



Solady cbirt & cbirtWad Audit Report

2024-07-31

About

<https://solady.org/>

<https://xuwinnie.review/>

Scope

<https://github.com/Vectorized/solady/blob/43f9d49815c8126d92771b26bd9bdbe2dbea87a5/src/units/FixedPointMathLib.sol>

Function cbirt

Function cbirtWad

Proof

Correctness of cbirt

The input u is an integer satisfying $0 \leq u < 2^{256}$, let $r = \sqrt[3]{u}$, we will prove the output is equal to $\lceil r \rceil$.

For $u < 2^{14}$, We manually verify the output is valid.

The first part of the code gives an initial guess of r , we name it a .

For each $u > 0$, there exists unique integers k, i , such that $2^{24k+4i} \leq u < 2^{24k+4(i+1)}$, where $i = 0, 1, \dots, 5$

Then

$$a = \begin{cases} 2^{8k} \cdot \frac{15}{7} & i = 0 \\ 2^{8k} \cdot \frac{30}{7} & i = 1 \\ 2^{8k+2} \cdot \frac{15}{5} & i = 2 \\ 2^{8k+2} \cdot \frac{30}{5} & i = 3 \\ 2^{8k+5} \cdot \frac{15}{6} & i = 4 \\ 2^{8k+5} \cdot \frac{30}{6} & i = 5 \end{cases}$$

We can prove

$$0.595213 < \frac{a-1}{r} < \frac{[a]}{r} \leq \frac{a}{r} < 2.142858 \quad (1)$$

The next part of the code iteratively improves the guess. Sequence $\{a_n\}$ is introduced, where

$$a_0 = [a] \text{ and } a_{n+1} = \left\lfloor \frac{\left\lfloor \frac{u}{a_n^2} \right\rfloor + 2a_n}{3} \right\rfloor$$

(It's easy to prove a_n^2 will not overflow and a_n will not be zero)

Then we have

$$a_{n+1} \leq \frac{\frac{u}{a_n^2} + 2a_n}{3} \quad (2)$$

And

$$a_{n+1} \geq \frac{\left\lfloor \frac{u}{a_n^2} \right\rfloor + 2a_n}{3} - \frac{2}{3} > \frac{\left(\frac{u}{a_n^2} - 1\right) + 2a_n}{3} - \frac{2}{3} = \frac{\frac{u}{a_n^2} + 2a_n}{3} - 1 \quad (3)$$

From (3), for $n > 0$, we have

$$a_n > \frac{\frac{u}{a_{n-1}^2} + 2a_{n-1}}{3} - 1 \geq r - 1 \quad (4)$$

We introduce another sequence $\{b_n\}$, let $b_0 = a_0 = [a]$ and $b_{n+1} = \left\lfloor \frac{\frac{u}{b_n^2} + 2b_n}{3} \right\rfloor$

Lemma 1: $b_7 < r + 1$

Proof: Let $c_n = \frac{b_n - r}{r}$, then $c_0 = \frac{[a]}{r} - 1$, $c_{n+1} = \frac{c_n^2(2c_n+3)}{3(c_n+1)^2}$, from (1) we know $-0.404787 < c_0 < 1.142858$.

let $f(x) = \frac{x^2(2x+3)}{3(x+1)^2}$, $f'(x) = \frac{2}{3}(1 - \frac{1}{(x+1)^3})$, we can see $f(x)$ is decreasing on $(-1, 0)$ and increasing on $(0, +\infty)$, with the minimum value of $f(0) = 0$.

So $0 \leq c_1 < \max(f(-0.404787), f(1.142858)) < \max(0.337687, 0.501164) = 0.501164$, and $0 \leq c_n < f_{n-1}(0.501164)$ for $n \geq 2$. Specifically, $c_7 < f_6(0.501164) < 1.443599 \times 10^{-28}$. So $b_7 = r + c_7 r < r + 1.443599 \times 10^{-28} \times 2^{\frac{256}{3}} < r + 0.007037 < r + 1$

Lemma 2: There exists an integer s , such that $1 \leq s \leq 7$ and $r - 1 < a_s < r + 1$

Proof: We prove by contradiction. If not, recall (4), we know a_1 to a_7 are all equal or greater than $r + 1$.

From (2), we have

$$a_{n+1} - a_n \leq \frac{\frac{u}{a_n^2} + 2a_n}{3} - a_n = \frac{\frac{r^3}{a_n^2} - a_n}{3} < 0 \quad (5)$$

Then $a_1 > a_2 > \dots > a_7 \geq r + 1$

Recall (2), we have $b_1 \geq a_1 \geq r + 1$, and if $b_n \geq a_n \geq r + 1$, then

$$b_{n+1} = \left\lfloor \frac{\frac{u}{b_n^2} + 2b_n}{3} \right\rfloor \geq \frac{\frac{u}{a_n^2} + 2a_n}{3} \geq a_{n+1} \geq r + 1$$

So $b_7 \geq r + 1$, which contradicts Lemma 1.

Lemma 3: If $r - 1 < a_s < r + 1$, then $r - 1 < a_{s+1} < r + 1$

Proof: If r is an integer, then $a_{s+1} = a_s = r$. Otherwise, a_s is either $\lceil r \rceil$ or $\lceil r \rceil + 1$. Recall (4), we only need to prove $a_{s+1} < r + 1$

When $a_s = \lceil r \rceil$, from (2) we have

$$a_{s+1} \leq \frac{\frac{u}{\lceil r \rceil^2} + 2\lceil r \rceil}{3} < \frac{\frac{(\lceil r \rceil + 1)^3}{\lceil r \rceil^2} + 2\lceil r \rceil}{3} = \lceil r \rceil + 1 + \frac{1}{\lceil r \rceil} + \frac{1}{3\lceil r \rceil^2} \leq \lceil r \rceil + 1 + \frac{1}{2^{14}} + \frac{1}{3 \cdot 2^{28}} < \lceil r \rceil + 2$$

Since a_{s+1} and $\lceil r \rceil + 2$ are both integers, $a_{s+1} \leq \lceil r \rceil + 1 < r + 1$

When $a_s = \lceil r \rceil + 1$, we know $a_s > r$, similar to (5) we have $a_{s+1} < a_s < r + 1$

From the above three lemmas, we know that a_7 is either $\lceil r \rceil$ or $\lceil r \rceil + 1$. At the final step, when $a_7 = \lceil r \rceil$, $\frac{u}{\lceil r \rceil^2} \geq \lceil r \rceil$, the output is $\lceil r \rceil$; when $a_7 = \lceil r \rceil + 1$, $\frac{u}{(\lceil r \rceil + 1)^2} < \lceil r \rceil + 1$, the final output is $\lceil r \rceil + 1 - 1 = \lceil r \rceil$

Correctness of cbtWad

The input v is an integer satisfying $\frac{2^{256}}{10^{36}} < v < 2^{256}$, let $s = 10^{12} \cdot \sqrt[3]{v}$, we will prove the output is equal to $\lceil s \rceil$.

Let n be an integer such that $n^3 \leq v < (n+1)^3$, then $b = \left\lceil \frac{\lceil \frac{10^{12} \cdot v}{(n+1)^2} \rceil + 2 \cdot 10^{12}(n+1)}{3} \right\rceil$.

We define c as $c = \frac{\frac{10^{12} \cdot v}{(n+1)^2} + 2 \cdot 10^{12}(n+1)}{3}$, then we consider both c and s as functions of v . We have $c'(v) = \frac{10^{12}}{3(n+1)^2}$, $s'(v) = \frac{10^{12}}{3v^{\frac{2}{3}}}$, noting that $c((n+1)^3) = s((n+1)^3) = 10^{12}(n+1)$, and $c'(v) < s'(v)$ holds for $n^3 \leq v < (n+1)^3$, we have

$$0 < c - s \leq c(n^3) - s(n^3) = 10^{12} \cdot \frac{3n+2}{3(n+1)^2} < \frac{10^{12}}{n+1} < 1 \quad (1)$$

We know $b \leq c$. We also have

$$b \geq \frac{\lceil \frac{10^{12} \cdot v}{(n+1)^2} \rceil + 2 \cdot 10^{12}(n+1)}{3} - \frac{2}{3} > \frac{(\frac{10^{12} \cdot v}{(n+1)^2} - 1) + 2 \cdot 10^{12}(n+1)}{3} - \frac{2}{3} = c - 1 \quad (2)$$

Combining (1) and (2), we have

$$s - 1 < b < s + 1 \quad (3)$$

So b is either $\lceil s \rceil$ or $\lceil s \rceil + 1$.

After obtaining b , the code introduces another p to differentiate between the two cases.

$$p = \begin{cases} v & 2^{249} \leq v < 2^{256} \\ v \cdot 10^2 & 2^{229} \leq v < 2^{249} \\ v \cdot 10^8 & 2^{199} \leq v < 2^{229} \\ v \cdot 10^{17} & \frac{2^{256}}{10^{36}} \leq v < 2^{199} \end{cases}$$

(We can verify $p < 2^{256}$ so it will not overflow)

let $b = s + r = 10^{12} \cdot \sqrt[3]{v} + r$, then

$$b^3 = (10^{12} \cdot \sqrt[3]{v} + r)^3 = 10^{36} \cdot v + 3 \cdot 10^{24} \cdot v^{\frac{2}{3}} r + 3 \cdot 10^{12} \cdot v^{\frac{1}{3}} r^2 + r^3$$

Let $\beta = 3 \cdot 10^{24} \cdot v^{\frac{2}{3}}r + 3 \cdot 10^{12} \cdot v^{\frac{1}{3}}r^2 + r^3$, we can prove

$$\frac{|\beta|}{p} = \frac{|3 \cdot 10^{24} \cdot v^{\frac{2}{3}}r + 3 \cdot 10^{12} \cdot v^{\frac{1}{3}}r^2 + r^3|}{p} \leq \frac{3.1 \cdot 10^{24} \cdot |v^{\frac{2}{3}}|}{p} < 0.354499 \quad (4)$$

Noting β is an integer and $b^3 \equiv \beta \pmod{p}$, from (4) we have

$$\begin{aligned} b = [s] + 1 &\implies r > 0 \implies \beta > 0 \implies \\ \text{mod}(b^3, p) = \beta &\implies 0 < \text{mod}(b^3, p) < \frac{p}{2} \implies \text{output is } [s] \end{aligned}$$

When $r < 0$, it's not hard to prove $\beta < 0$, similarly

$$\begin{aligned} b = [s] &\implies r \leq 0 \implies \beta \leq 0 \implies \\ \text{mod}(b^3, p) = 0 \text{ or } \text{mod}(b^3, p) = 1 + \beta &> \frac{p}{2} \implies \text{output is } [s] + 1 - 1 = [s] \end{aligned}$$