Multiplizieren und Dividieren mittels flacher Schaltkreise

Sommerakademie Rot an der Rot — AG 1
Wieviel Platz brauchen Algorithmen wirklich?

Benedikt Rieger

16. August 2010

Gliederung

Wieso werden schnelle Berechnungen gebraucht?

Multiplikationsproblem

Problemstellung:

Für ein gegebenes n soll die Funktion $m_n : \{0,1\}^{2n} \to \{0,1\}^{2n}$ berechnet werden
Die ersten n Bits der Eingabe sollen mit den zweiten n Bits multipliziert werden und das das Ergebnis zurückliefet

Ziel

Möglichst flacher Schaltkreis

NC^1

Ziel

Multiplikation in NC^1 mit einer Tiefe von $O(\log n)$

Das Problem

Schon die Addition zweier Zahlen brauchen eine Tiefe von $O(\log n)$

NC^1

Ziel

Multiplikation in NC^1 mit einer Tiefe von $O(\log n)$

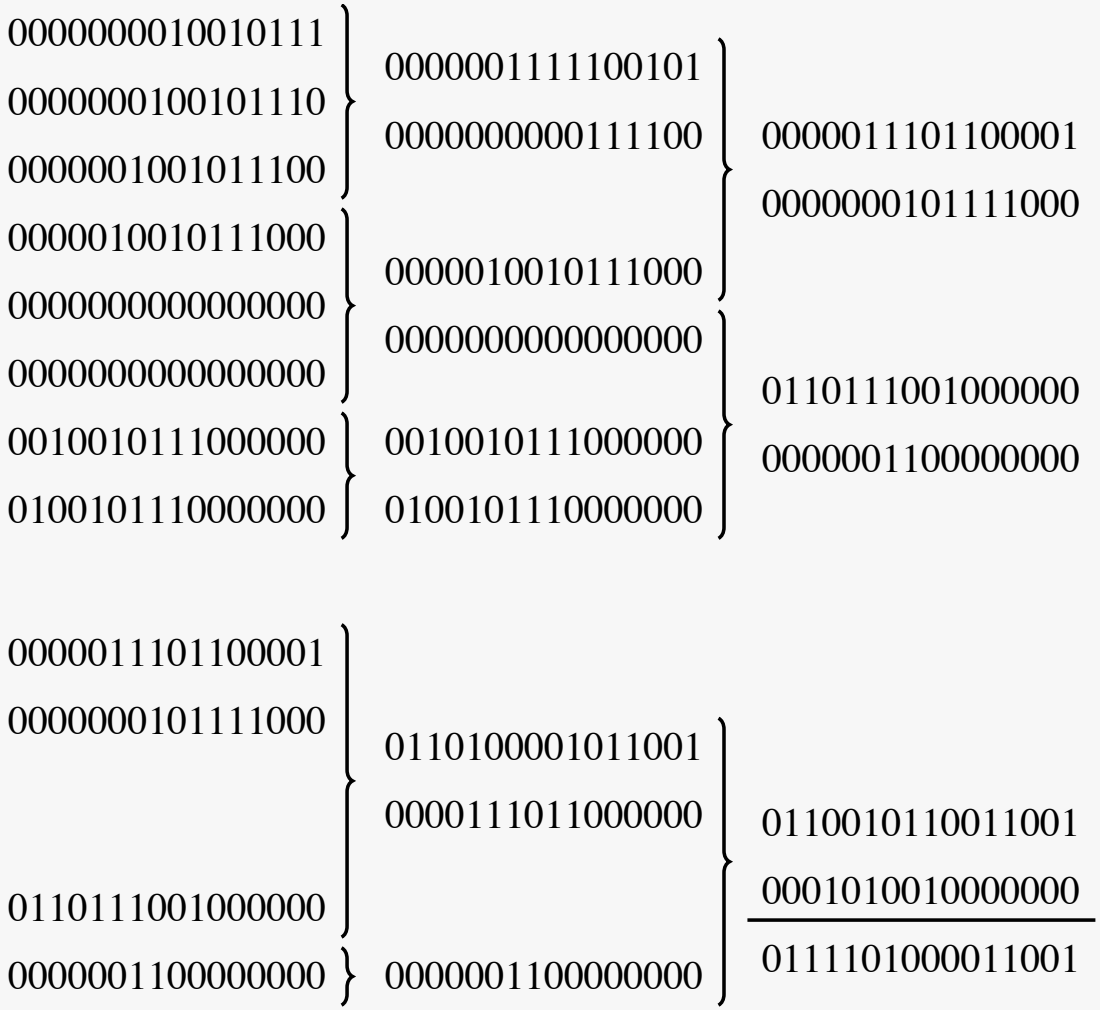
Das Problem

Schon die Addition zweier Zahlen brauchen eine Tiefe von $O(\log n)$

Lösungsidee

Addition von Zahlen in der Tiefe $O(1)$

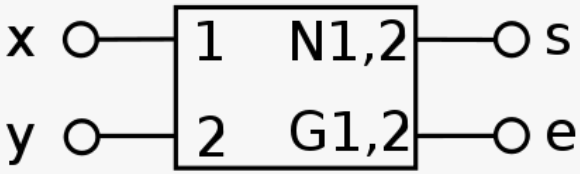
Beispiel

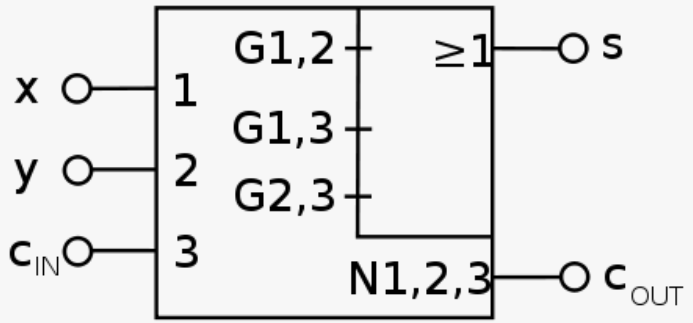

0000000010010111
0000000100101110
0000001001011100
0000010010111000
0000000000000000
0000000000000000
0010010111000000
0100101110000000
0000001111100101
0000000000111100
0000010010111000
0000000000000000
0010010111000000
0100101110000000
0000011101100001
0000000101111000
0110111001000000
0000001100000000
0000011101100001
0000000101111000
0110100001011001
0000111011000000
0000001100000000
0110010110011001
0001010010000000
0111101000011001

Addierer

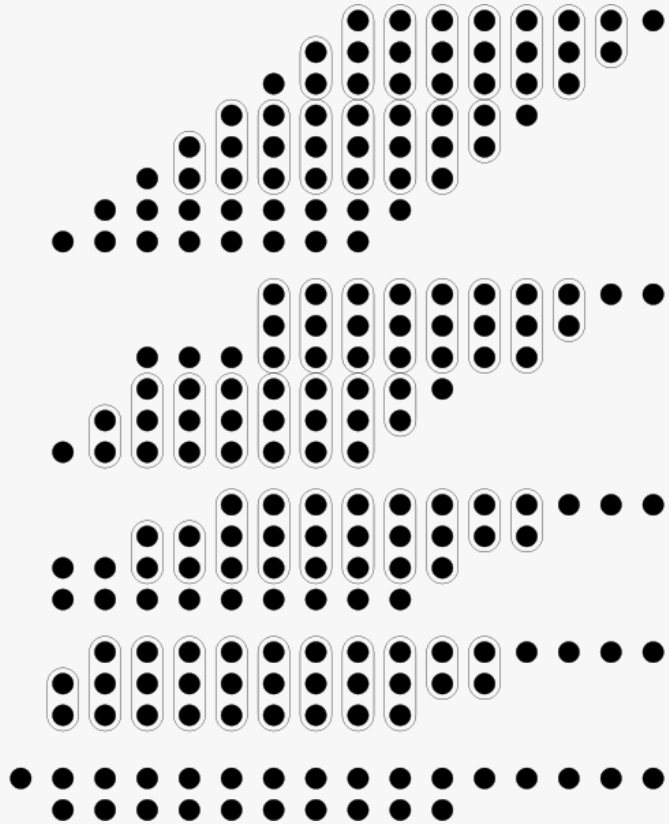
Volladdierer Addiert die drei Eingängen x, y, c_{in} zu s, die niederwertige Stelle des Ergebnisses und c_{out} die höherwertige

Halbaddierer Addiert zwei einstellige Binärzahlen. Dabei ist s die niederwertige Stelle des Ergebnisses und c die höherwertige

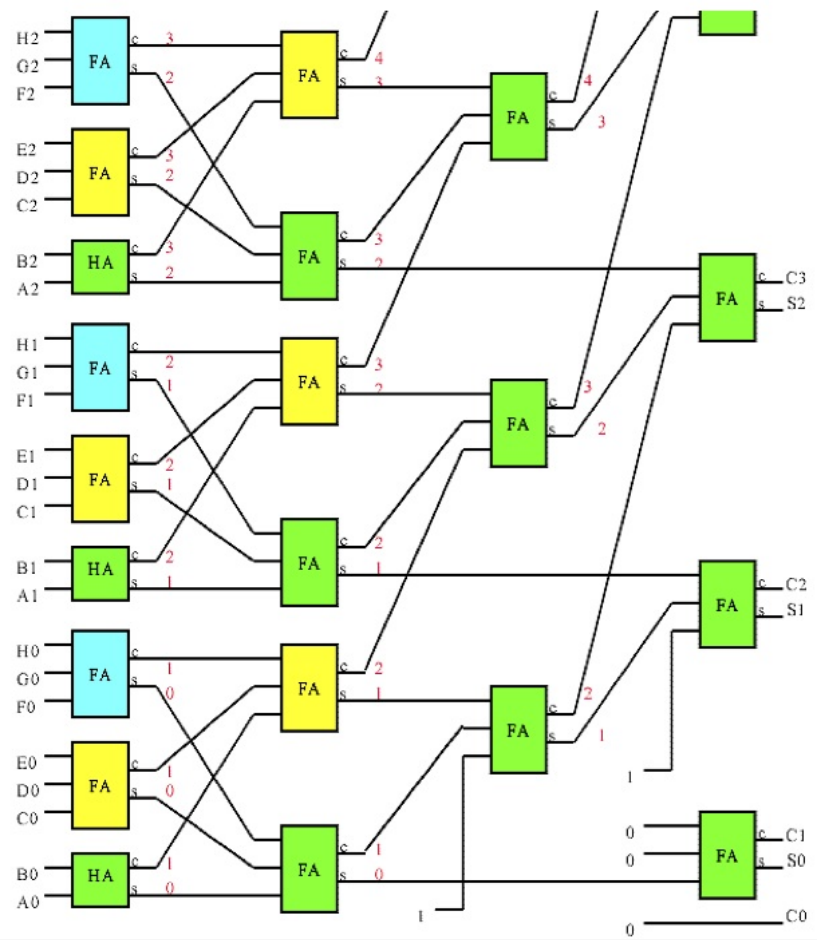




- Erzeuge n Zahlen, deren Summe das Ergebnis liefern
- Nimm 3 Ziffern der gleichen Gewichtung und verbinde mit einem Volladdierer
- Sind nur 2 Ziffern der gleichen Gewichtung übrig, verbinde mit Halbaddierer
- Ist nur eine Ziffer übrig, wird sie mit der nächsten Ebene verbunden
- Wiederhole diese Schritte, bis nur noch 2 Schichten übrig sind



Wallace-Tree



Division

Ziel

Möglichst Flacher Schaltkreis für die Division

Vereinfachungen

- $c/d = c \cdot (1/d) \rightarrow$ wir können schon Mutliplizieren

Lösungsmethode

Approximation von $d' = 1/d$

n-Approximation

Definition der n-Approximation

Sei $c \in \mathbb{R}$ eine Zahl. Eine n-Approximation von c ist eine Zahl $\tilde{c}$ mit

$$| c - \tilde{c} | \leq 2^{-n}$$

Problemstellung

Eingabe n-Bit Zahl d mit $1/2 \leq d \leq 1$

Ausgabe $2n$-Approximation von $1/d$

n-Approximation

Gesucht

Eine Funktion, deren Nullstelle $1/d$ ist

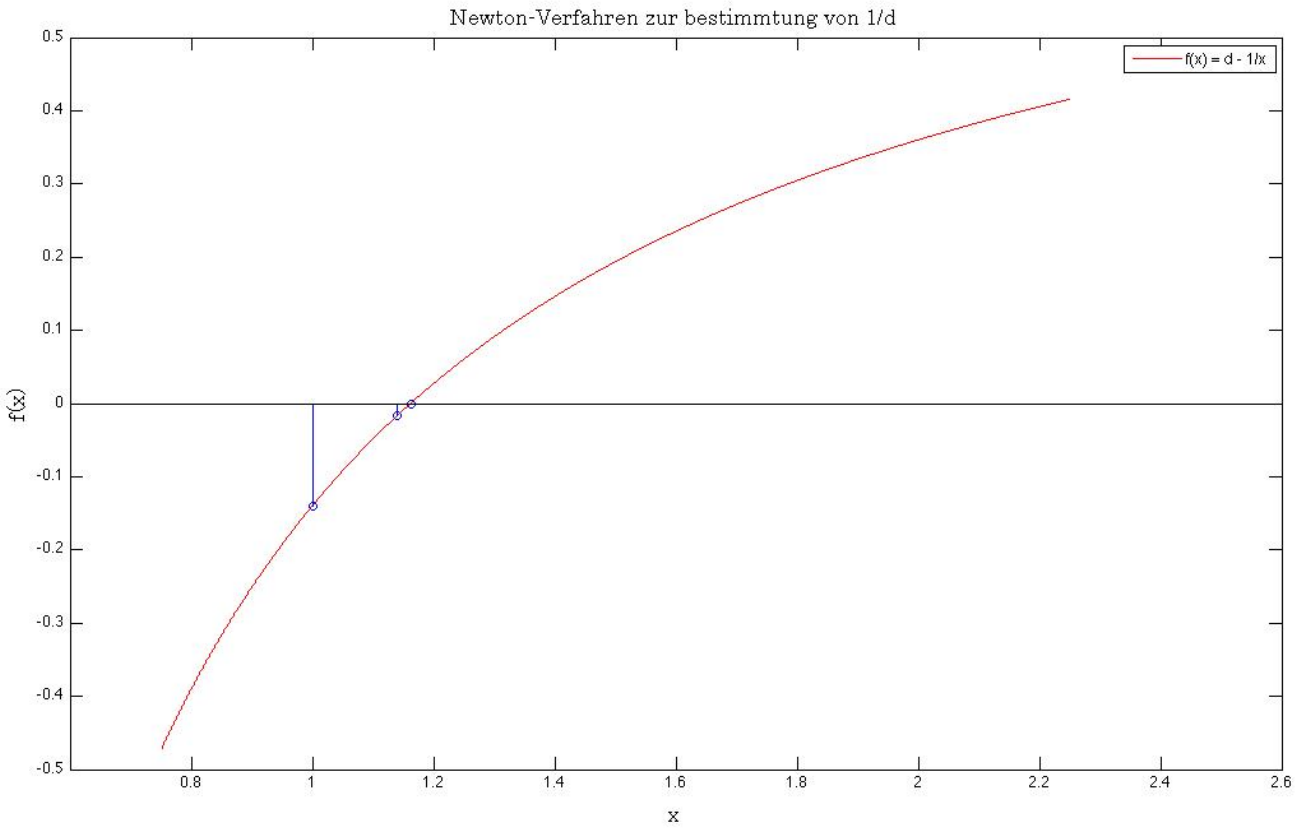
Lösung

Die Funktion $f(x) = d - 1/x$ erfüllt Bedingung

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} = x_n - \frac{d - 1/x_n}{1/x_n^2} = x_n(2 - dx_n)$$

Der Startwert sei $x_0 = 1$

Beispiel



$d = 0.86$

Newton-Verfahren Konvergezkriterium allgemein

Satz

Sei f eine im Intervall [a,b] zweifach stetig differenzierbare Funktion mit $f'(x) \neq 0$ für alle $x \in [a, b]$. Sei

$$\max_{x \in [a,b]} \left| \frac{f(x) \cdot f''(x)}{f'(x)^2} \right| \leq 1.$$

Dann exisitiert exakt eine Nullstelle x von f im Intervall [a,b] und die Folge

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, n \in \mathbb{N}$$

konvergiert gegen die Nullstelle für alle $x_0 \in [a, b]$

Zusammenfassung

Multiplikation in NC^1 mit der Tiefe $O(\log n)$ möglich

Division mit einer n-Approximation durch das Newton-Verfahren in NC^2 möglich

Vielen Dank für Ihre Aufmerksamkeit!

Newton-Verfahren Konvergezkriterium bei der Division

Satz

Sei d mit $1/2 \leq d \leq 1$ gegeben. Sei $x_0 = 1$ der feste Startwert und sei

$$x_{k+1} = x_k(2 - dx_k).$$

Dann ist $x_k$eine 2^{-2^k+2}-Approximation von $1/d$.

Beweis

- Es gilt $x_k = \sum_{i=0}^{2^k-1} (1-d)^i$.
- Es gilt, dass $x_{k+1} = \sum_{i=0}^{2k+1} (1-d)^i$ eine $2k$-Approximation von $1/d$ ist.

Zur Behauptung $x_k = \sum_{i=0}^{2^k-1} (1-d)^i$

$$\begin{aligned} x_{k+1} &= x_k(2 - dx_k) \\ &= \dots \\ &= \sum_{i=0}^{2^{k+1}-1} (1-d)^i \end{aligned}$$

Zur Behauptung $x_{k+1} = \sum_{i=0}^{2k+1} (1-d)^i$ seine eine $2k$-Approximation von $1/d$

$$\begin{aligned} \left| 1/d - \sum_{i=0}^{2k+1} (1-d)^i \right| &= \left| \sum_{i=0}^{\infty} (1-d)^i - \sum_{i=0}^{2k+1} (1-d)^i \right| \\ &= \sum_{i=2k+2}^{\infty} (1-d)^i \leq \sum_{i=2k+2}^{\infty} 2^{-i} \end{aligned}$$