The Cyclic Shift Channel*

Tjalling Tjalkens[1] Zhu Danhua[2]

[1] Eindhoven University of Technology

[2] Philips Research Europe

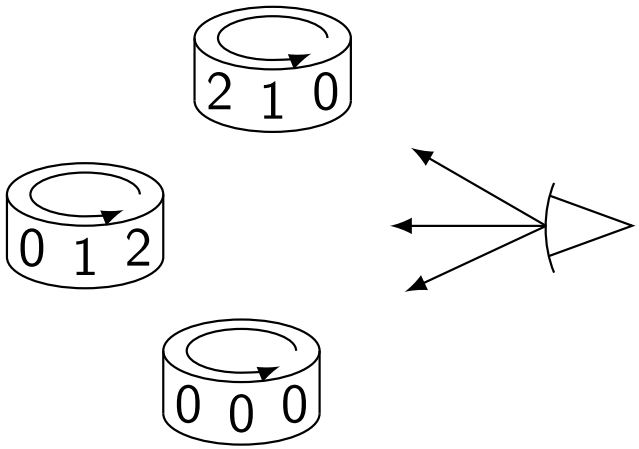
February 7, 2012

Email: t.j.tjalkens@tue.nl

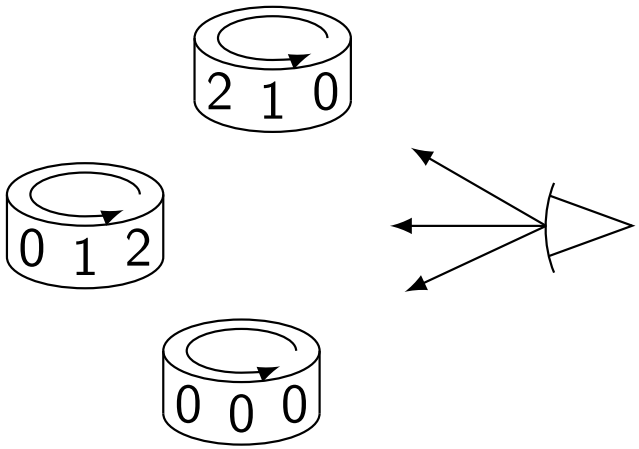
ITA Workshop 2012

*This work is in part supported by ENIAC Joint Undertaking, grant 270707-2, EnLight.

Problem statement

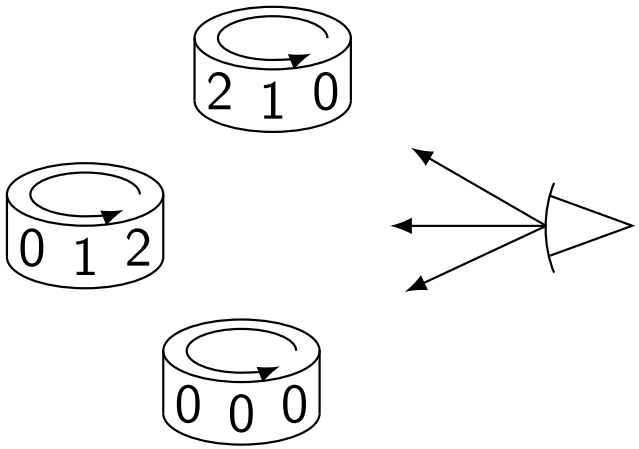


Problem statement



- It is known when a data word readout starts.
- The shift within a word is unknown.
  e.g. we can read:
  0 0 0, 1 2 0, 0 2 1.
- Or noisy:
  0 2 0, 1 1 1, 0 2 0.

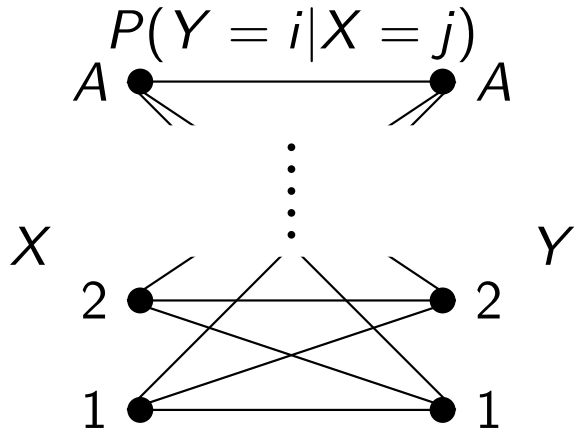
Problem statement

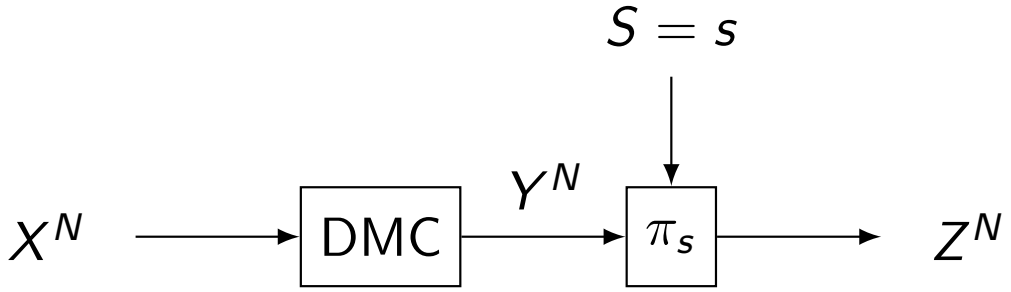


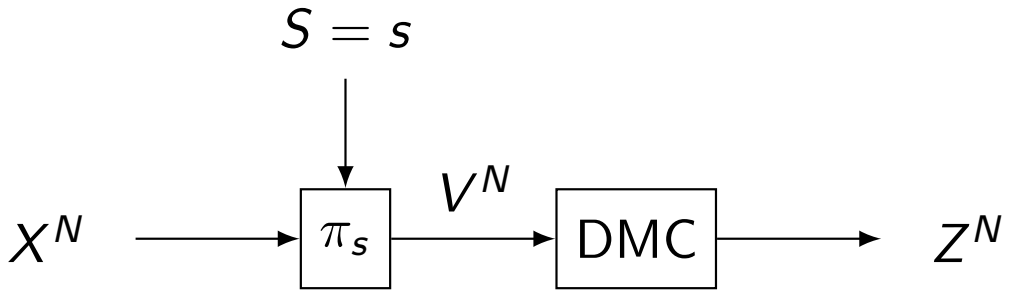
- It is known when a data word readout starts.
- The shift within a word is unknown.
  e.g. we can read:
  0 0 0, 1 2 0, 0 2 1.
- Or noisy:
  0 2 0, 1 1 1, 0 2 0.

- Coding against shifts and errors.
- Shifts over a full code word length.
- Interested in short code words.
- Synchronization prefixes are too expensive.

Channel model







Capacity

Basic discrete memoryless channel: $C_{\text{DMC}} = \max_{P(X)} I(X;Y)$.
After applying the shift π_S: $C_{\text{CSC}} = \lim_{N\to\infty} \sup_{P(X^N)} \frac{1}{N} I(X^N;Z^N)$.

Theorem

Let X^N be the input of a CSC of word length N and Z^N be the corresponding output. Let X^N also be the input of the constituent DMC channel based on the confusion matrix and let Y^N be its output. This implies that Z^N is a cyclic shift of Y^N over a random number of positions. The random variable S denotes this shift and we say that if $S = s$ then $Z^N = \pi_s Y^N$. We have

$$C_{CSC} = \lim_{N\to\infty} \sup_{P(X^N)} \frac{1}{N} I(X^N;Z^N) = \lim_{N\to\infty} \sup_{P(X^N)} \frac{1}{N} I(X^N;Y^N) = C_{DMC}.$$

- Key: $I(X^N;Z^N) = I(X^N;Y^N) - I(X^N;S|Z^N)$.
- $I(X^N;S|Z^N)$ is the unwanted information about the shift S.
- $I(X^N;S|Z^N) \leq H(S) \leq \log N$.

Properties

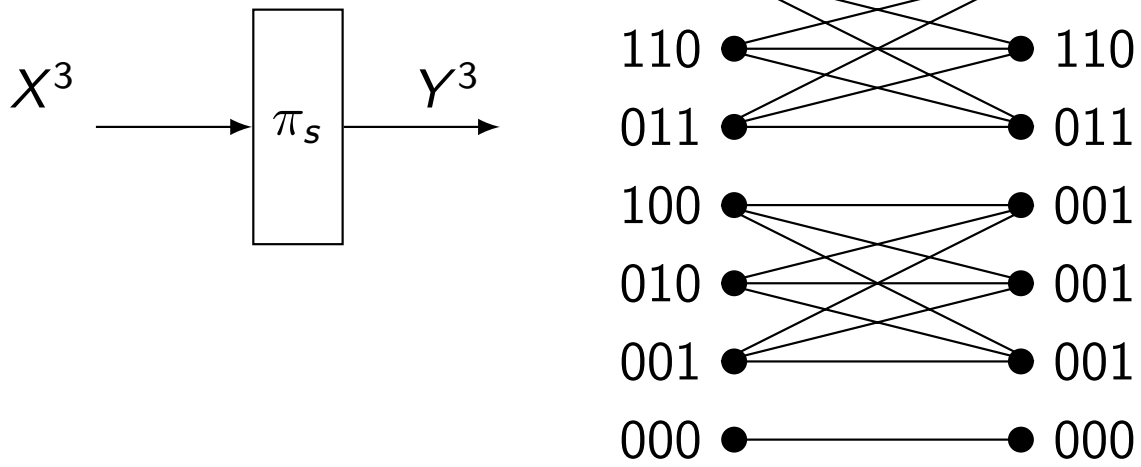
- Capacity achieving P_X equals the capacity achieving distribution of the DMC, so it is memoryless.
- At capacity Z^N and S are independent. So, no information about S is transferred.
- At capacity Z is i.i.d.

So, at capacity (asymptotically) all information and influence of the shift is gone.

But we are interested in short (non-asymptotic) code word lengths.

The "normal" shift channel

Fixed length shifts L, independent of the code word length.
And no errors.



- capacity achieving $P(X^3)$: uniform over the $L+1$ (four) groups.
- Capacity equals $\log L + 1$.
- Not a memoryless input distribution.

Codes for the cyclic shift channel

No synchronization prefix.
Let the symbol alphabet size $A = 2$.
Let the sequence length $N = 4$.
There are $2^N = 16$ possible words.
We find the following code words or sets, also called *cyclic classes*.

Word 1:	$\{0000\}$
Word 2:	$\{0001, 0010, 0100, 1000\}$
Word 3:	$\{0011, 0110, 1100, 1001\}$
Word 4:	$\{0101, 1010\}$
Word 5:	$\{0111, 1110, 1101, 1011\}$
Word 6:	$\{1111\}$

Error correcting codes

Definition

Let m_1 and m_2 be two cyclic classes over the set of sequences of length N over the alphabet $\mathcal{A}$. The *cyclic Hamming distance* $d_{cH}(m_1, m_2)$ is defined as the minimal Hamming distance between any pair of words from $m_1 \times m_2$,

$$d_{cH}(m_1, m_2) = \min\{d_H(x_1^N, x_2^N) : x_1^N \in m_1, x_2^N \in m_2\}.$$

Here $d_H(x_1^N, x_2^N)$ is the ordinary Hamming distance.

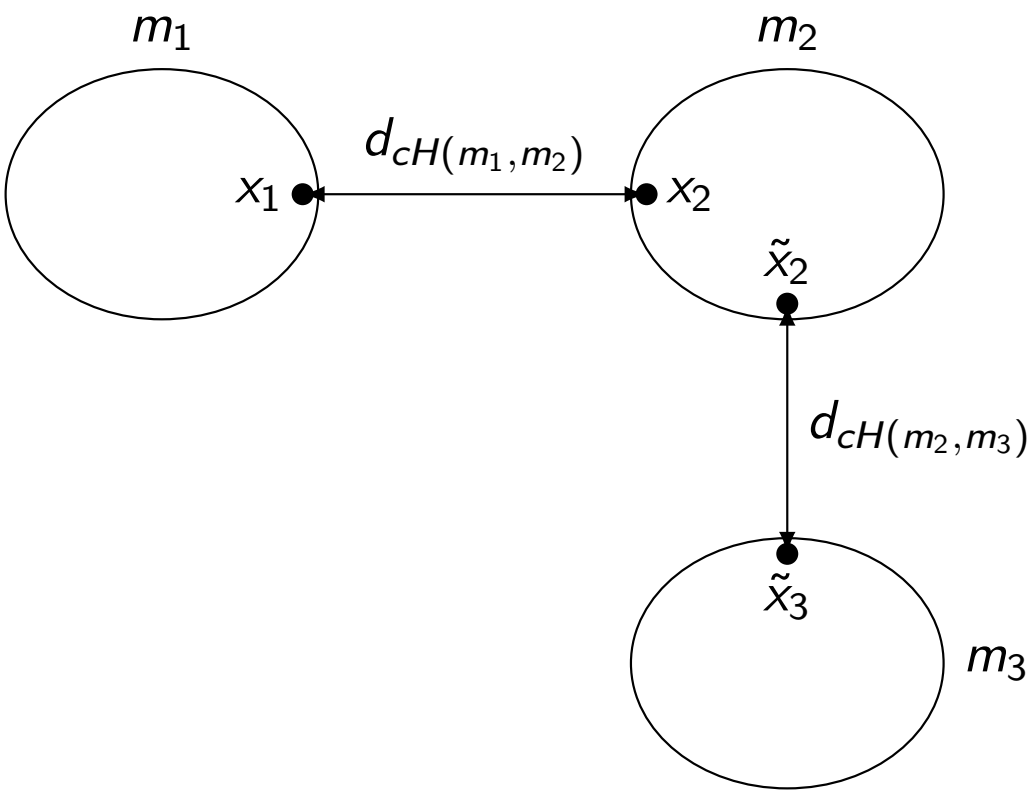
Note that for any two cyclic classes m_1 and m_2, $d_{cH}(m_1, m_2) = d_{cH}(m_2, m_1)$.

Triangle inequality

Theorem

Let m_1, m_2, and m_3 be three arbitrary cyclic classes of sequences of length N over an alphabet $\mathcal{A}$. The following inequality holds.

$$d_{cH}(m_1, m_3) \leq d_{cH}(m_1, m_2) + d_{cH}(m_2, m_3).$$

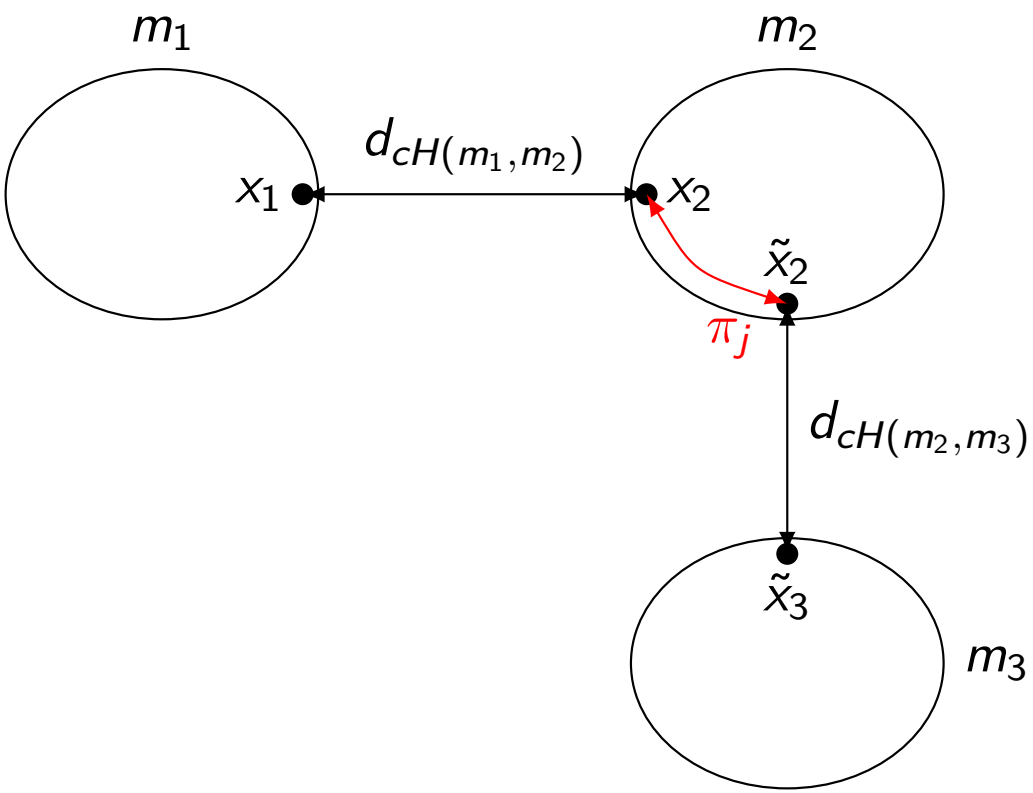


Triangle inequality

Theorem

Let m_1, m_2, and m_3 be three arbitrary cyclic classes of sequences of length N over an alphabet $\mathcal{A}$. The following inequality holds.

$$d_{cH}(m_1, m_3) \leq d_{cH}(m_1, m_2) + d_{cH}(m_2, m_3).$$

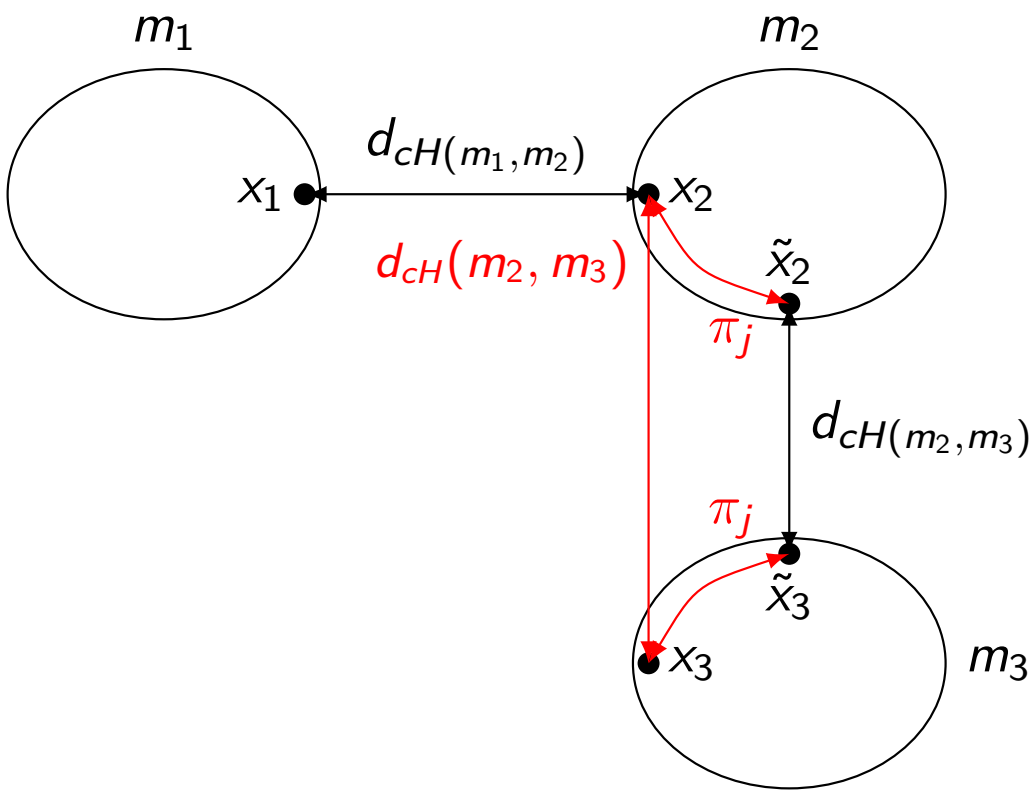


Triangle inequality

Theorem

Let m_1, m_2, and m_3 be three arbitrary cyclic classes of sequences of length N over an alphabet $\mathcal{A}$. The following inequality holds.

$$d_{cH}(m_1, m_3) \leq d_{cH}(m_1, m_2) + d_{cH}(m_2, m_3).$$

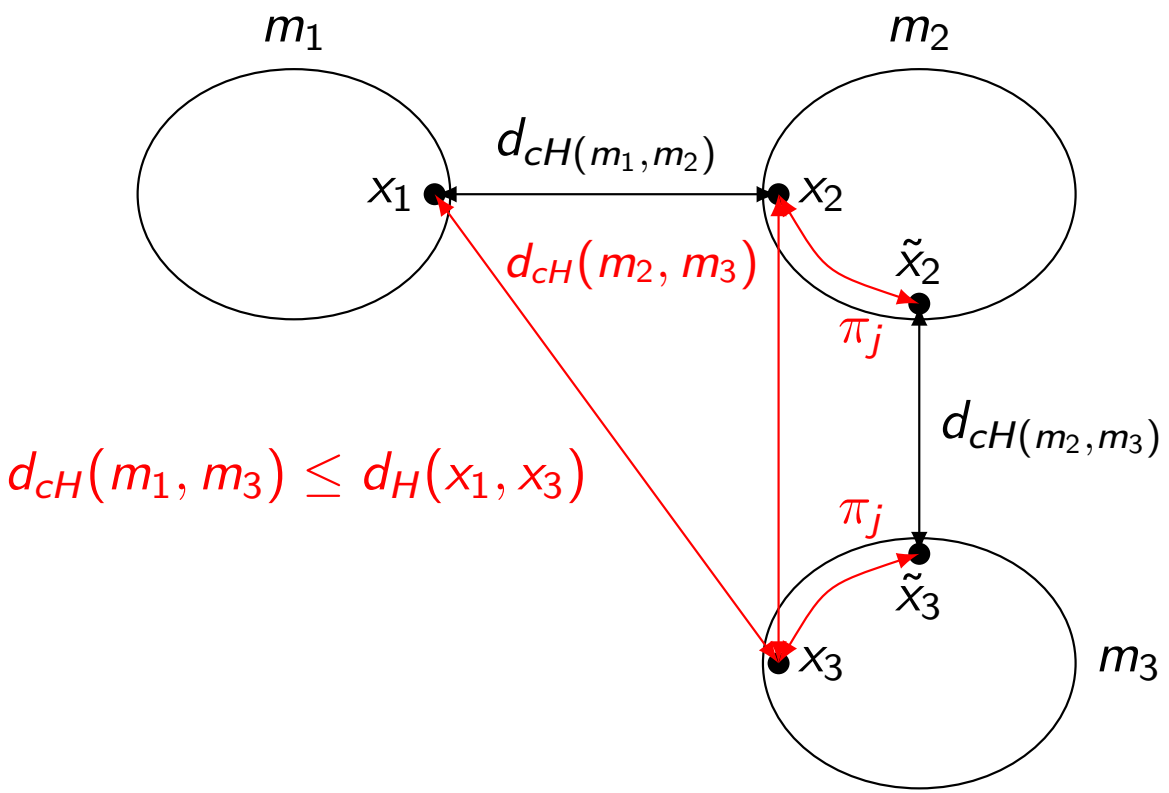


Triangle inequality

Theorem

Let m_1, m_2, and m_3 be three arbitrary cyclic classes of sequences of length N over an alphabet $\mathcal{A}$. The following inequality holds.

$$d_{cH}(m_1, m_3) \leq d_{cH}(m_1, m_2) + d_{cH}(m_2, m_3).$$



Mimimum distance decoding

Definition

For a given cyclic code C containing the cyclic classes $m_1, m_2, \ldots, m_K$ as the K code words, the *minimum cyclic Hamming distance*, $d_{cH,\min}(C)$ is defined as

$$d_{cH,\min}(C) = \min\left\{d_{cH}(m_1, m_2) : m_1 \in C, m_2 \in C, m_1 \neq m_2\right\}.$$

Theorem

Let m_1 and m_2 be two different code words from C. Let m_3 be an arbitrary cyclic class with distance $d_{cH}(m_1, m_3) = e \leq \left\lfloor \frac{d_{cH,\min}(C)-1}{2} \right\rfloor$. Then

$$d_{cH}(m_2, m_3) > \left\lfloor \frac{d_{cH,\min}(C) - 1}{2} \right\rfloor.$$

Code examples

N	A	$d_{cH,\min}$	nr words	code
3	3	2	5	{000, 012, 021, 111, 222}
3	3	3	3	{000, 111, 222}
4	3	2	9	{0000, 0011, 0022, 0101, 0202, 1111, 1122, 1212, 2222}
4	3	3	3	{0000, 0111, 0222}
5	3	2	17	{00000, 00011, 00101, 00122, 00212, 00221, 01022, 01112, 01121, 01202, 01211, 02021, 02111, 02222, 11111, 11222, 12122}
5	3	3	6	{00000, 00121, 01022, 02112, 11111, 22222}
6	3	3	10	{000000, 000111, 001021, 002122, 012012, 020202, 022211, 111111, 121212, 222222}
6	3	4	5	{000000, 001122, 002211, 111111, 222222}

Gilbert lower bound

Theorem

Let C be a cyclic code with word length N over an alphabet of size A and with a minimal cyclic Hamming distance $d_{cH,\min}$. Now, given N, A, and $d_{cH,\min}$, there must exist a cyclic code C with

$$|C| \geq \left\lceil \frac{A^N}{N \cdot V(N, A, d_{cH,\min} - 1)} \right\rceil,$$

where $V(N, A, d)$ is the volume of a sphere of radius d in $\mathcal{A}^N$.

Asymptotically, as $N \to \infty$ and $d_{cH,\min} = 2f \cdot N + 1$, we find

$$\lim_{N \to \infty} \frac{\log_A |C(N)|}{N} \geq 1 - h_A(2f),$$

where

$$h_A(p) = p \log_A(A-1) - p \log_A p - (1-p) \log_A(1-p),$$
$$\text{for all } p \in [0, 1 - \frac{1}{A}].$$

This is the same bound as for ordinary error correcting codes.

Conclusions

- Even though the cyclic shift channel does not appear to be a memoryless channel it (almost) performs the same as the underlying DMC.
- Cyclic class coding improved the detection probability and coding rate over the uncoded case for a particular application.
- The approximately $(\log N)/N$ loss in rate is visible in the code design, the Gilbert bound, and the capacity considerations.
- Whether we can find codes similar to linear codes is not clear but because we are interested in short code word lengths only this is not so important.