0254-6124/2009/29(4)-443–05 *Chin. J. Space Sci.* 空间科学学报

Xia Guojiang, Qi Jianzhong, Sun Huixian, Xiong Weiming. A class of quasi-cyclic LDPC codes and encoding. *Chin. J. Space Sci.*, 2009, **29**(4): 443∼447

一类准循环 LDPC 码及其编码*

夏国江[1,2] 齐建中[1] 孙辉先[1] 熊蔚明[1]

[1](中国科学院空间科学与应用研究中心 北京 100190)

[2](中国科学院研究生院)

摘 要 针对空间通信的特点, 对基于循环矩阵构造的一类正则准循环 LDPC 码进行了改进, 得到了一类非正则准循环 LDPC 码. 与原码相比, 这类非正则 LDPC 码的奇偶校验矩阵 $\boldsymbol{H}$ 具有 3 个特点: 行满秩, 具有下三角结构, 引入了一度变量节点. 前两个特性使得这种 LDPC 码的编码计算复杂度和结构复杂度都与校验位长度成正比, 从而便于编码器的软硬件实现. 第三个特性使码的迭代译码门限稍有降低, 但同时还能保证译码的收敛, 计算机仿真结果也证明了这一点. 本文还简化了对围长不小于 6 的条件的证明, 推导了系统码校验位的计算公式, 并在此基础上给出了利用移位寄存器的编码电路.

关键词 准循环 LDPC 码; 计算复杂度; 结构复杂度; 循环矩阵; 生成向量

中图法分类号 V 524 TN 911.2

A Class of Quasi-cyclic LDPC Codes and Encoding

XIA Guojiang[1,2] QI Jianzhong[1] SUN Huixian[1] XIONG Weiming[1]

[1](*Center for Space Science and Applied Research, Chinese Academy of Sciences, Beijing* 100190)

[2](*Graduate University of Chinese Academy of Sciences*)

Abstract Firstly, based on the characters of space communication, this study improves a class of regular quasi-cyclic LDPC codes which is based on circulant matrices and obtains a kind of irregular quasi-cyclic LDPC codes. Compared with original codes, the parity check matrix called $\boldsymbol{H}$ of this irregular LDPC ensemble has three characters: 1. $\boldsymbol{H}$ is row full rank; 2. $\boldsymbol{H}$ is lower triangulation; 3. $\boldsymbol{H}$ contains degree one variable nodes. With the first two characters, the encoding complexity of computation and architecture of this kind of LDPC are proportion to the length of check symbols, so encoders implemented with software and hardware are quite simple. This feature is very important to deep space communication because the resource on board is constrained. The third character makes the iterative decoding threshold lower than the original codes. Moreover, the computer simulation has proved this result. Secondly, the proof for the condition of girth not shorter than 6 is simplifed compared to the original ones. Last, the computing formula is derived for parity check symbols of systemic codes. Based on this formula, the encoding circuit has been investigated using shift registers.

* 中国科学院知识创新工程项目资助 (062134A45S)

2008-06-17 收到原稿, 2009-05-04 收到修定稿

E-mail: x@ee.buaa.edu.cn

Key words Quasi-cyclic LDPC codes, Computational complexity, Architectural complexity, Circulant matrices, Generating vectors

1 引言

低密度奇偶校验码 (LDPC) 于 1962 年由 Gallager 发明[1],[2], 但是由于其编译码的复杂度太高, 当时没有合适的电子器件能够实现, 所以很快被遗忘. 1981 年 Tanner[3] 从图的角度论述了 LDPC 码, 但是他的工作也没有引起其他编码研究人员的注意. 直到 20 世纪 90 年代中后期, 一些学者在研究图上的迭代算法时, 重新发现 LDPC 后, 才使其得到了学术界和产业界的重视.

LDPC 码性能优异, 在和积算法 (SPA) 下, 能接近香农限[4], 突破了信道截止速率的限制. 目前 LDPC 码已经成为 IEEE802.16, IEEE802.20, IEEE802.3 以及数字卫星广播 (DVB-S2) 等标准的信道编码方案.

LDPC 码的译码已经得到了比较好的解决, 和积算法的时间 (计算) 复杂度为 $O(n)$, (其中 n 为码长), 且能接近香农限[5]. 虽然文献 [6] 给出了一种能降低编码复杂度的方法, 但是 LDPC 码的编码过程仍然比较复杂, 必须存储 6 个与奇偶校验矩阵相关的子矩阵, 总存储量与原奇偶校验矩阵相同. 由于 LDPC 码的码长短则数千, 长则上万, 所以存储量巨大, 极耗电路资源. 在空间通信和移动通信中, 星载设备和手持设备的体积、功耗都是关键因素, 因此减小体积和功耗有着十分重要的意义. 近年来, 为了降低 LDPC 码的编译码复杂度, 人们进行了很多深入的研究[7]~[11]. 本文在文献 [7] 基础上对原构造方法进行了改进, 主要体现在以下几个方面.

(1) 奇偶校验矩阵是行满秩的.

(2) 奇偶校验矩阵具有完全的下三角结构.

(3) 引入了一个一度变量节点, 有利于降低译码门限.

(4) 编码后得到的是系统码.

进一步研究这类 LDPC 码编码的软硬件实现. 用软件实现时, 其时间复杂度为 $O(n)$, 用硬件实现时, 只需少量移位寄存器和逻辑门, 其存储量与校验位成比例. 另外, 为了适应高速数据传输, 还给出了一种并行编码电路.

2 准循环 LDPC 码

准循环码是指, 任意码字经循环移位某个确定的值后, 能得到另外一个码字的码. 文献 [12] 指出, 准循环码的奇偶校验矩阵经过适当的列置换后, 能使各子矩阵为循环矩阵. 这里讨论的 LDPC 码的奇偶校验矩阵, 就是由循环子矩阵构成的, 所以这种 LDPC 码是准循环码.

一个 (J, L) 正则准循环 LDPC 码的奇偶校验矩阵可以表达如下[7]:

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{I}(0) & \boldsymbol{I}(0) & \cdots & \boldsymbol{I}(0) \\ \boldsymbol{I}(0) & \boldsymbol{I}(P_{1,1}) & \cdots & \boldsymbol{I}(P_{1,L-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{I}(0) & \boldsymbol{I}(P_{J-1,1}) & \cdots & \boldsymbol{I}(P_{J-1,L-1}) \end{bmatrix} \tag{1}$$

这里 $\boldsymbol{I}(P_{j,l})$ 表示第 r 行 1 的位置在第 $[(r+P_{j,l}) \bmod q]$ 列的 $q\times q$ 循环置换矩阵, $0\leqslant r\leqslant q-1$, q 为素数, $1\leqslant j\leqslant J-1$, $1\leqslant l\leqslant L-1$. 显然 $\boldsymbol{I}(P_{j,l})$ 的各行可由其第一行逐次循环右移得到, 由此定义 $\boldsymbol{I}(P_{j,l})$ 的第一行为生成矢量 $\boldsymbol{i}_{j,l}^{(0)}$.

虽然存在多种方法生成合适的 $\boldsymbol{I}(P_{j,l})$, 本文主要讨论文献 [7] 给出的其中两种: (1) 乘积型 $P_{j,l}=jl \bmod q$ 且 $q=J=L$; (2) 指数型 $P_{j,l}=q_1^j q_2^l \bmod q$, q_1 和 q_2 在有限域 $GF(q)$ 中的阶分别为 J 与 L . 由后面一种方法得到的 $\boldsymbol{H}$ 矩阵, 与 式(1) 相比缺少第一行第一列. 若实际需要, 可对其扩展得到式 (1) 的形式, 并可保证对应的 Tanner 图中围长不减小[7]. 用这两种方法构造的 LDPC 码的码长 $n=Lq$, $\boldsymbol{H}$ 矩阵一般不是满秩矩阵, 其秩最多是 $Jq-J+1$.

乘积型和指数型 $P_{j,l}$ 都满足文献 [7] 的定理 2.2, 所以由这两种方法构造的 LDPC 码对应 Tanner 图的围长都不小于 6. 原文证明很复杂, 本文给出另外一种比较简单的证明. 首先, 要证明围长不小于 6, 只需证明 $\boldsymbol{H}$ 矩阵的任意两行, 最多只有一个 1 在相同的位置上.

证明 假设有两个 1 在相同的位置上, 从而

可以假设 $l_1 \neq l_2$: 对乘积型有

$$\left.\begin{aligned} j_1 l_1 + r_1 &= j_2 l_1 + r_2, \\ j_1 l_2 + r_1 &= j_2 l_2 + r_2. \end{aligned}\right\} \Rightarrow \left\{\begin{aligned} (j_1 - j_2) l_1 &= r_2 - r_1, \\ (j_1 - j_2) l_2 &= r_2 - r_1. \end{aligned}\right. \tag{2}$$

对指数型有

$$\left.\begin{aligned} q_1^{j_1} q_2^{l_1} + r_1 &= q_1^{j_2} q_2^{l_1} + r_2, \\ q_1^{j_1} q_2^{l_2} + r_1 &= q_1^{j_2} q_2^{l_2} + r_2. \end{aligned}\right\} \Rightarrow \left\{\begin{aligned} q_2^{l_1}(q_1^{j_1} - q_1^{j_2}) &= r_2 - r_1, \\ q_2^{l_2}(q_1^{j_1} - q_1^{j_2}) &= r_2 - r_1. \end{aligned}\right. \tag{3}$$

由式 (2) 和式 (3) 都可得 $l_1 = l_2$, 与假设矛盾, 所以假设不成立, 即围长不小于 6.

由于 $\boldsymbol{H}$ 矩阵不满秩, 所以在编码时首先要找到 $\boldsymbol{H}$ 矩阵极大线性无关组. 这在 $\boldsymbol{H}$ 矩阵比较大时 (实际上 $\boldsymbol{H}$ 矩阵一定很大) 很繁琐费时. 更重要的是, 这样做破坏了各子矩阵规则性, 使得硬件实现时需要付出更多的资源, 用软件实现时, 与随机构造的码相比也没有优势. 此外 $\boldsymbol{H}$ 矩阵秩值的不确定性, 使得设计码率与实际码率有较大的出入. 针对这些缺点, 本文对 $\boldsymbol{H}$ 矩阵进行了改进, 得到的一类非正则准循环码能够消除这些不足.

假设需要设计一个码率为 $R = 1 - M/N$ 的 $[N \times q, (N - M) \times q]$ 码, 首先在 $\boldsymbol{H}$ 矩阵中随机选取 M 行 N 列, $M \leqslant J$, $M < N \leqslant L$, 称得到的矩阵为 $\boldsymbol{H}_1$. 这样得到的 $\boldsymbol{H}_1$ 矩阵, 显然仍然保持任意两行最多只有一个 1 在相同的位置上; 然后从 $\boldsymbol{H}_1$ 中随机选取 $M-1$ 行, $M-1$ 列, 通过随机的行列置换后, 使选中的行和列分别成为 $\boldsymbol{H}_1$ 的前 $M-1$ 行和后 $M-1$ 列; 最后把 $\boldsymbol{H}_1$ 矩阵的第 t 行的最后 $M-t$ 个 q 阶方阵替换为 q 阶全零方阵, $1 \leqslant t \leqslant M-1$, 这样替换以后带来两个好处. 第一个好处是使最后一个变量成为一度节点, 有控制地引入一度节点有助于降低译码门限. 第二个好处是由于消除矩阵中的 1, 对应于删去图中的边, 所以这样得到的图的最短圈的个数比原图少, 符合 LDPC 码的构造规则. 最后, 在 $\boldsymbol{H}_2$ 矩阵各块行内作行置换, 使得块行最后一个元素为 $q \times q$ 的单位阵, 称得到的矩阵为 $\boldsymbol{H}_3$. 由线性码的性质知, 行置换后得到的码与原码相同. 显然 $\boldsymbol{H}_3$ 矩阵满秩, 各子矩阵是循环矩阵, 并具有下三角结构. 这些特性使得由 $\boldsymbol{H}_3$ 确定的 LDPC 码编码简单, 且设计码率与实际码率相等.

3　编码

对于准循环码的编码问题有很多处理方法, 但是这些方法都是基于生成矩阵的. 一般而言, LDPC 码的生成矩阵是稠密的, 所以利用生成矩阵对 LDPC 码进行编码, 没有利用 LDPC 码校验矩阵的稀疏特性来降低计算复杂度. 下文主要研究利用校验矩阵对 LDPC 码进行编码.

由于一般 LDPC 码的奇偶校验矩阵缺乏结构性, 所以这些 LDPC 码的编码时间复杂度为 $O(n^2)$[4]. 为了降低复杂度, 文献 [6] 把奇偶校验矩阵 $\boldsymbol{H}$ 化成了近似下三角结构, 如图 1 所示, 并指出编码时间复杂度为 $O(n + g^2)$. 这里构造的 LDPC 码 $\boldsymbol{H}$ 矩阵的 g 为零, 从而 $\boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}$ 不再存在, 所以编码的时间复杂度为 $O(n)$.

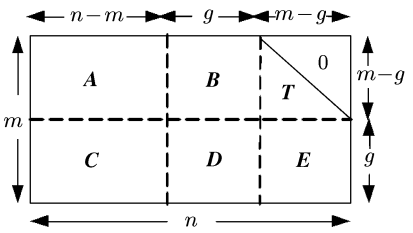


图 1　近似下三角 $\boldsymbol{H}$ 矩阵形式

Fig. 1　$\boldsymbol{H}$ matrix in approximate lower triangular form

根据奇偶校验矩阵与合法码字的内积为零, 可以推导出编码的过程和电路结构. 假设 $\boldsymbol{c} = (\boldsymbol{s}, \boldsymbol{p})$, $\boldsymbol{s}$ 为信息位, $\boldsymbol{p}$ 为奇偶校验位, 有

$$\boldsymbol{H}\boldsymbol{c}^{\mathrm{T}} = [\boldsymbol{A}\ \boldsymbol{T}] \begin{bmatrix} \boldsymbol{s}^{\mathrm{T}} \\ \boldsymbol{p}^{\mathrm{T}} \end{bmatrix} = \boldsymbol{A}\boldsymbol{s}^{\mathrm{T}} + \boldsymbol{T}\boldsymbol{p}^{\mathrm{T}} = 0^{\mathrm{T}}, \tag{4}$$

$$\boldsymbol{p} = \boldsymbol{s}(\boldsymbol{T}\ \boldsymbol{A}) = \boldsymbol{s}\boldsymbol{Y}. \tag{5}$$

其中, $\boldsymbol{Y} = (\boldsymbol{T}^{-1}\boldsymbol{A})^{\mathrm{T}}$ 为 $(n-m) \times m$ 矩阵, 并且循环矩阵的乘积、逆、转秩仍为循环矩阵[13], 可知 $\boldsymbol{Y}$ 是由 $(N-M) \times M$ 个 $q \times q$ 的子循环矩阵构成, $m = Mq$, $n = Nq$, 具有如下结构:

$$\boldsymbol{Y} = \begin{bmatrix} \boldsymbol{Y}_{1,1} & \boldsymbol{Y}_{1,2} & \cdots & \boldsymbol{Y}_{1,M} \\ \boldsymbol{Y}_{2,1} & \boldsymbol{Y}_{2,2} & \cdots & \boldsymbol{Y}_{2,M} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{Y}_{N-M,1} & & \cdots & \boldsymbol{Y}_{N-M,M} \end{bmatrix}. \tag{6}$$

其中, $\boldsymbol{Y}_{j,i}$ 可由其生成矢量 $\boldsymbol{y}_{j,i}^{(0)}$ 循环移位得到. 分别把 $\boldsymbol{s}$ 和 $\boldsymbol{p}$ 平均分成 $N-M$ 段和 M 段, 每段包含 q 位, 即 $\boldsymbol{S} = (\boldsymbol{S}_1, \boldsymbol{S}_2, \cdots, \boldsymbol{S}_{N-M})$,

$\boldsymbol{p}=(\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_M)$, $\boldsymbol{S}_j=(s_{(j-1)q+1},s_{(j-1)q+2},\cdots,s_{jq})$, $1\leqslant j\leqslant(N-M)$, $\boldsymbol{p}_i=(p_{(i-1)q+1},p_{(i-1)q+2},\cdots,p_{iq})$, $1\leqslant i\leqslant M$. 由矩阵乘法规则可知

$$\boldsymbol{p}_i=\boldsymbol{s}_1\boldsymbol{Y}_{1,i}+\boldsymbol{s}_2\boldsymbol{Y}_{2,i}+\cdots+\boldsymbol{s}_{N-M}\boldsymbol{Y}_{N-M,i}, \tag{7}$$

$$\boldsymbol{s}_j\boldsymbol{Y}_{j,i}=s_{(j-1)q+1}\,\boldsymbol{y}_{j,i}^{(0)}+s_{(j-1)q+2}\,\boldsymbol{y}_{j,i}^{(1)}+\cdots+s_{jq}\,\boldsymbol{y}_{j,i}^{(q-1)}. \tag{8}$$

这里 $1\leqslant i\leqslant M$, $1\leqslant j\leqslant N-M$ 生成矢量 $\boldsymbol{y}_{j,i}^{(0)}$, 循环移位 k $(1\leqslant k\leqslant q-1)$ 次得到 $\boldsymbol{y}_{j,i}^{(k)}$. 从式 (7) 和式 (8) 可知, 经过 q 次循环可算得 $\boldsymbol{s}_j\boldsymbol{Y}_{j,i}$, $(N-M)q$ 个时钟后得 p_i, 这正好是所有信息位都进入编码器所需的时间. 计算 $\boldsymbol{s}_j\boldsymbol{Y}_{j,i}$ 的单元电路如图 2 所示.

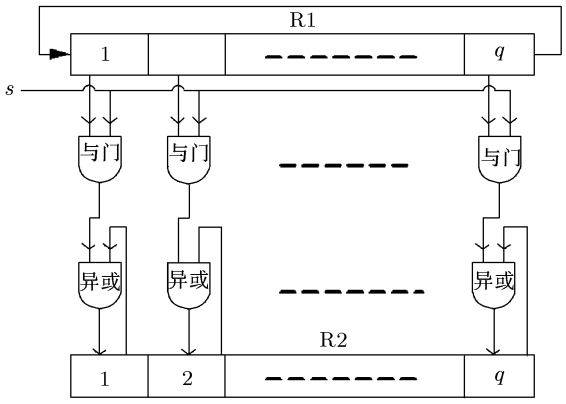


图 2 校验位计算单元电路

Fig. 2 Check symbol computation cell circuit

编码开始时, 把 $\boldsymbol{y}_{1,i}^{(0)}$ 存入上部循环移位寄存器 R1 中, 下部累加寄存器 R2 清零. 当信息比特 s_1 进入编码后, 经与门得乘积 $s_1\boldsymbol{y}_{1,i}^{(0)}$, 再经异或门与 R2 中值相加并存入 R2 中, 同时 s_1 送入信道. 然后 s_2 进入编码器和信道, R1 中数值右移一位得 $\boldsymbol{y}_{1,i}^{(1)}$, 经与门得乘积 $s_2\boldsymbol{y}_{1,i}^{(1)}$, 再经异或门与 R2 中值相加并存入 R2 中. 如此重复这个过程, 直到 s_q 进入编码器后, 寄存器 R2 中的数值为 $s_1\boldsymbol{y}_{1,i}$. 在 s_{q+1} 进入编码器的同时, 把 $\boldsymbol{y}_{2,i}^{(0)}$ 载入 R1 中, 编码电路重复计算 $s_1\boldsymbol{y}_{1,i}$ 的步骤. 当 s_{2q} 进入编码器后, R2 中的值为 $s_1\boldsymbol{y}_{1,i}+s_2\boldsymbol{Y}_{2,i}$. 这个过程一直重复进行到 $s_{(N-M)q}$ 进入编码器, 此时 R2 中的值为 $p_i=s_1\boldsymbol{Y}_{1,i}+s_2\boldsymbol{Y}_{2,i}+\cdots+s_{N-M}\boldsymbol{Y}_{N-M,i}$. 计算 p_i 的过程中, 对电路的操作可归纳如下: s_1 到来时 R2 清零, $s_{(j-1)q+1}$ 到来时把 $\boldsymbol{y}_{j,i}^{(0)}$ 载入 R1 中, $1\leqslant j\leqslant N-M$, 其余时刻对 R1 作循环右移. 为了计算所有的 $\boldsymbol{p}_i$, $1\leqslant i\leqslant M$, 共需要 M 组单元电路, 所以总触发器个数为 $2m$, 总与门和异或门数均为 m, 是校验位长度的 2 倍. 文献 [14] 从生成矩阵的角度出发, 给出了与本文类似的编码电路.

为了适应高速数据传输, 可以采用并行电路计算 p_i 以提高编码速率. 具体实现方法是并行计算式 (7) 右边的 $(N-M)$ 项, 这样只需 q 个时钟周期即可完成编码. 这种并行电路共需 $M\times(N-M)$ 组单元电路, 所以空间复杂度变为串行电路的 $(N-M)$ 倍.

4 仿真实例

在 AWGN 中, 采用 BPSK 调制, 接收端为相干解调的条件下, 对本文构造的两种 LDPC 码进行性能仿真, 译码采用和积算法, 最多迭代 50 次.

实例 1 指数型 $P_{j,l}$, 取 $q=181$ $q_1=5$ $q_2=42$ 则 $J=15$, $L=5$. $\boldsymbol{H}$ 矩阵由 5×15 个 181×181 的循环子矩阵组成. 现设计一个 $R=0.5$ 的 $(8\times181,4\times181)$ 码, 随机从 $\boldsymbol{H}$ 中取出 1 到 4 行, 6 到 14 列, 得到一个未经改进的 (1448, 727) 码. 然后, 按前文所述方法, 对该码的奇偶校验矩阵进行改造, 得到满足设计要求的码. 仿真结果表明, 改进后码的误码率为 10^{-5} 时, 距香农限 2 dB.

实例 2 乘积型 $P_{j,l}$, 取 $q=J=L=73$, $\boldsymbol{H}$ 矩阵共有 73×73 个 73×73 的循环子矩阵组成. 现设计一个 $R=0.92$ 的 $(72\times73,66\times73)$ 码, 随机从 $\boldsymbol{H}$ 中取出 1 到 6 行, 1 到 72 列, 得到一个未经改进的 (5256, 4823) 码, 在此基础上得到改造后满足设计要求的码. 仿真结果表明改进后码的误码率为 10^{-5} 时, 距香农限 1.25 dB.

以上两个实例的性能曲线如图 3 所示.

这两个仿真实例表明, 改进后的 LDPC 码与原码相比, 不但有前述各种优点, 而且码的性能也得到了提高. Mackay 指出[4], 通过子矩阵置换构造的 LDPC 码的最小距离, 不随码长线性增长. 所以有可能在误码率比较高的情况下, 就出现误码平台. 本文描述的 LDPC 码也属于由置换子矩阵构造的, 但是仿真结果表明, 在误码率为 10^{-6} 时, 也未出现误码平台.

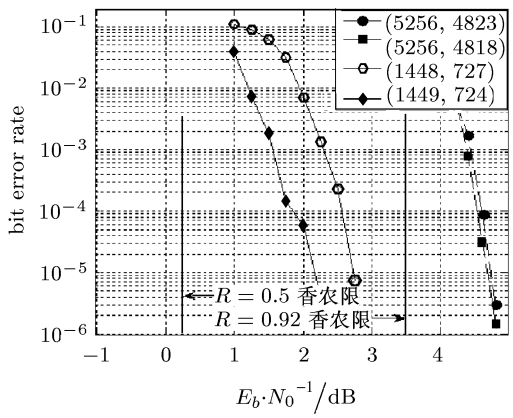


图 3　AWGN 下性能曲线

Fig. 3　Performances comparison in AWGN

5　结束语

利用循环矩阵构造了一类准循环非正则 LDPC 码, 构造方法简单, 与已有准循环 LDPC 码相比, 具有一些突出的优点. 这类 LDPC 码的设计码率与实际码率相等且是系统码, 方便设计得到特定码率的码和译码. 奇偶校验矩阵的下三角特性, 使得编码计算复杂度为 $O(n)$, 便于用通用处理器实现. 码的准循环特性, 导致用专用集成电路实现时, 可极大地节省电路资源, 适合在航空航天以及手持通信设备中应用. 性能仿真结果表明, 这类码在具备上述优点的同时, 没有牺牲误码率性能, 能够接近香农限.

参考文献

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

[2] Gallager R G. Low-density Parity-Check codes. Cambridge MA: MIT Press, 1963

[3] Tanner R M. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, 1981, **27**(5):533∼547

[4] MacKay D J C. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory*, 2001, **45**(2):399∼431

[5] Richardon T J, Urbanke R L. The capacity of low-density parity-check codes under message-passing decoding. *IEEE Trans. Inf. Theory*, 2001, **47**(2):599∼618

[6] Richardon T J, Urbanke R L. Efficient encoding of low-density parity-check codes. *IEEE Trans. Inf. Theory*, 2001, **47**(2):638∼656

[7] Fossorier M P C. Quasi-cyclic low-density parity-check codes form circulant permutation matrices. *IEEE Trans. Inf. Theory*, 2004, **50**(8):1788∼1793

[8] Hao Zhong, Tong Zhong, Erich F. Haratsch. Quasi-cyclic LDPC codes for the magnetic recording channel: Code design and VLSI implementation. *IEEE Trans. Magn.*, 2007, **43**(3):1118∼1123

[9] Lan Lan, Zeng Lingqi, *et al.* Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach. *IEEE Trans. Inf. Theory*, 2007, **53**(7):2429∼2457

[10] Fujisawa M, Sakata S. A class of quasi-cyclic regular LDPC codes from cyclic difference families with girth 8. In: Proc. IEEE Int. Symp. Information Theory, Adelaide, Australia, 2005, 2290∼2294

[11] Xu J, Chen L, Djurdjevic I, Lin S, Abdel-Ghaffar K. Construction of regular and irregular LDPC codes: Geometry decomposition and masking. *IEEE Trans. Inf. Theory*, 2007, **53**(1):121∼134

[12] Lin S, Costello D J. Error Control Coding: Fundamentals and Applications (2nd ed). Upper Saddle River. NJ: Prentice Hall, 2004. 185∼188

[13] Grays R M. Toeplitz and circulant matrices: a review. Standford: Department of Electric Engineering, Standford University, 2001. 31∼35

[14] Li Zongwang, Chen Lei, Lin Shu *et al.* Efficient en-coding of quasi-cyclic low-density parity-check codes. *IEEE Globe Com.*, 2005, 1205∼1210