On Radix Representation of Rings *

Asger Munk Nielsen
and
Peter Kornerup
Dept. of Mathematics and Computer Science
Odense University, Denmark
e-mail: {asger,kornerup}@imada.ou.dk

Abstract

This paper presents a thorough analysis of radix representations of elements from general rings, in particular we study the questions of redundancy, completeness and mappings into such representations. After a brief description of the more usual representations of integers, a more detailed analysis of various complex number systems is performed. This includes the "classical" complex number systems for the Gaussian integers, as well as the Eisenstein integers.

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. By conception designing a number system amounts to choosing a representation suitable for computer storage of the elements of a set of numbers, such that arithmetic operations can be performed with relative ease on these numbers, by merely manipulating their representation.

No number system has achieved the kind of wide spread acceptance and popularity that the radix representations have. Radix based number systems represent the elements of a set (like the integers) by a positional notation known as *radix polynomials*. Each element is represented as a weighted sum of *digits*, where the weights are increasing integer powers of the *base* or *radix*. This form of notation has the advantage that each digit can be drawn from a small finite *digit set*, 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.

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. It seems logical to investigate alternative number representations for these problems, addressing such issues as redundancy and storage efficiency, that has brought by the speed improvements of modern micro processor technology. Unfortunately assessing such important questions as completeness and redundancy, are no longer 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 [7, 8] to the general notion of rings, and gives a thorough analysis of representations of complex numbers.

2 On the Representation of Numbers

This paper is devoted to the study of radix representations of rings. As a foundation for this study, we will rely on the algebraic structure of sets of polynomials. If $\mathcal{R}$ is a

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

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

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

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

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_l x^l, \quad (2)$$

where $\infty > m \geq l > -\infty$ and $a_i \in \mathcal{R}$.

When an element of a ring is represented in positional notation, it is customary to use a weighted notation, where each digit has weight equal to some power of the radix. The radix is in itself an element of the ring and the digits of the number are elements of a finite subset of the ring, this subset is termed the *digit-set*. As described, a number 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 Σ. In this paper we will assume that the zero element of the ring is always part 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* Σ

$$\mathcal{P}_{\mathcal{I}}[\beta, \Sigma] = \{P([\beta]) = d_m[\beta]^m + d_{m-1}[\beta]^{m-1} + \ldots + d_0[\beta]^0\}$$
with $d_m, d_{m-1}, \ldots, d_0 \in \Sigma \wedge 0 \leq m < \infty$.

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

Definition 2.2 *Extended Radix Polynomials over* Σ

$$\mathcal{P}[\beta, \Sigma] = \{P([\beta]) = d_m[\beta]^m + d_{m-1}[\beta]^{m-1} + \ldots + d_l[\beta]^l\}$$
with $d_m, d_{m-1}, \ldots, d_l \in \Sigma \wedge -\infty < l \leq m < \infty$.

The extended radix polynomials may be thought of as algebraic objects representing numbers with fractional digits. If we replace $[\beta]$ by β 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*

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

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

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

Observe that i here may be negative, so the $\beta - ary$ numbers may contain fractional parts.

Example: For the ring $\mathcal{R} = \mathbb{Z}$ the set $\mathcal{A}_2$ constitutes the binary numbers, $\mathcal{A}_8$ the octal numbers, and $\mathcal{A}_{16}$ the hexadecimal numbers. □

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 $\mathcal{A}_\beta$.

Note that the evaluation mapping is not an isomorphism, since it is not necessarily one-to-one, for instance if one number can be represented by more that 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 Σ *is complete base* β *for the ring* $\mathcal{R}$ *iff*

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

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 non-fractional 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 Σ is complete base β for the ring $\mathcal{R}$, it is also complete for the $\beta - ary$ numbers, in the following sense:

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

Let $[z]$ denote [1] 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 $r_1 \equiv r_2 \mod I$. If a set S has exactly one element from each distinct co-set in $\mathcal{R}/I$ we will say that S is a *complete residue system modulo* I.

Example: For the ring of integers, the ideal generated by $\beta \in \mathbb{Z}$ is defined as $[\beta] = \{z\beta \mid z \in \mathbb{Z}\} = \{\ldots, -2\beta, -\beta, 0, \beta, 2\beta, \ldots\}$, i.e. all the numbers divisible

[1] The notation $[\cdot]$ is thus used for two different purposes, but which interpretation applies should be evident from the context.

by β. An example of a co-set is $3+[\beta] = \{\ldots, 3-2\beta, 3-\beta, 3, 3+\beta, 3+2\beta, \ldots\}$. The set $\{0, 1, \ldots, |\beta|-1\}$ is a complete residue system modulo $[\beta]$, thus $|\mathbb{Z}/[\beta]| = |\beta|$. □

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

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

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

with $\|P\| = e$. Now $\|P\| \equiv d_0 \equiv e \bmod [\beta]$ thus the element e is represented by the residue class $d_0 + [\beta]$ where $d_0 \in \Sigma$. Consequently Σ contains a complete residue system modulo $[\beta]$. □

The converse statement does not hold, e.g. the set $\Sigma = \{0, 1\}$ is not complete base $\beta = 2$ for the integers.

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 *A digit set Σ is* redundant *base β for the ring $\mathcal{R}$ iff*

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

and is non-redundant *base β iff*

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

Redundancy can complicate the determination of the sign or the range of a number, but redundancy can also be desirable, since by exploiting the redundancy, arithmetic operations can be performed more efficiently, e.g. performing addition and subtraction with limited carry propagation.

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

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

Proof: Since $|\Sigma| > |\mathcal{R}/[\beta]|$, there exists $d_1, d_2 \in \Sigma$ such that $d_1 \equiv d_2 \bmod [\beta]$ thus $\exists k \in \mathcal{R} : d_1 = d_2 + k\beta$. Since Σ is complete base β, there exists a polynomial $P \in \mathcal{P}_\mathcal{I}[\beta, \Sigma] : \|P\| = k$, by forming $P' = P[\beta] + d_2 \in \mathcal{P}_\mathcal{I}[\beta, \Sigma]$ with $\|P'\| = k\beta + d_2 = d_1$, we conclude that Σ is redundant base β.

□

The difference between two congruent digits is a multiple of the radix, if this multiple is in the digit-set or is representable then the digit-set is redundant. Thus redundancy can also occur in non-complete digit-sets. For instance if $\beta = 2$ and $\Sigma = \{0, 1, 2\}$ we have $0 \equiv 2 \bmod [2]$ 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 Σ is redundant. On the other hand Σ is not complete since no negative integer can be expressed.

Lemma 2.7 *If $|\Sigma| > |\mathcal{R}/[\beta]| = k_1$, 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 Σ is redundant base β.*

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. Σ is redundant base β. □

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

Proof: Consider the ring of integers $\mathcal{R} = \mathbb{Z}$. For $\beta \in \mathbb{Z}$ we have $|\mathbb{Z}/[\beta]| = |\beta| = k$. 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

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

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 $|\Sigma| > |\mathbb{Z}/[\beta]|$ implies that Σ is redundant base β. □

A similar result can be proven for the ring of Gaussian integers (see Lemma 4.17), in fact we have been unable to find rings where $|\Sigma| > |\mathbb{Z}/[\beta]|$ does not imply that Σ is redundant, thus it seems likely that the following conjecture holds.

Conjecture 2.9 *If $|\Sigma| > |\mathcal{R}/[\beta]|$, then Σ is redundant base β.*

Lemma 2.10 *If there exists no digits $d_1, d_2 \in \Sigma, d_1 \neq d_2$ belonging to the same residue class modulo $[\beta]$ (i.e. $|\Sigma| \leq |\mathcal{R}/[\beta]|$) then Σ is non-redundant base β for the ring $\mathcal{R}$.*

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

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

and consequently $p_k \equiv q_k \bmod [\beta]$, a contradiction. □

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 Σ, as $\eta = |\Sigma| - |\mathcal{R}/[\beta]|$.

From Lemma 2.4 we note that a negative redundancy index implies that Σ can not 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 non-redundant.

If $\mathcal{R}$ is an integral domain, $\mathcal{R}$ is said to be *ordered* iff $\mathcal{R}$ contains a non-empty 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 Σ is termed* semi-complete *base β for the ring $\mathcal{R}$, iff Σ is complete base β for the positive elements $\mathcal{R}^+$, in the sense that*

$$\forall r \in \mathcal{R}^+ : \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] :: \|P\| = r. \qquad (4)$$

If a digit-set is semi-complete for a ring $\mathcal{R}$, then by definition all the positive element 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 $N : \mathcal{R} \to \mathbb{R}$. 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. $N(a) = 0 - a = 0$.

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

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

If Σ 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 of Theorem 3.13.

Algorithm 3.12 *DGT-Algorithm*

Stimulus: *A base β, A digit set Σ, that is a complete residue system modulo β, 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*
  find $d_l \in \Sigma : d_l \equiv r_l \bmod [\beta]$
  $r_{l+1} \leftarrow (r_l - d_l)/\beta$
  $l \leftarrow l + 1$
  $OK \leftarrow (\forall j : 0 \leq j < l :: r_j \neq r_l)$
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 $1 \equiv 3 + 4i \bmod [\beta]$, thus $d_0 = 1$. Then $r_1 = \frac{r_0 - 1}{\beta}$, and the DGT-algorithm proceeds as indicated in the following table, and as depicted in Figure 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

Thus the radix polynomial $P = \Sigma_{j=0}^6 d_j[-1+i]^j = 1[-1+i]^6 + 1[-1+i]^5 + 1[-1+i]^4 + 1[-1+i]^3 + 1[-1+i]^2 + 1 \in \mathcal{P}_{\mathcal{I}}[-1 + i, \{0, 1\}]$ is a representation of $r = 3 + 4i$. □

Theorem 3.13 *Let $\mathcal{R}$ be a ring, and $N : \mathcal{R} \to \mathbb{R}$ a norm. Let Σ be a digit-set containing a complete residue system modulo $[\beta]$, then Σ is complete base β for the ring R iff*

$$\forall r \in \mathcal{R} : N(r) \leq \frac{d_{max}}{N(\beta) - 1} :: \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] : \|P\| = r \qquad (5)$$

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

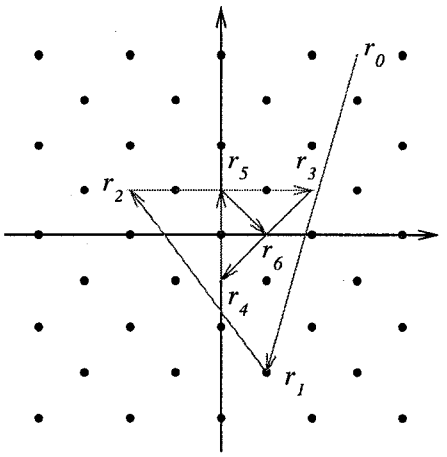

Figure 1. DGT-algorithm example: Conversion of $3+4i$ into a radix polynomial from $\mathcal{P}_{\mathcal{I}}[-1+i, \{0,1\}]$. The black dots represents the ideal $[-1+i]$.

Proof: If Σ is complete then by definition $\forall r \in \mathcal{R} : \exists P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] : ||P|| = r$, thus assume (5) holds. Choose any $r \in \mathcal{R}$, and in analogy with the DGT-algorithm choose a sequence of digits $d_0, d_1, d_2, \ldots$, from the remainders $r = r_0, r_1, r_2, \ldots$, such that $d_j \in \Sigma'$ and $d_j \equiv r_j \mod [\beta]$ (this is possible since Σ' contains a complete residue system modulo $[\beta]$). Form the subsequent remainders as:

$$r_{j+1} = \frac{r_j - d_j}{\beta}. \tag{6}$$

Notice that β divides $r_j - d_j$ since $d_j \equiv r_j \mod [\beta] \Rightarrow r_j - d_j \in [\beta] \Rightarrow \exists k \in \mathcal{R} : r_j - d_j = k\beta$.

From the properties of the norm N we deduce:

$$N(r_{j+1}) \leq \frac{N(r_j) + d_{max}}{N(\beta)} \tag{7}$$

thus

$$N(r_{j+1}) \begin{cases} < N(r_j) & , N(r_j) > \frac{d_{max}}{N(\beta)-1} \\ \leq \frac{d_{max}}{N(\beta)-1} & , N(r_j) \leq \frac{d_{max}}{N(\beta)-1} \end{cases} \tag{8}$$

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

$$N(r_j) \leq \frac{d_{max}}{N(\beta)-1}, \text{ for } j \geq k. \tag{9}$$

By assumption there exists a polynomial $P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$ with $||P|| = r_k$, and by recursion (6) we have

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

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

Theorem 3.13 together with the DGT-algorithm can be used to establish the completeness of a digit-set.

Corollary 3.14 *Let $\mathcal{R}$ be an ordered ring, with positive elements $\mathcal{R}^+$ and norm $N : \mathcal{R} \to \mathbb{R}$. Let Σ be a digit-set containing a complete residue system modulo $[\beta]$, then Σ is semi-complete iff*

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

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

Example: Let $\mathcal{R} = \mathbb{Z}, \beta > 1$ and $\Sigma = \{0, 1, \ldots, \beta - 1\}$. This digit set is not complete for the integers, since no negative number can be represented. On the other hand the integral domain $\mathbb{Z}$, is an ordered domain, thus using $\mathcal{R}^+ = \mathbb{Z}^+$ we conclude using Corollary (3.14) that Σ is semi-complete since

$$\left\{ r \mid r \in \mathbb{Z}^+ \wedge |r| \leq \frac{\beta - 1}{\beta - 1} = 1 \right\} = \{0, 1\} \subseteq \Sigma. \tag{10}$$

□

We will conclude this section with a study of the representation of the integers, that is the ring $\mathcal{R} = \mathbb{Z}$. Although this ring can be represented by a vast number of different digit sets, we will consider only *contiguous digit sets* of the form

$$\Sigma = \{r, r+1, \ldots, s-1, s\}, \text{ where } r \leq 0 \text{ and } s \geq 0$$

since it seems that there is no profound advantage gained by representing the integers by non contiguous digit sets.

Observation 3.15 *For the ring $\mathcal{R} = \mathbb{Z}$, the set $C = \{r, r+1, \ldots, s-1, s\}$ is a complete residue system modulo $[\beta]$, if the cardinality of C satisfies $|C| = s - r + 1 = |\beta| > 1$.*

Thus from Lemma 2.10 and Lemma 2.8 Σ is non-redundant base β if $|\Sigma| = s - r + 1 \leq |\beta|$ and redundant base β if $|\Sigma| = s - r + 1 > |\beta|$.

The absolute value is a norm on the integer ring. Employing this norm in connection with Theorem 3.13 it can be checked whether a digit-set is complete, e.g. it can be used in the proof of the following lemma.

Lemma 3.16 *The digit-set $\Sigma = \{r, r+1, \ldots s-1, s\}$ with $-|\beta| \leq r \leq 0 \leq s \leq |\beta|$ and $|\Sigma| = s - r + 1 \geq |\beta|$ is complete if*

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

and non-complete otherwise.

Digit-set	r, s	$\lvert\Sigma\rvert$	Redundant	Complete	η
Standard	$r = 0, s = \lvert\beta\rvert - 1$	$\lvert\beta\rvert$	false	$\beta < 0$	0
Extended	$r = 0, s = \beta > 0$	$\beta + 1$	true	false	1
Balanced	$r = -s$	$2s + 1 \geq \lvert\beta\rvert$	$2s + 1 > \lvert\beta\rvert$	true	≥ 0
Min. Red.	$-\lvert\beta\rvert \leq r \leq 0 \leq s \leq \lvert\beta\rvert$	$\lvert\beta\rvert + 1$	true	$(rs < 0 \wedge \beta > 0) \vee (\beta < 0)$	1
Max. Red.	$r = -\lvert\beta\rvert + 1, s = \lvert\beta\rvert - 1$	$2\lvert\beta\rvert - 1$	true	true	$\lvert\beta\rvert - 1$

Table 1. Classification of digit-sets.

Historically the digit-sets presented in Table 1 have proven to be useful [1, 10]. By applying Theorem 3.16 the depicted properties can be derived. As demonstrated not all of these digit sets are complete, but as is easily verified the digit sets are all semi-complete.

It is important to note that the set of numbers representable by extended polynomials over the integers is not isomorphic to the rationals, in fact $\mathcal{A}_\beta \subset \mathbb{Q}$, since not all rationals are representable. For instance $\frac{1}{3} \notin \mathcal{A}_2$. In general $1/p$ where p is prime in $\mathbb{Z}$ and not equal to β, can not be represented by a finite extended polynomial over the integers.

Example: Classical Number Representations.

1. Binary. $\beta = 2$ and $\Sigma = \{0, 1\}$. Standard digit set, non-redundant and semi-complete.
2. Nega-binary. $\beta = -2$ and $\Sigma = \{0, 1\}$. Standard digit set, non-redundant and complete.
3. Borrow-Save. $\beta = 2$ and $\Sigma = \{-1, 0, 1\}$. Minimally and maximally redundant digit set, complete.
4. Carry-Save. $\beta = 2$ and $\Sigma = \{0, 1, 2\}$. Extended and minimally redundant digit set, semi-complete.

□

4 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*.

4.1 Representing the Gaussian Integers

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

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}, \tag{12}$$

where $i = \sqrt{-1}$. It is a logical extension of the ring of integers, and as such the number systems for the two rings exhibits 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:

$$\mathbb{Z}[\sqrt{-d}] = \{a + \sqrt{-d}b \mid a, b \in \mathbb{Z}\}, \tag{13}$$

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 $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{R}$ defined as $N(a + \sqrt{-d}b) = \sqrt{a^2 + db^2}$ is a norm on $\mathbb{Z}[\sqrt{-d}]$, and that the set $C = \{r, r+1, \ldots, s\}$ 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 4.17 *For the ring $\mathcal{R} = \mathbb{Z}[\sqrt{-d}]$, $d \in \mathbb{Z}, d \geq 1$, if $|\Sigma| > \left|\mathbb{Z}[\sqrt{-d}]/[\beta]\right|$ then Σ is redundant base $\beta = \delta + \sqrt{-d}\gamma$.*

Proof: The number of distinct residue classes is given by $\left|\mathbb{Z}[\sqrt{-d}]/[\delta + \sqrt{-d}\gamma]\right| = \delta^2 + d\gamma^2 = k$, as can be derived from classsical results in algebraic number theory [11, pages 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:

$$\begin{aligned} \Phi_n &\leq \left(2\Delta \frac{N(\beta)^{n+1} - 1}{N(\beta) - 1} + 1\right)^2 \\ &\leq C \cdot (\delta^2 + d\gamma^2)^n + O(1) = C \cdot k^n + O(1). \end{aligned}$$

Thus by Lemma 2.7 the lemma is proven. □

4.2 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 Σ_r **and** Σ_i are complete digit sets base β for the integers, then $\Sigma = \Sigma_r + i\Sigma_i$ is complete base β for the Gaussian integers, furthermore if Σ_r **or** Σ_i is a redundant digit set base β for the integers, then Σ is redundant base β 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 $\Sigma = \{0,1\} + i\{0,1\}$. Non-redundant and non-complete.
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 non-complete but semi-complete.

□

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 [12]. Furthermore converting from a conventional representation to a complex representation and computing the complex conjugate are fairly simple tasks.

4.3 Imaginary Radix Number systems

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

Lemma 4.18 *The digit set* $\Sigma = \{r, r+1, \ldots, s\} \subset \mathbb{Z}$ *is complete base* $\beta = \sqrt{-d}$, $d \in \mathbb{Z}, d > 1$ *for the ring* $\mathbb{Z}[\sqrt{-d}]$ *iff* Σ *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

$$\mathcal{P}_{-1}[\beta, \Sigma] = \{P + p_{-1}[\beta]^{-1} \mid P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma] \wedge p_{-1} \in \Sigma\} \quad (14)$$

Definition 4.19 *A digit set* Σ *is* fraction-complete *base* β *for the ring* $\mathcal{R}$ *iff*

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

Lemma 4.20 *If* $\beta = \sqrt{-d}$, $d \in \mathbb{Z}, d > 1$ *and* $\Sigma = \{r, r+1, \ldots, s\}$, $-d \leq r \leq 0 \leq s \leq d$ *is complete base* β *for* $\mathbb{Z}[\sqrt{-d}]$ *then* Σ *is fraction-complete base* β *for the Gaussian integers iff* $\sqrt{d} \in \mathbb{Z}$ *(i.e.* d *is of the form* $d = k^2$ *for some* $k \in \mathbb{Z}, |k| > 1$*).*

Proof: Assume that $d = k^2$, $k \in N, k > 1$. Since Σ contains a complete residue system modulo k^2, there exists a set $\Sigma' = \{kp, k(p+1), \ldots, k(q-1), kq\}$, $-k \leq p \leq 0 \leq q \leq k$ such that $\Sigma' \subset \Sigma$ and the set $\Sigma'' = \{p, \ldots, q\}$ 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 Σ is complete base β for $\mathbb{Z}[\sqrt{-k^2}]$, for any $a + \sqrt{-k^2}b \in \mathbb{Z}[\sqrt{-k^2}]$ there exists a radix polynomial $P \in \mathcal{P}_{\mathcal{I}}[\beta, \Sigma]$ such that $||P|| = a + \sqrt{-k^2}b$.
Forming the polynomial $P' = P + d'[\beta]^{-1} \in \mathcal{P}_{-1}[\beta, \Sigma]$ with value $||P'|| = ||P|| + d'\frac{1}{\sqrt{-k^2}} = a + ki - \frac{d'}{k}i = a + iz$, we conclude that Σ 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. □

As in Section 3, we have classified a number of different digit sets (see Table 2). From Theorem 3.16, Lemmas 4.18 and 4.20 we derive the properties displayed in the Table.

Example: Imaginary Radix, Complex Number Representations.

1. Binary. $\beta = \sqrt{-2}$, $\Sigma = \{0,1\}$ and $\mathcal{R} = \mathbb{Z}[\sqrt{-2}]$. Standard digit set, non-redundant and complete.
2. Quarter-Imaginary. $\beta = \sqrt{-4} = 2i$ and $\Sigma = \{0,1,2,3\}$. Standard digit set, non-redundant, complete and fraction-complete (this number system was proposed by Knuth in [5]).
3. Borrow-Save (Quarter-Imaginary). $\beta = 2i$ and $\Sigma = \{-3, \ldots, 3\}$. Maximally redundant digit set, complete, fraction-complete (addition in Redundant number systems of this form has been examined in [3]).

□

4.4 Complex Radix Number Systems

As suggested in [9], we could use a fully complex base, e.g. $\beta = \gamma + i\delta$, $\gamma \neq 0$ and $\delta \neq 0$. We will only here

Digit-set	r, s	$\|\Sigma\|$	Redundant	η
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	$d - 1$

Table 2. Classification of digit-sets for $\mathbb{Z}[\sqrt{-d}]$.

examine number systems for which the digit set contains exclusively integer digits. Observe that the set $C = \{r, r + 1, \ldots, s\}$ 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 4.21 *The digit set* $\Sigma = \{r, \ldots, s\}$, $-A^2 \leq r \leq 0 \leq s \leq A^2$ *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.*

Proof: The proof is a slight generalization of the one given in [4]. □

Lemma 4.22 *The Symmetric digit set* $\Sigma = \{-s, \ldots, s\}$, $\lceil \frac{\gamma^2}{2} \rceil \leq s \leq \gamma^2$ *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 4.21 we have that Σ is complete base β, thus for any $a + ib \in \mathbb{Z}[i]$ there exists a radix polynomial $P = \Sigma_{j=0}^{n} d_j[-A - i]^j \in \mathcal{P}_{\mathcal{I}}[-A - i, \Sigma]$ 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 Σ is also complete base $\beta = A + i$.

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

The set of elements that can be represented using the standard digit set $\Sigma_{std} = \{0, 1, \ldots, A^2\}$ is a somewhat unsymmetric set, whereas the set of elements that can be represented using a symmetric redundant digit set has a higher degree of symmetry (see Figure 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 Non-redundant and complete.
2. Borrow-save. $\beta = \pm 1 \pm i$ and $\Sigma = \{-1, 0, 1\}$. Minimally and maximally redundant digit set, complete.

□

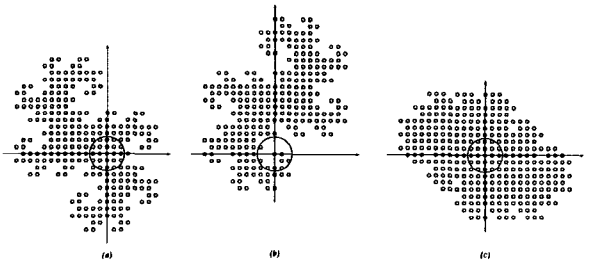

Figure 2. The Gaussian integers representable with radix polynomials of degree 7, using the number systems (a): $\beta = -1 + i$, $\Sigma = \{0, 1\}$, (b): $\beta = 1 + i$, $\Sigma = \{0, 1\}$, And in (c) the elements representable using polynomials of degree 5 and the redundant number system $\beta = 1 + i$, $\Sigma = \{-1, 0, 1\}$. The elements that lie within the circles all have norms less that $d_{max}/(N(\beta) - 1) = 1/(\sqrt{(2)} - 1)$, thus from Theorem 3.13 we immediately conclude that the number systems (a) and (c) are complete.

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

Lemma 5.23 *For the ring* $\mathbb{Z}[\rho]$, *if* $|\Sigma| > |\mathbb{Z}[\rho]/[\beta]|$ *then* Σ *is redundant base* $\beta \in \mathbb{Z}$, $|\beta| > 1$.

Proof: The proof is analogous to the one given for Lemma 4.17. □

From Lemma 5.23, we conclude that if a digit set has more than β^2 digits the digit set is redundant.

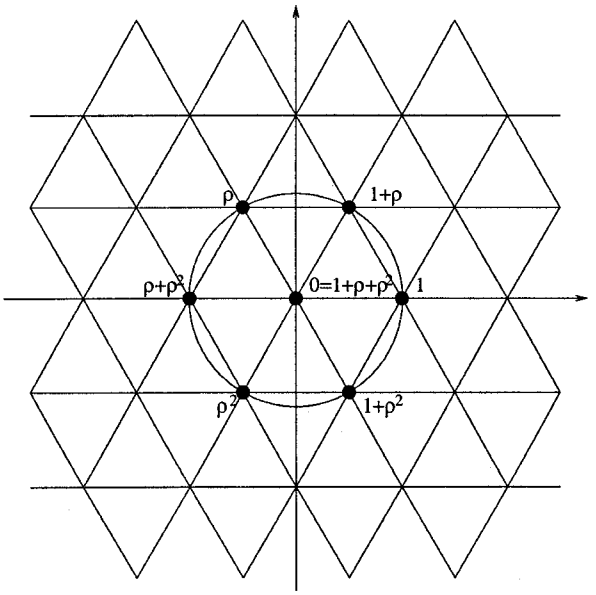

Figure 3. The ring $\mathbb{Z}[\rho]$ and the digit set $\Sigma = \{0,1\} + \{0,1\}\rho + \{0,1\}\rho^2$.

Theorem 5.24 *The digit set* $\Sigma = \{0,1,\ldots,|\beta|-1\} + \{0,1,\ldots,|\beta|-1\}\rho$ *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 $\Sigma_z = \{0,1,\ldots,|\beta|-1\}$ was complete base $\beta < -1$ for the integers. Thus there exists 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 $P' = P_0 + P_1\rho \in \mathcal{P}_I[\beta,\Sigma]$ with value $\|P'\| = a_0 + a_1\rho$ we conclude that Σ is complete. □

As shown in [2] it can be beneficial to represent the ring $\mathbb{Z}[\rho]$ using the redundant set $\mathcal{W} = \{a + b\rho + c\rho^2 \mid a,b,c \in \mathbb{N} \cup \{0\}\}$.

Theorem 5.25 *The digit set* $\Sigma = \{0,1,\ldots,\beta-1\} + \{0,1,\ldots,\beta-1\}\rho + \{0,1,\ldots,\beta-1\}\rho^2$ *is complete base* $\beta \in \mathbb{Z}$ *with* $\beta > 1$ *for the set* $\mathcal{W}$ *(as well as* $\mathbb{Z}[\rho]$*).*

Proof: Take any $a_0 + a_1\rho + a_2\rho^2 \in \mathcal{W}$. As demonstrated in Section 3, the digit set $\Sigma_z = \{0,1,\ldots,\beta-1\}$ is semi-complete base β for the integers, in the sense that

$$\forall a \in \mathbb{Z}^+ : \exists P \in \mathcal{P}_{\mathcal{I}}[\beta,\Sigma_z] :: \|P\| = a. \qquad (15)$$

In particular there exists polynomials $P_0, P_1, P_2 \in \mathcal{P}_{\mathcal{I}}[\beta,\Sigma_z]$ representing a_0, a_1 and a_2, thus forming the polynomial $P' = P_0 + P_1\rho + P_2\rho^2 \in \mathcal{P}_{\mathcal{I}}[\beta,\Sigma]$ with value $\|P'\| = a_0 + a_1\rho + a_2\rho^2$, we conclude that Σ is complete base β for $\mathcal{W}$. □

In particular the binary digit set $\Sigma = \{0,1\} + \{0,1\}\rho + \{0,1\}\rho^2$ is complete base $\beta = 2$. The digits of this number system are depicted in Figure 3. Note that apart from the number system being redundant, the digit set in it self contains redundancy, in the sense that there exists different digits that represent the same element of the ring, e.g. $1 + \rho + \rho^2 = 0$.

Since the $\beta - ary$ numbers written over $\mathbb{Z}[i]$ respectively $\mathcal{W}$ are not identical, conversion between elements from the two rings can not 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 does not exists 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 have been compiled in the form of Table 3.

The last two columns of the table deals 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:

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

Thus *eff* is the asymptotic value of 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.

In order to evaluate the relative merits of these number systems, we will now to turn our attention to arithmetic operations performed in these systems. If fast addition is needed the system should be redundant. As for storage, if digit serial arithmetic is an application, an encoding using few bits per digit will be desirable, since this will minimize module size and inter module wiring. 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 Σ is not closed under multiplication. But the systems $(\sqrt{-2}, \{-1,0,1\})$ and $(\pm 1 \pm i, \{-1,0,1\})$ seems very promising.

base	digit set	ring	compl.	redund.	closed	*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	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	$\frac{1}{2}$
$2i$	$\{0,1,2,3\}$	$\mathbb{Z}[i]$	true	false	false	2	1
$2i$	$\{-2,\ldots,2\}$	$\mathbb{Z}[i]$	true	true	false	3	$\frac{2}{3}$
$2i$	$\{-3,\ldots,3\}$	$\mathbb{Z}[i]$	true	true	false	3	$\frac{2}{3}$
$-1\pm i$	$\{0,1\}$	$\mathbb{Z}[i]$	true	false	true	1	1
$\pm1\pm i$	$\{-1,0,1\}$	$\mathbb{Z}[i]$	true	true	true	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	$\frac{2}{3}$

Table 3. Properties of low-radix systems for representing complex numbers

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 *the modified Booth recoding algorithm*, e.g. recoding from the non redundant 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.

References

[1] A. Avizienis. "Signed-Digit Number Representations for Fast Parallel Arithmetic". *IRE Transactions on Electronic Computers*, EC-10:389–400, September 1961.

[2] J. Duprat, Y. Herreros and S. Kla. "New Representation of Complex Numbers and Vectors". In *Proc. 10th IEEE Symposium on Computer Arithmetic*, 1991.

[3] A. Munk Nielsen and J-M. Muller: "Borrow-Save Adders for Real and Complex Number Systems"; *Proc. of 2nd Conf. on Real Numbers and Computers*, Marseille, France, April 1996.

[4] I. Katai and J. Szabo.: "Canonical Number Systems for Complex Integers"; *Acta Scientiarum Mathematicarum*, 1975, pp. 255–260.

[5] D. E. Knuth.: "An Imaginary Number System"; *CACM*, vol. 3, no. 4, Apr. 1960, pp. 245-247.

[6] P. Kornerup: "Digit-Set Conversions: Generalizations and Applications"; *IEEE Transactions on Computers*, vol. C-43, no. 6, May 1994, pp. 622–629.

[7] D. W. Matula.: "Radix Arithmetic: Digital Algorithms for Computer Architecture". In Raymond T. Yeh, editor, *Applied Computation Theory: Analysis, Design, Modeling*, chapter 9, pages 374–448. Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1976.

[8] D. W. Matula.: "Basic Digit Sets for Radix Representation"; *JACM*, vol. 29, no. 4, October 1982, pp. 1131–1143.

[9] W. Penney.: "A 'Binary' System for Complex Numbers" *JACM*, vol. 12, no2, Apr. 1965, pp. 247-248.

[10] B. Parhami.: "On the Implementation of Arithmetic Support Functions for generalized Signed Digit Number Systems". *IEEE Transactions on Computers*, C-42(3):379–384, march 1993.

[11] L.N. Steward and D.O.Toll *"Algebraic Number Theory "*. Chapman and Hall, London, 1979

[12] B. Wei, H. Du and H. Chen.: "A Complex-number Multiplier using Radix-4 Digits". In Proc. 12th Symposium on Computer Arithmetic, 1995, pp. 84-90.