УДК 004.052.4

Д. М. Романенко, ассистент

ИСПОЛЬЗОВАНИЕ ТРЕХМЕРНЫХ ИТЕРАТИВНЫХ КОДОВ В КАНАЛАХ ПЕРЕДАЧИ ДАННЫХ

The article are considered some aspects of realizing a new type of the codes – three-dimensional iterative codes, that will allow to reach the large scale reliability level in the data link.

Проблема повышения надежности передачи информации обусловлена несоответствием между требованиями, предъявляемыми при передаче данных, и качеством реальных каналов связи. В сетях передачи данных требуется обеспечить вероятность возникновения ошибки меньше 10^{-6}–10^{-9}, а при использовании реальных каналов связи указанная величина приблизительно равна 10^{-2}–10^{-5} [1]. Решением проблемы является использование методов и средств помехоустойчивого кодирования.

Важнейший параметр каналов связи – отношение сигнал / шум (E_b / N_0) (E_b – энергия бита, которую можно считать, как мощность сигнала, умноженную на время передачи бита; N_0 – спектральная плотность мощности шума, которую можно определить как отношение мощности шума к ширине полосы). Отношение же энергии кодового символа к спектральной плотности мощности шума (E_c / N_0) равно [1]

$$E_c / N_0 = \left(\frac{k}{n}\right) \cdot \frac{E_b}{N_0}, \qquad (1)$$

где k и n – длина информационной и кодовой последовательности.

Вероятность одиночной ошибки (p_1) в каналах, использующих ортогональную модуляцию (некогерентное обнаружение), будет определяться следующим соотношением [1]:

$$p_1 = \frac{1}{2} \cdot e^{-\frac{1}{2}\frac{E_c}{N_0}}. \qquad (2)$$

Вероятность появления ошибочного бита в результате декодирования рассчитывается по следующей зависимости [1]:

$$P_b = \frac{1}{n} \cdot C_{t+1}^{n} \cdot p_1^{t+1} \cdot (1 - p_1)^{n-t-1}, \qquad (3)$$

где t – кратность корректируемых ошибок.

Проанализируем возможность применения трехмерных итеративных кодов для защиты информации в подобных системах. Наибольший практический интерес представляет трехмерный линейный итеративный код (ТЛИК). Кодовые слова при использовании ТЛИК можно записывать в виде таблицы. Основной является форма записи кодовых слов, при которой все кодовые слова содержат четное число единиц. Например, при кодировании информационного слова X_k = = **01110111111011001100110111**0 получим следующие избыточные символы X_r = = *0100110000110100010110011111101101011*, как показано на рис. 1 (информационные символы выделены жирным шрифтом, а проверочные – курсивом).

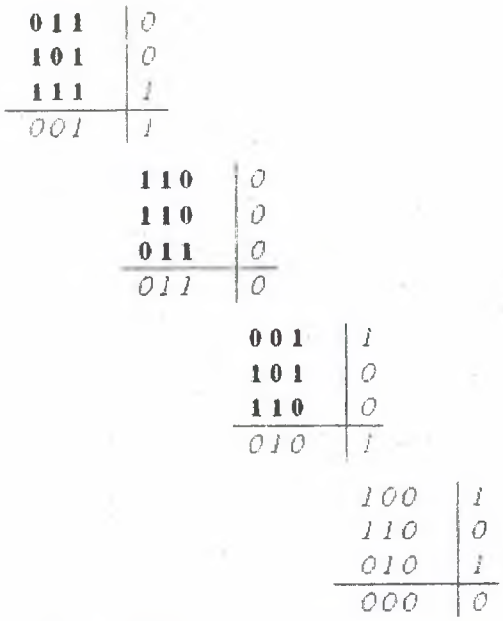

Рис. 1. Схематичное представление трехмерного линейного итеративного кода

В общем случае линейный трехмерный итеративный код (по основанию два) определим как блоковый (n_1, k_1, n_2, k_2, n_3, k_3)-код, формирующий кодовые последовательности длиной k ($k = k_1 \cdot k_2 \cdot k_3$) информационных и $(k_1 + k_2 + 1) \times (k_3 + 1) + k_1 \cdot k_2$ проверочных разрядов (в приведенном примере $k_1 = k_2 = k_3 = 3$). Для определенного набора k двоичных информационных символов кодовое слово можно представить в виде $k_1 \cdot k_3$ n_2-разрядных кодовых слов строк, $k_2 \cdot k_3$ n_1-разрядных кодовых слов столбцов; и $k_1 \cdot k_2$ n_3-разрядных кодовых z-слов ($n_1 = k_1 + 1$, $n_2 = k_2 + 1$, $n_3 = k_3 + 1$).

Рассмотрим свойства трехмерного линейного итеративного кода [2–3].

Длина информационного слова (количество информационных бит) k, а также величина избыточности (количество проверочных бит) r будут определяться следующими соотношениями [2–3]:

$$k = k_1 \cdot k_2 \cdot k_3; \quad (4)$$

$$r = k_1 \cdot k_2 + (k_1 + k_2 + 1) \cdot (k_3 + 1); \quad (5)$$

$$r = 3 \cdot k_m^2 + 3 \cdot k_m + 1, \quad (6)$$

где k_1, k_2 и k_3 – длины сторон параллелепипеда (в случае куба – $k_1 = k_2 = k_3 = k_m$).

Из (6) следует [2–3], что

$$n = k + r = k_m^3 + 3 \cdot k_m^2 + 3 \cdot k_m + 1. \quad (7)$$

Поэтому степень кодирования (R) и относительная избыточность ($r_{отн}$) равны [2–3]

$$R = \frac{k}{n} = \frac{k_m^3}{k_m^3 + 3 \cdot k_m^2 + 3 \cdot k_m + 1}; \quad (8)$$

$$r_{отн} = \frac{r}{n} \triangleq \frac{3 \cdot k_m^2 + 3 \cdot k_m + 1}{k_m^3 + 3 \cdot k_m^2 + 3 \cdot k_m + 1}. \quad (9)$$

Утверждение1 [5]. Прямым (кронекеровским) произведением двух кодов A и B является код C с параметрами $[n_1 \cdot n_2, k_1 \cdot k_2, d_1 \cdot d_2]$.

Утверждение 2. Минимальное кодовое расстояние трехмерного линейного итеративного кода равно восьми ($d = 8$).

Доказательство. Согласно структуре прямого произведения, минимальное кодовое расстояние ТЛИК можно определить как произведение расстояний Хэмминга соответствующих кодов-сомножителей (для ЛИК $d = 4$, свертки по модулю два – $d = 2$). Следовательно, трехмерный линейный итеративный код характеризуется $d = 2 \cdot 4 = 8$.

Теорема 1 [5–7]. Код с минимальным расстоянием d может исправлять $[(d - 1)/2]$ ошибок. Если d четное, то код может одновременно исправлять $(d - 2)/2$ и обнаруживать $d/2$ ошибок.

Утверждение 3. Трехмерный линейный итеративный код позволяет корректировать все ошибки, кратность которых не превышает трех и обнаруживать до четырех ошибок включительно.

Доказательство данного утверждения основывается на теореме 1 о соотношении числа обнаруживаемых и корректируемых ошибок: минимальное кодовое расстояние ТЛИК равно восьми ($d = 8$, d – четное), следовательно, кратность корректируемых ошибок равна $(d - 2) / 2 = (8 - 2) / 2 = 3$; кратность обнаруживаемых ошибок – $d / 2 = 8 / 2 = 4$.

Что касается других трехмерных итеративных кодов [2–3], то трехмерный линейный итеративный код с диагональными проверками характеризуется минимальным кодовым расстоянием $d = 10$, следовательно, кратность корректируемых ошибок равна четырем ($t = 4$), а для усеченного трехмерного линейного итеративного кода с диагональными проверками $d = 8$, следовательно $t = 3$.

В табл. 1 и 2 приведены результаты расчетов P_b при использовании для коррекции информации трехмерного линейного итеративного кода при различных длинах информационной последовательности (k) и отношениях E_b / N_0 («–» означает, что достигнут требуемый уровень вероятности P_b) (табл. 1 – для $E_b / N_0 = 5–7$, табл. 2 – для $E_b / N_0 = 8–10$).

Таблица 1

Вероятность появления ошибочного бита при декодировании при $E_b / N_0 = 5–7$

k	E_b / N_0		
	5	6	7
16	$4{,}30 \cdot 10^{-4}$	$1{,}14 \cdot 10^{-3}$	$2{,}21 \cdot 10^{-3}$
32	$2{,}02 \cdot 10^{-5}$	$1{,}39 \cdot 10^{-4}$	$5{,}18 \cdot 10^{-4}$
64	$3{,}81 \cdot 10^{-7}$	$1{,}05 \cdot 10^{-5}$	$9{,}70 \cdot 10^{-5}$
128	$4{,}45 \cdot 10^{-11}$	$2{,}28 \cdot 10^{-8}$	$1{,}61 \cdot 10^{-6}$
256	$3{,}62 \cdot 10^{-17}$	$2{,}20 \cdot 10^{-12}$	$3{,}82 \cdot 10^{-9}$
512	–	–	$9{,}03 \cdot 10^{-13}$
1024	–	–	–
4096	–	–	–

Таблица 2

Вероятность появления ошибочного бита при декодировании при $E_b / N_0 = 8–10$

k	E_b / N_0		
	8	9	10
16	$3{,}27 \cdot 10^{-3}$	$4{,}00 \cdot 10^{-3}$	$4{,}12 \cdot 10^{-3}$
32	$1{,}21 \cdot 10^{-3}$	$1{,}99 \cdot 10^{-3}$	$2{,}47 \cdot 10^{-3}$
64	$4{,}07 \cdot 10^{-4}$	$9{,}49 \cdot 10^{-4}$	$1{,}42 \cdot 10^{-3}$
128	$2{,}74 \cdot 10^{-5}$	$1{,}67 \cdot 10^{-4}$	$4{,}77 \cdot 10^{-4}$
256	$5{,}56 \cdot 10^{-7}$	$1{,}40 \cdot 10^{-5}$	$1{,}01 \cdot 10^{-4}$
512	$3{,}07 \cdot 10^{-9}$	$5{,}75 \cdot 10^{-7}$	$1{,}46 \cdot 10^{-5}$
1024	$1{,}73 \cdot 10^{-14}$	$2{,}66 \cdot 10^{-10}$	$1{,}22 \cdot 10^{-7}$
4096	–	–	$4{,}87 \cdot 10^{-9}$

Как видно из табл. 1 и 2, трехмерный линейный итеративный код при $k > 64$ бит позволяет обеспечить требуемый уровень надежности передачи данных ($P_b > 10^{-6} \div 10^{-9}$). При этом код позволяет корректировать не только одиночные, но и многократные ошибки.

Отметим, что аналогичные результаты (вероятность появления при декодировании оши-

бочного бита) показывают трехмерный линейный итеративный код с диагональными проверками ($t = 4$) и усеченный трехмерный линейный итеративный код с диагональными проверками ($t = 3$).

Использование кодов со столь большими значениями k (больше 128 бит) требует введения дополнительных операций на стадии кодирования и декодирования информации.

Пусть по каналам связи будет передаваться информация размером 16 бит. Для обеспечения целостности информации используется трехмерный линейный итеративный (729, 512)-код ($d = 8$, $t = 3$). Весь процесс кодирования данных можно условно разбить на стадии, показанные на рис. 2.

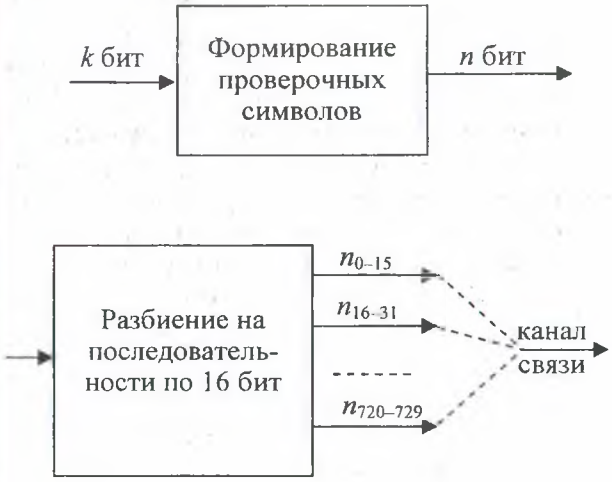

Рис. 2. Схема кодирования данных с использованием трехмерных линейных итеративных кодов

Данные длиной 16 бит передаются по каналу последовательно друг за другом. Перед декодированием необходимо выполнить обратную операцию (соединить все переданные информационные биты в кодовую последовательность длиной n).

Таким образом, трехмерные итеративные коды, несмотря на свою относительно высокую избыточность, обеспечивают требуемый уровень надежности передачи данных по каналам связи благодаря высокой кратности корректируемых ошибок. Необходимо также отметить, что трехмерные итеративные коды позволяют корректировать как одиночные многократные, так и группирующиеся ошибки.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – 2-е издание; Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

2. Романенко Д. М. Свойства трехмерного итеративного кода для систем полупроводниковой памяти с интеграцией на пластине // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: VII Республиканская научная конференция студентов и аспирантов. – Гомель: ГГУ, 2004. – С. 223–224.

3. Урбанович П. П., Романенко Д. М., Орлов А. В. Особенности реализации трехмерного итеративного кода для систем полупроводниковой памяти с интеграцией на пластине // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – 2004. – Вып. XII. – С. 141–144.

4. Урбанович П. П., Романенко Д. М. Коррекция многократных ошибок в информационных словах итеративным кодом // Труды БГТУ. Сер. VI. Физ.-мат. науки и информ. – 1998. – Вып. VI. – С. 88–92.

5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976–594 с.

6. Мак-Вильямс Ф. Дж., Слоэн Дж. А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

7. Fuja T., Heegard C., Goodman R. Liner sum codes for random acces memories // IEEE Transaction on computers. – Vol. 37. N 9, September 1988. – P. 1030–1041.