

# Redundant Radix Representations of Rings

Asger Munk Nielsen and Peter Kornerup, *Member, IEEE*

**Abstract**—This paper presents an analysis of radix representations of elements from general rings; in particular, we study the questions of redundancy and completeness in such representations. Mappings into radix representations, as well as conversions between such, are discussed, in particular where the target system is redundant. Results are shown valid for normed rings containing only a finite number of elements with a bounded distance from zero, essentially assuring that the ring is “discrete.” With only brief references to the more usual representations of integers, the emphasis is on various complex number systems, including the “classical” complex number systems for the Gaussian integers, as well as the Eisenstein integers, concluding with a summary on properties of some low-radix representations of such systems.

**Index Terms**—Radix representation of rings, integer and computer radix number systems, redundancy, number system conversion, computer arithmetic.



## 1 INTRODUCTION

NUMBER representations have for long been a central research topic in the field of computer arithmetic since choosing the wrong number system can have detrimental effects on such aspects of computer design as storage efficiency, accuracy, and speed of operation. Designing a number system amounts to choosing a representation suitable for computer storage and transfer of elements of a set of numbers such that arithmetic operations can be performed with relative ease on these by merely manipulating their representation.

No number system has achieved the kind of widespread acceptance and popularity that the radix representations have. Radix polynomials represent the elements of a set by a weighted sum of *digits*, where the weights are integer powers of the *base* or *radix*. This representation has the advantage that each digit can be drawn from a small finite *digit-set* easily encoded into machine states, and that arithmetic algorithms can be broken into atomic steps operating on individual digits. An important issue in the design of radix number systems is the notion of *completeness*, i.e., does a given base and digit-set combination have the desired effect of being able to represent all the elements of the set of numbers in question. Equivalently, the notion of *redundancy* is of importance, e.g., the presence of alternative radix polynomials representing the same element has had a profound influence on algorithms and speed of arithmetic operations in modern microprocessors. Redundancy may allow parallel, constant time addition and is thus paramount to fast implementation of multiplication, division, and other composite computations.

As microprocessors become increasingly more complex, the problems that can be solved in hardware likewise

increase in complexity. As an example, we are at the point where signal processing problems demanding fast and frequent execution of arithmetic operations on complex numbers can be solved by dedicated hardware [2]. It seems logical to investigate alternative number representations for these problems, addressing such issues as redundancy and storage efficiency. Unfortunately, assessing important questions, such as completeness and redundancy, are no longer quite as trivial tasks when we turn our attention to sets like complex numbers. Answering these questions requires a fundamental understanding of the underlying mathematical foundation of radix polynomials. The goal of this paper is to clarify some of these issues while providing usable tools for designing and evaluating number systems.

We will do this by using such well-founded and widely understood mathematical notions as rings, residue classes, and norms. This paper extends the work done by Matula in [11], [12] to the general notion of commutative rings, and gives an analysis of some previously discussed representations of complex numbers, e.g., [9], [16], [4], but here emphasizing redundant digit-sets for these representations. There are a number of results on nonredundant representations, also on the representation of complex numbers, e.g., [7], [5], [6], [1], but the question of redundancy beyond the usual integer-based systems (e.g., as treated in [10]) has had little treatment in the past. It is unavoidable that many of the results included for completeness may seem well-known, as they are straightforward generalizations or formalizations of known properties, possibly from the “folklore.”

Section 2 introduces the notation and definitions of completeness and redundancy of a digit-set, together with results on these properties, as generalizations of results from [11], [12]. Section 3 then discusses the determination of radix representations, nonredundant as well as redundant, together with an algorithm for determining whether a digit-set is complete, i.e., capable of representing all elements of the ring. Termination of these algorithms requires the ring to be “discrete” in the sense that, given a norm on the ring, only a finite number of elements has norm less than any given constant. This is likely to be satisfied for any rings of

- A. Munk Nielsen is with MIPS Technologies, Inc., Copenhagen, Denmark. E-mail: asgern@mips.com.
- P. Kornerup is with the Department of Mathematics and Computer Science, Odense University, Denmark. E-mail: kornerup@imada.ou.dk.

Manuscript received 14 Oct. 1998.

For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number 108031.

practical interest since most such rings have some kind of lattice structure.

Section 4 then discusses mappings between radix representations of different systems, in particular digit-set conversions. It is shown here that conversions are possible with a finite carry-set under the same condition for termination as above. For conversion into a redundant digit-set and, thus, addition as a special case, it is generally assumed possible to do so in parallel and with limited carry propagation if only the digit-set is redundant and complete. It is demonstrated that this is **not** the case in general; further conditions on the regularity of the digit-set are needed.

In Section 5, some of the systems presented in the past for representing complex numbers are then discussed, extending these also into redundant representations. Section 6 then concludes with a summary of some of the properties of practical concern for implementations of complex arithmetic.

## 2 ON THE REPRESENTATION OF NUMBERS

This paper is devoted to the study of radix representations of commutative rings. As a foundation for this study, we will rely on the algebraic structure of sets of polynomials. If  $\mathcal{R}$  is a ring, then the entity denoted by  $\mathcal{R}[x]$  is the set of polynomials over the ring  $\mathcal{R}$ . Each of these polynomials is a formal expression in the indeterminate  $x$  of the form

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad (1)$$

where  $n < \infty$  and each coefficient is an element of  $\mathcal{R}$ . The set of *Laurent polynomials* over the ring  $\mathcal{R}$ , denoted by  $\mathcal{R}^*[x]$ , is the set of polynomials of the form

$$P(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_l x^l, \quad (2)$$

where  $\infty > m \geq l > -\infty$  and  $a_i \in \mathcal{R}$ . Note that we will here require that  $l$  and  $m$  are finite so that any of the above polynomials only has a finite number of terms.

When an element of a ring (a "number") is represented in positional notation, each digit has a weight equal to some power of the radix. The radix is in itself an element of the ring and the digits are elements of a finite subset of the ring; this subset is termed the *digit-set*. An element of the ring may be represented by an algebraic structure termed a *radix polynomial*. These polynomials are similar to the polynomials over a ring and may be thought of as the algebraic objects expressible by a number system characterized by a fixed *base* or *radix*  $\beta \in \mathcal{R}$  and a digit-set  $\Sigma$ . In this paper, we will assume that the zero element of the ring is always a member of the digit-set and that the base is not equal to the zero element; neither is it a unit of the ring. For instance, if  $\mathcal{R} = \mathbb{Z}$ , i.e., the ring of integers, then we will assume  $0 \in \Sigma$  and  $|\beta| > 1$ .

**Definition 2.1.** *Radix Polynomials over  $\Sigma$*

$$\mathcal{P}_{\mathcal{I}}[\beta, \Sigma] = \{P([\beta]) = d_m[\beta]^m + d_{m-1}[\beta]^{m-1} + \dots + d_0[\beta]^0\}.$$

with  $d_m, d_{m-1}, \dots, d_0 \in \Sigma \wedge 0 \leq m < \infty$ .

In analogy with the definition of Laurent polynomials, assuming  $\beta^{-1}$  exists in some extension of  $\mathcal{R}$ , we define:

**Definition 2.2.** *Extended Radix Polynomials over  $\Sigma$*

$$\mathcal{P}[\beta, \Sigma] = \{P([\beta]) = d_m[\beta]^m + d_{m-1}[\beta]^{m-1} + \dots + d_l[\beta]^l\}$$

with  $d_m, d_{m-1}, \dots, d_l \in \Sigma \wedge -\infty < l \leq m < \infty$ .

The extended radix polynomials may be thought of as algebraic objects representing elements (numbers) with fractional digits. If we replace  $[\beta]$  by  $\beta$  in a radix polynomial, we evaluate the polynomial in the point  $x = \beta$  and thereby determine the element of the ring that the polynomial represents. This procedure may be formalized by the following function defined as the *evaluation mapping*

$$\|P([\beta])\| = P(x) |_{x=\beta}. \quad (3)$$

The radix polynomials map into the ring  $\mathcal{R}$  and the extended radix polynomials map into the set of elements defined as the  $\beta$ -ary elements:

$$\mathcal{A}_{\beta} = \{r\beta^i | r \in \mathcal{R} \wedge -\infty < i < \infty\}. \quad (4)$$

**Example.** For the ring  $\mathcal{R} = \mathbb{Z}$  the set  $\mathcal{A}_2$  constitutes the binary numbers,  $\mathcal{A}_8$  the octal numbers, and  $\mathcal{A}_{10}$  the decimal numbers.

Observe that  $i$  in (4) may be negative, so the  $\beta$ -ary elements may contain fractional parts, but note that then  $\mathcal{A}_2 \neq \mathcal{A}_{10}$  since  $i$  is finite.

Since the evaluation mapping  $\|\cdot\|$  is a homomorphism from  $\mathcal{P}[\beta, \mathcal{R}]$  into  $\mathcal{A}_{\beta}$ , arithmetic in the ring  $\mathcal{A}_{\beta}$  can be performed in the ring of (extended-) radix polynomials while preserving a correct representation of the elements in  $\mathcal{A}_{\beta}$ . But, the evaluation mapping is not an isomorphism since it is not necessarily one-to-one, for instance, if one element can be represented by more than one radix polynomial.

The goal of our study is to determine criteria for which radix polynomials written over a digit-set sufficiently represents a ring. By *sufficiently* we will understand that the number system is capable of representing all the elements of the ring in the sense that, for each element of the ring, there should exist at least one radix polynomial that represents this element.

**Definition 2.3 (Completeness).** *A digit-set  $\Sigma$  is a complete base  $\beta$  for the ring  $\mathcal{R}$  if and only if*

$$\forall r \in \mathcal{R} : \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] :: \|P\| = r.$$

The definition of completeness has deliberately been defined based on the radix polynomials and not on the extended radix polynomials since, in the latter case, this would lead to some obscure digit-sets being complete, i.e., digit-sets where fractional digits are needed to represent the nonfractional elements of  $\mathcal{A}_{\beta}$ . An example being  $\mathcal{R} = \mathbb{Z}$  with  $\beta = 2$  and  $\Sigma = \{-2, 0, 2\}$ , here, fractional digits are needed to express the odd integers. On the other hand, if a digit-set  $\Sigma$  is complete base  $\beta$  for the ring  $\mathcal{R}$ , it is also complete for the  $\beta$ -ary elements, in the following sense:

$$\forall a \in \mathcal{A}_{\beta} : \exists P \in \mathcal{P}[\beta, \Sigma] :: \|P\| = a.$$

Let  $\langle z \rangle$  denote the ideal  $I = \{kz | k \in \mathcal{R}\}$ , generated by  $z$  in the ring  $\mathcal{R}$ , then the set  $r + I$  is termed a *co-set*. Furthermore, let  $\mathcal{R}/I$  denote the set of distinct co-sets and  $|\mathcal{R}/I|$  the number of distinct co-sets. We will say that two elements  $r_1, r_2 \in \mathcal{R}$  are *congruent modulo  $I$*  if  $r_1 - r_2 \in I$ , and adopt the notation  $r_1 \equiv r_2 \pmod I$ . If a set  $S$  has exactly one element from each distinct co-set in  $\mathcal{R}/I$ , then  $S$  is a *complete residue system modulo  $I$* .

**Example.** For the ring of integers, the ideal generated by  $\beta \in \mathbb{Z}$  is  $\langle \beta \rangle = \{z\beta | z \in \mathbb{Z}\} = \{\dots, -2\beta, -\beta, 0, \beta, 2\beta, \dots\}$ , i.e., all the elements divisible by  $\beta$ . An example of a co-set is  $3 + \langle \beta \rangle = \{\dots, 3 - 2\beta, 3 - \beta, 3, 3 + \beta, 3 + 2\beta, \dots\}$ . The set  $\{0, 1, \dots, |\beta| - 1\}$  is a complete residue system modulo  $\beta$ , thus  $|\mathbb{Z}/\langle \beta \rangle| = |\beta|$ .

**Lemma 2.4.** *If  $\Sigma$  is complete base  $\beta$  for the ring  $\mathcal{R}$ , then  $\Sigma$  contains a complete residue system modulo  $\beta$  and, consequently,  $|\Sigma| \geq |\mathcal{R}/\langle \beta \rangle|$ .*

**Proof.** Let  $e \in \mathcal{R}$ . Since  $\Sigma$  is complete, there exists a polynomial  $P \in \mathcal{P}_I[\beta, \Sigma]$  of the form

$$P([\beta]) = d_m[\beta]^m + \dots + d_1[\beta] + d_0, d_i \in \Sigma$$

with  $\|P\| = e$ . Now,  $\|P\| \equiv d_0 \pmod{\beta}$ , thus the element  $e$  is represented by the residue class  $d_0 + \langle \beta \rangle$ , where  $d_0 \in \Sigma$ . Consequently,  $\Sigma$  contains a complete residue system modulo  $\beta$ .  $\square$

The converse statement does not hold, e.g., the digit-set  $\Sigma = \{-13, 0, 1\}$  is not complete base  $\beta = 3$  for the integers nor is  $\Sigma = \{-19, 0, 1\}$ , although both are complete residue systems modulo  $\beta = 3$ . However,  $\Sigma = \{-19, -13, 0, 1\}$  turns out to be complete for  $\beta = 3$ .

As previously noted, some digit-sets allow a single ring element to be represented by numerous radix-polynomials; these digit-sets are termed *redundant*.

**Definition 2.5 (Redundancy).** *A digit-set  $\Sigma$  is redundant base  $\beta$  for the ring  $\mathcal{R}$  if and only if*

$$\exists P, Q \in \mathcal{P}[\beta, \Sigma] : P \neq Q \wedge \|P\| = \|Q\|$$

*and is nonredundant base  $\beta$  if and only if*

$$\forall P, Q \in \mathcal{P}[\beta, \Sigma], P \neq Q : \|P\| \neq \|Q\|.$$

Redundancy can complicate the determination of the sign or the range of a number, but the presence of redundancy can also be desirable. By exploiting the redundancy, arithmetic operations can be performed more efficiently, e.g., addition and subtraction may then be performed with limited carry propagation and, hence, in constant time.

The following lemma provides a condition for the presence of redundancy.

**Lemma 2.6.** *If  $\Sigma$  is complete base  $\beta$  for the ring  $\mathcal{R}$  and  $|\Sigma| > |\mathcal{R}/\langle \beta \rangle|$ , then  $\Sigma$  is redundant base  $\beta$ .*

**Proof.** Since  $|\Sigma| > |\mathcal{R}/\langle \beta \rangle|$ , there exists  $d_1, d_2 \in \Sigma$  such that  $d_1 \equiv d_2 \pmod{\beta}$ , thus  $\exists k \in \mathcal{R} : d_1 = d_2 + k\beta$ . Since  $\Sigma$  is complete base  $\beta$ , there exists a polynomial  $P \in \mathcal{P}_I[\beta, \Sigma] : \|P\| = k$  by forming  $P' = P[\beta] + d_2 \in \mathcal{P}_I[\beta, \Sigma]$  with  $\|P'\| = k\beta + d_2 = d_1$ , we conclude that  $\Sigma$  is redundant base  $\beta$ .  $\square$

The difference between two congruent digits is a multiple of the radix; if the factor is in the digit-set or is representable, then the digit-set is redundant. Thus, redundancy can also occur in noncomplete digit-sets. For instance, if  $\beta = 2$  and  $\Sigma = \{0, 1, 2\}$ , we have  $0 \equiv 2 \pmod{2}$  and  $2 - 0 = 1 \cdot \beta$ , thus, since  $1 \in \Sigma$ , we have  $2[2]^0$  and  $1[2]^1$  expressing the same element of the ring  $\mathbb{Z}$ , thus  $\Sigma$  is redundant. On the other hand,  $\Sigma$  is not complete since no negative integer can be expressed.

**Lemma 2.7.** *If  $|\Sigma| > |\mathcal{R}/\langle \beta \rangle| = k_1$  and the number of elements from  $\mathcal{R}$  that can be represented with radix polynomials of degree at most  $n$  is bounded by  $\Phi_n \leq C \cdot k_2^n + O(1)$ , where  $k_2 < k_1 + 1$ , then  $\Sigma$  is redundant base  $\beta$ .*

**Proof.** Let  $\mathcal{Q}_n = \{P \in \mathcal{P}_I[\beta, \Sigma] \mid \deg(P) \leq n\}$  be the set of radix polynomials of degree at most  $n$ . The number of such polynomials is  $|\mathcal{Q}_n| = |\Sigma|^{n+1} \geq (k_1 + 1)^{n+1}$ . The ratio:

$$\frac{\Phi_n}{|\mathcal{Q}_n|} \leq \frac{C \cdot k_2^n + O(1)}{(k_1 + 1)^{n+1}}$$

has a limit value of zero as  $n$  tends towards infinity, thus there will be more polynomials than elements to represent, e.g.,  $\Sigma$  is redundant base  $\beta$ .  $\square$

**Theorem 2.8.** *For the ring of integers (i.e.,  $\mathcal{R} = \mathbb{Z}$ ), if  $|\Sigma| > |\mathbb{Z}/\langle \beta \rangle|$ , then  $\Sigma$  is redundant base  $\beta$ .*

**Proof.** Consider the ring of integers  $\mathcal{R} = \mathbb{Z}$ . For  $\beta \in \mathbb{Z}$ , we have  $|\mathbb{Z}/\langle \beta \rangle| = |\beta| = k$ . If  $\Delta = \max\{|d| \mid d \in \Sigma\}$ , then the largest numerical value that can be represented by a radix polynomial of degree at most  $n$  is given by

$$\max\{\|P\| \mid P \in \mathcal{Q}_n\} \leq \Delta \sum_{j=0}^n |\beta|^j = \Delta \frac{|\beta|^{n+1} - 1}{|\beta| - 1},$$

thus the number of integers that can be represented is bounded by

$$\Phi_n \leq 2\Delta \frac{|\beta|^{n+1} - 1}{|\beta| - 1} + 1 = C \cdot |\beta|^n + O(1) = C \cdot k^n + O(1).$$

As demonstrated, the condition of Lemma 2.7 is satisfied, thus  $|\Sigma| > |\mathbb{Z}/\langle \beta \rangle|$  implies that  $\Sigma$  is redundant base  $\beta$ .  $\square$

A similar result can be proven for the ring of Gaussian integers (see Lemma 5.1); in fact, we have been unable to find rings where  $|\Sigma| > |\mathcal{R}/\langle \beta \rangle|$  does not imply that  $\Sigma$  is redundant, thus it seems likely that the following conjecture holds.

**Conjecture 2.9.** *If  $|\Sigma| > |\mathcal{R}/\langle \beta \rangle|$ , then  $\Sigma$  is redundant base  $\beta$ .*

**Lemma 2.10.** *If there exist no digits  $d_1, d_2 \in \Sigma, d_1 \neq d_2$  belonging to the same residue class modulo  $\beta$  (i.e.,  $|\Sigma| \leq |\mathcal{R}/\langle \beta \rangle|$ ), then  $\Sigma$  is nonredundant base  $\beta$  for the ring  $\mathcal{R}$ .*

**Proof.** Assume that  $P = \sum_i^m p_i[\beta]^i \in \mathcal{P}[\beta, \Sigma]$  and  $Q = \sum_i^s q_i[\beta]^i \in \mathcal{P}[\beta, \Sigma]$  with  $P \neq Q$ , but  $\|P\| = \|Q\|$ . Let  $k$  be the smallest index such that  $p_k \neq q_k$ , then

$$\left\| \sum_k^m p_i[\beta]^{i-k} \right\| = \left\| \sum_k^s q_i[\beta]^{i-k} \right\|$$

and, consequently,  $p_k \equiv q_k \pmod{\beta}$ , a contradiction.  $\square$

As stated above, the amount of redundancy is closely related to the size of the digit-set, so we define the redundancy index of a digit-set  $\Sigma$  as  $\eta = |\Sigma| - |\mathcal{R}/\langle\beta\rangle|$ .

From Lemma 2.4, we note that a negative redundancy index implies that  $\Sigma$  cannot be complete and, for rings satisfying Conjecture 2.9, that a positive index implies that the digit-set is redundant and, finally, from Lemma 2.10, that an index less than or equal to zero implies that the digit-set is nonredundant.

If  $\mathcal{R}$  is an integral domain,  $\mathcal{R}$  is said to be *ordered* if and only if  $\mathcal{R}$  contains a nonempty subset  $\mathcal{R}^+$  such that

1.  $\forall a, b \in \mathcal{R}^+ : a + b \in \mathcal{R}^+ \wedge a \cdot b \in \mathcal{R}^+$ .
2. Each element of  $\mathcal{R}$  belongs to exactly one of the sets  $\mathcal{R}^+$ ,  $\{0\}$ , or  $\mathcal{R}^-$ , where  $\mathcal{R}^- = \{-x \mid x \in \mathcal{R}^+\}$ .

The set  $\mathcal{R}^+$  is termed the *positive* elements of  $\mathcal{R}$ . As an example, one easily checks that the integers are ordered since they can be divided into three sets, namely  $\mathbb{Z}^+ = \{z \in \mathbb{Z} \mid z > 0\}$ ,  $\{0\}$ , and  $\mathbb{Z}^- = \{z \in \mathbb{Z} \mid z < 0\}$ .

**Definition 2.11.** If  $\mathcal{R}$  is ordered, a digit-set  $\Sigma$  is termed *semi-complete base  $\beta$  for the ring  $\mathcal{R}$* , if and only if  $\Sigma$  is complete base  $\beta$  for the positive elements  $\mathcal{R}^+$ , in the sense that

$$\forall r \in \mathcal{R}^+ : \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] :: \|P\| = r. \quad (5)$$

If a digit-set is semicomplete for a ring  $\mathcal{R}$ , then by definition all the positive elements of the ring can be represented, thus if an element of  $\mathcal{R}$  is represented by its magnitude (i.e., a positive element), along with a sign indicating whether the element belongs to  $\mathcal{R}^+ \cup \{0\}$  or  $\mathcal{R}^-$ , then all elements of the ring can be represented. Historically, these representations are referred to as *sign-magnitude* representations.

### 3 DETERMINING A RADIX REPRESENTATION

This section covers the problem of determining a radix representation of a ring element, given a base and a finite digit-set. It will generally be assumed that the ring  $\mathcal{R}$  is an integral domain, and that the ring is *normed*, in the sense that there exists a norm  $N : \mathcal{R} \rightarrow \mathbb{R}^+$ . We will assume that the norm satisfies  $\forall a, b \in \mathcal{R}$ :

1.  $N(a + b) \leq N(a) + N(b)$ ,
2.  $N(ab) = N(a)N(b)$ ,
3.  $N(a) = 0 \Leftrightarrow a = 0$ .

Furthermore, we will assume that, given a real number  $k \in \mathbb{R}^+$ , there exists only a finite number of elements in  $\mathcal{R}$  that has at most norm  $k$ , i.e.,

$$\forall k \geq 0 : |\{r \in \mathcal{R} \mid N(r) < k\}| < \infty.$$

This assumption is needed for the termination of algorithms, essentially assuring that the ring is “discrete,” not having condensation points.

If  $\Sigma$  is a complete residue system modulo  $\beta$ , for any element  $r \in \mathcal{R}$  the following algorithm terminates after a finite number of steps. The correctness follows from arguments similar to those of the proof below of Theorem 3.2.

#### Algorithm 3.1 DGT-Algorithm

**Stimulus:** A base  $\beta$ , a digit-set  $\Sigma$  that is a complete residue system modulo  $\beta$ , and an element  $r \in \mathcal{R}$ .

**Response:** ( $OK = true$  and  $P = \sum_{i=0}^m d_i[\beta]^i \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$  with  $\|P\| = r$ ) or ( $OK = false$ ).

**Method:**  $l \leftarrow 0; r_0 \leftarrow r; OK \leftarrow true$   
**while**  $r_l \neq 0$  and  $OK$  **do**  
     $\langle$  find  $d_l \in \Sigma : d_l \equiv r_l \pmod{\beta}$   $\rangle$   
     $r_{l+1} \leftarrow (r_l - d_l)/\beta$   
     $l \leftarrow l + 1$   
     $OK \leftarrow (\forall j : 0 \leq j < l :: r_j \neq r_l)$   
**end**

**Example.** Consider the ring of Gaussian integers  $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ , where  $i = \sqrt{-1}$  and the number system  $\beta = -1 + i$ ,  $\Sigma = \{0, 1\}$ . Using the DGT-algorithm, we will determine a radix polynomial representing the Gaussian integer  $r = r_0 = 3 + 4i$ .

Since  $(3 + 4i) - 1 = (1 - 3i)\beta$ , we have  $1 \equiv 3 + 4i \pmod{\beta}$ , thus  $d_0 = 1$ . Then,  $r_1 = \frac{r_0 - 1}{\beta}$  and the DGT-algorithm proceeds, as indicated in Table 1 and as depicted in Fig. 1. Thus, the radix polynomial

$$\begin{aligned} P &= \sum_{j=0}^6 d_j[-1 + i]^j \\ &= 1[-1 + i]^6 + 1[-1 + i]^5 + 1[-1 + i]^4 + 1[-1 + i]^3 \\ &\quad + 1[-1 + i]^2 + 1 \in \mathcal{P}_{\mathcal{I}}[-1 + i, \{0, 1\}] \end{aligned}$$

is a representation of  $r = 3 + 4i$ .

The following theorem is based on the DGT-algorithm, and provides a test for the completeness of a digit-set, showing that it is sufficient to check the representability of a small set of ring elements.

**Theorem 3.2.** Let  $\mathcal{R}$  be a ring and  $N : \mathcal{R} \rightarrow \mathbb{R}$  a norm. Let  $\Sigma$  be a digit-set containing a complete residue system modulo  $\beta$ , then  $\Sigma$  is complete base  $\beta$  for the ring  $\mathcal{R}$  if and only if

$$\forall r \in \mathcal{R} : N(r) \leq \frac{d_{max}}{N(\beta) - 1} :: \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] : \|P\| = r, \quad (6)$$

where  $d_{max} = \max\{N(d) \mid d \in \Sigma'\}$ , for some  $\Sigma' \subseteq \Sigma$  and  $\Sigma'$  is a complete residue system modulo  $\beta$ .

**Proof.** If  $\Sigma$  is complete, then, by definition,  $\forall r \in \mathcal{R} : \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] : \|P\| = r$ , thus assume (6) holds. Choose any  $r \in \mathcal{R}$  and, in analogy with the DGT-algorithm, choose a sequence of digits  $d_0, d_1, d_2, \dots$  from the remainders  $r = r_0, r_1, r_2, \dots$  such that  $d_j \in \Sigma'$  and  $d_j \equiv r_j \pmod{\beta}$  (this is possible since  $\Sigma'$  contains a complete residue system modulo  $\beta$ ). Form the subsequence remainders as:

TABLE 1

$l$	0	1	2	3	4	5	6
$r_l$	$3 + 4i$	$1 - 3i$	$-2 - i$	$2 + i$	$-i$	$i$	1
$d_l$	1	0	1	1	1	1	1

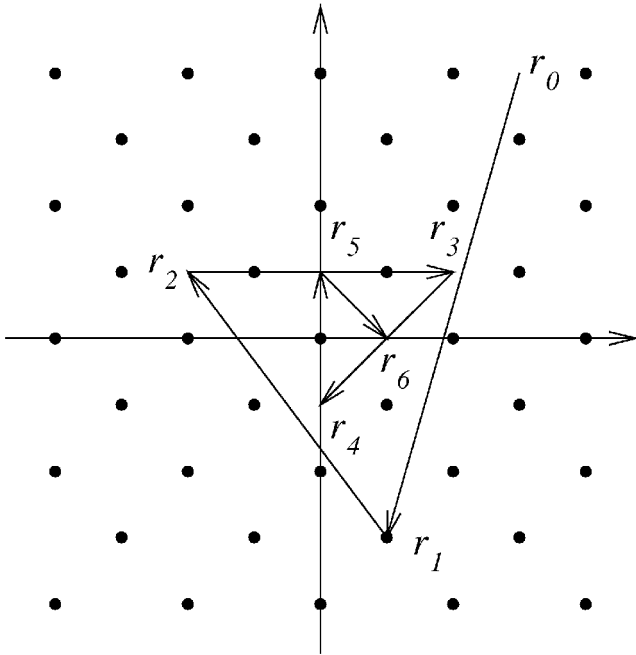


Fig. 1. DGT-algorithm example: Conversion of  $3 + 4i$  into a radix polynomial from  $\mathcal{P}_{\mathcal{I}}[-1 + i, \{0, 1\}]$ . The black dots represents the ideal  $[-1 + i]$ .

$$r_{j+1} = \frac{r_j - d_j}{\beta}. \tag{7}$$

Notice that  $\beta$  divides  $r_j - d_j$  since

$$d_j \equiv r_j \pmod{\beta} \Rightarrow r_j - d_j \in \langle \beta \rangle \Rightarrow \exists k \in \mathcal{R} : r_j - d_j = k\beta.$$

From the properties of the norm  $N$ , we deduce:

$$N(r_{j+1}) \leq \frac{N(r_j) + d_{max}}{N(\beta)}, \tag{8}$$

thus

$$N(r_{j+1}) \begin{cases} < N(r_j), & N(r_j) > \frac{d_{max}}{N(\beta)-1} \\ \leq \frac{d_{max}}{N(\beta)-1}, & N(r_j) \leq \frac{d_{max}}{N(\beta)-1}. \end{cases} \tag{9}$$

Since there exists only a finite number of elements of norm at most  $N(r_0)$ , after a finite number of steps we arrive at some remainder  $r_k$ , where, after

$$N(r_j) \leq \frac{d_{max}}{N(\beta)-1}, \text{ for } j \geq k. \tag{10}$$

By assumption, there exists a polynomial  $P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$  with  $\|P\| = r_k$ , and, by the recurrence (7), we have

$$r = r_k\beta^k + d_{k-1}\beta^{k-1} + \dots + d_1\beta + d_0,$$

thus the polynomial  $P' = P[\beta]^k + \sum_{i=0}^{k-1} d_i[\beta]^i \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$  with value  $\|P'\| = r$  is a representation of  $r$ , and  $\Sigma$  is complete base  $\beta$ .  $\square$

**Corollary 3.3.** *Let  $\mathcal{R}$  be an ordered ring, with positive elements  $\mathcal{R}^+$  and norm  $N : \mathcal{R} \rightarrow \mathbb{R}$ . Let  $\Sigma$  be a digit-set containing a complete residue system modulo  $\beta$ , then  $\Sigma$  is semicomplete if and only if*

$$\forall r \in \mathcal{R}^+ : N(r) \leq \frac{d_{max}}{N(\beta)-1} :: \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] : \|P\| = r,$$

where  $d_{max} = \max\{N(d) \mid d \in \Sigma'\}$ ,  $\Sigma' \subseteq \Sigma$ , and  $\Sigma'$  contains a complete residue system modulo  $\beta$ .

Theorem 3.2, together with the DGT-algorithm, can be used to establish the completeness of a digit-set.

**Example.** In Section 2, it was claimed that the digit-set  $\Sigma = \{-19, -13, 0, 1\}$  is complete for  $\beta = 3$ , but no proper subset is complete. By Theorem 3.2, it is sufficient to check the representability of the members of the set  $\{-6, -5, \dots, 6\}$  since  $d_{max} = 13$  can be chosen, using the absolute value as the norm. Here, it turns out that 2 is most difficult to represent, needing the digit  $-13$  as well as  $-19$  in its string representation  $1\ 0\ 0\ \overline{19}\ \overline{19}\ \overline{13}$ , whereas there is no finite representation if only one of these digits is available.

As an example, employing the absolute value as a norm on the integer ring, Theorem 3.2 can be used to check when a traditional, contiguous digit-set for the integers is complete, e.g., it can be used in the proof of the following lemma.

**Lemma 3.4.** *The digit-set  $\Sigma = \{r, r + 1, \dots, s - 1, s\}$  with  $-\lvert\beta\rvert \leq r \leq 0 \leq s \leq \lvert\beta\rvert$  and  $\lvert\Sigma\rvert = s - r + 1 \geq \lvert\beta\rvert$  is complete for the ring of integers  $\mathbb{Z}$  if*

$$(rs < 0 \wedge \beta > 0) \text{ or } \beta < 0 \tag{11}$$

and noncomplete otherwise.

Whenever  $\Sigma$  is complete for base  $\beta$ , by definition, any  $a \in \mathcal{R}$  has a radix polynomial representation, but Algorithm 3.1 (DGT) can only be applied when  $\Sigma$  is nonredundant ( $\Sigma$  is a complete residue system modulo  $\beta$ ). Theorem 3.2 provides a clue to a modified algorithm which can be applied also for redundant digit-sets. The problem here is that there may be infinitely many radix polynomial representations of a given  $a \in \mathcal{R}$  and, to assure termination, a finite representation must be enforced. But, for any  $a$  satisfying (6), we can choose a finite, shortest, *canonical* representation  $R_a \in \mathcal{P}[\beta, D]$ ,  $\|R_a\| = a$ , and these representations can then be tabulated. We may thus formulate a modified DGT-algorithm as follows:

**Algorithm 3.5.** *DGT-Algorithm for complete digit-sets*

**Stimulus:** A base  $\beta$ , a digit-set  $\Sigma$  that is complete for  $[\beta]$ , and an element  $r \in \mathcal{R}$ .

**Response:** A radix polynomial  $P = \sum_{i=0}^m d_i[\beta]^i \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$  with  $\|P\| = r$ .

**Method:**  $l \leftarrow 0$ ;  $r_0 \leftarrow r$ ;  $\delta \leftarrow \max_{d \in \Sigma} \{N(d)\}$

**while**  $r_l \neq 0$  **do**  
   **if**  $N(r_l) \leq \lfloor \frac{\delta}{N(\beta)-1} \rfloor$  **then**  
      $\langle$  choose  $d_l$  as the least significant digit of the canonical representation of  $r_l$   $\rangle$   
   **else**  
      $\langle$  choose some  $d_l \in \Sigma$  such that  $d_l \equiv r_l \pmod{\beta}$   $\rangle$   
      $r_{l+1} \leftarrow (r_l - d_l) / \beta$

$l \leftarrow l + 1$   
**end**

The algorithm thus needs a table containing for each  $r$  with  $N(r) \leq \lfloor \frac{\delta}{N(\beta)-1} \rfloor$ , the value of the least significant digit of the canonical polynomial of value  $r$ . If there is more than one polynomial of the lowest possible degree representing  $r$ , any one can be chosen as the canonical representation except when the degree is zero, where the canonical representation has to be chosen as a digit in the digit-set to assure termination.

#### 4 CONVERSION BETWEEN RADIX SYSTEMS

In practice, the most likely situation is that an element of a ring is given in some radix representation (the source system), but a conversion is needed into some other radix system (the target system) over the same ring. Algorithm 3.5 is sequential and, hence, does not exploit the possibilities of parallelism available if the digit-set of the target system is redundant.

In general, a conversion may be needed between systems with different radices (a base conversion), which can be performed by evaluating the source polynomial, and then applying one of the above DGT algorithms mapping the element into the target system.

However, in some cases, it is possible two use a parallel procedure. In general, this is the case if some power of the source base equals some power of the target base.

**Definition 4.1.** *The radices  $\beta_S$  and  $\beta_T$ , both elements of the same ring, are termed compatible if there exist integers  $p, q \geq 1$  and  $\delta \in \{-1, 1\}$  such that*

$$\beta_S^p = \delta \beta_T^q. \quad (12)$$

For instance  $-1 + i$  and 2 are compatible bases since  $(-1 + i)^4 = -4 = -1(2)^2$ , and 2 and 8 are compatible since  $2^3 = 8$ . Note that if  $\beta_S$  and  $\beta_T$  are compatible bases, then  $\mathcal{A}_{\beta_S} = \mathcal{A}_{\beta_T}$ , suggesting that if  $\Sigma_T$  is complete base  $\beta_T$ , then, for all  $P \in \mathcal{P}[\beta_S, \Sigma_S]$ , there exists at least one radix polynomial  $Q \in \mathcal{P}[\beta_T, \Sigma_T]$  such that  $\|P\| = \|Q\|$ .

To convert a polynomial  $P \in \mathcal{P}[\beta_S, \Sigma_S]$  into a polynomial in a representation using a compatible base  $\beta_T$ , we might proceed as follows (assuming  $\beta_S^p = \delta \beta_T^q$ ):

1. Convert from  $(\beta_S, \Sigma_S)$  into  $(\delta \beta_S^p, \Sigma') = (\beta_T^q, \Sigma')$ .
2. Convert from  $(\beta_T^q, \Sigma')$  into  $(\beta_T, \Sigma'')$ .

The first step of the conversion amounts to grouping digits and evaluating these groups as digits in an intermediate digit-set

$$\Sigma' = \left\{ \delta \sum_{j=0}^{p-1} d_j \beta_S^j \mid d_j \in \Sigma_S \wedge \delta \in \{-1, 1\} \right\}. \quad (13)$$

The second step is a bit more complicated since this step involves splitting digits from the set  $\Sigma'$  into groups of  $q$  digits from a final digit-set  $\Sigma''$ . The final digit-set  $\Sigma''$  should be chosen such that, for each digit  $d' \in \Sigma'$ , there should exist a  $q$ -digit radix polynomial in  $\mathcal{P}_T[\beta_T, \Sigma'']$  representing this

digit. The existence of such a digit-set is shown in the following lemma [14].

**Lemma 4.2.** *If  $\beta \in \mathcal{R}$ ,  $\Sigma' \subset \mathcal{R}$  and  $q > 0$ , then there exists a digit-set  $\Sigma'' \subset \mathcal{R}$  such that*

$$\Sigma' \subseteq \left\{ \sum_{j=0}^{q-1} d_j'' \beta^j \mid d_j'' \in \Sigma'' \right\}. \quad (14)$$

*Furthermore, if  $\Sigma'$  is redundant base  $\beta^q$ , then  $\Sigma''$  is necessarily redundant base  $\beta$ .*

**Example.** Let the source system be defined by  $\beta_S = 2$  and  $\Sigma_S = \{0, 1\} + i\{0, 1\}$ , and the target base be  $\beta_T = -1 + i$ . The bases are compatible since

$$\beta_S^2 = 2^2 = -1(-1 + i)^4 = -\beta_T^4,$$

thus  $p = 2$ ,  $q = 4$ , and  $\delta = -1$ .

The intermediate digit-set is calculated from (13) as

$$\begin{aligned} \Sigma' &= \{ \gamma(d_0 + d_1 2) \mid \gamma \in \{-1, 1\} \wedge d_1, d_2 \in \Sigma_S \} \\ &= (\{0, 1, 2, 3\} + i\{0, 1, 2, 3\}) \\ &\quad \cup (\{-3, -2, -1, 0\} + i\{-3, -2, -1, 0\}). \end{aligned}$$

This digit-set is redundant base  $\delta \beta_S^p = -4$ , thus, from Lemma 4.2, the final digit-set  $\Sigma''$  must also be redundant. It is easily shown that the redundant digit-set  $\Sigma'' = \{-1, 0, 1\}$  satisfies (14).

A table of  $q$ -digit polynomials from  $\mathcal{P}_T[\beta_T, \Sigma'']$  representing the digits in  $\Sigma'$  can now be constructed. When changing the base of a polynomial  $P \in \mathcal{P}[\beta_S, \Sigma_S]$ , groups of  $p = 2$  digits are used to generate intermediate digits from  $\Sigma'$ . From each of these digits groups of  $q = 4$  digits from  $\Sigma''$  are generated.

As an example, let us convert the polynomial

$$\begin{aligned} P &= 1[2]^5 + i[2]^4 + 1[2]^3 + (1 + i)[2]^2 + i[2] + 1 \\ &\in \mathcal{P}[2, \{0, 1\} + i\{0, 1\}] \end{aligned}$$

from the source system into a polynomial from the target system, using these steps.

$$\begin{array}{ccc} \underbrace{1+0 \quad 0+i}_{2+i} & \underbrace{1+0 \quad 1+i}_{-3-i} & \underbrace{0+i \quad 1+0}_{1+i2} \\ \underbrace{0 \quad \bar{1} \quad \bar{1} \quad 1}_{0 \quad \bar{1} \quad \bar{1} \quad 1} & \underbrace{\quad \quad \quad \quad}_{\bar{1} \quad 0 \quad 1 \quad 0} & \underbrace{\quad \quad \quad \quad}_{0 \quad \bar{1} \quad 0 \quad 1} \end{array}$$

Thus, the polynomial

$$\begin{aligned} Q &= -1[-1 + i]^{10} - 1[-1 + i]^9 + 1[-1 + i]^8 - 1[-1 + i]^7 \\ &\quad + 1[-1 + i]^5 - 1[-1 + i]^2 + 1 \end{aligned}$$

is a representation of  $\|P\|$  in the target system

$$\mathcal{P}[-1 + i, \{-1, 0, 1\}].$$

When converting a polynomial from the set  $\mathcal{P}[\beta, \Sigma_S]$  to a polynomial in the  $\mathcal{P}[\beta, \Sigma_T]$ , we will assume that the two systems are related in such a way that there exists a  $p \geq 1$  and a carry set  $C \subseteq \mathcal{R}$  such that, for all  $c \in C$  and  $d \in \Sigma_S$ , there exists  $c' \in C$  and  $e' \in \Sigma_T$  such that

$$c + d = c' \beta^p + e'. \quad (15)$$

It is useful in certain contexts with  $p > 1$ , e.g., when  $\Sigma_S$  and  $\Sigma_T$  are subsets of some subring  $\mathcal{S}$  of  $\mathcal{R}$  and there exists a  $p$  such that  $\beta^p \in \mathcal{S}$  so that also  $C \subset \mathcal{S}$ , e.g., when  $\mathcal{R} = \mathbb{Z}[i]$  and  $\mathcal{S} = \mathbb{Z}$  with  $\beta = \sqrt{2}i$  so  $\beta^2 = -2$  and for  $\beta = -1 + i$  where  $\beta^4 = -4$ .

We may then define a *conversion mapping*

$$\alpha_p : C \times \Sigma_S \rightarrow C \times \Sigma_T, \quad (16)$$

where  $\alpha_p(c, d) = (c', e')$  with  $c'$  and  $e'$  satisfying (15). Note that, for  $\Sigma_T$ , nonredundant  $\alpha_p$  is unique, while, for  $\Sigma_T$ , redundant there are several possible mappings  $\alpha_p$ . Also observe that the computation of carries in a conversion can take place as  $p$  parallel processes, each process taking care of one “carry-chain.”

Provided that the carry-set  $C$  is finite, a table of the conversion mapping may be constructed. Each entry of the table contains a pair  $c, e$  where  $c \in C, e \in \Sigma_T$ . Let  $C$  initially contain the zero element of  $\mathcal{R}$  and let  $d \in \Sigma_S$  be a digit from the source system. Since the target system is complete, there exists  $P', Q' \in \mathcal{P}[\beta, \Sigma_T]$  and  $e' \in \Sigma_T$  such that  $\|P'\| = d = \|Q'\|\beta^p + e'$ . Let  $c' = \|Q'\|$ , then  $c'$  is to be included in  $C$ . Repeat this for all  $d$  in  $\Sigma_S$ ; this takes care of the zero element in  $C$ . Now, repeat this process for any  $c \in C$ , mapping  $c + d$  into a pair  $c', e'$  such that  $c + d = c'\beta^p + e'$  for any  $d \in \Sigma_S$ , possibly adding new elements to  $C$ , and, thus, the need for new rows in the table. In this way, the complete carry set is deduced while constructing the conversion mapping. Under the same conditions on  $\mathcal{R}$  and its norm as for the DGT-Algorithms (3.1 and 3.5), we can now show termination of the construction:

**Theorem 4.3.** *For any  $\mathcal{P}[\beta, \Sigma_S]$  and  $\mathcal{P}[\beta, \Sigma_T]$  in a normed ring  $\mathcal{R}$  with  $\Sigma_T$  complete for  $\beta$ , there exist a conversion mapping,  $\alpha_p : C \times \Sigma_S \rightarrow C \times \Sigma_T$  with  $p \geq 1$  and finite carry-set  $C \subset \mathcal{R}$ .*

**Proof.** Let  $C_0 = \{c' \mid \exists e' \in \Sigma_T : d = c'\beta^p + e', d \in \Sigma_S\}$ . Relating to the algorithm described above, define

$$C_i = C_{i-1} \cup \{c' \mid \exists e' \in \Sigma_T : c + d = c'\beta^p + e', c \in C_{i-1}, d \in \Sigma_S\},$$

$i = 1, 2, \dots$ . Let  $\delta = \max\{N(d - e) \mid d \in \Sigma_S, e \in \Sigma_T\}$ , it is then easy to show that

$$N(c') \begin{cases} < N(c) & \text{for } N(c) > \frac{\delta}{N(\beta^p)-1} \\ \leq \frac{\delta}{N(\beta^p)-1} & \text{for } N(c) \leq \frac{\delta}{N(\beta^p)-1}, \end{cases}$$

hence,  $N(c'S)$  must remain bounded, so, for some  $n : C_n = C_{n-1}$ , and the algorithm can terminate with a finite carry-set  $C = C_n$ .  $\square$

**Example.** Consider conversion from the source digit-set  $\Sigma_S = \{-1, 0, 1\}$  into the target digit-set  $\Sigma_T = \{0, 1\}$  for the base  $\beta = -1 + i$  with  $p = 1$ . Note that  $\Sigma_S$  is redundant base  $\beta$ , whereas  $\Sigma_T$  is nonredundant. Table 2 shows the conversion mapping deduced while constructing the complete carry-set.

Employing the conversion mapping, it is possible to convert in linear time, starting at the least significant position, forwarding carries in the usual way. But, using parallelism, it is possible to convert faster. For simplicity of

TABLE 2

		$\Sigma_S$			
		-1	0	1	
C	$-1-i$	$i$ 1	$i$ 0	1	1
	$-i$	$i$ 0	$i$ 1	-1	0
	-1	$1+i$ 0	$1+i$ 1	0	0
	0	$1+i$ 1	0 0	0	1
	1	0 0	0 1	$-1-i$	0
	$i$	1 0	1 1	$-i$	0
	$1+i$	1 1	$-i$ 0	$-i$	1

notation in the following, we shall now assume that  $p = 1$ ; the generalization is trivial. Given a conversion mapping  $\alpha : C \times \Sigma_S \rightarrow C \times \Sigma_T$ , we then define a set of *carry-transfer functions*  $\{\gamma_d\}_{d \in \Sigma_S}, \gamma_d : C \rightarrow C$ :

$$\forall c \in C : \gamma_d(c) = c' \text{ where } \alpha(c, d) = (c', e').$$

and another set of functions  $\{\xi_d\}_{d \in \Sigma_S}, \xi_d : C \rightarrow \Sigma_T$ , the *digit-mapping functions*:

$$\forall c \in C : \xi_d(c) = e' \text{ where } \alpha(c, d) = (c', e').$$

Note that  $\gamma_d(c)$  is a function describing the mapping of an incoming carry value ( $c$ ) into its outgoing carry value ( $c'$ ), when “passing through” a particular digit value ( $d$ ) being converted. We can now immediately generalize carry-transfer functions to strings of digits:

$$\gamma_{d_k d_{k-1} \dots d_j}(c) = \gamma_{d_k}(\gamma_{d_{k-1}}(\dots \gamma_{d_j}(c) \dots))$$

or

$$\gamma_{d_k d_{k-1} \dots d_j} = \gamma_{d_k} \circ \gamma_{d_{k-1}} \circ \dots \circ \gamma_{d_j},$$

where  $\circ$  denotes functional composition. The function  $\gamma_{d_k d_{k-1} \dots d_j} : C \rightarrow C$  thus describes the carry transfer through the digit string  $d_k d_{k-1} \dots d_j$ . Since functional composition is associative, the carries into all positions can be computed in logarithmic time using parallel prefix computation.

This is optimal when  $\Sigma_T$  is nonredundant, but with  $\Sigma_T$  redundant, we expect to be able to perform the conversion in parallel and in constant time. The idea in the *multilevel conversion* is to perform it through (possibly several) conversions, each rewriting digits in parallel and moving carries one position forward, where the carries are absorbed. Note that the rewriting of a digit in each of these conversions is independent of the rewriting of its neighbors. Thus, there is only a limited carry propagation, corresponding to the fixed number of levels. This is the well-known technique used in redundant addition, which is a special case of conversion, converting from the digit-set consisting of digits formed as sums of two digits, back into the original digit-set. This type of addition can be performed in two or possibly three levels of conversions for standard digit-sets. Each conversion converts a digit  $d$  into some digit  $e$  and a carry  $c$  so that  $d = c\beta + e$  and then adds an incoming carry  $c'$  to  $e$  generating a digit  $e' = c' + e$ . Introducing the following notation for set operations in  $\mathcal{R}$ :

$$A + B = \{a + b \mid a \in A, b \in B\} \text{ for } A, B \subset \mathcal{R}$$

$$cA = \{ca \mid a \in A\} \text{ for } c \in \mathcal{R}, A \subset \mathcal{R},$$

each conversion maps a digit-set  $\Sigma_S \subseteq \Sigma + \beta C$  into the digit-set  $\Sigma + C \subseteq \Sigma_T$ , employing some intermediate digit-set  $\Sigma$  and carry-set  $C \neq \{0\}$ . The set  $\Sigma$  must be a complete residue set, but, as the target digit-set  $\Sigma_T$  is redundant, there may be several choices for  $\Sigma$  where  $\Sigma \subset \Sigma_T$ .

**Observation 4.4.** *Redundancy and completeness of the target digit-set are necessary, but not sufficient, conditions for the multilevel parallel, constant time conversion, or addition. The target digit-set has to be of the form  $\Sigma_T = \Sigma + C$ , where the set  $\Sigma$  must contain a complete residue system modulo  $\beta$  and  $C \neq \{0\}$ .*

This condition is trivially satisfied for the ordinary digit-sets consisting of a contiguous set of integers, e.g., for base 2 with  $\Sigma_T = \{-1, 0, 1\}$ , it is possible to choose either  $C = \{0, 1\}$  or  $C = \{-1, 0\}$ , so constant time conversion is possible from any subset of  $\{-1, 0\} + 2\{0, 1\} = \{-1, 0, 1, 2\}$ , respectively,  $\{0, 1\} + 2\{-1, 0\} = \{-2, -1, 0, 1\}$ . But, the redundant and complete digit-set  $\{-1, 0, 1, 4\}$  for base 3 does not allow such a splitting  $\Sigma_T = \Sigma + C$ , and constant time conversion into it is not possible, e.g., the number  $11 \cdots 12_3$  converts into either  $1\bar{1}\bar{1} \cdots \bar{1}\bar{1}_3$  or  $\bar{1}4\bar{1} \cdots \bar{1}\bar{1}_3$ , whereas  $11 \cdots 11_3$  maps into itself or various digit strings where 11 is substituted by 04. However, adding an extra digit 5 makes constant time conversion possible from any subset of the digit-set  $\{-3, -2, 0, 1, 2, 5\} = \{0, 1, 5\} + 3\{-1, 0\}$ , since  $\{-1, 0, 1, 4, 5\} = \{0, 1, 5\} + \{-1, 0\}$ , so here  $11 \cdots 12_3$  converts into  $11 \cdots 05_3$  with bounded carry propagation. Observe that there is also an alternative splitting of the digit-set  $\{-1, 0, 1, 4, 5\} = \{-1, 0, 4\} + \{0, 1\}$ , allowing parallel conversion from subsets of  $\{-1, 0, 2, 3, 4, 7\}$ .

Obviously, in the ring  $\mathbb{Z}$ , there are no particular reasons not to use contiguous digit-sets of the form  $\{r, r+1, \dots, s\}$ ,  $rs < 0$ ,  $s-r \geq \beta > 1$ , easily seen to satisfy the above conditions. Constant-time conversions into such redundant digit-sets were shown to be possible in [10]. But, the conditions on the structure of digit-sets as expressed by Observation 4.4 are of interest when investigating digit-sets from more general rings, e.g., in the complex domain and, in particular, when the ring does not have a lattice structure.

## 5 REPRESENTING COMPLEX NUMBERS

Using the formal framework developed in Sections 2 and 3, we shall investigate possible radix representations of the complex numbers. We will attempt to do this using two different approaches, the first being by examining the *Gaussian integers*, the second by examining a similar ring that we will refer to as *Eisenstein integers*.

### 5.1 Representing the Gaussian Integers

The Gaussian integers is a lattice on the field of complex numbers, defined as the set:

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}, \quad (17)$$

where  $i = \sqrt{-1}$ . It is a natural extension of the ring of integers and, as such, the number systems for the two rings exhibit many common characteristics. Designing a number system for complex numbers involves facing a larger number of decisions than when designing a number system for the integers, e.g., there is the possibility of choosing complex or integer valued digit-sets and a complex or integer base.

Initially, we will examine a more general ring of algebraic integers defined as:

$$\mathbb{Z}[\sqrt{-d}] = \{a + \sqrt{-d}b \mid a, b \in \mathbb{Z}\}, \quad (18)$$

with  $d \in \mathbb{Z}, d \geq 1$ . Note that if  $d = 1$ , then this ring is the ring of Gaussian integers. Furthermore, observe that the function  $N : \mathbb{Z}[\sqrt{-d}] \rightarrow \mathbb{R}$  defined as  $N(a + \sqrt{-d}b) = \sqrt{a^2 + db^2}$  is a norm on  $\mathbb{Z}[\sqrt{-d}]$  and that the set  $C = \{r, r+1, \dots, s\}$  is a complete residue system modulo  $\beta$ ,  $\beta = \sqrt{-d}$  and  $d \geq 2$  if the cardinality of  $C$  satisfies  $|C| = s - r + 1 = d$ .

**Lemma 5.1.** *For the ring  $\mathcal{R} = \mathbb{Z}[\sqrt{-d}]$ ,  $d \in \mathbb{Z}, d \geq 1$ , if  $|\Sigma| > |\mathbb{Z}[\sqrt{-d}]/\langle \beta \rangle| = \delta^2 + d\gamma^2$ , then  $\Sigma$  is redundant base  $\beta = \delta + \sqrt{-d}\gamma$ .*

**Proof.** The number of distinct residue classes is given by  $|\mathbb{Z}[\sqrt{-d}]/[\delta + \sqrt{-d}\gamma]| = \delta^2 + d\gamma^2 = k$ , as can be derived from classical results in algebraic number theory [18, pp. 62 and 121]. Let  $\Delta = \max\{N(d) \mid d \in \Sigma\}$  and  $\mathcal{Q}_n$  be the set of radix polynomials in  $\mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$  with degree at most  $n$ . The polynomials in  $\mathcal{Q}_n$  represent elements of  $\mathbb{Z}[\sqrt{-d}]$  that have norms bounded by:

$$\max\{N(\|P\|) \mid P \in \mathcal{Q}_n\} \leq \Delta \sum_{j=0}^n N(\beta)^j = \Delta \frac{N(\beta)^{n+1} - 1}{N(\beta) - 1}.$$

Since the norm of the base is  $N(\beta) = \sqrt{\delta^2 + d\gamma^2}$ , the number of elements that can be represented by radix polynomials of degree at most  $n$  is bounded by:

$$\Phi_n \leq \left( 2\Delta \frac{N(\beta)^{n+1} - 1}{N(\beta) - 1} + 1 \right)^2$$

$$\leq C \cdot (\delta^2 + d\gamma^2)^n + O(1) = C \cdot k^n + O(1).$$

Thus, by Lemma 2.7, the lemma is proven.  $\square$

### 5.2 Complex Number Systems with an Integer Radix

The straightforward approach for representing the elements of  $\mathbb{Z}[i]$  is to choose an integer base and a complex digit-set, e.g.,  $\beta \in \mathbb{Z}$  and  $\Sigma = \Sigma_r + i\Sigma_i = \{d_r + id_i \mid d_r \in \Sigma_r, d_i \in \Sigma_i\}$ . It is evident that if  $\Sigma_r$  and  $\Sigma_i$  are complete digit-sets base  $\beta$  for the integers, then  $\Sigma = \Sigma_r + i\Sigma_i$  is complete base  $\beta$  for the Gaussian integers; furthermore, if  $\Sigma_r$  or  $\Sigma_i$  is a redundant digit-set base  $\beta$  for the integers, then  $\Sigma$  is redundant base  $\beta$  for the Gaussian integers.

**Example.** The following base, digit-set combinations are examples of the large number of possible number systems that can be constructed combining two integer digit-sets:

1. Binary.  $\beta = 2$  and  $\Sigma = \{0, 1\} + i\{0, 1\}$ . Nonredundant and noncomplete.

TABLE 3  
Classification of Digit-Sets for  $\mathbb{Z}[\sqrt{-d}]$

Digit-set	$r, s$	$ \Sigma $	Redundant	$\eta$
Standard	$r = 0, s = d - 1$	$d$	false	0
Extended	$r = 0, s = d$	$d + 1$	true	1
Balanced	$r = -s$	$2s + 1 \geq d$	$2s + 1 > d$	$2s + 1 - d \geq 0$
Min. Red.	$-d \leq r \leq 0 \leq s \leq d$	$d + 1$	true	1
Max. Red.	$r = -d + 1, s = d - 1$	$2d - 1$	true	$d - 1$

- 2. Borrow-save.  $\beta = 2$  and

$$\Sigma = \{-1, 0, 1\} + i\{-1, 0, 1\}.$$

Redundant and complete.

- 3. Carry-Borrow-save.  $\beta = 2$  and

$$\Sigma = \{0, 1, 2\} + i\{-1, 0, 1\}.$$

Redundant and noncomplete, but semicomplete.

These number systems are constructed such that the real and imaginary parts of a number are written using, respectively, the real and imaginary parts of the digit-set. This has some obvious advantages since arithmetic can be based on the conventional integer arithmetic algorithms [19]. Furthermore, converting from a conventional representation to a complex representation and computing the complex conjugate are fairly simple tasks.

### 5.3 Imaginary Radix Number Systems

Instead of using an integer radix, we could alternatively use a purely imaginary radix.

**Lemma 5.2.** *The digit-set  $\Sigma = \{r, r + 1, \dots, s\} \subset \mathbb{Z}$  is complete base  $\beta = \sqrt{-d}$ ,  $d \in \mathbb{Z}$ ,  $d > 1$  for the ring  $\mathbb{Z}[\sqrt{-d}]$  if and only if  $\Sigma$  is complete base  $-d$  for the integers.*

If we allow a single extra digit immediately to the right of the radix point in the definition of completeness, it is in some cases possible to define number systems that are not only complete for the ring  $\mathbb{Z}[\sqrt{-d}]$ , but also for the Gaussian integers.

Define the set of radix polynomials with one fractional digit as

$$\mathcal{P}_{-1}[\beta, \Sigma] = \{P + p_{-1}[\beta]^{-1} \mid P \in \mathcal{P}_{\mathbb{I}}[\beta, \Sigma] \wedge p_{-1} \in \Sigma\}. \quad (19)$$

**Definition 5.3.** *A digit-set  $\Sigma$  is fraction-complete base  $\beta$  for the ring  $\mathcal{R}$  if and only if*

$$\forall r \in \mathcal{R} : \exists P \in \mathcal{P}_{-1}[\beta, \Sigma] : \|P\| = r.$$

**Lemma 5.4.** *If  $\beta = \sqrt{-d}$ ,  $d \in \mathbb{Z}$ ,  $d > 1$  and  $\Sigma = \{r, r + 1, \dots, s\}$ ,  $-d \leq r \leq 0 \leq s \leq d$  is complete base  $\beta$  for  $\mathbb{Z}[\sqrt{-d}]$ , then  $\Sigma$  is fraction-complete base  $\beta$  for the Gaussian integers if and only if  $\sqrt{d} \in \mathbb{Z}$  (i.e.,  $d$  is of the form  $d = k^2$  for some  $k \in \mathbb{Z}$ ,  $|k| > 1$ ).*

**Proof.** Assume that  $d = k^2$ ,  $k \in \mathbb{N}$ ,  $k > 1$ . Since  $\Sigma$  contains a complete residue system modulo  $k^2$ , there exists a set  $\Sigma' = \{kp, k(p + 1), \dots, k(q - 1), kq\}$ ,  $-k \leq p \leq 0 \leq q \leq k$

such that  $\Sigma' \subset \Sigma$  and the set  $\Sigma'' = \{p, \dots, q\}$  is a complete residue system modulo  $k$ .

Thus, for any  $z \in \mathbb{Z}$ , there exists  $b \in \mathbb{Z}$ ,  $d' \in \Sigma'$ , and  $d'' \in \Sigma''$  such that  $z = bk - d' = bk - d''/k$ .

Since  $\Sigma$  is complete base  $\beta$  for  $\mathbb{Z}[\sqrt{-k^2}]$ , for any  $a + \sqrt{-k^2}b \in \mathbb{Z}[\sqrt{-k^2}]$  there exists a radix polynomial  $P \in \mathcal{P}_{\mathbb{I}}[\beta, \Sigma]$  such that  $\|P\| = a + \sqrt{-k^2}b$ .

Forming the polynomial  $P' = P + d'[\beta]^{-1} \in \mathcal{P}_{-1}[\beta, \Sigma]$  with value  $\|P'\| = \|P\| + d' \frac{1}{\sqrt{-k^2}} = a + kib - \frac{d''}{k}i = a + iz$ , we conclude that  $\Sigma$  is fraction complete.

Assume  $\sqrt{d} \notin \mathbb{Z}$ , thus  $\sqrt{d}$  is an irrational number. In order to represent  $i = \sqrt{-d}/\sqrt{d}$ , we will implicitly have to represent  $1/\sqrt{d}$  using an extended radix polynomial with a finite number of digits from  $\mathcal{P}[-d, \Sigma]$ ; this is obviously not possible since  $1/\sqrt{d}$  is an irrational number.  $\square$

Classifying a number of different digit-sets, from Lemmas 3.4, 5.2, and 5.4, we derive the properties displayed in Table 3.

**Example.** Imaginary Radix, Complex Number Representations.

1. Binary.  $\beta = \sqrt{-2}$ ,  $\Sigma = \{0, 1\}$ , and  $\mathcal{R} = \mathbb{Z}[\sqrt{-2}]$ . Standard digit-set, nonredundant, and complete.
2. Quarter-Imaginary.  $\beta = \sqrt{-4} = 2i$  and  $\Sigma = \{0, 1, 2, 3\}$ .

Standard digit-set, nonredundant, complete and fraction-complete (this number system was proposed by Knuth in [9]).

3. Borrow-Save (Quarter-Imaginary).  $\beta = 2i$  and  $\Sigma = \{-3, \dots, 3\}$ . Maximally redundant digit-set, complete, fraction-complete (addition in Redundant number systems of this form has been examined in [13]).

### 5.4 Complex Radix Number Systems

As suggested in [16], we could use a fully complex base, e.g.,  $\beta = \gamma + i\delta$ ,  $\gamma \neq 0$  and  $\delta \neq 0$ . Here, we will only examine number systems for which the digit-set contains exclusively integer digits. Observe that the set  $C = \{r, r + 1, \dots, s\}$  is a complete residue system modulo  $\beta = \gamma + \delta i$ ,  $\gamma \in \mathbb{Z}$ ,  $|\gamma| \geq 1$  and  $\delta \in \{-1, 1\}$  if  $|C| = s - r + 1 = \gamma^2 + 1$ .

**Lemma 5.5.** *The digit-set  $\Sigma = \{r, \dots, s\}$ ,  $-A^2 \leq r \leq 0 \leq s \leq A^2$  and  $|\Sigma| = s - r + 1 \geq A^2 + 1$  is complete base  $\beta = -A + \delta i$ ,  $A \geq 1$ ,  $\delta \in \{-1, 1\}$  for the Gaussian integers.*

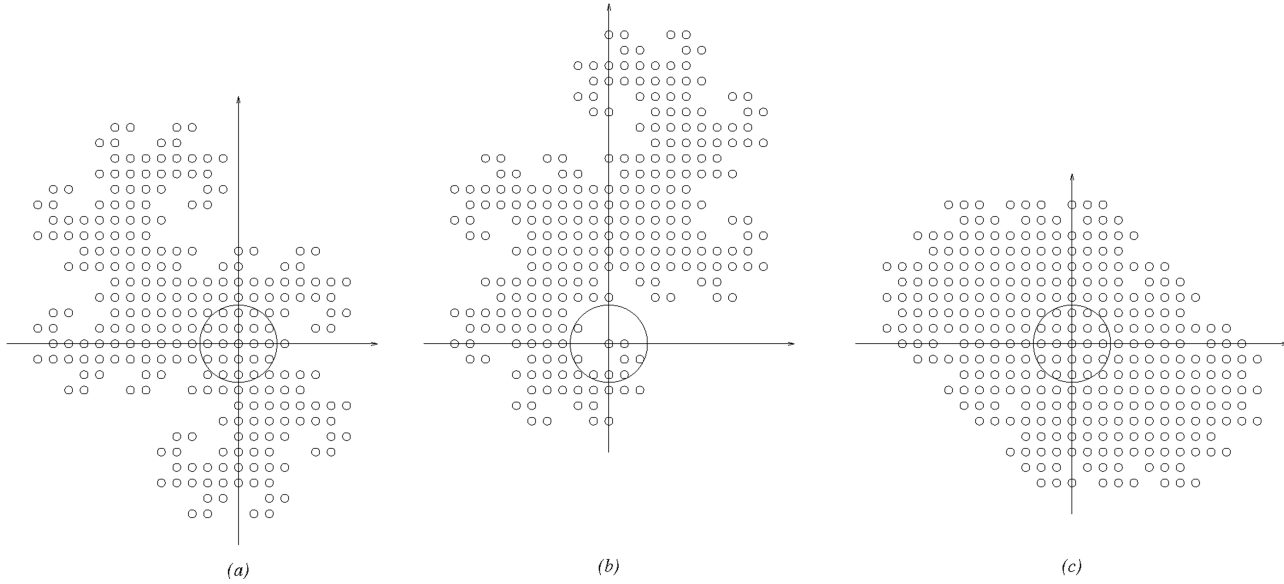


Fig. 2. The Gaussian integers representable with radix polynomials of degree 7, using the number systems: (a)  $\beta = -1 + i, \Sigma = \{0, 1\}$ , (b)  $\beta = 1 + i, \Sigma = \{0, 1\}$ , and, in (c), the elements representable using polynomials of degree 5 with the redundant number system  $\beta = 1 + i, \Sigma = \{-1, 0, 1\}$ . The elements that lie within the circles all have norms less than  $d_{max}/(N(\beta) - 1) = 1/(\sqrt{2} - 1)$ , thus, from Theorem 3.2, we immediately conclude that the number systems (a) and (c) are complete.

**Proof.** The proof is a slight generalization of the one given in [8].  $\square$

**Lemma 5.6.** *The symmetric digit-set  $\Sigma = \{-s, \dots, s\}$  with  $\lceil \frac{\gamma^2}{2} \rceil \leq s \leq \gamma^2$  is complete base  $\beta = \gamma + \delta i, \gamma \in \mathbb{Z}, |\gamma| \geq 1$ , and  $\delta \in \{-1, 1\}$  for the Gaussian integers.*

**Proof.** If  $\beta = -A - i$ , then by Lemma 5.5, we have that  $\Sigma$  is complete base  $\beta$ , thus, for any  $a + ib \in \mathbb{Z}[i]$ , there exists a radix polynomial  $P = \sum_{j=0}^n d_j [-A - i]^j \in \mathcal{P}_{\mathcal{I}}[-A - i, \Sigma]$  such that  $\|P\| = a + ib$ .

If, conversely,  $\beta = A + i$ , then by forming the polynomial:

$$\begin{aligned} P' &= \sum_{j=0}^n d_j (-1)^j [(-1)(-A - i)]^j \\ &= \sum_{j=0}^n d'_j [A + i]^j \in \mathcal{P}_{\mathcal{I}}[A + i, \Sigma], \end{aligned}$$

with value  $\|P'\| = \|P\| = a + ib$ , we conclude that  $\Sigma$  is also complete base  $\beta = A + i$ .

The case  $\beta = A - i$  is analogous to the above.  $\square$

The set of elements that can be represented using the standard digit set  $\Sigma_{std} = \{0, 1, \dots, A^2\}$  is a somewhat nonsymmetric set, whereas the set of elements that can be represented using a symmetric redundant digit-set has a higher degree of symmetry (see Fig. 2).

**Example.** The following base, digit-set combinations are examples of complete number systems:

1. Binary.  $\beta = -1 \pm i$  and  $\Sigma = \{0, 1\}$ . Standard digit-set, nonredundant, and complete.
2. Borrow-save.  $\beta = \pm 1 \pm i$  and  $\Sigma = \{-1, 0, 1\}$ . Minimally and maximally redundant digit-set, complete.

### 5.5 Representing Eisenstein Integers

This section is devoted to the study of the ring  $\mathbb{Z}[\rho] = \{a + b\rho \mid a, b \in \mathbb{Z}\}$ , where  $\rho = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$  (i.e., the third complex root of unity). This ring is a lattice on the complex field (Fig. 3); it is similar to the Gaussian integers, but, as will be shown, it exhibits some interesting properties.

Note that both  $\mathbb{Z}[i]$  and  $\mathbb{Z}[\rho]$  are algebraic integers since  $i$  and  $\rho$  are roots of the polynomials  $i^2 + 1 = 0$ , respectively,  $\rho^2 + \rho + 1 = 0$ , with rational coefficients. Furthermore, observe that the set  $C = \{0, 1, \dots, |\beta| - 1\} + \rho\{0, 1, \dots, |\beta| - 1\}$  is a complete residue system modulo  $\beta$  with  $\beta \in \mathbb{Z}$  and  $|\beta| > 1$ .

**Lemma 5.7.** *For the ring  $\mathbb{Z}[\rho]$ , if  $|\Sigma| > |\mathbb{Z}[\rho]/\langle\beta\rangle|$ , then  $\Sigma$  is redundant base  $\beta \in \mathbb{Z}, |\beta| > 1$ .*

**Proof.** Analogous to the one given for Lemma 5.1.  $\square$

From Lemma 5.7, we conclude that, if a digit-set has more than  $\beta^2$  digits, then the digit-set is redundant. It is easy to see that the ring  $\mathcal{W} = \{a_0 + a_1\rho + a_2\rho^2 \mid a_0, a_1, a_2 \in N \cup \{0\}\}$  is isomorphic to the ring  $\mathbb{Z}[\rho]$ . Thus, we conclude that, since  $\mathbb{Z}[\rho]$  and  $\mathcal{W}$  are essentially equivalent, we may instead study  $\mathcal{W}$  as a valid representation of the elements in  $\mathbb{Z}[\rho]$ . For convenience, we introduce the following notation:  $D_t = \{0, 1, \dots, t\}$  and  $H_t = D_t + D_t\rho + D_t\rho^2$ .

**Theorem 5.8.** *The digit-set  $\Sigma = D_{|\beta|-1} + \rho D_{|\beta|-1}$  is complete base  $\beta \in \mathbb{Z}$  for the ring  $\mathbb{Z}[\rho]$  if  $\beta < -1$ .*

**Proof.** Take any  $r = a_0 + a_1\rho \in \mathbb{Z}[\rho]$ . In Section 3, it was shown that the digit-set  $\Sigma_z = D_{|\beta|-1}$  is complete base  $\beta < -1$  for the integers. Thus, there exist polynomials  $P_0, P_1 \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma_z]$  representing the (possibly negative) integers  $a_0$ , respectively,  $a_1$ . Forming the polynomial  $P' = P_0 + P_1\rho \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$  with value  $\|P'\| = a_0 + a_1\rho$ , we conclude that  $\Sigma$  is complete.  $\square$

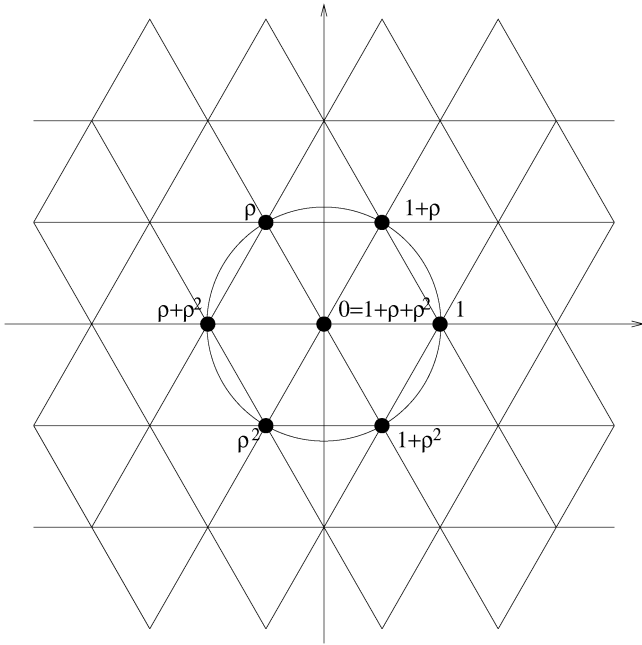


Fig. 3. The ring  $\mathbb{Z}[\rho]$  and the digit-set  $\Sigma = \{0, 1\} + \{0, 1\}\rho + \{0, 1\}\rho^2$ .

As shown in [4], it can be beneficial to represent the ring  $\mathbb{Z}[\rho]$  using the redundant set  $\mathcal{W} = \{a + b\rho + c\rho^2 \mid a, b, c \in \mathbb{N} \cup \{0\}\}$ . It was also shown that addition in  $H_{\beta-1}$  for  $\beta > 6$  is possible, using the following theorem, here reformulated in our terminology:

**Theorem 5.9.** *If  $a$  satisfies  $\frac{2}{3}\beta - 1 < a < \beta$ , then  $H_a$  is complete base  $\beta \in \mathbb{Z}$  with  $\beta > 1$  for the set  $\mathcal{W}$  and*

$$H_\beta \subset H_a + \beta H_1. \tag{20}$$

The proof in [4] is based on geometrical considerations of set coverings. By similar arguments it is possible to show the following additional set inclusion under the same conditions on  $a$  and  $\beta$ :

$$H_{2a+1} \subset H_a + \beta H_1. \tag{21}$$

Since  $H_{\beta-1} = D_{\beta-1} + D_{\beta-1}\rho + D_{\beta-1}\rho^2$  is redundant and complete for radix  $\beta$ , we expect to be able to perform

addition and conversion into this digit-set in parallel and constant time. In particular, the binary digit-set  $H_1 = \{0, 1\} + \{0, 1\}\rho + \{0, 1\}\rho^2$  is complete and redundant base  $\beta = 2$ . The digits of this digit-system were depicted in Fig. 3, and addition in this digit-set was shown possible in [4] by grouping three base 2 digits into digits of base 8. As an illustration of the use of Observation 4.4, we shall extend that result on addition in radix 2. The analysis in [4] was not sufficient to assure addition for  $\beta \leq 6$ , but, using the set inclusion (21) and Observation 4.4, we shall now show that conversion into, and addition in,  $H_{\beta-1}$  is possible for  $\beta \geq 4$ .

Observation 4.4 cannot be applied here for  $\beta = 2$  since, by Theorem 5.9, then the only possible value for  $a$  is 1 and  $H_a = H_1$  is not a proper subset of  $H_{\beta-1}$ .

For  $\beta = 3$ , choosing  $a = 2$  then, since  $H_{\beta-1} = H_2 = H_1 + H_1$ , Observation 4.4 can be applied, and constant time conversion from  $H_1 + \beta H_1 = H_1 + 3H_1$  into  $H_2$  is possible. But neither of the inclusions (20) and (21) are really applicable here; in fact, the largest set  $H_t$  satisfying  $H_t \subset H_1 + 3H_1$  is  $H_1$ .

However, for  $\beta \geq 4$  it is possible to choose  $a = \beta - 2$ . By Observation 4.4, it is possible to convert from

$$H_{\beta^2-\beta-1} = H_{\beta-1} + \beta H_{\beta-2}$$

into

$$H_{\beta-1} + H_{\beta-2} = H_{2\beta-3} = H_{2a+1} \subset H_a + \beta H_1$$

also using (21). But, since  $a = \beta - 2$ , in another conversion  $H_a + \beta H_1 = H_{\beta-2} + \beta H_1$  can be converted into  $H_{\beta-2} + H_1 = H_{\beta-1}$ . Thus, we have proven the following:

**Lemma 5.10.** *For  $\beta \geq 4$  conversion from the digit-set  $\Sigma_S = D_{\beta^2-\beta-1} + D_{\beta^2-\beta-1}\rho + D_{\beta^2-\beta-1}\rho^2$  into the digit-set  $\Sigma_T = D_{\beta-1} + D_{\beta-1}\rho + D_{\beta-1}\rho^2$  can be performed in constant time, with carries propagating at most two positions. In particular, addition in the set  $\mathcal{W}$  can be realized in constant time using the digit-set  $\Sigma_T$  for  $\beta = 2$  by base-conversion into radix-4.*

Since the  $\beta - ary$  numbers written over  $\mathbb{Z}[i]$ , respectively  $\mathcal{W}$ , are not identical, conversion between elements from the two extended rings cannot be exact. This is due to the fact that, since  $\rho = \frac{1+i\sqrt{3}}{2}$  and  $\frac{\sqrt{3}}{2}$  is an irrational number, there

TABLE 4  
Properties of Low-Radix Systems for Representing Complex Numbers

base	digit-set	ring	compl.	redund.	closed	fal	bpd	eff
2	$\{0, 1\} + i\{0, 1\}$	$\mathbb{Z}[i]$	false	false	false	-	2	1
2	$\{-1, 0, 1\} + i\{-1, 0, 1\}$	$\mathbb{Z}[i]$	true	true	false	2	4	$\frac{1}{2}$
$\sqrt{-2}$	$\{0, 1\}$	$\mathbb{Z}[\sqrt{-2}]$	true	false	true	-	1	1
$\sqrt{-2}$	$\{-1, 0, 1\}$	$\mathbb{Z}[\sqrt{-2}]$	true	true	true	2	2	$\frac{1}{2}$
$2i$	$\{0, 1, 2, 3\}$	$\mathbb{Z}[i]$	true	false	false	-	2	1
$2i$	$\{-2, \dots, 2\}$	$\mathbb{Z}[i]$	true	true	false	3	3	$\frac{2}{3}$
$2i$	$\{-3, \dots, 3\}$	$\mathbb{Z}[i]$	true	true	false	2	3	$\frac{2}{3}$
$-1 \pm i$	$\{0, 1\}$	$\mathbb{Z}[i]$	true	false	true	-	1	1
$\pm 1 \pm i$	$\{-1, 0, 1\}$	$\mathbb{Z}[i]$	true	true	true	2	2	$\frac{1}{2}$
-2	$\{0, 1\} + \rho\{0, 1\}$	$\mathbb{Z}[\rho]$	true	false	false	-	2	1
2	$\{0, 1\} + \rho\{0, 1\} + \rho^2\{0, 1\}$	$\mathbb{Z}[\rho]$	true	true	true	3	3	$\frac{2}{3}$

does not exist a finite extended radix polynomial in  $\mathcal{P}[\beta, \Sigma]$  with  $\beta \in \mathbb{Z}$  and  $\Sigma \subset \mathbb{Z}$  that represents  $\frac{\sqrt{3}}{2}$ .

## 6 CONCLUSION

A summary of some properties of various *low radix* number systems for representing complex numbers has been compiled in the form of Table 4.

The last two columns of the table deal with the efficiency of representation, *bpd* is the number of bits needed to encode the digits, and *eff* is a measure of efficiency of the combined representation and digit encoding, defined as follows:

$$eff = \lim_{k \rightarrow \infty} \frac{\lceil \log_2 |\{P \mid P \in \mathcal{P}_{0,k-1}[\beta, \Sigma]\}| \rceil}{k \lceil \log_2 |\Sigma| \rceil}.$$

Thus, *eff* is the asymptotic ratio between the number of bits needed to encode the values representable by radix polynomials and the number of bits needed to represent the digits of the polynomial, using a minimal binary encoding of the digits. Note that the actual encoding of digits can only influence the implementation logic of the primitives and, thus, only change the area and timing by constant factors.

In order to evaluate the relative merits of these number systems, we will now turn our attention to arithmetic operations performed in these systems. As for storage, and if digit serial arithmetic is an application, an encoding using few bits per digit (*bpd*) will be desirable since this will minimize module size and intermodule wiring. If fast addition is needed, the system should be redundant and need as few levels of logic as possible (*fal* is the number of full-adder levels needed for parallel, constant time addition). Furthermore, if a digit-set is closed under multiplication (i.e., the product of two arbitrary digits is again a digit), performing division and multiplication on radix polynomials written over the digit-set is simpler than if the digit-set is not closed under multiplication. In the latter case, when forming the product of a single digit and a number, the individual digit-by-digit products will introduce a carry effect into the neighboring positions. As an example, the binary integer system, e.g.,  $\beta = 2$  and  $\Sigma = \{0, 1\}$ , forms a closed group under multiplication. For the Gaussian integers, the number system  $\beta = 2$  with  $\Sigma = \{0, 1\} + i\{0, 1\}$  does not share this property since, for instance,  $(1+i)(-1+i) = -2 \notin \Sigma$ , thus  $\Sigma$  is not closed under multiplication. But, the systems  $(\sqrt{-2}, \{-1, 0, 1\})$  and  $(\pm 1 \pm i, \{-1, 0, 1\})$  seem very promising.

However, performing digit-by-register multiplication, as required in various multiplication and division algorithms, might also be relatively easy if the partial products can be generated by a shifting process possibly combined with negation. This is the reason why modified Booth recoding, e.g., conversion from the nonredundant system  $(4, \{0, 1, 2, 3\})$  into the redundant system  $(4, \{-2, 1, 0, 1, 2\})$ , is popular in multiplier design. It can be shown that, with proper encoding, partial products can be formed trivially in the system  $(2i, \{-2, -1, 0, 1, 2\})$  using a simple shifting rule.

## ACKNOWLEDGMENTS

This work has been supported by grant no. 5.21.08.02 from the Danish Research Council.

## REFERENCES

- [1] J.-P. Allouche, E. Cateland, W. Gilbert, H.-O. Peitgen, J. Shallit, and G. Skordev, "Automatic Maps in Exotic Number Systems," *Theory of Computing Systems*, vol. 30, pp. 285-331, 1997.
- [2] T. Aoki, H. Amada, and T. Higuchi, "Real/Complex Reconfigurable Arithmetic Using Redundant Complex Number Systems," *Proc. 13th IEEE Symp. Computer Arithmetic*, pp. 200-207, 1997.
- [3] A. Avizienis, "Signed-Digit Number Representations for Fast Parallel Arithmetic," *IRE Trans. Electronic Computers*, vol. 10, pp. 389-400, Sept. 1961.
- [4] J. Duprat, Y. Herreros, and S. Kla, "New Representation of Complex Numbers and Vectors," *Proc. 10th IEEE Symp. Computer Arithmetic*, pp. 2-9, 1991.
- [5] W. Gilbert, "Radix Representations of Quadratic Fields," *J. Math. Analysis and Applications*, vol. 83, pp. 264-274, 1981.
- [6] I. Kátai, "Number Systems in Imaginary Quadratic Fields," *Ann. Univ. Budapest, Sect. Comp.*, vol. 14, pp. 91-103, 1994.
- [7] I. Kátai and B. Kovács, "Canonical Number Systems in Imaginary Quadratic Fields," *Acta Math. Acad. Sci. Hungaricae*, vol. 37, pp. 1-3, 1981.
- [8] I. Kátai and J. Szabo, "Canonical Number Systems for Complex Integers," *Acta Sci. Math. (Szeged)*, vol. 37, pp. 255-260, 1975.
- [9] D.E. Knuth, "An Imaginary Number System," *Comm. ACM*, vol. 3, no. 4, pp. 245-247, Apr. 1960.
- [10] P. Kornerup, "Digit-Set Conversions: Generalizations and Applications," *IEEE Trans. Computers*, vol. 43, no. 6, pp. 622-629, June 1994.
- [11] D.W. Matula, "Radix Arithmetic: Digital Algorithms for Computer Architecture," *Applied Computation Theory: Analysis, Design, Modeling*, R.T. Yeh, ed., chapter 9, pp. 374-448, Englewood Cliffs, N.J.: Prentice Hall, 1976.
- [12] D.W. Matula, "Basic Digit Sets for Radix Representation," *J. ACM*, vol. 29, no. 4, pp. 1,131-1,143, Oct. 1982.
- [13] A. Munk Nielsen and J.-M. Muller, "Borrow-Save Adders for Real and Complex Number Systems," *Proc. Second Conf. Real Numbers and Computers*, Marseille, France, Apr. 1996.
- [14] A. Munk Nielsen and P. Kornerup, "Generalized Base and Digit-Set Conversion, Extended Abstract," *Proc. SCAN 97, Lyon*, pp. XII-8-11, Sept. 1997.
- [15] A. Munk Nielsen and P. Kornerup, "On Radix Representation of Rings," *Proc. 13th IEEE Symp. Computer Arithmetic*, pp. 34-43, 1997.
- [16] W. Penney, "A 'Binary' System for Complex Numbers," *J. ACM*, vol. 12, no. 2, pp. 247-248, Apr. 1965.
- [17] B. Parhami, "On the Implementation of Arithmetic Support Functions for Generalized Signed Digit Number Systems," *IEEE Trans. Computers*, vol. 42, no. 3, pp. 379-384, Mar. 1993.
- [18] L.N. Steward and D.O. Toll, *Algebraic Number Theory*. London: Chapman and Hall, 1979.
- [19] B. Wei, H. Du, and H. Chen, "A Complex-Number Multiplier Using Radix-4 Digits," *Proc. 12th Symp. Computer Arithmetic*, pp. 84-90, 1995.



**Asger Munk Nielsen** received the masters degree in computer engineering in 1995 and the PhD degree in 1997, both from Odense University. He is currently with MIPS technologies, Inc., Copenhagen. This work was performed while he was performing his PhD studies and initiated during a stay at ENS in Lyon, 1995. He also spent half a year in Dallas, 1996, with Southern Methodist University and Cyrix corporation. The title of his PhD dissertation is "Number Systems and Digit Serial Arithmetic," dealing in particular with the representation of, and arithmetic on complex numbers. His research interests are more general in computer architecture, in particular, computer arithmetic and number representations.



**Peter Kornerup** received the mag.scient. degree in mathematics from Aarhus University, Denmark, in 1967. After a period with the University Computing Center, from 1969, involved in establishing the computer science curriculum at Aarhus University, he helped found the Computer Science Department in 1971 and, through most of the 70s and 80s, he served as chairman of the department. He spent a leave during 1975/76 with the University of Southwestern Louisiana, Lafayette, and another in 1979 with Southern Methodist University, Dallas, Texas. Since 1988, he has been a professor of computer science at Odense University, Odense, Denmark, where he has also served as the chairman of its Department of Mathematics and Computer Science. His research interests include compiler construction, computer networks and computer architecture, but, in particular, computer arithmetic and number representations.

Professor Kornerup has served on the program committees for a number of IEEE, ACM, and other meetings, in particular, he has been on the Program Committee of the Fourth through the 13th IEEE Symposium on Computer Arithmetic and served as program cochair for these symposia in 1983, 1991, and, presently, for ARITH-14 in 1999. He also served as an associate editor of the *IEEE Transactions on Computers* during 1991-1995 and is a member of the IEEE.