Integer Division by Multiplication

Borderite • 18 Aug 2026

Integer Division by Multiplication

Borderite

August 18, 2026

The integer division instruction of an computer is typically ten to thirty times slower than the multiplication instruction, due to its complexity. If a divisor is execution-invariant, however, there is a way to replace the integer division operation with an integer multiplication and division by some power of two, the latter of which can be performed by using a bitwise right shift operation. We investigate this approach in this note. Many of the materials discussed in this note are found in (Granlund and Montgomery 1994) and (Henry S. Warren 2013), but some mathematical results and derivations in this note are original.

Introduction

We consider three kinds of divisions in this note: the one that rounds down the fractional part of the result, the one that rounds up the fractional part, and one that rounds the fractional part towards zero. Given a execution-invariant divisor $d \in \mathbb{Z}\backslash\{0\}$, define $q : \mathbb{Z} \to \mathbb{Z}$, $\bar{q} : \mathbb{Z} \to \mathbb{Z}$, and $q^0 : \mathbb{Z} \to \mathbb{Z}$ by

$$q(n) \equiv \lfloor n/d \rfloor,$$

$$\bar{q}(n) \equiv \lceil n/d \rceil,$$

and

$$q^0(n) \equiv \begin{cases} q(n) & \text{if } n \geq 0, \\ \bar{q}(n) & \text{otherwise.} \end{cases}$$

Let W be the bit width of integers we consider, which is basically the maximum size of dividends with which we perform division by d. We assume that $W \geq 3$. Define $\mathcal{N}_W \equiv \{z \in \mathbb{N} : \ z \leq 2^W - 1\}$. A type of division we consider is division whose dividend and divisor both belong to $\mathcal{N}_W$. We call such division *unsigned division*. The unsigned division may round down and round up the fractional part of the result.

Another type of division involves integers in $\mathcal{Z}_W \equiv \{z \in \mathbb{Z} : -2^{W-1} \le z \le 2^{W-1} - 1\}$. We call this type of division *signed division*. In signed division of $n \in \mathcal{Z}_W$ by $d \in \mathcal{Z}_W \backslash \{0\}$, the fractional part of the result can be rounded down (Euclidean division), rounded up, or rounded towards zero.

Just for a moment, suppose that we need to divide a real number x by another real number $y \neq 0$, where y is execution invariant. Then we can use the fact that

$$\frac{x}{y} = x \cdot \frac{1}{y},$$

to replace the division by multiplication of x by $z \equiv 1/y$, where z can be calculated beforehand and written into the code.

In the integer division with a dividend d, we can try something similar, but limit our operations to integer multiplications and bitwise right shifts (and some additions and subtractions when needed). The basic idea is that we can choose an integer m and a nonnegative integer p to let $m/2^p$ approximate $1/d$, so that

$$\frac{n}{d} \approx \frac{nm}{2^p},$$

for every n in the relevant range of integers. If the approximation is valid in an appropriate sense, the right-hand side can be calculated by multiplication of n by m and bitwise right shift of the product by p positions.

Division by a Power of Two

Bitwise shift operations

This section considers how to perform the division of integers by a power of two through bitwise shift operations. We assume that the CPU provides logical and arithmetic bitwise right shift instructions. Let b_0, …, b_{W-1} be functions from $\mathcal{N}_W$ to $\{0, 1\}$ such that for each $x \in \mathcal{N}_W$

$$x = \sum_{i=0}^{W-1} b_i(x) \cdot 2^i.$$

That is, $b_i(x)$ is the ith bit in the binary representation of x. Using the binary expansion, we can respectively define the logical and arithmetic bitwise right shift functions, $\mathtt{SHR}_W : \mathcal{N}_W \to \mathcal{N}_W$ and $\mathtt{SAR}_W : \mathcal{N}_W \to \mathcal{N}_W$, by

$$\texttt{SHR}_W(x,k) \equiv \sum_{i=0}^{W-1-k} b_{i+k}(x)\cdot 2^i$$

and

$$\texttt{SAR}_W(x,k) \equiv b_{W-1}(x)(2^W - 2^k) + \texttt{SHR}_W(x,k).$$

When x is the encoded signed integer in two's complement, $b_{W-1}(x)$ is the sign bit of x. The term $b_{W-1}(x)(2^W - 2^k)$ fills the kth through $(W-1)$st bit positions with the sign bit. When $x \geq 0$, it holds that $\texttt{SAR}_W(x,k) = \texttt{SHR}_W(x,k)$, because $b_{W-1}(x)$ is zero.

Unsigned division

Suppose that we want to divide integers in $\mathcal{N}_W$ by $d \equiv 2^k$, where $k \in \{0,1,\ldots,W-1\}$. Pick $n \in \mathcal{N}_W$ arbitrarily. Then the binary expansion of n is given by

$$n = \sum_{i=0}^{W-1} b_i(n)\cdot 2^i,$$

where each among $b_0(n)$, $b_1(n)$, …, $b_{W-1}(n)$ is zero or one. Division of n by d yields that

$$\frac{n}{d} = \sum_{i=0}^{W-1} b_i(n)\cdot 2^{i-k} = \sum_{i=0}^{W-1-k} b_{i+k}(n)\cdot 2^i + \sum_{j=1}^{k} b_{k-j}(n)\cdot 2^{-j}$$

On the right-hand side of this equality, the first term is an integer, while the second term resides between 0 and $\sum_{j=1}^{k} 2^{-j} = 1 - 1/2^k < 1$, so that

$$q(n) = \left\lfloor \frac{n}{d} \right\rfloor = \sum_{i=0}^{W-1-k} b_{i+k}(n)\cdot 2^i = \texttt{SHR}_W(n,k).$$

For computation of $\bar{q}(n)$, we can use the fact that for each $n \in \mathcal{N}_W$,

$$\bar{q}(n) = \left\lceil \frac{n}{d} \right\rceil = \begin{cases} \left\lfloor \dfrac{n+d-1}{d} \right\rfloor = \left\lfloor \dfrac{n-1}{d} \right\rfloor + 1 = q(n-1)+1 & \text{if } n \geq 1, \\ 0 & \text{otherwise} \end{cases},$$

which can be compactly rewritten as

$$\bar{q}(n) = q(n - 1_{n>0}) + 1_{n>0} \text{ for each } n \in \mathcal{N}_W.$$

It follows that

$$\bar{q}(n) = \texttt{SHR}_W(n - 1_{n>0}, k) + 1_{n>0} \text{ for each } n \in \mathcal{N}_W.$$

Signed division

We now consider division of integers in $\mathcal{Z}_W$ by $d = 2^k$ for some $k \in \{0, 1, \ldots, W-2\}$. Define $\mathtt{TCE}_W : \mathcal{Z}_W \to \mathcal{N}_W$ and $\mathtt{TCD}_W : \mathcal{N}_W \to \mathcal{Z}_W$ by

$$\mathtt{TCE}_W(z) \equiv \begin{cases} z & \text{if } z \geq 0 \\ 2^W + z & \text{otherwise} \end{cases}$$

and

$$\mathtt{TCD}_W(y) \equiv \begin{cases} y & \text{if } z \leq 2^{W-1} - 1 \\ y - 2^W & \text{otherwise,} \end{cases}$$

respectively. The function $\mathtt{TCE}_W$ encodes the given integer $z \in \mathcal{Z}_W$ in two's complement, and the function $\mathtt{TCD}_W$ decodes the encoded integer, i.e., $\mathtt{TCD}_W(\mathtt{TCE}_W(z)) = z$. Applying of $\mathtt{TCE}_W$ to a given integer $n \in \mathcal{Z}_W$ and then applying $\mathtt{SAR}_W$ for k position shifts yields that

$$\mathtt{SAR}_W(\mathtt{TCE}_W(n), k) = 1_{n<0}(2^W - 2^{W-k}) + \mathtt{SHR}_W(\mathtt{TCE}_W(n), k).$$

When $n \geq 0$, it holds that $\mathtt{TCE}_W(n) = n$ so that

$$\mathtt{SAR}_W(\mathtt{TCE}_W(n), k) = \mathtt{SAR}_W(n, k) = \mathtt{SHR}_W(n, k) = \left\lfloor \frac{n}{d} \right\rfloor.$$

It follows that

$$\mathtt{TCD}_W(\mathtt{SAR}_W(\mathtt{TCE}_W(n), k)) = \left\lfloor \frac{n}{d} \right\rfloor.$$

When $n < 0$, it holds that $\mathtt{TCE}_W(n) = 2^W + n$. It follows that

$$\mathtt{SHR}_W(\mathtt{TCE}_W(n), k) = \mathtt{SHR}_W(2^W + n, k) = \left\lfloor \frac{2^W + n}{d} \right\rfloor$$
$$= \left\lfloor 2^{W-k} + \frac{n}{d} \right\rfloor = 2^{W-k} + \left\lfloor \frac{n}{d} \right\rfloor$$

Because $1_{n<0} = 1$, it follows that

$$\mathtt{SAR}_W(\mathtt{TCE}_W(n), k) = (2^W - 2^{W-k}) + 2^{W-k} + \left\lfloor \frac{n}{d} \right\rfloor = 2^W + \left\lfloor \frac{n}{d} \right\rfloor.$$

Since $2^{W-1} \leq 2^W + \lfloor n/d \rfloor \leq 2^W - 1$, it further follows that

$$\mathtt{TCD}_W(\mathtt{SAR}_W(\mathtt{TCE}_W(n), k)) = 2^W + \left\lfloor \frac{n}{d} \right\rfloor - 2^W = \left\lfloor \frac{n}{d} \right\rfloor$$

Thus, we have verified that for any $n \in \mathcal{Z}_W$,

$$\mathtt{TCD}_W(\mathtt{SAR}_W(\mathtt{TCE}_W(n), k)) = \left\lfloor \frac{n}{d} \right\rfloor = q(n).$$

The arithmetic bitwise right shift can be used in downward division of signed integers by a power of two.

For computation of $\bar{q}(n)$, we use the fact that for each $n \in \mathcal{Z}_W \backslash \{-2^{W-1}\}$,

$$\bar{q}(n) = \left\lceil \frac{n}{d} \right\rceil = \left\lfloor \frac{n+d-1}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1,$$

while $\bar{q}(-2^{W-1}) = -2^{W-1-k}$. It follows that for each $n \in \mathcal{Z}_W$,

$$\begin{aligned}\bar{q}(n) &= \left\lfloor \frac{n - 1_{n \geq -2^{W-1}+1}}{d} \right\rfloor + 1_{n \geq -2^{W-1}+1} \\ &= q(n - 1_{n \geq -2^{W-1}+1}) + 1_{n \geq -2^{W-1}+1},\end{aligned}$$

Because $\texttt{TCD}_W(-2^{w-1}) = 2^{W-1}$, $1_{n \geq -2^{W-1}+1}$ can be conveniently evaluated by

$$1_{n \geq -2^{W-1}+1} = 1_{\texttt{TCD}_W(n) \neq 2^{W-1}} = 1_{\texttt{TCD}_W(n) \wedge 2^{W-1} \neq 0}$$

The value of $q(n - 1_{n \geq -2^{W-1}+1})$ then can be computed by using the arithmetic bitwise right shift as we have seen.

The division rounding towards zero can be performed by combining the downward and upward rounding divisions:

$$q^0(n) \equiv \begin{cases} q(n) & \text{if } n \geq 0 \\ \bar{q}(n) & \text{otherwise.} \end{cases}$$

This formula can be compactly rewritten as

$$q^0(n) = q(n - 1_{-2^{W-1}+1 \leq n \leq -1}) + 1_{-2^{W-1}+1 \leq n \leq -1}.$$

Finally, when we want to divide integers in $\mathcal{Z}_W$ by -2^k for some $\{1, 2, \ldots, W-2\}$, we first perform division by 2^k and then flip the sign of the result. In the division stage, we need to use the opposite rounding mode unless the desired mode is rounding towards zero.

Unsigned Division by a Number That Is Not a Power of Two

In this section, we mainly consider the downward-rounding version of unsigned division and then also cover the upward-round version at the end. Let N be a fixed natural number, and define

$$\mathbb{X}_N \equiv \{n \in \mathbb{Z} : \ 0 \leq n \leq N-1\}$$

Our goal is to investigate how to pick $p \in \mathbb{N}_0 \equiv \mathbb{N} \cup \{0\}$ and $m \in \mathbb{N}$ to ensure that

$$\left\lfloor \frac{nm}{2^p} \right\rfloor = q(n) \text{ for every } n \in \mathbb{X}_N, \tag{1}$$

if the equality is possible at all. We later apply the obtained results to the case where $N = 2^W$ (i.e., $\mathbb{X}_N = \mathcal{N}_W$). The divisor $d \neq 0$ belongs to $\mathbb{X}_N$, and it is treated as a constant throughout this section. .

Valid choice of p and m

Define $E : \mathbb{Z} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R}$ by

$$E(n, p, m) \equiv \frac{nm}{2^p} - q(n)$$

Then (1) holds if and only if

$$0 \leq E(n, m, p) < 1 \text{ for every } n \in \mathbb{X}_N. \tag{2}$$

The condition (2) can be rewritten as

$$q(n) \leq \frac{m}{2^p} \cdot n < q(n) + 1 \text{ for each } n \in \mathbb{X}_N. \tag{3}$$

We can interpret this condition using an analogy.

In the analogy, n represents a date, ranging from zero to $N - 1$. For convenience, we use a modified week system. *Monday* is any date that is a multiple of d. A *week* is the d-day period starting on a Monday. The day following a Monday is a *Tuesday*. The last day of a week is a *Sunday*.

Imagine that a household receives one dollar every Monday starting date zero. Then $q(n) = \lfloor n/d \rfloor$ is the total payment received by the household by the week immediately prior to the week of date n. Thus, the total payment received by date n is $q(n) + 1$. Also, imagine that the household spends $m/2^p$ dollars every day *from date one* to date $N - 1$ but spends no money on date zero. Then the total spending by date n is $(m/2^p)n$. Thus, we can interpret (3) as the requirements for the daily spending $m/2^p$.

The first inequality in (3) requires that the household's total spending up to each date be no less than the payments accumulated over the previous weeks. Note that the accumulated payments does not change during the week, while the total spending increases every day. Thus, this requirement is equivalent to that the spending accumulated up to each Monday is no less than the payments accumulated over the past weeks.

Recall that the household spends no money on the first Monday. In order for the requirement to be met on the second Monday, the total spending during the d day period between the first Tuesday and the second Monday must be no less than one dolor. It is therefore necessary that $m/2^p \geq 1/d$, or equivalently that $md/2^p \geq 1$. In each week after the second week, this pace of spending uses up one dollar received on Monday by the following Monday. Thus, it is also sufficient for the first inequality of (3) that $m/2^p \geq 1/d$. We now formally state and prove this result.

Proposition 0.1. *Let p and m be a nonnegative integer and a natural number, respectively. Then it holds that $E(n, m, p) \geq 0$ for every $n \in \mathbb{X}_N$ if and only if*

$$\frac{md}{2^p} \geq 1, \tag{4}$$

where the inequality is strict unless d is a power of two.

Proof. If $E(n, m, p) \geq 0$ for every $n \in \mathbb{X}_N$, setting $n = d$ yields that

$$E(d, p, m) = \frac{md}{2^p} - 1 \geq 0.$$

This establishes the necessity of (4). If instead (4) holds, then for each $n \in \mathbb{X}_N$

$$E(n, p, m) = \frac{md}{2^p} \cdot \frac{n}{d} - q(n) \geq \frac{n}{d} - q(n) = \frac{n}{d} - \left\lfloor \frac{n}{d} \right\rfloor \geq 0.$$

Thus, the condition (4) is sufficient.

Now suppose that $md/2^p = 1$. Then both m and d must be a power of two. Thus, the inequality in (4) is strict if the inequality holds, unless d is a power of two. □

The second inequality in (3) requires that the household's total spending up to date n is less than the payments accumulated up to the Monday in the week of the date. If the household spends $1/d$ dollars per day, the requirement is satisfied, because it receives one dollar every Monday. Recall, however, that the household spends no dollars on the first Monday. The $1/d$ dollars that were not spent on the first Monday can be used to increase the daily spending.

Define $\bar{n} \equiv N - (N \bmod d) - 1$. Then date $\bar{n}$ is the final Sunday. There are up to $d - 1$ days after date $\bar{n}$. This means that the daily spending satisfying the requirement in the first week also satisfies the requirement in the week after date $\bar{n}$ (if any). Consider spending $(1 + 1/\bar{n})/d$ dollars each day. This pace uses up the $1/d$ dollars that were not spent on date zero during the period between date one and date $\bar{n}$. Thus, the daily spending $m/2^p$ must be smaller than it, i.e., $m/2^p < (1 + 1/\bar{n})/d = ((\bar{n} + 1)/\bar{n})/d$ or equivalently, $md/2^p < (\bar{n} + 1)/\bar{n}$. The formal statement of this result and its proof follow.

Proposition 0.2. *Let p and m be a nonnegative integer and a natural number, respectively. Then it holds that $E(n, m, p) < 1$ for every $n \in \mathbb{X}_N$ if and only if*

$$\frac{md}{2^p} < \frac{\bar{n} + 1}{\bar{n}}. \tag{5}$$

Also, when (5) holds, it holds that $E(N, m, p) \leq 1$ if $N \bmod d \neq d - 1$ or $p \leq \log_2 N$.

Proof. If $E(n, p, m) < 1$ for every $n \in \mathbb{X}_N$, then it holds that $E(\bar{n}, p, m) < 1$, so that

$$\frac{\bar{n}m}{2^p} < 1 + q(\bar{n}).$$

Because $q(\bar{n}) = (\bar{n} - (d-1))/d$, we have that

$$\frac{\bar{n}m}{2^p} < 1 + \frac{\bar{n} - (d-1)}{d} = \frac{\bar{n}+1}{d}.$$

Multiplying both sides of this inequality by $d/\bar{n}$ yields (5) and establishes the necessity of (5).

Suppose instead that (5) holds. Pick $n \in \mathbb{X}_N$ arbitrarily. Then we have that

$$\frac{nm}{2^p} = \frac{md}{2^p} \cdot \frac{n}{d} < \frac{\bar{n}+1}{\bar{n}} \cdot \frac{n}{d}$$

Write $r_n \equiv n - q(n)d$. It follows from the above inequality that

$$\begin{aligned} E(n, p, m) &< \frac{\bar{n}+1}{\bar{n}} \cdot \frac{n}{d} - q(n) = \frac{\bar{n}+1}{\bar{n}} \cdot \frac{n}{d} - \frac{n - r_n}{d} \\ &= \frac{n}{\bar{n}} \cdot \frac{1}{d} + \frac{r_n}{d} \end{aligned} \tag{6}$$

If $n \le \bar{n}$, the right-hand side of this inequality is dominated by one, because

$$\frac{n}{\bar{n}} \cdot \frac{1}{d} + \frac{r_n}{d} \le 1 \cdot \frac{1}{d} + \frac{d-1}{d} = 1$$

When $n > \bar{n}$, it follows from the definition of $\bar{n}$ that $r_n \le d - 2$, $n - \bar{n} = r_n + 1$, and $\bar{n} \ge d - 1$. The right-hand side of (6) is again dominated by one, because

$$\begin{aligned} \frac{n}{\bar{n}} \cdot \frac{1}{d} + \frac{r_n}{d} &= \frac{\bar{n} + (n - \bar{n})}{\bar{n}} \cdot \frac{1}{d} + \frac{r_n}{d} = \left(r_n + 1 + \frac{n - \bar{n}}{\bar{n}}\right) \cdot \frac{1}{d} \\ &\le \left(r_n + 1 + \frac{r_n + 1}{d-1}\right) \cdot \frac{1}{d} = \frac{d \cdot (r_n+1)}{d-1} \cdot \frac{1}{d} = \frac{r_n+1}{d-1} \le \frac{d-1}{d-1} = 1. \end{aligned} \tag{7}$$

This establishes the sufficiency of (5).

Now suppose that (5) holds. If $N \bmod d \ne d - 1$, we have that $r_N \le d - 2$, so that (7) holds with $n = N$; hence, $E(N, p, m) < 1$. Suppose instead that $N \bmod d = n - 1$ and $p \le \log_2 N$. By rewriting (5), we obtain that

$$m\bar{n} < \frac{\bar{n}+1}{d} \cdot 2^p.$$

By the definition of $\bar{n}$, $(\bar{n}+1)/d$ is an integer, so that both sides of this inequality are integers. It follows that

$$m\bar{n} \le \frac{\bar{n}+1}{d} \cdot 2^p - 1$$

or equivalently,

$$m \leq \frac{2^p(\bar{n}+1)}{d\bar{n}} - \frac{1}{\bar{n}}.$$

Applying this inequality, we obtain that

$$\begin{aligned}
E(N,p,m) &= \frac{Nm}{2^p} - q(N) = \frac{Nm}{2^p} - \frac{\bar{n}+1}{d} \\
&\leq \frac{N}{2^p}\left(\frac{2^p(\bar{n}+1)}{d\bar{n}} - \frac{1}{\bar{n}}\right) - \frac{\bar{n}+1}{d} \\
&= \frac{N}{\bar{n}} \cdot \frac{\bar{n}+1}{d} - \frac{N}{2^p\bar{n}} - \frac{\bar{n}+1}{d} \\
&= \frac{N-\bar{n}}{\bar{n}} \cdot \frac{\bar{n}+1}{d} - \frac{N}{2^p\bar{n}} \\
&= \frac{d}{\bar{n}} \cdot \frac{\bar{n}+1}{d} - \frac{N}{2^p\bar{n}} = \frac{\bar{n}+1}{\bar{n}} - \frac{N}{2^p\bar{n}}.
\end{aligned}$$

Because $2^p \leq N$ by hypothesis, it follows that

$$E(N,p,m) \leq \frac{\bar{n}+1}{\bar{n}} - \frac{1}{\bar{n}} = 1.$$

□

Given Propositions 0.1 and 0.2, we can conveniently check if a given pair of $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ satisfies (1).

Proposition 0.3. *Let p and m be a nonnegative integer and a natural number, respectively. Then the condition (1) holds if and only if both (4) and (5) hold, i.e.,*

$$1 \leq \frac{md}{2^p} < \frac{\bar{n}+1}{\bar{n}}. \tag{8}$$

Whenever (8) holds, the first inequality in it is strict unless d is a power of two, while $E(N,m,p) \leq 1$ if $N \bmod d \neq d-1$ or $p \leq \log_2 N$.

Proof. The result immediately follows from Propositions 0.1 and 0.2. □

Feasibility

The condition (8) can be interpreted as giving the possible range of m to satisfy (1) given $p \in \mathbb{N}_0$, because they are equivalent to

$$\frac{2^p}{d} \leq m < \frac{\bar{n}+1}{\bar{n}} \cdot \frac{2^p}{d}. \tag{9}$$

Using this condition, we show that there exists a pair of $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ that satisfies (1).

Lemma 0.4. *It holds that $\bar{n} \geq \lfloor N/2 \rfloor$.*

Proof. If $d \leq \lfloor N/2 \rfloor$, then it holds that

$$\begin{aligned}\bar{n} &= N - (N \bmod d) - 1 \geq N - (d-1) - 1 = N - d \\ &\geq N - \lfloor N/2 \rfloor \geq \lfloor N/2 \rfloor.\end{aligned}$$

If instead $d \geq \lfloor N/2 \rfloor + 1$, then

$$\begin{aligned}\bar{n} &= N - (N \bmod d) - 1 = N - (N - d) - 1 \\ &= d - 1 \geq \lfloor N/2 \rfloor + 1 - 1 = \lfloor N/2 \rfloor.\end{aligned}$$

The result therefore follows. □

Proposition 0.5. *Write $\bar{p} \equiv \lceil \log_2(N-1) + \log_2 d \rceil$. Then there exists $m \in \mathbb{N}$ that satisfies (1) along with $p = \bar{p}$.*

Proof. By Proposition 0.3, it suffices to show that there exists $m \in \mathbb{N}$ that satisfies (8) with $p = \bar{p}$. Because

$$\begin{aligned}&\left(\frac{\bar{n}+1}{\bar{n}} \cdot \frac{2^{\bar{p}}}{d}\right) - \frac{2^{\bar{p}}}{d} = \frac{1}{\bar{n}} \cdot \frac{2^{\bar{p}}}{d} = \frac{1}{\bar{n}} \cdot \frac{2^{\lceil \log_2(N-1) + \log_2 d \rceil}}{d} \\ &\geq \frac{1}{\bar{n}} \cdot \frac{2^{\log_2(N-1) + \log_2 d}}{d} = \frac{N-1}{\bar{n}} \geq 1,\end{aligned}$$

there exists an integer m that satisfies (9), which is equivalent to (8). □

Along with Proposition 0.5, the next proposition shows that there are infinitely many pairs of $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ that satisfy (1).

Proposition 0.6. *Suppose that $(p_1, m_1) \in \mathbb{N}_0 \times \mathbb{N}$ satisfies (1) with $p = p_1$ and $m = m_1$. Write $p_2 \equiv p_1 + 1$ and $m_2 \equiv 2m_1$. Then (1) also holds with $p = p_2$ and $m = m_2$.*

Proof. By the equivalence between (1) and (8) established by Proposition 0.3, it suffices to show that (8) holds with $p = p_2$ and $m = m_2$ if it holds with $p = p_1$ and $m = m_1$. This is indeed the case, because

$$\frac{m_2 d}{2^{p_2}} = \frac{2m_1 d}{2^{p_1+1}} = \frac{m_1 d}{2^{p_1}}.$$

□

Ideal choice of p and m

Given that there are infinitely many pairs of p and m that satisfy (1), which pair should we use? Because the division by multiplication method requires the product of the dividend and m, we naturally prefer the pair with the smallest m to avoid overflow in the multiplication.

Proposition 0.7. *Given $p \in \mathbb{N}_0$, define*

$$\bar{m}_p \equiv \left\lceil \frac{2^p}{d} \right\rceil \tag{10}$$

Then (4) holds for each natural number $m \geq \bar{m}_p$, and it does not hold for any natural number $m < \bar{m}_p$.

Proof. By rewriting (4), we obtain an equivalent condition that

$$m \geq \frac{2^p}{d}.$$

This condition holds if and only if m is no less than the ceiling of the right-hand side, which is $\bar{m}_p$. $\square$

Given $p \in \mathbb{N}_0$, we should use $\bar{m}_p$ in the division by multiplication approach, provided that (1) holds with $m = \bar{m}_p$. The next proposition demonstrates some properties of $p \mapsto \bar{m}_p : \mathbb{N}_0 \to \mathbb{N}$.

Proposition 0.8. *For each $p \in \mathbb{N}_0$, $\bar{m}_p \leq \bar{m}_{p+1} \leq 2\bar{m}_p$.*

Remark. When $d = 1$, we have that $\bar{m}_p = 2^p$; the claim clearly holds. Otherwise, $\bar{m}_p$ is nondecreasing in p, but the growth rate is at most 100 percent.

Proof. The first inequality immediately follows from the fact that
$2^p/d < 2^{p+1}/d$. To verify the the second inequality, we use the fact that

$$\frac{2^{p+1}}{d} = 2 \cdot \frac{2^p}{d} \leq 2 \cdot \left\lceil \frac{2^p}{d} \right\rceil.$$

The right-hand side of this inequality, which is an integer, is one of the integers no less than the left-hand side. Thus,

$$\bar{m}_{p+1} = \left\lceil \frac{2^{p+1}}{d} \right\rceil \leq 2 \cdot \left\lceil \frac{2^p}{d} \right\rceil = 2\bar{m}_p.$$

$\square$

Proposition 0.7 implies that our best choice of the pair of p is the minimum p that satisfies (1) with $m = \bar{m}_p$. If d is a power of two, we really don't need the division by multiplication method, as we can simply apply the bitwise right shift operation, as Section **??** demonstrates. When d is not a power of two, there is a lower bound for p that can be used in the division by multiplication.

Proposition 0.9. *Suppose that d is not a power of two. If $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ satisfy (1), then it holds that $p \geq \lfloor \log_2 \lfloor N/2 \rfloor \rfloor + 1$.*

Remark. When $d = 2^k$ ($< N$) for some $k \in \mathbb{N}_0$, it can hold that $p < \log_2 \lfloor N/2 \rfloor$, because (1) trivially holds with $p = k$ and $m = 1$.

Proof. Propositions 0.5 and 0.6 imply that there exists $p^* \in \mathbb{N}_0$ such that for each integer $p \geq p^*$, (1) holds with some $m \in \mathbb{N}$. It thus suffices to show that $p^* \geq \lfloor \log_2 \lfloor N/2 \rfloor \rfloor + 1$, i.e., (1) does not hold with $p = \tilde{p} \equiv \lfloor \log_2 \lfloor N/2 \rfloor \rfloor$

regardless of the value of m. As Proposition 0.7 shows, $\bar{m}_{\tilde{p}}$ is the minimum value of m that satisfies (4) with $p = \tilde{p}$. Because $md/2^{\tilde{p}}$ is increasing in m, we can establish the result by showing that (5) does not hold with $m = \bar{m}_{\tilde{p}}$.

Write $e_{\tilde{p}} \equiv \bar{m}_{\tilde{p}} d - 2^{\tilde{p}}$. Then it holds that $e_{\tilde{p}} \geq 1$ because $\bar{m}_{\tilde{p}} = \lceil 2^{\tilde{p}}/d \rceil$, and d is not a power of two by hypothesis. It also follows from Lemma 0.4 that

$$\log_2 \bar{n} \geq \log_2 \lfloor N/2 \rfloor \geq \lfloor \log_2 \lfloor N/2 \rfloor \rfloor = \tilde{p},$$

i.e., $2^{\tilde{p}} \leq \bar{n}$. It thus holds that

$$\frac{\bar{m}_{\tilde{p}} d}{2^{\tilde{p}}} = \frac{2^{\tilde{p}} + e_{\tilde{p}}}{2^{\tilde{p}}} \geq \frac{2^{\tilde{p}} + 1}{2^{\tilde{p}}} \geq \frac{\bar{n} + 1}{\bar{n}}.$$

The result therefore follows. $\square$

Define

$$\begin{aligned} p^* &\equiv \min \left\{ p \in \mathbb{N}_0 : \frac{\bar{m}_p d}{2^p} < \frac{\bar{n}+1}{\bar{n}} \right\} \\ &= \min \left\{ p \in \mathbb{N}_0 : \bar{m}_p \bar{n} < \frac{\bar{n}+1}{d} \cdot 2^p \right\}, \end{aligned} \tag{11}$$

Propositions 0.5 and 0.9 establishes lower and upper bounds for p^*. With the bounds, we can find p^* by checking if each p between $\lfloor \log_2 \lfloor N/2 \rfloor \rfloor + 1$ and $\lceil \log_2 (N-1) + \log_2 d \rceil$ satisfies that

$$\bar{m}_p \bar{n} < \frac{\bar{n}+1}{d} \cdot 2^p. \tag{12}$$

Because $(\bar{n}+1)/d$ is an integer that depends on neither $\bar{m}_p$ nor p, we only need to compute it once in the search for p^*.

Because $p^* \leq \bar{p}$, $\bar{m}_{p^*}$ is no greater than $\bar{m}_{\bar{p}}$, whose upper bound is established in the next proposition.

Proposition 0.10. *It holds that $\bar{m}_{\bar{p}} \leq 2N - 3$.*

Proof. By definition, we have that

$$\begin{aligned} \bar{m}_{\bar{p}} = \left\lceil \frac{2^{\bar{p}}}{d} \right\rceil &= \lceil 2^{\lceil \log_2 (N-1) + \log_2 d \rceil - \log_2 d} \rceil \\ &< \lceil 2^{\log_2 (N-1) + 1} \rceil = 2 \cdot (N-1). \end{aligned}$$

Because $\bar{m}_{\bar{p}}$ is an integer, it follows that

$$\bar{m}_{\bar{p}} \leq 2 \cdot (N-1) - 1 = 2N - 3.$$

$\square$

Unsigned division of W-bit integers

We now focus on the case in which both the divisors and the dividend are W-bit unsigned integers, where W is an natural number, which is fixed for the rest of this section (e.g., $W = 32$ or $W = 64$). We set $N = 2^W$, so that $\mathbb{X}_N = \mathcal{N}_W$. We here restate the results established in Subsections **??**-**??** in this special case of our focus.

Proposition 0.11. *(a) Let p and m be a nonnegative integer and a natural number, respectively. Then it holds that*

$$\left\lfloor \frac{nm}{2^p} \right\rfloor = q(n) \text{ for every } n \in \mathcal{N}_W \tag{13}$$

if and only if

$$1 \leq \frac{md}{2^p} < \frac{\bar{n}+1}{\bar{n}} \tag{14}$$

where $\bar{n} = 2^W - (2^W \bmod d) - 1$. When (14) holds, the first inequality is strict unless d is a power of two, while it holds that $E(2^W, m, p) \leq 1$ if $2^W \bmod d \neq d - 1$ or $p \leq W$.

(b) There exists $m \in \mathbb{N}$ that satisfies (13) with $p = \bar{p} \equiv \lceil \log_2(2^W - 1) + \log_2 d \rceil$.

(c) Suppose that $(p_1, m_1) \in \mathbb{N}_0 \times \mathbb{N}$ satisfies (13) with $p = p_1$ and $m = m_1$. Write $p_2 \equiv p_1 + 1$ and $m_2 \equiv 2m_1$. Then (13) also holds with $p = p_2$ and $m = m_2$.

(d) Given $p \in \mathbb{N}_0$, the first inequality in (14) holds for each natural number $m \geq \bar{m}_p \equiv \lceil 2^p/d \rceil$, and it does not hold for any natural number $m < \bar{m}_p$.

(e) For each $p \in \mathbb{N}_0$, $\bar{m}_p \leq \bar{m}_{p+1} \leq 2\bar{m}_p$.

(f) Suppose that d is not a power of two. If $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ satisfy (13), then it holds that $p \geq W$.

(g) It holds that $\bar{m}_{\bar{p}} \leq 2^{W+1} - 3$.

Proof. Set $N = 2^W$. Then it holds that $\log_2 \lfloor N/2 \rfloor = W - 1$. The claims of the proposition trivially follows from Propositions 0.3 and 0.5–0.8. □

Given the facts stated in Proposition 0.11, we use the pair of p^* and $\bar{m}_{p^*}$, where p^* is the least integer between W and $\bar{p} = \lceil \log_2(2^W - 1) + \log_2 d \rceil$ satisfying (12).

The upper bound $\bar{p}$ is tight in the sense that p^* can be equal to $\bar{p}$. For example:

Example 1. *Suppose that $W = 32$ and $d = 7$. Then it holds that $p^* = 35$ and $\bar{p} = \lceil \log_2(2^{32} - 1) + \log_2 d \rceil = 35$.*

On the other hand, it is pretty rare that $p^* = W$, as the next proposition demonstrates.

Proposition 0.12. *It holds that $p^* = W$ if and only if $2^W \mod d = d - 1$.*

Remarks.

(a) If d is a power of two, then $2^W \mod d = 0$. It also obviously holds that $p^* = \log_2 d < W$ and $\bar{m}_{p^*} = 1$. When d is not a power of two, this proposition means that $p^* > W$ when $2^W \mod d \neq d - 1$.

(b) Note that $2^W \mod d = d - 1$ if and only if $(2^W + 1) \mod d = 0$. For each $k \in \mathbb{N}_0$, $F_k \equiv 2^{2^k} + 1$ is called a *Fermat number*. It is known that F_k is prime for $k \in \{0, 1, 2, 3, 4\}$. Thus, it never holds $2^W \mod d = d - 1$ if $W \in \{1, 2, 4, 8, 16\}$. It also has been verified that F_5 and F_6 are respectively prime-factorized as $F_5 = 641 \times 6,700,417$ and $F_6 = 274,177 \times 67,280,421,310,721$. This means that there are only two divisors d that satisfies that $2^W \mod d = d-1$ when $W = 32$ and when $W = 64$.

Proof. If d is a power of two, it holds that $p^* < W$ and that $2^W \mod d = 0 \neq d - 1$. Thus the claim holds.

Assume that d is not a power of two. Then it holds that $p^* \geq W$, as Proposition 0.11(f) claims. By Proposition 0.11(a), (d), it follows that $p^* = W$ if and only if

$$\frac{\bar{m}_W d}{2^W} < \frac{\bar{n} + 1}{\bar{n}}.$$

Because d is not a power of two, it holds that $r_{2^W} \equiv 2^W \mod d \geq 1$, and that

$$\bar{m}_W = \frac{2^W - r_{2^W} + d}{d} = \frac{2^W + e_W}{d},$$

where $e_W \equiv d - r_{2^W}$. Thus, we have that

$$\frac{\bar{m}_W d}{2^W} = \frac{2^W + e_W}{2^W}.$$

It follows that $p^* = W$ if and only if

$$\frac{2^W + e_W}{2^W} < \frac{\bar{n} + 1}{\bar{n}},$$

or equivalently,

$$\frac{e_W}{2^W} < \frac{1}{\bar{n}}.$$

Rearranging this inequality yields that

$$e_W \bar{n} < 2^W. \tag{15}$$

Thus, it suffices to show that (15) holds if $r_{2^W} = d - 1$, and that it does not hold when $r_{2^W} \leq d - 2$.

Suppose that $r_{2^W} = d - 1$. Then we have that $e_W = 1$, so that (15) clearly holds. Suppose instead that $r_{2^W} \leq d - 2$. Then we have that $e_W \geq 2$. (15) does not hold because

$$e_W \bar{n} \geq 2\bar{n} \geq 2 \cdot 2^{W-1} = 2^W,$$

where the second inequality follows from Lemma 0.4. □

Proposition 0.13. *It holds that $E(2^W, p^*, m^*) \leq 1$.*

Proof. If d is a power of two, we have that $E(2^W, p^*, m^*) = 0 \leq 1$. Suppose that d is not a power of two. By Proposition 0.12, it holds that either $2^W \bmod d \neq d - 1$ or $p^* = W$. The result therefore follows by the second claim of Proposition 0.11(a). □

Overflow consideration

While Proposition 0.11(g) guarantees that $\bar{m}_{p^*}$ never exceeds $2^{W+1} - 3$, it can be larger than $2^W - 1$, the maximum integer in $\mathcal{N}_W$.

Example 2. *Suppose that $W = 32$ and $d = 3$. Then it holds that $p^* = 33$ and that $\bar{m}_{p^*} = 2,863,311,531$, with which we have that $2^{31} \leq \bar{m}_{p^*} \leq 2^{32} - 1$.*

Example 3. *Suppose that $W = 32$ and $d = 5$. Then it holds that $p^* = 34$ and that $\bar{m}_{p^*} = 3,435,973,837$, with which we have that $2^{31} \leq \bar{m}_{p^*} \leq 2^{32} - 1$.*

Example 4. *Suppose that $W = 32$ and $d = 7$. Then it holds that $p^* = 35$ and that $\bar{m}_{p^*} = 4,908,534,053$, with which we have that $2^{32} \leq \bar{m}_{p^*} \leq 2^{33} - 3$.*

Suppose that our computer can handle multiplication of two W-bit unsigned integers. To compute $n\bar{m}_{p^*}/2^{p^*}$, we typically use one of two methods. The first method assumes that the hardware provides the product of two W-bit unsigned integers in a $2W$-bit register. It takes the product of $\bar{m}_{p^*}$ and n, and then logical bitwise right shifts the result by p^* positions.

The second method assumes that the upper W bits of the product is given in a W-bit register (either discarding the lower W bits or storing the lower bits in another register). It takes the product of $\bar{m}_{p^*}$ and n, and then bitwise right shifts the upper W bits the product by $p^* - W$ positions.

Both of the methods described above requires that $\bar{m}_{p^*} \in \mathcal{N}_W$, i.e., $\bar{m}_{p^*} \leq 2^W - 1$. But it is not unusual that $\bar{m}_{p^*} \geq 2^W$. In such cases, we need a twist in the computation methods. Write $\bar{M}_{p^*} \equiv \bar{m}_{p^*} - 2^W$ and $s = p^* - W$. Then it holds that $\bar{M}_{p^*} \leq 2^W - 3$ because $\bar{m}_{p^*} \leq 2^{W+1} - 3$. Using $\bar{M}_{p^*}$ and s, We can express $n\bar{m}_{p^*}/2^{p^*}$ as

$$\frac{n\bar{m}_{p^*}}{2^{p^*}} = \frac{n(\bar{M}_{p^*} + 2^W)}{2^{W+s}} = \frac{n\bar{M}_{p^*}}{2^W \cdot 2^s} + \frac{n}{2^s} = \left(\frac{n\bar{M}_{p^*}}{2^W} + n\right) \Big/ 2^s.$$

The values appearing on the right-hand side of this equality involves only values in $\mathcal{N}_W$. But the right shift instruction of the CPU rounds down the fractional prat in the result each time. It turns out that the replacement of the regular division by the round-down division preserves the equality:

$$\left\lfloor \frac{n\bar{m}_{p^*}}{2^{p^*}} \right\rfloor = \left\lfloor \left(\left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + n \right) \Big/ \, 2^s \right\rfloor \tag{16}$$

We verify this equality below.

Lemma 0.14. *Suppose x is a integer, and d_1, and d_2 are positive integers. Write $d_0 \equiv d_1 \cdot d_2$. Then it holds that*

$$\left\lfloor \frac{x}{d_0} \right\rfloor = \left\lfloor \frac{\lfloor x/d_1 \rfloor}{d_2} \right\rfloor .$$

Proof. Write $a_0 \equiv \lfloor x/d_0 \rfloor$, $b_0 \equiv x - a_0 d_0$, $a_1 \equiv \lfloor b_0/d_1 \rfloor$, $b_1 \equiv b_0 - a_1 d_1$. Then it holds that $0 \leq b_0 \leq d_0 - 1$, and that $0 \leq b_1 \leq d_1 - 1$. Using these quantities, we can write x as

$$x = a_0 d_0 + a_1 d_1 + b_1.$$

Using this equality, we obtain that

$$\left\lfloor \frac{x}{d_1} \right\rfloor = \left\lfloor a_0 d_2 + a_1 + \frac{b_1}{d_1} \right\rfloor = a_0 d_2 + a_1.$$

It follows that

$$\left\lfloor \frac{\lfloor x/d_1 \rfloor}{d_2} \right\rfloor = \left\lfloor a_0 + \frac{a_1}{d_2} \right\rfloor = a_0 + \left\lfloor \frac{a_1}{d_2} \right\rfloor .$$

The first term on the right-hand side is the left-hand side of the equality in question, while the second term on the right-hand side of this equality is zero, because

$$0 \leq \left\lfloor \frac{a_1}{d_2} \right\rfloor = \left\lfloor \frac{a_1 d_1}{d_1 d_2} \right\rfloor = \left\lfloor \frac{a_1 d_1}{d_0} \right\rfloor \leq \left\lfloor \frac{a_1 d_1 + b_1}{d_0} \right\rfloor = \left\lfloor \frac{b_0}{d_0} \right\rfloor = 0$$

The result therefore follows. □

Proposition 0.15. *The equality (16) holds for every $n \in \mathcal{N}_W$.*

Proof. Because $p^* = W + s$ and $\bar{m}_{p^*} = \bar{M}_{p^*} + 2^W$, it follows from Lemma 0.14 that

$$\begin{aligned} \left\lfloor \frac{n\bar{m}_{p^*}}{2^{p^*}} \right\rfloor &= \left\lfloor \left\lfloor \frac{n\bar{m}_{p^*}}{2^W} \right\rfloor \Big/ \, 2^s \right\rfloor = \left\lfloor \left\lfloor \frac{n(\bar{M}_{p^*} + 2^W)}{2^W} \right\rfloor \Big/ \, 2^s \right\rfloor \\ &= \left\lfloor \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} + n \right\rfloor \Big/ \, 2^s \right\rfloor \end{aligned}$$

Because n is integer, we have that

$$\left\lfloor \frac{n\bar{M}_{p^*}}{2^W} + n \right\rfloor = \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + n.$$

The result therefore follows. □

When we use (16), it is important to notice that $\lfloor n\bar{M}_{p^*}/2^W \rfloor + n$ can still overflow if the addition is performed using W-bit registers. If the CPU provides a means to logically bitwise right shift the bits in the carry flag and the register together, the overflow does not pose any problems.

When we have no access to such a means, we need to avoid the overflow by further rewriting (16). This requires that $s \geq 1$.

Proposition 0.16. *If $\bar{m}_{p^*} \geq 2^W$, it holds that $s \geq 1$.*

Proof. We can assume that d is not a power of two, because otherwise, $\bar{m}_{p^*} = 1$. By hypothesis, we have that

$$\left\lceil \frac{2^{p^*}}{d} \right\rceil = \bar{m}_{p^*} \geq 2^W.$$

It follows that

$$2^{p^*-1} = \frac{2^{p^*}}{2} > \frac{2^{p^*}}{d} > 2^W - 1 = 2^W \left(1 - \frac{1}{2^W}\right)$$

Division of both sides of this inequality by 2^{W-1} yields that

$$2^s > 2\left(1 - \frac{1}{2^W}\right).$$

It follows that

$$2^s > 2\left(1 - \frac{1}{2}\right) = 1,$$

so that $s \geq 1$. □

Knowing that $s \geq 1$, (16) can be rewritten as

$$\begin{aligned}
\left\lfloor \frac{n\bar{m}_{p^*}}{2^{p^*}} \right\rfloor &= \left\lfloor \left\lfloor \left(\left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + n \right) \Big/ 2 \right\rfloor \Big/ 2^{s-1} \right\rfloor \\
&= \left\lfloor \left\lfloor \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + \left(n - \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor \right) \Big/ 2 \right\rfloor \Big/ 2^{s-1} \right\rfloor \\
&= \left\lfloor \left(\left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + \left\lfloor \left(n - \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor \right) \Big/ 2 \right\rfloor \right) \Big/ 2^{s-1} \right\rfloor
\end{aligned} \tag{17}$$

On the right-hand side of this identity, we have that

$$0 \leq \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor \leq \left\lfloor \frac{n(2^W - 1)}{2^W} \right\rfloor \leq \lfloor n \rfloor = n.$$

It follows that $n - \lfloor n\bar{M}_{p^*}/2^W \rfloor$ does not overflow. Also, it holds that

$$\begin{aligned}&\left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + \left\lfloor \left(n - \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor\right) \Big/ 2 \right\rfloor \\ &\quad \le \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + \left(n - \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor\right) \Big/ 2 = \left(n + \left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor\right) \Big/ 2 \le n.\end{aligned}$$

These verify that no part in the expression on the right-hand side of (17) overflows using W-bit registers, once $\lfloor n\bar{M}_{p^*}/2^W \rfloor$ is calculated.

Large divisors

When $d \ge 2^{W-1}$, it holds that

$$q(n) \equiv 1_{n \ge d}.$$

The division by multiplication method is less efficient than the conditional assignment after checking the condition that $n \ge d$.

Round up division

When we want to compute $\bar{q}(n) = \lceil n/d \rceil$ instead of $\lfloor n/d \rfloor$, we can use the facts that for any $n \in \mathcal{N}_W \backslash \{0\}$,

$$\bar{q}(n) = \left\lfloor \frac{n+d-1}{d} \right\rfloor = \left\lfloor \frac{n-1}{d} \right\rfloor + 1 = q(n-1) + 1,$$

and that $\bar{q}(0) = 0$. Using these facts, we obtain:

Proposition 0.17. *For every $n \in \mathcal{N}_W$, it holds that*

$$\bar{q}(n) = q(\nu(n)) + 1_{n>0},$$

where $\nu(n) \equiv n - 1_{n>0}$.

In this proposition, $q(\nu(n))$ can be computed by using the division by multiplication method.

Signed Division by a Number That Is Not a Power of Two

Write $\mathcal{Z}_W \equiv \{z \in \mathbb{Z} : -2^{W-1} \le z \le 2^{W-1} - 1\}$. This is the typical range of signed integers in a W-bit register. This section mainly considers division of integers in $\mathcal{Z}_W$ by a execution-invariant positive divisor $d \in \mathcal{Z}_W$, where the fractional part of the result rounded towards zero

Division by the absolute dividend and negation

We can handle the nonnegative dividends in $\mathcal{Z}_W$ by replacing W with $W-1$ in the analysis of the previous section. We just need to pick $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ such that

$$1 \leq \frac{md}{2^p} < \frac{\bar{n}+1}{\bar{n}}, \tag{18}$$

where $\bar{n} \equiv 2^{W-1} - (2^{W-1} \bmod d) - 1$. For each negative dividend $n \in \mathcal{Z}_W$, we have that

$$\left\lceil \frac{n}{d} \right\rceil = -\left\lfloor \frac{-n}{d} \right\rfloor.$$

It follows that

$$\left\lceil \frac{n}{d} \right\rceil = -\left\lfloor \frac{-nm}{2^p} \right\rfloor,$$

except when $n = -2^{W-1}$ (i.e., $-n \notin \mathcal{N}_{W-1}$). Thus, it holds that for each $n \in \mathcal{Z}_W \backslash \{-2^{W-1}\}$,

$$\operatorname{sgn}(n) \left\lfloor \frac{\operatorname{sgn}(n) \cdot nm}{2^p} \right\rfloor = q_n^0.$$

This requires two additional negation operations (or one absolute value and one negation) compared to the case with a positive dividend. But there is an alternative approach.

Division by multiplication with a shift

Define $\bar{n} \equiv 2^{W-1} - (2^{W-1} \bmod d) - 1$ and let p^* be the integer given by (11) with this value of $\bar{n}$. It then holds by Propositions 0.11 and 0.13 that for each negative $n \in \mathcal{Z}_W$

$$0 \leq \frac{(-n)m_{p^*}}{2^{p^*}} - \left\lfloor \frac{-n}{d} \right\rfloor \leq 1. \tag{19}$$

The second inequality is not strict because the largest possible value of $-n$ is 2^{W-1}. By applying the fact that $-\lfloor -x \rfloor = \lceil x \rceil$ to this inequality, multiplying all terms by -1, and adding one to all terms yields that

$$0 \leq \frac{n\bar{m}_{p^*}}{2^{p^*}} + 1 - \left\lceil \frac{n}{d} \right\rceil \leq 1. \tag{20}$$

This inequality is almost what we want, as it implies that $\lfloor mn/2^p \rfloor + 1 = \lceil n/d \rceil$ or $\lfloor mn/2^p \rfloor + 1 = \lceil n/d \rceil + 1$. If the second inequality of (20) is strict, we can rule out the latter possibility. In fact, we know that the first inequality in (19) is strict unless d is a power of two. Under the strict inequality, we obtain that

$$0 \leq \frac{n\bar{m}_{p^*}}{2^{p^*}} + 1 - \left\lceil \frac{n}{d} \right\rceil < 1,$$

so that for each negative $n \in \mathcal{Z}_W$, $\lfloor n\bar{m}_{p^*}/2^{p^*} \rfloor + 1 = \lceil n/d \rceil$.

Proposition 0.18. *Define*

$$\hat{q}(n) \equiv \left\lfloor \frac{\bar{m}_{p^*} n}{2^{p^*}} \right\rfloor + 1_{n<0}, \quad n \in \mathcal{Z}_W.$$

If $d \geq 2$, then it holds that for each $n \in \mathcal{Z}_W$, $\hat{q}(n) = q^0(n)$.

Remark. When $d = 1$, we have that $\bar{m}_{p^*} = 1$ and that $p^* = 0$. The claimed equality does not holds for negative dividends (e.g., $\hat{q}(-1) = 0 \neq -1 = q^0(-1)$).

Proof. As we have seen above, the claim is true if d is not a power of two. When $d = 2^k$ for some $k \in \{0, \ldots, W-2\}$, we have that $p^* = k$ and $\bar{m}_{p^*} = 1$. For any nonnegative $n \in \mathcal{Z}_W$, it obviously holds that $\hat{q}(n) = q^0(n)$. For each negative $n \in \mathcal{Z}_W$, we have that

$$q^0(n) = \left\lceil \frac{n}{2^k} \right\rceil = \left\lfloor \frac{n + 2^k - 1}{2^k} \right\rfloor = \left\lfloor \frac{n-1}{2^k} \right\rfloor + 1.$$

Write $r_n \equiv n - \lfloor n/2^k \rfloor 2^k$. Then we have that $0 \leq r_n \leq 2^k - 1$, and that

$$\left\lfloor \frac{n-1}{2^k} \right\rfloor = \left\lfloor \frac{\lfloor n/2^k \rfloor 2^k + r_n - 1}{2^k} \right\rfloor = \left\lfloor \frac{n}{2^k} \right\rfloor + \left\lfloor \frac{r_n - 1}{2^k} \right\rfloor = \left\lfloor \frac{n}{2^k} \right\rfloor.$$

It follows that

$$q^0(n) = \left\lfloor \frac{n}{2^k} \right\rfloor + 1 = \hat{q}(n).$$

□

When $\bar{m}_{p^*} \geq 2^{W-1}$, $\bar{m}_{p^*}$ does not belong to $\mathcal{Z}_W$. Because it holds that $\bar{m}_{p^*} \leq 2^W - 3$, however,

$$\bar{M}_{p^*} \equiv \bar{m}_{p^*} - 2^W$$

satisfies that $-2^{W-1} + 1 \leq \bar{M}_{p^*} \leq -3$, so that $\bar{M}_{p^*} \in \mathcal{Z}_W$. Define $s \equiv p^* - W$. Then $\hat{q}(n)$ can be rewritten as

$$\hat{q}(n) = \left\lfloor \left(\left\lfloor \frac{n\bar{M}_{p^*}}{2^W} \right\rfloor + n \right) \Big/ 2^s \right\rfloor + 1_{n<0}.$$

On the right-hand side of this equality, we have that

$$-2^{2W-2} \leq -(2^{W-1} - 1)^2 \leq n\bar{M}_{p^*} \leq (-2^{W-1} + 1)(-2^{W-1}) \leq 2^{2W-2}.$$

so that $-2^{W-2} \leq \lfloor n\bar{M}_{p^*}/2^W \rfloor \leq 2^{W-2}$. Also, n and $\lfloor n\bar{M}_{p^*}/2^W \rfloor$ have opposite signs. It follows that the computation of $\hat{q}(n)$ never overflows using W-bit registers, once $\lfloor n\bar{M}_{p^*}/2^W \rfloor$ is calculated.

Euclidean division

The method described in Subsection **??** rounds down the fractional part of the quotient if the dividend is positive; otherwise rounds up the fractional part. We sometimes want to perform Euclidean division, which rounds down the fractional part regardless of the sign of the dividend.

Because the method of Subsection **??** delivers the desired result for nonnegative dividends, we only consider how to deal with negative dividends. If an integer $n \in \mathcal{Z}_W$ is negative, we have that

$$q(n) = \left\lfloor \frac{n}{d} \right\rfloor = \left\lceil \frac{n-(d-1)}{d} \right\rceil = \left\lceil \frac{n+1}{d} \right\rceil - 1 = \hat{q}(n+1) - 1$$

Thus:

Proposition 0.19. *If $d \geq 2$, it holds that for any $n \in \mathcal{Z}_W$,*

$$q(n) = \hat{q}(\mu_n) - 1_{n<0} = \left\lfloor \frac{\mu_n \bar{m}_{p^*}}{2^{p^*}} \right\rfloor + 1_{\mu_n<0} - 1_{n<0} = \left\lfloor \frac{\mu_n \bar{m}_{p^*}}{2^{p^*}} \right\rfloor - 1_{n=-1}$$

where $\mu_n \equiv n + 1_{n<0}$.

Round up division

To calculate $\bar{q}(n)$ correctly, we need to modify $\hat{q}(n)$ for positive dividends, as Subsection **??** does. The result is:

Proposition 0.20.

$$\bar{q}(n) = \hat{q}(\nu_n) + 1_{n>0} = \left\lfloor \frac{\nu_n \bar{m}_{p^*}}{2^{p^*}} \right\rfloor + 1_{n\neq 0}$$

for every $n \in \mathcal{Z}_W$, where $\nu_n \equiv n - 1_{n>0}$.

Negative divisor

Now, let's consider the case with $d < 0$. Because $n/d = (-n)/(-d) = n'/|d|$, where $n' \equiv -n$, we can relate the case to the signed division with a positive divisor by letting $|d|$ and n' take the roles of the divisor and the dividend, respectively. This, however, requires a little adjustment. The range of n' is $(\mathcal{Z}_W \backslash \{-2^{W-1}\}) \cup \{2^{W-1}\}$ ($\neq \mathcal{Z}_W$), to which $|d|$ also belongs. To include 2^{W-1} in the set of dividends, we need to adjust the choice of p and m in the division by multiplication approach.

We first consider the division of nonnegative dividends by $|d|$, where the set of dividends to cover is

$$\{-z : z \in \mathcal{Z}_W, z \leq 0\} = \{z \in \mathbb{Z} : 0 \leq z \leq 2^{W-1}\} = \mathbb{X}_{2^{W-1}+1}.$$

We here restate the main results from Section **??** adapted to the current problem.

Proposition 0.21. *(a) Let p and m be a nonnegative integer and a natural number, respectively. Then it holds that*

$$\left\lfloor \frac{n'm}{2^p} \right\rfloor = \left\lfloor \frac{n'}{|d|} \right\rfloor \quad \textit{for every } n' \in \mathbb{X}_{2^{W-1}+1} \tag{21}$$

if and only if

$$1 \le \frac{md}{2^p} < \frac{\bar{n}+1}{\bar{n}} \tag{22}$$

where $\bar{n} = 2^{W-1} - ((2^{W-1}+1) \bmod d')$. When (22) holds, the first inequality is strict unless d is a power of two, while it holds that $E(2^{W-1}+1, m, p) \le 1$ if $(2^{W-1}+1) \bmod |d| \ne |d|-1$ or $p \le \log_2(2^{W-1}+1)$.

(b) There exists $m \in \mathbb{N}$ that satisfies (21) with $p = \bar{p} \equiv \lceil W - 1 + \log_2 |d| \rceil$.

(c) Suppose that $(p_1, m_1) \in \mathbb{N}_0 \times \mathbb{N}$ satisfies (21) with $p = p_1$ and $m = m_1$. Write $p_2 \equiv p_1 + 1$ and $m_2 \equiv 2m_1$. Then (21) also holds with $p = p_2$ and $m = m_2$.

(d) Given $p \in \mathbb{N}_0$, the first inequality in (22) holds for each natural number $m \ge \bar{m}_p$, and it does not hold for any natural number $m < \bar{m}_p$.

(e) For each $p \in \mathbb{N}_0$, $\bar{m}_p \le \bar{m}_{p+1} \le 2\bar{m}_p$.

(f) Suppose that d is not a power of two. If $p \in \mathbb{N}_0$ and $m \in \mathbb{N}$ satisfy (21), then it holds that $p \ge W-1$.

(g) It holds that $\bar{m}_{\bar{p}} \le 2^W - 1$.

Proof. Set $N = 2^{W-1}+1$. Then it holds that $\log_2 \lfloor N/2 \rfloor = W - 2$. The claims of the proposition trivially follows from Propositions 0.3 and 0.5–0.8. □

Let $\bar{n}$ be as defined in Proposition 0.21 and define

$$p^* \equiv \min \left\{ p \in \mathbb{N}_0 : \bar{m}_p \bar{n} < \frac{\bar{n}+1}{|d|} \cdot 2^p \right\}$$

Because $W - 1 \le p^* \le \bar{p}$, we can easily find the value of p^*, as discussed in Subsection **??**.

We now know that

$$q^0(n) = \left\lfloor \frac{-n}{|d|} \right\rfloor = \left\lfloor \frac{n(-m_{p^*})}{2^{p^*}} \right\rfloor \quad \text{for every } n \in \{z \in \mathcal{Z}_W : z \le 0\}.$$

Suppose that d is not a power of two. Then this equality is equivalent to

$$0 < \frac{n(-m_{p^*})}{2^{p^*}} - \left\lfloor \frac{-n}{|d|} \right\rfloor < 1 \text{ for every } n \in \{z \in \mathcal{Z}_W : z \le 0\}. \tag{23}$$

Pick an arbitrary positive integer n in $\mathcal{Z}_W$. Then $-n$ is negative, and it belongs to $\mathcal{Z}_W$. So, we can plug $-n$ into n in (23) to obtain that

$$0 < \frac{n\bar{m}_{p^*}}{2^{p^*}} - \left\lfloor \frac{-(-n)}{|d|} \right\rfloor < 1.$$

By applying the fact that $-\lfloor -x \rfloor = \lceil x \rceil$ to this inequality, multiplying all terms by -1, and adding one to all terms yields that

$$0 < \frac{n\bar{m}_{p^*}}{2^{p^*}} + 1 - \left\lceil \frac{-n}{|d|} \right\rceil < 1.$$

It follows that

$$\left\lceil \frac{n}{d} \right\rceil = \left\lceil \frac{-n}{|d|} \right\rceil = \left\lfloor \frac{n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor + 1 \text{ for every } n \in \{z \in \mathcal{Z}_W : z > 0\}.$$

Combining this result with that for the case with nonpositive dividends, we obtain that

$$q^0(n) = \left\lfloor \frac{n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor + 1_{n>0} \text{ for every } n \in \mathcal{Z}_W. \tag{24}$$

In computation of the right-hand side of this equality, it may be useful that $1_{n>0} = 1_{n(-\bar{m}_{p^*})<0}$.

Proposition 0.22. *Define* $\tilde{q} : \mathcal{Z}_W \to \mathcal{Z}_W$ *by*

$$\tilde{q}(n) \equiv \left\lfloor \frac{n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor + 1_{n>0}.$$

If $d \leq -2$*, then it holds that*

$$\tilde{q}(n) = q^0(n) \textit{ for every } n \in \mathcal{Z}_W.$$

Remark. The equality in question does not hold for positive dividends if $d = 1$ (e.g. $\tilde{q}(1) = 0 \neq 1 = q^0(1)$).

Proof. If d is not a power of two, the claim holds as we have already verified. Suppose that $d = -2^k$ for some $k \in \{1, 2, \ldots, W-1\}$. Then it holds that $p^* = k$ and that $\bar{m}_{p^*} = 1$. For each negative $n \in \mathcal{Z}_W$ (so that $n/d > 0$), it holds that

$$\tilde{q}(n) = \left\lfloor \frac{-n}{2^k} \right\rfloor = \left\lfloor \frac{n}{-2^k} \right\rfloor = q^0(n).$$

For any positive $n \in \mathcal{Z}_W$, we have that

$$q^0(n) = \left\lceil \frac{n}{-2^k} \right\rceil = \left\lceil \frac{-n}{2^k} \right\rceil = \left\lfloor \frac{-n + 2^k - 1}{2^k} \right\rfloor = \left\lfloor \frac{-n-1}{2^k} \right\rfloor + 1$$

Write $r_{-n} \equiv -n - \lfloor -n/2^k \rfloor \cdot 2^k$. Then it holds that $0 \leq r_{-n} \leq 2^k - 1$, and that

$$\left\lfloor \frac{-n-1}{2^k} \right\rfloor = \left\lfloor \frac{\lfloor -n/2^k \rfloor \cdot 2^k + r_{-n} - 1}{2^k} \right\rfloor = \left\lfloor \frac{\lfloor -n/2^k \rfloor \cdot 2^k + r_{-n} - 1}{2^k} \right\rfloor$$
$$= \left\lfloor \frac{-n}{2^k} \right\rfloor + \left\lfloor \frac{r_{-n} - 1}{2^k} \right\rfloor = \left\lfloor \frac{-n}{2^k} \right\rfloor.$$

It follows that

$$q^0(n) = \left\lfloor \frac{-n}{2^k} \right\rfloor + 1 = \tilde{q}(n).$$

□

As in division by a positive divisor, the multiplier $-\bar{m}_{p^*}$ can be less than -2^{W-1}, the minimum value in $\mathcal{Z}_W$, but we know that $\bar{m}_{p^*} \leq 2^W - 1$. Suppose that $\bar{m}_{p^*} \geq 2^{W-1} + 1$. Define $\bar{M}_{p^*} \equiv \bar{m}_{p^*} - 2^W$ and $s \equiv p^* - 2^W$. Then we have that

$$-(2^{W-1} - 1) \leq \bar{M}_{p^*} \leq -1$$

so that $-\bar{M}_{p^*} \in \mathcal{Z}_W$. Thus, We can perform the multiplication of n by $-\bar{M}_{p^*}$ by rewriting (24) as

$$\tilde{q}(n) = \left\lfloor \left(\left\lfloor \frac{n(-\bar{M}_{p^*})}{2^W} \right\rfloor - n \right) \Big/ 2^s \right\rfloor + 1_{n>0}.$$

The subtraction n from $\lfloor n(-\bar{M}_{p^*})/2^W \rfloor$ never overflows the using W-bit register.

For the Euclidean and round-up divisions, we can also easily verify that for each $n \in \mathcal{Z}_W$

$$q(n) = \tilde{q}(\nu_n) - 1_{n>0} = \left\lfloor \frac{\nu_n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor + 1_{\nu_n>0} - 1_{n>0} = \left\lfloor \frac{\nu_n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor - 1_{n=1}$$

and

$$\bar{q}(n) = \tilde{q}(\mu_n) + 1_{n<0} = \left\lfloor \frac{\mu_n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor + 1_{\mu_n>0} + 1_{n>0} = \left\lfloor \frac{\mu_n(-\bar{m}_{p^*})}{2^{p^*}} \right\rfloor + 1_{n\neq 0},$$

where $\nu_n = n - 1_{n>0}$ and $\mu_n = n + 1_{n<0}$.

Conclusion

This note implements the division by multiplication method in signed and unsigned division in the round down, round up, and round towards zero mode and demonstrates why the implementations work.

Granlund, Torbjörn, and Peter L. Montgomery. 1994. "Division by Invariant Integers Using Multiplication." *SIGPLAN Notices* 29 (6): 61–72.

Henry S. Warren, Jr. 2013. *Hacker's Delight*. 2nd edition. Addison Wesley–Pearson Education.