Communication
Using an OR Channel

A.J. Han Vinck
University Duisburg-Essen
Duisburg-DSV

https://www.uni-due.de/dc/vinck-main.php
At the occasion of

the 2015 Aaron D. Wyner Distinguished Service Award

The Aaron D. Wyner Distinguished Service Award honors individuals who have shown outstanding leadership in—and provided long-standing exceptional service to—the IEEE Information Theory Community.

Han Vinck is receiving the award for his longstanding contributions with IEEE chapters, promotion of information theory and its applications, and organization of conferences and workshops.
Road map

1. access for the OR channel using information theory
   – Fundamental limits for communication using the OR channel (Shannon)

2. Signature transmission

3. Protocol sequences
Problem: uncoordinated users sharing the same medium

• Ex: RFID tags

• Ex: Computer communication using a bus system
Difference between controlled and un-controlled

**Classical (information theory)**

- **Controlled access**
  - Active users know each other

**Random access (networking)**

- **No control**
  - Active users do not know who

**Assumption:** the number of active users is small (as in telephony)
What is the channel model?
(energy detection, Photon counting)

binary in - binary out

tr 1 -> OR -> rec 1
tr 2 -> OR -> rec 2
tr T -> OR -> rec T

Only T out of N possible users are active: - users do not know who
Where does the OR model come from?

- Optical On-Off channel model
- CAN Bus communications  
  \((\text{CAN} = \text{Controller Area Network})\)
- Frequency Hopping sequence design
- Pulse Position Modulation
- UWB
A simple way to transmit:
Time-Division Multi Access TDMA

Every possible user gets a particular time slot

- efficiency = \(\frac{T}{N}\)

inefficient, but easy

A.J. Han Vinck, July 2015
Random-Access problem statement

In

User A

User B

User C

Out

OR

Q: did user C send?
Q: what?
The model from an information theory point of view

User $i$ transmits $x_i$ to receiver $i$. Other users are considered as noise for user $i$. The sum capacity is given by

$$\text{sum capacity} = T \max_p I(X_i; Y)$$

- Under the condition that all $T$ users behave in the same way.

A.J. Han Vinck, July 2015
Communication model for a particular user looks like

\[ q = 1-p \]

\[ C = \frac{T}{p} \max_p I(X_i;Y) \]

\[ C_{T \to \infty} = \ln 2 \text{ bits/tr.} \quad \text{for } p = \frac{\ln 2}{T} \]

References:


A. J. Han Vinck and K. Keuning, “On the capacity of the asynchronous T-user M-frequency noiseless multiple-access channel \textit{without intensity information},” IEEE Tr. on Information theory, pp. 2235-2238, 1996

A.J. Han Vinck, July 2015
To calculate the capacity is difficult in general

**REASON:**

Channel transition probabilities are a function of the input probabilities.

*Note:* classical information theory does not work here!

Channel for a particular user

- $p$
- $(1-p)^\Gamma-1$
- $0$
- $p$
- $1$
- $1$
- $0$

interference from others depends also on $p$!

**Problem is not convex anymore**

A.J. Han Vinck, July 2015
CONCLUSION for T uncoordinated access

- OR channel: \( C_{T \to \infty} = \ln 2 \approx 0.7 \) bits/tr.; for \( P_1 = \ln 2/T \)
  - We lose only 30% compared with fully coordinated (TDMA)!

=> code books needed with long - low weight- codewords!

=> For the XOR channel: \( C_{T \to \infty} \geq 0.38 \) bits/tr. (open problem!)
  - Why do we use the XOR operation in network coding?


A.J. Han Vinck, July 2015

13
Look at an old data bank (library, ...)

- Item properties are **coded** as non-holes on the card
- Cards **selection by pins**
- **Problems:**
  - Properties do not overlap, otherwise too many faulty selections
  - how to code many properties for limited space

- **We see the DIFFERENCE** between HARD and SOFTWARE

A.J. Han Vinck, July 2015
How to get a practical system?  
(Task of an engineer is to solve problems)

• Transmission using **signatures:**
  – Coordinated and uncoordinated

  Ex: $1 := 1 0 0 1 1 0 0 1$ and $0 := 0 0 0 0 0 0 0 0$

• Transmission using a **protocol**
Let us look at the following transmission scenario

- Users can transmit all **zero sequence** or a **signature sequence**

- Users **do not know** each other

Detector for user i looks for the presence of his signature
When do we have a correct detection?

Problem:
- how to distribute the signatures s.t. any set of < T active users does not produce a valid signature for a non active user?
Example: up to 2 active users; $n = 9$; $N = 12$

<table>
<thead>
<tr>
<th>User</th>
<th>signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>001 001 010</td>
</tr>
<tr>
<td>2</td>
<td>001 010 100</td>
</tr>
<tr>
<td>3</td>
<td>001 100 001</td>
</tr>
<tr>
<td>4</td>
<td>010 001 100</td>
</tr>
<tr>
<td>5</td>
<td>010 010 001</td>
</tr>
<tr>
<td>6</td>
<td>010 100 010</td>
</tr>
<tr>
<td>7</td>
<td>100 001 001</td>
</tr>
<tr>
<td>8</td>
<td>100 010 010</td>
</tr>
<tr>
<td>9</td>
<td>100 100 100</td>
</tr>
<tr>
<td>10</td>
<td>000 000 111</td>
</tr>
<tr>
<td>11</td>
<td>000 111 000</td>
</tr>
<tr>
<td>12</td>
<td>111 000 000</td>
</tr>
</tbody>
</table>

$R = \frac{2}{9}$

TDMA gives $R = \frac{2}{12}$

Example:

$011 101 101 = x \text{ OR } y$?

$\ln_2/T \approx \frac{1}{3}$
What are the problems to work on?

- Constructions? Bounds for blocklength $n(T,N)$?

\[ T \log_2 N < n < 3T^2 \log_2 N \] (asymptotic result)

at least, every user has to sends his identity

References:
Cover-Free Families and Superimposed Codes: Constructions, Bounds, and Applications to Cryptography and Group Testing
by Arkadii D’yachkov, Vladimir Lebedev, Pavel Vilenkin, Sergei Yekhanin

This paper deals with cover-free families or superimposed codes. They generalize the concept of superimposed s-codes and have several applications for cryptography and group testing. We present a new asymptotic bound on the rate of optimal codes and develop some constructions.
Some research problems:

- code design for T tags simultaneously?
  - realistic N and T (bound T\log_2 N)
- Combination with error correction?
- Interference problem?
Extension from 2-ary to M-ary with a surprising result

- Binary OR 0 + 1 = 1, 1 + 1 = 1, 0 + 0 = 0

- For PPM: symbols have a single pulse in M positions

  symbol „OR“: (00010) + (10000) = (10010)

  - we can obtain the same random access capacity (ln2)
  - not many code constructions

Reference:
Application in M-FSK frequency hopping or UWB

Figure 4. Frequency hopping allows each frequency to be used by several channels.

Allow overlap

=> Higher efficiency
PPM is not new

used by the ancient Greeks as an optical signaling PPM known as the Hydraulic telegraph of Aeneas

A.J. Han Vinck, July 2015
More possible applications

• Multiple RFID tag identification
  - is an example of OR communication

• protocol sequences (to be discussed later)

• All Optical receiver for speed improvements
Let us look at the following transmission scenario

- Users can transmit all \textit{zero sequence} or a \textit{signature sequence}

- Users \textit{do not know} each other and there is \textit{no} word synchronization

Detector for user $i$ looks for the presence of his signature
• **Shifted** signatures should not generate a valid signature

- Example: ... 1 0 0 1 0 1 0 0 ... user 1
  ... 1 0 1 0 1 0 0 0 ... user 2
  ... 1 0 1 0 0 0 1 0 ... user 3
**Definition of Optical Orthogonal Codes (OOC)**

**Definition 1:** A set $C$ of $n$-length binary vectors of weight $w$

\[ \mathbf{x} = (x_1, x_2, \ldots, x_n) \]

composes an $(n, w, \lambda_a, \lambda_c)$ OOC if the following properties for any codeword hold, where $t + \tau$ is calculated by modulo $n$.

1. **Auto-correlation**
   \[
   \sum_{t=1}^{n} x_t x_{t+\tau} \leq \lambda_a, \quad \tau \geq 1
   \]

2. **Cross-correlation**
   \[
   \sum_{t=1}^{n} x_t y_{t+\tau} \leq \lambda_c, \quad \tau \geq 0
   \]
Example of an OOC of length 7, \( w = 2, \lambda = 1 \)

\[
\begin{align*}
C &= 1100000 & \Delta_1 &= \{1, 6\} \\
    &\quad \Rightarrow 1010000 & \Delta_2 &= \{2, 5\} \\
    &\quad \Rightarrow 1001000 & \Delta_3 &= \{3, 4\}
\end{align*}
\]

There are more interesting variations on the correlation conditions

(no time, sorry)
Illustration of different condition selections

\[ x \leq \lambda_a \]
\[ y \leq \lambda_c \]
\[ y' \leq \lambda_s \]
An ALL Optical transmitter/receiver pair

\[ D^3 + D + 1 \]

channel

other users

\[ D^3 + D^2 + 1 \]

\[ D^5 + D^4 + 3D^3 + D^2 + D + 1 \]

sample

A.J. Han Vinck, July 2015
There are several different constructions

Mathematical design solutions:
- projective geometry (Chung, Salehi, Wei, Wu)
- balanced incomplete block designs (R.N.M. Wilson)
- difference sets (Jungnickel)

Japanese implementation reference: Tomoaki Ohtsuki (Univ. of Tokyo)

We used difference sets to construct codes for which:

\[(n, w, 1) \quad |OOC| \geq \frac{n}{w(w-1)^2}\]

\[(n, 4, 2) \quad \frac{n^2}{24} \geq |OOC| \geq \frac{n^2-2n-8}{36}\]

Optical Orthogonal Code Construction with Correlation 2, S. Martirosyan, Sosina Martirosyan, A.J. Han Vinck, the 23rd Symposium on Information Theory and its Applications (SITA 2000), Aso, Kumamoto, Japan, Oct. 10-13, 2000

A Construction for Optical Orthogonal Codes with Correlation 1, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E85-A No.1 pp.269-272, Samvel MARTIROSYAN A. J. Han VINCK

A.J. Han Vinck, July 2015
The main research questions

Construct Optical Orthogonal Codes of length $n$ with a maximum number of codewords for different correlation constraints

- Finding bounds on the cardinality of these codes
- Performance evaluation
Nice application in networking:

use signatures as protocol sequences

• A protocol tells us how to behave

Readers Protocols - LLRP
Low Level Reader Protocol

• The LLRP interface protocol is called low-level because it provides control of RFID air protocol operation timing and access to air protocol command parameters.
• The design of this interface recognizes that in some RFID systems, there is a requirement for explicit knowledge of RFID air protocols and the ability to control Readers that implement RFID air protocol communications.
• LLRP is specifically concerned with providing the formats and procedures of communications between a Client and a Reader.

• It is a kind of control
Instead of symbol -1- we transmit a packet

\[
C = \begin{cases} 1100000 & \Rightarrow P_1 P_1 0 0 0 0 0 \\ 1010000 & \Rightarrow P_2 0 P_2 0 0 0 0 \\ 1001000 & \Rightarrow P_3 0 0 P_3 0 0 0 \end{cases}
\]

2 protocol sequences can be used in any shifted position simultaneously:
1 position is always "collision free"

\[
\begin{array}{ccccccc}
0 & P_2 & 0 & P_2 & 0 & 0 & 0 \\
P_3 & 0 & 0 & P_3 & 0 & 0 & 0 \ldots \\
\end{array}
\]

collision

# users $N = 3$
- unsynchronized: $R = 2/7 \approx 0.3$
- synchronized: TDMA $\Rightarrow 0.33$
synchronized: 2 users can transmit collision free

<table>
<thead>
<tr>
<th>User</th>
<th>signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>001 001 010</td>
</tr>
<tr>
<td>2</td>
<td>001 010 100</td>
</tr>
<tr>
<td>3</td>
<td>001 100 001</td>
</tr>
<tr>
<td>4</td>
<td>010 001 100</td>
</tr>
<tr>
<td>5</td>
<td>010 010 001</td>
</tr>
<tr>
<td>6</td>
<td>010 100 010</td>
</tr>
<tr>
<td>7</td>
<td>100 001 001</td>
</tr>
<tr>
<td>8</td>
<td>100 010 010</td>
</tr>
<tr>
<td>9</td>
<td>100 100 100</td>
</tr>
<tr>
<td>10</td>
<td>000 000 111</td>
</tr>
<tr>
<td>11</td>
<td>000 111 000</td>
</tr>
<tr>
<td>12</td>
<td>111 000 000</td>
</tr>
</tbody>
</table>

R = 2/9  # users N = 12

TDMA gives  R = 2/12

Example:

011 101 101 = x OR y ?

\[ \ln 2/T \approx 1/3 \]
Friendship and cooperation in science is very important

- Who are these old guys?

Toby Berger (Cornell)
Me (UDE)
Daniel Costello (Notre Dame)
Sergio Verdu (Princeton)
What did we discuss?

• We pointed at a few interesting areas, where engineers, computer science and mathematics go together well!

• **Topics:**
  – capacity of or-channel communication
    • (coordinated and un-coordinated)
  – codes *(still many problems to be solved!)*
    • (synchronized and un-synchronized)