文章编号:1001-506X(2010)06-1146-05

基于有限域构造的 QC LDPC 码编码器设计

窦高奇,高 俊,张文娟
(海军工程大学通信工程系,湖北 武汉 430033)

摘 要:为了降低准循环低密度奇偶校验(quasi-cyclic low-density parity-check, QC LDPC)码编码的复杂度,提出了一种利用近似满秩(approximate full rank, AFR)矩阵实现 QC LDPC 码的高效编码方案。基于有限域 GF(q)乘群、加群构造出 AFR 校验矩阵,利用 AFR 矩阵可以快速得到其系统循环形式的生成矩阵。此方案不但可以实现线性化编码,而且编出的码都为系统码。仿真表明,该编码方案对于列重较小的 QC LDPC 码具有较好的通用性和实用价值。

关键词:编码器;低密度奇偶校验码;准循环码;有限域;校验矩阵
中图分类号:TN 911.22 **文献标志码**:A **DOI**:10.3969/j.issn.1001-506X.2010.06.009

Exploit of designing encoder for QC LDPC codes based on finite field approach

DOU Gao-qi, GAO Jun, ZHANG Wen-juan
(*Dept. of Communication Engineering, Naval Univ. of Engineering, Wuhan 430033, China*)

Abstract: To reduce the complexity of encoder for QC LDPC codes, an efficient encoding scheme by using the approximate-full-rank (AFR) parity check matrix is proposed. The AFR matrix is constructed based on finite field approach and can be used to find the systematic generator matrix efficiently. The scheme can be used to encode systematic LDPC codes with linear encoding complexity. Simulations verify its generality and practicality for QC LDPC codes with small column weights.

Keywords: encoder; low-density parity-check (LDPC) codes; quasi-cyclic codes; finite field; check matrix

0 引 言

低密度奇偶校验(low density parity check, LDPC)码是一种线性分组纠错码[1],它的奇偶校验矩阵由稀疏矩阵构成,这使得 LDPC 码存在高效的译码算法,译码复杂度和码长呈线性关系,克服了分组码在码长较长时所面临的巨大译码复杂度问题。与基于 MAP 译码算法的 turbo 码相比,基于和积译码算法的 LDPC 码的译码复杂度大大降低,从而使得 LDPC 长码在实际应用中成为可能。然而,其编码复杂度却成为制约其实用化的瓶颈。

LDPC 码的编码复杂度与校验矩阵 $\boldsymbol{H}$ 的结构密切相关,近年来涌现出大量的关于构造 $\boldsymbol{H}$ 的方法,大体可以分为两大类:(1) 基于计算机搜寻的随机构造法[2-3]。该方法按照特定的设计准则和 Tanner 图结构,如围长、度分布和停止集等特性搜寻满足要求的校验矩阵 $\boldsymbol{H}$;(2) 基于代数和几何工具的结构化方法[4-6]。该方法利用有限几何和组合数学等,构造具有循环或准循环结构的 LDPC 码。一般而言,随机构造的 LDPC 长码比等长的结构化 LDPC 码性能更好,然而也正因为其校验矩阵的随机性,使得人们难以找到简单的编码方法。相反,结构化 LDPC 码由于在码的构造、编译码复杂度以及存储空间等方面较随机 LDPC 码有明显优势。因此,就像构造 BCH 码和 RS 码那样,寻找系统的构造 LDPC 好码的方法成为当前研究的热点[7-9]。

准循环(quasi cyclic, QC)LDPC 作为一类非常重要的结构化 LDPC 码,其特殊的循环结构使得编码可以采用移位寄存器在线性时间内完成,译码可以采用计数器寻址,并且可以并行实现,从而可以大大提高译码吞吐量。本文针对列重 λ 较小的校验矩阵 $\boldsymbol{H}_{qc}$,提出了利用近似满秩(approximate full rank, AFR)矩阵实现快速编码的方法,并给出了利用有限域乘群、加群来构造 AFR 矩阵的方法。由校验矩阵不但可以得到生成矩阵的系统形式,而且生成矩阵也是由循环方阵构成的阵列。虽然生成矩阵中循环方阵往往不是稀疏的,但只需保存循环阵中的第一行(列)即可,编码时采用反馈移位寄存器循环移位编码。文献[10]针对 QC LDPC 码的校验矩阵是否满秩的情况,提出了两种不同的编码方案,并且给出了基于移位寄存器累加(shift register adder accumulator, SRAA)单元的串行编码、并行编码和两级编码器,后两种编码器要求校验矩阵是满秩矩阵。

收稿日期:2009-03-20; **修回日期**:2009-05-31。

作者简介:窦高奇(1981-),男,讲师,博士,主要研究方向为纠错编码和 Turbo 均衡技术。E-mail:gqdou0917@163.com

如何构造满秩矩阵是实现快速编码的关键。本文首先介绍了基于 GF(q)域乘群、加群构造校验矩阵的方法,然后提出了一种利用近似满秩校验矩阵实现快速编码的方案,该编码方法和编码电路与满秩情况完全相同,从而可以根据编码速率和复杂度灵活选择编码电路来满足不同要求。

1　基于有限域的校验矩阵构造方法

本节首先介绍了有限域构造 QC LDPC 码校验矩阵的基础:域元素的位置向量表示和矩阵扩展,然后介绍了两种具体的构造方法:GF(q)乘群构造法和 GF(q)素域加群构造法。构造的校验矩阵 $\boldsymbol{H}$ 都由循环置换阵和全零方阵组成,对应的 Tanner 图的围长 $g\geqslant 6$。

令 α 为伽罗华(Galois)域 GF(q)上的本原元,其中,$q=p^m$,p 为素数,m 为正整数。元素 $\alpha^{-\infty}=0,\alpha^0=1,\alpha,\alpha^2,\cdots,\alpha^{q-2}$ 构成 GF(q)上的全部元素且有 $\alpha^{q-1}=1$。GF(q)中的 $q-1$ 个非零元素构成乘运算下的循环群 $\mathcal{G}_q=\{\alpha^0=1,\alpha,\alpha^2,\cdots,\alpha^{q-2}\}$。对于 $\mathcal{G}_q$ 中的每个元素 α^i,构造一个 GF(2)上的 $q-1$ 维向量 $\boldsymbol{z}(\alpha^i)$ 与其对应

$$\boldsymbol{z}(\alpha^i)=(z_0,z_1,\cdots,z_{q-2}) \tag{1}$$

式中,$\boldsymbol{z}(\alpha^i)$ 中除第 i 个元素 $z_i=1$ 外,其他 $q-2$ 个元素都为零,称 $\boldsymbol{z}(\alpha^i)$ 为 α^i 的位置向量。由此可以看出,GF(q)中的 $q-1$ 个非零元素分别对应不同的位置向量。定义零元素 $\alpha^{-\infty}=0$ 对应一个全零向量 $\boldsymbol{z}(0)=(0,0,\cdots,0)$。令 β 为 GF(q)中的非零元素,则 $\alpha\beta$ 的位置向量 $\boldsymbol{z}(\alpha\beta)$ 可以看做是 β 的位置向量 $\boldsymbol{z}(\beta)$ 循环右移一位。依次以 $\beta,\alpha\beta,\cdots,\alpha^{q-2}\beta$ 的位置向量为行构造 $(q-1)\times(q-1)$ 的方阵 $\boldsymbol{A}$,则 $\boldsymbol{A}$ 为一循环置换阵。$\boldsymbol{A}$ 称作 GF(q)中元素 β 的矩阵扩展。域元素的位置向量表示和矩阵扩展是构造 QC LDPC 码校验矩阵的基础。

1.1　基于 GF(q)乘群的校验矩阵构造法

令 X 为 GF(q)中的任一元素,$a,b\in$ GF(q)且 $a\neq 0$,$Y=aX-b$ 表示域元素 X 到 Y 的映射,称 X 到 Y 的映射为仿射变换[9]。

对 GF(q)的非零元素 $\alpha^0,\alpha,\alpha^2,\cdots,\alpha^{q-2}$ 进行 $Y=\alpha^iX-\beta$ 变换,可以得到 $q-1$ 重矢量 $\boldsymbol{w}_i$

$$\boldsymbol{w}_i=(\alpha^i-\beta,\alpha^{i+1}-\beta,\cdots,\alpha^{i+(q-2)}-\beta)$$

式中,$\beta=\alpha^c$,$0\leqslant c\leqslant q-2$,称 β 为偏移常数,对 α 的幂次进行模 $(q-1)$ 运算。

以 $\boldsymbol{w}_0,\boldsymbol{w}_1,\cdots,\boldsymbol{w}_{q-2}$ 为行构造 GF(q)上的 $(q-1)\times(q-1)$ 基矩阵 $\boldsymbol{W}^{(1)}$

$$\boldsymbol{W}^{(1)}=\begin{bmatrix}\boldsymbol{w}_0\\ \boldsymbol{w}_1\\ \vdots\\ \boldsymbol{w}_{q-2}\end{bmatrix}=\begin{bmatrix}\alpha^0-\beta & \alpha-\beta & \cdots & \alpha^{q-2}-\beta\\ \alpha-\beta & \alpha^2-\beta & \cdots & \alpha^{q-1}-\beta\\ \vdots & \vdots & \ddots & \vdots\\ \alpha^{q-2}-\beta & \alpha^{q-1}-\beta & \cdots & \alpha^{2(q-2)}-\beta\end{bmatrix}$$

对每一行 $\boldsymbol{w}_i$,依次乘以 GF(q)中的非零域元素 $\alpha^0,\alpha,\cdots,\alpha^{q-2}$ 后得矩阵 $\boldsymbol{W}_i^{(1)}$,利用式(1)定义的位置向量代替 $\boldsymbol{W}_i^{(1)}$ 中对应的元素,则可得到一个 GF(2)下的 $(q-1)\times(q-1)^2$ 的矩阵 $\boldsymbol{B}_i^{(1)}$

$$\boldsymbol{B}_i^{(1)}=[\boldsymbol{A}_{i0}\quad\boldsymbol{A}_{i1}\quad\cdots\quad\boldsymbol{A}_{i,(q-2)}]$$

式中,$\boldsymbol{A}_{ij}$ 是由 $\boldsymbol{W}_i^{(1)}$ 中第 j 列元素 $\alpha^{i+j}-\beta,\alpha(\alpha^{i+j}-\beta),\cdots,\alpha^{q-2}(\alpha^{i+j}-\beta)$ 的位置向量构成的 $(q-1)\times(q-1)$ 循环方阵。由 $\boldsymbol{B}_1^{(1)},\boldsymbol{B}_2^{(1)},\cdots,\boldsymbol{B}_{q-2}^{(1)}$ 为行构造 $(q-1)\times(q-1)$ 的阵列矩阵 $\boldsymbol{H}^{(1)}$

$$\boldsymbol{H}^{(1)}=\begin{bmatrix}\boldsymbol{B}_0^{(1)}\\ \boldsymbol{B}_1^{(1)}\\ \vdots\\ \boldsymbol{B}_{q-1}^{(1)}\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}_{00} & \boldsymbol{A}_{01} & \cdots & \boldsymbol{A}_{0,q-2}\\ \boldsymbol{A}_{10} & \boldsymbol{A}_{11} & \cdots & \boldsymbol{A}_{1,q-2}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_{q-2,0} & \boldsymbol{A}_{q-2,1} & \cdots & \boldsymbol{A}_{q-2,q-2}\end{bmatrix}$$

式中,$\boldsymbol{A}_{0c},\boldsymbol{A}_{1,(c-1)\bmod(q-1)},\boldsymbol{A}_{2,(c-2)\bmod(q-1)},\cdots,\boldsymbol{A}_{q-2,(c-q-2)\bmod(q-1)}$ 为 $(q-1)\times(q-1)$ 的全零阵,其他 $\boldsymbol{A}_{ij}$ 为 $(q-1)\times(q-1)$ 的循环置换阵。由前面 $\boldsymbol{W}^{(1)}$ 的结构特性可知,对 $\boldsymbol{W}^{(1)}$ 进行垂直扩展和水平扩展后得到的阵列矩阵 $\boldsymbol{H}^{(1)}$ 满足 LDPC 码的行列(row column, RC)约束。$\boldsymbol{H}^{(1)}$ 是一个行重和列重都为 $q-2$ 的 $(q-1)^2\times(q-1)^2$ 矩阵,对应的 Tanner 图的 girth 至少为 6。

1.2　基于素域加群的校验矩阵构造法

前面给出了 GF(q)乘群下的 QC LDPC 码的构造方法,LDPC 码还可以利用 GF(q)加群来构造。当有限域为素数域时,可以构造出具有准循环结构的 LDPC 码。假定 q 为素数,整数集 GF(q)$=\{0,1,\cdots,q-1\}$ 在模 q 乘和模 q 加下构成一个素域。对于素域中的任一元素 $i\in$ GF(q),我们定义与其对应的 q 重位置矢量

$$\boldsymbol{z}(i)=(z_0,z_1,\cdots,z_{q-1}) \tag{2}$$

式中,$\boldsymbol{z}(i)$ 中除第 i 个分量 $z_i=1$ 外其余 $q-1$ 个分量全为零。与前面定义的位置向量不同的是,素域中元素 0 的位置向量为 $\boldsymbol{z}(0)=(1,0,\cdots,0)$。

构造 GF(q)上的 $q\times q$ 基矩阵 $\boldsymbol{W}^{(2)}$

$$\boldsymbol{W}^{(2)}=\begin{bmatrix}\boldsymbol{w}_0\\ \boldsymbol{w}_1\\ \vdots\\ \boldsymbol{w}_i\\ \vdots\\ \boldsymbol{w}_{q-1}\end{bmatrix}=\begin{bmatrix}0\cdot 0 & 0\cdot 1 & \cdots & 0\cdot(q-1)\\ 1\cdot 0 & 1\cdot 1 & \cdots & 1\cdot(q-1)\\ \vdots & \vdots & \ddots & \vdots\\ i\cdot 0 & i\cdot 1 & \cdots & i\cdot(q-1)\\ \vdots & \vdots & \ddots & \vdots\\ (q-1)\cdot 0 & (q-1)\cdot 1 & \cdots & (q-1)\cdot(q-1)\end{bmatrix}$$

对于 $\boldsymbol{W}^{(2)}$ 中每一行 $\boldsymbol{w}_i$,依次加 GF(q)中的域元素 $0,1,\cdots,q-1$ 后进行垂直扩展后得矩阵 $\boldsymbol{W}_i^{(2)}$,利用式(2)的位置向量代替 $\boldsymbol{W}_i^{(2)}$ 中的相应元素,对其进行水平扩展,则可得到一个 GF(2)下的 $q\times q^2$ 矩阵 $\boldsymbol{B}_i^{(2)}$

$$\boldsymbol{B}_i^{(2)}=[\boldsymbol{A}_{i0}\quad\boldsymbol{A}_{i1}\quad\cdots\quad\boldsymbol{A}_{i,(q-1)}]$$

式中,$\boldsymbol{A}_{ij}$ 是一个 $q\times q$ 的循环置换阵。由 $\boldsymbol{B}_0^{(2)},\cdots,\boldsymbol{B}_{q-1}^{(2)}$ 为行可以构造由 $q\times q$ 个循环置换阵组成的阵列 $\boldsymbol{H}^{(2)}$

$$\boldsymbol{H}^{(2)}=\begin{bmatrix}\boldsymbol{B}_0^{(2)}\\ \boldsymbol{B}_1^{(2)}\\ \vdots\\ \boldsymbol{B}_{q-1}^{(2)}\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}_{00} & \boldsymbol{A}_{01} & \cdots & \boldsymbol{A}_{0,q-1}\\ \boldsymbol{A}_{10} & \boldsymbol{A}_{11} & \cdots & \boldsymbol{A}_{1,q-1}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_{q-1,0} & \boldsymbol{A}_{q-1,1} & \cdots & \boldsymbol{A}_{q-1,q-1}\end{bmatrix}$$

式中，$\boldsymbol{H}^{(2)}$ 的第一行和第一列为单位阵。$\boldsymbol{H}^{(2)}$ 是行重和列重都为 q 的 $q^2\times q^2$ 矩阵。同样由 $\boldsymbol{W}^{(2)}$ 的结构特性可知，$\boldsymbol{H}^{(2)}$ 中不含长度为 4 的环。因此，$\boldsymbol{H}^{(2)}$ 满足 LDPC 码的 RC 约束条件。

2 QC LDPC 码的编码

定义 QC LDPC 码的校验矩阵为

$$\boldsymbol{H}_{qc}=\begin{bmatrix}\boldsymbol{A}_{11} & \boldsymbol{A}_{12} & \cdots & \boldsymbol{A}_{1\rho}\\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} & \cdots & \boldsymbol{A}_{2\rho}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_{\lambda 1} & \boldsymbol{A}_{\lambda 2} & \cdots & \boldsymbol{A}_{\lambda,\rho}\end{bmatrix} \tag{3}$$

式中，$\boldsymbol{A}_{ij}$ 为 $b\times b$ 的循环置换阵。

文献[8]针对式(3)中 $\boldsymbol{H}_{qc}$ 的结构特点，介绍了两种由校验矩阵求解系统生成矩阵的方法。第一种情况是针对 $\boldsymbol{H}_{qc}$ 的秩 $r=\lambda b$ 且 $\boldsymbol{H}_{qc}$ 中存在秩为 r 的 $\lambda\times\lambda$ 子阵列 $\boldsymbol{D}$ 的情况；第二种情况是针对 $r<\lambda b$ 或 $r=\lambda b$ 但 $\boldsymbol{H}_{qc}$ 中不存在秩为 r 的 $\lambda\times\lambda$ 子阵列 $\boldsymbol{D}$ 的情况。然而，针对有限域构造的校验矩阵进行编码，两种方法都存在一定的局限性。这是因为，对于由循环方阵构造的校验矩阵，很难达到第一种满秩情况的要求，更严格地说，完全由循环置换阵(不包括全零阵)构造的列重为 λ 校验矩阵 $\boldsymbol{H}_{qc}$ 的秩最大为 $\lambda b-\lambda+1$，必定是非满秩矩阵。对于第二种非满秩情况，它将待编码的信息组分为两部分：$\boldsymbol{a}=[\boldsymbol{a}_1,\boldsymbol{a}_2]$，编码之后码字不再是系统码，只有 $\boldsymbol{a}_1$ 部分与信息位相同，译码后需要额外的处理来恢复信息位 $\boldsymbol{a}_2$，而 $\boldsymbol{a}_2$ 部分与 $\boldsymbol{H}_{qc}$ 中线性相关行的数目有关。以式(3)为例，由循环置换阵构造的 $\boldsymbol{H}_{qc}$ 的秩最大为 $\lambda b-\lambda+1$，相应的相关行数目最少为 $\lambda-1$，此时对应的 $\boldsymbol{a}_2$ 信息长度也为 $\lambda-1$。

对于利用有限域方法构造的校验矩阵 $\boldsymbol{H}$，我们需要从 $\boldsymbol{H}$ 中选择部分循环置换阵来构造 QC LDPC 码的校验矩阵 $\boldsymbol{H}_{qc}$。对于行重、列重分别为 ρ 和 λ 的规则 QC LDPC 码的校验矩阵 $\boldsymbol{H}_{qc}$，通常选取 $\boldsymbol{H}$ 中 $\lambda\times\rho$ 个循环置换阵来构造 $\boldsymbol{H}_{qc}$。$\boldsymbol{H}_{qc}$ 可以看做是 $\boldsymbol{H}$ 的子阵列，其秩小于等于 $\lambda b-\lambda+1$。我们希望从 $\boldsymbol{H}$ 中选择 $\lambda\times\rho$ 个循环置换阵，在满足 LDPC 码 RC 约束的前提下，其秩达到最大值 $\lambda b-\lambda+1$。如果构造的校验矩阵 $\boldsymbol{H}_{qc}$ 中存在秩为 $\lambda b-\lambda+1$ 的 $\lambda\times\lambda$ 子阵列 $\boldsymbol{D}$，则 $\boldsymbol{H}_{qc}$ 中线性相关列的数目为 $\lambda-1$，当列重 λ 较小时 $\boldsymbol{H}_{qc}$ 近似为满秩矩阵，编码时可以令 $\boldsymbol{a}_2=0$，只进行 $\boldsymbol{a}_1$ 部分编码。该方法不但可以简化编码方法，而且编出的码都为系统码。本文的编码都是围绕如何构造出秩为 $\lambda b-\lambda+1$ 的 $\boldsymbol{H}_{qc}$ 展开的。

从构造的校验矩阵 $\boldsymbol{H}$ 中选取 $\lambda\times\rho$ 个循环置换阵，或者等价地从对应的矩阵 $\boldsymbol{W}$ 中选取 $\lambda\times\rho$ 个元素来构造 $\boldsymbol{H}_{qc}$ 要满足两个条件：一是要使构造的 $\boldsymbol{H}_{qc}$ 仍满足 LDPC 码的 RC 约束，此条件只要保证选取的 $\lambda\times\rho$ 个循环置换阵彼此之间的相对位置不变即可满足；另一是要使阵列 $\boldsymbol{H}_{qc}$ 的秩达到 $\lambda b-\lambda+1$。这里实现简化编码的关键，通常采用两种选取方式，一种是分块法；一种是随机选取法。分块法是直接从 $\boldsymbol{W}$ 中分出大小为 $\lambda\times\rho$ 的块作为基矩阵 $\boldsymbol{M}$ 来构造 $\boldsymbol{H}_{qc}$。由于 $\boldsymbol{W}$ 矩阵斜对角线元素都相等，具有较规则的结构，使得直接分出的基矩阵 $\boldsymbol{M}$ 生成的 $\boldsymbol{H}_{qc}$ 的秩很难达到其最大值 $\lambda b-\lambda+1$。随机选取法是首先生成 $0\sim b-1$ 之间的 λ 和 ρ 个不同的随机数构成坐标对，然后从 $\boldsymbol{W}$ 中选取对应的元素来构造基矩阵 $\boldsymbol{M}$。仿真表明，随机选取法通常都能找到满足要求的 $\boldsymbol{M}$，所构造的 $\boldsymbol{H}_{qc}$ 的秩都能达到 $\lambda b-\lambda+1$。本文的相关仿真都采用随机选取法来构造基矩阵 $\boldsymbol{M}$。下面针对秩为 $\lambda b-\lambda+1$ 的近似满秩矩阵 $\boldsymbol{H}_{qc}$，给出由 $\boldsymbol{H}_{qc}$ 求得其对应的生成矩阵 $\boldsymbol{G}_{qc}$ 的方法。求得的 $\boldsymbol{G}_{qc}$ 不但是系统形式的，而且也是由循环方阵构成的阵列。利用 $\boldsymbol{G}_{qc}$ 可以实现线性复杂度编码。

假设 $\boldsymbol{H}_{qc}$ 最右边的 $\lambda\times\lambda$ 子阵列 $\boldsymbol{D}$ 的秩为 $r=\lambda b-\lambda+1$。当不满足此条件时可通过列子阵重排获得。子阵列 $\boldsymbol{D}$ 为

$$\boldsymbol{D}=\begin{bmatrix}\boldsymbol{A}_{1,(\rho-\lambda+1)} & \boldsymbol{A}_{1,(\rho-\lambda+2)} & \cdots & \boldsymbol{A}_{1,\rho}\\ \boldsymbol{A}_{2,(\rho-\lambda+1)} & \boldsymbol{A}_{2,(\rho-\lambda+2)} & \cdots & \boldsymbol{A}_{2,\rho}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_{\lambda,(\rho-\lambda+1)} & \boldsymbol{A}_{\lambda,(\rho-\lambda+2)} & \cdots & \boldsymbol{A}_{\lambda,\rho}\end{bmatrix}$$

对于系统码集 C_{qc}，假定前 $(\rho-\lambda)b$ 为信息位，则其生成矩阵的系统形式为

$$\boldsymbol{G}_{qc}=\begin{bmatrix}\boldsymbol{G}_1\\ \boldsymbol{G}_2\\ \vdots\\ \boldsymbol{G}_{\rho-\lambda}\end{bmatrix}=$$

$$\begin{bmatrix}\boldsymbol{I} & \boldsymbol{0} & \cdots & \boldsymbol{0} & \boldsymbol{G}_{11} & \boldsymbol{G}_{12} & \cdots & \boldsymbol{G}_{1\lambda}\\ \boldsymbol{0} & \boldsymbol{I} & \cdots & \boldsymbol{0} & \boldsymbol{G}_{21} & \boldsymbol{G}_{22} & \cdots & \boldsymbol{G}_{2\lambda}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{I} & \boldsymbol{G}_{\rho-\lambda,1} & \boldsymbol{G}_{\rho-\lambda,2} & \cdots & \boldsymbol{G}_{\rho-\lambda,\lambda}\end{bmatrix}=[\boldsymbol{I}_{(\rho-\lambda)b}\boldsymbol{P}]$$

式中，$\boldsymbol{I}$ 为 $b\times b$ 的单位阵；$\boldsymbol{0}$ 为 $b\times b$ 的全零阵；$\boldsymbol{G}_{ij}$ 为 $b\times b$ 的循环方阵；$\boldsymbol{P}$ 是由 $(\rho-\lambda)\cdot\lambda$ 个循环方阵构成，因此 $\boldsymbol{G}_{qc}$ 具有系统循环形式。设子生成多项式 $\boldsymbol{g}_{ij}=(g_{ij}^1,g_{ij}^2,\cdots,g_{ij}^b)$ 为循环方阵 $\boldsymbol{G}_{ij}$ 的第一行，可知 $\boldsymbol{G}_{ij}$ 可由 $\boldsymbol{g}_{ij}$ 循环移位获得。从而可以得出，生成矩阵 $\boldsymbol{G}_{qc}$ 完全由 $(\rho-\lambda)\cdot\lambda$ 个子生成多项式决定，编码时只需存储 $(\rho-\lambda)\cdot\lambda$ 个子生成多项式即可。

令 $\boldsymbol{u}=(1,0,\cdots,0)$，$\boldsymbol{0}=(0,0,\cdots,0)$，这两个向量长度均为 b，对于 $1\leqslant i\leqslant\rho-\lambda$，行子阵 $\boldsymbol{G}_i$ 的第一行为

$$\boldsymbol{g}_i=(\boldsymbol{0},\cdots,\boldsymbol{u},\cdots,\boldsymbol{0},\boldsymbol{g}_{i1},\boldsymbol{g}_{i2},\cdots,\boldsymbol{g}_{i,\lambda})$$

式中，向量 $\boldsymbol{u}$ 在 $\boldsymbol{g}_i$ 的第 i 个位置。

校验矩阵和生成矩阵满足关系

$$\boldsymbol{H}_{qc}\boldsymbol{G}_{qc}^{\mathrm{T}}=[\boldsymbol{0}] \tag{4}$$

可得

$$\boldsymbol{H}_{qc}\boldsymbol{g}_i^{\mathrm{T}}=0$$

令 $\boldsymbol{z}_i=(\boldsymbol{g}_{i1},\boldsymbol{g}_{i2},\cdots\boldsymbol{g}_{i\lambda})$，$\boldsymbol{M}_i=[\boldsymbol{A}_{1i}^{\mathrm{T}}\quad\boldsymbol{A}_{2i}^{\mathrm{T}}\quad\cdots\quad\boldsymbol{A}_{\lambda i}^{\mathrm{T}}]^{\mathrm{T}}$ 为 $\boldsymbol{H}_{qc}$ 的第 i 个列子阵。由式(4)可得

$$\boldsymbol{M}_i\boldsymbol{u}^{\mathrm{T}}+\boldsymbol{D}\boldsymbol{z}_i^{\mathrm{T}}=\boldsymbol{0} \tag{5}$$

由于 $\boldsymbol{D}$ 不是满秩矩阵，无法直接求得其逆矩阵，需要对其进

行处理。方法是首先找到 $\boldsymbol{D}$ 中所有 $\lambda-1$ 个线性相关的列,记下相应的位置 $\boldsymbol{P}$,然后消去 $\boldsymbol{D}$ 中线性相关的行列,使 $\boldsymbol{D}$ 变成 $r\times r$ 的满秩方阵 $\boldsymbol{D}^*$,代入式(5)进行求解,得

$$\boldsymbol{z}_i^{\mathrm{T}}=\boldsymbol{D}^{*-1}\boldsymbol{M}_i\,\boldsymbol{u}^{\mathrm{T}} \tag{6}$$

求得 $\boldsymbol{z}_i$ 后将对应的位置 $\boldsymbol{P}$ 补零。由式(6)可得 $\boldsymbol{z}_1,\boldsymbol{z}_2,\cdots,\boldsymbol{z}_{t-c}$,从而可以确定 $\boldsymbol{G}_{qc}$ 的 $(\rho-\lambda)\cdot\lambda$ 个子生成多项式 $\boldsymbol{g}_{ij}$。需要注意的是,以上相乘、求逆等运算都是在 GF(2)域上进行的。

编码时,信息序列按 $(\rho-\lambda)b$ 进行分组,每一分组 $\boldsymbol{a}$ 进一步分为 $(\rho-\lambda)$ 段,每段 b 比特,即 $\boldsymbol{a}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_{\rho-\lambda})$,第 i 段为 $\boldsymbol{a}_i=(a_{(i-1)b+1},a_{(i-1)b+2},\cdots,a_{ib})$。经编码器编码后得 $\boldsymbol{c}=\boldsymbol{a}\boldsymbol{G}_{qc}=(\boldsymbol{a},\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_\lambda)$,其中,$\boldsymbol{p}_j=(p_{j1},p_{j2},\cdots p_{j,b})$。由 $\boldsymbol{c}=\boldsymbol{a}\boldsymbol{G}_{qc}$ 得

$$\boldsymbol{p}_j=\boldsymbol{a}_1\boldsymbol{G}_{1j}+\boldsymbol{a}_2\boldsymbol{G}_{2j}+\cdots+\boldsymbol{a}_{\rho-\lambda}\boldsymbol{G}_{(\rho-\lambda),j} \tag{7}$$

由式(7)可知,$\boldsymbol{a}_i\boldsymbol{G}_{ij}$ 实际上是 $\boldsymbol{G}_{ij}$ 的子生成多项式 $\boldsymbol{g}_{ij}$ 按 $\boldsymbol{a}_i$ 的 b 个连续信息比特进行循环移位累加(模 2)的结果。如图 1 为 SRAA 单元。首先 $\boldsymbol{G}_{qc}$ 第一行的 λ 个子生成多项式 $\boldsymbol{g}_{11},\boldsymbol{g}_{12},\cdots,\boldsymbol{g}_{1\lambda}$ 加载到 λ 个 SRAA 中,信息段 $\boldsymbol{a}_1$ 逐位输入,每输入一位,$\boldsymbol{g}_{1j}$ 循环移位一次。当输入信息位为 1 时,"与"门打开,进行累加。经 b 次循环后,开始信息段 $\boldsymbol{a}_2$ 输入,此时累加寄存器中 $\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_\lambda$ 保持不变,$\boldsymbol{g}_{21},\boldsymbol{g}_{22},\cdots,\boldsymbol{g}_{2\lambda}$ 加载 SRAA。经 $\rho-\lambda$ 次相同操作后,λ 个 SRAA 中累加寄存器保存值即为 λ 个校验位段 $\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_\lambda$,将其附在信息组 $\boldsymbol{a}$ 后完成编码,其编码复杂度与校验位长度成线性关系。

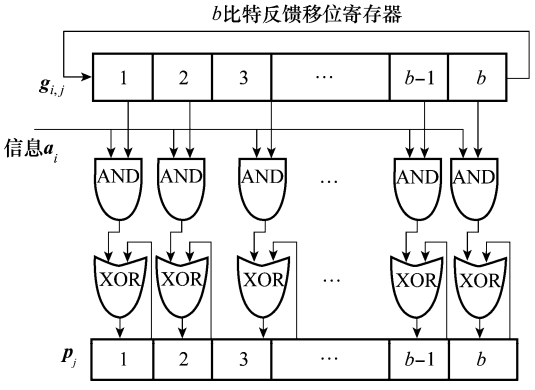

图 1　移位寄存器累加(SRAA)单元

3　性能和复杂度分析

Mackay 在其网站[11]提供了不同码长的随机 LDPC 码,称其为 Mackey 码。Mackey 码是一种性能较好的随机 LDPC 码,我们选择不同码长和不同码率的LDPC码与本文构造的 QC LDPC 码作对比。利用有限域乘群和加群构造 QC LDPC 码分别记为 QC mult(N,K)和 QC add(N,K)。其中,N 为码长,K 为信息分组。仿真图中横坐标表示信噪比 E_b/N_0,纵坐标 FER 表示误帧率,BER 表示误比特率,信道为加性高斯白噪声信道,译码采用 SP 译码算法,下面给出了 Mackey 随机好码与结构化 QC LDPC 码在不同码长下的性能对比。仿真时最大迭代次数为 50 次,每一信噪比下误帧率达到 30 帧时结束该信噪比仿真。

图 2 是利用 GF(137)乘群构造的码长为 816、码率 0.33、行重和列重分别为$(\lambda,\rho)=(4,6)$的 QC mult(816,272)码与相同参数的 Mackey 码的 FER 和 BER 性能曲线。从中可以看出,利用 GF(137)乘群构造的 QC LDPC 与相同参数的 Mackey 码性能基本相同。图 3 是利用 GF(53)素域加群构造的码长为 1 098、码率为 0.889、行重和列重分别为$(\lambda,\rho)=(4,36)$的 QC add(1 908,1 696)与相同参数的 Mackey码的性能曲线。由此可以看出,利用素域加群构造的高码率 QC LDPC 码与相同参数的 Mackey 码性能基本相同,在高信噪比时略微好一些。而本文所构造的 QC LDPC码可以采用反馈移位寄存器实现线性化编码,不但可以大大降低存储量,而且编出的码都为系统码。

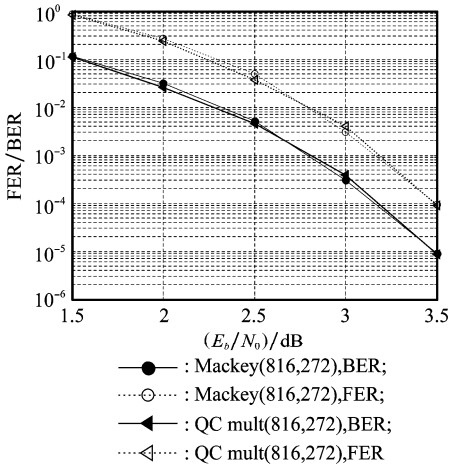

图 2　码长为 816 的 Mackey 码与 QC LDPC 码性能曲线

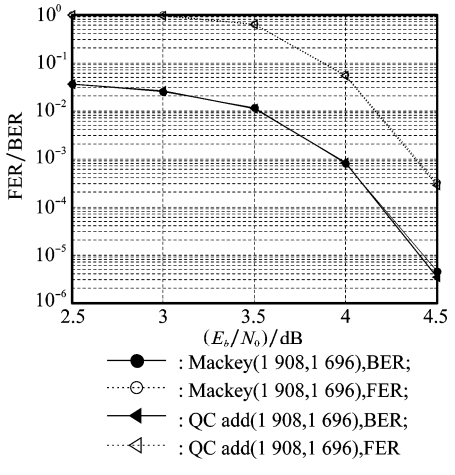

图 3　码长为 1 908 的 Mackey 码与 QC LDPC 码性能曲线

基于 SRAA 的串行编码器采用逐比特编码方式,其复杂度与码的奇偶校验位数 λb 成线性关系,编完一组码字需要的时钟节拍数为$(\rho-\lambda)b$;而基于 SRAA 的并行编码器要

等到所有信息比特到达后才进行编码，其复杂度与码长 ρb 成线性关系，编完一组码字所需的时钟节拍数为 λb；两级编码器所需的时钟节拍数为 b。后两种编码器的吞吐量大，可以满足高速通信需求，但要求校验矩阵为满秩矩阵，而一般 QC LDPC 码校验矩阵都是非满秩矩阵，如何构造出适合后两种编码的校验矩阵是实现快速编码的关键。本文构造的近似满秩矩阵不但可以简化编码结构，而且适用于基于 SRAA 的并行编码和两级编码，从而可以满足高速通信需求。表 1 给出了三种编码器编码速率和所需资源对比。可以看出，两级编码器的编码速率最快，所需的资源也比较少。

表 1 三种编码器编码速率和所需资源对比

编码方案	编码速率	触发器	XOR	AND
串行编码	$(\rho-\lambda)b$	$2\lambda b$	λb	λb
并行编码	λb	$(\rho-\lambda)b$	$(\rho-\lambda)b-1$	$(\rho-\lambda)b$
两级编码	b	ρb	$O(\lambda^2 b)$	0

4 结束语

编码复杂度是制约 LDPC 码实用化的一个重要原因。本文针对 QC LDPC 码校验矩阵的特殊结构，提出了利用 AFR 矩阵实现快速编码的方法，并且基于有限域乘群、加群构造出 AFR 校验矩阵。利用 AFR 校验矩阵可以快速得到系统循环形式的生成矩阵，编码时可以采用反馈移位寄存器循环移位编码。利用 AFR 矩阵不但可以简化编码方法，而且编出的码都为系统码。仿真表明，该编码方案对列重较小的 QC LDPC 码具有较好的通用性和实用价值。

参考文献：

[1] Gallager R G. Low-density parity-check codes[J]. *IRE Trans. on Information Theory*, 1962,8:21-28.

[2] MacKay D J C. Good error correcting codes based on very sparse matrices[J]. *IEEE Trans. on Information Theory*, 1999,45(2):399-431.

[3] Hu X Y, Eleftheriou E, Arnold D M. Regular and irregular progressive edge-growth tanner graphs[J]. *IEEE Trans. on Information Theory*, 2005,51(1):386-398.

[4] Sharon E, Litsyn S. Constructing LDPC Codes by error minimization progressive edge growth[J]. *IEEE Trans. on Communication*, 2008,56(3):359-368.

[5] Kou Y, Lin S, Fossorier M R C. Low-density parity-check codes based on finite geometries: a rediscovery and new result[J]. *IEEE Trans. on Information Theory*, 2001, 47(7): 2711-2736.

[6] Xu J, Chen L, Djurdjevic I, et al. Construction of regular and irregular LDPC codes: geometry decomposition and masking[J]. *IEEE Trans. on Information Theory*, 2007,53(1):121-134.

[7] Djurdjevic I, Xu J, Abdel-Ghaffar K, et al. Construction of low-density parity-check codes based on reed-Solomon codes with two information symbols[J]. *IEEE Communication Letter*, 2003,7(7):317-319.

[8] Freundlich S, Burshtein D, Litsyn S. Approximately lower triangular ensembles of LDPC codes with linear encoding complexity[J]. *IEEE Trans. on Information Theory*, 2007,53(4):1484-1494.

[9] Lan L, Zeng L Q, Tai Y Y, et al. Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach[J]. *IEEE Trans. on Information Theory*, 2007,53(7):2429-2458.

[10] Li Z W, Chen L, Zeng L Q, et al. Efficient encoding of quasi-cyclic low-density parity-check codes[J]. *IEEE Trans. on Communication*, 2006,54(1):71-81.

[11] Mackay D J C. Encyclopedia of sparse graph codes [EB/OL]. http://www.inference.phy.cam.ac.uk/mackay/codes/data.html.