Journal of Symbolic Computation 77 (2016) 175–188

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Shortest division chains in unique factorization domains

Maksim Vaskouski [a], Nikita Kondratyonok [b]

[a] Department of Higher Mathematics, Belarusian State University, Minsk 220030, Belarus
[b] Faculty of Applied Mathematics and Computer Science, Belarusian State University, Minsk 220030, Belarus

ARTICLE INFO

Article history:
Received 6 October 2015
Accepted 30 January 2016
Available online 5 February 2016

Keywords:
Euclidean algorithm
Unique factorization domain
Euclidean domain
Continued fraction

ABSTRACT

We investigate the problem on the validity of the Lazard theorem analogue (or the Kronecker–Vahlen theorem), which states that the least remainder Euclidean Algorithm (EA) has the shortest length over any other versions of EA, in unique factorization domains. There is obtained the existence criterion to represent a fixed element of the fractions field of a unique factorization domain in the form of a continued fraction of a fixed length. This criterion enables to obtain a formula for the length of the least remainder (on norm) EA as a function of elements, with respect to which EA is applied. This result gives us the class $\mathcal{T}$ of unique factorization domains, for which the Lazard theorem analogue is valid. We propose algorithms to check whether the given unique factorization domain belongs to the class $\mathcal{T}$. We find the necessary and sufficient conditions under which the number of steps in the worst case of the least remainder EA grows not faster than logarithm. In particular, these results hold for the least remainder EA in any Euclidean quadratic domain. We provide counterexamples, which show the essentiality of the conditions in the obtained theorems.

E-mail addresses: vaskovskii@bsu.by (M. Vaskouski), nkondr2006@rambler.ru (N. Kondratyonok).

http://dx.doi.org/10.1016/j.jsc.2016.02.003
0747-7171/

1. Introduction

Let a and b be two nonzero elements of a unique factorization domain (UFD) $\mathbb{K}$. In this paper we investigate the problem on searching for shortest division chains (DC)

$$r_i = r_{i-2} - q_i r_{i-1},\ i = 1, 2, \ldots, k, \tag{1}$$

where $q_1, \ldots, q_k \in \mathbb{K}$, $r_{-1} = a$, $r_0 = b$, $r_1, \ldots, r_{k-1} \in \mathbb{K}$, $r_k = 0$. If there exists finite DC (1), then it may be considered as a version of the Euclidean Algorithm (EA) and $r_{k-1} = \gcd(a, b)$.

Vahlen (1895) and Kronecker (1901) (see Bach and Shallit, 1996, p. 80) have proved that the least remainder EA requires no more division steps than any other EA which chooses between a remainder of $(a \mod b)$ or $((a \mod b) - b)$ at each step. Lazard (1977) has extended the Kronecker–Vahlen theorem on the case where any remainder is chosen at each step and also has proved the analogue of this theorem for polynomials over a field. Kaltofen and Rolletschek (1985) and Rolletschek (1986) have established the Lazard theorem analogue for special cases of imaginary quadratic domain $\mathbb{Z}[\sqrt{d}]$, d is a negative integer. Rolletschek (1990) has given a complete solution to the problem on shortest Euclidean algorithm in arbitrary imaginary quadratic domains $\mathbb{Z}[\sqrt{d}]$: the Lazard theorem analogue is valid in $\mathbb{Z}[\sqrt{d}]$, $d < 0$, if and only if $d \neq -11c^2$, $c \in \mathbb{N}$. Up to present the question on the validity of the Lazard theorem analogue is still open for all rings $\mathbb{Z}[\sqrt{d}]$ with $d > 1$. Vaskouski and Kondratyonok (2013) have found a class of Euclidean domains, for which the Lazard theorem analogue holds. The main purpose of this paper is to enlarge the class of unique factorization domain, for which the Lazard theorem analogue is valid, and estimate the length of chain (1) for fixed a and b.

The present paper is organized by the following way. Section 2 contains basic definitions and statements of main results. In section 3 we give general methods of main results proofs. Detailed proofs are given in section 4. Methods for validation of conditions in main theorems are given in section 5. Finally, section 6 is devoted to discuss the results, more precisely we provide some counterexamples to show essentiality of the conditions in main theorems. Also there is given an application to optimization of algorithm for solution of linear Diophantine equation in general UFD.

2. Main results

In this section we introduce some definitions and notation and give statements of the main results.

Definition 1. A function $\upsilon : \mathbb{K} \to \mathbb{N} \cup \{0, -\infty\}$ is called a *norm* in a UFD $\mathbb{K}$, if the following conditions hold:

1. $\upsilon(x) = -\infty$ iff $x = 0$;
2. $\upsilon(xy) \geq \upsilon(y)$ for any $x, y \in \mathbb{K}_*$;
3. If $x, y \in \mathbb{K}_*$, then $\upsilon(xy) = \upsilon(x)$ iff $y \in \mathbb{I}$, where $\mathbb{I}$ is the set of all invertible elements of $\mathbb{K}$.

Remark 1. Let $\mathbb{K}$ be a UFD, take an arbitrary element $x \in \mathbb{K}_*$. There exists a unique (up to multiplying of p_i by invertible elements of the domain $\mathbb{K}$) representation $x = \varepsilon p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\varepsilon \in \mathbb{I}$, $p_1, \ldots, p_k$ are prime elements of $\mathbb{K}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, $k \geq 0$ (if $k = 0$, then $x = \varepsilon$). It's clear that the function $\upsilon : \mathbb{K} \to \mathbb{N} \cup \{0, -\infty\}$, defined as $\upsilon(x) = \sum_{i=1}^{k} \alpha_i$, $x = \varepsilon p_1^{\alpha_1} \ldots p_k^{\alpha_k} \in \mathbb{K}_*$, $\upsilon(0) = -\infty$, is a norm in the UFD $\mathbb{K}$, where $\sum_{i=1}^{k} \alpha_i = 0$ for $k = 0$.

Remark 2. It's easy to check that any Euclidean norm $\upsilon(\cdot)$ is also norm in the sense of Definition 1.

Definition 2. Let $\mathbb{F}$ be the field of fractions of a UFD $\mathbb{K}$ with a norm υ. A function $\mathrm{fr} : \mathbb{F} \to \mathbb{F}$ is called a *fractional part* in $\mathbb{F}$ if the following holds:

1. $\mathrm{fr}(\alpha + q) = \mathrm{fr}(\alpha)$ for any $\alpha \in \mathbb{F}$, $q \in \mathbb{K}$;
2. If $m/n \in \mathbb{F}$, $\gcd(m, n) = 1$, then $\mathrm{fr}(m/n) = r/n$, where $r \in \mathbb{K}$, $(m-r)/n \in \mathbb{K}$, and $\upsilon(r) = \min\{\upsilon(s) | s \in \mathbb{K}, (m-s)/n \in \mathbb{K}\}$.