

使用边际信息降低复杂度的分阶统计软判决译码法

朱士信 虞艺超*

(合肥工业大学数学学院 合肥 230009)

摘要: 该文给出了在译码端使用边际信息缩小译码列表的算法, 深入分析了边际信息缩减译码列表的原因, 给出了基于移位寄存器序列的边际信息。相比于使用稳定信道传送边际信息的方法, 其不使用额外的信道, 不影响译码的性能与复杂度, 更易于工程实现。最后改进传统分阶统计译码法, 利用少量最可靠位作为边际信息, 显著缩减译码列表。

关键词: 列表译码; 边际信息; 移位寄存器序列; 分阶统计译码; 可靠性

中图分类号: TN911.22

文献标识码: A

文章编号: 1009-5896(2013)07-1682-05

DOI: 10.3724/SP.J.1146.2012.01595

Reduce Complexity of Ordered Statistics Soft-decision Decoding by Side Information

Zhu Shi-xin Yu Yi-chao

(School of Mathematics, Hefei University of Technology, Hefei 230009, China)

Abstract: An algorithm of complexity reduction of list decoding is given by using side information. Then in-depth analysis the reasons of complexity reduction and side information based on shift register sequence is provided. Compared with the method of using stable channel transmission side information, it does not use additional channel, and also not affect the decoding performance and complexity, more easy to engineering realization. Finally, the traditional ordered statistic decoding algorithm is improved by using a small amount of the most reliable bits as side information, thus the decoding list is significantly reduced.

Key words: List decoding; Side information; Shift register; Ordered Statistic Decoding (OSD); Reliability

1 引言

在收端的解调和译码过程中, 根据对接收码元处理方式的不同, 分为硬判决与软判决译码。与软判决译码相比, 在同一种译码算法下, 硬判决译码较为简单, 易于工程实现, 但在性能方面从理论上要损失 3 dB, 实际上损失 2 dB 左右。由于软判决译码是一个 NP 困难的问题, 其计算复杂度远远高于硬判决译码, 且随着码长的增加, 复杂度呈指数级增长。因而近些年来, 寻找次优的软判决译码算法, 来均衡误码率与计算复杂度, 一直是研究热点。其中一类是使用候选码字列表的软判决译码法^[1-7]。在这类算法中, 具有代表性的有以下几种算法: (1)文献[1]的分阶统计译码算法(OSD)及其改进译码法; (2)文献[8]中的盒子匹配(BMA)算法, 以增加空间复杂度来降低 OSD 的时间复杂度; (3)文献[9]的 3 种 chase 译码法。在这些算法提出以后,

人们对它们做了大量的研究与改进, 以降低复杂度, 同时又不会损失太多的译码性能, 然而, 对于长度大于 100 的线性码, 列表译码法的复杂度依然很高, 这就限制了列表译码法在长码译码中的应用。

文献[2]提出使用边际信息缩小译码的候选码字列表, 作者 Alnawayseh 与 Loskot 以 OSD 译码为例, 在译码端使用边际信息, 大大减小了 OSD 候选码字列表, 同时不影响误码率。他们提出的两种边际信息, 一种是对码字不重叠的区块增加校验子, 另一种是码字中选定码段的汉明重量, 两种边际信息均有效地缩小了译码列表。对于第 1 种边际信息, Alnawayseh 与 Loskot 基于增加校验位思想, 为码字中不重叠的字段各增加一个校验位, 而后用仿真实验的结果说明问题。另外他们假设边际信息使用稳定信道准确无误地发送给译码端, 这一假设过于理想化, 并且稳定的信道意味着更高的成本。

本文将增加校验位作为边际信息的译码算法推广到一般的情况, 给出列表缩减的理论说明, 并分析了列表缩减率; 给出了基于移位寄存器序列的边际信息, 节省了安全信道; 利用少量的最可靠位作

2012-12-07 收到, 2013-02-01 改回

国家自然科学基金(60973125)资助课题

*通信作者: 虞艺超 yuyichaodl@139.com

为边际信息,改进传统的 OSD 译码算法,以少量的性能损失换取 OSD 译码复杂度的降低。

2 基于边际信息的列表缩减

典型的 OSD 译码法操作如下。译码器首先对收到的码字序列 r 按可靠度降序排序,排序之后的前 k 位发生错误的概率最小。然后从排序之后的码字中找出一组最可靠的基,接下来使用列表译码。

(1)从列表选取最多可以纠正最可靠基 l 个错误的错误模式 $e \in E_L$;

(2)利用错误模式 e 生成一个测试码字 \tilde{c} , 计算它与收到序列的欧氏距离 $D_E(r, \tilde{c})$;

(3)及时更新与收到序列距离最小的码字 \tilde{c}^* , 及最小的欧氏距离 D^* ;

(4)检测最优码字是否已经找到,若没有找到,回到(1)继续从列表选取错误模式进行译码。

OSD 译码的整体复杂度与列表 E_L 的大小及码字的长度成正比,步骤(4)中的译码停止测试条件也能极大地降低译码复杂度。文献[2]仅研究使用边际信息缩小列表的平均复杂度,而不考虑译码停止的测试条件。利用额外添加的校验位作为边际信息实现如下。

设 C 是一个二元 $[n \ k \ d]$ 线性分组码, G 为它的一个生成矩阵,发送端编码器将信息 u 编为码字 c , 然后将 c 分为不重合的 l 段,每段添加一个校验子,通过一个 $n \times l$ 的矩阵 S 实现。编码器生成的码字 c 的边际信息 $s = cS$, s 通过稳定信道准确无误的传递给译码器。译码器将接收到的序列按稳定性排序,并确定一组最可靠基及其相关的生成矩阵 $\lambda(G)$ (λ 是一个列置换)。因为译码器已知发送端发送的码字满足边际校验信息 s , 从而译码器仅需测试那些满足边际校验信息的错误模式,若 $s_0 = \tilde{c}_0 S$ (\tilde{c}_0 为译码器收到的字), 那么用于测试的错误模式 e 应满足 $eS = s + s_0$, 在该前提条件下,可以略去译码列表中的许多错误模式,大大降低译码的复杂度。但是文献[2]忽略了当 S 的秩小于 l 时,列表的平均缩减率将大于或等于 $(1 - 2^{l-1}) \times 100\%$, 而且 l 个校验子不一定需要额外添加, C 中任何线性无关的 l 位都可以作为边际校验子信息使用。下面将给出具体的理论解释。

定理 1 设 C 是二元 $[n \ k \ d]$ 线性码, G 是 C 的一个生成矩阵, $I = \{i_1, i_2, \dots, i_l\}$ ($l < k$) 是 $\{1, 2, \dots, n\}$ 的一个真子集。若 G 的 i_1, i_2, \dots, i_l 列线性无关, 则 $\forall p \in F_2^k, C_p = \{c \in C \mid c_{i_1} = p_1, c_{i_2} = p_2, \dots, c_{i_l} = p_l\}$ 是码 C 的一个 $(n \ 2^{k-s} \ d_1)$ 非线性子码, 且 $d_1 \geq d$ 。

证明 不失一般性,可假设 $i_1 = n - l + 1, i_2 =$

$n - l + 2, \dots, i_l = n$, 令 $G_s = [g_{n-l+1}, g_{n-l+2}, \dots, g_n]$, 其中 g_i 为 G 的第 i 列。对 $\forall c \in C$, 有 $u \in F_2^k, c = uG$, 当 $c_i = p_i (n - l + 1 \leq i \leq n)$ 时, $(c_{n-l+1}, c_{n-l+2}, \dots, c_n) = p = uG_s$, 因 G_s 是秩为 l 的 $k \times l$ 矩阵, 那么 $xG_s = p$ 的解空间有 2^{k-l} 个元素, 从而 C_p 是 C 的 $(n \ 2^{k-s} \ d_1)$ 非线性子码, 自然有 $d_1 = d_H(C_p) \geq d_H(C) = d$ 。证毕

仍假设 $I = \{n - l + 1, n - l + 2, \dots, n\}$, $l < k$ 且 $G_1 = [g_1, g_2, \dots, g_{n-l}]$ 的秩为 k 。在发射端, 编码器将信息 u 编码为 $uG = (uG_1, uG_s) = (c_1, p)$, c_1 经普通信道发送, p 经可靠信道发送, 在接收端收到 c_1 的软判决带噪声信息 r_1 与无误的 p , 译码器将使用 (r_1, p) 完成译码。令 L 为利用列表译码法译 (r_1, p) 的所有候选码字集, 由于已知发送的码字最后 l 位为 p , 从而可以忽略 L 中最后 l 位不为 p 的候选码字, 由定理 1 得到缩减后的候选码字列表为: $\bar{L} = L \cap C_p$ 。

在每一次的译码过程中 C_p 由 p 唯一的确定并固定不变, 因而 \bar{L} 的大小取决于 L 的大小与 L 中候选码字的选取方式。对 i 阶重复处理的 OSD 算法:

$$|L| = \sum_{e=0}^i \binom{k}{e}, \text{ 显然序列 } (r_1, p) \text{ 中, } p \text{ 是绝对可信的 } l \text{ 位, 若将 } p \text{ 作为最可靠基中的 } l \text{ 位, 则可得 } |\bar{L}| = \sum_{e=0}^i \binom{k-l}{e} \approx \frac{(k-i)(k-i-1)\dots(k-l-i+1)}{k(k-1)\dots(k-l+1)} |L|。$$

文献[2]中, OSD 算法利用 r_1 包含的信息译码, p 不直接参与译码, 而是作为所发送码字的校验位以缩减译码列表, 缩减后列表的尺寸期望为 $E|\bar{L}| = |L|/2^l$, 远远好于直接将 p 加入最可靠基译码, i 阶重复处理的 OSD 算法处理的最可靠位(MRI)的错误模式集 $L_e = \{e \in F_2^k \mid w(e) \leq i\}$, 收到 r_1 后标准 OSD 算法如下处理: $r_1 \xrightarrow{\pi_1} r_1' \xrightarrow{\pi_2} r_1''$, $G_1 \xrightarrow{\pi_1} G_1' \xrightarrow{\pi_2} G_1'' \xrightarrow{\text{行变换}} G_m$ 。 r_1 各分量按可靠性从大到小排序后得 r_1' , 以及从 r_1 到 r_1' 的置换 π_1 , G_1 各列按 π_1 置换得到 G_1' , 这样 G_1' 各列按可靠性从左到右降序排列, 再使用贪心算法找到 G_1' 最靠右的 k 列线性无关列, 记为 MRI, 并将这 k 列按可靠性从左到右降序排列, 其余 $n - l - k$ 列紧随其后降序排列得到 G_1'' , 从 G_1' 到 G_1'' 得置换 π_2 。

G_m 为与 r_1'' 对应的码的系统生成矩阵, r_1'' 的前 k 位是 MRI。对 r_1'' 的前 k 作硬判决得 z_k , 计算 $z = z_k G_m$, 取 $\pi_1^{-1} \pi_2^{-1}[z]$ 得前 k 位记为 x , 令 $x = \pi_k[z]$, 计算 x 对应的边际信息 $s_0 = xG_s$, 那么对 $\forall e \in L_e$, 须满足 $\pi_k[(e + z_k)G_m]G_s = p$, 即 $\pi_k[eG_m]G_s = p + s_0 = \bar{p}$, 从而 L_e 中错误模式须满足:

$e\pi_k[G_m]G_s = \bar{p}$ 。又因 $C = \bigcup_{p \in F_2^l} C_p$ 且 $C_p \cap C_{\bar{p}} = \emptyset$ 当

$p \neq \bar{p}$ 时。根据文献[10], π_1 等可能取到 $(1, 2, \dots, n-l)$ 的任一排列, 而 π_2 由 π_1 唯一确定, 那么 G_1' 中任何线性无关的 k 列都等可能被取为 G_1' 的前 k 列, 数值计算结果得到的频率说明, 在每次译码中, 每组线性无关的 k 列被等可能地取到。从而对 $e \in L_e$, e 可能被编码为 C_p ($p \in F_2^l$) 中的码字, 最终 $E|\bar{L}| = |L|/2^l$, 接下来的仿真实验数据也得出同样结论。

3 基于移位寄存器的边际信息

文献[2]中的方案需要为传送边际信息准备额外的信道, 这种边际信息的获取方式增加了通信的成本。边际信息仅仅是告知译码器, 当前码字中必然包含某种信息, 那么我们可以换一种方式向译码器提供这一信息。

在编码端与译码端各放置一个同步的移位寄存器, 给定相同的初始状态, 它们将产生相同的随机序列。对二元 $[n \ k \ d]$ 线性码 C , 及边际信息长度 l ($l < k$), 编码器每次选取 $k-l$ 个要发送的信息, 再从移位寄存器序列中顺次取出 l 个随机数组成 k 个信息 u , u 编为码字 c , 删除 c 中的 l 个随机数得到删除后码字 \bar{c} , 将 \bar{c} 经普通信道发送, 在接收端收到 \bar{r} , 并从移位寄存器同步地取出 l 个随机数 p , 接下来译码器使用与前面同样的方法实现缩减列表, 完成对 $(\bar{r} \ p)$ 的译码。记这一译码算法为 ROSD(寄存器序列校验的分阶统计译码法), l 为边际信息长度。

虽然每次实际传送的是 $(n-l \ 2^{k-l} \ d_1)$ 码中的一个码字, 且每个码字包含 $k-l$ 个信息, 但是使用 i 阶 OSD 算法的列表包含 $\sum_{e=0}^i \binom{k-l}{e}$ 个候选码字, 当 l 较小时, 列表依然很大, 列表的缩减率并不明显。而与 p 组成 $(\bar{r} \ p)$ 后放在 C 中译码, 可以将 i 阶 OSD 算法的译码列表平均缩小到 $2^{-l} \sum_{e=0}^i \binom{k}{e}$, 远远要小于

$\sum_{e=0}^i \binom{k-l}{e}$, 译码的效率依然得到了显著的提高。使用

移位寄存器的边际信息, 每个码字包含的信息量减少了 l 个, 可是每次发送的码字长度也减少了 l 个, 同时码字的纠错能力并没有改变, 译码时列表的缩减效果没有丝毫的影响, 节省了额外的信道, 相对于使用稳定信道发送边际信息, 更易于工程实现。

4 使用最可靠位作为边际信息的分阶统计译码

第2节中, 我们假设经可靠信道传送的码字的边际信息 p 可以准确无误地被接收端收到, 然而现实的通信信道总是会有少量的错误, 并且可靠性越高的信道, 其建设、使用、维护的成本也相应的要高些。下面我们使用可能有少量错误的边际信息。

当译码端使用的边际信息 p 可能会有少量的错误时, 我们借鉴 OSD 重复处理的方法, 使用低阶 OSD 重复处理 p , 产生更多的候选校验位。若用一阶重复处理 p , 则最终发送端发送的码字可能在 $C_p \cup C_{p_1} \cup \dots \cup C_{p_l}$ 中 (p_i 表示 p 在第 i 位取反的边际信息), 此时缩减后的列表 $\bar{L} = L \cap \{C_p \cup C_{p_1} \cup C_{p_2} \cup \dots \cup C_{p_l}\}$ 平均大小为 $E|\bar{L}| = \frac{l+1}{2^l} |L|$ 。在传统的

OSD 译码算法中, 可靠性高的位发生错误的概率低, 从而可以将可靠性最高的几个分量挑选出来, 作为收到字的边际信息, 缩减 OSD 译码的列表。基于这一方法, 下面将给出最可靠位做边际信息的分阶统计译码。

C 是二元 $[n \ k \ d]$ 线性码, G 为其生成矩阵, $c = (c_1, c_2, \dots, c_n) \in C$ 先映射到 $x = (x_1, x_2, \dots, x_n)$, $x_i = 2c_i - 1$, x 经 BPSK 调制后通过 AWGN 信道, 在接收端解调后得 $r = (r_1, r_2, \dots, r_n)$, 其中 $r_i = x_i + w_i$, w_i 是独立同分布的随机变量, 服从 $N(0, n_0/2)$ (n_0 是噪声双边功率谱) 分布, 那么 r_i 的硬判决可靠性度量是 $|r_i|$ 。与 OSD 算法一样, 首先按 r 中各位的可靠性度量从大到小排序得到 $y = (y_1, y_2, \dots, y_n)$ 。给定 $l, l \ll \min(k, n-k)$, 且满足 G 中任何 l 列线性无关, 去掉 G 中的任何 l 列后所得矩阵的秩仍为 k 。取 y 前 l 个分量与后 $n-l$ 个分量置换得 $\bar{y} = (y_{l+1}, y_{l+2}, \dots, y_n, y_1, \dots, y_l)$, 从而 $|y_{l+1}| > |y_{l+2}| > \dots > |y_n|$, $|y_1| > \dots > |y_l|$ 。由 r 到 \bar{y} 可以得到置换 λ_1 , 对 G 的各列按 λ_1 置换得 $G' = \lambda_1[G] = [g'_1, g'_2, \dots, g'_n]$, g'_i 为 G' 的第 i 列, 显然 G 与 G' 生成等价的码。 $|y_i|$ 作为 g'_i 的可靠性度量, 从 G' 的第 1 列至 $n-l$ 列中, 找到 G' 的 k 个线性无关且可靠性度量最大的列(这一过程可以通过对 G' 进行初等行变换后, 使用贪心算法得到), 将这 k 列按可靠性从大到小放在最前面, 余下的 $n-l-k$ 列也按可靠性从大到小依次放在最可靠的 k 列之后, 组成一个新的 $k \times n$ 矩阵 G'' , 从 G' 到 G'' 又产生一个置换 λ_2 , 那么 $G'' = \lambda_2[G'] = \lambda_2\lambda_1[G]$, 令 $z = (z_1, z_2, \dots, z_k, z_{k+1}, \dots, z_{n-l}, z_{n-l+1}, \dots, z_n) = \lambda_2\lambda_1[y]$, $|z_{n-l+1}| > \dots > |z_n| > |z_1| > \dots > |z_k|, |z_{k+1}| > |z_{k+2}| > \dots > |z_{n-l}|$ 。 z 的最后 l 位作为最可靠校验位, 前 k 位为次可靠信息位。下面对 G'' 做初等行变换得 $G_1 =$

$[I_k, P_1, P_l], P_l$ 由 G_1 的最后 l 列组成。下面对 z 的前 k 位与最后 l 位做硬判决得 $\mathbf{a} = (a_1, a_2, \dots, a_k)$ 及 $\mathbf{p} = (p_1, p_2, \dots, p_l)$, \mathbf{p} 就是从最可靠位得到的边际信息。

接下来对 \mathbf{a} 做带校验测试的 i 阶重复处理, 找到与 z 相关性最大的候选码字完成译码, 这里选取文献[1]中用到的欧氏距离作为码字与 z 的相关性度量, 欧氏距离越小, 相关性越大。

(1)初始化 $\mathbf{c}_b = \mathbf{a}G_1, f_b = d_E(\mathbf{x}_b, z)$ (d_E 为欧氏距离, \mathbf{x}_b 为 \mathbf{c}_b 的 BPSK 像) $t (t < l)$;

(2)生成 \mathbf{a} 的所有重量在 1 与 i 之间的错误模式列表 L_i ;

(3)从 L_i 中取出一个错误模式 \mathbf{e} , 若 L_i 已空则停止译码;

(4)计算 $\bar{\mathbf{p}} = (\mathbf{a} + \mathbf{e})P_s$, 若 $d_H(\bar{\mathbf{p}}, \mathbf{p}) \leq t$, 则回到(3);

(5)生成候选码字 $\mathbf{c} = (\mathbf{a} + \mathbf{e})G_1$, 若 $d_E(\mathbf{x}_c, z) < f_b$, 重置 $f_b = d_E(\mathbf{x}_c, z), \mathbf{c}_b = \mathbf{c}$;

(6)若 L_i 未空则回到(3)。

最终当 L_i 为空后译码停止, $\lambda_1^{-1}\lambda_2^{-2}[c_b]$ 为最终的译码结果。记这个译码算法为 SOSD(最可靠位校验的分阶统计译码法)。

在本算法中, 使用了最可靠的 l 位作为校验位, 并限制其最多发生 t 个错误, 通过对 L_i 中的错误模式进行校验, 可以除去大部分的错误模式, 减少不必要的计算。当限制 l 个校验信息最多发生 t 个错误时, L_i 平均缩减 $(1 - \frac{T}{2^l}) \sum_{d=0}^i \binom{s}{d}$, $T = \sum_{j=0}^l \binom{l}{j}$, 相应的性能损失则随 l 的增加而增大。

5 数值仿真结果与比较

本节给出一些数值仿真来说明方法的有效性。仿真实验中, 每个码字 \mathbf{c} 经过 BPSK 调制后通过加性高斯白噪声(AWGN)信道, 接收端收到向量 \mathbf{r}, \mathbf{r}

中每个分量 $r_i = b_i + v_i$, 其中 $b_i = 2c_i - 1, v_i$ 是均值为 0, 方差为 $(2R \times 10^{\gamma_b/10})^{-1}$ 的相互独立高斯随机变量(R 是码率, γ_b 是每比特信噪比, $i = 1, 2, \dots, n$)。下面以二元[63 36 11]BCH 码为例仿真。

图 1 与表 1 是 ROSD(寄存器序列校验的分阶统计译码法)仿真结果与 OSD 仿真结果的比较。图中给出的仿真结果表明, ROSD 与传统 OSD 相比, 译码性能上无多大差别, 当 SNR 大于 4 以后 ROSD 比特错误率最多比 OSD 高 8×10^{-7} 。不同信噪比下, ROSD 译码列表平均候选码字数与 OSD 译码列表的候选码字数比值由表 1 给出, 从表中数据可得, 使用 l 个边际信息, 译码的列表缩小了大约 $(1 - 2^l) \times 100\%$ 。这是由于此处 l 个边际信息是码字中的一部分, 因此实际的 OSD 译码列表中候选码字数少于 $\sum_{e=0}^i \binom{k}{e}$ 个, 虽然每个候选码字的检测需要耗费一定的计算资源, 但是相对于计算候选码字与接收序列的相关度的浮点计算, 位运算要快的多。

图 2 与表 2 是 SOSD(最可靠位校验的分阶统计译码法)与 OSD 仿真结果的比较。在 $t = 0, l = 3$ 时即取得了较好的结果, 平均候选码字数也大大减少。从图中可以看出, 以最可靠位为边际信息的 SOSD 译码算法在性能上与经典 OSD 译码算法差别很小, 当 SNR 大于 4.0 dB 以后, SOSD 比特错误率比 OSD 最高 5×10^{-7} , 但是节省了大约 87.5% 的浮点计算量。

6 结论

本文对文献[2]中使用边际信息缩小译码列表的方法推广到一般的情况下, 并分析了边际信息缩减译码列表的原因, 给出了基于移位寄存器序列的边际信息, 相比于使用稳定信道传送的边际信息法, 基于移位寄存器序列的边际信息不使用额外的信

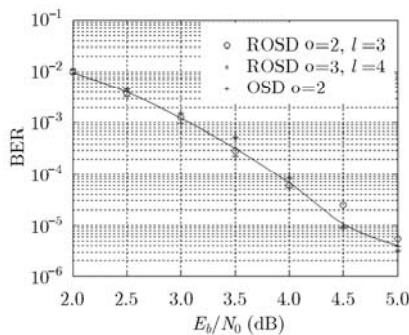


图 1 [63 36 11]二元 BCH 码在经典 OSD 译码算法与移位寄存器作为边际信息的 ROSD 译码算法的性能比较

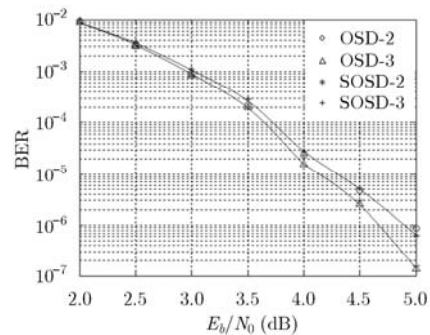


图 2 [63 36 11]二元 BCH 码在经典 OSD 译码算法与最可靠位作为边际信息的 SOSD 译码算法的性能比较, 其中 $l = 3, t = 0$

表 1 [63 36 11]二元 BCH 码在 ROSD 译码算法下平均候选码字数与经典 OSD 译码算法的候选码字数之比

SNR (dB)	2.0	2.5	3.0	3.5	4.0	4.5	5.0
ROSD, $l=3$	0.1472	0.1465	0.1464	0.1459	0.1456	0.1456	0.1454
ROSD, $l=4$	0.0782	0.0776	0.0774	0.0770	0.0768	0.0767	0.0766

表 2 [63 36 11]二元 BCH 码在 SOSD 译码算法下平均候选码字数与经典 OSD 译码算法的候选码字数之比

SNR (dB)	2.0	2.5	3.0	3.5	4.0	4.5	5.0
SOSD, $l=3, o=3, t=0$	0.1242	0.1237	0.1233	0.1231	0.1229	0.1228	0.1226
SOSD, $l=3, o=4, t=0$	0.1243	0.1242	0.1241	0.1240	0.1240	0.1240	0.1240

注: o 为 order 的缩写

道,不影响译码的性能与复杂度,更易于工程实现。利用码字中的最可靠位作为边际信息的译码算法,大大缩小了译码列表,而对纠错能力影响很小。本文给出的两种缩小译码列表的边际信息不仅可以用于 OSD 译码算法,也可以用于其他的列表译码算法。虽然边际信息的使用显著降低了译码列表的大小,但是长码的译码列表依然很大,需要更长的边际信息,更多的时间剔除无用的候选码字。

参考文献

- [1] Fossorier P C and Lin S. Soft-decision decoding of linear block codes based on ordered statistics[J]. *IEEE Transactions on Information Theory*, 1995, 41(5): 1379-1396.
- [2] Alnawayseh E A and Loskot P. Complexity reduction of ordered statistics decoding using side information[J]. *IEEE Communication Letters*, 2012, 16(2): 249-251.
- [3] Fossorier P C and Lin S. Complementary reliability-based decoding binary linear codes[J]. *IEEE Transactions on Information Theory*, 1997, 43(5): 1667-1672.
- [4] Sabbag E and Merhav N. Achievable error exponents for channel with side information-erasure and list decoding[J]. *IEEE Transactions on Information Theory*, 2010, 56(11): 5424-5431.
- [5] Fossorier P C, Lin S, and Snyders J. Reliability-based syndrome decoding of linear block codes[J]. *IEEE Transactions on Information Theory*, 1998, 44(1): 388-398.
- [6] Zeh A and Gentner C. An interpolation procedure for list decoding Reed-Solomon codes based on generalized key equation[J]. *IEEE Transactions on Information Theory*, 2011, 57(9): 5946-5959.
- [7] Mahdaviifar H and Vardy A. List-decoding of subspace codes and rank-metric codes up to singleton bound[C]. *IEEE International Symposium on Information Theory Proceedings*, Honolulu, 2012: 1488-1492.
- [8] Valembos A and Fossorier M. Box and match techniques applied to soft-decision decoding[J]. *IEEE Transactions on Information Theory*, 2004, 50(5): 796-810.
- [9] Chase D. A class of algorithm for decoding block codes with channel measurement information[J]. *IEEE Transactions on Information Theory*, 1972, 18(1): 170-182.
- [10] 孙泽山. 非参数统计讲义[M]. 北京: 北京大学出版社, 2000: 1-21.
Sun Ze-shan. Non-Parametric Statistics Lecture Notes[M]. Beijing: Peking University Press, 2000: 1-21.

朱士信: 男, 1962 年生, 教授, 博士生导师, 研究方向为代数编码、信息安全、非线性移位寄存器序列。

虞艺超: 男, 1989 年生, 硕士生, 研究方向为代数编码与密码。