

У ДК 681.32

МЕТОД ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ ПОМЕХОУСТОЙЧИВЫМИ КОДАМИ

Сорокин С.С., Болотная Ю.В.

Севастопольский национальный технический университет

Студгородок г. Севастополь, Украина, 99053

E-mail: root@sevgtu.sebastopol.ua

Предлагается новая конструкция помехоустойчивых кодов – структурированный код, использующий структурную избыточность. Описываются алгоритмы кодирования и декодирования. Приводятся оценки вероятности ошибки декодирования и оценки трудоемкости декодирования, а также результаты сравнения с трудоемкостью декодирования БЧХ-кодов.

1. Введение. За время существования теории и практики применения помехоустойчивого кодирования было разработано большое число кодов, обнаруживающих и исправляющих различные типы ошибок: коды Хемминга, код Голея, коды Боуза-Чоудхури-Хоквингема (БЧХ), обобщенные коды Рида-Малера, коды Рида-Соломона, сверточные и каскадные коды. Наиболее эффективными из них являются коды БЧХ, сверточные и каскадные [1].

Следует заметить, что указанные коды эффективны при вероятности искажения двоичного символа $q_0 < 0,002$, которой обладают известные каналы (кабельный, радиорелейный, тропосферный) [1]. Для систем специального назначения, работающих в условиях повышенного уровня пассивных и активных помех, вероятность искажения двоичного символа может достигать значения $q \approx 0,1$, кроме этого могут появляться и пачки ошибок сравнительно большой длины. Независимо от этого, разработчикам таких систем ставятся жесткие требования по обеспечению высокой достоверности принимаемой информации, например, эквивалентная вероятность ошибки приема одного информационного символа q_0 не должна превышать величины 10^{-5} при минимальной избыточности кода. Традиционно подобные задачи решаются с помощью длинных кодов (БЧХ, Рида-Соломона, каскадных). Так, например, БЧХ-код (255,37) позволяет исправлять ошибки кратности до $t=45$ и достигнуть $q_0 < 10^{-5}$ при $q = 0,1$. Примерно такой же результат может быть получен в случае применения структурированного кода (23,12):5×3. Для повышения эффективности этих кодов при исправлении пачек ошибок, возникающих в активных помехах, можно применять следующие приемы:

а) «перемешивать» версии кодовых слов» внутри длинных пакетов, т.е. разнести в определенном порядке отдельные версии структурированного кода на расстояния большие, чем максимальная длина пачки ошибок;

б) передавать отдельные части структурированного кода на разных частотах или по различным физическим каналам.

Основными достоинствами предлагаемых кодов являются:

- малая трудоемкость алгоритма декодирования, например, по сравнению с БЧХ-кодами;
- небольшой объем памяти, необходимой для декодирования (для кода Голя – 4 Кбайта);
- широкая возможность варьирования величинами параметров кода для получения оптимального решения.

2. Описание конструкции структурированного кода. Пусть (n, k, t) – двоичный линейный код, состоящий из n символов, k из которых являются информационными, а $r = n - k$ – контрольными. Код может исправлять до t ошибок.

Код задан с помощью левой канонической формы G' порождающей матрицы G и диагностической матрицы D :

$$G' = \begin{pmatrix} a_1 & a_2 & \dots & a_k & p_1 & p_2 & \dots & p_r \\ 1 & 0 & \dots & 0 & p_{11} & p_{12} & \dots & p_{1r} \\ 0 & 1 & \dots & 0 & p_{21} & p_{22} & \dots & p_{2r} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & p_{k1} & p_{k2} & \dots & p_{kr} \end{pmatrix} = \|IP\|, \quad (1)$$

где I – единичная матрица, т.е. матрица, у которой на главной диагонали стоят единицы, а вне диагонали – нули; P – матрица контрольных символов.

В памяти ЭВМ матрицу (1) удобно представлять только ее подматрицей P , сохраняя порядок строк, заданный матрицей G' ,

$$P = \|p_{ij}\|_{k \times r}, \quad p_{ij} \in \{0, 1\}. \quad (2)$$

Матрица (2) используется для вычисления b – контрольной части кодового слова (a, b) по следующей формуле:

$$b_j = \sum_{i=1}^k p_{ij} a_i, \quad j = 1, 2, \dots, r. \quad (3)$$

Диагностическая матрица $D = \|D^a D^b\|$ представлена двумя подматрицами $D^a = \|d_{i,i}^a\|_{2^r \times k}$ и $D^b = \|d_{i,j}^b\|_{2^r \times r}$ и предназначена для определения корректоров ошибок d_i^a и d_i^b информационной и контрольной частей вариантов базовых слов, соответственно. Обозначим структурированный код следующей записью: $(n, k, t): h_a \times h_b$, где h_a и h_b – количество версий информационной и контрольной частей базового кодового слова $c = (a, b)$ соответственно.

Код строится на основе исходного – базового кода (n, k, t) . Пусть,

например, $(n,k,t) = (23,12,3)$ – код Голя и $h_a = 3$, $h_b = 5$, тогда структурированный код $(23,12,3):3 \times 5$ условно можно представить структурной схемой, изображенной на рисунке 1.

Вычисление контрольной части b базового кодового слова (a,b) производится по формуле (3). Затем всем h_b версиям контрольной части структурированного кода, присваивается значение b . Всем h_a версиям информационной части структурированного кода присваивается значение информационной части a базового кодового слова (a,b) .

Кодовое слово

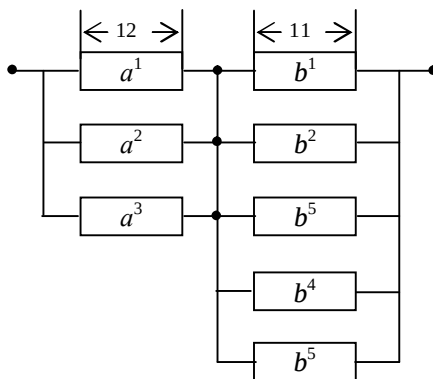


Рисунок 1 - Структурная схема структурированного кода $(23,12,3) : 3 \times 5$

структурированного кода обозначим как $S = (a^1, a^2, \dots, a^{h_a}, b^1, b^2, \dots, b^{h_b})$.

После передачи структурированного кодового слова S по каналу на приемной стороне может быть принято кодовое слово $\mathcal{E} = (\mathcal{E}^1, \mathcal{E}^2, \dots, \mathcal{E}^{h_a}, \mathcal{E}^1, \mathcal{E}^2, \dots, \mathcal{E}^{h_b})$, каждая часть которого может содержать как независимые ошибки, так и пакки ошибок.

Рассмотрим основные этапы алгоритма обнаружения и исправления ошибок, т.е. алгоритма декодирования принятого слова для вычисления скорректированной информационной части a^* .

3. Описание алгоритма декодирования

1⁰. Из h_a и h_b версий информационных и контрольных частей принятого кодового слова сформировать множество вариантов базовых кодовых слов

$$\mathcal{C} = \{(\mathcal{C}_u, \mathcal{C}_v)\} = \{(\mathcal{C}_{uv}, \mathcal{C}_{uv})\}, \quad u = 1, \dots, h_a, \quad v = 1, \dots, h_b, \quad uv = 1, \dots, h_{ab}, \quad h_{ab} = h_a \times h_b.$$

2⁰. Определить $\mathcal{C}^0$ опорное множество вариантов скорректированных базовых кодовых слов $\mathcal{C}^0 = \{c_{uv}^0\} = \{(a_{uv}^0, b_{uv}^0)\}, \quad uv = 1, \dots, h_{ab}.$

Определение c_{uv}^0 состоит из последовательности вычислений следующих двоичных векторов

$$1) \text{ синдрома } s_{uv} = \text{cod}(\mathcal{C}_{uv}) \oplus \mathcal{C}_{uv};$$

$$2) \text{ корректора } (d_{uv}^a, d_{uv}^b) = D[s_{uv}];$$

3) скорректированного варианта базового кодового слова

$$c_{uv}^0 = (\mathcal{E}_{uv} \oplus d_{uv}^a, \mathcal{E}_{uv} \oplus d_{uv}^b) = (a_{uv}^0, b_{uv}^0).$$

3⁰. Определить c_0^0 дополнительный вариант скорректированного базового кодового слова и включить его в опорное множество C^0 , получив таким образом расширенное множество скорректированных базовых кодовых слов C^e .

Определение c_0^0 состоит из последовательности вычислений следующих векторов:

1) векторов весов символов $W^a = \{w_i^a\}$, $W^b = \{w_j^b\}$ принятого структурированного кодового слова $\mathcal{E}$

$$w_i^a = \sum_{u=1}^{h_a} \mathcal{E}_u \wedge x_i, i = 1, \dots, k, w_i^a \in \{0, 1, \dots, h_a\},$$

$$w_j^b = \sum_{v=1}^{h_b} \mathcal{E}_v \wedge x_j, j = 1, \dots, r, w_j^b \in \{0, 1, \dots, h_b\},$$

где x_i, x_j – двоичные векторы, содержащие единицу в i -ом или j -ом разряде, соответственно и в остальных разрядах – нули; $\wedge$ – операция поразрядного логического умножения двоичных векторов.

2) мажорированного кодового слова $c^m = (a^m, b^m)$ с помощью операции мажорирования компонентов векторов W^a и W^b

$$a_i^m = \begin{cases} 1, & \text{если } w_i^a > \lfloor h_a / 2 \rfloor, \\ 0, & \text{в противном случае,} \end{cases}$$

$$i = 1, \dots, k;$$

$$b_j^m = \begin{cases} 1, & \text{если } w_j^b > \lfloor h_b / 2 \rfloor, \\ 0, & \text{в противном случае,} \end{cases}$$

$$j = 1, \dots, r;$$

3) синдрома $s_0 = \text{cod}(a^m) \oplus b^m$;

4) корректора $(d_0^a, d_0^b) = D[s_0]$;

5) скорректированного варианта мажорированного кодового слова

$$c_0^0 = (a^m \oplus d_0^a, b^m \oplus d_0^b) = (a_0^0, b_0^0);$$

6) включить в множество C^0 вектор c_0^0

$$C^e := C^0 \cup c_0^0, C^e = \{c_{uv}^e\} = \{(a_{uv}^e, b_{uv}^e)\}, uv = 0, 1, \dots, h_{ab}.$$

4⁰. Определить скорректированную информационную часть a^* принятого слова $\mathcal{S}$. Определение a^* состоит из последовательности вычислений следующих векторов:

1) вектора весов символов $W^{ae} = \{w_i^{ae}\}$, $W^{be} = \{w_j^{be}\}$ множества слов C^e

$$w_i^{ae} = \sum_{uv=0}^{h_{ab}} a_{uv}^e \wedge x_i, \quad i=1, \dots, k, \quad w_i^{ae} \in \{0, 1, \dots, h_{ab}\},$$

$$w_j^{be} = \sum_{v=0}^{h_{ab}} b_{uv}^e \wedge x_j, \quad j=1, \dots, k, \quad w_j^{be} \in \{0, 1, \dots, h_{ab}\},$$

где x_i, x_j и $\wedge$ определены в п.3⁰ данного алгоритма;

2) мажорированного кодового слова $c^{me} = (a^{me}, b^{me})$ с помощью операции мажорирования компонентов векторов W^{ae} и W^{be}

$$a_i^{me} = \begin{cases} 1, & \text{если } w_i^{ae} > \lfloor h_{ab} / 2 \rfloor, \\ 0, & \text{в противном случае,} \end{cases}$$

$$i=1, \dots, k;$$

$$b_j^{me} = \begin{cases} 1, & \text{если } w_j^{be} > \lfloor h_{ab} / 2 \rfloor, \\ 0, & \text{в противном случае,} \end{cases}$$

$$j=1, \dots, r;$$

3) синдрома $s = \text{cod}(a^{me}) \oplus b^{me}$;

4) корректора $(d^a, d^b) = D(s)$;

5) скорректированной информационной части a^* принятого слова $\mathcal{S}$
 $a^* = a^{me} \oplus d^a$.

4. Оценка трудоемкости алгоритма декодирования и результаты испытаний структурированных кодов

Этап 1. Формирование множества $\mathcal{C}$.

На составление h_{ab} вариантов базовых кодовых слов требуется $T_1 = h_{ab} \cdot t_0$ элементарных операций, где $t_0 = 3$ (приращение счетчиков циклов u, v и uv) + 3(вычисление адресов) + 1(операция пересылки) = 7.

Этап 2. Определение элементов множества C^0

$$T_2 = h_{ab}(t_0 + t_1 + t_2 + t_3),$$

где t_0 – как в этапе 1; $t_1 = 2k + 1$ – логические r -разрядные операции вычисления s_{uv} ; $t_2 = 2$ – операции выбора двух частей корректора; $t_3 = 2$ – логические операции поразрядного сложения по модулю два.

Итого, для выполнения этапа 2 требуется $T_2 = 2h_{ab}(K + 6)$ операций.

Этап 3. Определение дополнительного варианта скорректированного базового кодового слова

$$T_3 = t_1 + t_2 + t_3 + t_4 + t_5 + t_6,$$

где $t_1 = 2(kh_a + rh_b)$, $t_2 = 2(k + r)$, $t_3 = 2k + 1$, $t_4 = 2$, $t_5 = 2$, $t_6 = 2$.

Итого $T_3 = 2(kh_a + rh_b + 2k + r) + 7 < 2[k(2 + h_a) + r(1 + h_b) + 4]$.

Этап 4. Определение a^*

$$T_4 = t_1 + t_2 + t_3 + t_4 + t_5$$

где $t_1 = 2h_{ab}(k + r)$, $t_2 = 2(k + r)$, $t_3 = 2k + 1$, $t_4 = 2$, $t_5 = 2$.

Итого $T_4 = 2(h_{ab}(k + r) + 2k + r + 5) < 2[k(2 + h_{abb}) + r(1 + h_{ab}) + 3]$.

Трудоемкость алгоритма декодирования структурированного кода составляет

$$T_C = T_1 + T_2 + T_3 + T_4 = (2h_{ab} + 8)k + 4r + 11h_{ab} + 2(h_a + h_b + 11) \quad (4)$$

однотактных операций ЭВМ.

При использовании специального устройства декодирования можно:

1) распараллелить процедуры вычисления множеств $\mathcal{C}, C^0, W^a, W^b, W^{ae}, W^{be}$, добавив $(h_a + h_b)$ k -разрядных регистров и $(h_a + h_{ab})$ r -разрядных регистров, тогда в формуле (4) значения h_a, h_b, h_{ab} необходимо заменить на 1;

2) операции мажорирования реализовать соответствующими мажоритарными элементами;

3) операцию кодирования $cod(a)$ реализовать соответствующими шифраторами.

В этих условиях T_C существенно уменьшится и не будет зависеть от длины кодового слова.

В данной работе основное внимание уделено реализации кодирования и декодирования на ЭВМ, поэтому здесь не приводится оценка трудоемкости кода, построенного на базе специализированного устройства. Трудоемкость алгоритма декодирования БЧХ-кода согласно [1] при использовании t арифметических устройств составляет

$$T_{БЧХ}^t = n(1 + \log_2 n), \quad (5)$$

при использовании одной ЭВМ число элементарных операций может оцениваться величиной

$$T_{БЧХ}^1 = n^2 \log_2 n. \quad (6)$$

Вычислим для сравнения значения $T_C, T_{БЧХ}^t, T_{БЧХ}^1$ при условии, что ошибки декодирования Q_C и $Q_{БЧХ}$ одного порядка, и относительная избыточность сравниваемых кодов примерно одинакова

Пусть структурированный код построен на базе кода Рида-Маллера (24,12,3), синтезированного с помощью программы, описанной в работе [2]. Данный код имеет минимальное расстояние $d_{\min}=8$ и может исправлять до трех ошибок и обнаруживать четырехкратные ошибки. Возможность обнаруживать четырехкратные ошибки, позволяет существенно повысить корректирующую способность структурированного кода

Используемый в качестве примера структурированный код имеет следующие параметры: $k=12, r=12, t=3, h_a=5, h_b=3$. Вероятность искажения одного символа при передаче $q=0,1$.

После проведения серии статистических испытаний по методике, предложенной в работе [3], значения $Q_c=1,8 \cdot 10^{-5}$ при относительной избыточности кода $R_c = \frac{k(h_k - 1) + rh_b}{k} = 7$.

Аналитическая оценка $Q_{БЧХ}$ наиболее близкого по избыточности БЧХ-кода (255,29) $t=47$ составляет

$$Q_{БЧХ} = \sum_{i=t+1}^n c_n^i q^i (1-q)^{n-1} = 1,45 \cdot 10^{-5}.$$

Относительная избыточность этого кода равна

$$R_{БЧХ} = \frac{n-k}{k} = \frac{259-29}{29} = 7,79.$$

После подстановки значений соответствующих параметров в формулы (4)-(6) получим

$$T_c = 607, T_{БЧХ}^t = 2795, T_{БЧХ}^1 = 585225.$$

Отметим, что результаты сравнения приведенных значений трудоемкостей явно не в пользу кодов БЧХ.

Результаты испытаний некоторых вариантов структурированных кодов, построенных на базе вышеупомянутого кода Рида-Маллера (24,12) и оценки близких к ним БЧХ-кодов, приведены в таблице 1.

Таблица 1 – Сравнительные характеристики кодов

БЧХ-коды				Структурированные коды			
Код	t	R	Q	h_a	h_b	R	Q
(255,45)	43	4,77	$2,5 \cdot 10^{-4}$	3	3	5	$2,4 \cdot 10^{-4}$
(255,29)	47	7,79	$1,4 \cdot 10^{-5}$	5	3	7	$1,8 \cdot 10^{-5}$
(255,21)	55	11,11	$1,5 \cdot 10^{-8}$	5	5	9	$1,3 \cdot 10^{-7}$

5. Заключение. Таким образом, предлагается новая конструкция помехоустойчивых кодов – структурированный код, который строится на базе «коротких» блочных кодов, использующих синдромное декодирование. Кодовое слово такого кода может состоять из необходимогонечетного числа версий информационной части h_a и другого или такого же нечетного числа версий контрольной части h_b . По принятому слову составляются $h_{ab} = h_a \times h_b$ вариантов базовых кодовых слов. Для декодирования и исправления ошибок используется мажорированное базовое кодовое слово, значение разрядов которого (0,1) определяется по большинству значений соответствующих разрядов h_{ab} – вариантов базовых кодовых слов.

Сравнение структурированных кодов с БЧХ-кодами, имеющими почти одинаковую избыточность с предлагаемыми, показывает, что структурированные коды обладают следующими преимуществами:

- менее трудоемким алгоритмом декодирования ошибок при одинаковой вероятности ошибки декодирования
- требует меньшего объема памяти для представления диагностической матрицы коротких базовых кодов;
- обладают возможностью варьирования значениями h_a и h_b для получения структурированных кодов, удовлетворяющих требованиям достоверности декодирования структурированные коды являются высокоэффективным средством повышения достоверности передачи информации.

Библиографический список

1. Питерсон У. Коды, исправляющие ошибки: Пер. с англ. / У. Питерсон, Э. Уэлдон. — М.: Мир, 1976. — 594 с.
2. Сорокин С.С. Метод синтеза оптимальных линейных кодов, исправляющих и обнаруживающих ошибки / С.С. Сорокин, В.И. Мирянов // Вестн. СевГТУ: Сб. науч. тр. — Севастополь, 2000. — Вып. 26. — С. 70–78.
3. Болотная Ю.В. Оценка вероятности ошибки декодирования кодов / Ю.В. Болотная, С.С. Сорокин // Системы автоматики и автоматическое управление: Материалы студенч. науч.-техн. конф., г. Севастополь, 17-18 мая 2001 г. — Севастополь, 2001. — С. 100.

Поступила в редакцию 8.11.2001 г.