PAPER

The Cool'n Tacky al-Khwārizmī

K.TAKAHASHI[1)] G.HIRANO[2)] T.KAIDA[3)] S. KANEMITSU[4)] T. MATSUZAKI[5)]

概要：本論文は、月一回開催している学際セミナーのとくに、2012年度第14回、第15回セミナーで取り上げた「Elucidation and generalization of the Cooley-Tukey algorithm—CTA」において展開した、離散フーリエ変換の計算量を低減するアルゴリズムであるCTAを、群の表現を用いるダイアコーニス等の方法を用いて明らかにし、合わせて群とその表現（とくに群行列）の基礎を述べたものである。本セミナーの目的の一つである、大学教育における新たな教科書を作成する大いなる一歩であると確信している。本論文では、アーベル群の場合をのみを扱っているが、目標は、アウスランダー等の行った、冪零群の場合の非アーベル的フーリエ変換の計算量の低減を目標とする。ダイアコーニスの場合は、表現を付随させたベクトル値関数であり、ヴェンコフの場合のスペクトル理論の精神と類似しており、将来表現論的保型形式の研究にも通ずると信ずる。

Abstract: In this paper, we shall elucidate the celebrated Cooley-Tukey (Cool and Tacky) algorithm [4] from representation-theoretic view point, following [6] in general and [1] in the case of nilpotent groups. We are concerned with non-Abelian Fourier transforms, which have many applications including one of the symmetric groups to statistics. Considering the Fourier transform with vector-valued function is rather efficient and can be studied together with Venkov's theory of automorphic forms with representations [17], [18], to be pursued subsequently.
We shall also give some preliminaries on groups, linear representation of groups and group matrices.

キーワード：クーリータッキーアルゴリズム、有限フーリエ変換、表現論、計算量
Keywords: Cooley-Tukey algorithm (CTA), Discrete Fourier Transforms (DFT), Representation Theory, Amount of computation

1. Cooley-Tukey al-Khwārizmī

Our objective being an elucidation and generalization of the Cooley-Tukey al-Khwārizmī (abbreviated: CTA) in a representation-theoretic as well as a group-theoretic setting, we first reproduce the CTA rather faithfully in slightly modified notation, though.

1.1 Algebraic *intermezzo*

À propos, we recall the origin of two most important terminology, algorithm and algebra. On [12], one finds the passage: Mohammed ibn-Musa al- Khwārizmī composed, in Baghdad (at about 825), what is considered to be the most influential algebraic work of the period— *Kitāb al-jabrwa al- muqābalab* (The science of restoration and reduction). From the title ("al-jabr") comes the word "algebra" that we use today, since this was the first textbook used in Europe on that subject matter. Furthermore, the word "algorithm," used for any special method for solving a mathematical problem using a collection of exact procedural steps, comes from the distortion of al-Khwārizmī's name. *The Science of Restoration* was synonymous with the theory of equations for a few hundred years.

1.2 CTA

In this subsection, we state the CTA in its original form with slightly different notation which is in conformity with [6]. In §7, we shall use the notation of [6]. We write $\hat{f}(j)$ for $X(j)$, $f(k)$ for $A(k)$, and for $A(k_1, k_0)$, we write

(1.1) $$f_{k_0}(k_1) = f(k_1 r_2 + k_0),$$

which corresponds to (6.7).

Table 1. Corresponding notation

CT	$X(j)$	$A(k)$	$A(k_1, k_0)$
DR	$\hat{f}(j)$	$f(k)$	$f_{k_0}(k_1)$
GR	$\hat{f}(\rho)$	$f(\rho)$	$f_i(g_1)$

Let

(1.2) $$N = r_1 r_2$$

be a decomposition of the modulus N and let

(2) $$\zeta = e^{2\pi i/N}$$

be the piervotny$N$th root of 1. We want to compute the Fourier transform at frequency j

(1) $$\hat{f}(j) = \sum_{k=0}^{N-1} f(k)\zeta^{jk}, \quad 0 \le j \le N-1.$$

We write

(3-1) $$k = k_1 r_2 + k_0, \quad 0 \le k_0 \le r_2 - 1,\ 0 \le k_1 \le r_1 - 1.$$

Then (1) reads

(4) $$\hat{f}(j) = \sum_{k_0=0}^{r_2-1} \sum_{k_1=0}^{r_1-1} f(k_1 r_2 + k_0)\zeta^{jk_1 r_2} \cdot \zeta^{jk_0}.$$

Writing

(3-1) $$j = j_1 r_1 + j_0, \quad 0 \le j_0 \le r_1 - 1,\ 0 \le j_1 \le r_2 - 1,$$

we note that

(5) $$\zeta^{jk_1 r_2} = \zeta^{j_0 k_1 r_2},$$

which is the corrected form of [4].

By (5), $\zeta^{jk_1 r_2} = e^{2\pi \frac{j_0}{r_1} i k_1}$, so that the inner sum on the RHS of (4) is the Fourier transform $\widehat{f_{k_0}}$ of $f_{k_0}(k_1) = f(k_1 r_2 + k_0)$ at frequency $j_0 \pmod{r_1}$ (cf. (1.1)):

(6) $$\widehat{f_{k_0}}(j_0) = \sum_{k_1=0}^{r_1-1} f_{k_0}(k_1)\zeta^{j_0 r_2 k_1}.$$

1) 産業理工学部情報学科講師　ktakahas@fuk.kindai.ac.jp
2) 産業理工学部電気通信工学科講師　hira@fuk.kindai.ac.jp
3) 産業理工学部情報学科准教授　kaida@fuk.kindai.ac.jp
4) 産業理工学部情報学科教授　kanemitu@fuk.kindai.ac.jp
5) 産業理工学部電気通信工学科講師　takanori@fuk.kindai.ac.jp

Hence
(7)

$$\hat{f}(j_0,j_1)=\hat{f}(j_0r_1+j_1)=\hat{f}(j)=\sum_{k_0=0}^{r_2-1}\widehat{f_{k_0}}(j_0)\zeta^{jk_0}$$
$$=\sum_{k_0=0}^{r_2-1}\widehat{f_{k_0}}(j_0)\zeta^{(j_1r_1+j_0)k_0},$$

which corresponds to (6.6). I.e., the partial transforms $\widehat{f_{k_0}}$ are pasted together with the twiddle factor $\zeta^{jk_0}=e^{2\pi ijj_0/r_1r_2}$.

There are N^2 operations needed to compute all the Fourier transforms (1), so that for our intended application to symmetric groups, this could lead to a computational explosion. For by the Stirling formula, $N!\sim\sqrt{2\pi n}\left(\frac{N}{e}\right)^n$.

There are N terms in $\widehat{f_{k_0}}(j_0)$, each requiring r_1 operations, giving a total of Nr_1 operations. Similarly, in $\hat{f}(j_0,j_1)$, there is a total of Nr_2 operations needed. Hence it follows that $N(r_1+r_2)$ operations are needed to obtain $\hat{f}$. If we can choose $r_i\sim\sqrt{N}$, then this will give rise to the saving of order $\sqrt{N}$, which is a great saving.

Remark 1. The decomposition (1.2) is a delicate and intriguing problem connected with the RSA cryptosystem. There is no guarantee for a decomposition of N if N is large. On [10] we find the passages. In RSA cryptosystem, care must be taken in choosing the two primes p and q whose product is to be the public key. They are not to be too close (e.g. one must be a few digits longer than the other); $p-1$ and $q-1$ are to have a fairly small g.c.d. and both of them to have at least one large prime factor.

However, for our intended application to symmetric groups, the decomposition is guaranteed from the beginning.

2. Elements of group theory

We start from the elements of group theory. There are many excellent references on group theory, but a very concise but handy manual could be our forthcoming book [11].

Proposition 1.*Any subgroup of a cyclic group G is again cyclic. If G is finite, say $|G|=q$, then there are $\varphi(q)$ generators of G, where $\varphi(q)$ is the Euler function defined by*

$$\varphi(q)=\sum_{\substack{n\le q\\(n,q)=1}}1, \tag{2.1}$$

i.e. the number of integers $n\le q$ which are prime to q.

Proof. Let $G=<a>\neq 1$. Any subgroup $H\neq 1$ of G consists of elements of the form $a^m, m\in\mathbb{Z}$. Let

$$d=\min\{m\in\mathbb{N}|a^m\in H\}.$$

Then d must divide all m for which $a^m\in H$. For writing

$$m=dm'+r,\ 0\le r<d,$$

we have $a^m=(a^d)^{m'}a^r$, so that $a^r\in H$ and $r=0$. Hence any $a^m\in H$ is of the form $(a^d)^{m'}\in<a^d>$, whence $H=<a^d>$.

Now suppose G is finite and let the order of a(which is the order of G) be q, where the order of an element a is the smallest natural number such that $a^k=1$. The subgroup $H=<a^d>$ coincides with $G=<a>$ if and only $a\in<a^d>$, i. e, there is an integer m' such that

$$dm'\equiv 1\,(\mathrm{mod}\ q),$$

which is true if and only if $(d,q)=1$. Since there are $\varphi(q)$ such d's, the second assertion follows. □

Example 1.*Let μ_q denote the set of all q-th roots of 1:*

$$\mu_q=\{z\in\mathbb{C}|z^q=1\}.$$

Then μ_q is a cyclic group generated e. g. by $e^{2\pi i/q}$ – piervotnyi koren'.

Note that we may also prove this directly as follows. Clearly, $e^{2\pi i/q}$ is a generator of μ_q and $\mu_q=\{e^{2\pi ia/q}|a=0,1,\cdots,q-1\}$. For another member $e^{2\pi id/q}$ to be a generator, it is necessary and sufficient that $e^{2\pi i/q}\in<e^{2\pi id/q}>$, i.e that there is an integer x such that $dx\equiv 1\,(\mathrm{mod}\ q)$. The last holds if and only $(d,q)=1$ since then there are integers x, y such that $dx+qy=1$.

Example 2.*The group of residue classes modulo q is an additive cyclic group of order q generated by $1+q\mathbb{Z}$. The group of reduced residue classes modulo a prime is a cyclic group generated by a primitive root.*

Proposition 2. *Let $G=<a>$ be a cyclic group of order n. Then for every divisor d of n there exists a unique subgroup of order d with $\varphi(d)$ generators and we have the identity*

$$\sum_{d|n}\varphi(d)=n. \tag{2.2}$$

Proof. Recall from Proposition 1 that there are $\varphi(n)$ generators in G including a.

Now for each divisor d of n, the element $a^{n/d}$ generates a subgroup H_d of order d.

There are $\varphi(d)$ generators of H_d and $H_d\,(d|n)$ exhaust all the elements of G: $G=\cup_{d|n}H_d$ (disjoint). Hence (2.2) follows as the cardinality of both sides. □

The following theorem is a fundamental structure theorem for finite Abelian groups.

Theorem 1.*If G is a finite Abelian group, it is isomorphic to the direct product of cyclic groups of prime power order.*

This is a consequence of Theorem 2 with $R=\mathbb{Z}$:

Theorem 2.*Let R be a PID (principal ideal domain) and let M be a finitely generated R-module. Then M is isomorphic to*

$$R/e_1R\oplus\cdots\oplus R/e_lR,$$

where e_i may be chosen so that $e_i|e_{i+1}$ $(1\le i\le l-1)$ and in choosing so, they are uniquely determined up to associates. Or more concretely,

$$\mathbb{Z}/a_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/a_l\mathbb{Z}\oplus\underbrace{\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}}_{r\ times}, \tag{2.3}$$

where $1<a_1$, $a_i|a_{i+1}$ $(1\le i\le l-1)$ and the product $a=a_1\cdots a_l$ and r are uniquely determined.

$e_1,\cdots,e_l$ or $a_1,\cdots,a_l$ are called **elementary divisors**. r is called the R-**rank** of M. In the case of Theorem 1, $r=0$.

Definition 1.*Let H be a subgroup of a group G. Define a relation $\sim$ between elements x, y in G: $x \sim y$ if there exists an $a \in H$ such that $y = ax$. Then one can prove that this is an equivalence relation. The equivalence class containing $x \in G$ is of the form $Hx = \{ax | a \in H\}$ and is called the* **right coset**, *whose cardinality is $|H|$. If $H \setminus G = \{Hx_\nu | \nu \in N\}$, and $G = \bigcup_\nu H x_\nu$ (disjoint), is the right coset decomposition of G, then $\{x_\nu\}$ is called a* **complete set of right representatives***of G with respect to H. In a similar way, we may consider the* **left coset***decomposition of G with respect to H: $G/H = \{x_\mu H | \mu \in M\}$, with x_μ a complete set of left representatives of G with respect to H.*

Theorem 3.*The following two conditions are equivalent.*
$\{x_\nu\}$ forms a complete set of right representatives: $H \setminus G = \{Hx_\nu\}$.
$\{x_\nu^{-1}\}$ forms a complete set of left representatives: $G/H = \{x_\nu^{-1}H\}$.

Proof. Suppose the first is true. It is enough to show that $\{x_\nu^{-1}H\} = G/H$, i.e. that $x_\nu^{-1}H \neq x_\mu^{-1}H$ if $x_\nu = x_\mu$ and that any $a \in G$ is contained in some $x_\nu^{-1}H$. The first because if $x_\nu^{-1}H = x_\mu^{-1}H$, then $Hx_\nu = (x_\nu^{-1}H)^{-1} = \left(x_\mu^{-1}H\right)^{-1} = Hx_\mu$, whence $x_\nu = x_\mu$.
The second because for any $a \in G$, there exists an x_ν such that $a^{-1} \in Hx_\nu$, which means that there exists a $y \in H$ such that $a^{-1} = yx_\nu$. Hence $a = x_\nu^{-1}y^{-1} \in x_\nu^{-1}H$.□

Theorem 3 asserts that the cardinality of right cosets and left cosets are equal. If it is finite, we denote it by

$$(G:H)$$

and call it the **index** of H in G. Since each coset has $|H|$ elements, we have an important identity

(2.4) $$|G| = (G:H)|H|.$$

This is also valid for $|G| = |H| = \infty$ by interpreting both sides to be ∞. An example is

$$|\mathbb{Z}| = (\mathbb{Z}:q\mathbb{Z})|q\mathbb{Z}|,$$

where in this case $(\mathbb{Z}:q\mathbb{Z})$ is the order of the additive group $\mathbb{Z}/q\mathbb{Z}$ of residue classes mod q, $q \in \mathbb{N}$ (see below). Since each group contains the trivial group consisting of the identity element only, we have $|G| = (G:\{1\})$. Any subgroup N of the group G is called a **normal subgroup** if its right and left cosets coincide, i.e. $aN = Na$ for all $a \in G$, or what amounts to the same, N is invariant under the inner automorphism of G (in Example 4). Then one may form the quotient group G/N and the group index above is precisely the order of the quotient group G/N:

(2.5) $$(G:N) = |G/N|.$$

Eq.(2.4) gives the following chain of indices

(2.6) $$|G| = (G:G_1)(G_1:G_2)\cdots(G_{m-1}:G_m).$$

for the chain of subgroups

(2.7) $$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m.$$

For finite groups, the following corollary is fundamental.

Corollary 1.*(Lagrange). Let G be a finite group and let H be its subgroup. Then the order of H divides that of G:*

(2.8) $$|H| \,|\, |G|$$

and $|G|/|H| = (G:H)$.

3. Group actions

Theorem 4.(Burnside)*Let G be a transformation group on X, and let C_x be the class containingx. Then for a fixed element $x \in X$, the set $\mathcal{F}(x) = \{a \in G | ax = x\}$ forms a subgroup of G (called the* **stabilizer (of x)***) and we have $|G| = \#C_x|\mathcal{F}(x)|$, or*

(3.1) $$\#C_x = (G:\mathcal{F}(x)).$$

Proof. It is easy to see that $\mathcal{F}(x)$ forms a subgroup. Also it is easy to prove that the relation $a \sim b$ defined in G as follows, is an equivalence relation: $a \sim b$ if $ax = bx$. We denote the equivalence class containing a by $\widetilde{C_a}$. Since each element ax of C_x gives rise to one $\widetilde{C_a}$ of G consisting of all elements b of G such that $bx = ax$, G is decomposed into $\#C_x$ equivalence classes: $G = \bigcup_{i=1}^{\#C_x} \widetilde{C_{a_i}}$ (disjoint).

Now, since $b \in \widetilde{C_a}$ is equivalent to $bx = ax$, or $a^{-1}b \in H_x$, or to $b \in a\mathcal{F}(x)$, we have $\#\widetilde{C_a} = \#a\mathcal{F}(x) = |\mathcal{F}(x)|$. Hence each class $\widetilde{C_{a_i}}$ in $G/\sim$ contains the same number $|\mathcal{F}(x)|$ of elements, and so this proves the assertion. □

Example 3.*Recall Definition 1 in which we defined the equivalence of two elements a, b of a group G modulo a subgroup H of G. We may interpret Example 1 as the action of a subgroup H on $X = G$. Indeed, defining the action of H on G by $a(x) = ax$, $a \in H$, $x \in G$, we find that the orbit containing $x \in G$ is Hx, the right coset containing x, whose cardinality is $|H|$ and the stabilizer of x is 1. Hence* (3.1) *leads to a triviality $|H| = |Hx|$.*

Example 4. *If G is a group, two elements $x, y \in G$ are called* **conjugate** *if there is an element $a \in G$ such that $y = a^{-1}xa$. Viewed as a mapping, the correspondence $I_a(x) = a^{-1}xa$ is called the* **innerautomorphism**. *Let*

(3.2) $$C_G(x) = \{a \in G | a^{-1}xa = x\}$$

*be the***centralizer***of $x \in G$. We may define an action of G on G by*

(3.3) $$a(x) = I_a(x) = a^{-1}xa$$

Then the orbit containing x is called the **conjugateclass** *containing x and the centralizer is the stabilizer $\mathcal{F}(x)$ of x. Hence Theorem 4 implies that the number g_x of elements of the conjugate class C_x containing x has $(G:C_G(x))$ elements and a fortiori is a divisor of $|G|$. Since the conjugate class decomposition is a classification of G, we have the* **class equation**

(3.4) $$|G| = \sum_{\substack{x \in G \\ x:\, non-conjugate}} g_x.$$

Exercise 1.*Prove that the conjugacy is an equivalence relation, that (3.3) defines an action and that the centralizer is a subgroup. Also prove that the inner automorphism is an automorphism.*

4. Group matrices

Definition 2.*Let G be a finite group with $|G| = g$ elements. A homomorphism*

$$\rho:\ G \to \mathrm{GL}_n(\mathbb{C}),\quad \rho(\sigma) = S_\sigma,$$

*is called a***representation of order***n and we denote the set of all representations of order n by $\Gamma = \Gamma_n$. Here $\mathrm{GL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ indicates general linear group of all regular matrices of degree n in the ring of matrices of degree n with complex entries. One may consider a more general situation of the case of a module over a ring, but we restrict to the case of a field and then all representations may be considered as matrix representations.*

Let x_σ be the indeterminate corresponding to each element $\sigma \in G$
The matrix

$$X = \sum_{\sigma \in G} S_\sigma x_\sigma$$

*is called the***group matrix** *corresponding to* Γ.

Definition 3.*Given a group matrix X, if there exists a group matrix similar to X, of the form* $\begin{pmatrix} X_1 & 0 \\ * & X_2 \end{pmatrix}$, *Then X is called reducible. If there is no such a similar group matrix (save for the zero matrix), X is called irreducible.*

The corresponding representation is called **reducible***or***irreducible***as the case may be.*

Theorem 5. *A degree n group matrix X of rank r is similar to a matrix of the form*

$$\begin{pmatrix} X_1^* & & & & & \\ & \ddots & & & & \\ & & X_1^* & & O & \\ & & & \ddots & & \\ & O & & & X_h^* & \\ & & & & & \ddots \\ & & & & & & X_h^* \\ & & & & & & & O \end{pmatrix}. \tag{4.1}$$

with r_j copies of an irreducible matrix X_j^* $(1 \le j \le h)$, where the last diagonal element is the zero-matrix of degree $n - r$.

Definition 4.*The number r_j of the copies of an irreducible matrix X_j^* is called the***index***of X_j^* in X, and the totality of indices $\{r_1, \cdots, r_h\}$ is called the***index system** *of X.*

To determine h, we introduce

Definition 5.*Let*

$$X = (x_{\sigma^{-1}\tau}) \quad (\sigma, \tau \in G) \tag{4.2}$$

and call it the **regular group matrix**, *where $x_{\sigma^{-1}\tau}$ is the (i, j)-entry of X for $\sigma = \sigma_i$, $\tau = \sigma_j$.*

Theorem 6.*If in the system of indices $\{r_1, \cdots, r_{h^*}\}$ of the regular group matrix X, $\{r_1, \cdots, r_h\}$ are positive $(h \le h^*)$ and the remaining ones are 0, then*

$$r_j = f_j \quad (1 \le j \le h) \tag{4.3}$$

where f_j is the degree of the irreducible matrix X_j^* in Theorem 5.

Further the number h coincides with the number of conjugate classes of G.

Corollary 2.*The number h^* of irreducible matrices (of degree n) which are not conjugate each other is equal to the number h of conjugate classes of G*

$$h^* = h \tag{4.4}$$

Definition 6.*In a representation Γ of a finite group G, the trace of the matrix S_σ corresponding to σ is called a* **character** *of Γ and denoted by $\chi(\sigma)$.*

$$\chi(\sigma) = Tr(S_\sigma),\quad \sigma \in G$$

There are g characters of G. Those which corresponding to irreducible representations are called **simple characters**.

$$\chi_1(\sigma), \cdots, \chi_h(\sigma).$$

Let $r_1, \cdots, r_h$ be the system of indices of the group matrices corresponding to Γ, we express it as

$$\Gamma \sim r_1\Gamma_1 + \cdots + r_h\Gamma_h, \tag{4.5}$$

where the group matrix X_j corresponding to Γ_j.

By Theorem 6,

$$\chi(\sigma) = r_1\chi_1(\sigma) + \cdots + r_h\chi_h(\sigma). \tag{4.6}$$

Theorem 7.*We have the orthogonality relation*

$$\sum_j f_j \chi_j(\sigma) = \begin{cases} g, & \sigma = 1 \\ 0, & otherwise \end{cases} \tag{4.7}$$

5. Matrix representation of groups

Let $\mathrm{P} = \{\rho\} = \{\rho_1, \cdots, \rho_h\}$ be the set of all irreducible representations (of degree d_ρ) belonging to G. Then in the notation of Diaconis-Rockmore [6], (4.7) reads

$$\sum_{\rho \in \mathrm{P}} d_\rho \,\mathrm{Tr}(\rho(s)) = \begin{cases} |G|, & s = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{5.1}$$

We note the important relation

$$\sum {d_\rho}^2 = |G|, \tag{5.2}$$

whence it follows that $d_\rho \le \sqrt{|G|}$.

As in Diaconis and Rockmore [6], for any scalar function f on G, define its **Fourier transform** at ρ by

$$\hat{f}(\rho) = \sum_{s \in G} f(s)\rho(s). \tag{5.3}$$

Then

$$\begin{aligned} &\sum_{\rho \in \mathrm{P}} d_\rho \,\mathrm{Tr}\{\rho(r^{-1})\hat{f}(\rho)\} \\ &= \sum_{\rho \in \mathrm{P}} d_\rho \sum_{s \in G} f(s)\,\mathrm{Tr}(\rho(r^{-1})\rho(s)) \\ &= \sum_{s \in G} f(s) \sum_{\rho \in \mathrm{P}} d_\rho \,\mathrm{Tr}(\rho(r^{-1}s)) \\ &= |G| f(r) \end{aligned} \tag{5.4}$$

by (5.1). Hence the inversion formula holds:

$$f(r) = \frac{1}{|G|} \sum_{\rho \in \mathrm{P}} d_\rho \,\mathrm{Tr}\{\rho(r^{-1})\hat{f}(\rho)\}. \tag{5.5}$$

Let $T(G)$ denote the number of operations needed to calculate all the Fourier transforms of a finite group G at all its irreducible representations and let $M(d)$ denote the number of operations needed to multiply $d \times d$ matrices. It is assumed that $M(d) \sim d^2$. Then

direct computation of (43) requires $|G|\rho_d$ operations, whence we obtain $T(G) \sim |G|^2$ in view of (5.2).

Theorem 8.*Let H be a subgroup of a finite group G with index $k = (G:H)$, which is $|G|/|H|$ in the present case. Let*

$$G = s_1 H \cup \cdots \cup s_k H \quad (s_1 = 1)$$

be a coset decomposition. Then

$$\hat{f}(\rho) = \sum_{i=1}^{k} \rho(s_i) \sum_{h \in H} f_i(h)\rho(h)$$

$$= \sum_{i=1}^{k} \rho(s_i) \begin{pmatrix} \widehat{f_i}(\rho_1') & & 0 \\ & \ddots & \\ 0 & & \widehat{f_i}(\rho_j') \end{pmatrix}, \tag{5.6}$$

where

$$f_i(h) = f(s_i h), \quad 1 \le i \le k. \tag{5.7}$$

$\widehat{f_i}(\rho_\ell')$ may appear in several blocks as i varies over $1 \le i \le k$ and ℓ varies over irreducible representations of H, but these need to be calculated once, which is the heart of saving!

6. Group-theoretic interpretation of the CTA

Cooley and Tukey viewed their algorithm as "divide and conquer" algorithm ([1]). In this section, we follow [6] to give a group-theoretic interpretation of the CTA. For Abelian groups, the algorithm in §5 reduces to the CTA. Here we restrict to the Fourier transform on the residue classes $\mathbb{Z}/N\mathbb{Z}$, with $N = r_1\kappa_0$ (we now write κ_0 for r_2). We view $\mathbb{Z}/r_1\mathbb{Z}$ as embedded in $\mathbb{Z}/r_1\kappa_0\mathbb{Z}$ schematically as $0, \kappa_0, 2\kappa_0, \cdots, (r_1 - 1)\kappa_0$ and the natural choice of coset representative is

$$0,1,2,\cdots,\kappa_0 - 1 \tag{6.1}$$

and the coset decomposition is

$$(\mathbb{Z}/r_1\kappa_0\mathbb{Z})/(\mathbb{Z}/r_1\mathbb{Z}) = (\mathbb{Z}/r_1\mathbb{Z}) \oplus (1 + \mathbb{Z}/r_1\mathbb{Z}) \oplus \cdots \oplus (\kappa_0 - 1 + \mathbb{Z}/r_1\mathbb{Z}). \tag{6.2}$$

We may give an interpretation of this as follows in case r_1, κ_0 are relatively prime: $(r_1, \kappa_0) = 1$, where the parenthesis indicates the gcd of two integers. For then we have the decomposition into the direct product

$$\mathbb{Z}/r_1\kappa_0\mathbb{Z} \cong \mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/\kappa_0\mathbb{Z}. \tag{6.3}$$

Since what is stated amounts to the quotient group $(\mathbb{Z}/r_1\kappa_0\mathbb{Z})/(\mathbb{Z}/r_1\mathbb{Z})$, (6.3) gives an isomorphism

$$(\mathbb{Z}/r_1\kappa_0\mathbb{Z})/(\mathbb{Z}/r_1\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/\kappa_0\mathbb{Z}, \tag{6.4}$$

whence (6.2) follows.

Group-theoretically, we may express what precedes as

$$G_0 = G = \mathbb{Z}/r_1\kappa_0\mathbb{Z} \supset G_1 = \mathbb{Z}/r_1\mathbb{Z} \tag{6.5}$$

with $\kappa_0 = |G_0|/|G_1| = (G_0 : G_1)$ and Theorem 8 reads

Theorem 9.*Let G_1 be a subgroup of the finite group $G = G_0$ with index $\kappa_0 = (G_0 : G_1)$, which is $|G_0|/|G_1|$ in the present case. Let*

$$G = s_1 G_1 \cup \cdots \cup s_{\kappa_0} G_1 \quad (s_1 = 1)$$

be the coset decomposition. Then

$$\hat{f}(\rho) = \sum_{i=1}^{\kappa_0} \rho(s_i) \sum_{g_1 \in G_1} f_i(g_1)\rho(g_1) \tag{6.6}$$

where ρ is an irreducible representation of G (in CTA case, it is the exponential function) and

$$f_i(g_1) = f(s_i g_1), \quad 1 \le i \le \kappa_0 \tag{6.7}$$

correspondingly to(1.1).

(6.6) implies

$$T(G_0) = \kappa_0 T(G_1) + \kappa_0 |G_0|. \tag{6.8}$$

The new al-Khwārizmī given in Theorem 8 or Theorem 9 may be applied to any chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_m \supset G_{m+1} = 1, \tag{6.9}$$

where in the last step of recursion, the Fourier transform on G_m is to be computed directly.

For the group of binary n-tuples $(\mathbb{Z}/2\mathbb{Z})^n$ the algorithm reduces to the standard **fast Walsh transform**.

For Abelian groups, Theorem 1 provides a direct sum decomposition into cyclic groups of prime power order. Then Proposition 2 gives a decreasing chain of cyclic subgroups of prime power order $p^\alpha, p^{\alpha-1}, \cdots, p$ for each highest prime power p^α dividing G.

Let $T(G)$ denote the number (or an optimal estimate) of operations needed to calculate all the Fourier transforms of a finite group G and let $M(d)$ denote the number of operations needed to multiply $d \times d$ matrices. It is assumed that $M(d) \sim d^2$.

Theorem 10.(Diaconis-Rockmore)*The chain of subgroups that minimizes the number of operations $T(G)$ is such that the sum $\sum_{i=0}^{m}(G_i : G_{i+1})$ of group indices of the chain (54) is minimal.*

This follows from

$$T(G) = |G| \sum_{i=0}^{m} (G_i : G_{i+1}), \tag{6.10}$$

which in turn follows recursively from (6.8).

The fast Walsh transform for $(\mathbb{Z}/2\mathbb{Z})^n$ is assured to be the fastest or to be the one with minimum amount of computations by Theorem 10 in view of the chain

$$(\mathbb{Z}/2\mathbb{Z})^n \supset (\mathbb{Z}/2\mathbb{Z})^{n-1} \supset \cdots \supset 1. \tag{6.11}$$

Suppose G has a chain of subgroups similar to (2.7) or (6.9), i.e.

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset 1 \tag{6.12}$$

for which H_i is a normal subgroup of H_{i-1}, whence the quotient groups H_{i-1}/H_i being formed. If all these quotient groups are Abelian, then the chain (57) is called an **Abelian normal chain** and a group with an Abelian normal chain is called a **solvable group**. An Abelian group is a solvable group, but not conversely. These notions floated in the struggle of Abel and Galois in establishing the solvability of algebraic equations.

If in particular, the chain has the property that all H_i's are normal subgroups of G, thereby the quotient groups G/H_i being formed, and that

$$H_{i-1}/H_i \supset Z(G/H_i), \tag{6.13}$$

where $Z(G)$ is the **center** of the group G, which is the group of elements that commute with every element of G, then the chain is called a **central chain** and any group with a central chain is called a **nilpotent group**.

In the subsequent researches, we shall deal with similar problems of complexity of computations for nilpotent groups and those between nilpotent and solvable [20].

7. AusländischeAufgaben der Cool u. Tacky Algorithm

In this section, we use the notation of [6], i.e. $\hat{f}(j) = X(j)$, $f(k) = A(k)$, and $f_{k_0}(k_1) = f(k_1 r_2 + k_0) = A(k_1, k_0)$.

Letting $\zeta = \zeta_N$ be a primitive N-th root of 1, we define the *Fourier matrix*$F = F(N)$ on N points by

(7.1)
$$F = \left(\zeta^{jk}\right) = \begin{pmatrix} 1 & -1 & \cdots & 1 \\ 1 & \zeta^{-1} & \cdots & \zeta^{-(N-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \zeta^{-(N-1)} & \cdots & \zeta^{(N-1)(N-1)} \end{pmatrix},$$

where $0 \le j \le N-1$, $0 \le k \le N-1$. Then (1) reads

(7.2)
$$X(j)(= \hat{A}(j)) = \sum_{k=0}^{N-1} A(k)\zeta^{jk}, \quad 0 \le j \le N-1,$$

or

(7.3)
$$F(N)A = X,$$

where $A = \begin{pmatrix} A(0) \\ \vdots \\ A(N-1) \end{pmatrix}$ and $X = \begin{pmatrix} X(0) \\ \vdots \\ X(N-1) \end{pmatrix}$ are column vectors.

We define the **Fourier matrix**F by means of its conjugate transpose F^*:

(7.4)
$$F^* = \frac{1}{\sqrt{N}}\left(\zeta^{(i-1)(j-1)}\right) = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta & \cdots & \zeta^{N-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \zeta^{N-1} & \cdots & \zeta^{(N-1)(N-1)} \end{pmatrix},$$

where we mean ζ^{-1} by the conjugate of ζ i.e. ζ^{N-1}.

Theorem 11.([5])*Any circulant matrix C can be diagonalized as*

(7.5)
$$C = F^*\Lambda F$$

by the Fourier matrix F, where

(7.6)
$$\Lambda = \Lambda_C = \begin{pmatrix} p_\gamma(1.1) & 0 & \cdots & 0 \\ 0 & p_\gamma(\zeta) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & p_\gamma(\zeta^{N-1}) \end{pmatrix}.$$

Thus, in particular, the eigenvalues of C are $p_\gamma(1.1)$, $p_\gamma(\zeta)$, ..., $p_\gamma(\zeta^{n-1})$.

This was used in [8] to give a one-line proof of the Blahut theorem (referred to in [15]). In [4], by the Fourier matrix, it is meant (7.4) rather than its conjugate.

Lessons to learn:
Where there is smoke, there is fire.
Where there is a will, there is a way.
If there is a will, there may be no way.

We state the record of the seminars.

The 12th seminar (Feb. 22): “Legitimation of the use of fancy tools in engineering disciplines”

The 13th seminar (Apr. 25): Final check of the draft for the paper [7]

The 14th seminar (May 30): “Elucidation and generalization of the Cooley-Tukey al -Khwārizmī”

The 15th Seminar (Jun. 27): Supposed to be the penultimate checking of the present paper “The Cool’n Tacky al- Khwārizmī”, but failed to be organized because of the bad choice of the venue, the log -house, where there was too big a fuss to organize a sem.

References

[1]L. Auslander, R. Tolimieri and S. Winograd, Hecke’s theorem in quadratic reciprocity, finite nilpotent groups and the Cooley-Tukey algorithm, *Adv. Math.* (1982), 122-172.

[2]E. O. Brigham, *The Fast Fourier Transform*, Prentice-Hall, New Jersey 1974.

[3]N.-X. Chen, *Möbius inversion in physics*, World Sci., New Jersey, London, Singapore etc. 2012.

[4]J. W. Cooley and J. W. Tuckey, An algorith for machine calculation of complex Fourier series, *Math. Comp.* (1965), 297-301.

[5] Ph. J. Davis, Circulant matrices, Wiley New York etc. 1979.

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

[7] G. Hirano, K. Takahashi, T. Kaida, S. Kanemitsu and T. Matsuzaki, Legitimation of the use of fancy tools, Kayanomori (2012), to appear.

[8] L. Jiang, S. Kanemitsu and H. KitajimaCirculants, linear recurrences and codes, to appear.

[9] S. Kanemitsu and M. Waldschmidt, Matrices for finite abelian groups, finite Fourier transforms and codes, to appear.

[10] N. Koblitz, A course in number theory and cryptography, Springer Verl., New York-Berlin-Heidelberg etc. 1987.

[11] F.-H. Li, N.-L. Wang and S. Kanemitsu, *Number Theory and its Applications*, to appear, WS, 2012.

[12] M. Livio, *The Golden Ratio*, REVIEW, London 2002.

[13] R. M. Merseau and T. C. Speake, A unified treatment of Cooley-Tukey algorithm for evaluation of the multidimensional DFT, *IEEE Trans. Acoustics and Signal Processing* , No. 5 (1981), 1011-1017.

[14] D. J. Rose, Matrix identities of the fast Fourier transform, *Lin. Alg. Appl.* (1980), 423-443.

[15] K. Takahashi, G. Hirano, T. Kaida, S. Kanemitsu, H. Tsukada and T. Matsuzaki, Record of the second and the third interdisciplinary seminars, Kayanomori (2011), 64-72.

[16] K. Takahashi, G. Hirano, T. Kaida, S. Kanemitsu and T. Matsuzaki On linear recurrences and their applications, Kayanomori (2011), 13-20.

[17] A. B. Venkov, Spectral theory of automorphic functions, *Trudy Mat. Inst. Steklov* (1981), 3-171=Proc. Inst. Math. Steklov (1982), issue , 1-163.

[18] A. B. Venkov, *Spectral Theory of Automorphic Functions and its Applications*, Kluwer Acad. Publ., Dordrecht etc. 1990.

[19]H. J. Weaver, Applications of discrete and continuous Fourier transforms, Wiley, New York etc. 1983.

[20] M. Weinstein, Between nilpotent and solvable, Polygonal, Passaic, NJ 1982.

[21] A. Wintner, Arithmetical Approcah to Ordinary Fourier Seies, Wavery Press, Baltimore 1947.