

围长为 8 的 QC-LDPC 码的显式构造及其在 CRT 方法中的应用

张国华, 孙蓉, 王新梅

(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, 陕西 西安 710071)

摘 要: 对于任意码长 $PL(P \geq 3L^2/4 + L - 1)$, 利用完全确定的方式构造出一类围长为 8 的 $(4, L)$ QC-LDPC 码。将这类码作为分量码, 结合中国剩余定理(CRT)构造出一类围长至少为 8 且码长非常灵活的合成 QC-LDPC 码。在 1/2 码率和中等码长条件下的仿真结果表明, 这种合成码在 AWGN 信道下具有优异的性能。

关键词: 准循环低密度奇偶校验码; 围长; 显式构造; 中国剩余定理

中图分类号: TN911.22

文献标识码: A

文章编号: 1000-436X(2012)03-0171-06

Explicit construction of girth-eight QC-LDPC codes and its application in CRT method

ZHANG Guo-hua, SUN Rong, WANG Xin-mei

(State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China)

Abstract: For arbitrary code lengths of the form $PL(P \geq 3L^2/4 + L - 1)$, a new family of $(4, L)$ -regular quasi-cyclic (QC) low-density parity-check (LDPC) codes was proposed explicitly with girth eight. Employing the new code as a component code in the construction method of Chinese remainder theorem (CRT), a novel class of compound QC-LDPC codes was presented with both girth at least eight and very flexible code lengths. Simulation results show that the new compound codes with rate 1/2 and moderate code lengths perform very well over the additive white Gaussian noise (AWGN) channel.

Key words: QC-LDPC code; girth; explicit construction; Chinese remainder theorem (CRT)

1 引言

具有较大围长的准循环低密度奇偶校验(QC-LDPC)码, 由于具有线性时间可编码、需要的存储空间较小、译码性能优良等优点, 目前得到人们越来越多的研究。借助于计算机搜索, 人们提出了一些构造围长大于 6 的 QC-LDPC 码的准随机方法^[1,2]。这些基于搜索的方法虽然比较灵活, 但是由于没有解决码的存在性问题, 因此不可避免地存在

构造失败的可能性。相比而言, 确定性方法可以直接给出校验矩阵的显式表达式, 不存在构造失败的可能性, 但是确定性方法的设计具有很大的挑战性, 所以研究成果比较罕见。

(J, L) QC-LDPC 码的校验矩阵是一个 $J \times L$ 的阵列, 阵列中的每个元素都是一个 $P \times P$ 的循环置换矩阵(CPM)。到目前为止, 构造围长大于 6 的 QC-LDPC 码的确定性方法只有几种。对于列重 J 为 3 的情形, Tanner^[3]基于群结构提出了一类围长

收稿日期: 2010-06-18; 修回日期: 2011-10-11

基金项目: 国家重点基础研究发展计划(“973”计划)基金资助项目(2010CB328300); 国家自然科学基金资助项目(61001131, 61101148, 61001130); 高等学校学科创新引智计划(111 项目)基金资助项目(B08038)

Foundation Items: The National Basic Research Program of China (973 Program) (2010CB328300); The National Natural Science Foundation of China (61001131, 61101148, 61001130); The Program of Introducing Talents of Discipline to Universities (111 Program) (B08038)

几乎全部达到最大值 12 的(3,5)QC-LDPC 码 (码长为 $5P, P$ 为素数且 $P-1$ 可被 15 整除); B.Vasic^[4] 基于最早序列提出了一类 girth-8 (3, L)QC-LDPC 码; K.K.Liu^[5] 提出了一类 girth-8 (3, L) QC-LDPC 码; 张国华^[6] 受贪婪搜索启发提出了一类 girth-8 (3, L) QC-LDPC 码。对于列重为 4 的情形, 目前已知的确定性构造方法只有一种, 即 K.K.Liu 提出的一类 girth-8 (4, L) QC-LDPC 码^[7]。

本文提出了一种构造 girth-8(4, L)QC-LDPC 码的新的确定性方法。这种方法构造出的码允许码长在某个门限之上以 L 为步进连续取值; 更引人注目的是, 这种码的连续码长最小值不仅比文献[7]中码的连续码长最小值要小得多 (仅为其 3/4 左右), 而且几乎可以达到目前利用计算机大规模搜索得出的码长最小值。

本文组织如下: 第 2 节描述了这种新码的构造方法, 并证明了其围长特性; 第 3 节比较了新构造方法和一些著名的搜索方法得到的码长最小值; 第 4 节提出了这种新码的一种具体应用, 即结合中国剩余定理(CRT)构造出一类围长至少为 8 并且码长非常灵活的合成 QC-LDPC 码; 第 5 节是结束语。

2 构造方法

(4, L) QC-LDPC 码的校验矩阵可以表示为

$$H = \begin{bmatrix} I(p_{0,0}) & I(p_{0,1}) & L & I(p_{0,L-1}) \\ I(p_{1,0}) & I(p_{1,1}) & L & I(p_{1,L-1}) \\ I(p_{2,0}) & I(p_{2,1}) & L & I(p_{2,L-1}) \\ I(p_{3,0}) & I(p_{3,1}) & L & I(p_{3,L-1}) \end{bmatrix} \quad (1)$$

其中, $I(x)$ 表示一个受控于 x 的循环置换矩阵, 具体定义与文献[1]完全相同; 为了便于论述和证明, 下文使用 m 表示 x 的第一个索引标记, 使用 i, j, k 表示 x 的第二个索引标记。本文按照如下方式配置 $p_{m,j} (0 \leq m \leq 3, 0 \leq j \leq L-1)$:

$$p_{0,j} = 0, p_{1,j} = j, 0 \leq j < L \quad (2)$$

$$p_{2,0} = 0; p_{2,j+1} = p_{2,j} + \max(j+2, L-j), \\ 0 \leq j < L-1 \quad (3)$$

$$p_{3,j} = p_{1,j} + p_{2,j}, 0 \leq j < L \quad (4)$$

令上述配置下得到的矩阵用 H_D 表示。定义 H_D 中第 r, s, t 行 ($0 \leq r, s, t \leq 3$) 循环置换矩阵所构成的

矩阵为 $H_D(r, s, t)$ 。首先证明一些性质和引理。

性质 1 $p_{2,L-1} < 3L^2/4$ 。

证明 根据式(3), $p_{2,L-1} = \sum_{i=0}^{L-2} \max\{i+2, L-i\}$ 。经过简单计算可知: 当 L 为偶数时 $p_{2,L-1}$ 等于 $3L^2/4-1$, 当 L 为奇数时 $p_{2,L-1}$ 等于 $3(L^2-1)/4$ 。

性质 2 若 $j > i$, 则 $p_{2,j} > p_{2,i} + p_{1,j}$ 。

证明 对 j 采用数学归纳法。首先考察 $j=i+1$ 的情形。根据式(2)和式(3), $p_{2,i+1} > p_{2,i} + (i+1) = p_{2,i} + p_{1,i+1}$ 。现在假设 $p_{2,j-1} > p_{2,i} + p_{1,j-1}$, 则根据式(2)和式(3)有 $p_{2,j} > p_{2,j-1} + 1 > p_{2,i} + p_{1,j}$ 。

引理 1 对于任意整数 $P \geq 3L^2/4, H_D(0,1,2)$ 中无 4-环; 对于任意整数 $P \geq 3L^2/4 + L-1, H_D$ 中无 4-环。

证明 根据式(2)~式(4)和性质 2, 引理 1 很显然成立。

引理 2 对于任意整数 $P \geq 3L^2/4, H_D(0,1,2)$ 的围长为 8。

证明 根据引理 1, 只需证明不存在 6-环和证明存在 8-环。假设 $H_D(0,1,2)$ 中存在 6-环。则该环可用式(5)描述, 其中, $0 \leq i, j, k < L$ 互异。

$$(p_{0,i} - p_{1,i}) + (p_{1,j} - p_{2,j}) + (p_{2,k} - p_{0,k}) = 0 \pmod P \quad (5)$$

情形 1) $j > k, k \neq 0$: 式(5)变成 $p_{2,j} = p_{2,k} - p_{1,i} + p_{1,j} \pmod P$, 这是不可能的, 因为根据性质 2, 式(6)成立。

$$3L^2/4 > p_{2,j} > p_{2,k} - p_{1,i} + p_{1,j} > 0 \quad (6)$$

情形 2) $j > k, k = 0$: 式(5)变成 $p_{2,j} + p_{1,i} - p_{1,j} = 0 \pmod P$, 这是不可能的, 因为根据性质 2, 式(7)成立。

$$0 < p_{2,j} + p_{1,i} - p_{1,j} < \max\{p_{2,j}, p_{2,i}\} < 3L^2/4 \quad (7)$$

情形 3) $j < k$: 式(5)变成 $p_{2,k} = p_{2,j} + p_{1,i} - p_{1,j} \pmod P$, 这是不可能的, 因为根据式(3), 式(8)成立。

$$3L^2/4 > p_{2,k} = p_{2,j} + L - j > p_{2,j} + p_{1,i} - p_{1,j} > 0 \quad (8)$$

现在考虑 8-环。根据式(2), $H_D(0,1,2)$ 中总是存在一个由式(9)描述的不依赖于 P 的 8-环:

$$(p_{0,0} - p_{1,0}) + (p_{1,1} - p_{0,1}) + (p_{0,2} - p_{1,2}) + (p_{1,1} - p_{0,1}) = 0 \quad (9)$$

引理 3 对于任意整数 $P \geq 3L^2/4, H_D(1,2,3)$

中无 6-环。

证明 假设 $H_D(1,2,3)$ 中存在 6-环。则该环可用式(10)描述, 其中, $0 \leq i, j, k < L$ 互异。

$$(p_{2,i} - p_{3,i}) + (p_{3,k} - p_{1,k}) + (p_{1,j} - p_{2,j}) = 0 \pmod P \quad (10)$$

根据式(4), 式(10)变成 $(0 - p_{1,i}) + (p_{1,j} - p_{2,j}) + (p_{2,k} - 0) = 0 \pmod P$, 这意味着 $H_D(0,1,2)$ 中存在 6-环。与引理 1 矛盾。

引理 4 对于任意整数 $P \geq 3L^2/4 + L - 1$, $H_D(0,1,3)$ 中无 6-环。

证明 假设 $H_D(0,1,3)$ 中存在 6-环。则该环可用等式(11)描述, 其中, $0 \leq i, j, k < L$ 互异。

$$(p_{0,i} - p_{3,i}) + (p_{3,k} - p_{1,k}) + (p_{1,j} - p_{0,j}) = 0 \pmod P \quad (11)$$

根据式(4), 式(11)变成:

$$p_{2,i} = p_{2,k} - p_{1,i} + p_{1,j} \pmod P \quad (12)$$

情形 1) $i > k, k \neq 0$: 式(12)是不可能的, 因为式(13)导致式(14)成立。

$$j - i < L - k \leq \max(k + 2, L - k) \quad (13)$$

$$3L^2/4 > p_{2,i} \geq p_{2,k} + \max(k + 2, L - k) > p_{2,k} + j - i > 0 \quad (14)$$

情形 2) $i > k, k = 0$: 式(12)变成 $p_{2,i} + p_{1,i} = p_{1,j} \pmod P$, 这是不可能的, 因为根据性质 1, 式(15)成立。

$$3L^2/4 + L - 1 > p_{2,i} + p_{1,i} > p_{1,j} > 0 \quad (15)$$

情形 3) $i < k, i \neq 0$: 式(12)变成 $p_{2,k} = p_{2,i} + p_{1,i} - p_{1,j} \pmod P$, 这是不可能的, 因为根据式(3), 式(16)成立。

$$3L^2/4 > p_{2,k} \geq p_{2,i} + i + 2 > p_{2,i} + p_{1,i} - p_{1,j} > 0 \quad (16)$$

情形 4) $i < k, i = 0$: 等式(12)变成 $p_{2,k} + p_{1,j} = 0 \pmod P$, 这是不可能的, 因为式(17)成立。

$$0 < p_{2,k} + p_{1,j} < 3L^2/4 + L - 1 \quad (17)$$

引理 5 对于任意整数 $P \geq 3L^2/4 + L - 1$, $H_D(0,2,3)$ 中无 6-环。

证明 假设 $H_D(0,2,3)$ 中存在 6-环。则该环可用式(18)描述, 其中, $0 \leq i, j, k < L$ 互异。

$$(p_{0,i} - p_{3,i}) + (p_{3,k} - p_{2,k}) + (p_{2,j} - p_{0,j}) = 0 \pmod P \quad (18)$$

根据式(4), 式(18)变成:

$$-p_{1,i} - p_{2,i} + p_{1,k} + p_{2,j} = 0 \pmod P \quad (19)$$

情形 1) $i > j, j \neq 0$: 式(19)变成 $p_{2,i} = p_{2,j} - p_{1,i} + p_{1,k} \pmod P$, 这是不可能的, 因为根据式(3), 式(20)成立。

$$3L^2/4 > p_{2,i} \geq p_{2,j} + L - j > p_{2,j} + k - i > 0 \quad (20)$$

情形 2) $i > j, j = 0$: 式(19)变成 $p_{2,i} + p_{1,i} = p_{1,k} \pmod P$, 这是不可能的, 因为根据性质 1, 式(21)成立。

$$3L^2/4 + L - 1 > p_{2,i} + p_{1,i} > p_{1,k} \geq 0 \quad (21)$$

情形 3) $i < j, i \neq 0$: 式(19)变成 $p_{2,j} = p_{2,i} + p_{1,i} - p_{1,k} \pmod P$, 这是不可能的, 因为根据式(3), 式(22)成立。

$$3L^2/4 > p_{2,j} \geq p_{2,i} + i + 2 > p_{2,i} + i - p_{1,k} > 0 \quad (22)$$

情形 4) $i < j, i = 0$: 式(19)变成 $0 = p_{2,j} + p_{1,k} \pmod P$, 这是不可能的, 因为根据性质 1, 式(23)成立。

$$3L^2/4 + L - 1 > p_{2,j} + p_{1,k} > 0 \quad (23)$$

根据引理 1~引理 5 可以得到定理 1。

定理 1 对于任意整数 $P \geq 3L^2/4 + L - 1$, H_D 的围长均为 8。

3 最小 P 值的比较

K.K.Liu 最近提出了(4, L) QC-LDPC 码的一种确定性构造方法, 对于任意 $P \geq L^2$, 该方法构造出的 LDPC 码的围长均为 8。根据定理 1, 构造的 girth-8 (4,L) QC-LDPC 码的最小 P 值仅大约为 K.K.Liu (4,L) QC-LDPC 码的最小 P 值的 3/4。这说明, 构造的 girth-8 (4,L) QC-LDPC 码的码长具有更加广泛的取值范围。

构造的 girth-8 (4,L)QC-LDPC 码的最小 P 值甚至可以非常逼近基于计算机搜索的准随机方法所得到的最小 P 值。Fossorier^[1]和 Sullivan^[2]采用基于计算机搜索的准随机方法, 构造出了 P 值非常小的 girth-8 (4,L) QC-LDPC 码。对于 $L=4\sim 13$, Fossorier 给出了使得 girth-8 (4,L) QC-LDPC 码存在的最小 P 值。对于 $L=5\sim 12$, Sullivan 给出了对应的搜索结果。图 1 表明, 对于 $L=5\sim 13$ 本文新方法给出的最小 P 值与上述 2 种准随机方法给出的最小 P 值非常接近。

需要指出的是, 虽然图 1 中的 3 种方法得到的

最小 P 值非常接近，但是本文的方法是确定性的，不需要借助于任何计算机搜索过程。此外，该方法所对应的最小 P 值是 P 允许连续取值的最小值：只要 P 不小于该最小值，相应 LDPC 码的围长就为 8。对于 Fossorier 和 Sullivan 方法得到的最小 P 值而言，当 P 大于该最小值时 LDPC 码的围长不能保证必然为 8，除非利用他们的搜索算法再次搜索出满足 girth-8 条件的校验矩阵。

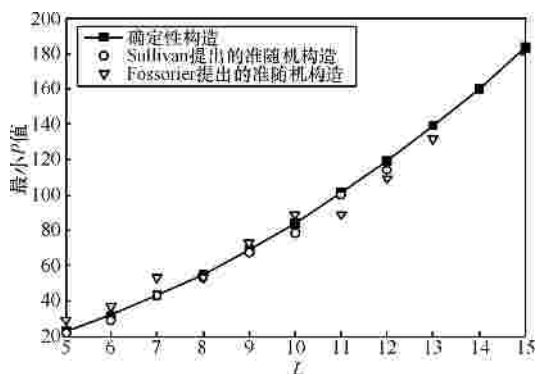


图 1 3 种方法得到的最小 P 值的比较

将 H_D 的零空间对应的二进码记为 D-QC-LDPC 码。下面首先分析 D-QC-LDPC 码的理论价值。文献[1]在 III-B 节中提出了一个相当难的问题（问题 1）：如何给出使 (J, L) QC-LDPC 码围长至少为 g 的最小 P 值的解析结果？由定理 1 可知，只要 $P \geq 3L^2/4 + L - 1$ 就存在围长至少为 8 的 $(4, L)$ QC-LDPC 码。显然，该结论对于条件 $g=8, J=4$ 下问题 1 的解决具有重要的理论参考价值。

另一方面，通过仿真发现，与文献[1]搜索出的 girth-8 准随机 QC-LDPC 码相比，D-QC-LDPC 码在译码性能上没有明显优势。但是，这并不说明 D-QC-LDPC 码就没有应用价值。相反，D-QC-LDPC 码作为一个基本模块可以在其他的 LDPC 码构造方法（例如 CRT 构造法）中发挥至关重要的作用。

4 基于 CRT 构造围长至少为 8 的 QC-LDPC 码

最近，中国剩余定理（CRT, Chinese remainder theorem）被应用到 QC-LDPC 码的构造中^[8,9]。利用 CRT 构造 LDPC 码的优势是，用若干个 QC-LDPC 短码作为分量码可以构造出 QC-LDPC 长码，并且 QC-LDPC 长码的围长不小于所有分量码的最大围长。将 array 码作为分量码，文献[8]利用 CRT 构造出了不含 4 环的 QC-LDPC 码，文献[9]利用 CRT

方法构造出了一类不含 4 环并且 6 环数量大大减少（但不能完全消除）的 QC-LDPC 码。由于 array 码的 CPM 尺寸为素数，因此这 2 种方法得到的 QC-LDPC 码的码长取值非常受限。本节将 D-QC-LDPC 码作为分量码，利用其 CPM 尺寸可以任意取值的优势，基于 CRT 方法构造出一类不仅完全消除 4 环和 6 环，而且码长非常灵活的 QC-LDPC 码。

4.1 构造方法

根据 CRT 原理，利用一个不含 6 环的 QC-LDPC 短码作为分量码，可以构造出一系列不含 6 环的 QC-LDPC 长码。D-QC-LDPC 码的围长为 8 且 CPM 尺寸可以任意取值，因而非常合适作为 CRT 方法中的这种分量码。

设 $J \in \{3, 4\}$ ， L 是满足 $L > J$ 的任意整数。令 $P_{th}(3, L) = 3L^2/4$ ， $P_{th}(4, L) = 3L^2/4 + L - 1$ 。设 $P_1 \geq P_{th}(J, L)$ 。D-QC-LDPC 码的校验矩阵 H_1 是由 $P_1 \times P_1$ 的 CPM 所组成的一个 $J \times L$ 阵列，其指数矩阵为 $E(H_1) = (p_{m,j}^{(1)})$ 。设 P_2 是满足 $\gcd(P_1, P_2) = 1$ 的整数（gcd 表示最大公约数）， H_2 是由 $P_2 \times P_2$ 的 CPM 所组成的一个 $J \times L$ 阵列，其指数矩阵为 $E(H_2) = (p_{m,j}^{(2)})$ 。令 $P = P_1 P_2$ ，定义指数矩阵 $E(H) = (p_{m,j})$ ，其中， $p_{m,j} = p_{m,j}^{(1)} A_1 P_2 + p_{m,j}^{(2)} A_2 P_1 \pmod P$ ， A_1 和 A_2 是满足 $\gcd(A_1, P_1) = 1$ 、 $\gcd(A_2, P_2) = 1$ 的 2 个任意正整数。根据 CRT 原理^[9]，校验矩阵 H 是由 $P \times P$ 的 CPM 所组成的一个 $J \times L$ 阵列矩阵，其围长可以确保至少为 8。

指数矩阵 $E(H_2)$ 共有 P_2^L 种选择方式，在不同方式下校验矩阵 H 的围长可能不同；即使围长相同，长度等于围长的短环数量也可能差别很大。下面提出一种选择指数矩阵 $E(H_2)$ 的启发式策略，以使校验矩阵 H 的围长尽可能大，并且短环数量尽可能小。

1) 指数矩阵 $E(H)$ 的首行首列元素初始化为 0，即 $p_{0,j} = 0 (0 \leq j \leq L - 1)$ ， $p_{m,0} = 0 (0 \leq m \leq J - 1)$ ，其余元素初始化为 ∞ 。

2) 按照 $p_{1,1}, p_{1,2}, \dots, p_{1,L}$ 的顺序，依次确定 $p_{m,j}^{(2)}$ 。确定 $p_{m,j}^{(2)}$ 的策略是在 0 至 $P_2 - 1$ 中选择使当前 H 围长最大的元素。如果有多个元素同时满足该条件，可以随机或按照固定方式选择其中一个。这里采用固定方式，即选择最小元素。

4.2 例子与仿真

相对于高码率的 LDPC 码而言，构造性能优良的中低码率 LDPC 码通常会更困难。例如，W E. Ryan 和 S.Lin 在系统总结目前 LDPC 码构造进展的最新专著《Channel Codes: Classical and Modern》^[10]中所给出的绝大多数 LDPC 码举例均对应于高码率(大于 0.75)，只有很少的几个例子对应于中低码率(0.5 及其以下)。下面利用 4.1 节所述方法构造了 2 个设计码率为 0.5 的合成 QC-LDPC 码。为了对新合成码的性能作出客观评价，选择 2 种比较基准。第一种比较基准是 1/2 码率条件下的 Shannon 限(0.188dB)。第二种比较基准是文献[10]中设计码率为 0.5 且码长与新合成码最为接近的 LDPC 码。

例 1 选择 $P_1 = 29, P_2 = 7, A_1 = 19, A_2 = 2$ 。根据 4.1 节构造方法，得到了校验矩阵 H 的指数矩阵 $E(H)$ ：

$$E(H) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 17 & 5 & 51 & 155 & 114 \\ 0 & 15 & 42 & 168 & 137 & 36 \end{bmatrix}$$

经验证，校验矩阵 H 的围长为 10。校验矩阵 H 的 CPM 维数为 $(29 \times 7) \times (29 \times 7) = 203 \times 203$ 。对应的合成码码长为 $203 \times 6 = 1218$ 、码率为 0.5016。在进行译码仿真时，和积译码算法的最大迭代次数设定为 80。在 $BER=10^{-6}$ 时，译码性能距离 Shannon 限仅 2.43dB(如图 2 所示)。文献[10]中 Example 11.8 利用基于 RS 码特殊子集的方法构造了一个码长为 1488、码率为 0.502 的 QC-LDPC 码，在 $BER=10^{-6}$ 时该码的译码性能距离 Shannon 限为 3.5dB。新合成码比 Example 11.8 码的性能改善了约 1.07dB。

例 2 选择 $P_1 = 64, P_2 = 7, A_1 = 21, A_2 = 2$ 。根据 4.1 节所述构造方法，得到了校验矩阵 H 的指数矩阵 $E(H)$ ：

$$E(H) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 19 & 166 & 441 & 76 & 31 & 50 & 5 \\ 0 & 24 & 157 & 79 & 46 & 32 & 37 & 61 \\ 0 & 107 & 3 & 328 & 314 & 63 & 23 & 2 \end{bmatrix}$$

经验证，校验矩阵 H 的围长为 8。校验矩阵 H 的 CPM 维数为 $(64 \times 7) \times (64 \times 7) = 448 \times 448$ 。对应的合成码码长为 $448 \times 8 = 3584$ 、设计码率为 0.5011。在进行译码仿真时，和积译码算法的最大迭代次数设

定为 80。在 $BER=10^{-6}$ 时，译码性能距离 Shannon 限仅 2.15dB(如图 2 所示)。文献[10]中 Example 11.12 基于素域中的加法群方法构造了一个码长为 4672、码率为 0.501 的(4,8)QC-LDPC 码，在 $BER=10^{-6}$ 时该码的译码性能距离 Shannon 限为 2.05dB。虽然新合成码比 Example 11.12 码的性能略差一些，但是前者码长要比后者码长短 1088bit。这说明新合成码的性能是非常优异的。

除了具有优异的译码性能，新合成码的一个突出优势在于码长取值的灵活性。对于例 1 和例 2 所述的基于 RS 码特殊子集的方法和基于素域中加法群的方法，其 CPM 尺寸与有限域的阶数(为素数或素数的幂)存在密切关联，因而 CPM 尺寸的选取不够灵活。而 4.1 节提出的新方法 CPM 尺寸为 $P = P_1 P_2$ ，其中 P_1 为满足 $P_1 \geq P_{th}(J, L)$ 的任意整数， P_2 只要满足 $\gcd(P_1, P_2) = 1$ 即可，所以 CPM 尺寸的取值非常灵活。此外，新合成码构造时不需要有限域知识背景，因此对于实际工程应用而言具有较大竞争力。

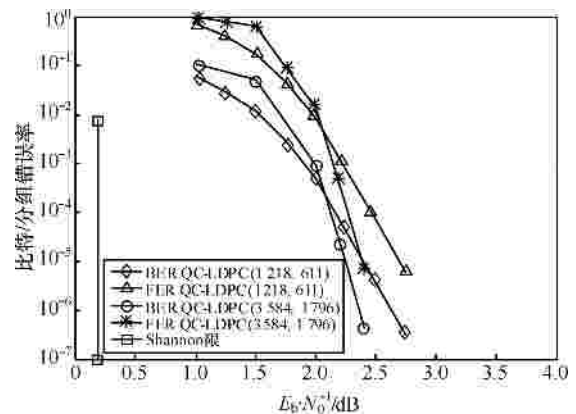


图 2 D-QC-LDPC 码作为分量码利用 CRT 得到的合成 QC-LDPC 码的性能曲线

5 结束语

本文提出了一种构造围长为 8 的(4,L)QC-LDPC 码的确定性方法。这类新码的最小 P 值与 Fossorier 和 Sullivan 利用准随机方法通过计算机大量搜索得到的最小 P 值非常接近。将新 QC-LDPC 码作为分量码，基于中国剩余定理构造出一类围长至少为 8 且码长取值非常灵活的合成 QC-LDPC 码。在 1/2 设计码率和中等码长条件下的仿真结果表明，这类新的合成 QC-LDPC 码在 AWGN 信道下具有优异的译码性能。显然，本文设计的矩阵 H_d 也可以用来构造围长至少为 8 的多元 QC-LDPC 码，

具体构造细节和译码性能仿真将是近期的研究内容之一。

参考文献：

- [1] FOSSORIER M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices[J]. IEEE Trans on Information Theory, 2004, 50(8):1788-1793.
- [2] O'SULLIVAN M E. Algebraic construction of sparse matrices with large girth[J]. IEEE Trans on Information Theory, 2006, 52(2): 718-727.
- [3] KIM S, NO J S, CHUNG H, *et al.* On the girth of tanner (3,5) quasi-cyclic LDPC codes[J]. IEEE Trans on Information Theory, 2006, 52(4):1739-1744.
- [4] VASIC B, PEDAGANI K, IVKOVIC M. High-rate girth-eight low-density parity-check codes on rectangular integer lattices[J]. IEEE Trans on Communications, 2004, 52(8):1248-1252.
- [5] LIU K K, FEI Z S, KUANG J M. Novel algebraic constructions of nonbinary structured LDPC codes over finite fields[A]. Proc 68th IEEE VTC Fall[C]. Calgary, Alberta, Canada, 2008. 1-5.
- [6] 张国华, 陈超, 杨洋等. Girth-8 (3,L)-规则 QC-LDPC 码的一种确定性构造方法[J]. 电子与信息学报, 2010, 32(5): 1152-1156.
- ZHANG G H, CHEN C, YANG Y, *et al.* Girth-8 (3, L)-regular QC-LDPC codes based on novel deterministic design technique[J]. Journal of Electronics & Information Technology, 2010, 32(5): 1152-1156.
- [7] LIU K K, FEI Z S, KUANG J M. Three algebraic methods for constructing nonbinary LDPC codes based on finite fields[A]. Proc 19th IEEE PIMRC[C]. Cannes, French Riviera, France, 2008.1-5.
- [8] MYUNG S, YANG K. A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem[J]. IEEE Communication Letters, 2005, 9(9):823-825.
- [9] LIU Y H, WANG X M, CHEN R W, *et al.* Generalized combining method for design of quasi-cyclic LDPC codes[J]. IEEE Communication Letters, 2008, 12(5):392-394.
- [10] RYAN W E, LIN S. Channel Codes: Classical and Modern[M]. Cambridge University Press, 2009.

作者简介：



张国华（1977-），男，山西临汾人，西安电子科技大学博士生，主要研究方向为信道编码理论和 ATM 交换技术。



孙蓉（1976-），女，陕西西安人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为信息论与信道编码理论。



王新梅（1937-），男，浙江浦江人，西安电子科技大学教授、博士生导师，主要研究方向为信道编码理论和密码学。