

МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ КОДОВ ХЭММИНГА В ЦИФРОВЫХ СЕТЯХ СВЯЗИ

Тукубаев З.Б.

(Международный Казахско-Турецкий университет имени
Ясауи, г.Туркестан, Казахстан)
zuhr@pochta.ru, zuhr08@rambler.ru

*В статье исследуются возможности применения кодов
Хэмминга в цифровых сетях связи.*

*In the article it is done research of usage possibility of Hamming
codes in digital networks.*

Ключевые слова: методы повышения достоверности передачи
данных, коэффициент верности передачи данных, циклические
коды, образующий полином, корректирующие коды, синдром
ошибок.

Достоверность каналов передачи данных используемых в
компьютерных сетях по требованию стандартов не должна
быть ниже $10^{-6} \div 10^{-8}$ ошибок на дв. символ [1]. Многие
реальные каналы передачи данных не отвечают требованиям
стандартов без применения методов повышения достоверности
(МПД). При этом, в зависимости от типа сетей передачи
данных, используемых каналов связи и от типа передаваемой
информации используются различные МПД.

В настоящей статье делается анализ МПД применяемых в
современных системах и сетях передачи данных, предлагаются
методы повышения эффективности кодов Хэмминга и
возможности использования его для передачи текстовой
информации.

В компьютерных сетях при применении протоколов X.25 и ISDN
сообщения передаются следующим образом: в поле
информации одного кадра уровня 2 располагается один пакет
уровня 3. Стандартизованы 2 формата для пакетов различного
назначения; при этом, форматы пакетов имеют такую



структуру: первые три октета предназначены для главного идентификатора формата, номеров групп логических каналов и логического канала, номеров пакета и подтверждаемого пакета. Форматы пакетов могут быть: 16, 32, 64, 128, 256, 512, 1024 байт. Далее идут абонентские данные. Стандартизованы следующие скорости передачи данных: 2400, 4800, 9600, ..., 48000 бит/с. В стандарте X.75 и в рекомендации G.703 предусмотрена скорость 64Кбит/с. В стандарте ITU-T скорости передачи доведены до 2096Мбит/с. Структура кадра стандартизована в ISO 3309, где кадр состоит из следующих полей: открывающий флажок -1 байт, адресное поле -1 байт, поле управления -1 байт, контрольная последовательность (CRC)- 2 байта, закрывающий флажок- 1 байт.

В стандарте CCITT серии V.41 используется сочетание циклического кода и решающей обратной связи; при этом, образующий полином имеет вид $g(x) = x^{16} + x^{12} + x^5 + 1$.

Длина блоков данных: 240, 500, 960 и 3860 бит. Из них 20 бит служебные; 16 – проверочные, 4 бит – служебные.

Протоколы транспортного уровня (протоколы TCP и UDP) допускают, что поле данных IP- пакета имеет максимальный размер 65536 байт. Но в других сетях максимальная единица транспортировки (Maximum Transfer Unit - MTU) гораздо меньше; например, в сети Ethernet -1500 байт, в сети FDDI - 4096 байт, в сети X.25 -128 байт. При прохождении пакета от одной сети в другую с разными MTU производится фрагментация в хостах или в маршрутизаторах. При фрагментации поле смещения показывает номера новых пакетов после фрагментации. В стандартных пакетах 20 байт отводится на заголовок. IP- маршрутизаторы производят дефрагментацию пакетов; она производится в конечном пункте. При этом, если один из пакетов не укладывается в допустимое время, то все пакеты стираются. Сообщение об ошибке при помощи протокола ICMP [2, 1].

Обнаружение ошибок и запрос повторения передачи пакета выполняется по-разному; в одних сетях на уровне каналов (канальный уровень), а в других – на уровне транспортного, в зависимости от типа сообщения. В соответствии со стандартом



1 IEEE 802.2 уровень управления логическим каналом LLC
2 представляет три типа процедур; LLC1- процедуру без
3 установления соединения и без подтверждения; LLC2 –
4 процедуру с установлением соединения и с подтверждением;
5 LLC3- процедуру без установления соединения, но с
6 подтверждением. При использовании протокола LLC1 для
7 передачи данных потребуется минимальное время задержек;
8 при этом, коррекция ошибок и упорядочение данных
9 выполняется протоколами вышестоящих уровней, т.е. на
10 транспортном уровне на оконечном узле. В стеке протоколов
11 TCP/IP уровень LLC всегда работает в режиме LLC1;
12 выполняет только извлечение из кадра, демультимплексирования
13 пакетов различных протоколов. LLC2 работает в режиме
14 скользящего окна. Процедуры восстановления после ошибок и
15 упорядочения потока блоков данных производятся в рамках
16 установленного соединения на канальном уровне. В LLC2
17 логический канал является дуплексным; положительные
18 квитанции на кадры доставляются в информационных кадрах
19 обратного канала. Если по такому протоколу реализуется
20 телефонный разговор, то максимальная задержка зависит от
21 максимального размера скользящего окна и скорости передачи
22 данных; стандартный размер окна в LLC2 равен 127 кадров. В
23 вышеотмеченных протоколах LLC2, LLC3 для обнаружения
24 ошибок данных используются циклические коды; а
25 исправление пакетов с ошибками производится путем
26 повторения их передач.

27 Широко используемые на практике радиоканалы дециметрового
28 и ультракоротковолнового диапазонов волн (ДКМ и УКВ)
29 имеют низкую достоверность (вероятность ошибки $\approx 10^{-2} \div 10^{-3}$), что делает неэффективным их использование в
30 сетях с пакетной коммутацией. Но эти каналы используются в
31 быстродействующих аппаратах автоматического
32 буквопечатания “Сокол -MP”, “СТР-114”, “СТБ-750”
33 фирмы “Philips”, которые широко используются в морской
34 подвижной службе (МПС) и военно-морских силах (ВМС [1, 4
35]. Аппаратуры “Сокол -MP”, “СТР-114” не имеют кодовую
36 избыточность и работают на основе стандарта МТК-2, где
37



обнаружение ошибок производится на основе анализа огибающей двоичных сигналов при помощи контрольного импульса. Исследования помехоустойчивости поэлементных способов контроля качества сигналов проведенные автором [3] показывают, что 1- элементы кодовой комбинации не имеют краевое искажение из-за коррекции сигналов в начале кодовой комбинации. В ионосферных каналах ошибки возникают, в основном, из-за краевых искажений вызываемых флуктуациями сигналов замирования. А ошибки вызываемые дроблениями кодовых посылок сигналов ничтожно малы по сравнению с ошибками из-за краевого искажения. Исправление ошибок производится путем запроса и повторения передач ошибочного знака.

А в специальных системах передачи данных обратный канал не используется по определенным причинам; например, для обеспечения высокой скрытности удаленных абонентов или же невозможности использования обратного канала в системах автоматики. В таких случаях целесообразно использование кодов с обнаружением и исправлением ошибок. В системах автоматики и телемеханики широко используются коды Хэмминга; например, код Хэмминга (7,4). Этот код имеет всего 4 информационного символа. В стандарте ISO-963 установлены правила образования 16 4-битных знаков из набора 7-битной таблицы ISO646. Такие символы используются в некоторых многотерминальных системах [1,5,6]. Но этот код невозможно использовать для передачи текстовых сообщений. С другой стороны, коды Хэмминга относятся к совершенным групповым кодам, которые обладают следующими замечательными свойствами;

- простота аппаратных реализации; состоит из одного сдвига с обратными связями;
- возможность оптимизации и нахождения кодов близких к оптимальным;
- возможность построения для них сравнительно простых алгоритмов и схем декодирования, реализуемых при помощи несложных устройств. Кроме этих достоинств групповые коды обладают следующими замечательными свойствами.



замкнутостью, ассоциативностью, обратимостью и наличием нулевого слова.

Семейство кодов (n, k) для которых выполняется условие:

$(2^p - 1, 2^p - 1 - p)$, где $p = n - k$, называется кодами Хэмминга

(КХ). Существуют следующие КХ:

$(7, 4), (15, 11), (31, 26), (63, 57), \dots$ КХ обладают следующими

замечательными свойствами:

1) Выполняется условие: $2^{n-k} = 1 + n$;

2) Полностью известен спектр; весовая функция

$A(x) = \sum_{i=0}^n A_i x^i$, где A_i - число кодовых слов с весами - i .

В статье предлагается следующие усовершенствования КХ;

1) КХ с $d = 3$ можно превратить в КХ с $d = 4$, т.е. КХ

$(8, 4)$:

Допустим, что для КХ $(7, 4)$ проверочная матрица задана в виде

$$H = \begin{pmatrix} 1110 & 100 \\ 1101 & 010 \\ 1011 & 001 \\ 1111 & 111 \end{pmatrix}.$$

Суммируя элементы строки по mod2 образуются дополнительно 8- элементы (8-столбец матрицы H_1).

$$H_1 = \begin{pmatrix} 1110 & 1000 \\ 1101 & 0100 \\ 1011 & 0010 \\ 1111 & 1111 \end{pmatrix}$$

Затем, последнюю строку заменяем суммой всех строк и получаем каноническую форму H_2 :

$$H_2 = \begin{pmatrix} 1110 & 1000 \\ 1101 & 0100 \\ 1011 & 0010 \\ 0111 & 0001 \end{pmatrix}$$



Такой код обнаруживает все нечетные ошибки. Избыточность кода равна 100%. Хотя обнаруживающая и исправляющая способности увеличиваются, информационные символы не хватает для кодирования букв даже английского алфавита (в английском алфавите 26 букв).

2) Для передачи букв английского и русского языков достаточно применить пятиэлементный стандарт МТК-2, образуя его из 8-элементного кода МТК-5 или ASCII. При этом, $1 \div 5$ элементы можно использовать как информационные, а остальные $6 \div 8$ элементы - как проверочные; поскольку в КХ(7,4) проверочные элементы 3, то информационные не должны превышать 4. Один информационный элемент остается незакодированным. Таким элементом предлагается первый элемент кодовой комбинаций, где отсутствуют краевые искажения. Алгоритм имеет вид; в передаче используются следующие двоичные символы: $b_1, b_2, b_3, b_4, b_5, \epsilon_{6np}, \epsilon_{7np}, \epsilon_{8np}$,

где b_1, b_2, b_3, b_4, b_5 -информационные, а $\epsilon_{6np}, \epsilon_{7np}, \epsilon_{8np}$ - проверочные символы. Последние образуются следующим образом: $\epsilon_{6np} = b_2 \oplus b_4 \oplus b_5$, $\epsilon_{7np} = b_3 \oplus b_4 \oplus b_5$, $\epsilon_{8np} = b_2 \oplus b_3 \oplus b_4$. На приемной стороне те же элементы

обозначены со штрихами: $b'_1, b'_2, b'_3, b'_4, b'_5, \epsilon'_{6np}, \epsilon'_{7np}, \epsilon'_{8np}$. На выходе проверочные символы определяются по тому же алгоритму: $\epsilon'^{\kappa}_{6np} = b'_2 \oplus b'_4 \oplus b'_5$, $\epsilon'^{\kappa}_{7np} = b'_3 \oplus b'_4 \oplus b'_5$, $\epsilon'^{\kappa}_{8np} = b'_2 \oplus b'_3 \oplus b'_4$.

Синдромы ошибок определяются таким образом:

$$C_1 = \epsilon_{6np} \oplus \epsilon'^{\kappa}_{6np}, \quad C_2 = \epsilon_{7np} \oplus \epsilon'^{\kappa}_{7np},$$

$$C_3 = \epsilon_{8np} \oplus \epsilon'^{\kappa}_{8np}. \quad \text{Далее, по значениям синдромов}$$

определяются номера разрядов с ошибками по таблице. В третьем столбце таблицы показаны номера позиции исправляемых ошибок. При этом, ошибки в первом разряде не исправляются, но обнаруживаются. Алгоритм исправления



ошибок следующие; Ошибка O_2 в разряде b_2' исправляется таким образом:

$$O_2 = b_2' \oplus (C_1 \cap C_3); O_3 = b_3' \oplus (C_2 \cap C_3);$$

$$O_4 = b_4' \oplus (C_1 \cap C_2 \cap C_3); O_5 = b_5' \oplus (C_1 \cap C_2).$$

В проверочных разрядах ошибки также исправляются таким образом; $O_6 = b_{6np}' \oplus (\overline{C_2 \cap C_3})$;

$$O_7 = b_{7np}' \oplus (\overline{C_1 \cap C_3}); O_8 = b_{8np}' \oplus (\overline{C_1 \cap C_2}).$$

В логических схемах используются операции: $\cup$ -дизъюнкция,

$\cap$ -конъюнкция, $\overline{}$ -отрицание

и $\oplus$ -сложение по модулю два.

Таблица № 1. Синдромов и векторов ошибок.

Номера разрядов в кода	Синдромы $C_3 C_2 C_1$			Вектор ошибки $O_i, i = 2 \div 8$
1	0	0	0	---- (соотв. 1-разряду)
2	0	0	1	6 - разряд
3	0	1	0	7 - разряд
4	0	1	1	5 - разряд
5	1	0	0	8 - разряд
6	1	0	1	2 - разряд
7	1	1	0	3 - разряд
8	1	1	1	4 - разряд

Выводы:

В современных цифровых сетях связи используются различные методы и алгоритмы повышения достоверности передачи данных. Для наибольшего повышения эффективности передачи в системе передачи данных используются несколько методов одновременно.

а.). В сетях с пакетной коммутацией при использовании протоколов LLC2, LLC3 в локальных сетях и протоколов TCP используются циклические полиномиальные коды для



обнаружения искаженных пакетов, а исправление производится путем повторения их передач. Использование в таком сочетании двух методов при оптимальной длине пакетов даст максимальную информационную скорость передачи данных.

б). В системах без обратной связи используются корректирующие коды. Среди них наиболее совершенным являются коды Хэмминга: КХ (7,4), КХ(15,11) и другие. Но они не приспособлены для передачи текстовой информации; в КХ (7,4) не хватает символов для полного алфавита текста, а КХ(15,11) обладает чрезмерно большой избыточностью (~114%) даже при использовании стандартов МТК-5 и ASCII.

Усовершенствование этих кодов дает следующие возможности; - построение- КХ (8,4) дает возможность увеличить обнаруживающую способность кода с $d = 3$ в КХ с $d = 4$ при некотором увеличении избыточности с 75% на 100%. Но, при этом, не удастся использовать его для передачи текстовой информации.

- предложенный автором КХ (8,5) можно использовать для передачи текстов при использовании стандарта МТК-2. При этом, избыточность составляет ~60%.

Л и т е р а т у р а

1. СТАНДАРТЫ И РЕКОМЕНДАЦИИ В ОБЛАСТИ ТЕЛЕОБРАБОТКИ ДАННЫХ.

Методические материалы и документация по пакетам прикладных программ, вып.11, справочник, ч.1,- М.: 1998 г.

2. СЕТИ TCP/IP. Ресурсы Microsoft Windows 2000. - М.: 2001.
3. ТУКУБАЕВ З.Б. "Исследование и внедрение методов элементных способов контроля качества сигналов ЭВМ". Кандидатская диссертация, г.Ташкент, 1978 г.
4. ВЕНСКАУСКАС К.К. Системы средств связи в МПС. Справочник, -Л.: "Судостроение", 1986. - 432 с.
5. ГЛУШКОВ В.М. и др. Сети ЭВМ. - М.: "Связь", 1977 г.



- 1 6. ЗЛОТНИК Б.М. *Помехоустойчивые коды в системах*
2 *связи*. Вып.31, -М.: “Радио и связь”, 1989 г. -232 с.
3

