信息安全数学基础
第七章 连分数

中山大学 数据科学与计算机学院

1. 有限连分数的概念

形如

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{x_4 + \cfrac{1}{x_5 + \cfrac{1}{x_6}}}}}}$$

的实数，其中$x_1, x_2, \ldots, x_6$均为正实数，被称为是一个6阶连分数(6条横线).
如果x_0是整数，且$x_1, x_2, \ldots, x_6$均为正整数，则该连分数被称为6阶简单连分数.
例如，

$$-3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{3 + \cfrac{1}{5 + \cfrac{1}{9 + \cfrac{1}{100}}}}}}$$

可以将上述连分数记为: $[x_0, x_1, x_2, x_3, x_4, x_5, x_6] = [-3, 2, 4, 3, 5, 9, 100]$.

一般地, 形如$[x_0, x_1, x_2, \ldots, x_n] =$

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\ddots + \cfrac{1}{x_{n-1} + \cfrac{1}{x_n}}}}}}$$

的实数, 其中x_0是实数, $x_1, x_2, \ldots, x_n$均为正实数, 被称为有限连分数.

如果x_0是整数, 且$x_1, x_2, \ldots, x_n$均为正整数, 则该连分数被称为有限简单连分数.

将$[x_0, x_1, x_2, \ldots, x_k]$称为是$[x_0, x_1, x_2, \ldots, x_n]$的第$k$个渐近分数, 记为

$$[x_0, x_1, x_2, \ldots, x_k] = \frac{P_k}{Q_k}.$$

例如,

$$\frac{P_1}{Q_1} = -3 + \frac{1}{2}, \quad \frac{P_2}{Q_2} = -3 + \frac{1}{2 + \frac{1}{4}}, \quad \frac{P_3}{Q_3} = -3 + \frac{1}{2 + \frac{1}{4 + \frac{1}{3}}}$$

都是$[-3, 2, 4, 3, 5, 9, 100] =$

$$-3 + \frac{1}{2 + \frac{1}{4 + \frac{1}{3 + \frac{1}{5 + \frac{1}{9 + \frac{1}{100}}}}}}$$

的渐近分数, 即它们的值越来越接近$[-3, 2, 4, 3, 5, 9, 100]$的值.

无限连分数

与有限连分数对应的是无限连分数.
形如

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots + \cfrac{1}{x_{n-1} + \cfrac{1}{x_n + \ddots}}}}}$$

的数, 其中$x_1, x_2, \ldots$,均为正实数, 被称为无限连分数, 记为$[x_0, x_1, x_2, \ldots, x_{n-1}, \ldots]$.
如果x_0是整数, 且$x_1, x_2, \ldots$均为正整数, 该连分数被称为无限简单连分数.
将$[x_0, x_1, x_2, \ldots, x_k]$称为是$[x_0, x_1, x_2, \ldots, x_n, \ldots]$的第$k(\geq 0)$个渐近分数.
令$\theta_k = [x_0, x_1, x_2, \ldots, x_k]$, 这样$\theta_0, \theta_1, \ldots$都是$\theta$ 的渐进分数. 如果有

$$\lim_{k \to \infty} [x_0, x_1, x_2, \ldots, x_k] = \theta$$

则称$[x_0, x_1, x_2, \ldots, x_n, \ldots]$是收敛的, θ即为其值, 记作$[x_0, x_1, \ldots, x_n, \ldots] = \theta$.
如果不存在极限, 则称无限连分数$[x_0, x_1, x_2, \ldots, x_n, \ldots]$是发散的.

$\sqrt{2} = [1, 2, 2, 2, \cdots]$的无限连分数表示

$$
\begin{aligned}
\sqrt{2} &= 1 + \cfrac{1}{1+\sqrt{2}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{1+\sqrt{2}}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1+\sqrt{2}}}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + (1 + \cfrac{1}{1+\sqrt{2}})}}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}},
\end{aligned}
$$

给定实数x, 可以构造x的简单连分数$x = [x_0, x_1, x_2, x_3, \cdots]$, 其中$x_0$是实数, $x_1 x_2, x_3, \cdots$均为整数.

1. 令$x_0 \leftarrow \lfloor x \rfloor$, $r \leftarrow x - x_0$;
2. 如果$r = 0$, 则终止并输出$x = [x_0]$. 否则, 令$x_1 \leftarrow \lfloor \frac{1}{r} \rfloor$, $r \leftarrow \frac{1}{r} - x_1$;
3. 如果$r = 0$, 则终止并输出$x = [x_0, x_1]$. 否则, 令$x_2 = \lfloor \frac{1}{r} \rfloor$, $r \leftarrow \frac{1}{r} - x_2$;
4. 如果$r = 0$, 则终止并输出$x = [x_0, x_1, x_2]$. 否则, 令$x_3 = \lfloor \frac{1}{r} \rfloor$, $r \leftarrow \frac{1}{r} - x_3$;
5. 如此继续下去...
6. 如果$r = 0$, 则终止并输出$x = [x_0, x_1, x_2, \cdots, x_k]$. 否则, 令$x_{k+1} = \lfloor \frac{1}{r} \rfloor$, $r \leftarrow \frac{1}{r} - x_{k+1}$;
7. 如此继续下去, 在需要的时候停止运算, 得到实数x的一个简单连分数逼近.

特别地, 如果x是有理数, 上述过程在有限步结束, 即得到x的有限简单连分数表示.

3. 有理分数的有限简单连分数表示

设$x=\frac{p}{q}$是有理数, 其中p和q为整数.

$$\frac{p}{q}=\lfloor\frac{p}{q}\rfloor+\cfrac{1}{\cfrac{1}{\frac{p}{q}-\lfloor\frac{p}{q}\rfloor}}=\lfloor\frac{p}{q}\rfloor+\cfrac{1}{\cfrac{q}{p-q\lfloor\frac{p}{q}\rfloor}}=\lfloor\frac{p}{q}\rfloor+\cfrac{1}{\cfrac{q}{r_0}},$$

其中$r_0=p-q\lfloor\frac{p}{q}\rfloor$, $p=q\lfloor\frac{p}{q}\rfloor+r_0$, 即$r_0$是欧几里得除法中的余数, 且$0\leq r_0<q$.

接下来, 对于$\frac{q}{r_0}$, 类似地有

$$\frac{q}{r_0}=\lfloor\frac{q}{r_0}\rfloor+\cfrac{1}{\cfrac{1}{\frac{q}{r_0}-\lfloor\frac{q}{r_0}\rfloor}}=\lfloor\frac{q}{r_0}\rfloor+\cfrac{1}{\cfrac{r_0}{q-r_0\lfloor\frac{q}{r_0}\rfloor}}=\lfloor\frac{q}{r_0}\rfloor+\cfrac{1}{\cfrac{r_0}{r_1}},$$

其中$q=r_0\lfloor\frac{q}{r_0}\rfloor+r_1$, 即$r_1$是欧几里得除法中的余数, 且$0\leq r_1<r_0$.

再接下来, 对于$\frac{r_0}{r_1}$, 类似地有$r_0 = r_1\lfloor\frac{r_0}{r_1}\rfloor + r_2$, 且$0 \le r_2 < r_1$.
再接下来, 对于$\frac{r_1}{r_2}$, 类似地有$r_1 = r_2\lfloor\frac{r_1}{r_2}\rfloor + r_3$, 且$0 \le r_3 < r_2$.
如此进行下去, 一定存在整数$k \ge 0$使得$r_0 > r_1 > r_2 > \ldots > r_k > r_{k+1} = 0$, 从而使得上述辗转相除法过程结束.

因此, 对于有理数$x = \frac{p}{q}$, 可以使用辗转相除法, 计算得到它的有限简单连分数表示

$$\frac{p}{q} = [\lfloor\frac{p}{q}\rfloor, \lfloor\frac{q}{r_0}\rfloor, \lfloor\frac{r_0}{r_1}\rfloor, \lfloor\frac{r_1}{r_2}\rfloor, \cdots, \lfloor\frac{r_{k-1}}{r_k}\rfloor],$$

其中, 对于$1 \le i \le k$有$r_i = r_{i-1}\lfloor\frac{r_{i-1}}{r_i}\rfloor + r_{i+1}$, 且$r_{k+1} = 0$.

定理

给定两个有限简单连分数$[a_0, a_1, \ldots, a_n]$和$[b_0, b_1, \ldots, b_s]$, 其中$a_n \ge 2$和$b_n \ge 2$均为整数. 如果$[a_0, a_1, \ldots, a_n] = [b_0, b_1, \ldots, b_s]$, 则必有$s = n, a_j = b_j (j = 0, 1, \ldots, s)$

证明: 对n使用数学归纳法

当$n=0$时, 如果$s\geq 1$的话,

$$a_0=[b_0,b_1,\dots,b_s]=[b_0,[b_1,\dots,b_s]]=b_0+\frac{1}{[b_1,\dots,b_s]}$$

因为$b_s>1$, 所以$[b_1,\dots,b_s]>1$, 于是, 上式不可能成立(左边是整数,右边是分数).
这样$s=0$, 从而$a_0=b_0$. 假设$n=k$时结论成立, 当$n=k+1$时,

$$[a_0,a_1,\dots,a_k,a_{k+1}]=a_0+\frac{1}{[a_1,\dots,a_{k+1}]},\quad [b_0,\dots,b_s]=b_0+\frac{1}{[b_1,\dots,b_s]}$$

又因为$a_{k+1}>1\Longrightarrow[a_1,\dots,a_{k+1}]>1$, 以及$b_s>1\Longrightarrow[b_1,\dots,b_s]>1$, 从而有

$$[a_0,\dots,a_k,a_{k+1}]=[b_0,\dots,b_s]\Longrightarrow a_0+\frac{1}{[a_1,\dots,a_{k+1}]}=b_0+\frac{1}{[b_1,\dots,b_s]}$$

$$\Longrightarrow\begin{cases} a_0=b_0 \\ \dfrac{1}{[a_1,\dots,a_{k+1}]}=\dfrac{1}{[b_1,\dots,b_s]}\Longrightarrow[a_1,\dots,a_{k+1}]=[b_1,\dots,b_s]\end{cases}$$

此时可以使用归纳假设, 得到$a_1=b_1,\dots$ $\diamond$

对于一个分子和分母很大的分数, 可以找到一个分子和分母较小的数来近似它.

$$
\begin{aligned}
\frac{103993}{33102} &= 3+\frac{4687}{33102} = 3+\frac{1}{\frac{33102}{4687}} = 3+\frac{1}{7+\frac{293}{4687}} \\
&= 3+\frac{1}{7+\frac{1}{\frac{4687}{293}}} = 3+\frac{1}{7+\frac{1}{15+\frac{292}{293}}} \\
&= 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{292}}}}
\end{aligned}
$$

扔掉这些'分数'中小于1的数可以得到$\frac{103993}{33102}$的近似值:

$$
3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \ldots
$$

它们的近似效果依次变好.

2. 有限连分数的性质

在讨论有限连分数$[x_0, x_1, \ldots, x_n]$性质时，总假设x_0是实数，$x_1, x_2, \ldots, x_n$为正实数.

1 **连分数'嵌套'**

$$[x_0, x_1, \ldots, x_{n-1}, x_n, x_{n+1}, \ldots, x_{n+r}] = [x_0, x_1, \ldots, x_{n-1}, [x_n, x_{n+1}, \ldots, x_{n+r}]]$$

例如,

$$-3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{3 + \cfrac{1}{5 + \cfrac{1}{9 + \cfrac{1}{100}}}}}} = -3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{\left(3 + \cfrac{1}{5 + \cfrac{1}{9 + \cfrac{1}{100}}}\right)}}}$$

即$[-3, 2, 4, 3, 5, 9, 100] = [-3, 2, 4, \bigstar]$, 其中$\bigstar = [3, 5, 9, 100]$.
所以, $[-3, 2, 4, 3, 5, 9, 100] = [-3, 2, 4, [3, 5, 9, 100]]$.

事实上, 又可以看到:

$$[3,5,9,100] = 3 + \frac{1}{\left(5 + \frac{1}{9 + \frac{1}{100}}\right)}$$

所以又有

$$[-3,2,4,3,5,9,100] = [-3,2,4,[3,5,9,100]] = [-3,2,4,3 + \frac{1}{[5,9,100]}]$$

所以, 关于连分数‘嵌套’, 我们还有

2 **连分数‘嵌套’**

$$\begin{aligned}
&[x_0, x_1, x_2, \ldots, x_{n-1}, x_n, x_{n+1}, \ldots, x_{n+r}] \\
=&[x_0, x_1, x_2, \ldots, x_{n-1}, [x_n, x_{n+1}, \ldots, x_{n+r}]] \\
=&[x_0, x_1, x_2, \ldots, x_{n-1}, x_n + \frac{1}{[x_{n+1}, \ldots, x_{n+r}]}].
\end{aligned}$$

设实数$\eta > 0$, 可以验证

$$-3+\cfrac{1}{2+\cfrac{1}{4}} < -3+\cfrac{1}{2+\cfrac{1}{4+\eta}}.$$

$$-3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{5}}}} < -3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{5+\eta}}}}$$

一般地,

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2}} < x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\eta}}.$$

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{x_4}}}} < x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{x_4+\eta}}}}$$

于此同时, 还可以验证

$$-3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3}}} > -3+\cfrac{1}{2+\cfrac{1}{4+\frac{1}{3\eta}}}$$

$$-3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{9}}}}} > -3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{9+\eta}}}}}$$

一般地,

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3}}} > x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\frac{1}{x_3+\eta}}}$$

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{x_4+\cfrac{1}{x_5}}}}} > x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{x_4+\cfrac{1}{x_5+\eta}}}}}$$

更一般地，我们有

3 偶数阶连分数'加η递增'

$$[x_0, x_1, x_2, \ldots, x_{2k-1}, x_{2k}] < [x_0, x_1, x_2, \ldots, x_{2k-1}, x_{2k} + \eta]$$

4 奇数阶连分数'加η递减'

$$[x_0, x_1, x_2, \ldots, x_{2k}, x_{2k+1}] > [x_0, x_1, x_2, \ldots, x_{2k}, x_{2k+1} + \eta]$$

设实数$\eta > 0$, 可以验证

$$-3+\cfrac{1}{2+\cfrac{1}{4}} < -3+\cfrac{1}{2+\cfrac{1}{4+\eta}}.$$

$$-3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{5}}}} < -3+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{5+\eta}}}}$$

一般地,

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2}} < x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\eta}}.$$

$$x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{x_4}}}} < x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{x_4+\eta}}}}$$

因为

$$[x_0, x_1, x_2, \ldots, x_{2k-1}, x_{2k}] < [x_0, x_1, x_2, \ldots, x_{2k-1}, x_{2k} + \eta]$$

结合连分数的'嵌套'性质，令$\eta = \frac{1}{x_{2k+1}}$，于是有

$$[x_0, x_1, \ldots, x_{2k-1}, x_{2k}] < [x_0, x_1, \ldots, x_{2k-1}, x_{2k} + \frac{1}{x_{2k+1}}] = [x_0, x_1, \ldots, x_{2k}, x_{2k+1}]$$

类似地，

$$\begin{aligned} [x_0, x_1, \ldots, x_{2k-1}, x_{2k}] &< [x_0, x_1, \ldots, x_{2k-1}, x_{2k} + \frac{1}{x_{2k+1} + \frac{1}{x_{2k+2}}}] \\ &= [x_0, x_1, \ldots, x_{2k}, x_{2k+1}, x_{2k+2}]. \end{aligned}$$

更一般地，令$\eta = 1/[x_{2k+1}, x_{2k+2}, \ldots, x_{2k+r}]$，我们有

5 偶数阶连分数'加r阶递增'

$$[x_0, x_1, \ldots, x_{2k-1}, x_{2k}] < [x_0, x_1, \ldots, x_{2k}, x_{2k+1}, x_{2k+2}, \ldots, x_{2k+r}],$$

其中$r \geq 1$. 记$\theta_n = [x_0, x_1, \ldots, x_n]$，则有

$$\theta_{2k} < \theta_{2k+r} \quad (r \geq 1)$$

同理, 因为

$$[x_0, x_1, x_2, \ldots, x_{2k}, x_{2k+1}] > [x_0, x_1, x_2, \ldots, x_{2k}, x_{2k+1} + \eta]$$

结合连分数的'嵌套'性质, 令$\eta = \frac{1}{x_{2k+2}}$, 于是有

$$[x_0, x_1, \ldots, x_{2k}, x_{2k+1}] > [x_0, x_1, \ldots, x_{2k}, x_{2k+1} + \frac{1}{x_{2k+2}}] = [x_0, x_1, \ldots, x_{2k+1}, x_{2k+2}].$$

类似地,

$$\begin{aligned}[x_0, x_1, \ldots, x_{2k}, x_{2k+1}] &> [x_0, x_1, \ldots, x_{2k}, x_{2k+1} + \frac{1}{x_{2k+2} + \frac{1}{x_{2k+3}}}] \\ &= [x_0, x_1, x_2, \ldots, x_{2k+1}, x_{2k+2}, x_{2k+3}].\end{aligned}$$

更一般地, 令$\eta = 1/[x_{2k+2}, x_{2k+2}, \ldots, x_{2k+1+r}]$, 我们有

6 奇数阶连分数'加r阶递减'

$$[x_0, x_1, \ldots, x_{2k}, x_{2k+1}] > [x_0, x_1, \ldots, x_{2k+1}, x_{2k+2}, x_{2k+3}, \ldots, x_{2k+1+r}],$$

其中$r \geq 1$. 记$\theta_n = [x_0, x_1, \ldots, x_n]$, 则有

$$\theta_{2k+1} > \theta_{2k+1+r} \quad (r \geq 1)$$

8 连分数$[x_0,x_1,x_2,x_3,\ldots]$的第$n(\geq 0)$个渐近分数$[x_0,x_1,\ldots,x_n]=\dfrac{P_n}{Q_n}$满足

$$P_n = x_nP_{n-1}+P_{n-2},\quad Q_n = x_nQ_{n-1}+Q_{n-2},$$

且$P_{-2}=0, P_{-1}=1, Q_{-2}=1, Q_{-1}=0$

对n使用数学归纳法: $n=0$的时候直接检验:

$$P_0 = x_0P_{-1}+0 = x_0, Q_0 = x_0\cdot 0+Q_{-2} \Longrightarrow \frac{P_0}{Q_0}=x_0$$

假设$n=k$时结论成立, 需要说明$n=k+1$时结论也成立.

此时, 使用归纳假设, 我们有

$$[x_0,x_1,\ldots,x_k+\frac{1}{x_{k+1}}] = \frac{(x_k+\frac{1}{x_{k+1}})P_{k-1}+P_{k-2}}{(x_k+\frac{1}{x_{k+1}})Q_{k-1}+Q_{k-2}}$$

$$= \frac{(x_kx_{k+1}+1)P_{k-1}+x_{k+1}P_{k-2}}{(x_kx_{k+1}+1)Q_{k-1}+x_{k+1}Q_{k-2}} = \frac{x_{k+1}(x_kP_{k-1}+P_{k-2})+P_{k-1}}{x_{k+1}(x_kQ_{k-1}+Q_{k-2})+Q_{k-1}}$$

$$= \frac{x_{k+1}P_k+P_{k-1}}{x_{k+1}Q_k+Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}}.$$

这个结论也给出了一种求连分数的方法.

8c 连分数$[x_0,x_1,x_2,x_3,\ldots]$的第$n(\geq -1)$个渐近分数$[x_0,x_1,\ldots,x_n]=\dfrac{P_n}{Q_n}$满足

$$\theta_n-\theta_{n-1}=\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{P_nQ_{n-1}-Q_nP_{n-1}}{Q_nQ_{n-1}}=\frac{(-1)^{n+1}}{Q_nQ_{n-1}}\quad(n\geq -1)$$

8d 连分数$[x_0,x_1,x_2,x_3,\ldots]$的第$n(\geq 0)$个渐近分数$[x_0,x_1,\ldots,x_n]=\dfrac{P_n}{Q_n}$满足

$$\theta_n-\theta_{n-2}=\frac{P_n}{Q_n}-\frac{P_{n-2}}{Q_{n-2}}=\frac{P_nQ_{n-2}-P_{n-2}Q_n}{Q_nQ_{n-2}}=\frac{(-1)^nx_n}{Q_nQ_{n-2}}\quad(n\geq 0)$$

4. 无限连分数的性质

定理

无限简单连分数$[x_0,x_1,x_2,\cdots]$一定是收敛的，即一定存在实数θ极限$\lim_{k\to\infty}\theta_k=\theta$，其中$\theta_k$是其第$k$个渐近连分数.

下标为奇数的渐进分数序列是有下界θ_0的严格递减数列，所以$\lim_{n\to\infty}\theta_{2n-1}=\theta''$
下标为偶数的渐近分数序列是有上届θ_1的严格递增数列，所以$\lim_{n\to\infty}\theta_{2n}=\theta'$.
于是,

$$\theta_1>\theta_3>\theta_5>\theta_7>\ldots>\theta'' \qquad \theta'>\ldots>\theta_6>\theta_4>\theta_2>\theta_0$$

又因为任意下标为奇数渐近分数值都>任意下标为偶数的渐近分数值，所以有这表明

$$0\le\theta''-\theta'\le\theta_{2k-1}-\theta_{2k}=\frac{1}{Q_{2k-1}Q_{2k}}$$

对无限简单连分数，可以看到

$$1=Q_0\le x_1=Q_1<Q_2<Q_3<Q_4<\ldots<Q_k<\ldots$$

，即当$k\to\infty$时$Q_k\longrightarrow\infty$，所以，$\theta'=\theta''$ $\diamond$