FREE FUNCTIONS WITH SYMMETRY

DAVID CUSHING†
J. E. PASCOE‡
RYAN TULLY-DOYLE

Abstract. In 1936, Margarete C. Wolf showed that the ring of symmetric free polynomials in two or more variables is isomorphic to the ring of free polynomials in infinitely many variables. We show that Wolf's theorem is a special case of a general theory of the ring of invariant free polynomials: every ring of invariant free polynomials is isomorphic to a free polynomial ring. Furthermore, we show that this isomorphism extends to the free functional calculus as a norm-preserving isomorphism of function spaces on a domain known as the row ball. We give explicit constructions of the ring of invariant free polynomials in terms of representation theory and develop a rudimentary theory of their structures. Specifically, we obtain a generating function for the number of basis elements of a given degree and explicit formulas for good bases in the abelian case.

Contents

Date: September 5, 2014.
2010 *Mathematics Subject Classification.* Primary 46L52 Secondary 05E05, 13A50, 17A50, 47A63 and 47A56.
Key words and phrases. Invariant theory, symmetric functions in noncommuting variables, noncommuatative invariant theory and free analysis.

† Partially supported by an EPSRC DTA grant and a Capstaff award.
‡ Partially supported by National Science Foundation Grant DMS 1361720.

1. Introduction

A **symmetric free polynomial** in the letters $x_1, \ldots, x_d$ is a free polynomial p which satisfies

$$p(x_1, \ldots, x_d) = p(x_{\sigma(1)}, \ldots, x_{\sigma(d)})$$

for all permutations σ of $\{1, \ldots, d\}$. For example,

$$p(x_1, x_2) = x_1 + x_2 + 7x_1x_1 + 7x_2x_2 + 3x_1x_2 + 3x_2x_1$$

is a symmetric free polynomial in two variables. Classically, Wolf proved the following theorem about the structure of the ring of symmetric free polynomials [21].

Theorem 1.1 (Wolf)**.** *The symmetric free polynomials in $d \geq 2$ variables is isomorphic to the ring of free polynomials in infinitely many variables.*

More recently, free symmetric polynomials have been investigated by numerous authors [5, 7, 11], and some deep connections with representation theory are now known.

We are concerned with the ring of invariant free polynomials. Let G be a finite group. Let $\pi : G \to \mathcal{U}_d$ be a unitary representation. That is, π is a homomorphism from the group G to the group of $d \times d$ unitary matrices over $\mathbb{C}$. An **invariant free polynomial with respect to** π is a free polynomial $p \in \mathbb{C}\langle x_1, \ldots, x_d \rangle$ which satisfies

$$p(x_1, \ldots, x_d) = p(\pi(\sigma)(x_1, \ldots, x_d))$$

for all σ in G. (Here, the $d \times d$ matrices $\pi(\sigma)$ are acting on $(x_1, \ldots, x_d)$ by matrix multiplication. That is, for example, if

$$A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right),$$

we define $A(x_1, x_2) = (x_1 + 2x_2, 3x_1 + 4x_2)$.) Notably, the invariant free polynomials form an algebra, which is called the **ring of invariant free polynomials.**

For example, the symmetric free polynomials in d variables are obtained in the special case where $G = S_d$ a symmetric group, and we define $\pi : S_d \to \mathcal{U}_d$ be the representation satisfying

$$\pi(\sigma)e_i = e_{\sigma(i)},$$

where e_i is the i-th elementary basis vector for $\mathbb{C}^d$.

We now define the domains on which we intend to execute the function theory of invariant free polynomials. Fix an infinite dimensional separable Hilbert space $\mathcal{H}$. There is only one infinite dimensional separable Hilbert space up to isomorphism [9], so what follows will be independent of the exact choice. Let Λ be an index set. Let $\mathcal{C}^\Lambda$ be the set of $(X_\lambda)_{\lambda\in\Lambda}$, sequences of elements in $\mathcal{B}(\mathcal{H})$ indexed by Λ, such that

$$\sum_{\lambda\in\Lambda} X_\lambda X_\lambda^* < 1,$$

where $A < B$ means that $B - A$ is strictly positive definite and $A \leq B$ means that $B - A$ is positive semidefinite. Here the sum $\sum_{\lambda\in\Lambda} X_\lambda X_\lambda^*$ is required to be absolutely convergent in the weak operator topology and have $\sum_{\lambda\in\Lambda} X_\lambda X_\lambda^* < 1$, or equivalently, there is an $\varepsilon > 0$ such that for every finite $\Lambda' \subset \Lambda$,

$$\sum_{\lambda\in\Lambda'} X_\lambda X_\lambda^* \leq 1 - \varepsilon.$$

If $\Lambda = d$ is a natural number, we identify d as a set with d elements. That is, $\mathcal{C}^d$ is the set of d-tuples of operators in $\mathcal{B}(\mathcal{H})$ such that

$$\sum_{i=1}^{d} X_i X_i^* < 1.$$

Some authors refer to $\mathcal{C}^\Lambda$ as the **row ball**, or the set of **row contractions** [14, 18]. Given a free polynomial p in the letters $(x_\lambda)_{\lambda\in\Lambda}$ and a point $X = (X_\lambda)_{\lambda\in\Lambda} \in \mathcal{C}^\Lambda$, we form $p(X)$ via the formula

$$p(X) = p((X_\lambda)_{\lambda\in\Lambda}),$$

which when $\Lambda = d$ reduces to $p(X) = p(X_1, \ldots, X_d)$.

Let $\mathcal{R}$ be a subalgebra of $\mathbb{C}\langle x_1, \ldots, x_d\rangle$. We define a **basis** for $\mathcal{R}$ to be an indexed sequence $(u_\lambda)_{\lambda\in\Lambda}$ of free polynomials which generate $\mathcal{R}$ as an algebra, which is minimal in the sense that there is no $\Lambda' \subsetneq \Lambda$ such that the sequence $(u_\lambda)_{\lambda\in\Lambda'}$ generate $\mathcal{R}$ as an algebra. We note that any basis for $\mathcal{R}$ is *countable*, since $\mathcal{R}$ has countable dimension as a vector space as it is a subspace of $\mathbb{C}\langle x_1, \dots, x_d\rangle$, and the minimality condition implies that the $(u_\lambda)_{\lambda\in\Lambda}$ are linearly independent.

We prove the following theorem.

Theorem 1.2. *Let G be a finite group. Let $\pi : G \to \mathcal{U}_d$ be a unitary representation. There exists a basis for the ring of invariant free polynomials $(u_\lambda)_{\lambda\in\Lambda}$ such that the map Φ on $\mathcal{C}^d$ defined by the formula*

$$\Phi(X) = (u_\lambda(X))_{\lambda\in\Lambda}$$

satisfies the following properties:

- *The map Φ takes $\mathcal{C}^d$ to $\mathcal{C}^\Lambda$.*
- *Furthermore, for p in the ring of invariant free polynomials for π, there exists a unique free polynomial $\hat{p}$ such that $p = \hat{p} \circ \Phi$.*
- *Moreover,*

$$\sup_{X\in\mathcal{C}^d} \|p(X)\| = \sup_{U\in\mathcal{C}^\Lambda} \|\hat{p}(U)\|.$$

Namely, the map taking $\hat{p}$ to p is an isomorphism of rings from the free algebra $\mathbb{C}\langle x_\lambda\rangle_{\lambda\in\Lambda}$ to the ring of invariant free polynomials.

Theorem 1.2 follows from Theorems 4.2 and 6.4. We note that a similar result was obtained for free functions on the domain

$$\mathcal{B}^2 = \{(X_1, X_2) \in \mathcal{B}(\mathcal{H}) | \, \|X_i\| < 1\}$$

for symmetric free functions in two variables by Agler and Young [4].

In general, the basis in Theorem 1.2 is hard to compute. However, the number of elements of a certain degree is computed in Section 7.1. An explicit basis can be obtained if G is abelian, which we give in Section 7.2.

1.1. **Some examples.** We now give some concrete examples of what our main result says. First, we give an analogous theorem to that obtained in Agler and Young for symmetric free functions in two variables [4].

Proposition 1.3. *Let*

$$\Phi(X_1, X_2) = (A, B^2, BAB, \dots, BA^nB, \dots)$$

where

$$A = \frac{X_1 + X_2}{\sqrt{2}}, B = \frac{X_1 - X_2}{\sqrt{2}}.$$

The map Φ satisfies the following properties:

- *Φ takes $\mathcal{C}^2$ to $\mathcal{C}^{\mathbb{N}}$.*

- *For any free polynomial p such that*
$$p(X_1, X_2) = p(X_2, X_1),$$
there exists a unique free polynomial $\hat{p}$ such that $p = \hat{p} \circ \Phi$.
- *Moreover,*
$$\sup_{X \in \mathcal{C}^2} \|p(X)\| = \sup_{U \in \mathcal{C}^{\mathbb{N}}} \|\hat{p}(U)\|.$$

Another simple example concerns the ring of even functions in two variables, that is, the ring of free polynomials in two variables f satisfying the identity
$$f(X_1, X_2) = f(-X_1, -X_2).$$
Here the group G in Theorem 1.2 is the cyclic group with two elements, $\mathbb{Z}_2 = \{0, 1\}$, and the representation π is given by
$$\pi(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pi(1) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proposition 1.4. *Let*
$$\Phi(X_1, X_2) = (X_1X_1, X_1X_2, X_2X_1, X_2X_2).$$
The map Φ satisfies the following properties:
- *Φ takes $\mathcal{C}^2$ to $\mathcal{C}^4$.*
- *For any free polynomial p such that*
$$p(X_1, X_2) = p(-X_1, -X_2),$$
there exists a unique free polynomial $\hat{p}$ such that $p = \hat{p} \circ \Phi$.
- *Moreover,*
$$\sup_{X \in \mathcal{C}^2} \|p(X)\| = \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|.$$

We discuss Proposition 1.4 in detail in Section 2. Here we see a concrete trade-off between the number of variables and degree in the optimization of a free polynomial: finding the maximum norm of a polynomial in 4 variables of degree d on $\mathcal{C}^4$ is the same as finding the norm of an even polynomial in 2 variables of degree $2d$ on $\mathcal{C}^2$.

Both Proposition 1.3 and Proposition 1.4 follow from our basis construction in the abelian case given in Theorem 7.4.

1.2. **Geometry.** Although the image of the map Φ in Theorem 1.2 may have high codimension, in the sense that it is far from being literally surjective, the function $\hat{f}$ is completely determined by f and has the same norm. We view this as an analogue of the celebrated work of Agler and McCarthy on norm preserving extensions of functions on varieties to whole domains [2, 1]. Additionally, since f totally determines

$\hat{f}$, the dimension of the Zariski closure of the image of a free polynomial map can apparently go up, in contrast with the commutative case [12]. Exploiting the aforementioned phenomenon is a critical step in the theory of change of variables for free polynomials and their generalizations, the free functions, which had been thought to be extremely rigid [13].

To prove Theorem 1.2, we develop a geometric theory of the ring of invariant free functions. As a consequence of the geometric structure, the ring of free invariant polynomials is always free (but perhaps infinitely generated), in contrast with the Chevalley-Shepard-Todd Theorem in the commutative case, in which freeness depends on the structure of G [8, 20].

1.3. **Free analysis.** A **free function on** $\mathcal{C}^\Lambda$ is a function from $\mathcal{C}^\Lambda$ to $\mathcal{B}(\mathcal{H})$ which is the uniform limit of free polynomials on the sets $r\overline{\mathcal{C}^\Lambda}$. We let $H(\mathcal{C}^\Lambda)$ denote the **algebra of free functions on** $\mathcal{C}^\Lambda$. The **Banach algebra of bounded free functions** $H^\infty(\mathcal{C}^\Lambda) \subset H(\mathcal{C}^\Lambda)$ is the space of all bounded functions in $H(\mathcal{C}^\Lambda)$ equipped with the norm

$$\|p\| = \sup_{X \in \mathcal{C}^\Lambda} \|p(X)\|.$$

We note that there are many equivalent characterizations of a free function, such as [3, 14, 15, 18].

We can reinterpret Theorem 1.2 as an isomorphism of function algebras analogous to Wolf's theorem. Let $H^\infty_\pi(\mathcal{C}^d)$ be the Banach algebra of bounded invariant free functions for π on $\mathcal{C}^d$.

Corollary 1.5. *There is a countable set* Λ *such that*

$$H^\infty_\pi(\mathcal{C}^d) \cong H^\infty(\mathcal{C}^\Lambda)$$

as Banach algebras.

Corollary 1.5 follows from Theorem 1.2 directly. That is, the map taking $\hat{f} \in H^\infty(\mathcal{C}^\Lambda)$ to $\hat{f} \circ \Phi \in H^\infty_\pi(\mathcal{C}^d)$ is such an isomorphism. The map is injective and surjective since it is already since it is an isomorphism on the level of formal power series, which uniquely define a free function [15].

2. Example: An even free function in two variables

To begin, we discuss a simple nontrivial example of a free ring of invariants. We will now explain what our main result, Theorem 1.2, says about a specific even free polynomial in two variables.

We say a free polynomial $p \in \mathbb{C}\langle x_1, x_2 \rangle$ is **even** if

$$p(X_1, X_2) = p(-X_1, -X_2).$$

We note that the even free functions form an algebra.

Consider the even free polynomial

$$p(X) = p(X_1, X_2) = 1 + 3X_1X_2 - 7X_1X_1 - X_2X_1X_2X_2$$

as a map on the domain $\mathcal{C}^2$.

We first note that it is clearly not a coincidence that p has no odd degree terms. Furthermore, if we let

$$\begin{aligned} u_1(X) = X_1X_1, \quad u_2(X) = X_1X_2, \\ u_3(X) = X_2X_1, \quad u_4(X) = X_2X_2, \end{aligned}$$

we get that

$$p(X) = 1 + 3u_2(X) - 7u_1(X) - u_3(X)u_4(X).$$

Let

$$\hat{p}(U) = \hat{p}(U_1, U_2, U_3, U_4) = 1 + 3U_2 - 7U_1 - U_3U_4$$

and

$$\Phi(X) = (X_1X_1, X_1X_2, X_2X_1, X_2X_2).$$

Thus,

$$p(X) = \hat{p} \circ \Phi(X).$$

We are interested in the analytical properties of $\hat{p}$ and Φ.

We will show the remarkable fact that

$$\Phi(\mathcal{C}^2) \subset \mathcal{C}^4.$$

Let $X \in \mathcal{C}^2$. That is,

$$XX^* = X_1X_1^* + X_2X_2^* < 1.$$

Since

$$\Phi(X) = (X_1X_1, X_1X_2, X_2X_1, X_2X_2)$$

we get that

$$\begin{aligned} \Phi(X)\Phi(X)^* &= X_1X_1(X_1X_1)^* + X_1X_2(X_1X_2)^* + X_2X_1(X_2X_1)^* \\ &\qquad + X_2X_2(X_2X_2)^* \\ &= X_1X_1X_1^*X_1^* + X_1X_2X_2^*X_1^* + X_2X_1X_1^*X_2^* + X_2X_2X_2^*X_2^* \\ &= X_1(X_1X_1^* + X_2X_2^*)X_1^* + X_2(X_1X_1^* + X_2X_2^*)X_2^* \\ &\leq X_1X_1^* + X_2X_2^* \\ &< 1. \end{aligned}$$

Thus, $\Phi(\mathcal{C}^2) \subset \mathcal{C}^4$.

We will now show a curious equality:

$$\sup_{X \in \mathcal{C}^2} \|p(X)\| = \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|.$$

First we show that

$$\sup_{X \in \mathcal{C}^2} \|p(X)\| \geq \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|.$$

Since p is a free polynomial and is thus continuous on the closure $\overline{\mathcal{C}^2} \subset \mathcal{B}(\mathcal{H})^2$, it is enough to show that

$$\sup_{X \in \overline{\mathcal{C}^2}} \|p(X)\| \geq \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|.$$

Let $(U_1, U_2, U_3, U_4) \in \mathcal{C}^4$. Define operators X_1 and X_2 with the following block structure

$$X_1 = \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$X_2 = \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

First,

$$\begin{aligned} X_1X_1^* + X_2X_2^* &= \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}^* + \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}^* \\ &= \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ U_1^* & 0 & 0 \\ U_2^* & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ U_3^* & 0 & 0 \\ U_4^* & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} U_1U_1^*+U_2U_2^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} U_3U_3^*+U_4U_4^* & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} U_1U_1^*+U_2U_2^*+U_3U_3^*+U_4U_4^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &\leq 1. \end{aligned}$$

That is, $(X_1, X_2) \in \overline{\mathcal{C}^2}$. Note

$$X_1X_1 = \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} U_1 & 0 & 0 \\ 0 & U_1 & U_2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$X_1X_2 = \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} U_2 & 0 & 0 \\ 0 & U_3 & U_4 \\ 0 & 0 & 0 \end{pmatrix}$$

$$X_2X_1 = \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & U_1 & U_2 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} U_3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & U_1 & U_2 \end{pmatrix}$$

$$X_2X_2 = \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & U_3 & U_4 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} U_4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & U_3 & U_4 \end{pmatrix}.$$

That is,

$$\Phi(X) = \left(\begin{smallmatrix} U & 0 \\ 0 & \tilde{J} \end{smallmatrix}\right)$$

where $\tilde{J}$ denotes some matrix tuple which is irrelevant to our aims. So,

$$\begin{aligned} p(X_1, X_2) &= (\hat{p} \circ \Phi)(X_1, X_2) \\ &= \hat{p}(X_1X_1, X_1X_2, X_2X_1, X_2X_2) \\ &= \begin{pmatrix} \hat{p}(U) & 0 \\ 0 & \hat{p}(\tilde{J}) \end{pmatrix}. \end{aligned}$$

Namely,

$$\|p(X)\| \geq \|\hat{p}(U)\|.$$

Thus,

$$\sup_{X \in \overline{\mathcal{C}^2}} \|p(X)\| \geq \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|.$$

To see that

$$\sup_{X \in \mathcal{C}^2} \|p(X)\| \leq \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|,$$

note that since $\Phi(X) \in \mathcal{C}^4$,

$$\begin{aligned} \sup_{X \in \mathcal{C}^2} \|p(X)\| &= \sup_{X \in \mathcal{C}^2} \|\hat{p}(\Phi(X))\| \\ &\leq \sup_{U \in \mathcal{C}^4} \|\hat{p}(U)\|. \end{aligned}$$

3. The space of free polynomials as an inner product space

We now seek to understand the geometry of free polynomials as a Hilbert space.

Definition 3.1. We define H^2_d to be the Hilbert space of free formal power series in d variables whose coefficients are in ℓ^2. We define $[H^2_d]_n$ to be the subspace of homogeneous free polynomials of degree n. For a free polynomial f in d variables, we define M_f to be the operator on H^2_d satisfying $M_f g = fg$.

The following lemma describes a grading structure on H^2_d.

Lemma 3.2 (Grading lemma)**.** *Let p, q be homogenous free polynomials of degree n and r, s be homogenous free polynomials of degree m. Then,*

$$\langle pr, qs \rangle = \langle p, q \rangle \langle r, s \rangle .$$

Thus, we identify $[H^2_d]_n \otimes [H^2_d]_m = [H^2_d]_{n+m}$.

Proof. Write

$$p(X) = \sum_{I \in \mathcal{I}_n} p_I X^I, q(X) = \sum_{I \in \mathcal{I}_n} q_I X^I,$$
$$r(X) = \sum_{J \in \mathcal{I}_m} r_J X^J, s(X) = \sum_{J \in \mathcal{I}_m} s_J X^J,$$

where $\mathcal{I}_k$ is the set of free multi-indicies of degree k. Observe that $\langle p, q\rangle = \sum_{I \in \mathcal{I}_n} p_I \overline{q_I}$ and $\langle r, s\rangle = \sum_{J \in \mathcal{I}_m} r_J \overline{s_J}$, which gives

$$\langle p, q\rangle \langle r, s\rangle = \sum_{I \in \mathcal{I}_n} \sum_{J \in \mathcal{I}_m} p_I \overline{q_I} r_J \overline{s_J}.$$

Observe that

$$p(X)r(X) = \sum_{I \in \mathcal{I}_n} \sum_{J \in \mathcal{I}_m} p_I r_J X^{IJ},$$
$$q(X)s(X) = \sum_{I \in \mathcal{I}_n} \sum_{J \in \mathcal{I}_m} q_I s_J X^{IJ},$$

which gives

$$\langle pr, qs\rangle = \sum_{I \in \mathcal{I}_n} \sum_{J \in \mathcal{I}_m} p_I r_J \overline{q_I s_J} = \langle p, q\rangle \langle r, s\rangle .$$

□

Corollary 3.3. *Let V be a subspace of $[H^2_d]_n$. Let $u_1, \ldots, u_k$ be an orthonormal basis for V and $v_1, \ldots, v_k$ be an orthonormal basis for V. Then,*

$$\sum u_k(X)u_k(X)^* = \sum v_k(X)v_k(X)^*.$$

Proof. Let $m_X = (X^I)_{|I|=n}$ be the row vector of free monomials of degree n. Note that, for any $p \in [H^2_d]_n$,

$$p(X)p(X)^* = m_X \overset{pp^*}{\underset{1}{\otimes}} m_X.$$

For example, if we took the polynomial $p = x_1 + 2x_2$, identifying $[H^2_2]_1$ with $\mathbb{C}^2$ we get that

$$p(X)p(X)^* = \begin{pmatrix} X_1 & X_2 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} X_1^* \\ X_2^* \end{pmatrix}.$$

So we get that

$$\sum u_i(X)u_i(X)^* = \sum m_X \overset{u_i u_i^*}{\underset{1}{\otimes}} m_X = m_X \overset{\sum u_i u_i^*}{\underset{1}{\otimes}} m_X.$$

Note that $\sum u_i u_i^*$ is the orthogonal projection onto V, and thus did not depend on the choice of basis, so we are done. □

4. Superorthogonality

We can now define superorthogonality. We will later see that the ring of invariant free polynomials is itself superorthogonal.

Definition 4.1. An algebra $\mathcal{A} \subseteq \mathbb{C}\langle x_1, \ldots, x_d\rangle$ is called **superorthogonal** if there exists a superorthonormal basis for $\mathcal{A}$, i.e. a basis $(u_\lambda)_{\lambda\in\Lambda}$ for $\mathcal{A}$ such that u_λ are homogeneous polynomials, $\|u_\lambda\|_{\mathcal{H}^2_d} = 1$, and for all $\lambda, \mu \in \Lambda$,

$$u_\lambda H^2_d \perp u_\mu H^2_d.$$

The goal of this section is to prove that a general version of Theorem 1.2 is true for superorthogonal algebras.

Theorem 4.2. *Let $\mathcal{A}$ be a superorthogonal algebra. Let $(u_\lambda)_{\lambda\in\Lambda}$ be a superorthogonal basis. The map Φ on $\mathcal{C}^d$ defined by the formula*

$$\Phi(X) = (u_\lambda(X))_{\lambda\in\Lambda}$$

satisfies the following properties:

- *The map Φ takes $\mathcal{C}^d$ to $\mathcal{C}^\Lambda$.*
- *Furthermore, for p in the ring of invariant free polynomials for π, there exists a unique free polynomial $\hat{p}$ such that $p = \hat{p} \circ \Phi$.*
- *Moreover,*

$$\sup_{X\in\mathcal{C}^d} \|p(X)\| = \sup_{U\in\mathcal{C}^\Lambda} \|\hat{p}(U)\|.$$

Namely, the map taking $\hat{p}$ to p is an isomorphism of rings from the free algebra $\mathbb{C}\langle x_\lambda\rangle_{\lambda\in\Lambda}$ to $\mathcal{A}$.

Theorem 4.2 follows from Lemma 4.3 and Lemma 4.5.

We now show that superorthogonal algebras are necessarily free.

Lemma 4.3. *A superorthogonal algebra $\mathcal{A}$ is isomorphic to a free algebra in perhaps infinitely many variables. Specifically, the map*

$$\varphi : \mathbb{C}\langle x_\lambda\rangle_{\lambda\in\Lambda} \to \mathcal{A}$$

satisfying $\varphi(x_\lambda) = u_\lambda$ is an isomorphism.

Proof. Note that it is enough to show that for any two distinct products $\prod_{i=1}^n u_{\lambda_i}, \prod_{j=1}^m u_{\kappa_j}$ of the same degree as free polynomials in $\mathcal{A} \subset \mathbb{C}\langle x_1, \ldots, x_d\rangle$ that

$$\left\langle \prod_{i=1}^n u_{\lambda_i}, \prod_{j=1}^m u_{\kappa_j} \right\rangle = 0,$$

since then the words in u_λ are linearly independent. Since the words are distinct, there is a p such that $\lambda_i = \kappa_i$ for all $i < p$ and $\lambda_p \neq \kappa_p$. So,

$$\left\langle \prod_{i=1}^{n} u_{\lambda_i}, \prod_{j=1}^{m} u_{\kappa_j} \right\rangle = \left\langle \prod_{i=1}^{p-1} u_{\lambda_i}, \prod_{j=1}^{p-1} u_{\kappa_j} \right\rangle \left\langle \prod_{i=p}^{n} u_{\lambda_i}, \prod_{j=p}^{m} u_{\kappa_j} \right\rangle .$$

Note that $\prod_{i=p}^{n} u_{\lambda_i} \in u_{\lambda_p} H^2_d$ and $\prod_{j=p}^{m} u_{\kappa_j} \in u_{\kappa_p} H^2_d$ which implies that the two products are orthogonal since u_{λ_p} and u_{κ_p} are superorthogonal and thus the desired inner product is 0. □

We now show that the superothogonal basis maps $\mathcal{C}^d$ into $\mathcal{C}^\Lambda$.

Lemma 4.4. *Let $\mathcal{A}$ be a superorthogonal algebra. For a superorthonormal basis (u_λ), the map $\Phi : \mathcal{C}^d \to \mathcal{B}(\mathcal{H})^\Lambda$ given by*

$$\Phi(x) = (u_\lambda(x))_{\lambda \in \Lambda}$$

has $\operatorname{ran} \Phi \subseteq \mathcal{C}^\Lambda$*, that is*

$$\Phi : \mathcal{C}^d \to \mathcal{C}^\Lambda.$$

We call Φ the **superorthogonal basis map***.*

Proof. Let $X \in \mathcal{C}^d$. That is,

$$\sum_{i=1}^{d} X_i X_i^* < 1.$$

Let $\mathcal{I}$ be the left ideal generated by $\mathcal{A} \setminus \{1\}$ in $\mathbb{C}\langle x_1, \ldots, x_d\rangle$, that is, the span of the elements of the form ab where $a \in \mathcal{A} \setminus \{1\}$ and $b \in \mathbb{C}\langle x_1, \ldots, x_d\rangle$.

To show that

$$\sum_{\lambda \in \Lambda} u_\lambda(X) u_\lambda(X)^* < 1,$$

we will show by induction that

$$\sum_{\lambda \in \Lambda, \deg u_\lambda \leq n} u_\lambda(X) u_\lambda(X)^* + \sum_{i=1}^{k_n} w_{i,n}(X) w_{i,n}(X)^* \leq \sum_{i=1}^{d} X_i X_i^* \tag{4.1}$$

where $w_{i,n}$ form an orthonormal basis for $(\mathcal{I} \cap [H^2_d]_n)^\perp$.

Note that for $n = 1$, Equation (4.1) becomes

$$\sum_{\lambda \in \Lambda, \deg u_\lambda = 1} u_\lambda(X) u_\lambda(X)^* + \sum_{i=1}^{k_1} w_{i,1}(X) w_{i,1}(X)^* = \sum_{i=1}^{d} X_i X_i^*$$

which holds by Lemma 3.3 since the set of u_λ of degree one combined with the set of $w_{i,1}$ must form a basis for $[H^2_d]_1$.

Now suppose that Equation (4.1) holds for n. That is,

$$\sum_{\lambda\in\Lambda,\deg\, u_\lambda\leq n} u_\lambda(X)u_\lambda(X)^* + \sum_{i=1}^{k_n} w_{i,n}(X)w_{i,n}(X)^* \leq \sum_{i=1}^{d} X_iX_i^*.$$

We will now show that it holds for $n+1$. Since

$$\sum_{i=1}^{d} X_iX_i^* < 1,$$

we get that

$$\sum_{\substack{\lambda\in\Lambda,\\ \deg\, u_\lambda\leq n}} u_\lambda(X)u_\lambda(X)^* + \sum_{i=1}^{k_n} w_{i,n}(X)(\sum_{j=1}^{d} X_jX_j^*)w_{i,n}(X)^* \leq \sum_{i=1}^{d} X_iX_i^*.$$

So

$$\sum_{\lambda\in\Lambda,\deg\, u_\lambda\leq n} u_\lambda(X)u_\lambda(X)^* + \sum_{i=1,j=1}^{k_n,d} w_{i,n}(X)X_jX_j^*w_{i,n}(X)^* \leq \sum_{i=1}^{d} X_iX_i^*.$$

Note that any u_λ of degree $n+1$ must be in the subspace $(\mathcal{I}\cap[H^2_d]_n)^\perp\otimes[H^2_d]_1$ by the definition of superorthogonality. Furthermore, the combination of the u_λ of degree $n+1$ and $w_{i,n+1}$ form an orthonormal basis for $(\mathcal{I}\cap[H^2_d]_n)^\perp\otimes[H^2_d]_1$. On the other hand, the $w_{i,n}x_j$ form an orthonormal basis for $(\mathcal{I}\cap[H^2_d]_n)^\perp\otimes[H^2_d]_1$. So, by Lemma 3.3, we get that

$$\sum_{i=1,j=1}^{k_n,d} w_{i,n}(X)X_jX_j^*w_{i,n}(X)^* =$$

$$\sum_{\substack{\lambda\in\Lambda,\\ \deg\, u_\lambda=n+1}} u_\lambda(X)u_\lambda(X)^* + \sum_{i=1}^{k_{n+1}} w_{i,n+1}(X)w_{i,n+1}(X)^*,$$

which immediately implies that

$$\sum_{\lambda\in\Lambda,\deg\, u_\lambda\leq n+1} u_\lambda(X)u_\lambda(X)^* + \sum_{i=1}^{k_{n+1}} w_{i,n+1}(X)w_{i,n+1}(X)^* \leq \sum_{i=1}^{d} X_iX_i^*.$$

□

Lemma 4.5. *Let $\mathcal{A}$ be a superorthogonal algebra. Let $p\in\mathcal{A}$. Then there exists a unique free polynomial $\hat{p}$ such that*

$$\hat{p}\circ\Phi = p,$$

where Φ is a superorthonormal basis map for $\mathcal{A}$ as in Lemma 4.4. Furthermore,

$$\sup_{X \in \mathcal{C}^d} \|p(X)\| = \sup_{U \in \mathcal{C}^\Lambda} \|\hat{p}(U)\|.$$

Proof. The existence of $\hat{p}$ follows from the fact that the coordinates of Φ form a basis for $\mathcal{A}$. The uniqueness of $\hat{p}$ follows from the fact that $\mathcal{A}$ is free by Lemma 4.3.

So it remains to show the equality

$$\sup_{X \in \mathcal{C}^d} \|p(X)\| = \sup_{U \in \mathcal{C}^\Lambda} \|\hat{p}(U)\|.$$

To show that

$$\sup_{X \in \mathcal{C}^d} \|p(X)\| \geq \sup_{U \in \mathcal{C}^\Lambda} \|\hat{p}(U)\|,$$

we show the equivalent inequality

$$\sup_{X \in \overline{\mathcal{C}^d}} \|p(X)\| \geq \sup_{U \in \mathcal{C}^\Lambda} \|\hat{p}(U)\|.$$

Similarly to our example for even functions (Section 2), given a $U \in \mathcal{C}^\Lambda$ we would like to find an $X \in \overline{\mathcal{C}^d}$ such that there is some projection P so that

$$P\hat{p}(\Phi(X))P = \hat{p}(U) \tag{4.2}$$

and thus that

$$\|p(X)\| \geq \|\hat{p}(U)\|.$$

Let

$$M_x = (M_{x_1}, \ldots, M_{x_d})$$

as in Definition 3.1. Note that $M_x \in \overline{\mathcal{C}^d}$. So, $\Phi(M_x) = (M_{u_\lambda})_{\lambda \in \Lambda}$. Decompose $H^2_d = \overline{\mathcal{A}}^{H^2_d} \oplus \mathcal{J}$. Since the algebra $\mathcal{A}$ is a joint invariant subspace for all the M_{u_λ}, we get that

$$M_{u_\lambda} = \begin{pmatrix} M_{x_\lambda} & J_\lambda \\ 0 & K_\lambda \end{pmatrix}$$

with respect to the decomposition, where J_λ and K_λ are some operators which will be irrelevant to this discussion. The Frazho-Popescu dilation theorem [10, 17] states that for any $U \in \mathcal{C}^\Lambda$, there is a projection $\tilde{P}$ such that for any free polynomial q,

$$\tilde{P}q((M_{x_\lambda} \otimes I))\tilde{P} = q(U).$$

Thus, there is indeed an X and a projection as desired in (4.2), namely, taking $X = (M_{x_1} \otimes I, \ldots, M_{x_d} \otimes I)$ and the projection as constructed above.

Thus, for every $U \in \mathcal{C}^\Lambda$ there exists an $X \in \overline{\mathcal{C}^d}$ such that

$$\|p(X)\| \geq \|\hat{p}(U)\|$$

and so

$$\sup_{X\in\overline{\mathcal{C}^d}} \|p(X)\| \geq \sup_{U\in\mathcal{C}^\Lambda} \|\hat{p}(U)\|.$$

To see that

$$\sup_{X\in\mathcal{C}^d} \|p(X)\| \leq \sup_{U\in\mathcal{C}^\Lambda} \|\hat{p}(U)\|$$

we note that $\Phi(X) \in \mathcal{C}^\Lambda$ by Lemma 4.4. □

Now Theorem 4.2 follows immediately.

5. Example: Free functions in three variables invariant under the natural action of the cyclic group with three elements

We now show how to construct a superorthonormal basis for the ring of free polynomials in three variables which are invariant under the natural action of the free group. That is, we want to understand free functions which satisfy the identity

$$f(X_1, X_2, X_3) = f(X_2, X_3, X_1)$$

and show that they form a superorthogonal algebra.

Let σ denote a generator of the cyclic group with three elements. Define the action of σ on free functions in three variables by

$$(\sigma \cdot f)(X_1, X_2, X_3) = f(X_2, X_3, X_1).$$

With this notation we are trying to understand functions such that

$$\sigma \cdot f = f.$$

Let ω be a nontrivial third root of unity. Consider the following three linear polynomials:

$$u_0(X_1, X_2, X_3) = \frac{X_1 + X_2 + X_3}{\sqrt{3}}$$
$$u_1(X_1, X_2, X_3) = \frac{X_1 + \omega X_2 + \overline{\omega} X_3}{\sqrt{3}}$$
$$u_{-1}(X_1, X_2, X_3) = \frac{X_1 + \overline{\omega} X_2 + \omega X_3}{\sqrt{3}}.$$

Clearly, the function u_0 is fixed by the natural action of the cyclic group with three elements. However,

$$\sigma \cdot u_1 = \omega u_1,$$

and

$$\sigma \cdot u_{-1} = \overline{\omega} u_1.$$

That is, they are *eigenfunctions* of the action σ on free polynomials in three variables.

In fact, any product of the u_i will be an eigenfunction of the action of σ. For example,

$$\sigma \cdot (u_{-1}u_1u_1) = \omega u_{-1}u_1u_1.$$

Thus, it can be observed that $\prod_j u_{i_j}$ is in the ring of invariant free polynomials under the action of the cyclic group with three elements if and only if $\sum_j i_j \equiv_3 0$, and furthermore that products satisfying this condition span the algebra of free polynomials in three variables which are fixed by the natural action of the cyclic group with three elements.

So, if we choose products $\prod_{j=1}^N u_{i_j}$ such that $\sum_j i_j \equiv_3 0$, which are primitive in that no partial product $\prod_{j=1}^n u_{i_j}$ is in the ring of invariant free polynomials, we will obtain a basis for our algebra. To show that this basis is superorthogonal, it is enough to show that any two distinct products $\prod_{j=1}^N u_{i_j}$, $\prod_{j=1}^N u_{k_j}$ are orthogonal. However, by the grading lemma,

$$\left\langle \prod_{j=1}^N u_{i_j}, \prod_{j=1}^N u_{k_j} \right\rangle = \prod_{j}^N \left\langle u_{i_j}, u_{k_j} \right\rangle.$$

Since the two products were assumed to be not equal, the orthogonality of the u_i implies that at least one of the $\left\langle u_{i_j}, u_{k_j} \right\rangle = 0$, so we are done.

For the action of a general finite group, an explicit construction of a superorthogonal basis for the ring of invariants is more difficult. However, the existence of such a basis can be established using some basic representation theory which we do in the next section. Later, we will return to the issue of an explicit construction for specific classes of groups for which the problem is tractible.

6. The ring of invariant free polynomials is superorthogonal

In order to prove Theorem 1.2 by Theorem 4.2, it is sufficient to show that the ring of invariant free polynomials is superorthogonal.

Definition 6.1. Let π be a unitary representation of a finite group G. Let π_n denote the action of π on $[H^2_d]_n$. We make the identification that $\pi_1 = \pi$.

Let $p \in [H^2_d]_n$ and $q \in [H^2_d]_m$. Note that

$$\pi_{n+m} \cdot pq = (\pi_n \cdot p)(\pi_m \cdot q),$$

which translates to the following formal observation by the grading lemma.

Observation 6.2. *Let π be a unitary representation of a finite group G. Then,*

$$\pi_n \otimes \pi_m = \pi_{n+m}$$

with the identification made in the grading lemma.

Observation 6.2 implies that the action on homogeneous polynomials of degree n is determined by the action on homogeneous polynomials of degree 1.

Corollary 6.3. *Let π be a unitary representation of a finite group G. Then,*

$$\pi_n = \pi^{\otimes n}$$

with the identification made in the grading lemma.

We can now prove that the ring of invariant free polynomials is superorthogonal by constructing a basis for it.

Theorem 6.4. *Let G be a finite group. Let $\pi : G \to U_d$ be a group representation. The ring of invariant free polynomials for π is superorthogonal.*

Proof. The action of the group on homogeneous polynomials of degree i is given by $\pi^{\otimes i}(g) = \pi_i(g)$. To show that the ring of invariant free polynomials is superorthogonal, we construct a superorthogonal basis recursively.

Let $V_1 = [H^2_d]_1$, and if $i > 1$, let

$$V_i = \tilde{V}_{i-1}^{\perp} \otimes [H^2_d]_1,$$

where $\tilde{V}_{i-1}$ is defined as follows. For each i, consider $\tilde{\pi}_i = \pi_i|_{V_i}$ and decompose $V_i = \tilde{V}_i \oplus \tilde{V}_i^{\perp}$, where $\tilde{V}_i$ is the space which is fixed by the action of $\tilde{\pi}_i$.

Let $(u_{i,k})$ be an orthonormal basis of V_i. We will show that for all p, q in the ring of invariant free polynomials,

$$u_{i,k}p \perp u_{j,l}q$$

for $j \leq i$, i.e. that $u_{i,k}$ and $u_{j,l}$ are superorthogonal.

When $i = j$, for $l \neq k$, by the grading lemma,

$$\begin{aligned} \langle u_{i,k}p, u_{j,l}q \rangle &= \langle u_{i,k}, u_{j,l} \rangle \langle p, q \rangle \\ &= 0. \end{aligned}$$

When $j < i$, by the recursive construction, $u_{i,k} \in \tilde{V}_j^{\perp} \otimes [H^2_d]_1^{\otimes a}$ and $u_{j,l} \in \tilde{V}_j \otimes [H^2_d]_1^{\otimes b}$ for some a, b, and therefore

$$\langle u_{i,k}p, u_{j,l}q \rangle = 0.$$

To show that our recursively generated sequence $(u_{i,k})$ is a basis, consider the following. If $p \in [H^2_d]_n$ is in the ring of invariant free polynomials, note that the projection of p onto any $u_{i,k}[H^2_d]_{n-i}$ is in the ring of invariant free polynomials. So for any p in the ring of invariant free polynomials,

$$p = \sum u_{i,k} q_{i,k} + r,$$

where $q_{i,k}$ is in the ring of invariant free polynomials, and $r \in \tilde{V_n}^{\perp}$ and in the ring of invariants. So, by construction, $r = 0$. □

7. Structure of the superorthogonal basis for the ring of invariants

7.1. **Counting.** We now calculate the number of elements in any superorthonormal basis for the ring of invariant free polynomials of a given degree in terms of generating functions. The main result of this section is as follows.

Theorem 7.1. *Let π be a unitary representation of a group G and $\chi = \operatorname{tr} \pi$ be the character corresponding to π. Let $\mathcal{C}_G$ be a set of representatives for the conjugacy classes of G. Let g_n be the number of free polynomials of degree n in some superorthogonal basis for the ring of invariant free polynomials of π. Then,*

$$g(z) = \sum_{n=0}^{\infty} g_n z^n = 1 - |G| \frac{\prod_{\sigma \in \mathcal{C}_G}(1 - \chi(\sigma)z)}{\sum_{\tau \in \mathcal{C}_G} \#C_\tau \prod_{\sigma \neq \tau}(1 - \chi(\sigma)z)}$$

where $\#C_\tau$ denotes the number of elements in the conjugacy class of τ.

Namely, the number of generators of a given degree is independent of the choice of superorthogonal basis.

We prove Theorem 7.1 in Section 7.1.1.

For example, consider symmetric functions in three variables. That is, take the group S_3 acting on $\mathbb{C}^3$ via the representation $\pi(\sigma)e_i = e_{\sigma(i)}$. According to Theorem 7.1, the necessary information can be conveniently compiled in the following table.

	e	$(1\ 2)$	$(1\ 2\ 3)$
χ	3	1	0
$\#C_\sigma$	1	3	2

So,

$$\begin{aligned}
g(z) &= 1 - 6\frac{(1-3z)(1-z)(1-0z)}{(1-z)(1-0z)+3(1-3z)(1-0z)+2(1-z)(1-3z)}, \\
&= \frac{z-2z^2}{1-3z+z^2}, \\
&= z + z^2 + 2z^2 + 5z^3 + 13z^4 + ..., \\
&= z + \sum_{n=2}^{\infty} F_{2n-3} z^n,
\end{aligned}$$

where F_n denotes the n-th Fibonacci number.

Thus, in general, with the help of computer algebra software, it is a simple exercise to calculate the number of free polynomials of degree n in some superorthogonal basis for the ring of invariant free polynomials of π.

7.1.1. *The proof of Theorem 7.1.* Let f_n be the dimension of invariant homogeneous free polynomials of degree n. Let g_n be the number of free polynomials of degree n in some superorthogonal basis for the ring of invariant free polynomials of π. Let

$$g(z) = \sum_{n=0}^{\infty} g_n z^n, f(z) = \sum_{n=0}^{\infty} f_n z^n.$$

Lemma 7.2.

$$g(z) = \frac{f(z)-1}{f(z)}.$$

Proof. It can be shown using enumerative combinatorics that

$$f_n = \sum_{i_1+...+i_k=n} \prod_{1}^{k} g_{i_j}.$$

Thus,

$$\begin{aligned}\frac{1}{1-g(z)} &= \frac{1}{1-\sum_{n=0}^{\infty} g_n z^n} \\ &= \sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} g_n z^n\right)^m \\ &= \sum_{l=0}^{\infty} \sum_{i_1+\ldots+i_k=n} \prod_{1}^{k} g_{i_j} z^l \\ &= \sum_{n=0}^{\infty} f_n z^n \\ &= f(z).\end{aligned}$$

Calculating g from f gives that

$$g(z) = \frac{f(z)-1}{f(z)}.$$

□

In order to calculate f_n, we use character theory (see Serre [19, Chapter 2]).

Let ρ be a representation for G. For each $\sigma \in G$, put $\chi_\rho(g) = \operatorname{tr}(\rho(\sigma))$. χ_ρ is the **character** of ρ. Let ϕ_1, ϕ_2 be functions from G into $\mathbb{C}$. The scalar product $\langle \cdot, \cdot \rangle$ is defined by

$$\langle \phi_1, \phi_2 \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \phi_1(\sigma)\overline{\phi_2(\sigma)}.$$

Let $\tau : G \to \mathcal{U}_1$ be the trivial representation. The dimension of the space of fixed vectors of the action of ρ is given by $\langle \chi_\rho, \tau \rangle$. (See Serre [19, Chapter 2])

We make the identification $\chi = \chi_\pi$.

Lemma 7.3.

$$f(z) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{1-\chi(\sigma) z}.$$

Proof. By Lemma 6.3, the action of π on homogenous polynomials is given by $\pi^{\otimes n}$.

$$\begin{aligned} f(z) &= \sum_{n=0}^{\infty} f_n z^n \\ &= \sum_{n=0}^{\infty} \langle \chi^n, \tau \rangle z^n \\ &= \frac{1}{|G|} \sum_{n=0}^{\infty} \sum_{\sigma \in G} \chi(\sigma)^n \overline{\tau(\sigma)} z^n \\ &= \frac{1}{|G|} \sum_{n=0}^{\infty} \sum_{\sigma \in G} (\chi(\sigma) z)^n \\ &= \frac{1}{|G|} \sum_{\sigma \in G} (1 - \chi(\sigma) z)^{-1}. \\ &= \frac{1}{|G|} \sum_{\sigma \in \mathcal{C}_G} \frac{\# C_\sigma}{1 - \chi(\sigma) z}. \end{aligned}$$

□

Now Theorem 7.1 follows as an immediate corollary of Lemma 7.2 and Lemma 7.3.

7.2. **The ring of invariants of a finite abelian group.**

Theorem 7.4. *Let G be a locally compact abelian group, and let $\pi : G \to U_d$ be a unitary representation of G. Let $v_1, \ldots, v_d$ be an orthonormal set of vectors of $[H^2_d]_1$ with corresponding characters $\chi_1, \ldots, \chi_d$ such that $\pi(g) v_i = \chi_i(g) v_i$. A basis for the free ring of invariants as a vector space is given by*

$$B = \left\{ v^J | \chi^J = \tau \right\}.$$

Furthermore,

$$\tilde{B} = \left\{ v^I \in B | \forall v^J, v^K \neq 1 \in B : v^I \neq v^J v^K \right\}$$

forms a superorthonormal basis.

Proof. Note that $\pi^n v^J = (\chi v)^J = \chi^J v^J$. So,

$$\frac{1}{|G|} \sum_{g \in G} \chi^J(g) v^J = \left\langle \chi^J, \tau \right\rangle v^J.$$

So, any invariant free polynomial is in the span of the $v^J \in B$, which are themselves invariant homogeneous free polynomials, since otherwise $\left\langle \chi^J, \tau \right\rangle = 0$ by the orthogonality of characters.

To show that $\tilde{B}$ is superorthogonal, note for any two distinct words,

$$\left\langle v^K, v^L \right\rangle = 0$$

by the grading lemma, which implies the claim.

□

So, the calculation of a superorthogonal basis for the ring of invariants of a finite abelian group is tractable in general.

The superorthogonal basis given in Theorem 7.4 also implies that off of some variety, the ring of invariant functions is finitely generated. So, there are finitely many invariant free rational functions such that any invariant free polynomial can be written in terms of them, in spite of the fact that the ring of invariant free polynomials is not itself finitely generated. Similar phenomena occur in real algebraic geometry, such as the fact that positive polynomials cannot be written as sums of squares of polynomials [16], but can be written as sums of squares of rational functions, i.e. Artin's resolution of Hilbert's seventeenth problem [6].

Theorem 7.5. *With the notation of Theorem 7.4 the ring of invariant functions in the algebra generated by* $v_1, \ldots, v_d, v_1^{-1}, \ldots, v_d^{-1}$ *is finitely generated.*

Proof. We note that by Pontryigan duality theorem [22, Theorem 1.7.2], the characters of an abelian group G form a group $\hat{G}$ under multiplication which is noncanonically isomorphic to G. Let F_d be the free group with d generators. Let $H = \{I \in F_d | \chi^I = 0\}$. Consider the short exact sequence

$$0 \to H \to F_d \to \hat{G} \to 0.$$

So, H is of finite index in F_d and is thus finitely generated, which then implies that the ring is finitely generated. □

7.3. **Example: Ad hoc methods for symmetric functions in three variables.** We now turn our attention to symmetric functions in three variables.

Let u_0, u_1, u_{-1} be as in Section 5 and let $(b_n)_{n\in\mathbb{N}}$ be the constructed superorthogonal basis for cyclic free polynomials in 3 variables, where we fix $b_0 = u_0$.

Let τ be the following action on a free function f:

$$\tau \cdot f(X_1, X_2, X_3) = f(X_1, X_3, X_2).$$

Note that

$$\tau \cdot u_0 = u_0,$$
$$\tau \cdot u_1 = u_{-1},$$
$$\tau \cdot u_{-1} = u_1.$$

We recall that each b_n is of the form

$$b_n = \prod_k u_{i_k}$$

such that $\sum_k i_k \equiv_3 0$. So, $\tau \cdot b_n = b_{\tilde{n}}$ for some $\tilde{n}$, since $\tau \cdot \prod_k u_{i_k} = \prod_k u_{-i_k}$, and so $\sum_k -i_k \equiv_3 0$.

For $n > 0$ define

$$c_n^0 = \frac{b_n + \tau \cdot b_n}{\sqrt{2}},$$

$$c_n^1 = \frac{b_n - \tau \cdot b_n}{\sqrt{2}}.$$

For $n = 0$, let $c_0^0 = u_0$.

Note that each c_n^0 is a symmetric free polynomial and that the product of an even number of c_n^1 is also symmetric. In fact,

$$\tau \cdot c_n^0 = c_n^0,$$

and

$$\tau \cdot c_n^1 = -c_n^1.$$

Set

$$B = \left\{ \Pi_{i=1}^N c_i^{k_i} | \sum_{i=1}^N k_i \equiv_2 0, \forall n < N, \sum_{i=1}^n k_i \not\equiv_2 0 \right\}.$$

Now, B is a superorthogonal basis for the symmetric free polynomials in 3 variables. The elements of B of degree 4 and less are given in the following table.

degree	basis elements
1	u_0
2	$\frac{u_1u_{-1}+u_{-1}u_1}{\sqrt{2}}$
3	$\frac{u_1^3+u_{-1}^3}{\sqrt{2}}, \frac{u_1u_0u_{-1}+u_{-1}u_0u_1}{\sqrt{2}}$
4	$\frac{u_1^2u_{-1}^2+u_{-1}^2u_1^2}{\sqrt{2}}, \frac{u_1u_0u_1^2+u_{-1}u_0u_{-1}^2}{\sqrt{2}}, \frac{u_1u_0^2u_{-1}+u_{-1}u_0^2u_1}{\sqrt{2}},$ $\frac{u_1^2u_0u_1+u_{-1}^2u_0u_{-1}}{\sqrt{2}}, (\frac{u_1u_{-1}-u_{-1}u_1}{\sqrt{2}})^2$

Note the table agrees with the generating function obtained earlier. As there are 13 elements of the basis of degree 5, we will stop here.

We remark that the method above of iteratively constructing can be applied, in principal, for any solvable group, since we exploited the fact that $\mathbb{Z}_2 \cong S_3/\mathbb{Z}_3$ acts on the ring of free polynomials invariant under $\mathbb{Z}_3$. Since the ring of free polynomials invariant under $\mathbb{Z}_3$ is itself isomorphic to a free algebra in infinitely many variables, we are essentially repeating the construction done for any abelian group.

References

[1] J. Agler and J.E. McCarthy. Norm preserving extensions of holomorphic functions from subvarieties of the bidisk. *Ann. of Math.*, 157(1):289–312, 2003.

[2] J. Agler and J.E. McCarthy. Distinguished varieties. *Acta Math.*, 194:133–153, 2005.

[3] J. Agler and J.E. McCarthy. Global holomorphic functions in several noncommuting variables. *Canad. J. Math.*, 2014. to appear, arXiv:1305.1636.

[4] J. Agler and N.J. Young. Symmetric functions of two noncommuting variables. *J. Funct. Anal.*, 266(9):5709 – 5732, 2014.

[5] Marcelo Aguiar, Carlos Andr, Carolina Benedetti, Nantel Bergeron, Zhi Chen, Persi Diaconis, Anders Hendrickson, Samuel Hsiao, I. Martin Isaacs, Andrea Jedwab, Kenneth Johnson, Gizem Karaali, Aaron Lauve, Tung Le, Stephen Lewis, Huilan Li, Kay Magaard, Eric Marberg, Jean-Christophe Novelli, Amy Pang, Franco Saliola, Lenny Tevlin, Jean-Yves Thibon, Nathaniel Thiem, Vidya Venkateswaran, C. Ryan Vinroot, Ning Yan, and Mike Zabrocki. Supercharacters, symmetric functions in noncommuting variables, and related hopf algebras. *Adv. Math.*, 229(4):2310 – 2337, 2012.

[6] E. Artin. Uber die zerlegung definiter funktionen in quadrate. *Abh. Math. Sem. Univ. Hamburg*, 5:85–99, 1927.

[7] N. Bergeron, C. Reutenauer, M. Rosas, and M. Zabrocki. Invariants and coinvariants of the symmetric group in noncommuting variables. *Canad. J. Math.*, 60:266 – 296, 2008.

[8] C. Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[9] J.B. Conway. *A course in Functional Analysis*. Springer-Verlag, New York, 1985.

[10] A.E. Frazho. Complements to models for noncommuting operators. *J. Funct. Anal.*, 59(3):445 – 461, 1984.

[11] I.M. Gelfand, D. Krob, B. Leclerc, A. Lascoux, V.S. Retahk, and J.-Y. Thibon. Noncommutative symmetric functions. *Adv. Math.*, 112:218 – 348, 1995.

[12] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1997.

[13] J.W. Helton, I. Klep, and S. McCullough. Proper free analytic maps. *J. Funct. Anal.*, 260(5):1476–1490, 2011.

[14] J.W. Helton, I. Klep, S. McCullough, and N. Slinglend. Noncommutative ball maps. *J. Funct. Anal.*, 257:47–87, 2009.

[15] D.S. Kaliuzhnyi-Verbovetskyi and V. Vinnikov. *Foundations of Free Noncommutative Function Theory*. Mathematical surveys and monographs. American Mathematical Society, 2014.

[16] T.S. Motzkin. The arithmetic-geometric inequality. In *Inequalities*, New York, 1967. Academic Press.

[17] G. Popescu. Isometric dilations for infinite sequences of noncommuting operators. *Trans. Amer. Math. Soc.*, 316:523–536, 1989.

[18] G. Popescu. Free holomorphic functions on the unit ball of $B(\mathcal{H})^n$. *J. Funct. Anal.*, 241:268–333, 2006.

[19] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Springer-Verlag, New York, 1977.

[20] G.C. Shepard and J.A. Todd. Finite unitary reflection groups. *Canad. J. Math.*, 6:274 – 304, 1954.

[21] M.C. Wolf. Symmetric functions of noncommuting elements. *Duke Math. J.*, 2:626 – 637, 1936.

[22] W.Rudin. *Fourier Analysis on Groups.* John Wiley and Sons, New York, 1962.