# CONNECTING HIGHLY NONLINEAR BOOLEAN FUNCTIONS TO (APPROXIMATELY) REAL MUTUALLY UNBIASED BASES

AJEET KUMAR, SUBHAMOY MAITRA, AND MOHIT PAL

Abstract. We establish a connection between (Approximately) Real Mutually Unbiased Bases (ARMUBs) of the $d$ dimensional real vector space $\mathbb{R}^d$, where $d = 2^n$, and Walsh transform of certain highly nonlinear $(n, m)$-Boolean functions. When $n$ is odd, then the state of the art results in this domain allow constructing 2 Real Mutually Unbiased Bases (RMUBs), whereas for $n$ even this is $d/2 + 1$ [Cameron and Seidel, 1973]. This result has been proved using a different technique in [Boykin et al., 2005]. Here we present another proof using the Kerdock codes and interpreting them as Boolean functions. Further, we show that for both odd and even $n$ we can construct $d + 1$ many ARMUBs with a little compromise in the inner products. More precisely, when $n$ is odd, the inner product between two vectors from two different bases is at most $\sqrt{2}/\sqrt{d}$ and is achieved for Almost Bent (AB) functions. When $n$ is even, then this bound is $2/\sqrt{d}$. Moreover, we show that using the generic construction method of Cao and Chou [Bull. Aust. Math. Soc., 2016], one can relax the permutation condition on $f$ by reversing the roles of $a$ and $b$.

## 1. Introduction

The history of mutually unbiased bases goes back to the seminal work of Schwinger [16], where he showed that if $B$ and $B'$ are two orthonormal bases of the $d$-dimensional Hilbert space $\mathbb{C}^d$ such that

$$|\langle b, b' \rangle|^2 = \frac{1}{d} \text{ for all } b \in B \text{ and } b' \in B',$$

then no information can be retrieved when a quantum system which is prepared in a basis state $B$ is measured with respect to the basis $B'$. We say such bases $B$ and $B'$ Mutually Unbiased Bases (MUBs). MUBs have applications in quantum cryptography, where they are the quantum states used in most QKD protocols [3, 4, 9]. Let $N(d)$ denote the maximum cardinality of any set containing pairwise MUBs of $\mathbb{C}^d$. It is well-known [2, 11] that $N(d) \leq d + 1$ and the equality holds when $d$ is a prime power. We call this set of $d + 1$ bases, a complete set of MUBs, or simply a complete MUB. 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 the smallest dimension $d = 6$. A long-standing open problem in quantum physics is whether or not $N(d) = d + 1$ holds for any dimension $d \geq 6$ that is not a prime power.

Another interesting problem in this direction is to find MUBs which are also real. Such MUBs are called Real Mutually Unbiased Bases (RMUBs). Let $M(d)$ denote the maximum

2020 *Mathematics Subject Classification.* 12E20, 11T06.

*Key words and phrases.* Boolean Functions, Cryptography, Mutually Unbiased Bases (MUBs), Quantum Information Theory, Walsh Transform.

cardinality of any set containing pairwise RMUBs of $\mathbb{R}^d$. As the problem is more constrained here, and thus $M(d)$ is even small. A general upper bound [6, 11] for $M(d)$ is $d/2+1$. In the particular case when $d = p^n$, where $p$ is a prime number, we have

$$M(d) = \begin{cases} 1 & \text{if } p > 2, \\ 2 & \text{if } p = 2 \text{ and } n \text{ is odd}, \\ d/2+1 & \text{if } p = 2 \text{ and } n \text{ is even}. \end{cases}$$

One may refer to [5, Table 1] for a comprehensive view on RMUBs. This scarcity of MUBs of $\mathbb{C}^d$ for composite numbers $d$ and RMUBs of $\mathbb{R}^d$ led the authors of [17] to define what is now known as Approximately Mutually Unbiased Bases (AMUBs).

**Definition 1.1.** Let $\mathbb{C}^d$ be the $d$-dimensional Hilbert space. The orthonormal bases of $\mathbb{C}^d$ in the set $\mathcal{B} = \{B_1, \ldots, B_N\}$ are called AMUBs if for all $u \in B_i, v \in B_j, 1 \leq i \neq j \leq N$, we have $|\langle u, v\rangle| \leq \delta$, where

$$\delta \in \left\{ \frac{1+o(1)}{\sqrt{d}}, O\left(\frac{1}{\sqrt{d}}\right), O\left(\frac{\log d}{\sqrt{d}}\right) \right\}.$$

When AMUBs are also real then we call them Approximately Real Mutually Unbiased Bases (ARMUBs).

1.1. **Contribution & Organization.** In this extended abstract, we shall restrict ourselves to dimensions $d = 2^n$, where $n$ is a positive integer, and study the problem of constructing RMUBs and ARMUBs of $\mathbb{R}^d$ from the perspective of $(n, m)$-Boolean functions, where $m \leq n$. We first establish a connection between the inner product values of two vectors taken from two different bases of $\mathbb{R}^d$ and the Walsh spectrum of $(n, m)$-Boolean functions. In this regard, in Section 2, we state some preliminary results that will be used in subsequent sections. Our contributions are as follows.

- Section 3 connects $(n, m)$-Boolean functions, where $n$ is even and $m \leq n$, to RMUBs. In Subsection 3.1, we present two constructions of $\sqrt{d}+1$ many RMUBs, where $d = 2^n$, using bent $(n, n/2)$-Boolean functions and maximum number of bent component $(n, n)$-functions. This is a suboptimal result as we can have at most $d/2+1$ many RMUBs.
- In Subsection 3.2, we describe a methodology to obtain $d/2+1$ many RMUBs using Kerdock codes. The main result is presented in Theorem 3.5. Note that this was first identified in [7] and later an alternative proof was given in [5]. Our result is arrived through a different technique exploiting the properties of the bent functions in Kerdock codes.
- In Section 4, we consider the approximate versions of RMUBs. Given the tight upper bounds from [7], the relaxation of inner product values is mandatory. We construct $d+1$ ARMUBs for both odd and even $n$. In our construction, when $n$ is odd, the inner product between two vectors from two different bases is at most $\sqrt{2}/\sqrt{d}$ , and this significantly increases the number of ARMUBs to $d+1$ from only 2 RMUBs, with a slight compromise in the inner product values. This result is available in Theorem 4.2

and is achieved for Almost Bent (AB) functions that exist only if $n$ is odd. When $n$ is even, then the inner product values in our construction are bounded by $2/\sqrt{d}$ and this result is explained in Theorem 4.4. Here, the improvement is from $d/2+1$ RMUBs to $d+1$ ARMUBs by doubling the inner product values. These results have been obtained exploiting different classes, for example, Gold, Kasami, Welch, Niho and Inverse functions. Additionally, we have noted that using the generic construction method of [8], we can relax the permutation condition of the function $f$ by reversing the roles of certain parameters, namely $a$ and $b$.

Section 5 concludes this extended abstract.

## 2. Preliminaries

Let $\mathbb{F}_d$ be the finite field with $d = p^n$ elements. In $\mathbb{F}_d$, we have two finite abelian groups, namely, the additive group and the multiplicative group of $\mathbb{F}_d$. In this extended abstract, we shall mainly focus on the characters pertaining to the additive group of the finite field and we shall use the term additive characters of $\mathbb{F}_d$ for them. Let $\mathrm{Tr}_1^n$ be the absolute trace map from $\mathbb{F}_d$ to $\mathbb{F}_p$, then the function $\chi_1$ defined by

$$\chi_1(c) = e^{\frac{2\pi i}{p}\mathrm{Tr}_1^n(c)} \quad \text{for all } c \in \mathbb{F}_d,$$

is a homomorphism from $\mathbb{F}_d$ into the multiplicative group $U$ of complex numbers of absolute value 1, and is called an additive character of $\mathbb{F}_d$. All additive characters of $\mathbb{F}_d$ can be expressed in terms of $\chi_1$ and are defined as, for $b \in \mathbb{F}_d$, $\chi_b(c) = \chi_1(bc)$ for all $c \in \mathbb{F}_d$. We can obtain the trivial additive character $\chi_0$ by taking $b = 0$, for which $\chi_0(c) = 1$ for all $c \in \mathbb{F}_d$. The additive characters of $\mathbb{F}_d$ satisfy the following orthogonality relations. For additive characters $\chi_a$ and $\chi_b$, we have

$$\sum_{c\in\mathbb{F}_d} \chi_a(c)\overline{\chi_b(c)} = \begin{cases} 0 & \text{for } a \neq b, \\ d & \text{for } a = b. \end{cases} \tag{2.1}$$

Let $\chi$ be a nontrivial additive character of $\mathbb{F}_d$, and let $f(X) \in \mathbb{F}_d[X]$ be a polynomial of degree $\ell > 0$. Then the sums of the form $\sum_{X\in\mathbb{F}_d} \chi(f(X))$ are called Weil sums. The problem of evaluating such character sums explicitly is difficult. It is easy to observe that when degree of $f$ is 1, then the Weil sum is zero. When the degree of $f$ is 2 and the characteristic of the finite field is odd, then (see [13, Theorem 5.37])

$$\left| \sum_{X\in\mathbb{F}_d} \chi(f(X)) \right| = \sqrt{d}. \tag{2.2}$$

For polynomials of degree $\geq 3$, we have following bound for the absolute value of the Weil sums, which is popularly known as Weil's bound.

**Lemma 2.1.** [13, Theorem 5.38] *Let $f(X) \in \mathbb{F}_d[X]$ be a polynomial of degree $\ell > 0$ with $\gcd(\ell, d) = 1$ and let $\chi$ be a nontrivial additive character of $\mathbb{F}_d$, then*

$$\left| \sum_{X \in \mathbb{F}_d} \chi(f(X)) \right| \leq (\ell - 1)\sqrt{d}. \tag{2.3}$$

The first result on explicit sets of complete MUBs in the case of primes $p \geq 5$ was due to Alltop [1]. Using the absolute value of the Weil sums (2.2) for polynomials of degree 2, Klappenecker and Rötteler [12] generalized the results of Alltop [1] to prime power dimensions. More precisely, using Weil sums (2.2), the authors gave a short proof of the following lemma which was first proved by Wootters and Fields [19] and later proved by Chaturvedi [10] and Bandyopadhyay et al. [2] using different techniques.

**Lemma 2.2.** [12, Theorem 2] *Let $\mathbb{F}_d$ be a finite field of odd characteristic. Define $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$, where*

$$v_{a,b} = \frac{1}{\sqrt{d}} \chi(aX^2 + bX)_{X \in \mathbb{F}_d}.$$

*Then the standard basis $B_\infty$ and the sets $B_a$ with $a \in \mathbb{F}_d$ form a complete MUB of $\mathbb{C}^d$.*

In [8], Cao and Chou used the orthogonality of additive characters and the Weil bound (2.3) to give the following generic constructions of AMUBs of $\mathbb{C}^d$ using permutation polynomials over the finite field $\mathbb{F}_d$.

**Lemma 2.3.** [8, Theorem 3.1] *Let $\ell$ be a positive integer with $\gcd(\ell, d) = 1$ and $f(X) \in \mathbb{F}_d[X]$ is a permutation polynomial of degree $\ell$ over $\mathbb{F}_d$. Denote by $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$ the set of vectors given by*

$$v_{a,b} = \frac{\theta(a)}{\sqrt{d}} \chi(aX + bf(X))_{X \in \mathbb{F}_d},$$

*where $\theta$ is a map from $\mathbb{F}_d$ to $\mathbb{C}$ such that $|\theta(a)| = 1$ for all $a \in \mathbb{F}_d$. Then the standard basis $B_\infty$ and the sets $B_a$ with $a \in \mathbb{F}_d$ form AMUBs of $\mathbb{C}^d$.*

In the above construction, for any permutation polynomial $f(X) \in \mathbb{F}_d[X]$ of degree $\ell$ with $\gcd(\ell, d) = 1$, we get an upper bound $\delta = (\ell - 1)/\sqrt{d}$. In the remaining part of this extended abstract, we shall assume that $p = 2$ and denote $\chi(X)$ by $(-1)^{\mathrm{Tr}_1^n(X)}$.

## 3. Connecting Boolean functions and RMUBs

In this section, we shall show the relation between the Walsh spectrum of $(n, m)$-Boolean functions and RMUBs of $\mathbb{R}^d$, where $d = 2^n$. Let $f$ be an $(n, m)$-Boolean function, where $m \leq n$. We denote, by $\mathrm{Tr}_1^n$ and $\mathrm{Tr}_1^m$, absolute trace functions from $\mathbb{F}_d$ to $\mathbb{F}_2$ and from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, respectively. For any $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_d$, define the vector

$$v_{a,b} = \left( \frac{(-1)^{\mathrm{Tr}_1^m(af(X)) + \mathrm{Tr}_1^n(bX)}}{\sqrt{d}} \right)_{X \in \mathbb{F}_d}. \tag{3.1}$$

Then the set $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$ forms an orthonormal basis of $\mathbb{R}^d$. As, for any $b_1, b_2 \in \mathbb{F}_d$, we have

$$\langle v_{a,b_1}, v_{a,b_2} \rangle = \frac{1}{d} \sum_{X \in \mathbb{F}_d} (-1)^{\mathrm{Tr}_1^n((b_1+b_2)X)} = \begin{cases} 1 & \text{if } b_1 = b_2, \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

Let $\mathcal{B} = \{B_a \mid a \in \mathbb{F}_{2^m}\}$ be the set of $2^m$ orthonormal bases of $\mathbb{R}^d$. It is easy to observe that the inner product of two vectors $v_{a_1,b_1}$ and $v_{a_2,b_2}$, taken from two different bases $B_{a_1}$ and $B_{a_2}$, is given by

$$\begin{aligned} \langle v_{a_1,b_1}, v_{a_2,b_2} \rangle &= \frac{1}{d} \sum_{X \in \mathbb{F}_d} (-1)^{\mathrm{Tr}_1^m((a_1+a_2)f(X)) + \mathrm{Tr}_1^n((b_1+b_2)X)} \\ &:= \frac{1}{d} \mathcal{W}_f(b_1+b_2, a_1+a_2). \end{aligned}$$

In the theory of $(n,m)$-Boolean functions, $\mathcal{W}_f : \mathbb{F}_d \times \mathbb{F}_{2^m} \to \mathbb{Z}$ is called the Walsh transform of $f$. The Walsh spectrum of $f$ is the set of values $\{\mathcal{W}_f(b,a) \mid b \in \mathbb{F}_d \text{ and } a \in \mathbb{F}_{2^m}\}$. A highly nonlinear function $f$ is one where all the values in the Walsh spectrum have small magnitude. This relationship suggests that highly nonlinear $(n,m)$-Boolean functions $f$ can be used to construct RMUBs and ARMUBs. It is well-known that

$$\max_{a \in \mathbb{F}_{2^m}^*,\ b \in \mathbb{F}_d} |\mathcal{W}_f(b,a)| \geq \sqrt{d}, \tag{3.3}$$

and is known as the covering redius bound. The $(n,m)$-Boolean functions $f$ which attain the bound (3.3) with equality are called bent functions. Bent functions are extremal combinatorial objects with several areas of application, such as coding theory, maximum length sequences, cryptography, the theory of difference sets to name a few. We refer interested readers to the books [14, 18]. In the following subsection, we shall use bent components of $(n,m)$-Boolean functions to construct RMUBs of $\mathbb{R}^d$.

3.1. **Bent components of $(n,m)$-Boolean functions and RMUBs.** Let $f$ be an $(n,m)$-Boolean function with $n$ even and $m \leq n$. Boolean functions $F_a := \mathrm{Tr}_1^m(af(X))$ for $a \in \mathbb{F}_{2^m}^*$ are called component functions of $f$. An $(n,m)$-Boolean function $f$ is called bent (sometimes also called vectorial bent) if and only if all its component functions $F_a$, $a \in \mathbb{F}_{2^m}^*$ are bent. Equivalently, $f$ has $2^m - 1$ bent components. Since bent $(n,m)$-Boolean functions exist if and only if $n$ is even and $m \leq n/2$, the maximum number of bent components of $(n,m)$-Boolean functions with $m > n/2$ is strictly less than $2^m - 1$. For $(n,n)$-Boolean functions $f$ with $n$ even, Pott et al. [15] showed that the number of bent components can be at most $2^n - 2^{n/2}$ and that this bound is sharp. An $(n,n)$-Boolean function which attain this bound is called maximum number of bent components (MNBC) $(n,n)$-function.

Recall that, when $d = 2^n$ with $n$ even then we have at most $d/2 + 1$ RMUBs of $\mathbb{R}^d$. Here, we give two constructions of RMUBs from bent components of $(n,m)$-Boolean functions. Our first construction uses bent $(n,m)$-Boolean functions and give $2^m + 1$ RMUBs. Since bent $(n,m)$-Boolean functions exist only for $m \leq n/2$, this construction can give at most

$2^{n/2}+1=\sqrt{d}+1$ many RMUBs. In the following theorem we shall use bent $(n,m)$-Boolean functions, where $n$ is even and $m \leq n/2$, to give $2^m+1$ RMUBs of $\mathbb{R}^d$.

**Theorem 3.1.** *Let $f$ be a bent $(n,m)$-Boolean function, where $n$ is even and $m \leq n/2$. Denote by $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$ the set of vectors given by*

$$v_{a,b} = \left( \frac{(-1)^{Tr_1^m(af(X))+Tr_1^n(bX)}}{\sqrt{d}} \right)_{X \in \mathbb{F}_d}.$$

*Then the standard basis $B_\infty$ and the sets $B_a$ with $a \in \mathbb{F}_{2^m}$ form RMUBs of $\mathbb{R}^d$.*

*Proof.* Let $e_i$ be an element of the standard basis of $\mathbb{R}^d$. Then, for any $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_d$, we have

$$|\langle v_{a,b}, e_i \rangle| = \left| \left( \frac{(-1)^{\mathrm{Tr}_1^m(af(X))+\mathrm{Tr}_1^n(bX)}}{\sqrt{d}} \right) \right| \text{ for some } X \in \mathbb{F}_d = \frac{1}{\sqrt{d}}.$$

The orthonormality of the bases $B_a$, where $a \in \mathbb{F}_{2^m}$ has been shown in (3.2). It only remains to show that the absolute value of the inner product of two vectors taken from two different bases is exactly $1/\sqrt{d}$. For any $a_1, a_2 \in \mathbb{F}_{2^m}, a_1 \neq a_2$ and $b_1, b_2 \in \mathbb{F}_d$, we have

$$\begin{aligned} |\langle v_{a_1,b_1}, v_{a_2,b_2} \rangle| &= \frac{1}{d} \left| \sum_{X \in \mathbb{F}_d} (-1)^{\mathrm{Tr}_1^m((a_1+a_2)f(X))+\mathrm{Tr}_1^n((b_1+b_2)X)} \right| \\ &= \frac{1}{d} |\mathcal{W}_f(b_1+b_2, a_1+a_2)| = \frac{1}{\sqrt{d}}, \end{aligned}$$

where the last equality holds because $f$ is a bent $(n,m)$-Boolean function. This completes the proof. □

**Corollary 3.2.** *Let $n$ be even and $f$ be a bent $(n, n/2)$-Boolean function. Then Theorem 3.1 gives $\sqrt{d}+1$ RMUBs of $\mathbb{R}^d$.*

Our second construction uses MNBC $(n,n)$-function to construct $\sqrt{d}+1$ RMUBs of $\mathbb{R}^d$. For any $(n,n)$-Boolean function $f$, let the set $S_f$ be defined by $S_f = \{a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_1^n(af(X)) \text{ is not bent}\}$. In 2018, Pott et al. [15] showed that for an MNBC $(n,n)$-function $f$, $|S_f| = 2^{n/2}$ and $S_f$ is a linear space of dimension $n/2$ over $\mathbb{F}_2$. One may note that in the proof of the mutually unbiased-ness of two bases $B_{a_1}$ and $B_{a_2}$ in Theorem 3.1, we use the bent-ness of the component function $\mathrm{Tr}_1^m((a_1+a_2)f(X))$. For an MNBC $(n,n)$-function $f$, define a set $\mathcal{S} \subset \mathbb{F}_d$ such that for $a_1, a_2 \in \mathcal{S}$ with $a_1 \neq a_2$, the component function $\mathrm{Tr}_1^n((a_1+a_2)f(X))$ is bent, i.e., $a_1+a_2 \notin S_f$. The following lemma gives the cardinality of the set $\mathcal{S}$.

**Lemma 3.3.** *Let $f$ be an MNBC $(n,n)$-function. Let $\mathcal{S} \subset \mathbb{F}_d$ be such that for $a_1, a_2 \in \mathcal{S}$ with $a_1 \neq a_2$, the component function $Tr_1^n((a_1+a_2)f(X))$ is bent. Then $|\mathcal{S}| = \sqrt{d}$.*

*Proof.* Let $\mathbb{F}_{2^n}$ be viewed as a vector space over $\mathbb{F}_2$ of dimension $n$, i.e., $\mathbb{F}_2^n$. Since $S_f$ is a linear space of dimension $n/2$ over $\mathbb{F}_2$, it is a subspace of $\mathbb{F}_2^n$. Consider the quotient space $V := \mathbb{F}_2^n/S_f$ having cardinality $2^{n/2}$. Let $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n/S_f$ be the canonical projection linear

transformation defined by $\pi(v) = v+S_f$. By definition, $\ker(\pi) = S_f$. Now, for any $s_1, s_2 \in \mathbb{F}_2^n$, the condition $s_1 + s_2 \notin S_f$ is equivalent to

$$\pi(s_1 + s_2) \neq 0 \implies \pi(s_1) + \pi(s_2) \neq 0 \implies \pi(s_1) \neq \pi(s_2).$$

Let the distinct cosets of $S_f$ in $\mathbb{F}_2^n$ be $C_1, C_2, \ldots, C_{2^{n/2}}$. Construct the set $\mathcal{S}$ by choosing exactly one representative $s_i$ from each coset $C_i$. For any two distinct $s_i, s_j \in \mathcal{S}$, they belong to different cosets, meaning $\pi(s_i) \neq \pi(s_j)$ and hence $s_i + s_j \notin S_f$. Thus, $|\mathcal{S}| \geq 2^{n/2}$. Now, suppose $|\mathcal{S}| = 2^{n/2} + 1$ then there must exist at least two distinct elements $s_a, s_b \in \mathcal{S}$ such that they belong to the same coset and hence $s_a + s_b \in S_f$. This completes the proof. □

The following theorem shows that an MNBC $(n, n)$-function $f$ can be used to construct $\sqrt{d}+1$ RMUBs of $\mathbb{R}^d$.

**Theorem 3.4.** *Let $f$ be an MNBC $(n, n)$-function, where $n$ is even. For any $a \in \mathcal{S}$ consider the orthonormal basis $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$, where $v_{a,b}$ is defined by*

$$v_{a,b} = \left( \frac{(-1)^{Tr_1^n(af(X)+bX)}}{\sqrt{d}} \right)_{X \in \mathbb{F}_d}.$$

*Then the set $\mathcal{B} = \{B_a \mid a \in \mathcal{S}\}$ together with the standard basis $B_\infty$ form RMUBs of $\mathbb{R}^d$.*

*Proof.* Notice that, for any two vectors $v_{a_1,b_1}$ and $v_{a_2,b_2}$, taken from two different bases $B_{a_1}$ and $B_{a_2}$, repectively, we have

$$|\langle v_{a_1,b_1}, v_{a_2,b_2} \rangle| = \frac{1}{d} \left| \sum_{X \in \mathbb{F}_d} (-1)^{\mathrm{Tr}_1^n((a_1+a_2)f(X)+(b_1+b_2)X)} \right| = \frac{1}{\sqrt{d}},$$

where the last equality holds because $a_1, a_2 \in \mathcal{S}$. This completes the proof. □

3.2. **Our optimal construction of RMUBs using Kerdock codes.** In Theorem 3.4, we have seen that even if we use MNBC $(n, n)$-function $f$, we are able to construct at most $\sqrt{d}+1$ many RMUBs. Instead of using bent components of a single $(n, n)$-Boolean function, we now consider a set of $n$ variable quadratic Boolean functions such that the sum of any two elements of this set is bent. Recall that, for every nonnegative integer $r$ and every positive integer $n \geq r$, the Reed-Muller code $RM(r, n)$ of order $r$, length $2^n$ and dimension $\sum_{i=0}^{r} \binom{n}{i}$ is the binary linear code of all words of length $2^n$ corresponding to the evaluations over $\mathbb{F}_{2^n}$ of all the Boolean functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ of algebraic degree at most $r$. For any $a \in \mathbb{F}_{2^{n-1}}$, where $n$ is even, define a Boolean function $f_a$ from $\mathbb{F}_{2^{n-1}} \times \mathbb{F}_2 \to \mathbb{F}_2$ in the following way

$$f_a(X, X_n) = \mathrm{Tr}_1^{n-1}\left( \sum_{i=1}^{\frac{n-2}{2}} (aX)^{2^i+1} \right) + X_n \mathrm{Tr}_1^{n-1}(X). \tag{3.4}$$

Then the Kerdock codes $\mathcal{K}_n$ of length $2^n$ and dimension $2n$ are defined as

$$\mathcal{K}_n = \bigcup_{a \in \mathbb{F}_{2^{n-1}}} f_a + RM(1, n).$$

The functions $f_a$, where $a \in \mathbb{F}_{2^{n-1}}$, have the special property that for any $a_1, a_2 \in \mathbb{F}_{2^{n-1}}$ with $a_1 \neq a_2$ the function $f_{a_1} + f_{a_2}$ is bent. In the following theorem, we use the functions $f_a$ to construct $d/2 + 1$ RMUBs of $\mathbb{R}^d$.

**Theorem 3.5.** *Let $n$ be an even positive integer. For any $a \in \mathbb{F}_{2^{n-1}}$ consider the orthonormal basis $B_a = \{v_{a,b} \mid b \in \mathbb{F}_{2^n}\}$, where $v_{a,b}$ is defined as*

$$v_{a,b} = \left( \frac{(-1)^{f_a(X) + Tr_1^n(bX)}}{\sqrt{d}} \right)_{X \in \mathbb{F}_d}.$$

*Then the standard basis $B_\infty$ and the set $\mathcal{B} = \{B_a \mid a \in \mathbb{F}_{2^{n-1}}\}$ form RMUBs of $\mathbb{R}^d$.*

## 4. Our new constructions for ARMUBs

In this section, we use $(n, n)$-Boolean functions to construct ARMUBs of $\mathbb{R}^d$, where $d = 2^n$. Notice that for $(n, n)$-Boolean functions $f$, $v_{a,b}$ in (3.1) reduces to

$$v_{a,b} = \left( \frac{(-1)^{\mathrm{Tr}_1^n(af(X) + bX)}}{\sqrt{d}} \right)_{X \in \mathbb{F}_d}. \tag{4.1}$$

It is worth mentioning here that if we change the roles of $a$ and $b$ in (4.1) and take $f$ to be a bijective function then this is precisely the generic construction given by Cao and Chou [8]. Thus, our construction is more general in the sense that it holds for non-permutation functions as well. We would also like to point out that if $f$ is a permutation, then the sets $B_b = \{v_{a,b} \mid a \in \mathbb{F}_d\}$, with $b \in \mathbb{F}_d$ together with $B_\infty$ will also form $d + 1$ ARMUBs. More precisely, in the following matrix

$$\mathcal{M} = \begin{pmatrix} v_{a_1,b_1} & v_{a_2,b_1} & \cdots & v_{a_d,b_1} \\ v_{a_1,b_2} & v_{a_2,b_2} & \cdots & v_{a_d,b_2} \\ \vdots & \vdots & & \vdots \\ v_{a_1,b_d} & v_{a_2,b_d} & \cdots & v_{a_d,b_d} \end{pmatrix}$$

each column of $\mathcal{M}$ forms an orthonormal basis of $\mathbb{R}^d$. However, if $f$ is a permutation then each row will also form an orthonormal basis of $\mathbb{R}^d$.

For any $(n, n)$-Boolean function $f$ of odd degree, the orthonormal bases $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$ for $a \in \mathbb{F}_d$, where $v_{a,b}$ is defined in (4.1), together with the standard basis $B_\infty$ give $(d + 1)$ ARMUBs having upper bound $\delta = \frac{\deg(f)-1}{\sqrt{d}}$. However, by choosing the function $f$ suitably, we can significantly improve this bound. We now recall the following lemma which gives a bound on the maximum absolute value of the Walsh spectrum entries of any $(n, n)$-Boolean function.

**Lemma 4.1.** *(Sidelnikov-Chabaud-Vaudenay (SCV) bound) Let $f$ be an $(n, n)$-Boolean function. Then*

$$\max_{\substack{a,b \in \mathbb{F}_d \\ a \neq 0}} |\mathcal{W}_f(a, b)| \geq \sqrt{2d}. \tag{4.2}$$

From the above lemma, we infer that for any $(n, n)$-Boolean function $f$ of odd degree, we have $\sqrt{2}/\sqrt{d} \leq \delta \leq (\deg(f) - 1)/\sqrt{d}$. It is well-known that the SCV bound can be tight only if $n$ is odd and the functions $f$ that achieve (4.2) with equality are called Almost Bent (AB) function. The following theorem gives $d+1$ ARMUBs of $\mathbb{R}^d$, where $d = 2^n$ with $n$ odd. Thus, when $n$ is odd, we are getting $d+1$ many ARMUBs with $\delta = \sqrt{2}/\sqrt{d}$ whereas with $\delta = 1/\sqrt{d}$, we have only 2 RMUBs.

**Theorem 4.2.** *Let $f$ be an almost bent $(n, n)$-Boolean function, where $n$ is odd. Then the orthonormal bases $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$ for $a \in \mathbb{F}_d$, where $v_{a,b}$ is defined in* (4.1)*, together with the standard basis $B_\infty$ give $d + 1$ ARMUBs having upper bound $\delta = \sqrt{2}/\sqrt{d}$.*

**Remark 4.3.** *The Gold function $X^{2^i+1}$ over $\mathbb{F}_{2^n}$, where $n$ is odd and $\gcd(i, n) = 1$ is an AB function. Thus,* [8, Theorem 3.3] *is a particular case of Theorem 4.2.*

When $n$ is even then the best known bound for the maximum absolute value of the Walsh spectrum entries of any $(n, n)$-Boolean function is $2\sqrt{d}$. Unlike AB functions for odd $n$, there is no specific name given to the class of functions, in the even $n$ case, attaining the bound $2\sqrt{d}$. Table 1 gives, upto the CCZ-equivalence, known classes of power maps that achieve the bound $2\sqrt{d}$, when $n$ is even. The following theorem gives $d + 1$ ARMUBs of $\mathbb{R}^d$, when

| Sr. No. | $e$ | Conditions |
|---|---|---|
| 1. | $2^{n-1} - 1$ | |
| 2. | $2^{2i} + 1$ | $n = 2m, \quad m > 1, \quad \gcd(i, m) = 1$ |
| 3. | $2^{4i} - 2^{2i} + 1$ | $n = 2m, \quad m > 1, \quad \gcd(i, m) = 1$ |
| 4. | $2^m + 2^{\frac{m+1}{2}} + 1$ | $n = 2m$ |
| 5. | $2^{m+1} + 3$ | $n = 2m$ |

TABLE 1. Known monomials $X^e$ on $\mathbb{F}_{2^n}$, upto CCZ-equivalence, having Walsh spectrum $\{0, \pm 2\sqrt{d}\}$.

$d = 2^n$ with $n$ even.

**Theorem 4.4.** *Let $n$ be even and $f(X) = X^e$ be a power map over $\mathbb{F}_{2^n}$, where $e$ is one of the exponents given in Table 1. Then the orthonormal bases $B_a = \{v_{a,b} \mid b \in \mathbb{F}_d\}$ for $a \in \mathbb{F}_d$, where $v_{a,b}$ is defined in* (4.1)*, together with the standard basis $B_\infty$ give $d+1$ ARMUBs having upper bound $\delta = 2/\sqrt{d}$.*

## 5. Conclusion

We connected highly nonlinear Boolean functions to RMUBs and ARMUBs of the $d$ dimensional real vector space $\mathbb{R}^d$, where $d = 2^n$. We then used this connection, when $n$ is even, to give two methods of constructing $\sqrt{d}+1$ many RMUBs using bent $(n, n/2)$-Boolean function and MNBC $(n, n)$-function. We also proposed a method of constructing $d/2+1$ RMUBs of $\mathbb{R}^d$, where $d = 2^n$ with $n$ even, using the Kerdock codes by interpreting them as Boolean functions. Further, we constructed $d + 1$ ARMUBs for odd and even $n$ having upper bound

$\sqrt{2}/\sqrt{d}$ and $2/\sqrt{d}$, respectively. We also showed that in the generic construction method of Cao and Chou [8], we can relax the permutation condition on $f$ by reversing the roles of $a$ and $b$.

## References


[1] W. O. Alltop, *Complex sequences with low periodic correlations*, IEEE Trans. Inf. Theory, 26(3) (1980) 350–354.

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

[3] H. Bechmann-Pasquinucci, A. Peres, *Quantum cryptography with* 3*-state systems*, Phys. Rev. Lett. 85(15) (2000) 3313–3316.

[4] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theor. Comput. Sci. 560(1) (2014) 7–11.

[5] P. O. Boykin, M. Sitharam, M. Tarifi, P. Wocjan, *Real mutually unbiased bases*, arXiv 2005. `https://arxiv.org/abs/quant-ph/0502024`

[6] R. Calderbank, P. Cameron, W. Kantor, J. Seidel. $\mathbb{Z}_4$*-kerdock codes, orthogonal spreads, and extremal Euclidean line-sets,* Proceedings of The London Mathematical Society, 75(3) (1997) 436–480.

[7] P. J. Cameron, J. J. Seidel, *Quadradic forms over GF(2)*, Indag-Math, 35 (1973) 1–8.

[8] X. Cao, W. S. Chou, *More constructions of approximately mutually unbiased bases*, Bull. Aust. Math Soc 93(2) (2016) 211–222.

[9] N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, *Security of quantum key distribution using d-level systems,* Phys. Rev. Lett. 88(12) (2002) 127902.

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

[11] P. Delsarte, J. M. Goethals, J. J. Seidel, *Bounds for systems of lines, and Jacobi polynomials*, Philips Res. Repts., (1975) 91–105.

[12] A. Klappenecker, M. Rötteler, *Constructions of mutually unbiased bases*, $\mathbb{F}_q$-7 2003, Lecture Notes in Computer Science, 2948 (eds. G. Mullen, A. Poli and H. Stichtenoth) (Springer, Berlin, 2003), 137–144.

[13] R. Lidl, H. Niederreiter, *Finite Fields (Ed. 2)*, Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge (1997).

[14] S. Mesnager, *Bent Functions: Fundamentals and Results*, Cham, Switzerland: Springer, (2016).

[15] A. Pott, E. Pasalic, A. Muratović-Ribić, S. Bajrić, *On the maximum number of bent components of vectorial functions,* IEEE Trans. Inf. Theory 64(1) (2018) 403–411.

[16] J. Schwinger, *Unitary operator bases*, Proc. Nat. Acad. Sci. U.S.A., 46 (2016) 570–579.

[17] I. E. Shparlinski, A. Winterhof, *Construction of approximately mutually unbiased bases*, Lecture Notes in Computer Science, 3887 (Springer, Berlin, 2006), 793–799.

[18] N. Tokareva, *Bent Functions: Results and Applications to Cryptography*, San Francisco, CA, USA: Academic, (2015).

[19] W. K. Wootters, B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Physics, 191 (1989) 363–381.


## Appendix

In Theorem 3.5, if we choose $n = 4$, then we get 9 RMUBs. Here, we give precise description of all the 9 RMUBs of $\mathbb{R}^{16}$ using Theorem 3.5. Consider the following quadratic bent Boolean

functions in four variables $x_1, x_2, x_3, x_4$.

$$\begin{aligned}
f_0 &= 0,\\
f_1 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,\\
f_2 &= x_1x_4 + x_2x_3 + x_3x_4,\\
f_3 &= x_1x_2 + x_1x_3 + x_3x_4,\\
f_4 &= x_1x_2 + x_1x_4 + x_2x_3,\\
f_5 &= x_1x_3 + x_2x_3 + x_2x_4,\\
f_6 &= x_1x_3 + x_1x_4 + x_2x_4,\\
f_7 &= x_1x_2 + x_2x_4 + x_3x_4.
\end{aligned}$$

Then the Kerdock code $\mathcal{K}_4$ of length $2^4$ is given by

$$\mathcal{K}_4 = \bigcup_{i=0}^{7} f_i + RM(1,4),$$

where $RM(1,4)$ is the first order Reed-Muller code of length $2^4$. For any fixed $f_i$, $i \in \{0,1,\ldots,7\}$, Let $M_{f_i}$ be the $16 \times 16$ matrix, whose rows are given by the vectors

$$v_b = ((-1)^{f_i + \mathrm{Tr}_1^4(bX)})_{X \in \mathbb{F}_{2^4}},$$

where $b \in \mathbb{F}_{2^4}$. Then the matrices $M_{f_i}$, $i = 0, 1, \ldots, 7$ together with the standard basis $M_\infty$ form 9 RMUBs of $\mathbb{R}^{16}$.

$$M_{f_0} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1\\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1\\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1\\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1\\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1\\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1\\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1\\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1\\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1\\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1\\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1
\end{pmatrix}$$

$$M_{f_1} = \begin{pmatrix}
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\
1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\
1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\
1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1
\end{pmatrix}$$

$$M_{f_2} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1
\end{pmatrix}$$

$$M_{f_3} = \begin{pmatrix}
1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 \\
1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\
1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1
\end{pmatrix}$$

$$M_{f_4} = \begin{pmatrix}
1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1
\end{pmatrix}$$

$$M_{f_5} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\
1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \\
1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1
\end{pmatrix}$$

$$M_{f_6} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\
1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & -1
\end{pmatrix}$$

$$M_{f_7} = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \end{pmatrix}$$

Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
*Email address*: ajeetk52@gmail.com

Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
*Email address*: subho@isical.ac.in

Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
*Email address*: mathmohit@outlook.com