Geometric Approach to Generating Legendre Pairs

Capt Jonathan Turner

Department of Mathematics and Statistics/ENC
Air Force Institute of Technology

1-4 August, 2019
1 Definitions

2 Generation

3 Sorting

4 Newly Discovered Legendre Pairs
1. Definitions
2. Generation
3. Sorting
4. Newly Discovered Legendre Pairs
Definitions

- Note: All index operations are modulo $\ell$, where $\ell$ is the length of $\mathbf{v}$.

- A **circulant shift** of a vector $\mathbf{v}$, denoted $c_j(\mathbf{v})$, is a transformation, such that $(c_j(\mathbf{v}))_i = \mathbf{v}_{i-j}$.

- A **circulant matrix** defined by a vector, $\mathbf{v}$, denoted $C_\mathbf{v}$, is a square matrix such that the $j^{th}$ row of $C_\mathbf{v}$ is $c_j(\mathbf{v})$.

- A **decimation** of a vector $\mathbf{v}$, denoted $d_j(\mathbf{v})$, is a transformation such that $(d_j(\mathbf{v}))_i = \mathbf{v}_{ij}$. 
Legendre Pairs

- The **periodic autocorrelation function** of a binary vector $v$ of length $\ell$ is a vector of length $\ell$ such that for each $j \in \mathbb{Z}_\ell$:

$$P_v = C_v v$$

- Vectors $u, v \in \mathbb{Z}_2^\ell$ constitute a **Legendre Pair** (LP) if and only if for some constant $a$:

$$P_v(j) + P_u(j) = a, \quad \forall \ j \neq 0$$

- $a = \frac{\ell+1}{2}$ for purpose of this research

- Each vector under consideration here has:
  - Odd length, $\ell$; Density $\frac{\ell+1}{2}$
Definitions

- A necklace, $U$, is an equivalence class under circulant shifts.

- A bracelet, $B$, is an equivalence class under circulant shifts and decimation by $-1$ (*reversals*).

- A decimation class, $D$, is an equivalence class of vectors of length $\ell$ under circulant shifts and decimation by $j \in \mathbb{Z}_\ell^*$.

- $U \subset B \subset D$
1. Definitions

2. Generation

3. Sorting

4. Newly Discovered Legendre Pairs
Necklace Generation Timeline


  - Djokovic 2015

- 2013: Sawada et al: CAT Fixed Density Necklace generation

- 2013: Karim et al: CAT Fixed Content Bracelet generation
Short DFT Refresher

- Define $\omega = e^{2\pi i / \ell}$, the $\ell^{th}$ root of unity.

- Define $F$ to be the $\ell \times \ell$ matrix such that $F_{j,k} = \omega^{jk}$

- For a vector $\mathbf{v}$ of length $\ell$, $\mu = F\mathbf{v}$ is the Discrete Fourier Transform (DFT) of $\mathbf{v}$. 
Effect of Circulant Shifts on DFT

- Let $\mu_1 = r_1 e^{i\theta_1}$ be the 1st DFT component of $v$.

- Let $u = c_j(v)$ and $\gamma_1 = r_1 e^{i\psi_1}$ be the 1st DFT component of $u$.

- Then $\psi_1 = \frac{2\pi j}{\ell} + \theta_1$. 
New Lexicon

- Consider the following Bracelet lexicon:

  \[ \mathbf{v} < \mathbf{u} \text{ if and only if } 0 \leq \theta_1 < \psi_1 < 2\pi \]

- If \( \theta_1 < 2\pi/\ell \), then \( \mathbf{v} \) is the necklace representative.
- If \( \theta_1 \leq \pi/\ell \), then \( \mathbf{v} \) is the bracelet representative.
Unrestricted Space
Necklace Space
Bracelet Space

Figure: Necklace

Figure: Bracelet
Decimation Class Feasible Space

- Fletcher et al’s PSD Test restricts $|\mu_k|^2 \leq \frac{\ell + 1}{2}$

- We proved every PSD contains a relatively prime component:

  $|\mu_k|^2 \leq \frac{\ell + 1}{4}$

- We can force that restriction on the first PSD
PSD Test

Figure: PSD Test

Figure: Half PSD
Spatial Comparison
Determining Attainable Region

- Assume $\mu$ is a combination of $k$ elements from $\{\omega^0, \omega^1, \ldots, \omega^j\}$

- Then indices $\{j + 1, \ldots, \ell - 1\}$ remain undetermined and exactly $\frac{\ell + 1}{2} - k$ indices must be active:
  - There exists the equivalent/symmetric problem of determining which indices to not activate.

- Attainable region representable as intersection of two disks
  - Centered around current location (no remaining indices activated)
  - Centered around distant location (all remaining indices activated)
Attainable
Feasible and Attainable
1. Definitions

2. Generation

3. Sorting

4. Newly Discovered Legendre Pairs
Pseudo-Symmetric Functions

- We define a Pseudo-Symmetric function to be any function which is symmetric over a defined subset.
  - Such as the set of all \( \ell \) indices, or set of relatively prime indices
  - Or set of indices corresponding to a specific divisor

- Correlation Energy: \( f(\mathbf{v}) = \sum_j (|\mu_j|^2)^2 \)
  - If \( \mathbf{u} \) and \( \mathbf{v} \) are LP, then \( f(\mathbf{v}) = f(\mathbf{u}) \)

- For each divisor \( \delta|\ell \), there exists a unique integer constant \( c \) such that
  \[
  \sum_{j=1}^{(\delta-1)/2} |\mu_{\delta j}|^2 = a\delta + c
  \]
  - Let \( \sum_{j=1}^{(\delta-1)/2} |\mu_{\delta j}|^2 = a\delta + c \); \( \sum_{j=1}^{(\delta-1)/2} |\gamma_{\delta j}|^2 = b\delta + c \)
  - If \( \mathbf{u} \) and \( \mathbf{v} \) are LP, then \( a + b \) is a constant.
Autocorrelation Logic

- If \( \mathbf{u} \) and \( \mathbf{v} \) are LP, then:
  \[
  \max_{j \in \mathbb{Z}_\ell^*} P_u(j) = \frac{\ell+1}{2} - \min_{j \in \mathbb{Z}_\ell^*} P_v(j)
  \]
  Djokovic 2018 (Algs for difference families in finite abelian groups)

- For each divisor \( \delta | \ell \)
  \[
  \max_{j \in \ell \mathbb{Z}_\delta} P_u(j) = \frac{\ell+1}{2} - \min_{j \in \ell \mathbb{Z}_\delta} P_v(j)
  \]

- \( | \max_{j \in \mathbb{Z}_\ell^*} P_u(j) | = | \min_{j \in \mathbb{Z}_\ell^*} P_v(j) | \)
Sorting

- Vectors are sorted into bins based upon preceding criteria
- Each bin is linked to a pair satisfying LP conditions
- New vectors are checked against all residents in paired bins
- Lots of bins means very few expensive comparisons
Memory Heuristic

- LP often have relatively low correlation energy
  - Within $2\ell$ of theoretical minimum

- Heuristic: Do not store any vector with Correlation Energy greater than $m + 2\ell$ where $m$ is theoretical minimum Correlation Energy
1 Definitions

2 Generation

3 Sorting

4 Newly Discovered Legendre Pairs
Algorithm Discovered LP

$\ell = 55$

$U = [000001110110101001001010010011100001100110101111011011]$  
$V = [0111100011111011000011111010101100100110010000001001001]$

Vectors Generated: 3,408,821 (1.96E-6)  
Time (sec): 115,341 (32.04 hrs) (1.34 days)

$\ell = 57$

$U = [000001111110110010101001110000100010100100110111101110101]$  
$V = [0100111011010010111001111110000110000101010000110110]$  

Vectors Generated: 21,537,161 (2.94E-6)  
Time (sec): 932,824 (259.12 hrs) (10.80 days)
### Newly Discovered Legendre Pairs

#### Interim LP Discoveries

<table>
<thead>
<tr>
<th>( \ell )</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U_1 )</td>
<td>[11111110100101000110000110110110000100111001010100110]</td>
</tr>
<tr>
<td>( V_1 )</td>
<td>[1000111100100011101010001110010011011110101100]</td>
</tr>
<tr>
<td>( U_2 )</td>
<td>[111111101100000111100110000100111010100001101001011010]</td>
</tr>
<tr>
<td>( V_2 )</td>
<td>[1010000000111110011001011000001110110010111101011]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \ell )</th>
<th>57</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U )</td>
<td>[11111110011010110110010100000010100111110110000101100111000]</td>
</tr>
<tr>
<td>( V )</td>
<td>[100100101111101011110001000011001100100011001011101001011]</td>
</tr>
</tbody>
</table>
Future Work

- Equation to replace Counting Algorithm
- Enforce novel bracelet definition on Chiarandini’s TABU Search
- Reduce computations in generation algorithm’s feasibility checks
- Alter generation procedure to encourage early LP generation
- Loopless Bracelet Generation
- Constant order decimation class representative verification