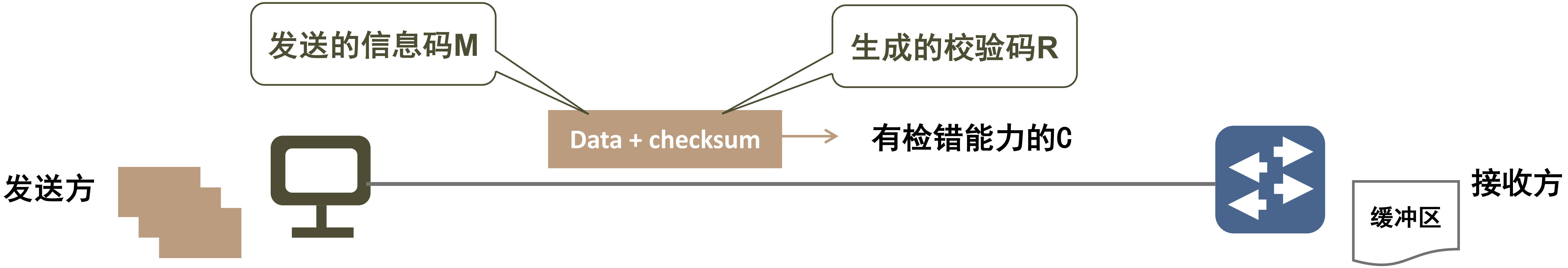
循环冗余差错校验

循环冗余校验码（CRC）

基本思想

- 发送方将要传送的信息分成码组M，按某种约定的规律对每一个信息码组附加一些校验码R，形成新的码C，使得C中的码元之间具有一定的相关性，再传输到接收方；
- 接收方根据这种相关性或规律性来校验码C是否正确，还可对出错码组的错定位加以相应的纠正，最后将码C还原成信息码M。



码多项式及其算术运算

假设 码$C = C_{n-1}\ C_{n-2}....\ C_2\ C_1\ C_0$ 长度为n

C的码多项式（称为n-1次多项式）

$C(x) = C_{n-1}\ x^{n-1} + C_{n-2}x^{n-2} + ...\ C_2\ x^2 + C_1\ x + C_0$

例如： C = 1100101

$C(x) = x^6 + x^5 + x^2 + 1$

码多项式算术运算

- 模2加
- 模2减
- 模2乘
- 模2除

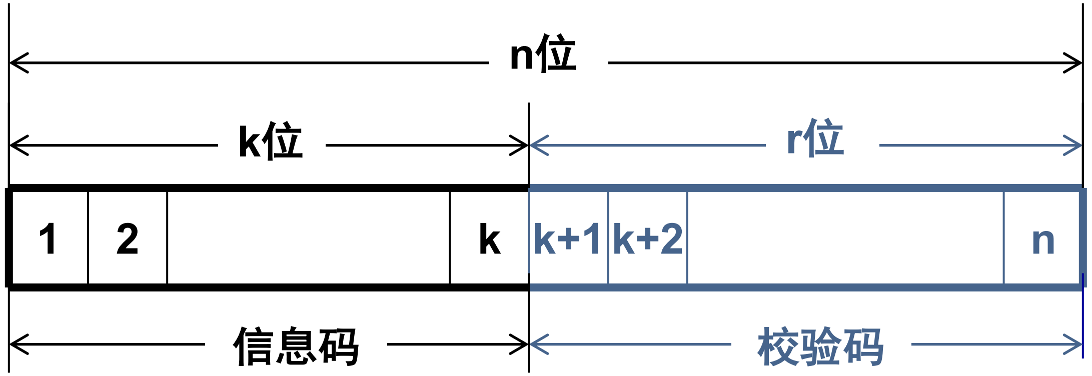
例如： 1101011011.0000 ÷ 10011

商数：1100001010

余数：1110

循环码与循环码生成多项式

对于一个码长为n，信息码为k位的循环码（n，k），其构成形式为：



循环码(n，k)用多项式表示：

$$C(x) = C_{n-1}\, x^{n-1}+C_{n-2}x^{n-2}+\ldots C_{n-k}\, x^{n-k}+C_{n-k-1}x^{n-k-1} \ldots C_2x^2+C_1x+C_0$$

在一个(n，k)循环码中，存在一个且只有一个(n-k)次的码多项式

$$\boxed{g(x) = x^{n-k}+g_{n-k-1}x^{n-k-1}+\ldots+g_2x^2+g_1x+1}$$

- 此循环码中任一码多项式都是g(x)的倍式
- 任意一个(n−1)次或(n−1)次以下又是g(x)倍式的多项式必定是此循环码的一个码多项式

生成多项式: (n-k)次且最高次系数非0的码多项式g(x).

校验码的产生

- 设生成多项式G(x)的最高幂次为r=n-k
- 将待编码码元序列表示为m(x)，乘以x^r，结果左移r位$x^r \cdot m(x)$
- 用G(x)去除 $x^r \cdot m(x)$，求得商式Q(x)和余式R(x)

$CRC\text{-}12=x^{12}+x^{11}+x^3+x^2+x+1$

$CRC\text{-}16=x^{16}+x^{15}+x^2+1$

$$[x^r \cdot m(x)]/G(x) = Q(x) + R(x)/G(x)$$

$$x^r \cdot m(x) = Q(x) \cdot G(x) + R(x)$$

$$x^r \cdot m(x) + R(x) = Q(x) \cdot G(x)$$

R(x)校验多项式。
其系数$C_{r-1}, C_{r-2}, \ldots, C_1$, C_0为校验码

为除法运算后变成的循环多项式C(x)的表示式

$$C(x) = C_{n-1}x^{n-1}+C_{n-2}x^{n-2}+ . +C_{n-k}x^{n-k}+C_{n-k-1}x^{n-k-1}+\ldots C_2x^2+C_1x+C_0$$

$$= C_{n-1}x^{n-1}+C_{n-2}x^{n-2}+ \ldots +C_{n-k}x^{n-k}+ C_{r-1}x^{r-1}+C_{r-2}x^{r-2} \ldots C_2x^2+C_1x+C_0$$

信息码 | 校验码

北京大学

循环码校验工作过程

发送方

发送缓冲区
m(x)

G(x)

R(x)+m(x)*x^r

接收缓冲区
m′(x)

接收方

G(x)

①待发送数据m(x)

②生成多项式G(x)　r = n-k

③ $\frac{m(x) * x^r}{G(x)} = Q(x) + \frac{R(x)}{G(x)}$

④ 实际发送：m(x) * x^r + R(x)

数据信息　校验信息

①收到的数据m’(x)

②生成多项式G(x)

③ $\frac{m'(x) * x^r}{G(x)} = Q'(x) + \frac{R'(x)}{G(x)}$

④ 接收方判断收到的数据信息是否正确

R′ (x)= R(x)传输正确

R′ (x)!= R(x)传输错误

校验和计算实例

示例1：设编码的信息码元为1101011011.试问给定生成多项式g(x)下发送的码组？

$m(x) = x^9 + x^8 + x^6 + x^4 + x^3 + x + 1,\qquad k = 10$

① 假设 $g(x) = x^4 + x + 1$

系数形成的位串为10011　　$r = 4 \rightarrow n = 14$

$r(x)$的最高幂次为 $r-1=3$

② $x^4 \cdot m(x) = 1101011011,0000$

③ $1101011011.0000 \div 10011$ →

商数：1100001010

余数：1110

$r(x) = x^3 + x^2 + x + 0$

④所需的循环编码C(x)为

$C(x) = x^r \cdot m(x) + r(x) =$ 1101011011，1110

多项式计算实例

示例2：多项式除法

1101011011.0000÷ 10011

```
                 1 1 0 0 0 0 1 0 1 0      ←— 商数
          ________________________
1 0 0 1 1 / 1 1 0 1 0 1 1 0 1 1,0 0 0 0   ←— 被除数 m(x)
    ↑       1 0 0 1 1
    |       ---------
  除数        1 0 0 1 1
  g(x)        1 0 0 1 1
              -------------
                   1 0 1 1 0
                   1 0 0 1 1
                   ---------
                     1 0 1 0 0
                     1 0 0 1 1
                     ---------
                       1 1 1 0  ←— 余数 r(x)
```

模2加＝模2减

0+0 = 0； 0+1 = 1+0 = 1； 1+1 = 0；

0−0 = 0； 0−1 = 1−0 = 1； 1−1 = 0；

模2乘

0*0 = 0*1 = 1*0 = 0； 1*1 = 1

模2除：模2乘的可逆运算

循环校验码的检错能力

- CRC循环校验码的检错能力
  - 检查全部单个错（1位错）
  - 检查全部离散的二位错（双错）
  - 检查全部的奇数个错（1，3，5…个错）
  - 检查全部长度等于(n-k)或小于(n-k)的突发错
  - 以$[1-2^{-(r-1)}]$的概率检查出长度为(r+1)的突发错以及以$[1-2^{-r}]$的概率检查出多于(r+1)的突发错

链路层基本功能小结

链路层主要功能

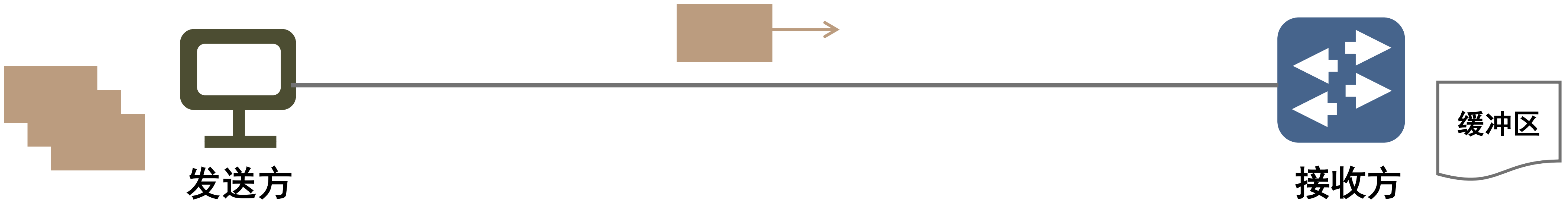
- 组成帧(结合协议介绍)
- 流量控制
- 差错控制
- 共享介质访问控制

控制机制的本质

- 任何控制都有代价
- 流量/差错控制代价
  ① 肯定/否定确认
  ② 额外的校验码
  ③ 缓冲区
  ④ 计算负担

传输性能的提高

- 滑动窗口
- 累计确认
- 捎带确认
- 否定确认
- 肯定确认
- 计时器（超时重发）



数据帧