Die Addition im Zweierkomplement

(Zusätzliche Betrachtungen zum Zweierkomplement)

Oliver Meyer / Jan Peleska

Das Zweierkomplement eignet sich aufgrund der Eigenschaften, die auf dem Beweispapier „Eigenschaften des Zweierkomplements“ gezeigt wurden, sehr gut, um negative Zahlen im Rechner zu repräsentieren. Dabei wird, um einen eindeutigen Indikator für eine Zweierkomplementdarstellung einer Bitkette zu haben, der Zahlenbereich so gewählt, dass das höchstwertigste Bit genau dann den Wert 1 erhält, wenn es sich bei der gespeicherten Zahl um eine negative Zahl handelt. Damit lassen sich dann eine Abstraktionsfunktion ρ und eine Operation $\tilde{+}$ definieren, die es ermöglichen, eine rechnerinterne Addition als eine Addition im Bereich der ganzen Zahlen zu deuten.

Im folgenden seien $x, y \in \{0, \ldots, 2^{n+1} - 1\}$ und $(x_n \ldots x_0)_2$ die Binärdarstellung einer Zahl x mit $x_i \in \{0, 1\}$.

Definition 1 (Abstraktionsfunktion)

Die Abstraktionsfunktion ρ (auch Retrievefunktion genannt), um aus einer rechnerinternen Binärdarstellung die entsprechende ganze Zahl zu bestimmen, ist folgendermassen definiert:

$$\rho(x) \quad = \quad \begin{cases} x & \textit{falls} \quad x_n = 0 \\ -(2^n - (x \; \underline{mod} \; 2^n)) & \textit{falls} \quad x_n = 1 \end{cases}$$

wobei der Wertebereich (range) $\underline{ran}\, \rho = \{-2^n, \ldots, 2^n - 1\}$ gilt.

Anmerkung: Im Fall $x_n = 1$ entspricht der Wert $\rho(x)$ dem Ergebnis des Ausdrucks $-K_2(x)$ (vgl. Lemma 3 des oben erwähnten Beweispapiers). □

Definition 2 (Addition auf $\mathbb{B}^{n+1}$)

$\tilde{+}$ ist eine längenbeschränkte Addition auf Binärzahlen, wobei eventuell entstehende Überträge abgeschnitten werden:

$$x \tilde{+} y \quad = \quad (x + y) \; \underline{mod} \; 2^{n+1}$$

Aufgrund der Anwendung in Kombination mit dem Zweierkomplement ist $\tilde{+}$ in seinem Definitionsbereich (domain) eingeschränkt:

$$\begin{aligned} \underline{dom}\, \tilde{+} \quad = \{(x, y) : \mathbb{B}^{n+1} \times \mathbb{B}^{n+1} \quad | \quad & (x_n = 1 \wedge y_n = 1 \wedge ((x_{n-1} \ldots x_0)_2 + (y_{n-1} \ldots y_0)_2) \geq 2^n) \\ & \vee \\ & (x_n \oplus y_n = 1) \\ & \vee \\ & (x_n = 0 \wedge y_n = 0 \wedge ((x_{n-1} \ldots x_0)_2 + (y_{n-1} \ldots y_0)_2) < 2^n)\} \end{aligned}$$

□

Mit diesen Definitionen lässt sich das folgende kommutierende Diagramm aufstellen:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\ \uparrow \rho \times \rho & & \uparrow \rho \\ \mathbb{B}^{n+1} \times \mathbb{B}^{n+1} & \xrightarrow{\tilde{+}} & \mathbb{B}^{n+1} \end{array}$$

Diese Diagramm besagt, dass eine binäre rechnerinterne Addition mit $\tilde{+}$ zu dem gleichen Ergebnis führt wie eine Addition in den Ganzen Zahlen, sofern die Abstraktionsfunktion ρ verwendet wird, um den Übergang von den Binärzahlen zu den Ganzen Zahlen zu realisieren.

Definition 3 (Verfeinerung von $+$)

$\tilde{+}$ ist eine Verfeinerung von $+$ bzgl. ρ falls gilt:

$$\forall (x,y): \ \underline{dom}\,\tilde{+} \quad \bullet \quad \rho(x) + \rho(y) = \rho(x \tilde{+} y)$$

□

Satz 1 (Verfeinerungseigenschaft)

Für alle $(x,y) \in \underline{dom}\,\tilde{+}$ gilt:

$$\rho(x \tilde{+} y) \quad = \quad \rho(x) + \rho(y)$$

Beweis

Für den Beweis des vorangehenden Satzes wird eine Fallunterscheidung entsprechend der drei Bereiche des Definitionsbereichs der Operation $\tilde{+}$ vorgenommen.

Fall 1: $x_n = 0 \wedge y_n = 0$

$$\begin{array}{rrcll} & x \tilde{+} y & = & (x+y) \ \underline{\mathrm{mod}} \ 2^{n+1} & [\text{Def. } \tilde{+}] \\ & & = & (x+y) \ \underline{\mathrm{mod}} \ 2^{n} & [(x,y) \in \underline{\mathrm{dom}}\,\tilde{+}] \\ \Rightarrow & \rho(x \tilde{+} y) & = & x + y & [\text{Def. von } \rho] \\ & & = & \rho(x) + \rho(y) & [x, y < 2^n, \text{Def. von } \rho] \end{array}$$

Fall 2: $x_n = 1 \wedge y_n = 1$

$$\begin{array}{rrcll} & x \tilde{+} y & = & (x+y) \ \underline{\mathrm{mod}} \ 2^{n+1} \geq 2^n & [\text{Def. } \tilde{+}, (x,y) \in \underline{\mathrm{dom}}\,\tilde{+}] \\ \Rightarrow & \rho(x \tilde{+} y) & = & -(2^n - (x+y) \ \underline{\mathrm{mod}} \ 2^n) & [\text{Def. von } \rho, \text{wg. Fallunterscheidung}] \\ & \rho(x) & = & -(2^n - x \ \underline{\mathrm{mod}} \ 2^n) & [\text{wg. Fallunterscheidung}] \\ & \rho(y) & = & -(2^n - y \ \underline{\mathrm{mod}} \ 2^n) & [\text{wg. Fallunterscheidung}] \\ \Rightarrow & \rho(x) + \rho(y) & = & -2 \cdot 2^n + x \ \underline{\mathrm{mod}} \ 2^n + y \ \underline{\mathrm{mod}} \ 2^n & \\ & & = & -2 \cdot 2^n + 2^n + (x+y) \ \underline{\mathrm{mod}} \ 2^n & [(x,y) \in \underline{\mathrm{dom}}\,\tilde{+}] \quad * \\ & & = & -2^n + (x+y) \ \underline{\mathrm{mod}} \ 2^n & \\ & & = & \rho(x \tilde{+} y) & \end{array}$$

In diesem Fall ist der Schritt * etwas erklärungswürdig: Aufgrund der Domain der Operation $\tilde{+}$ muss bei der Addition der niederwertigsten n Bits der Operanden x und y ein Übertrag stattfinden, da ansonsten das Ergebnis der Addition nicht mehr im Bereich der darstellbaren negativen Zahlen liegen würde. Dies wird hier ausgenutzt, um die beiden Modulo-Operationen zusammenfassen zu können.

Fall 3: O. b. d. A. : $x_n = 1 \wedge y_n = 0$

$$x \tilde{+} y \quad = \quad (x+y) \underline{\text{mod}}\ 2^{n+1} \quad \text{[Def. } \tilde{+}\text{]}$$

Fall 3.1: Negatives Ergebnis der Addition: $x \underline{\text{mod}}\ 2^n + y \underline{\text{mod}}\ 2^n < 2^n$

$$\begin{array}{rrcll}
\Rightarrow & (x+y) \underline{\text{mod}}\ 2^{n+1} & = & 2^n + (x+y) \underline{\text{mod}}\ 2^n & \\
\Rightarrow & \rho(x \tilde{+} y) & = & -(2^n - (x+y) \underline{\text{mod}}\ 2^n) & \text{[Def. } \rho, \text{wg. Fallunterscheidung]} \\
 & \rho(x) & = & -(2^n - x \underline{\text{mod}}\ 2^n) & \\
 & \rho(y) & = & y \ = \ y \underline{\text{mod}}\ 2^n & \\
\Rightarrow & \rho(x) + \rho(y) & = & -2^n + x \underline{\text{mod}}\ 2^n + y \underline{\text{mod}}\ 2^n & \\
 & & = & \rho(x \tilde{+} y) &
\end{array}$$

Fall 3.2: Positives Ergebnis der Addition: $x \underline{\text{mod}}\ 2^n + y \underline{\text{mod}}\ 2^n \geq 2^n$

$$\begin{array}{rrcll}
\Rightarrow & (x+y) \underline{\text{mod}}\ 2^{n+1} & = & (x+y) \underline{\text{mod}}\ 2^n & \text{[wg. Fallunterscheidung]} \\
\Rightarrow & \rho(x \tilde{+} y) & = & (x+y) \underline{\text{mod}}\ 2^n & \\
 & \rho(x) & = & -(2^n - x \underline{\text{mod}}\ 2^n) & \\
 & \rho(y) & = & y \ = \ y \underline{\text{mod}}\ 2^n & \\
\Rightarrow & \rho(x) + \rho(y) & = & -2^n + x \underline{\text{mod}}\ 2^n + y \underline{\text{mod}}\ 2^n & \\
 & & = & -2^n + 2^n + (x+y) \underline{\text{mod}}\ 2^n & \text{[siehe Fall 2(*) und Falluntersch.]} \\
 & & = & (x+y) \underline{\text{mod}}\ 2^n & \\
 & & = & \rho(x \tilde{+} y) &
\end{array}$$

$\square$