Formele afleidingen van binaire aritmetiek

door
A.H.J. Mathijssen

18 september 2003

Inleiding

Rekenkundige basisoperaties: optellen, aftrekken, vermenigvuldigen en delen

Probleem: geen of onvolledige correctheidsbewijzen voor implementaties van de rekenkundige basisoperaties

Doel: constructie combinatorische circuits voor de basisoperaties op gehele getallen, voorzien van correctheidsbewijzen

In deze presentatie alleen deling

Werkwijze

Onderscheid tussen 3 niveau's:

1	rekenkundig	:	gehele getallen
2	representatie	:	lijsten van bits
3	implementatie	:	combinatorische circuits

Resultaten van hogere niveau's worden gebruikt op lagere niveau's.

Functionele programmeertaal

Calculationele stijl van programmeren

Lijsten

Voor element b en lijst s:

- $\#s$ is de lengte van s
- $s \cdot i$ is element i van s, met $0 \leq i < \#s$
- [] is de lege lijst
- $b \triangleright s$ is de lijst met b als kop en s als staart
- $s \triangleleft b$ is de lijst met s als kop*lijst* en b als staart-*element*
- $[b]$ is de afkorting voor $b \triangleright [] \text{ en } [] \triangleleft b$

Representatie natuurlijke getallen

Definitie $v2$, voor binaire lijst s met lengte n:

$$v2 \cdot s = (\sum i : 0 \leq i < n : s \cdot i * 2^{n-1-i})$$

Recursieve definitie $v2$, voor bit b en binaire lijst s:

$$\begin{array}{ll} v2 \cdot [\,] & = 0 \\ v2 \cdot (s \triangleleft b) & = 2 * v2 \cdot s + b \end{array}$$

Representatie gehele getallen 1

Standaardrepresentaties:

- sign-and-magnitude
- one's complement
- **two's complement**

Definitie $vn2$, voor niet-lege binaire lijst s met lengte n:

$$vn2 \cdot s = -s \cdot 0 * 2^{n-1} + (\sum i : 1 \leq i < n : s \cdot i * 2^{n-1-i})$$

Recursieve definitie $vn2$, voor bit b en niet-lege binaire lijst s:

$$\begin{array}{ll} vn2 \cdot [\, b\,] & = -b \\ vn2 \cdot (s \triangleleft b) & = 2 * v2 \cdot s + b \end{array}$$

Eigenschap $vn2$, voor niet-lege binaire lijst s:

$$\begin{array}{l} vn2 \cdot s < 0 \equiv s \cdot 0 = 1 \\ 0 \leq vn2 \cdot s \equiv s \cdot 0 = 0 \end{array}$$

Bereik $vn2$, voor niet-lege binaire lijst s met lengte n:

$$vn2 \cdot s \in [-2^{n-1}, 2^{n-1} - 1]$$

Representatie gehele getallen 2

Signed one's representatie

Recursieve definitie $v2s1$, voor bit b en binaire lijst t:

$$\begin{aligned} v2s1 \cdot [\,] &= 0 \\ v2s1 \cdot (t \triangleleft b) &= 2 * (v2s1 \cdot t + b) - 1 \end{aligned}$$

Signed one's gerepresenteerde getallen zijn oneven of 0.

Integer deling 1

Positieve constante B is de noemer.

Specificatie dm, voor integer x:

$$dm{\cdot}x \;=\; \langle\, q, r \,\rangle$$
$$\textbf{whr } q, r\text{: } x = q * B + r \;\wedge\; 0 \leq r < B \textbf{ end}$$

Declaratie dm, voor bit b en integer x:

$$\begin{array}{lll} dm{\cdot}0 & = & \langle\, 0, 0 \,\rangle \\ dm{\cdot}(-1) & = & \langle\, -1, B-1 \,\rangle \\ dm{\cdot}(2*x+b) & = & \textbf{if } m < 0 \;\rightarrow\; \langle\, 2*h, l \,\rangle \\ & & [\!]\; 0 \leq m \;\rightarrow\; \langle\, 2*h+1, m \,\rangle \\ & & \textbf{fi } \textbf{whr } \langle\, h, k \,\rangle = dm{\cdot}x \;\&\; \\ & & l = 2*k+b \;\&\; m = l - B \textbf{ end} \end{array}$$

Bekend als restoring division.

Integer deling 2

Specificatie dm en gdm, voor integer x:

$$
\begin{array}{l}
dm{\cdot}x \;=\; \langle\, q\,,r\,\rangle \\
\;\mathbf{whr}\; q,r\colon\; x = q * B + r \;\wedge\; 0 \le r < B \;\mathbf{end} \\
gdm{\cdot}x \;=\; \langle\, q\,,r\,\rangle \\
\;\mathbf{whr}\; q,r\colon\; x = q * B + r \;\wedge\; -B \le r < B \;\mathbf{end}
\end{array}
$$

Alternatieve declaratie dm, voor bit b en integer x:

$$
\begin{array}{lll}
dm{\cdot}x \;=\; \mathbf{if} & r < 0 \;\rightarrow\; \langle\, q-1\,, r+B\,\rangle \\
\quad [\!] & 0 \le r \;\rightarrow\; \langle\, q\,,r\,\rangle \\
\quad \mathbf{fi} & \mathbf{whr}\; \langle\, q\,,r\,\rangle = gdm{\cdot}x \;\mathbf{end}
\end{array}
$$

Declaratie gdm, voor bit b en integer x:

$$
\begin{array}{lll}
gdm{\cdot}(-b) & = & \langle\, 0\,, -b\,\rangle \\
gdm{\cdot}(2*x+b) & = & \mathbf{if}\; l < 0 \;\rightarrow\; \langle\, 2*h-1\,, l+B\,\rangle \\
 & & [\!]\; 0 \le l \;\rightarrow\; \langle\, 2*h+1\,, l-B\,\rangle \\
 & & \mathbf{fi}\; \mathbf{whr}\; \langle\, h\,,k\,\rangle = gdm{\cdot}x \\
 & & \&\; l = 2*k+b \;\mathbf{end}
\end{array}
$$

Quotient is oneven of 0.

Bekend als non-restoring division.

Binaire deling 1

Constante $B2$ is een niet-lege binaire lijst, met:

$$vn2 \cdot B2 = B$$

Specificatie $dm2$, voor niet-lege binaire lijst s:

$$dm2 \cdot s = \langle\, t, u \,\rangle$$
$$\textbf{whr } t, u\text{: } \langle\, vn2 \cdot t, vn2 \cdot u \,\rangle = dm \cdot (vn2 \cdot s) \textbf{ end}$$

Restoring versie declaratie $dm2$, voor bit b en niet-lege binaire lijst s:

$$\begin{aligned}
dm2 \cdot [\,0\,] &= \langle\, [\,0\,], [\,0\,] \,\rangle \\
dm2 \cdot [\,1\,] &= \langle\, [\,1\,], dec \cdot 1 \cdot B2 \,\rangle \\
dm2 \cdot (s \lhd b) &= \textbf{if } w \cdot 0 = 1 \rightarrow \langle\, t \lhd 0, v \,\rangle \\
&\quad [] \;\; w \cdot 0 = 0 \rightarrow \langle\, t \lhd 1, w \,\rangle \\
&\quad \textbf{fi } \textbf{whr } \langle\, t, u \,\rangle = dm2 \cdot s \;\&\; v = u \lhd b \\
&\quad \;\&\; w = subt2 \cdot v \cdot B2 \textbf{ end}
\end{aligned}$$

Hardware implementaties

Richtlijnen:

- minimaliseer gevalsonderscheid
- maximaliseer hergebruik van expressies

Definitie sel, voor bit b en binaire lijsten s, t:

$$sel \cdot b \cdot s \cdot t = \textbf{if } b = 0 \to s \ [] \ b = 1 \to t \textbf{ fi}$$

Implementatie als multiplexer

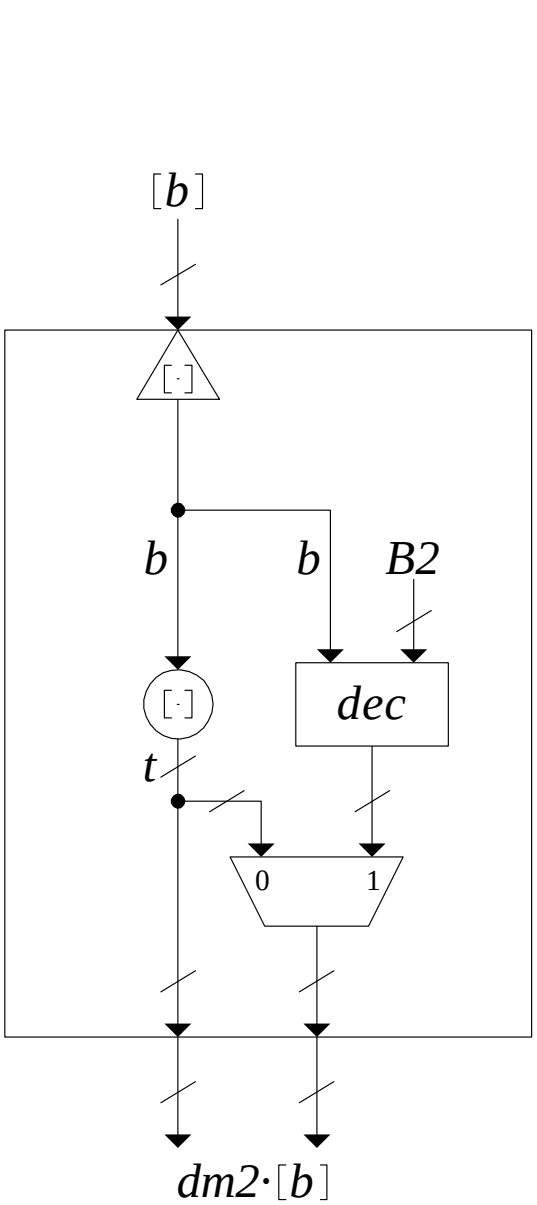
Binaire deling 2

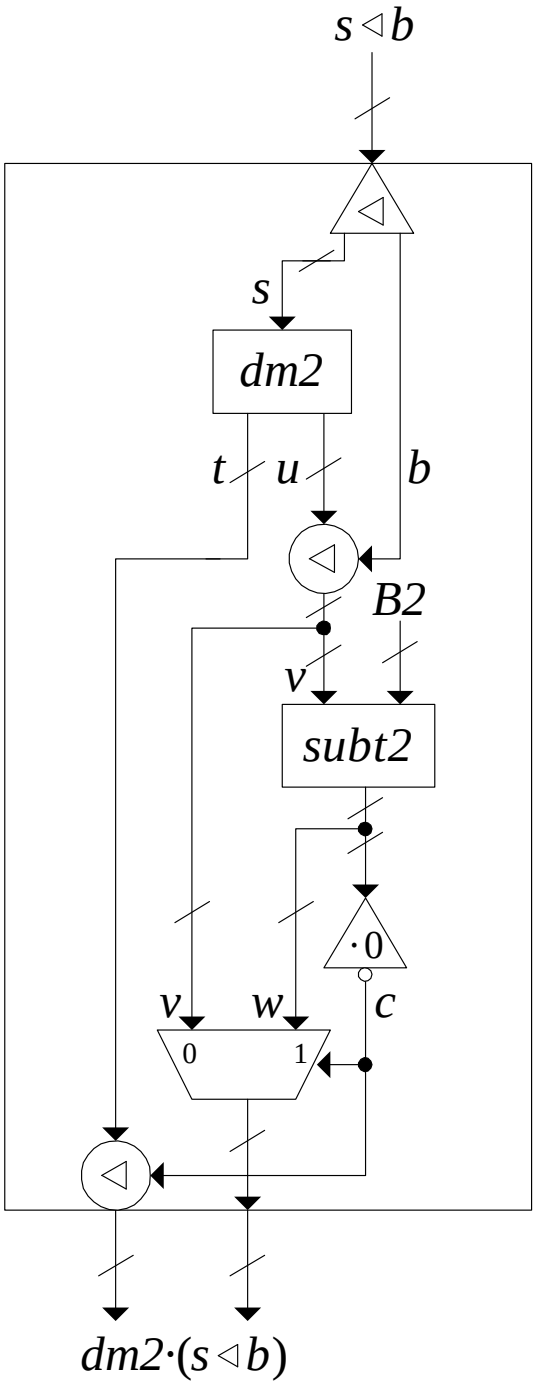
Uitwerking restoring versie declaratie $dm2$ voor hardware implementatie, voor bit b en niet-lege binaire lijst s:

$$\begin{aligned} dm2 \cdot [\,b\,] &= \langle\, t, sel \cdot b \cdot t \cdot (dec \cdot b \cdot B2) \,\rangle \\ &\quad \textbf{whr } t = [\,b\,] \textbf{ end} \\ dm2 \cdot (s \triangleleft b) &= \langle\, t \triangleleft c, sel \cdot c \cdot v \cdot w \,\rangle \\ &\quad \textbf{whr } \langle\, t, u \,\rangle = dm2 \cdot s \ \&\ v = u \triangleleft b \ \& \\ &\quad w = subt2 \cdot v \cdot B2 \ \&\ c = 1 - w \cdot 0 \textbf{ end} \end{aligned}$$

Hardware implementaties deling 1

Implementatie restoring versie declaratie $dm2$:





Binaire deling 3

Specificatie $dm2$ en $gdm2$, voor niet-lege binaire lijst s:

$$
\begin{array}{l}
dm2 \cdot s \;\; = \langle\, t, u \,\rangle \\
\;\; \mathbf{whr}\; t, u\colon \langle\, vn2 \cdot t, vn2 \cdot u \,\rangle = dm \cdot (vn2 \cdot s)\; \mathbf{end} \\
gdm2 \cdot s \;=\; \langle\, t, u \,\rangle \\
\;\; \mathbf{whr}\; t, u\colon \langle\, v2s1 \cdot t, vn2 \cdot u \,\rangle = gdm \cdot (vn2 \cdot s)\; \mathbf{end}
\end{array}
$$

Specificatie $ds1to2$, voor bit c en binaire lijst t:

$$vn2 \cdot (ds1to2 \cdot c \cdot t) = v2s1 \cdot t - c$$

Declaratie $ds1to2$, voor bits b, c en binaire lijst t:

$$
\begin{array}{lcl}
ds1to2 \cdot c \cdot [\,] & = & [\,c\,] \\
ds1to2 \cdot c \cdot (b \triangleright t) & = & (1 - b) \triangleright t \triangleleft (1 - c)
\end{array}
$$

Non-restoring versie declaratie $dm2$, voor niet-lege binaire lijst s:

$$
\begin{array}{lll}
dm2 \cdot s = & \mathbf{if} & u \cdot 0 = 1 \;\rightarrow\; \langle\, ds1to2 \cdot 1 \cdot t, add2 \cdot u \cdot B2 \,\rangle \\
& [\!] & u \cdot 0 = 0 \;\rightarrow\; \langle\, ds1to2 \cdot 0 \cdot t, u \,\rangle \\
& \mathbf{fi}\;\; \mathbf{whr}\; \langle\, t, u \,\rangle = gdm2 \cdot s\; \mathbf{end}
\end{array}
$$

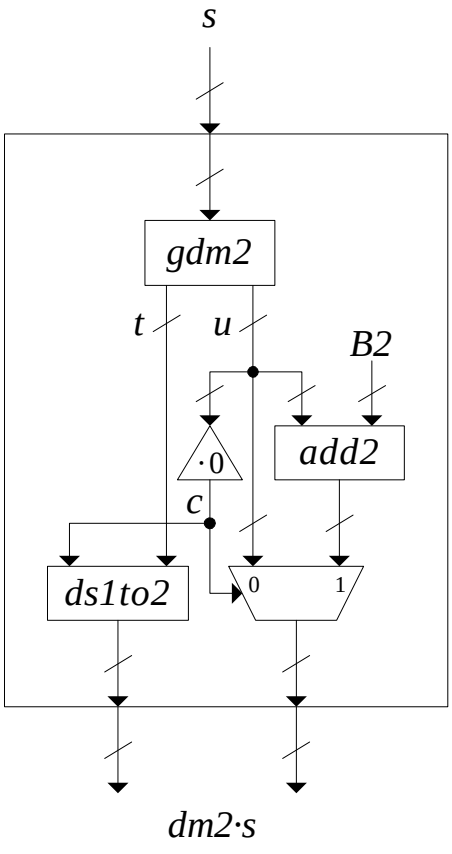
Binaire deling 4

Uitwerking non-restoring versie declaratie $dm2$ voor hardware implementatie, voor niet-lege binaire lijst s:

$$dm2 \cdot s \;=\; \langle\, ds1to2 \cdot c \cdot t \,,\, sel \cdot c \cdot u \cdot (add2 \cdot u \cdot B2) \,\rangle$$
$$\mathbf{whr}\ \langle\, t, u \,\rangle = gdm2 \cdot s\ \&\ c = u \cdot 0\ \mathbf{end}$$

Hardware implementaties deling 2

Implementatie non-restoring versie declaratie $dm2$:



Binaire deling 5

Specificatie $gdm2$, voor niet-lege binaire lijst s:

$$gdm2 \cdot s \;=\; \langle\, t, u \,\rangle \;\; \mathbf{whr}\; t, u\colon \langle\, v2s1 \cdot t, vn2 \cdot u \,\rangle = gdm \cdot (vn2 \cdot s)\; \mathbf{end}$$

Declaratie $gdm2$, voor bit b en niet-lege binaire lijst s:

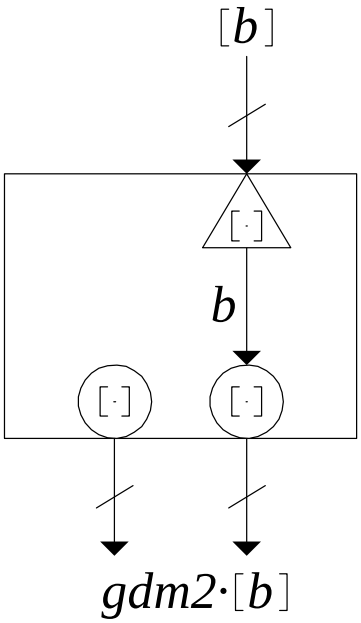
$$\begin{array}{lll} gdm2 \cdot [\, b \,] & = & \langle\, [\,], [\, b \,] \,\rangle \\ gdm2 \cdot (s \triangleleft b) & = & \mathbf{if}\;\; v \cdot 0 = 1 \;\rightarrow\; \langle\, t \triangleleft 0, add2 \cdot v \cdot B2 \,\rangle \\ & & [\!]\;\; v \cdot 0 = 0 \;\rightarrow\; \langle\, t \triangleleft 1, subt2 \cdot v \cdot B2 \,\rangle \\ & & \mathbf{fi}\;\; \mathbf{whr}\; \langle\, t, u \,\rangle = gdm2 \cdot s \;\&\; \\ & & v = u \triangleleft b\; \mathbf{end} \end{array}$$

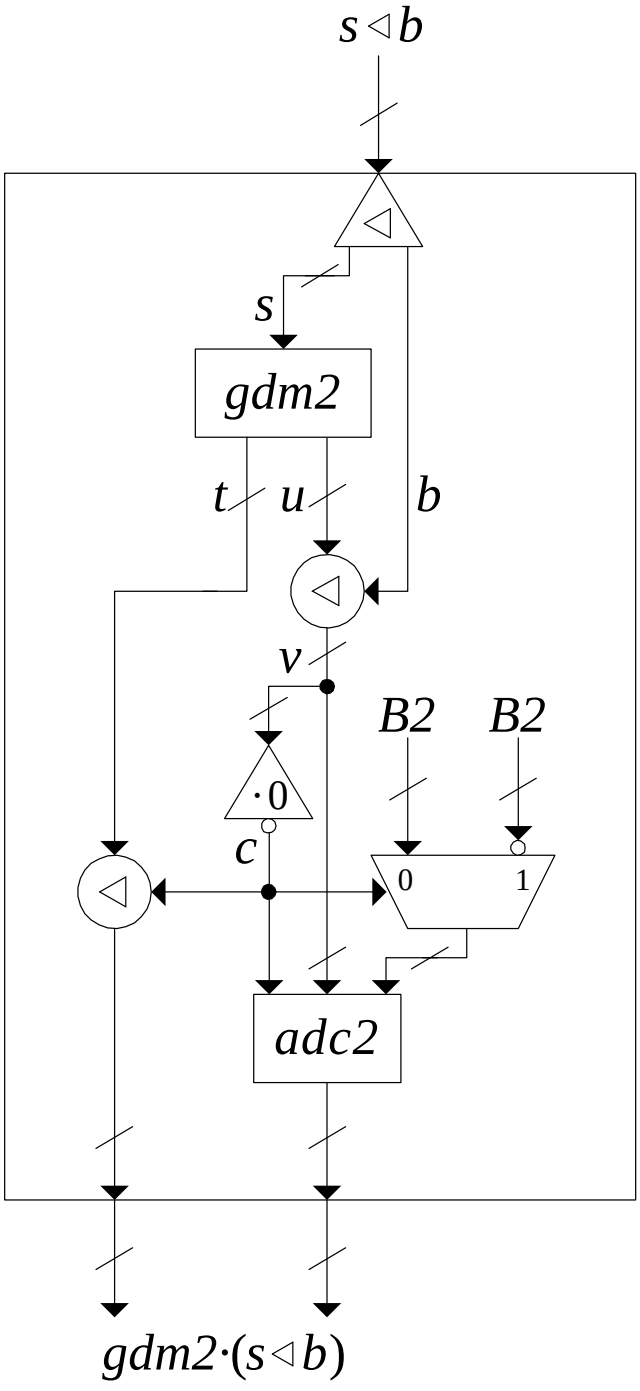
Uitwerking declaratie $gdm2$ voor hardware implementatie, voor bit b en niet-lege binaire lijst s:

$$\begin{array}{lll} gdm2 \cdot [\, b \,] & = & \langle\, [\,], [\, b \,] \,\rangle \\ gdm2 \cdot (s \triangleleft b) & = & \langle\, t \triangleleft c, adc2 \cdot c \cdot v \cdot (sel \cdot c \cdot B2 \cdot (cmpl \cdot B2)) \,\rangle \\ & & \mathbf{whr}\; \langle\, t, u \,\rangle = gdm2 \cdot s \;\&\; v = u \triangleleft b \;\& \\ & & c = 1 - v \cdot 0\; \mathbf{end} \end{array}$$

Hardware implementaties deling 3

Implementatie declaratie $gdm2$:





Conclusies en aanbevelingen

Gebruikte techniek:

- separation of concerns
- gebruik essentiële eigenschappen lagere niveau's op hogere niveau's

Uitbreidingen:

- meer complexe operaties
- andere integer representaties
- floating point getallen
- sequentiële circuits
- software implementaties