Finite Fields and Their Applications 55 (2019) 33–63

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Explicit equivalence of quadratic forms over $\mathbb{F}_q(t)$

Gábor Ivanyos[a], Péter Kutas[a,b,*], Lajos Rónyai[a,c]

[a] *Institute for Computer Science and Control, Hungarian Acad. Sci., Hungary*
[b] *Central European University, Department of Mathematics and its Applications, Hungary*
[c] *Dept. of Algebra, Budapest Univ. of Technology and Economics, Hungary*

ARTICLE INFO

Article history:
Received 3 November 2016
Received in revised form 3 September 2018
Accepted 8 September 2018
Available online xxxx
Communicated by James W.P. Hirschfeld

MSC:
68W30
11E12
11E20

Keywords:
Quadratic forms
Function field
Polynomial time algorithm

ABSTRACT

We propose a randomized polynomial time algorithm for computing non-trivial zeros of quadratic forms in 4 or more variables over $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is a finite field of odd characteristic. The algorithm is based on a suitable splitting of the form into two forms and finding a common value they both represent. We make use of an effective formula for the number of fixed degree irreducible polynomials in a given residue class. We apply our algorithms for computing a Witt decomposition of a quadratic form, for computing an explicit isometry between quadratic forms and finding zero divisors in quaternion algebras over quadratic extensions of $\mathbb{F}_q(t)$.

© 2018 Elsevier Inc. All rights reserved.

1. Introduction

In this paper we consider algorithmic questions concerning quadratic forms over $\mathbb{F}_q(t)$ where q denotes an odd prime power. The main focus is on the problem of finding a

[*] Corresponding author.
E-mail addresses: Gabor.Ivanyos@sztaki.mta.hu (G. Ivanyos), Kutas_Peter@phd.ceu.edu (P. Kutas), lajos@ilab.sztaki.hu (L. Rónyai).

https://doi.org/10.1016/j.ffa.2018.09.003
1071-5797/© 2018 Elsevier Inc. All rights reserved.

non-trivial zero of a quadratic form. The complexity of the problem of finding non-trivial zeros of quadratic forms in three variables has already been considered in ([4], [8]). However the same problem concerning quadratic forms of higher dimensions remained open.

Similarly, in the case of quadratic forms over $\mathbb{Q}$, the algorithmic problem of finding non-trivial zeros of 3-dimensional forms was considered in several papers ([5], [9]) and afterwards Simon and Castel proposed an algorithm for finding non-trivial zeros of quadratic forms of higher dimensions ([18], [3]). The algorithms for the low-dimensional cases (dimension 3 and 4) run in polynomial time if one is allowed to call oracles for integer factorization. Surprisingly, the case where the quadratic form is of dimension at least 5, Castel's algorithm runs in polynomial time without the use of oracles. Note that, by the classical Hasse–Minkowski theorem, a 5-dimensional quadratic form over $\mathbb{Q}$ is always isotropic if it is indefinite.

Here we consider the question of isotropy of quadratic forms in 4 or more variables over $\mathbb{F}_q(t)$. The main idea of the algorithm is to split the form into two forms and find a common value they both represent. Here we apply two important facts. There is an effective bound on the number of irreducible polynomials in an arithmetic progression of a given degree. An asymptotic formula, which is effective for large q, was proven by Kornblum [10], but for our purposes, we apply a version with a much better error term, due to Rhin [15, Chapter 2, Section 6, Theorem 4]. However, that statement is slightly more general; hence we cite a specialized version from [20]. A short survey on the history of this result can be found in [6, Section 5.3]. The other fact we use is the local-global principle for quadratic forms over $\mathbb{F}_q(t)$ due to Rauter [14].

Finally we solve these two equations separately using the algorithm from [4] and our Algorithm 1 in the 5-variable case. In the 4-dimensional case we are also able to detect if a quadratic form is anisotropic; note that a 5-dimensional form over $\mathbb{F}_q(t)$ is always isotropic. The algorithms are randomized and run in polynomial time. We also give several applications of these algorithms. Most importantly, we propose an algorithm which computes a transition matrix of two equivalent quadratic forms.

The paper is divided into five sections. Section 2 provides theoretical and algorithmic results concerning quadratic forms over fields. Namely, we give a general introduction over arbitrary fields and then over $\mathbb{F}_q(t)$, which is followed by a version of the Gram–Schmidt orthogonalization procedure which gives control of the size of the output.

In Section 3 we present the crucial ingredients of our algorithms. In Section 4 we describe the main algorithms and analyze their running time and the size of their output. In Section 5 we use the main algorithms to compute explicit equivalence of quadratic forms. In the final section we apply our results to find zero divisors in quaternion algebras over quadratic extensions of $\mathbb{F}_q(t)$ or, equivalently, to find zeros of ternary quadratic forms over quadratic extensions of $\mathbb{F}_q(t)$. The material of this part is the natural analogue of that presented in [11] over quadratic number fields.

Download English Version:

https://daneshyari.com/en/article/10224051

Download Persian Version:

https://daneshyari.com/article/10224051

Daneshyari.com