Das Stellenwertsystem

Polynomschreibweise

$d_n = \text{Ziffer} \in Z_n, R^n = \text{Wertigkeit}$

$N_n = d_n R^n + d_{n-1} R^{n-1} + ... + d_1 R^1 + d_0 R^0$

Dezimalsystem

$R_{10} = 10$ (Basis); $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Dualsystem

$R_2 = 2$ (Basis); $Z_2 = \{0, 1\}$

Beispiel

$N_2 = 110$ $N_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 4_d + 2_d = 6_d$

Oktalsystem

$R_8 = 8$ (Basis); $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Beispiel

$N_8 = 110$ $N_8 = 1 \cdot 8^2 + 1 \cdot 8^1 + 0 \cdot 8^0 = 72_d$

Kommazahlen

$\mathbb{R}_{10} = 110.13$ $N_{10} = 1 \cdot 10^2 + 1 \cdot 10^1 + 0 \cdot 10^0 + 1 \cdot 10^{-1} + 3 \cdot 10^{-2}$

$\mathbb{R}_2 = 101.110$ $N_2 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 + 1 \cdot 2^{-1} + 1 \cdot 2^{-2} + 0 \cdot 2^{-3} = 5.75_d$

Subtrahieren durch Addieren

Annahme: Bei 1000 gibt es einen **Überlauf**.

$753 + 247 = 0$, daraus folgt $753 \equiv -247$

Somit ist $620 - 247 \equiv 620 + 753 = 1373 \equiv 373$.

Additive Zahl berechnen

Gesucht: Additive Zahl von –247 (, also 753). hhhh

$$999 - 247 = 752 \text{ (Neunerkomplement)}$$
$$752 + 1 = 753 \text{ (Zehnerkomplement)}$$

Dualzahlen

-1:
$1 = 0001_2$.
Einerkomplement: 1110_2
Zweierkomplement: $1111_2 = -1$

Unsigned Multiplikation

Die unsigned Multiplikation ist eine Summe von Links-Shifts.

$a = 3, b = 5$

$$0011 * 0101$$
$$= 0101 + 1010$$

Signed Multiplikation

Die signed Multiplikation funktioniert analog zur unsigned Multiplikation, aber wenn einer der Operanden negativ ist, muss das Zweierkomplement davon gebildet werden:

Beispiel

$1101 * 0111$ $((-3) \cdot 7 = -21)$

1101 ist negativ, das Zweierkomplement ist 0011.

$0011 * 0111 = 0111 + 01110 = 010101$. Das Zweierkomplement davon ist 101011 (= –21).

Indexschreibweise

$b = 1010$

$b_3 = 1, b_2 = 0, b_1 = 1, b_0 = 0$

$b_{3..1} = 101, b[3..1] = 101$

Subtrahieren

Betrag mit Vorzeichen

$$5 - 1$$
$$5 = 0101$$
$$-1 = 1001$$
$$0101 - 0001 = 0100 = 4$$

Einerkomplement (b-1)

Von negativen Zahlen wird das Einerkomplement gebildet. Gibt es nach Addition einen Überlauf, muss noch +1 gerechnet werden.

$$5 - 1$$
$$5 = 0101$$
$$1 = 0001, -1 = 1110$$
$$0101 + 1110 = 10011$$
$$\Rightarrow \text{Überlauf} \Rightarrow 0011 + 1 = 0100 = 4$$

Zweierkomplement (b-Komplement)

$$5 - 1$$
$$5 = 0101$$
$$1 = 0001, -1 = 1111$$
$$0101 + 1111 = 10100 \Rightarrow \text{Überlauf} \Rightarrow 0100 = 4$$

Allgemeine Berechnung des b-Komplements

$$C_{b,n}(N) = b^n - N$$

- n = Anzahl Stellen
- b = Basis
- N = Zahl, von welcher das Komplement gebildet werden soll

Beispiel:

- $C_{8,2}(6) = 8^2 - 6 = 58_{10} = 72_8$

Im Dualsystem entspricht dies dem Zweierkomplement.

Excesscode

Der Excesscode, der den Zahlenbereich in zwei gleich grosse Hälften aufteilt, hat einen besonderen Stellenwert. Dabei gehört die 0 zu den negativen Zahlen. Beispiel: Bei vierstelligen Codes würde der Excess-7-Code $C_{\text{Ex},-7,4}(x)$ die Zahlen von –7 bis 8 darstellen. Der Bias ergibt sich dann durch $2^{n-1} - 1$.

Um eine Zahl a zu kodieren, wählt man die kleinste Zahl b im Wertebereich und bildet die Differenz $d = |a - b|$. Beispiel:

$$C_{\text{ex},-4,3}(-1) = ?$$
$$d = |-1 - (-4)| = 3 \Rightarrow 011$$

Fixkommazahlen

$C_{\mathrm{FK},k,n}(x)$, wobei
- k = Anzahl Nachkommastellen
- n = Länge der binären Schreibweise

Beispiel: $C_{\mathrm{FK},4,16}(453.1234) = 0001'1100'0101'0001$

Absoluter Fehler

$E_{\mathrm{abs}} = |x_{\mathrm{korrekt}} - x_{\mathrm{gerundet}}|$

Relativer Fehler

$E_{\mathrm{rel}} = \frac{|x_{\mathrm{korrekt}} - x_{\mathrm{gerundet}}|}{x_{\mathrm{korrekt}}}$

Gleitkommazahlen

Bei Gleitkommazahlen wird zusätzlich zum Bitmuster z auch die Stelle k mitgeführt, an der das Komma steht.
- z = Signifikand, Mantisse
- k = Exponent
- $C_{\mathrm{GK},k,n}(z) = z \cdot 2^k$

Beispiel: 6.25.

$6 = 0110, 0.25 = 0.01$

Fixkommarepräsentation: 0110.01

Gleitkommazahlrepräsentation: $1.1001 \cdot 2^2$

Für die Mantisse wird die Excess-Darstellung verwendet, d.h. bei 8-Bit-Mantisse der $C_{\mathrm{Ex},-127,8}$. Der Exponent 2 wird so zu 10000001.

Als 32-Bit-Gleitkommazahl: $0'10000001'10010000000000000000000$

0	10000001	10010000000000000000000
Vorzeichen	Exponent	Mantisse

Standard IEEE 754

- Single: 24 Bit Präzision, 8 Bit Exponent
- Double: 53 Bit Präzision, 11 Bit Exponent
- Quadruple: 113 Bit Präzision, 15 Bit Exponent

Addition

1. Wenn Vorzeichen unterschiedlich: Subtraktion
2. Hidden Bits ergänzen
3. Wenn Exponenten unterschiedlich: Signifikand der kleineren Zahl um entsprechend viele Bits nach rechts verschieben
4. Addition durchführen
5. Falls Carry = 1: Ergebnis normalisieren:
   - Exponent um 1 erhöhen
   - Signifikand um 1 nach rechts schieben

- $x = 1.5,\ y = 0.75$
- $x = 0\,|\,0111\ 1111\,|\,100\ 0000\ 0000\ 0000\ 0000\ 0000$
- $y = 0\,|\,0111\ 1110\,|\,100\ 0000\ 0000\ 0000\ 0000\ 0000$
- $x' = 0\,|\,0111\ 1111\,|(1)\,100\ 0000\ 0000\ 0000\ 0000\ 0000$ mit hidden Bit
- $y' = 0\,|\,0111\ 1111\,|(0)\,110\ 0000\ 0000\ 0000\ 0000\ 0000$ m.h.B., $a+1,\ m \cdot 2^{-1}$
- $z' = 0\,|\,0111\ 1111\,|(10)\,010\ 0000\ 0000\ 0000\ 0000\ 0000 = x' + y'$
- $z'' = 0\,|\,1000\ 0000\,|(1)\,001\ 0000\ 0000\ 0000\ 0000\ 0000\ \ a+1,\ m \cdot 2^{-1}$
- $z = 0\,|\,1000\ 0000\,|\,001\ 0000\ 0000\ 0000\ 0000\ 0000$ ohne hidden Bit
- $z = 2.25$

Gruppe, Ring und Körper

Körper

Ein Ring ist ein Körper, wenn:
a) Jedes Element des Rings (ausser der 0) ein multiplikatives Inverses hat
b) Die Multiplikation kommutativ ist: $ab = ba$ (Abel'sche Gruppe)

c) Das Distributivgesetz gilt: $a(1-b) = a - ab$
d) Wenn er eine 1 hat (multiplikatives neutrales Element)

Wir definieren Mengen wie:
- $\mathbb{Z}_2 = \{0, 1\}$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
- $\mathbb{Z}_M = \{0, 1, 2, ..., M-1\}$

Um die Abgeschlossenheit sicherzustellen, verwenden wir Operationen zusammen mit Modulo M. Beispiel:

$$\mathbb{Z}_5 = \{1, 2, 3, 4, 5\}$$
$$3 \cdot 4 = 12, 12 \notin \mathbb{Z}_5$$
$$12 \bmod 5 = 2, 2 \in \mathbb{Z}_5$$

Codewörter können als Elemente eines endlichen Ganzzahlkörpers betrachtet werden. In der Informatik bewegen wir uns in $\mathbb{Z}_2$. Die Anzahl der darstellbaren Codewörter wird durch die Codewortlänge bestimmt.
- Byte: 8 Bit
- Word: 16, 32, 64 Bit
- TCP-Paket: 1024 Bit

Im endlichen Ganzzahlkörper gibt es immer eine grösste und eine kleinste Zahl. Die Darstellung dieser Zahl kann durch Speicher oder Definition der Wortgrösse begrenzt werden ⟶ Keine Unendlichkeit.

Interpretation eines Codewortes

Ein Codewort 1001 kann auf verschiedene Arten interpretiert werden:
- Als Tupel (1, 0, 0, 1)
- Als Zahl $1001_2 = 9_{10}$. Es gelten die üblichen Operationen der Ganzzahlrechnung.
- Als Vektor $\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}^T$. Es gelten die üblichen Operationen der Vektorrechnung.
- Als Polynom: $g(u) = u^3 + 1$. Es gelten die üblichen Operationen der Polynomrechnung.

Die obigen Darstellungsformen sind äquivalent und beschreiben alle dasselbe Codewort. Alle Berechnungen erfolgen in $\mathbb{Z}_2$.

Interpretation eines Codewortes als Vektor

Vektorraum $\mathbb{Z}_2^3$:

$$\begin{pmatrix}1\\1\\0\end{pmatrix} + \begin{pmatrix}0\\0\\1\end{pmatrix} + \begin{pmatrix}0\\0\\1\end{pmatrix} \equiv \begin{pmatrix}1\\1\\0\end{pmatrix} \bmod 2$$

Vektoren werden in der Codierung zur Fehlererkennung und -behebung verwendet.

Interpretation als Polynom

Codewort 100101 als Polynom:

$$1u^5 + 0u^4 + 0u^3 + 1u^2 + 0u^1 + 1u^0 = u^5 + u^2 + u^0$$

Multiplikation zweier Polynome in $\mathbb{Z}_2$:

$$(u^5 + u^2 + u^0)(u^2 + u^0) \bmod 2$$
$$= (u^7 + u^5 + u^4 + 2u^2 + u^0) \bmod 2$$
$$= u^7 + u^5 + u^4 + 1$$

Das resultierende Codewort ist 1011 0001.

Zyklische Gruppe

Polynom $f(x) = x^3 + x + 1$, hat nach Fundamentalsatz der Algebra 3 Nullstellen. Die Frage ist nun, ob das Polynom in $\mathbb{Z}_2$ eine Lösung hat.

Eine zyklische Gruppe (gemäss Évariste Galois (1811 - 1832)):
- Wird von einem einzigen Element erzeugt
- Besteht nur aus Potenzen des Erzeugers

- Das erzeugende Element a wird als Lösung eingesetzt: $f(a) = a^3 + a + 1$

$a = a$

$a^2 = a^2$

$a^3 = a + 1$ Umstellung $f(a)$ in $\mathbb{Z}_2$

$a^4 = a(a + 1) = a^2 + a$

$a^5 = a(a^2 + a) = a^3 + a^2 = a^2 + a + 1$

$a^6 = a(a^2 + a + 1) = a^2 + 2a + 1 = a^2 + 1$

$a^7 = a(a^2 + 1) = 1$

$a^8 = a$ Zyklus beginnt von vorne