Constructions of Mutually Unbiased Bases

Andreas Klappenecker[1] and Martin Rötteler[2]

[1] Department of Computer Science,
Texas A&M University, College Station, TX 77843-3112, USA
klappi@cs.tamu.edu
[2] Department of Combinatorics and Optimization,
University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1
mroetteler@math.uwaterloo.ca

Abstract. Two orthonormal bases B and B' of a d-dimensional complex inner-product space are called mutually unbiased if and only if $|\langle b|b'\rangle|^2 = 1/d$ holds for all $b \in B$ and $b' \in B'$. The size of any set containing pairwise mutually unbiased bases of $\mathbb{C}^d$ cannot exceed $d + 1$. If d is a power of a prime, then extremal sets containing $d+1$ mutually unbiased bases are known to exist. We give a simplified proof of this fact based on the estimation of exponential sums. We discuss conjectures and open problems concerning the maximal number of mutually unbiased bases for arbitrary dimensions.

Key words: Quantum cryptography, quantum state estimation, Weil sums, finite fields, Galois rings.

1 Motivation

The notion of mutually unbiased bases emerged in the literature of quantum mechanics in 1960 in the works of Schwinger [18]. Two orthonormal bases B and B' of the vector space $\mathbb{C}^d$ are called *mutually unbiased* if and only if $|\langle b \,|\, b' \rangle|^2 = 1/d$ holds for all $b \in B$ and all $b' \in B'$. Schwinger realized that no information can be retrieved when a quantum system which is prepared in a basis state from B' is measured with respect to the basis B. A striking application is the protocol by Bennett and Brassard [5] which exploits this observation to distribute secret keys over a public channel in an information-theoretically secure way (see also [4]).

Any collection of pairwise mutually unbiased bases of $\mathbb{C}^d$ has cardinality $d + 1$ or less, see [3, 11, 13, 15, 22]. Extremal sets attaining this bound are of considerable interest. Ivanović showed that the density matrix of an ensemble of d-dimensional quantum systems can be completely reconstructed from the statistics of measurements with respect to $d + 1$ mutually unbiased bases [14]. Furthermore, he showed that the density matrix cannot be reconstructed from the statistics of fewer measurements.

Let $N(d)$ denote the maximum cardinality of any set containing pairwise mutually unbiased bases of $\mathbb{C}^d$. It is known that $N(d) = d + 1$ holds when d is a prime power, see [14, 22, 3]. We derive a simplified proof of this result, which takes advantage of Weil-type exponential sums. We present two different

constructions—both based on Weil sums over finite fields—in the case of odd prime power dimensions. We exploit exponential sums over Galois rings in the case of even prime power dimensions. If the dimension d is not a prime power, then the exact value of $N(d)$ is not known. We discuss lower bounds, conjectures, and open problems in the fourth section.

2 Odd Prime Powers

Let $\mathbb{F}_q$ be a finite field with q elements which has odd characteristic p. Denote the absolute trace from $\mathbb{F}_q$ to the prime field $\mathbb{F}_p$ by $\text{tr}(\,\cdot\,)$. Each nonzero element $x \in \mathbb{F}_q$ defines a non-trivial additive character $\mathbb{F}_q \to \mathbb{C}^\times$ by

$$y \mapsto \omega_p^{\text{tr}(xy)},$$

where $\omega_p = \exp(2\pi i / p)$ is a primitive p-th root of unity. All non-trivial additive characters are of this form.

Lemma 1 (Weil sums). *Let $\mathbb{F}_q$ be a finite field of odd characteristic and χ a non-trivial additive character of $\mathbb{F}_q$. Let $p(X) \in \mathbb{F}_q[X]$ be a polynomial of degree 2. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(p(x)) \right| = \sqrt{q}.$$

We refer to [17, Theorem 5.37] or [7, p. 313] for a proof. We will use this lemma in the following constructions of mutually unbiased bases.

Convention. In the following, we will tacitly assume that the elements of $\mathbb{F}_q$ are listed in some fixed order, and this order will be used whenever an object indexed by elements of $\mathbb{F}_q$ appears.

We begin with a historical curiosity. Schwinger introduced the concept of mutually unbiased bases in 1960. However, he did not construct extremal sets of mutually unbiased bases, except in low dimensions, and no further progress was made during the next twenty years. Alltop constructed in 1980 complex sequences with low correlation for spread spectrum radar and communication applications [1]. It turns out that the sequences given by Alltop provide $p + 1$ mutually unbiased bases in dimension p, for all primes $p \geq 5$. Unfortunately, Alltop was not aware of his contribution to quantum physics, and his work was not noticed until recently. Our first construction generalizes the Alltop sequences to prime power dimensions.

Theorem 1. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$. Let B_α denote the set of vectors*

$$B_\alpha = \{b_{\lambda,\alpha} \mid \lambda \in \mathbb{F}_q\}, \qquad b_{\lambda,\alpha} = \frac{1}{\sqrt{q}} \left(\omega_p^{\text{tr}((k+\alpha)^3 + \lambda(k+\alpha))} \right)_{k \in \mathbb{F}_q}.$$

The standard basis and the sets B_α, with $\alpha \in \mathbb{F}_q$, form an extremal set of $q + 1$ mutually unbiased bases of the vector space $\mathbb{C}^q$.

Proof. Notice that B_α is an orthonormal basis because

$$\langle b_{\kappa,\alpha}|b_{\lambda,\alpha}\rangle = \frac{1}{q}\sum_{k\in\mathbb{F}_q}\omega_p^{\mathrm{tr}((\kappa-\lambda)(k+\alpha))}.$$

Indeed, the right hand side equals 0 when $\kappa \neq \lambda$ because the argument $k + \alpha$ ranges through all values of $\mathbb{F}_q$; and equals 1 when $\kappa = \lambda$.

Note that all components of the sequence $b_{\lambda,\alpha}$ have absolute value $1/\sqrt{q}$, hence the basis B_α and the standard basis are mutually unbiased, for any $\alpha \in \mathbb{F}_q$.

By computing the inner product $|\langle b_{\kappa,\alpha}, b_{\lambda,\beta}\rangle|$ for $\alpha \neq \beta$, we see that the terms cubic in k cancel out and, moreover, that the exponent is given by the trace of a quadratic polynomial in k. By Lemma 1 the inner product evaluates to $q^{-1/2}$, hence B_α and B_β are mutually unbiased. $\square$

Remark 1. A remarkable feature of the previous construction is that knowledge of one basis B_α is sufficient because shifting the indices by adding a field element yields the other bases. The construction does not work in characteristic 2 and 3 because in these cases the sets B_α and B_β, with $\alpha \neq \beta$, are not mutually unbiased.

Ivanović gave a fresh impetus to the field in 1981 with his seminal paper [14]. Among other things, he gave explicit constructions of $p + 1$ mutually unbiased bases of $\mathbb{C}^p$, for p a prime. His construction was later generalized in the influential paper by Wootters and Fields [22], who gave the first proof of the following theorem. This proof was recently rephrased by Chaturvedi [9], and an alternate proof was given by Bandyopadhyay et al. [3]. We give a particularly short proof by taking advantage of Weil sums.

Theorem 2. *Let $\mathbb{F}_q$ be a finite field with odd characteristic p. Denote by $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q\}$ the set of vectors given by*

$$v_{a,b} = q^{-1/2}\left(\omega_p^{\mathrm{tr}(ax^2+bx)}\right)_{x\in\mathbb{F}_q}.$$

The standard basis and the sets B_a, with $a \in \mathbb{F}_q$, form an extremal set of $q + 1$ mutually unbiased bases of $\mathbb{C}^q$.

Proof. By definition

$$|\langle v_{a,b}|v_{c,d}\rangle| = \left|\frac{1}{q}\sum_{x\in\mathbb{F}_q}\omega_p^{\mathrm{tr}((c-a)x^2+(d-b)x)}\right|. \tag{1}$$

Suppose that $a = c$. The right hand side evaluates to 1 if $b = d$, and to 0 if $b \neq d$. This proves that B_a is an orthonormal basis. The coefficients of the vector $v_{a,b}$ have absolute value $q^{-1/2}$, hence B_a is mutually unbiased with the standard basis. On the other hand, if $a \neq c$, then the right hand side evaluates to $q^{-1/2}$ by Lemma 1, which proves that the bases B_a and B_c are mutually unbiased. $\square$

Example 1. In dimension 3, this construction yields the bases

$$B_0 = \{v_{0,0}, v_{0,1}, v_{0,2}\} = \{\quad 3^{-1/2}(1,1,1),\, 3^{-1/2}(1,\omega_3,\omega_3^2),\, 3^{-1/2}(1,\omega_3^2,\omega_3)\},$$
$$B_1 = \{v_{1,0}, v_{1,1}, v_{1,2}\} = \{\, 3^{-1/2}(1,\omega_3,\omega_3),\quad 3^{-1/2}(1,\omega_3^2,1),\quad 3^{-1/2}(1,1,\omega_3^2)\},$$
$$B_2 = \{v_{2,0}, v_{2,1}, v_{2,2}\} = \{\, 3^{-1/2}(1,\omega_3^2,\omega_3^2),\quad 3^{-1/2}(1,\omega_3,1),\quad 3^{-1/2}(1,1,\omega_3)\},$$

which form together with the standard basis four mutually unbiased bases.

3 Even Prime Powers

We showed in the last section that extremal sets of $q+1$ mutually unbiased bases exist in dimension q if q is a power of an odd prime. In this section we treat the case when q is a power of two. We cannot use Weil sums because Lemma 1 does not apply in even characteristics. However, it turns out that exponential sums over a finite Galois ring can serve as a substitute.

We recall some elementary facts about finite Galois rings, see [20] for more details. Let $\mathbb{Z}_4$ denote the residue class ring of integers modulo 4. Denote by $\langle 2 \rangle$ the ideal generated by 2 in $\mathbb{Z}_4[x]$. A monic polynomial $h(x) \in \mathbb{Z}_4[x]$ is called *basic primitive* if and only if its image in $\mathbb{Z}_4[x]/\langle 2 \rangle \cong \mathbb{Z}_2[x]$ under the canonical map is a primitive polynomial in $\mathbb{Z}_2[x]$. Let $h(x)$ be a monic basic primitive polynomial of degree n. The ring $\mathrm{GR}(4,n) = \mathbb{Z}_4[x]/\langle h(x)\rangle$ is called the Galois ring of degree n over $\mathbb{Z}_4$.

The construction ensures that $\mathrm{GR}(4,n)$ has 4^n elements. The element $\xi = x + \langle h(x)\rangle$ is of order $2^n - 1$. Any element $r \in \mathrm{GR}(4,n)$ can be uniquely written in the form $r = a+2b$, where $a, b \in \mathcal{T}_n = \{0,1,\xi,\dots,\xi^{2^n-2}\}$. This representation in terms of the Teichmüller set $\mathcal{T}_n$ is convenient, since it allows us to characterize the units of $\mathrm{GR}(4,n)$ as the elements $a + 2b$ with $a \neq 0$.

The automorphism $\sigma\colon \mathrm{GR}(4,n) \to \mathrm{GR}(4,n)$ defined by $\sigma(a+2b) = a^2 + 2b^2$ is called the Frobenius automorphism. This map leaves the elements of the prime ring $\mathbb{Z}_4$ fixed. All automorphisms of $\mathrm{GR}(4,n)$ are of the form σ^k for some integer $k \geq 0$. The trace map $\mathrm{tr}\colon \mathrm{GR}(4,n) \to \mathbb{Z}_4$ is defined by $\mathrm{tr}(x) = \sum_{k=0}^{n-1} \sigma^k(x)$.

Lemma 2. *Keep the notation as above. The exponential sum $\Gamma\colon \mathrm{GR}(4,n) \to \mathbb{C}$ defined by $\Gamma(r) = \sum_{x \in \mathcal{T}_n} \exp(\frac{2\pi i}{4} \mathrm{tr}(rx))$ satisfies*

$$|\Gamma(r)| = \begin{cases} 0 & \text{if } r \in 2\mathcal{T}_n,\ r \neq 0, \\ 2^n & \text{if } r = 0, \\ \sqrt{2^n} & \text{otherwise.} \end{cases}$$

The above lemma is proved in [8, Lemma 3], see also [23]. This lemma will be crucial in the next construction of mutually unbiased bases.

Theorem 3. *Let $\mathrm{GR}(4,n)$ be a finite Galois ring with Teichmüller set $\mathcal{T}_n$. For $a \in \mathcal{T}_n$, denote by $M_a = \{v_{a,b} \,|\, b \in \mathcal{T}_n\}$ the set of vectors given by*

$$v_{a,b} = 2^{-n/2}\left(\exp\left(\frac{2\pi i}{4}\mathrm{tr}(a+2b)x\right)\right)_{x \in \mathcal{T}_n}.$$

The standard basis and the sets M_a, with $a \in \mathcal{T}_n$, form an extremal set of $2^n + 1$ mutually unbiased bases of $\mathbb{C}^{2^n}$.

Proof. By definition,

$$|\langle v_{a,b}|v_{a',b'}\rangle| = \frac{1}{2^n}\left|\sum_{x \in \mathcal{T}_n} \exp\left(\frac{2\pi i}{4}\operatorname{tr}\left((a'-a) + 2(b'-b))x\right)\right)\right|$$

If both vectors belong to the same basis, *i.e.*, when $a = a'$, then Lemma 2 shows that the right hand side evaluates to 0 in case $b \neq b'$, and to 1 in case $b = b'$. This shows that M_a is an orthonormal basis.

If the vectors belong to different bases, *i.e.*, when $a \neq a'$, then Lemma 2 shows that $|\langle v_{a,b}|v_{a',b'}\rangle| = 2^{-n/2}$, hence M_a and $M_{a'}$ are mutually unbiased. The entries of the vectors $v_{a,b}$ have absolute value $2^{-n/2}$, thus the standard basis and M_a are mutually unbiased for all $a \in \mathrm{GR}(4, n)$. □

Example 2. We illustrate this construction by deriving five mutually unbiased bases in $\mathbb{C}^4$. In this case, the Galois ring $\mathrm{GR}(4, 2) = \mathbb{Z}_4[x]/\langle x^2 + x + 1\rangle$ with 16 elements is the basis of the construction. The Teichmüller set is given by $\mathcal{T}_2 = \{0, 1, 3\xi + 3, \xi\}$. Recall that an element of $\mathrm{GR}(4, 2)$ can be represented in the form $a + 2b$ with $a, b \in \mathcal{T}_2$. By definition, $\operatorname{tr}(a + 2b) = a + 2b + a^2 + 2b^2$. Computing the basis vectors yields

$$
\begin{aligned}
M_0 &= \left\{\tfrac{1}{2}(1, \ \ 1, \ \ 1, \ \ 1), \ \tfrac{1}{2}(1, 1, -1, -1), \ \tfrac{1}{2}(1, -1, -1, 1), \ \tfrac{1}{2}(1, -1, 1, -1)\right\}, \\
M_1 &= \left\{\tfrac{1}{2}(1, -1, -i, -i), \ \tfrac{1}{2}(1, -1, \ \ i, \ \ i), \ \tfrac{1}{2}(1, \ \ 1, \ \ i, -i), \ \tfrac{1}{2}(1, \ \ 1, -i, \ \ i)\right\}, \\
M_{3\xi+3} &= \left\{\tfrac{1}{2}(1, -i, -i, -1), \ \tfrac{1}{2}(1, -i, \ \ i, \ \ 1), \ \tfrac{1}{2}(1, \ \ i, \ \ i, -1), \ \tfrac{1}{2}(1, \ \ i, -i, \ \ 1)\right\}, \\
M_\xi &= \left\{\tfrac{1}{2}(1, -i, -i, -1), \ \tfrac{1}{2}(1, -i, \ \ i, \ \ 1), \ \tfrac{1}{2}(1, \ \ i, \ \ i, -1), \ \tfrac{1}{2}(1, \ \ i, -i, \ \ 1)\right\}.
\end{aligned}
$$

These four bases and the standard basis form an extremal set of five mutually unbiased bases of $\mathbb{C}^4$.

4   Non Prime Powers

In the previous two sections, we established that the number $N(d)$ of mutually unbiased bases in dimension d attains the maximal possible value, $N(d) = d+1$, when d is a prime power. In contrast, the exact value of $N(d)$ is not known for any dimension d which is divisible by at least two distinct primes, not even in small dimensions such as $d = 6$.

The problem to determine $N(d)$ is similar to the combinatorial problem to determine the number $M(d)$ of mutually orthogonal Latin squares of size $d \times d$. The number $M(d)$ is exactly known for prime powers but not in general when d is divisible by at least two distinct primes, see [6, 16] for more details. Lower bounds on the number of mutually orthogonal Latin squares can be obtained with the help of a lemma by MacNeish. Our next result formulates a similar statement for the number $N(d)$ of mutually unbiased bases.

Lemma 3. *Let $d = p_1^{a_1} \cdots p_r^{a_r}$ be a factorization of d into distinct primes p_i. Then*

$$N(d) \geq \min\{N(p_1^{a_1}), N(p_2^{a_2}), \ldots, N(p_r^{a_r})\}.$$

Proof. We denote the minimum by $m = \min_i N(p_i^{a_i})$. Choose m mutually unbiased bases $B_1^{(i)}, \ldots, B_m^{(i)}$ of $\mathbb{C}^{p^{a_i}}$, for all i in the range $1 \leq i \leq r$. Then

$$\{B_k^{(1)} \otimes \ldots \otimes B_k^{(r)} : k = 1, \ldots, m\}$$

is a set of m mutually unbiased bases of $\mathbb{C}^d$. $\quad\square$

An easily memorable form of the above lemma is $N(nm) \geq \min\{N(n), N(m)\}$ for all $m, n \geq 2$. A simple consequence is that $N(d) \geq 3$ for all dimensions $d \geq 2$, that is, in each dimension there are at least three mutually unbiased bases.

Many researchers in the quantum physics community seem to be under the impression that $N(d) = d + 1$ for all integers $d \geq 2$. However, there is some numerical evidence that considerably fewer mutually unbiased bases might be possible if the dimension is not a prime power. In fact, a conjecture by Zauner on the existence of affine quantum designs implies that $N(6) = 3$ rather than $N(6) = 7$, see [24].

Conjecture 1 (Zauner). The number of mutually unbiased bases in dimension 6 is given by $N(6) = 3$.

Apparently, Zauner did considerable numerical computations to bolster his conjecture. Our computational experiments indicate that $N(d)$ is in general smaller than $d + 1$ when d is not a prime power.

Problem 1. Does $N(d) = d + 1$ hold for any dimension $d \geq 2$ that is not a prime power?

Another interesting problem concerns lower bounds on $N(d)$. Recall that for mutually orthogonal Latin squares, $M(d) \to \infty$ for $d \to \infty$, as shown by Chowla, Erdős, and Strauss [10]. It is natural to ask whether a similar property holds for the number of mutually unbiased bases:

Problem 2. Does $N(d) \to \infty$ for $d \to \infty$ hold?

More constructions of mutually unbiased bases are needed to prove such a result. A result similar to Wilson's theorem on the number of mutually orthogonal Latin squares [21] would be particularly interesting.

5 Conclusions

Mutually unbiased bases are basic primitives in quantum information theory. They have applications in quantum cryptography and the design of optimal measurements. It is known that in dimension d at most $d + 1$ mutually unbiased bases can exist. In this paper, we gave a simplified proof of the fact that $d + 1$ mutually unbiased bases exist in $\mathbb{C}^d$ when d is a prime power.

Specifically, we were able to generalize the construction by Alltop to powers of a prime $p \geq 5$. Elementary estimates of Weil sums allowed us to derive a particularly short proof of a theorem by Wootters and Fields. For dimensions $d = 2^n$, we took advantage of known properties of exponential sums over $\mathrm{GR}(4, n)$ to obtain extremal sets of mutually unbiased bases.

An open problem is to determine the maximal number of mutually unbiased bases when the dimension is not a prime power. We derived an elementary lower bound for arbitrary dimensions and discussed some conjectures and open problems. Finally, we recommend the mean king's problem [19, 12, 2] as an enjoyable application of mutually unbiased bases.

References

1. W.O. Alltop. Complex sequences with low periodic correlations. *IEEE Transactions on Information Theory*, 26(3):350–354, 1980.
2. P.K. Aravind. Solution to the king's problem in prime power dimensions. *Z. Naturforschung*, 58a:2212, 2003.
3. S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan. A new proof of the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2002.
4. H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61(6):062308, 2000.
5. C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE Intl. Conf. Computers, Systems, and Signal Processing*, pages 175–179. IEEE, 1984.
6. T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*, volume 2. Cambridge University Press, Cambridge, 2nd edition, 1999.
7. B. Bollobás. *Random Graphs*. Academic Press, London, 1985.
8. C. Carlet. One-weight Z_4-linear codes. In J. Buchmann, T. Høholdt, H. Stichtenoth, and H. Tapia-Recillas, editors, *Coding Theory, Cryprography and Related Areas*, pages 57–72. Springer, 2000.
9. S. Chaturvedi. Aspects of mutually unbiased bases in odd-prime-power dimensions. *Phys. Rev. A*, 65:044301, 2002.
10. S. Chowla, P. Erdős, and E.G. Strauss. On the maximal number of pairwise orthogonal latin squares of given order. *Canadian J. Math.*, 12:204–208, 1960.
11. P. Delsarte, J.M. Goethals, and J.J. Seidel. Bounds for systems of lines, and Jacobi polynomials. *Philips Res. Repts.*, pages 91*–105*, 1975.
12. B.-G. Englert and Y. Aharonov. The mean king's problem: Prime degrees of freedom. *Phys. Letters*, 284:1–5, 2001.
13. S.G. Hoggar. t-designs in projective spaces. *Europ. J. Combin.*, 3:233–254, 1982.
14. I.D. Ivanović. Geometrical description of quantal state determination. *J. Phys. A*, 14:3241–3245, 1981.
15. G.A. Kabatiansky and V.I. Levenshtein. Bounds for packings on a sphere and in space. *Problems of Information Transmission*, 14(1):1–17, 1978.

16. C.F. Laywine and G.L. Mullen. *Discrete Mathematics Using Latin Squares.* John Wiley, New York, 1998.

17. R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications.* Cambridge University Press, 2nd edition, 1994.

18. J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U.S.A.*, 46:570–579, 1960.

19. L. Vaidman, Y. Aharonov, and D.Z. Albert. How to ascertain the values of σ_x, σ_y, and σ_z. *Phys. Rev. Lett.*, 58:1385–1387, 1987.

20. Z.-X. Wan. *Quaternary Codes.* World-Scientific, Singapore, 1997.

21. R.M. Wilson. Concerning the number of mutually orthogonal Latin squares. *Discr. Math.*, 9:181–198, 1974.

22. W.K. Wootters and B.D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191:363–381, 1989.

23. K. Yang, T. Helleseth, P. V. Kumar, and A. G. Shanbhag. On the weight hierarchy of Kerdock codes over Z_4. *IEEE Transactions on Information Theory*, 42(5):1587–1593, 1996.

24. G. Zauner. *Quantendesigns – Grundzüge einer nichtkommutativen Designtheorie.* PhD thesis, Universität Wien, 1999.