Über die Komplexität der Multiplikation in eingeschränkten Branchingprogrammmodellen

Philipp Wölfel

Zusammenfassung

In dieser Dissertation wird die Komplexität des mittleren Bits der Multiplikation in Branchingprogrammmodellen untersucht. Dabei werden im ersten Teil bekannte Ergebnisse für eingeschränkte Branchingprogrammmodelle verbessert und später werden für etwas allgemeinere Modelle die ersten exponentiellen unteren Schranken bewiesen. Zum Beweis dieser neuen Ergebnisse werden ganz andere Eigenschaften der Multiplikation herangezogen, als dies beim Nachweis unterer Schranken in früheren Arbeiten (z. B. bei Bryant 1991) der Fall war. So basieren alle hier vorgestellten unteren Schranken darauf, dass mithilfe der Multiplikation sog. universelle Hashklassen konstruiert werden können, und nutzen Eigenschaften aus, die sich für die Multiplikation aus dieser Tatsache ableiten lassen.

Im Einzelnen werden folgende Ergebnisse für das mittlere Bit der Multiplikation bewiesen. Zunächst wird die OBDD-Größe dieser Funktion untersucht und Bryants untere Schranke von $2^{n/8}$ aus dem Jahre 1991 verbessert. Es werden eine untere Schranke von $2^{n/2}/61$ sowie eine obere Schranke von $O\left(2^{4n/3}\right)$ nachgewiesen. Die untere Schranke belegt, dass das kleinste OBDD für das mittlere Bit der 64-Bit-Multiplikation aus mehr als 70 Millionen Knoten besteht – bei der 128-Bit-Multiplikation sind es sogar schon mehr als $3 \cdot 10^{17}$ Knoten. Damit ist erstmals die Vermutung bewiesen, dass mit heutigen Mitteln 128-Bit-Multiplikationsschaltkreise nicht mit OBDDs verifiziert werden können. Anschließend wird eine echt exponentielle untere Schranke von $\Omega\left(2^{n/4}\right)$ für die FBDD-Größe des mittleren Bits der Multiplikation gezeigt. Bisher war nur eine schwach exponentielle untere Schranke von $2^{\Omega(\sqrt{n})}$ bekannt (s. Ponzio, 1995).

Einige Aussagen zum Beweis der unteren Schranken für OBDDs und FBDDs beschreiben grundsätzliche Erkenntnisse über die Multiplikation. Im letzten Teil der Dissertation werden Techniken zum Beweis unterer Schranken für noch allgemeinere Branchingprogrammmodelle entwickelt, die zu diesen Erkenntnissen „passen“. Mithilfe dieser Techniken wird nachgewiesen, dass semantische $(1,+k)$-BPs zur Darstellung des mittleren Bits der Multiplikation eine Größe von $\Omega\left(2^{\frac{n}{48(k+1)}}\right)$ benötigen. Abschließend wird ein FBDD-Modell mit eingeschränktem Nichtdeterminismus betrachtet. Ein sog. $(\vee,k)$-FBDD entspricht einem nichtdeterministischen FBDD mit höchstens $k-1$ nichtdeterministischen Knoten, die auf jedem Pfad nur vor den deterministischen Knoten vorkommen dürfen. Es wird in diesem Modell eine untere Schranke von $\Omega\left(2^{n/(7k)}\right)$ für das mittlere Bit der Multiplikation bewiesen. Sowohl $(1,+k)$-BPs als auch $(\vee,k)$-FBDDs sind die ersten Branchingprogrammmodelle, die echt allgemeiner als FBDDs sind und für die superpolynomielle untere Schranken für die Komplexität der Multiplikation gezeigt werden konnten.