**ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ**

**Том 55** **2019** **Вып. 2**

УДК 621.391.15

© 2019 г. **В.А. Давыдов**

# О ПРИМЕНЕНИИ МОДУЛЬНОЙ МЕТРИКИ К РЕШЕНИЮ ЗАДАЧИ ДЕКОДИРОВАНИЯ ПО МИНИМУМУ ЕВКЛИДОВОГО РАССТОЯНИЯ

Доказывается эквивалентность использования модульной метрики и метрики Евклида для решения задачи мягкого декодирования в дискретном канале без памяти с двоичным входом и $Q$-ичным выходом. Дается пример конструкции двоичных кодов для рассмотренного канала, исправляющих $t$ двоичных ошибок в метрике Хэмминга. Построенные коды исправляют ошибки на выходе демодулятора с $Q$ уровнями квантования как $(t+1)(Q-1)-1$ ошибок в модульной метрике. Указывается, что полученные коды имеют полиномиальную сложность декодирования.

*Ключевые слова*: модульная метрика, метрика Евклида, мягкое декодирование, канал с двоичным входом и $Q$-ичным выходом, коды в модульной метрике.

**DOI:** 10.1134/S0555292319020037

## § 1. Модель симметричного канала без памяти с двоичным входным и $Q$-ичным выходным алфавитами

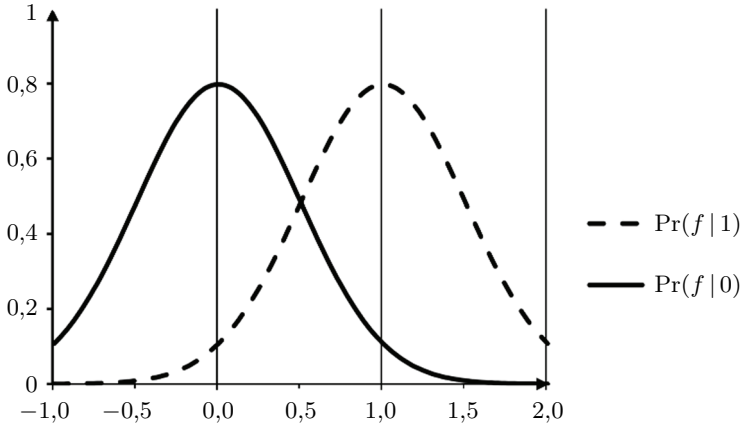
Симметричным каналом с двоичным входом и непрерывным выходом будем называть дискретный по времени канал со следующими свойствами:

- Входной алфавит $U \equiv \{0,1\}$ состоит из двух символов, обозначаемых 0 и 1. Обозначим через $U^n$ множество векторов длины $n$ с элементами из множества $U$;
- Выходной алфавит $F$ представлен как множество вещественных чисел;
- Выход $f \in F$ в заданный отсчет времени зависит только от одного входного символа;
- Для всех выходов $f$ выполняется свойство симметрии: $\Pr(f\,|\,0) = \Pr(f+1\,|\,1)$. Под $\Pr(f\,|\,x)$ понимается плотность распределения условной вероятности получения из канала символа $f$ при условии того, что по каналу передавался символ $x \in U$.

Пример функций $\Pr(f\,|\,0)$ и $\Pr(f\,|\,1)$ показан на рисунке.

Под вектором ошибки для кодового слова $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, $u_i \in U$, длины $n$ будем понимать вектор $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$, $e_i \in F$, такой же длины, соответствующие элементы которого равны разностям между вектором $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$, принятым из канала, и передаваемым словом: $e_i = f_i - u_i$, $1 \leqslant i \leqslant n$.

Декодирование по максимуму правдоподобия кода $\boldsymbol{G} \subset U^n$ означает нахождение по заданному принятому вектору $\boldsymbol{f}$ такого кодового слова $\boldsymbol{u} \in \boldsymbol{G}$, которое максимизирует вероятность того, что передавалось слово $\boldsymbol{u}$ при условии принятия вектора $\boldsymbol{f}$: $P(\boldsymbol{u}\,|\,\boldsymbol{f}) \to \max$ [1]. Канал без памяти с аддитивным белым гауссовским шумом согласован с метрикой Евклида. Декодирование по максимуму правдоподобия в этом случае заключается в поиске такого вектора $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{G}$, который находится на минимальном расстоянии Евклида от полученного вектора $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.




Пример зависимости $\Pr(f \mid 0)$ и $\Pr(f \mid 1)$ от $f$

В [2] рассматривается задача мягкого декодирования для канала с двоичным входом и $Q$-ичным выходом. В такой постановке значения компонент вектора $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$ остаются вещественными, но могут принимать ограниченное число значений, которое будем называть выходным алфавитом. Размерность выходного алфавита обусловлена числом уровней квантования выходного согласованного фильтра. Схема квантования с $Q = 8$ часто применяется в системах декодирования с мягким решением. Как отмечается в [2], характеристика такой схемы близка к характеристике, получающейся при бесконечном числе уровней квантования. Декодирование по максимуму правдоподобия для квантованного канала также заключается в поиске вектора $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{G}$, который находится на минимальном расстоянии Евклида от принятого вектора $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$.

В реальных системах связи, как отмечается в [2], используются не вещественные значения компонентов $f_i$, а числа, указывающие на тот уровень квантования $v_i \in \{0, 1, \ldots, Q-1\}$, которому соответствует значение $f_i$. В результате вектору $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$ ставится в соответствие $Q$-ичный вектор $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. Таким образом, мы получили описание дискретного канала с двоичным входом и $Q$-ичным выходным алфавитом. Данный канал полностью задается множеством переходных вероятностей $\Pr(j \mid x)$, где $\Pr(j \mid x)$ – условная вероятность того, что выходной символ равен $j$ при условии, что входной символ равен $x$. Будем считать, что канал симметричен и $\Pr(j \mid 0) = \Pr(Q - 1 - j \mid 1)$.

Если по каналу был передан двоичный вектор $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in U^n$, то вероятность того, что на выходе был получен вектор $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$, вычисляется по формуле

$$\Pr(\boldsymbol{v} \mid \boldsymbol{u}) = \prod_{i=1}^{n} \Pr(v_i \mid u_i).$$

Логарифмируя данное выражение, получим

$$\log(\Pr(\boldsymbol{v} \mid \boldsymbol{u})) = \sum_{i=1}^{n} \log(\Pr(v_i \mid u_i)). \tag{1}$$

Декодер должен максимизировать величину $\Pr(\boldsymbol{v} \mid \boldsymbol{u})$, которая будет максимальной, если отрицательная сумма в правой части (1) минимальна. В [2] вводится аппроксимирующее выражение для (1), более удобное для вычисления расстояния при

мягком решении, которое называется символьной метрикой. Соответствующие значения в такой метрике определяются по формуле $m_j = -A - B\log(\Pr(j\,|\,0))$. Константы $A$ и $B$ выбираются так, чтобы минимальное значение $m_j$ равнялось нулю, а остальные были положительны.

Наиболее часто используется схема, в которой $m_j = j$. Если число уровней равно $Q$, то метрика принимает значения из множества $\{0, 1, 2, \ldots, Q-1\}$. Как отмечается в [2], такой выбор метрики хорошо описывает многие используемые на практике декодеры.

Далее в данной статье рассматриваются только согласованные с евклидовой метрикой каналы, задаваемые переходными вероятностями. Таким образом, задача декодирования по максимуму правдоподобия решается путем нахождения ближайшего слова кода (в евклидовой метрике) к принятому слову.

## § 2. Взаимосвязь модульной и евклидовой метрики в канале с двоичным входным и $Q$-ичным выходным алфавитами

Рассмотрим канал из § 1, для которого выполняется условие $Q = 2^z + 1$. Пусть задано множество двоичных кодовых векторов $\boldsymbol{G} \subset U^n$, использующихся для передачи по каналу.

Двоичный вектор $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{G}$ с элементами из множества $\{0, 1\}$ при использовании $Q = 2^z + 1$ уровней квантования и отсутствии ошибок рассматривается демодулятором как двоичный вектор $\boldsymbol{v}^* = (v_1, v_2, \ldots, v_n) \in \boldsymbol{G}^*$ с элементами из множества $v_i \in \{0, 2^z\} \triangleq \boldsymbol{H}$. Таким образом, множество слов $\boldsymbol{G}$ из двоичного алфавита $\{0, 1\}$ будет рассматриваться демодулятором как множество двоичных слов $\boldsymbol{G}^*$ из двоичного алфавита $\{0, 2^z\}$.

В результате наложения ошибок в канале на вектор $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$ на выходе демодулятора получается $Q$-ичный вектор $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n)$ с элементами из множества $\{0, 1, 2, \ldots, 2^z\} \triangleq \boldsymbol{Z}$. Обозначим через $\boldsymbol{Z}^n$ множество векторов длины $n$ с элементами из множества $\boldsymbol{Z}$.

Задача декодирования кода $\boldsymbol{G}^*$ по максимуму правдоподобия с использованием $2^z+1$ подуровней для канала без памяти с гауссовским шумом осуществляется путем нахождения ближайшего кодового слова $\boldsymbol{v}^* = (v_1, v_2, \ldots, v_n) \in \boldsymbol{G}^*$ к полученному слову $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{Z}^n$ с использованием расстояния в метрике Евклида

$$d_E(\boldsymbol{y}^*; \boldsymbol{v}^*) = \sqrt{\sum_{i=1}^{n} (y_i - v_i)^2}. \tag{2}$$

Расстояние в модульной метрике $d_M(\boldsymbol{u}; \boldsymbol{v})$ между векторами $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \in \boldsymbol{Z}^n$ и $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \boldsymbol{Z}^n$ вычисляется по формуле

$$d_M(\boldsymbol{u}; \boldsymbol{v}) = \sum_{i=1}^{n} |u_i - v_i|. \tag{3}$$

Вес $w_M(\boldsymbol{u})$ вектора $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ в модульной метрике определяется как расстояние $d_M(\boldsymbol{u}; \boldsymbol{0})$, где $\boldsymbol{0}$ – нулевой вектор длины $n$. Если выполняется условие $d_M(\boldsymbol{u}; \boldsymbol{v}) = t$, то будем говорить, что вектор $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ получен $t$-кратными ошибками из вектора $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$.

Введем отношение частичного порядка на множестве $\boldsymbol{Z}^n$ векторов длины $n$. Положим $\boldsymbol{u} \gg \boldsymbol{v}$, если для всех $1 \leqslant i \leqslant n$ выполняется неравенство $v_i \leqslant u_i$. В том случае, если указанное неравенство выполнено не для всех $1 \leqslant i \leqslant n$, будем называть $\boldsymbol{u}$ и $\boldsymbol{v}$ несравнимыми векторами. Пусть $d_M(\boldsymbol{u}; \boldsymbol{v}) = t$ и выполняется условие

$\boldsymbol{u} \gg \boldsymbol{v}$. Тогда будем говорить, что вектор $\boldsymbol{u}$ получен из вектора $\boldsymbol{v}$ путем $t$ однонаправленных увеличивающих ошибок. Аналогично определяются однонаправленные уменьшающие ошибки.

Обозначим через $\boldsymbol{J}$ множество векторов длины $n$, компоненты которых принадлежат множеству $\{0, 1, 2, \ldots, 2^z\}$. Для мощности множества $\boldsymbol{J}$ выполняется условие $|\boldsymbol{J}| = (2^z + 1)^n$.

Пусть $\boldsymbol{u}^*$ и $\boldsymbol{v}^*$ – векторы длины $n$, компоненты которых принадлежат множеству $\{0, 2^z\} = \boldsymbol{H}$. Обозначим через $\boldsymbol{W}$ множество таких векторов. Заметим, что для мощности данного множества выполняется условие $|\boldsymbol{W}| = 2^n$ . Фактически векторы из множества $\boldsymbol{W}$ являются вершинами $n$-мерного куба, а вектор $\boldsymbol{y}^*$ – произвольной точкой такого куба. Для кода $\boldsymbol{B}^*$ и множеств $\boldsymbol{W}$ и $\boldsymbol{J}$ выполняется условие $\boldsymbol{B}^* \subset \subset \boldsymbol{W} \subset \boldsymbol{J}$.

Теорема. *Для любого вектора $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ и любой пары векторов $\boldsymbol{u}^* \in \boldsymbol{W}$ и $\boldsymbol{v}^* \in \boldsymbol{W}$ выполняется равенство*

$$d_E^2(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_E^2(\boldsymbol{y}^*; \boldsymbol{u}^*) = 2^z(d_M(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_M(\boldsymbol{y}^*; \boldsymbol{u}^*)). \tag{4}$$

Доказательство. Рассмотрим векторы $\boldsymbol{u}^* \in \boldsymbol{W}$ и $\boldsymbol{v}^* \in \boldsymbol{W}$ . Заметим, что множество позиций, в которых данные векторы совпадают, не оказывает влияния на тождество (4). Таким образом, будем рассматривать только позиции, в которых данные векторы различны. Без потери общности будем считать, что на первых $\ell$ позициях вектора $\boldsymbol{u}^*$ расположен символ $2^z$, а на следующих $m$ позициях – символ 0. Соответственно, на первых $\ell$ позициях вектора $\boldsymbol{v}^*$ расположен символ 0, а на следующих $m$ позициях – символ $2^z$. Оставшиеся $n-\ell-m$ позиций данных векторов совпадают, и в дальнейшем мы не будем их рассматривать. Тогда, исходя из (2), для левой части соотношения (4) имеет место тождество

$$\begin{aligned} d_E^2(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_E^2(\boldsymbol{y}^*; \boldsymbol{u}^*) &= \left( \sum_{i=1}^{\ell} y_i^2 + m2^{2z} - 2^{z+1} \sum_{i=\ell+1}^{\ell+m} y_i + \sum_{i=\ell+1}^{\ell+m} y_i^2 \right) - \\ &- \left( \sum_{i=1}^{\ell} y_i^2 + \ell 2^{2z} - 2^{z+1} \sum_{i=1}^{\ell} y_i + \sum_{i=\ell+1}^{\ell+m} y_i^2 \right) = \\ &= 2^z \left( \left( m2^z - 2 \sum_{i=\ell+1}^{\ell+m} y_i \right) - \left( \ell 2^z - 2 \sum_{i=1}^{\ell} y_i \right) \right). \end{aligned} \tag{5}$$

Рассмотрим теперь правую часть соотношения (4) в модульной метрике. Исходя из (3), получаем

$$\begin{aligned} d_M(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_M(\boldsymbol{y}^*; \boldsymbol{u}^*) &= \sum_{i=1}^{\ell} y_i + m2^{2z} - \sum_{i=\ell+1}^{\ell+m} y_i - \\ &- \left( -\sum_{i=1}^{\ell} y_i + \ell 2^z + \sum_{i=\ell+1}^{\ell+m} y_i \right) = \left( m2^z - 2 \sum_{i=\ell+1}^{\ell+m} y_i \right) - \left( \ell 2^z - 2 \sum_{i=1}^{\ell} y_i \right). \end{aligned} \tag{6}$$

Сравнивая (5) и (6), убеждаемся, что тождество (4) выполняется. ▲

Следствие. *Для любого вектора $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ и любой пары векторов $\boldsymbol{u}^* \in \boldsymbol{W}$ и $\boldsymbol{v}^* \in \boldsymbol{W}$ имеет место равносильность неравенств*

$$d_E(\boldsymbol{y}^*; \boldsymbol{v}^*) > d_E(\boldsymbol{y}^*; \boldsymbol{u}^*) \iff d_M(\boldsymbol{y}^*; \boldsymbol{v}^*) > d_M(\boldsymbol{y}^*; \boldsymbol{u}^*). \tag{7}$$

Доказательство. Пусть для вектора $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ и любой пары векторов $\boldsymbol{u}^* \in \boldsymbol{W}$ и $\boldsymbol{v}^* \in \boldsymbol{W}$ выполняется неравенство

$$d_E(\boldsymbol{y}^*; \boldsymbol{v}^*) > d_E(\boldsymbol{y}^*; \boldsymbol{u}^*).$$

Тогда возведение обеих частей в квадрат не меняет знак неравенства, т.е. имеет место неравенство

$$d_E^2(\boldsymbol{y}^*; \boldsymbol{v}^*) > d_E^2(\boldsymbol{y}^*; \boldsymbol{u}^*).$$

Данное утверждение следует из того, что множество $\{0, 1, 2, \ldots, 2^z\}$, которому принадлежат все компоненты векторов $\boldsymbol{u}^*$, $\boldsymbol{v}^*$ и $\boldsymbol{y}^*$, состоит из целых неотрицательных чисел.

Разделим обе части полученного неравенства на $2^z$. Получим неравенство с неизменным знаком

$$\frac{d_E^2(\boldsymbol{y}^*; \boldsymbol{v}^*)}{2^z} > \frac{d_E^2(\boldsymbol{y}^*; \boldsymbol{u}^*)}{2^z},$$

из которого следует

$$\frac{d_E^2(\boldsymbol{y}^*; \boldsymbol{v}^*)}{2^z} - \frac{d_E^2(\boldsymbol{y}^*; \boldsymbol{u}^*)}{2^z} > 0. \tag{8}$$

Из доказанного тождества (4) получаем, что неравенство (8) равносильно неравенству

$$d_M(\boldsymbol{y}^*; \boldsymbol{v}^*) - d_M(\boldsymbol{y}^*; \boldsymbol{u}^*) > 0.$$

Таким образом, требуемая эквивалентность (7) доказана. ▲

При получении вектора $\boldsymbol{y}^* = (y_1, y_2, \ldots, y_n) \in \boldsymbol{J}$ мягкое декодирование кода $\boldsymbol{B}^*$ по максимуму правдоподобия с использованием $2^z + 1$ подуровней для канала без памяти с гауссовским шумом осуществляется путем нахождения ближайшего в евклидовой метрике к полученному слову $\boldsymbol{y}^*$ слова $\boldsymbol{v}^* = (v_1, v_2, \ldots, v_n) \in \boldsymbol{W} \subset \boldsymbol{J}$, которое также должно быть кодовым словом $\boldsymbol{B}^* \in \boldsymbol{W}$.

С учетом доказанной эквивалентности (7) получаем, что использование модульной метрики возможно в процедуре мягкого декодирования вместо евклидовой метрики. При этом результат такого декодирования не изменяется.

## § 3. Коды в модульной метрике

Множество $\boldsymbol{G}(n, t) \subset \boldsymbol{Z}^n$ называется кодом, исправляющим $t$ однонаправленных увеличивающих ошибок, если для любой пары различных векторов $\boldsymbol{u} \in \boldsymbol{G}(n, t)$ и $\boldsymbol{v} \in \boldsymbol{G}(n, t)$ не существует вектора $\boldsymbol{c}$, такого что $\boldsymbol{c} \gg \boldsymbol{u}$, $\boldsymbol{c} \gg \boldsymbol{v}$, $d_M(\boldsymbol{c}; \boldsymbol{v}) \leqslant t$ и $d_M(\boldsymbol{c}; \boldsymbol{u}) \leqslant t$.

Выберем конечное поле $GF(q^m)$, где $q$ – простое число, $m$ – натуральное и выполняется неравенство $q^m > n$. Пусть $\alpha$ – примитивный элемент поля. Определим отображение $\mathcal{F}$ множества $\boldsymbol{Z}^n$ в множество полиномов от формальной переменной $x$ над полем $GF(q^m)$. Для этого поставим в соответствие $i$-й позиции $(1 \leqslant i \leqslant n)$ векторов множества $\boldsymbol{Z}^n$ ненулевой элемент $\alpha^i$ поля $GF(q^m)$. Из неравенства $q^m > n$ следует, что такое сопоставление возможно. Определим отображение $\mathcal{F}$ вектора $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ в многочлен $u(x)$ по правилу

$$\mathcal{F}(\boldsymbol{u}) \triangleq u(x) = \prod_{i=1}^{n} \Big(1 - \frac{x}{\alpha^i}\Big)^{u_i}.$$

Заметим, что для любых векторов $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{Z}^n$ выполняется условие $\mathcal{F}(\boldsymbol{u}) \equiv \mathcal{F}(\boldsymbol{v}) \equiv \equiv 1 \bmod x$.

Обозначим через $GF[x]$ кольцо многочленов от формальной переменной $x$ над полем $GF(q^m)$. Пусть $s(x) \in GF[x]$ – многочлен степени не выше $t$, младший коэффициент которого равен 1. В [3] доказывается, что множество слов

$$\boldsymbol{C} \triangleq \{\boldsymbol{u} \mid \boldsymbol{u} \in \boldsymbol{Z}^n,\ \mathcal{F}(\boldsymbol{u}) \equiv s(x) \bmod x^{t+1}\} \tag{9}$$

является кодом, исправляющим $t$ однонаправленных увеличивающих ошибок в модульной метрике. В [3] доказывается, что код $\boldsymbol{C}$, исправляющий $t$ однонаправленных увеличивающих ошибок в модульной метрике, также исправляет $t$ однонаправленных уменьшающих ошибок. В [3] доказывается, что для любого $0 \leqslant \sigma \leqslant 2t$ подмножество слов

$$\boldsymbol{B} \triangleq \left\{\boldsymbol{u} \;\middle|\; \boldsymbol{u} \in \boldsymbol{C},\ \sum_{i=1}^{n} u_i \equiv \sigma \bmod (2t+1)\right\} \subset \boldsymbol{C} \tag{10}$$

является кодом, исправляющим $t$ произвольных ошибок в модульной метрике. Помимо конструкций самих кодов, в [4] был также предложен алгоритм декодирования указанных кодов с полиномиальной сложностью, в основе которого лежит решение ключевого уравнения методом Евклида.

## § 4. Использование кодов в модульной метрике для мягкого декодирования в канале с двоичным входным и $Q$-ичным выходным алфавитами

Пусть заданы двоичные векторы $\boldsymbol{u} \in 2^n$ и $\boldsymbol{v} \in 2^n$. Обозначим через $d_H(\boldsymbol{u}; \boldsymbol{v})$ расстояние между данными векторами в метрике Хэмминга. Тогда для любых векторов $\boldsymbol{u}$ и $\boldsymbol{v}$ справедливо тождество

$$d_M(\boldsymbol{u}; \boldsymbol{v}) = d_H(\boldsymbol{u}; \boldsymbol{v}).$$

Пусть задано множество слов

$$\boldsymbol{C} \triangleq \{\boldsymbol{u} \mid \boldsymbol{u} \in 2^n,\ \mathcal{F}(\boldsymbol{u}) \equiv s(x) \bmod x^{t+1}\}.$$

Тогда подмножество слов

$$\boldsymbol{B} \triangleq \left\{\boldsymbol{u} \;\middle|\; \boldsymbol{u} \in \boldsymbol{C},\ \sum_{i=1}^{n} u_i \equiv \sigma \bmod 2(t+1)\right\} \subset \boldsymbol{C}$$

является двоичным кодом, исправляющим $t$ ошибок в метрике Хэмминга и в модульной метрике.

Будем строить для $\boldsymbol{B}$ схему мягкого декодирования. Выпишем в явном виде условие для кода $\boldsymbol{C}$:

$$\mathcal{F}(\boldsymbol{u}) \triangleq u(x) = \prod_{i=1}^{n}\Big(1 - \frac{x}{\alpha^i}\Big)^{u_i} = s(x) + f(x)x^{t+1}. \tag{11}$$

Будем считать, что $n < 2^m$ и $\alpha^i \in GF(2^m)$ при $1 \leqslant i \leqslant n$. Предположим, что декодер кода имеет $Q = 2^z + 1$ подуровней. Другими словами, на выходе демодулятором по каждому символу кода принимается решение, принадлежащее множеству $\{0, 1, 2, \ldots, 2^z\}$.

Возведем левую и правую части уравнения (11) в степень $2^z$. Поскольку действия производятся в поле характеристики 2, получим

$$u^*(x) = \left( \prod_{i=1}^{n} \Big(1 - \frac{x}{\alpha_i}\Big)^{u_i} \right)^{2^z} = s(x)^{2^z} + f(x)^{2^z} x^{(t+1)2^z}.$$

Это означает, что двоичный вектор $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{C}$ с элементами из множества $\{0, 1\}$ преобразовался в двоичный вектор $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$ с элементами из множества $\{0, 2^z\} = \boldsymbol{H}$.

Заметим, что степень полинома $s(x)^{2^z}$ удовлетворяет неравенству $\deg(s(x)^{2^z}) \leqslant \leqslant 2^z t$. Таким образом, $s(x)^{2^z}$ – многочлен степени не выше $2^z t$, младший коэффициент которого равен 1.

Заметим, что $2^z(t+1) = 1 + (2^z t + 2^z - 1)$. Следовательно, из (9) получаем, что

$$\boldsymbol{C}^* \triangleq \left\{ \boldsymbol{u}^* \mid \boldsymbol{u}^* \in \boldsymbol{H}^n,\ \mathcal{F}(\boldsymbol{u}^*) \equiv s(x)^{2^z} \bmod x^{2^z(t+1)} \right\}$$

является кодом, исправляющим $2^z t + 2^z - 1$ однонаправленных увеличивающих ошибок в модульной метрике, если за единичную ошибку считать изменение на один уровень из множества уровней $\{0, 1, 2, \ldots, 2^z\}$ в одном из $n$ символов вектора $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$.

Если для вектора $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \boldsymbol{C}$ выполняется условие

$$\sum_{i=1}^{n} u_i \equiv \sigma \bmod (2t+1),$$

то для вектора $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*) \in \boldsymbol{C}^*$ с элементами из множества $\{0, 2^z\} = \boldsymbol{H}$ выполняется условие

$$\sum_{i=1}^{n} 2^z u_i \equiv \sigma 2^z \bmod (2^z(2t+1)).$$

Тогда из равенства $2^z(t+1) = 1 + (2^z t + 2^z - 1)$ с учетом (10) получаем, что код

$$\boldsymbol{B}^* \triangleq \left\{ \boldsymbol{u}^* \;\middle|\; \boldsymbol{u}^* \in \boldsymbol{C}^*,\ \sum_{i=0}^{n} u_i^* \equiv \sigma 2^z \bmod (2^z(2t+1)) \right\} \subset \boldsymbol{C}^*$$

является кодом, исправляющим $2^z t + 2^z - 1$ произвольных ошибок в модульной метрике, если за единичную ошибку считать изменение на один уровень из множества уровней $\{0, 1, 2, \ldots, 2^z\}$ в одном из $n$ символом вектора $\boldsymbol{u}^* = (u_1^*, u_2^*, \ldots, u_n^*)$.

Алгебраическая структура полученного кода $\boldsymbol{B}^*$ может быть использована с применением алгоритма из [4] для нахождения с полиномиальной сложностью части ошибок, исправляемых кодом $\boldsymbol{B}^*$ в модульной метрике до его конструктивного расстояния $1 + (2^z t + 2^z - 1)$. При нахождении всех остальных ошибок, исправляемых кодом $\boldsymbol{B}^*$ в модульной метрике, получаем мягкое декодирование кода $\boldsymbol{B}^*$ по максимуму правдоподобия для канала с двоичным входным алфавитом и выходным алфавитом из $Q = 2^z + 1$ символов.

## СПИСОК ЛИТЕРАТУРЫ


1. *Колесник В.Д., Мирончиков Е.Т.* Декодирование циклических кодов. М.: Связь, 1968.
2. *Кларк Дж., мл., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи. М.: Радио и Связь, 1987.

3. *Давыдов В.А.* Коды, исправляющие ошибки в модульной метрике, метрике Ли и ошибки оператора // Пробл. передачи информ. 1993. Т. 29. № 3. С. 10–20.
4. *Давыдов В.А.* Методы исправления ошибок в модульной и порожденных ею метриках: Дис. канд. техн. наук: 05.13.01. Санкт-Петербург, 1993.

*Давыдов Вячеслав Анатольевич*
Московский институт электроники и математики
им. А.Н. Тихонова,
Национальный исследовательский университет
"Высшая школа экономики"
novdav2017@yandex.ru

Поступила в редакцию
09.05.2018
После доработки
23.03.2019
Принята к публикации
16.04.2019