

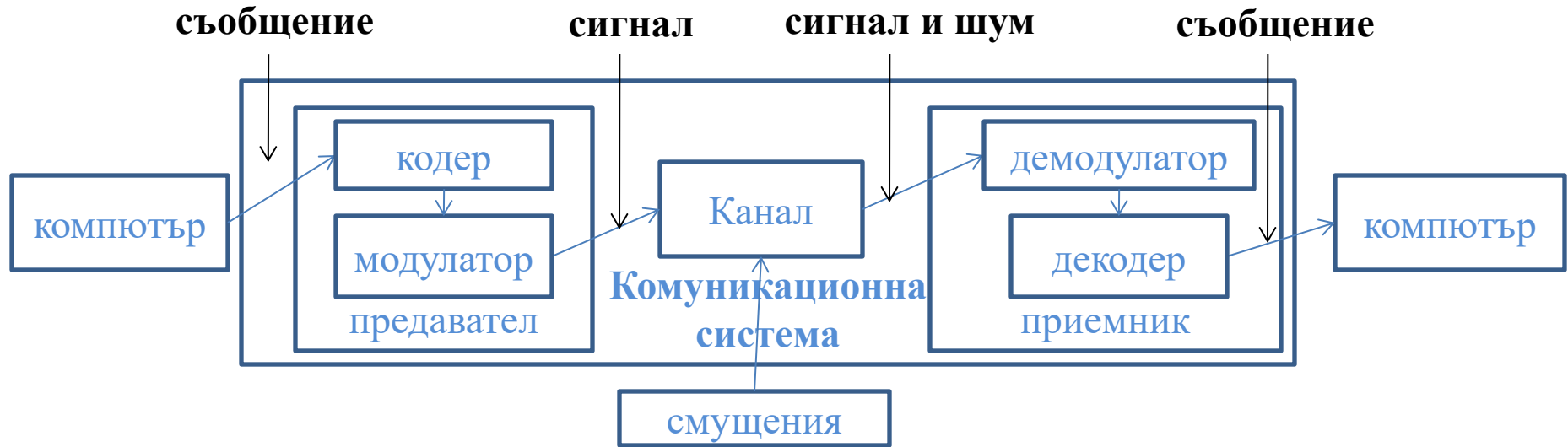
Кодиране на информацията.
Равномерно и неравномерно
кодиране. Кодове на Шенон -
Фано и Хафмън. Шумоустойчиво
кодиране. Циклични кодове.

доц. д-р инж. Айдын Хъкъ

ОСНОВНИ МОМЕНТИ

- Кодиране на информацията. Същност.
- Термини.
- Предназначение.
- Равномерно и неравномерно кодиране.
- Код на Шенон – Фано.
- Код на Хафмън.
- Шумоустойчиво кодиране.
- Циклични кодове.

Кодиране



- **Кодиране на информацията** е процес на преобразуване на съобщенията в сигнали.
- **Код** - алгоритъмът, по който съобщенията се превръщат в комбинация от различни сигнали. Това е система за пълно и точно съответствие между съобщенията и сигналите.

Предназначение на кодирането

- Повишаване верността чрез **откриване и коригиране** на появилите се грешки в отделни разреди на предаваната информация:
 - От затихване на сигнала
 - От завишаване на нивото на сигнала от шум
- Грешките имат случаен характер и се измерват с вероятност:
 $q = P(1/0)$ е вероятността да е изпратена 1, но да се интерпретира в получателя като 0
 $q = P(0/1)$ е вероятността да е изпратена 0, но да се интерпретира в получателя като 1

Възникване на грешки при предаване

- В компютърните комуникации се използват устройства, които са достижения на високи технологии, приложени в микроелектрониката.
- В резултат на това вероятността за възникване на грешки в комуникационните канали на компютърните мрежи за по-малко от 10г. се промени от $1 \cdot 10^{-1}$ до $1 \cdot 10^{-24}$.
- При такава малка вероятност за грешка се обезсмисля кодирането на съобщенията със сложни кодове за откриване и коригиране на грешки.

Решение без кодиране

- В стандартите за компютърните комуникации е заложено използване на циклични кодове за откриване на грешки, като процедурата за коригиране на грешките в комуникационните канали не е приложена.
- Обикновено когато при предаване на съобщения се открият грешки, **некоректните фрагменти на съобщението се унищожават.**
- Приемащото устройство, открило грешката, **връща на предаващото отрицателна квитанция**, която се възприема като заявка до източника да предаде отново в мрежата изкривените фрагменти на съобщението.
- Процедурата на повторения по подразбиране е ограничена до определено ниво, след което, ако се открие грешка, се счита, че комуникационният канал е загубил способността си за предаване на данни.

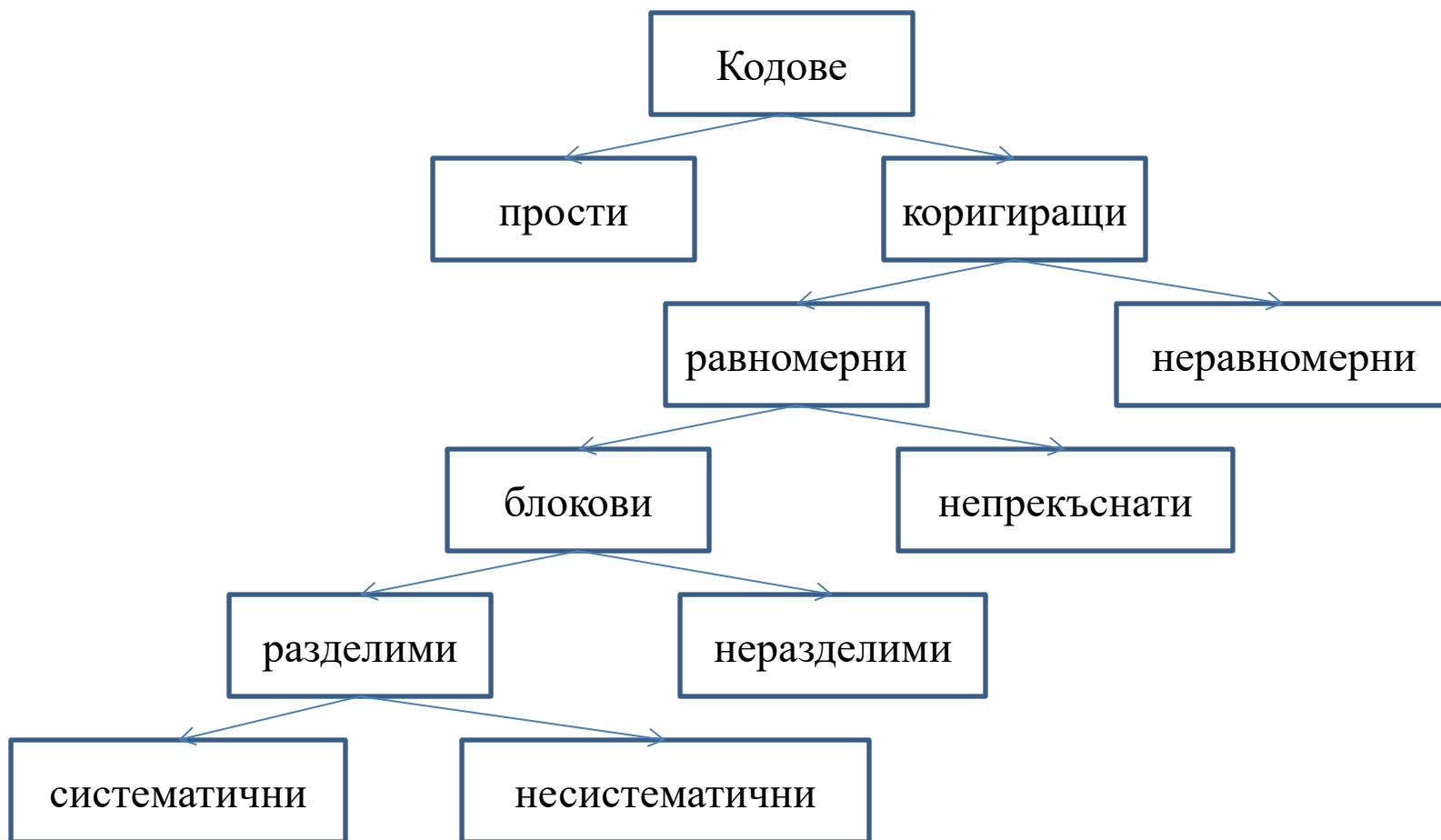
Теория на кодирането

- Тя е раздел от теорията на информацията, изучаваща кодовете, представени във вид на думи от символи на дадена азбука.
- Кодирането се извършва, за да се даде възможност за предаване на информацията по комуникационен канал при изпълнение на предварително зададени изисквания и за избор на най-добрите варианти, свързани с характеристиката на процеса на предаване на информацията: скорост, шумозащитеност и др.

Термини

- Кодът е набор от **кодови комбинации** $x_n, x_{n-1}, \dots, x_2, x_1$, като всяка кодова комбинация x_i е съчетание от елементарни символи, които изразяват буква, цифра или знак.
- **Дължината на кодовата комбинация** се определя от броя на елементарните символи в нея.
- **Кодова дума** - последователността от символи, която в процеса на кодиране се присвоява на всяко множество предадени съобщения.
- **Символ (разряд на кода)**- Двоичната цифра 0 или 1.
- Продължителността на един символ се нарича **единичен интервал** – t_0 .
- При предаването на дискретни съобщения, каквито са компютърните комуникации, основно приложение са намерили **двоичните кодове**.

Класификация на кодовете



Класификация на кодовете

- **Прости (нешумоустойчиви)** – без информационен излишък, отделните кодови комбинации се различават само по 1 разред. При грешка се получава валидна комбинация и грешката не може да бъде открита.
- **Коригиращи (шумоустойчиви)** – освен използваните кодови комбинации, които се различават с ≥ 2 разреда, има и забранени. При поява на забранена комбинация значи, че има грешка.

Блокови кодове

- **Неразделими** – малък брой, например телеграфен код с постоянно тегло
- **Разделими - (n,k) кодове** – n е общия брой разреди, k е броят на информационните разреди, $(n-k)$ са контролните разреди, всички комбинации са 2^n , разрешените са 2^k , излишество на кода е $(n-k)/n$
 - **Систематични** – контролните разреди са сума по модул 2 от информационните, например **код на Хеминг и циклични кодове** или кодове с проверка по четност и нечетност, код с повторение, корелационен код, инверсен код, кодове на Голей, Рид – Малер, Макдоналд, Варшамов и интерактивен код
 - **Несистематични** – не се ползват

Кодово разстояние

- **Кодово разстояние d** - минималният брой позиции, с които символите от една комбинация на даден код се отличават от символите на друга комбинация.
 - При прости кодове $d=1$
 - При коригиращи кодове $d>1$
- **Хемингово разстояние d_0** - Най-малкото от кодовите разстояния в даден код.
- В повечето кодове (код на Хеминг, циклични кодове) кодовото разстояние е еднакво за всички кодови комбинации: $d = d_0$
- **Пример:**

Ако кодовите комбинации са: 10101 и 11111, $d=2$.

Откриване и изправяне на грешки

- Броят на откриваните грешки (σ) се определя от:
 $d_0 \geq \sigma + 1$
- Броят на коригираните грешки (t) се определя от:
 $d_0 \geq 2t + 1$
- За да се открият и поправят грешки с по-голяма кратност:
 $d_0 = \sigma + t + 1$
- **Кратността на откриване на грешки (σ)** - относителният брой забранени комбинации между две разрешени
 $1 \leq \sigma \leq d - 1$
- **Кратността на поправяне на грешки (t)** - множеството на забранени кодови комбинации, принадлежащи към дадена разрешена комбинация

Коригиращи възможности на кода

В зависимост от:

- кодовото разстояние;
- кратността на откриване;
- кратността на коригиране на грешки.

d	σ	t	Коригираща възможност
1	0	0	Различава една кодова комбинация от друга
2	1	0	Открива еднократни грешки
3	1	1	Открива и коригира еднократни грешки
4	2	1	Открива двукратни и коригира еднократни грешки
4	3	0	Открива трикратни грешки
5	2	2	Открива и коригира двукратни грешки
5	3	1	Открива трикратни грешки и коригира еднократни
5	4	0	Открива четирикратни грешки

Характеристики на кода (1)

- **Дължина на кода n** - определя се от броя на разрядите (символите), съставляващи кодовата комбинация.
- **Основа на кода m** - броят на различаващите се един от друг импулсни признаци за означаване на разрядите
 - 0 или 1 при основа $m = 2$
- **Мощност на кода N_p** - разрешени кодови комбинации - броят на кодовите комбинации (работни кодови думи), използвани за предаване на съобщения. Мощността на кода с отчитане само на информационните символи се определя от израза $N_p = m^k$
- **Пълният брой на кодовите комбинации N** - броят на всички възможни кодови комбинации $N = m^n$ за m -ичните кодове.
- **Брой на информационните символи k** - количеството на символите на кодовата комбинация за предаване на съобщението.

Характеристики на кода (2)

- **Скорост на предаване на кодовите комбинации R** - отношението на броя на информационните разряди към дължината на кода – $R = k/n$.
- **Тегло на кодовата комбинация w** - количеството на единици в кодовата комбинация.
- **Теглова характеристика на кода $W(w)$** - броят на кодови комбинации с тегло w .
- **Коефициент на откриване и изправяне на грешки L** - отношението $L = A/(A+B)$, където:
 - A е броят на комбинациите, в които се открива или поправя грешката;
 - B е броят на комбинациите, в които грешката не се открива и поправя.
- **Коефициент на откриване на грешката $L_{откр}$** – $L_{откр} = (1 - N_p)/N$

Характеристики на кода (3)

- **Вероятност за неоткриване на грешки**
Рнг – вероятност за настъпване на събитие, при което приетата кодова комбинация се отличава от предадената и свойствата на кода не могат да открият наличие на грешка.
- **Оптималност на кода** – свойство на кода, което осигурява най-малка вероятност за неоткриване на грешки от всички кодове със същата дължина n и излишък $(n-k)$.

Баланс - скорост/надеждност

- Съчетаването на тези две изисквания е **НЕВЪЗМОЖНО**, защото те взаимно се **ИЗКЛЮЧВАТ**:
 - за увеличаване на скоростта трябва да се **намали ИЗЛИШЪКЪТ**
 - за увеличаване на надеждността трябва да се **увеличи ИЗЛИШЪКЪТ**
- **Оптимален код без излишък** е този код, при който кодираните съобщения са представени с кодови думи с минимална средна дължина, **излишъкът от информация** е **сведен до минимум**.

Код по четност

- Последователността от разряди се разделя на групи.
- Проверката по четност се извършва за всяка група като броят на единиците се допълва до четно число.
- Недостатък - невъзможността за откриване на грешки с четна кратност.
- Прилага се в местата, където са по-вероятни единичните грешки.

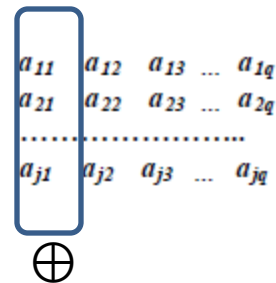
Пример:

Кодовата комбинация 0111110 се преобразува в 01111101

Матричен код по четност

Ако възникне една грешка при предаване, с голяма вероятност около нея има още грешки. Затова:

- Последователността от разряди се разделя на групи.
- Групите се записват в матричен вид и се проверяват по четност стълбовете на получената матрица.
- При наличие на една групова грешка с дължина по-малка от q , във всяка проверка ще се открие не повече от един символ.
- Грешките в този случай няма да се открият, ако са изкривени четен брой разряди в стълба.
- Ако грешките са независими, кодът е еквивалентен на код с проверка по четност в редовете.
- Ако грешките са корелирани, за сметка на декорелацията кодът ще е по-устойчив на изкривявания.
- Недостатък на този код е сложността на кодиращите и декодиращите устройства.
- Декорелацията на грешките се извършва, когато проверката по четност се реализира по диагоналите на матрицата.
- За повишаване на способността на кода за откриване на грешки, проверката по четност се извършва едновременно по стълбовете и диагоналите или по редовете и стълбовете.
- Притежават висока откриваща способност и намират широко приложение в апаратурите за предаване на цифрови данни.



Код с постоянно тегло

- Кодът с постоянно тегло е двоичен равномерен код, в който всички разрешени комбинации съдържат еднакъв брой единици.
- Открива всички грешки с изключение на случаите, когато еднакъв брой единици се превръщат в нули, и обратно – същият брой нули в единици.
- Кодирането на 0 или 1 се съдържа в два импулса с противоположна полярност и с определена последователност на смяна на полярността.
- Грешка в кодовата комбинация – от поява на лъжлив импулс или загуба на някой импулс.
- Грешка не може да се открие, когато в една двойка импулси, съответстващи на един информационен разряд, са се изкривили едновременно и двата импулса.
- Предимство – при асиметричните канали.
- Недостатък - поради липса на разделение между контролни и информационни разряди за кодиране и декодиране се използват много сложни кодопреобразуватели.
- Такива са кодовете от вида „2 от 5”, „3 от 6”, „3 от 7”, „3 от 8”, „4 от 8”.

Пример:

В „3 от 7” - комбинациите 3 единици към 4 нули са 35.

Код на К. Шенон – Р. Фано

1. Символите (x_i) се разполагат по реда на намаляване на вероятностите за появяването им в съобщенията - $P(x_i)$.
2. Групата се разделя на две подгрупи по такъв начин, че сумарните вероятности на символите в двете подгрупи по възможност да са равни.
3. На всеки символ от първата група се присвоява 0, а на втората – 1 (или обратно). Така се получават първите (старшите) цифри на кода.
4. Стъпки 2 и 3 се повтарят за всяка от новосъздадените подгрупи, докато във всяка от подгрупите остане по един символ.

Пример:

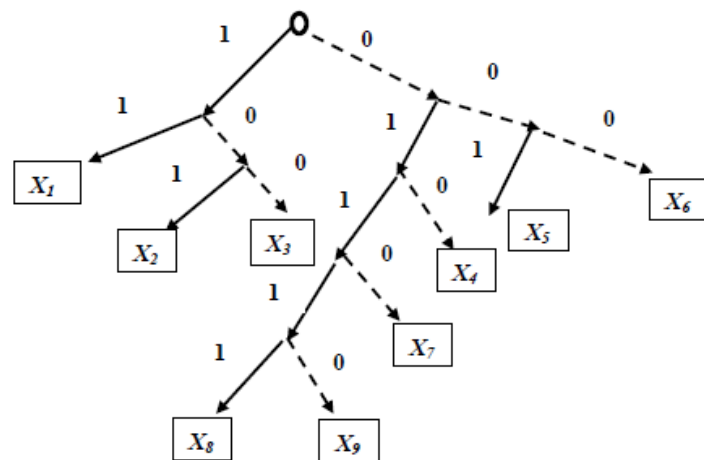
x_i	$P(x_i)$	Разбиване на подгрупи					Кодова дума	Дължина на кодовата дума
x_1	0,35	1	1				11	2
x_2	0,15	1	0				10	2
x_3	0,13	0	1	1			011	3
x_4	0,09	0	1	0			010	3
x_5	0,09	0	0	1	1		0011	4
x_6	0,08	0	0	1	0		0010	4
x_7	0,05	0	0	0	1		0001	4
x_8	0,04	0	0	0	0	1	00001	5
x_9	0,02	0	0	0	0	0	00000	5

Код на Хафмън

1. Символите (x_i) се разполагат по реда на намаляване на вероятностите появяването им в съобщението - $P(x_i)$.
2. На всяка стъпка се добавя възел в префиксното кодово дърво, по което се определят кодовите комбинации.
3. Двата символа с най-малки вероятности се обединяват, като по-горното от таблицата получава символ 1, а по-долното – символ 0 (в префиксното кодово дърво – символът отляво – 1, а отдясно - 0).
4. Техните две вероятности се събират и резултатът се записва в новообразуваната колона с вероятности, подредени отново в низходящ ред.
5. Стъпки 2 и 3 се повтарят, докато останат 2 стойности, чиито сбор е 1.

Пример:

x_i	$P(x_i)$	Обединяване на съобщенията							Кодова дума	Дължина на кодовата дума
		1)	2)	3)	4)	5)	6)	7)		
x_1	0,35	0,35	0,35	0,35	0,35	0,35	0,37	0,63	11	2
x_2	0,15	0,15	0,15	0,17	0,20	0,28	0,35	0,37	101	3
x_3	0,13	0,13	0,13	0,15	0,17	0,20	0,28		100	3
x_4	0,09	0,09	0,11	0,13	0,15	0,17			010	3
x_5	0,09	0,09	0,09	0,11	0,13				001	3
x_6	0,08	0,08	0,09	0,09					000	3
x_7	0,05	0,06	0,08						0110	4
x_8	0,04	0,05							01111	5
x_9	0,02								01110	5
	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00		



Код на Хеминг

- Коригиращ групов (n, k) код, в който матрицата на проверките $M(n, k)$ има $r=(n - k)$ редове и $(2^r - 1)$ стълбове.
- Информационните и контролните разряди са разделени и може да се посочи мястото им в кодовата комбинация.
- Всички r -разрядни двоични последователности са ненулеви.
- $d_0 = 3$
- Може да открива двойни грешки.
- Може да изправи всички единични грешки.
- Коригиращото число указва номера на изкривения елемент в кодовата комбинация.
- Броят на разрядите на коригиращото число е r ,
- За да може да се посочи всеки сгрешен елемент, трябва:
 $r > \log_2(n+1)$

Формиране на контролни разряди

- Тези елементи се формират в предавателя при предаване на кодовата комбинация.
- Оригиналната поредица битове е: $x_1 x_2 x_3 x_4 x_5 \dots$,
- Контролните разряди се разполагат на 1, 2, 4, 8.... позиции в предаваната кодова комбинация.
- Броят на контролните битове се определя от:

$$r = n - k \quad \text{и} \quad r > \log_2(n + 1)$$

- Контролните битове се получават:

$$b_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} \oplus a_{13} \dots$$

$$b_2 = a_2 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} \dots$$

$$b_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \dots$$

$$b_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \dots$$

- Предаваната поредица битове (кодовата комбинация) е:
 $a_1 a_2 a_3 a_4 a_5 \dots$

Предавана поредица	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	...
Информационни и кодови елементи	b_1	b_2	x_1	b_3	x_2	x_3	x_4	b_4	x_5	x_6	...

Коригиращо число на Хеминг

- Получаваната поредица битове (кодовата комбинация) е: $a_1 a_2 a_3 a_4 a_5 \dots$
- Коригиращото число (r) показва кой бит е сгрешен при предаването и трябва да се инвертира

$$r = E_r E_{r-1} \dots E_2 E_1$$

$$E_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} \oplus a_{13} \oplus a_{15} \oplus a_{17} \oplus a_{19} \oplus a_{21} \dots$$

$$E_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} \oplus a_{14} \oplus a_{15} \oplus a_{18} \oplus a_{19} \oplus a_{22} \dots$$

$$E_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \oplus a_{20} \oplus a_{21} \oplus a_{22} \dots$$

$$E_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15} \oplus a_{24} \oplus a_{25} \dots$$

$$E_5 = a_{16} \oplus a_{17} \oplus a_{18} \oplus a_{19} \oplus a_{20} \oplus a_{21} \oplus a_{22} \oplus a_{23} \oplus a_{24} \oplus a_{25} \dots$$

$$E_6 = a_{32} \oplus a_{33} \oplus a_{34} \oplus a_{35} \oplus a_{36} \oplus a_{37} \oplus a_{38} \oplus a_{39} \oplus a_{40} \oplus a_{41} \dots$$

- Във всяка последователност от елементи, обхващани от една проверка, трябва да влиза само един контролен елемент - елементът a_1 участва само в E_1 , a_2 – само в E_2 , a_4 – само в E_3 и т.н.
- Т.е. всеки първи елемент е контролен, тъй като той участва само в тази проверка.
- Тези елементи се формират при получаване на кодовата комбинация в приемника.

Пример

Да се преобразува седемелементният прост код в код на Хеминг, откриващ и коригиращ единична грешка.

$$k = 7$$

$$r = n - k = n - 7 > \log_2(n+1) \Rightarrow 2^{n-7} > n+1 \Rightarrow 2^n > 2^7(n+1) \Rightarrow n=11$$

$$r = n - k = 11 - 7 = 4$$

Ако съобщението е 1011010, то се изпраща 00100111010, защото:

$$b_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0$$

$$b_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 0$$

$$b_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0 \oplus 1 \oplus 1 = 0$$

$$b_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} = 0 \oplus 1 \oplus 0 = 1$$

Ако се приеме 00100111110, т.е. сгрешен е 9 разряд, това се разбира като се получава коригиращото число $r = E_4 E_3 E_2 E_1$

$$E_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$$

$$E_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{11} = 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 0$$

$$E_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0 \oplus 0 \oplus 1 \oplus 1 = 0$$

$$E_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} = 1 \oplus 1 \oplus 1 \oplus 0 = 1,$$

Т.е. коригиращото число е $r=1001$ – двоичен запис на цифрата 9 – сгрешеният елемент е 9-ия и трябва да се коригира (инвертира).

Циклични кодове (1)

- **Цикличен (n, k) код** се нарича кодът, чието множество от кодови комбинации, представлява съвкупност от многочлени от степен $n - 1$ и по-малка, делищи се на многочлен $P(x)$ на степен $n - k$, който се явява **образуващ многочлен**.
- Имат висока ефективност при откриване и коригиране на грешки в кодовите комбинации.
- Апаратната реализация на кодиращите и декодиращите устройства е сравнително опростена и лесна за изпълнение.
- Реализират се с полиноми. Ако броят на елементите на кодовата комбинация е n , съответният многочлен е от вида:

$$F(x) = C_{n-1} \cdot x^{n-1} + C_{n-2} \cdot x^{n-2} + \dots + C_2 \cdot x^2 + C_1 \cdot x^1 + C_0 \cdot x^0,$$

където коефициентите $C_0, C_1, C_2, \dots, C_{n-1}$ приемат значение 0 или 1.

$$x \cdot F(x) = C_{n-1} \cdot x^n + C_{n-2} \cdot x^{n-1} + \dots + C_2 \cdot x^3 + C_1 \cdot x^2 + C_0 \cdot x^1,$$

но n елементна кодова комбинация не може да превишава $(n-1)$ степен, т.е. променливата x^n е x^0 :

$$x \cdot F(x) = C_{n-2} \cdot x^{n-1} + \dots + C_2 \cdot x^3 + C_1 \cdot x^2 + C_0 \cdot x^1 + C_{n-1},$$

Така $(x \cdot F(x))$ се явява циклично преместена комбинация на $F(x)$.

Циклични кодове (2)

- Кодовият многочлен $F(x)$ може да се получи, като се умножи многочленът $G(x)$ по образуващия многочлен $P(x)$:
$$F(x) = G(x) \cdot P(x)$$
- Недостатък - Тук липсва строго разделяне на информационните и кодиращите елементи в кодовата комбинация. Изисква по-сложни схеми за декодиране.
- За да разделим информационни от кодиращи елементи, се умножава $G(x)$ по x^r - така с по-висок порядък ще са информационните елементи, а коефициентите от по-нисък порядък - контролните.
$$x^r \cdot G(x) = Q(x) \cdot P(x) + R(x)$$
- Но сумирането и изваждането по модул 2 са идентични действия:
$$x^r \cdot G(x) + R(x) = Q(x) \cdot P(x) = F(x),$$
т.к. $G(x)$ и $Q(x)$ са от една и съща степен
$$Q(x) = (x^r \cdot G(x) + R(x)) / P(x)$$
- Наличие на грешка в приетото съобщение $H(x)$ се открива:
 - ако $H(x)$ не се дели на $P(x)$
 - ако $H(x)$ се дели – няма грешка.

Пример

Задача:

За 12 елементен код ($k = 12$) се използва образуващ полином: $P(x) = x^5 + x^4 + x^2 + 1$. Да се определи значението на контролните елементи на комбинацията 010001011001.

Решение:

В случая броят на контролните елементи е 5 ($r=5$), а $G(x) = x^{10} + x^6 + x^4 + x^3 + 1$

$$(x^5 \cdot G(x)) / P(x) = x^5(x^{10} + x^6 + x^4 + x^3 + 1) / (x^5 + x^4 + x^2 + 1)$$

$Q(x) = x^{10} + x^9 + x^8 + 1$ и остатък $R(x) = x^4 + x^2 + 1$, т.е контролните елементи са 10101.

Тогава $F(x) = x^5 \cdot G(x) + R(x) = (x^{15} + x^{11} + x^9 + x^8 + x^5) + (x^4 + x^2 + 1)$,
информационните елементи са: 010001011001 и 10101 – контролни.

Нека се предава 010001011001 10101, а се получава
0100011100110101 и се представя с:

$$H(x) = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^2 + 1$$

Грешката се открива като:

$$F(x) - H(x) = (x^{15} + x^{11} + x^9 + x^8 + x^5 + x^4 + x^2 + 1) - (x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^2 + 1) = x^{10}$$

Свойства на цикличните кодове

- Цикличен код, на който образуващият полином $P(x)$ се състои от повече от един член, открива всички единични грешки.
- Цикличен код с образуващ многочлен $P(x) = x + 1$ открива не само единични, но и произволен нечетен брой грешки.
- Цикличен код с образуващ полином $P(x) = (x + 1)P^r(x)$ позволява да се открият всички единични, двойни и тройни грешки, ако степента r на неделимия многочлен $P^r(x)$ е такава, че $(2^r - 1) \geq n$, където n -брой елементи на кода.
- Цикличен код с образуващ многочлен от степен r открива всеки пакет с грешки с дължина r и по-малка.
- За всички значения на j и t съществува цикличен код с дължина $n = 2^j - 1$, изправящ всички грешки с кратност t и по-малка и съдържащ не повече от $r = j \cdot t$ контролни елементи.

Приложение на циклични кодове

- Полиномът $P(x) = x^8 + x^2 + x + 1$ се прилага в
 - цикличен код ITU CRC-8.
 - стандарт ATM за контрол на грешките в заглавната част на клетките
 - стандарт IEEE 802.6 за изграждане на регионални компютърни мрежи.
- Полиномът $P(x) = x^{16} + x^{12} + x^5 + 1$ се прилага в
 - цикличен код ITU CRC-16. Кодът открива грешки в пакети с дължина 16 бита. Последният член на полинома със стойност 1 генерира проверка по четност. Този код открива пакетните грешки с нечетност и грешки с четна кратност до 16.
 - в протокола HDLC
 - В протоколи от семейство LAP (LAPB, LAPD, LAPF...).
- Полиномът $P(x) = x^{32} + x^{26} + x^{23} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ се прилага в
 - цикличен код ITU CRC-32.
 - в стандартните локални компютърни мрежи IEEE 802.3. (Ethernet).

Въпроси ?

Благодаря за вниманието !