УДК 004.056.55

ДЕКОДИРОВАНИЕ МНОГОКРАТНЫХ ОШИБОК НЕ ПРИМИТИВНЫМИ КОДАМИ ХЕММИНГА МЕТОДОМ УЖАТИЯ ОРБИТ

А.О. ОЛЕКСЮК[1], В.А. ЛИПНИЦКИЙ[2]

[1]Военная академия Республики Беларусь
пр-т Независимости, 220, г. Минск, 220057, Республика Беларусь
Un_ami@mail.ru

[2]Военная академия Республики Беларусь
пр-т Независимости, 220, г. Минск, 220057, Республика Беларусь
6358549@mail.ru

Защита информации в инфокоммуникационных системах играет очень большую и важную роль, данный вопрос, по своей степени важности, занимает одно из первых мест. Особое внимание уделяется не только конфиденциальности передаваемой информации, но и защиты ее от помех. Реальные каналы связи неизбежно содержат различного рода шумы и помехи, что значительно сказывается на точности и достоверности передаваемых данных.

Ключевые слова: коды Хемминга, G-орбиты, микропроцессор.

В реальных каналах связи передача информации осуществляется под влиянием разного рода помех и шумов. Для борьбы с ними в цифровых системах передачи информации используется введение избыточности в передаваемое сообщение. Данная идея воплотилась применением помехоустойчивых кодах в цифровых ТКС.

В настоящее время существует огромный спектр разнообразных помехоустойчивых кодов. В современных информационно-коммуникационных системах (ИКС) наиболее применением класс линейных кодов. Характерными представителями линейных кодов являются коды Хемминга. Данные коды широко применяются в материнских платах, используются в пейджинговой, сотовой, космической связи [1-4].

По своей структуре коды Хемминга можно разделить на два основных класса: примитивные и не примитивные. Примитивные имеют завершенную теорию, четкую структуру и массовое применение. Не примитивные – остались за пределами приложений.

Данный доклад посвящен изучению требуемых кодов в классе не примитивных кодов Хемминга.

Применяемые в практике помехоустойчивого кодирования коды Хемминга задаются над полями Галуа (как правило, характеристика поля равна двум), то есть над полями $GF(2^m)$, $m > 2$. Длина n кода Хемминга является делителем числа $2^m - 1$ (при $n = 2^m - 1$ код Хемминга называют примитивным) [2]. При этом m минимально в том смысле что n не может быть делителем числа $2^\mu - 1$ для $\mu < m$. Мы рассматриваем циклические коды Хемминга задаваемые проверочной матрицей:

$$\overline{H} = \left(\beta^i\right)^T. \qquad (1)$$

Здесь $\beta = \alpha^\mu$ для $\mu = (2^m - 1)/n$ и примитивного элемента α поля Галуа $GF(2^m)$.

На сегодняшний день единственным реальным методом коррекции ошибок, кратность которых превосходит конструктивные возможности кода, является перестановочный метод, метод орбит [2]. В [2] основной упор делается на Г-орбиты.

В данной работе Г-орбиты объединяются в более крупные G-орбиты, содержащие, как правило, по *mn* векторов. Работа с G-орбитами, фактически, сжимает в *mn* раз информацию о корректируемых ошибках.

Разработан общий метод сжатия орбит ошибок не примитивного кода Хемминга. Предварительно составляется список 1 образующих G-орбит и значений их синдромов декодируемой совокупности K_t. Действующая ИКС, приняв очередное сообщение $\bar{x}$, вычисляет его синдром ошибок $S(\bar{x})$. Если $S(\bar{x}) = 0$, то сообщение не содержит ошибок и является правильным. Если же $S(\bar{x}) \neq 0$, то $\bar{x}$ подлежит коррекции, так как содержит неизвестную вектор-ошибку $\bar{e}$. Для нахождения этой вектор-ошибки полученный синдром $S(\bar{x})$ в двоичном виде и преобразуется по модулю $(2^m - 1)/n$, также значение $S(\bar{x})$ делится $(2^m - 1)/n$ и округляется до целого значения в большую сторону, округленное число t будет определять сдвиг начального местоположения ошибки в Г-орбите. Далее преобразованное значение $S(\bar{x})*$ по модулю $(2^m - 1)/n$ складывается само с собой r раз до того момента пока не совпадет с одним из значений указанных в списке 1, это означает, что искомая вектор-ошибка $\bar{e}$ принадлежит G-орбите, порожденной вектором $\bar{e}^*$ из данного списка. Далее вектор $\bar{e}^*$ в обратном порядке сдвигаем на r и t позиций, таким образом однозначно определяем вектор $\bar{e}$.

Реализация метода сжатия Г-орбит ошибок для конкретных кодов на конкретных длинах имеет индивидуальные особенности, так как зависит от кратности исправляемых ошибок и мощности многообразия K_t этих ошибок.

Список литературы

1. *MacWilliams, F.J.* The Theory of Error-Correcting Codes/ F.J. MacWilliams, N.J.A. Sloane // North-Holland Mathematical Library. –1977. –Vol.16. – 762 p.

2. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения/ В.А. Липницкий, В.К. Конопелько. – Мн.: Издат. Центр БГУ, 2007. – 216с.

3. *Конопелько, В.К.* Теория прикладного кодирования Том 1/ В.К. Конопелько [и др.]; под общ. ред. В.К. Конопелько. – Минск: БГУИР, 2004. – 288 с.

4. *Конопелько, В.К.* Теория прикладного кодирования Том 2/ В.К. Конопелько [и др.]; под общ. ред. В.К. Конопелько. – Минск: БГУИР, 2004. – 400 с.