1 Introduction

The schoolbook division functions in current GMP are based on 3-by-2 division, `https://gmplib.org/~tege/division-paper.pdf`. These notes explore the possibility to replace this by a 2-by-2 approximate division. We reuse the notational conventions from the above paper, in particular ℓ is the word size in bits and β denotes the bignum base, $\beta = 2^\ell$.

2 Divisor input

The divisor input are two words, $d = \langle d_1, d_0 \rangle$, where the top word is normalized, $\beta/2 \le d_1 < \beta$. In schoolbok division, these will be the most significant 2ℓ bits of a larger number. We will also use the same precomputed reciprocal as for 3-by-2, defined as

$$v = \lfloor (\beta^3 - 1)/d \rfloor - \beta$$

3 3-by-2 division

For 3-by-2 division, we take a 3-word numerator as input, $\langle n_2, n_1, n_0 \rangle$, with $\langle n_2, n_1 \rangle < \langle d_1, d_0 \rangle$. In schoolbok division, these will be the top three words of a larger number, after a normalization shift matching the normalization of the divisor. With the case of $\langle n_2, n_1 \rangle = \langle d_1, d_0 \rangle$ handled specially. The 3-by-2 division computes the quotient and remainder

$$\begin{aligned} q &= \lfloor \langle n_2, n_1, n_0 \rangle / \langle d_1, d_0 \rangle \rfloor \\ \langle r_1, r_0 \rangle &= \langle n_2, n_1, n_0 \rangle - q \langle d_1, d_0 \rangle \end{aligned}$$

This q is then used as a candidate quotient for the larger numbers; it is correct, or one too large. And it's usually correct, so that adjustment is unlikely.

Let us recall the way the 3-by-2 quotient q is determined. First compute

$$\langle q_1, q_0 \rangle = v n_2 + \langle n_2, n_1 \rangle = (\beta + v) n_2 + n_1$$

and use $q_1 + 1$ as candidate. From the definition of v, we have $(\beta + v)d = \beta^3 - k$, with $1 \le k \le d$. Hence,

$$\begin{aligned} r &= \langle n_2, n_1, n_0 \rangle - (q_1 + 1)d \\ &= \langle n_2, n_1, n_0 \rangle - \frac{(\beta + v)n_2 + n_1 - q_0)d}{\beta} - d \\ &= n_1\beta + n_0 + \frac{kn_2 + (q_0 - n_1)d}{\beta} - d \\ &= \frac{kn_2 + n_1(\beta^2 - d) + n_0\beta + q_0 d - \beta d}{\beta} \end{aligned}$$

3.1 Lower bound

Grouping terms in different ways, we get immediately that

$$\begin{aligned} r &\ge -d \\ r &\ge -\frac{d}{\beta}(\beta - q_o) > \beta q_0 - \beta^2 \end{aligned}$$

and it follows that

$$r \geq \max(-d, \beta q_0 + 1 - \beta^2)$$

3.2 Upper bound

We need a pretty tight bound. First use that $k \leq d$ and $n_2 = (\langle n_2, n_1 \rangle - n_1)/\beta \leq (d - 1 - n_1)/\beta$, to get

$$\begin{aligned} r &\leq \frac{d\,(d - 1 - n_1)/\beta + n_1(\beta^2 - d) + n_0\beta + q_0 d - \beta d}{\beta} \\ &= \frac{d^2 - (1 + n_1)d + n_1\beta(\beta^2 - d) + n_0\beta^2 + \beta q_0 d - \beta^2 d}{\beta^2} \\ &= \frac{d^2 - d + n_1(\beta^3 - \beta d - d) + + n_0\beta^2 + \beta q_0 d - \beta^2 d)}{\beta^2} \end{aligned}$$

Now we have collected terms involving n_1. If for a moment we assume that $d \leq \beta^2 - \beta$, so that $(\beta^3 - \beta d - d) \geq 0$, we can use $n_1 \leq \beta - 1$ to get

$$\begin{aligned} r &\leq \frac{d^2 - d + (\beta - 1)(\beta^3 - \beta d - d) + + n_0\beta + \beta q_0 d - \beta^2 d}{\beta^2} \\ &= \frac{d^2 - d + \beta^4 - \beta^3 - \beta^2 d + \beta d - \beta d + d + n_0\beta + \beta q_0 d - \beta^2 d}{\beta^2} \\ &= \frac{d^2 - 2\beta^2 d + \beta^4 + n_0\beta^2 - \beta^3 + \beta q_0 d}{\beta^2} \\ &= \frac{(\beta^2 - d)^2 + \beta q_0 d}{\beta^2} + n_0 - \beta \\ &= \left(1 - \frac{d}{\beta^2}\right)(\beta^2 - d) + \frac{d}{\beta^2}\beta q_0 + n_0 - \beta \\ &\leq \max(\beta^2 - d, \beta q_0) + n_0 - \beta \end{aligned}$$

where the final inequality follows from recognizing the first two terms as a convex combination.

Now consider the border line case $d > \beta^2 - b$. Then $\beta^2 - d \leq \beta - 1$. We get $v = 0$, and $\langle q_1, q_0 \rangle = \langle n_2, n_1 \rangle$. As before, we also have $n_2 \leq (d - 1 - n_1)/\beta$.

$$\begin{aligned} r &= \langle n_2, n_1, n_0 \rangle - (n_2 + 1)d \\ &= n_2\,(\beta^2 - d) + n_1\beta - d + n_0 \\ &\leq \frac{(d - 1 - n_1)(\beta - 1)}{\beta} + n_1\beta - d + n_0 \\ &= d - 1 - n_1 - \frac{d - 1 - n_1}{\beta} + n_1\beta - d + n_0 \\ &= n_0 - 1 - \frac{d - 1}{\beta} + n_1(\beta - 1 + 1/\beta) \\ &\leq n_0 - 1 - \frac{\beta^2 - \beta}{\beta} + q_0(\beta - 1 + 1/\beta) \\ &= n_0 - 1 - \beta + 1 + q_0(\beta - 1 + 1/\beta) \\ &\leq \beta q_0 + n_0 - \beta \end{aligned}$$

So in all cases, we have the upper bound

$$r \leq \max(\beta^2 - d, \beta q_0) + n_0 - \beta$$

4 Quotient requirements

For schoolbook division, since we're having an adjustment step, we don't really need a correct 3-by-2 quotient, we have slightly more freedom. Furthermore, the influence from n_0 on the quotient is very weak. So we could try to find an appropriate candidate quotient with only $\langle n_2, n_1 \rangle$ as input. To ensure that q isn't too small for schoolbook division, it's tempting to substitute the maximum value, $\beta - 1$, for n_0,

$$\begin{aligned} q &\approx \beta\langle n_2, n_1 \rangle / \langle d_1, d_0 \rangle \\ r &= \langle n_2, n_1, \beta - 1 \rangle - q\langle d_1, d_0 \rangle \end{aligned}$$

But that large n_0 makes the remainder upper bound slightly too large. To buy a little margein, we instead use the remainder defined by

$$r = \langle n_2, n_1, 0 \rangle - q\langle d_1, d_0 \rangle$$

To guarantee that the quotient isn't too small for schoolbook division, we then need to ensure that $r \leq d - \beta$, and sometimes produce a quotient approximation corresponding to a small but negative r.

To ensure that q it is at most one unit to large, we have to require that $r \geq -d$. However, we want error to be unlikely, hence, we'd prefer a lower bound much closer to zero. With the algorithm developed in these notes, we get like $r > -3\beta$.

5 Quotient approximation

We still assume $\langle n_2, n_1 \rangle < \langle d_1, d_0 \rangle$ (we could strengthen this to $n_2 < d_1$ is useful; for equality, we should use the quotient approximation $q = \beta - 1$, and this can be handled as a special case). Let us also assume that $d_0 > 0$, then

$$\beta^2 - d = \langle \beta - 1 - d_1, \beta - d_0 \rangle$$

We use the same candidate quotient as for regular 3-by-2, $q_1 + 1$. To compute the corresponding remainder, let $\langle p_1, p_0 \rangle = q_1 d_0$. Then

$$r = \langle n_2, n_1, 0 \rangle - (q_1 + 1)\langle d_1, d_0 \rangle = \beta\left(\langle n_2, n_1 \rangle - (q_1 + 1)d_1 - p_1\right) - d_0 - p_0$$

So we can compute the middle word, $r_1 = \lfloor (r \bmod \beta^2)/\beta \rfloor$ as

$$r_1 = n_1 - (q_1 + 1)d_1 - p_1 - 1 - [p_0 > (\beta - d_0)] \pmod{\beta}$$

Also let $r_0 = -(q_1 + 1)d_0 \bmod \beta$ denote the low word of the remainder, but we strive to avoid keeping track of this value. What can we say about r_1 and q_0?

First assume $r < 0$, then $r = \langle r_1, r_0 \rangle - \beta^2$. We have the lower bounds

$$r_1\beta + r_0 = r + \beta^2 \geq \max(\beta^2 - d, \beta q_0)$$

So it follows that $r_1 \geq q_0$. We also know that $r + d \geq 0$, but if we don't want to modify r_0 and handle carry propagation, we can get a positive value by adding $\beta(d_1 + 1)$.

Now, assume that $r \geq 0$. Then $r = \langle r_1, r_0 \rangle \leq \max(\beta^2 - d, \beta q_0) - \beta$. What if $r_1 \geq q_0$? Can we add $d_1 + 1$ to r_1 without overflow? We get

$$\langle r_1, r_0 \rangle \leq \beta^2 - d - \beta$$

and hence

$$\langle r_1, r_0 \rangle + (d_1 + 1)\beta \leq \beta^2 - d + d_1\beta = \langle \beta - 1, \beta - d_0 \rangle < \beta^2$$

So this won't overflow. This is the tightest of the involved bounds, and it depends on the choice $n_0 = 0$ and the requirement $d_0 > 0$.

Let's see where we are after this first adjustment step, if we set

$$\begin{array}{lll} q' = q_1 + 1 & r'_1 = r_1 & \text{if } r_1 < q_0 \\ q' = q_1 & r'_1 = (r_1 + d_1 + 1) \bmod \beta & \text{if } r_1 \geq q_0 \end{array}$$

The new remainder is $r' = \langle n_2, n_1, 0 \rangle - q' \langle d_1, d_0 \rangle$, and it's relation to r'_1 is subject to approximation.

In the first case (no adjustment), we still have $r' = \langle r_1, r_0 \rangle$. In the second case, we have

$$\begin{aligned} r' = r + d &= \langle r_1, r_0 \rangle + \langle d_1, d_0 \rangle \pmod{\beta^2} \\ &= \beta(r_1 + d_1) + r_0 + d_0 \pmod{\beta^2} \end{aligned}$$

and it follows that

$$r' = \beta r'_1 + (r_0 + d_0 - \beta)$$

From the schoolbook correctness condition, we need to increment the quotient in case $r > d - \beta = \langle d_1 - 1, d_0 \rangle$.

From the above equations, we see that $r' < \beta(r'_1 + 1)$. Then $r'_1 \leq d_1 - 2$ is sufficient to get

$$r' < \beta(d_1 - 1) < d - \beta$$

So the final quotient would then be

$$q = q_1 + [r_1 < q_0] + [r'_1 \geq d_1 - 1]$$

The final remainder may be negative, but how small? Before the final adjustment we have $r' \geq -\beta$. If we have an adjustment, then $r_1 \geq d_1 - 1$, then $r' \geq \beta(r_1 - 1) = \beta(d_1 - 2)$, hence after adjustment

$$r' - d \geq \beta(d_1 - 2) - d = -2\beta - d_0 > -3\beta$$

6 Quotient overflow?

One problem is that we may potentially produce an approximative quotient $q = \beta$, exceeding one word, when the correct quotient would be $\beta - 1$. This can happen when $n_2 = d_1$ (a case easy to exclude) or $n_2 = d_1 - 1$. But in both cases, maybe we can use $\beta - 1$ as appproximative quotient?

7 Possible improvements?

It would be nice if we could omit the $[p_0 > (\beta - d_0)]$ term in the computation of r_1, which may give an additional error of one unit in r_1. We can gain some improved margin by requiring that $n_2 < d_1$, but unclear if that is sufficient.