#CátedrasCiber

Recent Advances in the Construction of Hadamard Matrices Using Legendre Pairs

29/V/2025

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

UC | Universidad de Cantabria

Binary Legendre Pairs

Two sequences $\mathbf{a} = [a_1, \ldots, a_T], \mathbf{b} = [b_1, \ldots, b_T]$ of period T form a Legendre pair if

$$\mathrm{PAF}(\mathbf{a}, j) + \mathrm{PAF}(\mathbf{b}, j) = -2, \quad j = 1, \ldots, \left\lceil \frac{T}{2} \right\rceil .$$

where

$$\mathrm{PAF}(\mathbf{a}, j) = \sum_{i=1}^{T} a_i \cdot a_{i+j},$$

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Hadamard Matrices

Let $\mathrm{C_a}$ be the circulant matrix obtained from a, where the $(j+1)$-th row of $\mathrm{C_a}$ is a circulant shift of a by j, defined as:

$$\mathbf{C}_{i,j}(\mathbf{a}) = a_{(i-j) \bmod T}$$

for each $i, j \in \{1, \ldots, T\}$. Then the following matrix

$$H = \begin{bmatrix} -1 & -1 & \mathbf{1} & \mathbf{1} \\ -1 & 1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}' & \mathbf{1}' & \mathbf{C_b} & \mathbf{C_a} \\ \mathbf{1}' & -\mathbf{1}' & \mathbf{C_a}' & -\mathbf{C_b}' \end{bmatrix}$$

is a binary Hadamard Matrix (Theorem 3, Fletcher et al. 2001).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Known Constructions

The Legendre symbol is defined as,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue modulo p}, \\ -1 & \text{otherwise.} \end{cases}$$

The Legendre sequence ℓ of period p is defined as $\ell_1 = 1$, and $\ell_i = \left(\frac{i-1}{p}\right),\ i = 2, \ldots, p$.
This sequence gives the Paley construction.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Conjectures

- There exists binary Legendre Pairs for all T odd (Arasu et al. 2020)
- Values of the Power Spectral Density for $T \equiv 0 \mod 3, 5$ (Kotsireas, Koutschan, etc)
- Sums of the elements of the sequence can be fixed

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

M-Compression

For a sequence $\mathbf{a}$ of composite length $T = M \cdot N$, its *M-compression* is the sequence $\mathbf{A}$ defined as,

$$A_j = \sum_{i=1}^{M} a_{N \cdot i + j}.$$

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Take

$$1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1$$

its 9-compression is $1, 3, -3$.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

M-Compression

Let $(\mathbf{a}, \mathbf{b})$ be a binary Legendre Pair and (A, B) the M-compressions of the pair. Then the following relation

$$\mathrm{PAF}(\mathbf{A}, j) + \mathrm{PAF}(\mathbf{B}, j) = -2 \cdot M,$$

holds.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Candidates for compression pairs

Suppose that $T = p \cdot q^2$, the following sequences:

$$\mathbf{A}(p,q) = \left[1, q \cdot \left(\frac{1}{p}\right), \ldots, q \cdot \left(\frac{p-1}{p}\right)\right],$$
$$\mathbf{B}(p,q) = \left[1, -q \cdot \left(\frac{1}{p}\right), \ldots, -q \cdot \left(\frac{p-1}{p}\right)\right].$$

satisfies, $\mathrm{PAF}(\mathbf{A}(p,q), j) + \mathrm{PAF}(\mathbf{B}(p,q), j) = -2 \cdot q^2, \qquad j = 1, \ldots, p-1.$

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Conjecture (Kotsireas 2019)

For every odd primes p and q, the pair of sequences $(\mathbf{A}(p,q), \mathbf{B}(p,q))$ can indeed be uncompressed to a Binary Legendre pair of period $q^2 \cdot p$.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Decimations

Given a pair of sequences (s, r) and a positive integer d, if $r_i = s_{d \cdot i \mod T}$, for all $i \in \{1, \dots T\}$, then r is called a *d-decimation* sequence of s and it is denoted as $\mathrm{r} = \mathrm{s}^{(d)}$.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Decimations

Original sequence:

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

4-Decimated sequence:

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.

Decimations

Supposing that $(\mathbf{a}, \mathbf{b})$ is a binary Legendre pair whose q^2-compression is $(\mathbf{A}(p,q), \mathbf{B}(p,q))$ and $\gcd(d, T) = 1$,

- $(\mathbf{a}^{(d)}, \mathbf{b}^{(d)})$ is also a Legendre pair
- $(\mathbf{A}^{(d)}(p,q), \mathbf{B}^{(d)}(p,q))$ is the M-compression of $(\mathbf{a}^{(d)}, \mathbf{b}^{(d)})$
- $(\mathbf{A}(p,q)^{(d)}, \mathbf{B}(p,q)^{(d)})$ is either $(\mathbf{A}(p,q)^{(d)}, \mathbf{B}(p,q)^{(d)})$ or $(\mathbf{B}(p,q)^{(d)}, \mathbf{A}(p,q)^{(d)})$.
- for some d, the sum of the first q elements of $\mathbf{a}^{(d)}(p,q)$ satisfies

$$\sum_{i=1}^{p} a^{(d)}(p,q)_i \geq -q - 1.$$

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Generation of binary sequences

A binary sequence $\mathbf{s} \in \{0, 1\}$ satisfying

$$s_{i+L} = \sum_{j=0}^{L-1} c_j s_{i+j} \mod 2,$$

for all $i \in \mathbb{N}$ is called an (L-th order) *linear recurring sequence (LRS)*.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Discrete Fourier Transform over fields

We define the Discrete Fourier Special Transform $\mathrm{DFS}(\mathrm{s})$ as the T periodic sequence $\hat{\mathrm{S}}$ defined by

$$\hat{S}_k = \sum_{i=1}^{T} s_i \cdot \alpha^{i \cdot k} \quad k = 1, \ldots, T,$$

where α is a primitive element of a finite field of characteristic 2.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Properties of Legendre sequence (Helleseth et al.)

Define $\bar{s}$ as the sequence satisfying: $\ell = (-1)^{\bar{s}}$, then the linear complexity of the sequence is greater than $p/2$.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Conjecture

Supposing that (a, b) is a binary Legendre pair whose q^2-compression is $(\mathbf{A}(p,q), \mathbf{B}(p,q))$, then the linear complexity of $\overline{\mathrm{a}}$ and $\overline{\mathrm{b}}$ is greater than $q \cdot p^2/2$, where where

$$a_i = (-1)^{\overline{a}_i}, \quad b_i = (-1)^{\overline{b}_i}$$

for all $i \in \mathbb{N}$. Also, more than $q^2 \cdot p/2$ elements in $\mathrm{DFS}(\overline{\mathrm{a}})$ are non zero.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

Results and Conclusions

- Legendre Pairs are a promising construction for finding binary Hadamard Matrices
- For certain lengths, computer search can be improved due to existence of particular binary Legendre Pairs
- Thanks to the use of a Computer Cluster we found Legendre Pairs up to length 75

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
UC Universidad de Cantabria

#CátedrasCiber

Recent Advances in the Construction of Hadamard Matrices Using Legendre Pairs

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

UC | Universidad de Cantabria