Optimal Representations of Gaussian and Eisenstein Integers

A. Blažek, E. Pelantová, M. Svobodová

Department of Mathematics, Czech Technical University in Prague

Utrecht, Numeration 2024

Optimal Representations of Gaussian and Eisenstein Integers

A. Blažek, E. Pelantová, M. Svobodová

Department of Mathematics, Czech Technical University in Prague

Utrecht, Numeration $2024 = 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0$

Positional number system: base β and digit set $\mathcal{D}$

- Case 1: $\boldsymbol{\beta = \imath - 1}$, $\mathcal{D} = \{0, \pm 1, \pm \imath\}$
- Case 2: $\boldsymbol{\beta = \omega - 1}$, $\mathcal{D} = \{0, \pm 1, \pm \omega, \pm \omega^2\}$, $\boldsymbol{\omega = \exp \frac{2\pi\imath}{3}}$

Positional number system: base β and digit set $\mathcal{D}$

- Case 1: $\boldsymbol{\beta = \imath - 1}$, $\mathcal{D} = \{0, \pm 1, \pm \imath\}$
- Case 2: $\boldsymbol{\beta = \omega - 1}$, $\mathcal{D} = \{0, \pm 1, \pm \omega, \pm \omega^2\}$, $\boldsymbol{\omega = \exp \frac{2\pi \imath}{3}}$

Both these systems $(\beta, \mathcal{D})$ represent all complex numbers:

$$\left\{ \sum_{k<N} d_k \beta^k : N \in \mathbb{Z}, d_k \in \mathcal{D} \right\} = \mathbb{C}$$

$$\left\{ \sum_{k=0}^{N-1} d_k \beta^k : N \in \mathbb{N}, d_k \in \mathcal{D} \right\} = \begin{cases} \textbf{Gaussian integers } \mathbb{Z}[\imath] \text{ in Case 1} \\ \textbf{Eisenstein integers } \mathbb{Z}[\omega] \text{ in Case 2} \end{cases}$$

Positional number system: base β and digit set $\mathcal{D}$

- Case 1: $\boldsymbol{\beta = \imath - 1}$, $\mathcal{D} = \{0, \pm 1, \pm \imath\}$
- Case 2: $\boldsymbol{\beta = \omega - 1}$, $\mathcal{D} = \{0, \pm 1, \pm \omega, \pm \omega^2\}$, $\boldsymbol{\omega = \exp \frac{2\pi\imath}{3}}$

Both these systems $(\beta, \mathcal{D})$ represent all complex numbers:

$$\left\{ \sum_{k<N} d_k \beta^k : N \in \mathbb{Z}, d_k \in \mathcal{D} \right\} = \mathbb{C}$$

$$\left\{ \sum_{k=0}^{N-1} d_k \beta^k : N \in \mathbb{N}, d_k \in \mathcal{D} \right\} = \begin{cases} \textbf{Gaussian integers } \mathbb{Z}[\imath] \text{ in Case 1} \\ \textbf{Eisenstein integers } \mathbb{Z}[\omega] \text{ in Case 2} \end{cases}$$

The equalities are satisfied even with smaller alphabets $\mathcal{A} \subset \mathcal{D}$:

- $\mathcal{A} = \{0, 1\}$ for $\beta = \imath - 1$
- $\mathcal{A} = \{0, 1, -\omega\}$ for $\beta = \omega - 1$

but **bigger alphabets** $\mathcal{D}$ have benefits, while staying **closed under multiplication**, which simplifies multiplication of representations.

Why to use bigger alphabets than necessary

Parallel addition in $(\beta, \mathcal{D})$: constant time, *p*-local function

- minimal digit set size [Frougny, P., S. (2013)]
  - $\beta = \imath - 1$: no parallel addition if $\#\mathcal{D} < 5$
  - $\beta = \omega - 1$: no parallel addition if $\#\mathcal{D} < 7$
- Both system Case 1 and Case 2 do allow parallel addition [Legerský, S. (2019)]

Why to use bigger alphabets than necessary

Parallel addition in $(\beta, \mathcal{D})$: constant time, p-local function

- minimal digit set size [Frougny, P., S. (2013)]
  - $\beta = \imath - 1$: no parallel addition if $\#\mathcal{D} < 5$
  - $\beta = \omega - 1$: no parallel addition if $\#\mathcal{D} < 7$
- Both system Case 1 and Case 2 do allow parallel addition [Legerský, S. (2019)]

Non-adjacent form (NAF): small number of non-zero digits in $(\beta, \mathcal{D})$-representation $x = d_{n-1}d_{n-2}\cdots d_1 d_0$

- w-**NAF**: any block of length w of consecutive digits contains at most one non-zero digit
  - Case 1: any Gaussian integer has 3-NAF-representation
  - Case 2: any Eisenstein integer has 2-NAF-representation
- The w-**NAF**-representation of x is **unique**, and has the **minimal Hamming weight** among all representations of x, in both Cases 1 and 2 [Heuberger, Krenn (2011)]

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \overline{1}, \imath, \bar{\imath}\}$

Examples of NAF vs. general $(\beta, \mathcal{D})$-representations:

- $x = 1$: represented e.g. by strings 1, $\bar{\imath}\bar{\imath}$, $\bar{\imath}010\bar{\imath}0\overline{1}0\imath0\overline{1}0\bar{\imath}0\overline{1}$
- $x = 2 + \imath$: represented e.g. by strings $100\bar{\imath}$, $\imath0\imath$, $\bar{\imath}1$

A representation of x is called **optimal**, if no other representation of x has lower Hamming weight.

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \overline{1}, \imath, \bar{\imath}\}$

Examples of NAF vs. general $(\beta, \mathcal{D})$-representations:

- $x = 1$: represented e.g. by strings 1, $\overline{\imath\imath}$, $\bar{\imath}010\bar{\imath}0\overline{1}0\imath0\overline{1}0\bar{\imath}0\overline{1}$
- $x = 2 + \imath$: represented e.g. by strings $100\bar{\imath}$, $\imath0\imath$, $\bar{\imath}1$

A representation of x is called **optimal**, if no other representation of x has lower Hamming weight.

Our goal:

- find a formula to express

$$\boldsymbol{f(x)} = \textbf{ number of optimal representations of } x \in \mathbb{Z}[\beta]$$

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \bar{1}, \imath, \bar{\imath}\}$

Examples of NAF vs. general $(\beta, \mathcal{D})$-representations:

- $x = 1$: represented e.g. by strings 1, $\bar{\imath}\imath$, $\bar{\imath}010\bar{\imath}0\bar{1}0\imath0\bar{1}0\bar{\imath}0\bar{1}$
- $x = 2 + \imath$: represented e.g. by strings $100\bar{\imath}$, $\imath0\imath$, $\bar{\imath}1$

A representation of x is called **optimal**, if no other representation of x has lower Hamming weight.

Our goal:

- find a formula to express

$$\boldsymbol{f(x)} = \textbf{ number of optimal representations of } x \in \mathbb{Z}[\beta]$$

- for given $N \in \mathbb{N}$:
  - describe numbers $x \in \mathbb{Z}[\beta]$ having w-NAF-representation with Hamming weight $\leq N$ and with the **maximal value** $f(x)$

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \bar{1}, \imath, \bar{\imath}\}$

Examples of NAF vs. general $(\beta, \mathcal{D})$-representations:

- $x = 1$: represented e.g. by strings 1, $\overline{\imath\imath}$, $\bar{\imath}010\bar{\imath}0\bar{1}0\imath0\bar{1}0\bar{\imath}0\bar{1}$
- $x = 2 + \imath$: represented e.g. by strings $100\bar{\imath}$, $\imath0\imath$, $\bar{\imath}1$

A representation of x is called **optimal**, if no other representation of x has lower Hamming weight.

Our goal:

- find a formula to express

$$\boldsymbol{f(x)} = \textbf{ number of optimal representations of } x \in \mathbb{Z}[\beta]$$

- for given $N \in \mathbb{N}$:
  - describe numbers $x \in \mathbb{Z}[\beta]$ having w-NAF-representation with Hamming weight $\leq N$ and with the **maximal value** $f(x)$
  - determine the **average value of** $f(x)$ on the set

$$\boldsymbol{\mathcal{M}_N} = \{x \in \mathbb{Z}[\beta] : \text{length of } w\text{-NAF-representation of } x \text{ is } \leq N\}$$

Case 0: $\beta = 2$ and $\mathcal{D} = \{0, 1, \overline{1}\}$

System deeply explored, and questions already responded earlier:

Each $x \in \mathbb{Z}$ has **unique** 2-**NAF-representation** and its **Hamming weight** is **minimal** among all $(\beta, \mathcal{D})$-representations of x [Reitwiesner (1960)]

Case 0: $\beta = 2$ and $\mathcal{D} = \{0, 1, \bar{1}\}$

System deeply explored, and questions already responded earlier:

Each $x \in \mathbb{Z}$ has **unique** 2-**NAF-representation** and its **Hamming weight** is **minimal** among all $(\beta, \mathcal{D})$-representations of x [Reitwiesner (1960)]

Known results about **maximal and average values of** $f(x)$ [Grabner, Heuberger (2006)]:

- If 2-NAF-representation of $x \in \mathbb{Z}$ has at most N non-zero digits, then $\boldsymbol{f(x) \leq F_{N+1}}$, where $(F_N) =$ Fibonacci sequence.

Case 0: $\beta = 2$ and $\mathcal{D} = \{0, 1, \overline{1}\}$

System deeply explored, and questions already responded earlier:

Each $x \in \mathbb{Z}$ has **unique** 2-**NAF-representation** and its **Hamming weight** is **minimal** among all $(\beta, \mathcal{D})$-representations of x [Reitwiesner (1960)]

Known results about **maximal and average values of** $f(x)$ [Grabner, Heuberger (2006)]:

- If 2-NAF-representation of $x \in \mathbb{Z}$ has at most N non-zero digits, then $\boldsymbol{f(x) \leq F_{N+1}}$, where $(F_N) =$ Fibonacci sequence.
- Let $\lambda \in (2, 3)$ be a root of $t^3 - t^2 - 3t + 1$. There exists a constant $d > 0$ such that the average value of $f(x)$ equals

$$\frac{1}{\#\mathcal{M}_N} \sum_{x \in \mathcal{M}_N} f(x) = d\left(\frac{\lambda}{2}\right)^N (1 + o(1)),$$

with $\frac{\lambda}{2} \sim 1{,}08504$.

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \bar{1}, \imath, \bar{\imath}\}$

Step 1: **Transducer** on 21 vertices

- acts on input length = output length of **1 or 3 digits**
- transforms **general** $\mapsto$ 3-**NAF** representation of x in $(\beta, \mathcal{D})$
- outputs on edges: $\boxed{0}$, $\boxed{001}$, $\boxed{00\bar{1}}$, $\boxed{00\imath}$, $\boxed{00\bar{\imath}}$

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \bar{1}, \imath, \bar{\imath}\}$

Step 1: **Transducer** on 21 vertices

- acts on input length = output length of **1 or 3 digits**
- transforms **general** $\mapsto$ 3-**NAF** representation of x in $(\beta, \mathcal{D})$
- outputs on edges: $\boxed{0}$, $\boxed{001}$, $\boxed{00\bar{1}}$, $\boxed{00\imath}$, $\boxed{00\bar{\imath}}$

Step 2: Limiting the transducer only to **optimal** representations gives **graph** G **on 9 vertices**

$\rightarrow$ each oriented path in G **starting and ending in** 0 and respecting **colours of the** 3-**NAF representation** of x provides **optimal** representation of x

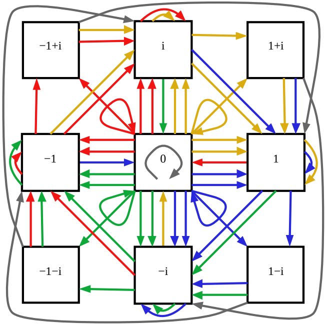
1-1 correspondence

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \bar{1}, \imath, \bar{\imath}\}$

Step 1: **Transducer** on 21 vertices

- acts on input length = output length of **1 or 3 digits**
- transforms **general** $\mapsto$ 3-**NAF** representation of x in $(\beta, \mathcal{D})$
- outputs on edges: $\boxed{0}$, $\boxed{001}$, $\boxed{00\bar{1}}$, $\boxed{00\imath}$, $\boxed{00\bar{\imath}}$

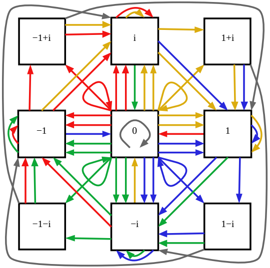
Step 2: Limiting the transducer only to **optimal** representations gives **graph** G **on 9 vertices**



$\rightarrow$ each oriented path in G **starting and ending in** 0 and respecting **colours of the** 3-**NAF representation** of x provides **optimal** representation of x

1-1 correspondence

Case 1: Example - optimal paths in G for $x = 2 + \imath$



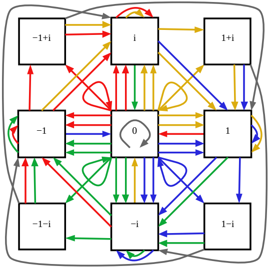
$x = 2 + \imath =$ | 001 | $00\bar{\imath}$ |

has 3 optimal $(\beta, \mathcal{D})$-representations:

- $2 + \imath = 100\bar{\imath}$
- $2 + \imath = \imath 0 \imath$
- $2 + \imath = \bar{\imath}1$

$\rightarrow$ 3 paths in G from 0 to 0 coloured with (red)(yellow)

Case 1: Example - optimal paths in G for $x = 2 + \imath$

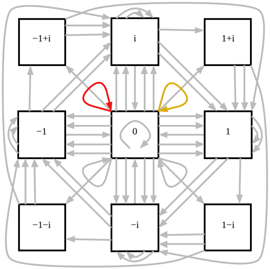


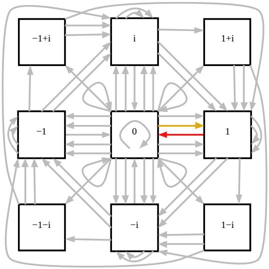
$x = 2 + \imath = \boxed{\color{red}{001}} \boxed{\color{orange}{00\bar{\imath}}}$

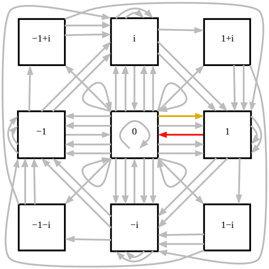
has 3 optimal $(\beta, \mathcal{D})$-representations:

- $2 + \imath = 100\bar{\imath}$
- $2 + \imath = \imath 0 \imath$
- $2 + \imath = \bar{\imath}1$

$\rightarrow$ 3 paths in G from 0 to 0 coloured with (red)(yellow)







Case 1: Number of paths in graph G

Step 3: **Incidence matrix $\boldsymbol{A_c} \in \mathbb{N}^{9\times 9}$** for each **colour in graph** G:

$$c \in \mathcal{C} := \{\boxed{0}, \boxed{001}, \boxed{00\bar{1}}, \boxed{00\imath}, \boxed{00\bar{\imath}}\} \quad \mapsto \quad A_c$$

$$A_{\boxed{001}} = \left(\begin{array}{c|cccc|cccc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right)$$

$(A_c)_{q',q}$ = **number of edges** from q to q' in G **with colour** c

Case 1: Number of paths in graph G

Step 3: **Incidence matrix $\boldsymbol{A_c} \in \mathbb{N}^{9\times 9}$** for each **colour in graph** G:

$$c \in \mathcal{C} := \{\boxed{0}, \boxed{001}, \boxed{00\bar{1}}, \boxed{00\imath}, \boxed{00\bar{\imath}}\} \quad \mapsto \quad A_c$$

$$A_{\boxed{001}} = \left(\begin{array}{c|cccc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$(A_c)_{q',q}$ = **number of edges** from q to q' in G **with colour** c

If $u_1 u_2 u_3 \cdots u_n \in \mathcal{C}^*$ is the 3-**NAF** representation of $x \in \mathbb{Z}[\imath]$, then the number of **optimal** representations of x is

$$\boldsymbol{f(x) = eA_{u_1}A_{u_2}\cdots A_{u_n}e^\top}, \quad \text{where } e = (1, 0, 0, \ldots, 0) \in \mathbb{Z}^9$$

Function $\boldsymbol{f} : \mathcal{C}^* \mapsto \mathbb{N}$ is a **recognizable series**, in terminology of [Berstel, Reutenauer (2013)]

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \overline{1}, \imath, \bar{\imath}\}$

Step 4: Finding the **maximal number** of **optimal** representations:

$\max\{eA_{u_1}A_{u_2}\cdots A_{u_n}e^\top$: Hamming weight of $u_1u_2\cdots u_n$ is $\leq N\}$

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \overline{1}, \imath, \bar{\imath}\}$

Step 4: Finding the **maximal number** of **optimal** representations:

$$\max\{eA_{u_1}A_{u_2}\cdots A_{u_n}e^\top : \text{Hamming weight of } u_1u_2\cdots u_n \text{ is } \leq N\}$$

Theorem

Let $(s_N)_{N\geq 0}$ *be the sequence with* $s_0 = 1$, $s_1 = \frac{3}{2}$, $s_2 = 3$, *and*

$$s_{N+3} = s_{N+2} + 2s_{N+1} + 2s_N \quad \text{for every } N \in \mathbb{N}\,.$$

- *If the 3-NAF representation of* x *contains at most* N *non-zero digits,* $N \geq 2$*, then the* **number of optimal representations** $\boldsymbol{f(x) \leq s_N}$.
- *There exist only 8 Gaussian integers* $x \in \mathbb{Z}[\imath]$, $x \notin \beta\mathbb{Z}[\imath]$ *whose 3-NAF representation contains* N *non-zero digits,* $N \geq 2$*, and which have* s_N *optimal representations.*

Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, 1, \overline{1}, \imath, \bar{\imath}\}$

$\mathcal{M}_N = \{x \in \mathbb{Z}[\imath]$: length of 3-NAF representation of x is $\leq N\}$.

Theorem

Let $\lambda \in (2, 3)$ be a root of $t^7 - t^6 - 8t^4 + 3t^3 + t^2 - 2t + 2$. Then the average number of optimal representations of Gaussian integers in $\mathcal{M}_N$ equals

$$\frac{1}{\#\mathcal{M}(N)} \sum_{x \in \mathcal{M}(N)} f(x) = \left(\tfrac{\lambda}{2}\right)^N (d + o(1)),$$

with $\frac{\lambda}{2} \sim 1{,}13674$ and $d \sim 0{,}76257$.

Case 2: $\beta = \omega - 1$ and $\mathcal{D} = \{0, \pm 1, \pm\omega, \pm\omega^2\}$

2-NAF representations of **Eisenstein integers** $\mathbb{Z}[\omega]$, $\omega = \exp\frac{2\pi\imath}{3}$

- 2-NAF using 7 digit blocks from set $\left\{\boxed{0}, \boxed{01}, \boxed{0\omega}, \boxed{0\omega^2}, \boxed{0\bar{1}}, \boxed{0\overline{\omega}}, \boxed{0\overline{\omega^2}}\right\}$ represented by **7 colours in graph** G
- **incidence matrix** $A_c \in \mathbb{N}^{7\times 7}$ for each colour in G

Case 2: $\beta = \omega - 1$ and $\mathcal{D} = \{0, \pm 1, \pm\omega, \pm\omega^2\}$

2-NAF representations of **Eisenstein integers** $\mathbb{Z}[\omega]$, $\omega = \exp\frac{2\pi\imath}{3}$

- 2-NAF using 7 digit blocks from set $\{\boxed{0}, \boxed{01}, \boxed{0\omega}, \boxed{0\omega^2}, \boxed{0\overline{1}}, \boxed{0\overline{\omega}}, \boxed{0\overline{\omega^2}}\}$ represented by **7 colours in graph** G
- **incidence matrix** $A_c \in \mathbb{N}^{7\times 7}$ for each colour in G

Theorem

Let $s_N = \lfloor \frac{1}{7}(6 \cdot 2^N + 1) \rfloor$, $N \in \mathbb{N}$ *be the sequence given by*
$$s_0 = 1,\ s_1 = 1,\ s_2 = 3, \text{ and } s_{N+3} = s_{N+2} + s_{N+1} + 2s_N + 1\ .$$

- *2-NAF representation of* x *with at most* N *non-zero digits has the* **number of optimal representations** $\boldsymbol{f(x) \le s_N}$.
- *For* $N \ge 4$, *there are only 12 Eisenstein integers* $x \in \mathbb{Z}[\omega]$, $x \notin \beta\mathbb{Z}[\omega]$ *with 2-NAF representation containing* N *non-zero digits, and having* s_N *optimal representations.*

Case 2: $\beta = \omega - 1$ and $\mathcal{D} = \{0, \pm 1, \pm\omega, \pm\omega^2\}$

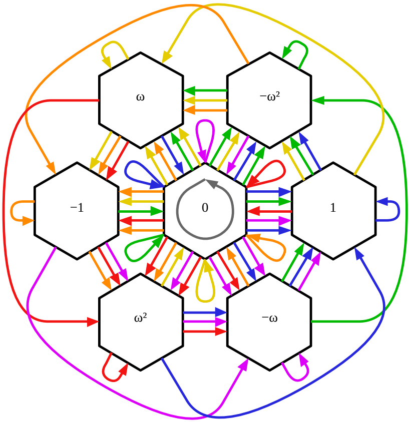
$$\mathcal{M}_N = \{x \in \mathbb{Z}[\omega] : \text{length of 2-NAF representation of } x \text{ is} \leq N\}.$$

Theorem

Let λ be the bigger root of $t^2 - 3t - 2$. Then the average number of optimal representations of Eisenstein integers in $\mathcal{M}_N$ equals

$$\frac{1}{\#\mathcal{M}(N)} \sum_{x \in \mathcal{M}(N)} f(x) \; = \left(\tfrac{\lambda}{3}\right)^N (d + o(1))\,,$$

with $\frac{\lambda}{3} \sim 1{,}18672$ *and* $d \sim 0{,}78144$.



Thanks for your attention