# Gröbner Bases and Identities in Witt Rings

Josef Schicho and Georg Regensburger
Johann Radon Institute for Computational and Applied Mathematics (RICAM)
Austrian Academy of Sciences
*{josef.schicho,georg.regensburger}@oeaw.ac.at*

*Special Semester on Gröbner Bases 2006*
*Gröbner Bases in Symbolic Analysis*
*"Difference equations and combinatorial identities"*
*Hagenberg, Austria, 8th May, 2006*

RICAM

# Quadratic Forms

$F$ field $\quad \mathrm{char} F \neq 2$

n-ary quadratic form

$$f(X_1, \ldots, X_n) = \sum_{i,j} a_{ij} X_i X_j \in F[X_1, \cdots, X_n] = F[X]$$

$\dim f = n$ $\qquad a_{ij} = a_{ji} \quad a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$

$M_f = (a_{ij})$ symmetric matrix

$f(X) = X^t \cdot M_f \cdot X \qquad X = (X_1, \ldots, X_n)^t$

$f$ is regular if $M_f$ is regular

All quadratic forms considered are regular

# Equivalent Forms

$f, g$ n-ary quadratic forms

$f \cong g$ if there exists $C \in \mathsf{GL}_n(F)$

$$f(X) = g(C \cdot X)$$

$$M_f = C^t \cdot M_g \cdot C$$

Example: $X_1 X_2 \cong X_1^2 - X_2^2$ $\quad$ $\begin{aligned} X_1 &\mapsto X_1 + X_2 \\ X_2 &\mapsto X_1 - X_2 \end{aligned}$

Every quadratic form is equivalent to a diagonal form

$$d_1 X_1^2 + \cdots + d_n X_n^2 \qquad d_i \in \dot{F}$$

Notation: $\langle d_1, \ldots, d_n \rangle$

Example: $X_1 X_2 \cong \langle 1, -1 \rangle$

# Quadratic Maps

$f$ quadratic form $M_f$

$q_f : F^n \to F \quad q_f(x) = x^t \cdot M_f \cdot x$

$x = (x_1, \cdots, x_n)^t \in F^n$

$q_f(ax) = a^2 q_f(x)$ quadratic

$$q_f = q_g \Rightarrow f = g$$

# Adding and Multiplying Quadratic Forms

$q_1, q_2 \quad \dim q_1, q_2 = m, n$

Orthogonal sum

$$q = q_1 \perp q_2 \qquad q(x \oplus y) = q_1(x) + q_2(y)$$

$\dim q = m + n$

$x \oplus y \in F^m \oplus F^n$

$$\langle a_1, \ldots, a_m \rangle \perp \langle b_1, \ldots, b_n \rangle \cong \langle a_1 \ldots, a_m, b_1, \ldots, b_n \rangle$$

Tensor product (Kronecker product)

$$q = q_1 \otimes q_2 \qquad q(x \otimes y) = q_1(x) \cdot q_2(y)$$

$\dim q = mn$

$x \otimes y \in F^m \otimes F^n$

$$\langle a_1, \ldots, a_m \rangle \otimes \langle b_1, \ldots, b_n \rangle \cong \langle a_1 b_1 \ldots, a_i b_j, \ldots, a_m b_n \rangle$$

Equivalence classes

commutative, associative, distributive

semiring

# Isotropic Forms and Hyperbolic Plane

$q \quad \dim q = n \qquad x \in F^n, x \neq 0$ isotropic if $q(x) = 0$

$q$ **isotropic** if there exists an isotropic vector

**anistropic** otherwise

$\dim q = 2 \qquad q$ isotropic $\Leftrightarrow q \cong \langle 1, -1 \rangle \Leftrightarrow q \cong X_1 X_2$

Equivalence class for $\langle 1, -1 \rangle$ is called the hyperbolic plane

$q$ isotropic $\Leftrightarrow \quad q \cong \langle 1, -1, a_3, \ldots, a_n \rangle \qquad a_i \in \dot{F}$

Witt decomposition: $\quad q = q_h \perp q_a \quad$ unique up to equivalence

hyperbolic

anisotropic

$$q_h \cong n \cdot \langle 1, -1 \rangle \cong X_1 X_2 + \cdots + X_{2m-1} X_m$$

# Witt’s Cancellation Theorem

$$q\perp q_1 \cong q\perp q_2 \Rightarrow q_1 \cong q_2$$

Can be done constructively:

| | | |
|---|---|---|
| $M_1, M_2$ | symmetric matrices | $q\perp q_1, q\perp q_2$ |
| $N_1, N_2$ | corresponding to | $q_1, q_2$ |

Given an invertible matrix $C$ such that

$$M_1 = C^t \cdot M_2 \cdot C$$

We can compute an invertible matrix $D$ such that

$$N_1 = D^t \cdot N_2 \cdot D$$

## The Witt Ring

$$q \cong q_h \perp q_a \qquad q' \cong q'_h \perp q'_a$$

$q \sim q'$ Witt similar if $q_a \cong q'_a$

Witt ring: $W(F)$ equivalence classes with $\perp$ and $\otimes$

$q = 0 \in W(F) \Leftrightarrow q$ is hyperbolic $q \cong n \cdot \langle 1, -1 \rangle$

$$q = q' \in W(F) \Leftrightarrow q \cong q'$$

$$\dim q = \dim q'$$

$$W(F): \quad \langle a \rangle \perp \langle -a \rangle = \langle a, -a \rangle = \langle 1, -1 \rangle = 0$$

$$\langle a^2 \rangle = \langle 1 \rangle \qquad a \in \dot{F}$$

## Identities in Witt Rings

Prop:

$$\langle a, b, c\rangle \text{ isotropic } \Leftrightarrow \langle bc, ac, ab, 1\rangle \text{ hyberpolic}$$

$$\Leftrightarrow \langle bc, ac, ab, 1\rangle = 0 \in W(F)$$

We want to prove:

$$\langle a, b, f\rangle, \langle 1, -f, -ab\rangle \text{ isotropic } \Rightarrow \langle a, b, ab\rangle \underset{\uparrow}{\cong} \langle 1, -f, -f\rangle$$

and we want to find an invertible matrix $C$

We have to show in $W(F)$

compute at every step the corresponding matrices (especially Witt cancellation)

$$\begin{array}{c} \langle bf, af, ab, 1\rangle = 0 \\ \langle abf, -ab, -f, 1\rangle = 0 \end{array} \Rightarrow \begin{array}{l} \langle a, b, ab\rangle - \langle 1, -f, -f\rangle \\ = \langle a, b, ab, -1, f, f\rangle = 0 \end{array}$$

# Gröbner Bases and Witt Rings I

$$\begin{array}{r} \langle bf, af, ab, 1\rangle = 0 \\ \langle abf, -ab, -f, 1\rangle = 0 \end{array} \Rightarrow \langle a, b, ab, -1, f, f\rangle = 0$$

Polynomials

$$f_1 = BF + AF + AB + 1$$

$$f_3 = A + B + AB - 1 + 2F$$

$$f_2 = ABF - AB - F + 1$$

$$g_1 = A^2 - 1, g_2 = B^2 - 1, g_3 = F^2 - 1$$

Gröbner Basis for the ideal $f_1, f_2, g_1, g_2, g_3$ $\mathbb{Z}[A, B, F]$ $<_{\text{lex}}, B < A < F$

$$G = f_3, g_1, g_2, g_3$$

$$\langle a, b, ab\rangle \underset{\underset{C}{\uparrow}}{\cong} \langle 1, -f, -f\rangle$$

Prove the result in the Witt ring

Can compute

Witness for the proof

# Gröbner Bases and Witt Rings II

$$f_1:\ BF+AF+AB+1=1-1+1-1=0$$

$$f_2:\ ABF-AB-F+1=1-1+1-1=0$$

$\mathrm{SP}(f_1,f_2)$ S-Polynomial $Bf_1-f_2$

$$Bf_1: B^2F+ABF+AFB^2+B=B-B+B-B=1-1+1-1=0$$

$$B^2F+ABF+AB^2+B=ABF-AB-F+1 \qquad -ABF$$

Witt cancellation

$$B^2F+AB^2+B=-AB-F+1 \qquad B^2=1$$

$$F+A+B=-AB-F+1 \qquad +F-A-B-1$$

$$2F-1+A-A+B-B=-AB-A-B+F-F+1-1$$

Witt cancellation

$$2F-1=-AB-A-B$$

$$\langle 1,-f,-f\rangle \cong \langle a,b,ab\rangle$$

# References

[Lam05] Lam, T. Y., *Introduction to quadratic forms over fields*, American Mathematical Society, 2005

[Sch00] Schicho, J., Proper parametrization of real tubular surfaces, J. Symbolic Comput., 2000, 30, 583-593