QUANTUM MECHANICS ON FINITE GROUPS

Stan Gudder
Department of Mathematics
University of Denver
Denver, Colorado 80208
stan.gudder@nsm.du.edu

Abstract

Although a few new results are presented, this is mainly a review article on the relationship between finite-dimensional quantum mechanics and finite groups. The main motivation for this discussion is the hidden subgroup problem of quantum computation theory. A unifying role is played by a mathematical structure that we call a Hilbert *-algebra. After reviewing material on unitary representations of finite groups we discuss a generalized quantum Fourier transform. We close with a presentation concerning position-momentum measurements in this framework.

1 Introduction

Practically since its inception, quantum mechanics has had a close connection to group theory. Most of the groups in this connection have been Lie groups of infinite order. However, recently there has been considerable interest in quantum mechanics associated with finite groups [3, 12, 13, 22]. The main motivation for this interest stems from quantum computation and quantum information theory in which finite-dimensional quantum mechanics plays a crucial role [8, 17, 18, 19].

An important unsolved problem in quantum computation theory is the hidden subgroup problem [5, 6, 7, 11, 12, 13, 22]. Let H be a subgroup

of a finite group G and let X be a nonempty set. A function $f\colon G \to X$ **separates cosets** of H if for every $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if $Hg_1 = Hg_2$. Thus, f separates cosets if and only if f is constant on each coset and different on different cosets. Now let G be a (known) group and let H be an unknown subgroup of G. Suppose we have a computer that contains a black box (oracle) that can evaluate $f(g)$, $g \in G$, for a function f that separates cosets of H. It is of interest to find the fewest number of oracle calls (queries) necessary to determine H.

All known classical algorithms require $\mathcal{O}(|G|)$ oracle calls where $|G|$ is the order of G. The hidden subgroup problem is to find a quantum algorithm that determines H in time $\mathcal{O}\left(\text{poly}\left(\log|G|\right)\right)$ including oracle calls and any needed classical post-processing time. This problem has been solved for abelian groups G and essentially no others [12, 13]. In the case of a cyclic group, this reduces to Shor's algorithm for factoring integers [17, 20]. If this problem could be solved for a general finite group it can be used to efficiently solve some hard problems such as the graph isomorphism problem and the shortest vector in a lattice problem [4, 10, 16].

In the quantum computation case we have the following situation. Let $\mathcal{H}$ be a $|G|$-dimensional Hilbert space with orthonormal basis $\{|g\rangle\colon g \in G\}$. Let $f\colon G \to G$ be a function that separates cosets of the subgroup H. We have two registers, the query and answer register each described by the $|G|$-qubit space $\mathcal{H}$. The answer register is initially set at a convenient start $|G|$-qubit $|y\rangle \in \mathcal{H}$. The f-oracle is described by a unitary operator $U_f\colon \mathcal{H}\otimes\mathcal{H} \to \mathcal{H}\otimes\mathcal{H}$ given by $U_f\left(|x\rangle|y\rangle\right) = |x\rangle|yf(x)\rangle$. Since

$$U_f\left(|x\rangle\big|zf(x)^{-1}\big\rangle\right) = |x\rangle\big|zf(x)^{-1}f(x)\big\rangle = |x\rangle|z\rangle$$

we see that U_f is indeed unitary because it sends the orthonormal basis $\{|x\rangle|y\rangle\colon x, y \in G\}$ for $\mathcal{H}\otimes\mathcal{H}$ onto itself. The operator U_f represents a quantum gate in the "circuit" of a quantum computer.

In the particular case of Shor's algorithm, G is the cyclic group $Z_N = \{0, 1, \ldots, N-1\}$ and $\mathcal{H}$ is the N-qubit space $\mathbb{C}^N$. In this case, a crucial role is played by the quantum Fourier transform which is a unitary operator $F\colon \mathbb{C}^N \to \mathbb{C}^N$ given by

$$F|j\rangle = \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$$

It is widely believed [12, 13] that a solution to the hidden subgroup problem will require a generalization of this quantum Fourier transform to an arbitrary finite group G. The definition of such a generalization is one of the principal points of this paper.

Although a few new results are presented, this article is mainly a review of known results that are scattered in the literature. Our main contribution is to unify, simplify and clarify these results. To aid the reader's understanding and to make this article self-contained we have included proofs of the theorems. For the theory of unitary representations of groups we have relied on [9, 14, 15, 21]. For more details concerning the hidden subgroup problem and the generalized Fourier transform we refer the reader to [2, 3, 12, 13].

Sections 2, 3 and 4 discuss group algebras, regular representations, irreducible representations and abelian groups. Most of this is known material although our work on Hilbert *-algebras in Section 2 appears to be new. Section 5 presents the generalized Fourier transform in a somewhat different way than the existing literature. In Section 6 we consider position and momentum vectors and their relationship to the generalized Fourier transform. Finally, Section 7 presents a novel discussion of position-momentum measurements.

2 Group Algebra

In this work all groups will be assumed to be finite and all Hilbert spaces will be finite dimensional. A **Hilbert *-algebra $\mathcal{A}$** is a complex *-algebra with identity that is a Hilbert space that satisfies $\langle AB \mid C\rangle = \langle B \mid A^*C\rangle$ and $\langle A^* \mid B\rangle = \langle B^* \mid A\rangle$ for all $A, B, C \in \mathcal{A}$. An example of a Hilbert *-algebra is any *-subalgebra of the matrix algebra $M_n(\mathbb{C})$ with the inner product $\langle A \mid B\rangle = \mathrm{tr}(A^*B)$. Notice that we are assuming linearity in the second argument of the inner product.

Let G be a group with elements denoted by lower case Latin letters e, g, h, x, y, z, where e is the identity. The **group algebra** for G is the set $\mathcal{F}(G) = \{\phi\colon G \to \mathbb{C}\}$. Now $\mathcal{F}(G)$ is a complex vector space under pointwise addition and scalar multiplication. Moreover, $\mathcal{F}(G)$ becomes a Hilbert space under the inner product

$$\langle \phi \mid \psi\rangle = \sum_{x\in G} \overline{\phi(x)}\psi(x)$$

Denoting the order of G by $|G|$ we see that $\mathcal{F}(G)$ has dimension $|G|$ and the functions δ_g, $g \in G$, given by $\delta_g(x) = \delta_{g,x}$ form an orthonormal basis. Any $\phi \in \mathcal{F}(G)$ has the form $\phi = \sum \phi(g)\delta_g$. We also use the Dirac notation $|g\rangle = \delta_g$ and $\langle\phi|$ denotes the linear function $\langle\phi|\,(|\psi\rangle) = \langle\phi \mid \psi\rangle$. It follows that $\phi(g) = \langle g \mid \phi\rangle$.

For $\phi, \psi \in \mathcal{F}(G)$ define the **convolution** $\phi \circ \psi \in \mathcal{F}(G)$ by

$$\phi \circ \psi(x) = \sum_{y \in G} \phi(xy^{-1})\psi(y)$$

Moreover, we define the **involution** $\phi^* \in \mathcal{F}(G)$ by $\phi^*(x) = \overline{\phi(x^{-1})}$.

Theorem 2.1. *The system $(\mathcal{F}(G), \circ, ^*)$ is a Hilbert *-algebra with identity δ_e.*

Proof. It is clear that δ_e is the identity and that $\phi\circ(\psi_1+\psi_2) = \phi\circ\psi_1+\phi\circ\psi_2$, $(\phi_1 + \phi_2) \circ \psi = \phi_1 \circ \psi + \phi_2 \circ \psi$, $\lambda(\phi \circ \psi) = (\lambda\phi) \circ \psi = \phi \circ (\lambda\psi)$
To prove that convolution is associative we have

$$\begin{aligned}
[\phi \circ (\psi \circ \eta)]\,(x) &= \sum_y \phi(xy^{-1})(\psi \circ \eta)(y) = \sum_{y,z} \phi(xy^{-1})\psi(yz^{-1})\eta(z) \\
&= \sum_{g,z} \phi(xz^{-1}g^{-1})\psi(g)\eta(z) = \sum_z (\phi \circ \psi)(xz^{-1})\eta(z) \\
&= [(\phi \circ \psi) \circ \eta]\,(x)
\end{aligned}$$

It is clear that $(\phi + \psi)^* = \phi^* + \psi^*$, $(\lambda\phi)^* = \overline{\lambda}\phi^*$ and $\phi^{**} = \phi$. Moreover,

$$\begin{aligned}
(\phi \circ \psi)^*(x) &= (\overline{\phi \circ \psi})(x^{-1}) = \sum_y \overline{\phi}(x^{-1}y^{-1})\overline{\psi}(y) = \sum_z \overline{\psi}(zx^{-1})\overline{\phi}(z^{-1}) \\
&= \sum_z \psi^*(xz^{-1})\phi^*(z) = (\psi^* \circ \phi^*)(x)
\end{aligned}$$

Thus, $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ so $(\mathcal{F}(G), \circ, ^*)$ is a *-algebra. Now

$$\begin{aligned}
\langle \phi \circ \psi \mid \eta\rangle &= \sum_x (\overline{\phi \circ \psi})(x)\eta(x) = \sum_{x,y} \overline{\phi}(xy^{-1})\overline{\psi}(y)\eta(x) \\
&= \sum_y \overline{\psi}(y) \sum_x \phi^*(yx^{-1})\eta(x) = \sum_y \overline{\psi}(y)(\phi^* \circ \eta)(y) \\
&= \langle \psi \mid \phi^* \circ \eta\rangle
\end{aligned}$$

Finally, we have that

$$\langle \phi^* \mid \psi \rangle = \sum_x \phi(x^{-1})\psi(x) = \sum_y \psi(y^{-1})\phi(y) = \sum_y \overline{\psi^*}(y)\phi(y)$$

$$= \langle \psi^* \mid \phi \rangle \qquad \square$$

The next result summarizes some of the properties of $\mathcal{F}(G)$.

Theorem 2.2. (i) $\delta_x \circ \delta_y = \delta_{xy}$, (ii) $\delta_x^* = \delta_{x^{-1}}$, (iii) $(\phi \circ \delta_x)(y) = \phi(yx^{-1})$, $(\delta_x \circ \phi)(y) = \phi(x^{-1}y)$, (iv) $\|\phi^*\| = \|\phi\|$ (v) $(\phi^* \circ \phi)(e) = \|\phi\|^2 \leq \|\phi^* \circ \phi\|$, (vi) $\|\phi \circ \psi\| \leq |G|^{1/2}\|\phi\|\,\|\psi\|$.

Proof. (i) $(\delta_x \circ \delta_y)(z) = \sum_g \delta_x(zg^{-1})\delta_y(g) = \delta_x(zy^{-1}) = \delta_{xy}(z)$

(ii) $\delta_x^*(y) = \overline{\delta}_x(y^{-1}) = \delta_x(y^{-1}) = \delta_{x^{-1}}(y)$

(iii) $(\phi \circ \delta_x)(y) = \sum_z \phi(yz^{-1})\delta_x(z) = \phi(yx^{-1})$

$(\delta_x \circ \phi)(y) = \sum_z \delta_x(yz^{-1})\phi(x) = \phi(x^{-1}y)$

(iv) $\|\phi\|^2 = \sum_x |\phi(x)|^2 = \sum_x \left|\overline{\phi}(x^{-1})\right| = \sum |\phi^*(x)|^2 = \|\phi^*\|^2$

(v) $(\phi^* \circ \phi)(e) = \langle \delta_e \mid \phi^* \circ \phi \rangle = \langle \phi \mid \phi \rangle = \|\phi\|^2$

Applying Schwarz's inequality gives

$\|\phi\|^2 = \langle \delta_e \mid \phi^* \circ \phi \rangle \leq \|\phi^* \circ \phi\|\,\|\delta_e\| = \|\phi^* \circ \phi\|$

(vi) By Schwarz's inequality we have

$$\|\phi \circ \psi\|^2 = \sum_x |(\phi \circ \psi)(x)|^2 = \sum_x \left|\sum_y \phi(xy^{-1})\psi(y)\right|^2$$

$$\leq \sum_x \left[\sum_y |\phi(xy^{-1})|\,|\psi(y)|\right]^2$$

$$\leq \sum_x \left[\sum_y |\phi(xy^{-1})|^2 \sum_z |\psi(z)|^2\right] = |G|\,\|\phi\|^2\|\psi\|^2 \qquad \square$$

Notice that $\mathcal{F}(G)$ is not a C^*-algebra. In fact, $\mathcal{F}(G)$ is not even a Banach *-algebra because the factor $|G|^{1/2}$ in Theorem 2.2(vi) is sharp. For example, let $\phi \in \mathcal{F}(G)$ be defined by $\phi(x) = 1$ for all $x \in G$. Then $\|\phi\|^2 = |G|$ but

$$(\phi \circ \phi)(x) = \sum_y \phi(xy^{-1})\phi(y) = |G|$$

Hence, $\|\phi \circ \phi\| = |G|^{3/2}$ so that $\|\phi \circ \phi\| = |G|^{1/2}\|\phi\|^2$. We shall see later that $\mathcal{F}(G)$ can be endowed with a different norm so that it becomes a C^*-algebra but we shall not need to do this.

Recall that $x, y \in G$ are **conjugate** ($x \sim y$) if there is a $z \in G$ such that $zxz^{-1} = y$. Now $\sim$ is an equivalence relation and $\{y \in G\colon y \sim x\}$ is called the **conjugacy class** of x. The number of conjugacy classes is the **conjugacy number** of G. A function $\phi \in \mathcal{F}(G)$ is a **class function** if ϕ is constant on conjugate classes. Thus, ϕ is a class function if and only if $\phi(yxy^{-1}) = \phi(x)$ for all $x, y \in G$. Equivalently, ϕ is a class function if and only if $\phi(xy) = \phi(yx)$ for all $x, y \in G$. Applying Theorem 2.2(iii), we see that ϕ is a class function if and only if $\phi \circ \delta_x = \delta_x \circ \phi$ for all $x \in G$. It follows that ϕ is a class function if and only if $\phi \circ \psi = \psi \circ \phi$ for every $\psi \in \mathcal{F}(G)$, that is, ϕ is in the center $Z(\mathcal{F}(G))$ of $\mathcal{F}(G)$. Now $Z(\mathcal{F}(G))$ is a commutative Hilbert *-algebra that is a sub *-algebra of $\mathcal{F}(G)$ and $\dim Z(\mathcal{F}(G))$ is the conjugacy number of G.

There are Hilbert *-algebras that are not isomorphic to a group algebra. For example, the Hilbert *-algebra $M_2(\mathbb{C})$ of complex 2×2 matrices cannot be isomorphic to the group algebra $\mathcal{F}(G)$ of a group G. If this were the case, then

$$|G| = \dim \mathcal{F}(G) = \dim M_2(\mathbb{C}) = 4$$

However, groups of order 4 are abelian so $\mathcal{F}(G)$ must be commutative. But $M_2(\mathbb{C})$ is noncommutative which leads to a contradiction. The next result gives a necessary and sufficient condition for a Hilbert *-algebra to be isomorphic to a group algebra. An element U of a Hilbert *-algebra is **unitary** if $UU^* = U^*U = I$. A **unitary basis** for $\mathcal{A}$ is an orthonormal basis of unitary elements U_i, $i = 0, 1, \ldots, n-1$, where $U_0 = I$, for every i, j there exists a k such that $U_iU_j = U_k$ and for every i there exists a j such that $U_j^* = U_i$.

Theorem 2.3. *A Hilbert *-algebra $\mathcal{A}$ is Hilbert *-isomorphic to a group algebra if and only if A possesses a unitary basis.*

Proof. Applying Theorem 2.2(i) and (ii) we conclude that $\{\delta_x\colon x \in G\}$ is a unitary basis for $\mathcal{F}(G)$. Hence, if $\mathcal{A}$ is isomorphic to $\mathcal{F}(G)$, then $\mathcal{A}$ possesses a unitary basis. Conversely, suppose that $\mathcal{A}$ has a unitary basis U_i, $i = 0, 1, \ldots, n-1$. It is easy to check that $G = \{U_0, U_1, \ldots, U_{n-1}\}$ is a group under the product $U_iU_j = U_k$. For $A = \sum \lambda_i U_i \in \mathcal{A}$ define $\alpha(A) \in \mathcal{F}(G)$ by $\alpha(A) = \sum \lambda_i \delta_{U_i}$. Then clearly $\alpha\colon \mathcal{A} \to \mathcal{F}(G)$ is a bijective linear map. Since α maps an orthonormal basis onto an orthonormal basis, α is a Hilbert space isomorphism. Moreover,

$$\alpha(A^*) = \sum \overline{\lambda}_i \delta_{U_i^*} = \sum \overline{\lambda}_i \delta_{U_i^{-1}} = \sum \overline{\lambda}_i \delta_{U_i}^* = \alpha(A)^*$$

so α preserves the involution. Finally, since

$$\alpha(U_iU_j) = \alpha(U_k) = \delta_{U_k} = \delta_{U_iU_j} = \delta_{U_i} \circ \delta_{U_j} = \alpha(U_i) \circ \alpha(U_1)$$

it follows by linearity that $\alpha(AB) = \alpha(A) \circ \alpha(B)$ for all $A, B \in \mathcal{A}$. Hence, α is a Hilbert *-isomorphism. $\square$

For every $x \in G$, let $R_x \colon \mathcal{F}(G) \to \mathcal{F}(G)$ be the linear operator given by $(R_x\phi)(y) = \phi(yx)$. Then

$$(R_xR_y\phi)(z) = (R_y\phi)(zx) = \phi(zxy) = (R_{xy}\phi)(z)$$

so that $R_xR_y = R_{xy}$. Thus, R is a representation of G on the Hilbert space $\mathcal{F}(G)$. Moreover,

$$\begin{aligned}\langle R_x\psi \mid R_x\phi\rangle &= \sum_y (\overline{R_x\psi})(y)R_x\phi(y) = \sum_y \overline{\psi}(yx)\phi(yx) \\ &= \sum_z \overline{\psi}(z)\phi(z) = \langle \psi \mid \phi\rangle\end{aligned}$$

so that R is a unitary representation called the **right regular representation**. Notice that

$$(R_x\delta_y)(z) = \delta_y(zx) = \delta_{yx^{-1}}(z)$$

so $R_x\delta_y = \delta_{yx^{-1}}$ for every $x, y \in G$. Under the adjoint operation * let $\mathcal{R}(G)$ be the *-algebra generated by $\{R_x \colon x \in G\}$. It is clear that $A \in \mathcal{R}(G)$ if and only if $A = \sum \alpha_x R_x$, $\alpha_x \in \mathbb{C}$. Also, $\mathcal{R}(G)$ is a Hilbert space with inner product $\langle A \mid B\rangle = |G|^{-1}\mathrm{tr}(A^*B)$. Furthermore,

$$\begin{aligned}\langle AB \mid C\rangle &= |G|^{-1}\mathrm{tr}(B^*A^*C) = \langle B \mid A^*C\rangle \\ \langle A^* \mid B\rangle &= |G|^{-1}\mathrm{tr}(A) = |G|^{-1}\mathrm{tr}(B^{**}A) = \langle B^* \mid A\rangle\end{aligned}$$

so that $\mathcal{R}(G)$ is a Hilbert *-algebra. Notice that

$$\frac{1}{|G|}\,\mathrm{tr}(R_x) = \frac{1}{|G|}\sum_y \langle \delta_y \mid R_x\delta y\rangle = \frac{1}{|G|}\sum_y \langle \delta_y \mid \delta_{yx^{-1}}\rangle = \delta_{x,e}$$

Hence,

$$\langle R_x \mid R_y\rangle = \frac{1}{|G|}\,\mathrm{tr}(R_x^*R_y) = \frac{1}{|G|}\,\mathrm{tr}(R_{x^{-1}y}) = \delta_{x,y}$$

Therefore, $\{R_x \colon x \in G\}$ is a unitary basis for $\mathcal{R}(G)$ and $\dim \mathcal{R}(G) = |G|$. We call $\mathcal{R}(G)$ the **right algebra** of G. The **right commuting algebra** of G is the commutant

$$\mathcal{R}(G)' = \{A \in \mathcal{B}(\mathcal{F}(G)) : AR_x = R_x A \text{ for all } x \in G\}$$

where $\mathcal{B}(\mathcal{F}(G))$ denotes the set of all linear operators on $\mathcal{F}(G)$.

In a similar way, we define $L_x \in \mathcal{B}(\mathcal{F}(G))$ by $(L_x\phi)(y) = \phi(x^{-1}y)$. Then

$$(L_xL_y\phi)(z) = (L_y\phi)(x^{-1}z) = \phi(y^{-1}x^{-1}z) = (L_{xy}\phi)(z)$$

so that $L_xL_y = L_{xy}$. As before, L is a unitary representation of G called the **left regular representation**. Again,

$$(L_x\delta_y)(z) = \delta_y(x^{-1}z) = \delta_{xy}(z)$$

so $L_x\delta_y = \delta_{xy}$. As before, the $|G|$-dimensional Hilbert *-algebra $\mathcal{L}(G)$ generated by $\{L_x \colon x \in G\}$ is called the **left algebra** of G and its commutant $\mathcal{L}(G)'$ is the **left commuting algebra**.

Theorem 2.4. (i) $\mathcal{R}(G)' = \mathcal{L}(G)$ *and* $\mathcal{L}(G)' = \mathcal{R}(G)$. (ii) *The Hilbert* **-algebras* $\mathcal{F}(G)$, $\mathcal{R}(G)$ *and* $\mathcal{L}(G)$ *are Hilbert* **-isomorphic.*

Proof. (i) Since

$$(L_xR_y\phi)(z) = (R_y\phi)(x^{-1}z) = \phi(x^{-1}zy) = (L_x\phi)(zy) = (R_yL_x\phi)(z)$$

we have that $L_xR_y = R_yL_x$ for every $x, y \in G$. Hence, $\mathcal{L}(G) \subseteq \mathcal{R}(G)'$. Now let $A \in \mathcal{R}(G)'$ and define $B \in \mathcal{L}(G)$ by

$$B = \sum_{x \in G} (A\delta_e)(x)L_x$$

Then

$$\begin{aligned}(B\delta_y)(x) &= \sum_x (A\delta_e)(x)(L_x\delta_y)(z) = \sum_x (A\delta_e)(x)\delta_{xy}(z) = (A\delta_e)(zy^{-1}) \\ &= R_{y^{-1}}(A\delta_e)(z) = A(R_{y-1}\delta_e)(z) = (A\delta_y)(z)\end{aligned}$$

Hence, $B\delta_y = A\delta_y$ for all $y \in G$ so that $A = B \in \mathcal{L}(G)$. It follows that $\mathcal{R}(G)' = \mathcal{L}(G)$. We then have that

$$\mathcal{R}(G) = \mathcal{R}(G)'' = \mathcal{L}(G)'$$

(ii) It is easy to show that $\mathcal{R}(G)$ and $\mathcal{L}(G)$ are Hilbert *-algebra isomorphic via the map $\sum \alpha_x R_x \mapsto \sum \alpha_x L_x$. To show that $\mathcal{F}(G)$ and $\mathcal{R}(G)$ are Hilbert *-algebra isomorphic, for every $\phi \in \mathcal{F}(G)$ define $T_\phi \in \mathcal{R}(G)$ by $T_\phi = \sum \phi(x) R_x$. It is clear that $\phi \mapsto T_\phi$ is linear and bijective. Since $T_{\delta_x} = R_x$ we have that

$$T_{\delta_x \circ \delta_y} = T_{\delta_{xy}} = R_{xy} = R_x R_y = T_{\delta_x} T_{\delta_y}$$

Hence, by linearity $T_{\phi \circ \psi} = T_\phi T_\psi$. Also, since $T_{\delta_x} = R_x$ it follows by linearity that $\phi \mapsto T_\phi$ preserves inner products. Finally,

$$T_{\phi^*} = \sum_x \phi^*(x) R_x = \sum_x \overline{\phi}(x^{-1}) R_x = \sum_x \overline{\phi}(x) R_{x^{-1}} = \sum_x \overline{\phi}(x) R_x^* = T_\phi^* \qquad \square$$

Corollary 2.5. *For $\phi \in \mathcal{F}(G)$ define the linear operator $S_\phi \in \mathcal{R}(G)'$ by $S_\phi = \sum_x \phi(x) L_x$. Then $\phi \mapsto S_\phi$ is a Hilbert *-algebra isomorphism of $\mathcal{F}(G)$ onto $\mathcal{R}(G)'$. Moreover, we have that*

$$S_\phi(\psi) = \sum_x \psi(x) R_{x^{-1}}(\phi)$$

for every $\phi, \psi \in \mathcal{F}(G)$.

Proof. As in the proof of Theorem 2.4(ii) we have that $\phi \mapsto S_\phi$ is a Hilbert *-algebra isomorphism. For the second statement we have

$$\begin{aligned}(S_\phi \psi)(y) &= \sum_z \phi(z)(L_z \psi)(y) = \sum_z \phi(z)\psi(z^{-1}y) = \sum_x \psi(x)\phi(yx^{-1}) \\ &= \sum_x \psi(x)(R_{x-1}\phi)(y)\end{aligned}$$

and the result follows. $\square$

We now begin presenting a quantum mechanical flavor for this framework. We think of the elements of G as representing the location or position of a quantum system such as a quantum particle. For $x \in G$, let $P_x \in \mathcal{B}(\mathcal{F}(G))$ be the one-dimensional projection onto the subspace generated by δ_x. The Hilbert *-algebra $\mathcal{A}(G)$ generated by the projections P_x, $x \in G$ is called the **position algebra**. The algebra $\mathcal{A}(G)$ is commutative, $|G|$-dimensional and consists of all operators of the form $\sum \alpha_x P_x$, $\alpha_x \in \mathbb{C}$. Since $(R_x \phi)(y) =$

$\phi(yx)$, we may think of R_x as a "translation" to a new position. We therefore view $\mathcal{R}(G)$ as a "momentum" algebra. Of course, $\mathcal{L}(G)$ would be just as good.

For $\Delta \subseteq G$, $x \in G$ we define $\Delta x = \{yx \colon y \in \Delta\}$. Moreover, we define the projection operator $P_\Delta \in \mathcal{A}(G)$ by $P_\Delta \psi = \chi_\Delta \psi$. Notice that $P_{\{x\}} = P_x$ as previously defined. It is clear that $\Delta \mapsto P_\Delta$ is a projection-valued measure. That is, $P_G = I$ and $P_{\Delta_1 \cup \Delta_2} = P_{\Delta_1} + P_{\Delta_2}$ whenever $\Delta_1 \cap \Delta_2 = \emptyset$. We now verify the **covariance condition** $R_x^* P_\Delta R_x = P_{\Delta x}$. Indeed,

$$\begin{aligned}(R_x^* P_\Delta R_x \psi)(y) &= (P_\Delta R_x \psi)(yx^{-1}) = \chi_\Delta(yx^{-1})(R_x\psi)(yx^{-1}) \\ &= \chi_\Delta(yx^{-1})\psi(y) = \chi_\Delta(y)\psi(y) = (P_{\Delta x}\psi)(y)\end{aligned}$$

A projection-valued measure P_Δ that satisfies the covariance condition is called a **system of imprimitivity base on** G for R.

3 Irreducible Representations

As usual, G will denote a finite group. A **representation** of G is a map $U \colon G \to \mathcal{B}(\mathcal{H}(U))$ where $\mathcal{H}(U)$ is a finite-dimensional complex linear space and U satisfies $U_{xy} = U_x U_y$ for all $x, y \in G$. If $\mathcal{H}(U)$ is a Hilbert space and U_x is unitary for all $x \in G$, then U is a **unitary representation** of G.

Lemma 3.1. *If U is a representation of G, then we can always endow $\mathcal{H}(U)$ with an inner product so that U is a unitary representation of G.*

Proof. We can always construct an inner product $\langle \phi, \psi \rangle$ on $\mathcal{H}(U)$. If U is not a unitary representation relative to this inner product, form a new inner product

$$\langle \psi \mid \psi \rangle = \sum_x \langle U_x \phi, U_x \psi \rangle$$

Then for every $y \in G$ we have that

$$\langle U_y \phi \mid U_y \psi \rangle = \sum_x \langle U_x(U_y \phi), U_x(U_y \psi) \rangle = \sum_x \langle U_{xy}\phi, U_{xy}\psi \rangle = \langle \phi \mid \psi \rangle$$

Hence, U_y is unitary under this new inner product. □

Because of Lemma 3.1 we can always assume a representation of G is unitary. For this reason, when we say that U is a representation we shall

mean that U is a unitary representation. If U and V are representations of G, U and V are **equivalent** (denoted by $U \approx V$) if there is an invertible linear transformation $T\colon \mathcal{H}(U) \to \mathcal{H}(V)$ such that $TU_xT^{-1} = V_x$ for all $x \in G$. (Applying the polar decomposition of T it follows that there is a unitary transformation $S\colon \mathcal{H}(U) \to \mathcal{H}(V)$ such that $SU_xS^{-1} = V_x$, but we shall not need this here.) The **direct sum** of two representations U and V of G is the unique representation $U \oplus V$ on $\mathcal{H}(U) \oplus \mathcal{H}(V)$ defined by

$$(U \oplus V)_x(\phi, \psi) = (U_x\phi, V_x\psi)$$

for all $x \in G$, $\phi \in \mathcal{H}(U)$, $\psi \in \mathcal{H}(V)$. When there are n summands of the same representation, we use the notation

$$nU = U \oplus \cdots \oplus U$$

If U is a representation of G and $\mathcal{K}$ is a subspace of $\mathcal{H}(U)$ then $\mathcal{K}$ is **invariant** if $U_x\mathcal{K} \subseteq \mathcal{K}$ for all $x \in G$. If $\mathcal{K}$ is invariant then the restriction $U \mid \mathcal{K}$ is a representation of G called the **subrepresentation** defined by $\mathcal{K}$. Note that if $\mathcal{K}$ is invariant then so is its orthogonal complement $\mathcal{K}^\perp$. Indeed, if $\psi \in \mathcal{K}^\perp$, then for any $\phi \in \mathcal{K}$ we have that

$$\langle U_x\psi \mid \phi\rangle = \langle \psi \mid U_x^*\phi\rangle = \langle \psi \mid U_{x^{-1}}\phi\rangle = 0$$

Hence, $U_x\psi \in \mathcal{K}^\perp$ for every $x \in G$. We then have that

$$U = U \mid \mathcal{K} \oplus U \mid \mathcal{K}^\perp$$

Any representation U has the two subrepresentations defined on $\mathcal{H}(U)$ itself and on $\{0\}$. The other subrepresentations, if they exist, are called **proper**. A representation with no proper subrepresentation is **irreducible**. It is clear that any representation is the direct sum of irreducible representations.

A linear transformation $T\colon \mathcal{H}(U) \to \mathcal{H}(V)$ such that $TU_x = V_xT$ for every $x \in G$ is an **intertwining operator**. The set of all intertwining operators is a vector space denoted by $\mathcal{I}(U, V)$ and $i(U, V) = \dim \mathcal{I}(U, V)$ is the **intertwining number** of U and V. Of course, $\mathcal{I}(R, R) = \mathcal{R}(G)'$ is the commuting algebra considered in Section 2.

Theorem 3.2. *The space $\mathcal{I}(U, V) = \{0\}$ if and only if no nonzero subrepresentation of U is equivalent to any nonzero subrepresentation of V.*

Proof. Suppose $T \in \mathcal{I}(U,V)$ with $T \neq 0$ and let $N_T = \text{Null}(T)$, $R_T = \text{Range}(T)$. Then $N_T \neq \mathcal{H}(U)$ is an invariant subspace of $\mathcal{H}(U)$. Indeed, if $T\phi = 0$ then $TU_x\phi = V_X T\phi = 0$ for every $x \in G$ so that $U_x N_T \subseteq N_T$. Also $R_T \neq \{0\}$ is an invariant subspace of $\mathcal{H}(V)$. Indeed, if $\psi = T\phi$ for some $\phi \in \mathcal{H}(U)$ then

$$V_x\psi = V_xT\phi = TU_x\phi$$

So that $V_xR_T \subseteq R_T$ for every $x \in G$. Now $T \mid N_T^\perp \colon N_T^\perp \to R_T$ is bijective and T gives an equivalence between the subrepresentation $U \mid N_T^\perp$ of U and the subrepresentation $V \mid R_T$ of V. Conversely, suppose a nonzero subrepresentation of U is equivalent to a nonzero subrepresentation of V. Then there exist subspaces $\mathcal{K} \subseteq \mathcal{H}(U)$, $\mathcal{L} \subseteq \mathcal{H}(V)$, $\mathcal{K}, \mathcal{L} \neq \{0\}$ and a linear bijection $T' \colon \mathcal{K} \to \mathcal{L}$ such that $T'U_x\psi = V_xT'\psi$ for every $\psi \in \mathcal{K}$, $x \in G$. Define $T \colon \mathcal{H}(U) \to \mathcal{H}(V)$ by

$$T\psi = \begin{cases} T'\psi & \text{if} \quad \psi \in \mathcal{K} \\ 0 & \text{if} \quad \psi \in \mathcal{K}^\perp \end{cases}$$

and extend by linearity. Then if $\psi \in \mathcal{H}(U)$ we can write $\psi = \psi_1 + \psi_2$, $\psi_1 \in \mathcal{K}$, $\psi_2 \in \mathcal{K}^\perp$. Hence,

$$TU_x\psi = TU_x\psi_1 + TU_x\psi_2 = T'U_x\psi_1 = V_xT'\psi_1 = V_xT(\psi_1 + \psi_2) = V_xT\psi$$

so that $T \in \mathcal{I}(U,V)$ and $T \neq 0$. □

If $\mathcal{I}(U,V) = \{0\}$ we say that U and V are **disjoint**.

Corollary 3.3. *Let U and V be irreducible representations of G.* (i) *Either U and V are disjoint or U and V are equivalent.* (ii) $\mathcal{I}(U,U) = \mathbb{C}I$. (iii) $i(U,V) = 0$ *or* 1.

Proof. (i) By the proof of Theorem 3.2, N_T and R_T are either $\{0\}$ or the whole space. Thus, $\mathcal{I}(U,V) = \{0\}$ or U and V are equivalent. (ii) Since U is irreducible, every nonzero member of $\mathcal{I}(U,U)$ is bijective. Hence, $\mathcal{I}(U,U)$ is a finite-dimensional division *-algebra. By Shur's Lemma $\mathcal{I}(U,U) = \mathbb{C}I$. This can also be shown directly as follows. Let $T \in \mathcal{I}(U,U)$ be self-adjoint and let λ be an eigenvalue of T. Then there exists a eigenvector $\phi \neq 0$ with $T\phi = \lambda\phi$. Now $\text{Null}(T - \lambda I) \neq \{0\}$ and $T - \lambda I \in \mathcal{I}(U,U)$. Hence, $T - \lambda I = 0$

so that $T = \lambda I$. Since every $T \in \mathcal{I}(U,U)$ has the form $T = T_1 + iT_2$ for $T_1, T_2 \in \mathcal{I}(U,U)$ self-adjoint, the result follows. (iii) This follows from (i) and (ii). □

It follows immediately from the definitions that

$$i(U_1 \oplus U_2, V) = i(U_1, V) + i(U_2, V)$$
$$i(U, V_1 \oplus V_2) = i(U, V_1) + i(U, V_2)$$

Thus, if U is a representation of G with the form

$$U = L^1 \oplus \cdots \oplus L^n$$

where the L^j are irreducible and M is any irreducible representation of G, then

$$i(M, U) = \sum_j i(M, L^j) = \text{number of } j \text{ with } L^j \approx M \tag{3.1}$$

Lemma 3.4. *Let $L^1 \oplus \cdots \oplus L^n \approx M^1 \oplus \cdots \oplus M^m$ where the L^j and M^k are irreducible representations of G. Then $m = n$ and there exists a permutation π of $\{1, \ldots, n\}$ such that $L^j \approx M^{\pi(j)}$, $j = 1, \ldots, n$.*

Proof. Let $U = L^j \oplus \cdots \oplus L^n$. Since $U \approx M^1 \oplus \cdots \oplus M^m$, we have that

$$i(U, M^1 \oplus \cdots \oplus M^m) \neq 0$$

so $\sum_j i(M^j, U) \neq 0$. Hence, there exists a j such that $i(M^j, U) \neq 0$. We can assume without loss of generality that $j = 1$ so that $i(M^1, U) \neq 0$. By (3.1) there is a k such that $L^k \approx M^1$. Again, we can assume that $k = 1$ so that $L^1 \approx M^1$. Now

$$L^2 \oplus \cdots \oplus L^n \approx M^2 \oplus \cdots \oplus M^m$$

and continue by induction. □

Lemma 3.4 shows that the decomposition of U into the direct sum of irreducible representations is unique to within order and equivalence. By (3.1), $i(M, U)$ is the unique number of irreducible summands of U equivalent to M and is called the **multiplicity** of M in U.

Theorem 3.5. *If V is a representation of G then the vector spaces $\mathcal{H}(V)$ and $\mathcal{I}(R,V)$ are isomorphic and hence $i(R,V) = \dim \mathcal{H}(V)$.*

Proof. For $\phi \in \mathcal{H}(V)$ define the linear transformation $S_\phi \colon \mathcal{F}(G) \to \mathcal{H}(V)$ by

$$S_\phi(\psi) = \sum_{x \in G} \psi(x) V_{x^{-1}}(\phi)$$

As in Corollary 2.5, $S_\phi \in \mathcal{I}(R,V)$ and we define the linear transformation $\mathcal{T} \colon \mathcal{H}(V) \to \mathcal{I}(R,V)$ by $\mathcal{T}(\phi) = S_\phi$. As in the proof of Theorem 2.1 $\mathcal{T}$ is bijective. □

Corollary 3.6. *The right regular representation of G contains every irreducible representation of G with multiplicity equal to its dimension.*

Corollary 3.7. *Let $L^1, \ldots, L^r$ be the inequivalent irreducible representations of G and let d_j be the dimension of L^j. Then*

$$d_1^2 + d_2^2 + \cdots + d_r^2 = |G|$$

Proof. By Corollary 3.6 we have that

$$R = d_1 L^1 \oplus d_2 L^2 \oplus \cdots \oplus d_r L^r \tag{3.2}$$

and the result follows. □

It follows from (3.2) that

$$\mathcal{R}(G)' \approx \mathcal{I}(d_1 L^1, d_1 L^1) \oplus \cdots \mathcal{I}(d_r L^r, d_r L^r)$$

But since $\mathcal{I}(L^j, L^j) = \mathbb{C}I$ is it not hard to show that $\mathcal{I}(d_j L^j, d_j L^j) \approx M_{d_j}$ the full algebra of $d_j \times d_j$ complex matrices. We conclude that

$$\mathcal{F}(G) \approx \mathcal{R}(G)' \approx M_{d_1} \oplus \cdots \oplus M_{d_r} \tag{3.3}$$

Notice that (3.3) is consistent with Corollary 3.7. Now the elements in the center $Z(M_{d_1} \oplus \cdots \oplus M_{d_r})$ have the form $\sum c_j I_{d_j}$ where $c_j \in \mathbb{C}$ and I_{d_j} is the identity matrix in M_{d_j}. Hence,

$$\dim Z\left(\mathcal{F}(G)\right) = \dim Z(M_{d_1} \oplus \cdots \oplus M_{d_r}) = r \tag{3.4}$$

We therefore have the following.

Theorem 3.8. *The number of inequivalent irreducible representations of G is the conjugacy number of G.*

Proof. We have seen that the conjugacy number of G equals $\dim Z(\mathcal{F}(G))$ and the result now follows from (3.4). □

Corollary 3.9. *A finite group G is abelian if and only if every irreducible representation of G is one-dimensional.*

Proof. If G is abelian, every conjugate class of G contains one element. Hence, the conjugacy number of G is $|G|$ and by Theorem 3.8 the number of inequivalent irreducible representations of G is $|G|$. By Corollary 3.7 every irreducible representation of G is one-dimensional. Conversely, suppose all irreducible representations of G are one-dimensional. By Corollary 3.7 there are $r = |G|$ distinct one-dimensional representations $\chi_1, \ldots, \chi_r$ of G (called the **characters** of G). We may think of these as functions $\chi_j \in \mathcal{F}(G)$ that satisfy $\chi_j(xy) = \chi_j(x)\chi_j(y)$ for all $x, y \in G$. Since $|G| < \infty$, for every $x \in G$ there is an $n \in \mathbb{N}$ such that $x^n = e$. Hence,

$$\chi_j(x)^n = \chi_j(x^n) = \chi_j(e) = 1$$

We conclude that $|\chi_j(x)| = 1$ and that $\chi_j(x)^{-1} = \overline{\chi}_j(x)$ for every j and x. Now for every $y \in G$ we have that

$$\sum_x \chi_j(x) = \sum_x \chi_j(xy) = \chi_j(y) \sum_x \chi(x)$$

Hence, $[1 - \chi_j(y)] \sum_x \chi_j(x) = 0$. Thus, if $\chi_j \neq 1$ then $\sum_x \chi_j(x) = 0$. If $\chi_j \neq \chi_k$ then

$$\chi_j(x)\chi_k(x)^{-1} = \chi_j(x)\overline{\chi}_k(x) = 1$$

for some $x \in G$. Since the product of characters is again a character we have that $\sum_x \overline{\chi}_j(x)\chi_k(x) = 0$. We conclude that $\chi_1/|G|^{1/2}, \ldots, \chi_r/|G|^{1/2}$ form an orthonormal basis for $\mathcal{F}(G)$. Since

$$\delta_x = \frac{1}{|G|} \sum \langle \chi_j \mid \delta_x \rangle \chi_j = \frac{1}{|G|} \sum \overline{\chi}_j(x)\chi_j$$

the map $x \mapsto (\chi_1(x), \ldots, \chi_r(x))$ is injective. Since this map is an isomorphism of G onto an abelian group, G must be abelian. □

Examples. The smallest nonabelian group is the six element group of all permutations of three objects. By Corollary 3.7, $d_1^2 + \cdots + d_r^2 = 6$ so $d_j \leq 2$, $j = 1, \ldots, r$. By Corollary 3.9, at least one $d_j > 1$. Hence, $d_1 = 2$, say. We thus have $d_1 = 2$, $d_2 = 1$, $d_3 = 1$ and the conjugacy number is 3. There is just one group of order 7 and it is abelian. There are two nonabelian groups of order 8. Now $d_1^2 + \cdots + d_r^2 = 8$ and as before $d_1 = 2$, say. Since every group has a one-dimensional representation (the constant functions in $\mathcal{F}(G)$), $d_2 = 1$, say. Hence, $d_1 = 2$, $d_2 = 1$, $d_3 = 1$, $d_4 = 1$, $d_5 = 1$ and the conjugacy number is 5. Similar analyses apply to other small order groups.

4 Abelian Groups

In the case of a finite abelian group G much of our previous work simplifies. As we say in Corollary 3.9, all the irreducible representations of G are one-dimensional and there are $r = |G|$ inequivalent ones. These r representations can be thought of as functions $\chi_j(xy) = \chi(x)\chi_j(y)$, $|\chi_j(x)| = 1$ so they are homomorphisms from G into the multiplicative group of complex numbers on the unit circle. We also saw in Corollary 3.9 that $\{r^{-1}\chi_j \colon j = 1, \ldots, r\}$ forms an orthonormal basis for $\mathcal{F}(G)$. Since

$$(\chi_i \circ \chi_j)(x) = \sum_y \chi_i(xy^{-1})\chi_j(y) = \chi_i(x) \sum_y \overline{\chi}_i(y)\chi_j(y) = \chi_i(x)\delta_{i,j}$$

we have that $\chi_i \circ \chi_j = \chi_j \delta_{i,j}$. Moreover, $\chi_j^* = \chi_j$ so the characters are self-adjoint idempotents in $\mathcal{F}(G)$. One consequence is that $\mathcal{F}(G)$ is a commutative Hilbert *-algebra. The set of characters $\widehat{G}$ of G is itself a group under pointwise multiplication.

Now suppose G is cyclic of order r with generator g. Then for a character χ we have that $\chi(g^j) = \chi(g)^j$ so χ is determined by $\chi(g) \in \mathbb{C}$. Since $g^r = e$

$$\chi(g)^r = \chi(g^r) = \chi(e) = 1$$

so that $\chi(g)$ is an rth root of 1. Thus, there is a character for each rth root of 1. Since both G and $\widehat{G}$ are isomorphic to the group of rth roots of 1 we conclude that $G \approx \widehat{G}$. If $G = G_1 \times G_2$ then the characters of G have the form $\chi(x, y) = \chi_1(x)\chi_2(y)$ where $\chi_i \in \widehat{G}_i$ so $(G_1 \times G_2)^\wedge \approx \widehat{G}_1 \times \widehat{G}_2$. An elementary theorem states that every finite abelian group is a direct product of cyclic groups so we conclude that $G \approx \widehat{G}$ whenever G is finite abelian. There is a

canonical isomorphism of G onto $\widehat{\widehat{G}}$ given by $x \mapsto \widehat{x}$ where $\widehat{x}(\chi) = \chi(x)$. In this way every element of G acts as a character on $\widehat{G}$.

It follows from Corollary 3.6 that the right regular representation has the form $R = \chi_1 \oplus \cdots \oplus \chi_r$. More generally, let V be an arbitrary representation of G on a Hilbert space $\mathcal{H}(V)$. For each $\chi \in \widehat{G}$, let P_χ be the operator

$$P_\chi = \frac{1}{|G|} \sum_x \overline{\chi}(x) V_x$$

Theorem 4.1. (i) $P_\chi^2 = P_\chi = P_\chi^*$. (ii) $P_{\chi_1} P_{\chi_2} = 0$ *if* $\chi_1 \neq \chi_2$.
(iii) $\sum_\chi P_\chi = I$. (iv) $V_x P_\chi = \chi(x) P_\chi$, *for every* $x \in G$, $\chi \in \widehat{G}$.

Proof. That $P_\chi = P_\chi^*$ is straightforward. To prove the rest of (i) and (ii) we have that

$$\begin{aligned} P_{\chi_1} P_{\chi_2} &= \frac{1}{|G|^2} \sum_{x,y} \overline{\chi}_1(x) \overline{\chi}_2(y) V_{xy} = \frac{1}{|G|^2} \sum_{x,z} \overline{\chi}_1(x) \overline{\chi}_2(x^{-1}z) V_z \\ &= \frac{1}{|G|^2} \left[\sum_x \overline{\chi}_1(x) \chi_2(x) \right] \left[\sum_z \overline{\chi}_2(z) V_z \right] = \langle \chi_1 \mid \chi_2 \rangle P_{\chi_2} \\ &= \delta_{\chi_1, \chi_2} P_{\chi_2} \end{aligned}$$

To prove (iii), notice that since $\widehat{x} \in \widehat{\widehat{G}}$ we have for $x \neq e$ that

$$\sum_\chi \chi(x) = \sum_\chi \widehat{x}(\chi) = 0$$

Hence,

$$\sum_\chi P_\chi = \frac{1}{|G|} \sum_\chi \sum_x \overline{\chi}(x) V_x = \frac{1}{|G|} \sum_x V_x \left[\sum_\chi \chi(x) \right] = V_e = I$$

To prove (iv) we have that

$$\begin{aligned} V_x P_\chi &= \frac{1}{|G|} \sum_y \overline{\chi}(y) V_{xy} = \frac{1}{|G|} \sum_z \overline{\chi}(x^{-1}z) V_z \\ &= \frac{\chi(x)}{|G|} \sum_x \overline{\chi}(z) V_z = \chi(x) P_\chi \end{aligned}$$

□

Let $\mathcal{H}_\chi$ be the range of the projection P_χ in $\mathcal{H}(V)$. Applying Theorem 4.1(i, ii, iii), every $\phi \in \mathcal{H}(V)$ has a unique representation $\phi = \sum \phi_\chi$, $\phi_\chi \in \mathcal{H}_\chi$. By Theorem 4.1(iv), if $\phi \in \mathcal{H}_\chi$ then $V_x(\phi) = \chi(x)\phi$. Thus, each $\mathcal{H}_\chi$ defines a subrepresentation V^χ of V of the form $x \mapsto \chi(x)I$ and $V = \oplus V^\chi$.

Let us consider the cyclic case in more detail. If G is cyclic of order N, then we may assume that G is the additive group $\{0, 1, \dots, N\}$ with addition $\mod N$. Every irreducible representation of G is one of the characters $\chi_0, \chi_1, \cdots, \chi_{N-1}$ where

$$\chi_j(k) = e^{2\pi ijk/N}, \qquad i = \sqrt{-1}$$

The group algebra $\mathcal{F}(G)$ is the set of functions $f\colon \{0, 1, \dots, N-1\} \to \mathbb{C}$ which we can identify with $\mathbb{C}^N$ and the right regular representation R satisfies $(R_k\phi)(j) = \phi(j+k) \mod N$. The functions

$$\phi_j(k) = |G|^{-1/2} e^{2\pi ijk/N}, \qquad j, k \in \{0, 1, \dots, N-1\}$$

form an orthonormal basis for $\mathcal{F}(G)$. Moreover,

$$\begin{aligned}(R_k\phi_j)(n) = \phi_j(n+k) &= \frac{1}{|G|} e^{2\pi ij(n+k)/N} = e^{2\pi ijk/N} \frac{1}{|G|} e^{2\pi ijn/N} \\ &= e^{2\pi ijk/N} \phi_j(n)\end{aligned}$$

Hence, $R_k\phi_j = e^{2\pi ijk/N}\phi_j = \chi_j(k)\phi_j$, $j, k \in \{0, 1, \dots, N-1\}$. Hence, ϕ_j, $j = 0, \dots, N-1$, spans a one-dimensional invariant subspace $\mathcal{H}_i$ of $\mathcal{F}(G)$ and R_k acting on $\mathcal{H}_j$ is just multiplication by $\chi_j(k)$. The expansion of any $\psi \in \mathcal{F}(G)$ in terms of ϕ_j is

$$\psi(k) = \sum c_j \phi_j(k) = \frac{1}{|G|} \sum_j c_j e^{2\pi ijk/N}$$

where

$$c_j = \langle \phi_j \mid \psi \rangle = \frac{1}{|G|} \sum_k e^{-2\pi ijk/N} \psi(k)$$

Of course, this is the finite Fourier expansion of ψ and gives the finite Fourier transform.

5 Generalized Fourier Transform

We have seen in (3.2) that the regular representation

$$R = d_1 L^1 \oplus \cdots \oplus d_r L^r$$

where L^j, $j = 1, \ldots, r$, are the irreducible representations of G and d_j is the dimension of L^j. As we mentioned in Section 1 it is important to define a Fourier transform for an arbitrary group G. For $\psi \in \mathcal{F}(G)$ the **operator generalized Fourier transform** [1, 3, 13] is given by the operator-valued vector

$$\widehat{\psi}(j) = \sqrt{\frac{d_j}{|G|}} \sum_{x \in G} \psi(x) L^j_{x^{-1}}, \qquad j = 1, \ldots, r \tag{5.1}$$

Thus, $\widehat{\psi}(j)$ is an operator on the Hilbert space $\mathcal{F}(G)$. Notice that

$$\widehat{\delta}_x(j) = \sqrt{\frac{d_j}{|G|}}\ L^j_{x^{-1}}, \qquad j = 1, \ldots, r$$

which states that the Fourier transform of "position" is "momentum." The next lemma shows how the function ψ can be recovered from its transform $\widehat{\psi}$.

Lemma 5.1. *For $\psi \in \mathcal{F}(G)$ we have that*

$$\psi(x) = \frac{1}{\sqrt{|G|}} \sum_{j=1}^{r} \sqrt{d_j}\ \mathrm{tr}\left[\widehat{\psi}(j) L^j_x\right]$$

Proof. Since

$$\mathrm{tr}\left[\widehat{\psi}(j) L^j_x\right] = \sqrt{\frac{d_j}{|G|}}\ \sum_y \psi(y) \mathrm{tr}(L^j_{y^{-1}x})$$

we have that

$$\begin{aligned} \frac{1}{\sqrt{|G|}} \sum_j \sqrt{d_j}\, \mathrm{tr}\left[\widehat{\psi}(j) L^j_x\right] &= \frac{1}{\sqrt{|G|}}\ \sum_y \psi(y) \sum_j d_j \mathrm{tr}(L^j_{y^{-1}x}) \\ &= \frac{1}{\sqrt{|G|}}\ \sum_y \psi(y) \mathrm{tr}(R_{y^{-1}x}) = \psi(x) \end{aligned}$$

□

We now show that this gives a generalization of the usual finite Fourier transform as described in Section 4. Let G be the cyclic group $Z_N = \{0, 1, \ldots, N-1\}$. We know that Z_N has N inequivalent irreducible one-dimensional representations χ^j, $j = 0, 1, \ldots, N-1$, where $\chi^j_k = e^{2\pi ijk/N}$, $k \in Z_N$. Then $\mathcal{F}(G) = \mathbb{C}^N$ and since $d_j = 1$, $j = 0, 1, \ldots, N-1$, we have that

$$\widehat{\psi}(j) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \psi(k)\overline{\chi}^j_k = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \psi(k)e^{-2\pi ijk/N}$$

and

$$\psi(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \widehat{\psi}(j)\chi)^j_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \widehat{\psi}(j)e^{2\pi ijk/N}$$

which is the usual Fourier transform.

It is clear that $\widehat{\ }$ is a linear transformation so its range $\mathrm{Hat}(G)$ is a linear space. For $\widehat{\phi} \in \mathrm{Hat}(G)$ define $\widehat{\phi}^*$ by $\widehat{\phi}^*(j) = \widehat{\phi}(j)^*$ and define an inner product on $\mathrm{Hat}(G)$ by

$$\left\langle \widehat{\phi} \mid \widehat{\psi} \right\rangle = \sum_j \mathrm{tr}\left[\widehat{\phi}(j)^*\widehat{\psi}(j)\right]$$

The next result shows that $\widehat{\ }$ possesses some important and useful properties.

Theorem 5.2. (i) $(\widehat{\phi})^* = (\phi^*)\widehat{\ }$. (ii) $\left\langle \widehat{\phi} \mid \widehat{\psi} \right\rangle = \langle \phi \mid \psi \rangle$. (iii) $(\phi \circ \psi)\widehat{\ }(j) = (|G|/d_j)^{1/2}\widehat{\phi}(j)\widehat{\psi}(j)$

Proof. (i) We have that

$$\widehat{\phi^*}(j) = \widehat{\phi}(j)^* = \sqrt{\frac{d_j}{|G|}} \left[\sum_x \phi(x)L^j_{x^{-1}}\right]^* = \sqrt{\frac{d_j}{|G|}} \sum_x \widehat{\phi}(x)L^j_x$$

$$= \sqrt{\frac{d_j}{|G|}} \sum_x \overline{\phi}(x^{-1})L^j_{x^{-1}} = (\phi^*)\widehat{\ }(j)$$

(ii) Since

$$\widehat{\phi}(j)^*\widehat{\psi}(j) = \frac{d_j}{|G|} \sum_{x,y} \overline{\phi}(x)\psi(y)L^j_{xy^{-1}}$$

We have that

$$\left\langle \widehat{\phi} \mid \widehat{\psi} \right\rangle = \sum_j \mathrm{tr}\left[\widehat{\phi}(j)^* \widehat{\psi}(j)\right] = \frac{1}{|G|} \sum_{x,y} \overline{\phi}(x)\psi(y) \sum_j d_j \mathrm{tr}(L^j_{xy^{-1}})$$
$$= \frac{1}{|G|} \sum_{x,y} \overline{\phi}(x)\psi(y)\mathrm{tr}(R_{xy^{-1}}) = \sum_x \overline{\phi}(x)\psi(x) = \langle \phi \mid \psi \rangle$$

(iii) We have that

$$(\phi \circ \psi)^\wedge(j) = \sqrt{\frac{d_j}{|G|}} \sum_x (\phi \circ \psi)(x) L^j_{x^{-1}} = \sqrt{\frac{d_j}{|G|}} \sum_x \sum_y \phi(xy^{-1})\psi(y) L^j_{x^{-1}}$$
$$= \sqrt{\frac{d_j}{|G|}} \sum_y \psi(y) \sum_z \phi(z) L^j_{y^{-1}z^{-1}}$$
$$= \sqrt{\frac{d_j}{|G|}} \sum_z \phi(z) L^j_{z^{-1}} \sum_y \psi(y) L^j_{y^{-1}} = \sqrt{\frac{|G|}{d_j}}\, \widehat{\phi}(j)\widehat{\psi}(j) \qquad \square$$

For, $\widehat{\phi}, \widehat{\psi} \in \mathrm{Hat}(G)$ define $\widehat{\phi} \circ \widehat{\psi}$ by

$$(\widehat{\phi} \circ \widehat{\psi})(j) = \sqrt{\frac{|G|}{d_j}}\, \widehat{\phi}(j)\widehat{\psi}(j)$$

Then by Theorem 5.2(iii) it follows that $\widehat{\phi} \circ \widehat{\psi} \in \mathrm{Hat}(G)$ and it is easy to show that with this product $\mathrm{Hat}(G)$ becomes a Hilbert *-algebra. We then conclude that $\mathcal{F}(G)$ and $\mathrm{Hat}(G)$ are Hilbert *-algebra isomorphic under the isomorphism $^\wedge$.

We would now like to define a Fourier transform that maps functions $\psi \in \mathcal{F}(G)$ to functions instead of operators. A natural way of doing this is the following. For each $j = 1, \ldots, r$, let $\{\phi^j_n\}$, $n = 1, \ldots, d_j$, be an orthonormal basis for the d_j-dimensional invariant subspace $\mathcal{H}^j$ on which L^j acts. We define the **generalized Fourier transform** of $\psi \in \mathcal{F}(G)$ as

$$\widetilde{\psi}(j, m, n) = \left\langle \phi^j_m \mid \widehat{\psi}(j)\phi^j_n \right\rangle, \qquad m, n = 1, \ldots, d_j \tag{5.2}$$

Notice that $\widetilde{\psi}(j, m, n)$ depends on the chosen basis ϕ^j_n. This may be an advantage because certain bases may provide a simplification. Let $\widetilde{\mathcal{F}}(G)$

be the Hilbert space of complex-valued functions $\phi(j,m,n)$, $j = 1,\dots,r$, $m,n = 1,\dots,d_j$, with the inner product

$$\langle \phi \mid \psi \rangle = \sum_{j,m,n} \overline{\phi}(j,m,n)\psi(j,m,n)$$

We call $\widetilde{\mathcal{F}}(G)$ the **momentum space** corresponding to the **position space** $\mathcal{F}(G)$. Of course, $\dim \widetilde{\mathcal{F}}(G) = |G|$.

Lemma 5.3. *The linear transformation $\sim\colon \mathcal{F}(G) \to \widetilde{\mathcal{F}}(G)$ is unitary.*

Proof. Applying Theorem 5.2(ii) gives

$$\begin{aligned}\left\langle \widetilde{\phi} \mid \widetilde{\psi} \right\rangle &= \sum_{j,m,n} \overline{\widetilde{\phi}}(j,m,n)\widetilde{\psi}(j,m,n) = \sum_{j,m,n} \left\langle \widehat{\phi}(j)\phi_n^j \mid \phi_m^j \right\rangle \left\langle \phi_m^j \mid \widehat{\psi}(j)\phi_n^j \right\rangle \\ &= \sum_{j,n} \left\langle \widehat{\phi}(j)\phi_n^j \mid \widehat{\psi}(j)\phi_n^j \right\rangle = \sum_{j,n} \left\langle \phi_n^j \mid \widehat{\phi}(j)^*\widehat{\psi}(j)\phi_n^j \right\rangle \\ &= \sum_j \operatorname{tr}\left[\widehat{\phi}(j)^*\widehat{\psi}(j)\right] = \left\langle \widehat{\phi} \mid \widehat{\psi} \right\rangle = \langle \phi \mid \psi \rangle \end{aligned}$$

□

Define the map $^*\colon \widetilde{\mathcal{F}}(G) \to \widetilde{\mathcal{F}}(G)$ by $\phi^*(j,m,n) = \overline{\phi}(j,n,m)$ and the map $\circ\colon \widetilde{\mathcal{F}}(G) \times \widetilde{\mathcal{F}}(G) \to \widetilde{\mathcal{F}}(G)$ by

$$(\phi \circ \psi)(j,m,n) = \sqrt{\frac{|G|}{d_j}} \sum_p \phi(j,m,p)\psi(j,p,n)$$

Theorem 5.4. *Under the operations * and $\circ$, $\widetilde{\mathcal{F}}(G)$ becomes a Hilbert *-algebra and $\sim\colon \mathcal{F}(G) \to \widetilde{\mathcal{F}}(G)$ is a Hilbert *-algebra isomorphism.*

Proof. To show that * is an involution we have that

$$\begin{aligned}(\phi \circ \psi)^*(j,m,n) &= \sqrt{\frac{|G|}{d_j}} \sum_p \overline{\phi}(j,n,p)\overline{\psi}(j,p,m) \\ &= \sqrt{\frac{|G|}{d_j}} \sum_p \psi^*(j,m,p)\phi^*(j,p,n) \\ &= (\psi^* \circ \phi^*)(j,m,n)\end{aligned}$$

Hence, $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ and the other properties of an involution are straightforward. Now

$$\begin{aligned}\langle \phi^* \mid \psi \rangle &= \sum_{j,m,n} \phi(j,n,m)\psi(j,m,n) = \sum_{j,m,n} \psi(j,m,n)\phi(j,n,m) \\ &= \langle \psi^* \mid \phi \rangle\end{aligned}$$

and

$$\begin{aligned}\langle \phi \circ \psi \mid \eta \rangle &= \sqrt{\frac{|G|}{d_j}} \sum_{j,m,n} \sum_{p} \overline{\phi}(j,m,p)\overline{\psi}(j,p,n)\eta(j,m,n) \\ &= \sqrt{\frac{|G|}{d_j}} \sum_{j,n,p} \overline{\psi}(j,p,n) \sum_{m} \phi^*(j,p,m)\eta(j,m,n) \\ &= \sqrt{\frac{|G|}{d_j}} \sum_{j,m,p} \overline{\psi}(j,p,n)(\phi^* \circ \eta)(j,p,n) = \langle \psi \mid \phi^* \circ \eta \rangle\end{aligned}$$

The other properties of a Hilbert *-algebra are again straightforward. To show that $\sim$ is an isomorphism, we have that

$$\begin{aligned}(\phi^*)^\sim(j,m,n) &= \left\langle \phi^j_m \mid (\phi^*)^\wedge(j) \mid \phi^j_n \right\rangle = \left\langle \phi^j_m \mid \widehat{\phi}(j)^* \mid \phi^j_n \right\rangle \\ &= \left\langle \widehat{\phi}(j)\phi^j_m \mid \phi^j_n \right\rangle = \overline{\left\langle \phi^j_n \mid \widehat{\phi}(j)\phi^j_m \right\rangle} \\ &= \overline{\overline{\phi}}(j,n,m) = (\widetilde{\phi})^*(j,m,n)\end{aligned}$$

Hence, $(\phi^*)^\sim = (\widetilde{\phi})^*$. Finally, by Theorem 5.2(iii) we have that

$$\begin{aligned}(\phi \circ \psi)^\sim(j,m,n) &= \left\langle \phi^j_m \mid (\phi \circ \psi)^\wedge(j)\phi^j_n \right\rangle = \sqrt{\frac{|G|}{d_j}} \left\langle \phi^j_m \mid \widehat{\phi}(j)\widehat{\psi}(j)\phi^j_n \right\rangle \\ &= \sqrt{\frac{|G|}{d_j}} \sum_{p} \left\langle \phi^j_m \mid \widehat{\phi}(j)\phi^j_p \right\rangle \left\langle \phi^j_p \mid \widehat{\psi}(j)\phi^j_n \right\rangle \\ &= \sqrt{\frac{|G|}{d_j}} \sum_{p} \widetilde{\phi}(j,m,p)\widetilde{\psi}(j,p,n) = (\widetilde{\phi} \circ \widetilde{\psi})(j,m,n)\end{aligned}$$

Hence, $(\phi \circ \psi)^\sim = \widetilde{\phi} \circ \widetilde{\psi}$. □

6 Position and Momentum Vectors

As in Section 5, for each $j = 1, \dots, r$, let $\{\phi_n^j\}$, $n = 1, \dots, d_j$, be an orthonormal basis for the d_j-dimensional invariant subspace $\mathcal{H}^j$ on which the irreducible representation L^j of G acts. For $g \in G$ we can represent the unitary operator L_g^j by a $d_j \times d_j$ unitary matrix $D_{mn}^j(g)$ given by [1]

$$D_{mn}^j(g) = \left\langle \phi_m^j \mid L_g^j \phi_n^j \right\rangle = \left\langle \phi_m^j \mid R_g \phi_n^j \right\rangle$$

$m, n = 1, \dots, d_j$. Using the Dirac notation we define the **position vectors** $|g\rangle = \delta_g$, $g \in G$. We define the **momentum vectors** $|jmn\rangle \in \mathcal{F}(G)$, $j = 1, \dots, r$, $m, n = 1, \dots d_j$, by

$$|jmn\rangle = \sqrt{\frac{d_j}{|G|}} \sum_g D_{mn}^j(g) \, |g\rangle \tag{6.1}$$

There is a close connection between the generalized Fourier transform of $\psi \in \mathcal{F}(G)$ and $|jmn\rangle$ given by

$$\widetilde{\psi}(j, m, n) = \langle jnm \mid \psi \rangle$$

Indeed, applying (5.1) and (5.2) we have that

$$\begin{aligned}
\widetilde{\psi}(j, m, n) &= \sqrt{\frac{d_j}{|G|}} \sum_g \psi(g) \left\langle \phi_m^j \mid L_{g^{-1}}^j \phi_n^j \right\rangle \\
&= \sqrt{\frac{d_j}{|G|}} \sum_g \overline{\left\langle \phi_n^j \mid L_g^j \phi_m^j \right\rangle} \psi(g) \\
&= \sqrt{\frac{d_j}{|G|}} \sum_g \overline{D_{nm}^j}(g) \psi(g) = \langle jnm \mid \psi \rangle
\end{aligned}$$

The next result summarizes important properties of $D_{mn}^j(g)$.

Theorem 6.1. *The complex numbers $D_{mn}^j(g)$ satisfy the following identities.* (i) $\sum_n D_{mn}^j(g) D_{np}^j(h) = D_{mp}^j(gh)$. (ii) $\sum_n D_{mn}^j(g) \overline{D_{pn}^j(g)} = \delta_{m,n}$.
(iii) $\sum_g D_{mn}^j \overline{D_{t,s}^i(g)} = (|G|/d_j) \, \delta_{i,j} \delta_{m,t} \delta_{n,s}$.
(iv) $\sum_{j,m,n} d_j D_{mn}^j(g) \overline{D_{mn}^j(h)} = |G| \delta_{g,h}$.

Proof. (i) Since $L^j_{gh} = L^j_g L^j_h$ for all $g, h \in G$ we have that

$$\begin{aligned}\sum_n D^j_{mn}(g) D^j_{np}(h) &= \sum_n \langle \phi^j_m \mid L^j_g \phi^j_n \rangle \langle \phi^j_n \mid L^j_h \phi^j_p \rangle \\ &= \sum_n \langle L^{j*}_g \phi^j_m \mid \phi^j_n \rangle \langle \phi^j_n \mid L^j_h \phi^j_p \rangle \\ &= \sum_n \langle L^{j*}_g \phi^j_m \mid L^j_h \phi^j_p \rangle = \sum \langle \phi^j_m \mid L^j_{gh} \phi^n_p \rangle \\ &= D^j_{mp}(gh)\end{aligned}$$

(ii) Follows from the unitarity of $D^j_{mn}(g)$.
(iii) Consider the operator $S \colon \mathcal{H}^i \to \mathcal{H}^j$ given by

$$S = \sum_g \left| L^j_g \phi^j_n \right\rangle \left\langle L^i_g \phi^i_s \right|$$

Now

$$\begin{aligned}S L^i_h \phi^i_t &= \sum_g \left| L^j_g \phi^j_j \right\rangle \langle L^i_g \phi^i_s \mid L^i_h \phi^i_t \rangle = \sum_g \left| L^j_g \phi^j_n \right\rangle \langle L^i_{h^{-1}g} \phi^i_s \mid \phi^i_t \rangle \\ &= \sum_x \left| L^j_{hx} \phi^j_n \right\rangle \langle L^i_x \phi^i_s \mid \phi^i_t \rangle = L^j_h \sum_x \left| L^j_x \phi^j_n \right\rangle \langle L^i_x \phi^i_s \mid \phi^i_t \rangle \\ &= L^j_h S \phi^i_t\end{aligned}$$

Hence, $S L^i_h = L^j_h S$ for every $h \in G$ so $S \in \mathcal{I}(L^i, L^j)$. Since L^i and L^j are inequivalent except when $i = j$ we have that $S = 0$ unless $i = j$. When $i = j$ we have that $S \in \mathcal{I}(L^j, L^j)$ so $S = c I_{d_j}$ a multiple of the identity on $\mathcal{H}^j$. To find c we have that

$$\begin{aligned}c d_j = \operatorname{tr}(S) &= \sum_t \langle \phi^j_t \mid S \phi^j_t \rangle = \sum_g \sum_t \langle \phi^i_t \mid L^j_g \phi^j_n \rangle \langle L_g \phi^j_s \mid \phi^i_t \rangle \\ &= \sum_g \langle L^j_g \phi^j_s \mid L^i_g \phi^i_n \rangle = \sum_g \langle \phi^j_s \mid \phi^j_n \rangle = |G| \delta_{s,n}\end{aligned}$$

Hence $c = d_j^{-1} |G| \delta_{s,n}$ so that $S = d_j^{-1} |G| \delta_{s,n} I_{d_j}$ when $i = j$. We conclude that

$$\langle \phi^j_m \mid S \phi^i_t \rangle = \frac{|G|}{d_j} \, \delta_{i,j} \delta_{n,s} \delta_{m,t}$$

Equation (iii) now follows.
(iv) For $g \in G$ we have that

$$\begin{aligned}\operatorname{tr}(R_g) &= \operatorname{tr}(R_e^* R_g) = |G|\langle R_e \mid R_g\rangle = |G|\langle T_{\delta_e} \mid T_{g^{-1}}\rangle \\ &= |G|\langle \delta_e \mid \delta_{g^{-1}}\rangle = |G|\delta_{e,g}\end{aligned}$$

Since $R_g = d_1 L^1 g \oplus \cdots \oplus d_r L_g^r$ we have by (i) that

$$\begin{aligned}\sum_{j,m,n} d_j D^j_{mn}(g)\overline{D^j_{mn}(h)} &= \sum_{j,m,n} d_j D^j_{mn}(g) D^j_{nm}(h^{-1}) \\ &= \sum_{j,m} d_j D^j_{mm}(gh^{-1}) = \sum_j d_j \operatorname{tr}(L^j_{gh^{-1}}) \\ &= \operatorname{tr}(R_{gh^{-1}}) = |G|\delta_{g,h}\end{aligned}$$

□

The next result gives the important properties of the momentum vectors $|jmn\rangle$.

Theorem 6.2. (i) *The vectors $|jmn\rangle$ form an orthonormal basis for $\mathcal{F}(G)$.*
(ii) *For $m = 1, \ldots, d_j$, $\{|jmn\rangle \colon n = 1, \ldots, d_j\}$ is an orthonormal basis for the mth invariant subspace for the subrepresentation L^j of R.*

Proof. (i) By Theorem 6.1(iii) we have that

$$\langle its \mid jmn\rangle = \frac{\sqrt{d_i d_j}}{|G|} \sum_g \overline{D^i_{tj}(g)}\, D^j_{mn}(g) = \delta_{i,j}\delta_{m,t}\delta_{n,s}$$

Since the $|jmn\rangle$ form an orthonormal set and there are $d_1^2 + \cdots + d_r^2 = |G|$ elements in the set, they form an orthonormal basis.
(ii) The vectors $|jmn\rangle$, $n = 1, \ldots, d_j$ are a basis for an invariant subspace for R because by Theorem 6.1 we have that

$$\begin{aligned}R_h|jmn\rangle &= \sqrt{\frac{d_j}{|G|}} \sum_g D^j_{mn}(g) R_h|g\rangle = \sqrt{\frac{d_j}{|G|}} \sum_g D^j_{mn}(g)\big|gh^{-1}\big\rangle \\ &= \sqrt{\frac{d_j}{|G|}} \sum_x D^j_{mn}(xh)|x\rangle = \sqrt{\frac{d_j}{|G|}} \sum_x \sum_p D^j_{mn}(x) D^j_{pn}(h)|x\rangle \\ &= \sqrt{\frac{d_j}{|G|}} \sum_p D^j_{pn}(h) \sum_x D^j_{mp}(x)|x\rangle \\ &= \sum_p D^j_{pn}(h)|jmp\rangle\end{aligned}$$

Now define the unitary operator T from the subspace spanned by $|jmn\rangle$, $n = 1, \ldots, d_j$, onto the subspace spanned by ϕ_n^j, $n = 1, \ldots, d_j$, given by $T|jmn\rangle = \phi_n^j$. Then we have that

$$\begin{aligned} R_h T|jmn\rangle = R_h\phi_n^j &= \sum_p \langle \phi_p^j \mid R_h\phi_n^j\rangle \phi_p^j \\ &= \sum_p D_{pn}^j(h)\phi_p^j = TR_h|jmn\rangle \end{aligned}$$

Hence, $R_hT = TR_h$ for every $h \in G$. Since ϕ_n^j, $n = 1, \ldots, d_j$ is a basis for the d_j-dimensional invariant subspace on which L^j acts, we have that R acting on the subspace spanned by $|jmn\rangle$, $n = 1, \ldots, d_j$ is equivalent to L^j and the result follows. □

We have seen that the generalized Fourier transform of $\psi \in \mathcal{F}(G)$ is given by

$$\widetilde{\psi}(j,m,n) = \sqrt{\frac{d_j}{|G|}} \sum_g \overline{D_{nm}^j(g)}\, \psi(g)$$

We now find the inverse transform.

Lemma 6.3. *If $\widetilde{\psi} \in \widetilde{\mathcal{F}}(G)$ then*

$$\psi(g) = \frac{1}{\sqrt{|G|}} \sum_{j,m,n} \sqrt{d_j}\, D_{nm}^j(g)\widetilde{\psi}(j,m,n)$$

Proof. Applying Theorem 6.1(iv) we have that

$$\begin{aligned} \frac{1}{\sqrt{|G|}} \sum_{j,m,n} \sqrt{d_j}\, D_{nm}^j(g)\widetilde{\psi}(j,m,n) &= \frac{1}{|G|} \sum_{j,m,n} d_j D_{nm}^j(g) \sum_h \overline{D_{nm}^j(h)}\, \psi(h) \\ &= \frac{1}{|G|} \sum_h \psi(h) \sum_{j,m,n} d_j D_{nm}^j(h)\overline{D_{nm}^j(h)} \\ &= \psi(g) \end{aligned}$$

□

In a similar way we can define a **generalized Fourier transform operator** $F\colon \mathcal{F}(G) \to \mathcal{F}(G)$ by

$$F = \sum_{g,j,m,n} \langle jnm \mid g\rangle |jmn\rangle\langle g|$$

It follows that F is a Hilbert *-algebra isomorphism.

7 Position-Momentum Measurements

Let $\mathcal{H}$ be a Hilbert space and let $G_i \in \mathcal{B}(\mathcal{H})$ satisfy $\sum G_i^* G_i = I$. A map $\mathcal{G}\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ of the form

$$\mathcal{G}(A) = \sum G_i A G_i^*$$

is a **quantum operation** with **operational elements** $\{G_i\}$ [17]. More technically, $\mathcal{G}$ is called a **trace preserving completely positive** map. If $\sum G_i G_i^* = I$ then $\mathcal{G}$ is called **unital**. If $\mathcal{G}$ is unital we define $\mathcal{G}^*\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ by

$$\mathcal{G}(A) = \sum G_i A G_i^*$$

Then $\mathcal{G}^*$ is a quantum operation with operational elements $\{G_i^*\}$. Now let $\mathcal{G}$ and $\mathcal{J}$ be quantum operations with operational elements $\{G_i\}$ and $\{J_i\}$ respectively. Then

$$\mathcal{J} \circ \mathcal{G}(A) = \sum_{i,j} J_j G_i A G_i^* J_j^* = \sum_{i,j} (J_j G_i) A (J_j G_i)^*$$

and

$$\sum_{i,j} (J_j G_i)^* J_j G_i = \sum_{i,j} G_i^* J_j^* J_j G_i = \sum_i G_i^* G_i = I$$

Hence, $\mathcal{J} \circ \mathcal{G}$ is a quantum operation with operational elements $\{J_j G_i\}$. Moreover, if $\mathcal{G}$ and $\mathcal{J}$ are both unital then so is $\mathcal{J} \circ \mathcal{G}$ and

$$(\mathcal{J} \circ \mathcal{G})^*(A) = \sum_{i,j} G_i^* J_j^* A J_j G_i = \sum_{i,j} G_i^* \mathcal{J}^*(A) G_i = \mathcal{G}^* \circ \mathcal{J}^*(A)$$

Hence, $(\mathcal{J} \circ \mathcal{G})^* = \mathcal{G}^* \circ \mathcal{J}^*$.

Now let $\mathcal{H}$ be the state space for a quantum system and let $\mathcal{D}(\mathcal{H})$ be the set of density operators on $\mathcal{H}$. Then the set of mixed states are represented by elements of $\mathcal{D}(\mathcal{H})$. A quantum measurement can be described by the restriction of a quantum operation $\mathcal{G}$ to $\mathcal{D}(\mathcal{H})$. The operational elements $\{G_i\}$ for $\mathcal{G}$ represent the possible outcomes of the measurement. If the measurement is performed for a system in state ρ and no outcome is observed then the resulting state is given by the Luders form

$$\mathcal{G}(\rho) = \sum G_i \rho G_i^*$$

If outcome i is observed then the post-measurement state is $G_i\rho G_i^*/\mathrm{tr}(G_i\rho G_i^*)$ and the probability of this observation is $\mathrm{tr}(G_i\rho G_i^*) = \mathrm{tr}(G_i^*G_i\rho)$.

We now consider the group algebra $\mathcal{F}(G)$ to be the state space of a quantum system. We then define the **position measurement** to be the quantum operation $\mathcal{Q}$ with operational elements $\{|g\rangle\langle g| \colon g \in G\}$ and the **momentum measurement** to be the quantum operation $\mathcal{P}$ with operational elements

$$\{|jmn\rangle\langle jmn| \colon j = 1, \dots, r, m, n = 1, \dots, d_j\}$$

Then $\mathcal{Q}$ and $\mathcal{P}$ are not only unital they are given by projection-valued measures. We call $\mathcal{E} = \mathcal{P} \circ \mathcal{Q}$ the **sequential position-momentum measurement**. Notice that the operational elements of $\mathcal{E}$ are $\{\langle jmn \mid g\rangle|jmn\rangle\langle g|\}$. Notice that $\mathcal{Q} = \mathcal{Q} \circ \mathcal{Q} = \mathcal{Q}^*$ and $\mathcal{P} = \mathcal{P} \circ \mathcal{P} = \mathcal{P}^*$. Hence,

$$\mathcal{E}^* = (\mathcal{P} \circ \mathcal{Q})^* = \mathcal{Q}^* \circ \mathcal{P}^* = \mathcal{Q} \circ \mathcal{P}$$

and we call $\mathcal{E}^*$ the **sequential momentum-position measurement**. Then $\mathcal{E}^*$ has operational elements $\{\langle g \mid jmn\rangle|g\rangle\langle jmn|\}$. We also have the following identities:

$$\mathcal{E}^* \circ \mathcal{E} = \mathcal{Q} \circ \mathcal{P} \circ \mathcal{P} \circ \mathcal{Q} = \mathcal{Q} \circ \mathcal{P} \circ \mathcal{Q} = \mathcal{Q} \circ \mathcal{E} = \mathcal{E}^* \circ \mathcal{Q}$$
$$\mathcal{E} \circ \mathcal{E}^* = \mathcal{P} \circ \mathcal{Q} \circ \mathcal{Q} \circ \mathcal{P} = \mathcal{P} \circ \mathcal{Q} \circ \mathcal{P} = \mathcal{E} \circ \mathcal{P} = \mathcal{P} \circ \mathcal{E}^*$$

We denote the operational elements of $\mathcal{E}$ by

$$W(g; jmn) = \langle jmn \mid g\rangle|jmn\rangle\langle g| = \sqrt{\frac{d_j}{|G|}}\,\overline{D^j_{mn}(g)}|jmn\rangle\langle g|$$

Then

$$W(g; jmn)^*W(g; jmn) = |\langle jmn \mid g\rangle|^2\,|g\rangle\langle g|$$

and

$$W(g; jmn)W(g; jmn)^* = |\langle jmn \mid g\rangle|^2\,|jmn\rangle\langle jmn|$$

are positive operator-valued measures on a discrete phase-space. The next result summarizes some of the properties of $W(g; jmn)$.

Theorem 7.1. *The operational elements $W(g;jmn)$ satisfy the following conditions.*

(i) $\displaystyle\sum_{g,j,m,n} W(g;jmn) = I$

(ii) $\displaystyle\sum_{g} W(g;jmn)W(g;jmn)^* = \sum_{g} W(g;jmn) = |jmn\rangle\langle jmn|$

(iii) $\displaystyle\sum_{j,m,n} W(g;jmn)^*W(g;jmn) = \sum_{j,m,n} W(g;jmn)^* = |g\rangle\langle g|$

(iv) $\displaystyle\sum_{g,j,m,n} W(g;jmn)^*W(g;jmn) = \sum_{g,j,m,n} W(g;jmn)W(g;jmn)^* = I$

(v) $W(g;jmn)W(g';j'm'n')^* = \delta_{g,g'}\langle jmn \mid g\rangle\langle g \mid j'm'n'\rangle|jmn\rangle\langle j'm'n'|$

(vi) $W(g';j'm'n')^*W(g;jmn) = \delta_{jmn}\delta_{j'm'n'}\langle g' \mid jmn\rangle\langle jmn \mid g\rangle|g'\rangle\langle g|$

Proof. Straightforward verification. □

If the system is in the state $\rho \in \mathcal{D}(\mathcal{H})$ then the probability that a sequential position-momentum measurement results in the outcome (g, jmn) becomes

$$P_\rho(g, jmn) = \operatorname{tr}\left[W(g;jmn)\rho W(g;mn)^*\right]$$

Now P_ρ is a probability distribution on the discrete phase-space and by Theorem 7.1 its position marginal distribution is given by

$$P_\rho(g) = \sum_{j,m,n} P_\rho(g, jmn) = \langle g \mid \rho \mid g\rangle$$

Of course, this is the usual position distribution in the state ρ. however, in general,

$$\sum_{g} P_\rho(g, jmn) \neq \langle jmn \mid \rho \mid jmn\rangle$$

This is because position is measured first and momentum second so that a position measurement interferes with a momentum measurement but not vise versa.

In a similar way we obtain the probability that a sequential momentum-position measurement results in the outcome (jmn, g)

$$P_\rho(jmn, g) = \mathrm{tr}\left[W(g; jmn)^* \rho W(g; jmn)\right]$$

Again, this gives a probability distribution whose momentum marginal distribution is given by

$$P_\rho(jmn) = \sum_g P_\rho(jmn, g) = \langle jmn \mid \rho \mid jmn \rangle$$

In this case the momentum measurement interfers with the position measurement so that

$$\sum_{j,m,n} P_\rho(jmn, g) \neq \langle g \mid \rho \mid g \rangle$$

Although the sequential probability distributions cannot be viewed as joint position-momentum distributions, we can define a **joint position-momentum amplitude**

$$W_\rho(g; jmn) = \mathrm{tr}\left[\rho W(g; jmn)\right] = \langle jmn \mid g \rangle \langle g \mid \rho \mid jmn \rangle$$

It follows immediately that

$$\sum_g W\rho(g; jmn) = \langle jmn \mid \rho \mid jmn \rangle$$
$$\sum_{j,m,n} W_\rho(g; jmn) = \langle g \mid \rho \mid g \rangle$$

Thus, the marginals of $W_\rho(g; jmn)$ give the correct position and momentum distributions even though $W_\rho(g; jmn)$ can have complex values in general.

If A is an operator on $\mathcal{F}(G)$, define the function

$$A(g; jmn) = \mathrm{tr}\left[AW(g; jmn)\right] = \langle jmn \mid g \rangle \langle g \mid A \mid jmn \rangle$$

In particular, if $\rho \in \mathcal{D}(H)$ is a state, then $\rho(g; jmn) = W_\rho(g; jmn)$. Thus operators and states are represented by functions on the discrete phase space. If G is abelian, then every irreducible representation is one-dimensional. In this case, $m = n = 1$ and we write $A(g; j) = A(g; j11)$, $D^j_{11} = \chi^j$ and $|j\rangle = |j11\rangle$.

Lemma 7.2. *If G is abelian, then for any operators A, B on $\mathcal{F}(G)$ we have that*

$$\sum_{g,j} A(g;j)\,\overline{B(g;j)} = \frac{1}{|G|}\,\mathrm{tr}(AB^*)$$

Proof. In the abelian case we have that

$$W(g;j) = \frac{1}{\sqrt{|G|}}\,\overline{\chi}^j(g)|j\rangle\langle g|$$

Hence,

$$A(g;j) = \mathrm{tr}\left[AW(g;j)\right] = \frac{1}{\sqrt{|G|}}\,\overline{\chi}^j(g)\langle g \mid A \mid j\rangle$$

Therefore,

$$\sum_{g,j} A(g;j)\,\overline{B(g;j)} = \frac{1}{|G|}\sum_{g,j}\langle g \mid A \mid j\rangle\langle j \mid B^* \mid g\rangle = \frac{1}{|G|}\sum_{g}\langle g \mid AB^* \mid g\rangle$$

$$= \frac{1}{|G|}\,\mathrm{tr}(AB^*) \qquad \square$$

If $A \in \mathcal{B}(\mathcal{F}(G))$ is an observable and $\rho \in \mathcal{D}(\mathcal{F}(G))$ then Lemma 7.2 shows that the expectation of A in the state ρ is

$$\mathrm{tr}(A\rho) = |G|\sum_{g,j} A(g;j)\overline{W(g;j)}$$

References

[1] S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda and R. Simon, Wigner distribution for finite dimensional quantum systems: An algebraic approach, 2005, quant-ph/0507094.

[2] R. Cleve and J. Watrous, Fast parallel circuits for the quantum Fourier transform, *Proceedings 41st Annual Symposium on Foundations of Computer Science*, vol. 454, 2000, 526–536.

[3] P. Diaconis and D. Rockmore, Efficient computation of the Fourier transform on finite groups,*J. Amer. Math. Soc.* **3** (1990), 297–332.

[4] M. Ettinger and P. Høyer, A quantum observable for the graph isomorphism problem, 1999, quant-ph/9901029.

[5] M. Ettinger and P. Høyer, On quantum algorithms for noncommutative hidden subgroup, *Advances in Applied Mathematics* **25** (2000), 239–251.

[6] M. Ettinger, P. Høyer and E. Knill, The quantum query complexity of the hidden subgroup problem is polynomial, *Information Processing Letters* **91** (2004), 43–48.

[7] M. Grigni, L. Schulman, M. Vazirani and U. Vazirani, Quantum mechanical algorithms for the nonabelian hidden subgroup problem, *Proc. 33rd ACM Symp. on Theory of Computing* 2001, 68–74.

[8] J. Gruska, *Quantum Computing*, McGraw-Hill, London, 1999.

[9] J. Harris and W. Fulton, *Representation Theory, Graduate Texts in Mathematics 129*, Springer-Verlag, New York, 1991.

[10] J. Köbler, U. Schöning and J. Torán, *The Graph Isomorphism Problem: Its Structural Complexity*, Birkhauser, Boston, 1993.

[11] G. Kuperberg, A subexponential-time algorithm for the dihedral hidden subgroup problem, 2003, quant-ph/0302112.

[12] S. Lomonaco and L. Kauffman, Quantum hidden subgroup problems: A mathematical perspective, 2002, quant-ph/0201095.

[13] C. Lomont, The hidden subgroup problem-review and open problems, 2004, quant-ph/0411037.

[14] G. Mackey, *Induced Representations and Quantum Mechanics*, Benjamin/Cummings, Reading, Mass., 1968.

[15] G. Mackey, *Unitary Group Representations in Physics, Probability and Number Theory*, Benjamin/Cummings, Reading, Mass., 1978.

[16] G. Miller, Graph isomorphism, general remarks, *J. Comp. Sys. Sci.* **18** (1979), 128–142.

[17] M. Nielsen and J. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[18] A. Pittenger, *An Introduction to Quantum Computing Algorithms*, Birkhäuser, Boston, 1999.

[19] J. Preskill, *Quantum Computation and Information*, California Institute of Technology, Pasadena, CA, 1998.

[20] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Computing* **26** (1997), 1484–1509.

[21] B. Simon, Representations of finite and compact groups, Graduate Studies in Mathematics 10, *American Mathematical Society*, 1996.

[22] J. Waltrous, Quantum algorithms for solvable groups, *Proc. 33rd ACM Symp. Theor. Comp.* 2001, 60–67.