Kapitel 1 – Grundlagen

1. Mathematische Grundlagen

2. Beispielrechner ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Mathematische Grundlagen

- Verständigung auf gemeinsame Basis
- Die meisten Begriffe sollten bekannt sein, bzw. werden in anderen Vorlesungen noch formal und im Detail eingeführt.
- Hier: Informale, möglichst intuitive Einführung
  - Mengen, Funktionen, Relationen
  - Boolsche Algebra $(\{0,1\},\wedge,\vee,\neg)$
  - Graphen, O-Notation
  - Beweistechniken

„Philosophie" der Mathematik

die gelten

- Gegeben gewisse Aussagen (Axiome), welche andere Aussagen lassen sich aus ihnen herleiten?
- Sind die Axiome wahr und existiert eine solche Herleitung (Beweis), so sind die Folgerungen unumstößlich und indiskutabel wahr!
- Beschreiben die Axiome etwa ein physikalisches System, so gelten die hergeleiteten Folgerungen für dieses System.
- Die Frage, ob Axiome Realitätsbezug haben, ist aber außerhalb der (reinen) Mathematik!

Menge (Naive Definition)

Definition

Eine Menge ist eine Zusammenfassung von wohldefinierten, paarweise verschiedenen Objekten zu einem Ganzen.

- Die Objekte nennt man Elemente der Menge.
  (Für eine formal vollständige Definition der Menge bräuchte man mehrere Vorlesungsstunden.)

- Notation: Sind $a_1, a_2, \ldots, a_n$ paarweise verschieden, so schreibt man die Menge M, die aus ihnen besteht, als $M = \{a_1, a_2, \ldots, a_n\}$.
  - $a_i \in M$ bezeichnet, dass a_i Element von M ist.

Beispiele für Mengen

- Leere Menge: $\cancel{\emptyset}$ (es gibt kein $a \in \emptyset$). $\mathbb{N}$
- Menge der natürlichen Zahlen: $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Menge der booleschen Werte: $\mathbb{B} = \{0, 1\}$. $\mathbb{B}$

  falsch wahr
- Achtung: Die Anordnung von Elementen der Menge und gegebenenfalls Wiederholungen sind belanglos: $\{a, b, c\} = \{c, a, b\} = \{a, a, b, c, a, b\}$.
- Eine Menge kann Elemente enthalten, die selber Mengen sind, z.B. $\{a, b, \{a\}, \{a, b\}\}$ = M enthält 4 Elemente, wobei die letzten beiden wieder Mengen sind.

Spezifikation von Mengen

- Man kann eine Menge durch Angabe von Zusatzbedingungen spezifizieren.

  Beispiele:

  - Menge der ganzen Zahlen:
    $\mathbb{Z} = \{z, -z \mid z \in \mathbb{N}\}$.

    $\{0, 1, 2, 3, 4, \ldots\}$

    Menge d. Brüche" bedeutet, dass sich p, q nur durch 1 teilen lassen.

  - Menge der rationalen Zahlen:
    $\mathbb{Q} = \{p/q \mid p \in \mathbb{N}, q \in \mathbb{Z}, q \neq 0, p, q \text{ teilerfremd}\}$.

    $\frac{4}{6} = \frac{2}{3}$

    nicht tf tf

  - Menge der endlichen Zeichenketten:
    $STRINGS = \{s_1 s_2 \ldots s_n \mid n \in \mathbb{N}, s_i \text{ ein Buchstabe}\}$.

Untermengen, Potenzmenge, Mächtigkeit

„$\subset$"

Menge $\{a\}$ ist Untermenge

- Menge U ist Untermenge von M, wenn jedes Element von U auch Element von M ist.
  - Notation: $U \subset M$ bzw. $M \supset U$
  - Achtung: $\{a\} \subset \{a,b,c\}$, aber $a \in \{a,b,c\}$

    a ist Element
- Potenzmenge von M : $Pot(M) = \{m \mid m \subset M\}$.
  - $|Pot(\{a,b,c\})| \rightsquigarrow 8$

    $= \{\underset{1}{\varnothing}, \underset{2}{\{a\}}, \underset{3}{\{b\}}, \underset{4}{\{c\}}, \underset{5}{\{a,b\}}, \underset{6}{\{a,c\}}, \underset{7}{\{b,c\}}, \underset{8}{\{a,b,c\}}\}$
- Die Anzahl $|M|$ der Elemente einer Menge M heißt Mächtigkeit oder Kardinalität von M.

Operationen auf Mengen 1/2

- Mengendifferenz: $M_1 \setminus M_2 = \{m \mid m \in M_1 \text{ und } m \notin M_2\}$

- Mengenschnitt: $M_1 \cap M_2 = \{m \mid m \in M_1 \text{ und } m \in M_2\}$

Operationen auf Mengen 2/2

- Mengenvereinigung: $M_1 \cup M_2 = \{m \mid m \in M_1 \text{ oder } m \in M_2\}$

- Kartesisches Produkt:

$$M_1 \times M_2 = \{(m_1, m_2) \mid m_1 \in M_1 \text{ und } m_2 \in M_2\}$$

  - (m_1, m_2) ist ein Tupel, bei dem es, im Gegensatz zu einer Menge $\{m_1, m_2\}$, auf die Reihenfolge ankommt!

    $\hookrightarrow = \{m_2, m_1\}$

  - Notation: $M^n = M \times \cdots \times M$ (n mal). $= \{(m_1, \ldots, m_n) \mid m_1 \in M, m_2 \in M, \ldots, m_n \in M\}$

$M^2 = M \times M$

Operationen auf Mengen 2/2

- Mengenvereinigung: $M_1 \cup M_2 = \{m \mid m \in M_1 \text{ oder } m \in M_2\}$

- Kartesisches Produkt:

$$M_1 \times M_2 = \{(m_1, m_2) \mid m_1 \in M_1 \text{ und } m_2 \in M_2\}$$

  - (m_1, m_2) ist ein Tupel, bei dem es, im Gegensatz zu einer Menge $\{m_1, m_2\}$, auf die Reihenfolge ankommt!
  - Notation: $M^n = M \times \cdots \times M$ (n mal).

SMILE – Mengen

$|\{\emptyset, \{1\}, \ldots \{5\}, \ldots\}|$

El. 1 $\notin UM_1$	1	2	3	4	5
UM_1	0	1	0	1	0
UM_2	1	1	0	0	0

$\{2,4\}$

$\{1,2\}$

Frage: Welche der folgenden Aussagen sind wahr?

a. $\text{Pot}(\{la, le, lu\}) = \{\emptyset, \{la\}, \{le\}, \{lu\}, \{la, le\}, \{la, lu\}, \{le, lu\}, \{la, le, lu\}\}$ 3 Elemente $\rightarrow 2^3 = 8$ Gilt

b. $|Pot(\{1,2,3,4,5\})| = 32$ unknown

$2^5 = 32$

00000
00001
00010
⋮

c. $\{a,a,b,c\} \setminus \{a,b\} = \{a,c\}$ gilt nicht!

$\{a,a,b,c\} = \{a,b,c\}$

$\{a,b,c\} \setminus \{a,b\} = \{c\}$

d. $|\{a,a,b,c\}| = 3$ gilt

$= |\{a,b,c\}| = 3$

e. $(\mathbb{Z} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{Z}$ gilt nicht!

Relationen

Definition

Eine Relation R zwischen den Mengen X und Y ist eine Teilmenge von $X \times Y$.

$R := <$

$0 < 1$

- Notation: Statt $(x,y) \in R$ schreibt man xRy.
- Beispiele:
  - Relation $<$ zwischen $\mathbb{N}$ und $\mathbb{N}$.
    $<= \{(0,1),(0,2),\ldots,(1,2),(1,3),\ldots\}$
  - $R = \{(a,b) \mid a,b \in \mathbb{N}, a+b \text{ ungerade }\}$

$< : \mathbb{N} \times \mathbb{N}$

$x = 0$

$y = 1$

$y = 2$

$y = 3$

$(2,5) \in R$

Funktionen

Definition

Seien X und Y Mengen. Eine Funktion $f : X \to Y$ ist eine Relation zwischen den Mengen X und Y, wobei für jedes $x \in X$ genau ein $y \in Y$ existiert, so dass $(x,y) \in f$.

- X heißt Definitionsbereich, Y Wertebereich von f.

- Notation: Statt $(x,y) \in f$ schreibt man $y = f(x)$.

- Beispiele: x y
  - Quadratfunktion $f : \mathbb{N} \to \mathbb{N}, f(x) = x^2$.
    $f = \{(0,0),(1,1),(2,4),(3,9),(4,16),(5,25),\dots\}$
  - Kardinalitätsfunktion $f : Pot(\{a,b,c\}) \to \mathbb{N}$. „M"
    $f = \{(\varnothing,0),(\{a\},1),(\{b\},1),(\{c\},1),(\{a,b\},2),$
    $(\{a,c\},2),(\{b,c\},2),(\{a,b,c\},3)\}$

    $\in f$

    da {a,b} besteht aus 2 Elementen

Beispiele: Relationen, Funktionen

- Jede Funktion ist auch eine Relation. ✓
- Aber es gibt natürlich Relationen, die keine Funktionen sind. (liegt an dem „genau" in Def. Folie 12)
- Beispiel:
  - $\sin^{-1}(x) = \{(\sin(x), x) \mid x \in \mathbb{R}\}$ ist eine Relation, aber keine Funktion!

Wertebereich — Bildbereich

$\sin(x) = \{(x, \sin(x)) \mid x \in \mathbb{R}\}$

Summen und Produkte (Notation)

- Wir schreiben für $f : \mathbb{N} \to \mathbb{R}$

$$\sum_{i=m}^{n} f(i) = f(m) + f(m+1) + \cdots + f(n-1) + f(n)$$

$$\prod_{i=m}^{n} f(i) = f(m) \cdot f(m+1) \cdot \cdots \cdot f(n-1) \cdot f(n)$$

- Beispiel:

$$\sum_{i=0}^{5} i^2 = 0^2 + 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$$

- Schreibweise mit beliebigen Bedingungen:

$$\sum_{i,j>0, i+2j\leq 5} (i^2/j) = (1^2/1) + (1^2/2) + (2^2/1) + (3^2/1) = 14,5$$

$i \in \{1,2,3\}$

$j \in \{1,2\}$

Boolesche Algebra $(\{0,1\}, \wedge, \vee, \neg)$ 1/4

Definition

$x, y, z \in \mathbb{B}$

$x \mapsto 0/1$
$y \mapsto 0/1$
$z \mapsto 0/1$

- $\mathbb{B} := \{0, 1\}$
- Konjunktion (UND-Verknüpfung) $\wedge : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$
  $0 \wedge 0 = 0, \quad 0 \wedge 1 = 0, \quad 1 \wedge 0 = 0, \quad 1 \wedge 1 = 1$
- Disjunktion (ODER-Verknüpfung) $\vee : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$
  $0 \vee 0 = 0, \quad 0 \vee 1 = 1, \quad 1 \vee 0 = 1, \quad 1 \vee 1 = 1$
- Negation $\neg : \mathbb{B} \to \mathbb{B}$
  $\neg 0 = 1, \quad \neg 1 = 0$
- Boolescher Ausdruck
  - Die Elemente aus $\mathbb{B}$ sind boolesche Ausdrücke.
  - Seien A und B boolesche Ausdrücke, dann sind $(A \wedge B)$, $(A \vee B)$, $(\neg A)$ wieder boolesche Ausdrücke.

$x \wedge (y + z)$

$x = 1$
$y = 0$
$z = 0$

$\| $

$1 \wedge (0 \vee 0)$
$= 1 \wedge 0$
$= 0$

Boolesche Algebra $(\{0,1\}, \wedge, \vee, \neg)$ 2/4

Konventionen

- Man schreibt auch $\cdot$ statt $\wedge$ und $+$ statt $\vee$.
- Für $\neg x$ sind viele Notationen üblich: $\sim x$, x' oder $\overline{x}$.
- Zur Vereinfachung der Notation bei booleschen Ausdrücken vereinbaren wir:
  Negation $\sim$ bindet stärker als Konjunktion $\cdot$, Konjunktion $\cdot$ / $\wedge$ bindet stärker als Disjunktion $+$ / $\vee$

Boolesche Algebra $(\{0,1\},\wedge,\vee,\neg)$ 3/4

$\cdot$ $+$

Axiome der booleschen Algebra

Kommutativität: $x+y=y+x$

$x\cdot y=y\cdot x$

Assoziativität: $x+(y+z)=(x+y)+z$

$x\cdot(y\cdot z)=(x\cdot y)\cdot z$

Absorption: $x+(x\cdot y)=x$

Auslöschung

$x\cdot(x+y)=x$

$x=1 \rightarrow 1\vee(1\cdot y)=1=x$

$x=0 \rightarrow 0\vee(\underbrace{0\cdot y}_{=0})=0\vee 0=0=x$

Distributivität: $x+(y\cdot z)=(x+y)\cdot(x+z)$

$x\cdot(y+z)=(x\cdot y)+(x\cdot z)$

Komplement: $x+(y\cdot\neg y)=x$

$x\cdot(y+\neg y)=x$

immer gleich

$(0\wedge\neg 0)=0\wedge 1=0$

$(1\wedge\neg 1)=1\wedge 0=0$

UNI FREIBURG

Boolesche Algebra $(\{0,1\}, \wedge, \vee, \neg)$ 3/4

Axiome der booleschen Algebra

Kommutativität:	$x+y=y+x$
	$x \cdot y = y \cdot x$
Assoziativität:	$x+(y+z)=(x+y)+z$
	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Absorption:	$x+(x \cdot y)=x$
	$x \cdot (x+y)=x$
Distributivität:	$x+(y \cdot z)=(x+y) \cdot (x+z)$
	$x \cdot (y+z)=(x \cdot y)+(x \cdot z)$
Komplement:	$x+(y \cdot \neg y)=x$
	$x \cdot (y+\neg y)=x$

SMILE – Boolesche Ausdrücke

$13 = 42$ ↯ gleichbed. mit $13 \neq 42$

Frage: Welche dieser Umformungen Boolescher Ausdrücke sind richtig? Das heißt, die Gleichung ist immer erfüllt für alle möglichen Werte von $x, y \in \mathbb{B}$.

a. $x + 1 = 1 + x \cdot y$ $\iff$ $1 = 1$

b. $x + \neg x = x$ $x = 0 \to 0 + 1 \neq 0$ ↯

c. $(x \cdot (\neg x + (y \cdot \neg y))) = x$

$\underbrace{\underbrace{\underbrace{\neg x + \underbrace{(y \cdot \neg y)}_{=0}}_{\neg x + 0}}_{\neg x}}_{x \cdot \neg x = 0}$ $\Rightarrow$ $0 = x$ ↯

x kann auch 1 sein $\Rightarrow 0 = 1$ ↯

Boolesche Algebra $(\{0,1\}, \wedge, \vee, \neg)$ 4/4

$\cdot \quad +$

- Neben der vorgestellten gibt es weitere boolesche Algebren, in denen diese Axiome gelten.
- Die folgenden Regeln sind aus den Axiomen ableitbar:

Weitere Regeln für boolesche Algebren

Doppeltes Komplement:	$\neg(\neg x) = x$
Idempotenz:	$x + x = x \cdot x = x$
De-Morgan-Regel:	$\neg(x + y) = (\neg x) \cdot (\neg y)$
	$\neg(x \cdot y) = (\neg x) + (\neg y)$
Consensus-Regel:	$(*)\ (x \cdot y) + ((\neg x) \cdot z)$
Resolutions-Regeln	$= (x \cdot y) + ((\neg x) \cdot z) + (y \cdot z)$
	$(x + y) \cdot ((\neg x) + z)$
	$= (x + y) \cdot ((\neg x) + z) \wedge (y + z)$

„mit $y = z = 1$ habe ich (*) erfüllt (= 1)"

$x = 1: (1+y) \wedge (0+z) = 1 \wedge z = z$

$x = 0: (0+y) \wedge (1+z) = y$

UNI FREIBURG

Boolesche Funktion

Definition

Eine boolesche Funktion f in n Variablen und mit m Ausgängen ist eine Funktion

$$f : \mathbb{B}^n \to \mathbb{B}^m (n, m \in \mathbb{N}).$$

Ein- Ausgänge

- Die Menge aller booleschen Funktionen in n Variablen mit m Ausgängen ist

$$\mathbb{B}_{n,m} := \{f \mid f : \mathbb{B}^n \to \mathbb{B}^m\}.$$

$f : \mathbb{B}^n \to \mathbb{B}$ $\quad$ $f_{SK} : \mathbb{B}^4 \to \mathbb{B}$

- Wir schreiben abkürzend $\mathbb{B}_n$ statt $\mathbb{B}_{n,1}$.
- Ein digitaler Schaltkreis ohne Speicherelemente, mit n Eingängen und m Ausgängen realisiert eine solche Funktion! (Details später)

Gerichteter Graph

Definition

$G = (V, E)$ ist ein gerichteter Graph, wenn folgendes gilt:

$Q(e_1) = v_1$

$Z(e_1) = v_2$

- V endliche, nichtleere Menge (Knoten)
  vertex
- E endliche Menge (Kanten)
  edge
- Abbildungen $Q : E \to V$ und $Z : E \to V$
  $Q(e)$ ist Quelle, $Z(e)$ Ziel einer Kante e
- Abbildungen $indeg : V \to \mathbb{N}$ und $outdeg : V \to \mathbb{N}$
  $indeg(v) = |\{e \mid Z(e) = v\}|$ ist der Eingangsgrad,
  $outdeg(v) = |\{e \mid Q(e) = v\}|$ der Ausgangsgrad von v.

outdeg = out degree

Pfade in gerichteten Graphen

- Ein Knoten mit
  - $indeg(v) = 0$ heißt Wurzel.
  - $outdeg(v) = 0$ heißt Blatt.
  - $outdeg(v) > 0$ heißt innerer Knoten.

- Ein Pfad (der Länge k) in G ist eine Folge von k Kanten $e_1, e_2, \ldots, e_k$ $(k \geq 0)$ mit $Z(e_i) = Q(e_{i+1})$ für alle i $(k-1 \geq i \geq 1)$

- Ein Zyklus in G ist ein Pfad der Länge ≥ 1 in G, bei dem Ziel und Quelle identisch sind (G heißt azyklisch, falls kein Zyklus in G existiert).

- Die Graph-Tiefe eines azyklischen Graphen ist definiert als die Länge des längsten Pfades in G.

Bäume, Binäre Bäume

Blätter

Definition

Ein Baum ist ein gerichteter, azyklischer Graph mit genau einer Wurzel w ($indeg(w) = 0$) und $indeg(v) = 1$ für alle andere Knoten v. Ein Baum heißt binär (bzw. Binärbaum), wenn für seine innere Knoten v $outdeg(v) \leq 2$ gilt.

Beispiele:

Baum:

Binärbaum:

Groß-O-Notation (1/2)

positive, reelle Zahlen (inklusive 0)

- Seien $f, g : \mathbb{R}_0^+ \to \mathbb{R}_0^+$.
  Man schreibt $f(x) \in O(g(x))$, wenn es $c \in \mathbb{R}_0^+, x_0 \in \mathbb{R}_0^+$ gibt, so dass $f(x) \leq c \cdot g(x)$ für alle $x > x_0$ gilt.
  - Beispiel: $5x + 2 \in O(x^2)$ ← besser: $o(x)$
    Beweis: Setze $c = 5, x_0 = 1$
    $5x + 2 \leq 5 \cdot x^2$, für $x > 1$.

    $x = 1$: $5 \cdot 1 + 2 = 7 \not\leq 5 \cdot 1^2 = 5$
    $x = 2$: $5 \cdot 2 + 2 = 12 \leq 5 \cdot 2^2 = 20$

- Groß-O-Notation wird verwendet, um Größe von parametrisierten Objekten (z.B. Graphen), Laufzeit von Algorithmen (Anzahl von Rechenschritten in Abhängigkeit von der Eingabe) usw. asymptotisch, d.h. bis auf eine multiplikative Konstante, abzuschätzen.

- Die Notation $f(x) = O(g(x))$ ist weit verbreitet, aber eigentlich falsch, da $O(g(x))$ eine Menge ist. So folgt aus $f(x) = O(g(x))$ und $h(x) = O(g(x))$ keinesfalls $f(x) = h(x)$!

$f(x) = 5x + 2$
$h(x) = 2x^2$
$\Rightarrow f(x), h(x) \in O(x^2)$

Groß-O-Notation (2/2)

Groß-O-Notation (2/2)

SMILE – O-Notation

Gegeben: blau schwarz grün

$f(x) = \sqrt{x} + 2, \quad g(x) = 0,5e^x, \quad h(x) = x + 1,$

Welche Aussagen sind dann wahr?

- $g \in O(h)$ NEIN
- $h \in O(f)$ NEIN
- $f \in O(g)$ JA

SMILE – O-Notation

Gegeben:

$f(x) = \sqrt{x} + 2, \quad g(x) = 0,5e^x, \quad h(x) = x + 1,$ g

Welche Aussagen sind dann wahr?

- $g \in O(h)$ –
- $h \in O(f)$ –
- $f \in O(g)$ +

$\forall x > x_0 : f(x) < h(x)$

Beweistechniken

- Sukzessive Folgerungen bzw. Direkter Beweis
- Indirekter Beweis bzw. Beweis durch Widerspruch
- Vollständige Induktion

Sukzessive Folgerungen

Gegeben Aussage A, es soll Aussage B bewiesen werden.

- Sukzessive Folgerungen:
  Aus A folgt C, aus C folgt D, aus D folgt B, also gilt B.

$$A \to C \to D \to \underline{B}$$

$\square$

q.e.d.

Beispiel: Sukzessive Folgerungen

„$f \rightsquigarrow g \rightsquigarrow h$"

- Gegeben f, g, h, $\quad f(x) \in O(g(x))$, $g(x) \in O(h(x))$.
  Dann gilt $f(x) \in O(h(x))$.

Beweis:

1. Aus $f(x) \in O(g(x))$ folgt die Existenz von $c_f, x_{0f} : f(x) \leq c_f \cdot g(x)$ für $x > x_{0f}$. Aus $g(x) \in O(h(x))$ folgt die Existenz von $c_g, x_{0g} : g(x) \leq c_g \cdot h(x)$ für $x > x_{0g}$.
2. Man setze $x_0 := max\{x_{0f}, x_{0g}\}$. Dann gilt für $x > x_0$ sowohl $f(x) \leq c_f \cdot g(x)$ als auch $g(x) \leq c_g \cdot h(x)$.
3. Man setze $c := c_f \cdot c_g$. Dann gilt für $x > x_0$:
   $f(x) \leq c_f \cdot g(x) \leq c_f(c_g \cdot h(x)) = c \cdot h(x)$.
   Dies bedeutet aber gerade $f(x) \in O(h(x))$

Indirekter Beweis 1/2

Annahme: $\neg S$

$31 = 42$ ↯ $\rightsquigarrow S$

Es soll Aussage S bewiesen werden.

- Indirekter Beweis: Man nimmt an, $\neg S$ (also die Umkehrung von S) würde gelten. Daraus leitet man einen Widerspruch her (z.B. “es gilt C **und** $\neg C$”, “$31 = 42$”, ...).
- Da der Widerspruch schrittweise aus $\neg S$ logisch hergeleitet wurde, kann $\neg S$ nicht gelten und somit muss S gelten.

Indirekter Beweis 2/2

aus A folgt B

$A = 1 \rightarrow B = 1$

- Betrachte den Spezialfall $S \cong A \Rightarrow B$.
  - Dann ist $\neg S \cong A \wedge \neg B$. Man nimmt also an, dass A gilt, aber $\neg B$.
  - Ergibt sich aus der Annahme ein Widerspruch, dann muss aus der Gültigkeit von A die Gültigkeit von B folgen.
  - Ergibt sich der Widerspruch speziell durch Herleitung von $\neg A$ aus $\neg B$, dann reduziert sich der Widerspruchsbeweis auf den Spezialfall Beweis der "Kontraposition" $\neg B \Rightarrow \neg A$.
  - $A \Rightarrow B$ und $\neg B \Rightarrow \neg A$ sind logisch äquivalent.

    $B = 0 \rightarrow A = 0$
  - Implizit setzt man immer die Gültigkeit sämtlicher Axiome voraus. Sei Ax die Aussage "Sämtliche Axiome gelten".
  - Dann ist $S' = (A \wedge Ax) \Rightarrow B$ zu beweisen.
  - Annahme ist dann also: $\neg S' = A \wedge Ax \wedge \neg B$ gilt.

Beispiel: Indirekter Beweis

- Zu zeigen: $x^2 \notin O(x)$

Beweis:

- Wir nehmen an, dass $x^2 \in O(x)$ wäre. Dann gibt es c und x_0, so dass für $x > x_0$ gilt:

$$x^2 \leq c \cdot x \tag{1}$$

- Nun suchen wir ein x_1, für das $x_1^2 = c \cdot x_1$. Dies ist für $x_1 = c$ der Fall.

$x \cdot x$ $\quad$ $x_1 < x$

- Für alle $x > x_1 = c$ ist $x^2 > c \cdot x$. Man wähle ein $x_2 > max\{x_0, x_1\}$. Dann gilt auch für x_2:

$x_2 > c$

$$x_2^2 > c \cdot x_2 \tag{2}$$

- Andererseits muss für x_2 auch (1) gelten. Widerspruch! Somit kann die Annahme nicht stimmen.

Vollständige Induktion

- Die vollständige Induktion ist eine Beweismethode für Aussagen, die für alle natürlichen Zahlen n gelten sollen.
- Zuerst wird die Aussage für den Basisfall $n = 0$ beweisen (manchmal auch $n = 1$ oder höher).
- Dann wird der Induktionsschritt durchgeführt: Unter der Annahme, dass die Aussage für n gilt (Induktionsvoraussetzung) wird bewiesen, dass die Aussage auch für $n + 1$ gilt.
- Daraus folgt die Gültigkeit der Aussage für alle natürlichen Zahlen.

$n=0$, n
1 – 1
2 – $(n+1)$
3 –

Vollständige Induktion: Beispiel (1/2)

- **Behauptung:**

  $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$ gilt für alle $n \in \mathbb{N}$.

- **Induktionsanfang:**
  Zeige die Behauptung für $n = 1$.

  $\sum_{k=1}^{1} \frac{1}{k(k+1)} = \frac{1}{1(1+1)} = \frac{1}{2} \overset{!}{=} \frac{1}{1+1}$

Vollständige Induktion: Beispiel (2/2)

- **Induktionsvoraussetzung** (IV)**:**
  Nehme an, die Behauptung gilt für *ein* $n \in \mathbb{N}$.
  Also: Es gibt ein n für das gilt: $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$

- **Induktionsschritt:**
  Zeige die Behauptung für $n+1$.

(n+1)-Summenglied

$$\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \boxed{\sum_{k=1}^{n} \frac{1}{k(k+1)}} + \frac{1}{(n+1)(n+2)} \overset{\text{IV}}{=} \frac{n}{n+1} + \frac{1}{(n+1)(n+2)}$$

$$= \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^{\cancel{2}}}{(\cancel{n+1})(n+2)} = \frac{(n+1)}{(n+2)} = \frac{(n+1)}{(n+1)+1} \quad \square$$

qed.

Kapitel 1 – Grundlagen

1. Mathematische Grundlagen
2. **Beispielrechner ReTI**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

ReTI (Rechner Technische Informatik)

- Ursprünglich eingeführt in [*Keller*, *Paul*] unter dem Namen ReSa.
- Hier wird ReTI zunächst abstrakt eingeführt.
  - Alle Speicher bestehen aus unendlich vielen Speicherzellen, die beliebig große ganze Zahlen aufnehmen können.
- Später wird die tatsächliche Implementierung von ReTI unter realistischen Annahmen thematisiert.

Abstrakte ReTI-Maschine

Harvard-Architektur
- getrennter Prg-/Datenspeicher

von Neumann:
gemeinsamer Prg.-/Datensp.

- Zwei unendlich große Speicher
  - Datenspeicher S für Daten (beliebig große Zahlen).
  - $S(i) =$ Inhalt von Zelle i des Datenspeichers, $i \in N$ Adresse.
  - Programmspeicher P für Maschinenbefehle.
  - Lade-/Speicher-, Rechen-, Sprungbefehle - siehe später.
  - $P(i) =$ Inhalt von Zelle i des Programmspeichers.
- Zentraleinheit CPU (Central Processing Unit)
  - Vier für Benutzer sichtbare Register.
  - $PC =$ Befehlszähler (Program Counter).
  - $ACC =$ Akkumulator.
  - $IN1$, $IN2 =$ Indexregister 1 und 2.

Aufbau von ReTI

Programmablauf

- Programme bzw. Daten stehen beim Start der Maschine in P bzw. S.
- Programm beginnt bei Zelle 0 von P.
- Inhalt von P wird nicht geändert.

  festes Programm, daher brauchen auch die Indexregister

- Maschine arbeitet in Schritten $t = 1, 2, \ldots$
  In jedem Schritt t:
  - Ausführung eines Befehls: $P(PC)$ wird als Befehl interpretiert und in Schritt t ausgeführt.
    aus der Zelle mit Index "PC"
  - PC erhält neuen Wert (abhängig von Befehl).
- Bei Programmstart ist $PC = 0$.

ReTI-Befehle und ihre Wirkung

- Load/Store: Laden von Werten aus dem Datenspeicher S bzw. Schreiben von Werten in S.
- Compute: Berechnungen (hier zunächst Addition und Subtraktion).
  - Mit Werten im Datenspeicher S.
  - Mit Absolutwerten (Immediate).

$ACC := ACC + S(i)$

$ACC := ACC + i$

- Indexregister: Indirekte Speicheradressierung (siehe unten).
- Sprungbefehle: Bedingte und unbedingte Sprünge.

– if-Anweisungen
– Schleifen realisieren zu können.

Load/Store

S

Transport von Daten zwischen *ACC* und Datenspeicher.

- LOAD *i*:
  Lädt Inhalt $S(i)$ von Speicherzelle *i* in Akkumulator *ACC* und erhöht *PC* um 1.

- STORE *i*:
  Speichert den Inhalt von *ACC* in $S(i)$ und erhöht *PC* um 1.

UNI FREIBURG

Load/Store: Übersicht

Befehl	Wirkung
LOAD i	$ACC := S(i) \quad PC := PC + 1$
STORE i	$S(i) := ACC \quad PC := PC + 1$

Beispielprogramm

Ein Programm, das Inhalte von Speicherzelle $S(0)$ $(= x)$ und $S(1)$ $(= y)$ vertauscht.

0	LOAD 0;	$ACC := S(0) = x$
1	STORE 2;	$S(2) := ACC = x$
2	LOAD 1;	$ACC := S(1) = y$
3	STORE 0;	$S(0) := ACC = y$
4	LOAD 2;	$ACC := S(2) = x$
5	STORE 1;	$S(1) := ACC = x$

$S(0) =$ y(3)
$S(1) = y$
$S(2) = x$ (1)
$ACC = x$ (0)
y (2)

Compute-Befehle

Verknüpfe den Inhalt von ACC mit $S(i)$ oder mit einer Konstante und speichere das Ergebnis in ACC ab.

- ADD, SUB = Compute *memory*-Befehle
- $ADDI, SUBI$ = Compute *immediate*-Befehle
- Beides zusammen ergibt die Compute-Befehle.

Bei Compute memory: Interpretiere Parameter i direkt als Speicheradresse.

Befehl	Wirkung
ADD i	$ACC := ACC + S(i) \quad PC := PC + 1$
SUB i	$ACC := ACC - S(i) \quad PC := PC + 1$

Immediate-Befehle

Interpretiere Parameter i direkt als Konstante.

Befehl	Wirkung	
LOADI i	$ACC := i$	$PC := PC + 1$
ADDI i	$ACC := ACC + i$	$PC := PC + 1$
SUBI i	$ACC := ACC - i$	$PC := PC + 1$

- Anmerkung: ADDI und SUBI sind Compute Befehle. LOADI ist den Load-/Store-Befehlen zuzuordnen.

Indexregister-Befehle

Befehl	Wirkung	
LOADINj i	$ACC := S(INj + i)$ $(j \in \{1,2\})$	$PC := PC + 1$
STOREINj i	$S(INj + i) := ACC$ $(j \in \{1,2\})$	$PC := PC + 1$
MOVE S D	$D := S$ $(D \in \{ACC, IN1, IN2\},$ $S \in \{ACC, IN1, IN2, PC\})$	$PC := PC + 1$
MOVE S PC	$PC := S$ $(S \in \{ACC, IN1, IN2\})$	

Source Destination

Unterscheidung, ob D = PC ist oder nicht!

Beispielprogramm für Indexregister-Befehle

$S(0) = x, S(1) = y$
Kopiere y in Zelle $S(x)$:

0	LOAD 0;	$ACC := S(0) = x$
1	MOVE ACC $IN1$;	$IN1 := ACC = x$
2	LOAD 1;	$ACC := S(1) = y$
3	STOREIN1 0;	$S(x) = S(IN1 + 0) := ACC = y$

$\Downarrow$

$S(x) = y$

Sprung-Befehle

Manipulation des Befehlszählers.

- JUMP für *unbedingte* Sprünge,
- JUMP_c mit $c \in \{<, =, >, \leq, \neq, \geq\}$ für *bedingte* Sprünge.
- Mit bedingten Sprüngen kann man *Programmschleifen* und *bedingte Anweisungen* realisieren!

unbedingt

bedingte

Befehl	Wirkung
JUMP i	$PC := PC + i \quad (i \in \mathbb{Z})$
$\text{JUMP}_c\ i$	$PC := \begin{cases} PC + i, & \text{falls } ACC\ c\ 0 \\ PC + 1, & \text{sonst} \end{cases}$ $(i \in \mathbb{Z}, c \in \{<, =, >, \leq, \neq, \geq\})$

for: Abbruch

Bed. prüfen

Schleifen-block

JUMP

PC = PC+1

Schleifen-zähler modifizieren

Beispielprogramm

$y=3 \to y=2 \to x$ | $y=1 \to x+x$ | $y=0 \to x+x+x$ | $y=-1$ DONE

SMILEY analog!

$S(0) = x;\ S(1) = y,\ y \geq 0$

$\Rightarrow$ Multiplikation von $x \cdot y = S(2)$

0	LOADI 0;	$ACC := 0$
1	STORE 2;	$S(2) := 0$ → Initialisierung
2	LOAD 1;	$ACC := S(1)$ → Schleifenzähler
3	SUBI 1;	$ACC := ACC - 1$ | $y = y-1$
4	STORE 1;	$S(1) := ACC$
5	JUMP ≤ 5;	$PC := PC + 5$, falls $ACC < 0$
6	LOAD 2;	$ACC := S(2)$
7	ADD 0;	$ACC := ACC + S(0)$
8	STORE 2;	$S(2) := ACC$
9	JUMP -7;	$PC := PC - 7$

Schleifenkörper

$S(2) = \underbrace{x + \ldots + x}_{y}$

$ACC = ACC + x$

Zusammenfassung

- Mathematik erlaubt es uns, reale Zusammenhänge formal zu fassen und allgemeingültige Folgerungen aus ihnen herzuleiten.
- Rechner ReTI wird uns im weiteren Verlauf der Vorlesung als Illustrator und Anwendungsbeispiel für die vorgestellten Konzepte dienen.

Motivation

TTL :

- Ein Rechner speichert, verarbeitet und produziert Informationen.
- Alle Ergebnisse müssen als Funktion der Anfangswerte exakt reproduzierbar sein.

→ Informationsspeicherung und Verarbeitung müssen exakt sein.

schön noise

- Probleme: Noise, Crosstalk, Abschwächung

→ Es gibt keine exakte Datenübertragung oder Datenspeicherung.

→ Ziel: Quantisierung der Informationsspeicherung mit Signal groß gegenüber maximaler Störung

- Binär-Codierung (nur zwei Zustände) ist die einfachste (und sicherste) Signal-Quantisierung.
- BIT (0, 1) als grundlegende Informationseinheit

Motivation

- Ein Rechner kann üblicherweise
  - Zeichen verarbeiten (Textverarbeitung)
  - mit Zahlen rechnen
  - Bilder, Audio- und Videoinformationen verarbeiten und darstellen ...
- Ein Algorithmus kann zwar prinzipiell mit abstrakten Objekten verschiedener Art operieren, aber diese müssen im Rechner letztendlich als Folgen von Bits repräsentiert werden.

→ Kodierung!

Kapitel 2.1 - Kodierung von Zeichen

- Wie werden im Rechner Zeichen dargestellt ?
- Codes fester Länge
- “Längenoptimale Kodierungen” von Zeichen: Häufigkeitscodes (Bsp.: Huffman-Code)

Kapitel 2 – Kodierung

1. **Kodierung von Zeichen**
2. Kodierung von Zahlen
3. Anwendung: ReTI ⇝ Kodierung von Befehlen

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Alphabete und Wörter

"a", "b", ...

Definition

Eine nichtleere Menge $A = \{a_1, \ldots, a_m\}$ heißt (endliches) Alphabet der Größe m.
$a_1, \ldots, a_m$ heißen Zeichen des Alphabets.

- $A^* = \{w \mid w = b_1 \ldots b_n \text{ mit } n \in \mathbb{N}, \forall i \text{ mit } 1 \leq i \leq n : b_i \in A\}$ ist die Menge aller Wörter über dem Alphabet A.
- $|b_1 \ldots b_n| := n$ heißt Länge des Wortes $b_1 \ldots b_n$.
- Das Wort der Länge 0 wird mit ε bezeichnet.

Beispiel:
Sei $A = \{a, b, c, d\}$.
Dann ist $bcada$ ein Wort der Länge 5 über A.

ε A^*

Code

$a_1 \in A \Rightarrow c(a_1) = 01001$

Codewörter können unters. Länge haben „$c: A \to \{0,1\}^{n'}$ mit $n' = 1, 2, 3, \ldots$"

Sei $A = \{a_1, \ldots, a_m\}$ ein endliches Alphabet der Größe m.

- Eine Abbildung $c : A \to \{0,1\}^*$ oder $c : A \to \{0,1\}^n$ heißt Code, falls c injektiv ist.

  ↳ Jedes Codewort hat Länge n!

- Die Menge $c(A) := \{w \in \{0,1\}^* \mid \exists a \in A : c(a) = w\}$ heißt Menge der Codewörter.
- Ein Code $c : A \to \{0,1\}^n$ heißt Code fester Länge.
- Für einen Code $c : A \to \{0,1\}^n$ fester Länge gilt: $n \geq \lceil \log_2 m \rceil$.
  - Ist $n = \lceil \log_2 m \rceil + r$ mit $r > 0$, so können die r zusätzlichen Bits zum Test auf Übertragungsfehler verwendet werden (siehe Kap. 6).

Linkseindeutig, d.h. für jedes Codewort gibt es genau ein $a_i \in A$.

Codes fester Länge

- Die Kodierung eines jeden Zeichens besteht aus n Bits.
  - ASCII (American Standard Code for Information Interchange): 7 Bits (es gibt Erweiterungen mit 8 Bits)
  - EBCDIC: 8 Bits
  - Unicode: 16 Bits
  - Vgl. „Rechnerarchitektur”
- Diese Kodierungen sind recht einfach zu behandeln. Unter Umständen wird für sie aber mehr Speicherplatz gebraucht als unbedingt nötig.

Beispiel: ASCII-Tabelle

erste 3 Bits

letzte 4 Bits	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
0000	nul	dle		0	@	P	`	p
0001	soh	dc1	!	1	A	Q	a	q
0010	sfx	dc2	"	2	B	R	b	r
0011	etx	dc3	#	3	C	S	c	s
0100	eot	dc4	$	4	D	T	d	t
0101	enq	nak	%	5	E	U	e	u
0110	ack	syn	&	6	F	V	f	v
0111	bel	etb	'	7	G	W	g	w
1000	bs	can	(	8	H	X	h	x
1001	ht	em	)	9	I	Y	i	y
1010	lf	sub	*	:	J	Z	j	z
1011	vt	esc	+	;	K	[	k	{
1100	ff	fs	,	<	L	\	l	|
1101	cr	qs	-	=	M	]	m	}
1110	so	rs	.	>	N	^	n	*
1111	si	us	/	?	O	_	o	del

Steuerzeichen

Schriftzeichen

Codierung dieser 10 Zeichen je einmal 7 Bit

carriage return

Häufigkeitsabhängige Codes

- **Ziel**: Reduktion der Länge einer Nachricht durch Wahl verschieden langer Codewörter für die verschiedenen Zeichen eines Alphabets (also kein Code fester Länge!)
- **Idee**:

Häufiges Zeichen	$\rightarrow$	kurzer Code
Seltenes Zeichen	$\rightarrow$	langer Code

- **Voraussetzungen**:
  - Häufigkeitsverteilung ist bekannt $\rightarrow$ statische Kompression
  - Häufigkeitsverteilung ist nicht bekannt $\rightarrow$ dynamische Kompression

1) Streame alle Zeichen, zähle die Häufigkeiten
2) kodieren
3) ~) Verteilung dem „Dekodierer" mitschicken.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Huffman-Code

- Der Huffman-Code ist der bekannteste häufigkeitsabhängige Code.
- Kommt als Teilschritt z.B. in MP3 oder JPEG vor.
- Beispiel:

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Baue binären Baum, indem die beiden kleinsten Häufigkeiten jeweils zu einem neuen Knoten addiert werden.

Markiere nun die linken Kanten mit 0 und die rechten Kanten mit 1, fertig ist der Huffman-Code!

Erzeugte Huffman-Kodierung

Zeichen	a	b	c	d	e	f	g	h	i	j
Häufigkeit [%]	20	25	15	8	7	6	5	5	5	4

Erzeugte Kodierung:

a	b	c	d	e	f	g	h	i	j
00	10	110	1110	0100	0101	0110	0111	11110	11111

Huffman-Code: Dekodierung

Problem: a = 01
b = 011

Erzeugte Kodierung:

a	b	c	d	e	f	g	h	i	j
00	10	110	1110	0100	0101	0110	0111	11110	11111

Bitstrom:

011.....

ist das "a" mit 1 oder ist das "b"?

1. Lesen des Bitstromes bis Symbol erkannt wurde.
2. Erkanntes Symbol ausgeben und weiter mit 1.

1 Schritt

Präfixcodes

Definition

"01" ist Pra"fix von "011"

Sei A ein Alphabet der Größe m.

- $a_1 \dots a_p \in A^*$ heißt Präfix von $b_1 \dots b_l \in A^*$, falls $p \leq l$ und $a_i = b_i \; \forall i, \; 1 \leq i \leq p$.

variabler Länge

- Ein Code $c : A \to \{0,1\}^*$ heißt Präfixcode, falls es kein Paar $i,j \in \{1,\dots,m\}$ gibt, so dass $c(a_i)$ Präfix von $c(a_j)$.
  - Der Huffman-Code ist ein Präfixcode.
  - Bei Präfixcodes können Wörter über $\{0,1\}$ eindeutig dekodiert werden. (Sie entsprechen Binärbäumen mit Codewörtern an den Blättern.)
  - Huffman-Code ist ein bzgl. mittlerer Codelänge optimaler Präfixcode (unter Voraussetzung einer bekannten Häufigkeitsverteilung) - ohne Beweis.

UNI FREIBURG

Präfixcodes

Definition

Sei A ein Alphabet der Größe m.

- $a_1 \dots a_p \in A^*$ heißt Präfix von $b_1 \dots b_l \in A^*$, falls $p \leq l$ und $a_i = b_i \; \forall i, \; 1 \leq i \leq p$.
- Ein Code $c : A \to \{0,1\}^*$ heißt Präfixcode, falls es kein Paar $i,j \in \{1,\dots,m\}$ gibt, so dass $c(a_i)$ Präfix von $c(a_j)$.
  - Der Huffman-Code ist ein Präfixcode.
  - Bei Präfixcodes können Wörter über $\{0,1\}$ eindeutig dekodiert werden. (Sie entsprechen Binärbäumen mit Codewörtern an den Blättern.)
  - Huffman-Code ist ein bzgl. mittlerer Codelänge optimaler Präfixcode (unter Voraussetzung einer bekannten Häufigkeitsverteilung) - ohne Beweis.

SMILE – Präfixcodes

Frage: Welche dieser Codes sind Präfixcodes

a. $c('A') = 01$, $c('B') = 110$, $c('C') = 011$ → Kein!
b. $c('A') = 01$, $c('B') = 110$, $c('C') = 111$ → JA
c. $c('1') = xz$, $c('2') = xy$, $c('3') = yz$ → JA
d. Keiner der Obigen. → Aussage kann nicht stimmen!

Weitere Verfahren

- Es gibt zahlreiche Ansätze zur Datenkompression. (Beispiel: Lempel-Ziv-Welch.)
- In Programmtexten gibt es häufig viele Leerzeichen, gleiche Schlüsselwörter und so weiter.

→ Kodiere Folgen von Leerzeichen bzw. Schlüsselwörter durch kurze Codes.

- Das wird z.B. bei GIF und TIFF genutzt.
- Das soll auch funktionieren, wenn man noch nicht weiß, welche Zeichenketten häufig vorkommen.

Kapitel 2 – Kodierung

1. Kodierung von Zeichen
2. **Kodierung von Zahlen**
3. Anwendung: ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Zahlensysteme

Definition

Ein Zahlensystem ist ein Tripel $S = (b, Z, \delta)$ mit den folgenden Eigenschaften:

- $b \geq 2$ ist eine natürliche Zahl, die Basis des Stellenwertsystems.
- Z ist eine b-elementige Menge von Symbolen, den Ziffern.
- $\delta : Z \to \{0, 1, \ldots, b-1\}$ ist eine Abbildung, die jeder Ziffer umkehrbar eindeutig eine natürliche Zahl zwischen 0 und $b-1$ zuordnet.

Beispiele für Zahlensysteme

- Dualsystem:
  $b = 2 \quad Z = \{0, 1\}$

  $\delta(0) \to 0$
  $\delta(1) \to 1$

- Oktalsystem:
  $b = 8 \quad Z = \{0, 1, 2, 3, 4, 5, 6, 7\}$

- Dezimalsystem:
  $b = 10 \quad Z = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

  $\delta(A) = 10$

  $\delta : Z \to \mathbb{N}$

- Hexadezimalsystem:
  $b = 16 \quad Z = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$

  10 11 12 13 14 15

Festkommazahlen

Definition

Eine Festkommazahl ist eine endliche Folge von Ziffern aus einem Zahlensystem zur Basis b mit Ziffernmenge Z.

- Sie besteht aus $n+1$ Vorkommastellen ($n \geq 0$) und $k \geq 0$ Nachkommastellen.

nicht-negative Zahl

- Der Wert $\langle d \rangle$ einer nicht-negativen Festkommazahl $d = d_n d_{n-1} \ldots d_1 d_0 d_{-1} \ldots d_{-k}$ mit $d_i \in Z$ ist gegeben durch

$$\langle d \rangle = \sum_{i=-k}^{n} b^i \cdot \delta(d_i)$$

Festkommazahlen: Schreibweise

Bsp. $n = 1, k = 2$

$d_1 \; 0 \; 1 \; 1 \; 0_2 \cong$ „$1, 1/2$" $= 1{,}5_{10}$

$d_0 \; d_{-1} \; d_{-2}$

$2^{-2} = 1/4$

$2^{-1} = 1/2$

- Vorkomma- und Nachkommastellen werden zur Verdeutlichung durch ein Komma oder einen Punkt getrennt:
  $d = d_n d_{n-1} \ldots d_1 d_0 . d_{-1} \ldots d_{-k}$
- Um anzudeuten, welches Zahlensystem zu Grunde liegt, wird gelegentlich die Basis als Index an die Ziffernfolge angehängt.

$d_3 \; d_2 \; d_1 \; d_0$

Keine Nachkommastelle

- Beispiel $(n = 3, k = 0)$:

$$
\begin{aligned}
0110_2 &= 6 &&= 2^2 + 2^1 = 4 + 2 = 6 \\
0110_8 &= 72 &&= 8^2 + 8^1 = 64 + 8 = 72 \\
0110_{10} &= 110 \checkmark \\
0110_{16} &= 272 &&= 16^2 + 16 = 256 + 16 = 272
\end{aligned}
$$

Negative Festkommazahlen

(Im Folgenden wird Basis 2 angenommen.)

- Bei der Darstellung negativer Festkommazahlen nimmt die höchstwertigste Stelle d_n eine Sonderrolle ein: $d_n = 1 \rightarrow$ negative Zahl
  - Ist $d_n = 0$, so handelt es sich um eine nichtnegative Zahl.
- Bei der Darstellung negativer Zahlen gibt es folgende Alternativen:

  $d_n = 0 \rightarrow (-1)^0 = 1$

  $d_n = 1 \rightarrow (-1)^1 = -1$

  - Darstellung durch Betrag und Vorzeichen:

    $$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_{BV} := (-1)^{d_n} \sum_{i=-k}^{n-1} d_i \, 2^i$$

    ← Spiegeln „an der 0"
  - Einer-Komplement-Darstellung:

    $$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_1 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n(2^n - 2^{-k})$$
  - Zweier-Komplement-Darstellung:

    $$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_2 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n \, 2^n$$

„Verschiebung des Wertebereichs!"

Betrag und Vorzeichen

Bsp.: $n=3, k=2$

Vz $\rightsquigarrow$ $d_3 d_2 d_1 d_0 . d_{-1} d_{-2}$

$1/2$ $1/4$

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_{BV} := (-1)^{d_n} \sum_{i=-k}^{n-1} d_i \, 2^i$$

Beispiel: $n = 2, k = 0$ → keine Nachkommastellen

7,75 max.

Wert = $2^n - 2^{-k} = 2^3 - 2^{-2} = 8 - 1/4 = 7{,}75$

a	000	001	010	011	100	101	110	111
$[a]_{BV}$	0	1	2	3	0	-1	-2	-3

$\cdot(-1)$

Bsp. mit $n=2, k=0$: $2^n - 2^{-k} = 2^2 - 2^0 = 4 - 1 = 3$

- Der Zahlenbereich ist symmetrisch:
  - Kleinste Zahl: $-(2^n - 2^{-k})$, größte Zahl: $2^n - 2^{-k}$
- Man erhält zu a die inverse Zahl, indem man das erste Bit komplementiert. $= -a$
- Zwei Darstellungen für die Null (000 und 100 im Beispiel).
- „Benachbarte Zahlen" haben gleichen Abstand 2^{-k}.

Einer-Komplement

$[a]_1 + [a']_1 = \underbrace{\sum a_i'' + \sum a_i''}_{= 2^n - 2^{-k}} - a_n \cdot (\dots) - a_n' \cdot (\dots) = 0$

größte darst. Wert

$$[d_n, d_{n-1}, \dots, d_0, d_{-1}, \dots, d_{-k}]_1 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n (2^n - 2^{-k})$$

Beispiel: $n = 2, k = 0$

100 101 111 000 001 010 011

-3 -2 -1 1 2 3

a	000	001	010	011	100	101	110	111
$[a]_1$	0	1	2	3	-3	-2	-1	0

$\cong 010$ komp. aller Bits $101 \cong -2$

- Der Zahlenbereich ist symmetrisch: $-(2^n - 2^{-k}) \dots 2^n - 2^{-k}$
- Zwei Darstellungen für die Null (000 und 111 im Beispiel).
- „Benachbarte Zahlen" haben gleichen Abstand 2^{-k}.
- Man erhält zu a die inverse Zahl, indem man alle Bits komplementiert (siehe Lemma nächste Folie).

Einer-Komplement: Inversion

Lemma

Sei a eine Festkommazahl, a' die Festkommazahl, die aus a durch Komplementieren aller Bits ($0 \to 1, 1 \to 0$) hervorgeht. Dann gilt $[a']_1 = -[a]_1$.

z.z.: $[a]_1 + [a']_1 = 0$

$= [a_1] - [a]_1$

Beweisidee: Addiert man Bits $n-1 \cdots -k$ von a und a', erhält man $111\ldots11$. Das ist aber gerade $(2^n - 2^{-k}) = (a_n + a'_n) \cdot (2^n - 2^{-k})$.

$=1$

$$\begin{array}{ll} (a_{n-1}, \ldots, a_{-k}) & 011011 \\ (a'_{n-1}, \ldots, a'_{-k}) & 100100 \\ \hline & 111111 \end{array}$$

größte darstellb. Zahl / Betrag

mit $< 111111 > = < (a_{n-1}, \ldots, a_{-k}) > + < (a'_{n-1}, \ldots, a'_{-k}) >$

UNI FREIBURG

Zweier-Komplement

100 101 110 111 000 001 010 011

-4 -3 -2 -1 0 1 2 3

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_2 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n \, 2^n$$

Beispiel: $n = 2, k = 0$

a	000	001	010	011	100	101	110	111
$[a]_2$	0	1	2	3	-4	-3	-2	-1

$= 2^2 - 1 = 3$

- Der Zahlenbereich ist asymmetrisch: $-2^n \ldots 2^n - 2^{-k}$
- Die Zahlendarstellung ist eindeutig, auch für die Null.
- „Benachbarte Zahlen" haben gleichen Abstand 2^{-k}.
- Man erhält zu a die inverse Zahl, indem man alle Bits komplementiert und an der niederwertigsten Stelle 1 addiert (siehe Lemma nächste Folie).

Zweier-Komplement: Inversion

$n=5, k=0$ $\quad d_5\, d_4\, d_3\, d_2\, d_1\, d_0$

$17_{10} = 0\ 1\ 0\ 0\ 0\ 1$

$-17_{10} = \underset{2^5}{1}\ 0\ \underset{8}{1}\ \underset{4}{1}\ \underset{2}{1}\ \underset{1}{1}$

$= 15$

$15 - 32 = -17_{10}$

Lemma

Sei a eine Festkommazahl, a' die Festkommazahl, die aus a durch Komplementieren aller Bits ($0 \to 1, 1 \to 0$) hervorgeht. Dann gilt $[a']_2 + 2^{-k} = -[a]_2$.

kleinste Betrag

Beweisidee: Addiert man Bits $n-1 \ldots 0$ von a und a', erhält man $111\ldots11$. Addiert man noch $000\ldots01$ hinzu, so erhält man gerade $2^n = (a_n + a'_n) \cdot 2^n$.

$(a_{n-1}, \ldots, a_{-k})$	011011
$(a'_{n-1}, \ldots, a'_{-k})$	100100
"2^{-k}"	000001
	1000000

$2^n = (2^n - 2^{-k}) + 2^{-k} = 2^n$

mit

$$< 1000000 > = < (a_{n-1}, \ldots, a_{-k}) > + < (a'_{n-1}, \ldots, a'_{-k}) > + 2^{-k}$$

Vorteil von Zweier-Komplement

Addition nach Schulmethode

$$\begin{array}{r} -17 \\ +23 \\ \hline 40 \end{array}$$

falsch

- Wir werden später Schaltungen betrachten, die zwei Zahlen als Eingaben nehmen und ihre Summe oder Differenz an den Ausgängen bereit stellen (Addierer, Subtrahierer).
- Es stellt sich heraus, dass diese Schaltungen besonders einfach sind, wenn Negativzahlen im Zweier-Komplement dargestellt werden.
- Daher wird in der Praxis oft die Zweier-Komplement-Darstellung verwendet.

Festkommazahlen - Übersicht

Betrag mit Vorzeichen

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_{BV} := (-1)^{d_n} \sum_{i=-k}^{n-1} d_i \, 2^i$$

Einerkomplement

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_1 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n(2^n - 2^{-k})$$

Zweierkomplement

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_2 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n \, 2^n$$

$n = 2,\ k = 0$

a	000	001	010	011	100	101	110	111
$[a]_{BV}$	0	1	2	3	0	-1	-2	-3
$[a]_1$	0	1	2	3	-3	-2	-1	0
$[a]_2$	0	1	2	3	-4	-3	-2	-1

	symmetrisch	symmetrisch	asymmetrisch
kleinste Zahl	$-(2^n - 2^{-k})$	$-(2^n - 2^{-k})$	-2^n
größte Zahl	$2^n - 2^{-k}$	$2^n - 2^{-k}$	$2^n - 2^{-k}$
Inverses durch	kompl. 1. Bit	kompl. alle Bits	kompl. alle Bits, add. 1
Null	2 Darstellungen	2 Darstellungen	1 Darstellung
Abstand	2^{-k}	2^{-k}	2^{-k}

Festkommazahlen - Übersicht

Betrag mit Vorzeichen

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_{BV} := (-1)^{d_n} \sum_{i=-k}^{n-1} d_i \, 2^i$$

Einerkomplement

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots, d_{-k}]_1 := \sum_{i=-k}^{n-1} d_i \, 2^i - d_n(2^n - 2^{-k})$$

Zweierkomplement

$$[d_n, d_{n-1}, \ldots, d_0, d_{-1}, \ldots$$
$$:= \sum_{i=-k}^{n-1} d_i \, 2^i - d_n$$

$n = 2,\ k = 0$

a	000	001	010	011	100	101	110	111
$[a]_{BV}$	0	1	2	3	0	-1	-2	-3
$[a]_1$	0	1	2	3	-3	-2	-1	0
$[a]_2$	0	1	2	3	-4	-3	-2	-1

	symmetrisch	symmetrisch	asymmetrisch
kleinste Zahl	$-(2^n - 2^{-k})$	$-(2^n - 2^{-k})$	-2^n
größte Zahl	$2^n - 2^{-k}$	$2^n - 2^{-k}$	$2^n - 2^{-k}$
Inverses durch	kompl. 1. Bit	kompl. alle Bits	kompl. alle Bits, add. 1
Null	2 Darstellungen	2 Darstellungen	1 Darstellung
Abstand	2^{-k}	2^{-k}	2^{-k}

SMILE – Festkommazahlen

b) $-7 - (-7) = -7 + 7 = 0$

-7

7

Frage: Welche der Aussagen sind wahr für die Zahl $[1001]_2$?

$d_3\, d_2\, d_1\, d_0$

$n=3$
$k=0$

a. $[1001]_2 = [0111]_{BV}$ Nein
b. $[1001]_2 - [1001]_2 = [10010]_2$ -14 Nein
c. $[1001]_2$ ist das (additive) Inverse zu $[0111]_2$ ✓
d. $[1001]_2 = [1000]_1$ ✓

-7

$1001 \xrightarrow{\text{INV.}} 0110 \xrightarrow{+1} 0111$ ✓

$(-2^n + 2^{-k}) + 0 = -7$

Probleme von Festkommazahlen

- Betrachte die Menge aller Zahlen, die eine Zweier-Komplement-Darstellung mit n Vor- und k Nachkommastellen haben.
  - Keine ganz großen bzw. kleinen Zahlen darstellbar!
    - Zahlen mit größtem Absolutbetrag: -2^n und $2^n - 2^{-k}$
    - Zahlen mit kleinstem Absolutbetrag: -2^{-k} und 2^{-k}
- Operationen sind nicht abgeschlossen!
  - $2^{n-1} + 2^{n-1}$ ist nicht darstellbar, obwohl die Operanden darstellbar sind.
- Assoziativ- und Distributivgesetz gelten nicht, da bei ihrer Anwendung evtl. der darstellbare Zahlenbereich verlassen wird!
  - Beispiel: $(\underbrace{2^{n-1} + 2^{n-1}}_{\text{überlauf} \to 0}) - 2^{n-1} \neq \underbrace{2^{n-1}}_{2^{n-1}} + (\underbrace{2^{n-1} - 2^{n-1}}_{=0})$

Gleitkomma-Zahlen

Vor + Nachkommastellen

„Position des Komma einzustellen"

- Die verfügbaren Bits werden in Vorzeichen S, Exponent E und Mantisse M unterteilt.
- $a = (-1)^S \cdot M \cdot 2^E$.

Gleitkomma:

Festkomma:

- Einfache Genauigkeit (insg. 32 Bit)

31	30 29 28 27 26 25 24 23	22 21 20 19 … 3 2 1 0
S	Exponent E	Mantisse M

- Doppelte Genauigkeit (insg. 64 Bit)

63	62 61 60 59 … 54 53 52	51 50 49 48 … 3 2 1 0
S	Exponent E	Mantisse M

  - Implementierungsdetails: siehe z.B. IEEE754-Standard

UNI FREIBURG

Kapitel 2 – Kodierung

1. Kodierung von Zeichen
2. Kodierung von Zahlen
3. **Anwendung: ReTI**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Realisierung von ReTI

Unterschiede abstrakter/realer ReTI

Adressbereich / raum
32 Bit

$2^{32} \cdot 4$ Byte
$= 16$ GB

- Bei realer Maschine nur ein Speicher M für Daten und Befehle.
  - M ist endlich (Größe 2^{32}). Für $i \in \{0, \ldots, 2^{32} - 1\}$ ist $M(i)$ Inhalt der i-ten Speicherzelle.
  - Speicherzellen können Elemente aus $\mathbb{B}^{32}$ aufnehmen. 32 bit breit
- CPU-Register $PC, ACC, IN1$ und $IN2$ können nur Elemente $w \in \mathbb{B}^{32}$ aufnehmen. w heißt Wort.
  - Ein Wort kann als Binärzahl (z.B. Adresse im M), Zweierkomplementzahl oder Bitstring interpretiert werden.
- Befehle sind ebenfalls Wörter aus $\mathbb{B}^{32}$.

Notation

- $b^j = \underbrace{(b, \ldots, b)}_{j \text{ mal}}$ für $b \in \{0, 1\}$

- $\langle A \rangle := B$

  (A Register oder Speicherzelle, $B \in \{0, ..., 2^{32} - 1\}$)
  bedeute $A := bin_{32}(B)$
  - Beispiel: $\langle PC \rangle := \langle PC \rangle + 1$

- $[A] := B$

  (A Register oder Speicherzelle, $B \in \{-2^{31}, ..., 2^{31} - 1\}$)
  bedeute $A := twoc_{32}(B)$
  B wird als Zweierkomplement-Zahl interpretiert.

Befehlsformate

ADDI i:

„ACC = ACC + i"

- Zur Erinnerung: Der Befehlssatz von ReTI besteht aus Load-/Store-, Compute-, Indexregister- und Sprungbefehlen.

- Sie werden als Wörter aus $\mathbb{B}^{32}$ kodiert. Etwaige Parameter sind in der Kodierung enthalten.
  - Notation: Sei $I = i_{31}, \ldots, i_0 \in \mathbb{B}^{32}$.
    $I[y,x] := i_y, i_{y-1}, \ldots, i_x$ für $0 \leq x \leq y \leq 31$.

- Allgemeines Instruktionsformat:

I:

31 30	29 … 24	23 … 0
Typ	Spezifikation	Parameter i

$I[31:30] \cong$ Typ des Befehls!

UNI FREIBURG

Typ einer Instruktion

I[31, 30]	Typ
0 0	Compute
0 1	Load
1 0	Store, Move
1 1	Jump

31 30	29 … 24	23 … 0
Typ	Spezifikation	Parameter i

Load-Befehle: Kodierungsprinzip

31 30	29 28	27 26	25 24	23 … 0
0 1	M	*	D	i

nicht genutzt

- M: Modus
- D: Vorerst irrelevant

↳ Destination

Load-Befehle: Kodierung

vorzeichenlose Binärdarstellg

2er-Kompl.

Typ	Modus	Befehl	Wirkung	
0 1	0 0	LOAD i	$ACC := M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$
0 1	0 1	LOADIN1 i	$ACC := M(\langle IN1 \rangle + [i])$	$\langle PC \rangle := \langle PC \rangle + 1$
0 1	1 0	LOADIN2 i	$ACC := M(\langle IN2 \rangle + [i])$	$\langle PC \rangle := \langle PC \rangle + 1$
0 1	1 1	LOADI i	$ACC := 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$

32 Bit

i nur 24 Bit

⇓

d.h. wir füllen mit 0 auf

Durchführung von Rechnungen $\langle x \rangle + [y]$ später.

$0^8 i$

$\underbrace{00000000 i_{23} \ldots i_0}_{32\text{ Bit}}$

Store-, Move-Befehle: Prinzip

31 30	29 28	27 26	25 24	23 … 0
1 0	M	S	D	i

- M: Modus
- S: Source
- D: Destination

Kodierung S, D

S, D	Register
0 0	PC
0 1	IN1
1 0	IN2
1 1	ACC

Store-, Move-Befehle: Kodierung

Typ	Modus	Befehl	Wirkung	
1 0	0 0	STORE i	$M(\langle i \rangle) := ACC$	$\langle PC \rangle := \langle PC \rangle + 1$
1 0	0 1	STOREIN1 i	$M(\langle IN1 \rangle + [i]) := ACC$	$\langle PC \rangle := \langle PC \rangle + 1$
1 0	1 0	STOREIN2 i	$M(\langle IN2 \rangle + [i]) := ACC$	$\langle PC \rangle := \langle PC \rangle + 1$
1 0	1 1	MOVE S D	$D := S$	$\langle PC \rangle := \langle PC \rangle + 1$

außer bei $D = 00$ (PC)

Compute-Befehle: Prinzip

31 30	29	28 27 26	25 24	23 … 0
0 0	MI	F	D	i

- MI: „compute **m**emory"/„compute **i**mmediate"
- F: Funktionsfeld
- D: Vorerst irrelevant
  Destination

Compute-Befehle: Kodierung

EXOR
„Exklusiv-ODer"

Typ	MI	F	Befehl	Wirkung	
0 0	0	0 1 0	SUBI i	$[ACC] := [ACC] - [i]$	$\langle PC \rangle := \langle PC \rangle + 1$
		0 1 1	ADDI i	$[ACC] := [ACC] + [i]$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 0	OPLUSI i	$ACC := ACC \oplus 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 1	ORI i	$ACC := ACC \vee 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 1 0	ANDI i	$ACC := ACC \wedge 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$
0 0	1	0 1 0	SUB i	$[ACC] := [ACC] - [M(\langle i \rangle)]$	$\langle PC \rangle := \langle PC \rangle + 1$
		0 1 1	ADD i	$[ACC] := [ACC] + [M(\langle i \rangle)]$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 0	OPLUS i	$ACC := ACC \oplus M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 1	OR i	$ACC := ACC \vee M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 1 0	AND i	$ACC := ACC \wedge M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$

Bitstring-Operationen am Beispiel von OPLUS

a	b	EXOR(a,b)
0	0	0
0	1	1
1	0	1
1	1	0

- $ACC := ACC \oplus 0^8 i_{23} \ldots i_0$

  $\cong (ACC_{31} \oplus 0, \ldots, ACC_{24} \oplus 0, ACC_{23} \oplus i_{23}, \ldots, ACC_0 \oplus i_0)$

Sprungbefehle: Prinzip

nicht benutzt

31 30	29 28 27	26 25 24	23 … 0
1 1	C	*	i

- C: Condition

gilt „ACC c 0" dann Sprung!

C	Bedingung c
0 0 0	nie
0 0 1	>
0 1 0	=
0 1 1	≥
1 0 0	<
1 0 1	≠
1 1 0	≤
1 1 1	immer

NOP → No operation, nur PC = PC+1

unbedingter Sprung

Bedingungskodierung nach Schema

29 28 27

C	Bedingung c
0 0 0	nie
0 0 1	$>$
0 1 0	$=$
0 1 1	$\geq$
1 0 0	$<$
1 0 1	$\neq$
1 1 0	$\leq$
1 1 1	immer

nur $I[29] = 1 \Leftrightarrow <$ wird abgefragt
nur $I[28] = 1 \Leftrightarrow =$ wird abgefragt
nur $I[27] = 1 \Leftrightarrow >$ wird abgefragt

Andere Abfragen durch Kombinationen,
z.B. $C = 101 : <$ oder $>$, also $\neq$.

Sprungbefehle: Kodierung

Typ	Befehl	Wirkung
1 1	JUMP$_c$ i	$\langle PC \rangle := \begin{cases} \langle PC \rangle + [i], & \text{falls } [ACC]\ c\ 0 \\ \langle PC \rangle + 1, & \text{sonst} \end{cases}$

„immer"

- Unbedingte Sprünge werden durch $C = 111$ ausgedrückt.
- Bei $C = 000$: Keine Wirkung des Befehls außer Inkrementieren des Befehlszählers
  $\Rightarrow$ NOP - Befehl (No Operation)

  (In Kap. 8 werden wir kurz auf die Notwendigkeit von NOP - Befehlen bei Piplining eingehen.)

Zusätzliche Befehle

- Zusätzliche Befehle sind durchaus sinnvoll und bei anderen Architekturen evtl. schon als Grundbefehl vorhanden.
- Nicht vorhandene Befehle müssen hier durch Befehlsfolgen “simuliert” werden.
- Beispiel: Multiplikation, siehe Kapitel 1.2..

Addition und Sign Extension

- Probleme bei Additionen:

  32Bit 24 Bit

  1. Addition verschieden langer Zahlen (z.B. $[ACC] + [i]$).
  2. Addition von Binärdarstellungen und Zweierkomplementzahlen (z.B. $M(\langle IN1 \rangle + [i]) := ACC$).

  Bin. 2er-kompl.

- Zu 1: Lösung durch Sign Extension
  - Sei $y \in \mathbb{B}^{24}$. $sext(y) := y_{23}^{8} y$ heißt sign extension von y.
  - Es gilt: $[y] = [sext(y)]$. (Beweis: Übung)
  - Dann wird $[ACC] + [i]$ zurückgeführt auf $[ACC] + [sext(i)]$.

    32Bit 32 Bit

- Zu 2: Siehe nächste Folie.

Addition von Binär- und Zweierkomplementzahlen

Binärzahl

carry out / Übertrag

Summe

Lemma

Sei $x \in \mathbb{B}^{32}, y \in \mathbb{B}^{24}, 0 \leq \langle x \rangle + [y] < 2^{32}$ und sei $\langle x \rangle + \langle sext(y) \rangle = \langle c, s \rangle$ mit $c \in \mathbb{B}, s \in \mathbb{B}^{32}$.
Dann gilt: $\langle x \rangle + [y] = \langle s \rangle$

- Bedeutung: Kommt es beim Addieren nicht zum Überlauf ($0 \leq \langle x \rangle + [y] < 2^{32}$), so kann man x und y als Binärzahlen interpretieren, addieren und Übertrag ignorieren!
- Zunächst ohne Beweis.
- Wir können somit Parameter i bei den Befehlen ohne Fallunterscheidung nach i postiv / negativ verwenden!

UNI FREIBURG

Zusammenfassung

- Kodierungen von Zeichen: Codes fester Länge (z.B. ASCII) sind einfacher aber weniger effizient als Codes variabler Länge (z.B. Huffman).
- Zweier-Komplement-Kodierung von Festkomma-Zahlen erlaubt in Verbindung mit Sign Extension effiziente Umsetzung arithmetischer Operationen in Hardware eines Rechners (tatsächliche Implementierung siehe Kapitel 3.5).
- Der Befehlssatz von ReTI ist auf der nächsten Folie zusammengefasst.

Load-Befehle		$I[25:24] = D$	
$I[31:28]$	Befehl	Wirkung	
0100	LOAD D i	$D := M(\langle i \rangle)$	
0101	LOADIN1 D i	$D := M(\langle IN1 \rangle + [i])$	$\langle PC \rangle := \langle PC \rangle + 1$ falls $D \neq PC$
0110	LOADIN2 D i	$D := M(\langle IN2 \rangle + [i])$	
0111	LOADI D i	$D := 0^8 i$	

Store-Befehle		MOVE: $I[27:24] = SD$	
$I[31:28]$	Befehl	Wirkung	
1000	STORE i	$M(\langle i \rangle) := ACC$	
1001	STOREIN1 i	$M(\langle IN1 \rangle + [i]) := ACC$	$\langle PC \rangle := \langle PC \rangle + 1$
1010	STOREIN2 i	$M(\langle IN2 \rangle + [i]) := ACC$	
1011	MOVE S D	$D := S$	$\langle PC \rangle := \langle PC \rangle + 1$ falls $D \neq PC$

Compute-Befehle		$I[25:24] = D$	
$I[31:26]$	Befehl	Wirkung	
000010	SUBI D i	$[D] := [D] - [i]$	
000011	ADDI D i	$[D] := [D] + [i]$	
000100	OPLUSI D i	$D := D \oplus 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$ falls $D \neq PC$
000101	ORI D i	$D := D \vee 0^8 i$	
000110	ANDI D i	$D := D \wedge 0^8 i$	
001010	SUB D i	$[D] := [D] - [M(\langle i \rangle)]$	
001011	ADD D i	$[D] := [D] + [M(\langle i \rangle)]$	
001100	OPLUS D i	$D := D \oplus M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$ falls $D \neq PC$
001101	OR D i	$D := D \vee M(\langle i \rangle)$	
001110	AND D i	$D := D \wedge M(\langle i \rangle)$	

Jump-Befehle			
$I[31:27]$	Befehl	Wirkung	
11000	NOP	$\langle PC \rangle := \langle PC \rangle + 1$	
11001	JUMP$_{>}$ i	$\langle PC \rangle := \begin{cases} \langle PC \rangle + [i], & \text{falls } [ACC]\ c\ 0 \\ \langle PC \rangle + 1, & \text{sonst} \end{cases}$	
11010	JUMP$_{=}$ i		
11010	JUMP$_{\geq}$ i		
11011	JUMP$_{<}$ i		
11100	JUMP$_{\neq}$ i		
11110	JUMP$_{\leq}$ i		
11111	JUMP i	$\langle PC \rangle := \langle PC \rangle + [i]$	

Kodierung S,D

S, D	Register
0 0	PC
0 1	$IN1$
1 0	$IN2$
1 1	ACC

SMILE – Programme

Loadi ACC=1 NOP

Ein ReTI-Programm P sieht folgendermaßen aus: $P =$
01111100000000000000000000000001110000000000000000000000000000
00001111000000000000000000000001100000000000000000000000000011

Frage: Welche der Aussagen über das Programm P sind wahr?

ADDI ACC=ACC+1 ⇝ ACC=2

Weil um 4 Store

a. Der *PC* ist nach Ausführung des Programms um 3 erhöht.
b. Das Programm besteht aus LOADI, NOP, ADDI, STORE.
c. Nach Ausführung des Programms steht in Speicherzelle 3 eine 2.
d. Das Programm verwendet alle möglichen Register der ReTI-Maschine. IN1, IN2 nicht
e. ~~Das Programm enthält einen Befehl, den man immer weglassen kann, da er nie Auswirkungen hat.~~

Kapitel 3 – Kombinatorische Logik

1. **Kombinatorische Schaltkreise**
2. Normalformen, zweistufige Synthese
3. Berechnung eines Minimalpolynoms
4. Arithmetische Schaltungen
5. Anwendung: ALU von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

Kombinatorische Schaltkreise

Definition

Kombinatorische Logik ist ein Modell von Hardware, die eine boolesche Funktion $f : \mathbb{B}^n \to \mathbb{B}^m (n, m \in \mathbb{N})$ implementiert.

- Ein kombinatorischer Schaltkreis (Schaltnetz) hat n Eingänge und m Ausgänge. Legt man an den Eingängen den Vektor $i \in \mathbb{B}^n$ an, berechnet der Schaltkreis den Vektor $f(i) \in \mathbb{B}^m$ und stellt ihn an den Ausgängen bereit.

- Es gibt weitere Arten von Hardware:
  - Sequentielle Logik mit speichernden Elementen (später).
  - Analog- und Mixed-Signal-Blöcke (nicht in TI).

Kombinatorische Logiksynthese

- Kombinatorische Logiksynthese ist das Problem, zu einer gegebenen Booleschen Funktion einen möglichst effizienten kombinatorischen Schaltkreis, d. h. einen mit möglichst geringen Kosten, zu finden.

- Die Definition von Kosten hängen von der verwendeten Technologie ab und können sich auf die Größe, Verzögerung, Energieverbrauch des Schaltkreises beziehen und eventuell weitere Parameter (Zuverlässigkeit, Testbarkeit, ...) berücksichtigen.

Technologien

- Wir konzentrieren uns hier auf zwei Arten von Technologien:

  1. Programmierbare Logikfelder (Programmable Logic Arrays, PLAs).
     - Implementieren sogenannter zweistufigen Realisierungen.
  2. Mehrstufige Realisierungen mit allgemeinen Bibliothekszellen (Logik-Gattern).

Logikgatter

Gatter: AND, OR, XOR

- Gatter sind kleine kombinatorische Blöcke, in der Regel mit bis zu 4 Eingängen und einem Ausgang.
- Gatter werden mit Transistoren realisiert.
- Gatter können zu größeren Schaltungen verbunden werden.
- Die Menge der verfügbaren Gattern ergibt eine Standardzellen-Bibliothek.

Einige wichtige Gatter

i_1	i_2	AND_2
0	0	0
0	1	0
1	0	0
1	1	1

i_1	i_2	OR_2
0	0	0
0	1	1
1	0	1
1	1	1

i_1	NOT_2
0	1
1	0

i_1	i_2	$NAND_2$
0	0	1
0	1	1
1	0	1
1	1	0

i_1	i_2	NOR_2
0	0	1
0	1	0
1	0	0
1	1	0

i_1	i_2	XOR_2
0	0	0
0	1	1
1	0	1
1	1	0

UNI FREIBURG 6

Logikgatter - verschiedene Notationen

Es gibt verschiedene Notationen für Logikgatter.

Wir werden in dieser Vorlesung die ANSI-Notation verwenden.

Transistoren

MOSFET

- Einen Transistor kann man vereinfacht als spannungsgesteuerten Schalter sehen:
  - Leitung *g* (gate) regelt Leitfähigkeit zwischen Quelle und Senke.

p-Kanal Transistor

n-Kanal Transistor

- Leitet, wenn an *g* eine 0 anliegt.
- Sperrt, wenn an *g* eine 1 anliegt.

- Leitet, wenn an *g* eine 1 anliegt.
- Sperrt, wenn an *g* eine 0 anliegt.

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

Eingang	Ausgang
0	1
1	0

Realisierung von Gattern in CMOS-Technologie

- Complementary Metal Oxide Semiconductor.
- Es werden p- und n-Kanal-Transistoren verwendet.
- Beispiel: CMOS-Inverter.

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

-16

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 1 am Gate

- Leitender Pfad zwischen Ausgang und Masse (logische 0).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

CMOS-Inverter mit 0 am Gate

- Leitender Pfad zwischen Ausgang und Spannungsversorgung (logische 1).

SMILE - CMOS

Welche Funktion wird mit Hilfe der p-Kanal und n-Kanal Transistoren realisiert?

Was muss passieren, damit Ausgang = 0 gilt?

$a = 1$

$b = 1$

Sonst?

a b	$\overline{ab}$	$\overline{a+b}$
0 0	1	1
0 1	1	0
1 0	1	0
1 1	0	0

CMOS-NAND-Gatter

- Ausgang ist 0
  $\Leftrightarrow$ Es existiert ein leitender Pfad von 0 zum Ausgang
  $\Leftrightarrow$ beide n-Kanal-Transistoren leiten
  $\Leftrightarrow a = b = 1, a \wedge b = 1$
  $\Leftrightarrow NAND(a,b) = 0$

- Ausgang ist 1
  $\Leftrightarrow$ Es existiert ein leitender Pfad von 1 zum Ausgang
  $\Leftrightarrow$ einer der p-Kanal-Transistoren leitet
  $\Leftrightarrow a = 0$ oder $b = 0, \neg a \vee \neg b = 1$
  $\Leftrightarrow NAND(a,b) = 1$

Weitere CMOS-Gatter

- Es gibt keine „direkte” Implementierung von AND- und OR-Gattern. Sie werden aus NAND-/NOR-Gattern plus Invertern zusammengesetzt.
- Zu jedem p-Kanal Transistor gibt es stets einen komplementären n-Kanal-Transistor, der genau dann sperrt, wenn der erste Transistor leitet und umgekehrt. Dadurch gibt es niemals einen leitenden Pfad von der Stromversorgung zur Masse. Dies reduziert Leistungsverluste.

Schaltkreise

- Idee:
  „gerichteter Graph mit einigen zusätzlichen Eigenschaften”

Gerichtete Graphen (Wiederholung)

- $G = (V, E)$ ist ein gerichteter Graph, genau dann, wenn
  - V endliche nichtleere Menge („Knoten”)
  - E endliche Menge („Kanten”)
  - Auf E sind Abbildungen $Q, Z : E \to V$ definiert ($Q(e)$ heißt Quelle, $Z(e)$ Ziel einer Kante e)

$(v_2, v_3) \in E$

$(v_2, v_4) \notin E$

- Die Abbildung $indeg : V \to \mathbb{N}, indeg(v) = |\{e \mid Z(e) = v\}|$ gibt den Eingangsgrad eines Knotens $v \in V$ an.

$indeg(v_2) = 3$

- Die Abbildung $outdeg : V \to \mathbb{N}, outdeg(v) = |\{e \mid Q(e) = v\}|$ gibt den Ausgangsgrad eines Knotens $v \in V$ an.

$outdeg(v_2) = 2$

- Ein Pfad (der Länge k) in G ist eine Folge von k Kanten $e_1, e_2, \ldots, e_k (k \geq 0)$ mit $Z(e_i) = Q(e_{i+1})\ \forall i$ mit $k - 1 \geq i \geq 1$. $Q(e_1)$ heißt Quelle, $Z(e_k)$ Ziel des Pfades.

Zyklus: $v_2 v_2$
$v_2 v_3 v_4 v_2$

- Ein Zyklus in G ist ein Pfad der Länge ≥ 1 in G, bei dem Ziel und Quelle identisch sind.
- G heißt azyklisch, falls kein Zyklus in G existiert.
- Die Graph-Tiefe eines azyklischen Graphen ist definiert als die Länge des längsten Pfades in G.

Modellierung durch Schaltkreise (1/2)

- Eine Zellenbibliothek $BIB \subset \bigcup_{n \in \mathbb{N}} \mathbb{B}_n$ enthält Basisoperatoren, die den Grundgattern entsprechen.
- Ein 5-Tupel $SK = (\vec{X}_n, G, typ, IN, \vec{Y}_m)$ heißt Schaltkreis mit n Eingängen und m Ausgängen über der Zellenbibliothek BIB genau dann, wenn
  - $\vec{X}_n = (x_1, \ldots, x_n)$ ist eine endliche Folge von Eingängen.
  - $G = (V, E)$ ist ein azyklischer, gerichteter Graph mit $\{0,1\} \cup \{x_1, \ldots, x_n\} \subseteq V$.
  - Die Menge $I = V \setminus (\{0,1\} \cup \{x_1, \ldots, x_n\})$ heißt Menge der Gatter. Die Abbildung $typ : I \to BIB$ ordnet jedem Gatter $v \in I$ einen Zellentyp $typ(v) \in BIB$ zu.
  - ...

Modellierung durch Schaltkreise (2/2)

E^* = beliebig (endlich) viele Elemente von E hintereinander

E^ω = unendlich viele Elemente

- ...
- Für jedes Gatter $v \in I$ mit $typ(v) \in \mathbb{B}_k$ gilt $indeg(v) = k$.
- $indeg(v) = 0$ für $v \in \{0, 1\} \cup \{x_1, \ldots, x_n\}$.
- Die Abbildung $IN : I \to E^*$ legt für jedes Gatter $v \in I$ eine Reihenfolge der eingehenden Kanten fest, d.h. falls $indeg(v) = k$, dann ist $IN(v) = (e_1, \ldots, e_k)$ mit $Z(e_i) = v \; \forall 1 \leq i \leq k$.
- Die Folge $\vec{Y}_m = (y_1, \ldots, y_m)$ zeichnet Knoten $y_i \in V$ als Ausgänge aus.

Modellierung durch Schaltkreise (2/2)

- ...
- Für jedes Gatter $v \in I$ mit $typ(v) \in \mathbb{B}_k$ gilt $indeg(v) = k$.
- $indeg(v) = 0$ für $v \in \{0, 1\} \cup \{x_1, \ldots, x_n\}$.
- Die Abbildung $IN : I \to E^*$ legt für jedes Gatter $v \in I$ eine Reihenfolge der eingehenden Kanten fest, d.h. falls $indeg(v) = k$, dann ist $IN(v) = (e_1, \ldots, e_k)$ mit $Z(e_i) = v \; \forall 1 \leq i \leq k$.
- Die Folge $\vec{Y}_m = (y_1, \ldots, y_m)$ zeichnet Knoten $y_i \in V$ als Ausgänge aus.

SMILE - Beispiel für einen mehrstufigen komb. Schaltkreis ($f \in \mathbb{B}_{8,2}$)

Welche Werte nehmen x und y gegeben der derzeitigen Eingabe an?

SMILE - Beispiel für einen mehrstufigen komb. Schaltkreis ($f \in \mathbb{B}_{8,2}$)

Formale Semantikdefinition für Schaltkreise (1/2)

- Sei $SK = (\vec{X}_n, G, typ, IN, \vec{Y}_m)$ ein Schaltkreis über einer Zellenbibliothek *BIB*.
- Sei eine Eingangsbelegung $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{B}^n$ gegeben.
- Eine Belegung $\Phi_{SK,\alpha} : V \to \mathbb{B}$ für alle Knoten $v \in V$ ist dann gegeben durch die folgenden Definitionen:
  - $\Phi_{SK,\alpha}(x_i) = \alpha_i \ \forall 1 \leq i \leq n$.
  - $\Phi_{SK,\alpha}(0) = 0$, $\Phi_{SK,\alpha}(1) = 1$.
  - falls $v \in I$ mit $typ(v) = g \in \mathbb{B}_k$, $IN(v) = (e_1, \ldots, e_k)$, dann ist $\Phi_{SK,\alpha}(v) = g(\Phi_{SK,\alpha}(Q(e_1)), \ldots, \Phi_{SK,\alpha}(Q(e_k)))$.
- Warum ist das wohldefiniert?
- Weil G azyklisch!

wende Gatterfunktion auf die Werte der Eingänge an!

42

Formale Semantikdefinition für Schaltkreise (2/2)

- $(\Phi_{SK,\alpha}(y_1), \ldots, \Phi_{SK,\alpha}(y_m))$ ist dann die unter Eingangsbelegung $\alpha = (\alpha_1, \ldots, \alpha_n)$ berechnete Ausgangsbelegung des Schaltkreises SK.
- Die Berechnung von $\Phi_{SK,\alpha}$ bei Eingangsbelegung α heißt auch Simulation von SK für Belegung α.

- Die an einem Knoten v berechnete Boolesche Funktion $\Psi(v) : \mathbb{B}^n \to \mathbb{B}$ ist definiert durch

$$\Psi(v)(\alpha) := \Phi_{SK,\alpha}(v)$$

  für ein beliebiges $\alpha \in \mathbb{B}^n$.
- Die durch den Schaltkreis berechnete Funktion ist

$$f_{SK} := (\Psi(y_1), \ldots, \Psi(y_m)).$$

Standardzellen-Bibliothek

- Eine Standardzellen-Bibliothek enthält eine Menge von Gattern und kleinen kombinatorischen Schaltungen (Standardzellen).
  - Z. B. einen 8-Bit-Addierer
- Für jedes Element der Bibliothek werden Parameter wie Fläche auf dem Chip, Schaltgeschwindigkeit, Leistungsaufnahme des Gatters bzw. der Standardzelle abgespeichert.
- Es sind oft z. B. mehrere Inverter unterschiedlicher Größe und Geschwindigkeit vorhanden.

Kombinatorische Logiksynthese

- Allgemeine kombinatorische Logiksynthese optimiert mehrere Parameter gleichzeitig.
- Exakte Verfahren existieren, stoßen aber schon für kleinste Schaltkreise an ihre Grenzen.
- In der Praxis werden Heuristiken eingesetzt, die auf Ausschnitten eines großen Schaltkreises lokale Optimierungen durchführen.
- Hier beschränken wir uns auf eine wichtige Unterklasse von kombinatorischen Schaltkreisen:
  Die zweistufige Logik. ← optimale Schaltungen eines bestimmten Strukturs
- Allgemeinere kombinatorische Schaltkreise betrachten wir später bei der Einführung arithmetischer Schaltkreise.

Kapitel 3 – Kombinatorische Logik

1. Kombinatorische Schaltkreise
2. **Normalformen, zweistufige Synthese**
3. Berechnung eines Minimalpolynoms
4. Arithmetische Schaltungen
5. Anwendung: ALU von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Kombinatorische Schaltkreise

$f(x) = 3x^2 + 4x + 2$ reell

$f(x,y,z) = \underbrace{x'y}_{\text{Monom}} + xy'$

- **Ziel:**
  Wir werden zeigen, dass sich jede boolesche Funktion als ein Polynom, also eine Disjunktion (ODER-Verknüpfung) von Monomen, die ihrerseits Konjunktionen (UND-Verknüpfungen) von Eingangsvariablen und negierten Eingangsvariablen sind, darstellen lässt.

- Wir werden für solche Darstellungen Kostenkriterien aufstellen und diese optimieren.

- Monome und Polynome sind spezielle boolesche Ausdrücke (s. auch Kap. 7)

Beispielfunktion

- 3 Eingangsvariablen x_1, x_2, x_3
- Wird im Folgenden zur Illustration verwendet.

x_1	x_2	x_3	f_1
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Literale

Definition

Als Literal einer booleschen Funktion $f \in \mathbb{B}_n$ wird der Ausdruck x_i oder x_i' bezeichnet, wobei $x_i, i \in 1, \ldots, n$, eine Eingangsvariable von f.

- x_i (auch x_i^1 geschrieben) wird positives Literal,
  x_i' (auch x_i^0 geschrieben) wird negatives Literal genannt.

- Literale werden zur kompakten Beschreibung von booleschen Funktionen verwendet. So bezeichnet das Literal x_i die boolesche Funktion $g \in \mathbb{B}_n$ mit $g(\alpha_1, \ldots, \alpha_n) = 1$ genau dann, wenn $\alpha_i = 1$.
  Analog gilt: x_i' bezeichnet die boolesche Funktion $h \in \mathbb{B}_n$ mit $h(\alpha_1, \ldots, \alpha_n) = 1$ genau dann, wenn $\alpha_i = 0$.
  Wir schreiben vereinfachend auch $g = x_i$ bzw. $h = x_i'$.

Monome

Definition

„leeres" Monom

„Verundung"

- Ein Monom ist eine Konjunktion von Literalen, in der kein Literal mehr als einmal vorkommt und zu keiner Variable sowohl das positive als auch das negative Literal vorkommt. Außerdem ist „1" ein Monom.
  - $x_1 x_2 x_3'$ und $x_1' x_3$ sind Monome, $x_2 x_3 x_3'$ ist kein Monom.
- Ein Monom heißt vollständig oder Minterm, wenn jede Variable entweder als positives oder als negatives Literal vorkommt.
  - Wenn drei Variablen x_1, x_2, x_3 betrachtet werden, ist $x_1 x_2 x_3'$ ein Minterm, $x_1' x_3$ ist kein Minterm.
- Für eine Eingabebelegung $\alpha \in \mathbb{B}^n$ heißt

$m(010) = \bar{x}_1 x_2 \bar{x}_3$

$$m(\alpha) = \bigwedge_{i=1}^{n} x_i^{\alpha_i} \quad \text{(Notation: } x_i^1 := x_i, x_i^0 := x_i'\text{)}$$

der zu α gehörende Minterm.

UNI FREIBURG 5

Monome als Beschreibung boolescher Funktionen

- Beispiel: Das Monom $m = x_i x_j'$ bezeichnet die boolesche Funktion $f \in \mathbb{B}_n$ mit $f(\alpha_1, \ldots, \alpha_n) = 1$ genau dann, wenn $\alpha_i = 1$ und $\alpha_j = 0$. Wir schreiben vereinfachend auch $f = x_i x_j'$.

Polynome

- Eine Disjunktion von paarweise verschiedenen Monomen heißt Polynom. Sind alle Monome des Polynoms vollständig, so heißt das Polynom vollständig.

  Beispiel: Bei einer booleschen Funktion mit drei Variablen x_1, x_2, x_3 wäre:
  - $x_1' x_2 + x_2' x_3$ ein Polynom.
  - $x_1' x_2' x_3 + x_1 x_2' x_3$ ein vollständiges Polynom.
  - Das Polynom $x_1' x_2 + x_2' x_3$ beschreibt die boolesche Funktion $f \in \mathbb{B}_3$ mit $f(\alpha_1, \alpha_2, \alpha_3) = 1$ genau dann, wenn $\alpha_1 = 0, \alpha_2 = 1$ oder $\alpha_2 = 0, \alpha_3 = 1$. Wir schreiben vereinfachend auch $f = x_1' x_2 + x_2' x_3$.

Disjunktive Normalform

$$DNF: \quad \overline{x_1}\, x_2 + \overline{x_2}\, x_3$$

$$KNF: \quad (\overline{x_1} + x_2) \cdot (\overline{x_2} + x_3)$$

- Eine disjunktive Normalform (DNF) von f ist ein Polynom, das f beschreibt. Eine kanonische disjunktive Normalform (KDNF) von f ist ein vollständiges Polynom von f.
  - $f_1 = x_1' x_2' + x_2' x_3 + x_1 x_2$ ist in DNF, aber nicht in KDNF.

$$f_1 = \overline{x_1}\, x_2 + \overline{x_2}$$

$$f_2 = \overline{x_1}\, x_2 + \frac{\dfrac{x_1 \overline{x_2} + \overline{x_1}\, \overline{x_2}}{(x_1 + \overline{x_1})\, \overline{x_2}}}{\overline{x_2}}$$

Bestimmung der kanonischen disjunktiven Normalform

- Für $f : \mathbb{B}^n \to \mathbb{B}$ heißt $ON(f) := \{\alpha \in \mathbb{B}^n \mid f(\alpha) = 1\}$ die Erfüllbarkeitsmenge von f.
- Die KDNF ist gegeben durch $f = \sum_{\alpha \in ON(f)} m(\alpha)$
- Die KDNF ist (bis auf Anordnung von Literalen in Mintermen und von Termen im Polynom) eindeutig.
- Beispiel: KDNF für $f_1 = x_1' x_2' + x_2' x_3 + x_1 x_2$

$$
\begin{aligned}
f_1 &= m(000) + m(001) \\
&\quad + m(101) + m(110) + m(111) \\
&= x_1' x_2' x_3' + x_1' x_2' x_3 \\
&\quad + x_1 x_2' x_3 + x_1 x_2 x_3' + x_1 x_2 x_3
\end{aligned}
$$

x_1	x_2	x_3	f_1
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

- Anmerkung: Analog zur Erfüllbarkeitsmenge ist $OFF(f) := \{\alpha \in \mathbb{B}^n \mid f(\alpha) = 0\}$ als die Unerfüllbarkeitsmenge definiert.

Realisierungen von DNF

- Erste Möglichkeit: Benutze „gewöhnliche” UND- und ODER-Gatter.
- Zweite Möglichkeit: PLAs
  - Programmierbare logische Felder können nur Funktionen in DNF implementieren.
  - Sie benötigen dafür weniger Transistoren als eine Realisierung mit UND- und ODER-Gattern.

UNI FREIBURG

Realisierung durch Logikgatter

- Bilde erst alle Monome durch UND-Gatter.
- Verbinde dann alle Monome mit ODER-Gattern.
  - Notation: Man verzichtet in der Regel auf die Abbildung von Invertern.

- Die Kosten ergeben sich dann aus allen benötigten UND- und ODER-Gattern.

Programmierbare logische Felder (PLA)

Zweistufige Darstellung zur Realisierung von booleschen Polynomen.
$f_i = m_{i1} + m_{i2} + \cdots + m_{ik}$ mit m_{iq} aus $\{m_1, \ldots, m_s\}$

Enthält Monom m_j k Literale, so werden k Transistoren in der entsprechenden Zeile des **UND-Feldes** benötigt.

Besteht die Beschreibung von Funktion f_t aus p Monomen, so benötigt man p Transistoren in der entsprechenden Spalte des **ODER-Feldes**.

Fläche: $\sim (m + 2n) \times$ (Anzahl der benötigten Monome)

PLAs: Realisierungsdetails

Beispiel

$f_1 = x_1'x_2' + x_2'x_3 + x_1x_2$
$f_2 = x_2'x_3$

1-Leitung 0 $\Leftrightarrow$ $x_1 = 1 \vee x_2 = 1$

Konkrete Belegung

Beispiel

$f_1 = x_1' x_2' + x_2' x_3 + x_1 x_2$
$f_2 = x_2' x_3$

Bei Belegung von $x_1 = 1, x_2 = 1$ und $x_3 = 1$ liegt folgende Situation vor:

Kosten von PLA-Realisierungen von Monomen und Polynomen

- Sei $q = q_1 \cdot \dots \cdot q_r$ ein Monom, dann sind die Kosten $|q|$ von q gleich der Anzahl der zur Realisierung von q benötigten Transistoren im PLA, also $|q| := r$.
- Seien $p_1, \dots, p_m$ Polynome, dann bezeichne $M(p_1, \dots, p_m)$ die Menge der in diesen Polynomen verwendeten Monome.
  - Die primären Kosten $cost_1(p_1, \dots, p_m)$ einer Menge $p_1, \dots, p_m$ von Polynomen sind gleich der Anzahl der benötigten Zeilen im PLA, um $p_1, \dots, p_m$ zu realisieren, also $cost_1(p_1, \dots, p_m) = |M(p_1, \dots, p_m)|$.
  - Die sekundären Kosten $cost_2(p_1, \dots, p_m)$ einer Menge $\{p_1, \dots, p_m\}$ von Polynomen sind gleich der Anzahl der benötigten Transistoren im PLA, also $cost_2(p_1, \dots, p_m) = \underbrace{\sum_{q \in M(p_1, \dots, p_m)} |q|}_{\text{und-Feld}} + \underbrace{\sum_{i=1,\dots,m} |M(p_i)|}_{\text{oder-Feld}}$.

-15

Kombiniertes Kostenmaß

- Sei im Folgenden $cost = (cost_1, cost_2)$ die Kostenfunktion mit der Eigenschaft, dass für zwei Polynommengen $\{p_1, \ldots, p_m\}$ und $\{p'_1, \ldots, p'_m\}$ die Ungleichung

$$cost(p_1, \ldots, p_m) \leq cost(p'_1, \ldots, p'_m)$$

gilt, wenn

  - entweder $cost_1(p_1, \ldots, p_m) < cost_1(p'_1, \ldots, p'_m)$
  - oder $cost_1(p_1, \ldots, p_m) = cost_1(p'_1, \ldots, p'_m)$ und $cost_2(p_1, \ldots, p_m) \leq cost_2(p'_1, \ldots, p'_m)$

SMILE – Kosten der Realisierung

Welche der folgenden PLAs ist die kostengünstigste Lösung?

a. PLA 1 mit 10 Zeilen und 19 Transistoren.
b. PLA 2 mit 15 Zeilen und 30 Transistoren.
c. PLA 3 mit 12 Zeilen und 15 Transistoren.
d. PLA 4 mit 12 Zeilen und 19 Transistoren.

Das Problem der zweistufigen Logikminimierung

- **Gegeben:** Eine boolesche Funktion $f = (f_1, \ldots, f_m)$ in n Variablen und m Ausgängen in Form einer Tabelle der Dimension $(n+m) \cdot 2^n$ oder einer Menge von m Polynomen $\{q_1, \ldots, q_m\}$ mit $f_i = q_i$.
- **Gesucht:** m Polynome $p_1, \ldots p_m$, so dass p_i für alle i der Funktion f_i entspricht und die Kosten $cost(p_1, \ldots, p_m)$ minimal sind.
- Ab sofort werden nur noch Funktionen mit einem Ausgang betrachtet.

Veranschaulichung von Monomen und Polynomen

1-dim Würfel

2-dim Würfel

3-dim Würfel

4-dim Würfel

Veranschaulichung durch Würfel

- Jede boolesche Funktion f in n Variablen und einem Ausgang kann über einen n-dimensionalen Würfel durch Markierung der $ON(f)$-Menge spezifiziert werden.
  - **Beispiel**:
    $f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_1' x_2' x_3' + x_1 x_2' x_3' x_4$

Monome und Polynome als Teilwürfel

- Monome der Länge k entsprechen $(n-k)$-dimensionalen Teilwürfeln!
- Ein Polynom entspricht einer Vereinigung von Teilwürfeln.
- **Beispiel**:

$$f(x_1,x_2,x_3,x_4) = x_1x_2 + x_1'x_2'x_3' + x_1x_2'x_3'x_4$$

- **Gegeben**: Boolesche Funktion f in n Variablen und **einem** Ausgang, in Form eines markierten n-dimensionalen Würfels.
- **Gesucht**: Eine minimale Überdeckung der markierten Knoten durch maximale Teilwürfel im n-dimensionalen Würfel.

Entspricht einer Minimallösung:

$x_1 x_2 + x_1' x_2' x_3' + x_2' x_3' x_4$

- **Gegeben**: Boolesche Funktion f in n Variablen und **einem** Ausgang, in Form eines markierten n-dimensionalen Würfels.

- **Gesucht**: Eine minimale Überdeckung der markierten Knoten durch maximale Teilwürfel im n-dimensionalen Würfel.

Entspricht einer Minimallösung:

$x_1 x_2 + x_1' x_2' x_3' + x_2' x_3' x_4$

SMILE – Minimale Kosten

Gegeben ein PLA mit $m > 1$ Ausgängen und jede Funktion ist durch ein Minimalpolynom, also eine Minimallösung, die die • Funktion überdeckt wie auf der vorherigen Folie, realisiert. Sind die gesamten Kosten des PLA folglich auch minimal?

a. Ja.

b. Nein.

-24-

Implikanten und Primimplikanten

Definition

Eine boolesche Funktion $f \in \mathbb{B}_n$ ist kleiner gleich einer anderen booleschen Funktion $g \in \mathbb{B}_n$ ($f \leq g$), wenn $\forall \alpha \in \mathbb{B}_n : f(\alpha) \leq g(\alpha)$. (Das heißt, wenn f an einer Stelle 1 ist, dann auch g.)

Definition

Sei f eine boolesche Funktion mit einem Ausgang. Ein Implikant von f ist ein Monom q mit $q \leq f$. Ein Primimplikant von f ist ein maximaler Implikant q von f, das heißt es gibt keinen Implikanten s ($s \neq q$) von f mit $q \leq s$.
Implikanten und Primimplikanten können durch n-dimensionale Würfel veranschaulicht werden.

Veranschaulichung durch Würfel

- Ein Implikant von f ist ein Teilwürfel, der nur markierte Knoten enthält.
- Ein Primimplikant von f ist ein maximaler Teilwürfel mit dieser Eigenschaft.

Illustration für konkrete Funktion

Implikanten

- alle markierten Knoten
- alle Kanten, deren Ecken alle markiert sind
- alle Flächen, deren Ecken alle markiert sind
- alle 3-dimensionalen Würfel, deren Ecken alle markiert sind

Allgemein

- Die Implikanten sind die Teilwürfel, deren Ecken alle markiert sind.

Bestimmung von Primimplikanten

Es gibt 3 Primimplikanten, der durch unseren Würfel definierten Funktion:

- x_2

Bestimmung von Primimplikanten

Es gibt 3 Primimplikanten, der durch unseren Würfel definierten Funktion:

- x_2
- $x_1' x_3'$

Bestimmung von Primimplikanten

Es gibt 3 Primimplikanten, der durch unseren Würfel definierten Funktion:

- x_2
- $x_1' x_3'$
- $x_3' x_4$

Polynome und Implikanten einer Funktion f

Lemma

Die Monome eines Polynoms p von f sind alle Implikanten von f.

Beweis:

- Enthält ein Polynom p von f ein Monom m, welches nicht Implikant von f ist, so gilt nicht: $m \leq f$
- Das heißt es gibt eine Belegung $(\alpha_1, \ldots, \alpha_n)$ der Variablen $(x_1, \ldots, x_n)$ mit
  - $f(\alpha_1, \ldots, a_n) = 0$
  - $m(\alpha_1, \ldots, \alpha_n) = 1$, also auch $p(\alpha_1, \ldots, \alpha_n) = 1$
- Das heißt Monom m ist ein Teilwürfel, bei dem eine Ecke nicht markiert ist.

Demnach ist Polynom p kein Polynom von f.
$\Rightarrow$ **Widerspruch!**

Kapitel 3 – Kombinatorische Logik

1. Kombinatorische Schaltkreise
2. Normalformen, zweistufige Synthese
3. **Berechnung eines Minimalpolynoms**
4. Arithmetische Schaltungen
5. Anwendung: ALU von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Billigste Überdeckung der markierten Ecken

Wir suchen ein sogenanntes Minimalpolynom, das heißt ein Polynom mit minimalen Kosten.

Definition

Ein Minimalpolynom p einer booleschen Funktion f ist ein Polynom von f mit minimalen Kosten, das heißt mit der Eigenschaft $cost(p) \leq cost(p')$ für jedes andere Polynom p' von f.

Quine's Primimplikantensatz

Satz

Jedes Minimalpolynom p einer booleschen Funktion f besteht ausschließlich aus Primimplikanten von f.

Beweis:

- Nehme an, dass p einen nicht primen Implikanten m von f enthält.
- m wird durch einen Primimplikanten m' von f überdeckt, ist also in m' enthalten.
- Es gilt demnach $cost(m') < cost(m)$.
- Ersetzt man in p den Implikanten m durch den Primimplikanten m', so erhält man ein Polynom p', das ein Polynom von f ist mit $cost(p') < cost(p)$.
- **Widerspruch** dazu, dass p ein Minimalpolynom ist.

Berechnung von Implikanten

Lemma 1

Ist m ein Implikant von f, so auch $m \cdot x$ und $m \cdot x'$ für jede Variable x, die in m weder als positives, noch als negatives Literal vorkommt.

Beweis:

- $m \cdot x$ und $m \cdot x'$ sind Teilwürfel des Würfels m.
- Sind also alle Ecken von m markiert, so auch alle Ecken von $m \cdot x$ und $m \cdot x'$.

Lemma 2

Sind $m \cdot x$ und $m \cdot x'$ Implikanten von f, so auch m.

Beweis:

- $f \geq m \cdot x + m \cdot x' = m \cdot (x + x') = m$

$$\left.\begin{array}{l} f \geq mx \\ f \geq mx' \end{array}\right\} f \geq mx + mx'$$

UNI FREIBURG

Charakterisierung von Implikanten

Satz

Ein Monom m ist genau dann ein Implikant von f, wenn entweder

- m ein Minterm von f ist, oder
- $m \cdot x$ und $m \cdot x'$ Implikanten von f sind für eine Variable x, die nicht in m vorkommt.

- Äquivalente Schreibweise:

$$m \in Implikant(f)$$
$$\Leftrightarrow (m \in Minterm(f)) \vee (m \cdot x, m \cdot x' \in Implikant(f))$$

- Beweis folgt unmittelbar aus Lemma 1 und Lemma 2.

Berechnung eines Minimalpolynoms

- Verfahren von Quine-McCluskey zur Berechnung aller Primimplikanten.
  - Idee: Berechne sogar alle Implikanten. Dann ist klar, welche Primimplikanten sind.

- Verfahren zur Lösung des „Überdeckungsproblems".
  - Treffe unter den Primimplikanten eine geeignete Auswahl, so dass die Disjunktion der ausgewählten Primimplikanten ein Polynom für f ist und minimale Kosten hat.

6

Verfahren von Quine: Der Algorithmus

$\overline{x_1}\,\overline{x_2}$ $x_1 x_2$

Prime implicants function **Quine** ($f : \mathbb{B}^n \to \mathbb{B}$)

$mx + m\overline{x} \rightsquigarrow m$

$= m(x+\overline{x}) = m$

begin

$L_0 := Minterm(f);$

$i := 0;$

$//L_i$ enthält alle Implikanten von f der Länge $n-i$.

$Prim(f) := \varnothing$

while ($L_i \neq \varnothing$) **and** ($i < n$)

loop $L_{i+1} := \{m \mid m \cdot x$ und $m \cdot x'$ sind in L_i für ein $x\}$;

$Prim(f) := Prim(f) \cup$

$\{m' \mid m' \in L_i$ und m' wird von keinem $q \in L_{i+1}$ überdeckt$\}$;

$i := i + 1$

end loop;

return $Prim(f) \cup L_i$;

end;

Verbesserung durch McCluskey

- Vergleiche nur Monome untereinander
  - die die gleichen Variablen enthalten und
  - bei denen sich die Anzahl der positiven Literale nur um 1 unterscheidet.
- Dies wird erreicht durch:
  - Partitionierung von L_i in Klassen L_i^M, mit $M \subseteq \{x_1, \ldots, x_n\}$ und $|M| = n - i$.
  - L_i^M enthält die Implikanten aus L_i, deren Literale alle aus M sind.
  - Anordnung der Monome in L_i^M gemäß der Anzahl der positiven Literale.

Beispiel Quine-McCluskey

ON(f)

$L_0^{\{x_1,x_2,x_3,x_4\}}$:

0 0 0 0
0 0 0 1
0 1 0 0
1 0 0 0
0 0 1 1
0 1 0 1
1 0 0 1
1 0 1 0
1 1 0 0
0 1 1 1
1 1 0 1
1 1 1 0

$\bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4$
$\bar{x}_1\bar{x}_2\bar{x}_3x_4$
$\bar{x}_1\bar{x}_2\bar{x}_3$

steht für $x_1'x_2'x_3'x_4'$

$\bar{x}_1\bar{x}_3\bar{x}_4$

$\bar{x}_2\bar{x}_3\bar{x}_4$

steht für $x_1x_2'x_3'x_4$

Vergleiche im Folgenden nur Monome aus benachbarten Blöcken!

Beispiel Quine-McCluskey: Bestimmung von L_1 (1/4)

$L_0^{\{x_1,x_2,x_3,x_4\}}$:

0 0 0 0
0 0 0 1
0 1 0 0
1 0 0 0
0 0 1 1
0 1 0 1
1 0 0 1
1 0 1 0
1 1 0 0
0 1 1 1
1 1 0 1
1 1 1 0

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -

Beispiel Quine-McCluskey: Bestimmung von L_1 (2/4)

$L_0^{\{x_1,x_2,x_3,x_4\}}$:

0 0 0 0
0 0 0 1
0 1 0 0
1 0 0 0
0 0 1 1
0 1 0 1
1 0 0 1
1 0 1 0
1 1 0 0
0 1 1 1
1 1 0 1
1 1 1 0

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -

$L_1^{\{x_1,x_3,x_4\}}$:

0 - 0 0

Beispiel Quine-McCluskey: Bestimmung von L_1 (3/4)

$L_0^{\{x_1,x_2,x_3,x_4\}}$:

0 0 0 0
0 0 0 1
0 1 0 0
1 0 0 0
0 0 1 1
0 1 0 1
1 0 0 1
1 0 1 0
1 1 0 0
0 1 1 1
1 1 0 1
1 1 1 0

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -

$L_1^{\{x_1,x_3,x_4\}}$:

0 - 0 0
0 - 1 1

Beispiel Quine-McCluskey: Bestimmung von L_1 (4/4)

$L_0^{\{x_1,x_2,x_3,x_4\}}$:

0 0 0 0
0 0 0 1
0 1 0 0
1 0 0 0
0 0 1 1
0 1 0 1
1 0 0 1
1 0 1 0
1 1 0 0
0 1 1 1
1 1 0 1
1 1 1 0

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -

$L_1^{\{x_1,x_3,x_4\}}$:

0 - 0 0
0 - 1 1

Nicht kürzbar, da nicht Ecken der gleichen Kante. (Consensus existiert nicht!)

Beispiel Quine-McCluskey: Alle bestimmten Mengen L_1

1+a ⇝ 0 - - 1
1+b geht nicht

2+a ⇝ geht nicht
2+b ⇝ 1 - - 0

$L_1^{\{x_1,x_2,x_4\}}$:

0 0 - 1	1
1 0 - 0	2
0 1 - 1	a
1 1 - 0	b

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -
0 1 0 -
1 0 0 -
1 1 0 -

$L_1^{\{x_2,x_3,x_4\}}$:

- 0 0 0
- 0 0 1
- 1 0 0
- 1 0 1

$L_1^{\{x_1,x_3,x_4\}}$:

0 - 0 0
0 - 0 1
1 - 0 0
0 - 1 1
1 - 0 1
1 - 1 0

Alle Minterme von f sind Eckpunkte von Kanten, die Implikanten sind: $Prim(f) = \emptyset$

Beispiel Quine-McCluskey: Bestimmung von L_2 (1/2)

$L_1^{\{x_1,x_2,x_4\}}$:

0 0 - 1
1 0 - 0
0 1 - 1
1 1 - 0

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -
0 1 0 -
1 0 0 -
1 1 0 -

$L_1^{\{x_2,x_3,x_4\}}$:

- 0 0 0
- 0 0 1
- 1 0 0
- 1 0 1

$L_1^{\{x_1,x_3,x_4\}}$:

0 - 0 0
0 - 0 1
1 - 0 0
0 - 1 1
1 - 0 1
1 - 1 0

Alle Implikanten aus $L_1\{x_1,x_2,x_4\}$ sind Kanten von Flächen, die Implikanten sind: $Prim(f) = \emptyset$

Beispiel Quine-McCluskey: Bestimmung von L_2 (2/2)

$L_1^{\{x_1,x_2,x_4\}}$:

0 0 - 1
1 0 - 0
0 1 - 1
1 1 - 0

$L_1^{\{x_1,x_2,x_3\}}$:

0 0 0 -
0 1 0 -
1 0 0 -
1 1 0 -

$L_1^{\{x_2,x_3,x_4\}}$:

- 0 0 0
- 0 0 1
- 1 0 0
- 1 0 1

$L_1^{\{x_1,x_3,x_4\}}$:

0 - 0 0
0 - 0 1
1 - 0 0
0 - 1 1
1 - 0 1
1 - 1 0

Alle Implikanten aus L_1M sind Kanten von Flächen, die Implikanten sind: $Prim(f) = \emptyset$

Beispiel Quine-McCluskey: Bestimmung von L_3 (1/2)

$L_2^{\{x_1,x_2\}}$:

$L_2^{\{x_1,x_3\}}$:

0 - 0 -
1 - 0 -

$L_2^{\{x_1,x_4\}}$:

0 - - 1 | $\bar{x}_1 x_4$
1 - - 0 | $x_1 \bar{x}_4$

$L_2^{\{x_2,x_3\}}$:

- 0 0 -
- 1 0 -

$L_2^{\{x_2,x_4\}}$:

$L_2^{\{x_3,x_4\}}$:

- - 0 0
- - 0 1

- - 0 -
x_3

Die markierten Implikanten-Flächen sind nicht Rand eines 3-dim. Implikanten. Sie sind also prim! $\Rightarrow$ $Prim(f) = \{x_1' x_4, x_1 x_4'\}$

Beispiel Quine-McCluskey: Bestimmung von L_3 (2/2)

$L_2^{\{x_1,x_2\}}$:

$L_2^{\{x_1,x_4\}}$:

0 - - 1
1 - - 0

keine Vereinfachung möglich → Prim impl.

$L_2^{\{x_2,x_4\}}$:

$\bar{x}_1 x_4$, $x_1 \bar{x}_4$

$L_2^{\{x_1,x_3\}}$:

0 - 0 -
1 - 0 -

- - 0 -

$L_2^{\{x_2,x_3\}}$:

- 0 0 -
- 1 0 -

- - 0 -

$L_2^{\{x_3,x_4\}}$:

- - 0 0
- - 0 1

- - 0 -

Die markierten Implikanten-Flächen sind Rand eines 3-dimensionalen Implikanten. Sie sind also nicht prim! ⇒ $Prim(f) = \{x_1' x_4, x_1 x_4'\}$

18

Beispiel Quine-McCluskey: Ende

$L_3^{\{x_1\}}$:

$L_3^{\{x_2\}}$:

$L_3^{\{x_3\}}$:

- - 0 -

Primimplikant $\overline{x_3}$

$L_3^{\{x_4\}}$:

$Prim(f) = \{x_1' x_4, x_1 x_4'\}$

$\Rightarrow Prim(f) = \{x_1' x_4, x_1 x_4', x_3'\}$

$p_{complete}(f) = x_1' x_4 + x_1 x_4' + x_3'$

Korrektheit von Quine-McCluskey (1/2)

Prime implicants function **Quine** ($f : \mathbb{B}^n \to \mathbb{B}$)

begin
  $L_0 := Minterm(f)$;
  $i := 0$;
  $//L_i$ enthält alle Implikanten von f der Länge $n - i$.
  $Prim(f) := \varnothing$
  while ($L_i \neq \varnothing$) **and** ($i < n$)
  loop $L_{i+1} := \{m \mid m \cdot x$ und $m \cdot x'$ sind in L_i für ein $x\}$;
    $Prim(f) := Prim(f) \cup$
    $\{m' \mid m' \in L_i$ und m' wird von keinem $q \in L_{i+1}$ überdeckt$\}$;
    $i := i + 1$
  end loop;
  return $Prim(f) \cup L_i$;
end;

Korrektheit von Quine-McCluskey (2/2)

Satz

Für alle $i = 0, 1, \ldots, n$ gilt:

- L_i enthält nur Monome mit $n - i$ Literalen.
- L_i enthält genau die Implikanten von f mit $n - i$ Literalen.
- Nach Iteration i enthält $Prim(f)$ genau die Primimplikanten von f mit mindestens $n - i$ Literalen.

Beweis:
Induktion über i:

- Abbruchbedingung $(L_i = \emptyset)$ oder $(i = n)$:
- $L_i = \emptyset$ bedeutet, dass keine Implikanten bei der "Partnersuche" entstanden sind, d.h. L_{i-1} ist vollständig in $Prim(f)$ aufgegangen.
- $i = n$ bedeutet, dass L_n berechnet wurde, es gilt dann $L_n = \emptyset$ oder $L_n = \{1\}$, letzteres bedeutet f ist die Eins-Funktion und $Prim(f) = \{1\}$.

Kosten des Verfahrens

Lemma

Es gibt 3^n verschiedene Monome in n Variablen.

Beweis:
Für jedes Monom m und jede der n Variablen x liegt genau eine der drei folgenden Situationen vor:

- m enthält weder das positive noch das negative Literal von x.
- m enthält das positive Literal x.
- m enthält das negative Literal x'.

Jedes Monom ist durch diese Beschreibung auch eindeutig bestimmt.

22

Komplexität des Verfahrens von Quine-McCluskey

Satz

Die Laufzeit des Verfahrens liegt in $O(n^2 \cdot 3^n)$ beziehungsweise in $O(\log^2(N) \cdot N^{\log(3)})$, wobei $N = 2^n$ die Größe der Funktionstabelle ist.

$n = \log_2 N$

$3^{\log N}$

Beweisidee:
Jedes der 3^n Monome wird im Verlauf des Verfahrens mit höchstens n anderen Monomen verglichen.

- Gegeben sei ein Monom mx. Die Erzeugung von mx' und die Suche nach mx' in L_i ist bei Verwendung geeigneter Datenstrukturen in $O(n)$ durchführbar.

$O(n^2 \cdot 3^n) = O(\log^2(N) \cdot N^{\log(3)})$ durch Nachrechnen:

$$3^n = (2^{\log(3)})^n = (2^n)^{\log(3)} = N^{\log(3)}$$

UNI FREIBURG

Das Matrix-Überdeckungsproblem

- Wir haben nun durch das Verfahren von Quine-McCluskey alle Primimplikanten von f bestimmt.
- Die Disjunktion aller Primimplikanten ist ein Polynom, das f implementiert. Es ist aber im Allgemeinen kein Minimalpolynom von f.
- Für das Minimalpolynom benötigen wir eine kostenminimale Teilmenge M von $Prim(f)$, so dass die Monome von M f überdecken.
- Diese Art von Problemen wird Matrix-Überdeckungsproblem genannt.

Das Matrix-Überdeckungsproblem

- Wir haben nun durch das Verfahren von Quine-McCluskey alle Primimplikanten von f bestimmt.
- Die Disjunktion aller Primimplikanten ist ein Polynom, das f implementiert. Es ist aber im Allgemeinen kein Minimalpolynom von f.
- Für das Minimalpolynom benötigen wir eine kostenminimale Teilmenge M von $Prim(f)$, so dass die Monome von M f überdecken.
- Diese Art von Problemen wird Matrix-Überdeckungsproblem genannt.

SMILE - Das Matrix-Überdeckungsproblem: Einfaches Beispiel

- Für eine Expedition wird ein Fahrer, ein Messtechniker und ein Kameramann benötigt. Es stehen fünf Kandidaten mit unterschiedlichen Fähigkeiten und Gehaltsvorstellungen zur Auswahl. Welches ist das kostengünstigste Team?

Kandidat	Fahrer?	Messtechniker?	Kameramann?	Gehalt
Alice	Ja	Nein	Ja	4000
Dilbert	Ja	Ja	Nein	2000
Dogbert	Ja	Ja	Ja	5000
Ted	Nein	Nein	Ja	1000
Wally	Nein	Ja	Ja	1500

Primimplikantentafel

- Definiere eine boolesche Matrix $PIT(f)$, die Primimplikantentafel von f:
  - Die Zeilen entsprechen eindeutig den Primimplikanten von f.
  - Die Spalten entsprechen eindeutig den Mintermen von f.
  - Sei $min(\alpha)$ ein beliebiger Minterm von f.
    Dann gilt für Primimplikant m : $PIT(f)[m, min(\alpha)] = 1 \Leftrightarrow m(\alpha) = 1$.
- Der Eintrag an der Stelle $[m, min(\alpha)]$ ist also genau dann 1, wenn $min(\alpha)$ eine Ecke des Würfels m beschreibt.

Gesucht:
Eine kostenminimale Teilmenge M von $Prim(f)$, so dass jede Spalte von $PIT(f)$ überdeckt ist,
d.h. $\forall \alpha \in ON(f) \quad \exists m \in M$ mit $PIT(f)[m, min(\alpha)] = 1$.

Primimplikantentafel: Beispiel (1/2)

$$Prim(f) = \{x_1' x_4, x_1 x_4', x_3'\}$$

Primimplikantentafel $PIT(f)$:

1010 1110 0000 0001

	0	1	3	4	5	7	8	9	10	12	13	14
$x_1' x_4$		1	1		1	1						
$x_1 x_4'$							1		1	1		1
x_3'	1	1		1	1		1	1		1	1	

Primimplikantentafel: Beispiel (2/2)

Gesucht:
Eine kostenminimale Teilmenge M von $Prim(f)$, so dass jede Spalte von $PIT(f)$ überdeckt ist,
d.h. $\forall \alpha \in ON(f) \quad \exists m \in M$ mit $PIT(f)[m, min(\alpha)] = 1$.

$Prim(f) = \{x_1' x_4, x_1 x_4', x_3'\}$

Primimplikantentafel $PIT(f)$:

	0	1	3	4	5	7	8	9	10	12	13	14
$x_1' x_4$		1	1		1	1						
$x_1 x_4'$							1		1	1		1
x_3'	1	1		1	1		1	1		1	1	

Erste Reduktionsregel - Wesentlicher Implikant

Definition

Ein Primimplikant m von f heißt wesentlich, wenn es einen Minterm $min(\alpha)$ von f gibt, der nur von diesem Primimplikanten überdeckt wird, also:

- $PIT(f)[m, min(\alpha)] = 1$
- $PIT(f)[m', min(\alpha)] = 0$

für jeden anderen Primimplikanten m' von f.

Lemma

Jedes Minimalpolynom von f enthält alle wesentlichen Primimplikanten von f.

1. Reduktionsregel: Entferne aus der Primimplikantentafel $PIT(f)$ alle wesentlichen Primimplikanten und alle Minterme, die von diesen überdeckt werden.

Erste Reduktionsregel: Beispiel (1/2)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1				1												
2		1				1											
3			1				1										
4				1				1									
5									1								1
6						1				1							1
7							1				1						
8								1				1					
9									1				1				
10										1				1			1
11											1				1		
12												1				1	
13													1	1	1	1	

31

Erste Reduktionsregel: Beispiel (2/2)

wesentlich

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1				1												
2		1				1											
3			1				1										
4				1				1									
5					1				1								1
6						1				1							1
7							1				1						
8								1				1					
9									1				1				
10										1				1			1
11											1				1		
12												1				1	
13													1	1	1	1	

Nach Anwendung der 1. Reduktionsregel

	9	10	11	12	13	14	15	16	17
5	1								1
6		1							1
7			1						
8				1					
9	1				1				
10		1				1			1
11			1				1		
12				1				1	
13					1	1	1	1	

Die Matrix enthält keine wesentlichen Zeilen mehr!

Zweite Reduktionsregel - Spaltendominanz

Definition

Sei A eine boolesche Matrix. Spalte j von A dominiert Spalte i von A, wenn für jede Zeile k gilt: $A[k,i] \leq A[k,j]$.

- Nutzen für unser Problem: Dominiert ein Minterm w' von f einen anderen Minterm w von f, so braucht man w' nicht weiter zu betrachten, da w' auf jeden Fall überdeckt werden muss und hierdurch auch Minterm w' überdeckt wird.

- Jeder in $PIT(f)$ vorhandene Primimplikant p, der w überdeckt, überdeckt auch w'.

2. Reduktionsregel: Entferne aus der Primimplikantentafel $PIT(f)$ alle Minterme, die einen anderen Minterm in $PIT(f)$ dominieren.

Zweite Reduktionsregel: Beispiel

	9	10	11	12	13	14	15	16	17
5	1								1
6		1							1
7			1						
8				1					
9	1				1				
10		1				1			1
11			1				1		
12				1				1	
13					1	1	1	1	

Spalte 17 dominiert Spalte 10
$\Rightarrow$ Spalte 17 kann gelöscht werden!

35

Dritte Reduktionsregel - Zeilendominanz

Kosten

3	a	0	1	1	0
~~3~~	~~b~~	~~0~~	~~1~~	~~0~~	~~0~~
2	c	0	0	1	0

Definition

Sei A eine boolesche Matrix. Zeile i von A dominiert Zeile j von A, wenn für jede Spalte k gilt: $A[i,k] \geq A[j,k]$.

- Nutzen für unser Problem: Dominiert ein Primimplikant m einen Primimplikanten m', so braucht man m' nicht weiter zu betrachten, wenn $cost(m') \geq cost(m)$ gilt.

- Der Primimplikant m überdeckt jeden noch nicht überdeckten Minterm von f, der von m' überdeckt wird, obwohl er nicht teurer ist.

3. Reduktionsregel: Entferne aus der Primimplikantentafel $PIT(f)$ alle Primimplikanten, die durch einen anderen, nicht teureren Primimplikanten dominiert werden.

Dritte Reduktionsregel: Beispiel

Nehme an, dass die Zeilen 5 bis 12 gleiche Kosten haben.

	9	10	11	12	13	14	15	16
5	1							
6		1						
7			1					
8				1				
9	1				1			
10		1				1		
11			1				1	
12				1				1
13					1	1	1	1

Dritte Reduktionsregel: Beispiel

Nehme an, dass die Zeilen 5 bis 12 gleiche Kosten haben.

werden dominiert

	9	10	11	12	13	14	15	16
5	1							
6		1						
7			1					
8				1				
9	1				1			
10		1				1		
11			1				1	
12				1				1
13					1	1	1	1

Nach Anwendung der 3. Reduktionsregel

	9	10	11	12	13	14	15	16
9	$\boxed{1}$				1			
10		$\boxed{1}$				1		
11			$\boxed{1}$				1	
12				$\boxed{1}$				1
13					1	1	1	1

- Offensichtlich kann nun wieder die erste Reduktionsregel angewendet werden, da die Zeilen 9, 10, 11, 12 wesentlich sind.
  - Die resultierende Matrix ist leer.
  - Das gefundene Minimalpolynom ist:
    $1 + 2 + 3 + 4 + 9 + 10 + 11 + 12$

Nach Anwendung der 3. Reduktionsregel

	9	10	11	12	13	14	15	16
9	$\boxed{1}$				1			
10		$\boxed{1}$				1		
11			$\boxed{1}$				1	
12				$\boxed{1}$				1
13					1	1	1	1

- Offensichtlich kann nun wieder die erste Reduktionsregel angewendet werden, da die Zeilen 9, 10, 11, 12 wesentlich sind.
  - Die resultierende Matrix ist leer.
  - Das gefundene Minimalpolynom ist:
    1 + 2 + 3 + 4 + 9 + 10 + 11 + 12

SMILE - Ein weiteres Beispiel

Welche Reduktionsregel(n) können in dem Beispiel angewendet werden?

$Prim(f) = \{\{7,5\},\{5,13\},\{13,9\},\{9,11\},\{11,3\},\{3,7\}\}$

Primimplikantentafel $PIT(f)$:

	3	5	7	9	11	13
$\{7,5\}$		1	1			
$\{5,13\}$		1				1
$\{13,9\}$				1		1
$\{9,11\}$				1	1	
$\{11,3\}$					1	
$\{3,7\}$	1		1			

Lösungsmöglichkeit: Fallunterscheidung: branch & bound

SMILE - Ein weiteres Beispiel

Welche Reduktionsregel(n) können in dem Beispiel angewendet werden?

$Prim(f) = \{\{7,5\},\{5,13\},\{13,9\},\{9,11\},\{11,3\},\{3,7\}\}$

Primimplikantentafel $PIT(f)$:

	3	5	7	9	11	13
$\{7,5\}$		1	1			
$\{5,13\}$		1				1
$\{13,9\}$				1		1
$\{9,11\}$				1	1	
$\{11,3\}$	1				1	
$\{3,7\}$	1		1			

Kein Primimplikant ist wesentlich!

$Prim(f) = \{\{7,5\},\{5,13\},\{13,9\},\{9,11\},\{11,3\},\{3,7\}\}$

Zyklische Überdeckungsprobleme

Definition

Eine Primimplikantentafel heißt reduziert, wenn keine der drei Reduktionsregeln anwendbar ist.

- Ist eine reduzierte Tafel nicht-leer, spricht man von einem zyklischen Überdeckungsproblem.
- In der Praxis werden solche Probleme heuristisch gelöst. Es gibt auch exakte Methoden (Petrick, Branch-and-Bound).

Primimplikantentafel $PIT(f)$:

	3	5	7	9	11	13
$\{7,5\}$		1	1			
$\{5,13\}$		1				1
$\{13,9\}$				1		1
$\{9,11\}$				1	1	
$\{11,3\}$	1				1	
$\{3,7\}$	1		1			

Petrick's Methode

Verfahren:

- Übersetze die PIT in ein Produkt von Summen, d.h. in ein (OR, AND)-Polynom, das alle Möglichkeiten der Überdeckung enthält.

	3	5	7	9	11	13
$a : \{7,5\}$		1	1			
$b : \{5,13\}$		1				1
$c : \{13,9\}$				1		1
$d : \{9,11\}$				1	1	
$e : \{11,3\}$	1				1	
$f : \{3,7\}$	1		1			

- Multipliziere das (OR, AND)-Polynom aus, so dass ein (AND-OR)-Polynom entsteht.

wird übersetzt in

$$(e+f)\cdot(a+b)\cdot(a+f)\cdot(c+d)\cdot(d+e)\cdot(b+c)$$
$$= (ea+eb+fa+fb)\cdot(ac+ad+fc+fd)$$
$$\cdot(db+dc+eb+ec)$$
$$\vdots$$
$$= ace+acde+abcde+abcd+\cdots+bdf$$

- Die gesuchte minimale Überdeckung ist gegeben durch das Monom, das einer PI-Auswahl mit minimalen Kosten entspricht.

Bei gleichen Kosten für alle PIs sind *ace* und *bdf* minimal.

„Greedy-Heuristik” zur Lösung von Überdeckungsproblemen

1. Wende alle möglichen Reduktionsregeln an.
2. Ist die Matrix A leer, ist man fertig.
3. Sonst wähle die Zeile i, die die meisten Spalten überdeckt. Lösche diese Zeile und alle von ihr überdeckten Spalten und gehe zu 1.

- Dieser Algorithmus liefert nicht immer die optimale Lösung!
  - Hinweis: Bei der Ausgangs-Matrix aus unserem Beispiel überdeckt Zeile 13 die meisten Spalten.
    Diese ist nicht Teil der gefundenen Lösung!

-45

Zusammenfassung Schaltkreise

$f_n = x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n$

$\rightarrow 2^{n-1}$ Minterme

- Schaltkreise stellen boolesche Funktionen dar.
- Optimale boolesche Polynome können sehr viel größer sein, als entsprechende Schaltkreise.
  - exponentielle Unterschiede möglich
  - Rechtfertigung für Einsatz von Schaltkreisen statt PLAs
- Es gibt auch Algorithmen zur Berechnung optimaler (mehrstufiger) Schaltkreise.
  - anspruchsvoller als Optimierung von booleschen Polynomen
  - meist heuristisch (Näherungsverfahren)
  - nicht Gegenstand dieser Vorlesung
- Hier: Schaltkreise für spezielle Funktionen, insbesondere Arithmetik.

Kapitel 3 – Kombinatorische Logik

1. Kombinatorische Schaltkreise
2. Normalformen, zweistufige Synthese
3. Berechnung eines Minimalpolynoms
4. **Arithmetische Schaltungen**
5. Anwendung: ALU von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Arithmetische Schaltungen

- Addieren nach der Schulmethode: Carry-Ripple-Addierer.
- Effizienteres Addieren: Conditional-Sum-Addierer.
- Addition von Zweierkomplement-Zahlen.
- Subtrahierer.
- Exkurs: Multiplizierer.

Kosten von Schaltkreisen

- Um unterschiedliche Schaltkreise, die eine Funktion (z.B. Addierer) implementieren, miteinander zu vergleichen, benötigt man ein Kostenmaß.

Definition

Die Kosten $C(SK)$ eines Schaltkreises SK sind durch die Anzahl seiner Gatter gegeben.

- Deutet auf die Fläche und den Energieverbrauch der resultierenden Hardware-Blöcke hin.

hier: nur 2er-Gatter
keine negierten Gatteseingänge

Definition

Die Tiefe $depth(SK)$ eines Schaltkreises ist die maximale Anzahl von Gattern auf einem Pfad von einem beliebigen Eingang zu einem beliebigen Ausgang von SK.

- Deutet auf die Signallaufzeit durch SK und somit die maximal mögliche Taktfrequenz (Geschwindigkeit) des Schaltkreises hin.

Beispiel: Kosten und Tiefe

$C(SK) = 8$

$Depth(SK) = 3$

Teilschaltkreise, hierarchischer Entwurf (informell)

- Illustration eines Teilschaltkreises.

Hierarchische Schaltkreise

- In hierarchischen Schaltkreisen sind Teilschaltkreise durch Symbole ersetzt.
- Den zugehörigen („flachen") Schaltkreis erhält man, indem man die Symbole durch Einsetzen der Teilschaltkreise wieder entfernt.

Wiederholung Zahlendarstellung

$\langle 1011 \rangle = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

$8 + 0 + 2 + 1 = 11$

Sei $a = a_{n-1} \ldots a_0$ eine Folge von Ziffern, $a_i \in \{0, 1\}$.

- Binärdarstellung: $\langle a \rangle = \sum_{i=0}^{n-1} a_i 2^i$
- Zweierkomplement: $[a_n a_{n-1} \ldots a_0] = \sum_{i=0}^{n-1} a_i 2^i - a_n 2^n$

  $\langle a_{n-1} \ldots a_0 \rangle - a_n 2^n$
- Rechenregel: $-[a] = [\overline{a}] + 1$

mit $\overline{a} = \overline{a}_n \overline{a}_{n-1} \ldots \overline{a}_0$.

Addierer für nichtnegative Zahlen

010011
001110
111101
100001

- **Gegeben:**
  2 positive Binärzahlen $\langle a \rangle = \langle a_{n-1} \dots a_0 \rangle, \langle b \rangle = \langle b_{n-1} \dots b_0 \rangle$ mit Eingangsübertrag $c \in \{0, 1\}$.

- **Gesucht:**
  Schaltkreis, der Binärdarstellung s von $\langle a \rangle + \langle b \rangle + c$ berechnet.

  Eingänge: $\underset{\langle a \rangle}{n} + \underset{\langle b \rangle}{n} + \underset{c}{1}$

- Wegen $\langle a \rangle + \langle b \rangle + c \leq 2 \cdot (2^n - 1) + 1 = 2^{n+1} - 1$ genügen $n + 1$ Stellen für die Darstellung von s, d.h. der Schaltkreis hat $n + 1$ Ausgänge.

Formale Definition n-Bit-Addierer

- Ein n-Bit-Addierer ist ein Schaltkreis, der die folgende boolesche Funktion berechnet:

$$+_n : \mathbb{B}^{2n+1} \to \mathbb{B}^{n+1},$$
$$+_n : (a_{n-1}, \ldots, a_0, b_{n-1}, \ldots, b_0, c) = (s_n, \ldots, s_0)$$
$$\text{mit } \langle s \rangle = \langle s_n \ldots s_0 \rangle = \langle a_{n-1} \ldots a_0 \rangle + \langle b_{n-1} \ldots b_0 \rangle + c$$

Addieren nach der Schulmethode (1/4)

- Wir werden im Folgenden den einfachsten Addierertypen einführen, der die „Schulmethode” umsetzt.
- Hierzu werden einige Grundschaltungen (Halb- und Volladierer) notwendig sein.
- Beispiel für die Schulmethode:

$$
\begin{array}{rl}
 & a \quad 1\cdot 0\,1\,1 \\
+ & b \quad \cdot 0\,1\,1\,0 \\
 & \quad\;\; 1\;1\;1\;1\;0 \\
\hline
 & \quad\;\; 1\,0\,0\,0\,1
\end{array}
$$

Addieren nach der Schulmethode (2/4)

								HA
	a			1	0	1	1	a_0
+	b			0	1	1	0	b_0
			1	1	1	0		ha_1
			1	0	0	0	1	ha_0

a_0	b_0	ha_1 (And)	ha_0 (Xor)
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Halbaddierer (Half Adder, *HA*)

- Ein Halbaddierer dient zur Addition zweier 1-Bit-Zahlen ohne Eingangsübertrag.
- Er berechnet die Funktion $ha : \mathbb{B}^2 \to \mathbb{B}^2$ mit $ha(a_0, b_0) = (ha_1, ha_0)$, wobei $2ha_1 + ha_0 = a_0 + b_0$.

a_0	b_0	ha_1	ha_0
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

$$ha_0(a_0, b_0) = a_0 \oplus b_0$$
$$ha_1(a_0, b_0) = a_0 \wedge b_0$$

Schaltkreis eines Halbaddierers

dabei gilt:

$C(HA) = 2, \quad depth(HA) = 1$

Addieren nach der Schulmethode (3/4)

Volladierer (Full Adder, *FA*)

- Ein Volladdierer dient zur Addition zweier 1-Bit-Zahlen mit Eingangsübertrag.
- Er berechnet die Funktion $fa : \mathbb{B}^3 \to \mathbb{B}^2$ mit $fa(a_0, b_0, c) = (fa_1, fa_0)$ wobei $2fa_1 + fa_0 = a_0 + b_0 + c$

a_0	b_0	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

-15

Volladdierer als Funktion von *HA*s

Aus der Tabelle folgt:

$fa_0 = a_0 \oplus b_0 \oplus c$
$= ha_0(c, ha_0(a_0, b_0))$

$fa_1 = (a_0 \wedge b_0) \vee (c \wedge (a_0 \oplus b_0))$
$= ha_1(a_0, b_0) + ha_1(c, ha_0(a_0, b_0))$

Kosten und Tiefe eines *FA*:
$C(FA) = 5, \quad depth(FA) = 3$

a_0	b_0	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

UNI FREIBURG

Schaltkreis eines Volladdierers

HA: $c = 2$
$d = 1$

$c = 5$
$d = 3$

Addieren nach der Schulmethode (4/4)

Aufbau eines Carry-Ripple-Addierers

Induktive Definition des Carry-Ripple-Addierers CR

- Für $n = 1$: $CR_1 = FA$
- Für $n > 1$: Folgender Schaltkreis:

c_{-1}: Eingangsübertrag

c_i: Übertrag von Stelle i nach $i+1$

Zwei (identische) Darstellungen von *CR*

Carry-Ripple-Addierer

Satz

CR_n ist ein n-Bit-Addierer.

Beweis (duch Induktion):

- $n = 1$ ($CR_1 = FA$) ✓
- $n-1 \to n$: Eingabe an $CR_n : (a_{n-1}, \ldots, a_0, b_{n-1}, \ldots, b_0, c-1)$
  Zeige für Ausgabe $(s_n, \ldots, s_0)$ von CR_n:
  $\langle s \rangle = \langle s_n \ldots s_0 \rangle = \langle a_{n-1} \ldots a_0 \rangle + \langle b_{n-1} \ldots b_0 \rangle + c_{-1}$.
- Nach Induktionsvoraussetzung gilt für CR_{n-1}:
  $\langle s_n \ldots s_1 \rangle = \langle a_{n-1} \ldots a_1 \rangle + \langle b_{n-1} \ldots b_1 \rangle + c_0$. (a)
  Wegen FA-Eigenschaft gilt $\langle c_0, s_0 \rangle = a_0 + b_0 + c_{-1}$. (b)
- Insgesamt: $\langle s_n \ldots s_0 \rangle = 2 \cdot \langle s_n \ldots s_1 \rangle + s_0$
  $\overset{(a)}{=} 2 \cdot (\langle a_{n-1} \ldots a_1 \rangle + \langle b_{n-1} \ldots b_1 \rangle + c_0) + s_0$
  $= 2 \cdot (\langle a_{n-1} \ldots a_1 \rangle + \langle b_{n-1} \ldots b_1 \rangle) + 2 \cdot c_0 + s_0$ $= a_0 + b_0 + c_{-1}$
  $\overset{(b)}{=} 2 \cdot \langle a_{n-1} \ldots a_1 \rangle + a_0 + 2 \cdot \langle b_{n-1} \ldots b_1 \rangle + b_0 + c_{-1}$
  $= \langle a \rangle + \langle b \rangle + c_{-1}$

Schaltbild und Komplexität von *CR*

- $C(CR_n) = n \cdot C(FA) = 5n$.
- $depth(CR_n) = ?$.

Schaltbild und Komplexität von *CR*

- $C(CR_n) = n \cdot C(FA) = 5n$.
- $depth(CR_n) = 3 + 2(n-1)$.
- Sowohl die Kosten als auch die Tiefe von *CR* sind somit linear in n.

- Es gibt (asymptotisch) bessere Addierer. Wir werden hier den Conditional-Sum-Addierer kennen lernen, für den wir wieder eine Hilfsschaltung (Multiplexer) benötigen.
- Eine weitere wichtige Schaltung ist der Inkrementer.

n-Bit-Inkrementer

Definition

Ein n-Bit-Inkrementer INC_n berechnet die Funktion
$inc_n : \mathbb{B}^{n+1} \to \mathbb{B}^{n+1}$
$inc_n(a_{n-1}, \ldots, a_0, c) = (s_n, \ldots, s_0)$ mit $\langle s_n \ldots s_0 \rangle = \langle a \rangle + c$

- Ein Inkrementer ist ein Addierer mit $b_i = 0$ für alle i.
  $\Rightarrow$ Ersetze in CR_n die FA durch HA.
- Kosten und Tiefe:
  - $C(INC_n) = n \cdot C(HA) = 2n$
  - $depth(INC_n) = n \cdot depth(HA) = n$

n-Bit-Multiplexer

Definition

Ein n-Bit-Multiplexer MUX_n berechnet die Funktion

$sel_n : \mathbb{B}^{2n+1} \to \mathbb{B}^n$

$$sel_n(a_{n-1}, \ldots, a_0, b_{n-1}, \ldots, b_0, s) = \begin{cases} (a_{n-1} \ldots a_0), & \text{falls } s = 1 \\ (b_{n-1} \ldots b_0), & \text{falls } s = 0 \end{cases}$$

- Es gilt: $(sel_n)_i = s \cdot a_i + \overline{s} \cdot b_i$

Aufbau von MUX_n

Tiefe : 3
Kosten : $3n+1$

$sel_0 = (s \wedge a_0) \vee (\neg s \wedge b_0)$

$s=1$: $(1 \wedge a_0) \vee (0 \wedge b_0) = a_0$
$s=0$: $(0 \wedge a_0) \vee (1 \wedge b_0) = b_0$

Schaltbild und Kosten MUX_n

Kosten und Tiefe:

$C(MUX_n) = 3n + 1.$
$depth(MUX_n) = 3.$

Rückkehr zum Addierer

Gibt es billigere Addierer als CR_n?

Untere Schranken:
$C(+_n) \geq 2 \cdot n, \quad depth(+_n) \geq \log(n) + 1$

Sei $f \in \mathbb{B}_n$. Dann sind $C(f)$ und $depth(f)$ definiert durch
$C(f) = min\{C(SK) | f_{SK} = f\}$ und
$depth(f) = min\{depth(SK) | f_{SK} = f\}$.

Binäre Bäume mit $2n + 1$ Blättern haben $2n$ innere Knoten.
Binäre Bäume mit n Blättern haben mindestens Tiefe $\lceil \log(n) \rceil$.

Im Folgenden sei $n = 2^k$.

Conditional-Sum-Addierer (CSA)

- Idee: Nutze Parallelverarbeitung, um Tiefe zu reduzieren!

$$
\begin{array}{lr|r}
 & a_{n-1} \dots a_{\frac{n}{2}} & a_{\frac{n}{2}-1} \dots a_0 \\
+ & b_{n-1} \dots b_{\frac{n}{2}} & b_{\frac{n}{2}-1} \dots b_0 \\
+ & c_{\frac{n}{2}-1} & c_{-1} \\
\hline
 & s_n s_{n-1} \dots s_{\frac{n}{2}} & s_{\frac{n}{2}-1} \dots s_0
\end{array}
$$

- $CSA_1 = FA$.
- CSA_n: Siehe nächste Folie.
- Im Folgenden sei $n = 2^k$.

Aufbau von CSA_n

$a_{n-1} \dots a_0$ — a_l, a_h

depth $(CSA_{n/2})$

depth 3

$$\text{cost}(CSA_n) = 3 \cdot C(CSA_{n/2}) + C(MUX_{n+1}) = 3 \cdot C(CSA_{n/2}) + 3(n+1) + 1$$

$$\text{depth}(CSA_n) = \text{depth}(CSA_{n/2}) + 3$$

Komplexität von CSA_n: Tiefe

Satz

CSA_n hat Tiefe $\leq 3\log(n) + 3$.

Beweis: Setze $n = 2^k$ voraus.

$n = 2^k$

- $n = 1$: $depth(CSA_1) = depth(FA) = 3$.

- $n > 1$: $depth(CSA_n) \leq depth(CSA_{\frac{n}{2}}) + depth(MUX_{\frac{n}{2}+1})$
  $\leq depth(CSA_{\frac{n}{2}}) + 3$
  $\leq depth(CSA_{\frac{n}{4}}) + 3 + 3$
  $\leq depth(CSA_{\frac{n}{8}}) + 3 + 3 + 3$
  $\ldots$
  $\leq depth(CSA_{\frac{n}{2^k}}) + k \cdot 3$
  $= depth(CSA_1) + k \cdot 3$
  $\leq 3 \cdot (k+1) = 3\log(n) + 3.$

Komplexität von CSA_n: Kosten

Satz (ohne Beweis)

$C(CSA_n) = 10n^{\log(3)} - 3n - 2.$

$C(CSA_n) = 3 \cdot C(CSA_{n/2}) + 3n + 4$

- Man kann den hier vorgestellten *CSA* in einfacher Weise modifizieren, so dass
  - Tiefe = $O(\log(n))$,
  - Kosten = $O(n \cdot \log(n))$.
- Es gibt auch Addierer mit linearen Kosten und logarithmischer Tiefe.
  - Carry-Lookahead-Addierer (*CLA*).
  - $C(CLA_n) \leq 11n$,
  - $depth(CLA_n) \leq 4 \cdot \log(n) + 2$.

Addition von Zweierkomplementzahlen

- Auszurechnen ist:

$$[a_n a_{n-1} \ldots a_0] + [b_n b_{n-1} \ldots b_0] = (-a_n 2^n) + (-b_n 2^n) + \sum_{i=0}^{n-1} a_i 2^i + \sum_{i=0}^{n-1} b_i 2^i$$

- Im Fall von $(n+1)$-Bit-Zweierkomplementzahlen können Ergebnisse im Bereich $R_n = \{-2^n, \ldots, 2^n - 1\}$ dargestellt werden; andernfalls kommt es zu einem Überlauf.

- Der Satz auf der nächsten Folie sagt aus:
  - Kommt es bei der Addition nicht zu einem Überlauf, so kann man den „gewöhnlichen" Binäraddierer zur Addition von Zweierkomplementzahlen benutzen.
  - Ob es zu einem Überlauf kommt, lässt sich anhand von Werten a_n, b_n und s_n im Binäraddierer entscheiden.

Zweierkomplement-Addition formal

Satz

Seien $a, b \in \mathbb{B}^{n+1}$, $c_{-1} \in \{0,1\}$ und $s \in \{0,1\}^{n+1}$,
so dass $\langle c_n, s\rangle = \langle a\rangle + \langle b\rangle + c_{-1}$.

Dann gilt:

- $[a] + [b] + c_{-1} \notin R_n \Leftrightarrow (a_n = b_n) \wedge (b_n \neq s_n)$ Überlauferkennung
- $[a] + [b] + c_{-1} \in R_n \Rightarrow [a] + [b] + c_{-1} = [s]$

- Beweis durch Fallunterscheidung ($[a], [b]$ beide positiv, beide negativ, $[a]$ positiv / $[b]$ negativ) und Nachrechnen (Induktion).

- Man kann einen alternativen Überlauftest zeigen:

$$[a] + [b] + c_{-1} \notin R_n \Leftrightarrow c_n \neq c_{n-1}$$

Addierer für $(n+1)$-Bit-Zweierkomplement-Zahlen

Subtraktion

- Wegen $-[b] = [\overline{b}] + 1$ kann $[a] - [b]$ zurückgeführt werden auf $[a] + [\overline{b}] + 1$.

c_{-1}

- **Beispiel:**

$$[a] = [0110] = 6_{10}, \quad [b] = [0111] = 7_{10}, \quad [\overline{b}] = [1000]$$

$$\begin{array}{rr} & 0\,1\,1\,0 \\ + & 1\,0\,0\,0 \\ + & 1 \\ \hline & 1\,1\,1\,1 \end{array} \qquad 1111 = (-1)_{10}$$

- Den Schaltkreis für Subtraktion gewinnt man aus einem Addierer.
- Kombinierter Addierer/Subtrahierer.

Subtrahierer

$b \oplus 0 = b$
$b \oplus 1 = \neg b$

reiner Subtrahierer

sub = 1
subtraktion
sub = 0
Addition

$b_i \oplus 0 = b_i$ $\quad$ $sub = 0 : [a] + [b] + 0$

$b_i \oplus 1 = \overline{b_i}$ $\quad$ $sub = 1 : [a] + [\overline{b}] + 1 = [a] - [b]$

Exkurs – Multiplizierer

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Multiplizierer

- **Gesucht**: Schaltkreis zur Multiplikation zweier Binärzahlen $< a_{n-1}, \ldots, a_0 >, < b_{n-1}, \ldots, b_0 >$.

$$\begin{array}{r} 243 \cdot 12 \\ \hline 2430 \\ 486 \\ \hline 2916 \end{array}$$

- **Beispiel**:

$$\underbrace{(110)}_{6_{10}} \cdot \underbrace{(101)}_{5_{10}}$$

$$\begin{array}{cccccc} & & & 1 & 1 & 0 \\ + & & 0 & 0 & 0 & 0 \\ + & 1 & 1 & 0 & 0 & 0 \\ \hline & 1 & 1 & 1 & 1 & 0 \end{array}$$

$i = 0 \quad b_i = 1$

$i = 1 \quad b_i = 0$

$i = 2 \quad b_i = 1$

$= 30_{10}$

Allgemeines zum Multiplizierer

- Wieviele Stellen werden für das Ergebnis benötigt?

$$
\begin{aligned}
< a > \cdot < b > \quad &\leq \quad (2^n - 1) \cdot (2^n - 1) \\
= \quad 2^{2n} - 2^{n+1} + 1 \quad &\leq \quad 2^{2n} - 1
\end{aligned}
$$

- **Also**:
  $2n$ Stellen zur Multiplikation von Binärzahlen.

Vorgehen bei der Multiplikation

- Multipliziere die Beträge der Zahlen.
- Bestimme das Vorzeichen des Produkts.
- Setze das Endergebnis zusammen.

n-Bit-Multiplizierer

Definition

Ein n-Bit-Multiplizierer ist ein Schaltkreis, der die folgende Funtkion berechnet:

$mul_n : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$
$mul_n(a_{n-1}, \ldots, a_0, b_{n-1}, \ldots, b_0) = (p_{2n-1}, \ldots, p_0)$ mit
$< p_{2n-1}, \ldots, p_0 > = < a > \cdot < b >$

<a> + i Nullen
oder <0> + i Nullen

$$< a > \cdot < b > = < a > \cdot \sum_{i=0}^{n-1} b_i \cdot 2^i = \sum_{i=0}^{n-1} (< a > \cdot b_i \cdot 2^i)$$

Die Multiplikationsmatrix

$$\begin{pmatrix} pp_0 \\ pp_1 \\ \vdots \\ pp_{n-1} \end{pmatrix} =$$

1 And-Gatter

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_{n-1}b_0 & a_{n-2}b_0 & \dots & a_1b_0 & a_0b_0 \\ 0 & 0 & \dots & 0 & a_{n-1}b_1 & a_{n-2}b_1 & a_{n-3}b_1 & \dots & a_0b_1 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & a_{n-1}b_{n-1} & \dots & a_2b_{n-1} & a_1b_{n-1} & a_0b_{n-1} & \underbrace{0 \quad \dots \quad 0 \quad 0}_{n-1 \text{ Nullen}} \end{pmatrix} \begin{matrix} i=0 \\ i=1 \\ i=2 \\ \\ i=n-1 \end{matrix}$$

- Realisierung der Multiplikationsmatrix mit n^2 AND-Gattern (und n^2 Konstanten 0).

Daraus entstehende Aufgabe:

- Schnelle Addition von n Partialprodukten der Länge $2n$.
- Mit Carry-Lookahead-Addierern (CLAs) lösbar mit Kosten $O(n^2)$, Tiefe $O(n\ log(n))$ bei *linearem Aufsummieren* der Partialprodukte $((((pp_0 + pp_1) + pp_2) + \ldots) + pp_{n-1})$,

  Tiefe $O(log^2(n))$ bei *baumartigem Zusammenfassen* der Partialprodukte.

bisher: $C(Mul_n) = O(n^2)$
$depth(Mul_n) = O(\log^2 n)$ mit optimalem Addierer!

Verbesserung

- Verwende Carry-Save-Addierer.

- Reduktion von 3 Eingabeworten u, v, w zu zwei Ausgabeworten s, c mit
  $< u > + < v > + < w > = < s > + < c >$.

$$
\begin{array}{cccccccc}
 & u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & u_0 \\
 & v_{n-1} & v_{n-2} & \cdots & v_2 & v_1 & v_0 \\
 & w_{n-1} & w_{n-2} & \cdots & w_2 & w_1 & w_0 \\
\hline
c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_1 & c_0 & 0 \\
0 & s_{n-1} & s_{n-2} & \cdots & s_2 & s_1 & s_0
\end{array}
$$

- Gelöst durch Nebeneinandersetzen von Volladdierern (keine Carry-Chain!)

Carry-Save-Addierer (CSavA)

$\langle u \rangle + \langle v \rangle + \langle w \rangle = \langle c \rangle + \langle s \rangle$

Volladdierer sind <u>nicht</u> verbunden!!

Tiefe = 3

Kosten = 5n

Bemerkung zum Aufbau des CSavA

- Speziell bei Partialprodukten:
  Reduziere 3 2n-Bit-Zahlen zu 2 2n-Bit-Zahlen.

$$
\begin{array}{cccc}
pp_{0,2n-1} & \cdots & pp_{0,1} & pp_{0,0} \\
pp_{1,2n-1} & \cdots & pp_{1,1} & pp_{1,0} \\
pp_{2,2n-1} & \cdots & pp_{2,1} & pp_{2,0} \\
\hline
c_{2n-2} & \cdots & c_0 & 0 \\
s_{2n-1} & \cdots & s_1 & s_0
\end{array}
$$

- ($c_{2n-1} = 0$: Carry-Ausgang des letzten FA nicht verwendet.)

1. Serielle Lösung

- Hintereinanderschalten von n-2 CSavA-Addierern der Länge 2n.
  - Fasse *n* Partialprodukte zu 2 2n-Bit-Worten zusammen.
- Addiere die 2n-Bit-Worte mit CLA.
- *siehe Abb. einer Addierstufe*
- Kosten $O(n^2)$, Tiefe $O(n)$

Addierstufe im Multiplizierer

2. Baumartige Lösung

- Neue Grundzelle zur Reduktion von 4 2n-Bit-Eingabeworten zu zwei Ausgabeworten, bestehend aus 2 CSavA-Addierern (*siehe Abb. zur Reduktionszelle*).
- Baumartiges Zusammenfassen der Partialprodukte mit 4-zu-2-Bausteinen zu 2 2n-Bit Worten.
- Addiere die 2n-Bit-Worte mit CLA.
- *siehe Abb. der Addierstufe mit log. Zeit*
- Kosten $O(n^2)$, Tiefe $O(logn)$

4-zu-2 Reduktions-Grundzelle

Addierstufe des log-Zeit-Multiplizierers für 16 Bit

Kapitel 3 – Kombinatorische Logik

1. Kombinatorische Schaltkreise
2. Normalformen, zweistufige Synthese
3. Berechnung eines Minimalpolynoms
4. Arithmetische Schaltungen
5. **Anwendung: ALU von ReTI**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Anwendung: ALU von ReTI

- Die ALU (Arithmetic Logic Unit, arithmetisch-logische Einheit) dient der Berechnung von arithmetischen und logischen Operationen.
- Sie wird von den Compute-Befehlen verwendet und übernimmt weitere Aufgaben, z.B. Berechnung von Speicheradressen oder Erhöhung des *PC*.
- Erinnerung: Der Befehlssatz von ReTI hat die folgenden Compute-Befehle (s. nächste Folie).

Compute-Befehle: Kodierung

Typ	MI	F	Befehl	Wirkung	
0 0	0	0 1 0	SUBI i	$[ACC] := [ACC] - [i]$	$\langle PC \rangle := \langle PC \rangle + 1$
		0 1 1	ADDI i	$[ACC] := [ACC] + [i]$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 0	OPLUSI i	$ACC := ACC \oplus 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 1	ORI i	$ACC := ACC \vee 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 1 0	ANDI i	$ACC := ACC \wedge 0^8 i$	$\langle PC \rangle := \langle PC \rangle + 1$
0 0	1	0 1 0	SUB i	$[ACC] := [ACC] - [M(\langle i \rangle)]$	$\langle PC \rangle := \langle PC \rangle + 1$
		0 1 1	ADD i	$[ACC] := [ACC] + [M(\langle i \rangle)]$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 0	OPLUS i	$ACC := ACC \oplus M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 0 1	OR i	$ACC := ACC \vee M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$
		1 1 0	AND i	$ACC := ACC \wedge M(\langle i \rangle)$	$\langle PC \rangle := \langle PC \rangle + 1$

Spezifikation der ALU für ReTI

- Eine n-Bit-ALU mit:
  - Zwei n-Bit-Operanden a, b, Eingangscarry c,
    - ReTI: $n = 32$.
  - Einem m-Bit select-Eingang, der ausgewählt, welche Funktion ausgeführt wird,
    - Hier: 8 Funktionen (s. nächste Folie), daher $m = 3$ Bits.
  - Einem $(n+1)$-Bit-Ausgang.
    - $n = 32$.

- Insgesamt 68 Ein- und 33 Ausgänge.

Select-Eingang bei ReTI-ALU

Funktionsnummer			ALU-Funktion
s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Mögliche Realisierungen der ALU (1/2)

- **Option 1**: Realisiere Funktionen $f_0, \ldots, f_{2^m-1}$ getrennt durch SK_{f_i} für f_i, dann Auswahl durch einen verallgemeinerten Multiplexer.

Realisierung durch einen verallgemeinerten Multiplexer

Mögliche Realisierungen der ALU (2/2)

- **Option 1**: Realisiere Funktionen $f_0, \ldots, f_{2^m-1}$ getrennt durch SK_{f_i} für f_i, dann Auswahl durch einen Verallgemeinerten Multiplexer.

- **Option 2**: Gemeinsame Behandlung ähnlicher Funktionen.
  - Komplexer, aber effizienter.

Schaltrealisierung der ALU (1/2)

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Schaltrealisierung der ALU (2/2)

SMILE - Vergleich Option 1 mit Option 2

Wie verhalten sich Kosten und Tiefe der beiden Realisierungsoptionen zueinander?

a. $(\mathit{Tiefe}(\mathit{Option}1) \leq \mathit{Tiefe}(\mathit{Option}2))$ und $(\mathit{Kosten}(\mathit{Option}1) \leq \mathit{Kosten}(\mathit{Option}2))$
b. $(\mathit{Tiefe}(\mathit{Option}1) \geq \mathit{Tiefe}(\mathit{Option}2))$ und $(\mathit{Kosten}(\mathit{Option}1) \leq \mathit{Kosten}(\mathit{Option}2))$
c. $(\mathit{Tiefe}(\mathit{Option}1) \leq \mathit{Tiefe}(\mathit{Option}2))$ und $(\mathit{Kosten}(\mathit{Option}1) \geq \mathit{Kosten}(\mathit{Option}2))$
d. keine der obigen

Zusammenfassung Kombinatorische Logik

- Kombinatorische Schaltkreise setzen boolesche Funktionen um.
- PLAs sind zweistufig, mehrstufige Schaltungen bestehen aus Gattern und diese aus Transistoren.
- Minimierung von PLAs mit Verfahren von Quine-McCluskey und Lösen des Überdeckungsproblems.
- Statt Minimierung allgemeiner mehrstufiger Schaltkreise wurde eine Klasse (Addierer für Binär- und Zweierkomplementzahlen) betrachtet und ihre Integration in der ALU von ReTI diskutiert.

Kapitel 4 – Sequentielle Logik

1. **Speichernde Elemente**
2. Sequentielle Schaltkreise
3. Entwurf sequentieller Schaltkreise
4. SRAM
5. Anwendung: Datenpfade von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Schaltkreis (1/2)

$typ(v_1) = typ(v_2) = NAND$
$typ(v_3) = NOR$

x_4	y_1
0	0
1	1

Schaltkreis mit Eingabebelegung $a = (1, 1, 1, a_4)$.

Schaltkreis (2/2)

Schaltpläne (1/3)

- Analyse von Schaltplänen $SP = (\vec{X}_n, G, typ, IN, \vec{Y}_m)$ mit G nicht notwendigerweise azyklisch.

Schaltpläne (2/3)

- Eine Zellenbibliothek $BIB \subseteq \bigcup_{n \in \mathbb{N}} \mathbb{B}_n$ enthält Basisoperationen, die den Grundgattern entsprechen.
- Ein 5-Tupel $SP = (\vec{X}_n, G, typ, IN, \vec{Y}_m)$ heißt Schaltplan mit n Eingängen und m Ausgängen über der Zellenbibliothek BIB genau dann, wenn
  - $\vec{X}_n = (x_1, \ldots, x_n)$ ist eine endliche Folge von Eingängen.
  - $G = (V, E)$ ist ein gerichteter Graph mit $\{0, 1\} \cup \{x_1, \ldots, x_n\} \subseteq V$.
  - Die Menge $I = V \setminus (\{0, 1\} \cup \{x_1, \ldots, x_n\})$ heißt Menge der Gatter.
    Die Abbildung $typ : I \to BIB$ ordnet jedem Gatter $v \in I$ einen Zellentyp $typ(v) \in BIB$ zu.
  - ...

Schaltpläne (3/3)

- ...
- Für jedes Gatter $v \in I$ mit $typ(v) \in B_k$ gilt $indeg(v) = k$.
- $indeg(v) = 0$ für $v \in \{0, 1\} \cup \{x_1, \ldots, x_n\}$.
- Die Abbildung $IN : I \to E^*$ legt für jedes Gatter $v \in I$ eine Reihenfolge der eingehenden Kanten fest, d.h. falls $indeg(v) = k$, dann ist $IN(v) = (e_1, \ldots, e_k)$ mit $Z(e_i) = v \quad \forall 1 \leq i \leq k$.
- Die Folge $\vec{Y}_m = (y_1, \ldots, y_m)$ zeichnet Knoten $y_i \in V$ als Ausgänge aus.

Belegungen von Schaltplänen (1/2)

Sei nun ein Schaltplan $SP = (\vec{X}_n, G, typ, IN, \vec{Y}_n)$ gegeben.

- Eine Abbildung $\Phi_{SP,a} : V \to \{0,1\}$ für $a = (a_1, \ldots, a_n) \in \mathbb{B}^n$ heißt Belegung für Eingabebelegung a, falls
  - $\Phi_{SP,a}(x_i) = a_i \; \forall 1 \leq i \leq n$,
  - $\Phi_{SP,a}(0) = 0$, $\Phi_{SP,a}(1) = 1$.

Belegung von Schaltplänen (2/2)

Interessant für uns sind stabile Belegungen.

- Eine Belegung $\Phi_{SP,a} : V \to \{0,1\}$ heißt stabil, wenn gilt:
  - Für alle $v \in I$ mit $typ(v) = g \in B_k, IN(v) = (e_1, \ldots, e_k)$ ist $\Phi_{SP,a}(v) = g(\Phi_{SP,a}(Q(e_1)), \ldots, \Phi_{SP,a}(Q(e_k)))$.
  - $(\Phi_{SP,a}(y_1), \Phi_{SP,a}(y_2), \ldots, \Phi_{SP,a}(y_n))$ heißt Ausgangsbelegung von SP bei Eingangsbelegung a.

Es ist möglich, dass es zu einer Eingangsbelegung a

- keine stabile Signalbelegung $\Phi_{SP,a}$ gibt,

- mehrere stabile Signalbelegungen $\Phi_{SP,a}$ gibt.

Ein weiterer Schaltkreis (1/2)

$e_1 = \overline{x_2 x_3}$

$e_2 = \overline{x_1 e_1} = \overline{x_1 \overline{x_2 x_3}}$

$y_1 = \overline{e_1 + e_2}$

$=$

$$a = (a_1, a_2, a_3)$$

Ein weiterer Schaltkreis (2/2)

Ausschnitt aus vorherigem Schaltplan

Hinweis: Gatter benötigen Zeit bis ihr “Ergebnis” am Ausgang bereit liegt. Was passiert wenn man die Eingabebelegung nach einer Zeit (mehrfach) ändert?

RS-Flipflop (RS-FF)

- Die vorherige Schaltung heißt RS-Flipflop.
- Sie hat mindestens zwei stabile Zustände.

Zustand $Q = 0$

Zustand $Q = 1$

Übergang (1/2)

- Für das Umschalten von einem Zustand zum anderen in einer realen Implementierung eines RS-FFs ist es von entscheidender Bedeutung, dass reale Gatter Verzögerungszeiten haben.
- D.h.: Wenn sich die Eingangsbelegung eines Gatters ändert, dann erfolgt die daraus resultierende Änderung des Ausgangswertes nicht direkt, sondern mit einer gewissen Verzögerung.
- (Detailliertere Betrachtung in Kapitel 5, Physikalische Eigenschaften von Gattern.)

Übergang (2/2)

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).
- Nach Zeit $t_{P/SQ}$ ist $Q = 1$.
- Nach Zeit $t_{P/S/Q}$ ist $/Q = 0$.

Weitere Bezeichnungen

- Umschalten des FF in Zustand $Q = 1$ heißt Setzen (set).
- Umschalten des FF in Zustand $Q = 0$ heißt Zurücksetzen (reset).
- $/S$ heißt Set-Signal.
- $/R = /C$ heißt Reset- oder Clear-Signal.
- Weil $/R, /S$ durch Absenken aktiviert werden, nennt man sie active low.
- Signalnamen von active-low-Signalen beginnen in der Regel mit /.

“Zustand” $Q = 1$, $/Q = 1$

- Stabile Signalbelegung bei Eingangsbelegung $/S = 0$, $/Q = 0$
- Aber warum ist es trotzdem problematisch, $/S$ und $/R$ gleichzeitig zu aktivieren ($/S = 0$, $/R = 0$)?

Flackern

Annahme:

- $/S$ und $/R$ werden nach ihrer Aktivierung beide gleichzeitig inaktiv ($00 \rightarrow 11$)
- G_1 und G_2 schalten exakt gleich schnell, d.h. haben exakt die gleiche Verzögerungszeit

- $\Rightarrow$ Es kommt es zum Flackern ("metastabiler" Zustand).
- In der Praxis wird in der Regel nach einer gewissen Zeit einer der beiden stabilen Zustände angenommen (weil Gatterverzögerungen leicht variieren).

Schaltsymbol eines RS-FF

Nachteil von RS-FF

Beim Speichern eines Wertes 0 oder 1 muss man den Wert kennen:

- 0 $\rightarrow$ Aktiviere $/R$
- 1 $\rightarrow$ Aktiviere $/S$

Ziel:

- Speichern unbekannter Werte.

D-Latch (1/2)

W	D	$/S$	$/R$
0	0		
0	1		
1	0		
1	1		

- W ist active high.
  - $W = 0 \Rightarrow /S, /R$ inaktiv
  - $W = 1 \Rightarrow \begin{cases} /S \text{ aktiv, falls } D = 1 \\ /R \text{ aktiv, falls } D = 0 \end{cases}$

D-Latch (2/2)

W	D	/S	/R
0	0	1	1
0	1	1	1
1	0	1	0
1	1	0	1

Symbol:

Ansteuerung: Schreibimpuls

- Die Daten müssen für eine gewisse Zeit t_{SDW}, genannt Setup-Zeit, an D stabil anliegen.
- Dann geht W von 0 auf 1, bleibt für eine Zeit y, genannt Pulsweite, auf 1 und geht auf 0 zurück.
- Anschließend müssen die Daten für eine Zeit t_{HDW}, genannt Hold-Zeit, an D stabil gehalten werden.

Timing-Diagramm

Wie lange müssen die einzelnen Signale aktiv sein, damit der Schreibvorgang reibungslos abläuft?

⇒ Siehe nächstes Kapitel (Timing).

Weitere Eigenschaften eines D-Latches

- Bisher: Keine Datenänderungen während des Schreibpulses auf W.
- Man kann das D-Latch aber auch im transparenten Modus betreiben:
  - Das D-Latch heißt transparent, wenn das Schreibsignal aktiv ist.
  - Hält man W lange aktiv und ändert D zur Zeit t, dann ändert sich Q zur Zeit $t + t_{PDQ}$.
  - Auch hier sind zeitliche Bedingungen zu beachten: Keine Datenänderungen kurz nach Beginn des Transparenzmodus bzw. kurz vor Ende des Transparenzmodus.

Taktflankengesteuertes D-Flipflop (1/2)

- Taktflankengesteuerte Flipflops wie das D-Flipflop übernehmen Daten zu einem bestimmten Zeitpunkt (kein transparenter Modus!), nämlich bei der steigenden Flanke des Clocksignals.

D	*ck*	*Q*	*/Q*
0	⌐	0	1
1	⌐	1	0
X	0	*Q*	*/Q*
X	1	*Q*	*/Q*

- Vorteil: Daten müssen lediglich bei der steigenden Taktflanke stabil sein (zzgl. Setup- und Holdzeit).

Taktflankengesteuertes D-Flipflop (2/2)

- Realisierung: Wesentlich komplexer als bei taktzustandsgesteuerten D-Latches
- Analyse des Schaltplanes (und entsprechende Timing-Analyse) wesentlich komplizierter.

D-FF: Realisierung mit RS-Flipflops

Einfache Bausteine mit Flipflops

- Register
- Schieberegister
- Zähler

n-Bit Register

- n D-Flipflops mit gemeinsamen Clocksignal.

- Entsprechend: n-Bit Latch = n D-Latches mit gemeinsamem Schreibsignal W.

Schieberegister

- In jedem Takt (bei jeder steigenden Flanke von *ck*) werden die Werte im Register um eine Position nach rechts verschoben.

Zähler

Ein n-Bit-Zähler ist eine Schaltung mit folgenden Ein- und Ausgängen:

- Dateneingänge $X = (X_{n-1}, \ldots, X_0)$
- Datenausgänge $Y = (Y_{n-1}, \ldots, Y_0)$
- Dateneingang C_{in} für Eingangsübertrag
- Datenausgang C_{out} für Ausgangsübertrag
- Eingänge für Kontrollsignale:
  - $/C$ (Clear)
  - $/L$ (Load)
  - ck (Clock)

Aufbau eines Zählers

n-Bit Zähler: Funktionalität

- Ein Zähler speichert ein n-Bit-Wort, das an den Ausgängen Y erscheint (Zählerstand).
- Bei jeder steigenden Flanke von ck wird ein neuer Zählerstand Y_{neu} gespeichert. Für Y_{neu} gilt :

$$Y_{neu} = \begin{cases} 0\ldots0, & \text{falls } /C = 0 \\ X, & \text{falls } /C = 1, /L = 0 \\ bin_n((\langle Y \rangle + C_{in}) mod 2^n), & \text{falls } /C = 1, /L = 1 \end{cases}$$

n-Bit Zähler kaskadieren

- Ausgangsübertrag C_{out} ermöglicht es, den Zähler zu kaskadieren, zum Beispiel aus s n-Bit-Zählern einen $(s \cdot n)$-Bit-Zähler zu bauen.

Kapitel 4 – Sequentielle Logik

1. Speichernde Elemente
2. **Sequentielle Schaltkreise**
3. Entwurf sequentieller Schaltkreise
4. SRAM
5. Anwendung: Datenpfade von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Sequentielle Schaltkreise

- Im Folgenden werden keine allgemeinen Schaltpläne mehr analysiert, sondern sogenannte Schaltwerke (auch (synchrone) sequentielle Schaltkreise genannt).
- Diese bestehen aus einem Register und einem (kombinatorischen) Schaltkreis (auch kombinatorischer Kern genannt).
- Im Gegensatz zu (kombinatorischen) Schaltkreisen können Schaltwerke (= sequentielle Schaltkreise) Zyklen enthalten. Die Zyklen müssen aber durch Flipflops des Registers gehen.
- Der Zustand eines Schaltwerkes ist gegeben durch die im Register gespeicherten Werte.
- Schaltwerke (= sequentielle Schaltkreise) entsprechen endlichen Zustandsautomaten.

Beispiel: Zähler als sequentieller Schaltkreis

Endliche Zustandsautomaten

- Endliche Zustandsautomaten (Finite State Machines, FSMs) sind ein Formalismus, um sequentielles (zeitabhängiges) Verhalten zu spezifizieren.
  - Mealy- und Moore-Automaten
  - In der theoretischen Informatik werden endliche Automaten mit akzeptierenden Zustände betrachtet. Diese sind mit FSMs verwandt, aber nicht identisch.
- Aus einer FSM-Spezifikation kann der sequentielle Schaltkreis hergeleitet werden (Sequentielle Synthese).

Halbautomat

Definition

Das Quadrupel $H = (I, S, S_0, \delta)$ heißt deterministischer, endlicher Halbautomat. Dabei bezeichnet:

- I eine endliche Menge von erlaubten Eingabesymbolen ("Eingabealphabet"),
- S eine endliche Menge von Zuständen,
- $S_0 \subseteq S$ ist eine endliche Menge von erlaubten Anfangszuständen,
- $\delta : S \times I \to S$ eine Übergangsfunktion.

Beispiel: Kaffeeautomat

Auswahl:
- Kaffee
- Tee
- Zucker

korrekter Münzeinwurf oder Fertig

Darstellung als Zustandsdiagramm

- Knoten: Zustände des Automaten.
- Kanten: Zustandsübergänge.
- Kantenmarkierung: Eingabe (bzw. Ereignis).

Mealy- und Moore-Automat

Definition

Ein Mealy-Automat $M = (I, O, S, S_0, \delta, \lambda)$ ist ein endlicher deterministischer Halbautomat H erweitert um:

- eine endliche Menge O von Ausgabesymbolen („Ausgabealphabet"),
- eine Ausgabefunktion $\lambda : S \times I \to O$.

$\delta : S \times I \to S$

Definition

Ein Moore-Automat $M = (I, O, S, S_0, \delta, \lambda)$ ist ein endlicher, deterministischer Halbautomat H erweitert um:

- eine endliche Menge O von Ausgabesymbolen,
- eine Ausgabefunktion $\lambda : S \to O$.

Beispiel: Getränkeauswahl - Mealy-Automat

- Knoten: Zustände des Automaten.
- Kanten: Zustandsübergänge.
- Kantenmarkierung: Ein-/Ausgabe (Mealy-Automat).
- Beim Moore-Automaten werden die Zustände mit der Ausgabe beschriftet.
- ε bedeutet keine Eingabe/Ausgabe.

Mealy- vs. Moore-Automat (1/2)

- Beim Mealy-Automaten ist:
  - die Ausgabe abhängig vom aktuellen Zustand und der aktuellen Eingabe,
  - der Folgezustand abhängig vom aktuellen Zustand und der aktuellen Eingabe.
- Ein Moore-Automat ist ein spezieller Mealy-Automat, bei dem die Ausgabe nur vom aktuellen Zustand und nicht von der Eingabe abhängt.
- Moore- und Mealy-Automaten kann man ineinander überführen.

Mealy- vs. Moore-Automat (2/2)

- Überführung Moore $\rightarrow$ Mealy: trivial
- Überführung Mealy $\rightarrow$ Moore:
  Grundidee:“Ziehe Ausgabe in den Zustand”

Beispiel: Moore-Automat von Zustand “Bereit”

Unterschiedliche Darstellungen von endlichen Zustandsautomaten

a) Zustands- und Ausgangstafel:

x	*state*	*next-state*	y
1	s_1	s_1	0
0	s_1	s_2	1
-	s_2	s_1	0

b) Flusstafel:

	$x = 0$	$x = 1$
s_1	$s_2, 1$	$s_1, 0$
s_2	$s_1, 0$	$s_1, 0$

c) Zustandsdiagramm:

d) Sequentieller Schaltkreis:

$y = \overline{s + x}$

1

- Im Folgenden: Weg von *c)* zu *d)*

Sequentielle Schaltkreise allgemein

$$y_i^t = \lambda_i(x_1^t, x_2^t, \ldots, x_k^t, s_1^t, s_2^t, \ldots, s_p^t)$$
$$s_i^{t+1} = \delta_i(x_1^t, x_2^t, \ldots, x_k^t, s_1^t, s_2^t, \ldots, s_p^t)$$

Die Belegung s_t der Flipflops im Register heißt Zustand des sequentielle Schaltkreises zum Zeitpunkt t.

Kombinatorischer Kern

- Der kombinatorische Kern hat vier Arten von Ein- und Ausgängen:
  - Primäre Eingänge bekommen Werte „von außen”.
  - Primäre Ausgänge liefern Werte „nach außen”.
  - Sekundäre Eingänge sind mit den Datenausgängen der Flipflops im Register verbunden. Auf diese Weise kann der aktuelle Zustand des Schaltkreises in Funktionen δ und λ berücksichtigt werden.
  - Sekundäre Ausgänge sind mit den Dateneingängen der Flipflops verbunden. Durch sie wird der nächste Zustand des Schaltkreises spezifiziert.

Primäre und sekundäre Ein- und Ausgänge

$$y_i^t = \lambda_i(x_1^t, x_2^t, \ldots, x_k^t, s_1^t, s_2^t, \ldots, s_p^t)$$
$$s_i^{t+1} = \delta_i(x_1^t, x_2^t, \ldots, x_k^t, s_1^t, s_2^t, \ldots, s_p^t)$$

Sequentielle Schaltung für einen FSM

Mealy-Automat

Moore-Automat

- Eingabevektor: $X = (x_1, x_2, \ldots, x_k)$
- Ausgabevektor: $Y = (y_1, y_2, \ldots, y_m)$
- Zustandsvektor: $S = (s_1, s_2, \ldots, s_p)$

- Ausgabefunktion (Mealy): $Y^t = \lambda(X^t, S^t)$
- Übergangsfunktion: $S^{t+1} = \delta(X^t, S^t)$
- Ausgabefunktion (Moore): $Y^t = \lambda(S^t)$

x
y
r_0
r_1

00
10
01
11
0/1
1/1
1/0
0/1
0/1
1/0
0/1
1/1

Kapitel 4 – Sequentielle Logik

1. Speichernde Elemente
2. Sequentielle Schaltkreise
3. **Entwurf sequentieller Schaltkreise**
4. SRAM
5. Anwendung: Datenpfade von ReTI

.

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Entwurf sequentieller Schaltkreise

X = beliebig

Zustandsdiagramm:

⇒

Zustands- und Ausgangstafel:

s^t	x_1^t	x_2^t	s^{t+1}	y^t
0	0	0	0	0
0	0	1	0	0
0	1	0	1	1
0	1	1	1	0
1	0	0	1	1
1	0	1	0	0
1	1	0	1	1
1	1	1	0	1

Sequentieller Schaltkreis:

⇒

Entwurfsschritte

- Optimierung des Zustandsdiagramms: Zustandsminimierung
  - Identifikation der äquivalenten Zustände.
  - Ergebnis: Ein (evtl. kleineres) Zustandsdiagramm.

- Wahl der Zustandskodierung.
  - Ergebnis: Anzahl der Flipflops im Register, Funktionen δ und λ (Zustands- und Ausgangstafel).

- Implementierung von δ und λ.
  - Kombinatorische Logiksynthese, z.B. Quine-McCluskey.

Zustandsminimierung

Idee:

Bestimme und verschmelze äquivalente Zustände.

- Zwei Zustände sind äquivalent, wenn der Automat von ihnen aus bei gleichen Eingabefolgen stets die gleichen Ausgabefolgen produziert.

Weiteres Beispiel (1/4)

- Hinreichende Bedingung: Wenn bei zwei Zuständen bei gleicher Eingabe auch die gleiche Ausgabe erzeugt wird und der gleiche Folgezustand angenommen wird, dann sind die Zustände sicherlich äquivalent.
- Äquivalente Zustände können durch einen einzigen Zustand ersetzt werden (siehe nächste Folie).

Weiteres Beispiel (2/4)

Zustand e und d sind äquivalent.

Weiteres Beispiel (3/4)

Zustand e eliminiert.
Zustand b und c sind äquivalent.

Weiteres Beispiel (4/4)

Zustand c eliminiert.

Entwurfsschritte

- Optimierung des Zustandsdiagramms: Zustandsminimierung
  - Identifikation der äquivalenten Zustände.
  - Ergebnis: Ein (evtl. kleineres) Zustandsdiagramm.

- Wahl der Zustandskodierung.
  - Ergebnis: Anzahl der Flipflops im Register, Funktionen δ und λ (Zustands- und Ausgangstafel).

- Implementierung von δ und λ.
  - Kombinatorische Logiksynthese, z.B. Quine-McCluskey.

Zustandskodierung

Kodierung $S_1 \equiv 00, S_3 \equiv 10, S_4 \equiv 01$: 9 Literale

$$\delta_1(s,i) = s_2 i + s_1 \bar{i}$$
$$\delta_2(s,i) = \overline{s_1}\,\overline{s_2} i$$
$$\lambda(s,i) = \overline{s_2} i$$

s	x	s'	y
00	0	00	0
01	1	10	0

Kodierung $S_1 \equiv 01, S_3 \equiv 11, S_4 \equiv 10$: 11 Literale

$$\delta_1(s,i) = s_1 s_2 \bar{i} + \overline{s_1} i + \overline{s_2} i$$
$$\delta_2(s,i) = s_1 + i$$
$$\lambda(s,i) = s_2 i$$

s	x	s'	y
01	0	01	0

- **Ziel:** Wähle Zustandskodierung, die nachfolgende kombinatorische Synthese erleichtert.
- Dafür gibt es (heuristische) Verfahren.

Entwurf eines einfachen sequentiellen Schaltkreises am Beispiel

- Aufgabenbeschreibung (Textspezifikation): Modulo-4 Vorwärts/Rückwärtszähler
  - Der Zähler soll von 0 bis 3 zählen können.
  - Ist der Steuereingang x auf 1 gesetzt, so soll vorwärts gezählt werden, d.h. die Zahlenfolge $0, 1, 2, 3$ durchlaufen werden.
  - Ist x auf 0 gesetzt, so soll rückwärts gezählt werden, d.h. die Zahlenfolge $3, 2, 1, 0$ durchlaufen werden.
  - Am Ausgang ist der Zählerstand anzugeben (Ausgabevektor y_0, y_1). Der Zähler ist als Ringzähler zu realisieren.

SMILE - Zustände im Zustandsdiagramm

Wie viele Zustände benötigt das Zustandsdiagramm für den Zähler bei der gegebenen Spezifikation?

a. 1
b. 2
c. 4
d. 8
e. 16

Von der Textspezifikation zum Zustandsdiagramm

- 4 Zustände erforderlich.
- Startzustand 0.

Vom Zustandsdiagramm zur Zustands- und Ausgangstafel

- Zustandsminimierung ⇒ Keine äquivalente Zustände.
- Zustandskodierung: $0 \to 00, 1 \to 01, 2 \to 10, 3 \to 11$.

	x	z_1^t	z_0^t	z_1^{t+1}	z_0^{t+1}	y_1	y_0
Vorwärts-zählen	1	0	0	0	1	0	0
	1	0	1	1	0	0	1
	1	1	0	1	1	1	0
	1	1	1	0	0	1	1
Rückwärts-zählen	0	1	1	1	0	1	1
	0	1	0	0	1	1	0
	0	0	1	0	0	0	1
	0	0	0	1	1	0	0

Eingänge — Ausgänge

$$z_1^{t+1} = \bar{x}\,\bar{z}_1\,\bar{z}_0 + \bar{x}\,z_1 z_0 + x\,z_1\,\bar{z}_0 + x\,\bar{z}_1 z_0$$

Implementierung des kombinatorischen Kerns

	x	z_1^t	z_0^t	z_1^{t+1}	z_0^{t+1}	y_1	y_0
Vorwärts-zählen	1	0	0	0	1	0	0
	1	0	1	1	0	0	1
	1	1	0	1	1	1	0
	1	1	1	0	0	1	1
Rückwärts-zählen	0	1	1	1	0	1	1
	0	1	0	0	1	1	0
	0	0	1	0	0	0	1
	0	0	0	1	1	0	0

Übergangsfunktion:

$$z_0^{t+1} = x\overline{z}_1^t\overline{z}_0^t + xz_1^t\overline{z}_0^t + \overline{x}z_1^t\overline{z}_0^t + \overline{x}\,\overline{z}_1^t\overline{z}_0^t$$

$$z_1^{t+1} = x\overline{z}_1^t z_0^t + xz_1^t\overline{z}_0^t + \overline{x}z_1^t z_0^t + \overline{x}\,\overline{z}_1^t\overline{z}_0^t$$

Implementierung des komb. Kerns: Logikminimierung

Ausgangsfunktion: $y_0^t = z_0^t, \quad y_1^t = z_1^t$

Übergangsfunktion:

$$z_0^{t+1} = x\overline{z}_1^t\overline{z}_0^t + xz_1^t\overline{z}_0^t + \overline{x}z_1^t\overline{z}_0^t + \overline{x}\,\overline{z}_1^t\overline{z}_0^t$$

$$z_1^{t+1} = \underbrace{x\overline{z}_1^t z_0^t}_{1} + \underbrace{xz_1^t\overline{z}_0^t}_{1} + \underbrace{\overline{x}z_1^t z_0^t}_{1} + \underbrace{\overline{x}\,\overline{z}_1^t\overline{z}_0^t}_{3}$$

Minimierung:

$$z_0^{t+1} = \overline{z}_0^t$$

$$z_1^{t+1} = x\overline{z}_1^t z_0^t + xz_1^t\overline{z}_0^t + \overline{x}z_1^t z_0^t + \overline{x}\,\overline{z}_1^t\overline{z}_0^t$$

Beispiel: Ergebnis

Resultierender Automat ist Moore-Automat.

Ausgabefunktion ist Identität auf den Zustandsbits.

Kapitel 4 – Sequentielle Logik

1. Speichernde Elemente
2. Sequentielle Schaltkreise
3. Entwurf sequentieller Schaltkreise
4. **SRAM**
5. Anwendung: Datenpfade von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

SRAM

- Static Random-Access Memory.
- Konzeptuell: Eine (sehr große) Anzahl N von Speicherzellen sowie ein (sehr großer) Multiplexer, um auf die einzelnen Zellen zuzugreifen.
- Durch die Größe spielen Beschränkungen eine Rolle, die bei einer Realisierung beachtet werden müssen.
  - Fanout-Beschränkung: Eine Leitung kann nicht beliebig verzweigen $\Rightarrow$ Treiberbäume
  - Fanin-Beschränkung: Ein Gatter kann nicht beliebig viele Eingänge haben (Hier: N-faches ODER als Baum).

SRAM: Ein-/Ausgänge und Zeichen

- Sei $n \in \mathbb{N}, N = 2^n$. Ein N-Bit statischer Speicher oder SRAM hat:
  - n Eingänge $A = (A_{n-1}, \ldots, A_0)$ „Adresse",
  - Dateneingang D_{in},
  - Datenausgang D_{out},
  - Kontrollsignal W „write"

SRAM: Funktionalität

- Der Speicher enthält N Speicherzellen $L_0, \ldots, L_{N-1}$, die je ein Bit speichern können.
- Zelle $L_{\langle A \rangle}$ wird mit Hilfe der Adresse A ausgewählt.
  - An D_{out} erscheint der Inhalt von $L_{\langle A \rangle}$.
  - Durch Schreibpuls an W wird D_{in} nach $L_{\langle A \rangle}$ übernommen.

N-Bit-SRAM, $N \times s$-Bit-SRAM: Aufbau

- Ein $N \times s$-Bit-SRAM besteht aus s N-Bit SRAMs mit gemeinsamen Adress- und Schreibsignalen.
  - s heißt Bitbreite des $N \times s$-Bit-SRAMs.
- Ein N-Bit-SRAM besteht im Prinzip aus 3 Hilfsschaltkreisen:
  - mehrfaches ODER
  - Treiberbäume
  - Dekodierer

SRAM: Schaltbild

O_N: Mehrfaches ODER

- Ein N-faches ODER O_N mit $N = 2^n$ ist ein Schaltkreis, der N-faches Oder berechnet.
- Balancierter Baum, um Verzögerungszeit zu minimieren (Tiefe $O(\log N) = O(n)$).

Treiberbäume

- Ein Treiber ist ein Gatter mit einem Eingang X und einem Ausgang Y, das die Identität $Y = X$ berechnet.
  - Eingesetzt, um Fanout-Beschränkung zu überwinden.
  - Beispiel: Fanout-Beschränkung von 3.

F_N: Treiberbäume im SRAM

- Zur Erinnerung: Ein Baum ist ein azyklischer gerichteter Graph $G = (V, E)$ mit:
  - Genau einer Quelle w,
  - $indeg(v) = 1$ für alle $v \in V \setminus \{w\}$
  - Blätter = Knoten $v \in V$ mit $outdeg(v) = 0$
  - Innere Knoten = Knoten $v \in V$ mit $outdeg(v) \geq 1$.
- Im SRAM für Realisierung von F_N eingesetzt.
- Fanout-Beschränkung von 10 $\rightarrow$ 10-äre Bäume.

10-äre Bäume (1/2)

B_0:

B_1:

B_s:

- Anzahl der Blätter von B_s: $L(B_s)$.
  - Entspricht dem erreichten Verzweigungsgrad.
- Anzahl der inneren Knoten von B_s: $I(B_s)$.
  - Entspricht der benötigten Anzahl von Treibern.

$$L(B_s) = 10^s$$

$$I(B_s) = \sum_{i=0}^{s-1} 10^i = \frac{10^s - 1}{10 - 1} < \frac{L(B_s)}{9}$$

10-äre Bäume (2/2)

- Benutze also B_s zum 10^s-fachen Vervielfältigen eines Signals
- Innere Knoten des Baumes werden durch Treiber ersetzt
- $\Rightarrow$ Treiberbaum mit Fanoutbeschränkung 10

Treiberbäume: Allgemeiner Fall (1/2)

- Angenommen, ein Signal soll N-fach vervielfältigt werden mit $10^{s-1} < N < 10^s$ keine Zehnerpotenz.
- Ziel: Balancierte Treiberbäume, d.h. alle Pfade von der Wurzel zu einem Blatt haben gleiche Länge.

N = 11, unbalanciert

N = 11, balanciert

Treiberbäume: Allgemeiner Fall (2/2)

- Idee: “Fülle Bäume von links her 10-är auf” und sorge zusätzlich für gleiche Tiefe der Blätter!
- Beispiel: ...

Lemma

$\forall s \in \mathbb{N}$ und $N \in \{10^{s-1}+1, \ldots, 10^s\}$ gibt es einen Baum $T(N)$ mit Ausgangsgrad ≤ 10 an jedem inneren Knoten und den folgenden Eigenschaften:

1. $T(N)$ hat N Blätter.
2. $T(N)$ hat $\leq \frac{N}{9} + s$ innere Knoten.
3. Alle Pfade von der Wurzel zu einem Blatt haben genau die Länge $s = \lceil \log_{10} N \rceil$ mit $\lceil \log_{10} N \rceil < \frac{1}{3} \log_2 N + 1$.

- Beweis: Induktion über $s \Rightarrow$ Übung

Notation: Invertierender Treiberbaum

- Invertierender Treiberbaum $/F_x$:
  Ersetze den Treiber an der Wurzel durch einen Inverter.

D_n: Dekodierer

- Sei $n \in \mathbb{N}$, $N = 2^n$. Ein n-Bit-Dekodierer D_n ist ein Schaltkreis, der die Funktion $d : \mathbb{B}^n \to \mathbb{B}^N$ berechnet, wobei gilt:

$$d_i(a) = \begin{cases} 1, & \text{falls } \langle a \rangle = i \\ 0, & \text{sonst} \end{cases} \qquad \forall i = 0, \ldots, N-1$$

  ($d_i(a)$ ist Bit i des N-Tupels $d(a)$.)

- Induktive Konstruktion von D_n: Siehe nächste Folie.

Dekodierer: Rekursiver Aufbau

$C(D_1) = 1$

$C(D_n) = C(D_{n-1}) + 2^n + O(2^n)$

AND

SMILE - Dekodierer

Welche Tiefe hat ein n-Bit Dekodierer, der - wie auf der vorhergehenden Folie dargestellt - rekursiv aufgebaut wird?

a. O(1)
b. O(log(n))
c. O(n)
d. Keine der obigen.

SRAM: Lesevorgang ($W = 0$)

- D_n setzt $Y_i = 1$ für $i = \langle A \rangle$, $Y_j = 0$ für $j \neq i$.

- Der Inhalt der i-ten Zelle L_i steht an G_i, für alle $j \neq i$ steht an G_j der Wert 0.

SRAM: Schreibvorgang (Puls auf W)

- D_{in} an D-Eingänge sämtlicher Latches angelegt.
- Schreibpuls nur am W-Eingang von L_i (da $Y_i = 1$).

Tristate-Treiber und Busse

- Tristate-Treiber sind Treiber mit Eingangssignal x und zusätzlichem Signal $/OE$, dem Output-Enable-Signal.

- Am Ausgang y erscheint

$$y = \begin{cases} x, & \text{falls } /OE = 0 \\ Z, & \text{sonst } /OE = 1 \end{cases}$$

- Z bezeichnet den Zustand hoher Impedanz (high-Z).

Zustand hoher Impedanz

- Wir haben bisher Schaltungen betrachtet, die aus CMOS-Gattern bestehen. Dort ist jede Leitung zu jedem Zeitpunkt entweder mit V_{DD} (logisch-1) oder Masse (logisch-0) verbunden.

- Eine Leitung im Zustand Z, also der Ausgang eines Treibers mit $/OE = 1$, ist weder mit V_{DD} noch mit Masse verbunden. Man sagt, der Treiber ist disabled ($/OE = 0$: enabled).

n-Bit-Treiber

- n-Bit-Treiber: n Treiber mit gemeinsamen $/OE$.
- Im Gegensatz zu Ausgängen üblicher Gatter kann man Ausgänge von Tristate-Treibern zusammenschalten. Man muss dafür sorgen, dass zu jeder Zeit höchstens ein Treiber enabled ist.
- Ein n Bit breiter Bus ist ein Bündel aus n Leitungen, welches die Ausgänge von mehreren n-Bit-Treibern verbindet.

Bus vs. Multiplexer

- k Tristate-Treiber, die durch einen Bus verbunden sind, wirken ähnlich wie ein k-fach-Multiplexer.

- Vorteile Bus gegenüber Multiplexer:
  - Leicht erweiterbar.
  - Datentransport in verschiedene Richtungen zu verschiedenen Zeiten.
- Nachteil von Bus:
  - Man muss Bus Contention vermeiden, d.h. es darf nie mehr als ein Treiber auf einem Bus gleichzeitig enabled sein (sonst Folgen bis hin zur physikalischen Zerstörung der Schaltung)!

Bus zur Kommunikation mit SRAM

- SRAM mit gemeinsamem Datenein- und -ausgang.

- Lesezugriff auf den Speicher: $/DOE_1$ enabled, alle anderen Treiber, z.B. $/DOE_2$, disabled.

- Schreibzugriff: D_{in} nimmt den Wert vom Bus, $/DOE_1$ disabled.

Kapitel 4

Sequentielle Logik:

1. Speichernde Elemente
2. Sequentielle Schaltkreise
3. Entwurf sequentieller Schaltkreise
4. SRAM
5. **Anwendung: Datenpfade von ReTI**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Zur Erinnerung: ReTI bisher

Zur Erinnerung: Datenpfade von ReTI

- ReTI besteht aus
  - 4 benutzersichtbaren Registern *PC*, *ACC*, *IN*1, *IN*2
    $\rightarrow$ Realisiert durch Zähler (*PC*) bzw. Register.
  - Einem 2^{32}-Wort-Speicher (Wortbreite von 32 Bit), der Daten und Befehle enthält
    $\rightarrow$ Realisiert durch SRAM.
- ReTI unterstützt Load-/Store-, Compute-, Indexregister- und Sprungbefehle.

31 30	29 ... 24	23 ... 0
Typ	Spezifikation	Parameter *i*

Zur Erinnerung: ReTI-Befehle im Überblick

	31 30	29 28	27 26	25 24	23 … 0
Load	0 1	M	*	D	i

	31 30	29 28	27 26	25 24	23 … 0
Store	1 0	M	S	D	i

	31 30	29	28 27 26	25 24	23 … 0
Compute	0 0	MI	F	D	i

	31 30	29 28 27	26 25 24	23 … 0
Jump	1 1	C	*	i

M - Modus ; S - Source ; D - Destination ; MI - memory/immediate ;
F - Function ; C - Condition

Umsetzung von ReTI: Externe Sicht

- 3-Bus-Architektur zur Ansteuerung von Speicher und I/O-Geräten:
  - 32 Bit breiter Datenbus $D = D[31:0]$,
  - 32 Bit breiter Adressbus $A = A[31:0]$,
  - Kontrollbus C (Breite später festgelegt).

Umsetzung von ReTI: Interne Sicht

- *CPU* besteht aus:
  - Zähler *PC*.
  - 3 für Benutzer sichtbaren Registern *ACC*, *IN*1, *IN*2,
  - Instruktionsregister *I*,
  - *ALU*,
  - *CPU*-internen Bussen:
    - *L*, *R* für linken bzw. rechten Operanden der *ALU*,
    - internem Datenbus *DI*.
- Register, *PC*, *ALU*, Busse und die zugehörigen Treiber sind 32 Bit breit.

Interner Aufbau der ReTI-CPU

Load I Acc ↓

SMILE - ReTI, interner Aufbau/Befehlstypen

Bisher haben wir Compute-Befehle nur über den Akkumulator (ACC) definiert.
Ist es mit dem internen Aufbau der ReTI - wie auf der vorherigen Folie dargestellt - möglich, die Compute-Befehle auch auf die Register PC, IN1 und IN2 zu erweitern?

a. Ja, aber nur für den PC.
b. Ja, aber nur für IN1 und IN2.
c. Ja, für alle 3.
d. Nein.

Hinweise zum Schaltbild

- Namenskonvention für Treiber: Treiber zwischen Bus/Baustein *X* und Bus/Baustein *Y*: *XYd*;
  - Output-Enable-Signal: *XYdoe*.
  - *0Ld* und *0Rd* können 0^{32} auf *L* bzw. *R* legen.

- Busse *A* und *D* sind an den Speicher (sowie I/O-Geräte) angeschlossen, s. nächste Folie.
- Das Bild enthält keine Steuerleitungen:
  - Output-Enable-Signale der Treiber,
  - Funktionsauswahl der ALU,
  - Clock-Signale und “Clock-Enable-Signale” der Register.

Speicher SM von ReTI

- Datenein- und ausgänge mit Datenbus *D* der *CPU* verbunden.
- Adressleitungen mit Adressbus *A* der *CPU* verbunden.
- Treiber *ASMd* immer enabled.

Verfeinerung des Schaltbilds

Verarbeitung der Daten im Register I

- Im Instruktionsregister I steht der gerade verarbeitete Befehl.
  - $I[31:24]$: Befehlskodierung (für die im Schaltbild nicht dargestellten Steuersignale benötigt).
  - $I[23:0]$: Speicheradresse oder Konstante für die ALU.
    - Speicheradresse wird mit acht Nullen aufgefüllt. $0^8 I[23:0]$ wird auf Bus A gelegt (IAd enabled).
    - Natürliche 24-Bit-Konstante wird mit acht Nullen aufgefüllt. $0^8 I[23:0]$ wird auf R gelegt (IRd enabled).
    - Ganzzahlige 24-Bit-Konstante wird vorzeichenerweitert. $sext(I[23:0])$ wird auf R gelegt (IRd enabled).

Verfeinerung

- Neues Kontrollsignal sext:
  - $sext = 0$: Ersetze $I[31:0]$ durch $0^8 I[23:0]$.
  - $sext = 1$: Ersetze $I[31:0]$ durch $sext(I[23:0])$.

Weitere Verfeinerung für Register (1/3)

- Im Buch von Keller / Paul werden die Clockeingänge aller Register Reg mit einem Clocksignal Regck verbunden, das durch die Kontrolllogik berechnet wird.
- $\Rightarrow$ Datenübernahme zu ausgewählten Zeitpunkten

- Vorgehen bei Realisierung der ReTI auf einer Platine mit diskreten Bausteinen ok!
- Nicht ok bei heutigen Designs, die Prozessoren auf einem einzigen Chip integrieren.

Weitere Verfeinerung für Register (2/3)

- Gründe für “Designrule”, die es verbietet, Clockeingänge mit berechneten Datensignalen zu verbinden:
  - Spezielle Methoden (“Clock–Tree–Synthese”) gewährleisten, dass die steigende Flanke der globalen Clock an allen Clockeingängen zum gleichen Zeitpunkt ankommt (z.B. durch Ausgleich des Effekts unterschiedlicher Leitungsverzögerungen m.H. von Treibern). Datensignale auf Clockeingängen verhindern Clock–Tree–Synthese.
  - Heutige Werkzeuge zur automatischen Timing–Analyse (und Berechnung der maximalen Clockfrequenz) sind nicht in der Lage, mit berechneten Clocksignalen umzugehen.
  - Spezielle Anforderungen an “Flankensteilheit” der Clocksignale (siehe Kapitel über physikalische Eigenschaften)

Weitere Verfeinerung für Register (3/3)

- Transformation bzw. Verfeinerung:

Programmabarbeitung durch ReTI

- Zwei sich abwechselnde Phasen der *CPU*:
  - Fetch-Phase: Lädt nächsten auszuführenden Befehl aus Memory ins Instruktionsregister *I* der *CPU*.
  - Execute-Phase: Befehl, der in *I* steht, wird ausgeführt.
- Vorgehen:
  1. Definition der Datenpfade, d.h. der benötigten Datenverbindungen zwischen den Komponenten der *CPU*.
  2. Herleitung der Kontrollsignale zur Ansteuerung der im Punkt 1 hergeleiteten Datenpfade.
     - Treiber-OE, *ALU*-Funktionsselektion, Register-Clock.
  3. Sequentielle Synthese.

Datenpfade: Fetch-Phase

SMILE - Fetch-Phase, Treiber

Welche Treiber müssen in der Fetch-Phase enabled sein?

a. ALUAd
b. ASMd
c. DDId
d. IAd
e. IRd
f. PCAd
g. PCLd

Datenpfade: Fetch-Phase

Bedeutung des Diagramms

- In der Fetch-Phase muss:
  - Bus *A* mit *PC* verbunden sein, d.h. *PCAd* enabled.
  - Register *I* den Wert von Bus *D* übernehmen, d.h. *Icken* muss enabled werden.
  - Alle anderen Treiber (außer denen, die stets enabled sind) sind disabled, um Bus Contentions zu vermeiden.
- Die Steuersignale müssen in der Fetch-Phase entsprechend gesetzt sein.
  - Z.B. $/PCAdoe = 0$, $/ALUAdoe = 1$, usw. (active low!)

Fetch: Die durchgeschalteten Pfade

Datenpfade in der Execute-Phase

- Betrachte unterschiedliche Befehlstypen.
  - *Compute Immediate*,
  - *Compute Memory*,
  - *JUMP*,
  - *LOAD*,
  - *LOADIN*1 (*LOADIN*2 analog),
  - *LOADI*,
  - *STORE*,
  - *STOREIN*1, (Store IN2)
  - *MOVE*.

Datenpfade: *Compute Immediate* (1/2)

ADD I ACC <v>

Datenpfade: *Compute Immediate* (2/2)

Datenpfade: *Compute Memory* (1/2)

Datenpfade: *Compute Memory* (2/2)

Datenpfade: *JUMP* (1/2)

Datenpfade: *JUMP* (2/2)

Datenpfade: *LOAD i* (1/2)

Datenpfade: *LOAD i* (2/2)

Datenpfade: *LOADIN*1 *i* (1/2)

Datenpfade: *LOADIN*1 *i* (2/2)

Datenpfade: *LOADI i* (1/2)

Datenpfade: *LOADI i* (2/2)

Datenpfade: *STORE i* (1/2)

Datenpfade: *STORE i* (2/2)

Datenpfade: *STOREIN*1 *i* (1/2)

Datenpfade: *STOREIN1 i* (2/2)

Datenpfade: *MOVE ACC IN1* (1/2)

Datenpfade: *MOVE ACC IN*1 (2/2)

Zusätzliche Befehle

- Man kann weitere Befehle ohne zusätzliche Hardware realisieren!
- Load- und Compute-Befehle mit beliebigem Zielregister $r \in \{PC, IN1, IN2, ACC\}$.
  - Kein $\langle PC \rangle := \langle PC \rangle + 1$, wenn $r = PC$.
- Befehlsformat: *LOAD r i*; *ADD r i*; etc.
- Befehlskodierung:

	31 30	29 28	27 26	25 24	23 . . . 0
Load	0 1	M	*	**D**	i

	31 30	29	28 27 26	25 24	23 . . . 0
Compute	0 0	MI	F	**D**	i

Zur Illustration: ReTI-Simulator „Neumi”

- Verfügbar in Ilias (Zusatzmaterial)
  - Simulator der ReTI-Maschine.
  - Anleitungen und zwei Beispielprogramme.
- Für die Ausführung wird Java benötigt.
  - Für Windows: `http://www.java.com/de/download/manual.jsp`
  - Für Linux: Nicht den GNU-, sondern den SUN-Compiler verwenden (Neumi funktioniert nicht mit GCJ).
  - Für Solaris und MacOS sollte die richtige Java-Version vorliegen.
- Syntax geringfügig gegenüber Vorlesung abgewandelt.
  - Kommas zwischen Operanden: „ADDI ACC, 1” statt „ADDI ACC 1”.
  - Jump-Befehle anders geschrieben: „JUMP ge, 2” statt „JUMP$_{\geq}$ 2”.
  - Details: Anleitungen auf der Webseite.

Implementierung von ReTI (1/2)

- Im Buch von Keller/Paul wird ReTI (bzw. ReSa) mit sogenannten diskreten FAST-Bausteinen realisiert.
  - Register, Zähler, ALU, Treiber, Speicher: Bausteine aus der FAST-Bibliothek, teilweise mehrere Bausteine, um Bitbreite 32 zu erreichen.
  - Kontrollsignale werden durch sog. PALs realisiert
    - Programmable Array Logic (Bausteine von AMD).
    - Spezielle Beschreibungssprache PALASM.
    - PALs werden heute nur noch selten verwendet.

Implementierung von ReTI (2/2)

- Im Gegensatz dazu verwenden wir State-of-the-Art-Bausteine der NanGate-Bibliothek (`http://www.si2.org/openeda.si2.org/projects/nangatelib`) im Hinblick auf eine VLSI–Implementierung auf einem einzigen Chip.
- Auf Basis einer solchen Implementierung behandeln wir später wesentliche Konzepte für eine „Timing-Analyse". Wir beginnen zunächst mit der Realisierung der Kontrollsignale (Output–Enable, Clock–Enable ...).
- Kontrollsignale werden durch einen Endlichen Automaten generiert. Wir skizzieren hier das Vorgehen.

Zu generierende Kontrollsignale

- Clock–Enable–Signale für alle Register r, Bez.: $rcken$.
- Output enable Signale (active low) für alle Treiber XYd, Bez.: $/XYdoe$.
- Funktions-Select-Signale $f[2:0]$ zum Selektieren der Funktion, die von ALU ausgeführt wird.
- Signale $/PCclear$, $/PCload$ für PC.
- $sext$ zur Berechnung der Füllbits bei 24-Bit-Immediate-Konstanten.
- Für den Speicher benötigen wir die Kontrollsignale (active low) $/SMDdoe$, $/SMw$.

Idealisierte Timing-Diagramme

- Grobe Ablaufplanung mit idealisierten Timing-Diagrammen.
- Vereinfachende Annahme: Verzögerungszeit aller Bausteine = 0 (exakte Analyse mit Verzögerungszeiten später).
- Befehlsabarbeitung ist unterteilt in Takte (= Folge von Taktsignalen *high*, *low*).
- Fragen:
  - Wie sollen Kontrollsignale zusammenspielen? /
  - In welchem Takt sollen welche Treiber aktiviert, welche Registerclock enabled werden?

Befehlsabarbeitung in Takten

- Sowohl Fetch- als auch Execute-Phase bestehen aus 4 Takten gleicher Länge.
- Kontrollsignal:
  - $E = 0$: Fetch-Phase,
  - $E = 1$: Execute-Phase.

- Signale s_0, s_1 = Binärkodierung der Nummer des Taktes (innerhalb Fetch, Execute), in dem ReTI sich befindet.
- Steigende Flanken (Anfang des Taktes) werden mit P_i, fallende (Mitte des Taktes) mit N_i bezeichnet ($i = 0, \ldots, 3$).
- Clock ck, Signale s_0, s_1 und E werden Phasensignale genannt. Weitere (Kontroll-)Signale werden aus den Phasensignalen erzeugt.

Erzeugung der Phasensignale

3-Bit-Zähler, zählt bei jeder positiven Flanke von ck um 1 hoch.

Idealisiertes Timing-Diagramm

$/SMDdoe = \neg s_0 \wedge \neg s_1$

SMILE - Kontrollsignale

Welche der folgenden Funktionen realisiert das Signal /SMDdoe, wie es bei der Ausführung eines entsprechenden Befehls gebraucht wird?

a. $(E \cdot (s0 + s1)')$

b. $s0' \cdot s1'$

c. $s0 + s1$

d. Keine der obigen

Zur Erinnerung: Datenpfade

Entwurfsziele

- Nutze Busse möglichst lange (unter Vermeidung von Bus Contention).
- Clock-Enable-Signale der Register möglichst spät
  $\rightarrow$ viel Zeit für Berechnung neuer Daten.
- Nach dem Entwurfsende muss das Timing der *CPU* mit den konkreten Werten der eingesetzten Fertigungstechnologie überprüft werden. (“Wie schnell kann man maximal takten, um korrektes Funktionieren zu garantieren?”)
  - Siehe nächstes Kapitel.

Aufbau der Kontrolllogik (1/2)

- Die eigentliche Kontrollogik wird realisiert durch einen Endlichen Automaten.
- Die Kontrollsignale sind als Ausgangssignale des Endlichen Automaten implementiert.
- Ist ein Kontrollsignal *active low*, dann bezeichnen wir es z.B. mit $/x$. Das Ausgangssignal $/x$ ergibt sich dann durch Negation des Ausgangssignals x eines entsprechenden FFs mit Eingangssignal x_{pre}.
- Ist ein Kontrollsignal *active high*, dann bezeichnen wir es z.B. mit x. Das Ausgangssignal x entspricht dem Ausgangssignal eines FFs mit Eingangssignal x_{pre}.

Aufbau der Kontrolllogik (2/2)

Berechnung von *lcken* als erstes Beispiel (1/2)

Berechnung von *Icken* als erstes Beispiel (2/2)

- $Icken_{pre}$ hat steigende Flanke bei $P1$, fallende bei $P2$ von Fetch.
- Realisierung: $Ick_{pre} = \overline{E} \cdot \overline{s_1} \cdot s_0$.

$S_0 = 1$
$S_1 = 0$
$E = 0$

Berechnung von *ACCcken*, *IN1cken*, *IN2cken*, *PCcken*

- Analog, unter Berücksichtigung der Tatsache, dass Register nur bei bestimmten Befehlen neu beschrieben werden dürfen

Berechnung von *ACCcken* als Beispiel (1/3)

Berechnung von *ACCcken* als Beispiel (2/3)

- $ACCcken_{pre}$ hat steigende Flanke bei $P1$, fallende bei $P2$ von Execute.
- Aber nur bei folgenden Befehlen:
  - Compute mit $D = ACC$
  - Load mit $D = ACC$
  - Move mit $D = ACC$

- Compute: $\overline{I_{31}} \cdot \overline{I_{30}}$
- Load: $\overline{I_{31}} \cdot I_{30}$
- Move: $I_{31} \cdot \overline{I_{30}} \cdot I_{29} \cdot I_{28}$
- $D = ACC$: $I_{25} \cdot I_{24}$

Kodierung S, D

S, D	**Register**
0 0	PC
0 1	IN1
1 0	IN2
1 1	ACC

Berechnung von *ACCcken* als Beispiel (3/3)

$$ACCcken_{pre} = \underline{E \cdot \overline{s_1} \cdot s_0 \cdot} \quad \text{// P1 von execute}$$

$$I_{25} \cdot I_{24} \cdot \quad \text{// } D = ACC$$

$$\left(\underbrace{\overline{I_{31}} \cdot \overline{I_{30}}}_{\text{Comp.}} + \underbrace{\overline{I_{31}} \cdot I_{30}}_{\text{Load}} + \underbrace{I_{31} \cdot \overline{I_{30}} \cdot I_{29} \cdot I_{28}}_{\text{Move}} \right) \quad \text{// Compute, Load oder Move}$$

Datenpfade und Treiber auf *L* und *R*

Idealisiertes Timingdiagramm

Treiber auf Bussen L und R

- $0Ld, PCLd, IN1Ld, IN2Ld, ACCLd, 0Rd, IRd, DRd$.
- Enabled in der ganzen Execute-Phase.
- Beispiel für Realisierung: $/PCLdoe$.
  - Enabled für
    - JUMP ($I[31:30] = 11$)
    - Compute-Befehle ($I[31:30] = 00$) mit $D = PC$ ($I[25:24] = 00$)
    - MOVE ($I[31:28] = 1011$) mit $S = PC$ ($I[27:26] = 00$).

Berechnung von /*PCLdoe* (1/2)

- *PCLdoe*$_{pre}$ hat steigende Flanke bei *P*3 von Fetch.

Zeitpunkt für ersten Takt, in dem $PCLdoe_{pre} = 1$ ist:

$S_0 \wedge S_1 \wedge \neg E$

Berechnung von $/PCLdoe$ (2/2)

$$
\begin{aligned}
PCLdoe_{pre} = \; & \Big(\overline{E} \cdot s_1 \cdot s_0 \cdot && \text{// P3 von fetch} \\
& \big[I_{31} \cdot I_{30} + && \text{// JUMP} \\
& \overline{I_{31}} \cdot \overline{I_{30}} \cdot \overline{I_{25}} \cdot \overline{I_{24}} && \text{// Compute mit } D = PC \\
& I_{31} \cdot \overline{I_{30}} \cdot I_{29} \cdot I_{28} \cdot \overline{I_{27}} \cdot \overline{I_{26}} \big] \Big) && \text{// MOVE mit } S = PC \\
& + PCLdoe \cdot E \cdot \overline{s_1} \cdot \overline{s_0} && \text{// Halten in Takt 0 von execute} \\
& + PCLdoe \cdot E \cdot \overline{s_1} \cdot s_0 && \text{// Halten in Takt 1 von execute} \\
& + PCLdoe \cdot E \cdot s_1 \cdot \overline{s_0} && \text{// Halten in Takt 2 von execute}
\end{aligned}
$$

- Output-Enable-Signale für andere Treiber auf L und R analog.

Datenpfade und Treiber auf Adressbus

Treiber auf Adressbus

- *PCAd*: enabled (unabhängig vom Befehl) bei *N*0 der Fetch-Phase, disabled bei *N*3 der Fetch-Phase.
- *IAd*, *ALUAd*: enabled bei *N*0, disabled bei *N*3 von Execute (aber nicht bei allen Befehlen).
- Die D-FFs zu Output-Enable-Signalen auf dem Adressbus werden mit der invertierten Clock getaktet (Verschiebung um einen halben Takt!)

Idealisiertes Timingdiagramm

Weitere Kontrollsignale

- Treiber auf *D*, *DI*
- Signale */PCload*, */PCclear*
- Speicheransteuerung: s. nächste Folie.
- Kontrolle der ALU und Sign–Extension:
  - Funktions-Select-Signale f[2:0] der ALU
  - Eingangsübertrag c_{in}
  - sext und fill
  - All diese Signale werden durch den kombinatorischen Schaltkreis (ohne zusätzliche FFs) berechnet.

Idealisiertes Timing-Diagramm

Speicheransteuerung

- Output-Enable */SMDdoe* für SMDd (Treiber am Speicherausgang) aktiviert von P1 bis P0 bei Leseoperationen, d.h. bei
  - Fetch
  - Compute Memory
  - LOAD, LOADINj
- Schreibsignal für Speicher */SMw* (memory write) aktiviert von P2 bis P3 von execute bei Schreiboperationen, d.h. bei
  - STORE, STOREINj

Zusammenfassung Sequentielle Logik

- Sequentielle Schaltkreise bestehen aus speichernden Elementen (Latches, Flipflops) und einem kombinatorischen Kern.
- Sie implementieren endliche Zustandsautomaten.
- Der Entwurf eines sequentiellen Schaltkreises besteht aus der Aufstellung des Zustandsdiagramms, der Zustandsminimierung, der Zustandskodierung und der Synthese der kombinatorischen Logik.
- Nun war es uns möglich, den Entwurf von ReTI zu vervollständigen (exakte Timing-Analyse folgt).

Kapitel 5

Timing:

1. **Physikalische Eigenschaften**
2. Timing wichtiger Komponenten
3. Exaktes Timing von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Wiederholung: Übergang beim RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).
- Nach Zeit $t_{P/SQ}$ ist $Q = 1$. Nach Zeit $t_{P/S/Q}$ ist $/Q = 0$.
- „Gatter brauchen Zeit zum Schalten!" Aber wie lange ist $t_{P/SQ}$, $t_{P/S/Q}$? Oder wie lange muss ein Puls mindestens dauern? (= Pulsweite).

Wiederholung: Timing-Diagramm D-LATCH

- Wie lange müssen die einzelnen Signale aktiv sein, damit der Schreibvorgang reibungslos abläuft?
- D. h. Wie lange ist Setup–Zeit t_{SDW}, Hold–Zeit $t_{\cancel{HDW}}$, Pulsweite y?

t_{HWD}

Physikalische Signale ↔ Logische Signale

$$I(U) = \begin{cases} 0, & \text{falls } U \leq V_L \\ 1, & \text{falls } U \geq V_H \\ \text{undef.}, & \text{sonst} \end{cases}$$

- In jeder Technologie gibt es eine Versorgunsspannung VCC (z.B. 1.1 V bei NanGate).
- Eine Spannung $U \in [0, VCC]$ wird als logischer Wert $I(U)$ interpretiert.
  - Am Eingang (Input) eines Gatters: V_{IL}, V_{IH}.
  - Am Ausgang (Output) eines Gatters: V_{OL}, V_{OH}.
- $V_{IL}, V_{IH}, V_{OL}, V_{OH}$ eines Bausteins sind gegeben.

SMILE – Physikalische Signale

Unter welchen Bedingungen laufen die Schaltvorgänge be
untenstehehenden Schaltung reibungslos ab?

$V_{OL} \leq V_{IL}$

$V_{OH} \geq V_{IH}$

SMILE – Physikalische Signale

Unter welchen Bedingungen laufen die Schaltvorgänge bei der untenstehehenden Schaltung reibungslos ab?

$\Rightarrow$ Fazit: Es sollte $V_{OL}(u) \leq V_{IL}(v)$ und $V_{OH}(u) \geq V_{IH}(v)$ gelten.

Zusammenschalten von Gattern

- Will man den Ausgang eines Gatters u mit dem Eingang eines Gatters v verbinden, dann sollte gelten:
  - $V_{OL}(u) \leq V_{IL}(v)$ und
  - $V_{OH}(u) \geq V_{IH}(v)$.
- Sonst werden Signale falsch interpretiert.

Beispiel: NanGate

$V_{IL} = 30\% \cdot VCC = 0.33\ V$
$V_{IH} = 70\% \cdot VCC = 0.77\ V$

Entsprechend Output-Pegel V_{OL}, V_{OH}.

Verzögerung

Beispiel-Spannungsverlauf $x(t)$, $y(t)$

$x(t)$

Zwei Beispiele für $y(t)$

Allgemeine Bemerkung zu Verzögerungszeiten

- Im Allgemeinen gilt nicht $y(t) = x(t - t_p)$, so dass man nicht einfach t_p als Verzögerungszeit definieren kann.
  $y(t)$ wird verformt.

- Die Verzögerungszeit (Propagation Delay) wird definiert als $t_p := (t_2 - t_1)$ bezüglich einer festen „Referenzspannung" M mit $V_L < M < V_H$
  (Bsp.: $M = 0.5VCC = 0.55\ V$ bei NanGate).

- Bestimme t_1, t_2 mit $x(t_1) = y(t_2) = M$.

Angaben zur Verzögerungszeit

- In der Regel gibt es verschiedene Verzögerungszeiten für Übergänge am Ausgang:
  - t_{PLH}: Verzögerungszeit bei $0 \rightarrow 1$.
  - t_{PHL}: Verzögerungszeit bei $1 \rightarrow 0$.

Modellierung der Verzögerungszeit

- **Problem** bei der Modellierung der Verzögerungszeit bezüglich fester Spannung M:
  - Keine Aussage darüber, wann logische Signale 0 oder 1 sind, d. h. physikalische Signale unterhalb V_{OL} oder oberhalb V_{OH} sind.

Illustration des Problems

→ Ähnliches Problem am Gattereingang.

Anstiegs- und Abfallzeiten

- Für jedes Signal braucht man also zusätzliche Informationen über:
  - Anstiegszeit (Rise Time) =
    Zeit, in der Signal von V_L nach V_H steigt.
  - Abfallzeit (Fall Time) =
    Zeit, in der Signal von V_H nach V_L fällt.
  - Bzw. noch genauer würde man eigentlich benötigen:
    - Anstiegszeit von M nach V_H
    - Abfallzeit von M nach V_L

Beschränkung dieser Zeiten

$t_{yH} - t_{xL} \leq \delta + t_{pLH} + \delta$

- Die in unseren Analysen verwendeten Gatter haben die folgende angenehme Eigenschaft:
- $\exists \delta$ mit folgender Eigenschaft:

  Falls rise/fall time $\leq \delta$ am Gattereinang,
  dann rise/fall time $\leq \delta$ am Gatterausgang.

Beispiel: NanGate

- $V_{IL} = 30\% \cdot VCC = 0.33$ V
  $V_{IH} = 70\% \cdot VCC = 0.77$ V
- NanGate für $M = 0.55$ V spezifiziert.
  Bausteine $NAND, NOT, AND, OR, EXOR$.
- t_p zwischen 0.00 ns und 0.21 ns.
- $\delta = 0.13$ ns (1 ns = 10^{-9} s)
- Die Zeiten, an denen die entsprechenden Signale wohldefinierte logische Werte 0, 1 annehmen, unterscheiden sich von denen für M um höchstens δ.

Bemerkung

- Eine rise/fall time $\leq \delta$ an den primären Eingängen einer Schaltung kann man garantieren, wenn man den Schaltvorgang zur Zeit t_0 beginnt und spätestens zur Zeit $t_0 + \delta$ abschließt.

SMILE – Verzögerungszeit

Nach welcher Zeit ist der Schaltvorgang bei Y_n von 0 nach 1 spätestens abgeschlossen, nachdem der Schaltvorgang von 0 nach 1 bei x angefangen hat?

a. $n \cdot (t_{PLH} + \delta)$

b. $t_{PLH} + n\delta$

c. $n \cdot t_{PLH} + 2\delta$

d. $n \cdot t_{PLH} + \frac{n}{n-1}\delta$

Analyse der Verzögerungszeit einer Kette von n Gattern (2/3)

Analyse der Verzögerungszeit einer Kette von n Gattern (3/3)

- Durchläuft $X(t)$ nach Zeit $m(0)$ die Spannung M, dann durchläuft $Y_n(t)$ die Spannung M nach $m(0) + n \cdot t_{PLH}$.
- Falls $X(t)$ mit Anstiegszeit $\leq \delta$, dann auch $Y_1(t), \ldots, Y_n(t)$.
- Also ist Y_n auf jeden Fall zur Zeit $m(0) + n \cdot t_{PLH} + \delta$ logisch 1.
- Beginnt man im Beispiel den Schaltvorgang bei t_0 und beendet ihn bei $t_0 + \delta$, dann gilt $m(0) \leq t_0 + \delta$ und Y_n ist spätestens nach $t_0 + n \cdot t_{PLH} + 2\delta$ logisch 1.

Vereinbarungen

- Im Folgenden soll

  Signal X wird zum Zeitpunkt t_1 abgesenkt/angehoben

  bedeuten

  X wird abgesenkt/angehoben mit $X(t_1) = M$.

- Desweiteren sind alle Zeitangaben in *ns*.

Einfluss auf Verzögerungszeiten

- Verzögerungszeiten von Gattern sind nicht konstant, sondern werden beeinflusst durch:
  - Betriebstemperatur
  - Fertigungsprozess des Chips
  - kapazitive Last am Gatterausgang (Fanout) (Gattereingänge, die mit einem Gatterausgang verbunden sind, verhalten sich wie Kondensatoren, d. h. sie werden beim Schalten ge- bzw. entladen.)

Worst-case Timing-Analyse

- Wegen Abhängigkeit der Verzögerungszeit von Temperatur, Fertigungsprozess und Fanout werden vom Hersteller keine festen Zeiten t_{PLH}/t_{PHL} angegeben, sondern 3 Werte:
  - t^{min} = untere Schranke
  - t^{max} = obere Schranke
  - t^{typ} = *typischer* Wert (???)

min, *max* und *typ* (1/2)

- Für die tatsächliche Verzögerungszeit t_p gilt:

$$t^{min} \leq t_p \leq t^{max}$$

- Wir nehmen in den folgenden Analysen an, dass t_p im Intervall $[t^{min}, t^{max}]$ liegt, falls
  - die Temperatur im Bereich T liegt („kommerzieller Temperaturbereich“ 0 – 70 °C, „militärischer Temperaturbereich“ −55 – 125 °C)
  - und eine bestimmte kapazitive Last C_0 nicht überschritten wird.

- C_0 wird so gewählt, dass mit Einhalten einer Fanoutbeschränkung von 10 C_0 auf keinen Fall überschritten wird.

min, *max* und *typ* (2/2)

- Für t^{typ} gilt ebenfalls $t^{min} \leq t^{typ} \leq t^{max}$.
- Beim Rechnen mit t^{typ} macht man aber einen *Fehler mit unbekannter Größe*.

→ Kein Rechnen mit t^{typ}, sondern mit Intervallen $[t^{min}, t^{max}]$.

$[a+c, b+d]$

Exkurs: Rechnen mit Intervallarithmetik (1/2)

Definition

Ein Intervall $[a,b] := \{x \in \mathbb{R} \mid a \leq x \leq b\} \subset \mathbb{R}$ auf $\mathbb{R}$ ist eine zusammenhängende und abgeschlossene Teilmenge von $\mathbb{R}$. Man bezeichnet es auch als das abgeschlossene Intervall von a bis b.

- Wir betrachten hier nur die Menge der abgeschlossenen Intervalle IR auf $\mathbb{R}$.
- Es gilt:
  - $\min[a,b] = a$
  - $\max[a,b] = b$
  - $a \in \mathbb{R} \simeq [a,a] \in \mathrm{IR}$
    (eine reelle Zahl a kann aufgefasst werden als das Punktintervall von a bis a)

$(a,b]$ $a < x \leq b$

Exkurs: Rechnen mit Intervallarithmetik (2/2)

Definition

Gegeben ein Operator $_{op} \in \{+,-,\cdot\}$ in $\mathbb{R}$. Der dazugehörige Operator $\circledcirc_{op}$ auf IR ist definiert als:
Für $a,b,c,d \in \mathbb{R}$:
$[a,b] \circledcirc_{op} [c,d] := \{x \ _{op} \ y \mid x \in [a,b], y \in [c,d]\}$

Beispiele:

$[2,3] \oplus [0,5] = [2,8]$

$[2,3] \ominus [0,5] = [-3,3]$

- $[a,b] \oplus [c,d] = [\underline{a+c}, \underline{b+d}]$
- $[a,b] \ominus [c,d] = [a-d, b-c]$
- $[a,b] \odot [c,d] = [\min(\underline{a \cdot c}, \underline{a \cdot d}, \underline{b \cdot c}, \underline{b \cdot d}), \max(a \cdot c, a \cdot d, b \cdot c, b \cdot d)]$

Bemerkungen

- Wir schreiben vereinfachend nur $_{op}$ statt $\textcircled{op}$.
- Für unsere Belange sind ausschließlich $+$, $-$ und $\cdot$ Operator von Bedeutung. ($\cdot$ mit Punktinvervallen)
- Ein Intervall bezeichnen wir mit $\tau = [t^{min}, t^{max}]$.

Beispiel: AND-Gatter

AND

$\tau_{PLH} = [0.02, 0.12]$

$\tau_{PHL} = [0.02, 0.12]$

Bzw.:

AND	$t^{\min}$	$t^{\max}$
τ_{PLH}	0.02	0.12
τ_{PHL}	0.02	0.12

Fall 1

AND	$t^{\min}$	$t^{\max}$
τ_{PLH}	0.02	0.12
τ_{PHL}	0.02	0.12

- A, E fest auf 1.
- B von 0 auf 1 zum Zeitpunkt t_0.

→ Änderung von C zur Zeit

$$\begin{aligned}\tau_1 &= t_0 + \tau_{PLH}\,(\text{AND})\\ &= t_0 + [0.02, 0.12]\end{aligned}$$

→ Änderung von D zur Zeit

$$\begin{aligned}\tau_2 &= \tau_1 + \tau_{PLH}\,(\text{AND})\\ &= t_0 + 2 \cdot \tau_{PLH}\,(\text{AND})\\ &= t_0 + 2 \cdot [0.02, 0.12]\\ &= t_0 + [0.04, 0.24]\end{aligned}$$

Fall 1 - Timing-Diagramm

Fall 2

- A, B, E können sich zum Zeitpunkt t_0 ändern, sind vorher und nachher stabil.
- Es ist unbekannt, wieviele Signale sich ändern und wie sie sich ändern.

→ Gröbere Abschätzungen

Gröbere Abschätzung

- Bestimmung von Zeitintervallen, zu denen Gatter überhaupt schalten können.
- Beispiel:

$\tau_{PLH} = [t_{PLH}^{min}, t_{PLH}^{max}]$
$\tau_{PHL} = [t_{PHL}^{min}, t_{PHL}^{max}]$

u ist beliebiges Gatter oder eine Schaltung.

- Gesucht ist ein Intervall τ_p in dem die Verzögerungsintervalle aller möglichen Schaltvorgänge enthalten sind.
- Definiere
$$t_p^{min} := min(t_{PLH}^{min}, t_{PHL}^{min})$$
$$t_p^{max} := max(t_{PLH}^{max}, t_{PHL}^{max})$$
- Dann ist $\tau_p := [t_p^{min}, t_p^{max}]$ das gesuchte Intervall.

SMILE – Timing Abschätzung

In welchem Intervall $\tau_p(S)$ kann S schalten?

$$\tau_p(u) = [a_1, b_1]$$
$$\tau_p(v) = [a_2, b_2]$$
$$\tau_p(w) = [a_3, b_3]$$

$a : t_0 + [a_1, b_1]$

$b : t_0 + [a_2, b_2]$

$[\min(a_1, a_2), \max(b_1, b_2)] + [a_3, b_3]$

Fall 2

AND	$t^{\min}$	$t^{\max}$
τ_{PLH}	0.02	0.12
τ_{PHL}	0.02	0.12

- Wenn die Gatter schalten, dann in folgenden Intervallen:
  - A, B, E: $t_0 + [0.0, 0.0]$
  - C: $t_0 + [0.02, 0.12]$
  - D: $t_0 + [0.0, 0.12] + [0.02, 0.12] = t_0 + [0.02, 0.24]$

Fall 2 - Timing-Diagramm

Interpretation des Timing-Diagramms

- Was kann im grauen Bereich passieren?
- **Beispiel**:
  t_0: $\underline{A, B, E}$ $110 \rightarrow 101$

- **Annahme**:
  AND-Gatter haben folgende Verzögerungszeiten.
- 1. AND-Gatter: $t_{PLH} = 0.12$, $t_{PHL} = 0.12$
  2. AND-Gatter: $t_{PLH} = 0.02$, $t_{PHL} = 0.02$

$t_{PLH}^{AND} = [0.02, 0.12]$

Timing-Diagramm zum Beispiel

110 → 101

1. AND: $t_{PLH} = 0.12$ $t_{PHL} = 0.12$
2. AND: $t_{PLH} = 0.02$ $t_{PHL} = 0.02$

Spikefreies Umschalten von Gattern

- **Ziel**:
  Übergang von $A = 1, B = 0$ zu $A = 0, B = 1$, ohne Spike am Ausgang.

- **Bemerkung**:
  Der Übergang $(0,1) \rightarrow (1,0)$ bzw. umgekehrt ist der einzige, bei dem an *AND*/*NAND*-Gattern ein Spike auftreten kann.

AND-Gatter

wähle sicheren Abstand

t_0 $\quad$ $t_1 = t_0 + \underbrace{0.12}_{t_{pHL}} + \delta$ $\quad$ $t_2 = t_1 + \delta$

Sicherer Abstand für Senken von A und Anheben von B

Lemma

Man kann zeigen, dass Übergänge für A und B mit

$$0.12\,\text{ns} + 2\delta = 0.38\,\text{ns}$$

sicher sind, d. h. keine Spikes am Ausgang entstehen können.

Zum Beweis - Timing im Gatter

1. Senke A bei $t_0 = 0$.
   - $\rightarrow$ $C = 0$ wegen $A = 0$ spätestens bei $t_1 = t_0 + 0.12 + \delta$
   - Grund:
     - Bei tatsächlichem Schalten von $C = 0$ wegen $A = 0$ würde das Signal spätestens nach $t_{PHL}^{max} = 0.12$ ns den Wert M durchlaufen und wäre 0 spätestens nach $0.12 + \delta$ ns.
     - Interner Umschaltvorgang „$C = 0$ wegen $A = 0$" muss also spätestens nach $0.12 + \delta$ ns beendet sein.
2. Hebe B (bzgl. M!) zum Zeitpunkt $t_2 = t_1 + \delta$.
   - $\rightarrow$ Zum Zeitpunkt t_1 gilt auf jeden Fall noch $B = 0$.

- Also:
  Vor t_1: $B = 0 \Rightarrow C = 0$
  Nach t_1: $A = 0 \Rightarrow C = 0$

$\rightarrow$ Übergänge für A und B mit Abstand $t_2 - t_0 = 0.12 + 2\delta = 0.38 \quad (\delta = 0.13)$.

AND	t^{min}	t^{max}
τ_{PLH}	0.02	0.12
τ_{PHL}	0.02	0.12

Regel für spikefreies Umschalten

- Wähle den Abstand für die Signaländerungen am Eingang eines Gattes so, dass
  - die maximiale Verzögerung des ersten Schaltvorganges *und*
  - $2\times$ die rise-/fall-time (δ)

  zwischen den beiden Schaltvorgängen am Eingang liegt.

$\delta = 0.13$

- Beispiel: NAND

NAND	$t^{\min}$	$t^{\max}$
τ_{PLH}	0.02	0.15
τ_{PHL}	0.02	0.12

- Kritischer Übergang: Zuerst $A : 1 \rightarrow 0$, dann $B : 0 \rightarrow 1$.
- Daraus ergibt sich der Abstand $\max(\tau_{PLH}) + 2\delta = 0.41$

$0.15 + 2 \cdot 0.13 =$

Kapitel 5

Timing:

1. Physikalische Eigenschaften
2. **Timing wichtiger Komponenten**
3. Exaktes Timing von ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Timing - Übersicht

- Timing für ein paar (bereits bekannte) Schaltpläne:
  - RS-Flipflop
  - D-Latch
  - D-Flipflop
- Timing weiterer Komponenten, die bei der Realisierung der ReTI genutzt werden:
  - Kontrolllogik
  - Register mit Clock-Enable
  - ALU
  - Speicher

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).

- Nach Zeit $t_{P/SQ}$ ist $Q = 1$.

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).

- Nach Zeit $t_{P/SQ}$ ist $Q = 1$.

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).
- Nach Zeit $t_{P/SQ}$ ist $Q = 1$.
- Nach Zeit $t_{P/S/Q}$ ist $/Q = 0$.

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).
- Nach Zeit $t_{P/SQ}$ ist $Q = 1$.
- Nach Zeit $t_{P/S/Q}$ ist $/Q = 0$.

RS-Flipflop

- Zustand $Q = 0 \rightarrow$ Zustand $Q = 1$:

- Senke $/S$ zur Zeit t_0 ab und hebe zu $t_0 + x$ wieder an (einen solchen Signalverlauf nennt man Puls).
- Nach Zeit $t_{P/SQ}$ ist $Q = 1$.
- Nach Zeit $t_{P/S/Q}$ ist $/Q = 0$.
- Wähle x so, dass kein Spike entsteht.

Übergang - graphisch

NAND	t^{min}	t^{max}
G_1 τ_{PLH}	0.01	0.15
G_2 τ_{PHL}	0.01	0.12

muss spikefreies Umschalten von G_1 gewährleisten!!!

Spikefreier Übergang

- Nach den Regeln des spikefreien Umschaltens von Gattern entsteht kein Spike, falls:

$$(\cancel{t_0} + x) - (\cancel{t_0} + 0.27) \geq 0.41 \Leftrightarrow x \geq 0.68ns$$

- Wechsel von Zustand $Q = 1$ zu Zustand $Q = 0$ aus Symmetriegründen analog.

Symbole und Bezeichnungen

Symbol	Bezeichnung	t^{min}	t^{max}
x	Pulsweite	0.68	
$\tau_{P/SQ}$	Verzögerungszeit von $/S$ bis Q	0.01	0.15
$\tau_{P/S/Q}$	Verzögerungszeit von $/S$ bis $/Q$	0.02	0.27
$\tau_{P/RQ}$	Verzögerungszeit von $/R$ bis Q	0.02	0.27
$\tau_{P/R/Q}$	Verzögerungszeit von $/R$ bis $/Q$	0.01	0.15

D-Latch

- W ist *active high*.
  - $W = 0 \Rightarrow /S, /R$ inaktiv
  - $W = 1 \Rightarrow \begin{cases} /S \text{ aktiv}, & \text{falls } D = 1 \\ /R \text{ aktiv}, & \text{falls } D = 0 \end{cases}$

- Wie beim RS-Flipflop (minimale Pulsweite!) muss man auch beim D-Latch bestimmte Forderungen an den zeitlichen Verlauf der Signale stellen, um Spikefreiheit zu garantieren.

Timing-Diagramm

Timing-Bedingungen für das D-Latch

- W muss beim Schreiben lange genug 1 sein, um minimale Pulsweite x des RS-FFs zu garantieren.
- Vor $W : 0 \rightarrow 1$ werden Daten für Zeit t_{SDW} stabil gehalten, um Spikes auf $/S$, $/R$ zu vermeiden (der kritischste Fall ist das Verhindern von Spikes auf $/R$ bei Schreiben von 1).
- Nach $W : 1 \rightarrow 0$ werden Daten für Zeit t_{HWD} stabil gehalten, um Spikes auf $/S$, $/R$ zu vermeiden (der kritischste Fall ist das Verhindern von Spikes auf $/S$ beim Schreiben von 0).

Man rechnet nach:

Der Schreibvorgang beim D-Latch funktioniert mit den Parameterwerten aus der Tabelle (siehe Übung).

Symbol	**Bezeichnung**	t^{min}	t^{max}
y	Pulsweite des Schreibimpulses	0.79	
t_{SDW}	Setupzeit von D bis W	0.49	
t_{HDW}	Holdzeit von W nach D	0.41	
τ_{PWQ}	Verzögerungszeit von W bis Q	0.02	0.39
$(\tau_{PDQ}$	Verzögerungszeit von D bis Q	0.02	0.54)

Mögliche Realisierung: D-Flipflop

Timing: D-Flipflop

- Vorgehen analog zu RS-Flipflop und D-Latch.
- Wir verzichten daher auf weitere Details.
- Die NanGate-Bibliothek enthält bereits ein D-FF mit folgenden charakteristischen Zeiten (in *ns*):

Symbol	**Bezeichnung**	t^{min}	t^{max}
t_{SDC}	Setupzeit von *D* bis *ck*	0.08	
t_{HCD}	Holdzeit von *D* nach *ck*	0.14	
τ_{PCQ}	Verzögerungszeit von *ck* bis *Q*	0.12	0.26

Aufbau der Kontrolllogik, zur Erinnerung

- Generierung der Kontrollsignale (OE von Treibern, ALU-Ansteuerung, ...).
- Ist ein Kontrollsignal *active low*, dann bezeichnen wir es z.B. mit $/x$. Das Ausgangssignal $/x$ ergibt sich dann durch Negation des Ausgangssignals x eines entsprechenden FFs mit Eingangssignal x_{pre}.
- Ist ein Kontrollsignal *active high*, dann bezeichnen wir es z.B. mit x. Das Ausgangssignal x entspricht dem Ausgangssignal eines FFs mit Eingangssignal x_{pre}.

Kontrolllogik

INV	t^{min}	t^{max}
τ_{PLH}	0.01	0.15
τ_{PHL}	0.00	0.08

- Die Dauer eines Taktes bezeichnen wir als Zykluszeit t_c.
- Active-High-Ausgangssignale der Kontrolllogik, bei denen das FF mit ck gesteuert ist, sind gegenüber der steigenden Flanke von ck um Zeit $\tau^+_{p,ah}$ verzögert (resultiert aus D-FF-Verzögerung).
- Active-Low-Ausgangssignale der Kontrolllogik, bei denen das FF mit ck gesteuert ist, sind gegenüber der steigenden Flanke von ck um Zeit $\tau^+_{p,al}$ verzögert (resultiert aus D-FF-Verzögerung + Inverterverzögerung).
- Active-High-Ausgangssignale der Kontrolllogik, bei denen das FF mit $/ck$ gesteuert ist, sind gegenüber der letzten steigenden Flanke von ck um Zeit $\tau^-_{p,ah} = \tau^+_{p,ah} + t_c/2 + \tau_{PLH,Inv}$ verzögert.
- Active-Low-Ausgangssignale der Kontrolllogik, bei denen das FF mit $/ck$ gesteuert ist, sind gegenüber der letzten steigenden Flanke von ck um Zeit $\tau^-_{p,al} = \tau^+_{p,al} + t_c/2 + \tau_{PLH,Inv}$ verzögert.

Timing: Kontrolllogik

- Mit geeigneter Implementierung des kombinatorischen Teiles erhält man folgende charakteristische Zeiten.

Symbol	**Bezeichnung**	$t^{\min}$	$t^{\max}$
$\tau^{+}_{p,ah}$	Verzögerungszeit *ck* bis *Q*, active high	0.12	0.26
$\tau^{+}_{p,al}$	Verzögerungszeit *ck* bis *Q*, active low	0.12	0.41
$\tau^{-}_{p,ah}$	Verzögerungszeit *ck* bis *Q* (von $/ck$ angesteuert, active high)	$t_c/2+0.13$	$t_c/2+0.41$
$\tau^{-}_{p,al}$	Verzögerungszeit *ck* bis *Q* (von $/ck$ angesteuert, active high)	$t_c/2+0.13$	$t_c/2+0.56$
t^{+}_{SDC}	Setupzeit von *D* bis *ck*	0.88	
t^{-}_{SDC}	Setupzeit von *D* bis $/ck$	0.88	
t^{+}_{HCD}	Holdzeit von *D* nach *ck*	0.06	
t^{-}_{HCD}	Holdzeit von *D* nach $/ck$	0.06	

Register mit Clock-Enable

- Bei der Implementierung benötigen wir noch einen Treiberbaum der Tiefe 2, um *Regcken* auf 32 1–Bit–Multiplexer zu verteilen.

Symbol	Bezeichnung	t^{min}
t_{SDC}	Setup-Zeit von *D* vor *ck*	0.23
t_{HDC}	Hold-Zeit von *D* nach *ck*	0.11
t_{SEC}	Setup-Zeit von *Regcken* vor *ck*	0.46
t_{HEC}	Hold-Zeit von *Regcken* nach *ck*	0.08

- t_{SDC} ergibt sich aus Setupzeit D-FF + maximale Verzögerungszeit Multiplexer (Daten bis Ausgang) (0.08 + 0.15).
- t_{HDC} ergibt sich aus Holdzeit D-FF - minimale Verzögerungszeit Multiplexer (Daten bis Ausgang) (0.14 - 0.03).
- t_{SEC} ergibt sich aus Setupzeit D-FF + maximale Verzögerungszeit Multiplexer (Select bis Ausgang) + 2 x maximale Verzögerungszeit Treiber (0.08 + 0.16 + 2 x 0.11).
- t_{HEC} ergibt sich aus Holdzeit D-FF - minimale Verzögerungszeit Multiplexer (Select bis Ausgang) - 2 x minimale Verzögerungszeit Treiber (0.14 - 0.02 - 2 x 0.02).

Schaltrealisierung der ALU

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Timing: ALU

- Annahme: ALU mit 32-Bit-Addierer (Conditional Sum).
- Man zeigt:
  - Längster Pfad über ALU läuft durch den Addierer.
  - Annahme:
    - Die Funktion–Select–Bits sind mindestens t_{select} = 0.28 ns vor den Operanden gültig.
    - Dann ist garantiert, dass der kritische Pfad nicht durch die select–Eingänge bestimmt wird.
  - Zeitverhalten der ALU:

Symbol	**Bezeichnung**	t^{min}	t^{max}
t_{select}		0.28	
t_{ALU}	Verzögerungszeit von a, b bzw. c_{in} bis Ausgang		3.25

SRAM

SRAM
A
n
D_{out}
W
D_{in}
W
D_{in}
F_N
F_N
N
N
W'
D'
D-Latch
D
Q
Q_i
W_i
W
Y_0
Y_i
Y_{N-1}
A
n
D_n
G_0
G_i
G_{N-1}
O_N
D_{out}

Timing: SRAM

- Auch hier wäre das Vorgehen analog zu den bereits vorgestellten Analysen möglich. Zuvor muss man sich noch Gedanken machen um das Timing von:
  - Dekodierer
  - Treiberbäume
  - OR-Baum
- Eine detaillierte Timinganalyse ist aufwändig.
- Für die folgenden Timinganalysen orientieren wir uns an dem kommerziell angebotenen SRAM CY7C1079DV33 der Firma Cypress Semiconductor (siehe folgende Folien).

Interface zu CY7C1079DV33

Timing: CY7C1079DV33

- Aus dem Datenblatt entnimmt man:

Symbol	Bezeichnung	t^{min}	t^{max}
t_{acc}	Lesezugriffszeit		12.0
t_{OED}	Zeit von $/SMDdoe = 0$ bis D		7.0
t_{OEZ}	Zeit von $/SMDdoe = 1$ bis high-Z		7.0
t_{wc}	Schreibzykluszeit	12.0	
t_{SAW}	Setupzeit von A bis W	0.0	
t_{SAEW}	Setupzeit von A bis Ende W	9.0	
t_{HWA}	Holdzeit von A nach W	0.0	
w	Schreibpulsweite	9.0	
t_{SDEW}	Setupzeit von D bis Ende W	7.0	
t_{HWD}	Holdzeit von D nach W	0.0	

Kapitel 5

Timing:
1. Physikalische Eigenschaften
2. Timing wichtiger Komponenten
3. **Exaktes Timing von ReTI**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer
Professur für Rechnerarchitektur
WS 2016/17

UNI FREIBURG

Es gilt:

- Bei hinreichend langsamem Takt funktioniert der Rechner.

Frage:

- Wie schnell kann man den Rechner takten?
  Wie lange muss ein Takt mind. sein?

→ Ersetze idealisiertes Timing durch exakte Timinganalyse

→ Gesucht:
Untere Grenze für Zykluszeit t_c

Schritte der Analyse

1. Einhalten von Setup- und Hold-Zeiten der Kontrolllogik
2. Vermeidung von Bus-Contention
3. PC-Inkrementierung
4. Compute-Befehle:
   OE: Compute Memory
5. *Fetch*, *Load*, *Store*, *Jump*

- Wir werden uns auf Compute-Befehle beschränken.

Timing der Kontrolllogik (1/3)

Symbol	Bezeichnung	t^{min}	t^{max}
$\tau^{+}_{p,ah}$	Verzögerungszeit *ck* bis *Q*, active high	0.12	0.26
$\tau^{+}_{p,al}$	Verzögerungszeit *ck* bis *Q*, active low	0.12	0.41
$\tau^{-}_{p,ah}$	Verzögerungszeit *ck* bis *Q* (von $/ck$ angesteuert, active high)	$t_c/2+0.13$	$t_c/2+0.41$
$\tau^{-}_{p,al}$	Verzögerungszeit *ck* bis *Q* (von $/ck$ angesteuert, active high)	$t_c/2+0.13$	$t_c/2+0.56$
t^{+}_{SDC}	Setupzeit von *D* bis *ck*	0.88	
t^{-}_{SDC}	Setupzeit von *D* bis $/ck$	0.88	
t^{+}_{HCD}	Holdzeit von *D* nach *ck*	0.06	
t^{-}_{HCD}	Holdzeit von *D* nach $/ck$	0.06	

- Setupzeit der Dateneingänge bis *ck* ist $t^{+}_{SDC} \geq 0.88$, Setupzeit der Dateneingänge bis $/ck$ ist $t^{-}_{SDC} \geq 0.88$.
- Dateneingänge ($s_0, s_1, E, I, ACC, reset$) müssen rechtzeitig bereit sein.
- Alle Dateneingänge sind Ausgangssignale von FFs, die mit *ck* getaktet werden.

Timing der Kontrolllogik (2/3)

- Wähle eine beliebige steigende Taktflanke *Pi* als zeitlichen Bezugspunkt.
- Die Dateneingänge sind also bereit zur Zeit $\tau_{PCQ} = [0.12, 0.26]$ (Verzögerung eines D-FF).
- Die nächste steigende Taktflanke von $/ck$ ist bei $\frac{t_c}{2} + [0.01, 0.15]$, die nächste steigende Taktflanke von ck bei t_c.

INVERTER

$$\Rightarrow \frac{t_c}{2} + \underbrace{0.01}_{\text{Inverterverzögerung}} \geq \underbrace{0.88}_{t^-_{SDC}} + \underbrace{0.26}_{\tau_{PCQ}\text{ für FFs}}, \text{ d.h. } t_c \geq 2.26.$$

$$\Rightarrow t_c \geq \underbrace{0.88}_{t^+_{SDC}} + \underbrace{0.26}_{\tau_{PCQ}\text{ für FFs}} = 1.14$$

Timing der Kontrolllogik (3/3)

- Hold-Zeiten sind unkritisch:
  - FFs, die mit *ck* getaktet sind:
    $t^{+}_{HDC} \geq 0.06$ und Eingangsdaten werden mindestens noch 0.12 ns nach steigender Flanke von *ck* gehalten (Verzögerung D-FF).
  - FFs, die mit $/ck$ getaktet sind:
    $t^{-}_{HDC} \geq 0.06$ und Eingangsdaten werden sowieso noch einen halben Takt nach steigender Flanke von $/ck$ gehalten (+ D-FF-Verzögerung).

Constraints

- $t_c \geq 2.26$

Compute-Befehle

- Am zeitkritischsten ist Compute memory!

$[r] := [r] + [M(\langle i \rangle)]$; hier: $[PC] := [PC] + [M(\langle i \rangle)]$

Analyse allgemein

- Beginn der Analyse bei *P3* von Fetch als zeitlicher Bezugspunkt.
- Bei *P3* von Fetch wird der Befehl ins Instruktionsregister übernommen.

I-Ausgänge (1/2)

I-Ausgänge gültig bei

$$\tau_1 = \underbrace{[0.12, 0.26]}_{\tau_{PCQ} \text{ von Register } I}$$

D-FF Verzögerung

D-FF	Bezeichnung	t^{min}	t^{max}
t_{SDC}	Setupzeit von D bis ck	0.08	
t_{HCD}	Holdzeit von D nach ck	0.14	
τ_{PCQ}	Verzögerungszeit von ck bis Q	0.12	0.26
τ_{PDQ}	Verzögerungszeit von D bis Q	0.10	0.21

- $0^8 I_{23} \ldots I_0$ wird über Treiber *IAd* auf Adressbus gegeben.
- 0^8 ist eine Konstante und steht daher ebenfalls zu τ_1 bereit.

Constraints

- $\tau_1 = [0.12, 0.26]$

- $t_c \geq 2.26$

I-Ausgänge (2/2)

IAd enabled bei *N0* von Execute, d.h. /*IAdoe* aktiv zur Zeit

$$\begin{aligned}\tau_2 &= t_c + t_{p,al} \\ &= t_c + \frac{t_c}{2} + [0.13, 0.56] \\ &= \frac{3}{2} t_c + [0.13, 0.56]\end{aligned}$$

I schon gültig vor Aktivierung von *IAd* bei Punkt 2, falls

$$\begin{aligned}\max(\tau_1) &\leq \min(\tau_2) \Leftrightarrow \\ 0.26 &\leq \frac{3}{2} t_c + 0.13 \Leftrightarrow \\ \frac{3}{2} t_c &\geq 0.13 \Leftarrow \\ t_c &\geq 0.09\end{aligned}$$

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2} t_c + [0.13, 0.56]$

- $t_c \geq 2.26$
- $t_c \geq 0.09$

-14-

Gültiges A (1/2)

$\rightarrow$ A gültig zur Zeit

$$\tau_3 = \tau_2 + \underbrace{[0.03, 0.11]}_{\text{Enable Zeit Treiber}}$$

$$= \frac{3}{2} t_c + [0.16, 0.67]$$

	Tristate-Treiber	min	max
τ_{PZL}	Enable-Zeiten	0.03	0.10
τ_{PZH}	Enable-Zeiten	0.03	0.11
τ_{PLZ}	Disable-Zeiten	0.03	0.11
τ_{PHZ}	Disable-Zeiten	0.03	0.10
τ_{PLH}	Umschaltverzögerung bei $/OE = 0$	0.02	0.07
τ_{PHL}	Umschaltverzögerung bei $/OE = 0$	0.03	0.10

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2} t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2} t_c + [0.16, 0.67]$

- $t_c \geq 2.26$
- $t_c \geq 0.09$

Gültiges A (2/2)

- *ASMd* immer enabled

→ nur Treiber-Verzögerung berücksichtigt

→ A an SM bei

- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2} t_c + [0.18, 0.77]$

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2} t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2} t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2} t_c + [0.18, 0.77]$

- $t_c \geq 2.26$
- $t_c \geq 0.09$

UNI FREIBURG

Daten am Speicherausgang (1/3)

- Lesezugriffszeit von *SRAM*: [0.0, 12.0] (siehe Daten von CY7C1079DV33)

→ Gültige Daten am Speicherausgang bei

$$
\begin{aligned}
\tau_5 &= \tau_4 + [0.0, 12.0] \\
&= \frac{3}{2} t_c + [0.18, 0.77] + [0.0, 12.0] \\
&= \frac{3}{2} t_c + [0.18, 12.77]
\end{aligned}
$$

- Das ist aber nur korrekt, wenn der Ausgangstreiber durch /*SMDdoe* rechtzeitig enabled ist!

-19

Daten am Speicherausgang (2/3)

SRAM CY7C1079DV33			
Symbol	**Bezeichnung**	t^{min}	t^{max}
t_{acc}	Lesezugriffszeit		12.0
t_{OED}	Zeit von $/SMDdoe = 0$ bis D		7.0
...			

- $/SMDdoe$ aktiviert zur Zeit $\tau' = 2 \cdot t_c + \tau^+_{p,al} = 2 \cdot t_c + [0.12, 0.41]$.
- Daten am Speicherausgang aufgrund Treiber-Enable gültig zur Zeit $\tau'' = \tau' + [0.0, 7.0] = 2 \cdot t_c + [0.12, 7.41]$.

$\Rightarrow$ Daten am Speicherausgang gültig spätestens zur Zeit $t''' = \max(\max(\tau_5), \max(\tau''))$.

Daten am Speicherausgang (3/3)

- Daten am Speicherausgang gültig zur Zeit $t''' = \max(\max(\tau_5), \max(\tau''))$.
- Bedingung für $\max(\tau_5) \geq \max(\tau'')$:

$$\begin{aligned} \frac{3}{2}t_c + 12.77 &\geq 2 \cdot t_c + 7.41 \Leftrightarrow \\ \frac{1}{2}t_c &\leq 5.36 \Leftrightarrow \\ t_c &\leq 10.72 \end{aligned}$$

- Wir nehmen ab jetzt an, dass die Taktperiode $t_c \leq 10.72$ ist und rechnen mit $\max(\tau_5)$ weiter.
- (Es gilt auf jeden Fall $\min(\tau_5)\ (= \frac{3}{2}t_c + 0.18) < \min(\tau'')\ (= 2 \cdot t_c + 0.12)$
- Sollte sich später ergeben, dass die minimale Taktperiode $t_c > 10.72$, dann müssten wir die Rechnung nochmals korrigieren.

21

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2}t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2}t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2}t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2}t_c + [0.18, 12.77]$

Spätestens hier liegen SRAM-Daten auf D

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$

22

Daten auf *R*

DRd enabled bei *P*0 von Execute, also einen Takt vor Ausgangstreiber von *SM*
→ Enable nicht kritisch
→ Daten auf *R* spätestens bei

$$\tau_6 = \tau_5 + [0.02, 0.10] \text{ (Treiber-Verzögerung)}$$
$$= \frac{3}{2} t_c + [0.20, 12.87]$$

PC = PC + M(<i>)

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2} t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2} t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2} t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2} t_c + [0.18, 12.77]$
- $\tau_6 = \tau_5 + [0.2, 0.10] = \frac{3}{2} t_c + [0.20, 12.87]$

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$

Daten auf L

- Registerausgänge $r \in \{PC, ACC, IN1, IN2\}$ schon seit letzter Execute-Phase gültig.

$\rightarrow$ nicht kritisch

- Treiber *rLd* enabled bei $P0$ von Execute, d.h. wie auch bei *DRd* ist Zeit zum Enablen unkritisch im Vergleich zu t_6.

$f[2:0], c_{in}$

- $f[2:0], c_{in}$ werden durch den kombinatorischen Schaltkreis der Kontrolllogik aus $I_{31}, \ldots, I_{24}$ berechnet.
- I-Ausgänge aber schon gültig bei $\tau_1 = [0.12, 0.26]$.
  D-FF
- Verzögerungszeit des kombinatorischen Schaltkreises $< t^+_{SDC} = 0.88$
- $f[2:0], c_{in}$ gültig spätestens bei $t_7 = 0.26 + 0.88 = 1.14$.

$\rightarrow$ völlig unkritisch verglichen mit $\max(\tau_6) = \frac{3}{2} t_c + 12.87$

UNI FREIBURG

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2}t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2}t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2}t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2}t_c + [0.18, 12.77]$
- $\tau_6 = \tau_5 + [0.2, 0.10] = \frac{3}{2}t_c + [0.20, 12.87]$
- $t_7 = 1.14$

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$

UNI FREIBURG

Voraussetzungen für die exakte Timinganalyse von *Compute memory*

- *ALU*
- Analyse der ALU (32-Bit mit Conditional Sum) unter folgender Annahme:
  - Funktionsselect-Signale liegen 0.28 ns vor den Daten an (unkritisch, da $t_7 + 0.28 = 1.14 + 0.28 = 1.42 < \min(\tau_6) = \frac{3}{2}t_c + 0.20$).

    $t_c \geq 2.26$
  - Resultatsausgänge gültig 3.25 ns nachdem die Daten anliegen.

Symbol	**Bezeichnung**	t^{min}	t^{max}
t_{select}		0.28	
t_{ALU}	Verzögerungszeit von a, b bzw. c_{in} bis Ausgang		3.25

28

ALU-Ausgänge

- Spätestens gültig bei

$$t_8 = \max(\tau_6) + \underbrace{3.25}_{\text{Delay ALU}} = \frac{3}{2}t_c + 12.87 + 3.25$$

$$= \frac{3}{2}t_c + 16.12$$

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2}t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2}t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2}t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2}t_c + [0.18, 12.77]$
- $\tau_6 = \tau_5 + [0.2, 0.10] = \frac{3}{2}t_c + [0.20, 12.87]$
- $t_7 = 1.14$
- $t_8 = \max(\tau_6) + 3.25 = \frac{3}{2}t_c + 16.12$

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$

DI

- /*ALUDIdoe* wird wie /*SMDdoe* aktiviert bei *P*1 von Execute
- Daten kommen an *ALUDId* später an als an als Daten am internen *SRAM*–Treiber
- Enable–Zeit von *ALUDId* jedoch kürzer als bei *SRAM*
- Mit $t_c \leq 10.72$ ist auf jeden Fall auch für *ALUDId* gewährleistet, dass Treiber enabled, wenn Daten kommen.

→ Berücksichtige nur Treiberverzögerung.

→ Gültig spätestens bei

$$
\begin{aligned}
t_9 &= t_8 + 0.10 \\
&= \frac{3}{2} t_c + 16.12 + 0.10 \\
&= \frac{3}{2} t_c + 16.22
\end{aligned}
$$

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2}t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2}t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2}t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2}t_c + [0.18, 12.77]$
- $\tau_6 = \tau_5 + [0.2, 0.10] = \frac{3}{2}t_c + [0.20, 12.87]$
- $t_7 = 1.14$
- $t_8 = \max(\tau_6) + 3.25 = \frac{3}{2}t_c + 16.12$
- $t_9 = t_8 + 0.10 = \frac{3}{2}t_c + 16.22$

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$

Datenübernahme in Register *r*

- Clocksignale bei *P*3 von Execute
  - → steigende Flanke bei $\tau_{10} = 4t_c$
- Minimale Taktperiode wird aus Setup-Zeit von *r* berechnet (Setup-Zeit am größten, wenn $r = PC$)

33

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2}t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2}t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2}t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2}t_c + [0.18, 12.77]$
- $\tau_6 = \tau_5 + [0.2, 0.10] = \frac{3}{2}t_c + [0.20, 12.87]$
- $t_7 = 1.14$
- $t_8 = \max(\tau_6) + 3.25 = \frac{3}{2}t_c + 16.12$
- $t_9 = t_8 + 0.10 = \frac{3}{2}t_c + 16.22$
- $\tau_{10} = 4 \cdot t_c$

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$

Timing: Zähler

- Aus einer Analyse des Zählers in einer Implementierung gemäß Kapitel 4.1 (aber mit zusätzlichem Clock–Enable für das Register!) ergeben sich folgende Zeiten:

Symbol	Bezeichnung	t^{min}	t^{max}
t_{SDC}	Setup-Zeit von *D* vor *ck*	0.53	
t_{HDC}	Hold-Zeit von *D* nach *ck*	0.05	
t_{SLC}	Setup-Zeit von $/L$ vor *ck*	0.76	
t_{HLC}	Hold-Zeit von $/L$ nach *ck*	0.02	
t_{SEC}	Setup-Zeit von $/PCcken$ vor *ck*	0.46	
t_{HEC}	Hold-Zeit von $/PCcken$ nach *ck*	0.08	
...	...	...	...

Setup-Zeit von Zähler

- Setup-Zeit: $t_{SDC} = 0.53\ ns$ (siehe Aufbau Zähler)

→ Bedingung:

- $t_9 + 0.53 \leq \min(\tau_{10})$
  $\Leftrightarrow \frac{3}{2}t_c + 16.75 \leq 4t_c$
  $\Leftrightarrow \frac{5}{2}t_c \geq 16.75$
  $\Leftrightarrow t_c \geq 6.70$

Constraints

- $\tau_1 = [0.12, 0.26]$
- $\tau_2 = t_c + \tau^{-}_{p,al} = \frac{3}{2}t_c + [0.13, 0.56]$
- $\tau_3 = \tau_2 + [0.03, 0.11] = \frac{3}{2}t_c + [0.16, 0.67]$
- $\tau_4 = \tau_3 + [0.02, 0.10] = \frac{3}{2}t_c + [0.18, 0.77]$
- $\tau_5 = \tau_4 + [0.0, 12.0] = \frac{3}{2}t_c + [0.18, 12.77]$
- $\tau_6 = \tau_5 + [0.2, 0.10] = \frac{3}{2}t_c + [0.20, 12.87]$
- $t_7 = 1.14$
- $t_8 = \max(\tau_6) + 3.25 = \frac{3}{2}t_c + 16.12$
- $t_9 = t_8 + 0.10 = \frac{3}{2}t_c + 16.22$
- $\tau_{10} = 4 \cdot t_c$

- $t_c \geq 2.26$
- $t_c \geq 0.09$
- $t_c \leq 10.72$
- $t_c \geq 6.70$

37

Es bleiben zu beachten:

Holdzeit D-FF = 0.14 − 0.03

- Hold-Zeit t_{HCD}
- Maximal bei $r \in \{ACC, IN1, IN2\}$, $t_{HCD} = 0.11$
  - Unproblematisch, da alle Treiber noch mindestens $\frac{1}{2}$ Takt nach *rck* enabled sind.

38

Setup- und Hold-Zeiten von *rcken*

- *rcken* aktiv bei $P2$ von Execute, inaktiv bei $P3$ von Execute, d.h. aktiv von:
  - $\tau_{11} = 3t_c + \tau^+_{p,ah} = 3t_c + [0.12, 0.26]$ bis
  - $\tau_{12} = 4t_c + \tau^+_{p,ah} = 4t_c + [0.12, 0.26]$
- Setup-Zeit:
  - Für alle $r \in \{PC, ACC, IN1, IN2\}$: $t_{SEC} = 0.46$

  $\Rightarrow$ $\max(\tau_{11}) + 0.46 \leq 4t_c$, d.h. $3t_c + 0.26 + 0.46 \leq 4t_c$ bzw.

  $\Rightarrow$ $t_c \geq 0.72$ (unkritisch im Vergleich zu bisherigen Constraints)
- Hold-Zeit:
  - Für alle $r \in \{PC, ACC, IN1, IN2\}$: $t_{HEC} = 0.08$

  $\Rightarrow$ $\min(\tau_{12}) \geq 4t_c + 0.08$, d.h. $0.12 \not\geq 0.08$
- (Analog auch für alle anderen Takte.)

Setup- und Hold-Zeiten $/PCload$ beim Zähler

- Setup $/L$ bis ck: $t_{SLC} = 0.76$
- Hold $/L$ nach ck: $t_{HLC} = 0.02$
- $/PCload$ (benötigt, wenn **neue** Werte in Zähler kommen) aktiv bei $P2$ von Execute, inaktiv bei $P0$ von Fetch, d.h. aktiv von:
  - $\tau_{13} = 3t_c + \tau^{+}_{p,al} = 3t_c + [0.12, 0.41]$ bis
  - $\tau_{14} = 5t_c + \tau^{+}_{p,al} = 5t_c + [0.12, 0.41]$

(* r = PC, IN1, IN2, ACC)

40

Bedingungen für Setup- und Hold-Zeiten /*PCload* beim Zähler

- Setup:

  $\max(\tau_{13}) + 0.76 \leq \min(\tau_{10}) \Leftrightarrow$
  $3t_c + 0.41 + 0.76 \leq 4t_c \Leftrightarrow$
  $t_c \geq 1.18$

- Hold:

  $\min(\tau_{14}) \geq \max(\tau_{10} + 0.02) \Leftrightarrow$
  $5t_c + 0.12 \geq 4t_c + 0.02 \Leftrightarrow$
  $t_c \geq -0.10$

$t_c \geq 6.70$

→ Beide unkritisch im Vergleich zu bisherigen Constraints.

41

Fazit: Zykluszeit und Befehlsrate

- Vorläufiges Ergebnis: Falls sich durch andere Befehle keine schärferen Bedingungen an die Zykluszeit ergeben, dann lautet sie:
  - $t_c \geq 6.70\ ns$
- Taktfrequenz:
  - $v = \frac{1}{6.70} \cdot 10^9\ Hz = 149.2\ MHz$
- 8 Takte pro Befehl $\rightarrow$ 18.6 Millionen Befehle pro Sekunde, d.h. Befehlsrate von 18.6 *MIPS* (= Million Instructions per Second)

Anmerkungen zur Timing–Analyse

- Eine „echte” Timing–Analyse müsste noch Leitungslaufzeiten auf dem Chip berücksichtigen.
- Dazu muss dann aber schon das Layout des Chips bekannt sein, um die Leitungslängen und -kapazitäten zu berechnen.
- Leitungslaufzeiten waren früher bei einem Aufbau mit diskreten Bausteinen vernachlässigbar, sind es bei den heutigen Technologien aber nicht mehr.

⇒ Exakte Timing-Analysen sind heute daher kaum ohne maschinelle Unterstützung durchführbar.

- Synthesetools sind in der Lage, durch Optimierung der Treiberstärken von Grundgattern (verschiedene Versionen in der Bibliothek!) Laufzeiten zu minimieren.
- Wird das SRAM nicht auf dem Chip integriert (d.h. stattdessen ein kommerzielles externes SRAM angeschlossen), dann muss man noch Verzögerungszeiten für I/O–Pads des Chips mit eventueller Anpassung von Spannungspegeln berücksichtigen.

Ausblick 1/2

- Beschleunigung
  - Schnellere Komponenten, z.B. ALU (siehe Übung)
  - Schnellere Adressberechnung (Treiber schon bei P0 öffnen)
  - Verkürzung des Fetch-Zyklus um 1 Takt
  - Pipelining
  - Schnellerer Speicher
  - ...

Ausblick (2/2)

- Fehlertoleranz (Kapitel 6)
  - Wie umgehen mit Übertragungsfehlern auf den Leitungen?
  - Parity-Check, Hamming-Code
  - Andere Fehler ...
- Verifikation (Kapitel 7)
  - Ist der Entwurf der ReTI überhaupt korrekt?
  - Automatische Methoden für den Beweis der Korrektheit
- Architekturkonzepte (Kapitel 8)
  - Speicherhierarchie
  - Pipelining
  - Parallelität

Kapitel 6

Fehlertoleranz

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Motivation

- Bisher: Rechnerarchitektur am Beispiel von ReTI
- Fehler auf verschiedenen Ebenen entdecken und beheben
  - → Fehler durch Fertigungsdefekte, Störungen: Kapitel 6
  - → Konzeptuelle Fehler, Entwurfsfehler: Kapitel 7
- Allgemeine Rechnerarchitektur und Entwurfskonzepte

Physikalische Fehler

- Bei der Informationsverarbeitung und -Übermittlung können physikalische Störungen auftreten.
  - Elektrisches Rauschen, Radiation, Defekte.
  - Absichtliche Manipulation durch Angreifer.
- Die Störungen äußern sich darin, dass Wert 0 statt Wert 1 berechnet/übertragen wird und umgekehrt.
  - „Kippen" des Werts $0 \rightarrow 1$, $1 \rightarrow 0$.
- Hier konzentrieren wir aus auf Fehler bei der Datenübertragung.
  - Manche Fehler betreffen direkt die Hardware oder andere Systemteile. Ihre Behandlung ist komplexer.

Wiederholung

Sei $A = \{a_1, \ldots, a_m\}$ ein endliches Alphabet der Größe m.

- Eine Abbildung $c : A \to \{0,1\}^n$ heißt Code fester Länge, falls c injektiv ist.
- Die Menge $c(A) := \{w \in \{0,1\}^n \mid \exists a \in A : c(a) = w\}$ heißt Menge der Codewörter.
- Minimale Codelänge: Für einen Code $c : A \to \{0,1\}^n$ fester Länge gilt: $n \geq \lceil \log_2 m \rceil$.

a → 000	e → 100
b → 001	f → 101
c → 010	g → 110
d → 011	h → 111

Fehler bei Datenübertragung (1/2)

$w \neq \tilde{w}$

$w \longrightarrow \tilde{w}$

Annahme:

- Sei c ein Code minimaler fester Länge n.
- Ein Datum a (z.B. ein Buchstabe, eine Zahl) wird, durch ein Codewort $w = c(a)$ repräsentiert übertragen.
- Sei $\tilde{w} \in \{0,1\}^n$ das empfangene Wort.
- Bei der Übertragung (z.B. über Internet) können einzelne Bits von $c(a)$ kippen. Dann ist $w \neq \tilde{w}$.

Fehler bei Datenübertragung (2/2)

Ziel:

- Durch Verändern des Codes c in einen Code C fester Länge $n + r$ sollen diese Bits
  - erkannt

    $\rightarrow$ Fehlererkennende Codes
    Bsp. für 1-fehlererkennenden Code: Parity-Code
  - korrigiert

    $\rightarrow$ Fehlerkorrigierende Codes
    Bsp. für 1-fehlerkorrigierenden Code: Hamming-Code

  werden.

Fehlererkennende Codes

Idee:

- Wähle Codewörter $w \in c(A)$ so, dass nach Kippen von Bits Wörter $\tilde{w} \in \{0,1\}^n$ entstehen, die keine Codewörter sind, d.h. $\tilde{w} \notin c(A)$.
- Wird ein Nicht-Codewort empfangen, so muss ein Übertragungsfehler aufgetreten sein.
- Benutze Codes mit $n = \lceil log_2 m \rceil + r$ mit $r > 0$.
- Benutze die r zusätzlichen Bits zum Test auf Übertragungsfehler.
- Beispiel: Parity-Code

c n+r

$|r| = 1$

a	000	0
b	001	1
	010	1
	011	0
	100	1
	101	0
	110	0
	111	1

„Kugel"

Umgebung, wo alle Wörter max. 1 Bit unterschied haben

Parity-Code

- Eine Bitfolge $w \in \{0,1\}^n$ besteht den Paritätstest (engl. Parity-Check), wenn die Anzahl der auf 1 gesetzten Bitstellen gerade ist.

- Sei $c : A \to \{0,1\}^n$ ein Code fester Länge von A. Betrachte den Code $C : A \to \{0,1\}^{n+1}$, der aus Code c entsteht, in dem eine Bitstelle an jedes Codewort $c(a)$ hinten angefügt wird und so gesetzt wird, dass der neue Code $C(a)$ den Paritätstest besteht.

Fehlererkennender Code

- Ein Code $c : A \to \{0,1\}^n$ fester Länge heißt k-fehlererkennend, wenn der Empfänger in jedem Fall entscheiden kann, ob ein gesendetes Codewort durch Kippen von bis zu k Bits verfälscht wurde.

- Der Parity-Code C ist 1-fehlererkennend.
  - **Beweis**: Kippt bei der Übertragung von $C(a)$ genau eine Bitstelle, so kommt eine Bitfolge an, die den Paritätstest nicht besteht und somit kein Codewort von C darstellt. Überprüft der Empfänger die Parität der empfangenen Bitfolge, kann er auf einen Fehler schließen.

Fehlererkennender Code

- Ein Code $c : A \to \{0,1\}^n$ fester Länge heißt k-fehlererkennend, wenn der Empfänger in jedem Fall entscheiden kann, ob ein gesendetes Codewort durch Kippen von bis zu k Bits verfälscht wurde.

- Der Parity-Code C ist 1-fehlererkennend.
  - **Beweis**: Kippt bei der Übertragung von $C(a)$ genau eine Bitstelle, so kommt eine Bitfolge an, die den Paritätstest nicht besteht und somit kein Codewort von C darstellt. Überprüft der Empfänger die Parität der empfangenen Bitfolge, kann er auf einen Fehler schließen.

SMILE - Fehlererkennung bei Parity-Code

Welche Fehler bei der Übertragung werden durch den Paritätstest beim Empfänger erkannt? Das letzte Bit bei Sender und Empfänger sei dabei das Parity-Bit.

a. Sender: 100010101, Empfänger: 100010101 ✗
b. Sender: 100110100, Empfänger: 100010100 ✓
c. Sender: 111010101, Empfänger: 101010101 ✓
d. Sender: 000000000, Empfänger: 100000001 ✗

UNI FREIBURG

Hamming-Abstand (1/2)

Definition

Der Hamming-Abstand $dist(v, w)$ zweier n-Bitfolgen v und w ist die Anzahl der Stellen, an denen v und w sich unterscheiden.

- $dist(00001101, 10001100) = 2$
- $dist(00001101, 00001101) = 0$
- Ist v das übertragene und w das empfangene Codewort, so liegt ein Übertragungsfehler genau dann vor, wenn $dist(v, w) \neq 0$.
  - Ein Übertragungsfehler heißt einfach, wenn $dist(v, w) = 1$.
- Der Hamming-Abstand eines Codes $c : A \to \{0,1\}^n$ ist der kleinste Abstand zweier Codewörter von c:
  $dist(c) := min\{dist(c(a_i), c(a_j)); a_i, a_j \in A \text{ mit } a_i \neq a_j\}$.

000 1
010 6
101 3
2
dist(..)=1

UNI FREIBURG

Hamming-Abstand (2/2)

Lemma

Ein Code c fester Länge ist genau dann k-fehlererkennend, wenn $dist(c) \geq k+1$ gilt.

1+1 ⇒ 1-fehlererkennend

- **Beweisidee:** Durch das Kippen von bis zu $l \leq k$ Bits kann aus Codewort $a \in c(A)$ kein anderes Codewort $a^* \in c(A)$ entstehen, denn sonst wäre $dist(c(a), c(a^*)) = l$, was kleiner als der Hamming-Abstand des Codes wäre.

Fehlerkorrigierende Codes

Idee:

- Benutze r zusätzliche Bits, so dass das gesendete Codewort aus dem empfangenen Wort rekonstruiert werden kann.

- Beispiel: Hamming-Code

UNI FREIBURG

Hamming-Code

3 2 1 6 5 4 3 2 1
000 → 00_0__
001 00_1__
010
011
100
101
110
111

- Benutze die Bitstellen 2^0, 2^1, …, 2^{r-1} als Überprüfungsbits, wobei die Bitstelle 2^j die Bitstellen überprüft, deren Binärdarstellungen an der j-ten Stelle eine 1 haben.

$2^0=1$ $2^1=2$ $2^2=4$

- Die Bitstelle 2^j wird so belegt, dass gerade viele Bitstellen, deren Binärdarstellungen an der j-ten Stelle eine 1 haben, gesetzt sind. (vgl. Paritätstest)

-15

Hamming-Code an einem Beispiel

- Uncodiertes Wort: 0111 0101 0000 1111.
  $\rightarrow m = 16$.
  ↳ Länge des Code Wort
- Konstruktion des Hamming-codierten Codeworts:
  - Das Wort wird unter Auslassung der „Zweierpotenz"-Bitstellen aufgeschrieben:
    01110 _ 1010000 _ 111 _ 1 _ _.
    2^4 2^8 2^2 2^1 2^0
  - Dies ergibt insgesamt 21 Bitstellen ($r = 5$).
  - Die „Zweierpotenz"-Bitstellen werden als Überprüfungsbits benutzt (Nummerierung beginnt rechts mit der Stelle 1).
  - Zur Erinnerung: Die Bitstelle 2^j wird so belegt, dass gerade viele Bitstellen, deren Binärdarstellungen an der j-ten Stelle eine 1 haben, gesetzt sind.

-16-

Hamming-Code-Beispiel (1/4)

0111010100001111

01110_1010000_111_1__

21 ... 321

	2^4	2^3	2^2	2^1	2^0	zu codierende Bitfolge
3						1
5						1
6						1
7						1
9						0
10						0
11						0
12						0
13						1
14						0
15						1
17						0
18						1
19						1
20						1
21						0

11
101
110
111
1001
1010
⋮

Das Überprüfungsbit 2^j überprüft die Bitstellen, die in ihrer Binärdarstellung an der j-ten Stelle eine 1 haben.

UNI FREIBURG

Hamming-Code-Beispiel (2/4)

	2^4	2^3	2^2	2^1	2^0	zu codierende Bitfolge
3				_	_	1
5			_		_	1
6			_	_		1
7			_	_	_	1
9		_			_	0
10		_		_		0
11		_		_	_	0
12		_	_			0
13		_	_		_	1
14		0	0	0		0
15		1	1	1	1	1
17	_				_	0
18	_			_		1
19	_			_	_	1
20	_		_			1
21	_		_		_	0

Das Überprüfungsbit 2^j überprüft die Bitstellen, die in ihrer Binärdarstellung an der j-ten Stelle eine 1 haben.

$10101_2 = 21_{10}$

4 3 2 1 0

-18

Hamming-Code-Beispiel (3/4)

	2^4	2^3	2^2	2^1	2^0	zu codierende Bitfolge
3				1	1	1
5			1		1	1
6			1	1		1
7			1	1	1	1
9		0			0	0
10		0		0		0
11		0		0	0	0
12		0	0			0
13		1	1		1	1
14		0	0	0		0
15		1	1	1	1	1
17	0				0	0
18	1			1		1
19	1			1	1	1
20	1		1			1
21	0		0		0	0
	1	0	0	0	0	

Parity Code

$2^3 + 2^1 = 10$

Der Prüfbitwert ergibt sich aus der Summe modulo 2 der jeweiligen Spalte.

Das Überprüfungsbit 2^j überprüft die Bitstellen, die in ihrer Binärdarstellung an der j-ten Stelle eine 1 haben.

Hamming-Code Beispiel (4/4)

- Die Bitfolge 0111 0101 0000 1111
- wird mit dem Hamming-Code zum Codewort
  0 1110 1101 0000 0111 0100.

UNI FREIBURG

Und wie findet man einen Fehler? (1/2)

- Nehme einen Übertragungsfehler an Position 13 des Codeworts an.

- Fehlerhaft empfangenes Wort:
  0 1110 1100 0000 0111 0100.

21

Und wie findet man einen Fehler? (2/2)

	2^4	2^3	2^2	2^1	2^0	empfangene Bitfolge
3				1	1	1
5			1		1	1
6			1	1		1
7			1	1	1	1
9		0			0	0
10		0		0		0
11		0		0	0	0
12		0	0			0
13		0	0		0	0
14		0	0	0		0
15		1	1	1	1	1
17	0				0	0
18	1			1		1
19	1			1	1	1
20	1		1			1
21	0		0		0	0
	1	0	0	0	0	

⇒ Fehler muss sich in Zeile 8 + 4 + 1 = 13 befinden!

$1101_2 = 13_{10}$

Die Spalten 8,4 und 1 bestehen den Paritätstest nicht!

22

Fehlerkorrigierende Codes

Definition

Ein Code $c : A \to \{0,1\}^n$ fester Länge heißt k-fehlerkorrigierend, wenn der Empfänger in jedem Fall entscheiden kann, ob ein gesendetes Codewort w durch Kippen von bis zu k Bits verfälscht wurde und daraufhin w aus dem empfangenen Wort $\tilde{w}$ rekonstruiert werden kann.

- Der Hamming-Code ist 1-fehlerkorrigierend. Die Anzahl der Zusatzbits $r = 1 + \lfloor log_2 m \rfloor$ ist minimal (Korrektheit folgt aus noch folgendem Satz).

Zusammenhang Hamming-Abstand und Fehlerkorrektur

Lemma

Ein Code c fester Länge ist genau dann k-fehlerkorrigierend, wenn $dist(c) \geq 2k+1$ gilt.

$2 \cdot 1 + 1 = 3$

Beweis:

- Sei $M(c(a_i),k) := \{w \in \{0,1\}^n \mid dist(c(a_i),w) \leq k\}$ die Kugel um $c(a_i)$ mit Radius k.
- Dann gilt:
  c ist k-fehlerkorrigierend $\Leftrightarrow \forall a_i, a_j i \neq j$ gilt: $M(c(a_i),k) \cap M(c(a_j),k) = \emptyset$.
- Für den Beweis ist also zu zeigen:
  $[\forall a_i, a_j\ i \neq j : M(c(a_i),k) \cap M(c(a_j),k) = \emptyset] \Leftrightarrow dist(c) \geq 2k+1$.

Beweis der Hilfs-Behauptung

$A \Rightarrow B$ $\quad \neg B \Rightarrow \neg A$

$c(a_i) = b_0$
$c(a_j) = 2_{2k}$

„A" „B"

- $[\forall a_i, a_j\ i \neq j : M(c(a_i), k) \cap M(c(a_j), k) = \emptyset] \Leftrightarrow dist(c) \geq 2k+1$.

- Beweis „$\Rightarrow$":
  - Annahme: $dist(c) < 2k+1$
  - D.h. $\exists\ a_i, a_j$ mit $dist(c(a_i), c(a_j)) = l$ und $l < 2k+1$;
  - also gibt es eine Folge: $c(a_i) = b_0, b_1, \ldots, b_{k-1}, b_k, b_{k+1}, \ldots, b_{2k} = c(a_j)$ mit $dist(b_i, b_{i+1}) = 0$ oder $dist(b_i, b_{i+1}) = 1$ (für alle $i = 0, \ldots, 2k-1$),
  - also $b_k \in M(c(a_i), k) \cap M(c(a_j), k)$. ↯ $\Rightarrow$ „$\neg A$"

$b_k \in M(c(a_i), k)$

$b_k \in M(c(a_j), k)$

- Beweis „$\Leftarrow$":
  - Annahme: $M(c(a_i), k) \cap M(c(a_j), k) \neq \emptyset$.
  - Es gibt also b im Durchschnitt mit:
    $dist(c) \leq dist(c(a_i), c(a_j)) \leq dist(c(a_i), b) + dist(b, c(a_j)) \leq k + k$. ↯

$\leq k$ $\quad \leq k$

Anzahl Zusatzbits für Fehlerkorrigierende Codes

Satz

Für einen 1-fehlerkorrigierenden Code $c : A \to \{0,1\}^{m+r}$ fester Länge über A mit $|A| = 2^m$ gilt: $r \geq 1 + \lfloor log_2 m \rfloor$.

Beweis:

- $M_1(a) := \{b \in \{0,1\}^{m+r} :$
  b entsteht aus $c(a)$ durch Kippen von bis zu 1 Bit$\}$.
- Nach Lemma muss gelten: $M_1(a_1) \cap M_1(a_2) = \emptyset$ für alle $a_1, a_2 \in A$,
- es gilt $|M_1(a)| = m + r + 1$ für alle $a \in A$.
- Also müssen 2^m überschneidungsfreie Kugeln, jede mit $(m+r+1)$ Elementen, im Raum $\mathbb{B}^{m+r}$ enthalten sein: $2^m(m+r+1) \leq 2^{m+r}$.
- Behauptung: Aus $2^m(m+r+1) \leq 2^{m+r}$ folgt $r \geq 1 + \lfloor log_2 m \rfloor$.
- Sei hierzu $k := \lfloor log_2 m \rfloor \Rightarrow 2^k \leq m$.
- $2^m(m+r+1) \leq 2^{m+r} \Leftrightarrow m+r+1 \leq 2^r \Rightarrow 2^k + \cancel{r} + 1 \leq 2^r \Rightarrow 2^k + 1 \leq 2^r \Rightarrow$
  $k < r \Leftrightarrow k+1 \leq r \Leftrightarrow \lfloor log_2 m \rfloor + 1 \leq r$.

Ausblick

- Wir haben bisher angenommen, dass Fehler auf Kommunikationskanälen auftreten.
- Es gibt auch Fehler in der Hardware selbst.
  - Permanente Fehler (Fertigungsdefekte)
    → Testmethoden (Rechnerarchitektur, Spezialvorlesung „Testen”)
  - Latente Fehler („Beinahe-Defekte”)
    → Stresstest (Spezialvorlesung „Testen”)
  - Transiente Fehler (Störungen während des Betriebs)
    → Fehlertoleranz, Redundanz (Spezialvorlesung „Testen”)
  - Absichtlich herbeigeführte Fehler (Angriffe)
    - Aus Vergleich des Systemverhaltens mit und ohne Fehler auf geschützte Daten schließen (Fault-Based Cryptanalysis). (*Seminar*)
- Vor allem bei sicherheitskritischen Systemen in neuesten Fertigungstechnologien sind Fehler problematisch.

Kapitel 7

Formale Spezifikation von Hardware:

1. **Boolesche Ausdrücke**
2. Binäre Entscheidungsdiagramme (BDDs)
3. Anwendung: Formale Verifikation

binary decision diagram

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Motivation

- Der Entwurf von ReTI hat (hoffentlich) gezeigt, dass Hardware-Synthese komplex und fehleranfällig ist.
- Es gibt automatische Methoden, um Fehler zu finden oder ihre Abwesenheit nachweisen zu können.
- Für ihre Anwendbarkeit muss ein Schaltkreis formal vollständig spezifiziert werden.
- Wir schauen uns daher boolesche Funktionen nochmals (und genauer) an und lernen effiziente Algorithmen und Datenstrukturen zu ihrer Handhabung.

Motivation

- Der Entwurf von ReTI hat (hoffentlich) gezeigt, dass Hardware-Synthese komplex und fehleranfällig ist.
- Es gibt automatische Methoden, um Fehler zu finden oder ihre Abwesenheit nachweisen zu können.
- Für ihre Anwendbarkeit muss ein Schaltkreis formal vollständig spezifiziert werden.
- Wir schauen uns daher boolesche Funktionen nochmals (und genauer) an und lernen effiziente Algorithmen und Datenstrukturen zu ihrer Handhabung.

Boolesche Algebren - allgemein

Operation

- Es sei M eine Menge auf der zwei binäre Operationen $\cdot$ und $+$ und eine unäre Option $\sim$ definiert sind.

$\wedge$ $\vee$

- Das Tupel $(M, \cdot, +, \sim)$ heißt boolesche Algebra, falls M eine nichtleere Menge ist und für alle $x, y, z \in M$ die folgenden Axiome gelten:

Kommutativität	$x + y = y + x$	$x \cdot y = y \cdot x$
Assoziativität	$x + (y + z) = (x + y) + z$	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Absorption	$x + (x \cdot y) = x$	$x \cdot (x + y) = x$
Distributivität	$x + (y \cdot z) = (x + y) \cdot (x + z)$	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
Komplement	$x + (y \cdot \sim y) = x$	$x \cdot (y + \sim y) = x$

4

Beispiele boolescher Algebren

$\{0,1\}$

- $(\mathbb{B}, \wedge, \vee, \neg)$
- Boolesche Algebra der Teilmengen einer Menge S: $(Pot(S), \cap, \cup, ^C)$
- Boolesche Algebra der booleschen Funktionen in n Variablen: $(\mathbb{B}_n, \cdot, +, \sim)$

Potenzmenge

$S = \{a, b, c\}$

$Pot(S) = \{\emptyset, \{a\}, \{b\}, \ldots, \{a,b,c\}\}$

$\Rightarrow$ **Allgemein**: Lässt sich eine Aussage direkt aus den Axiomen herleiten, dann gilt sie in allen booleschen Algebren!

- Man darf beim Beweis der Aussage aber auch wirklich nur die Axiome verwenden und keine Eigenschaften der konkreten booleschen Algebra.

UNI FREIBURG

5

Boolesche Algebra der Teilmengen von S $(Pot(S), \cap, \cup, ^C)$

Komplement/
Inverse/
Negation

- Menge: Potenzmenge von S
- $\cdot : Pot(S) \times Pot(S) \to Pot(S);\ (M_1, M_2) \mapsto M_1 \cap M_2$
- $+ : Pot(S) \times Pot(S) \to Pot(S);\ (M_1, M_2) \mapsto M_1 \cup M_2$
- $^C : Pot(S) \to Pot(S);\ M \mapsto M^C := S \setminus M$

Satz

$(Pot(S), \cap, \cup, ^C)$ ist eine boolesche Algebra.

- **Beweis**: Nachrechnen, dass alle Axiome gelten.

  Beispiel: Absorption

  - Seien $M_1, M_2 \in Pot(S)$.
  - Dann ist $(M_1 + (M_1 \cdot M_2)) = (M_1 \cup \overbrace{(M_1 \cap M_2)}^{M' \subseteq M_1}) = M_1$ und $(M_1 \cdot (M_1 + M_2)) = (M_1 \cap (M_1 \cup M_2)) = M_1$.

UNI FREIBURG 6

Boolesche Algebra der Funktionen in n Variablen $(\mathbb{B}_n, \cdot, +, \sim)$

- Menge: $\mathbb{B}_n$ (Menge der booleschen Funktionen in n Variablen)
- $\cdot$: $\mathbb{B}_n \times \mathbb{B}_n \to \mathbb{B}_n$; $(f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$ für alle $\alpha \in \mathbb{B}^n$
- $+$: $\mathbb{B}_n \times \mathbb{B}_n \to \mathbb{B}_n$; $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ für alle $\alpha \in \mathbb{B}^n$
- $\sim$: $\mathbb{B}_n \to \mathbb{B}_n$; $(\sim f)(\alpha) = 1 \Leftrightarrow f(\alpha) = 0$ für alle $\alpha \in \mathbb{B}^n$

Satz

$(\mathbb{B}_n, \cdot, +, \sim)$ ist eine boolesche Algebra.

- **Beweis**: Nachrechnen, dass alle Axiome gelten.

  Beispiel: Kommutativität
  - Seien $f, g \in \mathbb{B}_n$.
  - Für alle $\alpha \in \mathbb{B}^n$ gilt: $(f+g)(\alpha) = \underbrace{f(\alpha) + g(\alpha)}_{+:\ \mathbb{B}\times\mathbb{B}\to\mathbb{B}} = g(\alpha) + f(\alpha) = \underbrace{(g+f)(\alpha)}_{+:\ \mathbb{B}_n\times\mathbb{B}_n\to\mathbb{B}_n}$.
  - Also $f + g = g + f$.

Weitere, aus den Axiomen ableitbare Regeln:

- Existenz neutraler Elemente:
  $\exists \mathbf{0} : x + \mathbf{0} = x,\ x \cdot \mathbf{0} = \mathbf{0} \quad \exists \mathbf{1} : x \cdot \mathbf{1} = x,\ x + \mathbf{1} = \mathbf{1}$
- Doppeltes Komplement:
  $(\sim(\sim x)) = x$
- Eindeutigkeit des Komplements:
  $(x \cdot y = \mathbf{0} \text{ und } x + y = \mathbf{1}) \Rightarrow y = (\sim x)$
- Idempotenz:
  $x + x = x \quad x \cdot x = x$
- de Morgan-Regel:
  $\sim(x + y) = (\sim x) \cdot (\sim y) \quad \sim(x \cdot y) = (\sim x) + (\sim y)$
- Consensus-Regel: / Resolution
  $(x \cdot y) + ((\sim x) \cdot z) = (x \cdot y) + ((\sim x) \cdot z) + (y \cdot z)$
  $(x + y) \cdot ((\sim x) + z) = (x + y) \cdot ((\sim x) + z) \cdot (y + z)$
- Diese Regeln gelten in allen booleschen Algebren!

Dualitätsprinzip bei booleschen Algebren

Prinzip der Dualität

Gilt eine aus den Gesetzen der booleschen Algebra abgeleitete Gleichung p, so gilt auch die zu p duale Gleichung, die aus p hervorgeht durch gleichzeitiges Vertauschen von $+$ und $\cdot$, sowie **0** und **1**.

Consensusregel

- **Beispiel**:
  - $(x \cdot y) + ((\sim x) \cdot z) + (y \cdot z) = (x \cdot y) + ((\sim x) \cdot z)$
  - $(x + y) \cdot ((\sim x) + z) \cdot (y + z) = (x + y) \cdot ((\sim x) + z)$

UNI FREIBURG 9

Boolesche Ausdrücke - allgemein

- Formal vollständige Definition boolescher Ausdrücke
  - Syntax (korrekte Schreibweise) $\rightarrow$ Def. boolescher Ausdrücke $BE(X_n)$
  - Semantik (Bedeutung) $\rightarrow$ Interpretationsfunktion Ψ von $BE(X_n)$

$\rightarrow$ Zweck: Einem Rechner unzweifelhaft „beibringen", was und was nicht ein boolescher Ausdruck ist und was seine Funktion bezüglich einer booleschen Algebra ist.

$\rightarrow$ Zum Beispiel: Unterschied zwischen dem Ausdruck „$\underbrace{(x_1 \cdot (\sim x_2))}_{BE}$" und der Funktion $\underbrace{f = x_1 \wedge \neg x_2}_{\Psi}$.

UNI FREIBURG

Syntax boolescher Ausdrücke

- Sei $X_n = \{x_1, \ldots, x_n\}$ eine endliche Menge von Symbolen/Variablen.
- Sei $A = X_n \cup \{0, 1, +, \cdot, \sim, (,)\}$ ein Alphabet.

Definition

Die Menge $BE(X_n)$ der vollständig geklammerten booleschen Ausdrücke über X_n ist eine Teilmenge von A^*, die folgendermaßen induktiv definiert ist:

- $0, 1$ und $x_i \in X_n$ $i = 1, \ldots, n$ sind boolesche Ausdrücke
- Sind g und h boolesche Ausdrücke, so auch
  - die Disjunktion $(g + h)$,
  - die Konjunktion $(g \cdot h)$,
  - die Negation $(\sim g)$.

11

Schreibweise von $BE(X_n)$

- **Konvention**: Negation $\sim$ bindet stärker als Konjunktion $\cdot$, Konjunktion $\cdot$ bindet stärker als Disjunktion $+$.
  - $\rightarrow$ Klammern können weggelassen werden, ohne dass Mehrdeutigkeiten entstehen.
- Je nach Kontext (betrachtete boolesche Algebra) schreibt man auch
  - statt $0, 1$: Die entsprechenden neutralen Elemente,
  - statt $\cdot$: $\wedge, \cap$,
  - statt $+$: $\vee, \cup$,
  - statt $\sim x$: $\neg x, x^C, x', \overline{x}$.

$\rightarrow$ So „vereinfachte" Ausdrücke entsprechen zwar nicht genau der obigen Definition, es gibt aber für jeden solchen Ausdruck einen äquivalenten vollständig geklammerten Ausdruck im Sinne der Definition.

- **Beispiel**: Der äquivalente vollständige geklammerte Ausdruck für „$x_1 \wedge \neg x_2$" wäre „$(x_1 \cdot (\sim x_2))$".

Semantik boolescher Ausdrücke

typischerweise $\mathbb{B}_n$

- Sei $\widetilde{M} = (M, \cdot, +, \sim)$ eine beliebige boolesche Algebra.
- Seien $0, 1 \in M$ die neutralen Elemente von B.

Definition

Jedem booleschen Ausdruck $BE(X_n)$ kann durch eine Interpretationsfunktion $\Psi : BE(X_n) \to M_n$ eine boolesche Funktion $M_n : M^n \to M$ zugeordnet werden.

$\mathbb{B}^n \to \mathbb{B}$

Ψ wird folgendermaßen induktiv definiert:

- $\Psi(0) = \mathbf{0}$; $\Psi(1) = \mathbf{1}$;
  $\Psi(x_i)(\alpha_1, \ldots, \alpha_n) = \alpha_i$ für alle $\alpha \in M^n$ (Projektion)
- $\Psi((g + h)) = \Psi(g) + \Psi(h)$ (Disjunktion)
- $\Psi((g \cdot h)) = \Psi(g) \cdot \Psi(h)$ (Konjunktion)
- $\Psi((\sim g)) = \sim (\Psi(g))$ (Negation)

Interpretation boolescher Ausdrücke

- Sei e ein boolescher Ausdruck.
  - $\Psi(e)(\alpha)$ für ein $\alpha \in M^n$ ergibt sich durch Ersetzen von x_i durch α_i in e, für alle i und Rechnen in der booleschen Algebra $\widetilde{M}$.
  - Gilt $\Psi(e) = f$ für eine boolesche Funktion $f \in M_n$, so sagen wir, dass e ein boolescher Ausdruck für f ist, bzw. dass e die boolesche Funktion f beschreibt.

    n-elem. Tupel aus M
  - Zwei boolesche Ausdrücke e_1 und e_2 heißen äquivalent ($e_1 \equiv e_2$) genau dann, wenn $\Psi(e_1) = \Psi(e_2)$.
    Sie sind gleich, wenn $e_1 = e_2$.
- Wir betrachten folgend nur noch die Interpretation in $B = (\mathbb{B}, \wedge, \vee, \neg)$.

-14

Boolesche Ausdrücke $\leftrightarrow$ boolesche Funktionen

Lemma 1

Zu jedem booleschen Ausdruck $e \in BE(X_n)$ existiert eine boolesche Funktion f, die durch e beschrieben wird.

- **Beweis**: $f := \Psi(e)$

Lemma 2

Zu jeder booleschen Funktion f existiert ein boolescher Ausdruck, der f beschreibt.

Minterme

BE

- **Beweis**: Es gilt: $f = \Psi(\sum_{\alpha \in ON(f)} m(\alpha))$.

  m.a.W. Die DNF ist ein Boolescher Ausdruck.

  mit anderen Worten

-15

Zusammenhang mit Schaltkreisen

Lemma 3

Zu jedem booleschen Ausdruck $e \in BE(X_n)$ gibt es einen kombinatorischen Schaltkreis, der e implementiert.

$e \in BE(X_n) \rightsquigarrow f = \varphi(e)$

- **Beweis**: Übung

$\uparrow \downarrow SK_f$

- Zu jeder booleschen Funktion gibt es einen kombinatorischen Schaltkreis, der sie implementiert (zum Beispiel zweistufige Umsetzung der DNF/KDNF).
- Zu jedem kombinatorischen Schaltkreis gibt es sowohl eine boolesche Funktion, als auch einen boolescher Ausdruck.

Kapitel 7

Formale Spezifikation von Hardware:

1. Boolesche Ausdrücke
2. **Binäre Entscheidungsdiagramme (BDDs)**
3. Anwendung: Formale Verifikation

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Motivation: Eindeutigkeit der Darstellung boolescher Funktionen

- Die Darstellung einer gegebenen booleschen Funktion als Schaltkreis oder als boolescher Ausdruck ist im Allgemeinen nicht eindeutig.
- **Beispiel**: „$x_1 \cdot \sim x_2 + x_3$" und „$x_1 \cdot \sim x_2 + x_3 + x_3$".
- Wir kennen eindeutige Darstellungen einer booleschen Funktion.
- **Zum Beispiel**:
  - Funktionstabelle
  - Kanonische disjunktive Normalform (alle Minterme) KNF
- **Aber**: Diese eindeutigen Darstellungen sind „sehr sperrig".

  $\Rightarrow$ 2^n Einträge/alle Minterme für Funktionen in n Variablen.
- **Ziel**: Finde eine eindeutige, aber kompakte Darstellung boolescher Funktionen.

Wozu Eindeutigkeit?

- Zur schnellen Überprüfung, ob zwei boolesche Funktionen äquivalent sind.

- **Beispiel**:
  - Ein Designer hat Optimierungen an der Hardware vorgenommen und 15 Gatter gespart. Hat er dabei vielleicht die Funktionalität verändert?

  → Erzeuge eindeutige Darstellung für alten und neuen Block und vergleiche.

→ Dieses Vorgehen nennt man formalen Äquivalenzcheck.

Illustration: Formaler Äquivalenztest

Eindeutige Darstellung der durch C_1 realisierten booleschen Funktion.

Eindeutige Darstellung der durch C_2 realisierten booleschen Funktion.

Binäre Entscheidungsdiagramme (Binary Decision Diagrams)

im Vgl. zur Fkt.-Tabelle

- BDDs repräsentieren boolesche Funktionen eindeutig und (oft) kompakt zugleich.

  unter gew. Voraussetzungen

  → Enthält genau die gleiche Information, wie eine Funktionstabelle.

- Es gibt Verfahren, um schnell ein BDD aus einem Schaltkreis zu erzeugen.

  → Man muss nicht erst die Funktionstabelle erzeugen.

- Es existieren Software-Packages, die Erzeugung und Manipulation von BDDs unterstützen.
  - CUDD von der Colorado University: `http://vlsi.colorado.edu/~fabio/CUDD/cuddIntro.html`
  - Zahlreiche Optimierungen bei Cache-Ausnutzung, Garbage Collection, usw.

UNI FREIBURG 5

Binary Decision Diagram – Syntax

- Sei $X_n = \{x_1, \ldots, x_n\}$ eine endliche Menge von Variablen.

Definition

Ein BDD ist

- ein azyklischer gerichteter Graph $G = (V, F)$ mit
  - genau einer Wurzel, ⇝ entspricht d. repräsentierten bool. Fkt. bzw. Schaltkreis-ausgang
  - $outdeg(v) = 2$ für alle inneren Knoten v.
- Jeder Knoten v hat eine Markierung
  - $label(v) = \begin{cases} x_i \in X_n, & v \text{ ist innerer Knoten} \\ c \in \{0,1\}, & v \text{ ist Blatt} \end{cases}$
- Die Nachfolger (Kinder) eines inneren Knoten v sind
  - das Low-Kind: $low(v)$,
  - das High-Kind: $high(v)$.

UNI FREIBURG 6

BDDs: Semantik

- Gegeben sei ein BDD.

Definition

- Sei f_v die Funktion, die ein Teil-BDD ausgehend von Knoten v beschreibt.
  - Ist v ein Blatt, so beschreibt v die konstante Funktion, die jede Variablenbelegung auf $label(v) \in \{0, 1\}$ abbildet.
  - Ist v ein innerer Knoten mit $label(v) = x_j$, so gilt die Kompositionsregel: $f_v = (x_j \wedge f_{high(v)}) \vee (x'_j \wedge f_{low(v)})$.

BDDs: Beispiel

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

UNI FREIBURG

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs: Beispiel

$$f_v = (x_j \wedge f_{high(v)}) \vee (x_j' \wedge f_{low(v)})$$

BDDs von typischen Funktionen

Seien x_1, x_2 beliebige boolsche Variablen.

$f(x_1) = x_1$

x_1:

UNI FREIBURG

BDDs von typischen Funktionen

Seien x_1, x_2 beliebige boolsche Variablen.

$f(x_1) = x_1$:

x_1':

UNI FREIBURG

BDDs von typischen Funktionen

Seien x_1, x_2 beliebige boolsche Variablen.

$f(x_1, x_2) = x_1 \cdot x_2$

x_1:

x_1':

$x_1 \cdot x_2$:

-19

BDDs von typischen Funktionen

Seien x_1, x_2 beliebige boolsche Variablen.

x_1:

x_1':

$x_1 \cdot x_2$:

$x_1 + x_2$:

BDDs von typischen Funktionen

Seien x_1, x_2 beliebige boolsche Variablen.

x_1:

x_1':

$x_1 \cdot x_2$:

Reihenfolge: x_1, x_2

Reihenfolge x_2, x_1:

$x_1 + x_2$:

$x_1 \oplus x_2$:

21

Variablenordnung

Definition

- Ein BDD heißt geordnet, wenn auf jedem Pfad von der Wurzel zu einem Blatt jede Variable höchstens einmal (oder keinmal) als Markierung vorkommt und die Variablen stets in der selben Reihenfolge abgefragt werden.
- Diese Reihenfolge heißt Variablenordnung.

UNI FREIBURG

Beispiel für unterschiedliche Variablenordnung

$$x_1x_2x_3 + x_1x_2x_3'x_4 + x_1x_2'x_4 + x_1'x_2'x_4 + x_1'x_2x_3'x_4$$

Variablenordnung

x_1, x_2, x_3, x_4

geordnet

23

Beispiel für unterschiedliche Variablenordnung

$$x_1x_2x_3 + x_1x_2x_3'x_4 + x_1x_2'x_4 + x_1'x_2'x_4 + x_1'x_2x_3'x_4$$

Variablenordnung

x_1, x_2, x_3, x_4

$$x_1x_4 + x_1x_2x_3x_4' + x_1'x_2'x_4 + x_1'x_2x_3'x_4$$

Variablenordnung

x_1, x_4, x_2, x_3

Beispiel für unterschiedliche Variablenordnung

Variablenordnung

x_1, x_2, x_3, x_4

Variablenordnung

x_1, x_4, x_2, x_3

$\Rightarrow$ Beide BDDs beschreiben die boolesche Funktion $x_1x_2x_3 + x_2'x_4 + x_3'x_4$.

Vollständiges BDD

Fkt.-Tabelle

x_1	x_2	x_3	f
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

- Ist ein geordnetes BDD, wobei alle Pfade von der Wurzel zu einem Blatt maximale Länge haben und $indeg(v) = 1$ für alle Knoten v.
- Entspricht genau der Funktionstabelle (Beweis klar)

Zusammenhang: BDD $\leftrightarrow$ Boolesche Funktion

Lemma 1

Jedes (geordnete) BDD stellt eine boolesche Funktion dar.

v mit x_j markiert!

- **Beweis**: Ist v die Wurzel des BDDs, dann erhält man mit der Kompositionsregel die dargestellte boolesche Funktion f_v.

$f_v = (x_j \wedge f_{High}) \vee (\overline{x_j} \wedge f_{low})$

Lemma 2

Zu jeder booleschen Funktion existiert ein (geordnetes) BDD, das diese darstellt.

- **Beweis**: Konstruiere vollständiges BDD aus Funktionstabelle.

27

Eindeutigkeit von BDDs

- Nicht geordnete BDDs sind nicht eindeutige Darstellungen, ebenso BDDs mit unterschiedlicher (nicht fester) Variablenordnung.

- Die vollständigen BDDs sind eindeutige Darstellungen (da die Funktionstabelle eindeutig ist).

- **Aber**: Ineffizient $\rightarrow$ Reduktion von BDDs

UNI FREIBURG

Reduzierte BDDs

Idee: Stelle Information möglichst kompakt dar, „isomorphe Teil-BDDs" werden identifiziert.

Redundant

$f = (x \cdot f_{high}) \vee (\bar{x} \cdot f_{low})$

$= x \cdot G \vee \bar{x} \cdot G$

$= G$

Definition

Ein BDD heißt reduziert, wenn es

- keinen nichtterminalen Knoten v gibt, mit Label x und $f_{high(v)} = f_{low(v)}$.
- keine verschiedenen Knoten v und w gibt, die gleich markiert sind und deren low- und high-Kind (falls existent) jeweils identisch sind.

Isomorphie

29

Beispiel für reduzierte und nicht reduzierte BDDs (1/2)

Ordnung: x_2, x_3, x_4, x_1

dann wird x_4 redundant!

x_3 wird redundant!

„Die machen alle dasselbe!"

↳ isomorph!

Fkt.: $\overline{x_4}$

„beide berechnen $\overline{x_1}$"

30

Beispiel für reduzierte und nicht reduzierte BDDs (1/2)

Beispiel für reduzierte und nicht reduzierte BDDs (1/2)

32

Beispiel für reduzierte und nicht reduzierte BDDs (2/2)

Beispiel für reduzierte und nicht reduzierte BDDs (2/2)

Beispiel für reduzierte und nicht reduzierte BDDs (2/2)

Beispiel: Reduktion eines BDDs (1/7)

Beispiel: Reduktion eines BDDs (1/7)

Beispiel: Reduktion eines BDDs (2/7)

Beispiel: Reduktion eines BDDs (3/7)

Beispiel: Reduktion eines BDDs (4/7)

Beispiel: Reduktion eines BDDs (5/7)

Beispiel: Reduktion eines BDDs (5/7)

Beispiel: Reduktion eines BDDs (6/7)

Beispiel: Reduktion eines BDDs (7/7)

Beispiel: Reduktion eines BDDs (7/7)

Satz von Bryant (1986)

Satz

ROBDDs (Reduced Ordered BDDs, geordnete, reduzierte BDDs) sind kanonische Darstellungen boolescher Funktionen.

- Ohne Beweis.
- **Bedeutung**: Für eine fixe Variablenordnung ist ein ROBDD eine eindeutige Darstellung für eine boolesche Funktion.
- **Notation**: Ab sofort bezeichen wir ROBDDs als BDDs.

Kofaktoren und Shannon-Zerlegung

- Für eine boolesche Funktion $f : \mathbb{B}^n \to \mathbb{B}$ heißt $f_{x_i=1} : \mathbb{B}^n \to \mathbb{B}$ definiert durch $f_{x_i=1}(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$ für alle $\alpha \in \{0,1\}^n$ der Kofaktor von f nach $x_i = 1$.

- Entsprechend heißt $f_{x_i=0} = f(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$ der Kofaktor von f nach $x_i = 0$.

Shannonscher Entwicklungssatz

Es gilt für beliebiges f:

$f(x_1 \ldots, x_n)$

pos. kof. neg. kof.

$$f = (x_i \wedge f_{x_i=1}) \vee (x_i' \wedge f_{x_i=0})$$

$1 \wedge f_{x_i=1}$ $0 \wedge \ldots$

$x_i = 1 : f = f_{x_i=1}$

analog $x_i = 0$: $f = f_{x_i=0}$

- $f = (x_i \wedge f_{x_i=1}) \vee (x_i' \wedge f_{x_i=0})$ heißt Shannon-Zerlegung von f.

Zusammenhang Kompositionsregel, Kofaktoren und Shannon-Zerlegung

- Sei v ein innerer Knoten eines geordneten BDDs, der mit x_i markiert ist.
- Dann kommt x_i in Kindern von v nicht vor (sonst mehrfaches Vorkommen auf dem gleichen Pfad).

- Also sind die Subfunktionen $f_{high(v)}$, $f_{low(v)}$ von f_v von x_i unabhängig, d.h. für alle $\alpha \in \{0,1\}^n$ gilt:
  - $f_{high(v)}(\alpha_1,\ldots,\alpha_{i-1},1,\alpha_{i+1},\ldots,\alpha_n) = f_{high(v)}(\alpha_1,\ldots,\alpha_{i-1},0,\alpha_{i+1},\ldots,\alpha_n)$
  - $f_{low(v)}(\alpha_1,\ldots,\alpha_{i-1},1,\alpha_{i+1},\ldots,\alpha_n) = f_{low(v)}(\alpha_1,\ldots,\alpha_{i-1},0,\alpha_{i+1},\ldots,\alpha_n)$
- Es folgt dann: $f_{high(v)} = \underbrace{f_{v,x_i=1}}_{\text{pos. Kofaktor}}$, $f_{low(v)} = \underbrace{f_{v,x_i=0}}_{\text{neg. Kofaktor}}$.
- Somit wird an v die Shannon-Zerlegung berechnet:
  $f_v = (x_i \wedge f_{high(v)}) \vee (x_i' \wedge f_{low(v)}) = (x_i \wedge f_{v,x_i=1}) \wedge (x_i' \wedge f_{v,x_i=0})$.

Konstruktion von BDDs

Variablenordnung $x_1, \dots, x_4$

- Über die Kofaktoren.
  - **Beispiel**: Um ein bdd_f von $f = x_1x_2x_3 + x_2'x_4 + x_3'x_4$ bzgl. der Variablenordnung x_1, x_2, x_3, x_4 zu konstruieren, konstruiere BDDs von $f_{x_1=1} = x_2x_3 + x_2'x_4 + x_3'x_4$ und $f_{x_1=0} = x_2'x_4 + x_3'x_4$. Sie stellen die Söhne des Knotens x_1 dar. Wende dies rekursiv an.

$f_{x_1=1, x_2=0} = x_4 + x_3' x_4$

$f_{x_1=1, x_2=1} = x_3 + x_3' x_4$

- Aus einem booleschen Ausdruck über boolesche Operationen.
- Aus einem Schaltkreis über boolesche Operationen (Symbolische Simulation).

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

Variablenordnung: a, b, c

f(a, b, c)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

c	$f_{a=1,b=1}$
0	1
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

c	$f_{a=1,b=1}$
0	1
1	1

c	$f_{a=1,b=0}$
0	0
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

c	$f_{a=1,b=1}$
0	1
1	1

c	$f_{a=1,b=0}$
0	0
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

c	$f_{a=1,b=1}$
0	1
1	1

c	$f_{a=1,b=0}$
0	0
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

c	$f_{a=1,b=1}$
0	1
1	1

c	$f_{a=1,b=0}$
0	0
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (1/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=1}(b,c) = b \cdot f_{a=1,b=1}(c) + b' \cdot f_{a=1,b=0}(c)$.

b	c	$f_{a=1}$
0	0	0
0	1	1
1	0	1
1	1	1

c	$f_{a=1,b=1}$
0	1
1	1

c	$f_{a=1,b=0}$
0	0
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot \underline{f_{a=0,b=1}}(c) + b' \cdot \underline{f_{a=0,b=0}}(c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

c	$f_{a=0,b=1}$
0	0
1	1

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

c	$f_{a=0,b=1}$
0	0
1	1

c	$f_{a=0,b=0}$
0	0
1	0

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

c	$f_{a=0,b=1}$
0	0
1	1

c	$f_{a=0,b=0}$
0	0
1	0

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

c	$f_{a=0,b=1}$
0	0
1	1

c	$f_{a=0,b=0}$
0	0
1	0

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

c	$f_{a=0,b=1}$
0	0
1	1

c	$f_{a=0,b=0}$
0	0
1	0

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (2/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.
- $f_{a=0}(b,c) = b \cdot f_{a=0,b=1}(c) + b' \cdot f_{a=0,b=0}(c)$.

b	c	$f_{a=0}$
0	0	0
0	1	0
1	0	0
1	1	1

c	$f_{a=0,b=1}$
0	0
1	1

c	$f_{a=0,b=0}$
0	0
1	0

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (3/3)

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (3/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (3/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD des Carry-Bits $f := fa_1$ eines Volladierers aus Kofaktoren (3/3)

- $f(a,b,c) = a \cdot f_{a=1}(b,c) + a' \cdot f_{a=0}(b,c)$.

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

BDD aus einem booleschen Ausdruck

- Konstruiere BDD bdd_f von $f = x_1x_2x_3 + x_2'x_4 + x_3'x_4$.
  - Generiere bdd_{x_1}, bdd_{x_2}, bdd_{x_3}, bdd_{x_4}.
  - Berechne $bdd_{x_1x_2} := AND(bdd_{x_1}, bdd_{x_2})$.
  - Berechne $bdd_{x_1x_2x_3} := AND(bdd_{x_1x_2}, bdd_{x_3})$.
  - Berechne $bdd_{x_2'} := NOT(bdd_{x_2})$.
  - Berechne $bdd_{x_2'x_4} := AND(bdd_{x_2'}, bdd_{x_4})$.
  - Berechne $bdd_{x_3'} := NOT(bdd_{x_3})$.
  - Berechne $bdd_{x_3'x_4} := AND(bdd_{x_3'}, bdd_{x_4})$.
  - Berechne $bdd_{x_1x_2x_3+x_2'x_4} := OR(bdd_{x_1x_2x_3}, bdd_{x_2'x_4})$.
  - Berechne $bdd_f := OR(bdd_{x_1x_2x_3+x_2'x_4}, bdd_{x_3'x_4})$.
- Berechnung von AND, OR, NOT: Später!

BDD aus Schaltkreis: Symbolische Simulation

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,
bdd_{11}
$:= XOR(bdd_{x_9}, bdd_{x_{10}})$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,
bdd_{11}
$:= XOR(bdd_{x_9}, bdd_{x_{10}})$,
bdd_{out_1}
$:= OR(bdd_{x_1}, bdd_{x_{11}})$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,
bdd_{11}
$:= XOR(bdd_{x_9}, bdd_{x_{10}})$,
bdd_{out_1}
$:= OR(bdd_{x_1}, bdd_{x_{11}})$,
bdd_{12}
$:= OR(bdd_{x_6}, bdd_{x_7})$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,
bdd_{11}
$:= XOR(bdd_{x_9}, bdd_{x_{10}})$,
bdd_{out_1}
$:= OR(bdd_{x_1}, bdd_{x_{11}})$,
bdd_{12}
$:= OR(bdd_{x_6}, bdd_{x_7})$,
bdd_{13}
$:= AND(bdd_{x_{10}}, NOT(bdd_{x_8}))$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,
bdd_{11}
$:= XOR(bdd_{x_9}, bdd_{x_{10}})$,
bdd_{out_1}
$:= OR(bdd_{x_1}, bdd_{x_{11}})$,
bdd_{12}
$:= OR(bdd_{x_6}, bdd_{x_7})$,
bdd_{13}
$:= AND(bdd_{x_{10}}, NOT(bdd_{x_8}))$,
bdd_{14}
$:= AND(bdd_{x_{12}}, bdd_{x_8})$,

BDD aus Schaltkreis: Symbolische Simulation

BDD-Operationen:

$bdd_{x_1}, bdd_{x_2}, \ldots, bdd_{x_8}$,
bdd_9
$:= XOR(bdd_{x_2}, bdd_{x_3})$,
bdd_{10}
$:= AND(bdd_{x_4}, bdd_{x_5})$,
bdd_{11}
$:= XOR(bdd_{x_9}, bdd_{x_{10}})$,
bdd_{out_1}
$:= OR(bdd_{x_1}, bdd_{x_{11}})$,
bdd_{12}
$:= OR(bdd_{x_6}, bdd_{x_7})$,
bdd_{13}
$:= AND(bdd_{x_{10}}, NOT(bdd_{x_8}))$,
bdd_{14}
$:= AND(bdd_{x_{12}}, bdd_{x_8})$,
bdd_{out_2}
$:= OR(bdd_{x_{13}}, bdd_{x_{14}})$.

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

87

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

91

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Beispiel: BDD des Carry-Bits $f := fa_1$ eines FAs aus Schaltkreis

Übrigens …

- Wir haben soeben einen Äquivalenzcheck durchgeführt!

a	b	c	fa_1	fa_0
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Spezifikation

Implementierung

Realisierung von booleschen Operationen zwischen BDDs

- Gegeben BDDs a und b, berechne BDD $c = AND(a,b)$.
- Erste Option: Berechne die Funktionstabelle von $(a \cdot b)$, erzeuge daraus das BDD mit der Kofaktor-Methode $\rightarrow$ sehr ineffizient!
- Besserer Ansatz: If-Then-Else-Funktion (ITE).
  - $ITE(F,G,H) := FG + F'H$.
  - Alle binären Operationen sind auf ITE zurückführbar.
    - $AND(F,G) = ITE(F,G,0)$ $= F \cdot G + F' \cdot 0 = F \cdot G$ ✓
    - $OR(F,G) = ITE(F,1,G)$ $= F \cdot 1 + F' \cdot G = F + F' \cdot G$
    - $NOT(F) = ITE(F,0,1)$ $= F \cdot 0 + F' \cdot 1 = F'$ $= F + G$ ✓
    - $XOR(F,G) = ITE(F,G',G)$ $= F \cdot G' + F' \cdot G$ ✓

97

Realisierung von booleschen Operationen zwischen BDDs

- Gegeben BDDs a und b, berechne BDD $c = AND(a,b)$
- Erste Option: Berechne die Funktionstabelle von $(a \cdot b)$, erzeuge daraus das BDD mit der Kofaktor-Methode $\rightarrow$ sehr ineffizient!
- Besserer Ansatz: If-Then-Else-Funktion (ITE).
  - $ITE(F,G,H) := FG + F'H$.
  - Alle binären Operationen sind auf ITE zurückführbar.
    - $AND(F,G) = ITE(F,G,0)$
    - $OR(F,G) = ITE(F,1,G)$
    - $NOT(F) = ITE(F,0,1)$
    - $XOR(F,G) = ITE(F,G',G)$

Berechnung von *ITE* auf BDDs-Prinzip

- Gegeben sind drei BDDs F, G und H mit der gleichen Variablenordnung. Gesucht ist BDD für $ITE(F,G,H)$.
- Es gilt für eine Variable x:
- $$\begin{aligned} & ITE(F,G,H) \\ &= FG + F'H \\ &= x(FG+F'H)_{x=1} + x'(FG+F'H)_{x=0} \\ &= x(F_{x=1}G_{x=1} + (F_{x=1})'H_{x=1}) + x'(F_{x=0}G_{x=0} + (F_{x=0})'H_{x=0}) \\ &= x \cdot ITE(F_{x=1},G_{x=1},H_{x=1}) + x' \cdot ITE(F_{x=0},G_{x=0},H_{x=0}). \end{aligned}$$

  pos. Kofaktor

  neg. Kofaktor
- *ITE*-Berechnung im vollständigen BDD:
  - Sei x die oberste Variable in BDDs F, G und H.
  - BDDs für $F_{x=1}, G_{x=1}, H_{x=1}, F_{x=0}, G_{x=0}, H_{x=0}$ sind Kinder von x.
  - Berechne BDDs $ITE(F_{x=1},G_{x=1},H_{x=1})$ und $ITE(F_{x=0},G_{x=0},H_{x=0})$ rekursiv. x mit diesen BDDs als Kinder ist das gesuchte BDD.

ITE auf reduzierten BDDs

- $ITE(F,G,H)$
  $= x \cdot ITE(F_{x=1},G_{x=1},H_{x=1}) + x' \cdot ITE(F_{x=0},G_{x=0},H_{x=0})$.

- Rekursive Vorgehensweise:
  - Berechne BDDs $ITE(F_{x=1},G_{x=1},H_{x=1})$ und $ITE(F_{x=0},G_{x=0},H_{x=0})$.
  - Falls $\underbrace{ITE(F_{x=1},G_{x=1},H_{x=1})}_{ITE_1} = \underbrace{ITE(F_{x=0},G_{x=0},H_{x=0})}_{ITE_0}$, so ist $ITE(F,G,H) = ITE(F_{x=1},G_{x=1},H_{x=1}) = ITE(F_{x=0},G_{x=0},H_{x=0})$.
  - Redundanz-Check! Sonst generiere einen neuen Knoten x, dessen high-Kante auf $ITE(F_{x=1},G_{x=1},H_{x=1})$ und low-Kante auf $ITE(F_{x=0},G_{x=0},H_{x=0})$ zeigt.
  - **Terminalfälle**:
    $ITE(1,F,G) = ITE(0,G,F) = ITE(F,1,0) = ITE(G,F,F) = F$.

ITE-Berechnung: Beispiel (1/2)

$F :=$ $a \cdot b$

$G :=$ $(a \oplus b) \wedge c$

$R :=$

- Wir haben vorhin gerechnet: $R = OR(F, G)$
- Dies entspricht: $R = ITE(F, 1, G)$. $= F \cdot 1 + F' G = F + G$
- Wir wollen nun die rekursive *ITE*-Berechnung nachvollziehen.
- Es liegt kein Terminalfall vor, obere Variable: a.

101

ITE-Berechnung: Beispiel (2/2)

$F :=$

$G :=$

$R :=$

- Berechne zunächst rekursiv $ITE(F_{a=1}, 1_{a=1}, G_{a=1})$.

$F_{a=1} =$

$, 1_{a=1} = 1,$ $G_{a=1} =$

- Rechne rekursiv mit Variable b weiter:
  $ITE(F_{a=1}, 1_{a=1}, G_{a=1}) = b \cdot ITE(F_{a=1,b=1}, 1_{a=1,b=1}, G_{a=1,b=1}) +$
  $b' \cdot ITE(F_{a=1,b=0}, 1_{a=1,b=0}, G_{a=1,b=0})$.

← Shannon-Zerlegung

102

Beispiel: $ITE(F_{a=1}, 1_{a=1}, G_{a=1})$

$F_{a=1} =$

$, 1_{a=1} = 1,$ $G_{a=1} =$

- $ITE(F_{a=1}, 1_{a=1}, G_{a=1}) = b \cdot ITE(F_{a=1,b=1}, 1_{a=1,b=1}, G_{a=1,b=1})$
  $+ b' \cdot ITE(F_{a=1,b=0}, 1_{a=1,b=0}, G_{a=1,b=0})$.
  - $F_{a=1,b=1} = 1_{a=1,b=1} = 1, G_{a=1,b=1} = 0,$
    $ITE(1,1,0) = 1$ **(Terminalfall)**.
  - $F_{a=1,b=0} = 0, 1_{a=1,b=0} = 1, G_{a=1,b=0} = c =$
    $ITE(0,1,c) = c$ **(Terminalfall)**.

$ITE(F, G, H)$
$(F_s, 1_s, G_s)$

- Insgesamt:
  $ITE(F_{a=1}, 1_{a=1}, G_{a=1}) =$

Beispiel: $ITE(F_{a=0}, 1_{a=0}, G_{a=0})$

$F :=$

$G :=$

$R :=$

- Berechne zunächst rekursiv $ITE(F_{a=0}, 1_{a=0}, G_{a=0})$.

$F_{a=0} = 0, \quad 1_{a=0} = 1, \quad G_{a=0} =$

Ein **Terminalfall** liegt vor:
$ITE(0, 1, G_{a=0}) = G_{a=0} =$

Beispiel - Ende

- $ITE(F,1,G) = a \cdot ITE(F_{a=1},1_{a=1},G_{a=1}) + a' \cdot ITE(F_{a=0},1_{a=0},G_{a=0})$.

$ITE(F_{a=1},1_{a=1},G_{a=1}) =$

$ITE(F_{a=0},1_{a=0},G_{a=0}) =$

- Durch die Verwendung der sogenannten Computed Tables (s.u.) sind die berechneten BDDs bereits reduziert:

- Somit muss *ITE* nur noch einen Knoten *a* einfügen und seine ausgehenden Kanten „richtig lenken”.

Zur Komplexität von *ITE*

- Bei der rekursiven Konstruktion von *ITE* überprüft man, ob die BDDs $ITE(F_{x=1}, G_{x=1}, H_{x=1})$ und $ITE(F_{x=0}, G_{x=0}, H_{x=0})$ vielleicht bereits generiert wurden und in der sogenannten Computed Table (CT) vorliegen.

- Nur wenn dies nicht der Fall ist, werden die BDDs erzeugt und in die CT eingefügt.

- Implementiert man dies effizient, wird die Komplexität von *ITE* zu $O(|F| \cdot |G| \cdot |H|)$.
  - Ohne Beweis.

- Somit lässt sich etwa die Komplexität von $AND(F,G) = ITE(F,G,0)$ durch $O(|F| \cdot |G|)$ abschätzen (0 ist das BDD für die konstante 0-Funktion, das aus 1 Knoten besteht.)

106

ITE-Algorithmus

$F \cdot G + F' \cdot H = 1 \cdot G + 0 \cdot H$

$ITE(F, G, H)\{$

if $(F == 1)$ **return** G; // Überprüfe erst 4 Terminalfälle.
if $(F == 0)$ **return** H;
if $((G == 1)$ **and** $(H == 0))$ **return** F;
if $(G == H)$ **return** G;

$x = Top_Variable(F, G, H)$; // Gleiche Variablenordnung.
$high = ITE(F_{x=1}, G_{x=1}, H_{x=1})$;
$low = ITE(F_{x=0}, G_{x=0}, H_{x=0})$;
if $(high == low)$ **return** low;
$R = Find_Or_Add_in_Computed_Table(x, high, low)$;
return R;

$\}$

Redundanz-Check:

Größe von BDDs

- Oft exponentiell.
- Hängt stark von der Variablenordnung ab.
  - Siehe Beispiel auf der nächsten Folie.
- Für viele in der Praxis vorkommende Funktionen sind BDDs zumindest für einige Variablenordnungen kompakt.
- BDD-Minimierung: Finden einer „guten” Variablenordnung (NP-vollständiges Problem).
  - Exakte und heuristische Verfahren.
  - Für einige Funktionen, u.a. Multiplizierer, ist BDD-Größe für jede Variablenordnung exponentiell.

108

Einfluss der Variablenordnung

- **Beispiel**: $f^n(x_1, \ldots, x_{2n}) = x_1 x_{n+1} + x_2 x_{n+2} + \cdots + x_n x_{2n}$.

Einfluss der Variablenordnung

$n=3$

$x_1, \dots, x_6$

- **Beispiel**: $f^n(x_1,\dots,x_{2n}) = x_1x_{n+1} + x_2x_{n+2} + \cdots + x_nx_{2n}$.

$= x_1x_4 + x_2x_5 + x_3x_6$

exponentielle Größe

$x_1 \dots x_6$

110

Einfluss der Variablenordnung

- **Beispiel**: $f^n(x_1,\ldots,x_{2n}) = x_1x_{n+1} + x_2x_{n+2} + \cdots + x_nx_{2n}$.

exponentielle Größe

lineare Größe

$x_1, x_4, x_2, x_5, x_3, x_6$

111

Schaltkreis direkt aus BDD

Schaltkreis direkt aus BDD

Schaltkreis direkt aus BDD

Schaltkreis direkt aus BDD

Schaltkreis direkt aus BDD

Schaltkreis direkt aus BDD

… beschreibt die boolesche Funktion $x_1' x_2' x_3' + x_1' x_2 + x_1 x_2'$.

Kapitel 7

Formale Spezifikation von Hardware:

1. Boolesche Ausdrücke
2. Binäre Entscheidungsdiagramme (BDDs)
3. **Anwendung: Formale Verifikation**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Formale Verifikation

- **Ziel**: Mit formalen Methoden weitgehend automatisch feststellen, ob der Entwurf korrekt ist.
  - **Hier**: Nur grobe Prinzipien, es gibt eine Vielzahl von Weiterentwicklungen, die auch im Einsatz sind.
- Äquivalenz-Check: Verleich der Spezifikation mit der Implementierung.
  - **Hier**: Komplexeres Beispiel (ein „Slice" der ReTI-CPU) mit Hilfe von BDDs.
- Eigenschafts-Check: Überprüfung, ob bestimmte Eigenschaften gelten.
  - **Hier**: Abwesenheit von Bus Contention auf einem Bus.

Schaltrealisierung der ALU

arithm. Operation

Bitweise Operationen

O.te Bit

O.te Bit

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

„0-tes Slice der ALU”

- Das „0-te Slice” ist der Teil der kombinatorischen Logik, der den 0. Ausgang der ALU berechnet.
- Das Vorgehen für die gesamte CPU wäre identisch, die BDDs jedoch (sehr) viel größer.
- **Vorgehen**:
  - Erstelle die Funktionstabelle für den 0. Ausgang der ALU („Spezifikation”) und berechne das BDD dazu. ≅ RoBDD
  - Bestimme die Hardware, welche den 0. Ausgang ansteuert („Implementierung”) und berechne das BDD dazu.
  - Sind die BDDs gleich, ist die Implementierung korrekt! gg. Spezifikation

Spezifikation für das 0-te Slice

s_2	s_1	s_0	0. Ausgang
0	0	0	$(0\ldots0)_0 = \boxed{0}$
0	0	1	$([b]-[a])_0 = b_0 \oplus a'_0 \oplus 1 = a_0 \oplus b_0$
0	1	0	$([a]-[b])_0 = a_0 \oplus b'_0 \oplus 1 = a_0 \oplus b_0$
0	1	1	$([a]+[b]+c)_0 = a_0 \oplus b_0 \oplus c$
1	0	0	$(a \oplus b)_0 = a_0 \oplus b_0$
1	0	1	$(a \vee b)_0 = a_0 \vee b_0$
1	1	0	$(a \wedge b)_0 = a_0 \wedge b_0$
1	1	1	$(1\ldots1)_0 = \boxed{1}$

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

UNI FREIBURG

5

BDD für die Spezifikation

$s_2 = 0$
alle aud. Variablen = 1
$\Rightarrow$ Fkt.-Wert = 1

- Variablenordnung: $s_2, s_1, s_0, c, a_0, b_0$.
- Reduziert bis auf Terminalknoten (wegen Übersichtlichkeit).

Schaltrealisierung der ALU

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Hardware für das „0-te Slice”

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

BDD für die Schaltrealisierung

$S_2 = 0$, aller anderen Variablen $= 1$
$\Rightarrow$ Fkt.-Wert $= \underline{0}$

- Das BDD entspricht nicht dem für die Spezifikation!
- Irgendwo muss ein Entwurfsfehler sein!

Im Entwurf ist ein Fehler – aber wo?

- Wir wollen nicht nur wissen, dass der Entwurf fehlerhaft ist, sondern den Fehler finden (und dann beheben)!

$0 \otimes 1 = 1$
$1 \otimes 0 = 1$

- Dies wird „Diagnose von Entwurfsfehlern" genannt.
- Ein mögliches Vorgehen: Finde eine Belegung der Eingänge, für die Spezifikation und Implementierung nicht übereinstimmen.
- Wir suchen also eine Belegung von $(s_2, s_1, s_0, c, a_0, b_0)$, für welche gilt:
  $Implem.(s_2, s_1, s_0, c, a_0, b_0) \neq Spez.(s_2, s_1, s_0, c, a_0, b_0)$.
- Mit BDDs ist das ganz einfach: Berechne BDD für
  0 $Implem.(s_2, s_1, s_0, c, a_0, b_0) \oplus Spez.(s_2, s_1, s_0, c, a_0, b_0)$ 1
  und betrachte einen beliebigen Pfad zu 1-Terminalknoten.

bspw. per ITE-Funktion

-10-

Fehlerdiagnose

$s_2 = 0$, alle aucl. Variablen auf 1 → Fk.-Wert = 1

- Ergebnis der XOR-Verknüpfung der beiden BDDs:

tauchen nicht im BDD auf

- Ein Pfad zum 1-Terminal: $s_2 = 0$, $s_1 = 1$, $s_0 = 0$, $c = 0$.
- a_0, b_0 sind unbestimmt; setze z.B. $a_0 = 0$, $b_0 = 0$.
- Die ALU soll also $[a] - [b]$ berechnen (da $s_2 s_1 s_0 = 010$).

11

Simulation der gefundenen Belegung (1/3)

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Simulation der gefundenen Belegung (2/3)

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Simulation der gefundenen Belegung (3/3)

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Analyse der Simulationsergebnisse

gerade Zahl

- Es werden zwei Zahlen subtrahiert, die mit „0” enden. Das Ergebnis soll mit „1” enden.
  ungerade
- Das kann nicht sein, die ALU subtrahiert falsch.
- Die Dateneingänge des Addierers sind richtig.
- Der Übertragseingang des Addierers ist aber falsch, er hätte bei Subtraktion 1 sein müsen!
- Der Fehler muss in der Logik liegen, die den Übertragseingang steuert. Das sind 4 Gatter.
- Tatsächlich sind ein AND- und ein XOR-Gatter vertauscht. Vgl. die (richtige) Folie aus Kap. 3.5.

-15

Original-Folie aus Kapitel 3

s_2	s_1	s_0	
0	0	0	$0\ldots0$
0	0	1	$[b]-[a]$
0	1	0	$[a]-[b]$
0	1	1	$[a]+[b]+c$
1	0	0	$a \oplus b = (a_{n-1} \oplus b_{n-1}, \ldots, a_0 \oplus b_0)$
1	0	1	$a \vee b = (a_{n-1} \vee b_{n-1}, \ldots, a_0 \vee b_0)$
1	1	0	$a \wedge b = (a_{n-1} \wedge b_{n-1}, \ldots, a_0 \wedge b_0)$
1	1	1	$1\ldots1$

Was hat die formale Analyse gebracht?

- Wir mussten den Fehler nach wie vor manuell suchen, ...
- ... allerdings in den 4 Gattern und nicht in der gesamten Schaltung!
- Es gibt (komplexere) Diagnose-Ansätze, die voll-automatisch (oder fast voll-automatisch) arbeiten.
- Außerdem würden wir, wenn wir die Analyse mit der korrigierten Schaltung wiederholen, wissen, dass die Implementierung nun korrekt ist und wir keine weiteren Fehler suchen müssen!

Ist die Analyse den Aufwand wert?

- Es ist sehr kompliziert, BDDs aufzuschreiben und ihre Verknüpfungen auszurechnen.
- Dadurch ist es auch fehleranfällig.
  - Woher weiß man, dass man bei den BDD-Operationen keinen Rechen- oder Schreibfehler gemacht hat?
- **Antwort**: Software-Werkzeuge, die Manipulation von BDDs übernehmen!
  - Diese können BDDs mit Millionen Knoten repräsentieren und in vertretbarer Zeit verarbeiten.
  - Spezifikation und Implementierung werden aus Dateien eingelesen und BDDs automatisch erzeugt/verglichen.
  - Standard in modernen Entwurfsabläufen!

Eigenschaftsprüfung

- **Ziel**: Nachweis, dass eine bestimmte Eigenschaft immer gilt, manchmal gilt oder nie gelten kann.
- Es gibt spezielle Sprachen, um solche Eigenschaften zu formulieren. LTL, CTL, CTL*
- An dieser Stelle soll das Vorgehen am Beispiel von Bus Contention auf Bus L von ReTI illustriert werden.
- Konkret wollen wir zeigen, dass Treiber *PCLd* und *0LD* nie gleichzeitig enabled sind.

UNI FREIBURG

Zur Erinnerung: ReTI-Aufbau

Eigenschaftsprüfung: Bus Contention (1/2)

low-aktiv

E
I[31..24]

- Weise nach, dass es keine Eingangsbelegung gibt, für die $/PCLdoe$ und $/0Ldoe$ beide aktiv sind.
  - $/PCLdoe$ enabled in der Execute-Phase ($E = 1$) für Befehle JUMP ($I[31:30] = 11$), Compute-Befehle ($I[31:30] = 00$) mit $D = PC$ ($I[25:24] = 00$) und für MOVE-Befehl ($I[31:28] = 1011$) mit $S = PC$ ($I[27:26] = 00$).
  - $/0Ldoe$ enabled in der Execute-Phase ($E = 1$) für Befehl LOADI ($I[31:28] = 0111$).

21

Eigenschaftsprüfung: Bus Contention (2/2)

- **Eigenschaft**: Für alle Belegungen der relevanten Signale $(E, I_{31}, I_{30}, I_{29}, I_{28}, I_{27}, I_{26}, I_{25}, I_{24})$ gilt stets:

$$(/PCLdoe(E, I_{30}, I_{29}, I_{28}, I_{27}, I_{26}, I_{25}, I_{24}) \vee /0Ldoe(E, I_{30}, I_{29}, I_{28}, I_{27}, I_{26}, I_{25}, I_{24})) = 1.$$

I_{31} I_{31} 0

OR → $\boxed{1}$

  - **Bedeutung**: Zu jedem Zeitpunkt muss mindestens eines der Signale 1 sein, sie sind nie gleichzeitig 0 (aktiv).

ITE-Fkt.

- **Vorgehen**: Berechne BDD für $/PCLdoe$, BDD für $/0Ldoe$ und die OR-Verknüpfung der beiden BDDs. Diese muss 1 sein, d.h. aus nur einem 1-Terminalknoten bestehen.
  - Falls nicht, liefern die Pfade zum 0-Terminalknoten die Belegungen, für welche die Eigenschaft verletzt ist!

Eigenschaftsprüfung: Diskussion

- Wir haben eine selbstverständliche Aussage bewiesen (Signale bei unterschiedlichen Befehlen aktiv).
  - Der Entwerfer hätte aber, etwa bei der Logik-Optimierung, einen Fehler machen können, die zur Verletzung der Eigenschaft geführt hätte.
- Wir sind noch lange nicht fertig.
  - Auf dem L-Bus und auf anderen Bussen gibt es noch viele Möglichkeiten, wie Bus Contention auftreten kann.
  - Selbst wenn wir sämtliche Quellen für Bus Contention ausschließen, wissen wir noch nicht, dass der Prozessor korrekt implementiert ist. Wir wissen nur, dass keine Bus Contention auftritt.

Formale Verifikation in der Praxis

- Eigene Produktklasse der Entwurfsautomatisierungsindustrie (auch in Deutschland).
- Äquivalenzprüfung ist Routine-Bestandteil beim Entwurf von komplexen Hardware-Produkten.
- Eigenschaftsprüfung spielt im Hardware- und im Software-Bereich eine immer größere Rolle, der Einsatz ist jedoch mit Schwierigkeiten verbunden.
  - Formulierung von Eigenschaften erfordert hochqualifizierte (und teure) Mitarbeiter.
  - Es ist oft nicht klar, wann genug Eigenschaften erstellt wurden und das Produkt als korrekt anzusehen ist.

Zusammenfassung: Formale Spezifikation

- Boolesche Funktionen, boolesche Ausdrücke, kombinatorische Schaltkreise und BDDs sind ineinander transformierbar.
- Formale Verifikation kann Entwurfsqualität enorm steigern und die Entwurfszeiten reduzieren.
- Ein Großteil des Aufwandes kann von einem Rechner geleistet werden.
- Voraussetzung dafür ist eine formal-mathematische Beschreibung, die der Rechner ohne menschliche Hilfe interpretieren kann.

~~Bescherung 4.0~~

~~Smarte Helferlein am nördlichen Polarkreis~~

Wie hat der Weihnachtsmann die ganze Arbeit auch dieses Jahr wieder geschafft?

Albert-Ludwigs-Universität Freiburg

Tobias Schubert, Sabrina Reinshagen
Lehrstuhl für Rechnerarchitektur
Institut für Informatik
Technische Fakultät

Weihnachts-Wertschöpfungskette

- Wunschzettel-Dilemma
- Next Generation Rentierschlitten
- Rentierschlitten-Packstation
- Hermes der Weihnachtsbote
- Smarte Häuser für die optimale Bescherung
- Heute schon an Ostern denken

Wunschzettel-Dilemma

Einmal geschah dem Weihnachtsmann etwas Seltsames. Von Annika bekam er einen Wunschzettel, der ganz anders war als alle Wunschzettel, die er bisher bekommen hatte. Sein Problem: Er verstand Annikas Wünsche nicht!

Da war guter Rat teuer…

[Angelehnt an X. Jiang & A. Clausing, WWU Münster]

Annikas Wunschzettel (Teil 1)

Lieber Weihnachtsmann!

Wenn ich zum Fest von Dir ein Netflix Abo bekomme, dann möchte ich nicht das neue Silbermond-Album haben. Und wenn Du mir ein iPhone 6s bringst, dann möchte ich keine weißen Adidas Superstar bekommen. Doch bringst Du mir den dritten Tribute von Panem Band, dann wünsche ich mir dazu ein Netflix Abo und Tickets für Justin Bieber.

Wenn Du mich nicht mit weißen Adidas Superstar beschenkst, dann möchte ich entweder den dritten Tribute von Panem Band oder einen Selfie-Stick bekommen. Wenn Du mir aber keinen Selfie-Stick auf den Gabentisch legst, dann bitte ich Dich, sofern ich ein Glätteisen bekommen sollte, ein iPhone 6s beizulegen.

Annikas Wunschzettel (Teil 2)

Bringst Du mir ein Glätteisen, dann möchte ich bitte keinen Selfie-Stick bekommen. Wenn Du mir entweder ein Netflix Abo oder weiße Adidas Superstar schenkst (also genau eins von beiden), dann möchte ich, falls ich nicht das neue Silbermond-Album kriege, auch keine Tickets für Justin Bieber geschenkt bekommen.

Wenn Du mir meinen Wunsch, ein Netflix Abo zum Fest zu erhalten, erfüllst, dann möchte ich, sofern ich nicht ein iPhone 6s, wohl aber Tickets für Justin Bieber bekomme, keinen Selfie-Stick zu Weihnachten haben. Und wenn Du mir nicht den dritten Tribute von Panem Band schenken magst, dann lege mir bitte ein Glätteisen unter den Weihnachtsbaum.

Mehr Wünsche habe ich nicht!

Deine Annika

Wunschzettel-Dilemma

In seiner Not wandte sich der Weihnachtsmann an eine(n) Informatiker*in seines Vertrauens, der/die im sogleich erklärte:

„Das kann man mit einem SAT-Algorithmus lösen!“

Boolean Satisfiability Problem (SAT)

- Given
  - A Boolean formula φ in Conjunctive Normal Form (CNF)
    - A CNF is a conjunction of clauses: $C_1 \wedge \ldots \wedge C_m$
    - A clause is a disjunction of literals: $(l_1 \vee \ldots \vee l_k)$
    - A literal l is a Boolean variable or its negation: l or $\neg l$
- Question
  - Is there a valuation of the variables that satisfies φ?
- Example

  $(1) \wedge (1) = 1$

  - $x_1 = x_2 = 0, x_3 = 1$ satisfies
    $\varphi = (\neg x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee \neg x_3)$
- Techniques for solving instances of the SAT problem are called SAT algorithms or SAT solvers
- Complexity of the "general" SAT problem: NP-complete (S.A. Cook, 1971)

Boolean Satisfiability Problem (SAT)

Focus here is on complete methods

- Due to a systematic procedure complete solvers are able to prove the unsatisfiability of a CNF formula
- DP algorithm
  - M. Davis, H. Putnam, 1960
  - Based on resolution
- DLL algorithm
  - M. Davis, G. Logemann, D. Loveland, 1962
  - Based on depth-first search
- Modern SAT algorithms
  - Based on the DLL algorithm, but enriched with efficient data structures and several acceleration & optimization techniques
  - zChaff, MiniSat, MiraXT, lingeling, antom, Glucose

Annikas Wunschzettel als SAT-Instanz

F(x0, x1, x2, x3, x4, x5, x6, x7) =

(x0 → –x1) * (x2 → –x3) * (x4 → (x0 * x5)) *

(–x3 → (x4 + x6)) * (–x6 → (x7 → x2)) * (x7 → –x6) *

((x0 xor x3) → (–x1 → –x5)) *

(x0 → ((–x2 * x5) → –x6)) * (–x4 → x7)

Mit

x0 = Netflix Abo

x1 = Silbermond-Album

x2 = iPhone 6s

x3 = Adidas Superstar

x4 = Tribute von Panem

x5 = Tickets Justin Bieber

x6 = Selfie-Stick

x7 = Glätteisen

sowie

→ = Implikation

* = UND

+ = ODER

– = Negation

Wunschzettel-Dilemma

Jetzt fiel es dem Weihnachts-mann wie Schuppen von den Augen: „Noch schnell die Formel in CNF transformiert, an einen SAT-Solver zum Lösen weitergegeben und schon weiß ich, welche Geschenke zu Annikas Wunschzettel passen!“

Annikas Wunschzettel als SAT-Instanz

F(x0, x1, x2, x3, x4, x5, x6, x7) =

(x0 → –x1) * (x2 → –x3) * (x4 → (x0 * x5)) *

(–x3 → (x4 + x6)) * (–x6 → (x7 → x2)) * (x7 → –x6) *

((x0 xor x3) → (–x1 → –x5)) *

(x0 → ((–x2 * x5) → –x6)) * (–x4 → x7)

$\Rightarrow F(\ldots) = 1$

Eine erfüllende Belegung (Menge „passender“ Geschenke) lautet:

Netflix Abo (x0 = true),

Adidas Superstar (x3 = true),

Tribute von Panem Band 3 (x4 = true),

Tickets für Justin Bieber (x5 = true).

Für die restlichen Variablen gilt: x1 = x2 = x6 = x7 = false

Weihnachts-Wertschöpfungskette

- Wunschzettel-Dilemma
- Next Generation Rentierschlitten
- Rentierschlitten-Packstation
- Hermes der Weihnachtsbote
- Smarte Häuser für die optimale Bescherung
- Heute schon an Ostern denken

Next Generation Rentierschlitten

Vorbei sind die guten alten Zeiten…

Next Generation Rentierschlitten

Vorbei sind die guten alten Zeiten…

…der Rentierschlitten von heute ist vollgepackt mit modernster Technik!

Next Generation Rentierschlitten

Vorbei sind die guten alten Zeiten…

…der Rentierschlitten von heute ist vollgepackt mit modernster Technik!

→ Sicherheitskritische Komponenten, die es vor dem Einsatz zu verifizieren gilt (dem Weihnachtsmann soll ja nichts passieren!)

Welche HW-Probleme können auftreten?

Entwurfsfehler

- Fehler, die bei der Umsetzung einer Spezifikation in die zu fertigende integrierte Schaltung entstehen
- Liegt ein Entwurfsfehler vor, sind alle gefertigten Chips dieses Entwurfs fehlerhaft

→ Einsatz formaler Methoden wie etwa Combinational Equivalence Checking (CEC)

Welche HW-Probleme können auftreten?

Entwurfsfehler

- Fehler, die bei der Umsetzung einer Spezifikation in die zu fertigende integrierte Schaltung entstehen
- Liegt ein Entwurfsfehler vor, sind alle gefertigten Chips dieses Entwurfs fehlerhaft

→ Einsatz formaler Methoden wie etwa Combinational Equivalence Checking (CEC)

Fertigungsfehler

- Defekte, die bei der physikalischen Fertigung einzelner Chips entstehen und deren Funktionsweise ändern
- Ursachen können bspw. Verunreinigungen, verschobene Belichtungsmasken, Staubkörner, falsche Dotierung sein

→ Einsatz formaler Methoden für z.B. Automatic Test Pattern Generation (ATPG)

Combinational Equivalence Checking

Gegeben

- Spezifikation und Implementierung eines kombinatorischen Schaltkreises

Gefragt

- Sind Spezifikation und Implementierung äquivalent?

SAT-basiertes Vorgehen

- Bilde aus Spezifikation und Implementierung einen Miter-Schaltkreis
- Erzeuge aus dem Miter eine CNF
- Löse die CNF mit einem SAT-Solver
- Spezifikation und Implementierung äquivalent gdw. die zuvor generierte CNF unerfüllbar ist

Combinational Equivalence Checking

→ Verbinde korrespondierende Eingänge

Combinational Equivalence Checking

→ Verknüpfe korrespondierende Ausgänge per XOR-Gatter

Combinational Equivalence Checking

→ Miter-Schaltkreis

Combinational Equivalence Checking

→ M = 1 gdw. Spezifikation & Implementierung nicht äquivalent!

Automatic Test Pattern Generation

Gegeben

- Kombinatorischer Schaltkreis sowie das gewünschte Fehlermodell (bspw. „single stuck-at“), bzgl. dessen der Schaltkreis geprüft werden soll

Gefragt

- Finde für alle theoretisch möglichen Stellen innerhalb des Schaltkreises, an denen ein Fehler des betrachteten Fehler-modells auftreten kann, jeweils min. ein Testmuster

SAT-basiertes Vorgehen

- Ähnlich zu CEC, bilde Miter aus fehlerhaftem und korrektem Schaltkreis, erzeuge entsprechende CNF und löse die Instanz mit einem SAT-Solver
- Fehler detektierbar gdw. CNF erfüllbar

Automatic Test Pattern Generation

(a) Correct circuit

(b) Faulty circuit, s@1-error at x_5

Stuck at 1 - Fehler, d.h. Leitung kaputt, immer "1" weitergeleitet

Automatic Test Pattern Generation

Automatic Test Pattern Generation

Testmuster: (x1, x2, x3) = { (0, 0, 1), (1, 0, 1), (0, 1, 1) }

Zuvor skizzierte Problemstellungen…

…decken nur einen Bruchteil möglicher Einsatzgebiete von SAT und Co. im Bereich „Test und Verifikation integrierter Schaltkreise“ ab!

Anwendungen wie etwa

- (Bounded) Model Checking,
- Black Box Checking,
- Hybrid System Verification,
- Delay Fault Testing, …

erfordern in der Regel über „reines“ SAT hinausgehende Techniken wie bspw.

- MaxSAT,
- #SAT,
- (Dependency) QBF,
- SAT Modulo Theory.

Next Generation Rentierschlitten

…all der Aufwand, damit dem Weihnachtsmann u.a. nicht folgendes passiert:

Weihnachts-Wertschöpfungskette

- Wunschzettel-Dilemma
- Next Generation Rentierschlitten
- Rentierschlitten-Packstation
- Hermes der Weihnachtsbote
- Smarte Häuser für die optimale Bescherung
- Heute schon an Ostern denken

Motivation

Industrie 4.0

- „Informatisierung der Fertigungstechnik hin zu einer stark individualisierten Smart Production“ auf Basis intelligenter, miteinander vernetzter Maschinen (Internet der Dinge, Cyber-Physical Systems, Losgröße 1, vorausschauende Wartung, neuartige Geschäftsmodelle, …)

Smart MiniFab (SMF)

- Geeigneter Demonstrator, um…
  - Studierenden der Technischen Fakultät Herausforderungen auf dem Gebiet „Industrie 4.0“ näher zu bringen
  - Fragestellungen zu bearbeiten, die Unternehmen „auf den Nägeln brennen“ (und diese mitunter aktuell auch daran hindern, stärker ins Thema „Industrie 4.0“ einzusteigen)

SMF als Rentierschlitten-Packstation

Themenspektrum

- Vielfältige Kommunikationsschnittstellen
  - Anbindung an Rechner/ Server/ Smartphone
  - M2M-Kommunikation
  - Diverse Funkmodule (WLAN, RFID, …)
- Programmieren & Testen der diversen Stationen
- Condition Monitoring
- Power Management
- Dynamische Routenplanung mit Echtzeitbedingungen
- Model-Driven Development
- Safety & Security
- Augmented Reality
- Big Data (ja, auch in einer Mini-Fab kann Big Data entstehen, ☺)

Weihnachts-Wertschöpfungskette

- Wunschzettel-Dilemma
- Next Generation Rentierschlitten
- Rentierschlitten-Packstation
- Hermes der Weihnachtsbote
- Smarte Häuser für die optimale Bescherung
- Heute schon an Ostern denken

Hermes der Weihnachtsbote

Aufgrund der Vielzahl an Auslieferungen bittet der Weihnachtsmann einen Subunternehmer um Hilfe:

Hermes
Weil's gut ankommt.

Nun ist der Weihnachtsmann ein kritischer Zeitgenosse und fragt sich…

- wie der Zustand der ausgelieferten Güter zuverlässig über den gesamten Transportweg protokolliert und überwacht werden kann?
- wie im Schadensfall die Schuldfrage geklärt werden kann?

Hermes der Götterbote

Paketsensor 4.0

- Einfache, sichere, lückenlose und kostengünstige Transport- bzw. Zustandsüberwachung von Gütern mittels eines wiederverwendbaren „Embedded System“
- In der hier angedachten Form noch nicht erhältlich
- Masterarbeit Marc Pfeifer, WS15/16

Reale Anwendungsgebiete

- Transportüberwachung „sensibler“ und teurer Güter
  - Kunstgegenstände
  - Medizinprodukte (dürfen z.T. nicht einmal gekippt werden)
  - Elektronik
- Überwachung von Kühlketten bei Lebensmitteln

Gesamtsystem

Herausforderungen

Hardware

- Auswahl der System-Komponenten: Trade-Off zwischen Funktionalität und Stromverbrauch/ Größe/ Preis
- Drahtungebundenes Laden des Akkus
- Funkkommunikation zum Konfigurieren, Aktivieren und Auslesen des Sensorsystems

Software

- Erkennen kritischer Fallhöhen
- Unterscheiden zwischen Aufprall auf dem Boden und einem möglichen „Auffangen“
- „Wake Up“-Funktionalität zum Speichern von kritischen Zuständen (bspw. hinsichtlich Temperatur oder Feuchtigkeit)

Fallversuche

Beschleunigungsverlauf bei freiem Fall mit Aufprallen auf dem Boden

Weitere Aspekte

Security

- Software-Manipulation
  - Aktivieren nur per Pin-Code möglich
  - Einmal aktiviert nur noch Lesezugriffe erlaubt
  - Verschlüsselung der gespeicherten Daten
- Hardware-Manipulation
  - Entfernen des Systems vom Paket protokollieren
  - Öffnen des Gehäuses protokollieren

Auf dem Weg zur Serienproduktion…

- Rechtliche Fragen
- Nachweis der Korrektheit des Systems
- Feldversuche über einen längeren Zeitraum

Prototyp Gesamtsystem

Prototyp Gesamtsystem

Weihnachts-Wertschöpfungskette

- Wunschzettel-Dilemma
- Next Generation Rentierschlitten
- Rentierschlitten-Packstation
- Hermes der Weihnachtsbote
- Smarte Häuser für die optimale Bescherung
- Heute schon an Ostern denken

Smarte Häuser für die Bescherung

Vision: In einem intelligenten Haus kann zur Weihnachtszeit „bequem“ der Weihnachtsmodus aktiviert werden, bei dem…

- die Lichterkette am Weihnachtsbaum eingeschaltet,
- das sonstige Licht stimmungsvoll gedimmt,
- die Heizung auf „kuschelig warm“ gesetzt,
- die Stereoanlage eingeschaltet wird und
- Weihnachtslieder abgespielt werden.

Smarte Häuser für die Bescherung

Vision: In einem intelligenten Haus kann zur Weihnachtszeit „bequem“ der Weihnachtsmodus aktiviert werden, bei dem…

- die Lichterkette am Weihnachtsbaum eingeschaltet,
- das sonstige Licht stimmungsvoll gedimmt,
- die Heizung auf „kuschelig warm“ gesetzt,
- die Stereoanlage eingeschaltet wird und
- Weihnachtslieder abgespielt werden.

…und nach der Bescherung wird dann vollautomatisch ordentlich durchgesaugt!

Smarte Häuser für die Bescherung

Spracherkennung in Smart-Home Systemen

- Masterarbeit Benjamin Völker, WS15/16
- Motivation: „Warum boomt Smart-Home (noch) nicht?“
  - Flexibilität und Einfachheit der Steuerung
    - „Muss ich erst mein Smartphone suchen, um das Licht einschalten zu können?“
  - Sicherheit
    - „Kann der Nachbar meine Heizung steuern?“
  - Nachhaltigkeit & Preis
    - „Kann ich bereits vorhandene Geräte weiterhin nutzen?“

Smarte Häuser für die Bescherung

Spracherkennung in Smart-Home Systemen

- Masterarbeit Benjamin Völker, WS15/16
- Motivation: „Warum boomt Smart-Home (noch) nicht?“
  - Flexibilität und Einfachheit der Steuerung → Sprachsteuerung
    - „Muss ich erst mein Smartphone suchen, um das Licht einschalten zu können?“
  - Sicherheit → Offline-Betrieb
    - „Kann der Nachbar meine Heizung steuern?“
  - Nachhaltigkeit & Preis → Einsatz von bspw. Schaltsteckdosen
    - „Kann ich bereits vorhandene Geräte weiterhin nutzen?“

Grundkonzept

- Dezentrale Keyword-Erkennung zum Aktivieren des Systems
- Digitalisieren und Senden der Sprachdaten an einen Server
- Zentrale Erkennung und Ausführung von Sprachbefehlen

Grundkonzept

- Dezentrale Keyword-Erkennung zum Aktivieren des Systems
- Digitalisieren und Senden der Sprachdaten an einen Server
- Zentrale Erkennung und Ausführung von Sprachbefehlen

Grundkonzept

- Dezentrale Keyword-Erkennung zum Aktivieren des Systems
- Digitalisieren und Senden der Sprachdaten an einen Server
- Zentrale Erkennung und Ausführung von Sprachbefehlen

Grundkonzept

- Dezentrale Keyword-Erkennung zum Aktivieren des Systems
- Digitalisieren und Senden der Sprachdaten an einen Server
- Zentrale Erkennung und Ausführung von Sprachbefehlen

Herausforderungen

- Dezentrale, verlässliche Keyword-Erkennung auf einem Microcontroller mit begrenzten Ressourcen
  - Problemloses Erkennen freigeschalteter Nutzer
  - Zuverlässiges Abweisen unberechtigter Nutzer
- Realisierung der Server-Funktionalität
  - Auswerten & Ausführen von Sprachbefehlen
  - Erweiterbares, personalisierbares Interface
  - Modularer Aufbau
- Reaktionszeit des Gesamtsystems
- Prototypische Implementierung

Microcontroller-Modul

Microcontroller-Modul

User-Interface des Servers

User-Interface des Servers

„Devices“ wurden im Rahmen der Smart-X-Praktika SS14 & SS15 entwickelt

Weihnachts-Wertschöpfungskette

- Wunschzettel-Dilemma
- Next Generation Rentierschlitten
- Rentierschlitten-Packstation
- Hermes der Weihnachtsbote
- Smarte Häuser für die optimale Bescherung
- Heute schon an Ostern denken

Heute schon an Ostern denken

Weihnachten ist vorbei…

Heute schon an Ostern denken

Silvester ist vorbei…

Heute schon an Ostern denken

Kerngedanke: Verantwortungsvolle Hühnerhaltung ist gut für die Tiere und wirkt sich auch unmittelbar auf den Geschmack der Eier aus!

[Bastian Becker, Kurt Metzler, Johanna Schüssler]

Heute schon an Ostern denken

Kerngedanke: Verantwortungsvolle Hühnerhaltung ist gut für die Tiere und wirkt sich auch unmittelbar auf den Geschmack der Eier aus!

→ Hühner 4.0 Projekt

[Bastian Becker, Kurt Metzler, Johanna Schüssler]

Haltungsformen

- Bio-Freilandhaltung
  - Max. 3000 Hühner pro Stall
  - Max. 6 Hühner pro m² Stall / 18cm Sitzstange pro Huhn
  - Min. 4m² Auslauffläche pro Huhn mit überwiegend Pflanzenbewuchs
  - Nester für ungestörte Eiablage
  - Futter aus ökologischem Anbau
  - Im Krankheitsfall sind Naturheilmittel zu bevorzugen
  - Künstliche Beleuchtung max. 16 Stunden/Tag
- Freilandhaltung
- Bodenhaltung
- Kleingruppen-/Käfighaltung

[siehe Vorgaben Bundesministerium für Ernährung und Landwirtschaft]

Hühner 4.0 Projektziele

Umsetzen der Richtlinien zur Bio-Freilandhaltung mit maximalem Automatisierungsgrad

- Öffnen/Schließen der Klappen zum Außengelände in Abhängigkeit von Zeit & Helligkeit
- Steuern der künstlichen Beleuchtung
- „Austreiben“ aus den Legenestern

…in einem mobilen Stall mit autarker Stromversorgung

Komponenten

- 4 Linearmotoren
- 5 LED-Lichtleisten
- Solarmodul inklusive Laderegler
- 12V-Autobatterie
- Steuerelektronik
  - Microcontroller
  - Motortreiber
  - Echtzeituhr
  - Helligkeitssensor
  - Display
  - Joystick

Steuerelektronik

- Microcontroller
  - Teensy++ 2.0
  - 8-Bit AVR-Prozessor
  - 128kB Flash, 8kB RAM, 4kB EEPROM
  - 46 digitale & 8 analoge Pins
  - 9 PWM-Ausgänge
  - SPI- & I²C-Schnittstelle
  - Arduino-kompatibel

- Motortreiber
  - Zwei L298 H-Brückentreiber
  - Bis zu vier DC-Motoren gleichzeitig steuerbar
  - 3A Peak Output Current (2A im normalen Betrieb)

Steuerelektronik

- Echtzeituhr
  - Sparkfun Real Time Clock Module
  - Integrierte Pufferbatterie
  - Ansteuerung per I²C-Schnittstelle

- Helligkeitssensor
  - Adafruit RGB Color Sensor mit IR-Filter
  - Ansteuerung per I²C-Schnittstelle
  - Hier genutzt zur Messung der Beleuchtungsstärke [lx]

Steuerelektronik

- Display
  - Adafruit 2.2 Zoll, 18-Bit TFT LCD
  - Integrierter MicroSD-Kartenslot
  - 320x240 Pixel Auflösung
  - Ansteuerung per SPI-Schnittstelle

- Joystick
  - Adafruit 2-Axis Thumb Joystick
  - Analoge Bestimmung der X-/Y-Ausrichtung
  - Digitaler „Select Button“

Impressionen

Impressionen

Impressionen

Vor Ort debuggen?

Vor Ort debuggen?

…eher schwierig!

Vor Ort debuggen?

…eher schwierig!

Smart Mini Chicken
Ressort Deluxe

Kapitel 8 – Entwurfs- und Architekturkonzepte

1. **VLSI-Entwurf**
2. Rechnerarchitektur

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

VLSI-Entwurf

- Im Schnelldurchgang ...
- VLSI: Very Large-Scale Integration
- Entwurfs-Flow kann für Mikroprozessoren oder beliebige andere Schaltungen verwendet werden!

Übersicht (1/6)

CAE = Computer Aided Engineering

FPGA = Field Programmable Gate Array

Logic Element:

Funktionstabelle

verallgemeinerung

PLA = Programmable Logic Array

Übersicht (1/6)

Textbeschreibung, formale Beschreibungssprachen

Gatter-Netzliste

Korrekter Entwurf

Zum späteren Testen nötige Daten und On-Chip-Blöcke

Maskendaten für Transistoren und Metallisierung

Chip-Entwurf

Übersicht (2/6)

Spezifikation

- Ein digitales System kann auf verschiedene Weise beschrieben werden:
  - Beschreibung als Grafik (z.B. als Schaltplaneingabe),
  - Textuelle Beschreibung als Netzliste (z.B. EDIF),
  - Textuelle Beschreibung auf Basis einer Hardwarebeschreibungssprache (z.B. VHDL, Verilog)
  - ... oder auf noch höherer Abstraktionsebene.

Übersicht (3/6)

Synthese

- Aufgabe der Synthese ist das Umsetzen einer Spezifikation in eine (Schaltkreis-)Realisierung.
- Syntheseschritte:
  - High-Level-Synthese (Rechnerarchitektur)
  - Logiksynthese, meist noch technologieunabhängig (siehe auch Kap. 3.3 - Zweistufige Logiksynthese mit Quine/McCluskey für PLAs)
  - Technologiemapping: Abbildung einer technologieunabhängigen Netzliste auf eine Bauteilebibliothek eines Halbleiterherstellers.

Übersicht (4/6)

Simulation

- Aufgabe von Simulation und Verifikation ist der Nachweis, dass Spezifikation und Realisierung übereinstimmen.
- Validierung durch Simulation (unvollständig!)

Verifikation

- Formale Verifikation ist der Beweis von Eigenschaften der Realisierung, durch:
  - Äquivalenztests (z.B. mit BDDs, siehe Kap. 7.3)
  - Model Checking (Nachweis von Eigenschaften, einfaches Beispiel siehe Kap. 7.3)
  - Automatentraversierung (z.B. endlicher Zustandsautomat, siehe Kap. 4.3)
- Diese und weitere Formalismen werden behandelt in der Vorlesung Rechnerarchitektur, sowie in diversen Spezialvorlesungen (Verifikation eingebetteter Systeme, Verifikation probabilistischer und hybrider Systeme, ...)

Übersicht (5/6)

Testen (1/2)

- Aufgabe des Testens ist die Überprüfung eines Chips auf Fehler nach der Fertigung des Chips.
- **Motivation**: Es ist nicht ungewöhnlich, dass 60 – 70% der gefertigten Chips fehlerhaft sind.
- **Ziel**: Aussortieren der fehlerhaften Chips.

UNI FREIBURG

Testen (2/2)

- Aufgabe des Testens ist die Überprüfung eines Chips auf Fehler nach der Fertigung des Chips.
- Daher vor der Fertigung der Chips: Maßnahmen zur Vorbereitung bzw. Erleichterung des Testens, z.B.
  - Berechnung von Testmustern für den späteren Fertigungstest
    - Testen der Funktionalität
    - Testen der Geschwindigkeit
    - ATPG = „Automatic Test Pattern Generation"
    - Fehlersimulation: Bewertung von gegebenen Testmustern
  - Designänderungen, um „Testbarkeit" und „Zuverlässigkeit" zu verbessern. (DFT = „Design for testability")
  - Zusatzhardware zum Testen (BIST = „Built-in Self-Test").
- (Ausführlich in Rechnerarchitektur und Spezialvorlesung Test und Zuverlässigkeit).

15

Übersicht (6/6)

Placement, Routing

- Die erzeugte Netzliste wird verwendet, um die Elemente der Schaltung zu platzieren und zu verdrahten.
- 1. Schritt:
  Geometrisches Platzieren vorgefertigter Standardzellen.
- 2. Schritt:
  Verdrahtung der Zellen, d.h. Herstellen leitender Verbindungen zwischen Standardzellen gemäß der Netzliste.
- Danach:
  Erzeugen von Maskendaten, verwendet zum Belichten der Chipherstellung.

Beispiel: Placement, Routing

Zusammenfassung

- Herausforderungen:
  - Chips mit ~~Millionen~~/Milliarden von Transistoren in annehmbarer Zeit entwerfen,
  - gleichzeitig Entwurfskorrektheit garantieren,
  - neue Problemstellungen durch immer kleinere Strukturgrößen („nano scale"-Entwürfe),
    ↳ bestehen irgendwann nur noch aus wenigen Atomlagen
  - ganze Systeme auf einem Chip.
- Designaufgabe bleibt "beherrschbar" bei
  - hierarchischem Vorgehen und Wiederverwenden vorhandener Entwürfe (Design Re-Use),
  - Entwurfsautomatisierung,
  - ausreichendem Aufwand für Entwurfskorrektheit.

Kapitel 8 – Entwurfs- und Architekturkonzepte

1. VLSI-Entwurf
2. **Rechnerarchitektur**

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

UNI FREIBURG

Rechnerarchitektur

- Designprinzipien
- Pipelining, Parallelverarbeitung
- Speicheroganisation

- Details s. Vorlesung Rechnerarchitektur

UNI FREIBURG

2

Designprinzipien für Rechner

- Was sind die Schlüsseloperationen für diesen speziellen Rechnertyp?
- Entwurf des Datenpfades (Rechenwerk mit Verbindungsstruktur) für diese Schlüsseloperationen.
- Entwurf der Maschinenbefehle mit dem Ziel, dass möglichst jeder Befehl in einem Datenpfadszyklus (Fetch-Execute) ausführbar ist.
- Erweiterung des Befehlssatzes nur dann, wenn dadurch die Maschine nicht langsamer wird; ggfs anwendungsspezifische Zusatzhardware bereitstellen.
- Schnittstelle nach außen (Speicher, Input/Output)

Reduced Instr. Set Computer

RISC vs. CISC

Complex Instr. ...

UNI FREIBURG

Pipelining

- Performanz von Rechnern lässt sich durch Pipelining steigern.
  - Prinzip der Fließbandverarbeitung
  - Probleme der Fließbandverarbeitung

Das Prinzip an einem alltäglichen Beispiel

- Personen A, B, C und D kommen aus dem Urlaub; es ist viel schmutzige Wäsche zu waschen!
- Zur Verfügung stehen:
  - eine Waschmaschine (1/2 Stunde Laufzeit)
  - ein Trockner (1/2 Stunde Laufzeit)
  - ein Bügeleisen (1/2 Stunde Arbeit zum Bügeln)
  - ein Wäscheschrank (1/2 Stunde Arbeit zum Einräumen)
- jeder der Personen A, B, C, D aus dem Haushalt wäscht seine Wäsche selbst.
- Es gibt grundsätzlich zwei Möglichkeiten, die vier Waschvorgänge auszuführen!

UNI FREIBURG

Das Prinzip an einem Beispiel

Dauer der Arbeiten:
8 Stunden

Mit Pipelining:

Dauer der Arbeiten:
$3\frac{1}{2}$ Stunden

Aufteilung der Befehlsabarbeitung in Phasen

- Um Pipelining im Datenpfad ausnutzen zu können, muss die Abarbeitung eines Maschinenbefehls in mehrere Phasen mit möglichst gleicher Dauer aufgeteilt werden.
- Eine sinnvolle Aufteilung ist abhängig vom Befehlssatz und der verwendeten Hardware.
- Beispiel: Abarbeitung in 4 Schritten:
  - Befehls-Holphase (instruction fetch)
  - Dekodierphase / Lesen von Operanden aus Registern
  - Ausführung / Adressberechnung
  - Abspeicherphase (result write back phase)

- Pipelining ist schwierig, wenn die Dauer der Dekodier- und Ausführungsphase bei denen verschiedenen Maschinenbefehlen sehr unterschiedlich ist.

Pipelining: Illustration

- **Annahme**: Aufteilung der Befehlsabarbeitung in 4 gleichlange Phasen.

alle Stufen d. CPU gefüllt.

t

	W	T	B	S						
Befehl 1:	P1	P2	P3	P4						
Befehl 2:		P1	P2	P3	P4					
Befehl 3:			P1	P2	P3	P4				
Befehl 4:				P1	P2	P3	P4			
Befehl 5:					P1	P2	P3	P4		
Befehl 6:						P1	P2	P3	P4	
Befehl 8:							P1	P2	P3	P4
Zeitschritt:	1	2	3	4	5	6	7	8	9	10

Pipelining: Speedup (1/2)

- **Annahmen**:
  - Abarbeitungszeit eines Befehls ohne Pipelining: t
  - k Pipelinestufen, gleiche Laufzeit der Stufen

  $\Rightarrow$ Laufzeit einer Stufe der Pipeline: $\frac{t}{k}$

- Beschleunigung bei m auszuführenden Instruktionen:

  $m = 1$: Laufzeit mit Pipeline $= k \cdot \frac{t}{k} = t$
  $\Rightarrow$ keine Beschleunigung

  $m = 2$: Laufzeit mit Pipeline $= t + \frac{t}{k} = (k+1)\frac{t}{k}$
  $\Rightarrow$ Beschleunigung um Faktor $\frac{2k}{k+1}$

  $k=4 \Rightarrow \frac{8}{5} = 1.6$

1. Befehl
2. Befehl

t t/k

P1	P2	P3	P4
	P1	P2	P3	P4	2. Bef

Speedup: $\frac{2 \cdot t}{(k+1)\frac{t}{k}} = \frac{2 \cdot t \cdot k}{(k+1)t}$

Pipelining: Speedup (2/2)

1. Befehl

2. bis m. Befehl

$\frac{k\cdot(m+k-1)}{m+k-1} - \frac{k(k-1)}{m+k-1}$

- $m \geq 1$: Laufzeit mit Pipeline $= t + (m-1)\frac{t}{k}$,
  Laufzeit ohne Pipeline $= m \cdot t$.

  $\Rightarrow$ Beschleunigung um $\frac{mt}{t+(m-1)\cdot\frac{t}{k}} = \frac{mk}{m+k-1} = k - \frac{k(k-1)}{m+k-1}$

- **Ergebnis**:

  Für $m >> k$ nähert sich der Speedup also der Anzahl k der Pipelinestufen.

IF-THEN-ELSE

neue Werte

- Es wurde vorausgesetzt, dass sich die Ausführung der Befehle ohne weiteres „verzahnen" läßt. Dies ist in der Praxis nicht immer der Fall
  $\Rightarrow$ Pipelinehemmnisse, sog. Hazards!

IF	P1	P2	P3	P4
B2		P1	P2	
B1			P1	

Sind entweder „if" oder „else".

neue Werte holen

Pipelining: Zusammenfassung

- Beschleunigung um bis zu Faktor k durch Einsatz einer Pipeline
  (k = Anzahl der Pipeline-Stufen).
- Hazards verringern die Beschleunigung.
- Viele Möglichkeiten Hazards zu vermeiden, sowohl durch Software- als auch Hardwaremaßnahmen

Übersicht: Formen der Parallelität

- Parallelität auf Bitebene: bis etwa 1985
  - Kombinatorische Addierer und Multiplizierer, etc.
  - wachsende Wortbreite auf 64 Bit
- Parallelität auf Instruktionsebene: 1985 bis heute
  - Pipelining der Instruktionsverarbeitung
  - Mehrere Funktionseinheiten (superskalare Prozessoren) bei mehr als 4 Funktionseinheiten werden Datenabhängigkeiten oft zum Hindernis für eine effiziente Ausnutzung.
  - Vektorprozessoren führen eine Operation parallel auf vielen Daten durch
- Parallelität auf Prozessor-/Rechnerebene

Hm?

  - Nur so scheinen Beschleunigungen um Faktor 50 und mehr möglich.

12

Speicherorganisation im Überblick

- **Fragen**:
  - Wie kann verhindert werden, dass ein Rechner durch Hauptspeicherzugriffe zu sehr verlangsamt wird?
  - Was passiert, wenn nicht alle Daten in den Hauptspeicher passen?
  - Welche sonstigen Speichermedien gibt es?
- **Begriffe**:
  - Speicherhierarchie
  - Cache
  - Virtueller Speicher, Verdrängungsstrategien
  - Festplatte, Flash, CDROM / DVD / Blu-Ray, Magnetband

Gründe für komplexe Speicherorganisation

- Ein Zugriff auf eine Hauptspeicherzelle ist langsamer, als ein Zugriff auf ein Register.
  - Hauptspeicherzellen sind DRAM-Zellen (dynamische Speicherzellen), während Register in der Regel SRAM-Zellen (statische Speicherzellen) sind!
  - Bei einem Registerzugriff kommt man ohne Bus-Operation aus!
- **Idee**: Man stellt dem Prozessor einfach einige Mbyte Register zur Verfügung.
  - Aber: SRAM-Zellen sind wesentlich größ er als DRAM-Zellen (Faktor 3-4).
  - So abwegig ist die Idee nicht!
  - Mit der weiteren Technologieentwicklung (noch kleinere Strukturen) wird die verfügbare Chip-Fläche vorwiegend dazu benutzt werden, um schnellen Speicher zu integrieren.

Speicherorganisation heute

Programm
1-8 bytes

Cache
8-128 bytes

OS
512-4K bytes

Benutzer
MByte, GByte, TByte

Speicherhierarchie (1/3)

Geschwindigkeit:	Am schnellsten	Am langsamsten
Größe:	Am kleinsten	Am größten
Kosten:	Am teuersten	Am billigsten

Speicherhierarchie (2/3)

Geschwindigkeit:	Am schnellsten	Am langsamsten
Größe:	Am kleinsten	Am größten
Kosten:	Am teuersten	Am billigsten

Speicherhierarchie (3/3)

- Grundprinzip:
  - Wenig schneller und teurer Speicher
  - Viel langsamer und billiger Speicher
  - Speicherhierarchie
- Wieso funktioniert das?
  - Wegen Prinzip der Lokalität!

Prinzip der Lokalität (1/2)

Typische Programme verbringen 80% der Ausführungszeit in etwa 10% des Gesamtprogramms.

Anteil der Instruktionen des Gesamtcodes, die 80% (gelb) bzw. 90% (rot) der Ausführungszeit ausmachen.

Patterson, Hennessey Computer Architecture a Quantitative Approach

Prinzip der Lokalität (2/2)

- Es gibt zwei Arten von Lokalität:
  - Zeitliche Lokalität (Locality in Time): Wenn ein Datum verwendet wird, wird es auch bald wieder verwendet werden.
  - Räumliche Lokalität (Locality in Space): Wenn ein Datum verwendet wird, werden auch die Adressen in dessen Nähe bald verwendet werden.
  - Siehe z.B. Schleifen …
- Wegen Lokalität kommt man auf höheren Ebenen der Speicherhierarchie mit weniger Speicher aus.

Speicherorganisation heute

Programm
1-8 bytes

Cache
8-128 bytes

OS
512-4K bytes

Benutzer
MByte, GByte, TByte

Überblick

Kap. 0 Einführung/Umfeld	8		
	7	Formale Spezifikation v. Hardware: Boolesche Ausdrücke, BDDs	Formale Verifikation, ReTI ALU
	6	Fehlertoleranz fehlererkenn./fehlerkorrig. Codes	Parity, Hamming Code
	5	Physikalische Eigenschaften Timing	ReTI: Exaktes Timing
	4	Sequentielle Logik	ReTi: Datenpfade, Idealisiertes Timing
	3	Komb. Logik Minimalpolynome Arithmetik	ReTI: ALU
	2	Kodierung von Zeichen/Zahlen	ReTI: Befehls-Kodierung
	1	ReTI abstrakt	Kap. 12
		Mathem. Grundlagen	Kap. 11

Überblick

Kap. 0 Einführung/Umfeld	8	Entwurfs- und Architekturkonzepte	
	7	Formale Spezifikation v. Hardware: Boolesche Ausdrücke, BDDs	Formale Verifikation, ReTI ALU
	6	Fehlertoleranz fehlererkenn./fehlerkorrig. Codes	Parity, Hamming Code
	5	Physikalische Eigenschaften Timing	ReTI: Exaktes Timing
	4	Sequentielle Logik	ReTi: Datenpfade, Idealisiertes Timing
	3	Komb. Logik Minimalpolynome Arithmetik	ReTI: ALU
	2	Kodierung von Zeichen/Zahlen	ReTI: Befehls-Kodierung
	1	ReTI abstrakt	Kap. 12
		Mathem. Grundlagen	Kap. 11

Kapitel 8.2b
Speicherhierarchie

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer
Professur für Rechnerarchitektur
Institut für Informatik
Technische Fakultät

Folien gehen zurück auf die Vorlesung…

Technische Grundlagen der Informatik II
– Speicherhierarchie –

Dr. Tobias Schubert

Institut für Informatik

Lehrstuhl für Technische Informatik

1. Einführung

- Ein Speichersystem muss Speicher zur Verfügung stellen
  - „Soviel Speicher wie möglich“
  - Speicher sollte so schnell wie möglich sein
  - Speicher sollte so günstig wie möglich sein

Laden/Entladen von „Kondensatoren“

- Typische Werte im Jahr 2004

FlipFlops

Speichertechnologie	Zugriffszeit	Kosten pro GByte
SRAM (statisch) Register Cache	0.5 – 5 ns	$4'000 – $10'000
DRAM (dynamisch)	50 – 70 ns	$100 – $200
Festplatte	5 – 20 ms	$0.5 – $2

Hauptspeicher

- Ziel: „Unbegrenzte“ Menge von sehr schnellem Speicher kostengünstig zur Verfügung zu stellen

1. Technologische Trends

- Entwicklung der Performance von CPUs und DRAM

µProc
60%/yr.
(2X/1.5yr)

DRAM
9%/yr.
(2X/10 yrs)

DRAM wird immer mehr zum Flaschenhals

2. Lokalitätsprinzip

- Lokalitätsprinzip: Programme greifen in einem kleinen Zeitintervall auf einen relativ kleinen Teil des Adressraums zu

- Temporale Lokalität (Lokalität in der Zeit)
  - Wenn ein Zugriff auf eine Adresse erfolgt, wird auf diese Adresse mit „großer“ Wahrscheinlichkeit bald wieder zugegriffen
    - Abarbeitung von Schleifen

- Räumliche Lokalität (Lokalität im Raum)
  - Wenn ein Zugriff auf eine Adresse erfolgt, werden mit „großer“ Wahrscheinlichkeit bald Zugriffe auf in der Nähe liegende Adressen erfolgen
    - Verarbeitung von Array-Daten

- Aufgrund der Lokalität kann man Speichersysteme hierarchisch aufbauen
  - Obere Stufe der Hierarchie: schneller und teurer Speicher (wenig)
  - Untere Stufe der Hierarchie: langsamer und billiger Speicher (viel)

2. Übersicht – Speicherhierarchie

CPU Registers
100s Bytes

Cache
M-Bytes
1-0.1 cents/bit

Hauptspeicher
G-Bytes
.0001-.00001 cents /bit

Festplatten
G/T-Bytes
10^{-5} - 10^{-6} cents/bit

Band
unendlich
10^{-8} cents/bit

Prog./Compiler
1 - 8 Bytes

Cache Controller
8 - 128 Bytes

Betriebssystem
512 Bytes - 4 KB

User/Operator
M-Bytes

Höhere Stufe

Schneller

Größer

Niedrigere Stufe

2. Speicherhierarchie

- Funktionsprinzip
  - Daten werden in bestimmten Einheiten zwischen den Ebenen der Speicherhierarchie übertragen
  - Daten werden nur zwischen benachbarten Ebenen übertragen
  - Ist eine Dateneinheit auf einer Ebene vorhanden, muss sie auch auf den tieferen Ebenen vorhanden sein

2. Terminologie

- Hit (Treffer): Daten befinden sich im Speicher der Ebene, auf die aktuell zugegriffen wird
  - Hit-Rate: Anteil der erfolgreichen Speicherzugriffe
    - So hoch, dass man immer von Miss-Rate spricht
  - Hit-Time: Zeit für einen erfolgreichen Zugriff
    - Zeit, um Hit festzustellen & Zeit für den eigentlichen Datenzugriff
- Miss (Fehlzugriff): Daten befinden sich nicht im Speicher der Ebene, sondern müssen erst aus unterhalb gelegener Ebene geholt werden
  - Miss-Rate: Anteil der Fehlzugriffe auf einer Ebene
    - Miss-Rate = 1 – Hit-Rate
  - Miss-Penalty (Miss-Strafe): Zeit für das Bereitstellen der Daten aus der unteren Ebene
    - *Zugriffszeit zur niedrigeren Speicherebene*
    - *Übertragungszeit zur höheren Speicherebene*
- Mittlere Speicherzugriffszeit = Hit-Time + Miss-Rate * Miss-Penalty
  (gemessen in bspw. ns or clocks)

2. Caches

- Speicherhierarchie: Cache ↔ Hauptspeicher

- Wichtige Fragen
  - Auf welchen Cacheblock wird ein Speicherblock abgebildet?
  - Wie stellt man fest, ob ein Datum im Cache ist, und falls ja, in welchem Cacheblock?
  - Welcher Cacheblock wird bei einem Cache-Miss ersetzt?
  - Was geschieht beim Schreiben eines Datums?

2. Cache mit direkter Abbildung

- Beim Cache mit direkter Abbildung (direct mapping) kann jeder Speicherblock nur an einer Stelle im Cache stehen

  Wo steht das Datum im Cache?

  - Einfachste Abbildung

    Cacheblockadresse = Speicherblockadresse *mod* (Anzahl Cacheblöcke)

    ↳ Wo im DRAM?

  - Die Cacheblockadresse wird auch als Index bezeichnet

  - I.A. wählt man für die Anzahl der Cacheblöcke eine 2er-Potenz
    - Dadurch lässt sich die *mod* Operation besonders einfach realisieren
    - Für *mod* (2^n) muss man nur die n niederwertigsten Bits der Adresse nehmen

      z. B. $n=3$ → 8 Cacheblöcke bzw. 8 Cacheeinträge

      → 3 niederwertigsten Bits d. Speicheradresse

2. Cache mit direkter Abbildung

- Beispiel $= 2^3$
  - 8 Cacheblöcke; ein Block besteht aus einem Wort
    - Cacheblockadresse = Speicherblockadresse *mod* 8 = Speicherblockadresse[2:0]

2. Cache-Struktur

- Cache Tag
  - Der Index (Cacheblockadresse) kann nicht eindeutig einer Speicherblockadresse zugeordnet werden
  - Inhalt des Caches an dieser Position somit nicht eindeutig
  - Deshalb verwendet man die restlichen Bits der Speicherblockadresse als so genannten Tag
    - Zu jedem Block im Cache auch den entsprechenden Tag speichern
  - Auffinden von Daten durch Abgleich der Tags des gesuchten Blocks und des Cacheeintrages

- Valid Bit
  - Gibt an, ob ein Cacheeintrag gültig ist oder nicht
    - Am Anfang – und nach jedem Leeren des Caches – enthält der Cache keine gültigen Daten (Valid Bit wird auf 0 gesetzt)
    - Wenn der Cacheeintrag gültig ist, wird das Valid Bit auf 1 gesetzt

2. Cache-Zugriffe

- Beispiel
  - 5-Bit Adressen, Cache mit direkter Abbildung, 8 Cacheblöcke, ein Block besteht aus einem Wort → 32 Speicherblöcke

Zeit ↓

	Speicheradresse	Hit / Miss	Cacheblock
(1)	22_{10} = 10110	miss	10110 *mod* 8 = 110
(2)	26_{10} = 11010	miss	11010 *mod* 8 = 010
(3)	22_{10} = 10110	hit	10110 *mod* 8 = 110
(4)	26_{10} = 11010	hit	11010 *mod* 8 = 010
(5)	16_{10} = 10000	miss	10000 *mod* 8 = 000
(6)	3_{10} = 00011	miss	00011 *mod* 8 = 011
(7)	16_{10} = 10000	hit	10000 *mod* 8 = 000
(8)	18_{10} = 10010	miss	10010 *mod* 8 = 010

2. Cache-Struktur

Beispiel

4 KByte Cache mit direkter Abbildung
32-Bit Adressen,
1024 Cacheblöcke,
ein Block besteht aus einem Datenwort

Nutzdaten

= zu 32 Bit, d.h. 4 Byte

Wie viele Speicherbits braucht man für die Implementierung eines solchen 4 KByte (=32 KBit) Cache?

→ 2^{10}*(32+20+1) = 53 KBit !

= 1024

= 6.6 kB

data

tag

valid bit

2. Cache mit direkter Abbildung

- Daten werden im Cache in größere Blöcke abgelegt
  - Cache-Eintrag besteht aus mehreren Datenwörtern
  - Nutzung der räumlichen Lokalität
  - Effizientere Datenübertragung

  - Jeder Block hat einen Tag
  - Die einzelnen Worte im Block haben aufsteigende Adressen
  - Die l-Bit Adresse wird aufgeteilt in
    - einen Tag,
    - einen n-Bit Index und
    - einen m-Bit Blockoffset
      - Der Blockoffset wählt unter den Worten eines Blocks aus

2. Cache mit direkter Abbildung

- Beispiel
  - $l = 32$ = 32 Bit-Adresse, 32 Bit Daten
  - $n = 8$ = Index ⇝ 256 Cachezeilen
  - $m = 4$

Blockoffset

$16 = 2^4$ vers. Positionen innerhalb einer Cachezeile identifizieren

2. Cache mit direkter Abbildung

- Mehrere Worte pro Block (Multiword Cache Block)
  - Vorteile
    - Durch die Nutzung räumlicher Lokalität sinkt die Miss-Rate
    - Effizientere Speicherung, d.h. weniger Overhead durch Tags und Valid Bits
    - Effizienterer Datentransfer

1 Tag pro Cachezeile, aber >1 Wort pro Cachezeile

  - Nachteile
    - Wachsende Blockgröße → weniger Cacheblöcke (bei konstanter Cachegröße)
      - Blöcke werden immer öfter ersetzt, so dass die Lokalität nur schlecht ausgenutzt werden kann → Miss-Rate steigt wieder
    - Größere Miss-Penalty
      - Bei einem Cache-Miss müssen mehr Daten aus dem Speicher geladen werden

- Weitere Maßnahmen zur Reduktion der Miss-Rate
  - Größerer Cache (teuer!)
  - Assoziativer Cache

2. Assoziativer Cache

- Assoziativer Cache hat für jeden Cacheindex k Einträge (Blöcke)
  - Satz: Menge von Blöcken, die mit einem Indexwert referenziert werden
- Cache-Zugriff
  - Auswahl des Satzes mit dem Index der Adresse
  - Parallel dazu Vergleich des Tag der Adresse mit allen k Tags der Cacheblöcke in diesem Satz
  - bei 2^n Cacheblöcken:

    $k = 1$: Cache mit direkter Abbildung

    $k > 1$: k-fach satzassoziativer Cache (k-Way Set Associative Cache), teilassoziativer Cache

    $k = 2^n$: voll assoziativer Cache (Full Associative Cache)
  - Vorteil
    - Miss Rate wird reduziert
  - Nachteile
    - Hit Time wird etwas vergrößert
    - Bei großem k wird der Hardwareaufwand beträchtlich

2. Assoziativer Cache

- Beispiel : k=4

4-fach satzassoziativer Cache
mit m=0 (kein Multiword Cache)

eher im Vgl. zu Folie 14 zu sehen, nicht zu Folie 16

2. Assoziativer Cache

Kein Multiword

- Beispiel: $n = 3$, $m = 0$

↳ $2^3 = 8$ Cacheeinträge

One-way set associative (direct mapped)

Block	Tag	Data
0		
1		
2		
3		
4		
5		
6		
7		

Two-way set associative

Set	Tag	Data	Tag	Data
0				
1		0		0
2				
3				

Four-way set associative

Set	Tag	Data	Tag	Data	Tag	Data	Tag	Data
0		–		–		–		–
1		x		y		z		a

Eight-way set associative (fully associative)

1 Zeile

Tag	Data	Tag	Data	Tag	Data	Tag	Data	Tag	Data	Tag	Data	Tag	Data	Tag	Data

2. Verdrängungsstrategien

- Welcher Block wird verdrängt, wenn ein neuer Block geladen werden muss und keine freien Cacheblöcke mehr vorhanden sind?

- Cache mit direkter Abbildung
  - Keine Auswahl, da jeder Speicherblock auf genau einen Cacheblock abgebildet wird

- Assoziativer Cache
  - Zufällige Auswahl eines Blocks
    - Einfach in Hardware zu implementieren
  - Least Recently Used: der am längsten nicht benutzte Block wird ersetzt
    - Zugriffszeiten auf die Blöcke müssen gespeichert werden
    - Aufwendig in Hardware zu realisieren, wird typischerweise bis $k = 4$ gemacht

2. Schreibtechniken

- Durchgängiges Schreiben (write-through)
  - Worte werden in den Cache und gleichzeitig in den Hauptspeicher geschrieben
    - Hauptspeicher und Cache immer konsistent, aber jede Schreib-Operation greift immer auch auf den (langsamen) Hauptspeicher zu
  - Modifikation der Daten erfolgt immer nur im Cache
    - Bei einem Write-Miss wird zuerst der Block in den Cache geladen und dann das Wort in den Cache und gleichzeitig in den Hauptspeicher geschrieben
  - Entlastung des Prozessor durch die Verwendung eines Pufferspeichers (write buffer)
    - Schreiben der Daten in Cache und (schnellen) Pufferspeicher, danach kann der Prozessor sofort weiterarbeiten
    - Ist die Rate, mit der der Prozessor Schreibinstruktionen ausführt, kleiner als die mittlere DRAM-Schreibzykluszeit, funktioniert write-through mit write buffer gut
    - Wenn nicht, füllt sich der Pufferspeicher und der Prozessor muss anhalten und warten, bis im Pufferspeicher wieder Platz ist

2. Schreibtechniken

- Durchgängiges Schreiben (write-through & write buffer)

2. Schreibtechniken

- Zurückkopieren (write-back)
  - Beim Schreiben wird das Wort nur in den Cache geschrieben
    - Hauptspeicher und Cache sind inkonsistent
  - Erst wenn der Cacheblock ersetzt werden muss, wird er in den Hauptspeicher zurückgeschrieben
    - Ein Dirty Bit gibt an, ob der Block verändert wurde oder nicht
      - Dirty Bit wird bei jedem Schreibzugriff auf den Block gesetzt
      - Beim Ersetzen des Blocks wird dieser nur dann in den Hauptspeicher zurückgeschrieben, wenn das Dirty Bit gesetzt ist
  - Vorteil
    - Wenn die Schreibrate hoch ist, höhere Performance als write-through
  - Nachteil
    - Aufwendigere Steuerung als write-through

2. Weitere Maßnahmen zur Cache-Optimierung

- Reduktion der Miss-Rate
  - Cacheorganisation
    - Größere Blöcke
    - Größere Caches
    - Höhere Assoziativität
  - Compileroptimierungen
    - Instruktionen: Umordnen der Instruktionen, um Instruction Misses zu reduzieren
    - Daten: array merging, loop interchange, loop fusion, blocking, ...
- Reduktion der Miss-Penalty
  - Multi-level Cache
    - Kleiner 1st Level Cache optimiert auf Hit-Time (geringe Assoziativität, kleine Blöcke)
    - Großer 2nd Level Cache optimiert auf Miss-Rate (höhere Assoziativität, große Blöcke)
  - Victim Cache
    - Zusätzlicher "Cache", der kürzlich ersetzte Cacheblöcke ("victims") speichert

2. Weitere Maßnahmen zur Cache-Optimierung

- Reduktion der Miss-Penalty und der Miss-Rate
  - Blöcke werden auf Verdacht in Register, Caches oder so genannten Prefetch-Puffer geladen
    - Macht nur Sinn, wenn das Speichersystem freie Bandbreite zur Verfügung hat
  - Hardware Prefetching
    - Prefetching von Instruktionen

      Bsp.: Alpha 21064 lädt zwei Blöcke bei einem Instruction Miss, der zweite Block kommt in einen separaten Puffer („Stream Buffer“); beim nächsten Instruction Miss wird zuerst im „Stream Buffer“ nach benötigtem Block gesucht
    - Prefetching von Daten

      Bsp.: Stream Buffer, die dauernd mit den Blöcken der nächsten Adressen nachgeladen werden
  - Software Prefetching
    - Compiler fügt spezielle prefetch-Instruktionen ein

3. Zusammenfassung – 4 wesentliche Fragen

1. Wo wird ein Block platziert?
   - direkt abgebildet
   - teilassoziativ
   - vollassoziativ

2. Wie wird ein Block gefunden?
   - direkt abgebildet: Index
   - teilassoziativ: Index & Suche unter den Blöcken (paralleler Vergleich)
   - vollassoziativ: Suche unter allen Blöcken bzw. Tabelle mit Abbildungen

3. Welcher Block wird bei einem Miss ersetzt?
   - Zufällig bestimmter Block
   - „Least Recently Used“-Strategie

4. Was geschieht beim Schreiben?
   - Durchgängiges Schreiben
   - Zurückkopieren