Grbner-Fcher fr lineare Codes

Daniel Rembold

Technische Universität Hamburg Harburg

daniel.rembold@tuhh.de

26. August 2014

Inhaltsverzeichnis

Motivation

- Grbnerbasen
-

Monome

Monom

- Produkt von Variablen ber ein endliches Feld $\mathbb{K}[X_1, X_2, \ldots, X_n]$
- Schreibweise $m = X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}$ und $u_i \in \mathbb{N}_0$

Grad eines Monoms: $deg(m) = \sum_{i=1}^{n} u_i$.

Termordnung

Termordnung $>$

- Relation $>$ zu der Menge von allen Monomen in $\mathbb{K}[X_1, X_2, \ldots, X_n]$

Termordnung

- Lexikographische Ordnung $>_{lex}$
- grad $>_{grlex}$
- Ordnung mit Gewichtsvektor $c = (c_1, \ldots, c_n) \in \mathbb{R}^n$

Leitterm

Leitterm $\mathrm{LT}(f)$

- Polynom $p \in \mathbb{K}[X_1, X_2, \ldots, X_n]$ besitzt Term hchster Ordnung in Bezug auf $>$

Beispiel

Sei $f = x^2 + 3xyz + y^3$

- lex-Order : $f = \underline{x^2} + 3xyz + y^3$
- grlex-Order : $f = \underline{3xyz} + y^3 + x^2$
- $(1,2,1)$: $f = \underline{y^3} + 3xyz + x^2$

Ideale

Ideal

- Kollektion von Polynomen $f_1, \ldots, f_s$:

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in \mathbb{K}[X_1, \ldots, X_n] \right\}.$$

Beispiel

Sei $I = \langle f_1, f_2 \rangle = \langle x^2 + y, x + y + 1 \rangle$ und
$f = x^2 y + x^2 + y^2 + xy + x$
Dann gilt $f = y \cdot f_1 + x \cdot f_2, \; f \in I$.

Divisionsalgorithmus

NVIDIA-Template

- Zerlegung der Matrix in Blöcken
- Verwendung von lokalem Speicher

Grbner Basis

Grbner Fcher

Torische Ideale

BLABLA

Performancemessung auf ATI und NVIDIA

Vergleich

Mögliche Verbesserungen

Quellen

University of Bristol
Optimizing OpenCL performance
http://www.cs.bris.ac.uk/home/simonm/workshops/OpenCL_lecture3.pdf

NVIDIA
OpenCL SDK Code Samples
https://developer.nvidia.com/opencl

Vasily Volkov (UC Berkeley , September 22, 2010)
Better Performance at Lower Occupancy
http://www.cs.berkeley.edu/~volkov/volkov10-GTC.pdf

Vielen Dank für eure Aufmerksamkeit!