Advances in Education 教育进展, 2022, 12(11), 4231-4235
Published Online November 2022 in Hans. http://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2022.1211646

Hans汉斯

浅谈线性代数在网络编码中的应用

刘双庆

苏州科技大学数学科学学院，江苏 苏州

收稿日期：2022年9月26日；录用日期：2022年10月26日；发布日期：2022年11月1日

摘　要

线性代数是普通高校理工科的一门公共课，许多学生在学习完本课程后，未能很好地将相关知识与实际问题之间建立起联系。本文主要介绍利用线性代数课程中的矩阵和线性空间等相关知识，构造在网络编码中有着重要作用的子空间码。从而让学生更好的理解线性代数在实际问题中的应用，引导学生将所学知识运用到实际中去。

关键词

矩阵，子空间，编码

The Application of Linear Algebra in Network Coding

Shuangqing Liu

School of Mathematical Sciences, Suzhou University of Science and Technology, Suzhou Jiangsu

Received: Sep. 26th, 2022; accepted: Oct. 26th, 2022; published: Nov. 1st, 2022

Abstract

Linear algebra is a common required course in science and engineering departments in universities. However, many students are not very well establish the relationship between learned knowledge and practical question after learning this course. This paper mainly introduces the application of linear algebra to subspace codes, which play an important role in the network coding, and also guides the students to apply learned knowledge to practice question.

Keywords

Matrix, Subspace, Coding

文章引用: 刘双庆. 浅谈线性代数在网络编码中的应用[J]. 教育进展, 2022, 12(11): 4231-4235.
DOI: 10.12677/ae.2022.1211646

1. 引言

在传统路由网络中，网络节点只能执行数据的复制和转发这两项操作，不能对接收到的数据进行相应的线性、非线性的编码操作，从而对信息的传输造成了不便。为了解决此问题，Ahlswede 等人[1]在 2000 年提出的网络编码的概念。作为一种新型网络数据传输方式，网络编码具有平衡网络链路的负载、提高宽带利用率、增强传输安全性等优点。

为了使网络编码更加的具有实用性，Ho 等人[2]进一步提出了随机网络编码的概念。如今它也被广泛应用于社交网络、P2P、分布式存储系统、BT 下载等各领域。虽然随机网络编码方法可以在结构动态变化的网络(如无线网络)环境中以很高的概率成功传输信息，但网络信道中数据包的丢失和错误问题仍为影响其传输性能的主要因素。为了纠正错误的数据和恢复数据包丢失的数据，Kötter 和 Kschischang [3]提出子空间码模型，并证明了当 $4t+2s$ 小于等于给定的子空间距离时，子空间码可以纠正 t 个数据包错误和恢复 s 个数据包遗失。

子空间码的传输模型可由其空间对应的基矩阵来刻画。假设发送矩阵 $\boldsymbol{X}$ 的行向量为数据包，利用满秩的随机传输矩阵 $\boldsymbol{F}$ 进行编码，理想状况下，接收方收到矩阵 $\boldsymbol{FX}$ 的行向量为接收到的数据包。即如果将发送矩阵的行所张成的向量空间当作码字，接收端可以正确地恢复出发送的空间。然而，当有插入错误发生(如恶意攻击)时，发送空间将是接收空间的一个子空间。而当有删除发生(如数据包丢失)时，接收到的空间将是发送空间的一个子空间。在此情况下，子空间编码也可以恢复出发送的空间。

子空间编码作为网络编码的核心问题之一，受到了广泛的关注。本文主要介绍利用有限域上的矩阵和线性子空间等知识构造子空间码。本文结构如下：第 2 章介绍子空间码方面的一些基础知识；第 3 章利用秩度量码给出子空间码的提升构造方法；第 4 章是对本文的总结与展望。

2. 预备知识

在本文中，F_q 表示 q 阶有限域，F_q^n 表示 F_q 上所有 n 长向量的集合，即 F_q 上的 n 维向量空间，$F_q^{m\times n}$ 表示 F_q 上所有 $m\times n$ 的矩阵的集合，$P_q(n)$ 表示 F_q^n 上的所有子空间构成的集合，$G_q(n,k)$ 表示 F_q^n 上的所有 k 维子空间构成的集合。

2.1. 子空间距离和子空间码

由于子空间码是一种距离纠错码，所以下面先给出子空间距离和子空间码[3]的概念。

定义 1 [3]对于任意两个子空间 $\mathrm{U},\mathrm{V}\in G_q(n,k)$，定义其子空间距离为

$$d_s=\dim(\mathrm{U}+\mathrm{V})-\dim(\mathrm{U}\cap\mathrm{V}).$$

定义 2 [3]称 $\mathrm{C}\subseteq P_q(n)$ 是一个参数为 $(n,d)_q$ 的子空间码，如果 C 中任意两个码字的子空间距离大于等于 d。C 中的每个子空间都称为子空间码的一个码字。进一步，若 C 中所有码字都是 k 维的，则称 C 是参数为 $(n,|\mathrm{C}|,d,k)_q$ 的常维子空间码，$|\mathrm{C}|$ 表示子空间码 C 中的码字个数。

由线性代数知识可知，任何一个线性空间都可以由其一组基来刻画。为了保证表示的唯一性，这里采用行最简基矩阵表示。

定义 3 [3] 一个基矩阵称为行最简基矩阵，若此矩阵满足：

1) 每一行左起的第一个非零元(非零首元)为 1，并且此非零元所在的列除了它本身其它位置皆为 0；
2) 任取两行的非零首元，记其位置为分别为$(i_1,j_1),(i_2,j_2)$，则当$i_1<i_2$，有$j_1<j_2$。

利用行最简基矩阵，可以唯一的表示子空间[4] [5]。故本文利用线性空间所对应的行最简基矩阵表示其对应的线性空间。

2.2. 秩距离和秩度量码

定义 4 [6] [7] 对于两个矩阵$\boldsymbol{A},\boldsymbol{B}\in F_q^{m\times n}$，定义其秩距离为

$$d_R(\boldsymbol{A},\boldsymbol{B})=rank(\boldsymbol{A}-\boldsymbol{B}).$$

定义 5 [6] [7]称$C\subseteq F_q^{m\times n}$是一个参数为$[m\times n,k,d]_q$秩度量码，若 C 是 k 维线性子空间，并且满足任意两个码字的秩距离大于等于 d。由码的线性性，易知 C 中的每一个非零码字的秩皆大于等于 d。对于秩度量码，有如下的 Singleton 型上界[6] [7]。

定理 1 对于任意的$[m\times n,k,d]_q$秩度量码，有

$$k\le\max\{m,n\}(\min\{m,n\}-d+1)$$

成立。

证明：不失一般性，可假设$m\ge n$ (否则可考虑其转置)。设 C 是一个参数为$[m\times n,k,d]_q$的秩度量码。记$\bar{C}$表示 C 中的所有码字都删除最右侧$d-1$列后所形成的秩度量码。则$\bar{C}$中的每个码字都是尺寸为$m\times(n-d+1)$的矩阵。因为 C 中的每一个非零码字的秩皆大于等于 d，且每个码字删除$d-1$列后秩最多减小$d-1$，所以$\bar{C}$中的码字仍旧是两两不同的，并且秩距离大于等于 1。此外，由 C 的线性，可得知$\bar{C}$也是线性的，即为一个线性空间。

综上所述，可知$\bar{C}$是一个参数为$[m\times(n-d+1),k,1]_q$的秩度量码。又因为F_q上的尺寸为$m\times(n-d+1)$、且两两不同(即秩距离大于等于 1)的矩阵至多有$q^{m(n-d+1)}$个，即这些矩阵最大可生成一个$m\times(n-d+1)$维的线性子空间。所以，$k\le m(n-d+1)$。

若定理中等号成立时，称之为最大秩度量码，记为 MRD$[m\times n,d]_q$码。Delsarte [6]和 Gabidulin [7]分别于 1978 年和 1985 年独立构造出了第一类 MRD 码：Gabidulin 码，从而证明了任意参数的秩度量码都可达到此上界，并确定了 MRD 码的秩分布。Gabidulin 码可以由摩尔(Moore)矩阵构造。例如一个参数为$[m\times n,d]_q$的 MRD 码，可由如下摩尔矩阵构造：

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{q^{n-d}} & g_2^{q^{n-d}} & \cdots & g_n^{q^{n-d}} \end{pmatrix},$$

其中，$g_1,g_2,\cdots,g_n\in F_{q^m}$是$F_q$-线性无关的元素。摩尔矩阵也可以看作范德蒙德矩阵的 q 模拟。

3. 子空间码的提升构造

不利用最大秩度量码和子空间的基矩阵表示，Silva 等人[8]提出了一种简单有效构造渐近最优子空间码的方法——提升最大秩度量码的构造法。

定理 2 存在参数为$\left(n,q^{(n-k)\left(k-\frac{d}{2}+1\right)},d,k\right)_q$的常维数子空间码。

证明：构造

$$\mathrm{C}=\left\{\left(I_k \mid \boldsymbol{A}\right): \boldsymbol{A} \in \overline{\mathrm{C}}\right\},$$

其中 $\overline{\mathrm{C}}$ 是 MRD$\left[k\times(n-k), \frac{d}{2}\right]_q$ 码。易得，C 的码字个数即为所填充的 MRD 码的码字个数，所以由定理 1 可知，

$$|\mathrm{C}|=|\overline{\mathrm{C}}|=q^{(n-k)\left(k-\frac{d}{2}+1\right)}.$$

下面验证其子空间距离。任取两个码字 $\boldsymbol{U}=\left(\boldsymbol{I}_k \mid \boldsymbol{A}\right), \boldsymbol{V}=\left(\boldsymbol{I}_k \mid \boldsymbol{B}\right) \in \mathrm{C}$，由子空间距离的定义可知，

$$d_s(\boldsymbol{U}, \boldsymbol{V})=\dim(\boldsymbol{U}+\boldsymbol{V})-\dim(\boldsymbol{U} \cap \boldsymbol{V}),$$

应用维数公式可得，

$$d_s(\boldsymbol{U}, \boldsymbol{V})=2\dim(\boldsymbol{U}+\boldsymbol{V})-\dim(\boldsymbol{U})-\dim(\boldsymbol{V}),$$

由和空间的定义可知，和空间 $\boldsymbol{U}+\boldsymbol{V}$ 是由 $\boldsymbol{U}$ 中的一组基和 $\boldsymbol{V}$ 中的一组基生成的空间，所以 $\dim(\boldsymbol{U}, \boldsymbol{V})=rank\begin{pmatrix}\boldsymbol{U}\\ \boldsymbol{V}\end{pmatrix}$。

又因为 $\boldsymbol{U}, \boldsymbol{V}$ 都是 k 维的，故，

$$\begin{aligned}
d_S(\boldsymbol{U}, \boldsymbol{V}) &= 2rank\begin{pmatrix}\boldsymbol{U}\\ \boldsymbol{V}\end{pmatrix}-2k \\
&= 2rank\begin{pmatrix}\boldsymbol{U}\\ \boldsymbol{V}\end{pmatrix}-2k \\
&= 2rank\begin{pmatrix}\boldsymbol{I}_k & \boldsymbol{A}\\ \boldsymbol{I}_k & \boldsymbol{B}\end{pmatrix}-2k \\
&= 2rank\begin{pmatrix}\boldsymbol{I}_k & \boldsymbol{A}\\ \boldsymbol{O} & \boldsymbol{B}-\boldsymbol{A}\end{pmatrix}-2k \\
&= 2rank(\boldsymbol{B}-\boldsymbol{A}) \\
&\geq d.
\end{aligned}$$

综上所述，C 是一个参数为 $\left(n, q^{(n-k)\left(k-\frac{d}{2}+1\right)}, d, k\right)_q$ 的常维数子空间码。

4. 结论

子空间码作为一类新型的纠错码，与经典的纠错码有所不同。首先，子空间码的每个码字都是一个线性空间，经典的纠错码的每个码字是一个向量；其次，子空间码中应用的度量是子空间度量，经典纠错码中应用的度量为汉明度量。子空间码模型更适用于随机的网络编码。本文主要介绍线性代数在构造子空间码方面的应用。关于子空间码的进一步构造，可以结合文献[9] [10]进一步提升子空间码的下界。此外，线性代数在经典的线性纠错码[11]领域也有许多重要的应用。但在实际教学中，如何巧妙的将线性代数的理论知识与相关的应用问题联系起来，引导学生更好的学以致用，也是需要进一步探索的问题。

基金项目

江苏省自然科学基金(BK20210858)。

参考文献

[1] Ahlswede, R., Cai, N., Li, S. and Yeung, R.W. (2000) Network Information Flow. *IEEE Transactions on Information Theory*, **46**, 1204-1216. https://doi.org/10.1109/18.850663

[2] Médard, M., Koetter, R., Karger, D.R., Effros, M., Shi, J. and Leong B. (2006) A Random Linear Network Coding Approach to Multicast. *IEEE Transactions on Information Theory*, **52**, 4413-4430. https://doi.org/10.1109/TIT.2006.881746

[3] Kötter, R. and Kschischang, F.R. (2008) Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information Theory*, **54**, 3579-3591. https://doi.org/10.1109/TIT.2008.926449

[4] 吴建荣, 谷建胜. 线性代数[M]. 北京: 高等教育出版社, 2009.

[5] 丘维声. 简明线性代数[M]. 北京: 北京大学出版社, 2002.

[6] Delsarte, P. (1978) Bilinear Forms over a Finite Field, with Applications to Coding Theory. *Journal of Combinatorial Theory A*, **25**, 226-241. https://doi.org/10.1016/0097-3165(78)90015-8

[7] Gabidulin, È.M. (1985) Theory of Codes with Maximum Rank Distance. *Problemy Peredachi Informatsii*, **21**, 3-16.

[8] Silva, D., Kschischang, F.R. and Kötter, R. (2008) A Rank-Metric Approach to Error Control in Random Network Coding. *IEEE Transactions on Information Theory*, **54**, 3951-3967. https://doi.org/10.1109/TIT.2008.928291

[9] Liu, S., Chang, Y. and Feng, T. (2020) Parallel Multilevel Constructions for Constant Dimension Codes. *IEEE Transactions on Information Theory*, **66**, 6884-6897. https://doi.org/10.1109/TIT.2020.3004315

[10] Niu, Y., Yue, Q. and Huang, D. (2022) New Constant Dimension Subspace Codes from Parallel Linkage Construction and Multilevel Construction. *Cryptography and Communications*, **14**, 201-214. https://doi.org/10.1007/s12095-021-00504-z

[11] 冯克勤. 纠错码的代数理论[M]. 北京: 清华大学出版社, 2005.