Proc. Nat. Acad. Sci. USA
Vol. 73, No. 4, pp. 1005–1006, April 1976
Mathematics

On computing the Discrete Fourier Transform

(algorithm/computational complexity)

SHMUEL WINOGRAD

IBM Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598

Communicated by R. E. Gomory, December 29, 1975

ABSTRACT **New algorithms for computing the Discrete Fourier Transform of n points are described. For n in the range of a few tens to a few thousands these algorithms use substantially fewer multiplications than the best algorithm previously known, and about the same number of additions.**

Computing the Discrete Fourier Transform (DFT) of n points:

$$A_j = \sum_{i=0}^{n-1} w^{ij}a_i, \quad j = 0,\ldots,n-1, \quad w = e^{\frac{2\pi i}{n}} \qquad [1]$$

has many applications in scientific and engineering calculation. In 1965 Cooley and Tukey (1) described an algorithm for computing DFT in $n/2 \log_2 n/2$ complex multiplications and $n \log_2 n$ complex additions, when $n = 2^s$ is a power of 2. In this note we will describe a new algorithm for computing the DFT. For n in the range of a few tens to a few thousands this algorithm uses substantially fewer multiplications than that described by Cooley and Tukey, and about the same number of additions as theirs.

Theoretical background

In ref. 2 we considered the following problem: Let $P_n = u^n + \sum_{i=0}^{n-1} a_i u^i$ be a polynomial with coefficients in a field G, let $R_n = \sum_{i=0}^{n-1} x_i u^i$ and $S_n = \sum_{i=0}^{n-1} y_i u^i$ be two polynomials with indeterminate coefficients. What is the minimum number of multiplications needed to compute the coefficients of $T_p = R_n \cdot S_n \bmod P_n$ when multiplications by an element $g \in G$ are not counted? Let $\bar{T}_P$ denote the set of coefficients. It was proved that:

THEOREM. If $P_n = \Pi_{i=1}^{k} Q_i^{1_i}$ where Q_i is irreducible (over G) and $(Q_i, Q_j) = 1$ for $i \neq j$, then the minimum number of multiplications needed to compute $\bar{T}_P$ is $2n - k$.

Let p be a prime and consider computing the DFT of p elements. The difficult part of the computation is that of computing $\bar{A}_k = \sum_{j=1}^{p-1} w^{kj}a_j$, $k = 1,2,\ldots, p-1$, $w = \exp(2\pi i)/p$. The exponent of w is $k \cdot j \bmod p$, and since the group of non-zero integers with operation of multiplication modulo p is isomorphic to Z_{p-1} it follows that there exists a permutation Π of $\{1,2,\ldots,p-1\}$ such that the matrix whose (i,j) element is $w^{\pi(i)\cdot\pi(j)}$ is cyclic. Therefore computing $\bar{A}_{\pi(j)} = \sum_{i=1}^{p-1} w^{\pi(i)\pi(j)} a_{\pi(j)}$ $j = 1,2,\ldots,p-1$ is the same as computing the coefficients of

$$\left(\sum_{i=1}^{p-1} w^{\pi(i)}u^{i-1}\right)\left(a_{\pi(1)} + \sum_{i=2}^{p-1} a_{\pi(p-1-i)}u^{i-1}\right) \bmod u^{p-1} - 1. \qquad [2]$$

According to the theorem this can be done in $2(p-1)-k$ multiplications, where k is the number of irreducible factors (over the rationals) of $u^{p-1}-1$.

Similar results are obtained when $n = p^r$ is a power of a prime. In this case we use the result that the group of integers relatively prime to p with group operation of multiplication modulo p^r is $Z_{(p-1)p^{r-1}}$ for $p \neq 2$ and is $Z_2 \times Z_{2^{r-2}}$ for $p = 2$.

Summary of results

All known algorithms for computing $\bar{T}_P$ in the minimum number of multiplications require a large number of additions when P has large irreducible factors. Therefore the algorithms for DFT as outlined in the previous section are not of practical interest unless the number of points n is small. Table 1 summarizes the number of multiplications and additions used to compute DFT for small n. We will need later to consider multiplication by $w^0 = 1$ as a multiplication, and we therefore indicate these multiplications as well in the table.

For all these algorithms the factor which depends on w^{ij} is either real or pure imaginary. It is easy to verify that this property is general and will happen whenever the algorithm is derived as outlined in the end of the last section. Therefore each multiplication is either one multiplication of real numbers (in case the data points are real) or two real multiplications (in case the data points are complex).

To obtain algorithms for larger value of n, we consider those numbers which have more than one prime divisor. Let $n = n_1 \cdot n_2$ where $(n_1,n_2) = 1$. Using the Chinese Remainder Theorem, we represent every integer $i \in \{0,1,\ldots,n-1\}$ by a pair of integers (i_1,i_2) where $i_1 = i \bmod n_1$, $i_2 = i \bmod n_2$. Consequently:

$$w^{ij} = w^{(i_1,i_2)(j_1,j_2)} = w^{(i_1\cdot j_1,\, i_2\cdot j_2)} = w^{(i_1\cdot j_1,\,0)} \cdot w^{(0,\,i_2\cdot j_2)} \qquad [3]$$

This means that the computation of DFT of $n = n_1 \cdot n_2$ points can be decomposed into computing the DFT for n_1 points in which each multiplication is replaced by computing the DFT of n_2 points. For example, computing the DFT of $21 = 3.7$ complex data points we use the DFT of 3 points and substitute for each addition the addition of 7 dimension-

Table 1. DFT for small n

n	No. multiplications	No. multiplications by w^0	No. additions
2	0	2	2
3	2	1	6
4	0	4	8
5	5	1	17
7	8	1	36
8	2	6	26
9	12	1	44
16	10	8	74

Abbreviation: DFT, Discrete Fourier Transform.

Table 2. Examples of complexity of the new algorithm

n	No. multiplications real data	No. additions real data	No. multiplications complex data	No. additions complex data	$2n \log_2 n$	$3n \log_2 n$
30	36	198	72	384	295	442
48	54	336	108	636	537	805
60	72	486	144	888	709	1,064
120	144	1,242	288	2,076	1,658	2,487
168	216	2,022	432	3,492	2,484	3,726
240	324	3,042	648	5,016	3,796	5,693
420	648	6,654	1,296	11,352	7,320	10,980
504	936	8,946	1,872	14,796	9,050	13,574
840	1,296	15,198	2,592	24,804	16,320	24,480
1,008	2,106	21,546	4,212	35,244	20,115	30,172
2,520	5,616	64,170	11,232	102,348	56,949	85,423

al vectors, and for each multiplication (including multiplication by w^0) the DFT of 7 points. Altogether the computation uses 6.7 + 3.36 = 150 additions of complex numbers, and 3.9 = 27 multiplications of a real number by a complex number.

Using the algorithms summarized in Table 1 we obtain algorithms for computing the DFT of n points for n in the range of a few tens to a few thousands. The number of real multiplications and real additions used by these algorithms, for several values of n in the range, are given in Table 2. Since the numbers are different for real and complex data we give both numbers. For the sake of comparing these algorithms with the Fast Fourier Transform of ref. 1, we also give $2n \log_2 n$ (the number of real multiplications for the Fast Fourier Transform if n is a power of 2) and $3n \log_2 n$ (the number of additions for the Fast Fourier Transform).

1. Cooley, J. W. & Tukey, J. W. (1965) "An algorithm for the machine calculation of complex Fourier series," *Math. of Comp.*, **19**, 297–301.
2. Winograd, S. (1975) "The effect of the field of constants on the number of multiplications," *Proceedings of the 16th Annual Symposium on Foundations of Computer Science, 1975*, pp. 1–2.