

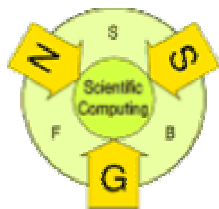
Gröbner Bases and Identities in Witt Rings

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

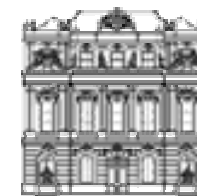
Gröbner Bases in Symbolic Analysis

"Difference equations and combinatorial identities"

Hagenberg, Austria, 8th May, 2006

FWF

Der Wissenschaftsfonds.



RICAM

Quadratic Forms

F field $\text{char}F \neq 2$

n -ary quadratic form

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

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

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

$$f(X) = X^t \cdot M_f \cdot X \quad X = (X_1, \dots, X_n)^t$$

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 $C \in \text{GL}_n(F)$

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

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

Example: $X_1 X_2 \cong X_1^2 - X_2^2$ $X_1 \mapsto X_1 + X_2$
 $X_2 \mapsto X_1 - X_2$

Every quadratic form is equivalent to a diagonal form

$$d_1 X_1^2 + \cdots + d_n X_n^2 \quad d_i \in F$$

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

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

Quadratic Maps

f quadratic form M_f

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

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

$$q_f(ax) = a^2 q_f(x) \quad \text{quadratic}$$

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

Adding and Multiplying Quadratic Forms

Orthogonal sum q_1, q_2 $\dim q_1, q_2 = m, n$

$$q = q_1 \perp q_2 \quad q(x \oplus y) = q_1(x) + q_2(y)$$
$$\dim q = m + n \quad x \oplus y \in F^m \oplus F^n$$
$$\langle a_1, \dots, a_m \rangle \perp \langle b_1, \dots, b_n \rangle \cong \langle a_1, \dots, a_m, b_1, \dots, b_n \rangle$$

Tensor product (Kronecker product)

$$q = q_1 \otimes q_2 \quad q(x \otimes y) = q_1(x) \cdot q_2(y)$$
$$\dim q = mn \quad x \otimes y \in F^m \otimes F^n$$
$$\langle a_1, \dots, a_m \rangle \otimes \langle b_1, \dots, b_n \rangle \cong \langle a_1 b_1, \dots, a_i b_j, \dots, a_m b_n \rangle$$

Equivalence classes

commutative, associative, distributive

semiring

Isotropic Forms and Hyperbolic Plane

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

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

anisotropic otherwise

$\dim q = 2$ 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 $\Leftrightarrow q \cong \langle 1, -1, a_3, \dots, a_n \rangle$ $a_i \in F$

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

↑ ↑

hyperbolic anisotropic

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

Witt's Cancellation Theorem

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

Can be done constructively:

$$\begin{array}{lll} M_1, M_2 & \text{symmetric matrices} & q \perp q_1, q \perp q_2 \\ N_1, N_2 & \text{corresponding to} & q_1, q_2 \end{array}$$

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

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

$$q \sim q' \text{ Witt similar if } q_a \cong q'_a$$

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

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

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

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

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

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

Identities in Witt Rings

Prop:

$$\begin{aligned} \langle a, b, c \rangle \text{ isotropic} &\Leftrightarrow \langle bc, ac, ab, 1 \rangle \text{ hyperbolic} \\ &\Leftrightarrow \langle bc, ac, ab, 1 \rangle = 0 \in W(F) \end{aligned}$$

We want to prove:

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

and we want to find an invertible matrix

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

We have to show in $W(F)$

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

Gröbner Bases and Witt Rings I

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

Polynomials

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

$$f_2 = ABF - AB - F + 1 \quad f_3 = A + B + AB - 1 + 2F$$

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

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

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

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

Prove the result in the Witt ring

Can
compute

\uparrow
 C

Witness for
the proof

Gröbner Bases and Witt Rings II

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

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

SP(f_1, f_2) S-Polynomial $Bf_1 - f_2$

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

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

Witt cancellation

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

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

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

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