Изв. АН АрмССР (сер. ТН), т. XLI, № 5, 1988

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

А. В. МАРКАРЯН

МОДИФИКАЦИЯ КОДОВ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА

Рассмотрена разработка кодов с конструктивным расстоянием $d=5$, позволяющих построить кодек по модульной структуре и эффективно использовать существующие разработки БИС кодеков на основе кодов Хэмминга с $d=3$ [1] для исправления двойных ошибок (ДО).

Необходимым и достаточным требованием достижения цели является выбор таких кодов, подматрицы в матрице H контроля четности которых совпадают с H кодов Хэмминга. В этих условиях среди известных наиболее целесообразно использование кодов Боуза-Чоудхури-Хоквингема (БЧХ) с $d=5$, которые являются расширением кодов Хэмминга на случай исправления многократных ошибок и принадлежат с точки зрения корректирующей способности и информационной избыточности к наилучшему классу кодов [2].

Ниже анализируется структура H кодов БЧХ с $d=5$ с учетом указанного требования и доказывается, что это требование выполняется не для всех длин n кодов. На этой основе предлагается модификация кодов БЧХ (МБЧХ) с $d=5$ и показывается, что цель достигается только за счет несущественного ухудшения корректирующей способности.

Матрица H кодов БЧХ может быть реализована и представлена в наиболее близкой к H кодов Хэмминга форме [2]

$$H=\begin{vmatrix} 1 & \alpha^1 & \alpha^2 & \dots & \alpha^i & \dots & \alpha^{i(n-1)} \\ 1 & \alpha^{3} & \alpha^{6} & \dots & \alpha^{3i} & \dots & \alpha^{3i(n-1)} \end{vmatrix}, \qquad (1)$$

где α^i — примитивный элемент поля Галуа $GF(2^r)$ по модулю неприводимого примитивного многочлена степени r; $r=\log_2(n+1)$; $n=2^r-1$; $i=0-(n-1)$; значения i и $3i$ берутся по $\bmod n$; число m информационных разрядов определяется как $m=n-2r$, а разрядность синдрома S равна $2r$; $\alpha^n=1$; H имеет размеры $2r\times n$. Подматрица $H_1=|1\,\alpha^1\,\alpha^2\dots\alpha^i\dots\alpha^{(n-1)}|$ совпадают с H кодов Хэмминга для любых n, поскольку α^i является примитивным элементом $GF(2^r)$, а подматрица $H_3=|1\,\alpha^3\,\alpha^6\dots\alpha^{3i}\dots\alpha^{3(n-1)}|$ не совпадает с H кодов Хэмминга в случае $n=0 \bmod 3$ (n, кратных 3), поскольку α^{3i} не является примитивным элементом $GF(2^r)$ [2]. Отсюда следует, что в общем случае коды БЧХ не удовлетворяют указанному требованию совпадения H.

Определим коды, подматрицы которых совпадают с H кодов Хэмминга. Представим H в виде

$$H=\begin{vmatrix} 1 & \alpha^1 & \alpha^2 & \dots & \alpha^i & \dots & \alpha^{(n-1)} \\ f(0) & f(1) & f(2) & \dots & f(i) & \dots & f(n-1) \end{vmatrix}. \qquad (2)$$

где $f(i)$ некоторая функция от i. Указанное требование предлагается удовлетворить выбором $f(i)$ так, чтобы любой элемент α^i имел свое „отражение" в $f(i)$, т. е. чтобы в H' существовали такие $i_1 \neq i_2 \in i$, для которых выполняется $\alpha^{i_1} = f(i_2)$. Такое отражение в отличие от $H(1)$, где выбрано $f(i) = \alpha^{2i}$, можно обеспечить с учетом $\alpha^{-i} = \alpha^{n-i}$ и выбором $f(i) = \alpha^{-i}$.

Докажем теорему о корректирующей способности кодов, для которых $f(i) = \alpha^{-i}$. Предложенные в результате коды назовем кодами МБЧХ, учитывая, что значения H_1 для МБЧХ и БЧХ кодов совпадают.

Теорема. Двоичные коды МБЧХ с матрицей

$$H = \begin{vmatrix} 1 & \alpha^1 & \alpha^2 \dots \alpha^i \dots \alpha^{i(n-1)} \\ 1 & \alpha^{-1} & \alpha^{-2} \dots \alpha^{-i} \dots \alpha^{-(n-1)} \end{vmatrix} \qquad (3)$$

исправляют для $n \neq 0 \bmod 3$ все n одиночных ошибок (00) и все сочетания $\binom{n}{2}$ ДО, а для $n = 0 \bmod 3$ — все 00 и $\left(\binom{n}{2} - n\right)$ ДО.

Доказательство. Коды МБЧХ исправляют все 00 независимо от n, т. к. H_1 совпадает с H кодов Хэмминга.

В случае ДО, обозначив для $H(3)$ соответственно номера первой и второй ошибок через x^{i_1} и x^{i_2}, с учетом $f(i) = \alpha^{-i}$ верна следующая система уравнений:

$$\begin{cases} \alpha^{i_1} + x^{i_2} = S_1; \\ \alpha^{-i_1} + \alpha^{-i_2} = S_{-1}, \end{cases} \qquad (4)$$

где $S = [S_1 \; S_{-1}]$.

Система (4) является системой из двух независимых уравнений, т. к. $S_{-1}(\alpha^{i_1} + \alpha^{i_2}) \neq S_1$ и $\alpha^{i_1}\alpha^{i_2} = S_1 S_{-1}$. Следовательно, по $H(3)$ можно отличить значения $S = [S_1 \; S_{-1}]$ всех $\binom{n}{2}$ ДО. Однако представляется возможным случай, когда $S_1^{-1} = S_{-1}$, что также выполняется в случае 00. Тогда кодек не сможет отличить 00 от ДО. Определим в каких случаях выполняется $S_1^{-1} = S_{-1}$, если имеет место ДО. С этой целью преобразуем систему (4) к виду

$$\begin{cases} \alpha^{i_1} + \alpha^{i_2} = S_1, \\ 1 \cdot \alpha^{i_1} + 1 \cdot \alpha^{i_2} = 1 \cdot S_{-1}. \end{cases} \qquad (5)$$

Откуда $S_1 = \alpha^{i_1}\alpha^{i_2}(\alpha^{i_1} + \alpha^{i_2})$ и после подстановки в это уравнение значения $\alpha^{i_1} = S_1 + \alpha^{i_2}$ из верхнего уравнения системы (5) получим $(\alpha^{i_2})^2 + S_1\alpha^{i_2} + S_1^2 = 0$. Разделив все члены последнего уравнения на S_1^2:

$$(\alpha^{i_2} S_1)^2 + (\alpha^{i_2} S_1) + 1 = 0. \qquad (6)$$

Нетрудно показать, что в $GF(2^r)$ корнями $X^2 + X + 1 = 0$ являются $X^{(2^r-1)/3}$ и $1/X$, если (2^r-1) делится на 3, а в противном случае — $X^2 + X + 1 \neq 0$. Приняв $X = \alpha^{i_1}/S_1$, следует, что равенство (6) выполняется, т. е. $S_1^{-1} = S_{-1}$ только в случаях, когда $\alpha^{i_1}/S_1 = \alpha^{\pm n/3}$ и $n = 0 \mod 3$, а учитывая, что S_1 по $H(3)$ может принимать максимум n значений — для $n = 0 \mod 3$ из возможных $\binom{n}{2}$ сочетаний существует n сочетаний пары $(i_1 i_2)$, для которых $S_1^{-1} = S_1$. Откуда и вытекает доказательство теоремы.

Поскольку размеры $H(1)$ и $H(3)$ совпадают, то коды МБЧХ характеризуются такой же избыточностью, что и коды БЧХ.

Докажем, что корректирующая способность кодов МБЧХ несущественно хуже, чем кодов БЧХ. Вероятность $P_{до}$ исправления ДО, равная отношению числа исправляемых ДО к возможному, для любых n кодов БЧХ равна 1. Из приведенной теоремы вытекает, что для кодов МБЧХ

$$P_{до} = \begin{cases} 1, & \text{если } n \neq 0 \mod 3, \\ \left.\left[\binom{n}{2} - n\right] \middle/ \binom{n}{2}\right. = (n-1)/(n-3), & \text{если } n = 0 \mod 3, \end{cases}$$

т. е. с возрастанием n значение $P_{до}$ стремится к 1. Так, при $18 \leqslant n \leqslant 31$ значение $P_{до} = 1$ и практически для всех $n \geqslant 63$ также можно принять $P_{до} \cong 1$. Исключая случай $n < 8$, не представляющий практического интереса, минимальное $P_{до} \cong 0{,}95$ получается при $n = 32$, которое, очевидно можно считать несущественно меньшим относительно $P_{до} = 1$.

В заключение отметим, что предложенные коды МБЧХ позволяют без потерь на проектирование и освоение новых модификаций БИС эффективно использовать существующие разработки БИС кодеков на основе кодов Хэмминга для исправления ДО—цель достигается только за счет несущественного ухудшения корректирующей способности кодов МБЧХ по сравнению с наилучшими в этом отношении кодами БЧХ с $d = 5$.

ЕрНИИММ

10. VII. 1986

Ս. Վ. ՄԱՐԴԻՐՅԱՆ

ԲՈՈՒԶ-ՉՈՈՒԴՀՈՒՐԻ-ՀՈԿՎԻՆԳԵՄԻ ԿՈԴԵՐԻ ՁԵՎԱՓՈԽՈՒԹՅՈՒՆԸ

Ամփոփում

ԲՉՀ-ի կոդերը վերլուծվում են կրկնակի սխալներն ուղղող կոդեկի կառուցման տեսանկյունով Հեմինգի կոդերի՝ ներկայումս գոյություն ունեցող ԲԻՍ կոդեկների մշակումների օգտագործմամբ։ Ցույց է տրվում, որ այդպիսի

իրագործումը նպատակահարմար է միայն 3-ի բաժանվող n երկարության կոդերի համար: Առաջարկվում է ԲՉՀ-ի կոդերի մի ձևափոխություն, որը հնարավորություն է տալիս n-ի ցանկացած արժեքների դեպքում կրկնակի սխալները ուղղելու համար արդյունավետ օգտագործել գոյություն ունեցող ԲՉՀ կոդեկները: Ցույց է տրվում, որ համեմատած ԲՉՀ-ի կոդերի հետ նպատակին կարելի է հասնել ընդամենը ուղղող հատկությունների ոչ էական վատացման հաշվին:

ЛИТЕРАТУРА

1. *Борисов В. С.* Обнаружение и исправление ошибок в запоминающих устройствах // Зарубежная радиоэлектроника.—1984.—№ 10.—С. 21—41.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки.—М.: Связь, 1979.—744 с.

Изв. АН АрмССР (сер. ТН), т. XLI, № 5, 1988

ГИДРАВЛИКА

А. А. МИХНЮК, В. Б. ЦАГРЯН, Т. Д. ГОЦЕРИДЗЕ

НЕЛИНЕЙНЫЕ ВЗАИМОДЕЙСТВИЯ ВОЛН ПРИ ЛАБОРАТОРНОМ МОДЕЛИРОВАНИИ НЕРЕГУЛЯРНОГО ВОЛНЕНИЯ

Моделирование волн больших водоемов с помощью создания регулярных волн на модели не позволяет с точностью воспроизвести их воздействие на береговые участки. В настоящее время осуществляется постепенный переход к воспроизведению реального или близкого к нему нерегулярного волнения. Наиболее перспективным направлением развития методов генерации нерегулярного волнения считается введение в системы управления волновоспроизводящими установками ЭВМ, работающих в реальном режиме времени [1]. При этом предусматривается как прямое воспроизведение нерегулярного волнения с натурной записи с использованием встроенных или программно заданных передаточных функций типа функции Базеля, так и синтез управляющего воздействия с использованием обратного преобразования Фурье или методов цифровой фильтрации [2].

В работе приводятся результаты изучения взаимодействия волн различных частот, при которых происходит искажение высокочастотной области спектра нерегулярного волнения. Эти искажения существенно влияют на фазовые скорости данной области спектра.

Рассмотрим взаимодействие двух гармоник спектра, которые значительно отличаются по частоте и по волновому числу. Такое взаимодействие можно рассматривать по типу «волна на течении». Исходя из уравнения адиабатического приближения, записанного в системе координат, движущейся с фазовой скоростью длинной волны C, в первом