УДК 621.37.037 Вестник УрФО № 1(43) / 2022, с. 5–10

Петухов А.Г., Степанцова А.М., Делог А.Н.

DOI: 10.14529/secur220101

ИСПОЛЬЗОВАНИЕ КОРРЕКТИРУЮЩИХ КОДОВ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Передавая какие-либо сведения по каналу связи, абсолютно любая кодовая комбинация несет полученную информацию. В связи с тем, что не исключено возможное внешнее воздействие, либо внутренние сбои в работе аппаратуры, могут возникать помехи, которые искажают кодовые комбинации. Одним из способов повышения помехоустойчивости систем передачи информации является применение корректирующих кодов, которые позволяют обнаруживать или исправлять ошибки, возникающие при передаче информации из-за влияния помех. На сегодняшний день известно огромное количество корректирующих кодов, разных по строению и отличающихся друг от друга своими основными характеристиками. В данной статье рассматривается их классификация, принцип обнаружения ошибок и помехоустойчивого кодирования, геометрическая модель кода.

Ключевые слова: *корректирующий код, разрешенные и запрещенные комбинации, кодовое расстояние, бинарный код, помехоустойчивость.*

Petukhov A.G., Stepantsova A.M., Delog A.N.

THE USE OF CORRECTION CODES TO INCREASE THE NOISE IMMUNITY OF INFORMATION TRANSMISSION SYSTEMS

Transmitting any information over the communication channel, absolutely any code combination carries the received information. Due to the fact that possible external influences or internal failures in the operation of the equipment are not excluded, interference may occur that distort the code combinations. One of the ways to increase the noise immunity of information transmission systems is the use of correction codes that allow you to detect or correct errors that occur during the transmission of information due to the influence of interference. To date, a huge number of corrective codes are known, different in structure and differing from each other in their main characteristics. This article discusses their classification, the principle of error detection and noise-resistant coding, the geometric model of the code.

Keywords: *correcting code, permitted and prohibited combinations, code distance, binary code, noise immunity.*

Корректирующие коды подразделяются на два класса: обнаруживающие и исправляющие. Первые позволяют установить факт наличия искажения кодовых комбинаций. Вторые (корректирующие) позволяют обнаружить ошибку и установить ее место в кодовой комбинации, что дает возможность ее исправить.

Принцип обнаружения ошибок состоит в следующем. Если число возможных кодовых комбинаций при заданном основании m и значности кода n равно $N = m^n$, то для передачи сообщений используется некоторая часть их $N_p < N$.

Используемые в данном коде комбинации называются разрешенными, а остальные $N – N_p$ неиспользуемые комбинации – запрещенными [1,11].

На рисунке 1 представлена диаграмма вероятностных переходов при передаче N_p сообщений. Символами A_i обозначены разрешенные, а символами B_j – запрещенные комбинации, в которые могут перейти разрешенные в результате различного сочетания ошибок при приеме.

Очевидно, что каждая из разрешенных комбинаций при воздействии помехи, приводящей к ошибкам при приеме, может превратиться в любую из N возможных комбинаций, за исключением самой себя (в последнем случае ошибка отсутствует). Таким образом, общее количество ошибочных комбинаций при передаче N_p сообщений равно N_p (N-1). Из этого количества ошибки могут быть замечены только в том случае, если разрешенная кодовая комбинация переходит в запрещенную [2]. Следовательно, количество фиксируемых ошибок при передаче одного сообщения будет равно $N–N_p$, а при N_p сообщениях будет N_p $(N– N_p)$.

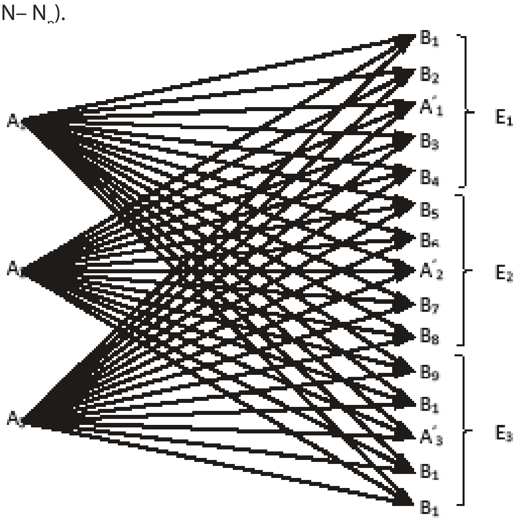

Рис. 1. Диаграмма вероятностных переходов для корректирующего кода

Доля обнаруженных ошибок $\eta_{об}$ составляет:

$$\eta_{об} = \frac{Np(N-Np)}{Np\ (N-1)} = \frac{N}{N-1} - \frac{Np}{N-1}.$$

Так как обычно N>>1, то:

$$\eta_{об} = 1 - \frac{Np}{N}.$$

Как следует из последнего, доля обнаруживаемых ошибок возрастает с увеличением числа избыточных кодовых комбинаций.

При использовании кода в качестве исправляющего в приемнике производится разбиение всего множества возможных кодовых комбинаций N на N_p непересекающихся областей E_i (непересекающиеся подмножества), причем каждая из областей E_i приписывается к одной из разрешенных кодовых комбинаций A_i, Если принятая кодовая комбинация находится в области E_i, то при приеме считается, что передано сообщение A_i. Очевидно, что количество исправляемых ошибок при передаче одного сообщения будет равно числу запрещенных комбинаций, входящих в данную область E_i а общее количество исправляемых ошибок при N_p разрешенных кодовых комбинаций равно общему числу запрещенных кодовых комбинаций $N– N_p$.

Отношение числа исправляемых ошибочных комбинаций к числу обнаруживаемых ошибочных комбинаций составляет:

$$\eta_{и} = \frac{N-Np}{Np\ (N-Np)} = \frac{1}{Np}.$$

Таким образом, обнаруживающая и исправляющая способность кода зависит прежде всего от количества избыточных (запрещенных) кодовых комбинаций. Практически увеличение количества кодовых комбинаций по сравнению с требуемым для передачи определенного числа сообщений при данном методе кодирования может быть достигнуто увеличением значности кода, т. е. удлинением кодовых посылок [3]. В настоящее время хорошо разработаны только бинарные корректирующие коды. Поэтому в дальнейшем будем полагать m = 2.

Если в системе связи необходимо передать N_p – 2^h сообщений, то для придания коду корректирующих способностей необходимо увеличить число кодовых комбинаций до $N = 2^n$, причём n>k. Следовательно, комбинации корректирующего кода должны содержать n символов, из которых k являются информационными, а (n – k) – дополнительными контрольными или проверочными символами.

Выше было установлено количество комбинаций, которые можно исправить данным корректирующим кодом, из общего числа возможных ошибочных комбинаций. Естественным критерием при выборе типов исправляемых кодовых комбинаций является минимизация средней ошибки. Если ошибки при приеме каждого символа независимы, то их вероятность убывает с повышением кратности. Следовательно, для уменьшения средней вероятности ошибки необходимо в первую очередь исправлять ошибки низшей кратности.

Установим связь между кратностью исправляемых ошибок и количеством контрольных символов в кодовой комбинации. Предположим, что код используется для исправления ошибок кратности от 1 до r включительно. Так как количество ошибок кратности i в комбинации, состоящей из n символов, равно числу сочетаний из n элементов по i, то общее количество ошибок λ_r кратности от 1 до r, возможных в одной комбинации, равно:

$$\lambda_r = \sum_{i=1}^{r} c_n^i.$$

Тогда общее количество ошибок, исправляемых в N_p комбинациях, составляет $N_p\lambda_r$.

С другой стороны, код может исправить не более $N-N_p$ ошибочных комбинаций. Следовательно, величины N и N_p должны выбираться так, чтобы выполнялось неравенство:

$$N_p\lambda r \leq N - N_p,$$

откуда $N \geq N_p (1 + \lambda_r)$.

Поскольку $N = 2^n$ и $N_p - 2^k$, то подставляя значение λ_r и логарифмируя последнее неравенство по основанию 2, получим:

$$n-k \geq \log_2 \sum_{i=0}^{r} c_n^i. \quad (1)$$

При выводе формулы (1) было использовано тождество $C^0_n = 1$. С помощью формулы (1) можно определить количество контрольных символов в кодовых комбинациях, необходимое для придания коду определенной исправляющей способности [4,5]. Знак «$\geq$» в ней означает, что округление величины log должно производиться в сторону увеличения до ближайшего целого значения. На практике обычно известной является величина k, так как она связана с количеством передаваемых сообщений. Однако формула непосредственной связи величин n и k оказывается сравнительно громоздкой, особенно при высокой кратности исправляемых ошибок. Поэтому для определения необходимого количества символов корректирующего кода обычно прибегают к составлению таблиц (таблица 1) зависимости между n и k для определенной кратности исправляемых ошибок.

С помощью подобной таблицы можно легко определить количество необходимых символов в комбинациях корректирующего кода n при заданном k и r. Например, пусть количество информационных символов k = 5, а код должен исправлять все однократные ошибки. По этим данным в таблице находим значение n = 9.

Таблица 1

Таблица зависимости для определения кратности исправляемых ошибок

k		1	2	3	4	5	6	7	8	9
n	$r = 1$	3	5	6	7	9	10	11	12	13
	$r = 2$	5	7	9	10	12	13	15	16	17

Из таблицы 1 следует, что в большинстве случаев неравенство (1) выполняется с запасом. Это свидетельствует о том, что исправление ошибок кратности до r часто не исчерпывает всех возможностей данного кода. При этом $N - N_p = 2^n - 2^k > N_p\lambda r$. Так, для вышеприведенного примера n = 9, k = 5, r = 1 код способен исправить $2^9 - 2^5 = 480$ ошибочно принятых кодовых комбинаций, в то время как количество однократных ошибок равно $2^5 - 9 = 288$. Следовательно, кроме однократных ошибок код способен исправить 480 – 288 = 122 кодовые комбинации, например, двукратных.

Реализация корректирующих способностей зависит от принципа построения кода [6]. Код, который полностью использует возможности по исправлению ошибок, называется оптимальным, причем оптимальность рассматривается в смысле полноты использования корректирующей способности при данном числе контрольных символов.

Для объяснения сущности процесса обнаружения и исправления ошибок при приеме кодовых комбинаций введем понятие кодового расстояния. Под кодовым расстоянием d_{ij} между двумя комбинациями понимают число идентичных позиций с несовпадающими символами. Например, расстояние между комбинациями A_1= 10111, A_2=01100 равно 4, так как они различаются символами в четырех позициях. Можно заметить, что кодовое расстояние равно числу единиц в сумме комбинаций по модулю 2^1. Так, для приведенных комбинаций имеем:

$$\begin{array}{r} \oplus\ 10111 \\ \underline{01100} \\ 11011 \end{array}$$

Понятию кодового (хэммингового) расстояния можно придать геометрический смысл [12].

Бинарный код представляет собой последовательность нулей и единиц, общее число которых равно значности кода n. Если в n-мерной системе координат по каждой оси отложить значение определенного разряда, то геометрической моделью бинарного n-разрядного кода будет n-мерный единичный куб. При этом каждая вершина куба представляет комбинацию, входящую в данный код.

На рисунке 2 для наглядности изображена геометрическая модель трехзначного кода. Из рисунка видно, что кодовое расстояние равно расстоянию, измеряемому вдоль ребер куба от одной вершины до другой. Например, кодовое расстояние между комбинациями $A_1 = 000$ и $A_6 = 101$ равно 2, так как при перемещении из A_1 в точку A_6 необходимо пройти вдоль двух ребер куба [7, 8]. Перейдем к пояснению процесса обнаружения и исправления ошибок.

Если для передачи сообщений используются все возможные для данного кода комбинации $N = N_p$, то минимальное кодовое расстояние между комбинациями равно 1 и обнаружение ошибок невозможно, так как при воздействии помех происходит транс-

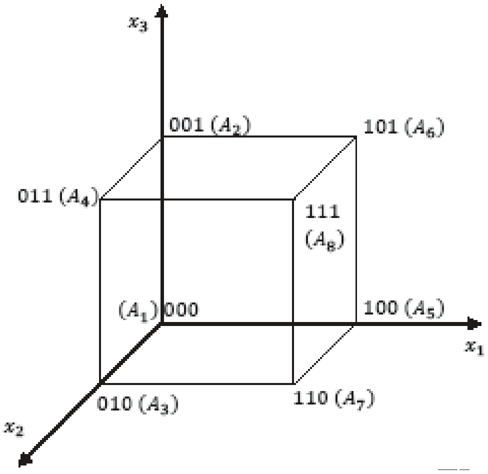

Рис. 2. Геометрическая модель кода

формация одной разрешенной комбинации в другую.

Пусть теперь минимальное расстояние между кодовыми комбинациями $d_{min} = 2$. Например, используются комбинации $A_1 = 000$, $A_4 = 011$, $A_6 = 101$, $A_7 = 110$. При воздействии помех, приводящих к однократной ошибке, расстояние между переданной комбинацией и любой другой из разрешенных изменится на единицу. Но при этом принятая комбинация преобразуется в запрещенную, и ошибка будет обнаружена. Таким образом, для обнаружения одиночных ошибок необходимо, чтобы $d_{min} \geq 2$. Это условие. реализуется, например, в коде с четной защитой. Принцип построения такого кода состоит в том, что к кодовым комбинациям обычного бинарного кода без избыточности добавляется один разряд. Знак этого разряда (1 или 0) выбирается так, чтобы сумма единиц во всех кодовых комбинациях была четной. Однократная ошибка при приеме кодовой комбинации нарушает четность числа единиц и легко обнаруживается с помощью простейшего счетчика числа единиц в комбинации. Кроме того, код с четной защитой способен обнаруживать все ошибки нечетной кратности.

Рассуждая аналогично, можно получить следующее соотношение между минимальным кодовым расстоянием d_{min} и кратностью обнаруживаемых ошибок:

$$d_{min} > r_{об} + 1.$$

Для исправления ошибок необходимо, чтобы кодовое расстояние между принятой ошибочно комбинацией и переданной было меньше, чем между принятой и любой другой разрешенной кодовой комбинацией. По этому правилу производится разбиение множества возможных комбинаций N на области E_i при приеме (рисунок 1). Для исправления одиночных ошибок область E_i должна содержать по крайней мере три комбинации, из которых одна разрешенная, а две других стоят от разрешенной по обе стороны на d = 1 и являются запрещенными [9].

Таким образом, минимальное кодовое расстояние для исправления одиночных ошибок должно быть не менее трех, а для ошибок кратности $r_и$:

$$d_{min} \geq 2r_и + 1.$$

Произведем оценку эффективности. использования корректирующих кодов для повышения помехоустойчивости систем передачи информации. Воспользуемся для этого формулой для вероятности r-кратных ошибок (2):

$$P_n(r) = C^r_n p^r (1 - p)^{n-r}. \qquad (2)$$

Если корректирующий код исправляет все ошибки кратности до r включительно, то вероятность безошибочного приема кодовой комбинации Q_r, состоящей из n элементов, будет выражаться суммой вероятностей ошибок с кратностью от 0 до r включительно:

$$Q_r = \sum_{i=0}^{r} c_n^i\, p^i\, (1 - p)^{n-i}.$$

Вероятность ошибочного приема Pr как событие противоположное будет равно:

$$P_r = 1 - \sum_{i=0}^{r} c_n^i\, p^i\, (1 - p)^{n-i}.$$

Повышение помехоустойчивости при использовании корректирующих кодов достигается за счет введения избыточности, которая определяется как разность между количеством элементов n в комбинациях данного кода и количеством информационных элементов k. Чаще употребляется понятие относительной избыточности:

$$R = \frac{n-k}{n} = 1 - \frac{k}{n}.$$

Введение избыточности при кодировании приводит к необходимости увеличения времени передачи одного сообщения, что влечет за собой увеличение энергии, необходимой для передачи сообщения. Но при увеличении длительности передачи уменьшается также вероятность ошибочного приема элемента комбинации при кодировании без избыточности. Поэтому при одинаковой скорости передачи информации вероятность ошибочного приема элемента обычно больше в коде с избыточностью [10]. В сряди с этим возникает вопрос о том, каким условиям должен удовлетворять код с избыточностью, чтобы его применение позволило повысить достоверность приема информации по сравнению с кодом без избыточности при том же времени передачи сообщения и одинаковой мощности сигнала.

Применение корректирующих кодов целесообразно в том случае, если выполняется неравенство:

$$r > \frac{n}{k} - 1,$$

где r – наибольшая кратность ошибок, полностью исправляемых данным кодом.

Для того чтобы повышение достоверности корректирующим кодом окупало усложнение кодирующей и декодирующей аппаратуры, знак неравенства необходимо усиливать.

[1] Сложение по модулю 2 производится по следующему правилу: 1 ⊕ 0 = 1, 1 ⊕ 1 = 0, 0 ⊕ 1 = 1, 0 ⊕ 0 = 0.

Литература

1. Борисов В.И., Зинчук В.М., Лимарев А.Е. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2000. 20 с.

2. Вернер М. Основы кодирования: Учебник для вузов: Пер. с нем. М.: Техносфера, 2004. 288 с.

3. Гриценко В.М., Недвоичные арифметические корректирующие коды, Проблемы передачи информации, 1969. С. 19 – 27.

4. Злотник Б.М. Помехоустойчивые коды в системах связи. М.: Радио и связь, 1989. 232 с.

5. Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник. М.: Горячая линия - Телеком, 2004. 126 с.

6. Ковалгин Ю.А., Вологдин Э. И. Цифровое кодирование звуковых сигналов. Издательство: Корона-Принт, 2004. 240 с.

7. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. М.: Наука, 2006.

8. Микропроцессорные кодеры и декодеры / В.М. Муттер, Г.А. Петров и др. М.: Радио и связь, 1991. 184 с.

9. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. 320 с.

10. Питерсон У. Коды, исправляющие ошибки, пер. с англ., М., 1964.

11. Пучков Ю.И., Корректирующий код с повторением [Международный журнал информационных технологий и энергоэффективности], Смоленск, 2020, 8 - 13 с.

12. Рыжов А.А., Гончаров С.Н., Одинцов М.В., Устройство формирования корректирующего кода [XIII всероссийской молодежной научно-инновационной школы], Саров, Издательство: Интерконтакт, 2019, 98-100 с.

References

1. Borisov V.I., Zinchuk V.M., Limarev A.Ye. i dr. Pomekhozashchishchen-nost' sistem radiosvyazi s rasshireniyem spektra signalov metodom psevdo-sluchaynoy perestroyki rabochey chastoty. M.: Radio i svyaz', 2000. 20 s.

2. Verner M. Osnovy kodirovaniya: Uchebnik dlya vuzov: Per. s nem. M.: Tekhnosfera, 2004. 288 s.

3. Gritsenko V.M., Nedvoichnyye arifmeticheskiye korrektiruyushchiye kody, Problemy peredachi informatsii, 1969. S. 19 – 27.

4. Zlotnik B.M. Pomekhoustoychivyye kody v sistemakh svyazi. M.: Radio i svyaz', 1989. 232 c. 5. Zolotarev V.V., Ovechkin G.V. Pomekhoustoychivoye kodirovaniye. Me-tody i algoritmy: Spravochnik. M.: Goryachaya liniya - Telekom, 2004. 126 s.

6. Kovalgin YU.A., Vologdin E. I. Tsifrovoye kodirovaniye zvukovykh signalov. Izdatel'stvo: Korona-Print, 2004. 240 s.

7. Kolesnik V.D., Poltyrev G.SH. Kurs teorii informatsii. M.: Nauka, 2006.

8. Mikroprotsessornyye kodery i dekodery / V.M. Mutter, G.A. Petrov i dr. M.: Radio i svyaz', 1991. 184 s.

9. Morelos-Saragosa R. Iskusstvo pomekhoustoychivogo kodirovaniya. Metody, algoritmy, primeneniye. M.: Tekhnosfera, 2005. 320 s.

10. Piterson U. Kody, ispravlyayushchiye oshibki, per. s angl., M., 1964.

11. Puchkov YU.I., Korrektiruyushchiy kod s povtoreniyem [Mezhdunarod-nyy zhurnal informatsionnykh tekhnologiy i energoeffektivnosti], Smo-lensk, 2020, 8 - 13 s.

12. Ryzhov A.A., Goncharov S.N., Odintsov M.V., Ustroystvo formiro-vaniya korrektiruyushchego koda [XIII vserossiyskoy molodezhnoy nauchno-innovatsionnoy shkoly], Carov, Izdatel'stvo: Interkontakt, 2019, 98 - 100 s.

ПЕТУХОВ Александр Георгиевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: putnik0879@mail.ru

PETUKHOV Alexander Georgievich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: putnik0879@mail.ru

СТЕПАНЦОВА Алёна Михайловна, студентка, «Сибирский государственный университет телекоммуникации и информатики». Россия, 630102, Сибирский федеральный округ, Новосибирская область, г. Новосибирск, ул. Кирова, д. 86. E-mail: alena169vega@yandex.ru

STEPANCOVA Aljona Mihajlovna, student, "Siberian State University of Telecommunications and Informatics". Russia, 630102, Siberian Federal District, Novosibirsk region, Novosibirsk, Kirova str., 86. E-mail: alena169vega@yandex.ru

ДЕЛОГ Андрей Николаевич, инженер, войсковая часть 15644. Россия, 416540, Астраханская обл., г. Знаменск. E-mail: delog_mga@mail.ru

DELOG Andrey Nikolaevich, engineer, military unit 15644. Russia, 416540, Astrakhan region, Znamensk. E-mail: delog_mga@mail.ru