

REALIZATION AND INTERPOLATION
via
GRÖBNER BASES

Patrick Fitzpatrick
Mathematics Department, National University of Ireland
&
National Microelectronics Research Centre
Cork, Ireland

INTRODUCTION TO GROÖBNER BASES

- References

Cox, Little, and O'Shea,
Ideals, Varieties, and Algorithms

———, Using Algebraic Geometry

Beker and Weispfenning

Adams and Loustaneau

SOLVING CONGRUENCES MODULO AN IDEAL

- Let $R = F[x_1, \dots, x_n]$
- Let $R = \langle 1 \rangle = I_0 \supset I_1 \supset \dots \supset I_N = I$
where $I_k = \langle \phi_k, I_{k+1} \rangle$ and $x_i \phi_k \in I_{k+1}$ for all i
- Problem: Find solutions to congruences such as

$$a \equiv bh \pmod{I}$$

where h is given mod I

- More generally given h_j solve

$$\sum a_j h_j \pmod{I} \quad j = 1..r \tag{1}$$

- Often only want the “minimal element” for some appropriate definition of minimality

RECURSIVE ALGORITHM

Input

Sequence of ideals I_k and terms ϕ_k , polynomials h_j
Term order $<$.

Output

Gröbner basis \mathcal{W} of the solution module M of (1)
relative to $<$

Initialize

$\ell := 0$; $\mathcal{W} := \text{ord}([1e_k, 1 \leq k \leq r])$

Main program

while $\ell < N$ do

for j from 1 to $|\mathcal{W}|$ do

$\alpha_{\ell j} := \alpha(\mathcal{W}[j], \ell + 1)_j$

$q := \text{least } j \text{ for which } \alpha_{\ell j} \neq 0$

for j from $q + 1$ to $|\mathcal{W}|$ do

$\mathcal{W}[j] := \mathcal{W}[j] - (\alpha_{\ell j} / \alpha_{\ell q}) \mathcal{W}[q]$

replace $\mathcal{W}[q]$ by $[x_i \mathcal{W}[q], 1 \leq i \leq n]$

order(\mathcal{W})

$\ell := \ell + 1$

THEOREM *The set \mathcal{W} is a GB of M relative to $<$.
 $\mathcal{W}[1]$ is the minimal element of M relative to $<$.*

ALTERNANT CODES

- $F = F_{q^m}$
- $\xi_i, i = 1..N$ distinct elements in F
- $\alpha_i, i = 1..N$ non-zero elements in F
- parity check matrix

$$\mathbf{H} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_N \\ \alpha_1 \xi_1 & \alpha_2 \xi_2 & \dots & \alpha_N \xi_N \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1 \xi_1^{s-1} & \alpha_2 \xi_2^{s-1} & \dots & \alpha_N \xi_N^{s-1} \end{pmatrix}$$

- $\mathcal{C} = \text{nullsp}(H) \cap F_q^N$
- $d_{\min}(\mathcal{C}) \geq s + 1$
- Received word w :
syndromes

$$h_i = \sum_{j=1}^n \alpha_j w_j \xi_j^i \quad i = 0..s-1$$

- $h(x) = h_0 + h_1 x + \dots + h_{s-1} x^{s-1}$
- Key equation $\sigma h \equiv \omega \pmod{x^s}$
(error locator σ , error evaluator ω)

DECODING PROBLEM

- Determine (σ, ω) such that $\sigma h \equiv \omega \pmod{x^s}$ with *minimality condition*

$$\delta\omega < \delta\sigma \leq \left\lfloor \frac{s}{2} \right\rfloor \text{ and } \omega, \sigma \text{ relatively prime}$$

- Essentially a *partial realization* problem
- Solution techniques:
 - Peterson-Gorenstein-Zierler '60-'61
 - Berlekamp-Massey '68-'69
 - Sugiyama++ '75, Reed++ '79, Truong++ '88 (Euclid/CF, incorporation of erasures)
 - Welch-Berlekamp '83: conversion to *interpolation problem*
 - Fitzpatrick-Flynn '92: multivariable Padé approximation via Gröbner bases
 - Chambers++ '93: iterative solution to WB problem
 - Fitzpatrick '95: decoding alternant codes via Gröbner bases (PGZ, BM, E)
 - Jennings '95: Gröbner basis solution to WB problem
 - Blackburn '97: Rational interpolation and WB
 - Fitzpatrick '96: Scalar rational interpolation via Gröbner bases
 - Fitzpatrick '97: solving multivariable congruences

RATIONAL APPROXIMATION PROBLEM

- Solution module

$$M = \{(a, b) \in F[x]^2 : ah \equiv b \pmod{x^s}\}$$

- More generally let $h_i \in R = F[x_1, \dots, x_n], i = 1..t$ and let I be an ideal in R then

$$M = \{(a_1, \dots, a_t) \in R^t : \sum_{i=1}^t a_i h_i \equiv 0 \pmod{I}\}$$

- Define a new term order such that the *required solution* (e.g. (σ, ω)) satisfying the minimality condition must lie in a GB w.r.t. that new order
- Use recursive algorithm to determine minimal element
- ASIDE Natural basis $(1, h), (x^s, 0)$ is a GB w.r.t. $<_1$
Convert directly to GB for required $<_2 \rightarrow$ Euclid
Convert using FGLM to GB for required $<_2 \rightarrow$ Peterson-Gorenstein-Zierler

SCALAR RATIONAL INTERPOLATION PROBLEM

- Points

$$(\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_N, \beta_N)$$

- Allowing multiple points with the same first component

$$\begin{aligned} &(\alpha_{j_1}, \beta_{j_1,0}), (\alpha_{j_1}, \beta_{j_1,1}), \dots, (\alpha_{j_1}, \beta_{j_1, n_{j_1}-1}) \\ &(\alpha_{j_2}, \beta_{j_2,0}), (\alpha_{j_2}, \beta_{j_2,1}), \dots, (\alpha_{j_2}, \beta_{j_2, n_{j_2}-1}) \\ &\dots \\ &(\alpha_{j_t}, \beta_{j_t,0}), (\alpha_{j_t}, \beta_{j_t,1}), \dots, (\alpha_{j_t}, \beta_{j_t, n_{j_t}-1}) \end{aligned}$$

- Polynomials: $h_t \in A = F[x]$ by

$$h_i = \sigma_{i,0} + \sigma_{i,1}(x - \tau_i) + \dots + \sigma_{i, n_i-1}(x - \tau_i)^{n_i-1}$$

- Parameterize all rational functions $y(x) = \frac{a(x)}{b(x)}$

interpolating these points i.e. such that

$$\frac{a(\tau_i)}{b(\tau_i)} \equiv h_i \pmod{(x - \tau_i)^{n_i}}, \quad i = 1, \dots, t$$

and satisfying the *minimality condition*

$$\max\{\delta a, \delta b + r\} \text{ as small as possible}$$

(frequently $r = 0$ or $r = -1$)

- Solution module

$$M = \{(a, b) \in F[x]^2 : a \equiv bh \pmod{(x - \tau_i)^{n_i}} \text{ for all } i\}$$

- Find a Gröbner basis relative to a term order defined by minimality condition
- Use recursive algorithm
- Combinations of basis elements solve interpolation problem: unique solution, or parametrized solution set
- Iterative (“recursive”) algorithm incorporating one new point at each step

PARTIAL-PADÉ/PADÉ-TYPE APPROXIMANTS

- Given h, c, s , find all a, b such that

$$ah \equiv b \pmod{x^s}$$

and

c divides a

$$\delta a \leq \ell, \delta b \leq m, \ell + m < s + \delta c$$

- Solution module

$$M = \{(a, b) \in F[x]^2 : a'(ch) \equiv b \pmod{x^s}\}$$

use recursive algorithm (and a different term order)

- Special case: errors and erasures decoding (initialization with c as in BM)

COMPLEXITY OF 1-VARIABLE RECURSIVE ALGORITHM

- THEOREM

1-variable algorithms have the same complexity as Berlekamp-Massey

(with Sylvia Jennings)

TYPICAL COMPUTATION (1-VARIABLE)

- Solution modules $M_i = \{(a, b) : ah \equiv b \pmod{x^i}\}$

- THEOREM

If $\{(a_1, b_1), (a_2, b_2)\}$ is a Gröbner basis of M_i then either

$$\{(a_1, b_1), (xa_2, xb_2)\}$$

or

$$\{(xa_1, xb_1), (a_2, b_2) - \frac{\gamma_2}{\gamma_1}(a_1, b_1)\}$$

is a Gröbner basis of M_{k+1} , where γ_j is the coefficient of x^i in the expansion of $a_j - b_jh$ (the “discrepancy”).

APPLICATION TO SYSTEM THEORY

(with Henry O’Keeffe)

- “Multivariable” (= matrix) case
- Given discrete-time, vector valued time series $w_i, i = 1..t$ determine linear, time-invariant models
- This is equivalent to:
given polynomials

$$h_{ij} \in F[x], i = 1..t, j = 0..s - 1$$

determine all (a_1, \dots, a_t) such that

$$\sum_{i=1}^t a_i h_{ij} \equiv 0 \pmod{x^{s_i}} \text{ for all } i$$

- Recursive modelling of discrete-time systems
- Look for special bases e.g. minimal controllable models
- More generally, allow multivariable polynomials and an ideal modulus
- Generalization of the theorems/algorithms with simpler proofs

BACK TO CODING THEORY

- Decoding algebraic geometry codes (with Mike O'Sullivan)
- Decoding codes over Galois rings (with Eimear Byrne)

CONCLUDING REMARKS

- Methods centre on construction of Gröbner bases of modules relative to chosen term orders
- When a special solution is required we make a *canonical choice* relative to an appropriate term order
- Natural theoretical foundation
- Unification of classical methods