

文章编号: 1004-4353(2015)01-0017-04

内积空间中的互不偏基

雷丽霞¹, 南华², 张军^{2*}

(1. 延吉市第七中学, 吉林 延吉 133000; 2. 延边大学理学院 数学系, 吉林 延吉 133002)

摘要: 将量子信息理论中的互不偏基概念进行了代数化, 在内积空间中引进和推广了互不偏基的概念, 讨论了欧氏空间中的相关性质, 并分别在欧氏空间和酉空间中给出互不偏基的例子.

关键词: 内积空间; 标准正交基; 互不偏基; 正交矩阵

中图分类号: O151.2

文献标识码: A

Mutually unbiased bases in inner product space

LEI Lixia¹, NAN Hua², ZHANG Jun^{2*}

(1. Teaching and Guiding Office Yanji No. 7 Middle School, Yanji 133000, China;
2. Department of Mathematics, College of Science, Yanbian University, Yanji 133002, China)

Abstract: The concept of mutually unbiased bases in quantum information theory is expressed as algebraic form in this paper, which is defined and extended in inner product space. And the related properties are discussed in Euclidean space. Moreover the examples of mutually unbiased basis are given in Euclidean space and unitary space separately.

Key words: inner product space; standard orthogonal bases; mutually unbiased bases; orthogonal matrix

近年来, 量子信息处理技术不断得到发展和完善, 其中互不偏基问题的研究已从单体空间^[1]转向多体空间. 在量子纠缠的作用下, 构造互不偏基已成了一个新的研究课题^[2]. 互不偏基由于具有内积模不变的优点, 被用于解决量子态层析和加密协议等问题^[3-4]. 随着对互不偏基问题的深入研究, 其应用也会更加广泛. 互不偏基的概念为: 给定 m 个 C^d 空间上的标准正交基 $B_k = \{|\psi_i^k\rangle\}_{i=1}^d, k=1, 2, \dots, m$, 如果 md 个基向量中任意两个都满足 $|\langle\psi_i^k|\psi_{i'}^{k'}\rangle| = \begin{cases} \delta_{ii'}, & k=k'; \\ \frac{1}{\sqrt{d}}, & k \neq k', \end{cases}$ 其中 $k, k'=1, 2, \dots, m$, 则称 $\{B_1, B_2, \dots, B_m\}$ 是互不偏基^[5]. 本文将量子信息理论中的互不偏基概念进行了代数化, 在内积空间中引进和推广了互不偏基的概念, 分别在欧氏空间和酉空间中给出互不偏基的例子, 并对欧氏空间中互不偏基的存在性进行了论证.

1 互不偏基的推广

定义 1^[6] 设 V 是数域 F (实数域或复数域) 上的 n 维内积空间, $\{\alpha_1, \alpha_2, \dots, \alpha_n\}, \{\beta_1, \beta_2, \dots, \beta_n\}$ 是 V 的两组标准正交基, 若两组基中任意两个向量的内积满足: $|\langle\alpha_i, \beta_j\rangle| = \frac{1}{\sqrt{n}}, i, j=1, 2, \dots, n$, 则称 $\{\alpha_1,$

$\alpha_2, \dots, \alpha_n\}$ 与 $\{\beta_1, \beta_2, \dots, \beta_n\}$ 是互不偏基.

定义 2 设 V 是数域 F (实数域或复数域) 上的 kn 维内积空间, $\alpha_{is} (i=1, 2, \dots, n; s=1, 2, \dots, k)$, $\beta_{jt} (j=1, 2, \dots, n; t=1, 2, \dots, k)$ 是 V 的两组标准正交基, 若两组基中任意两个向量的内积满足:

$$|(\alpha_{is}, \beta_{jt})| = \begin{cases} \frac{1}{\sqrt{n}}, & s=t, i, j=1, 2, \dots, n; \\ 0, & s \neq t, i, j=1, 2, \dots, n, \end{cases} \quad \text{则称 } \alpha_{is} (i=1, 2, \dots, n; s=1, 2, \dots, k) \text{ 和 } \beta_{jt} (j=1, 2, \dots, n; t=1, 2, \dots, k) \text{ 是广义互不偏基.}$$

$t=1, 2, \dots, k)$ 是广义互不偏基.

若内积空间有多组标准正交基, 且任意两组标准正交基都是 (广义) 互不偏基, 则称其为 (广义) 互不偏基组.

显然, 当定义 2 中的 k 取 1 时, 即得定义 1 的条件和结论.

例 1 设 F^2 为 2 维内积空间, 即 $\forall \alpha = (x_1, x_2), \beta = (y_1, y_2) \in F^2$, 定义内积为

$$(\alpha, \beta) = \alpha \bar{\beta}^T = x_1 \bar{y}_1 + x_2 \bar{y}_2.$$

当 $F = \mathbf{R}$ 时, 取欧氏空间 \mathbf{R}^2 的两组标准正交基: $\varepsilon_1 = (1, 0), \varepsilon_2 = (0, 1); \alpha_1 = \frac{1}{\sqrt{2}}(1, 1), \alpha_2 = \frac{1}{\sqrt{2}}(1, -1)$, 则有 $|(\varepsilon_i, \alpha_j)| = \frac{1}{\sqrt{2}}, i, j=1, 2$. 即欧氏空间 \mathbf{R}^2 的两组标准正交基 $\{\varepsilon_1, \varepsilon_2\}$ 和 $\{\alpha_1, \alpha_2\}$ 是互不偏基.

当 $F = \mathbf{C}$ 时, 取酉空间 \mathbf{C}^2 的三组标准正交基^[7]: $\varepsilon_1 = (1, 0), \varepsilon_2 = (0, 1); \alpha_1 = \frac{1}{\sqrt{2}}(1, 1), \alpha_2 = \frac{1}{\sqrt{2}}(1, -1); \beta_1 = \frac{1}{\sqrt{2}}(1, i), \beta_2 = \frac{1}{\sqrt{2}}(1, -i)$, 则有 $|(\varepsilon_i, \alpha_j)| = |(\varepsilon_i, \beta_k)| = |(\alpha_j, \beta_k)| = \frac{1}{\sqrt{2}}, i, j, k=1, 2$. 即酉空间 \mathbf{C}^2 的三组标准正交基: $\{\varepsilon_1, \varepsilon_2\}, \{\alpha_1, \alpha_2\}, \{\beta_1, \beta_2\}$ 是互不偏基组.

例 2 设 \mathbf{C}^3 为 3 维酉空间, 即 $\forall \alpha = (x_1, x_2, x_3), \beta = (y_1, y_2, y_3) \in \mathbf{C}^3$, 定义内积为

$$(\alpha, \beta) = \alpha \bar{\beta}^T = x_1 \bar{y}_1 + x_2 \bar{y}_2 + x_3 \bar{y}_3.$$

取酉空间 \mathbf{C}^3 的四组标准正交基^[7]:

$$\varepsilon_1 = (1, 0, 0), \varepsilon_2 = (0, 1, 0), \varepsilon_3 = (0, 0, 1);$$

$$\alpha_1 = \frac{1}{\sqrt{3}}(1, 1, 1), \alpha_2 = \frac{1}{\sqrt{3}}(1, \omega, \bar{\omega}), \alpha_3 = \frac{1}{\sqrt{3}}(1, \bar{\omega}, \omega);$$

$$\beta_1 = \frac{1}{\sqrt{3}}(1, \omega, \omega), \beta_2 = \frac{1}{\sqrt{3}}(1, \bar{\omega}, 1), \beta_3 = \frac{1}{\sqrt{3}}(1, 1, \bar{\omega});$$

$$\gamma_1 = \frac{1}{\sqrt{3}}(1, \bar{\omega}, \bar{\omega}), \gamma_2 = \frac{1}{\sqrt{3}}(1, 1, \omega), \gamma_3 = \frac{1}{\sqrt{3}}(1, \omega, 1),$$

其中 $\omega = \frac{-1 + \sqrt{3}i}{2}$, $\bar{\omega}$ 为 ω 的共轭, 且有^[6]:

$$\begin{pmatrix} (\alpha_1, \beta_1) & (\alpha_1, \beta_2) & (\alpha_1, \beta_3) \\ (\alpha_2, \beta_1) & (\alpha_2, \beta_2) & (\alpha_2, \beta_3) \\ (\alpha_3, \beta_1) & (\alpha_3, \beta_2) & (\alpha_3, \beta_3) \end{pmatrix} = \begin{pmatrix} \alpha_1 \bar{\beta}_1^T & \alpha_1 \bar{\beta}_2^T & \alpha_1 \bar{\beta}_3^T \\ \alpha_2 \bar{\beta}_1^T & \alpha_2 \bar{\beta}_2^T & \alpha_2 \bar{\beta}_3^T \\ \alpha_3 \bar{\beta}_1^T & \alpha_3 \bar{\beta}_2^T & \alpha_3 \bar{\beta}_3^T \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 1 + 2\bar{\omega} & 2 + \omega & 2 + \omega \\ 2 + \omega & 1 + 2\bar{\omega} & 2 + \omega \\ 2 + \omega & 2 + \omega & 1 + 2\bar{\omega} \end{pmatrix},$$

其中 $|1 + 2\bar{\omega}| = |2 + \omega| = \sqrt{3}$, 即 $|(\alpha_i, \beta_j)| = \frac{1}{\sqrt{3}}, i, j=1, 2, 3$. 同理可知

$$|(\varepsilon_i, \alpha_j)| = |(\varepsilon_i, \beta_k)| = |(\varepsilon_i, \gamma_l)| = |(\alpha_j, \gamma_l)| = |(\beta_k, \gamma_l)| = \frac{1}{\sqrt{3}}, i, j, k, l=1, 2, 3.$$

故酉空间 \mathbf{C}^3 的四组标准正交基 $\{\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \boldsymbol{\varepsilon}_3\}$, $\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3\}$, $\{\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \boldsymbol{\beta}_3\}$, $\{\boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \boldsymbol{\gamma}_3\}$ 是互不偏基组.

例 3 设 \mathbf{C}^6 为 6 维酉空间, 即 $\forall \boldsymbol{\alpha} = (x_1, x_2, x_3, x_4, x_5, x_6)$, $\boldsymbol{\beta} = (y_1, y_2, y_3, y_4, y_5, y_6) \in \mathbf{C}^6$, 定义内积为 $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \boldsymbol{\alpha} \bar{\boldsymbol{\beta}}^T = x_1 \bar{y}_1 + x_2 \bar{y}_2 + x_3 \bar{y}_3 + x_4 \bar{y}_4 + x_5 \bar{y}_5 + x_6 \bar{y}_6$.

将酉空间 \mathbf{C}^6 看成 $\mathbf{C}^{3 \times 2}$ 时, 有广义互不偏基组:

$$\begin{aligned} \boldsymbol{\varepsilon}_{11} &= (1, 0, 0, 0, 0, 0), \boldsymbol{\varepsilon}_{21} = (0, 1, 0, 0, 0, 0), \boldsymbol{\varepsilon}_{12} = (0, 0, 1, 0, 0, 0), \\ \boldsymbol{\varepsilon}_{22} &= (0, 0, 0, 1, 0, 0), \boldsymbol{\varepsilon}_{13} = (0, 0, 0, 0, 1, 0), \boldsymbol{\varepsilon}_{23} = (0, 0, 0, 0, 0, 1); \\ \boldsymbol{\alpha}_{11} &= \frac{1}{\sqrt{2}}(1, 1, 0, 0, 0, 0), \boldsymbol{\alpha}_{21} = \frac{1}{\sqrt{2}}(1, -1, 0, 0, 0, 0), \boldsymbol{\alpha}_{12} = \frac{1}{\sqrt{2}}(0, 0, 1, 1, 0, 0), \\ \boldsymbol{\alpha}_{22} &= \frac{1}{\sqrt{2}}(0, 0, 1, -1, 0, 0), \boldsymbol{\alpha}_{13} = \frac{1}{\sqrt{2}}(0, 0, 0, 0, 1, 1), \boldsymbol{\alpha}_{23} = \frac{1}{\sqrt{2}}(0, 0, 0, 0, 1, -1); \\ \boldsymbol{\beta}_{11} &= \frac{1}{\sqrt{2}}(1, i, 0, 0, 0, 0), \boldsymbol{\beta}_{21} = \frac{1}{\sqrt{2}}(1, -i, 0, 0, 0, 0), \boldsymbol{\beta}_{12} = \frac{1}{\sqrt{2}}(0, 0, 1, i, 0, 0), \\ \boldsymbol{\beta}_{22} &= \frac{1}{\sqrt{2}}(0, 0, 1, -i, 0, 0), \boldsymbol{\beta}_{13} = \frac{1}{\sqrt{2}}(0, 0, 0, 0, 1, i), \boldsymbol{\beta}_{23} = \frac{1}{\sqrt{2}}(0, 0, 0, 0, 1, -i). \end{aligned}$$

将酉空间 \mathbf{C}^6 看成 $\mathbf{C}^{2 \times 3}$ 时, 有广义互不偏基组:

$$\begin{aligned} \boldsymbol{\varepsilon}_{11} &= (1, 0, 0, 0, 0, 0), \boldsymbol{\varepsilon}_{21} = (0, 1, 0, 0, 0, 0), \boldsymbol{\varepsilon}_{31} = (0, 0, 1, 0, 0, 0), \\ \boldsymbol{\varepsilon}_{12} &= \frac{1}{\sqrt{3}}(0, 0, 0, 1, 1, 1), \boldsymbol{\varepsilon}_{22} = \frac{1}{\sqrt{3}}(0, 0, 0, 1, \omega, \bar{\omega}), \boldsymbol{\varepsilon}_{32} = \frac{1}{\sqrt{3}}(0, 0, 0, 1, \bar{\omega}, \omega); \\ \boldsymbol{\alpha}_{11} &= \frac{1}{\sqrt{3}}(1, 1, 1, 0, 0, 0), \boldsymbol{\alpha}_{21} = \frac{1}{\sqrt{3}}(1, \omega, \bar{\omega}, 0, 0, 0), \boldsymbol{\alpha}_{31} = \frac{1}{\sqrt{3}}(1, \bar{\omega}, \omega, 0, 0, 0), \\ \boldsymbol{\alpha}_{12} &= (0, 0, 0, 1, 0, 0), \boldsymbol{\alpha}_{22} = (0, 0, 0, 0, 1, 0), \boldsymbol{\alpha}_{32} = (0, 0, 0, 0, 0, 1); \\ \boldsymbol{\beta}_{11} &= \frac{1}{\sqrt{3}}(1, \omega, \omega, 0, 0, 0), \boldsymbol{\beta}_{21} = \frac{1}{\sqrt{3}}(1, \bar{\omega}, 1, 0, 0, 0), \boldsymbol{\beta}_{31} = \frac{1}{\sqrt{3}}(1, 1, \bar{\omega}, 0, 0, 0), \\ \boldsymbol{\beta}_{12} &= \frac{1}{\sqrt{3}}(0, 0, 0, 1, \bar{\omega}, \bar{\omega}), \boldsymbol{\beta}_{22} = \frac{1}{\sqrt{3}}(0, 0, 0, 1, 1, \omega), \boldsymbol{\beta}_{32} = \frac{1}{\sqrt{3}}(0, 0, 0, 1, \omega, 1); \\ \boldsymbol{\gamma}_{11} &= \frac{1}{\sqrt{3}}(1, \bar{\omega}, \bar{\omega}, 0, 0, 0), \boldsymbol{\gamma}_{21} = \frac{1}{\sqrt{3}}(1, 1, \omega, 0, 0, 0), \boldsymbol{\gamma}_{31} = \frac{1}{\sqrt{3}}(1, \omega, 1, 0, 0, 0), \\ \boldsymbol{\gamma}_{12} &= \frac{1}{\sqrt{3}}(0, 0, 0, 1, \omega, \omega), \boldsymbol{\gamma}_{22} = \frac{1}{\sqrt{3}}(0, 0, 0, 1, \bar{\omega}, 1), \boldsymbol{\gamma}_{32} = \frac{1}{\sqrt{3}}(0, 0, 0, 1, 1, \bar{\omega}). \end{aligned}$$

广义互不偏基组的构成有多种组合形式, 例 3 中仅给出了其中一种组合.

2 欧氏空间中互不偏基的存在性

在一般欧氏空间中不一定存在互不偏基, 如 3 维欧氏空间中, 除了 $\boldsymbol{\varepsilon}_1 = (1, 0, 0)$, $\boldsymbol{\varepsilon}_2 = (0, 1, 0)$, $\boldsymbol{\varepsilon}_3 = (0, 0, 1)$ 之外, 再不存在另一组满足互不偏基定义的标准正交基, 甚至不会存在满足互不偏基定义的两个正交的单位向量. 事实上, $\boldsymbol{\alpha} = (x_1, x_2, x_3)$, $\boldsymbol{\beta} = (y_1, y_2, y_3) \in \mathbf{R}^3$, 且同时满足条件 $\|\boldsymbol{\alpha}\| = \|\boldsymbol{\beta}\| = 1$, $|x_i| = |y_j| = \frac{1}{\sqrt{3}}$, $i, j = 1, 2, 3$, $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \boldsymbol{\alpha} \boldsymbol{\beta}^T = x_1 y_1 + x_2 y_2 + x_3 y_3 = 0$ 是不可能的.

根据互不偏基的定义, 只要在 n 维欧氏空间中找到分量的绝对值皆为 $\frac{1}{\sqrt{n}}$ 的标准正交基即可. 换言之, 只要找到所有元素的绝对值皆为 $\frac{1}{\sqrt{n}}$ 的 n 阶正交矩阵即可. 下面证明在特定维数的欧氏空间中存在互不偏基.

定理 1 2^m 维欧氏空间中存在互不偏基.

证明 (数学归纳法) 当 $m=0$ 时, 欧氏空间为 1 维空间, 有 1 阶正交矩阵 $\mathbf{A}_0=(1)$, 命题显然成立.

现构造 2 阶矩阵 $\mathbf{A}_1=\frac{1}{\sqrt{2}}\begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_0 \\ \mathbf{A}_0 & -\mathbf{A}_0 \end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, 由例 1 知, 欧氏空间中存在互不偏基, 即 $m=1$

时, 命题成立.

假设 $m=k$ 时, 命题成立, 即存在所有元素的绝对值皆为 $\frac{1}{\sqrt{2^k}}$ 的 2^k 阶矩阵 $\mathbf{A}_k=\frac{1}{\sqrt{2}}\begin{pmatrix} \mathbf{A}_{k-1} & \mathbf{A}_{k-1} \\ \mathbf{A}_{k-1} & -\mathbf{A}_{k-1} \end{pmatrix}$,

满足 $\mathbf{A}_k\mathbf{A}_k^T=\frac{1}{2}\begin{pmatrix} \mathbf{A}_{k-1} & \mathbf{A}_{k-1} \\ \mathbf{A}_{k-1} & -\mathbf{A}_{k-1} \end{pmatrix}\begin{pmatrix} \mathbf{A}_{k-1} & \mathbf{A}_{k-1} \\ \mathbf{A}_{k-1} & -\mathbf{A}_{k-1} \end{pmatrix}^T=\begin{pmatrix} \mathbf{A}_{k-1}\mathbf{A}_{k-1}^T & \mathbf{O} \\ \mathbf{O} & \mathbf{A}_{k-1}\mathbf{A}_{k-1}^T \end{pmatrix}=\begin{pmatrix} \mathbf{E}_{2^{k-1}} & \mathbf{O} \\ \mathbf{O} & \mathbf{E}_{2^{k-1}} \end{pmatrix}=\mathbf{E}_{2^k}.$

现构造 2^{k+1} 阶矩阵 $\mathbf{A}_{k+1}=\frac{1}{\sqrt{2}}\begin{pmatrix} \mathbf{A}_k & \mathbf{A}_k \\ \mathbf{A}_k & -\mathbf{A}_k \end{pmatrix}$, 其所有元素的绝对值皆为 $\frac{1}{\sqrt{2^{k+1}}}$, 且有

$$\mathbf{A}_{k+1}\mathbf{A}_{k+1}^T=\frac{1}{2}\begin{pmatrix} \mathbf{A}_k & \mathbf{A}_k \\ \mathbf{A}_k & -\mathbf{A}_k \end{pmatrix}\begin{pmatrix} \mathbf{A}_k & \mathbf{A}_k \\ \mathbf{A}_k & -\mathbf{A}_k \end{pmatrix}^T=\begin{pmatrix} \mathbf{A}_k\mathbf{A}_k^T & \mathbf{O} \\ \mathbf{O} & \mathbf{A}_k\mathbf{A}_k^T \end{pmatrix}=\begin{pmatrix} \mathbf{E}_{2^k} & \mathbf{O} \\ \mathbf{O} & \mathbf{E}_{2^k} \end{pmatrix}=\mathbf{E}_{2^{k+1}},$$

故 $m=k+1$ 时, 命题也成立.

由归纳法知, 2^m 维欧氏空间中存在互不偏基.

例 4 欧氏空间 \mathbf{R}^4 中的互不偏基.

因 $4=2^2$, 由定理 1 可知, 所有元素的绝对值皆为 $\frac{1}{2}$ 的 4 阶正交矩阵存在, 即

$$\mathbf{A}_2=\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

显然, 矩阵 \mathbf{A}_2 的 4 个行向量构成 \mathbf{R}^4 的标准正交基, 记为 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

现取 4 阶单位矩阵的 4 个行向量构成的 \mathbf{R}^4 的标准正交基, 记为 $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$. 作内积, 并取绝对值有

$|(\varepsilon_i, \alpha_j)|=\frac{1}{2}, i, j=1, 2, 3, 4$, 由互不偏基定义可知 $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\}$ 和 $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ 是互不偏基.

参考文献:

- [1] Brierley S, Weigert S. All mutually unbiased bases in dimensions two to five[J]. Quantum Info Comp, 2010, 10: 803-820.
- [2] CHEN Bin, FEI Shaoming. Unextendible maximally entangled bases and mutually unbiased bases [J]. Phys Rev A, 2013, 88(3):034301(4).
- [3] Adamson R B A, Steinberg A M. Improving quantum state estimation with mutually unbiased bases[J]. Phys Rev Lett, 2010, 105(3):030406(4).
- [4] Fernández-Pérez A, Klimov A B, Saavedra C. Quantum process reconstruction based on mutually unbiased basis [J]. Phys Rev A, 2011, 83(5):052332(6).
- [5] YU I C, Lin F L, Huang C Y. Quantum secret sharing with multilevel mutually (un)biased bases[J]. Phys Rev A, 2008, 78(1):012344(5).
- [6] 同济大学应用数学系. 高等代数与解析几何[M]. 北京: 高等教育出版社, 2005.
- [7] Wiesniak M, Paterek T, Zeilinger A. Entanglement in mutually unbiased bases[J]. New J Phys, 2011, 13:053047.