

## REKURSIONEN UND DAS JOSEPHUS-PROBLEM

MANUEL AMANN

*Rekursionen* begegnen uns sehr häufig in der Mathematik. Angefangen von dem Trivialbeispiel

$$\begin{aligned}f(0) &= a \\f(n) &= f(n-1) + b\end{aligned}$$

für  $n \geq 1$  und mit  $a, b \in \mathbb{R}$ , bis hin zu den berühmten Fibonacci-Zahlen

$$\begin{aligned}\text{fib}(0) &= 0 \\ \text{fib}(1) &= 1 \\ \text{fib}(n) &= \text{fib}(n-1) + \text{fib}(n-2)\end{aligned}$$

für  $n \geq 2$ .

Wir sehen, dass die Folgen nicht *geschlossen*, d.h. mittels der Variable  $n$  definiert sind, sondern auf vorherige Folgenwerte „zurückgreifen“.

Ziel ist es oft, eine geschlossene Darstellung der Folge zu finden. Hat man eine solche Form potentiell ermittelt, beweist man ihre Richtigkeit in der Regel mittels vollständiger Induktion. Im ersten Fall ist das schnell getan, wir ermitteln  $f(n) = n \cdot b + a$ .

In der Tat, der Induktionsanfang ist  $f(0) = a$ ; wir nehmen also an, unsere geschlossene Form ist korrekt bis zu einem festen  $n-1$ . Wir zeigen, dass sie dann auch für  $n$  korrekt ist. Es gilt aus der Rekursion, dass  $f(n) = f(n-1) + b$ . Mit der Induktionsannahme folgt  $f(n) = ((n-1) \cdot b + a) + b = n \cdot b + a$ . Das ist unsere geschlossene Form für  $f(n)$ .

Im Falle der Fibonacci-Folge geht man gleichermaßen vor. Hier ist die geschlossene Form allerdings ein wenig komplizierter:

$$\text{fib}(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)$$

Rekursionen ergeben sich nicht selten direkt aus konkreten Problemstellungen. Die Fibonacci-Folge läßt sich mit dem Wachstum einer Kaninchenpopulation motivieren: Die Funktion  $f$  stellt die Zahl der Kaninchenpaare im Monat  $n$  dar. Zum Zeitpunkt 1, d.h. im ersten Monat existiert ein (trächtiges) Kaninchenpaar, das im zweiten Monat und dann in jedem darauffolgenden Monat ein neues Kaninchenpaar wirft. Jedes neue Kaninchenpaar wirft ab dem zweiten Monat jeweils monatlich ein neues Kaninchenpaar.

Das heißt, die Population im Monat  $n$  ist die bestehende aus dem Monat  $n-1$ , wobei zusätzlich zu jedem Paar aus dem Monat  $n-2$  ein weiteres hinzukommt, was den Summanden  $\text{fib}(n-2)$  erklärt.

Die geschlossene Form erlaubt es uns nun nicht nur, effektiv den Bestand im  $10^{23}$ -ten Monat zu berechnen, sondern sogar direkte Rückschlüsse auf

---

*Date:* 22. Oktober 2012.

PROSEMINAR „EULERS TRICKKISTE“

die Geschwindigkeit des Wachstums zu ziehen: Wie üblich bei ungestört wachsenden Populationen, ist das Wachstum exponentiell!

Wir wollen im folgenden eine weitere Klasse von Rekursionen betrachten und folgen dabei Kapitel [1, 1.3].

### DAS JOSEPHUS-PROBLEM

Wir stellen wieder ein klassisches Problem vor, das uns auf die zu betrachtenden Rekursionen führen wird:

Flavius Josephus, bekannter jüdischer Historiker – der insbesondere eine der wenigen Quellen zum Leben Jesu liefert – soll im römisch-jüdischen Krieg mit 41 Kameraden den Selbstmord der Gefangenschaft vorgezogen haben. Dazu stellten sie sich in einem Kreis auf; nacheinander sollte sich jeder dritte in der Reihe umbringen – bis schließlich niemand übrig blieb. Davon nicht begeistert, fand Josephus heraus, an welche Position im Kreis er sich stellen mußte, um als letzter übrig zu bleiben, also überleben zu können.

Das Problem ist also das folgende: Es stehen  $n$  (z.B.  $n = 10$ ) Personen in einem Kreis. Wir eliminieren der Einfachheit halber jeden zweiten. Nacheinander sterben also die Personen Nummer 2, 4, 6, 8, 10 (in unserem Beispiel mit  $n = 10$ ) und weiter 3, 7, 1, 9. Nummer 5 bleibt übrig. Offensichtlich definiert uns dieses Verfahren eine Funktion  $J(n)$ , wobei  $J(n)$  die Nummer der Person ist, die überlebt. Einfaches Durchprobieren ergibt also die folgende Tabelle:

$n$	1	2	3	4	5	6
$J(n)$	1	1	3	1	3	5

Die erste Beobachtung, die wir anstellen, ist, dass alle Zahlen  $J(n)$  gerade sind. Das ist trivialerweise so, da wir in der ersten Runde, im ersten Durchlauf des Kreises alle gerade Zahlen eliminieren.

Unser Ziel ist es natürlich, eine Rekursionsgleichung für die Funktion  $J(n)$  zu finden.

**Satz.** *Es gilt:*

$$J(2n) = 2J(n) - 1 \quad \text{und} \quad J(2n + 1) = 2J(n) + 1$$

für  $n \geq 1$ .

**BEWEIS.** Wir beginnen mit  $2n$  vielen Leuten. Nach der ersten Runde stehen die Nummern 1, 3, 5, 7,  $\dots$ ,  $2n - 3$ ,  $2n - 1$  noch im Kreis. Die Nummer 3 eröffnet die nächste Runde. Bis auf Umbenennen ist Runde zwei damit aber gleichzusetzen mit Runde 1 des Problems für  $n$  Personen. Das heißt, wir benennen Nummer  $i$  in Nummer  $(i + 1)/2$  um – 3 wird zu 2, 5 wird zu 3 usw. – und starten das Problem für  $n$ . Das ändert natürlich nichts daran, wer am Ende übrig bleibt. Umgekehrt, um von der Benennung in Runde zwei auf die in Runde eins zu kommen, verwenden wir  $i \mapsto 2i - 1$ . In anderen Worten  $J(2n) = 2J(n) - 1$ .

Für den ungeraden Fall von  $2n + 1$  Personen argumentieren wir ähnlich: Hier wird Nummer eins nach Nummer  $2n + 1$  ausgelöscht und die zweite Runde lautet 3, 5, 7, 9,  $\dots$ ,  $2n - 1$ ,  $2n + 1$  – wir beginnen also wieder mit Nummer 3. Das entspricht dem Problem in  $n$  Personen, wenn wir, um von Runde zwei auf die Benennung in Runde eins zu schließen, die Umbenennung

$i \mapsto 2i + 1$  – also z.B.  $1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 7, \dots$  – anwenden. Also ergibt sich  $J(2n + 1) = 2J(n) + 1$ .  $\square$

Wir haben also nicht eine, sondern zwei Rekursionen – je nachdem ob  $n$  gerade oder ungerade ist – gefunden, die  $J(n)$  nun aber vollständig beschreiben.

$$(1) \quad \begin{aligned} J(1) &= 1 \\ J(2n) &= 2J(n) - 1 \\ J(2n + 1) &= 2J(n) + 1 \end{aligned}$$

für  $n \geq 1$ .

Eine Beispielrechnung für  $n = 10$ : Wir wenden zuerst die Rekursion für gerade Zahlen an, d.h.  $J(10) = J(2 \cdot 5) = 2J(5) - 1$ . Nun die Rekursion für ungerade Zahlen usw., d.h.

$$\begin{aligned} J(10) &= J(2 \cdot 5) \\ &= 2 \cdot J(5) - 1 \\ &= 2 \cdot J(2 \cdot 2 + 1) - 1 \\ &= 2 \cdot (2 \cdot J(2) + 1) - 1 \\ &= 2 \cdot (2 \cdot J(2 \cdot 1) + 1) - 1 \\ &= 2 \cdot (2 \cdot (2 \cdot J(1) - 1) + 1) - 1 \\ &= 2 \cdot (2 \cdot (2 \cdot 1 - 1) + 1) - 1 \\ &= 5 \end{aligned}$$

Man beachte weiterhin, dass die Zahl der Rekursionsschritte logarithmisch (zur Basis 2) in  $n$  ist, da  $J(2n)$  (oder  $J(2n + 1)$ ) via  $J(n)$  berechnet wird, also das Problem auf ein halb so großes reduziert wird. Das Problem kann also jetzt schon effektiv von einem Computer gelöst werden.

Wir können also auf jeden Fall mit nicht zu großem Aufwand die folgende Tabelle berechnen. Das Ziel bleibt weiterhin, eine geschlossene Form zu finden.

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1

Die vertikalen Linien deuten an, dass wir sinnvollerweise die Zahlen in Gruppen der Länge  $2^k$  (mit  $k = 0, 1, 2, \dots$ ) unterteilen. Dann „wiederholt“ sich  $J(n)$  entsprechend.

Der folgende Satz formalisiert das und beschreibt die gewünschte geschlossene Form für jede Zahl  $n \geq 1$ . (Wir beobachten, dass die Einschränkungen an  $l$  es genau erlauben, alle Zahlen zwischen  $2^m$  und  $2^{m+1}$  darzustellen.)

**Satz.** *Es gilt:  $J(2^m + l) = 2l + 1$  für  $m \geq 0$  und  $0 \leq l < 2^m$ .*

**BEWEIS.** Wir beweisen das Resultat mittels Induktion nach  $m$ . Für  $m = 0$  folgt notwendigerweise  $l = 0$  aus unseren Einschränkungen. Wir haben also  $J(2^m + l) = J(1) = 1$ . Das ist der Induktionsanfang.

Im Induktionsschritt unterscheiden wir zwei Fälle, je nachdem, ob  $l$  gerade oder ungerade ist. Gilt  $m > 0$  und  $2^m + l = 2n$ , ist also  $l$  gerade, folgt

$$J(2^m + l) = J(2 \cdot (2^{m-1} + l/2)) = 2 \cdot J(2^{m-1} + l/2) - 1$$

Mit eingesetzter Induktionsannahme folgt

$$\begin{aligned} J(2^m + l) &= J(2 \cdot (2^{m-1} + l/2)) \\ &= 2 \cdot J(2^{m-1} + l/2) - 1 \\ &= 2(2 \cdot l/2 + 1) - 1 \\ &= 2l + 1 \end{aligned}$$

Für den ungeraden Fall gehen wir entweder analog vor oder folgern einfach aus den Gleichungen (1), dass  $J(2n + 1) - J(2n) = 2$ . Das impliziert, dass für ungerades  $l$  folgendes gilt:

$$J(2^m + l) = J(2^m + l - 1) + 2 = (2(l - 1) + 1) + 2 = 2l + 1$$

□

Damit ist unser Ziel erreicht. Wir können ganz einfach nun  $J(n)$  in konkreten Fällen berechnen. Natürlich gilt  $J(2^n) = 1$ ,

$$J(10) = J(8 + 2) = J(2^3 + 2) = 2 \cdot 2 + 1 = 5$$

wie wir oben mühsam errechnet haben. Oder:

$$J(1000) = J(512 + 488) = J(2^9 + 488) = 2 \cdot 488 + 1 = 977$$

#### ALTERNATIVE BESCHREIBUNG UND EIGENSCHAFTEN

Die vorangegangenen Untersuchungen legen es nahe, dass  $J$  eine schöne Beschreibung in Form von binären Operationen besitzen sollte. Wir schreiben dafür unsere Zahlen  $n$  in Binärdarstellung. D.h.

$$n = b_m 2^m + b_{m-1} 2^{m-1} + \dots + b_1 \cdot 2^1 + b_0$$

und in Kurzschreibweise

$$n = (b_m b_{m-1} \dots b_1 b_0)_2$$

mit  $b_i \in \{0, 1\}$ . Beispielsweise gilt  $2 = (10)_2$ ,  $5 = (101)_2$ ,  $10 = (1010)_2$ ,  $17 = (10001)_2$ . Schreiben wir wieder, wie oben,  $n = 2^m + l$ , so ergibt dies folgende Relationen in Binärdarstellung:

$$n = (1b_{m-1}b_{m-2} \dots b_1b_0)_2$$

wobei

$$l = (0b_{m-1}b_{m-2} \dots b_1b_0)_2$$

Damit berechnen wir dann

$$2l = (b_{m-1}b_{m-2} \dots b_1b_00)_2$$

da Multiplikation mit 2 binär schlicht ein Bit-shift nach links ist und weiter

$$2l + 1 = (b_{m-1}b_{m-2} \dots b_1b_01)_2$$

Wir können damit nun aus der geschlossenen Form  $J(n) = J(2^m + l) = 2l + 1$  direkt

$$J(n) = (b_{m-1}b_{m-2} \dots b_1b_01)_2 = (b_{m-1}b_{m-2} \dots b_1b_0b_m)_2$$

schließen, da  $b_m = 1$ —vgl. Darstellung von  $n$ . Alles zusammengenommen bedeutet das schlicht, dass

$$J((b_m b_{m-1} \dots b_1 b_0)_2) = (b_{m-1} \dots b_1 b_0 b_m)_2$$

Wir erhalten also  $J(n)$  aus  $n$  durch Bitrotation!

Wir verstehen damit sogar die Iteration der Funktion  $J$  sehr gut. Man könnte nun versucht sein anzunehmen, eine iterative Anwendung der Funktion  $J$ , sprich, einer solchen Rotation, könne unter Umständen nicht in einem Fixpunkt enden - Rotationen haben ja sozusagen klassischerweise keine Fixpunkte. Jedoch weist das folgende Beispiel den Weg.

Es gilt:

$$\begin{aligned} J^\infty(10) &= J^\infty(J^2(10)) \\ &= J^\infty(J^2((1010)_2)) \\ &= J^\infty(J((0101)_2)) \\ &= J^\infty(J((101)_2)) \\ &= J^\infty((011)_2) \\ &= J^\infty((11)_2) \\ &= (11)_2 \\ &= 3 \end{aligned}$$

Wir machen also folgende Beobachtungen:

- Die Iteration  $(J^k(n))_{k \in \mathbb{N}}$  ist monoton fallend, sprich, da sie nur natürliche Zahlen produziert, hat sie einen Fixpunkt.
- Die Iteration entfernt sukzessive alle Nullen aus der Binärdarstellung, jedoch keine Einsen. Der Fixpunkt  $J^\infty(n)$  ist also genau kodiert durch  $(1111 \dots 1)_2$ , wobei die Zahl der Einsen durch die Funktion

$$\nu(n) = \#\text{Einsen in Binärdarstellung von } n$$

gegeben ist.

Damit gilt für den Fixpunkt der Iteration

**Satz.**  $J^\infty(n) = 2^{\nu(n)} - 1$ .

□

Zur weiteren Illustration wollen wir nun die Situation charakterisieren, wann  $J(n) = n/2$  eintritt. Dazu berechnen wir

$$J(n) = n/2 \iff 2l + 1 = (2^m + l)/2 \iff l = (2^m - 2)/3$$

Das bedeutet also, dass genau dann, wenn  $l = (2^m - 2)/3$  eine ganze Zahl ist, die Zahl  $n = 2^m + l$  eine Lösung der Gleichung  $J(n) = n/2$  ist. Es gilt nun aber, dass  $[2^m] = [2]^m \in \mathbb{Z}/3$  und weiter  $[2]^0 = [1]$ ,  $[2]^1 = [2]$ ,  $[2]^2 = [1]$ ,  $\dots$ . Das heißt, Potenzieren liefert alternierend  $[1]$  und  $[2]$ . Also folgt, dass die Zahl  $2^m - 2$  genau dann durch 3 teilbar ist, wenn  $[2^m] = [2]$ , also  $m$  ungerade ist. Das führt auf folgende Tabelle

$m$	$l$	$n = 2^m + l$	$J(n) = 2l + 1 = n/2$	$n$ in Binärdarstellung
1	0	2	1	$(10)_2$
3	2	10	5	$(1010)_2$
5	10	42	21	$(101010)_2$
7	42	170	85	$(10101010)_2$

Das Muster in der Binärdarstellung erklärt sich folgendermaßen: Die Zahlen sind genau diejenigen, für die die Berechnung des Überlebenden, sprich, der „Linksrotation“ identisch mit dem Rechts-shift, also der Division durch 2, ist.

### VERALLGEMEINERUNGEN

Wir verallgemeinern nun die Rekursionsvorschrift (1), d.h. wir variieren die Koeffizienten in der Form

$$(2) \quad \begin{aligned} f(1) &= \alpha \\ f(2n) &= 2f(n) + \beta \\ f(2n+1) &= 2f(n) + \gamma \end{aligned}$$

für  $n \geq 1$  und  $\alpha, \beta, \gamma \in \mathbb{R}$ . Die ursprünglichen Koeffizienten waren  $\alpha = 1, \beta = -1, \gamma = 1$ . Wieder berechnen wir eine Tabelle mit exemplarischen Werten.

$n$	$f(n)$
1	$\alpha$
2	$2\alpha + \beta$
3	$2\alpha + \gamma$
4	$4\alpha + 3\beta$
5	$4\alpha + 2\beta + \gamma$
6	$4\alpha + \beta + 2\gamma$
7	$4\alpha + 3\gamma$
8	$8\alpha + 7\beta$
9	$8\alpha + 6\beta + \gamma$

Es ist induktiv klar, dass wir eine Darstellung der Form

$$(3) \quad f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma$$

mit Funktionen  $A, B, C$  annehmen können.

Wir raten nun folgende Darstellung:

$$(4) \quad \begin{aligned} A(n) &= 2^m \\ B(n) &= 2^m - 1 - l \\ C(n) &= l \end{aligned}$$

für  $n = 2^m + l$ . Da wir verschiedene Techniken lernen wollen, werden wir diese Form nicht durch Induktion beweisen, sondern wollen uns geschickter anstellen.

Wir müssen also die Parameter-Funktionen  $A, B, C$  bestimmen. Wir wollen dafür verschiedene Spezialfälle betrachten, die uns Rückschlüsse auf die Funktionen zulassen. Wir betrachten dazu zuerst den Fall  $\alpha = 1, \beta = \gamma = 0$ ,

d.h. den Fall für den wir  $f(n) = A(n) = 2^m$  (mit  $n = 2^m + l$ ) geraten haben. Die Vorschrift (2) wird damit zu

$$\begin{aligned} A(1) &= 1 \\ A(2n) &= 2A(n) \\ A(2n+1) &= 2A(n) \end{aligned}$$

für  $n \geq 1$ .

Aus einer Induktion über  $m$  (wobei, wie üblich,  $n = 2^m + l$ ) können wir  $A(n) = A(2^m + l) = 2^m$  folgern. In der Tat gilt  $A(2^0 + 0) = A(1) = 1 = 2^0$ . Der Induktionsschritt (mit Induktionsannahme für festes  $m \geq 1$ ) stellt sich als

$$A(2^{m+1} + l) = A(2 \cdot (2^m + l/2)) = 2A(2^m + l/2) = 2 \cdot 2^m = 2^{m+1}$$

dar und beweist die Aussage. In der Tat müssen wir hier annehmen, dass  $l$  gerade ist. Da aber  $A$  nicht zwischen geraden und ungerade Werten unterscheidet, können wir gegebenenfalls  $l$  durch  $l - 1$  ersetzen. Wir kennen nun also  $A(n)$ .

Um die Rekursion (2) weiter zu untersuchen, setzen wir zwei spezielle Funktionen  $f$  ein.

(i) Für  $f \equiv 1$  erhalten wir aus (2)

$$\begin{aligned} 1 &= \alpha \\ 1 &= 2 \cdot 1 + \beta \\ 1 &= 2 \cdot 1 + \gamma \end{aligned}$$

die Werte  $(\alpha, \beta, \gamma) = (1, -1, -1)$  und aus (3) die Gleichung

$$A(n) - B(n) - C(n) = f(n) = 1$$

(ii) Für die Funktion  $f(n) = n$  verfahren wir gleichermassen:

$$\begin{aligned} 1 &= \alpha \\ 2n &= 2 \cdot n + \beta \\ 2n + 1 &= 2 \cdot n + \gamma \end{aligned}$$

Diese Gleichungen gelten für  $(\alpha, \beta, \gamma) = (1, 0, 1)$ . Aus (3) folgt die Gleichung

$$A(n) + C(n) = f(n) = n$$

Wir argumentieren nun folgendermaßen: Die Parameter  $(\alpha, \beta, \gamma) = (1, -1, -1)$  bzw.  $(\alpha, \beta, \gamma) = (1, 0, 1)$  bestimmen eindeutig die Lösungsfunktionen  $f(n) = 1$  respektive  $f(n) = n$  – schlicht nach Konstruktion und da die Iteration (2) die Funktion  $f$  gänzlich bestimmt. Das bedeutet, dass unsere Lösungsfunktion (3) insbesondere identisch mit diesen zwei Funktionen sein muss, wenn wir die entsprechenden Parameter wählen. Die gefundenen Eigenschaften liefern also das folgende Gleichungssystem:

$$\begin{aligned} A(n) &= 2^m \\ A(n) - B(n) - C(n) &= 1 \\ A(n) + C(n) &= n \end{aligned}$$

mit  $n = 2^m + l$  und  $0 \leq l < 2^m$ . Das ist ein lineares Gleichungssystem in den drei Unbekannten  $A(n), B(n), C(n)$ , das aus drei linear unabhängigen Gleichungen besteht. Wir können das System also leicht lösen und erhalten genau unseren Tipp (4).

Unsere Vorgehensweise war also deshalb so erfolgreich, da wir eine Lösungsfunktion haben, die *linear* von Parametern abhängt, auf die wir durch Betrachtung von Spezialfällen schließen können.

Wir wollen auch jetzt wieder diese Rekursion mittels Binärkodierung beschreiben. Dazu beschreiben wir die Rekursion in der Form

$$(5) \quad \begin{aligned} f(1) &= \alpha \\ f(2n + j) &= 2f(n) + \beta_j \end{aligned}$$

mit  $j \in \{0, 1\}$  und  $\beta_0 = \beta, \beta_1 = \gamma$ . Wir berechnen

$$\begin{aligned} f((b_m b_{m-1} \dots b_1 b_0)_2) &= 2f((b_m b_{m-1} \dots b_1)_2) + \beta_{b_0} \\ &= 4f((b_m b_{m-1} \dots b_2)_2) + 2\beta_{b_1} + \beta_{b_0} \\ &\quad \vdots \\ &= 2^m f((b_m)_2) + 2^{m-1} \beta_{b_{m-1}} + \dots + 2\beta_{b_1} + \beta_{b_0} \\ &= 2^m \alpha + 2^{m-1} \beta_{b_{m-1}} + \dots + 2\beta_{b_1} + \beta_{b_0} \end{aligned}$$

Wir schreiben letztere Zahl nun „suggestiv“ in Binärdarstellung, d.h. wir erlauben in der Binärdarstellung als Koeffizienten nicht nur Nullen und Einsen, sondern beliebige Zahlen. Dann folgt

$$f((b_m b_{m-1} \dots b_1 b_0)_2) = (\alpha \beta_{b_{m-1}} \beta_{b_{m-2}} \beta_{b_1} \beta_{b_0})_2$$

Wir rechnen ein Beispiel; und zwar verwenden wir die Parameter unseres ursprünglichen Josephus-Problems, nämlich  $(\alpha, \beta, \gamma) = (1, -1, 1)$ . Wir berechnen also  $J(100) = f(100) = f((1100100)_2)$ . Es folgt

$$\begin{aligned} &f((1100100)_2) \\ &= (\alpha \beta_1 \beta_0 \beta_0 \beta_1 \beta_0 \beta_0)_2 \\ &= (\alpha \gamma \beta \beta \gamma \beta \beta)_2 \\ &= (1 \ 1 \ -1 \ -1 \ 1 \ -1 \ -1)_2 \\ &= 1 \cdot 2^6 + 1 \cdot 2^5 + (-1) \cdot 2^4 + (-1) \cdot 2^3 + 1 \cdot 2^2 + (-1) \cdot 2^1 + (-1) \cdot 2^0 \\ &= 64 + 32 - 16 - 8 + 4 - 2 - 1 \\ &= 73 \end{aligned}$$

In diesem Fall sehen wir auch aus dieser allgemeineren Beschreibung die Tatsache, dass sich  $J$  durch Bit-Linksrotation ergibt: Wir unterteilen den Bitcode in Ausschnitte der Form  $(10 \dots 0)_2$ . Das Bild eines solchen Blocks ist  $(1 \ -1 \ \dots \ -1)_2 = (0 \dots 01)_2$ . Die zyklische Shift-Eigenschaft folgt, da die 1 in  $(0 \dots 01)_2$  nun entweder durch die Linksverschiebung der direkt rechts davon stehenden 1 herrührt, oder, dass sie die Rotation der an höchster Stelle stehenden 1 darstellt.

Geht man die obigen Argumente nochmals sorgsam durch, so ist es nun direkt einsichtlich, dass eine abermals verallgemeinerte Iterationsvorschrift

$$\begin{aligned} f(j) &= \alpha_j && \text{für } 1 \leq j < d \\ f(dn + j) &= cf(n) + \beta_j && \text{für } 0 \leq j < d \text{ und } n \geq 1 \end{aligned}$$

mit  $\alpha_j \in \mathbb{R}$ ,  $c > 0$  die Lösung

$$(6) \quad f((b_m b_{m-1} \dots b_1 b_0)_d) = (\alpha_{b_m} \beta_{b_{m-1}} \beta_{b_{m-2}} \dots \beta_{b_1} \beta_{b_0})_c$$

besitzt. Hierfür macht man sich klar, dass der Faktor  $c$  die geometrische Summenzerlegung des Bildes zur Basis  $c$  bestimmt, sprich, die Zerlegung im  $c$ -er System. Der Faktor  $d$  bestimmt das Zahlensystem der Eingabe.

Ein weiteres Beispiel soll unsere Betrachtungen abschließen. Wir betrachten die Rekursion

$$\begin{aligned} f(1) &= 34 \\ f(2) &= 5 \\ f(3n) &= 10f(n) + 76 \\ f(3n + 1) &= 10f(n) - 2 \\ f(3n + 2) &= 10f(n) + 8 \end{aligned}$$

für  $n \geq 1$ . Das entspricht obiger Iteration mit  $c = 10$  und  $d = 3$ . Wir wollen  $f(21)$  berechnen. Dazu stellen wir 21 im 3-er System als  $21 = (210)_3$  dar. Gleichung (6) liefert nun

$$f(22) = f((210)_3) = (5 \quad -2 \quad 76)_{10} = 5 \cdot 100 - 2 \cdot 10 + 76 \cdot 1 = 556$$

#### REFERENCES

- [1] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

MANUEL AMANN  
 FAKULTÄT FÜR MATHEMATIK  
 INSTITUT FÜR ALGEBRA UND GEOMETRIE  
 KARLSRUHER INSTITUT FÜR TECHNOLOGIE  
 KAISERSTRASSE 89–93  
 76133 KARLSRUHE  
 GERMANY

manuel.amann@kit.edu  
<http://hans.math.upenn.edu/~mamann/>