Prof. Martin Hofmann, PhD
Dr. Steffen Jost

Ludwig-Maximilians-Universität München
Institut für Informatik
7. Juli 2015

11. Übung zur Vorlesung

Programmierung und Modellierung

A11-1 ***Auswertestrategie*** Werten Sie den Programmausdruck entweder mit der Auswertestrategie Call-By-Name oder Call-By-Value Schritt-für-Schritt aus, wie in der Vorlesung gezeigt. Unterstreichen Sie jeweils den Redex, welchen Sie im nächsten Schritt auswerten.

Welche Auswertestrategie haben Sie jeweils gewählt und warum?

a) `(\(x,y) -> y) (1 + (2 + 3), 4 + 5)`

b) `(\x -> x + x) ((\y -> y * y) (1+1))`

A11-2 ***Poset*** Überprüfen Sie anhand der gegebenen Definition in Foliensatz 12, welches der Nachfolgenden eine partiell geordnete Menge (poset) ist. Zeichnen Sie für jedes poset ein Hasse-Diagramm!

a) $(\mathbb{N}, \neq)$

b) $\big(\{Stein, Schere, Papier\}, \succcurlyeq\big)$ wobei $\succcurlyeq$ wie folgt definiert ist:

$$\begin{aligned}\succcurlyeq := \{&(Stein, Stein), (Schere, Schere), (Papier, Papier),\\ &(Stein, Schere), (Schere, Papier), (Papier, Stein)\}\end{aligned}$$

c) $(\{1,2,3,4,5,6,7,8,9\}, |)$ wobei $x|y$ bedeutet "x ist ganzzahliger Teiler von y"

A11-3 ***Umgang mit Monaden***

Schnell mit Papier und Bleistift: Zu was werten die folgenden Ausdrücke aus?

a) `forM [1..3] (\x -> if even x then Just x else Nothing)`

b) `mapM print [1..4]`

c) `forM [1..3] (\x -> print x >> return (x+1))`

d) `runPar $ do { xs <- forM [1..3] (\x -> spawnP (x*x)); mapM get xs }`

A11-4 ***Verzögerte Auswertung*** Betrachten Sie das folgende Haskell Programm:

```
ps = iterate (+1) 0
qs = iterate (*2) 1
rs = iterate (^2) 2

iterate f x = x : iterate f (f x)

foo (_:x:xs) ys@(y:_) zs
  | x  > y    = x
  | otherwise = foo ys zs xs
```

Aufgrund der verzögerten Auswertestrategie von Haskell wird z.B. die Liste `ps` anfangs nur als ein Verweis auf den Code `iterate (1+) 0` abgespeichert. Erst sobald auf das erste Element dieser Liste zugegriffen wird, wird zeigt `ps` auf die Liste `0: iterate (+1) (0+1)`. Wird später dann auch noch das zweite Element benötigt, so zeigt der Bezeichner `ps` nun auf die Liste `0:1: iterate (+1) (1+1)` im Speicher.

Bis zu welchem Element werden die Listen `ps`, `qs`, `rs` im Speicher ausgewertet, wenn nur der Aufruf `foo ps qs rs` ausgeführt wird?

H11-1 ***Auswertestrategie II*** (3 Punkte; Abgabeformat: Text oder PDF)
Werten Sie den Programmausdruck entweder mit der Auswertestrategie Call-By-Name oder Call-By-Value schrittweise aus. Unterstreichen Sie jeweils den ausgewerteten Redex.

```
(\x -> \y -> y ( y x )) 9 ((\a b -> b+b) (7*(2+3)))
```

Welche Auswertestrategie haben Sie gewählt und warum?

H11-2 ***Hasse-Diagramm*** (2 Punkte; Abgabeformat: Text oder PDF)
Zeichne das Hasse-Diagramm zu der geordneten Menge $(\mathcal{P}(M), \subseteq)$, für $M = \{1, 2, 3, 4\}$.

H11-3 ***Kodeknacker*** (4 Punkte; Datei `H11-3.hs` als Lösung abgeben)
Heimtückischerweise konnten Sie eine Übertragung der Musterlösung zur kommenden ProMo-Klausur abfangen! Leider wurde jede Teilaufgabe mit einem anderen Schlüssel verschlüsselt. Glücklicherweise konnte Ihnen ein fleißiger (aber gewissenloser) Kommilitone, der eine Vorlesung über Kryptographie aufmerksam besucht hatte, Ihnen ein Haskell-Programm zum Knacken der Verschlüsselung erstellen (siehe Dateivorlage `H11-3.hs`). Das Programm funktioniert, doch die Berechnung dauert viel zu lange! Ihr Kommilitone versicherte, dass eine weitere grundlegende Optimierung dieses Algorithmus sehr unwahrscheinlich ist. Als letzter Ausweg bleibt also nur die Parallelisierung des gegebenen sequentiellen Programms!

a) Beschleunigen Sie die Ausführung der Vorlage durch den Einsatz der `Par`-Monade! Mit 4 Kernen sollten Sie eine Beschleunigung um Faktor ≥ 3 erreichen können.

Das verwendete Kryptoverfahren ist zur Lösung der Aufgabe nicht so wichtig. Es reicht hier, die zeitaufwändige Funktion zu identifizieren:

```
slowFactor :: (Integer,Integer) -> Integer -> Maybe Integer
```

Der Aufruf `slowFactor (lo,hi) n` sucht einen Faktor von `n` im Intervall `(lo,hi)`. Damit ist die Idee zur Parallelisierung auch schon klar: Wir zerlegen das gegebene Intervall in mehrere ungefähr gleich-große Teilintervalle. Anstatt *einem* langwierigem Aufruf von `slowFactor` mit einem großen Intervall, führen wir dann *mehrere* parallele Aufrufe von `slowFactor` mit kleinen Teilintervallen durch. Damit können wir die Suche nach einem der Primfaktoren beschleunigen!

Hintergrundwissen für Interessierte, zur Lösung nicht relevant: In dieser Aufgabe arbeiten wir mit dem RSA Kryptoverfahren. Dies ist ein asymmetrisches Verfahren, d.h. jeder kann mit einem öffentlich bekannten Schlüssel eine Nachricht kodieren, welche nur der Empfänger mit seinem privaten Schlüssel lesen kann. Die Sicherheit beruht dabei auf einer sogenannten "Einwegfunktion mit Falltür": Die Berechnung der Kodierung geht schnell (wie z.B. Multiplikation zweier Primzahlen) während die Umkehrfunktion (im Beispiel also Primfaktorzerlegung) eine aufwendige Berechnung ist, falls man nicht bereits einen der beiden Primfaktoren im Voraus kennt. Bei RSA gibt es einen öffentlich bekannten Schlüssel (e, N) und einem geheimen Schlüssel (d, N). Dabei ist N ein Produkt aus zwei großen Primzahlen. Zum Brechen des Codes muss man "nur" N in seine beiden Primfaktoren zerlegen.

b) Sobald einer der beiden Primfaktoren gefunden wurde, kann die Suche abgebrochen werden, da der andere Primfaktor wegen $N = p \cdot q$ dann ja leicht durch eine einzige Division berechnet werden kann. Deshalb wäre es doch noch schneller, wenn die komplette Suche abgebrochen wird, sobald irgendeiner der beiden Primfaktoren gefunden wurde!

Bei Verwendung der `Par`-Monade können Sie Ihr Programm so schreiben, dass die Suche abgebrochen wird, wenn der kleinere Primfaktor gefunden wurde. Sie können es auch so schreiben, dass abgebrochen wird, wenn der größere Primfaktor gefunden wurde. Sie können Ihr Programm mit der `Par`-Monade jedoch nicht so formulieren, dass die Suche abgebrochen wird so bald *einer* der beiden Primfaktoren gefunden wurde (also egal ob der kleinere oder größere Primfaktor, dessen Berechnung am schnellsten gelang).

Warum ist dies mit der `Par`-Monade grundsätzlich nicht möglich?

Abgabe: Lösungen zu den Hausaufgaben können bis Dienstag, den 14.07.2015, 11:00 Uhr mit UniworX abgegeben werden.

Aufgrund des Klausurbonus müssen die Hausaufgaben von Ihnen alleine gelöst werden. Abschreiben bei den Hausaufgaben gilt als Betrug und kann zum Ausschluss von der Klausur zur Vorlesung führen.