Hartley Number Theoretic Transforms

R. M. Campello de Souza, H. M. de Oliveira, L. B. Espinola Palma e M. M. Campello de Souza
Communications Research Group-UFPE, C.P.7800, 50711-970, Recife-PE, Brasil, Ricardo@npd.ufpe.br

Abstract - **In this paper, the Hartley Number Theoretic Transform (HNTT) is introduced. In particular, the Mersenne HNTT is defined and some multiplication free transforms are given.**

I. INTRODUCTION

A Discrete Fourier Transform over finite fields (FFFT) was introduced in [1] and applied as a tool to perform discrete convolutions using integer arithmetic. When the FFFT relates vectors with components in GF(p), the arithmetic performed is modulo p and the transforms are called Number Theoretic Transforms (NTT). Hartley transforms can also be defined over finite fields [2]. In this paper, a new Number Theoretic Transform, the Hartley Number Theoretic Transform (HNTT) is introduced.

II. HARTLEY NUMBER THEORETIC TRANSFORMS

Definition 1: Let $f = (f_0, f_1, \ldots, f_{N-1})$ be a vector of length N and components in GF(q), where $q = p^r$. The vector $F = (F_0, F_1, \ldots, F_{N-1})$, with components in $GF(q^m)$ given by $F_k = \sum_{i=0}^{N-1} f_i \alpha^{ki}$, where α is an element of order N in $GF(q^m)$, is the FFFT of f. When $r = m = 1$, the FFFT maps vectors with elements in GF(p) and is called a Fourier Number Theoretic Transform (FNTT). The FNTT has blocklength N (a divisor of p-1) and is attractive due to its low computational complexity and ease of implementation. In what follows, $GI(q^m)$ denotes the set of gaussian integers over $GF(q^m)$, i.e., the set of integers of the form a+jb where $a,b \in GF(q^m)$ and $j \in GF(q^{2m})$ is such that $j^2 = -1$. By analogy with the complex numbers, the elements of $GF(q^m)$ and of $GI(q^m)$ are said to be real and complex, respectively.

Definition 2: Let $v = (v_0, v_1, \ldots, v_{N-1})$ be a vector of length N with components in GF(q), where $q=p^r$, r an odd integer and $p \equiv 3 \pmod 4$. The vector $V = (V_0, V_1, \ldots, V_{N-1})$, with components in $GI(q^m)$ given by $V_k = \sum_{i=0}^{N-1} v_i \mathrm{cas}_k(\zeta^i)$, where ζ is an element of order N in $GI(q^m)$, is the Finite Field Hartley Transform (FFHT) of v. The FFHT kernel is the cas(.) (*cosine and sine*) function in a finite field, given by $\mathrm{cas}_k(\zeta^i) = \cos_k(\zeta^i) + \sin_k(\zeta^i)$, where $\cos_k(\zeta^i) = (\zeta^{ik} + \zeta^{-ik})/2$ and $\sin_k(\zeta^i) = (\zeta^{ik} - \zeta^{-ik})/2j$ are the sine and cosine functions defined in a finite field [2].

The Hartley NTTs are obtained from proposition 1 below.

Proposition 1: If $\zeta = a+jb$ is the argument of the cas(.) function used in definition 2 above, then the components $V_k \in GF(p)$ (i.e., they are real) if $a^2+b^2 \equiv 1 \pmod p$.

Proposition 1 shows that it is possible to construct an FFHT mapping vectors with components in GF(p) by imposing a constraint over the kernel $\mathrm{cas}_k(\zeta^i)$. Such a condition is not too restrictive once that, if $\zeta = a+jb$ satisfies proposition 1, then so does every element in the set $\Gamma = \{b+ja, (p-a)+jb, b+j(p-a), a+j(p-b), (p-b)+ja, (p-a)+j(p-b), (p-b)+j(p-a)\}$. We are now in a position to define a number theoretic transform of the Hartley type.

Definition 3: Let $v = (v_0, v_1, \ldots, v_{N-1})$ be a vector of length N with components in GF(p), $p \equiv 3 \pmod 4$. Then the Hartley Number Theoretic Transform of v is the vector $V = (V_0, V_1, \ldots, V_{N-1})$, with components in GF(p) given by $V_k = \sum_{i=0}^{N-1} v_i \mathrm{cas}_k(\zeta^i)$, where $\zeta = a+jb$ is an element of order N in GF(p) satisfying $a^2+b^2 \equiv 1 \pmod p$.

Theorem 1: The inverse HNTT of V is the vector v of components in GF(p) given by $v_i = \frac{1}{N \pmod p} \sum_{k=0}^{N-1} V_k \mathrm{cas}_k(\zeta^i)$.

III. HARTLEY-MERSENNE NTTs

When p is a Mersenne prime we get the Hartley-Mersenne NTTs (HMNTT). In this case $p = 2^s-1 \equiv 3 \pmod 4$ and the conditions of definition 2 are satisfied. The HMNTTs are of interest because the finite fields where the operation of multiplication is most straightforward are those of the form $GF(2^s-1)$. The blocklengths for an HMNTT are the divisors of $p+1=2^s$, i.e., powers of 2. Therefore, any HNTT in $GF(2^s-1)$ may be computed via the radix 2 Cooley-Tukey FFT algorithm. It is interesting to note that the Fourier-Mersenne NTTs cannot be computed in this way, since $(2^s-1)-1$ is not a power of 2. Multiplication free transforms are also possible with HNTTs. In this case the elements of the transform matrix assume only the values 0, 1 and -1, or nontrivial powers of ± 2, and the transform can be computed with only shifts.

Proposition 2: In $GF(2^s-1)$, multiplications free HMNTTs of blocklength N=8, can be constructed with $\zeta = a + jb = 2^{\frac{s-1}{2}} + j2^{\frac{s-1}{2}}$.

Multiplication free transforms can be constructed for other values of p, as shown in proposition 3 below.

Proposition 3: Let $p = 2^{2k}+3$, $k \geq 1$. Then $\zeta = 2^k + j2$ is a root of unity in GF(p).

V. CONCLUSIONS

In this paper the Hartley Number-Theoretic Transform was introduced. The HNTT is obtained from the Finite Field Hartley Transform, by a choice of its kernel $\mathrm{cas}_k(\zeta^i)$ that results in a transform with components in GF(p). That means that it is not necessary to restrict the extension field to GF(p) so as to obtain a number-theoretic transform, which means that N, the transform blocklength, is a divisor of (p-1)(p+1). Therefore, for a given p, a greater number of choices for the value of N are possible. In the particular case when p is a Mersenne prime, the corresponding transforms are called Hartley-Mersenne NTTs. The HMNTT has blocklengths that are a power of two, so they can be computed by a Cooley-Tukey type FFT, differently from what happens with the Fourier-Mersenne NTT. Implementations that require only additions and cyclic shifts are also possible.

ACKNOWLEDGEMENTS - The authors thank Mr. A.N. Kauffman from Nortelnetworks for valuable comments.

REFERENCES

[1] J. M. Pollard, *The Fast Fourier Transform in a Finite Field*, Math. Comp., vol. 25, No.114, pp. 365-374, Apr. 1971.

[2] R. M. Campello de Souza, H. M. de Oliveira and A. N. Kauffman, *Trigonometry in Finite Fields and a New Hartley Transform*, Proc. of the IEEE Int. Symp. on Info. Theory, p. 293, Cambridge, MA, Aug. 1998.

0-7803-7123-2/01/$10.00 ©2001 IEEE