arXiv:2302.00505v1 [math.NT] 1 Feb 2023

关于 Pisot 单位与 $\mathbb{Q}$的伽罗瓦扩张的基本域

Christian Porter、Alexandre Bali、Alar Leibak

2023年2月2日

摘要

本文给出了两个主要结果。设 K 是一个数域，它以次数 $r+2s$伽罗瓦扩张于 $\mathbb{Q}$，其中 r 是实嵌入的数量， s 是复嵌入对的数量。第一个结果表明， K 的约化域（因而也是基本域）的面数不超过$O\left(\left(\frac{1}{2}(r+s-1)^{\delta}(r+s)^{1+\frac{1}{(r+s-1)}}\right)^{r+s-1}\right)\cdot\left(e^{1+\frac{1}{2e}}\right)^{r+s}(r+s)!$，其中，若 $r+s\leq 11$，则 $\delta=1/2$；否则 $\delta=1$。第二个结果表明，存在一种线性时间算法，可以约化全正一元型 axx^*，使得与 a 等价的新全正元素 a'的迹不超过迹型 Tr(axx^*) 的整数最小值乘以一个常数；该常数由此数域中的最短 Pisot 单位决定。这可能应用于基于环的密码学。最后，我们证明此数域中最短 Pisot 单位的韦伊高度不超过$[K:\mathbb{Q}]^{\frac{1}{2}}\left(\frac{\gamma}{2}(r+s-1)^{\delta-\frac{1}{(r+s-1)}}R_K^{\frac{1}{r+s-1}}+(r+s-1)\epsilon\right)$，其中 R_K 表示 K的调节子；若 K 是全实的，则 $\gamma=1$；否则为 2；而 $\epsilon>0$ 是某个任意小的常数。

1 引言

设 K 是一个次数为 $n=r+2s$ 的代数域（其中 r 是实嵌入的个数， s 是复嵌入对的个数），它是 $\mathbb{Q}$ 上的扩张，其整数环为 $\mathcal{O}_K$，单位群为 $\mathcal{O}_K^*$。我们将典范嵌入 $\sigma_1,\ldots,\sigma_r,\sigma_{r+1},\ldots,\sigma_{r+s},\ldots,\sigma_{r+2s}$ 与 K 对应起来，它们嵌入到 $\mathbb{C}$ 中，其中 $\sigma_{r+s+k}(x)=\sigma_{r+k}(x)^*$ 对所有 $1\leq k\leq s$ 都成立，而 $*$ 表示复共轭。

定义 $K_{\mathbb{R}}=K\otimes_{\mathbb{Q}}\mathbb{R}$。注意到 $K_{\mathbb{R}}=\mathbb{R}^r\times\mathbb{C}^s$。我们定义典范对合 $*\colon K_{\mathbb{R}}\to K_{\mathbb{R}}$，它在 $\mathbb{R}^r$ 上作用为恒等映射，在 $\mathbb{C}^s$ 上作用为复共轭。对于任意 $\alpha=(\alpha_1,\ldots,\alpha_{r+s})$ $\beta=(\beta_1,\ldots,\beta_{r+s})\in K_{\mathbb{R}}$，定义 $\alpha\beta=(\alpha_1\beta_1,\alpha_2\beta_2,\ldots,\alpha_{r+s}\beta_{r+s})$。若元素 $\alpha=(\alpha_1,\ldots,\alpha_{r+s})\in K_{\mathbb{R}}$ 的每个 $\alpha_i\in\mathbb{R}^+$ 都为正，则称其为全正的。本文中，我们将假设所考虑的任意数域 K 都是 $\mathbb{Q}$ 上的 Galois 扩张。事实上，只有引理 3 需要这一性质，但遗憾的是，该引理对于证明本文的结果至关重要，因此我们必须将讨论限于此类域。

考虑

$$\mathrm{Tr}(axx^*),\quad x,a\in K_{\mathbb{R}},$$

其中 a 是全正元素。它生成一个维数为 $r+s$ 的实正定二次型。我们称 axx^* 为一元型。

我们将 $\mathcal{O}_{K_\mathbb{R}}$ 定义为元素集 $(\sigma_1(x)\ldots,\sigma_{r+s}(x))$，其中 $x\in\mathcal{O}_K$；并将 $\mathcal{O}^*_{K_\mathbb{R}}$ 定义为满足 $u\in\mathcal{O}^*_K$的元素集 $(\sigma_1(u)\ldots,\sigma_{r+s}(u)$。若全正元素 a 满足

$$\mathrm{Tr}(a)\le\mathrm{Tr}(avv^*), \tag{1}$$

对所有 $v\in\mathcal{O}^*_{K_\mathbb{R}}$均成立，则称其为约化的。若 $v=(\sigma_1(u)\ldots,\sigma_{r+s}(u))$，我们用记号 $v^{-1}=(\sigma_1(u^{-1})\ldots,\sigma_{r+s}(u^{-1}))\in\mathcal{O}^*_{K_\mathbb{R}}$。若对于某个 $v\in\mathcal{O}^*_{K_\mathbb{R}}$有 $a'=avv^*$，则称两个全正元素 a、a' 等价。注意，由于 $a=a'v^{-1}v^{-1*}$，a 可由其等价类表示，其中等价关系由将 a 乘以满足 $v\in\mathcal{O}^*_{K_\mathbb{R}}$的 vv^* 来确定，因此实二次型 $\mathrm{Tr}(axx^*)$、$\mathrm{Tr}(a'xx^*)$等价。$K_\mathbb{R}$的约化域记为$\mathcal{F}_{K_\mathbb{R}}$，它是 $K_\mathbb{R}$中所有约化的全正元素组成的集合，因此显然每个正元素都等价于 $\mathcal{F}_{K_\mathbb{R}}$中的一个元素。注意，约化域是 K的全正元素集合的一个基本域。已知约化域是有限多个完美锥的并（[2, Satz 4]）。在 [3], 中，确定了任意给定全实数域中完美一元形式数量的一个上界。锥 $\mathcal{F}_K$ 的面由不等式 1 定义，并且已知约化域的面数量有限；这意味着只需满足有限多个不等式，即可判断一元型是否为约化的。

设 $x\in\mathcal{O}_K$ 是 K 的代数整数。若 x 的绝对值大于 1，而除对应于复共轭的共轭外，其所有伽罗瓦共轭的绝对值都小于 1，则称 x 为 Pisot–Vijayaraghavan数（简称 Pisot数）。若 $x\in\mathcal{O}^*_K$，则称 x 为 Pisot 单位。

由狄利克雷单位定理可知，$\mathcal{O}^*_K$ 的秩为 $r+s-1$。因此，假设 $\mathcal{O}^*_K$ 由元素 u_1、u_2、...、u_{r+s-1} 和 ζ 乘法生成，其中 ζ 是 $\mathcal{O}_K$ 中的某个单位根。考虑对数嵌入：

$$\begin{aligned}\mathrm{Log}:K\to\mathbb{R}^{r+s}:\mathrm{Log}(x)=&(\log(|\sigma_1(x)|),\log(|\sigma_2(x)|),\ldots,\log(|\sigma_r(x)|),\\&2\log(|\sigma_{r+1}(x)|),2\log(|\sigma_{r+2}(x)|),\ldots,2\log(|\sigma_{r+s}(x)|)).\end{aligned}$$

注意，在对数嵌入下，$\Lambda_K:=\mathrm{Log}(\mathcal{O}^*_K)$ 在空间中生成一个格

$$V=\left\{(x_1,\ldots,x_{r+s})\in\mathbb{R}^{r+s}:\sum_{i=1}^{r+s}x_i=0\right\}. \tag{2}$$

设 $\mathbf{v}\|$ 是元素 $\mathbf{v}\in\mathbb{R}^{r+s}$ 的 l_p 范数。本文中，我们将使用如下记号

$$\rho^p(\Lambda)=\max_{x\in W}\min_{v\in\Lambda_K}\|x-v\|_p$$

对于任意格 Λ，其中 W 是 Λ 满秩所在的空间。我们还将使用以下记号

$$\lambda_{i,K}(\Lambda)=\min\{c\in\mathbb{R}_{\ge0}:\dim(\Lambda\cap cK)=i\},$$

称为 Λ的第 i 个逐次极小值，而 K 是某个 0 对称凸体。我们将使用记号 $\lambda_{i,\ p}(\Lambda)$ 表示相对于由 l_p-范数定义的凸体， Λ 的第 i 个逐次极小值。

本文旨在证明以下结果。

定理 1. 设 N_K 表示 $K_{\mathbb{R}}$的约化域的面数。那么

$$\begin{aligned} N_K <& 2(r+s-1) \\ &+ 2\left(\frac{1}{2}(r+s-1)^{\delta}(r+s)^{1-\frac{1}{2(r+s-1)}} + \frac{r+s-1}{2}\frac{\log\left(\frac{r+s+1}{r+s-1}\right)}{R_K^{\frac{1}{r+s-1}}} + \frac{\log\left(\frac{r+s-1}{2}\right)}{R_K^{\frac{1}{r+s-1}}}\right)^{r+s-1} \\ &\cdot (r+s)\sum_{k=0}^{\lfloor\frac{r+s}{2}\rfloor}(-1)^k\binom{r+s}{k}\left(\frac{r+s}{2}-k\right)^{r+s-1}, \end{aligned}$$

其中

$$\delta = \begin{cases} 1/2, & 1 \le r+s-1 \le 10, \\ 1, & 10 < r+s-1. \end{cases}$$

且 R_K 是 K的调节子。

利用引理 9，以及对所有数域 K [11]都有 $R_K > 0.2052\ldots$这一事实，可得

$$N_K < O\left(\left(\frac{1}{2}(r+s-1)^{\delta}(r+s)^{1-\frac{1}{2(r+s-1)}}\right)^{r+s-1}\right)\cdot\left(e^{1+\frac{1}{2e}}\right)^{r+s}(r+s)!.$$

数值证据似乎表明，上述表达式中的项 $\left(e^{1+\frac{1}{2e}}\right)^{r+s}$ 也可以省略。

代数数 x in K 的对数魏尔高度定义为

$$h(x) = \frac{1}{[K:\mathbb{Q}]}\left(\sum_{i=1}^{r}\log^{+}|\sigma_i(x)| + 2\sum_{i=1}^{s}\log^{+}|\sigma_i(x)|\right),$$

其中 $\log^{+}(\alpha) = \max\{\log(\alpha)\ 0\}$。我们还证明了以下有趣的命题，对魏尔高度最小的 Pisot 单位的高度给出了上界。

命题 1. 对所有 $\epsilon > 0$，都存在一个魏尔高度为 $h(u)$ 的 Pisot 单位，使得

$$h(u) \le \frac{1}{[K:\mathbb{Q}]}\left(\frac{\gamma}{2}(r+s-1)^{\delta-\frac{1}{2(r+s-1)}}R_K^{\frac{1}{r+s-1}} + (r+s-1)\epsilon\right),$$

其中 δ 的定义同前；若 K 是全实的，则为 $\gamma = 1$；若 K 是全复的，则为 $\gamma = 2$。

利用本文提出的思路，我们还给出了一种约化一元形式的算法，该算法可能应用于基于环的密码学（参见例如 [4], [5], [6]）。

定理 2. 对任意全正元素 $a \in K_{\mathbb{R}}$，定义为

$$\mu(a) \triangleq \min_{x \in \mathcal{O}_{K_{\mathbb{R}}} \setminus \{0\}} Tr(axx^*).$$

那么，给定一个全正元素 a、一个 Pisot 单位 u 和某个参数 $\min_{j \neq 1} |\sigma_j(u)|^2 < \delta < 1$，存在一种算法，可以计算出一个与之等价的元素 a'，使得

$$Tr(a') \leq \max \left\{ \frac{t_K(u,\delta)^2}{\min_{x \in \mathcal{S}} Tr(xx^*)}, 1 \right\} \mu(a), \tag{3}$$

其中

$$t_K(u,\delta) = \sqrt{1 + \frac{|u|^2 - \delta}{\delta - \max_{j \neq 1} |\sigma_j(u)|^2}},$$

而 $\mathcal{S}$ 表示 $\mathcal{O}_{K_{\mathbb{R}}}$ 中在 $\mathcal{O}_K$ 内不对应于单位根或零的元素。另外，如果

$$\mu(a) = Tr(axx^*)$$

对于某个 $x \in \mathcal{O}_{K_{\mathbb{R}}}$，那么

$$Tr(xx^*) \leq t_K(u,\delta)^2.$$

此外，该算法至多需要 $\mathcal{O}(\log(X)((r+s+1)\log(X) + (r+s)\log(\max_i |\sigma_i(u)|)))$ 次位操作，其中 $X = \max_i a_i$，其中 $a = (a_1, \ldots, a_{r+s})$。

2 利用 Pisot 单位约简一元形式及若干有用引理

命题 2. 如果 K 既不是 $\mathbb{Q}$，也不是虚二次（即具有非平凡的单位群），那么对于任意 $\varepsilon > 0$，都存在一个 Pisot 单位 u，使得

$$\begin{aligned} e^{(r+s-2)\rho^\infty(\Lambda_K)+(r+s-1)\varepsilon} \leq & |u| \leq e^{(r+s)\rho^\infty(\Lambda_K)+(r+s-1)\varepsilon}, \\ e^{-(2\rho^\infty+\varepsilon)} \leq & |\sigma_i(u)| \leq e^{-\varepsilon}, \end{aligned}$$

对所有 $i \neq 1$均成立。

证明。如果 u 是一个 Pisot 单位，那么显然，对于任何不对应于复共轭的伽罗瓦共轭σ，$\log(|u|) > 0$，且 $\log(|\sigma(u)|) < 0$。设 $x = (x_1, \ldots, x_{r+s})$ 是V的一个元素。根据定义，$\sum_{i=1}^{r+s} x_i = 0$，并且

$$\min_{w \in \Lambda_K} \|x - w\|_\infty = \|x - v\|_\infty = \max_{1 \leq i \leq r+s} |x_i - v_i| \leq \rho^\infty(\Lambda_K),$$

对于某个适当的 $v=(v_1,\dots,v_{r+s})\in\Lambda_K$。令 $x_1=(r+s-1)\rho^\infty(\Lambda_K)+(r+s-1)\varepsilon$，$x_2=x_3=\cdots=x_{r+s}=-\rho^\infty(\Lambda_K)-\varepsilon$，其中 $\varepsilon>0$。那么我们必有

$$\begin{aligned}
&|(r+s-1)\rho^\infty(\Lambda_K)-v_1+(r+s-1)\varepsilon|\le\rho^\infty(\Lambda_K),\\
&|v_2+\rho^\infty(\Lambda_K)+\varepsilon|\le\rho^\infty(\Lambda_K),\\
&|v_3+\rho^\infty(\Lambda_K)+\varepsilon|\le\rho^\infty(\Lambda_K),\\
&\vdots\\
&|v_{r+s}+\rho^\infty(\Lambda_K)+\varepsilon|\le\rho^\infty(\Lambda_K).
\end{aligned}$$

显然，如果 K 既不是 $\mathbb{Q}$ 也不是虚二次域，则 $\rho^\infty(\Lambda_K)$ 非零，因此这些不等式给出以下不等式:

$$\begin{aligned}
0<(r+s-2)\rho^\infty(\Lambda_K)+(r+s-1)\varepsilon\le& v_1\le(r+s)\rho^\infty(\Lambda_K)+(r+s-1)\varepsilon,\\
-2\rho^\infty(\Lambda_K)-\varepsilon\le& v_2\le-\varepsilon<0,\\
-2\rho^\infty(\Lambda_K)-\varepsilon\le& v_3\le-\varepsilon<0,\\
&\vdots\\
-2\rho^\infty(\Lambda_K)-\varepsilon\le& v_{r+s}\le-\varepsilon<0,
\end{aligned}$$

这就证明了该引理。 □

引理 3. 设 $a=(a_1,a_2,\dots,a_{r+s})\in K_{\mathbb{R}}$ 是一个全正元素。令 $u\in\mathcal{O}_K^*$为一个 Pisot 单位，并设

$$Tr(av_iv_i^*)\ge Tr(a),$$

对所有 $1\le i\le r+2s$ 其中 v_i 是将 $\sigma_i(u)$嵌入到 $K_{\mathbb{R}}$中所得到的 $K_{\mathbb{R}}$ 的元素。令

$$t_K(u)=\sqrt{1+\frac{|u|^2-1}{1-\max_{2\le j\le r+s}|\sigma_j(u)|^2}}.$$

那么，对任意满足 $\mathrm{Tr}(xx^*)\ge t_K(u)^2$, $\mathrm{Tr}(axx^*)\ge\mathrm{Tr}(a)$ 的 $x\in K_{\mathbb{R}}$,

证明。根据假设，对于每个 $1\le i\le r+2s$,

$$\begin{aligned}
&\mathrm{Tr}(av_iv_i^*)=\left(\sum_{j=1}^{r}+2\sum_{j=r+1}^{r+s}\right)a_j|\sigma_j(\sigma_i(u))|^2\ge\mathrm{Tr}(a)=\left(\sum_{j=1}^{r}+2\sum_{j=r+1}^{r+s}\right)a_j\\
\iff&\left(\sum_{j=1}^{r}+2\sum_{j=r+1}^{r+s}\right)a_j(|\sigma_j(\sigma_i(u))|^2-1)\ge0.
\end{aligned}$$

假设对于某个 k 的值，有 $|\sigma_k(\sigma_i(u))|=|u|$。那么

$$\begin{aligned}
&(|u|^2-1)a_k\ge\left(\sum_{j\ne k=1}^{r}+2\sum_{j\ne k=r+1}^{r+s}\right)a_j\ge(1-\max_{j\ne1}|\sigma_j(u)|^2)\left(\sum_{j\ne k=1}^{r}+2\sum_{j\ne k=r+1}^{r+s}\right)a_j\\
\iff&\mathrm{Tr}(a)\le t_K(u)^2a_k.
\end{aligned}$$

遍历 $1 \le i \le r+s$ 的所有取值，我们即可对所有 $1 \le k \le r+s$ 得到上述不等式，因此，如果 $x = (x_1, \dots, x_{r+s}) \in K_{\mathbb{R}}$ 且 $\mathrm{Tr}(xx^*) \ge t_K(u)^2$,

$$\mathrm{Tr}(axx^*) = \sum_{j=1}^{r+s} a_j |x_j|^2 \ge t_K(u)^{-2} \mathrm{Tr}(a) \sum_{j=1}^{r+s} |x_j|^2 = t_K(u)^{-2} \mathrm{Tr}(a) \mathrm{Tr}(xx^*) \ge \mathrm{Tr}(a),$$

如所要求。 □

引理 4。令 $\rho^\infty(\Lambda)$ 表示格 Λ 在 l_∞ 范数下的覆盖半径，其中该格的秩为 n 、体积为 $\mathrm{Vol}(\Lambda)$；并且假设 Λ 是良圆的（即逐次极小值的数值均相等）。则

$$\rho^\infty(\Lambda) \le \begin{cases} \frac{\sqrt{n}}{2} Vol(\Lambda)^{\frac{1}{n}}, & 1 \le n \le 10, \\ \frac{n}{2} Vol(\Lambda)^{\frac{1}{n}}, & 10 < n. \end{cases} \tag{4}$$

证明。为证明第一个不等式，首先注意到 $\rho^\infty(\Lambda) \le \rho^2(\Lambda)$。文献 [7] 已证明，对于所有秩为 n 的格，有 $\rho^2(\Lambda) \le \frac{\sqrt{n}}{2} \mathrm{Vol}(\Lambda)$，其中 $n \le 10$。

对于第二种情形，首先注意到 $\lambda_{i,\infty}(\Lambda) \le \lambda_{i,2}(\Lambda) \le \sqrt{n} \lambda_{i,\infty}(\Lambda)$。众所周知，

$$\rho^2(\Lambda) \le \frac{\sqrt{n}}{2} \lambda_{n,2}(\Lambda),$$

由于假设 Λ 是良圆的，我们得到

$$\rho^\infty(\Lambda) \le \rho^2(\Lambda) \le \frac{\sqrt{n}}{2} \lambda_{n,2}(\Lambda) \le \frac{n}{2} \lambda_{n,\infty}(\Lambda) = \frac{n}{2} \lambda_{1,\infty}.$$

同样众所周知，对于任意格 Λ，都有 $\lambda_{1,\infty} \le \mathrm{Vol}(\Lambda)^{\frac{1}{n}}$，因此第二个不等式成立。

□

引理 5（[8]）。设 $\mathcal{C}(R)$ 表示边长为 R 的 n 维超立方体，并设 V 表示第 2 节中的 $n-1$ 维半平面。那么

$$Vol(\mathcal{C}(R) \cap V) = \frac{R^{n-1}\sqrt{n}}{(n-1)!} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n}{k} \left(\frac{n}{2} - k\right)^{n-1}.$$

引理 6（[9]）。设 K 是秩为 n 的凸 0 对称体。那么

$$|K \cap \mathbb{Z}^n| \le n! \, Vol(K) + n.$$

3 确定 $\mathcal{F}_K$ 的面数上界

定理的证明　　1. 根据引理 3，任意全正元素 $a = (a_1, \dots, a_{r+s}) \in \mathcal{F}_K$ 都有

$$\mathrm{Tr}(axx^*) \ge \mathrm{Tr}(a),$$

对所有 $x \in K_{\mathbb{R}}$，$\mathrm{Tr}(xx^*) \geq t_K^2$，其中 $t_K = \min_{u\in\mathcal{P}} t_K(u)$，而 $\mathcal{P}$是 K的所有 Pisot 单位构成的集合。因此，如果 $u \in \mathcal{O}_{K_{\mathbb{R}}}^*$ 确定约化域的一个面，则它必须满足

$$\mathrm{Tr}(uu^*) \leq t_K^2 \iff \log(\mathrm{Tr}(uu^*)) \leq 2\log(t_K).$$

令 $\epsilon(u) = \max_i\{|\sigma_i(u)|, 1/|\sigma_i(u)| : 1 \leq i \leq r+s\}$。那么，恰有一半的（非平凡）单位群满足 $\epsilon(u) = \max_i |\sigma_i(u)|$，而恰有一半满足 $\epsilon(u) = \max_i |\sigma_i(u)|^{-1}$，因为若 $\epsilon(u) = \max_i |\sigma_i(u)|$，则 $\epsilon(1/u) = \max_i |\sigma_i(u)|^{-1}$。我们只考虑满足$\epsilon(u) = |\sigma_i(u)|$的单位，因此

$$2\log(t_K) \geq \log(\mathrm{Tr}(uu^*)) \geq 2\|\mathrm{Log}(u)\|_\infty,$$

因此，满足 $\epsilon(u) = \max_i |\sigma_i(u)|$ 且可能构成约化域的面的唯一可能单位，必须满足 $\|\mathrm{Log}(u)\|_\infty \leq \log(t_K)$。因此，我们要确定 Λ_K 中包含的格点数，该凸体为

$$C = \left\{x \in \mathbb{R}^{r+s} : \|x\|_\infty \leq \log(t_K)\right\}. \tag{5}$$

现在，由于 Λ_K 在半平面 V 中是满秩的（如 2 中所述），我们需要考虑 0 对称凸体 $C \cap V$。根据引理 5，该形状的体积等于

$$\mathrm{Vol}(C\cap V) = \frac{\log(t_K)^{r+s-1}\sqrt{r+s}}{(r+s-1)!}\sum_{k=0}^{\lfloor\frac{r+s}{2}\rfloor}(-1)^k\binom{r+s}{k}\left(\frac{r+s}{2}-k\right)^{r+s-1}.$$

我们应用将 Λ_K 变换为集合 $\mathbb{Z}^{r+s-1}$的变换，并将其旋转 $\mathbb{R}^{r+s}$，使其位于半平面 V内。然后，对凸体 $C \cap V$应用类似的变换，得到新的凸体 K，其体积为

$$\mathrm{Vol}(K) = \frac{\log(t_K)^{r+s-1}(r+s)}{R_K(r+s-1)!}\sum_{k=0}^{\lfloor\frac{r+s}{2}\rfloor}(-1)^k\binom{r+s}{k}\left(\frac{r+s}{2}-k\right)^{r+s-1},$$

其中 R_K是域 K的调节子，利用 $\mathrm{Vol}(\Lambda_K) = R_K/\sqrt{r+s}$这一事实（见 [10]）。然后根据引理 6，$K$ 内整数格点的数量至多为

$$r+s-1+\frac{\log(t_K)^{r+s-1}(r+s)}{R_K}\sum_{k=0}^{\lfloor\frac{r+s}{2}\rfloor}(-1)^k\binom{r+s}{k}\left(\frac{r+s}{2}-k\right)^{r+s-1}.$$

还需证明 $\log(t_K)$ 的一个界。显然，对于任意 Pisot 单位 u，$\max_{j\neq 1}|\sigma_j(u)|^2 < 1$

$$1 < \frac{1}{1-\max_{j\neq 1}|\sigma_j(u)|^2},$$

so

$$t_K = \min_{u\in\mathcal{P}}\sqrt{1+\frac{|u|^2-1}{1-\max_{j\neq i}|\sigma_j(u)|^2}} < \min_{u\in\mathcal{P}}\sqrt{\frac{|u|^2}{1-\max_{j\neq 1}|\sigma_j(u)|^2}},$$

其中 $\mathcal{P}$ 表示 K 的 Pisot 单位集合。因此，根据引理 2，必有

$$\log(t_K) < (r+s)\rho^{\infty}(\Lambda) + (r+s-1)\epsilon - \log(1-e^{-2\epsilon}),$$

对任意 $\epsilon > 0$。上述不等式右侧在 $\epsilon = \frac{1}{2}(\log(r+s+1) - \log(r+s-1))$ 处取得最小值，由此得到

$$\log(t_K) < (r+s)\rho^{\infty}(\Lambda) + \frac{r+s-1}{2}\log\left(\frac{r+s+1}{r+s-1}\right) + \log\left(\frac{r+s-1}{2}\right).$$

最后，由引理 4 以及对数单位格相对于无穷范数是良圆的这一事实（因为 K 是 Galois 的；例如，若 $\mathrm{Log}(u)$ 是最短向量，则 $\mathrm{Log}(\sigma_i(u))$ 在无穷范数下的长度与之相同，并且存在 $r+s-1$ 个线性无关的此类向量），

$$\rho^{\infty}(\Lambda_K) \le \begin{cases} \frac{\sqrt{r+s-1}}{2\sqrt{r+s}^{\frac{1}{r+s-1}}} R_K^{\frac{1}{r+s-1}}, & 1 \le r+s-1 \le 10, \\ \frac{(r+s-1)}{2\sqrt{r+s}^{\frac{1}{r+s-1}}} R_K^{\frac{1}{r+s-1}}, & 10 < r+s-1. \end{cases}$$

于是，由于我们恰好数出了所需整数格点的一半，得到

$$\begin{aligned} N_K <& 2(r+s-1) \\ &+ 2\left(\frac{1}{2}(r+s-1)^{\delta}(r+s)^{1-\frac{1}{2(r+s-1)}} + \frac{r+s-1}{2}\frac{\log\left(\frac{r+s+1}{r+s-1}\right)}{R_K^{\frac{1}{r+s-1}}} + \frac{\log\left(\frac{r+s-1}{2}\right)}{R_K^{\frac{1}{r+s-1}}}\right)^{r+s-1} \\ &\cdot (r+s)\sum_{k=0}^{\lfloor\frac{r+s}{2}\rfloor}(-1)^k\binom{r+s}{k}\left(\frac{r+s}{2}-k\right)^{r+s-1}, \end{aligned}$$

其中

$$\delta = \begin{cases} 1/2, & 1 \le r+s-1 \le 10, \\ 1, & 10 < r+s-1. \end{cases}$$

□

3.1 [K : 有理数域] = $[K$ 的特殊情形: $\mathbb{Q}] = 3$

当 $[K: \mathbb{Q}] = 3$ 时，可以单独处理，因为在这种情况下，单位群中的每个元素要么是 ± 1，要么是 Pisot 单位、Pisot 单位的逆元、Pisot 单位的共轭元或 Pisot 单位的共轭逆元。我们先证明以下有用的引理。

引理 7. 假设 $\mathbf{b}_1 = (\alpha, \beta, -\alpha-\beta)$ 且 $\mathbf{b}_2 = (\gamma, \delta, -\gamma-\delta)$，其中某些 $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ 满足 $|\alpha|, |\beta|, |\gamma|, |\delta|, |\alpha+\beta|, |\gamma+\delta| > 0$，并假设 $\mathbf{b}_1, \mathbf{b}_2$ 在 $\mathbb{R}$ 上线性无关。再假设 $\mathbf{b}_1, \mathbf{b}_2$ 满足

$$\|\mathbf{b}_1\|_{\infty} \le \|\mathbf{b}_2\|_{\infty} \le \|\mathbf{b}_1 \pm \mathbf{b}_2\|_{\infty}. \tag{6}$$

令 $\mathbf{v} = x\mathbf{b}_1 + y\mathbf{b}_2,$，其中 $x, y \in \mathbb{Z}$。那么，除非 $(|x|, |y|)$ 属于以下集合：

$$S = \{(0,0), (1,0), (0,1), (1,1), (2,1), (1,2)\}, \tag{7}$$

$\|\mathbf{v}\|_{\infty} \ge 2\lambda^{\infty}$。

证明。参见附录。 □

现在，设 K 是 $\mathbb{Q}$ 上次数为 3 的数域。假设向量 $\mathbf{b}_1,\mathbf{b}_2$ 生成 $\mathrm{Log}(\mathcal{O}_K^*)$，并且不失一般性地假设 $\mathbf{b}_1,\mathbf{b}_2$ 满足 6。令 u 表示在对数嵌入下，对应于 $\mathrm{Log}(\mathcal{O}_K^*)$ 中最短非零元素的单位。我们可以假设 u 是 Pisot 单位；否则， u 要么是某个 Pisot 单位的逆元，要么是其共轭（或两者兼具），这不会影响该元素在对数嵌入下的长度。因此

$$t_K(u) = \sqrt{1 + \frac{|u|^2 - 1}{1 - \max_{j\neq 1}|\sigma_j(u)|^2}} < \sqrt{1 + \frac{|u|^2 - 1}{\prod_{j\neq 1}(1 - |\sigma_j(u)|^2)}}.$$

由于 K 是 Galois 的， K 必定是全实的。显然， $1-u^2$ 是代数整数，因此 $|\mathrm{Nm}_{K/\mathbb{Q}}(1-u^2)| \geq 1$，由此得到

$$|\mathrm{Nm}_{K/\mathbb{Q}}(1-u^2)| = (u^2-1)\prod_{j\neq 1}(1-\sigma_j(u)^2) \geq 1 \iff \prod_{j\neq 1}(1-\sigma_j(u)^2) \geq (u^2-1)^{-1},$$

因此

$$t_K(u) < \sqrt{1 + (u^2-1)^2}.$$

不失一般性地假设

$$\mathrm{Tr}(au^2) \geq \mathrm{Tr}(a)$$

（这不失一般性，因为否则我们可以找到一个等价的全正元素 a' ，使得上述条件成立）。根据构造， $\|\mathrm{Log}(u)\|_\infty = \lambda_1^\infty$。采用与上一节构造 5 中凸体时类似的论证，我们要寻找满足下列不等式的整数解

$$\|x\mathbf{b}_1 + y\mathbf{b}_2\|_\infty \leq \frac{1}{2}\log(1 + (\sigma_i(u)^2 - 1)^2) = \frac{1}{2}\log(1 + (\exp(2\lambda^\infty) - 1)^2),$$

由此得到

$$\frac{\|x\mathbf{b}_1 + y\mathbf{b}_2\|_\infty}{\lambda^\infty} \leq \frac{1}{2}\log((1 + (\exp(2\lambda^\infty) - 1)^2)^{1/\lambda^\infty}).$$

不等式右侧在 $\lambda^\infty \to \infty$ 时趋于 2，因此上述方程的解 (x, y) 的绝对值仅限于集合 S 中的值（见 7）。

4 线性复杂度约简算法

通常，当 axx^* 时，我们称型为约化的；不过，约化的概念也可以作更广泛的定义。例如，有理二次型的约化方式包括闵可夫斯基约化 [12], 、Korkin-Zolotarev [13] 和 Lenstra-Lovasz-Lovasz（LLL）约化 [14]。我们给出一种非常简单的算法：给定某个全正元素 $a \in K_\mathbb{R}$，即可找到一个具有“理想”性质的等价全正元素 a' 。

算法 1：简单约化算法。

输入：全正元素 $a \in K_{\mathbb{R}}$、单位 $u \in \mathcal{O}_K^*$ 及其关联元素 $v_i \in \mathcal{O}_{K_{\mathbb{R}}}^*$，其中 v_i 是将 $\sigma_i(u)$ 嵌入到 $K_{\mathbb{R}}$ 后的结果，以及某个实常数 $0 < \delta \leq 1$。

输出：与 a 等价的全正元素 a'。

1 设定 $j = 1$。

2 如果 $j = r + s$，返回 a 并结束算法。

3 如果 $\mathrm{Tr}(av_jv_j*) < \delta \mathrm{Tr}^{K/\mathbb{Q}}(a)$，设置 $a \to av_jv_j^*$ 并返回步骤 1。否则，设置 $j \to j + 1$ 并返回步骤 2。

命题 3。输入为 δ、b 和 u，且假设 δ 严格小于 1，算法 1 至多执行 $\mathcal{O}(\log(X)((r+s+1)\log(X) + (r+s)\log(\max_i |\sigma_i(u)|)))$ 次位操作，其中 $X = \max_i a_i$，其中 $a = (a_1, \ldots, a_{r+s})$。

证明。显然，算法的每一轮完整迭代要么导致算法终止，要么我们找到某个等价的 a'，使得 $\mathrm{Tr}(a') < \delta \mathrm{Tr}(a)$；因此，由于 $\delta < 1$，算法最多只能执行 $\mathcal{O}(\log(X))$ 轮。在最坏情况下，一轮完整迭代需要计算 $\mathrm{Tr}(av_jv_j^*)$ 的值 $r + s$ 次。a_i 的值有上界 X，而 $|\sigma_j(u)|$ 的值有上界 $\max_j |\sigma_j(u)|$，因此一轮最多需要 $\mathcal{O}((r+s)\log(\max_i |\sigma_i(u)|) + (r+s+1)\log(X))$ 次位运算。 □

定理 8. 假设算法 1 的输入是全正元素 $a = (a_1, a_2, \ldots, a_{r+s}) \in K_{\mathbb{R}}$、Pisot 单位 u 以及某个参数 $0 < \delta \leq 1$，并输出某个与 a 等价的 $a' = (a'_1, a'_2, \ldots, a'_{r+s})$。记

$$\mu(a) \triangleq \min_{x \in \mathcal{O}_{K_{\mathbb{R}}} \setminus \{0\}} Tr(axx^*).$$

Then

$$Tr(a') \leq \max\left\{\frac{t_K(u,\delta)^2}{\min_{x \in \mathcal{S}} Tr(xx^*)}, 1\right\} \mu(a), \tag{8}$$

其中

$$t_K(u,\delta) = \sqrt{1 + \frac{|u|^2 - \delta}{\delta - \max_{j \neq 1} |\sigma_j(u)|^2}},$$

并且 $\mathcal{S}$ 表示 $\mathcal{O}_{K_{\mathbb{R}}}$ 中不对应于 $\mathcal{O}_K$ 中单位根或零的元素。此外，如果

$$\mu(a) = Tr(axx^*)$$

对于某个 $x \in \mathcal{O}_{K_{\mathbb{R}}}$，则

$$Tr(xx^*) \leq t_K(u,\delta)^2. \tag{9}$$

证明。首先，根据一个 ar 与引理 3 中的论证类似，每个 $1 \le i \le r+s$ 的 a'_i 必须满足

$$a'_i \ge \mathrm{Tr}(a')t_K(u,\delta)^{-2}.$$

假设 $x = (x_1, \ldots, x_{r+s}) \in \mathcal{O}_{K_\mathbb{R}}$ 是满足 $\mathrm{Tr}(a'xx^*) = \mu(a)$ 的元素。显然，如果 x 对应于 $\mathcal{O}_K$ 中的一个单位根，则不等式 8 成立，因此我们假设 $x \in \mathcal{S}$。于是

$$\mu(a) = \mathrm{Tr}(a'xx^*) = \left(\sum_{j=1}^{r} + 2\sum_{j=r+1}^{r+s}\right) a'_i x_i x_i^* \ge t_K(u,\delta)^{-2}\mathrm{Tr}(a') \left(\sum_{j=1}^{r} + 2\sum_{j=r+1}^{r+s}\right) x_i x_i^*.$$

不等式 8 和 9 得证。 □

参考文献

[1] Vavra, T., Veneziano, F.: 《数域中的 Pisot 单位生成元》。《符号计算杂志》，第 89 卷，第 94–109 页（2018）。

[2] Koecher, M.: 《关于正性区域约化理论的贡献 I》。《数学年鉴》，第 141 卷，第 384–432 页（1960）。

[3] Porter, C.，Mendelsohn, A.: “全实数域中完美一元形式类数的一个上界”。预印本。

[4] Cramer R.、Ducas L.、Peikert C. 和 Regev O.: “在分圆环中恢复主理想的短生成元”。载于《密码学进展——EUROCRYPT 2016》第35届年度国际会议论文集——体积 9666。施普林格出版社，柏林、海德堡，第559–585页。

[5] Kim, T.、Lee, C.: “欧几里得环上的格约化及其在密码分析中的应用”，《密码学与编码》，第16届IMA国际会议，体积 10655，第371–391页（2017年）。

[6] Porter, C.、Leibak, A.、Ling, C.: “单位可约域上自由模的约化理论”。预印本，`https://arxiv.org/abs/2111.06937`。

[7] Kathuria, L., Raka, M.: 《关于 Minkowski 和 Woods 对 $n = 10$ 的猜想》。《数学科学论文集》，第 132 卷，第 45 期（2022 年）。

[8] achille hui: 《与平面$\sum_{i=1}^{n} x_i = 0$相交的 n维单位超立方体的体积》。数学 Stack Exchange `https://math.stackexchange.com/q/4611874`（2023 年）。

[9] Blichfeldt, H.F.: 《数的几何中的一个新原理及其若干应用》。《美国数学会汇刊》，第 15 卷，第 3 期，第 227-235 页（1914 年）。

[10] Neukirch, J.: 《代数数论》。Norbert Schappacher 德译，卷 322。柏林：施普林格（1999）。

[11] Friedman, E.：《数域调节子的解析公式》。《数学发明》，第 98 卷，第 599–622 页（1989）。

[12] 闵可夫斯基，H.：《数的几何》。莱比锡—柏林：B.G. Teubner 出版社（1910）。

[13] Lagarias, J.c., Lenstra, H.w., Schnorr, C.P.：《格及其倒格的 Korkin-Zolotarev 基与连续极小值》。《组合数学》10 卷，333–348 页（1990）。

[14] Lenstra, A.K., Lenstra, H.W., Lov´asz, L.：《有理系数多项式的因式分解》，《数学年刊》261(4)，515–534 页（1982）。

附录

引理 7 的证明。在整个证明中，我们令 $\mathbf{v} = x\mathbf{b}_1 + y\mathbf{b}_2$，其中 $(x, y) \in \mathbb{Z}^2$ 是某个整数对。我们的证明方法是，假设存在一对 (x, y)，它不属于 S，且满足 $\|\mathbf{v}\|_\infty < 2\lambda^\infty$，并且 $\mathbf{b}_1$,$\mathbf{b}_2$ 满足不等式 6，然后证明由此会导致矛盾。我们略去 x 或 y 为零的情形，因为显然这时会导致矛盾。在整个证明中，我们可以不失一般性地假设 $\|\mathbf{b}_1\|_\infty = \alpha > 0$。我们还将始终假设 $\|\mathbf{b}_2\|_\infty < 2\|\mathbf{b}_1\|_\infty$；否则，由于已在 [?] 中证明，在不等式 6 成立的假设下，对于所有非零的 x、y，都有 $\|x\mathbf{b}_1 + y\mathbf{b}_2\|_\infty \geq \|\mathbf{b}_2\|$，因此会导出矛盾。

在证明的下一部分中，我们将假设 $\|\mathbf{b}_2\|_\infty = \gamma > 0$，因为通过变号可以使$\gamma$ 为正。根据 6，以下不等式中至少有一个成立：

$$|\alpha - \gamma| \geq \|\mathbf{b}_2\|_\infty, , \tag{10}$$
$$|\beta - \delta| \geq \|\mathbf{b}_2\|_\infty, \tag{11}$$
$$|\alpha + \beta - \gamma - \delta| \geq \|\mathbf{b}_2\|_\infty. \tag{12}$$

显然，由于 $\gamma > 0$ 且 $\gamma = \|\mathbf{b}_2\| < 2\alpha$，10 显然不可能成立。因此，我们需要考虑的不等式可能是

$$|\beta - \delta| \geq \gamma, , \tag{13}$$
$$|\alpha + \beta - \gamma - \delta| \geq \gamma. \tag{14}$$

假设成立。由于 $|\alpha + \beta| \leq \alpha$，我们必须有 $\beta < 0$，因此必然也有 $\delta > 0$。但是，$|\gamma + \delta| \leq \gamma$ 也意味着 $\delta < 0$，这就产生了矛盾。因此，转而假设成立。于是

$$\max\{\alpha + \beta - \gamma - \delta, \gamma + \delta - \alpha - \beta\} \geq \gamma.$$

但这不可能成立：

$$\alpha + \beta - \gamma - \delta \geq \gamma \iff \alpha > \alpha + \beta \geq 2\gamma + \delta,$$

但 $|\gamma + \delta| \leq \gamma$ 意味着 $\delta < 0$，因此这将意味着 $\alpha > \gamma$，这是一个矛盾，而且

$$\gamma + \delta - \alpha - \beta \geq \gamma \iff \delta \geq \alpha + \beta > 0,$$

但我们再次需 ed $\delta < 0$，这是一个矛盾。因此， $\gamma = \|\mathbf{b}_2\|_\infty$ 不可能成立 .

在证明的下一部分中，我们将假设 $\|\mathbf{b}_2\|_\infty = \delta > 0$，因为通过变号可以使$\delta$ 为正；并且不再对 γ 的符号作任何假设。事实上， $|\gamma + \delta| \leq \delta$必然意味着此时 $\gamma < 0$ 。根据 6，以下不等式至少有一个成立：

$$|\alpha + \gamma| \geq \|\mathbf{b}_2\|_\infty, \tag{15}$$
$$|\beta + \delta| \geq \|\mathbf{b}_2\|_\infty, \tag{16}$$
$$|\alpha + \beta + \gamma + \delta| \geq \|\mathbf{b}_2\|_\infty. \tag{17}$$

由于 $\gamma < 0$ 和 $\alpha \leq \delta$，显然 15 不成立。此外，显然 16 也不成立，因为必然有 $\beta < 0$。因此，这里唯一需要考虑的情形是

$$|\alpha + \beta + \gamma + \delta| \geq \delta.$$

由于 $\alpha \geq -\beta$ 和 $\delta \geq -\gamma$，

$$\alpha + \beta + \gamma + \delta \geq \delta \iff \alpha \geq -\beta - \gamma$$

因此，若 x、 y 的符号相反，

$$\|\mathbf{v}\|_\infty \geq \max\{|x|\alpha + |y||\gamma|, |x||\beta| + |y|\delta\},$$

当 $\min\{|x|, |y|\} \geq 2$ 时，它大于或等于 $2\lambda^\infty$，因此我们假设 x、 y 的符号相同。于是

$$\|\mathbf{v}\|_\infty \geq ||x|(\alpha + \beta) + |y|(\gamma + \delta)| \geq |x|\alpha + |y|\delta - \max\{|x|, |y|\}\alpha \geq \min\{|x|, |y|\}\alpha,$$

它大于或等于 $2\lambda^\infty$ if $\min\{|x|, |y|\} \geq 2$，因此，若假设 $\|\mathbf{b}_2\|_\infty = \delta$，就会得到另一个矛盾。

在证明的其余部分，我们假设 $\|\mathbf{b}_2\|_\infty = \gamma + \delta > 0$，因为通过变号，我们可以使 $\gamma + \delta$ 为正；而对于 δ，我们不再假设其符号。由于$\alpha + \beta > 0$，显然现在 12 不成立，因此我们需要考虑可能的不等式：

$$|\alpha - \gamma| \geq \gamma + \delta, \tag{18}$$
$$|\beta - \delta| \geq \gamma + \delta. \tag{19}$$

事实上，注意到 γ, δ必定同号，否则就会有 $|\gamma + \delta| < \min\{|\gamma|, |\delta|\}$。因此，根据假设， $\gamma, \delta > 0$，因为 $\gamma + \delta > 0$。因此，18 不成立，因为 $|\alpha - \gamma| < \alpha$，而根据假设，$\gamma < \gamma + \delta < 2\alpha$ 。所以唯一的可能性是

$$|\beta| + \delta \geq \gamma + \delta \iff |\beta| \geq \gamma. \tag{20}$$

如果 x、 y 同号，

$$\|\mathbf{v}\| \geq \max\{|x|\alpha, |y|(\gamma + \delta)\}$$

若 $\min\{|x|, |y|\} \geq 2$，则其大于或等于 $2\lambda^\infty$，因此假设 x、 y 符号相反。于是

$$\|\mathbf{v}\| \geq |x||\beta| + |y|\delta \geq |x|\gamma + |y|\delta,$$

若 $\min\{|x|,|y|\} \geq 1$，则其大于或等于 $2\lambda^\infty$。因此假设 $\min\{|x|,|y|\} = 1$。若 $\min\{|x|,|y|\} = |x| = 1$，则

$$\|\mathbf{v}\| \geq |y|(\gamma+\delta) - (\alpha+\beta) \geq (|y|-1)\alpha,$$

它大于或等于 $2\lambda^\infty$ if $|y| \geq 3$。最后，假设 $\min\{|x|,|y|\} = |y| = 1$。那么根据 20,

$$\|\mathbf{v}\| \geq |x|\alpha - \gamma \geq |x|\alpha - |\beta| \geq (|x|-1)\alpha,$$

它大于或等于 $2\lambda^\infty$ if $|x| \geq 2$。因此，我们在所有情况下都得出了矛盾，所以引理成立。 □

引理 9. $\sum_{k=0}^{\lfloor \frac{r+s}{2} \rfloor} (-1)^k \binom{r+s}{k} \left(\frac{r+s}{2} - k\right)^{r+s-1} \leq \left(\frac{\sqrt{e}}{2\pi} + o(1)\right) \left(e^{1+\frac{1}{2e}}\right)^{r+s} (r+s-1)!$ as $r+s \to +\infty$。

证明。由于我们将 $r+s$ 视为单个变量，因此定义 $n = r+s$ 作为替代。现在，左侧可以写为 $\left|\sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1}\right|$。交错和使计算相当繁琐，因此从这里开始，我们将把求和拆分为偶数部分和奇数部分，得到

$$\left|\sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1}\right| = \left|\sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1} - \sum_{\substack{k=1 \\ k \text{ odd}}}^{\lfloor n/2 \rfloor} \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1}\right|$$

为了判断最终是奇数项（负项）和还是偶数项（正项和）更大，我们可以根据引理 5 得出，$\sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1} = \text{体积}(\mathcal{C}(R) \cap V) \cdot \frac{(n-1)!}{R^{n-1}\sqrt{n}} \geq 0$，因此：

$$\sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1} \leq \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \binom{n}{k} \left(\frac{n}{2}-k\right)^{n-1}$$

首先，我们将 $\binom{n}{k}$ 展开为 $\frac{n!}{k!\,(n-k)!}$。由于这些都是正项和，只要对其中的被加数给出渐近界，就能得到具有相似渐近关系的和。

事实上，对于定义在整数上的正值函数 f 和 g，$f(n) = o(g(n))$ 意味着 $\sum_n f(n) = o\left(\sum_n g(n)\right)$，并且 $f(n) \sim cg(n) \Longrightarrow \sum_n f(n) = (c+o(1)) \sum_n g(n)$。我们将利用斯特林公式处理偶数项之和，该公式指出 $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$。根据斯特林公式，我们将把 $\frac{n!}{k!\,(n-k)!}$ 公式中的 $(n-k)!$ 项展开为其渐近形式：

$$\sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \frac{n!}{k!\,(n-k)!} \left(\frac{n}{2}-k\right)^{n-1} \sim \frac{e^n \cdot n!}{\sqrt{2\pi}} \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \frac{1}{k!\,(n-k)^{n-k+1/2}} \left(\frac{1}{e}\right)^k \left(\frac{n}{2}-k\right)^{n-1}$$

为了让处理稍微简单一些，我们将对被加数取上界，以得到一个更简单的表达式。我们注意到 $n/2 \le n-k \le n$。因此：

$$\frac{e^n \cdot n!}{\sqrt{2\pi}} \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \frac{1}{k!\,(n-k)^{n-k+1/2}} \left(\frac{1}{e}\right)^k \left(\frac{n}{2}-k\right)^{n-1} \le \frac{e^n \cdot n!}{\sqrt{2\pi}(n/2)^{3/2}} \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \frac{1}{k!} \left(\frac{n}{2e}\right)^k$$

我们将尝试求出被加数的上确界。为此，我们将计算 $x \mapsto (n/(2e))^x/\Gamma(x+1)$ 的导数：

$$\frac{\partial}{\partial x}\left(\frac{1}{\Gamma(x+1)}\left(\frac{n}{2e}\right)^x\right) = \frac{1}{\Gamma(x+1)}\left(\frac{n}{2e}\right)^x \left(\log\left(\frac{n}{2e}\right) - \psi(x+1)\right),$$

其中，ψ 是双伽马函数。ψ 在 $(0,+\infty)$ 上严格递增，并且在此区间内取遍 $\mathbb{R}$ 中的所有值，这意味着它恰有一个根。由于当 $n \to +\infty$ 时 $\log \frac{n}{2e} \to +\infty$，$\psi(x) = \log(x) + o(1)$，更准确地说，$\exp \psi(x) = x + O(1)$，我们可以推断该导数的根与 $\frac{n}{2e}$ 渐近等价，其中 $n \to +\infty$。

因此，我们可以推出以下关系：

$$\begin{aligned}
\frac{e^n \cdot n!}{\sqrt{2\pi}(n/2)^{3/2}} \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \frac{1}{k!}\left(\frac{n}{2e}\right)^k &\le \frac{e^n \cdot n!}{\sqrt{2\pi}(n/2)^{3/2}} \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \sup_{k' \in [0,n/2]} \left\{\frac{1}{k'!}\left(\frac{n}{2e}\right)^{k'}\right\} \\
&\sim \frac{e^n \cdot n!}{\sqrt{2\pi}(n/2)^{3/2}} \sum_{\substack{k=0 \\ k \text{ even}}}^{\lfloor n/2 \rfloor} \frac{1}{\Gamma(\frac{n}{2e}+1)}\left(\frac{n}{2e}\right)^{\frac{n}{2e}} \\
&= \frac{e^n \cdot n!}{\sqrt{2\pi}(n/2)^{3/2}} \left\lfloor \frac{n}{4} \right\rfloor \frac{1}{\Gamma(\frac{n}{2e}+1)}\left(\frac{n}{2e}\right)^{\frac{n}{2e}}
\end{aligned}$$

再次使用斯特林近似，此时 $\Gamma(x+1) \sim \sqrt{2\pi x}(x/e)^x$，以及 $\lfloor x \rfloor \sim x$，

$$\frac{e^n \cdot n!}{\sqrt{2\pi}(n/2)^{3/2}} \left\lfloor \frac{n}{4} \right\rfloor \frac{1}{\Gamma(\frac{n}{2e}+1)}\left(\frac{n}{2e}\right)^{\frac{n}{2e}} \sim \frac{\sqrt{e}}{2\pi}\left(e^{1+\frac{1}{2e}}\right)^n (n-1)!$$

证明至此结束。 □