1. INTRODUCTION

The number-theoretic transform (NTT) was introduced as a generalization of the discrete Fourier transform (DFT) over residue class rings of integers in order to implement fast cyclic convolution and correlation without round-off errors and with better efficiency than the fast Fourier transform. Interesting applications of the NTT are in fast cyclic convolution and correlation without round-off errors and with better efficiency than the fast Fourier transform.

For standard signal processing applications the main drawback of the NTT is a rigid relationship between computer word length and transform length and a limited choice of possible word length. A large number of transform methods are developed to relieve some of the length limitations of Fermat number and Mersenne number transforms on conventional computers with binary arithmetics. In order to further enlarge the transform length of conventional NNTs, number-theoretic transforms over extension rings of the residue class ring of integers modulo \( m \) were introduced. These NTTs have a similar structure and properties like the DFT, particularly the cyclic convolution property.

However, it is not easy to find convenient modules \( m \) that are large enough to avoid overflow, and to find primitive \( N \)-th roots of unity modulo \( m \) with small binary weight for transform lengths \( N \) that are highly factorizable and large enough for practical applications.

The solution to this problem for arbitrary finite commutative rings with unity was found by studying cyclotomic polynomials. Simple constructive methods for the finding of all convenient modules \( m \) for complex NTTs under the assumption that a special transform length \( N \) and a special element \( \alpha \) with small binary weight are given. Using the concept of factorization of cyclotomic polynomials one can obtain valuable results for the determination of convenient parameters (transform length \( N \), module \( m \), primitive root of unity \( \alpha \) modulo \( m \)) for NTTs over various finite commutative rings.

2. NUMBER-THEORETIC TRANSFORMS – NTT

Let \( \mathbb{Z} \) be the ring of integers and \( m > 1 \) an odd integer with prime factorization

\[
m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.
\]

Then \( \alpha \in \mathbb{Z} \) is called primitive \( N \)-th root of unity modulo \( m \) if

\[
\alpha^N \equiv 1 \mod m,
\]

and

\[
\gcd(\alpha^n - 1, m) = 1 \text{ for every } n = 1, \ldots, N - 1.
\]

The NTT of length \( N \) with a primitive \( N \)-th root of unity modulo \( m \) and its inverse are defined between \( N \)-point integer sequences

\[
X_n \equiv \sum_{k=0}^{N-1} x_k \alpha^{nk} \mod m, \quad n = 0, \ldots, N - 1,
\]

\[
x_k \equiv N' \sum_{n=0}^{N-1} X_n \alpha^{-nk} \mod m, \quad k = 0, \ldots, N - 1,
\]

where \( N' \equiv 1 \mod m \).

The NTT has similar structure and properties like the DFT, particularly the cyclic convolution property.

From the numerical point of view the following three essential conditions on the NTTs are required:

- the transform length \( N \) has to be large enough and highly factorizable in order to implement fast algorithms like prime-factor-, Winograd-, single-radix-, mixed-radix algorithms,
- the primitive \( N \)-th root \( \alpha \) should have a simple binary representation (2, 4, 8, 16, for example), so that the binary arithmetic modulo \( m \) is easy to perform,
- the modulus \( m \) has to be large enough to avoid overflow but on the other hand small enough, so that the machine word length is not exceeded.

For instance, the Fermat number transform (FNT) which was studied extensively in various papers is a good compromise between these various conditions.
3. REFERENCES


[27] BAILEY, D.: Schnelle Algorithmen zur Spektraltransformation endlicher Gruppen. Diploma work, University of Karlsruhe, August 1988


[58] BLAHUT, R. E.: Transform techniques for error control codes. IBM J. Res. Develop. 23 (1979), pp. 299-315


[61] BLAHUT, R. E.: Theory and Practice of Error Control Codes. Addison Wesley: Reading (MA) 1984


[65] BONNEAU, R. J.: A class of finite computation structures supporting the fast Fourier transform. Project MAC, Memo 31 1973


[78] BURRUS, C. S.: Notes on the FFT. Report, Rice University, Houston, December 1987


STEIDL, G.: Modified discrete Fourier transforms and fast algorithms. Habilitation (in German), University of Rostock, Dept. Mathematics 1990


VARMA, D. - TRACHTENBERG, E. A.: Design automation tools for efficient implementation of logic
functions by decomposition. IEEE Trans. CAD \textbf{8} (1989), No. 8, pp. 901-916


