中 国 科 学
1986 年 3 月　　A 辑　　第 3 期

近似计算有效位数的增长不超过几何级数

洪 加 威
（北京计算机学院）

摘　要

假定我们要用加、减、乘、除开方等运算去计算任何一个实数或复数，并且假定每次运算都是绝对精确的.我们证明了：不论用什么方法，如果不能在有限步之内达到绝对精确的值，则要精确到 n 位小数，至少需要正比于 $\log n$ 的运算次数. 换言之，若不能在常数步之内求得精确解，则计算的有效位数的增长不能超过一个几何级数，中间的情况是不存在的. 如果只许可使用四则运算，那末逼近一个无理数的最高速度是平方收敛.

一、主 要 结 果

假定我们要计算某个实数或复数，例如 e，π，或者某个方程的根. 手头上能够用的数归根到底只能是某个范围内的整数. 所能使用的工具不外乎加减乘除、开方等代数运算. 如果能在有限步之内求得精确解，当然万事大吉. 否则就要近似地计算. 有时，随着计算步数的增加，计算结果的有效位数也线性地增长；有时，随着计算步数的增长，计算的有效位数成几何级数增长. 用 Newton 切线法来求根就是有效位数成几何级数增长的例子. 有没有更快的收敛速度呢？这是计算理论和代数逼近理论中一个有趣的问题，但却未被深入地研究过. 作者在本文中严格证明了：如果使用四则运算和开方运算，那末有效数字的位数不能超过运算步数的一个指数函数. 如果只使用算术四则运算，那末最快的收敛速度是平方收敛.

作者在研究用例证法证明几何定理[1]时用到这一结果. 本文中的某些引理是继续了吴文俊[2,3]和 Ritt[4,5] 的工作并加以复杂性分析以后得到的.

设我们想要计算某个实数或复数 ρ. 在计算过程中，把每一步运算后得到的数依次写下来，得到一个序列

$$a_1, a_2, a_3, \cdots, \tag{1}$$

其中的某个子序列

$$a_{i_1}, a_{i_2}, a_{i_3}, \cdots \tag{2}$$

应该趋向我们想得到的数 ρ：

本文 1985 年 7 月 15 日收到.

$$\lim_{j\to\infty} a_{i_j} = \rho. \tag{3}$$

(1)式中,每个 a_i 或是在一个固定范围内的整数,或是它前面的某个数的方根,或是它前面的某两个数的和、差、积或者商. 更一般地,我们可以假定 $a_1, a_2, \cdots, a_i$ 之间满足一个整系数的代数方程

$$F_i(x_1, x_2, \cdots, x_i) = 0.$$

这里 F_i 是 $x_1, x_2, \cdots, x_i$ 的整系数多元多项式,当用 $a_1, a_2, \cdots, a_{i-1}$ 代替 $x_1, x_2, \cdots x_{i-1}$ 之后得到一个关于 x_i 的多项式 $F_i(a_1, a_2, \cdots, a_{i-1}, x_i)$,而且 x_i 是真正在里面出现的. 换句话说,x_i 的某个非 0 次方幂的系数不为 0. 把 a_i 代入 $F_i(a_1, a_2, \cdots, a_{i-1}, x_i)$中的 x_i,应该使多项式的值为 0. 于是 $a_1, a_2, \cdots, a_i$ 都是些代数数. 现在可以给出下面的定义.

定义 1. 如果用 a_i 代替 x_i 后满足一组整系数代数方程 $F_i(x_1, x_2, \cdots, x_i) = 0$ ($i = 1, 2, 3, \cdots$),而且 x_i 在 $F_i(a_1, a_2, \cdots, a_{i-1}, x_i)$中有某个非 0 次幂系数不为0,则称(1)式为一个代数数列.

这个定义太一般了,我们下面对 F_i 作一点限制. 把 $F_i(x_1, x_2, \cdots, x_i)$ 展开成一些单项式之和,把这些单项式的最高次数称为 F_i 的次数,把这些单项式前面的系数(都是些整数)取绝对值后求和,称为 F_i 的项数. 例如若 $F_3(x_1, x_2, x_3) = 2x_1^2x_2 - 3x_3^3$, 则次数为 3,项数为 5. 次数和项数有下面简单的性质: 多项式和的次数不大于各多项式次数的最大值. 多项式和的项数不大于项数的和. 多项式的乘积的次数等于各多项式次数之和. 多项式积的项数不大于各多项式项数之积.

定义 2 如果定义 1 中的每个 $F_i(x_1, x_2, \cdots, x_i)$ 的次数和项数都不超过某一个常数 m,则称(1)式为一个 m-代数数列.

显然,在普通计算过程中,用加、减、乘、除、开方所得到的数列都是某一m-代数数列. 它的一个重要性质是: 其中任何一项,如果不等于 0,则不能非常的小. 可以精确地被表述为下面的裂缝定理. 它的证明构成了本文的主要内容.

定理 1 设 $a_1, a_2, a_3, \cdots$ 是一个 m-代数数列. 那末 $a_i = 0$ 或者$|a_i| \geqslant 2^{-c}$,其中 c 是仅依赖于m的一个常数.

现在假定 m-代数数列(1)式的某个子序列(2)式趋向于 ρ. 我们把 $|\rho - a_{i_j}|$ 称作逼近的理论误差. 但是 ρ 还没有算出来,所以$|\rho - a_{i_j}|$是多少是不知道的,这个定义没有什么用处. 在实践上,往往用最后两次逼近值的差取绝对值来作为逼近程度的度量. 因此我们给出下述定义.

定义 3. 设 m-代数数列(1)式的子序列(2)趋向于 ρ,且(2)式中相邻两项都是不相等的. 称 a_{i_j} 为 ρ 的第 j 次逼近值,i_j 为第 j 次逼近时已经经过的计算步数. $|a_{i_j} - a_{i_{j-1}}|$ 为第 j 次逼近后的实用误差,$\lfloor -\log |a_{i_j} - a_{i_{j-1}}| \rfloor$为第 j 次逼近后得到的有效位数.

定义中的对数是以 2 为底的,但是在讨论中以什么为底都没有关系. 从定理 1 可以得到关于逼近速度的定理2. 它说明了在近似计算中有效位数的增长不会超过一个几何级数.

定理 2. 第 j 次逼近得到的有效位数不超过第 j 次逼近已经使用的计算步数 i_j 的一个指数函数.

证. 考虑代数方程组

$$\begin{cases} F_1(x_1) = 0, \\ F_2(x_1, x_2) = 0, \\ \vdots \\ F_{i_j}(x_1, x_2, \cdots, x_{i_j}) = 0, \\ x_{i_j+1} - (x_{i_j} - x_{i_{j-1}}) = 0. \end{cases}$$

它是由原来的代数方程组中的前 i_j 个方程再加上 $x_{i_j+1} - (x_{i_j} - x_{i_{j-1}}) = 0$（第 i_j+1 个）而得到的. 数列 $a_1, a_2, \cdots, a_{i_j}, a_{i_j} - a_{i_{j-1}}$ 显然满足以上的方程组，因而是一个 m-代数数列. 根据定理 1，它的第 $i_j + 1$ 项 $(a_{i_j} - a_{i_{j-1}})$ 应该满足

$$|a_{i_j} - a_{i_{j-1}}| \geqslant 2^{-c^{i_j+1}}$$

于是第 j 次逼近后的有效位数

$$\lfloor -\log |a_{i_j} - a_{i_{j-1}}| \rfloor \leqslant c^{i_j+1} \leqslant (c^2)^{i_j}$$

不超过计算步数 i_j 的一个指数函数.

本文的第 2 节证明一些引理，第 3 节证明主要的定理 1，第 4 节讨论算术数列逼近的速度.

二、关于代数数列的若干引理

设有变元 $x_1, x_2, x_3, \cdots$ 的无穷序列. 考虑这些变元上的某个整系数多项式 F. 显然，其中只能出现有限多个变元. 设 x_i 是其中最后一个变元，于是可以把该多项式写为 $F(x_1, x_2, \cdots, x_i)$. 考虑所有这样的多项式，它仅含变元 $x_1, x_2, \cdots, x_i$，次数 $\leqslant p$，项数 $\leqslant t$，变元 x_i 的最高方幂数 $\leqslant u$. 这样的多项式只有有限多个，把它们的集合记为 $\mathscr{P}(i,p,t,u)$. m-代数数列的前 i 项所应满足的方程组

$$F_j(x_1, x_2, \cdots, x_j) = 0 \quad (j = 1, 2, \cdots, i),$$

一共只有有限多种不同的可能. 用 $\mathscr{A}_i$ 代表所有长度为 i 的 m-代数数列 $(a_1, a_2, \cdots, a_i)$ 的集合，用 $\mathscr{B}_i$ 代表其中第 i 项所构成的集合，即

$$\mathscr{B}_i = \{a_i | (a_1, a_2, \cdots, a_i) \in \mathscr{A}_i\},$$

这些集合都是有限的，所以可以再定义

$$M_i = \operatorname{Max}\{|a| \,\big|\, a \in \mathscr{B}_i\},$$

$$M_i(p,t,u) = \operatorname{Max}\{|F(a_1, \cdots, a_i)| \,\big|\, F \in \mathscr{P}(i,p,t,u), (a_1, \cdots, a_i) \in \mathscr{A}_i\},$$

$$m_i(p,t,u) = \operatorname{Min}\{|F(a_1, \cdots, a_i)| \,\big|\, F \in \mathscr{P}(i,p,t,u), (a_1, \cdots, a_i) \in \mathscr{A}_i,$$

$$F(a_1, \cdots, a_i) \neq 0\}.$$

显然，$M_i, M_i(p,t,u)$ 是各变元的不减函数，$m_i(p,t,u)$ 是不增函数.

引理 1. $M_i(p,t,u) \leqslant t \cdot M_i^p$.

证. 设 $F \in \mathscr{P}(i,p,t,u)$，则 $F(a_1, a_2, \cdots, a_i)$ 中最多只有 t 个单项，每项是不超过 p 个因子的乘积，而每个因子的绝对值都 $\leqslant M_i$，于是 $|F(a_1, a_2, \cdots, a_i)| \leqslant t \cdot M_i^p$. 引理得证.

引理 2. $$M_i \leqslant \frac{m \cdot M_{i-1}(m,m,m)}{m_{i-1}(m,m,m)}.$$

证. a_i 应该满足方程 $F_i(a_1,a_2,\cdots,a_i)=0$. 不妨设

$$F_i(a_1,\cdots,a_i)=F_{i0}(a_1,\cdots,a_{i-1})a_i^v+F_{i1}(a_1,\cdots,a_{i-1})a_i^{v-1}+\cdots$$
$$+F_{iv}(a_1,\cdots,a_{i-1})=0.$$
$$1\leqslant v\leqslant m,\quad F_{i0}(a_1,\cdots,a_{i-1})\not\equiv 0.$$

如果 $|a_i|\leqslant 1$ 则引理不证自明,故可设 $|a_i|\geqslant 1$. 于是由移项可得:

$$|a_i|\leqslant\left|\frac{|F_{i1}(a_1,\cdots,a_{i-1})|+\cdots+|F_{iv}(a_1,\cdots,a_{i-1})|}{F_{i0}(a_1,\cdots,a_{i-1})}\right|\leqslant\frac{m\cdot M_{i-1}(m,m,m)}{m_{i-1}(m,m,m)}.$$

这是因为 $F_{i0}, F_{i1},\cdots, F_{iv}$ 都属于 $\mathscr{P}(i-1,m,m,m)$.

引理 3.

$$\begin{cases} m_i^p(m,m,m)\geqslant m_i(pm,m^p,pm),\\ M_i^p(m,m,m)\leqslant M_i(pm,m^p,pm).\end{cases}$$

证. 因为若有 p 个 $\mathscr{P}(i,m,m,m)$ 中的多项式相乘,则它们的乘积属于 $\mathscr{P}(i,pm,m^p,pm)$.

引理 4. 设 $H\in\mathscr{P}(i,p,t,u), G\in\mathscr{P}(i,q,s,v), u\geqslant v\geqslant 1$. 那末存在 $G_0\in\mathscr{P}(i-1,q,s,q-1), L\in\mathscr{P}(i,p+uq,(2s)^ut,u-v), R\in\mathscr{P}(i,p+uq,(2s)^ut,v-1)$, 使得下式成立:

$$G_0^{u'}H+LG=R,\quad u'\leqslant u.$$

证. 实际上是用 G 对 H 作带余除法. 设

$$H=H_0(x_1,\cdots,x_{i-1})x_i^u+H_1(x_1,\cdots,x_{i-1})x_i^{u-1}+\cdots+H_u(x_1,\cdots,x_{i-1}),$$
$$G=G_0(x_1,\cdots,x_{i-1})x_i^v+G_1(x_1,\cdots,x_{i-1})x_i^{v-1}+\cdots+G_v(x_1,\cdots,x_{i-1}),$$

令 $H'=G_0H-H_0Gx_i^{u-v}$, 显然 x_i^u 的项被消掉了,故可以写成

$$H'=H_0'(x_1,\cdots,x_{i-1})x_i^{u-1}+H_1'(x_1,\cdots,x_{i-1})x_i^{u-2}+\cdots+H_{u-1}'(x_1,\cdots,x_{i-1}),$$

不难验证 $H'\in\mathscr{P}(i,p+q,2st,u-1)$. 若 $u-1\geqslant v$, 我们再作 $H''=G_0H'-H_0'Gx_i^{u-v-1}$, 消去 x_i^{u-1} 的项,不难验证 $H''\in\mathscr{P}(i,p+2q,(2s)^2t,u-2)$. 这样用 $H_0',H_0'',\cdots$ 表示 $H',H'',\cdots$ 的首项系数,得到一串等式:

$$H'=G_0H-H_0Gx_i^{u-v},\qquad H_0',H'\in\mathscr{P}(i,p+q,2st,u-1),$$
$$H''=G_0H'-H_0'Gx_i^{u-v-1},\qquad H_0'',H''\in\mathscr{P}(i,p+2q,(2s)^2t,u-2),$$
$$\cdots\cdots\qquad\qquad\cdots\cdots$$
$$H^{(u-v+1)}=G_0H^{(u-v)}-H_0^{(u-v)}G, H_0^{(u-v+1)},H^{(u-v+1)}\in\mathscr{P}(i,p+(u-v+1)q,(2s)^{u-v+1}t,v-1).$$

将以上各式分别乘以 $G_0^{u-v}, G_0^{u-v-1},\cdots, 1$, 全部加起来,就得到:

$$G_0^{u-v+1}H-(H_0G_0^{u-v}x_i^{u-v}+H_0'G_0^{u-v-1}x_i^{u-v-1}+\cdots+H_0^{(u-v)})G=H^{(u-v+1)}.$$

我们已经知道 $G_0\in\mathscr{P}(i-1,q,s,q-1)$, $H^{(u-v+1)}\in\mathscr{P}(i,p+(u-v+1)q,(2s)^{u-v+1}t,v-1)\subseteq\mathscr{P}(i,p+uq,(2s)^ut,v-1)$, 令 $L=-(H_0G_0^{u-v}x_i^{u-v}+\cdots+H_0^{(u-v)})$, $R=H^{(u-v+1)}$ 就有

$$G_0^{u-v+1}H+LG=R.$$

其中 L 的次数 $\leqslant p+uq$, 项数 $\leqslant ts^{u-v}+t\cdot 2s\cdot s^{u-v-1}+t\cdot(2s)^2\cdot s^{u-v-2}+\cdots+t(2s)^{u-v}\leqslant(2s)^{u-v+1}t\leqslant(2s)^ut$. 故 $L\in\mathscr{P}(i,p+uq,(2s)^ut,u-v)$, 引理全部证毕.

引理 4 是用 G 去除 H，使余式 R 中 x_i 的次数低于 x_i 在 G 中的次数. 得到 R 以后又可以用 R 去除 G，把 G 中 x_i 的方幂再降低，这就是碾转相除法. 利用这个方法可以证明引理 5. 为了方便起见，我们将用 $*$ 号代表一个常数. 但是等式左右的 $*$ 号不一定代表同一个常数，于是我们可以写成 $m \leqslant *$，$2^* = *$，$*^2 \leqslant *$，$(*"t^*)^* = *"t^*$ 等等.

引理 5. 设 $a_1, a_2, \cdots, a_{i-1}$ 是 m-代数数列中的前 $i-1$ 项，$H \in \mathscr{P}(i,p,t,u)$，$G \in \mathscr{P}(i,q,s,v)$，$u,v \leqslant m$. 那末存在 $H', G', L \in \mathscr{P}(i, *(p+q), (2ts)^*, *)$，使得 $G'H + H'G = L$，且 $L(a_1,a_2,\cdots,a_{i-1},x_i)$ 是 $H(a_1,a_2,\cdots,a_{i-1},x_i)$ 和 $G(a_1,a_2,\cdots a_{i-1},x_i)$ 的作为 x_i 的多项式的最大公因子.

证. 将 $a_1,a_2,\cdots,a_{i-1}$ 代入 H 和 G 中，和引理 4 一样，对 H 和 G 作形式地碾转相除. 碾转相除的次数不超过 m，是一个常数. 最后可得一个最大公因子 L. 我们现在来观察，用 G 去除一次 H（假定 x_i 在 H 中的次数不低于在 G 中的次数）得到余式 R，然后再用 R 去除一次 G，在这样一个往复中，各有关多项式复杂程度的变化. 根据引理 4，有 $C,D,R \in \mathscr{P}(i, *(p+q), (2st)^*, m)$ 使

$$CH + DG = R.$$

再对 G 和 R 用一次引理 4，有 $E, F, S \in \mathscr{P}(i, *(*(p+q)+q), (2(2st)^*s)^*, m) \subseteq \mathscr{P}(i, *(p+q), (2st)^*, m)$ 使 $EG + FR = S$. 从这两式可得

$$(E + DF)G + CFH = S.$$

于是，存在 $C_1,D_1,E_1,F_1,H_1,G_1 \in \mathscr{P}(i, *(p+q), 2st)^*, *)$ 使

$$\begin{cases} C_1H + D_1G = H_1, \\ E_1H + F_1G = G_1. \end{cases}$$

H_1，G_1 中 x_i 的方幂数比 H, G 中 x_i 的方幂数都降低了. 再对 H_1 和 G_1 反复使用这个结果（常数多次），就知道存在 $H', G', L \in \mathscr{P}(i, *(p+q), (2st)^*, *)$ 使得 $G'H + H'G = L$，且 $L(a_1, \cdots, a_{i-1}, x_i)$ 是 $H(a_1,\cdots,a_{i-1},x_i)$ 和 $G(a_1,\cdots,a_{i-1},x_i)$ 作为 x_i 的多项式的最大公因子.

引理 6. 设 $F \in \mathscr{P}(i,p,t,u)$，$G \in \mathscr{P}(i,q,s,v)$，$G(a_1,a_2,\cdots,a_i) = 0$，$u,v \leqslant m$，$F(a_1, \cdots, a_{i-1}, x_i)$ 与 $G(a_1, a_2 \cdots, a_{i-1}, x_i)$ 作为 x_i 的多项式是互素的. 则

$$F(a_1, a_2, \cdots, a_i) = \frac{L(a_1,\cdots,a_{i-1})}{G_0^*(a_1,\cdots,a_{i-1})F(a_1,\cdots,a_{i-1},b_2)\cdots F(a_1,\cdots,a_{i-1},b_v)}.$$

其中 $b_1 = a_i, b_2, b_3, \cdots, b_v$ 是 $G(a_1,\cdots,a_{i-1},x_i)$ 的 v 个根. $G_0 \in \mathscr{P}(i-1, q, s, q)$ 是 $G(x_1, \cdots, x_i)$ 中 x_i 的首项系数，$L \in \mathscr{P}(i-1, *(p+q), (2st)^*, *(p+q))$，$L(a_1,\cdots,a_{i-1}) \neq 0$.

证. 因为 F 和 G 没有公根，所以 $F(a_1,\cdots,a_{i-1},b_j) \neq 0 (j = 1,2,\cdots,v)$. 于是

$$F(a_1,\cdots,a_i) = \frac{F(a_1,\cdots,a_{i-1},b_1)F(a_1,\cdots,a_{i-1},b_2)\cdots F(a_1,\cdots,a_{i-1},b_v)}{F(a_1,\cdots,a_{i-1},b_2)\cdots F(a_1,\cdots,a_{i-1},b_v)}$$

把分子形式地乘开，是一个关于 $a_1, a_2, \cdots, a_{i-1}, b_1, b_2, \cdots, b_v$ 的多项式. 它关于 $b_1, b_2, \cdots, b_v$ 是对称的，总次数 $\leqslant pm$，项数 $\leqslant t^m$，关于 $b_1, b_2, \cdots, b_v$ 的次数 $\leqslant uv = *$. 因为它关于 G 的根 $b_1, \cdots, b_v$ 对称，故可以用初等对称多项式 $\sigma_1, \sigma_2, \cdots, \sigma_v$ 表出. 每个形如 $\sum_i b_i^3$，$\sum_{i \neq j} b_i^2 b_j$，$\sum_{i \neq j} b_i^3 b_j$，$\cdots$ 的对称式需要用多少项初等对称多项式才能表出，是只依赖于 m 的，因此是一个常数. 因此，分子可以写为一个关于 $a_1,\cdots,a_{i-1},\sigma_1,\sigma_2,\cdots,\sigma_v$ 的多项式，其次数 $\leqslant pm$，项数 $\leqslant *t^*$. 关于 $\sigma_1, \sigma_2, \cdots, \sigma_v$ 的次数 $\leqslant uv = *$. 设

$$G(a_1,\cdots,a_{i-1},x_i)=G_0(a_1,\cdots,a_{i-1})x_i^v+\cdots+G_v(a_1,\cdots,a_{i-1}),$$

这里 $G_0,G_1,\cdots,G_v\in\mathscr{P}(i-1,q,s,q)$. 把 $\sigma_1,\sigma_2,\cdots,\sigma_v$ 分别用 $G_1/G_0,G_2/G_0,\cdots,G_v/G_0$ 代入,得到

$$F(a_1,\cdots,a_i)=\frac{L(a_1,\cdots,a_{i-1})}{G_0^*F(a_1,\cdots,a_{i-1},b_2)\cdots F(a_1,\cdots,a_{i-1},b_v)},$$

其中 $L\in\mathscr{P}(i-1,*(p+q),(2st)^*,*(p+q))$, $F\in\mathscr{P}(i,p,t,u)$, $G_0\in\mathscr{P}(i-1,q,s,q)$. 分母中 G_0 的方幂不超过原式分子中 $\sigma_1,\cdots,\sigma_v$ 的次数,故是一个常数 $*$.

三、代数逼近的速度

在本节中,我们要证明主要的定理 1. 为此需要先给出两个递推的不等式.

引理 7.

$$M_i(p,t,p)\leqslant\left(\frac{M_{i-1}(*p,*^pt^*,*p)}{m_{i-1}(*p,*^pt^*,*p)}\right)^*.$$

证. 因为 $M_{i-1}(p,t,p)\geqslant t$, 根据引理 1, 2 得到:

$$M_i(p,t,p)\leqslant tM_i^p\leqslant\frac{tm^pM_{i-1}^p(m,m,m)}{m_{i-1}^p(m,m,m)}\leqslant\frac{M_{i-1}(m,t,m)M_{i-1}^{2p}(m,m,m)}{m_{i-1}^p(m,m,m)}$$

$$\leqslant\frac{M_{i-1}(m,t,m)\cdot M_{i-1}^2(*p,*^p,*p)}{m_{i-1}(*p,*^p,*p)}\leqslant\frac{M_{i-1}^*(*p,*^pt^*,*p)}{m_{i-1}^*(*p,*^pt^*,*p)}.$$

引理 8.

$$m_i(p,t,p)\geqslant\left(\frac{m_{i-1}(*p,*^pt^*,*p)}{M_{i-1}(*p,*^pt^*,*p)}\right)^*.$$

证. 设 $F\in\mathscr{P}(i,p,t,p)$, F_i 是定义 m-代数数列的代数方程,故 $F_i\in\mathscr{P}(i,m,m,m)$. 在引理 4 中令 G 为 F_i, 可知存在 $F_{i0}\in\mathscr{P}(i-1,m,m,m)$, $R\in\mathscr{P}(i,*p,*^pt,*)$, $u\leqslant p$, 使得

$$F_{i0}^uF+LF_i=R. \tag{1}$$

下面求 $F_i(a_1,\cdots,a_{i-1},x_i)$与 $R(a_1,\cdots,a_{i-1},x_i)$的最大公因子 H. 根据引理 5,有 H_1, H_2, $H\in\mathscr{P}(i,*p,*^pt^*,*)$使得

$$H_1F_i+H_2R=H.$$

根据引理4,用H去除 F_i 得到

$$SF_i=HF_i'.$$

其中 $S\in\mathscr{P}(i-1,*p,*^pt^*,*p)$, $F_i'\in\mathscr{P}(i,*p,*^pt^*,*p)$. 上式仅在用 $a_1,\cdots,a_{i-1}$ 代替 $x_1,\cdots,x_{i-1}$ 时成立. 现在 $R(a_1,\cdots,a_{i-1},x_i)$与$F_i'(a_1,\cdots,a_{i-1},x_i)$ 互素(因为我们可以假定没有重根,如有重根,则可以用求导数、求最大公因子及除法把重根消去,得到一个新的 F_i 仍属于 $\mathscr{P}(i,*,*,*)$),故可以使用引理 6. 用 R 和 F_i' 代替引理 6 中的 F 和 G 得到

$$R(a_1,\cdots,a_i)=\frac{L(a_1,\cdots,a_{i-1})}{F_{i0}'^*(a_1,\cdots,a_{i-1})\cdot R(a_1,\cdots,a_{i-1},b_2)\cdots R(a_1,\cdots,a_{i-1},b_v)}. \tag{2}$$

其中 $L\in\mathscr{P}(i-1,*p,*^pt^*,*p)$, $F_{i0}'\in\mathscr{P}(i-1,*p,*^pt^*,*p)$, $R\in\mathscr{P}(i,*p,*^pt,*)$. 所以可以得到如下的等式:

$$|F(a_1,\cdots,a_i)|=\left|\frac{R(a_1,\cdots,a_i)}{F_{i0}^u(a_1,\cdots,a_{i-1})}\right|$$ 从(1)式得到

$$= \left| \frac{L(a_1,\cdots,a_{i-1})}{F^u_{i0}(a_1,\cdots,a_{i-1})F'^*_{i0}(a_1,\cdots,a_{i-1})R(a_1,\cdots,a_{i-1},b_2)\cdots R(a_1,\cdots a_{i-1},b_v)} \right|$$

从(2)式得到

$$\geqslant \left| \frac{m_{i-1}(*p,*^pt^*,*p)}{M^p_{i-1}(*,*,*)M^*_{i-1}(*p,*^pt^*,*p)\cdot M^*_i(*p,*^pt^*,*p)} \right|$$

$u \leqslant p, v \leqslant *$

$$\geqslant \left| \frac{m_{i-1}(*p,*^pt^*,*p)m^{*p}_{i-1}(*,*,*)}{M^p_{i-1}(*,*,*)M^*_{i-1}(*p,*^pt^*,*p)\cdot *^pt^*m^{*p}M^{*p}_{i-1}(*,*,*)} \right|$$

从引理 1，2

$$\geqslant \left| \frac{m_{i-1}(*p,*^pt^*,*p)m^*_{i-1}(*p,*^p,*p)}{M_{i-1}(*p,*^p,*p)M^*_{i-1}(*p,*^pt^*,*p)M^*_{i-1}(*p,*^p,*p)} \right|$$

从引理 3

$$\geqslant \left(\frac{m_{i-1}(*p,*^pt^*,*p)}{M_{i-1}(*p,*^pt^*,*p)} \right)^*.$$

令 $\alpha_i(p,t) = m_i(p,t,p)/M_i(p,t,p)$ 则有

引理 9. $\alpha_i(p,t) \geqslant \alpha_{i-1}(*p,*^pt^*)$.

证.

$$\alpha_i(p,t) = \frac{m_i(p,t,p)}{M_i(p,t,p)} \geqslant \left(\frac{m_{i-1}(*p,*^pt^*,*p)}{M_{i-1}(*p,*^pt^*,*p)} \right)^{2*}$$

$$\geqslant \frac{m_{i-1}(2*^2p,(*^pt^*)^{2*},2*^2p)}{M_{i-1}(2*^2p,(*^pt^*)^{2*},2*^2p)} \geqslant \frac{m_{i-1}(*p,*^pt^*,*p)}{M_{i-1}(*p,*^pt^*,*p)}$$

$$= \alpha_{i-1}(*p,*^pt^*).$$

定理 1 的证明. 从引理 9 可以递归地得到

$$\alpha_i(p,t) \geqslant \alpha_{i-1}(p_1,t_1) \geqslant \alpha_{i-2}(p_2,t_2) \geqslant \cdots \geqslant \alpha_0(p_i,t_i),$$

其中 $p_i = cp_{i-1}$，$t_i = c^{p_{i-1}}t^c_{i-1}$，$c$ 是某一常数. 于是 $p_i = c^ip$，$t_i = c^{ip}c^{i-1}t^{c^i}$（不难用归纳法证明），故

$$\alpha_i(p,t) \geqslant \alpha_0(c^ip, c^{ip}c^{i-1}t^{c^i}).$$

根据 $m_0(p,t,u)$和 $M_0(p,t,u)$的定义可知，$m_0(p,t,u) = 1$，$M_0(p,t,u) = t$. 故得

$$\alpha_i(p,t) \geqslant c^{-ic^{i-1}p}t^{-c^i}.$$

$$|a_i| \geqslant m_i(1,1,1) \geqslant \alpha_i(1,1) \geqslant c^{-ic^{i-1}} \geqslant 2^{-c^i_1}.$$

现在我们考虑更一般的带参数的情形.

定义 4. 设 $u_1, u_2, \cdots, u_s$ 是一组参数. 如果用 a_i 代替 x_i 后满足一组整系数代数方程

$$F_i(u_1,u_2,\cdots,u_s,x_1,,x_2,\cdots,x_i) = 0 \quad (i = 1,2,3,\cdots),$$

而且 x_i 在 $F_i(u_1,u_2,\cdots,u_s,a_1,a_2,\cdots a_{i-1},x_i)$ 中有某个非 0 次幂系数不等于 0，则称 $a_1,a_2,\cdots$ 为一个带参数的代数数列. 如果 F_i 的次数（包括 $u_1, u_2,\cdots$ 的次数）和项数都不超过一个常数 m，则称 $a_1, a_2,\cdots$ 为一个带参数的 m-代数数列.

我们以上的讨论对于带参数的 m-代数数列完全适用，引理 9 的递推公式仍然成立，故

$$\alpha_i(p,t) \geqslant \alpha_0(c^ip, c^{ic^{i-1}p}t^{c^i}).$$

若我们假定 $u_1,\cdots,u_s$ 都是一些$\leqslant M$的整数，则有：$m_0(p,t,u) \geqslant 1$，$M_0(p,t,u) \leqslant tM^p$. 所以

可得

$$\alpha_i(p,t) \geqslant c^{-ic^{t-1}p_t-c^t}M^{-c^tp},$$

$$|a_i| \geqslant m_i(1,1,1) \geqslant \alpha_i(1,1) \geqslant c^{-ic^{t-1}}M^{-c^t} \geqslant M^{-c_1^t} \quad (M \geqslant 2\text{时}),$$

定理 3. 若 a_i 是带参数的 m-代数数列的第 i 项，参数都是绝对值不超过 M 的整数，$M \geqslant 2$. 那末 $a_i = 0$ 或 $|a_i| \geqslant M^{-c^t}$. 其中 c 是只依赖于 m 的常数.

四、算术逼近的最快速度

以上讨论了代数逼近的最快速度. 关于几何定理证明的许多结论和它密切相关. 我们如果只允许算术四则运算(这更符合实际计算的情形),问题就变得简单得多. 而且可以证明,平方收敛就是最快的收敛速度.

定义 5. 若整数 p,q 互素,则有理数 $\alpha = p/q$ 的模定义为 $m(\alpha) = \mathrm{Max}\{|p|,|q|\}$.

引理 10. 设 α,β 为有理数,那末

(1) $m(\alpha\beta) \leqslant m(\alpha)m(\beta)$,

(2) $m(\alpha/\beta) \leqslant m(\alpha)m(\beta)$,

(3) $m(\alpha\pm\beta) \leqslant 2m(\alpha)m(\beta)$.

证. 设 $\alpha = p_1/q_1, \beta = p_2/q_2, (p_1,q_1) = (p_2,q_2) = 1$.

$$\begin{aligned} m(\alpha\beta) &\leqslant \mathrm{Max}\{|p_1p_2|,|q_1q_2|\} \leqslant \mathrm{Max}\{|p_1|,|q_1|\}\cdot\mathrm{Max}\{|p_2|,|q_2|\} \\ &= m(\alpha)\cdot m(\beta). \end{aligned}$$

$$\begin{aligned} m(\alpha/\beta) &= m(p_1q_2/p_2q_1) \leqslant \mathrm{Max}\{|p_1q_2|,|p_2q_1|\} \\ &\leqslant \mathrm{Max}\{|p_1|,|q_1|\}\cdot\mathrm{Max}\{|p_2|,|q_2|\} = m(\alpha)m(\beta). \end{aligned}$$

$$\begin{aligned} m(\alpha\pm\beta) &= m((p_1q_2\pm p_2q_1)/q_1q_2) \\ &\leqslant \mathrm{Max}\{|p_1q_2\pm p_2q_1|,|q_1q_2|\} \\ &\leqslant \mathrm{Max}\{|p_1q_2|,|q_1q_2|\} + \mathrm{Max}\{|p_2q_1|,|q_1q_2|\} \\ &\leqslant |q_2|m(\alpha) + |q_1|m(\beta) \\ &\leqslant m(\beta)m(\alpha) + m(\alpha)m(\beta) \\ &= 2m(\alpha)m(\beta). \end{aligned}$$

定理 4. 设有有理数的序列 $a_1,a_2,a_3,\cdots$，每个 a_i 都是前面某两项的和、差、积或商,或是某范围内的整数 $|a_i| \leqslant c$. 那末,若 $a_i \neq 0$, 则有 $|a_i| \geqslant (\sqrt{2c})^{-2^i}$.

证. 定义 $M_i = \mathrm{Max}\{m(a_1), m(a_2),\cdots, m(a_i)\}$ 则对每个 i 都有 $M_i \leqslant \mathrm{Max}\{2M_{i-1}^2, c\}$ 于是可得:

$$\mathrm{M}_1(a_1) \leqslant c,$$

$$\mathrm{M}_2(a_2) \leqslant 2c^2,$$

$$\mathrm{M}_3(a_0) \leqslant 2(2c^2)^2$$

$$\cdots$$

$$\mathrm{M}_i(a_i) \leqslant c^{2^{i-1}}\cdot 2^{1+2+4+\cdots+2^{i-2}} \leqslant c^{2^{i-1}}\cdot 2^{2^{i-1}} = (2c)^{2^{i-1}}.$$

若 $a_i \neq 0$, 则

$$|a_i| \geqslant (2c)^{-2^{i-1}} = (\sqrt{2c})^{-2^i}.$$

定理 5. 如果用四则运算来逼近一个无理数，那末实用有效位数的增长不超过公比为 2 的一个几何级数．换言之，最快的收敛速度是平方收敛．

证．同定理 2．

参　考　文　献

[1] 洪加威，能用例证法来证明几何定理吗？中国科学 A 辑，1986，4：3：234—242．

[2] Wu Wen-tsün, Basic principle of mechanical theorem proving in elementary geometry, 系统科学与数学，4 (1984)，207—235．

[3] Wu Wen-tsun, Some remark on mechanical theorem proving in elementary geometry. *Acta Math. Scientia*, 3(1983), 4: 357—360.

[4] Ritt, J. F., *Differential algebra, Amer. Math. Soc.*, 1950.

[5] ————., *Differential equetions from the algebraic standpoint*, Amer. Math. Soc. 1932.