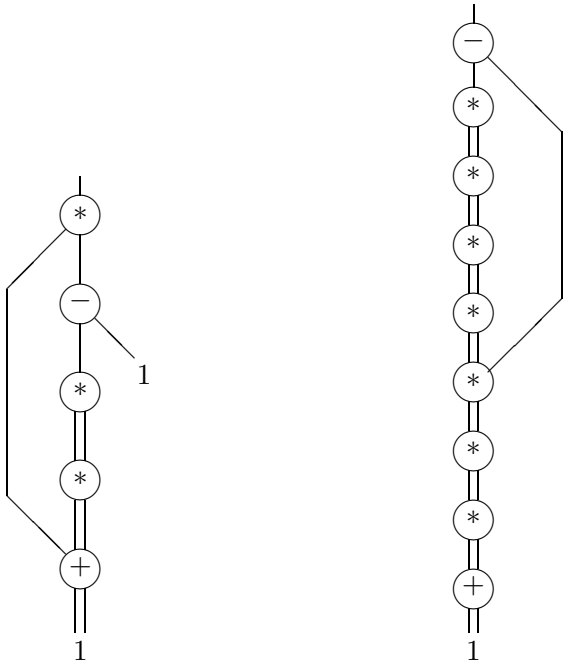
Eberhard Karls Universität Tübingen
Wilhelm-Schickard-Institut für Informatik (WSI)
Arbeitsbereich für Theoretische Informatik/Formale Sprachen

Themenvorschlag für eine Studien- oder Diplomarbeit 5. Dezember 2007

Viele verschiedene Primfaktoren mit wenigen Operationen

Es geht um folgenden "mathematischen Lego-Baukasten": Der Grundbaustein des Baukastens ist die Zahl 1. Verbindungsstücke sind die Operationen Addition $+$, Subtraktion $-$, und Multiplikation $*$. Aus den Operationen darf man sukzessive einen "Turm" bauen, d.h. dass eine neu dazukommende Operation nur auf Eingaben zurückgreifen darf, die im bisherigen Turm schon vorhanden sind. Die Größe eines Turms sei die Anzahl seiner Operationen. Wenn der Turm fertig ist, ergibt die oberste Operation im Turm nach der Ausführung der Operationen eine ganze Zahl, den *Ergebniswert* des Turms. Z.B. hat der linke Turm unten den Ergebniswert 30, der rechte hat den Ergebniswert $2^{128}-2^8$.



Der Ergebniswert 30 des linken Turms hat die Primfaktorzerlegung $2 * 3 * 5$, das sind 3 verschiedene Primfaktoren, der Ergebniswert $2^{128} - 2^8$ des rechten Turms hat die Primfaktorzerlegung $2^8 * 3^2 * 5^2 * 7 * 11 * 13 * 17 * 31 * 41 * 61 * 151 * 241 * 331 * 1321 * 61681 * 4562284561$, das sind 16 verschiedene Primfaktoren. Sei die *Kraft* eines Turms die Anzahl der verschiedenen Primfaktoren seines Ergebniswerts. Interessant sind die Türme, bei den das Verhältnis von Kraft zu Größe möglichst groß ist. Der rechte Turm zeigt, dass dieses Verhältnis größer als 1 sein kann.

Die Studienarbeit soll ein Computer-Programm schreiben, das sytematisch alle Türme bis zu einer bestimmten Größe aufbaut (bis Größe ca. 10 oder 15 müsste das gehen) und deren Kraft bestimmt. Dabei sollen natürlich die Türme mit optimalem Kraft-zu-Größe Verhältnis ausgegeben werden. Eine Diplomarbeit soll darüberhinaus auch algebraisch an dieses Optimierungsproblem herangehen und außerdem eine mögliche Verbindung zum Faktorisierungsproblem untersuchen: Kann ein Turm mit einem Kraft/Größe Verhältnis von sagen wir 2 oder 3 bekannte Faktorisierungs-Algorithmen beschleunigen, zum Beispiel den Pollard-rho-Algorithmus?

Betreuer: Dr. Bernd Borchert, Dr. Klaus Reinhardt
Email: borchert/reinhard at informatik dot uni-tuebingen dot de
http://www-fs.informatik.uni-tuebingen.de/~borchert