NOTE ON COMPUTATION OF INTEGER SQUARE ROOTS

DANIEL HAST

The integer square root function $m \mapsto \lfloor \sqrt{m} \rfloor$ can be implemented efficiently using [1, Algorithm 1.13]. Fix integers $m \geq 1$ and $x_0 \geq \lfloor \sqrt{m} \rfloor$. Recursively define a sequence as follows:

$$x_{n+1} = \left\lfloor \frac{x_n + \lfloor m/x_n \rfloor}{2} \right\rfloor.$$

Note that since x_n is an integer, we also have

$$x_{n+1} = \left\lfloor \frac{x_n + m/x_n}{2} \right\rfloor.$$

In [1, Theorem 1.7], it is shown that this sequence decreases until reaching $\lfloor \sqrt{m} \rfloor$.

Here we analyze this algorithm in more detail: We show that the sequence either attains a fixed point at $\lfloor \sqrt{m} \rfloor$ or oscillates between $\lfloor \sqrt{m} \rfloor$ and $\lfloor \sqrt{m} \rfloor + 1$, and we prove a bound proportional to $\log_2(\log_2(m))$ on the number of steps required for the sequence to stabilize in this manner.

This allows Algorithm 1.13 to be turned into a *constant-time* algorithm by running the algorithm for a number of steps depending only on the bit-width of the unsigned integer type used to represent m, not the value m itself, and then taking the minimum of the final two values to account for the possibility of oscillation. (Of course, for this to yield a constant-time algorithm, we must also use constant-time implementations of addition, division, the minimum function, etc.)

Lemma. (1) If $x_n = \lfloor \sqrt{m} \rfloor$, then $x_{n+1} \in \{x_n, x_n + 1\}$.

(2) If $x_n > \lfloor \sqrt{m} \rfloor$, then $\lfloor \sqrt{m} \rfloor \leq x_{n+1} < x_n$.

(3) If $x_n > \lfloor \sqrt{m} \rfloor$, then

$$x_n - \sqrt{m} > 2(x_{n+1} - \sqrt{m}).$$

(4) For all $k > 2$, if $1 < x_n/\sqrt{m} < k/(k-2)$, then

$$x_n - \sqrt{m} > k(x_{n+1} - \sqrt{m}).$$

Proof. Suppose $x_n = \lfloor \sqrt{m} \rfloor$. For any $s \geq 1$, we have

$$\lfloor s \rfloor (\lfloor s \rfloor + 3) = \lfloor s \rfloor^2 + 3\lfloor s \rfloor \geq \lfloor s \rfloor^2 + 2\lfloor s \rfloor + 1 = (\lfloor s \rfloor + 1)^2 > s^2.$$

Setting $s = \sqrt{m}$, we obtain $x_n(x_n + 3) > m$, so $\lfloor m/x_n \rfloor \leq m/x_n < x_n + 3$. Thus

$$x_{n+1} = \left\lfloor \frac{x_n + \lfloor m/x_n \rfloor}{2} \right\rfloor \leq \left\lfloor \frac{x_n + (x_n + 2)}{2} \right\rfloor = x_n + 1.$$

Furthermore, $\lfloor m/x_n \rfloor \geq x_n$, so $x_{n+1} \geq x_n$. This proves (1).

Now suppose $x_n > \lfloor \sqrt{m} \rfloor$. Then $x_n > \sqrt{m}$, so $m/x_n < x_n$. Thus

$$x_{n+1} = \left\lfloor \frac{x_n + m/x_n}{2} \right\rfloor < x_n.$$

Furthermore, by the AM–GM inequality,

$$\frac{x_n + m/x_n}{2} > \sqrt{m},$$

so

$$x_{n+1} = \left\lfloor \frac{x_n + m/x_n}{2} \right\rfloor \geq \left\lfloor \sqrt{m} \right\rfloor .$$

This proves (2). (Note that (2) is also proved as part of [1, Theorem 1.7].) Moreover, $x_n > \sqrt{m}$ implies $m/x_n < \sqrt{m}$, so

$$x_n - \sqrt{m} > x_n + m/x_n - 2\sqrt{m} = 2\left(\frac{x_n + m/x_n}{2} - \sqrt{m}\right) \geq 2(x_{n+1} - \sqrt{m}),$$

proving (3) as well.

Finally, fix $k > 2$ and suppose $x_n > \sqrt{m}$ and $x_n/\sqrt{m} < k/(k-2)$. Then $(k-2)x_n < k\sqrt{m}$, so

$$\begin{aligned} 0 &< (x_n - \sqrt{m})\left(k\sqrt{m} - (k-2)x_n\right) \\ &= (2k-2)x_n\sqrt{m} - (k-2)x_n^2 - km \\ &= x_n\left((2k-2)\sqrt{m} - (k-2)x_n - km/x_n\right) \\ &= x_n\left(2(x_n - \sqrt{m}) - k(x_n + m/x_n - 2\sqrt{m})\right). \end{aligned}$$

Thus

$$2(x_n - \sqrt{m}) > k(x_n + m/x_n - 2\sqrt{m}) \geq 2k(x_{n+1} - \sqrt{m}),$$

proving (4). □

Theorem. Suppose $x_0 < 3\sqrt{m}$. Then for all $n > \max(1, \log_2(\log_2(m)) - \log_2(3))$,

$$\min(x_n, x_{n+1}) = \left\lfloor \sqrt{m} \right\rfloor .$$

Proof. Let $d_n = \log_2(x_n - \sqrt{m})$ if $x_n > \sqrt{m}$ and $d_n = -\infty$ otherwise. By parts (2) and (3) of the lemma, if $d_n \neq -\infty$, then $d_n - d_{n+1} > 1$. By part (4) of the lemma applied to $k = 2^i$, if $0 < (x_n - \sqrt{m})/\sqrt{m} < 2/(2^i - 2)$, then $d_n - d_{n+1} > i$. In particular, if $d_n \neq -\infty$ and $d_n < \log_2\sqrt{m}$, then $d_n - d_{n+1} > 2$. Also, if $d_n \neq -\infty$ and $d_n \leq \log_2\sqrt{m} + 1 - i$, then $d_n - d_{n+1} > i$.

If $x_0 < 3\sqrt{m}$, then $x_1 - \sqrt{m} < \frac{1}{2}(x_0 - \sqrt{m}) < \sqrt{m}$, so $d_1 < \log_2\sqrt{m}$. Thus $d_1 - d_2 > 2$, so $d_2 < \log_2\sqrt{m} + 1 - 3$. If $d_2 \neq -\infty$, this implies $d_2 - d_3 > 3$, so $d_3 < \log_2\sqrt{m} + 1 - 6$. Continuing inductively, we see that for all $n \geq 2$,

$$d_n < \log_2\sqrt{m} + 1 - 3 \cdot 2^{n-2}$$

as long as $d_0, \ldots, d_n \neq -\infty$. In particular, applying part (1) of the lemma, if $3 \cdot 2^{n-1} > \log_2\sqrt{m}$, then either x_n or x_{n+1} is equal to $\lfloor\sqrt{m}\rfloor$. Taking logarithms of both sides of this inequality yields the theorem. □

Corollary. If $2^{b-1} \leq m < 2^b$ and $x_0 = 2^{\lceil b/2 \rceil}$, then for all $n \geq \max(2, \lfloor\log_2(b)\rfloor + 1)$,

$$\min(x_n, x_{n+1}) = \left\lfloor \sqrt{m} \right\rfloor .$$

Proof. Since $x_0 < 2 \cdot 2^{b/2} = 2\sqrt{2}(2^{b-1})^{1/2} \leq 2\sqrt{2}\sqrt{m} < 3\sqrt{m}$, this follows from the theorem. □

References

[1] Richard Brent and Paul Zimmermann, *Modern Computer Arithmetic*, Cambridge Monographs on Applied and Computational Mathematics, Cambridge University Press, 2010.