WIKIPEDIA

Discrete Fourier transform (general)

In mathematics, the **discrete Fourier transform** over an arbitrary ring generalizes the discrete Fourier transform of a function whose values are complex numbers.

Contents

Definition

Inverse

Matrix formulation

Polynomial formulation[2]

Special cases

- Complex numbers
- Finite fields
- Number-theoretic transform
- Discrete weighted transform

Properties

Fast algorithms

See also

References

External links

Definition

Let R be any ring, let $n \geq 1$ be an integer, and let $\alpha \in R$ be a principal *n*th root of unity, defined by:[1]

$$\alpha^n = 1$$
$$\sum_{j=0}^{n-1} \alpha^{jk} = 0 \text{ for } 1 \leq k < n \qquad (1)$$

The discrete Fourier transform maps an *n*-tuple $(v_0, \ldots, v_{n-1})$ of elements of R to another *n*-tuple $(f_0, \ldots, f_{n-1})$ of elements of R according to the following formula:

$$f_k = \sum_{j=0}^{n-1} v_j \alpha^{jk}. \qquad (2)$$

By convention, the tuple $(v_0, \ldots, v_{n-1})$ is said to be in the *time domain* and the index j is called *time*. The tuple $(f_0, \ldots, f_{n-1})$ is said to be in the *frequency domain* and the index k is called *frequency*. The tuple $(f_0, \ldots, f_{n-1})$ is also called the *spectrum* of $(v_0, \ldots, v_{n-1})$. This terminology derives from the applications of Fourier transforms in signal processing.

If R is an integral domain (which includes fields), it is sufficient to choose α as a primitive *n*th root of unity, which replaces the condition (1) by:[1]

$$\alpha^k \neq 1 \text{ for } 1 \leq k < n$$

Proof: take $\beta = \alpha^k$ with $1 \leq k < n$. Since $\alpha^n = 1$, $\beta^n = (\alpha^n)^k = 1$, giving:

$$\beta^n - 1 = (\beta - 1)\left(\sum_{j=0}^{n-1} \beta^j\right) = 0$$

where the sum matches (1). Since α is a primitive root of unity, $\beta - 1 \neq 0$. Since R is an integral domain, the sum must be zero. ∎

Another simple condition applies in the case where *n* is a power of two: (1) may be replaced by $\alpha^{n/2} = -1$.[1]

Inverse

The inverse of the discrete Fourier transform is given as:

$$v_j = \frac{1}{n}\sum_{k=0}^{n-1} f_k \alpha^{-jk}. \qquad (3)$$

where $1/n$ is the multiplicative inverse of n in R (if this inverse does not exist, the DFT cannot be inverted).

Proof: Substituting (2) into the right-hand-side of (3), we get

$$\begin{aligned}
&\frac{1}{n}\sum_{k=0}^{n-1} f_k \alpha^{-jk} \\
&= \frac{1}{n}\sum_{k=0}^{n-1}\sum_{j'=0}^{n-1} v_{j'} \alpha^{j'k} \alpha^{-jk} \\
&= \frac{1}{n}\sum_{j'=0}^{n-1} v_{j'} \sum_{k=0}^{n-1} \alpha^{(j'-j)k}.
\end{aligned}$$

This is exactly equal to v_j, because $\sum_{k=0}^{n-1} \alpha^{(j'-j)k} = 0$ when $j' \neq j$ (by (1) with $k = j' - j$), and $\sum_{k=0}^{n-1} \alpha^{(j'-j)k} = n$ when $j' = j$. ∎

Matrix formulation

Since the discrete Fourier transform is a linear operator, it can be described by matrix multiplication. In matrix notation, the discrete Fourier transform is expressed as follows:

$$\begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{bmatrix}.$$

The matrix for this transformation is called the DFT matrix.

Similarly, the matrix notation for the inverse Fourier transform is

$$\begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{bmatrix} = \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(n-1)} & \alpha^{-2(n-1)} & \cdots & \alpha^{-(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{bmatrix}.$$

Polynomial formulation[2]

Sometimes it is convenient to identify an n-tuple $(v_0, \ldots, v_{n-1})$ with a formal polynomial

$$p_v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1}.$$

By writing out the summation in the definition of the discrete Fourier transform (2), we obtain:

$$f_k = v_0 + v_1 \alpha^k + v_2 \alpha^{2k} + \cdots + v_{n-1} \alpha^{(n-1)k}.$$

This means that f_k is just the value of the polynomial $p_v(x)$ for $x = \alpha^k$, i.e.,

$$f_k = p_v(\alpha^k).$$

The Fourier transform can therefore be seen to relate the *coefficients* and the *values* of a polynomial: the coefficients are in the time-domain, and the values are in the frequency domain. Here, of course, it is important that the polynomial is evaluated at the nth roots of unity, which are exactly the powers of α.

Similarly, the definition of the inverse Fourier transform (3) can be written:

$$v_j = \frac{1}{n}(f_0 + f_1 \alpha^{-j} + f_2 \alpha^{-2j} + \cdots + f_{n-1} \alpha^{-(n-1)j}). \qquad (5)$$

With

$$p_f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{n-1} x^{n-1},$$

this means that

$$v_j = \frac{1}{n} p_f(\alpha^{-j}).$$

We can summarize this as follows: if the *values* of $p(x)$ are the *coefficients* of $q(x)$, then the *values* of $q(x)$ are the *coefficients* of $p(x)$, up to a scalar factor and reordering.

Special cases

Complex numbers

If $F = \mathbb{C}$ is the field of complex numbers, then the nth roots of unity can be visualized as points on the unit circle of the complex plane. In this case, one usually takes

$$\alpha = e^{\frac{-2\pi i}{n}},$$

which yields the usual formula for the complex discrete Fourier transform:

$$f_k = \sum_{j=0}^{n-1} v_j e^{\frac{-2\pi i}{n} jk}.$$

Over the complex numbers, it is often customary to normalize the formulas for the DFT and inverse DFT by using the scalar factor $\frac{1}{\sqrt{n}}$ in both formulas, rather than 1 in the formula for the DFT and $\frac{1}{n}$ in the formula for the inverse DFT. With this normalization, the DFT matrix is then unitary. Note that $\sqrt{n}$ does not make sense in an arbitrary field.

Finite fields

If $F = GF(q)$ is a finite field, where q is a prime power, then the existence of a primitive nth root automatically implies that n divides $q-1$, because the multiplicative order of each element must divide the size of the multiplicative group of F, which is $q-1$. This in particular ensures that $n = \underbrace{1+1+\cdots+1}_{n \text{ times}}$ is invertible, so that the notation $\frac{1}{n}$ in (3) makes sense.

An application of the discrete Fourier transform over $GF(q)$ is the reduction of Reed–Solomon codes to BCH codes in coding theory. Such transform can be carried out efficiently with proper fast algorithms, for example, cyclotomic fast Fourier transform.

Number-theoretic transform

The **number-theoretic transform (NTT)** is obtained by specializing the discrete Fourier transform to $F = \mathbb{Z}/p$, the integers modulo a prime p. This is a finite field, and primitive nth roots of unity exist whenever n divides $p-1$, so we have $p = \xi n + 1$ for a positive integer ξ. Specifically, let ω be a primitive $(p-1)$th root of unity, then an nth root of unity α can be found by letting $\alpha = \omega^{\xi}$.

e.g. for $p = 5$, $\alpha = 2$

$$
\begin{aligned}
2^1 &= 2 \pmod 5 \\
2^2 &= 4 \pmod 5 \\
2^3 &= 3 \pmod 5 \\
2^4 &= 1 \pmod 5
\end{aligned}
$$

when $N = 4$

$$
\begin{bmatrix} F(0) \\ F(1) \\ F(2) \\ F(3) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} f(0) \\ f(1) \\ f(2) \\ f(3) \end{bmatrix}
$$

The number theoretic transform may be meaningful in the ring $\mathbb{Z}/m$, even when the modulus m is not prime, provided a principal root of order n exists. Special cases of the number theoretic transform such as the Fermat Number Transform ($m = 2^k+1$), used by the Schönhage–Strassen algorithm, or Mersenne Number Transform ($m = 2^k - 1$) use a composite modulus.

Discrete weighted transform

The **discrete weighted transform (DWT)** is a variation on the discrete Fourier transform over arbitrary rings involving weighting the input before transforming it by multiplying elementwise by a weight vector, then weighting the result by another vector.[3] The Irrational base discrete weighted transform is a special case of this.

Properties

Most of the important attributes of the complex DFT, including the inverse transform, the convolution theorem, and most fast Fourier transform (FFT) algorithms, depend only on the property that the kernel of the transform is a principal root of unity. These properties also hold, with identical proofs, over arbitrary rings. In the case of fields, this analogy can be formalized by the field with one element, considering any field with a primitive *n*th root of unity as an algebra over the extension field $\mathbf{F}_{1^n}$.

In particular, the applicability of $O(n \log n)$ fast Fourier transform algorithms to compute the NTT, combined with the convolution theorem, mean that the number-theoretic transform gives an efficient way to compute exact convolutions of integer sequences. While the complex DFT can perform the same task, it is susceptible to round-off error in finite-precision floating point arithmetic; the NTT has no round-off because it deals purely with fixed-size integers that can be exactly represented.

Fast algorithms

For the implementation of a "fast" algorithm (similar to how FFT computes the DFT), it is often desirable that the transform length is also highly composite, e.g., a power of two. However, there are specialized fast Fourier transform algorithms for finite fields, such as Wang and Zhu's algorithm,[4] that are efficient regardless of whether the transform length factors.

See also