doi:10.11959/j.issn.1000-436x.2015048

基于改进 2-D GRS 码的 QC-LDPC 码高效构造

赵明，张晓林
（北京航空航天大学 电子信息工程学院，北京 100191）

摘 要：利用 GRS(generalized reed-solomon)码的生成多项式提出了基于改进的 2-D GRS(two-dimensional GRS)码设计和构造 QC-LDPC(quasi-cyclic low density parity-check)码的方法，使所构造的码具有较好的译码性能。同时在码的构造过程中，考虑到了准双对角线结构和合适的度分布。不同码率的 LDPC 码用于和新设计的 QC-LDPC 码进行测试和比较。实验结果表明，所提出的码构造方法可加快 LDPC 码校验矩阵的构造，同时基于所提出方法构造的 QC-LDPC 码可提高译码性能，并降低编码复杂度。

关键词：QC-LDPC 码；码构造；改进的 2-D GRS 码；矩阵扩展；度分布
中图分类号：TN911.2 **文献标识码**：A

Novel construction of QC-LDPC codes with modified 2-D GRS codes

ZHAO Ming, ZHANG Xiao-lin
（School of Electronic and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100191, China）

Abstract: The construction method for QC-LDPC (quasi-cyclic low density parity-check) code with modified two-dimensional generalized reed-solomon (2-D GRS) code is proposed using the generator polynomial of GRS code, so thus the constructed code can have better decoding performance. Meanwhile both the quasi dual-diagonal structure and proper weight distributions are considered during the construction. The QC-LDPC codes with different rates are used to compare with the new designed codes. Experimental results show that the proposed method can accelerate the construction and QC-LDPC codes constructed from the proposed method can have better decoding performance while with low encoding complexity.

Key words: QC-LDPC code; code construction; modified 2-D GRS code; matrix dispersion; degree distributions

1 引言

LDPC 码具有接近 Shannon 极限的译码性能，且具有较低的译码复杂度和并行译码的潜力[1,2]，因此 LDPC 码在许多通信系统的信道编码标准中都有很好的应用。LDPC 码可分为 2 大类：随机 LDPC 码和 QC-LDPC 码。无 4 环的随机 LDPC 码的最小码重和码间距离近似为码长的线性函数，但其编译码和相应的硬件实现较为困难。而 QC-LDPC 码是由一组循环矩阵构成的，易于高效编码和译码，且便于硬件实现。

在 LDPC 好码的构造中，主要考虑的因素有：1)LDPC 码的校验矩阵 $\boldsymbol{H}$ 中任意 2 行或 2 列不会有 2 处或 2 处以上在相同的位置上有“1”，这种对 $\boldsymbol{H}$ 的行和列的约束通常称为行列约束条件(row-column- constraint)，这种行列约束条件实际上是保证 LDPC 码对应的 Tanner 图不存在长度为 4 的环，即 Tanner 图中的围长至少为 6[3~5]；2) LDPC 码的最小码间距，即其生成矩阵 $\boldsymbol{G}$ 的行相关问题。事实上，最小码间距在很大程度上决定了利用迭代方法对 LDPC 码进行译码所产生的误码平层。因此，LDPC 码的最小码间距必须保证尽可能大。对于基

收稿日期：2013-07-29；**修回日期**：2013-11-11
基金项目：中国国家地面数字电视研究工程应用基金资助项目
Foundation Item: The Application of China National Terrestrial Digital TV System Research Project

于迭代译码的非规则 LDPC 码，其译码性能还取决于对应 Tanner 图中变量节点和校验节点的度分布，或其校验矩阵 $\boldsymbol{H}$ 的行列重分布[4,5]。

对于 QC-LDPC 码的构造，需要设计校验矩阵中的基矩阵。为降低编译码复杂度，QC-LDPC 码是基于循环移位矩阵的阵列构造校验矩阵。Kou 等[5]提出了利用有限几何的方法来设计 QC-LDPC 码的校验矩阵，从而降低编码复杂度，同时提高译码性能。Lan 等[6]提出利用有限域方法来构造具有很好译码性能的 QC-LDPC 码。Kamiya 等[7,8]总结了有限几何和有限域 2 种方法，并提出利用循环 MDS (maximum distance separable)码和生成多项式构造 QC-LDPC 码。Chen 等[9]提出了利用 2-D MDS 码设计基校验矩阵的方法并给出了构造的简单实例。

利用有限几何方法可有效地保证所构造的 QC-LDPC 码的 Tanner 图不存在 4 环，从而在一定程度上提高译码性能，但无法确保较大的最小码间距[5]。而有限域的方法是基于近世代数中的群、环、域思想进行校验矩阵的构造，可从代数方法上对码的基本性质进行分析和研究[6,10]。但基于有限域方法构造码的 Tanner 图不能保证不存在 4 环，即需要对 Tanner 图进行分析。

为降低编码复杂度同时获得较高的性能，本文提出了利用改进的 2-D GRS 码构造基校验矩阵，同时确保其 Tanner 图不存在 4 环，并利用掩模技术对所得的矩阵进行稀疏化设计，以满足准双对角线结构[11,12]。经过优化设计的 QC-LDPC 码可提高译码性能，同时降低编码复杂度。

2 QC-LDPC 码的代数构造

2.1 基于有限域的 QC-LDPC 码构造

令 s 为正整数，考虑在 $GF(2^s)$ 中，令 $\alpha \in GF(2^s)$ 为本原域元素，则 α 的各次幂，$\alpha^{-\infty}=0,\alpha^0=1,\alpha,\alpha^2,\cdots,\alpha^{2^s-2}$，构成 $GF(2^s)$ 的元素且 $\alpha^{2^s-1}=1$。

对于任意 $\alpha^i \in GF(2^s)$ 且 $\alpha^i \neq 0, i \in [0,2^s-1)$，定义 $GF(2)$ 上的 (2^s-1) 维向量 $\boldsymbol{Z}(\alpha^i)=(z_0, z_1,\cdots,z_{2^s-2})$，向量中 $z_i=1$ 且其他元素均为 0，这些向量对应于 $GF(2^s)$ 中的 (2^s-1) 个元素。这个 (2^s-1) 维向量 $\boldsymbol{Z}(\alpha^i)$ 称为域元素 α^i 的二进制位置向量。

令 β 为 $GF(2^s)$ 中的非零元素，则 $\alpha\beta$ 的二进制位置向量 $\boldsymbol{Z}(\alpha\beta)$ 即是 β 的二进制位置向量 $\boldsymbol{Z}(\beta)$ 循环右移一位的结果。于是依次以 $\beta,\alpha\beta,\cdots,\alpha^{2^s-2}\beta$ 的二进制位置向量为行所构成的 $(2^s-1)\times(2^s-1)$ 阶矩阵即为 $GF(2)$ 上的循环移位矩阵(CPM, circulant permutation matrix)，称为 β 的 (2^s-1) 重二进制矩阵扩展。

令 $\alpha \in GF(2^s)$ 为本原域元素，考虑由 $GF(2^s)$ 中的 n 维向量 $\boldsymbol{w}_0,\boldsymbol{w}_1,\cdots,\boldsymbol{w}_{m-1}$ 为行所构成的 $m\times n$ 阶 $GF(2^s)$ 上的矩阵 $\boldsymbol{W}$

$$\boldsymbol{W}=\begin{bmatrix}\boldsymbol{w}_0\\ \boldsymbol{w}_1\\ \vdots\\ \boldsymbol{w}_{m-1}\end{bmatrix}=\begin{bmatrix}w_{0,0} & w_{0,1} & \cdots & w_{0,n-1}\\ w_{1,0} & w_{1,1} & \cdots & w_{1,n-1}\\ \vdots & \vdots & \ddots & \vdots\\ w_{m-1,0} & w_{m-1,1} & \cdots & w_{m-1,n-1}\end{bmatrix} \tag{1}$$

若矩阵 $\boldsymbol{W}$ 满足以下 2 个约束条件，则称 $\boldsymbol{W}$ 满足 α 乘积的行距(RD, row distance)约束。

1) 对任意的 $0\leqslant i<m$ 和 $0\leqslant k,l<q-1$ 且 $k\neq l$，$\alpha^k\boldsymbol{w}_i$ 和 $\alpha^l\boldsymbol{w}_i$ 至少有 $n-1$ 个位置不同。

2) 对任意的 $0\leqslant i,j<m, i\neq j$ 和 $0\leqslant k,l<q-1$ 且 $k\neq l$，$\alpha^k\boldsymbol{w}_i$ 和 $\alpha^l\boldsymbol{w}_j$ 至少有 $n-1$ 个位置不同。

其中，约束条件 1)表明矩阵 $\boldsymbol{W}$ 的每一行至多有 $GF(2^s)$ 中的一个 0 元素；约束条件 2)表明 $\boldsymbol{W}$ 中的任 2 行至少有 $(n-1)$ 个位置不同。

对任意的 $0\leqslant i<m$ 和 $0\leqslant j<n$，将矩阵 $\boldsymbol{W}$ 的每个元素 $w_{i,j}$ 扩展为二进制的 $(2^s-1)(2^s-1)$ 阶 CPM 或全零矩阵 $\boldsymbol{A}_{i,j}$，得到由 $(2^s-1)(2^s-1)$ 阶子矩阵构成的 $m\times n$ 阶 $GF(2)$ 上的分块矩阵 $\boldsymbol{H}_b$

$$\boldsymbol{H}_b=\begin{bmatrix}\boldsymbol{B}_0\\ \boldsymbol{B}_1\\ \vdots\\ \boldsymbol{B}_{m-1}\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}_{0,0} & \boldsymbol{A}_{0,1} & \cdots & \boldsymbol{A}_{0,n-1}\\ \boldsymbol{A}_{1,0} & \boldsymbol{A}_{1,1} & \cdots & \boldsymbol{A}_{1,n-1}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_{m-1,0} & \boldsymbol{A}_{m-1,1} & \cdots & \boldsymbol{A}_{m-1,n-1}\end{bmatrix} \tag{2}$$

其中，$\boldsymbol{B}_i=[\boldsymbol{A}_{i,0}\quad \boldsymbol{A}_{i,1}\quad \cdots\quad \boldsymbol{A}_{i,n-1}], i=0,1,\cdots,m-1$。$GF(2)$ 上的 $m(2^s-1)\times n(2^s-1)$ 阶矩阵 $\boldsymbol{H}_b$ 称为矩阵 $\boldsymbol{W}$ 的 (2^s-1) 重二进制扩展，称 $\boldsymbol{W}$ 为基矩阵。

可以证明若矩阵 $\boldsymbol{W}$ 满足 α 乘积的 RD-约束，则其扩展矩阵 $\boldsymbol{H}_b$ 的 Tanner 图中围长至少为 6[6, 10]。因此扩展矩阵 $\boldsymbol{H}_b$ 或其子矩阵就可成为校验矩阵并得到一个 QC-LDPC 码。

2.2　掩模(masking)设计

利用二进制扩展得到的矩阵具有较大的密度，因此需要利用全 0 矩阵替换部分 CPM，这种替换设计被称为掩模[6,10]。

考虑由式(2)的分块矩阵 $\boldsymbol{H}_b$ 中选定的 CPM 组成的 $\gamma\times\rho$ 阶子矩阵 $\boldsymbol{H}_b(\gamma,\rho)=[\boldsymbol{A}_{i,j}]$，令 $\boldsymbol{D}(\gamma,\rho)=[d_{i,j}]$ 为 $GF(2)$ 上的低密度 $\gamma\times\rho$ 阶矩阵，于是进行如下矩阵乘法

$$\boldsymbol{M}_b(\gamma,\rho)=\boldsymbol{D}(\gamma,\rho)\otimes\boldsymbol{H}_b(\gamma,\rho)=[d_{i,j}\boldsymbol{A}_{i,j}] \tag{3}$$

其中，当 $d_{i,j}=1$ 时 $d_{i,j}\boldsymbol{A}_{i,j}=\boldsymbol{A}_{i,j}$，当 $d_{i,j}=0$ 时 $d_{i,j}\boldsymbol{A}_{i,j}=0$(一个与 $\boldsymbol{A}_{i,j}$ 大小相同的全 0 矩阵)。称 $\boldsymbol{D}(\gamma,\rho)$ 为掩模矩阵(masking matrix)，$\boldsymbol{H}_b(\gamma,\rho)$ 为原矩阵(base matrix)，$\boldsymbol{M}_b(\gamma,\rho)$ 为掩码矩阵(masked matrix)。

不论掩模矩阵如何，若原矩阵满足 RD 约束，则掩码矩阵也满足 RD 约束，即其相应的 Tanner 图的围长至少为 6。由掩模方法构造的 LDPC 码的性能取决于掩模矩阵的选择[10]。

3　基于改进 2-D GRS 码的 QC-LDPC 码构造

3.1　基于改进 2-D GRS 码的 QC-LDPC 码广义构造

GRS 码构成了范围很广的 MDS 码[13]，其定义如下。

定义 1　设 $L=(\alpha_1,\alpha_2,\cdots,\alpha_n)=\boldsymbol{\alpha}$，其中 $\alpha_i(i=1,2,\cdots,n)$ 是 $GF(q^s)$ 中的不同元素，q 为素数，s 为正整数。$\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$ 是 $GF(q^s)$ 中的非 0 元素集合(不一定不同)，则矢量 $(v_1F(\alpha_1),v_2F(\alpha_2),\cdots,v_nF(\alpha_n))$ 的集合称为 $GF(q^s)$ 上的 $[n,k,n-k+1]$ GRS 码，记为 $GRS_k(\boldsymbol{\alpha},\boldsymbol{v})$，其中 $F(x)$ 的次数为 $(k-1)$，且系数来自 $GF(q^s)$ 的任意多项式。

文献[9]中直接在 $GF(q^s)$ 中选择 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$，由于在构造中选择的范围极大，则可能会得到译码性能较差的原矩阵。若令 $v_i=g^{-1}(\alpha_i),i=1,2,\cdots,n$，由于 $g(z)$ 为系数在 $GF(q^s)$ 上 GRS 码的 z 生成多项式，且在实际构造中选择若干行和列组成的矩阵作为原矩阵，因此可在设计中确保 $g(z)$ 不在集合 $L=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 中。于是由文献[13]可知，当码长 $n\to\infty$ 时，可获得达到沃尔沙莫夫—吉尔伯特(V-G, varshamov-gibert)限的码，即可获得性能更好的原矩阵。

于是根据 $GRS_k(\boldsymbol{\alpha},\boldsymbol{v})$ 码的定义，取多项式次数 $\partial\circ F(x)=1$，即 $k=2$，为获得性能更好的原码矩阵和简化构造复杂度，取 $v_i=g^{-1}(\alpha_i),i=1,2,\cdots,n$，其中 $g(z)$ 为系数在 $GF(q^s)$ 上的 GRS 码的 z 生成多项式。构造 $GF(q^s)$ 上的 $(q^s+1)\times n$ 维矩阵

$$\boldsymbol{W}_{GRS_2}=\begin{bmatrix} g^{-1}(\alpha_1)f_0 & g^{-1}(\alpha_2)f_0 & \cdots & g^{-1}(\alpha_n)f_0 \\ g^{-1}(\alpha_1)(\alpha_1f_1^0+f_0) & g^{-1}(\alpha_2)(\alpha_2f_1^0+f_0) & \cdots & g^{-1}(\alpha_n)(\alpha_nf_1^0+f_0) \\ \vdots & \vdots & \ddots & \vdots \\ g^{-1}(\alpha_1)(\alpha_1f_1^{q^s-2}+f_0) & g^{-1}(\alpha_2)(\alpha_2f_1^{q^s-2}+f_0) & \cdots & g^{-1}(\alpha_n)(\alpha_nf_1^{q^s-2}+f_0) \\ g^{-1}(\alpha_1)\alpha_1f_1 & g^{-1}(\alpha_2)\alpha_2f_1 & \cdots & g^{-1}(\alpha_n)\alpha_nf_1 \end{bmatrix} \tag{4}$$

其中，f_0 和 f_1 是 $GF(q^s)$ 中的 2 个非 0 元素，$f_1\neq1$，且矩阵中的 (q^s+1) 行即为 $[n,2,n-1]$ GRS 码的 (q^s+1) 个非 0 码字。

由于 L 决定了码元的位置，故又称 L 为码的位置集合。由于 $g(\alpha_i)\neq0,i=1,2,\cdots,n$，且 α_i 和 $g(z)$ 均是 $GF(q^s)$ 上的，故若 L 扩展到整个 $GF(q^s)$，则必存在一个 α_w，使 $g(\alpha_w)=0$，所以此时能得到的最长码长为 $n=q^s-1$，即为使所构造的矩阵有意义，将矩阵中含有 $g^{-1}(\alpha_w)$ 因子的一列去除。

下面证明可基于式(4)中的矩阵 $\boldsymbol{W}_{GRS_2}$ 并利用有限域方法构造 QC-LDPC 校验矩阵。

定理 1　矩阵 $\boldsymbol{W}_{GRS_2}$ 满足 α 乘积的 RD-约束。

证明　令 α 为 $GF(q^s)$ 中的一个本原域元素。

1) 矩阵 $\boldsymbol{W}_{GRS_2}$ 中的每个元素均可表示为 $\alpha^t,t=-\infty,0,1,\cdots,s$。

由于在式(4)中 f_0 和 f_1 是 $GF(q^s)$ 中的 2 个非 0 元素，且 $g(\alpha_i)\neq0,i=1,2,\cdots,n$，则矩阵 $\boldsymbol{W}_{GRS_2}$ 中第一行不存在 0 元素。

对于第 $r(2\leqslant r<q^s)$ 行，若存在 0 元素，当且仅当行中某个元素的因式满足

$$\alpha_if_1^t+f_0=2f_0,i\in\{1,2,\cdots,n\} \tag{5}$$

最后 1 行若存在 0 元素，当且仅当 $\alpha_i=\alpha^{-\infty}=0$,

$i \in \{1,2,\cdots,n\}$，即只有此时 $g^{-1}(\alpha_i)\alpha_i f_1 = 0$。

矩阵 $\boldsymbol{W}_{GRS_2}$ 中每行至多有 1 个 0 元素，则对任意的 $0 \leqslant i < q^s+1$和$0 \leqslant k,l < q-1$且$k \neq l$，$\alpha^k \boldsymbol{w}_i$ 和 $\alpha^l \boldsymbol{w}_i$ 至多有 1 个位置相同且同为 0 元素，即至少有 $(n-1)$个位置不同，其中 $\boldsymbol{w}_i$ 为矩阵 $\boldsymbol{W}_{GRS_2}$ 的任一行。

2) 令任意的 $0 \leqslant i,j < q^s+1, i \neq j$，在式(4)中 f_0 和 f_1 是 $GF(q^s)$ 中的 2 个非 0 元素，$f_1 \neq 1$，$g(z)$ 为 GRS 码的生成多项式，且 $[n,2,n-1]$ GRS 码为 MDS 码，则其中任意 2 个非 0 码字的距离至少为 $n-1$，即必然有 $n-1$ 个位置不同[13]。

根据 $\boldsymbol{W}_{GRS_2}$ 的构造过程可知，由于 $\boldsymbol{W}_{GRS_2}$ 中的 (q^s+1)行可看作为$[n,2,n-1]$ GRS码的(q^s+1)个非0码字构成的校验矩阵，于是$\boldsymbol{W}_{GRS_2}$ 中的任意 2 行 $\boldsymbol{w}_i$ 和 $\boldsymbol{w}_j$ 也至少有$(n-1)$个位置不同。又由 1)可得矩阵 $\boldsymbol{W}_{GRS_2}$ 中的每个元素均可表示为 $\alpha^t, t=-\infty,0,1,\cdots,q^s-1$，且矩阵 $\boldsymbol{W}_{GRS_2}$ 中每行至多有 1 个 0 元素，则当 $0 \leqslant k,l < q-1$且$k \neq l$ 时，$\alpha^k \boldsymbol{w}_i$ 和 $\alpha^l \boldsymbol{w}_j$ 至少有 $n-1$ 个位置不同。

综上可知，式(4)中所构造的矩阵 $\boldsymbol{W}_{GRS_2}$ 满足 α 乘积的 2 个 RD-约束。

由于将式(4)中的 $\boldsymbol{W}_{GRS_2}$ 作为构造 QC-LDPC 码的基矩阵框架，且 $\boldsymbol{W}_{GRS_2}$ 满足 α 乘积的 RD-约束，则其扩展矩阵 $\boldsymbol{H}_b(\boldsymbol{W}_{GRS_2})$ 的 Tanner 图中围长至少为 6[6,10]。因此扩展矩阵 $\boldsymbol{H}_b(\boldsymbol{W}_{GRS_2})$ 或其子矩阵就可成为校验矩阵并得到一个 QC-LDPC 码。

3.2 基于掩模方法的具体构造

虽然文献[9]提出了基于 2-D MDS 码构造 QC-LDPC 码的基本方法，但在码的具体构造中没有考虑码校验矩阵的稀疏化设计，同时也没有考虑校验矩阵的特殊结构。为构造出实用的 QC-LDPC 码，在完成校验矩阵的矩阵框架设计后，在具体构造中需要考虑 2 个方面的因素。

1) 校验矩阵具有准双对角线结构的 QC-LDPC 码具有较低的编码复杂度，因此可利用掩模设计使所构造的校验矩阵具有准双对角线结构，从而降低编码复杂度，同时加快构造速度。

2) 由于所构造QC-LDPC码的校验矩阵具有准双对角线结构，则校验矩阵的列重必含有“2”和“3”。通过大量的实验验证，为获得较好的译码性能，可适当提高校验矩阵的列重，同时，校验矩阵的行重需要确保没有较大的变化，从而充分发挥每个校验行的纠错能力。在利用掩模方法对校验矩阵进行稀疏化处理时，可适当参考对应码率的非规则码的Tanner图中变量节点和校验节点的最优度分布。

3.3 QC-LDPC 码的构造实例

例 1 利用对基矩阵的非规则掩码构造非规则 QC-LDPC 码。在本例中，构造码长为 2 268，码率为 1/2 的 QC-LDPC 码，选择 $q=2, s=6$，扩展因子 $z=63$。取 GRS 码的生成多项式 $g(z)=z^2+z+1$，α 为 $GF(2^6)$ 中的一个本原域元素，α 的本原域多项式是 x^6+x+1。

取 $f_1=\alpha$ 和 $f_0=1$，$\alpha_i (i=1,2,\cdots,64)$ 的取值集合 $L=GF(2^6)=\{0,1,\alpha,\cdots,\alpha^{62}\}$，则依据式(4)可得

$$\boldsymbol{W}_{GRS_2}=\begin{bmatrix} g^{-1}(0) & g^{-1}(1) & g^{-1}(\alpha) & \cdots & g^{-1}(\alpha^{62}) \\ g^{-1}(0) & g^{-1}(1)(1+1) & g^{-1}(\alpha)(\alpha\cdot 1+1) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}\cdot 1+1) \\ g^{-1}(0) & g^{-1}(1)(\alpha+1) & g^{-1}(\alpha)(\alpha\cdot\alpha+1) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}\cdot\alpha+1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{-1}(0) & g^{-1}(1)(\alpha^{62}+1) & g^{-1}(\alpha)(\alpha\cdot\alpha^{62}+1) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}\cdot\alpha^{62}+1) \\ 0 & g^{-1}(1)\alpha & g^{-1}(\alpha)\alpha\cdot\alpha & \cdots & g^{-1}(\alpha^{62})\alpha^{62}\cdot\alpha \end{bmatrix}$$

$$=\begin{bmatrix} g^{-1}(0) & g^{-1}(1) & g^{-1}(\alpha) & \cdots & g^{-1}(\alpha^{62}) \\ g^{-1}(0) & 0 & g^{-1}(\alpha)(\alpha+1) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}+1) \\ g^{-1}(0) & g^{-1}(1)(\alpha+1) & g^{-1}(\alpha)(\alpha^2+1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{-1}(0) & g^{-1}(1)(\alpha^{62}+1) & 0 & \cdots & g^{-1}(\alpha^{62})(\alpha^{61}+1) \\ 0 & g^{-1}(1)\alpha & g^{-1}(\alpha)\alpha^2 & \cdots & g^{-1}(\alpha^{62}) \end{bmatrix} \tag{6}$$

由于 $g(\alpha_i)\neq 0,(i=1,2,\cdots,64)$，则可知式(6)的构造方法满足定义 1 中 GRS 码的条件。利用 masking 方法构造码长为 2 268，码率为 1/2 的非规则 QC-LDPC 码。首先，从以上矩阵 $\boldsymbol{W}_{GRS_2}$ 中任意取出所要求的 18 行 36 列构成 18×36 阶矩阵 $\boldsymbol{H}_b(18,36)$ 并以此矩阵作为 masking 的原矩阵。然后，构造 $GF(2)$ 上的 18×36 阶 masking 矩阵 $\boldsymbol{D}(18,36)$，其列重和行重分布接近以下码率为 0.5 非规则码的 Tanner 图中变量节点和校验节点的度分布(节点角度)，如下

$$\lambda(X)=0.455\,4X+0.343\,3X^2+0.160\,3X^7+0.040\,9X^{29}$$

$$\rho(X)=0.100\,3X^7+0.899\,7X^8$$

其中，X^i 的系数表示度为 $i+1$ 的节点数占所有节点数的比例。

利用 $\boldsymbol{D}(18,36)$ 对原矩阵 $\boldsymbol{H}_b(18,36)$ 进行掩模，则可得 18×36 阶掩码矩阵 $\boldsymbol{M}_b(18,36)$，通过大小为 $z=63$ 的矩阵扩展即可得 $GF(2)$ 上的 $1\,134\times 2\,268$ 阶矩阵。masking 矩阵 $\boldsymbol{D}(18,36)$ 的列和行重分布如表 1 所示。于是此矩阵的零空间给出码率为 1/2 的非规则(2 268, 1 134)QC-LDPC 码。

表 1　非规则 masking 矩阵 $\boldsymbol{D}(18,36)$列和行重分布

列重分布		行重分布	
列重	列数	行重	行数
2	17	7	8
3	14	8	10
12	5		

例 2　构造码长为 2 268，码率为 2/3 的 QC-LDPC 码，所使用的参数与例 1 基本相同，不同的是，取 $f_1=\alpha$，$f_0=\alpha$，$\alpha_i(i=1,2,\cdots,64)$ 的取值集合 $L=GF(2^6)=\{0,1,\alpha,\cdots,\alpha^{62}\}$，则依据式(4)可得

$$\boldsymbol{W}_{GRS_2}=\begin{bmatrix} g^{-1}(0)\alpha & g^{-1}(1)\alpha & g^{-1}(\alpha)\alpha & \cdots & g^{-1}(\alpha^{62})\alpha \\ g^{-1}(0)\alpha & g^{-1}(1)(1+\alpha) & g^{-1}(\alpha)(\alpha\cdot 1+\alpha) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}\cdot 1+\alpha) \\ g^{-1}(0)\alpha & g^{-1}(1)(\alpha+\alpha) & g^{-1}(\alpha)(\alpha\cdot\alpha+\alpha) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}\cdot\alpha+\alpha) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{-1}(0)\alpha & g^{-1}(1)(\alpha^{62}+\alpha) & g^{-1}(\alpha)(\alpha\cdot\alpha^{62}+\alpha) & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}\cdot\alpha^{62}+\alpha) \\ 0 & g^{-1}(1)\alpha & g^{-1}(\alpha)\alpha\cdot\alpha & \cdots & g^{-1}(\alpha^{62})\alpha^{62}\cdot\alpha \end{bmatrix}$$

$$=\begin{bmatrix} g^{-1}(0)\alpha & g^{-1}(1)\alpha & g^{-1}(\alpha)\alpha & \cdots & g^{-1}(\alpha^{62})\alpha \\ g^{-1}(0)\alpha & g^{-1}(1)(1+\alpha) & 0 & \cdots & g^{-1}(\alpha^{62})(\alpha^{62}+\alpha) \\ g^{-1}(0)\alpha & 0 & g^{-1}(\alpha)(\alpha^2+\alpha) & \cdots & g^{-1}(\alpha^{62})(1+\alpha) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{-1}(0)\alpha & g^{-1}(1)(\alpha^{62}+\alpha) & g^{-1}(\alpha)(1+\alpha) & \cdots & g^{-1}(\alpha^{62})(\alpha^{61}+\alpha) \\ 0 & g^{-1}(1)\alpha & g^{-1}(\alpha)\alpha^2 & \cdots & g^{-1}(\alpha^{62}) \end{bmatrix} \tag{7}$$

构造 $GF(2)$ 上的 12×36 阶 masking 矩阵 $\boldsymbol{D}(12,36)$，其列和行重分布接近以下码率为 2/3 非规则码的度分布(节点角度)，如下

$$\lambda(X)=0.373\,1X+0.3935\,X^2+0.156\,3X^8+0.077\,1X^{31}$$

$$\rho(X)=0.172\,2X^7+0.827\,8X^8$$

masking 矩阵 $\boldsymbol{D}(12,36)$ 的列重和行重分布如表 2 所示。于是此矩阵的零空间给出码率为 2/3 的非规则(2 268, 1 512)QC-LDPC 码。

表 2　非规则 masking 矩阵 $\boldsymbol{D}(12,36)$列和行重分布

列重分布		行重分布	
列重	列数	行重	行数
2	11	11	7
3	17	12	5
8	8		

4　实验结果与讨论

利用前一部分的 2 个实例，对基于 2-D GRS 码

所构造的不同 QC-LDPC 码进行仿真。在实验中选取了不同标准中不同码率的 QC-LDPC 码与所构造的 QC-LDPC 码进行性能比较[14,15]。所有 LDPC 码的性能仿真均设置在二进制移相键控(BPSK)调制和加性高斯白噪声(AWGN)的信道条件下。在不同信噪比(SNR)条件下，使用分层 BP 译码(layered BP)算法，得到 QC-LDPC 码的误码率(BER)和误帧率(FER)，其中设置最大的迭代次数为 30 次。

为充分显示所提出方法的特性，构造了不同码率的 QC-LDPC 码。在例 1 中，利用 2-D GRS 码构造了码长为 2 268，码率为 1/2 的 QC-LDPC 码，并依据基矩阵的列重和行重分布对掩模矩阵进行设计，从而得到符合要求的 QC-LDPC 码。基于文献[9]的方法构造出了同样码长和码率的 QC-LDPC 码。在例 1 中，QC-LDPC 码的校验矩阵选取矩阵 $\boldsymbol{W}_{GRS_2}$ 中的前 18 行 36 列作为原矩阵。基于不同构造方法得到的码和标准中对应 QC-LDPC 码的译码性能曲线如图 1 所示。从图中可看出，基于所提出方法构造的 QC-LDPC 码的译码性能最优。

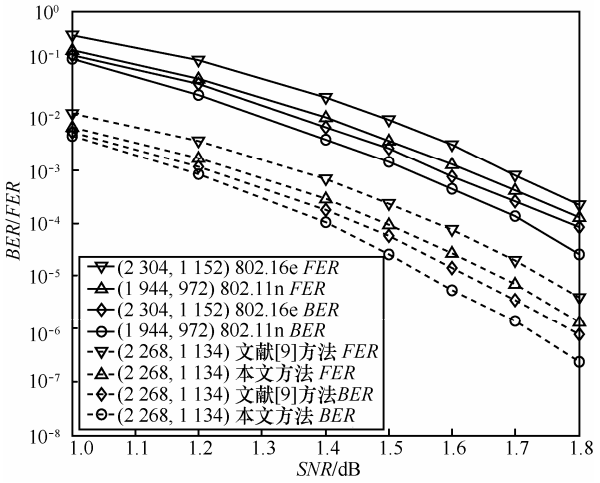


图 1 2 个构造的码率为 1/2 的 QC-LDPC 码与 IEEE 802.16e、802.11n 标准对应码率 QC-LDPC 码的性能对比

在例 2 中，利用 2-D GRS 码构造了码长为 2 268，码率为 2/3 的 QC-LDPC 码，并依据列重和行重分布设计符合要求的 QC-LDPC 码。基于文献[9]的方法构造出了同样码长和码率的 QC-LDPC 码。在例 2 中，QC-LDPC 码的校验矩阵选取矩阵 $\boldsymbol{W}_{GRS_2}$ 中最后 12 行和前 36 列作为原矩阵。基于不同构造方法得到的码和标准中对应 QC-LDPC 码的译码性能曲线如图 2 所示。从图中可看出，基于所提出方法构造的 QC-LDPC 码的译码性能最优。

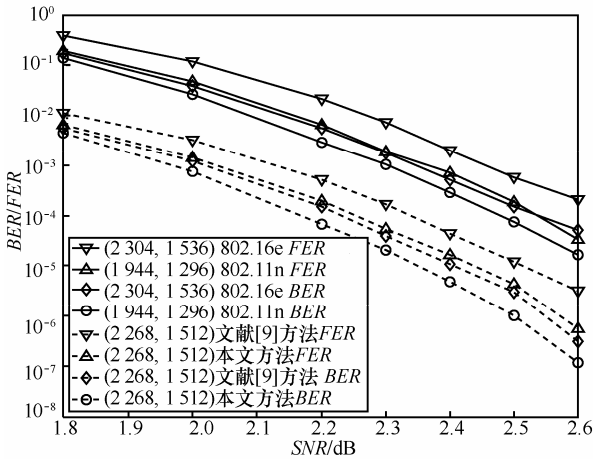


图 2 2 个构造的码率为 2/3 的 QC-LDPC 码与 IEEE 802.16e、802.11n 标准对应码率 QC-LDPC 码的性能对比

在进行 QC-LDPC 码校验矩阵的设计和实验中可知，基于 2-D GRS 码可简单而有效地构造性能优异的 QC-LDPC 码。这种基于有限域的方法可使所构造的校验矩阵的原矩阵首先具有无 4 环的特性，同时通过对掩模矩阵的优化设计使所构造的校验矩阵具有准双对角线结构，降低编码复杂度。

5 结束语

本文提出了基于 2-D GRS 码构造 QC-LDPC 码校验矩阵的方法，并对所构造的 QC-LDPC 码进行了仿真和分析。该方法利用有限域理论和 2-D GRS 码设计出 QC-LDPC 码校验矩阵的矩阵框架并满足 α 乘积的 RD 约束，从而确保原矩阵对应 Tanner 图的围长至少为 6。利用掩模技术对所构造的原矩阵进行优化设计，确保所构造 QC-LDPC 码校验矩阵具有准双对角线结构，并可依据优化设计的相应码率的非规则码对应 Tanner 图中的变量节点和校验节点的度分布指导掩模矩阵的优化设计。本文利用 2-D GRS 码构造出了不同码率的 QC- LDPC 码，并与不同的 QC-LDPC 码进行了实验仿真对比。实验结果表明，所构造 QC-LDPC 码的译码性能优于其他 QC-LDPC 码。

参考文献：

[1] CHUNG S Y, FORNEY G D, RICHARDSON T J. On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit[J]. IEEE Commun Lett, 2001, 5(1): 58-60.

[2] MOHAMMAD M M. A turbo-decoding message-passing algorithm for sparse parity-check matrix codes[J]. IEEE Trans Signal Processing, 2006, 54(11): 4376-4392.

[3] RYAN W E, LIN S. Channel Codes: Classical and Modern[M]. Cambridge University Press, 2009.

[4] RICHARDSON T J, SHOKROLLAHI A, URBANKE R. Design of capacity approaching irregular low-density parity-check codes[J]. IEEE Trans Inform Theory, 2001, 47(1): 619-637.

[5] KOU Y, LIN S, FOSSORIER M P C. Low-density parity-check codes based on finite geometries: a rediscovery and new results[J]. IEEE Trans Inf Theory, 2001, 47(1): 2711-2736.

[6] LAN L, ZENGL Q, TAI Y Y. Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach[J]. IEEE Trans Inf Theory, 2007, 53(7): 2429-2458.

[7] KAMIYA N, SASAKI E. Efficient encoding of QC-LDPC codes related to cyclic MDS codes[J]. IEEE J Sel Areas Communication, 2009, 27(6): 846-854.

[8] KAMIYA N, SASAKI E. Efficiently encodable irregular QC-LDPC codes constructed from self-reciprocal generator polynomials of MDS codes[J]. IEEE Commun Lett, 2010, 14(9): 860-862.

[9] CHEN C, BAI B, WANG X M. Construction of quasi-cyclic LDPC codes based on a two-dimensional MDS code[J]. IEEE Commun Lett, 2010, 14(5): 447-449.

[10] KANG J, HUANG Q. Quasi-cyclic LDPC codes: an algebraic construction[J]. IEEE Trans Communication, 2010, 58(5):1383-1396.

[11] MYUNG S, YANG K, KIM J. Quasi-cyclic LDPC codes for fast encoding[J]. IEEE Trans Information Theory, 2005, 51(8): 2894-2901.

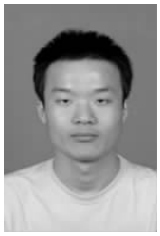
[12] TAM W M, LAU C M, CHI K T. A class of QC-LDPC codes with low encoding complexity and good error performance[J]. IEEE Commun Lett, 2010, 14(2):169-171.

[13] MACWILLIAMS F J, SLOANE N J A. The Theory of Error-Correcting Codes[M]. New York: North Holland, 1977.

[14] IEEE Standard for Local and Metropolitan Area Network Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems[S]. IEEE P802.16e/2009, 2009.

[15] IEEE Standard for Information Technology Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications Amendment 5: Enhancements for Higher Throughput[S]. IEEE P802.11n/2009, 2009.

作者简介：



赵明（1987-），男，安徽巢湖人，北京航空航天大学博士生，主要研究方向为通信系统设计、信息论、信道编解码理论、FPGA 设计和数字 SoC 设计等。

张晓林（1952-），男，北京人，北京航空航天大学教授、博士生导师，主要研究方向为信息传输与处理、飞行器通信与电子系统、集成电路 SoC 设计等。