综述

调和分析与信道编解码研究

献给陆善镇教授 75 华诞

湛稳固*, 吴国清

北京应用物理与计算数学研究所, 北京 100088

E-mail: chenwg@iapcm.ac.cn, wu-guoqing@iapcm.ac.cn

收稿日期: 2013-08-19; 接受日期: 2013-08-25; * 通信作者

国家自然科学基金 (批准号: 10931001, 11371183, 11271050 和 61003083)、中国工程物理研究院科学技术发展基金 (批准号: 2012B0202024 和 2013B0403068) 和北京数学与信息交叉科学 2011 协同创新中心资助项目

摘要 信道编码是通信系统的关键技术之一, 其传统的理论工具是代数和有限域 $GF(p)$. 本文在有噪信道的信道编码数学模型基础上, 介绍基于调和分析的新型信道编码理论, 分别应用调和分析的重要工具压缩感知与 Walsh-Hadamard 变换实现信道编解码和信道编码盲识别. 本文综述基于调和分析的信道编码的一些基本结果并介绍最新进展, 主要包括: Gilbert-Varshamov 界、 l_1 解码、RIP (restricted isometry property) 条件和 Walsh-Hadamard 变换等.

关键词 调和分析 信道编码 压缩感知 Walsh-Hadamard 变换

MSC (2010) 主题分类 65T50, 68P30

1 引言

在高速通信过程中, 信号无论是经过有线信道传输还是无线信道传输, 不可避免地会受到信号衰落、噪声和人为的干扰, 影响信号传输质量, 使得接收到的数据出现差错. 信道编码 (也称差错控制编码) 的作用就是控制数字信号的差错, 提高传输可靠性, 实现高速稳定通信. 它的原理是通过在发送端传输的信息码组中附加一些监督码元, 这些多余的码元与信息码元之间以某种确定的规则相互关联, 接收端根据相应的规则检验信息码元与监督码元之间的关系, 一旦传输过程中发生差错, 则信息码与监督码之间的关系将受到破坏, 从而可以发现错误, 甚至纠正接收码组中的误码, 使得噪声干扰造成的损失降至最低. 因此, 信道编码已经成为高速通信系统的关键技术之一.

信道编码的应用范围越来越广, 应用层次也越来越深. 例如, 无线网络和卫星通信都属于误码率高的通信网络; 带宽不确定性和信道噪声的存在会导致传输过程中数据的丢失和错误的产生. THz (time terahertz) 通信在雨雾环境中, 信号衰减较大, 为了保证信号在经过恶劣的传输信道之后, 微弱的信号码流或者掺杂了干扰信号的码流在接收端能够被正确译码, 必须采用信道编码来减少信号传输的误码率. 我们在进一步扩大通信容量或加大通信距离时, 也可以在基本不增加射频系统经费投入的情况下, 采用信道编码获得可贵的高编码增益. 在信息安全领域, 信道编码也发挥了重要作用. 在数据存储系统的存储介质 (如硬盘和 DVD 等) 中, 由于制造工艺的限制和人为操作不当, 也会使存储的数据发生

错误, 可以采用信道编码技术对存储介质进行误码纠错, 从而达到保护数据信息的目的. 在信息对抗领域, 一方面, 通过研究代数编码理论, 设计出性能优异的信道编码, 增强己方信号的隐蔽性和可靠性; 另一方面, 通过研究差错控制机理, 从而设计出有效的算法, 迅速判别出敌对方信号所采用的编码类型和编码参数, 再通过解码还原其原始信息.

本文主要介绍基于调和分析发展的新颖信道编码理论, 介绍当前的一些研究进展及问题. 本文结构如下: 第 2 节介绍信道编码的数学模型; 第 3 节介绍如何利用调和分析理论的重要工具压缩感知求解该数学模型, 并实现不同于传统基于代数和有限域工具的信道编码方法; 第 4 节介绍信道编码的反问题 - 信道编码盲识别, 并利用调和分析理论的重要工具 Walsh-Hadamard 变换来求解该问题; 最后, 第 5 节总结全文.

2 信道编解码的数学模型

差错控制编码的目的是设计和实现成对的信道编码和译码器, 使得信息可以在有噪环境下尽可能地传输或记录; 信息在信道译码器的输出端能够可靠地重现; 将实现编码器和译码器的代价降低到可接受的范围内, 其传统的理论工具是代数和有限域 $GF(p)$ [1, 2]. 对有噪信道中信道编解码可以建立以下数学模型, 对输入信息向量 f (也称为“明文”), 设 f 是 n 维向量, 设计编码器或编码矩阵 A 是一个 $m \times n$ 编码矩阵 (通常 $m > n$), 接收信息为 m 维向量 $y = Af$ (也称为“密文”). 如果 A 满秩, 显然可以由 Af 恢复 f . 由于受到有噪信道干扰, 接收信息 $y' = Af + e$, e 是误码向量, 由 y' 恢复 f , 这就是信道解码问题. 本文主要考虑有噪信道解码问题, 即是否有可能从数据 y' 准确恢复 f . 如果能, 怎样恢复? 如果当误码向量 e 至多有 r 个非零元时, 都可以从接收信息 $Af + e$ 恢复原始信息向量 f , 则称其为一个 (m, n, r) 码, n/m 称为码率, $\rho = r/m$ 称为误码率. 显然, 如果误码个数 r 所占比例过大, 是无法正常恢复 f 的. 例如, 当 $n + 2r > m$ 时, 由基本的线性代数知识, 存在原文 $f, f' \in \mathbb{R}^n$ 和具有至多 r 个非零元的 $e, e' \in \mathbb{R}^m$, 使得 $Af + e = Af' + e'$, 即信息向量的解不唯一. 特别地, 如果误码率 $\rho = \frac{r}{m}$ 超过 $1/2$, 则不论码率多大, 都不可能构成一个 (m, n, r) 码. 这提出一个重要的问题: 对多大误码率 ρ , 解码是可能的或存在 (m, n, r) 码, 且有复杂度至多是码长 m 的多项式阶的译码算法?

令 $y = Af$, 设 $Y \subset \mathbb{R}^m$ 是 A 的像集, 可以把上述问题重新表述: 已知一个向量 $y' \in \mathbb{R}^m$, 怎样在 $\mathbb{R}^m$ 的一个 n 维子空间 Y (码字集合) 中重构码字 y , 使得 y 与 y' 的汉明 (Hamming) 距离 $d(y, y') \leq r$?

如果 A 是随机矩阵 (如 Gauss 随机矩阵), 只要满足条件 $n + 2r \leq m$, 则在信息论意义下一定可以区分所有明文. 然而, 这个结论并没有提供怎样从有误差的密文 $Af + e$ 恢复明文 f 的算法. Gilbert-Varshamov 界定理说明信道编码的码率具有下界.

定理 2.1 [3, 4] (Gilbert-Varshamov 界) 构造具有多项式时间复杂度的编解码算法, 编码参数必须满足 Gilbert-Varshamov 条件, 即

$$\frac{n}{m} \geq 1 - H\left(\frac{Cr}{n}\right),$$

其中, $H(x)$ 表示熵函数, C 为正常数.

3 基于调和分析的信道编解码方法

经典的 Shannon 采样定理是信息科学中最基本的结果之一, 是现代脉冲编码调制通信系统的理论基础. 文献 [5, 6] 提出了压缩感知理论 (compressed sensing, CS), 应用调和分析理论证明了, 在确保

恢复误差很小的条件下, 可以用远低于常规方法所需的样本数量高概率地重构一类稀疏或可以压缩的信号和图像. 压缩感知是 Shannon 采样定理的革命性理论, 并迅速成为信号和图像处理领域的研究热点. 压缩感知理论中关于稀疏性、随机性和凸最优化的结论可以直接应用于设计差错控制编码. 本节介绍 Candes 和 Tao^[7,8] 如何把压缩感知方法成功应用于差错编解码问题.

为了从接收到的有误差数据 $y' = Af + e$ 恢复原始信息 f , 考虑解以下 l_1 - 极小问题:

$$(P_1) \quad \min_{\tilde{f} \in \mathbb{R}^n} \|y' - A\tilde{f}\|_{l_1}$$

或等价地,

$$(P'_1) \quad \min_{\tilde{y} \in Y} \|y' - \tilde{y}\|_{l_1}.$$

这样, (P'_1) 的极小子 y^* 是 y' 到向量空间 Y 上对于 l_1 模的投影, 它可以等价为一个线性规划 (LP) 问题. 事实上, l_1 - 极小问题 (P_1) 等价于

$$\min \sum_{i=1}^m t_i, \quad -t \leq y' - A\tilde{f} \leq t,$$

其中, 优化变量是 $t \in \mathbb{R}^m$ 和 $\tilde{f} \in \mathbb{R}^n$ (向量 $x \leq y$ 是指对所有坐标 i , $x_i \leq y_i$). 因此, (P_1) 是一个带不等式约束条件的 LP, 可以利用成熟的优化算法有效求解.

Candes 和 Tao 证明了, 对编码矩阵 A 加适当条件, 只要误差向量 e 的支集不太大, 信道编解码问题具有唯一解. LP 的解 f^* 实际上是真正的解 $f^* = f$ (等价地, $y^* = y$). 为了求解 f , 关键是求解误差向量 e , 一旦 e 确定, 则 $Af = y' - e$ 也可知, 因此, f 可求解出来. 方法是构造满足 $BA = 0$ 的矩阵 B , 作用 B 于等式两端 $y' = Af + e$, 得到 $\tilde{y} = By' = B(Af + e) = Be$, 于是重构 f 的问题转化为从观测到的 $Be = By'$ 重构稀疏向量 e , 这完全可以应用压缩感知方法实现求解.

对欠定线性方程组 $Be = By'$, 在所有满足 $Bd = By'$ 的向量 $d \in \mathbb{R}^m$ 中, 最稀疏解由

$$(P_0) \quad \min_{d \in \mathbb{R}^m} \|d\|_{l_0} \quad \text{满足} \quad Bd = By'$$

给出, 其中, $\|d\|_{l_0}$ 表示 d 的零范数, 即其中非零元素的个数. 据我们所知, 解这个问题本质要求对 B 的列的所有子集的穷尽搜索, 过程本质上是组合的, 有指数复杂度. 能否找到一个更为有效的解码算法? 考虑以下 l_1 - 极小模:

$$(P''_1) \quad \min_{d \in \mathbb{R}^m} \|d\|_{l_1} \quad \text{满足} \quad Bd = By'.$$

与 l_0 - 模枚举非零坐标不同, l_1 - 模是凸的. (P''_1) 等价于 (P_1) 或 (P'_1) , 也可以改写为一个线性规划 (LP).

为了方便阐述解的存在唯一性, 首先介绍受限等距常数概念. 对一个 $p \times m$ 矩阵 B , $T \subset \{1, \dots, m\}$, 令 B_T 是一个 $p \times |T|$ 子矩阵, 由 B 中指标属于 T 的列组成.

定义 3.1 矩阵 B 的 S - 受限等距常数 δ_S 是使得不等式

$$(1 - \delta_S)\|c\|_{l_2}^2 \leq \|B_T c\|_{l_2}^2 \leq (1 + \delta_S)\|c\|_{l_2}^2$$

对所有子集 T ($|T| \leq S$) 和序列 $(c_j)_{j \in T}$ 都成立的最小常数.

对于信道编解码问题解的存在唯一性, Candes 和 Tao^[7,8] 给出了如下结论.

定理 3.2 设 $f \in \mathbb{R}^n$, A 是一个 $m \times n$ 矩阵, $e \in \mathbb{R}^m$ 至多有 r 个非零坐标. 令 $y' = Af + e$, B 是一个矩阵, 满足 $BA = 0$ 且满足条件

$$\delta_{3r} + 3\delta_{4r} < 2,$$

则 (P_1'') 的解唯一且等于 e , 或 (P_1) 和 (P_1') 的解唯一且分别等于 f 和 y . 特别地, A 是一个 (m, n, r) -码, (P_1) 为精确恢复算法.

该结果表明, 不论误差结构怎样, 只要误差向量的支撑不太大, 通过极小化 l_1 -模, 能恢复所有信号 $f \in \mathbb{R}^n$. 定理要求矩阵 B 具有好的受限等距常数 δ_S , 怎样构造矩阵 B , 使之对尽量大的 S 满足定理条件是一个复杂的问题, 详细介绍参见文献 [9–11]. 下面定理表明一个 $m \times n$ Gauss 随机矩阵高概率地为 (m, n, r) 码, 因为 Gauss 随机矩阵的零化子 B 可以选取为另一个 Gauss 随机矩阵.

定理 3.3 假设 $n < m$, $p = m - n$, B 是一个 $p \times m$ Gauss 随机矩阵, 即元素是独立随机变量, 服从期望为 0、方差为 $\frac{1}{p}$ 的 Gauss 分布, 则定理 3.2 的条件满足的概率不小于

$$1 - e^{-\alpha m}$$

对某个常数 $\alpha > 0$, 只要 $r \leq \rho^* m$, ρ^* 只依赖于码率 $\frac{n}{m}$.

如下定理表明, 对于 Gauss 随机矩阵, 当误差支撑 r 小时, 可以接近理论极限 $n + 2r \leq m$.

定理 3.4 假设 $n, m, r < cm$ 是正整数使得

$$m = n + R, \quad R \geq Cr \log(m/r). \quad (3.1)$$

设 G 是一个 $m \times n$ 矩阵, 其元素是独立随机变量, 服从标准正态分布. 则矩阵 G 是一个 (m, n, r) 码的概率不小于

$$1 - e^{-cR},$$

且 (P_1') 为精确恢复算法.

定理 3.4 中的假设 (3.1) 相差一个常数倍达到了 Gilbert-Varshamov 界.

前面介绍了基于调和分析的信道编解码原理, 其关键在于编码矩阵 A 和零化子 B 的构造. 此外, 在解码过程中还要求解最优化问题, 下面介绍一些实用算法: 基追踪算法 (basis pursuit, BP) [12, 13] 和贪婪算法 (matching pursuit, MP) [14, 15] 等. BP 算法的基本思想是, 利用凸的 l_1 范数对非凸的 l_0 范数进行松弛, 从而将 (P_0) 转化为 (P_1') , 更进一步, 凸规划 (P_1') 可以等价于线性规划 (LP), 然后应用单纯形算法或内点法加以解决. 贪婪算法的具体实现有正交贪婪算法 (OMP)、规整化正交贪婪算法 (ROMP) 和分段正交贪婪算法 (STOMP) 等. BP 算法与 MP 算法相比较, BP 算法求解全局最优解, 理论性能好, 但计算时间复杂度高; MP 算法用局部最优解逼近全局最优解, 计算时间复杂度较低, 但稳定性差.

4 基于调和分析的信道编码反问题求解

我们在第 3 节介绍了基于调和分析的信道编解码方法. 进一步的问题是, 如果编码矩阵 A 也未知, 如何由 y' 恢复明文信息 f 和编码矩阵 A ? 即仅由接收到的信息序列, 识别编码矩阵 A 和其他编码参数 m 和 n , 进而解码恢复信息序列 f , 这就是信道编码盲识别问题, 它在通信对抗中具有重要意义. 非合作方为了解译陌生信号中隐含的信息向量, 必须针对截获的数字信号, 设计算法判别出其采用的编码参数, 它是恢复原始信息的前提.

目前常用的信道编码有 BCH (Bose-Chaudhuri-Hocquenghem) 码、RS (Reed-Solomon) 码、卷积码、Turbo 码和 LDPC (low-density parity-check) 码等, 其中, BCH 码和 RS 码都属于线性分组码, 在短码和中等码长下, 具有很好的纠错性能; 卷积码在编码过程中引入了寄存器, 增加了码元之间的相关

性, 在相同复杂度下可以获得比线性分组码更高的编码增益, 但是这种相关性同时也增加了分析和设计卷积码的复杂度. 卷积码是 1955 年 Elias^[16] 最早提出, 稍后, 1957 年 Wozencraft^[17] 提出了一种有效译码方法, 即序列译码. 1963 年 Massey^[18] 提出了一种性能稍差, 但比较实用的门限译码方法, 由于这一实用性进展使卷积码从理论走向实用化. 而后, 1967 年 Viterbi^[19] 提出了最大似然译码法. 它对存储器级数较小的卷积码的译码很容易实现, 人们后来称为 Viterbi 算法或 Viterbi 译码, 并广泛地应用于现代通信中. 关于卷积码的详细内容参见文献 [20–22]. 本节介绍利用调和分析理论的重要工具 Walsh-Hadamard 变换来求解卷积码编码参数. 先介绍一些概念, 用来描述主要问题.

设 F 是二元域, $F[D]$ 为多项式环, $F(D)$ 是有理函数域. 称 $F(D)^m$ 的任意一个 n 维子空间 C 是码率为 n/m 的卷积码. 如果 $G(D)$ 是 $F(D)$ 上的矩阵且行向量构成了 C 的一组基, 则称 $G(D)$ 是 C 的一个生成矩阵. 如果 $G(D)$ 是多项式生成矩阵, 且 $G(0)$ 是满秩的, 则称 $G(D)$ 是编码矩阵. 如果 $G(D)$ 是编码矩阵, 且存在右逆, 则称 $G(D)$ 是基本编码矩阵. (m, n, k) 卷积码的编码器是由一个有 n 个输入位, m 个输出位, 且具有 k 节移位寄存器所构成的有限状态的有记忆系统, 通常称为时序网络.

我们要解决的主要问题是, 设 S 是有误码的卷积码序列, 由 S 确定源卷积码 C 的码长 m , 信息长度 n , 最后找出生成矩阵, 这就是卷积码的盲识别问题.

以码率 $(m-1)/m$ 为例 (实际应用中, 利用码率 $1/2$ 的源码来生成 $(m-1)/m$ 码率的目标删除码是最常见最实用的情形). 设校验多项式为

$$H(D) = [H^{(1,1)}(D)H^{(1,2)}(D)\cdots H^{(1,m)}(D)],$$

其中,

$$H^{(1,i)}(D) = h_{0,i} + h_{1,i}D + h_{2,i}D^2 + \cdots + h_{d,i}D^d, \quad 1 \leq i \leq m,$$

$$d = \max_{1 \leq i \leq m} (\deg H^{(1,i)}(D)).$$

考虑两种情形:

(1) 无误码情形. 此时接收信号字序列 $R(D)$ 即为码字序列, 从而,

$$R(D) = V(D) = [r_1(D) r_2(D) \cdots r_m(D)],$$

$$r_i(D) = r_{0,i} + r_{1,i}D + r_{2,i}D^2 + \cdots, \quad 1 \leq i \leq m.$$

根据码字与校验矩阵之间的约束关系 $V(D)H(D)^T = 0$ (T 表示矩阵的转置), 有

$$[r_1(D) r_2(D) \cdots r_m(D)][H^{(1,1)}(D) H^{(1,2)}(D) \cdots H^{(1,m)}(D)]^T = 0$$

$$\Leftrightarrow \sum_{j=1}^m r_j(D) H^{(1,j)}(D) = 0$$

$$\Leftrightarrow \sum_{j=1}^m \left(\sum_{i=0}^{\infty} r_{i,j} D^i \cdot \sum_{i=0}^d h_{i,j} D^i \right) = 0.$$

把频域多项式乘法回到时域, 可归结为求解如下的线性方程组:

$$(D^k): \quad \sum_{j=1}^m \sum_{i=0}^d h_{i,j} r_{k-i,j} = 0, \quad k = d, d+1, \dots, d+N,$$

这里设码字序列长度为 $(d + N + 1)m$. 把线性方程组写成如下的矩阵形式:

$$\begin{bmatrix} r_{d,1} & \cdots & r_{0,1} & \cdots & r_{d,m} & \cdots & r_{0,m} \\ r_{d+1,1} & \cdots & r_{1,1} & \cdots & r_{d+1,m} & \cdots & r_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ r_{d+N,1} & \cdots & r_{N,1} & \cdots & r_{d+N,m} & \cdots & r_{N,m} \end{bmatrix} \begin{bmatrix} h_{0,1} \\ \vdots \\ h_{d,1} \\ \vdots \\ h_{0,m} \\ \vdots \\ h_{d,m} \end{bmatrix} = 0, \quad (4.1)$$

简记 (4.1) 为

$$R \cdot x^T = 0.$$

该线性方程组共有 $N + 1$ 个方程, $(d + 1)m$ 个未知量 $\{h_{0,1}, \dots, h_{d,1}, \dots, h_{0,m}, \dots, h_{d,m}\}$. 要使方程组 (4.1) 可解, 一般要求 $N \geq (d + 1) \times m$. 卷积码的盲识别需要构造算法, 选取正确的参数 d 和 m (这些参数均未知), 构造恰当的系数矩阵 R , 求解线性方程组 (4.1), 选取 (极小) 校验矩阵. 实际问题中, $d < 15$, $m \leq 8$. 一般可以使用 Gauss 消元法求解 (4.1), 求解速度也比较快.

(2) 有误差情形. 此时接收的信号字序列 $R(D) = V(D) + e(D)$, $e(D)$ 为误差多项式. 校正子

$$R(D)H(D)^T = S(D) \neq 0 \quad (\text{如果 } e(D) \neq 0).$$

所以, (4.1) 是容错线性方程组. 卷积码的盲识别需要构造算法, 求解容错线性方程组 (4.1) (求解方程成立个数最多的解向量), 选取校验多项式矩阵.

线性方程组 (4.1) (包含容错情形) 的求解可应用 Walsh-Hadamard 变换. Walsh-Hadamard 变换是连续信号中 Fourier 变换的离散模拟, 所以也称为离散 Fourier 变换, 用来作脉冲信号的频谱分析. 定义参见文献 [2, 23, 24].

Walsh-Hadamard 变换是由 Walsh-Hadamard 矩阵定义的, 而 $2^n \times 2^n$ 阶 Walsh-Hadamard 矩阵 $H(n)$ 由下列递推方式确定:

$$H(0) = [1], \quad H(n) = \begin{bmatrix} H(n-1) & H(n-1) \\ H(n-1) & -H(n-1) \end{bmatrix}.$$

由这个递推公式, 可得

$$H(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H(2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

设 $\{f(k)\}$ ($k = 0, 1, \dots, N - 1, N = 2^{n-1}$) 为数据向量, 则向量

$$\{F(k)\} = \frac{1}{N} H(n-1) \{f(k)\}$$

称为 Walsh-Hadamard 变换. 下面介绍 Walsh-Hadamard 矩阵的重要性质和应用.

$H(n)$ 的第 u 行 v 列元素为

$$h_{uv} = (-1)^{\vec{u}_n \cdot \vec{v}_n^T}, \quad u, v = 0, 1, \dots, 2^n - 1,$$

其中,

$$(\vec{u}_n)_{\text{二进制}} = (u_{n-1}u_{n-2} \cdots u_0) = (u)_{\text{十进制}},$$

$$(\vec{v}_n)_{\text{二进制}} = (v_{n-1}v_{n-2} \cdots v_0) = (v)_{\text{十进制}}.$$

因为

$$h_{uv} = \begin{cases} 1, & \text{如果 } \vec{u}_n \cdot \vec{v}_n^T = 0, \\ -1, & \text{如果 } \vec{u}_n \cdot \vec{v}_n^T = 1. \end{cases}$$

所以, Walsh-Hadamard 矩阵中的行向量 h_u 表示了与 u 的二进制表示的向量 $\vec{u}_n$ 相乘为 0 的所有解的情形, 即使

$$\vec{u}_n \cdot x^T = 0$$

的解是 h_u 中为 1 的列的位置 v 的二进制表示 $\vec{v}_n$. 当求一个方程

$$\vec{u}_n \cdot x^T = 0$$

的解时, 可以将 $\vec{u}_n$ 化为十进制数 u , 在 $2^n \times 2^n$ 的 Walsh-Hadamard 矩阵中找到第 u 行, 该行为 1 的位置 v 的二进制表示的向量 $\vec{v}_n$ 就是方程的解, 这样的解有 2^{n-1} 个. 这里仅考虑了一个方程的情形, 当考虑方程组情形时, 可以将相应的 Walsh-Hadamard 矩阵的行向量在实数域相加, 得到的新的行向量中值为方程个数的元素的位置 v 的二进制表示的向量就是方程的解, 即按以下步骤求解二元域上的方程组 (对应方程组 (4.1), 以下 $n = (d+1)m$):

第 1 步 将每个方程的系数向量表示为十进制数, $N+1$ 个方程就得到 $N+1$ 个十进制数.

第 2 步 用这些十进制数构造一个新的 2^n 维向量 A' . 构造方法是将与十进制数对应的向量 A' 中的位置设为 1, 其余设为 0.

第 3 步 按以下公式计算 2^n 维实数域向量 B' :

$$A' \times H(n) = B'.$$

第 4 步 检查向量 B' , 如果 B' 中有等于方程个数的元素, 则该元素的位置 u 的二进制表示的向量 $\vec{u}_n$ 就是方程组的解 (可能有多个解). 如果 B' 中除了第 0 列外, 所有元素都小于方程个数, 则该方程组无解.

下面用简单的例子说明此过程.

例 1 求

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} B = 0$$

的解.

解 将 101, 110 和 011 化为十进制数分别为 5, 6 和 3. 构造新向量 (0, 0, 0, 1, 0, 1, 1, 0), 将新向量与 8×8 的 Walsh-Hadamard 矩阵相乘:

$$[0, 0, 0, 1, 0, 1, 1, 0] \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} = [3, -1, -1, -1, -1, -1, -1, 3],$$

结果第 0 列和第 7 列最大为 3, 所以, 解为 $[0, 0, 0]^T$ 和 $[1, 1, 1]^T$ (第 0 列除外, 因为 0 向量是任何方程的解).

上面第 3 步求 B' 就是求 A' 的 Walsh-Hadamard 变换, B' 就是谱系数. 在本文的应用中, 谱系数 B' 具有明显的物理意义, 前面已指出, 如果 $h_{uv} = 1$, 则表示 $\vec{u}_n \cdot \vec{v}_n^T = 0$; 如果 $h_{uv} = -1$, 则表示 $\vec{u}_n \cdot \vec{v}_n^T = 1$. 所以, B' 的物理意义就是, B' 中的每个元素的值表示该元素位置 u 的二进制表示的向量 $\vec{u}_n$ 使方程组成立的方程个数与不成立方程个数之差. 由于求解方程组的过程就是 Walsh-Hadamard 变换, 可以利用快速 Walsh-Hadamard 变换减少计算量, 使总计算次数从 N^2 降到 $N \log N$.

对谱系数 B' 的物理意义有了清楚的认识后, 可以将 Walsh-Hadamard 变换求解方程组的方法推广到方程组中含有错误方程的情况, 对于容错方程组, 其最可能的解就是最大谱系数对应位置 u 的二进制表示的向量 $\vec{u}_n$. 可按以下步骤求解二元域上的容错方程组:

第 1 步 将每个方程 (可能含错) 的系数向量表示为十进制数, $N+1$ 个方程就得到 $N+1$ 个十进制数.

第 2 步 用这些十进制数构造一个新的 2^n 维向量 A' . 构造方法是将与十进制数对应的向量 A' 中的位置设为 t (t 是这个十进制数出现的次数), 其余设为 0.

第 3 步 按公式 $A' \times H(n) = B'$ 计算 2^n 维实数域向量 B' .

第 4 步 检查向量 B' , 找出 B' 中最大的元素 l , 则该元素的位置 u 的二进制表示的向量 $\vec{u}_n$ 就是方程组最有可能的解.

第 5 步 检验该结果的置信度. 当采用 Walsh-Hadamard 变换求解方程时, 由于接收卷积码序列有误差, 有必要从概率角度讨论解向量的置信度问题. 假设 $c = (c_1, c_2, \dots, c_n)$ 是 n 元容错线性方程组的解向量, 方程成立的概率为 p , 当 c 满足第 i 个方程时, 令 $\xi_i = 1$, 当 c 不满足第 i 个方程时, 令 $\xi_i = -1$, 则 $\sum_{i=1}^j \xi_i$ 的期望和方差分别为 $E(\sum_{i=1}^j \xi_i) = j(p-q)$, $D(\sum_{i=1}^j \xi_i) = 4j pq$, 其中, j 为方程个数, $q = 1-p$. 当 j 足够大时, 由中心极限定理有 $\sum_{i=1}^j \xi_i - j(p-q) / \sqrt{4j pq} \propto \mathcal{N}(0, 1)$. 设把 c 代入容错线性方程组, 方程成立的个数为 n_1 , 不成立的个数为 n_2 . 令 $z = n_1 - n_2$, 计算统计量:

$$T = z - \frac{j(p-q)}{\sqrt{4j pq}}. \quad (4.2)$$

如果显著性水平为 α , 则

$$\frac{\alpha}{2} = 1 - F(t), \quad (4.3)$$

其中, $F(t)$ 是 t 的概率分布函数. 由 (4.3) 可以解出一个标准 t . 在求解容错线性方程组时, 要求 $T \geq t$. 取 $p = q = 0.5$, 则 $T = z/\sqrt{j}$. 可以根据此式来判别解向量的置信度. 当 $t \geq 3$ 时, 错误概率为 0.00135, 在数学上一般称为不可能事件.

例 2 (实例分析) 下面以 $(2, 1, k)$ 卷积码盲识别的计算实例说明上述方法的正确性. 在误码率为 10^{-2} 情况下获取一段码序列如下:

1 0 1 0 1 1 0 1 0 1 1 1 1 0 0 0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1.

按照文中办法对以上数据作 $2^8 \times 2^8$ 阶 Walsh-Hadamard 变换, 其中共有 7 组解向量的 T 大于阈值. 解向量不唯一是由于构造系数矩阵时将编码约束度估计过大引起的. 此时仅需求出任意一组解向量的最大公因式, 排除产生第一类无限误差传播的编码矩阵即可. 最终可以识别出此卷积码的编码矩阵为 $G(D) = [1 + D + D^2 + D^3, 1 + D + D^2]$.

再对 $(2, 1, k)$ 卷积码进行仿真实验. 针对不同误码率和不同编码约束度, 用 Matlab 各生成 1000 组仿真数据, 通过 Monte Carlo 仿真实验统计了识别概率. 仿真实验表明, 在误码率为 10^{-2} 情况下该算法的正确率能达到 90% 以上. 该方法对 $(2, 1, k)$ 的卷积码实现了有效识别, $1/m$ 的卷积码可以看成 $m-1$ 个 $1/2$ 卷积码的组合, 也可实现盲识别.

5 总结

本文介绍了基于调和分析工具的信道编码理论, 分别应用压缩感知与 Walsh-Hadamard 变换实现信道编解码和信道编码盲识别, 具体阐述了调和分析工具的理论应用和研究现状. 调和分析是一个理论及应用具有广泛潜力的研究方向, 对该方向的深入研究将会促进多个理论及应用学科的发展.

致谢 本文第一作者是陆善镇教授 93 级的博士生, 在此衷心感谢导师的辛勤培养.

参考文献

- 1 万哲先. 代数与编码. 北京: 科学出版社, 1976
- 2 冯克勤, 刘凤梅. 代数与通信. 北京: 高等教育出版社, 2005
- 3 Gilbert E N. A comparison of signalling alphabets. Bell System Tech J, 1952, 31: 504–522
- 4 Varshamov R R. Estimate of the number of signals in error correcting codes. Dokl Acad Nauk SSSR, 1957, 117: 739–741
- 5 Donoho D L. Compressed sensing. IEEE Trans Inform Theory, 2006, 52: 1289–1306
- 6 Candès E, Romberg J, Tao T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete Fourier information. IEEE Trans Inform Theory, 2006, 52: 489–509
- 7 Candès E, Tao T. Decoding by linear programming. IEEE Trans Inform Theory, 2005, 51: 4203–4215
- 8 Candès E, Tao T. Near optimal signal recovery from random projections: Universal encoding strategies? IEEE Trans Inform Theory, 2006, 52: 5406–5425
- 9 许志强. 压缩感知. 中国科学: 数学, 2012, 42: 865–877
- 10 Baraniuk R G, Davenport M, DeVore R, et al. A simple proof of the restricted isometry property for random matrices. Constr Approx, 2008, 28: 253–263
- 11 Bourgain J, Dilworth S J, Ford K, et al. Explicit constructions of RIP matrices and related problems. Duke Math J, 2011, 159: 145–185
- 12 戴琼海, 付长军, 季向阳. 压缩感知研究. 计算机学报, 2011, 34: 425–436
- 13 Mallat S, Zhang Z. Matching pursuits with time-frequency dictionaries. IEEE Trans Signal Process, 1993, 41: 3397–3415
- 14 Xu Z. A remark about orthogonal matching pursuit algorithm. Adv Adapt Data Anal, 2012, 4: 1250026

- 15 Zhang T. Sparse recovery with orthogonal matching pursuit under RIP. *IEEE Trans Inform Theory*, 2011, 57: 6215–6225
- 16 Elias P. Coding for noisy channels. *IRE Conv Record*, 1955, 4: 37–47
- 17 Wozencraft J M. Sequential decoding for reliable communication. PhD Thesis. Boston: Massachusetts Institute of Technology, 1957
- 18 Massey J L. Threshold Decoding. Cambridge, MA: MIT Press, 1963
- 19 Viterbi A J. Error bounds for convolutional codes and an asymptotically optimal decoding algorithm. *IEEE Trans Inform Theory*, 1967, 13: 260–269
- 20 Lin S, Costello D J. 差错控制编码. 晏坚等译. 机械工业出版社, 2007
- 21 刘健, 王晓君, 周希元. 基于 Walsh-Hadamard 变换的卷积码盲识别. *电子与信息学报*, 2010, 32: 884–888
- 22 陆佩忠, 沈利, 邹艳, 等. 删除卷积码的盲识别. *中国科学: 信息科学*, 2005, 35: 173–185
- 23 Fino B J, Algazi V R. Unified matrix treatment of the fast Walsh-Hadamard transform. *IEEE Trans Comput*, 1976, 25: 1142–1146
- 24 游凌, 朱中梁. Walsh 函数在解二元域方程组上的应用. *信号处理*, 2000, 16: 27–31

Harmonic analysis and research on channel coding and decoding

CHEN WenGu & WU GuoQing

Abstract The channel coding is one of the key technologies in communication systems and its traditional theory is based on algebra and the finite field $GF(p)$. This paper firstly establishes the mathematical model of the channel coding in noisy cases, then introduces the novel channel coding theory based on harmonic analysis and applies important tools of harmonic analysis including compressed sensing and Walsh-Hadamard transform to achieve the decoding and blind recognition of channel coding. Some elementary results and newly progress of channel coding based on harmonic analysis are surveyed including Gilbert-Varshamov bound theorem, l_1 decoding, RIP condition, Walsh-Hadamard transform.

Keywords harmonic analysis, channel coding, compressed sensing, Walsh-Hadamard transform

MSC(2010) 65T50, 68P30

doi: 10.1360/N012013-00118