Annales Univ. Sci. Budapest., Sect. Comp. 14 (1994) 241-248

ÜBER DIE VERTEILUNG DER B–ELEMENTE IN EINEM POLYNOMRING ÜBER EINEM ENDLICHEN KÖRPER

R. Wagner (Paderborn, Deutschland)

Herrn Professor Karl-Heinz Indlekofer zum 50. Geburtstag gewidmet

Abstract. The purpose of this short note is to describe the distribution of B-elements (i.e. of elements, which are sums of two squares) in the polynomial ring $F_q[x]$ over a finite field F_q. In the case $q \equiv 3 \bmod 4$ the number of representations as sum of two squares is also regarded. Some of the results are very similar to those known about the B-numbers in $\mathbf{N}$.

1. Zunächst sollen einige wohlbekannte Ergebnisse aus der Algebra zusammengestellt werden, die hier, um eine geschlossene Darstellung zu erreichen, ohne Beweis gebracht werden.

(1) *Ein Element a in einem Ring R heißt B-Element, wenn es $b, c \in R$ mit $a = b^2 + c^2$ gibt.*

(2) *Das Produkt von B-Elementen ist wieder ein B-Element.*

(3) *In einem kommutativen Ring R mit 1, in dem 2 invertierbar ist und in dem es ein $\varepsilon \in R$ mit $\varepsilon^2 = -1$ gibt, ist jedes Element B-Element.*

(4) *In F_q (F_q endlicher Körper mit $q = p^m$ vielen Elementen, $p \neq 2$ Primzahl) ist jedes von 0 verschiedene Element B-Element.*[1]

(5) *In F_q (q ungerade) ist -1 genau dann ein Quadrat, wenn $q \equiv 1 \bmod 4$ ist.*

Bemerkung. Die Aussage (5) hat zur Folge, daß in $F_q[x]$ für $q \equiv 1 \bmod 4$ jedes Element B-Element ist, ein für statistische Betrachtungen uninteressanter

[1] Für $p = 2$ ist in F_q jedes Element sogar Quadrat.

Fall. [2] Für die Anzahl der Darstellungen ergibt sich im Falle $q \equiv 1 \bmod 4$: 0 hat unendlich viele Darstellungen als Summe von zwei Quadraten in $F_q[x]$, ein von 0 verschiedenes Element f hat $\frac{T(f)}{4}$ viele Darstellungen als Summe von zwei Quadraten in $F_q[x]$, wobei mit $T(f)$ die Anzahl der verschiedenen Teiler von f bezeichnet wird.[3] Im Fall $q = 2^m$ hat man in jedem Fall unendlich viele Darstellungen.

2. Wir wollen uns nun ausschließlich mit dem Fall $q \equiv 3 \bmod 4$ befassen. Zunächst benötigen wir ein Analogon des Lemmas von Thue:

(6) *Es sei* $f, g \in F_q[x]$, $q \equiv 3 \bmod 4$ *mit* $f, g \neq 0$. *Es sei* $n = \delta(g)$ *(*δ *Grad), und* f *und* g *seien teilerfremd. Dann gibt es* $r, s \in F_q[x]$ *mit* $r, s \neq \neq 0$ *und* $\delta(r) \leq \left[\frac{n}{2}\right], \delta(s) \leq \left[\frac{n}{2}\right]$ *([ ] Gaußklammer), so daß* $rf - s = wg$ *mit geeignetem* $w \in F_q[x]$ *ist.*

Beweis. Allgemein bezeichne $\langle h \rangle_g$ den Rest von $h \in F_q[x]$ bei der Division durch g. Es sei $N_t = \{h \in F_q[x] \mid \delta(h) \leq t\}$. Dann gilt $\sharp(N_t) = q^{t+1}$. Wir definieren $\Phi : N_{[\frac{n}{2}]} \times N_{[\frac{n}{2}]} \to N_{n-1}$ durch $\Phi(\rho, \sigma) := \langle \rho f - \sigma \rangle_g$. Φ ist nicht injektiv, denn

$$\sharp(N_{[\frac{n}{2}]} \times N_{[\frac{n}{2}]}) = q^{2([\frac{n}{2}]+1)} \geq q^{n+1} > q^n = \sharp(N_{n-1}).$$

Aus $\Phi(\rho_1, \sigma_1) = \Phi(\rho_2, \sigma_2)$ folgt mit $r = \rho_1 - \rho_2$, $s = \sigma_1 - \sigma_2$ offenbar $\langle rf - s \rangle_g = \\ = 0$.

Es kann dabei nicht 0 sein, denn sonst wäre s gleich 0. Es kann auch nicht $s = 0$ sein; sonst wäre $rf = wg$, und wegen $\delta(r) < \delta(g)$ würden f und g nicht teilerfremd sein.

Unmittelbar aus (6) folgt nun eine Charakterisierung der exakten Primpotenzteiler der B-Elemente in $F_q[x]$, $q \equiv 3 \bmod 4$.

---

[2] Für $q = 2^m$ gilt: Die B-Elemente sind gerade die Polynome der Form $\sum_{k=0}^{n} a_{2k} x^{2k}$.

[3] $f = w_1 + w_2$ (w_1, w_2 Quadrate) und $f = w_2 + w_1$ sollen dabei als verschiedene Darstellungen angesehen werden, wenn $w_1, w_2 \neq 0$ und $w_1 \neq w_2$ ist. Dagegen soll $f = 0 + w$, $f = w + 0$, (w Quadrat) nur als eine Möglichkeit gezählt werden.

(7) *In* $F_q[x]$, $q \equiv 3 \bmod 4$, *gilt: Wenn ein Primelement* g *ein B-Element* f, $f \neq 0$, *teilt, so ist* g *B-Element oder* $g^{2m} || f$.

Beweis. Nehmen wir an, daß $g^m || f$ und m ungerade ist. Es gelte $f = u^2 + v^2$. Dabei ist $u, v \neq 0$, da sonst f Quadrat ist. Es gelte $g^r || u$ und $g^s || v$; dann ist auch $h = \frac{f}{g^{\min(2r,2s)}}$ ein B-Element, und es gilt $h = \tilde{u}^2 + \tilde{v}^2$ mit $\langle h \rangle_g = 0$. Dabei ist $\langle \tilde{u} \rangle_g \neq 0$ oder $\langle \tilde{v} \rangle_g \neq 0$. Falls $\langle \tilde{v} \rangle_g \neq 0$ ist, folgt $\langle -1 \rangle_g = \frac{(\langle \tilde{u} \rangle_g)^2}{(\langle \tilde{v}_g \rangle)^2}$.

Nach dem Analogon des Lemmas von Thue folgt dann für ε mit $(\langle \varepsilon \rangle_g)^2 = \langle -1 \rangle_g$: Es gibt $r, s \in F_q[x] \setminus \{0\}$ mit $\delta(r) \leq \left[\frac{\delta(g)}{2}\right], \delta(s) \leq \left[\frac{\delta(g)}{2}\right]$ und mit $\langle r\varepsilon - s \rangle_g = \langle 0 \rangle_g$. Dies inpliziert $\langle r\varepsilon + s \rangle_g \cdot \langle -r\varepsilon + s \rangle_g = \langle r^2 + s^2 \rangle_g = \langle 0 \rangle_g$. Somit erhält man $r^2 + s^2 = wg$. Wegen $\delta(r^2 + s^2) \leq n$ gilt dann $w \in F_q \setminus \{0\}$ und $g = \frac{1}{w}(r^2 + s^2)$. Da $\frac{1}{w}$ B-Element ist, ist auch g B-Element.

Wir kommen nun zur Charakterisierung der B-Primelemente.

(8) *In* $F_q[x]$ *mit* $q \equiv 3 \bmod 4$ *sind die Primelemente* g *mit geradem* $\delta(g)$ *die B-Primelemente.*

Beweis. Zunächst ist klar, daß der grad jedes B-Elementes f durch 2 teilbar ist. Dies sieht man für $f = u^2 + v^2$ mit $\delta(u) \neq \delta(v)$ sofort ein. Im Falle $f = u^2 + v^2$ mit $\delta(u) = \delta(v) = n$ erhält man $\delta(f) = 2n$, da der formale Koeffizient bei x^{2n} als Summe von zwei nicht verschwindenden Quadraten $\neq 0$ ist.

Sei g Primelement mit $\delta(g) = 2n$. Dann ist ord $((F_q[x]/g \cdot F_q[x]) \setminus \{0\}, \cdot) = q^{2n} - 1$ durch 4 teilbar. Damit gibt es, da $F_q[x]/g \cdot F_q[x] \setminus \{0\}$ zyklisch ist, ein $\varepsilon \in F_q[x]$ mit $(\langle \varepsilon \rangle_g)^2 = \langle -1 \rangle_g$.

Hieraus folgt wie beim Beweis von (7), daß g B-Element ist. Wir betrachten nun die arithmetische Halbgruppe G (siehe Knopfmacher [3]) der Elemente f in $F_q[x]$ mit höchstem Koeffizienten 1.

(9) *Jedes B-Element in* G *hat die Darstellung* $f = g_1^{t_1} \ldots g_k^{t_k} h_1^{s_1} \ldots h_l^{s_l}$ *mit* $g_1, \ldots, g_k, h_1, \ldots, h_l \in G$, *wobei* $g_1, \ldots, g_k$ *verschiedene B-Primelemente und* $h_1, \ldots, h_l$ *verschiedene Primelemente sind, die nicht B-Elemente sind, und* $s_1, \ldots, s_l$ *gerade natürliche Zahlen bezeichen. (Die Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.)*

Beweis. Die Möglichkeit für die beschriebene Darstellung ergibt sich daraus, daß in $F_q \setminus \{0\}$ jedes Element B-Element ist.

(10) *Für die Anzahl ρ der verschiedenen Darstellungen als Summe von zwei Quadraten*[4] *erhält man, wenn f eine Primfaktorzerlegung der Form aus (9) hat,*

$$\rho(f) = \rho(1) \cdot (t_1 + 1) \dots (t_k + 1).$$

Beweis. Setzt man $\varepsilon := \sqrt{-1}$, und $g_j = (a_j + \varepsilon b_j)(a_j - \varepsilon b_j)$, so hat f in $F_q(\varepsilon)[x]$ die Primfaktorzerlegung

$$f = (a_1 + \varepsilon b_1)^{t_1}(a_1 - \varepsilon b_1)^{t_1} \dots (a_k + \varepsilon b_k)^{t_k}(a_k - \varepsilon b_k)^{t_k} h_1^{s_1} \dots h_l^{s_l}.$$

Wie im Fall der natürlichen Zahlen erhält man aus $f = a^2 + b^2$ sofort $f = (a + \varepsilon b) \cdot (a - \varepsilon b)$. Je vier Elemente der Form $a + \varepsilon b$ führen dabei zur selben Darstellung $f = a^2 + b^2$. $a + \varepsilon b$ ist dann von der Form

$$u \cdot (a_1 + \varepsilon\beta_1)^{m_1}(a_1 - \varepsilon\beta_1)^{t_1 - m_1} \cdot \dots \cdot (a_K + \varepsilon\beta_K)^{m_K}(a_K - \varepsilon\beta_K)^{t_K - m_K} \cdot h_1^{s_1/2} \dots h_l^{s_l/2}$$

mit $u \in F_q(\varepsilon) \setminus \{0\}$ und $0 \le m_i \le t_i$. Für u hat man $4\rho(1)$ viele Möglichkeiten, für die Wahl der m_i je $t_i + 1$ Möglichkeiten, woraus sich ingesamt die behauptete Formel ergibt.

3. Es sei b die charakterische Funktion der B-Zahlen. Es sei $r = \dfrac{\rho}{\rho(1)} \cdot b$ und r sind auf G im Falle $q \equiv 3 \ mod\ 4$ multiplikative Funktionen.

Wir betrachten zunächst b. Es sein $B(n) := \sum\limits_{\substack{a \in G \\ \delta(a) = n}} b(a)$ und $B^{\mathrm{I}}(y) := \sum\limits_{n=0}^{\infty} B(n) y^n$. B^{I} ist für $|y| < \dfrac{1}{q}$ analytisch, und man hat für $|y| < \dfrac{1}{q}$ die Produktdarstellung[5]

$$B^{\mathrm{I}}(y) = \prod_{\substack{p \in \mathbf{P} \\ \delta(p) \text{ gerade}}} \left(1 + \sum_{k=1}^{\infty} y^{k\delta(p)}\right) \cdot \prod_{\substack{p \in \mathbf{P} \\ \delta(p) \text{ ungerade}}} \left(1 + \sum_{k=1}^{\infty} y^{2k\delta(p)}\right) =$$

$$= \prod_{l=1}^{\infty} \frac{1}{(1 - y^{2l})^{P(2l)}} \cdot \prod_{\substack{l=1 \\ l \text{ ungerade}}}^{\infty} \frac{1}{(1 - y^{2l})^{P(l)}}.$$

[4] Die Verschiedenheit der Darstellung soll hier wie in Fußnote 3 definiert sein.

[5] **P** Menge der Primelemente, $P(n)$ Anzahl der Primelemente vom Grade n.

Logarithmierung ergibt

$$\log B^{\natural}(y) = \sum_{l=1}^{\infty}(-P(2l))\log(1-y^{2l}) + \sum_{l \text{ ungerade}}(-P(l))\log(1-y^{2l}) =$$

$$= \sum_{l=1}^{\infty} P(2l) \sum_{k=1}^{\infty} \frac{y^{2lk}}{k} + \sum_{l \text{ ungerade}} P(l) \sum_{k=1}^{\infty} \frac{y^{2lk}}{k}.$$

Ordnet man nach Potenzen von y, so erhält man

$$\log B^{\natural}(y) = \sum_{n \text{ gerade}} \left(\left(\sum_{\substack{d|n \\ d \text{ gerade}}} \frac{P(d)d}{n} \right) + \left(\sum_{\substack{d|n \\ d \text{ ungerade}}} \frac{2 \cdot P(d)d}{n} \right) \right) y^n =$$

$$= \sum_{n \text{ gerade}} \left(\sum_{d|n} \frac{P(d)d}{n} \right) y^n + \sum_{n \text{ gerade}} \left(\sum_{\substack{d|n \\ d \text{ ungerade}}} \frac{P(d)d}{n} \right) y^n.$$

Vergleicht man dies mit der entsprechenden Rechnung für die 1-Funktion, deren erzeugende Funktion die ζ-Funktion ist (siehe Knopfmacher [3]), so erhält man $\sum_{d|n} P(d)d = G(n) = \sharp\{a \in G | \delta(a) = n\} = q^n$.

Man erhält also

$$\log B^{\natural}(y) = \sum_{n \text{ gerade}} \frac{q^n y^n}{n} + \sum_{n \text{ gerade}} \left(\sum_{\substack{d|n \\ d \text{ ungerade}}} \frac{P(d)d}{n} \right) y^n =$$

$$= \frac{1}{2} \sum_{m=1}^{\infty} \frac{(q^2y^2)^m}{m} + \sum_{l=1}^{\infty} \frac{1}{2^l} \sum_{m \text{ ungerade}} \sum_{d|m} \frac{P(d)d}{m} \left(y^{2^l}\right)^m =$$

$$= \frac{1}{2} \log\left(\frac{1}{1-q^2y^2}\right) + \sum_{l=1}^{\infty} \frac{1}{2^l} \sum_{m \text{ ungerade}} \frac{q^m}{m} \left(y^{2^l}\right)^m =$$

$$= \frac{1}{2} \log\left(\frac{1}{1-q^2y^2}\right) + \sum_{l=1}^{\infty} \frac{1}{2^{l+1}} \log\left(\frac{1+qy^{2^l}}{1-qy^{2^l}}\right).$$

Damit ergibt sich

$$B^{\natural}(y) = \underbrace{(1-q^2y^2)^{-\frac{1}{2}}}_{H_q(y)} \cdot \underbrace{\prod_{l=1}^{\infty} \left(\frac{1+qy^{2^l}}{1-qy^{2^l}}\right)^{\frac{1}{2^{l+1}}}}_{N_q(y)}$$

Der Term $N_q(y)$ stellt für $|y| < \frac{1}{\sqrt{q}}$ eine holomorphe Funktion dar. Sowohl H_q als auch N_q sind gerade. Es sei nun $N_q(y) = \sum_{k=0}^{\infty} d_{2k} y^{2k}$. Dann gilt $|d_{2k}| \leq$ $\leq c_\varepsilon q^{(1+\varepsilon)k}$ mit beliebigen $\varepsilon > 0$ und geeigneten $c_\varepsilon > 0$, und es folgt mit $c_k := \frac{d_{2k}}{q^k}$

$$B(2m) = \sum_{k=0}^{m} \binom{-\frac{1}{2}}{m-k} (-1)^{m-k} q^{2m-2k} q^k c_k.$$

Wir formen um

$$B(2m) =$$

$$q^{2m} \frac{1}{\sqrt{2m}} \left(\sum_{k=0}^{m-1} \binom{-\frac{1}{2}}{m-k} (-1)^{m-k} q^{-k} c_k \sqrt{2m-2k} \sqrt{\frac{2m}{2m-2k}} + c_m \sqrt{2m} q^{-m} \right)$$

und schätzen den Term

$$\sum_{k=0}^{m-1} \binom{-\frac{1}{2}}{m-k} (-1)^{m-k} q^{-k} c_k \sqrt{2m-2k} \sqrt{\frac{2m}{2m-2k}} +$$

$$+ c_m \sqrt{2m} q^{-m} - \sum_{k=0}^{\infty} \sqrt{\frac{2}{\pi}} c_k q^{-k}$$

ab. Es gilt

$$\left| \sum_{k=0}^{m-1} \binom{-\frac{1}{2}}{m-k} (-1)^{m-k} q^{-k} c_k \sqrt{2m-2k} \sqrt{\frac{2m}{2m-2k}} + \right.$$

$$\left. + c_m \sqrt{2m} q^{-m} - \sum_{k=0}^{\infty} \sqrt{\frac{2}{\pi}} c_k q^{-k} \right| \leq$$

$$\leq \underbrace{\left| \sum_{k=0}^{[m^\alpha]} \binom{-\frac{1}{2}}{m-k} (-1)^{m-k} \sqrt{2m-2k} \sqrt{\frac{2m}{2m-2k}} c_k q^{-k} - \sum_{k=0}^{[m^\alpha]} \sqrt{\frac{2}{\pi}} c_k q^{-k} \right|}_{\text{Term I}} +$$

$$+ \underbrace{\left| \sum_{k=[m^\alpha]+1}^{m-1} \binom{-\frac{1}{2}}{m-k} (-1)^{m-k} \sqrt{2m-2k} \sqrt{\frac{2m}{2m-2k}} c_k q^{-k} \right|}_{\text{Term II}} +$$

$$+ \underbrace{\left| c_m \sqrt{2m} q^{-m} \right|}_{\text{Term III}} + \underbrace{\left| \sum_{k=[m^\alpha]+1}^{\infty} \sqrt{\frac{2}{\pi}} c_k q^{-k} \right|}_{\text{Term IV}}$$

(hierbei kann $\alpha \in (0,1)$ beliebig gewählt werden).

Die restlichen Abschätzungen beruhen auf der Tatsache, daß

$$\lim_{n\to\infty} \binom{-\frac{1}{2}}{n} \sqrt{2n}(-1)^n = \sqrt{\frac{2}{\pi}}$$

ist; genauer gilt wegen $\frac{1^2 \cdots (2n-1)^2}{2^2 \cdots (2n)^2} \cdot 2n = \frac{\pi}{2} + O(\frac{1}{n})$ auch

$$\binom{-\frac{1}{2}}{n} (-1)^n \sqrt{2n} = \sqrt{\frac{2}{\pi}} + O\left(\frac{1}{n}\right).$$

Wegen $\sqrt{\dfrac{2m}{2m-2k}} = 1 + O\left(\dfrac{1}{m^{1-\alpha}}\right)$ für $k \le [m^\alpha]$ erhält man

$$\text{Term I} = O\left(\frac{1}{m^{1-\alpha}}\right).$$

Weiter gilt

$$\text{Term II} = O\left(\sqrt{m} \cdot \sum_{k=[n^\alpha]+1}^{m-1} c_k q^{-k}\right) = O\left(\sqrt{m} q^{(-1+\epsilon)[m^\alpha]}\right) = O\left(\frac{1}{m^{1-\alpha}}\right)$$

und

$$\text{Term III} = O\left(\frac{1}{m^{1-\alpha}}\right) \quad \text{und} \quad \text{Term IV} = O\left(\frac{1}{m^{1-\alpha}}\right).$$

Insgesamt erhält man im Falle $q \equiv 3 \bmod 4$ die Asymptotik:

(11) $B(2m) = \dfrac{q^{2m}}{\sqrt{2m}} N_q\left(\dfrac{1}{q}\right) \sqrt{\dfrac{2}{\pi}} \left(1 + O\left(\dfrac{1}{m^\beta}\right)\right)$, *wobei* $\beta \in (0,1)$ *beliebig gewählt werden kann.*

Bemerkenswert ist hierbei $\lim\limits_{\substack{q\to\infty \\ q\equiv 3 \bmod 4}} N_q\left(\dfrac{1}{q}\right) = 1.$

(12) *Es sei* $R^\natural$ *die erzeugende Funktion von* r *mit* $R^\natural(y) = \sum\limits_{m=1}^{\infty} R(m) y^m$.[6] *Dann gilt* $R(2m+1) = 0$ *und* $R(2m) = q^{2m}$.[7]

---

[6] $R(m) = \sum\limits_{\delta(a)=n} r(a)$.

[7] Der Beweis kann vom Leser leicht nachvollzogen werden.

Literatur

[1] **Hardy H. and Wright E.M.**, *An introduction to the theory of numbers*, 5th ed., Clarendon Press, Oxford, 1979.

[2] **Indlekofer K.-H.**, The abstract prime number theorem for function fields, *Acta Math.Hung.*, **62** (1-2) (1993), 137-148.

[3] **Knopfmacher J.**, *Analytic arithmetic of algebraic function fields, Lecture Notes in Pure and Applied Mathematics Vol. 50*, Marel Rekker, New York, 1979.

R. Wagner
Universität-GH Paderborn FB 17
Warburger Str. 100.
D-33098 Paderborn, BRD