# OBERE UND UNTERE SCHRANKE FÜR DIE KOMPLEXITÄT VON BOOLESCHEN FUNKTIONEN

Hanke Bremer
Institut für angewandte Mathematik
Joh. Wolfg. Goethe Univ. Frankfurt

Eine Menge Boolescher Funktionen heiße n - stellig , wenn alle enthaltenen Funktionen auf den gleichen n Variablen definiert sind. Alle n-stelligen Mengen der Mächtigkeit t werden zu

$$M_{t,n} = \left\{ F \;\middle|\; |F| = t,\ F \text{ ist n-stellig} \right\}$$

zusammengefaßt. Im folgenden soll eine obere und eine untere Schranke für die Komplexität von F in Abhängigkeit von n und t angegeben werden. Zur Berechnung von F seien als o - stellige Operationen mit den Kosten o die Konstanten o und 1 und die Projektionen $x_1, \ldots, x_n$ zugelassen, als 2-stellige Operationen die Multiplikation und die Addition mod 2 mit den Kosten 1.

Lemma 1

Für die Komplexität L(F) einer Menge Boolescher Funktionen F aus $M_{t,n}$ gilt

$$L(F) \leq \frac{t2^n}{\mathrm{ldt}} \left( 1 + c \frac{\mathrm{ldldt}}{\mathrm{ldt}} \right) \quad .$$

Darin ist c eine von n und t unabhängige Konstante.

Der Beweis ist in [1] angegeben , jedoch ohne Abschätzung des Fehlergliedes. Dazu werden erst alle Produkte aus Variablen und negierten Variablen berechnet. Diese $2^n$ Produkte werden in $\lceil 2^n/p \rceil$ Gruppen zu je p Stück geteilt. In jeder Gruppe werden alle Linearkombinationen berechnet , aus denen dann durch Addition die t Ergebnisse zusammengesetzt werden. Es kommt die Schranke des Lemmas heraus, die jedoch nur für große t gut ist. Deshalb der folgende Satz.

Satz 2

Für die Komplexität L(F) einer Menge Boolescher Funktionen F aus $M_{t,n}$ gilt

$$L(F) \leq \frac{t2^n}{\mathrm{ldt}2^n} \left( 1 + c \, \frac{\mathrm{ldldt}2^n}{\mathrm{ldt}2^n} \right) .$$

Darin ist c eine von n und t unabhängige Konstante.

Der Beweis ist für eine Funktion ohne Abschätzung des Fehlergliedes in [1] gegeben. Es muß jedoch der Parameter m genauer gewählt und schärfer abgeschätzt werden, damit das Verfahren für Mengen F kleiner Mächtigkeit zum Ziel führt. Für große F reicht schon Lemma 1 aus. Eine Berechnung von $F = \{f_1,\ldots,f_t\} \in M_{t,n}$ ist gegeben durch die Zerlegung

$$f_i(x_1,\ldots,x_n) = \sum_{e_{m+1},\ldots,e_n \in \{0,1\}} g^{(i)}_{e_{m+1},\ldots,e_n}(x_1,\ldots,x_m) \cdot x_{m+1}^{e_{m+1}} \ldots x_n^{e_n} ,$$

worin die Funktionenmenge $G = \{g^{(i)}_{\ldots}(\ldots)\}$ in $M_{s,m}$ mit $s \leq t2^{n-m}$ liegt. G wird nach dem Lemma 1 berechnet und F aus G und den restlichen Variablen gemäß der Zerlegung.

Nun soll eine untere Schranke für L(F) von der gleichen Größenordnung gezeigt werden, wozu jedoch zwei Ausnahmen zu machen sind. Einmal müssen allzu einfache Funktionen ausgenommen werden, die aber nur selten auftreten. Außerdem führt die angewendete Abzählung der Berechnungen nur für relativ kleine Mengen F zum Ziel. Deshalb die zwei folgenden Definitionen.

$$M = \bigcup_{t \leq 2^{2^{n/4}}} M_{t,n}$$

$N \subset M$ heißt Nullmenge, wenn

$$\lim_{t2^n \to \infty} \frac{|M_{t,n} \cap N|}{|M_{t,n}|} = o .$$

Satz 3

Für fast alle $F$ aus $M$ , d. h. für alle außerhalb einer Nullmenge $N$ , gilt

$$L(F) \geq \frac{t2^n}{\mathrm{ld}t2^n} \left( 1 - \frac{\mathrm{ldld}t2^n}{\mathrm{ld}t2^n} \right) ,$$

falls $F$ aus $M_{t,n}$.

Zum Beweis des Satzes werden alle $F$ aus $M$ , für die die Ungleichung nicht gilt zur Menge $N$ zusammengefaßt. Es bleibt zu zeigen , daß $N$ eine Nullmenge ist , wozu die normalen Berechnungen mit vorgegebener Länge wie in [1] abgezählt werden.

Nun ist eine obere und eine untere Schranke für die Komplexität von Mengen Boolescher Funktionen angegeben. Weiterhin ist die Lücke zwischen diesen beiden Schranken klein und bekannt , so daß es nun möglich ist, Ersparnisse bei gemeinsamer Berechnung anzugeben. Definiert man etwa die Ersparnis durch

$$E = \frac{L(f_1)+\ldots+L(f_t) - L(f_1,\ldots,f_t)}{t2^n/n}$$

so kommt

$$E \gtrless \frac{\mathrm{ld}t}{n+\mathrm{ld}t} \mp 2c \frac{\mathrm{ld}n}{n}$$

heraus. Genaue Angaben über die Ersparnis sind also nur möglich, wenn ldt $\gg$ ldn ist. So erhält man etwa bei gemeinsamer Berechnung von $2^n$ Funktionen , die nicht in der Nullmenge liegen , für große n eine Ersparnis von genau 50%. Selbst bei Berechnung von relativ wenig Funktionen im Vergleich zu allen kann man also erheblich sparen.

[1] V. STRASSEN:
Berechnungen in partiellen Algebren endlichen Typs
Computing 11/3

[2] D. E. MULLER:
Complexity in Electronic Switching Circuits
IRE Transactions on Electronic Computers, March 1956

[3] H. BREMER:
Berechnungskomplexität von Mengen Boolescher Funktionen
und von Polynomen über endlichen Körpern
Diplomarbeit, Institut für angewandte Mathematik an der
Johann Wolfgang Goethe Universität in Frankfurt