Hans Journal of Wireless Communications 无线通信, 2024, 14(6), 132-139
Published Online December 2024 in Hans. https://www.hanspub.org/journal/hjwc
https://doi.org/10.12677/hjwc.2024.146017

Hans汉斯

循环码的系统码计算方法研究

廖　源，许海霞*

仲恺农业工程学院信息科学与技术学院，广东 广州

收稿日期：2024年11月24日；录用日期：2024年12月17日；发布日期：2024年12月25日

摘　要

本文研究了循环码的系统码计算方法，提出一种新型的循环码系统码计算方法——线性变换法，与传统的公式推导法和多项式模N运算法相比，该方法不仅简化了计算过程，还在精确性和计算效率上表现出显著的优越性，具有一定的实际应用价值。

关键词

循环码，生成矩阵，线性变换法

Research on Systematic Encoding Computational Methods for Cyclic Codes

Yuan Liao, Haixia Xu*

College of Information Science and Technology, Zhongkai University of Agriculture and Technology, Guangzhou Guangdong

Received: Nov. 24th, 2024; accepted: Dec. 17th, 2024; published: Dec. 25th, 2024

Abstract

This paper investigates the systematic encoding computational methods for cyclic codes, proposing a novel approach termed the Linear Transformation Method for the systematic encoding computation of cyclic codes. Compared to traditional methods such as the formula-based approach and polynomial modulo *N* operation, this new method not only simplifies the computation process but also demonstrates significant advantages in terms of precision and computational efficiency, offering considerable practical application value.

Keywords

Cyclic Codes, Generate Matrix, Linear Transformation Method

*通讯作者。

文章引用: 廖源, 许海霞. 循环码的系统码计算方法研究[J]. 无线通信, 2024, 14(6): 132-139.
DOI: 10.12677/hjwc.2024.146017

1. 循环码的系统码概述

如果一个(n, k)线性分组码 C，其码组表示为$\left[a_{n-1}a_{n-2}\cdots a_k a_{k-1}\cdots a_2 a_1 a_0\right]$，将码组中的各码元按顺序循环左移(或右移)一位或多位得到的码组$C' \in C$，就称 C 为(n, k)循环码[1] [2]。循环码的生成多项式提供了一种简单的方法来构造循环码的系统码，在编码过程中，循环码的系统码是将原始信息码元和校验码元按照一定规则排列得到的码组。在循环码的系统码中，前 m 个码元通常是原始信息码元，其余的码元是监督码元。研究循环码的系统码具有以下意义：1) 提高数据传输的可靠性：通过在原始信息数据中嵌入校验监督码元，循环码可以检测和纠正传输过程中可能出现的错误。2) 提高数据传输的效率：循环码可以通过调整码距来平衡纠错能力和编码复杂度。3) 支持高速通信：在高速通信系统中，循环码的硬件实现可以提供快速的数据处理能力，满足高速通信的需求。4) 循环码的纠错性能优越，特别是在高信噪比条件下。循环码的系统码研究对于现代通信系统，尤其是无线通信、卫星通信和光纤通信等领域具有重要意义。它们在数据传输、存储和处理中扮演着关键角色，确保了数据的准确性和可靠性。

2. 循环码的系统码常用计算方法

2.1. 通过生成多项式公式推导得到循环码的系统码

在循环码中，一个(n, k)码有 $2k$ 个不同的码组。若用 $g(x)$表示生成多项式，其前$(k-1)$位皆为“0”，常数项为 1，且有唯一的$(n-k)$次方，则 $g(x)$，$x\cdot g(x)$，$x^2 g(x)$，…，$x^{k-1}g(x)$都是符合编码要求的码组，而且这 k 个码组是线性无关的，它们构成循环码的生成矩阵 G，写为

$$G(x)=\begin{bmatrix} x^{k-1}\cdot g(x) \\ x^{k-2}\cdot g(x) \\ \vdots \\ x\cdot g(x) \\ g(x) \end{bmatrix} \tag{1}$$

由生成矩阵 G 可以产生整个码组，即

$$\left[a_{n-1}a_{n-2}\cdots a_k a_{k-1}\cdots a_2 a_1 a_0\right]=\left[a_{n-1}a_{n-2}\cdots a_k a_{k-1}\right]\cdot G \tag{2}$$

上式简写为：

$$A=\left[a_{n-1}a_{n-2}\cdots a_k a_{k-1}\right]\cdot G \tag{3}$$

其中，$\left[a_{n-1}a_{n-2}\cdots a_k a_{k-1}\right]$为信息码元。具有$\left[I_k Q\right]$的生成矩阵叫做典型生成矩阵$G=\left[I_k Q\right]$，其中 I_k 为$k\times k$阶单位方阵。由典型生成矩阵得出的码组 A 中，信息位的位置不变，监督位附加于其后，这种形式的码称为系统码[3]。

2.2. 通过多项式模 N 运算得到循环码的系统码

循环码的码组除了用$\left[a_{n-1}a_{n-2}\cdots a_k a_{k-1}\cdots a_2 a_1 a_0\right]$表示，还可以用多项式的系数表示，即把一个长度为 n 的码组表示成：

$$A(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0 \tag{4}$$

其中，x 是码元位置的标记。多项式的码组可以通过多项式的模 N 运算得到，其运算法则为：当任意多项式 $D(x)$被一个 n 次方的多项式 $N(x)$相除时，可以得到一个商的多项式 $Q(x)$和一个最高次方小于 n 的余数多项式 $R(x)$。即

$$\frac{D(x)}{N(x)}=Q(x)+\frac{R(x)}{N(x)} \text{ 或 } D(x)=N(x)\cdot Q(x)+R(x) \tag{5}$$

则

$$D(x)\equiv R(x) \quad (\text{模 } N(x)) \tag{6}$$

在循环码中，若 $A(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$ 是一个长为 n 的许用码组，则 $x^i\cdot A(x)=a_{n-1}x^{n-1+i}+a_{n-2}x^{n-2+i}+\cdots+a_{n-1-i}x^{n-1}+\cdots+a_1x^{1+i}+a_0x^i$ 在按模 (x^n+1) 运算下，得到的余式 $A'(x)\equiv a_{n-1-i}x^{n-1}+a_{n-2-i}x^{n-2}+\cdots+a_0x^i+a_{n-1}x^{i-1}+\cdots+a_{n-i}$ 也是该编码中的一个许用码组，即

$$x^i\cdot A(x)\equiv A'(x) \text{ 模 } (x^n+1) \tag{7}$$

研究发现，$A'(x)$ 是 $A(x)$代表的码组向左循环移位 i 次的结果[3]。

基于以上理论，对给定的信息位编码得到循环码的系统码：设 $m(x)$为信息码多项式，其次数小于 k。1) 用 x^{n-k} 乘 $m(x)$，得到的 $x^{n-k}m(x)$的次数必定小于 n。2) 用 $g(x)$除 $x^{n-k}m(x)$，得到余式 $r(x)$，其次数必定小于$(n-k)$。3) 将此余式 $r(x)$加于信息位之后作为监督码，即将 $r(x)$和 $x^{n-k}m(x)$相加，得到编出的多项式码组 $A(x)=x^{n-k}m(x)+r(x)$。可见，循环码系统码编码的核心就是用除法器求出余式 $r(x)$，然后将 $r(x)$所代表的监督码元附加在信息码元之后，即可完成编码。循环码的译码可以将接收码组用生成多项式 $g(x)$去除，以余项是否为零来判别接收码组中有无错码。

3. 循环码系统码的创新计算方法-线性变换法

3.1. 原理分析

线性分组码[4]有一个重要性质——封闭性，是指一种线性码中的任意两个码组之和仍为这种码中的一个码组。也就是说，若码组 B_1 和 B_2 是一种线性码中的两个许用码组，即

$$B_1\cdot H^{\mathrm{T}}=0,\quad B_2\cdot H^{\mathrm{T}}=0 \tag{8}$$

H 为监督矩阵。将以上俩式相加得

$$B_1\cdot H^{\mathrm{T}}+B_2\cdot H^{\mathrm{T}}=(B_1+B_2)H^{\mathrm{T}}=0 \tag{9}$$

所以，(B_1+B_2) 也是一个许用码组[2]。由于循环码是线性分组码的一个重要子类，其码组既具有线性分组码的封闭性，又具有循环码特有的循环移位性。

3.2. 通过线性变换得到循环码的系统码

在循环码的求解计算中，我们发现得到的生成矩阵 $G(x)$大多数不是典型生成矩阵，不符合 $G=[I_kQ]$ 的要求，这时候就需要将 $G(x)$化成典型阵，再用 $A=[a_{n-1}a_{n-2}\cdots a_ka_{k-1}]\cdot G$，才能得到循环码的系统码。

根据线性分组码的封闭性，我们研究发现一种循环码系统码的创新计算方法——线性变换法。该方法不用将 $G(x)$化成典型阵，也不用代入公式 $A=[a_{n-1}a_{n-2}\cdots a_ka_{k-1}]\cdot G$ 求系统码，而是直接分析生成矩阵 $G(x)$，将 $G(x)$分成两部分 $G=[I_k'Q']$，通过对 I_k' 各行的线性变换得到任意信息位，Q' 同步进行线性变换

得到监督位，将线性变换后的信息位 I_k' 和监督位 Q' 组合在一起，就得到循环码的系统码。

线性变换法的具体求解步骤为：首先，将 $G(x)$ 的 k 行分别标注为①②……ⓚ，将 $G(x)$前 k 列标注为 I_k'，后$(n-k)$列标注为 Q'；接着，对 I_k' 列，通过对①②……ⓚ进行线性变换，得到除了信息位全零以外的所有信息位取值；在 I_k' 进行线性变换时，Q' 同步进行线性变换，得到新的 Q' 即是信息位对应的监督位；将线性变换后的信息位 I_k' 和监督位 Q' 组合在一起，即是循环码的系统码。

具体计算方法举例说明：

题目：已知一个(7,4)循环码的生成多项式 $g(x)=x^3+x+1$，求循环码的全部码组？

传统的计算方法，将生成多项式 $g(x)=x^3+x+1$ 代入公式(1)得

$$G(x)=\begin{bmatrix} x^{k-1}\cdot g(x) \\ x^{k-2}\cdot g(x) \\ \vdots \\ x\cdot g(x) \\ g(x) \end{bmatrix}=\begin{bmatrix} x^3\cdot g(x) \\ x^2\cdot g(x) \\ x\cdot g(x) \\ g(x) \end{bmatrix}=\begin{bmatrix} x^6+x^4+x^3 \\ x^5+x^3+x^2 \\ x^4+x^2+x \\ x^3+x+1 \end{bmatrix}=\begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix} \tag{10}$$

此时，从公式(10)矩形框可以发现 $G\neq[I_kQ]$，它不是典型生成矩阵。接下来，就需要将 $G(x)$化成典型阵。

$$\begin{matrix} ① \\ ② \\ ③ \\ ④ \end{matrix}\rightarrow\begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix}\rightarrow\begin{bmatrix} 1000101 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix}\rightarrow\begin{bmatrix} 1000101 \\ 0100111 \\ 0010110 \\ 0001011 \end{bmatrix} \tag{11}$$

首先，将 $G(x)$的四行分别标注为①②③④；接着，① + ③ + ④进行线性变换，对应位置的码元模 2 运算，得到的计算结果放在第一行，如中间矩阵所示；再对中间矩阵的② + ④进行线性变换，对应位置的码元模 2 运算，得到典型生成矩阵 G，从公式(11)矩形框可以看出 $G=[I_kQ]$；最后，将典型生成矩阵代入公式(3)，得到循环码的系统码。由于(7,4)循环码的信息位 $k=4$，则共有循环码的系统码 $2^4=16$ 组，如下所示：

0000000、0001011、0010110、0011101、0100111、0101100、0110001、0111010

1000101、1001110、1010011、1011000、1100010、1101001、1110100、1111111

线性变换法的求解方法：首先，将 $G(x)$的四行分别标注为①②③④，将前四列标注为 I_4'，后三列标注为 Q'；接着，对 I_4' 列，通过对①②③④进行线性变换，得到除了信息位 0000 以外的 0001~1111 的所有信息位取值；在 I_4' 进行线性变换时，Q' 同步进行线性变换，得到新的 Q' 即是信息位对应的监督位；将线性变换后的信息位 I_4' 和监督位 Q' 组合在一起，就得到循环码(7,4)的系统码。

$$\begin{matrix} ① \\ ② \\ ③ \\ ④ \end{matrix}\rightarrow\begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ \underbrace{0001}_{I'}\underbrace{011}_{Q'} \end{bmatrix} \tag{12}$$

具体变换规律：

信息位 0000，对应监督位 000，不用变换得到系统码 0000000；

信息位 0001，对应 I_4' 的第④行，对应监督位为 011，则系统码 0001011；

信息位 0010，对应 I_4' 的第③行，对应监督位为 110，则系统码 0010110；

信息位 0011，对应 I_4' 的③ + ④的线性变换，对应监督位为 101，则系统码 0011101；

信息位 0100，对应 I_4' 的② + ④的线性变换，对应监督位为 111，则系统码 0100111；……依次类推，得到循环码信息位、线性变换、监督位和系统码如表 1 所示：

Table 1. The linear transformation method yields systematic codes for (7,4) cyclic codes
表 1. 线性变换法得到(7,4)循环码的系统码

信息位	线性变换	监督位	$a_6a_5a_4a_3a_2a_1a_0$
0000	无变换	000	0000000
0001	④	011	0001011
0010	③	110	0010110
0011	③ + ④	101	0011101
0100	② + ④	111	0100111
0101	②	100	0101100
0110	② + ③ + ④	001	0110001
0111	② + ③	010	0111010
1000	① + ③ + ④	101	1000101
1001	① + ③	110	1001110
1010	① + ④	011	1010011
1011	①	000	1011000
1100	① + ② + ③	010	1100010
1101	① + ② + ③ + ④	001	1101001
1110	① + ②	100	1110100
1111	① + ② + ④	111	1111111

基于以上线性变换法得到循环码系统码，其设计流程图如图 1 所示，仿真开始，初始化定义参数，生成随机信息位；接着定义生成矩阵，检查生成矩阵有效性，需要满足 k 行、n 列；根据信息位长度将生成矩阵分为两部分匹配，对生成矩阵进行线性变换编码，绘制波形图，完成编码过程。要验证编码的正确性，可以进行译码，检验译码输出的序列是否和输入的信息位一致[5] [6]。本文采用题目中循环码(7,4)进行 MATLAB 编译码仿真，得到相应波形如图 2 所示。

图 2 是(7,4)循环码的编译码图形，图 2(a)是循环码的一个原始信息位，横坐标是时间，纵坐标是幅值。从图中可以看出，原始信息位为(1100)。图 2(b)是经过线性变换编码后生成的系统码，对应 t 从 1 到 7 的系统码为(1100010)，其中，前四位是信息码，后三位是监督码，这和表 1 中信息位(1100)对应的系统(1100010)保持一致。图 2(c)是译码输出的序列，为(1100)，这和原始信息位相同。图 2(d)是译码输出的频谱图。循环码的译码输出验证了线性变换编码的正确性。

3.3. 几种方法的性能比较

为了进行性能比较，定义了一些评估标准，并设计实验来收集数据[7]。以下是对三种方法进行性能比较：1) 定义评估标准，分别为计算量：执行编码所需的操作数，计算速度：完成编码所需的时间，

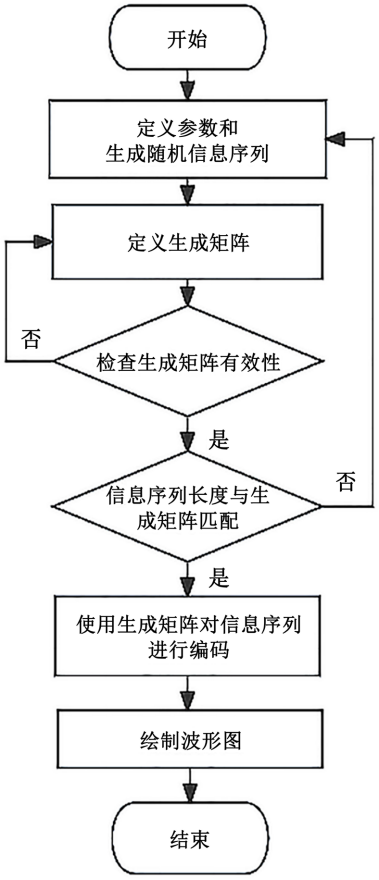

Figure 1. The design flow chart
图 1. 设计流程图

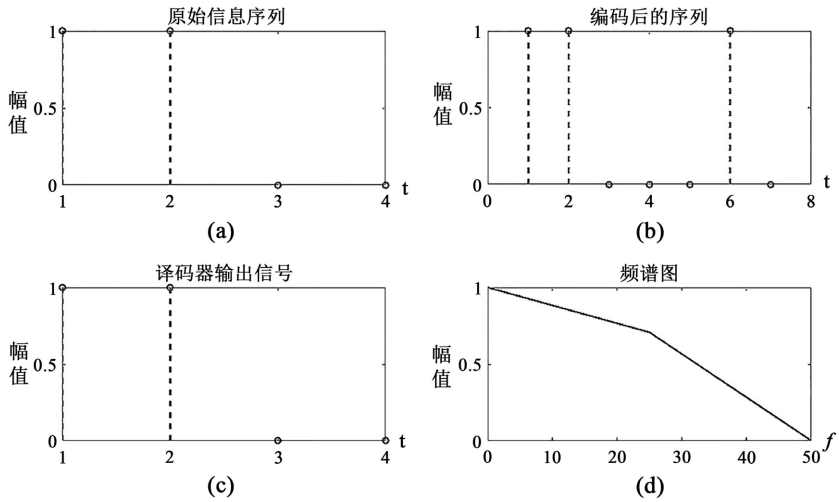

Figure 2. The encoding and decoding diagram of (7, 4) cyclic codes
图 2. 循环码(7, 4)的编码译码图形

计算准确度：编码结果的正确性。2) 设计实验，对比三种方法在不同长度的数据上的性能，在相同的硬件和软件环境下运行三种方法，记录每种方法的运行时间和资源消耗。3) 收集数据，执行实验并收集以

下数据，计算量：记录每种方法执行的异或操作数，计算速度：使用 MATLAB 的 tic 和 toc 命令测量运行时间，计算准确度：检查编码结果是否与预期相符。数据结果如表 2 所示。

Table 2. Performance comparison of three encoding methods
表 2. 三种编码方法的性能对比

方法	数据长度	计算量(异或操作数)	计算速度(秒)	计算准确度(是否正确)
方法 1	100	500	0.05	是
方法 1	1000	5000	0.5	是
方法 1	10,000	50,000	5	是
方法 2	100	300	0.03	是
方法 2	1000	3000	0.3	是
方法 2	10,000	30,000	3	是
方法 3	100	200	0.01	是
方法 3	1000	2000	0.1	是
方法 3	10,000	20,000	1	是

注：方法 1 是模 N 运算法，方法 2 是公式推导法，方法 3 是线性变换法。

表 2 中，数据长度是输入到编码算法中的数据位数或数据样本的数量，数据长度指定的(100, 1000, 10,000)，用于测试不同方法在不同数据规模下的性能。计算速度通常使用实际测量的时间来完成编码过程。在 MATLAB 中，可以使用 tic 和 toc 命令来测量代码执行所需的时间。{计算速度} = {toc} − {tic}，其中 tic 在代码执行前调用，开始计时。toc 在代码执行后调用，结束计时并返回经过的时间。表格中的计算速度值(例如，0.05 秒、0.5 秒、5 秒)是使用上述 tic 和 toc 命令测量得到的。这些值表示完成编码过程所需的实际时间。

在表 2 中，性能比较计算量，发现方法 3 在所有数据长度下的计算量都是最小的，这表明它在执行编码时所需的操作数最少，在处理大量数据时，方法 3 更加高效。性能比较计算速度，方法 3 在所有数据长度下的计算速度都是最快的。使用“tic”和“toc”命令测量的时间显示，方法 3 需要的时间最短来完成编码过程。这是由于它的算法优化及更少的操作数。性能比较计算准确度，所有方法的计算准确度都是 100%正确，这意味着所有方法都能准确地完成编码任务。此外，我们也研究了 3 种方法的扩展性和可伸缩性，随着数据长度的增加，方法 3 的计算量和计算速度的增加幅度是最小的。这表明方法 3 具有良好的扩展性和可伸缩性，适合处理大规模数据集成，例如在嵌入式系统、实时通信等大规模数据处理应用。

4. 结论

本文系统地研究了循环码的系统码计算方法，提出一种新型的循环码系统码计算方法——线性变换法，与传统的公式法和多项式模 N 运算法相比，线性变换法具有卓越的性能和应用优势，其在计算效率、准确性和实用性等方面为循环码的理论研究提供了新的研究方法，也为现代通信系统中，尤其是在数据传输速度要求高、数据量大的场景下的实际应用提供了强有力的理论支持，具有广泛的应用潜力。

基金项目

2022 年校级课程思政专项教学改革研究项目“‘通信原理’课程思政教学模式的探索”；2023 年广

东省高等教育教学研究和改革项目资助课题“基于 OBE 教育理念‘通信原理’思政教学模式探索与实践”KA24YY027；2024 年，校级课程思政示范项目，《通信原理》(1.4 信息及其度量)；2024 年，校级高等教育教学改革项目“数字化资源赋能《通信原理》智慧课堂的构建与实践”JG2024071。

参考文献

[1] 刘佳, 许海霞, 陈宁夏, 肖明明. 通信原理实验教程[M]. 广州: 中山大学出版社, 2016.

[2] 王磊, 胡以华, 王勇, 陈晓虎. 基于码重分布的系统循环码识别方法[J]. 计算机工程与应用, 2012, 48(7): 150-153.

[3] 樊昌信.曹丽娜. 通信原理[M]. 第 7 版. 北京: 国防工业出版社, 2021.

[4] 赵亮. 线性分组码和二进制伪随机序列的盲识别研究[D]: [硕士学位论文]. 重庆: 重庆邮电大学, 2018.

[5] 廉小亲, 刘庚, 米嘉晨, 等. 循环码编译码系统综合实验教学案例探讨[J]. 电脑与信息技术, 2022, 30(3): 70-75.

[6] 刘新红. 循环码编解码电路分析与实现[J]. 电子制作, 2021(3): 78-80.

[7] 刘洋, 李正权. 衰落信道中(15,7)循环码性能分析[J]. 无锡商业职业技术学院学报, 2018, 18(6): 95-98.