



Интернет: Обнаружение ошибок передачи

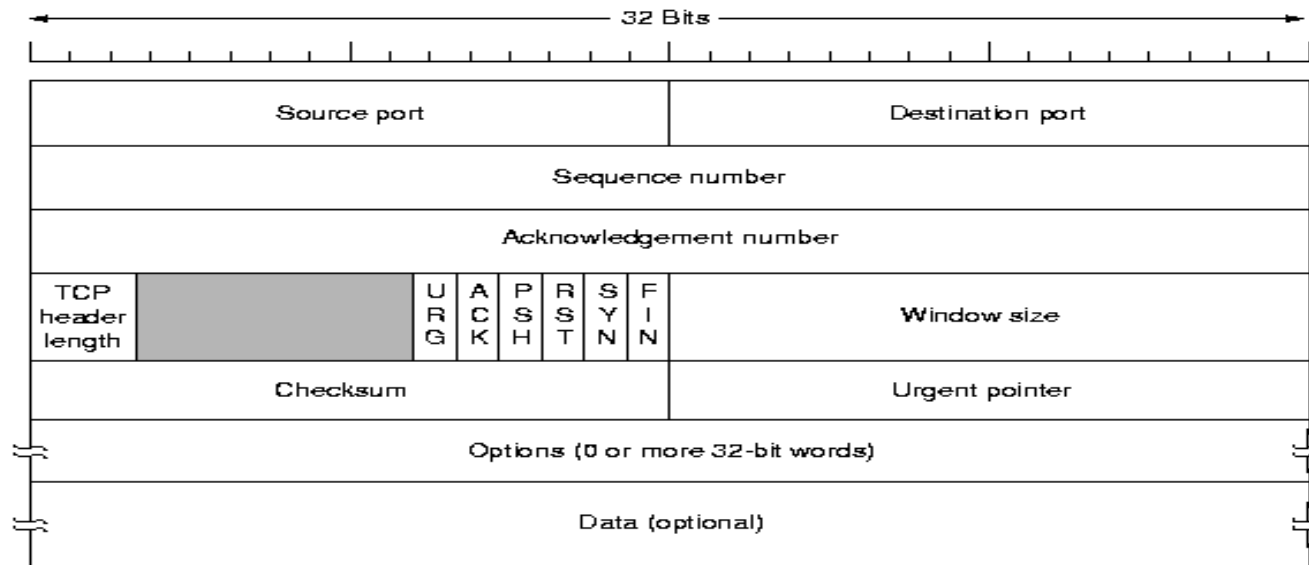
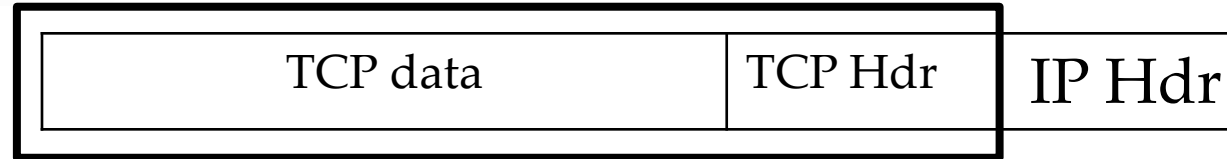
(Смелянский Компьютерные сети. т.1, стр. 116-122)

Введение в компьютерные сети

проф. Смелянский Р.Л.
Лаборатория Вычислительных комплексов
ф-т ВМК МГУ

Обнаружение ошибок

← IP data →



Способы обнаружения ошибок

- **Добавление контрольной суммы в пакеты IP, TCP**
 - Быстро, аппаратно, но можно и программно
 - Не очень надежно
- **Полиномиальные CRC коды (Ethernet)**
 - Дороже контрольной суммы (вычисляются аппаратно)
 - Защищают от групповых ошибок, пакетов ошибок и ошибок четности
- **Использование специальных кодов**

контрольная сумма в IP пакете

- *IP, UDP и TCP используют один и тот же алгоритм комплементарной контрольной суммы:*
 - *Установить поле checksum= 0*
 - *Сложить все 16 разрядные слова в пакете*
 - *Установить разряд четности*
 - *Контрольная сумма должны быть такой чтобы сумма всего пакета, включая контрольную сумму была бы 0xffff*
- *Основное достоинство - простота*
- *Недостаток - слабая защита от ошибок (только одиночные ошибки).*

Обнаружение и исправление ошибок

(см. учебник т.1 стр.116-122)

- *Ошибки единичные и групповые (блочные)*
- *Коды с обнаружением ошибок*
 - *кодослово*
 - *расстояние Хемминга*
- *Коды исправляющие ошибки*
0000000000, 0000011111, 1111100000, 1111111111
$$(n+1)2^m \leq 2^n; (m+r+1) \leq 2^r$$

Коды с исправлением ошибок

- Код Хемминга для единичных ошибок
 - разряды кодослова нумеруют слева направо, начиная с 1;
 - все биты, номера которых есть степень 2 (1,2,4,8,16 и т.д.) - контрольные, остальные - биты сообщения;
 - каждый контрольный бит отвечает за четность группы битов, включая себя. Один и тот же бит может относиться к разным группам. Значение бита сообщения определяется по значениям контрольных битов. Чтобы определить какие контрольные биты контролируют бит в позиции k надо представить значение k по степеням двойки. Например, $11 = 1 + 2 + 8$, $39 = 1 + 2 + 4 + 32$.



Char.	ASCII	Check bits
H	1001000	00110010000
a	1100001	10111001001
m	1101101	11101010101
m	1101101	11101010101
i	1101001	01101011001
n	1101110	01101010110
g	1100111	11111001111
	0100000	10011000000
c	1100011	11111000011
o	1101111	00101011111
d	1100100	11111001100
e	1100101	00111000101

Order of bit transmission

Код Хемминга для исправления одиночных ошибок

Коды обнаруживающие ошибки

- Групповые ошибки
- Биты четности не позволяют эффективно бороться с групповыми ошибками
- Иногда перепослать дешевле, чем исправить
- CRC код (Cyclic Redundancy Code)
 - строка 110001 представляет полином $x^5+x^4+x^0$
 - арифметика выполняется по модулю 2

Коды обнаруживающие ошибки (CRC)

- Отправитель и получатель договариваются о конкретном генераторе полиномов $G(x)$ степени r (коэффициенты при старшем члене и при младшем члене должны быть равны 1).
- Для вычисления контрольной суммы блока из m бит надо чтобы обязательно $m > r$.
- Добавить контрольную сумму к передаваемому блоку, рассматриваемому как полином $M(x)$ так, чтобы передаваемый блок с контрольной суммой был кратен $G(x)$. Когда получатель получает блок с контрольной суммой, он делит его на $G(x)$. Если есть остаток, то были ошибки при передаче.

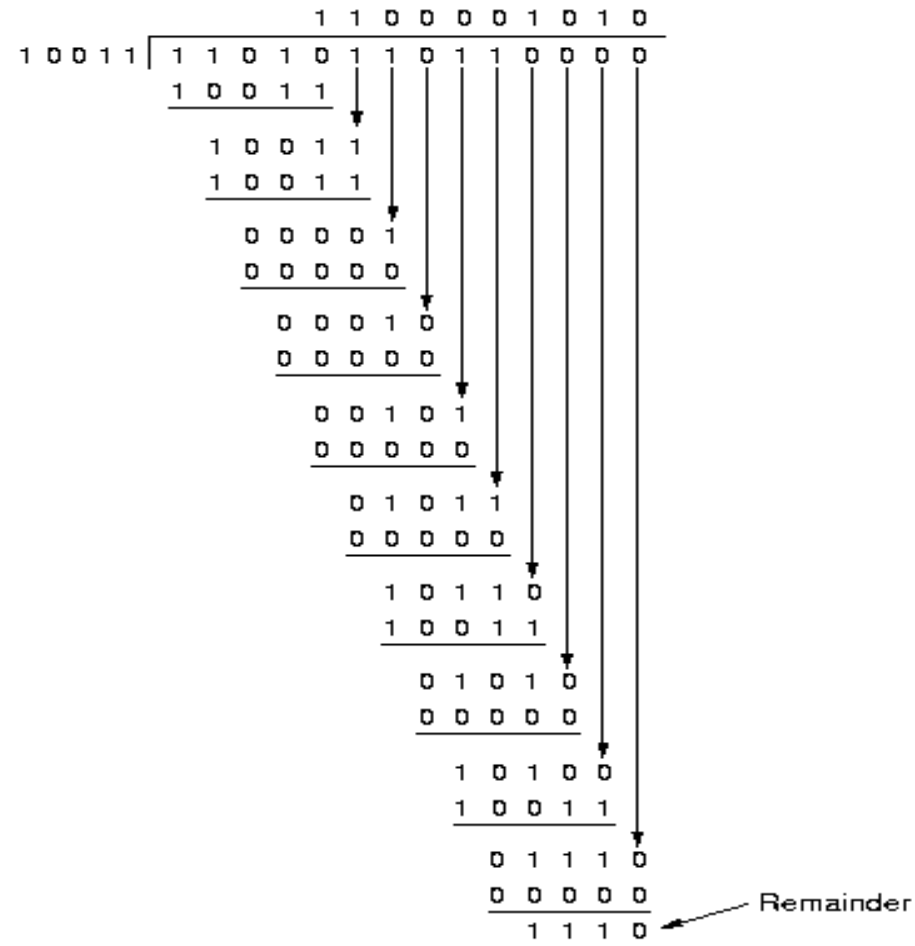
Коды обнаруживающие ошибки

- Алгоритм вычисления контрольной суммы:
 - Добавить r нулей в конец блока так, что он теперь содержит $t+r$ разрядов и соответствует полиному $x^r M(x)$;
 - Разделить по модулю 2 полином $x^r M(x)$ на $G(x)$;
 - Вычесть остаток (длина которого всегда не более r разрядов) из строки, соответствующей $x^r M(x)$, по модулю 2. Результат и есть блок с контрольной суммой (назовем его $T(x)$).

Frame : 1 1 0 1 0 1 1 0 1 1

Generator: 1 0 0 1 1

Message after appending 4 zero bits: 1 1 0 1 0 1 1 0 0 0 0



Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 0

Коды обнаруживающие ошибки

- Существует три международных стандарта на вид $G(x)$:
 - $CRC-12$ $= x^{12} + x^{11} + x^3 + x^2 + x + 1$
 - $CRC-16$ $= x^{16} + x^{15} + x^2 + 1$
 - $CRC-CCITT$ $= x^{16} + x^{12} + x^5 + 1$
- $CRC-12$ используется для передачи символов из 6 разрядов. Два остальных - для 8 разрядных. $CRC-16$ и $CRC-CCITT$ ловят одиночные, двойные ошибки, групповые ошибки длины не более 16 и нечетное число изолированных ошибок с вероятностью 99,997%.

Message Auth. Code

- *Message Authentication Code (MAC)*
 - Не путать с Media Access Control!
- *Использует криптографию для вычисления* $m = \text{MAC}(M, s),$
 $|m| \ll |M|$
 - M известно, s - секретно \Rightarrow можем проверить $m = \text{MAC}(M, s), |m| \ll |M|$
 - Если s не известно, то получить m практически не возможно
 - Если известно m , то практически не возможно вычислить M ,
- *Не столь устойчиво к ошибкам как CRC*
- *Защищает от злоумышленников*

Схемы обнаружения ошибок

- *Контрольная сумма добавляется в IP, TCP, UDP пакеты*
 - *Быстро, дешево*
 - *Неустойчиво*
- *CRC коды используются в Ethernet кадрах*
 - *Дороже чем контрольная сумма*
 - *Устойчивы к двукратным ошибкам, групповым ошибкам и ошибкам четности*
- *Использование кодов с обнаружением ошибок (бит четности)*