New Tales of the Mean King

Andreas Klappenecker* and Martin Rötteler†

Once upon a time on an island far far away there lived a mean King who loved cats. The King started to hate physicists once he learned what had happened to Schrödinger's cat. One evening a terrible storm came on, there was thunder and lightning, and the rain poured down in torrents. Alice, a physicist, got stranded during that storm and the King's men captured her and brought her to the royal laboratories. Alice was told that she can prepare a silver atom in any state of her choosing, then the King's men will secretly measure one of the three cartesian spin components and hand the atom back to her. Alice is then free to perform any experiment with the silver atom before the King tells her which type of measurement has been done by his men. Once the King reveals this secret, she must immediately state the correct result of the measurement or she will die a cruel death.

The First Problem

The first problem of the King was brought to us by Aharanov, Vaidman, and Albert [19], although they did not dare[1] to reveal the tale of the King. The story was later told by Aharanov and Englert [1, 2] and we retold the tale. In more modern terms, Alice has the problem to prepare a quantum bit in a certain state, then the King's men perform a von Neumann measurement with respect to one of the Pauli spin observables σ_x, σ_y, or σ_z. Alice can then perform another measurement. Once the King reveals which observable was measured, she has to quickly find the answer.

Alice thought about the problem. She quickly realized that it is too risky to prepare the state of a single silver atom, but then she had an idea. She asked Tweedledee and Tweedledum to help her prepare a pair of silver atoms in a Schrödinger cat state. After they prepared the state, the King's men went to measure one atom. Once the atom was returned, Alice measured the system. To the great annoyance of the King, she was able to correctly guess the King's observation. Alice was set free and tried to live happily ever after.

We do not exactly know how Alice solved the problem, but we give a possible explanation. Recall that the spin matrices σ_z, σ_x, and σ_y are

[1] This is quite understandable; the cruel deeds of the Mean King can easily scare young physicists and we therefore do not recommend these tales for bedtime reading. Reader discretion is advised.

complementary observables; hence, their eigenbases

$$B_0 = \{v_{0,1}, v_{0,2}\}, \quad B_1 = \{v_{1,1}, v_{1,2}\}, \quad B_2 = \{v_{2,1}, v_{2,2}\},$$

are mutually unbiased orthonormal bases of $\mathbf{C}^2$. The particular nature of these bases is not really relevant, but the property that $|\langle v_{a,b}|v_{a',b'}\rangle|^2 = 1/2$ holds when $a \neq a'$ is crucial for our argument. One consequence is that

$$\varphi = \tfrac{1}{\sqrt{2}} v_{a,1} \otimes \overline{v_{a,1}} + \tfrac{1}{\sqrt{2}} v_{a,2} \otimes \overline{v_{a,2}} \in \mathbf{C}^2 \otimes \mathbf{C}^2$$

is the same state for all $a \in \{0, 1, 2\}$, which is in fact maximally entangled. Alice prepares the two silver atoms in this state. If the King's men perform a von Neumann measurement with respect to, say, the basis B_a and observe the value b, then the state of the two silver atoms collapses to $v_{a,b} \otimes \overline{v_{a,b}}$.

The trick is that Alice can set up a measurement such that she will learn a function $f\colon \{0, 1, 2\} \to \{1, 2\}$ that correctly maps the selected basis to the observed values. For instance, Alice can perform a von Neumann measurement with respect to the basis

$$\psi_{f_k} = -\varphi + \tfrac{1}{\sqrt{2}} \sum_{a=0}^{2} v_{a,f_k(a)} \otimes \overline{v_{a,f_k(a)}}, \qquad k \in \{1, 2, 3, 4\},$$

where the functions $f_k\colon \{0, 1, 2\} \to \{1, 2\}$ are given by

$$\begin{array}{lll} f_1(0) = 1, & f_1(1) = 1, & f_1(2) = 1, \\ f_2(0) = 1, & f_2(1) = 2, & f_2(2) = 2, \\ f_3(0) = 2, & f_3(1) = 1, & f_3(2) = 2, \\ f_4(0) = 2, & f_4(1) = 2, & f_4(2) = 1. \end{array}$$

For example, suppose that the King's men have measured in the basis B_a, $a = 2$, and observed the value $b = 1$. If Alice measures the resulting state in the basis $\{\psi_{f_1}, \psi_{f_2}, \psi_{f_3}, \psi_{f_3}\}$, then she will learn the function

$$\begin{array}{lll} f_1 & \text{with probability} & |\langle v_{2,1} \otimes \overline{v_{2,1}}\,|\psi_{f_1}\rangle|^2 = 1/2, \\ f_2 & \text{with probability} & |\langle v_{2,1} \otimes \overline{v_{2,1}}\,|\psi_{f_2}\rangle|^2 = 0, \\ f_3 & \text{with probability} & |\langle v_{2,1} \otimes \overline{v_{2,1}}\,|\psi_{f_3}\rangle|^2 = 0, \\ f_4 & \text{with probability} & |\langle v_{2,1} \otimes \overline{v_{2,1}}\,|\psi_{f_4}\rangle|^2 = 1/2. \end{array}$$

If the King finally reveals to her that his men have chosen the basis $a = 2$, then she will predict, either way, the value $f_1(2) = f_4(2) = 1$. In fact, it can be checked that this von Neumann measurement allows Alice to always correctly predict the observation made by the King's men, regardless of the choice of a and b! We will reveal the reason for this most curious behavior in the next section, but we encourage the reader to check our claim.

Remark. There exists a variation of the first problem by Hayashi, Horibe, and Hashimoto [10] that does not require mutually unbiased bases. Another variation can be obtained by the method described in the section on the King's third problem.

The Second Problem

She tried to leave the kingdom as soon as possible. When Alice finally reached the shore, some of the King's guards captured her, again! 'What do you want?', said Alice. One guard replied: 'We take you into custody, because you are still a physicist'. Alice finally understood why the monarch was known as the 'Mean King'. The King explained to Alice that the first problem was too easy. Then the King said 'I will hand you an atom with a prime power q of different basis states. You can prepare it in any state, then my men will secretly measure the atom with one of q+1 complementary observables'. He was leaning forward and said 'You can perform one more experiment, but then you have to guess the observation made by my men, or...'. In spite of dark foreboding, Alice replied sternly 'Fine!'.

The second problem was developed in a series of papers. Aharonov and Englert discussed a solution if the atom has a prime number of levels, see [1] and [2]. Aravind was the first to find a solution of the Mean King problem for atoms with a prime power of basis states [3], followed by Durt [5] and very recently by Hayashi, Horibe, and Hashimoto [9]. The latter approach is based on maximal sets of mutually orthogonal latin squares and turns out to be equivalent to our exposition, although it was developed independently. We use a more geometric approach based on affine planes.

For several days Alice was frantically scribbling and drawing on parchment. She certainly did not want to make any mistake. Finally, she had found a geometric solution. She asked Tweedledee and Tweedledum to help her in the royal laboratories. They prepared the state, the King's men measured and returned the atom. Alice then performed another experiment and after the King revealed the measurement basis, she correctly guessed the value that has been observed by the King's men.

Designs. We recall some terminology from combinatorial design theory, see [4,18,20] for details. Let X be a finite set of v points. A (v,k,λ) design over X is a family $\mathcal{B}$ of k-element subsets of X, called blocks, such that every pair of distinct points is contained in exactly λ blocks. A consequence of the definition is that a point lies in $r=(v-1)\lambda/(k-1)$ blocks and there is a total of $b=vr/k$ blocks. Sometimes we list all five parameters and talk about a (v,b,r,k,λ) design to save the reader the trouble to derive the parameters b and r.

A parallel class of a (v, k, λ) design over X is a subset of disjoint blocks whose union is X. The design $(X, \mathcal{B})$ is called resolvable if there exists a partition of $\mathcal{B}$ into parallel classes. A resolvable (v, b, r, k, λ) design consists of v/k blocks, so $v \equiv 0 \bmod k$; it has r parallel classes, because a point occurs in r blocks and each class contains a point exactly once. The reader familiar with [7] might notice that parallel classes and "striations" actually are the same objects.

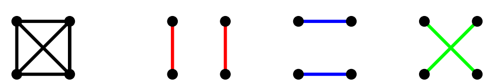
Remark. Some authors refer to our (v, k, λ) designs as simple (v, k, λ) balanced incomplete block designs, but we prefer brevity, following [13].

Affine Planes. For the second problem, we need a more general set of functions in our construction of Alice's measurement. We will obtain this set of functions from an affine plane of order n.

An $(n^2, n^2 + n, n + 1, n, 1)$ design is called an *affine plane* of order n. For affine planes, one usually uses a more geometric language and refers to blocks as lines. In other words, an affine plane of order n has n^2 points, $n^2 + n$ lines, and each line contains n points.

An affine plane of order n is the prototype of a resolvable design. It is possible to partition the set of lines into $n + 1$ parallel classes that contain n disjoint (parallel) lines each. A small example might help to convey the main idea.

Example 1. *The affine plane of order* 2 *consists of a set of* 4 *points and a family of 6 lines. The figure below illustrates this affine plane:*



The three parallel classes of this affine plane are depicted on the right in the colors red, blue, and green. Put differently, it is a $(4, 2, 1)$ *design* $(X, \mathcal{B})$ *with four points* $X = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ *and six lines* $\mathcal{B} = L_0 \cup L_1 \cup L_2$ *given as a union of the three parallel classes*

$$\begin{aligned} L_0 &= \{\{(1, 1), (1, 2)\}, \{(2, 1), (2, 2)\}\}, \\ L_1 &= \{\{(1, 1), (2, 1)\}, \{(1, 2), (2, 2)\}\}, \\ L_2 &= \{\{(1, 1), (2, 2)\}, \{(1, 2), (2, 1)\}\}. \end{aligned}$$

Functions. We will now derive a set of n^2 functions from an affine plane of order n. As a guiding example, we will see how the four functions $f_1, \ldots, f_4$ from the first section can be derived from Example 1.

Let $X = \{(x, y) \,|\, 1 \leq x, y \leq n\}$ be a set of n^2 points. Suppose that $(X, \mathcal{B})$ is an affine plane of order n. We denote by $L_0, \ldots, L_n$ the $n + 1$ parallel classes of lines that partition the set of lines, $\mathcal{B} = L_0 \cup L_1 \cup \cdots \cup L_n$.

Without loss of generality, we assume that the lines in the parallel class L_0 are given by

$$\ell_x = \{(x,y) \,|\, 1 \leq y \leq n\}, \quad \text{where} \quad x \in \{1,\dots,n\}.$$

Indeed, we can always achieve this by renaming the points in X.

Recall that two lines from different parallel classes meet in one point. In particular, if we choose a line ℓ that is not contained in L_0, then $\ell \cap \ell_x \neq \emptyset$ for all $1 \leq x \leq n$. Therefore, for each x in the range $1 \leq x \leq n$ there exists an integer y_x such that $(x, y_x) \in \ell$.

Given a parallel class L_i, with $1 \leq i \leq n$, and a line ℓ in L_i, we define a function $f_{i,\ell}\colon \{0,1,\dots,n\} \to \{1,\dots,n\}$ by

$$f_{i,\ell}(a) = \begin{cases} i & \text{if } a = 0 \\ b & \text{if } (a,b) \in \ell, a \neq 0 \end{cases}$$

Our convention for labeling the points in X ensures that this function is defined for all $a \in \{0,\dots,n\}$.

We denote by $\Delta_{f,g}$ the collision set of two functions f and g, defined by

$$\Delta_{f,g} = \{x \mid f(x) = g(x)\}.$$

Lemma 1. *If $f, g \in \{f_{i,\ell} \mid 1 \leq i \leq n, \ell \in L_i\}$ are distinct functions, then the functions have exactly one collision, $|\Delta_{f,g}| = 1$.*

Proof: Suppose that $f = f_{i,\ell}$ and $g = f_{i^*,\ell^*}$. If $i = i^*$, then ℓ and ℓ^* are parallel lines; hence, $f(a) \neq g(a)$ for $1 \leq a \leq n$, and a single collision is given by $f(0) = g(0) = i$.

If $i \neq i^*$, then $f(0) \neq g(0)$. Furthermore, ℓ and ℓ' are lines from distinct parallel classes, so ℓ and ℓ' have exactly one point in common; hence, f and g have once again one collision. □

Example 1 (cont'd). *In the affine plane of order 2, we choose the parallel class $L_1 = \{\ell_1, \ell_2\}$ that consists of the lines $\ell_1 = \{(1,1),(2,1)\}$ and $\ell_2 = \{(1,2),(2,2)\}$. The associated functions $f_1 = f_{1,\ell_1}$ and $f_2 = f_{1,\ell_2}$ are given by*

$$\begin{array}{lll} f_{1,\ell_1}(0) = 1, & f_{1,\ell_1}(1) = 1, & f_{1,\ell_1}(2) = 1, \\ f_{1,\ell_2}(0) = 1, & f_{1,\ell_2}(1) = 2, & f_{1,\ell_2}(2) = 2. \end{array}$$

Reconstruction. We will now derive an orthonormal basis of $\mathbf{C}^n \otimes \mathbf{C}^n$. The basis is determined by the n^2 functions that we have obtained in Lemma 1 from an affine plane. It turns out that this basis allows Alice to extract all necessary information so that she can guess the value that has been observed by the King's men with certainty.

Let $B_a = \{v_{a,b} \,|\, 0 \leq b < n\}$, with $0 \leq a \leq n$, denote a set of $n+1$ mutually unbiased bases [12,22] of $\mathbf{C}^n$; that is, each set B_a is an orthonormal basis of $\mathbf{C}^n$ and the squared-modulus of the inner product between vectors of different bases satisfies $|\langle v_{a,b}|v_{a',b'}\rangle|^2 = 1/n$ for $a \neq a'$ and all b and b'. Given a function $f\colon \{0,\dots,n\} \to \{1,\dots,n\}$, we define the vectors

$$\varphi = \frac{1}{\sqrt{n}} \sum_{b=1}^{n} v_{0,b} \otimes \overline{v_{0,b}}\,, \qquad \gamma_f = \frac{1}{\sqrt{n}} \sum_{a=0}^{n} v_{a,f(a)} \otimes \overline{v_{a,f(a)}},$$

and $\psi_f = -\varphi + \gamma_f$.

Lemma 2. *Let $f, g : \{0,1,\dots,n\} \to \{1,\dots,n\}$ be functions and denote by ψ_f and ψ_g the associated vectors in $\mathbf{C}^n \otimes \mathbf{C}^n$. The inner product $\langle \psi_f|\psi_g\rangle = 0$ if and only if $|\Delta_{f,g}| = 1$. Furthermore, $\langle \psi_f|\psi_f\rangle = 1$.*

Proof: If $a \neq a'$ then $\langle v_{a,b} \otimes \overline{v_{a,b}}|v_{a',b'} \otimes \overline{v_{a',b'}}\rangle = 1/n$. Furthermore, we note that $\langle v_{a,b} \otimes \overline{v_{a,b}}|\varphi\rangle = 1/\sqrt{n}$ for $0 \leq a \leq n$ and $1 \leq b \leq n$. We obtain

$$\begin{aligned} \langle \psi_f|\psi_g\rangle &= \langle \varphi|\varphi\rangle - \langle \varphi|\gamma_g\rangle - \langle \gamma_f|\varphi\rangle + \langle \gamma_f|\gamma_g\rangle \\ &= 1 - 2\frac{(n+1)}{n} + \frac{1}{n}\sum_{a=0}^{n}\sum_{a'=0}^{n} |\left\langle v_{a,f(a)}|v_{a',g(a')}\right\rangle|^2 \\ &= 1 - 2\frac{(n+1)}{n} + \frac{1}{n}\left(|\Delta_{f,g}| \cdot 1 + n(n+1) \cdot \frac{1}{n}\right) \\ &= \frac{n - 2(n+1) + |\Delta_{f,g}| + n + 1}{n} = \frac{|\Delta_{f,g}| - 1}{n}. \end{aligned} \tag{1}$$

Hence, $\langle \psi_f|\psi_g\rangle = 0$ if and only if $|\Delta_{f,g}| = 1$. Furthermore, from this we also obtain that $\langle \psi_f|\psi_f\rangle = 1$. □

Corollary 3. *If a complete set of $n+1$ mutually unbiased bases exists in $\mathbf{C}^n$ and an affine plane of order n exists, then there exist a set S of n^2 functions $\{0,1,\dots,n\} \to \{1,\dots,n\}$ such that*

$$\{\psi_f \,|\, f \in S\}$$

forms an orthonormal basis of $\mathbf{C}^n \otimes \mathbf{C}^n$.

Proof: If an affine plane exists, then Lemma 1 shows that n^2 functions that have exactly one collision in common. It follows from Lemma 2 that the corresponding states form an orthonormal basis of $\mathbf{C}^n \otimes \mathbf{C}^n$. □

The crucial property of a von Neumann measurement with respect to the basis $\{\psi_f \mid f \in S\}$ is that one can extract information from the state returned by the King's men thanks to the following lemma:

Lemma 4. *$\langle v_{a,b} \otimes \overline{v_{a,b}} | \psi_f \rangle \neq 0$ if and only if $f(a) = b$.*

Proof: By definition of ψ_f, we have

$$\begin{aligned} \langle v_{a,b} \otimes \overline{v_{a,b}} | \psi_f \rangle &= -\langle v_{a,b} \otimes \overline{v_{a,b}} | \varphi \rangle + \frac{1}{\sqrt{n}} \sum_{a'=0}^{n} |\langle v_{a,b} | v_{a',f(a')} \rangle|^2 \\ &= -\frac{1}{\sqrt{n}} + \frac{n}{\sqrt{n}} \times \frac{1}{n} + \frac{1}{\sqrt{n}} [f(a) = b], \end{aligned}$$

where the last expression is the Iverson-Knuth bracket that is 1 if $f(a) = b$ and 0 otherwise. □

Remark. If n is a power of a prime, then there exists both an affine plane of order n and a maximal set of $n+1$ mutually unbiased bases; see, for instance, [4, 18] and [12, 22]. If n is not a power of a prime, then neither an affine plane of order n nor $n+1$ mutually unbiased bases are known to exists. There exist some speculations that a set of $n+1$ mutually unbiased bases exist in $\mathbf{C}^n$ if and only if an affine plane of order n exists, but there is little evidence in support of such a claim and it is doubtful whether one should elevate this to a conjecture.

Summary. Let $B_a = \{v_{a,b} \mid 0 \leq b < n\}$, with $0 \leq a \leq n$, denote a set of $n+1$ mutually unbiased bases. Suppose that the King's men will perform a von Neumann measurement with respect to one of the $n+1$ bases. Then Alice can guess the outcome of the measurement by the following procedure:

- Alice starts by preparing the state

$$\varphi = \frac{1}{\sqrt{n}} \sum_{b=1}^{n} v_{a,b} \otimes \overline{v_{a,b}}.$$

  Note that we obtain the same state for each a in $0 \leq a \leq n$.

- The King's men perform a measurement with respect to one basis B_a. Suppose that the result is b, then the state collapses to $v_{a,b} \otimes \overline{v_{a,b}}$. The King's men hand the atom back to Alice but do not yet reveal the measurement basis nor the outcome of the measurement.

- Alice performs a von Neumann measurement on $\mathbf{C}^n \otimes \mathbf{C}^n$ with respect to the basis $\{\psi_f \mid f \in S\}$ given in Corollary 3. By Lemma 4, we have $\langle v_{a,b} \otimes \overline{v_{a,b}} | \psi_f \rangle \neq 0$ if and only if $f(a) = b$. Put differently, the outcome of Alice's measurement is a function f such that $f(a) = b$.

- Finally, the King's men reveal the label a of the basis B_a.
- Alice can respond with the value b such that $f(a) = b$, and the outcome b is exactly what the King's men have observed.

Theorem 5. *If an affine plane of order n and a set of $n + 1$ mutually unbiased bases in $\mathbf{C}^n$ exist, then Alice can solve the second problem of the King with certainty.*

The Third Problem

Having successfully solved the King's problems, Alice assumed that she might now leave the island and return home to safety. The King on the other hand was frustrated since his challenges have been solved so easily. He lamented for several days and finally told his woes to his wife. What she conveyed to him came as a big surprise: Envious of the gifted physicist who spends so much quality time with her husband, she had sent a spy to Alice's chamber to observe her experiments. The spy reported that some part of Alice's state actually remained in Alice's lab and was later used for the reconstruction of the King's measurement.

Furious with anger about this trickery, the King arrested Alice once again and gave her a new challenge. She has to prepare a quantum state of her own liking involving three silver atoms. They have to be handed over to the King and she would not be allowed to have any quantum state left in her possession which could be entangled with the three atoms. Then the King secretly picks an arbitrary one of these atoms and measures it either one of three complementary bases. Subsequently, the state is returned to Alice, who is allowed to perform one experiment on it. Afterwards, the King reveals which bit has been measured and Alice immediately has to answer with the correct outcome or else she will die an even more cruel death.

We now turn to a generalization of the Mean King's problem where the vectors do not necessarily come in groups of mutually unbiased bases and in which we consider more general combinatorial designs than affine planes.

Affine Resolvable Designs. For a general design no restriction is made about the number of points in which two blocks can intersect. A particularly interesting case arises when any two blocks either intersect in the same number of points or do not intersect at all.

A (v, k, λ) design is called an *affine resolvable design*, or simply an *affine design*, if it is a resolvable design and any two nonparallel blocks intersect at a fixed number m of points.

Lemma 6. *Let $(X, \mathcal{B})$ denote an affine (v, b, r, k, λ) design such that nonparallel blocks intersect at m points. Then the parameters satisfy the relations:*

(i) $m = k^2/v$;
(ii) $\lambda(v-k) = k(k-1)$;
(iii) $r = k + \lambda$;
(iv) $b = v + r - 1$.

Proof: The relations are standard facts about the parameters of affine designs, see [4, 18, 21]. □

In the Euclidean plane there is exactly one line which passes through a given point and is parallel with a fixed line; we need the combinatorial analogue of this geometric fact.

Lemma 7. *Let $(X, \mathcal{B})$ be an affine resolvable design, $B \in \mathcal{B}$ and $p \in X$ a point such that $p \notin B$. There exists precisely one block $C \in \mathcal{B}$ such that $B \cap C = \emptyset$ and $p \in C$.*

Proof: Since X is resolvable, we have a resolution of the blocks in $\mathcal{B}$ into parallel classes. The block B is contained in one parallel class, say in $\mathcal{C}$. Each parallel class partitions X; hence, there is a block $C_0 \in \mathcal{C}$ such that $p \in C_0$. Since $p \notin B$, it follows that $B \cap C_0 = \emptyset$.

Seeking a contradiction, we suppose that there is another block $C_1 \in \mathcal{B}$ with $C_1 \neq C_0$ such that $p \in C_1$ and $B \cap C_1 = \emptyset$. Since C_0 and C_1 are both parallel to B they have to be in the same parallel class; hence, $C_0 \cap C_1 = \emptyset$ in contradiction to $p \in C_0 \cap C_1$. □

Examples. Basically two constructions of affine resolvable designs are known: designs coming from affine geometries and Hadamard designs. The following table summarizes the properties of these two classes:

Design	v	b	r	k	λ
Affine plane	q^2	q^2+q	$q+1$	q	1
Affine space	q^m	$q^{m-d}\left[{m \atop d}\right]_q$	$\left[{m \atop d}\right]_q$	q^d	$\left[{m-1 \atop d-1}\right]_q$
Hadamard designs	$4m$	$8m-2$	$4m-1$	$2m$	$2m-1$

Table 1 Parameters of affine designs. In this table $m \geq 1$ and $1 \leq d < m$. The Gaussian q-binomial coefficient $\left[{m \atop d}\right]_q$ equals the number of d-dimensional subspaces of $\mathbb{F}_q^m$, see [14]. Constructions for affine planes and spaces with the parameters given in this table are known when q is a power of a prime; it is conjectured that Hadamard designs exist for all $m \geq 1$.

Representation. In the following, we will relate the discrete combinatorial structures to vectors in a finite dimensional Hilbert space. This is in the same spirit as the "quantum nets" introduced in [7], where a map between the blocks of a design to vectors in Hilbert space with prescribed inner products was used to define a discrete Wigner transform (see also [6, 15–17]).

Let $(X, \mathcal{B})$ be an affine (v, b, r, k, λ) design. We associate with each block B in $\mathcal{B}$ a vector of unit norm in $\mathbf{C}^v$, and we denote this vector by $|B\rangle$. We encode the information about the parallel classes of the design in the angles between the vectors. We require from the vectors $|B\rangle$ with $B \in \mathcal{B}$ that they satisfy

$$\langle B|C\rangle = \begin{cases} \delta_{B,C} & \text{if } B \text{ and } C \text{ are parallel,} \\ k/v & \text{if } B \text{ and } C \text{ are not parallel.} \end{cases} \tag{2}$$

We will call a vector system $\{|B\rangle \,|\, B \in \mathcal{B}\}$ that satisfies the constraints (2) a *realization* of the affine design $(X, \mathcal{B})$.

Lemma 8. *An affine (v, k, λ) design $(X, \mathcal{B})$ has a realization in $\mathbf{C}^v$.*

Proof: Suppose that v_B is the incidence vector of the block B. Then $|B\rangle = \frac{1}{\sqrt{k}} v_B$, with $B \in \mathcal{B}$, is a realization of X in $\mathbf{C}^v$. □

Example 2. *Let n be a power of a prime, and let $(X, \mathcal{B})$ be an affine plane of order n. Suppose that $\mathcal{B}$ is the disjoint union of the parallel classes L_m, $\mathcal{B} = L_0 \cup \cdots \cup L_n$. Let $B_a = \{v_{a,b} \,|\, 1 \leq b \leq n\}$, with $0 \leq a \leq n$, denote a set of $n+1$ mutually unbiased bases of $\mathbf{C}^n$. Suppose that the parallel class L_a is given by the set of lines $L_a = \{\ell_{a,b} \,|\, 1 \leq b \leq n\}$. If we define*

$$|\ell_{a,b}\rangle = v_{a,b} \otimes \overline{v_{a,b}} \in \mathbf{C}^{n^2}, \tag{3}$$

then $\langle \ell_{a,b} | \ell_{a',b'} \rangle = 1/n = n/n^2$ if the lines are from different parallel classes, $L_a \neq L_{a'}$; and $\langle \ell_{a,b} | \ell_{a,b'} \rangle = \delta_{b,b'}$ for parallel lines. The vectors in (3) are a realization of the affine plane in $\mathbf{C}^{n^2}$.

Reconstruction. We saw in the previous two sections how one can explore properties of the previous example to solve the first two problems of the Mean King. A far reaching generalization is provided by the realizations of affine designs. We begin with a generalization of Corollary 3.

Theorem 9. *Let $(X, \mathcal{B})$ be an affine (v, b, r, k, λ) design. Suppose that $\mathcal{C}$ is an arbitrary parallel class of X, and $\{|B\rangle : B \in \mathcal{B}\}$ a realization of X in $\mathbf{C}^v$. If we define*

$$|\psi_p\rangle = -\alpha \left(\sum_{B \in \mathcal{C}} |B\rangle \right) + \beta \left(\sum_{B : p \in B} |B\rangle \right), \tag{4}$$

with $\alpha = (r-1)\sqrt{k}/v$ and $\beta = 1/\sqrt{k}$, then $\{|\psi_p\rangle : p \in X\}$ forms an orthonormal basis of $\mathbf{C}^v$.

Proof: Let p, q be two arbitrary points in X. Before we compute the inner product of the states $|\psi_p\rangle$ and $|\psi_q\rangle$ we first consider the following intersection scenarios.

Let $P = \{B \in \mathcal{B} \,|\, p \in B\}$ and $Q = \{C \in \mathcal{B} \,|\, q \in C\}$. We shall be interested in the inner products $\langle B|C\rangle$ with $B \in P$ and $C \in Q$. Since each point is incident with r blocks, we obtain precisely r^2 such pairs. In the case $p \neq q$, we get

a) $\langle B|C\rangle = k/n$ for $r(r-1)$ pairs (B,C), since there are $r(r-1)$ ways to choose pairs (B,C) such that B and C belong to different parallel classes;

b) $\langle B|B\rangle = 1$ for λ pairs $(B,B) = (B,C)$, since there are λ blocks B in the intersection $P \cap Q$;

c) $\langle B|C\rangle = 0$ for the remaining $r - \lambda$ pairs (B,C) that are in the same parallel class, but satisfy $B \cap C = \emptyset$.

In the case $p = q$, we obtain

a) $\langle B|B\rangle = 1$ for r pairs of the form $(B,B) = (B,C)$, where B and C belong to the same parallel class.

b) $\langle B|C\rangle = k/n$ for the remaining $r(r-1)$ pairs, where B and C belong to different parallel classes.

Suppose that we have a point p and a parallel class $\mathcal{C}$. We are interested in the values of the inner products $\langle B|C\rangle$ of pairs (B,C) with $B \in P$ and $C \in \mathcal{C}$. Since the parallel class $\mathcal{C}$ contains v/k blocks, we obtain rv/k such pairs, and

a) $\langle B|C\rangle = 1$ for one pair $(B,B) = (B,C)$ with $B \in \mathcal{C}$;

b) $\langle B|C\rangle = 0$ for the $v/k - 1$ pairs (B,C) with $B \in \mathcal{C}$ and $B \cap C = \emptyset$;

c) $\langle B|C\rangle = k/n$ for the remaining $(r-1)v/k$ pairs with $B \notin \mathcal{C}$.

These design-theoretic arguments enable us to compute the inner product $\langle \psi_p|\psi_q\rangle$ of two states,

$$\begin{aligned}
\langle \psi_p|\psi_q\rangle &= \alpha^2 \sum_{B,B' \in \mathcal{C}} \langle B|B'\rangle - 2\alpha\beta \sum_{B \in \mathcal{C}} \sum_{B': p \in B'} \langle B|B'\rangle + \beta^2 \sum_{B: p \in B} \sum_{B': q \in B'} \langle B|B'\rangle \\
&= \alpha^2 \left(\frac{v}{k}\right) - 2\alpha\beta \left(1 + \left(\frac{v}{k} - 1\right) \cdot 0 + \frac{v}{k}(r-1)\frac{k}{v}\right) \\
&\qquad + \begin{cases} \beta^2 \left(\lambda + (r-\lambda) \cdot 0 + (r^2 - r)\frac{k}{v}\right) & \text{if } p \neq q, \\ \beta^2 \left(r + (r^2 - r)\frac{k}{v}\right) & \text{if } p = q. \end{cases}
\end{aligned}$$

We now solve this for α and β with respect to the constraints $\langle \psi_p|\psi_q\rangle = \delta_{p,q}$ and show that the given values for α and β indeed are solutions.

Subtracting the first equation from the second yields $\beta^2(r-\lambda) = 1$. We know from Lemma 6 (iii) that $k = r - \lambda$; hence, $\beta = 1/\sqrt{k}$. Therefore, the quadratic equation for α simplifies to

$$\left(\frac{v}{k}\right)\alpha^2 - \left(\frac{2r}{\sqrt{k}}\right)\alpha + \left(\frac{\lambda}{k} + \frac{r^2-r}{v}\right) = 0.$$

Solving for α, we obtain

$$\begin{aligned}
\alpha_{1,2} &= \left(\frac{2r}{\sqrt{k}} \pm \sqrt{\frac{4r^2}{k} - 4\frac{v}{k}\left(\frac{\lambda}{k} + \frac{r^2-r}{v}\right)}\right)\Big/\left(\frac{2v}{k}\right) \\
&= \left(\frac{2r}{\sqrt{k}} \pm \sqrt{-4\frac{v\lambda}{k^2} + 4\frac{r}{k}}\right)\Big/\left(\frac{2v}{k}\right)
\end{aligned}$$

By Lemma 6 (ii), we have $v\lambda = k\lambda + k(k-1)$. If we subsitute this relation into the previous expression, then we can simplify the solution further by taking the relation $k = r - \lambda$ into account:

$$\begin{aligned}
\alpha_{1,2} &= \left(\frac{2r}{\sqrt{k}} \pm \sqrt{-\frac{4(\lambda k + k(k-1))}{k^2} + 4\frac{r}{k}}\right)\Big/\left(\frac{2v}{k}\right) \\
&= \left(\frac{2r}{\sqrt{k}} \pm \sqrt{\frac{4}{k}(r-\lambda) - 4\frac{k-1}{k}}\right)\Big/\left(\frac{2v}{k}\right) \\
&= \frac{2}{\sqrt{k}}(r \pm 1)\frac{k}{2v} = \frac{\sqrt{k}}{v}(r \pm 1).
\end{aligned}$$

Since we have chosen $\alpha = (r-1)\sqrt{k}/v$ and $\beta = 1/\sqrt{k}$, it follows from our calculation that $\{|\psi_p\rangle \,|\, p \in X\}$ is an orthonormal basis of $\mathbf{C}^v$. □

A remarkable property of the basis given in the previous theorem is that if we measure a state $|B\rangle$, with $B \in \mathcal{B}$, then we will only observe points p that are incident with B, that is, the state $|B\rangle$ can only collapse to $|\psi_p\rangle$ with $p \in B$. The reader should contrast the next theorem with Lemma 4, which serves the same purpose in the case of affine planes.

Theorem 10. *Let $(X, \mathcal{B})$ be an affine (v, b, r, k, λ) design. Suppose that $\{|B\rangle : B \in \mathcal{B}\}$ is a realization of X in $\mathbf{C}^v$, and let $\{|\psi_p\rangle : p \in X\}$ be the associated orthonormal basis given in Theorem 9. If $B \in \mathcal{B}$, then $\langle\psi_p|B\rangle \neq 0$ if and only if $p \in B$.*

Proof: Let $\mathcal{C}$ be an arbitrary parallel class of X. Note that the normalized state $|\varphi_{\mathcal{C}}\rangle = 1/\sqrt{|\mathcal{C}|}\sum_{B\in\mathcal{C}}|B\rangle$ has the property that $|\varphi_{\mathcal{C}}\rangle = |\varphi_{\mathcal{C}'}\rangle$

for any other parallel class $\mathcal{C}'$. Indeed, the computation of the inner product of two such states reveals that

$$\begin{aligned} \langle \varphi_{\mathcal{C}} | \varphi_{\mathcal{C}'} \rangle &= \frac{1}{|C|} \sum_{B \in \mathcal{C}} \sum_{B' \in \mathcal{C}'} \langle B | B' \rangle \\ &= \frac{1}{|C|} \cdot |C|^2 \cdot \frac{k}{v} = 1. \end{aligned}$$

Now, let $B_0 \in \mathcal{B}$ be an arbitrary block. We distinguish the two cases (i) $p \in B_0$ and (ii) $p \notin B_0$. First, in case (i) we assume that $p \in B_0$ and let $\mathcal{C}$ be the parallel class containing B. We obtain that

$$\begin{aligned} \langle \psi_p | B_0 \rangle &= -\alpha \sum_{B \in \mathcal{C}} \langle B | B_0 \rangle + \beta \sum_{B : p \in B} \langle B | B_0 \rangle \\ &= -\alpha + \beta \cdot r \cdot \frac{k}{v} = -\frac{\sqrt{k}}{v}(r-1) + \frac{rk}{\sqrt{k} v} = \frac{\sqrt{k}}{v} \neq 0. \end{aligned}$$

In case (ii) we have that $p \notin B_0$. We now apply Lemma 7 and obtain that there is precisely one block which contains p and which is disjoint from B_0. Of all the r blocks which pass through p all the other $r-1$ ones intersect nontrivially with B_0. Hence, we obtain that in this case

$$\begin{aligned} \langle \psi_p | B_0 \rangle &= -\alpha \sum_{B \in \mathcal{C}} \langle B | B_0 \rangle + \beta \sum_{B : p \in B} \langle B | B_0 \rangle \\ &= -\alpha + \beta \cdot (r-1) \cdot \frac{k}{v} - \frac{\sqrt{k}}{v}(r-1) + \frac{\sqrt{k}}{v}(r-1) = 0. \end{aligned}$$

Hence, a measurement of $|B_0\rangle$ in the basis given by the vectors $|\psi_p\rangle$ can only yield a result for values of p such that $p \in B_0$. □

Generic King's Problem. The previous two theorem are the key to a much more general class of Mean King's problems. We briefly sketch the idea of the generic version, and then illustrate it with an example in the next section. Suppose that $(X, \mathcal{B})$ is an affine (v, b, r, k, λ) design, and the vector system $\{\, |B\rangle \mid B \in \mathcal{B}\}$ is a realization of X in $\mathbf{C}^v$.

1. Alice constructs the state $\varphi = \frac{1}{\sqrt{|C|}} \sum_{B \in \mathcal{C}} |B\rangle$ for some parallel class $\mathcal{C}$.

2. Alice hands the state to the King.

3. The King's men perform a measurement on a subsystem that corresponds to one of the parallel classes $\mathcal{C}'$ of X, so that the state collapses to $|B\rangle$ with $B \in \mathcal{C}'$.

4. The King's men hand the quantum system back to Alice. And Alice performs a von Neumann measurement with respect to the basis $|\psi_p\rangle$, $p \in X$. She will only observe points p that are incident with the block B.

5. The King reveals the measurement or, equivalently, the parallel class $\mathcal{C}'$. Alice simply checks which block B' in $\mathcal{C}'$ contains the point p, and announces that block B'. The block B' derived by Alice and the block B observed by the King's men must coincide, because precisely one block of a parallel class contains p.

Step 3 is quite ambiguous and the designer of problem has considerable freedom to realize this requirement.

Solution to the Third Problem

Since Alice was very familiar with the work of Jacques Hadamard, she quickly had an idea as to which quantum state she might prepare. This time she chose an entangled state of the three atoms which has the property that no matter which of the nine measurements the King performs, the results can be distinguished from her own measurement data and the King's revelation of the basis. She passed the test with flying colours and left the island and the flabbergasted King behind.

Hadamard Designs. We denote the transpose of a matrix A by A^t. Recall that a Hadamard matrix or order n is a ± 1 matrix H_n of size $n \times n$ with the property that $H_n H_n^t = n\mathbf{1}_n$. A necessary condition for the existence of a Hadamard matrix is that either $n = 2$ or $n \equiv 0 \bmod 4$. A long-standing conjecture is that Hadamard matrices exist for all such n, but a proof is elusive; see [4, 11, 18] for a wealth of constructions of Hadamard matrices.

The Hadamard matrix $H_2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and the tensor product of Hadamard matrices is again a Hadamard matrix; hence, there exist Hadamard matrices H_{2^k} for $k \geq 1$. In particular, a Hadamard matrix for $n = 8$ is given by

$$H_8 = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{pmatrix}. \qquad (5)$$

where the entries ± 1 have been abbreviated to $+/-$. We obtain a design as follows. Define the set of points to be $X = \{1, \ldots, 8\}$. The blocks are obtained from the rows of H_8 which are different from the all-ones row.

For each row we obtain two blocks by grouping the elements which are respectively labeled "+" and "−" together. Explicitly, we obtain the blocks

$$\begin{array}{ll} B_1^+ = \{1,3,5,7\}\ , & B_1^- = \{2,4,6,8\}, \\ B_2^+ = \{1,2,5,6\}\ , & B_2^- = \{3,4,7,8\}, \\ B_3^+ = \{1,4,5,8\}\ , & B_3^- = \{2,3,6,7\}, \\ B_4^+ = \{1,2,3,4\}\ , & B_4^- = \{5,6,7,8\}, \\ B_5^+ = \{1,3,6,8\}\ , & B_5^- = \{2,4,5,7\}, \\ B_6^+ = \{1,2,7,8\}\ , & B_6^- = \{3,4,5,6\}, \\ B_7^+ = \{1,4,6,7\}\ , & B_7^- = \{2,3,5,8\}. \end{array}$$

The blocks B_i^+ and B_i^- are parallel for $1 \le i \le 7$, and blocks $B_i^\pm$ and $B_k^\pm$ with $i \neq j$ intersect in 2 points. Put differently, we have obtained an affine $(8, 14, 7, 4, 3)$ design.

Remark. If there exists a Hadamard matrix H_n of size n, then there exists an affine $(n, 2n-2, n-1, n/2, n/2-1)$ design, see [18, p. 110].

Representation. Let us define a realization of the affine $(8, 14, 7, 4, 3)$ design X in $\mathbf{C}^8$ by the vectors

$$\begin{array}{ll} |B_1^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |011\rangle), & |B_1^-\rangle = \frac{1}{\sqrt{2}}(|101\rangle + |110\rangle), \\ |B_2^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |101\rangle), & |B_2^-\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |110\rangle), \\ |B_3^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle), & |B_3^-\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |101\rangle), \end{array}$$

$$|B_4^+\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle),$$

$$|B_4^-\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle - |111\rangle),$$

$$|B_5^+\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle - i|001\rangle - i|010\rangle + |011\rangle + i|100\rangle + |101\rangle + |110\rangle + i|111\rangle),$$

$$|B_5^-\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle + i|001\rangle + i|010\rangle + |011\rangle - i|100\rangle + |101\rangle + |110\rangle - i|111\rangle),$$

$$|B_6^+\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle - i|001\rangle + i|010\rangle + |011\rangle - i|100\rangle + |101\rangle + |110\rangle + i|111\rangle),$$

$$|B_6^-\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle + i|001\rangle - i|010\rangle + |011\rangle + i|100\rangle + |101\rangle + |110\rangle - i|111\rangle),$$

$$|B_7^+\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle + i|001\rangle - i|010\rangle + |011\rangle - i|100\rangle + |101\rangle + |110\rangle + i|111\rangle),$$

$$|B_7^-\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle - i|001\rangle + i|010\rangle + |011\rangle + i|100\rangle + |101\rangle + |110\rangle - i|111\rangle).$$

Recall that the parallel classes $\mathcal{C}_k$ of the design X are given by $\mathcal{C}_k = \{B_k^+, B_k^-\}$ for $1 \le k \le 7$. One can check that

$$\langle B_i^+|B_i^-\rangle = 0, \quad \langle B_i^+|B_j^-\rangle = 1/2, \quad \langle B_i^+|B_j^+\rangle = 1/2, \quad \langle B_i^-|B_j^-\rangle = 1/2,$$

holds for distinct i and j in the range $1 \leq i, j \leq 7$, so the system of vectors forms indeed a realization of the affine $(8, 14, 7, 4, 3)$ design X.

The King's Measurements. Alice prepares the state

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|B_k^+\rangle + |B_k^-\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle). \tag{6}$$

We note that $|\varphi\rangle$ can be obtained from the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ by applying a Hadamard gate to each qubit [8].

The King can perform nine different measurements; namely, he can measure one of the three spin components of either the first, second, or third qubit. The three measurements are performed with respect to standard basis B_s, the Hadamard basis B_h or a third complementary basis B_u; explicitly,

$$B_s = \big\{|0\rangle, |1\rangle\big\}, \quad B_h = \big\{\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle, \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle\big\},$$
$$B_u = \big\{\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{i}{\sqrt{2}}|1\rangle, \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{i}{\sqrt{2}}|1\rangle\big\}.$$

The corresponding projectors on one qubit are respectively given by

$$\begin{aligned} P_s^+ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, & P_s^+ &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \\ P_h^+ &= \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, & P_h^- &= \tfrac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \\ P_u^+ &= \tfrac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, & P_u^- &= \tfrac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}. \end{aligned}$$

It is straightforward to verify that the nine measurements corrspond the seven parallel classes $\mathcal{C}_1, \dots, \mathcal{C}_7$ as follows: A measurement in the standard basis on qubit k amounts to applying P_s^+ or P_s^- to any of the three qubits and collapses $|\varphi\rangle$ to either $|B_k^+\rangle$ or $|B_k^-\rangle$, where $k \in \{1, 2, 3\}$. The three Hadamard measurements amount to applying P_h^+ or P_h^- and map the state $|\varphi\rangle$ either to $|B_4^+\rangle$ or to $|B_4^-\rangle$. Finally, the three measurements in the basis B_u amount to applying P_u^+ or P_u^- and map the state $|\varphi\rangle$ to either $|B_k^+\rangle$ or $|B_k^-\rangle$, where $k \in \{5, 6, 7\}$. Table 2 summarizes the King's measurement outcomes.

Alice's Measurement. The key to Alice's success is that she devices a measurement that allows her to infer a point p that is incident with the block that the King's men have measured. If the King later reveals the measurement, or parallel class, then Alice simply needs to identify the block that contains p.

Measurement	Outcome “0”	Outcome “1”
$M_{1,s}$	$\lvert B_1^+\rangle$	$\lvert B_1^-\rangle$
$M_{2,s}$	$\lvert B_2^+\rangle$	$\lvert B_2^-\rangle$
$M_{3,s}$	$\lvert B_3^+\rangle$	$\lvert B_3^-\rangle$
$M_{1,h}$, $M_{2,h}$, $M_{3,h}$	$\lvert B_4^+\rangle$	$\lvert B_4^-\rangle$
$M_{1,u}$	$\lvert B_5^+\rangle$	$\lvert B_5^-\rangle$
$M_{2,u}$	$\lvert B_6^+\rangle$	$\lvert B_6^-\rangle$
$M_{3,u}$	$\lvert B_7^+\rangle$	$\lvert B_7^-\rangle$

Table 2 The table shows the resulting states after measuring $|\varphi\rangle$ in one of the nine different bases. We use $M_{k,s}$ to denote that the kth qubit has been measured with respect to the standard basis B_s, we use $M_{k,h}$ to denote that the kth qubit has been measured with respect to the Hadamard basis B_h, and we denote $M_{k,u}$ to denote that the kth qubit has been measured with respect to the third complementary basis B_u. Note that the resulting states for $M_{1,h}$, $M_{2,h}$, and $M_{3,h}$ are the same.

Alice can use Theorem 9 to construct a suitable orthonormal basis. Since the parameters of our design are $v = 8$, $r = 7$, and $k = 4$, we find that $\alpha = (r-1)\sqrt{k}/v = 3/2$ and $\beta = 1/\sqrt{k} = 1/2$. We can compute the states

$$|\psi_p\rangle = -\frac{3}{2}\left(\sum_{B\in\mathcal{C}} |B\rangle\right) + \frac{1}{2}\left(\sum_{B:p\in B} |B\rangle\right).$$

Explicitly, we get

$$|\psi_{1,5}\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |001\rangle), \quad |\psi_{2,6}\rangle = \frac{1}{\sqrt{2}}(|110\rangle \pm |100\rangle),$$

$$|\psi_{3,7}\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |010\rangle), \quad |\psi_{4,8}\rangle = \frac{1}{\sqrt{2}}(|101\rangle \pm |111\rangle).$$

The result obtained from this measurement corresponds to a point $p \in \{1,\ldots,8\}$. If now the King reveals his measurement, i. e., discloses which qubit was measured and if the standard basis or Hadamard basis was used, then this uniquely specifies a parallel class $\mathcal{C}_1,\ldots,\mathcal{C}_7$. Now, the correct outcome “0” or “1” of the King's measurement is given by the unique block B in this class, such that $p \in B$.

For instance, starting from $|\varphi\rangle$, assume that the King decides the measure the second qubit in the Hadamard basis. Assume that his measurement result was “1”. Then the state has collapsed to $|B_4^-\rangle$, where $B_4^- = \{5,6,7,8\}$. Alice will now measure one of $|\psi_5\rangle$, $|\psi_6\rangle$, $|\psi_7\rangle$, $|\psi_8\rangle$, the other states do not occur in her measurement. Now, if the King discloses that he performed a measurement of the second qubit in the Hadamard basis, then Alice knows that this measurement yields either $|B_4^+\rangle$ or $|B_4^-\rangle$. The point p that Alice had measured is an element of $\{5, 6, 7, 8\}$, and either choice yield the block B_4^-, the block corresponding to the result "1".

Acknowledgments. The research of A.K. was supported by NSF CAREER award CCF-0347310, NSF grant CCR-0218582, a TEES Select Young Faculty award, and a Texas A&M TITF grant. This work was carried out while M.R. was at the Institute for Quantum Computing, University of Waterloo, Canada.

We thank Thomas Beth, Mauro D'Ariano, Ernesto Galvao, Chris Godsil, Markus Grassl, and Aidan Roy several interesting discussions. A very special thanks to Yannis Haralambous for designing such beautiful fonts!

We apologize for taking the typographical liberty to typeset **paſſable** as **passable**, but we found that most readers have difficulties to **diſtinguiſh** the former version from **paffable**.

References

[1] Y. Aharonov and B.-G. Englert. The mean king's problem: Prime degrees of freedom. *Physics Letters A*, 284:1–5, 2001.

[2] Y. Aharonov and B.-G. Englert. The mean king's problem: Spin 1. *Zeitschrift für Naturforschung A*, 56a:16–19, 2003.

[3] P. K. Aravind. Solution to the King's Problem in prime power dimensions. *Zeitschrift für Naturforschung A*, 58a:85–92, 2003.

[4] Th. Beth, D. Jungnickel, and H. Lenz. *Design Theory*, volume I of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, 2nd edition, 1999.

[5] Th. Durt. Bell states, mutually unbiased bases, and the mean kings's problem. ArXiv preprint quant–ph/0401037, 2004.

[6] E. Galvao. Discrete Wigner functions and quantum computational speed-up. ArXiv preprint quant–ph/0405070, 2004.

[7] K. S. Gibbons, M. J. Hoffman, and W. Wootters. Discrete phase space based on finite fields. ArXiv preprint quant–ph/0401155, 2003.

[8] D. Greenberger, M. Horne, and A. Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, pages 73–76. Kluwer, Dordrecht, 198.

[9] A. Hayashi, M. Horibe, and T. Hashimoto. The King's problem with mutually unbiased bases and orthogonal latin squares. ArXiv preprint quant–ph/0502092.

[10] A. Hayashi, M. Horibe, and T. Hashimoto. Solution to the King's problem with observables being not mutually complementary. ArXiv preprint quant–ph/0410206.

[11] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays – Theory and Applications*. Springer, 1999.

[12] I. D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A*, 14(12):3241–3245, 1981.

[13] S. Jukna. *Extremal Combinatorics*. Springer, 2001.

[14] V. Kac and P. Cheung. *Quantum Calculus*. Springer, 2002.

[15] J. P. Paz. Discrete Wigner functions and the phase space representation of quantum teleportation. ArXiv preprint quant–ph/0204150, 2002.

[16] J. P. Paz, A. J. Roncaglia, and M. Saraceno. Qubits in phase space: Wigner function approach to quantum error correction and the mean king problem. ArXiv preprint quant–ph/0410117, 2004.

[17] A. O. Pittenger and M. H. Rubin. Wigner Functions and Separability for Finite Systems. ArXiv preprint quant–ph/0501104, 2005.

[18] D. Stinson. *Combinatorial Designs*. Springer, 2003.

[19] L. Vaidman, Y. Aharonov, and D. Z. Albert. How to ascertain the values of σ_x, σ_y, and σ_z of a spin-$\frac{1}{2}$ particle. *Phys. Rev. Letters*, 58:1385–1387, 1987.

[20] J. H. van Lindt and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 2nd edition, 2001.

[21] W. D. Wallis. *Combinatorial Designs*. Marcel Dekker, Inc., 1988.

[22] W. Wootters and B. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191(2):363–381, 1989.

[*]Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA, `klappi <at-sign> cs.tamu.edu`

[†]NEC Laboratories America, Inc., 4 Independence Way, Princeton, NJ 08540, USA, `mroetteler <at-sign> nec-labs.com`

Summary. The Mean King's problem asks to determine the outcome of a measurement that is randomly selected from a set of complementary observables. We review this problem and offer a combinatorial solution. More generally, we show that whenever an affine resolvable design exists, then a state reconstruction problem similar to the Mean King's problem can be defined and solved. As an application of this general framework we consider a problem involving three qubits in which the outcome of nine different measurements can be determined without using ancillary qubits. The solution is based on a measurement derived from Hadamard designs.