Anmerkungen zur Übung vom 20.11.

Aufgabenblatt 3 vom 3. 11. (Lösungen)

S3-1 $F_0 = 0,\ F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}$ für $n > 1$

Kommentar: grundsätzliches Vorgehen: (a) Beispiele erzeugen, (b) Vermutung ableiten, (c) beweisen.

Bei (a) kann die Maschine helfen. Man braucht hier gar keine symbolischen Rechnungen, eine beliebige (z.B. funktionale) Programmiersprache reicht. Bei (c) wird sicher Induktion benutzt, das kann Maxima (u.ä.) nicht, aber z.B. Isabelle `http://isabelle.in.tum.de/`

Zu (a): Maxima kennt die Funktion `fib`. Details dazu in der Datei `serie-3.txt`.

Zum Ausrechnen der F-Zahlen:

0. naiv ist das:

```
f :: Int -> Integer
f n = if n > 1 then f (n-1) + f (n-2)
      else if n == 1 then 1 else 0
```

Rechenzeit allerdings exponentiell: $f(7)$ ruft $f(6)$ und $f(5)$ auf, $f(6)$ ruft $f(5)$ und $f(4)$ auf – $f(5)$ wurde also schon zweimal aufgerufen. Untersuchen Sie, wie oft bei der Berechnung von $f(n)$ der Funktionsaufruf $f(n-k), k < n$ abgesetzt wird.

1. durch „dynamische Programmierung/Optimierung“ wird die Zahl der Funktionsaufrufe linear: man speichert die berechneten Funktionswerte ab, d.h. rechnet sie nur einmal aus. Die (lazy) Liste aller F-Zahlen:

```
fs = 0 : 1 : zipWith (+) fs (tail fs)
```

2. Durch weiteres Nachdenken wird es logarithmisch.

Es gilt

$$\begin{pmatrix} F_{k+2} \\ F_{k+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F_{k+1} \\ F_k \end{pmatrix}$$

und deswegen

$$\begin{pmatrix} F_{k+1} \\ F_k \end{pmatrix} = M^k \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{für} \quad M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Die Potenz M^k kann man durch Quadrieren und Multiplizieren mit $O(\log(k))$ Operationen bestimmen.

Eine solche Matrix-Multiplikation ist in Maxima implementiert (`^^`), aber nicht für das Rechnen in Matrizen über einem Restklassenring. Auch hier muss also die Matrixmultiplikation für die speziellen Zwecke nachimplementiert werden. Einfacher ist es in einem System wie zum Beispiel dem CAS AXIOM, in dem eine Funktionsdefinition `matPower(M,n,R)` für Matrizen M über einem Ring R als Parameter möglich ist.

3. Für die Aufgabe benötigt man die Zahlen F_k überhaupt nicht, sondern nur ihre Restklassen. Deswegen sollte man auch alle Operationen (plus und mal innerhalb der Matrix-Operationen) direkt mit Restklassen(repräsentanten) ausführen. Damit wird Langzahlarithmetik komplett vermieden.

Zur Lösung der Aufgabe selbst (ohne Rechnen, nur Nachdenken): zu zeigen ist:

$$\forall e : \exists k : F_k \equiv -1 \pmod{10^e}.$$

Wir schreiben $m = 10^e$ (auf den Wert von m kommt es überhaupt nicht an) und zeigen:

> Die Folge der Paare der Reste $(F_{k+1} \pmod m, F_k \pmod m)$ ist rein periodisch (d.h. ohne Vorperiode).

„Schließlich periodisch“ ist klar, da der Wertebereich endlich ist und aus zwei Vorgängern sich die nächste Zahl eindeutig berechnet. Nach endlich vielen Schritten muss sich aber wegen der Endlichkeit der Reste ein solches Paar wiederholen.

Auch kann man aus zwei Nachfolgern den Vorgänger eindeutig berechnen: $F_{n-2} = F_n - F_{n-1}$, die Fibonaccifolge kann so auch in den Bereich $n < 0$ eindeutig fortgesetzt werden. Damit kann es keine Vorperiode geben und die Folge ist rein periodisch. Dort ist weiter $F_{-2} = -1$.

Die in der Datei `serie-3.txt` beschriebenen Untersuchungen legen eine Vermutung über die Periodenlänge nahe, die mit diesem groben Argument nicht zu beweisen ist.

Aufgabe: Stellen Sie eine Vermutung für eine Formel $k = k(l)$ auf, so dass für die oben angegebene „Fibonacci-Matrix“ $M^k \pmod{10^l}$ gleich der Einheitsmatrix ist, und beweisen Sie diese Vermutung (z.B. durch Induktion).

Termordnungen

Die in der Übung vorgestellten Beispiele finden Sie in `serie-3.txt`.

Termordnungen auf dem Termmonoid $T(X)$ und dessen Quotient $Q(X) = \{X^a,\ a \in \mathbb{Z}^n\}$.

- Jede Termordnung auf $T(X)$ lässt sich eindeutig auf $Q(X)$ fortsetzen: Jedes Element $a \in \mathbb{Z}^n$ kann als $a = a' - a''$ mit $a', a'' \in \mathbb{N}^n$ dargestellt werden. Setze

  $$X^a > X^b \iff X^{a'+b''} > X^{a''+b'}$$

  und zeige, dass eine solche Definition von der Darstellung $a = a' - a''$ unabhängig ist.

- In $Q(X)$ gilt $X^a > X^b \iff X^{a-b} > X^0 = 1$. Jede Termordnung kann also durch ihren *Positivbereich* $P(>) = \{a \in \mathbb{Z}^n, X^a > 1\}$ beschrieben werden.

- Dieser Positivbereich $P(>)$ ist ein Kegel (mit zwei Vektoren liegt auch deren Summe im Positivbereich).

- Kegel, Hyperebenen und lineare Funktionale.

wfmPA

Finde eine kompatible wohlfundierte monotone Algebra (wfmA)...

Ich hatte mehrfach die Kollegen aus Innsbruck erwähnt. Die haben auch ein Programm, das Terminationsbeweise findet `http://cl-informatik.uibk.ac.at/software/ttt2/` Dort gibt es Binaries, Quelltexte, Weboberfläche. Man muß dann das Terminationsproblem in der offiziellen Syntax darstellen

```
(VAR x y)
(RULES P(Z,y) -> y
       P(S(x),y) -> S(P(x,y))  )
```

und ttt2 mit geeigneten Optionen aufrufen, z.B.

```
ttt2 -s 'poly -direct -nl2 -heuristic 1' a3-1a.trs
```

Das geht für A3-1a (Addition) und A3-1c (Multiplikation),

aber nicht für A3-1b (Addition und Multiplikation). Dann sollte man untersuchen (wie vorige Übung), ob das daran liegt, daß die Ableitungen zu lang werden (weil das für uns bis jetzt die einzige Möglichkeit ist, zu zeigen, daß es keine kompatible wfmPA gibt).

Vervollständigung

$\boxed{\textbf{A3-3a}}$ Komplettiere das Gleichungssystem $\{a(b(a(1))) \approx 1\}$ unter einer geeigneten Orientierungsordnung.

$\boxed{\textbf{A3-3b}}$ Komplettiere das Gleichungssystem $\left\{f^{(5)}(a) \approx a, f^{(3)}(a) \approx a\right\}$ unter einer geeigneten Orientierungsordnung.

Eine wfmA findet man für die Aufgabe wie früher beschrieben, etwa $[a]() = 0,\ [f](x) = x+1$. Folgende Schritte:

- Anfangs ist $E = \left\{f^5(a) = a, f^3(a) = a\right\}$.
- Orient: $f^3(a) = a$, ergibt $R = \left\{f^3(a) \to a\right\},\ E = \left\{f^5(a) = a\right\}$.
- Simplify: $f^5(a) \to f^2(a)$ ersetzt $f^5(a) = a$ durch $f^2(a) = a$ in E: $E = \left\{f^2(a) = a\right\}$.
- Orient: $f^2(a) = a$, ergibt $R = \left\{f^3(a) \to a, f^2(a) \to a\right\},\ E = \{\}$.
- Deduce: $f^3(a)$, ergibt $R = \left\{f^3(a) \to a, f^3(a) \to f(a)\right\},\ E = \{f(a) = a\}$.
- Orient: $f(a) = a$, ergibt $R = \left\{f^3(a) \to a, f^2(a) \to a, f(a) \to a\right\},\ E = \{\}$.

Details finden Sie wie in der Übung besprochen in `serie-3.txt`.

$\boxed{\textbf{A3-3c}}$ Komplettiere das Gleichungssystem $\{f(a,a) \approx a, f(x, f(y,z)) \approx f(f(x,y),z)\}$ unter einer geeigneten Orientierungsordnung.

Weitere Autotool-Aufgaben

$\boxed{\textbf{A2-2}}$ $F = \{f(x, f(y, z)) \approx f(f(x, y), z), f(e, x) \approx x, f(i(x), x) \approx e\}$.
Zeige $f(x, e) \approx_F x$.

$\boxed{\textbf{A2-3}}$ $G = \{f(x, f(y, z)) \approx f(f(x, y), z), f(f(x, y), x) \approx x\}$.
Zeige (a) $f(x, x) \approx_G x$ und (b) $f(f(x, y), z) \approx_G f(x, z)$

$\boxed{\textbf{A2-4}}$ $H = \{f(x, f(y, z)) \approx f(f(x, y), z), f(e, x) \approx x, f(x, i(x)) \approx e\}$.
(Beachten Sie die korrigierte Aufgabenstellung (A2-4r), die einen Schreibfehler berichtigt).

Zeige $f(x, e) \not\approx_H x$.

Lösungen zu den Aufgaben (A2-2) und (A2-3a) finden Sie ebenfalls in der Datei `serie-3.txt`.