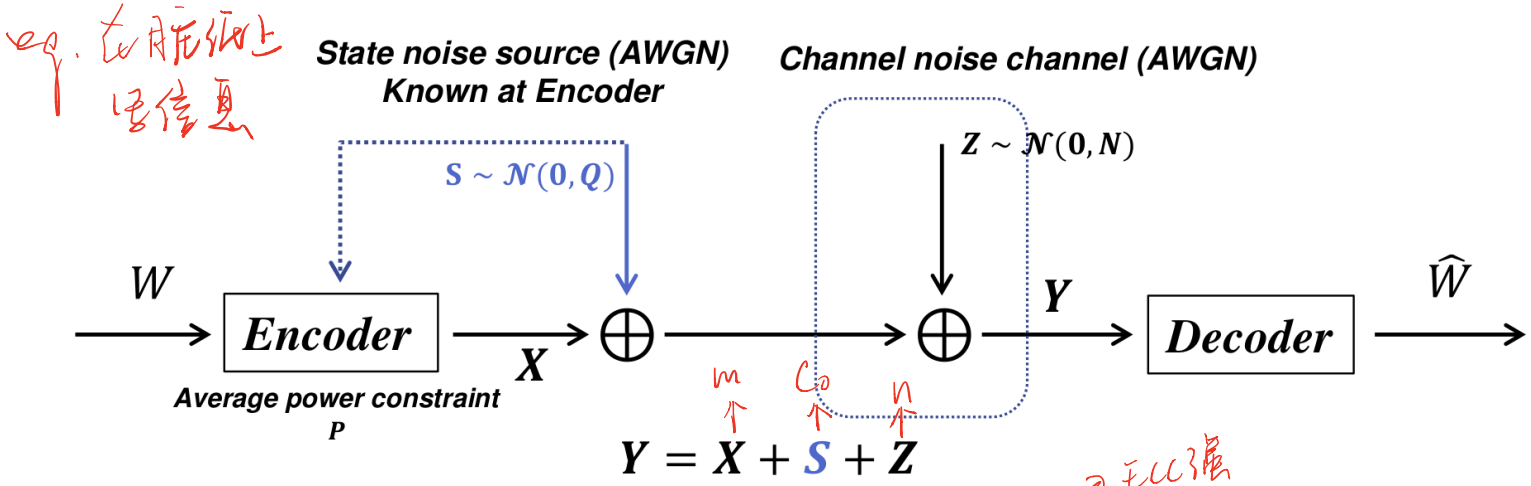
5.2 Watermarking Using Side Information

An Interesting Question

- We have a piece of paper covered with independent dirt spots ... and we write a message on it with a limited amount of ink.
- The dirty paper, with the message on it, is then sent to someone else, and acquires more ... dirt along the way.
- If the recipient cannot distinguish between the ink and the dirt, how much information can we reliably send?



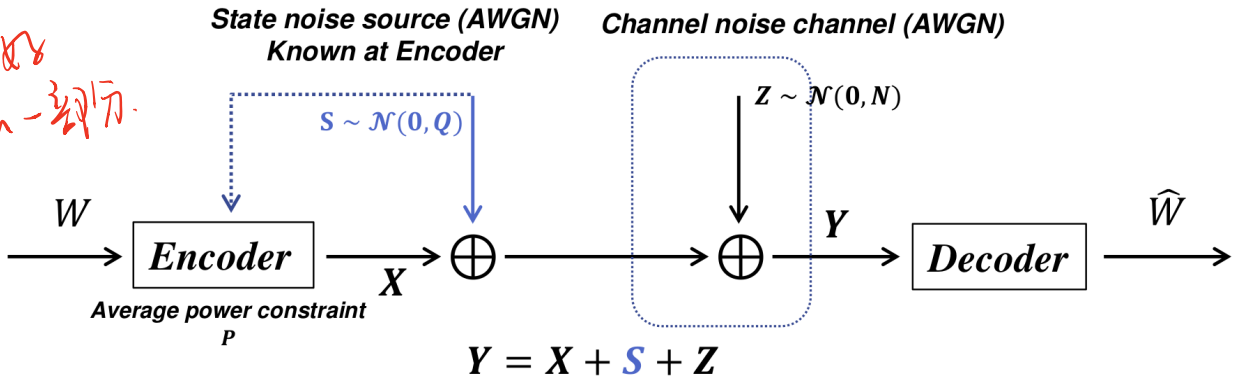
Costa's idea: $R = \frac{1}{2} \ln \left(1 + \frac{P}{N+Q}\right)$?

Shannon-Hartley Theorem

- A paper sent along a path that picks up less dirt can reliably deliver more information than another paper sent along a path that picks up more dirt.
- Error detection and correction.
- Most people expected that the same thing would happen when dirt is added to the paper **before the message was written**-the more dirt, the less information can be reliably sent.

The surprising result

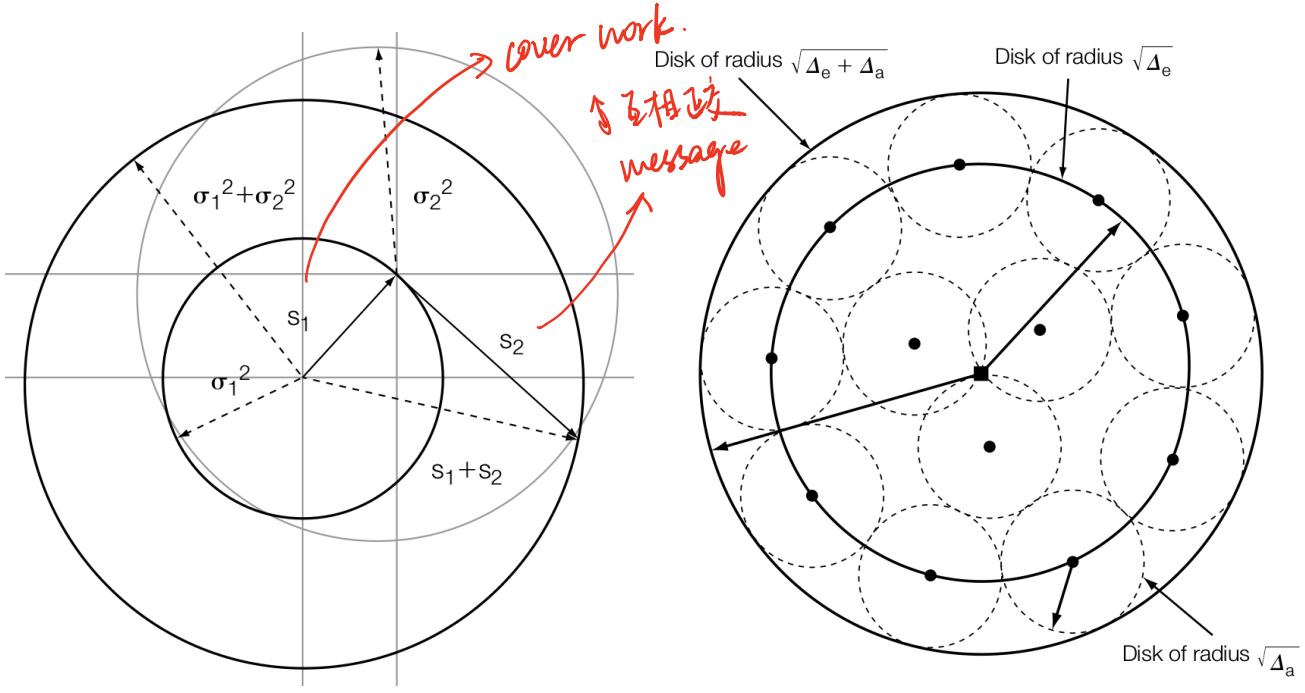
- Costa (1983): We can send just **as much information** on such a dirty piece of paper as we can when writing on a clean sheet of paper, and gave a way to get that capacity.



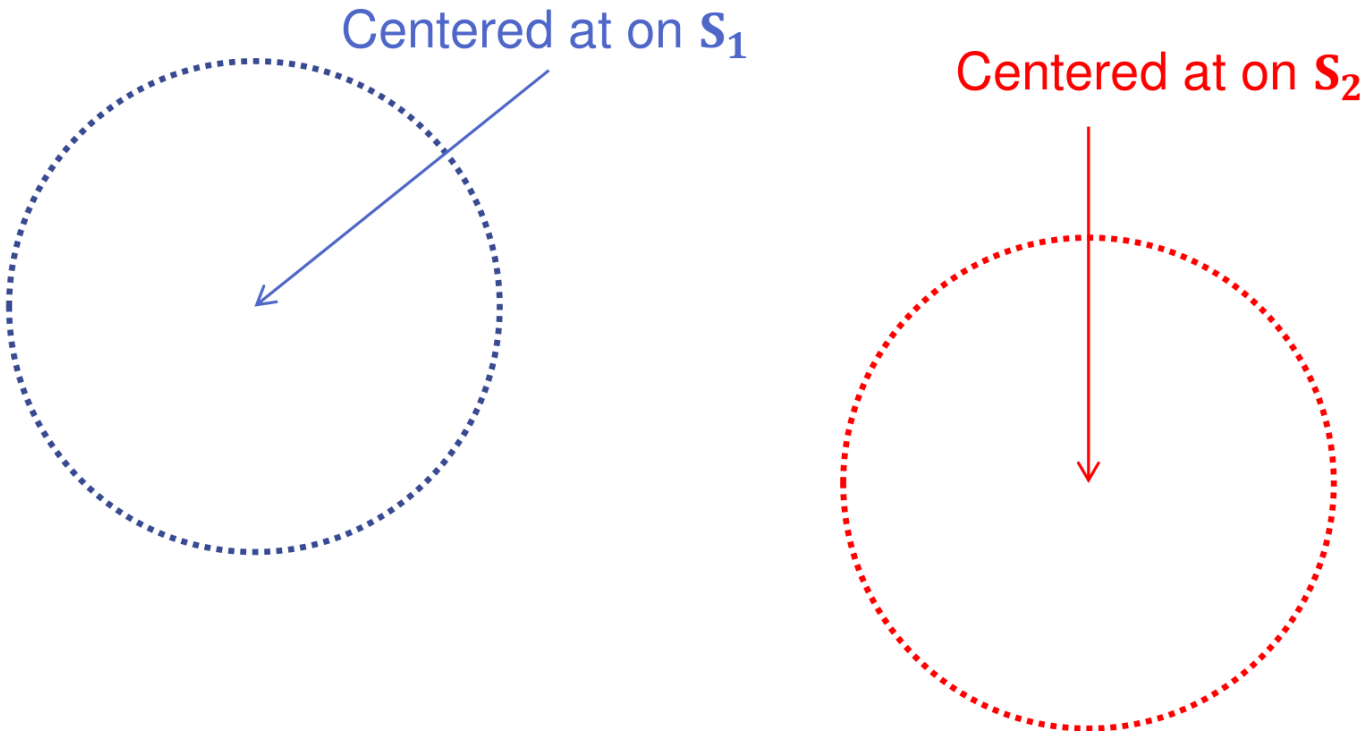
Costa's idea: Nothing about Q or S!

$$R = \frac{1}{2}\ln\left(1 + \frac{P}{N}\right), \text{ or } R = \frac{1}{2}\ln\left(1 + \frac{P_e}{P_a}\right).$$

Shannon's Theorem



S Independent



5.3 Dirty-Paper Codes

Dirty-Paper Code

Classical notion of a code:

- One message, one code word.

Dirty-paper code

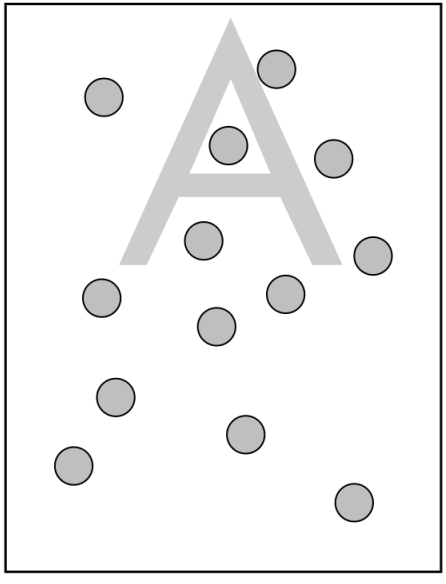
- One message, a set of candidate code words.

message <=> 一组 code words

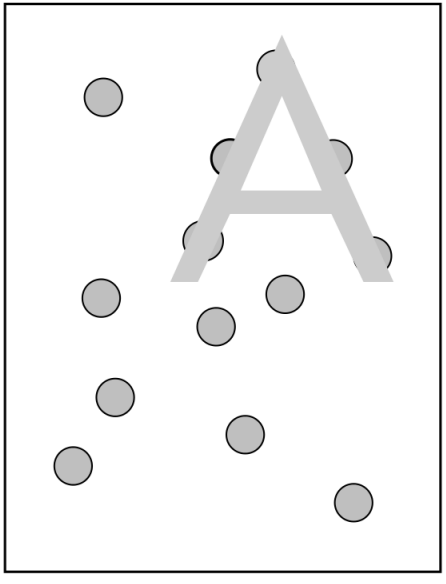
根据 Co 来选一个 code word

Find the code word fits best the host signal for a message.

An Illustration



Blind writing

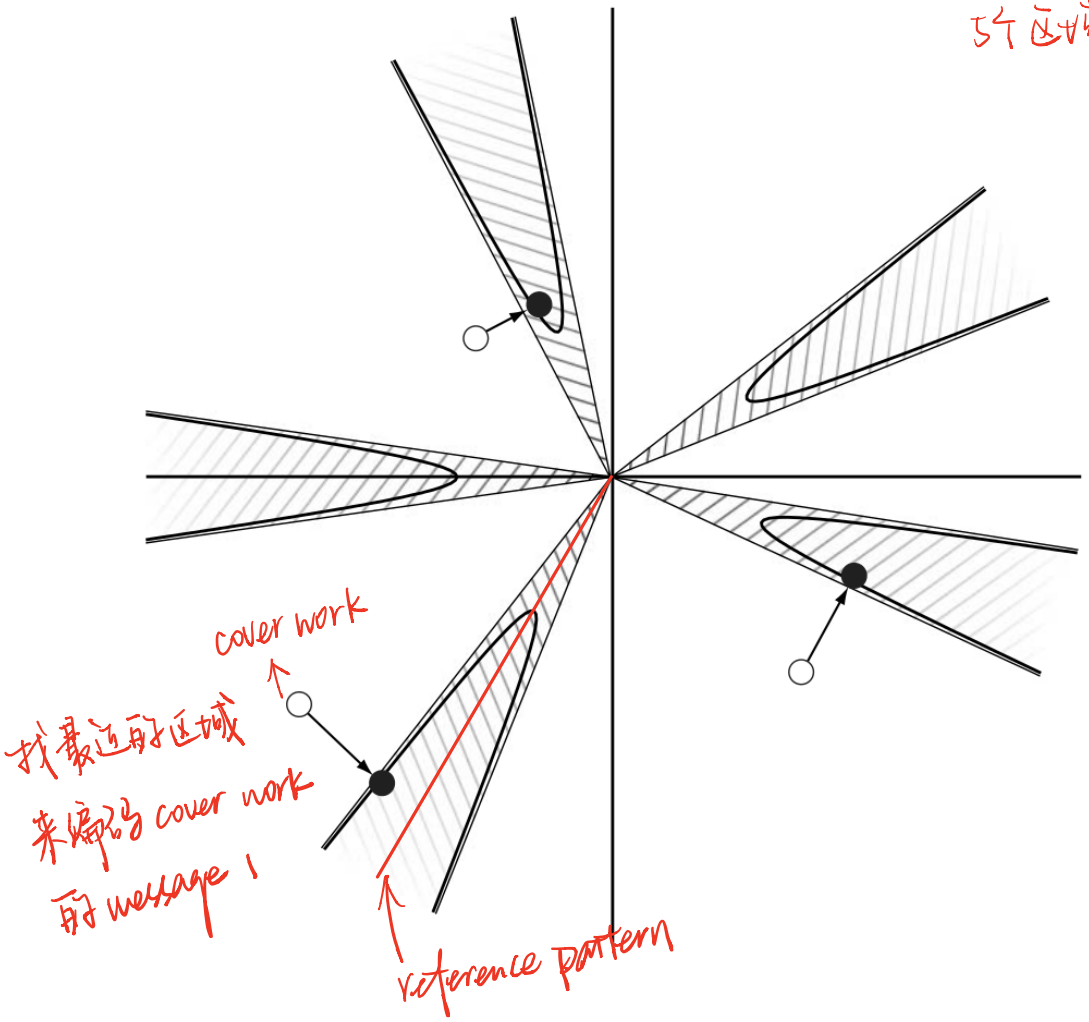


Informed writing

System 8: E_DIRTY_PAPER/D_DIRTY_PAPER

- Based on E_BLK_FIXED_R/D_BLK_CC
- TWO SETS of reference marks, $\mathcal{W}_0$ and $\mathcal{W}_1$, to encode ONE BIT of information.
- Embed 0: use the reference mark in $\mathcal{W}_0$
  - Has highest correlation with $\mathbf{v_o}$.
- Embed 1: use the reference mark in $\mathcal{W}_1$
  - Has highest correlation with $\mathbf{v_o}$.

Illustration



Performance

- False positive rate:

$$(|\mathcal{W}_0| + |\mathcal{W}_1|)P_{fp0}$$

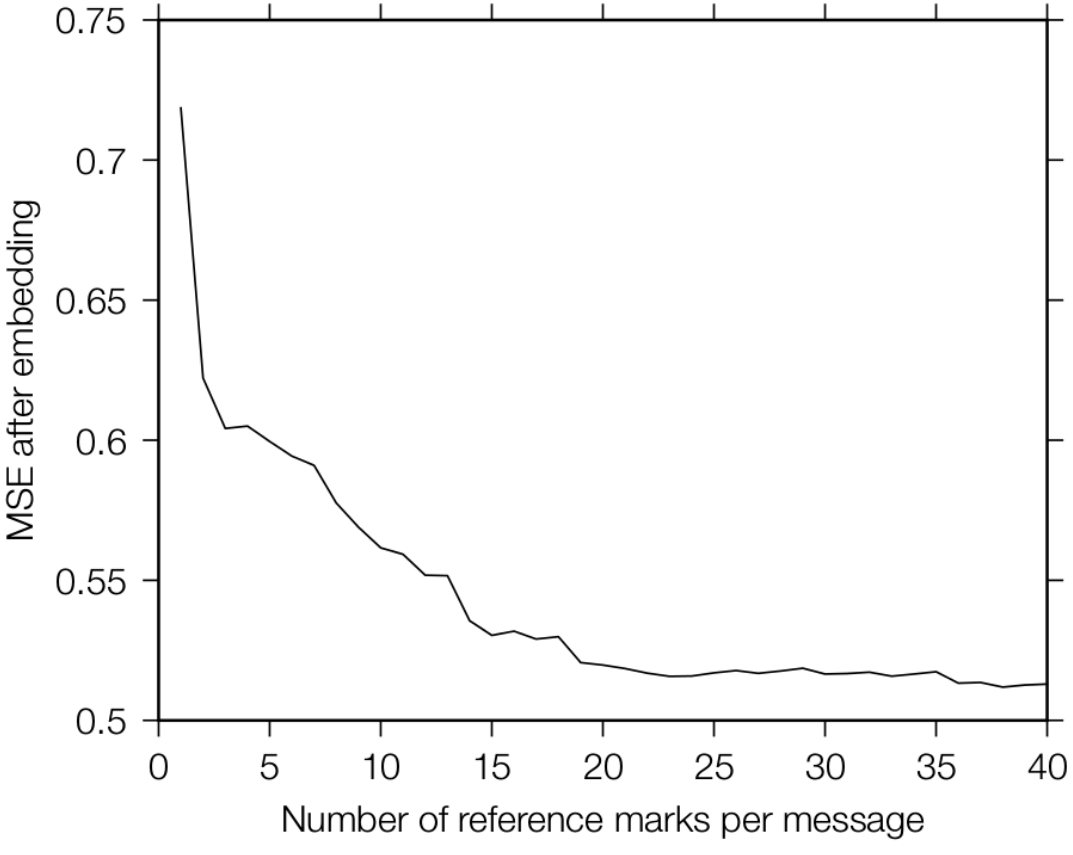
多 reference pattern
阈值升高.
↑
让阴影区域变小点
来减少 fp rate.

  - Keep it constant: adjust numbers of reference marks and threshold.
- Constant payload (1-bit).
- Constant robustness.

Now why vary the number of reference marks?

- Fidelity.

Average Mean Squared Error



Limitation

The embedder and detector both use exhaustive search to find the best matches in $\mathcal{W}_0$ and $\mathcal{W}_1$, this system is only practical when the size of these sets is small.

Least significant bit (LSB) watermarking

Modify $\mathbf{c_o}$ so that the least significant bit encodes the message.

Embed 10000011

- Cover image $\Longrightarrow$ Watermarked image:

$$\begin{pmatrix} 00100111 \\ 11101001 \\ 11001000 \\ 00100111 \\ 11001000 \\ 11101001 \\ 11001000 \\ 00100111 \end{pmatrix} \Longrightarrow \begin{pmatrix} 00100111 \\ 11101000 \\ 11001000 \\ 00100110 \\ 11001000 \\ 11101000 \\ 11001001 \\ 00100111 \end{pmatrix}$$

又改最后一位

Examples

1-bit

Examples

2-bit

Examples

4-bit

Examples

6-bit

Examples

8-bit

Simple

Advantages

- High Payload
- Good fidelity for 1-bit only.

Drawbacks

- Not robust ECC
- False positive probability? 校验码. (pad / valid message)

↑ payload 变小.

Quantization Index Modulation

LSB is a QIM.

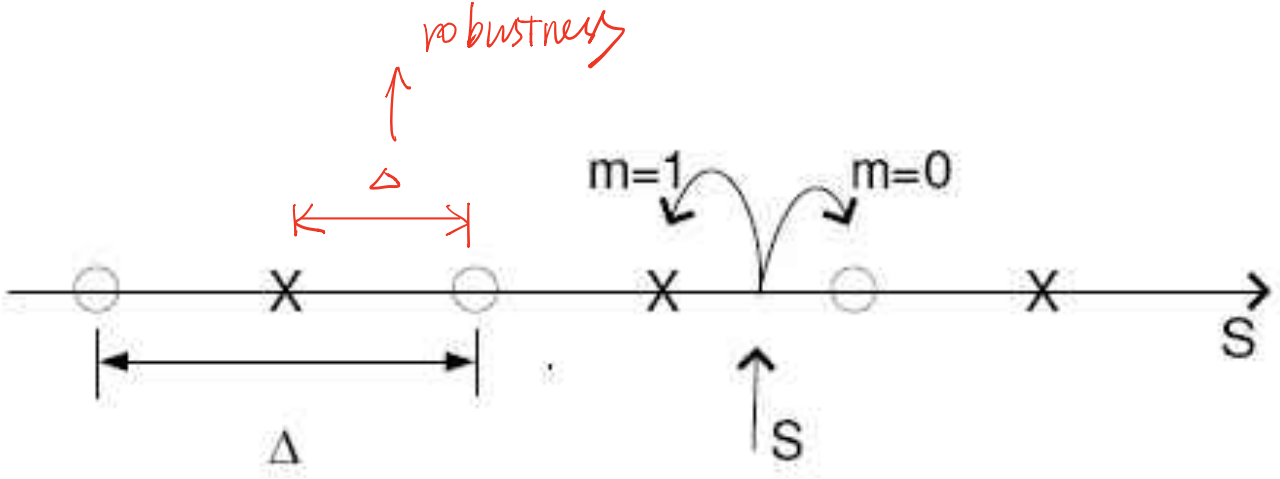
Separate the range of scalar into two sets

- even for 0
- odd for 1

Or in a 2-ary scalar watermarking, the code book $\mathcal{C}_0, \mathcal{C}_1$ are defined as

$$\mathcal{C}_m = \{(m + 2k) | k \in \mathbb{Z}, m \in \{0, 1\}\}. \quad (1)$$

Illustration



The closest code.

good fidelity.

Why Quantization?

From exhaustive search to simple rounding!

In General

For a M-ary scalar watermarking

- The code books $\mathcal{C}_m, m \in \{0, 1, \cdots, M-1\}$

$$\mathcal{C}_m = \{(m + kM)\Delta | k \in \mathbb{Z}\}.$$

- Embedding m into s: find k so that

$$\min_k |s - (m + kM)\Delta|.$$

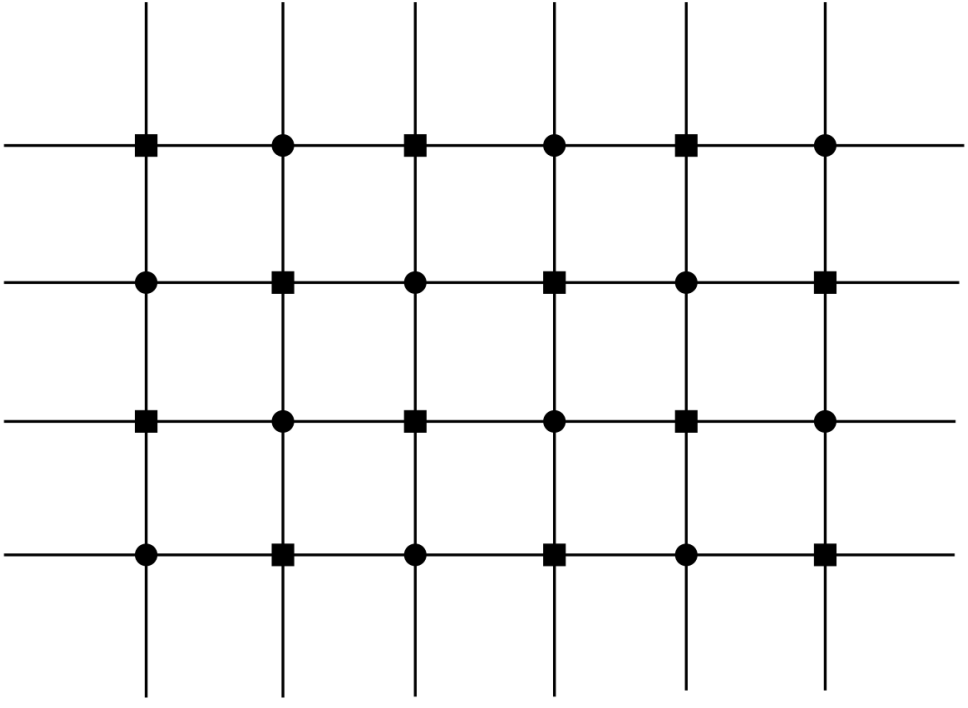
- Detection

$$[y/\Delta] \mod M.$$

Lattice Codes

From one dimension to two dimension

$$\mathcal{C}_0 = \{(k_1 + k_2) \mod 2 = 0\}$$
$$\mathcal{C}_1 = \{(k_1 + k_2) \mod 2 = 1\}.$$



More General

Binning scheme

- Hashing
- ...

Presentation: 8.2

General form of a perceptual model

Presentation: Project 1

- E_BLIND
- D_LC

The key points

- The tips
  - Scaling and shifting of the reference mark etc.
  - Noise from value clipping
    - Use low/high contrast image
- Performance: the plot of detection value
  - Using different reference mark
  - Using different cover work