Tanner 图中最短圈的计数

陈汝伟[1,2]，黄华伟[3]，杜小妮[4]，丁 勇[2]，肖国镇[1]

(1. 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；2. 桂林电子科技大学 数学与计算机科学学院,广西 桂林 541004；3. 华南农业大学 信息学院,广东 广州 510642；4. 西北师范大学 数学与信息科学学院,甘肃 兰州 730070)

摘要： 应用 Chen 等提出的研究线性分组码校验矩阵与 Tanner 图中圈的关系的方法,证明了围长为 $2k$ 的校验矩阵中满足一定条件的 k 行组合与其 Tanner 图中最短圈的一一对应关系. 由这一结论,对 Chen 等提出的计算 Tanner 图中最短圈数量的算法加以改进,减少一个运算步骤,而仍然得到同样准确的结果.

关键词： 低密度校验(LDPC)码；Tanner 图；最短圈；$2k$-圈矩阵

中图分类号： TN911.21 **文献标识码：** A **文章编号：** 1001-2400(2008)06-0983-03

On the number of shortest cycles of Tanner graphs

CHEN Ru-wei[1,2]，*HUANG Hua-wei*[3]，*DU Xiao-ni*[4]，*DING Yong*[2]，*XIAO Guo-zhen*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China; 2. School of Math. and Computational Sci., Guilin Univ. of Electronic Tech, Guilin 541004, China; 3. College of Inform. South China Agricultural Univ., Guangzhou 510642, China; 4. College of Math. and Inform. Sci., Northwest Normal Univ., Lanzhou 730070, China)

Abstract: By the method for investigating the relation between parity-check matrixes and cycles of associated Tanner graphs proposed by Chen et al., the one-to-one correspondence between k-row-combinations satisfying a certain condition in a parity-check matrix of grith k and shortest cycles in the associated Tanner graph is proved. As a consequence, the algorithm for counting the shortest cycels of Tanner graphs proposed by Chen et al. is improved. The improved algorithm is as accurate as the original one while omitting one of the main steps.

Key Words: low-density parity-check (LDPC) code; Tanner graph; shortest cycle; $2k$-cycle-matrix

Gallager 于1962年首次提出了低密度校验码(LDPC码)[1],但是,这一卓越的创造在当时并没有得到应有的重视. 1981年,Tanner 从图的角度研究了低密度校验码[2]. Tanner 的工作同样没有引起编码学界的关注. 直到1996年,Mackay 和 Neal 证实了低密度校验码可以获得接近香农限的误码性能[3],低密度校验码被编码学界忽视的状况才得以改变. 自此以后,低密度校验码成为编码学界研究的热点[4~6],而 Tanner 图也成为研究低密度校验码不可或缺的重要工具. 编码研究者对研究 Tanner 图中的圈表现出了极大的兴趣. 普遍认为:好的低密度校验码的 Tanner 图不应具有过多的短圈[7,8]. Tanner 图中最短圈的长度称为围长. 好的低密度校验码构造应尽量避免其 Tanner 图中有短圈出现,使其围长不至于很小. 然而,大的围长仍然不足以保证低密度校验码具有好的性能. 文献[9]的研究结果表明,具有相同围长、其他条件相似的两个低密度校验码,如果它们 Tanner 图中短圈的数量不同,则可能导致很大的性能差异：Tanner 图中短圈数量少的低密度校验码性能优于 Tanner 图中短圈数量多的低密度校验码. Tanner 图中短圈的分布也对低密度校验码的性能有所影响：Tanner 图中短圈分布较不均匀的低密度校验码性能优于 Tanner 图中短圈分布较均匀的

收稿日期： 2007-10-14

基金项目： 国家自然科学基金资助(60073028)

作者简介： 陈汝伟(1974-),男,西安电子科技大学博士研究生,E-mail：spring2.718@163.com.

低密度校验码.

在文献[10]中,研究了校验矩阵与 Tanner 图中圈的关系,其中给出了一个最短圈计数的算法.笔者在文献[10]的基础上给出了关于校验矩阵与 Tanner 图中最短圈的进一步结果,改进和简化了文献[10]中给出的计算 Tanner 图中最短圈数量的算法.

1 校验矩阵与 Tanner 图中的最短圈

设 $\boldsymbol{H}_{mn}$ 是一个 $m\times n$ 校验矩阵, G 是 $\boldsymbol{H}_{mn}$ 的 Tanner 图,并且 G 的围长$g=2k\ (k>2)$.

引理 1 若 $\boldsymbol{H}_{mn}$ 中 k 个行 $r_1,r_2,\cdots,r_k$ 的和(在这里,若干个向量的和并不指它们在 GF(2)上的向量和,而只是把它们看作一般整数按对应位置相加.) S 至少有 k 个分量不小于 2,则可以肯定 S 中没有大于 2 的分量,且 S 中只有 k 个分量等于 2.

证明 记与 $r_1,r_2,\cdots,r_k$ 相对应的 Tanner 图 G 中的校验节点分别为 $p_1,p_2,\cdots,p_k$.

假设 S 有一个分量大于 2.不失一般性,假设这一分量对应着 $\boldsymbol{H}_{mn}$ 中的第 c_1 列.记 $\boldsymbol{H}_{mn}$ 中对应着 S 中另外 $k-1$ 个不小于 2 的分量的列分别为 $c_2,c_3,\cdots,c_k$,记对应于 $c_1,c_2,\cdots,c_k$ 的 Tanner 图 G 中的变量节点分别为 $v_1,v_2,\cdots,v_k$,记位于以上 k 行 k 列交叉点上的 $\boldsymbol{H}_{mn}$ 的子矩阵为 $\boldsymbol{M}'$.由于 $\boldsymbol{M}'$ 中的 c_1 列至少有 3 个“1”,至少有 3 种不同的选择来使 $\boldsymbol{M}'$ 中的一些“1”转变为“0”,以使转变后的矩阵的每一列中只有 2 个“1”.由文献[10]定理 3.3 中“(c)⇒(b)”的证明,可以知道以上每一种不同的选择结果得到一个不同的 $2k$- 圈矩阵.不同的 $2k$-圈矩阵对应着 Tanner 图 G 中不同的最短圈(圈长为 $2k$).因此,G 中至少有 3 个不同的最短圈皆以 $p_1,p_2,\cdots,p_k$ 和 $v_1,v_2,\cdots,v_k$ 为圈上的所有节点.这显然是不可能的.因此,S 不可能有大于 2 的分量.

下面证明 S 中只有 k 个等于 2 的分量.否则,假设 S 中至少有 $k+1$ 个等于 2 的分量.记对应于 S 中 $k+1$ 个等于 2 的分量的 $\boldsymbol{H}_{mn}$ 中列分别为 $c_1,c_2,\cdots,c_k,c_{k+1}$,记位于 $r_1,r_2,\cdots,r_k$ 与 $c_2,\cdots,c_k,c_{k+1}$ 交叉点上的 $\boldsymbol{H}_{mn}$ 的子矩阵为 $\boldsymbol{M}_1$,记位于 $r_1,r_2,\cdots,r_k$ 与 $c_1,c_3,\cdots,c_k,c_{k+1}$ 交叉点上的 $\boldsymbol{H}_{mn}$ 的子矩阵为 $\boldsymbol{M}_2$.由上面的证明及文献[10]定理 3.3 中“(c)⇒(b)”的证明,可以知道 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 都是 $2k$- 圈矩阵.$\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 有 $k-1$ 个共同的列.由文献[10] 中 $2k$- 圈矩阵的定义,容易知道在 $\boldsymbol{M}_1$ 中对应于 c_2 的列等于在 $\boldsymbol{M}_2$ 中对应于 c_1 的列,并且这 2 列都有 2 个“1”.因此,$\boldsymbol{H}_{mn}$ 中的 c_1 列与 c_2 列有 2 对对应的“1”在相同的位置上.由此可知,Tanner 图 G 的围长是 4.这与设定的条件“G 的围长$g=2k\ (k>2)$”矛盾.因此,S 中不可能有超过 k 个等于 2 的分量,而只能恰好有 k 个等于 2 的分量.

容易看出,若将引理 1 中的“行”改为“列”,引理 1 依然成立.

下面的引理是引理 1 的直接结果:

引理 2 若 $p_1,p_2,\cdots,p_k$ 是 Tanner 图 G 中一个最短圈上的 k 个校验节点,则 G 中只有一个最短圈以 $p_1,p_2,\cdots,p_k$ 为圈上的全部校验节点.

同样,如果将引理 2 中的“校验节点”改为“变量节点”, 引理 2 依然成立.

2 Tanner 图中最短圈的计数

在文献[10]中,给出了一个直接由校验矩阵 $\boldsymbol{H}_{mn}$ 计算其 Tanner 图 G 中最短圈数量的算法.现将这一算法的步骤叙述如下:

(1) 逐个从校验矩阵 $\boldsymbol{H}_{mn}$ 中取出所有可能的 k 行组合.

(2) 将在第(1)步得到的每一个 k 行组合里的 k 行相加,记所得的和为 S.S 中不小于 2 的分量的个数记为 u.若 $u<k$,则 Tanner 图 G 中没有最短圈以这 k 行对应的 k 个校验节点为圈上的全部校验节点;若 $u\geqslant k$,则 Tanner 图 G 中有 $\binom{u}{k}=\dfrac{u(u-1)\cdots(u-k+1)}{k(k-1)\cdots 2\cdot 1}$ 个最短圈以这 k 行对应的 k 个校验节点为圈上的全部校验节点.

(3) 逐个把第(2)步计算出的对应于每个 k 行组合的最短圈的个数相加,得到 Tanner 图 G 中最短圈的

总数.

由引理 2,知道对于 $\boldsymbol{H}_{mn}$ 中每个 k 行组合,Tanner 图 G 中最多只有一个最短圈以这 k 行对应的 k 个校验节点为圈上的全部校验节点. 利用这一结论,文献[10]给出的计算 Tanner 图中最短圈数量的算法可以被简化. 简化后的算法可以叙述为以下定理:

定理 1　Tanner 图 G 中最短圈的数量等于具有以下性质的 $\boldsymbol{H}_{mn}$ 中的 k 行组合的数量:这些 k 行组合每一个组合中的 k 行相加的和 S 有且仅有 k 个分量等于 2.

定理 1 实际上给出了一种从校验矩阵 $\boldsymbol{H}_{mn}$ 计算其 Tanner 图中最短圈数量的算法:要计算 Tanner 图 G 中最短圈数量,可以逐个从校验矩阵 $\boldsymbol{H}_{mn}$ 中取出所有可能的 k 行组合,计算满足定理 2 条件的 k 行组合的总数. 这一算法明显比文献[10]中给出的算法有所改进. 容易证明,若将定理 1 中的“行”改为“列”,定理 1 依然成立.

3　结 束 语

应用了 Chen 等在文献[10]中提出的研究线性分组码校验矩阵与 Tanner 图中圈的关系的方法,探讨了线性分组码校验矩阵与 Tanner 图中最短圈的关系,改进和简化了 Chen 等在文献[10]中给出的计算 Tanner 图中最短圈数量的算法.

参考文献:

[1]　Gallager R G. Low Density Parity Check Codes [J]. IRE Trans on Inform Theory, 1962, IT-8: 21-28.

[2]　Tanner R M. A Recursive Approach to Low Complexity Codes[J]. IEEE Trans on Inf Theory, 1981, 27(5): 533-547.

[3]　MacKay D J C, Neal R M. Near Shannon Limit Performance of Low Density Parity Check Codes[J]. IEE Electron Lett, 1996, 32(18): 1 645-1 646.

[4]　童胜,王鹏,王单,等. LDPC 码量化和积译码的高效实现[J]. 西安电子科技大学学报,2004, 31(5): 709-713.
Tong Sheng, Wang Peng, Wang Dan, et al. Efficient Implementation of the Sum-product Algorithm for Quantized Decoding of LDPC Codes[J]. Journal of Xidian University, 2004, 31(5): 709-713.

[5]　王鹏,王新梅. LDPC 码的快速编码研究[J]. 西安电子科技大学学报,2004, 31(6): 934-938.
Wang Peng, Wang Xinmei. Study of Efficient Encoding of LDPC Codes[J]. Journal of Xidian University, 2004, 31(6): 934-938.

[6]　Lin S, Costello D J. Error Control Coding: Fundamentals and Applications [M]. 2nd Edition. Upper Saddle River: Prentice Hall, 2004.

[7]　Mao Y, Banihashemi A H. A Heuristic Search for Good Low Density Parity-check Codes at Short Block Lengths[C]// Proc Int Conf Communications: Vol 1. Finland: Helsinki, 2001: 41-44.

[8]　Benedetto S, Montorsi G. Design of Parallel Concatenated Convolutional Codes[J]. IEEE Trans on Commun, 1996, 44(5): 591-600.

[9]　Halford T R, Chugg K M. An Algorithm for Counting Short Cycles in Bipartite Graphs[J]. IEEE Trans on Inf Theory, 2006, 52(1): 287-292.

[10]　Chen R, Huang H, Xiao G. Relation Between Parity-Check Matrixes and Cycles of Associated Tanner Graphs [J]. IEEE Communications Letters, 2007, 11(8): 674-676.

(编辑: 齐淑娟)