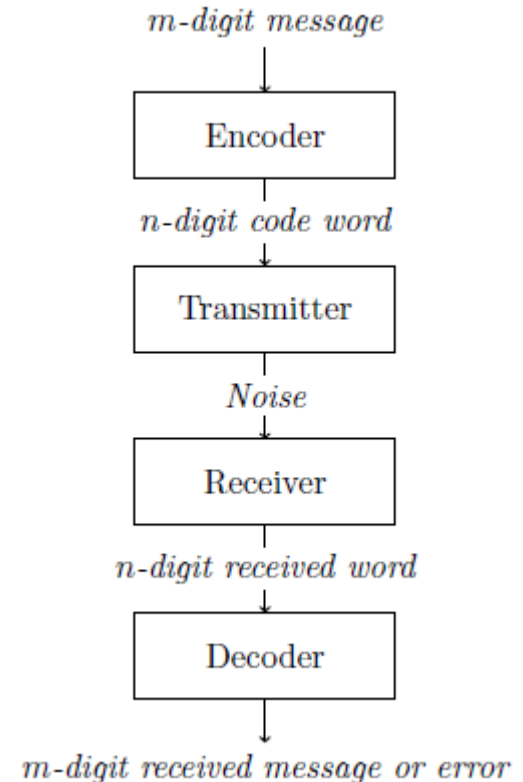
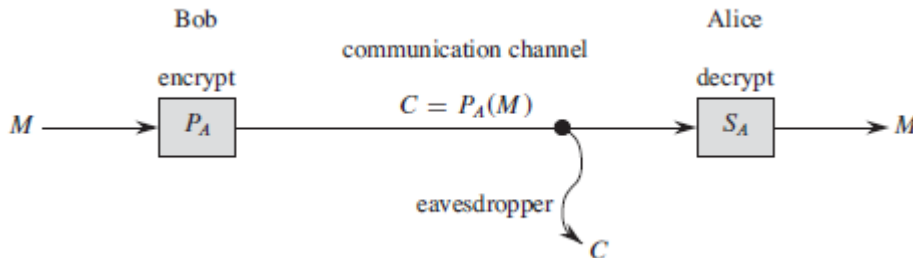


- 教材讨论
– TJ第8章

问题1： 编码

- 同样是“编码→信道→解码”，你认为这两周讨论的问题有哪些区别？
- 你能结合这两个公式解释编码、查错、解码的具体步骤吗？
 - $Gx=y$
 - $Hy=0$



问题2：奇偶校验

- 上周我们提到过简单的奇偶校验码(m+1)，现在你对它有什么新的认识？你能用这周所学内容来解释它吗？

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

$$\mathbf{x} = (x_1, x_2, x_3, x_4, x_5, x_6)^T$$

$$\mathbf{0} = H\mathbf{x} = \begin{pmatrix} x_2 + x_3 + x_4 \\ x_1 + x_2 + x_5 \\ x_1 + x_3 + x_6 \end{pmatrix}$$

$$H = (1 \ 1 \ 1 \ 1)$$

$$\mathbf{x} = (x_1, x_2, x_3, x_4)^T$$

$$0 = H\mathbf{x} = x_1 + x_2 + x_3 + x_4$$

Theorem 8.7 *Let $H \in \mathbb{M}_{m \times n}(\mathbb{Z}_2)$ be a canonical parity-check matrix. Then $\text{Null}(H)$ consists of all $\mathbf{x} \in \mathbb{Z}_2^n$ whose first $n - m$ bits are arbitrary but whose last m bits are determined by $H\mathbf{x} = \mathbf{0}$. Each of the last m bits serves as an even parity check bit for some of the first $n - m$ bits. Hence, H gives rise to an $(n, n - m)$ -block code.*

问题2: 奇偶校验 (续)

- 现在, 你学习Hamming code是不是更容易了?

The following general algorithm generates a single-error correcting (SEC) code for any number of bits.

1. Number the bits starting from 1: bit 1, 2, 3, 4, 5, etc.
2. Write the bit numbers in binary: 1, 10, 11, 100, 101, etc.
3. All bit positions that are powers of two (have only one 1 bit in the binary form of their position) are parity bits: 1, 2, 4, 8, etc. (1, 10, 100, 1000)
4. All other bit positions, with two or more 1 bits in the binary form of their position, are data bits.
5. Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.

Bit position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Encoded data bits	p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8	d9	d10	d11	p16	d12	d13	d14	d15
Parity bit coverage	p1	X		X		X		X		X		X		X		X		X		X
	p2		X	X			X	X			X	X			X	X			X	X
	p4				X	X	X	X				X	X	X	X					X
	p8								X	X	X	X	X	X	X					
	p16																X	X	X	X

- Hamming code怎么编码? 怎么解码? 怎么查错? 怎么纠错?
- 同样是奇偶校验码, m+1和Hamming code各有什么优缺点?

问题2: 奇偶校验 (续)

- 如果我们用Hamming code将4位数据编码为7位, 你能根据G和H在编码、查错、解码中的用法, 直接写出Hamming code对应的G和H吗?

Bit position	1	2	3	4	5	6	7	
Encoded data bits	p1	p2	d1	p4	d2	d3	d4	
Parity bit	p1	X		X		X		X
	p2		X	X			X	X
	p4				X	X	X	X

$$\mathbf{x}=(d1,d2,d3,d4)^T$$

$$\mathbf{y}=(p1,p2,d1,p4,d2,d3,d4)^T$$

G

1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	1

H

1	0	1	0	1	0	1
0	1	1	0	0	1	1
0	0	0	1	1	1	1

- 你的结果和教材中的形式相符吗? 如果不, 你能解释吗?

$$H = (A \mid I_m)$$

$$G = \begin{pmatrix} I_{n-m} \\ A \end{pmatrix}$$

问题3: linear code

- 实际上我们只是要找一种奇偶校验码，为什么要刻意选择 linear code，它的特殊性质能给我们带来什么好处？

问题3: linear code (续)

A code is a *linear code* if it is determined by the null space of some matrix $H \in \mathbb{M}_{m \times n}(\mathbb{Z}_2)$.

- 你觉得“linear”在这里是什么意思？
 - codeword的linear combination仍是codeword
 - 即：所有codeword构成了一个linear subspace
- linear subspace和null space of matrix之间有什么关系？
 - 每个linear subspace都可以表示为某个矩阵的null space
- 现在你感觉到linear code的第一个好处了吗？
 - 查错很方便： $Hy=0$

问题3: linear code (续)

- “linear”这个性质，在这个定理证明的哪一步中被用上了？你能解释每一步推导的理由吗？

Theorem 8.5 *Let d_{\min} be the minimum distance for a group code C . Then d_{\min} is the minimum of all the nonzero weights of the nonzero codewords in C . That is,*

$$d_{\min} = \min\{w(x) : x \neq 0\}.$$

PROOF. Observe that

$$\begin{aligned} d_{\min} &= \min\{d(x, y) : x \neq y\} \\ &= \min\{d(x, y) : x + y \neq 0\} \\ &= \min\{w(x + y) : x + y \neq 0\} \\ &= \min\{w(z) : z \neq 0\}. \end{aligned}$$

- 你感受到这个定理的重大意义了吗？这就是linear code的第二个好处！

问题4：查错和纠错

- 从查错和纠错的角度
 - $d_{\min}=1$ 意味着什么？
 - $d_{\min}=2$ 呢？
 - $d_{\min}=3$ 呢？
- 如果要求能查出所有 n 位错误， $d_{\min}=?$
- 如果要求能纠正所有 n 位错误， $d_{\min}=?$

- 在纠错时，你其实做了一个什么假设？
 - We will assume that transmission errors are rare, and, that when they do occur, they occur independently in each bit; that is, if p is the probability of an error in one bit and q is the probability of an error in a different bit, then the probability of errors occurring in both of these bits at the same time is pq . We will also assume that a received n -tuple is decoded into a codeword that is closest to it; that is, we assume that the receiver uses maximum-likelihood decoding.

问题4：查错和纠错 (续)

- H 要满足什么条件才能实现 $d_{\min}=2$? 为什么?
 $d_{\min}=3$ 呢?

$$\begin{aligned}d_{\min} &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} + \mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{x} + \mathbf{y}) : \mathbf{x} + \mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{z}) : \mathbf{z} \neq \mathbf{0}\}.\end{aligned}$$

Theorem 8.12 *Let H be an $m \times n$ binary matrix. Then the null space of H is a single error-detecting code if and only if no column of H consists entirely of zeros.*

$$H\mathbf{e}_i \neq \mathbf{0}$$

Theorem 8.13 *Let H be a binary matrix. The null space of H is a single error-correcting code if and only if H does not contain any zero columns and no two columns of H are identical.*

$$\mathbf{0} = H(\mathbf{e}_i + \mathbf{e}_j) = H\mathbf{e}_i + H\mathbf{e}_j$$

问题4：查错和纠错 (续)

Theorem 8.13 *Let H be a binary matrix. The null space of H is a single error-correcting code if and only if H does not contain any zero columns and no two columns of H are identical.*

- 因此，在满足这个条件的前提下， $H=(A||I_m)$ 最多有几列？
- 我们为什么希望列越多越好？
- 这个方法的**最大编码率**是多少？ $(2^m-(1+m)) / (2^m-1)$
- **Hamming code**的**最大编码率**又是多少？

Bit position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Encoded data bits	p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8	d9	d10	d11	p16	d12	d13	d14	d15
Parity bit coverage	p1	X		X		X		X		X		X		X		X		X		X
	p2		X	X			X	X			X	X			X	X			X	X
	p4				X	X	X	X					X	X	X	X				X
	p8								X	X	X	X	X	X	X	X				
p16																X	X	X	X	X

Block length	$2^r - 1$ where $r \geq 2$
Message length	$2^r - r - 1$
Rate	$1 - r/(2^r - 1)$

- 你能找到**编码率比Hamming code更高**的方法吗？

问题4：查错和纠错 (续)

- 如果 $H\mathbf{y} \neq \mathbf{0}$ ，我们怎么纠错，或者说，哪一位错了？为什么？

Theorem 8.15 *Let $H \in \mathbb{M}_{m \times n}(\mathbb{Z}_2)$ and suppose that the linear code corresponding to H is single error-correcting. Let \mathbf{r} be a received n -tuple that was transmitted with at most one error. If the syndrome of \mathbf{r} is $\mathbf{0}$, then no error has occurred; otherwise, if the syndrome of \mathbf{r} is equal to some column of H , say the i th column, then the error has occurred in the i th bit.*

$$H\mathbf{x} = H(\mathbf{c} + \mathbf{e}) = H\mathbf{c} + H\mathbf{e} = \mathbf{0} + H\mathbf{e} = H\mathbf{e}.$$

- 我们今天讨论了这么多，“群”去哪儿了？