标题

小组报告

李浩斌

信息与计算科学

2024 年 6 月 7 日

目录

问题 (2)

给出一种码字较多的码中不能一一比较距离的译码方法 (错误时). 即不妨记码为 C, 且 $\forall x \in C, \#\{C\} = M$(较大), 若 $\exists y \notin C$, 则 y 可译为 C 中的哪一元素.

- 根据文献[4] 中 115 页首段描述: 对于码字个数较多的线性码使用**伴随式译码方案**较之于标准阵译码方案速度更快, 且由 124 页可知其仅需存储陪集代表元和相应的陪集.
- 以下我们首先给出相关定义:

线性码的定义

定义 (线性码[4])

如果 $C \subseteq V(n,q)$ 是 $V(n,q)$ 的一个子空间, 则称 C 为一个 q 元**线性码**[4]. 如果 C 是 $V(n,q)$ 的一个 k 维子空间, 则称 C 为一个 q 元 $[n,k]$ 线性码. 进一步, 如果 C 的最小距离为 d, 则称 C 为一个 q 元 $[n,k,d]$ 线性码.

线性码具有以下性质:

- $\forall \mathbf{x}, \mathbf{y} \in C$, 都有 $\mathbf{x} + \mathbf{y} \in C$;
- $\forall \mathbf{x} \in C, a \in \mathbb{GF}(q)$, 都有 $a\mathbf{x} \in C$.

线性码的生成矩阵

由于 $[n,k]$ 是 $V(n,q)$ 线性子空间, 则存在一组基. 不妨设 $\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{k-1}$ 为 $[n,k]$ 的一组基, 构造一个矩阵

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix},$$

这个矩阵称为**生成矩阵**, 缘由如下: 任何一个码字 $\mathbf{c} \in [n,k]$, 总可以找到一组元素 $u_0, u_1, \cdots, u_{k-1} \in \mathbb{GF}(q)$, 使得

$$\mathbf{c} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \cdots + u_{k-1}\mathbf{g}_{k-1}, \quad \text{i.e.} \quad \mathbf{c} = uG.$$

且经过初等行列变换后必定可将 G 变换为形如 $(I_k|A)$ 的形式, 我们称之为其**标准型生成矩阵**.

线性码的校验矩阵

定义 (线性码的对偶码)

设 C 是一个 q 元的 $[n,k]$ 线性码, 定义

$$C^{\perp} \overset{def}{=} \{\mathbf{x} \in V(n,q) | \forall \mathbf{a} \in C, \mathbf{x} \cdot \mathbf{a} = 0\}.$$

称为 C 的**对偶码**.

需要指出的是, 上述“点积”形式是域 $\mathbb{GF}(q)$ 上的运算. 可以验证, 对偶码自身也是线性码, 且维数为 $n-k$. 设

$$H = \begin{bmatrix} \mathbf{h}_0 & , \cdots , & \mathbf{h}_{n-k-1} \end{bmatrix}^T,$$

是对偶码的生成矩阵, 则称其为原码的**校验矩阵**.

由于 $(I_k|A)\,(-A, I_{n-k})^T = 0$, 则 $H = (-A^T | I_{n-k})$ 为生成矩阵标准型为 $G = (I_k|A)$ 的校验矩阵.

线性码的伴随式译码方法

定义 (陪集、代表元及伴随)

设 C 是一个 q 元的 $[n, k]$ 线性码, 其校验矩阵为 H,$\mathbf{a} \in V(n, q)$. 定义

$$\mathbf{a} + C \overset{def}{=} \{\mathbf{a} + \mathbf{x} | \mathbf{x} \in C\},$$

称为 C 的一个**陪集**. 在 C 的一个陪集中, 重量最小的向量称为陪集的**代表元**. 对任意的 $\mathbf{y} \in V(n, q)$, 称 $\mathbf{y}H^T$ 为 $\mathbf{y}$ 的**伴随**, 记为 $S(\mathbf{y})$.

则有如下伴随式译码方法:

- 设 $\mathbf{y}$ 是在信号接收端接收到的向量. 计算 $\mathbf{y}$ 的伴随 $S(\mathbf{y})$;
- 在伴随式列表中找到 $S(\mathbf{y})$ 所对应的陪集代表元 $\mathbf{a}$;
- 将 $\mathbf{y}$ 译为码字 $\mathbf{y} - \mathbf{a}$.

□

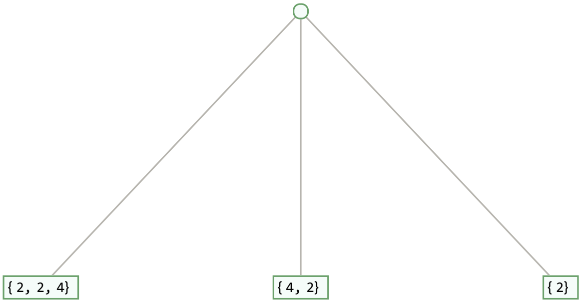
问题 (3)

对于码 $C=\{0000,1100,0011,1111\}$, 能否增加一位使得 $d'=d+1$.

由 Mathematica:

In[1]:=
```
A = {{0, 0, 0, 0}, {1, 1, 0, 0}, {0, 0, 1, 1}, {1, 1, 1, 1}};
Table[Table[HammingDistance[A⟦i⟧, A⟦j⟧], {j, i + 1, 4}], {i, 1, 3}] // Tree
```
表格 表格 汉明间距 树

Out[2]=



则 $d(C)=\min\limits_{x,y\in C} d(x,y)=2.$

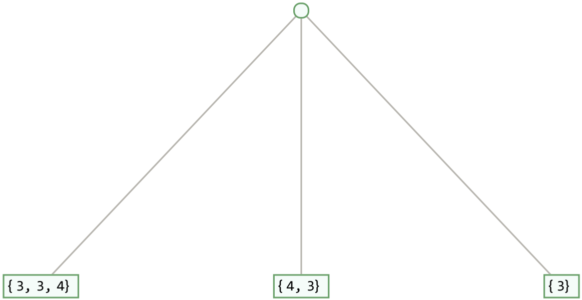
问题三

- 若令 $C' = \{00000, 11001, 00111, 11110\}$

由 Mathematica:

```
In[1]:= A = {{0, 0, 0, 0, 0}, {1, 1, 0, 0, 1}, {0, 0, 1, 1, 1}, {1, 1, 1, 1, 0}};
        Table[Table[HammingDistance[A⟦i⟧, A⟦j⟧], {j, i + 1, 4}], {i, 1, 3}] // Tree
        表格    表格    汉明间距                                              树
```

Out[2]=



则 $d(C') = \min\limits_{x,y \in C'} d(x, y) = 3.$ $\square$

参考文献

[1] 杨碧水, 梁浩森, 杜庆洋, 等. Viterbi 软判决译码的改进方法及应用[C]//2013 第一届中国指挥控制大会论文集. 2013: 2-7.

[2] GOLDSMITH A. Wireless communications[M]. Cambridge University Press, 2005.

[3] 陈. 请大牛们帮忙解释一下什么是 hard decision and soft decision(硬软判决)?[EB/OL]. 2021. https://www.zhihu.com/question/22019466/answer/1967818641.

[4] 陈鲁生, 沈世镒. 编码理论基础[M]. 高等教育出版社, 2005.

Thank you!