Lecture 32: Convolution
In today’s lecture we shall study about an important property of the Fourier basis functions that makes them special, namely, additive homomorphism.

This additive homomorphism property shall help us prove interesting properties of an important technical tools in Fourier analysis called Convolution.
Let $f : \{0, 1\}^n \rightarrow \mathbb{R}$ be an arbitrary function.

We say that $f$ exhibits “additive homomorphism” if, for all $x, y \in \{0, 1\}^n$, we have

$$f(x + y) = f(x) \cdot f(y)$$

Observe that all the Fourier basis functions $\chi_S$ satisfy this additive homomorphism property.
Let $F = \{f_0, f_1, \ldots, f_{N-1}\}$ be a set of functions $\{0, 1\}^n \to \mathbb{R}$ such that

1. **Orthonormality.** The functions in $F$ are orthonormal with respect to an “inner-product”

2. **Symmetry.** For all $i \in \{0, \ldots, N\}$ and $x \in \{0, 1\}^n$, we have $f_i(x) = f_x(i)$

3. **Additive Homomorphism.** For all $x, y \in \{0, 1\}^n$, and $i \in \{0, \ldots, N - 1\}$, we have $f_i(x + y) = f_i(x) \cdot f_i(y)$

Any analysis that we perform in this course extends to any basis $F$ with the properties mentioned above

Think: These properties imply that $f_0(x) = 1$, for all $x \in \{0, 1\}^n$!
Intuition of the Convolution Operator

- Let $X, Y$ be probability distributions over $\{0, 1\}^n$
- Consider the following algorithm
  
  1. Sample $x \sim X$ and sample $y \sim Y$
  2. Output $z = x \oplus y$

- Note that the output of this algorithm is a distribution over the sample space $\{0, 1\}^n$. Let us represent the output distribution of this algorithm by $Z$ (also referred to as the distribution $X \oplus Y$)
- **Question:** What is the $P[Z = z]$?
  
  - Note that $x$ can be anything in $\{0, 1\}^n$. However, given $x$ and $z$, there is a unique $y = x \oplus z$ such that $x \oplus y = z$
  - So, we have
    
    $$P[Z = z] = \sum_{x \in \{0, 1\}^n} P[X = x] P[Y = x \oplus z]$$

- The distribution $Z$ is (a scaling) of the convolution of the distributions $X$ and $Y$. 
Let $f, g: \{0, 1\}^n \rightarrow \mathbb{R}$ be two functions.

The convolution of $f$ and $g$ is the function $(f \ast g): \{0, 1\}^n \rightarrow \mathbb{R}$ defined as follows:

$$(f \ast g)(x) = \frac{1}{N} \sum_{y \in \{0, 1\}^n} f(y) \cdot g(x - y)$$

Note that if $X$ and $Y$ are two function representing probability distributions over $\{0, 1\}^n$, then $N(X \ast Y)$ is the function corresponding to the probability distribution $X \oplus Y$.

Note that the Convolution is a bilinear operator!
Given two functions $f$ and $g$, we are interested in expressing the function $(f * g)$ using the functions $\hat{f}$ and $\hat{g}$.

We shall prove the following result.

**Lemma**

For all functions $f, g : \{0, 1\}^n \to \mathbb{R}$ and $S \in \{0, 1\}^n$, we have

$$(f * g)(S) = \hat{f}(S) \cdot \hat{g}(S)$$

We shall provide a direct proof for this result:

$$(f * g)(S) = \frac{1}{N} \sum_{x \in \{0, 1\}^n} (f * g)(x) \chi_S(x)$$

$$= \frac{1}{N} \sum_{x \in \{0, 1\}^n} \frac{1}{N} \sum_{y \in \{0, 1\}^n} f(y)g(x - y)\chi_S(x)$$
Fourier Transform of Convolution II

\[
\hat{f}(S) = \frac{1}{N^2} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} f(y)g(x - y)\chi_S(y)\chi_S(x - y)
\]

The final step above is a consequence of the additive homomorphism of the function \(\chi_S\). Let us continue with the simplification.

\[
(f \ast g)(S) = \frac{1}{N^2} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} f(y)g(x - y)\chi_S(y)\chi_S(x - y)
\]

\[
= \frac{1}{N^2} \sum_{y \in \{0,1\}^n} f(y)\chi_S(y) \sum_{r \in \{0,1\}^n} g(r)\chi_S(r)
\]

\[
= \left(\frac{1}{N} \sum_{y \in \{0,1\}^n} f(y)\chi_S(y)\right) \left(\frac{1}{N} \sum_{r \in \{0,1\}^n} g(r)\chi_S(r)\right)
\]

\[
= \hat{f}(S) \cdot \hat{g}(S)
\]
We can succinctly summarize this result as follows:
\[
(\hat{f} \ast \hat{g}) = \hat{f} \cdot \hat{g}
\]

Exercise: Express \( \hat{f} \cdot \hat{g} \) using \( \hat{f} \) and \( \hat{g} \)
Offset of a Function

- Let \( f : \{0, 1\}^n \rightarrow \mathbb{R} \)
- Define \( g : \{0, 1\}^n \rightarrow \mathbb{R} \) as \( g(x) = f(x - c) \), for some \( c \in \{0, 1\}^n \)
- We are interested in expressing \( \hat{g}(S) \) using \( \hat{f}(S) \) and \( c \)

\[
\hat{g}(S) = \frac{1}{N} \sum_{x \in \{0,1\}^n} g(x) \chi_S(x)
\]

\[
= \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x - c) \chi_S(x - c) \chi_S(c)
\]

\[
= \chi_S(c) \frac{1}{N} \sum_{x \in \{0,1\}^n} f(x - c) \chi_S(x - c)
\]

\[
= \chi_c(S) \cdot \hat{f}(S)
\]
That is, we conclude that $\hat{g} = \chi_c \cdot \hat{f}$. Recall that $\chi_c(S) \in \{+1, -1\}$. So, $\chi_c(S) \cdot \hat{f}(S)$ is either $\hat{f}(S)$ or $-\hat{f}(S)$.

Intuition: If $g$ is an offset of the function $f$, then $\hat{g}$ is a “twisting/rotation” of the function $\hat{f}$. So, by studying the magnitudes of the Fourier transform, we can study the function “independent of their offsets”.

Additional Perspective: In fact, this result also implies that $g$ can be rewritten as $N(\chi_c \ast f)$.