Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 4. Basic Message Coding

之前只传达1个message (m=0/1)

Lecturer: Jin HUANG

↓

多个 message.

4.1 Mapping Messages into Message Vectors

Overview

编码方式

message → symbol → physical signal

One bit only to more complicated message.

- Source coding: maps messages into sequences of symbols.

  → symbol 不等于 bit

  - Direct message coding
  - Code separation
- Modulation: maps sequences of symbols into physical signals.
  - Time-division multiplexing
  - Space-division multiplexing
  - Frequency-division multiplexing
  - Code-division multiplexing

Direct Message Coding

A unique, predefined message mark $w \in \mathcal{W}$ to represent each message $m \in \mathcal{M}$.

一一对应

- One-one mapping: $|\mathcal{W}| = |\mathcal{M}|$.

Detector: maximum likelihood detection

- $w(m)$ with the highest detection value.

Design of $\mathcal{W}$

- False positive rate
- Fidelity
- Robustness
- ...

很多 message.

Code separation: far away from each other.

- To avoid confusion

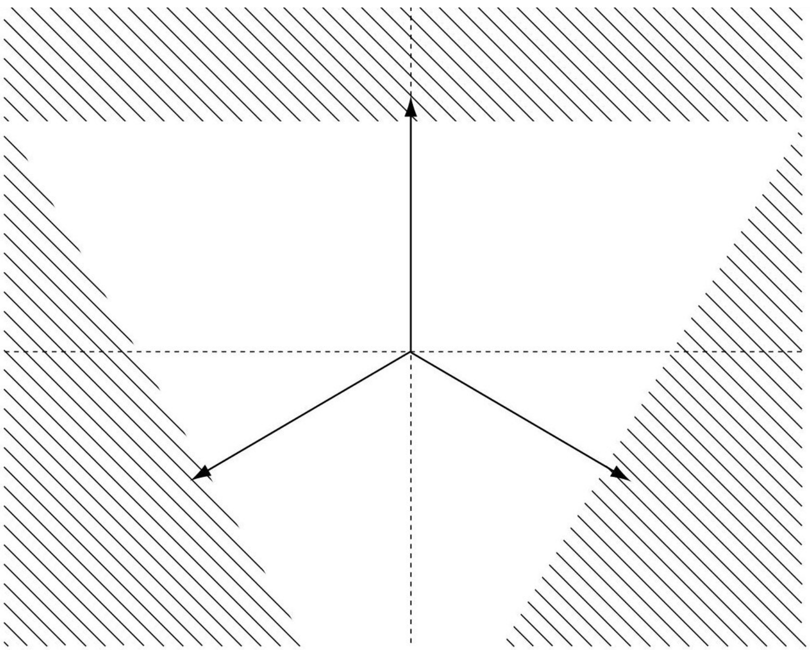
Correlation in $\mathcal{W}$

- Low correlations with one another: good.
- Negative correlation with one another: better.
  - Embedding one **decreases** the other.
  - E.g. $\underset{M}{m = \{0, 1\}} \Rightarrow (2m - 1) = \underset{W}{\{1, -1\}}$. 负相关

More Messages

Placing $|\mathcal{M}|$ points on the surface of an N-dimensional sphere.

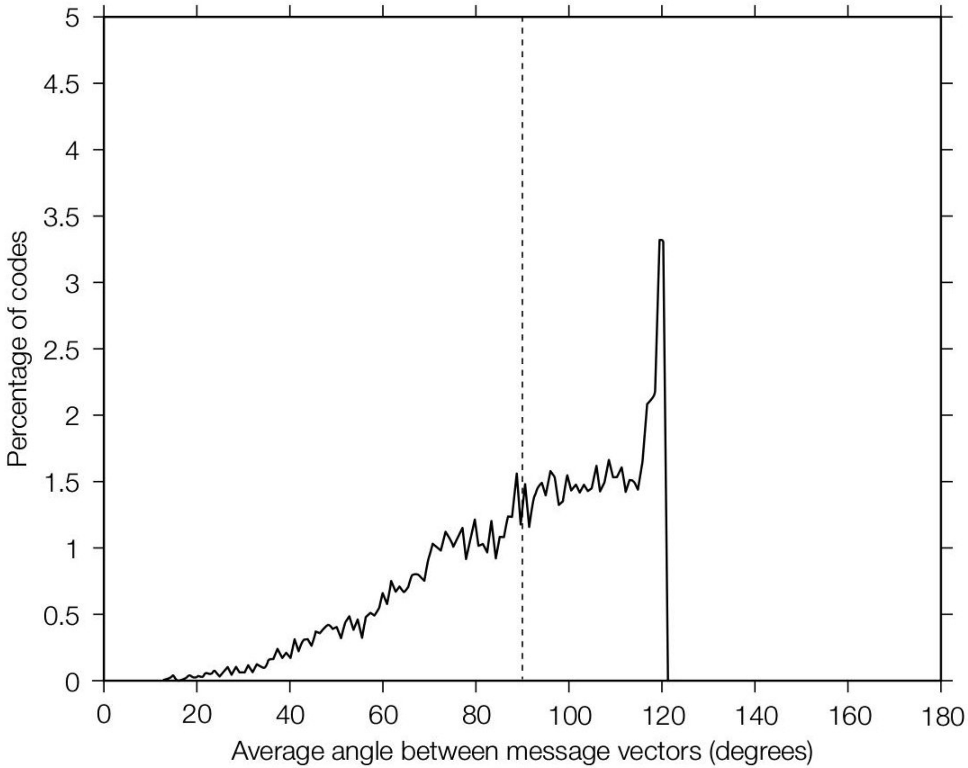
生成N个点视为负荷.



Three message mark vectors in a two-dimensional plane of marking space.

Low Dimension

$N \leq |\mathcal{M}|$: randomly generated codes are good.

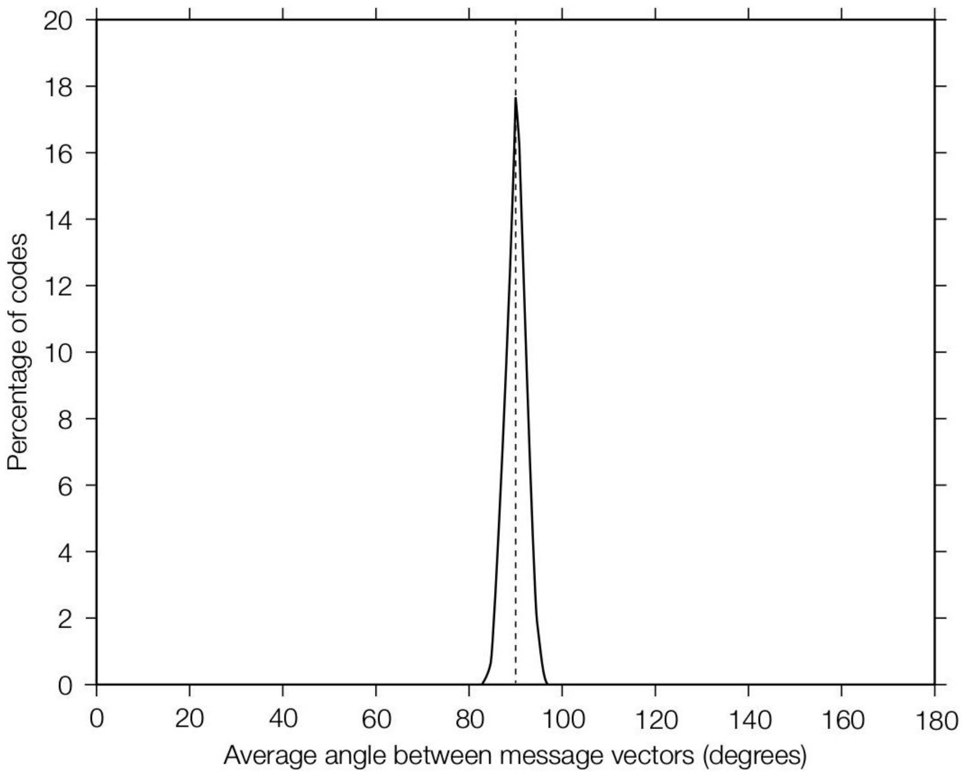


Three-message vectors in three-dimensional space.

High Dimension

$N \gg |\mathcal{M}|$: close to be orthogonal. 正交的.

最好要加上前一个的负向量.

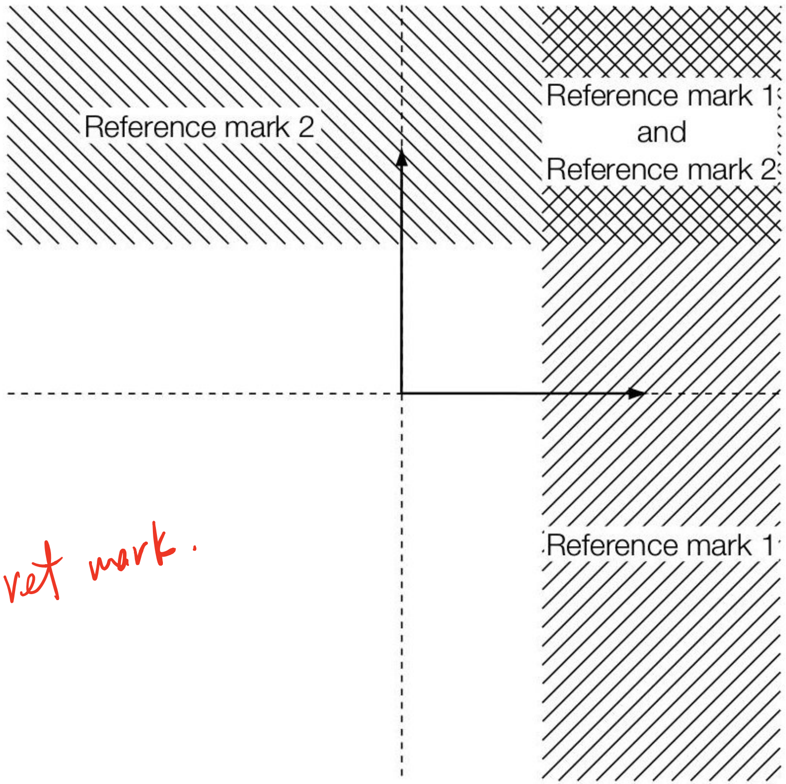


Three-message vectors in 256-dimensional space.

The Use of "Orthogonal"

Multiple messages in a work for

- Linear correlation.



携带多个 ref mark.

Multisymbol Message Coding

Direct message coding is not efficient

- Detect for **all** marks.
- For a 16 bit information: 65536.
- Detector: compare with 65536 marks.

Multisymbol Message Coding!

Sequence of Symbols

Giving an alphabet $\mathcal{A}$, a length L **sequence**:

- $|\mathcal{A}|^L$ different messages.
- Sequence: the order is important!
- Direct message coding: $L = 1$.

16 bit information

1个 symbol 2^{16} 个 alphabet $(2^{16})^1 = 2^{16}$

- $|\mathcal{A}|^1 = 65536$ for direct message coding. 比 2^{16} 次

8个 symbol 4个 alphabet. $(4)^8 = 2^{16}$

- $|\mathcal{A}|^8 = 65536$ for 4-symbol 8-length coding. 比32次
    - For each index/order: compare with 4 marks.

(alphabet 大小)

总共比较次数 = 每一位需要比较次数 * 总位数

The Index/Order

- Time-division multiplexing
- Space-division multiplexing
- Frequency-division multiplexing
- Code-division multiplexing

Time- and Space-Division Multiplexing

体现顺序性.

Divide the work into disjoint regions

- In space or time
- One symbol in each part.

Samples: A length 4 sequence.

- Audio: 4 clips in $1/4$ length.
- Image: 4 blocks in 2×2 layout.

Frequency-Division Multiplexing

Disjoint bands in the frequency domain

- One symbol in each band. 不同detector读不同band
- Frequency domain 嵌水印时改 x
  - Basis $\Phi[i]$: $\mathbf{f} = \sum_i \mathbf{x}[i]\Phi[i] = \Phi\mathbf{x}$. 频域分解.
  - Decomposition: $\mathbf{x} = \Phi^{-1}\mathbf{f}$.
  - Marking space
    - via a linear transformation $\mathcal{T}$ from media space.

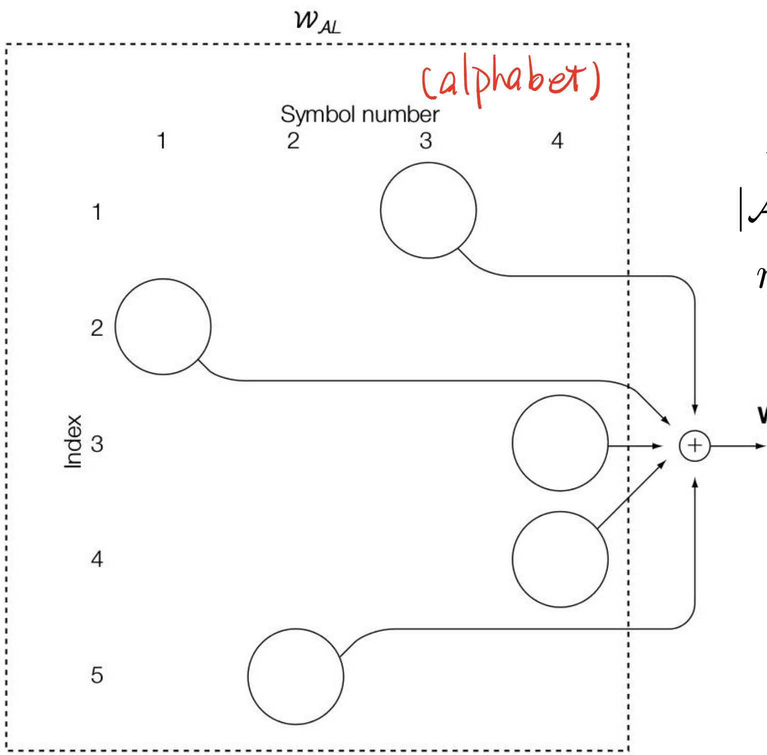
Samples:

- Audio: Fourier Transform
- Image: Discrete Cosine Transform

Code-Division Multiplexing

A table $\mathcal{W}_{\mathcal{AL}}$ in index and alphabet.

- $L \times |\mathcal{A}|$ reference marks.



$$L = 5$$
$$|\mathcal{A}| = 4$$
$$m = \text{“31442”}$$
$$\Longrightarrow$$
$$\mathbf{w}_m = \mathcal{W}_{\mathcal{AL}}[1,3] + \mathcal{W}_{\mathcal{AL}}[2,1] + \mathcal{W}_{\mathcal{AL}}[3,4] + \mathcal{W}_{\mathcal{AL}}[4,4] + \mathcal{W}_{\mathcal{AL}}[5,2].$$

Requirements on $\mathcal{W}_{\mathcal{AL}}$

Marks in $\mathbf{w}_m$:

不同行之间尽可能无关

- $m[i]$ and $m[j]$ have little correlation.
  - Close to orthogonal: concurrent presence.

$$\mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[j,b] \to 0, \text{if } i \neq j.$$

- Only one symbol in a index.

同一行内，尽可能负相关

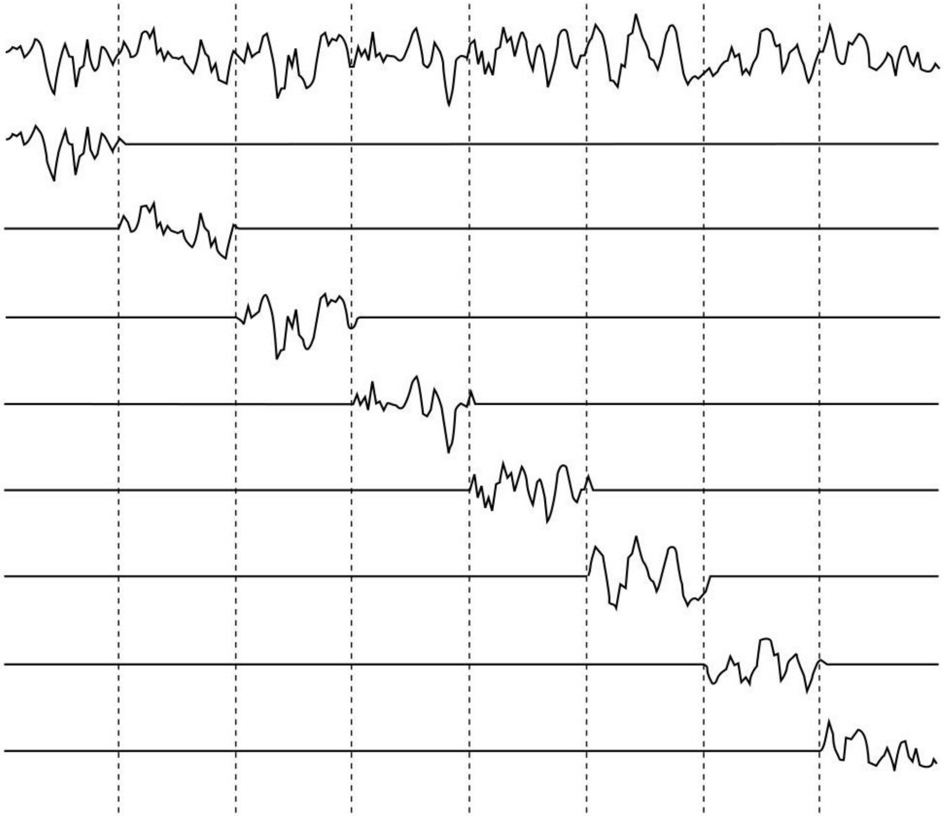
  - Negative correlation: distinguishable.

$$\mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[i,b] \to -1, \text{if } a \neq b. \qquad (1)$$

负相关

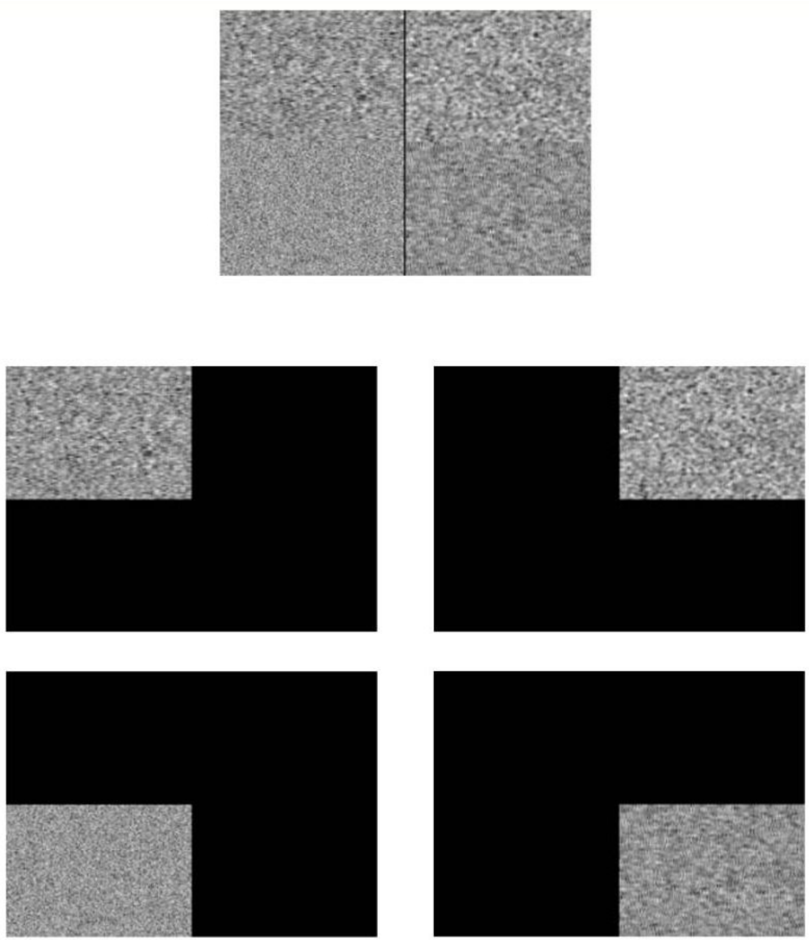
Equivalence to Time-Division

Pad the marks with zeros



Equivalence to Space-Division

Pad the marks with zeros



Equivalence to Frequency-Division

分成不同频域

Convert symbols in each band back to the temporal or spatial domains.

只在自己的频段中修改

If the transform is linear:

重叠

- Overlap in time or space.
- But zero correlation.

E_SIMPLE_8/D_SIMPLE_8 1

8位，每一位 0/1

8-bit integer: length 8 binary string,
$L = 8, |\mathcal{A}| = 2$.

- At each position
  - Distinguishable: negative correlation.
  - $\mathcal{W}_{\mathcal{AL}}[i, 1] = \mathbf{w}_{ri} = -\mathcal{W}_{\mathcal{AL}}[i, 0]$.
- Among positions
  - Gaussian distributions with zero mean.
- Normalize $\mathbf{w}_m$ to unit length. (以才有意义)

Project: System 4

E_SIMPLE_8/D_SIMPLE_8

Embedder:

- $\mathbf{c}_w = \mathbf{c}_o + \alpha \mathbf{w}_m$.

Detector:

- For each i: check $\mathbf{w}_{ri}$.
- If is not watermarked
  - The output message is random. *read 4.3*

Performance

6 8-bit integers in each of 2000 images.

- Larger embedding strength $\alpha = 2$.
  - The message pattern is scaled to have unit standard deviation, thus $\alpha/\sqrt{8}$. ?
- 26 out of 12000 are wrong: confused by $m_a, m_b, a \neq b$.
- Reason:
  - Maximum correlation between two different message vectors is high.

Presentation: Hamming

- Hamming distance.
- Hamming code.
- Strategy of using Hamming code in watermark

4.2 Error Correction Coding

Motivation

In the set of all multisymbol sequences $\mathcal{S}$.

- $\mathbf{w}_{m_a}, \mathbf{w}_{m_b}, m_a, m_b \in \mathcal{S}, a \neq b$ may be similar.

Sample

- $L = 3, |\mathcal{A}| = 4, \mathcal{W}_{\mathcal{AL}}[i,j] \cdot \mathcal{W}_{\mathcal{AL}}[i,j] = N$
  - $\mathbf{w}_{312} = \mathcal{W}_{\mathcal{AL}}[1,3] + \mathcal{W}_{\mathcal{AL}}[2,1] + \mathcal{W}_{\mathcal{AL}}[3,2]$.
  - $\mathbf{w}_{314} = \mathcal{W}_{\mathcal{AL}}[1,3] + \mathcal{W}_{\mathcal{AL}}[2,1] + \mathcal{W}_{\mathcal{AL}}[3,4]$.
  - Inner product:

$$
\begin{aligned}
&\mathcal{W}_{\mathcal{AL}}[i,a] \cdot \mathcal{W}_{\mathcal{AL}}[j,b] = 0, \quad i \neq j \\
\Longrightarrow \quad &\mathbf{w}_{312} \cdot \mathbf{w}_{314} = \mathcal{W}_{\mathcal{AL}}[1,3] \cdot \mathcal{W}_{\mathcal{AL}}[1,3] \\
&\qquad + \mathcal{W}_{\mathcal{AL}}[2,1] \cdot \mathcal{W}_{\mathcal{AL}}[2,1] \\
&\qquad + \mathcal{W}_{\mathcal{AL}}[3,2] \cdot \mathcal{W}_{\mathcal{AL}}[3,4] \\
&\qquad \geq N + N - N = N
\end{aligned}
$$

长度L序列.

L-h 相同

h个不同.

- h different symbols in a length L sequence

$$(L - 2h)N.$$

L-h 正

h 负

The Idea of Error Correction Codes

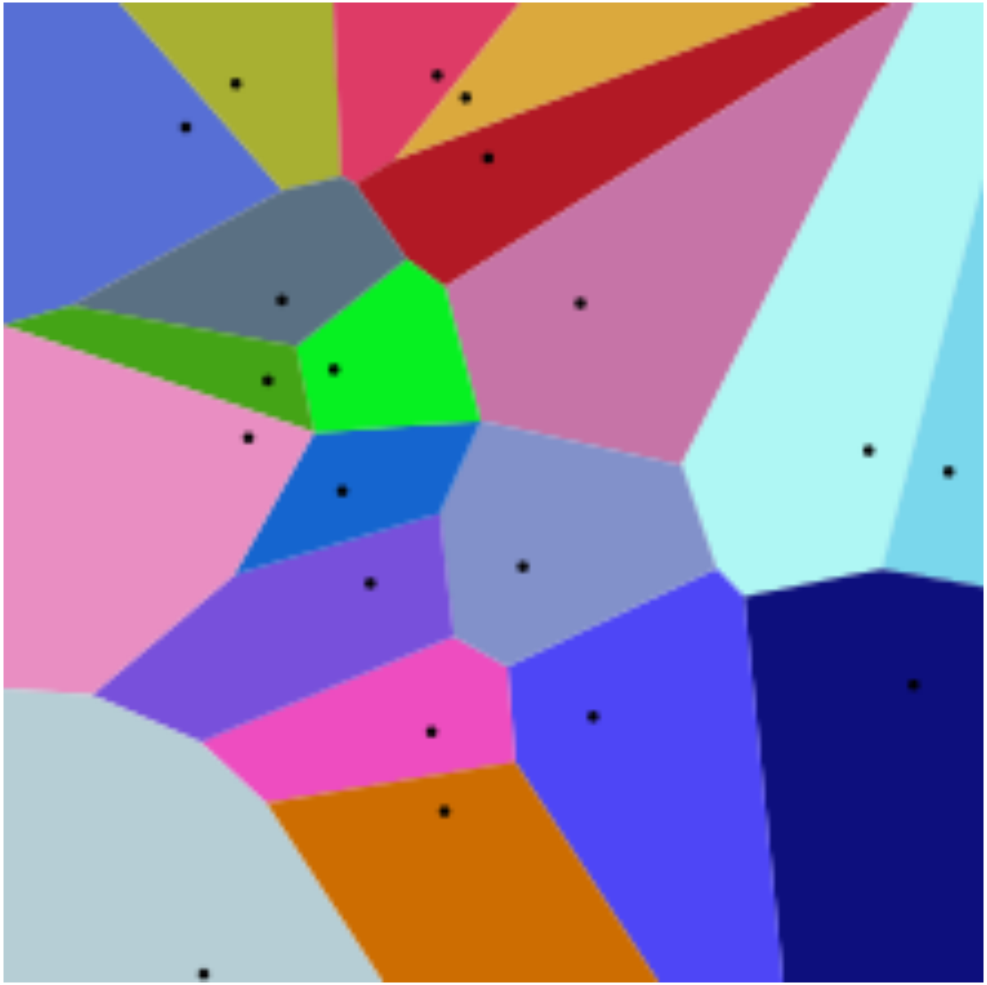
Decompose all possible sequences $\mathcal{S}$ into $\mathcal{S}_c \cup \bar{\mathcal{S}}_c$.

- $\mathcal{S}_c$: Code words 标准（无干扰）
  - Messages to encode.
  - Well separate to each other.

损坏

- $\bar{\mathcal{S}}_c$: Corrupted code words
  - Polluted messages.
  - Associated with the closest code word.

$\mathcal{S}_c \cup \bar{\mathcal{S}}_c$



Error Correction Code (ECC)

To preserve the capacity

- Increase the length of sequence.
- Expand the alphabet.

Increase the Length of Sequence

Sample

- 4-bits message set $\mathcal{M}$
  - Length 4 binary sequence, 16 messages.
- 7-bits word space $\mathcal{S}$ $L=7$ $h=3$
  - Length 7 binary sequence, 128 words.
  - $|\mathcal{S}_c| = |\mathcal{M}| = 16$.

    $L-h-h = L-2h = 7-2\times 3 = 1$
  - $a, b \in \mathcal{S}_c, a \neq b$ have at less 3 different bits.

    2位的话.
    a, b各翻一位即相同
    - Why 3? Flip one bit for each of the two.

    所以帮助不够大
  - Decode $s \in \mathcal{S}$: find $c \in \mathcal{S}_c$ has at most one different bit.

quiz

$L = 2^{n-1}$

$|A| = 2$

$x \leq \frac{1}{2}$

$m = 2^L$

$1 + x + \frac{1}{2}(x-1)x$

$2^L (C_x^0 + C_x^1 + \cdots + C_x^n) \leq 2^x$