二次同余序列构造规则 LDPC 码*)

刘文明　朱光喜　邓勇强
(华中科技大学电子与信息工程系　武汉 430074)

摘　要　本文提出了二次同余序列构造规则 LDPC 码的方法。该种方法可以通过确定的方式构造编码器，在实现中大大节省了存储空间。仿真结果表明该种方法能达到随机方法生成的不存在四线循环的 LDPC 码的性能。

关键词　LDPC 码，二次同余序列，四线循环，确定性

Construction of Low Density Parity Check Codes Using Quadratic Congruential Sequences

LIU Wen-Ming　ZHU Guang-Xi　DENG Yong-Qiang
(Department of Electronics and Information Engineering of Huazhong University of Science and Technology, Wuhan 430074)

Abstract　In this paper a method using quadratic congruential sequences to design regular LDPC code is proposed. The main advantage of this method is that the structure of the encoder is deterministic, rather than having to store the encoder structure graph in memory. Simulation results show that these codes provide almost the same performance of a constrained pseudorandom construction that explicitly avoids cycles of length less than or equal to four.

Keywords　LDPC code, Quadratic congruential sequences, Cycles of length four, Deterministic

1　前言

低密度奇偶校验(LDPC)码是继 Turbo 码后又一种性能逼近 Shannon 信道容量限的编码方法，其理论上的完善性以及错误译码的可检测性等特点都要优于 Turbo 码。LDPC 码是由 Gallager[1,2]在 20 世纪 60 年代初首先提出来的，D. J. C Mackay[4]等人的研究，使 LDPC 码的研究跨入了一个新的阶段。LDPC 码是线性纠错码，它的校验矩阵是一个稀疏矩阵。每个码字满足一定数目的线性约束，而约束的数目通常是非常小的。同时由于 LDPC 码的约束是由一个稀疏图定义的，因而使得它的译码变得较为容易。目前，LDPC 码是编码领域的一个新的研究热点。

在实际应用中，如果校验矩阵采用随机方式生成，我们需要在接收端存储校验矩阵。对于不同的编码长度以及编码速率，我们需要存储相应的结构形式。因此，为了节省存储空间，采用代数方法构造二分图就显得十分重要。本文提出一种二次同余序列构造二分图的确定性的设计方法。本文第 2 节介绍该编码方法的结构，第 3 节给出二次同余序列的设计方法，第 4 节进行仿真与性能分析，最后进行了总结。

2　规则 LDPC 码的二分图结构

我们用二分图来说明规则(N,K)LDPC 码编码器的构成原理。正则的(λ,ρ)LDPC 码，每个信息节点与 λ 个校验节点相连，每个校验节点与 ρ 个信息节点相连。如图(1)所示，$\lambda=3,\rho=6$。信息节点与校验节点之间共有 $M=N\lambda$ 条连接路径。左边的连接节点$(i\lambda,i\lambda+1,\cdots,i\lambda+\lambda-1)$为 i 信息节点的连接节点，右边的$\{j\rho,j\rho+1,\cdots,j\rho+\rho-1\}$为 j 校验节点的连接节点，图中的每条连接线连接左边的信息节点与右边的检验节点。为了描述的方便，我们按照顺序列出了每个信息节点的连接节点以及每个校验节点的连接节点，图中画出了第 p 条信息节点的连接节点(属于$\lfloor p/\lambda \rfloor$信息节点)，与校验节点的连接节点 A_p 相连接，而 A_p 为$\lfloor q/\rho \rfloor$校验节点的连接节点。随机设计的 LDPC 码，其每条连接线是随机产生的，也就是说，$A_0,A_1,\cdots A_p,\cdots,A_{M-1}$是随机产生的序列。在本文中，我

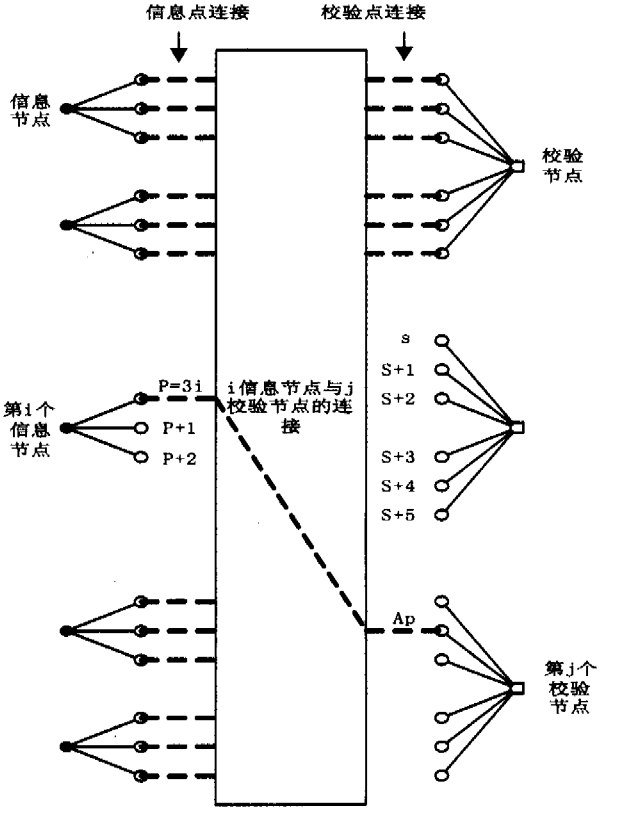

图 1　LDPC 码二分图结构示意图

*)基金项目：国家自然科学基金重大项目"未来移动通信系统基础理论与技术研究"(No. 60496315)；国家高技术研究发展计划(863 计划)(No. 2003AA12331005)。**刘文明**　博士生，研究方向为 Turbo 码、LDPC 码等。**朱光喜**　教授，博士生导师，主要从事无线通信系统和多媒体信息处理方向研究。

们讨论 $\lambda=3$ 的情况，如图 1 所示。显然，信息节点的连接节点与校验节点的连接节点之间是一一映射的。

3 基于二次同余序列的二分图设计

根据上面的分析，校验矩阵可以通过一组一一映射来构造，A 是包含元素$\{0,1,\cdots,M-1\}$的集合，其中的一个排列可以表示为置换器 I_M，其映射函数为：$d_{I_M}:A\to A$，$d_{I_M}:i\to j$，$i,j\in A$。

3.1 二次同余序列的设计方法

$$d_{I_M}(i)=\frac{ki(i+1)}{2}+\upsilon(\mathrm{mod}\ M)\quad 0\leqslant i\leqslant M-1 \tag{1}$$

其中 k、υ 必须满足以下条件：

1、$k<M$，$\upsilon<M$；

2、υ 与 N 互质；

3、k 为奇数；

4、$M=2^n$，n 为正整数。

对于(1)式，满足上面条件时，可以生成一一映射的二次同余序列。

在应用中，我们可以通过中间变量设计一个长度 M 的置换，映射函数为 $D_M:d_{D_M}:c_m\mapsto c_{m+1}(\mathrm{mod}\ M)$，$0\leqslant m<M$，其实现算法如下：

1、$c_0=0$

2、$c_m=c_{m-1}+km(\mathrm{mod}\ M)$，$0\leqslant m<M$，$k$ 为常数。

上式的迭代过程可以简化为一个二次同余的式子：

$$c_m=\frac{km(m+1)}{2}(\mathrm{mod}\ M),\ 0\leqslant m<M,\ k\text{ 为奇数} \tag{2}$$

但在 $M\neq 2^n$，采用式(1)不构成一一映射。下面阐述一种缩短的二次同余构造一一映射的方法。

3.2 缩短的二次同余序列

式(1)、式(2)构造二次同余序列要求 M 为 2 的幂次形式，对于长度 S 不为 2 的幂次形式的情况，我们通过元素两两相互交换位置来设计缩短的二次同余序列，$\frac{M}{2}<s\leqslant M$，$M=2^r$，且 $\upsilon=0$，$h=M/2$。其具体实现算法如下：

```
Step 1: stored←false
Step 2: i←0
Step 3: while(i≤S)
        x←c_{i+1}
        y←c_i+N/2(mod N)
        if(x<S&&y<S)
          swap positions x and y
        if(x<S&&y≥S)
          if(stored=true)
            swap positions x and t
            stored←false
          else
              t←x
              stored←true
        if(x≥S&&y<S)
          if(stored=true)
            swap positions y and t
            stored←false
          else
              t←y
              stored←true
        increment i by 1.
```

3.3 二分图的设计

通过上面的方法得到了一个 M 元素的一一映射，即得到序列 $d_0,d_1,\cdots d_\rho,\cdots d_{m-1}$，我们就可以生成校验矩阵 H。

$$\begin{cases}H(\lfloor d_i/\rho\rfloor,\lfloor i/\lambda\rfloor)=1,0\leqslant i\leqslant M-1,\\ \text{其它为 }0\end{cases}$$

这样就得到了 H。

3.4 环的分析与算法的改进

当信息节点有两条边连接到同一个校验节点上，则形成二线循环，选取 $\lambda=3$，假设跟同一个信息节点相连的 3 条边为 A_n、A_{n+1}、A_{n+2}。为了消除二线循环，必须满足以下条件：

D1. $\rho-1<(A_{n+1}-A_n)\ \mathrm{mod}\ M<M-(\rho-1)\ \forall n$

A_{n+1} 与 A_n 不属于同一校验节点。

D2. $\rho-1<(A_{n+2}-A_n)\ \mathrm{mod}\ M<M-(\rho-1)\ \forall n$

A_{n+2} 与 A_n 不属于同一校验节点。

为了分析的方便，我们采用(1)式进行讨论。首先讨论满足 D1 以及 D2 的条件，显然 $(A_{n+1}-A_n)\ \mathrm{mod}\ M=k(n+1)\ \mathrm{mod}\ M$，以及 $(A_{n+2}-A_n)\ \mathrm{mod}\ M=k(2n+3)\mathrm{mod}\ M$。可以看到，由于映射后相邻序列之间的距离满足线性关系，调整 k 的值不能完全消除二线循环。为了消除二线循环，我们采用下面的算法去除二线循环，具体步骤如下：

1、在校验矩阵 H 中，找出列重量小于 λ 的列 $c_0,\cdots,c_{L-1}$；

2、找出行重量小于 ρ 的行 $r_0,\cdots,r_{P-1}$，显然行数等于列数，即 $L=P$；

3、校验矩阵 H 需要在对应的行与列中增加重量 1，即把其中的一个 0 变为 1，从 r_0 行开始，在 $c_0,\cdots,c_{L-1}$ 列中寻找 $H(r_0,c_i)=0$ 的列 c_i，使得 $H(r_0,c_i)=1$；对于 r_1 行，从剩余的列中找出 $H(r_0,c_j)=0$ 的列 c_j，并改变 $H(r_1,c_j)=1$；依次类推，补完 L 个 1，就得到了无二线循环的校验矩阵。

说明：对于步骤 3，可以采用随机的方法进行列的选取，则得到具有随机性的校验矩阵；也可以按照顺序选取列，此时得到确定性的校验矩阵，本文实验采用顺序进行补“1”处理。

4 仿真与分析

根据以上方法，我们采用二次同余序列设计规则 LDPC 码。选取 N=432 以及 N=2048 两种分组长度进行仿真，$\lambda=3$，$\rho=6$，编码效率为 $\frac{1}{2}$，采用和积算法进行译码，BPSK 调制方式，加性高斯白噪声信道。我们分别测试了采用随机方法与二次同余方法的误码率性能。其仿真结果如图 2、3 所示。可以看到：与随机方式构成的 LDPC 码相比，本文提出的通过二次同余序列构成 LDPC 码具有近似的性能；但本文提出的方法在实际应用中只需要存储几个参数，就能即时生成校验矩阵，节省了存储空间，便于实际应用，因此说本文提出的二次同余序列设计 LDPC 码是一种较优的方法。

结论 本文提出了一种二次同余序列设计 LDPC 码的方法，并提出了消除二线循环的方法。和以前关于采用随机方法构造 LDPC 码相比，我们得到了一种确定性的规则 LDPC 码的设计方法，在实际应用中，不需要存储校验矩阵，节省了存储空间；同时该方法能得到与随机方法一样的性能，无论从应用实现还是性能方面看，都是一种较优的设计方法。

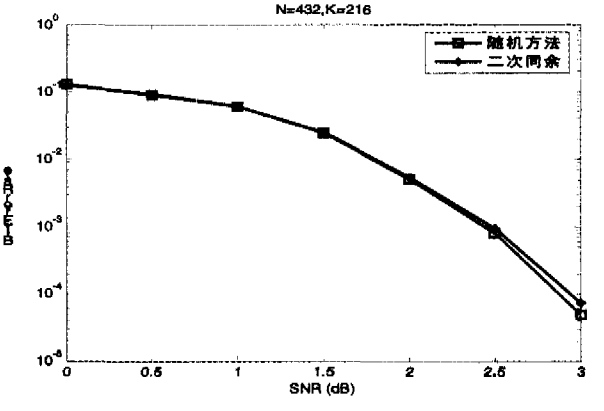

图 2 长度 N=432，K=216 的性能曲线(50 次迭代)

(下转第 295 页)

资源-客体教学区，客体教学区-用户的分阶段授权方式，利用客体教学区这一中间层就可以屏蔽访问控制机制的异构。主体教学区可以用本地的方式决定将资源共享给哪些客体教学区并拥有最终控制权，它不必关心客体教学区中用户的具体信息，所使用的访问控制策略以及组织结构，客体教学区的有关变动对资源共享不会带来任何影响。同样，客体教学区对所获得的共享资源在本教学区内使用，可以依据自己的访问控制策略、组织结构、用户信息对资源进行分配，主体教学区的内部变化对资源共享也不会带来任何影响。

在现实生活中，各个教学区中的教育资源一般都能够为它的所有者带来一定的经济效益，教学区之间的资源共享必然是以对经济效益的分配约定为前提的，当这种约定改变时，所有者为中心的基于角色的层次访问控制策略就能方便主体教学区将资源的访问权限收回或加以进一步的限制，这就同时保证了访问控制策略的灵活性、可扩展性、通用性和自主性。

2.4 统一的身份认证机制

统一的身份认证机制是指用户可以在任何地点、通过任何接入设备登录基于网格计算的远程教育系统，但用户不会因为地理位置的差异和接入设备的区别而看到不同的内容。由于用户的登录行为可能随时发生在网格的任一节点，最简单的方法是在每一个节点都记录所有的用户信息，但用户数量十分巨大，这个方法显然是不可行的。另外一种方法是所有的用户信息都分别存储在每个教学区的用户数据库中，这样虽然提高了效率，但当某个教学区增加用户时就需要将用户的信息通过网络通知其他所有的用户数据库，这是十分危险的。

通过观察分析，在某个教学区中的用户，一般情况下只在该教学区中的某一节点执行登录操作。所以基于这一出发点，考虑只把用户注册在本地教学区中，这样在绝大多数情况下都可以直接在本地进行登录处理，减少了在网络中传播用户信息的危险。

但在极少数情况下，用户会在其他教学区中登录系统，这时，登录教学区就找不到用户信息，需要执行远程登录的步骤。首先，要求用户输入所属教学区的名字，然后由登录教学区将用户名和密码传送到目标教学区中进行身份认证并返回结果。如果认证通过，目标教学区会将用户的权限等信息传给登录教学区，用户就可以在登录教学区中进行登录。当用户退出远程教育系统时，登录教学区就将相关信息删除。

3 模型评价

① 以教学区为单位划分教育资源的归属，符合现实社会中资源都属于某些人或某些组织的情况，方便资源所有者对资源进行管理。

② 分层次的分布式元信息数据库结构，避免了数据备份引起的不一致问题以及数据在网络中传输的安全问题。

③ 资源三重命名空间使资源的所有者和使用者可以按各自的习惯对资源命名，任何一方对资源名称的修改都不会影响另一方对资源的使用。

④ 以服务方式封装了对用户和应用访问数据资源请求的响应过程，可以方便地构造统一的数据访问接口，还降低了集成遗留系统的复杂度。

⑤以所有者为中心的基于角色的层次访问控制策略，将授权的过程分成两个阶段进行，这样，不同教学区之间异构的安全机制就不需要转换，还降低了授权的工作量。

⑥用户管理采取分教学区分布式管理的模式，将登录分为本地登录和远地登录两种，降低了构造统一身份认证机制的难度，避免了建立全局统一用户数据库的麻烦。

结束语 基于网格计算的远程教育系统模型具有较高的研究价值，随着网格技术的发展及其应用的逐渐深入，我们深信，在不久的将来它必将获得飞跃的发展，并为网络远程教育注入新的活力。

参 考 文 献

1 徐志伟，冯百明，李伟. 网格计算技术[M]. 北京：电子工业出版社，2004
2 Foster I, Kesselman C. 金海，等译. 网格计算(第二版)[M]. 北京：电子工业出版社，2004
3 welch V, et al. Security for Grid Services. http://xxx.lanl.gov
4 Baker R, et al. A Model for Grid User Management [J]. Computer in High Energy and Nuclear Physics, California, March, 2003
5 Mcnab A. Grid based Access Control for Unix environments, Filesystem and Web Sites. http://. xxx. lanl. gov

(上接第 292 页)

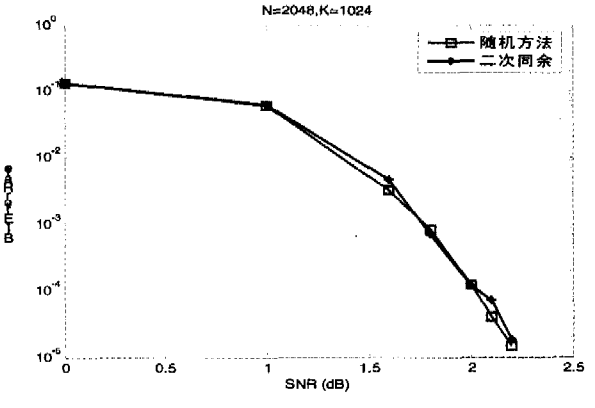

图 3 长度 N=2048，K=1024 的性能曲线(30 次迭代)

参 考 文 献

1 Gallager R G. Low Density Parity Check Codes [J]. IRE Trans on Information Theory, 1962, 8(3):208～220
2 Gallager R G. Low Density Parity Check Codes [M]. Cambridge, Mass: MIT Press, 1963
3 Berrou C, Blavieux A, Thitimajshima P. Near Shannon Limit Error Correcting Coding and Decoding: Turbo Codes [A]. In: Proc. 1993 IEEE International Conference on Communications [C]. Geneva, Switzerland, 1993. 1064～1070
4 Mackay D J C. Good Error Correcting Codes Based on Very Sparse Matrices [J]. IEEE Trans on Information Theory, 1999, 45(2):399～431
5 Richardson T, Urbanke R. Capacity of low-density parity-check codes under message passing decoding, IEEE Trans. Inform. Theory, Feb. 2001, 47:599～618
6 Prabhakar A, Narayanan K. Pseudorandom Construction of Low-Density parity-check codes using Linear Congruential sequences, IEEE. Trans on commu. Sep. 2002, 50(9)
7 Teng H, Xu J, Lin S, Abdel-Ghaffar A S. Codes on Finite Geometries, IEEE Transaction Theory, Feb. 2005, 51(2):572～596