Schieberegister, Spiele

und endliche Automaten

Johannes Waldmann

Institut für Informatik, Uni Leipzig

Schieberegister-Folgen

Gegeben $f :: \{0,1\}^T \to \{0,1\}$. Die Folge $x = S_f$ ist

$$\begin{aligned} -T \le i < 0 &: x(i) = 1 \\ 0 \le i &: x(i) = f(x(i-T), \ldots, x(i-1)) \end{aligned}$$

Der *Zustand* zur Zeit i ist die Teilfolge $x(i - T \ldots i - 1)$.

Die Fortsetzung ist durch den Zustand eindeutig bestimmt.

Es kommen $\le 2^T$ verschiedene Zustände vor.

Die Folge x ist schließlich periodisch,
Vorperiodenlänge und Periodenlänge sind $\le 2^T$.

Perioden finden für Folgen $z_i = f^i(z_0)$

naiv: testen, ob z_i in $\{z_0, \ldots, z_{i-1}\}$ vorkommt.

implementiere Menge als Array, Hashtabelle, Suchbaum, ...

geschickt (Pollards ρ-Methode):

benutze Folge $h_i = z_{2i}$, bestimme $j > 0$ mit $z_j = h_j$.

```
h := z := z0 ; repeat z := f (z) ; h := f (f (h)) until h == z;
```

```
head $ filter (uncurry (==))
     $ tail $ zip ( iterate f z0 ) ( iterate (f . f) z0 )
```

$(z_j = z_{2j}) \Rightarrow$ zwischen j und $2j$ liegt (wenigstens eine) Periode.

läuft in linearer Zeit und konstantem Platz.

Vollständige XOR-Folgen

$f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 = x_1 + x_2 \pmod 2$ ergibt
$S_f = (1, 1, 1, 1, 0 \ldots)$
mit Periodenlänge $15 = 2^4 - 1$.

Satz: Zu jedem T gibt es $1 \le t_1 < \ldots < t_k \le T$,
so daß für $f(x_1, \ldots, x_T) = x_{t_1} \oplus \ldots \oplus x_{t_k}$
die Folge S_f die Periode $2^T - 1$ besitzt.

Aufgabe: Finde Beispiele für $T = 5, 6, 7, 8, \ldots$

Beweis: Zerfällungskörper von GF(2) bzgl. $x^T - 1 = 0$.

Literatur:
S.W. Golomb, Shift Register Sequences, 1982.

NAND-Folgen mit langer Periode

nichtlinear $\Rightarrow$ algebraische Theorie nicht anwendbar

$$1 \le t_1 < \ldots < t_k = T$$

$$\begin{aligned} -T \le i < 0 &: x(i) = 1 \\ 0 \le i &: x(i) = \neg\,(x(i - t_1) \wedge \ldots \wedge x(i - t_k)) \end{aligned}$$

untersucht von Althöfer, Bültermann, Flammenkamp (1990 ff.)
`http://wwwhomes.uni-bielefeld.de/achim/diss.ps.gz`

offen: gibt es eine Familie von Parametern $t = (t_1, \ldots, t_k)$,
so daß periode(t) $= 2^{\Theta(T)}$?

bis jetzt ist nur polynomielles Wachstum bekannt
($\Theta(T^4)$ sicher, $\Theta(T^6)$ vermutet).

Beispiel: NAND-Perioden-Struktur

```
cd ~/autotool
hugs -98 +o -Putil: Shift/Period.hs

Shift.Period> take 100 $ folge [4,6,11,15]
----++++++-++++++++--+-++++-+-++-+
+++++-+-++++-+--+-++++++-++++++-+--+-++++-+-++++++-++-+-++++-+--++

Shift.Period> take 10 $ group $ folge [4,6,11,15]
[----,++++++,-,++++++++,--,+,-,++++,-,+]

Shift.Period> take 50 $ map length $ group $ folge [4,6,11,15]
[4,6,1,8,2,1,1,4,1,1,1,2,1,6,1,1,1,
4,1,1,2,1,1,6,1,6,1,1,2,1,1,4,1,1,1,
6,1,2,1,1,1,4,1,1,2,8,1,6,4,6]
```


Beispiel: NAND-Perioden-Struktur

$t(k) = (2k, 3k, 5k + 1, 7k + 1)$ für $k > 0$, Bsp: $t(2) = (4, 6, 11, 15)$

```
period k =
    do l <- [ 0 .. k-1 ]
       ( if l == 0
         then [ 2*k, 3*k, 1, 4*k, k, 1, k-1, 2*k ]
         else [ l, k-l, k, l, k-l, 2*k ]
         ) ++ do m <- [ 1 .. l ]
                 do d <- [ 0 .. 1 ]
                    [ m , k-m, m+d, 3*k, l-m+1-d, k-l+m ]
                      ++ if m < l then [ k-m, l  , k-l,   2*k ]
                                  else [ k-m, l+d, k-l-d, 2*k ]
           ++ do m <- [ l+1 .. k-1 ]
                 do d <- [ 0 .. 1 ]
                    [ l+1, k-l-1, m+d, k+l-m+1-d, m-l , 3*k
                      , k-m, m+d, k-m-d, 2*k  ]
```

Periodenlänge ist $18k^3 - 11k^2 + 6k + 1$

Struktur von NAND-Perioden

Beschreibung durch geschachtelte Schleifen
mit linear variierten Parametern (Faktoren $\in \{-1, 0, 1\}$)

(Schachteltiefe $\approx$ Grad des Wachstum-Polynoms)

Programmier-Aufgaben:

a) Beschreibung finden (raten), b) Beschreibung verifizieren

c) nicht programmieren, sondern beweisen:

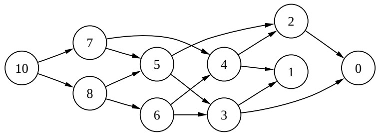
Vermutung: jede NAND-Folge besitzt so eine Beschreibung.

Folgerung: NAND-Folgen haben polynomiell lange Perioden.

Subtraktionsspiele

für zwei Spieler. Parameter: Folge $1 \leq t_1, \dots t_k \leq T$.

Spiel-Situation: eine Zahl $n \geq 0$.
Spiel-Zug: wähle i, ziehe $n \mapsto (n - t_i)$.
Spiel-Ziel: letzter Zug. (Wer nicht mehr ziehen kann, verliert.)



Situations-Bewertung: $b : n \mapsto$ (wenn anziehender Spieler eine Gewinnstrategie besitzt, dann 0 else 1)
$b(n) = \neg(b(n - t_1) \wedge \ldots \wedge b(n - t_k))$.

Abstrakte (neutrale) Spiele

M : Menge von Spielpositionen

R : (erlaubte Züge) eine wohlfundierte Relation $\subseteq M^2$

$\Rightarrow$ endliches Zweipersonen-Nullsummenspiel: abwechselnd ziehen; wer nicht mehr kann, verliert.

$N \subseteq M$: Positionen, in denen der anziehende (*nächste*) Spieler eine Gewinnstrategie besitzt

$P \subseteq M$: ... nachziehende (= vorige, *previous*) ...

Spiel ist endlich, kein Remis $\Rightarrow$ (P, N) ist eine Partition von M.

Wort-Ersetzungs-Spiele

Beispiel: $\Sigma = \{a\}, M = \Sigma^*$, Parameter $1 \leq t_1 < \ldots < t_i = T$ und Regeln

$$R = \{(a^{t_i}, \epsilon) \mid 1 \leq i \leq k\}$$

ergibt genau die Subtraktionsspiele.

Zustandsfolge des Schieberegisters ist schließlich periodisch $\Rightarrow$
Positionsbewertung $b : \mathbb{N} \to \{0, 1\}$ ist schließlich periodisch $\Rightarrow$
Gewinn- und Verlustmenge (N, P) sind reguläre Sprachen.

Beispiel: $\Sigma = \{a, b\}$. für $R = \{ab \to \epsilon\}$ ist
$P \cap a^*b^* = \{a^{2n}b^{2n} \mid n \geq 0\} \notin$ REG.

Aufgabe: bestimme eine CF-Grammatik für P (und eine für N).

Suffix-Ersetzungs-Spiele

gestatten Regelanwendungen nur *am (rechten) Wort-Ende*

Regelmenge $R \subseteq \Sigma^* \times \Sigma^*$ erzeugt Relation
$u \to_R v := \exists (l, r) \in R, w \in \Sigma^* : u = wl \wedge v = wr$.

Satz: wenn $\to_R$ terminiert, dann sind P_R und N_R reguläre Sprachen.

vergleiche: Satz (Büchi, 1960): wenn $L \in$ REG, dann
$R^*(L) = \{v \mid L \ni u \to_R^* v\} \in$ REG.

Grund-Term-Ersetzungs-Spiele

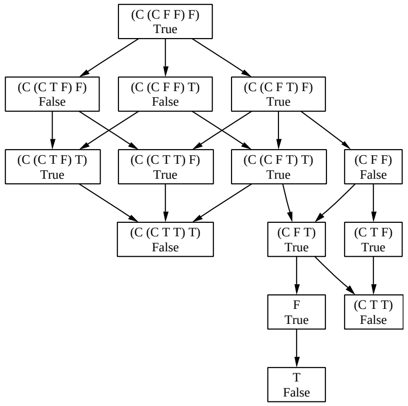
Signatur $\Sigma = \Sigma_0 \cup \ldots \cup \Sigma_k$,

(Σ_k enthält k-stellige Symbole).

Beispiel $\Sigma_0 = \{F, T\}, \Sigma_2 = \{C\}$.

(Grund-)Ersetzungs-Regeln

$R = \{F \to T, C(F,T) \to F\}$.



Eigenschaften von GTRS

Vermutung: für jedes GTRS-Spiel sind P und N reguläre Baumsprachen.

d. h. erzeugbar durch eine Baumgrammatik mit Regeln der Form $M \to f(M_1, \ldots, M_k)$.

vergleiche: Satz: für jedes GTRS R und $L \in$ REG gilt $R^*(L) \in$ REG.

Teilwort-Ersetzung (Beispiel Autobahn)

$\Sigma = \{0, 1, 2\}$

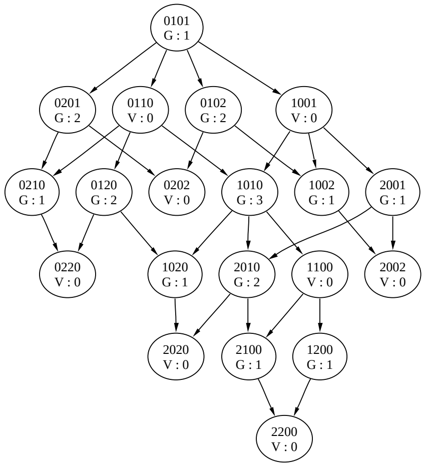
$R = \{01 \to 10, 1 \to 2\}$.

Relation $u \to_R v :=$
$\exists (l,r) \in R : \exists x, y \in \Sigma^* :$
$u = xly \land v = xry$.

Autobahn:
0 = frei, 1 = Auto, 2 = kaputt

Vermutung: $(01)^{4*} \subseteq P$,

d. h. $\epsilon, 01010101, (01)^8, \ldots$
sind verloren.



Teilwort-Ersetzung (Beispiel Officers)

offene Frage: für $R = \{11 \to 10\}$, ist P regulär?