Abstract.
Properties of the asymmetric two-sided Fermat Number Theoretic Transform are discussed. The Fermat transform matrix does not have a Kronecker structure, however the Fermat transform of Mosaics presents this structure. For mosaics with a 2 by 2 seed, the Walsh transform allows a fast calculation of the Fermat spectrum.

1 Introduction
Number Theoretic Transforms (NTTs) were developed in the early 70s as a computational efficient alternative to the Discrete Fourier Transform (DFT). This was motivated by the fact that in those years the computational world was based on “mainframes” running at low KHz rates and main memories of a few MB. NTTs work with integer arithmetic constrained by a modulo (see below), meanwhile the DFT works in the complex plane. Under special conditions, the kernel of an NTT may consist of powers of 2, meanwhile that of the DFT consists of powers of complex valued roots of unity. The needed products with powers of 2 could then be realized by appropriate shifts of the binary representation of the data values, leading to a valuable speed-up.

In the context of the computational power and speed of the present generation computers, the former “speed-up argument” is no longer as important as 40 years ago; however there are aspects of NTTs that still remain attractive, as the fact that NTTs work with integer arithmetic, thus achieving an accuracy that is not impaired by rounding effects. This is important for the multiplication of big numbers, digital watermarking, and some applications of Cryptography and signal processing. Furthermore the developments on ubiquitous computing and distributed embedded systems require small size – low power accurate and efficient devices, which again make NTTs interesting.

Most work related to NNTs is devoted to one dimensional transforms. Multidimensional transforms have been considered, but mostly as an effective way of computing one dimensional convolutions. In the present paper an asymmetric two-sided Fermat Number Theoretic Transform is introduced and its use to analyze properties of (classes of) patterns is explored.

The discrete Walsh transform is well known for its applications in Logic Design, Pattern Recognition, and Signal Processing. There are however “other” areas, where Walsh functions appear rather unexpectedly. In [11], for instance, it was reported that discrete Walsh functions in sequency order “appear quite naturally” in the layout of telephone lines to minimize cross-modulation effects. In [8] it was shown how Walsh matrices in Hadamard order appear in the Factorial Design of Industrial experiments [3]. The present paper contributes to illustrate how the Walsh transform also unexpectedly appears in the context of Number Theoretic Fermat Transforms of mosaics.

2 Basics of NNTs
NTTs were initially developed as a computationally efficient pendant to the Discrete Fourier Transform (DFT). The basic requirement of the kernel of the DFT on N points is
\[ \phi^N = 1, \]
where
\[ \phi = e^{j2\pi/N}, \]
i.e. \( \phi \) is an \( N \)-th root of unity computed on the unit circle.
In the case of an NNT the requirement is
\[ \alpha^N = 1 \mod M, \]

1 German proverb meaning "all good things come in groups of three". Work leading to this paper was partially supported by the Foundation for the Advance of Soft Computing, Asturias, Spain, and by the CICYT Spain, under project TIN 2011-29827-C02-01.
where $M$ is a modulus required to be an odd prime integer and $\alpha$ is a primitive $N$-th root of unity. Furthermore, for all $k < N$, $\alpha^{k}-1$ must be relative prime to $M$.

Notice that since all $N$ $N$-th roots of unity must be different, if $N$ is even

$$\alpha^{N/2} = \sqrt{\alpha} = -1 \mod M.$$ (4)

Finally if $\alpha$ is a primitive $N$-th root of unity and $Q$ is an integer larger than $N$, then

$$\alpha^{Q} \mod M = \alpha^{Q \mod N} \mod M.$$ (5)

**Definition 1** Let $\Gamma = [\gamma_{ij}]$, $ij \in \mathbb{Z}_{N}$, with $\gamma_{ij} = \alpha^{ij}$ modulo $M$ and $\alpha$ is a primitive $N$-th root of unity mod $M$.

It is fairly obvious that $\forall \ ij \in \mathbb{Z}_{N}$, $\gamma_{ij} = \gamma_{ji}$, since both are congruent with $\alpha^{ij}$ modulo $M$. Therefore $\Gamma = \Gamma^{T}$

If $M$ is chosen to be a Fermat number [2], then $N$ is a power of 2. Proper selection of $N$ will allow to work with $\alpha = 2$. It is well known that only the first 5 Fermat numbers are prime, but $F_{2}$ is more than large enough for the application studied in the present paper.

**Definition 2** A Fermat number has the structure $2^{2^{c}}+1$, where $c \in \mathbb{N}$. Fermat numbers will be denoted as $F_{c}$.

Table 1 shows the first 5 Fermat numbers and the values of $N = 2^{c+1}$ leading to $\alpha = 2$. (Notice that $2^{c} = N/2$, therefore $F_{c} = 2^{N/2}+1$.)

<table>
<thead>
<tr>
<th>$c$</th>
<th>$N = 2^{c+1}$</th>
<th>$M = F_{c} = 2^{N/2}+1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>$F_{1} = 2^2 + 1 = 5$</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>$F_{2} = 2^3 + 1 = 17$</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>$F_{3} = 2^5 + 1 = 257$</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
<td>$F_{4} = 2^{10} + 1 = 65,537$</td>
</tr>
<tr>
<td>5</td>
<td>64</td>
<td>$F_{5} = 2^{20} + 1 = 4,294,967,297$</td>
</tr>
</tbody>
</table>

In what follows, unless otherwise specified, operations on indices or exponents will be done modulo $N$, and operations on the values of components will be done modulo $M$.

**Lemma 1**

$$\sum_{i,j \in \mathbb{Z}_{N}} \gamma_{ij} = \begin{cases} N & \text{if } i \text{ or } j = 0 \\ 0 & \text{otherwise} \end{cases}$$ (6)

Proof:

If $i = 0$ then $\gamma_{ij} = 1$ and the summation over $j$ adds up to $N$. Similarly, if $j = 0$, the summation over $i$ adds up to $N$.

Recall that $\gamma_{ij} = \alpha^{ij}$. For $0 < i < N$ holds

$$\alpha^{N-1} = 1 + \alpha^{i} + \alpha^{2i} + \ldots + \alpha^{(N-1)i}$$

Since $\alpha^{N-1} = 0 \mod M$, then

$$1 + \alpha^{i} + \alpha^{2i} + \ldots + \alpha^{(N-1)i} = 0 \mod M$$

**Corollary 1.1**

If $k = N/p$, (where $p$ is a power of 2), then the polynomial used in Lemma 1 will have $p$ repetitions of length $k$, since $\alpha^{pk} = \alpha^{N} = 1 \mod M$. It is simple to see that

$$1 + \alpha^{k} + \alpha^{2k} + \ldots + \alpha^{(p-1)k} = 0 \mod M$$

If $k$ is a power of 2, then

$$1 + \alpha^{k} + \alpha^{2k} + \ldots + \alpha^{(N-1)k} = 0 \mod M$$

Let $S = [s_{ij}]$ be a square permutation matrix of dimension $N$, such that $\forall \ i \in \mathbb{Z}_{N}$, $s_{i(k-1)/2}$ (or simply $s_{k-1}$) equals 1, otherwise 0. It is easy to show that $S$ is symmetric and self-inverse.

**Definition 3**

Let $S = [s_{ij}]$ be a square permutation matrix of dimension $N$, such that $\forall \ i \in \mathbb{Z}_{N}$, $s_{i(k-1)/2}$ (or simply $s_{k-1}$) equals 1, otherwise 0. It is easy to show that $S$ is symmetric and self-inverse.

**Definition 4**

Let $a = [a_{ij}]$ be a square matrix such that $\forall \ i,j \in \mathbb{Z}_{N}$, $a_{ij} \in \mathbb{Z}_{M}$. Then $a^{*} := [a_{i-k,j-l}]$.

**Lemma 3** $a^{*} = S \cdot a \cdot S$ (8)

Proof:

Let $S \cdot a \cdot S = b$ Then $\forall \ k, l \in \mathbb{Z}_{N}$ holds:
\[ b_{k,\ell} = \sum_{i,j \in Z_N} a_{i,j} s_{j,\ell} = a_{k,\ell}. \]

**Corollary 3.1** \( \Gamma^* = \Gamma \) \hspace{1cm} (9)

Moreover, from \( S \cdot \Gamma = \Gamma \) follows \( S \cdot \Gamma^* = \Gamma \).

**Lemma 4** \hspace{1cm} (10)

\[ \Gamma^{-1} = N^{-1}S \Gamma = N^{-1} \Gamma S \mod M \]

**Proof:**
Let \( \Gamma = [g_{\ell,\ell}] \). Then \( \forall k, \ell \in Z_N \) holds:

\[ g_{k,\ell} = \sum_{i,j \in Z_N} a_{i,j} \alpha^i = \sum_{i,j} x^i \alpha^j = \sum_{j \in N} (x^{j+1}j). \]

From Lemma 1 follows:
\[ g_{k,\ell} = \begin{cases} N & \text{if } k = \ell \\ 0 & \text{otherwise} \end{cases} \]

In other words, \( \Gamma = N \cdot S \), from where \( \Gamma = N \cdot S \Gamma^{-1} \) and \( \Gamma^{-1} = N^{-1} \cdot S \Gamma = N^{-1} \mod M \).

Notice that since \( M \) is a prime, \((Z_M +, \cdot)\) is a field and since \( N < M \), then \( N^{-1} \) is well defined in \( Z_M \).

**Definition 5**
Let \( C \) be a set of colours with \( |C| = M \), and let \( \varphi : C \rightarrow Z_M \) be a bijection. Patterns are considered to be arrays of pixels with individual colours from \( C \). With \( \varphi \), patterns may be represented as numerical matrices with entries in \( Z_M \). It is assumed that operations on matrices induce discrete geometric or chromatic changes that have a meaning on patterns. In what follows, the word "pattern" will be used to denote both the pictorial and its corresponding matrix representation.

3 The two-sided asymmetric Fermat number theoretic transform of patterns

In this section, \( N \) and \( M \) are always taken from Table 1, thus guaranteeing that \( \alpha = 2 \).

**Definition 6**
Let \( a \) denote an \( N \) by \( N \) pattern with possibly different colours from \( C \). Its two-sided asymmetric Fermat number theoretic transform, or, for short here, its Fermat transform is given by:

\[ F(a) = A = \Gamma a \Gamma S \mod M. \]

From Lemma 4, the inverse transform is obtained as:

\[ F^{-1}(A) = a = \Gamma^{-1} A \Gamma^{-1} S = N^{-1} S \Gamma A \Gamma \mod M. \]

**Remark:** \( \Gamma S \) in Eq. (11) plays the role of the adjoint in complex valued transforms (see e.g. [6]). Similarly for \( S \Gamma \) in (12).

**Lemma 5**
The Fermat transform preserves the linear combination of patterns and (up to a scaling factor) it also preserves the matrix product of patterns.

**Proof:**
Let \( a \) and \( b \) be \( N \) by \( N \) patterns with different colours from \( C \). Furthermore, let \( p \) and \( q \) be scalars taken from \( Z_M \). Finally let \( y = pa + qb \mod M \) and \( w = a \cdot b \mod M \).

From (11),

\[ F(y) = \Gamma y \Gamma S = \Gamma (pa + qb) \Gamma S \mod M = \Gamma (pa) \Gamma S + \Gamma (qb) \Gamma S \mod M = p \Gamma a \Gamma S + q \Gamma b \Gamma S \mod M = pa + qb \mod M = pF(a) + qF(b) \mod M \]

\[ F(w) = \Gamma w \Gamma S = \Gamma a \Gamma b \Gamma S \mod M. \]

Let \( I_N \) denote the \( N \) by \( N \) identity matrix.

From (10) follows that \( I_N = N^{-1} \Gamma S \Gamma \mod M \). Therefore

\[ F(w) = \Gamma a \Gamma b \Gamma S = \Gamma a I_N \Gamma b \Gamma S \mod M = N^{-1} \Gamma a \Gamma S \Gamma b \Gamma S = N^{-1} (\Gamma a \Gamma S) (\Gamma b \Gamma S) \mod M \]

\[ = N^{-1} A B \mod M = N^{-1} A \Gamma S \Gamma \mod M. \]

**Definition 7**
Let \( n \mid N \). A pattern is a mosaic if it may be expressed as the Kronecker product of an \( N/n \) by \( N/n \) structure, all whose entries are 1, and an \( n \) by \( n \) seed. Figure 1 shows a simple example of a mosaic.

\[ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \]

**Structure**

Seed

**Mosaic**

Fig. 1: Example of a mosaic with four repetitions of a seed of dimension \( N/2 \).

It is easy to understand that a constant pattern is a trivial mosaic, with a 1 by 1 seed and an \( N \) by \( N \) structure. (A constant pattern is also obviously a mosaic with an \( n \) by \( n \) constant seed and an \( N/n \) by \( N/n \) structure, for any \( n \mid N \).)

**Lemma 6**
Let \( c \) be a constant pattern, all whose entries have the value \( c \in Z_M \). The Fermat transform of this pattern (mosaic) is a two dimensional Dirac delta scaled by \( cN^2 \mod M \).

**Proof:**
Let \( \Gamma cI_N \cdot \Gamma S = c \cdot [0, 1] \mod M \). Then \( \forall k, \ell \in Z_N \) holds:
\[ c_{f,k} = c \sum_{i,j} \sum_{Z_{n}} a_{i,j} f_{i,j} = c \sum_{i,j} \sum_{Z_{n}} a_{i,j}. \]

With Lemma 1, \( c_{f,k} = cN^2 \) if \( k = \ell = 0 \) and otherwise is 0.

**Theorem 1**

The Fermat transform reverses the Kronecker structure inherent in mosaics:

\[ F \begin{array}{c}
\text{Structure} \\
\otimes \\
\text{seed} \\
\end{array} \begin{array}{c}
\text{image} \\
\otimes \\
\delta_{0,0} \\
\end{array} \]

where the image is of the same dimension of the seed and \( \delta_{0,0} \) represents the Fermat transform of the structure down-scaled by the square of its dimension. I.e., \( \delta_{0,0} \) denotes a square matrix of dimension \( N/n, \) s.t. the upper left entry is 1 and all others are 0.

Proof: Let \( \text{MOS} = \text{structure} \otimes \text{seed} = [m_{i,j}] \) denote a mosaic. \( F(\text{MOS}) = \Gamma(\text{MOS}) \Gamma = [\omega_{i,j}] \).

For all \( p, q \in Z_{n} \)

\[ \omega_{p,q} = \sum_{i,j} \sum_{Z_{n}} a_{i,j}^{p} m_{i,j} a_{i,j}^{q} \mod M. \] (14)

Notice that for all \( r, t \in Z_{n} \) and \( u, v \in Z_{n}/n \)

\[ \text{mos}_{r,t} = \text{seed}_{r,t} = m_{s_{r,t}} + un, t + vn \] (15)

Introducing (15) in (14) the following is obtained:

\[ \omega_{p,q} = \sum_{i,j} \sum_{Z_{n}} a_{i,j}^{p} m_{i,j} a_{i,j}^{q} \sum_{u,v} \sum_{Z_{n}/n} a_{i,j}^{u} a_{i,j}^{v} \cdot (\text{mod } M). \] (16)

Case 1: Let \( p = q = 0 \) in Eq. (16):

\[ \omega_{0,0} = (N/n)^2 \sum_{i,j} m_{i,j} \mod M. \] (17)

Case 2: Let \( p = y/n \) and \( q = z/n \), with \( y, z \in Z_{n} \).

Then Eq. (16) gives:

\[ \omega_{p,q} = \left( \sum_{i,j} \sum_{Z_{n}} a_{i,j}^{y/n} m_{i,j} \frac{z}{n} \right) \cdot (\text{mod } M). \] (18)

\[ \omega_{p,q} = \left( \sum_{u,v} \sum_{Z_{n}/n} a_{u,v}^{y/n} m_{u,v} \frac{z}{n} \right) \mod M. \]

The second factor of Eq. (18) will become:

\[ \sum_{u,v} \sum_{Z_{n}/n} a_{u,v}^{y/n} m_{u,v} \frac{z}{n} = \sum_{u,v} a_{u,v}^{y/n} m_{u,v} \frac{z}{n} \mod M. \]

Assume that \( v \in Z_{n}/n \) \( \setminus 0 \)

\[ \sum_{u} a_{u,v}^{y/n} m_{u,v} \frac{z}{n} = \sum_{u} a_{u,v}^{y/n} m_{u,v} \frac{z}{n} \mod M. \]

However since \( a^{N} \equiv 1 \mod M \), then

\[ \sum_{u} a_{u,v}^{y/n} m_{u,v} \frac{z}{n} = \sum_{u} a_{u,v}^{y/n} m_{u,v} \mod M, \] (22)

and

\[ \sum_{u} a_{u,v}^{y/n} m_{u,v} = 1 + a^{y/n} + a^{2y/n} + \ldots + a^{(N/n-1)y/n} \equiv 1 + a^{y/n} + a^{2y/n} + \ldots + a^{(N/n-1)y/n} \mod M. \]

But

\[ a^{N/n} = a^{N/n} = 1 \mod M. \]

Then \( a^{(N/w - w)} = a^{N/n - w} \mod M \), which leads to:

\[ \sum_{u} a_{u,v}^{y/n} m_{u,v} = 1 + a^{y/n} + a^{2y/n} + \ldots + a^{(N/w - w)} \mod M. \]

According to Lemma 1, (setting \( i = w/v \)), this polynomial adds up to 0. Therefore (21) takes the value 0, and in (18), \( \omega_{p,q} = 0 \). Similarly, when \( u \in Z_{n}/n \) \( \setminus 0 \)

\[ \sum_{v} a_{u,v}^{y/n} m_{u,v} = 0. \]

Therefore with \( p \) and \( q \) as specified in Case 3, \( \omega_{p,q} = 0 \).
Summarizing, Eq. (17) is a special case of Eq. (20). These Eqs. specify the (non-necessarily 0) value of the entries of F(MOS), which are spaced at a distance N/n of each other and have as reference, the (0,0) entry. All other entries of F(MOS) are 0.

Define an n by n matrix called image such that
\[ \text{image}_{(y,z)} = F(\text{MOS})_{(y,z),N/n} \quad y, z \in Z_n \]
then
\[ F(\text{MOS}) = \text{image} \otimes \delta_{0,0} \]
where \( \delta_{0,0} \) denotes a 2D Dirac delta, of dimension N/n by N/n, and it corresponds to the Fermat transform of the structure of the mosaic, normalized by its Hamming weight. Notice that formally for this transform work should have been done with an \( N' = N/n \) and a modulus \( M' = 2^{N'/2} \), providing an \( \alpha' = 2 \) (even if \( N/n = 2 \); see below).

**Example 1:**
Let \( N = 8 \), \( M = 17 \), \( \alpha = 2 \), and \( n = 4 \).

Define
\[ \text{MOS} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 4 & 1 & 2 & 3 \\ 3 & 0 & 2 & 1 \\ 5 & 2 & 3 & 1 \\ 1 & 3 & 2 & 5 \end{bmatrix} \]
\[ \text{MOS} = \begin{bmatrix} 4 & 1 & 2 & 3 \\ 3 & 0 & 2 & 1 \\ 5 & 2 & 3 & 1 \\ 1 & 3 & 2 & 5 \end{bmatrix} \]
\[ F(\text{MOS}) = \begin{bmatrix} 1 \end{bmatrix} \]
From where
\[ F(\text{MOS}) \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \]
Notice that by extrapolating backwards one obtains:
\[ F_0 = 3, \text{ with } N = 2 \text{ and } \alpha = 2, \text{ since } 2^2 = 1 \text{ mod } 3 \text{ and } \text{gcd}(2^2, 3) = 1. \]

(\[ \begin{array}{cccc} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{array} \] mod 3
\[ \text{(The Hamming weight of the structure is } 4, \text{ but } 4 \equiv 1 \text{ mod 3)\]}

**Theorem 2:**
Let the seed of an \( N \) by \( N \) mosaic be of dimension 2 by 2, then the image in Eq. (13) is obtained as the **Walsh transform** of the seed, up to a scaling factor \((N/2)^2\), and all calculations are done modulo \( M \).

Proof:
Let seed = \[ \begin{bmatrix} \sigma_{p,0} & \sigma_{p,N/2} \\ \sigma_{0,0} & \sigma_{0,N/2} \end{bmatrix} \]
then MOS = \[ \begin{bmatrix} 1 & \ldots & 1 \\ \ldots & \ldots & \ldots \\ 1 & \ldots & 1 \end{bmatrix} \otimes \begin{bmatrix} \sigma_{0,0} & \sigma_{0,1} \\ \sigma_{0,1} & \sigma_{1,1} \end{bmatrix} \]
From Theorem 1,
\[ F(\text{MOS}) = \text{image} \otimes \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \end{bmatrix} = [\omega_{p,q}] \]
and image = \[ \begin{bmatrix} \omega_{0,0} & \omega_{0,N/2} \\ \omega_{N/2,0} & \omega_{N/2,N/2} \end{bmatrix} \]
From Eq. (17),
\[ \omega_{0,0} = \left( \frac{N}{2} \right)^2 \sum_{i,j \in \{0,1\}} \alpha_{i,j} \text{ mod } M. \quad (23) \]
From Eq. (20),
\[ \omega_{p,q} = \left( \frac{N}{2} \right)^2 \sum_{i,j \in \{0,1\}} \alpha_{i,j} \left( \frac{\psi_{i,j} y z}{N} \right)^2, \]
with \( y, z \in \{0, 1\} \) corresponding to \( p, q \in \{0, N/2\} \). Then
\[ \omega_{N/2,0} = \left( \frac{N}{2} \right)^2 \sum_{i,j \in \{0,1\}} \alpha_{i,j} \left( \frac{\psi_{i,j} y z}{N} \right)^2, \]
Since \( -N/2 \equiv N/2 \text{ mod } N \), and \( \alpha \equiv -1 \text{ mod } M \), then:
\[ \omega_{0,0} = \left( \frac{N}{2} \right)^2 (\sigma_{0,0} + \sigma_{1,0} - \sigma_{0,1} - \sigma_{1,1}) \text{ mod } M. \quad (24) \]

Similarly,
\[ \omega_{0,N/2} = \left( \frac{N}{2} \right)^2 (\sigma_{0,0} - \sigma_{1,0} + \sigma_{0,1} - \sigma_{1,1}) \text{ mod } M. \quad (25) \]
\[ \omega_{N/2,0} = \left( \frac{N}{2} \right)^2 (\sigma_{0,0} - \sigma_{1,0} - \sigma_{0,1} + \sigma_{1,1}) \text{ mod } M. \quad (26) \]

On the other hand, the two sided Walsh transform of the seed is:
\[ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \]
\[
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\begin{bmatrix}
\sigma_{0,0} & \sigma_{0,1} \\
\sigma_{1,0} & \sigma_{1,1}
\end{bmatrix}
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
= \\
\begin{bmatrix}
\sigma_{0,0} + \sigma_{1,0} & \sigma_{0,1} + \sigma_{1,1} \\
\sigma_{0,0} - \sigma_{1,0} & \sigma_{0,1} - \sigma_{1,1}
\end{bmatrix}
\]
\[
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
= \\
\begin{bmatrix}
\sigma_{0,0} + \sigma_{1,0} + \sigma_{1,1} & \sigma_{0,0} + \sigma_{1,0} - \sigma_{0,1} - \sigma_{1,1} \\
\sigma_{0,0} - \sigma_{1,0} + \sigma_{0,1} - \sigma_{1,1} & \sigma_{0,0} - \sigma_{1,0} - \sigma_{0,1} + \sigma_{1,1}
\end{bmatrix}
= \\
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\]

(28)

A comparison of Eqs. (23) to (26) with the entries of

\[
image = (N/2)^2 \cdot W_2 \cdot \text{seed} \cdot W_2 \mod M
\]

Example 2: Let \( N = 8, M = 17, \alpha = 2, \) and \( n = 2 \)

\[
\text{MOS} = \begin{bmatrix}
1 & 1 & 1 \\
1 & 1 & 1 \\
1 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix}
\otimes
\begin{bmatrix}
4 & 2 \\
2 & 1
\end{bmatrix}
\]

\[
\text{MOS} = \begin{bmatrix}
1 & 2 & 4 \\
1 & 2 & 4 \\
1 & 2 & 4 \\
1 & 2 & 4
\end{bmatrix}
\]

\[
F(\text{MOS}) = \begin{bmatrix}
8 & 14 \\
14 & 16
\end{bmatrix}
\]

Applying Theorem 2:

\[
\left(\frac{8}{2}\right)^3 \begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\begin{bmatrix}
4 & 2 \\
2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\mod 17 = \\
16 \begin{bmatrix}
6 & 3 \\
2 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
= 16 \begin{bmatrix}
9 & 3 \\
3 & 1
\end{bmatrix}
= \begin{bmatrix}
8 & 14 \\
14 & 16
\end{bmatrix}
\mod 17
\]

Therefore

\[
F(\text{MOS}) = \begin{bmatrix}
8 & 14 \\
14 & 16
\end{bmatrix}
\otimes
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\mod 17
\]

Notice that if instead of the Walsh transform a Fermat transform with \( N = 2 \) and \( M = 3 \) as in example 1 had been used to process the seed, then the seed would have been immersed in a modulo 3 computation and the 4 entry would have been falsified to 1 (since 4 = 1 mod 3). A wrong result would have been the consequence.

References
