41.ps`.
9. J. A. Solinas. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In "Advances in Cryptology – CRYPTO '97", *Lecture Notes in Computer Science* **1294** (1997), 357–371. An extended version of the paper is available from `http://www.cacr.math.uwaterloo.ca/techreports/1999/corr99-46.ps`.
10. J. A. Solinas. Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography* **19** (2000), 195–249.

A Some values of x which give NADS

We list the all values of x from -1 to -10000 for which $\{0, 1, x\}$ is a NADS:

-1	-505	-1133	-2129	-2669	-4133	-4777	-7333	-8201	-8797
-5	-509	-1145	-2137	-2677	-4141	-4801	-7345	-8213	-8825
-13	-517	-1165	-2141	-2693	-4145	-5021	-7381	-8221	-8837
-17	-521	-1265	-2153	-3245	-4153	-5077	-7393	-8233	-8921
-25	-533	-1273	-2161	-3265	-4157	-5093	-7397	-8237	-8977
-29	-541	-1277	-2165	-3337	-4201	-5101	-7465	-8297	-9089
-37	-557	-1289	-2173	-3385	-4205	-5105	-7477	-8305	-9101
-53	-565	-1297	-2185	-3421	-4217	-5113	-7561	-8317	-9133
-61	-601	-1325	-2189	-3509	-4253	-5129	-7597	-8333	-9157
-65	-605	-1345	-2197	-3541	-4261	-5137	-7613	-8341	-9161
-113	-613	-1349	-2237	-3557	-4273	-5153	-7621	-8369	-9181
-121	-629	-1357	-2273	-3629	-4285	-5165	-7649	-8417	-9209
-125	-641	-1621	-2285	-3653	-4297	-5189	-7741	-8429	-9221
-137	-653	-1637	-2293	-3673	-4337	-5197	-7817	-8437	-9245
-145	-673	-1733	-2297	-3761	-4345	-5213	-7865	-8441	-9341
-149	-821	-1745	-2321	-3797	-4349	-5273	-7877	-8453	-9353
-157	-869	-1765	-2353	-3853	-4373	-5281	-7901	-8485	-9421
-233	-913	-1885	-2365	-3877	-4393	-5365	-7949	-8497	-9425
-241	-937	-1933	-2369	-3881	-4397	-5377	-8045	-8501	-9433
-253	-977	-1949	-2381	-3917	-4469	-5381	-8053	-8573	-9461
-257	-989	-1985	-2393	-3925	-4537	-5393	-8065	-8581	-9473
-265	-1013	-1993	-2405	-3929	-4541	-5405	-8069	-8593	-9497
-269	-1021	-2017	-2425	-3961	-4573	-5437	-8081	-8597	-9505
-277	-1025	-2021	-2497	-4001	-4589	-5441	-8093	-8665	-9509
-281	-1033	-2033	-2525	-4033	-4597	-6565	-8101	-8669	-9581
-305	-1037	-2041	-2533	-4037	-4601	-6613	-8117	-8681	-9665
-317	-1045	-2045	-2557	-4085	-4621	-6773	-8129	-8693	-9673
-325	-1061	-2053	-2593	-4093	-4633	-6805	-8165	-8717	-9677
-437	-1073	-2069	-2609	-4097	-4645	-6929	-8173	-8725	-9697
-481	-1081	-2101	-2621	-4105	-4649	-6973	-8177	-8741	-9761
-485	-1097	-2105	-2641	-4117	-4661	-7033	-8185	-8753	-9925
-493	-1117	-2113	-2645	-4121	-4693	-7277	-8189	-8789	-9997