文章编号:1001-2486(2011)03-0115-06

BSC信道下线性分组码的差错概率下界分析*

许 拔[1,2],何英亮[3],周昌术[4],张尔扬[1]

(1. 国防科技大学 电子科学与工程学院,湖南 长沙 410073; 2. 总参第六十三研究所,江苏 南京 210007;
3. 国防科技大学 计算机学院,湖南 长沙 410073; 4. 湖南省军区预备役师通信科,湖南 长沙 410016)

摘 要:针对BSC信道,提出了一种线性分组码的最大似然译码差错概率下界的计算方法。根据最大似然译码算法原理,首先将译码差错概率转化为差错事件的联合概率,基于改进的Dawson-Sankoff界的优化准则,推导出BSC信道下线性分组码差错冗余事件的判决准则,最后得到差错概率下界的计算表达式。该下界只依赖于码字的Hamming重量分布与信道的交叉概率。针对不同的LDPC码的仿真结果表明:较之常见的下界和sphere packing bound,本算法得到的下界性能更好、计算复杂度更低。

关键词:LDPC;最大似然译码;Hamming重量分布函数;优化准则

中图分类号:TN911.22 **文献标识码**:A

Analysis of Lower Bound for the Error Probability of Linear Block Codes over the BSC Channel

XU Ba[1,2], *He Ying-liang*[3], *ZHOU Chang-shu*[4], *ZHANG Er-yang*[1]

(1. Colleges of Electronics Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China;
2. The 63rd Research Institute of PLA General Staff Headquarter, Nanjing 210007, China;
3. Colleges of Computer, National Univ. of Defense Technology, Changsha 410073, China;
4. The Communication Section of Reserve Division, Hunan Military Region, Changsha 410016, China)

Abstract: A lower bound on the error rate of linear binary block codes (under maximum likelihood decoding) over BSC channels is proposed. According to the principle of the maximum likelihood (ML) decoding algorithm, the decoding error probability is firstly converted into the joint probability of the error events, and the judge rule of the redundant error events is deduced based on the optimization rule of the improved Dawson-Sankoff bound. Moreover, the calculation expression about lower bound of the error probability solely depends on the Hamming weight enumerator function of the code and the crossover probability of the channel. The simulation results applying to various LDPC codes show that the new lower bound outperforms those generic lower bounds and the sphere packing bound. Its computational complexity is also lower.

Key words: low density parity check codes; maximum likelihood decoding; hamming weight enumerator function; optimization rule

不同于计算机仿真,分析性能界时,只需知道码字的汉明重量分布(Hamming Weight Enumerator Function,WEF)或输入-输出重量分布函数(Input-Output Weight Enumerator Function,IOWEF),就可以得出纠错码误码率的上、下界,从而对纠错码的性能进行估计。长期以来,对性能界的研究与分析备受学者的关注,这是理论分析码字性能、了解码字结构对性能影响的重要手段,能够为好码的构造提供理论依据,对于信息论与编码理论的发展具有重要的意义。

对性能界的研究包括两个方面:性能上界和性能下界,本文主要针对下界进行研究。随着数学理论的发展,利用联合概率事件的下界来估计码字的纠错性能受到越来越多的青睐[1-11]。文献[1]将文献[2]提出的de Caen's不等式应用于二进制线性分组码的性能估计,得到了BPSK-modulated AWGN信道下误码率下界,该下界仅仅依赖于码字的WEF,当信噪比(E_b/N_0)趋于无穷大时,能够收敛于码字的联合上界(union upper bound);文献[3]在文献[1]的基础上,通过在de Caen's不等式中引入优化函数,根据优化函数的不同推导出两种性能下界:norm bound与dot-product bound,同时证明了文献[1]提出的Seguin's bound是这两种界的特殊情况,这两种界的性能

* 收稿日期:2010-09-18
作者简介:许拔(1981—),男,工程师,博士。

比 Seguin's bound 的更好。文献[4]提出了联合概率的 KAT 界,并证明了该下界比 de Caen 界[2]与 Dawson-Sankoff 界[5]更接近联合概率的真实值,为下界的发展指明了新的方向。文献[6]分析了 BPSK-modulated AWGN 信道下编码信号的性能,提出了两种简化的下界计算方法:LB-f 和 LB-s,两种算法既降低了计算复杂度,同时提高了性能估计的精度,其中:LB-f 仅利用最小 Hamming 重量码字的 WEF 和码字两两之间乘积的重量分布;LB-s 只需知道码的 WEF。

上述差错概率的下界主要针对 AWGN 信道,只有文献[3]和[7]对 BSC 信道下的下界进行了研究。然而,这些下界的计算复杂度偏高,计算时间长,同时下界性能有较大的提升空间。本文在文献[8]的基础上,提出了基于改进的 Dawson-Sankoff 界的 BSC 信道下线性分组码差错冗余事件的判断准则,推导出差错概率下界的计算表达式,并针对各种 Regular-LDPC 码进行了仿真,结果表明:在所有交叉概率(p)的范围内,本文提出的下界比文献[3]中下界的值更高,性能更好,计算时间明显缩短;并且,随着 p 的增大,性能的相对优势更明显。

1 Dawson-Sankoff 界

1.1 传统的 Dawson-Sankoff 界

Dawson-Sankoff 界最早于 1967 年在文献[5]中被提出,定理 1 给出了该传统下界的具体描述。

定理 1 假设 $A_1, A_2, \cdots, A_N$ 是概率空间 (Ω, P) 上的有限事件集合,则有

$$P(\bigcup_{i=1}^{N} A_i) \geqslant \frac{(1-\theta)\cdot S_1^2}{2S_2 + (1-\theta)\cdot S_1} + \frac{\theta \cdot S_1^2}{2S_2 + (2-\theta)\cdot S_1} \tag{1}$$

其中:$S_1 \triangleq \sum_{i=1}^{N} P(A_i)$, $S_2 \triangleq \sum_{i=1}^{N}\sum_{j=1}^{i-1} P(A_i \cap A_j)$, $\theta \triangleq \frac{2S_2}{S_1} - \lfloor \frac{2S_2}{S_1} \rfloor$。

定理 1 中得到的 Dawson-Sankoff 界仅依赖于单个事件概率和事件成对出现的联合概率;但当 N 很大时,计算复杂度仍很大;文献[4]严格证明了该下界是 KAT 界的特例,性能不如 KAT 界的好。

1.2 Dawson-Sankoff 界的改进

为了简化 Dawson-Sankoff 界的计算同时提高其性能,Hoppe 在文献[8]中通过理论与实例证明:通过移除满足优化准则的冗余事件可以提高联合概率的下界。这里以定理 2 的形式给出文献[8]的结论,相关证明详见文献[8]。

定理 2 假设 $A_1, A_2, \cdots, A_N$ 是概率空间 (Ω, P) 上的有限事件集合,则有

$$P(\bigcup_{i=1}^{N} A_i) \geqslant \max_{I}\left\{\frac{[1-\theta(I)]\cdot S_1^2(I)}{2S_2(I) + [1-\theta(I)]\cdot S_1(I)} + \frac{\theta(I)\cdot S_1^2(I)}{2S_2(I) + [2-\theta(I)]\cdot S_1(I)}\right\} \tag{2}$$

这里 $I \subseteq \{1,2,\cdots,N\}$, $S_1(I) = \sum_{i\in I} P(A_i)$, $S_2(I) = \sum_{i\in I}\sum_{j\in I, j<i} P(A_i \cap A_j)$, $\theta(I) = \frac{2S_2(I)}{S_1(I)} - \lfloor \frac{2S_2(I)}{S_1(I)} \rfloor$。

其中,(2)式右边的最大值在 $I = I^*$ 时取得,而对于 $\forall j \in \{1,2,\cdots,N\}$,当且仅当:

$$\begin{cases} A_j \subseteq \bigcup_{i\in I^*} A_i \\ P(A_j) - \frac{1}{K}\cdot \sum_{i\in I^*} P(A_j \cap A_i) < 0 \end{cases} \tag{3}$$

成立时,$A_j \notin A_{I^*}$。这里有:$A_{I^*} \triangleq \{A_i \mid i \in I^*\}$, $K \triangleq 1 + \lfloor \frac{2S_2(A_{I^*} \cup A_j)}{S_1(A_{I^*} \cup A_j)} \rfloor$。

式(3)即为去除冗余事件的优化准则,通过判断式(3)是否成立来决定是否从 I^* 中移除当前事件。根据式(2)能得到联合概率的更紧的下界,同时简化了下界计算的复杂度。

2 基于改进 Dawson & Sankoff 界的差错概率下界分析

线性码码长为 N,编码后码字个数为 M,分别为 $c_0, c_1, \cdots, c_{M-1}$。假设 c_t 经 BSC 信道传输后,接收码字为 R,R 也为 N 维矢量,有

$$R = c_t + e \tag{4}$$

e 为 N 维二进制错误矢量。在接收端,采用最大似然译码(ML)算法将 R 译成与其 Hamming 距离最短的码字,即 $\underset{c_i}{\operatorname{argmin}}\, d_H(c_i, R)$。因此,传输 c_t 的条件错误概率为

$$P(\varepsilon \mid c_t) = \Pr[\bigcup_{\substack{i=0 \\ i\neq t}}^{M-1} \varepsilon_{ti} \mid c_t] \tag{5}$$

这里:$\varepsilon_{ti} = \{R \mid d_H(R, c_i) < d_H(R, c_t)\}$;$d_H(\cdot,\cdot)$ 表示码字之间的汉明距离。

文献[10]的 Proposition 1 指出:在对称无记忆信道中,线性分组码条件错误概率与传输的码字无关,证明可参考文献[10]的 Appendix B。因此

$$P(\varepsilon) = \sum_{t=0}^{M-1} P(\varepsilon \mid c_t)\times P(c_t) = P(\varepsilon \mid c_0) = \Pr[\bigcup_{i=1}^{M-1} \varepsilon_{0i} \mid c_0] \tag{6}$$

c_0 表示全 0 码字。

2.1 基于传统 Dawson-Sankoff 界的错误概率下界的推导

令:$A_i = \varepsilon_{0i} = \{R \mid d_H(R,c_i) < d_H(R,c_0)\}$,$A_i \cap A_j = \varepsilon_{0i} \cap \varepsilon_{0j} = \{R \mid d_H(R,c_i) < d_H(R,c_0), d_H(R,c_j) < d_H(R,c_0)\}$,则式(6)转化为

$$P(\varepsilon) = \Pr[\bigcup_{i=1}^{M-1} \varepsilon_{0i} \mid c_0] = \Pr[\bigcup_{i=1}^{M-1} A_i] \tag{7}$$

这里,为了利用定理 1 的结论来计算式(7)的下界,首先需计算 $P(A_i)$ 与 $P(A_i \cap A_j)$ 值。又因为

$$\begin{cases} P(A_i) = \sum\limits_{x \in A_i} p^{w(x)} \cdot (1-p)^{N-w(x)} \\ \qquad = \sum\limits_{x \in \varepsilon_{0i}} p^{w(x)} \cdot (1-p)^{N-w(x)} \\ P(A_i \cap A_j) = \sum\limits_{x \in A_i \cap A_j} p^{w(x)} \cdot (1-p)^{N-w(x)} \\ \qquad = \sum\limits_{x \in \varepsilon_{0i} \cap \varepsilon_{0j}} p^{w(x)} \cdot (1-p)^{N-w(x)} \end{cases} \tag{8}$$

其中,$w(\cdot)$ 表示码字的 Hamming 重量,p 表示 BSC 信道的交叉概率,$p < 1/2$。根据码字的支撑概念可推导出 $P(A_i)$ 与 $P(A_i \cap A_j)$ 最终表达式为

$$P(A_i) = \sum_{l=\lfloor \frac{w(c_i)}{2} \rfloor + 1}^{w(c_i)} \sum_{m=0}^{N-w(c_i)} \binom{w(c_i)}{l} \cdot \binom{N-w(c_i)}{m} \cdot p^{l+m} \cdot (1-p)^{N-l-m} \tag{9}$$

$$P(A_i \cap A_j) = \sum_{l=0}^{w(c_ic_j)} \sum_{m=\lfloor \frac{w(c_i)}{2} \rfloor + 1 - l}^{w(c_i)-w(c_ic_j)} \sum_{n=\lfloor \frac{w(c_j)}{2} \rfloor + 1 - l}^{w(c_j)-w(c_ic_j)} \sum_{k=0}^{N-w(c_i)-w(c_j)+w(c_ic_j)} \binom{w(c_ic_j)}{l} \cdot \binom{w(c_i)-w(c_ic_j)}{m} \cdot \binom{w(c_j)-w(c_ic_j)}{n} \cdot \binom{N-w(c_i)-w(c_j)+w(c_ic_j)}{k} \cdot p^{l+m+n+k} \cdot (1-p)^{N-l-m-n-k} \tag{10}$$

上式中 $P(A_i \cap A_j)$ 不仅依赖于码字的 Hamming 重量分布,还与 $w(c_ic_j)$ 有关。而 $w(c_ic_j)$ 表示码字 c_i 与 c_j 同为 1 的元素个数,显然有:$w(c_ic_j) \leqslant \min[w(c_i), w(c_j)]$;又因为 $w(c_ic_j) \leqslant [w(c_i) + w(c_j) - D_{\min}]/2$,其中 $D_{\min}$ 表示码的最小 Hamming 距离。因此有

$$w(c_ic_j) \leqslant \min\{w(c_i), w(c_j), [w(c_i) + w(c_j) - D_{\min}]/2\} \tag{11}$$

根据文献[3]的 Proposition 4.1 知:式(10)右边关于 $w(c_ic_j)$ 单调递增,因此用式(11)右边的项代替 $w(c_ic_j)$ 将使 $P(A_i \cap A_j)$ 变大,令 $w(c_ic_j) \triangleq \min\{w(c_i), w(c_j), [w(c_i) + w(c_j) - D_{\min}]/2\}$。为简化,后面的计算均采用 (c_ic_j) 代替 $w(c_ic_j)$。定理 1 的(1)式中 $P(A_i \cap A_j)$ 出现在分母部分,因此替代操作使得性能下界变小,性能变差;不过,经过替代之后性能下界的表达式将完全由码字的 Hamming 重量分布和 BSC 信道的交叉概率 p 决定,极大地简化了性能下界的计算。

根据定理 1 对 S_1 和 S_2 的定义可推导出

$$\begin{aligned} S_1 &= \sum_{i=D_{\min}}^{N} B_i \cdot \tilde{P}_1(i) \\ 2S_2 &= \sum_{i=D_{\min}}^{N} [(B_i - 1) \cdot \tilde{P}_2(i,i) + \sum_{\substack{j=D_{\min} \\ j \neq i}}^{N} B_j \cdot \tilde{P}_2(i,j)] \end{aligned} \tag{12}$$

其中,B_i 表示 Hamming 重量为 i 的码字个数,即 $B_i = |c : c \in C, w(c) = i|$,$D_{\min}$ 表示码字的最小 Hamming 重量;同时,$\tilde{P}_1(i)$、$\tilde{P}_2(i,i)$ 与 $\tilde{P}_2(i,j)$ 分别定义如下:

$$\tilde{P}_1(i) \triangleq \sum_{l=\lfloor \frac{i}{2} \rfloor + 1}^{i} \sum_{m=0}^{N-i} \binom{i}{l} \cdot \binom{N-i}{m} \cdot p^{l+m} \cdot (1-p)^{N-l-m} \tag{13}$$

$$\tilde{P}_2(i,i) \triangleq \sum_{l=0}^{\lceil i - \frac{D_{\min}}{2} \rceil} \sum_{m=\lfloor \frac{i}{2} \rfloor + 1 - l}^{\lceil \frac{D_{\min}}{2} \rceil} \sum_{n=\lfloor \frac{i}{2} \rfloor + 1 - l}^{\lceil \frac{D_{\min}}{2} \rceil} \sum_{k=0}^{N-i-\lceil \frac{D_{\min}}{2} \rceil} \binom{\lceil i - \frac{D_{\min}}{2} \rceil}{l} \cdot \binom{\lceil \frac{D_{\min}}{2} \rceil}{m} \cdot \binom{\lceil \frac{D_{\min}}{2} \rceil}{n} \cdot \binom{N - i - \lceil \frac{D_{\min}}{2} \rceil}{k} \cdot p^{l+m+n+k} \cdot (1-p)^{N-l-m-n-k} \tag{14}$$

$$\tilde{P}_2(i,j) \triangleq \sum_{l=0}^{\lceil \frac{i+j-D_{\min}}{2} \rceil} \sum_{m=\lfloor \frac{i}{2} \rfloor + 1 - l}^{\lceil \frac{i-j+D_{\min}}{2} \rceil} \sum_{n=\lfloor \frac{j}{2} \rfloor + 1 - l}^{\lceil \frac{j-i+D_{\min}}{2} \rceil} \sum_{k=0}^{N-\lceil \frac{i+j+D_{\min}}{2} \rceil} \binom{\lceil \frac{i+j-D_{\min}}{2} \rceil}{l} \cdot \binom{\lceil \frac{i-j+D_{\min}}{2} \rceil}{m} \cdot$$

$$\binom{\lceil \frac{j-i+D_{\min}}{2} \rceil}{n} \cdot \binom{N-\lceil \frac{i+j+D_{\min}}{2} \rceil}{k} \cdot p^{l+m+n+k} \cdot (1-p)^{N-l-m-n-k} \tag{15}$$

根据上述讨论,综合(1)、(7)与(12)得到 BSC 信道下基于传统 Dawson & Sankoff 界的错误概率下界的表达式为

$$P(\varepsilon) \geqslant \frac{(1-\theta) \cdot \left(\sum_{i=D_{\min}}^{N} B_i \cdot \tilde{P}_1(i) \right)^2}{\sum_{i=D_{\min}}^{N} \left\{ (B_i - 1) \cdot \tilde{P}_2(i,i) + \sum_{\substack{j=D_{\min} \\ j \neq i}}^{N} B_j \cdot \tilde{P}_2(i,j) \right\} + (1-\theta) \cdot \left(\sum_{i=D_{\min}}^{N} B_i \cdot \tilde{P}_1(i) \right)} + \frac{\theta \cdot \left(\sum_{i=D_{\min}}^{N} B_i \cdot \tilde{P}_1(i) \right)^2}{\sum_{i=D_{\min}}^{N} \left\{ (B_i - 1) \cdot \tilde{P}_2(i,i) + \sum_{\substack{j=D_{\min} \\ j \neq i}}^{N} B_j \cdot \tilde{P}_2(i,j) \right\} + (2-\theta) \cdot \left(\sum_{i=D_{\min}}^{N} B_i \cdot \tilde{P}_1(i) \right)} \tag{16}$$

上式中,$\theta \triangleq \frac{2S_2}{S_1} - \lfloor \frac{2S_2}{S_1} \rfloor$。从式(16)可看出,基于传统 Dawson & Sankoff 界的错误概率下界仅由码字的 Hamming 重量分布和 BSC 信道的交叉概率 p 共同决定,不需要码的其它具体构造信息。而从上文的讨论可知,对 $w(c_i c_j)$ 的替代操作弱化了错误概率下界性能,同时根据文献[4]可知 KAT 界性能优于传统的 Dawson & Sankoff 界的性能,因此有必要对式(16)得到的下界性能进行优化。

2.2 基于改进 Dawson & Sankoff 界的错误概率下界的推导

为了改善传统的 Dawson & Sankoff 界的性能,并进一步降低下界的计算复杂度,文献[8]提出了利用最优子集求解联合概率下界的思想,同时给出了判断冗余事件的优化准则,上文以定理 2 的形式给出了相关结论,式(3)即为优化准则。利用定理 2 的结论改善上文提出的错误概率下界的关键在于如何将式(3)的优化准则转化为码字冗余判断准则。根据前面的讨论,并结合式(3)、(9)与(10),推导出码字冗余的判断准则为

$$\begin{aligned} &\sum_{l=\lfloor \frac{w(c_j)}{2} \rfloor + 1}^{w(c_j)} \sum_{m=0}^{N-w(c_j)} \binom{w(c_j)}{l} \cdot \binom{N-w(c_j)}{m} \cdot p^{l+m} \cdot (1-p)^{N-l-m} \\ &< \frac{1}{K} \cdot \sum_{i \in I^*} \sum_{l=0}^{\bar{w}(c_i c_j)} \sum_{m=\lfloor \frac{w(c_i)}{2} \rfloor + 1 - l}^{w(c_i) - \bar{w}(c_i c_j)} \sum_{n=\lfloor \frac{w(c_j)}{2} \rfloor + 1 - l}^{w(c_j) - \bar{w}(c_i c_j)} \sum_{k=0}^{N-w(c_i)-w(c_j)+\bar{w}(c_i c_j)} \binom{\bar{w}(c_i c_j)}{l} \cdot \binom{w(c_i) - \bar{w}(c_i c_j)}{m} \cdot \\ &\binom{w(c_j) - \bar{w}(c_i c_j)}{n} \cdot \binom{N - w(c_i) - w(c_j) + \bar{w}(c_i c_j)}{k} \cdot p^{l+m+n+k} \cdot (1-p)^{N-l-m-n-k} \end{aligned} \tag{17}$$

即:当不等式(17)满足时,$A_j \notin A_{I^*}$,其中:$A_{I^*} \triangleq \{A_i \mid i \in I^*\}$,$K \triangleq 1 + \lfloor \frac{2S_2(A_{I^*} \cup A_j)}{S_1(A_{I^*} \cup A_j)} \rfloor$。

上式中计算 K 的关键是计算 $S_1(A_{I^*} \cup A_j)$ 与 $S_2(A_{I^*} \cup A_j)$,由定理 2 中对两者的定义可以很容易得到

$$\begin{cases} S_1(A_{I^*} \cup A_j) = \sum_{l=\lfloor \frac{w(c_j)}{2} \rfloor + 1}^{w(c_j)} \sum_{m=0}^{N-w(c_j)} \binom{w(c_j)}{l} \cdot \binom{N-w(c_j)}{m} \cdot p^{l+m} \cdot (1-p)^{N-l-m} + S_1(A_{I^*}) \\ S_2(A_{I^*} \cup A_j) = S_2(A_{I^*}) + \sum_{i \in I^*} \sum_{l=0}^{\bar{w}(c_i c_j)} \sum_{m=\lfloor \frac{w(c_i)}{2} \rfloor + 1 - l}^{w(c_i) - \bar{w}(c_i c_j)} \sum_{n=\lfloor \frac{w(c_j)}{2} \rfloor + 1 - l}^{w(c_j) - \bar{w}(c_i c_j)} \sum_{k=0}^{N-w(c_i)-w(c_j)+\bar{w}(c_i c_j)} \binom{\bar{w}(c_i c_j)}{l} \cdot \\ \binom{w(c_i) - \bar{w}(c_i c_j)}{m} \cdot \binom{w(c_j) - \bar{w}(c_i c_j)}{n} \cdot \binom{N - w(c_i) - w(c_j) + \bar{w}(c_i c_j)}{k} \cdot p^{l+m+n+k} \cdot (1-p)^{N-l-m-n-k} \end{cases} \tag{18}$$

在已知 $S_1(A_{I^*})$ 与 $S_2(A_{I^*})$ 前提下,根据式(18)能很快求出 $S_1(A_{I^*} \cup A_j)$ 与 $S_2(A_{I^*} \cup A_j)$,

因此可很容易判断出式(17)是否满足。

综上所述,得到基于改进 Dawson & Sankoff 界的错误概率下界算法,具体步骤如下所示。

Step 1　(初始化) $I^{*(0)}=\{i\mid w(c_i)=D_{\min}\}$,令迭代次数 $l=0$, $\bar{C}^{(0)}=C\setminus C_{I^{*(0)}}$,并计算 $S_1(A_{I^*})$ 与 $S_2(A_{I^*})$:

$$\begin{cases}S_1(A_{I^{*(0)}})=B_{D_{\min}}\times\tilde{P}_1(D_{\min})\\ S_2(A_{I^{*(0)}})=B_{D_{\min}}(B_{D_{\min}}-1)\times\tilde{P}_2(D_{\min},D_{\min})/2\end{cases}$$

Step 2　选取 $\bar{C}^{(l)}$ 中 Hamming 重量最小的 c_j 对应的 A_j 进行考虑,据式(18)计算 $S_1(A_{I^{*(l)}}\cup A_j)$ 与 $S_2(A_{I^{*(l)}}\cup A_j)$,同时令:$\bar{C}^{(l+1)}=\bar{C}^{(l)}\setminus\{c_j\}$,并判断是否满足式(17):

① 如果满足,则 $A_j\notin A_{I^*}$, $I^{*(l+1)}=I^{*(l)}$, $S_1(A_{I^{*(l+1)}})=S_1(A_{I^{*(l)}})$, $S_2(A_{I^{*(l+1)}})=S_2(A_{I^{*(l)}})$, $l=l+1$,并转 Step 3;

② 否则,$A_j\in A_{I^*}$, $I^{*(l+1)}=I^{*(l)}\cup\{j\}$,并对 $S_1(A_{I^{*(l+1)}})$ 与 $S_2(A_{I^{*(l+1)}})$ 进行赋值:$S_1(A_{I^{*(l+1)}})=S_1(A_{I^{*(l)}}\cup A_j)$, $S_2(A_{I^{*(l+1)}})=S_2(A_{I^{*(l)}}\cup A_j)$, $l=l+1$,并转 Step 3;

Step 3　如果 $\bar{C}^{(l)}\neq\phi$,转 Step 2;否则,转 Step 4;

Step 4　计算 $\theta(I^{*(l)})=\dfrac{2S_2(A_{I^{*(l)}})}{S_1(A_{I^{*(l)}})}-\left\lfloor\dfrac{2S_2(A_{I^{*(l)}})}{S_1(A_{I^{*(l)}})}\right\rfloor$,并通过式(19)得到误码率下界:

$$P(\varepsilon)=\Pr[\bigcup_{i=1}^{M-1}\varepsilon_{0i}\mid s_0]=P(\bigcup_{i=1}^{N}A_i)\geqslant\frac{[1-\theta(I^{*(l)})]\cdot S_1^2(A_{I^{*(l)}})}{2S_2(A_{I^{*(l)}})+[1-\theta(I^{*(l)})]\cdot S_1(A_{I^{*(l)}})}+\frac{\theta(I^{*(l)})\cdot S_1^2(A_{I^{*(l)}})}{2S_2(A_{I^{*(l)}})+[2-\theta(I^{*(l)})]\cdot S_1(A_{I^{*(l)}})}\tag{19}$$

3　仿真结果与分析

本节主要针对 Regular-LDPC 码进行仿真。Regular-LDPC 码主要由参数对 (n,j,k) 决定,其中:n 表示码字长度,也为校验矩阵的列数;j, k 分别表示校验矩阵中每列与每行所含 1 的个数。根据 Regular-LDPC 码的定义知,码率 $R=1-j/k$。仿真中用到的 Regular-LDPC 均采用 David J. C. Mackay 的随机构造思想,其校验矩阵来自 David J. C. Mackay 的主页[12]。

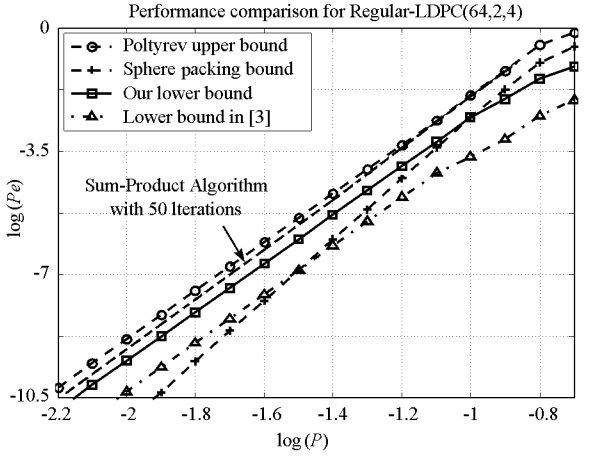

图 1　针对 Regular-LDPC (64,2,4)的性能对比

Fig. 1　Performance comparison to LDPC (64,2,4)

实验 1　针对 Regular-LDPC(64,2,4)码,比较了信道交叉概率 $p\in[10^{-2.2},10^{-0.9}]$ 范围内本文提出的下界与文献[3]提出的下界的性能优劣。为了进一步比较,同时给出了 Poltyrev upper bound、Sphere packing bound 以及采用 Sum-Product 译码算法迭代 50 次的结果,比较结果如图 1 所示。从图中可以看出,交叉概率在图中所示的范围内,本文提出的下界一直在文献[3]提出的下界的上方,更接近 Poltyrev upper bound 与采用 Sum-Product 算法实际仿真的结果,并且随着交叉概率 p 的增大,两者之间的相对差距更大,性能的相对优势更明显。另外,只有当交叉概率 p 高于 $10^{-0.995}$ 时,本文提出的下界才处于 Sphere packing bound 的下方,而文献[3]提出的下界从 $p=10^{-1.5}$ 处开始就小于 Sphere packing bound,进一步说明了本文下界的优越性能。实际上 BSC 信道的交叉概率不会太大,因此应该首先保证下界在较小的交叉概率处的性能。

实验 2　固定 $j=3$, $k=4$,仿真了码长分别为

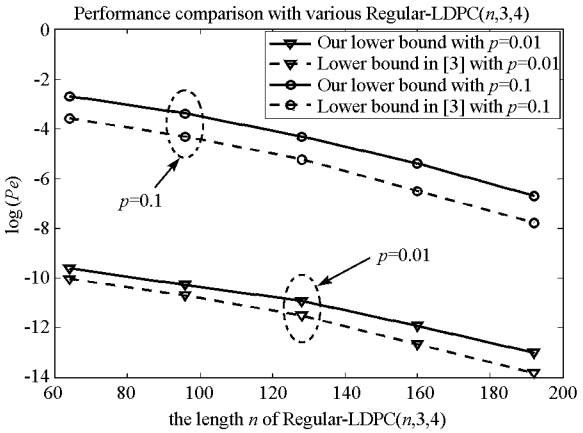

图 2　针对不同 n 的 LDPC (n,3,4)的性能对比

Fig. 2　Performance comparison to LDPC (n,3,4)

64、96、128、160 与 192 时的下界性能，对 $p=0.1$ 与 0.01 情况下下界的性能进行了对比，如图 2 所示。上方的两条曲线为 $p=0.1$ 时的下界，下方为 $p=0.01$ 时的曲线，这与“信道条件越差，通信的差错概率越高”的结论相符。从图上还可以看出：① 无论 p 取何值、码字长度为何值，新下界的性能均优于文献[3]的下界。如果固定 p 值，两者的性能差距随着码字长度的增长而增大；如果固定码字长度 n，p 值越大，两者的性能差距越大。② 在 p 值一定时，两种下界的值均随码字长度的增大而减小，码的纠错性能增强。

实验 3　针对 LDPC(96, $k-1$, k)，仿真了行重 k 分别为 3、4、6 与 8 时的下界性能，结果如图 3(a)所示；针对 LDPC(n, 3, 4)，在相同的操作系统与仿真环境下，比较了 n 取不同值时新的下界与文献[3]下界仿真时间，如图 3(b)所示。从图(a)可以看出：固定码长 n，交叉概率 p 与行重 k(列重 j 也确定)的情况下，本文提出下界优于文献[3]的下界；不过，两者之间的差距并不随行重 k 的增加(意味着码率减小)而变大，结合实验 2 的结论可知，两种下界对码率的灵敏度相当，而本文提出的下界在长码上优势更明显。从图(a)还可以知道，无论 p 取何值，两种下界并不是一直随 k 的增大而降低，这主要是因为：随着 k 增加，码率降低的同时，校验矩阵中行重与列重都会增加，对码的性能有一定的负面影响。从图(b)可以看出：本文提出的下界的仿真时间更短，随着码长增长，时间上的优势更明显，说明新下界的计算复杂度比文献[3]的低。

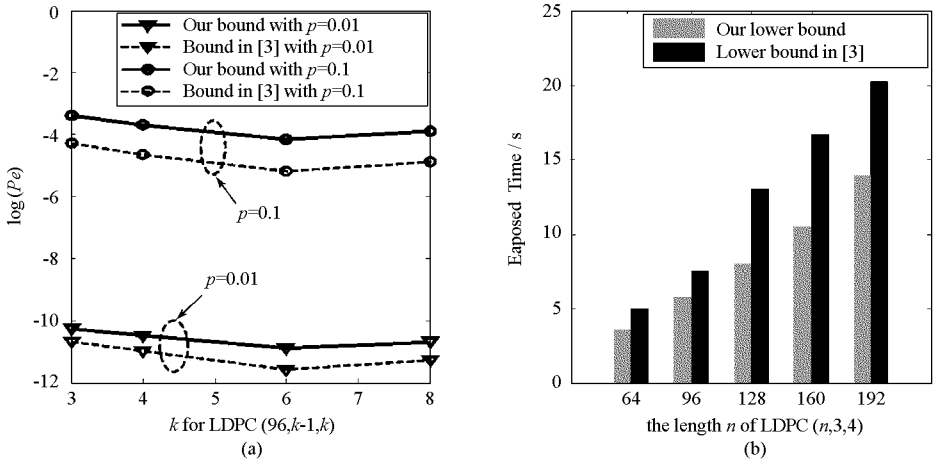

图 3　针对不同行重 k 与码长 n 的 Regular-LDPC 码的性能与时间对比

Fig.3　Performance and time comparison to LDPC with different n and k

4　结束语

本文在文献[8]的基础上提出了 BSC 信道下线性分组码差错概率事件冗余的判断准则，推导了差错概率下界的表达式，该下界只依赖于码字的 Hamming 重量分布函数与 BSC 信道的交叉概率 p。对比文献[3]提出的下界，该下界性能更优，仿真时间更短。针对不同的 Regular-LDPC 的仿真结果证明了该下界的优异性能。

参 考 文 献：

[1] Seguin G E. A Lower Bound on the Error Probability for Signals in White Gaussian Noise [J]. IEEE Trans. Inform. Theory, 1998, 44(7): 3168 – 3175.

[2] Caen D D. A Lower Bound on the Probability of a Union [J]. Discrete Mathematics, 1997, 169: 217 – 220.

[3] Cohen A, Merhav N. Lower Bounds on the Error Probability of Block Codes Based on Improvements on de Caen's Inequality [J]. IEEE Trans. Inform. Theory, 2004, 50(2): 290 – 310.

[4] Kuai H, Alajaji F, Takahara G. A Lower Bound on the Probability of a Finite Union of Events [J]. Discrete Mathematics, 2000, 215: 147 – 158.

[5] Dawson D A, Sankoff D. An Inequality for Probabilities [C]//Proc. Amer. Math. Soc, 1967, 18: 504 – 507.

[6] Behnamfar F, Alajaji F, Linder T. Improved Lower Bounds for the Error Rate of Linear Block Codes [C]//Proceedings 43rd Allerton Conference on Control, Computing and Communications, Monticello, Illinois, USA, 2005: 2227 – 2236.

[7] Keren O, Litsyn S. A Lower Bound on the Probability of Decoding Error over a BSC Channel [C]//Proc. 21st IEEE Electrical and Electronic Engineers in Israel Conf, 2000: 271 – 273.

[8] Hoppe F M. The Effect of Redundancy on Probability Bounds [J]. Discrete Mathematics, 2009: 123 – 127.

[9] Sason I, Shamai S. Performance Analysis of Linear Codes Under Maximum-Likelihood Decoding: A Tutorial [J]. Foundations and Trends in Communications and Information Theory, 2006, 3(1 – 2): 1 – 222.

[10] Hof E, Sason I, Shamai S. Performance Bounds for Nonbinary Linear Block Codes Over Memoryless Symmetric Channels [J]. IEEE Trans. Inform. Theory, 2009, 55(3): 977 – 996.

[11] 许拔，何英亮，杨少华，等. AWGN 信道下线性分组码的差错概率下界分析[J]. 国防科技大学学报, 2010, 32(2): 103 – 108.

[12] http://www.inference.phy.cam.ac.uk/mackay/CodesFiles.html.