On Cobham's theorem for Gaussian integers

Wieb Bosma[*], Robbert Fokkink, and Thijmen Krebs [†]

June 2014

Abstract

The extension of Cobham's theorem from $\mathbb{Z}$ to $\mathbb{Z}[i]$ has been studied before for special bases. It is well known that this extension involves issues from diophantine approximation. In this paper, we consider the extension of Cobham's theorem for general bases.

According to Cobham's theorem $X \subset \mathbb{N}$ is α-automatic and β-automatic for multiplicatively independent α and β if and only if X is ultimately periodic. Does there exist a similar theorem for the Gaussian integers? To address this question, we restate the theorem in a different, but equivalent, form.

Theorem 1 (A variation on Cobham's theorem)**.** *Suppose that $X \subset \mathbb{N}$ and let $V(X) \subset \mathbb{N}$ be the subset of all natural numbers $\alpha > 1$ such that X is α-automatic. Then $V(X)$ is either equal to $\{\beta^n : n \in \mathbb{N}\}$ for some β or it is equal to all natural numbers $\alpha > 1$.*

The corresponding statement also holds for $\mathbb{Z}$, although the result does become more involved: for $\mathbb{N}$ the canonical numeration system with base α has digits $\{0, 1, \ldots, \alpha - 1\}$ but if we include negative integers, we may also consider negative digits. For instance, $(\{-1, 0, 1\}, 3)$ is a numeration system (with respect to base 3) for $\mathbb{Z}$. One first has to settle that the notion of automaticity does not depend on the digit system; the same problem arises if one wants to extend the theorem to $\mathbb{Z}[i]$.

Remark 1. Already a formulation of the Theorem of Cobham for $\mathbb{N}$ that is amenable to generalization (to rings like $\mathbb{Z}$ and $\mathbb{Z}[i]$) is problematic; one such formulation (given by Cobham himself, cf. [4]) is that a subset of $\mathbb{N}$ is m- and n-automatic for multiplicatively independent natural numbers m and n if and only if it is ultimately periodic. Here an ultimately periodic subset of $\mathbb{N}$ is defined by Cobham as, 'with finitely many exceptions, the union of a system of residue classes modulo some fixed positive integer'. The corresponding statement with $\mathbb{N}$ replaced by $\mathbb{Z}$ everywhere is not true (even leaving aside the digit dependence), since any $\mathbb{N}$-ultimately periodic set of positive integers will not be $\mathbb{Z}$-ultimately periodic anymore. The same problem prevents an obvious generalization to $\mathbb{Z}[i]$ using residue classes modulo $\alpha \in \mathbb{Z}[i]$.

An alternative, used by Allouche and Shallit, as well as by Rigo and Waxweiler, is to define ultimately periodic for a subset of $\mathbb{N}$ as being, with finitely many exceptions, a finite union of arithmetic progressions $x + p \cdot y$, with fixed $x, y \in \mathbb{N}$, and p ranging over $\mathbb{N}$. For the generalization to $\mathbb{Z}$ one then replaces $\mathbb{N}$ by $\mathbb{Z}$ everywhere, except for the range of p. It is then proved in [2] that a subset X of $\mathbb{Z}$ is n-automatic (in $\mathbb{Z}$) if and only if both $X \cap \mathbb{N}$ and $-X \cap \mathbb{N}$ are n-automatic in $\mathbb{N}$.

We conjecture that the following version of Cobham's theorem holds for $\mathbb{Z}[i]$.

[*]Radboud Universiteit Nijmegen
[†]Technische Universiteit Delft

Conjecture 1. *Suppose that $X \subset \mathbb{Z}[i]$ and let $V(X) \subset \mathbb{Z}[i]$ be the set of Gaussian integers α with $|\alpha| > 1$ such that X is α-automatic. Then $V(X)$ is equal to either*

1. *the set of all Gaussian integers $|\alpha| > 1$; or*
2. *the set of Gaussian integers $|\alpha| > 1$ for which some power $\alpha^j \in \mathbb{N}$; or*
3. *the set $\{\beta^n : n \in \mathbb{N}\}$ for some Gaussian integer β with $|\beta| > 1$.*

Allouche et al [1] have developed the notion of automatic sequences for rings such as $\mathbb{Z}[i]$. They have shown that the concept of automatic set is inpendent of the choice of the digits. In [1], p. 325 and [2], p. 415 it is proved that $(\{0,1\}, -1+i)$-automaticity is equivalent to $(\{0,1\},2)$-automaticity on the four $\mathbb{N} \times \mathbb{N}$-quadrants in $\mathbb{Z}[i]$. Hansel and Safer [7] studied the extension of Cobham's theorem to $\mathbb{Z}[i]$ for basis $-n+i$, which allows the digit set $\{0, 1, \ldots, n^2-1\}$. Our paper appears to be the first that deals with an arbitrary basis.

The separate cases of our conjecture all occur:

1. Any finite set X will be α-automatic for any α.
2. The set $X = \{\beta^n : n \in \mathbb{N}\}$ is α-automatic if and only if α and β are multiplicatively dependent. This follows from Theorem 3 below.
3. $\mathbb{N} \subset \mathbb{Z}[i]$ is α-automatic if and only if $\alpha^j \in \mathbb{N}$ for some $j \in \mathbb{N}$. This is Theorem 4 below.

The proof of the difficult direction of Cobham's theorem for $\mathbb{N}$ (see [9] and [6] for a discussion) makes use of the syndeticity of automatic sets (gaps between elements are bounded) and depends on the fact that the multiplicative group

$$G_{\alpha,\beta} = \{\alpha^n \beta^m : n, m \in \mathbb{Z}\}$$

is dense in $\mathbb{R}_{>0}$, for independent α, β. It is natural to expect that the closure of such groups is important in the case of the Gaussian integers as well.

Indeed, the results in our paper are based on the observation that $G_{\alpha,\beta}$ is dense in itself if α and β are multiplicatively independent. To derive stronger results, deeper observations are needed. To prove that $G_{\alpha,\beta}$ is dense in $\mathbb{C}$ is equivalent to proving the $\mathbb{Q}$-linear independence of 1, $z = \frac{\log|\alpha|}{\log|\beta|}$, and $z\frac{\arg\alpha}{2\pi} - \frac{\arg\beta}{2\pi}$, see [7]. This would follow if the four exponentials conjecture holds. Hansel and Safer have used this to show that if X is syndetic if $G_{\alpha,\beta}$ if it is α and β automatic, for special bases, assuming that the four exponentials conjecture is true.

Numeration systems for $\mathbb{Z}[i]$ have been developed by Davio et al [5], but this work is not widely available. So we review these numeration systems first before deriving our results.

1 Numeration systems in $\mathbb{Z}[i]$

Let $\beta \in R$ in a semi-ring R and let D be a set of representatives for the residue classes modulo β. We say that (β, D) is a numeration system if $0 \in D$ and every element of $r \in R$ has a unique representation

$$r = b_j \beta^j + b_{j-1}\beta^{j-1} \cdots + b_0$$

with every $b_i \in D$ and $b_j \neq 0$. The digits can be computed recursively by setting $b_0 \equiv r \mod \beta$ and continuing with $r' = (r - b_0)/\beta$ until zero. This procedure may not terminate and the digit set D has to be selected carefully.

We are interested in the ring of Gaussian integers, which is a normed ring (under the usual complex absolute value). Let $s \in R \setminus D$ be an element of minimal norm. We say that D is a *compact digit set* if $|d| < |s||\beta - 1|$ for all $d \in D$. For example, the digit set $D = \{-1, 0, \ldots, |k|-2\}$ forms a compact digit set for base $k \in \mathbb{Z}$ if $|k| > 2$.

Lemma 1. *Consider a normed ring R such that $\{|r| \colon r \in R\}$ is discrete. If D is a compact digit set, then (β, D) is a numeration system.*

Proof. We prove that the recursive procedure terminates. It certainly does if $r \in D$ so we assume that $r \in R \setminus D$. Then

$$|r'| = \frac{|r - b_0|}{|\beta|} \leq \frac{|r| + |b_0|}{|\beta|} < \frac{|r| + |r|(1 - |\beta|)}{|\beta|} = |r| \tag{1}$$

so the norm reduces under the recursive operation. On the discrete set of norms, this recursive operation must terminate. □

If $r = b_j\beta^j + b_{j-1}\beta^{j-1} \cdots + b_0$ then it is customary to represent r as a string $b_j b_{j-1} \cdots b_0$. We write $\ell(r) = j$ for the length of the string, starting the count at zero.

Lemma 2. *Let D be a compact digit set on the normed ring R. There exists $\gamma > 0$ such that $\ell(r) \leq n$ if $|r| \leq \gamma|\beta|^n$, for $r \in R$.*

Proof. Define $\Delta = \max\{|d| \colon d \in D\}$, and let

$$\gamma = |s| - \frac{\Delta}{|\beta| - 1}.$$

By compactness of the digit set, $\gamma > 0$. We prove by induction that $|r| < \gamma|\beta|^n + \frac{\Delta}{|\beta|-1}$ implies $\ell(r) \leq n$. If $n = 0$ then $|r| < |s|$ so necessarily $r \in D$ and $\ell(r) = 0$. Using (1) we find

$$|r'| \leq \frac{|r| + \Delta}{|\beta|} < \gamma|\beta|^{n-1} + \frac{\Delta}{|\beta|(|\beta| - 1)} + \frac{\Delta}{|\beta|} = \gamma|\beta|^{n-1} + \frac{\Delta}{|\beta| - 1}.$$

By the induction hypothesis $\ell(r') \leq n - 1$ and the result follows. □

Theorem 2. *If $\beta \in \mathbb{Z}[i]$ satisfies $|\beta| > \sqrt{8}$ then there exists a compact digit set D such that (β, D) is a numeration system for the Gaussian integers.*

Proof. We need to show that $B = \{z \colon |z| < |s|\,(|\beta| - 1)\}$ contains a representative for each residue class modulo β. Since $|\beta| > \sqrt{8}$, all elements $a + bi$ with $|a| \leq 1$ and $|b| \leq 1$ represent different residue classes modulo β, so we may include them in our digit set, and then $|s| \geq 2$. In this case, $\text{area}(B) \geq 4\pi\,(|\beta| - 1)^2$. By Minkowski's theorem, $z + B$ intersects the lattice $\beta\mathbb{Z}[i]$ if $\text{area}(B) > 4|\beta|^2$, so we need to verify that

$$\pi > \frac{|\beta|^2}{(|\beta| - 1)^2}$$

The right-hand side of the inequality decreases with $|\beta|$, so it suffices to verify that $\pi > 8/(\sqrt{8} - 1)^2$. □

2 Proof of the main theorems

Lemma 3. *Let $\alpha, \beta \in \mathbb{Z}[i]$ be of modulus $|\alpha|, |\beta| > 1$. Then 1 is an accumulation point of $\{\alpha^m \beta^n : m, n \in \mathbb{Z}\}$ unless α, β are multiplicatively dependent.*

Proof. The multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is locally compact and $A = \{\alpha^n : n \in \mathbb{Z}\} \subset \mathbb{C}^*$ is a discrete subgroup. The quotient group $\mathbb{C}^*/A$ is homeomorphic to a torus. Let C be the closure in $\mathbb{C}^*$ of the multiplicative group $\{\alpha^m \beta^n : m, n \in \mathbb{Z}\}$. Then C/A is a closed subgroup of a torus. So it is either finite, or it consists of a finite number of circles, or it is the entire torus. In the first case, α and β are multiplicatively dependent. In the second case, 1 is an accumulation point of $\{\alpha^m \beta^n : m, n \in \mathbb{Z}\}$. □

If 1 is an accumulation point, then there exists a sequence $\alpha^n \beta^m \to 1$. Since $|\alpha|, |\beta| > 1$ the sign of n and m is opposite. So there exist $i, j \in \mathbb{N}$ such that $\frac{\alpha^i}{\beta^j} \to 1$.

Lemma 4. *Let (β, D) be a numeration system for $\mathbb{Z}[i]$. Then for every $u \in \{\alpha^m \beta^n : m, n \in \mathbb{Z}\}$ there exist arbitrarily large $p, q \in \mathbb{N}$ such that $\alpha^p = u\beta^q + z$ for some $z \in \mathbb{Z}[i]$ with $\ell(z) \leq q$.*

Proof. If α and β are multiplicatively dependent, then we may even take $z = 0$. So assume that they are independent; let $u = \alpha^n \beta^m$ with $n, m \in \mathbb{Z}$. Since 1 is an accumulation point there exists a sequence of pairs $i, j \in \mathbb{N}$ such that $|\frac{\alpha^i}{\beta^j} - 1| \to 0$. Therefore $\frac{\alpha^i}{\beta^j} u = \frac{\alpha^{i+n}}{\beta^{j-m}}$ converges to u and we find a sequence of pairs $p, q \in \mathbb{N}$ such that $\frac{\alpha^p}{\beta^q} \to u$. Then $|\alpha^p - \beta^q u| < \gamma |\beta^q|$ for large enough p, q with γ as in Lemma 2. Now put $z = \alpha^p - \beta^q u$. □

Before Cobham proved his theorem, Büchi [3] showed that the set $\{\alpha^n : n \in \mathbb{N}\}$ is β-automatic if and only if α and β are multiplicatively dependent for $\alpha, \beta \in \mathbb{N}$. Our next theorem extends Büchi's result to $\mathbb{Z}[i]$.

Theorem 3. *The set $\{\alpha^n : n \in \mathbb{N}\}$ is not β-automatic if $\alpha, \beta \in \mathbb{Z}[i]$ are multiplicatively independent.*

Proof. We may assume without loss of generality that $|\beta| > \sqrt{8}$ so that there exists a numeration system (β, D) with compact digit set D which includes digit 1. Arguing by contradiction, suppose that $A = (Q, q_0, D, \delta, F)$ is a DFA that generates the characteristic function f of the set $\{\alpha^n : n \in \mathbb{N}\}$. The power $\beta^{|Q|}$ is represented by $10^{|Q|}$ in the numeration system. Since there are $|Q|$ states, there exist a $0 \leq j < k \leq |Q|$ such that 10^j and 10^k reach the same final state in the DFA. So we can pump $k - j$ additional zeroes in $10^{|Q|}$ and still reach the same final state. Our DFA accepts powers of α. So if α^q is represented by $10^{|Q|}v$ in our β-numeration system, then we can pump $k - j$ additional zeroes into the prefix and obtain another power of α. We will derive a contradiction from this.

By the previous lemma, there are infinitely many powers of α that have prefix $10^{|Q|}1$ in our β-numeration system. So two of these representations have the same length modulo $k - j$, and we can pump zeroes into the prefix of the shorter representation so that we get two words of equal length. One of these has prefix $10^{|Q|}1$ and the other has prefix $10^{|Q|}0$ so they represent two different powers $\alpha^{q_1}, \alpha^{q_2}$. Since they both have prefix $10^{|Q|}$, their difference is equal to

$$\alpha^{q_1} - \alpha^{q_2} = \sum_{i=0}^{m} (d_i - d_i')\beta^i$$

for digits $d_i, d_i' \in D$ and m smaller than the minimum of $\ell(\alpha^{q_1}), \ell(\alpha^{q_2})$. Denote this difference by $z \neq 0$. By pumping additional zeroes into both prefixes, we obtain pairs of higher powers of α that all have the same difference z. In other words, $\alpha^n - \alpha^m = z$ has infinitely many solutions for $z \neq 0$. Clearly, this is impossible. We conclude that $\{\alpha^n : n \in \mathbb{N}\}$ is not β-automatic. □

Theorem 4. *$\mathbb{N} \subset \mathbb{Z}[i]$ is β-automatic if and only if $\beta^j \in \mathbb{N}$ for some $j \in \mathbb{N}$.*

Proof. If $\beta^j \in \mathbb{N}$ then clearly $\mathbb{N}$ is β-automatic. So assume $\beta^j \notin \mathbb{N}$ for every $j \in \mathbb{N}$. Suppose that $A = (Q, q_0, D, \delta, F)$ is a DFA that generates the characteristic function f of $\mathbb{N}$. Choose any natural number $\alpha > 1$. Then α and β are multiplicatively independent and all powers of α are accepted by our DFA. There exists a power of α that is represented by a word with prefix $10^{|Q|}$ in the β-numeration system. There exists an integer $k < |Q||$ such that we can pump an arbitrary multiple of k zeroes into the prefix so that and the resulting word also gets accepted by the DFA. In other words, these all represent numbers in $\mathbb{N}$: $\beta^{m+jk} - \beta^m \in \mathbb{N}$ for some power m. It follows that both $\beta^{m+k} - \beta m$ and $\beta^{m+2k} - \beta m + k$ are natural numbers. Taking quotients, we find $\beta^k \in \mathbb{Q}$ and since it is an algebraic integer, $\beta^k \in \mathbb{N}$. □

References

[1] J.P. Allouche, E. Cateland, W.J. Gilbert, H.O. Peitgen, J.O. Shallit, G. Skordev, *Automatic maps in exotic numeration systems*, Theory Comput. Syst. **30** (1997), 258–331.

[2] J.P. Allouche, J.O. Shallit, *Automatic sequences*, Cambridge University press, 2003.

[3] J.R. Büchi, *Weak second-order arithmetic and finite automata*, Z. Math. Logik Grundlagen Math. 6 (1960), 66–92.

[4] A. Cobham, *On the base-dependence of sets of numbers recognizable by finite automata*, Math. Systems Theory, **3** (1969), 186–192.

[5] M. Davio, J.P. Deschamps, and C. Gossart,*Complex arithmetic*, Technical Report R369, MBLE Research Laboratory, Brussels, Belgium, May 1978.

[6] Fabien Durand, Michel Rigo, *On Cobham's theorem*, preprint chapter Handbook Automata.

[7] G. Hansel, T. Safer, *Vers un thèorème de Cobham pour les entiers de Gauss*, Bull. Belg. Math. Soc. Simon Stevin **10**, vol. 5 (2003), 723–735.

[8] T. Krebs, *Automatic maps on the Gaussian integers*, MSc thesis, TU Delft, 2013.

[9] M. Rigo, L. Waxweiler, *A note on syndeticity, recognizable sets and Cobham's theorem*, Bull. European Assoc. Theor. Comput. Sci. **88** (2006), 169–173.