Untere Schranke für die Paritätsfunktion

bearbeitet von Christian Stahl

Gliederung

1. Motivation

Die Frage nach der Existenz bzw. Nicht-Existenz von kombinatorischen Schaltkreisen für die Paritätsfunktion ist seit langem untersucht worden, da sich viele andere Funktionen mit Hilfe der Paritätsfunktion ausdrücken bzw. auf diese zurückführen lassen.
1984 wurde von Furst, Saxe und Sipser die Methode der „probabilistischen Restriktion“ eingeführt. Mit dieser Methode konnte bewiesen werden, dass die Paritätsfunktion sich nicht durch UND-ODER Schaltkreise polynomialer Grösse und konstanter Tiefe berechnen lässt.
Probabilistisch bedeutet hier, das Fixieren der Variablen, die dann ebenso wie die Werte zufällig gewählt werden. Die Restriktion ist in diesem Beweis die Einschränkung des Definitionsbereiches, so dass der eingeschränkte Definitionsbereiches ebenfalls die Paritätsfunktion berechnet.

2. Definition der Paritätsfunktion

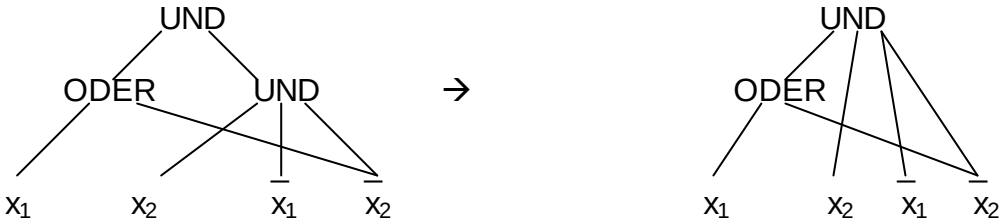
Unter der *Paritätsfunktion*, kurz: PARITY, verstehen wir die unendliche Folge von Funktionen $par_n : \{0, 1\}^n \rightarrow \{0, 1\}$, n = 1, 2, ... mit

$$par_n(x_1,\ldots,x_n) = \left(\sum_{i=1}^{n} x_i\right) \bmod 2$$

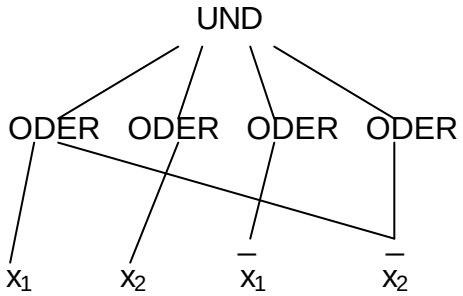
Wir betrachten im folgenden eine Art von Schaltkreis, der nur aus UND- und ODER-Gattern mit unbeschränktem Fan-in besteht. Eingänge dieses Schaltkreises sind sowohl Variablen x_i als auch ihre Negation $\overline{x_i}$.

3. Eigenschaften der UND-ODER-Schaltkreise

Direkt aufeinanderfolgende Gatter desselben Typs können miteinander verschmolzen werden, ohne das sich die vom Schaltkreis zu berechnende Funktion ändert.



Weiterhin können Schaltkreise dieser Art in eine gewisse normalisierte („Schichten“-) Form gebracht werden, indem man gegebenfalls künstlich durch Gatter mit Fan-in = 1 auffüllt.



Unser Schaltkreis hat nun (von unten nach oben) auf der ersten Schicht nur ODER-Gatter, auf der zweiten Schicht nur UND-Gatter, und gegebenenfalls alternierend immer so weiter.

Hinweis 1:

Alle n-stelligen Booleschen Funktionen lassen sich durch einen 2-schichtigen Schaltkreis berechnen, dessen Grösse im allgemeinen exponential ist.
Dies gilt, da sich jede n-stellige Boolesche Funktion äquivalent in DNF bzw. KNF umformen lässt, die einem 2-schichtigen ODER-UND bzw. UND-ODER-Schaltkreis entsprechen.

Hinweis 2:

Mittels der Distributivgesetze der Booleschen Algebra

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

lassen sich 2-schichtige UND-ODER-Schaltkreise in 2-schichtige ODER-UND-Schaltkreise umformen.
Beispiel:

$$(x_1 \vee \overline{x_2}) \wedge (x_2) \wedge (\overline{x_1}) \wedge (\overline{x_2})$$

$$\Leftrightarrow (x_2 \wedge \overline{x_1} \wedge \overline{x_2}) \wedge (x_1 \vee \overline{x_2})$$

$$\Leftrightarrow_{Distrib} (x_2 \wedge \overline{x_1} \wedge \overline{x_2} \wedge x_1) \vee (x_2 \wedge \overline{x_1} \wedge \overline{x_2} \wedge \overline{x_2})$$

Hinweis 3:

Bei der Umformung eines 2-schichtigen UND-ODER-Schaltkreises mit

- alle ODER-Gatter der ersten Schicht haben in Fan-in von c

- das UND-Gatter der zweiten Schicht hat ein Fan-in von d

erhält man einen ODER-UND-Schaltkreis dessen Fan-in bei den UND-Gattern auf der ersten Stufe d ist und beim ODER-Gatter auf der zweiten Stufe c^d ist.

Ein allgemeiner Beweisansatz wäre:

$$(x_{11} \vee \ldots \vee x_{1c}) \wedge \ldots \wedge (x_{d1} \vee \ldots \vee x_{dc})$$

ausmultiplizieren :

$$(x_{11} \wedge x_{21} \wedge x_{31} \ldots \wedge x_{d1}) \vee (x_{11} \wedge x_{22} \wedge x_{31} \ldots \wedge x_{d1}) \vee \ldots \vee$$
$$(x_{11} \wedge x_{21} \wedge \ldots \wedge x_{d1}) \vee \ldots \vee (x_{1c} \wedge \ldots \wedge x_{d1}) \vee \ldots \vee \underbrace{(x_{1c} \wedge \ldots \wedge x_{dc})}_{d}$$

Hinweis 4:

Angenommen es gibt einen Schaltkreis für das Komplement der Paritätsfunktion, $\overline{par_n}$, der aus t Schichten und g Gattern besteht. Dann gibt es auch einen Schaltkreis mit t Schichten und g Gattern der par_n berechnet.

Diesen Schaltkreis erhält man durch Anwendung der de Morgan'schen Regeln

$$\overline{x \vee y} = \overline{x} \wedge \overline{y}$$
$$\overline{x \wedge y} = \overline{x} \vee \overline{y}$$

auf $\overline{par_n}$. Speziell für die Paritätsfunktion gilt aufgrund der Gleichheit $\overline{par(x_1,\ldots,x_n)} = par(\overline{x_1},\ldots,x_n)$, dass nur alle x_1 Eingänge durch $\overline{x_1}$ und umgekehrt vertauscht werden brauchen.

Hinweis 5:

Angenommen, wir haben einen Schaltkreis für par_n gegeben. Setzt man nun einige der x_i auf 0 und andere auf 1, kann man, falls ein ODER-Gatter einen Eingang erhalten hat, der 1 bzw. ein UND-Gatter dessen Eingang 0 ist, das jeweilige Gatter eliminieren und durch 1 bzw. 0 ersetzen. Dieser reduzierte Schaltkreis entspricht wieder der Paritätsfunktion bzw. deren Komplement mit entsprechend weniger Eingangsvariablen.

Dies gilt, weil

$$par_n(0, x_2,\ldots,x_n) = par_{n-1}(x_2,\ldots,x_n)$$
$$par_n(1, x_2,\ldots,x_n) = \overline{par_{n-1}}(x_2,\ldots,x_n) \quad .$$

4. Einführung in den Beweis

Die Frage lautet jetzt:

> Gibt es eine Konstante t und ein Polynom p, so dass sich für alle n die Boolesche Funktion par_n durch einen t-stufigen Schaltkreis mit höchstens p(n) Gattern berechnen lässt?

Man beachte, dass t mit wachsendem n nicht mitwachsen darf, sondern konstant ist.

Hinweis 6:

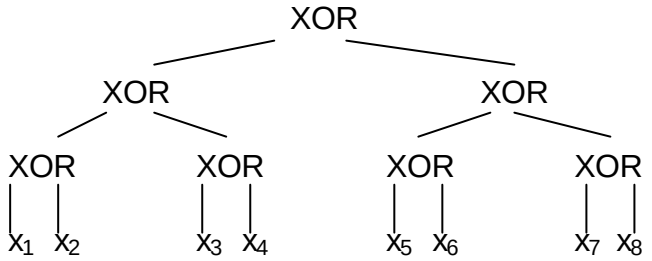
PARITY kann nicht durch 2-stufige ODER-UND-Schaltkreise mit polynomialer Grösse berechnet werden.

Man zeigt zuerst, dass jedes UND-Gatter auf Stufe 1 in einem 2-stufigen Schaltkreis für par_n die Eingangszahl n haben muss, d.h. jede Variable oder ihr Komplement muss einen Eingang bilden. Angenommen wir haben ein UND-Gatter, wo o.B.d.A. die Variable x_n fehlt. Die vorhandenen Eingänge sind $x_1^{i_1},...,x_{n-1}^{i_{n-1}}$ mit $i_j \in \{-1,+1\}$. Dieses UND-Gatter liefert also eine 1 (und damit der Schaltkreis insgesamt eine 1), wenn wir $x_j = 1$ setzen genau dann, wenn $i_j = 1$ (j = 1, ..., n-1). Wenn wir nun x_n wahlweise mit 0 oder 1 belegen, ändert sich an der Situation des UND-Gatters nichts. Daher ist der Schaltkreis inkorrekt, wir erhalten einen Widerspruch und unsere Annahme ist damit falsch. Jedes UND-Gatter muss somit n Eingänge haben und deshalb gibt es 2^n Belegungen von denen die Hälfte, also 2^{n-1} Belegungen wahr ergeben ($par_n = 1$). Somit hat das ODER-Gatter 2^{n-1} Eingänge = Anzahl der UND-Gatter.

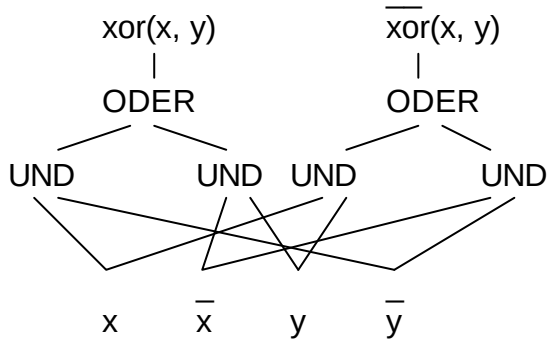
Hinweis 7:

PARITY lässt sich mittels O(log n)-stufiger Schaltkreise mit polynomialer Grösse berechnen.

Man kann zeigen, dass sich mit einem XOR-Gatter mit 2 Eingängen die Parität in Form eines balancierten Baumes berechnen lässt.



Jedes XOR-Gatter kann jetzt durch UND- und ODER-Gatter ersetzt werden, wobei allerdings am Eingang und am Ausgang das eigentliche Signal und das komplementäre Signal bereit gestellt wird.



Wir kommen hierbei mit UND- und ODER-Gatter mit einem konstantem Fan-in = 2 aus. Die Booleschen Funktionen, die sich durch konstantes Fan-in und Tiefe $O((\log n)^k)$ berechnen lassen, fasst man in der Klasse NC^k zusammen. Tatsächlich haben wir $PARITY \in NC^1$ gezeigt. Es gilt:

$L \in NC^k \Leftrightarrow \forall n \exists Schaltkreis\, C\ polynomialer\ Grösse, Tiefe\, O\left((\log n)^k\right)$

$\Rightarrow Tiefe\left(NC^1\right) \leq p(\log n)$

$\text{Tiefe} = \text{konstant} \Rightarrow \text{Schaltkreisgrösse exponentiell}$

$\text{Tiefe} = \log \text{n} \Rightarrow \text{Schaltkreisgrösse polynomial}$

Mit der Komplexitätsklasse AC^k fassen wir alle Booleschen Funktionen zusammen, die sich durch $O((\log n)^k)$-stufige Schaltkreise polynomialer Grösse berechnen lassen, wobei die UND- und ODER-Gatter unbeschränktes Fan-in haben. Hinweis 7 zeigt, dass $PARITY \in AC^1$. Wir wollen zeigen, dass $PARITY \notin AC^0$ gilt. Man beachte, dass $O((\log n)^0) = O(1)$. Hinweis 7 bildet hierfür den Induktionsanfang.
Der Beweis gelang Furst, Saxe und Sipser[1] mit der oben erwähnten Beweistechnik der „probabilistischen Reduktion". Technisch verbessert – und zwar von „nicht-polynomial" zu „mindestens exponential" – wurde das Resultat später noch von Yao und dann von Hastad[2], dessen Beweis als der wesentliche Durchbruch angesehen wird.
Wir werden im folgenden die Furst - Saxe - Sipser Version nachvollziehen. Dafür benötigt man etwas Wahrscheinlichkeitsrechnung. Ein Zufallsexperiment mit zwei möglichen Ausgängen, wobei mit der Wahrscheinlichkeit p „Erfolg" und mit der Wahrscheinlichkeit (1 – p) „Misserfolg" eintritt, hat, wenn man es n-mal unabhängig wiederholt, eine Wahrscheinlichkeit für genau k-mal Erfolg von $\binom{n}{k} p^k q^{n-k}$ (Binomialverteilung).

Hinweis 8:

Sei X die Zufallsvariable, die angibt, wie oft man bei n Versuchen Erfolg hat. Dann haben der Erwartungswert E(X) und die Varianz V(X) folgende Grösse:

Sei Y_i die Zufallsvariable, die den Wert 1 erhält, wenn im i-ten Versuch Erfolg vorliegt, sonst 0.
$E(Y_i) = 1 * p + 0 * (1 - p) = p$
Somit gilt:

$E(X) = E\left(\sum_{i=1}^{n} Y_i\right) = \sum_{i=1}^{n} E(Y_i) = \underline{n * p}$

$V(X) = E((X - E(X))^2) = E(X^2) - E(X)^2$

$$= E\left(\left(\sum_{i=1}^{n} Y_i\right)^2\right) - (np)^2$$

$$= E\left(\sum_{i=1}^{n}\sum_{j=1}^{n} Y_i Y_j\right) - (np)^2$$

$$= \underbrace{\text{n} * (n\text{-}1) * p^2}_{\text{i} \neq \text{j}} + \underbrace{n * p}_{i=j} - (n * p)^2 \quad \left(\rightarrow \text{E}(x_i, x_j) = p^2 \text{ für i} \neq \text{j}\right)$$

$$= \underline{n * p * (1 - p)}$$

[1] Parity, circuits, and the polynomial-time hierarchy, Mathematical Systems Theory 17 (1984) 13-27
[2] Almost optimal lower bounds for small depth circuits, Proc. Of the 18th Annual ANC Symposium on Theory of Computing, 1986, 6-12

Hinweis 9:

Die Tschebyscheff-Ungleichung lautet:

$$\Pr\left[\left|X - E(X)\right| \geq a\right] \leq \frac{V(X)}{a^2}, a \in \Re^+$$

Beispiel: (Aufgabe 111)

$\Pr[X \leq 17]$ für $n = 100, p = 0{,}3$

$$\begin{aligned}\Pr[X \leq 17] &\leq \Pr\left[\left|X - E(X)\right| \geq 13\right] \\ &= \left|17 - 0{,}3 * 100\right| \\ &\leq \frac{V(X)}{13^2} \\ &\leq \frac{100 * 0{,}3 * 0{,}7}{169} \\ &= 0{,}124\end{aligned}$$

Hinweis 10:

Eine weitere Abschätzung zur Binomialverteilung, die sich allerdings nur dann sinnvoll einsetzen lässt, wenn die rechte Seite kleiner 1 wird:

$$\Pr[X \geq a] \leq p^a * 2^n$$

Beweis:

$$\begin{aligned}\Pr[X \geq a] &= \sum_{i=a}^{n} \binom{n}{i} p^i (1-p)^{n-i} \quad \text{(Binomialv erteilung)} \\ &\leq \sum_{i=a}^{n} \binom{n}{i} p^i \\ &\leq p^a \sum_{i=a}^{n} \binom{n}{i} \quad \text{(wegen } p \leq 1\text{)} \\ &\leq \underline{p^a * 2^n} \quad \text{(wegen *)}\end{aligned}$$

* Binomische r Satz :

$$\begin{aligned}(a+b)^n &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \ldots + \binom{n}{n} b^n \\ (1+1)^n &= \binom{n}{a} 1^n + \binom{n}{a+1} 1^{n-1} 1 + \ldots + \binom{n}{n} 1^n \\ 2^n &= \sum_{i=a}^{n} \binom{n}{i}\end{aligned}$$

Es lässt sich eine noch bessere Abschätzung zeigen:

$$\Pr[X \geq a] = \sum_{i=a}^{n} \binom{n}{i} p^i (1-p)^{n-i} \quad \text{(Binomialv erteilung)}$$

$$= \sum_{i=0}^{n-a} \binom{n}{a+i} p^{a+i} (1-p)^{n-a-i}$$

$$\leq \sum_{i=0}^{n-a} \binom{n}{a} \binom{n-a}{i} p^{a+i} (1-p)^{n-a-i} \quad \text{(folgt weg en *)}$$

$$= \binom{n}{a} p^a \sum_{i=0}^{n-a} \binom{n-a}{i} p^i (1-p)^{n-a-i}$$

$$= \binom{n}{a} p^a \quad \text{(folgt weg en **)}$$

$$\leq n^a p^a \quad \text{(folgt weg en ***)}$$

$$= \underline{(np)^a}$$

* Nebenrechnung :

$$\binom{n}{a+1} \leq \binom{n}{a} \binom{n-a}{i}$$

nach Def :

$$\frac{n!}{(a+i)! * (n-a-i)!} \leq \frac{n!}{a!(n-a)!} * \frac{(n-a)!}{i! * (n-a-i)!} = \frac{n!}{a! * i! * (n-a-i)!}$$

$$\Leftrightarrow \frac{1}{(a+i)!} \leq \frac{1}{a! * i!}$$

$$\Leftrightarrow (a+i)! \geq a! * i!$$

** Nebenrechnung :

$$1 = \sum_{i=0}^{n-a} \binom{n-a}{i} p^i (1-p)^{n-a-i}$$

mit dem Binomische n Satz

$$(p + (1-p))^{n-a} = \binom{n-a}{0} p^0 (1-p)^{n-a} + \ldots + \binom{n-a}{n-a} p^{n-a} (1-p)^0$$

$$= 1^{n-a}$$

$$= 1$$

*** Nebenrechnung :

$$\binom{n}{a} p^a \leq n^a p^a \quad \text{(wegen } p^a > 0)$$

$$\binom{n}{a} \leq n^a$$

$$\frac{n!}{a! * (n-a)!} = \frac{n * (n-1) * \ldots * (n-a+1)}{a!} \leq n^a$$

5. Der Beweis

Jetzt wollen wir zeigen, dass PARITY nicht von Schaltkreisen mit unbeschränkten Fan-in, polynomialer Grösse und konstanter Tiefe berechnet werden kann. Dazu genügt es die folgende (schwächere) Behauptung zu beweisen.

Behauptung:

$$\forall t\ \forall c\ \forall \text{Polynome } p: \text{PARITY lässt sich nicht durch } t\text{-stufige Schaltkreise der Grösse } p(n) \text{ mit Eingangs-fan-in} \le c \text{ (d.h. konstantes Fan-in auf Stufe 1) berechnen.}$$

Satz: $PARITY \notin AC^0$
(denn AC^0 hat kein konstantes Fan-in auf Stufe 1)

Beweis des Satzes:
Der Satz ist eine direkte Folgerung aus der Behauptung.
Angenommen, es gibt eine Folge von Schaltkreisen für PARITY, die aus t Schichten und polynomialer Grösse bestehen. In dem wir künstlich eine weitere erste Schicht aus Gattern mit Fan-in 1 hinzufügen, erhält man (t + 1)-stufige Schaltkreise polynomialer Grösse und konstantem Eingangs-fan-in. Das widerspricht der Behauptung.

Beweis der Behauptung:

Im Hinweis 6 haben wir bereits die Behauptung für den Fall t = 2 bewiesen. Dabei haben wir gezeigt, dass weder das Eingangs-fan-in konstant sein kann, noch die Grösse des Schaltkreises polynomial sein kann.

Beweisidee:
Wir treffen die Annahme, die Behauptung ist falsch und bauen uns ein Schema zurecht, um die Annahme Widerspruch zu führen. Die Wahrscheinlichkeiten für gewisse unerwünschte Restriktionen werden wir nach oben durch eine Funktion, die für $n \to \infty$ gegen Null strebt, abschätzen. Dann bleibt die Wahrscheinlichkeit für das Auftreten mindestens einer dieser endlich vielen unerwünschten Fälle echt kleiner als 1. Damit können wir zeigen, dass für jedes n eine Restriktion existiert, die nur erwünschte Eigenschaften hat und zeigen damit, dass unser Schema eintreten kann. Angenommen die Behauptung ist falsch. Dann gibt es eine Tiefe t > 2, so dass sich die Parität durch t-stufige, polynomial-grosse Schaltkreise berechnen lässt, die ein konstantes Eingangs-fan-in haben. Dabei sei t minimal gewählt. Das Polynom, das die Schaltkreisgrösse beschränkt, habe echt kleineren Grad als k, und die Konstante für das Eingangs-fan-in sei c. Wir werden zeigen, dass es dann auch entsprechende (t – 1)-stufige Schaltkreise polynomialer Grösse mit konstantem Eingangs-fan-in gibt, die PARITY berechnen. Das Polynom für die Grösse dieser Schaltkreise wird einen Grad grösser k haben und die Konstante für das Eingangs-fan-in grösser als c sein. Damit haben wir eine Widerspruch zur Minimalität von t und somit die Behauptung bewiesen.

Wir gehen wie folgt vor:
Wenn $S_1, S_2, S_3, \ldots$ die fiktiven t-stufigen Schaltkreise für PARITY sind (S_i sind Schaltkreise für PARITY in Abhängigkeit der Eingangsvariable), konstruieren wir eine neue (t – 1)-stufige Schaltkreisfolge $S_1', S_2', S_3', \ldots$, indem wir zur Konstruktion von S_n'

einen Schaltkreis der S-Folge mit mehr als n Variablen heranziehen, etwa den Schaltkreis S_{4n^2}, dann wie im Hinweis 5 besprochen, „geeignete“ $4n^2 - n$ Variablen durch Konstanten $\in \{0,1\}$ ersetzen, so dass n Eingangsvariablen übrigbleiben. Dieser Schaltkreis sollte so beschaffen sein, dass sich mittels Distributivgesetz (siehe Hinweis 2) die Anordnung der UND- bzw. ODER-Gatter auf Stufe 1 und 2 vertauschen lässt, ohne das sich der Schaltkreis in seiner Grösse exponentiell aufbläht. Hierzu genügt es zu zeigen, dass nach der Restriktion alle Gatter der 2.Schicht nur von konstant vielen Eingangsvariablen abhängen. Nach Anwenden des Distributivgesetzes wird ein konstantes neues Eingangs-fan-in garantiert, denn nur konstant viele Eingänge gehen in den Exponenten (hier: n). Somit haben wir lediglich ein polynomiales Wachsen der Schaltkreisgrösse. Nach dieser Umkonstruktion sind die Gatter in der Schicht 2 und 3 vom selben Typ und können daher jeweils in ein einziges Gatter dieses Typs verschmolzen werden. Der entstehende Schaltkreis hat dann eine Schicht weniger, also t – 1 Schichten.
Die Frage ist jetzt, wie soll man solche „geeigneten“ $4n^2 - n$ Variablen finden, die durch Konstanten ersetzt werden? Wir führen hierzu eine Zufallssubstitution oder -restriktion durch, d.h. wenn die Wahrscheinlichkeit für das Entstehen eines geeigneten Schaltkreises $S_n^{'}$ positiv ist, schliessen wir, dass es eine geeignete Substitution gibt. Wir verwenden folgende Zufallsrestriktion r : Für jede Variable x_i wird unabhängig von den anderen Variablen ein Zufallsexperiment ausgeführt, das 3 mögliche Ausgänge hat:

$$x_i^r = \begin{cases} x_i, \text{mit } P(x_i^r) = \frac{1}{\sqrt{n}} \\ 0, \text{mit } P(x_i^r) = \frac{1-\frac{1}{\sqrt{n}}}{2} \\ 1, \text{mit } P(x_i^r) = \frac{1-\frac{1}{\sqrt{n}}}{2} \end{cases} .$$

$x_i^r \in \{x_i, 0, 1\}$ x_i^r ist Resultat von x_i nach Zufallsrestriktion r

Wie kommt man auf diese Wahrscheinlichkeiten? Dabei ist eine Randbedingung, dass die Wahrscheinlichkeiten für 0 und 1 gleich gross sein sollten, damit aus Dualitätsgründen UND- und ODER-Gatter auch vertauscht werden können. Weiterhin zeigt sich bei den folgenden Wahrscheinlichkeitsabschätzungen, dass es günstig ist, die Wahrscheinlichkeit für das Bestehenbleiben einer Variablen möglichst klein anzusetzen. Dabei darf diese Wahrscheinlichkeit nur polynomial kleiner sein als n.
S^r bezeichnet den Schaltkreis S nach Ausführen der Zufallsrestriktion. Wegen Hinweis 5 ist klar, dass S^r wieder eine Paritätsfunktion – oder deren Komplement - in entsprechend weniger Variablen berechnet. Mit Hinweis 4 folgt, dass es dann auch einen Schaltkreis für die Paritätsfunktion derselben Tiefe und Grösse gibt. Mit Hilfe von Hinweis 8 errechnet man den Erwartungswert für die Anzahl der verbleibenden Variablen in S_n^r und die Varianz:

$$E(X) = n * p = n * \frac{1}{\sqrt{n}} = \sqrt{n}$$

$$V(X) = n * p * (1-p) = n * \frac{1}{\sqrt{n}} * \left(1 - \frac{1}{\sqrt{n}}\right) \leq \sqrt{n}$$

Die Anzahl der tatsächlich verbleibenden Variablen sollte noch in umgekehrt polynomialen Verhältnis zu der ursprünglichen Variablenanzahl n stehen und nicht exponential abnehmen, sonst könnte man die Grösse des entstehenden Schaltkreises nach oben nicht polynomial in der verbleibenden Variablenzahl abschätzen.

Man kann zeigen das $\Pr\left[\text{es bleiben we niger als } \frac{\sqrt{n}}{2} \text{ Variablen in } S_n^r \text{ übrig}\right] = O\left(\frac{1}{\sqrt{n}}\right)$ (Hinweis 11).

Mit Hilfe der Tschebyscheff-Ungleichung (Hinweis 9) erhält man

X - Zufallsvariable, die die Anzahl der verbleibenden Variablen in S_n^r angibt

$$\Pr\left[\text{es bleiben we niger als } \frac{\sqrt{n}}{2} \text{ Variablen in } S_n^r \text{ übrig}\right] \le \Pr\left[\left|X - E(X)\right| \ge \frac{\sqrt{n}}{2}\right]$$

$$\le \frac{V(X)}{\left(\frac{\sqrt{n}}{2}\right)^2}$$

$$= \frac{\sqrt{n}}{\left(\frac{\sqrt{n}}{2}\right)^2}$$

$$= O\left(\frac{1}{\sqrt{n}}\right)$$

Das heisst, mit hoher Wahrscheinlichkeit bleiben mehr als $\frac{\sqrt{n}}{2}$ viele Variablen übrig.

Aus der Folge $S_1, S_2, S_3, \ldots$ erhält man nach der Zufallsrestriktion eine lückenlose Folge $S_1', S_2', S_3', \ldots$ (Hinweis 12).

Dazu muss man zeigen, dass für jedes n ein Schaltkreis mit genau n Eingängen gefunden werden kann. Sei n gegeben. Wir betrachten als Ausgangsschaltkreis S_{4n^2}.

Mit Wahrscheinlichkeit von grösser 0 hat $S_{4n^2}^r$ nach Hinweis 11 mindestens $\frac{\sqrt{4n^2}}{2} = n$ verbleibende Variablen. Also existiert ein Schaltkreis, der $m \ge n$ Eingänge hat, wobei $m \le 4n^2$. Die Grösse des Schaltkreises ist $O\left(\left(4n^2\right)^k\right) = O\left(n^{2k}\right)$. Indem wir nun m – n beliebige Eingabevariablen auf 0 festlegen, erhalten wir den gewünschten Schaltkreis polynomialer Grösse mit genau n Eingängen.

Als nächstes zeigen wir, dass die Gatter der 2. Schicht mit hoher Wahrscheinlichkeit nach der Restriktion nur von konstant vielen Eingangsvariablen abhängen. Wir treffen dabei die Annahme, dass die Gatter der 1. Schicht ODER-Gatter und der 2. Schicht UND-Gatter sind. Das funktioniert, weil nach dem Dualitätsprinzip UND-ODER, 0-1, bzw. $x_i - \overline{x_i}$ miteinander vertauscht werden können.

Wir greifen uns ein beliebiges, festes UND-Gatter der 2. Schicht heraus und zeigen, dass der unerwünschte Effekt – die Abhängigkeit von zu vielen Variablen – höchstens mit der Wahrscheinlichkeit $O\left(\frac{1}{n^k}\right)$ auftritt. Da nach Voraussetzung das Polynom, das die Schaltkreisgrösse beschränkt einen Grad < k hat, gibt es insgesamt nur

$O(n^{k-1})$ Gatter. Deswegen tritt der unerwünschte Effekt an irgendeinem UND-Gatter mit einer Wahrscheinlichkeit von $O\left(\frac{1}{n^k} * n^{k-1}\right) = O\left(\frac{1}{n}\right)$ auf. Somit haben alle UND-Gatter der 2. Schicht mit hoher Wahrscheinlichkeit die gewünschten Eigenschaften.

Behauptung:

Für jeden UND-ODER-Schaltkreis, dessen Eingangs-fan-in bei den ODER-Gattern durch c beschränkt ist, gibt es eine Konstante $e = e_c$, so dass die Wahrscheinlichkeit, dass das UND-Gatter nach der Zufallsrestriktion von mehr als e Variablen abhängt, höchstens $O\left(\frac{1}{n^k}\right)$ ist.

Beweis: Induktion nach c

Induktionsanfang (c = 1):

Die ODER-Gatter entfallen und wir haben es nur mit den UND-Gattern zu tun. Wir unterscheiden 2 Fälle, je nachdem, ob das UND-Gatter im ursprünglichen Zustand vor der Zufallsrestriktion „weitgefächert“ ist oder nicht.

Induktionsanfang-Fall 1: Das UND-Gatter hat mindestens (4*k*ln n) Eingänge.

Es ist sehr wahrscheinlich, dass mindestens eine Eingangsvariable den Wert 0 erhält und damit das UND-Gatter zu 0 wird – das UND-Gatter hängt dann von 0 Variablen ab. Dazu zeigen wir:

$\Pr[\text{UND} - \text{Gatter wir d nicht zu } 0] = O\left(\frac{1}{n^k}\right)$ (Hinweis 13), denn

$$\Pr[\text{Und - Gatter wird nicht zu } 0]$$
$$\leq \Pr[\text{alle Eingänge werden} \neq 0]$$
$$\leq \Pr[\text{ein beliebiger fester Eingang wird nicht } 0]^{4*k*\ln n}$$
$$= \left(1 - \frac{1 - \frac{1}{\sqrt{n}}}{2}\right)^{4*k*\ln n} \qquad (= (1 - P(0)))$$
$$= \left(\frac{1}{2} + \frac{1}{2*\sqrt{n}}\right)^{4*k*\ln n}$$
$$\leq \left(\frac{3}{4}\right)^{4*k*\ln n} \qquad (\text{für } n \geq 4 \text{ wegen } *)$$
$$= n^{4*k*\ln\left(\frac{3}{4}\right)} \qquad (\text{wegen } **)$$
$$\underline{\leq n^{-k}}$$

$$*: \left(\frac{3}{4}\right)^{4*k*\ln n} = e^{\ln\left(\frac{3}{4}\right)^{4*k*\ln n}}$$
$$= e^{4*k*\left(\ln\frac{3}{4}\right)*\ln n}$$
$$= e^{(\ln n)^{4*k*\left(\ln\frac{3}{4}\right)}}$$
$$= n^{4*k*\left(\ln\frac{3}{4}\right)} \qquad \left(\Rightarrow a^{\ln b} = b^{\ln a}\right)$$
$$**: 4*k*\left(\ln\frac{3}{4}\right) = k*\underbrace{(4*\ln 3 - 4*\ln 4)}_{<-1}$$

Induktionsanfang-Fall 2: Das UND-Gatter hat weniger als (4*k*ln n) Eingänge.

Es ist sehr wahrscheinlich, dass durch die Zufallsrestriktion nur noch konstant viele Variablen übrigbleiben, denn für den Erwartungswert für die Anzahl X der verbleibenden Variablen gilt: $E(X) \leq (4 + k*\ln n)*\left(\frac{1}{\sqrt{n}}\right) \xrightarrow[n\to\infty]{} 0$. Wir können zeigen:

$\Pr[\text{UND - Gatter hängt von mehr als } 10*\text{k Eingaben ab}] = O\left(\frac{1}{n^k}\right)$ (Hinweis 14), denn

$$\Pr[\text{UND-Gatter hängt von mehr als a Variablen ab}]$$

$$\leq \sum_{i=a}^{4k*\ln n} \binom{4k*\ln n}{i} * \left(\frac{1}{\sqrt{n}}\right)^i * \left(1-\frac{1}{\sqrt{n}}\right)^{n-i}$$

$$\leq \left(\frac{1}{\sqrt{n}}\right)^a * 2^{4*k*\ln n} \qquad \text{(Hinweis 10)}$$

$$\leq n^{-\frac{a}{2}} * n^{4*k}$$

$$= n^{4*k-\frac{a}{2}}$$

$$\rightarrow 4*k-\frac{a}{2} = -k \Leftrightarrow a = 10k$$

Die 10k sind uninteressant, wichtig ist, dass der Wert konstant also unabhängig von n ist.

Induktionsschritt: Schliesse von e_{c-1} auf e_c

Induktionsschritt-Fall 1: Das UND-Gatter der 2. Schicht hat vor der Zufallsrestriktion mindestens d*ln n viele ODER-Gatter mit variablendisjunkten Eingängen unter sich, wobei d = $k*4^c$.

Wir zeigen, dass es sehr wahrscheinlich ist, dass eines der ODER-Gatter nach der Zufallsrestriktion nur Nullen an den Eingängen hat, damit insgesamt den Wert 0 erhält, wodurch das UND-Gatter den Wert 0 annimmt. In diesem Fall hängt das UND-Gatter von keiner Variablen ab, und die Behauptung ist gezeigt. (Alle ODER-Gatter der 1. Schicht haben nach Voraussetzung höchstens c viele Eingangsvariable.)
Wir zeigen:

$\Pr[\text{das UND-Gatter wir d nicht konstant} = 0] = O\left(\frac{1}{n^k}\right)$ (Hinweis 15), denn

$$\Pr[\text{das UND - Gatter wir d nicht konstant} = 0]$$
$$\leq \Pr[\text{keines der ODER - Gatter erhält den Wert } 0]$$
$$\leq (\Pr[\text{ein beliebiges , festes ODER - Gatter erhält nicht den Wert } 0])^{d*\ln n}$$
$$\leq \left(1 - \frac{1}{2*\sqrt{n}}^{-c}\right)^{d*\ln n}$$
$$\leq \left(1 - 4^{-c}\right)^{d*\ln n} \quad (\text{für } n \geq 4)$$
$$= n^{d*\ln\left(1-4^{-c}\right)} \quad (\text{wegen } *)$$
$$\leq n^{-d*4^{-c}} \quad (\text{wegen } **)$$
$$\leq \underline{n^{-k}} \quad \left(\text{wegen } d = k*4^{c}\right)$$

$*$: $\left(1-4^{-c}\right)^{d*\ln n} = e^{\ln\left(1-4^{-c}\right)^{d*\ln n}}$
$$= e^{d*\ln\left(1-4^{-c}\right)*\ln n}$$
$$= e^{(\ln n)^{d*\ln\left(1-4^{-c}\right)}}$$
$$= n^{d*\ln\left(1-4^{-c}\right)}$$

$**$: $d * \underbrace{\ln\left(\underbrace{1-4^{-c}}_{<1,\, da\ c>0}\right)}_{<0} \leq -d*4^{-c}$

es gilt : $\ln(1 - x) \leq -x$

Induktionsschritt-Fall 2: Es gibt vor der Zufallsrestriktion weniger als d*ln n viele ODER-Gatter unterhalb des UND-Gatters, die variablendisjunkt sind.

Wähle eine maximale Menge von variablendisjunkten ODER-Gattern. Sei H die Menge der Variablen, die bei diesen ODER-Gattern vorkommen. Die Frage ist, wie gross ist |H| maximal (Hinweis 16)?
Wegen der Fallunterscheidung gibt es maximal d * ln n solche ODER-Gatter und jedes hat einen maximalen Fan-in von höchstens c, deshalb ist $\underline{|H| = c * d * \ln n}$.
Weiterhin bleibt noch zu zeigen, wieso in jedem ODER-Gatter mindestens eine Eingangsvariable aus der Menge H stammt (Hinweis 17).
Wenn es ein ODER-Gatter gäbe, dessen Variablen disjunkt zu H wären, wäre die Menge der disjunkten ODER-Gatter nicht maximal (Voraussetzung von Induktionsschritt-Fall 2) und man könnte dieses Gatter noch hinzunehmen.

Es gibt für die Variablen aus H insgesamt $l = 2^{|H|}$ mögliche Belegungen. Wenn man jetzt jede dieser möglichen Belegungen in den ursprünglichen UND-ODER-Schaltkreis einsetzt, fällt in jedem ODER-Gatter mindestens ein Eingang weg (wenn nämlich eine Variable 0 ist). Daher haben alle ODER-Gatter nach dem Einsetzen ein Fan-in von höchstens c – 1. Für alle diese durch Einsetzung entstehenden l Schaltkreise A_1, ..., A_l gilt nach Induktionsvoraussetzung, dass die Wahrscheinlichkeit da-

für, dass der Funktionswert von A_j^r (also nach der Zufallsrestriktion) von mehr als e_{c-1} Variablen abhängt, durch $O\left(\frac{1}{n^k}\right)$ beschränkt ist.
Somit kann die vom UND-ODER-Schaltkreis berechnete Funktion eindeutig durch die A_j's beschrieben werden.

Beispiel: Sei H = {x_1, x_2}, somit l = 2^2 = 4

$$f = (x_1 \cdot x_2 \cdot A_1) \vee (\overline{x_1} \cdot x_2 \cdot A_2) \vee (x_1 \cdot \overline{x_2} \cdot A_3) \vee (\overline{x_1} \cdot \overline{x_2} \cdot A_4)$$

Die Wahrscheinlichkeit, dass f von mehr als l * e_{c-1} Variablen abhängt, kann somit mit $l * O\left(\frac{1}{n^k}\right)$ abgeschätzt werden.
Anstatt die Abhängigkeit von den Variablen nach der Zufallsrestriktion direkt am UND-ODER-Schaltkreis zu betrachten, diskutieren wir dies vorteilhafter an obiger äquivalenten Darstellung von f.
Mit hoher Wahrscheinlichkeit ergibt sich, dass H nach der Zufallsrestriktion nur noch aus konstant vielen Variablen besteht und damit auch die Zahl der nicht-verschwindenden Terme in obiger Formel konstant ist. Sei h die Zufallsvariable, die die Anzahl der verbleibenden Variablen in H angibt. (Wir haben es wieder mit einer Binomialverteilung mit $p = \frac{1}{\sqrt{n}}$ zu tun.) Man kann ähnlich wie in Induktionsanfang-Fall 2 abschätzen:

$\Pr[h > 4*c*d + 2*k] = O\left(\frac{1}{n^k}\right)$ (Hinweis 18), denn

nach Hinweis 16 ist $|H| \le c*d*\ln n$ und mit Hinweis 10 erhalten wir:

$$\Pr[h > a] \le p^a * 2^n$$

$$= \left(\frac{1}{\sqrt{n}}\right)^a * 2^{c*d*\ln n} \quad \text{(wegen *)}$$

$$\le n^{2*c*d} * n^{-\frac{a}{2}}$$

$$= \underline{n^{2*c*d-\frac{a}{2}}}$$

$$\to 2*c*d - \frac{a}{2} = -k \Leftrightarrow \underline{a = 4*c*d + 2*k}$$

$$*: \left(\frac{1}{\sqrt{n}}\right)^a * 2^{c*d*\ln n} = n^{-\frac{a}{2}} * n^{c*d*\ln 2} \quad (a^{\ln b} = b^{\ln a})$$

$$\le n^{-\frac{a}{2}} * n^{2*c*d}$$

Da es nicht auf den Wert der Konstanten ankommt, können auch grössere Konstante verwendet werden.

Mit hoher Wahrscheinlichkeit ist somit $h \le 4*c*d + 2*k$ und f besteht somit aus höchstens $2^h \le 2^{4*c*d+2*k} := m$ Termen, die nicht 0 werden. Wenn man die Wahrschein-

lichkeitsabschätzungen zusammenfügt und $e_c = m * e_{c-1}$ setzt, erhält man:

$$\Pr[\text{f hängt von mehr als } e_c \text{ Variablen ab}]$$
$$\leq \Pr[h > 4*c*d + 2*k] + m * \Pr[\text{ein festes } A_j \text{ hängt von mehr als } e_{c-1} \text{ Variablen ab}]$$
$$\leq O\left(\frac{1}{n^k}\right) + m * O\left(\frac{1}{n^k}\right)$$
$$= O\left(\frac{1}{n^k}\right)$$

Damit haben wir den Induktionsbeweis erbracht.

Wir haben gezeigt:
Es existiert eine Restriktion, die insgesamt genügend Variablen hinterlässt. Jeder einzelne UND-ODER-Schaltkreis auf Stufe 2 und 1 hängt nur von konstant vielen Variablen ab. Daher kann mit nur konstantem Mehraufwand das Distributivgesetz angewandt werden, so dass die 2.Schicht eine ODER-Schicht und die 1. Schicht eine UND-Schicht wird. Nach dem Verschmelzen der Schichten 2 und 3 (beides ODER-Schichten) erhalten wir Schaltkreise polynomialer Grösse, mit t – 1 Schichten und konstantem Eingangs-fan-in, die der Minimalitätsangabe widersprechen.
Damit erhalten wir einen Widerspruch zu unserer Annahme und haben die Behauptung bewiesen.