基于素域构造的准循环低密度校验码

林国庆[①②] 陈汝伟[③] 王新梅[②] 肖国镇[②]
[①](长安大学汽车学院 西安 710064)
[②](西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)
[③](桂林电子科技大学数学与计算科学学院 桂林 541004)

摘 要：该文提出一种基于素域构造准循环低密度校验码的方法。该方法是 Lan 等所提出基于有限域构造准循环低密度校验码的方法在素域上的推广，给出了一类更广泛的基于素域构造的准循环低密度校验码。通过仿真结果证实：所构造的这一类准循环低密度校验码在高斯白噪声信道上采用迭代译码时具有优良的纠错性能。

关键词：低密度校验码；准循环码；素域；本原元
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2010)03-0609-04
DOI:10.3724/SP.J.1146.2009.00208

Construction of Quasi-Cyclic LDPC Codes From Prime Fields

Lin Guo-qing[①②] Chen Ru-wei[③] Wang Xin-mei[②] Xiao Guo-zhen[②]
[①](*School of Automobile*, *Chang'an University*, *Xi'an* 710064, *China*)
[②](*State Key Lab of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)
[③](*School of Mathematics and Computational Science*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: This paper presents a method to construct quasi-cyclic LDPC codes from prime fields. This method is a generalization of a method proposed by Lan et al to construct quasi-cyclic LDPC codes based on finite fields, and gives a much larger class of quasi-cyclic LDPC codes based on prime fields. Simulations show that quasi-cyclic LDPC codes constructed by the proposed method perform well over AWGN channels with iterative decoding.

Key words: Low-Density Parity-Check (LDPC) code; Quasi-cyclic code; Prime field; Primitive element

1 引言

Gallager 于 1962 年首次提出了低密度校验(LDPC)码[1]，但是这一卓越的创造在当时并没有得到应有的重视。直到 1996 年，Mackay 和 Neal 证实了低密度校验码可以获得接近香农限的误码性能[2]，低密度校验码被编码学界忽视的状况才得以改变。自此以后，低密度校验码成为编码学界研究的热点。目前，低密度校验码已在深空通信、卫星通信、光纤通信、磁\光存储、ADSL、无线局域网等领域得到应用，并被视为未来最有发展潜力的一类编码。

低密度校验码的构造方法大致可以分为随机构造和代数构造两个大类。随机构造可以构造出误码性能很好的低密度校验矩阵，但随机构造的校验矩阵缺少有规律的结构，使编码过程变得复杂，且需要较大的存储空间来存储校验矩阵，这些缺陷妨碍了随机构造的应用。代数构造的准循环低密度校验码可以克服随机构造的缺陷，并可以简化编码及译码过程，应用时对硬件的要求也较低[3–5]。在文献[6]中，Lan 等利用有限域构造出了几类性能优良的准循环低密度校验码。本文将提出一种基于素域构造准循环低密度校验码的方法。这一方法是 Lan 等所提出基于有限域构造准循环低密度校验码的方法—[6]在素域上的推广， 给出了一类更广泛的基于素域构造的准循环低密度校验码。通过仿真结果证实，采用本文方法构造的准循环低密度校验码在高斯白噪声信道上采用迭代译码时，具有良好的纠错性能，并且有较低的错误平层。

2 基于素域构造的准循环低密度校验码

构造从素域 GF(p) 上有以下形式的一个矩阵开始，

$$\boldsymbol{W}=\begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{p-2} \end{bmatrix} = \begin{bmatrix} \alpha^0-\alpha^{g_0} & \alpha-\alpha^{g_0} & \cdots & \alpha^{p-2}-\alpha^{g_0} \\ \alpha-\alpha^{g_1} & \alpha^2-\alpha^{g_1} & \cdots & \alpha^{p-1}-\alpha^{g_1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{p-2}-\alpha^{g_{p-2}} & \alpha^{p-1}-\alpha^{g_{p-2}} & \cdots & \alpha^{2(p-2)}-\alpha^{g_{p-2}} \end{bmatrix} \tag{1}$$

2009-02-20收到，2009-08-18改回
国家自然科学基金(U0635003)，国家 863 计划项目(2007AA01Z215)和桂林电子科技大学科学研究基金(UF09006Y)资助课题
通信作者：林国庆 linguoqinghao@163.com

在式(1)中，α 为素域 GF(p) 的一个本原元；$g_0,g_1,\cdots,g_{p-2}$ 均为集合 $\{0,1,\cdots,p-2\}$ 中的元素，满足以下条件：若 $0\le i,j<p-1$ 且 $i\ne j$,则有 $i-g_i\not\equiv j-g_j(\mathrm{mod}(p-1))$。我们并不要求 $g_0,g_1,\cdots,g_{p-2}$ 互不相等。由于取定素域 GF(p) 之后，α 可以在 $(p-1)$ 个本原元中任意选取，而满足条件的 $g_0,g_1,\cdots,g_{p-2}$ 一共有 $(p-1)!$ 组，因此，我们总共可以构造出 $(p-1)\cdot(p-1)!$ 个具有式(1)形式的矩阵。在文献[6]中，Lan 等所构造的矩阵 $\boldsymbol{W}^{(1)}$ 是本文式(1)中 $\boldsymbol{W}$ 每个参数 $g_i(0\le i<p-1)$ 均取值为 0 的特例。

引理1 在由式(1)给出的矩阵 $\boldsymbol{W}$ 中，每行每列有且只有一个零元素。

证明 矩阵 $\boldsymbol{W}$ 中第 i ($0\le i<p-1$)行(本文中,行列及分量位置的序数均从0开始)的第 s ($0\le s<p-1$)个元素为零的充要条件为 $i+s\equiv g_i(\mathrm{mod}(p-1))$。容易看出，给定 i 和 g_i 之后，s 有且只有一个解。因此，矩阵 $\boldsymbol{W}$ 中每行有且只有一个零元素。还需要证明 $\boldsymbol{W}$ 中每列有且只有一个零元素。若 $\boldsymbol{W}$ 中不是每列有且只有一个零元素，则存在一个列至少有2个零元素，设这一列为第 k ($0\le k<p-1$)列，并设第 k 列上第 i 个分量和第 j 个分量上的元素为零，则 $\alpha^{i+k}-\alpha^{g_i}=0$，$\alpha^{j+k}-\alpha^{g_j}=0$。由于 α 为素域 GF(p) 的本原元，故有 $i+k\equiv g_i(\mathrm{mod}(p-1))$，$j+k\equiv g_j(\mathrm{mod}(p-1))$。容易得到

$$i-g_i\equiv j-g_j(\mathrm{mod}(p-1)) \tag{2}$$

式(2)与选取 $g_0,g_1,\cdots,g_{p-2}$ 所满足的条件矛盾。由此可知，$\boldsymbol{W}$ 中每列有且只有一个零元素。

引理2 由式(1)给出的矩阵 $\boldsymbol{W}$ 具有以下性质：

(1)若 $0\le i<p-1$,$0\le k,l<p-1$ 且 $k\ne l$，则 $\alpha^k w_i$ 与 $\alpha^l w_i$ 最多只有一个对应相等的分量；

(2) 若 $0\le i,j<p-1$, $i\ne j$ 且 $0\le k,l<p-1$, $\alpha^k w_i$ 与 $\alpha^l w_j$ 最多只有一个对应相等的分量。

证明 由 $\boldsymbol{W}$ 中每行 $p-1$ 个元素互不相同，且 α 为素域 GF(p) 的本原元，容易知道性质(1)成立。下面我们用反证法证明性质(2)成立。否则存在 i,j,k,l ,满足 $0\le i,j<p-1$, $i\ne j$ 且 $0\le k,l<p-1$,使 $\alpha^k w_i$ 与 $\alpha^l w_j$ 至少有两个对应相等的分量。记 $\alpha^k w_i$ 与 $\alpha^l w_j$ 有相等的分量的两个位置分别为 s , t ($0\le s,t<p-1$)，则有

$$\alpha^k(\alpha^{i+s}-\alpha^{g_i})=\alpha^l(\alpha^{j+s}-\alpha^{g_j}) \tag{3}$$

$$\alpha^k(\alpha^{i+t}-\alpha^{g_i})=\alpha^l(\alpha^{j+t}-\alpha^{g_j}) \tag{4}$$

将式(3)的左边乘以式(4)的右边，式(3)的右边乘以式(4)的左边，消去 α^{k+l} 后得到

$$(\alpha^{i+s}-\alpha^{g_i})(\alpha^{j+t}-\alpha^{g_j})=(\alpha^{j+s}-\alpha^{g_j})(\alpha^{i+t}-\alpha^{g_i}) \tag{5}$$

由式(5)可以推得

$$\alpha^{i+g_j}(\alpha^s-\alpha^t)=\alpha^{j+g_i}(\alpha^s-\alpha^t) \tag{6}$$

由于 $s\not\equiv t(\mathrm{mod}(p-1))$，$\alpha^s-\alpha^t\ne 0$，我们可以在式(6)两边消去 $\alpha^s-\alpha^t$，得到 $\alpha^{i+g_j}=\alpha^{j+g_i}$。由于 α 为素域 GF(p) 的本原元 ， $i+g_j\equiv j+g_i(\mathrm{mod}(p-1))$，即

$$i-g_i\equiv j-g_j(\mathrm{mod}(p-1)) \tag{7}$$

式(7)与选取 $g_0,g_1,\cdots,g_{p-2}$ 所满足的条件矛盾。由此，性质(2)得到证明。

利用式(1)给出的矩阵 $\boldsymbol{W}$，构造 $(p-1)^2\times(p-1)$ 矩阵 $\boldsymbol{M}$：

$$\boldsymbol{M}=\begin{bmatrix}\boldsymbol{M}_0\\ \boldsymbol{M}_1\\ \vdots\\ \boldsymbol{M}_{p-2}\end{bmatrix} \tag{8}$$

其中，大小为 $(p-1)\times(p-1)$ 的子矩阵 $\boldsymbol{M}_i$ ($0\le i<p-1$)由下式给出：

$$\boldsymbol{M}_i=\begin{bmatrix}\alpha^0 w_i\\ \alpha^1 w_i\\ \vdots\\ \alpha^{p-2} w_i\end{bmatrix} \tag{9}$$

子矩阵 $\boldsymbol{M}_i$ ($0\le i<p-1$)的第 0 行是式(1)给出的矩阵 $\boldsymbol{W}$ 的第 i 行。

为了叙述的方便，这里我们引入以下定义：

定义1 令 α 为素域 GF(p) 的一个本原元，$\beta=\alpha^k$ 是素域 GF(p) 的一个非零元素，则

$$\boldsymbol{B}_k=\begin{bmatrix}\alpha^0\beta\\ \alpha^1\beta\\ \alpha^2\beta\\ \alpha^3\beta\\ \vdots\\ \alpha^{p-2}\beta\end{bmatrix} \tag{10}$$

称为素域 GF(p) 乘法循环群的一个循环列。

定理 1 式(1)给出的矩阵 $\boldsymbol{M}$ 具有以下性质：

(1) $\boldsymbol{M}$ 中每行有且只有1个零元素；

(2) $\boldsymbol{M}$ 中任意两行最多只有1个对应相等的分量；

(3)每个 $\boldsymbol{M}_i$ ($0\le i<p-1$)中有且只有1个全零列，其它列均为 GF(p) 中乘法循环群的循环列；

(4)各个 $\boldsymbol{M}_i$ ($0\le i<p-1$)的全零列分布在矩阵 $\boldsymbol{M}$ 不同的列中，即矩阵 $\boldsymbol{M}$ 的每一列均包含且仅包含某一个 $\boldsymbol{M}_i$ 的全零列 。

证明 (1)是引理1的直接结果。(2)是引理2的直

接结果。由于引理1及α为素域GF(p)的本原元，容易知道(3)和(4)成立。

将$(p-1)^2\times(p-1)$矩阵$\boldsymbol{M}$表示为

$$\boldsymbol{M}=\begin{bmatrix} m_{0,0} & m_{0,1} & \cdots & m_{0,p-2} \\ m_{1,0} & m_{1,1} & \cdots & m_{1,p-2} \\ \vdots & \vdots & \ddots & \vdots \\ m_{(p-1)^2-1,0} & m_{(p-1)^2-1,1} & \cdots & m_{(p-1)^2-1,p-2} \end{bmatrix} \tag{11}$$

根据式(11)表示的矩阵$\boldsymbol{M}$，构造GF(2)上$(p-1)^2\times(p-1)^2$矩阵$\boldsymbol{H}$：

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{H}_{0,0} & \boldsymbol{H}_{0,1} & \cdots & \boldsymbol{H}_{0,p-2} \\ \boldsymbol{H}_{1,0} & \boldsymbol{H}_{1,1} & \cdots & \boldsymbol{H}_{1,p-2} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{H}_{(p-1)^2-1,0} & \boldsymbol{H}_{(p-1)^2-1,1} & \cdots & \boldsymbol{H}_{(p-1)^2-1,p-2} \end{bmatrix} \tag{12}$$

其中$\boldsymbol{H}_{i,j}$($0\le i\le(p-1)^2-1$，$0\le j\le p-2$)是满足以下条件的$1\times(p-1)$子矩阵：

(1)若$m_{i,j}=0$，则$\boldsymbol{H}_{i,j}$是全零向量;

(2)若$a_{i,j}=\alpha^k$($0\le k\le p-2$)，则$\boldsymbol{H}_{i,j}$第k个分量是1，其它分量均为0。

由定理1的性质(2)，容易知道矩阵$\boldsymbol{H}$满足RC-约束条件，即$\boldsymbol{H}$中任意两行在对应相同位置上的“1”最多只有1个。

将式(12)给出的$(p-1)^2\times(p-1)^2$矩阵$\boldsymbol{H}$划分为$(p-1)\times(p-1)$个大小为$(p-1)\times(p-1)$的子矩阵：

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{P}_{0,0} & \boldsymbol{P}_{0,1} & \cdots & \boldsymbol{P}_{0,p-2} \\ \boldsymbol{P}_{1,0} & \boldsymbol{P}_{1,1} & \cdots & \boldsymbol{P}_{1,p-2} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{P}_{p-2,0} & \boldsymbol{P}_{p-2,1} & \cdots & \boldsymbol{P}_{p-2,p-2} \end{bmatrix} \tag{13}$$

定理 2　在式(13)给出的阵列中，每行每列均有且仅有1个大小为$(p-1)\times(p-1)$的全零子矩阵，其余的子矩阵均为$(p-1)\times(p-1)$循环置换矩阵。

证明　$\boldsymbol{P}_{i,j}$($0\le i,j\le p-2$)由$\boldsymbol{M}_i$的第j列得来。若$\boldsymbol{M}_i$的第j列是全零列，则$\boldsymbol{P}_{i,j}$是大小为$(p-1)\times(p-1)$的全零子矩阵。若$\boldsymbol{M}_i$的第j列是GF(p)中乘法循环群的循环列，则$\boldsymbol{P}_{i,j}$是与$\boldsymbol{M}_i$第j列关联的$(p-1)\times(p-1)$循环置换矩阵。定理2是定理1的直接结果。

3　结构性质

利用上面所构造的$(p-1)\times(p-1)$个大小为$(p-1)\times(p-1)$的循环置换矩阵阵列及其转置，可以得到许多个准循环低密度校验码的校验矩阵。下面只讨论由$\boldsymbol{H}$得到的准循环低密度校验码的校验矩阵。

取$\boldsymbol{H}(k,l)$($1\le k,l\le p-1$)为式(13)的一个$k\times l$子阵列，则$\boldsymbol{H}(k,l)$是GF(2)上的$k(p-1)\times l(p-1)$矩阵。$\boldsymbol{H}(k,l)$是$\boldsymbol{H}$的子矩阵，亦满足RC-约束条件。若$\boldsymbol{H}(k,l)$中不包含式(13)中的零子方阵，则$\boldsymbol{H}(k,l)$具有固定的行重l和固定的列重k。以$\boldsymbol{H}(k,l)$为校验矩阵，得到一个码长为$l(p-1)$的正则准循环LDPC码，记为C_1。$\boldsymbol{H}(k,l)$的秩至多为$k(p-1)-k+1$，C_1的码率至少为$((l-k)(p-1)+k-1)/l(p-1)$。由于$\boldsymbol{H}(k,l)$满足RC-约束条件，其Tanner图最小圈长至少为6；$\boldsymbol{H}(k,l)$中$t(t<k+1)$列的和不可能是零向量，故C_1的最小距离至少为$k+1$。$\boldsymbol{H}(k,l)$是置换矩阵的阵列，其奇数列之和必不为0，因此C_1的最小距离必是偶数。当k是偶数时，C_1的最小距离至少为$k+2$。如果$\boldsymbol{H}(k,l)$中含有式(13)中的零子方阵，则其列重可能有k和$k-1$两个值；行重也可能有l和$l-1$两个值。这时以$\boldsymbol{H}(k,l)$为校验矩阵可能得到一个近正则准循环LDPC码，这个近正则准循环LDPC码的最小距离至少为$\boldsymbol{H}(k,l)$的最小列重加1。

4　仿真结果

用本文提出的方法构造了2个码，与用文献[6]中方法构造的2个码作了仿真结果比较。结果如图1所示。仿真在加性高斯白噪声(AWGN)信道上进行，采用BPSK调制及SPA译码。这些码采用SPA译码时都收敛得很快，100次迭代和5次迭代的性能差距小于0.1 dB，因此，在仿真中我们只用了5次迭代。选用的第1个码是在素域GF(131)上用本文方法构造的一个(6500,5983)准循环低密度校验码。取GF(131)的本原元2，按本文方法构造由130×130个大小为130×130的循环置换矩阵组成式(13)形式的阵列(参数$g_0,g_1,\cdots,g_{p-2}$随机选取)，选取阵列中的第0行到第3行及第0列到第49列的循环置换矩阵，得到一个(6500,5983)准循环低密度校验码。我们将这个码标记为GP(6500,5983)。GP(6500,5983)的码率是0.92046。在误码率10^{-6}时，GP(6500,5983)与香农限仅有约1.05 dB的差距。在5次迭代的条件下，这是一个很好的结果。将GP(6500,5983)的仿真结果与采用文献[6]中方法一构造、标记为LP(6500,5983)的准循环低密度校验码作了比较，发现两个码具有完全相同的纠错性能。仿真中选用的第二个码是在素域GF(157)上用本文方法构造的一个(9360,8736)准循环低密度校验码。取GF(157)的本原元5，按本文方法构造由156×156个大小为156×156的循环置换矩阵组成式(13)形式的阵列，选取阵列中的第0行到第3行及第0列到第59列的循环置换矩阵，得到一个(9360,8736)准循环低密度校验码。将

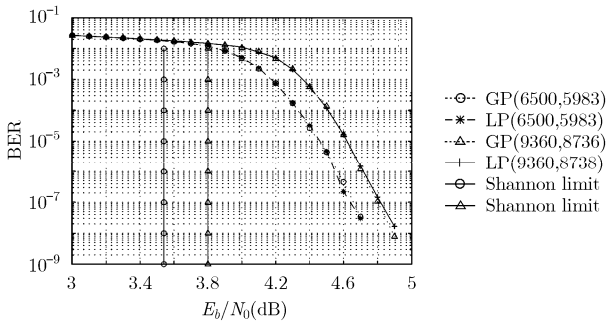

图 1 GP(6500,5983)与 LP(6500,5983)及
GP(9360,8736)与 LP(9360,8738)的误码性能比较

这个码标记为 GP(9360, 8736) 。 GP(9360, 8736) 的码率是 0.93333。在误码率10^{-6}时， GP(9360, 8736) 与香农限仅有约 0.9 dB 的差距。在 5 次迭代的条件下，这同样是一个很好的结果。将 GP(9360, 8736) 的仿真结果与用文献[6]中方法一构造的 LP(9360, 8738) 作了比较，这两个码也具有几乎完全相同的性能。我们没有估计所构造的低密度校验码的错误平层。但是在仿真中可以看到采用本文方法构造的低密度校验码的错误平层在10^{-8}之下。

5 结论

代数构造的准循环低密度校验码具有编码及译码较为简单、易于实现等优点。本文给出了一种基于素域构造准循环低密度校验码的方法。这一方法是 Lan 等所提出基于有限域构造准循环低密度校验码的方法在素域上的推广，给出了一类更广泛的基于素域构造的准循环低密度校验码。通过仿真结果证实：所构造的这一类准循环低密度校验码在高斯白噪声信道上采用迭代译码时具有优良的纠错性能，并具有较低的错误平层。

参 考 文 献

[1] Gallager R G. Low density parity check codes[J]. *IEEE Information Theory*, 1962, IT-8(1): 21–28.

[2] MacKay D J C and Neal R M. Near Shannon limit performance of low density parity check codes[J]. *IEE Electron. Letters.*, 1996, 32(18): 1645–1646.

[3] Dai Y, Yan Z, and Chen N. Optimal overlapped message passing decoding of quasi-cyclic LDPC codes[J]. *IEEE Very Large Scale Integration Systems*, 2007, 16(5): 565–578.

[4] LiZ, Chen L, Zeng L, Lin S, and Fong W. Efficient encoding of quasi-cyclic low-density parity-check codes[J]. *IEEE Communication*, 2006, 54(1): 71–81.

[5] Wang Z and Cui Z. A memory efficient partially parallel decoder architecture for QC-LDPC codes[J]. *IEEE Very Large Scale Integration Systems*, 2007, 15(4): 483–488.

[6] Lan L, Zeng L Q Y, Tai Y, Chen L, Lin S, and Abdel-Ghaffar K. Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach[J]. *IEEE Information Theory*, 2007, 53(7): 2429–2458.

林国庆： 男，1978 年生，助理工程师，研究方向为信道编码、网络编码.

陈汝伟： 男，1974 年生，讲师，研究方向为信道编码.

王新梅： 男，1937 年生，教授，研究方向为信道编码、密码学.

肖国镇： 男，1934 年生，教授，研究方向为信道编码、密码学.