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 $J = ((2^{ms} + \cdots + 2^s + 1)(2^{(m-1)s} + \cdots + 2^s + 1))/(2^s + 1)$ 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 α 为 $GF(2^{(m+1)s})$ 的本原元，则 $GF(2^{(m+1)s})$ 中的非零元素 $\alpha^0, \alpha^1, \cdots, \alpha^{n-1}$ 组成了射影平面 $PG(m, 2^s)$ 中的点。设 α^i, α^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 α^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 $\boldsymbol{H}_{PG}^{(1)}(m, 0, s)$ 的行，射影平面 $PG(m, 2^s)$ 中的点对应于 $\boldsymbol{H}_{PG}^{(1)}(m, 0, s)$ 的列。$\boldsymbol{H}_{PG}^{(1)}(m, 0, s)$ 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 $\boldsymbol{H}_{PG}^{(1)}(m, 0, s)$ 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 $\boldsymbol{C}_{PG}^{(1)}(m, 0, s)$，其最小距离至少为 $(2^{ms} - 1)/(2^s - 1) + 1$。

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 $q = 2^s, n = (2^{(m+1)s} - 1)/(2^s - 10$ 得 $m = 2, s = 5$，即要考虑有限域 $GF(2^5)$ 上的 2 维射影平面 $PG(2, 2^5)$。$PG(2, 2^5)$ 中的点是有 $GF(2^{(m+1)s}) = GF(2^{15})$ 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 $p(x) = x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^5+x^4+x^3+x^2+x^1+1$ 生成的。由此，我们可以得到 $GF(2^{15})$。
2) 令 α 为 $GF(2^{15})$ 的一个本原元。令 $\beta = \alpha^n$，则 β 的阶为 $2^s - 1$，$\{0, 1, \beta, \beta^2, \cdots, \beta^{2^s-2}\}$ 可以构成 $GF(2^5)$。令 $\Gamma = \{\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{n-1}\}$，则 $\{\alpha^i, \beta\alpha^i, \beta^2\alpha^i, \cdots, \beta^{2^s-2}\alpha^i\}$ 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 α^i, α^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 η_1 与 η_2，使得 (η_1, η_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，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 基于循环置换矩阵的 Array LDPC

基于循环置换矩阵的 Array LDPC 码是一种结构化的 LDPC 码构造方法，其构造过程主要由三个参数控制 p, j, k，其中 p 为质数。在这种构造方法下，校验矩阵为

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{I} & \boldsymbol{I} & \cdots & \boldsymbol{I} \\ \boldsymbol{I} & \boldsymbol{\alpha} & \boldsymbol{\alpha}^2 & \cdots & \boldsymbol{\alpha}^{k-1} \\ \boldsymbol{I} & \boldsymbol{\alpha}^2 & \boldsymbol{\alpha}^4 & \cdots & \boldsymbol{\alpha}^{2(k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{I} & \boldsymbol{\alpha}^{j-1} & \boldsymbol{\alpha}^{2(j-1)} & \cdots & \boldsymbol{\alpha}^{(j-1)(k-1)} \end{bmatrix}$$

其中 $\boldsymbol{I}$ 是 $p \times p$ 的单位矩阵，$\boldsymbol{\alpha}$ 是大小为 $p \times p$ 的左移或右移一位的置换矩阵。例如，当 $p = 5$ 时

$$\boldsymbol{\alpha} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ 或 } \boldsymbol{\alpha} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{1}$$

对于题目的要求可取 $p = k = 31, j = 5$

4 总结

本次实验，安装部署了强化学习实验框架，阅读了一系列深度强化学习的论文，运行了一系列相关实验，可谓受益匪浅。强化学习确实是十分有趣的研究课题，但由于时间比较紧，很多算法细节仍然不甚了了，希望在以后的学习科研中能够继续深入了解。