Finding nontrivial zeros of quadratic forms over rational function fields of characteristic 2

Tímea Csahók Péter Kutas Mickaël Montessinos
Gergely Zábrádi

ISSAC
Wednesday 6th July, 2022

Algorithms for solving quaternary quadratic forms

Problem

Let Q be a regular quaternary quadratic form over a computable field K. Decide whether Q is isotropic. If it is, find an isotropic vector.

- For $K = \mathbb{Q}$: Simon, 2005
- For $K = \mathbb{F}_q(t)$, q odd: Ivanyos, Kutas, Rónyai 2019
- For K a finite extension of $\mathbb{F}_q(t)$, q odd: Koprowski 2021
- For $K = \mathbb{F}_q(t)$, q even: Csahók, Kutas, Zábrádi, M.

Strategy

Odd characteristic:

1. $Q(x_1, x_2, x_3, x_4) = 0$
2. $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0$
3. $a_1x_1^2 + a_2x_2^2 = c$
   $a_3x_3^2 + a_4x_4^2 = -c$
4. Find modular conditions for c
5. Find $c \in \mathbb{F}_q(t)$ satisfying the conditions
6. Solve $a_1x_1^2 + a_2x_2^2 = cy_1^2$
   $a_3x_3^2 + a_4x_4^2 = -cy_2^2$

Even characteristic:

1. $Q(x_1, x_2, x_3, x_4) = 0$
2. $a_1(x_1^2 + x_1x_2 + a_2x_2^2)$
   $+a_3(x_3^2 + x_3x_4 + a_4x_4^2) = 0$
3. $a_1(x_1^2 + x_1x_2 + a_2x_2^2) = c$
   $a_3(x_3^2 + x_3x_4 + a_4x_4^2) = c$
4. Find modular conditions for c
5. Find $c \in \mathbb{F}_q(t)$ satisfying the conditions
6. Solve $x_1^2 + x_1x_2 + a_2x_2^2 = \frac{c}{a_1}y_1^2$
   $x_3^2 + x_3x_4 + a_4x_4^2 = \frac{c}{a_3}y_2^2$

Reduced quaternary quadratic forms

General reduced form

If Q is a regular quaternary quadratic form over $\mathbb{F}_{2^n}(t)$, there exists $a_1, a_2, a_3, a_4 \in \mathbb{F}_{2^n(t)}$ such that Q is similar to

$$a_1(x_1^2 + x_1x_2 + a_2x_2^2) + a_3(x_3^2 + x_3x_4 + a_4x_4^2)$$

and with the following properties:

- $a_1, a_3 \in \mathbb{F}_{2^n}[t]$ and $\gcd(a_1, a_3) = 1$.
- a_2 and a_4 both have odd valuation at their respective poles.

Theorem (Local-global principle)

A non-degenerate ternary quadratic form over $\mathbb{F}_{2^n}(t)$ is isotropic if it is isotropic in every completion of $\mathbb{F}_{2^n}$ except possibly one.

Quadratic residues in characteristic 2

Odd or zero characteristic	Even characteristic
$x \in F^\times$	$x \in F$
$x \mapsto x^2$	$x \mapsto \wp(x) = x^2 + x$
$(xy)^2 = x^2y^2$	$\wp(x+y) = \wp(x) + \wp(y)$
$x^2 = (-x)^2$	$\wp(x) = \wp(x+1)$
$\left(\frac{a}{\pi}\right)$	$[a, \pi)$

Table: Quadratic residues in even and odd characteristic. [1]

[1] Heavily inspired by a similar table in Keith Conrad's notes.

When π is not a pole of the even index coefficients

Theorem

Let π be an irreducible element of $\mathbb{F}_{2^q}[t]$, or let $v_\pi(.) = -\deg(.)$. Assume $v_\pi(a) \geq 0$.

- *If $v_\pi(b)$ is even, then the equation $x^2 + xy + ay^2 = b$ has a solution in $\mathbb{F}_{2^n}(t)_\pi$.*
- *If $v_\pi(b)$ is odd, then the equation $x^2 + xy + ay^2 = b$ has a solution in $\mathbb{F}_{2^n}(t)_\pi$ if and only if $[a, \pi) = 0$.*

$$(t^2 + t + 1)(x_1^2 + x_1x_2 + tx_2^2) = c \tag{1}$$

$$x_3^2 + x_3x_4 + x_4^2 = c \tag{2}$$

At $\pi = t^2 + t + 1$,

$$[t, \pi) = 1, \text{ and } [1, \pi) = 0$$

Hence $v_\pi(c)$ must be odd.

Handling the place at infinity

$$(t^2 + t + 1)(x_1^2 + x_1x_2 + tx_2^2) = c \tag{1}$$

$$x_3^2 + x_3x_4 + x_4^2 = c \tag{2}$$

Apply $\varphi : t \mapsto \frac{1}{t}$:

$$\left(\frac{1}{t^2} + \frac{1}{t} + 1\right)\left(y_1^2 + y_1y_2 + \frac{1}{t}y_2^2\right) = \varphi(c)$$

$$y_3^2 + y_3y_4 + y_4^2 = \varphi(c)$$

Normalize:

$$(t^2 + t + 1)\left(z_1^2 + z_1z_2 + \frac{1}{t}z_2^2\right) = \varphi(c) \tag{3}$$

$$z_3^2 + z_3z_4 + z_4^2 = \varphi(c) \tag{4}$$

When π is a pole of an even index coefficient

Theorem

Let $a, b \in \mathbb{F}_{2^n}(t)_f$ such that $v_\pi(a) = 0$ and $v_\pi(b) = 0$ or 1. Then the equation

$$\pi^{2r+1}x^2 + \pi^{2r+1}xy + ay^2 = \pi^{2r}b$$

admits a solution in $\mathbb{F}_{2^n}(t)_\pi$ if and only if it admits one modulo π^{4r+3}.

$$(t^2 + t + 1)\left(z_1^2 + z_1z_2 + \frac{1}{t}z_2^2\right) = \varphi(c) \tag{3}$$

$$z_3^2 + z_3z_4 + z_4^2 = \varphi(c) \tag{4}$$

Equation 3 has a solution in F_t if $\varphi(c) = t^2 + t + 1 \mod t^3$

Looking for the common value

Lemma (Wan 97)

Let $a, n \in \mathbb{F}_q(t)$ be coprime, with m non constant. Let N be a positive integer, and let

$$S_N(a, m) := \#\{f \in \mathbb{F}_q(t) \text{ monic irred.} \mid f \equiv a \mod m, \deg(f) = N\}.$$

Let $M = \deg(m)$ and $\Phi(m)$ be the number of invertible residue classes mod m. Then

$$|S_N(a, m) - \frac{q^N}{\Phi(m)N}| \leq \frac{1}{N}(M+1)q^{\frac{N}{2}}.$$

Conditions:

- At $t^2 + t + 1$: $v_\pi(c) = 1$
- At inf: $\deg(c) = 2n$, and the coefficients of degrees $2n-1$ and $2n-2$ are 1.
- Everywhere else (except possibly once): $v_\pi(c) = 0$

Solving the equation

We find $h = t^6 + t + 1$, irreducible and such that $(t^2 + t + 1)h = t^8 + t^7 + t^6 + t^3 + 1$.
We must now solve:

$$(x_1^2 + x_1x_2 + tx_2^2) = t^6 + t + 1$$

$$(x_3^2 + x_3x_4 + x_4^2) = (t^2 + t + 1)(t^6 + t + 1)$$

Using an algorithm by Ivanyos, Kutas and Rónyai, we get:

$$x_1 = t^3 + t^2 + 1,\ x_2 = t,\ x_3 = t^4 + 1,\ \text{and } x_4 = t^3.$$

In conclusion

Theorem (Csahók,Kutas,Zábrádi,M.)

There exists a polynomial-time algorithm for finding a non-trivial isotropic vector of a non-degenerate quaternary quadratic form over $\mathbb{F}_{2^n}(t)$.

Steps

1. Reduce the input form to a suitable reduced form which is a orthogonal sum of two binary forms
2. List conditions for a polynomial to be a common value of both binary forms
3. Find a polynomial satisfying these conditions (or output $\perp$ if the conditions are incompatible).
4. Solve the resulting ternary forms