Fourier Transform Over Semisimple Algebras and Harmonic Analysis for Probabilistic Algorithms[1]

François Bergeron and Luc Favreau

1. Introduction

Given a finite group G (with 1 as unit) we study in this paper some aspects of probabilistic algorithms of the form

```
r := 1;
repeat
    choose g ∈ G with probability p(g);
    r :=  r · g
until satisfied
```

where $p : G \longrightarrow [0,1]$ is a probability distribution on G. We are also interested in questions such as the explicit computation of the probability of obtaining some element $g \in G$ after n iteration of the loop. This study is clearly equivalent to the computation of successive powers, in the group algebra $\mathcal{A}(G)$ of G, of

$$\alpha = \sum_{g \in G} p(g)\, g.$$

However, these powers are often hard to calculate in a nice closed form. For this reason we shall consider their Fourier transforms in some suitable context. The idea being that intricate computation of products in the group algebra are replaced by simple point wise products. More precisely, we shall derive new extended versions of a formula of Garsia (see (1) below) and of similar formulas obtained in [4], as well as generalizations of those. All these formulas can be considered to give, in explicit form, a Fourier transform such as defined below.

Let $\mathcal{A}$ be a semisimple algebra, and let $B = v_1, v_2, \ldots, v_n$ be some fixed (linear) basis for the subalgebra $\mathcal{B}$, of $\mathcal{A}$, spanned by the complete set of primitive idempotents $e_1, e_2, \ldots, e_n$ of $\mathcal{A}$. Recall that these idempotents are such that

$$e_k e_j = \begin{cases} e_k & \text{if } k = j \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_{k=1}^{n} e_k = 1.$$

[1] LACIM, UQAM, Montréal H3P 3P8, Canada. Email: bergeron@lacim.uqam.ca. With support from NSERC.

Moreover, none of them can be written as the sum of two orthogonal idempotents. The *Fourier transform* $\widehat{f}$ (with respect to B) of $f = \sum_k f_k v_k \in \mathcal{B}$ is defined to be the vector $(\widehat{f_1}, \widehat{f_2}, \ldots, \widehat{f_n})$ of coordinates of f in this canonical basis $(e_k)_{1\leq k\leq n}$

$$f = \sum_{k=1}^{n} \widehat{f_k} e_k.$$

This transform clearly enjoys the usual nice property, of the Fourier transform, of sending convolution to component wise product. For a finite group G, if $\mathcal{B}$ is the center $C(G)$ of the group algebra of G, then the canonical idempotents are essentially given by the characters χ_ρ of irreducible representations ρ of G, considered as elements of the group algebra

$$e_\rho = \frac{\chi_\rho(1)}{|G|} \sum_{g\in G} \chi_\rho(g^{-1})\, g.$$

If the basis B is chosen to be the set of conjugacy classes in G

$$c_\rho = \sum_{g\in c(\rho)} g,$$

where $c(\rho) = \{h^{-1}\rho h \mid h \in G\}$ and $\rho \in G$, the Fourier transform with respect to this basis is the usual Fourier transform over G. Consider for instance the cyclic group $\langle x\rangle$ of order n generated by x. Since the group is abelian, any element of the group algebra of $\langle x\rangle$

$$f(x) = \sum_{k=0}^{n-1} f_k x^k,$$

is an element of the center $C(\langle x\rangle)$. Moreover, the irreducible characters give in this case, the following idempotents

$$e_j = \frac{1}{n}\sum_{k=0}^{n-1} q^{-kj} x^k,$$

where $q = e^{2i\pi/n}$, for $0 \leq j \leq n-1$. One concludes that

$$f(x) = \sum_{j=0}^{n-1} \widehat{f_j} e_j,$$

where

$$\begin{aligned}\widehat{f_j} = f(x)e_j|_1 &= \frac{1}{n}\sum_{k=0}^{n-1} f_k q^{-(n-k)j} \\ &= \frac{1}{n} f(q^j).\end{aligned}$$

This is the traditional definition of the discrete Fourier Transform.

2. The descent algebra of A_n

The semisimple algebras considered in this paper are subalgebras of the group algebra of finite Coxeter groups. For the Fourier transform, we give explicit expression, with respect to given basis for these algebras. As a guiding example, let us consider the semisimple subalgebra $\Gamma[A_{n-1}] = \Gamma[S_n]$ of the symmetric group spanned by the linearly independent descent classes

$$D_k = \sum_{d(\sigma)=k} \sigma,$$

where $0 \le k \le n-1$ and $d(\sigma) = Card\{1 \le i \le n-1 \mid \sigma(i) > \sigma(i+1)\}$. The fact that this is a subalgebra and that it is semisimple is shown in [10]. Now, in [9] A. Garsia gives a beautiful explicit formula

$$\sum_{k=1}^{n} t^k e_k = \frac{1}{n!} \sum_{k=0}^{n-1} (t-k)^{(n)} D_k, \tag{1}$$

relating the basis D_k and the canonical idempotents e_k of $\Gamma(S_n)$. Here, $(t)^{(n)}$ stands for the rising factorial

$$(t)^{(n)} = t(t+1)(t+2)\cdots(t+n-1).$$

For $t \ge 1$,

$$\frac{1}{t^n} \sum_{k=1}^{n} t^k e_k = \sum_{k=0}^{n-1} \frac{(t-k)^{(n)}}{n!t^n} D_k,$$

is a probability distribution on S_n. It follows immediately from the orthogonality of the e_k's that

$$\begin{aligned}
\left(\sum_{k=0}^{n-1} \frac{(t-k)^{(n)}}{n!t^n} D_k\right)^j &= \left(\frac{1}{t^n}\sum_{k=1}^{n} t^k e_k\right)^j \\
&= \frac{1}{t^{jn}} \sum_{k=1}^{n} t^{jk} e_k \\
&= \sum_{k=0}^{n-1} \frac{(t^j-k)^{(n)}}{n!t^{jn}} D_k.
\end{aligned}$$

This gives an answer to a problem of the type considered at the beginning of this text. In order to generalize this last computation, we extend formula (1) using an umbral argument. Thus we obtain

$$\sum_{k=1}^{n} t_k e_k = \sum_{k=0}^{n-1} \left(\sum_{j=1}^{n} \Psi_n(k,j) t_j \right) D_k,$$

where the $\Psi_n(k,j)$'s are the coefficients appearing in the expansion of the polynomial

$$\psi_k^n(t) = \frac{1}{n!}(t-k)^{(n)} = \sum_{j=1}^{n} \Psi_n(k,j) t^j. \tag{2}$$

Hence if Φ_n stands for the inverse of the matrix Ψ_n, then the Fourier transform, with respect to the basis $(D_k)_{0 \le k \le n-1}$, is

$$\widehat{s}_k = \sum_{j=1}^{n} \Phi_n(k,j) s_j. \tag{3}$$

Thus Φ_n is the matrix for the Fourier transform and Ψ_n is the inverse Fourier transform. For example

$$\Phi_5 = \begin{bmatrix} 1 & -4 & 6 & -4 & 1 \\ 1 & -2 & 0 & 2 & -1 \\ 1 & 2 & -6 & 2 & 1 \\ 1 & 10 & 0 & -10 & -1 \\ 1 & 26 & 66 & 26 & 1 \end{bmatrix} \qquad \Phi_6 = \begin{bmatrix} 1 & -5 & 10 & -10 & 5 & -1 \\ 1 & -3 & 2 & 2 & -3 & 1 \\ 1 & 1 & -8 & 8 & -1 & -1 \\ 1 & 9 & -10 & -10 & 9 & 1 \\ 1 & 25 & 40 & -40 & -25 & -1 \\ 1 & 57 & 302 & 302 & 57 & 1 \end{bmatrix}$$

If $\varphi_k^n(t) = \sum_{j=1}^{n} \Phi_n(k,j) t^j$ stands for the enumerating polynomial of the k^{th} row of the matrix Φ_n, then it is readily observed on the previous examples that $\varphi_n^n(t)$ appear to be the well known *eulerian polynomials*

$$\mathbf{A}_n(t) = \sum_{\sigma \in S_n} t^{d(\sigma)+1},$$

whose generating function is

$$\mathbf{A}(x,t) = \frac{1-t}{1-te^{x(1-t)}}. \tag{4}$$

In general, we can characterized the entries of Φ_n as follows

Proposition 1. *The enumerating polynomial of the k^{th} row of the matrix $\Phi_n = \Psi_n^{-1}$, for the Fourier transform from the basis of D_k's to the basis of orthogonal idempotents e_k of the descent algebra $\Gamma(A_{n-1})$, is*

$$\varphi_k^n(t) = (1-t)^{(n-k)} \mathbf{A}_k(t). \tag{5}$$

Proof. Using expression (3) for the generating function $\mathbf{A}(x,t)$, one readily verifies that

$$(1-xt)\frac{\partial}{\partial t}\mathbf{A}(x,t) = \; t\mathbf{A} + t(1-t)\frac{\partial}{\partial x}\mathbf{A}(x,t).$$

Comparing respective coefficients of $x^k/k!$ in this last equation, we obtain

$$\mathbf{A}_{k+1}(x) = xk\mathbf{A}_k + \mathbf{A}_k + x(1-x)\mathbf{A}_k', \tag{6}$$

for $k \geq 2$, and $\mathbf{A}_1(x) = 1$. Multiplying both sides of (6) by $(1-t)^{n-k}$, and using the definition of $\varphi_k^n(t)$, it follows that

$$\varphi_{k+1}^{n+1}(t) = t(1+k)\varphi_k^n(t) + t(1-t)\frac{d}{dt}\varphi_k^n(t). \tag{7}$$

A direct translation of (7) in term of Φ_n gives

$$\Phi_n = \begin{bmatrix} \Phi_n(1,1) & \dots & \Phi_n(1,n) \\ & \Phi_{n-1}M_{n-1} & \\ & & \end{bmatrix} \tag{8}$$

where M_{n-1} has the following expression

$$M_{n-1} = \begin{bmatrix} 1 & n-1 & 0 & \dots & 0 & 0 \\ 0 & 2 & n-2 & \dots & 0 & 0 \\ 0 & 0 & 3 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & n-1 & 1 \end{bmatrix}$$

Now, let us set

$$[\Phi_n : 0] = \begin{bmatrix} \Phi_n(1,1) & \Phi_n(1,2) & \dots & \Phi_n(1,n) & 0 \\ \Phi_n(2,1) & \Phi_n(2,2) & \dots & \Phi_n(2,n) & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \Phi_n(n,1) & \Phi_n(n,2) & \dots & \Phi_n(n,n) & 0 \end{bmatrix}$$

and the analogous convention for $[0 : \Phi_n]$. The definition of $\varphi_k^n(t)$ implies that $\varphi_k^n(t) = (1-t)\varphi_k^{n-1}(t)$, whenever $1 \leq k \leq n-1$. It follows that

$$\Phi_n = \begin{bmatrix} & [\Phi_{n-1} : 0] \; - \; [0 : \Phi_{n-1}] & \\ \Phi_n(n,1) & \dots & \Phi_n(n,n) \end{bmatrix} \tag{9}$$

We want to show that $n!\Psi_n\Phi_n = n!\mathrm{I}_n$. Denoting by ψ_{kj}^n the entries of the k^{th} row of $n!\Psi_n$, that is $\psi_{kj}^n = n!\Psi_n(k,j)$, it is easy to check that

$$\begin{aligned}(\psi_{k1}^n, \psi_{k2}^n, \dots, \psi_{kn}^n) &= (0, \psi_{k1}^{n-1}, \psi_{k2}^{n-1}, \dots, \psi_{k(n-1)}^{n-1}) \\ &\quad + (n-k)(\psi_{k1}^{n-1}, \psi_{k2}^{n-1}, \dots, \psi_{k(n-1)}^{n-1}, 0),\end{aligned} \tag{10}$$

for $1 \leq k \leq n-1$, and that

$$\begin{aligned}(\psi_{n1}^n, \psi_{n2}^n, \dots, \psi_{nn}^n) &= (0, \psi_{(n-1)1}^{n-1}, \psi_{(n-1)2}^{n-1}, \dots, \psi_{(n-1)(n-1)}^{n-1}) \\ &\quad + (1-k)(\psi_{(n-1)1}^{n-1}, \psi_{(n-1)2}^{n-1}, \dots, \psi_{(n-1)(n-1)}^{n-1}, 0).\end{aligned} \tag{11}$$

The proof of the proposition is by a straightforward induction on n using an adequate mixture of (8) and (9) with (10) and (11). The crucial portion of the argument is to use in the decomposition given in (10) (or (11)) the first part together with (8) and the second part with (9). ∎

As we shall see, this is an instance of a general expression for the rows of the Fourier transform of the descent algebras of many Coxeter groups. But before going on with these other cases, let us derive other properties of $\Gamma[A_{n-1}]$ using (1). The following theorem appears (up to a small variation) in [11] as theorem 1.1. However we give a different proof that will allow us to derive new similar results for descent algebras of other Coxeter groups.

Proposition 2. *The descent class D_1 is an algebraic generator for $\Gamma[A_{n-1}]$ with minimal polynomial*

$$p(x) = \prod_{i=1}^{n}(x - 2^i + n + 1)$$

Proof. First, observe that

$$\begin{aligned}\sum_{i=1}^{n} 2^i e_i &= \frac{1}{n!}\sum_{k=0}^{n}(2-k)^{(n)} D_k \\ &= \frac{1}{n!}((2)^{(n)} D_0 + (1)^{(n)} D_1) \\ &= (n+1)D_0 + D_1,\end{aligned} \tag{12}$$

since $(t)^{(n)} = 0$ whenever $t < 0$. Recall also that $D_0 = \sum e_i$. Now using (3), one sees that the successive powers D_1^k, $k = 0, 1, \ldots, n-1$, form a basis of $\Gamma[A_{n-1}]$ because the transition matrix between the basis of the e_k's and that of the D_1^k's is the (invertible) Vandermonde

$$V = \begin{bmatrix} 1 & 2-(n+1) & \cdots & (2-(n+1))^{n-1} \\ 1 & 4-(n+1) & \cdots & (4-(n+1))^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^i-(n+1) & \cdots & (2^i-(n+1))^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^n-(n+1) & \cdots & (2^n-(n+1))^{n-1} \end{bmatrix}$$

Moreover, the coefficients $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ of the linear combination of the columns of V giving the expression of D_1^n in term of the D_1^k, $0 \leq k \leq n-1$, are such that the polynomial

$$p(x) = x^n - (\alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1})$$

has zeros at $2-(n+1), 4-(n+1), \ldots, 2^n-(n+1)$, hence p(x) can only be

$$\prod_{i=1}^{n} (x - 2^i + n + 1)$$

as announced. ■

This makes it clear why $\Gamma[A_{n-1}] \simeq \mathbb{Q}[x]/\langle p(x) \rangle$ is a commutative semisimple algebra, because we are led back to a close relative of the usual Fourier transform for which the underlying semisimple algebra is isomorphic to $\mathbb{Q}[x]/\langle x^n - 1 \rangle$. The point of this last remark being that in both cases the modulo is taken with respect to a polynomial with distinct roots in which case we have the following (see theorem 1.2 in [11])

Proposition 3. *For a polynomial $p(x)$ with distinct roots $r_1, r_2, \ldots, r_n$, the algebra $\mathbb{Q}[x]/\langle p(x) \rangle$ is commutative and semisimple, and its primitive idempotents are given by the interpolating Lagrange polynomials*

$$e_i = \frac{\prod_{j \neq i}(x - r_j)}{\prod_{j \neq i}(r_i - r_j)}$$

Proof. Straightforward. ■

It follows directly from this last proposition that the idempotents for the algebra $\Gamma[A_{n-1}]$ admit the following expression

$$e_i = \frac{\prod_{j \neq i}(D_1 - (2^j - n - 1)D_0)}{\prod_{j \neq i}(2^i - 2^j)}.$$

Using (1) twice, we can also express the successive powers D_1^k, for $0 \le k \le n-1$, in term of the descent classes D_m, for $0 \le m \le n-1$, as follows

$$\begin{aligned} D_1^k &= \sum_{i=1}^{n} (2^i - (n+1))^k e_i \\ &= \sum_{i=1}^{n} \sum_{j=0}^{k} \binom{k}{j} (-n-1)^{k-j} 2^{ij} e_i \\ &= \sum_{j=0}^{k} \binom{k}{j} (-n-1)^{k-j} \left(\sum_{i=1}^{n} 2^{ji} e_i \right) \\ &= \sum_{j=0}^{k} \binom{k}{j} (-n-1)^{k-j} \left(\frac{1}{n!} \sum_{m=0}^{n-1} (2^j - m)^{(n)} D_m \right) \\ &= \sum_{m=0}^{n-1} \left(\sum_{j=0}^{k} \binom{k}{j} \binom{2^j - m + n}{n} (-n-1)^{k-j} \right) D_m. \end{aligned}$$

Hence we have explicit forms of the various relations between the three basis of $\Gamma(A_{n-1})$.

3. B_n AND OTHER COXETER GROUPS

Similar consideration can be made in the context of the group algebra of the hyperoctahedral group B_n (see [4]), if one considers the semisimple subalgebra $\Gamma[B_n]$ of the symmetric group spanned by the linearly independent descent classes

$$D_k = \sum_{d(\sigma)=k} \sigma,$$

where $0 \le k \le n$ and $d(\sigma) = Card\{0 \le i \le n-1 \mid \sigma(i) > \sigma(i+1)\}$. Recall that elements of B_n are signed permutations and that for convenience sake one can set $\sigma(0) = 0$. It was shown in [4] that there is in this context a Garsia like formula

$$\sum_{k=0}^{n} t^k e_k = \frac{1}{2^n n!} \sum_{k=0}^{n} (t-2k)^{((n))} D_k, \tag{13}$$

relating the basis D_k and the canonical basis of idempotents e_k of $\Gamma(B_n)$. Here, $(t)^{((n))}$ stands for the double rising factorial

$$(t)^{((n))} = (t+1)(t+3)\cdots(t+2n-1).$$

Once again umbral considerations on (12) imply that

$$\sum_{k=0}^{n} t_k e_k = \sum_{k=0}^{n} \left(\sum_{j=0}^{n} \Psi_n(k,j) t_j \right) D_k,$$

where the $\Psi_n(k,j)$'s are the coefficients appearing in the expansion of the polynomial

$$\frac{1}{2^n n!}(t-2k)^{((n))} = \sum_{j=0}^{n} \Psi_n(k,j) t^j.$$

The matrices for $n = 4, 5$ are

$$\Phi_4 = \begin{bmatrix} 1 & -4 & 6 & -4 & 1 \\ 1 & -2 & 0 & 2 & -1 \\ 1 & 4 & -10 & 4 & 1 \\ 1 & 22 & 0 & -22 & -1 \\ 1 & 76 & 230 & 76 & 1 \end{bmatrix} \qquad \Phi_5 = \begin{bmatrix} 1 & -5 & 10 & -10 & 5 & -1 \\ 1 & -3 & 2 & 2 & -3 & 1 \\ 1 & 3 & -14 & 14 & -3 & -1 \\ 1 & 21 & -22 & -22 & 21 & 1 \\ 1 & 75 & 154 & -154 & -75 & -1 \\ 1 & 237 & 1682 & 1682 & 237 & 1 \end{bmatrix}$$

As in the A_n case, one can observe that the generating polynomials for the last row of these matrices appear to be corresponding hyperoctahedral descent polynomials

$$\mathbf{B}_n(x) = \sum_{\sigma \in B_n} x^{d(\sigma)},$$

In general, one is led to deduce the following proposition in a manner similar to the proof of proposition 1.

Proposition 4. *The enumerating polynomial of the k^{th} row of the matrix $\Phi_n = \Psi_n^{-1}$, for the Fourier transform from the basis of D_k's to the basis of orthogonal idempotents e_k of the descent algebra $\Gamma(B_n)$, is*

$$\varphi_k^n(x) = (1-x)^{(n-j)} \mathbf{B}_j(x). \tag{14}$$

■

In order to unfold the proof of (6), one needs an expression for the generating function of the polynomials $\mathbf{B}_n(x)$, but it is easy to verify that they satisfy the following recurrence

$$\mathbf{B}_{n+1}(x) = (1+x)\mathbf{B}_n(x) + 2xn\mathbf{B}_n(x) + (2x - 2x^2)\frac{d}{dx}\mathbf{B}_n(x),$$

hence that their exponential generating function is

$$\sum_{n\geq 0} \mathrm{B}_n(x)\frac{u^n}{n!} = \frac{(1-x)e^{u(1-x)}}{1-xe^{2u(1-x)}}.$$

The proof of the following proposition is also similar to that of proposition 2.

Proposition 5. *The descent class D_1 is an algebraic generator for $\Gamma[B_n]$ with minimal polynomial*

$$p(x) = \prod_{i=0}^{n}(x - 3^i + n + 1)$$

Hence the idempotents of $\Gamma(B_n)$ admit the expression

$$e_i = \frac{\prod_{j\neq i}(D_1 - (3^j - n - 1)D_0)}{\prod_{j\neq i}(3^i - 3^j)},$$

by proposition 2. Moreover, for $0 \leq k \leq n$ and $0 \leq m \leq n$, we have

$$D_1^k = \sum_{m=0}^{n-1}\left(\sum_{j=0}^{k}\binom{k}{j}\binom{3^j - m + n}{n}(-n-1)^{k-j}\right)D_m.$$

For all Coxeter groups W of type A_n, B_n, H_3 or $I_2(p)$, the following Garsia like formula has been derived in [4]

$$\sum_{i=0}^{n} e_i t^i = \frac{1}{|W|}\sum_{k=0}^{n}\pi_k^W(t)D_k,$$

where the e_i's are a basis of orthogonal idempotents for the subalgebra of $\Sigma(W)$ spanned by the descent classes

$$D_k = \{w \in W \mid d(w) = k\},$$

and where the polynomials $\pi_k^W(t)$ are defined in term of the *exponents* (ϵ_k) of the group W as

$$\pi_k^W(t) = (t-\epsilon_k)(t-\epsilon_{k-1})\cdots(t-\epsilon_1)(t+\epsilon_1)\cdots(t+\epsilon_{n-k}).$$

Recall that the descent set of an element $w \in W$ is defined to be

$$desc(w) = \{s \in S \mid \ell(ws) < \ell(w)\},$$

where S is the set of Coxeter generators of W, and $\ell(w)$ is the so called *length* of W, that is the length of a reduced expression for w in term of the generators (see [12]). With this definition of descent set, one sets $d(w) = \#desc(w)$. For the descent algebra of the dihedral groups $I_2(p)$, the Fourier transform matrices are simply

$$\begin{bmatrix} 1 & -2 & 1 \\ 1 & 0 & -1 \\ 1 & 2p-2 & 1 \end{bmatrix}.$$

Observe that the last row of the matrix is again given by the coefficients of the polynomial enumerating elements of $I_2(p)$ with respect to number of descents. The same kind of results also hold for finite Coxeter groups that are direct products of groups of type A_n, B_n, H_3 or the dihedral groups since the corresponding descent algebras are simply tensor products of the descent algebras of the respective components. The Fourier transform matrices are the tensor product of the matrices corresponding to the transforms of individual terms in the product.

4. The shuffle algebra

Another family of closely related problems is obtained in the following manner. Consider the anti-automorphism θ of any group algebra, defined on the elements of the group by

$$\theta(g) = g^{-1}.$$

This anti-automorphism sends the descent algebras into other nice algebras who evidently share the properties of the original algebras. Thus for the symmetric group case, $\theta(\Gamma(S_n))$ is the algebra generated by

$$\Xi_k = \theta(D_k).$$

Let us denote $\sqcup\!\sqcup$ the usual *shuffle product*, that is

$$12 \sqcup\!\sqcup 34 = 1234 + 1324 + 1342 + 3124 + 3142 + 3412,$$

and observe, using (3), that

$$\Xi_1 + (n+1)\Xi_0 = 1\,2 \cdots j \sqcup\!\sqcup (j+1)\,(j+2) \cdots n$$

Thus a problem considered by Diaconis in [2 and 3] is equivalent to the computation of powers of

$$\frac{1}{2^n}(\Xi_1 + (n+1)\Xi_0) = \frac{1}{2^n}\sum_{j=0}^{n} 1\,2 \cdots j \sqcup\!\sqcup (j+1)\,(j+2) \cdots n.$$

Applying (back and forth) θ on Garsia's formula with $t = 2$ gives

$$\left[\frac{1}{2^n}(\Xi_1 + (n+1)\Xi_0)\right]^N = \frac{1}{2^N n!}\sum_{k=0}^{n-1}(2^N - k)_{(n)}\,\Xi_k,$$

as discussed in [4]. This last expression is essentially what is used in [3] to study the number of shuffles needed in order to really mix a deck of n cards. A similar expression can be obtained for the B_n case involving a mixture of shuffles and the following operation on words $w = a_1 a_2 \dots a_k$ on the alphabet $\{1, \overline{1}, 2, \overline{2}, \dots, n, \overline{n}\}$

$$\overline{a_1 a_2 \dots a_k} = \overline{a_k} \dots \overline{a_2}\, \overline{a_1},$$

where

$$\overline{a} = \begin{cases} i & \text{if } a = \overline{i}, \\ \overline{i} & \text{if } a = i, \end{cases}$$

for $1 \leq i \leq n$.

Clearly, considering any automorphisms or antiautomorphisms would lead to other isomorphic algebras for which these cconsideration are interesting. One nice example is the linear extension of

$$\eta(g) = \mathrm{sign}(g) g.$$

5. Various related problems

Another nice example (see [7]) is the case $\mathbb{Z}_2^n$ for which we consider the algebra $\mathcal{B}$ spanned by

$$D_k = [0]^{n-k} \sqcup\!\sqcup [1]^k,$$

where [0] and [1] stand for the elements of $\mathbb{Z}_2$, with $0 \leq k \leq n$. This algebra is semisimple with canonical idempotents e_i characterized by the formula

$$\sum_{k=0}^{n} t^k e_k = \frac{1}{2^n} \sum_{k=0}^{n} (1-t)^{(n-k)} (1+t)^k D_k.$$

From this, one readily derives the expression for the Fourier transform with respect to the basis corresponding to the D_k's. In this case, the descent polynomial is simply $(1+t)^n$, and the rest of the Fourier transform is obtained in the same manner as for the algebras $\Gamma(A_n)$ and $\Gamma(B_n)$. The study of the powers of

$$\alpha = \frac{1}{n+1}(D_0 + D_1),$$

corresponds to the study of successive random changing of one bit in an n-bit word. Computing the Fourier transform of α, we obtain

$$\alpha = \sum_{k=0}^{n} \left(1 - \frac{2k}{n+1}\right) e_k,$$

hence the j^{th} power of α is the inverse Fourier transform of

$$\sum_{k=0}^{n} \left(1 - \frac{2k}{n+1}\right)^{j} e_k.$$

For n large enough and taking $j = s\,\frac{(n+1)}{2}$, this last expression becomes

$$\begin{aligned}\sum_{k=0}^{n} \left(1 - \frac{2k}{n+1}\right)^{s\,\frac{(n+1)}{2}} e_k &\approx \sum_{k=0}^{n} (t^s)^k e_k \\ &\approx \frac{1}{2^n} \sum_{k=0}^{n} (1 - t^s)^{(n-k)} (1 + t^s)^k D_k,\end{aligned}$$

where $t = \frac{1}{e}$.

This example can readily be generalized to G^n for any finite group G. However, for simplicity's sake, we shall only outline what happens in the case $\mathbb{Z}_3^n$. We consider the algebra $\mathcal{B}$ generated by

$$D_{jkl} = [0]^j \sqcup\!\sqcup [1]^k \sqcup\!\sqcup [2]^l,$$

where [0], [1] and [2] stand for the elements of $\mathbb{Z}_3$, with $j + k + l = n$. This algebra is semisimple with canonical idempotents e_{jkl} characterized by the formula

$$\sum_{j+k+l=n} s^j t^k r^l e_{jkl} = \frac{1}{3^n} \sum_{j+k+l=n} (s+t+r)^j (s + \xi t + \xi^2 r)^k (s + \xi^2 t + \xi r)^k D_{jkl}, \tag{15}$$

where ξ is a primitive third root of unity. This last expression is easily derived by taking the n^{th} tensor power of both sides of

$$s e_0 + t e_1 + r e_2 = \frac{1}{3} \left((s+t+r)[0] + (s + \xi t + \xi^2 r)[1] + (s + \xi^2 t + \xi r)[2] \right),$$

where the idempotents e_i's are the characters of the irreducible representations of $\mathbb{Z}_3$. The Fourier transform with respect to the basis corresponding to the D_{jkl}'s is easily computed using (15).

6. Conclusion

Many other problems of the form treated in this text can be studied using the Fourier transform formulas outlined above. Some have been considered by various authors such as: Aldous [1], Diaconis [6], Letac and Takacs [14], Flatto, Odlyzko and Wales [8]; and range from walks on graphs, to problems appearing in coding theory. Another interesting source of semisimple algebras is through *Hecke algebras*

$$\mathcal{H}(G,e) = e\mathcal{A}(G)e$$

where e is any idempotent of the group algebra $\mathcal{A}(G)$ of G. *Gelfand pairs* (G,H), for H a subgroup of G, correspond to the special case when the semisimple algebra $\mathcal{H}(G,e_H)$ is commutative, with

$$e_H = \frac{1}{|H|}\sum_{h\in H} h.$$

Natural extensions of this work would include Fourier transform formulas for the subalgebra, of the complete descent algebra $\Sigma(S_n)$ considered by Garsia and Reutenauer in [10], spanned by the idempotents E_λ (λ partition of n); as well as the subalgebra spanned by the corresponding idempotents (constructed in [5]) for the complete descent algebras of any other finite Coxeter groups.

References

[1] D. Aldous, *Minimization algorithms and random walks on the d-cube*, Ann. Prob. **11**, 1983, 403–413.

[2] D. Aldous and P. Diaconis, *Shuffling Cards and Stopping Times*, Amer. Math. Monthly **93**, 1986, 333–348.

[3] D. Bayer and P. Diaconis, *Trailing the Dovetail Shuffle to its Lair*, Technical Report No. 2, Dept. Statistics, Stanford University, 1990.

[4] F. Bergeron and N. Bergeron, *Orthogonal Idempotents in the Descent Algebra of B_n*, J. of Pure and Appl. Algebra, (accepted 1991).

[5] F. Bergeron, N. Bergeron, R. B. Howlett and D. E. Taylor, *A Decomposition of the Descent Algebra of Finite Coxeter Groups*, Journal of Algebraic Combinatorics, Vol.1, No.1, 1992, 23–42.

[6] P. Diaconis, *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics, Hayward, CA, 1988.

[7] P. Diaconis, R. L. Graham and J. A. Morisson, *Asymptotic Analysis of a Random Walk on a Hypercube with Many Dimensions*, Random Structures and Algorithms, Vol. 1, No. 1, 1990.

[8] L. Flatto, A. Odlyzko and D. Wales, *Random shuffles and group representations*, Ann. Prob. **13**, 154–178.

[9] A. Garsia, *Combinatorics of the Free Lie Algebra and the Symmetric Group*, Analysis, Et Cetera, Research papers published in honor of Jurgen Moser's 60th birthday, ed: Paul H. Rabinowitz and Eduard Zehnder, Academic Press, 1990.

[10] A. Garsia and C. Reutenauer, *A Decomposition of Solomon's Descent Algebras*, Adv. in Math. **77**, No 2, 1989, 189–262.

[11] M. Gerstenhaber and S. D. Schack, *A Hodge-Type Decomposition for Commutative Algebra Cohomology*, J. Pure Appl. Algebra **48**, 1987, 229-247.

[12] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, 1990.

[13] G. Letac, *Problèmes classiques de probabilité sur un couple de Gelfand*, SLN in Math. **861**, Springer-Verlag.

[14] G. Letac and L. Takacs, *Random Walks on the m-dimensional Cube* , J. Reine Angew. Math. **310**, 187–195.