Методы структурной, информационной и временной избыточности в ИВС

Основные цели применения

- обеспечение **качества и надежности ИВС (программных, аппаратных, аппар-прогр средств)** - организация работ на основе международных стандартов серии **ISO 9000** или *TQM (Total Quality Management)* - Международная организация по стандартизации (*International Standard Organization, ISO*)
- **используемые методы**

  1) *увеличение наработки*, 2) *снижение интенсивности отказов*, 3) *улучшение восстанавливаемости*, 4) *резервирование* - третью и четвертую группы можно объединить под единым названием – ***избыточных методов***
- **различают:** ***структурную, временную, информационную избыточность*** (redundancy) либо их комбинации

- системы с **временной избыточностью** – **системы с повторениями (**передачи)

Классика: Реализуется введением в структуру ТС накопительного звена, позволяющего в течение определенного времени выполнять основную функцию при отказе элемента за накопительным звеном. Если избыточное время будет выше времени восстановления отказавшего элемента, то функция по назначению будет выполняться непрерывно и даже при отказе.

- **информационная избыточность –** обусловливает возможность применения функций **сжатия информации**

Информ избыточность сообщений *R* определяется по формуле

$$R = 1 - H / \log_2 k \,, \qquad (1)$$

где *k* — число букв алфавита, а *H* — *энтропия* источника на букву сообщения

- **Комбинированные методы - на основе использования специальных кодов (избыточных кодов или помехоустойчивых кодов)**

МЕТОДЫ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ДАННЫХ

Классификация кодов

- **Блочные коды** —каждому сообщению из **k** (X_k)символов (бит) сопоставляется блок из **n** символов (кодовый вектор X_n длиной **n=k + r**).
- **Непрерывные (рекуррентные**, **цепные**, **свёрточные**) **коды -**непрерывная последовательность символов, не разделяемая на блоки. Передаваемая последовательность образуется путём размещения в определённом порядке проверочных символов между информационными символами исходной послед-ти.
- **Систематические коды** характеризуются тем, что сумма по модулю 2 двух разрешённых кодовых комбинаций кодов снова даёт разрешённую кодовую комбинацию.

Проверочные символы вычисляются как линейная комбинация информационных, откуда и возникло другое наименование этих кодов — **линейные**. Для кодов принимается обозначение [**n,k**] - **код,**

- **Несистематические коды** не обладают отмеченными выше свойствами (к ним относятся итеративные коды).
  4
- ***Циклические коды*** *– относятся к линейным систематическим.*

Основное свойство, давшее им название, состоит в том, что каждый вектор, получаемый из исходного кодового вектора путём циклической перестановки его символов, также является разрешённым кодовым вектором. Принято описывать циклические коды при помощи **порождающих полиномов G(X)** степени **r**

Среди ЦК особое место занимает класс кодов, предложенных Боузом и Чоудхури и независимо от них Хоквингемом. Коды Боуза-Чоудхури-Хоквингема получили сокращённое наименование **БЧХ- коды : CRC-32 (CRC-16).**

БЧХ- коды являются обобщением **кодов Хемминга** на случай исправления нескольких независимых ошибок ($t_и$ **>1**).

Основные понятия

- **Определение 1**. Сообщение $\mathbf{X_k}$ (**k** – длина сообщения, *символов* или *бит*), называется ***информационным словом***.
- **Определение 2**. Избыточные символы длиной **r** символов (бит) составляющие ***избыточное слово*** $\mathbf{X_r}$.
- **Определение 3.** *Слово* $\mathbf{X_n}$ длиной **n=k+r** символов $\mathbf{X_n = X_k\, X_r}$

называется ***кодовым словом*.**

Информацию содержит только информационное слово. Назначение избыточности X_r – обнаружение и исправление ошибок.

- **Определение 4.** ***Вес по Хеммингу*** произвольного двоичного слова **X** (**w(X)**) равен количеству ненулевых символов в слове.

Пример 1. X=1101. Тогда w(X=1101) = 3.

- **Определение 5.** ***Расстояние*** **по Хеммингу** или кодовое расстояние (**d**) между двумя произвольными словами (**X,Y**) одинаковой длины равно количеству позиций, в которых **X** и **Y** отличаются между собой.

Кодовое расстояние можно вычислить как вес от суммы по модулю 2 этих двух слов: $\mathbf{d(X,Y) = w(X \oplus Y)}$.

Пример 2. X=101,Y=111). Очевидно, что d(X,Y) = 1.

Пример 3. X=1011, Y=0000; d(X,Y)=3:

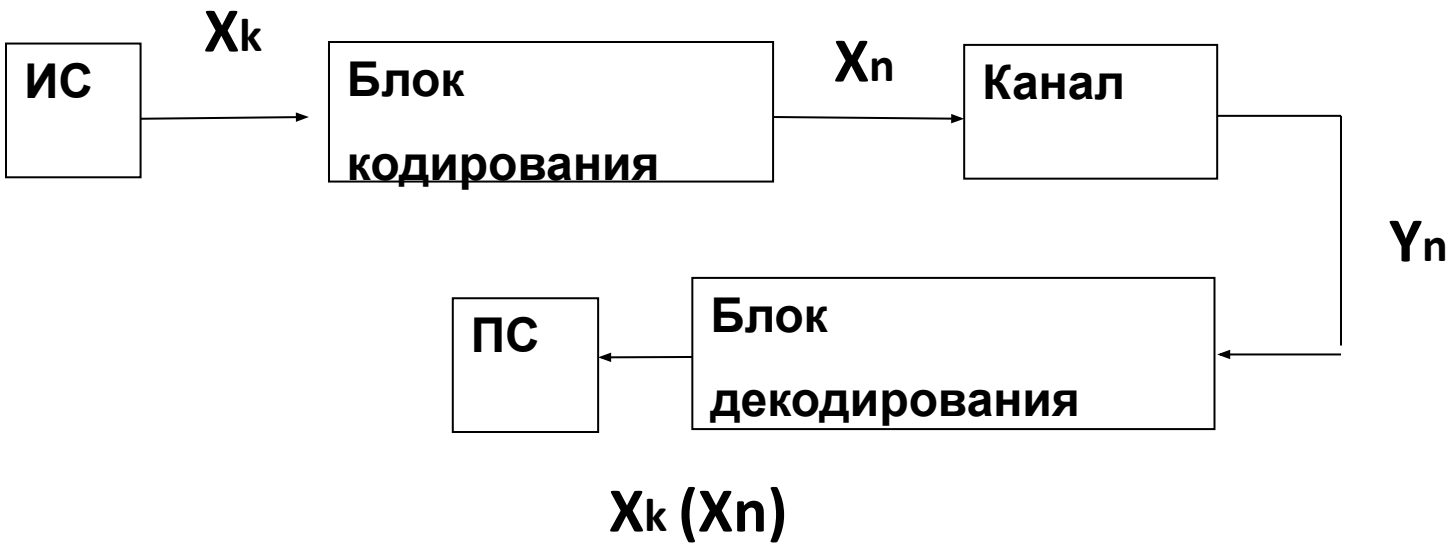

Рис.1.

где $X_n = y_1, y_2, \ldots, y_n$; $Y_n = y_1, y_2, \ldots, y_n$.

Теоретические основы линейных блочных кодов

- Для формирования проверочных символов (**Xr**) используется ***порождающая матрица***: совокупность базисных векторов будем записывать в виде матрицы **G** размерностью ***k*** x ***n*** с единичной подматрицей (***I)*** в первых ***k*** строках и столбцах:

$$G = [\, P \mid I \,] \qquad (2)$$

- Кодовые слова являются линейными комбинациями строк матрицы ***G*** (кроме слова, состоящего из нулевых символов).
- Кодирование заключается в умножении вектора сообщения X_k длиной ***k*** на **G** по правилам матричного умножения (все операции выполняются по модулю два);

при этом последние ***r*** символов (**Xr**) образуются как линейные комбинации первых (X_k **)**

- Для всякой порождающей матрицы ***G*** существует матрица ***H*** размерности ***r*** x ***n***, удовлетворяющая равенству

$$G * H^T = 0 \quad (3)$$

- Матрица **H** называется ***проверочной*** и записывается как

$$H = [P^T | I] \quad (4)$$

Определение 6. Результат умножения вектора сообщения (Y_n) на транспонированную проверочную матрицу (***H***) называется ***синдромом*** (вектором ошибки) ***S***:

$$S = H^T * Y_n = H * (Y_n)^T \quad (5)$$

Если **S=0** (все **r** символов синдрома – нулевые) – в принятом сообщ ошибок нет; в противном случае - $t_и > 1$.

Определение 7. ***Проверочным (избыточным) словом*** X_r кодового слова X_n является вектор-строка, удовлетворяющая тождеству:

$$H^T * X_n = H * (X_n)^T = 0 \quad (6)$$

Определение 8. **n-разрядным вектором ошибки** называем последовательность вида:

$$E_n = X_n + Y_n \qquad (7)$$

В (6) суммирование – по мод 2

Определение 9. **Корректирующие способности кода** определяются исключительно **минимальным кодовым расстоянием** (d_{min}) между двумя произвольными кодовыми словами, принадлежащими коду:

$$tu = \begin{cases} \dfrac{d-1}{2}, & d - нечетное, \\ \dfrac{d-2}{2}, & d - четное. \end{cases} \qquad (8)$$

***to* = d/2** , **d -** четное

to = (d-1)/2 , d - нечетное (9)

Алгоритм использования КК

На стороне **ИС**

1. Построить проверочную матрицу $\mathbf{H}_{n,k}$ для заданного **k** ($\mathbf{X}_k$)
2. Вычислить символы избыточного слова $\mathbf{X}_r$ (на основе (6))
3. Сформировать кодовое слово $\mathbf{X}_n = \mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_k,\mathbf{x}_{k+1},\ldots\mathbf{x}_{k+r}$ и осуществить его передачу

На стороне **ПС**

1. Получение сообщения ($\mathbf{Y}_n = \mathbf{y}_1,\mathbf{y}_2,\ldots,\mathbf{y}_k,\mathbf{y}_{k+1},\ldots\mathbf{y}_{k+r}$)
2. Вычисление синдрома (на основе (5)), используя ту же $\mathbf{H}_{n,k}$:

$$S = H^T * Y_n = H * (Y_n)^T = H^T * (X_n + E_n) = H^T * X_n + H^T * E_n = H^T * E_n$$

(10)

для этого вычисляем $\mathbf{Y}_r' = \mathbf{y}_{ri}'$: $y_{ri}' = y_{k+i}' = \Sigma\, h_{ij} * y_j$

(11)

и далее: $S = s_1,s_2,\ldots s_r$, где $s_i = y_{k+i} + y_{ri}'$ →

(12)

Теорема 1. **Минимальное кодовое расстояние линейного кода равно минимальному весу ненулевых кодовых слов**

- $R_и = r/k$ — **относительная избыточность кода**
- $R_c = k/n$ - **скорость кода**
- **Выбор кода** определяется вероятностью ошибки в канале, **p** (чем больше **p,** тем с большим **d** , т.е. с большим **r** следует выбирать код, однако это снижает R_c)

Определение 10. Пропускная способность ДСК с вероятностью ошибки p равна

$$C(p) = 1 - p \log_2 p + q \log_2 q \qquad (14)$$

Теорема 2 (Шеннона). **Для любого ДСК и любого ε >0 существует (n,k)- двоичный код со скоростью R_c, если $R_c < C(p)$, n достаточно велико и $p < ε$.**

ОСНОВНАЯ ПРОБЛЕМА ТЕОРИИ КОДИРОВАНИЯ:

Избыточный код простой четности

- Простейший избыточный код;
- Основан на контроле четности (либо нечетности) единичных символов в сообщении.
- Количество избыточных символов **r** всегда равно **1** и не зависит от **k**.
- Значение этого символа будет **нулевым**, если сумма всех символов кодового слова по модулю 2 равна нулю – при контроле четности.

Пример 4. Пусть X_k **= 1010**

Построить проверочную матрицу **H** кода и вычислить значение проверочного символа.

Код Хемминга

- код характеризуется минимальным кодовым расстоянием $d_{min}=3$,

используется расширенный контроль четности групп символов информационного слова,

- вес столбцов подматрицы **P** (см (4)) должен быть больше либо равен **2**,
- позволяет не только обнаруживать, но и исправлять одиночную ошибку в кодовом слове ($t_o=1$, $t_и=1$),
- параметры кода: $n = 2^r - 1$

$$k = 2^r - r - 1 \qquad (14)$$

- Для упрощенного вычисления **r** можно воспользоваться следующим простым соотношением:

$$r = \log_2 k + 1 \qquad (15)$$

Пример 5. Построить матрицу **H**, если $X_n = 010110$