Extremal Combinatorics
Seminar Sommersemester 2004

Blockings Sets und ihre Dualität

Seminararbeit im Studiengang Informatik von

Bettina Akkapurathu
Matrikelnummer: 227403

Lehr- und Forschungsgebiet Theoretische Informatik
Professor P. Rossmanith
RWTH Aachen

21. Juli 2004

Die folgende Ausarbeitung, die auf dem Kapitel „Blocking Sets and the Duality“ des Buches „Extremal Combinatorics“ von Stasys Jukna basiert, beschäftigt sich mit einem Bereich der Kombinatorik, genauer gesagt mit dem Themenbereich der extremalen Mengentheorie.

Im Folgenden werden wir zunächst eine der fundamentalen Eigenschaften von Familien von Mengen, nämlich ihre Dualität, näher betrachten.

1 Dualität

Definition 1.1
*Unter einer **Familie von Mengen $\mathcal{F}$** versteht man eine Menge, deren Elemente wiederum Mengen sind.*

Beispiel:
Das wohl am weitesten verbreitete Beispiel einer Familie von Mengen ist die Potenzmenge.
Die Potenzmenge $\mathcal{P}(A)$ einer Menge A ist die Menge aller Teilmengen von A.
Formal: $\mathcal{P}(A) = \{B : B \subseteq A\}$
Sei $A = \{1, 2, 3\}$. Dann ist $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Definition 1.2
Sei $\mathcal{F}$ eine Familie von Mengen.
*Eine Menge T heißt **blocking set** von $\mathcal{F}$, wenn sie jede Menge in $\mathcal{F}$ schneidet, also mit jeder Menge in $\mathcal{F}$ mindestens ein Element gemeinsam hat.*
*Wenn keine Untermenge von T ein blocking set von F ist, dann ist T **minimal**. Solche minimalen blocking sets werden auch **transversals** von $\mathcal{F}$ genannt.*
*Das **Dual von** $\mathcal{F}$ ist die Familie aller minimalen blocking sets von $\mathcal{F}$ und wird mit $\boldsymbol{b(\mathcal{F})}$ bezeichnet.*

Beispiel:
Sei $\mathcal{F}$ die folgende Familie von Mengen: $\{\{1\}, \{1{,}2\}, \{2{,}3\}\}$.
$T_1 = \{1, 2, 3\}$ ist ein blocking set. Es ist aber nicht minimal.
$T_2 = \{1, 2\}$ und $T_3 = \{1, 3\}$ sind minimale blocking sets, also Elemente des Dual von $\mathcal{F}$ und zwar die einzigen.

Definition 1.3
Sei $\mathcal{F}$ eine Familie von Mengen.
*Dann heißt $\mathcal{F}$ eine **antichain** (oder **Sperner-System**), wenn keine Menge von $\mathcal{F}$ eine Teilmenge einer anderen ist.*
Formal: $A, B \in \mathcal{F}$ und $A \neq B \;\Rightarrow\; A \nsubseteq B$ und $B \nsubseteq A$.

Beispiel:
Sei $M = \{1, 2, \ldots, n\}$.
Dann sind einige antichains über M die Familien aller Mengen mit fester Kardinaltät k, wobei $k = 0, 1, \ldots, n$. Jede dieser antichains besteht aus $\binom{n}{k}$ Elementen.
Für $M = \{1, 2\}$ sind die antichains die folgenden: $\emptyset$, $\{\{1\}\}$, $\{\{2\}\}$, $\{\{1\}, \{2\}\}$, $\{\{1, 2\}\}$.
(Bemerkung: Einelementige Klassen von Mengen sind immer antichains.)

Satz 1.1
Sei $\mathcal{F}$ eine Familie von Mengen.
Wenn $\mathcal{F}$ eine antichain ist, dann ist $b(b(\mathcal{F})) = \mathcal{F}$.

Beweis:
Idee: Wir werden per Widerspruch zeigen, dass es keine Elemente in $b(b(F)) - F$ und keine in $F - b(b(F))$ geben kann und daher $F = b(b(F))$ gelten muss.

- $b(b(\mathcal{F})) \subseteq \mathcal{F}$:
  Sei $B \in b(b(\mathcal{F}))$ und $B \notin \mathcal{F}$.

  Aus dem Letzteren folgt, dass in jeder Menge $A \in \mathcal{F}$ mindestens ein Element x_A existiert, das nicht in B enthalten ist. Die Menge $\{x_A | A \in \mathcal{F}\}$ all solcher Elemente ist ein blocking set von $\mathcal{F}$ und enthält mindestens ein minimales blocking set $T \in b(\mathcal{F})$. Da aber B ein blocking set von $b(\mathcal{F})$ ist, muss es ein Element mit T gemeinsam haben. Die Elemente in T wurden aber so gewählt, dass $T \cap B = \emptyset$ gilt. Dies ist ein Widerspruch. Somit gilt $b(b(\mathcal{F})) - \mathcal{F} = \emptyset$.

- $\mathcal{F} \subseteq b(b(\mathcal{F}))$:
  Sei $B \in \mathcal{F}$ und $B \notin b(b(\mathcal{F}))$.

  Wir wollen uns zunächst eine schwächere Annahme anschauen, nämlich dass $B \in \mathcal{F}$ und B kein blocking set für $b(\mathcal{F})$ ist.
  Demzufolge existiert eine Menge $M \in b(\mathcal{F})$ mit $M \cap B = \emptyset$. Hieraus und aus der Annahme, dass $B \in \mathcal{F}$, folgt aber, dass M kein blocking set für $\mathcal{F}$ ist, was einen Widerspruch darstellt.

  Nun wollen wir die eigentliche Annahme näher betrachten.
  Aus $B \notin b(b(\mathcal{F}))$ folgt, dass ein $x \in B$ existiert, so dass $B \backslash \{x\}$ ein blocking set für $b(\mathcal{F})$ ist. D.h. insbesondere, dass eine Teilmenge B' von B mit $B' \in b(b(\mathcal{F}))$ existiert. Aus dem Beweis der obigen schwächeren Annahme folgt nun $B' \in \mathcal{F}$.
  Wegen $B' \subset B$, wobei $B, B' \in \mathcal{F}$, folgt auch, dass $\mathcal{F}$ keine antichain ist. Dies ist offensichtlich ein Widerspruch. Somit gilt $\mathcal{F} - b(b(\mathcal{F})) = \emptyset$.

$\square$

Als nächstes befassen wir uns mit dem folgenden Problem von Berge 1989:
In diesem Problem „keys of the safe“ betrachten wir einen Verwaltungsrat, der aus einer Menge X an Personen besteht. Die Stimme eines jeden von ihnen hat in Abstimmungen eine bestimmte Gewichtung, und um einen Mehrheitsentscheid herbeizuführen, muss ein bestimmter Grenzwert überschritten werden. Die Mehrheit $A \subseteq X$, die insgesamt genügend Gewichtung aufbringt, hat dann Zugriff auf Dokumente in einem durch mehrere Schlösser geschützten Tresor. Das bedeutet, dass die Ratsmitglieder verschiedene Koalitionen miteinander eingehen können, um den Tresor zu öffnen. Eine antichain $\mathcal{F}$ wäre die Menge der kleinsten notwendigen Koalitionen, die erforderlich ist, um den Tresor zu öffnen. Nun erhält jedes Ratsmitglied einen oder mehrere Schlüssel zum Tresor. Wir wollen jedoch sicher gehen, dass der Tresor nur dann geöffnet werden kann, wenn die Mindestkoalition anwesend ist. Das Problem besteht nun darin, die kleinstmögliche Anzahl Schlösser zu ermitteln, die dazu notwendig sind. Die Lösung dieses Problems liefert der folgende Satz.

Satz 1.2
Sei $\mathcal{F}$ eine Familie von minimalen Koalitionen.
Dann reichen $l = |b(\mathcal{F})|$ Schlösser aus, um den Tresor zu öffnen.

Beweis:
Sei $\mathcal{F}$ eine antichain und $b(\mathcal{F}) = \{T_1, \ldots, T_l\}$ ein minimales blocking set von $\mathcal{F}$. Jedes Mitglied von T_i erhalte den Schlüssel zum i-ten Schloss. Da die Mengen T_i in $b(\mathcal{F})$ jeweils blocking sets sind, besitzt nun jede Koalition $A \in \mathcal{F}$ die Schlüssel zu allen l Schlössern und kann daher den Tresor öffnen, um an die Dokumente zu gelangen.
Betrachten wir den Fall, dass irgendeine Menge B von Personen keine Koalition enthält, d.h. $b \notin \mathcal{F}$. Dann folgt aus Satz 1.1, dass die Menge B kein blocking set von $b(\mathcal{F})$ ist. Also gibt es in $b(\mathcal{F})$ eine Menge, in der die einzelnen Elemente von B nicht vorhanden sind, d.h. es gilt $B \cap T_i = \emptyset$ für ein i. Aber dies würde bedeuten, dass die Personen in der Menge B den i-ten Schlüssel benötigen würden, was zu zeigen war. □

Zur Veranschaulichung betrachten wir folgendes Beispiel:
Sei $X = \{F, G, Z, R\}$ der Rat.
Die Gewichtung der einzelnen Ratsmitglieder sei $w(F) = 6, w(Z) = 8, w(G) = 3, w(R) = 1$.
Als Grenzwert nehmen wir die Zahl 7.
Nun wäre als minimale Koalition $\mathcal{F} = \{\{Z\}, \{F, G\}, \{F, R\}\}$ denkbar. ($\mathcal{F}$ ist also eine antichain).
Dann ist $b(\mathcal{F}) = \{\{Z, F\}, \{Z, G, R\}\}$. Beide Mengen bekommen jetzt verschiedene Schlüssel. Wir sehen, dass tatsächlich zwei Schlösser genügen, damit jede Koalition an die Dokumente gelangen kann.

Definition 1.4
Sei $\mathcal{F}$ eine Familie von Mengen.
*Dann heißt $\mathcal{F}$ **selbst-dual**, wenn $b(\mathcal{F}) = \mathcal{F}$ gilt.*

Beispiel:

1.) Die Familie $\mathcal{F}$ aller k-elementigen Teilmengen einer $(2k-1)$-elementigen Menge M ist selbst-dual.
Sei $k = 2$ und $M = \{1, 2, 3\}$. Dann ist $\mathcal{F} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\} = b(\mathcal{F})$.

2.) Die Familie $\mathcal{F}$ von Mengen der Größe $r + 1$ mit folgenden Eigenschaften: Eine von diesen Mengen besitzt r beliebige Elemente und die restlichen r Mengen enthalten jeweils 2 Elemente, wobei eine von diesen Elementen mit einem beliebigen Element aus der Menge mit den r Elementen identisch sein muss und das jeweils andere Element in allen r Mengen gleich sein müssen.

- $\mathcal{F} = \{\{1, 2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}$ ist selbst-dual.
- $\mathcal{F} = \{\{1, 2, 3\}, \{4, 5\}, \{6, 7\}, \{8, 9\}\}$ ist nicht selbst-dual.
- $\mathcal{F} = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$ ist auch nicht selbst-dual.
  Hier ist $b(\mathcal{F}) = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$. (Die Menge $\{1, 2, 3\}$ wird ja bei $b(\mathcal{F})$ nicht mit aufgeführt, weil es Untermengen davon gibt, die minimale blocking sets sind.)

Nun könnten wir uns die Frage stellen, welche anderen Familien von Mengen selbst-dual sind. Unser nächstes Ziel ist zu zeigen, dass eine Familie von Mengen genau dann selbst-dual ist, wenn sie intersecting und nicht zweifärbbar ist. Dazu werden wir zunächst einmal diese beiden Begriffe klären.

Definition 1.5
Sei $\mathcal{F}$ eine Familie von Mengen.
*Dann bezeichnet man $\mathcal{F}$ als **intersecting**, wenn je zwei Mengen von $\mathcal{F}$ einen nichtleeren Durchschnitt haben, d.h. wenn $A \cap B \neq \emptyset$ für $A, B \in \mathcal{F}$ gilt.*

Definition 1.6
Sei $\mathcal{F}$ eine Familie von Mengen und $\mathcal{F} \subseteq \mathcal{P}(X)$ (Potenzmenge von X), wobei X die Menge aller Elemente (die Grundmenge) ist, die in $\mathcal{F}$ vorkommen.

*Die **chromatische Zahl** $\chi(\mathcal{F})$ von $\mathcal{F}$ ist die kleinste Anzahl von Farben, mit der die Elemente aus X so gefärbt werden können, dass keine Menge $M \in \mathcal{F}$ mit $|M| > 1$ nur Elemente einer Farbe enthält.*
*Wenn $\chi(\mathcal{F}) = 2$ ist, dann heißt die Familie **zweifärbbar**.*

Alle Elemente in X werden gefärbt (man kann gleiche Farben verwenden, solange keine nichttriviale Menge einfarbig bleibt) und zwar so, dass in jeder Menge aus $\mathcal{F}$, die mehr als ein Element enthält, auch mehr als eine Farbe vorkommt.
Das heißt insbesondere, dass man mindestens zwei Farben braucht, also $\chi(\mathcal{F}) \geq 2$ ist, sobald eine nichttriviale Menge (eine Menge mit mehr als einem Element) von $\mathcal{F}$ dabei ist.

Die 2-färbbaren Familien sind für uns im Folgenden von besonderem Interesse.
Eine alternative Charakterisierung dafür ist die folgende:

$\mathcal{F}$ ist *zweifärbbar* gdw. wir X so in $S \subseteq X$ und X-S partitionieren können, dass kein $A \in \mathcal{F}$ mit $|A| \geq 2$ Teilmenge von S oder X-S ist.
Formal: $\exists S \subseteq X$ mit$A \not\subseteq S$ und $A \not\subseteq X - S$ für jedes $A \in \mathcal{F}$.

Es ist hier wichtig zu beachten, dass diese alternative Charakterisierung nicht für diejenigen Familien $\mathcal{F}$ gilt, in denen eine Menge A mit $|A| = 1$ vorkommt (z.B. $\mathcal{F} = \{\{1\}, \{2, 3\}, \{2, 4\}\}$ mit $\chi(\mathcal{F}) = 2$). Denn dann kann man kein solches S finden, da die einelementige Menge immer eine Teilmenge von S oder $X - S$ ist.

Beispiel: (Gültige 2-Färbung über vier Elementen ($\chi(\mathcal{F}) = 2$))

$X = \{1, 2, 3, 4\}$
$\mathcal{F} = \{\{1\}, \{1, 2\}, \{2, 3\}, \{2, 4\}, \{1, 2, 3, 4\}\}$
$S = \{2\}, \quad X - S = \{1, 3, 4\}$

Definition 1.7
Seien $\mathcal{F}$ und $\mathcal{G}$ Familien von Mengen.
Wenn für jedes $N \in \mathcal{F}$ ein $M \in \mathcal{G}$ mit $M \subseteq N$ existiert, dann notiert man dies als $\boldsymbol{\mathcal{F} \succ \mathcal{G}}$.

Beispiel:

$\{\{1, 2, 3\}, \{3, 4, 5\}\} \succ \{\{1\}, \{2\}, \{5\}, \{7\}\}$, aber
$\{\{1, 2, 3\}, \{3, 4, 5\}\} \not\succ \{\{1\}, \{2\}, \{7\}\}$.

Satz 1.3

(i) Eine Familie $\mathcal{F}$ ist genau dann intersecting, wenn $\mathcal{F} \succ b(\mathcal{F})$ gilt.

(ii) Wenn $\mathcal{F}$ eine antichain ist, dann gilt $\chi(\mathcal{F}) > 2$ genau dann, wenn $b(\mathcal{F}) \succ \mathcal{F}$ gilt.

Beweis:

(i) „$\Rightarrow$“:
Sei $\mathcal{F}$ intersecting. Dann ist jede Menge $A \in \mathcal{F}$ auch ein blocking set von $\mathcal{F}$, die insbesondere mindestens ein minimales blocking set als Untermenge enthält.
Daraus folgt, dass $\mathcal{F} \succ b(\mathcal{F})$.

„$\Leftarrow$“:
Sei $\mathcal{F} \succ b(\mathcal{F})$. Nach Definition enthält jede Menge $A \in \mathcal{F}$ ein blocking set von $\mathcal{F}$.
Folglich schneidet A alle anderen Mengen von $\mathcal{F}$.

(ii) „$\Rightarrow$“:
Wir zeigen diese Richtung per Widerspruch. Sei $\chi(\mathcal{F}) > 2$ und $b(\mathcal{F}) \not\succ \mathcal{F}$.
Nach Definition des Letzteren existiert ein blocking set T von $\mathcal{F}$, das keine Obermenge einer Menge von $\mathcal{F}$ ist. Dies bedeutet also, dass keine Menge von $b(\mathcal{F})$ eine Menge von $\mathcal{F}$ komplett „blockiert“. Aber das Komplement $X - T$ (X ist das Universum von $\mathcal{F}$) ist ebenfalls keine Obermenge einer Menge von $\mathcal{F}$, da ja ansonsten T nicht alle Mengen von $\mathcal{F}$ „blockieren“ könnte. Somit ist $(T, X - T)$ 2-färbbar, d.h. es gilt $\chi(\mathcal{F}) = 2$. Dies stellt aber einen Widerspruch zu unserer Annahme, nämlich $b(\mathcal{F}) \not\succ \mathcal{F}$, dar.

„$\Leftarrow$“:
Auch diese Richtung zeigen wir per Widerspruch. Sei $b(\mathcal{F}) \succ \mathcal{F}$ und $\chi(\mathcal{F}) = 2$ (eigentlich $\chi(\mathcal{F}) <= 2$, aber die 1-Färbung existiert nicht).
Nach Definition des Letzteren existiert eine 2-Färbung $(S, X - S)$ (X wie oben), was insbesondere bedeutet, dass S ein blocking set von $\mathcal{F}$ ist. Es existiert folglich ein $S' \in b(\mathcal{F})$ mit $S' \subseteq S$, woraus zusammen mit der Annahme $b(\mathcal{F}) \succ \mathcal{F}$ folgt, dass ein $A \in \mathcal{F}$ mit $A \subseteq S'$ existieren muss. Dies impliziert insbesondere $A \subseteq$ S, d.h. die Menge $A \in \mathcal{F}$ ist einfarbig. Das ist ein Widerspruch zur Annahme $\chi(\mathcal{F}) = 2$.

Korollar 1.1
Sei $\mathcal{F}$ eine antichain. Dann sind die folgenden drei Aussagen äquivalent:

(1) $b(\mathcal{F}) = \mathcal{F}$;

(2) $\mathcal{F}$ ist intersecting und $\chi(\mathcal{F}) > 2$;

(3) Sowohl $\mathcal{F}$ als auch $b(\mathcal{F})$ sind intersecting.

Beweis:
Die Äquivalenz von (1) und (2) folgt unmittelbar aus Satz 1.3.
Die Äquivalenz von (1) und (3) folgt aus der Tatsache, dass sowohl $\mathcal{F}$ als auch $b(\mathcal{F})$ antichains sind. □

2 Entscheidungsbäume

Blocking sets spielen in der Theorie der booleschen Funktionen eine wichtige Rolle. Im Folgenden werden wir einige Ergebnisse in dieser Richtung darlegen.

Definition 2.1
Sei $f : \{0,1\}^n \to \{0,1\}$ eine boolesche Funktion.
*Ein **Entscheidungsbaum** für f ist ein Binärbaum, dessen innere Knoten mit Elementen aus der Menge $\{1,\ldots,n\}$ und dessen Blätter mit Elementen aus der Menge $\{0,1\}$ beschriftet sind.*

Wir können folgendes Verfahren anwenden, um den Wert einer Eingabe der booleschen Funktion f anhand eines Entscheidungsbaumes zu ermitteln:
Wir prüfen von der Wurzel ausgehend, welche Beschriftung dieser Knoten hat. Wenn der Knoten die Beschriftung x_i hat, nehmen wir das i-te Bit der Eingabe. Hat nun das i-te Bit den Wert 0, so steigen wir in den linken Teilbaum hinab, wohingegen wir in den rechten Teilbaum absteigen, wenn das i-te Bit den Wert 1 besitzt. Dieses Verfahren wenden wir solange an, bis wir ein beschriftetes Blatt erreichen, welches dann den Wert der booleschen Funktion f darstellt.

Beispiel:

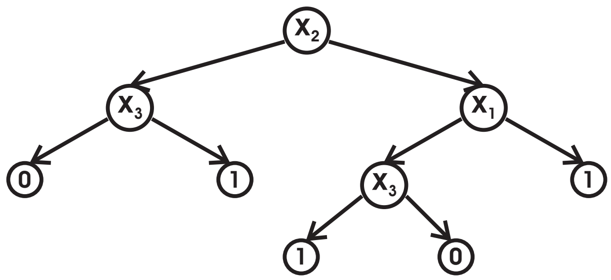

Abbildung 1: Entscheidungsbaum für eine Funktion f_1

Die Funktion $f_1 : \{0,1\}^3 \to \{0,1\}$ besitzt die folgenden Eingaben (von links nach rechts): (*,0,0), (*,0,1), (0,1,0), (0,1,1), (1,1,*), wobei * hier für „0“ oder „1“ steht.

Wir wenden nun das oben vorgestellte Verfahren auf die Eingabe $x_1 = 1$, $x_2 = 0$, $x_3 = 1$ an:
Da die Wurzel die Beschriftung x_2 hat und mit dem Wert 0 belegt ist, müssen wir laut Verfahren in den linken Teilbaum von x_2 absteigen. Hier befindet sich ein Knoten, der mit x_3 beschriftet und mit 1 belegt ist, weswegen wir im rechten Teilbaum weitergehen müssen. Ohne die Variable x_1 getestet zu haben, kommen wir nun zu einem Blatt mit der Beschriftung 1, das den Funktionswert von $f(1,0,1)$ darstellt.

An diesem Beispiel sehen wir, dass es nicht notwendig ist, jede Variable in jedem Berechnungspfad zu berücksichtigen; dies wäre außerdem nicht sinnvoll, denn dann wären selbst bei trivialen Funktionen die Entscheidungsbäume riesengroß.

Definition 2.2
Gegeben sei ein Entscheidungsbaum für f.
*Die **Tiefe** eines Entscheidungsbaumes ist die Anzahl der Kanten in dem längsten Pfad von der Wurzel zu einem Blatt oder, äquivalent dazu, die maximale Anzahl von geprüften Bits auf einem Pfad.*
*Mit **DT(f)** bezeichnen wir die minimale Tiefe eines Entscheidungsbaumes, der f berechnet.*

Anders ausgedrückt versteht man unter $DT(f)$ den kleinsten Wert unter den Tiefen aller Entscheidungsbäume für f.

Beispiel:

1) Die Funktion $f_2(x_1, x_2, x_3) = x_1$ hat DT(f) = 1, weil wir nur x_1 testen müssen, um das Ergebnis zu ermitteln.

2) Abbildung 1: Der Entscheidungsbaum für f_1 besitzt die Tiefe 3; dies entspricht auch der maximalen Anzahl von geprüften Bits in einem Pfad, nämlich 3 Tests von Bits. Also ist $DT(f_1) = 3$, sofern es keinen Entscheidungsbaum geringerer Tiefe für f_1 gibt.

Es reicht vollkommen aus, $DT(f)$-viele Bits von einer Eingabe $a = (a_1, \ldots, a_n)$ zu sehen, um die Ausgabe einer booleschen Funktion $f : \{0,1\}^n \to \{0,1\}$ zu bestimmen. Eine Berechnung von f durch einen entsprechenden Entscheidungsbaum T entspricht einem Pfaddurchlauf in T und deshalb kann die Berechnung auch höchstens so lange dauern, wie der längste Pfad Knoten besitzt, und das ist gerade die Größe DT(f).

Es stellt sich nun die Frage, ob wir nicht eine kleinere Anzahl von Bits finden können, um den Wert der Funktion f zu bestimmen. Die Idee ist nun die, dass wir für jede Eingabe a die kleinste Menge von Bits wählen, um den Funktionswert zu ermitteln. Dies kann wie folgt formalisiert werden.

Definition 2.3
*Sei $f : \{0,1\}^n \to \{0,1\}$ eine boolesche Funktion, und seien $x_1, \ldots, x_n$ die Eingabevariablen von f. Ein **Zertifikat** von einer Eingabe $a = (a_1, \ldots, a_n)$ ist eine Menge von Variablen $Y = \{x_1, \ldots, x_k\}$ mit $k \leq n$, so dass wir den Funktionswert von f(a) allein durch die Bestimmung der k Werte erhalten.*

Beispiel:

1) Abbildung 1:
Sei $a = (0,0,1)$ die Eingabe. Dann ist $\{x_2, x_3\}$ ein Zertifikat von a, da die Ausgabe für $x_2 = 0$ und $x_3 = 1$ unabhängig von der Variablen x_1 ist.

2) Für die Funktion $f(x_1, \ldots, x_n) = x_1 \vee x_2 \vee \ldots \vee x_n$ ist $\{x_1\}$ ein Zertifikat von allen Eingaben $a = (a_1, \ldots, a_n)$ der Form (1,*,. . . ,*), da f unabhängig von den Variablen stets den Wert 1 besitzt, wenn x_1 mit 1 belegt ist.

Als nächstes wollen wir den Zusammenhang von Zertifikaten mit blocking sets erstellen. Dafür brauchen wir die folgende Aussage:
Sei Y_a ein Zertifikat von a mit $f(a) = 0$. Weiter sei Y_b ein Zertifikat von b mit $f(b) = 1$.
Y_a muss die Zertifikate Y_b von allen Eingaben b schneiden, und umgekehrt (denn sonst könnte die Funktion beide Werte 0 und 1 für die gleiche Eingabe annehmen, was natürlich unmöglich ist). $(*)$

Nehmen wir mal an, dass Y_a das Zertifikat Y_b nicht schneidet. Dann können wir ohne Weiteres

- alle in Y_a bzw. Y_b enthaltenen Eingabevariablen x_i mit den zugehörigen Werten a_i bzw. b_i belegen, und

- alle bis dahin nicht belegten Variablen beliebig belegen

Wir stellen hier fest, dass die gesamte Belegung x beide Voraussetzungen erfüllt. Nach Definition von Zertifikat gilt jetzt sowohl $f(x) = 0$ als auch $f(x) = 1$, weil wir die Variablenbelegungen in Y_a bzw. Y_b jeweils so gewählt haben, dass $x_i = a_i$ bzw. $x_i = b_i$ gilt. Dies ist aber ein Widerspruch, da $f(x)$ nicht beide Werte zugleich annehmen kann.

Wir können unter der Voraussetzung, dass $f(a) = f(b)$ gilt, zwei Zertifikate Y_a für a und Y_b für b mit $Y_a \cap Y_b = \emptyset$ finden. Dies sehen wir z.B. an der Funktion $f(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3$. Hier ist a=(1,0,0) eine Eingabe mit f(a)=1 und Zertifikat $\{x_1\}$. Weiter ist b=(0,1,0) eine Eingabe mit f(b)=1 und Zertifikat $\{x_2\}$. Es ist also $\{x_1\} \cap \{x_2\} = \emptyset$.

Der Zusammenhang von blocking sets und Zertifikaten ist also folgender: Wie wir bereits wissen, ist ein blocking set eine Menge, die jedes Element einer Familie von Mengen schneidet. Wenn wir uns nun die Aussage $(*)$ anschauen, stellen wir fest, dass jedes Zertifikat von a mit $f(a) = 0$ einen blocking set darstellt, da es die Familie aller Zertifikate von b mit $f(b) = 1$ schneidet.

Definition 2.4
Sei f eine boolesche Funktion und a eine Eingabe für f.
Dann bezeichnet ***C(f,a)*** *die minimale Größe eines Zertifikats für a.*
Die ***Zertifikatskomplexität*** *von f ist* $\boldsymbol{C(f) = \max\{C_0(f),\, C_1(f)\}}$*, wobei*

- $\boldsymbol{C_0(f) = \max_a\{C(f,a) : f(a) = 0\}}$,
  d.h. $\boldsymbol{C_0(f)}$ *ist die maximale Größe eines minimalen Zertifikats für jede Eingabe a mit f(a)=0,*
- $\boldsymbol{C_1(f) = \max_a\{C(f,a) : f(a) = 1\}}$,
  d.h. $\boldsymbol{C_1(f)}$ *ist die maximale Größe eines minimalen Zertifikats für jede Eingabe a mit f(a)=1.*

Beispiel:

1) Sei $f = f(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$.   (XOR)

   - $C_0(f) = C_1(f) = n$, weil $f(a_1, ...a_n) = 0$ / $f(a_1, ...a_n) = 1$ nur dann gilt, wenn die Anzahl der Einsen in der Eingabe gerade / ungerade ist, d.h. also, dass man alle n Belegungen der Variablen $x_1, ...x_n$ benötigt. Demzufolge existiert kein kleineres Zertifikat für eine beliebige n-stellige Eingabe als $\{x_1, ...x_n\}$.

   $\Rightarrow C(f) = \max\{n,\, n\} = n$.

2) Abbildung 1:

   - $C_0(f) = 3$, da z.B. für die Eingabe $a = (0, 1, 1)$ mit $f(a) = 0$ nur $\{x_1, x_2, x_3\}$ ein Zertifikat für a ist.
   - $C_1(f) = 3$, da z.B. für die Eingabe $a = (0, 1, 0)$ mit $f(a) = 1$ wiederum nur $\{x_1, x_2, x_3\}$ ein Zertifikat für a ist.

   $\Rightarrow C(f) = \max\{3,\, 3\} = 3$.

Es gilt $C(f) \leq DT(f)$. D.h. also, dass es für jede Eingabe a vollkommen ausreicht, $DT(f)$-viele Bits zu sehen, um den Wert der Funktion f zu bestimmen. Es stellt sich nun die Frage, ob diese obere Grenze optimal ist. Das folgende Beispiel zeigt, dass dies nicht der Fall ist.

Gegeben sei die Funktion $f = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{m} x_{ij}$. Weiter sei T ein beliebiger Entscheidungsbaum für f. Unser Ziel ist zu zeigen, dass T die Tiefe m^2 besitzt. Die Idee ist nun, eine möglichst schlechte Belegung in dem Sinne zu wählen, dass sie einen langen Pfad, insbesondere der Länge m^2, erzwingt.
Dabei gehen wir wie folgt vor: Wir belegen nur die letzte ungetestete Variable aus dem i-ten OR-Ausdruck $(x_{i1}, \ldots, x_{im})$ mit 1 und damit alle anderen zuvor getesteten Variablen auf dem Pfad mit 0. Somit nimmt der i-te OR-Ausdruck erst bei der letzten noch zu testenden Variablen den Wert 1 an. Da wir insgesamt ein AND berechnen, muss dies für jeden der m verschiedenen i Ausdrücke gelten, so dass der bewusst schlecht gewählte Pfad die Länge m^2 haben muss.
Demzufolge ist $C(f) = m$ und $DT(f) = m^2$. Folglich ist für die Funktion f $DT(f) = C_0(f) * C_1(f)$.
Hieraus können wir schließen, dass es unwesentlich ist, wie ein Entscheidungsbaum für diese Funktion aussieht, da wir immer eine passende schlechte Belegung erstellen können, so dass die Tiefe stets m^2 ist. Der Extremfall tritt dann auf, wenn T ein vollständiger Entscheidungsbaum ist. Dieser Baum besitzt $2^{m^2} - 1$ innere Knoten und 2^{m^2} Blätter. Da hat jeder Berechnungspfad die Länge m^2.

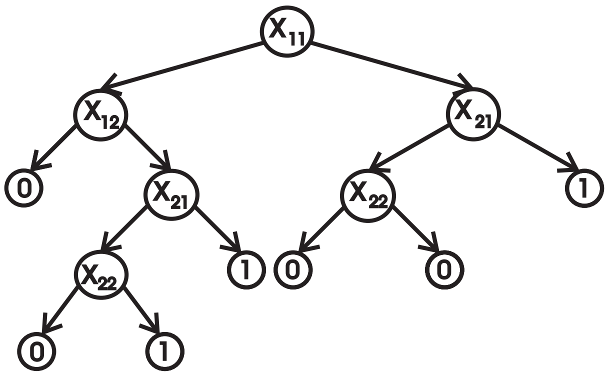

Abbildung 2: Möglicher Entscheidungsbaum für $f = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{m} x_{ij}$ (m=2)

Hier ist DT(f) $= m^2 = 4$.

Es wird sich herausstellen, dass das obige Beispiel den worst case darstellt. Unser nächstes Ziel ist, eine untere Schranke über allen möglichen Entscheidungsbäumen T zu bestimmen. Dazu gibt der folgende Satz Aufschluss.

Satz 2.1
Sei f eine boolesche Funktion.
Dann gilt:

$$DT(f) \leq C_0(f) * C_1(f).$$

Beweis: Induktion über die Anzahl der Variablen n.

IA: n=1

- Die Funktion f ist konstant ($f(x) = 0$ bzw. $f(x) = 1$). Hier genügt ein Baum, der lediglich aus dem Blatt 0 bzw. 1 besteht.
  $DT(f) = 0$, $C_0(f) = 0, C_1(f) = 0$
  $\Rightarrow DT(f) = 0 \leq 0 = C_0(f) * C_1(f) \quad \surd$
- Es existiert eine Variable mit je einer Kante zum Blatt mit der Beschriftung 0 bzw. 1.
  $DT(f) = 1$, $C_0(f) = 1, C_1(f) = 1$
  $\Rightarrow DT(f) = 1 \leq 1 = C_0(f) * C_1(f) \quad \surd$

IS: $n - k \rightarrow n$
Sei f(0,...,0)=0. Dann existiert ein Zertifikat Y für die Eingabe a=(0,...,0) mit f(a)=0, wobei $|Y| = k \leq C_0(f)$. D.h. also, dass die Funktion unabhängig von den anderen Variablen gleich 0 ist, wenn wir diesen k Variablen den Wert 0 zuordnen.
Wir können o.B.d.A. annehmen, dass die Menge $Y = \{x_1, \ldots, x_k\}$ der ersten k Variablen diese Eigenschaft besitzt.

Weiter sei T_0 ein vollständiger Entscheidungsbaum der Tiefe k auf diesen k Variablen, d.h. dass jeder Pfad die Tiefe k hat und jede Variable genau einmal in jedem Pfad auftaucht. Der Entscheidungsbaum besitzt genau $2^k - 1$ innere Knoten und 2^k Blätter, wobei jedes Blatt eindeutig einer Belegung $a = (a_1, \ldots, a_k) \in \{0,1\}^k$ der Eingabebits x_1 bis x_k entspricht. Welchen Wert genau jedes einzelne Blatt besitzt, interessiert uns nicht.

Um nun die übrigen n-k Variablen auch noch berücksichtigen zu können, ersetzen wir jedes Blatt durch einen dazu geeigneten Entscheidungsbaum T_a mit minimaler Tiefe für die Subfunktion $f_a = f(a_1, \ldots, a_k, x_{k+1}, \ldots, x_n)$. Hierbei setzen wir also die ersten k Eingabebits fest und zwar gemäß der Belegung a.
Es gilt $C_0(f_a) \leq C_0(f)$ und $C_1(f_a) \leq C_1(f)$, weil die Funktion nun weniger abhängig von den Eingabebits ist, so dass die Zertifikatsgrößen lediglich sinken, aber garantiert nicht steigen können.

Wir behaupten nun, dass eine stärkere Ungleichung gilt, nämlich

$$C_1(f_a) \leq C_1(f) - 1. \quad (1)$$

Dies können wir folgendermaßen beweisen: Sei $(a_{k+1}, \ldots, a_n)$ eine beliebige Eingabe von f_a, wobei $f_a(a_{k+1}, \ldots, a_n) = 1$ gilt. Zusammen mit $a = (a_1, \ldots, a_k)$ führt dies zu einer Eingabe der Funktion f mit $f(a_1, \ldots, a_n) = 1$. Nach Definition von $C_1(f)$ muss es nun eine Menge $Z = \{x_1, \ldots, x_m\}$ von $m \leq C_1(f)$ Variablen geben, so dass der Wert unabhängig von den anderen Variablen 1 wird, wenn wir den Variablen $x_1, \ldots, x_m$ die entsprechenden Werte $a_1, \ldots, a_n$ zuordnen.

Eine einfache, aber äußerst wichtige Beobachtung ist jetzt, dass

$$Y \cap Z \neq \emptyset. \quad (2)$$

(Dies wurde weiter oben schon behandelt.) Nehmen wir an, dass $Y \cap Z = \emptyset$ gilt. Dann sollte $f(0, \ldots, 0, a_{k+1}, \ldots, a_n) = 0$ sein, weil wir ja die Variablen in Y mit 0 belegt haben, so dass der

Funktionswert von f ebenfalls 0 ist. Aber der Funktionswert von f sollte zugleich 1 sein, da wir die Variablen in Z ja mit den entsprechenden Werte a_i belegt haben, so dass die Funktion den Wert 1 besitzt. Dies ist offensichtlich ein Widerspruch.

Deswegen müssen wir wegen (2) nur $|Z - Y| \leq m - 1$ Variablen von $(a_{k+1}, \ldots, a_n)$ belegen, damit die Unterfunktion f_a die konstante Funktion 1 erhält. Somit haben wir (1) bewiesen.

Wenn wir nun die Induktionsvoraussetzung auf jede der Subfunktionen f_a mit $a \in \{0,1\}^k$ anwenden, erhalten wir

$$DT(f_a) \leq C_0(f_a)C_1(f_a) \leq C_0(f)(C_1(f) - 1).$$

Insgesamt erhalten wir dann für die Gesamttiefe des Entscheidungsbaumes

$$DT(f) \leq k + \max_a DT(f_a) \leq C_0(f) + C_0(f)(C_1(f) - 1) = C_0(f)C_1(f).$$

d.h. $DT(f)$ ist höchstens so groß wie Summe von k (k ist die Tiefe des vollständigen Entscheidungsbaumes über den Variablen x_1 bis x_k) und der größten Tiefe unter den jeweils optimalen Bäumen für die verschiedenen f_a. □

Literatur:

[JUKNA 2001] JUKNA, S(2001). *Extremal Combinatorics. With Applications in Computer Science.* Springer Verlag Berlin Heidelberg, ISBN-3540663134.

www.kfunigraz.ac.at/diplomand-seminar/Folien/KR