MATH. SCAND. 58 (1986), 149–160

ERWEITERUNG DREIELEMENTIGER BASEN BEI KONSTANTER FROBENIUSZAHL, II

CHRISTOPH KIRFEL

Der vorliegende Artikel ist eine unmittelbare Fortsetzung von Kirfel [2]. Alle Hinweise auf die Formeln (1)–(7) gehen darauf zurück.

In [2] haben wir das Erweiterungsproblem dreielementiger Basen bei konstanter Frobeniuszahl im Falle $a_1 < a_2 < a_3$, $a < a_2$ völlig abgeschlossen. Das sich anschließende Problem, $a < a_3$, wurde auch damals schon erwähnt und ein Kriterium für die Konstanz der Frobeniuszahl angegeben, allerdings damals ohne Beweis. Das soll jetzt nachgeholt werden.

Zunächst einige Vorbemerkungen. Wir definieren

$$F_d = \left\langle \frac{d\alpha - (s_v - s_{v+1} - 1)}{s_v} \right\rangle$$

$$D = \max\{d \in \mathbf{Z} \mid P_{v+1} - 1 \geqq F_d P_v\}.$$

Zur Berechnung von D bemerken wir, daß

$$F_D \leqq \frac{P_{v+1}-1}{P_v} < F_{D+1} \Rightarrow F_D \leqq \left[\frac{P_{v+1}-1}{P_v}\right] < F_{D+1}$$

$$\Rightarrow \frac{D\alpha - (s_v - s_{v+1} - 1)}{s_v} \leqq q_{v+1} - 1 < \frac{(D+1)\alpha - (s_v - s_{v+1} - 1)}{s_v}$$

$$\Rightarrow D\alpha \leqq q_{v+1}s_v - s_{v+1} - 1 < (D+1)\alpha \Rightarrow D = \left[\frac{s_{v-1}-1}{\alpha}\right].$$

Da $s_{v-1} > s_v > \alpha$, wissen wir auch, daß $D \geqq 1$.

Als erstes beweisen wir:

SATZ 2′. *Sei* $A_4 = A_3 \cup \{a\}$, *a unabhängig von* A_3 *und* $1 < a < a_3$. *Gilt zusätzlich* $P_v a_3 \geqq s_{v+1} a_2$, *dann sind die folgenden beiden Aussagen äquivalent:*

(i)′ $\alpha \geqq s_v - s_{v+1}$, $\beta = 0$; $F_d R_v \geqq dR$, $1 \leqq d \leqq D$

(ii) $g(A_3) = g(A_4)$.

Eingegangen am 11. Märtz, 1985.

BEWEIS. Wir zeigen zunächst (ii) $\Rightarrow$ (i)'. Aus II.1) in [2] folgt $g(A_3) > g(A_4)$, falls $\alpha < s_v - s_{v+1}$, und aus (7) folgt dasselbe, falls $\alpha \geqq s_v - s_{v+1}$, $\beta > 0$. Also $\alpha \geqq s_v - s_{v+1}$, $\beta = 0$ und $a = \alpha a_2 - Ra_1$, wenn (ii) gelten soll.

Wie in Satz 1 aus [2] benutzen wir L_i, x_i und y_i. Dann ist $L_0 = g(A_3) + a_1$ und für $1 \leqq d \leqq D$ gilt

$$L_d = (s_v - s_{v+1} - 1 - d\alpha + F_d s_v)a_2 + (P_{v+1} - 1 - F_d P_v)a_3 + da,$$

denn

$$L_d - g(A_3) - a_1 = d(a - \alpha a_2) + F_d(s_v a_2 - P_v a_3) = (F_d R_v - dR)a_1,$$

und

$$0 \leqq x_d = s_v - s_{v+1} - 1 - d\alpha + F_d s_v < s_v$$
$$0 \leqq y_D = P_{v+1} - 1 - F_D P_v \leqq y_d = P_{v+1} - 1 - F_d P_v \leqq y_1 < P_{v+1} - P_v,$$

letzteres weil $F_1 > 0$ und $1 \leqq d \leqq D$. Wegen (ii) gilt hier

$$0 \leqq L_d - g(A_3) - a_1 = (F_d R_v - dR)a_1, \quad 1 \leqq d \leqq D,$$

also ist (i)' gezeigt.

In der anderen Beweisrichtung (i)' $\Rightarrow$ (ii) müssen wir nun zeigen, daß $L_d > g(A_3)$ für alle $d \geqq 0$. Aus dem obengenannten geht bereits hervor, daß $L_d > g(A_3)$ für $0 \leqq d \leqq D$ und

$$D = \max\{d \in \mathbf{Z} \mid y_0 \geqq \langle (d\alpha - x_0)/s_v \rangle P_v\}.$$

Natürlich ist $y_0 = P_{v+1} - 1$ und $x_0 = s_v - s_{v+1} - 1$. Dies dient uns jetzt als Anfang in einem Induktionsbeweis.

Wir definieren

$$F_e^{(l)} = \left\langle \frac{e\alpha - x_l}{s_v} \right\rangle, \text{ also } F_e^{(0)} = F_e.$$

Angenommen $L_d > g(A_3)$ für $l \leqq d = l + e \leqq k = l + \varepsilon$ mit

$$\varepsilon = \max\{e \in \mathbf{Z} \mid y_l \geqq F_e^{(l)} P_v\}$$

sei bereits gezeigt. Hier gilt dann ähnlich wie oben

$$x_{l+e} = x_l - e\alpha + F_e^{(l)} s_v, \quad y_{l+e} = y_l - F_e^{(l)} P_v.$$

Für die Berechnung von L_{k+1} benötigen wir eine Vorbemerkung: In jeder Darstellung $ta_2 + za_3 \equiv 0 \pmod{a_1}$ der Restklasse $0 \pmod{a_1}$ können die Koeffizienten $t, z \in \mathbf{Z}$ folgendermaßen ausgedrückt werden:

(8) $\quad t = ps_v + q(s_v - s_{v+1}), \quad z = -pP_v + q(P_{v+1} - P_v); \quad p, q \in \mathbf{Z}.$

Denn wegen $(a_1, a_2, a_3) = 1$ gilt $\varphi = (a_1, a_2) \mid z$ und wegen

$$(-P_v, P_{v+1} - P_v) = (P_{v+1}, P_v) = \varphi$$

(siehe dazu [2]) läßt sich z darstellen als

$$z = -\hat{p}P_v + \hat{q}(P_{v+1} - P_v), \quad \hat{p}, \hat{q} \in \mathsf{Z}.$$

Dann ist wegen (2)

$$t = \hat{p}s_v + \hat{q}(s_v - s_{v+1}) + wa_1/\varphi$$

mit einem $w \in \mathsf{Z}$. Setzen wir

$$p = \hat{p} + w(P_{v+1} - P_v)/\varphi \quad \text{und} \quad q = \hat{q} + wP_v/\varphi,$$

so erhalten wir (8), weil $P_{v+1}s_v - P_v s_{v+1} = a_1$ ist (siehe dazu [5, S. 175]).

Für

$$L_{k+1} = x_{k+1}a_2 + y_{k+1}a_3 + (k+1)a$$

finden wir deshalb

$$x_{k+1} = x_k - \alpha + ps_v + q(s_v - s_{v+1}), \quad y_{k+1} = y_k - pP_v + q(P_{v+1} - P_v).$$

Wäre $q \leqq 0$, so wäre

$$p \geqq \langle (\alpha - x_k)/s_v \rangle = F^{(l)}_{\varepsilon+1} - F^{(l)}_{\varepsilon},$$

weil $x_k = x_l - \varepsilon\alpha + F^{(l)}_{\varepsilon} s_v$ und damit

$$y_{k+1} \leqq y_k - pP_v = y_l - F^{(l)}_{\varepsilon} P_v - pP_v \leqq y_l - F^{(l)}_{\varepsilon+1} P_v < 0,$$

welches unmöglich ist. Also ist $q \geqq 1$.

Wäre $p < 0$, so ergäbe $q \geqq 1$, daß $y_{k+1} \geqq y_k + P_{v+1}$, was auch unmöglich ist. Also ist $p \geqq 0$.

Im Falle

$$0 \leqq x_{k+1} = x_k - \alpha + ps_v + q(s_v - s_{v+1}) < s_v - s_{v+1}$$

(welches für $p = 0$ der Fall ist, weil dann $y_{k+1} \geqq P_{v+1} - P_v$), ist

$$L_{k+1} - L_k = (pR_v + q(R_v - R_{v+1}) - R)a_1 \geqq (R_v - R)a_1 \geqq 0,$$

wegen $p \geqq 0$, $q > 0$, $R_{v+1} \leqq 0$ und (i)′ für $d = 1$, weil $F_1 = 1$ ist. Mit der Induktionsannahme bekommen wir dann $L_{k+1} \geqq L_k > g(A_3)$. Hier ist dann

$$\begin{aligned} -Za_1 = g(A_3) + a_1 - L_{k+1} = (s_v - s_{v+1} - 1 - x_{k+1})a_2 + \\ + (P_{v+1} - 1 - y_{k+1})a_3 - (k+1)a, \end{aligned}$$

also $(k+1)a = Va_2 + Wa_3 + Za_1$, $V, W, Z \in \mathbb{N}_0$. Damit lohnt sich die Verwendung von $k+1$ oder mehr a bei einer eventuellen Darstellung der Restklasse von $g(A_3)$ modulo a_1 nicht und wir sind fertig.

Von nun ab können wir uns auf den Fall $p \geqq 1$, $q \geqq 1$, $x_{k+1} \geqq s_v - s_{v+1}$ (und damit $y_{k+1} < P_{v+1} - P_v$) beschränken. Dann ist

$$L_{k+1} - L_k = \big(pR_v + q(R_v - R_{v+1}) - R\big)a_1 \geqq R_v a_1.$$

Wir zeigen nun $L_d > g(A_3)$ für $k+1 \leqq d = k+1+e \leqq k+1+E = K$ mit

$$E = \max\{e \in \mathbb{Z} \mid y_{k+1} \geqq F_e^{(k+1)} P_v\} \geqq 0,$$

womit wieder die Ausgangssituation hergestellt ist, jetzt aber für $K > k$. Setzen wir $F_e^{(k+1)} = G_e$, so gilt wie früher für $0 \leqq e \leqq E$:

$$L_d = L_{k+1+e} = (x_{k+1} - e\alpha + G_e s_v)a_2 + (y_{k+1} - G_e P_v)a_3 + (k+1+e)a.$$

Hier ist

$$\begin{aligned} L_d - L_k &= L_{k+1+e} - L_{k+1} + L_{k+1} - L_k \geqq (G_e R_v - eR)a_1 + R_v a_1 \\ &= \big((G_e+1)R_v - eR\big)a_1 \geqq (F_e R_v - eR)a_1 \geqq 0, \end{aligned}$$

weil

$$G_e + 1 = \left\langle \frac{e\alpha - x_{k+1} + s_v}{s_v} \right\rangle \geqq \left\langle \frac{e\alpha - (s_v - s_{v+1} - 1)}{s_v} \right\rangle = F_e,$$

$$\begin{aligned} 0 \leqq e \leqq E &= \max\{e \in \mathbb{Z} \mid y_{k+1} \geqq G_e P_v\} \\ &\leqq \max\{e \in \mathbb{Z} \mid P_{v+1} - P_v - 1 \geqq G_e P_v\} \\ &= \max\{e \in \mathbb{Z} \mid P_{v+1} - 1 \geqq (G_e+1)P_v\} \\ &\leqq \max\{e \in \mathbb{Z} \mid P_{v+1} - 1 \geqq F_e P_v\} = D. \end{aligned}$$

Setzt man $H_c = [(cs_v - s_{v+1} - 1)/\alpha]$ und $C = q_{v+1} - 1$, so können wir schreiben

$$[1, D] = \bigcup_{c \in [1, C]} I_c, \quad I_c = [H_c + 1, H_{c+1}].$$

Nun ist $F_d = c$ für $d \in I_c$. Dies gibt

$$\min_{d \in [1,D]} \frac{F_d}{d} = \min_{c \in [1,C]} \left\{ \min_{d \in I_c} \frac{F_d}{d} \right\} = \min_{c \in [1,C]} \frac{c}{H_{c+1}}.$$

Die letzte Bedingung in (i)′ bekommt dann die Form

$$\frac{R}{R_v} \leqq \min_{d \in [1,D]} \frac{F_d}{d} = \min_{c \in [1,C]} \frac{c}{H_{c+1}} \Leftrightarrow cR_v \geqq RH_{c+1}, \quad c \in [1, C].$$

Gewöhnlicherweise reduziert sich dann die Anzahl D der Bedingungen in (i)'. Damit ist jetzt auch Satz 2 aus [2] bewiesen.

Ein Beispiel soll Satz 2 erläutern helfen. Sei $t \geqq 2$, $a_1 = 3t-1$, $a_2 = 3t$, $a_3 = 3t+2$ und $a = 3t+1$, dann ist $s_0 = 3$, $q_1 = t$, $s_1 = 1$, $P_0 = 1$, $P_1 = t$, $v = 0$ und $g(A_3) = 3t^2 - t - 1$, $\alpha = 2$, $\beta = 0$, $R = 1$, $R_v = R_0 = 2$. Nun ist

$$\left[\frac{(c+1)s_v - s_{v+1} - 1}{\alpha}\right] R = \left[\frac{3c+1}{2}\right] \leqq 2c = cR_v, \quad 1 \leqq c \leqq C = t-1.$$

Hier ist also (i) aus Satz 2 erfüllt und es muß gelten $g(A_3) = g(A_4)$. Gleichzeitig zeigt das Beispiel auch, daß die Anzahl C der Bedingungen in (i) beliebig groß werden kann. Hier kann $g(A_4)$ auch auf andere Art berechnet werden, da A_4 eine arithmetische Folge bildet. Verwendet man die Formel für diese Folgen aus Selmer [7, S. 6], so ergibt sich genau $g(A_4) = 3t^2 - t - 1 = g(A_3)$, und Satz 2 ist in diesem Falle bestätigt.

Verwendet man statt des Restsystems $T(a_1)$ jetzt $T(a_2)$, das minimale Restsystem modulo a_2, welches mit $T(a_1)$ stark verwandt ist, so kann man mit genau der gleichen Argumentation wie oben auch den Fall $P_v a_3 < s_{v+1} a_2$ behandeln und erhält das folgende Resultat:

Zunächst bestimmen wir γ, δ und S eindeutig mit

$$a = \gamma a_1 + \delta a_3 - S a_2$$
$$(0 \leqq \gamma < R_v \wedge 0 \leqq \delta < P_{v+1}) \vee (R_v \leqq \gamma < R_v - R_{v+1} \wedge 0 \leqq \delta < P_v).$$

D.h. $\gamma a_1 + \delta a_3 \in T(a_2)$, vergleiche dazu Metternich [3, S. 48].

SATZ 3. *Sei $A_4 = A_3 \cup \{a\}$, a unabhängig von A_3 und $1 < a < a_3$. Gilt zusätzlich $P_v a_3 < s_{v+1} a_2$, dann sind die folgenden beiden Aussagen äquivalent:*

(i) $\gamma \geqq R_v$, $\delta = 0$;

$$c(s_v - s_{v+1}) \geqq \left[\frac{(c+1)(R_v - R_{v+1}) + R_{v+1} - 1}{\gamma}\right] S,$$

$$1 \leqq c \leqq \left[\frac{P_{v+1} - 1}{P_{v+1} - P_v}\right].$$

(ii) $g(A_3) = g(A_4)$.

Details findet man in Kirfel [1, S. 61–64].

Anwendung auf das Reichweitenproblem. Es zeigt sich, daß die bisherigen Resultate über Basiserweiterung bei konstanter Frobeniuszahl sich auf das sogenannte Reichweitenproblem, siehe Selmer [8], [9] und [10], übertragen lassen.

Sei $B_k = \{b_1 = 1 < b_2 < \ldots < b_k\}$ eine Basis. Wir betrachten die kleinste Zahl N, die sich nicht unter Verwendung von höchstens h Summanden aus der Basis B_k darstellen läßt. $N-1$ nennen wir die *h-Reichweite* $n_h(B_k)$ von B_k. Der folgende Zusammenhang zwischen Frobenius- und Reichweitenproblem, der für genügend große h gilt, wurde von Meures [4] entdeckt:

$$n_h(B_k) + 1 = hb_k - g(\bar{B}_k). \tag{9}$$

Dabei ist

$$\bar{B}_k = A_k = \{a_k = b_k - b_{k-1}, \ldots, a_2 = b_k - b_1,\ a_1 = b_k\}$$

die sogenannte *Spiegelbasis* von B_k. Rödseth [6] zeigt, daß (9) im Falle $k = 3$ bereits für $h \geqq h_0 = b_2 + [b_3/b_2] - 2$ gültig ist.

Wir erweitern nun die Basis B_3 mit $b \neq b_2$, $1 < b < b_3$ zu $B_4 = B_3 \cup \{b\}$ und setzen $a = b_3 - b$, $A_3 = \bar{B}_3$ und $A_4 = A_3 \cup \{a\}$. Im vorliegenden Fall ist die Größenordnung der Basiselemente

$$a_3 = b_3 - b_2 < a_2 = a_1 - 1 < a_1, \quad 1 < a = b_3 - b < a_2,$$

d.h. anders als in den bisherigen Untersuchungen. Jedoch können so gut wie alle Argumente übernommen werden, zumal die Bedingung $a_1 = \min A_3$ aus [2] nur bei der Untersuchung der abhängigen Basiserweiterungen eine Rolle spielt.

$n_h(B_3) < n_h(B_4)$ ist gleichbedeutend damit, daß $n_h(B_3) + 1$ mit höchstens h Summanden aus B_4 darstellbar ist, also mit (9) für $h = h_0$:

$$h_0 b_3 - g(\bar{B}_3) = n_{h_0}(B_3) + 1 = z_1 b_1 + z_2 b_2 + z_3 b_3 + z_4 b, \quad \sum z_i \leqq h_0$$
$$g(\bar{B}_3) = g(A_3) = (h_0 - z_1 - z_2 - z_3 - z_4)a_1 + z_1 a_2 + z_2 a_3 + z_4 a.$$

Dies bedeutet, daß $g(A_3)$ mit höchstens h_0 Summanden aus A_4 darstellbar ist. Andererseits sieht man leicht (vergleiche Selmer [10, Kap. 16]), daß

$$g(A_3) = g(A_4) \Rightarrow n_h(B_3) = n_h(B_4), \quad h \geqq h_0. \tag{10}$$

Im weiteren soll nun das Erweiterungsproblem

$$n_h(B_3) = n_h(B_4) \tag{11}$$

untersucht werden. Wir können uns dabei, wie Selmer zeigt, auf den Fall $h = h_0$ beschränken.

Wir benutzen die aus dem bisherigen bekannten Formeln und Resultate für das Frobeniusproblem. Hier gilt auch

$$1 < a = \alpha a_2 + \beta a_3 - R a_1 < (\alpha + \beta - R) a_1 \quad \text{und damit} \quad R < \alpha + \beta.$$

Für $R = 0$ ist $a = \beta a_3$ und wegen der Abhängigkeit von a ist natürlich $g(A_3) = g(A_4)$, also wegen (10)

$$n_h(1, b_2, b_3) = n_h(1, b_2, b_3 - \beta(b_3 - b_2), b_3), \quad h \geqq h_0,\ 1 < \beta < \frac{b_3 - 1}{b_3 - b_2},$$

siehe dazu auch Selmer [10, (16.8)]. Von nun ab sei $R > 0$.

Im weiteren Verlauf werden wir beim Abzählen der Summanden in den eventuellen Darstellungen von $g(A_3)$ immer wieder von einer Formel Gebrauch machen, die wir hier entwickeln wollen. Dabei greifen wir auf Rödseth [6, S. 175 ff] zurück. Er geht dort von den Algorithmusgrößen $s_{-1} = b_3,\ s_0 = b_2$ aus. Wie man leicht sieht, entspricht dies genau dem euklidischen Divisionsalgorithmus aus [2], ausgehend von a_1, a_2 und a_3 (wobei jetzt $d = (a_1, a_2) = 1$). Wir können deshalb die früheren Größen s_i, P_i, R_i und v übernehmen und bestimmen auch Q_i folgendermaßen:

$$Q_{-1} = -1,\ \ Q_0 = 0,\ \ Q_{i+1} = q_{i+1} Q_i - Q_{i-1} > 0,\ \ i = 0, \ldots, m.$$

In Lemma 5 findet Rödseth für $v > 0$ und alle (x_v, y_v) mit

$$\begin{aligned}&(0 \leqq x_v < s_v - s_{v+1} \wedge 0 \leqq y_v < P_{v+1})\\ &\quad \vee (s_v - s_{v+1} \leqq x_v < s_v \wedge 0 \leqq y_v < P_{v+1} - P_v),\end{aligned}$$

daß

(12) $$x_{v-1} + y_{v-1} + Q_v - 1 \leqq h_0, \quad \text{falls } P_v \leqq s_v$$

(13) $$x_v + y_v + R_v - 1 \leqq h_0, \quad \text{falls } P_v > s_v.$$

Er zeigt auch

$$x_{v-1} = x_v + [y_v/P_v] s_v,\ y_{v-1} = y_v - [y_v/P_v] P_v.$$

Das gibt uns in (12):

(14) $$x_v + y_v + [y_v/P_v]\,(s_v - P_v) + Q_v - 1 \leqq h_0, \quad \text{falls } P_v \leqq s_v.$$

In jedem Fall ist jedoch

(15)
$$\max\{x_v + y_v\} = \max\{s_v - s_{v+1} + P_{v+1} - 2,\ s_v + P_{v+1} - P_v - 2\} \leqq h_0,$$

weil $R_v > 0$ und für $v > 0$ auch $Q_v > 0$. Allgemein können wir $v > 0$ voraussetzen, denn für $v = 0$ ist B_3 „*angenehm*" (Selmer [8, S. 46]), und dann ist immer (11) unmöglich (Selmer [10, Kap. 16]).

Wir nennen $\lambda(n)$ die minimale Anzahl an Summanden in einer eventuellen Darstellung von $n \in \mathbb{N}_0$ mit A_4, also

$$\lambda(n) = \min\{u_1+u_2+u_3+u_4 \mid n = u_1a_1+u_2a_2+u_3a_3+u_4a,\ u_i \geqq 0\}.$$

Wir zeigen nun, daß in den meisten Fällen $\lambda(g(A_3)) \leqq h_0$ gilt, daß also $g(A_3)$ mit höchstens h_0 Summanden aus A_4 darstellbar ist, welches wiederum $n_h(B_3) < n_h(B_4)$ bewirkt.

A) $P_v a_3 \geqq s_{v+1} a_2$.

1) $\alpha < s_v - s_{v+1}$. Wegen II. 1) in [2] und $R < \alpha + \beta$ ist jetzt nach (15):

$$\lambda(g(A_3)) \leqq (s_v - s_{v+1} + P_{v+1} - 2) + (R - \alpha - \beta) < h_0,$$

und (11) ist unmöglich.

2) $\alpha \geqq s_v - s_{v+1}$. Sei zunächst $\beta > 0$. Aus $\beta a_3 a_1 = \beta a_3 a_2 + \beta a_3 \equiv 0 \pmod{a_1}$ folgt $\beta a_3 \geqq s_v > \alpha$, weil sonst die Restklasse 0 zweimal im Restsystem $T(a_1)$ vertreten wäre. Wegen $a \equiv \beta a_3 - \alpha \pmod{a_1}$, $\beta a_3 > \alpha$ und $a < a_1$ ergibt sich $a < \beta a_3$. Für $\alpha > s_v - s_{v+1}$ oder $\beta > 0$ folgt dann aus II. 2) in [2] und $a < a_2$, daß

$$\lambda(g(A_3)) \leqq (s_v - s_{v+1} + P_{v+1} - 2) + (R - \alpha - \beta) + (s_v - P_v - R_v) < h_0,$$

wegen $s_v - P_v - R_v = -Q_v$ (Rödseth [6, S. 176]).

Sei nun $\alpha = s_v - s_{v+1} > 1$ und $\beta = 0$. Aus II. 2) in [2] und $a < a_2$ folgt

$$\lambda(g(A_3)) \leqq (s_v - s_{v+1} + P_{v+1} - 2) + 2(R - \alpha - \beta) + (s_v - P_v - R_v) + 1 < h_0.$$

Für $\alpha = s_v - s_{v+1} = 1$ und $\beta = 0$ ist $0 < a \equiv a_2 \pmod{a_1}$ ein Widerspruch zu $a < a_2 < a_1$.

Alles in allem ist (11) unmöglich im Falle $P_v a_3 \geqq s_{v+1} a_2$.

B) $P_v a_3 < s_v a_2$.

1) $\beta < P_{v+1} - P_v$. Wegen I. 1) in [2] ist jetzt nach (15):

$$\lambda(g(A_3)) \leqq (s_v + P_{v+1} - P_v - 2) + (R - \alpha - \beta) < h_0.$$

2) $\beta \geqq P_{v+1} - P_v$. Sei zunächst $R + R_{v+1} > 0$. Aus I. 2) in [2] folgt dann

$$\lambda(g(A_3)) \leqq s_v - s_{v+1} - \alpha + 2P_{v+1} - P_v - \beta + R + R_{v+1} - 2.$$

Jetzt kann uns aber (15) nicht mehr weiterhelfen, und wir benötigen eine neue Abschätzung. Natürlich gilt

$$\begin{aligned} &(s_v - s_{v+1} - \alpha)a_2 + (\beta - (P_{v+1} - P_v))(a_1 - a_3) > 0 \\ \Rightarrow\ &(R_v - R_{v+1})a_1 + (\beta - (P_{v+1} - P_v))a_1 > \alpha a_2 + \beta a_3 > Ra_1 \\ \Rightarrow\ &R_v - R_{v+1} + \beta - P_{v+1} + P_v \geqq R + 1. \end{aligned}$$

Weil $\alpha \geqq 0$, erhalten wir damit, falls $P_v > s_v$:

$$\lambda(g(A_3)) \leqq (s_v - s_{v+1} - 1) + (P_{v+1} - 1) + (R_v - 1) \leqq h_0$$

nach (13). Im Falle $P_v \leqq s_v$ ist wegen $R_v = s_v - P_v + Q_v$:

$$\lambda(g(A_3)) \leqq (s_v - s_{v+1} - 1) + (P_{v+1} - 1) + (s_v - P_v) + (Q_v - 1) \leqq h_0$$

nach (14), wo jetzt $[y_v/P_v] = [(P_{v+1} - 1)/P_v] \geqq 1$.

Sei nun $R + R_{v+1} \leqq 0$, d.h. $\alpha = 0$ nach (6). Aus $P_v a_3 < s_{v+1} a_2$ folgt dann

$$\begin{aligned} -R_{v+1} a_1 &= P_{v+1} a_3 - s_{v+1} a_2 < (P_{v+1} - P_v) a_3 \\ &\leqq \beta a_3 = R a_1 + a < (R+1) a_1, \end{aligned}$$

also $0 \leqq R + R_{v+1}$ und somit insgesamt $R + R_{v+1} = 0$. Jetzt ist

$$g(A_3) = (s_v - s_{v+1} - 1) a_2 + (2P_{v+1} - P_v - 1 - 2\beta) a_3 + (R-1) a_1 + 2a.$$

Falls $2P_{v+1} - P_v > 2\beta$ ergibt dies mit (15):

$$\begin{aligned} \lambda(g(A_3)) &\leqq (s_v - s_{v+1} + P_{v+1} - 2) + (P_{v+1} - P_v - \beta) + \\ &\quad + (R - \alpha - \beta + 1) \leqq h_0. \end{aligned}$$

Sei nun $2P_{v+1} - P_v \leqq 2\beta$, also

$$\begin{aligned} 2s_{v+1} a_2 &= 2R_{v+1} a_1 + 2P_{v+1} a_3 \leqq -2R a_1 + 2\beta a_3 + P_v a_3 \\ &= 2a + P_v a_3 < 2a + s_{v+1} a_2, \end{aligned}$$

und deshalb $s_{v+1} = 1$. Damit ergibt $a = a_2 - (P_{v+1} - \beta) a_3$, daß

$$g(A_3) = (s_v - i) a_2 + \big(i(P_{v+1} - \beta) - P_v - 1\big) a_3 + (R-1) a_1 + ia.$$

Falls $s_v \geqq (P_v + 1)/(P_{v+1} - \beta)$, so ist $g(A_3)$ darstellbar mit

$$i = \langle (P_v + 1)/(P_{v+1} - \beta) \rangle$$

und

$$\begin{aligned} \lambda(g(A_3)) &\leqq (s_v - i) + (P_{v+1} - \beta - 1) + (R-1) + i \\ &= (s_v - s_{v+1} + P_{v+1} - 2) + (R - \alpha - \beta + 1) \leqq h_0. \end{aligned}$$

Abschließend betrachten wir den Fall $P_v a_3 < s_{v+1} a_2$ mit

$$\alpha = 0, \quad \beta \geqq P_{v+1} - P_v, \quad R_{v+1} + R = 0, \quad s_{v+1} = 1, \quad s_v < \frac{P_v - 1}{P_{v+1} - \beta}.$$

Hier ist dann

$$a = a_2 - (P_{v+1} - \beta)a_3,\ P_v a_3 \geqq s_v(P_{v+1} - \beta)a_3 = s_v(a_2 - a),$$
$$\text{also } s_v a \geqq R_v a_1.$$

Um diesen letzten Fall erschöpfend zu behandeln, benötigen wir das minimale Restsystem $T(a_3)$ modulo a_3:

$$T(a_3) = \{xa_2 + ya_1 \mid 0 \leqq x < s_{v+1},\ 0 \leqq y < R_v - R_{v+1}\} \cup$$
$$\cup \{xa_2 + ya_1 \mid s_{v+1} \leqq x < s_v,\ 0 \leqq y < -R_{v+1}\},$$

mit $|T(a_3)| = a_3$. Dies ist in Metternich [3, S. 50] gezeigt, folgt aber auch leicht aus denselben Argumenten, die Rödseth [5] für die Bestimmung von $T(a_1)$ entwickelt.

Setzen wir $a_3 = a_1'$, $a_2 = a_2'$, $a_1 = a_3'$, so gilt wie in [2] $a_1' < a_2' < a_3'$. Führt man wie dort den Divisionsalgorithmus durch und versieht man die dabei erhaltenen Größen P_i, s_i, m und R_i mit einem Strich und bestimmt man $-1 \leqq v' \leqq m'$ nach der Ungleichung $R'_{v'+1} \leqq 0 < R'_{v'}$, so finden wir eine andere Darstellung des Minimalsystems $T(a_3)$. Nun ist dieses aber eindeutig bestimmt, weil $(a_1, a_2) = 1$. Ein Vergleich von $T(a_3)$ und $T(a_1')$ zeigt, daß

$$s_{v+1} = s'_{v'} - s'_{v'+1},\ R_v - R_{v+1} = P'_{v'+1},\ s_v = s'_{v'},\ -R_{v+1} = P'_{v'+1} - P'_{v'}.$$

Daraus folgt

$$s_{v+1} = s'_{v'} - s'_{v'+1} = 1$$
$$a = a_2 - (P_{v+1} - \beta)a_3 \equiv a_2' \pmod{a_1'}$$
$$s'_{v'} a = s_v a \geqq R_v a_1 = P'_{v'} a_3 > (s_v - s_{v+1})a_2 = s'_{v'+1} a_2'.$$

Die letzte Ungleichung gilt wegen $R_v a_1 = s_v a_2 - P_v a_3 > (s_v - s_{v+1})a_2$. Satz 1 aus [2] besagt dann, daß $g(A_3) = g(A_4)$, und aus (10) folgt (11) für $h \geqq h_0$.

B_4 soll in diesem Spezialfall bestimmt werden. Aus $v > 0$ folgt $P_v \geqq 2$, daher $a_2 = s_{v+1} a_2 > P_v a_3 \geqq 2a_3$, also $b_3 < 2b_2$. Damit können wir setzen

$$b_3 = b_2 + r,\ 0 < r < b_2;\ \ b_2 = \tau r + \rho + 1,\ 0 \leqq \rho < r,$$
$$b = b_3 - a = a_1 - a_2 + (P_{v+1} - \beta)a_3 = 1 + tr \quad \text{mit } t = P_{v+1} - \beta.$$

Selmer [8, S. 53–54] hat für diesen Fall die Reichweite $n_{h_0}(B_3)$ berechnet und auch die Algorithmusgrößen bestimmt:

$$P_i = i + 1,\ \ Q_i = i,\ \ s_i = (\tau - i)r + \rho + 1,\ \ R_i = (\tau - i)r + \rho$$

für $0 \leqq i \leqq \tau$, also $R_\tau = \rho \geqq 0$. Wegen $-R_{v+1} = R > 0$ ist der Fall $R_\tau = 0$ ausgeschloßen.

Also ist $v \geqq \tau$. Wegen

$$P_v a_3 = P_v r < s_{v+1} a_2 = a_2 = (\tau+1)r + \rho < (P_\tau + 1)r$$

ist $P_v < P_\tau + 1$ und $v < \tau + 1$, also $v = \tau$. Schließlich ist (siehe Selmer)

$$1 = s_{v+1} = s_{\tau+1} = q_{\tau+1}(\rho+1) - (r+\rho+1) \Rightarrow r \equiv -1 \pmod{\rho+1}$$

$$s_v a \geqq R_v a_1 \Leftrightarrow a \geqq \frac{\rho a_1}{\rho+1} \Leftrightarrow b = b_3 - a \leqq \frac{r(\tau+1)}{\rho+1} + 1$$

$$\Leftrightarrow 0 < t \leqq \left[\frac{\tau+1}{\rho+1}\right].$$

Das gesamte Ergebnis möchten wir nun in einem Satz zusammenfassen.

SATZ 4. *Sei* $B_4 = B_3 \cup \{b\}$, $b_1 = 1 < b_2 < b_3$, $b \neq b_2$, $1 < b < b_3$. *Dann gibt es genau zwei Fälle mit* $n_{h_0}(B_3) = n_{h_0}(B_4)$, *nämlich:*

1) $B_3 = \{1, b_2, b_3\}$, $b = b_3 - \beta(b_3 - b_2)$, $1 < \beta < \dfrac{b_3 - 1}{b_3 - b_2}$.

2) $B_3 = \{1, b_2 = \tau r + \rho + 1,\ b_3 = (\tau+1)r + \rho + 1\}$,
$0 < r < b_2$, $0 < \rho < r - 1$,

$$b = tr + 1,\ 0 < t \leqq \left[\frac{\tau+1}{\rho+1}\right],\ r \equiv -1 \pmod{\rho+1}.$$

BEMERKUNG. $\rho = r - 1$ ergäbe einen Widerspruch zu $r \equiv -1 \pmod{\rho+1}$ und kann deshalb ausgeschloßen werden.

Im zweiten Fall gilt nach Selmer [8, S. 53]:

$$n_{h_0}(B_3) = n_{h_0}(B_4) = (h_0 + r)(h_0 + 2 - \rho) - r - (h_0 + r - \rho)\left(\frac{r+1}{\rho+1} - 1\right).$$

Satz 4 entspricht Theorem 16.1 und 16.2 in Selmer [10].

Professor E. S. Selmer möchte ich für seine Hilfe bei der Ausarbeitung und seine gründliche Durchsicht des Artikels hier wärmstens danken.

LITERATURHINWEISE

1. C. Kirfel, *Erweiterung dreielementiger Basen bei konstanter Frobeniuszahl und Reichweite*, Hovedoppgave, Math. Inst., Univ. Bergen, 1982.
2. C. Kirfel, *Erweiterung dreielementiger Basen bei konstanter Frobeniuszahl*, Math. Scand. 54 (1984), 310–316.

3. H. Metternich, *Über ein Problem von Frobenius. Basiserweiterung bei konstanter Frobeniuszahl*, Diplomarbeit Math., Johannes Gutenberg-Univ., Mainz, 1981.
4. G. Meures, *Zusammenhang zwischen Reichweite und Frobeniuszahl*, Staatsexamensarbeit, Johannes Gutenberg-Univ., Mainz, 1977.
5. Ö. J. Rödseth, *On a linear diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171–178.
6. Ö. J. Rödseth, *On h-bases for n*, Math. Scand. 48 (1981), 165–183.
7. E. S. Selmer, *On the linear diophantine problem of Frobenius*, J. Reine Angew. Math. 293/294 (1977), 1–17.
8. E. S. Selmer, *On the postage stamp problem with three stamp denominations*, Math. Scand. 47 (1980), 29–71.
9. E. S. Selmer und A. Rödne, *On the postage stamp problem with three stamp denominations*, II, Math. Scand. 53 (1983), 145–156.
10. E. S. Selmer, *On the postage stamp problem with three stamp denominations*, III, Math. Scand. 56 (1985), 105–116.

MATHEMATISCHES INSTITUT
UNIVERSITÄT BERGEN
N-5000 BERGEN
NORWEGEN