

УДК 004.56.55

**ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДА ВЫБОРА  
ЗАМОРОЖЕННЫХ БИТОВ ДЛЯ ПОЛЯРНОГО КОДА**

**Амангельдиев Азамат Нуркасымович**  
[amangeldievaza@gmail.com](mailto:amangeldievaza@gmail.com)

Магистрант кафедры «Вычислительная техника»  
ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан  
Научный руководитель - Д.Ж. Сатыбалдина

При построении полярного кода, выбор замороженных битов существенно влияет на эффективность исправления ошибок. Несколько алгоритмов, основанных на расчетах, были предложены для бинарных дискретных каналов без памяти, для каналов с аддитивным белым гауссовым шумом. Но они ограничены в применении из-за высокой сложности и временных ограничений, связанных с последовательным декодированием. В связи с этим являются актуальными исследования итеративного декодирования полярных кодов на основе алгоритма передачи сообщений по графу кодирования полярных кодов. В данной работе исследуется метод выбора замороженных битов, основанный на оптимизации по методу Монте-Карло и декодировании по методу распространения доверия. Результаты численного моделирования в среде Matlab показывают, что предлагаемый алгоритм может эффективно улучшить характеристики частоты появления ошибок по битам (BER) и частоты ошибок по кадрам (FER) по сравнению с традиционным методом выбора, особенно в области с высоким отношением сигнал-шумов. Более того, алгоритм может использоваться для построения полярных кодов с любой скоростью в течение полной итерации.

## **Введение**

Полярные коды вызвали большой исследовательский интерес в области канального кодирования, поскольку это первая схема кодирования, работающая вблизи пропускной способности для бинарных дискретных каналов без памяти (a binary-input discrete memoryless channel, B-DMC) с низкой сложностью реализации [1]. Основная проблема в построении полярных кодов состоит в том, как выбрать позиции информационных и замороженных битов. За исключением двоичного канала со стираниями при декодировании с последовательным исключением (a successive cancellation SC decoding), до сих пор не существует способа выбора оптимальных фиксированных битов для B-DMC каналов, например, для канала с аддитивным белым гауссовым шумом (an additive white Gaussian noise, AWGN). Поэтому были предложены некоторые алгоритмы выбора замороженных битов, основанные на расчетах, такие как алгоритмы эволюции плотности и Гауссова приближения [2, 3, 4]. Эти алгоритмы достигли аналогичной производительности по сравнению с эвристическим способом, введенным Ариканом [1]. Однако все представленные алгоритмы предназначены для SC декодирования. Что касается декодирования по методу распространения доверия (a belief propagation BP, decoding), то для него нет специального алгоритма оптимизации для выбора замороженных битов. Для дальнейшего улучшения возможности исправления ошибок полярного кода при декодировании BP актуальны исследования альтернативных методов, таких как выбор замороженных битов на основе моделирования.

В связи с этим целью настоящей работы является анализ эффективности метода выбора замороженных битов полярных кодов для использования алгоритма декодирования BP. Предложен метод выбора инкрементных информационных битов, основанный на моделировании по методу Монте-Карло. Имитационное моделирование выполняется в рамках модели канала AWGN, но метод выбора замороженных битов может быть применен для других моделей каналов. Мы демонстрируем конструкцию для двух полярных кодов с длиной кода 128 и 256. Результаты моделирования показывают, что предложенный алгоритм может эффективно улучшить характеристики BER и FER по сравнению с традиционным методом, особенно в области высокого соотношения сигнал-шум [1].

## **Построение полярного кода**

Важной концепцией для полярных кодов является информационный набор  $A [N]$  с количеством элементов  $K$ . Пусть  $N = 2^N$  обозначает длину кода, а  $K$  обозначает количество информационных битов, таким образом, кодовая скорость  $R = K / N$ , которая варьируется от 0 до 1.Процесс кодирования полярных кодов можно разделить на два этапа. Во-первых,

объединить  $K$  информационных битов  $u_A$  с  $(N - K)$  замороженными битами  $u_{AC}$ , чтобы получить исходный двоичный вектор  $u_{N1} = (u_A, u_{AC}) = \{u_1, u_2, \dots, u_{N-1}, u_N\}$ . Как правило,  $u_{AC}$  является нулевым вектором. Информация / фиксированные позиции битов, а именно набор  $A$  /  $A_C$ , известны как передатчику, так и приемнику. Затем этот исходный вектор  $u_{N1}$  отображается на вектор кодового слова  $x_{N1} = \{x_1, x_2, \dots, x_{N-1}, x_N\}$  посредством полярного уравнения кодирования:

$$X_{N1}^N = u_{N1}^N G^N = u_{N1}^N B^N F^{\otimes N} \quad (1)$$

где  $G^N$  - матрица генератора порядка  $N$ ,  $B^N$  - матрица перестановки битовых инверсий, а  $F^{\otimes N}$  -  $n$ -е произведение Кронекера матрицы ядра  $F$ :

$$F^{\otimes N} = F \otimes F^{\otimes N-1}, F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad (2)$$

На рис. 1 приведен фактор-график полярного кода с  $N = 8$  и  $R = 1/2$ . В этом примере,  $u_0, u_2, u_4$  и  $u_6$  являются замороженными битами и установлены в ноль. Кроме того, каждый круг в графе представляет узел, который хранит и передает сообщение убеждения [1].

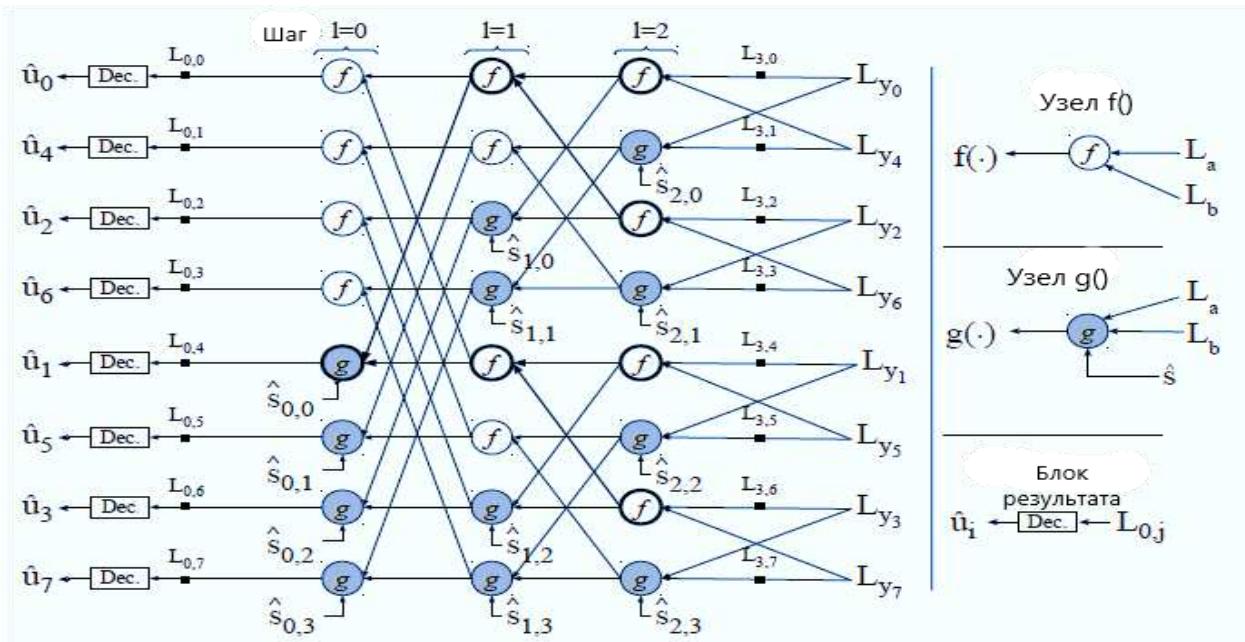


Рис. 1. Факторный график полярного кода с  $N = 8$  и  $R = 0,5$ .

### Алгоритм декодирования ВР

Полученное кодовое слово обозначается как  $y_{N1} = \{y_1, y_2, \dots, y_{N-1}, y_N\}$ , которое содержит некоторый шумовой сигнал. Декодирование ВР выполняется на основе факторного графика на рис. 1. Сообщение пересекает узел  $(i, j)$  справа налево (слева направо) и обозначается как  $L_{i,j}(R_{i,j})$ . Во-первых, самые левые исходные векторные узлы инициализируются согласно информационному набору  $A$  [1]:

$$R_{1,j} = \begin{cases} 0 & \text{if } j \in A \\ \infty & \text{if } j \in A^C \end{cases} \quad (3)$$

и самые правые узлы кодового слова иницируются с выходными значениями логарифмического отношения правдоподобия (log-likelihood ratio — LLR):

$$L_{n+1,j} = \ln \frac{P(y_j|x_j=0)}{P(y_j|x_j=1)} \quad (4)$$

Затем LLR узла будут обновляться слева направо и возвращаться обратно через граф коэффициентов как одноразовая итерация. Следуя направлению расчета доверия на общих факторных графах [1,4], все выражения итеративного декодирования ВР можно выразить как:

$$L_{i,j} = g(L_{i+1,2j-1}, L_{i+1,2j} + R_{i,j+N/2}) \quad (5)$$

$$L_{i,j+N/2} = g(R_{i,j}, L_{i+1,2j-1}) + L_{i+1,2j} \quad (6)$$

$$R_{i+1,2j-1} = g(R_{i,j}, L_{i+1,2j}) + R_{i,j+N/2} \quad (7)$$

$$R_{i+1,2j} = g(R_{i,j}, L_{i+1,2j-1}) + R_{i,j+N/2} \quad (8)$$

где  $g(x, y) = \log(\cosh((x + y)/2)) - \log(\cosh((x - y)/2))$ .

В конце концов, после достижения указанного числа итераций, жесткое решение может быть принято для каждого информационного бита в соответствии с уравнением. (6) и  $u_{N1}$ , можно получить оценку  $u_{N1}$ .

$$u_j = \begin{cases} 0 & \text{if } R_{1,j} \geq 0 \\ 1 & \text{else} \end{cases} \quad (9)$$

### **Алгоритм выбора информационных битов**

В данном разделе описан метод на основе моделирования для выбора информационных битов при ВР декодировании. Полярный код строится на основе факта поляризации канала, который указывает на то, что некоторые подканалы имеют тенденцию быть более устойчивыми, а другие - более слабыми. Чтобы выбрать информацию / замороженные биты на самом деле, чтобы выбрать надежные подканалы. В соответствующем алгоритме декодирования SC [1] каждый информационный бит декодируется на основании предположения, что все предыдущие биты декодированы правильно. Таким образом, для алгоритма выбора замороженных битов мы также можем предположить, что каждый выбор является оптимальным. Аналогично, выбор заключается в том, как выбрать один бит из  $N$  битов кодового слова в качестве информационного бита, когда все другие биты известны или остаются замороженными. Имитационное моделирование может быть применено, чтобы узнать, какой из них является лучшим выбором.

На основании вышеприведенного наблюдения информационные биты должны выбираться последовательно, и каждый шаг выбора основан на результатах предыдущих выборов. Весь алгоритм выбора сводится к следующему [4]:

Шаг 1: Инициализация. Для заданного полярного кода длиной  $N$  установить количество информационных битов равным  $K = 0$ , набор информации  $A = \{\phi\}$  и количество элементов в наборе  $A^C$  равным  $N$ .

Шаг 2: Генерация кода. Установить  $K = K + 1$ . Взять бит из набора  $A^C$  в качестве информационного бита и сгенерировать  $(N, K, A)$  полярный код. Общее число возможных кодов будет  $|A^C|$ .

Шаг 3: Моделирование. Запустить симуляцию методом Монте-Карло для всех возможных кодов  $|A^C|$  и выбрать тот, чью производительность лучше. Это  $N-K$  исчерпывающий поиск, и для каждого кода 100 кадров ошибок собираются для определенного соотношения SNR, чтобы получить статистическую оценку. Обновить наборы  $A$  и  $A^C$  в соответствии с этим лучшим кодом. Шаг 2 и шаг 3 выполняются итеративно, пока не будет достигнута желаемая скорость кодирования.

Предложенный алгоритм выбирает информационные биты инкрементно. Это гарантирует оптимальный выбор информационного бита для  $K = 1$ . Для других кодовых скоростей алгоритм получит только локальный оптимальный выбор вместо глобального оптимального выбора. Чтобы ускорить процесс выбора, можно выбрать несколько бит вместо одного бита каждый раз. Это сократит время итерации, но может привести к некоторой потере производительности.

### **Численные результаты**

С помощью предложенного алгоритма построены полярные коды с длиной кода  $N = 64$  и  $N = 128$ . Модель строится на основе модель канала AWGN и модуляции с двоичной фазовой манипуляцией (BPSK). Максимальное число итераций устанавливается равным 50. Кроме того, отношение сигнал-шум  $E_b / N_0$  устанавливается равным 4,0 дБ. Для кода с  $N =$

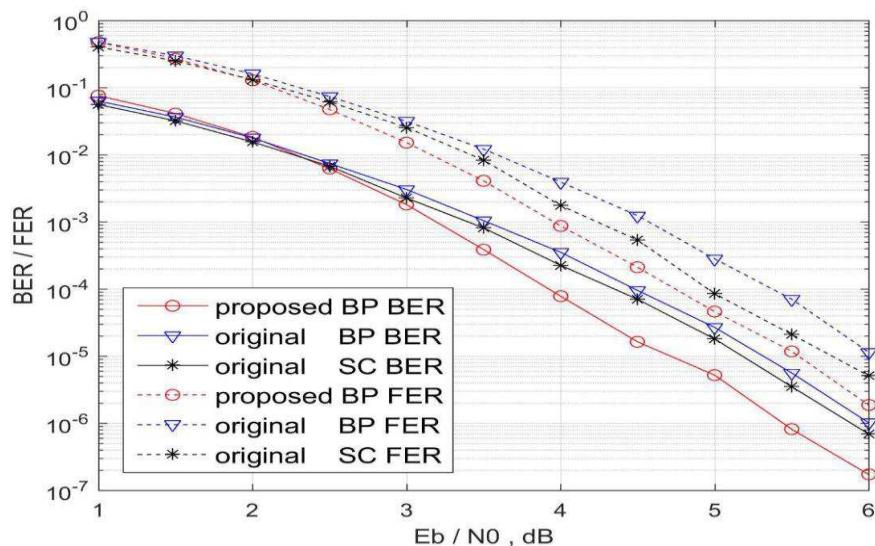
128 один информационный бит выбирается в каждой итерации, а четыре бита выбираются для кода  $N = 256$ . Для сравнения, одинаковые по скорости полярные коды, построенные с помощью эвристического метода Ариканы [1,4, также конструируются и моделируются.

На рис. 2 показано сравнение производительности различных полярных кодов с кодовой скоростью 1/2. Производительность эвристического метода при декодировании SC также указана, использованы данные работы [1, 2]. Как видно из сравнения, по сравнению с обычным кодом код, созданный с помощью предложенного алгоритма, достигает улучшения более чем на 0,3 dB в области высокого SNR, что более сопоставимо с характеристиками исходного декодирования SC.

На рис.3 показано сравнение производительности (128, K) полярных кодов с различными скоростями кодирования. Хорошо видно, что предлагаемый код превосходит обычный код, когда кодовая скорость выше 0,35 ( $K > 45$ ) [1].

### Заключение

В этой статье предлагается алгоритм выбора замороженных битов для полярных кодов, основанный на моделировании Монте-Карло и декодировании BP. С помощью предложенного алгоритма строятся полярные коды  $N = 64$  и  $N = 128$ . Результаты моделирования показали, что коды, построенные с использованием предложенного алгоритма, демонстрируют значительно лучшую производительность, чем обычные коды в диапазоне низких значений BER. Стоит отметить, что предложенный алгоритм может быть применен и для построения более длинных и практических полярных кодов.



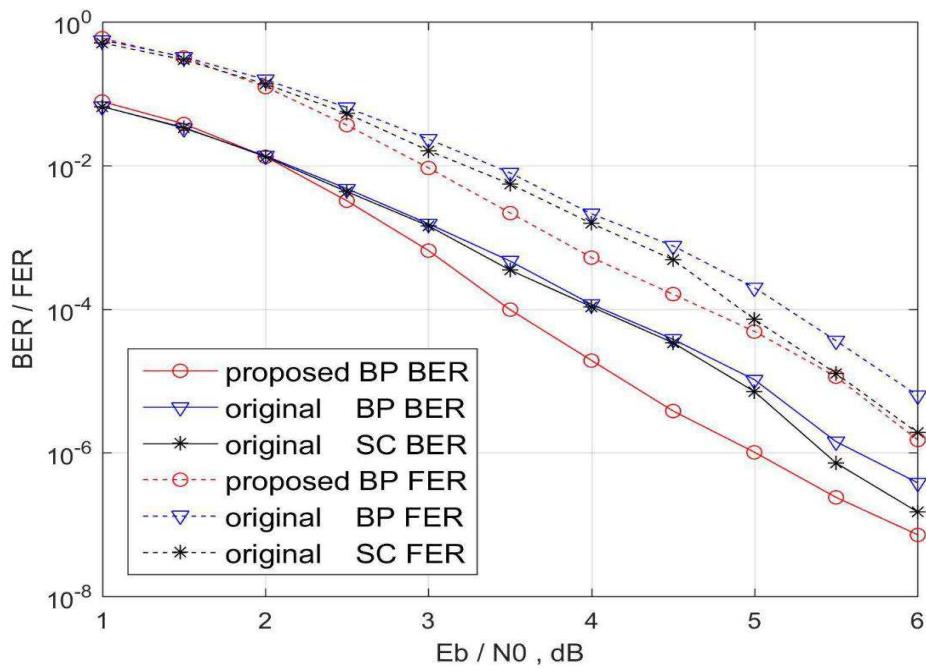


Рис.2 Сравнение производительности полярных кодов, построенных с использованием обычного и предложенного метода. (а) Характеристики BER и FER полярного кода (64,128),  
(б) Характеристики BER и FER полярного кода (128,256).

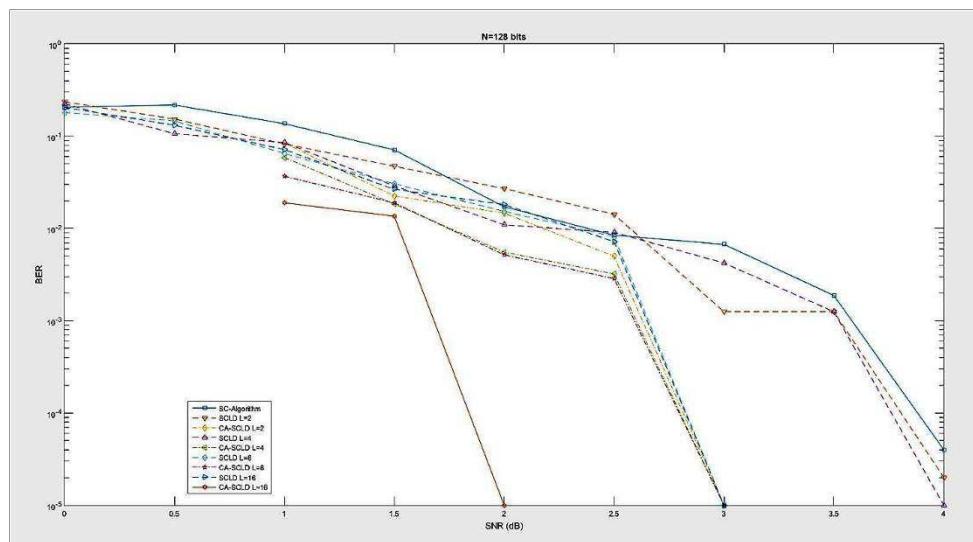


Рис.3: Сравнение производительности полярных кодов с различными скоростями кодирования ( $K / N$ ) и методами построения при  $Eb / N0 = 4,0$  дБ.

#### Список использованных источников

1. Jingbo Liu: “Frozen bits’ selection for polar codes based on simulation and BP decoding”, School of Electrical Science and Engineering
2. Abedi A., Khandani A. An analytical method for approximate performance evaluation of binary linear block codes // IEEE Transactions on Communications. — 2004. —February. — Vol. 52, no. 2. — Pp. 228–235.
3. Declercq D., Fossorier M. P. Decoding algorithms for nonbinary LDPC codes over GF( $q$ ) // IEEE Transactions on Communications. — 2007. —April. —Vol. 55, no. 4. — Pp. 633–643.

4. Erdal Arikan: “Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” IEEE Transactions on Information Theory 55 (2009) 3051 (DOI:10.1109/TIT.2009.2021379.

5. В.В. Золоторев, Д.Ж. Сатыбалдина, А.Н. Исаинова, А.Н. Амангельдиев:” Исследование характеристик полярных кодов для квантового распределения ключа” Евразийский Национальный Университет имени Л.Н. Гумилева, Нур-Султан, Казахстан. — 2017.