Submitted to Journal of Fourier Analysis and Applications, September 1997, revised February 1999

Designing Local Orthogonal Bases on Finite Groups I: Abelian Case

Riccardo Bernardini
University of Padova
35131 Padova, Italy
Phone: +39-49-8277827
bernardi@dei.unipd.it

Jelena Kovačević
Bell Laboratories
Murray Hill, NJ 07974, USA
Phone: +1-908-582-6504
jelena@bell-labs.com

February 15, 1999

Abstract

We extend to general finite groups a well-known relation used for checking the orthogonality of a system of vectors as well as for orthogonalizing a nonorthogonal one. This, in turn is used for designing local orthogonal bases obtained by unitary transformations of a single prototype filter. The first part of this work considers abelian groups. The second part considers nonabelian groups where, as an example, we show how to build such bases where the group of unitary transformations consists of modulations and rotations. These bases are useful for building systems for evaluating image quality.

1 Introduction

In the past decade the field of image processing has grown considerably, and although various successful techniques have been developed for tasks such as image compression, understanding and segmentation, one final piece is missing. Bearing in mind that ultimately, an image is evaluated by a human observer, the usual mean-square error is not appropriate and thus we still lack subjective measures of image quality. Several works in recent years have tried to address this problem, notably [1, 2, 3, 4].

Several approaches to subjective distance of images rely on a weighted measure of the error in frequency, with the justification that the visual system is lowpass and high-frequency errors are less noticeable (thus lowpass parts have more weight). Sometimes the error is processed with a log-like nonlinear function. However, this approach works better for audio than for images since one could argue that, while perception of audio is in the frequency domain, perception of images is in the spatial domain. Indeed, people are so aware of the spatial structure of the noise that sometimes they recognize it and give it names such as "blocking effect", "ringing", "blurring" and so on. Moreover, some types of noise are more disturbing than others. For example, a slight blurring or a slight scaling is both less noticeable and less annoying than the blocking effect. A subjective measure of image

quality has to account for this, and such a goal can be accomplished only by considering the image from a more high-level perspective.

The course we want to pursue is that we can recognize certain "structures" in an image. It is widely believed that the more structured noise is, the more annoying it is. Some physiological results point out that the early stage of the human visual system (HVS) works like a filter bank on the retinal image. These filters can be seen as being obtained by rotation and modulation of an original prototype filter. Other theories suggest that, starting from the response of the first low-level stage, the visual system performs some higher-level processing by recognizing regularities in the filter bank output.

To find a measure of subjective quality of an image in a structure domain, one could do the following: Use the technique developed for the design of local orthogonal bases [5] and design a filter bank made of modulations and rotations of a prototype filter. With such a filter bank analyze a class of images and determine how the structures reflect themselves in the output. Identify the characteristics of structures associated with noise and/or artifacts. Develop an algorithm capable of recognizing image structures from the filter bank response. By comparing the output of such an algorithm with the results of psychophysical experiments, determine a function mapping the structure content of an image into a physiological quality score.

This work concentrates on one part of the proposed system – the design of local bases obtained by unitary transformations of one or more prototype filters. As an example useful for our image processing problem, in the second part of this work [6] we show how to obtain such filter families where the group is that of modulations and rotations. To construct such a basis, we extend the following well-known fact:

$$\langle f(t), f(t-n)\rangle \;=\; \delta(n) \Leftrightarrow \sum_{k=-\infty}^{\infty} |F(\omega + 2\pi k)|^2 = 1, \tag{1}$$

where $f(t)$ is a continuous-time function and $F(\omega)$ is its Fourier transform. Property (1) proves its usefulness both in testing the orthogonality of $f(t)$ with respect to its integer translations as well as in producing functions enjoying such a property. Property (1) can also be seen as a necessary and sufficient condition for the orthogonality of f with respect to the functions obtained by applying to f a group of unitary linear transformations, here the translations by integer values.

We extend (1) so the group of integer translations is replaced by a more general group. Note, however, that although the underlying group in (1) is infinite (integer translations in $\mathbb{Z}$), in this work we use only finite groups. Relation (1) serves only as a guiding light. It is often proved by observing that the left-hand side of the equation

is the deterministic autocorrelation of f sampled on $\mathbb{Z}$ and the right-hand side follows from the Poisson formula. Although such a proof is simple and elegant, it cannot be easily generalized.

This paper consists of two parts: In the first part, we study the problem of extending (1) where the underlying group is a finite abelian group of unitary transformations of a given vector space onto itself. Even though this is covered by the treatment on nonabelian groups presented in the second part of the work [6], it is simple and highlights the main concepts of our procedure without introducing many technical difficulties. In [6] we also discuss the filter design problem and give an example of a design where the group consists of modulations and rotations. Appendix A presents a self-contained introduction to the subject of group representations, characters and Fourier analysis on groups. Vector sets are developed and explained in Appendix B while in Appendix C we prove Property 1.

2 How it Works on a Simple Example

Consider a vector space $\mathcal{V}$, with an inner product $\langle \cdot, \cdot \rangle$, and let Γ be a finite group of unitary transformations of $\mathcal{V}$ onto itself, that is, Γ is a set of linear transformations such that for each $U \in \Gamma$ and $\boldsymbol{b}, \boldsymbol{c} \in \mathcal{V}$, $\langle U\boldsymbol{b}, U\boldsymbol{c} \rangle = \langle \boldsymbol{b}, \boldsymbol{c} \rangle$[1].

Our aim is, given such a group Γ, find necessary and sufficient conditions on a vector $\boldsymbol{b} \in \mathcal{V}$ such that the set $\mathcal{O} = \{\mathbf{c} \mid \mathbf{c} = U\boldsymbol{b}, U \in \Gamma\}$ is an orthonormal set of vectors (not necessarily a basis). The analogy with (1) is immediate.

We can put the condition of the orthogonality of $\mathcal{O}$ in a form closer to (1) as

$$\langle \boldsymbol{b}, U\boldsymbol{b} \rangle \;=\; \begin{cases} 1 & \text{if } U = \mathcal{I}, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Equation (2) can be written in a more compact form by defining, analogously to the usual Kronecker delta,

$$\delta_U \;\triangleq\; \begin{cases} 1 & \text{if } U = \mathcal{I}, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Then, (2) becomes

$$\langle \boldsymbol{b}, U\boldsymbol{b} \rangle = \delta_U, \qquad U \in \Gamma. \tag{4}$$

For simplicity, let us give a name to Property (4).

Definition 1 *Vector $\boldsymbol{b}$ is said to be orthogonal with respect to the action of Γ if it satisfies (4).*

[1] In the case of (1), $\mathcal{V}$ is $L^2(\mathbb{R})$ and Γ is the set of integer translations of the functions of $L^2(\mathbb{R})$.

Our aim is to prove something of the type

$$\langle \boldsymbol{b}, U\boldsymbol{b} \rangle \;=\; \delta_U \;\Leftrightarrow\; ??? \;=\; 1, \tag{5}$$

where "???" is a (still to be found) function of $\boldsymbol{b}$. Since the couple $(\delta, 1)$ usually form a Fourier transform pair, one can think of using some sort of a Fourier transform to find "???".

Indeed, the scalar product $\langle \boldsymbol{b}, U\boldsymbol{b} \rangle$ can be seen as a function $\varphi(U)$ defined on the group Γ, and since it is known that it is possible to define the Fourier transform on rather general groups we can make this our line of work. The definition of Fourier transforms on groups relies on group-theoretical concepts such as group representations, irreducible representations and characters. To make this work self-contained we give in Appendix A some basic definitions and properties. More details on these topics can be found in the text by Serre [7].

2.1 Example

We start by presenting an example which, although simple, displays all the properties found in a more general setting. Consider $\mathcal{V} = \mathbb{R}^2$ and

$$\Gamma \;=\; \left\{ \mathcal{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}, \tag{6}$$

that is, the group performing the exchange of the components of vectors from $\mathbb{R}^2$. Condition (4) here becomes

$$\varphi(U) \;=\; \langle \boldsymbol{b}, U\boldsymbol{b} \rangle \;=\; \begin{cases} \boldsymbol{b}^T\boldsymbol{b} & = 1, \quad U = \mathcal{I}, \\ \boldsymbol{b}^T V \boldsymbol{b} & = 0, \quad U = V. \end{cases} \tag{7}$$

2.2 Fourier Transform as an Analysis Tool

Remember that most of the concepts pertaining to Fourier transform on groups used in this section can be found in Appendix A and [8]. Since Γ in (6) is isomorphic to the abelian group $\mathbb{Z}/2\mathbb{Z}$, it has two one-dimensional irreducible representations, namely

$$\begin{aligned} \pi_1(\mathcal{I}) &= 1, \quad & \pi_1(V) &= 1, \\ \pi_{-1}(\mathcal{I}) &= 1, \quad & \pi_{-1}(V) &= -1. \end{aligned} \tag{8}$$

By using (8), the Fourier transform of any function $\varphi(U)$ is seen as a signal Φ defined on $\{1, -1\}$ which we can compute in the following way:

$$\Phi(\omega) \;=\; \sum_{U \in \Gamma} \varphi(U)\pi_\omega(U) \;=\; \varphi(\mathcal{I})\pi_\omega(\mathcal{I}) \;+\; \varphi(V)\pi_\omega(V). \tag{9}$$

Thus, when $\varphi(U)$ is the inner product $\langle \boldsymbol{b}, U\boldsymbol{b} \rangle$ and with representations given in (8)

$$\begin{aligned} \Phi(1) &= \varphi(\mathcal{I}) + \varphi(V) \;=\; \boldsymbol{b}^T\boldsymbol{b} + \boldsymbol{b}^T V \boldsymbol{b}, \\ \Phi(-1) &= \varphi(\mathcal{I}) + (-1)\varphi(V) \;=\; \boldsymbol{b}^T\boldsymbol{b} - \boldsymbol{b}^T V \boldsymbol{b}. \end{aligned} \tag{10}$$

Thus, (7) in "frequency" domain becomes

$$\Phi(\omega) \;=\; 1, \text{ for } \omega \;=\; \pm 1. \tag{11}$$

Equation (11) is precisely the equivalent of (1) when the group is given by (6). Note that (10) can also be written as

$$\begin{array}{rcl} \Phi(1) & = & \boldsymbol{b}^T (\mathcal{I} + V)\, \boldsymbol{b} \;=\; \boldsymbol{b}^T \mathcal{U}_1 \boldsymbol{b}, \\ \Phi(-1) & = & \boldsymbol{b}^T (\mathcal{I} - V)\, \boldsymbol{b} \;=\; \boldsymbol{b}^T \mathcal{U}_{-1} \boldsymbol{b}, \end{array} \tag{12}$$

where

$$\mathcal{U}_\omega \;=\; \sum_{U \in \Gamma} U\, \pi_\omega(U), \tag{13}$$

that is,

$$\begin{array}{rcl} \mathcal{U}_1 \;\stackrel{\triangle}{=}\; (\mathcal{I} + V) & = & \left[\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right], \\ \mathcal{U}_{-1} \;\stackrel{\triangle}{=}\; (\mathcal{I} - V) & = & \left[\begin{array}{cc} 1 & -1 \\ -1 & 1 \end{array} \right], \end{array} \tag{14}$$

can be seen as the Fourier transforms of the matrices constituting Γ. Equations (12) give the analysis algorithm: we can first compute matrices $\mathcal{U}_\omega$ (that do not depend on $\boldsymbol{b}$), then we can check if every product $\boldsymbol{b}^T \mathcal{U}_\omega \boldsymbol{b}$ is equal to 1.

2.3 Orthonormalization with the Fourier Transform

Observe the following properties of matrices $\mathcal{U}_1$ and $\mathcal{U}_{-1}$:

$$\begin{array}{rcll} \mathcal{U}_\omega \mathcal{U}_{\omega_1} & = & \mathbf{0}, & \omega \neq \omega_1, \\ \mathcal{U}_\omega \mathcal{U}_\omega & = & 2\mathcal{U}_\omega, & \omega = -1, 1, \\ {\mathcal{U}_\omega}^T & = & \mathcal{U}_\omega, & \omega = -1, 1. \end{array} \tag{15}$$

In other words, $\mathcal{U}_1/2$ and $\mathcal{U}_{-1}/2$ are two orthogonal projections. Hence, $\Phi(\omega) = \boldsymbol{b}^T \mathcal{U}_\omega \boldsymbol{b}$ is always nonnegative. Next define

$$\hat{\boldsymbol{b}} \;\stackrel{\triangle}{=}\; \frac{1}{\sqrt{\Phi(1)}} \frac{\mathcal{U}_1}{2} \boldsymbol{b} \;+\; \frac{1}{\sqrt{\Phi(-1)}} \frac{\mathcal{U}_{-1}}{2} \boldsymbol{b}. \tag{16}$$

It is easy to check that $\{U\hat{\boldsymbol{b}}\}_{U \in \Gamma}$ is an orthonormal system in $\mathbb{R}^2$ (actually it is a basis, since $\mathbb{R}^2$ has dimension two). To show this, we resort to the frequency-domain condition, that is, we prove that $\hat{\Phi}(\omega) = 1$, for $\omega = \pm 1$. Since $\Phi(\omega) = \boldsymbol{b}^T \mathcal{U}_\omega \boldsymbol{b}$, then for $\omega = 1$,

$$\hat{\Phi}(1) \;=\; \hat{\boldsymbol{b}}^T \mathcal{U}_1 \hat{\boldsymbol{b}} = \left(\frac{1}{2\sqrt{\Phi(1)}} \mathcal{U}_1 \boldsymbol{b} + \frac{1}{2\sqrt{\Phi(-1)}} \mathcal{U}_{-1} \boldsymbol{b} \right)^T \mathcal{U}_1 \left(\frac{1}{2\sqrt{\Phi(1)}} \mathcal{U}_1 \boldsymbol{b} + \frac{1}{2\sqrt{\Phi(-1)}} \mathcal{U}_{-1} \boldsymbol{b} \right). \tag{17}$$

The product in (17) can be written as a sum of four terms

$$\begin{array}{ll} \frac{1}{4\Phi(1)}\boldsymbol{b}^T{\mathcal{U}_1}^T\mathcal{U}_1\mathcal{U}_1\boldsymbol{b}, & \frac{1}{4\sqrt{\Phi(-1)\Phi(1)}}\boldsymbol{b}^T{\mathcal{U}_{-1}}^T\mathcal{U}_1\mathcal{U}_1\boldsymbol{b}, \\ \frac{1}{4\sqrt{\Phi(-1)\Phi(1)}}\boldsymbol{b}^T{\mathcal{U}_1}^T\mathcal{U}_1\mathcal{U}_{-1}\boldsymbol{b}, & \frac{1}{4\Phi(-1)}\boldsymbol{b}^T{\mathcal{U}_{-1}}^T\mathcal{U}_1\mathcal{U}_{-1}\boldsymbol{b}. \end{array} \tag{18}$$

Because of orthogonality relation in (15), only the top left term in (18) is nonzero; moreover, ${\mathcal{U}_1}^T\mathcal{U}_1\mathcal{U}_1 = 2\mathcal{U}_1\mathcal{U}_1 = 4\mathcal{U}_1$ because of (15). Therefore, (17) becomes

$$\hat{\Phi}(1) \;=\; \hat{\boldsymbol{b}}^T\mathcal{U}_1\hat{\boldsymbol{b}} \;=\; \frac{4}{4\Phi(1)}\boldsymbol{b}^T\mathcal{U}_1\boldsymbol{b} \;=\; \frac{\Phi(1)}{\Phi(1)} \;=\; 1. \tag{19}$$

An analogous derivation can be carried out for $\hat{\Phi}(-1)$.

Note the role played by (15) in the derivation of (17). In particular, it is the orthogonality of the two projections that allows us to apply two different normalizing factors in an effective way. Although obtained for this particular example, relations (15) hold in a more general case and the derivation of the counterpart of (16) is carried out with a more general language.

2.4 Geometric Interpretation

An interesting observation about the projection matrices $\mathcal{U}_\omega$ that still holds in the general case, is that they are projections on spaces invariant with respect to the action of the matrices of Γ (Γ-invariant). For example, the matrix $\mathcal{U}_1$ is the projection on the vector space spanned by the vector $[1,1]^T$ that maps into itself when transformed with matrix V. Similarly, $\mathcal{U}_{-1}$ projects on the space generated by $[1,-1]^T$ which only changes sign under the action of V.

With this interpretation expression (16) can be expressed in words as:

> Project $\boldsymbol{b}$ on the two orthogonal Γ-invariant spaces, normalize the two projections and sum them to obtain $\hat{\boldsymbol{b}}$.

Another way to read (16) is to say that a vector $\boldsymbol{b}$ orthogonal with respect to the action of Γ can be decomposed as the sum of unit vectors belonging to the Γ-invariant spaces. Note that this second interpretation allows us to construct such vectors without starting with a vector $\boldsymbol{b}$. Figure 1(a) shows the projection of $\boldsymbol{b}$ on the two spaces relative to $\mathcal{U}_1$ and $\mathcal{U}_{-1}$. In Figure 1(b) the two projections are normalized and recombined in Figure 1(c).

Let us finish this subsection with a summary of the above properties that hold also for general abelian groups and, with some minor variations, for nonabelian groups as well.

1. Condition $\boldsymbol{b}^T U \boldsymbol{b} = \delta_U$, $U \in \Gamma$, can be expressed in the frequency domain as $\boldsymbol{b}^T \mathcal{U}_\omega \boldsymbol{b} = 1$, for all ω, where $\mathcal{U}_\omega$ can be interpreted as the Fourier transform of the matrices U.

2. Normalized matrices $\mathcal{U}_\omega$ form a set of orthogonal projections.

3. The space on which each $\mathcal{U}_\omega$ projects is invariant with respect to the action of Γ.

4. If the set $\{U\boldsymbol{b} \mid U \in \Gamma\}$ is not orthogonal with respect to the action of U, it can be orthogonalized via (16).

3 General Abelian Groups

We are ready now to work on general abelian groups. Remember that our problem is:

> Given a finite abelian group Γ of unitary transformations of a vector space $\mathcal{V}$ onto itself, find $\boldsymbol{b}$ orthogonal with respect to the action of Γ, that is, such that (4) is satisfied.

We proceed as in Section 2.1. Note that since we are talking about abelian groups, all irreducible representations are one-dimensional (see Appendix A for details).

3.1 Fourier Transform as an Analysis Tool

Consider now the definition of the Fourier transform on a finite[2] abelian group as given in Appendix A. Then, the Fourier transform of the function $\varphi(U) = \langle \boldsymbol{b}, U\boldsymbol{b} \rangle$ is:

$$\Phi(\omega) \;=\; \sum_{U \in \Gamma} \varphi(U)\pi_\omega(U) \;=\; \sum_{U \in \Gamma} \pi_\omega(U)\langle \boldsymbol{b}, U\boldsymbol{b} \rangle \;=\; \langle \boldsymbol{b}, \sum_{U \in \Gamma} U\pi_\omega(U)\boldsymbol{b} \rangle \;=\; |\Gamma|\langle \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b} \rangle \tag{20}$$

where matrices $\mathcal{U}_\omega$ are defined as

$$\mathcal{U}_\omega \;\stackrel{\triangle}{=}\; \frac{1}{|\Gamma|} \sum_{U \in \Gamma} U\pi_\omega(U), \tag{21}$$

and can again be interpreted as the Fourier transforms of matrices $U \in \Gamma$. Let us now find the Fourier transform of δ_U (see (4))

$$\Delta(\omega) \;=\; \sum_{U \in \Gamma} \delta_U \pi_\omega(U) \;=\; \pi_\omega(\mathcal{I}) \;=\; 1, \tag{22}$$

because $\pi_\omega(\mathcal{I}) = 1$ for each ω. Therefore, in the frequency domain, orthogonality condition (4) becomes

$$\Phi(\omega) \;=\; |\Gamma|\langle \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b} \rangle \;=\; 1, \tag{23}$$

for all ω. Equation (23) is the generalization both of (1) and (11); therefore, it can be viewed as an analysis algorithm that permits us to verify if vectors $\{U\boldsymbol{b} \mid U \in \Gamma\}$ form an orthonormal system.

[2] The definition of the Fourier transform is the same for infinite groups; we just stress here that we work with finite ones.

3.2 Orthonormalization with the Fourier Transform

In general, $\Phi(\omega)$ is not equal to 1; however, $\Phi(\omega)$ is always a nonnegative real number (since $\mathcal{U}_\omega$ is an orthogonal projection) . If each $\Phi(\omega)$ is nonzero (we will see in the following the interpretation of $\Phi(\omega)$ equal to zero), we define, analogously to (16)

$$\hat{\boldsymbol{b}} \stackrel{\triangle}{=} \sum_{\omega \in \hat{\Gamma}} \mathcal{U}_\omega \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega)}}. \tag{24}$$

It is possible to show that, because of the group structure of Γ and the orthogonality relations between π_ω, the following property, generalizing (15), holds:

Property 1 *Let Γ be a finite abelian group and let π_ω, with $\omega \in \hat{\Gamma}$ the index set, denote its irreducible representations. Then the matrices defined in (21) are orthogonal projections, that is*

$$\mathcal{U}_\omega \mathcal{U}_{\omega_1} = 0, \qquad \text{if } \omega \neq \omega_1, \quad \mathcal{U}_\omega \mathcal{U}_\omega = \mathcal{U}_\omega, \quad {\mathcal{U}_\omega}^T = \mathcal{U}_\omega. \tag{25}$$

The proof of this property is given in Appendix C. By exploiting (24) and (25), one can write

$$\begin{aligned} \langle \hat{\boldsymbol{b}}, \mathcal{U}_\omega \hat{\boldsymbol{b}} \rangle &= \langle \sum_{\omega_1 \in \hat{\Gamma}} \mathcal{U}_{\omega_1} \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega_1)}}, \sum_{\omega_2 \in \hat{\Gamma}} \mathcal{U}_\omega \mathcal{U}_{\omega_2} \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega_2)}} \rangle, \\ &= \sum_{\omega_1, \omega_2 \in \hat{\Gamma}} \langle \mathcal{U}_{\omega_1} \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega_1)}}, \mathcal{U}_\omega \mathcal{U}_{\omega_2} \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega_2)}} \rangle. \end{aligned} \tag{26}$$

The terms in (26) are the general form of the terms in (18) and as in (18), each term contains the product of $\mathcal{U}_\omega$ with two other matrices $\mathcal{U}_{\omega_1}$ and $\mathcal{U}_{\omega_2}$. As in the previous example, orthogonality relations play a major role in (26). Indeed, because of (25), in (26) only the term for $\omega_1 = \omega_2 = \omega$ remains and by repeating the same reasoning used for (19), (26) becomes

$$\langle \hat{\boldsymbol{b}}, \mathcal{U}_\omega \hat{\boldsymbol{b}} \rangle = \langle \mathcal{U}_\omega \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega)}}, \mathcal{U}_\omega \mathcal{U}_\omega \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega)}} \rangle = \langle \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega)}}, \mathcal{U}_\omega \mathcal{U}_\omega \mathcal{U}_\omega \boldsymbol{b} \frac{1}{\sqrt{\Phi(\omega)}} \rangle = \frac{1}{\Phi(\omega)} \langle \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b} \rangle = \frac{1}{\Phi(\omega)} \Phi(\omega) = 1. \tag{27}$$

We can summarize what has been found so far in the following property:

Property 2 *Let Γ be a finite abelian group of unitary linear transformations acting on a vector space $\mathcal{V}$ with inner product $\langle \cdot, \cdot \rangle$ and let $\boldsymbol{b}$ be a vector of $\mathcal{V}$. The following set:*

$$\{ U\boldsymbol{b} \mid \quad U \in \Gamma \}, \tag{28}$$

is an orthonormal system if and only if

$$|\Gamma| \langle \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b} \rangle = 1, \tag{29}$$

for each ω. Moreover, if (29) is not satisfied, system (28) can be orthonormalized via (24).

The orthogonalization technique presented above has a very interesting property, namely:

Property 3 *If vector* $\boldsymbol{b}$ *is orthogonalized via (24), the resulting vector* $\hat{\boldsymbol{b}}$ *is the vector orthogonal with respect to the action of* Γ *such that* $\|\boldsymbol{b} - \hat{\boldsymbol{b}}\|$ *is minimum.*

Property 3 can be generalized to nonabelian groups (as we will do in [6]). The proof of that more general property (from which, of course, Property 3 descends as a particular case) can be found in Appendix C in [6]. Property 3 and the corresponding one in [6] simplify the design of filters associated with $\boldsymbol{b}$. We will elaborate more on this when designing filters in [6].

3.3 Geometric Interpretation

We now show that the spaces associated with the projections $\mathcal{U}_\omega$ are invariant. Each vector belonging to the space associated with $\mathcal{U}_\omega$ can be expressed as $\mathcal{U}_\omega \boldsymbol{v}$. By applying $V \in \Gamma$ to $\mathcal{U}_\omega \boldsymbol{v}$ one obtains

$$V\mathcal{U}_\omega \boldsymbol{v} \;=\; V\frac{1}{|\Gamma|}\sum_{U\in\Gamma} U\pi_\omega(U)\boldsymbol{v} \;=\; \frac{1}{|\Gamma|}\sum_{U\in\Gamma} VU\pi_\omega(U)\boldsymbol{v}. \tag{30}$$

Let $VU = R$ and rewrite (30) as

$$\begin{aligned} V\mathcal{U}_\omega \boldsymbol{v} \;&=\; \frac{1}{|\Gamma|}\sum_{R\in\Gamma} R\pi_\omega(RV^{-1})\boldsymbol{v} \;=\; \frac{1}{|\Gamma|}\sum_{R\in\Gamma} R\pi_\omega(R)\pi_\omega(V^{-1})\boldsymbol{v}, \\ &=\; \pi_\omega(V)^{-1}\frac{1}{|\Gamma|}\sum_{R\in\Gamma} R\pi_\omega(R)\boldsymbol{v} \;=\; \pi_\omega(V)^{-1}\mathcal{U}_\omega \boldsymbol{v}, \end{aligned} \tag{31}$$

that is, the space associated with $\mathcal{U}_\omega$ is Γ-invariant (since $\pi_\omega(U)$ is just a scalar). With this property we can rephrase (24) as

> To orthogonalize vector $\boldsymbol{b}$ with respect to the action of Γ, project $\boldsymbol{b}$ on the Γ-invariant subspaces (left product with $\mathcal{U}_\omega$), orthogonalize the resulting vectors (product with $1/\sqrt{\Phi(\omega)}$) and recombine them.

Another way to state the same fact is to say that each system that is orthogonal with respect to the action of Γ can be decomposed as the sum of orthonormal systems belonging to the invariant subspaces of Γ. Of course, according to the theory of representations, each of these invariant subspaces corresponds to one of the irreducible representations of Γ.

4 Some Discussions and Extensions

4.1 Comparison with Gram-Schmidt Orthogonalization Procedure

We now look at (24) in a different light. Consider the set of vectors $U\boldsymbol{b}$ as a vector–valued function $\eta(U) \stackrel{\triangle}{=} U\boldsymbol{b}$ defined on Γ. Its Fourier transform is

$$N(\omega) \stackrel{\triangle}{=} \sum_{U\in\Gamma} \eta(U)\pi_\omega(U) = \sum_{U\in\Gamma} U\pi_\omega(U)\boldsymbol{b} = |\Gamma|\mathcal{U}_\omega\boldsymbol{b}. \tag{32}$$

To apply (24) means to multiply signal $N(\omega)$ by $1/(|\Gamma|\sqrt{\Phi(\omega)})$ and then sum over ω. The Fourier transform on groups still retains the property that multiplication in the frequency domain is equivalent to convolution in the temporal one. Therefore, the signal $N(\omega)/(|\Gamma|\sqrt{\Phi(\omega)})$ is the Fourier transform of

$$\hat{\eta}(V) = \sum_{U\in\Gamma} \psi(VU^{-1})\eta(U), \tag{33}$$

where $\psi(U)$ is the inverse Fourier transform of $1/(|\Gamma|\sqrt{\Phi(\omega)})$ (see Appendix A). To obtain $\hat{\boldsymbol{b}}$, we have to compute the sum of $N(\omega)/(|\Gamma|\sqrt{\Phi(\omega)})$. Since this is the inverse Fourier transform for $U = \mathcal{I}$, we are computing

$$\hat{\boldsymbol{b}} = \sum_{\omega\in\hat{\Gamma}} \frac{N(\omega)}{|\Gamma|\sqrt{\Phi(\omega)}} = \hat{\eta}(\mathcal{I}) = \sum_{U\in\Gamma} \psi(U^{-1})\eta(U) = \sum_{U\in\Gamma} \psi(U^{-1})U\boldsymbol{b}. \tag{34}$$

Equation (34) can be read as follows (remember that $\psi(U^{-1})$ is just a scalar):

> The orthogonalized vector, $\hat{\boldsymbol{b}}$, is obtained as a linear combination of the vectors of the original set $\{U\boldsymbol{b} \mid U \in \Gamma\}$.

Moreover, this is true not only for $\hat{\boldsymbol{b}}$; indeed, for each $V\hat{\boldsymbol{b}}$, with $V \in \Gamma$,

$$V\hat{\boldsymbol{b}} = \sum_{U\in\Gamma} \psi(U^{-1})VU\boldsymbol{b} = \sum_{R\in\Gamma} \left(\psi(VR^{-1})\right) R\boldsymbol{b}, \tag{35}$$

that is, *each* $V\hat{\boldsymbol{b}}$ is a linear combination of $\{U\boldsymbol{b} \mid U \in \Gamma\}$. Hence,

Property 4 *The vector space spanned by vectors* $\{U\hat{\boldsymbol{b}} \mid U \in \Gamma\}$ *is equal to the vector space spanned by* $\{U\boldsymbol{b} \mid U \in \Gamma\}$.

Therefore, (34) can be interpreted as a method for orthonormalizing a basis of a vector space. It is interesting to compare (34) with the Gram-Schmidt orthogonalization procedure. Gram-Schmidt is a sequential method; we start by normalizing the first vector and the other ones are orthogonalized with respect to it; then the second vector is normalized and so on. Equation (34) is a parallel method: it acts on all the vectors at once.

4.2 When $\Phi(\omega) = 0$

In Section 3 we saw that to orthonormalize $\boldsymbol{b}$ with respect to the action of Γ it is necessary that $\Phi(\omega) \neq 0$ for each ω. We now give a geometric interpretation of

$$\Phi(\omega) \;=\; |\Gamma|\langle \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b}\rangle \;=\; 0. \tag{36}$$

Because of (25), (36) can be rewritten as

$$|\Gamma|\langle \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b}\rangle \;=\; |\Gamma|\langle \boldsymbol{b}, \mathcal{U}_\omega \mathcal{U}_\omega \boldsymbol{b}\rangle \;=\; |\Gamma|\langle \mathcal{U}_\omega \boldsymbol{b}, \mathcal{U}_\omega \boldsymbol{b}\rangle \;=\; |\Gamma|\|\mathcal{U}_\omega \boldsymbol{b}\| \;=\; 0, \tag{37}$$

which is equivalent to $\mathcal{U}_\omega \boldsymbol{b} = 0$, that is, if $\Phi(\omega) = 0$, then $\boldsymbol{b}$ is orthogonal to the space associated with $\mathcal{U}_\omega$.

In the example from Section 2, if $\boldsymbol{b} = [1, 1]^T$, then it is orthogonal to $[1, -1]^T$ and the component of $\boldsymbol{b}$ with respect to that space cannot be normalized. In other words, if $\boldsymbol{b} = [1, 1]^T$, then $V\boldsymbol{b} = \boldsymbol{b}$ and set $\{\boldsymbol{b}, V\boldsymbol{b}\}$ spans a one-dimensional space that implies (via Property 4) that it cannot be orthogonalized to span a two-dimensional one.

4.3 Extension to Vector Sets

Often the cardinality of Γ is less than the dimension of the vector space[3]. Recall the example from Section 2 and suppose $\mathcal{V} = \mathbb{R}^4$. Then, $\{U\boldsymbol{b} \mid U \in \Gamma\}$ can never be a complete set; however, we can try to find two vectors $\boldsymbol{b}_1$, $\boldsymbol{b}_2$ such that the set

$$\{U\boldsymbol{b}_1, U\boldsymbol{b}_2\} \tag{38}$$

is an orthonormal set (and, in this case, a basis of $\mathbb{R}^4$). By defining

$$\boldsymbol{B} \;\triangleq\; \left[\; \boldsymbol{b}_1 \quad \boldsymbol{b}_2 \;\right], \tag{39}$$

orthonormality of (38) can be rewritten as

$$\boldsymbol{B}^T\boldsymbol{B} \;=\; \boldsymbol{I}, \quad \boldsymbol{B}^T U \boldsymbol{B} \;=\; 0, \qquad U \neq \mathcal{I} \tag{40}$$

or

$$\boldsymbol{B}^T V \boldsymbol{B} \;=\; \boldsymbol{I}\delta_V, \qquad V \in \Gamma. \tag{41}$$

[3] Note that it can never be greater, otherwise $\{U\boldsymbol{b} \mid U \in \Gamma\}$ would have more vectors than the dimension of $\mathcal{V}$ and it could not be orthogonalized.

Similar, we try to find L vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_L$ such that $\{U\boldsymbol{b}_k \mid U \in \Gamma, k = 1, \ldots, L\}$ is an orthonormal set. By defining matrix $\boldsymbol{B} \stackrel{\triangle}{=} [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_L]$ we obtain a new orthogonality condition formally equal to (40). It is possible to repeat all the arguments made in Section 3 by using (40) instead of (4). The main difference encountered is that (20) and (23) become, respectively

$$|\Gamma|\boldsymbol{B}^T\mathcal{U}_\omega\boldsymbol{B} \;=\; \Phi(\omega), \tag{42}$$

and

$$\Phi(\omega) \;=\; \boldsymbol{I}_L, \tag{43}$$

where $\Phi(\omega)$ is a symmetric and positive semi-definite matrix because $\boldsymbol{B}^T\mathcal{U}_\omega\boldsymbol{B} = \boldsymbol{B}^T\mathcal{U}_\omega\mathcal{U}_\omega\boldsymbol{B}$. The symmetry and the positive semi-definiteness of $\Phi(\omega)$ imply that such a matrix can always be decomposed, via singular value decomposition, as

$$\Phi(\omega) = \Psi(\omega)^T\mathcal{S}(\omega)^2\Psi(\omega), \tag{44}$$

where, for each ω, $\Psi(\omega)$ is a unitary matrix and $\mathcal{S}(\omega)$ is a diagonal matrix with nonnegative values on the diagonal.

If $\Phi(\omega)$ has full rank (the interpretation of this condition not being true is similar to $\Phi(\omega) = 0$), $\mathcal{S}(\omega)$ is an invertible matrix, that is, it has only positive values on its main diagonal. If (43) is not true and $\Phi(\omega)$ has full rank, matrix $\boldsymbol{B}$ can be normalized as

$$\hat{\boldsymbol{B}} \;\stackrel{\triangle}{=}\; \sum_{\omega\in\hat{\Gamma}} \mathcal{U}_\omega\boldsymbol{B}\;\Psi(\omega)^T\mathcal{S}(\omega)^{-1}\Psi(\omega), \tag{45}$$

where $\Psi(\omega)^T\mathcal{S}(\omega)^{-1}\Psi(\omega)$ plays the role of $1/\sqrt{\Phi(\omega)}$. Similarity to (45) with (24) is clear.

These considerations work for $\mathcal{V} = \mathbb{R}^N$ and with the scalar product defined as $\langle \boldsymbol{v}_1, \boldsymbol{v}_2\rangle \stackrel{\triangle}{=} \boldsymbol{v}_1{}^T\boldsymbol{v}_2$. It is possible to generalize them (for example, $\mathcal{V} = L^2(\mathbb{R})$, that does not have finite dimension) by replacing matrix $\boldsymbol{B}$ with the concept of a vector set. The reason for introducing matrix $\boldsymbol{B}$ in (39) was to keep together the two vectors $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ to work previously on both. Therefore, in (39) there is nothing that says that $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ belong to $\mathbb{R}^N$; they could be, for example, two functions of $L^2(\mathbb{R})$.

Of course, if $\boldsymbol{B}$ is not a matrix, conditions (40) do not make sense, unless we define a product between vector sets. To do so, observe that the matrix product $\mathbf{B}^T\mathbf{C}$ can be interpreted as the matrix having in position (i, j)

the scalar products between the ith column of $\mathbf{B}$ and the jth column of $\mathbf{C}$. Then we define $\{\mathbf{B}, \mathbf{C}\}$ as a matrix having in position (i, j) the scalar product $\langle \boldsymbol{b}_i, \boldsymbol{c}_j \rangle$:

$$(\boldsymbol{B}, \boldsymbol{C})_{i,j} \stackrel{\triangle}{=} \langle \boldsymbol{b}_i, \boldsymbol{c}_j \rangle. \tag{46}$$

Moreover, it is possible to define a left product between a linear transformation and a vector set and a right product between a vector set and a matrix. Such definitions are compatible with the matrix interpretation and enjoy some intuitive properties listed, with all details, in Appendix B.

With this notation, all arguments in this section still hold when they are interpreted in the vector set sense. All these extensions can be summarized in the following property, extension of Property 2:

Property 5 *Let Γ be an abelian group of unitary linear transformations acting on a vector space $\mathcal{V}$ with inner product $\langle \cdot, \cdot \rangle$ and let $\boldsymbol{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_L\}$ be a set of vectors of $\mathcal{V}$. The set*

$$\{U\boldsymbol{b}_k \mid \quad U \in \Gamma,\ k = 1, \ldots, L\} \tag{47}$$

is an orthonormal system if and only if

$$\Phi(\omega) \ = \ |\Gamma| \langle \boldsymbol{B}, \mathcal{U}_\omega \boldsymbol{B} \rangle = \boldsymbol{I}_L, \tag{48}$$

for each ω. Moreover, if (48) is not satisfied, system (47) can be orthonormalized via (44) and (45), assuming each $\Phi(\omega)$ has full rank.

5 Fast Algorithm

The intrinsic structure of set $\mathcal{B} \stackrel{\triangle}{=} \{U\boldsymbol{b} \mid U \in \Gamma\}$, that is, the fact that all the vectors are obtained from a prototype filter, allows for the existence of a fast algorithm. Indeed, the fast algorithm does not require the orthogonality of $\mathcal{B}$ (its elements can also be linearly dependent); the only structure required is that vectors in $\mathcal{B}$ are obtained by applying transformations from Γ to $\boldsymbol{b}$.

We want to compute

$$\boldsymbol{c}^T U \boldsymbol{b}, \qquad U \in \Gamma, \tag{49}$$

and we know that we can always find a matrix $\boldsymbol{A}$ such that $\boldsymbol{A}^{-1} U \boldsymbol{A}$ is diagonal for each $U \in \Gamma$ and the elements on the diagonal are complex numbers on the unitary circle. We can always permute the rows and columns of

$\boldsymbol{A}^{-1}U\boldsymbol{A}$ in order to obtain

$$\boldsymbol{A}^{-1}U\boldsymbol{A} = \begin{bmatrix} \alpha_1\boldsymbol{I}_{\mu_1} & & & \\ & \alpha_2\boldsymbol{I}_{\mu_2} & & \\ & & \ddots & \\ & & & \alpha_N\boldsymbol{I}_{\mu_N} \end{bmatrix}. \tag{50}$$

By changing the basis with $\boldsymbol{A}$ in (49) and partitioning

$$\hat{\boldsymbol{c}} \triangleq \boldsymbol{A}\boldsymbol{c}, \quad \hat{\boldsymbol{b}} \triangleq \boldsymbol{A}\boldsymbol{b}, \tag{51}$$

according to (50), (49) can be written as

$$\sum_{n=0}^{N} \hat{\boldsymbol{c}}_n^T \hat{\boldsymbol{b}}_n {\alpha_n}^k. \tag{52}$$

If we can find a fast algorithm to compute the product with $\boldsymbol{A}$ and the sum in (52), that algorithm is the fast algorithm for the computation of (49).

A Representations, Characters and Fourier Analysis on Groups

This section aims at providing a self-contained introduction into the subject of group representations, characters and Fourier analysis on finite groups. No prior background is required except for elementary concepts on vector spaces. We particularly stress results that are used in our current work.

Classical Fourier analysis considers the real line, the integers and the unit circle. In the last half-century, many mathematicians have felt that a more concise presentation of Fourier analysis is possible if one considers a more general setting; that is, locally compact groups. This allows one to use the tools with which we are very familiar while working on groups. Here we define just the necessary concepts that allow us to use the Fourier transform on the types of groups we are considering. For a more detailed and rigorous mathematical treatment, see the texts by Folland [8] and Rudin [9].

The definition of Fourier transform on groups is based on certain group-theoretic concepts, such as representations and characters. We begin this section by introducing the concept of a representation, followed by a summary of the basic representation and Fourier theory on finite abelian groups. To do the same with nonabelian groups, we need to introduce the concept of a character; this is done in Section A.3 followed by the Fourier formulae for nonabelian groups. This presentation is based mostly on the excellent text by Jean-Pierre Serre [7].

A.1 Basic Facts on Representations

Let Γ be a group, $\mathcal{V}$ a vector space over the field $\mathbb{C}$ and $\mathrm{GL}(\mathcal{V})$ the group of nonsingular linear transformations a from $\mathcal{V}$ into $\mathcal{V}$. A *representation* π of Γ is a homomorphic mapping of Γ to $\mathrm{GL}(\mathcal{V})$. When $\mathcal{V}$ is of dimension n, each linear transformation $a : \mathcal{V} \rightarrow \mathcal{V}$ can be represented by a square matrix of order n, whose elements a_{ij} are complex numbers and are given by $a_{ij} = \langle a(e_j), e_i \rangle$ [10], e_i, $i = 1, \ldots, n$ being a basis for $\mathcal{V}$. Thus, the group $\mathrm{GL}(\mathcal{V})$ is the group of invertible square matrices of order n. This also means that the representation $\pi(U)$ is a square matrix of order n. The dimension n is also called the *degree of the representation*. If we are given two representations π and π' of the same group, we say that they are isomorphic if there exists an invertible matrix T such that $T\pi(U) = \pi'(U)T$, for all $U \in \Gamma$.

Digressing for a moment, recall that a subspace W of $\mathcal{V}$ is called *invariant* under the action of Γ (Γ-*invariant*), if for every $x \in W$, $\pi(U)x$ belongs to W as well. Then we can define a *subrepresentation* as the restriction of π onto W and call it π^W.

Theorem A.1 *Let $\pi : \Gamma \rightarrow GL(\mathcal{V})$ be a linear representation of Γ in $\mathcal{V}$ and let W be a vector subspace of $\mathcal{V}$ invariant under Γ. Then there exists an orthogonal complement W^0 of W in $\mathcal{V}$ which is invariant under Γ.*

If we restrict π to W and W^0 respectively, then these restrictions define subrepresentations on W and W^0, and determine the representation for $\mathcal{V}$ as well. In other words, if π^W and π^{W^0} are representations for W and W^0, respectively, then the following is called their *direct sum*

$$\pi(U) \;=\; \begin{pmatrix} \pi^W & 0 \\ 0 & \pi^{W^0} \end{pmatrix}.$$

We say that a representation is *irreducible* if $\mathcal{V}$ is not 0 and no other subspace of $\mathcal{V}$ is invariant under Γ (except 0 and $\mathcal{V}$). By Theorem A.1, this also means that the representation π of $\mathcal{V}$ is not a direct sum of two representations. We now have the following result:

Theorem A.2 *Every representation is a direct sum of irreducible representations.*

Together with the direct sum operation, we can define a *tensor product* (also called *Kronecker product*) of given representations as the tensor product of corresponding matrices, that is, $\pi(U) \;=\; \pi^1(U) \otimes \pi^2(U)$.

As examples of representations, consider:

- A representation of degree 1 (scalar), that is, a mapping $\pi : \Gamma \rightarrow \mathbb{C}^*$. Here, all $\pi(U)$ are roots of unity (since every element of Γ has finite order); in particular, $|\pi(U)| = 1$. In section on abelian groups, we will see that all irreducible representations of such groups are scalars.

- If $\pi(U) = 1$, for all $U \in \Gamma$, then such a π is called a *unit* or *trivial* representation.

- Another interesting representation is called *regular* and is obtained if $\mathcal{V}$ is of dimension g where $g = |\Gamma|$ is the order of the group Γ by defining a map $\pi(U) : e_V \rightarrow e_{UV}$, where (e_U) is a basis of $\mathcal{V}$ indexed by the elements of Γ.

A.2 Facts on Representations and Fourier Theory on Finite Abelian Groups

Since we do not yet have the machinery in place to derive the important results on representation on abelian groups, we just summarize them here. The interested reader is urged to read the section on characters and nonabelian groups to see how these results are actually derived.

Theorem A.3 *The following properties are equivalent:*

1. Γ *is abelian.*

2. *All the irreducible representations of* Γ *have degree* 1 *(that is, they are scalars).*

The following is true as well:

- $\overline{\pi_\omega(U)} = 1/\pi_\omega(U) = \pi_\omega(U^{-1})$.

- If Γ is isomorphic to $\mathbb{Z}/N\mathbb{Z}$, then its representations are $\pi_k(n) = e^{j\,2\pi\frac{kn}{N}}, n \in \mathbb{Z}/N\mathbb{Z}, k \in \mathbb{Z}/N\mathbb{Z}$.

Note that the current choice for ω is so that it resembles the Fourier-type formulae. Moreover, representations of abelian groups satisfy the following orthogonality relations:

$$\sum_{U \in \Gamma} \pi_\omega(U)\overline{\pi_{\omega_1}(U)} \;=\; |\Gamma|\;\delta_{\omega,\omega_1}. \tag{53}$$

This is a consequence of Theorem A.4, presented later in this section.

We now give the definition of the Fourier transform on finite abelian groups. Note that these definitions are "operational", that is, we just write what we need to use. For a rigorous mathematical treatment, see the text by Folland [8].

If Γ is an abelian group, we know that all of its representations are scalars. Then, the Fourier transform of a function $h(U)$, defined on Γ, is a function H defined on the set of irreducible representations of Γ, with the index being in $\hat{\Gamma}$. Such a function should be denoted as $H(\pi_\omega)$, but, in order to avoid cumbersome notation, we shorten it to $H(\omega)$. Function $H(\omega)$ is [8]:

$$H(\omega) \;=\; \sum_{U\in\Gamma} h(U)\pi_\omega(U). \tag{54}$$

As an example, consider $\Gamma = \mathbb{Z}/N\mathbb{Z}$; then each representation can be expressed as

$$\pi_k(n) \;=\; e^{j\,2\pi\frac{nk}{N}}, \quad k = 0,\ldots,N-1, \tag{55}$$

where $n \in \mathbb{Z}/N\mathbb{Z}$. Expression (54) becomes

$$H[k] \;=\; \sum_{n\in\mathbb{Z}/N\mathbb{Z}} h[n]e^{j\,2\pi\frac{nk}{N}} \;=\; \sum_{n=0}^{N-1} h[n]e^{j\,2\pi\frac{nk}{N}}, \quad k = 0,\ldots,N-1, \tag{56}$$

that is, the usual discrete-time Fourier series on N points.

A.3 Basic Facts on Characters

We now proceed onto the concept of a character, which, as we will see, reduces the study of representations to the study of their characters. A *character* of the representation $\pi(U)$ is given by

$$\chi_\pi(U) \;=\; \mathrm{Tr}(\pi(U)), \tag{57}$$

where $\mathrm{Tr}(\pi(U))$ denotes the trace of the matrix $\pi(U)$, that is, the sum of its diagonal elements (or its eigenvalues). The following hold for a character of a representation of degree n:

$$\chi(1) \;=\; n, \tag{58}$$

$$\chi(U^{-1}) \;=\; \overline{\chi(U)}, \qquad U \in \Gamma, \tag{59}$$

$$\chi(VUV^{-1}) \;=\; \chi(U), \qquad U, V, \in \Gamma. \tag{60}$$

If we are given two representations of the same group with two characters χ_1 and χ_2, then

1. The character χ of the direct sum representation $\mathcal{V}_1 \oplus \mathcal{V}_2$ is given by $\chi_1 + \chi_2$.

2. The character χ of the tensor product representation $\mathcal{V}_1 \otimes \mathcal{V}_2$ is given by $\chi_1 \cdot \chi_2$.

The following lemma, called *Schur's lemma*, is used (among other things) to find orthogonality relations between representations as well as characters.

Lemma A.1 (Schur) *Let π^1 and π^2 be two irreducible representations of the same group Γ, and let f be a linear mapping of $\mathcal{V}_1$ into $\mathcal{V}_2$ such that $\pi^2(U)f = f\pi^1(U)$, for all $U \in \Gamma$. Then:*

1. *If π^1 and π^2 are not isomorphic, we have $f = 0$.*

2. *If $\mathcal{V}_1 = \mathcal{V}_2$ and $\pi^1 = \pi^2$, f is a multiple of the identity.*

If we write π^k in matrix form given by its elements $\pi^k_{i_k,j_k}$, as a result of the previous lemma, we have that:

1. When π^1 and π^2 are not isomorphic,

$$\frac{1}{g}\sum_{U\in\Gamma} \pi^2_{i_2,j_2}(U^{-1})\pi^1_{j_1,i_1}(U) \;=\; 0.$$

2. When $\mathcal{V}_1 = \mathcal{V}_2$ and $\pi^1 = \pi^2$,

$$\frac{1}{g}\sum_{U\in\Gamma} \pi^2_{i_2,j_2}(U^{-1})\pi^1_{i_1,j_1}(U) \;=\; \frac{1}{n}\delta_{i_2 i_1}\delta_{j_2 j_1} \;=\; \begin{cases} 1/n & \text{if } \; i_1 = i_2 \text{ and } \; j_1 = j_2, \\ 0 & \text{otherwise.} \end{cases}$$

If ϕ and ψ are functions on Γ, then we can define

$$\langle \phi, \psi \rangle \;=\; \frac{1}{g}\sum_{U\in\Gamma} \phi(U^{-1})\psi(U) \;=\; \frac{1}{g}\sum_{U\in\Gamma} \psi(U^{-1})\phi(U). \tag{61}$$

Then we can restate the previous two facts as

1. When π^1 and π^2 are not isomorphic,

$$\langle \pi^2_{i_2,j_2}, \pi^1_{j_1,i_1} \rangle \;=\; 0.$$

2. When $\mathcal{V}_1 = \mathcal{V}_2$ and $\pi^1 = \pi^2$,

$$\langle \pi^2_{i_2,j_2}, \pi^1_{j_1,i_1} \rangle \;=\; \frac{1}{n}\delta_{i_2 i_1}\delta_{j_2 j_1}.$$

If ϕ and ψ are two complex-valued functions on Γ, then define

$$(\phi|\psi) \;=\; \frac{1}{g}\sum_{U\in\Gamma} \phi(U)\overline{\psi(U)},$$

which is a scalar product. In particular, if χ is a character of a representation, then $\langle \phi, \chi \rangle = (\phi|\chi)$, for all functions ϕ on Γ. We then have

Theorem A.4 *The following are true:*

1. *If χ is the character of an irreducible representation, we have that $(\chi|\chi) = 1$ (that is, χ is of norm 1).*

2. *If χ and χ' are the characters of two nonisomorphic irreducible representations, we have $(\chi|\chi') = 0$ (that is, they are orthogonal).*

For abelian groups, the above theorem leads to the orthogonality of representations as well characters. This is true since any representation of an abelian group is a scalar, and thus equal to its character. This result was given in Section A.2.

We now present a few results that reduce the study of representations to that of their characters. In particular

Theorem A.5 *Let $\mathcal{V}$ be a linear representation[4] of Γ, with character ϕ, and suppose $\mathcal{V}$ decomposes into a direct sum of irreducible representations:*

$$\mathcal{V} \;=\; W_1 \oplus \cdots \oplus W_k.$$

Then, if W is an irreducible representation with character χ, the number of W_i isomorphic to W is equal to the scalar product $(\phi|\chi) = \langle \phi, \chi \rangle$.

Corollary 1 *The number of W_i isomorphic to W does not depend on the chosen decomposition.*

Corollary 2 *Two representations with the same character are isomorphic.*

If $\chi_1, \ldots, \chi_k$ are the distinct irreducible characters of Γ, and if $W_1, \ldots W_k$ denote the corresponding representations, then each representation $\mathcal{V}$ is isomorphic to a direct sum

$$\mathcal{V} \;=\; m_1 W_1 \oplus \cdots \oplus m_k W_k, \qquad m_i \geq 0, m_i \in \mathbb{Z}.$$

The character ϕ of $\mathcal{V}$ is equal to

$$\phi \;=\; m_1\chi_1 + \ldots + m_k\chi_k, \quad \text{with } m_i = (\phi|\chi_i). \tag{62}$$

Moreover, the orthogonality conditions among characters imply that

$$(\phi|\phi) \;=\; \sum_{i=1}^{k} m_i^2. \tag{63}$$

This leads us to the following theorem:

Theorem A.6 *If ϕ is a character of a representation $\mathcal{V}$, $(\phi|\phi)$ is a positive integer and we have $(\phi|\phi) = 1$ if and only if $\mathcal{V}$ is irreducible.*

[4] Note that by abuse of language, we call $\mathcal{V}$ the linear representation of Γ, although it should properly be called representation space of Γ.

This theorem gives us an irreducibility criterion that is fairly easy to verify. Let us now turn to the regular representation we introduced earlier which is useful in determining the irreducible representations of a group Γ.

Proposition A.1 *The character r_Γ of the regular representation is given by the formulae:*

$$\begin{aligned} r_\Gamma(U) &= g, \quad \text{for } U = 1, \\ r_\Gamma(U) &= 0, \quad \text{for } U \neq 1. \end{aligned}$$

Corollary 3 *Every irreducible representation W_i is contained in the regular representation with multiplicity equal to its degree n_i.*

Corollary 4 *The following are true:*

1. *The degrees n_i satisfy the relation $\sum_{i=1}^k n_i^2 = g$.*
2. *If $U \in \Gamma$ is different from 1, we have $\sum_{i=1}^k n_i \chi_i(U) = 0$.*

From these results we can see that for nonisomorphic irreducible representations to be irreducible representations of Γ, it is necessary and sufficient that $n_1^2 + \ldots + n_k^2 = g$.

We digress for a moment here and introduce the concept of classes. A function f on Γ satisfying (60), or $f(UV) = f(VU)$ is called a *class function*. Two elements U and U' of Γ are said to be *conjugate* if there exists $V \in \Gamma$ such that $U' = VUV^{-1}$. Since this is an equivalence relation, it partitions Γ into *classes* (or *conjugacy classes*). For example, for abelian groups, each conjugacy class of Γ consists of a single element. Moreover, each function on Γ is a class function. This leads us to the proof of Theorem A.3 if we remember that the degree of the group is the sum of squares of degrees of its distinct irreducible representations, and there are as many as there are classes in the group. However, since we know that each class in this case consists of a single element, then the degree of the group is equal to the number of classes if and only if each degree of an irreducible representation is equal to 1. As a consequence, each irreducible representation in an abelian group is a complex number with unit modulus. Also as a consequence, there are $|\Gamma|$ irreducible representations. These results also imply the bulleted facts in Section A.2.

Now call H the space of class functions on Γ. Then

Theorem A.7 *The irreducible characters $\chi_1, \ldots, \chi_k$ form an orthonormal basis for H.*

Theorem A.8 *The number of irreducible representations of* Γ *(up to isomorphism) is equal to the number of classes of* Γ.

The previous results help us determine the number of irreducible representations.

Finally, we turn to a canonical decomposition of a representation, which is the only unique decomposition (however, it is "coarser" than the decomposition into irreducible representations). Let $\chi_1, \ldots, \chi_k$ be the distinct characters of the irreducible representations $W_1, \ldots, W_k$ of Γ and $n_1, \ldots, n_k$ their degrees. What we do is decompose $\mathcal{V}$ into its irreducible representations and then gather all those that are isomorphic into a single one, that is $\mathcal{V} = \mathcal{V}_1 \oplus \ldots \oplus \mathcal{V}_k$. Then

Theorem A.9 *The following are true:*

1. *The decomposition* $\mathcal{V} = \mathcal{V}_1 \oplus \ldots \oplus \mathcal{V}_k$ *does not depend on the initially chosen decomposition of* $\mathcal{V}$ *into irreducible representations.*

2. *The projection* p_i *of* $\mathcal{V}$ *onto* $\mathcal{V}_i$ *associated with this decomposition is given by the formula:*

$$p_i = \frac{n_i}{g} \sum_{U \in \Gamma} \overline{\chi_i(U)} \pi(U). \tag{64}$$

This gives us the tools for decomposing $\mathcal{V}$ into its representations. First, one finds a canonical decomposition with the help of projections p_i. Then, one decomposes each $\mathcal{V}_i$ into a direct sum of isomorphic W_i as $\mathcal{V}_i = W_i \oplus \cdots \oplus W_i$, which can be done in infinitely many ways.

A.4 Fourier Analysis on Nonabelian Groups

If the group is not abelian, an irreducible representation, in general, maps an element $U \in \Gamma$ into a matrix $\pi_\omega(U)$; we denote the element (i, j) of the matrix $\pi_\omega(U)$ as $\pi_\omega^{ij}(U)$. Because of this, the Fourier transform becomes a function with three indices

$$\Phi(\omega, i, j) \stackrel{\triangle}{=} \sum_{U \in \Gamma} \varphi(U) \pi_\omega^{ij}(U), \tag{65}$$

where ω determines the representation and i and j are the row and column indices of $\pi_\omega^{ij}(U)$[5]. The inverse Fourier transform is

$$\varphi(U) \triangleq \frac{|\hat{\Gamma}|}{|\Gamma|} \sum_{\omega,i,j} \overline{\pi_\omega^{ij}(U)} \Phi(\omega,i,j). \tag{66}$$

B Vector Sets and their Properties

In Section 4 we introduced the concept of vector set in order to be able to orthogonalize more than one vector with respect to the action of a group Γ, even when the vectors belong to a vector space of infinite dimension. In this section we give the formal definitions and properties that are necessary to obtain Property 5 with vector sets. Let us start with the following definitions:

Definition 2 *A* vector set *of dimension $N < \infty$ is an ordered N-tuple of vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N$ belonging to a given vector space $\mathcal{V}$. The following operations are defined on vector sets:*

- *If $\boldsymbol{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N]$ and $\boldsymbol{C} = [\boldsymbol{c}_1, \ldots, \boldsymbol{c}_N]$ are two vector sets, their sum is defined as*

$$\boldsymbol{B} + \boldsymbol{C} \triangleq [\boldsymbol{b}_1 + \boldsymbol{c}_1, \ldots, \boldsymbol{b}_N + \boldsymbol{c}_N]. \tag{67}$$

- *The product of $\boldsymbol{B}$ by a scalar α is*

$$\alpha \boldsymbol{B} \triangleq [\alpha \boldsymbol{b}_1, \ldots, \alpha \boldsymbol{b}_N]. \tag{68}$$

- *If $\boldsymbol{B}$ and $\boldsymbol{C}$ are vector sets of dimension N, we denote as $\{\boldsymbol{B}, \boldsymbol{C}\}$ a matrix whose element (i,j) is*

$$\langle \boldsymbol{b}_i, \boldsymbol{c}_j \rangle \tag{69}$$

Now we want to define, as anticipated in Section 3, a left product by a linear transformation and a right product by a matrix, in such a way that generalizes of the usual matrix product. The definition of the left product with a linear transformation is straightforward:

Definition 3 *If $\boldsymbol{B}$ is a vector set and $\boldsymbol{K}$ is a linear transformation on a vector space $\mathcal{V}$, then $\boldsymbol{KB}$ is defined as*

$$\boldsymbol{KB} = [\boldsymbol{K}\boldsymbol{b}_1, \ldots, \boldsymbol{K}\boldsymbol{b}_N]. \tag{70}$$

[5] A convenient way to visualize (65) is to think that the matrices $\pi_\omega(U)$ are arranged as in Figure 2(a). Matrices $\pi_\omega(U)$ of the same representation ω are clustered together and lined up according to $U \in \Gamma$. The values $\pi_\omega^{ij}(U)$ can be found along a ray penetrating a single cluster of matrices. Analogously, function $\varphi(U)$ can be seen as a set of values arranged parallel to the "group axis", as displayed in Figure 2(b). Computation of (65) corresponds to taking the inner products between $\varphi(U)$ and "rays" $\pi_\omega^{ij}(U)$; the result is a set of numbers shown in Figure 2(c), arranged like the matrices, but in only one plane.

Instead, to define a right product with a matrix observe that the matrix product $\boldsymbol{EF}$ can be interpreted both as the linear transformation represented by $\boldsymbol{E}$ acting on the columns of $\boldsymbol{F}$ and as the operation of taking linear combinations of the columns of $\boldsymbol{E}$, with coefficients taken from the columns of $\boldsymbol{F}$. According to this last interpretation we give the following definition:

Definition 4 *If $\boldsymbol{B}$ is a vector set of dimension N and $\boldsymbol{A}$ is an $N \times M$ matrix with entries $\mathbf{A}_{ij}$, then $\boldsymbol{BA}$ is defined as (that is, it is a vector set of dimension M):*

$$\boldsymbol{BA} \stackrel{\triangle}{=} [\sum_{i=1}^{N} \boldsymbol{b}_i \mathbf{A}_{i1}, \ldots, \sum_{i=1}^{N} \boldsymbol{b}_i \mathbf{A}_{iM}] \tag{71}$$

Here we give some properties of operations on vector sets used in this work:

Property 6 *In what follows $\boldsymbol{C}$, $\boldsymbol{D}$, $\boldsymbol{B}$ are vector sets of the same dimension, $\boldsymbol{K}$ is a linear transformation on $\mathcal{V}$, $\boldsymbol{K}^*$ is its adjoint and $\boldsymbol{A}$ is a matrix.*

$$\{\boldsymbol{C}, \boldsymbol{D}\} = \{\boldsymbol{D}, \boldsymbol{C}\}^T, \tag{72}$$

$$\{\boldsymbol{C} + \boldsymbol{D}, \boldsymbol{B}\} = \{\boldsymbol{C}, \boldsymbol{B}\} + \{\boldsymbol{D}, \boldsymbol{B}\}, \tag{73}$$

$$\{\alpha \boldsymbol{C}, \boldsymbol{D}\} = \alpha\{\boldsymbol{C}, \boldsymbol{D}\}, \tag{74}$$

$$\{\boldsymbol{KC}, \boldsymbol{D}\} = \{\boldsymbol{C}, \boldsymbol{K}^* \boldsymbol{D}\}, \tag{75}$$

$$\{\boldsymbol{C}, \boldsymbol{DA}\} = \{\boldsymbol{C}, \boldsymbol{D}\}\boldsymbol{A}. \tag{76}$$

An easy way of remembering and using these properties is to think that when $\boldsymbol{B}$ and $\boldsymbol{C}$ are matrices then $\{\boldsymbol{B}, \boldsymbol{C}\} = \boldsymbol{B}^T \boldsymbol{C}$. Then, equalities in Property 6 follow from the usual matrix properties.

Corollary 5 *If $\boldsymbol{C}$, $\boldsymbol{D}$ are vector sets, $\boldsymbol{K}_1$ and $\boldsymbol{K}_2$ linear transformations and $\boldsymbol{E}$, $\boldsymbol{F}$ matrices, then*

$$\{\boldsymbol{K}_1 \boldsymbol{CE}, \boldsymbol{K}_2 \boldsymbol{DF}\} = \boldsymbol{E}^T \{\boldsymbol{C}, \boldsymbol{K}_1{}^* \boldsymbol{K}_2 \boldsymbol{D}\} \boldsymbol{F}. \tag{77}$$

Proof: It follows by applying (72), (75) and (76). ■

Observe that if $\mathcal{V}$ has finite dimension, each vector set can be identified with the corresponding matrix and (72) to (77) can be rewritten in a more familiar form. For example, (77) becomes

$$\{\boldsymbol{K}_1 \boldsymbol{CE}, \boldsymbol{K}_2 \boldsymbol{DF}\} = (\boldsymbol{K}_1 \boldsymbol{CE})^T (\boldsymbol{K}_2 \boldsymbol{DF}) = \left(\boldsymbol{E}^T \boldsymbol{C}^T \boldsymbol{K}_1{}^T \boldsymbol{K}_2 \boldsymbol{DF}\right) = \boldsymbol{E}^T \{\boldsymbol{C}, \boldsymbol{K}_1{}^T \boldsymbol{K}_2 \boldsymbol{D}\} \boldsymbol{F}. \tag{78}$$

Finally, let us introduce a norm for vector sets. The most natural norm for a set of vectors is the sum of the norms of individual vectors. More precisely,

Definition 5 *The norm of a vector set* $\boldsymbol{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N]$ *is defined as*

$$\|\boldsymbol{B}\| \stackrel{\triangle}{=} \sqrt{\sum_{k=1}^{N} \|\boldsymbol{b}_k\|^2} = \sqrt{\sum_{k=1}^{N} \langle \boldsymbol{b}_k, \boldsymbol{b}_k \rangle}. \tag{79}$$

It is worth noting that the scalar products in (79) can be found on the diagonal of the matrix $\{\boldsymbol{B}, \boldsymbol{B}\}$, that is, (79) can be rewritten as

$$\|\boldsymbol{B}\|^2 = \mathrm{Tr}(\{\boldsymbol{B}, \boldsymbol{B}\}). \tag{80}$$

Equation (80) resembles the definition of the Frobenius matrix norm. Moreover, it suggests that norm (79) could possibly be expressed using $\{\cdot, \cdot\}$; such a hypothesis is supported by the fact that $\mathrm{Tr}(\boldsymbol{A}^T \boldsymbol{E})$ is a scalar product between matrices. Indeed,

$$\langle\langle \boldsymbol{B}, \boldsymbol{C} \rangle\rangle \stackrel{\triangle}{=} \mathrm{Tr}(\{\boldsymbol{B}, \boldsymbol{C}\}) \tag{81}$$

is a scalar product between vector sets, that is, the usual properties valid for scalar products hold here as well:

$$\begin{aligned}
\langle\langle \boldsymbol{B} + \boldsymbol{C}, \boldsymbol{D} \rangle\rangle &= \langle\langle \boldsymbol{B}, \boldsymbol{D} \rangle\rangle + \langle\langle \boldsymbol{C}, \boldsymbol{D} \rangle\rangle, \\
\langle\langle \boldsymbol{B}, \alpha \boldsymbol{C} \rangle\rangle &= \alpha \langle\langle \boldsymbol{B}, \boldsymbol{C} \rangle\rangle, \\
\langle\langle \boldsymbol{B}, \boldsymbol{C} \rangle\rangle &= \overline{\langle\langle \boldsymbol{C}, \boldsymbol{B} \rangle\rangle}, \\
\langle\langle \boldsymbol{B}, \boldsymbol{B} \rangle\rangle &\geq 0, \\
\langle\langle \boldsymbol{B}, \boldsymbol{B} \rangle\rangle &= 0 \Leftrightarrow \boldsymbol{B} = 0.
\end{aligned} \tag{82}$$

Such properties are readily proved from the definition and Property 6.

Note that with the operations defined in Definition 2 and scalar product $\langle\langle \cdot, \cdot \rangle\rangle$, the class of vector sets is a vector space with inner product inducing norm (79). This has two important consequences:

1. All the usual theorems on vector spaces with inner product apply also to vector sets. For example, Cauchy-Schwarz inequality, Pythagorean theorem, triangle inequality, and so on. In the following, for example, we use the Pythagorean theorem, that is

$$\|\boldsymbol{B} + \boldsymbol{C}\|^2 = \|\boldsymbol{B}\|^2 + \|\boldsymbol{C}\|^2 \Leftrightarrow \langle\langle \boldsymbol{B}, \boldsymbol{C} \rangle\rangle = 0. \tag{83}$$

2. Since vector sets are vectors with an inner product, one can define also sets of vector sets and sets of sets of vector sets, and so on. However, such a possibility is not used in this work.

Finally, we present a property of vector sets that is similar to the singular value decomposition (SVD) of matrices and that is instrumental in proving certain properties in Part II of this work [6].

Property 7 (Singular value decomposition for vector sets) *Let $\boldsymbol{B}$ a vector set of length N. Suppose that the matrix $\{\boldsymbol{B},\boldsymbol{B}\}$ has full rank. Then $\boldsymbol{B}$ can be written as*

$$\boldsymbol{B} \;=\; \boldsymbol{CSO} \tag{84}$$

where $\boldsymbol{S}$ and $\boldsymbol{O}$ are $N \times N$ matrices, the former diagonal with positive elements, the latter orthogonal, and $\boldsymbol{C}$ a vector set such that

$$\{\boldsymbol{C},\boldsymbol{C}\} \;=\; \boldsymbol{I}. \tag{85}$$

The similarity with SVD is clear; here $\boldsymbol{C}$ plays the role of the left orthogonal matrix in SVD. Note that (85), when written in matrix form, becomes the usual condition for the orthogonality of a matrix.

Proof: Since $\{\boldsymbol{B},\boldsymbol{B}\}$ is invertible, it is positive definite and can be decomposed as

$$\{\boldsymbol{B},\boldsymbol{B}\} \;=\; \boldsymbol{O}^T\boldsymbol{S}^2\boldsymbol{O} \tag{86}$$

with $\boldsymbol{S}$ a diagonal matrix and $\boldsymbol{O}$ an orthogonal matrix. We can choose $\boldsymbol{S}$ having only positive values on the main diagonal. By defining the vector set $\boldsymbol{C} \stackrel{\triangle}{=} \boldsymbol{B}\boldsymbol{O}^T\boldsymbol{S}^{-1}$ we see that $\boldsymbol{B} \;=\; \boldsymbol{CSO}$ is the wanted decomposition of $\boldsymbol{B}$. One needs only to verify that $\boldsymbol{C}$ satisfies (85). Indeed,

$$\begin{aligned}\{\boldsymbol{C},\boldsymbol{C}\} \;&=\; \{\boldsymbol{B}\boldsymbol{O}^T\boldsymbol{S}^{-1},\boldsymbol{B}\boldsymbol{O}^T\boldsymbol{S}^{-1}\}\\ &=\; \boldsymbol{S}^{-T}\boldsymbol{O}\{\boldsymbol{B},\boldsymbol{B}\}\boldsymbol{O}^T\boldsymbol{S}^{-1}\\ &=\; (\boldsymbol{S}^{-T}\boldsymbol{O})\,(\boldsymbol{O}^T\boldsymbol{S}^2\boldsymbol{O})\,(\boldsymbol{O}^T\boldsymbol{S}^{-1}) \;=\; \boldsymbol{I}\end{aligned} \tag{87}$$

■

The SVD for vector sets is introduced because of an important property that is used in the following, and generalizes its matrix counterpart.

Property 8 *With the hypothesis of Property 7, if $\boldsymbol{B} = \boldsymbol{CSO}$ is the SVD of vector set $\boldsymbol{B}$, then vector set*

$$\boldsymbol{CO} \tag{88}$$

is the orthonormal vector set having minimum distance from $\boldsymbol{B}$.

Proof: The square of the distance between two vector sets, $\boldsymbol{B}$ and $\boldsymbol{D}$, can be written as

$$\|\boldsymbol{B}-\boldsymbol{D}\|^2 \;=\; \|\boldsymbol{B}\|^2+\|\boldsymbol{D}\|^2-2\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle \tag{89}$$

Here $\boldsymbol{B}$ is given and the first term in the sum (89) is fixed. The second term is fixed too, since we are looking for $\boldsymbol{D}$ orthogonal and thus $\{\boldsymbol{D},\boldsymbol{D}\}=\boldsymbol{I}$, that is

$$\|\boldsymbol{D}\|^2 \;=\; \mathrm{Tr}(\{\boldsymbol{D},\boldsymbol{D}\}) \;=\; \mathrm{Tr}(\boldsymbol{I}). \tag{90}$$

Therefore, to minimize (89) is equivalent to maximizing $\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle$ over $\boldsymbol{D}$. To accomplish this, we first compute the value of $\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle$ for $\boldsymbol{D}=\boldsymbol{CO}$ and then we show that it is the maximum value. Computing $\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle$ with $\boldsymbol{D}=\boldsymbol{CO}$ one obtains

$$\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle \;=\; \Re\mathrm{Tr}(\{\boldsymbol{CSO},\boldsymbol{CO}\}) \;=\; \Re\mathrm{Tr}(\boldsymbol{O}^T\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{C}\}\boldsymbol{O}) \;=\; \Re\mathrm{Tr}(\boldsymbol{O}^T\boldsymbol{SIO}) \;=\; \Re\mathrm{Tr}(\boldsymbol{O}^T\boldsymbol{SO}). \tag{91}$$

In (91) $\boldsymbol{O}^T\boldsymbol{SO}$ is similar to $\boldsymbol{S}$ because $\boldsymbol{O}^T=\boldsymbol{O}^{-1}$; therefore, they have the same trace and (91) becomes

$$\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle \;=\; \mathrm{Tr}(\boldsymbol{S}). \tag{92}$$

Now we have to prove that $\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle \le \mathrm{Tr}(\boldsymbol{S})$ for $\{\boldsymbol{D},\boldsymbol{D}\}=\boldsymbol{I}$. Using the SVD of $\boldsymbol{B}$,

$$\Re\langle\langle \boldsymbol{B},\boldsymbol{D}\rangle\rangle \;=\; \Re\mathrm{Tr}(\{\boldsymbol{B},\boldsymbol{D}\}) \;=\; \Re\mathrm{Tr}(\{\boldsymbol{CSO},\boldsymbol{D}\}) \;=\; \Re\mathrm{Tr}(\boldsymbol{O}^T\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{D}\}) \;=\; \Re\mathrm{Tr}(\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{DO}^T\}). \tag{93}$$

Then, since $\{\boldsymbol{D},\boldsymbol{D}\}=\boldsymbol{I}$, $\boldsymbol{O}^T\boldsymbol{O}=\boldsymbol{I}$, $\boldsymbol{DO}^T$ is an orthogonal vector set. Therefore, $\{\boldsymbol{C},\boldsymbol{DO}^T\}$ is a matrix of scalar products between vectors with unitary norm, and by the Cauchy-Schwarz inequality they have modulus less than one, that is, $|\langle \boldsymbol{C}_i,(\boldsymbol{DO}^T)_i\rangle| \le \underbrace{\|\boldsymbol{C}_i\|}_{1}\underbrace{\|(\boldsymbol{DO}^T)_i\|}_{1} \;=\; 1$. Because of this, each diagonal element of the matrix $\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{DO}^T\}$ has its modulus always less than the corresponding elements of $\boldsymbol{S}$, and thus

$$\Re\mathrm{Tr}(\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{DO}^T\}) \le |\mathrm{Tr}(\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{DO}^T\})| \le \mathrm{Tr}(|\boldsymbol{S}\{\boldsymbol{C},\boldsymbol{DO}^T\}|) \le \mathrm{Tr}(\boldsymbol{S}). \tag{94}$$

■

C Proof of Property 1

We proceed in three steps: first we prove orthogonality of $\mathcal{U}_\omega$ and $\mathcal{U}_{\omega_1}$, followed by idempotency of $\mathcal{U}_\omega$, and finally, self-adjointness of $\mathcal{U}_\omega$.

Orthogonality of $\mathcal{U}_\omega$ and $\mathcal{U}_{\omega_1}$ By replacing in the first equation of (25) $\mathcal{U}_\omega$ and $\mathcal{U}_{\omega_1}$ with their definitions, one obtains

$$\frac{1}{|\Gamma|^2}\sum_{U\in\Gamma} U\pi_\omega(U)\sum_{V\in\Gamma} V\pi_{\omega_1}(V) \;=\; \frac{1}{|\Gamma|^2}\sum_{U,V\in\Gamma} UV\pi_\omega(U)\pi_{\omega_1}(V). \tag{95}$$

With the variable change $R \triangleq UV$, (95) can be rewritten as

$$\frac{1}{|\Gamma|^2}\sum_{U,R\in\Gamma} R\pi_\omega(U)\pi_{\omega_1}(U^{-1}R). \tag{96}$$

By remembering that π_{ω_1} is a homomorphism, that is, $\pi_{\omega_1}(U^{-1}R) = \pi_{\omega_1}(U^{-1})\pi_{\omega_1}(R)$, (96) becomes

$$\begin{aligned}\frac{1}{|\Gamma|^2}\sum_{U,R\in\Gamma} R\pi_\omega(U)\pi_{\omega_1}(U^{-1})\pi_{\omega_1}(R) \;&=\; \frac{1}{|\Gamma|^2}\sum_{U,R\in\Gamma} R\pi_\omega(U)\overline{\pi_{\omega_1}(U)}\pi_{\omega_1}(R),\\ &=\; \frac{1}{|\Gamma|^2}\sum_{U\in\Gamma}\pi_\omega(U)\overline{\pi_{\omega_1}(U)}\sum_{R\in\Gamma} R\pi_{\omega_1}(R).\end{aligned} \tag{97}$$

The first sum in the last term of (97) is zero because of the orthogonality relations between representations (see (53) Appendix A).

Idempotency of $\mathcal{U}_\omega$ The same reasoning made in the previous step can be repeated until (97). Here, however, $\pi_{\omega_1} = \pi_\omega$ and the first sum evaluates to $|\Gamma|$, while the second sum is, by definition, $\mathcal{U}_{\omega_1} = \mathcal{U}_\omega$ (see (21)). Therefore, (97) can be rewritten as

$$\mathcal{U}_\omega\mathcal{U}_\omega \;=\; \frac{1}{|\Gamma|}|\Gamma|\frac{1}{|\Gamma|}\sum_{R\in\Gamma} R\pi_\omega(R) \;=\; \mathcal{U}_\omega. \tag{98}$$

Proof of self-adjointness of $\mathcal{U}_\omega$ Use the definition of $\mathcal{U}_\omega$ in the last equation of (25) to show that

$$\mathcal{U}_\omega{}^T \;=\; \left(\sum_{U\in\Gamma} U\pi_\omega(U)\right)^T \;=\; \sum_{U\in\Gamma} U^T\overline{\pi_\omega(U)}. \tag{99}$$

Remember that each $U \in \Gamma$ is a unitary matrix and that $\overline{\pi_\omega(U)} = 1/\pi_\omega(U) = \pi_\omega(U^{-1})$ (see Section A.2). Then, (99) can be rewritten as

$$\mathcal{U}_\omega{}^T \;=\; \sum_{U\in\Gamma} U^{-1}\pi_\omega(U^{-1}) \;=\; \sum_{U\in\Gamma} U\pi_\omega(U) \;=\; \mathcal{U}_\omega. \tag{100}$$

Acknowledgement: We would like to thank Jim Mazo for his comments which improved considerably the exposition of this work.

References

[1] P. C. Teo and D. J. Heeger, "Perceptual image distortion," in *Proc. IEEE Conf. on Image Proc.*, (Austin, TX), pp. II:982–986, November 1994.

[2] S. A. Karunasekera and N. G. Kingsbury, "A distortion measure for blocking artifacts in images based on human visual sensitivity," *IEEE Trans. Image Proc.*, vol. 4, pp. 713–724, June 1995.

[3] A. B. Watson, "Visually optimal DCT quantization matrices for individual images," in *Proc. Data Compr. Conf.*, (Snowbird, UT), pp. 178–187, March 1993.

[4] S. Daly, *Visual Factors in Electronic Image Communications*, ch. The Visible Differences Predictor: An Algorithm for the Assessment of Image Fidelity. MIT Press, 1993.

[5] R. Bernardini and J. Kovačević, "Local orthogonal bases I: Construction," *Multidim. Syst. and Sign. Proc., special issue on Wavelets and Multiresolution Signal Processing*, vol. 7, pp. 331–370, July 1996. Invited paper. Reprinted in *Multidimensional Filter Banks and Wavelets*, S. Basu and B. Levy eds., Kluwer Academic Publishers, 1997.

[6] R. Bernardini and J. Kovačević, "Designing local orthogonal bases on finite groups II: Nonabelian case," *Journal of Fourier Analysis and Applications*, September 1997. Submitted.

[7] J. Serre, *Linear Representations of Finite Groups*. New York: Springer-Verlag, 1971.

[8] G. Folland, *A Course in Abstract Harmonic Analysis*. London: CRC Press, 1995.

[9] W. Rudin, *Fourier Analysis on Groups*. New York: Wiley, 1990.

[10] I. Gohberg and S. Goldberg, *Basic Operator Theory*. Boston, MA: Birkhauser, 1981.

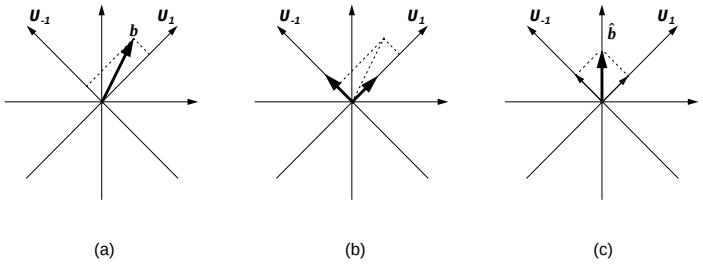

Figure 1: Geometric interpretation of the orthogonalization procedure using the Fourier transform as a tool. The group is $\Gamma = \{\mathcal{I}, V\}$, where V performs the exchange of the components of vectors from R^2. (a) Projection of $\mathbf{b}$ on the Γ-invariant subspaces relative to $\mathcal{U}_1$ and $\mathcal{U}_{-1}$. (b) Normalization of the two projections. (c) Recombination of the normalized projections yielding the generating vector $\hat{\mathbf{b}}$. It is now clear that $\hat{\mathbf{b}}$ and $V\hat{\mathbf{b}}$ are orthogonal.

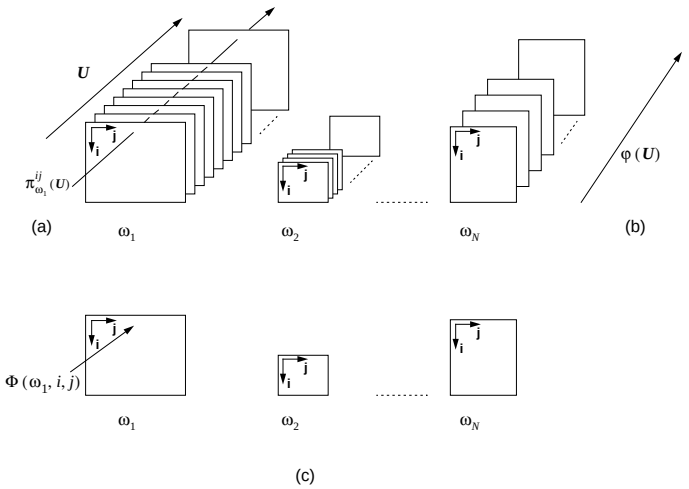

Figure 2: Visualization of the Fourier transform for nonabelian groups. (a) Irreducible representations $\pi_{\omega_1}(U), \ldots \pi_{\omega_\mathcal{N}}(U)$ clustered by ω_k and lined by U. (b) Function $\varphi(U)$. (c) Fourier transform of $\varphi(U)$, obtained by scalar products between (b) and the "rays" of (a).