Оглавление

Введение

В процессе хранения или передачи информации от источника к потребителю на информацию воздействуют различные неблагоприятные факторы, например, возможны случайные помехи на линиях связи, ошибки и сбои аппаратуры, частичное разрушение носителей данных и т.д. Таким образом, в реальных системах связи существует проблема защиты информации от случайных воздействий. Для обеспечения надежной передачи информации по зашумленным каналам требуется использовать помехоустойчивое кодирование, т.е. некоторый способ внесения избыточности в передаваемые данные.

В теории помехоустойчивого кодирования было построено большое число разнообразных кодов, исправляющих ошибки. Однако характеристики большинства из них остаются весьма далекими от теоретических пределов, а вероятность ошибки декодирования, демонстрируемая ими при использовании в системах передачи информации, оказывается значительно хуже достижимой. Одной из причин этого является невозможность практического использования оптимальных алгоритмов декодирования, сложность которых оказывается чрезмерно высокой.

Существование помехоустойчивых кодов, достигающих пропускной способности канала, доказано Шенноном в 1948 году. Однако, алгоритм построения таких кодов не был описан.

В качестве решения, Е. Ариканом в 2008г. были предложены полярные коды, которые достигают пропускной способности широкого класса каналов передачи информации, что означает: для любой сколь угодно малой величины $p > 0$ существует такое целое число m, что полярный код длины $\mathrm{n} = 2^{\mathrm{m}}$ со скоростью R, меньшей пропускной способности канала, обеспечивает вероятность ошибки $< p$. Полярные коды – первая явная кодовая конструкция, достигающая пропускной способности симметричного канала. Отличительной особенностью полярных кодов является простота процедур их построения, кодирования и декодирования, что делает их привлекательными для практического использования.

Постановка задачи

Изучить теорию помехоустойчивого кодирования, и в частности [1], изучить теорию кодирования дискретных каналов с шумом, реализовать AWGN+BPSK, реализовать кодировщик, описанный Е. Ариканом, и декодер последовательного исключения.

Полярные коды

Определение

В основе конструкции полярных кодов лежит линейное преобразование, задаваемое матрицей $F^{\otimes m}$, где $\otimes m -$ m-кратное Кронекеровское произведение матрицы с собой, F – обратимая $l \times l$ матрица над $\mathbb{F}_q$, называемая ядром. В работе рассматривались только полярные коды с 2×2 ядром (матрица Арикана является наиболее известным примером ядра $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$).

Определение 1 [2] $(n = l^m, k)$ полярным кодом называется линейный блоковый код, порождаемый k строками матрицы поляризующего преобразования $G_n = B^{(l,m)}F^{\otimes m}$ с множеством кодовых слов $\{c_0^{n-1} = u_0^{n-1}G_n | u_0^{n-1} \in \{0,1\}^n, \forall i \in \mathcal{F}\ u_i = 0\}$
$B^{(l,m)}$– перестановочная матрица, такая, что для любого $i_0^{m-1} \in \{0,..,l-1\}^m$ выполняется $B_{i,i'}^{(l,m)} = 1$, где $i = \sum_{j=0}^{m-1} i_j\, l^j$ и $i' = \sum_{j=0}^{m-1} i_{m-1-j}\, l^j$
$\mathcal{F}$- множество замороженных символов, $\mathcal{F} \subset \{0,..,n-1\}$ и $|\mathcal{F}| = n - k$

Нас интересует двоичный симметричный по выходу канал без памяти - W: $\mathbb{F}_2 \to \mathcal{Y}$. На вход передаются 0 или 1 с равной вероятностью, на выход поступают символы из множества $\mathcal{Y}$. Для канала передачи данных W с переходными вероятностями W(y|0) и W(y|1), где y ∈ $\mathcal{Y}$, пропускная способность [1]

$$I(W) = \sum_{\mathrm{y} \in \mathcal{Y}} \sum_{\mathrm{x} \in \mathbb{F}_2} \frac{1}{2} W(y|x) \log \frac{W(y|x)}{\frac{1}{2}W(y|0) + \frac{1}{2}W(y|1)}$$

и параметр Бхаттачарьи [1]

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

I(W) – пропускная способность, т.е. наибольшая возможная скорость, при которой возможна надежная передача данных по каналу W (под определением скорости мы принимаем отношение числа информационных символов к общему числу передаваемых символов).

Пусть символы c_i кодового слова c_0^{n-1} передаются по каналу W независимо, мы можем рассматривать это как передачу кодового слова по n независимым копиям канала W.
Если мы объединим эти копии, то получим канал с переходной вероятностью

$$W_{G_n}(y_0^{n-1}|u_0^{n-1}) = \prod_{j=0}^{n-1} W(y_i|c_j)$$

В [1] показано как полученный канал мы можем представить в виде объединения n подканалов $W_{G_n}^{(i)}: \mathbb{F}_2 \to \mathcal{Y}^n \times {\mathbb{F}_2}^i, 0 \le i < n$, которым соответствуют переходные вероятности:

$$W_{G_n}^{(i)}(y_0^{n-1}, u_0^{i-1}|u_i) = \sum_{u_{i+1}^{n-1} \in \mathbb{F}_2^{n-i-1}} \frac{1}{2^{n-1}} W_{G_n}(y_0^{n-1}|u_0^{n-1})$$

Определение 2 [3] Классическим полярным кодом будем называть полярный код, порождаемый строками с индексами i матрицы поляризующего преобразования G_n, которым соответствуют подканалы $W_{G_n}^{(i)}$с наименьшими вероятностями ошибки P_i

Каналы передачи информации

В данной работе рассматривается следующая модель каналов передачи информации: Аддитивный гауссовский канал, для которого принятый сигнал может быть представлен как $y_i = 2 * (c_i - 0.5) + \eta$ (будем считать, что при модуляции символ 0 представляется как +1, а 1 как -1), $\eta \sim N(0, \sigma 2)$, т.е.

$$W(y_i|c_i) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y_i - 2(c_i - 0.5))^2}{2\sigma^2}}$$

Параметр Бхаттачарьи

Параметр Бхаттачарьи Z(W) является верхней границей для вероятности принятия неправильного решения относительно значения символа, полученного на выходе канала W. Границы Бхаттачарьи являются самым простым способом построения полярного кода и были первым методом, предложенным Ариканом [1]. Также в [1] показано, что для ядра Арикана параметр Бхаттачарьи подканалов $W_{G_n}^{(i)}$ удовлетворяет следующим условиям:

$$Z\left(W_{G_{2n}}^{(2i)}\right) \leq 2Z\left(W_{G_n}^{(i)}\right) - Z\left(W_{G_n}^{(i)}\right)^2$$

$$Z\left(W_{G_{2n}}^{(2i+1)}\right) \leq Z\left(W_{G_n}^{(i)}\right)^2$$

В нашем случае для AWGN канала $z_1^i = -\frac{E_b}{N_o}$

Алгоритм нахождения параметров Бхаттачарьи

```
function init_bhatt(bhatt_0){
        bhatt_z[1..2*N];
        i = 2;
        bhatt_z[0] = bhatt_0;
        для каждого b ∈ bhatt_z:
                bhatt_z[b+i] <- bhatt_z[b]^2;
                bhatt_z[b+i-1] <- 2 * bhatt_z[b] - bhatt_z[b+i];
                i++;
        return(bhatt_z[N..2*N])
}
```

На h-слое мы находим сначала $Z\left(W_{G_{2n}}^{(2i+1)}\right)$, а затем $Z\left(W_{G_{2n}}^{(2i)}\right)$.

Процедура работает за линейное время O(2*N-1)=O(N) (мы находим параметры Бхаттачарьи за один проход по массиву).

Если мы рассмотрим изначальную рекурсивную формулу, убедимся по ф-ле геометрической прогрессии, что нам необходимо минимум (2*N-1) операций.

Далее мы сортируем все каналы в порядке возрастания их Z-параметра, т.к. чем меньше Z-параметр, тем более подходящим для передачи информации является этот канал.

Кодирование полярных кодов с ядром Арикана

Полярное преобразование размера N определяется как $G_n = B^{(l,m)}F^{\otimes m}$ и является фундаментальной основой для построения кодов Арикана.

Основная идея состоит в том, чтобы построить вектор сообщений u, в котором элементы $u_i, i \in \mathcal{A} \subseteq \{1,..N\}$ содержат информацию, а другие элементы $u_j, j \in \mathcal{A}^c$ содержат значения, известные в приемнике (например, фиксированы 0). Т.е. передача информации осуществляется только по «хорошим» подканалам, для плохих каналов значение передаваемых бит фиксируется, или замораживается. Выбор замороженных бит строится для различных каналов непосредственным вычислением вероятностей ошибок (в данной работе). Затем кодовое слово $c_0^{n-1} = u_0^{n-1}G_n$ передается в канал.

Мы используем следующие свойства матрицы $F^{\otimes m}$.

1. Матрицы $F^{\otimes m}$ связаны рекурсивным соотношением: $\begin{pmatrix} F^{\otimes m} & 0_{2^m} \\ F^{\otimes m} & F^{\otimes m} \end{pmatrix}$, где 0_{2^m} – нулевая матрица $2^m \times 2^m$.
2. $F^{\otimes m}$ – нижнетреугольная матрица с единичной диагональю, всегда обратима.

Также нам будут полезны различные рекурсивные определения, например рекурсия[4] $B^{(n)} = R_n(I_2 \otimes B^{(n)})$, где $R_n = S_{2,n/2}^T$, подразумевает, что $G_n = R_n\left(I_2 \otimes B^{\left(\frac{n}{2}\right)}\right)F^{\otimes m} = R_n\left(I_{\frac{n}{2}} \otimes F\right)(I_2 \otimes F)$ Это представление естественным образом приводит к рекурсивному алгоритму кодирования, подразумеваемому в [1].

Алгоритм рекурсивной реализации полярного преобразования

```
function polar_transform(u){
        if (length(u) == 1)
                x <- u;
        else {
                u1u2 <- mod(u(1:2:end)+u(2:2:end), 2);
                u2 <- u(2:2:end);
        }

        x <- [polar_transform(u1u2), polar_transform(u2)];
        return(x);
}
```

Сложность алгоритма кодирования O (Nlog(N)).
Полярное преобразование можно представить в виде графа с N(1 + log(N)) вершин.
Процесс кодирования начинается с первого «слоя» с последовательным применением операции (U1, U2) → (U1 ⊕ U2, U2)
Далее мы модулируем передачу сообщения по AWGN каналу.

Декодирование полярных кодов

Задача декодирования входной последовательности y_0^{n-1} в двоичном полярном коде длины n = l^m и ядром l×l состоит в том, чтобы найти $\max_{u_0^{n-1}:u_{0,\mathcal{F}}^{n-1}=0} P(u_0^{n-1}|y_0^{n-1})$[3].

С помощью алгоритма последовательного исключения, предполагающего последовательное принятие решений относительно значений символов входной последовательности, мы можем найти субоптимальное решение задачи декодирования.

На i шаге алгоритма принимается решение:

$$\widehat{u_i} = \begin{cases} \arg\max_{u_i \in \{0,1\}} P(\hat{u}_0^{i-1}, u_i | y_0^{n-1}), i \notin \mathcal{F} \\ 0, i \in \mathcal{F} \end{cases}$$

Для заданного u_0^i вероятность P($u_0^i|y_0^{n-1}$) может быть рекурсивно вычислена как:

$$P\left(u_0^{ls+t}\middle|y_0^{n-1}\right) = \sum_{u_{ls+t+1}^{l(s+1)-1}} \prod_{j=0}^{l-1} \pi_j$$

Вероятность ошибки декодирования полярного кода методом последовательного исключения выражается как

$$P^{(e)} = 1 - \prod_{i \notin \mathcal{F}} (1 - P_i)$$

$P_i -$ вероятность ошибки в подканале $W_{G_n}^{(i)}$

Вероятность P_i может быть вычислена по заданному распределению логарифмических отношений правдоподобия (ЛОП) для символа u_i

$$L_{0,i} = \log \frac{P(y_0^{n-1}, \hat{u}_0^{i-1}|u_i = 0)}{P(y_0^{n-1}, \hat{u}_0^{i-1}|u_i = 1)}$$

Согласно [5], для полярных кодов с ядром Арикана, такие ЛОП могут быть рекурсивно вычислены как:

$$L_{\lambda,i} = 2\tanh^{-1}(\tanh\left(\frac{L_{\lambda+1,i}}{2}\right) * \tanh\left(\frac{L_{\lambda+1,i+\eta}}{2}\right))$$

$$L_{\lambda,i+\eta} = L_{\lambda+1,i} + (-1)^{\hat{v}_{\lambda,i}} L_{\lambda+1,i+\eta}$$

$L_{m,i} = \log \frac{P(y_i|0)}{P(y_i|1)}, 0 \le \lambda < m, \eta = 2^{m-l-1}, i \in \{2\eta h + j | 0 \le h < 2^l, 0 \le j < \eta\}$

Для AWGN $L_{m,i} = \frac{-2y_i}{\sigma^2}$

$\hat{v}_{h,j}$ – оценка j-го промежуточного символа на h-ом слое:

$$\hat{v}_{h,j} = \begin{cases} \hat{u}_j, & h = 0 \\ \hat{v}_{h-1,j} \oplus \hat{v}_{h-1,j+2^{m-h}}, & ((j \bmod 2^{m-h-1}) < 2^{m-h}) \wedge (h > 0) \\ \hat{v}_{h-1,j}, & ((j \bmod 2^{m-h-1}) \geq 2^{m-h}) \wedge (h > 0) \end{cases}$$

Алгоритм последовательного исключения принимает решение $\hat{u}_j = 1$ при $L_{0,i} < 0$ и $\hat{u}_j = 0$ при $L_{0,i} \geq 0$.

Алгоритм последовательного исключения

В каждый момент времени может быть декодирован как минимум один бит – поэтому алгоритм называют методом последовательных исключений (Successive cancellation decoding). По сути алгоритм декодирования задает обход графа полярного преобразования и распространения сообщений на этом графе.
Эффективный способ обхода этого графа представлен рекурсивной реализацией декодера:

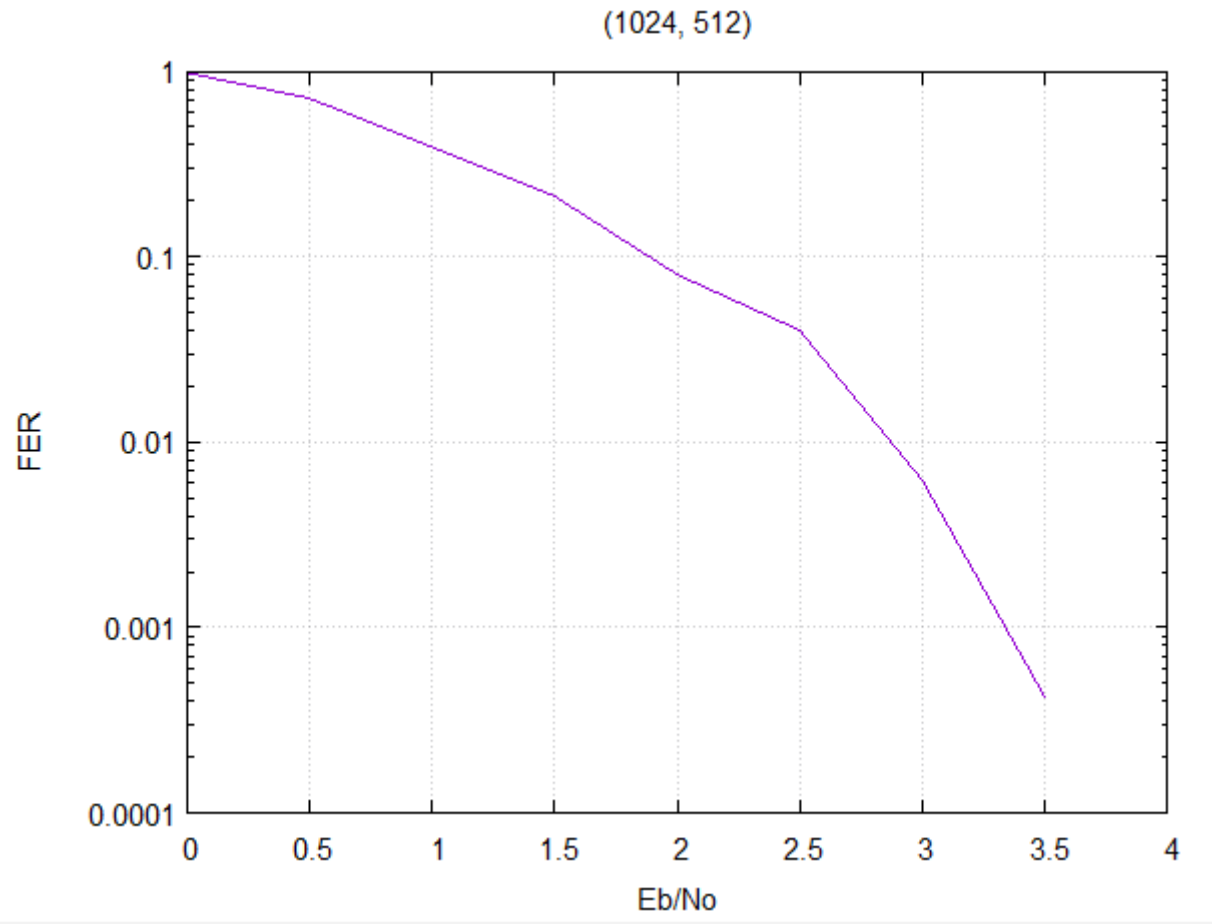
```
function cnop_llr(l_1, l_2) {
        return( 2 * atanh(tanh(l_1 / 2) * tanh(l_2 / 2)));
}
function vnop_llr(l_1, l_2, b_1) {
        return((-1) ^ b_1) * l_1 + l_2;
}
function polar_sc_recursive_llr(llr_in, f){
        N = size(llr_in, 2);
        if (i==0 && N == 1)
                return ((f == 0) * (llr_in < 0));
        else
                llr_u <-  cnop(llr_in(1:2:end), llr_in(2:2:end));
                cwd_u <- polar_sc_recursive_llr(llr_u, f(1:(N / 2)));
                llr_l <- vnop(llr_in(1:2:end), llr_in(2:2:end), cwd_u);
                cwd_l <- polar_sc_recursive_llr(llr_l, f((N / 2 + 1):end));
                return(reshape([mod(cwd_u + cwd_l, 2); cwd_l], 1, []));
}
```

Доказано, что с помощью полярного преобразования можно построить коды, достигающие пропускной способности симметричного канала. Метод последовательных исключений – простой алгоритм декодирования. Время декодирования O (N*log(N)) Параллельное выполнение невозможно, что создает проблемы для длинных кодов.

Результаты моделирования

Вероятность ошибки декодирования

Длина кодового слова
N - 1024
Кол-во информационных битов K – 512



Для Eb/No = 3.5
Кол-во переданных кодовых слов – 10^5, кол-во ошибок - 42
Выборочное среднее – 0.00042
Дисперсия – 0.00041928
Среднеквадратическое отклонение – 0.02048
Для доверительной вероятности 0.99 ty = 2.58
Точность оценки – 0.00016709
Доверительный интервал (0.00025; 0.00059)

Заключение

В результате данной работы были реализованы кодер/декодер последовательного исключения и построена модель вероятности ошибки декодирования.

Список использованной литературы

1. Arikan E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels // IEEE Transactions on Information Theory.— 2009. — July.— Vol. 55, no. 7.— Pp. 3051-3073
2. Трифонов П.В. Методы построения и декодирования многочленных кодов – 2018. – 254с.
3. Милославская В.Д. Методы построения и декодирования полярных кодов – 2014. – 206с.
4. Henry D. Pfister Notes for Introduction to Error-Correcting Codes – October 8th, 2017. – 17с.
5. Mori R., Tanaka T. Performance and construction of polar codes on symmetric binary-input memoryless channels / / Proceedings of IEEE International Symposium on Information Theory. — 2009.