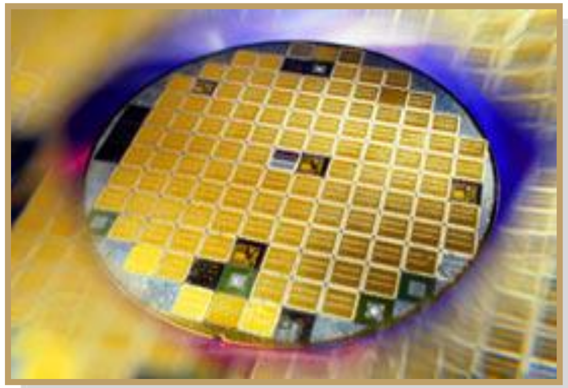
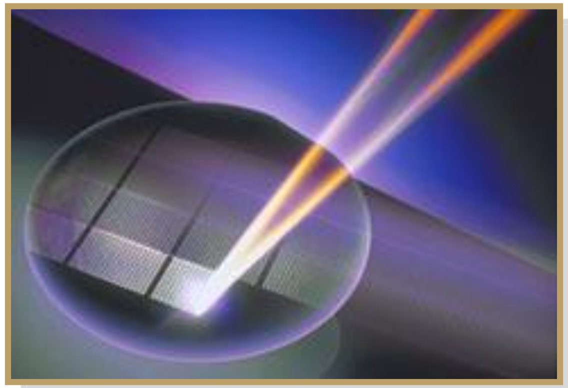
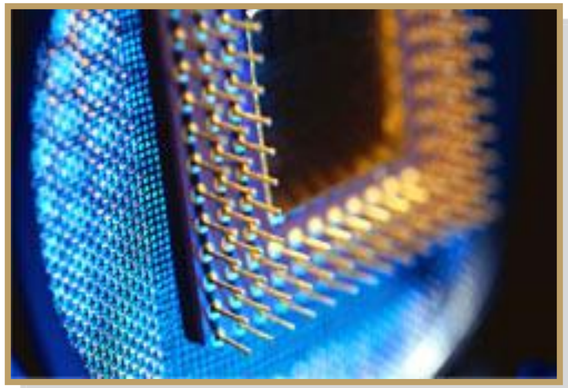
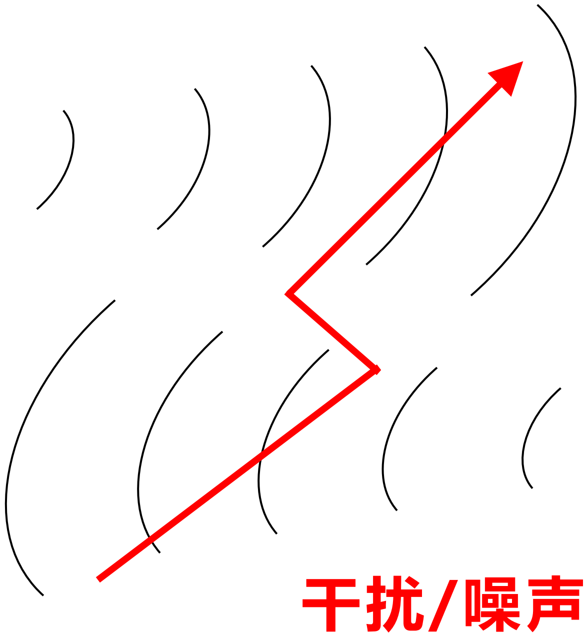
《VLSI数字通信原理与设计》课程

第十三章：信道编解码（1）

语音中的干扰与噪声

011010100111010……



0110100000110110……

图像传输的干扰与噪声

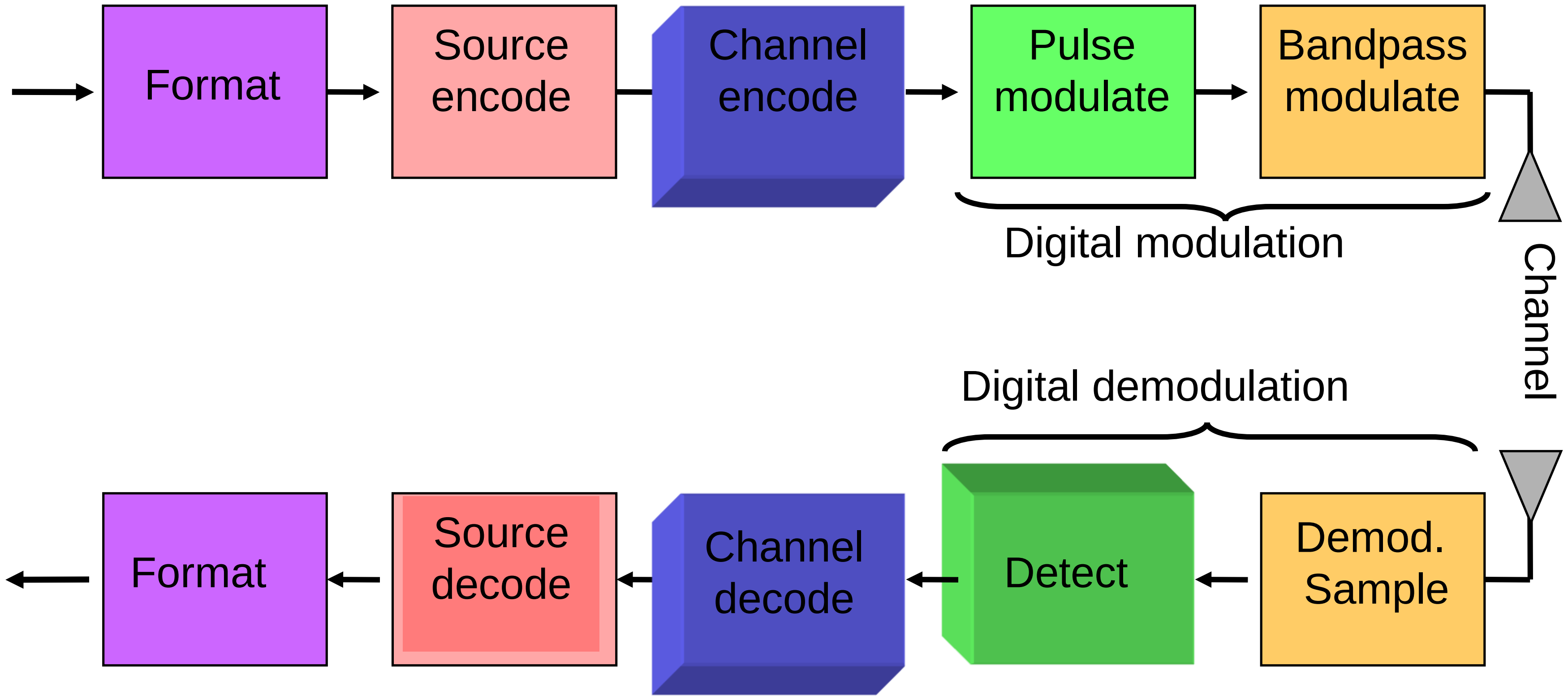
发送端：

有干扰的信道传播

接收端：


目录

01. 数字通信系统



Format
Source encode
Channel encode
Pulse modulate
Bandpass modulate
Digital modulation
Channel
Digital demodulation
Format
Source decode
Channel decode
Detect
Demod. Sample

01. 信道编码 —— 目的

- 在复杂性、可靠性和有效性之间选择一个好的工作点（有时还要考虑延时）。

- 目的：提高信号传输的可靠性

- 方法：增加冗余比特，以发现或纠正错误。即将信息空间映射到更大的信道空间，以提高不同码字间的差异程度，从而获得编码增益。

01. 信道编码 —— 基本原理

实质就是在信息码中增加一定数量的多余码元（称为监督码元），使它们满足一定的约束关系。

- 发送端将信息码元和监督码元共同组成一个由信道传输的码字；
- 一旦传输过程中发生错误，则信息码元和监督码元间的约束关系被破坏；
- 在接收端按照既定的规则校验这种约束关系，从而可达到发现和纠正错误的目的。

01. 信道编码 —— 分类

线性码	信息码与监督码之间的关系为线性关系；
非线性码	信息码与监督码之间的关系为非线性关系。
分组码	信息码与监督码以组为单位建立关系；
卷积码	监督码与本组和前面码组中的信息码有关。
系统码	编码后码组中信息码保持原图样顺序不变；
非系统码	编码后码组中原信息码原图样发生变化。

01. 信道编码 —— 分类

- 信道编码
  - 分组码
    - 线性分组码
      - 汉明码
      - 循环码
        - CRC
        - BCH码
    - 非线性分组码
  - 卷积码
    - 线性卷积码
    - 非线性卷积码

01. 误码的主要形式

随机错误

- 误码的位置随机（误码间无关联），随机误码主要由白噪声引起。

突发错误

- 误码成串出现，主要由强脉冲及雷电等突发的强干扰引起。

混合错误

- 以上两种误码及产生原因的组合。

三位二进制码的三种编码方法。三位二进码共有8种可能的组合：000，001，010，011，100，101，110，111。

a) 若8个码组均用于表示不同的信息，任一位或一位以上的错误都会变成另一码组，所以无法检错和纠错。

b) 若将8个码组分成许用和禁用两类：

许用码组	000，011，101，110
禁用码组	111，100，010，001

因任何一位误码，都会变成禁用码组，所以可检出一位误码。

c) 若只用 000，111两个码组，其余为禁用码组，则可发现两位及以下的误码，并纠正一位误码。

01. 编码效率和冗余度

假定分组码的长度为n，其中信息位为k，相应的监督位为n - k

编码效率定义为：

$$\text{编码效率}=\frac{k}{n}$$

冗余度定义为：

$$\text{冗余度}=\frac{n-k}{k}$$

码重W

- 码组/码字中非零码元的数目；

码距d（Hamming距）

- 两码组/码字中对应码元位置上取值不同的个数称为码组/码字间的距离，简称码距；

最小码距d_{min}

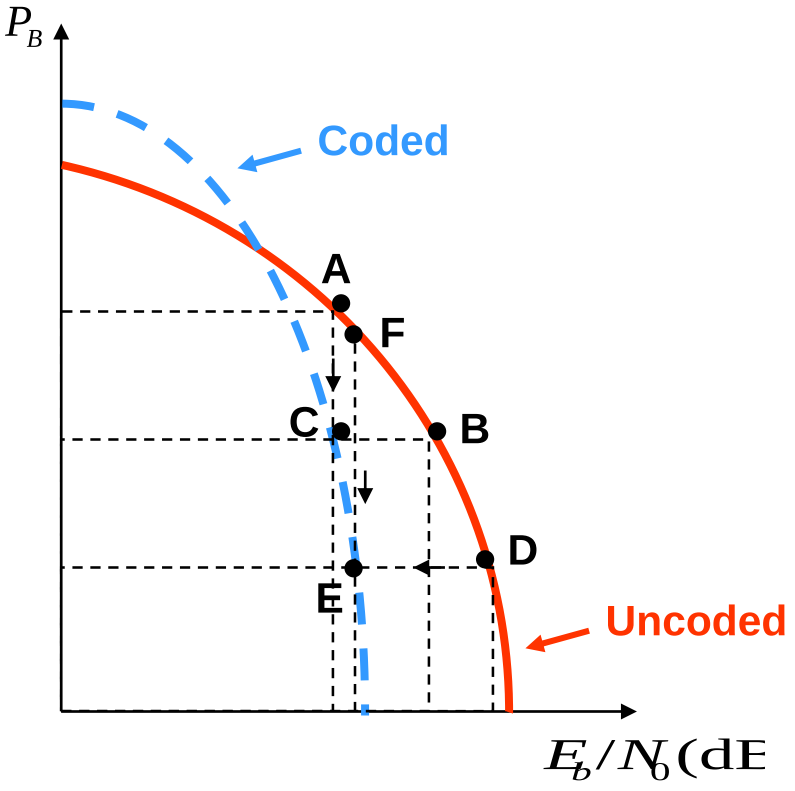
- 准用码组/码字空间中任两码组间的最小距离。

01.使用错码编码的原因

典型编码与未编码方案的差错性能比较

- 一般情况下，编码后，在同样的Eb/N0下，编码后系统有更好的性能。

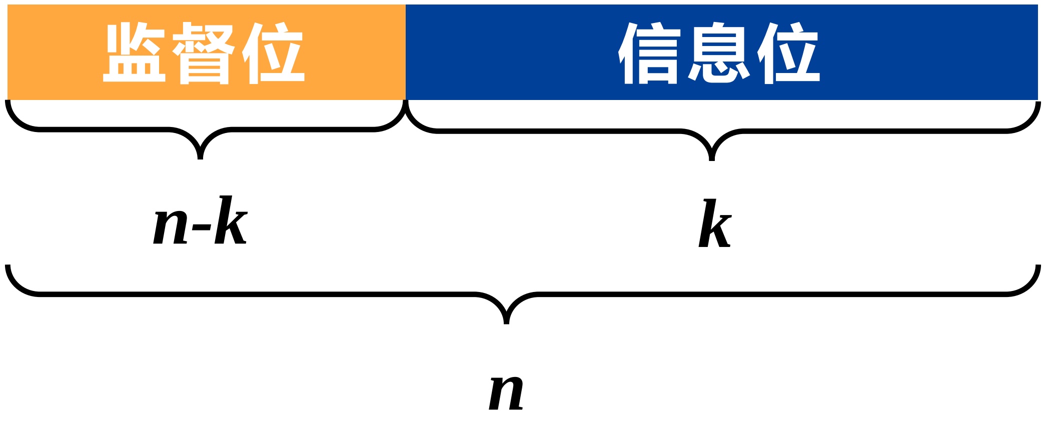
- 当Eb/N0下降到一定门限值后，编码后性能会劣化。（当Eb/N0较小时，解调器性能的下降会超过引入纠错性能的改善。）



目录

02. 线性分组码的基本概念——线性分组码的定义

- 把信源输出的k位信息序列，通过编码器产生r个监督位，输出长为$n=k+r$的码字，所得码字的全体，称为（n,k）线性分组码。
- 码组中的信息位和监督位之间的关系由线性方程确定



信息 (m_1, m_2, m_3)	码字 $(p_1, p_2, p_3, m_1, m_2, m_3)$
0 0 0	0 0 0 0 0 0
1 0 0	1 1 0 1 0 0
0 1 0	0 1 1 0 1 0
0 0 1	1 0 1 0 0 1
1 1 0	1 0 1 1 1 0
1 0 1	0 1 1 1 0 1
0 1 1	1 1 0 0 1 1
1 1 1	0 0 0 1 1 1

$$\begin{cases} p_1 = m_1 \oplus m_3 \\ p_2 = m_1 \oplus m_2 \\ p_3 = m_2 \oplus m_3 \end{cases}$$

监督位由信息位**线性组合**得到

02. 线性分组码的编码方法——生成矩阵

从（n,k）线性分组码中任取k个线性无关的码字，按行的形式写成矩阵G，则称为该线性分组码的**生成矩阵**。

信息 (m_1, m_2, m_3)	码字 $(p_1, p_2, p_3, m_1, m_2, m_3)$
0 0 0	0 0 0 0 0 0
1 0 0	1 1 0 1 0 0
0 1 0	0 1 1 0 1 0
0 0 1	1 0 1 0 0 1
1 1 0	1 0 1 1 1 0
1 0 1	0 1 1 1 0 1
0 1 1	1 1 0 0 1 1
1 1 1	0 0 1 1 1 1

$$\boldsymbol{G}=\begin{pmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}$$

生成矩阵G

$$G=\begin{pmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}=\begin{pmatrix}V_1\\V_2\\V_3\end{pmatrix}$$

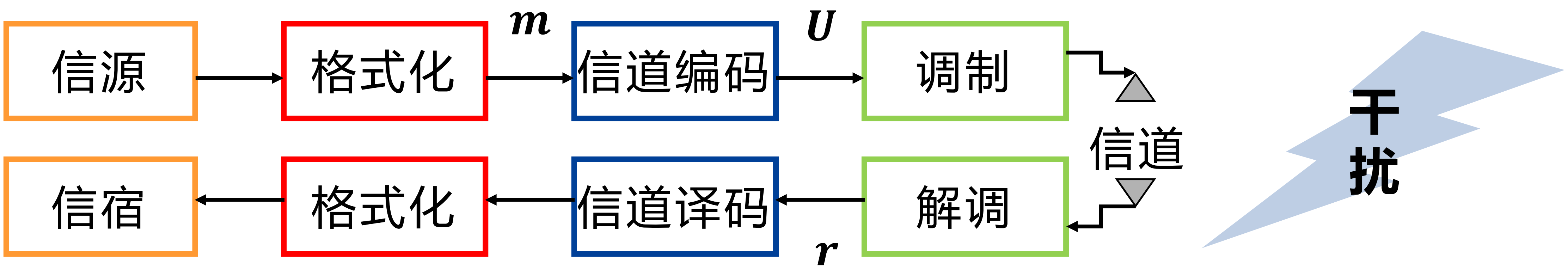
输入信息110，通过$U=mG$便能计算出编码后的码字U

$$U=m\cdot G=(1\quad 1\quad 0)\begin{pmatrix}V_1\\V_2\\V_3\end{pmatrix}=1\cdot V_1+1\cdot V_2+0\cdot V_3$$

$$=(1\quad 1\quad 0\quad 1\quad 0\quad 0)+(0\quad 1\quad 1\quad 0\quad 1\quad 0)+(0\quad 0\quad 0\quad 0\quad 0\quad 0)$$

$$=(1\quad 0\quad 1\quad 1\quad 1\quad 0)$$

02. 线性分组码的纠错译码——信道中的信息传输



当接收码字准确无误，即为101110时 → 得到信息 110

$$r = U + e$$

$r = (r_1, r_2, \dots, r_n)$，是接收码字

$e = (e_1, e_2, \dots, e_n)$，是错误图样

如何纠正错误？

当接收码字有误，即为101111时 → 得到错误信息 111

- **若（n，k）线性分组码的生成矩阵G形如**

$$G = (P \mid I_k)$$

其中G为$k \times n$阶矩阵，I_k是k阶单位阵，P为$k \times (n-k)$阶子阵

- **则其对应的监督矩阵为**

$$H = (I_{(n-k)} \mid P^T)$$

其中H为$(n-k) \times n$阶矩阵

$$GH^T = (P \mid I_k)(I_{(n-k)} \mid P^T)^T = (P \mid I_k)\begin{pmatrix} I_{(n-k)} \\ P \end{pmatrix}$$
$$= P\, I_{(n-k)} + I_k\, P = P + P = [0]$$

对于生成矩阵

$$G=\begin{pmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}$$

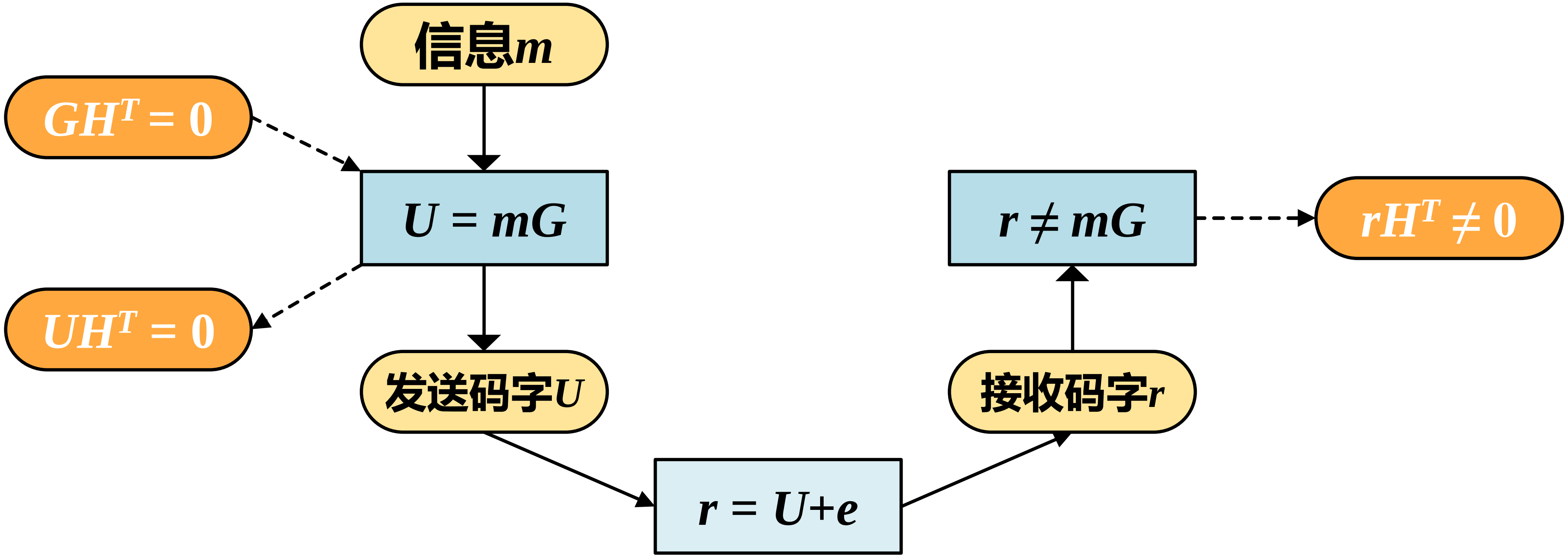
对应的监督矩阵

$$H=\begin{pmatrix}1&0&0&1&0&1\\0&1&0&1&1&0\\0&0&1&0&1&1\end{pmatrix}$$

$$GH^T=\begin{pmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&1&0\\0&1&1\\1&0&1\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}$$

信道传输引入错误图样

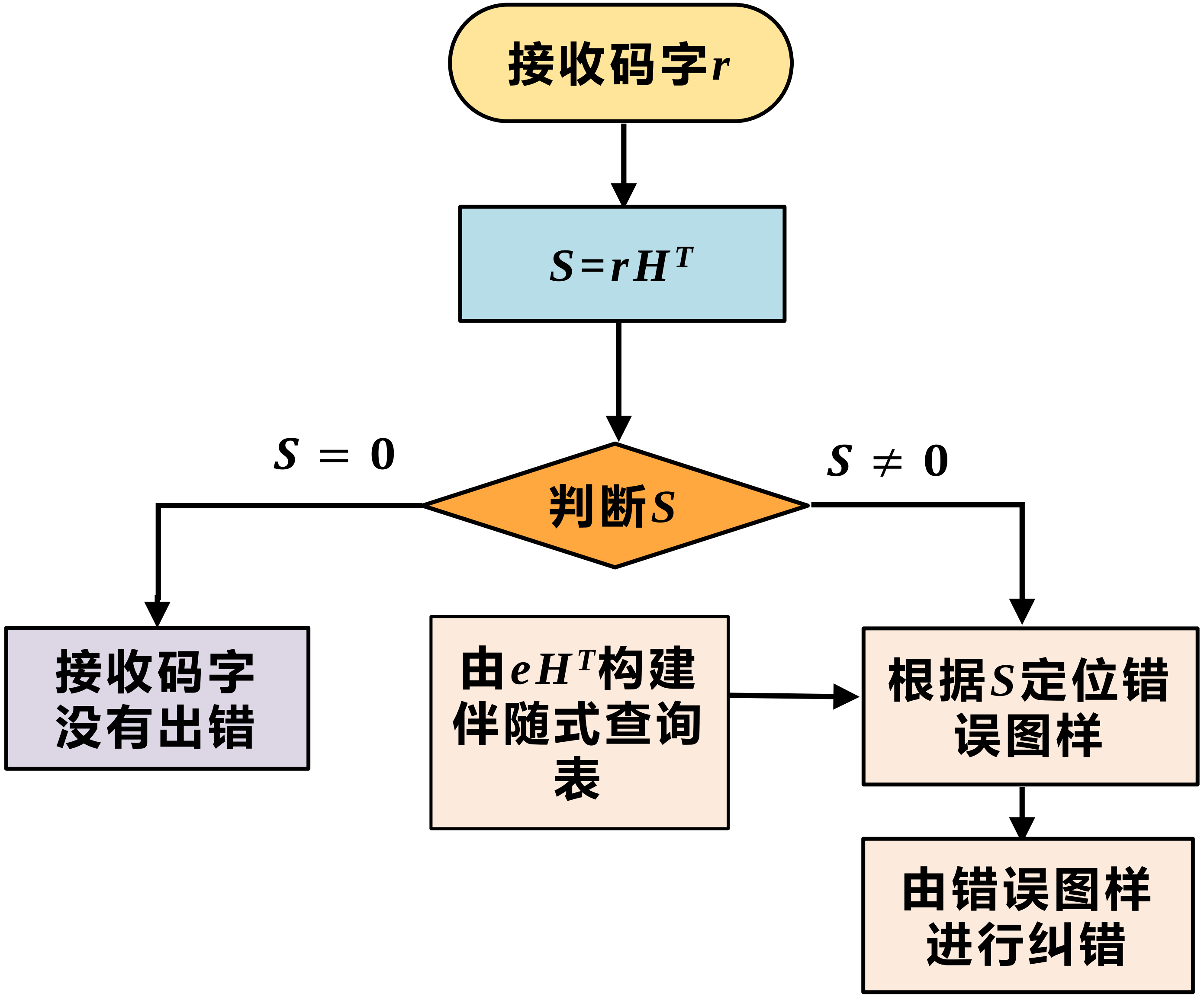
约束关系 $GH^T=0$ 被破坏



02. 线性分组码的纠错译码——(n,k) 线性分组码的译码方法

伴随式

$$
\begin{aligned}
S &= rH^T \\
&= (U+e)H^T \\
&= UH^T + eH^T \\
&= eH^T
\end{aligned}
$$



构建伴随式错误图样查询表

由$S = eH^T$计算错误图样对应的伴随式

错误图样	伴随式
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100
010001	111

(6,3)线性分组码生成矩阵

$$H^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$(0\ 0\ 0\ 0\ 0\ 1)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} = 101$$

设：　原始信息m为：　　110

发送码字U为：　　101110

接收码字r为：　　101111

$$H^T=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&1&0\\0&1&1\\1&0&1\end{pmatrix}$$

计算接收码字r的伴随式

$$S=rH^T=(1\quad 0\quad 1\quad 1\quad 1\quad 1)\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&1&0\\0&1&1\\1&0&1\end{pmatrix}=(1\quad 0\quad 1)$$

(6,3)线性分组码的伴随式查询表

错误图样	伴随式
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100
010001	111

错误图样$\hat{e}$为000001

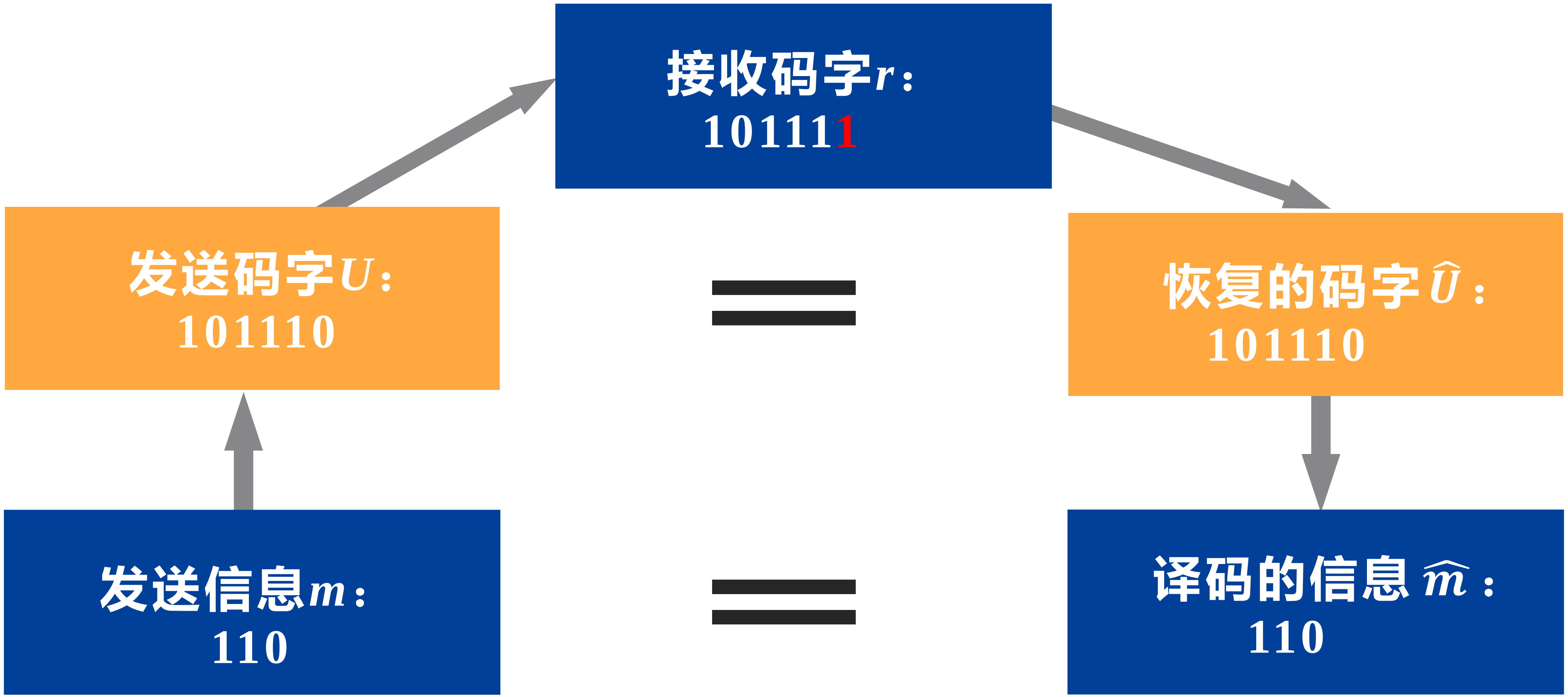
根据错误图样进行差错恢复

$$\hat{U} = r + \hat{e}$$
$$= (101111) + (000001)$$
$$= 101110$$

译码

$$\hat{U} = 101\boxed{110}$$
$$\hat{m} = 110$$

02. 线性分组码的纠错译码——（6,3）线性分组码的译码过程（3）



02. 线性分组码的检错与纠错能力

定理：任何一个（n, k）分组码，若要在任何码字内

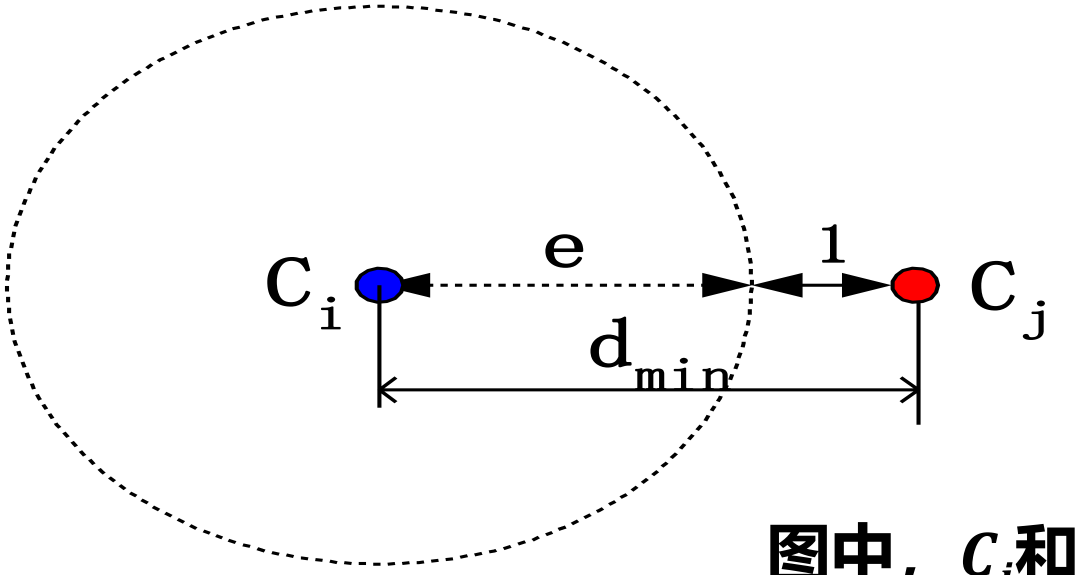
a）能检测e个随机错误，则要求最小Hamming距离$d \geq e+1$。

b）能纠正t个随机错误，则要求$d \geq 2t+1$。

c）能纠正t个随机错误，同时检测出e（≥t）个错误，则要求$d \geq t+e+1$。

要在一个码组中检出e个误码，要求 $\boxed{d_{min} \geq e+1}$

即任一码产生小于等于e个误码时，都不会变成另一准用码组。

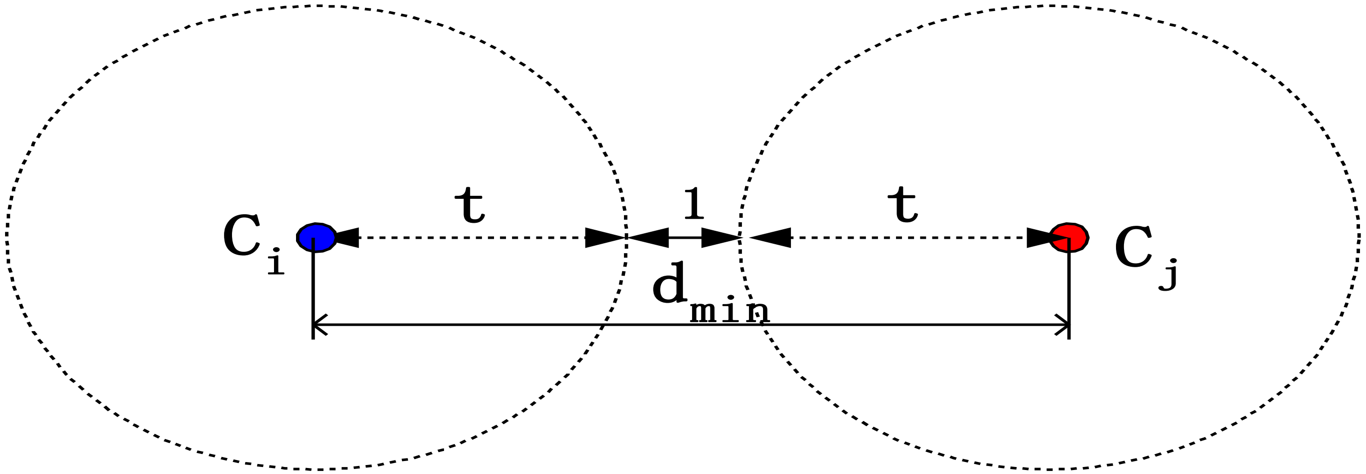


图中，C_i和C_j是两个准用码组

02. 线性分组码的检错与纠错能力

要在一个码组中能纠正t个误码，要求 $\boxed{d_{min} \geq 2t+1}$

将以t为半径的“球”内所有的禁用码组均判为球心中的准用码组，可纠正t个以内的错误。



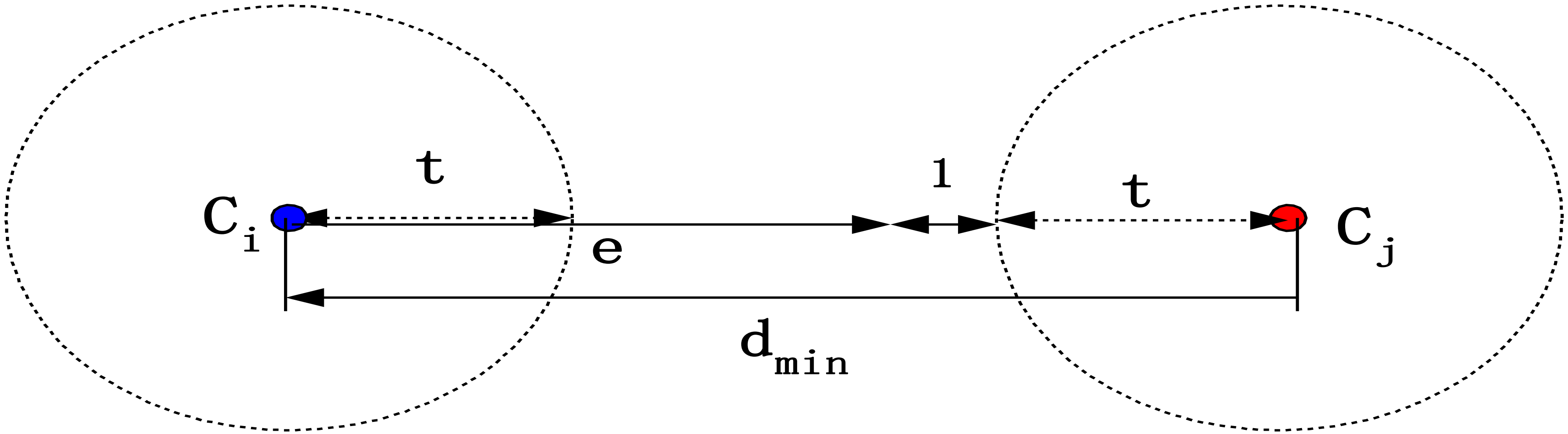
图中，C_i和C_j是两个准用码组

02. 线性分组码的检错与纠错能力

要在一个码组中能纠正t个误码，同时检出e ($e \geq t$) 个误码，要求 $\boxed{d_{min} \geq e + t + 1}$

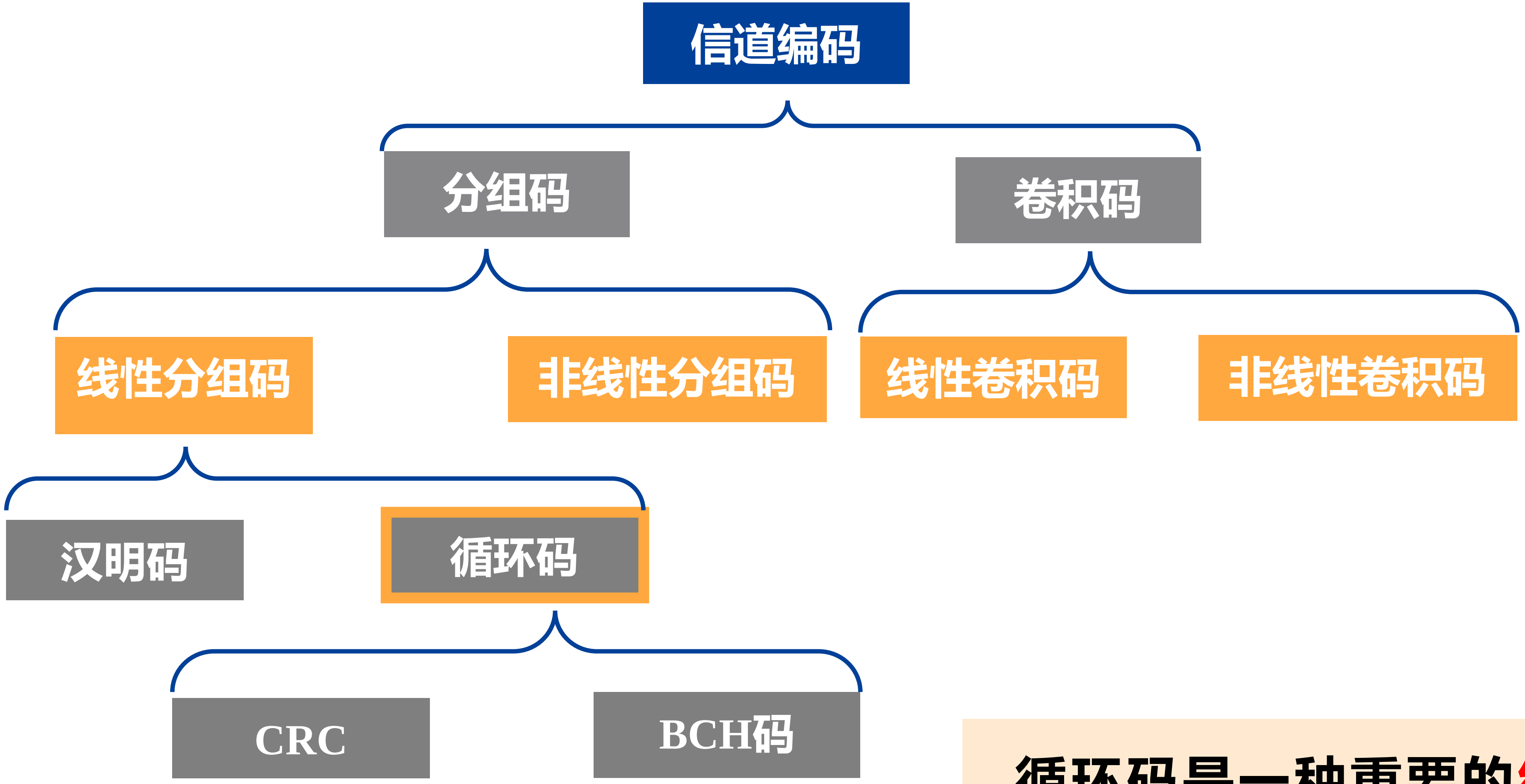
当误码数小于等于t时，可纠正；

当误码数大于 t 小于等于 e 时,不会落入另一码组的纠错范围内。



目录

03. 信道编码的分类



循环码是一种重要的**线性分组码**

循环码：

码长为n，信息位为k的(n,k)线性分组码，若具有下列属性：

如果$U=[u_0,u_1,u_2,\cdots,u_{n-1}]$是子空间$S$的一个码字，

经过i次循环移位得到的

$$U^{(i)}=[u_{n-i},u_{n-i+1},\cdots,u_{n-1},u_0,u_1,\cdots,u_{n-i-1}]$$

也是S中的一个码字（$i\geq 0$）

这种具有循环移位特点的码被称为**循环码**。

循环码是一种重要的线性分组码

010

010 1110

信息m → $U=mG$ → 发送码字U

信息m通过生成矩阵G编码为码字U

增加冗余，构建约束关系

$$U(x)\ mod\ g(x)=0$$

$g(x)$：**生成多项式**

$U(x)$：**码字多项式**

对于（7, 3）循环码，发送信息为010

- 1. 由$g(x) = x^4 + x^2 + x + 1$可得到3个多项式

$$\begin{bmatrix} x^2g(x) \\ xg(x) \\ g(x) \end{bmatrix} = \begin{bmatrix} x^6 + x^4 + x^3 + x^2 \\ x^5 + x^3 + x^2 + x \\ x^4 + x^2 + x + 1 \end{bmatrix}$$

- 2. 取多项式的系数构成矩阵，得到生成矩阵G

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

03. 循环码的编码特性 —— （7,3）循环码的编码实例（2）

对于（7, 3）循环码，发送信息为010

➢ 3. 由生成矩阵G求输入信息010的码字

$$U = mG = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

输入信息010，编码后码字为0101110

循环左移2位

输入信息011，编码后码字为0111001

03. 循环码的解码方法—— 理想信道传输（无差错传输）时的解码

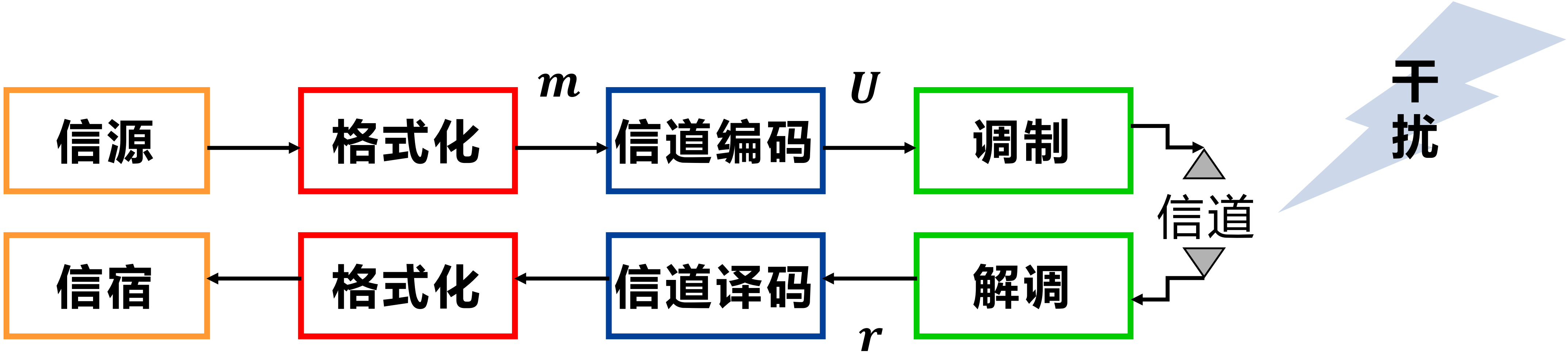
- **当接收码字准确无误，即为0101110，如何解码？**
- **约束关系：** $U(x)\ mod\ g(x) = 0$

接收码元多项式$x^5 + x^3 + x^2 + x$**，生成多项式**$x^4 + x^2 + x + 1$

$$
\begin{array}{r|l}
 & \boxed{x} \\
\cline{2-2}
x^4 + x^2 + x + 1 & x^5 \qquad + x^3 + x^2 + x \\
 & x^5 \qquad + x^3 + x^2 + x \\
\cline{2-2}
 & \qquad\qquad\qquad\qquad 0
\end{array}
$$

得到信息 010

03. 循环码的解码方法——信道传输引入错误图样



$$r = U + e$$

$r = (r_1, r_2, \dots, r_n)$，是接收码字

$e = (e_1, e_2, \dots, e_n)$，是错误图样

当接收码字出现错误，即为1101110

码元多项式$x^6+x^5+x^3+x^2+x$，生成多项式x^4+x^2+x+1

$$
\begin{array}{r|l}
 & \boxed{x^2+x+1} \\
\hline
x^4+x^2+x+1 & x^6+x^5+x^3+x^2+x \\
 & x^6+x^4+x^3+x^2 \\
\hline
 & x^5+x^4+x \\
 & x^5+x^3+x^2+x \\
\hline
 & x^4+x^3+x^2 \\
 & x^4+x^2+x+1 \\
\hline
 & x^3+x+1
\end{array}
$$

无法得到正确信息

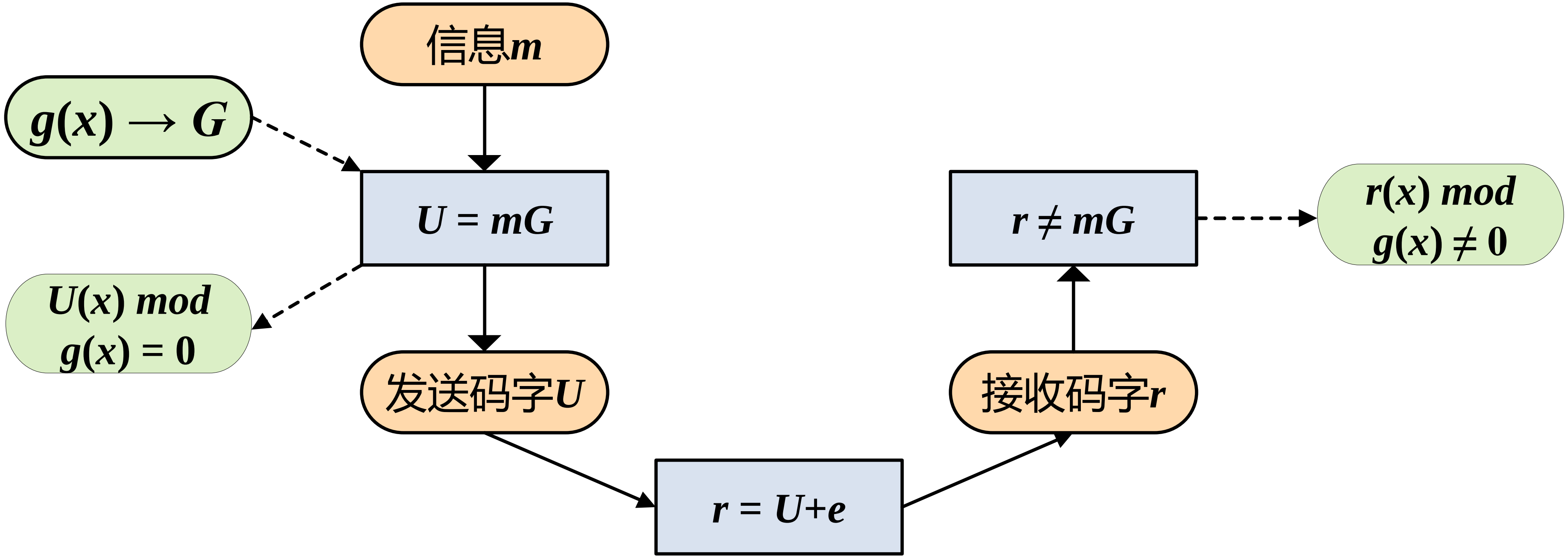
如何纠正错误?

不满足：$U(x)\ mod\ g(x)=0$

03.循环码的解码方法——错误图样引起约束关系破坏

信道传输引入错误图样

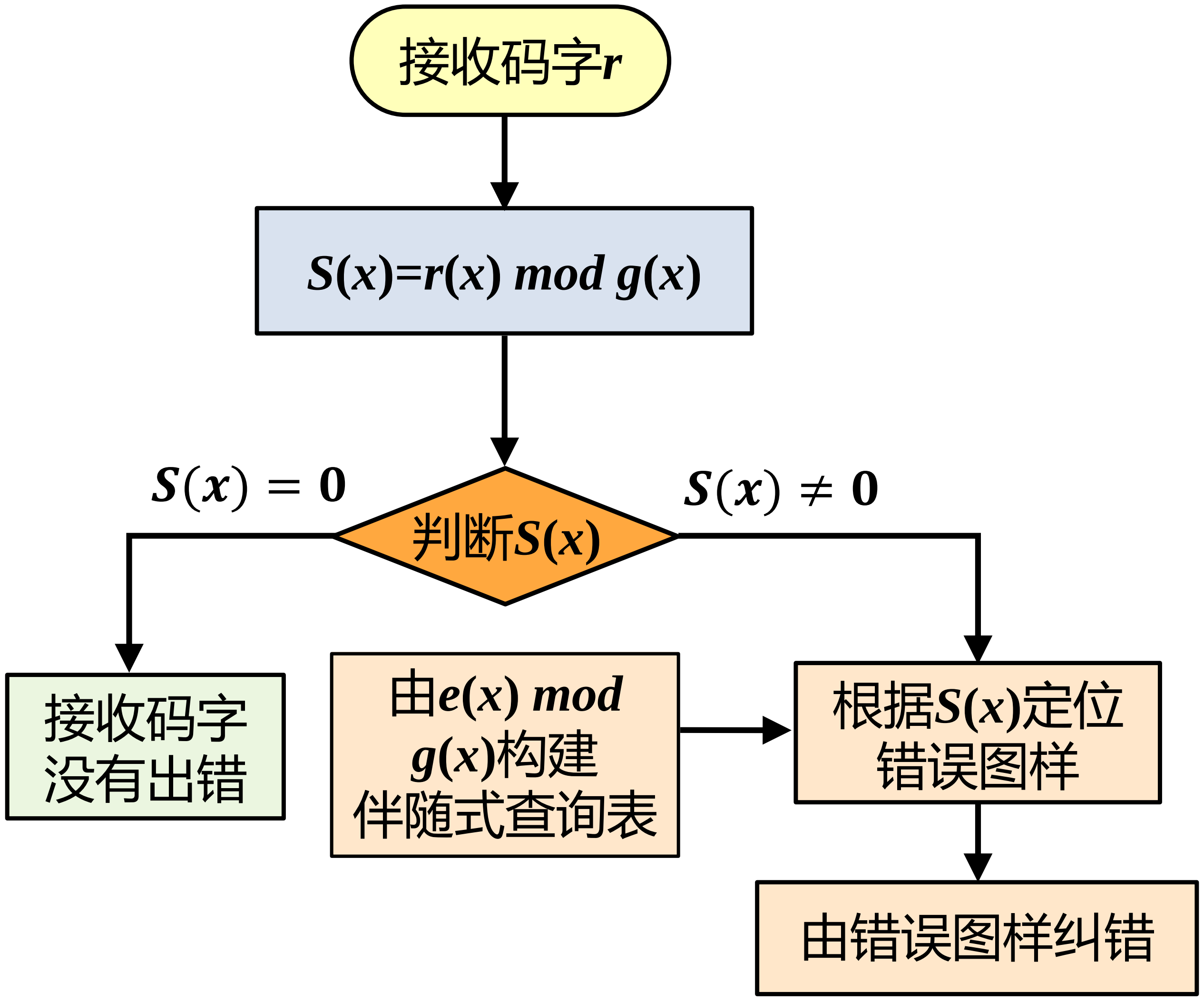
约束关系$U(x)\ mod\ g(x) = 0$被破坏



伴随式

伴随式可以由$r(x)$对生成多项式$g(x)$取模计算得到

$$\begin{aligned} S(x) &= r(x)\ mod\ g(x) \\ &= [U(x)+e(x)]\ mod\ g(x) \\ &= e(x)\ mod\ g(x) \end{aligned}$$



03.循环码的解码方法——伴随式错误图样查询表

构建伴随式错误图样查询表

➢ （7，3）循环码的生成多项式为$g(x) = x^4 + x^2 + x + 1$

➢ 由$S(x) = e(x)\ mod\ g(x)$计算各个错误图样多项式对应的伴随式

错误图样e	错误图样多项式$e(x)$	伴随式$S(x)$
1000000	x^6	$x^3 + x + 1$
0100000	x^5	$x^3 + x^2 + x$
0010000	x^4	$x^2 + x + 1$
0001000	x^3	x^3
0000100	x^2	x^2
0000010	x	x
0000001	1	1

$$x^2 + 1$$

$$x^4 + x^2 + x + 1 \ \big)\ x^6$$

$$x^6 + x^4 + x^3 + x^2$$

$$x^4 + x^3 + x^2$$

$$x^4 + x^2 + x + 1$$

$$x^3 + x + 1$$

03.循环码的编解码实例 —— 伴随式

设：发送码字U为：**0101110**

接收码字r为 ：**1101110**

$$g(x) = x^4 + x^2 + x + 1$$

计算接收码字r的伴随式

$$S(x) = r(x)\ mod\ g(x)$$

$$= (x^6+x^5+x^3+x^2+x)$$

$$mod(x^4+x^2+x+1)$$

$$= x^3+x+1$$

$$
\begin{array}{r}
x^2+x+1 \\
x^4+x^2+x+1 \overline{)\, x^6+x^5+x^3+x^2+x} \\
x^6+x^4+x^3+x^2 \\
\hline
x^5+x^4+x \\
x^5+x^3+x^2+x \\
\hline
x^4+x^3+x^2 \\
x^4+x^2+x+1 \\
\hline
x^3+x+1
\end{array}
$$

03.循环码的编解码实例—— 差错恢复

在伴随式查询表中寻找错误图样

错误图样	错误图样多项式	伴随式
1000000	x^6	x^3+x+1
0100000	x^5	x^3+x^2+x
0010000	x^4	x^2+x+1
0001000	x^3	x^3
0000100	x^2	x^2
0000010	x	x
0000001	1	1

错误图样$\hat{e}$为1000000

根据错误图样进行差错恢复

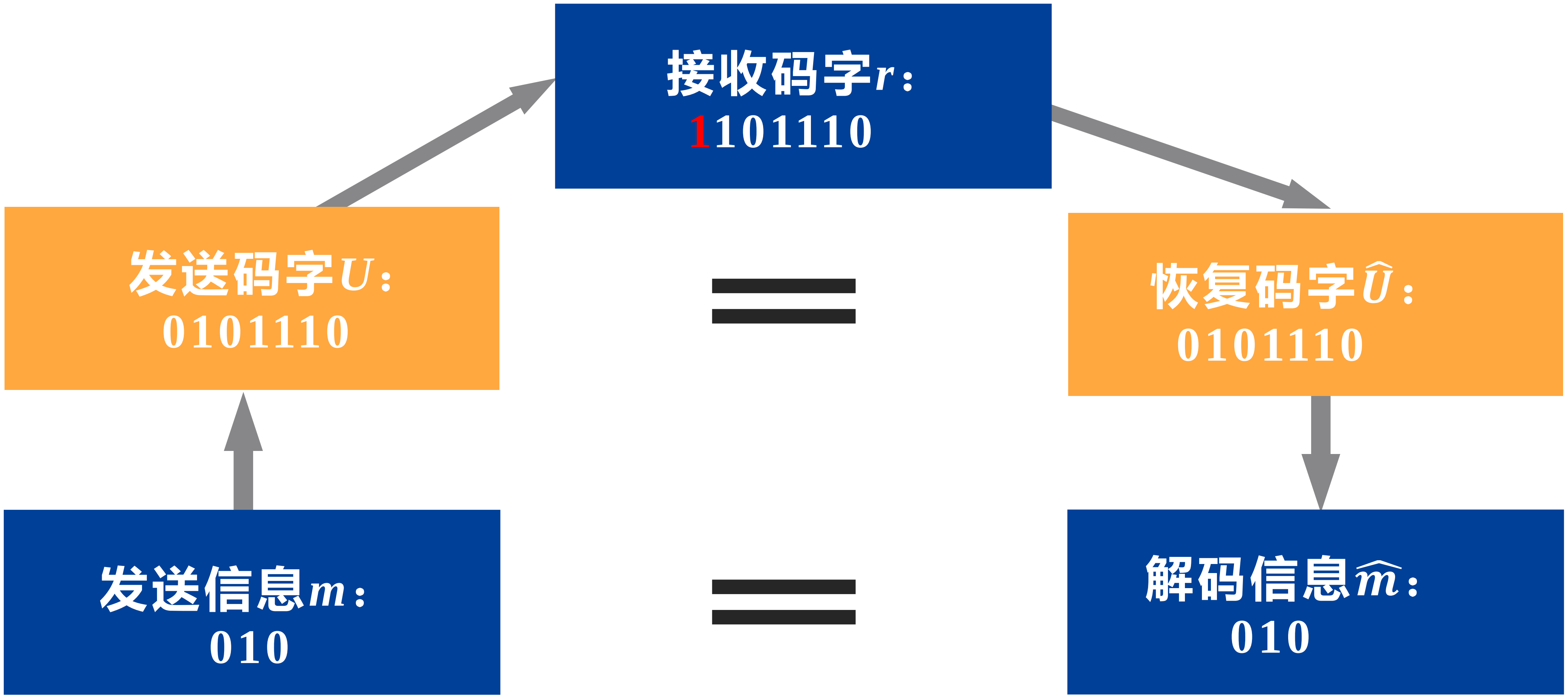
$$\hat{U} = r + \hat{e} = (1101110) + (1000000) = (0101110)$$

解码

$$\hat{m}(x) = \hat{U}(x)\ mod\ g(x) = \left(x^5 + x^3 + x^2 + x\right) mod \left(x^4 + x^2 + x + 1\right) = x$$

$$\hat{m} = 010$$

03.循环码的编解码实例



03. 循环码的应用 —— CRC码的特点及其应用

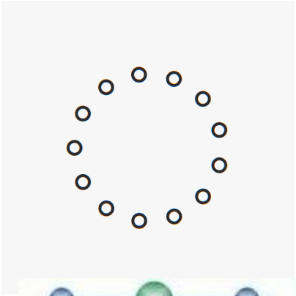
CRC的特点

- 检错能力极强
- 开销很小
- 易于实现

CRC的应用

- ZIP压缩软件使用CRC-32

- GIF等图像存储格式



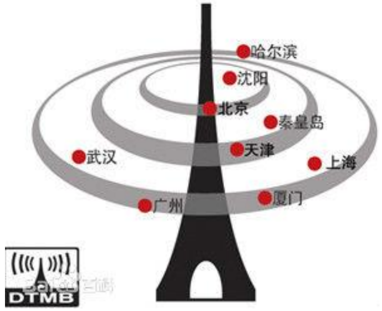
- 链路层接口协议

03. 循环码的应用 —— BCH码的应用

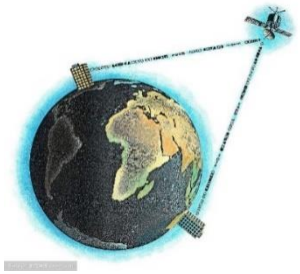
BCH码的应用

- 数字机顶盒的编解码模块

- DTMB数字电视地面广播系统的编码模块



- 卫星通信的编解码模块



03. 循环码的应用 —— 纠错解码效果

011010100111010……

干扰/噪声

011010100111010……

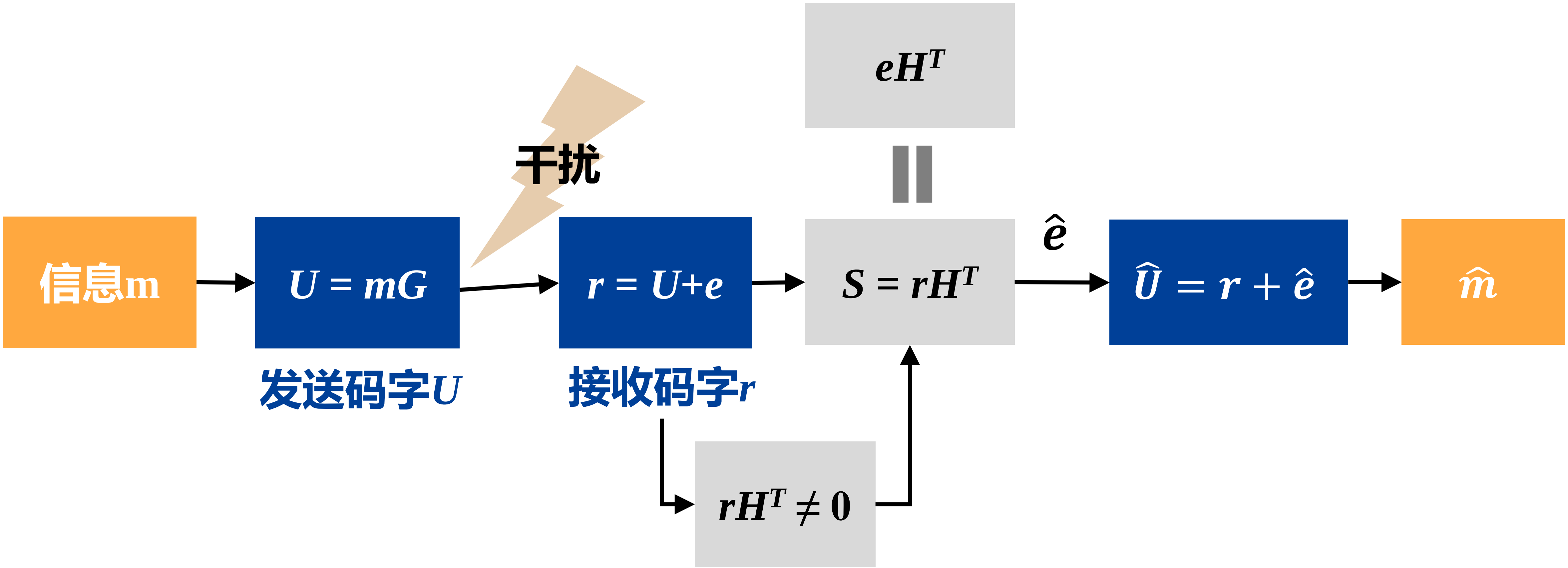
纠错译码后：

目录

04. 总结

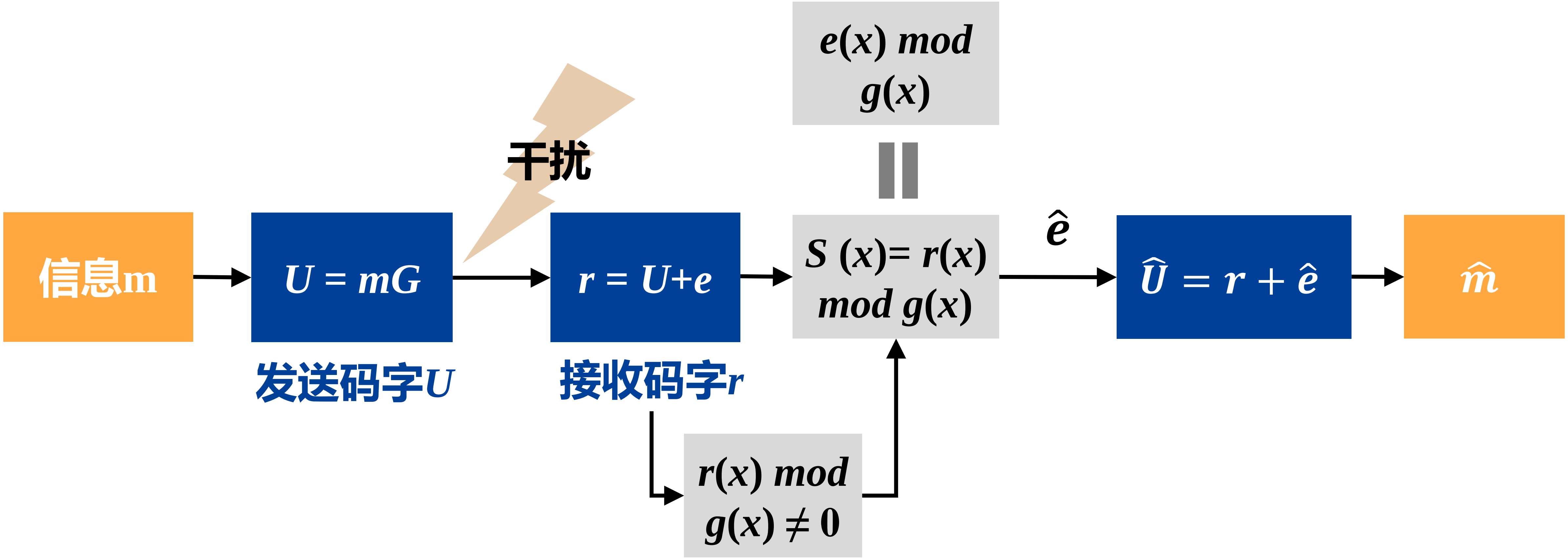
结合编码时引入的约束关系 $GH^T = 0$ 进行纠错译码

线性分组码



结合编码时引入的约束关系进行纠错解码

循环码



阅读与思考

阅读文献后回答：信道编码在非易失存储器中有什么作用？

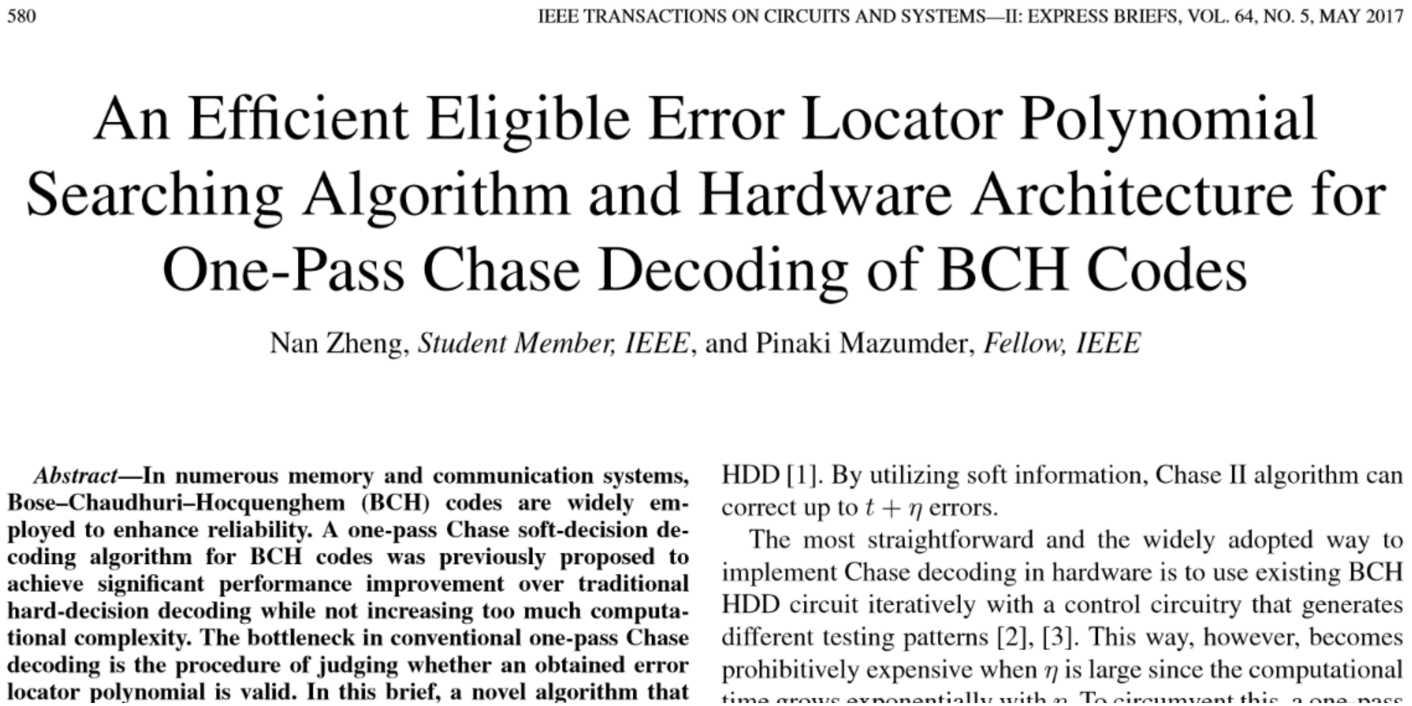
Channel Coding for Nonvolatile Memory Technologies: Theoretical Advances and Practical Considerations

By LARA DOLECEK, *Senior Member IEEE*, AND YUVAL CASSUTO, *Senior Member IEEE*

ABSTRACT | Every bit of information in a storage or memory device is bound by a multitude of performance specifications, and is subject to a variety of reliability impediments. At the other end, the physical processes tamed to remember our bits offer a constant source of risk to their reliability. These include a variety of noise sources, access restrictions, intercell interferences, cell variabilities, and many more issues. Tying together this vector of lies an interesting theoretical framework, building on deep ideas from mathematics and the information sciences. We also survey some of the most fascinating bridges between deep theory and storage performance. While the focus of this survey is primarily on the pervasive multilevel NAND Flash, we envision that other benefiting memory technologies will include phase change memory, resistive memories, and others.

L.Dolecek, and Yuval Cassuto. "Channel Coding for Nonvolatile Memory Technologies: Theoretical Advances and Practical Considerations." *Proceedings of the IEEE* 105.9 (2017): 1705-1724.

阅读文献后回答：BCH循环码解码硬件电路如何实现？



580 IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 64, NO. 5, MAY 2017

An Efficient Eligible Error Locator Polynomial Searching Algorithm and Hardware Architecture for One-Pass Chase Decoding of BCH Codes

Nan Zheng, *Student Member, IEEE*, and Pinaki Mazumder, *Fellow, IEEE*

***Abstract*—In numerous memory and communication systems, Bose–Chaudhuri–Hocquenghem (BCH) codes are widely employed to enhance reliability. A one-pass Chase soft-decision decoding algorithm for BCH codes was previously proposed to achieve significant performance improvement over traditional hard-decision decoding while not increasing too much computational complexity. The bottleneck in conventional one-pass Chase decoding is the procedure of judging whether an obtained error locator polynomial is valid. In this brief, a novel algorithm that**

HDD [1]. By utilizing soft information, Chase II algorithm can correct up to $t + \eta$ errors.

The most straightforward and the widely adopted way to implement Chase decoding in hardware is to use existing BCH HDD circuit iteratively with a control circuitry that generates different testing patterns [2], [3]. This way, however, becomes prohibitively expensive when η is large since the computational

Zheng, Nan, and Pinaki Mazumder. "An Efficient Eligible Error Locator Polynomial Searching Algorithm and Hardware Architecture for One-Pass Chase Decoding of BCH Codes." IEEE Transactions on Circuits and Systems II: Express Briefs 64.5 (2017): 580-584.

课后作业

6.21：（15,5）循环码生成多项式如下：

$$g(X) = 1 + X + X^2 + X^5 + X^8 + X^{10}$$

a）画出该码的编码器框图

b）求出消息$m(X) = 1 + X^2 + X^4$的码多项式（系统形式）

c） $V(X) = 1 + X + X^4$生成的（15,11）循环码

谢谢！