Annales Univ. Sci. Budapest., Sect. Comp. 54 (2023) 161–170

DISCRETE FOURIER TRANSFORM AND AUTOMORPHISM

János Gonda (Budapest, Hungary)

Communicated by Péter Burcsi
(Received April 30, 2023; accepted August 10, 2023)

Abstract. It is well known that in the discrete Fourier transform of a real vector, the components are not completely independent of each other, namely, in the case of $1 \leq i < n$, in the transformed vector the component belonging to the index $n-i$ is the conjugate of the i-th component. In the following article, we generalize this fact to the case of an arbitrary field and an arbitrary automorphism of that field.

In this article $\mathbb{N}$ denotes the non-negative integers, $\mathbb{N}^+$ the positive ones, $\mathbb{F}_q$ denotes the field of q elements and e denotes the neutral element of the multiplicative semigroup of a ring.

1. Introduction

Integral transformations are important and thoroughly studied procedures in mathematics. One of them is the Fourier transform, which has very important applications in physics and engineering sciences based on it, especially in mechanical and electrical engineering. The general spread of digital technology brought with it the widespread use of the discrete version, the discrete Fourier transform, for example in signal processing. The discrete Fourier transform and its inverse can be easily determined and can be quickly calculated using the fast Fourier transform, making it an important and useful tool. In certain aspects, if the transformation is performed with special data, the transformed vector can also show a special property, so it is interesting to investigate such cases.

Key words and phrases: Discrete Fourier transform, automorphism.
2010 Mathematics Subject Classification: 65T50.

There is a generalization of the discrete Fourier transform that acts on finite Abelian groups, often called a group-theoretic transform, or GTT for short. [3] deals with the connection of the GTT and the automorphism group. This article examines the relationship between the permutation of input signals and the rearrangement of transformed signals. An important result of this article is that if the signals are constant over each of the orbits of the permutations of the input data then the same is true for the output signals.

Also another article deals with the effect of changes in the order of data on the discrete Fourier transform. In [2] the authors study classical DFT, the discrete Fourier transform over the field of complex numbers. For them, too, the main question is what is the relationship between the permutation of input signals and the permutation of transformed signals. They investigate what permutation does not change the set of output signals or the collection of the absolute values of the output signals. The question is important, for example, in the encryption of speech signals.

The automorphism of a finite algebraic structure is also a permutation of the elements of the set and this relationship is also evident in the two articles mentioned above.

In the article below, we examine the question, what is the effect on the output elements of the discrete Fourier transform if the input signals are elements of a subfield invariant against an automorphism acting on the field containing the data.

1.1. On the discrete Fourier transform, on the DFT

The discrete Fourier transform can be introduced and discussed in many ways. We define and examine it below from a strongly algebraic point of view. Although it is possible to define the discrete Fourier transform over more general structures, in this article we only deal with questions that talk about the transform over a field, so we will investigate DFT only over fields.

In the following the set of the elements of an algebraic structure, say $\mathcal{A}$ is denoted by A.

If $\mathcal{K} = (K; +, \cdot)$ is a field and $n \in \mathbb{N}$, then K^n by component-wise addition and multiplication, that is, the n-th direct sum of the field and by multiplying the elements of K^n by the elements of K as a scalar is an n-rank algebra over $\mathcal{K}$. In the following, the addition and multiplication of the elements of K^n are denoted by the operation symbols in $\mathcal{K}$. $(K^n; +, \cdot)$ is a commutative ring with a neutral element, where the neutral element is the n-tuple of which all components are e, the neutral element of $\mathcal{K}$. This ring is zero-divisor free if and only if $n = 1$.

Another algebra is obtained if the addition and the scalar multiplication are the same as before, but the multiplication is a cyclic convolution denoted by $*$, i.e. if $\mathbf{u}$ and $\mathbf{v}$ are two not necessarily different elements of K^n, then $\mathbf{w} = \mathbf{u} * \mathbf{v}$ is the n-tuple in K^n whose components with index $n > i \in \mathbb{N}$ are $w_i = \sum_{j=0}^{n-1} u_j v_{(i-j) \bmod n}$ respectively. Also this algebra is commutative, has a neutral element, namely the n-tuple, where the component, belonging to the index of 0, is the identity of $\mathcal{K}$ and every other component of the vector is 0, and is zero-divisor free if and only if $n = 1$.

Now let n be a positive integer, $\mathcal{K}$ be a field, z an n-th root of unity over $\mathcal{K}$, and let $\mathbf{A}_z$ be an n-order quadratic matrix where the element associated with the index pair $n > i \in \mathbb{N}$, $n > j \in \mathbb{N}$ is $a_{i,j}^{(z)} = (z^{-i})^j$. This matrix is symmetric, as $a_{j,i}^{(z)} = (z^{-j})^i = z^{-ji} = z^{-ij} = (z^{-i})^j = a_{i,j}^{(z)}$. The determinant of the matrix is of Van der Monde type, so the matrix has an inverse if and only if the generator elements are different in each pair. This condition is equivalent to z being a primitive n-th root of unity. There is a primitive n-th root of unity over a field for a given positive integer n exactly in the case if n is not divisible by the characteristic of the field. This is obviously true for a field with characteristic 0, in which case n can be any positive integer, while in the other case the characteristic is some prime number p, in which case n cannot be a multiple of p. Easy calculation shows that if the order of z is n, then $\mathbf{A}_z\mathbf{A}_{z^{-1}} = n\mathbf{I}^{(n)} = (ne)\mathbf{I}^{(n)}$, where $\mathbf{I}^{(n)}$ is the n-th order unit matrix over $\mathcal{K}$. Since n is not divisible by the characteristic of the field, $ne \neq 0$, ne has an inverse, so from $\mathbf{A}_z\mathbf{A}_{z^{-1}} = (ne)\mathbf{I}^{(n)}$ we get that $\mathbf{A}_z^{-1} = (ne)^{-1}\mathbf{A}_{z^{-1}}$.

Now we are looking for a relationship between the two rings previously constructed over K^n using $\mathbf{A}_z$. But first, let's see what the set $\{\mathbf{A}_z\mathbf{u} | \mathbf{u} \in K^n\}$ will be. From now on if $\mathbf{u}$ is an element of K^n, then $\mathbf{A}_z\mathbf{u}$ is denoted by $\mathbf{U}$, and if $\mathbf{A}_z$ has inverse, then $\mathbf{A}_z^{-1}\mathbf{U}$ is denoted by $\mathbf{u}$. Let first $\mathbf{u}$ be such that all of the components are 0, except for one with index 0, which is equal to an arbitrary element c of K. Then $U_i = \sum_{j=0}^{n-1} (z^{-i})^j u_j = u_0 = c$, so $K \subseteq \{(\mathbf{A}_z\mathbf{u})_i | \mathbf{u} \in K^n\}$ for any nonnegative integer i less than n. Secondly, let's look at the vector whose components are again 0, except for the last one, the one belonging to the index $n-1$, which this time should be the unity of the field, that is, e. In this case, $U_i = \sum_{j=0}^{n-1} (z^{-i})^j u_j = (z^{-i})^{n-1} u_{n-1} = z^i e = z^i$, which in turn shows that $z^i \in \{(\mathbf{A}_z\mathbf{u})_i | \mathbf{u} \in K^n\}$, so a field that contains the i-index components of image vectors must contain $K(z^i)$. However, for any $\mathbf{u} \in K^n$ in such a field, the field contains $\sum_{j=0}^{(n-1)} (z^{-i})^j u_j$, too, so $K(z^i)$ is the narrowest field containing the i-index elements of the image vectors. This is also true for $i = 1$, and since for any integer i, $K(z^i) \subseteq K(z)$, then any $\mathcal{L}$ field with which $\{\mathbf{A}_z\mathbf{u} | \mathbf{u} \in K^n\} \subseteq L^n$, is an extension of $K(z)$, which can also be $K(z)$.

By a small calculation, it can be seen that if $\mathcal{K}$ and $\mathcal{L}$ are fields, n is a positive integer, z is an n-th root of unity over $\mathcal{K}$, and $K(z) \subseteq L$, then the correspondence $\mathbf{u} \mapsto \mathbf{A}_z\mathbf{u}$ mapping K^n into L^n is surjective only if and injective exactly in the case if z is a primitive n-th root of unity.

Theorem 1.1. *Let $n \in \mathbb{N}^+$, $\mathcal{K}$ be a field, z an n-th root of unity over $\mathcal{K}$, and $\mathcal{L}|\mathcal{K}(z)$. Then $\mathbf{u} \mapsto \mathbf{A}_z u$ is a $\varphi : (K^n; +, *) \to (L^n; +, \cdot)$ algebra homomorphism, which is an isomorphism exactly if the order of z is equal to n and $L \subseteq K$.*

Proof. Even before the theorem was stated, we saw that $Im(\varphi) \subseteq (K(z))^n$, and it is certainly true that for every element of K^n, $\mathbf{A}_z\mathbf{u}$ is clearly defined, so φ is indeed a mapping of K^n into L^n. Let's look at operation preserving first. $\mathbf{A}_z(a\mathbf{u} + b\mathbf{v}) = a(\mathbf{A}_z\mathbf{u}) + b(\mathbf{A}_z\mathbf{v})$, where a and b are elements of K, $\mathbf{u}$ and $\mathbf{v}$ are in K^n, thus φ is a modulus homomorphism. As a special case, φ is sum-preserving, and

$$
\begin{aligned}
(\mathbf{A}_z(\mathbf{u} * \mathbf{v}))_i &= \sum_{j=0}^{n-1} (z^{-i})^j (\mathbf{u} * \mathbf{v})_j = \\
&= \sum_{j=0}^{n-1} ((z^{-i})^j \sum_{k=0}^{n-1} u_k v_{(j-k) \bmod n}) = \\
&= \sum_{k=0}^{n-1} \sum_{j=0}^{n-1} ((z^{-i})^k u_k)((z^{-i})^{(j-k) \bmod n} v_{(j-k) \bmod n}) = \qquad (1.1) \\
&= \left(\sum_{k=0}^{n-1} \left(z^{-i}\right)^k u_k \right) \left(\sum_{j=0}^{n-1} \left(z^{-i}\right)^j v_j \right) = \\
&= (\mathbf{A}_z\mathbf{u})_i \, (\mathbf{A}_z\mathbf{v})_i = ((\mathbf{A}_z\mathbf{u}) \cdot (\mathbf{A}_z\mathbf{v}))_i
\end{aligned}
$$

thus, φ is also product preserving, so the mapping φ is indeed an algebra homomorphism.

Let m be the order of z. Bijection is required for isomorphism, so L cannot be larger than $K(z)$. If $m < n$, then we saw that the mapping is not surjective, and thus not an isomorphism. Let $m = n$ henceforth. Then there is an inverse of $\mathbf{A}_z$, and $\mathbf{A}_z\mathbf{u}_1 = \mathbf{A}_z\mathbf{u}_2$ is only possible if $\mathbf{u}_1 = \mathbf{u}_2$, i.e. the mapping must be injective. If in $\mathbf{U} \in K^{(n)^n}, U_l = \delta_{i,(l+1) \bmod n}(ne)$, then $\left(\mathbf{A}_z^{-1}\mathbf{U}\right)_i = z^i$, and if the mapping is surjective, then the former $\mathbf{U}$ is also an element of the image set, which is only possible if $z \in K$. This shows that isomorphism requires the condition $L \subseteq K(z) \subseteq K$. Finally, let $\mathbf{w}$ be an element of the space over $\mathcal{K}$. Then $\mathbf{A}_z^{-1}\mathbf{w} = (ne)^{-1} \mathbf{A}_{z^{-1}}\mathbf{w}$ is also included in K^n, and thus $\mathbf{w} = \mathbf{A}_z\left(\mathbf{A}_z^{-1}\mathbf{w}\right)$, the assignment is also surjective, and then φ is bijective, and with operation preserving it is an isomorphism ■

Corollary 1.1. *If $z \in K$ is a primitive n-th root of unity, then* $\mathbf{A}_z^{-1}(\mathbf{U} \cdot \mathbf{V}) = \left(\mathbf{A}_z^{-1}\mathbf{U}\right) * \left(\mathbf{A}_z^{-1}\mathbf{V}\right)$

Proof. If z is a primitive n-th root of unity, then there exists $\mathbf{A}_z^{-1}$, and the mapping given in the theorem is bijective and operation preserving, so the uniquely determined preimage of the product of the image elements is the convolution of the similarly uniquely determined preimages. ■

If $\mathbf{u}$ is considered as a serial of coefficients of a polynomial $u = \sum_{i=0}^{n-1} u_i x^i$, then the theorem states that U_i is the substitution value of the polynomial at the point of z^{-i} of the field $\mathcal{K}$, while the corollary gives the uniquely determined polynomial of degree at most $n-1$ whose value in z^{-i} is U_i. The result is essentially the same as for complex numbers.

1.2. Automorphism of a field

A. Let $\mathcal{L}$ be an arbitrary field and σ be an arbitrary automorphism of $\mathcal{L}$. Then there is always a subfield of $\mathcal{L}$ on which σ is the identitic mapping. An example of such a subfield is the prime field of the field, that is a prime field: a prime field has no automorphism other than the identitic mapping to itself. If $\mathcal{L}$ is an extension of $\mathcal{K}$, and $\mathcal{K}$ is invariant with respect to σ, then σ is a relative automorphism of $\mathcal{L}$ for $\mathcal{K}$.

B. **Definition 1.1.** If $\mathcal{L}$ is an extension of the field $\mathcal{K}$, then the relative automorphism of $\mathcal{L}$ over $\mathcal{K}$ is an automorphism of $\mathcal{L}$ that leaves the elements of K in place.

It is easy to check that the relative automorphisms of the field $\mathcal{L}$ for the subfield of $\mathcal{K}$ form a group.

On a q^m-element field the mapping $u \mapsto u^{q^n}$ into itself is an automorphism, that is a relative automorphism, for example, with respect to the subfield $\mathbb{F}_q$. As a special case, in any extension $\mathcal{L}$ of a q-element field $\mathcal{K}$ for any $k \in \mathbb{N}$ the mapping $a \mapsto a^{q^k}$ is its relative automorphism over $\mathcal{K}$, and for finite $\mathcal{L}$ there is no other possibility, as shown in the theorem below.

Theorem 1.2. *Let the finite field $\mathcal{L}$ be an extension of degree t of the q-element field $\mathcal{K}$, and let $\sigma : a \mapsto a^q$ for the elements of L. Then the relative automorphisms of $\mathcal{L}$ over $\mathcal{K}$ form a t-order cyclic group with the generator element σ.*

2. New results

Notation. Let $n \in \mathbb{N}^+$, $k \in \mathbb{N}$ and $\mathbf{u} \in K^n$. Then $\mathbf{u}^{(k)} \in K^n$ denotes the vector whose $n > i \in \mathbb{N}$-index component $u_i^{(k)} = \left(\mathbf{u}^{(k)}\right)_i = u_{(ki) \bmod n}$.

The correspondence $\mathbf{u} \mapsto \mathbf{u}^{(k)}$ applied to the elements of K^n is sum-preserving and product-preserving if the multiplication is done component by component, and its scalar product image is the scalar product of the image, so the former mapping is an endomorphism of the ring $(K^n; +, \cdot)$. If k and n are relative primes, then $k \mapsto ki \bmod n$ is a permutation of the set of nonnegative integers less than n, and thus in this case $\mathbf{u} \mapsto \mathbf{u}^{(k)}$ is an automorphism of the former ring.

In the case of complex numbers, it seems natural to carry out the discrete Fourier transformation with the one belonging to the angle $2\pi/n$ among the n distinct n-th roots of unity, but in the case of an abstract field there is no such, in some respects primary, n-th root of unity among the primitive n-th roots of unity, so it is an interesting and important question what happens if we perform the transformation with one n-th root of unity instead of another.

Theorem 2.1. *For any integer k $\mathbf{A}_{z^k}\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(k)}$, and if z is a primitive n-th root of unity, then for any n-th root of unity y there exists a $k \in \mathbb{N}$ such that $\mathbf{A}_y\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(k)}$.*

Proof. Applying the definition of the transform

$$
\begin{aligned}
(\mathbf{A}_{z^k}\mathbf{u})_i &= \sum_{j=0}^{n-1} ((z^k)^{-i})^j u_j = \sum_{j=0}^{n-1} (z^{(-ki)})^j u_j = \\
&= \sum_{j=0}^{n-1} (z^{(-ki) \bmod n})^j u_j = \\
&= (\mathbf{A}_z\mathbf{u})_{ki \bmod n} = ((\mathbf{A}_z\mathbf{u})^{(k)})_i
\end{aligned} \tag{2.1}
$$

If the order of z is n then every n-th root of unity is a power of z with an exponent of a nonnegative integer less than n, so with some integer k $y = z^k$, and the second statement follows from the above. ■

Theorem 2.2. *Let $n \in \mathbb{N}^+$ and $\mathcal{L}$ be a field such that the n-th cyclotomic field over $\mathcal{L}$ is contained in $\mathcal{L}$, let σ be an automorphism of $\mathcal{L}$, and let $\mathcal{K}$ be the largest subfield of $\mathcal{L}$, on which σ is the identical mapping. Let $\underline{\sigma}$ denote the componentwise extension of σ onto $\mathcal{L}^n$, and let z be a primitive n-th root of unity. Then there is an $n > k \in \mathbb{N}$ coprime to n such that*

1. *for $\mathbf{u} \in L^n$ $\underline{\sigma}(\mathbf{A}_z\mathbf{u}) = \mathbf{A}_{z^k}\underline{\sigma}(\mathbf{u})$*

2. $\mathbf{u} \in K^{(n)}$ *if and only if* $\underline{\sigma}(\mathbf{U}) = \mathbf{U}^{(k)}$

3. *for* $\mathbf{u} \in K^n$, $\mathbf{U}$ *is in* K^n *if and only if* $\mathbf{u} = \mathbf{u}^{(k')}$ *where* $kk' \equiv 1\,(n)$ *with* k *mentioned above, and then* $\mathbf{U} = \mathbf{U}^{(k)}$

Proof.

1. In the case of an automorphism, the image of an n-th root of unity is an n-th root of unity and the image of a primitive n-th root of unity is a primitive n-th root of unity, so there is an $n > k \in \mathbb{N}$ so that $\sigma(z) = z^k$ and $(k, n) = 1$. Then

$$
\begin{aligned}
(\underline{\sigma}(\mathbf{A}_z\mathbf{u}))_i &= \sigma((\mathbf{A}_z\mathbf{u})_i) = \\
&= \sigma(\sum_{j=0}^{n-1}(z^{-i})^j u_j) = \sum_{j=0}^{n-1}(\sigma(z)^{-i})^j\sigma(u_j) = \\
&= \sum_{j=0}^{n-1}((z^k)^{-i})^j\sigma(u_j) = (\mathbf{A}_{z^k}\underline{\sigma}(\mathbf{u}))_i
\end{aligned} \tag{2.2}
$$

and from the previous theorem we get the first statement.

2. $\mathbf{u} \in K^n$ is fulfilled if and only if $\underline{\sigma}(\mathbf{u}) = \mathbf{u}$. Now on the one hand $\mathbf{U}^{(k)} = (\mathbf{A}_z\mathbf{u})^{(k)} = \mathbf{A}_{z^k}\mathbf{u}$, on the other hand $\underline{\sigma}(\mathbf{U}) = \underline{\sigma}(\mathbf{A}_z\mathbf{u}) = \mathbf{A}_{z^k}\underline{\sigma}(\mathbf{u})$, hence $\mathbf{U}^{(k)} = \sigma(\mathbf{U})$ will be exactly when $\mathbf{A}_{z^k}\mathbf{u} = \mathbf{A}_{z^k}\underline{\sigma}(\mathbf{u})$. z^k is a primitive n-th root of unity, so $\mathbf{A}_{z^k}$ is invertible, and then the above equality is true exactly if $\mathbf{u} = \underline{\sigma}(\mathbf{u})$, i.e. $\mathbf{u} \in K^n$ and $\underline{\sigma}(\mathbf{U}) = \mathbf{U}^{(k)}$ equivalent conditions.

3. $\mathbf{U} \in K^n$ is fulfilled if and only if $\underline{\sigma}(\mathbf{U}) = \mathbf{U}$ so with a $\mathbf{u}$ contained in K^n exactly then if $\mathbf{A}_z\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(k)} = \mathbf{A}_z\mathbf{u}^{k'}$ that is if $\mathbf{u} = \mathbf{u}^{(k')}$ and then $\mathbf{U} = \mathbf{A}_z\mathbf{u} = (\mathbf{A}_z\mathbf{u})^{(k)} = \mathbf{U}^{(k)}$. ■

First, let $\mathcal{L} = \mathbb{C}$ that is $\mathcal{L}$ is the field of the complex numbers and $\sigma : a \mapsto \overline{a}$ the complex conjugation ($\overline{u}$, as usual, denotes the conjugate of u). Then $\mathcal{K} = \mathbb{R}$, so now $\mathcal{K}$ is the field of the real numbers, and for the condition that $\mathbf{u} \in \mathbb{R}^n$ is necessary and sufficiant the eqality $\underline{\sigma}(\mathbf{U}) = \mathbf{U}^{(-1)}$. Indeed, $z \mapsto \overline{z}$ is bijective and operation-preserving on $\mathbb{C}$, so, the complex conjugation is an automorphism of $\mathbb{C}$, and $\mathbb{R}$ is the largest subfield of $\mathbb{C}$, in which conjugation is the identical mapping. z is now a complex n-th root of unity, so $\overline{z} = z^{-1} = z^{n-1}$, that is $k = n - 1$, and $(\mathbf{A}_z\mathbf{u})^{(n-1)} = (\mathbf{A}_z\mathbf{u})^{(-1)}$.

As a second case, let $\mathcal{L}$ be $\mathbb{F}_{q^m}$. where m is a positive integer, let $\sigma : a \mapsto a^{q^l}$, $l \in \mathbb{N}^+$ and let $d = (m, l)$. Let $\tilde{q}$, $\tilde{m}$ and $\tilde{l}$ be q^d, $\frac{m}{d}$ and $\frac{l}{d}$ respectively. Then $\mathcal{L} = \mathbb{F}_{\tilde{q}^{\tilde{m}}}$, $\sigma : a \mapsto a^{\tilde{q}^{\tilde{l}}}$ and $(\tilde{m}, \tilde{l}) = \tilde{d} = 1$, thus, in the following, we assume that m and l are relatively primes.

Then $\mathcal{K} = \mathbb{F}_q$, and $\mathbf{u} \in K^n$ is satisfied if and only if $\underline{\sigma}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z\mathbf{u})^{(q^l)} = \mathbf{U}^{(q^l)}$. This is true because on any extension of a q-element field, $a \mapsto a^{q^l}$ is automorphizm, and this takes z to z^{q^l}, and this mapping moves into themselves exactly the elements of K on the set of the elements of L (because for $0 \neq u \in L$ $u^{q^m-1} = e$, $u = u^{q^l}$ is true exactly if $u^{q^l-1} = e$, and the two equalities together are satisfied if and only if $e = u^{(q^m-1,q^l-1)} = u^{q^{(m,l)}-1} = u^{q-1}$, i.e. if $u^q = u$), that is, $\mathcal{K}$ is the maximal subfield in $\mathcal{L}$ on which the constraint of the transform is the identical mapping.

3. Special cases

In this section, we take a closer look at the meaning of the special cases mentioned above.

3.1. DFT over the field of complex numbers

If $\mathbf{u}$ is a real vector, then $\overline{(\mathbf{A}_z\mathbf{u})_k} = (\mathbf{A}_z\mathbf{u})_{(-k) \bmod n}$. It follows that $(\mathbf{A}_z\mathbf{u})_0$ is real, and for any integer i greater than 0 but less than n, $\overline{(\mathbf{A}_z\mathbf{u})_i} = (\mathbf{A}_z\mathbf{u})_{n-i}$ (so if n is even, say $n = 2m$, then the m-th component is also real), and this means that only $\lceil (n+1)/2 \rceil$ components can be independent (or even fewer). This is also true backwards, i.e. if the conjugate of the transform $\mathbf{U}$ of the complex vector $\mathbf{u}$ is identical to $\mathbf{U}^{(-1)}$, then $\mathbf{u}$ is real. If $k = -1$, then k' is -1, too, i.e. $\mathbf{u} = \mathbf{u}^{(k')}$ now, as before $\mathbf{U}$, means $u_i = u_{(n-i) \bmod n}$. For real $\mathbf{u}$, if this is true, and only then, all components of $\mathbf{U}$ are real, and for each component of the vector, $U_i = U_{(n-i) \bmod n}$.

3.2. DFT over finite fields

The case for a finite field says that if the components of the vector are from the q-element field, then the component belonging to the index of $q^l i$ mod n of the transformed vector is the q^l-th power of the component of the original vector belonging to the index of i. Let r_i be the smallest positive integer such that $i(q^l)^{r_i} \equiv i \pmod{n}$. q and n are coprimes, because the characteristic of the field does not divides n, so there is such an r_i exponent, namely $r_i = o_{o_n^+(i)}\left(q^l\right) = \frac{o_{o_n^+(i)}(q)}{\left(o_{o_n^+(i)}(q), l\right)} = o^+_{o_n^+(i)}(q)\,(l)$, and if $l = 1$, then, more simply, $r_i = o_{o_n^+(i)}(q)$ ($o_m(a)$ denotes the (multiplicative) order of a by modulo m and $o_m^+(a)$ denotes the additive order of a by modulo m). Now for $r_i > t \in \mathbb{N}$ U_i determines the components of $\mathbf{U}$ belonging to the indices of

$\left(\left(q^l\right)^t i\right) \bmod n = \left(q^{lt} i\right) \bmod n$. Then

$$
\begin{aligned}
U_{((q^l)^{r_i} i) \bmod n} &= U_i^{\left(q^l\right)^{r_i}} = \left(\sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j\right)^{\left(q^l\right)^{r_i}} = \\
&= \sum_{j=0}^{n-1} \left(\left(z^{-i}\right)^j\right)^{\left(q^l\right)^{r_i}} u_j = \sum_{j=0}^{n-1} \left(z^{-i\left(q^l\right)^{r_i}}\right)^j u_j = \\
&= \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = U_i,
\end{aligned} \tag{3.1}
$$

as it should be, since $\left(q^l\right)^{r_i} i \bmod n = i$. $U_i^{\left(q^l\right)^{r_i}} = U_i$ means that U_i is an element of the $\left(q^l\right)^{r_i}$-element field, and as it is an element of the field of q^m elements, so it is an element of the intersection of that two fields, too. The size of that field is q^s, where $s = (m, lr_i) = (m, r_i)$ (as $(m, l) = 1$).

Conversely, if in $\mathbf{U}$ for every $n > i \in \mathbb{N}$ it is fulfilled, that the component belonging to the index of $\left(q^l i\right) \bmod n$ is equal to the q^l-th power of U_i, then $\mathbf{u}$ is the vector belonging to the n-th direct sum of the q-element field $\mathcal{K}$.

Finally, let $\mathbf{u}$ be again a vector over $\mathbb{F}_q$. Now $\mathbf{U}$ is in $\mathbb{F}_q^n$ if and only if $u_i = u_{q^{l'} i \bmod n}$, where l' is the opposite of l modulo $o_n(q)$, that is $l' = (-l) \bmod o_n(q)$, and in that case $U_i = U_{q^l i \bmod n}$.

4. Example

Let's see an example. Let $q = 3$, $m = 3$, $l = 2$ and $n = 13$. Then $q^m = 27$ and $(m, l) = (3, 2) = 1$, that is, $\mathcal{K} = \mathbb{F}_3$ and $\mathcal{L} = \mathbb{F}_{27}$. $n = 13 \,|\, 26 = 27 - 1$, so it also holds that $L^{(n)} \subseteq L$ where $\mathcal{L}^{(n)}$ denotes the n-th cyclotomic field over $\mathcal{L}$. Now $q^l = 3^2 = 9$, i.e. $\sigma(v) = v^9$ for the elements of L, and if $v \in K$, then $\sigma(v) = v^9 = v$. Let's look at $\left(q^l i\right) \bmod n = (9i) \bmod 13$ for $13 > i \in \mathbb{N}$:

i	0	1	2	3	4	5	6	7	8	9	10	11	12
$(9i) \bmod 13$	0	9	5	1	10	6	2	11	7	3	12	8	4

Based on the table, there are five disjoint cycles:

$$
\begin{array}{lllllllll}
0 & \to & 0 & & & & & & \\
1 & \to & 9 & \to & 3 & \to & 1 & & \\
2 & \to & 5 & \to & 6 & \to & 2 & & \\
4 & \to & 10 & \to & 12 & \to & 4 & & \\
7 & \to & 11 & \to & 8 & \to & 7 & &
\end{array}
$$

and accordingly we get – omitting the one-element class – the components of the transformed vector:

$$\begin{array}{lllllllllllll}
U_1 & \to & U_9 = U_1^9 & \to & U_3 = U_9^9 = U_1^{81} = U_1^3 & \to & U_1 = U_3^9 = U_1^{27} = U_1 \\
U_2 & \to & U_5 = U_2^9 & \to & U_6 = U_5^9 = U_2^{81} = U_2^3 & \to & U_2 = U_6^9 = U_2^{27} = U_2 \\
U_4 & \to & U_{10} = U_4^9 & \to & U_{12} = U_{10}^9 = U_4^{81} = U_4^3 & \to & U_4 = U_{12}^9 = U_4^{27} = U_4 \\
U_7 & \to & U_{11} = U_7^9 & \to & U_8 = U_{11}^9 = U_7^{81} = U_7^3 & \to & U_7 = U_8^9 = U_7^{27} = U_7
\end{array}$$

The table shows that $r_i = 3$ for all i except 0. Indeed: $o_n^+(i) = o_{13}^+(i) = \frac{13}{(13,i)} = 13$ for every i, since 13 is a prime number. In this case, the value of r_i is the same for each i, it is sufficient to define for $i = 1$. $o_{13}(9)$ is a divisor of $\varphi(13) = 12$, so the order can only be 1, 2, 3, 4, 6, and 12. 1 is only the order of 1. $9^2 = 81 \equiv 3 \pmod{13}$, and 3 is not congruent to 1 modulo 13, so even 2 is not the desired order, but $9^3 \equiv 9 \cdot 3 = 27 \equiv 1 \pmod{13}$, so we got $r_1 = 3$, and then $r_i = 3$ for every other positive integer i less than 13. This also means that, with the exception of U_0, each element of the transformed vector can be any element of the 27-element field (while U_0 necessarily belongs to K). The fact that every cycle (except for the one containing 0) has the same length, and every element of the transformed vector can be any element of the entire field, is not generally true, it is just a feature of this example.

Now $l' = (-l) \mod o_n(q) = (-2) \mod 3 = 1$, so if $u_{(3i) \bmod 13} = u_i \in \mathbb{F}_3$ for $13 > i \in \mathbb{N}$, then $U_{(9i) \bmod 13} = U_i^9 = U_i \in \mathbb{F}_3$.

References

[1] **Cooley, J., P. Lewis and P. Welch,** The finite Fourier transform, *IEEE Transactions on Audio and Electroacoustics*, **17(2)** 1969, 77–85.

[2] **Hui, S. and S.H. Żak,** Discrete Fourier transform and permutations, *Bull. Polish Acad. Sci. Tech. Sci.*, **67(6)** (2019), 995–1005.

[3] **Kekre, H.B., M.D. Wagh and Sh.V. Kanetkar, Sh. V.,** On group theoretic transforms and the automorphism groups, *Inform. and Control*, **41(2)**(1979), 147-–155.

[4] **Lidl, R. and H. Niederreiter,** *Finite Fields*, Addison-Wesley Publishing Inc., Reading, Mass., 1983.

[5] **Lidl, R. and G. Pilz,** *Applied Abstract Algebra*, Springer Verlag, New York, 1998.

J. Gonda
Department of Computer Algebra
Eötvös Loránd Universitiy
H-1117 Budapest, Pázmány Péter sétány 1/C
Hungary
andog@inf.elte.hu