The two-modular Fourier transform
of binary functions

Yi Hong (Monash University, Melbourne, Australia)
Emanuele Viterbo (Monash University, Melbourne, Australia)
Jean-Claude Belfiore (Telecom ParisTech)
$N$ samples of a discrete-time signal (real or complex) form the time-domain vector $x = (x[n])_{n=0}^{N-1}$

The discrete Fourier transform (DFT) of $x$ is the frequency-domain vector $X = (X[k])_{k=0}^{N-1}$

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-j2\pi \frac{nk}{N}} \quad k = 0, \ldots, N - 1$$

The inverse discrete Fourier transform (IDFT) of $X$ is

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k] e^{j2\pi \frac{nk}{N}} \quad n = 0, \ldots, N - 1$$
The vector $\mathbf{x} = (x[n])_{n=0}^{N-1}$ gives the $N$ samples of a time-domain function $f : \mathbb{Z} \rightarrow \mathbb{C}$

If $f$ is periodic by $N$ samples then $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ (assumption for DFT to provide the discrete spectrum)

The time axis $\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}$ is an additive group $G = (\mathbb{Z}_N, +)$ with addition mod $N$ then $f : G \rightarrow \mathbb{C}$

In the frequency domain $\mathbf{X} = (X[k])_{k=0}^{N-1}$ represents the transform of $f$ as a periodic function $\hat{f} : G \rightarrow \mathbb{C}$

The frequency axis has the same additive group structure $G = (\mathbb{Z}_N, +)$
The Discrete Fourier Transform

- The DFT matrix \( \mathbf{F} = \{ e^{-j2\pi \frac{nk}{N}} \}^{N-1}_{n,k=0} \) is a unitary matrix such that
  \[
  \mathbf{X}^T = \mathbf{F}\mathbf{x}^T \quad \mathbf{x}^T = \frac{1}{N} \mathbf{F}^H \mathbf{X}^T
  \]

- The vectors \( \mathbf{x} \) and \( \mathbf{X} \) are a two representations of the signal \( x[n] \) in different coordinate systems, defined by the time basis and frequency basis.

\[\text{Diagram:} \quad \begin{aligned}
\text{time} & \quad \text{frequency} \\
\mathbf{x} & \quad \mathbf{X} \\
x[n] & \quad \text{Coordinate Systems}
\end{aligned}\]
One-dimensional group representation

The Abelian group \( G = (\mathbb{Z}_N, +) \) with addition mod \( N \) admits the following one-dimensional representations

\[
\chi_k : G \to S_k \subset \mathbb{C} \quad \chi_k(n) = e^{-j2\pi \frac{nk}{N}}
\]

where \( k = 0, \ldots, N - 1 \) and

\[
S_k = \left\{ 1, e^{-j2\pi \frac{k}{N}}, e^{-j2\pi \frac{2k}{N}}, \ldots, e^{-j2\pi \frac{(N-1)k}{N}} \right\}
\]

The representation \( \chi_k \) is a group homomorphism transforming the addition mod \( N \) in \( G \) into the multiplication of \( N \)-th roots of unity in \( S_k \), i.e., for any \( a, b \in G \)

\[
\chi_k(a + b) = \chi_k(a)\chi_k(b) \quad \text{since} \quad e^{-j2\pi \frac{(a+b)k}{N}} = e^{-j2\pi \frac{ak}{N}} e^{-j2\pi \frac{bk}{N}}
\]
Example $\mathbb{Z}_6$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$S_k = { \chi_k(g), g \in G = {0, 1, 2, 3, 4, 5} }$</th>
<th>$\text{Ker}(\chi_k), \ G/\text{Ker}(\chi_k)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>${1}$</td>
<td>${0, 1, 2, 3, 4, 5}, {0}$</td>
</tr>
<tr>
<td>1</td>
<td>${1, e^{-j\frac{2\pi}{6}}, e^{-j\frac{4\pi}{6}}, e^{-j\frac{6\pi}{6}}, e^{-j\frac{8\pi}{6}}, e^{-j\frac{10\pi}{6}}}$</td>
<td>${0}, {0, 1, 2, 3, 4, 5}$</td>
</tr>
<tr>
<td>2</td>
<td>${1, e^{-j\frac{4\pi}{6}}, e^{-j\frac{8\pi}{6}}}$</td>
<td>${0, 3}, {0, 2, 4}$</td>
</tr>
<tr>
<td>3</td>
<td>${1, -1}$</td>
<td>${0, 2, 4}, {0, 3}$</td>
</tr>
<tr>
<td>4</td>
<td>${1, e^{j\frac{4\pi}{6}}, e^{j\frac{8\pi}{6}}}$</td>
<td>${0, 3}, {0, 2, 4}$</td>
</tr>
<tr>
<td>5</td>
<td>${1, e^{j\frac{2\pi}{6}}, e^{j\frac{4\pi}{6}}, e^{j\frac{6\pi}{6}}, e^{j\frac{8\pi}{6}}, e^{j\frac{10\pi}{6}}}$</td>
<td>${0}, {0, 1, 2, 3, 4, 5}$</td>
</tr>
</tbody>
</table>
Example $\mathbb{Z}_6$ (cont.)

<table>
<thead>
<tr>
<th>$g \in G$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_0(g)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_1(g)$</td>
<td>$e^{-j \frac{2\pi}{6}}$</td>
<td>$e^{-j \frac{4\pi}{6}}$</td>
<td>$e^{-j \frac{6\pi}{6}}$</td>
<td>$e^{-j \frac{8\pi}{6}}$</td>
<td>$e^{-j \frac{10\pi}{6}}$</td>
<td>$\psi_0$</td>
</tr>
<tr>
<td>$\chi_2(g)$</td>
<td>1</td>
<td>$e^{-j \frac{4\pi}{6}}$</td>
<td>$e^{-j \frac{8\pi}{6}}$</td>
<td>1</td>
<td>$e^{-j \frac{4\pi}{6}}$</td>
<td>$e^{-j \frac{8\pi}{6}}$</td>
</tr>
<tr>
<td>$\chi_3(g)$</td>
<td>1</td>
<td>$-1$</td>
<td>1</td>
<td>$-1$</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>$\chi_4(g)$</td>
<td>1</td>
<td>$e^{j \frac{4\pi}{6}}$</td>
<td>$e^{j \frac{8\pi}{6}}$</td>
<td>1</td>
<td>$e^{j \frac{4\pi}{6}}$</td>
<td>$e^{j \frac{8\pi}{6}}$</td>
</tr>
<tr>
<td>$\chi_5(g)$</td>
<td>1</td>
<td>$e^{j \frac{2\pi}{6}}$</td>
<td>$e^{j \frac{4\pi}{6}}$</td>
<td>$e^{j \frac{6\pi}{6}}$</td>
<td>$e^{j \frac{8\pi}{6}}$</td>
<td>$e^{j \frac{10\pi}{6}}$</td>
</tr>
</tbody>
</table>

$$F = \begin{pmatrix} \psi_0 \\ \vdots \\ \psi_5 \end{pmatrix}$$
DFT using representations as Fourier basis

- The representations $\chi_k$ for $k = 0, \ldots, N - 1$ are all inequivalent.
- Some are one-to-one and some are many-to-one and the images can be associated with subgroups of $G$
- We can formally rewrite the DFT as

$$X[k] = \langle x, \psi_k \rangle = \sum_{g \in G} x[g] \chi_k(g) \quad k = 0, \ldots, N - 1$$

- The complex vectors $\psi_k = [\chi_k(g)]_{g \in G}$ form the discrete Fourier basis vectors
- Each representation provides a “lens” through which we observe the time-domain signal $x[n]$. 

Emanuele Viterbo
The two-modular Fourier transform
Given a normal subgroup $H \leq G$ we define the quotient group $G/H$ consisting of the coset leaders $u$ of the cosets $u + H$.

The direct product of $H$ and $G/H$ is isomorphic to $G$ i.e.,

$$G = \{ u + v | u \in H, v \in G/H \} \approx H \times G/H$$

All $u \in H = \text{Ker}(\chi_k)$ are mapped to the same value $\chi_k(u) = \chi_k(0) = 1 \in S_k$.

Then we can compute the DFT more efficiently as

$$X[k] = \sum_{g \in G} x[g] \chi_k(g) = \sum_{v \in G/H} \sum_{u \in H} x[u + v] \chi_k(u + v)$$

$$= \sum_{v \in G/H} \left( \sum_{u \in H} x[u + v] \right) \chi_k(v) \quad k = 0, \ldots, N - 1$$
Known generalizations of the DFT concept

- \( f : G \rightarrow \mathbb{C} \), where \( G \) can be an arbitrary group (not only Abelian): Fourier coefficients are complex matrices.
- These generalizations make use of multi-dimensional representations of the group \( G \) with matrices over \( \mathbb{C} \).
- The inverse Fourier transform uses \( \frac{1}{|G|} \text{Tr}(\cdot) \) the Trace operator of a matrix to get back to time domain scalar values of \( f \).
- \( f : G \rightarrow K \), where \( K \) is a field of characteristic \( p \) and \( p \) does not divide \( |G| \): Fourier coefficients are scalars in \( K \) since an “exponential” function can be defined using a primitive element \( \alpha \in K \).
The missing Fourier Transform for binary functions

- We consider a finite commutative ring $\mathcal{R}$ of characteristic $p = 2$, e.g., $\mathbb{F}_2[X]/\phi(X)$, where $\phi(X)$ is a binary-coefficient polynomial of degree $m$.
- Elements of $\mathcal{R}$ are represented by $m$-bit vectors (or polynomials of degree at most $m - 1$) and multiplications are computed by polynomial multiplication mod $\phi(X)$.
- Let $G = C_2^n$ be the additive group of $\mathbb{F}_2^n$ ($n$ bit vectors).
- We study binary functions $f : G \rightarrow \mathcal{R}$ ($n$ bit to $m$ bit) and their convolutions (group ring $\mathcal{R}[G]$).

What does not work? If $p = 2$ divides $|G| = 2^n = N$, the inverse DFT term $1/N$ is not defined in $\mathcal{R}$ and the Trace fails to work in the generalized inverse DFT.
The two-modular representations of $G$

- Let $G = C_2 = \{0, 1\}$ then a two-modular representation as $2 \times 2$ binary matrices over $\mathbb{R}$, is given by the two matrices

\[ E_0 = \pi_1(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad E_1 = \pi_1(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \]

The matrix entries are the ‘zero’ and ‘one’ element in $\mathbb{R}$.

- The $n$-fold direct product of $C_2$, $G = C_2^n = C_2 \times \cdots \times C_2$ can be represented as the Kroneker product of the representations of $C_2$, i.e.,

\[ \pi_n(G') \triangleq \pi_1(C_2) \otimes \cdots \otimes \pi_1(C_2) \]
The two-modular representations of $G = C_2 \times \cdots \times C_2$

Let the binary vectors $\mathbf{b} = (b_1, \ldots, b_n)$ represent the elements of $G$ with bitwise addition mod 2 (XOR). Then

$$\pi_n(\mathbf{b}) = E_{\mathbf{b}} = \pi_1(b_1) \otimes \cdots \otimes \pi_1(b_n)$$

Example $G = C_2 \times C_2$

$$E_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad E_{01} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad E_{10} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad E_{11} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
The two-modular Fourier basis for $G = C_2 \times \cdots \times C_2$

- Consider the two-modular representations ($2^k \times 2^k$ matrices) of the nested subgroups of $G = C_2^m$,

$$H_0 = \{0_n\} \triangleleft H_1 \triangleleft \cdots \triangleleft H_k \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = G$$

where $H_1 \cong C_2$, $H_2 \cong C_2 \times C_2$, $H_3 \cong C_2 \times C_2 \times C_2$, etc.

- The Fourier basis ‘vectors’ are made up of all the inequivalent two-modular representations $\pi_k$

$$H_0 \cong \text{Im}(\pi_0) = \{1\}$$
$$H_1 \cong \text{Im}(\pi_1) = \{E_0, E_1\}$$
$$H_2 \cong \text{Im}(\pi_2) = \{E_{00}, E_{01}, E_{10}, E_{11}\}$$
$$H_3 \equiv \text{Im}(\pi_3) = \{E_{000}, E_{001}, E_{010}, E_{011}, E_{100}, E_{101}, E_{110}, E_{111}\}$$
$$\vdots$$
Example $G = C_2^3$

The Fourier basis ‘vectors’ $\psi_k = [E_{\tau_k}(g) : g \in G]$ are the $2^n$-component vectors (indexed by $g$) of $2^k \times 2^k$ matrices from the set $\text{Im}(\pi_k)$

<table>
<thead>
<tr>
<th>$g \in G$</th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pi_0(g)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\pi_1(g)$</td>
<td>$E_0$</td>
<td>$E_1$</td>
<td>$E_0$</td>
<td>$E_1$</td>
<td>$E_0$</td>
<td>$E_1$</td>
<td>$E_0$</td>
<td>$E_1$</td>
</tr>
<tr>
<td>$\pi_2(g)$</td>
<td>$E_{00}$</td>
<td>$E_{01}$</td>
<td>$E_{11}$</td>
<td>$E_{10}$</td>
<td>$E_{00}$</td>
<td>$E_{01}$</td>
<td>$E_{11}$</td>
<td>$E_{10}$</td>
</tr>
<tr>
<td>$\pi_3(g)$</td>
<td>$E_{000}$</td>
<td>$E_{010}$</td>
<td>$E_{001}$</td>
<td>$E_{011}$</td>
<td>$E_{111}$</td>
<td>$E_{101}$</td>
<td>$E_{110}$</td>
<td>$E_{100}$</td>
</tr>
</tbody>
</table>
We abstractly define the $k$-th Fourier coefficients as the $2^k \times 2^k$ matrix with elements in $\mathcal{R}$

$$\hat{f}_k = \langle f, \psi_k \rangle \triangleq \sum_{g \in G} f(g)E_{\tau_k}(g) \quad \text{for} \quad k = 0, \ldots, n \quad (1)$$

where $E_{\tau_k}(g) \in \psi_k$ selected by $g$ according to a (surjective) group homomorphism $\tau_k : G \mapsto C_2^k$ ($n$-bit to $k$-bits).
We can represent the elements of $H_k \cong C_2^k$ as $n$-bit vectors with the first $n - k$ bits set to zero i.e.,

$H_k = \{(0, \ldots, 0, b_{n-k+1}, \ldots, b_n) | b_i \in \{0, 1\}\} \cong C_2^k$  \quad k = 1, \ldots, n

The quotient groups $G/H_k$ are represented as $n$-bit vectors with the last $k$ bits set to zero i.e.,

$G/H_k = \begin{cases} 
\{(b_1, \ldots, b_{n-k}, 0, \ldots, 0) | b_i \in \{0, 1\}\} & k = 1, \ldots, n - 1 \\
\{0_n\} & k = n .
\end{cases}$

Consider the binary subgroup $\langle d_k \rangle = \{0, d_k\}$ of $H_k$ where

$d_k = (0, \ldots, 0, b_{n-k+1} = 1, 0 \ldots, 0)$

Then

$$\underbrace{G}_{2^n} \cong \underbrace{H_k/\langle d_k \rangle \times \langle d_k \rangle \times G/H_k}_{2^{2k-1} \times 2 \times 2^{2n-k}}$$
The $k$-th Fourier coefficients $\hat{f}_k$ can be explicitly computed by collecting the terms with the same $E_{\tau_k}(g)$, i.e.,

$$\hat{f}_k = \sum_{u \in H_k/d_k} \left\{ \left[ \sum_{v \in G_n/H_k} f(u + v) \right] E_{\sigma_k}(u) \right. + \left. \left[ \sum_{v \in G_n/H_k} f(u + d_k + v) \right] E_{\sigma_k}(u) \right\} \quad k = 0, \ldots, n$$

where $\sigma_k(u)$ is a map converting the $n$ bit vector $u \in H_k/d_k$ to a $k$ bit vector in $G_2^k$, i.e., it removes the first $n - k$ zero bits of the $n$ bit vector $u$. The corresponding $\overline{\sigma_k(u)}$ is the binary complement of the bits of $\sigma_k(u)$. 
Let $\pi_k(g) = E_{\tau_k}(g)$ be the $2^k \times 2^k$ representation of an element $g \in C_2^k$ then we define the character of $g$ as

$$\Phi_k(E_{\tau_k}(g)) \triangleq (E_{\tau_k}(g))_{(1,2^k)} \in \{0, 1\}$$

i.e., $\Phi$ extracts the top-right corner element of the matrix $E_g$. The representation of the all ones vector $1 = (1, 1, \ldots, 1)$ yields $\Phi(E_1) = 1$, while any other binary vector representation is mapped to zero.

Since $\Phi_k$ is an homomorphism, we have

$$\Phi_k(E_a E_b) = \Phi_k(E_{a \oplus b}) = \begin{cases} 1 & \text{iff } a \oplus b = 1 \text{ (or } a = \overline{b}) \\ 0 & \text{otherwise} \end{cases}$$
The inverse Fourier transform is given by

\[ f_j = f_c = \hat{f}_0 + \sum_{k=1}^{n} \Phi_k \left( \hat{f}_k E_{\tau_k(c)} \right) \quad j = 0, \ldots, 2^n - 1 \quad (2) \]

where \( c = (c_n, \ldots, c_k, \ldots, c_1) \) and \( j = D(c) \) is the decimal representation of \( c \).
The two-modular Fourier transform can be used to transform convolution in the ‘time-domain’ defined as

\[(f_1 \ast f_2)(a) \triangleq \sum_{b \in G} f_1(ab^{-1})f_2(b) = \sum_{b \in G} f_1(a \oplus b)f_2(b)\]

into the product in the ‘frequency domain’ i.e.,

\[\hat{(f_1 \ast f_2)}(\rho) = \hat{f}_1(\rho)\hat{f}_2(\rho)\]

This is where the multiplicative structure of \(R\) plays a role.
Potential applications of the two-modular Fourier transform

- reliable computation of binary functions
- classification of binary functions (polynomial vs. transcendental over \( \mathbb{R} \))
- cryptography
- complexity of binary functions
Thank you!