3131100063 · **编码理论**

Review 第五章 RM 码

胡玉斌 / 202111054

October 11, 2021

线性码性质回顾

定义 1

一个码长为 n 的 p 元码 C 叫做线性码，是指 C 是向量空间 F_p^n 的向量子空间，即 C 满足如下的性质：对 F_p 中任意元素 α 和 β，如果 c_1 和 c_2 属于 C，则 $\alpha c_1+\beta c_2$ 也属于 C。

定理 1

设 C 是参数为 $[n,k]$ 的 p 元线性码。

(1) 若 G 是 C 的一个生成矩阵，而 H 是 F_p 上一个 $(n-k)$ 行 n 列的矩阵，则 H 是 C 的一个校验矩阵当且仅当 $rank(H)=n-k$，并且 $HG^T=0_{n-k,k}$

(2) 若 $G=(I_k,P)$，$H=(=P^T,I_{n-k})$，则 G 是 C 的一个生成矩阵上去仅当 H 是 C 的一个校验矩阵

定义 2

设 C 是一个 p 元线性码，参数为 n,k,d。从 C 是 F_p^n 的一个 k 维向量子空间。考虑 F_p^n 中的如下子集和：

$$C'=\{a\in F_p^n|\forall\ c\in C,(a,c)=0\}$$

即 C' 是与 C 中所有码字都正交的那些向量组成的集合。称 C' 为 C 的对偶码。

定理 2

若 C 是参数为 $[n,k]$ 的 p 元线性码。则 C' 也是 p 元线性码，码长和信息位数分别为 n 和 $n-k$。

如果 $C\in C'$，称 C 为自正交码。如果 $C=C'$，称 C 为自对偶码。

RM 码的定义

定义 3

设 m 为正整数。一个 m 元布尔函数 $f=f(x_1,...,x_m)$ 是由 F_2^m 到 F_2 的映射，即 m 个变量 $x_1,...,x_m$ 均取值于 F_2，并且函数值也属于 F_2。

由于 F_2^m 中向量的个数为 2^m，而 f 在每个向量的取值均彼此独立地可取 1 或 0，所以 m 元布尔函数共有 2^{2^m} 。

定理 3

每个 m 元布尔函数 $g(x_1,...,x_m)$ 均可唯一地表示为 $g(x_1,...,x_m)=c+c_1x_1+..+c_mx_m+c_{12}x_1x_2+c_{13}x_1x_3+...+c_{m-1,m}x_{m-1}x_m+c_{123}x_1x_2x_3+...+c_{12...m}x_1x_2...x_m$(其中所有系数和常数都属于 F_2)

定义 4

设 $m \geq 1, n = 2^m, 0 \leq r \leq m$。向量空间 F_2^n 的子集合

$$RM(r,m) = \{c_f = (f(v_0), f(v_1), ..., f(v_{n-1})) \in F_2^n | f \in B_m, deg(f) \leq r\}$$

叫做 r 阶的 Reed-Muller 码 (简称 RM 码)。这里 $v_i \in F_2^m$

定理 4

设 $m \geq 1, f \in B_m$，当 $r \leq m-1$ 时，$w(c_f)$ 为偶数。

定理 5

RM 码 $RM(r,m)$ 是线性码，基本参数为 $[n,k,d] = [2^m, \sum_{t=0}^{r} \binom{m}{t}, 2^{m-r}]$。

定理 6

当 $0 \leq m-1$ 时，$RM(r,m)$ 的对偶码为 $RM(m-r-1.m)$。

RM 码的编译码

1. RM 码的生成矩阵
2. RM 码的校验矩阵
3. RM 码编译码实例

心得体会 & 建议

第一次翻转课堂，同学准备用心，ppt 也很棒，上台讲课的同学很卖力。美中不足的是，内容有些许枯燥，例子不够充分，证明不够明确，给我们后面的同学也是一种提醒。