Spur-kompatible Polynomfolgen über endlichen Körpern

Alfred Scheerhorn
Deutsche Bundespost Telekom
Forschungs- und Technologiezentrum, FZ 123b
64276 Darmstadt
Germany

1 Einführung

Spur-kompatible Polynomfolgen über endlichen Körpern finden Anwendung in der Computeralgebra bei der Implementierung des algebraischen Abschlusses endlicher Körper (siehe [5]). Es wird beschrieben, wie in einigen speziellen Fällen sehr schnell spur-kompatible Folgen erzeugt werden können. Die Beweise sämtlicher hier aufgeführter Sätze findet man in [5].

Die Definition des Begriffes Spur-Kompatibilität erfordert einige Vorbereitungen. Es bezeichne $q > 1$ eine Primzahlpotenz und $K = \mathrm{GF}(q)$ den endlichen Körper der Ordnung q. Sei α ein Element des Erweiterungskörpers $E = \mathrm{GF}(q^m)$, $m \in \mathbb{N}$, und E die kleinste Erweiterung von $\mathrm{GF}(q)$, die α enthält. Die Elemente

$$\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$$

heißen die *Konjugierten* von α über $\mathrm{GF}(q)$. Die *Spur* $\mathrm{T}_{E/K}(\alpha)$ von α über $\mathrm{GF}(q)$ ist definiert als die Summe der Konjugierten von α über $\mathrm{GF}(q)$:

$$\mathrm{T}_{E/K}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i}.$$

Eine Basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ von $\mathrm{GF}(q^m)$ über $\mathrm{GF}(q)$, die aus den Konjugierten eines Elements $\alpha \in \mathrm{GF}(q^m)$ besteht, wird *Normalbasis* genannt. Erzeugt α eine Normalbasis von $\mathrm{GF}(q^m)$ über $\mathrm{GF}(q)$, dann heißt α *normal* in $\mathrm{GF}(q^m)$ über $\mathrm{GF}(q)$. Mit α wird auch das Minimalpolynom

$$f(X) = \prod_{i=0}^{m-1} (X - \alpha^{q^i}) \in \mathrm{GF}(q)[X]$$

von α über $\mathrm{GF}(q)$ normal genannt.

Zur die Definition der Kompatibilität sei I eine unter Teilbarkeit abgeschlossenen Menge natürlicher Zahlen, d.h. mit $n \in I$ gehören auch alle Teiler von n zu I.

Definition 1 *Eine Folge* $(\alpha_n)_{n\in I}$ *von Elementen* $\alpha_n \in \mathrm{GF}(q^n)$ *heißt* spur-kompatibel *über* $\mathrm{GF}(q)$, *wenn für alle* $n \in I$ *gilt:*

1. α_n *ist normal in* $\mathrm{GF}(q^n)$ *über* $\mathrm{GF}(q)$ *und*

2. *Für alle Teiler* d *von* n *gilt für die Spur* $\mathrm{T}_{n:d}(\alpha_n)$ *von* $\mathrm{GF}(q^n)$ *auf* $\mathrm{GF}(q^d)$*:*

$$\mathrm{T}_{n:d}(\alpha_n) = \alpha_d.$$

Eine Folge $(f_n)_{n\in I}$ *von Polynomen* $f_n \in \mathrm{GF}(q)[X]$, $\deg(f_n) = n$, *heißt* spur-kompatibel *über* $\mathrm{GF}(q)$, *wenn für alle* $n \in I$ *gilt:*

1. f_n *ist normal über* $\mathrm{GF}(q)$ *und*

2. *Für jede Wurzel* $\alpha \in \mathrm{GF}(q^n)$ *von* f_n *ist die Spur* $\mathrm{T}_{n:d}(\alpha)$ *von* α *über* $\mathrm{GF}(q^d)$ *eine Wurzel von* f_d*, für alle Teiler* d *von* n*.*

Die Existenz spur-kompatibler Elementefolgen $(\alpha_n)_{n\in\mathbb{N}}$ wird in [4] bewiesen.

Sei nun $(\alpha_n)_{n\in\mathbb{N}}$ spur-kompatible über $\mathrm{GF}(q)$. Wenn man für alle $n \in \mathbb{N}$ die Elemente von $\mathrm{GF}(q^n)$ bezüglich der von α_n erzeugten Normalbasis darstellt, erhält man leicht berechenbare Einbettungen zwischen den Normalbasis-Darstellungen verschiedener Erweitrungen: $\gamma \in \mathrm{GF}(q^d)$ habe die Darstellung

$$\gamma = \sum_{i=0}^{d-1} c_i \alpha_d^{q^i}, \quad c_i \in \mathrm{GF}(q),$$

bezüglich der von α_d erzeugten Normalbasis. Wegen

$$\mathrm{T}_{m:d}(\alpha_m) = \sum_{j=0}^{(m/d)-1} \alpha^{q^{dj}} = \alpha_d,$$

folgt nun

$$\gamma = \sum_{i=0}^{d-1} c_i \mathrm{T}_{m:d}(\alpha_m)^{q^i} = \sum_{i=0}^{d-1} c_i \sum_{j=0}^{(m/d)-1} \alpha_m^{q^{jd+i}} = \sum_{i=0}^{m-1} c_{(i \mod d)} \alpha_m^{q^i}.$$

Die Einbettung der Normalbasis-Darstellung von $\mathrm{GF}(q^d)$ in die von $\mathrm{GF}(q^m)$ entspricht somit einer (m/d)-fachen Konkatenation des Koordinatenvektors $(c_0, c_1, \ldots, c_{d-1})$ von γ.

Mit dem folgendem Satz läßt sich die Bestimmung eines spur-kompatiblen Elementes in $\mathrm{GF}(q^n)$, $n = \prod p^{e_p}$, reduzieren auf die Bestimmung spur-kompatibler Elemente in den Erweiterungen der Primzahlpotenzgrade p^{e_p} über $\mathrm{GF}(q)$.

Satz 1 *Für Primzahlen* p *seien bereits spur-kompatible Elementefolgen* $(\alpha_{p^e})_{e\geq 0}$ *über* $\mathrm{GF}(q)$ *gegeben. Dann ist die Folge* $(\alpha_n)_{n\geq 1}$ *spur-kompatibel über* $\mathrm{GF}(q)$*, wenn für alle zusammengesetzten* $n \in \mathbb{N}$ *mit der Primfaktorisierung* $n = \prod_{i=1}^{r} p_i^{e_i}$ *definiert wird:*

$$\alpha_n = \alpha_1^{1-r} \prod_{i=1}^{r} \alpha_{p_i^{e_i}}.$$

In [5] Kapitel 2.6 wird ein Algorithmus zur Berechnung spur-kompatibler Elementefolgen $(\alpha_{p^e})_{e\geq 0}$, p prim, über $\mathrm{GF}(q)$ beschrieben, der eine Komplexität von $O(m^3 \log m \log q)$ $\mathrm{GF}(q)$-Operationen hat. Wir beschreiben im folgenden, wie für spezielle Paare (q,p) auf einfachere Weise spur-kompatible Folgen berechnet werden können.

2 Der Fall $\mathrm{char}(\mathrm{GF}(q)) = p$

Diese Situation ist aus der Artin-Schreier-Theorie wohlbekannt. Die Untersuchungen orientieren sich an Trinomen der Form

$$X^p - X - \alpha.$$

Hier gilt ein sehr einfaches Normalitätskriterium: Ein Element α_n vom Grad p^n über $\mathrm{GF}(q)$ ist genau dann normal über $\mathrm{GF}(q)$, wenn die Spur von α_n über $\mathrm{GF}(q)$ ungleich 0 ist. Diese Spur ist am Minimalpolynom von α_n über $\mathrm{GF}(q)$ ablesbar.

Zur Beschreibung des folgenden Ergebnisses benötigen wir *reziproke* Polynome. Für $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$ aus $\mathrm{GF}(q)[X]$ heißt

$$f^*(X) := \frac{1}{a_0}(a_0 X^m + a_1 X^{m-1} + \ldots + a_{m-1}X + 1) = \frac{1}{a_0} X^m f(\frac{1}{X})$$

das zu f reziproke Polynom.

Satz 2 *Sei $K = \mathrm{GF}(q)$ ein endlicher Körper der Charakteristik p und $\beta_0 \in K$ mit absoluter Spur $\mathrm{T}_K(\beta_0) \neq 0$ und $\mathrm{T}_K(\beta_0^{-1}) \neq 0$. Weiter sei $f_1(X) = X^p - X - \beta_0^{-1} \in K[X]$. Für $n > 0$ definieren wir bei ungeradem p rekursiv jedes Polynom $g_n \in K[X]$ durch Wahl einer der drei Möglichkeiten*

1. *$g_n(X) = -f_n^*(-1-X)$ oder*
2. *$g_n(X) = -f_n^*(1-X)$ oder*
3. *$X^{p^n} g_n(X - X^{-1}) = -f^*(-X)f(X)$,*

für $p = 2$ definieren wir $g_n(X) = f_n^*(X+1)$. Unabhängig von der Charakteristik sei $f_{n+1} \in K[X]$ durch $f_{n+1}(X) = g_n^*(X^p - X)$ definiert. Dann ist die Folge von Polynomen $(g_n)_{n\geq 1}$ spur-kompatibel über K.

Auf die folgende Weise läßt sich ein Element $\beta_0 \in K = \mathrm{GF}(p^r)$ berechnen, dessen absolute Spur $\mathrm{T}_K(\beta_0) \neq 0 \neq \mathrm{T}_K(\beta_0^{-1})$ ist:

Gilt $\mathrm{ggT}(p,r) = 1$, dann wählen wir $\beta_0 = 1 \in K$ und haben $\mathrm{T}_K(\beta_0) = \mathrm{T}_K(\beta_0^{-1}) = r \neq 0$.

Gilt $\mathrm{ggT}(p,r) > 1$ dann sei $r = p^s u$ mit $\mathrm{ggT}(u,p) = 1$. Jetzt liefert uns Satz 2 angewandt auf $K = \mathrm{GF}(p^u)$ und $\beta_0 = 1$ ein Polynom $g_s \in \mathrm{GF}(p^u)[X]$, dessen Wurzeln in $\mathrm{GF}(p^r)$ die gewünschten Bedingungen erfüllen.

3 Der Fall $p = 2$, q ungerade

Für geeignete Polynome $f_1 \in \mathrm{GF}(q)[X]$ vom Grad 2 sind alle Polynome der Folge $(f_n)_{n\geq 1}$, definiert durch

$$f_{n+1}(X) = (2X)^{2^n} f_n(\frac{X + X^{-1}}{2}), \quad n \geq 1,$$

irreduzibel über $\mathrm{GF}(q)$ (vergleiche Cohen [2]). In [5] Kapitel 3.3 wird gezeigt, daß die Polynome dieser Folge (bei geeignetem f_1) für $q \equiv \pm 3 \bmod 8$ und $q \equiv 9 \bmod 16$ normal über $\mathrm{GF}(q)$ sind. Durch eine leichte Abänderung der obigen Rekursionsvorschrift zu

$$g_{n+1}(X) = X^{2^n} g_n(X + 2^{-2n} X^{-1}), \quad n \geq 1,$$

erhält man (bei geeignetem g_1) in den angegebenen Fällen eine spur-kompatible Polynomfolge. Wir vermuten, daß das dieses Verfahren unabhängig von q in ungerader Charakteristik eine spur-kompatible Polynomfolge liefert.

Satz 3 *Sei $q \equiv \pm 3 \bmod 8$ oder $q \equiv 9 \bmod 16$ und sei $g_1 \in \mathrm{GF}(q)[X]$ normiert, irreduzibel vom Grad 2 und normal über $\mathrm{GF}(q)$. Im Falle $q \equiv 1 \bmod 4$ sei g_1 selbstreziprok gewählt. Weiter sei $g_1(1)g_1(-1)$ kein Quadrat in $\mathrm{GF}(q)$. Dann ist die Folge $(g_n)_{n\geq 1}$, definiert durch*

$$g_{n+1}(X) = X^{2^n} g_n(X + 2^{-2n} X^{-1}), \quad n \geq 1,$$

spur-kompatibel über $\mathrm{GF}(q)$.

An der folgenden Überlegung erkennt man, daß es Startpolynome $f = g_1$ für solche Folgen gibt.

- Sei $q \equiv 1 \bmod 4$. Es gibt nach Cohen [1] $(q-1)/2$ selbstreziproke, irreduzible, normierte Polynome vom Grad 2 über $\mathrm{GF}(q)$. Zu diesen Polynomen gehört nicht (X^2+1), da -1 ein Quadrat in $\mathrm{GF}(q)$ ist. Deshalb sind alle irreduziblen Polynome der Art $f(X) = X^2 + aX + 1$ normal über $\mathrm{GF}(q)$, d.h. es gilt $a \neq 0$. Wegen der Irreduzibilität von f ist $4 - a^2 = f(1)f(-1)$ kein Quadrat in $\mathrm{GF}(q)$.

- Sei $q \equiv 3 \bmod 4$. Dann gibt es keine selbstreziproken, irreduziblen, normierten Polynome f vom Grad 2 über $\mathrm{GF}(q)$, für die $f(1)f(-1)$ kein Quadrat in $\mathrm{GF}(q)$ ist. Denn $f(X) = X^2 + aX + 1$ ist genau dann irreduzibel, wenn $a^2 - 4$ kein Quadrat in $\mathrm{GF}(q)$ ist. Damit ist aber $-(a^2 - 4) = f(1)f(-1)$ ein Quadrat in $\mathrm{GF}(q)$.

  Sei nun $f(X) = X^2 + aX + b$ irreduzibel und $f(1)f(-1)$ kein Quadrat in $\mathrm{GF}(q)$. Dann ist f auch schon normal über $\mathrm{GF}(q)$, denn $a = 0$ würde $f(1)f(-1) = (1 + b)^2$ implizieren. Die Anzahl der gesuchten Polynome f stimmt überein mit der Anzahl selbstreziproker, irreduzibler, normierter Polynome vom Grad 4 über $\mathrm{GF}(q)$, die nach Cohen [1] durch $(q^2 - 1)/4$ gegeben ist.

4 Der Fall $p|(q-1)$, wobei $q \equiv 1 \bmod 4$, falls $p=2$

Für $n \geq 0$ bezeichne ξ_n eine primitve p^n-te Einheitswurzel über $\mathrm{GF}(q)$ mit

$$\xi_{n+1}^p = \xi_n \quad \text{und} \quad K_n := \mathrm{GF}(q^{p^n}).$$

Sei r der Exponent von p in $(q-1)$:

$$q-1 = p^r u, \quad \mathrm{ggT}(p,u) = 1.$$

Dann gilt $\xi_1, \ldots, \xi_r \in \mathrm{GF}(q)$ und nach [3] Theorem 3.75 ist $X^{p^n} - \xi_r$ für alle $n \geq 0$ irreduzibel über $\mathrm{GF}(q)$, so daß

$$\xi_{r+n} \in K_n \quad \text{und} \quad K_{n+1} = K_n(\xi_{n+1+r}).$$

Nun gilt

Lemma 1 *Für alle $n \geq 1$ ist $(\xi_{n+r}-1)^{-1}$ normal in K_n über* $\mathrm{GF}(q)$ *mit der Spur*

$$\mathrm{T}_{K_n/K_{n-1}}(\frac{1}{\xi_{n+r}-1}) = p\frac{1}{\xi_{n-1+r}-1}.$$

Diese Lemma erlaubt die Konstruktion spur-kompatibler Folgen mit

Satz 4 *Die Folge $(\gamma_n)_{n\geq 0}$, definiert durch*

$$\gamma_n = \frac{1}{p^n} \cdot \frac{1}{\xi_{n+r}-1}, \quad n \geq 0,$$

ist spur-kompatible über $\mathrm{GF}(q)$*.*

Für $n \geq 0$ ist $f_n(X) = X^{p^n} - \xi_r$ das Minimalpolynom von ξ_{n+r} über $\mathrm{GF}(q)$. Deshalb ist

$$\left(p^{np^n} f_n(\frac{X}{p^n}+1)\right)^*$$

das Minimalpolynom von γ_n über $\mathrm{GF}(q)$. Dieses Polynom hat die explizite Form

$$f_n(X) = X^{p^n} - \frac{1}{\xi_r - 1} \sum_{0 \leq i < p^n} \binom{p^n}{i} (p^n)^{i-p^n} X^i.$$

5 Der Fall $p|(q+1)$, p ungerade

Es bezeichne wiederum ξ_n eine primitive p^n-te Einheitswurzel über $\mathrm{GF}(q)$, $K_n = \mathrm{GF}(q^{p^n})$ und r den Exponenten von p in (q^2-1). Wegen $p|(q^2-1)$ und [3] Theorem 3.75 ist in diesem Fall $\xi_{n+r} \in \mathrm{GF}(q^{2p^n})$ vom Grad $2p^n$ über $\mathrm{GF}(q)$. Aus $p \not| (q-1)$ folgt $p^r|(q+1)$, so daß

$$\mathrm{T}_{\mathrm{GF}(q^2)/\mathrm{GF}(q)}(\xi_r) = \xi_r + \xi_r^q = \xi_r + \xi_r^{-1}.$$

Allgemeiner ist $(\xi_{n+r} + \xi_{n+r}^{-1}) \in K_n$ vom Grad p^n über $\mathrm{GF}(q)$. Nun gilt

Lemma 2 *Für $n \geq 1$ ist $(\xi_{n+r} + \xi_{n+r}^{-1})^{-1}$ normal in K_n über $\mathrm{GF}(q)$ mit der Spur*

$$\mathrm{T}_{K_n/K_{n-1}}\left(\frac{1}{\xi_{n+r} + \xi_{n+r}^{-1}}\right) = p(-1)^{(p-1)/2} \frac{1}{\xi_{n-1+r} + \xi_{n-1+r}^{-1}}.$$

Diese Lemma erlaubt die Konstruktion spur-kompatibler Folgen mit

Satz 5 *Sei $c = p(-1)^{(p-1)/2}$. Dann ist die Folge $(\gamma_n)_{n\geq 0}$, definiert durch*

$$\gamma_n = \frac{1}{c^n} \cdot \frac{1}{\xi_{n+r} + \xi_{n+r}^{-1}},$$

spur-kompatible über $\mathrm{GF}(q)$.

Zur Berechnung der Minimalpolynome dieser Elemente benötigen wir *normalisierte Tschebyscheff-Polynome 1.Art C_n*, die rekursiv definiert sind durch

$$C_0(X) = 2,\ C_1(X) = X,\ C_{n+1}(X) = XC_n(X) - C_{n-1}(X),\ n \geq 1.$$

Diese Polynome erfüllen

$$C_n(X + X^{-1}) = X^n + X^{-n}$$

für $n \geq 0$ und sind unter Komposition abgeschlossen, d.h. für $n, m \in \mathbb{N}$ gilt

$$C_n(C_m) = C_{nm} = C_m(C_n).$$

Das Minimalpolynom von $(\xi_{n+r} + \xi_{n+r}^{-1})$ läßt sich damit ausdrücken als $f_n(X) := C_{p^n}(X) - \xi_r - \xi_r^{-1}$. Weiter ergibt sich das Minimalpolynom des Elementes γ_n zu

$$\left(c^{np^n} f_n\left(\frac{X}{c^n}\right)\right)^*,$$

wobei $c = p(-1)^{(p-1)/2}$. Dieses Polynom hat die explizite Form

$$f_n(X) = X^{p^n} - \frac{1}{\xi_r + \xi_r^{-1}} \sum_{i=0}^{(p^n-1)/2} \frac{p^n}{p^n - i} \binom{p^n - i}{i} (-1)^i \left(\frac{X}{c^n}\right)^{2i}.$$

6 Der Fall: q primitiv modulo p und $q^{p-1} \not\equiv 1 \bmod p^2$

In diesem Fall ist q für alle $n \geq 1$ primitiv modulo p^n. Weiter impliziert diese Bedingung, daß p ungerade ist und jede primitive p^{n+1}-te Einheitswurzel

$$\xi_{n+1} \in \mathrm{GF}(q^{(p-1)p^n})$$

für alle $n \geq 0$ vom Grad p^n über $\mathrm{GF}(q^{(p-1)})$ ist.

Satz 6 *Für $n \geq 1$ bezeichne α_n die Spur von ξ_{n+1} auf $\mathrm{GF}(q^{p^n})$. Weiter sei s das multiplikative Inverse von p modulo der Charakteristik von $\mathrm{GF}(q)$: $sp \equiv 1(\mathrm{mod}\ \mathrm{char}\ \mathrm{GF}(q))$. Dann ist die Folge $(\gamma_n)_{n\geq 0}$, definiert durch*

$$\gamma_0 = 1, \quad \gamma_n = (\alpha_n + s)\gamma_{n-1}, \quad n \geq 1,$$

spur-kompatibel über $\mathrm{GF}(q)$.

References

[1] Cohen S.D., On Irreducible Polynomials of certain Types over Finite Fields, *Proc. Camb. Phil. Soc.* **66**, S. 335-344, (1969).

[2] Cohen S.D., The explicit Construction of Irreducible Polynomials over Finite Fields, *Designs, Codes and Cryptography* **2**, S.169-174, (1992).

[3] Lidl R., Niederreiter H., *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol.20, Addison-Wesley, Reading, Mass. (1983).

[4] Scheerhorn A., Trace- and Norm-Compatible Extensions of Finite Fields, erscheint in *Appl. Alg. in Eng., Comm. and Comp.*

[5] Scheerhorn A., *Darstellungen des algebraischen Abschlusses endlicher Körper und spur-kompatible Polynomfolgen*, Dissertation, Erlangen, (1993).