Advances in Applied Mathematics 应用数学进展, 2021, 10(3), 651-653
Published Online March 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.103070

Hans汉斯

[10, 3, 5]二元线性码的构造

刘　颖，牛　帅，许　娟

临沂大学数学与统计学院，山东　临沂
Email: xujuan0120@126.com

收稿日期：2021年2月8日；录用日期：2021年3月3日；发布日期：2021年3月10日

摘　要

本文恰当地利用了二元[7, 4, 3]汉明码的校验矩阵构造了[10, 3, 5]二元线性码，并论述这一方法可以推广到其他元码的构造中。

关键词

线性码，汉明码，推广

The Construction of [10, 3, 5] Binary Linear Codes

Ying Liu, Shuai Niu, Juan Xu

School of Mathematics and Statistics, Linyi University, Linyi Shandong
Email: xujuan0120@126.com

Received: Feb. 8th, 2021; accepted: Mar. 3rd, 2021; published: Mar. 10th, 2021

Abstract

In this paper, we construct [10, 3, 5] binary linear codes by using the check matrix of [7, 4, 3] binary Hamming codes, and discuss that this method can be extended to the construction of other linear codes.

Keywords

Linear Code, Hamming Code, Extend

文章引用: 刘颖, 牛帅, 许娟. [10, 3, 5]二元线性码的构造[J]. 应用数学进展, 2021, 10(3): 651-653.
DOI: 10.12677/aam.2021.103070

1. 引言

在 F_q 上的线性码(或称线性分组码) C 是线性空间 F_q^n 中的子空间。特别地，当 $q=2$ 时，称为二元线性码。如果这个线性子空间的维数是 k，则称 C 是一个 $[n,k]$ 码，其中 n 是码长，k 是码的维数。对于线性码 C，若又有 $d=d(C)=\min\{w(c),c\neq 0\in C\}$，即 d 是 C 中所有 q^k-1 个非零码字中 Hamming 权的最小值，则记线性码 C 为 $[n,k,d]$ 码。设 $c_i=(c_{i1},c_{i2},\cdots,c_{in}),i=1,2,\cdots,k$ 是 F_q 上的 k 个线性独立的码字，即构成 C 的一组基，这样，对于 C 中的每一个码字 $c=(c_1,c_2,\cdots,c_n)$ 总存在 k 个在 F_q 中的系数 $a_1,a_2,\cdots,a_k$ 使得 $c=(c_1,c_2,\cdots,c_n)=(a_1,a_2,\cdots,a_k)\begin{pmatrix}c_{11}&c_{12}&\cdots&c_{1n}\\c_{21}&c_{22}&\cdots&c_{2n}\\\vdots&\vdots&\ddots&\vdots\\c_{k1}&c_{k2}&\cdots&c_{kn}\end{pmatrix}$。一个 $k\times n$ 矩阵为码 C 的生成矩阵，如果它的行向量构成 C 的一组基，通常用 G 来表示生成矩阵，若有 $GH^{\mathrm{T}}=0$ 则 H 称为该码的校验矩阵[1] [2]。

2. [10, 3, 5]二元线性码的构造

我们首先确定一个含有八个码字且能纠正 2 个错误位的码长应该是 $n\geq 10$ 的。根据二元码的 Plotkin 界知，一个码长为 9 并且最小距离为 5 的二元码最多含有 6 个码字。设一个参数为 $(9,K,5)$ 的二元码 C^1，由此再重新考虑一个新码 $C=\{(c_1,c_2,\cdots,c_9,c_{10})|(c_1,c_2,\cdots,c_9)\in C^1,c_1+c_2+\cdots+c_9+c_{10}=0\}$，于是，新码 C 的参数为 $(10,K,6)$，由于 $\left[\frac{d}{2d-n}\right]=\left[\frac{6}{2\times 6-10}\right]=3$，从而 $K\leq 2\left[\frac{d}{2d-n}\right]=6$，于是我们可以确定一个含有八个码字且能纠正 2 个错误位的码字长度至少为 10。

汉明码是一类非常重要的完全线性码，设 $m\geq 2$，以 $H_m=(u_1,u_2,\cdots,u_n)$ 为校验矩阵的 q 元线性码叫做汉明码，其中 $u_i,i=1,2,\cdots,n$ 是 F_q^m 中 q^m-1 个非零向量的各等价类里面的代表向量，长度为 m，每个等价类里面恰有 $q-1$ 个向量。汉明码的参数为 $[n,k,d]=\left[\frac{q^m-1}{q-1},\frac{q^m-1}{q-1}-m,3\right]$，当 $q=2$ 时，二元汉明码的参数为 $[n,k,d]=[2^m-1,2^m-1-m,3]$，若又 $m=3$，此时 $[n,k,d]=[7,4,3]$ 且

$$H_3=(u_1,u_2,\cdots,u_7)=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}。$$

在校验矩阵 H_3 中，我们发现向量的长度为 7，每行向量的非零元个数为 4，且两两向量相加的非零元个数是 4，三个向量相加得到的向量非零个数亦是 4。

我们要构造的二元线性码含有 8 个码字，信息元为三位，即

$$m_0=(0,0,0),m_1=(0,0,1),m_2=(0,1,0),m_3=(0,1,1),$$
$$m_4=(1,0,0),m_5=(1,0,1),m_6=(1,1,0),m_7=(1,1,1)$$

从中选取任意三个相互独立的向量与 H_3 中的行向量共同组成[10, 3, 5]码的生成矩阵 G。比如，我们选取 $m_1=(0,0,1)$, $m_2=(0,1,0)$, $m_4=(1,0,0)$ 并适当调整排列顺序得到系统码的生成矩阵，即生成矩阵

$G=\begin{pmatrix}c_1\\c_2\\c_3\end{pmatrix}=\begin{pmatrix}1&0&0&0&0&0&1&1&1&1\\0&1&0&0&1&1&0&0&1&1\\0&0&1&1&0&1&0&1&0&1\end{pmatrix}=(I_3,H_3)$，其中$c_1,c_2,c_3$为三个相互独立的码字且码重都为5。

由$k_1c_1+k_2c_2+k_3c_3,k_i=0,1$我们可以得到八个码字，即$c_0=(0,0,0,0,0,0,0,0,0,0)$，$c_1=(1,0,0,0,0,0,1,1,1,1)$，$c_2=(0,1,0,0,1,1,0,0,1,1)$，$c_3=(0,0,1,1,0,1,0,1,0,1)$以及$c_4=(1,1,0,0,1,1,1,1,0,0)$，$c_5=(1,0,1,1,0,1,1,0,1,0)$，$c_6=(0,1,1,1,1,0,0,1,1,0)$和$c_7=(1,1,1,1,1,0,1,0,0,1)$，显然，构造出的码最小距离为5，可以检出4位错误并能纠正2位错误。

由于汉明码校验矩阵的形式，上述我们得到的构造方法可以推广到其他元码字的构造，比如$q=3,m=3$，此时三元汉明码的校验矩阵为

$$H_3=(u_1,u_2,\cdots,u_{13})=\begin{pmatrix}1&0&0&0&0&1&1&1&1&1&1&1&1\\0&1&0&1&1&0&0&1&2&1&1&2&2\\0&0&1&1&2&1&2&0&0&1&2&1&2\end{pmatrix}$$

我们可以构造码长为13的三元线性码。

致　谢

在学习和本论文的写作过程中，我们得到了许娟老师的悉心指导和帮助，在此向她表示感谢！

基金项目

山东临沂大学大学生创新创业训练计划项目编号X202010452128。

参考文献

[1] 冯良贵, 吴新文, 著. 代数几何码[M]. 北京: 科学出版社, 2000.

[2] 冯克勤, 著. 纠错码的代数理论[M]. 北京: 清华大学出版社, 2006.