Seminar Computeralgebra

Das Verfahren von Niederreiter zur Faktorisierung von Polynomen über kleinen endlichen Primkörpern

Matthias Köppe*

7. Januar 1999

Gegenstand des Vortrages ist der Algorithmus von Niederreiter [Nie93] zur Faktorisierung von Polynomen über kleinen endlichen Primkörpern, insbesondere über $\mathbf{F}_2$.

Die Reduzierung des Problems auf die Faktorisierung *quadratfreier* Polynome wurde bereits im Vortrag [Gas98] zum Berlekamp-Verfahren vorgestellt. Sei daher $f \in \mathbf{F}_p[x]$ bereits ein quadratfreies monisches Polynom mit der Faktorisierung $f = g_1 \cdots g_m$ in irreduzible Faktoren. Wir betrachten die Differentialgleichung

$$L(y) = y^{(p-1)} + y^p = 0 \tag{L}$$

über dem Körper $\mathbf{F}_p(x)$ der rationalen Funktionen über $\mathbf{F}_p$.

Satz 1 *Der Raum der Lösungen y der Differentialgleichung (L) mit festem quadratfreien Nenner $f = g_1 \cdots g_m$ besitzt die $\mathbf{F}_p$-Basis $\left\{ \frac{g_i'}{g_i} : i = 1, \dots, m \right\}$.*

Beweisskizze. Erfüllt $y = h/f$ mit $h \in \mathbf{F}_p[x]$ die Gleichung (L), so liefert ein einfaches Grad-Argument, daß y eine echte rationale Funktion ist ($\deg h < \deg f$). Ist E der Zerfällungskörper von f über $\mathbf{F}_p$, so sind die Wurzeln $\alpha_1, \dots, \alpha_d$ von f in E paarweise verschieden, da f quadratfrei ist (Minimalpolynomargument). Daher besitzt y eine eindeutige Partialbruchzerlegung mit linearen Nennern,

$$y = \sum_{r=1}^{d} \frac{\beta_r}{x - \alpha_r}, \quad \beta_r \in E.$$

Eine Rechnung unter Verwendung des Satzes von Wilson[1] liefert damit die Darstellung

$$y^{(p-1)} = -\sum_{r=1}^{d} \frac{\beta_r}{(x - \alpha_r)^p}. \tag{$*$}$$

*E-Mail: `mkoeppe@cs.uni-magdeburg.de`.

[1] Ein Resultat aus der elementaren Zahlentheorie: *Für jede Primzahl p gilt*

$$(p-1)! \equiv -1 \pmod{p}.$$

Zum Beweis siehe etwa [Leu96, Seite 47].

Ein Koeffizientenvergleich in (L) liefert nun: $\beta_r^p = \beta_r$, also $\beta_r \in \mathbf{F}_p$, für alle $r = 1, \ldots, d$. Zudem sind die zu einem festen g_i gehörenden β_r einander konjugiert und damit identisch; wir bezeichnen sie als $c_i \in \mathbf{F}_p$. Unter Beachtung der Produktregel liefert dies

$$y = \sum_{i=1}^{m} c_i \sum_{\substack{r=1 \\ g_i(\alpha_r)=0}}^{d} \frac{1}{x - \alpha_r} = \sum_{i=1}^{m} c_i \frac{g_i'}{g_i}.$$

Tatsächlich erfüllen rationale Funktionen y dieser Gestalt die Differentialgleichung (L). – Die Eindeutigkeit der Partialbruchzerlegung liefert zudem die $\mathbf{F}_p$-lineare Unabhängigkeit der $\frac{g_i'}{g_i}$. $\square$

Ist $y = h/f$ mit f fest, $\deg f = d$, und $h = \sum_{k=0}^{d-1} h_k x^k \in \mathbf{F}_p[x]$, so läßt sich die Differentialgleichung (L) in der Form

$$f^p \left(\frac{h}{f}\right)^{(p-1)} = -h^p \qquad (\mathrm{L}_f)$$

schreiben. Unter Beachtung von $(*)$ zeigt sich, daß beide Seiten Polynome in x^p mit x-Grad $\leq (d-1)p$ sind. Der Vergleich der Koeffizienten von x^{jp}, $0 \leq j \leq d-1$, führt auf ein äquivalentes lineares Gleichungssystem für $h_0, \ldots, h_{d-1}$:

$$\mathbf{M}_p(f) \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{d-1} \end{pmatrix} = - \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{d-1} \end{pmatrix} \qquad \left|\begin{array}{l} x^{0p} \\ x^{1p} \\ \vdots \\ x^{(d-1)p} \end{array}\right.$$

Mit $\mathbf{h} := (h_0, \ldots, h_{d-1})^\top \in \mathbf{F}_p^d$ erhalten wir die Schreibweise

$$\big(\mathbf{M}_p(f) + \mathbf{I}_d\big)\mathbf{h} = \mathbf{0}. \qquad (\mathrm{M})$$

Satz 2 *Es gilt*

$$\mathrm{rg}\big(\mathbf{M}_p(f) + \mathbf{I}_d\big) = d - m,$$

d. h., die Anzahl der irreduziblen Faktoren von f ist gleich der Dimension des Kerns dieser Matrix. Insbesondere ist f genau dann irreduzibel über $\mathbf{F}_p$, wenn $\mathrm{rg}\big(\mathbf{M}_p(f) + \mathbf{I}_d\big) = d - 1$ gilt.

Beweis. Nach Konstruktion ist der Kern der Matrix genau die Koordinatisierung des Raums der Lösungen h der Differentialgleichung (L_f) bezüglich der Basis $\{x^0, \ldots, x^{d-1}\}$. $\square$

Beispiel Für $p = 3$ lautet (L_f):

$$\left[f^3 \left(\frac{h}{f}\right)'' = \right] f^2 h'' - f f'' h + f f' h' - (f')^2 h = -h^3.$$

Ist $d = 2$, also $f = f_2 x^2 + f_1 x + f_0$ und $h = h_1 x + h_0$, so liefert eine Rechnung:

$$-f_2^2 h_1 x^3 + f_0 f_1 h_1 + (f_0 f_2 - f_1^2) h_0 = h_1 x^3 + h_0.$$

Durch Vergleich der Koeffizienten von x^0 und x^3 erhalten wir das Gleichungssystem

$$\begin{aligned}(f_0 f_2 - f_1^2)h_0 + f_0 f_1 h_1 &= h_0 \\ -f_2^2 h_1 &= h_1,\end{aligned}$$

woraus wir die Matrix $\mathbf{M}_3(f)$ ablesen:

$$\mathbf{M}_3(f) = \begin{pmatrix} f_0 f_2 - f_1^2 & f_0 f_1 \\ 0 & -f_2^2 \end{pmatrix}.$$

Durch Einsetzen des irreduziblen Polynoms $f_1 = x^2 - x - 1$ und des Polynoms $f_2 = x^2 - 1 = (x-1)(x+1)$ bestätigt man die Aussage des Satzes. $\square$

Im binären Fall ($p = 2$) ergibt sich eine wesentliche Vereinfachung. Die Differentialgleichung (L_f) hat hier die Form:

$$(fh)' = h^2. \tag{$\mathrm{L}_f\,2$}$$

Die Matrix $\mathbf{M}_2(f)$ erhalten wir durch Vergleich der Koeffizienten von x^{2j} für $0 \le j \le d-1$. Wegen $(x^{2k+1})' = (2k+1)x^{2k} = x^{2k}$ in $\mathbf{F}_2[x]$ sind die Koeffizienten von x^{2j} auf der linken Seite aber genau die Koeffizienten von x^{2j+1} in fh. Die Matrix $\mathbf{M}_2(f)$ kann damit einfach vom Polynom f abgelesen werden.

Beispiel ($d = 5$)

$$\begin{array}{c} \\ x^0 \\ x^2 \\ x^4 \\ x^6 \\ x^8 \end{array}
\begin{array}{c} \begin{array}{ccccc} h_0 & h_1 & h_2 & h_3 & h_4 \end{array} \\ \begin{pmatrix} f_1 & f_0 & & & \\ f_3 & f_2 & f_1 & f_0 & \\ f_5 & f_4 & f_3 & f_2 & f_1 \\ & f_6 & f_5 & f_4 & f_3 \\ & & & f_6 & f_5 \end{pmatrix} \end{array}$$

Man beachte, daß die Matrix noch immer $\Theta(d^2)$ viele Einträge besitzt. Ist jedoch das Polynom f schwach besetzt, etwa mit c Nichtnullkoeffizienten, so hat die Matrix nur noch $\Theta(cd)$ viele Einträge. Dies kann zur Verbesserung der Zeitkomplexität der Lösung des Gleichungssystems (M) ausgenutzt werden.

Im folgenden sei $m \ge 2$. Nach Satz 1 sind die Lösungen der Differentialgleichung (L_f) genau die

$$h = \sum_{i=1}^{m} c_i b_i \quad \text{mit } c_i \in \mathbf{F}_p \text{ und } b_i = \tfrac{g_i'}{g_i} f \in \mathbf{F}_p[x].$$

Für solche h definieren wir die *Trägermenge* $J(h) = \{\, 1 \le j \le m : c_j \ne 0 \,\}$. Dann erhalten wir durch Erweitern mit $\prod_{j \notin J(h)} g_j$:

$$h = \Bigl(\prod_{j \notin J(h)} g_j \Bigr) \sum_{i \in J(h)} c_i g_i' \prod_{\substack{j \in J(h) \\ j \ne i}} g_j.$$

Daraus folgt unter Beachtung von $\mathrm{ggT}(g_i', g_i) = 1$ die Beziehung

$$\mathrm{ggT}(f, h) = \prod_{j \notin J(h)} g_j.$$

Insbesondere liefert ggT(f, h) *einen nichttrivialen Faktor von f für alle h mit* $1 \leq |J(h)| \leq m-1$. Das sind $p^m - (p-1)^m - 1$ der p^m Lösungen. Für $p = 2$ führen nur zwei der Lösungen auf eine triviale Faktorisierung, d. h., nach $O(1)$ Auswahlschritten wird ein nichttrivialer Faktor gefunden. Für andere kleine p wird eine randomisierte Auswahl von Lösungen in einer niedrigen erwarteten Laufzeit nichttriviale Faktoren liefern.

Die Vorgehensweise des NIEDERREITER-Algorithmus kann wie folgt zusammengefaßt werden.

1. Sichere Quadratfreiheit von f.
2. Bestimme die Matrix $\mathbf{M}_p(f)$.
3. Berechne den Kern der Matrix $\mathbf{M}_p(f) + \mathbf{I}_d$. (Dimension ist Anzahl der irreduziblen Faktoren.)
4. Für Polynome $h \neq 0$, repräsentiert durch Elemente $\mathbf{h}$ des Kerns, berechne ggT(f, h), um nichttriviale Faktoren ggT$(f, h) \neq 1$ von f zu erhalten.

Literatur

[Gas98] GAST, ENRICO: *Der Berlekamp-Algorithmus.* Vortrag im Seminar Computeralgebra, Universität Magdeburg, 1998.

[Knu81] KNUTH, DONALD E.: *Seminumerical Algorithms*, Band 2 der Reihe *The Art of Computer Programming.* Addison–Wesley, Reading, Massachusetts, Zweite Auflage, 1981.

[Leu96] LEUTBECHER, ARMIN: *Zahlentheorie: Eine Einführung in die Algebra.* Springer-Verlag, Berlin–Heidelberg–New York, 1996.

[Nie93] NIEDERREITER, HARALD: *A new efficient factorization algorithm for polynomials over small finite fields.* Applicable Algebra, 4:81–87, 1993.