BLOCK-CIRCULANT MATRICES WITH CIRCULANT BLOCKS, WEIL SUMS AND MUTUALLY UNBIASED BASES, II. THE PRIME POWER CASE

Monique Combescure

October 30, 2007

Abstract

In our previous paper [7] we have shown that the theory of circulant matrices allows to recover the result that there exists $p+1$ Mutually Unbiased Bases in dimension p, p being an arbitrary prime number. Two orthonormal bases $\mathcal{B}$, $\mathcal{B}'$ of $\mathbb{C}^d$ are said mutually unbiased if $\forall b \in \mathcal{B}$, $\forall b' \in \mathcal{B}'$ one has that

$$|b \cdot b'| = \frac{1}{\sqrt{d}}$$

($b \cdot b'$ hermitian scalar product in $\mathbb{C}^d$). In this paper we show that the theory of block-circulant matrices with circulant blocks allows to show very simply the known result that if $d = p^n$ (p a prime number, n any integer) there exists $d+1$ mutually Unbiased Bases in $\mathbb{C}^d$. Our result relies heavily on an idea of Klimov, Muñoz, Romero [11]. As a subproduct we recover properties of quadratic Weil sums for $p \geq 3$, which generalizes the fact that in the prime case the quadratic Gauss sums properties follow from our results.

1 INTRODUCTION

The Mutually Unbiased Bases in dimension d are a set $\{\mathcal{B}_1, ..., \mathcal{B}_N\}$ of orthonormal bases in $\mathbb{C}^d$ such that for any $b_j^{(k)} \in \mathcal{B}_k$, $b_{j'}^{(k')} \in \mathcal{B}_{k'}$ one has

$$\left| b_j^{(k)} \cdot b_{j'}^{(k')} \right| = \frac{1}{\sqrt{d}}, \ \forall j, j' = 1, ..., d, \ \forall k' \neq k = 1, ..., N$$

where $b \cdot b' = \sum_{j=1}^d b_j^* b'_j$ is the usual scalar product in $\mathbb{C}^d$.
This notion of mutually unbiased bases emerged in the seminal work of Schwinger

[14] and turned out to be a cornerstone in the theory of quantum information. Furthemore it is strongly linked with the theory of Hadamard matrices [9] and to the Gauss Sums properties.

An important problem is the maximum number of mutually unbiased bases (MUB) in dimension d. The problem has been completely solved for $d = p^n$ where p is a prime number, and n any integer, in which case one can find $N = d + 1$ MUB's [2][16][18] [10][5].

In a previous paper [7] (hereafter refered to as I) we have provided a construction of $d + 1$ MUB's for d a prime number using a new method involving circulant matrices. Then the MUB problem reduces to exhibit a circulant matrix C which is a unitary Hadamard matrix, such that its powers are also circulant unitary Hadamard matrices. Then using the Discrete Fourier Transform F_d which diagonalizes all circulant matrices, we have shown that a MUB in that case is just provided by the set of column vectors of the set of matrices $\left\{F_d, \mathbb{1}, C, C^2, ..., C^{d-1}\right\}$. Properties of quadratic Gauss sums follow as a by-product of the method.

The present paper is a continuation of I, where we consider $d = p^n$. Here circulant matrices are replaced by a set of block-circulant with circulant blocks matrices. Again the discrete Fourier transform which in this case will be simply $F \equiv F_p \otimes F_p \otimes ... \otimes F_p$ will play a central role since it diagonalizes all block-circulant with circulant blocks matrices. We follow an idea of [11] to define them. The new result developed here is that these block-circulant matrices with circulant blocks together with F will solve the MUB problem in that case.

Let $\mathcal{B}_k = \left\{b_0^{(k)}, b_1^{(k)}, ..., b_{d-1}^{(k)}\right\}$ be orthonormal bases. Then in any given base, they are represented by unitary matrices B_k. Taking $\mathcal{B}_0$ to be the natural base, we have that

$$b_j^{(k)} \cdot b_{j'}^{(k')} = (B_k^* B_{k'})_{j,j'}$$

Thus in order that the bases $\mathcal{B}_k$ be unbiased, we just need that all the unitary matrices $B_k^* B_{k'},\ k \neq k'$ have matrix elements of modulus $d^{-1/2}$. Such matrices are known as **unitary Hadamard Matrices** ([9]).

2 THE SQUARE OF A PRIME

Let p be a prime number. One defines a primitive p-th root of unity :

$$\omega = \exp\left(\frac{2\pi i}{p}\right)$$

The Discrete Fourier Transform in $\mathbb{C}^p$ is

$$F_p = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & 1 & 1 & . & . & 1 \\ 1 & \omega & \omega^2 & . & . & \omega^{p-1} \\ 1 & \omega^2 & \omega^4 & . & . & \omega^{2(p-1)} \\ . & . & . & . & . & . \\ 1 & \omega^{p-1} & \omega^{2(p-1)} & . & . & \omega^{(p-1)(p-1)} \end{pmatrix}$$

Definition 2.1 *Consider a d-periodic sequence* $a_0, a_1, ..., a_{d-1}, a_0, a_1, ...$
(i) A $d \times d$ *matrix* D *is diagonal and called* $\mathrm{diag}(a_0, ..., a_{d-1})$ *if its matrix elements satisfy*

$$D_{j,k} = a_k \delta_{j,k}, \ \forall j, k = 0, 1, ..., d-1$$

(ii) A $d \times d$ *matrix* C *is called circulant and denoted* $C = \mathrm{circ}(a_0, ..., a_{d-1})$ *if its matrix elements satisfy*

$$C_{j,k} = a_{(d-1)j+k}$$

Thus it can be written as :

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & . & . & a_{d-1} \\ a_{d-1} & a_0 & a_1 & . & . & a_{d-2} \\ . & . & . & . & . & . \\ a_1 & a_2 & a_3 & . & . & a_0 \end{pmatrix}$$

(iii) A diagonal and circulant matrix must be a multiple of the identity matrix $\mathbb{1}$.
(iv) A $d^2 \times d^2$ *matrix is said to be block-circulant if it is of the form*

$$C = \mathrm{circ}(C_0, C_1, ..., C_{d-1})$$

where the C_j *are* $d \times d$ *matrices.*
(v) It is block-circulant with circulant blocks if furthermore the C_j *are circulant.*
(vi) A $d \times d$ *matrix* H *is a unitary Hadamard matrix if*

$$|H_{j,k}| = d^{-1/2}, \text{ and } \sum_{k=0}^{d-1} H^*_{j,k} H_{k,l} = \delta_{j,l}$$

We define the following $p \times p$ unitary matrices

$$X = \mathrm{circ}(0, 0, ..., 1)$$

$$Z = \mathrm{diag}(1, \omega, ..., \omega^{p-1})$$

They obey the ω- commutation rule :

Lemma 2.2 *(i)* $X^p = Z^p = \mathbb{1}$
(ii)

$$ZX = \omega XZ$$

(iii) Furthemore one has

$$F_p X F_p^* = Z$$

(i) and (ii) are obvious. For a proof of (iii) see [8].

Proposition 2.3 *Let* $C = \mathrm{circ}(a_0, ..., a_{p-1})$*.*
(i) One has

$$C = \sum_{k=0}^{p-1} a_k X^{p-k}$$

(ii)The discrete Fourier transform diagonalizes the circulant matrices :

$$F_p C F_p^* = \mathrm{diag}(\tilde{a}_0, ..., \tilde{a}_{p-1})$$

where

$$\tilde{a}_j = \sum_{k=0}^{p-1} a_k \omega^{-jk}$$

(iii) The set of circulant $p \times p$ *matrices is a commutative algebra.*

Proof :

$$F_p C F_p^* = \sum_{k=0}^{p-1} a_k Z^{p-k}$$

But $Z^{-k} = \mathrm{diag}(1, \omega^{-k}, ..., \omega^{-k(p-1)})$, hence (ii) follows. (iii) is a consequence of (i).

Corollary 2.4 *If the sequence* $\{a_k\}_{k \in \mathbb{F}_d}$ *is such that*

$$|a_k| = d^{-1/2} \text{ and } |\tilde{a}_k| = 1$$

then C *is a circulant unitary Hadamard matrix.*

Proof : C is unitarily equivalent to an unitary matrix if $|\tilde{a}_k| = 1$. Furthemore $|a_k| = d^{-1/2}$, hence the result follows (see [7]).

The discrete Fourier transform in $\mathbb{C}^{p^2}$ is defined as follows

$$F = F_p \otimes F_p \tag{2.1}$$

It has the following important property (similar to the property that the discrete Fourier transform diagonalizes all circulant matrices) :

Proposition 2.5 *(i)* F *is an unitary Hadamard matrix.*
(ii) All block-circulant matrices C *with circulant blocks are diagonalized by* F *:*

$$FCF^* = D$$

where D *is a* $p^2 \times p^2$ *diagonal matrix.*

For a proof of this result see [8].

We shall be interested in finding block-circulant with circulant blocks unitary matrices in $\mathbb{C}^{p^2}$ that are Hadamard matrices. An example is of course $C \otimes C'$ where $C,\ C'$ are unitary circulant Hadamard matrices.

For p a prime number, denote by $\mathbb{F}_p$ the field of residues modulo p. The corresponding Galois field $GF(p^2)$ is defined as follows. For any p there exists an irreducible polynomial of degree two, with coefficients in $\mathbb{F}_p$ so that if we denote by α a root of this polynomial,

$$GF(p^2) = \{m\alpha + n\}_{m,n\in\mathbb{F}_p}$$

The product $\theta \cdot \theta' \in GF(p^2)$ for $\theta,\ \theta' \in GF(p^2)$ is obtained using the irreducible polynomial which expresses α^2 in terms of α and 1.
The additive characters $\chi(\theta)$ in $GF(p^2)$ are defined as follows:

Definition 2.6 *The additive characters on $GF(p^2)$ are :*

$$\chi(\theta) = \exp\left(\frac{2i\pi}{p}\mathrm{tr}\theta\right)$$

where

$$\mathrm{tr}\theta = \theta + \theta^p$$

Lemma 2.7 *They satisfy :*
(i) $\chi(\theta + \theta') = \chi(\theta)\chi(\theta')$
(ii) One has :

$$\sum_{\theta\in GF(p^2)} \chi(\theta) = 0$$

(iii)

$$\sum_{\theta'\in GF(p^2)} \chi(\theta \cdot \theta') = p^2\delta_{\theta,0} \tag{2.2}$$

We take as natural basis in $\mathbb{C}^{p^2}$ the set of states labelled by $\theta \in GF(p^2)$, in the following order :

$$\mathcal{B} \equiv \{|0\rangle, |\alpha\rangle, |2\alpha\rangle, ..., |1\rangle, |1+\alpha\rangle, ..., |p-1\rangle, ..., |p-1+(p-1)\alpha\rangle\}$$

Labelled by $\theta \in GF(p^2)$ we define a set of unitary operators in $\mathbb{C}^{p^2}$ such that :

Definition 2.8 *(i) The set of operators $\mathcal{F} \equiv \{X_\theta\}_{\theta\in GF(p^2)}$ obeys*

$$X_\theta|\theta'\rangle = |\theta + \theta'\rangle,\ \forall\theta' \in GF(p^2) \tag{2.3}$$

(ii) The set of diagonal operators $\mathcal{F}' \equiv \{Z_\theta\}_{\theta\in GF(p^2)}$ obeys

$$Z_\theta|\theta'\rangle = \chi(\theta \cdot \theta')|\theta\rangle,\ \forall\theta' \in GF(p^2) \tag{2.4}$$

They obey :

Proposition 2.9 *(i)*

$$Z_\theta X_{\theta'} = \chi(\theta \cdot \theta') X_{\theta'} Z_\theta \tag{2.5}$$

(ii) The operators in $\mathcal{F}$, $\mathcal{F}'$ obey the group commutative property :

$$X_{\theta+\theta'} = X_\theta X_{\theta'} = X_{\theta'} X_\theta, \quad Z_{\theta+\theta'} = Z_\theta Z_{\theta'} = Z_{\theta'} Z_\theta \tag{2.6}$$

(iii) $Z_0 = X_0 = \mathbb{1}$

Proof : Take any $\varphi \in GF(p^2)$. Then

$$Z_\theta X_{\theta'} |\varphi\rangle = \chi(\theta \cdot (\theta' + \varphi)) |\theta' + \varphi\rangle = \chi(\theta \cdot \theta') X_{\theta'} Z_\theta |\varphi\rangle = \chi(\theta \cdot \theta') \chi(\theta \cdot \varphi) |\theta' + \varphi\rangle$$

We also have (ii) :

$$Z_{\theta+\theta'} |\varphi\rangle = \chi((\theta + \theta') \cdot \varphi) |\varphi\rangle = \chi(\theta \cdot \varphi) \chi(\theta' \cdot \varphi) |\varphi\rangle = Z_\theta Z_{\theta'} |\varphi\rangle$$

□

Theorem 2.10 *(i)*

$$\mathcal{F} = \{X^m \otimes X^n\}_{m,n \in \mathbb{F}_p}$$

More precisely one has

$$X_{m\alpha+n} = X^n \otimes X^m \tag{2.7}$$

(ii) All operators in $\mathcal{F}$ are represented by unitary block-circulant with circulant blocks $p^2 \times p^2$ matrices.
(iii)

$$\mathcal{F}' = \{Z^m \otimes Z^n\}_{m,n \in \mathbb{F}_p}$$

(iv) All operators in $\mathcal{F}'$ are represented by diagonal $p^2 \times p^2$ matrices.
(v) For any $\theta' \in GF(p^2)$ there exists a $\theta \in GF(p^2)$ such that

$$F X_{\theta'} F^* = Z_\theta \tag{2.8}$$

Proof of (i) : It is enough to see that $X_\alpha = \mathbb{1} \otimes X$ and $X_1 = X \otimes \mathbb{1}$ since the other matrices $X_{m\alpha+n}$ will be given by the chain rule :

$$X_{m\alpha+n} = X_\alpha^m X_1^n$$

But these are obviously block-circulant with circulant blocks matrices.
One has for $\theta' = m\alpha + n$:

$$F X_{m\alpha+n} F^* = F X_\alpha^m X_1^n F^* = (F_p \otimes F_p)(X^n \otimes X^m)(F_p^* \otimes F_p^*) = Z^n \otimes Z^m$$

which is Z_θ for some $\theta \in GF(p^2)$. □
One recalls a famous result [8] :

Proposition 2.11 *All block-circulant matrices with circulant blocks commute and are diagonalized by F.*

Proof : It follows from (2.8) that if $C = \sum_{\theta'} \lambda_{\theta'} X_{\theta'}$ is a block-circulant matrix with circulant blocks, one has

$$FCF^* = \sum_{\theta' \in GF(p^2)} \lambda_{\theta'} F X_{\theta'} F^* = \sum_{\theta' \in GF(p^2)} \lambda_{\theta'} Z_{f(\theta')}$$

which is a diagonal matrix.

To find the MUB's in dimension p^2 it is enough to exhibit a partition of the set of unitary operators :

$$\mathcal{E} \equiv \{Z_\theta X_{\theta'}\}_{\theta,\theta' \in GF(p^2)}$$

into a set of commutant families : We define

$$\mathcal{F}_0 = \mathcal{F} \setminus \{\mathbb{1}\}$$

One wants :

$$\mathcal{E} = \mathcal{F}_0 \bigcup_{\theta \in GF(p^2)} \mathcal{C}_\theta \cup \{\mathbb{1}\}$$

The family $\mathcal{C}_\theta$ will be defined as follows :

Definition 2.12 *Let for any $\theta \in GF(p^2)$*

$$\mathcal{E}_\theta = \{Z_{\theta'} X_{\theta \cdot \theta'}\}_{\theta' \in GF(p^2)}$$

Define

$$\mathcal{C}_\theta = \mathcal{E}_\theta \setminus \{\mathbb{1}\}$$

Proposition 2.13 *(i) $\mathcal{E}_0 = \mathcal{F}'$*
(ii) $\mathcal{E}_\theta$ is a commuting family $\forall \theta \in GF(p^2)$.
(iii) $\mathcal{E} = \mathcal{F}_0 \bigcup_{\theta \in GF(p^2)} \mathcal{C}_\theta \cup \{\mathbb{1}\}$ is a partition of $\mathcal{E}$.

Proof : (i) is obvious.
(ii) $\forall \theta', \ \theta'' \in GF(p^2)$ one has

$$Z_{\theta'} X_{\theta \cdot \theta'} Z_{\theta''} X_{\theta'' \cdot \theta} = \chi(-\theta \cdot \theta' \cdot \theta'') Z_{\theta' + \theta''} X_{\theta \cdot (\theta' + \theta'')} = Z_{\theta''} X_{\theta \cdot \theta''} Z_{\theta'} X_{\theta \cdot \theta''}$$

(iii) $\mathcal{C}_\theta$ and $\mathcal{F}_0$ contain $p-1$ elements. The classes $\mathcal{C}_\theta$ for different θ are disjoint. Therefore

$$\bigcup_{\theta \in GF(p^2)} \mathcal{C}_\theta$$

contains $p(p-1)$ elements. One has :

$$p - 1 + p(p-1) + 1 = p^2$$

which is the total number of elements in $\mathcal{E}$.

Since all the unitary operators in $\mathcal{C}_\theta$ commute, they can be diagonalized by the same operator R_θ. In the above cited work [11] they are defined as "rotation operators". In fact we shall see that they are represented in the basis $\mathcal{B}$ by block-circulant with circulant block matrices. The first main result of this paper is the following :

Theorem 2.14 *(i) There exists a set* $\{R_\theta\}_{\theta\in GF(p^2)}$ *of unitary operators which diagonalize all the operators of the class* $\mathcal{C}_\theta,\ \forall\theta \in GF(p^2)$.
(ii) The operators R_θ for $\theta \neq 0$ *are represented in the basis* $\mathcal{B}$ *by block-circulant with circulant block matrices which are unitary Hadamard matrices.*
(iii) For $p \geq 3$ *they obey the group law :*

$$R_{\theta+\theta'} = R_\theta R_{\theta'},\ \forall\theta,\ \theta' \in GF(p^2)$$

Proof : It is enough to show that for any $\theta \in GF(p^2)\backslash\{0\}$ the R_θ can be expanded as

$$R_\theta = \sum_{\theta'\in GF(p^2)} \lambda^{(\theta)}_{\theta'} X_{\theta'} \tag{2.9}$$

since they will automatically represented in the basis $\mathcal{B}$ by block-circulant with circulant blocks matrices. One has to check that

$$R_\theta^{-1} Z_{\theta'} X_{\theta\cdot\theta'} R_\theta = \mu_{\theta,\theta'} Z_{\theta'},\ \forall\theta' \in GF(p^2)$$

Since the operators $Z_{\theta'}X_{\theta\cdot\theta'}$ are unitary, the $\mu_{\theta,\theta'}$ are necessarily complex numbers of modulus one. But

$$Z_{\theta'}X_{\theta\cdot\theta'}\sum_{\theta''}\lambda^{(\theta)}_{\theta''}X_{\theta''} = Z_{\theta'}\sum_{\theta''}\lambda^{(\theta)}_{\theta''}X_{\theta''+\theta\cdot\theta'} = \mu_{\theta,\theta'}\sum_{\theta'''}\lambda^{(\theta)}_{\theta'''}X_{\theta'''}Z_{\theta'} = \mu_{\theta,\theta'}Z_{\theta'}\sum_{\theta'''}\chi(-\theta'\cdot\theta''')\lambda^{(\theta)}_{\theta'''}X_{\theta'''}$$

Equating the coefficients of $X_{\theta'''}$ in both sides we get

$$\lambda^{(\theta)}_{\theta'''-\theta\cdot\theta'} = \mu_{\theta,\theta'}\chi(-\theta'\cdot\theta''')\lambda^{(\theta)}_{\theta'''}$$

Taking $\theta''' = 0$ and assuming that $\lambda^{(\theta)}_0 = p^{-1},\ \forall\theta \in GF(p^2)$ we get

$$\lambda^{(\theta)}_{-\theta\cdot\theta'} = p^{-1}\mu_{\theta,\theta'}$$

or equivalently, since $\theta \neq 0$

$$\lambda^{(\theta)}_{\theta'} = p^{-1}\mu_{\theta,-\theta^{-1}\cdot\theta'}$$

This proves that all the $\lambda^{(\theta)}_{\theta'}$ must be of modulus p^{-1}.
Therefore since all the X_θ are represented by unitary matrices that have non-zero elements (actually 1) where all the others have zeros, and since every matrix element of R_θ is of the form $\lambda^{(\theta)}_{\theta'}$ for some $\theta' \in GF(p^2)$, this proves that all the R_θ are represented by Hadamard matrices.

Now we have to check the compatibility condition. We reexpress it in terms of $\mu_{\theta,\theta'}$. Supressing the index θ in the $\mu_{\theta,\theta'}$ for simplicity, we need to have $\forall\theta',\ \theta'' \in GF(p^2)$

$$\mu_{-\theta^{-1}(\theta''-\theta\theta')} = \mu_{\theta'}\mu_{-\theta^{-1}\theta''}\chi(-\theta'\cdot\theta'')$$

or in other terms

$$\mu_{\theta'+\theta''} = \mu_{\theta'}\mu_{\theta''}\chi(\theta\cdot\theta'\cdot\theta'') \tag{2.10}$$

But this results easily from the group property of the X_θ's and Z_θ's (2.3, 2.4) :

$$R_\theta^{-1}Z_{\theta'+\theta''}X_{\theta\cdot(\theta'+\theta'')}R_\theta = \chi(\theta\theta'\theta'')R_\theta^{-1}Z_{\theta'}X_{\theta\theta'}R_\theta R_\theta^{-1}Z_{\theta''}X_{\theta\theta''}R_\theta = \chi(\theta\theta'\theta'')\mu_{\theta,\theta'}\mu_{\theta,\theta''}Z_{\theta'+\theta''}$$

In [11] it is shown that for $p \geq 3$ the solution of (2.10) with $\mu_{\theta,0} = 1$ is

$$\mu_{\theta,\theta'} = \chi(2^{-1}\theta\cdot\theta'^2) \tag{2.11}$$

Thus we deduce that

$$\lambda_{\theta'}^{(\theta)} = p^{-1}\chi(2^{-1}\theta^{-1}\cdot(\theta')^2) \tag{2.12}$$

We now prove the unitarity of R_θ. For $\theta = 0$ this is obvious since $R_0 = \mathbb{1}$. It is enough to check that for $\theta \neq 0$ one has :

$$\sum_{\theta'\in GF(p^2)} (\lambda_{\theta'}^{(\theta)})^*\lambda_{\theta'+\theta''}^{(\theta)} = \delta_{\theta'',0}$$

One has :

$$\sum_{\theta'\in GF(p^2)} (\lambda_{\theta'}^{(\theta)})^*\lambda_{\theta'+\theta''}^{(\theta)} = \frac{1}{p^2}\sum_{\theta'\in GF(p^2)} \mu^*_{\theta,-\theta^{-1}.\theta'}\mu_{\theta,-\theta^{-1}\cdot(\theta'+\theta'')}$$

$$= \frac{1}{p^2}\sum_{\theta'\in GF(p^2)} |\mu_{\theta,-\theta^{-1}.\theta'}|^2\mu_{\theta,-\theta^{-1}.\theta''}\chi(\theta^{-1}\theta'\theta'') = \mu_{\theta,-\theta^{-1}.\theta''}\frac{1}{p^2}\sum_{\theta'\in GF(p^2)}\chi(\theta^{-1}\theta'\theta'') = \delta_{\theta'',0}$$

where we have used (2.10) and (2.2), together with the fact that $\theta^{-1}\cdot\theta'' = 0$ implies $\theta'' = 0$ due to the field property of $GF(p^2)$. Thus one has

$$R_\theta^{-1} = R_\theta^*,\ \forall\theta \in GF(p^2)$$

(iii) The group law $R_{\theta+\theta'} = R_\theta R_{\theta'}$ for $p \geq 3$ has been established in [11]. For $p = 2$ it has to be suitably modified as shown in [11] (see remark below). Let us see how it works for $p \geq 3$:

$$(R_1^*)^n(R_\alpha^*)^m Z_{\theta'}X_{(n+m\alpha)\cdot\theta'}R_1^nR_\alpha^m = (R_1^*)^n(R_\alpha^*)^m Z_{\theta'}X_{\theta'\cdot m\alpha}R_\alpha^m X_{n\theta'}R_1^n = \mu(m\alpha,\theta')(R_1^*)^n Z_{\theta'}X_{n\theta'}R_1^n$$

$$= \mu_{m\alpha,\theta'}\mu_{n,\theta'}Z_{\theta'} = \mu_{m\alpha+n,\theta'}Z_{\theta'}$$

holds for $p \geq 3$ since

$$\mu_{m\alpha+n,\theta'} = \mu_{m\alpha,\theta'}\mu_{n,\theta'},\ \forall\theta' \in GF(p^2)$$

which easily follows from (2.11) for $p \geq 3$, and the additivity of the characters.

Remark 2.15 *For $p = 2$ the group law is not satisfied (see [11]). One has instead a very similar property (modified group law) :*

$$R_\alpha R_{\alpha+1} = R_{\alpha+1} R_\alpha = R_1$$

$$R_\alpha R_1 = R_{\alpha+1} X_{\alpha+1}$$
$$R_{\alpha+1} R_1 = R_\alpha X_\alpha$$
$$R_\alpha^2 = X_{\alpha+1}$$
$$R_{\alpha+1}^2 = X_\alpha$$
$$R_1^2 = X_1$$

The second main result of this paper is the following :

Theorem 2.16 *The set of operators $\{F, R_\theta\}_{\theta \in GF(p^2)}$ defines a set of $p^2 + 1$ MUB's in $\mathbb{C}^{p^2}$.*

Proof : Each R_θ is represented by an unitary Hadamard matrix, and so is F. Due to the group property, $R_\theta^* R_{\theta'} = R_{\theta'-\theta}$ thus is an unitary Hadamard matrix. It remains to show that $R_\theta F^*$ is an unitary Hadamard matrix $\forall \theta \in GF(p^2)$. But we have

$$R_\theta F^* = F^* D_\theta, \quad \forall \theta \in GF(p^2)$$

with D_θ an unitary diagonal matrix, since F diagonalizes all block-circulant matrices with circulant blocks. The product of D_θ with the unitary Hadamard matrix F^* is obviously an unitary Hadamard matrix.
In the case of dimension 2^2 one has instead of the group property that

$$\forall \theta,\ \theta', \quad \exists \theta'' \text{ such that } R_\theta^* R_{\theta'} = R_{\theta'-\theta} X_{\theta''}$$

Since $X_{\theta''}$ has exactly one non-vanishing element (1) on each line and column, the product $R_{\theta'-\theta} X_{\theta''}$ is indeed an unitary Hadamard matrix. □

3 THE CASE $d = p^n$

The case $d = p^n$ with general power n can be treated similarly. There is a notion of block-circulant matrices with block-circulant blocks and building block $p \times p$ matrices which are circulant which generalizes the case $n = 2$. These are diagonalized by the Discrete Fourier Transform F in $\mathbb{C}^{p^n}$ which is

$$F = F_p \otimes F_p \otimes ... \otimes F_p$$

(n times) which is obviously an unitary Hadamard matrix.
The Galois field $GF(p^n)$ is defined through the irreducible polynomial which is of

power n, with coefficients in $\mathbb{F}_p$. Thus elements of the Galois field $GF(p^n)$ are of the form

$$\theta = \sum_{i=0}^{n-1} c_i \alpha^i$$

where $c_i \in \mathbb{F}_p$ and α is a root of the characteristic polynomial.
The characters are

$$\chi(\theta) = \exp\left(\frac{2i\pi}{p}\mathrm{tr}(\theta)\right)$$

where

$$\mathrm{tr}(\theta) = \theta + \theta^p + ... + \theta^{p^{n-1}}$$

For any $\theta \in GF(p^n)$ the operators $X_\theta,\ Z_\theta,\ R_\theta$ are defined in [11] and the R_θ obey a group law (resp. a modified group law) if $p \geq 3$ (resp. $p = 2$).
As previously we have $X_\theta \in \left\{X^{k_1} \otimes X^{k_2} \otimes ... \otimes X^{k_n},\ \text{with } k_j \in \mathbb{F}_p\right\}$ and

$$Z_\theta \in \left\{Z^{k_1} \otimes Z^{k_2} \otimes ... \otimes Z^{k_n}\right\}_{k_i \in \mathbb{F}_p}$$

and

$$R_\theta = \sum_{\theta' \in GF(p^n)} \lambda_{\theta'}^{(\theta)} X_{\theta'}$$

with $\lambda_{\theta'}^{(\theta)}$ of modulus $\frac{1}{\sqrt{p^n}}$. The $\lambda_{\theta'}^{(\theta)}$ are given for $p \geq 3$ similarly to (2.12) by

$$\lambda_{\theta'}^{(\theta)} = p^{-n/2}\chi(2^{-1}\theta^{-1}(\theta')^2) \tag{3.13}$$

All the results of the previous section are easily generalized.

Theorem 3.1 *The unitary Hadamard matrices F, R_θ* for $\theta \in GF(p^n)$ *define a set of $p^n + 1$ MUB's in $\mathbb{C}^{p^n}$.*

4 Weil sums for $d = p^n,\ p \geq 3$

The Weil sums in dimension p^n are the equivalent of the Gauss sums for $d = p$ (p prime number). The characters $\chi(\theta),\ \theta \in GF(p^n)$ replace the powers $\omega^n,\ n \in \mathbb{F}_p$. Usually in the literature (see for example [18]), the Weil sums properties are used to solve the MUB problem. Here, as in [7], we do the converse. In the previous sections we have constructed the $d+1$ bases, and we shall **deduce the Weil sums properties** from this construction.

Theorem 4.1 *Let $p \geq 3$. Then for any $\theta \in GF(p^n)\backslash\{0\}$ and any $\theta' \in GF(p^n)$ we have*

$$\left|\sum_{\theta'' \in GF(p^n)} \chi(\theta \cdot (\theta'')^2 + \theta' \cdot \theta'')\right| = \sqrt{p^n} \tag{4.14}$$

Proof : The matrix elements of a given row in F are of the form

$$\frac{1}{\sqrt{p^n}}\chi(\theta' \cdot \theta'')_{\theta'' \in GF(p^n)}$$

for some $\theta' \in GF(p^n)$. Since

$$R_\theta = \frac{1}{\sqrt{p^n}} \sum_{\theta'' \in GF(p^n)} \chi((2\theta)^{-1} \cdot (\theta'')^2) X_{\theta''}$$

the matrix elements of the first column of the matrices $R_\theta,\ \theta \neq 0$ are of the form

$$\frac{1}{\sqrt{p^n}}\chi(2^{-1}\theta^{-1} \cdot (\theta'')^2)_{\theta'' \in GF(p^n)}$$

where we have used (3.13). But the elements $(2\theta)^{-1}$ when $\theta \in GF(p^n)\setminus\{0\}$ span all $\theta_1 \in GF(p^n)\setminus\{0\}$. We have established that the matrix FR_θ is Hadamard. This implies that all its matrix elements have modulus $p^{-n/2}$. All matrix elements of the first column of FR_θ are thus of the form

$$p^{-n} \sum_{\theta'' \in GF(p^n)} \chi(\theta_1 \cdot (\theta'')^2 + \theta' \cdot \theta'')$$

with $\theta_1 = (2\theta)^{-1}$. Writing that its modulus is $p^{-n/2}$ yields equ. (4.14).

References

[1] Albouy O., Kibler M., *SU_2 nonstandard bases : the case of mutually unbiased bases*, Symmetry, Integrability and Geometry : Methods and Applications, (2007)

[2] Bandyopadhyay S., Boykin P.O., Roychowdhury V., Vatan F., *A new proof of the existence of mutually unbiased bases*, Algorithmica, **34**, 512-528, (2002)

[3] Berndt B. C., Evans R. J., Williams K. S., *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol 21, Wiley, (1998)

[4] Björck G. Saffari B, *New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries*, C. R. Acad. Sci. Paris, **320** Serie 1, (1995), 319-324

[5] Chaturvedi S. *Aspects of mutually unbiased bases in odd-prime-power dimensions*, Phys. Rev. A **65**, 044301, (2002)

[6] Combescure M. *The Mutually Unbiased Bases Revisited*, Contemporary Mathematics, (2007), to appear

[7] Combescure M., *Circulant matrices, Gauss sums and the Mutually Unbiased Bases, I. The prime number case* to appear (2007)

[8] Davis P. J. , *Circulant matrices*, Wiley, (1979)

[9] Hadamard J., *Résolution d'une question relative aux déterminants*, Bull. Sci. Math. **17**, 2460-246 (1893)

[10] Ivanovic I. D. *Geometrical description of quantum state determination* J. Phys. A **14**, 3241-3245, (1981)

[11] Klimov A. B., Muñoz C., Romero J. L., *Geometrical approach to the discrete Wigner function*, arXiv:quant-ph/0605113, (2006)

[12] Klimov A. B., Sanchez-Soto L. L., de Guise H. *Multicomplementary operators via finite Fourier Transform*, Journal of Physics A **38**, 2747–2760 (2005)

[13] Planat M., Rosu H., *Mutually unbiased phase states, phase uncertainties, and Gauss sums*, Eur Phys. J. D **36**, 133-139, (2005)

[14] Schwinger J., *Unitary Operator Bases*, Proc Nat. Acad. Sci. U.S.A. **46**, 560 (1960)

[15] Saffari B., *Quadratic Gauss Sums*, to appear

[16] Turyn R. *Sequences with small correlation*, In *Error correcting codes*, H. B. Mann Ed., Wiley (1968), 195-228

[17] Weyl H., *Gruppentheorie and Quantenmechanik*, Hirzel, Leipzig, (1928)

[18] Wootters W. K., Fields B. D., *Optimal State- Determination by Mutually Unbiased Measurements*, Ann. Phys. **191**, 363-381, (1989)