A simple lecture on MUBs

M. D. Sheppeard

Abstract

Schwinger introduced the notion of a set of mutually unbiased bases for quantum measurement. Maximal sets are known for prime power dimensions, but in other dimensions d very little is known, even for $d = 6$. This is a concrete introduction to MUBs, describing the maximal sets for $d \leq 6$.

In quantum measurements with d possible outcomes, one is interested in the case where every outcome is equally likely [1]. We consider one preparation basis together with a measurement basis. Define a pair of *mutually unbiased bases* in d dimensions [2][3] to be two bases V and W for $\mathbb{C}^d$ such that for every $v \in V$ and $w \in W$,

$$|\langle v \cdot w \rangle| = \frac{1}{\sqrt{d}}. \tag{1}$$

Spin in $d = 2$ is the first example given below. For $d = 1$, any phase $\theta \in \mathbb{C}$ is mutually unbiased with respect to any other.

A basis will be written as a set of d column vectors. Such a basis B_1 is equivalent to any other matrix B_2 obtained through arbitrary phase multiples on the columns, and arbitrary permutations of the columns are permitted. That is,

$$B_2 \simeq B_1 C \tag{2}$$

for a diagonal phase matrix C. We usually begin with the standard basis, the identity matrix I_d. It turns out that a second special choice is the quantum Fourier matrix F_d, defined by the examples below. Observe that any basis B_i that is mutually unbiased with respect to I_d must have entries that are complex phases, up to the normalisation factor $\sqrt{d}^{-1}$, since (1) picks out a single entry at a time. These are known as generalised Hadamard matrices.

The vectors in a basis are the eigenvectors for some measurement operators in dimension d. One is interested in finding the largest possible set of bases such that every basis is mutually unbiased with respect to every other. We call this a set of MUBs.

$d = 2$:

A maximal set of mutually unbiased bases in $d = 2$ is the set of eigenvectors for the three Pauli spin matrices

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

This is the triplet of matrices $\{I_2, F_2, R_2\}$, where

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad R_2 \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{4}$$

For each matrix, check that each column is orthogonal to every other column in the basis.

It turns out that $d+1$ is the maximal number of MUBs in any dimension d.

$d = 3$:

Let $\omega = \exp(2\pi i/3)$ be the primitive cubed root of unity, and $\overline{\omega}$ its complex conjugate. A set of 4 mutually unbiased bases is given by I_3, the Fourier matrix [4]

$$F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \overline{\omega} \\ 1 & \overline{\omega} & \omega \end{pmatrix}, \tag{5}$$

and the two circulants

$$R_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \omega & 1 \\ 1 & 1 & \omega \\ \omega & 1 & 1 \end{pmatrix}, \quad {R_3}^{-1} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \overline{\omega} \\ \overline{\omega} & 1 & 1 \\ 1 & \overline{\omega} & 1 \end{pmatrix}. \tag{6}$$

$d = 4$:

As for $d = 2$ and $d = 3$, there is a maximal set of $d+1 = 5$ mutually unbiased bases in dimension 4. It is still possible to find these by hand, using only the fourth roots of unity. Along with I_4, we have

$$F_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad B_1 = \frac{1}{2} \begin{pmatrix} i & i & -1 & 1 \\ i & i & 1 & -1 \\ -1 & 1 & -i & -i \\ 1 & -1 & -i & -i \end{pmatrix}, \tag{7}$$

$$B_2 = \frac{1}{2} \begin{pmatrix} 1 & i & 1 & -i \\ i & -1 & -i & -1 \\ i & 1 & i & -1 \\ -1 & i & 1 & i \end{pmatrix}, \quad B_3 = \frac{1}{2} \begin{pmatrix} i & -1 & i & -1 \\ -1 & -i & 1 & i \\ i & 1 & i & 1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

$d = p^r$ an odd prime power:

When $d = p^r$ for an odd prime p, there exists a maximal set of $d+1$ mutually unbiased bases [2]. Let $\omega_d = \exp(2\pi i/d)$. The construction of a maximal set of MUBs in $d = p^r$ uses the finite field $\mathbb{F}_{p^r}$. For $z \in \mathbb{F}_{p^r}$, the *trace* in $\mathbb{F}_p$ is defined by [5]

$$\mathrm{tr}(z) = z + z^p + \cdots + z^{p^{k-1}}. \tag{8}$$

Along with the standard basis I_d, there are d bases B_n for $n \in \{0, 1, \cdots, d-1\}$, defined by the vectors $v_{n,m}$ with $m \in \{0, 1, \cdots, d-1\}$ [6], whose entries are

$$(v_{n,m})_x = \frac{1}{\sqrt{d}}(\omega_p)^{\mathrm{tr}(nx^2+mx)} \tag{9}$$

for $x \in \{0, 1, \cdots, d-1\}$. The quantum Fourier basis F_d is B_0. For $f(x) = nx^2 + mx$, the phases in $v_{n,m}$ are the canonical additive character $\chi_1(f(x))$ for $\mathbb{F}_d$. That these bases are all mutually unbiased follows directly from [5][7],

Theorem 0.1. *If χ_1 is the canonical additive character for $\mathbb{F}_d$ with $d = p^r$ an odd prime power, and $f(x) = ax^2 + bx$ with $a \neq 0$, then*

$$|\sum_{y \in \mathbb{F}_d} \chi_1(f(y))| = \sqrt{d}$$

Proof: The multiplicative quadratic character η on ${\mathbb{F}_d}^*$ is defined by $\eta(y) = 1$ if y is a square and $\eta(y) = -1$ otherwise. For an additive character χ of $\mathbb{F}_d$, the quadratic Gaussian sum is

$$G(\eta, \chi) = \sum_{y \in {\mathbb{F}_d}^*} \eta(y)\chi(y). \tag{10}$$

Observe that $\langle v_{n,m} | v_{s,t} \rangle$ has the form $\sum \chi_1(f(x))$ for $a \neq 0$ whenever $n \neq s$. Theorem 5.33 of [5] then evaluates

$$\sum_{x \in \mathbb{F}_d} \chi_1(f(x)) = \chi_1(\frac{b^2}{4a}) \cdot \eta(a) \cdot G(\eta, \chi_1), \tag{11}$$

which has the same norm as $G(\eta, \chi_1)$. Theorem 5.15 of [5] gives the values of $G(\eta, \chi_1)$, equal to $(-1)^{r-1}\sqrt{d}$ if $p = 1$ mod 4, and $(-1)^{r-1} i^r \sqrt{d}$ for $p = 3$ mod 4. That the norms are all $\sqrt{d}$ is a basic property of Gaussian sums $G(\psi, \chi)$ for any non trivial multiplicative character ψ and non trivial χ.

That is, as explained in the historical paper by Weil [8],

$$|G(\psi,\chi)|^2 = \overline{G(\psi,\chi)}G(\psi,\chi) \tag{12}$$

$$= \sum_{y\in\mathbb{F}_d{}^*}\sum_{z\in\mathbb{F}_d{}^*} \overline{\psi(y)\chi(y)}\psi(z)\chi(z) \tag{13}$$

$$= \sum_y\sum_z \psi(y^{-1}z)\chi(z-y) \tag{14}$$

$$= \sum_y\sum_w \psi(w)\chi(y(w-1)) \tag{15}$$

$$= \psi(1)(d-1) + (-\psi(1))(-\chi(0)) \tag{16}$$

$$= \psi(1)d, \tag{17}$$

with the second last step splitting the cases $w = 1$ and $w \neq 1$, noting that $\sum_y \chi(y) = 0$ in $\mathbb{F}_d$ and similarly for ψ in $\mathbb{F}_d{}^*$. Gaussian sums are like Fourier coefficients for $\chi(x)$ as a series in all the multiplicative characters.

$d = 6$:

The maximal number of MUBs for $d = 6$ is unknown. A special case of Zauner's conjecture [9] suggests that there are only 3 MUBs in a maximal set. Once again, let $\omega = \exp(2\pi i/3)$. Using $F_6 = F_3 \otimes F_2$,

$$F_6 = \frac{1}{\sqrt{6}}\begin{pmatrix} 1 & \omega & \overline{\omega} & \omega & \overline{\omega} & 1 \\ 1 & \overline{\omega} & \omega & \overline{\omega} & \omega & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \overline{\omega} & -\omega & -\overline{\omega} & -1 \\ 1 & \overline{\omega} & \omega & -\overline{\omega} & -\omega & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix} \tag{18}$$

one finds a third basis

$$R_6 = \frac{1}{\sqrt{6}}\begin{pmatrix} 1 & \overline{\omega} & 1 & \overline{\omega} & 1 & 1 \\ 1 & 1 & \overline{\omega} & 1 & \overline{\omega} & 1 \\ \overline{\omega} & 1 & 1 & 1 & 1 & \overline{\omega} \\ i & i\overline{\omega} & i & -i\overline{\omega} & -i & -i \\ i & i & i\overline{\omega} & -i & -i\overline{\omega} & -i \\ i\overline{\omega} & i & i & -i & -i & -i\overline{\omega} \end{pmatrix} \tag{19}$$

by noting that a vector $v \in R_6$ must be of norm $\sqrt{6}^{-1}$ in order to be mutually unbiased with respect to the vector $(1,1,1,1,1,1)$. There are few such vectors, using only 12th roots of unity. Grassl has shown [10] that there are only 48 vectors in total that are mutually unbiased with respect to I_6 and F_6.

The $d = 6$ MUBs are a special case of the following observation [6]. If d has a prime factorisation ${p_1}^{k_1}{p_2}^{k_2}\cdots{p_r}^{k_r}$, let

$$N_l(d) \equiv \min \{N({p_i}^{k_i})\}_{i=1,2,\cdots,r}$$

where $N(n)$ is the maximal number of MUBs in dimension n. This $N_l(d)$ defines a lower bound for the maximal number in dimension d, since one can mix together a choice of $N_l(d)$ bases for each prime power factor ${p_i}^{k_i}$ using tensor products. For example, when $d = 12$ we can choose the 4 bases I_{12}, $F_4 \otimes B_1$, $R_3 \otimes B_2$ and ${R_3}^{-1} \otimes B_3$.

So in any dimension $d \geq 2$, there are at least 3 MUBs. As for $d = 2$, one such set is given by the eigenvectors of three operators σ_X, σ_Z and σ_{XZ}, where σ_X is the cyclic permutation $(23 \cdots d1)$ and σ_Z is the phase diagonal with entries $D_i = (\omega_d)^i$.

The difficulty of Zauner's conjecture is in showing that F_d is an essential element of a maximal set of MUBs. One can always obtain the vector $(1, 1, \cdots, 1)$ in one basis B through a diagonal transformation DB_i on all bases B_i in a set, and then set one entry in each column to 1 with a phase multiple, but this still leaves $(d-1)^2$ entries in B.

Observe that all the concrete examples above may be written in the form DF_d for a phase diagonal D. It is clear that this transformation D on an arbitrary basis preserves the orthogonality relations from F_d. For $d = 3$ one creates bases using the diagonals $(1, 1, \omega)$ and $(1, 1, \overline{\omega})$, and in $d = 4$ we may use

$$(i, i, -1, 1), \quad (1, i, i, -1), \quad (i, -1, i, 1).$$

References

[1] J. Schwinger, Proc. Nat. Acad. Sci. U.S.A. **46** (1960) 570.

[2] W. K. Wootters and B. D. Fields, 1989, Annal. Phys. **191** (1989) 363.

[3] J. Lawrence, Phys. Rev. A **84** (2011) 022338.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 2000, Cambridge.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, 1997, Cambridge.

[6] A. Klappenecker and M. Rotteler, arXiv:quant-ph/0309120.

[7] M. N. Huxley, *Area, Lattice Points and Exponential Sums*, 1996, Oxford.

[8] A. Weil, Bull. Amer. Math. Soc. **55** (1949) 497.

[9] G. Zauner, Thesis, University of Vienna, 1999.

[10] M. Grassl, arXiv:quant-ph/0406175.