

## Die Taktzahl beim von-Neumann-Addierwerk

Gegeben  $x = (x_n, \dots, x_0)$  und  $y = (y_n, \dots, y_0)$ .

**Definition:** Ein 1-Block in  $(x, y)$  der Länge  $\ell \geq 0$  an der Position  $i$  liegt vor, wenn  $x_i = y_i = 1$  ist und für alle  $j$  mit  $i + 1 \leq j \leq i + \ell$  gilt, dass  $x_j \oplus y_j = 1$  ist.

**Definition:**  $L(x, y)$  sei gleich  $-1$ , falls es keinen 1-Block in  $(x, y)$  gibt und sei sonst die Länge des längsten 1-Blocks in  $(x, y)$ .

**Bsp.:**

$$\begin{aligned} x &= (0, 1, 0, 1, 0) \\ y &= (0, 0, 1, 1, 0) \end{aligned}$$

hat als längsten 1-Block einen der Länge 2 an der Position 1, damit ist  $L(x, y) = 2$ .

**Satz:** Auf Eingaben  $(x, y)$  braucht das von-Neumann-Addierwerk maximal  $L(x, y) + 2$  Takte.

**Beweis:** Durch Induktion über  $L(x, y)$ . Wenn  $L(x, y) = -1$  ist, dann enthält  $(x, y)$  keinen 1-Block. Auf solchen Inputs braucht das von-Neumann-Addierwerk aber maximal einen Takt: Denn entweder ist  $y = (0, \dots, 0)$ , dann wird überhaupt kein Takt benötigt. Oder es ist  $y^{neu} = (0, \dots, 0)$ , da alle  $x_i \wedge y_i = 0$  sind (es gibt keine 1-Blöcke). Dann ist also nach einem Takt Schluss.

Nun zum Induktionsschritt. Dann ist  $L(x, y) \geq 0$ .

Es reicht, zu zeigen, dass  $L(x^{neu}, y^{neu}) \leq L(x, y) - 1$  ist, da das von-Neumann-Addierwerk ja in genau einem Takt aus  $(x, y)$  die Zahlen  $(x^{neu}, y^{neu})$  macht.

Fall 1:  $(x^{neu}, y^{neu})$  enthält keinen 1-Block. Dann ist  $L(x^{neu}, y^{neu}) = -1 \leq L(x, y) - 1$ .

Fall 2: Es gibt mindestens einen 1-Block in  $(x^{neu}, y^{neu})$ . Einen solchen greifen wir uns heraus und überlegen uns, wie  $x$  und  $y$  ausgesehen haben können.

Erste Überlegung: Wenn für irgendein  $j$  gilt, dass  $x_j^{neu} = 1$  ist, dann kann nicht  $y_{j+1}^{neu} = 1$  sein, denn aus  $x_j^{neu} = x_j \oplus y_j = 1$  folgt  $x_j \wedge y_j = 0$ .

Wenn wir also einen 1-Block in  $(x^{neu}, y^{neu})$  haben, der an Position  $i$  beginnt und Länge  $\ell$  hat, dann sieht dieser so aus:

Spaltennr.:	$i + \ell$	$\dots$	$i + 1$	$i$
$x^{neu}$	1	$\dots$	1	1
$y^{neu}$	0	$\dots$	0	1

Wegen  $y_i^{neu} = 1$  wissen wir  $x_{i-1} = 1$  und  $y_{i-1} = 1$  und wegen  $x_j^{neu} = 1$  für  $j = i, \dots, i + \ell$  wissen wir nach Definition der  $x_j^{neu}$  auch, dass  $x_j \oplus y_j = 1$  für  $j = i, \dots, i + \ell$ .

Damit haben wir in  $(x, y)$  die Existenz eines 1-Blocks nachgewiesen, der an Position  $i-1$  beginnt und Länge mindestens  $\ell + 1$  hat.

Somit folgt natürlich (mit Wahl von  $\ell = L(x, y)$ ), dass

$$L(x, y) \geq L(x^{neu}, y^{neu}) + 1, \quad \text{also } L(x^{neu}, y^{neu}) \leq L(x, y) - 1.$$

Das von-Neumann-Addierwerk startet zur Addition der beiden Binärzahlen  $a_{n-1}, \dots, a_0$  und  $b_{n-1}, \dots, b_0$  mit den beiden Zahlen

$$x = (0, a_{n-1}, \dots, a_0) \text{ und } y = (0, b_{n-1}, \dots, b_0).$$

Für zufällige Inputs  $(a_{n-1}, \dots, a_0)$  und  $(b_{n-1}, \dots, b_0)$ , bei denen jedes Bit unabhängig von den anderen die Werte 0 und 1 mit Wahrscheinlichkeit  $1/2$  annimmt, ist die Zahl  $L(x, y)$  eine Zufallsvariable. Wenn  $E(L)$  den Erwartungswert von  $L(x, y)$  bezeichnet, so ist  $E(L) + 2$  eine obere Schranke für die erwartete Taktzahl des von-Neumann-Addierwerks. Es ist

$$\begin{aligned} E(L) &= \sum_{i=-1}^{n-1} i \cdot \text{Prob}(L = i) \leq \sum_{i=0}^{n-1} i \cdot \text{Prob}(L = i) \\ &= \sum_{i=1}^{n-1} \text{Prob}(L \geq i) \quad (*) \\ &= \sum_{i=1}^{\lceil \log n \rceil} \text{Prob}(L \geq i) + \sum_{i=\lceil \log n \rceil+1}^{n-1} \text{Prob}(L \geq i) \\ &\leq \lceil \log n \rceil + \sum_{i=\lceil \log n \rceil+1}^{n-1} n \cdot 2^{-i} \\ &= \lceil \log n \rceil + n \cdot \sum_{i=\lceil \log n \rceil+1}^{n-1} 2^{-i} \quad (**) \\ &\leq \lceil \log n \rceil + n \cdot 2^{-\lceil \log n \rceil} \leq \lceil \log n \rceil + 1 \end{aligned}$$

Die Gleichheit (\*) erklärt sich wie folgt:

$$\begin{aligned} \text{Prob}(L \geq 1) &= \text{Prob}(L = 1) + \text{Prob}(L = 2) + \text{Prob}(L = 3) + \dots \\ \text{Prob}(L \geq 2) &= \text{Prob}(L = 2) + \text{Prob}(L = 3) + \dots \\ \text{Prob}(L \geq 3) &= \text{Prob}(L = 3) + \dots \end{aligned}$$

Die Summe von  $\text{Prob}(L \geq 1)$  bis  $\text{Prob}(L \geq n-1)$  enthält also jedes  $\text{Prob}(L = i)$  genau  $i$  mal. Die Ungleichung (\*\*) ergibt sich aus der folgenden Überlegung:

Wir beobachten zunächst, dass bei zufällig gewählten  $x$  und  $y$  gilt, dass  $x_j \oplus y_j = 1$  mit Wahrscheinlichkeit  $1/2$  ist.

Wenn  $L \geq i$  ist, gibt es eine Position  $T \in \{0, \dots, n-1\}$  mit  $x_T = y_T = 1$  und  $x_j \oplus y_j = 1$  für alle  $j = T+1, \dots, T+i-1$ . Die Wahrscheinlichkeit dafür ist bei festem  $T$  höchstens  $(1/2)^i$ . Da es maximal  $n$  Möglichkeiten gibt,  $T$  zu wählen, ist die Wahrscheinlichkeit  $\text{Prob}(L \geq i) \leq n \cdot 2^{-i}$ .