Finite Fields and Their Applications 51 (2018) 191–203

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On common zeros of a pair of quadratic forms over a finite field

A.S. Sivatski

Departamento de Matemática, Universidade Federal do Rio Grande do Norte, Natal, Brazil

ARTICLE INFO

Article history:
Received 11 December 2016
Received in revised form 7 December 2017
Accepted 16 January 2018
Available online xxxx
Communicated by L. Storme

MSC:
11E04
11E81
11R99
11T99

Keywords:
Quadratic form
Brumer's theorem
Global field
The Hasse–Minkowski theorem
Second residue map

ABSTRACT

Let F be a finite field of characteristic distinct from 2, f and g quadratic forms over F, $\dim f = \dim g = n$. A particular case of Chevalley's theorem claims that if $n \geq 5$, then f and g have a common zero. We give an algorithm, which establishes whether f and g have a common zero in the case $n \leq 4$. The most interesting case is $n = 4$. In particular, we show that if $n = 4$ and $\det(f + tg)$ is a squarefree polynomial of degree different from 2, then f and g have a common zero. We investigate the orbits of pairs of 4-dimensional forms (f, g) under the action of the group $\mathrm{GL}_4(F)$, provided f and g do not have a common zero. In particular, it turns out that for any polynomial $p(t)$ of degree at most 4 up to the above action there exist at most two pairs (f, g) such that $\det(f + tg) = p(t)$, and the forms f, g do not have a common zero. The proofs heavily use Brumer's theorem and the Hasse–Minkowski theorem.

0. Introduction

Let $F = \mathbb{F}_q$ be the finite field of odd order q, f and g quadratic forms over F of dimension n (considered as homogeneous quadratic polynomials in n variables). It follows

E-mail address: alexander.sivatski@gmail.com.

https://doi.org/10.1016/j.ffa.2018.01.007

from Chevalley's theorem ([6], Ch. 2, 15.4) that if $n \geq 5$, then f and g have a common zero. Another way to prove this is to note that since $F(t)$ is a global function field, then by the Hasse–Minkowski theorem the form $f+tg$ is isotropic. Now the statement follows from Brumer's theorem ([1]), which claims that f *and* g *have a common zero if and only if the form* $f+tg$ *over the rational function field* $F(t)$ *is isotropic.*

If $n \leq 4$, then, as easy to see, there are examples of pairs (f,g) without a common zero, and it is a natural question to ask how one can determine whether the forms have a common zero or not. In the present paper we investigate separately the cases $n=2,3,4$ (in fact, the case $n=2$ is trivial), and classify pairs (f,g) without common zero.

Our notation is standard, but for the convenience of the reader we recall some definitions and basic results, which we need in the sequel.

- $\mathrm{GL}_n(k)$ is the group of invertible square matrices of order n over the field k.
- S^t is the transpose of the matrix S.
- If p is an irreducible polynomial in one variable over the field k, then k_p is the quotient $k[t]/p$. For a polynomial $f \in k[t]$ its image in k_p is denoted by $\overline{f}$.
- $\mathbb{A}^1_k$ is the affine line over the field k. Clearly, closed points of $\mathbb{A}^1_k$ are in one-to-one correspondence with monic irreducible polynomials in one variable over k.
- $\mathbb{P}^1_k$ is the projective line over k. The difference $\infty = \mathbb{P}^1_k \setminus \mathbb{A}^1_k$ is called the infinity point. For a closed point $v \in \mathbb{P}^1_k$ we denote by $\widehat{k_v}$ the completion of the field $k(t)$ with respect to the discrete valuation determined by v. It is clear that the residue field of $\widehat{k_p}$ coincides with k_p for any $p \in \mathbb{A}^1_k$.
- $\langle a_1, \dots, a_n \rangle$ is the diagonal quadratic form with coefficients $a_1, \dots, a_n \in k^*$.
- The form $\langle\langle a_1, \dots, a_n \rangle\rangle := \langle 1, -a_1 \rangle \otimes \cdots \otimes \langle 1, -a_n \rangle$ is called an n-fold Pfister form.
- We use the sign $\simeq$ for isomorphism of forms and $=$ for the equality of elements in the Witt ring of a field.
- For any field k denote as usual by $W(k)$ the Witt group of k. It is well known (see, for example, [6], Ch. 6, §3) that the sequence of abelian groups

$$0 \to W(k) \xrightarrow{\text{res}} W(k(t)) \xrightarrow{\coprod \partial_p} \coprod_{p \in \mathbb{A}^1_k} W(k_p) \to 0 \tag{$*$}$$

is exact. Here $\partial_p : W(k(t)) \to W(k_p)$ is the residue homomorphism well defined by the rule

$$\partial_p(\langle f \rangle) = \begin{cases} 0 & \text{if } v_p(f) = 0 \\ \langle \overline{fp^{-1}} \rangle & \text{if } v_p(f) = 1 \end{cases},$$

where v_p is the discrete valuation on $k(t)$ corresponding to p. For the infinity point ∞ there is a homomorphism $\partial_\infty : W(k(t)) \to W(k)$ defined by the rule

$$\partial_\infty(\langle f(t) \rangle) = \partial_u(\langle f(u^{-1}) \rangle) = \langle \frac{1-(-1)^n}{2} l(f) \rangle,$$