Lösen von Wortgleichungen mit diophantischen Systemen

Zuverlässige Systeme - Dirk Nowotka

Projektbeschreibung

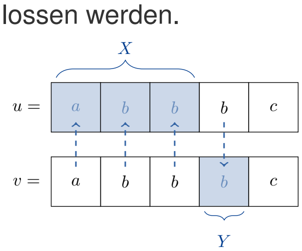
Seit der Geburt der Informatik sind Wortgleichungen eines der beeindruckendsten Probleme, da sie trotz ihrer einfach anmutenden Gestalt komplexe Mechanismen zur Lösung erfordern. Gegeben seien zwei Alphabete $\Sigma = \{ a_1, a_2, \ldots, a_n \}$ von Buchstaben und $\Gamma = \{ X_1, X_2, \ldots, X_m \}$ von Variablen, sowie zwei Wörter $u, v \in (\Sigma \cup \Gamma)^*$. Eine Wortgleichung ist nun die Fragestellung, ob es eine Funktion $S : (\Sigma \cup \Gamma)^* \to \Sigma^*$ (eine Substitution der Variablen) gibt, sodass $S(u) = S(v)$ gilt. Betrachten wir zwei Wörter $u = Xbc$ und $v = abbYc$ über einem Alphabet $\Sigma = \{ a, b, c \}$ und $\Gamma = \{ X, Y \}$, so würde die Substitutionsfunktion $S = \{ (X, abb), (Y, b) \}$ eine Lösung induzieren. Es gilt $S(Xbc) = abbbc = S(abbYc)$.

Die einfache Gestalt der Fragestellung trügt. Um eine Lösung zu finden, müssten prinzipiell alle möglichen Wörter für eine Substitution der Variablen getestet werden.

Eben dieser Nichtdeterminismus macht die Implementierung in der Praxis sehr schwer. Im Jahr 2000 wurde von Karhumäki, Mignosi und Plandowski ein Ansatz vorgestellt, welcher mit Kenntnis über die Längen der Variablen auf das direkte Raten der Variablenbelegung durch die Substitutionsfunktion S verzichten kann. Um die Längen der Variablen geschickt zu Finden, bieten sich bei linearen Wortgleichungen diophantische Gleichungssysteme an. Eine solches System sucht nach ganzzahligen Lösungen. Wortgleichungen können auf unterschiedliche Arten in ein diophantisches Gleichungssystem überführt werden. Eine Lösung ist jedoch in der Regel parametrisiert, wohingegen wir für die Wortgleichungen an konkreten Wörtern interessiert sind.

An dieser Stelle treffen wir auf eine Grenze unserer Computer, welche uns das Auflisten von möglicherweise unendlich vielen Zahlen nicht ermöglicht. Auf naive Art können wir die obige Wortgleichung durch die Gleichung $Y \cdot (1) + X \cdot (-1) + 2 = 0$ kodieren. Es ergibt sich die parametrisierte Lösung $|X| = t_0$ und $|Y| = t_0 - 2$ für $t_0 \in \mathbb{Z}$.

Die gezeigte Lösung korrespondiert zur Betrachtung von $t_0 = 3$. Wir erhalten $|X| = 3$ und $|Y| = 1$. Auf die Lösung kann somit, wie in der folgenden Grafik dargestellt, geschlossen werden.



An dieser Stelle kommt die Fragestellung des Projektes zum Tragen: *Ist es möglich eine obere- und untere Schranke für die Längen der zu prüfenden Variablen anzugeben?*

Im Rahmen dieser Arbeit entwickeln die Studierenden einen Ansatz, diese Schranken anzugeben und durch präzise mathematische Argumentation zu verifizieren. Des Weiteren wird als Anteil der Realisierbarkeit der Idee, eine Implementierung angefertigt, welche anschließend im Wortgleichungslöser Vuurds eingesetzt werden soll.

Richtet sich an

Bachelorstudierende
Masterstudierende

Schlüsselwörter

Wortgleichungen
Diophantische Gleichungssysteme
Algorithmenentwicklung

Kontaktperson

Mitja Kulczynski
@ mku@informatik.uni-kiel.de