РЕАЛИЗАЦИЯ УНИВЕРСАЛЬНОГО ДЕШИФРАТОРА ДЛЯ КОРРЕКТИРУЮЩИХ КОДОВ НА ОДНОРОДНЫХ СТРУКТУРАХ

Т.М. Кокочашвили

(Москва)

Как известно, система передачи информации состоит из передатчика, преобразующего сообщение в сигнал, канала связи , по которому передается сигнал, приемника, вновь преобразующего сигнал в сообщение. Сообщение поступает в передатчик от источника сообщений. Приемник выдает информацию получателю сообщений (рис.I).

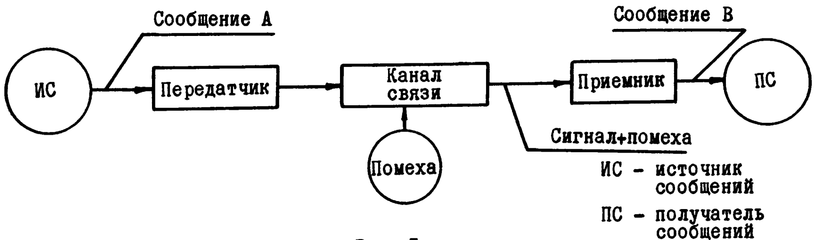

Рис. I.

Конечная цель системы заключается в передаче сообщения от источника к получателю. Цель можно считать достигнутой, если принятое получателем сообщение В в точности соответствует переданному сообщению А .

Однако система передачи информации находится под воздействием помех, которые искажают передаваемые по каналу связи сигналы. Одним из действенных методов борьбы с помехами и повышения надежности передаваемой информации является использование корректирующих кодов.

Корректирующими называются коды,позволяющие обнаруживать и исправлять ошибки, происходящие из-за помех [I] .

Говорят о различной кратности ошибок, имея при этом в виду число q искажений символов в пределах одной кодовой комбинации.

Идея возможности обнаружения ошибки предельно проста. Она заключается в том, что в равномерном блочном коде для передачи информации используются не все $N = m^n$ возможные кодовые комбинации, а лишь некоторая часть из них N_0 :

$$N_0 < N, \tag{I}$$

где m - основание кода (будем рассматривать только $m = 2$),т.е. число различных символов в кодовом слове;

n - значность кода, т.е. число символов в кодовой комбинации.

Комбинации N_0 называются разрешенными, а остальные неиспользуемые $N - N_0$, - запрещенными.

Говоря об общем числе возможных ошибок, здесь и в дальнейшем будем иметь в виду, что может передаваться любая из разрешенных N_0 комбинаций и что каждая из них может превратиться в любую из N возможных кодовых комбинаций.

Для исправления обнаруженных ошибок все запрещенные кодовые комбинации должны быть разбиты на N_0 непересекающихся групп (по числу разрешенных кодовых комбинаций). Каждой группе (назовем их декодированными) соответствует одна разрешенная кодовая комбинация. Смысл дешифрирования заключается в преобразовании искаженной (запрещенной) кодовой комбинации в соответствующую ей разрешенную кодовую комбинацию.

Для использования корректирующей способности кода в структуру кода необходимо вводить избыточность, которая зависит от способа кодирования и декодирования. Используя избыточную структуру кода, стремятся максимально упростить техническую реализацию кодирующих и декодирующих устройств, применяя для различных кодов разные принципы кодирования и декодирования.Большой интерес представляет создание универсального дешифратора. Под универсальным дешифратором понимается дискретное устройство, при помощи которого можно было бы исправить любое количество ошибок в любом сочетании. Такую задачу можно решить двумя путями.

I. Создать универсальный код, который путем изменения структуры изменял бы свою корректирующую способность в зависимости от вводимой избыточности так, чтобы при этом не менялся принцип кодирования и декодирования.

2. Выделяя отдельно дешифрирующее устройство, можно значительно упростить поставленную задачу, создав универсальный дешифратор и использовав только корректирующую способность кода. Универсальный дешифратор можно реализовать следующим образом. Представим каждую кодовую комбинацию,как переключательную функцию, реализующую элементарную конъюнкцию от n переменных, где n -значность кодовой комбинации.

Дешифратор будет представлять собой дискретное устройство, имеющее $\{x_1,\dots,x_n\}$ входов и $\{y_1,\dots,y_n\}$ выходов. На входы поступают различные кодовые комбинации, при этом допускаются любые искажения, вносимые помехами и известна корректирующая способность кода. Каждой разрешенной кодовой комбинации $x_1,\dots,x_n$ соответствует один из выходов y_i ,а также группа запрещенных кодовых комбинаций, отстоящих от неё на расстояние

$$d < 2q + 1, \tag{2}$$

где d - наименьшее расстояние между разрешенными кодовыми словами;

q - кратность ошибки.

Очевидно, число членов таких групп зависит от корректирующей способности кода и равно:

$$\sum_{q=1}^{q=k} C_n^q .$$

Избыточность, которую необходимо вводить в дешифратор,определяется возможностью реализации всех $N_0\left(\sum_{q=k}^{q=k} C_n^q + 1\right)$ элементарных конъюнкций. Реализация такого универсального дешифратора требует большего количества элементов и поэтому практически выполнима для малых n и q. Такой подход является общим для всех дискретных устройств, реализующих только комбинационные функции.

Использование однородных структур позволяет решить более общую задачу , а именно: создать структуру, обладающую такой универсальностью, которая позволила бы моделировать в ней лю-

бую комбинационную схему,а также универсальный дешифратор для корректирующих кодов (в том смысле, как он определен выше), сложность L^{P} которого определяется следующим неравенством

$$L^{P} < N_0 K_0 \left(\sum_{q=1}^{q=k} C_n^q + 1 \right). \qquad (3)$$

Под сложностью понимается количество настроечной информации, вводимой в структуру.

K_0 - коэффициент, зависящий от алгоритма функционирования однородной структуры. Он определяется тем, что для любой однородной структуры при моделировании в ней элементарных конъюнкций, содержащих инверсные члены, необходимо число элементов больше, чем n , где n - ранг конъюнкции, соответствующий значности кода.

Правую часть неравенства (3) можно уменьшить только за счет члена $\sum_{q=1}^{q=k} C_n^q + 1$, который требует при моделировании на однородной структуре наибольшего количества элемента и тем самым определяет сложность структуры.

Ни одна из однородных структур описанных в работах [2, 3, 5] не позволяют уменьшить сложность так, чтобы выполнялось неравенство (3), однако алгоритм функционирования однородной структуры из КЭ [5] при некотором дополнении позволяет значительно уменьшить сложность L^{P} . Покажем это на структуре с наименьшей координатой [5].

Изменив несколько таблицу переходов I [5], но при этом сохранив возможность моделирования комбинационных функций, получим таблицу переходов I'.

Таблица I'

V_{2t}	V_{1t}	V_{0t}	$V_{1,t+1}$	$V_{2,t+1}$	K_1	K_2
0	0	0	0	0	0	0
0	0	I	I	I	0	0
0	I	0	0	0	0	0
0	I	I	I	I	0	I
I	0	0	0	0	0	0
I	0	I	I	I	I	0
I	I	0	I	0	I	I
I	I	I	0	I	0	I

Дополним её следующими правилами коммутации.

I. Пусть имеются элементы α_1 и β_2 ,(рис.2) которые в момент времени t находятся в состоянии "I" и при этом коммутируют друг с другом.

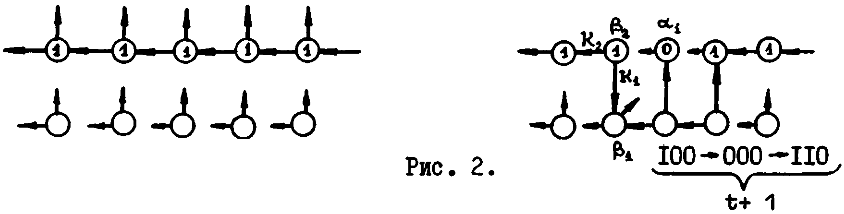

Рис. 2.

Если в момент времени $t+1$ α_1 изменит свое состояние на "0" ("I" → "0") и при этом α_1 отключает свой коммутационный выход K_2 ,а β_2 своего состояния не изменило и существует элемент β_1 с координатой v_1 относительно β_2, то в момент времени $t+1$ β_2 свой коммутационный выход K_1 подключает к β_1 .

Если такого элемента α_1 в $t+1$ не существует, то β_1 состояния своего коммутационного выхода K_1 не меняет.

2. Если состояние входов элемента α_1 в момент времени t было I00 и в момент времени $t+1$ изменилось на 000,то в момент времени $t+1$ состояние входов станет II0, причем

$$t + \nu_1 + \nu_2 = t + 1.$$

Моделирование универсального дешифратора для корректирующих кодов на структуре, функционирующей по такому алгоритму, позволяет значительно уменьшить L^D .

Представим каждую разрешенную кодовую комбинацию,как конъюнкцию длиной n

$$x_1, x_2, \ldots, x_n,$$

затем разобьем дешифрируемое слово на подслова длиной l ,сохраняя при этом последовательность разрядов. Каждое подслово длиной l моделируется на однородной структуре с наименьшей координатой, образуя участки проводимости (что соответствует единичному значению переключательной функции $f(x_1, x_2, \ldots, x_n)$. Объединив последовательно все участки, получим выход для дешифрируемого слова $x_1, x_2, \ldots, x_n$. Разрядность подслова длиной l зависит от кратности ошибки и равно $r+1$, где $r = 2$ при $q \leq 2$ и $r=q$ при $q \geq 2$.

При моделировании последнего разряда разрешенного кодового слова $\{x_1, x_2, \ldots, x_n\}$ к последнему символу x_n добавляем

первые t символов разрешенной кодовой комбинации $x_1, x_2, \dots, x_n$, причем

$$t = \begin{cases} l - (n - \left[\frac{n}{l}\right] l), & \text{если } l \mid n, \\ 0 & \text{, если } l \nmid n, \end{cases}$$

где $\left[\frac{n}{l}\right]$ означает целое число, не превосходящее $\left[\frac{n}{l}\right]$. При таком моделировании разрешенной кодовой комбинации её структура не меняется, и при этом получаем ровно nl подслов.

На каждом участке однородной структуры из КЭ, моделирующем подслова l, происходит исправление (коррекция) поступающей на вход дешифратора разрешенной кодовой комбинации.

Таким образом, в каждый квантованный отрезок времени на одном из выходов y_i будем иметь "I", соответствующую именно тому сообщению, которое было послано в момент времени t, а на остальных $y_1, y_2, \dots y_{i-1}, y_{i+1}, \dots y_n$ выходах имеем "0". Этим контролируется правильность дешифрации. Сложность дешифратора при этом будет:

$$L^D = K_1 (r + 1) n N^0,$$

K_1 - коэффициент, линейно зависящий от r.

Каждая разрешенная кодовая комбинация состоит из "I" и "0". При моделировании её на структуре проводимость создается, когда на входы подаются α_i - ые значения переменных, если кодовое слово содержит "I", констант "I", если кодовое слово содержит "0". Ошибки могут быть либо $1 \to 0$, либо $0 \to 1$ в пределах каждой кодовой комбинации,

Возможность исправления ошибок вытекает из того, что при переходе $1 \to 0$ и $0 \to 1$ возникают обходные участки проводимости, которые исчезают при поступлении разрешенной кодовой комбинации. Нетрудно заметить, что при этом принцип максимального правдоподобия выполняется автоматически.

Любая кодовая комбинация состоит из "I" и "0". Под ошибкой понимается переход $1 \to 0$ или $0 \to 1$ в пределах одной кодовой комбинации. На рис. 3-6 показано, как необходимо моделировать дешифрируемое слово $x_1 x_2 \dots x_n$ на однородной структуре и как распределить при этом константы "I".

На рис.3 показано исправление любой одиночной ошибки в кодовом слове II...I. Каждый из x_i подается на α_i Одиноч-

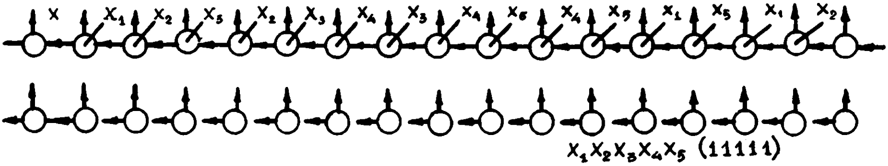

Рис. 3.

ные ошибки означают изменение состояния $\alpha_1(I)$ на $\alpha_1(0)$ в момент времени $t + 1$, при этом α_1 в момент времени t коммутировало с β_2. В момент времени $t+1$ состояние β_2 не меняется (остается в состоянии "I"). Алгоритм функционирования структуры при использовании добавочных правил коммутации I-2 позволяет создать обходные участки проводимости (корректирующая способность структуры). При восстановлении единичного состояния элемента α_1 обходной участок исчезает , и коммутация происходит между элементами α_1 и β_2, так же как и в момент времени t.

На рис.4 показано моделирование дешифрируемого слова и

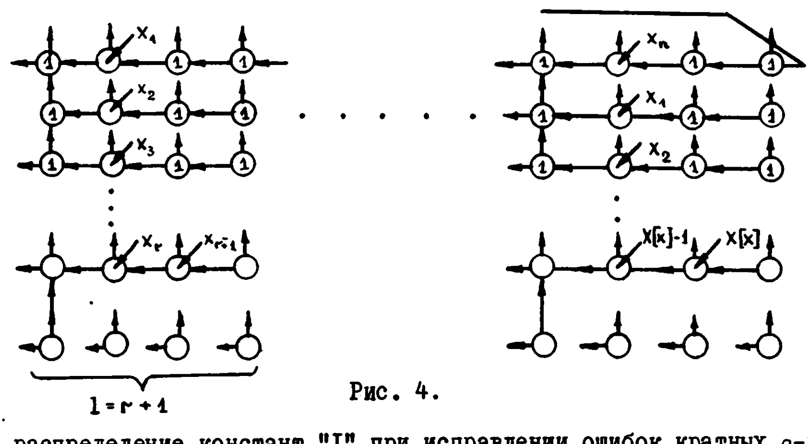

Рис. 4.

распределение констант "I" при исправлении ошибок кратных q=2. На рис.5 показано исправление одиночной ошибки и распределение констант "I" в кодовом слове 00...0. Проводимость между a и b соответствует кодовому слову 00...0. Ошибка, обусловленная помехой, означает переход $0 \to 1$, при этом также возникает обходной участок (согласно таблице переходов I'), который исчезает при обратном переходе $1 \to 0$.

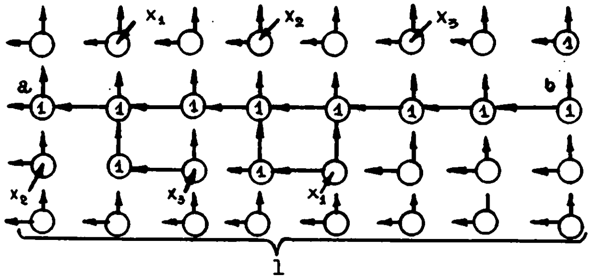

Рис.5

На рис.6 показано исправление ошибки кратной k и распределение констант "I" для кодового слова 00...0.

Как следует из правил коммутации, наибольшее количество элементов необходимо для образования инверсии при моделировании комбинационных функций или при моделировании универсального дешифратора для кодового слова 000...0.

Поэтому сложность структуры определяется сложностью моделирования кодового слова 00...0. При исправлении одиночной ошибки

$$L^{\flat}_{1} = 24\ N_0 n. \tag{4}$$

При исправлении ошибок кратности k

$$L^{\flat}_{k} = 2\ N_0 n\ (k + 1)(k + 3). \tag{5}$$

Если не использовать корректирующую способность структуры[5] то сложность будет определяться количеством элементов, необходимых для моделирования правой части неравенства (3), и равна соответственно

$$L = \left[3(n + 2) \left(\sum_{q=1}^{q=k} C^{q}_{n} + 1 \right) \right] N_0. \tag{6}$$

Из выражений (5) и (6) следует, что $L^{\flat}_{k} < L$.

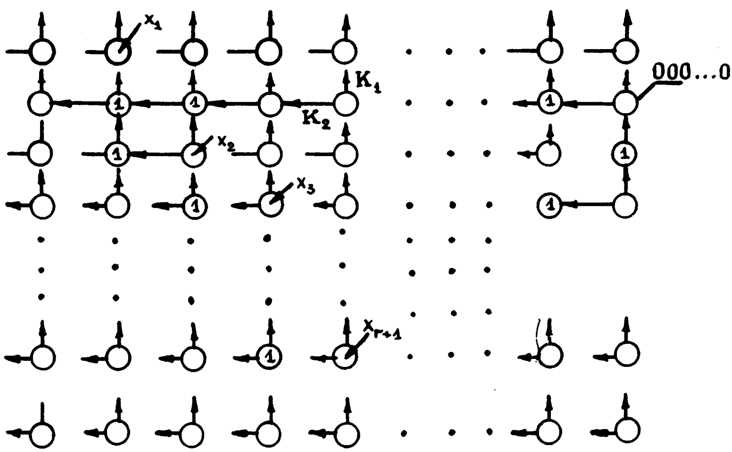

Рис. 6.

ЛИТЕРАТУРА

I. А.А. Харкевич. Борьба с помехами, М., 1965.

2. И.В. Прангишвили, Е.В. Бабичева, З.В. Игнатущенко. Новые принципы реализации логических и вычислительных устройств на основе микроэлектронных однородных структур. - Автоматика и телемеханика, 1965, № 10.

3. Э.В. Евреинов. Теоретические основы построения универсальных вычислительных сред. Вычислительные системы. Новосибирск, Изд-во "Наука" Сибирское отделение, 1965, вып. 16.

4. У. Питерсон. Коды, исправляющие ошибки. Изд-во " Мир", 1964.

5. Т.М. Кокочашвили. Один вариант однородной дискретной структуры с коллективным поведением ячеек.- Данный сборник, стр.