ON MINIMAL EXPANSIONS IN REDUNDANT NUMBER SYSTEMS: ALGORITHMS AND QUANTITATIVE ANALYSIS

CLEMENS HEUBERGER AND HELMUT PRODINGER

Abstract. We consider digit expansions in base $q \geq 2$ with arbitrary integer digits such that the length of the expansion plus the sum of the absolute values of the digits is minimal. Since this does not determine a unique minimal representation, we describe some reduced minimal expansions.

We completely characterize its syntactical properties, give a simple algorithm to compute the reduced minimal expansion and a formula to compute a single digit without having to compute the others, and we calculate the average cost of such an expansion.

1. Introduction

On several occasions, representations of integers in redundant number systems have been studied. The motivation usually comes from various applications where "better" representations of an integer result in faster computations.

We give an example from public key cryptography using elliptic curves: These cryptosystems rely on the fact that it is rather easy to compute a multiple nP of a given point on an elliptic curve $E(\mathbb{F}_q)$, but there is no known efficient way to calculate n from the knowledge of P and nP. Of course, if the computation of nP can be done even faster, larger values of the parameters can be chosen in order to make the system less vulnerable. The usual way to calculate nP is a repeated doubling and addition algorithm, see Knuth [12]. As it was remarked by Morain and Olivos [13], a repeated doubling and addition or subtracting scheme can be applied using a representation $n = \sum_{i=0}^{l} \varepsilon_i 2^i$ where $\varepsilon_i \in \{0, \pm 1\}$. The time to compute nP decreases as $l + 1 + \sum_i |\varepsilon_i|$ decreases, since it is as easy to add a point on an elliptic curve as to subtract it.

Additionally, in the last years differential power analysis of cryptosystems has attracted attention: it tries to recover secret keys by monitoring power signals of cryptographic devices. Since in the usual doubling and addition scheme it can easily be detected whether an addition and a doubling or a doubling alone takes place, the binary representation of n can be guessed. But if digits ± 1 are used, a potential attacker can gain less information. We refer to Coron [4] for further discussions.

The first author has been partially supported by the Spezialforschungsbereich F 003 "Optimierung und Kontrolle"/Projektbereich Diskrete Optimierung.

This motivates the study of representations of an integer n in base $q \geq 2$ with arbitrary digits, and we will denote the set of such representations by

$$R_q(n) := \left\{ \varepsilon = (\varepsilon_0, \dots, \varepsilon_l) : l \in \mathbb{N}, \varepsilon_i \in \mathbb{Z}, n = \sum_{i=0}^{l} \varepsilon_i q^i \right\}. \tag{1.1}$$

We define the *cost of a representation* $\varepsilon \in R_q(n)$ as

$$c(\varepsilon) = c(\varepsilon_0, \dots, \varepsilon_l) := l + 1 + \sum_{i=0}^{l} |\varepsilon_i| \tag{1.2}$$

and look for representations of n with minimum cost.

At several places in this paper, we will also consider a modified cost function, which we will call *relaxed costs,* namely

$$c'(\varepsilon) = c'(\varepsilon_0, \dots, \varepsilon_l) := \sum_{i=0}^{l} |\varepsilon_i| . \tag{1.3}$$

We note that in general there is no unique minimal representation: Both $(-1, 2) \in R_3(5)$ and $(2, 1) \in R_3(5)$ are representations of 5 in base 3 with cost $c(-1, 2) = c(2, 1) = 5$. It will be a consequence of Theorem 1 that there are no cheaper expansions in $R_3(5)$.

Our first aim in Section 2 is to describe a special minimal representation (which we will call a reduced representation), which will be unique (cf. Theorem 1). The proof of uniqueness will immediately give an efficient algorithm to compute the reduced representation (cf. Algorithm 1). The corresponding results for relaxed costs and the conversion rules between the two representations will be discussed in Section 3.

In Sections 4 and 5 we will give an explicit formula for the digits of the reduced representation in the case of odd and even q, respectively. These formulæ will be very useful for the computation of the frequencies of digits and the expected costs of the representations, as will be shown in Section 6.

An overview on previous work in this area is postponed to Section 7, where all required definitions will be available.

We assume without loss of generality that $n > 0$. The following notations will be used throughout the paper: the set of nonnegative integers is $\mathbb{N} := \{0, 1, \dots\}$, by $\{x\} := x - \lfloor x \rfloor$ we denote the fractional part of a real number x, for a set A, A^+ is defined as $\bigcup_{n\geq 1} A^n$, and & is the concatenation function $\& : A^+ \times A \to A^+$; $(a_0, \dots, a_l) \,\&\, a_{l+1} := (a_0, \dots, a_l, a_{l+1})$. As usual, the minimum of the empty set is defined as ∞. We write $\log_q(n) := \log(n)/\log(q)$ for the logarithm to base q. We will use Iverson's convention as in [7], i. e. for any expression *expr*, $[expr] = 1$ if *expr* is true and $= 0$ otherwise.

2. Reduced Representations

Let $n > 0$ and $q \geq 2$ be fixed. We will describe "reduction rules" of the shape $(\eta_0, \dots, \eta_r) \to (\eta'_0, \dots, \eta'_r)$. To apply such a rule to a representation ε means to replace the first occurrence (from the left, i. e. the least significant digits) of $(\eta_0, \dots, \eta_r)$

in ε by $(\eta'_0, \dots, \eta'_s)$. Additionally, reduction rules $(\eta_0, \dots, \eta_r) \twoheadrightarrow (\eta'_0, \dots, \eta'_s)$ will occur, which we are only allowed to apply at the end of the representation, i. e. if $\varepsilon = (\varepsilon_0, \dots, \varepsilon_{l-r-1}, \eta_0, \dots, \eta_r)$. Note that in the case of rules at the end, the length of the representation may change. We emphasize that a reduction rule must be applied at the first occurrence of the pattern.

Furthermore, define $f : R_q(n) \to R_q(n)$ in the following way: Given $\varepsilon = (\varepsilon_0, \dots, \varepsilon_l) \in R_q(n)$, try the following reduction rules (in the given order) until ε first changes and return this result.

(2.1) $(0) \twoheadrightarrow ()$.
(2.2) For $|\eta_0| > q/2$, $\eta_1 \in \mathbb{Z}$, and $u := \lceil |\eta_0|/q - 1/2 \rceil$: $(\eta_0, \eta_1) \to (\eta_0 - uq\operatorname{sign}(\eta_0), \eta_1 + u\operatorname{sign}(\eta_0))$.
(2.3) For $|\eta_0| > (q+1)/2$ and $u := \lceil |\eta_0|/q - 1/2 \rceil$: $(\eta_0) \twoheadrightarrow (\eta_0 - uq\operatorname{sign}(\eta_0), u\operatorname{sign}(\eta_0))$.
(2.4) For $2 \nmid q$: $(-(q-1)/2, 1) \twoheadrightarrow ((q+1)/2)$.
(2.5) For $2 \mid q$: $(-q/2, -q/2+1, 1) \twoheadrightarrow (q/2, q/2)$.
(2.6) For $\eta_0 < 0$ and $2 \mid q$: $(q/2, \eta_0) \to (-q/2, \eta_0 + 1)$.
(2.7) For $\eta_0 > 0$ and $2 \mid q$: $(-q/2, \eta_0) \to (q/2, \eta_0 - 1)$.
(2.8) For $\eta_0 < q/2$ and $2 \mid q$: $(q/2, q/2, \eta_0) \to (-q/2, -q/2+1, \eta_0 + 1)$.
(2.9) For $-q/2 < \eta_0$ and $2 \mid q$: $(-q/2, -q/2, \eta_0) \to (q/2, q/2 - 1, \eta_0 - 1)$.
(2.10) For $2 \mid q$: $(q/2, q/2, q/2) \twoheadrightarrow (-q/2, -q/2+1, -q/2+1, 1)$.

We note that f is well defined since all of the above reduction rules indeed transform representations of n to representations of n.

We say that $\varepsilon \in \mathbb{N}^+$ is *reduced* if $f(\varepsilon) = \varepsilon$. This is the case if and only if the following holds:

(2.11) There are no trailing zeros.
(2.12) $-q/2 \le \varepsilon_i \le q/2$ for $0 \le i \le l-1$ and $|\varepsilon_l| \le (q+1)/2$.
(2.13) The sequence does not end on $(-(q-1)/2, 1)$ or $(-q/2, -q/2+1, 1)$.
(2.14) If $\varepsilon_i = q/2$ then $0 \le \varepsilon_{i+1} \le q/2 - 1$ except when $i = l-1$, where only $0 \le \varepsilon_{i+1} \le q$ is required, or when $i = l$.
(2.15) If $\varepsilon_i = -q/2$ then $-q/2+1 \le \varepsilon_{i+1} \le 0$ (except when $i = l$).

Lemma 1. *Given $\varepsilon \in R_q(n)$. Then the sequence defined by*

$$\varepsilon^{(0)} := \varepsilon, \qquad \varepsilon^{(i+1)} := f(\varepsilon^{(i)}) \qquad \text{for } i \ge 0$$

stabilizes, i. e. there is some $m \ge 0$ such that $\varepsilon^{(i)} = \varepsilon^{(m)}$ for all $i \ge m$.

Additionally, $c(\varepsilon^{(i+1)}) \le c(\varepsilon^{(i)})$ for $i \ge 0$.

Proof. We define $\omega : \mathbb{Z}^+ \to (\mathbb{Z} \cup \infty)^8$ by

$$\begin{aligned}\varepsilon = (\varepsilon_0, \dots, \varepsilon_l) \mapsto \big(c(\varepsilon), &\\ & - \min\{0 \le i \le l : |\varepsilon_i| > q/2\},\\ & - \min\{0 \le i \le l : |\varepsilon_i| > (q+1)/2\},\\ & \operatorname{card}\{0 \le i \le l : |\varepsilon_i| = q/2\},\\ & - \min\{0 \le i \le l-1 : (\varepsilon_i, \varepsilon_{i+1}) = (q/2, q/2)\},\\ & \min\{1 \le i \le l-1 : \exists \eta_0 < q/2 : (\varepsilon_{i-1}, \varepsilon_i, \varepsilon_{i+1}) = (q/2, q/2, \eta_0)\},\\ & - \min\{0 \le i \le l-1 : (\varepsilon_i, \varepsilon_{i+1}) = (-q/2, -q/2)\},\\ & \min\{1 \le i \le l-1 : \exists \eta_0 > -q/2 : (\varepsilon_{i-1}, \varepsilon_i, \varepsilon_{i+1}) = (-q/2, -q/2, \eta_0)\}\big)\end{aligned}$$

and $\prec$ to be the relation on $\mathbb{Z}^+$ defined by

$$\varepsilon \prec \varepsilon' :\iff \omega(\varepsilon) <_{lex} \omega(\varepsilon').$$

It is straightforward to prove that for all $\varepsilon \in R_q(n)$

$$f(\varepsilon) = \varepsilon \text{ or } f(\varepsilon) \prec \varepsilon; \tag{2.16}$$

we show the most complicate case only, namely the rule (2.9).

Let

$$\begin{aligned}\varepsilon &= (\varepsilon_0, \dots, \varepsilon_{m-1}, -q/2, -q/2, \eta_0, \varepsilon_{m+3}, \dots, \varepsilon_l),\\ \varepsilon' &= (\varepsilon_0, \dots, \varepsilon_{m-1}, q/2, q/2-1, \eta_0 - 1, \varepsilon_{m+3}, \dots, \varepsilon_l).\end{aligned}$$

Since rule (2.7) could not be applied (in that case, we would not have been allowed to apply (2.9)), we have $\eta_0 \le 0$ and therefore $-q/2 \le \eta_0 - 1 < 0$.

We calculate that $c(\varepsilon') - c(\varepsilon) = -1 + |\eta_0 - 1| - |\eta_0| = 0$. Since $2 \mid q$ and rules (2.2) and (2.3) could not be applied, all $|\varepsilon_i|, |\varepsilon_i'| \le q/2$ and $\omega_2(\varepsilon) = \omega_2(\varepsilon') = \omega_3(\varepsilon) = \omega_3(\varepsilon') = -\infty$.

We see that $\omega_4(\varepsilon') \le \omega_4(\varepsilon)$ with equality if and only if $\eta_0 = -q/2 + 1$.

We note that $\varepsilon_{m-1} = q/2$ cannot happen (either since $m = 0$ or since rule (2.6) would have been applied), therefore, the positions of blocks $(q/2, q/2)$ have not been changed, and we obtain $\omega_5(\varepsilon') = \omega_5(\varepsilon)$ and $\omega_6(\varepsilon') = \omega_6(\varepsilon)$.

Let $s := -\omega_7(\varepsilon)$. Obviously $s \le m$. If $s \ge m-1$ then we have $-\omega_7(\varepsilon') > s$, otherwise, we have $-\omega_7(\varepsilon') = s$, but $\omega_8(\varepsilon) = m+1 > \omega_8(\varepsilon') = m-1$. Therefore, (2.16) is proved for rule (2.9).

Since the maximum length of the occurring representations is bounded by $c(\varepsilon^{(0)})$, $\omega(\varepsilon^{(i)})$ lies in the finite set

$$\{-\infty, -c(\varepsilon^{(0)}), \dots, 0, \dots, c(\varepsilon^{(0)}), \infty\}^8$$

for $i \ge 0$ and there must be an $m \ge 0$ with the required properties. ∎

Lemma 2. *Let n, q be fixed and $\varepsilon \in R_q(n)$ be reduced. Let $a := n \bmod q$ and $b := (n-a)/q \bmod q$. Then*

$$\varepsilon_0 = \begin{cases} a & \text{if } a < q/2 \text{ or } (a = q/2 \text{ and } b < q/2) \text{ or } n \in \{(q+1)/2, q/2 + q^2/2\},\\ a - q & \text{otherwise.}\end{cases}$$

Proof. From
$$a \equiv n \equiv \varepsilon_0 \pmod{q},$$
$|\varepsilon_0| < q$ and rules (2.2) and (2.3) we obtain that either $\varepsilon_0 = a$ or $\varepsilon_0 = a - q$.

We note that by rules (2.2) and (2.3) and $n > 0$ we have $|\varepsilon_0| \leq q/2$ except when $l = 0$ and $\varepsilon_0 = n = (q+1)/2 = a$.

Let $a < q/2$. Since $a - q < -q/2$, we get $\varepsilon_0 = a$.

Let $a = q/2$ and $b < q/2$. If $\varepsilon_0 = a - q = -q/2$, then by rule (2.7) we have $l = 0$ (which is impossible since $n > 0$) or $\varepsilon_1 \leq 0$. Since $\varepsilon_1 \equiv b + 1 \pmod{q}$, this implies $\varepsilon_1 = b + 1 - q < -q/2 + 1$ (since $n > 0$, this implies $l \geq 2$) and therefore $\varepsilon_1 = -q/2$. Rule (2.9) leads to a contradiction, which yields $\varepsilon_0 = a$.

If $n = (q+1)/2$ and $\varepsilon_0 = a - q = -(q-1)/2$, then we obtain $\sum_{i=0}^{l-1} \varepsilon_{i+1} q^i = 1$. We note that from
$$q^{l-1} \leq \left|\varepsilon_l q^{l-1}\right| = \left|1 - \sum_{i=0}^{l-2} \varepsilon_{i+1} q^i\right| \leq 1 + \frac{q}{2} \cdot \frac{q^{l-1} - 1}{q - 1},$$
we get $l \leq 1$ (because $2 \nmid q$ and therefore $q \geq 3$), which implies $l = 1$ and $\varepsilon_1 = 1$. This is a contradiction to rule (2.4), which shows $\varepsilon_0 = a$.

Consider now the case $a > q/2$. $\varepsilon_0 = a$ yields $l = 0$, $\varepsilon_0 = n = (q+1)/2$, which has been considered above. Therefore $\varepsilon_0 = a - q$.

We turn to the case $a = q/2$ and $b \geq q/2$. If $\varepsilon_0 = a = q/2$ then $b \equiv \varepsilon_1 \pmod{q}$. By rule (2.6) we get $\varepsilon_1 \geq 0$ which implies $\varepsilon_1 = b \geq q/2$ and therefore $\varepsilon_1 = q/2$. By rules (2.8) and (2.10) this leads to $n = q/2 + q^2/2$.

Finally, we have to consider $n = q/2 + q^2/2$. If $\varepsilon_0 = a - q = -q/2$, then we get $\sum_{i=0}^{l-1} \varepsilon_{i+1} q^i = q/2 + 1$, i. e. $\varepsilon' = (\varepsilon_1, \ldots, \varepsilon_l) \in R_q(q/2 + 1)$ and ε' is reduced. By the proven parts of this lemma, this implies $(\varepsilon_1, \ldots, \varepsilon_l) = (-q/2 + 1, 1)$ and therefore $\varepsilon = (-q/2, -q/2 + 1, 1)$, which is a contradiction to rule (2.5). ∎

Algorithm 1 Computation of the reduced minimal representation of n

Input: $n > 0, q \geq 2$ integers.
Output: $\varepsilon \in R_q(n)$ such that $c(\varepsilon) = \min\{c(\varepsilon') : \varepsilon' \in R_q(n)\}$ and ε is reduced.

```
ε ← ()
m ← n
while m > 0 do
  a ← (m mod q).
  if not (a < q/2 or (a = q/2 and {m/q^2} < 1/2) or m = (q+1)/2 or m = q/2+q^2/2)
  then
    a ← a − q
  end if
  m ← (m − a)/q
  ε ← ε & a
end while
```

Theorem 1. *Let $q \geq 2$ and $n > 0$ be integers. Then there is a unique reduced representation $\varepsilon \in R_q(n)$; this representation is minimal with respect to* (1.2)*, and it can be computed by Algorithm 1.*

Proof. The existence follows from Lemma 1 applied to any representation of n.

Let $\varepsilon = (\varepsilon_0, \dots, \varepsilon_l) \in R_q(n)$ be a reduced representation. By Lemma 2, ε_0 is uniquely given in terms of n. Additionally, $\varepsilon' := (\varepsilon_1, \dots, \varepsilon_l) \in R_q((n-\varepsilon_0)/q)$ is reduced. By iterating Lemma 2 we see that all digits are uniquely determined by n, which proves uniqueness.

Since $\{n/q^2\} = (a + bq)/q^2$ (where a and b are defined as in Lemma 2), we obtain that $\{n/q^2\} < 1/2$ if and only if $b < q/2$ (if $2 \mid q$; otherwise, we never have to consider a digit $q/2$); and therefore, Algorithm 1 computes the reduced representation of n.

Let $\varepsilon' \in R_q(n)$ be a representation of n with minimum costs. Construct the sequence ${\varepsilon'}^{(i)}$ as in Lemma 1. By this lemma, there is some $m \geq 0$ such that $f^m(\varepsilon') = \varepsilon$ and $c(\varepsilon) \leq c(\varepsilon')$. Therefore, ε has minimum costs. □

3. Relaxed Reduced Representations

If we are looking for minimal representations with respect to (1.3), the main ideas of the previous section remain the same, so we will only sketch the differences.

Since the length of a representation is not important, we may think of a representation as of an infinite sequence of integers with finitely many non-zero entries. This implies that we do not have to consider the reduction rules which could only be applied at the end.

Therefore, we define $f' : R_q(n) \to R_q(n)$ by the reduction rules (as in the previous section, we have to apply the first rule which matches) (2.2), (2.6), (2.7), (2.8) and (2.9). A representation ε is called *relaxed reduced*, if $f'(\varepsilon) = \varepsilon$ and (if written as a finite sequence) ε has no trailing zeros. It is easily seen that ε is relaxed reduced if and only if the following conditions are satisfied:

(3.1) There are no trailing zeros.
(3.2) $-q/2 \leq \varepsilon_i \leq q/2$ for $i \geq 0$.
(3.3) If $\varepsilon_i = q/2$ then $0 \leq \varepsilon_{i+1} \leq q/2 - 1$.
(3.4) If $\varepsilon_i = -q/2$ then $-q/2 + 1 \leq \varepsilon_{i+1} \leq 0$.

In the proof of the analogue of Lemma 1, the length of the representations is not bounded a priori by $c'(\varepsilon_0)$. However, if the sequence does not terminate, then there are some M and $i_0 \in \mathbb{N}$ such that $c'(\varepsilon^{(i)}) = M$ for all $i \geq i_0$. We note that there cannot be any j such that $\left|\varepsilon_j^{(i)}\right| \geq q$ for $i \geq i_0$ since we could apply rule (2.2) and the costs would strictly decrease in this case. Therefore, let $l_i := \max\{j \in \mathbb{N} : \varepsilon_j^{(i)} \neq 0\}$, and we get

$$q^{l_i} \leq n + (q-1) \sum_{j=l_i-M-1}^{l_i-1} q^j = n + q^{l_i} - q^{l_i-M+1}.$$

This implies $l \leq M - 1 + \log_q n$, i. e. $\omega(\varepsilon^{(i)})$ lies in the finite set

$$\{-\infty, -c(\varepsilon^{(0)}) - \lfloor \log_q |n| \rfloor + 1, \dots, 0, \dots, c(\varepsilon^{(0)}) + \lfloor \log_q |n| \rfloor - 1, \infty\}^8$$

for $i \geq i_0$, which leads to a contradiction, and the analogue of Lemma 1 is proved.

The analogue of Lemma 2 is

Lemma 3. *Let n, q be fixed and $\varepsilon \in R_q(n)$ be relaxed reduced. Let $a := n \bmod q$ and $b := (n-a)/q \bmod q$. Then*

$$\varepsilon_0 = \begin{cases} a & \text{if } a < q/2 \text{ or } (a = q/2 \text{ and } b < q/2), \\ a - q & \text{otherwise, i. e. if } a > q/2 \text{ or } (a = q/2 \text{ and } b \geq q/2). \end{cases}$$

Algorithm 2 Computation of the relaxed reduced minimal representation of n

Input: $n > 0, q \geq 2$ integers.
Output: $\varepsilon \in R_q(n)$ such that $c'(\varepsilon) = \min\{c'(\varepsilon') : \varepsilon' \in R_q(n)\}$ and ε is relaxed reduced.

```
ε ← ()
m ← n
while m > 0 do
   a ← (m mod q).
   if a > q/2 or (a = q/2 and {m/q²} ≥ 1/2) then
      a ← a − q
   end if
   m ← (m − a)/q
   ε ← ε & a
end while
```

This leads to the following result:

Theorem 2. *Let $q \geq 2$ and $n > 0$ be integers. Then there is a unique relaxed reduced representation $\varepsilon \in R_q(n)$; this representation is minimal with respect to* (1.3)*, and it can be computed by Algorithm 2.*

Finally, we have to clarify the relation between the relaxed reduced and the reduced representations:

Theorem 3. *Let $q \geq 2$ and $n > 0$ be integers and $\varepsilon = (\varepsilon_0, \dots, \varepsilon_l)$ and $\varepsilon' = (\varepsilon'_0, \dots, \varepsilon'_{l'})$ the reduced and the relaxed reduced representation of n, respectively.*

Then we have the following relations

$$\varepsilon = \begin{cases} (\varepsilon'_0, \dots, \varepsilon_{l'-2}, (q+1)/2) & \text{if } (\varepsilon'_{l'-1}, \varepsilon'_{l'}) = (-(q-1)/2, 1), \\ (\varepsilon'_0, \dots, \varepsilon_{l'-3}, q/2, q/2) & \text{if } (\varepsilon'_{l'-2}, \varepsilon'_{l'-1}, \varepsilon'_{l'}) = (-q/2, -q/2+1, 1), \\ \varepsilon' & \text{otherwise}, \end{cases} \tag{3.5}$$

$$\varepsilon' = \begin{cases} (\varepsilon_0, \dots, \varepsilon_{l-1}, -(q-1)/2, 1) & \text{if } \varepsilon_l = (q+1)/2, \\ (\varepsilon_0, \dots, \varepsilon_{l-2}, -q/2, -q/2+1, 1) & \text{if } (\varepsilon_{l-1}, \varepsilon_l) = (q/2, q/2), \\ \varepsilon & \text{otherwise.} \end{cases} \tag{3.6}$$

Proof. It is obvious that $f(\varepsilon') = \varepsilon'$ unless ε' corresponds to one of the two exceptional cases in (3.5), in which $f(\varepsilon')$ is the expression on the right hand side of (3.5). To see that this expression is indeed reduced, we note that the only rules which might apply are (2.10) and (2.7), but this cannot be the case since ε' was relaxed reduced which implies that $\varepsilon'_{l'-3} \notin \{\pm q/2\}$. The other direction follows easily. □

4. Formula for Odd q

Theorem 4. *Let $q \geq 3$ be odd and n be a positive integer. Let*

$$\varepsilon_r := b_q^{(r)}(2n) - b_q^{(r)}(n), \qquad r \geq 0,$$

where $b_q^{(r)}(n)$ is the r-th digit of the "usual" q-adic expansion of n, i. e.

$$b_q^{(r)}(n) = \left\lfloor \frac{n}{q^r} \right\rfloor - q \left\lfloor \frac{n}{q^{r+1}} \right\rfloor,$$

and $l := \max\{r \geq 0 : \varepsilon_r \neq 0\}$. Then $\varepsilon = (\varepsilon_0, \dots, \varepsilon_l)$ is the relaxed reduced minimal representation.

Proof. By definition, we have

$$\begin{aligned} \varepsilon_r = b_q^{(r)}(2n) - b_q^{(r)}(n) &= \left\lfloor \frac{2n}{q^r} \right\rfloor - q \left\lfloor \frac{2n}{q^{r+1}} \right\rfloor - \left\lfloor \frac{n}{q^r} \right\rfloor + q \left\lfloor \frac{n}{q^{r+1}} \right\rfloor \\ &= \left\lfloor 2q \frac{n}{q^{r+1}} \right\rfloor - q \left\lfloor 2 \frac{n}{q^{r+1}} \right\rfloor - \left\lfloor q \frac{n}{q^{r+1}} \right\rfloor + q \left\lfloor \frac{n}{q^{r+1}} \right\rfloor. \end{aligned}$$

For any positive integer a and any real number x the relation

$$\lfloor ax \rfloor = \sum_{i=0}^{a-1} \left\lfloor x + \frac{i}{a} \right\rfloor \tag{4.1}$$

is well-known (see for instance [7, 3.26]). Setting $x := n/q^{r+1}$ we obtain

$$\begin{aligned} \varepsilon_r &= \sum_{l=0}^{2q-1} \left\lfloor x + \frac{l}{2q} \right\rfloor - q \left(\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor \right) - \sum_{l=0}^{q-1} \left\lfloor x + \frac{l}{q} \right\rfloor + q \lfloor x \rfloor \\ &= -(q-1) \left\lfloor x + \frac{1}{2} \right\rfloor + \sum_{\substack{m=0 \\ m \neq (q-1)/2}}^{q-1} \left\lfloor x + \frac{2m+1}{2q} \right\rfloor. \end{aligned}$$

Let $0 \leq j \leq q$ such that

$$\frac{2j-1}{2q} \leq \{x\} < \frac{2j+1}{2q}.$$

Then

$$\sum_{m=0}^{q-1} \left\lfloor x + \frac{2m+1}{2q} \right\rfloor = q \lfloor x \rfloor + j$$
$$q \left\lfloor x + \frac{1}{2} \right\rfloor = q \lfloor x \rfloor + q \left[j \geq \frac{q+1}{2} \right],$$

which shows that

$$-\frac{q-1}{2} \leq \varepsilon_r \leq \frac{q-1}{2}. \tag{4.2}$$

By construction, $\varepsilon_r \in R_q(n)$. By (3.2) and (4.2) we see that ε_r is the relaxed reduced representation of n. □

5. Formula for Even q

We derive a formula for the digits of the relaxed reduced expansion (which yields a formula for the reduced expansion by Theorem 3), which will enable us to study the distribution of the digits in the next section.

Theorem 5. *Let $q \geq 2$ be even. For $r \geq 0$ define*

$$\begin{aligned}
\varepsilon_r := \sum_{i=0}^{q/2-1} \Bigg(\sum_{j=0}^{q/2-1} & \left\lfloor \frac{n}{q^{r+2}} + \frac{1 + \frac{q}{2} + (q+1)(iq+j)}{q^2(q+1)} \right\rfloor \\
& -(q-1) \left\lfloor \frac{n}{q^{r+2}} + \frac{\frac{q}{2} + (q+1)(iq+q/2)}{q^2(q+1)} \right\rfloor \\
& + \sum_{j=q/2+1}^{q-1} \left\lfloor \frac{n}{q^{r+2}} + \frac{\frac{q}{2} + (q+1)(iq+j)}{q^2(q+1)} \right\rfloor \Bigg) \\
+ \sum_{i=q/2}^{q-1} \Bigg(\sum_{j=0}^{q/2-2} & \left\lfloor \frac{n}{q^{r+2}} + \frac{1 + \frac{q}{2} + (q+1)(iq+j)}{q^2(q+1)} \right\rfloor \\
& -(q-1) \left\lfloor \frac{n}{q^{r+2}} + \frac{1 + \frac{q}{2} + (q+1)(iq+q/2-1)}{q^2(q+1)} \right\rfloor \\
& + \sum_{j=q/2}^{q-1} \left\lfloor \frac{n}{q^{r+2}} + \frac{\frac{q}{2} + (q+1)(iq+j)}{q^2(q+1)} \right\rfloor \Bigg).
\end{aligned} \tag{5.1}$$

Let $l := \max\{r \geq 0 : \varepsilon_r \neq 0\}$. Then $\varepsilon = (\varepsilon_0, \ldots, \varepsilon_l) \in R_q(n)$ is the relaxed reduced minimal representation.

Example 1. For $q = 2$, (5.1) is

$$\varepsilon_r = \left\lfloor \frac{n}{2^{r+2}} + \frac{5}{6} \right\rfloor - \left\lfloor \frac{n}{2^{r+2}} + \frac{4}{6} \right\rfloor - \left\lfloor \frac{n}{2^{r+2}} + \frac{2}{6} \right\rfloor + \left\lfloor \frac{n}{2^{r+2}} + \frac{1}{6} \right\rfloor, \tag{5.2}$$

which is the formula also obtained in [14] (cf. Section 7).

Example 2. It is perhaps a good idea to explain what the formula (5.1) *does*, which we will do for the instance $q=6$:

$$\begin{aligned}\varepsilon_r = &+\left\lfloor y+\frac{248}{252}\right\rfloor+\left\lfloor y+\frac{241}{252}\right\rfloor+\left\lfloor y+\frac{234}{252}\right\rfloor-5\left\lfloor y+\frac{228}{252}\right\rfloor+\left\lfloor y+\frac{221}{252}\right\rfloor+\left\lfloor y+\frac{214}{252}\right\rfloor\\
&+\left\lfloor y+\frac{206}{252}\right\rfloor+\left\lfloor y+\frac{199}{252}\right\rfloor+\left\lfloor y+\frac{192}{252}\right\rfloor-5\left\lfloor y+\frac{186}{252}\right\rfloor+\left\lfloor y+\frac{179}{252}\right\rfloor+\left\lfloor y+\frac{172}{252}\right\rfloor\\
&+\left\lfloor y+\frac{164}{252}\right\rfloor+\left\lfloor y+\frac{157}{252}\right\rfloor+\left\lfloor y+\frac{150}{252}\right\rfloor-5\left\lfloor y+\frac{144}{252}\right\rfloor+\left\lfloor y+\frac{137}{252}\right\rfloor+\left\lfloor y+\frac{130}{252}\right\rfloor\\
&+\left\lfloor y+\frac{122}{252}\right\rfloor+\left\lfloor y+\frac{115}{252}\right\rfloor-5\left\lfloor y+\frac{108}{252}\right\rfloor+\left\lfloor y+\frac{102}{252}\right\rfloor+\left\lfloor y+\frac{95}{252}\right\rfloor+\left\lfloor y+\frac{88}{252}\right\rfloor\\
&+\left\lfloor y+\frac{80}{252}\right\rfloor+\left\lfloor y+\frac{73}{252}\right\rfloor-5\left\lfloor y+\frac{66}{252}\right\rfloor+\left\lfloor y+\frac{60}{252}\right\rfloor+\left\lfloor y+\frac{53}{252}\right\rfloor+\left\lfloor y+\frac{46}{252}\right\rfloor\\
&+\left\lfloor y+\frac{38}{252}\right\rfloor+\left\lfloor y+\frac{31}{252}\right\rfloor-5\left\lfloor y+\frac{24}{252}\right\rfloor+\left\lfloor y+\frac{18}{252}\right\rfloor+\left\lfloor y+\frac{11}{252}\right\rfloor+\left\lfloor y+\frac{4}{252}\right\rfloor,\end{aligned}$$

where $y=n/6^{r+2}$.

Let us think about y as a real variable. It is plain to see that the expression with q^2 terms is periodic in y. For $y=0$ it is 0; when y reaches $\frac{4}{252}$, the first term changes to 1; when y reaches $\frac{11}{252}$, the second term also changes to 1, and so on. Accordingly, the digit changes from 0 to 1, then to 2, then to 3, then to $-2,-1,0$. That describes the first line of terms. This patterns repeats twice, but then in the second half the general pattern switches from $0,1,2,3,-2,-1$ to $0,1,2,-3,-2,-1$. The digits $0,1,2,3,-2,-1$ are not symmetric around 0, and $0,1,2,-3,-2,-1$ are not, either. However, in combination, both coming with "probability" $\frac{1}{2}$, the distribution of the digits becomes symmetric.

Proof. We rewrite (5.1) as

(5.3)
$$\varepsilon_r=\sum_{i=0}^{q-1}\sum_{j=0}^{q-1}\left\lfloor\frac{n}{q^{r+2}}+\frac{j}{q^2}+\frac{[j<q/2]+q/2}{q^2(q+1)}+\frac{i}{q}\right\rfloor-q\sum_{i=0}^{q-1}\left\lfloor\frac{n}{q^{r+2}}+\frac{i}{q}+\frac{[i<q/2]+q/2}{q(q+1)}\right\rfloor.$$

Interchanging the order of summation in the first part, using (4.1), renaming i to j in the second part and collecting the two resulting sums, we get

$$\varepsilon_r=\sum_{j=0}^{q-1}\left(\left\lfloor\frac{n}{q^{r+1}}+\frac{j}{q}+\frac{[j<q/2]+q/2}{q(q+1)}\right\rfloor-q\left\lfloor\frac{n}{q^{r+2}}+\frac{j}{q}+\frac{[j<q/2]+q/2}{q(q+1)}\right\rfloor\right).$$

Therefore, we calculate that

$$\sum_{r=0}^{\infty} \varepsilon_r q^r = \sum_{j=0}^{q-1} \left\lfloor \frac{n}{q} + \frac{j}{q} + \frac{[j < q/2] + q/2}{q(q+1)} \right\rfloor. \tag{5.4}$$

We write $n = r + sq$ for $0 \le r < q$ and observe that for an integer $0 \le m < 2q$ and for $\sigma \in \{0, 1\}$

$$\left\lfloor \frac{m}{q} + \frac{\sigma + q/2}{q(q+1)} \right\rfloor = [m \ge q].$$

Evaluating (5.4) in this way we obtain

$$\sum_{r=0}^{\infty} \varepsilon_r q^r = \sum_{j=0}^{q-1} (s + [j \ge q - r]) = n, \tag{5.5}$$

and we proved that $\varepsilon = (\varepsilon_0, \dots, \varepsilon_l) \in R_q(n)$ is indeed a representation of n.

In order to investigate further properties of ε we fix some $r \ge 0$, write $x := \{n/q^{r+2}\}$ and define

$$\xi_{i,j} := \frac{[j < q/2] + q/2 + (q+1)(iq+j)}{q^2(q+1)} \qquad \text{and} \qquad h_{i,j} := \lfloor x + \xi_{i,j} \rfloor \tag{5.6}$$

for $i, j \in \{0, \dots, q-1\}$. We note that for $(i, j) <_{lex} (i', j')$ we have $0 < \xi_{i,j} < \xi_{i',j'} < 1$ and rewrite (5.1) as

$$\begin{aligned} \varepsilon_r = \sum_{i=0}^{\frac{q}{2}-1} & h_{i,0} + \dots + h_{i,\frac{q}{2}-2} + \qquad h_{i,\frac{q}{2}-1} - (q-1)\, h_{i,\frac{q}{2}} + h_{i,\frac{q}{2}+1} + \dots + h_{i,q-1} \\ + \sum_{i=\frac{q}{2}}^{q-1} & h_{i,0} + \dots + h_{i,\frac{q}{2}-2} - (q-1)\, h_{i,\frac{q}{2}-1} + \qquad h_{i,\frac{q}{2}} + h_{i,\frac{q}{2}+1} + \dots + h_{i,q-1}. \end{aligned}$$

Choose (i_0, j_0) lexicographically minimal such that $x + \xi_{i_0,j_0} \ge 1$ — if $x + \xi_{q-1,q-1} < 1$ then we set $(i_0, j_0) := (\infty, \infty)$ —, which implies that $h_{i,j} = [(i,j) \ge_{lex} (i_0, j_0)]$ and therefore

$$\varepsilon_r = \tag{5.7}$$
$$\begin{cases} h_{i_0,0} + \dots + h_{i_0,\frac{q}{2}-2} + \qquad h_{i_0,\frac{q}{2}-1} - (q-1)\, h_{i_0,\frac{q}{2}} + h_{i_0,\frac{q}{2}+1} + \dots + h_{i_0,q-1} & \text{if } i_0 < \frac{q}{2} \\ h_{i_0,0} + \dots + h_{i_0,\frac{q}{2}-2} - (q-1)\, h_{i_0,\frac{q}{2}-1} + \qquad h_{i_0,\frac{q}{2}} + h_{i_0,\frac{q}{2}+1} + \dots + h_{i_0,q-1} & \text{if } i_0 \ge \frac{q}{2} \\ 0 & \text{if } i_0 = \infty. \end{cases}$$

From (5.7) we see that $|\varepsilon_r| \le q/2$ and that

$$\begin{aligned} \varepsilon_r = q/2 &\iff j_0 = q/2 \text{ and } i_0 \ge q/2 \\ \varepsilon_r = -q/2 &\iff j_0 = q/2 \text{ and } i_0 < q/2. \end{aligned} \tag{5.8}$$

Assume $j_0 = q/2$. By definition of (i_0, j_0) and by (5.6) this implies that

$$\left\lfloor \frac{n}{q^{2+r}} \right\rfloor + 1 - \frac{i_0}{q} - \frac{q+2}{2q(q+1)} \le \frac{n}{q^{2+r}} < \left\lfloor \frac{n}{q^{2+r}} \right\rfloor + 1 - \frac{i_0}{q} - \frac{1}{2(q+1)}.$$

Dividing by q, denoting $x' := \{n/q^{3+r}\}$ and $a_{r+2} := \lfloor n/q^{2+r} \rfloor - q\lfloor n/q^{3+r} \rfloor$ — we remark that $0 \le a_{r+2} < q$ —, we obtain

$$\frac{a_{r+2}+1}{q} - \frac{i_0}{q^2} - \frac{q+2}{2q^2(q+1)} \le x' < \frac{a_{r+2}+1}{q} - \frac{i_0}{q^2} - \frac{1}{2q(q+1)}. \tag{5.9}$$

Define

$$(i_1, j_1) := \begin{cases} (q-1-a_{r+2}, i_0+1) & \text{if } q/2 \le i_0 < q-1 \\ (q-a_{r+2}, 0) & \text{if } i_0 = q-1 \text{ and } a_{r+2} \ne 0 \\ (\infty, \infty) & \text{if } i_0 = q-1 \text{ and } a_{r+2} = 0 \\ (q-1-a_{r+2}, i_0) & \text{if } 0 \le i_0 < q/2. \end{cases} \tag{5.10}$$

Using (5.9) we check that in all cases, (i_1, j_1) is lexicographically minimal such that $x' + \xi_{i_1,j_1} \ge 1$. From (5.8), (5.10), and (5.7) we can deduce that

$$\begin{aligned} \varepsilon_r = q/2 &\Longrightarrow \varepsilon_{r+1} \in \{0, \dots, q/2-1\} \\ \varepsilon_r = -q/2 &\Longrightarrow \varepsilon_{r+1} \in \{-q/2+1, \dots, 0\}. \end{aligned} \tag{5.11}$$

From the fact that $|\varepsilon_i| \le q/2$, (5.11), (3.2), (3.3), and (3.4), we conclude that ε is indeed the relaxed reduced expansion. ☐

6. Counting Digits in the Minimal Representations

We are interested to count how often a given digit i occurs in the relaxed reduced expansion among the numbers 1, ..., n; call that $\#_i(n)$. By Theorem 3 the corresponding values for the reduced expansion will differ by at most $2n$, which will not appear in the main term of the asymptotic formula anyway.

In the case q odd, the reduced representation is actually the (q, d) representation, with $d = -\frac{q-1}{2}$, and digits $d, d+1, \dots, d+q-1$. Digit counting in this representation is well known, see [11]. Every digit occurs with the same frequency $\frac{1}{q}$, and

$$\#_i(n) = \frac{1}{q} n \log_q n + \mathcal{O}(n). \tag{6.1}$$

Actually, more is known about the error term. It can be made fully explicit and is basically given by n times a periodic function in $\log_q n$. Here, we don't bother to compute the periodic functions in detail.

Summing (6.1), (multiplied by $|i|$), over all possible digits i, we get the average value of $c'(\varepsilon)$. It is

$$\left(\frac{q}{4} - \frac{1}{4q}\right) \log_q n + \mathcal{O}(1);$$

the constant is computed via

$$2 \sum_{i=1}^{(q-1)/2} i \frac{1}{q}.$$

In the instance q even, things are a bit more complicated, but fortunately not by much. The formula (5.1) tells us that digit 0 occurs with frequency $\frac{q+2}{q(q+1)}$, digits $\pm 1, \dots, \pm\frac{q}{2} - 1$ with frequency $\frac{1}{q}$, digits $\pm\frac{q}{2}$ each with frequency $\frac{1}{2(q+1)}$. So we see that digit 0 appears a bit more often than the other digits, and the digits $\pm\frac{q}{2}$ (combined) appear a bit less often than the other digits. In terms of costs, this is fortunate. Anyway, it leads to

$$\begin{aligned}
\#_0(n) &= \frac{q+2}{q(q+1)} n \log_q n + \mathcal{O}(n), \\
\#_i(n) &= \frac{1}{q} n \log_q n + \mathcal{O}(n), && \text{for } i = \pm 1, \dots, \pm\frac{q}{2} - 1, \\
\#_i(n) &= \frac{1}{2(q+1)} n \log_q n + \mathcal{O}(n), && \text{for } i = \pm\frac{q}{2}.
\end{aligned}$$

Again, summing this, (multiplied by $|i|$), over all possible digits i, we get the average value of $\sum |\varepsilon_i|$:

$$\left(\frac{q}{4} - \frac{1}{2(q+1)}\right) \log_q n + \mathcal{O}(1).$$

The computation of the constant is done via

$$2 \sum_{i=1}^{q/2-1} i \frac{1}{q} + 2 \frac{q}{2} \frac{1}{2(q+1)}.$$

The average length of the representation is given by $\log_q n + \mathcal{O}(1)$.

We sum up these results in the following theorem:

Theorem 6. *Let $q \geq 2$ and $n \geq 1$. Then the average costs $c(\varepsilon)$ of the reduced expansions of the integers $1, \dots, n$ are*

$$\begin{aligned}
\left(1 + \frac{q}{4} - \frac{1}{2(q+1)}\right) \log_q n + \mathcal{O}(1) & \qquad \textit{if } q \textit{ is even}, \\
\left(1 + \frac{q}{4} - \frac{1}{4q}\right) \log_q n + \mathcal{O}(1) & \qquad \textit{if } q \textit{ is odd}.
\end{aligned}$$

7. Previous Work

We start our overview on related papers with the relaxed reduced expansion for $q = 2$. In this case, (3.2), (3.3), and (3.4) are clearly equivalent to $\varepsilon_i \in \{0, \pm 1\}$ and $\varepsilon_i \varepsilon_{i+1} = 0$. This means that for $q = 2$ our relaxed reduced expansion is the so-called "non-adjacent-form" (NAF) or "sparse signed digit representation" or "balanced binary representation" or "Paul representation" (cf. Güntzer and Paul [8]) which has been studied — at least partly independently — by several authors; we refer to [1, IV.2.4] and [6] for some references. It goes back at least to Reitwiesner [15], who proved existence and uniqueness of a NAF and that it has minimum c'. Jedwab and Mitchell [10] describe an algorithm which computes the NAF from every redundant binary expansion with digits $0, \pm 1$.

Morain and Olivos [13] first applied the idea to elliptic curves as sketched in the introduction and empirically found two algorithms, which yield good results. Actually, the second of these algorithms leads exactly to the NAF, therefore, Morain and Olivos reach the minimum c' (and by Theorem 3 the minimum c by up to one). They give the main term of the expected costs (as in our calculations in Section 6), whereas Thuswaldner [16] gives a further asymptotic term. Further properties of the NAF have been described by the second author in [14].

Demetrovics, Pethő, and Rónyai [5] take up Morain and Olivos' motivation and consider c for $q = 2$. They translate the minimization problem into an infinite graph where minimal expansions correspond to shortest paths and apply Dijkstra's algorithm to the solution of the problem. This has been generalized to general q by the first author in [9], and it was proved that there exists a minimal expansion such that $|\varepsilon_i| \leq q/2$, which characterizes the case of odd q almost completely. It is worth noting that [9, Algorithm 1] is not guaranteed to yield an expansion with digits $|\varepsilon_i| \leq q/2$ because the choice between two paths of equal length leading to the same vertex is made arbitrarily. If expansions with small digits are preferred, then the algorithm yields the reduced representation of our Algorithm 1. Of course, both algorithms need $O(\log_q n)$ time, computational experiments show that Algorithm 1 is faster by a factor of 3.

Another generalization of the non-adjacent-form to arbitrary bases is described in Clark and Liang [3]. It is unique, minimizes $c''(\varepsilon) := \operatorname{card}\{i : \varepsilon_i \neq 0\}$ and can be computed from the usual q-adic expansions of $(q+1)/q$ and $1/q$, similarly to our Theorem 4. In the case $q = 2$, this property goes back to Chang and Tsao-Wu [2].

The generalized NAF (GNAF) and our reduced expansions were designed for different cost functions, however, it may be instructive to compare how the two expansions behave with respect to both cost functions. To this aim, we calculate an explicit formula for the r-th digit of the GNAF as we did it for the reduced expansion in Section 4 and we follow the lines of Section 6. The result is shown in Table 1.

Expansion	Expected $c'(\varepsilon)$	Expected $c''(\varepsilon)$
Clark and Liang	$\frac{q-1}{3} \log_q n + \mathcal{O}(1)$	$\left(1 - \frac{2}{q+1}\right) \log_q n + \mathcal{O}(1)$
Relaxed Reduced, even q	$\left(\frac{q}{4} - \frac{1}{2(q+1)}\right) \log_q n + \mathcal{O}(1)$	$\left(1 - \frac{q+2}{q(q+1)}\right) \log_q n + \mathcal{O}(1)$
Relaxed Reduced, odd q	$\left(\frac{q}{4} - \frac{1}{4q}\right) \log_q n + \mathcal{O}(1)$	$\left(1 - \frac{1}{q}\right) \log_q n + \mathcal{O}(1)$

TABLE 1. Comparison of the GNAF and the relaxed reduced expansion

References

[1] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, vol. 265, Cambridge University Press, 1999.

[2] S. H. Chang and N. Tsao-Wu, *Distance and structure of cyclic arithmetic codes*, Proc. Hawaii International Conference on System Sciences, vol. 1, 1968, pp. 463–466.

[3] W. Edwin Clark and J. J. Liang, *On arithmetic weight for a general radix representation of integers*, IEEE Trans. Information Theory **IT-19** (1973), 823–826.

[4] J.-S. Coron, *Resistance against differential power analysis for elliptic curve cryptosystems*, Workshop on Cryptographic Hardware and Embedded Systems (Ç. Koç and Ch. Paar, eds.), Lecture Notes in Computer Science, vol. 1717, Springer, 1999, pp. 292–302.

[5] J. Demetrovics, A. Pethő, and L. Rónyai, *On* ± 1*-representations of integers*, Acta Cybernet. **14** (1999), 27–36.

[6] D. M. Gordon, *A survey of fast exponentiation methods*, J. Algorithms **27** (1998), no. 1, 129–146.

[7] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics. A foundation for computer science*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994.

[8] U. Güntzer and M. Paul, *Jump interpolation search trees and symmetric binary numbers*, Inform. Process. Lett. **26** (1987), no. 4, 193–204.

[9] C. Heuberger, *Minimal expansions in redundant number systems and shortest paths in graphs*, Computing **63** (1999), 341–349.

[10] J. Jedwab and C. J. Mitchell, *Minimum weight modified signed-digit representations and fast exponentiation*, Electron. Lett. **25** (1989), no. 17, 1171–1172.

[11] P. Kirschenhofer and H. Prodinger, *Subblock occurrences in positional number systems and Gray code representation*, J. Inform. Optim. Sci. **5** (1984), no. 1, 29–42.

[12] D. E. Knuth, *Seminumerical algorithms*, The Art of Computer Programming, vol. 2, Addison-Wesley, Bonn, 1998.

[13] F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), no. 6, 531–543.

[14] H. Prodinger, *On binary representations of integers with digits* $-1, 0, 1$, Integers **0** (2000), A08, available at `http://www.integers-ejcnt.org/vol0.html`.

[15] G. W. Reitwiesner, *Binary arithmetic*, Advances in computers, Vol. 1, Academic Press, New York, 1960, pp. 231–308.

[16] J. M. Thuswaldner, *Summatory functions of digital sums occurring in cryptography*, Period. Math. Hungar. **38** (1999), 111–130.

Institut für Mathematik, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria

E-mail address: `cheub@weyl.math.tu-graz.ac.at`

URL: `http://finanz.math.tu-graz.ac.at/~cheub/`

The John Knopfmacher Centre for Applicable Analysis and Number Theory, Department of Mathematics, University of the Witwatersrand, P. O. Wits, 2050 Johannesburg, South Africa

E-mail address: `helmut@gauss.cam.wits.ac.za`

URL: `http://www.wits.ac.za/helmut/index.htm`