4

Fourier Transforms over Semi-simple Algebras

François Bergeron
UQAM, Montréal

[summary by Dominique Gouyou-Beauchamps]

1 Introduction

Given a finite group G, we study some aspects of probabilistic algorithms of the form:

$r := 1$

repeat

choose $g \in G$ with probability $p(g)$

$r := r.g$

until the probability distribution of r is close to uniform

where $p : G \longrightarrow [0,1]$ is a probability distribution on G. We are also interested in some questions such as the explicit computation of the probability of obtaining some element $g \in G$ after n iterations 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.

Example 1: We have an n-tuple of bits $w \in \{0,1\}^n$. At time $t = 1, 2, 3, \ldots$, we randomly choose one bit of w and we change the value of this bit $(0 \leftrightarrow 1)$. At time t, what is the probability that we obtain a given n-tuple $w_0 \in \{0,1\}^n$?

Example 2: We consider $G = \mathcal{S}_n$, the symmetric group, and we compute powers of $\frac{1}{2^n} \sum_{j=0}^{n} 1\,2 \ldots j \sqcup\!\sqcup (j+1)(j+2) \ldots n$ where $\sqcup\!\sqcup$ denotes the shuffle product. This problem has been considered by Diaconis in [1, 2].

Example 3: We can also consider powers of $\frac{1}{\binom{n}{2}} \sum_{i \neq j} (i,j)$ where (i,j) denotes the transposition that exchanges i and j.

All these formulas can be considered to give, in explicit form, a Fourier transform such as defined below.

Let $\mathcal{A}$ be a semi-simple commutative algebra (i.e. having a basis of orthogonal idempotents), 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

$$e_k e_j = \begin{cases} e_k & \text{if } k = j \\ 0 & \text{otherwise} \end{cases} \qquad \text{and} \qquad \sum_{k=1}^{n} e_k = 1.$$

Moreover, none of them can be written as the sum of two orthogonal idempotents. The *Fourier transform* $\hat{f}$ (with respect to B) of $f = \sum_k f_k v_k \in \mathcal{B}$ is defined to be the vector $(\hat{f}_1, \hat{f}_2, ..., \hat{f}_n)$ of coordinates of f in this canonical basis $(e_k)_{1 \le k \le n}$

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

And the powers of f can be written

$$f^N = \sum_{k=1}^{n} \hat{f}_k^N e_k.$$

2 Example 1

Let $\mathcal{B}$ be the center $C(G)$ of the group algebra of a finite group G. 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 $\rho \in G$.
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 $G = \mathcal{S}_n$, a conjugacy class is a partition of the integer n because two permutations are in the same class if and only if they have the same cycle decomposition.
If $G = \langle x \rangle$, the cyclic group of order n generated by x ($x^n \equiv 1$), 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 $C(\langle x \rangle)$. The group algebra can be seen as $\mathcal{A} = \mathbb{C}[x]/\langle x^n - 1 \rangle$. Moreover the irreducible characters give, in this case, the following idempotents

$$e_j = \frac{1}{n} \sum_{k=0}^{n-1} e^{-2ikj\pi/n} x^k,$$

for $0 \le j \le n-1$. One concludes that

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

where

$$\hat{f}_j = \frac{1}{n} \sum_{k=0}^{n-1} f^k e^{-2i(n-k)j\pi/n}$$

$$= \frac{1}{n} f(q^j).$$

This is the traditional definition of the discrete Fourier Transform.

3 Example 2

The semi-simple algebras considered in this example are subalgebras of the group algebra of finite Coxeter groups. As a guiding example, let us consider the semi-simple subalgebra $\Gamma[A_{n-1}] = \Gamma[\mathcal{S}_n]$ of the symmetric group spanned by the linearly independent descent classes

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

where $0 \leq k \leq n-1$ and $d(\sigma) = \mathrm{Card}\{1 \leq i \leq n-1 \mid \sigma(i) > \sigma(i+1)\}$ (cf [5]). Now, in [4] A. Garsia gives a beautiful explicit formula

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

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

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

This formula is closely related to the shuffle algebra and to a problem considered by Diaconis in [1, 2]. It is used in [2] to study the number of shuffles needed in order to really mix a deck of n cards. If we denote

$$\hat{\alpha} = \widehat{\sum_g \alpha_g g} = \sum_g \alpha_g g^{-1},$$

then $\widehat{D_{\leq i}} = w_1 \sqcup\!\sqcup\, w_2 \sqcup\!\sqcup\, ... \sqcup\!\sqcup\, w_i$ if $w_1 w_2 ... w_i = 1\,2...n$.
Example: $\sigma = 34681257$, $d(\sigma) = 1$, $\sigma^{-1} = 56127384 \in 1234 \sqcup\!\sqcup\, 5678$.
Applying Garsia's formula with $t = 2$ gives

$$\sum_{k=1}^{n} \frac{2^k}{2^n} \widehat{e_k} = \frac{1}{2^n} \sum_{k=0}^{n-1} 1\,2...k \sqcup\!\sqcup\, (k+1)...n\ .$$

The idempotent e_n is dominating in this formula because its coefficient is the greatest. But e_n is equal to $\sum_{\sigma\in\mathcal{S}_n} \frac{1}{n!}\sigma$ which is nothing else than the uniform distribution.
For $t \geq 1$, $\frac{1}{t^n} \sum_{k=1}^{n} t^k e_k = \sum_{k=0}^{n-1} \frac{(t-k)^{(n)}}{n! t^n} D_k$ is a probability distribution on $\mathcal{S}_n$. It follows immediately from the orthogonality of the e_k's that

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

In order to generalise this last computation, we extend Garsia's formula 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 $\Psi_n(k,j)$ are the coefficients appearing in the expression of the polynomial

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

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

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

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

$$\Phi_1 = [1] \qquad \Phi_2 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \qquad \Phi_3 = \begin{bmatrix} 1 & -2 & 1 \\ 1 & 0 & -1 \\ 1 & 4 & 1 \end{bmatrix} \qquad \Phi_4 = \begin{bmatrix} 1 & -3 & 3 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 3 & -3 & -1 \\ 1 & 11 & 11 & 1 \end{bmatrix}$$

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

The last row of these matrices is readily seen to be given by the coefficients of the Eulerian polynomials

$$\mathbf{A}_n(x) = \sum_{\sigma \in \mathcal{S}_n} x^{d(\sigma)},$$

hence

$$\Phi_n(n,k) = \mathrm{Card}\{\sigma \in \mathcal{S}_n \mid d(\sigma) = k\}.$$

In general the entries of j^{th} row of Φ_n are the coefficients of $(1-x)^{(n-j)} \mathbf{A}_j(x)$.

4 Example 3

Similar consideration can be made in the context of the group algebra of the hyperoctahedral group ($\mathcal{B}_n$ in the Coxeter's classification), if one considers the semi-simple subalgebra $\Gamma[\mathcal{B}_n]$ 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 $d(\sigma) = \mathrm{Card}\{1 \le i \le n-1 \mid \sigma(i) > \sigma(i+1)\}$.
Recall that elements of $\mathcal{B}_n$ are signed permutations and that for sake of convenience one can set $\sigma(0) = 0$. It was shown in [3] that there is in this context a Garsia like formula

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

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

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

As in the previous case, the last row of the matrices for the Fourier transform is readily seen to be given by the coefficients of the hyperoctahedral descent polynomials

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

and the entries of j^{th} row of Φ_n are the coefficients of $(1-x)^{(n-j)}\mathbf{B}_j(x)$. It is easy to verify that the polynomials $\mathbf{B}_n(x)$ 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

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

References

[1] D. Aldous and P. Diaconis. Shuffling cards ans stopping times. *American Mathematical Monthly*, 93:333–348, 1986.

[2] D. Bayer and P. Diaconis. Trailing the dovetail shuffle to its lair. Technical Report 2, Dept. of Statistics, Stanford University, 1990.

[3] F. Bergeron and N. Bergeron. Orthogonal idempotents in the descent algebra of B_n. *Journal of Pure and Applied Algebra*, accepted in 1991.

[4] A. Garsia. Combinatorics of the free Lie algebra and the symmetric group. In P. H. Rabinowitz and E. Zehnder, editors, *Research papers published in honor of Jurgen Moser's* 60^{th} *birthday*. Academic Press, 1990.

[5] A. Garsia and C. Reutenauer. A decomposition of Solomon's descent algebras. *Advances in Mathematics*, 77(2):189–262, 1989.