CUBO A Mathematical Journal
Vol.11, Nº 04, (73–86). September 2009

Circulant Matrices, Gauss Sums and Mutually Unbiased Bases, I. The Prime Number Case

Monique Combescure
Institut de Physique Nucléaire de Lyon (IPNL),
4 rue Enrico Fermi F-69622 Villeurbanne Cedex, France.
email: mcombe@ipnl.in2p3.fr

ABSTRACT

In this paper, we consider the problem of Mutually Unbiased Bases in prime dimension d. It is known to provide exactly $d+1$ mutually unbiased bases. We revisit this problem using a class of circulant $d \times d$ matrices. The constructive proof of a set of $d+1$ mutually unbiased bases follows, together with a set of properties of Gauss sums, and of bi-unimodular sequences.

RESUMEN

En este artículo consideramos el problema de bases insesgadas mutuamente en dimensión prima d. Se sabe cómo obtener exactamente $d+1$ bases insesgadas mutuamente. Revisamos el problema usando una clase de matrices circulantes $d \times d$. La demostración constructiva obtiene un conjunto de $d+1$ bases insesgadas mutuamente junto con un conjunto de propiedades de sumas gausianas y de sucesiones biúnimodulares.

Key words and phrases: *Mutually unbiased bases, circulant matrices, Gauss sums.*

Math. Subj. Class.: *81P68, 15A30, 11T23*

1 Introduction

Mutually Unbiased Bases (MUB's) are a set $\{\mathcal{B}_0, ..., \mathcal{B}_N\}$ of orthonormal bases of $\mathbb{C}^d$ such that the scalar product in $\mathbb{C}^d$ of any vector in $\mathcal{B}_j$ with any vector in $\mathcal{B}_k$, $\forall j \neq k$ is of modulus $d^{-1/2}$. Starting

from the natural base $\mathcal{B}_0$ consiting of vectors $v_1 = (1, 0, ...0),\ v_2 = (0, 1, 0, ..., 0), ..., v_d = (0, 0, ..., 1)$, it is known that this problem reduces to find N unitary Hadamard matrices P_j such that $P_j^* P_k$ is also a unitary Hadamard matrix $\forall j \neq k$. (A unitary matrix is Hadamard if all its entries are of modulus $d^{-1/2}$). The problem has been solved in prime power dimension $d = p^n,\ p, n \in \mathbb{N}, p$ prime, and yields exactly $d+1$ MUB's which is the maximum number of MUB's ([2] and references herein contained).
If d is factorizable in $p_1^{m_1} p_2^{m_2}...$ with $p_i \neq p_j$ prime numbers, it is known that one has at least $N = \min\ p_i^{m_i}$ [5].

In this paper we show that in prime dimension $d = p$, the Discrete Fourier Transform F together with a suitable circulant matrix C allow to construct a set of $d + 1$ MUB's. In addition this construction allows to obtain, as a by-product, a set of properties of Gauss sums of the following form :

$$\left| \sum_{k=0}^{d-1} \exp\left(\frac{2i\pi}{d} \left[\frac{lk(k+1)}{2} + jk \right] \right) \right| = \sqrt{d}, \qquad \forall j \in \mathbb{F}_d, l \in \mathbb{F}_d \text{ coprime with d},\ d \geq 3 \tag{1.1}$$

($\mathbb{F}_d$ is the field of residues modulo d). A direct proof of this property is given in [12]. Similar results on generalized Gauss Sums appear in [1]. The definition of F and of circulant matrices is given below. The natural role played by circulant matrices in this context is a new result. The circulant unitary matrices are known to be in one-to-one correspondence with the bi-unimodular sequences $c = \ (c_1, c_2, ..., c_d)$ [4], namely sequences such that $|c_j| = |(Fc)_j| = 1$, where F is the discrete Fourier transform. Not surprisingly Gauss sums appear naturally in this context, since suitable Gauss sequences are examples of bi-unimodular sequences.
At the end of this paper, we consider the case of non-prime dimension, and show that Gauss sums properties can be deduced in the odd and in the even dimension cases. In a forthcoming work we shall consider the case of prime power dimensions and show that the theory of block-circulant matrices with circulant blocks solve the MUB problem in that case.

A $d \times d$ matrix is Hadamard if all its entries have equal moduli [7], and

$$H^* H = d\ \mathbb{1}$$

Definition 1. *A $d \times d$ matrix H is Hadamard if* $|H_{j,k}|$ is constant $\forall j, k = 1, ..., d$, *and* $H^* H = d\ \mathbb{1}$. *We call H a "unitary Hadamard matrix" if*

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

Definition 2. *A $d \times d$ matrix C is called* **circulant** *[6], and denoted* $\mathrm{circ}(c_0, c_1, ..., c_{d-1})$, *if all its* *rows and columns are successive circular permutations of the first. It is of the form*

$$C = \begin{pmatrix} c_0 & c_{d-1} & . & . & c_1 \\ c_1 & c_0 & . & . & c_2 \\ . & . & . & . & . \\ c_{d-1} & c_{d-2} & . & . & c_0 \end{pmatrix}$$

Proposition 1.1. *(i) The set $\mathcal{C}$ of all $d \times d$ circulant matrices is a commutative algebra.*
(ii) $\mathcal{C}$ is a subset of **normal matrices**
(ii) Let $V = \mathrm{circ}(0, 0, ..., 1)$. Clearly $V^d = \mathbb{1}$. Then C is circular if and only if it commutes with V, and one has for any sequence $c = (c_1, ..., c_d) \in \mathbb{C}^d$, $C = \mathrm{circ}(c_1, ..., c_d)$:

$$C = P_c(V) = c_0 \mathbb{1} + c_{d-1} V + ... + c_1 V^{d-1}$$

where P_c is the polynomial

$$P_c(x) = \sum_{k=0}^{d} c_k x^{-k}$$

Proof : See [6]
For the product of two circulant matrices C, C' (that therefore commute with V), one has

$$VCC' = CVC' = CC'V$$

which establishes that CC' is indeed circulant.

Moreover it is well-known that there is a close link between the circulant matrices and the discrete Fourier transform. Namely the latter diagonalizes all the circulant matrices. The Discrete Fourier Transform is defined by the following $d \times d$ unitary matrix F with matrix elements :

$$F_{j,k} = d^{-1/2} \exp\left(\frac{2i\pi jk}{d}\right), \quad j, k = 0, 1, ..., d-1 \tag{1.2}$$

Proposition 1.2. *(i) The circulant matrix $V = \mathrm{circ}(0, 0, ..., 1)$ is such that*

$$F^* V F = U \equiv \mathrm{diag}(1, \omega, \omega^2, ..., \omega^{d-1})$$

where

$$\omega = \exp\left(\frac{2i\pi}{d}\right) \tag{1.3}$$

(ii) Let $C = \mathrm{circ}(c_0, c_1, ..., c_{d-1})$ be a circulant $d \times d$ matrix. Then

$$F^* C F = \sqrt{d}\ \mathrm{diag}(\hat{c}_0, \hat{c}_{-1}, ..., \widehat{c}_{-(d-1)})$$

where

$$\hat{c}_l = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} c_k \omega^{kl} \tag{1.4}$$

Proof : (i) It is enough to check that v_k, the k-th column vector of F which has components

$$(v_k)_j = \frac{\omega^{jk}}{\sqrt{d}}, \quad j,k = 0,1,...,d-1$$

is eigenvector of V with eigenvalue ω^k, which is immediate since

$$(Vv_k)_j = \frac{\omega^{k(j+1)}}{\sqrt{d}} = \omega^k (v_k)_j$$

(ii) One has (Proposition 1.3(ii))

$$C = \sum_{k=0}^{d-1} c_k V^{-k}$$

Thus

$$F^*CF = \sum_{k=0}^{d-1} c_k (F^*VF)^{-k} = \sum_{k=0}^{d-1} c_k U^{-k} = \mathrm{diag}(d_0, ..., d_{d-1})$$

with

$$d_l = \sum_{k=0}^{d-1} c_k \omega^{-lk} = \sqrt{d}\ \hat{c}_{-l}$$

Lemma 1.3. *For any $k \in \mathbb{N}$, we denote by $[k]$ the rest of the division of k by d. Given any sequence $c = (c_0, ..., c_{d-1}) \in \mathbb{C}^d$ its autocorrelation function obeys*

$$\sum_{k=0}^{d-1} \bar{c}_k c_{[j+k]} = \sum_{l=0}^{d-1} |\hat{c}_l|^2 \omega^{-jl}$$

where the Fourier transform $\hat{c}$ of c has been defined in (1.4).

Proof : For any $j = 0, ..., d-1$, one has

$$\sum_{l=0}^{d-1} |\hat{c}_l|^2 \omega^{-jl} = \frac{1}{d} \sum_{l=0}^{d-1} \omega^{-jl} \sum_{k=0}^{d-1} \bar{c}_k \omega^{-lk} \sum_{k'=0}^{d-1} c_{k'} \omega^{k'l}$$

$$= \sum_{k,k'=0}^{d-1} \bar{c}_k c_{k'} \frac{1}{d} \sum_{l=0}^{d-1} \omega^{l(k'-k-j)} = \sum_{k=0}^{d-1} c_{[j+k]} \bar{c}_k$$

since

$$d^{-1} \sum_{l=0}^{d-1} \omega^{l(k'-j-k)} = \delta_{k',[j+k]}$$

It is known ([4], [13]) that **circulant unitary Hadamard matrices** are in one-to-one correspondance with **bi-unimodular sequences** $c = (c_0, c_1, ..., c_{d-1})$.

Definition 3. *A sequence $c = (c_0, c_1, ..., c_{d-1})$ is called bi-unimodular if one has $|c_j| = |\hat{c}_j| = 1$, $\forall j = 1, ..., d$, where $\hat{c}_j$ is defined by (1.4).*

Proposition 1.4. *Let* $(c_0, ..., c_{d-1})$ *be a bi-unimodular sequence. Then the circulant matrix* $C = d^{-1/2}\text{circ}(c_0, c_1, ..., c_{d-1})$ *is an unitary Hadamard matrix.*

Proof : This is a standard "if and only if" statement. One uses Lemma 1.5 :

$$\sum_{k=0}^{d-1} \bar{c}_k c_{[j+k]} \sum_{l=0}^{d-1} |\hat{c}_l|^2 \omega^{-jl}$$

But since $|\hat{c}_l| = 1,\ \forall l = 0, ..., d-1$, the RHS is simply $d\delta_{j,0}$, and therefore

$$\sum_{k=0}^{d-1} \bar{c}_k c_{[k+j]} = d\ \delta_{j,0}$$

which proves the unitarity of the circulant Hadamard matrix C.

In all that follows we call indifferently F or P_0 the discrete Fourier transform.

In [8], the authors introduce for any dimension d being the power of a prime number a set of operators called "rotation operators" which can be viewed as "circulant matrices" (this property is however not put forward explicitely by the authors). In this paper, restricting ourselves to the **prime number case**, we show that these operators can be used to define a set of $d+1$ Mutually Unbiased Bases in dimension d.

Mutually Unbiased bases are extensively studied in the framework of Quantum Information Theory. They are defined as follows :

Definition 4. *A set* $\{B_1, B_2, ..., B_m\}$ *of orthonormal bases of* $\mathbb{C}^d$ *is called MUB if for any vector* $b_j^{(k)} \in B_k$ *and any* $b_{j'}^{(k')} \in B_{k'}$ *one has*

$$|b_j^{(k)} \cdot b_{j'}^{(k')}| = d^{-1/2},\ \forall k \neq k' = 1, ..., m,\ \forall j, j' = 1, ..., d$$

where the dot represents the Hermitian scalar product in $\mathbb{C}^d$.

Remark 1.5. *It is trivial to show that if the orthonormal bases* B_k *are the column vectors of an unitary matrix* A_k*, then the property that must satisfy the* A_k*'s in order that* $\{\mathbb{1}, B_1, ..., B_m\}$ *are MUB's is that all* $A_k,\ k = 1, ..., m$ *and* $A_k^* A_{k'},\ k \neq k' = 1, ..., m$ *are unitary Hadamard matrices. Namely if* $u_j,\ v_k$ *are column vectors for unitary matrices* $A,\ A'$ *respectively, then*

$$u^j \cdot v^k = (A^* A')_{j,k}$$

Thus **unitary Hadamard matrices** *play a major role in the MUB problem.*

It is known that the maximum number of MUB's in any dimension d is $d+1$, and that this number is attained if $d = p^m$, p being a prime number. In this paper, restricting ourselves to

$m = 1$, we revisit the proof of this property, using circulant matrices introduced by [8]. We then show that it implies beautiful properties of Gauss sums, namely the following ([12]) :

Proposition 1.6. *Let $d \geq 3$ be an odd number. Then $\forall k = 1, ..., d-1$ coprime with d the sequences*

$$g^{(k)} := \left(\exp\left(\frac{i\pi kj(j+1)}{d} \right) \right)_{j=0,\dots,d-1} \tag{1.5}$$

are bi-unimodular. Thus (1.1) holds true.

This property will appear as a subproduct of our study of MUB's for d a prime number ≥ 3 via the circulant matrices method. As stressed above, the link between circulant matrices and bi-unimodular sequences is well established. What is new here is the fact that the MUB problem via a circulant matrix method allows to recover the bi-unimodularity of Gauss sequences. The crucial role played by the Gauss sequence is due to the crucial role played by the Discrete Fourier Transform (or in other therms the Fourier-Vandermonde matrices) in the MUB problem for prime numbers. Let us introduce it now explicitely.

It is known since Schwinger ([11]) that a simple toolbox of unitary $d \times d$ matrices sometimes refered to as "generalized Pauli matrices" U, V allows to find MUB's. U, V generate the discrete Weyl-Heisenberg group [14]. Denote by ω the primitive root of unity (1.3). The matrix U is simply

$$U = \mathrm{diag}(1, \omega, \omega^2, ..., \omega^{d-1})$$

which generalizes the Pauli matrix σ_z to dimensions higher than two. The matrix V generalizes σ_x :

$$V = \mathrm{circ}(0, 0, ..., 1) = \begin{pmatrix} 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 \\ 1 & 0 & 0 & . & . & 0 \end{pmatrix}$$

Then one has the following result :

Theorem 1.7. *(i) The U, V matrices obey the ω-commutation rule :*

$$VU = \omega UV$$

(ii) The Discrete Fourier Transform matrix $P_0 = F$ defined by (1.2), namely

$$P_0 = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & 1 & . & . & 1 \\ 1 & \omega & \omega^2 & . & . & \omega^{d-1} \\ 1 & \omega^2 & \omega^4 & . & . & \omega^{2(d-1)} \\ . & . & . & . & . & . \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & . & . & \omega^{(d-1)(d-1)} \end{pmatrix}$$

diagonalizes V, namely

$$V = P_0 U P_0^* = P_0^* U^* P_0$$

(iii) One has $P_0^4 = \mathbb{1}$

(ii) is simply Proposition 1.4(i). For the proof of (iii) reminiscent to the properties of continuous Fourier transform, it is enough to check that

$$P_0^2 = W = \begin{pmatrix} 1 & 0 & 0 & 0 & . & . & 0 \\ 0 & 0 & 0 & 0 & . & . & 1 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 1 & 0 & . & . & 0 \\ 0 & 1 & 0 & 0 & . & . & 0 \end{pmatrix}$$

Thus $W = \mathbb{1}$ in dimension $d = 2$, and $W^2 = \mathbb{1}, \quad \forall d \geq 3$.

In [5] we have shown that for d odd one can add to the general toolbox of unitary Schwinger matrices $U,\ V$ a diagonal matrix D of the form

$$D = \mathrm{diag}(1, \omega, \omega^3, ..., \omega^{k(k+1)/2}, ..., 1)$$

so that the MUB problem for odd prime dimension reduces to properties of $U,\ V,\ D$, and that certain properties of quadratic Gauss sums follow as a by-product.

2 The d=2 Case

We have $U = \sigma_z$ and $V = \sigma_x$, $\sigma_z,\ \sigma_x$ being the usual Pauli matrices. Since $UV = \sigma_y$, finding MUB's in dimension $d = 2$ amounts to diagonalize $\sigma_x,\ \sigma_y$. One has :

$$\sigma_x = P_0 \sigma_z P_0^*$$
$$\sigma_y = P_1 \sigma_z P_1^*$$

with

$$P_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

P_1 is circulant.

Proposition 2.1. *The set $\{\mathbb{1}, P_0, P_1\}$ defines three MUB's in dimension 2.*

Since the matrices $P_0,\ P_1$ are trivially unitary Hadamard matrices, it is enough to check that $P_0^* P_1$ is itself a unitary Hadamard matrix, which holds true since

$$P_0^* P_1 = \frac{e^{i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -i & -i \end{pmatrix}$$

3 The Prime Dimension $d \geq 3$

d being prime, we denote by $\mathbb{F}_d$ the Galois field of integers mod d.
Let us recall the definition of the "rotation operator" of [8], which, as already stressed in nothing but a **circulant matrix** in the odd prime dimension d.

Definition 5. *Define R as an unitary operator commuting with V and diagonalizing VU.*

Proposition 3.1. *(i) R is a circulant matrix.*
(ii) R^k is also circulant $\forall k \in \mathbb{Z}$.

This follows from Proposition 1.3.

Therefore we are led to consider a subclass of circulant matrices that are unitary. They must satisfy :
$\forall k = 0, ..., d-1 \quad |c_k| = d^{-1/2}$ and
$\forall k = 1, ..., d-1 \quad \sum_{j=0}^{d-1} \bar{c}_j c_{[d-k+j]} = 0$ (orthogonality condition).

Now it remains to show that such a matrix R exists. In [5] we have constructed a unitary matrix P_1 that diagonalizes VU. It is defined as

$$P_1 = D^{-1} P_0$$

for any d odd integer (not necessarily prime).
We have established the following result :

Proposition 3.2. *(i) For any odd integer d, the matrix $P_0^* P_1$ is a unitary Hadamard matrix.*
(ii) For $d \geq 3$ odd integer, let $P_k := D^{-k} P_0$. Then $P_0^* P_k$ is a unitary Hadamard matrix for all k coprime with d.
(iii) The matrix D defined above is such that

$$|\mathrm{Tr} D^k| = \sqrt{d}, \ \forall k \in \mathbb{F}_d \text{ coprime with } d$$

For the simple proof of this result see [5]. (iii) is a simple consequence of (i) and(ii). Namely the eigenvector of VU belonging to the eigenvalue 1 has components

$$v_j = d^{-1/2} \omega^{-\frac{j(j+1)}{2}}$$

Since $P_0^* P_1$ is unitary Hadamard matrix, the element of $P_0^* P_1$ of the first row and first column is simply

$$d^{-1} \sum_{j=0}^{d-1} \omega^{-\frac{j(j+1)}{2}}$$

and since its modulus must be $d^{-1/2}$ we obtain (iii) for $k = 1$. The proof for any k coprime with d can be obtained similarly using (ii).

The "problem" is that P_1 is not circulant. However the circulant matrix R is obtained from P_1 by multiplying the kth column vector of P_1 by a phase which is

$$\omega^{-\frac{k(k-1)}{2}}$$

This operation preserves the fact that it is unitary and that it diagonalizes VU. We thus have :

$$VU = P_1 U P_1^* = RUR^* \tag{3.1}$$

Proposition 3.3. *Let R be the matrix :*

$$R = d^{-1/2}\text{circ}\ (1, \omega^{-1}, \omega^{-3}, ..., \omega^{-k(k+1)/2}, ..., 1)$$

It is a unitary Hadamard matrix.

Proof : By construction it is a unitary Hadamard matrix, since P_1 is. To prove the fact that it is circulant, it is enough to know that

$$(P_1)_{j,k} = d^{-1/2}\omega^{jk-\frac{j(j+1)}{2}}$$

thus

$$R_{jk} = d^{-1/2}\omega^{jk-\frac{j(j+1)}{2}-\frac{k(k-1)}{2}} = d^{-1/2}\omega^{-\frac{(j-k)(j-k+1)}{2}} \tag{3.2}$$

since

$$jk - \frac{j(j+1)}{2} - \frac{k(k-1)}{2} = -\frac{(j-k)(j-k+1)}{2}$$

Thus all column vectors are obtained from the first by the circularity property.

Furthermore the R^k have the property that they diagonalize $V^k U$, $\forall k = 1, ..., d-1$:

Theorem 3.4. *(i) $R = \alpha P_0 D P_0^*$ where $\alpha := d^{-1/2}\sum_{k=0}^{d-1}\omega^{-k(k+1)/2}$ is a complex number of modulus 1.*
(ii) $R^d = \alpha^d \mathbb{1}$ where $\mathbb{1}$ denotes the unity $d \times d$ matrix.
(iii)

$$R^k U (R^*)^k = V^k U,\ \forall k = 0, ..., d$$

The proof is extremely simple :
(i) We have shown that $c_j = \omega^{\frac{-j(j+1)}{2}}$ is a bi-unimodular sequence, thus α is a complex number of modulus one. Moreover from Proposition 1.4 (ii), the unitary matrix $R = d^{-1/2}\text{circ}(c_j)$ is such that

$$\hat{R} = P_0^* R P_0 = \text{diag}(\hat{c}_{-k})$$

But

$$\hat{c}_{-k} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-jk-\frac{j(j+1)}{2}} \alpha \omega^{\frac{k(k+1)}{2}}$$

since

$$\sum_{j=0}^{d-1} \omega^{-\frac{j(j+1)}{2}} = \sum_{j=0}^{d-1} \omega^{-\frac{(j+k)(j+k+1)}{2}} = \sum_{j=0}^{d-1} \omega^{-jk-\frac{j(j+1)}{2}-\frac{k(k+1)}{2}}$$

Therefore

$$\hat{R} = \alpha \mathrm{diag}(\omega^{\frac{k(k+1)}{2}}) = \alpha D$$

(ii) is simply a consequence of (i) since $D^d = \mathbb{1}$.
(iii) is obtained by recurrence. Namely it is true for $k = 1$ by (3.1). For $k \geq 2$ one has :

$$R^k U (R^*)^k = R V^{k-1} U R^* = V^{k-1} R U R^*$$

since R commutes with V. But

$$V^{k-1} R U R^* = V^{k-1}(VU) = V^k U$$

There is a direct link between the matrices P_k that diagonalize VU^k and the R^k that diagonalize $V^k U$:

Theorem 3.5. *α being the complex number of modulus one defined above, we have for any $k = 0, ..., d-1$*

$$P_k = \alpha^k P_0^* R^{-k} P_0^2$$

Proof : In [5] we have proven that $P_k = D^{-k} P_0$ diagonalizes VU^k. But one has

$$D^{-k} = D^{d-k} = \alpha^{k-d} P_0^* R^{d-k} P_0$$

so the result follows immediately.

Corollary 3.6. *For any $k = 1, ..., d-1$, R^k is a unitary Hadamard circulant matrix when $d \geq 3$ is prime.*

Proof : R^k is circulant and unitary since R is. Therefore we have only to check that it is Hadamard. We have :

$$R^{-k} = \alpha^{-k} P_0^2 P_0^* P_k P_0^2$$

But we recall that P_0^2 equals the permutation matrix W. Thus all matrix elements of R^k equal, up to a phase, some matrix elements of $P_0^* P_k$. But we have established in [5] that the matrix $P_0^* P_k$ is unitary Hadamard $\forall k = 1, ..., d-1$, thus all its matrix elements are equal in modulus to $d^{-1/2}$. This completes the proof.

Now we show how this property of the matrix R reflects itself in Gauss sums properties.

Proposition 3.7. *(i) Let d be an odd prime. Then for any $k = 1, 2, ..., d-1$ R^k is an unitary Hadamard matrix if and only if one has*

$$\left|\sum_{j=0}^{d-1} \exp\left(\frac{i\pi}{d}[kj^2 + j(k+2m)]\right)\right| = \sqrt{d},\ \forall m = -d+1, ..., d-1$$

(ii) Under the same conditions R^k is a unitary Hadamard matrix if and only if

$$\left|\sum_{j=0}^{k-1} \exp\left(\frac{i\pi}{k}dj^2 + (k+2m)j\right)\right| = \sqrt{k}$$

Proof : Since $R^k = \alpha^k P_0 D^k P_0^*$, the matrix elements of R^k are

$$(R^k)_{m,l} = \frac{\alpha^k}{d}\sum_{j=0}^{d-1} \omega^{j(m-l)+k\frac{j(j+1)}{2}}$$

Since R^k is circulant, it is unitary Hadamard matrix if and only if the matrix elements of the first column (l=0) are of modulus $d^{-1/2}$, thus if and only if

$$\left|\sum_{j=0}^{d-1} \exp\left(\frac{i\pi}{d}[kj^2 + j(k+2m)]\right)\right| = \sqrt{d}$$

which proves (i).
(ii) Using the reciprocity theorem for Gauss sums ([3]), we have for all integers a, b with $ac \neq 0$ and $ac + d$ even that the quantity

$$S(a,b,d) := \sum_{j=0}^{d-1} \exp\left(\frac{\pi i}{d}(aj^2 + bj)\right)$$

obeys

$$S(a,b,d) = \left|\frac{d}{a}\right|^{1/2} \exp\left(\frac{\pi i}{4}[\mathrm{sgn}(ad) - b^2/ad]\right) S(-d,-b,a)$$

Thus $|S(a,b,d)| = \sqrt{d}$ if and only if $|S(-d,-b,a)| = \sqrt{a}$. Applying if to $a = k = 1, ..., d-1$ coprime with d and $b = 2m + k$, and taking the complex conjugate yields the result. Namely $ad + b = dk + k + 2m$ is even for all $k = 0, ..., d-1$ since d is odd.

Corollary 3.8. *Let $d \geq 3$ be a prime number. Then for any $k = 1, 2, ..., d-1$ the sequences*

$$g^{(k)} := \left(\omega^{k\frac{j(j+1)}{2}}\right)_{j=0,\dots,d-1}$$

are bi-unimodular.

Remark 3.9. *This property is known, but has an extension in the non prime odd dimensions. See next section.*

It is known that the diagonalization of $VU^k,\ k=0,...,d-1$ provides a set of $d+1$ MUB's for a prime p. Here we show that the same is true with the diagonalization of $V^kU,\ k=0,...,d-1$.

Theorem 3.10. *Let $d \geq 2$ be a prime dimension. Then the orthonormal bases defined by the unitary matrices $\mathbb{1}, P_0, R, R^2, ..., R^{d-1}$ provide a set of $d+1$ MUB's.*

Proof : For $d=2$ this has been already proven in Section 2. For $d \geq 3$ (thus odd, since it is prime), it is enough to check that :
(i) $P_0, R^k,\ k=1,...,d-1$ are unitary Hadamard matrices, together with
(ii) $P_0^* R^k,\ k=1,...,d-1$ and $(R^{k'})^* R^k,\ 1 \leq k' < k \leq d-1$.
Since (i) has been already established, it remains to show (ii). Since $R^k = \alpha^k P_0 D^k P_0^*$ we have

$$P_0^* R^k = \alpha^k D^k P_0^*$$

which is trivially an unitary Hadamard matrix (since P_0 is, α is of modulus 1 and D is diagonal and unitary). For $(R^*)^{k'} R^k$ it is trivial since

$$(R^*)^{k'} R^k = R^{k-k'}$$

which is unitary Hadamard for any $k \neq k',\ k, k' = 1, ..., d-1$.

4 The Case of Arbitrary Odd Dimension

We have shown in [5] that for any odd dimension $d \geq 3$ the matrices $P_0^* P_k$ is an unitary Hadamard matrix **provided k is co-prime with d**. This can be transfered to a similar property for the matrix R^{-k}, and therefore to the bi-unimodularity of the sequence $g^{(k)}$ defined in (1.5).

Proposition 4.1. *Let $d \geq 3$ be an odd integer, and k be any number coprime with d. Then*
(i) R^k is an unitary Hadamard matrix.
(ii) The sequence $g^{(k)}$ is bi-unimodular.
(iii) Both properies are equivalent.

This implies Proposition 1.10.

Theorem 4.2. *Let d be odd and $k > 2$ be the smallest divisor of d. Then the orthonormal bases defined by the unitary matrices $\left\{\mathbb{1}, F, R, R^2, ..., R^{k-1}\right\}$ provide a set of $k+1$ MUB's in dimension d.*

5 The Case of Arbitrary Even Dimension

Let d be even and

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

We denote $\omega^{1/2} = e^{i\pi/d}$. One defines the Discrete Fourier Transform F as usually.
The theory of circulant matrices is also pertinent for even dimensions $d \geq 4$. Namely in that case the matrix

$$D' = \mathrm{diag}(1, \omega^{-1/2}, ..., \omega^{-k^2/2}, ..., \omega^{-1/2})$$

has been shown ([5]) to be such that the unitary Hadamard matrix

$$P_1 = D'F$$

diagonalizes VU. But the circulant matrix R obtained by multiplying the k-th column vector of P_1 by $\omega^{-k^2/2}$ also diagonalizes VU :

Proposition 5.1. *The circulant matrix whose matrix elements are*

$$R_{j,k} = \frac{1}{\sqrt{d}} \omega^{-(j-k)^2/2}$$

diagonalizes VU and is such that F^*R is an unitary Hadamard matrix.

Proof :

$$(P_1)_{j,k} = \frac{1}{\sqrt{d}} \omega^{-\frac{j^2}{2} + jk}$$

thus

$$R_{j,k} = \frac{1}{\sqrt{d}} \omega^{-\frac{(j-k)^2}{2}}$$

$R_{j,k}$ only depends on $j-k$ thus is circulant (and unitary). Therefore it is diagonalized by F, namely there exists an unitary diagonal matrix D'' such that

$$F^*RF = D''$$

Again this implies that F^*R is an unitary Hadamard matrix.

Corollary 5.2. *(i) The orthonormal bases defined by the unitary matrices $\{\mathbb{1}, F, R\}$ provide a set of 3 MUB's in arbitrary even dimension d.*
(ii) One has the following property of quadratic Gauss sums for d even :

$$\left| \sum_{k=0}^{d-1} \exp\left(\frac{ik^2\pi}{d}\right) \right| = \sqrt{d}$$

Remark 5.3. *R^2 is circulant, unitary, but not Hadamard. Thus it does not help to find more than 3 MUB's in even dimensions. In dimensions $d = 2^n$, another method is necessary to prove that there exists $d+1$ MUB's.*

Acknowledgments : It is a pleasure to thank B. Helffer for his interest in this work, and to Bahman Saffari for interesting discussions and for providing to me reference [12].

Received: August 2008. Revised: September 2008.

References

[1] Albouy, O. and 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. and Vatan, F., *A new proof of the existence of mutually unbiased bases*, Algorithmica, **34**, 512-528, (2002)

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

[4] Bjrck, G. and 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] Combescure, M., *The Mutually Unbiased Bases Revisited*, Contemporary Mathematics, (2007), to appear

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

[7] Hadamard, J., *Rsolution d'une question relative aux dterminants*, Bull. Sci. Math. **17**, 2460-246 (1893)

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

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

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

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

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

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

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