可逆 QC-LDPC 码的构造及其在水声通信系统中的性能

戚肖克* 李 宇 黄海宁
(中国科学院声学研究所 北京 100190)

摘 要：该文提出一种通过合理设置零矩阵构造可逆准循环低密度奇偶校验码(QC-LDPC)的方法，解决了传统 QC-LDPC 码校验矩阵不满秩及编码复杂度高的问题。将循环矩阵对应于有限域中的多项式，利用扩展的欧几里德算法构造可逆校验矩阵，克服了传统 QC-LDPC 码码率大于设计码率的问题。编码时先将校验矩阵分块，然后利用扩展欧几里德算法回溯求解循环矩阵的逆矩阵，显著降低了编码复杂度。EXIT 图证明了译码器的收敛性。仿真表明短码时纠错性能优于随机 LDPC 码，适用于水声通信系统。另外，将可逆 QC-LDPC 码应用于 ZP-OFDM 系统的仿真表明 QC-LDPC 码能较大地提高水下通信系统的鲁棒性。

关键词：信道编码；准循环低密度奇偶校验码；循环矩阵；水声通信；零填充正交频分复用系统
中图分类号：TN911.22 **文献标识码**： A **文章编号**：1009-5896(2012)08-1986-07
DOI: 10.3724/SP.J.1146.2011.01373

Construction of Reversible QC-LDPC Codes and Its Performance in Underwater Acoustic Communication System

Qi Xiao-ke Li Yu Huang Hai-ning
(*Institute of Acoustics, Chinese Academy of Sciences, Beijing* 100190, *China*)

Abstract: A construction scheme of reversible Quasi Cyclic-Low Density Parity Check (QC-LDPC) codes is proposed by setting rationally zero matrices. This solves the problems of singular check matrix and high encoding complexity in conventional QC-LDPC codes. With circulant matrix corresponding to polynomial in finite fields, the scheme exploits the extended version of Euclid's algorithm to conquer the problem of QC-LDPC construction rate lager than design rate. Moreover, in the encoding process, first dividing the check matrix into blocks, and then the extended version of Euclid's algorithm is used to invert a circulant matrix, it results in dynamic complexity decrease. EXtrinsic Information Transfer (EXIT) chart implies the convergence of decoder. More simulations illustrate that the performance of the proposed construction structure is better than random LDPC when the code length is short, which is suitable for UnderWater Acoustic Communication (UWAC). Finally, applying QC-LDPC to Zero Padding-Orthogonal Frequency Division Multiplexing (ZP-OFDM) for evaluating the performance in UWAC, extended simulation shows that the reversible QC-LDPC codes can dynamically improve the system robustness.

Key words: Channel coding; Quasi Cyclic-Low Density Parity Check (QC-LDPC) codes; Circulant matrix; Under Water Acoustic Communication (UWAC); Zero padding OFDM(ZP- OFDM) system

1 引言

信道编码是提高系统可靠性的一种方法，在通信系统中占有重要的地位。低密度奇偶校验(Low-Density Parity-Check, LDPC)码是由文献[1]提出的一种特殊的线性分组码，文献[2]发现 LDPC 长码可获得与 Turbo 码近似的误码性能并提出了置信传播译码算法后，成为编码领域的热点。与其它编码方式相比，LDPC 码有对相关衰落的衰落速度不敏感、自交织性良好、译码方法简单、合理构造校验矩阵时误码平台较低等特性。

根据构造校验矩阵的方式不同，LDPC 码分为随机 LDPC 码和结构化 LDPC 码。随机 LDPC 码校验矩阵由计算机搜索构成，具有的随机特性使编码复杂度过高，硬件实现困难；结构化 LDPC 码校验矩阵遵循一定的结构构成，在编码复杂度、存储空间等方面存在显著优势，并且在中短码长下，其纠错性能甚至能超过随机 LDPC 码[3,4]，因此近年来结构化 LDPC 码受到越来越多的重视。

准循环(Quasi-Cyclic, QC)LDPC 码是结构化

2011-12-26 收到，2012-04-18 改回
国家 863 计划项目(2006AA09Z117, 2009AA093601)和国家自然科学基金(60672118, 10904160)资助课题
*通信作者：戚肖克 qixiaoke09@mails.gucas.ac.cn

LDPC 码的一种，其校验矩阵由多个置换矩阵构成，有构造简单、易消去短环等优点，吸引了众多学者进行研究[3−10]。为降低编码复杂度，一般将 QC 校验矩阵构造为近似上三角的结构形式，如双对角结构[8]、三角结构加双对角结构[9]、三对角结构[10]等，但是这些方法对置换矩阵的维数有限制，并且当码率较低时，校验矩阵中低度数节点过多，造成码的纠错性能变差。

本文提出了一种适用于高低码率情况的可逆 QC-LDPC 码校验矩阵构造方式，通过合理设置零矩阵构造不规则 QC-LDPC 码。编码时将循环矩阵的逆矩阵求解问题转化为有限域多项式求逆运算[11,12]，利用扩展的欧几里德算法，降低了编码复杂度。经外部信息转移图(EXtrinsic Information Transfer chart, EXIT chart)分析，本文提出的构造方式可使译码器达到收敛。仿真表明，在中短码长下其误码性能略优于随机 LDPC 码。为评估提出的 QC-LDPC 码在水声通信中的性能，采用从海试数据中获得的信道作为通信信道，将 QC-LDPC 码用于零填充正交频分复用(Zero Padding-Orthogonal Frequency Division Multiplexing, ZP-OFDM)系统进行仿真，结果表明 QC-LDPC 码能显著提高水下通信系统的鲁棒性。

2　LDPC 码

根据构造校验矩阵的方式不同，LDPC 码分为随机 LDPC 码和结构化 LDPC 码。随机 LDPC 码的校验矩阵没有一定结构，在硬件实现中将产生以下问题：

(1)编码复杂度高，无法进行实时传输；

(2)接收端必须存储与编码端相同的校验矩阵才能进行解码，码长越长需要的存储空间就越大，有可能超出数据空间范围；

(3)较难进行变码率编码，因为变码率编码意味着要存储多个校验矩阵，实现代价太大。

因此，期望通过结构化的 LDPC 码解决以上问题。QC-LDPC 码是一种由置换矩阵组成的结构化 LDPC 码，它的校验矩阵具有准循环结构，在构造中容易去除短环，硬件实现简单，可对码长和码率进行实时控制，并且接收端只需要几个参数(如码率、行重及码长)就可以构造出与发送端相同的校验矩阵，节省了存储空间。

2.1 QC-LDPC 码概述

码长为 N、校验位长为 M、行重和列重分别为 L 和 J 的 QC-LDPC 码校验矩阵 $\boldsymbol{H}$ 的结构如式(1)所示。

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{I}(p_{1,1}) & \boldsymbol{I}(p_{1,2}) & \cdots & \boldsymbol{I}(p_{1,L})\\ \boldsymbol{I}(p_{2,1}) & \boldsymbol{I}(p_{2,2}) & \cdots & \boldsymbol{I}(p_{2,L})\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{I}(p_{J,1}) & \boldsymbol{I}(p_{J,2}) & \cdots & \boldsymbol{I}(p_{J,L})\end{bmatrix} \tag{1}$$

式中 $\boldsymbol{I}$ 为 P 阶单位矩阵，$\boldsymbol{I}(p_{j,l})$ 为 $\boldsymbol{I}$ 循环右移 $p_{j,l}$ 后的置换矩阵，$P=M/J=N/L$。

LDPC 码的解码器采用基于 Tanner 图消息传递的和积译码算法，短环将严重影响解码器的性能，因此，Tanner 图中的最小环长要尽可能大。由文献[3]可知，若定义 $\Delta_{j_x,j_y}(l)=p_{j_x,l}-p_{j_y,l}$，则环长至少为 $2c$ 的充分必要条件为

$$\sum_{k=0}^{m-1}\Delta_{j_k,j_{k+1}}(l_k)\neq 0 \pmod{P} \tag{2}$$

式中 $2\le m\le c-1$，$1\le j_k,j_{k+1}\le J$，$1\le l_k\le L$，且 $j_0=j_m$，$j_k\neq j_{k+1}$，$l_k\neq l_{k+1}$。

因此要得到设定的最小环长，矩阵偏移量 $p_{j,l}$ 需满足式(2)。

准循环结构的校验矩阵解决了随机 LDPC 码的校验矩阵存储的问题，并且可以实时生成校验矩阵、控制码长和码率，但是仍有以下问题：

(1)编码码率不固定　由置换矩阵构成的校验矩阵的秩 $\mathrm{rank}(\boldsymbol{H})\le M-J+1$，因此编码后的实际码率 $R'=1-\mathrm{rank}(\boldsymbol{H})/N$，大于设定码率 $R=1-M/N$，给系统设计带来困难；

(2)没有从根本上解决编码复杂度高的问题

本文提出一种新的可逆校验矩阵的构造方法，在保持各块矩阵循环特性及码字特性的前提下合理设置零矩阵的位置，构造出可逆的校验矩阵，使编码码率等于设计码率。编码过程中，利用校验矩阵的特殊结构及扩展的欧几里德算法显著降低了编码复杂度。

2.2 本文提出的 QC-LDPC 构造方式

本文提出的列重为 3、行重为 L 的不规则 QC-LDPC 码的校验矩阵的结构如式(3)所示。

$$\boldsymbol{H}_c=\left[\begin{array}{ccc:ccc}\boldsymbol{I} & \boldsymbol{0} & \boldsymbol{I}(p_{1,3}) & \boldsymbol{I}(p_{1,4}) & \cdots & \boldsymbol{I}(p_{1,L})\\ \boldsymbol{0} & \boldsymbol{I} & \boldsymbol{I}(p_{2,3}) & \boldsymbol{I}(p_{2,4}) & \cdots & \boldsymbol{I}(p_{2,L})\\ \boldsymbol{I} & \boldsymbol{I}(p_{3,2}) & \boldsymbol{I}(p_{3,3}) & \boldsymbol{I}(p_{3,4}) & \cdots & \boldsymbol{I}(p_{3,L})\end{array}\right] \tag{3}$$

由于初等行变换不改变矩阵的零空间，因此将校验矩阵的每行的第 1 个非零块设为单位矩阵不会对码字产生影响。对式(3)进行块高斯消去，得到式(4)：

$$\boldsymbol{H}_c^{'}=\left[\begin{array}{ccc:ccc} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{I}(p_{1,3}) & \boldsymbol{I}(p_{1,4}) & \cdots & \boldsymbol{I}(p_{1,L}) \\ \boldsymbol{0} & \boldsymbol{I} & \boldsymbol{I}(p_{2,3}) & \boldsymbol{I}(p_{2,4}) & \cdots & \boldsymbol{I}(p_{2,L}) \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}(p_{3,3}^{'}) & \boldsymbol{I}(p_{3,4}^{'}) & \cdots & \boldsymbol{I}(p_{3,L}^{'}) \end{array}\right] \tag{4}$$

式中 $\boldsymbol{I}(p_{3,l}^{'})=\boldsymbol{I}(p_{3,l})+\boldsymbol{I}(p_{1,l})+\boldsymbol{I}((p_{2,l}+p_{3,2})\bmod P)$，$l=3,4,\cdots,L$。

由于 $\boldsymbol{I}(p_{j,l})$ 为置换矩阵，因此 $\boldsymbol{I}(p_{3,l}^{'})$ 为循环矩阵，于是，校验矩阵的行满秩问题转化为 P 阶循环矩阵 $\boldsymbol{I}(p_{3,3}^{'})$ 的可逆性问题。将循环矩阵 $\boldsymbol{I}(p_{3,3}^{'})$ 对应于域 F_2 上的多项式

$$f(x)=\sum_{i=0}^{P-1}a_i x^i \tag{5}$$

式中，当 $i=p_{3,3},p_{1,3},((p_{2,3}+p_{3,2})\bmod P)$ 时，$a_i=1$，否则，$a_i=0$。当满足 $f(x)$ 与 x^P-1 互质，即 $\gcd(f(x),\,x^P-1)=1$ 时，$f(x)$ 对应的循环矩阵是可逆的[11,12]，式中，$\gcd(\bullet)$ 表示最大公因式。求解两个多项式的最大公因式可采用扩展的欧几里德算法，若最大公因式为 1，则表示 $f(x)$ 对应的循环矩阵是可逆的；否则，循环矩阵是奇异的。

扩展欧几里德算法通过一系列除法建立除式与余式之间的关系，首次除法用开始的两个因式分别作为被除式和除式，然后将除式作为下次计算的被除式，余式作为下次计算的除式，最终以余式为 0 结束，最后一次运算的除式即为两个多项式的最大公因式。例如，首行为[1 0 1 0 1]的循环矩阵 $\boldsymbol{Q}$，对应 F_2 上的多项式 $f(x)=1+x^2+x^4$，采用扩展欧几里德算法求 $\gcd(f(x),x^5-1)$ 有

$$x^5-1=x(x^4+x^2+1)+x^3+x+1=xf(x)+r_1(x) \tag{6}$$

$$f(x)=x(x^3+x+1)+x+1=xr_1(x)+r_2(x) \tag{7}$$

$$r_1(x)=(x^2+x)(x+1)+1=(x^2+x)r_2(x)+r_3(x) \tag{8}$$

$$r_2(x)=(x+1)+0=(x+1)r_3(x)+0 \tag{9}$$

由式(9)知，$\gcd(f(x),x^5-1)=r_3(x)=1$，表明循环矩阵 $\boldsymbol{Q}$ 是可逆的。

综上所述，构造可逆 QC-LDPC 码校验矩阵的流程为：

(1)初始化：码率 R，信息位长 K，最小环长 g；

(2)计算其它参数：码长 $N=K/R$，校验位长 $M=N-K$，行重 $L=3/(1-R)$，置换矩阵维数 $P=N/L$；

(3)选择满足式(2)的偏移量 $p_{3,3}$，$p_{1,3}$，$p_{2,3}$ 和 $p_{3,2}$；

(4)根据式(5)计算 $f(x)$，采用扩展的欧几里德算法求解 $\gcd(f(x),x^P-1)$，如果结果不为 1，则返回步骤(3)；

(5)选择满足式(2)的其它偏移量 $p_{j,l}$，其中 $j=1,2,3$，$4\le l\le L$；

(6)按照式(3)构造校验矩阵。

2.3 快速编码算法

传统 LDPC 码编码时首先利用高斯消去法将校验矩阵转化为系统生成矩阵，然后进行编码，分别需要 $O(N^3)$ 和 $O(N^2)$ 的计算复杂度[4]，复杂度较高。文献[13]中的算法将随机 LDPC 编码的复杂度降为 $O(N+h^2)$，但是该方法存在几个问题：(1) h 依赖于特定的校验矩阵，当 h 较大时，复杂度渐近于传统编码复杂度；(2)编码前先将矩阵进行行列置换，增加了复杂度；(3)中间计算时用了 3 次串行编码，延长了处理过程。本文基于文献[13]的思想并利用提出的 QC-LDPC 码校验矩阵的特殊性进行并行编码，不需要行列变换，显著降低了复杂度。

为进行快速编码，首先将校验矩阵 $\boldsymbol{H}_c^{'}$ 按照式(10)的形式分块：

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{A} & \boldsymbol{B} & \boldsymbol{T}\\ \boldsymbol{0} & \boldsymbol{D} & \boldsymbol{E}\end{bmatrix} \tag{10}$$

式(10)中 $\boldsymbol{A}$ 为 $2P$ 阶单位矩阵，$\boldsymbol{B}=\begin{bmatrix}\boldsymbol{I}(p_{1,3})\\ \boldsymbol{I}(p_{2,3})\end{bmatrix}$ 为 $2P\times P$ 矩阵，$\boldsymbol{T}=\begin{bmatrix}\boldsymbol{I}(p_{1,4}) & \cdots & \boldsymbol{I}(p_{1,L})\\ \boldsymbol{I}(p_{2,4}) & \cdots & \boldsymbol{I}(p_{2,L})\end{bmatrix}$ 为 $2P\times(J-3)P$ 矩阵，$\boldsymbol{D}=\boldsymbol{I}(p_{3,3}^{'})$ 为 P 阶循环矩阵，$\boldsymbol{E}=[\boldsymbol{I}(p_{3,4}^{'})\ \cdots\ \boldsymbol{I}(p_{3,L}^{'})]$ 为 $P\times(L-3)P$ 矩阵。

设经 LDPC 编码后的码字为 $\boldsymbol{c}=[\boldsymbol{p}_2,\boldsymbol{p}_1,\boldsymbol{s}]$，其中，$\boldsymbol{s}$ 为长度为 K 的信息位，$\boldsymbol{p}_2$ 和 $\boldsymbol{p}_1$ 分别为长度 $2P$ 和 P 的校验位，则有

$$\boldsymbol{H}\boldsymbol{c}^{\mathrm{T}}=\boldsymbol{0} \tag{11}$$

将式(11)分成两个方程

$$\boldsymbol{A}\boldsymbol{p}_2^{\mathrm{T}}+\boldsymbol{B}\boldsymbol{p}_1^{\mathrm{T}}+\boldsymbol{T}\boldsymbol{s}^{\mathrm{T}}=\boldsymbol{0} \tag{12}$$

$$\boldsymbol{D}\boldsymbol{p}_1^{\mathrm{T}}+\boldsymbol{E}\boldsymbol{s}^{\mathrm{T}}=\boldsymbol{0} \tag{13}$$

由式(12)与式(13)中可得

$$\boldsymbol{p}_1^{\mathrm{T}}=\boldsymbol{D}^{-1}\boldsymbol{E}\boldsymbol{s}^{\mathrm{T}} \tag{14}$$

$$\boldsymbol{p}_2^{\mathrm{T}}=\boldsymbol{A}^{-1}(\boldsymbol{B}\boldsymbol{p}_1^{\mathrm{T}}+\boldsymbol{T}\boldsymbol{s}^{\mathrm{T}})=\boldsymbol{B}\boldsymbol{p}_1^{\mathrm{T}}+\boldsymbol{T}\boldsymbol{s}^{\mathrm{T}} \tag{15}$$

因为循环矩阵的逆矩阵仍为循环矩阵，所以当 $\boldsymbol{D}$ 为循环矩阵时 $\boldsymbol{D}^{-1}$ 也为循环矩阵。由 2.2 节的分析可知，求 $\boldsymbol{D}^{-1}$ 等价于求解 F_2 上的多项式 $g(x)=\sum_{i=0}^{P-1}b_i x^i$，使得 $f(x)g(x)\equiv 1\,(\bmod\, x^P-1)$，式中的 $g(x)$ 可通过回溯扩展的欧几里德算法[11]得到，进而得到相应的逆矩阵 $\boldsymbol{D}^{-1}$。

综上所述，当校验矩阵有式(3)的形式时，QC-LDPC 的编码算法如下：

(1)将 2.2 节的步骤(4)的算法回溯，得到 $\boldsymbol{D}^{-1}$；

(2)通过式(14)计算 $\boldsymbol{p}_1$，通过式(15)计算 $\boldsymbol{p}_2$；

(3)得到编码码字 $\boldsymbol{c}=[\boldsymbol{p}_2,\boldsymbol{p}_1,\boldsymbol{s}]$。

由于 $\boldsymbol{D}^{-1}$ 的度最大为 $P-1$，因此计算 $\boldsymbol{p}_1$ 最多需 $P(P-1+3(L-3))$ 次异或运算，而计算 $\boldsymbol{p}_2$ 需 $2P(L-2)$ 次异或运算，因此整个编码过程最多需要 $P(P+5L-14)$ 次异或运算，另外，异或运算可通过位操作代替，编码复杂度显著降低。

接收端 QC-LDPC 译码器采用有近似最优性能的基于置信传播的迭代和积译码算法[14]，仅有线性复杂度。

3　性能仿真及分析

3.1 复杂度对比分析

首先分析算法的时间复杂度。根据 LDPC 码编码的过程，对构造校验矩阵和编码过程的时间复杂度依次进行对比分析。为对各算法复杂度有直观的认识，本文采用从算法运行时间上对比复杂度的方法。各算法的性能值均在 CPU 为 Pentium(R) E5500 的计算机上，用 Matlab7.9.0(R2009b)仿真获得，时间为运行 100 次的平均时间。

图 1 对比了码率为 1/2 时随机 LDPC 码与本文提出的 QC-LDPC 码构造校验矩阵时的用时情况。可以看出，随机码构造校验矩阵时所用时间与码长的 3 次方成正比，远高于 QC 码构造校验矩阵所用时间。这是因为随机码在去除 4 线循环时，需要将每列中 1 的位置与其它列进行比较，时间复杂度为 $O(N^3)$，而 QC 码利用校验矩阵的结构可简单去除 4 线循环，所用时间仅与置换矩阵块数及计算 P 维循环矩阵可逆性时的除法次数有关，复杂度为 $O(P\log P\log P)$。从图 1 中可知，各算法的用时变化趋势与理论曲线相拟合。

图 2 对比了码率为 1/2 时传统编码算法、文献[13]编码算法与本文提出的 QC-LDPC 快速编码算法的用时情况。可以看出，相同码长下，3 种编码算法用时依次降低。传统编码算法所用时间约与码长的 3 次方成正比，这与理论中校验矩阵变为生成矩阵 $O(N^3)$ 的复杂度，编码 $O(N^2)$ 的复杂度相符合。文献[13]算法所用时间约为平方增长，这是因为虽然文献[13]的编码复杂度为 $O(N+h^2)$，但预处理过程中的行列置换复杂度为 $O(N^{3/2})$ [13]，所以整个编码过程复杂度高于 $O(N^{3/2})$，与 $O(N^2)$ 接近。本文算法用时低于其它两个算法，主要是因为 QC 码的校验矩阵具有特定的结构，编码过程可利用循环结构进行控制及简化。

最后，对随机 LDPC 码和本文提出的 QC-LDPC 码算法的空间复杂度进行对比。随机码需要对校验矩阵中的每个元素进行处理，如去 4 线循环、编码等，空间复杂度为 $O(JLP^2)$，而本文算法仅需知道置换矩阵块的偏移量，空间复杂度为 $O(JL)$，因此本文算法的空间复杂度远远低于随机码，这是因为 QC 码是一种结构化的码，可以根据几个参数推测出整个矩阵。

3.2 QC-LDPC 码在高斯白噪声信道中的性能

首先采用 EXIT 图分析本文提出的 QC-LDPC 构造方法的译码器的收敛性。EXIT 图从互信息的角度分析译码器的收敛性，将变量节点与校验节点之间的信息传递看成多个变量节点译码器(Variable Nodes Decoder, VND)与校验节点译码器(Check Nodes Decoder, CND)之间的信息传递。图 3 为码率 1/2 信噪比分别为 1 dB 和 1.5 dB 时 QC-LDPC 的 EXIT 图，其中 $I_{A,\mathrm{VND}}$ ($I_{A,\mathrm{CND}}$)表示 VND(CND)从 CND(VND)中获得的互信息，$I_{E,\mathrm{VND}}$ ($I_{E,\mathrm{CND}}$)表示 VND(CND)输出的附加互信息，由于两个译码器之间的信息相互传递，因此，$I_{A,\mathrm{VND}}=I_{E,\mathrm{CND}}$, $I_{E,\mathrm{VND}}=I_{A,\mathrm{CND}}$。从图 3 可以看出，信噪比为 1 dB 时，曲线相交于纵坐标 0.74，小于 1，说明译码器不能完全

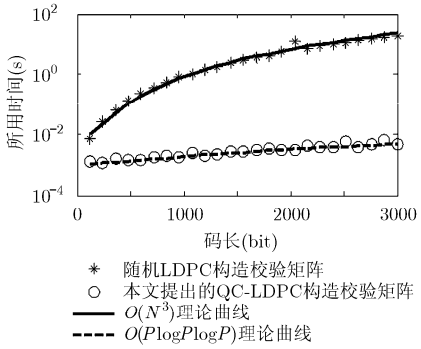


图 1 各算法构造校验矩阵用时对比

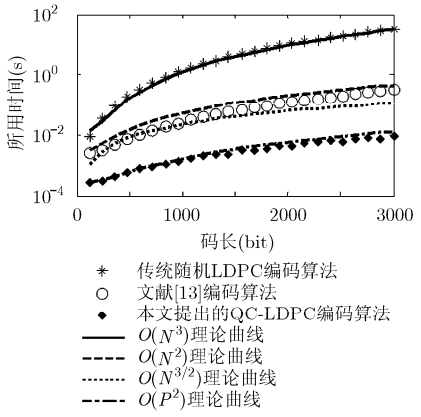
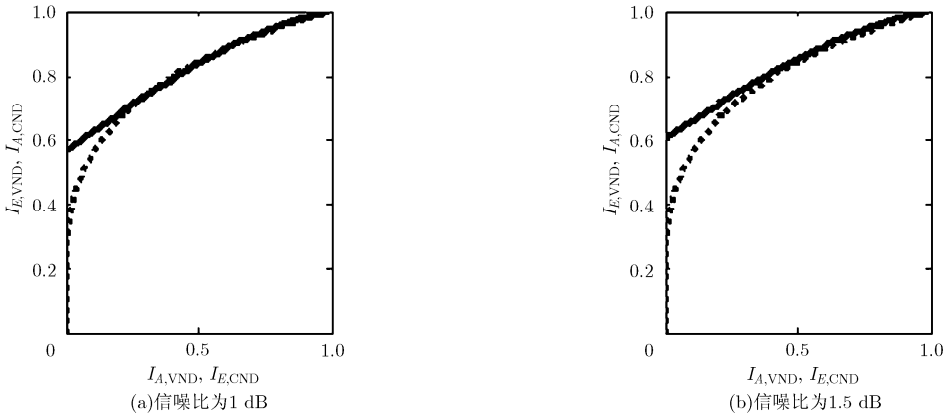


图 2 各算法编码用时对比



(a)信噪比为1 dB (b)信噪比为1.5 dB

图 3 码率 1/2 时提出 QC-LDPC 码的 EXIT 图

正确译码；信噪比为 1.5 dB 时，曲线相交于纵坐标 1，说明 1.5 dB 时译码器已达到收敛，多次迭代后可以完全正确译码，因此本文构造的码为好码。

图 4，图 5 仿真了高斯白噪声信道下本文提出的 QC-LDPC 码和随机 LDPC 码的纠错性能对比。图 4 仿真参数为码率 1/2，码长 240 bit 和 768 bit，可以看出，相同码长下本文提出的 QC 码的纠错性能略优于随机码，在误码率为 10^{-5} 时，码长为 240 的 QC 码优于随机码约 0.17 dB，码长为 768 的 QC 码优于随机码约 0.09 dB。图 5 仿真参数为码率 2/3，码长 810 bit，可以看出，信噪比小于 2.5 dB 时，本文提出的 QC 码纠错性能略优于随机码，信噪比更高时，本文提出的 QC 码纠错性能的优势较为明显，在误码率为 10^{-5} 时，优于随机码约 0.2 dB。更多的仿真表明，当码字较短时，本文提出的 QC 码性能优于随机码；当码字变长时，本文提出的 QC 码的性能渐渐与随机码的性能相当；当码字更长时，QC 码受本身最小汉明距离的限制，性能不如随机码。

3.3 LDPC-OFDM 系统在水声信道中的性能

为评估 QC-LDPC 码在水声通信中的系统性能，将本文提出的 QC-LDPC 编码方法应用于 ZP-OFDM 系统在水声信道中传输，这里的水声信道从 2010 年的海试数据中处理获得，试验中收发换能器相距 1 km，均位于水下 10 m 处，收发换能器上方分别固定在收发船上，收发船静止，此时，多普勒效应由收发换能器随水流晃动、海面的风浪、时钟的漂移等引入。从海试数据中处理获得的水声信道的多径径数为 2~7 条，为了平均多径对数据的影响，选择图 6 所示的信道作为仿真用的水声信道，其中横坐标表示数据在信道中延时的符号数，纵坐标表示信道冲激响应 $h(t)$ 的幅度，可以看出信道中能量较高的多径径数为 4 条，符号延时较长。另外，为仿真水声信道中的多普勒效应，在信道中加入了均匀分布的随机载波频率偏移。

LDPC-OFDM 系统的各参数如表 1 所示。

接收端采用文献[15]中的最小二乘算法进行信道估计及载波频率偏移(Carrier Frequency Offset,

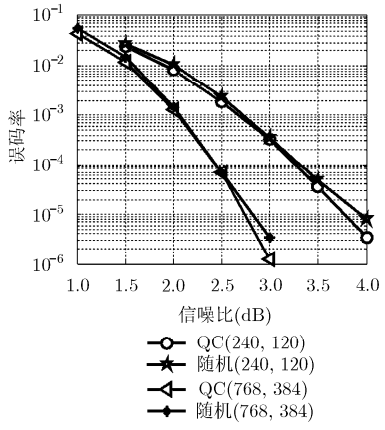


图 4 码率为 1/2 时 QC-LDPC 与随机 LDPC 码性能对比

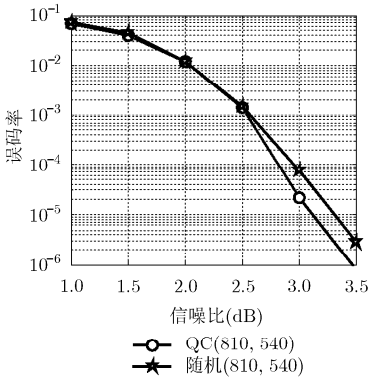


图 5 码率为 2/3 时 QC-LDPC 与随机 LDPC 码性能对比

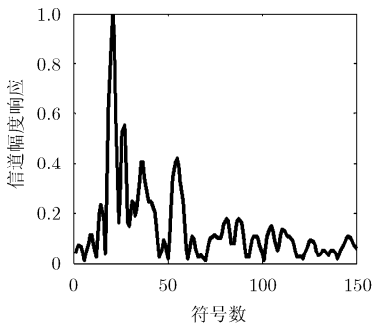


图 6 仿真用的浅海水声信道

表 1 仿真参数

OFDM 数据长度	1024
保护间隔	600
导频符号数	256
调制方式	QPSK
信道编码方式	本文的 QC-LDPC 码
编码码率	2/3, 1/2
码长	768

CFO)估计。具体方法为：首先利用已知的导频符号根据最小二乘准则估计信道，然后在一定频率范围内对最小二乘拟合误差进行 1 维搜索，误差最小时对应的频率即为估计的 CFO。对数据进行 CFO 估计及校正后，先采用迫零均衡器对数据进行均衡，然后进行 QC-LDPC 解码，得到系统的误码性能如图 7 所示。

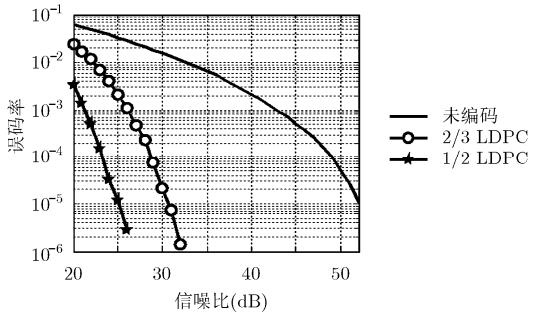


图 7 不同情况下的接收性能对比

由图 7 可知，未编码 OFDM 系统误码率降到 10^{-5} 时需要的信噪比为 52 dB。与高斯白噪声信道下的结果相比，未编码 OFDM 系统性能较差，原因有以下几点：(1)浅海信道中较为严重的多径、较长的传播延时以及多普勒效应严重影响了接收性能；(2)接收端采用的迫零均衡器对噪声有放大作用；(3)OFDM 调制的频率分集数为 1，即若信道在某一子载波频率处存在零值，OFDM 系统将无法恢复出此子载波上的数据。2/3 码率和 1/2 码率编码的 OFDM 系统在误码率为 10^{-5} 时，所需的信噪比分别为 30.8 dB 和 25.2 dB，对比未编码系统分别获得了 21.2 dB 和 26.8 dB 的增益，1/2 码率编码的系统对比 2/3 码率编码的系统有 5.6 dB 的增益，因此，采用 QC-LDPC 编码可以大幅改善系统的误码性能，提高系统的鲁棒性，这是因为编码的 OFDM 系统的频率分集数增加，改善了系统性能，另外，编码增加的冗余信息也提高了系统的可靠性。

4 结论

本文提出了一种低复杂度的可逆 QC-LDPC 码校验矩阵的构造方式，克服了传统 LDPC 码的几个问题：(1)随机 LDPC 码校验矩阵使用不灵活，接收端必须存储与发送端相同的校验矩阵才能正确解码，不能满足自适应码长码率控制等要求；(2)QC-LDPC 码校验矩阵不满秩，致使实际构造码率大于设计码率，为系统设计带来困难；(3)编码复杂度过高。

本文提出的构造方式通过合理设置零矩阵构造可逆的校验矩阵，利用循环矩阵与有限域多项式的关系，采用扩展的欧几里德算法判断矩阵的可逆性并求解逆矩阵，降低了编码复杂度，接收端只需几个参数就可生成与编码端相同的校验矩阵，节省了大量存储空间。

对本文提出的可逆 QC-LDPC 码算法的复杂度进行了分析，结果表明，提出的算法与传统随机码算法及文献[13]的算法相比，时间复杂度和空间复杂度都大大降低。EXIT 图证明了该构造方式的译码器的收敛性。对性能的仿真表明，短码长时构造的 QC-LDPC 码性能优于随机 LDPC 码，随着码长增长，QC-LDPC 码受本身最小汉明距离特性的限制，性能渐渐劣于随机 LDPC 码。考虑到在水声通信中，每次传输数据较短，采用这种码是合适的。

将 QC-LDPC 码应用于 ZP-OFDM 系统，经过水声信道(对海试数据处理获得)的仿真结果表明：采用 QC-LDPC 编码提高了 ZP-OFDM 系统的性能及鲁棒性，在误码率为 10^{-5} 时，2/3, 1/2 码率编码的 OFDM 系统对比未编码 OFDM 系统分别获得了 21.2 dB 和 26.8 dB 的信噪比增益。但是编码系统的性能增益以降低通信速率为代价，且码率越低，性能增益越高，代价越大。在实际系统设计中应在性能与通信速率之间取折中。

参 考 文 献

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

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

[3] Fossorier M P C. Quasi cyclic low-density parity-check codes from circulant permutation matrices[J]. *IEEE Transactions on Information Theory*, 2004, 50(8): 1788–1793.

[4] Tanner R M, Sridhara D, Sridharan A, *et al*.. LDPC block and convolutional codes based on circulant matrices[J]. *IEEE Transactions on Information Theory*, 2004, 50(12): 2966–2984.

[5] Tam W M, Lau F C M, and Tse C K. A class of QC-LDPC codes with low encoding complexity and good error performance[J]. *IEEE Communications Letters*, 2010, 14(2): 169–171.

[6] Kang J Y, Huang Q, Zhang L, *et al*.. Quasi-cyclic LDPC codes: an algebraic construction[J]. *IEEE Transactions on Communications*, 2010, 58(5): 1384–1396.

[7] 林国庆, 陈汝伟, 王新梅, 等. 基于素域构造的准循环低密度校验码[J]. 电子与信息学报, 2010, 32(3): 609–612.
Lin Guo-qing, Chen Ru-wei, Wang Xin-mei, *et al*.. Construction of quasi-cyclic LDPC codes from prime fields[J]. *Journal of Electronics & Information Technology*, 2010, 32(3): 609–612.

[8] Kamiya N. Efficiently encodable irregular QC-LDPC codes constructed from self-reciprocal generator polynomials of MDS codes[J]. *IEEE Communications Letters*, 2010, 14(9): 860–862.

[9] He Z, Fortier P, and Roy S. A class of irregular LDPC codes with low error floor and low encoding complexity[J]. *IEEE Communications Letters*, 2006, 10(5): 372–374.

[10] Xu Y and Wei G. On the construction of quasi-systematic block-circulant LDPC codes[J]. *IEEE Communications Letters*, 2007, 11(11): 886–888.

[11] Bini D, Corso G M D, Manzini G D, *et al*.. Inversion of circulant matrices over Z_m[J]. *Mathematics of Computation*, 2000, 70(235): 1169–1182.

[12] Rivest R L. The invertibility of the XOR of rotations of a binary word[J]. *International Journal of Computer Mathematics*, 2011, 88(2): 281–284.

[13] Richardson T and Urbanke R. Efficient encoding of low density parity check codes[J]. *IEEE Transactions on Information Theory*, 2001, 47(2): 638–656.

[14] Richardson T and Urbanke R. The capacity of low-density parity check codes under message-passing decoding[J]. *IEEE Transactions on Information Theory*, 2001, 47(2): 599–618.

[15] Muquet B, Wang Z D, Giannakis G B, *et al*.. Cyclic prefixing or zero padding for wireless multicarrier transmissions[J]. *IEEE Transactions on Communications*, 2002, 50(12): 2136–2148.

戚肖克： 女，1987 年生，博士生，研究方向为水声通信，信道编码.

李 宇： 男，1977 年生，博士，副研究员，研究方向为水声通信及水下信号处理.

黄海宁： 男，1969 年生，博士，研究员，研究方向为水声通信及水下信号处理.