0.1 组合数论类问题

例题 0.1 设 A 为 $n\times n$ 实矩阵, 其中元素 $A(i,j)\in\{-1,1\}$, 且 A 的行向量两两正交. 若对任意的 $i\in\{1,2,\ldots,k\}$,$j\in\{1,2,\ldots,l\}$, 都有 $A(i,j)=1$, 证明:$kl\leqslant n$.

证明 设 $\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_k$ 是矩阵 A 的前 k 个行向量. 根据题意, 这些向量两两正交. 即对于任意 $i\neq j$ 且 $1\leq i,j\leq k$, 我们有:

$$\mathbf{a}_i\cdot\mathbf{a}_j=\sum_{p=1}^{n}A(i,p)A(j,p)=0.$$

我们可以将这个求和式分解为两部分: 前 l 个分量和后 $n-l$ 个分量.

$$\sum_{p=1}^{l}A(i,p)A(j,p)+\sum_{p=l+1}^{n}A(i,p)A(j,p)=0$$

根据题设, 对于 $1\leq i\leq k$ 和 $1\leq p\leq l$, 都有 $A(i,p)=1$. 所以, 对于任意 $1\leq i,j\leq k$ 且 $i\neq j$, 上式的第一部分为:

$$\sum_{p=1}^{l}A(i,p)A(j,p)=\sum_{p=1}^{l}(1)(1)=l$$

将此结果代入, 我们得到:

$$l+\sum_{p=l+1}^{n}A(i,p)A(j,p)=0\implies\sum_{p=l+1}^{n}A(i,p)A(j,p)=-l$$

现在, 我们定义 k 个新的向量 $\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_k\in\mathbb{R}^{n-l}$, 其中每个向量 $\mathbf{c}_i$ 由对应行向量 $\mathbf{a}_i$ 的后 $n-l$ 个分量构成:

$$\mathbf{c}_i=(A(i,l+1),A(i,l+2),\ldots,A(i,n)).$$

对于这些新向量, 我们有如下的点积关系:

(i) 对于 $i\neq j$,$\mathbf{c}_i\cdot\mathbf{c}_j=\sum\limits_{p=l+1}^{n}A(i,p)A(j,p)=-l$.

(ii) 对于 $i=j$,$\mathbf{c}_i\cdot\mathbf{c}_i=\sum\limits_{p=l+1}^{n}(A(i,p))^2=\sum\limits_{p=l+1}^{n}1^2=n-l$, 因为 $A(i,p)\in\{-1,1\}$.

考虑这些向量的和向量 $\mathbf{v}=\sum\limits_{i=1}^{k}\mathbf{c}_i$. 我们来计算其模的平方 $\|\mathbf{v}\|^2$.

$$\begin{aligned}\|\mathbf{v}\|^2=\mathbf{v}\cdot\mathbf{v}&=\left(\sum_{i=1}^{k}\mathbf{c}_i\right)\cdot\left(\sum_{j=1}^{k}\mathbf{c}_j\right)\\&=\sum_{i=1}^{k}\sum_{j=1}^{k}(\mathbf{c}_i\cdot\mathbf{c}_j)=\sum_{i=1}^{k}(\mathbf{c}_i\cdot\mathbf{c}_i)+\sum_{1\leq i\neq j\leq k}(\mathbf{c}_i\cdot\mathbf{c}_j).\end{aligned}$$

在上式中, 对角线上的项 $(i=j)$ 有 k 个, 非对角线上的项 $(i\neq j)$ 有 $k(k-1)$ 个. 代入我们之前计算的点积值:

$$\begin{aligned}\|\mathbf{v}\|^2&=k\cdot(n-l)+k(k-1)\cdot(-l)=kn-kl-k^2l+kl\\&=kn-k^2l=k(n-kl)\end{aligned}$$

因为向量模的平方必须是非负的, 所以 $\|\mathbf{v}\|^2\geq 0$.

$$k(n-kl)\geqslant 0$$

根据题意,k 是行数, 所以 $k\geq 1$(如果 $k=0$ 或 $l=0$, 则 $kl=0\leq n$ 显然成立). 故

$$n-kl\geqslant 0.$$

这直接导出了我们要证明的结论:

$$kl\leq n$$

证明完毕.

□

例题 0.2 设 $n \geq 4$. 设 n 阶实方阵 $A = (a_{ij})$ 满足 $a_{ij} = \pm 1$ 且它的行向量两两正交. 证明:

(1) A 的列向量两两正交.

(2) n 是偶数, 并且 n 是 4 的倍数.

证明

(1) 设 A 的列向量分块为 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, 则由 A 的行向量两两正交可知

$$AA^T = nI_n \Longrightarrow A^TA = nI_n \Longrightarrow \begin{pmatrix} (\alpha_1,\alpha_1) & (\alpha_1,\alpha_2) & \cdots & (\alpha_1,\alpha_n) \\ (\alpha_2,\alpha_1) & (\alpha_2,\alpha_2) & \cdots & (\alpha_2,\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha_n,\alpha_1) & (\alpha_n,\alpha_2) & \cdots & (\alpha_n,\alpha_n) \end{pmatrix} = \begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{pmatrix}.$$

故 $(\alpha_i, \alpha_j) = 0, i \neq j$. 因此 A 的列向量也两两正交.

(2) 不妨设 A 的第一行全为 1, 否则对第一行中 -1 所在列乘 -1. 由 A 的第一行与第二行正交知

$$\sum_{j=1}^{n} a_{1j}a_{2j} = \sum_{j=1}^{n} a_{2j} = 0.$$

从而 A 的第二行元素中 1 和 -1 的个数相同, 因此 $2|n$. 不妨设

$$a_{2j} = 1, \quad j = 1, \cdots, \frac{n}{2};$$
$$a_{2j} = -1, \quad j = \frac{n}{2} + 1, \cdots, n.$$

再由 A 的第三行与第一行正交以及第三行与第二行正交可得

$$\sum_{j=1}^{\frac{n}{2}} a_{1j}a_{3j} + \sum_{j=\frac{n}{2}}^{n} a_{1j}a_{3j} = \sum_{j=1}^{\frac{n}{2}} a_{3j} + \sum_{j=\frac{n}{2}}^{n} a_{3j} = 0,$$
$$\sum_{j=1}^{\frac{n}{2}} a_{2j}a_{3j} + \sum_{j=\frac{n}{2}}^{n} a_{2j}a_{3j} = \sum_{j=1}^{\frac{n}{2}} a_{3j} - \sum_{j=\frac{n}{2}}^{n} a_{3j} = 0.$$

由此可得

$$\sum_{j=1}^{\frac{n}{2}} a_{3j} = \sum_{j=\frac{n}{2}}^{n} a_{3j} = 0.$$

因此 $a_{31}, a_{32}, \cdots, a_{3,\frac{n}{2}}$ 中 -1 和 1 的个数相同, 故 $2|\frac{n}{2}$, 即 $4|n$.

□

例题 0.3

(1) 证明: 不存在 $A, B, C \in \mathbb{Z}^{2\times 2}$ 使得 $\det A = \det B = \det C = 1$, $A^4 + B^4 = C^4$.

(2) 是否存在 $A, B, C \in \mathbb{Z}^{2\times 2}$ 使得 $\det A = \det B = \det C = 1$, $A^2 + B^2 = C^2$?

证明

(1) 反证, 假设存在 $A, B, C \in \mathbb{Z}^{2\times 2}$, 使得结论成立. 则由 $\det A = \det B = \det C = 1$ 知,A, B, C 的特征多项式可设为

$$|xI - A| = x^2 - ax + 1, \quad |xI - B| = x^2 - bx + 1, \quad |xI - C| = x^2 - cx + 1,$$

其中 $\mathrm{tr}(A) = a$,$\mathrm{tr}(B) = b$,$\mathrm{tr}(C) = c$, 且 $a, b, c \in \mathbb{Z}$. 由 Cayley-Hamilton 定理知

$$A^2 - aA + I = 0, \quad B^2 - bB + I = 0, \quad C^2 - cC + I = 0.$$

即

$$A^2 = aA - I, \quad B^2 = bB - I, \quad C^2 = cC - I.$$

进而

$$\mathrm{tr}(A^2) = a^2 - 2, \quad \mathrm{tr}(B^2) = b^2 - 2, \quad \mathrm{tr}(C^2) = c^2 - 2.$$

从而

$$A^4 = (A^2)^2 = (aA - I)^2 = a^2A^2 - 2aA + I,$$

$$B^4 = (B^2)^2 = (bB - I)^2 = b^2B^2 - 2bB + I,$$

$$C^4 = (C^2)^2 = (cC - I)^2 = c^2C^2 - 2cC + I.$$

于是

$$\mathrm{tr}(A^4) = \mathrm{tr}(a^2A^2 - 2aA + I) = a^4 - 4a^2 + 2,$$

$$\mathrm{tr}(B^4) = \mathrm{tr}(b^2B^2 - 2bB + I) = b^4 - 4b^2 + 2,$$

$$\mathrm{tr}(C^4) = \mathrm{tr}(c^2C^2 - 2cC + I) = c^4 - 4c^2 + 2.$$

由 $A^4 + B^4 = C^4$ 知

$$\mathrm{tr}(A^4 + B^4) = \mathrm{tr}(C^4) \Longleftrightarrow a^4 + b^4 - 4(a^2 + b^2) + 4 = c^4 - 4c^2 + 2$$

$$\Longleftrightarrow a^4 + b^4 - c^4 = 4(a^2 + b^2 - c^2) - 2. \tag{1}$$

注意到任意的完全平方数除 4 的余数只有 0 或 1, 故

$$a^4, b^4, c^4 \equiv 0或1 \pmod 4.$$

又 $4(a^2 + b^2 - c^2) - 2 \equiv 2 \pmod 4$, 故

$$a^4 + b^4 - c^4 \equiv 2 \pmod 4.$$

因此 $a^4, b^4 \equiv 1 \pmod 4$,$c^4 \equiv 0 \pmod 4$. 故 a, b 都是奇数,c 是偶数. 设 $a = 2k_1 + 1$,$b = 2k_2 + 1$,$c = 2k_3$, 则

$$a^4 = (2k_1 + 1)^4 = (4k_1^2 + 4k_1 + 1)^2 = 16k_1^4 + 32k_1^3 + 24k_1^2 + 8k_1 + 1,$$

$$b^4 = (2k_2 + 1)^4 = (4k_2^2 + 4k_2 + 1)^2 = 16k_2^4 + 32k_2^3 + 24k_2^2 + 8k_2 + 1,$$

$$c^4 = (2k_3)^4 = 16k_3^4.$$

从而 $a^4, b^4 \equiv 1 \pmod 8$,$c^4 \equiv 0 \pmod 8$. 于是 $a^4 + b^4 - c^4 \equiv 2 \pmod 8$. 因此再由(1)式可得

$$4(a^2 + b^2 - c^2) - 2 \equiv 2 \pmod 8 \Longrightarrow 4(a^2 + b^2 - c^2) - 4 \equiv 0 \pmod 8.$$

故存在 $k \in \mathbb{Z}$, 使得

$$4(a^2 + b^2 - c^2) - 4 = 8k \Longrightarrow (a^2 + b^2 - c^2) - 1 = 2k \Longrightarrow c^2 = a^2 + b^2 - (2k + 1).$$

又因为 a, b 都是奇数, 所以 $c^2 = a^2 + b^2 - (2k + 1) \equiv 1 \pmod 2$, 即 c^2 是奇数. 这与 c 是偶数矛盾!

(2) 存在. 只需取 $A \in \mathbb{Z}^{2\times 2}$ 满足 $\det A = 1$ 且 $\mathrm{tr}(A) = 1$,$B = I - A$, 再取 $C \in \mathbb{Z}^{2\times 2}$ 满足 $\det C = 1$ 且 $C^2 = -I$,$\mathrm{tr}(C) = 0$. 此时由 Cayley-Hamilton 定理定理知 $A^2 - A + I = 0$,$C^2 + I = 0$ 从而

$$\det B = \det(I - A) = \det(A^2) = 1,$$

$$A^2 + B^2 = A^2 + (I - A)^2 = 2A^2 - 2A + I = -I = C^2.$$

因此我们可取 $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$,$B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$,$C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

□