A nearly correctly-rounded cube root

Robin Leroy (eggrobin)

TODO(egg): 2017-03-36

This document describes the error analysis of the real cube root function Cbrt implemented in numerics/cbrt.cpp.

On root finding methods studied by Lagny, Halley, Householder, *et alii*

We start with a historical overview of a family of root-finding methods. In [Fan91a], Lagny first presents the iterates

$$a \mapsto \frac{1}{2}a + \sqrt{\frac{1}{4}a^2 + \frac{b}{3a}},$$
 (1)

hereafter the irrational method, and

$$a \mapsto a + \frac{ab}{3\sigma^3 + b},\tag{2}$$

the *rational method*, for the computation of the cube root $\sqrt[3]{a^3 + b}$, mentioning the existence of similar methods for arbitrarily higher powers. In [Fan91b] the above methods are again given, with an outline of the general method for higher powers, and a mention of their applicability to finding roots of polynomials other than $z^p - r$.

That general method is given in detail in [Fan92, p. 19]. Modernizing the notation, the general rule is as follows for finding a root of the monic polynomial of degree $p \ge 2$

$$f(z)\coloneqq z^p+c_1z^{p-1}+\cdots+c_{p-1}z+c_p \eqqcolon z^p-R(z)$$

with an initial approximation a.

Separate the binomial expansion of $\left(x + \frac{1}{2}a\right)^p$ into alternating sums of degree p and p-1 in z,

$$S_1 := \sum_{\substack{k=0 \ 2lk}}^p \binom{p}{k} x^{p-k} \left(\frac{1}{2}a\right)^k$$

$$S_2 := \sum_{\substack{k=0\\2lk}}^{p} {p \choose k} x^{p-k} \left(\frac{1}{2}a\right)^k$$

and consider the polynomials in x

$$E_p := S_1 - \frac{1}{2}R\left(x + \frac{1}{2}a\right)$$
$$E_{p-1} := S_2 - \frac{1}{2}R\left(x + \frac{1}{2}a\right).$$

Let E_{n-1} be the remainder of the polynomial division of E_{n+1} by E_n .

The iterate is $a \mapsto x + \frac{1}{2}a$, where x is a root of E_2 for the irrational method, and the root of E_1 for the rational method.

Theorem. The iterate of Lagny's rational method for a polynomial f of degree p is

$$a \mapsto a + (p-1) \frac{(1/f)^{(p-2)}(a)}{(1/f)^{(p-1)}(a)}$$
 (3)

Proof. Let $E_p = d_0 x^p + \dots + d_p$, $E_p = e_0 x^{p-1} + \dots + e_{p-1}$. As shown in [Hou70, pp. 52–54], the polynomial remainders E_k is are given up to a constant factor by [Hou70, p. 19] equation (23), *i.e.*, for some α ,

$$\frac{E_k}{\alpha_k} = \det \begin{pmatrix} (E_p)_{p-1-k} \\ (E_{p-1})_{p-k} \end{pmatrix},$$

where the expression on the right-hand side is the *bigradient* defined in [Hou68] (3.2) or [Hou70, p. 19] (20),

$$\frac{E_k}{\alpha_k} = \det \begin{pmatrix} d_0 & d_1 & d_2 & \cdots & d_{2(p-k)-3} & x^{p-k-2}E_p \\ 0 & d_0 & d_1 & \cdots & d_{2(p-k)-4} & x^{p-k-3}E_p \\ \vdots & \ddots & & \vdots & & & \vdots \\ 0 & \cdots & 0 & d_0 & d_1 & \cdots & d_{p-k-1} & x^0E_p \\ 0 & \cdots & 0 & 0 & e_0 & \cdots & e_{p-k-2} & x^0E_{p-1} \\ \vdots & & \ddots & & & \vdots \\ 0 & 0 & e_0 & \cdots & e_{2(p-k)-4} & x^{p-k-2}E_p \\ 0 & e_0 & e_1 & \cdots & e_{2(p-k)-4} & x^{p-k-2}E_p \\ e_0 & e_1 & e_2 & \cdots & e_{2(p-k)-3} & x^{p-k-1}E_p \end{pmatrix} =: \det \mathbf{E}_k,$$

where $d_n := 0$ for n > p, and $e_n := 0$ for n > p - 1.

In particular, for k = 1, the matrix \mathbf{E}_1 is

$$\begin{pmatrix} d_0 & d_1 & d_2 & \cdots & d_{p-3} & d_{p-2} & d_{p-1} & d_p & 0 & \cdots & 0 & x^{p-3}E_p \\ 0 & d_0 & d_1 & \cdots & d_{p-4} & d_{p-3} & d_{p-2} & d_{p-1} & d_p & \ddots & 0 & x^{p-4}E_p \\ \vdots & & \ddots & & & & \vdots & & \vdots \\ 0 & \cdots & 0 & d_0 & d_1 & d_2 & & \cdots & & d_{p-2} & x^0E_p \\ 0 & \cdots & 0 & 0 & e_0 & e_1 & & \cdots & & e_{p-3} & x^0E_{p-1} \\ \vdots & & & \ddots & & & & \vdots \\ 0 & 0 & e_0 & \cdots & e_{p-5} & e_{p-4} & e_{p-3} & e_{p-2} & e_{p-1} & \ddots & 0 & x^{p-5}E_{p-1} \\ 0 & e_0 & e_1 & \cdots & e_{p-4} & e_{p-3} & e_{p-2} & e_{p-1} & 0 & \cdots & 0 & x^{p-4}E_{p-1} \\ e_0 & e_1 & e_2 & \cdots & e_{p-3} & e_{p-2} & e_{p-1} & 0 & 0 & \cdots & 0 & x^{p-3}E_{p-1} \end{pmatrix}.$$

Observe that, since the value of x used in the rational method is the root of E_1 , for that value of x, det E = 0, *i.e.*, E is singular.

 $^{^{1}}$ While the rest of the method is a straightforward translation, this step bears some explanations; its description in [Fan92] is

De ces deux égalitez, ou prifes féparément, ou comparées enfemble felon la methode des problèmes plus que déterminez tirez en une valeur d'x rationelle, ou fimplement d'un degré commode.

It is assumed that the reader is familiar with this "comparison according to the method of more-thandetermined problems". While the application of the root-finding method is described in painstaking detail in [Fan33], which outlines the treatment of overdetermined problems, it is perhaps this remark from [Fan97, p. 494] which lays it out most clearly:

Il n'y a rien de nouveau à remarquer fur les Problemes plus que déterminez du quatriéme degré. La Regle générale est d'égaler tout à zero, & de diviser la plus haute équation par la moins élevée, ou l'également élevée l'une par l'autre, continuellement jusques à ce que l'on trouve le reste ou le diviseur le plus simple.

Lemma (Left as an exercise to the reviewer). The matrix E_1 is singular if and only if

$$\mathbf{C} \coloneqq \begin{pmatrix} x - \frac{1}{2}a & c_0 & & & \\ -1 & c_1 & c_0 & & & \\ 0 & c_2 & & \ddots & \\ \vdots & \vdots & \ddots & c_0 \\ 0 & c_{p-1} & \cdots & c_2 & c_1 \end{pmatrix}$$

is singular, where $c_0 := 1$.

Proof. Observe that:

— since $\det \mathbf{E}_1$ is a polynomial of degree 1, all terms divisible by x^2 must cancel out in the Laplace expansion of that determinant on the last column, the determinant is equal to

$$\pm \delta_1 x E_p \mp \delta_2 E_p \pm \delta_3 E_{p-1} \mp \delta_4 x E_{p-1}$$
,

where the δ_i are determinants of real matrices;

 by the same reasoning, only the linear and constant terms of the polynomials remain in the above expression, which simplifies to

$$\pm \delta_1 d_p x \mp \delta_2 (d_{p-1}x+d_p) \pm \delta_3 (e_{p-2}x+e_{p-1}) \mp \delta_4 e_{p-1}x;$$

- $E_1 - E_2 = S_1 - S_2$, which, by Lagny's theoreme fondamental [Fan92, p. 17], is $\left(x - \frac{1}{2}a\right)^p$.

The proof is a calculation.

The theorem follows from the lemma and theorem 4.4.2 from [Hou70, p. 169]: the iterate (3) corresponds to Householder's (14) with $g \equiv 1$; for that value of g, theorem 4.4.2 states that (14) is equivalent to (12) from the same page, which, substituting the iterate $a \mapsto x + \frac{1}{2}a$, is det C = 0. By the lemma, this is equivalent the definition of Lagny's rational method.

Names

As seen in the proof of the theorem, the iterate (3) was described by Householder for an arbitrary analytic functions f in [Hou70, p. 169] (equation (14), wherein one should take $g \equiv 1$; see also [SG01] which explicitly gives that form).

For p=2 and f an arbitrary polynomial, (3) is Newton's method, presented by Wallis in [Wal85, p. 338].

For p=3 and f an arbitrary polynomial, it is Halley's rational method, given in [Hal94, pp. 142–143] in an effort to generalize Lagny's (2). It is usually simply known as Halley's method, as the irrational method (which likewise generalizes Lagny's

Has Regulas, cum nondum librum videram, ab amico communicatas habui

and it appears that said friend communicated only the formulæ for the cube and fifth root, as opposed to the general method and its proof, as Halley writes

[...] D. de Lagney [...] qui cum totus fere fit in eliciendis Potestatum purarum radicibus, præfertim Cubicâ, pauca tantum eaque perplexa nec fatis demonstrata de affectarum radicum extractione subjungit.

or, about Lagny's irrational method for the fifth root,

Author autem nullibi inveniendi methodum ejufve demonstrationem concedit, etiamsi maxime desiderari videatur [...].

Being unaware of this generality, Halley sets out to generalize (1) and (2) to arbitrary polynomials, and does so by keeping the order constant.

²Lagny's method is general, in that an iterate is given for any polynomial, albeit one whose order changes with the degree. However, while he refers to its results—and even corrects a misprint therein—, Halley did not have access to a copy of [Fan92],

irrational method for p = 3, while retaining constant order as the degree changes) has comparatively fallen into obscurity; see [ST95].

Considering that a method remains the same when generalized from arbitrary polynomials to arbitrary analytic functions, we call the iterate (3)

- Newton's method when p = 2, for arbitrary f;
- Lagny's rational method when p > 2 and f is a polynomial of degree p;
- Halley's (rational) method when p = 3 and f is not a polynomial of degree 3;
- the Lagny-Householder method otherwise.

Note that we avoid the name "Householder's method" in this last case, as it is often used to refer to a different third order iterate instead, see TODO CITATION.

Computing a real cube root

We now turn to the computation in numerics/cbrt.cpp.

Overview

The general approach to compute the cube root of y > 0 is the same as the one described in [KBo1]:

- 1. integer arithmetic is used to get a an initial quick approximation q of $\sqrt[3]{y}$;
- 2. a root finding method is used to improve that that to an approximation ξ with a third of the precision;
- 3. ξ is rounded to a third of the precision, resulting in the rounded approximation x whose cube x^3 can be computed exactly;
- 4. a single high order iterate of a root finding method is used to get the final result

Notation

We define the fractional part as frac $a := a - \lfloor a \rfloor \in [0, 1[$, regardless of the sign of a.

The quantities $p \in \mathbb{N}$ (precision in bits) and $bias \in \mathbb{N}$ are as defined in IEEE 754-2008.

We use capital letters fixed-point numbers involved in the computation, and A > 0 for the normal floating-point number a > 0 reinterpreted as a binary fixed-point number with t bits after the binary point³,

$$A := bias + \lfloor \log_2 a \rfloor + \operatorname{frac}(2^{-\lfloor \log_2 a \rfloor}a)$$
$$= bias + \lfloor \log_2 a \rfloor + 2^{-\lfloor \log_2 a \rfloor}a - 1,$$

and vice versa,

$$a := 2^{\lfloor A \rfloor - bias} (1 + \operatorname{frac} A).$$

This corresponds to [KBo1]'s B + K + F.

For both fixed- and floating-point numbers, given $\alpha \in \mathbb{R}$, we write $[\![\alpha]\!]$ for the nearest representable number (rounding ties to even). For fixed-point numbers, we write $[\![\alpha]\!]_0$ for directed rounding towards 0 to the fixed-point precision (as in division implemented with integer division).

Except in the section on rescaling, the input y and all intervening floating-point numbers are taken to be normal; the rescaling performed to avoid overflows also avoids subnormals.

 $^{^{3}}$ The implementation uses integers (obtained by multiplying the fixed-point numbers by 2^{p-1}). For consistency with [KBo1] we work with fixed-point numbers here. Since we do not multiply fixed point numbers together, the expressions are unchanged.

1 Quick approximation

The quick approximation q is computed using fixed-point arithmetic as

$$Q \coloneqq C + \left[\left[\frac{Y}{3} \right] \right]_0,$$

where the fixed-point constant C is defined as⁴

$$C := \left[\frac{2 \operatorname{bias} - \gamma}{3} \right]$$

for some $\nu \in \mathbb{R}$

Let $\varepsilon := \frac{q}{\sqrt[3]{y}} - 1$, so that $\sqrt[3]{y}(1 + \varepsilon) = q$; the relative error of q as an approximation of $\sqrt[3]{y}$ is $|\varepsilon|$. Considering Y, Q, q, and ε as functions of y, we have

$$Y(8y) = Y(y) + 3,$$

$$Q(8y) = Q(y) + 1,$$

$$q(8y) = 2q(y),$$

$$\varepsilon(8y) = \varepsilon(y),$$

so that the properties of ε need only be studied on some interval of the form $[\eta, 8\eta[$. Pick $\eta := 2^{|\gamma|}$, and $y \in [\eta, 8\eta[= [2^{|\gamma|}, 2^{|\gamma|+3}[$, so that $\log_2 y \in [|\gamma|, |\gamma| + 3[$. Let $k := [\log_2 y] - |\gamma|$; note that $k \in \{0, 1, 2\}$. Let $f := \operatorname{frac}(2^{-|\log_2 y|}y) \in [0, 1[$. Up to at most 1.5 units in the last place from rounding,

$$\begin{split} Q &\approx Q' \coloneqq bias + \frac{\lfloor \log_2 y \rfloor}{3} + \frac{\operatorname{frac}(2^{-\lfloor \log_2 y \rfloor} y) - \gamma}{3}, \\ &= bias + \frac{\lfloor \gamma \rfloor + k}{3} + \frac{f - \gamma}{3}, \\ &= bias + \frac{k + f - \operatorname{frac} \gamma}{3}. \end{split}$$

Since $k \in [0, 2]$, the numerator $k + f - \text{frac } \gamma$ lies in]-1,3[. Further, it is negative only if k = 0, so that

$$[Q'] = \begin{cases} bias - 1 & \text{if } k = 0 \text{ and } \operatorname{frac} \gamma > \operatorname{frac}(2^{-|\gamma|} \gamma), \\ bias & \text{otherwise,} \end{cases}$$
 and
$$\operatorname{frac} Q' = \begin{cases} 1 + \frac{f - \operatorname{frac} \gamma}{3} & \text{if } k = 0 \text{ and } \operatorname{frac} \gamma > f, \\ \frac{k + f - \operatorname{frac} \gamma}{3} & \text{otherwise.} \end{cases}$$

Accordingly, for the quick approximation q, we have, again up to at most 1.5 units in the last place,

$$q \approx q' = \begin{cases} 1 + \frac{f - \operatorname{frac} \gamma}{6} & \text{if } k = 0 \text{ and } \operatorname{frac} \gamma > f, \\ 1 + \frac{k + f - \operatorname{frac} \gamma}{3} & \text{otherwise,} \end{cases}$$

With $\sqrt[3]{y} = 2^{\frac{|y|+k}{3}} \sqrt[3]{1+f}$, we can define

$$\varepsilon' \coloneqq \frac{q'}{\sqrt[3]{y}} - 1,$$

which we can express piecewise as a function of f and k. This gives us a bound on the relative error,

$$|\varepsilon| \le |\varepsilon'| + 1.5 \cdot 2^{p-1} (1 + |\varepsilon'|).$$

The values $\gamma = 0.1009678$ and $\varepsilon < 3.2\%$ from [KBo1] may be recovered by choosing γ minimizing the maximum of $|\varepsilon'|$ over $\gamma \in [\eta, 8\eta[$, or equivalently.

$$\gamma_{Kahan} \coloneqq \underset{\gamma \in \mathbb{R}}{\operatorname{argmin}} \max_{y \in [\eta, 8\eta[} |\varepsilon'| = \underset{\gamma \in \mathbb{R}}{\operatorname{argmin}} \max_{(f, k)} |\varepsilon'|$$

⁴Note that there is a typo in the corresponding expression C := (B - 0.1009678)/3 in [KBo1]; a factor of 2 is missing on the bias term.

where the maximum is taken over $(f, k) \in [0, \operatorname{frac} \gamma[\times \{0\} \cup [0, 1[\times \{1, 2\}, 1]])]$

$$= \underset{\gamma \in \mathbb{R}}{\operatorname{argmin}} \max_{(f,k) \in \mathcal{E} \cup \mathcal{L}} |\varepsilon'|,$$

where $\mathcal{E} \coloneqq \{(\operatorname{frac} \gamma, 0)\} \cup \{(0, k) \mid k \in \{0, 1, 2\}\}$ is the set of the endpoints of the intervals whereon q' is piecewise affine, and $\mathcal{L} \coloneqq \left\{ \left(\frac{k - \operatorname{frac} \gamma}{2}, k \right) \mid k \in \{1, 2\} \right\}$ are the local extrema.

The values are more precisely⁵

 $\gamma_{Kahan} \approx 0.10096\,78121\,55802\,88786\,36993\,42643\,55358\,06489\,88235\,75289$ with

 $\max_{y} |\varepsilon'| \approx 0.03155\,46327\,73624\,80606\,11789\,73328\,17135\,58940\,02093\,40816,$

leading to $C_{Kahan} = {}_{16}2A9F76253119\,D328 \cdot 2^{-52}$ for IEEE 754-2008 binary64. However, as we will see in the next section, this value does not optimize the final error, so it is not the one that we use.

2 Getting to a third of the precision

We use a single iterate of Lagny's rational method to compute ξ ,

$$\xi := \left\lVert q - \left\lceil \frac{\llbracket (\llbracket \llbracket q^2 \rrbracket q \rrbracket - y) q \rrbracket}{\llbracket 2 \llbracket \llbracket q^2 \rrbracket q \rrbracket + y \rrbracket} \right\rceil \right\rceil \right\rceil.$$

Note that the subtraction in the numerator is exact by Sterbenz's lemma. Let $\Delta := \frac{\xi}{3\sqrt{\nu}} - 1$ and

$$\xi' = q' - \frac{({q'}^3 - y)q'}{2{q'}^3 + y}.$$

We have, up to rounding errors (TODO: bound those),

$$\Delta \approx \Delta' \coloneqq \frac{\xi'}{\sqrt[3]{\nu}} - 1.$$

With $q' = \sqrt[3]{y}(1 + \varepsilon')$, we can express Δ' using the transformation of the relative error error by one step of Lagny's rational method on the cube root,

$$\Delta' = \frac{2{\varepsilon'}^3 + {\varepsilon'}^4}{3 + 6{\varepsilon'} + 6{\varepsilon'}^2 + 2{\varepsilon'}^3}.$$

If q' is computed using $\gamma = \gamma_{Kahan}$, we get

$$\max_{\nu} |\Delta'| \approx 0.00002196,$$

$$\log_2 \max_{y} |\Delta'| \approx -15.47.$$

However, γ_{Kahan} , which minimizes $\max_{\gamma} |\varepsilon|$, does not minimize $\max_{\gamma} |\Delta'|$. This is because while Δ' is monotonic as a function of ε' , it is not odd: positive errors are reduced more than negative errors are, so that the minimum is attained for a different value of γ . Specifically, we have

$$\gamma_{L} \coloneqq \underset{\gamma \in \mathbb{R}}{\operatorname{argmin}} \max_{y} |\Delta'|$$

 $\approx 0.09918746152985599525661492076131234347202306792759$

with

 $\max_{y} |\varepsilon'| \approx 0.03103\,20521\,29929\,93577\,08166\,75859\,02139\,33719\,41389\,93269,$

but

 $\max_{y} |\Delta'| \approx 0.00002\,08686\,35536\,39593\,48770\,92008\,39844\,10254\,14831\,61229.$

The corresponding fixed-point constant is $C_L := {}_{16}2A9F7893782DA1CE \cdot 2^{-52}$ for binary 64.

⁵These may be computed formally, but the expressions are unwieldy.

References

- [Fan33] T. Fantet de Lagny. "Analyse Générale, ou Méthodes nouvelles pour résoudre les Problèmes de tous les Genres & de tous les Degrez à l'infini". In: Recueil des Mémoires de l'Académie Royale des Sciences depuis 1666 jusqu'à 1699. Ed. by C. Richer. Vol. XI. Par la compagnie des libraires, 1733. eprint: https://books.google.fr/books?id=KwP-kH6gmlEC.
- [Fan91a] T. Fantet de Lagny. "Nouvelle methode de Mr. T. F. de Lagny pour l'approximation des Racines cubiques". In: Le Journal des sçavans 1691.17 (14th May 1691), pp. 200-203. eprint: https://gallica.bnf.fr/ark:/12148/bpt6k56538h/f202.double.
- [Fan91b] T. Fantet de Lagny. Méthode nouvelle, infiniment générale et infiniment abrégée, Pour l'Extraction des Racines quarrées, cubiques, &c. & pour l'Approximation des mêmes Racines à l'infini dans toutes sortes d'égalitez. Proposée à examiner aux Mathématiciens de l'Europe. De l'Imprimerie d'Antoine Lambin, ruë S. Jacques, au Miroir, 1691.

 eprint: https://gallica.bnf.fr/ark:/12148/bpt6k1039787.
- [Fan92] T. Fantet de Lagny. Methodes nouvelles et abbregées pour l'extraction et l'approximation des racines. Et pour resoudre par le cercle et la ligne droite, plusieurs problèmes solides & sursolides ; comme la duplication du cube, l'invention de deux & de quatre moyennes proportionnelles, &c. dans toute la précision possible, & d'une maniere praticable. Avec une dissertation sur les methodes d'arithmetique & d'analyse ; où l'on établit des principes generaux pour en juger. De l'Imprimerie de Jean Cusson, ruë saint Jacques, à l'Image de saint Jean Baptiste, 1692.

 eprint: https://nubis.univ-paris1.fr/ark:/15733/3415.
- [Fan97] T. Fantet de Lagny. Nouveaux elemens d'arithmetique et d'algebre, ou introduction aux mathematiques. Chez Jean Jombert, prés des Augustins, à l'Image Nôtre-Dame, 1697.

 eprint: https://books.google.fr/books?id=IbTtzq_fixAC.
- [Halo9] E. Halley. "A new, exact, and easy Method of finding the Roots of any Equations generally, and that without any previous Reduction". In: *The Philosophical Transactions of the Royal Society of London, from their commencement, in 1665, to the year 1800; Abridged, with notes and biographic illustrations.* Ed. by C. Hutton, G. Shaw and R. Pearson. Vol. III from 1683 to 1694. Translated from the Latin [Hal94]. 1809, pp. 640–649.
- [Hal94] E. Halley. "Methodus Nova Accurata & Facilis Inveniendi Radices Æquationum quarumcumque generaliter, sine prævia Reductione". In: *Philosophical Transactions of the Royal Society* 18.210 (May 1694), pp. 136–148. DOI: 10.1098/rst1.1694.0029. English translation: [Halo9].
- [Hou68] A. S. Householder. "Bigradients and the Problem of Routh and Hurwity". In: SIAM Review 10.1 (Jan. 1968), pp. 56–66.
 DOI: 10.1137/1010003.
- [Hou70] A. S. Householder. *The Numerical Treatment of a Single Nonlinear Equation*. International Series in Pure and Applied Mathematics. McGraw-Hill, 1970.
- [KBo1] W. Kahan and D. Bindel. "Computing a Real Cube Root". 2001 retypesetting by Bindel of a purported 1991 version by Kahan, at https://csclub.uwaterloo.ca/~pbarfuss/qbrt.pdf. 21st Apr. 2001.
- [SGo1] P. Sebah and X. Gourdon. "Newton's method and high order iterations". In: *Numbers, constants and computation*. 3rd Oct. 2001. eprint: http://numbers.computation.free.fr/Constants/Algorithms/newton.html.
- [ST95] T. R. Scavo and J. B. Thoo. "On the Geometry of Halley's Method". In: *The American Mathematical Monthly* 102.5 (May 1995), pp. 417–426. DOI: 10.2307/2975033.

[Wal85] J. Wallis. A Treatise of Algebra, both Historical and Practical. Shewing, the Original, Progress, and Advancement thereof, from time to time; and by what Steps it hath attained to the Heighth at which now it is. Richard Davis, 1685. eprint: https://books.google.fr/books?id=TXpmAAAACAAJ.