Noncommutative convolutional error correcting codes

Marion Candau

June 21, 2012

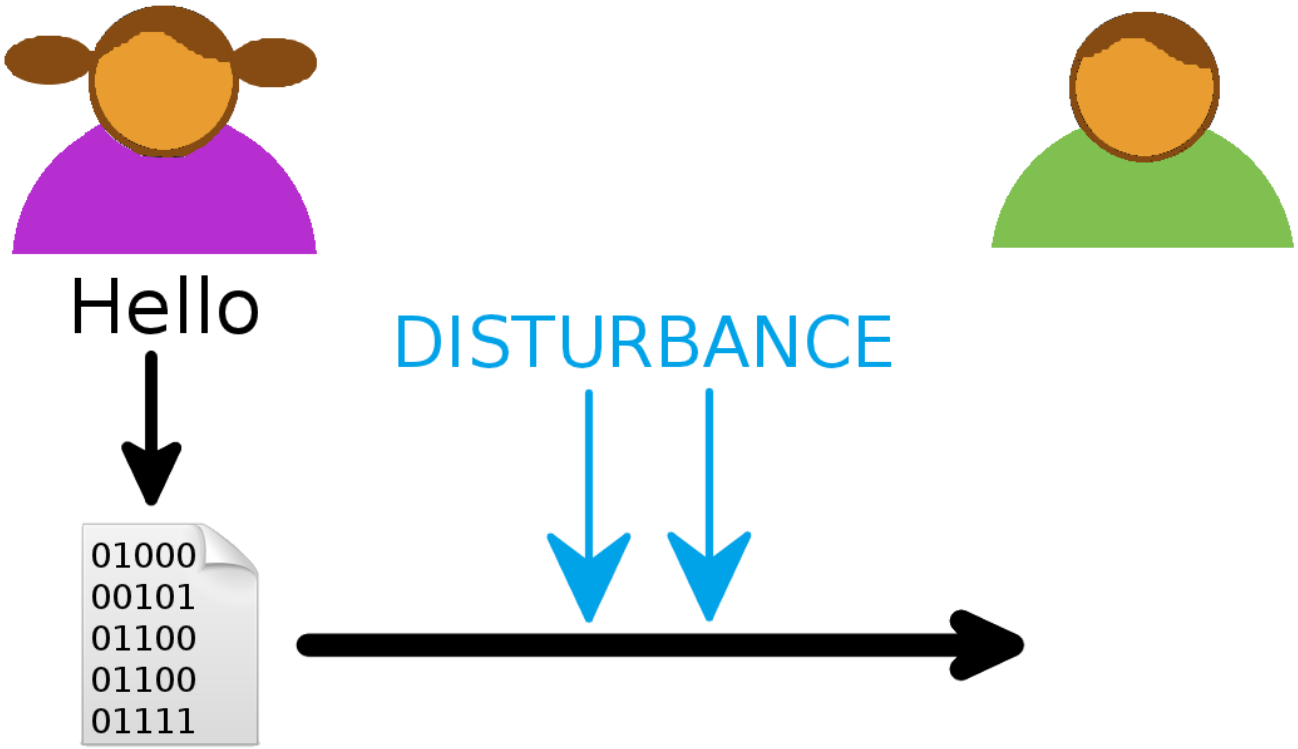
Table of contents

Table of contents

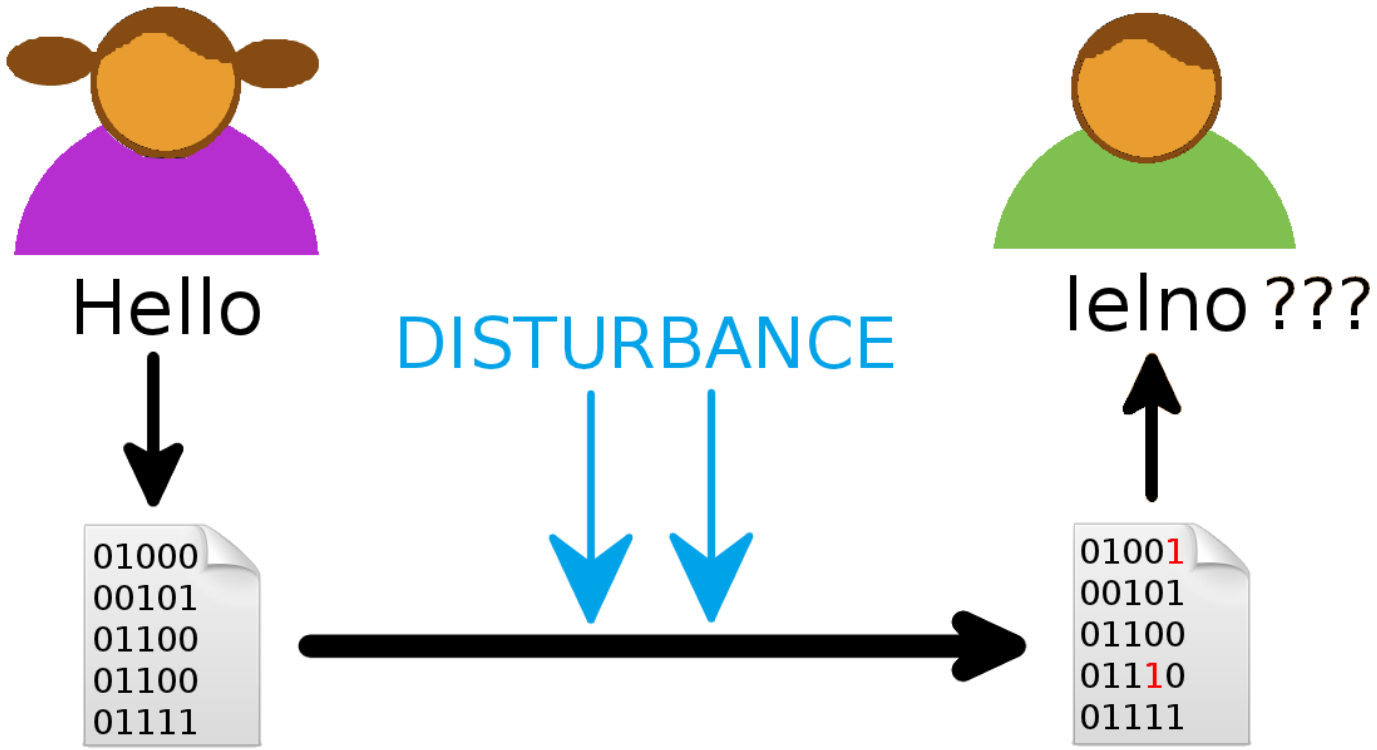
Problem

Problem

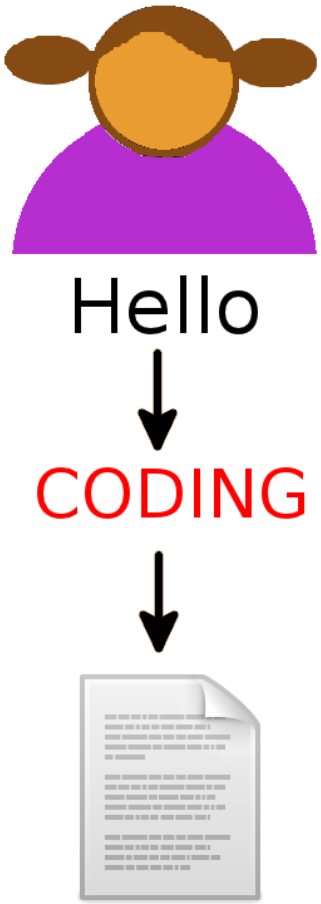
Problem



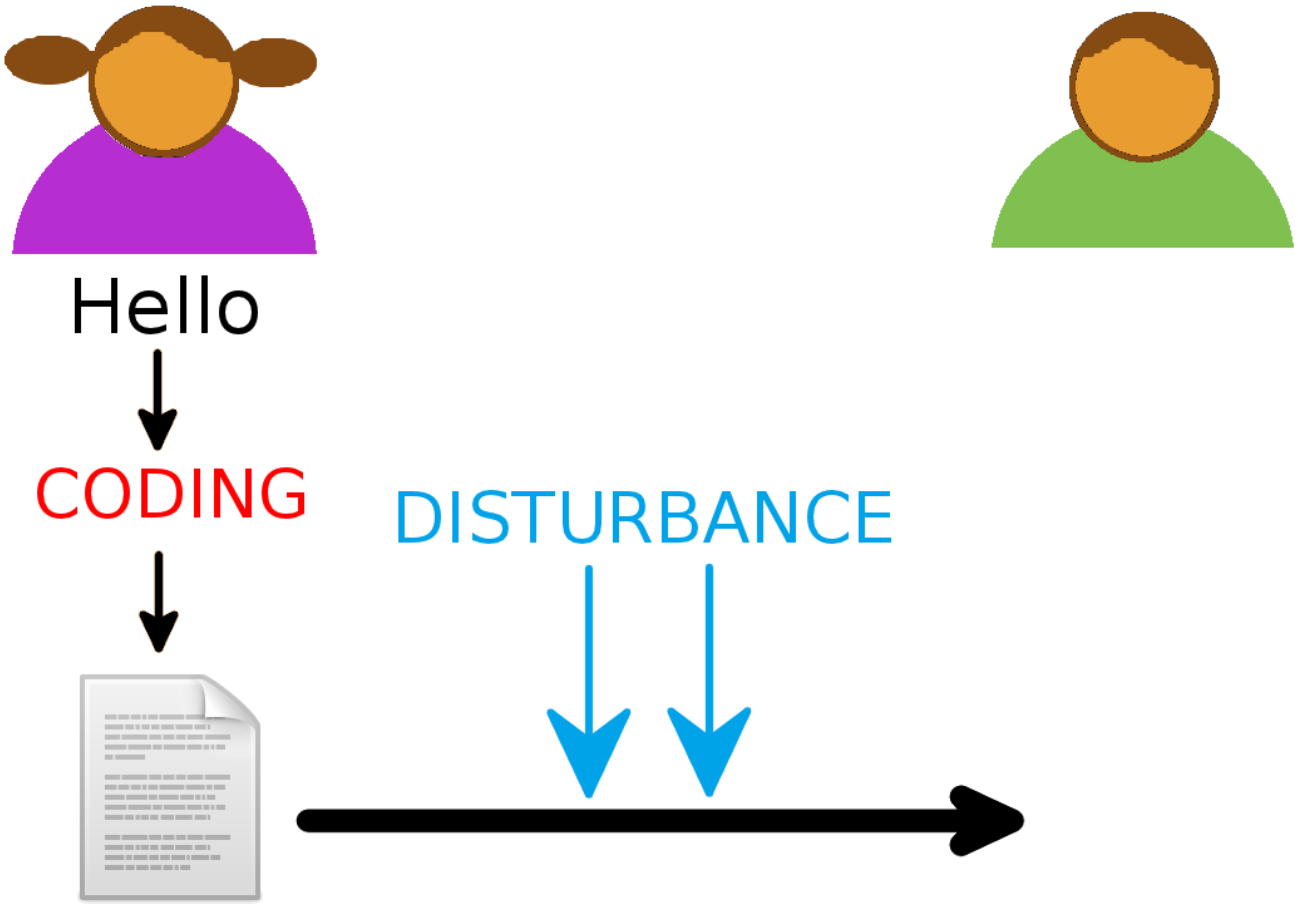
Problem


Hello
01000
00101
01100
01100
01111
DISTURBANCE
Ielno ???
01001
00101
01100
01110
01111

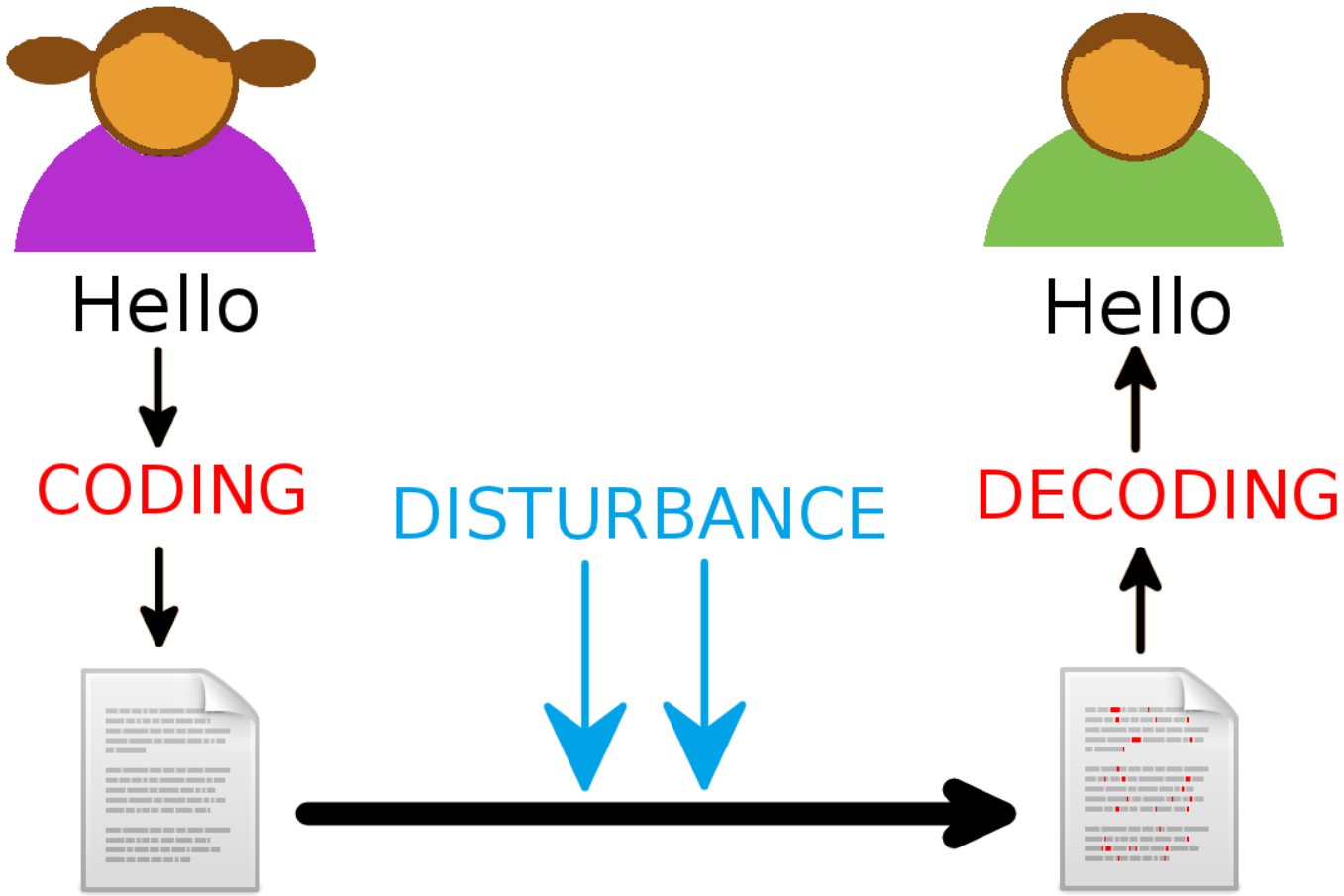
Solution is error correcting codes



Solution is error correcting codes



Solution is error correcting codes

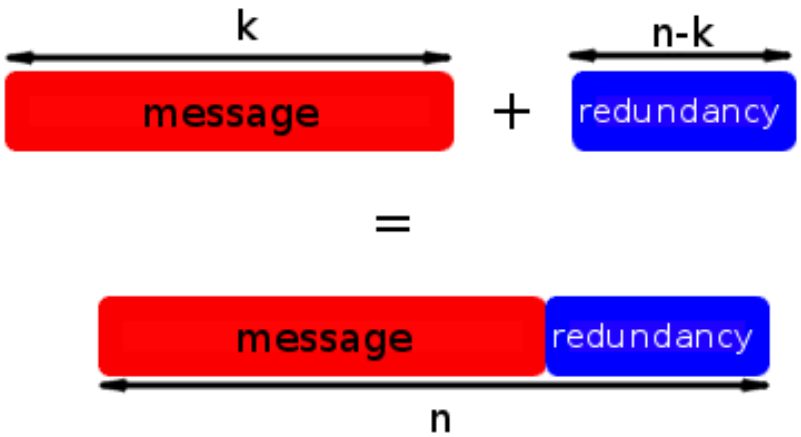


Coding is...

- add redundancy

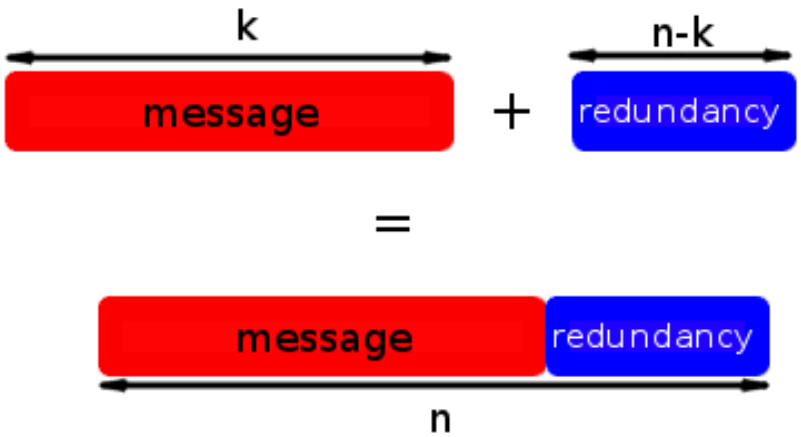
Coding is...

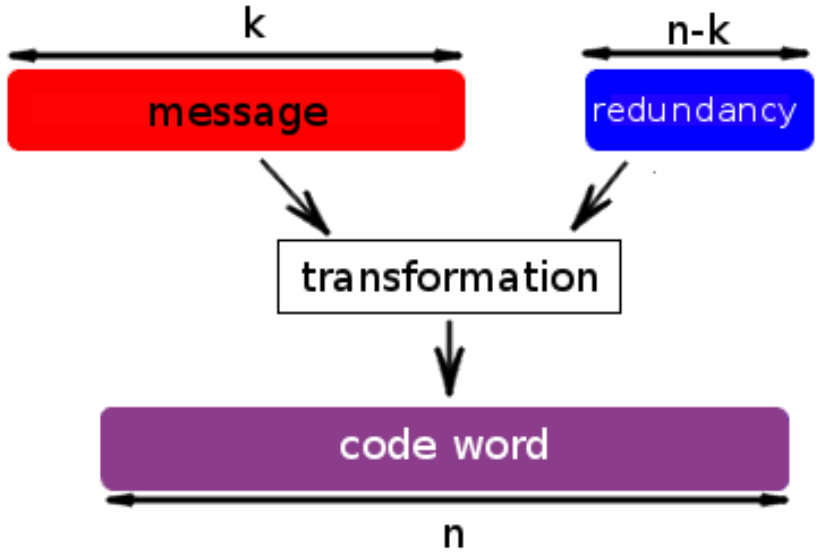
- add redundancy
- Two ways



Coding is...

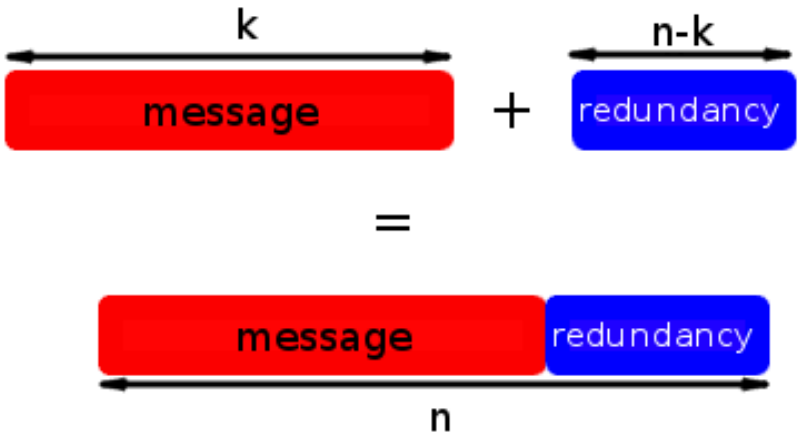
- add redundancy
- Two ways

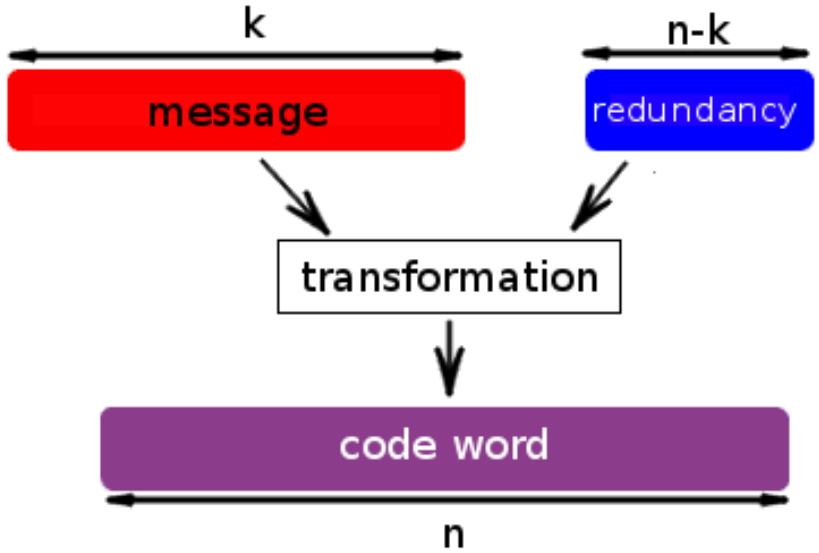




Coding is...

- add redundancy
- Two ways





- In the words of length n, few code words
- The part of redundancy must be as small as possible

Hamming distance

Definition

The distance between two words is the number of positions at which the corresponding symbols are different.

Example :

1011101 and 1001001 is 2.

Definition

The Hamming distance of a code, d_H, is the minimum of distance between all code words.

Decoding is to seek the code word nearest to the received word

Capacity of correction

- Example :
  code words are

$$100100, 011100, 011011$$

  You receive

$$010100$$

  What is the good code word ?

Capacity of correction

- Example :
  code words are

$$100100, 011100, 011011$$

  You receive

$$010100$$

  What is the good code word ?
- it's 011100 because

$$010100 \text{ and } 100100 \text{ is } 2$$
$$010100 \text{ and } 011100 \text{ is } 1$$
$$010100 \text{ and } 011011 \text{ is } 4$$

- correct $\frac{d_H}{2}$ errors.

Repetition codes

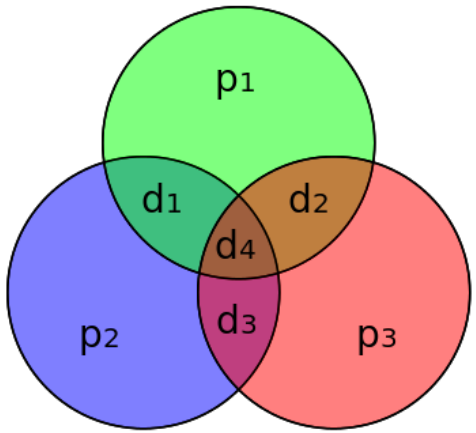
- the simplest code
- if the message is 01, the code word is 0101.
- Detection of errors but no correction
- 2 repetitions : $01 \to 010101$ can correct one error but not efficient

Hamming codes

Definition

A parity bit is a bit which is added to a message to mean that the number of 1 in the message is even or odd.

- Simplest Hamming code : $k = 4$ and $n = 7$.
- d_1, d_2, d_3, d_4 are bits of message, p_1, p_2, p_3 are bits of parity



- Correct one error

Table of contents

History and uses

- invented in 1955 by Peter Elias
- most famous : turbocodes invented by Claude Berrou and Alain Glavieux in Telecom Bretagne in 1993
- Standard of mobile communication
- also used in digital video, radio, and satellite communication

Convolution

- operation that we perform when we multiply two polynomials
- Example :

$$(1+X)(X+X^2) = 1 \times X + 1 \times X^2 + X \times X + X \times X^2$$
$$= X^3 + 2X^2 + X$$

But in binary, $2 = 0$, so

$$= X^3 + X$$

If you have a message f, then you convolute it with a transfer function g :

$$(f * g)(k) = \sum_{i \geqslant 0} f(i)g(k-i)$$

Commutativity

It's the property that :

$$x \times y = y \times x$$

If this property is false, we say that the group of x, y is noncommutative.

Consequence in the convolution

$$(f * g)(k) = \sum_{i \geqslant 0} f(i)g(k-i)$$

i take the values $1, 2, 3, \ldots$.
If i take its values in a noncommutative group G, the convolution will be :

$$(f * g)(k) = \sum_{i \in G} f(i)g(i^{-1}k)$$

where i^{-1} satisfies the property $i \times i^{-1} = 1$
(Example, $5^{-1} = \frac{1}{5}$ because $\frac{1}{5} \times 5 = 1$).

Table of contents

Conclusion

Aims of my thesis are :

- to find noncommutative groups
- to find a decoding algorithm
- to hope they are better properties than classical convolutional codes