

# 信道编码大作业实验报告

夏志康 刘祥 芦迪 吴舒登

清华大学深圳国际研究生院信息科学与技术学部，深计研 19 班

日期：June 5, 2020

## 1 分工情况

## 2 构造射影平面 LDPC 码

基于射影平面构造的循环 LDPC 码其实就是利用射影平面的点线关联矩阵。考虑在有限域  $GF(2^s)$  上的  $m$  维射影平面  $PG(m, 2^s)$ 。这个平面包含有  $n$  个点，其中  $n = (2^{(m+1)s} - 1)/(2^s - 1)$ 。在  $PG(m, 2^s)$  中有  $J = ((2^{ms} + \dots + 2^s + 1)(2^{(m-1)s} + \dots + 2^s + 1))/(2^s + 1)$  条直线，每条直线上包含有  $2^s + 1$  个点，每个点上又有  $(2^{ms} - 1)/(2^s - 1)$  条线交叉。伽罗华域  $GF(2^{(m+1)s})$  是有限域  $GF(2^s)$  的扩展，且可以看做是射影平面  $PG(m, 2^s)$  的一个实现。令  $\alpha$  为  $GF(2^{(m+1)s})$  的本原元，则  $GF(2^{(m+1)s})$  中的非零元素  $\alpha^0, \alpha^1, \dots, \alpha^{n-1}$  组成了射影平面  $PG(m, 2^s)$  中的点。设  $\alpha^i, \alpha^j$  是射影平面  $PG(m, 2^s)$  中的两个线性独立的点，那么下面点的集合  $\{\alpha^i + \beta\alpha^j : \beta \in GF(2^s)\}$  就是  $PG(m, 2^s)$  里通过点  $\alpha^i$  的一条线。两条线没有交点就是平行的，如果有交点也只能有一个交点。

令  $PG(m, 2^s)$  中直线的关联矢量作为矩阵  $\mathbf{H}_{PG}^{(1)}(m, 0, s)$  的行，射影平面  $PG(m, 2^s)$  中的点对应于  $\mathbf{H}_{PG}^{(1)}(m, 0, s)$  的列。 $\mathbf{H}_{PG}^{(1)}(m, 0, s)$  行重为  $\rho = 2^s + 1$ ，列重为  $\gamma = (2^{ms} - 1)/(2^s - 1)$ ，密度为  $r = (2^{2s} - 1)/(2^{(m+1)s} - 1)$ 。对  $m \geq 2, s \geq 2$ ， $r$  非常小，因此  $\mathbf{H}_{PG}^{(1)}(m, 0, s)$  是一个低密度矩阵。它的零空间给出了一个长度为  $n$  的 LDPC 码  $\mathbf{C}_{PG}^{(1)}(m, 0, s)$ ，其最小距离至少为  $(2^{ms} - 1)/(2^s - 1) + 1$ 。校验位长度为  $n - k = 1 + (C_{m+1}^m)^s$ 。

实验要求构造  $q = 32, n = q^2 + q + 1 = 1057$  的 PG-LDPC 码。构造过程如下：

- 1) 由  $q = 2^s, n = (2^{(m+1)s} - 1)/(2^s - 1)$  得  $m = 2, s = 5$ ，即要考虑有限域  $GF(2^5)$  上的 2 维射影平面  $PG(2, 2^5)$ 。 $PG(2, 2^5)$  中的点是用  $GF(2^{(m+1)s}) = GF(2^{15})$  中的元素表示的，可以先构造伽罗华域  $GF(2^{15})$ 。 $GF(2^{15})$  是由本原多项式  $p(x) = x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^5 + x^4 + x^3 + x^2 + x + 1$  生成的。由此，我们可以得到  $GF(2^{15})$ 。
- 2) 令  $\alpha$  为  $GF(2^{15})$  的一个本原元。令  $\beta = \alpha^n$ ，则  $\beta$  的阶为  $2^s - 1$ ， $\{0, 1, \beta, \beta^2, \dots, \beta^{2^s-2}\}$  可以构成  $GF(2^s)$ 。令  $\Gamma = \{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{n-1}\}$ ，则  $\{\alpha^i, \beta\alpha^i, \beta^2\alpha^i, \dots, \beta^{2^s-2}\alpha^i\}$  可将  $GF(2^{15})$  划分为  $n$  个不相交的子集。
- 3) 需要求出经过某一点的任意一条不过原点的直线上的所有其他点。取  $PG(2, 2^5)$  中的任意不同的两个点  $\alpha^i, \alpha^j$ ，则通过这两个点的直线由  $\{\eta_1\alpha^i + \eta_2\alpha^j\}$  这样形式的点组成，且有  $2^s + 1$  即 33 个不同的点，只需选择  $\eta_1$  与  $\eta_2$ ，使得  $(\eta_1, \eta_2)$  不是另一个选择  $(\eta'_1, \eta'_2)$  的倍数即可。简单起见，我们取  $i = 0, j = 1$ ，那么  $\alpha^i = 1, \alpha^j = \alpha$ 。最终得到含有 33 个点的一条直线。

- 4) 得到直线后, 由该直线求其关联矢量。该矢量由  $n = 1057$  个点组成。如果某点在直线上, 则关联矢量该点处值为 1, 否则为 0. 由所得的关联矢量作为校验矩阵的第一行, 对该矢量向右循环移位 1056 次, 每次得到的矢量均作为校验矩阵的一行。校验位数目为  $1 + (C_3^2)^5 = 244$ , 因此信息位的数目位 813。校验矩阵的大小为  $244 \times 1057$ , 这样就得到了长为 1057, 信息位为 813 的二维射影平面 LDPC 码的校验矩阵。

### 3 总结