

# 基于软判决下的不删余极化码参数识别

吴昭军<sup>1</sup>, 钟兆根<sup>2</sup>, 张立民<sup>1</sup>, 但波<sup>3</sup>

(1. 海军航空大学航空作战勤务学院, 山东 烟台 264001; 2. 海军航空大学航空基础学院, 山东 烟台 264001;  
3. 海军航空大学岸防兵学院, 山东 烟台 264001)

**摘要:** 针对极化码盲识别问题, 首先证明了能表征实际极化码码长、码率关系的定理 1 和定理 2 及区别冻结比特位和信息比特位的定理 3。基于这 3 个定理, 通过遍历可能的码长值, 构建了码字矩阵和克罗内克矩阵, 然后遍历信息比特位, 检测码字空间与疑似对偶空间的校验关系。为了检测校验关系, 引入了对数似然比概念, 基于其统计特性和最优准则, 估计出该遍历码长下的码率及信息比特位置, 最终完成参数的识别。仿真结果表明, 3 个定理的结论与仿真结果一致, 且算法具有较强的容错性, 在信噪比为 6.5 dB、码长为 1 024 条件下, 参数识别率能够达到 98% 以上。

**关键词:** 极化码; 软判决; 码长; 信息比特位; 冻结比特位; 识别

**中图分类号:** TN911.7

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-436x.2020254

## Recognition of non-drilled polar codes based on soft decision

WU Zhaojun<sup>1</sup>, ZHONG Zhaogen<sup>2</sup>, ZHANG Limin<sup>1</sup>, DAN Bo<sup>3</sup>

1. The School of Aviation Support, Naval Aviation University, Yantai 264001, China  
2. The School of Basis of Aviation Science, Naval Aviation University, Yantai 264001, China  
3. The School of Coastal Defense, Naval Aviation University, Yantai 264001, China

**Abstract:** In order to solve the problem of the blind recognition of polar codes, the theorem 1 and theorem 2 were proved firstly, which reflects the relationship between length and rate of actual polar codes, and then theorem 3 which could distinguish frozen bit and information bit positions was also proved. Based on these three theorems, the codewords matrixes and Kronecker matrixes were constructed by traversing the possible code length values. Then the information bits were traversed to detect the check relationship between the codewords and the suspected dual space. In order to detect the check relationship, log likelihood ratio was introduced, based on its characteristics and optimal criteria, the code rate and information bit positions were estimated. The simulation results show that the conclusions of the three theorems are consistent with the results. At the same time, the proposed algorithm has a strong error tolerance. Under 6.5 dB and code length of 1024, the rate of recognition can reach more than 98%.

**Key words:** polar code, soft decision, code length, information bit position, frozen bit position, recognition

## 1 引言

为了对抗信道噪声的干扰, 信道编码技术被广泛应用于无线通信系统中。在各种信道编码类型

中, 极化码是已从理论上证明, 性能可逼近香农极限的编码, 目前这种编码已经被确定为 5G 通信中 eMBB 场景控制信道的编码方案, 可以预见, 在不久的将来, 应用了极化码的数字通信系统会越来越

收稿日期: 2020-09-16; 修回日期: 2020-12-01

通信作者: 钟兆根, zhongzhaogen@163.com

基金项目: 国家自然科学基金资助项目 (No.91538201); 泰山学者工程专项经费基金资助项目 (No.ts201511020); 信息系统安全技术重点实验室基金资助项目 (No.6142111190404)

**Foundation Items:** The National Natural Science Foundation of China (No.91538201), The Taishan Scholar Special Foundation (No.ts201511020), The National Key Laboratory of Science and Technology on Information System Security (No.6142111190404)

多地出现，然而，针对极化码参数识别的研究目前还未见报道，对于非合作通信领域而言，极化码参数识别问题是一个亟待解决的问题。

目前，信道编码盲识别问题已经是非合作通信领域研究的热点。从公开发表的文献来看，针对编码识别的算法主要集中于线性分组码、循环码、卷积码、Turbo 码、LDPC (low density parity check) 码等，而单独针对极化码参数识别的算法还未见公开报道。针对线性分组码而言，目前大部分算法主要基于秩准则算法<sup>[1-3]</sup>完成参数识别，这种算法计算量大，且容错性不好；为了提高秩准则方法的容错性，文献[4]分析了码字经高斯消元后，每一列上 0-1 分布特征，通过设定门限识别出线性相关列，从而检测出秩亏，该方法容错性有较大的提升，但是计算复杂度有明显的增加；文献[5]在高斯信道下，基于码字之间的欧氏距离分布，对码字进行聚类，从而识别出码长、生成矩阵等参数，该方法适用于低码率、短码长下的分组码；针对循环码而言，目前算法主要基于其严格的代数结构进行识别，如基于码重统计方法<sup>[6]</sup>、欧几里得辗转相除法<sup>[7]</sup>及基于多项式分解算法<sup>[8-9]</sup>等，这些方法都具有较好的工程实用性；针对卷积码而言，文献[10]采用迭代的高斯消元方法获取对偶向量，由于卷积码约束长度较短，故该方法实时性较好，同时还具有一定的容错性；为了进一步提升文献[10]算法的容错性，文献[11-13]提出基于快速 Walsh-Hadamard 变换 (FWHT, fast Walsh-Hadamard transform) 的识别方法，该方法本质上是一种穷举算法，虽然具有较好的容错性，但是随着约束长度增加，算法的计算复杂度呈指数增加；此外还有欧几里得算法<sup>[14]</sup>、快速双合冲算法<sup>[15]</sup>等，这些算法复杂度低，适用于低误码情况；由于 Turbo 码编码结构较为复杂，故针对 Turbo 码识别主要分为三部分，即帧结构识别、分量编码器识别和随机交织识别。对于帧结构识别，文献[16-17]充分利用了 Turbo 码的编码结构，提出了基于差分预处理的参数识别方法，该方法能够在信道环境恶劣的情况下，完成 Turbo 码帧同步、交织长度及码率等参数识别，这为后续分量编码器及交织器识别准备了条件；针对分量编码器，文献[18-19]构造出关于多项式系数的目标函数，然后基于梯度迭代优化的方法求解多项式系数，该方法具有较强的实用性；对于随机交织器识别，文献[20-21]综合了校验符合度方法及 Turbo 码反馈迭代译码的思想，提出了预估矫

正识别方法，该方法具有较强的容错性，克服了随交织长度增加，算法性能会急剧恶化的问题；针对 LDPC 码的识别，文献[22-23]首次提出了基于高斯消元及 2 阶、多阶行消元的稀疏校验矩阵重建方法；为了提升重建方法的容错性，文献[24]将 LDPC 码迭代译码的思想引入重建过程中，这使在有噪声条件下，LDPC 码重建率有较大的提高，但是计算复杂度也有较大幅度的增加。从上述分析来看，单独针对极化码参数识别的算法还未出现，而目前实际工程中极化码的应用越来越广泛，对于非合作通信而言，极化码参数识别问题是一个亟待解决的难题。

基于此，本文提出了基于软判决序列下的不删余极化码识别算法，该算法基于极化码的编码结构，首先给出并证明了有关极化码码长、信息比特与冻结比特位置的 3 个定理，这 3 个定理是识别极化码参数的理论基础；其次，引入了对数似然比 (LLR, log-likelihood ratio) 概念，为了检测极化码信息比特与冻结比特位置，详细分析了 LLR 的统计特性，基于最小错误判决准则，设定最优判决门限，最终实现了参数的识别。仿真结果证明了所提算法的有效性及其较好的容错性。

## 2 极化码基本原理

对于一个二进制离散无记忆信道  $W$  重复使用  $n$  次，可以得到  $n$  个相互独立的信道，然后通过某种线性变换，将其转化为  $n$  个相互关联的信道  $W_n^i: X \rightarrow Y^n X^{i-1}$ ，其中， $X$  为信道  $W$  的输入符号  $\{0,1\}$ ； $Y$  为信道输出符号，为任意实数； $Y^n$  表示  $Y$  的  $n$  维随机向量， $X^{i-1}$  表示  $X$  的  $i-1$  维随机向量。当  $n$  充分大时，极化信道  $W_n^i (1 \leq i \leq n)$  将趋近于 2 个极端，即一部分极化信道容量趋近于 1，剩余部分信道容量趋近于 0。在信息发送过程中，信息容量为 1 的极化信道用来发送信息比特，而信道容量为 0 的极化信道用来发送冻结比特（冻结比特通常为 0），从而实现信息快速可靠的发送。极化码原理包含信道合并、信道分裂两部分，下面分别就信道合并、信道分裂及编码方法进行简要介绍。

### 2.1 信道合并过程

将  $n$  个独立无关联的信道合并成  $W_n: X^n \rightarrow Y^n$ ，其中  $n=2^m$ 。在信道合并过程中，由于系统的信道容量不变，信道的转移概率为

$$W_n(y_1^n | u_1^n) = W^n(y_1^n | u_1^n G_n) \quad (1)$$

其中,  $\mathbf{y}_1^n$  为信道输出符号, 即  $\mathbf{y}_1^n = (y_1, y_2, \dots, y_n)$ ;  $\mathbf{u}_1^n$  为信道输入符号, 即  $\mathbf{u}_1^n = (u_1, u_2, \dots, u_n)$ ;  $\mathbf{G}_n$  为极化码生成矩阵。以  $n=2$  为例, 即  $W_2: X^2 \rightarrow Y^2$ , 该信道由 2 个独立的信道  $W$  经信道合并而成, 如图 1 所示。

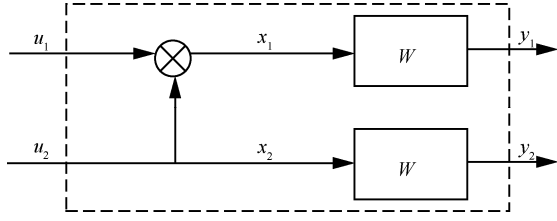


图1  $W_2$  信道结构

此时,  $W_2$  的信道转移概率为

$$W_2(y_1, y_2 | u_1, u_2) = W(y_1 | u_1 \oplus u_2)W(y_2 | u_2) = W^2((y_1, y_2) | (u_1 \oplus u_2, u_2)) = W^2(\mathbf{y}_1^2 | \mathbf{u}_1^2 \mathbf{G}_2) \quad (2)$$

其中,  $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ 。

对于一个码长为  $n$  ( $n=2^m$ ) 的极化码, 其生成矩阵满足条件<sup>[25]</sup>为

$$\mathbf{G}_n = \mathbf{B}_n \mathbf{F}^{\otimes m} \quad (3)$$

其中,  $\mathbf{B}_n$  为比特反转置换矩阵, 主要作用为将矩阵  $\mathbf{F}^{\otimes m}$  的行顺序按照某种规则置换。以  $n$  等于 4 为例, (0,1,2,3) 的二进制数为 (00,01,10,11), 将其二进制反转后得到 (00,10,01,11), 对应的十进制数为 (0,2,1,3), 从而得到比特反转置换矩阵为

$$\mathbf{B}_n = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (4)$$

而  $\mathbf{F}^{\otimes m}$  为  $\mathbf{F}$  的  $m$  次克罗内克幂矩阵。在给出克罗内克幂矩阵定义之前, 首先给出两矩阵克罗内克积的定义, 设矩阵  $\mathbf{A}_{J \times T} = [a_{i,j}] (1 \leq i \leq J, 1 \leq j \leq T)$ , 矩阵  $\mathbf{Q}_{R \times S} = [q_{i,j}] (1 \leq i \leq R, 1 \leq j \leq S)$ , 则矩阵  $\mathbf{A}_{J \times T}$  与  $\mathbf{Q}_{R \times S}$  的克罗内克积定义为

$$\mathbf{A}_{J \times T} \otimes \mathbf{Q}_{R \times S} = \begin{bmatrix} a_{1,1} \mathbf{Q}_{R \times S} & a_{1,2} \mathbf{Q}_{R \times S} & \cdots & a_{1,T} \mathbf{Q}_{R \times S} \\ a_{2,1} \mathbf{Q}_{R \times S} & a_{2,2} \mathbf{Q}_{R \times S} & \cdots & a_{2,T} \mathbf{Q}_{R \times S} \\ \vdots & \vdots & \ddots & \vdots \\ a_{J,1} \mathbf{Q}_{R \times S} & a_{J,2} \mathbf{Q}_{R \times S} & \cdots & a_{J,T} \mathbf{Q}_{R \times S} \end{bmatrix} \quad (5)$$

此时矩阵  $\mathbf{A}_{J \times T}$  与  $\mathbf{Q}_{R \times S}$  的克罗内克积结果为

$JR \times TS$  的矩阵, 而  $\mathbf{F}$  的  $m$  次克罗内克幂矩阵为  $\mathbf{F}^{\otimes m} = \mathbf{F} \otimes \mathbf{F}^{\otimes m-1}$ , 其中  $\mathbf{F}^{\otimes 0} = 1$ , 通常有  $\mathbf{F} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ , 故有

$$\mathbf{F}^{\otimes m} = \begin{bmatrix} \mathbf{F}^{\otimes m-1} & \mathbf{0} \\ \mathbf{F}^{\otimes m-1} & \mathbf{F}^{\otimes m-1} \end{bmatrix} \quad (6)$$

### 2.2 信道分裂过程

将  $n$  个相互独立的信道经过信道合并, 得到  $W_n$ , 然后将  $W_n$  分裂为  $n$  个相互关联的信道  $\{W_n^i: X \rightarrow Y^n \times X^{i-1}\}, 1 \leq i \leq n$ , 则分裂后的子信道  $W_n^i$  的转移概率<sup>[25]</sup>为

$$W_n^i(\mathbf{y}_1^n, \hat{\mathbf{u}}_1^{i-1} | u_i) = \sum_{\mathbf{u}_{1:i}^n \in X^{n-i}} \frac{1}{2^{n-i}} W_n(\mathbf{y}_1^n | \mathbf{u}_1^n) \quad (7)$$

其中,  $(\mathbf{y}_1^n, \hat{\mathbf{u}}_1^{i-1})$  与  $u_i$  为分裂子信道  $W_n^i$  的输入与输出,  $\mathbf{y}_1^n$  为分裂信道的输入,  $\hat{\mathbf{u}}_1^{i-1}$  为已估计的前  $i-1$  个信息序列。对于子信道  $W_n^i$  的转移概率, 通常采用递推迭代关系<sup>[25]</sup>来计算, 即

$$W_{2n}^{2i-1}(\mathbf{y}_1^{2n}, \hat{\mathbf{u}}_1^{2i-2} | u_{2i-1}) = \sum_{u_{2i}} \frac{1}{2} W_n^i(\mathbf{y}_1^n, \hat{\mathbf{u}}_{1,o}^{2i-1} \oplus \hat{\mathbf{u}}_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}) W_n^i(\mathbf{y}_{n+1}^{2n}, \hat{\mathbf{u}}_{1,e}^{2i-2} | u_{2i}) \quad (8)$$

$$W_{2n}^{2i}(\mathbf{y}_1^{2n}, \hat{\mathbf{u}}_1^{2i-1} | u_{2i}) = \frac{1}{2} W_n^i(\mathbf{y}_1^n, \hat{\mathbf{u}}_{1,o}^{2i-2} \oplus \hat{\mathbf{u}}_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}) W_n^i(\mathbf{y}_{n+1}^{2n}, \hat{\mathbf{u}}_{1,o}^{2i-2} | u_{2i}) \quad (9)$$

其中,  $\hat{\mathbf{u}}_{1,o}^{2i-1}$  表示估计出的前  $2i-1$  个序列中奇数位置上的信息, 而  $\hat{\mathbf{u}}_{1,e}^{2i-2}$  表示已估计出的前  $2i-1$  个序列中偶数位置上的信息。

$n$  个独立信道经过线性变换合并为  $W_n$ , 然后分裂为  $n$  个相互关联的子信道  $W_n^i (1 \leq i \leq n)$ , 当  $n$  趋近于无穷大时, 一部分子信道容量会趋近于 1, 而其余子信道容量会趋近于 0, 这就是信道极化现象。为了衡量量子信道的可靠性, 引入巴氏参数<sup>[25]</sup>, 其定义为

$$Z(W) = \sum_{y \in Y} \sqrt{W(y|0)W(y|1)} \quad (10)$$

从信道可靠性而言, 巴氏参数含义正好与信道容量相反, 即  $Z(W)$  值越大, 信道可靠性越差, 对于巴氏参数的计算, 目前有密度进化方法、高斯进

化方法等，当信道为二进制删除信道时，巴氏参数的递推计算表达式<sup>[25]</sup>为

$$Z(W_{2n}^{2i}) = Z(W_n^i)^2 \quad (11)$$

图 2 给出了在接收端擦除符号误判概率为 0.5 下，码长为 1 024，码率为  $\frac{1}{2}$  的极化码信道巴氏参数分布，从图 2 可以明显看出分裂信道的可靠性趋近于 2 个极端。

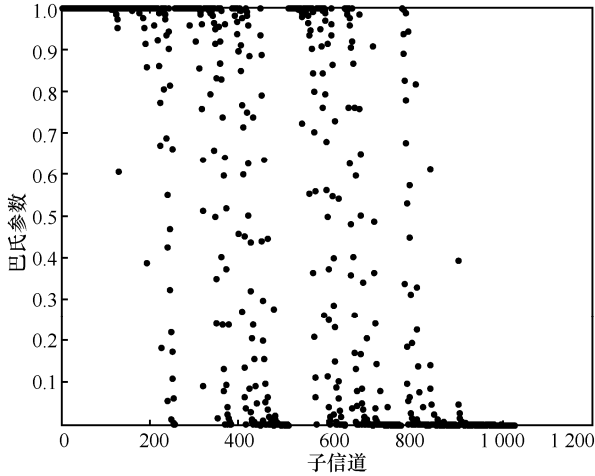


图 2 子信道的巴氏参数分布

### 2.3 极化码编码

极化码主要利用信道极化的思想来编码，即利用可靠性较高的分裂信道来传输有用的信息比特，而利用可靠性较差的子信道传输冻结比特。设极化码中信息比特位置集合为  $A = \{\pi(1), \pi(2), \dots, \pi(k)\}$ ，其补集  $A^c = \{1, 2, \dots, n\} \setminus A$ ，对应的极化码码率为  $\frac{k}{n}$ ，其编码  $x_1^n$  为

$$x_1^n = u_A G_n(A) \oplus u_{A^c} G_n(A^c) \quad (12)$$

其中， $G_n$  已由式(3)给出， $G_n(A)$  的行向量在  $G_n$  中的标号为集合  $A$ ， $G_n(A^c)$  的行向量在  $G_n$  中的标号对应于集合  $A^c$ ， $u_A$  为发送的信息比特， $u_{A^c}$  为冻结比特，通常冻结比特为 0，故  $u_{A^c}$  为全零向量，式(12)可以进一步简化为  $x_1^n = u_A G_n(A)$ 。

由极化码的编码结构可知，对于不删余极化码盲识别而言，需要识别的参数为极化码码长、信息比特位及冻结比特位。由于在实际通信系统中，发送的数据都有固定的帧结构，在每一帧数据前会有 2 B 的同步码，故本文假设已经利用帧同步码完成了码字同

步，主要的研究内容是利用软判决序列完成不删余极化码码长、信息比特位置及冻结比特位置的识别。

## 3 极化码识别模型建立

### 3.1 极化码码长识别

由于极化码码长满足  $n = 2^m$  ( $m$  为正整数) 关系，故可以遍历  $m$  的值，构造不同码长下的码字，然后寻找某固定的特征，实现极化码码长识别，在给出具体的码长识别步骤之前，首先给出定理 1 及定理 2。

**定理 1** 对于码长为  $n$ ，码率为  $\frac{k}{n}$  的极化码码

字  $(c_1, c_2, \dots, c_n)$ ，如果将其分割为长度为  $\frac{n}{2}$  的码字  $(c_1, c_2, \dots, c_{\frac{n}{2}}), (c_{\frac{n}{2}+1}, c_{\frac{n}{2}+2}, \dots, c_n)$ ，则  $(c_1, c_2, \dots, c_{\frac{n}{2}}), (c_{\frac{n}{2}+1}, c_{\frac{n}{2}+2}, \dots, c_n)$  等价于码长为  $\frac{n}{2}$  的极化码，且其码率大于  $\frac{k}{n}$ 。

**证明** 设原极化码码长为  $n = 2^m$ ，首先构造  $m$  次

的克罗内克幂矩阵，即  $F^{\otimes m} = \begin{bmatrix} F^{\otimes m-1} & \mathbf{0}_{2^{m-1} \times 2^{m-1}} \\ F^{\otimes m-1} & F^{\otimes m-1} \end{bmatrix}$ ，

其中， $\mathbf{0}_{2^{m-1} \times 2^{m-1}}$  是维度为  $2^{m-1} \times 2^{m-1}$  的全零矩阵。经过矩阵  $B_n$  行置换后  $F^{\otimes m}$  变为  $G_n$ ，抽取用于发送信息比特位置集合  $A = (\pi(1), \pi(2), \dots, \pi(k))$ ，不妨设  $(\pi(1), \pi(2), \dots, \pi(i))$  为集合  $\{1, 2, \dots, \frac{n}{2}\}$  的子集，而  $(\pi(i+1), \pi(i+2), \dots, \pi(k))$  为集合  $\{\frac{n}{2}+1, \frac{n}{2}+2, \dots, n\}$  的子集，则极化码的生成矩阵为

$$G_n(A) = \begin{bmatrix} g_{\pi(1),1} & g_{\pi(1),2} & \cdots & g_{\pi(1),\frac{n}{2}} & 0 & 0 & \cdots & 0 \\ g_{\pi(2),1} & g_{\pi(2),2} & \cdots & g_{\pi(2),\frac{n}{2}} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{\pi(i),1} & g_{\pi(i),2} & \cdots & g_{\pi(i),\frac{n}{2}} & 0 & 0 & \cdots & 0 \\ g_{\pi(i+1),1} & g_{\pi(i+1),2} & \cdots & g_{\pi(i+1),\frac{n}{2}} & g_{\pi(i+1),1} & g_{\pi(i+1),2} & \cdots & g_{\pi(i+1),\frac{n}{2}} \\ g_{\pi(i+2),1} & g_{\pi(i+2),2} & \cdots & g_{\pi(i+2),\frac{n}{2}} & g_{\pi(i+2),1} & g_{\pi(i+2),2} & \cdots & g_{\pi(i+2),\frac{n}{2}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{\pi(k),1} & g_{\pi(k),2} & \cdots & g_{\pi(k),\frac{n}{2}} & g_{\pi(k),1} & g_{\pi(k),2} & \cdots & g_{\pi(k),\frac{n}{2}} \end{bmatrix} \quad (13)$$

其中,  $\mathbf{G}_n(\mathbf{A})$  中第  $j$  行元素对应于  $\mathbf{G}_n$  中第  $\pi(j)$  行元素。当码长为  $n$  的极化码被分割为码长为  $\frac{n}{2}$  的码字后, 对应的新码字生成矩阵变为

$$\mathbf{G}'_{\frac{n}{2}} = \begin{bmatrix} \mathbf{g}_{\pi(1),1} & \mathbf{g}_{\pi(1),2} & \cdots & \mathbf{g}_{\pi(1),\frac{n}{2}} \\ \mathbf{g}_{\pi(2),1} & \mathbf{g}_{\pi(2),2} & \cdots & \mathbf{g}_{\pi(2),\frac{n}{2}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{g}_{\pi(i),1} & \mathbf{g}_{\pi(i),2} & \cdots & \mathbf{g}_{\pi(i),\frac{n}{2}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{g}_{\pi(k),1} & \mathbf{g}_{\pi(k),2} & \cdots & \mathbf{g}_{\pi(k),\frac{n}{2}} \end{bmatrix} \quad (14)$$

式(14)去除矩阵  $\mathbf{G}_n(\mathbf{A})$  对折后出现的重复行后, 分2种情况来讨论矩阵  $\mathbf{G}'_{\frac{n}{2}}$  的秩情况。

**情况 1** 矩阵  $\mathbf{G}'_{\frac{n}{2}}$  中每一行向量互不相同。

由于  $\mathbf{G}'_{\frac{n}{2}}$  本质上是由  $\mathbf{G}_n(\mathbf{A})$  对折得到的, 故  $\mathbf{G}'_{\frac{n}{2}}$  每一行元素都能在  $m-1$  次的克罗内克幂矩阵中出现, 因此  $\mathbf{G}'_{\frac{n}{2}}$  生成的码字为码长为  $\frac{n}{2}$  的极化码。由于  $\mathbf{G}'_{\frac{n}{2}}$  中每一行向量互不相同, 故  $\mathbf{G}'_{\frac{n}{2}}$  为一个行满秩矩阵, 从而得到由  $\mathbf{G}'_{\frac{n}{2}}$  生成的码字码率为  $\frac{2k}{n}$ 。

**情况 2** 矩阵  $\mathbf{G}'_{\frac{n}{2}}$  中存在相同的行向量。

不妨设矩阵  $\mathbf{G}'_{\frac{n}{2}}$  中相同的行向量数目为  $s$  个, 由于  $m-1$  次的克罗内克幂矩阵为满秩矩阵, 故  $\mathbf{G}'_{\frac{n}{2}}$  中第 1 行到第  $i$  行以及第  $i+1$  行到第  $k$  行中不会出现重复行, 故式(14)中重复行只能出现在前  $i$  行与后  $k-i$  行的交集中, 不妨设重复行集合为  $\text{set}$ , 则有  $\text{set} = \{\mathbf{g}_{\pi(1)}, \mathbf{g}_{\pi(2)}, \dots, \mathbf{g}_{\pi(i)}\} \cap \{\mathbf{g}_{\pi(i+1)}, \mathbf{g}_{\pi(i+2)}, \dots, \mathbf{g}_{\pi(k)}\}$  (15) 其中,  $\mathbf{g}_{\pi(j)} (1 \leq j \leq k)$  为  $\mathbf{G}'_{\frac{n}{2}}$  中第  $j$  行向量。下面分  $i < \frac{k}{2}, i > \frac{k}{2}$  及  $i = \frac{k}{2}$  这 3 种情况讨论由  $\mathbf{G}'_{\frac{n}{2}}$  生成的码字码率情况。

当  $i < \frac{k}{2}$  时, 由于  $\text{set} \subseteq \{\mathbf{g}_{\pi(1)}, \mathbf{g}_{\pi(2)}, \dots, \mathbf{g}_{\pi(i)}\}$ , 故  $s \leq i < \frac{k}{2}$ , 矩阵  $\mathbf{G}'_{\frac{n}{2}}$  的秩  $k-s > \frac{k}{2}$ , 故码率  $\frac{2(k-s)}{n} > \frac{k}{n}$ 。

当  $i > \frac{k}{2}$  时, 由于  $\text{set} \subseteq \{\mathbf{g}_{\pi(i+1)}, \mathbf{g}_{\pi(i+2)}, \dots, \mathbf{g}_{\pi(k)}\}$ ,  $k-i < \frac{k}{2}$ , 故  $s \leq k-i < \frac{k}{2}$ , 同理可知, 码率  $\frac{2(k-s)}{n} > \frac{k}{n}$ 。

当  $i = \frac{k}{2}$  时, 分 2 种情况讨论。当  $\{\mathbf{g}_{\pi(1)}, \mathbf{g}_{\pi(2)}, \dots, \mathbf{g}_{\pi(i)}\} \neq \{\mathbf{g}_{\pi(i+1)}, \mathbf{g}_{\pi(i+2)}, \dots, \mathbf{g}_{\pi(k)}\}$  时, 此时  $s < i$  且  $s < k-i$ , 故  $s < \frac{k}{2}$ , 所以码率  $\frac{2(k-s)}{n} > \frac{k}{n}$ ; 当  $\{\mathbf{g}_{\pi(1)}, \mathbf{g}_{\pi(2)}, \dots, \mathbf{g}_{\pi(i)}\} = \{\mathbf{g}_{\pi(i+1)}, \mathbf{g}_{\pi(i+2)}, \dots, \mathbf{g}_{\pi(k)}\}$ , 由于极化码的信息比特位置是按照巴氏参数的大小进行选择, 故只有当  $k=n$  时, 会出现这种情况, 此时原极化码码率等于 1, 这与实际码率小于 1 的情况相矛盾, 故该情况在  $\frac{k}{n} < 1$  条件下不会出现。

综合上述几种情况可知, 经分割后的码字码率一定小于  $\frac{k}{n}$ 。证毕。

需要指出的是, 定理 1 具有递推性, 即分割的码字长度为  $\frac{n}{4}, \frac{n}{8}, \dots, 2$  时, 码率会逐渐增大, 直到增加到 1。

**定理 2** 对于码长为  $n$ , 码率为  $\frac{k}{n}$  的极化码  $(c_1, c_2, \dots, c_n), (c'_1, c'_2, \dots, c'_n)$ , 被扩展为码长为  $2n$  的  $(c_1, c_2, \dots, c_n, c'_1, c'_2, \dots, c'_n)$  码字后, 则扩展后的码字等价于新的极化码, 且新的极化码码率等于  $\frac{k}{n}$ 。

**证明** 不妨设码长为  $n$  的极化码生成矩阵为  $\mathbf{G}'_n$ , 其中每一行对应式(13)中的行标号为  $\pi'(1), \pi'(2), \dots, \pi'(k)$ , 即

$$\mathbf{G}'_n = \begin{bmatrix} \mathbf{g}_{\pi'(1),1} & \mathbf{g}_{\pi'(1),2} & \cdots & \mathbf{g}_{\pi'(1),n} \\ \mathbf{g}_{\pi'(2),1} & \mathbf{g}_{\pi'(2),2} & \cdots & \mathbf{g}_{\pi'(2),n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{g}_{\pi'(k),1} & \mathbf{g}_{\pi'(k),2} & \cdots & \mathbf{g}_{\pi'(k),n} \end{bmatrix} \quad (16)$$

扩展为码长为  $2n$  的码字生成矩阵为

$$\mathbf{G}'_{2n} = \begin{bmatrix} \mathbf{G}'_n & \mathbf{0}_{k \times n} \\ \mathbf{0}_{k \times n} & \mathbf{G}'_n \end{bmatrix} \quad (17)$$

其中,  $\mathbf{0}_{k \times n}$  为  $k \times n$  的全零矩阵。

由于  $\mathbf{G}'_{2n}$  为行满秩矩阵, 故由  $\mathbf{G}'_{2n}$  生成的码字码率为  $\frac{2k}{2n}$ , 即  $\frac{k}{n}$ 。将  $\mathbf{G}'_{2n}$  矩阵前  $n$  项与后  $n$  项相叠加, 得到

$$\mathbf{G}''_{2n} = \begin{bmatrix} \mathbf{G}'_{2n} & \mathbf{0}_{k \times n} \\ \mathbf{G}'_{2n} & \mathbf{G}'_{2n} \end{bmatrix} \quad (18)$$

由于行变换不会改变码字空间的结构, 故生成矩阵  $\mathbf{G}''_{2n}$  与  $\mathbf{G}'_{2n}$  的码字空间一样, 又因为  $\mathbf{G}''_{2n}$  的每一行正好为  $m+1$  次克罗内克幂次矩阵中一部分, 故  $\mathbf{G}''_{2n}$  生成的码字正好为码长为  $2n$  的极化码。证毕。

定理 2 同样具有递推性, 即当扩展的码长为  $4n, 8n, \dots$  时, 码率同样会保持不变。

由定理 1 和定理 2 可知, 利用截获的序列构造不同码长下的极化码码字, 当码长小于实际极化码码长时, 该码字对应的码率会大于实际的极化码码率; 反之, 当码长大于实际的码长时, 对应的码字码率会等于实际极化码码率, 由此可知, 在遍历一系列码长中, 真实的码长等于最小码率对应的最小码长。从上述分析可知, 极化码码长识别的关键在于准确识别出不同遍历码长下的码字码率, 传统方法一般基于高斯消元方法求取码率, 但是这种方法容错太长。从极化码编码原理来看, 如果能识别出克罗内克矩阵中信息比特位和冻结比特位, 则不仅可以间接识别出码率, 还能识别出极化码的生成矩阵, 下面重点讨论极化码信息比特位与冻结比特位的识别方法。

### 3.2 信息比特位与冻结比特位识别

由第 2 节中极化码的编码原理可知, 极化码的生成矩阵中每一行向量都是克罗内克幂矩阵中行向量的一部分, 故需要判断出克罗内克幂矩阵中哪些是信息比特位置, 哪些为冻结比特位置, 在给出具体的识别方法之前, 首先给出定理 3。

**定理 3** 记极化码的  $m$  次克罗内克幂矩阵为  $\mathbf{H}_n (n=2^m)$ , 发送的信息比特位置集合  $\mathbf{A} = \{\pi(1), \pi(2), \dots, \pi(k)\}$ , 剔除掉矩阵  $\mathbf{H}_n$  中第  $i$  行向量后, 得到新的矩阵为  $\mathbf{H}_n^i$ ,  $\mathbf{H}_n^i$  对应的对偶向量为  $\mathbf{h}_i$ , 当  $i \in \mathbf{A}$  且位置  $i$  对应的信息比特不为零时,  $\mathbf{h}_i$  与码字不构成交关系; 反之, 当  $i \notin \mathbf{A}$  时,  $\mathbf{h}_i$  正交于码字空间。

**证明** 不妨设  $\mathbf{H}_n$  的行向量为  $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n$ , 即

$$\mathbf{H}_n = [\mathbf{g}_1^T, \mathbf{g}_2^T, \dots, \mathbf{g}_n^T]^T \quad (19)$$

当剔除  $\mathbf{H}_n$  中第  $i$  行, 且  $i \notin \mathbf{A}$  时, 有

$$\{\mathbf{g}_{\pi(1)}, \mathbf{g}_{\pi(2)}, \dots, \mathbf{g}_{\pi(k)}\} \subseteq \{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{i-1}, \mathbf{g}_{i+1}, \dots, \mathbf{g}_n\} \quad (20)$$

不妨设由  $\mathbf{g}_{\pi(1)}, \mathbf{g}_{\pi(2)}, \dots, \mathbf{g}_{\pi(k)}$  张成的空间为  $V_1$ ,

由  $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{i-1}, \mathbf{g}_{i+1}, \dots, \mathbf{g}_n$  张成的空间为  $V_2$ , 则  $V_1 \subseteq V_2$ , 其对偶空间满足  $V_2^\perp \subseteq V_1^\perp$ , 又因为  $V_2^\perp$  由  $\mathbf{h}_i$  张成, 故有  $\mathbf{h}_i$  正交于  $V_1$ , 即  $\mathbf{h}_i$  与极化码码字正交; 当  $i \in \mathbf{A}$  且位置  $i$  对应的信息比特不为零时,  $V_1 \not\subseteq V_2$ , 故有  $V_2^\perp \not\subseteq V_1^\perp$ , 即  $\mathbf{h}_i$  不再与极化码码字正交。证毕。

从定理 3 可知, 为了识别出码长为  $n$  的极化码信息比特位, 可以首先构造  $m$  次克罗内克幂矩阵, 其中,  $n$  满足  $n=2^m$ , 然后从第 1 行到第  $n$  行依次剔除克罗内克幂矩阵中行向量, 然后求取其对应的对偶向量, 如果对偶向量与码字构成正交关系, 剔除的位置为冻结比特位, 反之则为信息比特位, 从而识别出在遍历的码长  $n$  下, 所有的信息比特位及冻结比特位, 然后间接求解出码率。由于矩阵  $\mathbf{H}_n^i$  的维度为  $(n-1) \times n$ , 故  $\mathbf{H}_n^i$  的对偶空间维度为  $1 \times n$ , 利用初等行变换与列变换可以得到

$$\mathbf{R}_i \mathbf{H}_n^i \mathbf{S}_i = \left[ \mathbf{I}_{(n-1) \times (n-1)} \mid \mathbf{P}_{(n-1) \times 1} \right] \quad (21)$$

其中,  $\mathbf{R}_i$  为行变换矩阵,  $\mathbf{S}_i$  为列变换矩阵,  $\mathbf{I}_{(n-1) \times (n-1)}$  为  $(n-1) \times (n-1)$  的单位矩阵。由式(21)可以直接获得  $\mathbf{H}_n^i$  的对偶向量  $\mathbf{h}_i$  为

$$\mathbf{h}_i = \mathbf{S}_i \begin{bmatrix} \mathbf{P}_{(n-1) \times 1} \\ 1 \end{bmatrix} \quad (22)$$

即  $\mathbf{H}_n^i \mathbf{h}_i^T = 0$ 。

由于在信息传输过程中, 码字会受到噪声的干扰, 不妨设剔除的行标号为  $k'$ , 则无论遍历的位置  $k'$  是否为冻结比特位置,  $\mathbf{h}_{k'}$  与码字都不会完全构成校验关系, 此时有必要对码字是否与  $\mathbf{h}_{k'}$  构成校验关系进行检测, 由于极化码码长较长, 硬判决序列不可避免会造成信息的丢失, 故本文利用软判决序列来对码字的校验关系进行检测。

设信号的调制方式为 BPSK, 即星座图映射方式为码元 1 映射为 +1, 0 映射为 -1。设遍历的极化码码长为  $n'$ , 利用截获的软判决序列  $\mathbf{r}$  构造出  $N$  个码字, 则码字矩阵  $\mathbf{T}$  为

$$\mathbf{T} = \begin{bmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n'} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,n'} \\ \vdots & \vdots & \ddots & \vdots \\ r_{N,1} & r_{N,2} & \cdots & r_{N,n'} \end{bmatrix} \quad (23)$$

其中,  $\mathbf{r} = [r_{1,1}, r_{1,2}, \dots, r_{1,n'}, \dots, r_{N,1}, r_{N,2}, \dots, r_{N,n'}]$ 。

设  $c_{i,j}$  ( $1 \leq i \leq N, 1 \leq j \leq n'$ ) 对应于  $r_{i,j}$  ( $1 \leq i \leq N, 1 \leq j \leq n'$ ) 的码元, 则有

$$r_{i,j} = 2c_{i,j} - 1 + n_{i,j} \quad (24)$$

其中,  $n_{i,j}$  服从均值为 0、方差为  $\sigma^2$  的高斯分布, 即  $n_{i,j} \sim \mathcal{N}(0, \sigma^2)$ 。

首先定义  $r_{i,j}$  ( $1 \leq i \leq N, 1 \leq j \leq n'$ ) 的对数似然比为

$$l_{i,j} = \ln \left( \frac{P_r(c_{i,j} = 0 | r_{i,j})}{P_r(c_{i,j} = 1 | r_{i,j})} \right) = \frac{-2r_{i,j}}{\sigma^2} \quad (25)$$

在信息比特与冻结比特位置遍历过程中, 设当遍历到第  $k'$  行时, 对应的对偶向量为  $\mathbf{h}_{k'}^T = [h_{k',1}, h_{k',2}, \dots, h_{k',n'}]^T$ 。为了方便说明码字与  $\mathbf{h}_{k'}^T$  之间的校验关系, 不妨单独提出式(23)中第  $i$  行元素来研究即  $\mathbf{r}_i = [r_{i,1}, r_{i,2}, \dots, r_{i,n'}]$ , 对应于发送时的比特序列为  $\mathbf{c}_i = [c_{i,1}, c_{i,2}, \dots, c_{i,n'}]$ , 则定义在  $\mathbf{r}_i$  条件下,  $\mathbf{c}_i$  与  $\mathbf{h}_{k'}^T$  构成校验关系的概率为

$$Y_{i,k'} = P_r \left( \sum_{t=1}^{n'} \oplus c_{i,t} h_{k',t} = 0 | \mathbf{r}_i \right) \quad (26)$$

设  $\mathbf{h}_{k'}^T$  的码重为  $w$ , 元素为 1 的位置为  $v_{k,1}, v_{k,2}, \dots, v_{k,w}$ , 则由式(26)可进一步得到

$$Y_{i,k'} = P_r \left( \sum_{t=1}^w \oplus c_{i,v_{k,t}} h_{k',t} = 0 | \mathbf{r}_i \right) \quad (27)$$

则  $Y_{i,k'}$  的对数似然比为

$$lY_{i,k'} = \ln \left( \frac{Y_{i,k'}}{1 - Y_{i,k'}} \right) = \sum_{t=1}^w \boxplus_{i,v_{k,t}} \quad (28)$$

其中, “ $\boxplus$ ” 表示盒子格运算, 即

$$x_1 \boxplus x_2 \triangleq \ln \left( \frac{1 + \tanh \frac{x_1}{2} \tanh \frac{x_2}{2}}{1 - \tanh \frac{x_1}{2} \tanh \frac{x_2}{2}} \right) \quad (29)$$

由文献[26]可知,  $lY_{i,k'}$  可进一步化简为

$$lY_{i,k'} \approx \prod_{t=1}^w \text{sign}(l_{i,v_{k,t}}) \min_{t=1, \dots, w} (|l_{i,v_{k,t}}|) \quad (30)$$

式(30)仅仅考虑了第  $i$  个码字与  $\mathbf{h}_{k'}^T$  的校验关系, 如果将全体码字考虑进去, 可进一步得到平均对数似然比, 即

$$lY_{k'} = \frac{1}{N} \sum_{i=1}^N lY_{i,k'} \quad (31)$$

本文将  $lY_{k'}$  作为  $\mathbf{h}_{k'}^T$  是否与码字构成校验关系的统计量, 首先考虑以下两类假设检验。

$\mathcal{H}_1$ :  $\mathbf{h}_{k'}^T$  与极化码码字构成校验关系, 即位置  $k'$  为冻结比特位置。

$\mathcal{H}_0$ :  $\mathbf{h}_{k'}^T$  与极化码码字不构成校验关系, 即位置  $k'$  为信息比特位置。

为了方便讨论, 令随机变量  $X_{i,k'} = \prod_{t=1}^w \text{sign}(l_{i,v_{k,t}})$ ,  $Y_{i,k'} = \min_{t=1, \dots, w} |l_{i,v_{k,t}}|$ 。在假设条件  $\mathcal{H}_0$  下, 由于  $\mathbf{h}_{k'}^T$  与码字不构成校验关系, 故  $E(lY_{i,k'} | \mathcal{H}_0) = 0$ , 由方差的计算方法可知

$$\begin{aligned} \text{Var}(lY_{i,k'} | \mathcal{H}_0) &= E(lY_{i,k'}^2 | \mathcal{H}_0) - \\ &E(lY_{i,k'} | \mathcal{H}_0)^2 = E(lY_{i,k'}^2 | \mathcal{H}_0) \end{aligned} \quad (32)$$

因为  $lY_{i,k'}^2 = X_{i,k'}^2 Y_{i,k'}^2$ , 又由于  $X_{i,k'}$  为 +1 或是 -1, 故  $X_{i,k'}^2 = 1$ , 故  $lY_{i,k'}^2 = Y_{i,k'}^2$ , 从而有  $E(lY_{i,k'}^2 | \mathcal{H}_0) = E(X_{i,k'}^2 Y_{i,k'}^2 | \mathcal{H}_0) = E(Y_{i,k'}^2 | \mathcal{H}_0)$ 。因为没有  $X_{i,k'}$  的影响, 也就不存在  $\mathcal{H}_0$  和  $\mathcal{H}_1$  限制, 故  $Y_{i,k'}^2$  的取值与假设条件  $\mathcal{H}_1$  与  $\mathcal{H}_0$  无关, 从而有  $\text{Var}(lY_{i,k'} | \mathcal{H}_0) = E(Y_{i,k'}^2)$ 。

在假设条件  $\mathcal{H}_1$  下, 由于  $\mathbf{h}_{k'}^T$  与码字存在构成校验关系, 由于受到噪声干扰, 码字中可能会出现误码。在存在误码条件下, 校验关系仍然成立的条件为码字中出现误码的位置为  $\mathbf{h}_{k'}$  中元素 1 所对应的位置, 同时出现误码的个数必须为偶数个, 由此可知, 在假设条件  $\mathcal{H}_1$  下,  $lY_{i,k'}$  的期望为

$$E(lY_{i,k'} | \mathcal{H}_1) = (2P - 1)E(Y_{i,k'} | \mathcal{H}_1) \quad (33)$$

其中,  $P$  为

$$P = \sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} C_w^{2i} p_e^{2i} (1 - p_e)^{w-2i} \quad (34)$$

其中,  $p_e$  为 BPSK 调制和噪声方差为  $\sigma^2$  下的误码率值, 即

$$p_e = 0.5 \text{erfc} \left( \sqrt{\frac{1}{2\sigma^2}} \right) \quad (35)$$

其中， $\operatorname{erfc}(x)$  为互补误差函数，定义为

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dx.$$

在假设条件  $\mathcal{H}_1$  下， $l_{i,k'}$  的方差为

$$\operatorname{Var}(l_{i,k'} | \mathcal{H}_1) = E(Y_{i,k'}^2) - E(l_{i,k'} | \mathcal{H}_1)^2 \quad (36)$$

对于  $E(Y_{i,k'}^2)$  与  $E(l_{i,k'} | \mathcal{H}_1)$  而言，可以利用期望的定义，直接利用截获的软判决序列求取。

在假设条件  $\mathcal{H}_0$  与  $\mathcal{H}_1$  下，随机变量  $l_{i,k'}$  统计特性得到之后，本文可以很容易得到  $l_{i,k'}$  在两类假设条件下的均值与方差，即  $E(l_{i,k'} | \mathcal{H}_0) = 0$ ，

$$\operatorname{Var}(l_{i,k'} | \mathcal{H}_0) = \frac{\operatorname{Var}(X_{i,k'} Y_{i,k'} | \mathcal{H}_0)}{N}, \quad E(l_{i,k'} | \mathcal{H}_1) =$$

$$E(X_{i,k'} Y_{i,k'} | \mathcal{H}_1), \quad \operatorname{Var}(l_{i,k'} | \mathcal{H}_1) = \frac{\operatorname{Var}(X_{i,k'} Y_{i,k'} | \mathcal{H}_1)}{N}.$$

为方便描述，记  $\mu_0 = E(l_{i,k'} | \mathcal{H}_0)$ ， $\sigma_0^2 = \operatorname{Var}(l_{i,k'} | \mathcal{H}_0)$ ， $\mu_1 = E(l_{i,k'} | \mathcal{H}_1)$ ， $\sigma_1^2 = \operatorname{Var}(l_{i,k'} | \mathcal{H}_1)$ 。

设两类假设的判决门限为  $A$ ，则虚警概率  $P_f$  与漏警概率  $P_a$  分别为

$$P_f = \int_A^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_0} e^{-\frac{(x-\mu_0)^2}{2\sigma_0^2}} dx \quad (37)$$

$$P_a = \int_{-\infty}^A \frac{1}{\sqrt{2\pi}\sigma_1} e^{-\frac{(x-\mu_1)^2}{2\sigma_1^2}} dx \quad (38)$$

在无先验知识的情况下，两类假设条件出现的概率相同，故平均错误判决概率  $P_{er}$  为

$$P_{er} = \frac{1}{2} P_f + \frac{1}{2} P_a \quad (39)$$

将  $P_{er}$  对  $A$  求导数，并令其导数等于 0，得到

$$\frac{1}{\sigma_1} e^{-\frac{(A-\mu_1)^2}{2\sigma_1^2}} = \frac{1}{\sigma_0} e^{-\frac{(A-\mu_0)^2}{2\sigma_0^2}} \quad (40)$$

式(40)等号两边取对数，将其化为一元二次方程，求得最小错误判决门限为

$$A_{opt} = \frac{(\sigma_0^2 \mu_1 - \sigma_1^2 \mu_0) - \sigma_0 \sigma_1 \sqrt{(\mu_0 - \mu_1)^2 + (\sigma_1^2 - \sigma_0^2) \ln \frac{\sigma_1}{\sigma_0}}}{(\sigma_0^2 - \sigma_1^2)} \quad (41)$$

利用截获的数据构造出不同码长的极化码，然后剔除  $m$  次克罗内克矩阵中第  $k'$  行元素，求解校

验向量，同时计算统计量  $l_{i,k'}$  及门限  $A_{opt}$ ，一旦  $l_{i,k'} > A_{opt}$  时，可以断定位置  $k'$  为冻结信息位置，反之则判定为信息比特位置，从而实现极化码生成矩阵的识别。

### 3.3 极化码参数识别算法流程

利用 3.2 节中求解的门限  $A_{opt}$  与统计量  $l_{i,k'}$  进行比较，一旦  $l_{i,k'} \leq A_{opt}$ ，则判定假设条件  $\mathcal{H}_0$  成立，此时剔除的矩阵行对应的位置可判定为信息比特位置，从而实现在该遍历码长下码率及信息比特位置的识别，最后利用定理 1 和定理 2 的结论识别出真实极化码码长，同时获得该码长下的信息比特位置，具体如算法 1 所示。

#### 算法 1 极化码参数识别算法

输入  $n_{min}, n_{max}$ , 软判决序列  $r$

输出 码长  $\hat{n}$  与生成矩阵  $\hat{G}$

1) 初始化:  $j = 0$ ,  $\mathbf{set} = \emptyset$

2) for  $n = n_{min}$  to  $n_{max}$  do

3)  $\mathit{cout} = 0$ ,  $j = j + 1$ ,  $\mathbf{set}_0 = \emptyset$

4) 构造  $m$  次的克罗内克矩阵  $\mathbf{D}_{n \times n}$  及码长为  $n$  的码字矩阵

5) for  $k' = 1$  to  $n$  do

6) 剔除  $\mathbf{D}_{n \times n}$  中第  $k'$  行元素，求取对偶

向量  $\mathbf{h}_k^T$

7) 求取统计量  $l_{i,k'}$  与门限  $A_{opt}$

8) if  $l_{i,k'} < A_{opt}$  do

9) 判定位置  $k'$  为信息比特位置

10)  $\mathit{cout} = \mathit{cout} + 1$

11)  $\mathbf{set}_0 = [\mathbf{set}_0; \mathbf{D}_{n \times n}(k', :)]$

12) end if

13) end for

14) end for

14)  $\rho(j) = \frac{\mathit{cout}}{n}$

15)  $\mathit{index} = \mathit{find}(\rho = \min(\rho))$

16)  $\hat{n} = 2^{\mathit{lb}(n_{min}) + \mathit{index}(1) - 1}$

17)  $\hat{G} = \mathbf{set}\{\mathit{index}(1)\}$

### 3.4 算法计算复杂度分析

不妨设截获的数据量为  $L$ ，遍历的码长范围为  $2^{m_{min}} \sim 2^{m_{max}}$ 。当遍历的码长为  $2^m$  ( $m_{min} \leq m \leq m_{max}$ ) 时，需要对  $2^m$  个信息比特位置进行遍历，而对每一个信息比特位置进行遍历时，需要进行  $\left\lfloor \frac{L}{2^m} \right\rfloor$  次元素

大小比较、 $\left\lfloor \frac{L}{2^m} \right\rfloor$  次向量加法运算及一次门限解算。

由于克罗内克积矩阵构造是固定的，故在识别之前，可以将对偶向量求解并保存，从而减少计算量。为方便描述，本文把一次比较大小等价于一次向量加法运算，将以此门限计算等价于 20 次向量乘法，故对码长为  $2^m$  进行遍历时，需要  $20 \times 2^m$  次向量乘法和  $L2^m$  次加法运算。对不同遍历码长下的计算量求和，得到总的乘法计算复杂度为  $\sum_{m=m_{\min}}^{m_{\max}} 20 \times 2^m$ ，加法复杂度为

$$\sum_{m=m_{\min}}^{m_{\max}} L2^m$$

。由此可见，本文算法计算量近似与截获的数据长度及遍历的最大码长成线性增加。

### 4 仿真分析

在本节仿真中，首先验证本文算法对极化码参数识别的有效性；其次，考察极化码码长、截获码字数目及码率 3 个因素对算法正确识别率的影响；

最后，对比了在硬判决与软判决 2 种条件下算法的性能，以突出软判决序列的优势。

#### 4.1 算法有效性验证

本节中设定极化码码长为 128，码率为  $\frac{1}{2}$ ，设定遍历的码长为 4~1 024（对应  $m$  取值范围为 2~10）。考察在高信噪比及低信噪比 2 种情况下算法有效性。设高信噪比为 35 dB，低信噪比为 5 dB，设定码字数为 5 000 个。在这 2 种情况下，记录不同码长对应的码率及在码长为 128 的情况下，平均 LLR 值及门限，结果如图 3 所示。

首先，从图 3(a)和图 3(c)来看，当遍历的极化码码长小于实际码长 128 时，码长逐渐减小，码率逐渐增加，直到增加到 1；而当编码的码长大于 128 时，码长逐渐增加，而码率保持不变，这与定理 1 与定理 2 的结果完全一致；其次，分析图 3(b)及图 3(d)可知，当剔除的位置为冻结比特位置时，对应的对偶向量与码字能够保持校验关系，反之当

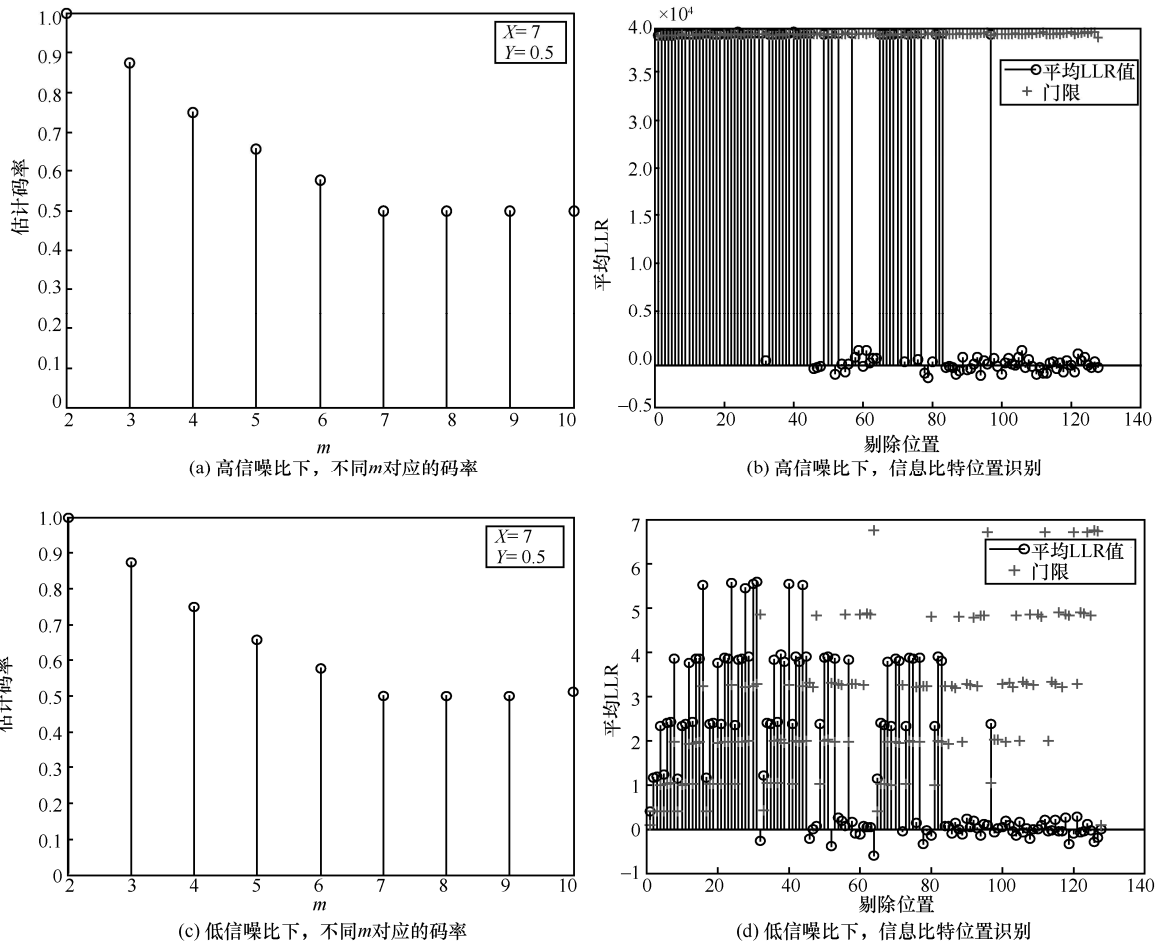


图 3 低信噪比与高信噪比下，本文所提算法的有效性验证

剔除的是信息比特位置时，对偶向量与码字之间的校验关系不在成立，这说明定理 3 的结论是一致的。通过设定的判决门限来检测这种校验关系，正好能识别出信息比特位置，从而完成极化码生成矩阵的识别。虽然图 3(d)中码字受到了噪声的干扰，但是设定的门限仍然能够有效地完成参数识别，这说明本文提出的算法对噪声具有较强的稳健性。

#### 4.2 算法容错性验证

##### 1) 码长对算法性能的影响

仿真设定极化码码长分别为 32、64、128、256、512 和 1 024，每种极化码的码率为  $\frac{1}{2}$ ，每一种极化码下的码字为 2 000 个，设定信噪比范围为  $-2 \sim 8$  dB，间隔为 0.25 dB，蒙特卡罗实验次数为 1 000，统计在不同信噪比下每种极化码参数（包括码长、信息比特位和冻结比特位）的识别率，结果如图 4 所示。

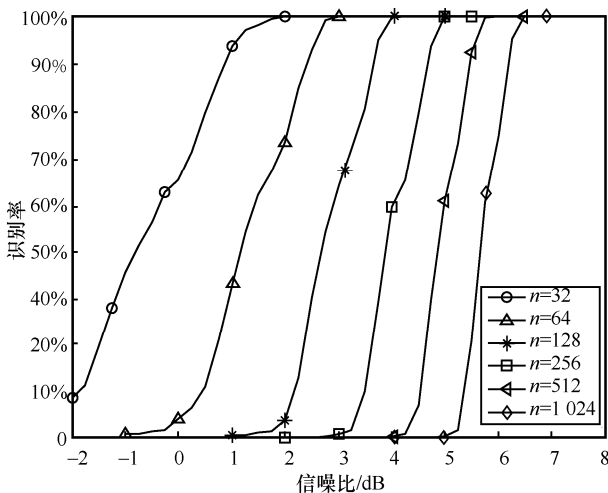


图 4 不同码长对算法影响

从图 4 结果来看，本文所提算法的性能随着码长的增加，性能逐渐变差，主要原因在于，在同一码率条件下，码长越长，需要准确识别的极化码的信息比特位置就越多，故在同等条件下，码长越长，出现对信息比特位置的误判概率就越大，故越难识别极化码参数。此外，从识别率来看，本文所提算法在信噪比为 6.5 dB 条件下，对码长为 1 024 的极化码参数识别率达到 98% 以上，这说明了算法具有较好的低信噪比稳健性。

##### 2) 码字数目对算法影响

仿真设定极化码码长为 256，码率为  $\frac{1}{2}$ ，设截

获的码字数分别为 1 000、2 000、3 000、4 000 和 5 000，信道噪声环境为 2.5~5.5 dB，蒙特卡罗实验次数为 1 000，统计在不同信噪比下，极化码参数正确识别率，结果如图 5 所示。

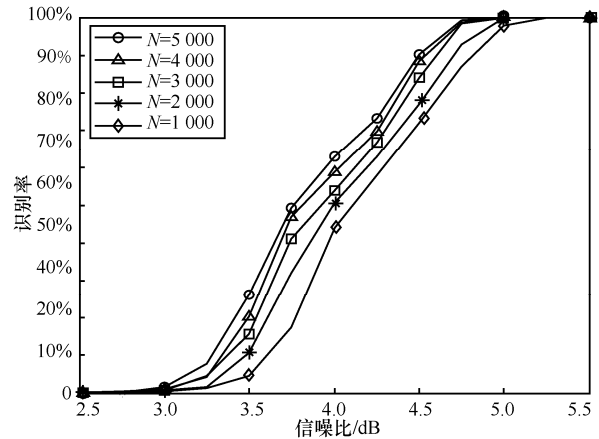


图 5 不同码字数目对算法影响

从图 5 结果来看，通过增加极化码码字数，可以有效地提高参数识别正确率。主要原因在于，码字数越大，求取的统计量就越近理论均值，此时对信息比特位置的误判概率就会减少，从而算法识别性能就增加了。

##### 3) 码率对算法影响

仿真设定极化码码长为 64 和 128，每种码长下的极化码码率分别为  $\frac{1}{4}$ 、 $\frac{1}{3}$ 、 $\frac{1}{2}$  及  $\frac{3}{5}$ 。设定截获的码字数为 2 000 个，蒙特卡罗实验次数为 1 000 次，统计 2 种码长在不同码率下极化码参数的正确识别率，结果如图 6 所示。

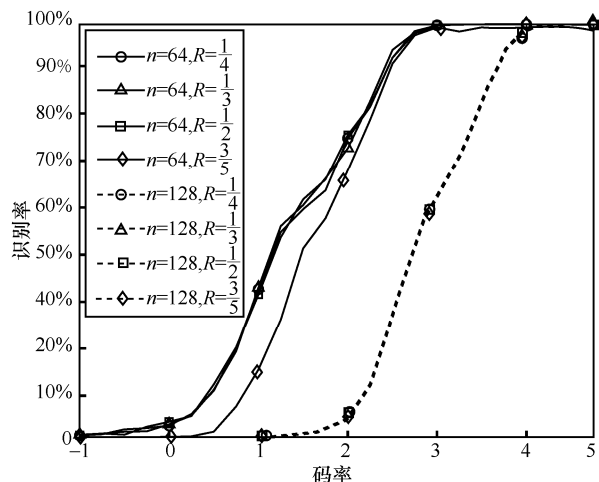


图 6 不同码率对算法的影响

从图 6 结果来看，极化码参数识别概率与码率

大小关系不大。主要原因在于，虽然码率增加，会导致信息比特位置的增加，但是在识别过程中，每种码率上的信息比特位置所对应的对偶向量码重却非常接近并且都比较小，即使码率增加，信息比特位置的误判率变化也不会太大，故在不同码率下，极化码识别非常接近。

### 4.3 与硬判决方法对比

为了突出采用软判决序列的优势，本节将采用了硬判决序列的算法进行对比。仿真设定极化码码长为 64、128、256 及 512，每种极化码码率为  $\frac{1}{2}$ ，截获的码字个数为 2 000，设定信噪比范围为 0~7 dB，间隔 0.25 dB 取值，蒙特卡罗实验次数为 1 000，统计在 2 种不同序列类型下，算法的识别性能，结果如图 7 所示。

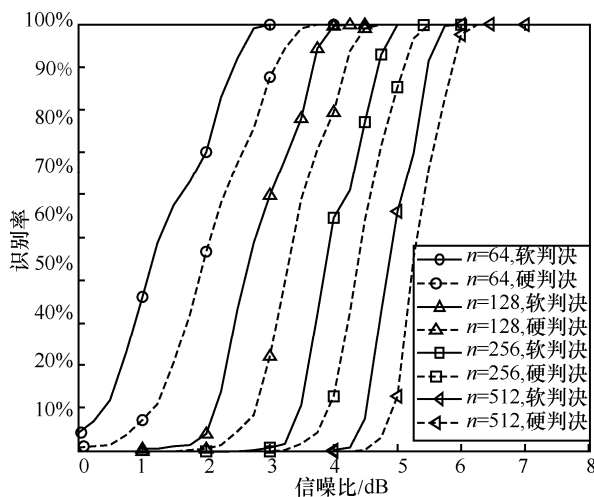


图 7 与硬判决算法对比

从图 7 结果来看，基于软判决序列的识别方法性能要明显好于基于硬判决的方法，软判决算法的性能提升近 0.5 dB。主要原因在于，与硬判决序列相比，软判决序列包含丰富的信道噪声信息，而本文所提算法能够充分利用软判决序列，故其在低信噪比下的稳健性会更强。

## 5 结束语

基于极化码的编码结构，首先给出并证明了定理 1 和定理 2，即原始极化码具有最小的码率，同时所有具有最小码率的极化码码长中，原始极化码的码长最短；其次为了求解不同码长下极化码的码率、信息比特位及冻结比特位，给出并证明了定理 3；然后为了在低信噪比情况下实现极化码信息比特位置参数识别，引入了 LLR 概念，基于定理 3 及

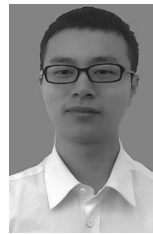
LLR 的统计特性，设定出最优的信息比特判决门限，从而在低信噪比下，快速识别出极化码编码参数。仿真结果验证了本文所提算法的有效性和较强的低信噪比下的容错性，在非合作通信领域具有较好的应用前景。

### 参考文献:

- [1] CLUZEAU M, FINIASZ M. Recovering a code's length and synchronization from a noisy intercepted bitstream[C]// 2009 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2009: 2737-2741.
- [2] RAMABADRAN S, MADHU A, KUMAR S, et al. Blind recognition of LDPC code parameters over erroneous channel conditions[J]. IET Signal Processing, 2019,13(1): 86-95.
- [3] SHARMA A, PILLAI N R. Blind recognition of parameters of linear block codes from intercepted bit stream[C]// 2016 International Conference on Computing, Communication and Automation. Piscataway: IEEE Press, 2016: 1262-1266.
- [4] 刘杰, 张立民, 占超. 基于矩阵分析的线性分组码盲识别[J]. 系统工程与电子技术, 2017,39(2):404-409.  
LIU J, ZHANG L M, ZHAN C. Blind recognition of linear block codes based on matrix analysis[J]. Systems Engineering and Electronics, 2017, 39(2):404-409.
- [5] BONVARD A, HOUCKE S, GAUTIER R, et al. Classification based on Euclidean distance distribution for blind identification of error correcting codes in noncooperative contexts[J]. IEEE Transactions on Signal Processing, 2018, 66(10): 2572-2583.
- [6] 郑瑞瑞, 汪立新. 基于码重分布概率方差的循环码识别方法[J]. 太赫兹科学与电子与信息学报, 2013, 11(5): 792-796.  
ZHENG R R, WANG L X. Recognition method of cyclic codes based on code weight distribution probability variance[J]. Journal of Terahertz Science and Electronic Information Technology, 2013,11(5): 792-796.
- [7] 杨晓静, 闻年成. 基于秩函数和 Euclidean 算法的循环码盲识别[J]. 电路与系统学报, 2012, 17(5): 120-129.  
YANG X J, WEN N C. A blind method of cyclic codes based on rank function and euclidean arithmetic[J]. Journal of Circuits and Systems, 2012, 17(5): 120-129.
- [8] 吴昭军, 张立民, 钟兆根, 等. 低信噪比下循环码识别[J]. 电子学报, 2020, 48(3): 478-485.  
WU Z J, ZHANG L M, ZHONG Z G, et al. Blind recognition of cyclic codes at low SNR[J]. Acta Electronica Sinica, 2020, 48(3): 478-485.
- [9] ARTI D Y, SARAVANAN V, ANIMESH K. Blind recognition of binary cyclic codes from unsynchronized bitstream[J]. IEEE Transactions on Communications, 2016, 64(7): 2693-2706.
- [10] MARAZIN M, GAUTIER R, BUREL G. Blind recovery of  $k/n$  rate convolutional encoders in a noisy environment[J]. EURASIP Journal on Wireless Communications and Networking, 2011(1):168-177.
- [11] HUANG L, CHEN W G, CHEN E H, et al. Blind recognition of  $k/n$  rate convolutional encoders from noisy observation[J]. Journal of Systems Engineering and Electronics, 2017, 28(2): 235-243.
- [12] 张立民, 刘杰, 钟兆根. 基于改进 Walsh-Hadamard 变换的  $(n,1,m)$  卷积码盲识别[J]. 电子与信息学报, 2018, 40(4): 839-845.  
ZHANG L M, LIU J, ZHONG Z G. Blind recognition of  $(n,1,m)$  con-

- volutional codes based on modified Walsh-Hadamard transform[J]. Journal of Electronics & Information Technology, 2018, 40(4): 839-845.
- [13] 姚智刚, 解辉, 韩壮志, 等. 基于分段 Walsh-hadamard 变换的卷积码盲重建算法[J]. 电子与信息学报, 2019, 41(9): 2047-2054.  
YAO Z G, XIE H, HAN Z Z, et al. Blind recognition of convolutional code based on partitioned Walsh-Hadamard transform[J]. Journal of Electronics & Information Technology, 2019, 41(9): 2047-2054.
- [14] 解辉, 王峰华, 黄知涛, 等. 基于改进欧几里得算法的卷积码快速盲识别算法[J]. 国防科技大学学报, 2012, 34(6): 159-162.  
XIE H, WANG F H, HUANG Z T, et al. A fast method for blind recognition of convolutional codes based on improved Euclidean algorithm[J]. Journal of National University of Defense Technology, 2012, 34(6): 159-162.
- [15] 邹艳, 陆佩忠. 关键方程的新推广[J]. 计算机学报, 2006, 29(5): 711-718.  
ZOU Y, LU P Z. A new generalization of key equation[J]. Chinese Journal of Computers, 2006, 29(5): 711-718.
- [16] 吴昭军, 张立民, 钟兆根. 高误码率下归零 Turbo 码参数识别[J]. 兵工学报, 2018, 39(4): 731-742.  
WU Z J, ZHANG L M, ZHONG Z G. Blind identification of turbo codes on trellis termination at high bit error rate[J]. ACTA Armamentarii, 2018, 39(4): 731-742.
- [17] 吴昭军, 张立民, 钟兆根, 等. 低信噪比下归零 Turbo 码码长及其帧同步识别[J]. 电子与信息学报, 2019, 41(9): 2063-2070.  
WU Z J, ZHANG L M, ZHONG Z G, et al. Blind recognition of code length and synchronization of Turbo codes on trellis termination at low SNR[J]. Journal of Electronics & Information Technology, 2019, 41(9): 2063-2070.
- [18] 吴昭军, 张立民, 钟兆根, 等. 低信噪比下 RSC 码快速迭代寻优识别算法[J]. 电子学报, 2019, 47(7): 1566-1574.  
WU Z J, ZHANG L M, ZHONG Z G, et al. Fast iterative recognition of RSC encoder at low SNR[J]. Acta Electronica Sinica, 2019, 47(7): 1566-1574.
- [19] WU Z J, ZHANG L M, ZHONG Z G. A maximum cosinoidal cost function method for parameter estimation of RSC Turbo codes[J]. IEEE Communications Letters, 2019, 23(3): 390-393.
- [20] 陈泽亮, 李静, 彭华, 等. 利用 Gibbs 采样进行优化的 Turbo 码交织器识别[J]. 电子学报, 2018, 46(1): 15-23.  
CHEN Z L, LI J, PENG H, et al. An optimization method using gibbs sampler for turbo code interleaver identification[J]. ACTA Electronica Sinica, 2018, 46(1): 15-23.
- [21] 吴昭军, 张立民, 钟兆根. 基于最大序列相关性的 Turbo 码交织器识别[J]. 航空学报, 2019, 40(6): 322764.  
WU Z J, ZHANG L M, ZHONG Z G. Blind recognition of interleaver for turbo codes based on maximum sequence correlation[J]. Acta Aeronautica et Astronautica Sinica, 2019, 40(6): 322764.
- [22] 包昕, 周磊珂, 何可, 等. 误码条件下的 LDPC 码盲识别算法[J]. 西安电子科技大学学报, 2015, 49(12): 53-58.  
BAO X, ZHOU L K, HE K, et al. A recognition algorithm for LDPC codes in a noisy environment[J]. Journal of Xi'an Jiaotong University, 2015, 49(12): 53-58.
- [23] 包昕, 周磊珂, 何可, 等. LDPC 码稀疏校验矩阵的重建方法[J]. 电子科技大学学报, 2016, 45(2): 191-196.  
BAO X, ZHOU L K, HE K, et al. A method of restructuring LDPC parity-check matrix[J]. Journal of University of Electronic Science and Technology of China, 2016, 45(2): 191-196.
- [24] 陈泽亮, 彭华, 巩克现, 等. 误码条件下 LDPC 码参数的盲估计[J]. 电子学报, 2018, 46(3): 652-658.  
CHEN Z L, PENG H, GONG K X, et al. A method for blind recognition of LDPC codes in a noisy environment[J]. ACTA Electronica Sinica, 2018, 46(3): 652-658.
- [25] ARIKAN E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels[J]. IEEE Transactions on Information Theory, 2009, 55(7): 3051-3073.
- [26] HAGENAUER J, OFFER E, PAPKL E. Iterative decoding of binary block and convolutional codes[J]. IEEE Transactions on Information Theory, 1996, 42(2): 429-445.

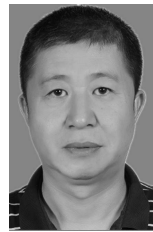
## [作者简介]



吴昭军 (1992-), 男, 四川遂宁人, 海军航空大学博士生, 主要研究方向为信道编码盲识别。



钟兆根 (1984-), 男, 江西南昌人, 博士, 海军航空大副教授, 主要研究方向为通信信号盲分离与统计信号处理。



张立民 (1966-), 男, 辽宁开原人, 博士, 海军航空大学教授, 主要研究方向为卫星信号处理及应用。

但波 (1985-), 男, 四川遂宁人, 博士, 海军航空大学讲师, 主要研究方向为目标选择与识别。