Blocking Sets und ihre Dualität
Extremal Combinatorics

Bettina Akkapurathu

Lehr- und Forschungsgebiet Theoretische Informatik
RWTH Aachen

Dualität

Definition

Unter einer Familie vo Mengen F versteht man eine Menge, deren Elemente wiederum Mengen sind.

Beispiel: Potenzmenge

$A = \{1,2,3\}$

$P(A) = \{Ø,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$

Definition

Eine Menge T heißt blocking set von F, wenn sie jede Menge in F schneidet.

T ist minimal, wenn keine Untermenge von T ein blocking set von F ist.

Das Dual von F ist die Familie aller minimalen blocking sets von F. Bezeichung: b(F)

Beispiel

$F = \{\{1\}, \{1,2\}, \{2,3\}\}$

- blocking set: $T_1 = \{1,2,3\}$
- minimale blocking sets: $T_2 = \{1,2\}$, $T_3 = \{2,3\}$

Definition

F heißt eine antichain (oder Sperner-System), wenn keine Menge von F eine Teilmenge einer anderen ist.

Beispiel

A = {1,2,...,n}

Antichains: Familien aller Mengen mit fester Kardinalität k, wobei k = 0,1,...,n.

A = {1,2}
Antichains: Ø, {{1}}, {{2}}, {{1}, {2}}, {{1,2}}

Satz

Wenn F eine antichain ist, dann ist $b(b(F)) = F$.

Beweis:

- $b(b(F)) \subseteq F$:

  Sei $B \in b(b(F))$ und $B \notin F$.

$\Rightarrow$ In jeder Menge $A \in F$ ist mindestens ein Element x_A enthalten, das nicht in B enthalten ist.

Die Menge $\{x_A\}$ ist ein blocking set von F und enthält mindestens ein minimales blocking set $T \in F$.

$B \in b(F) \Rightarrow B \cap T \neq \emptyset$

Die Elemente in T wurden aber so gewählt, dass sie alle nicht in B sind.

Widerspruch!

W

Satz

Wenn F eine antichain ist, dann ist b(b(F)) = F.

Beweis:

- $F \subseteq b(b(F))$:

  Sei $B \in F$ und $B \notin b(b(F))$.

  1. Fall: B ist kein blocking set für b(F).

$\Rightarrow$ Es existiert eine Menge $M \in b(F)$ mit $M \cap B = \emptyset$.

Aus $M \cap B = \emptyset$ und $B \in F$ folgt aber, dass M kein blocking set für F ist.

Widerspruch!

Satz

Wenn F eine antichain ist, dann ist $b(b(F)) = F$.

Beweis:

- $F \subseteq b(b(F))$:

  Sei $B \in F$ und $B \notin b(b(F))$.

  2. Fall: B ist kein minimales blocking set für b(F).

$\Rightarrow$ Es existiert ein $x \in M$, so dass auch $B \setminus \{x\} \in b(b(F))$ ist.

$\Rightarrow$ Es existiert ein $B' \subset B$ mit $B' \in b(b(F))$.

Nach dem 1.Fall gilt $B' \in F$.

Aus $B \in F$, $B' \in F$ und $B' \subset B$ folgt, dass F keine antichain ist.

Widerspruch! W

Problem: „Keys of the Safe“

Gegeben:

- Verwaltungsrat, bestehend aus einer Menge X an Personen
- Die Stimme jeder Person hat in Abstimmungen eine bestimmte Gewichtung
- Für einen Mehrheitsentscheid ist die Überschreitung eines bestimmten Grenzwertes notwendig
- Die Mehrheit $A \subseteq X$ hat Zugriff auf einen durch mehrere Schlösser geschützten Tresor

Problem: „Keys of the Safe“

- Antichain F: Menge der kleinsten Koalitionen, die erforderlich ist, um den Tresor zu öffnen
- Jedes Ratsmitglied erhält mindestens einen Schlüssel.
- Der Tresor soll nur dann geöffnet werden können, wenn eine der Mindestkoalitionen anwesend ist

<u>Gesucht:</u>

Kleinstmögliche Anzahl Schlösser

Satz

Sei F eine Familie von minimalen Koalitionen.
Dann reichen n = |b(F)| Schlösser aus, um den Tresor zu öffnen.

Beweis:

Gegeben:

antichain F, minimales blocking set b(F) = $\{T_1,...T_n\}$ von F.

- Jedes Mitglied von T_i erhalte den Schlüssel zum i-ten Schloss.
- Mengen $T_i \in$ b(F) sind jeweils blocking sets

$\Rightarrow$ jede Koalition A$\in$ F besitzt die Schlüssel zu allen n Schlössern.

Beispiel

Gegeben:

Rat:	X = {F,G,Z,R}
Gewichtung:	w(F) = 6, w(Z) = 8, w(G) = 3, w(R) = 1
Grenzwert:	7

F = {{Z}, {F,G}, {F,R}} (antichain)
b(F) = {{Z,F}, {Z,G,R}}

Jede Menge in b(F) erhält einen voneinander verschiedene Schlüssel.

$\Rightarrow$ Jede Koalition kann den Tresor öffnen

Definition

F heißt selbst-dual, wenn b(F) = F gilt.

Beispiel

Familie F aller k-elementigen Teilmengen einer (2k-1)-elementigen Menge M

k = 2, M = {1,2,3}

F = {{1,2}, {1,3}, {2,3}} = b(F)

Nächstes Ziel:

Wir wollen zeigen, dass eine Familie von Mengen genau dann selbst-dual ist, wenn sie intersecting und nicht zweifärbbar ist.

Definition

Man bezeichnet F als intersecting, wenn je zwei Mengen von F einen nichtleeren Durchschnitt haben.

$$A \cap B \neq \emptyset \text{ für } A, B \in F$$

Definition

Sei F eine Familie von Mengen und X die Menge aller Elemente, die in F vorkommen.

Die chromatische Zahl χ (F) von F ist die kleinste Anzahl von Farben, mit der die Elemente aus X so gefärbt werden können, dass keine Menge $M \in F$ mit $|M| > 1$ nur Elemente einer Farbe enthält.

Wenn χ (F) = 2, ist dann heißt die Familie 2-färbbar.

Alternative Charakterisierung von 2-färbbaren Familien

F ist *2-färbbar* gdw. wenn wir X so in $S \in X$ und X-S partitionieren können, dass kein $A \in F$ mit $|A| \geq 2$ Teilmenge von S oder X-S ist.

Beispiel: (Gültige 2-Färbung über vier Elementen)

$F = \{\{1\}, \{1,2\}, \{2,3\}, \{2,4\}, \{1,2,3,4\}\}$

$X = \{1, 2, 3, 4\}$

$F = \{\{1\}, \{1,2\}, \{2,3\}, \{2,4\}, \{1,2, 3,4\}\}$

$S = \{2\}$

$X\text{-}S = \{1,3,4\}$

Definition

Seien F und G Familien von Mengen.

Wenn $M \subseteq N$ für ein beliebiges $M \in G$ und für alle Mengen $N \in F$ gilt, dann bezeichnet man dies als $F \dagger G$.

Beispiel

$\{\{1,2,3\}, \{3,4,5\}\} \dagger \{\{1\}, \{2\}, \{5\}, \{7\}\}$

$\{\{1,2,3\}, \{3,4,5\}\} \dagger \{\{1\}, \{2\}, \{7\}\}$ gilt nicht!

Satz

i. Eine Familie F ist genau dann intersecting, wenn $F \not\supset b(F)$ gilt.

ii. Wenn F eine antichain ist, dann gilt $\chi(F) > 2$ genau dann wenn $b(F) \not\supset F$ gilt.

i. Eine Familie F ist genau dann intersecting, wenn $F \not\subset b(F)$ gilt.

Beweis:

„$\Rightarrow$“ :

Sei F intersecting.

Dann ist jede Menge $A \in F$ auch ein blocking set von F, die insbesondere mindestens ein minimales blocking set enthält.

$\Rightarrow F \not\subset b(F)$

i. Eine Familie F ist genau dann intersecting, wenn F f b(F) gilt.

Beweis:

„⇐“:

Sei F f b(F).

Nach Definition enthält jede Menge A∈ F ein blocking set von F.

⇒ A schneidet alle anderen Mengen von F.

W

ii. Wenn F eine antichain ist, dann gilt $\chi(F) > 2$ genau dann wenn $b(F) \not\subset F$ gilt.

Beweis:

„$\Rightarrow$“ :

Sei $\chi(F) > 2$ und $b(F) \not\subset F$ gilt nicht.

Es existiert ein $T \in b(F)$ mit $A \in T$, wobei $A \in F$

$\Rightarrow$ Kein $T \in b(F)$ „blockiert“ ein $A \in F$ komplett.

Aber $A \not\subset X\text{-}T$ gilt auch, wobei $A \in F$, da T sonst nicht alle Mengen von F „blockieren“ könnte.

$\Rightarrow$ (T,X-T) ist 2-färbbar, d.h, es gilt $\chi(F) = 2$.

ii. Wenn F eine antichain ist, dann gilt $\chi(F) > 2$ genau dann wenn $b(F) \not\subseteq F$ gilt.

Beweis:

„$\Leftarrow$“ :

Sei $b(F) \not\subseteq F$ und $\chi(F) = 2$.

Es existiert eine 2-Färbung (S,X-S), d.h. $S \in b(F)$.

$\Rightarrow$ Es existiert ein $S' \in b(F)$ mit $S' \subseteq S$.

Zusammen mit der Annahme $b(F) \not\subseteq F$ folgt, dass ein $A \in F$ mit $A \subseteq S'$ existieren muss.

$\Rightarrow A \subseteq S$, d.h. die Menge ist einfarbig.

Widerspruch!

W

Korollar

Sei F eine antichain. Dann sind die folgenden drei Aussagen äquivalent:

1) b(F) = F;
2) F ist intersecting und $\chi(F) = 2$:
3) Sowohl F als auch b(F) sind intersecting.

Beweis:

Äquivalenz von 1) und 2) folgt unmittelbar aus dem letzten Satz.

Äquivalenz von 1) und 3) folgt aus der Tatsache, dass F und b(F) antichains sind.

W

Entscheidungsbäume

Definition

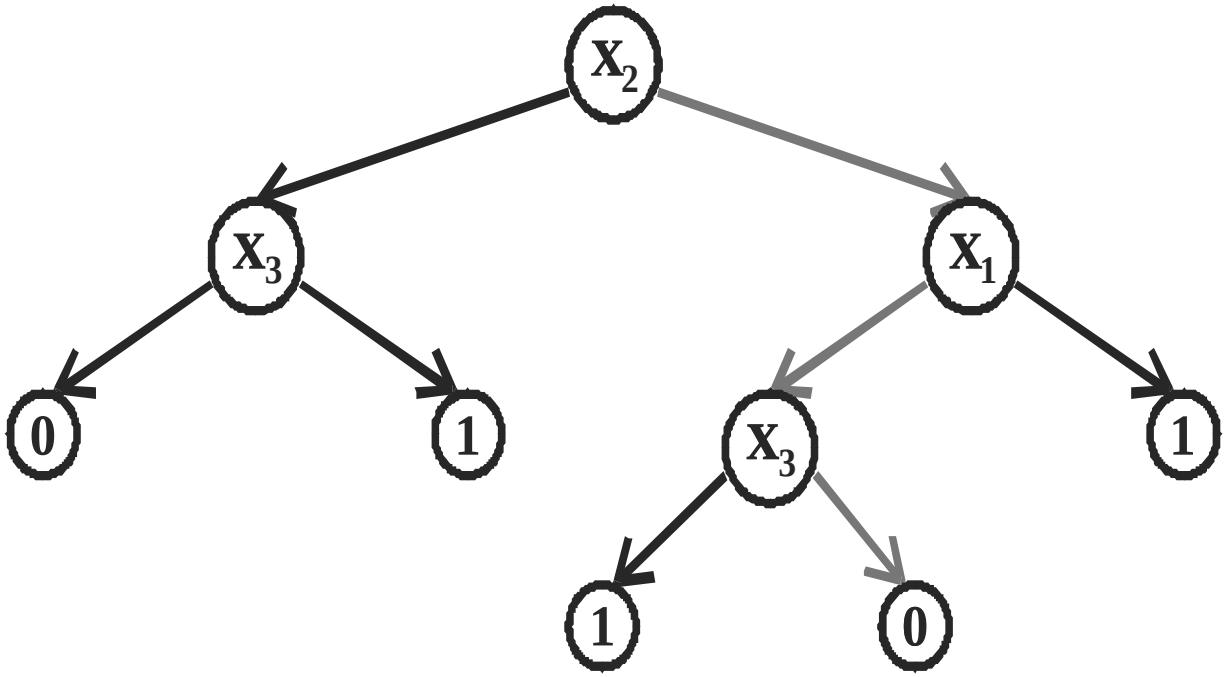
Ein Entscheidungsbaum für eine boolesche Funktion f ist ein Binärbaum, dessen innere Knoten mit Elementen aus der Menge {1,2,...n} und die Blätter mit Elementen aus der Menge {0,1} beschriftet sind.

Verfahren zur Bestimmung des Funktionswertes

- Start: Wurzel
- Man nimmt das i-te Bit der Eingabe bei einem Knoten mit der Beschriftung i
- Beim Wert 0 des i-ten Bits steigt man in den linken Teilbaum ab, beim Wert 1 in den rechten
- Iteration, bis man ein beschriftetes Blatt erreicht

$\Rightarrow$ Wert von f

Beispiel



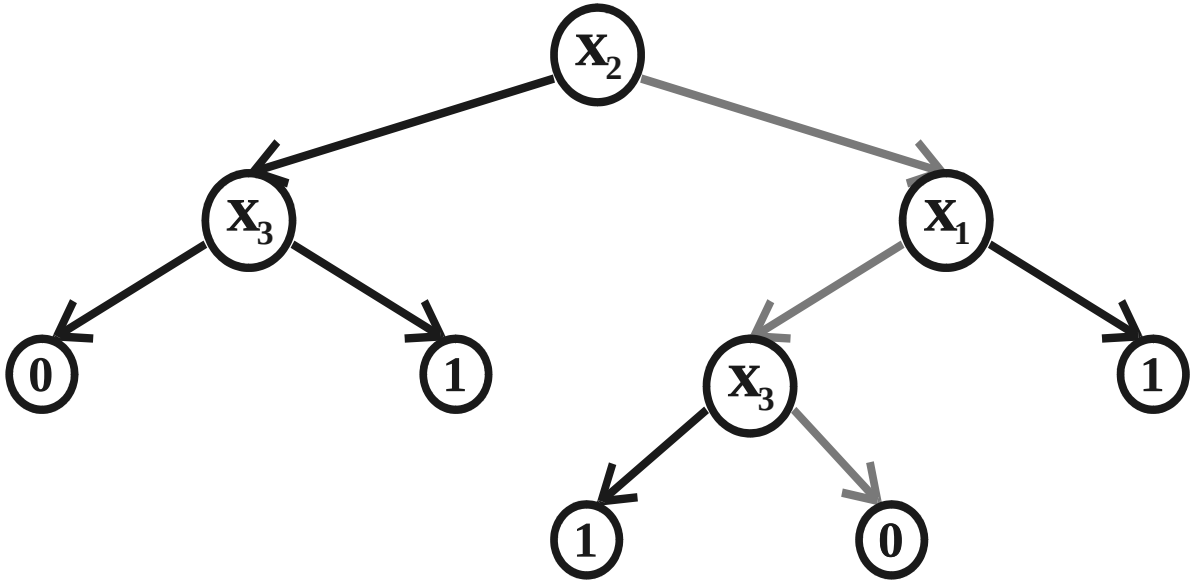
Eingabe: (0,1,1)

Definition

Die Tiefe eines Entscheidungsbaums ist die Anzahl der Kanten in dem längsten Pfad von der Wurzel zu einem Blatt.
(äquivalent: die maximale Anzahl von geprüften Bits auf einem Pfad).

Mit DT(f) bezeichnet man die minimale Tiefe eines Entscheidungsbaums, der f berechnet.

Beispiel



DT(f) = 3, sofern kein Entscheidungsbaum geringerer Tiefe für f existiert.

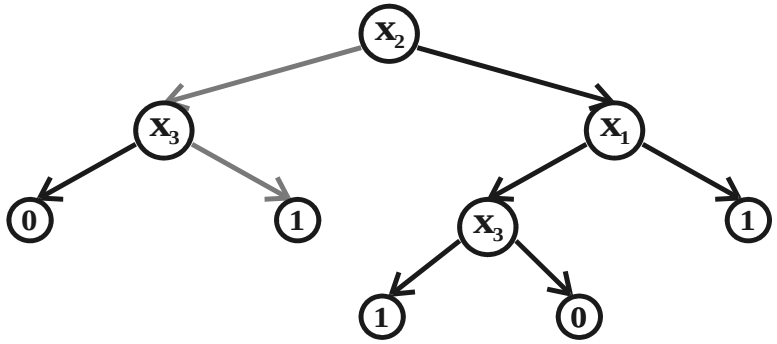
Es reicht aus, DT(f)-viele Bits von einer Eingabe zu sehen, um die Ausgabe einer booleschen Funktion $f:\{0,1\}^n \rightarrow \{0,1\}$ zu bestimmen.

Können wir nicht eine kleinere Anzahl von Bits finden, um den Funktionswert zu bestimmen?

Definition

Ein Zertifikat von einer Eingabe $a=(a_1,...,a_n)$ ist eine Menge von Variablen $Y=\{x_1 ,...,x_k\}$ mit $k \leq n$, so dass man den Funktionswert von f(a) allein durch die Bestimmung der k Werte erhält.

Beispiel



Für die Eingabe a = (0,0,1) ist $\{x_2 ,x_3\}$ ein Zertifikat von a.

Zusammenhang mit blocking sets

- Sei X ein Zertifikat von einer Eingabe a mit f(a) = 0.
- Sei Y ein Zertifikat von einer Eingabe b mit f(b) = 1.

$\Rightarrow$ Das Zertifikat X schneidet die Zertifikate Y von allen Eingaben b, und umgekehrt.

Zusammenhang mit blocking sets

Blocking sets sind Mengen, die eine Familie von Mengen in dem Sinne blockieren, dass sie mit ihnen jeweils nichtleere Schnitte haben.

Genau das leistet jedes Zertifikat X von a mit f(a) = 0 für die Familie aller Zertifikate von b mit f(b) = 1.

Definition

C(f,a) bezeichnet die minimale Größe eines Zertifikats für eine Eingabe a.

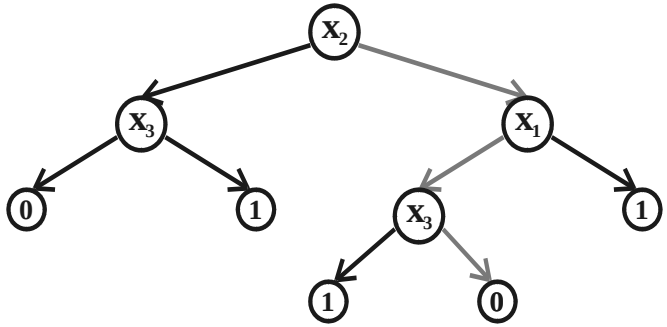
Die Zertifikatskomplexität von f ist
$C(f) = \max\{C_0(f), C_1(f)\}$, wobei

- $C_0(f) = \max_a\{C(f,a) \mid f(a) = 0\}$,

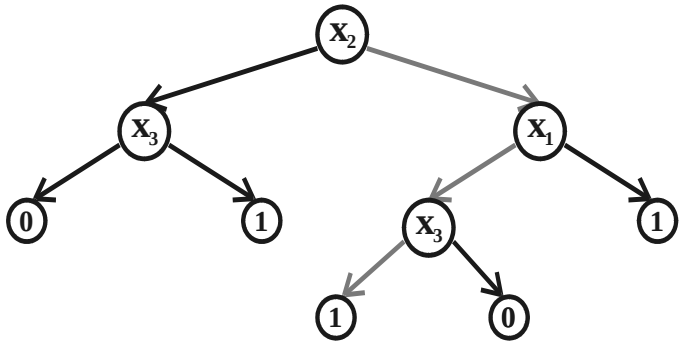
  d.h. $C_0(f)$ ist die maximale Größe eines minimalen Zertifikats für jede Eingabe a mit f(a) = 0.
- $C_1(f) = \max_a\{C(f,a) \mid f(a) = 1\}$,

  analog

Beispiel



$C_0(f) = 3$, da für a =(0,1,1) nur $\{x_1,x_2,x_3\}$ ein Zertifikat für a ist.



$C_1(f) = 3$, da für a =(0,1,0) nur $\{x_1,x_2,x_3\}$ ein Zertifikat für a ist.

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

Es gilt:

$$C(f) \leq DT(f) .$$

$\Rightarrow$ Für jede Eingabe a reicht es vollkommen aus, DT(f)-viele Bits zu sehen, um den Wert der Funktion f zu bestimmen.

Ist diese obere Grenze DT(f) optimal?

Nächstes Ziel:
Bestimmung einer unteren Schranke über allen
möglichen Entscheidungsbäumen.

Satz

Es gilt:

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

Beweis: Induktion über die Anzahl der Variablen

IA: n=1

- Die Funktion f ist konstant

$\Rightarrow DT(f) = 0 \leq 0 = C_0(f) * C_1(f)$ √

- Es existiert eine Variable mit je einer Kante zum Blatt mit der Beschriftung 0 bzw. 1

$\Rightarrow DT(f) = 1 \leq 1 = C_0(f) * C_1(f)$ √

Beweis:

Induktionsschluss: (n-k) $\rightarrow$ n

- Sei f(0,...0)=0.

$\Rightarrow$ Es existiert ein Zertifikat Y für die Eingabe a=(0,...,0) mit f(a)=0, wobei $|Y|=k \leq C_0(f)$.

Wir können o.B.d.A annehmen, dass $Y=\{x_1,...,x_k\}$ diese Eigenschaft besitzt.

Beweis:

Induktionsschluss: (n-k) → n

- Sei T_0 ein vollständiger Entscheidungsbaum der Tiefe k auf diesen k Variablen.
- Jedes Blatt entspricht eindeutig einer Belegung $a=(a_1,...a_k) \in \{0,1\}^k$ der Eingabebits x_1 bis x_k.
- Jedes Blatt wird durch einen Entscheidungsbaum T_a mit minimaler Tiefe für die Subfunktion $f_a = f(a_1,...,a_k, x_{k+1},...x_n)$ ersetzt.

Beweis:

Induktionsschluss: (n-k) $\rightarrow$ n

Es gilt

$$C_0(f_a) \leq C_0(f) \text{ und } C_1(f_a) \leq C_1(f) .$$

Es gilt sogar

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

Beweis:

Induktionsschluss: (n-k) $\rightarrow$ n

Es gilt: $C_1(f_a) \leq C_1(f) - 1$

Beweis:

- Sei $(a_{k+1},...a_n)$ eine Eingabe von f_a , wobei $f_a(a_{k+1},...,a_n) = 1$ gilt.

  Zusammen mit $a=(a_1,...,a_k)$: $f(a_1,...,a_n) = 1$.

- Nach Definition von $C_1(f)$:
  Es existiert eine Menge $Z=\{x_1,...x_m\}$ von $m \leq C_1(f)$ Variablen.

Beweis:

Induktionsschluss: (n-k) $\rightarrow$ n

Wichtige Beobachtung: $Y \cap Z \neq \emptyset$

Annahme: $Y \cap Z = \emptyset$

$\Rightarrow$ $f(0,...,0,a_{k+1},...,a_n) = 0$, weil wir die Variablen in Y mit 0 belegt haben so dass f den Wert 0 besitzt.

Aber: $f(0,...,0,a_{k+1},...,a_n) = 1$ weil wir die Variablen in Z mit den entsprechenden a_i, belegt haben, so dass f den Wert 1 besitzt.

$\Rightarrow$ Widerspruch!

Beweis:

Induktionsschluss: (n-k) $\rightarrow$ n

$\Rightarrow$ Wegen $Y \cap Z \neq \emptyset$ müssen wir nur $|Z\text{-}Y| \leq$ m-1Variablen von $(a_{k+1}...,a_n)$ belegen, damit $f_a = 1$ gilt.

$\Rightarrow C_1(f_a) \leq C_1(f) - 1$

Beweis:

Induktionsschluss: (n-k) $\rightarrow$ n

Anwendung der Induktionsvoraussetzung
$DT(f) \leq C_0(f) * C_1(f)$ auf jede Subfunktion f_a mit $a \in \{0,1\}^k$

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

<u>Insgesamt:</u>

$$\begin{aligned} DT(f) &\leq k + \max_a DT(f_a) \\ &\leq C_0(f) + C_0(f) (C_1(f) - 1) \\ &= C_0(f) C_1(f) \end{aligned}$$