FFTs in Graphics and Vision

Groups and Representations

Outline

Groups

Representations

Schur's Lemma

Correlation

Groups

A group is a set of elements G with a binary operation (often denoted "·") such that for all $f, g, h \in G$, the following properties are satisfied:

- Closure:
$$g \cdot h \in G$$
- Associativity:
$$f \cdot (g \cdot h) = (f \cdot g) \cdot h$$
- Identity: $\exists 1 \in G$ s.t.:
$$1 \cdot g = g \cdot 1 = g$$
- Inverse: $\forall g \in G \; \exists g^{-1} \in G$ s.t.:
$$g \cdot g^{-1} = g^{-1} \cdot g = 1$$

If it is also true that $f \cdot g = g \cdot f$ for all $f, g \in G$, the group is called commutative, or abelian.

Groups

Examples

Under what binary operations are the following groups, what is the identity element, and what is the inverse:

- $\mathbb{Z}$: integers?
- $\mathbb{R}^{>0}$: positive real-numbers?
- $\mathbb{R}^2/(2\pi\mathbb{Z}^2)$: points in $\mathbb{R}^2$ modulo addition by integer multiples of 2π in either coordinate?
- V: vectors in a fixed vector space?
- $GL(V)$: invertible linear transformations of a vector space?

Groups

Examples

Are these groups commutative:

- $\mathbb{Z}$ under addition?
- $\mathbb{R}^{>0}$ under multiplication?
- $\mathbb{R}^2/(2\pi\mathbb{Z}^2)$ under addition?
- V under addition?
- $GL(V)$ under composition?

Representations

Often, we think of a group as a set of elements that act on some space:

E.g.:

- Invertible linear transformations act on vector spaces
- 2D rotations act on 2D arrays
- 3D rotations act on 3D arrays

A representation is a way of formalizing this…

Representations

A <u>representation</u> of a group G <u>on a vector space</u> V, denoted (ρ, V), is a map ρ that sends every element in G to an invertible linear transformation on V, preserving the group structure:

$$\rho(g \cdot h) = \rho(g) \cdot \rho(h) \quad \forall g, h \in G.$$

For simplicity, we will write:

$$\rho(g) = \rho_g$$

<u>Note</u>:

- $\rho(1) = 1$ since:

$$\rho(g) = \rho(g \cdot 1) = \rho(g) \cdot \rho(1)$$

- $\left(\rho(g)\right)^{-1} = \rho(g^{-1})$ since:

$$\rho(1) = \rho(g \cdot g^{-1}) = \rho(g) \cdot \rho(g^{-1})$$

Unitary Representations

If the vector space V has a Hermitian inner product, and the representation preserves the inner product:

$$\langle v, w \rangle = \langle \rho_g(v), \rho_g(w) \rangle \qquad \forall g \in G; v, w \in V$$

the representation is called unitary.

Note:

For nice (e.g. finite, compact) groups we can always massage the Hermitian inner product so that the representation becomes unitary.

Unitary Representations

Examples

- $V = \mathbb{R}^n$ is the space of n-dimensional arrays with the standard inner-product
- $G = GL_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices
- ρ is the map:

$$\rho_{\mathbf{M}}(\mathbf{v}) = \mathbf{M}\mathbf{v}$$

Representation?

Unitary?

Unitary Representations

Examples

- $V = \mathbb{R}^n$ is the space of n-dimensional arrays with the standard inner-product
- $G = GL_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices
- ρ is the map:

$$\rho_{\mathbf{M}}(\mathbf{v}) = \mathbf{M}\mathbf{v}$$

Representation? **Yes**

Unitary? **No**

Unitary Representations

Examples

- $V = \mathbb{R}^n$ is the space of n-dimensional arrays with the standard inner-product
- $G = GL_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices
- ρ is the map:

$$\rho_{\mathbf{M}}(\mathbf{v}) = \mathbf{v}$$

Representation?

Unitary?

Unitary Representations

Examples

- $V = \mathbb{R}^n$ is the space of n-dimensional arrays with the standard inner-product
- $G = GL_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices
- ρ is the map:

$$\rho_{\mathbf{M}}(\mathbf{v}) = \mathbf{v}$$

Representation? **Yes**

Unitary? **Yes**

This is called the *trivial representation*.

Unitary Representations

Examples

- V is a complex Hermitian inner product space
- $G = SU(V)$ is the group of (special) unitary transformations on V
- ρ is the map:

$$\rho_U(v) = Uv$$

Representation?

Unitary?

Unitary Representations

<u>Examples</u>

- V is a complex Hermitian inner product space
- $G = SU(V)$ is the group of (special) unitary transformations on V
- ρ is the map:

$$\rho_U(v) = Uv$$

Representation? **Yes**

Unitary? **Yes**

Unitary Representations

<u>Examples</u>

- $V = L^2(S^2)$ is the space of functions on a sphere with the standard inner-product
- $G = SO(3)$ is the group of 3D rotations
- ρ is the map:

$$[\rho_R(f)](p) = f(Rp) \;\; \forall R \in G$$

Representation?

Unitary?

Unitary Representations

<u>Examples</u>

- $V = L^2(S^2)$ is the space of functions on a sphere with the standard inner-product
- $G = SO(3)$ is the group of 3D rotations
- ρ is the map:

$$[\rho_R(f)](p) = f(Rp) \ \ \forall R \in G$$

Representation? **No**

$$\begin{aligned}\left[\rho_R\left(\rho_S(f)\right)\right](p) &= [\rho_S(f)](Rp)\\ &= f(SRp)\\ &= [\rho_{SR}(f)](p)\\ &\neq [\rho_{RS}(f)](p)\end{aligned}$$

Unitary Representations

<u>Examples</u>

- $V = L^2(S^2)$ is the space of functions on a sphere with the standard inner-product
- $G = SO(3)$ is the group of 3D rotations
- ρ is the map:

$$[\rho_R(f)](p) = f(R^{-1}p) \quad \forall R \in G$$

Representation?

Unitary?

Unitary Representations

<u>Examples</u>

- $V = L^2(S^2)$ is the space of functions on a sphere with the standard inner-product
- $G = SO(3)$ is the group of 3D rotations
- ρ is the map:

$$[\rho_R(f)](p) = f(R^{-1}p) \quad \forall R \in G$$

Representation? **Yes**

$$\begin{aligned}\left[\rho_R\left(\rho_S(f)\right)\right](p) &= [\rho_s(f)](R^{-1}p)\\ &= f(S^{-1}R^{-1}p)\\ &= f\left((RS)^{-1}p\right)\\ &= [\rho_{RS}(f)](p)\end{aligned}$$

Unitary? **Yes**

Unitary Representations

<u>Examples</u>

- $V = L^2\left(\mathbb{R}^2/(2\pi\mathbb{Z}^2)\right)$ is the space of periodic functions in the plane
- $G = \mathbb{R}^2/(2\pi\mathbb{Z}^2)$ is the group $\mathbb{R}^2$ modulo addition by integer multiples of 2π in either coordinate
- ρ is the map:

$$\left[\rho_{a,b}(f)\right](x,y) = f(x-a, y-b)$$

Representation?

Unitary?

Unitary Representations

<u>Examples</u>

- $V = L^2\left(\mathbb{R}^2/(2\pi\mathbb{Z}^2)\right)$ is the space of periodic functions in the plane
- $G = \mathbb{R}^2/(2\pi\mathbb{Z}^2)$ is the group $\mathbb{R}^2$ modulo addition by integer multiples of 2π in either coordinate
- ρ is the map:
$$\left[\rho_{a,b}(f)\right](x,y) = f(x-a, y-b)$$

Representation? **Yes**

Unitary? **Yes**

Big Picture

Our goal is to try to better understand how a group acts on a vector space:

- How translational shifts act on periodic functions,
- How rotations act on functions on a sphere/circle
- Etc.

To do this we would like to simplify the “action” of the group into bite-size chunks.

We will always be assuming that our representations are unitary

Sub-Representation

Given a representation (ρ, V) of a group G, if there exists a subspace $W \subset V$ such that the representation fixes W:

$$\rho_g(w) \in W \qquad \forall g \in G \text{ and } w \in W$$

then we say that W is a <u>sub-representation</u> of V.

Sub-Representation

Maschke's Theorem:

If W is a sub-representation of V, then the perpendicular space $W^\perp$ will also be a sub-representation of V.

Formally:

$W^\perp$ is defined by the property that every vector in $W^\perp$ is perpendicular to every vector in W:

$$\langle w, w' \rangle = 0 \quad \forall w \in W \text{ and } w' \in W^\perp$$

Sub-Representation

Claim: $W^{\perp}$ will also be a sub-representation of V.

Proof: (By contradiction)

We would like to show that the representation ρ sends $W^{\perp}$ back into itself…

Sub-Representation

Claim: $W^\perp$ will also be a sub-representation of V.

Proof: (By contradiction)

We would like to show that the representation ρ sends $W^\perp$ back into itself… Assume not.

There exist $w' \in W^\perp$, $w \in W$, and $g \in G$ s.t.:

$$\langle w, \rho_g(w') \rangle \neq 0$$

Since ρ is unitary, this implies that:

$$\langle \rho_{g^{-1}}(w), \rho_{g^{-1}}\left(\rho_g(w')\right) \rangle \neq 0$$

$$\Updownarrow$$

$$\langle \rho_{g^{-1}}(w), w' \rangle \neq 0$$

Sub-Representation

Claim: $W^{\perp}$ will also be a sub-representation of V.

Proof: (By contradiction)

We would like to show that the representation ρ sends $W^{\perp}$ back into itself… Assume not.

There exist $w' \in W^{\perp}$, $w \in W$, and $g \in G$ s.t.:

Since ρ

But this would contradict the assumption that the representation ρ maps W back into itself!

$$\Updownarrow$$

$$\langle \rho_{g^{-1}}(w), w' \rangle \neq 0$$

Sub-Representation

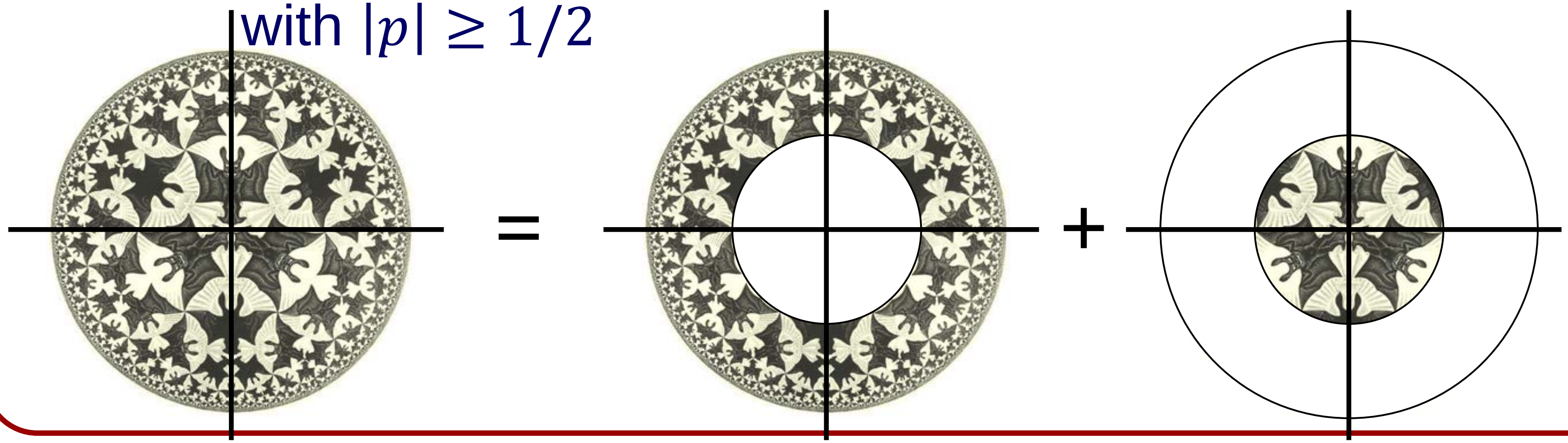
Example:

1. Consider the group $G = SO(2)$ of 2D rotations, acting on vectors in $\mathbb{R}^3$ by rotating around the y-axis.
   What are the two sub-representations?
   a) The y-axis: The group acts on this sub-space trivially, mapping every vector to itself
   b) The xz-plane: The group acts as a 2D rotation on this 2D space.

Sub-Representation

<u>Example</u>:

2. Consider the group $G = SO(2)$ of 2D rotations, acting on functions on the unit disk $L^2(D^2)$. What are two sub-representations?
   a) The space of functions that are zero for all points p with $|p| < 1/2$
   b) The space of functions that are zero for all points p with $|p| \geq 1/2$



Irreducible Representations

Given a representation (ρ, V) of a group G, the representation is said to be irreducible if the only subspaces of V that are sub-representations are:

$$W = V \quad \text{and} \quad W = \{0\}$$

Structure Preservation

We had talked about linear transformations as maps between vector spaces, that preserve the underlying vector space structure:

$$L(\alpha v + \beta w) = \alpha L(v) + \beta L(w)$$

We had talked about a representation as a map from a group into the group of invertible linear transforms that preserves the group structure:

$$\rho(g \cdot h) = \rho(g) \cdot \rho(h)$$

Structure Preservation

Given a representation (ρ, V) a group G, what does it mean for a map $\Phi: V \to V$ to preserve the representation structure?

- Since Φ is a map between vector spaces, it should preserve the vector space structure:
  $\Rightarrow$ Φ is a linear transformation.
- Φ should also preserve the group action structure:

$$\Phi\left(\rho_g(v)\right) = \rho_g\left(\Phi(v)\right)$$

Such a map is called G-linear.

Structure Preservation

Note:

If $\Phi, \Psi: V \to V$ are G-linear, then so is their linear combination:

$$\begin{aligned}(\alpha\cdot\Phi+\beta\cdot\Psi)\left(\rho_g(v)\right) &= \alpha\cdot\Phi\left(\rho_g(v)\right)+\beta\cdot\Psi\left(\rho_g(v)\right)\\ &= \alpha\cdot\rho_g\left(\Phi(v)\right)+\beta\cdot\rho_g\left(\Psi(v)\right)\\ &= \rho_g\left(\alpha\cdot\Phi(v)\right)+\rho_g\left(\beta\cdot\Psi(v)\right)\\ &= \rho_g\left(\alpha\cdot\Phi(v)+\beta\cdot\Psi(v)\right)\\ &= \rho_g\left((\alpha\cdot\Phi+\beta\cdot\Psi)(v)\right)\end{aligned}$$

Structure Preservation

Claim:

If $\Phi: V \to V$ is G-linear, then both the kernel and the image of Φ are sub-representations.

Structure Preservation

Claim:
If $\Phi: V \to V$ is G-linear, then both the kernel and the image of Φ are sub-representations.

Proof:

If $v \in \text{Kernel}(\Phi)$ then, for $g \in G$ we have:

$$0 = \Phi(v) = \rho_g\big(\Phi(v)\big)$$
$$= \Phi\left(\rho_g(v)\right)$$
$$\Updownarrow$$
$$\rho_g(v) \in \text{Kernel}(\Phi)$$

Structure Preservation

Claim:

If $\Phi: V \to V$ is G-linear, then both the kernel and the image of Φ are sub-representations.

Proof:

If $w = \Phi(v) \in \mathrm{Image}(\Phi)$ then, for $g \in G$ we have:

$$\begin{aligned}\rho_g(w) &= \rho_g\big(\Phi(v)\big)\\ &= \Phi\left(\rho_g(v)\right)\\ &\in \mathrm{Image}(\Phi)\end{aligned}$$

Schur's Lemma

Given an irreducible representation (ρ, V) of a group G, if Φ is G-linear then Φ is scalar multiplication:

$$\Phi = \lambda \cdot \mathrm{Id}.$$

Schur's Lemma

Proof:

1. Since Φ is a linear transformation, it has a (complex) eigenvalue λ.
2. Since Φ and $\mathrm{Id.}$ are G-linear, so is $(\Phi - \lambda \cdot \mathrm{Id.})$.

Schur's Lemma

Proof:

3. Since λ is an eigenvalue of Φ, $(\Phi - \lambda \cdot \mathrm{Id.})$ must have a non-trivial kernel $W \subset V$.

4. This implies that the kernel of $(\Phi - \lambda \cdot \mathrm{Id.})$ must be a sub-representation of V.

5. Since (ρ, V) is irreducible and the kernel of $(\Phi - \lambda \cdot \mathrm{Id.})$ is not empty, $W = V$.

6. Since the kernel is the entire vector space:
$$(\Phi - \lambda \cdot \mathrm{Id.}) = 0 \quad \Leftrightarrow \quad \Phi = \lambda \cdot \mathrm{Id.}$$

Schur's Lemma (Corollary)

Corollary:

All irreducible representations of commutative groups must be one-dimensional.

Schur's Lemma (Corollary)

Proof:

1. Fix some element $h \in G$.

Schur's Lemma (Corollary)

Proof:

1. Fix some element $h \in G$.
2. Since G is commutative, ρ_h must be G-linear:

$$\begin{aligned}\rho_g\left(\rho_h(v)\right) &= \rho_{g\cdot h}(v)\\ &= \rho_{h\cdot g}(v)\\ &= \rho_h\left(\rho_g(v)\right)\end{aligned}$$

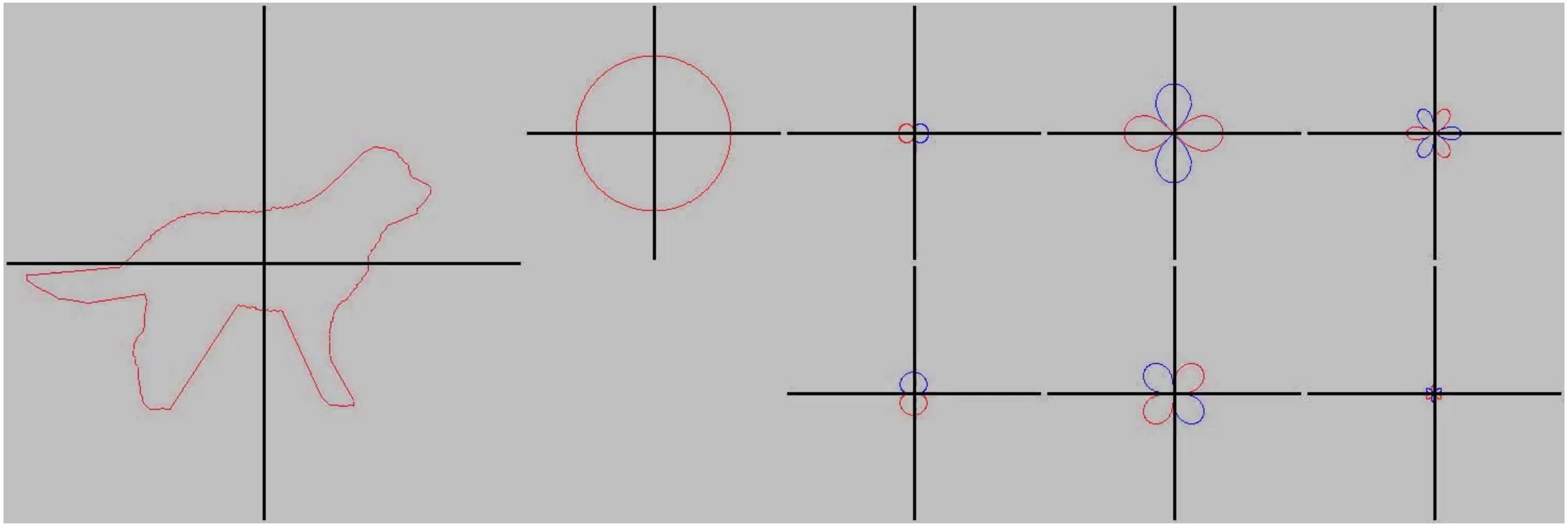
Schur's Lemma (Corollary)

Proof:

1. Fix some element $h \in G$.
2. Since G is commutative, ρ_h must be G-linear.
3. Since (ρ, V) is irreducible, $\rho_h = \lambda \cdot \mathrm{Id}$.
4. Since this is true for any $h \in G$, any subspace $W \subset V$ is a sub-representation.
5. Since V is irreducible, V is one-dimensional.

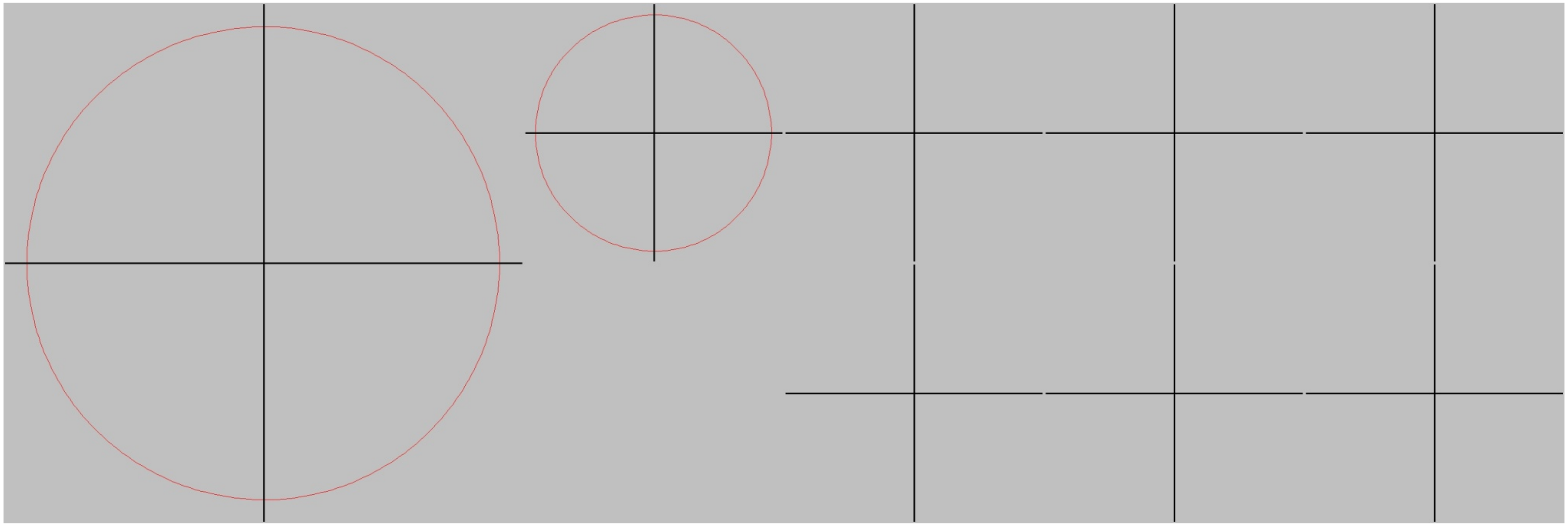
Example:

Since 2D rotations commute, we can decompose the space of functions on a circle into one (complex) dimensional subspaces that rotate into themselves.



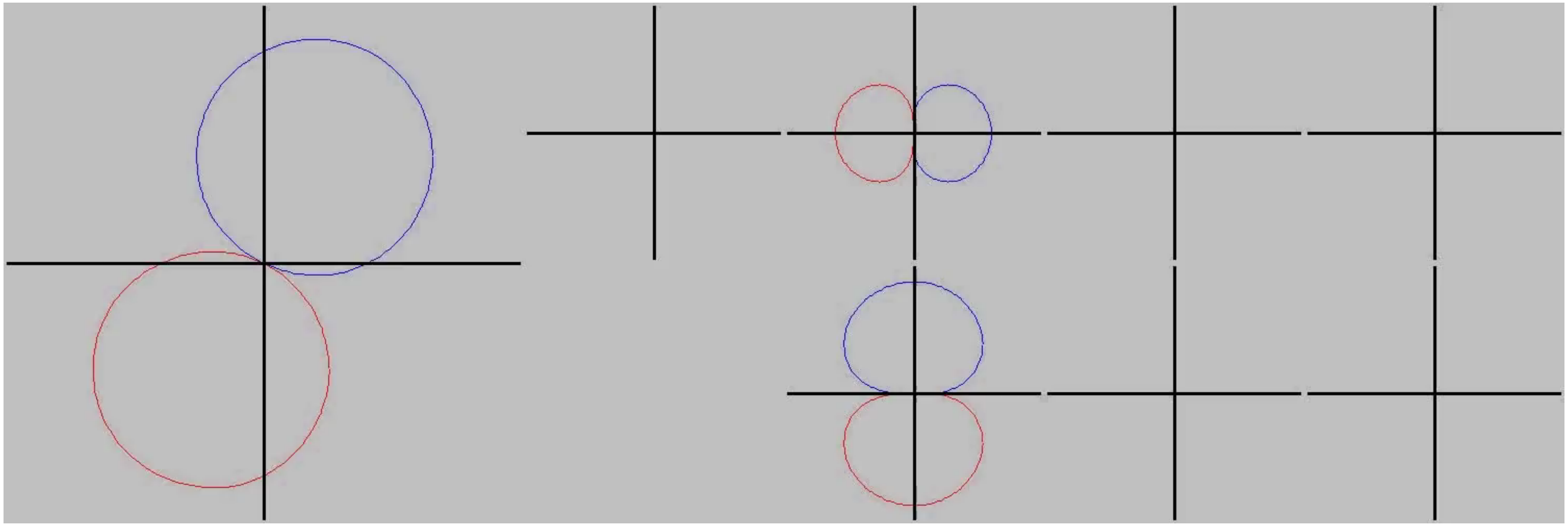
Example:

Since 2D rotations commute, we can decompose the space of functions on a circle into one (complex) dimensional subspaces that rotate into themselves.



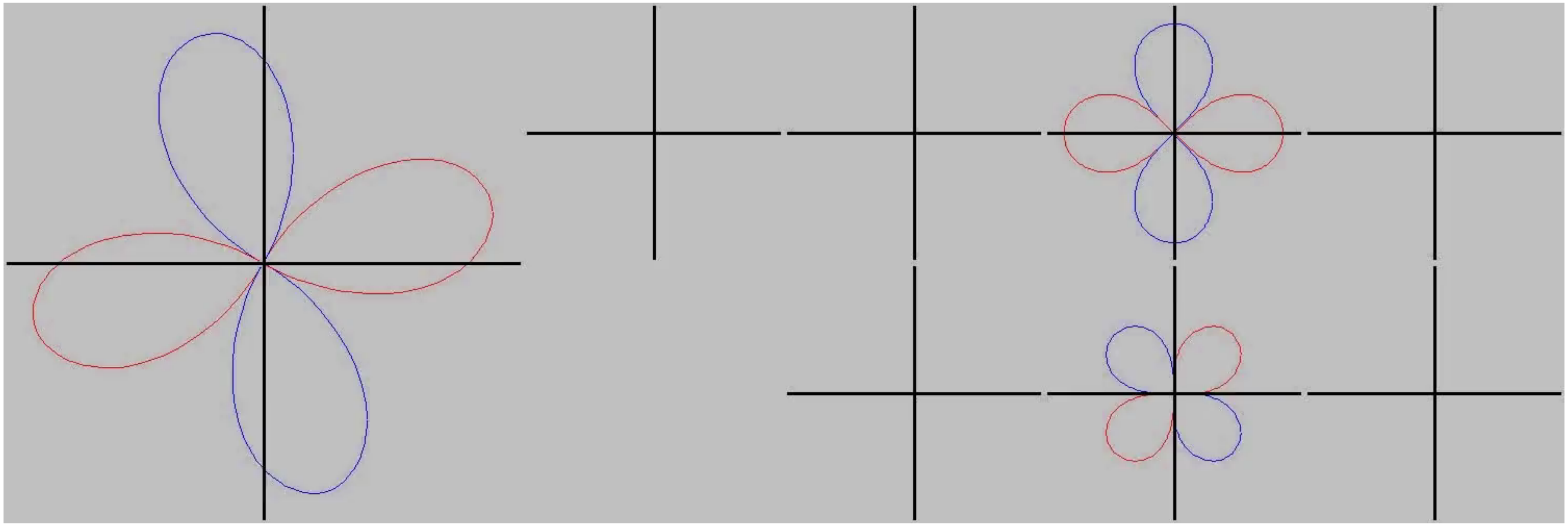
Example:

Since 2D rotations commute, we can decompose the space of functions on a circle into one (complex) dimensional subspaces that rotate into themselves.



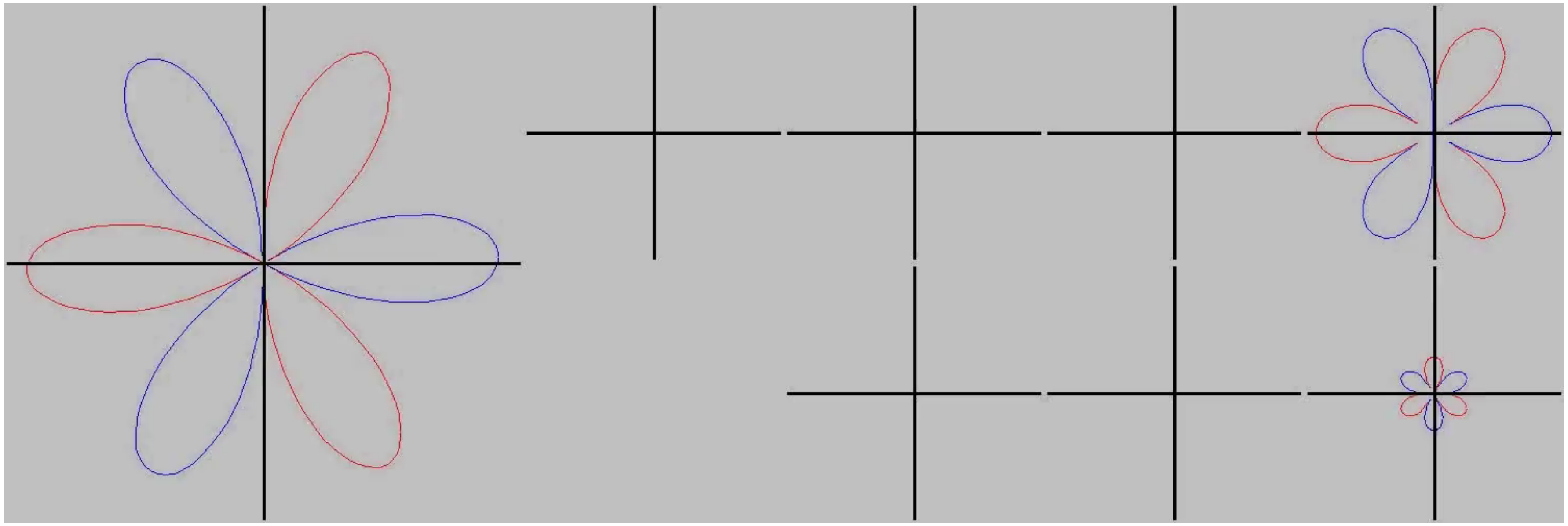
Example:

Since 2D rotations commute, we can decompose the space of functions on a circle into one (complex) dimensional subspaces that rotate into themselves.



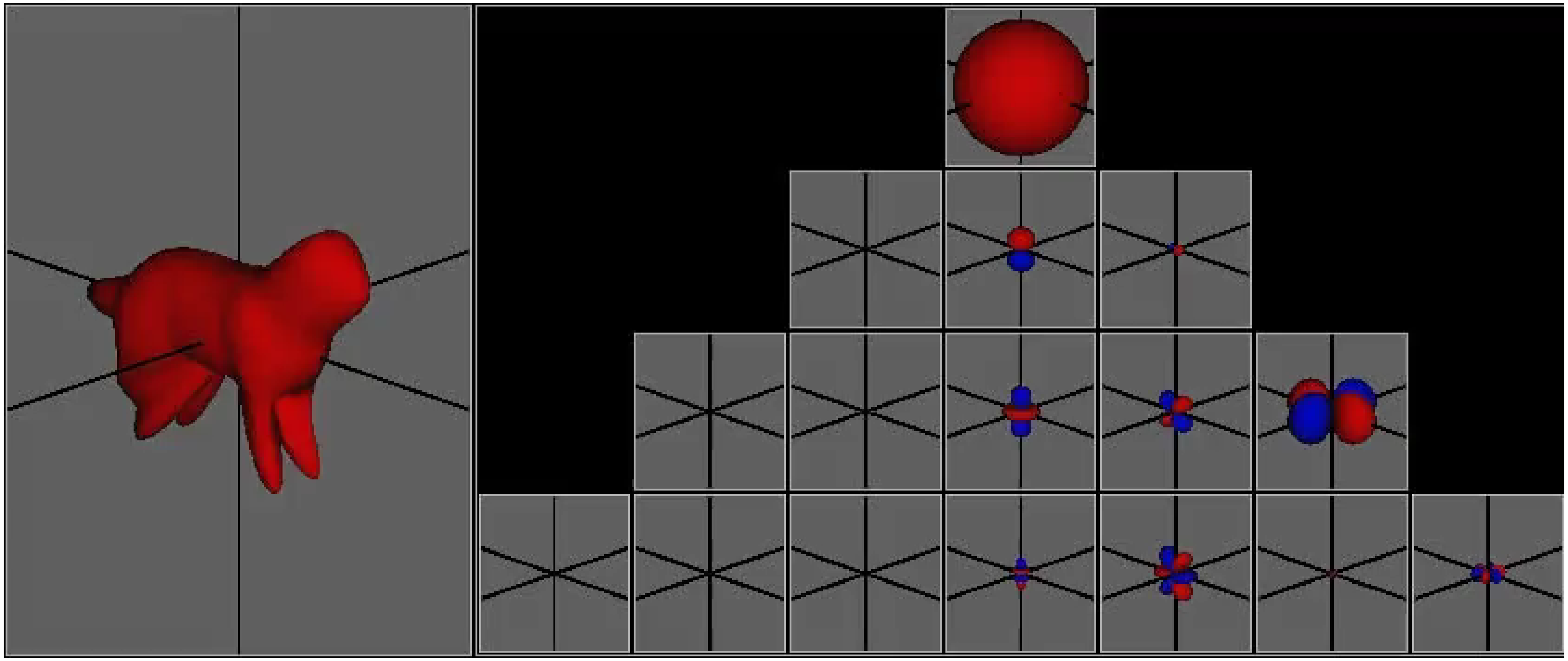
Example:

Since 2D rotations commute, we can decompose the space of functions on a circle into one (complex) dimensional subspaces that rotate into themselves.



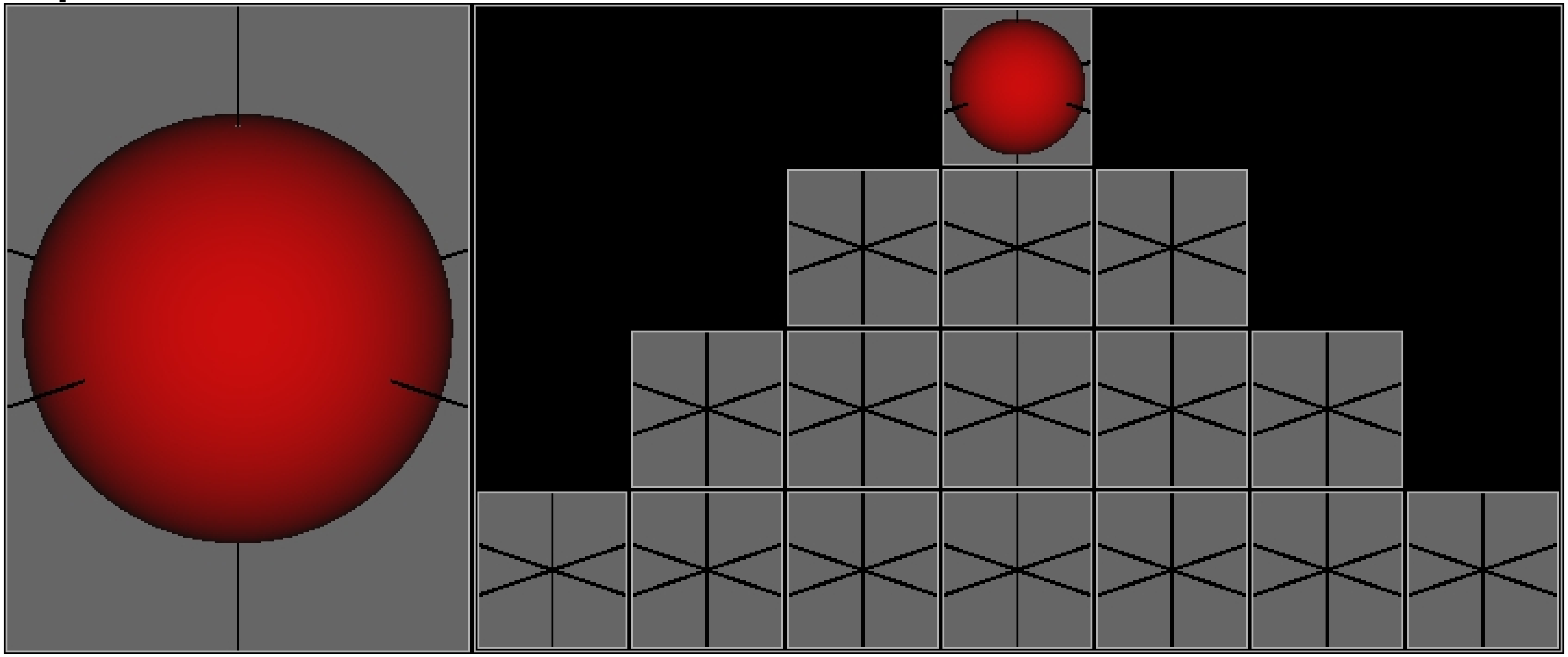
Example:

3D rotations don't commute, so the space of spherical functions need not decompose into one (complex) dimensional irreducible sub-representations.



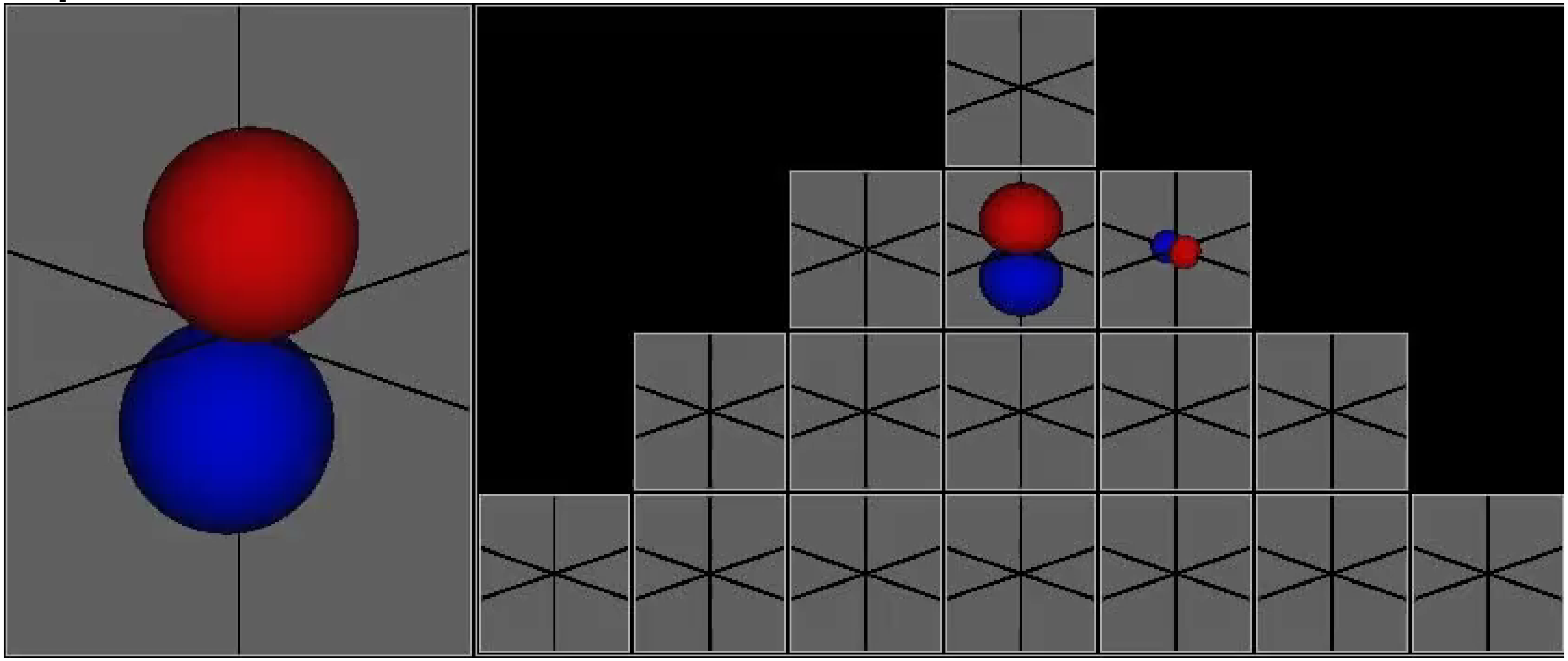
Example:

3D rotations don't commute, so the space of spherical functions need not decompose into one (complex) dimensional irreducible sub-representations.



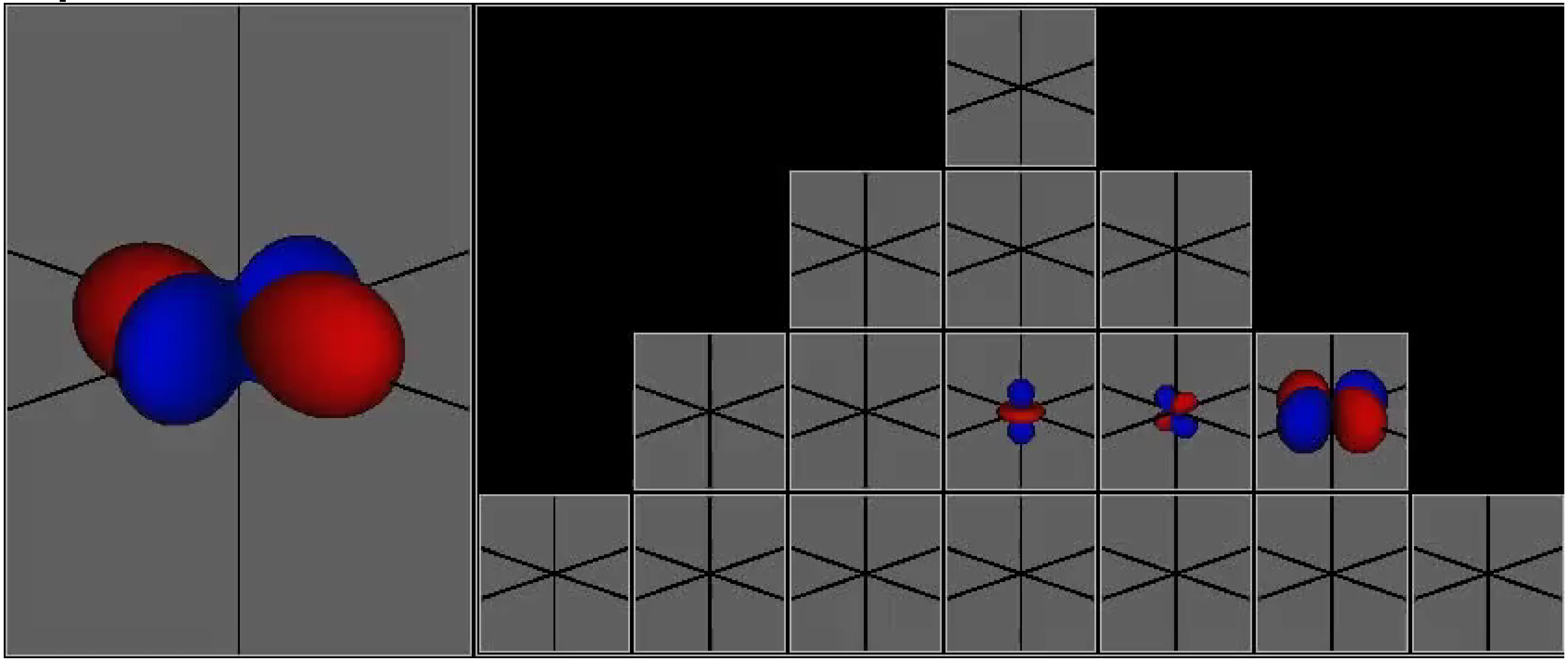
Example:

3D rotations don't commute, so the space of spherical functions need not decompose into one (complex) dimensional irreducible sub-representations.



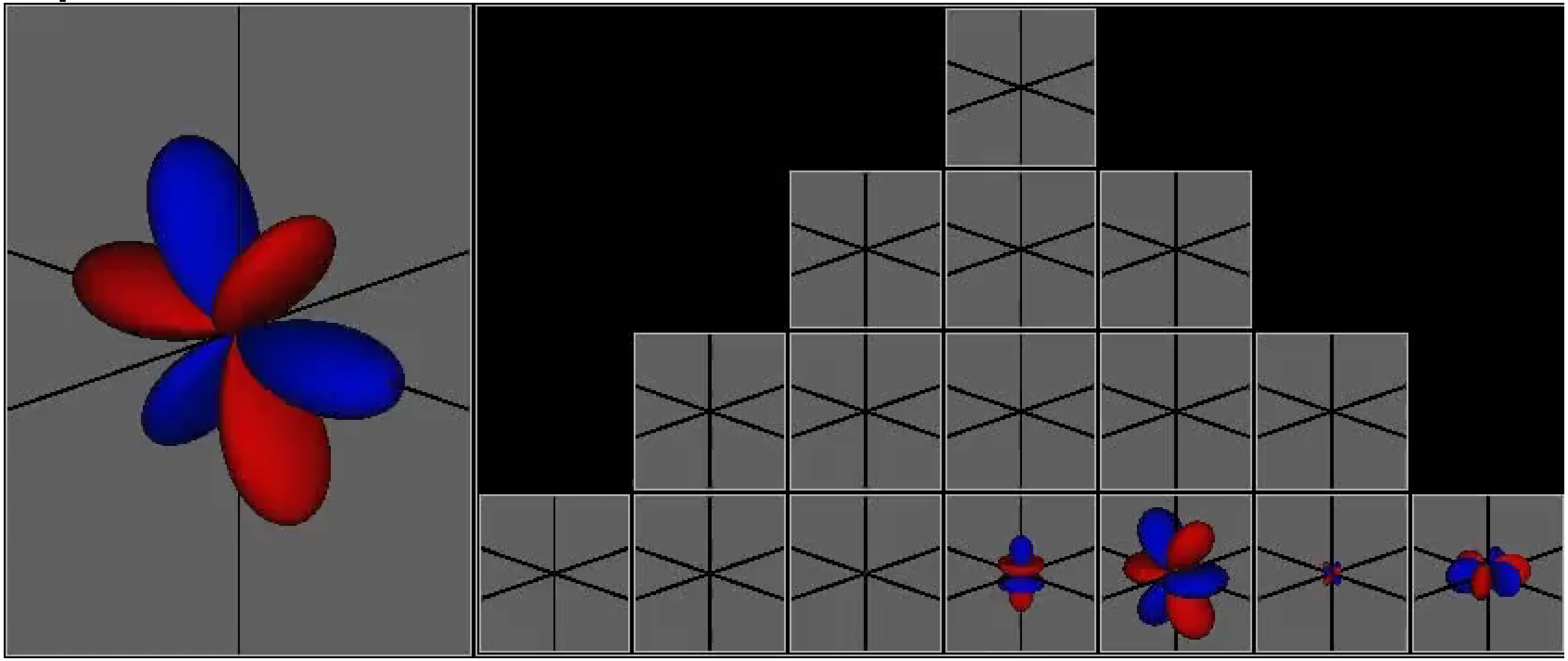
Example:

3D rotations don't commute, so the space of spherical functions need not decompose into one (complex) dimensional irreducible sub-representations.



Example:

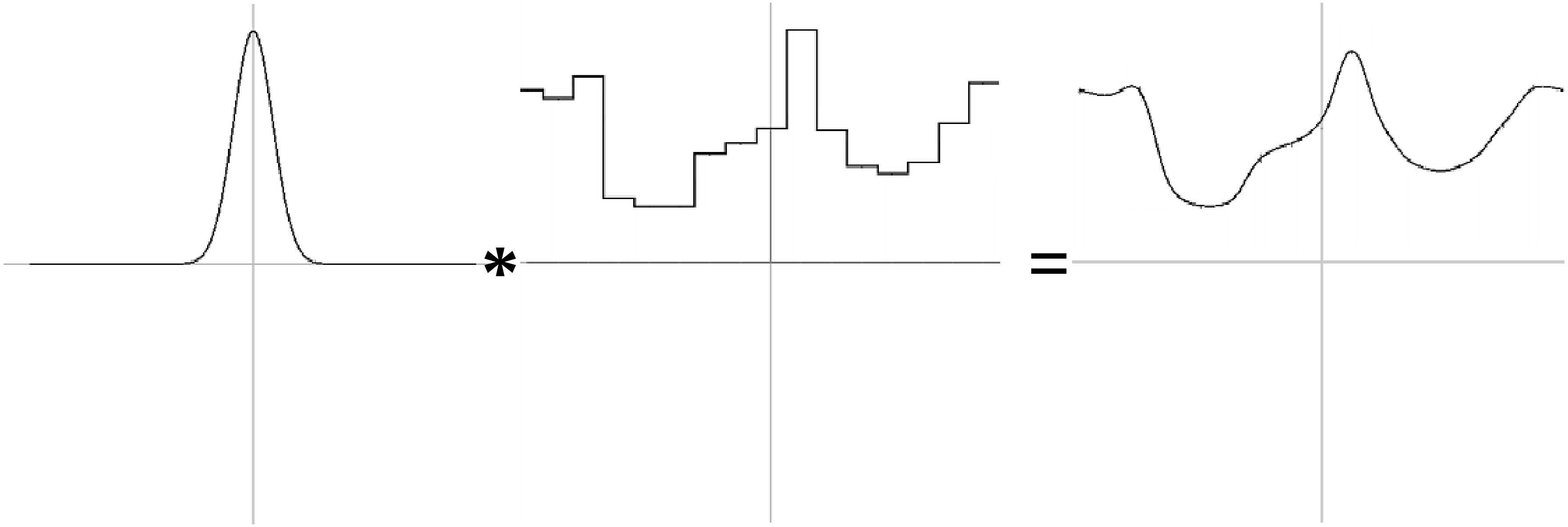
3D rotations don't commute, so the space of spherical functions need not decompose into one (complex) dimensional irreducible sub-representations.



Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

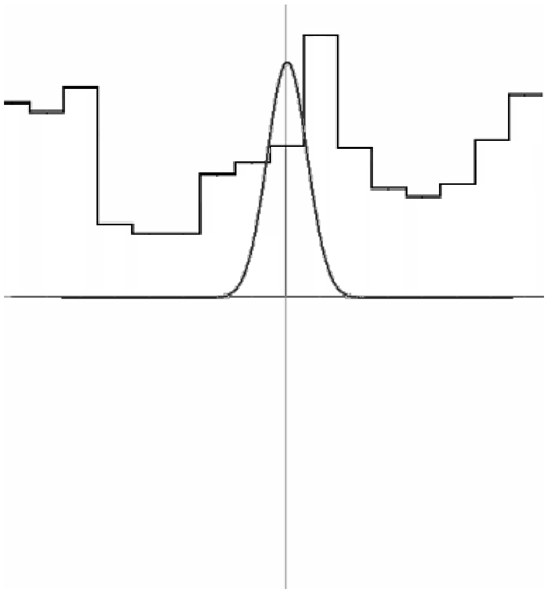
E.g. Smoothing:

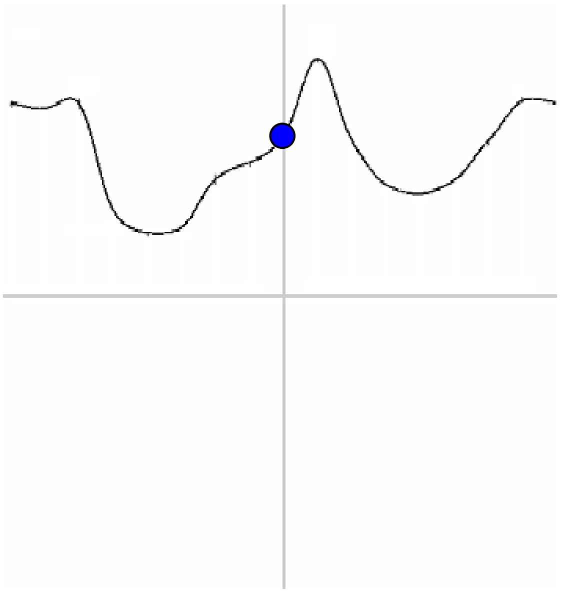


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

E.g. Smoothing:

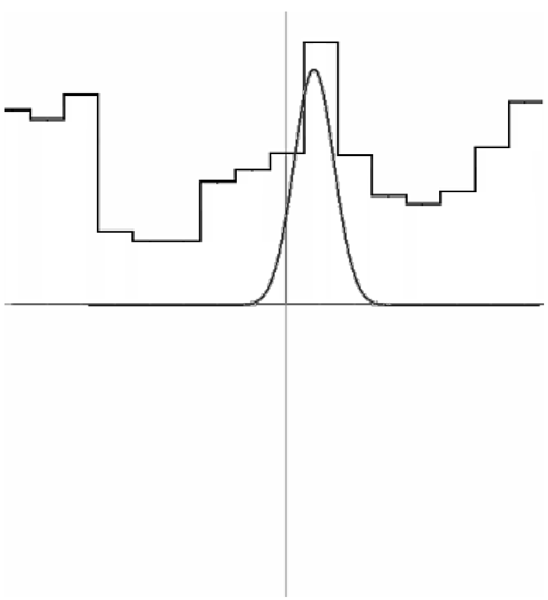


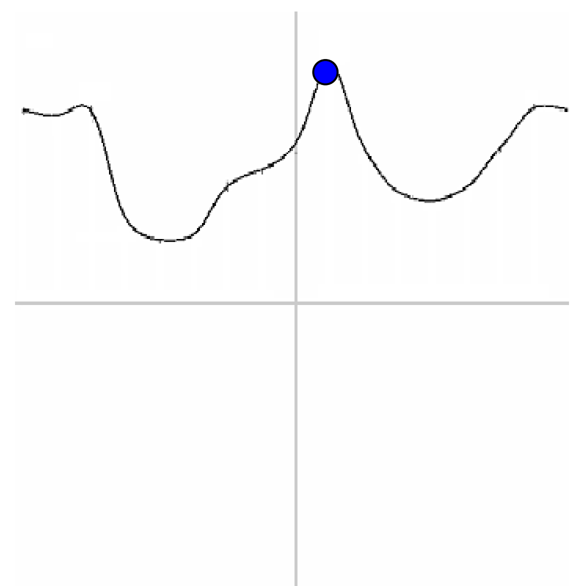


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

E.g. Smoothing:

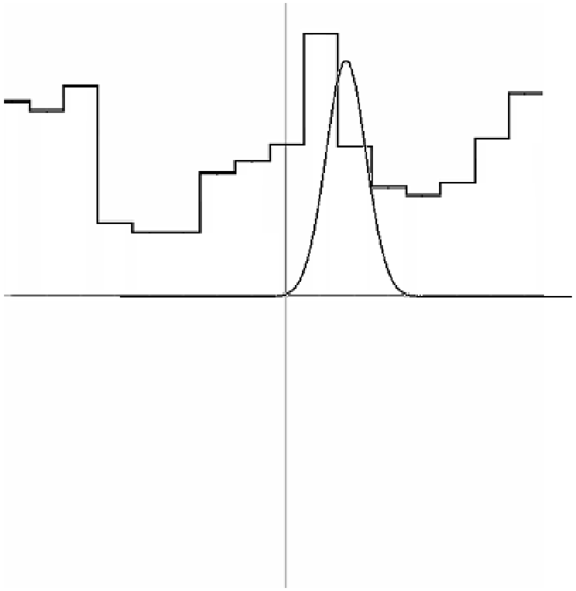


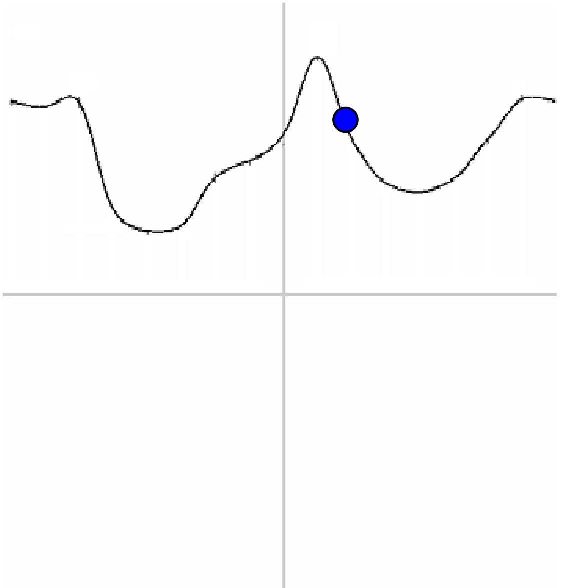


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

E.g. Smoothing:

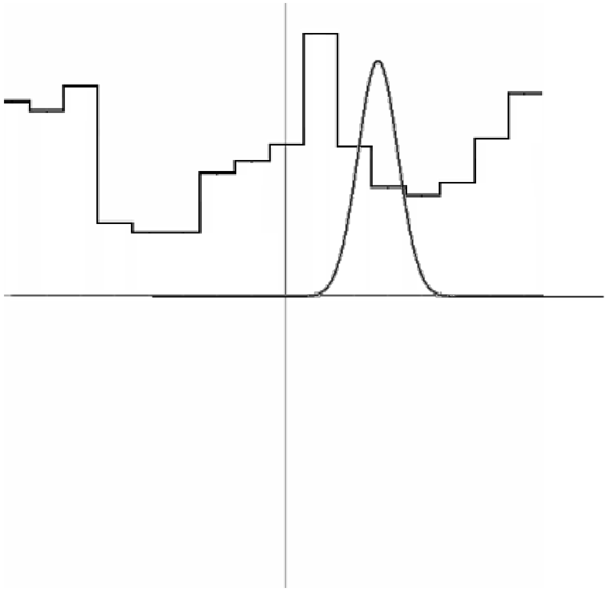


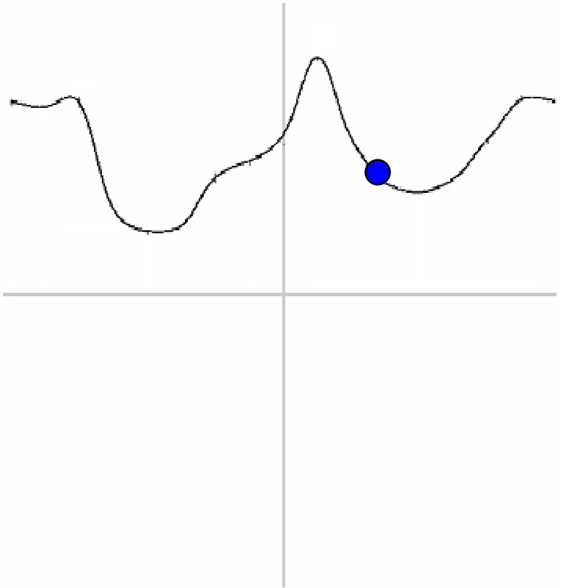


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

E.g. Smoothing:

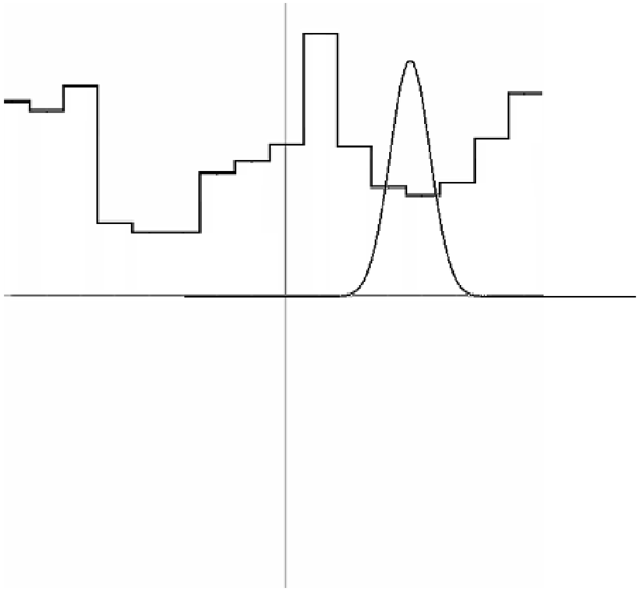


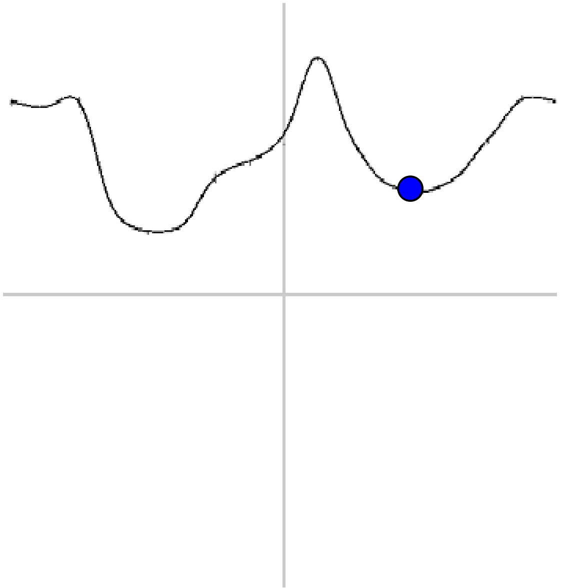


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

E.g. Smoothing:

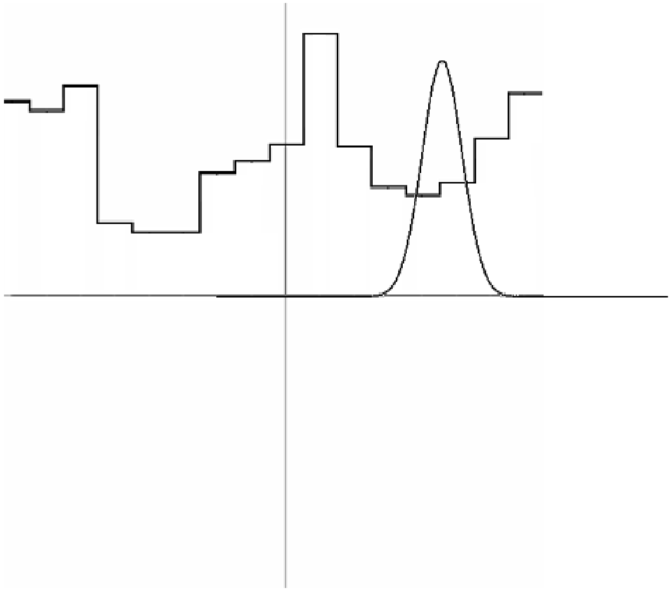


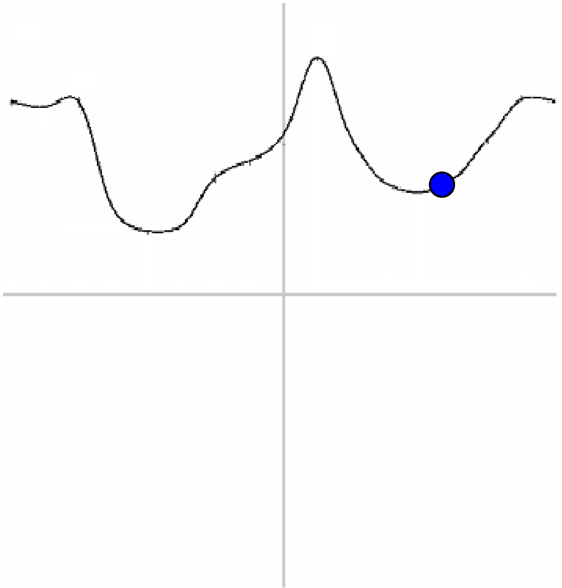


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

E.g. Smoothing:

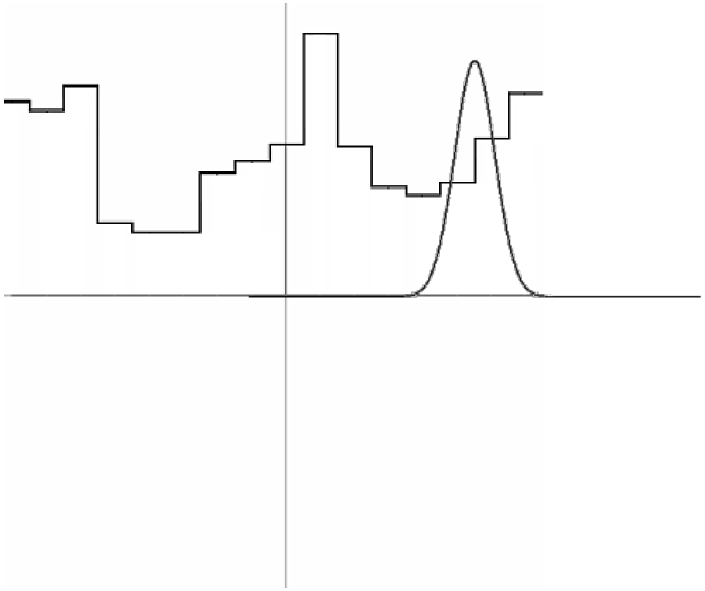


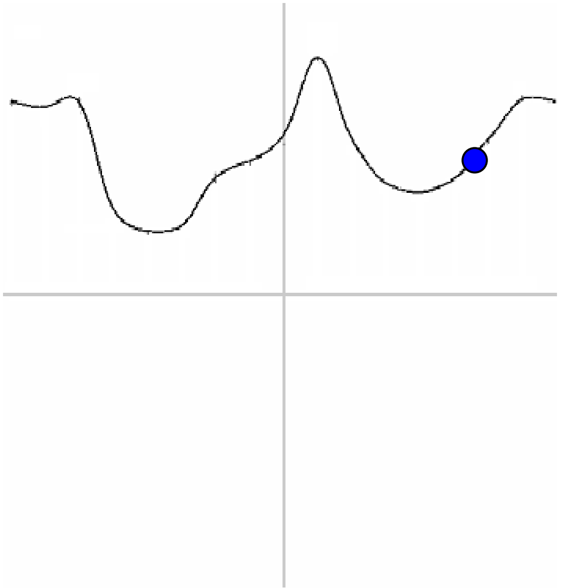


Why do we care?

In signal/image/voxel processing, we are often interested in applying a filter to some initial data.

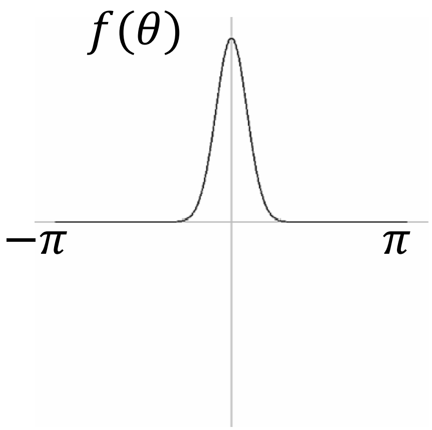
E.g. Smoothing:

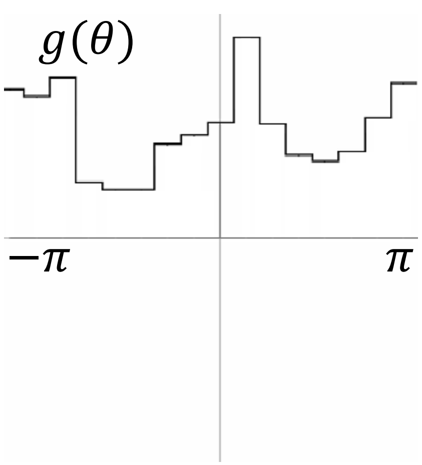


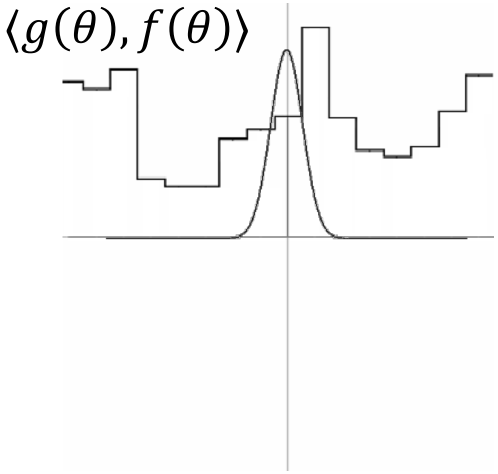


Correlation

What we are really doing is computing a moving inner product:

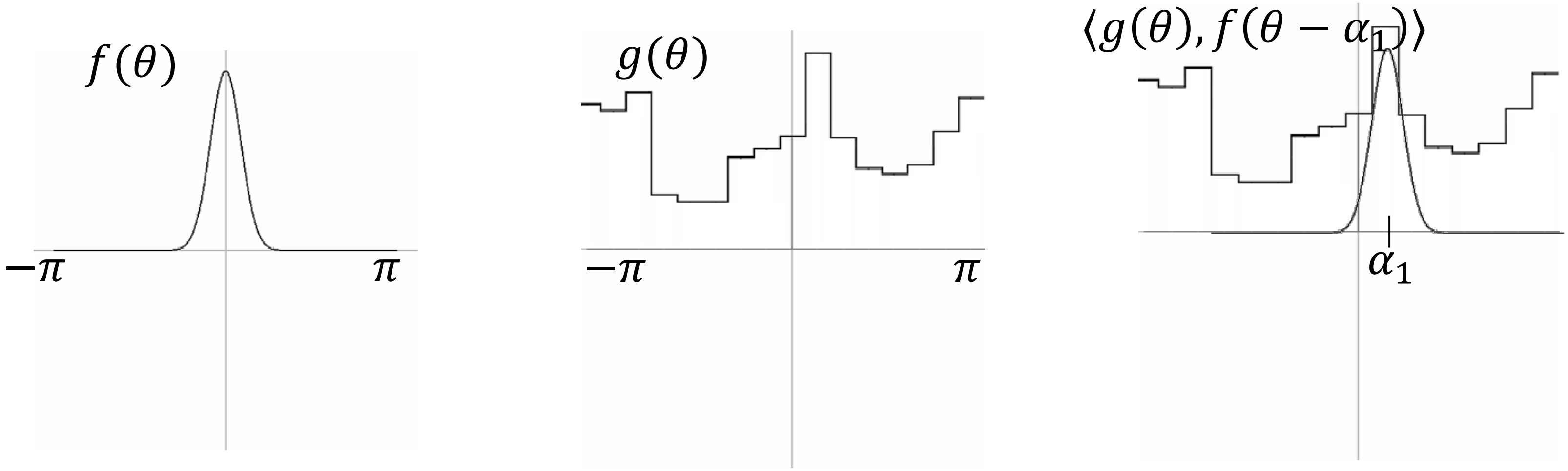






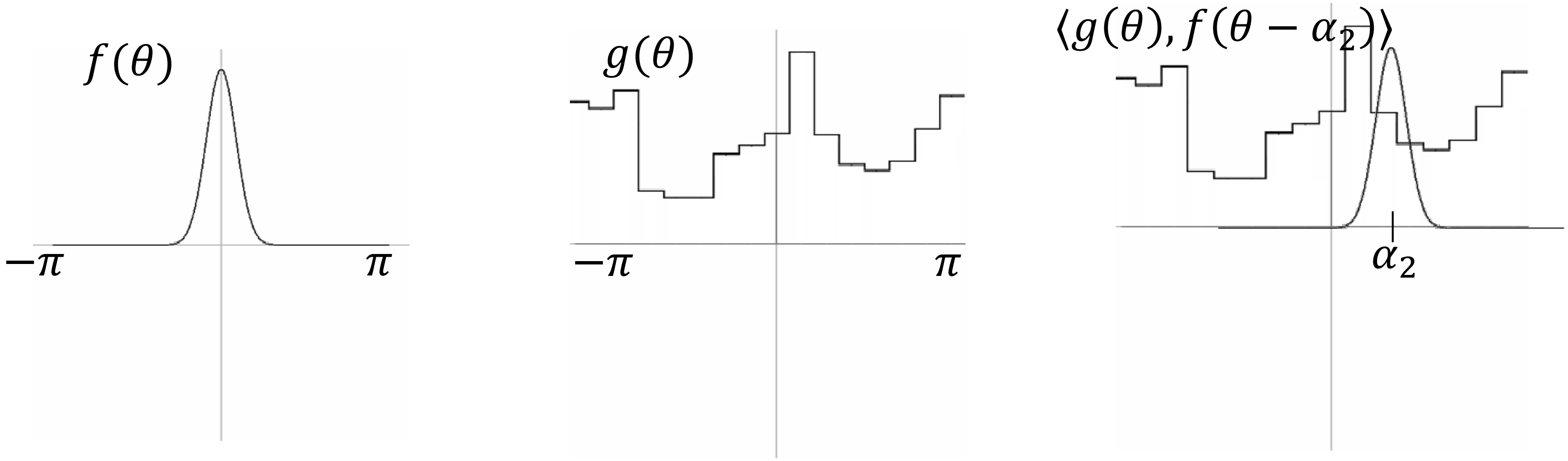
Correlation

What we are really doing is computing a moving inner product:



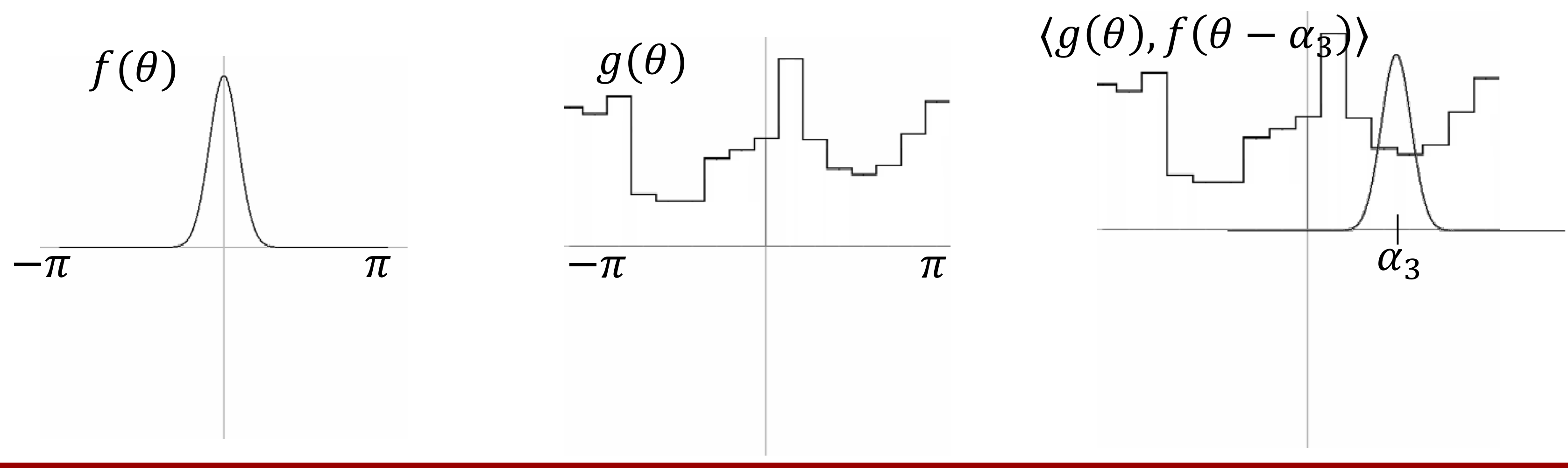
Correlation

What we are really doing is computing a moving inner product:



Correlation

What we are really doing is computing a moving inner product:

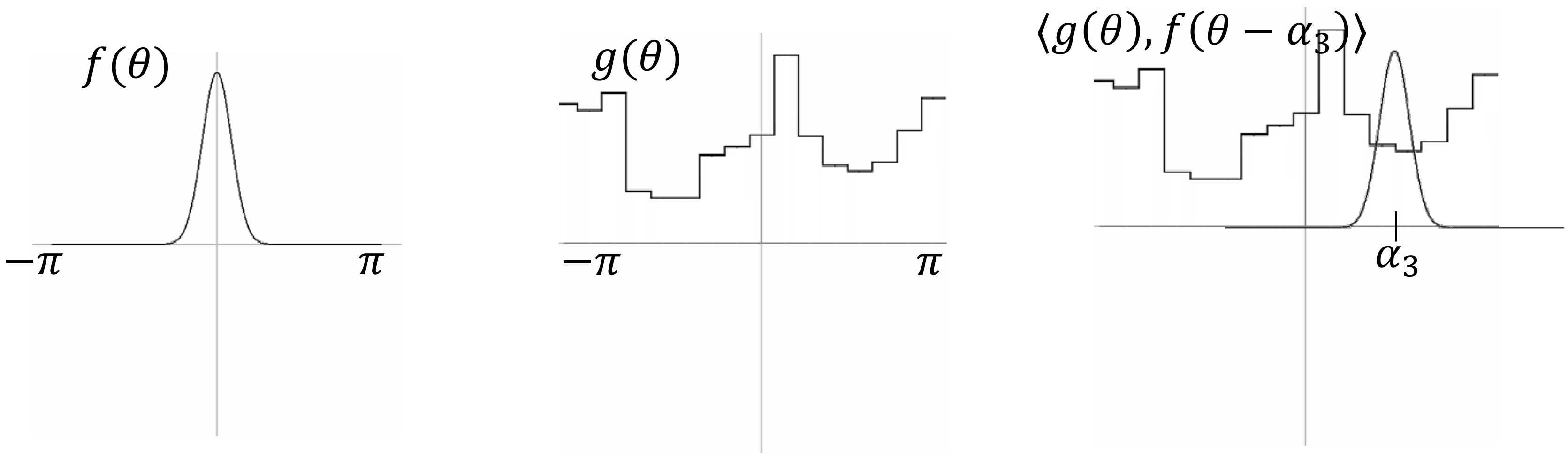


Correlation

We can write out the operation of smoothing a signal g by a filter f as:

$$(g \star f)(\alpha) = \langle g, \rho_\alpha(f) \rangle$$

where ρ_α is the linear transformation that translates a periodic function by α.



Correlation

We can think of this as a representation:

- $V = L^2(\mathbb{R}/2\pi\mathbb{Z})$ is the space of periodic functions on the line
- $G = \mathbb{R}/2\pi\mathbb{Z}$ is the group $\mathbb{R}$ modulo addition by integer multiples of 2π
- ρ_α is the representation translating a function by α.

This is a representation of a commutative group…

Warning:

The domain of functions in V and the space G are both parametrized by points in the range $[0,2\pi)$.

- Though the parameters domains are the same, we should think of them as distinct. (The former is the circle S^1, the latter is the rotation group $SO(2)$.)

Correlation

$\boldsymbol{\zeta}^j \in V, \chi^j: G \to \mathbb{C}$

⇒ There exist orthogonal one-dimensional (complex) subspaces $V_1, \cdots, V_n \subset V$ that are the irreducible representations of V.*

Setting $\boldsymbol{\zeta}^j \in V_j$ to be a unit-vector, we know that the group acts on $\boldsymbol{\zeta}^j$ by scalar multiplication.

That is, there exist $\chi^j: G \to \mathbb{C}$ s.t.:

$$\rho_\alpha\left(\zeta^j\right) = \chi^j(\alpha) \cdot \boldsymbol{\zeta}^j$$

Since the ζ^j are unit vectors:

$$\chi^j(\alpha) = \langle \rho_\alpha\left(\boldsymbol{\zeta}^j\right), \boldsymbol{\zeta}^j \rangle$$

*In reality, there are infinitely many such subspaces.

Correlation

$\boldsymbol{\zeta}^j \in V,\ \chi^j : G \to \mathbb{C}$

⇒ There exist orthogonal one-dimensional (complex) subspaces $V_1, \cdots, V_n \subset V$ that are the irreducible representations of V.*

Setting $\boldsymbol{\zeta}^j \in V_j$ to be a unit-vector, we know that the group acts on $\boldsymbol{\zeta}^j$ by scalar multiplication.

That is, there exist $\chi^j : G \to \mathbb{C}$ s.t.:

Note:
Since the V_i are orthogonal, the function basis $\{\zeta^1, \cdots, \zeta^n\}$ is orthonormal.

Since

$$\chi^j(\alpha) = \langle \rho_\alpha(\boldsymbol{\zeta}^j), \boldsymbol{\zeta}^j \rangle$$

*In reality, there are infinitely many such subspaces.

Correlation

$\boldsymbol{\zeta}^j \in V, \chi^j : G \to \mathbb{C}$

Setting $\boldsymbol{\zeta}^j \in V_j$ to be a unit-vector, we know that the group acts on $\boldsymbol{\zeta}^j$ by scalar multiplication:

$$\rho_\alpha\left(\boldsymbol{\zeta}^j\right) = \chi^j(\alpha) \cdot \boldsymbol{\zeta}^j$$

We can write out vectors $f, g \in V$ in the basis $\{\zeta^1, \ldots, \zeta^n\}$ as:

$$f = \hat{f}_1 \cdot \boldsymbol{\zeta}^1 + \cdots + \hat{f}_n \cdot \boldsymbol{\zeta}^n$$
$$g = \hat{g}_1 \cdot \boldsymbol{\zeta}^1 + \cdots + \hat{g}_n \cdot \boldsymbol{\zeta}^n$$

with $\hat{\mathbf{f}}, \hat{\mathbf{g}} \in \mathbb{C}^n$.

Correlation

$\zeta^j \in V, \chi^j: G \to \mathbb{C}$

Then the correlation can be written as:

$$(g \star f)(\alpha) = \langle g, \rho_\alpha(f) \rangle$$

Expanding in the function basis $\{\zeta^1, \dots, \zeta^n\}$:

$$(g \star f)(\alpha) = \left\langle \sum_j \hat{g}_j \cdot \zeta^j, \rho_\alpha\left(\sum_k \hat{f}_k \cdot \zeta^k\right) \right\rangle$$

Key Idea:

Since the subspaces V_i are orthogonal sub-representations, we shouldn't have to consider the inner-product between vectors from different subspaces.

Correlation

$$\boldsymbol{\zeta}^j \in V,\ \chi^j : G \to \mathbb{C}$$

$$(g \star f)(\alpha) = \left\langle \sum_j \hat{g}_j \cdot \boldsymbol{\zeta}^j , \rho_\alpha\left(\sum_k \hat{f}_k \cdot \boldsymbol{\zeta}^k\right)\right\rangle$$

Using the linearity of ρ_α and the (conjugate)-symmetry of the inner-product:

$$= \left\langle \sum_j \hat{g}_j \cdot \boldsymbol{\zeta}^j , \sum_k \hat{f}_k \cdot \rho_\alpha\left(\boldsymbol{\zeta}^k\right)\right\rangle$$

$$= \sum_j \hat{g}_j \left\langle \boldsymbol{\zeta}^j , \sum_k \hat{f}_k \cdot \rho_\alpha\left(\boldsymbol{\zeta}^k\right)\right\rangle$$

$$= \sum_{j,k} \hat{g}_j \cdot \bar{\hat{f}}_k \left\langle \boldsymbol{\zeta}^j , \rho_\alpha\left(\boldsymbol{\zeta}^k\right)\right\rangle$$

Correlation

$\boldsymbol{\zeta}^j \in V,\ \chi^j : G \to \mathbb{C}$

$$(g \star f)(\alpha) = \sum_{j,k} \hat{g}_j \cdot \bar{\hat{\bar{f}}}_k \langle \boldsymbol{\zeta}^j, \rho_\alpha(\boldsymbol{\zeta}^k) \rangle$$

Because ρ_α is scalar multiplication in V_i:

$$(g \star f)(\alpha) = \sum_{j,k} \hat{g}_j \cdot \bar{\hat{\bar{f}}}_k \langle \boldsymbol{\zeta}^j, \chi^k(\alpha) \cdot \boldsymbol{\zeta}^k \rangle$$

$$= \sum_{j,k} \hat{g}_j \cdot \bar{\hat{\bar{f}}}_k \cdot \bar{\chi}^k(\alpha) \langle \boldsymbol{\zeta}^j, \boldsymbol{\zeta}^k \rangle$$

And finally, by the orthonormality of $\{\boldsymbol{\zeta}^1, \ldots, \boldsymbol{\zeta}^n\}$:

$$= \sum_{j} \hat{g}_j \cdot \bar{\hat{\bar{f}}}_j \cdot \bar{\chi}^j(\alpha)$$

Correlation

$\zeta^j \in V, \chi^j : G \to \mathbb{C}$

$$(g \star f)(\alpha) = \sum_j \hat{g}_j \cdot \bar{\hat{f}}_j \cdot \bar{\chi}^j(\alpha)$$

This implies that we can compute the correlation by multiplying the coefficients of f and g.

Correlation in the spatial domain is multiplication in the frequency domain!

Correlation

$\zeta^j \in V,\ \chi^j : G \to \mathbb{C}$

What is $\chi^j(\alpha)$?

Since the representation is unitary, $|\chi^j(\alpha)| = 1$.

$$\Downarrow$$

$$\exists \tilde{\chi}^j : G \to \mathbb{R} \quad \text{s.t.} \quad \chi^j(\alpha) = e^{-i\tilde{\chi}^j(\alpha)}$$

Correlation

$\zeta^j \in V, \chi^j: G \to \mathbb{C}$

What is $\chi^j(\alpha)$?

$$\chi^j(\alpha) = e^{-i\tilde{\chi}^j(\alpha)} \text{ for some } \tilde{\chi}^j: G \to \mathbb{R}.$$

Since it's a representation:

$$\Downarrow$$

$$\chi^j(\alpha+\beta) = \chi^j(\alpha)\cdot\chi^j(\beta) \quad \forall \alpha,\beta \in G$$

$$\Downarrow$$

$$\tilde{\chi}^j(\alpha+\beta) = \tilde{\chi}^j(\alpha) + \tilde{\chi}^j(\beta)$$

$$\Downarrow$$

$$\exists \kappa_j \in \mathbb{R} \quad \text{s.t.} \quad \tilde{\chi}^j(\alpha) = \kappa_j \cdot \alpha$$

Correlation

$\zeta^j \in V,\ \chi^j: G \to \mathbb{C}$

What is $\chi^j(\alpha)$?

$$\chi^j(\alpha) = e^{-i\kappa_j\alpha} \text{ for some } \kappa_j \in \mathbb{R}.$$

Since it's a representation:

$$\Downarrow$$

$$1 = \chi^j(2\pi) = e^{-i\kappa_j 2\pi}$$

$$\Downarrow$$

$$\kappa_j \in \mathbb{Z}$$

Correlation

$\zeta^j \in V, \chi^j : G \to \mathbb{C}$

<u>What is $\chi^j(\alpha)$</u>?

$$(g \star f)(\alpha) = \sum_j \hat{g}_j \cdot \bar{\hat{f}}_j \cdot \bar{\chi}^j(\alpha)$$

Thus, the correlation of the signals $f, g : S^1 \to \mathbb{C}$ can be expressed as:

$$(g \star f)(\alpha) = \sum_j \hat{g}_j \cdot \bar{\hat{f}}_j \cdot e^{i\kappa_j \alpha}$$

where $\kappa_j \in \mathbb{Z}$.

Correlation

$\boldsymbol{\zeta}^j \in V, \chi^j : G \to \mathbb{C}$

What is $\boldsymbol{\zeta}^j$?

By definition of χ^j, we have:

$$\rho_\alpha\left(\boldsymbol{\zeta}^j\right) = \chi^j(\alpha) \cdot \boldsymbol{\zeta}^j = e^{-ik_j\alpha} \cdot \boldsymbol{\zeta}^j$$

for some $k_j \in \mathbb{Z}$.

On the other hand, we have:

$$\begin{aligned}\left[\rho_\alpha\left(\boldsymbol{\zeta}^j\right)\right](\theta) &= \boldsymbol{\zeta}^j(\theta - \alpha) \\ &= \boldsymbol{\zeta}^j(\theta) \cdot e^{-ik_j\alpha}\end{aligned}$$

$$\Downarrow$$

$$\boldsymbol{\zeta}^j(\theta) = c_j \cdot e^{ik_j\theta}$$