УДК 621.391.7

ПРИМЕНЕНИЕ НИЗКОСКОРОСТНЫХ КОДОВ ГОППА В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

САЛОМАТИН С. Б., ПАНЬКОВА В. В.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

Аннотация. Целью данной работы является исследование низкоскоростных кодов Гоппа. Рассматриваются алгоритмы кодирования и декодирования на основе алгоритма Паттерсона. Приводятся результаты моделирования алгоритма декодирования кода с бинарной фазовой модуляцией в аддитивном гауссовском канала передачи. Исследуется функция неопределенности сигналов, построенных на основе кода Гоппа. Отмечается низкий уровень боковых лепестков функции неопределенности.

Annotation. The purpose of this paper is to study low-rate Gopp codes. We consider algorithms for encoding and decoding based on the Patterson algorithm. The results of simulation of the algorithm for decoding a code with binary phase modulation in an additive Gaussian transmission channel are presented. We study the uncertainty function of signals built on the basis of the Gopp code. It is noted that the level of side lobes of the uncertainty function is low.

Коды Гоппа

Определим полином Гоппа $g(x)$ над полем $GF(p^m)$ как полином $g(x) = g_0 + g_1 x + \cdots + g_t x^t$, где $g_i \in GF(p^m)$ [1].

Пусть L образует конечное подмножество расширенного поля $GF(p^m)$, p – простое число, $L = \{\alpha_1, \dots, \alpha_n\} \subseteq GF(p^m)$, такое, что $g(\alpha_i) \neq 0$ для всех $\alpha_i \in L$. Задавая кодовый вектор $c = (c_1, \dots, c_n)$ над $GF(q)$ мы получаем функцию

$$R_c(z) = \sum_{i=1}^{n} \frac{c_i}{x-\alpha_i}, \quad (1)$$

где $\frac{1}{x-\alpha_i}$.

Единственный полином, удовлетворяющий условию

$$(x - \alpha_i) * \frac{1}{x-\alpha_i} \equiv 1 \bmod g(x), \quad (2)$$

степень которого меньше или равна $(t-1)$.

Код Гоппа $\Gamma\big(L, g(x)\big)$ содержит все кодовые векторы с такие, что $R_c(z) \equiv 0 \bmod g(x)$. Это означает, что $g(x)$ делит $R_c(z)$.

Параметры кода Гоппа

Код Гоппа – линейный код с параметрами (n, k, d_{min}). Длина n зависит от подмножества L. Размерность k кода Гоппа $\Gamma\big(L, g(x)\big)$ над полем $GF(p^m)$ длины n больше или равна величине $n - mt$ или $k \geq n - mt$. Минимальное кодовое расстояние d_{min} кода Гоппа $\Gamma\big(L, g(x)\big)$ длины n больше или равно $(t+1)$ или $d_{min} \geq t + 1$.

Проверочная матрица бинарного кода Гоппа определяется как такая матрица **H,** для которой справедливо соотношение $\mathbf{Hc}^T = 0$ для всех векторов кодовых слов **c** в $GF(2^m)$, удовлетворяющих требованиям кода Гоппа.

Предложение. Пусть $g(x)$ – неприводимый полином над полем $GF(2^m)$ и пусть $\mathbf{H} = \mathbf{XYZ}$, где

$$\mathbf{Y} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \dots & \alpha_n^{t-1} \end{bmatrix}, \mathbf{X} = \begin{bmatrix} g_t & 0 & 0 \cdots & 0 \\ g_{t-1} & g_t & 0 \cdots & 0 \\ \vdots & \vdots & \vdots \ddots & \vdots \\ g_1 & g_2 & g_3 \cdots & g_t \end{bmatrix}, \mathbf{Z} = \begin{bmatrix} 1/g(\alpha_1) & 0 & \cdots & 0 \\ 0 & 1/g(\alpha_2) & & \cdots 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1/g(n) \end{bmatrix}, \quad (3)$$

тогда матрица **H** является проверочной матрицей кода Гоппа $\Gamma\big(L, g(x)\big)$.

Генераторная матрица **G** может быть найдена через соотношение ортогональности $\mathbf{GH}^T = 0 \bmod p$ и преобразования нуль-пространства Nullspace(H) mod 2.

Алгоритмы кодирования и декодирования

На передающей стороне кодовое слово **c** формируется путем умножения информационного вектора **m** на порождающую матрицу **G**

$$(m_1, m_2, \dots, m_k) * G = (c_1, \dots, c_n).$$

Коррекция ошибок. Пусть $\boldsymbol{y}$ будет принимаемый вектор с количеством ошибок $r \leq t$. Тогда

$$\mathbf{y} = (y_1, \dots, y_n) = (c_1, \dots, c_n) + (e_1, \dots, e_n),$$

где r – количество не равных нулю элементов $e_i \neq 0$ в векторе **y**.

Алгоритм декодирования в общем случае обнаруживает наличие ошибок, определяет их позиции $E = \{i \text{ такие, что } e_i \neq 0\}$ и величины e_i для всех $i \in E$. Для бинарных кодов достаточно решить две первые задачи – обнаружения и определение позиций ошибок.

Полином локаторов ошибок $\sigma(x)$ определяется из выражения

$$\sigma(x) = \textstyle\sum_{i \in E}(x - a_i). \quad (4)$$

Алгоритм Паттерсона [2]. Алгоритм корректирует $r \leq t$ ошибок для кода, использующего неприводимый полином $g(x)$ в поле $GF(2^m)$.

1. Пусть $\mathbf{y} = (y_1, \dots, y_n)$ – принимаемый вектор, представляющий собой аддитивную сумму кодового слова и вектора ошибок.

Синдром ошибок определяется как

$$s(x) = \textstyle\sum_{i=1}^{n} y_i/(x - a_i) \bmod g(x). \quad (5)$$

2. Вычисление полинома локаторов ошибок $\sigma(x)$:

2.1. Находим полином $h(x)$, удовлетворяющий соотношению $s(x)h(x) \equiv 1 \bmod g(x)$. Если $h(x) = x$, то принимаем $\sigma(x) = x$.

2.2. Вычисляем полином $d(x)$, удовлетворяющий соотношению $d^2(x) \equiv h(x) + x \pmod{g(x)}$.

2.3. Находим полиномы $a(x)$ и $b(x)$ решая сравнение $d(x)b(x) \equiv a(x) \bmod g(x)$, где полином $b(x)$ имеет наименьшую степень.

2.4. Определяем полином локаторов ошибок как $\sigma(x) = a^2(x) + b^2(x)x$.

3. Находим корни $\{\lambda_i\}$ полинома локаторов ошибок, решая уравнение $\sigma(x)$=0. Определяем по индексам корней $\{i \to \lambda_i\}$ позиции ошибок $E = \{i \text{ такое, что } \sigma(a_i) = 0\}$.

4. Формируем вектор ошибок $\mathbf{e} = (e_1, \dots, e_n)$, размещая единичные символы $e_i = 1$ на позициях $i \in E$ и нулевые символы $e_i = 0$ на оставшихся позициях.

5. Проводим корректировку принятого вектора $\mathbf{y}$, вычитая из него сформированный вектор ошибок $\mathbf{e}$ $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$.

6. Извлечение информационной части $\mathbf{m} = (m_1, m_2, \dots, m_k)$ из вектора $\hat{\mathbf{c}}$.

На рис.1 показан результат моделирования работы алгоритма в канале с аддитивным гауссовским шумом и бинарной модуляцией несущего колебания.

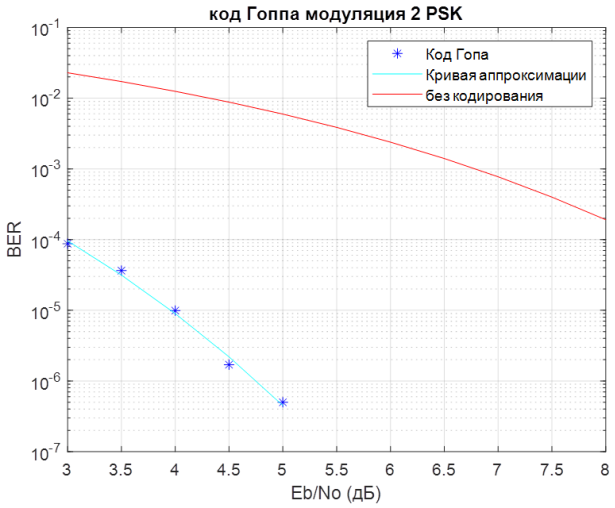
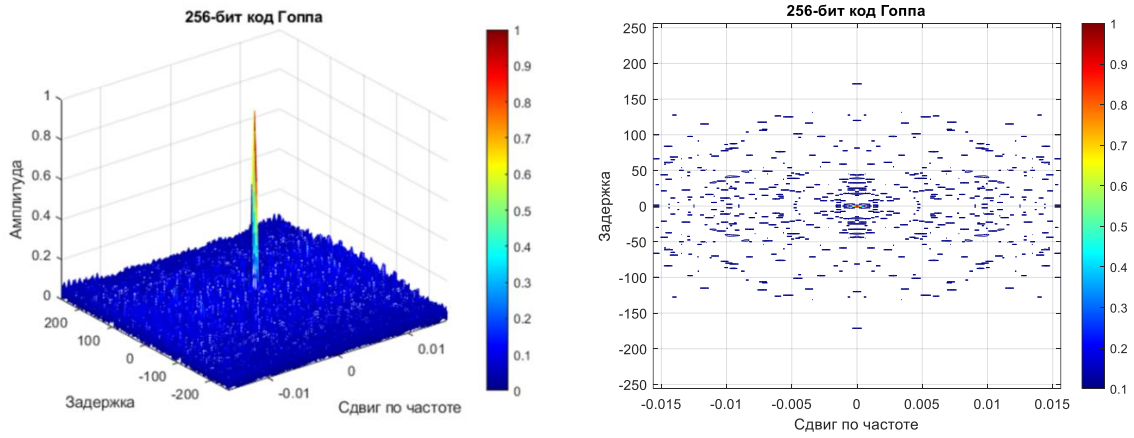


Рис. 1. Зависимость вероятности ошибки на бит (BER) от отношения сигнал шум E_b/N_0

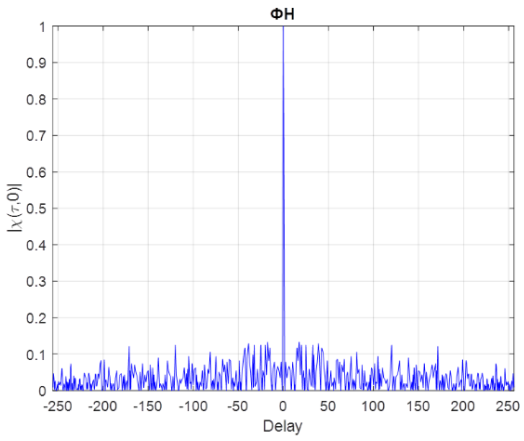
Выигрыш от кодирования кодом Гопа с параметрами n= 256, k=8 и количеством исправляемых ошибок t=31 для алгоритма декодирования Патерсона достигает 6 дБ.

В мобильных системах передачи особую роль играют корреляционные свойства сигналов в частотно-временной области.

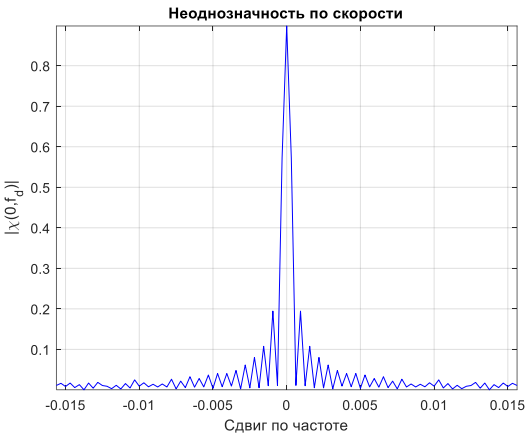
На рис 2. приведены результаты моделирования функции неопределенности последовательности, полученной с помощью низкоскоростного кода Гоппа путем замены символов $0 \to 1, 1 \to -1$.



а) б)



в)



г)

Рис. 2. Функция неопределенности последовательности кода Гоппа $(n, k) = (256,8)$: а) – функция неопределенности; б) – сечение ФН, вид сверху; в) – сечение ФН по временной оси; г) – сечение ФН по частотной оси

Результаты моделирования показывают, что уровень максимального бокового лепестка функции неопределенности не превышает $3\sqrt{n}$, где n – длина кодового слова.

Заключение

Низкоскоростные коды Гоппа позволяют построить кодовые помехоустойчивые системы с исправлением достаточно большого числа ошибок. Отличительной особенностью сигналов, построенных на основе низкоскоростных кодов Гоппа, является дельтаобразная форма функции неопределенности с низким уровнем боковых лепестков.

Такое свойство сигналов позволяет рекомендовать применение низкоскоростных кодов Гоппа для применения в системах синхронизации мобильных систем передачи информации.

Список использованных источников

1.Гоппа В. Д. Новый класс линейных корректирующих кодов // Проблемы передачи информации. 1970. Т. 6, № 3. С. 24–30.
2.Patterson Nicholas J., The algebraic decoding of Goppa codes", IEEE Transactions on Information Theory 21, 203