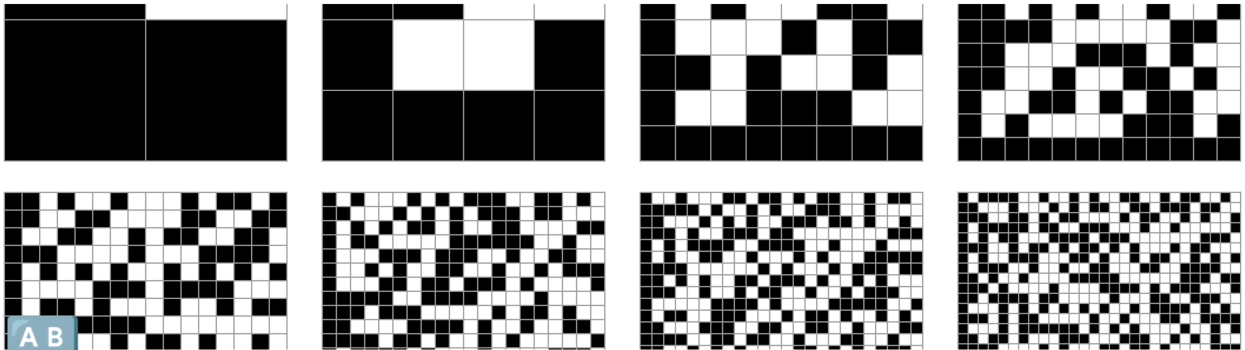

Plotkin bound & Hadamard design

Creat time	@August 15, 2022
Type	Essay
Topic	Combinatorics
Port time	@August 15, 2022
P.S.	
Property	

Introduction

> **Example 10** In a botanical classifier, a plant is identified by n features. Each feature can either be present or absent. A classifier is considered to be good if any two plants have **less than half** of their features in common. Prove that a good classifier cannot describe **more than** $n+1$ plants for odd n, or $\frac{n}{2}+1$ plants for even n.

💡 Here we may rephrased the question in the language of coding theory,

> What is the largest binary code with length n and distance $\lfloor n/2 \rfloor + 1$?

▼ **Proof**

We denote S as the set of binary code. For any possible S, $m := |S|$.

Let X be a random variable such that $X_i = 1$ whenever the chosen pair differs in the i-th entry, $X_i = 0$ otherwise. It is clear that $X \sim B(0,1)$. The expectation of pairs in S distinct in the i-th entry is

$$\mathbb{E}X_i = \frac{m_i(m-m_i)}{\binom{m}{2}} \leq \frac{m^2}{4 \cdot m(m-1)/2} = \frac{m}{2(m-1)}.$$

Here m_i is the number of $v \in S$ taking value 1 in the i-th entry. Since $\sum_{i=1}^n X_i$ is the total number of entries where pairs taking different values, we shall exclude those m such that

$$\begin{aligned} \mathbb{E}\sum_{i=1}^n X_i &\leq \frac{mn}{2(m-1)} < \frac{n+1}{2} \quad \text{when } n \text{ is odd,} \\ \mathbb{E}\sum_{i=1}^n X_i &\leq \frac{mn}{2(m-1)} < \frac{n}{2}+1 \quad \text{when } n \text{ is even.} \end{aligned}$$

Therefore, $\sup|S| \leq n+1$ for odd n, $\sup|S| \leq n/2$ for even n.

Question: When the equality holds? IT IS ALREADY ANSWERED in Plotkin bound & Hadamard design.

Basic definitions

See this page to know baisc definitions to coding theory.

The main theorem

Theorem The theorem says that

> *The maximum number of a length n binary code with minimum distance $\lceil n/2 \rceil$ is*
>
> 1. $4k+4$, *if* $n = 4k+3$;
> 2. $2k+2$, *if* $n = 4k+2$;
> 3. $2k+2$, *if* $n = 4k+1$;
> 4. $4k+4$, *if* $n = 12k+8$;
> 5. $4k+2$, *if* $n = 12k+4$;

> 6. $4k$, if $n = 12k$.
>
> We denote them by **Case I** to **VI**.

Theorem* (in equivalent statement) Let $\Sigma^n = \{\pm 1\}^n$. Then for each set $S \subset \Sigma^n$ such that

$$\forall x, y \in S, \langle x, y \rangle < 0,$$

we have

1. $|S| \le 4k + 4$, if $n = 4k + 3$,
2. ……

Construction

Definition We call $H_m \in \{\pm 1\}^{m \times m}$ an **Hadamard matrix** whenever $H_m \cdot H_m^T = m \cdot I$.

Theorem The Hadamard matrix H_m does not exist if $m \notin (4\mathbb{N} \cup \{1, 2\})$.

▼ **Proof of the theorem**

Consider the first 3 rows, i.e.,

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \\ b_1 & b_2 & \cdots & b_{n-1} & b_n \end{pmatrix}.$$

Let $N_{\delta,\varepsilon}$ denotes the the number of pairs $(a_j, b_j) = (\delta, \varepsilon)$. Here $\delta, \varepsilon \in \{\pm 1\}$. Then

- $N_{1,\varepsilon} = N_{-1,\varepsilon}$ since $r_1 \perp r_2$,
- $N_{\delta,1} = N_{\delta,-1}$ since $r_1 \perp r_3$,
- $N_{1,1} + N_{-1,-1} = N_{1,-1} + N_{-1,1}$ since $r_2 \perp r_3$.

As a result, $N_{\varepsilon,\delta} = \frac{n}{4}$. Thus n is a mutiple of 4.

Conjecture There is a Hadamard matrix of order $n = 4k$ for every integer $k \ge 1$.

> 💡 **Fact 1** The undecided cases for $n < 2000$ are $668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964$.
>
> **Fact 2** The Kronecker product of Hadamard matrices is also an Hadamard matrix. Especially, if the Hadamard matrix of q exists, then $H_{2^\ell \cdot q}$ exists for each $\ell \in \mathbb{N}$. One feasible construction is by iterating $\otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Notation Let $H_m = (h_{ij})_{m \times m}$ be an Hadamard matrix.

> 💡 Without the loss of generality, take $h_{i,j} = 1$ if $\min(i, j) = 1$.

- Let H_m' be an $m \times (m-1)$ matrix given by deleting the first column of H_m.
- Let H_m'' be an $\frac{m}{2} \times (m-2)$ matrix given by deleting all rows from H_m' whose first entry is -1. Then deleting the first column of the remainder.

Example For instance,

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$H_4' = \begin{pmatrix} \xcancel{1} & 1 & 1 & 1 \\ \xcancel{1} & 1 & -1 & -1 \\ \xcancel{1} & -1 & 1 & -1 \\ \xcancel{1} & -1 & -1 & 1 \end{pmatrix},$$

$$H_4'' = \begin{pmatrix} \xcancel{1} & \xcancel{1} & 1 & 1 \\ \xcancel{1} & \xcancel{1} & -1 & -1 \\ \xcancel{1} & \xcancel{-1} & \xcancel{1} & \xcancel{-1} \\ \xcancel{1} & \xcancel{-1} & \xcancel{-1} & \xcancel{1} \end{pmatrix}.$$

Construction

- The **theorem** says that

  The maximum number of a length n binary code with minimum distance $\lceil n/2 \rceil$ is

  1. $4k+4$, if $n = 4k+3$;
  2. $2k+2$, if $n = 4k+2$;
  3. $2k+2$, if $n = 4k+1$;
  4. $4k+4$, if $n = 12k+8$;
  5. $4k+2$, if $n = 12k+4$;
  6. $4k$, if $n = 12k$.

  We denote them by **Case I** to **VI**.

- **Construction of Case I**

  Consider the set of rows in H'_{n+1}.

  - **Example of $n = 7$**

    Here the **black**-coloured part is H'_8.

$$\begin{pmatrix} \cancel{1} & \cancel{1} & \cancel{1} & \cancel{1} & \cancel{1} & \cancel{1} & \cancel{1} & \cancel{1} \\ \cancel{1} & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ \cancel{1} & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ \cancel{1} & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \cancel{1} & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \cancel{1} & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ \cancel{1} & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ \cancel{1} & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

- **Construction of Case II**

  Consider the set of rows in H''_{n+2}.

  - **Example of $n = 6$**

    Here the **black**-coloured part is H''_8.

$$\begin{pmatrix} \cancel{1} & \cancel{1} & 1 & 1 & 1 & 1 & 1 & 1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} \\ \cancel{1} & \cancel{1} & -1 & -1 & 1 & 1 & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} \\ \cancel{1} & \cancel{1} & 1 & 1 & -1 & -1 & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} \\ \cancel{1} & \cancel{1} & -1 & -1 & -1 & -1 & 1 & 1 \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} \end{pmatrix}.$$

- **Construction of Case III**

  1️⃣ Take the set of rows in of H''_{n+3}.

  2️⃣ Delete any column in what is obtained in 1️⃣.

  - **Example of $n = 5$**

    1️⃣ Here the **black**-coloured part is H''_8.

$$\begin{pmatrix} \cancel{1} & \cancel{1} & 1 & 1 & 1 & 1 & 1 & 1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} \\ \cancel{1} & \cancel{1} & -1 & -1 & 1 & 1 & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} \\ \cancel{1} & \cancel{1} & 1 & 1 & -1 & -1 & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} \\ \cancel{1} & \cancel{1} & -1 & -1 & -1 & -1 & 1 & 1 \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} \end{pmatrix}.$$

2️⃣ The remainder is our desired result.

$$\begin{pmatrix} \cancel{1} & \cancel{1} & \cancel{1} & 1 & 1 & 1 & 1 & 1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} \\ \cancel{1} & \cancel{1} & \cancel{-1} & -1 & 1 & 1 & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} \\ \cancel{1} & \cancel{1} & \cancel{1} & 1 & -1 & -1 & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} \\ \cancel{1} & \cancel{1} & \cancel{-1} & -1 & -1 & -1 & 1 & 1 \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} \end{pmatrix}.$$

▼ **Construction of Case IV**

1️⃣ Let $m = \frac{n+4}{3}$.

2️⃣ Concatenate 3 copies of H'_m horizontally.

3️⃣ Delete any column in what is obtained in 2️⃣.

▼ **Example of $n = 8$**

1️⃣ As $n = 8$, $m = 4$.

2️⃣ Concatenate 3 copies of H'_4 horizontally, i.e.,

$$\left(\begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \end{array}\right).$$

3️⃣ Delete any column, e.g.,

$$\left(\begin{array}{ccc|ccc|ccc} \cancel{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \cancel{1} & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ \cancel{-1} & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ \cancel{-1} & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \end{array}\right).$$

▼ **Construction of Case V**

1️⃣ Let $a = \frac{n+8}{3}$, $b = \frac{2(n+2)}{3}$.

2️⃣ Concatenate first $\frac{b}{2}$ rows of H'_a horizontally with H''_b.

3️⃣ Delete any column of the outcome in 2️⃣.

▼ **Example of $n = 4$**

1️⃣ As $n = 4$, $a = b = 4$.

2️⃣ Concatenate first 2 rows of H'_4 horizontally with H''_4. i.e.,

$$\left(\begin{array}{cccc|cccc} \cancel{1} & 1 & 1 & 1 & \cancel{1} & \cancel{1} & 1 & 1 \\ \cancel{1} & 1 & -1 & -1 & \cancel{1} & \cancel{1} & -1 & -1 \\ \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} & \cancel{1} & \cancel{-1} \\ \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} & \cancel{1} & \cancel{-1} & \cancel{-1} & \cancel{1} \end{array}\right).$$

3️⃣ Delete any column, e.g.,

$$\left(\begin{array}{cccc|cccc} \xcancel{1} & \xcancel{1} & 1 & 1 & \xcancel{1} & \xcancel{1} & 1 & 1 \\ \xcancel{1} & \xcancel{1} & -1 & -1 & \xcancel{1} & \xcancel{1} & -1 & -1 \\ \xcancel{1} & \xcancel{-1} & \xcancel{1} & \xcancel{-1} & \xcancel{1} & \xcancel{-1} & \xcancel{1} & \xcancel{-1} \\ \xcancel{1} & \xcancel{-1} & \xcancel{-1} & \xcancel{1} & \xcancel{1} & \xcancel{-1} & \xcancel{-1} & \xcancel{1} \end{array}\right).$$

▼ Construction of Case VI

1️⃣ Let $a = \frac{n}{3}$, $b = \frac{2n}{3} + 4$.

2️⃣ Concatenate first a rows of H''_b horizontally with H'_a.

3️⃣ Delete any column of the outcome in 2️⃣.

▼ Example of $n = 12$

1️⃣ As $n = 12$, $a = 4$ and $b = 12$.

▼ Hadamard matrix H_{12}

The first 4 column of H''_{12} is ***marked***.

1	1	*1*	*1*	*1*	*1*	*1*
1	1	*-1*	*-1*	*1*	*-1*	*1*
1	1	*-1*	*-1*	*-1*	*1*	*-1*
1	1	*1*	*-1*	*-1*	*-1*	*1*
1	1	1	1	-1	-1	-1
1	1	-1	1	1	1	-1
1	-1	1	-1	1	1	1
1	-1	-1	1	-1	1	1
1	-1	1	-1	-1	1	-1
1	-1	-1	1	-1	-1	1
1	-1	-1	-1	1	-1	-1
1	-1	1	1	1	-1	-1

2️⃣ Concatenate first 4 rows of H''_{12} horizontally with H'_4. i.e.,

$$\left(\begin{array}{cccccccccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \end{array}\right).$$

3️⃣ Delete any column, e.g.,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \xcancel{1} & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & \xcancel{1} & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & \xcancel{-1} & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & \xcancel{-1} & -1 & 1 \end{pmatrix}.$$

▼ Hadamard 矩阵拷贝懒人包

See here for data basis of Hadamard matrices.

以下给出一种处理 Hadamard 矩阵的捷径. 以构造 H''_{12} 的前四行与 H'_4 之并列复合为例:

1️⃣ 在数据库中搜寻 H_{12}, 例如此处.

2️⃣ 将 1️⃣ 中结果复制至 spreadsheet 文件中, 例如 `Microsoft excel`.

3️⃣ 使用 `数据->分列->分隔符号(D)->空格` 指令进行分列.

4️⃣ 采用 `筛选`, `排序` 等指令调整矩阵. 若需调换 `1<->(-1)`, 可考虑 `(-1)->2, 1->(-1), 2->1` 三步.

5️⃣ 如需要复制为 LaTeX 矩阵, 替换 `1->1&`, 最末一行进行替换 `&->//`.

6️⃣ 将所得者拷贝至 `记事本`, 依个人喜好替换空格与 `tab` 缩进.