

Defining Computation

فصل ۳ - تعریف محاسبه

اصلی یادیگری: در این سه میتوان محاسبات را دستی و مکانیکی نمود.

Straight-line programs و Boolean-circuits یادیگری مدل‌گیری محاسباتی هستند.

NAND و AND/OR/NOT نهم معادل بودن Boolean-circuits هستند.

مثال کوچی از محاسبات در جهان نیزیکی است.

محاسبه طی نمایند و این فعل بروز است.

ما می‌توانیم با استفاده از عملیات منطقی، مانند NOT، OR، AND و دو دیگری دسته خروجی را محاسبه کنیم.

که راه است برای این سه با ترتیب درون عملیات منطقی Boolean-circuit پایه، تابع پیویستی را محاسبه کنیم.

مدل ریاضی (برنامه DAG) در نظر نمی‌گیریم و هم میتوان آن را در جهان نیزیکی با بعضی کمی مختلف پیاده سازی کرد.

میتوان Straight-line programs را به مدل Boolean-circuit تبدیل کرد. این نوع از برنامه، صحیح ساختاری برای حلقة ندارد (مانند for، while).

NAND، NOT، OR، AND و محدود دارد از عملیات این امکان وجود ندارد.

پیاده سازی کنیم (و بالعکس).

این اصلی فصل: دو مدل محاسباتی معادل هستند اور میتوان مجموعه پیاده سازی از توابع را با صردو مدل پیاده سازی کرد.

تعریف غیر رسمی از الگوریتم:

که الگوریتم، یک مجموعه دستور العمل برای حلولی محاسبه یا فرآیند ورودی را استفاده از دنباله‌ای از قدر کوچی استدایی است.

An algorithm A, computes a function F. If for every input n, if we follow the instructions of A on the input n, we obtain the output $F(n)$.

که الگوریتم، یک محاسبه کمپیوئی را به تعدادی قسم ساده‌تر تبدیل می‌نماید.

تابعیت ساده میانی در سیستمی کامپیوئی زیادی استفاده می‌شوند. وابع است که عملیات محاسباتی نمی‌توانند ساده‌تر از AND/OR/NOT باشند؛ با این قدرت محاسبه، از ترکیب کردن این اجزای ساده نشأت می‌برند.

Commutativity

برخی از خواص هر دو عمل، خاست جایی و پیروزی در associativity

Distributive law

این توزیع بینی دارد: OR, AND

$$a, b, c \in \{0, 1\}, a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

فران می‌نمی‌شود بیش مبتدا، True، False بمعنای u+v is positive برابر با $u, v \in \mathbb{N}$ خواهی داشت: if and only if $u \vee v$ is True

و

u, v is Positive

if and only if $u \wedge v$ is True

از عبارات باز تجربه شویم:

for every $a, b, c \in \{0, 1\}$:

$a \wedge (b \vee c)$ is True

if and only if $a \cdot (b + c)$ is positive

(بررسی)

$(a \wedge b) \vee (a \wedge c)$ is True

if and only if $a \cdot b + a \cdot c$ is positive

حق تابع توزع پرسی استاندارد (توزيع بزرگ جمع و ضرب) :

$$\underline{a \cdot (b+c) = a \cdot b + a \cdot c}$$

بنی می دایم که این عبارت True است.

با $a \wedge (b \vee c)$ و $a \cdot b + a \cdot c$ و $(a \wedge b) \vee (a \wedge c)$ بین تر نشان دویم عبارت $a \cdot (b+c)$

نیز بین می توانیم که $a \wedge b$ و $a \wedge c$ در طبق تابع True باشند از آن بعده True و می توانیم $a \wedge (b \vee c)$ را در طبق تابع True باشند.

عنصر حواسته نهاده نیز نیز برداشت داشته باشد.

AND/OR/NOT لیکن XOR چیست؟

Algorithm 3.2

Input: $a, b \in \{0, 1\}$.

Output: $\text{XOR}(a, b)$. Lemma 3.3: For every $a, b \in \{0, 1\}$

1: $w_1 \leftarrow \text{AND}(a, b)$

on input a, b , Algorithm 3.2

2: $w_2 \leftarrow \text{NOT}(\bar{w}_1)$

outputs $a+b \bmod 2$.

3: $w_3 \leftarrow \text{OR}(a, b)$

4: return $\text{AND}(w_2, w_3)$

$\text{XOR}(a, b) = 1$ if and only if

$a \neq b$, a و b می باشند : $\neg w_1$

a is different from b.

If $a=b=0$ then $w_3 = \text{OR}(a, b) = 0 \rightarrow$ خوبی نیست

If $a=b=1$ then $w_2 = \text{NOT}(\text{AND}(a, b)) = 0 \rightarrow$ خوبی نیست

If $a=1$ and $b=0$ (or vice versa) then both w_3 and $w_2 = 1$,

خوبی نیست

غیر حل شده: محاسبه XOR برای ۳ ورودی

$$XOR_3 : \{0,1\}^3 \rightarrow \{0,1\} \xrightarrow{\sim} XOR_3(a,b,c) = (a+b+c) \bmod 2.$$

Lemma 3.3

نابرابری $a+b+c$ که می تواند فرد باشد در در غیر این صورت می باشد است. $(a+b)+c \neq a+(b+c)$

می دانیم که عمل جمع را می خواسته شرکت بذیری و حافظه ای داشته باشد.

حال که XOR را به شکل جمع بیان کنیم، می توانیم بگوییم که این خواص در

$$XOR_3(a,b,c) = (a \oplus b) \oplus c$$

$$XOR(a,b,c) = XOR(XOR(a,b),c)$$

بعد از ترتیب توانیم XOR با ۳ ورودی را به دو ورودی تبدیل کنیم و نخواهد بیاره سازی XOR با دو ورودی را نیز می دانیم.

تعریف نئه رسی الگوریتم:

لَكَ الْأُورِيْمِ از یک دناله ای از قدر که بی شک «مد مقدار» جدید را با استفاده از AND/OR/NOT از روی مقادیر محاسبه شده قبلی حساب کن «تکلیف شده است. غصه شده ورودی نزد مرحله قبلی محاسبه شده است.

این رکی تعریف: آن غیر رسی ۲: استفاده از AND/OR/NOT بر تناوب

در نظر نگرفتن نزدیکی ریز

۳: ارتباط تعریف با محاسبه راضعیت

Boolean Circuits

AND, OR, NOT

یک Gate circuit از تعدادی Boolean circuit که با یکم

ب هم متصل شوند

Remark 3.4

عمل کی میں کسی مداری میں نہ ازایا بے کی شئی نیز کی
ارتباط ندارد؛ اسی توان آن کا را بے مدارت فیزیکی نیز پیدا کر.

All equal

عمل حل شده: تعریف تابع بولینگی متماری یا سادی کامل

$$\text{ALLEG}: \{0,1\}^4 \rightarrow \{0,1\}$$

$$\text{input} = n \in \{0,1\}^4$$

$$\text{output} = 1 \text{ if and only if } n_0 = n_1 = n_2 = n_3$$

برای این تابع طراحی کنیم Boolean Circuit

عمل: بکار راندیر برای بیان تابع متماری، بے مدارت زیر است:

$$\text{output} = 1 \text{ if and only if } n = 0^4 \text{ or } n = 1^4$$

عبارت $n = 1^4$ باید این مدارت نوشت:

$$n_0 \wedge n_1 \wedge n_2 \wedge n_3$$

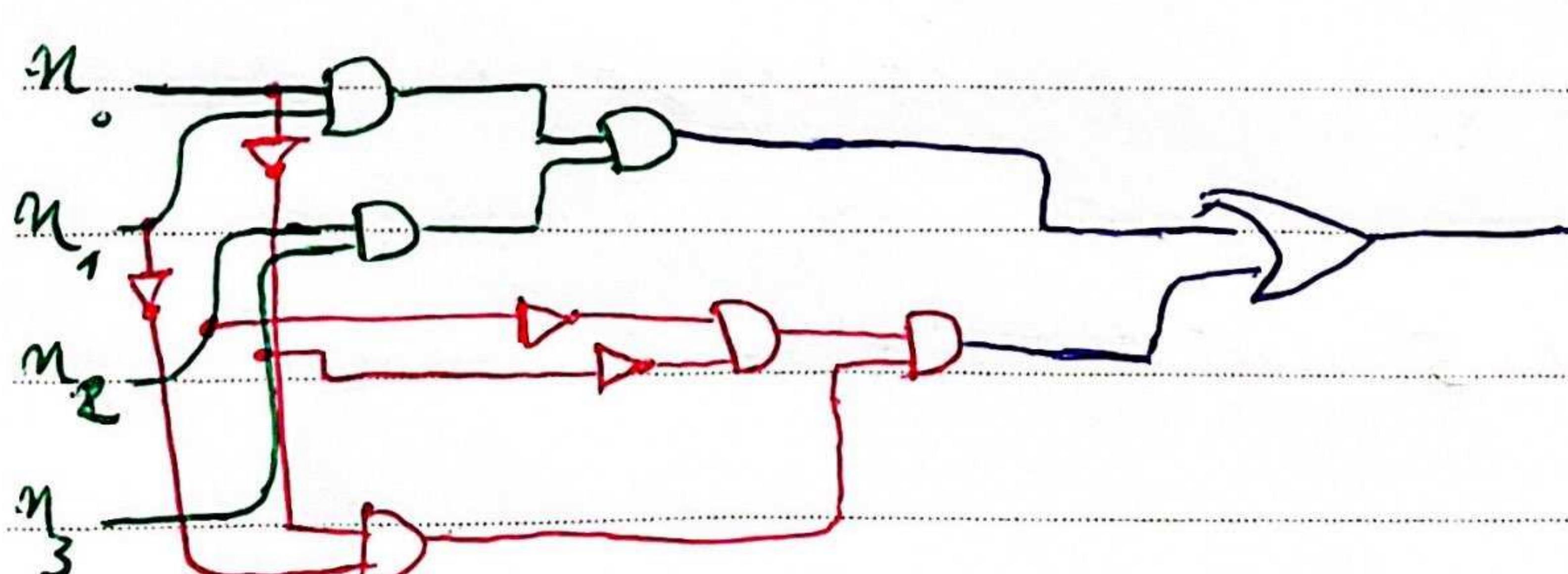
که این عبارت با AND تابل بیان سازی است

مخفی عبارت $n = 0^4$ بے مدارت زیر قابل نوشت است:

$$\bar{n}_0 \wedge \bar{n}_1 \wedge \bar{n}_2 \wedge \bar{n}_3$$

که این عبارت نیز با AND، NOT و بیان سازی می شود.

تابع ALLEG دو عبارت دارد. در نتیجه این تابع می توان با OR، AND، NOT و بکار مداری کامل Boolean circuit بیان کرد.



n, s, m are positive integers.

3.5 تعریف اسلوی ←

Sym

A Boolean Circuit with n inputs, m outputs and S gates, is
 a DAG $G = (V, E)$ with $S + n$ vertices with following properties:

کُنْسِی مائید بے نا Gate میں حصہ می رکوندہ Gate

بِرْجِ لَدَنْيِ سُونْهِ اسْتَ، Gate کے رضوی ورودی بہ تَقدَارِ

* درودی و صدیقی دارند * بیل صوانی مجاز است *

لئے کیا جائیں۔ اسی مخصوصی کی وجہ سے اس کو Gate کا نام دیا گی۔

لائلی مدار کی اسٹریکشن Boolean Circuit Construction

3.6 Boolean Circuit

فرض می‌شود که نابع به رسالت فرض می‌شود که

برای هر $n \in \mathbb{N}$ ، $C(n)$ با n ورودی و m خروجی است

Theorem 1.26 زیر تعریف می‌شود:

minimal layering / topological sorting

فرض می‌شود که $h: V \rightarrow \mathbb{N}$ باشد که متراز توبولوژیک از C است.

با فرض این که L_i لایه i است، برای $L = \bigcup_{i=0}^m L_i$

دایم:

برای هر $v \in V$ داشته باشیم $h(v) \leq i$ کی از مقدار زیرا باید

$i \in [n]$

اگر v یک رُس input باشد، $X[v]$ برشیب لناری ننده.

آن‌ها مقادیر n به v نسبت داده می‌شود

اگر v یک رُس Gate است، v برشیب لناری ننده و در

همایه ورودی آن w_1, w_2, \dots, w_n همایه v باشند، آن‌ها حاصل AND مقادیر w_1, w_2, \dots, w_n را به v

نسبت می‌دهیم. (از آن‌جا که w_1, w_2, \dots, w_n همایه کی ورودی v هستند، می‌توان نسبت معرفت داد. اگر باسی تری از آن قرار دارند؛ بنابراین مقادیر آن‌ها زوایر متناسب ننده اند.)

اگر v یک رُس Gate است، v برشیب لناری ننده و در همایه

ورودی آن w_1, w_2, \dots, w_n هستند، آن‌ها حاصل OR مقادیر w_1, w_2, \dots, w_n را به v نسبت می‌دهیم.

اگر v یک رُس Gate است، v برشیب لناری ننده و مید

همایه ورودی w به v دارد، آن‌ها مقادیر w را به v نسبت می‌دهیم.

نیه فرآیند ساده تر، مقدار $y \in \{0,1\}^m$ خواهد بود، به طوری که برای هر $j \in [m]$ مقادیری است که به راس با بجای γ_j متن داشته باشد.

Let $f: \{0,1\}^n \rightarrow \{0,1\}^m$.

We say that the circuit C computes f if:

for every $n \in \{0,1\}^n$, $C(n) = f(n)$

Remark 3.7

Boolean Circuit

در ادبیات تعریف 3.5، مکرر سری انتساب کی تکنیک محبت شرطی که ضرورت نداشته باشد برای ادامه درس را توانند بقید باند.

به عنوان مثال، مثال کی صفاتی (برای $a_{1111}, a_{1110}, a_{1101}$) که

تحابیه تغایر جدیدی نمایند. با این حال در ادامه مدارکی خواصیم دید که از مجموعه کلی تری از Gate که تشکیل شده اند.

همین شرط این که هر input های پرده هایه ضروری را شناسد،

ضرورتی ندارد، زیرا همین نمی توان برای دسترسی به این input Gate کوئی اضافه کرد.

با این حال برای راضی این صور تعریف شده زیر تفسیم می کند که تعداد input های

حداکثر، سُرشار نیز از بعد برابر اندازه صار نمی شود. زیرا هر Gate در هر

خروجی دارد.

Straight-Line Programs

(یاد آوری: Straight-line program که یه حلقه ای ندارند)

programming language

می دانیم که می توان Straight-line کرا به لام BooleanCircuit که تو اینست نمود.

برای این که این زبان را دقیق تر تعریف کنیم، ابتدا که زبان برنامه نویسی ها دار باشد.

AND/OR/NOT معرفی می نیم. این زبان BooleanCircuit

AND/OR/NOT

Date:

Sub:

$$\underline{n_0 \wedge n_1}, \quad n \in \{0, 1\}^2$$

مثال برای AON-CIRC

AON-CIRC زبان

$$\rightarrow \text{temp} = \text{AND}(X[0], X[1])$$

$$Y[0] = \text{NOT}[\text{temp}]$$

ای زبان بیش برای اعداد امتدادی طایی نموده و آن جان چنین کاربری ندارد؟ با این حال می‌توان به راحتی رعی کرد که سیستم آن را پیاده کرد.

با توجه به این سه در ادامه باید عبارت ریاضیاتی در صورت زبان AON-CIRC ابتداء نمی‌باشد ای زبان را به صورت دقیق تعریف کنیم.

ای زبان، دنالهای از رسمتی است که از شرایط زیر پروری می‌کند:

← صریح line به کوی از شکل کوی زیرنوشته می‌شود:

$$as \text{ AND } (b, c) \quad as \text{ OR } (b, c) \quad a = \text{NOT}(x) \quad (\text{اصوف} / \text{و} / \text{کل شان سیفر} / \text{من})$$

← صنایع را می‌توان با هر ترتیب رسمتی از صروف، اعدار، - و [] مثان دار. دو نوع صنایع خاص وجود دارد: $X[i], i \in \{0, 1, \dots, n-1\}$ که صنایعی محدودی می‌دانند و $Y[j]$ که صنایع خروجی می‌دانند.

← باید بنامه صحیح با ای زبان، در صریح line، شامل صنایعی ورودی به فرم $[1, \dots, m-1, \dots, 0]$ باشد. صنایعی خروجی به فرم $Y[0], \dots, Y[m-1]$ می‌باشد و اعداد n, m میانه می‌باشد و کوییم تعداد ورودی که n و تعداد خروجی که m است.

← در اینجا باید بنامه صحیح با ای زبان، در صریح line، صنایعی میانه می‌باشد و دیگر آنکه پیشتر مذکون نموده است.

Date:

Sub:

اگر P میکند بزرگ سمع بازیان AON-CIRC باشد و دردی، m ضریب دارد، آن‌هاه بزرگ مرد $\kappa \in \{0,1\}^m$ از دردی κ ، رشته $y \in \{0,1\}^m$ خواهد بود که به صورت زیر تعریف می‌شود:

- مقدار دهی متفاوتی و دردی $X[0], \dots, X[n-1], \dots, X[m]$ به مدادی $\kappa, \dots, \kappa, -r, \dots, -r$.

اگری ضعوط عملیاتی P ، به ترتیب و لایی بیو (که ده خواهد

مقدار علیات سخت است به تغیر سخت همچنین نسبت داده می‌شود)

فرضی می‌شود ضریب دریابین اول $(Y[0], \dots, Y[m-1])$ ، رشته

$y \in \{0,1\}^m$ است.

ضریب بزرگ $P(n)$ از دردی κ می‌شود

آنرا میکند بزرگ بازیان AON-CIRC باشد که آن برابر است.

حال که بزرگ کی $AON-CIRC$ ضریب میزد منس نهاده، چیزی که میتوان کنون می‌باشد تابع با این بزرگ را تعریف کرد:

تعریف: میکند تابع بازیان $AON-CIRC$

فرضی میکند $f: \{0,1\}^n \rightarrow \{0,1\}^m$ بزرگ بازیان $AON-CIRC$ میکند

و دردی κ ضریب است. میتوانیم f را میاسه نهاده از

for every $\kappa \in \{0,1\}^n$ $P(n) = f(\kappa)$

Date:

Sub:

مثال حل شده:

تابع مقابل را در نظر بگیرید $f: \{0,1\}^4 \rightarrow \{0,1\}$ بیانی داده شده است در درستی $\text{CMP}: \{0,1\}^4 \rightarrow \{0,1\}$

$\text{CMP}(a,b,c,d) = 1$ iff $2a+b > 2c+d$

برای محاسبه AON-CIR برابر با CMP بتوانیم

حل: برای محتوا سه دو بعدی طبیعی است ابتدا بسته بر ارزش آن که را مقایسه نمایم
اگر بسته بر ارزش آن که برابر بود، بسته که بیش از ارزش مقایسی کتر را مقایسه می کنیم

برای محتوا سه دو بعدی طبیعی است ابتدا بسته بر ارزش آن که برابر نباشد
- بسته بر ارزش صردو عدد برابر داشته باشد
- بسته بر ارزش صردو عدد برابر نباشد

$$\text{CMP}(X) = 1 \text{ iff } 2X[0] + X[1] > 2X[2] + X[3]$$

$\begin{cases} \text{temp_1} = \text{NOT}(X[2]) \\ \text{temp_2} = \text{AND}(X[0], \text{temp_1}) \\ \text{temp_3} = \text{OR}(X[0], \text{temp_1}) \\ \text{temp_4} = \text{NOT}(X[3]) \\ \text{temp_5} = \text{AND}(X[1], \text{temp_4}) \\ \text{temp_6} = \text{AND}(\text{temp_5}, \text{temp_3}) \\ Y[0] = \text{OR}(\text{temp_2}, \text{temp_6}) \end{cases}$	$a, \bar{c} \text{ are}$ \bar{c} $a \wedge \bar{c}$ (1 iff equal) $a \vee \bar{c}$ \bar{d} $b \wedge \bar{d}$ $(b \wedge \bar{d}) \wedge (a \vee \bar{c})$ $(a \wedge \bar{c}) \vee [(b \wedge \bar{d}) \wedge (a \vee \bar{c})]$
---	--

اگر بسته جعلی بولن بودن AON-CIR باشد

$f: \{0,1\}^n \rightarrow \{0,1\}^m$ داشته باشد، $f: \{0,1\}^n \rightarrow \{0,1\}^m$ مغایر باشد؛ Theorem 3.9

اگر S بسته جعلی محاسبه خطا نماید، اگر و فقط اگر توسط

نمایشی بولن قابل محاسبه باشد AON-CIR

است: نوعی است که در این ساده theoreم است و فقط اس آنست، باید مدار بودن

را از سر در طرف اثبات نشانیم $\{n \in \mathbb{N} : f(n) = f(40,13^n)\}$

مرینی نیم P یک بنای AON-CIR است که فرآنشابی است. حال مدار به این صورت تعریف می‌کیم:

• عدای n ورودی دارد

• برای سر $[5] \times [5]$ یعنی آنچه line شماره n است

که AND Gate (a, b) است، آنکه a, b عدای کی

آنکه به دست آمده (آنکه a, b عدای کی AND Gate

که خروجی به line کی قابل است) متعال شود که عدای a, b از

آنکه به دست آمده (آنکه a, b عدای کی AND Gate

و خروجی Gate a, b متعال می‌شوند)

• آنکه متعارض باشد، همین بوضیع را

به Gate معرفی نیت می‌ریسم تا شان دفعه ضریب است.

هیچ فرآنش برای NOT, OR

• پیری سر ورودی $\{n \in \mathbb{N} : f(n) = 1\}$ است، آنچه line را اثبات نمی‌کند، مقدار به

دست آمده در line شماره n ، رفتیا همان مقدار به دست آمده

از Gate شماره n خواهد بود. بنابراین می‌توان نتیجه

for every $n \in \mathbb{N}$, $C(n) \leq P(n)$

پیری اثبات از طرف مقابله، فرض می‌نماییم یک مدار با دیدگردی و دادروغی

است که باعث می‌شود مدار می‌کند

• اثبات Gate کی C را لاین ترتیب تغییراتی کی مرتب کرد و آنکه

لاین $-1, -2, -3, \dots$ می‌نویسیم

حالی توانیم برای \oplus با خط عملیات به صورت زیر بتویم:

برای سر $i \in [S]$ اس v_i با صارکی AND Gate مدل کنیم.

و دری v_j, v_k است، آن‌ها خواهند برابر باشد اگر و تنوعی شود:

$$\text{temp}_i = \text{AND}(\text{temp}_j, \text{temp}_k)$$

(مکانیکی این را می‌دانیم که از روش i input و i output است که این

صورت پراستاری AND $\wedge[-]$ است، $X[-]$ به $\wedge[-]$ تبدیل می‌شوند)

از آن حالت طبق ترتیب تولید کردم، تفسیم شده که مقادیر v_k

در مراحل قبلی مشخص شده است

* همین ترانزیستوری NOT, OR نیز انجام می‌شود

محبذا حقیقتی نیست که برای صورت \oplus معامل $P(n)$ باشد

معکار $C(n)$ خواهد شد

به خاطر داشته باشید که مدار معتبر و منطقی با تعریف 3.5

است که در آن سریس input، حالت i صفاتی ضروری و دستیار m عدد

با برجسته کی output Gate

بنابراین $\wedge[m-1], \wedge[m-2], \dots, \wedge[0]$ و $X[n-1], X[n-2], \dots, X[0]$ در برای P

نمایه خواهند شد

سازی فیزیکی وسیله کی محاسباتی

→ عبارتی مفهوم انتزاعی است که اینجا به سازی فیزیکی خود مستقل است.

در طول تاریخ محاسبه به وسیله کامپیوتری متوجه مانند یک کامپیوتر باز و باعده

اجام شده است.

در نخستین باره کامپیوتری سازی فیزیکی Boolean Circuit را تشریح خواهیم کرد.