Ball arithmetic in MPC

Andreas Enge

CANARI project-team
INRIA Bordeaux
andreas.enge@inria.fr
http://enge.math.u-bordeaux.fr/

MPFR/MPC/MPFI/FLINT Workshop, Bordeaux, June 17–19, 2024
Complex ball arithmetic

- Used internally to replace hand calculations of error bounds
- As a tool to implement Taylor and Laurent series
- As a building block for polynomials, class polynomials, etc.
- Only four basic arithmetic operations and square root?
- Need for real ball arithmetic? interface with MPFI?
- Representation as rectangles? as balls?
Dagstuhl 2018: New number type to implement

Complex ball arithmetic
- Used internally to replace hand calculations of error bounds
- As a tool to implement Taylor and Laurent series
- As a building block for polynomials, class polynomials, etc.
- Only four basic arithmetic operations and square root?
- Need for real ball arithmetic? interface with M P F I?
- Representation as rectangles? as balls?

Release 1.3.0 “Ipomoea batatas”, December 2022:
- Ball arithmetic (marked experimental)
- New function mpc_agm
- New function mpc_eta_fund
If any of $x_1, y_1, x_2$ or $y_2$ equals 0, then the algorithm has either finished in the second step, or the corresponding norm is computed exactly already at precision $2p < p'$, a contradiction. So the case of interest is that these four input values are non-zero. Then write $z_k = \sqrt{(x_k^2 + y_k^2)}$ with integers $x_k^2$ and $y_k^2$ satisfying $2^{-p} < x_k^2, y_k^2 < 2^p$, and furthermore $d_k \geq 0$ since $y_k \geq x_k$. We have $m_k = 2^{p - p'} \cdot (m_k)$ with the integer $m_k = (x_k^2 + y_k^2) / 2$. If any of the exponent differences satisfies $d_k < 0$, then $m_k < 2^p \ll 2^{2p}$, and $m_k$ is computed exactly at precision $p'$, a contradiction.

So $d_k > p$. The integer $m_k$, read from the least to the most significant bits, consists of $(x_k^2)^p$ encoded with $2p$ bits (with potentially a leading bit 0), followed by $2d_k - 2p \geq 2$ bits 0, followed by $(y_k^2)^p$ encoded with $2p$ bits (with potentially one leading bit 0). So the $2p$ most significant bits of $m_k$, excluding leading bits 0, have the following shape: if $y_k^2 > \sqrt{2} 2^{-p}$, they encode exactly $(y_k^2)^p$. If $y_k^2 < \sqrt{2} 2^{-p}$, the $2p - 1$ leading bits encode $(y_k^2)^p$, and they are followed by a digit 0, so the $2p$ leading bits encode $2(y_k^2)^p$.

Since $n_1 = n_2$, in particular their leading $2p$ bits coincide; so either $(y_k^2)^p = (y_k^2)^{2p}$, $(y_k^2)^p = 2(y_k^2)^p$ or $(2(y_k^2)^p) = (y_k^2)^{2p}$, where the last two cases are impossible for integers.

Comparing the exponents of the $m_k$ yields $c_1 + d_2 = c_2 + d_2$, so $y_2 = y_2$, a contradiction since the algorithm has proceeded beyond the second step.

3.10 npc_AGM

**Definition.** Let $a$, $b$ be non-zero complex numbers. Define sequences of arithmetic mean ($\lambda_a$) and geometric mean ($\lambda_b$) by $a_0 = a$, $b_0 = b$, $a_{n+1} = a_n \cdot b_n$ and $b_{n+1} = a_n / b_n$. At each step, there is a choice of sign for the square root. If $a_n$ and $b_n$ form an (unoriented) angle different from 0 and $\pi$, then they define a two-dimensional pointed cone in the complex plane. Notice that $a_{n+1}$ lies in this cone. Following [5] we call right the choice that makes also $b_{n+1}$ lie in the cone, and following [5] we call the resulting sequence optimal. (An equivalent definition is that $|a_{n+1} - b_{n+1}| \leq |a_n - b_n|$. There is a common limit of the sequences, the arithmetic-geometric mean ($\lambda_a$, $\lambda_b$).

It is immediate that AGM is symmetric, that is, $\text{AGM}(a, b) = \text{AGM}(b, a)$, and homogeneous, that is, $\text{AGM}(\alpha a, \lambda) = \lambda \text{AGM}(a, b)$ for any non-zero complex number $\lambda$.

So we may assume that $|a| \geq |b|$, and $\text{AGM}(a, b) = a \cdot \text{AGM}(a_0, b_0)$ with $a_0 = a$, $b_0 = b$, $a_{n+1} = a_n / b_n$ and $b_{n+1} = a_n \cdot b_n$.

We need to examine the corner cases. If one or both of $a$ and $b$ are zero, all geometric means are zero, and $\text{AGM}(a, b) = 0$. If the absolute value of $a$ and $b$ is 0, then $b_0$ is a positive real number, and $\text{AGM}(1, b_0)$ may be computed with $\text{erf}$. If the absolute value of $a$ and $b$ is 1, then $b_0$ is in $[-1, 0)$. The arithmetic mean of 1 and 1 is zero, so $\text{AGM}(1, 1) = 0$. If $b_0 > 1$, we take the first geometric mean with a positive imaginary part, so that also $3(\text{AGM}(1, b_0))$ will be positive. Notice that $3(\text{AGM}(1, b_0))$ has the same sign as $3(b_0)$ unless $b_0$ is real, so this choice determines our branch cut for AGM.

So in the following, we analyse the computation of $\text{AGM}(1, b_0)$ with $b_0 = b_0$ for $b_0$ in the unit disk centered at the origin (except $-1$ and 1), where the real and imaginary parts of $b_0$ are rounded towards 0, which ensures $|\text{Re}(b_0)| < 1$ and $|\text{Im}(b_0)| \leq 1$ with absolute errors of the real and imaginary parts at most 1 ulp. In the following, relative errors will be most convenient to work with; by Proposition 10 we have $\text{reler}(b_0) < 2^{-p}$, where $p \geq 2$ is the working precision.

**Warm-up — a note on angle 0.** As said, when the angle between $a$ and $b$ is 0, which is immediately detected from $3(b_0) = 0$ (computed at any precision), then $\text{AGM}(a, b) = a \cdot \text{AGM}(1, b_0)$ with a real number $0 < b_0 < 1$. We need to consider the error induced by computing $3(b_0) = 3(\text{AGM}(1, b_0))$ instead.

Recall that $b_0 = (1 + \varepsilon b_0) 2^{-p}$ with $-3 \leq \varepsilon \leq 3$. Since for positive real numbers each step of the AGM is increasing in each of the two arguments, so is the AGM itself, and we have

$$\text{AGM}(a, b) = \text{AGM} \left( \left(1 + (1 + \varepsilon) b_0\right) \right) \leq \text{AGM} \left(1 + (1 + \varepsilon) b_0\right) \leq \{1 + \varepsilon\} \text{AGM} \left(1, b_0\right)\right.$$  

By the same kind of argument

$$\text{AGM}(1, b_0) = (1 - \varepsilon) \text{AGM} \left(1, b_0\right).$$

So the relative error of at most $\varepsilon$ in the input $b_0$ is preserved by the AGM.

By Proposition 7 applied to non-representable numbers and Proposition 3 this relative error translates into an absolute error satisfying

$$|\text{AGM}(1, b_0) - \text{AGM} \left(1, b_0\right)| \leq 2 \cdot 2^{p - 1} \cdot \text{AGM}(1, b_0) - \varepsilon < 2 \cdot 2^{p - 1} \cdot \text{AGM}(1, b_0) - \varepsilon$$

of at most 2 ulp of the rounded value, and the final rounding of the $\text{AGM} (\cdot, \cdot)$ function leads to a total error bounded by 3 ulp.

We multiply this value by the exact $\varepsilon$, applying (2) with $k_1 \sim 3$ and $k_2 = 0$ and taking the final rounding into account leads to an error of at most 7 ulp for the real and for the imaginary parts of the complex AGM.

The first iteration — entering a quadrant. If $\text{Re}(b_0) < 0$, then significant cancellation may occur for the arithmetic mean in the first iteration, which thus needs to be analysed separately.

From now on, we use arbitrary rounding modes and apply Proposition 11 with $\varepsilon = 1$.

We let $b_1 = \sqrt{b_0}$ and $b_2 = b_0 / (\sqrt{b_0})$ with

$$\text{reler}(b_0) \leq 2^{-p - 1} + (1 + 2^{-p}) 2^{-p} \leq (1 + 2^{-p}) 2^{-p}$$

by (18) (where we use $\varepsilon = 2$ since $2^2 \leq 2^p \leq 2^1$, $c_1$ being the relative error on $b_0$) and Proposition 11, and where we have bounded $2 + 2^{-p} \leq 2.5$ by $(1 + 2^{-p}) \approx 2.83$. We let $a_1 = 1/2 + b_1/2$ and $a_2 = b_1/2 - 1/2$. The imaginary part of $a_2$ has an error of at most 1 ulp, and the same holds for the real part if $\text{Re}(b_0) = 0$ or equivalently if $\text{Re}(b_0) = 0$, the real part of $a_1$ has an absolute error bounded by

$$\max \left\{2, 2 \cdot 2^{p \text{opt}(\text{reler}(b_0)) - 1}\right\} \text{ulp}(\text{reler}(a_1)).$$

31
Indeed, let \( x \) be the real part of \( \tilde{b}_0 \), and \( y \) the real part of \( \tilde{a}_1 \), we have \( y = \circ\left(\frac{1}{2} + \frac{x}{2}\right) \).

Remember that \(-1 < x < 1\). If \(-1/2 < x < 1/2\) and \( y > 1/4 \), and \( \text{Exp}(y) \geq \text{Exp}(x/2) \), and from (1.3.1) the error on \( y \) is at most \( 2\uparrow n \) (one from the error on \( x/2 \), and one from the addition). If on the other hand \(-1 < x < -1/2\), then \( 1/2 + x/2 \) is exact by Sterbenz’s lemma, and the only error comes from that on \( x/2 \), which by (1.3.1) is bounded above by \( 2^{2\exp(x/2)} 2^\text{quant}(x/2) \).

Since \(-1/2 < x/2 < -1/4\), we have \( \text{Exp}(x/2) = -1 \) and the above result follows. This bound also holds when \( \Re(b) = 0 \). So by Proposition 10,

\[
\text{rele}(\tilde{a}_1) \leq \max\left\{2, 2^{\text{Exp}(\Im(b))} \right\} 2^{1-p}.
\]

If \( \Re(b) \geq 0 \), then \( \text{Exp}(\Re(a)) \geq 0 \), and we obtain a bound that is similar to the one above for \( \text{rele}(\tilde{b}_1) \). If \( b_0 \) approaches \(-1\), the relative error in \( \tilde{a}_1 \) becomes arbitrarily bad, as \( \tilde{a}_1 \) becomes arbitrarily small.

Letting

\[
k_1 = \max\left\{3, -2\text{Exp}(\Re(\tilde{a}_1)) - 2\right\}
\]

we obtain an upper bound of

\[
\text{rele}(\tilde{a}_1), \text{rele}(\tilde{b}_1) \leq \left(\sqrt{2}\right)^{k_1} 2^{1-p}
\]

on the loss of precision in the first iteration.

Notice that, independently of the rounding mode, \( \tilde{a}_1 \) and \( \tilde{b}_1 \) lie in the same complex quadrant of numbers having non-negative real part and an imaginary part of the same sign as that of \( b_0 \) (or of positive imaginary part if \( b_0 \) is real). During the remainder of the algorithm, we will not leave this quadrant and thus not see any more cancellation in the arithmetic mean.

The idea of the analysis. Let us first give the basic idea of the following, rather technical analysis. Assume a target precision of \( N \) bits, that is, a target relative error of about \( 2^{-N} \). If \( \alpha_0 \) and \( \beta_0 \) are of the same order of magnitude, the AGM iteration converges quadratically, that is, the number of correct digits doubles in each step, and we need about \( \log_2 N \) iterations. Unfortunately, when \( \alpha_0 \) and \( \beta_0 \) are of different orders of magnitude, we have slower convergence. To illustrate this, consider \( \alpha_1 - 1 = \beta_1 = 2^{-4} \), during the first iterations, \( \alpha_n \approx 2^{-n} \) and \( \beta_n \approx 2^{-2n} \). So we need to increase the number of iterations by roughly \( \log_2 \) of the absolute value of the exponent of \( \beta_0/\alpha_0 \): the precise bound \( B(N, \beta_0, \tilde{a}_1) \) on the number of iterations is given in (36). Moreover, when \( \Re(\tilde{a}_1) < 0 \), the situation of very different exponents in \( a \) and \( b \) may occur after one iteration through cancellation as explained above.

Unlike Newton iterations, AGM iterations are not auto-correcting, due to rounding errors, we lose a constant number of bits per iteration; so to reach the desired precision of \( N \) bits, we need to carry out all computations at a working precision of \( p \in N + O\left(B(N, \beta_0, \tilde{a}_1)\right) \). The following discussion provides explicit bounds for all those quantities.

Rounding error propagation. Let \( a_0 = a_0 - \circ 1/a_0 \), \( \alpha_1 = a_0 \cdot \circ b_0 - 1 \), \( b_0 = \circ \sqrt{a_0} \). The computation of \( \tilde{a}_1 \) and \( b_1 \) and their error analysis have been given above. For \( n \geq 2 \), we compute the sequences

\[
\alpha_n = \circ \left(\frac{\alpha_{n-1} + b_{n-1}}{2}\right), \quad \beta_n = \circ \left(\frac{\beta_{n-1} - b_{n-1}}{2}\right), \quad b_n = \circ \left(\sqrt{\alpha_n}\right).
\]

Then one sees by induction that \( \tilde{a}_n \) and \( \tilde{b}_n \) lie in the same quadrant as \( \tilde{a}_1 \) and \( \tilde{b}_1 \) (or, for that matter, \( \alpha_1 \) and \( \beta_1 \)).

Let \( \alpha_n = \text{rele}(\tilde{a}_n), \gamma_n = \text{rele}(\tilde{a}_n) \) and \( \beta_n = \text{rele}(\tilde{b}_n) \).
By (17) and Proposition 11,

\[
\alpha_n \leq \sqrt{2} \max(\alpha_{n-1}, \beta_{n-1}) (1 + 2^{1-p}) + 2^{1-p} \tag{26}
\]

By (10) and Proposition 11,

\[
\gamma_n \leq \circ (\alpha_{n-1} + \beta_{n-1} + \circ (\alpha_{n-1} - \beta_{n-1})) (1 + 2^{1-p}) + 2^{1-p}. \tag{27}
\]

By (18) and Proposition 11,

\[
\beta_n \leq \frac{1}{\sqrt{2}} \gamma_n (1 + 2^{1-p}) + 2^{1-p} \text{ if } \gamma_n \leq \frac{1}{4}. \tag{28}
\]

Let \( \epsilon_n = \circ(\sqrt{2})^{n+1} - 1 \) \( r_1 \) for some integer \( r_1 \) such that \( \alpha_0, \beta_0 \leq r_12^{1-p} \). We may use \( r_1 = \circ(\sqrt{2})^{k_1} \) with \( k_1 \) as in (24), so that \( r_1 \leq \circ(\sqrt{2})^{k_1+1} \). We now show by induction
that $\alpha_n, \beta_n \leq r_0 2^{-p}$ if the number $n$ of iterations is not too large compared to the working precision $p$. For $n=1$, this follows from (25) and the definition of $r_1$.

As a preparation for the induction step and taking the shape of (26) to (28) into account, we carry out the following computation for $n \geq 2$, $p \geq 2$, $a_n, b_n \leq r_0 2^{-p}$, $\gamma \leq 2$ (we will only need $\gamma \in (\sqrt{2}, 2)$ later) and $0 \leq \delta \leq 1$ (we will only need $\delta \in (0,1)$):

$$R(n, \gamma, \delta) = (\gamma + 2^{-p} \gamma^2 (1 + 2^{-p})) + 1 + (1 + 2^{p-1} (\gamma + 2^{-p} \gamma^2 (1 + 2^{-p}))) r_{n-2} + 1 + 2^{-p} (\sqrt{\gamma} + 2^{p-1} \gamma^2).$$

So assuming $p \geq \frac{\ln 2 + 1}{\ln 3}$ we have

$$R(n, \gamma, \delta) \leq \frac{\gamma + \delta (\sqrt{\gamma})^2}{\sqrt{\gamma}} r_n + 2^{n/2} \frac{\gamma + \delta (\sqrt{\gamma})^2}{\sqrt{\gamma}} (\gamma_n - \sqrt{\gamma} r_{n-1}).$$

Therefore, we need bounds on $\sqrt{\gamma}$, $\gamma$ and on $a_n$ of iterations $b_n$ and $c_n$ instead of the correct values, we may wish to replace $b_n$ by $b_n$ and $a_n$ by $a_n$. (In fact the arguments will be quite delicate and switch between the different quantities.) The relative errors derived above on $b_n$ and $a_n$ of (21) and $\gamma_n$ of (23) with $p \geq \frac{\ln 2 + 1}{\ln 3}$ $5$ show that

$$|1 - 2^{p-1} b_n| \leq |b_n| \leq (1 + 2^{p-1} b_n)$$

and

$$|1 - 2^{-p} a_n| \leq |a_n| \leq (1 + 2^{-p} a_n).$$

Since $b_n = c_n$ with both parts rounded towards zero, we even have $b_n = c_n$. Altogether we have the (much coarser) following bounds:

$$|b_n| \leq |a_n| \leq \sqrt{\gamma} |b_n|$$

and

$$|1 - 2^{p-1} b_n| \leq |b_n| \leq (1 + 2^{p-1} b_n)$$

and

$$|1 - 2^{-p} a_n| \leq |a_n| \leq (1 + 2^{-p} a_n).$$

Mathematical error. We also need to estimate the error made by carrying out only a finite number of iterations. Let $\zeta$ satisfy $\Re(\zeta) > 0$ and $\zeta \neq 0, 1$, and consider the optimal AGM sequences $(a_n^\delta)$ and $(b_n^\delta)$ computed (with infinite precision) from $a_0^\delta = 1$ and $b_0^\delta = z$.

Let $N_0 \in \mathbb{N}$ and

$$n > B(N_0, z) := \max (1, \frac{\log \Re(z) + \log \Re(\zeta)}{\log(2N^2 + 2) + 2})$$

(we may assume $\log \Re(0) = 0$, but after one iteration, $\log B(N_0, z) > 0$).

We consider $z = b_0^\delta = b_0^\delta /\zeta$, so that by homogeneity, $a_n^\delta - a_n^\delta = b_n^\delta$ and $AGM(b_0^\delta, 1) = AGM(z, 1)$. Thus we need bounds on

$$|z| = \frac{|b_0^\delta|}{|a_0^\delta|} = \frac{|b_0^\delta|}{|a_0^\delta|} = |\zeta|.$$
The above bound $B'$ for the required number of iterations $n$ grows with $|\log_2 |z||$, so problematic situations may occur when $|z|$ is either very large or very small; the former may happen when $|b_0|$ is large and/or $|a_1|$ is small, the latter when $|b_0|$ is small and/or $|a_1|$ is large. Remember that in our setting we have the bounds

$$|b_0| \leq 1,$$

so that $|a_2| = \frac{|b_0| + 1}{2} \leq 1$.

This interesting situations can occur only when either $|b_0|$ is small or $|a_1|$ is small, that is, $\lambda$ is close to $-1$; and both cannot happen simultaneously. This leads to the following case distinction:

(a) Assume $\text{Exp}(b_0), \text{Exp}(\tilde{b}_0) \leq -1$.

By (31) this is equivalent to $\text{Exp}(b_0), \text{Exp}(\tilde{b}_0) \leq -1$, whence $\Re(b_0), \Im(b_0) < 1/2$ and

$$|b_0| \leq \sqrt{2}/2 < 1.$$

This implies $1 - \sqrt{2}/2 \leq 2|a_1| \leq 1 + \sqrt{2}/2$ and $1/8 \leq |a_1| \leq 1$ and we know $\sqrt{|a_1|} \geq \sqrt{\sqrt{2}}$ by (30). Collecting these upper and lower bounds, we obtain for $z = \sqrt{\sqrt{2}/a_1}$ that

$$\sqrt{|b_0|} \leq |z| < 8 \quad \text{and} \quad |\log_2 |z|| \leq \max \left(1, 1 - \frac{1}{2} \log_2 |\sqrt{a_1}|\right).$$

Using the estimate

$$|a_1| \geq \max \left(|\Re(b_0)|, |\Im(b_0)|\right) > 2^{\frac{1}{2} \max\left(\text{Exp}(b_0), \text{Exp}(\tilde{b}_0)\right) - 1},$$

we finally obtain

$$|\log_2 |z|| \leq \max \left(1, \frac{3}{2}\right) \left(\text{Exp}(b_0), \text{Exp}(\tilde{b}_0)\right) + \frac{1}{2},$$

(b) Assume $\text{Exp}(b_0) \leq -1$ and $\text{Exp}(\tilde{b}_0) \leq -2$.

By (32) the first condition implies $\text{Exp}(\tilde{a}_1) \leq -2$ or $|\Im(a_1)| < 1/4$. The second condition together with the first inequality of Proposition 3 implies that $\text{Exp}(b_0) < -2$, or $|\Re(b_0)| < 1/2$. So in fact $-1 < |b_0| < -1/2$, and then $-1 < \Re(b_0) < -1/2$ as well. This in turn implies $0 < |a_1| < 1/4$.

Putting these together, we obtain

$$\frac{1}{2} \leq |\Re(a_1)| \leq |b_0| or 1/\sqrt{2} \leq |\sqrt{a_1}|,$$

and we already know $|b_0| \leq 1$ or $|\sqrt{a_1}| \leq 1$ from our general setting and $|a_1| \geq |\tilde{a}_1|/\sqrt{2}$ by (30), whence

$$2 \leq |z| \leq \sqrt{2} \quad \text{and} \quad |\log_2 |z|| \leq -\log_2 \sqrt{a_1} + \frac{1}{2}.$$

Using the estimate

$$|\tilde{a}_1| \geq \max \left(|\Re(a_1)|, |\Im(a_1)|\right) > 2^{\max\left(\text{Exp}(a_1), \text{Exp}(\tilde{a_1})\right) - 1},$$

and (32) we finally obtain

$$|\log_2 |z|| \leq -\max\left(\text{Exp}(a_1), \text{Exp}(\tilde{a_1})\right) + 1 + \frac{3}{2}.$$

(c) In the remaining case, since we are not in (a), at least one of $\text{Exp}(b_0)$ and $\text{Exp}(\tilde{b}_0)$, or equivalently by (31) at least one of $\text{Exp}(b_0)$ and $\text{Exp}(\tilde{b}_0)$ is 0 or larger, so that

$$\frac{1}{2} \leq \max\left(|\Re(b_0)|, |\Re(\tilde{b}_0)|\right) \leq |b_0| \leq 1 \quad \text{and} \quad \frac{1}{2} \leq \sqrt{|b_0|} \leq 1.$$

If $\text{Exp}(\tilde{b}_0) > 0$, then $\text{Exp}(\tilde{a}_1) > -1$ by (32) and

$$|a_1| \geq |\tilde{a}_1| \geq 1/4.$$

Otherwise since we are not in (b), $\text{Exp}(\tilde{a}_1) \geq -1$ or $|\Re(a_1)| \geq 1/4$; as it is known to be positive in fact $\Re(a_1) \geq 1/4$. In precision at least 5, the value $1/4 - 31/32$ is representable and smaller than $1/4$ so that the value rounded to $\tilde{a}_1$ satisfies $1 + \Re(a_1)/2 > 31/128$ and $\Re(\tilde{a}_1) > -33/64$. In precision at least 5, the value $-34/64$ is representable and smaller than $-33/64$ so that the unrounded value satisfies $\Re(\tilde{a}_1) > -17/32$, which implies $|\Re(a_1)| > 15/64 > 1/8$ and

$$|a_1| \geq |\Re(a_1)| \geq 1/8.$$

We also know $|a_1| \leq 1$ in our general setting. Altogether

$$\frac{1}{\sqrt{2}} \leq |z| \leq 8 \quad \text{and} \quad |\log_2 |z|| \leq 3.$$
Algorithm for AGM

Letting $L(\tilde{b}_0, \tilde{a}_1)$ denote the above bound on $|\log_2 |z||$ depending on the exponents occurring in $\tilde{b}_0$ and $\tilde{a}_1$, and counting the additional first iteration to compute $\tilde{a}_1$ and $\tilde{b}_1$, not present in the above analysis, we fix a number of iterations $n$ such that $n \geq B(N, \tilde{b}_0, \tilde{a}_1)$ with
\[
B(N, \tilde{b}_0, \tilde{a}_1) = \max \left\{ 1, \left[ \log_2 L(\tilde{b}_0, \tilde{a}_1) \right] \right\} + \left[ \log_2 |N| + 4 \right] + 3.
\]

Then $\alpha_n = (1 + \phi) AGM(1, b_0)$ with $|\phi| \leq 2^{-N+2}$.

Total error and working precision. Combining with (29), we obtain for a sufficiently large precision $p$ and sufficiently many iterations $n$ that $AGM(1, b_0, \tilde{a}_1)$ with $|\phi| \leq 2^{-N+2}$, and so that
\[
|\phi| \leq \frac{|\phi| + |\phi|}{|N| - |\phi|} \leq \frac{1}{2 \left( 1 - 2^{-N} \right)} \left( 1 - 2^{-N} \right) + 2^{-N+2}
\]
for $N \geq 2$. So after $n = B(N, \tilde{b}_0, \tilde{a}_1)$ steps of the AGM iteration at a working precision of $p \geq N + \min\{100, N\}$ we obtain $z_n$ which approximates $AGM(1, b_0)$ with a relative error bounded by $2^{-N}$.

Finally, we let $z = AGM(a, b) = a AGM(1, b_0)$ and $\tilde{z} = \langle an \rangle$, where $n$ is known exactly. By (10) and Proposition 11, using that $N \geq 2$ and $k_1 \leq 3$ imply $n = B(N, \tilde{b}_0, \tilde{a}_1) \geq 7$ and $p \geq N + 8 \geq 10$, this leads to a relative error bounded by $2^{-N}$.

Summary. In our analysis, the working precision $p$ depends on
\[
k_1 = \max(3, 2 \exp(\hat{m}(\tilde{z})) - 2)
\]
of (24), which in turn depends not only on the input precision $\hat{m}$, but also on the working precision of the first AGM iteration. It is not enough to carry out this computation at arbitrarily low precision. Since $\hat{m}$ is computed as $\hat{m}/10$ or $\hat{m}/20$ depending on the respective sizes of the numbers and it is rounded, the computation of $\hat{m}(\tilde{z})$ requires double rounding, which may even lead to a wrong exponent if the precision is too low. Precisely, the exponent of $\hat{m}(\tilde{z})$ may only be wrong if $\hat{m}(\tilde{z})$ is so close to $-1$ that it is rounded towards zero to $-1$ plus 1 ulp, that is, $\hat{m}(\tilde{z}) = -(1 - 2^{-k})$. Then $\hat{m}(\tilde{z}) = 2^{-k}$ with $\exp(\hat{m}(\tilde{z})) = -p$ has lost all information on $\hat{m}(\tilde{z})$ and reflects only the rounding error. In all other cases a significant digit is retained and the exponent is correct. So $k_1$ may be computed by increasing the precision for this precomputation until $\exp(\hat{m}(\tilde{z})) > -p$.

Then we fix a desired accuracy $N$ (around the target precision plus a safety margin), compute $L(\tilde{b}_0, \tilde{a}_1)$ by (33), (34) or (35) and the number of iterations $n = B(N, \tilde{b}_0, \tilde{a}_1)$ by (36) (more often than not, this will result in $n = \left[ \log_2 |N| + 5 \right]$). Then the working precision is given by
\[
p = N + \left\lfloor \frac{\alpha_n + k_1 + 7}{2} \right\rfloor.
\]

Using Propositions 9 and 7, the complex relative error of $2^{-N}$ may be translated into an error expressed in ulp. With $\tilde{z} = \tilde{x} + i\tilde{y}$ the computed approximation of $z = AGM(a, b)$, let $k_0 = \max(\exp(\tilde{x}) - \exp(\tilde{x}) + 1, 0) + 1$, and $k_1 = \max(\exp(\tilde{y}) - \exp(\tilde{y}) + 1, 0) + 1$. Then we have $|\tilde{z}| \leq 2^{k_0 + k_1 + \tilde{z}_{ulp}(\tilde{z})}$ and $\tilde{z}_{ulp}(\tilde{z}) \leq 2^{k_1 + k_0 + \tilde{z}_{ulp}(\tilde{z})}$.

In practice, one should take this additional loss into account. If rounding fails after the first computation, nevertheless the value of $k_0$ and $k_1$ will most likely not change with a larger precision. So one should let $k' = \max(k_0, k_1)$, replace $N$ by $N + k'$ and adapt the number of iterations and the working precision accordingly.

The number of iterations is also slightly pessimistic in practice, in particular the additional constant in (36). So the computations may be stopped earlier if the numbers occurring in the AGM iterations do not change any more, since then additional iterations will fix the result.

4 Complex ball arithmetic

We propose a simple implementation of complex balls, which keep track of rounding errors over several operations. The originality of our implementation is that it uses relative complex errors as in (11.1.4).

A complex ball of type $mpcb_t$ is defined by a non-zero centre $c$ of type $mpc_t$ and a relative radius $r$ of type $mcr_t$, and it represents all complex numbers $z = c(1 + \theta)$ with $|\theta| \leq r$, or equivalently the closed circle with centre $c$ and radius $r[1]$. In the following, we use the notation $(c, r)$ for this complex ball.

The radius type represents the non-negative real half-axis from 0 to $\infty$, including this special infinite number. It is implemented internally as a non-negative floating point value with a signed 64 bit integer mantissa $m$, normalised to 31 bits, so that two mantissas may be multiplied without rounding. The sign is used to encode $-r = \infty$, a zero mantissa encodes 0, otherwise a mantissa is always positive. The exponent is encoded as a 64 bit integer $e$ such that (for finite radii) $r = m \cdot 2^e$ with $0 \leq m < 2^{31}$. In most applications a radius $r \geq 1$ will be meaningless, so that in practice we will almost always have $r \leq c$ or $e = -\infty$.

Mathematical functions are then understood to work on sets and to “round up”. They return a complex ball containing the set obtained by applying the function to every combination of arguments from the input balls. Reasonable efforts are made to return small balls, but there is no guarantee that the returned ball is minimal.

In any case, the centre of the resulting ball is obtained by applying the corresponding MPC function on the centres of the input balls with rounding to nearest. The analysis of §3 then provide upper bounds on the radius.

Compared to a representation decomposed along the real and imaginary parts, with separate relative or absolute errors, which leads to rectangles instead of circles, our representation simplifies multiplicative operations and makes additive operations more complicated. Determining branch cuts, which often depend on the decomposition of a complex number into real and imaginary parts, are probably also made more complicated. The biggest drawback is that intervals centred in 0 may not be represented at all. More generally, intervals containing 0 are also not meaningful: They correspond to balls
Algorithm for AGM using ball arithmetic

with \( r \geq 1 \), which means that even the most significant digit of the centre is uncertain.

### 4.1 Crossing the axes

\[ c = x + iy \]

To correctly evaluate functions at branch cuts, it may be useful to examine how complex balls are positioned with respect to the axis. As already mentioned above, a ball \((c, r)\) contains the origin if and only if \( r \geq 1 \).

For \( c = x + iy \), it crosses (or touches) the real axis if and only if it contains the point \( x \), which means that

\[
\| x - c \| \leq | r | \iff \| y \| \leq | r | \iff y^2 \leq r^2 (x^2 + y^2) \iff (1 - r^2) y^2 \leq r^2 x^2.
\]

When does a complex ball touch the real axis? This means that \((1 - r^2)y^2 = r^2 x^2\), which happens obviously when \( r = 0 \) and \( y = 0 \), so that the ball is a point located on the real axis, or when \( r = 1 \) and \( x = 0 \), so that the ball is centred on the imaginary axis and touches the origin. All other cases are actually impossible with machine-representable numbers. Assuming otherwise, recall that \( x, y \) and \( r \) are rational numbers with denominator a power of 2. If \( r \) is an integer, then it is either 1, which we already covered; or larger, and then the origin is contained in the interior of the ball, which must cross the real axis. So let \( r = \sqrt{a/b} \) with \( a \) an odd integer and \( b \geq 1 \). Then \( 4^b a^2 = 4^b (1 - r^2) = (2^b a^2 - 1)^2 \) is the square of an odd integer. But all odd squares are 1 modulo 4, whereas the left-hand side is 3 modulo 4, a contradiction.

Symmetrically, the complex ball \((x + iy, r)\) crosses (or touches) the imaginary axis if and only if

\[
(1 - r^2) x^2 \leq r^2 y^2.
\]

It touches the imaginary axis if and only if \( r > 0 \) and \( x = 0 \), so that the ball is a point on the imaginary axis, or \( r = 1 \) and \( y = 0 \), so that the ball is centred on the real axis and touches the origin.

The ball has a common point with the negative real axis (including the origin) if and only if either \( x \leq 0 \) and the ball has a common point with the real axis (since then \( x \) is such a common point), or \( x > 0 \) and the ball contains the origin.

### 4.2 mpqc-agm

Implementing the AGM (see §3.10) for complex balls would require to check whether the input crosses the negative real axis, where we have placed the branch cut (which is inherited from the branch cut of the complex square root). However if the input is a complex number which can be considered to be exact, then an implementation using complex balls can obtain a correctly rounded result with a greatly simplified analysis compared to §3.10.

In a first step, assuming that \( |a| \geq |b| \), we compute \( h_0 = h/a \) as a complex ball centred around \( h_0 \).

If \( 3(h_0 - 0) \leq 0 \), then the angle between \( a \) and \( b \) is 0 or \( \pi \). Regardless of the rounding direction, \( R(b) \) also has the same sign as \( R(h_0) \). If \( R(b) > 0 \), then the angle is 0 and the computation can be outsourced to a real AGM as described in §3.10. If \( R(h_0) < 0 \), then the angle is \( \pi \), and the complex ball containing \( h_0 \) crosses the negative real axis; the first step of the AGM with an implementation of \text{mpqc-agm} that respects the branch cut would end up with a ball containing \( \pm \sqrt{h_0} \cdot i \) and thus the origin, which is completely useless. We may, however, in this case use an implementation of the square root placing the branch cut differently and returning a ball centred at some approximation of \( \pm \sqrt{h_0} \cdot i \) and then continue with the AGM iterations.

After \( n \) iterations starting from 1 and a ball around \( h_0 \), we end up with balls \((a_n, r_n)\) and \((b_n, r_n)\) such that the exact values satisfy \( a_n = (1 + \varphi_b) a_n \) with \( |\varphi_b| \leq r_n \) and \( b_n = (1 + \varphi_a) b_n \) with \( |\varphi_a| \leq r_n \).

By [6, p.87] we have \( |\text{AGM}(1, h_0) - a_n| \leq |a_n - h_0| \). Plugging the expressions for \( a_n \) and \( b_n \) into this inequality yields

\[
|\text{AGM}(1, h_0) - (1 + \varphi_b) a_n| \leq |a_n - h_0| + |\varphi_a a_n| + |\varphi_b b_n|.
\]

The lower triangle inequality gives

\[
|\text{AGM}(1, h_0) - (1 + \varphi_b) a_n| \leq |a_n - h_0| + |\varphi_a a_n| + |\varphi_b b_n|,
\]

and putting these inequalities together we obtain

\[
|\text{AGM}(1, h_0) - a_n| \leq \left( \frac{|a_n - h_0|}{|\varphi_a|} + 2|\varphi_b| \right) |a_n| + |\varphi_a a_n| + |\varphi_b b_n|.
\]

Write \( h_0 = (1 + \varphi_b) a_n\) and \( r_{n+1} = |\varphi_a|; \) then we obtain

\[
|\text{AGM}(1, h_0) - a_n| \leq (r_{n+1} + 2r_{n+1}(1 + r_{n+1})|a_n|) \leq 2(r_{n+1} + r_{n+1})|a_n| \text{ if } r_{n+1} \leq 1.
\]

Otherwise said, \( AGM(1, h_0) \) is contained in the ball \((a_n, r_{n+1} + 2(r_{n+1} + r_{n+1}))\) and multiplying this with the ball \((a, b)\) we obtain a ball containing \(\text{AGM}(a, b)\). If this can be rounded to a unique MFC number with the desired rounding mode, then we have correctly computed \text{mpqc-agm}; otherwise we need to repeat the computations at a higher precision, and the exponent of the radius gives an indication on the necessary precision increase.

In practice convergence of the sequences of \( a_n \) and \( b_n \) is often such that \( a_n \approx b_n \) and thus \( r_n \approx 1 \). Otherwise the two generally differ by only 1 ulp, and a very coarse estimate of \( r_{n+1} \) as a power of 2

\[
r_{n+1} \leq 2^{\max\{\text{Exp}(\text{Re}(c_n)) - \text{Exp}(\text{Re}(c_n - C_n))\}, \text{Exp}(\text{Re}(C_n)) - 1\} - (\text{max}\{0, \text{Exp}(\text{Re}(c_n))\})} - 1\}
\]

is enough, where \( \text{Exp}(0) \) is considered as \(-\infty\).
Complex balls

Centre and radius as relative error

\[(c, r) = \{ z \in \mathbb{C} : |z - c| \leq r|c| \} = \{ z = c(1 + \vartheta) : |\vartheta| \leq r \}\]
Complex balls

Centre and radius as relative error

\[(c, r) = \{ z \in \mathbb{C} : |z - c| \leq r|c| \}\]

\[= \{ z = c(1 + \psi) : |\psi| \leq r \}\]

- Scaling is easy

\[s(c, r) \subseteq (sc, r) \text{ for } s \in \mathbb{R}\]

- Multiplication is easy

\[(c_1, r_1) + (c_2, r_2) \subseteq (c_1 c_2, r_1 + r_2 + r_1 r_2)\]

- Square root is easy

\[\sqrt{(c, r)} \subseteq (\sqrt{c}, r/2)\]

- Addition is more difficult

\[(c_1, r_1) + (c_2, r_2) \subseteq (c_1 + c_2, (|c_1| r_1 + |c_2| r_2)/|c_1 + c_2|)\]

0 is not representable.
typedef struct {
    mpc_t  c;
    mpcr_t r;
} mpcb_t;
typedef struct {
    mpc_t c;
    mpcr_t r;
} mpcb_t;

typedef struct {
    int64_t mant;
    int64_t exp;
} mpcr_t;
typedef struct {
    mpc_t c;
    mpcr_t r;
} mpcb_t;

typedef struct {
    int64_t mant;
    int64_t exp;
} mpcr_t;

- radius 0: mant = 0
- radius $\infty$: mant < 0
- 31 bit normalised mantissa: $2^{30} \leq \text{mant} < 2^{31}$
Functions on radii

Surprisingly many and quirky functions...
Results are normalised and rounded up (unless exception).

- **Predicates**
  - mpcr_inf_p
  - mpcr_zero_p
  - mpcr_lt_half_p
  - mpcr_cmp

- **Setters**
  - mpcr_set_inf
  - mpcr_set_zero
  - mpcr_set_one
  - mpcr_set
  - mpcr_set_ui64_2si64
  - mpcr_max

- **Output**
  - mpcr_out_str
Functions on radii

- Arithmetic
  - `mpcr_add`, `mpcr_mul`, ...
  - `mpcr_sub_rnd`
    Takes MPFR_RNDU, MPFR_RNDD.
  - `mpcr_c_abs_rnd`
    Used for error of addition

\[(c_1, r_1) + (c_2, r_2) \subseteq (c_1 + c_2, (|c_1|r_1 + |c_2|r_2)/|c_1 + c_2|)\]
Functions on radii

- **Arithmetic**
  - mpcr_add, mpcr_mul, ...
  - mpcr_sub_rnd
    Takes MPFR_RNDU, MPFR_RNDD.
  - mpcr_c_abs_rnd
    Used for error of addition
    \[(c_1, r_1) + (c_2, r_2) \subseteq (c_1 + c_2, (|c_1| r_1 + |c_2| r_2)/|c_1 + c_2|)\]
  - mpcr_add_rounding_error (r, p, rnd)
    Accounts for shift of centre by 1/2 ulp or 1 ulp depending on rnd.
    Adds \((1 + r)2^{-p}\) or twice this to \(r\).
    Called once at the end of each operation.
Principles of complex balls

1. \((c_1, r_1) \odot (c_2, r_2) \subseteq (c_1 \odot c_2, r)\)

2. One precision for real and imaginary part

3. initialised without precision: mpcb_init \((z)\), mpcb_clear \((z)\)

4. Precisions are tracked automatically.
   - \(z_1 \odot z_2\) gets minimum precision of \(z_1\) and \(z_2\).
   - Precision is not decreased when radius increases.
Setting complex balls

- `mpcb_set_inf (z)`
- `mpcb_set (z, z1)`

Challenges: Exact input and inputs with errors.
Setting complex balls

- mpcb_set_inf (z)
- mpcb_set (z, z1)

Challenges: Exact input and inputs with errors.

- mpcb_set_ui_ui (z, re, im, prec)
  Uses maximum of prec and sizeof (ulong).

- mpcb_set_c (z, c, prec, err_re, err_im)
  Assumes c has err_re and err_im half-ulp errors.
  ▶ If prec large and err_re and err_im = 0: exact, r = 0.
  ▶ Otherwise, r encodes err_re, err_im and rounding of c.
Computations with complex balls

- `mpcb_neg (z, z1)`
- `mpcb_add (z, z1, z2)`
- `mpcb_mul (z, z1, z2)`
- `mpcb_sqr (z, z1, z2)`
- `mpcb_pow_ui (z, z1, e)`
- `mpcb_sqrt (z, z1)`
- `mpcb_div (z, z1, z2)`
- `mpcb_div_2ui (z, z1, e)`
mpcb_round (c, z, rnd)
Rounds the centre of z to c (with its own precision).
Rounding complex balls

- `mpcb_round (c, z, rnd)`
  Rounds the centre of `z` to `c` (with its own precision).

- `mpcb_can_round (z, prec_re, prec_im, rnd)`
  `true`
  if rounding any complex (mathematical) number in `z` to a complex (floating point) number of precision `(prec_re, prec_im)` in direction `rnd` yields the same result and ternary return value.

Beware of infinite loops for exact results.

Andreas Enge
Ball arithmetic in MPC

Bordeaux 2024
Rounding complex balls

- `mpcb_round (c, z, rnd)`
  Rounds the centre of \( z \) to \( c \) (with its own precision).

- `mpcb_can_round (z, prec_re, prec_im, rnd)`
  
  true
  
  if rounding any complex (mathematical) number in \( z \) to
  a complex (floating point) number of precision (\( \text{prec\_re} \), \( \text{prec\_im} \))
  in direction \( \text{rnd} \)
  yields the same result and ternary return value.

- Beware of infinite loops for exact results.
“Normal” functions using balls

- mpc_agm
  Uses a priori error analysis.
  Tests compare with mpc_mpcb_agm.
“Normal” functions using balls

- **mpc_agm**
  Uses a priori error analysis.
  Tests compare with **mpc_mpcb_agm**.

- **mpc_eta_fund** \((\text{rop}, z, \text{rnd})\)

\[
q^{1/24} = \exp\left(\frac{2\pi iz}{24}\right)
\]
\[
q = \left(q^{1/24}\right)^{24}
\]
\[
\eta = q^{1/24} \left(1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \cdots\right)
\]

\(q^{1/24}\) is computed as **mpc** with an a priori error analysis, then handled with **mpcb_set_c**.

Andreas Enge

Ball arithmetic in MPC

Bordeaux 2024
What is next?

- Question the design choices.
- Handle 0?
  - Exact 0 is easily encoded, but needs case distinctions.
  - Balls around 0 need absolute radius encoding and more case distinctions.
- Use balls internally for series (special values of special functions)?
- Use balls in existing functions instead of error analysis?
- Implement functions on balls?