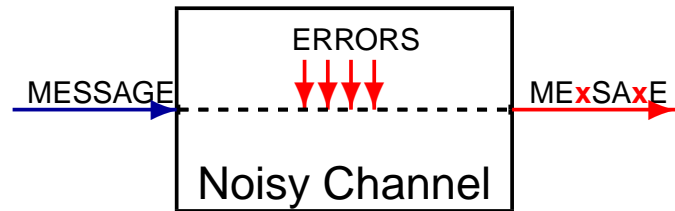


Hadamard and pseudo-noise matrices are equivalent;

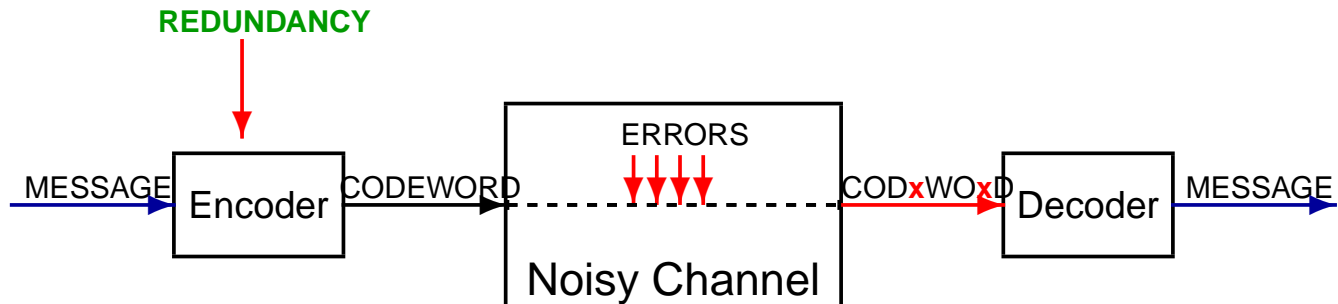
Tom Bella (joint work with Vadim Olshevsky and Lev Sakhnovich)

Department of Mathematics
University of Connecticut
Storrs, CT 06269 USA

Transmission over Noisy Channel, **No Coding Theory**

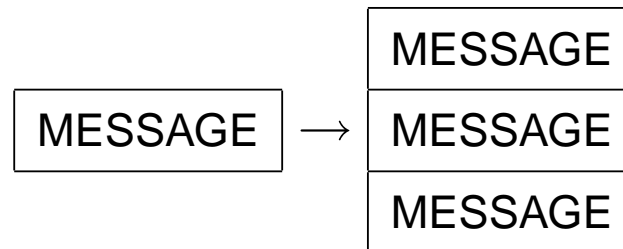


Transmission over Noisy Channel, **With Coding Theory**

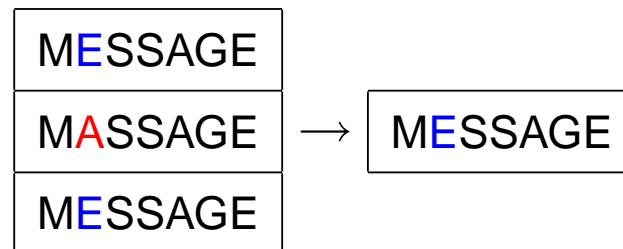


(A terrible) Example of Redundancy

Redundancy by Repetition:



Then the decoder is able to detect errors:

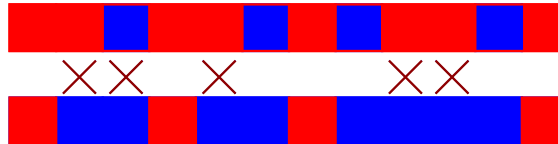


Redundancy by repetition is terrible. The code = { set of codewords } $3n$ -tuples (with the period n) is terrible. It allows one to correct only one error.

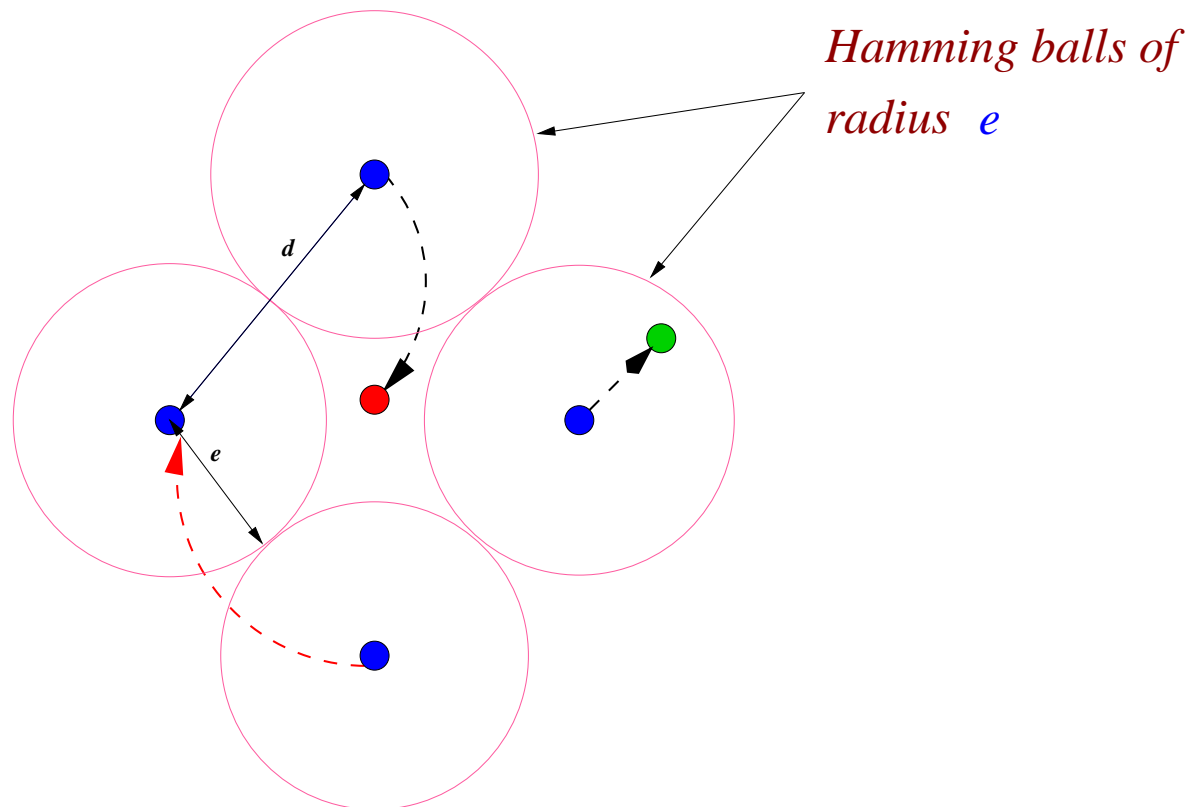
How to design codes with better error-correcting properties?

Minimum Distance Between Codewords

➡ The **Hamming distance**:



➡ The **code** with the **minimum distance** d allows to correct $e = \frac{d-1}{2}$ errors.



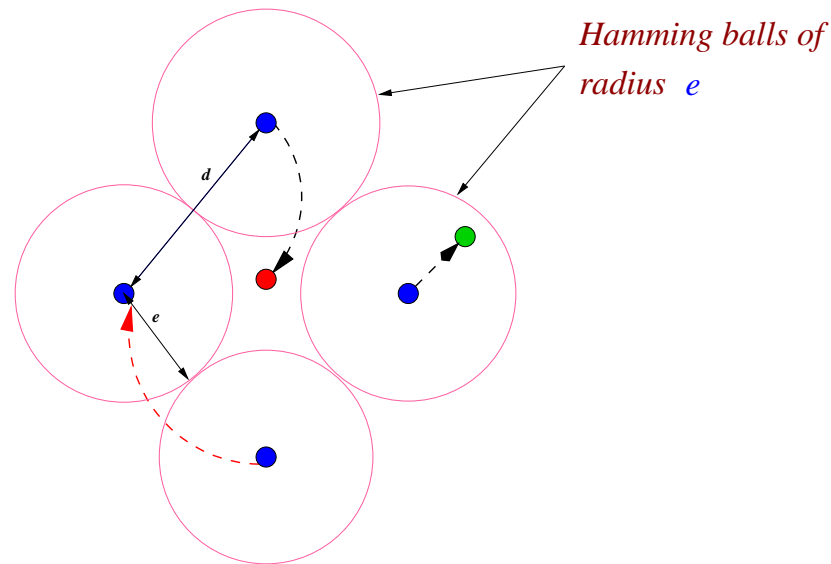
One of the Objectives of Coding Theory

Find Codes with **Large Minimum Distance**

- ▣▣▣▣ **Examples** of good codes with a large minimum distance :
 - ▣▣▣▣ The columns of **Hadamard matrices**
 - ▣▣▣▣ The columns of **PN matrices**
- ▣▣▣▣ **Why orthogonal matrices?**

What makes **Orthogonal Matrices** to be Useful for Coding?

- **Rows & Columns Orthogonal** - Any two rows/columns of an $n \times n$ matrix **disagree** in exactly $\frac{n}{2}$ places.
- The **minimum distance** between the columns is large: $\frac{n}{2}$



- This code is capable of **correcting** up to $\frac{n-2}{4}$ errors.

Two classical examples

▣▶ **Hadamard Matrices**

▣▶ **Pseudo-Noise (Pseudo-Random) Matrices**

Hadamard Matrices

Hadamard matrices of size $n \times n$, are $(-1, 1)$ matrices such that

$$H_n^T H_n = nI_n$$

A special case: **Hadamard-Sylvester matrices**

$$H_1 = [1], \quad H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

For example,

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

What are the **PN sequences** and the **PN matrices**?

- ▶ **Pseudo-Noise (Pseudo-Random) Sequences**
- ▶ **Pseudo-Noise (Pseudo-Random) Matrices**

Linear Recurring Sequences.

Linear m -term recurrence relation:

$$a_i = a_{i-1}h_{m-1} + a_{i-2}h_{m-2} + \cdots + a_{i-m+1}h_1 + a_{i-m}h_0 \quad \text{for } i \geq m$$

$m \times m$ Matrix formulation

$$\begin{bmatrix} a_{i-(m-1)} \\ a_{i-(m-2)} \\ a_{i-(m-3)} \\ \vdots \\ a_{i-1} \\ a_i \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ h_0 & h_1 & h_2 & \cdots & h_{m-2} & h_{m-1} \end{bmatrix} \begin{bmatrix} a_{i-(m)} \\ a_{i-(m-1)} \\ a_{i-(m-2)} \\ \vdots \\ a_{i-2} \\ a_{i-1} \end{bmatrix}$$

PN Sequences

➡ The output

$$a_0, a_1, a_2, a_3, a_4, \dots$$

of m -term recurrence relations is **PERIODIC!**

➡ **Fact:** The recurrence relations are m -term implying

$$\text{PERIOD} \leq (2^m - 1)$$

➡ **Definition:** A **sequence** is called **Pseudo-Noise sequence** if

$$\text{PERIOD} = (2^m - 1)$$

➡ **Example** In the above example with $m = 4$ we have:

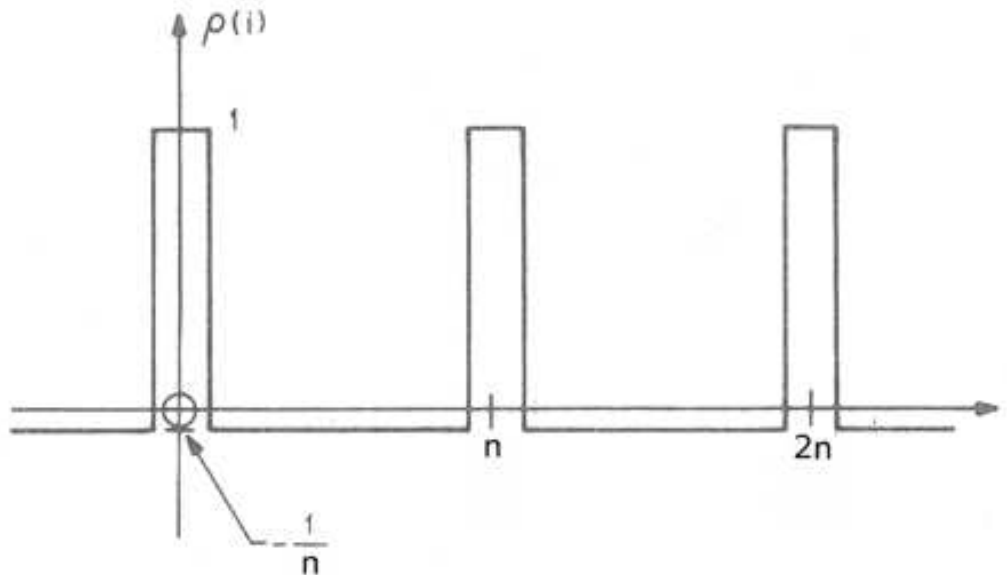
$$\underbrace{100011110101100}_{\text{period 15}} \underbrace{100011110101100}_{\text{period 15}} \underbrace{100011110101100}_{\text{period 15}} \dots$$

More Properties of PN Sequences

Autocorrelation function ρ given by

$$\rho(\tau) = \begin{cases} 1 & \tau = 0 \\ -\frac{1}{n} & 1 \leq \tau \leq n - 1 \end{cases}$$

where n is the length of the PN sequence, and τ is the shift.



Applications of PN Sequences

- **Digital Rights Management** - Including digital watermarking, steganography, etc, demonstrating and protecting copyright ownership of digital media is an important application.

Swanson-Zhu-Tewfik (1996)

- **Interference Estimation** - An important application to cellular systems.

Luo-Blostein (1998)

- **Synchronization Tasks** - Carrier phase, time, frequency, or frame synchronization.

Hoeher-Tufvesson (1999)

- **Communication Scrambling**

Feistel-Notz-Smith (1970)

PN Matrices

▣▣▣▣ A **Pseudo Noise Matrix** is one of the form

$$T = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & \tilde{T} & & \\ 0 & & & \end{bmatrix}$$

where \tilde{T} is a **circulant Hankel** matrix whose rows are **PN sequences**.

Theorem

- The $(0, 1)$ Hadamard-Sylvester matrices and the $(0, 1)$ PN matrices are equivalent, i.e., they can be obtained one from another via row and column permutations.
- **Sakhnovich(1998)** proved this result for $n = 16$ using combinatorial tricks.
- Our proof applies to arbitrary n , and it is based on the observation that the $(0, 1)$ Hadamard-Sylvester matrices of the size $2^m \times 2^m$ have rank m .

Proof

$$T = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

these $m = 4$ columns form a basis of the column space of \tilde{T}

Observation: the PN matrix has the rank m

$$\Rightarrow \text{rank}(\tilde{T}) = m$$

A Decomposition of PN Matrices

$$\tilde{T} = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix} \begin{bmatrix} I & R \end{bmatrix}$$

where $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$ is a $2^m - 1 \times m$ matrix, and $\begin{bmatrix} I & R \end{bmatrix}$ is an $m \times 2^m - 1$ matrix.

- \Rightarrow Uniqueness of rows of \tilde{T} imply uniqueness of rows in $\begin{bmatrix} M_1 \\ M_2 \end{bmatrix}$
- \Rightarrow Uniqueness of columns of \tilde{T} imply uniqueness of columns in $\begin{bmatrix} I & R \end{bmatrix}$
- \Rightarrow This uniqueness and the sizes of these matrices imply they contain **all possible binary m -tuples** as rows and columns.

A Decomposition of Hadamard-Sylvester Matrices

▣▣▣▣ Let H'_n denote the Hadamard-Sylvester matrix H_n with $(1, -1) \rightarrow (0, 1)$.

▣▣▣▣ Then H'_n has the decomposition

$$H'_n = \mathbf{L}_m \mathbf{L}_m^T$$

where $L_m = [l_{ij}]$ is an $n \times m$ matrix with $l_{ij} \in \{0, 1\}$ and the rows of L_m corresponding to all possible binary m -tuples.

Proof

This decomposition can be seen inductively:

▣▣▣▣ For $H'_2 = L_1 L_1^T$, we have $L_1 = [0 \ 1]^T$

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix}$$

▣▣▣▣ Assuming $H'_m = L_m L_m^T$ is true for size m one sees that

$$H'_{(m+1)} = \begin{bmatrix} H'_m & H'_m \\ H'_m & H'_m \end{bmatrix} = \underbrace{\begin{bmatrix} 0_m & L_m \\ 1_m & L_m \end{bmatrix}}_{L_{m+1}} \underbrace{\begin{bmatrix} 0_m^T & 1_m^T \\ L_m^T & L_m^T \end{bmatrix}}_{L_{m+1}^T}$$

$$\text{where } 0_m = \underbrace{[0 \ 0 \ \dots \ 0]^T}_{m \text{ zeros}} \quad 1_m = \underbrace{[1 \ 1 \ \dots \ 1]^T}_{m \text{ ones}}$$

This demonstrates the equivalence!

One more theorem on the rank structure of the Hadamard Matrices

▣▣▣▣ Let H_n be an arbitrary $n \times n$ Hadamard matrix

$$H_n \cdot H_n^T = nI.$$

▣▣▣▣ Then there are two cases:

▣▣▣▣ If n is divisible by 8 then

$$\text{rank} \widetilde{H}_n \leq \frac{n}{2}$$

▣▣▣▣ If n not divisible by 8 then

$$\text{rank} \widetilde{H}_n = n - 1.$$

▣▣▣▣ Here \widetilde{H}_n denotes H_n with -1 replaced by 0 's.