Journal de Théorie des Nombres
de Bordeaux **14** (2002), 517–528

Minimal redundant digit expansions in the Gaussian integers

par Clemens HEUBERGER

Résumé. Un résultat récent établit qu'il suffit de connaître les deux derniers chiffres significatifs du développement en base q usuel d'un entier pour calculer le dernier chiffre significatif dans le développement en base q redondant minimal. Nous montrons que l'énoncé analogue pour les entiers de Gauss est faux.

Abstract. We consider minimal redundant digit expansions in canonical number systems in the Gaussian integers. In contrast to the case of rational integers, where the knowledge of the two least significant digits in the "standard" expansion suffices to calculate the least significant digit in a minimal redundant expansion, such a property does not hold in the Gaussian numbers: We prove that there exist pairs of numbers whose non-redundant expansions agree arbitrarily well but which have different least significant digits in minimal redundant expansions.

1. Introduction

Let n and $q \geq 2$ be positive rational integers. Redundant q-ary expansions $n = \sum_{i=0}^{l} \varepsilon_i q^i$ with arbitrary digits $\varepsilon_i \in \mathbb{Z}$ have been studied by several authors, motivated by applications from cryptography and coding theory. For general positional number systems, we refer to Knuth [3, Section 4.1.]. An overview over results on redundant q-ary digit expansions is contained in [1]. The aim is to minimize the cost of an expansion which is given by

$$c(\varepsilon_0, \ldots, \varepsilon_l) := \sum_{j=0}^{l} |\varepsilon_j| \,. \tag{1}$$

Recently, we proved [1] that the knowledge of the first two digits η_0, η_1 of the "standard" expansion $n = \sum_{j=0}^{l'} \eta_j q^j$ with $0 \leq \eta_j < q$ suffices to decide what digit ε_0 should be taken in order to achieve a minimal expansion with respect to the costs (1). By using this information, we could provide an efficient algorithm to compute a minimal expansion, a formula to compute

Manuscrit reçu le 20 décembre 2000.

a single digit without having to compute the others, and we gave estimates for the average costs of such an expansion.

A natural question is whether such a result is also true if we replace the q-ary expansion in the rational integers by an expansion in a canonical number system in some algebraic number field. In this paper, we give a negative answer for the case of the Gaussian integers.

Let R be a subring of the ring of integers in an algebraic number field K. For $\beta \in R$, $(\beta, \{0, \dots, N_{K/\mathbb{Q}}(\beta) - 1\})$ is called a *canonical number system* if all $\alpha \in R$ have a unique representation

$$\alpha = \sum_{j=0}^{l} a_j \beta^j, \qquad a_j \in \{0, \dots, N_{K/\mathbb{Q}}(\beta) - 1\} \text{ for } 0 \le j \le l, a_l \neq 0. \tag{2}$$

We refer to Kovács and Pethő [4] for further discussions on canonical number systems.

Kátai and Szabó [2] characterized canonical number systems in the Gaussian integers: $\beta \in \mathbb{Z}[i]$ is a base of a canonical number system if and only if $\operatorname{Re}\beta < 0$ and $\operatorname{Im}\beta = \pm 1$.

Let β be such a base and $\alpha \in \mathbb{Z}[i]$. A *redundant expansion of α in base β* is a tuple $(r_0, \dots, r_l)$ with $r_j \in \mathbb{Z}$ for $0 \le j \le l$ such that

$$\alpha = \sum_{j=0}^{l} r_j \beta^j. \tag{3}$$

A *minimal redundant expansion of α in base β* is a redundant expansion with minimum costs

$$c(r_0, \dots, r_l) := \sum_{j=0}^{l} |r_j|. \tag{4}$$

The main result of this note is the following theorem.

Theorem 1. *Let β be a base of a canonical number system in the Gaussian integers. For all $L \ge 0$ there is a pair of numbers α, α' with the following properties:*

1. *Let $\alpha = \sum_{j=0}^{l} a_j \beta^j$ and $\alpha' = \sum_{j=0}^{l'} a'_j \beta^j$ be the unique representations according to (2) with $l, l' \ge L$. Then $a_j = a'_j$ for $0 \le j \le L$.*
2. *For all pairs $(r_0, \dots, r_s)$ and $(r'_0, \dots, r'_{s'})$ of minimal redundant expansions of α and α', respectively, we have $r_0 \neq r'_0$.*

This implies that there are numbers where the knowledge of the first $L+1$ digits in the "standard" expansion (2) cannot be used to derive the first digit of a minimal expansion. We call a pair α, α' as described in Theorem 1 a *critical pair.*

According to the result of Kátai and Szabó we have to consider $\beta = -n \pm i$ for $n \geq 1$; without loss of generality we may assume $\beta = -n + i$. We first discuss general properties of minimal expansions in Section 2. We show that not all integers can occur in a minimal expansion. This implies that there are usually two choices for the least significant digit of the expansion. We demonstrate how to prove rules which can avoid branching in some cases. Some of these rules are based on the fact that some digits cannot occur, other rules have to be proved by checking minimal expansions of a certain set of numbers. Then we construct a critical pair for $n \geq 3$ in Section 3. The special cases $n = 1$ and $n = 2$ are investigated in Sections 4 and 5, respectively. The construction of critical pairs is done as follows. First, we collect enough rules in order to derive minimal expansions of some numbers recursively. In a second step, we take all possible least significant digits for one component of the pretended critical pair, use the known expansions from the previous step in order to calculate the minimum costs for all alternatives and see that only one of the possible least significant digits leads to a minimal expansion. By doing the same for the other component of the critical pair we prove that the least significant digits in minimal redundant expansions differ.

For an $A \subset \mathbb{Z}$ we use the notation

$$A^* := \{(a_k)_{k \geq 0} : a_k \in A \text{ and } a_k = 0 \text{ for almost all } k\}.$$

We identify finite sequences $(a_0, \dots, a_l)$ with the corresponding infinite sequences $(a_0, \dots, a_l, 0, \dots)$. The indices of all sequences start with 0 unless otherwise stated.

For given β and for $\alpha \in \mathbb{Z}[i]$ and $a \in \mathbb{Z}^*$ we write $\alpha \simeq_\beta a$ if $\alpha = \sum_{j=0}^{\infty} a_j \beta^j$. Similarly, we write $a \simeq_\beta b$ for $a, b \in \mathbb{Z}^*$ if $\sum_{j=0}^{\infty} a_j \beta^j = \sum_{j=0}^{\infty} b_j \beta^j$.

We define

$$\operatorname{opt}_\beta(\alpha) := \{r \in \mathbb{Z}^* : r \text{ is a minimal redundant expansion of } \alpha \text{ in base } \beta\}$$

and extend this notation to $a \in \mathbb{Z}^*$ by $\operatorname{opt}_\beta(a) := \operatorname{opt}_\beta(\sum_{j=0}^{\infty} a_j \beta^j)$.

The concatenation of finite sequences is denoted by

$$(a_0, \dots, a_l) \,\&\, (b_0, \dots, b_m) := (a_0, \dots, a_l, b_0, \dots, b_m).$$

This notation is extended to concatenations of a finite sequence $a \in \mathbb{Z}^l$ with a set of infinite sequences $R \subset \mathbb{Z}^*$: $a \,\&\, R := \{a \,\&\, b : b \in R\}$. Finally, the repetition of a sequence is defined by $(a_0, \dots, a_l)^{(k)} := (a_0, \dots, a_l) \,\&\, (a_0, \dots, a_l) \,\&\, \dots \,\&\, (a_0, \dots, a_l)$, where the block $(a_0, \dots, a_l)$ is repeated k times.

2. Properties of Minimal Expansions

We write $M := N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) = n^2 + 1$ and note that

$$(M, 2n, 1) \simeq_\beta 0. \tag{5}$$

Let us first state the following observation:

Lemma 2. *Let $a, b \in \mathbb{Z}^*$ such that $a \simeq_\beta b$. Then $a_0 \equiv b_0 \pmod{M}$.*

Proof. There is some $\gamma \in \mathbb{Z}[i]$ such that $a_0 - b_0 = \beta\gamma$. Since $\gamma/\bar{\beta} \in \mathbb{Q}$ and $-(\gamma/\bar{\beta}) = (\gamma/\bar{\beta}) \operatorname{Im} \bar{\beta} = \operatorname{Im} \gamma \in \mathbb{Z}$, we have $M = \beta\bar{\beta} \mid (a_0 - b_0)$. □

Not all integers can occur as digits in a minimal expansion, as is shown in the following lemma.

Lemma 3. *Let $n \geq 1$, $\beta = -n + i$, and $\alpha \in \mathbb{Z}[i]$. We define*

$$D := \{-n^2, \dots, n^2\}, \tag{6a}$$

$$U_n := \begin{cases} 2 & \text{if } n = 1, \\ 8 & \text{if } n = 2, \\ \frac{n^2}{2} + n + 1 & \text{if } n \geq 3. \end{cases} \tag{6b}$$

Then we have

$$\operatorname{opt}_\beta(\alpha) \cap D^* \neq \emptyset, \tag{7a}$$

$$\operatorname{opt}_\beta(\alpha) \subset ([-U_n, U_n] \cap \mathbb{Z})^*. \tag{7b}$$

Proof. We consider first the case $n \geq 3$. Assume that (7b) is not true. Then there is some $r \in \operatorname{opt}_\beta(\alpha)$ and some j such that $|r_j| > n^2/2 + n + 1$. By (5), $r' := (r_0, \dots, r_{j-1}, r_j - \sigma M, r_{j+1} - \sigma 2n, r_{j+2} - \sigma, r_{j+3}, \dots)$ is also a redundant expansion of α for $\sigma = \operatorname{sign}(r_j)$. We have

$$\begin{aligned} c(r') - c(r) &= |r_j - \sigma M| + |r_{j+1} - \sigma 2n| + |r_{j+2} - \sigma| - |r_j| - |r_{j+1}| - |r_{j+2}| \\ &\leq |r_j - \sigma M| - |r_j| + 2n + 1. \end{aligned}$$

If $|r_j| > M$, we conclude that

$$c(r') - c(r) \leq -M + 2n + 1 < 0,$$

otherwise, we get

$$c(r') - c(r) \leq M - 2|r_j| + 2n + 1 < 0.$$

This is a contradiction to the assumption that r is a minimal expansion. Therefore, (7b) is proved for $n \geq 3$. Because $n^2/2 + n + 1 < M$ for $n \geq 3$, this yields (7a) also.

The proof of (7b) for $n = 1$ and $n = 2$ is similar: We repeat the above argument using the expansions

$$3 \simeq_{-1+i} (-1, 0, 0, 0, -1) \quad \text{and} \quad (-10, -3, 2, 1) \simeq_{-2+i} 0$$

instead of relation (5).

Now, we prove (7a) for $n = 1$. Assume that $\mathrm{opt}_\beta(\alpha) \cap D^* = \emptyset$ and let $r \in \mathrm{opt}_\beta(\alpha)$. By assumption, there is some j such that $|r_j| = 2$. Let $\sigma := \mathrm{sign}(r_j)$.

If $j \le l-3$, we may replace r by $r' = (r_0, \ldots, r_{j-1}, 0, r_{j+1}, r_{j+2}+\sigma, r_{j+3}+\sigma, r_{j+4}, \ldots, r_l)$, since $(-2, 0, 1, 1) \simeq_\beta 0$ and $c(r') - c(r) \le 0$. We emphasize that r and r' are of same length. Therefore we repeat this process finitely many times in order to obtain an $r := (r_0, \ldots, r_l) \in \mathrm{opt}_\beta(\alpha)$ such that $|r_j| \le 1$ for $0 \le j \le l-3$.

We may replace (r_{l-2}, r_{l-1}, r_l) by any element of $\mathrm{opt}_\beta(r_{l-2}, r_{l-1}, r_l)$. It can easily be checked that $\mathrm{opt}_\beta(r_{l-2}, r_{l-1}, r_l) \cap D^* \ne \emptyset$ for all choices $(r_{l-2}, r_{l-1}, r_l) \in \{-2, -1, 0, 1, 2\}$.

Finally, we note that for $n = 2$, (7a) can be proved similarly using relation (5). □

We note that Lemma 2 and Lemma 3 can be used to calculate one (or all) minimal expansion in exponential time. Assume that we want to compute $\mathrm{opt}_\beta(\alpha)$ for some $\alpha = a+bi$. Since $\alpha \equiv (a+nb) \pmod{\beta}$, the set of possible least significant digits is contained in $R := (a+nb+M\mathbb{Z}) \cap [-U_n, U_n]$. This yields

$$\mathrm{opt}_\beta(\alpha) \subset \bigcup_{r \in R} (r) \,\&\, \mathrm{opt}_\beta\big((\alpha - r)/\beta\big). \tag{8}$$

An implementation of these ideas in Mathematica can be obtained from `http://www.opt.math.tu-graz.ac.at/~cheub/publications/minimal redundantgauss/`.

The following lemma shows how to prove some rules of the following type: If the standard expansion (2) starts with digits $(a_0, \ldots, a_l)$, then there is an optimal expansion which starts with the digit r_0.

Lemma 4. *Let $n \ge 1$, $\beta = -n+i$, $a \in D^{l+1}$, $\alpha \simeq_\beta a$ and $r_0 \in \mathbb{Z}$ with $|r_0| < M$. Then the following conditions are equivalent:*

1. *For all $t \in \mathbb{Z}^*$ we have $\mathrm{opt}_\beta(a \,\&\, t) \cap r_0 \,\&\, \mathbb{Z}^* \ne \emptyset$.*
2. *For all α' that satisfy $\alpha' \equiv \alpha \pmod{\beta^{l+1}}$ and for which there is an $s \in D^{l+1}$ with $\alpha' \simeq_\beta s$ we have*

$$\mathrm{opt}_\beta(\alpha') \cap r_0 \,\&\, \mathbb{Z}^* \ne \emptyset.$$

Note that s in condition 2 and a are of same length $l+1$.

Proof. Assume condition 1. Since $\alpha' \equiv \alpha \pmod{\beta^{l+1}}$ there is an expansion $\alpha' \simeq_\beta a \,\&\, t$ for some $t \in \mathbb{Z}^*$. Therefore there exists some $s \in \mathbb{Z}^*$ such that $(r_0) \,\&\, s \in \mathrm{opt}_\beta(a \,\&\, t) = \mathrm{opt}_\beta(\alpha')$.

Conversely, assume condition 2. Let $t \in \mathbb{Z}^*$ and define $\alpha'' \simeq_\beta a \,\&\, t$. Choose some $s \in D^* \cap \operatorname{opt}_\beta(a \,\&\, t) = \operatorname{opt}_\beta(\alpha'')$. This intersection is non-empty by (7a).

We define $\alpha' := \sum_{j=0}^{l} s_j\beta^j$ and note that $\alpha' \equiv \alpha'' \equiv \alpha \pmod{\beta^{l+1}}$. By assumption, there is some $l' \geq l$ and some $r = (r_1, \ldots, r_{l'}) \in \mathbb{Z}^{l'}$ (we do not enforce $r_{l'} \neq 0$) such that $(r_0) \,\&\, r \in \operatorname{opt}_\beta(\alpha')$.

By construction of r, we get

$$\begin{aligned}\alpha'' &= \sum_{j=0}^{l} s_j\beta^j + \sum_{j=l+1}^{l'} s_j\beta^j + \sum_{j=l'+1}^{\infty} s_j\beta^j\\ &= \sum_{j=0}^{l} r_j\beta^j + \sum_{j=l+1}^{l'} (s_j + r_j)\beta^j + \sum_{j=l'+1}^{\infty} s_j\beta^j,\end{aligned}$$

and $c(s) \geq c\big((r_0) \,\&\, u\big)$ for $u = (r_1, \ldots, r_l, s_{l+1} + r_{l+1}, \ldots, s_{l'} + r_{l'}, s_{l'+1}, \ldots)$. Since $s \in \operatorname{opt}_\beta(\alpha'')$, this proves that $(r_0) \,\&\, u \in \operatorname{opt}_\beta(\alpha'') = \operatorname{opt}_\beta(a \,\&\, t)$. $\square$

The following lemma shows that condition 2 of Lemma 4 can be checked efficiently:

Lemma 5. *Let $n \geq 1$, $\beta = -n + i$, $a, a' \in D^{l+1}$, $\alpha \simeq_\beta a$, $\alpha' \simeq_\beta a'$ such that $\alpha' \equiv \alpha \pmod{\beta^{l+1}}$. Then there is some $\gamma \in \mathbb{Z}[i]$ with*

$$|\gamma| \leq \frac{2n^2}{|\beta| - 1}\left(1 - \frac{1}{|\beta|^{l+1}}\right) \leq \frac{2n^2}{|\beta| - 1}$$

such that $\alpha' = \alpha + \gamma\beta^{l+1}$.

Proof. Let $\gamma \in \mathbb{Z}[i]$ such that $\alpha' - \alpha = \gamma\beta^{l+1}$. We obtain

$$|\gamma| \leq \frac{1}{|\beta|^{l+1}} \sum_{j=0}^{l} 2n^2 \, |\beta|^j \,.$$

$\square$

3. Critical Pair for $n \geq 3$

The following lemma calculates the minimal expansion of some special numbers which will occur in the construction of a critical pair.

Lemma 6. *Let $n \geq 3$, $\beta = -n + i$, and*

$$x := \frac{1}{2}n^2 - n + \frac{9}{2} + \frac{\sigma}{2}, \qquad \sigma := \begin{cases} 1 & \text{if } n \text{ is even,} \\ 0 & \text{if } n \text{ is odd.} \end{cases} \tag{9}$$

Then $x \in \mathbb{Z}$, and for $k \geq 1$ we have

$$\{(x)\} = \operatorname{opt}_\beta(x), \tag{10a}$$

$$\{(x-M)\,\&\,(x-2n,x-1-M)^{(k-1)}\,\&\,(x-2n,-1)\} = \operatorname{opt}_\beta\big((x)^{(2k)}\big), \tag{10b}$$

$$(x-M)\,\&\,(x-2n,x-1-M)^{(k-1)}\,\&\,(x-2n,x-1) \in \operatorname{opt}_\beta\big((x)^{(2k+1)}\big), \tag{10c}$$

$$\{(x-1)\} = \operatorname{opt}_\beta(x-1), \tag{10d}$$

$$\{(x-1-M,x-2n)^{(k)}\,\&\,(-1)\} = \operatorname{opt}_\beta\big((x-1)\,\&\,(x)^{(2k-1)}\big), \tag{10e}$$

$$(x-1-M,x-2n)^{(k)}\,\&\,(x-1) \in \operatorname{opt}_\beta\big((x-1)\,\&\,(x)^{(2k)}\big). \tag{10f}$$

Proof. For $R \in \mathbb{Z}^*$, Lemma 2 and (7b) imply

$$\operatorname{opt}_\beta\big((x-2n)\,\&\,R\big) = (x-2n)\,\&\,\operatorname{opt}_\beta(R), \tag{11a}$$

$$\operatorname{opt}_\beta\big((x-2n-1)\,\&\,R\big) = (x-2n-1)\,\&\,\operatorname{opt}_\beta(R), \tag{11b}$$

$$\operatorname{opt}_\beta\big((-1)\,\&\,R\big) = (-1)\,\&\,\operatorname{opt}_\beta(R). \tag{11c}$$

By Lemma 2 and (7b), an optimal expansion of x may start with x or $x-M$. Since $|x-M|+1 > |x|$ for $n \geq 5$, we proved (10a) in this case. For $n \in \{3,4\}$, relation (10a) can be checked directly. Similarly, we can verify (10d).

Relation (5) yields $\operatorname{opt}_\beta(x,x) \subset x\,\&\operatorname{opt}_\beta(x) \cup (x-M)\,\&\operatorname{opt}_\beta(x-2n,-1)$. By (10a), (11a) and (11c), we have $\operatorname{opt}_\beta(x,x) \subset \{(x,x)\} \cup \{(x-M,x-2n,-1)\}$. We note that $|x-M|+|x-2n|+1 < |x|+|x|$, which proves (10b) for $k=1$.

The proofs of (10c), (10e), and (10f) for $k=1$ are similar.

An inductive argument completes the proof of the lemma. □

We are now able to construct a critical pair:

Proposition 7. *Let $n \geq 3$, $\beta = -n+i$, and*

$$x := \frac{1}{2}n^2 - n + \frac{9}{2} + \frac{\sigma}{2}, \qquad \sigma := \begin{cases} 1 & \text{if } n \text{ is even,} \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

Then

$$(12)\quad \operatorname{opt}_\beta(x-2,x^{(l)}) = \begin{cases} \{(x-2)\} & \text{if } l=0,\\ \{(x-2,x-M)\,\&\,(x-2n,x-1-M)^{(k-1)}\,\&\,(x-2n,-1)\} & \\ & \text{if } l=2k \text{ and } k\geq 1,\\ \{(x-2-M,x-2n)\,\&\,(x-1-M,x-2n)^{(k)}\,\&\,(-1)\} & \\ & \text{if } l=2k+1 \text{ and } k\geq 0. \end{cases}$$

Proof. We first consider the case $l = 2k$ with $k \geq 2$. As in (8), relations (7b) and (11a) imply $\operatorname{opt}_\beta\big((x-2)\,\&\,(x)^{(2k)}\big) \subset (x-2)\,\&\operatorname{opt}_\beta\big((x)^{(2k)}\big) \cup (x-2-M, x-2n)\,\&\operatorname{opt}_\beta\big((x-1)\,\&\,(x)^{(2k-2)}\big)$. We can now use the expansions calculated in (10b) and (10f) to obtain the following candidates for minimal expansions of $(x-2)\,\&\,(x)^{(2k)}$.

$$\{(x-2,x-M)\,\&\,(x-2n,x-1-M)^{(k-1)}\,\&\,(x-2n,-1)\} = (x-2)\,\&\operatorname{opt}_\beta\big((x)^{(2k)}\big),$$

$$(x-2-M,x-2n)\,\&\,(x-1-M,x-2n)^{(k-1)}\,\&\,(x-1) \in (x-2-M,x-2n)\,\&\operatorname{opt}_\beta\big((x-1)\,\&\,(x)^{(2k-2)}\big).$$

Since

$$|x-2|+|x-M|+(k-1)\,|x-2n|+(k-1)\,|x-1-M|+|x-2n|+1 < |x-2-M|+|x-2n|+(k-1)\,|x-1-M|+(k-1)\,|x-2n|+|x-1|\,,$$

the first alternative has to be taken in order to minimize the costs. We note that we proved equality in (10b), which yields (12) for $l = 2k \geq 4$.

The other cases can be proved similarly. □

4. Critical Pair for $n = 1$

In Table 1, we collect some choices $(a, r_0) \in D^{l+1} \times D$ for which the conditions of Lemma 4 are fulfilled.

The following lemma will be needed for the construction of a critical pair for $n = 1$:

Lemma 8. *Let $\beta = -1 + i$, $R \in \mathbb{Z}^*$, $q \geq 0$, $0 < r \leq 5$, and $s = 5q + r$. Then*

$$(1,-1,0,0,0)^{(3q)}\,\&\operatorname{opt}_\beta\big((1,1,0)^{(r)}\,\&\,R\big) \subset \operatorname{opt}_\beta\big((1,1,0)^{(s)}\,\&\,R\big).$$

$(a_0,\dots,a_l)$	r_0
(0)	0
$(1,0,0,0)$	1
$(1,0,1,1)$	-1
$(1,1,0)$	1
$(1,1,1)$	-1

TABLE 1. Some valid choices for $n=1$, a, and r_0 in Lemma 4

Proof. First, we prove that

$$(1,-1,0,0,0)\ \&\ \mathrm{opt}_\beta\big((-1)\ \&\ R\big) \subset \mathrm{opt}_\beta\big((1,1,0)^{(2)}R\big). \tag{13}$$

From Table 1 we derive

$$\begin{aligned}\mathrm{opt}_\beta\big((1,1,0)\ \&\ (1,1,0)\ \&\ R\big) &\supset (1)\ \&\ \mathrm{opt}_\beta\big((1,0,1,1)\ \&\ (0)\ \&\ R\big)\\ &\supset (1,-1)\ \&\ \mathrm{opt}_\beta\big((0,2,2,0)\ \&\ R\big)\\ &\supset (1,-1,0)\ \&\ \mathrm{opt}_\beta\big((0,0,-1)\ \&\ R\big)\\ &\supset (1,-1,0,0,0)\ \&\ \mathrm{opt}_\beta\big((-1)\ \&\ R\big).\end{aligned}$$

Using (13) and noting that $(-1,1,1,0) \simeq_\beta (1,1,0,-1)$ and that $(-1,-1,-1) \simeq_\beta (1,1,0)$ leads to

$$\begin{aligned}\mathrm{opt}_\beta\big((110)^{(6)}R\big) &\supset (1,-1,0,0,0)\ \&\ \mathrm{opt}_\beta\big((-1)\ \&\ (1,1,0)^{(4)}\ \&\ R\big)\\ &\supset (1,-1,0,0,0)\ \&\ \mathrm{opt}_\beta\big((1,1,0)^{(4)}\ \&\ (-1)\ \&\ R\big)\\ &\supset (1,-1,0,0,0)^{(2)}\ \&\ \mathrm{opt}_\beta\big((-1)\ \&\ (1,1,0)^{(2)}\ \&\ (-1)\ \&\ R\big)\\ &\supset (1,-1,0,0,0)^{(2)}\ \&\ \mathrm{opt}_\beta\big((1,1,0)^{(2)}\ \&\ (-1,-1)\ \&\ R\big)\\ &\supset (1,-1,0,0,0)^{(3)}\ \&\ \mathrm{opt}_\beta\big((-1,-1,-1)\ \&\ R\big)\\ &\supset (1,-1,0,0,0)^{(3)}\ \&\ \mathrm{opt}_\beta\big((1,1,0)\ \&\ R\big).\end{aligned}$$

Applying this relation q times completes the proof. □

We are now able to construct a critical pair (which proves Theorem 1 for $n=1$).

Proposition 9. *Let $n=1$, $\beta=-1+i$, $q\geq 1$ and*

$$\begin{aligned}a &:= \big((1,0,1,0,0,0)\ \&\ (1,1,0)^{(5q+1)}\big),\\ a' &:= \big((1,0,1,0,0,0)\ \&\ (1,1,0)^{(5q+1)}\ \&\ (1,1,1)\big).\end{aligned}$$

Let $\alpha \simeq_\beta a$ and $\alpha' \simeq_\beta a'$.

Then

$$\mathrm{opt}_\beta(\alpha) \subset (-1)\ \&\ \mathbb{Z}^*, \qquad \mathrm{opt}_\beta(\alpha') \subset (1)\ \&\ \mathbb{Z}^*. \tag{14}$$

Proof. From (7b) we see that $\mathrm{opt}_\beta(\alpha) \subset (1) \mathbin{\&} \mathbb{Z}^* \cup (-1) \mathbin{\&} \mathbb{Z}^*$. We note that α can also be represented by $\bigl((-1,0,2,1,0,0) \mathbin{\&} (1,1,0)^{(5q+1)}\bigr)$. We use Table 1 and Lemma 8 to calculate

$$\begin{aligned}(15)\quad \mathrm{opt}_\beta\bigl((0,1,0,0,0) \mathbin{\&} (1,1,0)^{(5q+1)}\bigr)\\ &\supset (0) \mathbin{\&} \mathrm{opt}_\beta\bigl((1,0,0,0) \mathbin{\&} (1,1,0)^{(5q+1)}\bigr)\\ &\supset (0,1,0,0,0) \mathbin{\&} (1,-1,0,0,0)^{(3q)} \mathbin{\&} \mathrm{opt}_\beta(1,1,0)\\ &\ni (0,1,0,0,0) \mathbin{\&} (1,-1,0,0,0)^{(3q)} \mathbin{\&} (1,1,0).\end{aligned}$$

Similarly, we obtain

$$\begin{aligned}(16)\quad \mathrm{opt}_\beta\bigl((0,2,1,0,0) \mathbin{\&} (1,1,0)^{(5q+1)}\bigr)\\ &\ni (0,0,-1,1,0) \mathbin{\&} (0,0,0,1,-1)^{(3q)}.\end{aligned}$$

Since by (15) an optimal expansion of $\bigl((0,1,0,0,0) \mathbin{\&} (1,1,0)^{(5q+1)}\bigr)$ has cost $3+6q$ and an optimal expansion of $\bigl((0,2,1,0,0) \mathbin{\&} (1,1,0)^{(5q+1)}\bigr)$ has cost $2+6q$, we get (14) for α.

Analogously, we note that

$$\begin{aligned}\mathrm{opt}_\beta\bigl((0,1,0,0,0) \mathbin{\&} (1,1,0)^{(5q+1)} \mathbin{\&} (1,1,1)\bigr)\\ &\ni (0,1,0,0,0) \mathbin{\&} (1,-1,0,0,0)^{(3q)} \mathbin{\&} (1,-1),\end{aligned}$$

where the optimal cost is $6q+3$. On the other hand, α' can be represented by $(-1,0,2,1,0,0) \mathbin{\&} (1,1,0)^{(5q+1)} \mathbin{\&} (1,1,1)$, which yields

$$\begin{aligned}\mathrm{opt}_\beta\bigl((0,2,1,0,0) \mathbin{\&} (1,1,0)^{(5q+1)} \mathbin{\&} (1,1,1)\bigr)\\ &\ni (0,0,-1,1,0,0,0,0) \mathbin{\&} (1,-1,0,0,0)^{(3q)} \mathbin{\&} (-1,-1)\end{aligned}$$

with optimal cost $6q+4$. This completes the proof. □

In the case $n=1$, Table 1 shows that in most cases it is sufficient to know a few more digits in the "standard" expansion to derive the correct digit in an optimal expansion. Therefore, an algorithm to compute an optimal expansion could precompute some more entries for Table 1 and branch only in those cases where no information is known.

We note that the relation $(-1+i)^4 = -4$ strongly relates the standard expansion in base $-1+i$ to the expansion in base -4 in $\mathbb{Z}$. However, this observation cannot be used for minimal expansions because this correspondence does not respect the costs (4).

5. Critical Pair for $n = 2$

We will repeatedly use the relation $(5,-1,-3,-1) \simeq_\beta 0$ and the rules according to Lemma 4 which are given in Table 2.

$(a_0,\dots,a_l)$	r_0	$(a_0,\dots,a_l)$	r_0	$(a_0,\dots,a_l)$	r_0
(0)	0	$(1,3)$	1	$(3,1,0,1)$	3
$(1,0)$	1	$(2,1,3)$	2	$(3,1,1)$	-2
$(1,1)$	1	$(2,4,4,1)$	2	$(4,4)$	-1

TABLE 2. Some valid choices for $n = 2$, a, and r_0 in Lemma 4

Lemma 10. *Let $n = 2$, $\beta = -2+i$, $u \geq 0$, $s \geq 0$, $r \in \{0,1\}$, and $u = 2s + r$. Then we have*

$$(1,-2,2,-1,0,0)^{(s)} \,\&\, (1,3,1)^{(r)} \in \operatorname{opt}_\beta\bigl((1,3,1)^{(u)}\bigr).$$

Proof. As in the proof of Lemma 8, repeated application of rules in Table 2 yields

$$\operatorname{opt}_\beta\bigl((1,3,1)^{(2)} \,\&\, R\bigr) \supset (1,-2,2,-1,0,0) \,\&\, \operatorname{opt}_\beta(R)$$

for $R \in \mathbb{Z}^*$. Iterating this result and noting that $(1,3,1) \in \operatorname{opt}_\beta(1,3,1)$ proves the lemma. □

The proof of the following proposition completes the proof of Theorem 1 for $n = 2$:

Proposition 11. *Let $n = 2$, $\beta = -2+i$, $u \geq 0$. Then*

$$\operatorname{opt}_\beta\bigl((3,4,4,1) \,\&\, (1,3,1)^{(u)}\bigr) \subset \begin{cases} (3) \,\&\, \mathbb{Z}^* & \text{if } u \text{ is even,} \\ (-2) \,\&\, \mathbb{Z}^* & \text{if } u \text{ is odd.} \end{cases}$$

Proof. Let $\alpha \simeq_\beta (3,4,4,1) \,\&\, (1,3,1)^{(u)}$. We write $u := 2s + r$ with $r \in \{0,1\}$. According to (7b), we have to consider first digits $-7, -2, 3, 8$. All possible expansions are given in Table 3, which has been computed using Table 2, Lemma 10 and an inductive argument (for expansions starting with -7). □

$\alpha \simeq_\beta \dots$	minimal expansion	minimum costs
$(-2,0,3,1) \,\&\, (1,3,1)^{(u)}$	$(-2,0,-2,2,-1) \,\&\, (0,0,1,-2,2,-1)^{(s-1+r)}$ $\&(1,3,1)^{(1-r)}$	$6s + r + 6$
$(3,4,4,1) \,\&\, (1,3,1)^{(u)}$	$(3,-1,0,0) \,\&\, (1,-2,2,-1,0,0)^{(s)}$ $\&(1,3,1)^{(r)}$	$6s + 5r + 4$
$(-7,1,6,2) \,\&\, (1,3,1)^{(u)}$	$(-7,1,1) \,\&\, \operatorname{opt}_\beta\bigl((3,4,4,1) \,\&\, (1,3,1)^{(u-1)}\bigr)$	$3u + 10$
$(8,3,1,0) \,\&\, (1,3,1)^{(u)}$	$(8,3,1,0) \,\&\, (1,-2,2,-1,0,0)^{(s)} \,\&\, (1,3,1)^{(r)}$	$6s + 5r + 12$

TABLE 3. Minimal Expansions of α for $n = 2$ and $u \geq 1$

References

[1] C. HEUBERGER, H. PRODINGER, *On minimal expansions in redundant number systems: Algorithms and quantitative analysis.* Computing **66** (2001), 377–393.

[2] I. KÁTAI, J. SZABÓ, *Canonical number systems for complex integers.* Acta Sci. Math. (Szeged) **37** (1975), 255–260.

[3] D. E. KNUTH, *Seminumerical algorithms*, third ed. The Art of Computer Programming, vol. 2, Addison-Wesley, 1998.

[4] B. KOVÁCS, A. PETHŐ, *Number systems in integral domains, especially in orders of algebraic number fields.* Acta Sci. Math. (Szeged) **55** (1991), 287–299.

Clemens HEUBERGER
Institut für Mathematik
Technische Universität Graz
Steyrergasse 30
A-8010 Graz
Austria
E-mail : `clemens.heuberger@tugraz.at`
URL: `http:www.opt.math.tu-graz.ac.at/~cheub/`