

引用格式:张永光. RM 码特征分析[J]. 微电子学与计算机, 2020, 37(5): 39-42. [ZHANG Y G. Research on RM code feature analysis [J]. Microelectronics & Computer, 2020, 37(5): 39-42.]

RM 码特征分析

张永光^{1,2}

(1 通信信息控制和安全技术重点实验室, 浙江 嘉兴 314033;

2 中国电子科技集团公司 第 36 研究所, 浙江 嘉兴 314033)

摘 要: 针对 RM 码的特征分析问题, 通过线性变换确定等价系统码的生成矩阵, 从而确定分析码字的码长和信息位长, 结合对码长取值、生成矩阵行重的约束, 假定分析数据采用 RM 编码, 求出 RM 码阶数, 得到 RM 码的生成矩阵, 如等价系统码的生成矩阵可从 RM 码的生成矩阵通过行线性组合得到, 则可确认采用了 RM 编码, 且生成矩阵求解正确. 实验仿真表明, 在仅得到码编码数据序列的情况下, 实际数据的编码参数识别分析结果和所设前提完全一致, 表明了分析方法的正确性.

关键词: RM 码; 生成矩阵; 码重; 线性变换

中图分类号: TN971

文献标识码: A

文章编号: 1000—7180(2020)05—0039—04

Research on RM code feature analysis

ZHANG Yong-guang^{1,2}

(1 Science and Tech. on Communication Information Security Control Lab, Jiaxing 314033, China;

2 The 36th Research Institute of CETC, Jiaxing 314033, China)

Abstract: For the feature analysis problem of RM code, the generator matrix of the equivalent system code is determined by linear transformation, thereby determining the code length and information length of the analyzed codeword, combining the constraints on the row weight of the generator matrix, assuming that the analysis data is RM coded, the RM code order is obtained, and the generator matrix of the RM code is obtained. If the generation matrix of the equivalent system code can be obtained by linear combination of the generator matrix of the RM code, it can be confirmed that the RM code is used and the generator matrix is solved correctly. The experimental simulation shows that the recognition result of the coding parameters of the actual data is exactly the same as the premise of the RM code encoded data sequence, which indicates the correctness of the analysis method.

Key words: RM code; generator matrix; code weight; linear transform

1 引言

RM 码是一类经典的线性分组码, 由 Muller 于 1954 年提出^[1], RM 码同时也是一种代数码. 虽然 RM 码的纠错性能不如 Turbo 码或 LDPC 码, 但 RM 码也有诸多优点, 如译码延时短, 无错误平层现象, 其误码率会随着信噪比增加无限趋近于零, 故而 RM 码可适应多种不同的信道, 满足有实时性要求

的应用环境, 既可单独使用, 也可作为内码与 RS 码等级联使用, 从而大大提升纠错性能.

RM 码作为一种不等保护码, 经常用于保护某些重点位置上的信息, 如在 DVB-S2 和 Tetra 中的应用^[2]. 深空通信领域, RM 码早在 1972 年就被用于传输“水手号”发送的火星照片. 通用移动通信领域, RM 码也获得了广泛应用, 3GPP 物理层技术很多都采用了 RM 码, 如 TD-SCDMA 和 LTE 等. 作

为 5G 时代编码方案的极化码与 RM 码有天然的相似性,极化码可看作 RM 码的另一种形式,人们甚至一度认为 RM 码可以取代极化码^[3].

2 RM 码概念及特征

同一般线性分组码一样,可以通过生成矩阵来定义 RM 码. 对于两个正整数 r 和 m ,存在一个 r 阶码长为 $n = 2^m$ 的 RM 码. 生成矩阵 $\mathbf{G}$ 由矩阵块 $\mathbf{G}_0, \mathbf{G}_1, \dots, \mathbf{G}_r$ 组成

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \vdots \\ \mathbf{G}_r \end{bmatrix}$$

式中, $\mathbf{G}_0$ 是码长为 2^m 的全 1 向量, $\mathbf{G}_1$ 是 $m \times 2^m$ 阶矩阵,由所有 m 重二进制列向量组成,且从左至右的各列依顺序递增, $\mathbf{G}_1$ 的最左列为全 0 向量,最右列为全 1 向量. $\mathbf{G}_i$ 的行是由所有 $\mathbf{G}_1$ 的 i 个行向量作逻辑积所得的向量组成,故 $\mathbf{G}_i$ 是一个 $C_m^i \times 2^m$ 阶矩阵.

当 $\mathbf{G}$ 的各行线性无关时, r 阶 RM 码的信息位最小码距为 2^{m-r} , 如 $m = 3, r = 1$, 则存在 (8, 4) RM 码, 当 $m = 4, r = 1, 2, 3$ 时, RM 码的编码参数分别为 (16, 5), (16, 11), (16, 15).

$$k = \sum_{i=0}^r C_m^i$$

由于一阶 RM 码拥有特殊结构可以实现快速的极大似然译码, 因而实际使用最广泛的是一阶 RM 码.

如 $r = 0, k = 1$, 生成矩阵为 $n = 2^m$ 的 RM 码为全 1 向量 v_0 , 是一种重复码. 如 $r = 1, k = m + 1$, 生成矩阵为 $(m + 1) \times 2^m$ 阶矩阵的 RM 码, 第一行为 v_0 , 其余 m 行为 $v_i, i = 1, 2, \dots, m$, 其中

$$v_i = \underbrace{0 \dots 0}_{2^{i-1}} \underbrace{1 \dots 1}_{2^{i-1}} \dots \underbrace{0 \dots 0}_{2^{i-1}} \underbrace{1 \dots 1}_{2^{i-1}}$$

可见每一行长均为 2^m , 由 2^{m-i+1} 个交替的连 0、连 1 段组成, 每段长为 2^{i-1} .

从 RM 码的定义可以看出, 一个 r 阶 RM 码可以通过增广一个 $(r-1)$ 阶 RM 码得到, 而一个 $(r-1)$ 阶 RM 可以由删信一个 r 阶 RM 码而获得. 对高阶 (> 1) RM 码, 其生成矩阵除了包含 v_0 和 v_i 外, 还包含 v_i 之间的相互乘积. 记 $v_{x_1 x_2 \dots x_i} = v_{x_1} v_{x_2} \dots v_{x_i}$, 各矢量相同位置上的元素需要进行模 2 乘. 生成矩阵具有如下形式

$$\mathbf{G} = [\underbrace{v_0}_{G_0}; \underbrace{v_1 \dots v_m}_{G_1} \dots \underbrace{v_{12 \dots i} \dots v_{(m-i)(m-i+1) \dots m}}_{G_i} \dots \underbrace{v_{12 \dots i} \dots v_{(m-1)(m-1+1) \dots m}}_{G_i}]$$

包含了所有 r 个或以下的 v_i 点对点乘积.

如对 $m = 3, r = 2$ 时的 (8, 7) RM 码

$$\mathbf{G}_0 = [11111111] = [v_0]$$

$$\mathbf{G}_1 = \begin{bmatrix} 01010101 \\ 00110011 \\ 00001111 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

$$\mathbf{G}_2 = \begin{bmatrix} 00010001 \\ 00000101 \\ 00000011 \end{bmatrix} = \begin{bmatrix} v_{12} \\ v_{13} \\ v_{23} \end{bmatrix}$$

对 r 阶 RM 码, 生成矩阵 $\mathbf{G}$ 中 $\mathbf{G}_i$ 的每行重量为 2^{m-i} , $\mathbf{G}$ 的每行都为偶重量, 因而 $\mathbf{G}$ 的行线性组合也为偶重量^[4], 故 RM 码的码字重量均为偶数, 且最小重量不大于 2^{m-r} .

由于 RM 码为非系统码, 因此一般分析线性分组码的方法并不能直接用于分析 RM 码, 需要根据 RM 码的特征讨论 RM 码的分析方法.

在仅获取比特流序列的情况下, 从 RM 码的定义可以看出, RM 码的分析问题就是通过对比特流序列进行处理分析, 解决以下问题:

(1) 该比特流序列是否采用了 RM 编码?

(2) 如采用 RM 编码, RM 码的 r, n, k, m 值为多少?

(3) 确定 RM 码的生成矩阵.

需要指出的是, RM 码的译码算法 (如 Reed 算法择多逻辑判决法) 只与生成矩阵各行向量相关, 而与各行向量的先后顺序无关, 所以 RM 码生成矩阵的分析只需分析得到各行量即可进行译码恢复, 而无需恢复其顺序.

3 RM 码参数分析

RM 码的参数分析难点在于其为非系统码, 虽然非系统码和系统码之间的生成矩阵可以相互转化, 并且它们的编码约束度、线性约束关系也完全相同, 但在译码恢复编码前数据时, 必须采用正确的生成矩阵, 否则得不到正确的编码前数据.

对 RM 码这样的线性分组码, 如采用常规方法进行分析, 从获得的比特流数据数据构造识别序列 $\mathbf{C}$, 通过各种识别分析法得到校验矩阵 $\mathbf{H}$ ^[5], 且 $\mathbf{H}$ 满足如下关系

$$\mathbf{C}\mathbf{H}^T = 0$$

进一步,生成矩阵 $\mathbf{G}$ 和校验矩阵 $\mathbf{H}$ 之间满足 $\mathbf{GH}^T = \mathbf{0}$

对系统码而言,校验矩阵和生成矩阵是一对一的关系,但非系统码的校验矩阵和生成矩阵则是一对多的关系.实数域情况下,从 $\mathbf{GH}^T = \mathbf{0}$ 求解 $\mathbf{G}$,在有解的情况下必然存在着无穷多个满足方程组的解.

在得到校验矩阵 $\mathbf{H}$ 后,虽然无法从 $\mathbf{GH}^T = \mathbf{0}$ 求解 $\mathbf{G}$,但从 $\mathbf{H}$ 可以直接得到线性分组码的码长 n 和信息位长 k .

对 RM 码的分析即基于 $n, k, \mathbf{H}$ 开展.

从校验矩阵 $\mathbf{H}$,可直接得到线性约束关系上等价的系统码生成矩阵 $\mathbf{G}'$,且 $\mathbf{G}'$ 必定能由 RM 码的生成矩阵 $\mathbf{G}$ 通过初等变换得到.

由于 $n = 2^m$,则 $m = \log_2 n$,故如 $\log_2 n$ 不为整数,则可直接判断该数据未采用 RM 编码.

又 RM 码的码字重量均为偶数, $\mathbf{G}'$ 因是 $\mathbf{G}$ 的行线性组合也必为偶重量,故如 $\mathbf{G}'$ 的各行重量有非偶数的情况,则可直接判断为非 RM 码数据.

进一步,由 $m = \log_2 n$ 和 $k = \sum_{i=0}^r C_m^i$,求出 r .

当假定分析数据采用 RM 编码时,从已经确定的 r, n, k, m ,结合 RM 码生成矩阵特征,可直接求出 RM 码的生成矩阵

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \vdots \\ \mathbf{G}_r \end{bmatrix}$$

从 $\mathbf{G}$ 出发,如 $\mathbf{G}'$ 各行均可从 $\mathbf{G}$ 的行线性组合得到,则可判断分析数据采用了 RM 编码,且其生成矩阵为 $\mathbf{G}$,如 $\mathbf{G}'$ 各行不能从 $\mathbf{G}$ 的行线性组合得到,则判断为非 RM 码数据. RM 码的参数分析流程如图 1 所示.

4 分析举例

以对 $m = 4, r = 1$ 时的(16,5)RM 码的参数分析为例,其生成矩阵

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \end{bmatrix}$$

其中

$$\mathbf{G}_0 = [1111111111111111] = [v_0]$$

$$\mathbf{G}_1 = \begin{bmatrix} 0101010101010101 \\ 0011001100110011 \\ 0000111100001111 \\ 0000000011111111 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix}$$

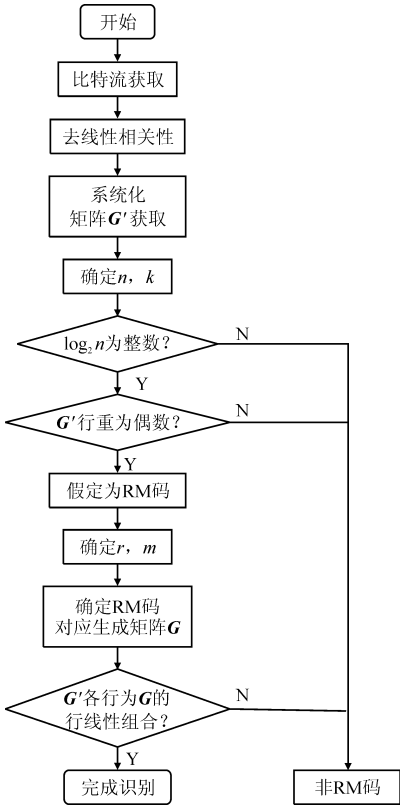


图 1 RM 码参数分析流程

对待分析的比特流数据,获取校验矩阵可采用基于矩阵初等行变换的单位化方法,但容错有限,也可采用具有一定容错能力的 Gauss-Jordan 消元法^[6]. 获取校验矩阵的过程其实就是去除相关长度内信息位的线性加权过程,目的是为了从编码数据中提取出最小的线性无关组,其中的校验位都可由信息位的线性加权得到,对信息位起约束作用.

对线性分组码求取校验矩阵和生成矩阵的具体方法见参考文献[5],单位化后的系统化简矩阵如图 2.

$$\begin{array}{cccccccccccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

图 2 单位化系统化简

从图 2 可得到等价系统码生成矩阵 $\mathbf{G}'$ 的行向量(图 2 下划线所示),可得

$$\mathbf{G}' = \begin{bmatrix} 1001011001101001 \\ 0101010101010101 \\ 0011001100110011 \\ 0000111100001111 \\ 0000000011111111 \end{bmatrix} = \begin{bmatrix} v_0' \\ v_1' \\ v_2' \\ v_3' \\ v_4' \end{bmatrix}$$

可见 $\mathbf{G}'$ 为 5×16 阶矩阵,可知线性分组码的码长 $n = 16$,信息位长 $k = 5$.

从 $m = \log_2 n = \log_2 16 = 4$ 为整数,不能判断分析数据未采用 RM 编码.

进一步,从 $\mathbf{G}'$ 中各行向量 $v_0', v_1', v_2', v_3', v_4'$ 重量均为偶数,也不能判断分析数据未采用 RM 编码.

由 $k = \sum_{i=0}^r C_m^i$,代入已知值, $5 = \sum_{i=0}^r C_4^i = C_4^0 + C_4^1 + C_4^2 + C_4^3 + C_4^4$,可得 $r = 1$.

当假定分析数据采用 RM 编码时,已确定 $r = 1, n = 16, k = 5, m = 4$. 结合 RM 码生成矩阵特征,可知 RM 码的生成矩阵

$$\mathbf{G} = \begin{bmatrix} 1111111111111111 \\ 0101010101010101 \\ 0011001100110011 \\ 0000111100001111 \\ 0000000011111111 \end{bmatrix} = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix}$$

从 $\mathbf{G}$ 出发,可知 $v_0' = v_0 + v_1 + v_2 + v_3 + v_4, v_1' = v_1, v_2' = v_2, v_3' = v_3, v_4' = v_4$. 可见 $\mathbf{G}'$ 各行均可从 $\mathbf{G}$ 的行线性组合得到,据此可判断分析数据采用了 RM 编码,且其生成矩阵为 $\mathbf{G}$.

5 结束语

本文提出了 RM 码的特征分析方法,通过线性

变换确定等价系统码的生成矩阵,从而确定分析码字的码长和信息位长,结合对码长取值、生成矩阵行向量重量的约束,可进行是否为 RM 编码的初步判断.进而假定分析数据采用 RM 编码,求出 RM 码阶数,得到 RM 码的生成矩阵,如等价系统码的生成矩阵可从 RM 码的生成矩阵通过行线性组合得到,则可确认采用了 RM 编码,且生成矩阵求解正确.

参考文献:

[1] MULLER D E. Application of Boolean algebra to switching circuit design and to error detection [J]. Transactions of the IRE Professional Group on Electronic Computers, 1954, EC-3(3): 6-12.

[2] ETSI TR 102 580 V1. 1. 1, Terrestrial Trunked Radio (TETRA); Release 2; Designer's Guide; TETRA High-Speed Data (HSD); TETRA Enhanced Data Service (TEDS) [S]. 2007: 54-59.

[3] ARIKAN E. A performance comparison of polar codes and Reed-Muller codes [J]. Communications Letters IEEE, 2008, 12(6): 447-449.

[4] 刘玉君. 信道编码[M]. 郑州: 河南科学技术出版社, 2001: 44-46.

[5] 张永光, 翟绪论. 比特流分析[M]. 北京: 电子工业出版社, 2018: 95-98.

[6] 黄丽, 湛稳固, 黄雨佳, 等. 信道编码中交织器的盲识别[J]. 强激光与粒子束, 2015, 27(10): 103250-2.

作者简介:

张永光 男, (1979-), 硕士, 研究员. 研究方向为通信信号处理. E-mail: 43766435@qq. com.

(上接第 38 页)

[11] 张玉龙, 张国山. 基于关键帧的视觉惯性 SLAM 闭环检测算法[J]. 计算机科学与探索, 2018, 12(11): 1777-1787.

[12] 侯荣波, 魏武, 黄婷, 等. 基于 ORB-SLAM 的室内机器人定位和三维稠密地图构建[J]. 计算机应用, 2017, 37(5): 1439-1444.

[13] 赵洋, 刘国良, 田国会, 等. 基于深度学习的视觉 SLAM 综述[J]. 机器人, 2017, 39(6): 889-896.

作者简介:

孙楠 女, (1993-), 硕士研究生. 研究方向为无人机视觉-

惯性导航.

裴信彪 男, (1990-), 博士, 助理研究员. 研究方向为多旋翼无人机多传感器的数据融合与控制方法.

王春军 男, (1983-), 硕士, 工程师. 研究方向为自动驾驶和视觉导航.

李继辉 男, (1994-), 硕士研究生. 研究方向为无人机目标检测.

彭程 女, (1987-), 博士, 助理研究员. 研究方向为微小型无人机自动控制.

白越(通讯作者) 男, (1979-), 博士, 研究员, 博士生导师. 研究方向为微小型无人飞行器动力学与控制.

E-mail: baiy@ciomp. ac. cn.