

Chomsky-Grammatik zur Ausführung der modulo-Operation

Modulo

- „Division mit Rest“
- $a \bmod b = r$
- $a = b * c + r$
- $r = a - (b * c)$

Chomsky-Grammatik

- $G = (V, \Sigma, P, S)$ mit
- $V = \{S, S_1, S_2, L, R, A, B, C, D, E, F, G, H, I, X\}$
- $\Sigma = \{a, L, R\}$

Ersetzungsregeln

- $P = \{$
 - $S \rightarrow LS_1KDXES_2R$
 - $S_1 \rightarrow A\dots A$ (Dividend)
 - $S_2 \rightarrow B\dots B$ (Divisor)
 - $BC \rightarrow CB$
 - $AC \rightarrow D$
 - $ADC \rightarrow D$
 - $ADB \rightarrow KADXBE$
 - $AK \rightarrow KA$
 - $EB \rightarrow BE$
 - $LK \rightarrow LF$
 - $ER \rightarrow GR$
 - $FA \rightarrow AF$
 - $BG \rightarrow GB$
 - $FDXG \rightarrow \varepsilon$
 - $AB \rightarrow \varepsilon$
 - $LD \rightarrow LH$
 - $H \rightarrow \varepsilon$
 - $FDX \rightarrow DXF$
 - $DXG \rightarrow GDX$
 - $FGB \rightarrow H$
 - $HB \rightarrow H$
 - $DXH \rightarrow H$
 - $AH \rightarrow A$
 - $A \rightarrow a$
 - $AFG \rightarrow AI$
 - $IA \rightarrow AI$
 - $IB \rightarrow CB$
 - $IR \rightarrow R$
 - $IDXB \rightarrow DIBX$
 - $IB \rightarrow CB$
 - $XB \rightarrow CBX$
 - $XR \rightarrow R$
 - $La..aR \rightarrow |a| \in \mathbb{N}$
 - $LR \rightarrow 0 \}$

Idee

Iterativ: Prüfen, ob mehr As oder Bs

- Mehr A: A zählen
- Mehr B: Subtraktion; von vorne
- Gleiche Anzahl: Auflösen

Beispiel: $5 \bmod 2 = 1$

S \rightarrow LS₁KDXES₂R \rightarrow LAAAAAKDXEBBR \rightarrow LAAAAKADXBEBR
 \rightarrow LAAAKAADXBBER \rightarrow LAAKAAADXBBGR \rightarrow
LAKAAAADXBGGBR \rightarrow LKAAAADXGBBR \rightarrow
LFAAAAAGDXBBR \rightarrow ... \rightarrow LAAAAAFGDXXBBR \rightarrow
LAAAAAIDXBBR \rightarrow LAAAAADIBXBR \rightarrow LAAAAADCBCBXR \rightarrow
LAAAADCBBR \rightarrow LAAADBBER \rightarrow LAAKADXBEBR \rightarrow
LAKAADXBBER \rightarrow LKAAADXBBGR \rightarrow LFAAADXBGGBR \rightarrow
LFAAADXGBBR \rightarrow LAAFAGDXBBR \rightarrow LAAFAGDXBBR \rightarrow
LAAAIDXBBR \rightarrow LAAADIBXBR \rightarrow LAAADCBCBXR \rightarrow
LAAADCBBR \rightarrow LADBBER \rightarrow LKADXBEBR \rightarrow LFADXBBER \rightarrow
LAFDXBBGR \rightarrow LADXFBGGBR \rightarrow LADXFGBBR \rightarrow LADXHBR \rightarrow
LADXHR \rightarrow LAHR \rightarrow LAR \rightarrow LaR \rightarrow 1

Beispiel: $3 \bmod 3 = 0$

LAAKDXEBBRR → LAAKADXBEBRR →
LAKAADXBBER → LKAAADXBBBER →
LFAAADXBBBGR → LFAADXBBGRR →
LAAFADXGBBRR → LAAFDXGBBRR →
LAAABBBR → LAABBR → LABR → LR → 0

Komplexität

- Worterzeugung: 3 Regelanwendungen, 2 Zeitschritte

$S \rightarrow LSKDXESR \rightarrow LA..AKDXESR \rightarrow LA..AKDXEB..BR$

- Prüfen: $1 + 2|A| + 2|B|$ Anwendungen, $2 * \max(|A|, |B|)$ Zeitschritte

Komplexität

- Alternativen:
 - Mehr As als Bs:
Substraktion:
 $2 + |B| + |A| + |B-1| + |B-2| + \dots$ Anwendungen, $2 + |B|$ Zeitschritte
 - Gleich viele As wie Bs:
 $1 + |B| + |A|$ Anwendungen, $1 + |B| + |A|$ Zeitschritte
 - Mehr Bs als As:
„Löschen“ der Bs und Zwischenvariablen, Umwandeln der As in Terminale, Auswertung:
 $4 + |B| + |A|$ Anwendungen, $4 + |B| + |A|$ Zeitschritte

Komplexität

- Insgesamt:

- „Division mit Rest“
- $a \bmod b = r$
- $a = b * c + r$
- $r = a - (b * c)$

Komplexität

- Insgesamt:

- Regelanwendungen:

- $3 + (c + 1) * \text{Prüfen} + c * \text{Subtraktion} + \text{Auflösen der Differenz}$

=

- $3 + (c + 1) * (1 + 2|A| + 2|B|) + c * (2 + |B| + |A| + |B-1| + |B-2| + \dots)$ + [1 ODER 4] + |B| + |A|

=

[5 ODER 8] + 3c + 4|A| + 3|B| + 2c|A| + 3c|B| + c(|B-1| + |B-2| + ..)

Komplexität

- Insgesamt:
 - Zeitschritte:
 - $3 + 2(c+1) * \max(|A|, |B|) + c*(2 + |B|) + [1 \text{ ODER } 4]$
 $+ |B| + |A|$
~
 $O(|A| + |B|)$