Chapter 5
Finite Geometries and Mutually Unbiased Bases

Abstract Finite geometries, mutually unbiased bases, and weak mutually unbiased bases, are discussed.

In this section we first discuss the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a finite geometry [1–3], and its link to the subject of mutually unbiased bases [4–22]. There are deep mathematical problems related to these bases, and they also have important applications in quantum communications and quantum cryptography. For these reasons, they have been studied extensively in the literature.

We make the distinction between two cases:

- $d = p$, where p is a prime number. In this case, $\mathbb{Z}(p)$ is a field. $\mathbb{Z}(p) \times \mathbb{Z}(p)$ is a near-linear finite geometry, based on the axiom that two lines have at most one point in common. The number of mutually unbiased bases is $p + 1$ and there is a duality between the finite geometry and the mutually unbiased bases. These results can be extended to the case that $d = p^e$, using the Galois field $GF(p^e)$, as discussed later in Sect. 9.7.
- d is not a prime number. In this case, $\mathbb{Z}(d)$ is a ring. $\mathbb{Z}(d) \times \mathbb{Z}(d)$ is a non-near-linear finite geometry, and two lines might have more than one point in common (the axiom that two lines have at most one point in common does not hold). The number of mutually unbiased bases is not known, but it is probably smaller than $d+1$ (although there is no rigorous proof of this). Here there is no duality between the finite geometry and the mutually unbiased bases. Motivated by this, Refs. [23–26] have introduced weak mutually unbiased bases, which are dual to lines in the finite geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$. In order to avoid a complex notation, and without loss of generality, we discuss the case with $d = p_1 p_2$, where p_1, p_2 are odd prime numbers, different from each other.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science
and Technology, DOI 10.1007/978-3-319-59495-8_5

5.1 The $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a Non-near-linear Finite Geometry

A finite geometry [1–3] is a finite set P of points, and a set L of some subsets of P which are called lines. In our context, $P = \mathbb{Z}(d) \times \mathbb{Z}(d)$. The geometry (P, L) satisfies certain axioms. A special class of finite geometries are the near-linear geometries, with the axiom that two lines have at most one point in common. We will see below, that this axiom is valid when d is a prime number (in which case $\mathbb{Z}(d)$ is a field), but it is not valid when d is not a prime number (in which case $\mathbb{Z}(d)$ is a ring). Therefore our geometry is a non-near-linear geometry, in the case of non-prime d.

A line through the point (α, β) is the set of points

$$L(\rho, \sigma|\alpha, \beta) = \{(\tau\rho + \alpha, \tau\sigma + \beta)|\tau \in \mathbb{Z}(d)\}; \quad \rho, \sigma, \alpha, \beta \in \mathbb{Z}(d) \tag{5.1}$$

Below we only consider lines through the origin (0, 0), which we denote as $L(\rho, \sigma)$:

$$L(\rho, \sigma) = \{(\tau\rho, \tau\sigma)|\tau \in \mathbb{Z}(d)\}. \tag{5.2}$$

Mathematically this is a cyclic module generated by (ρ, σ), but in a physical context we will use the intuitive term line. In this section we present three propositions which describe $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a finite geometry [23–26].

Proposition 5.1 *(1) The number of points in $L(\rho, \sigma)$ is $d/\mathrm{GCD}(\rho, \sigma, d)$. We call maximal lines the ones with d points (i.e., the lines with $\mathrm{GCD}(\rho, \sigma, d) = 1$).*

(2) If λ is an invertible element in $\mathbb{Z}(d)$ ($\lambda \in [\mathbb{Z}(d)]^*$), then $L(\rho\lambda, \sigma\lambda) = L(\rho, \sigma)$. If λ is a non-invertible element, then $L(\rho\lambda, \sigma\lambda) \subset L(\rho, \sigma)$.

(3) The intersection of two lines $L(\rho_1, \sigma_1)$ and $L(\rho_2, \sigma_2)$ is a line, which we call subline. The number of common points between these two lines, is a divisor of d.

Proof (1) For a given ρ, as τ takes all values in $\mathbb{Z}(d)$, the $\rho\tau$ takes $d/\mathrm{GCD}(\rho, d)$ different values, because there are $\delta = \mathrm{GCD}(\rho, d)$ different values of τ which give the same $\rho\tau$. We next need to find how many different values of $\tau\sigma$, correspond to these δ values of τ (which give the same $\rho\tau$).

The δ values of τ, lead to δ values of $\sigma\tau$, but using the same argument we find that only $\delta/\mathrm{GCD}(\sigma, \delta)$, are different from each other. Therefore the total number of pairs $(\rho\tau, \sigma\tau)$ is

$$\frac{d}{\mathrm{GCD}(\rho, d)} \frac{\delta}{\mathrm{GCD}(\sigma, \delta)} = \frac{d}{\mathrm{GCD}(d, \rho, \sigma)}. \tag{5.3}$$

(2) For any $\lambda \in \mathbb{Z}(d)$, if $(\rho\lambda\tau, \sigma\lambda\tau)$ is a point in $L(\rho\lambda, \sigma\lambda)$ then this point can also be written as $(\rho\tau', \sigma\tau')$ with $\tau' = \lambda\tau$ and therefore it belongs to the line $L(\rho, \sigma)$. This proves that $L(\rho\lambda, \sigma\lambda) \subseteq L(\rho, \sigma)$.

For $\lambda \in [\mathbb{Z}(d)]^*$, if $(\rho\tau, \sigma\tau)$ is a point in $L(\rho, \sigma)$ and then this point can also be written as $(\rho\lambda\tau', \sigma\lambda\tau')$ with $\tau' = \lambda^{-1}\tau$, and therefore it belongs to the line $L(\rho\lambda, \sigma\lambda)$. This proves that for an invertible element λ, $L(\rho\lambda, \sigma\lambda) = L(\rho, \sigma)$.

(3) If $(\rho, \sigma) \in L(\rho_1, \sigma_1)$ and also $(\rho, \sigma) \in L(\rho_2, \sigma_2)$ then clearly for any $\tau \in \mathbb{Z}(d)$, we have $(\rho\tau, \sigma\tau) \in L(\rho_1, \sigma_1)$ and also $(\rho\tau, \sigma\tau) \in L(\rho_2, \sigma_2)$. Therefore the common points of two lines, form a line (which we call subline, and which according to the first part of the proposition, has a divisor of d as number of points).

In the case $d = p$ where p is a prime number, the $\mathbb{Z}(p)$ is a field. In this case the only divisor of p is 1, and two lines through the origin have one point in common. Consequently the geometry $\mathbb{Z}(p) \times \mathbb{Z}(p)$ is a near-linear geometry. In the case of non-prime d, the $\mathbb{Z}(d)$ is a ring (which is not a field). In this case the geometry is a non-near-linear geometry, and has both maximal lines and sublines.

Example 5.1 Examples of maximal lines in $\mathbb{Z}(15) \times \mathbb{Z}(15)$ are

$$\begin{aligned} L(1,2) = \; & \{(0,0), (1,2), (2,4), (3,6), (4,8), (5,10), (6,12), (7,14), \\ & (8,1), (9,3), (10,5), (11,7), (12,9), (13,11), (14,13)\}, \end{aligned} \tag{5.4}$$

and

$$\begin{aligned} L(1,7) = \; & \{(0,0), (1,7), (2,14), (3,6), (4,13), (5,5), (6,12), (7,4), \\ & (8,11), (9,3), (10,10), (11,2), (12,9), (13,1), (14,8)\}. \end{aligned} \tag{5.5}$$

The $L(3,6)$ is an example of a line through the origin which is not maximal line (it has 5 points):

$$L(3,6) = \{(0,0), (3,6), (6,12), (9,3), (12,9)\}. \tag{5.6}$$

The intersection of the maximal lines $L(1,2)$ and $L(1,7)$, is $L(3,6)$:

$$L(1,2) \cap L(1,7) = L(3,6). \tag{5.7}$$

This is shown in Fig. 5.1.

5.1.1 Symplectic Transformations in the Finite Geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$

In order to perform symplectic transformations on a point $(\rho, \sigma) \in \mathbb{Z}(d) \times \mathbb{Z}(d)$, we multiply the row (ρ, σ) times the matrix $g(\kappa, \lambda|\mu, \nu) \in Sp[2, \mathbb{Z}(d)]$:

$$g(\kappa, \lambda|\mu, \nu) \circ (\rho, \sigma) = (\rho, \sigma) g(\kappa, \lambda|\mu, \nu) = (\kappa\rho + \mu\sigma, \lambda\rho + \nu\sigma) \tag{5.8}$$

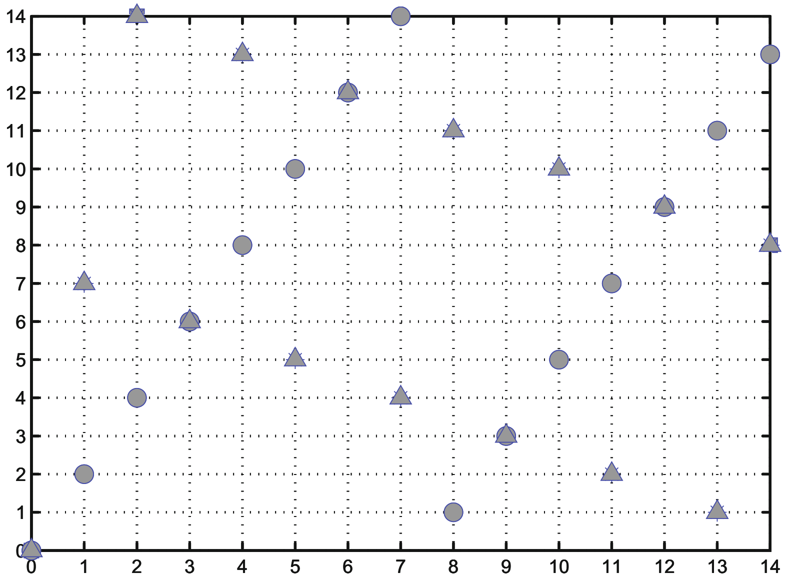

Fig. 5.1 The *maximal lines* $L(1,2)$ (*circles*), and $L(1,7)$ (*triangles*) in the $\mathbb{Z}(15)\times\mathbb{Z}(15)$ finite geometry

This is consistent with the 'right multiplication rule' in Eq. (3.35). In particular we note that the Fourier matrix $\mathscr{F}$ of Eq. (3.41) maps the points $(\alpha,0)$ on the 'horizontal axis', to the points $(0,\alpha)$ on the 'vertical axis':

$$\mathscr{F}\circ(\alpha,0)=(\alpha,0)g(0,1|-1,0)=(0,\alpha) \tag{5.9}$$

Symplectic transformations on points lead to symplectic transformations on lines:

$$g(\kappa,\lambda|\mu,\nu)\circ L(\rho,\sigma)=L(\kappa\rho+\mu\sigma,\lambda\rho+\nu\sigma). \tag{5.10}$$

In particular, with the Fourier matrix we get:

$$\mathscr{F}\circ L(\rho,\sigma)=L(-\sigma,\rho). \tag{5.11}$$

Example 5.2 In $\mathbb{Z}(15)$ we act with the matrix $g(3,4|2,8)\in Sp[2,\mathbb{Z}(15)]$ on the line $L(1,2)$ and we get:

$$g(3,4|2,8)\circ L(1,2)=L(7,5). \tag{5.12}$$

This is shown in Fig. 5.2.

Proposition 5.2 *For prime p, the geometry $\mathbb{Z}(p)\times\mathbb{Z}(p)$ is a near-linear geometry, which has only maximal lines with p points, given in terms of symplectic transfor-*

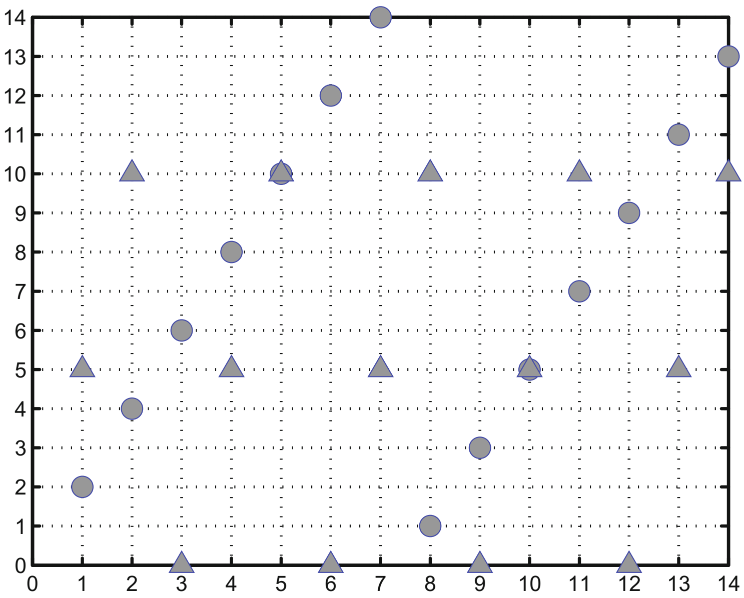

Fig. 5.2 The *maximal lines* $L(1, 2)$ (*circles*), and $L(7, 5) = g(3, 4|2, 8) \circ L(1, 2)$ (*triangles*) in the $\mathbb{Z}(15) \times \mathbb{Z}(15)$ finite geometry

mations as

$$g(0, -1|1, \nu) \circ L(0, 1) = L(1, \nu). \tag{5.13}$$

The $L(0, 1)$ together with the $L(1, \nu)$ with $\nu = 0, ..., p - 1$, form the set of all $\psi(p) = p + 1$ lines through the origin, in this geometry (ψ is the Dedekind psi).

Proof For the proof we use symplectic transformations in conjunction with Proposition 5.1.

Notation 5.1 *For a prime p, we introduce the notation*

$$\mathscr{L}(\nu) = L(1, \nu); \quad \mathscr{L}(-1) = L(0, 1). \tag{5.14}$$

In $\mathscr{L}(\nu)$, the ν takes the $\psi(p) = p + 1$ values $-1, ..., p - 1$.

5.1.2 Factorization of the Finite Geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$ Based on the Chinese Remainder Theorem

As we mentioned earlier, for simplicity and without loss of generality, we consider the case where $d = p_1p_2$ where p_1, p_2 are odd prime numbers. The following proposition describes the maximal lines through the origin in $\mathbb{Z}(p_1 p_2) \times \mathbb{Z}(p_1 p_2)$, as products of lines in $\mathbb{Z}(p_1) \times \mathbb{Z}(p_1)$ and $\mathbb{Z}(p_2) \times \mathbb{Z}(p_2)$.

There is an analogy between the factorization of the finite geometry, and the factorization of position and momentum states in Sect. 4.9, with the points $(\alpha, 0)$ in the 'horizontal axis' corresponding to position states, and the points $(0, \beta)$ in the 'vertical axis' corresponding to momenta. Motivated by this we factorize the points (α, β) using the dual map in Eq. (3.22) for α, and the map of Eq. (3.21) for β:

$$(\alpha, \beta) \;\leftrightarrow\; ((\overline{\alpha}_1, \beta_1), (\overline{\alpha}_2, \beta_2)); \quad \overline{\alpha}_i, \beta_i \in \mathbb{Z}(p_i). \tag{5.15}$$

This is consistent with the relation of Eq. (3.52) that factorized the Fourier matrix. Indeed

$$\mathscr{F} \circ (\alpha, \beta) = (-\beta, \alpha) \;\leftrightarrow\; ((\overline{\beta}_1, \alpha_1), (\overline{\beta}_2, \alpha_2)) \tag{5.16}$$

Also

$$\mathscr{F} \circ (\alpha, \beta) \leftrightarrow (g_1(0, r_1| - t_1, 0) \circ (\overline{\alpha}_1, \beta_1), g_2(0, r_2| - t_2, 0) \circ (\overline{\alpha}_2, \beta_2)) \tag{5.17}$$

with

$$\begin{aligned} g_1(0, r_1| - t_1, 0) \circ (\overline{\alpha}_1, \beta_1) &= (\overline{\beta}_1, \alpha_1) \\ g_2(0, r_2| - t_2, 0) \circ (\overline{\alpha}_2, \beta_2) &= (\overline{\beta}_2, \alpha_2). \end{aligned} \tag{5.18}$$

Proposition 5.3 *There are $\psi(p_1 p_2)$ maximal lines through the origin in $\mathbb{Z}(p_1 p_2) \times \mathbb{Z}(p_1 p_2)$, which belong to one of the following four categories:*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$

$$\mathscr{L}(\nu_1, \nu_2) \equiv L_1(1, \nu_1) \times L_2(1, \nu_2) = L(p_1 + p_2, \nu_1 s_1 + \nu_2 s_2) \tag{5.19}$$

There are $p_1 p_2$ lines in this category, with $\nu_1 = 0, ..., p_1 - 1$, and $\nu_2 = 0, ..., p_2 - 1$. The $\mathscr{L}(\nu_1, \nu_2)$ is another notation for these lines, which we call 'factorized notation'. We call the $L(p_1 + p2, \nu_1 s_1 + \nu_2 s_2)$, unfactorized notation.

(2) If $\nu_2 \in \mathbb{Z}(p_2)$

$$\mathscr{L}(-1, \nu_2) \equiv L(0, 1) \times L(1, \nu_2) = L(p_1, s_1 + \nu_2 s_2) \tag{5.20}$$

There are p_2 lines in this category, with $\nu_2 = 0, ..., p_2 - 1$. $\mathscr{L}(-1, \nu_2)$ is the factorized notation for these lines.

(3) If $\nu_1 \in \mathbb{Z}(p_1)$

$$\mathscr{L}(\nu_1, -1) \equiv L(1, \nu_1) \times L(0, 1) = L(p_2, \nu_1 s_1 + s_2) \tag{5.21}$$

There are p_1 lines in this category, with $\nu_1 = 0, ..., p_1 - 1$. $\mathscr{L}(\nu_1, -1)$ is the factorized notation for these lines.

(4)

$$\mathscr{L}(-1, -1) \equiv L(0, 1) \times L(0, 1) = L(0, 1). \tag{5.22}$$

$\mathscr{L}(-1, -1)$ is the factorized notation for this line.

Proof From Eq. (5.10) follows that

$$g(\kappa, \lambda|\mu, \nu) \circ L(0, 1) = L(\mu, \nu). \tag{5.23}$$

We note here that the $L(\mu, \nu)$ does not depend on κ, λ, and this should be compared and contrasted with Eq. (4.53). The proof then follows immediately from Corollary 3.1.

Example 5.3 In $\mathbb{Z}(15) \times \mathbb{Z}(15)$ there are $\psi(15) = 24$ maximal lines through the origin. As an example we consider the following line

$$\mathscr{L}(2, 1) = L_1(1, 2) \times L_2(1, 1) \tag{5.24}$$

$L_1(1, 2)$ is a line in $\mathbb{Z}(3) \times \mathbb{Z}(3)$, and $L_2(1, 1)$ is a line in $\mathbb{Z}(5) \times \mathbb{Z}(5)$. In the unfactorized notation the $\mathscr{L}(2, 1)$ is $L(8, 2s_1 + s_2)$. We have seen in Eq. (3.30) that

Table 5.1 The points in the line $L(1, 7) = \mathscr{L}(2, 1)$ (in the unfactorized and factorized notations). The corresponding points in the first factor line $L_1(1, 2)$ (in $\mathbb{Z}(3) \times \mathbb{Z}(3)$), and in the second factor line $L_2(1, 1)$ (in $\mathbb{Z}(5) \times \mathbb{Z}(5)$) are also shown

$L(1, 7)$		$L_1(1, 2)$		$L_2(1, 1)$	
0	0	0	0	0	0
1	7	2	1	2	2
2	14	1	2	4	4
3	6	0	0	1	1
4	13	2	1	3	3
5	5	1	2	0	0
6	12	0	0	2	2
7	4	2	1	4	4
8	11	1	2	1	1
9	3	0	0	3	3
10	10	2	1	0	0
11	2	1	2	2	2
12	9	0	0	4	4
13	1	2	1	1	1
14	8	1	2	3	3

$s_1 = 10$ and $s_2 = 6$, and therefore $2s_1 + s_2 = 26 = 11 \pmod{15}$. Therefore in the unfactorized notation the $\mathscr{L}(2, 1)$ is $L(8, 11) = L(1, 8^{-1} \times 11) = L(1, 7)$. The points in this line, and also in its factor lines $L_1(1, 2)$ and $L_2(1, 1)$ are shown in Table 5.1.

5.2 Mutually Unbiased Bases

There is a lot of work on various aspects of mutually unbiased bases [4–22]. Their study incorporates many areas of discrete Mathematics. Below we summarize the main points. Mutually unbiased bases in systems with variables in Galois fields, are discussed later in Sect. 9.7.

Definition 5.1 A set of orthonormal bases in $H[\mathbb{Z}(d)]$ are called mutually unbiased, if the vectors in any two of these bases obey the relation

$$|\langle X; m|Y; n\rangle|^2 = \frac{1}{d}; \quad m, n \in \mathbb{Z}(d). \tag{5.25}$$

for all m, n.

Proposition 5.4 *The number of mutually unbiased bases in* $H[\mathbb{Z}(d)]$, *is*

$$\mathscr{M}(d) \leq d + 1. \tag{5.26}$$

Proof A measurement with the projectors $|X; m\rangle\langle X; m|$ gives d probabilities, $d - 1$ of which are independent. A density matrix has $d^2 - 1$ degrees of freedom, and therefore we need at least $d + 1$ measurements in order to get all the information in it. If the information that we get from each measurement is totally independent from the information that we get from the other measurements, then the total number of measurements needed is exactly $d + 1$. This is the case with the mutually unbiased bases. Indeed

$$\langle X; m|\rho|X; m\rangle = \frac{1}{d} + \sum_{n_1 \neq n_2} \langle X; m|Y; n_1\rangle\langle Y; n_1|\rho|Y; n_2\rangle\langle Y; n_2|X; m\rangle. \tag{5.27}$$

This shows that the information obtained from the measurement with the projectors $|X; m\rangle\langle X; m|$, is contained entirely in the off-diagonal terms $\langle Y; n_1|\rho|Y; n_2\rangle$ with $n_1 \neq n_2$. The measurement with the projectors $|X; m\rangle\langle X; m|$ gives totally independent information from the measurement with the projectors $|Y; m\rangle\langle Y; m|$. Consequently, the maximum number of mutually unbiased bases is $d + 1$. We note that the argument does not guarantee the existence of $d + 1$ mutually unbiased bases.

In systems with prime, or power of prime dimension, the inequality in Eq. (5.26) becomes equality. In the following proposition we consider a system with prime dimension p, and construct a set of $\mathcal{M}(p) = p + 1$ mutually unbiased bases. The construction is based on symplectic transformations. This result is generalized to systems with power of prime dimension p^e, and variables in the Galois fields $GF(p^e)$, later in Sect. 9.7.

5.2.1 Mutually Unbiased Bases in $H[\mathbb{Z}(p)]$

Notation 5.2 *In $H[\mathbb{Z}(p)]$ where p is an odd prime, we consider the p orthonormal bases*

$$|\mathcal{X}(\nu); m\rangle = S(0, -1|1, \nu)|X; m\rangle; \quad \nu, m \in \mathbb{Z}(p) \tag{5.28}$$

where $S(0, -1|1, \nu)$ are symplectic matrices (discussed in Sect. 4.5). In the case $\nu = 0$, this is the basis of momentum states:

$$|\mathcal{X}(0); m\rangle = S(0, -1|1, 0)|X; m\rangle = F^{\dagger}|X; m\rangle = |P; -m\rangle. \tag{5.29}$$

In addition to them, we also consider the orthonormal basis of position states, and we use the convention

$$|\mathcal{X}(-1); m\rangle = |X; m\rangle. \tag{5.30}$$

So we have $p + 1$ orthonormal bases

$$|\mathcal{X}(\nu); m\rangle; \quad \nu \in \{-1\} \cup \mathbb{Z}(p). \tag{5.31}$$

There should be no confusion between the $\nu = -1$ which is used as an extra element that indicates position states, and the $p - 1 = -1 \pmod p$ which is an element of $\mathbb{Z}(p)$.

Proposition 5.5 *For $\nu \neq \nu'$,*

$$|\langle \mathcal{X}(\nu'); n|\mathcal{X}(\nu); m\rangle|^2 = \frac{1}{p}; \quad \nu, \nu' \in \{-1\} \cup \mathbb{Z}(p). \tag{5.32}$$

Therefore they are a set of $p + 1$ mutually unbiased bases.

Proof We consider the following four cases.

(1) In the first case $\nu, \nu' = 1, ..., p - 1$. We use Eq. (4.65) with $d = p$, $\kappa = 0$, $\lambda = -1$, $\mu = 1$, and we get

$$|\mathcal{X}(\nu); m\rangle = \frac{1}{p} G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)] \sum_r \omega(2^{-1}r^2\nu - rm)|X; r\rangle. \tag{5.33}$$

Here G is the Gauss sum. Therefore

$$\begin{aligned}\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle &= \frac{1}{p^2}G[-2^{-1}(\nu')^{-1}; \mathbb{Z}(p)]G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)]\\ &\times \sum_r \omega(-2^{-1}r^2\nu' + rn + 2^{-1}r^2\nu - rm). \end{aligned}\tag{5.34}$$

We replace the variable r with $R = r + (\nu - \nu')^{-1}(n - m)$ and we show that

$$\begin{aligned}\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle &= \frac{1}{p^2}G[-2^{-1}(\nu')^{-1}; \mathbb{Z}(p)]G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)]\\ &\times G[2^{-1}(\nu - \nu'); \mathbb{Z}(p)]\\ &\times \omega(-2^{-1}(\nu - \nu')^{-1}(n - m)^2]. \end{aligned}\tag{5.35}$$

This result is actually true for any odd dimension. We now use the fact that for prime p and $\alpha \neq 0$, we get $|G[\alpha; \mathbb{Z}(p)]| = \sqrt{p}$ (see Eq. (3.9)). Therefore

$$\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle = \frac{1}{\sqrt{p}}. \tag{5.36}$$

(2) In the second case $\nu = 1, ..., p - 1$ and $\nu' = -1$, and we prove that

$$|\langle X; n|\mathscr{X}(\nu); m\rangle| = \frac{1}{\sqrt{p}}. \tag{5.37}$$

Eq. (5.38) gives

$$\langle X; n|\mathscr{X}(\nu); m\rangle = \frac{1}{p}G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)]\omega(2^{-1}n^2\nu - nm). \tag{5.38}$$

Taking into account Eq. (3.9), we prove Eq. (5.37).

(3) In the third case $\nu = 1, ..., p - 1$ and $\nu' = 0$, and we prove that

$$|\langle P; n|\mathscr{X}(\nu); m\rangle| = \frac{1}{\sqrt{p}}. \tag{5.39}$$

The proof here is very similar to the previous cases.

(4) In the fourth case $\nu = -1$ and $\nu' = 0$ and we see immediately that

$$|\langle P; n|X; m\rangle| = \frac{1}{\sqrt{p}}. \tag{5.40}$$

This completes the proof.

Table 5.2 The six lines through the origin in the finite geometry $\mathbb{Z}(5) \times \mathbb{Z}(5)$, and the corresponding mutually unbiased bases in $H[\mathbb{Z}(5)]$

Lines in $\mathbb{Z}(5) \times \mathbb{Z}(5)$	Bases in $H[\mathbb{Z}(5)]$
$\mathscr{L}(-1) = L(0,1)$	$\lvert\mathscr{X}(-1); m\rangle = \lvert X; m\rangle$
$\mathscr{L}(0) = L(1,0) = \mathscr{F}^{\dagger} \circ L(0,1)$	$\lvert\mathscr{X}(-0); m\rangle = F^{\dagger}\lvert X; m\rangle = \lvert P; -m\rangle$
$\mathscr{L}(1) = L(1,1) = g(0,-1\lvert 1,1) \circ L(0,1)$	$\lvert\mathscr{X}(1); m\rangle = S(0,-1\lvert 1,1)\lvert X; m\rangle$
$\mathscr{L}(2) = L(1,2) = g(0,-1\lvert 1,2) \circ L(0,1)$	$\lvert\mathscr{X}(2); m\rangle = S(0,-1\lvert 1,2)\lvert X; m\rangle$
$\mathscr{L}(3) = L(1,3) = g(0,-1\lvert 1,3) \circ L(0,1)$	$\lvert\mathscr{X}(3); m\rangle = S(0,-1\lvert 1,3)\lvert X; m\rangle$
$\mathscr{L}(4) = L(1,4) = g(0,-1\lvert 1,4) \circ L(0,1)$	$\lvert\mathscr{X}(4); m\rangle = S(0,-1\lvert 1,4)\lvert X; m\rangle$

Proposition 5.6 *There is a duality between the $\psi(p) = p + 1$ lines through the origin in the near-linear finite geometry $\mathbb{Z}(p) \times \mathbb{Z}(p)$, and the $\psi(p) = p + 1$ mutually unbiased bases in the Hilbert space $H[\mathbb{Z}(p)]$, where*

$$\mathscr{L}(\nu) \quad \leftrightarrow \quad \{\lvert\mathscr{X}(\nu); m\rangle\}; \quad \nu = -1, ..., p - 1. \tag{5.41}$$

The p points in the line $\mathscr{L}(\nu)$ correspond to the p vectors in the basis $\{\lvert\mathscr{X}(\nu); m\rangle\}$.

Proof We compare and contrast Eqs. (5.13), (5.14) with Eqs. (5.28), (5.29), (5.30). We get

$$\mathscr{L}(-1) = L(0,1) \quad \leftrightarrow \quad \lvert\mathscr{X}(-1); m\rangle = \lvert X; m\rangle \tag{5.42}$$

for $\nu = -1$, and

$$\mathscr{L}(\nu) = g(0,-1\lvert 1,\nu) \circ L(0,1) \quad \leftrightarrow \quad \lvert\mathscr{X}(\nu); m\rangle = S(0,-1\lvert 1,\nu)\lvert X; m\rangle \tag{5.43}$$

for $\nu = 0, ..., p - 1$. This proves the proposition.

Example 5.4 In the finite geometry $\mathbb{Z}(5) \times \mathbb{Z}(5)$ there are six lines through the origin, shown in Table 5.2. The corresponding mutually unbiased bases in $H[\mathbb{Z}(5)]$ are also shown.

We note that the above duality between mutually unbiased bases and finite geometries, does not hold for non-prime dimensions. This motivates the revision of the concept of mutually unbiased bases into another concept (which we call weak mutually unbiased bases), so that this duality is preserved. This is studied in the section below.

5.3 Weak Mutually Unbiased Bases and Duality with Finite Geometries

In systems where the variables take values in a field ($\mathbb{Z}(p)$ or $GF(p^e)$ with prime p) the number of mutually unbiased bases is equal to the maximum possible value $d+1$ (where d is the dimension of the system). In systems where the variables take values in a ring ($\mathbb{Z}(d)$ with non-prime d), it seems that the maximum number of mutually unbiased bases is smaller than $d+1$ (but there is no rigorous proof of this). The existence of non-invertible elements (apart from zero) in rings, seems to be linked to the fact that the number of mutually unbiased bases is smaller than $d+1$.

In this section we discuss the concept of weak mutually unbiased bases [23–26] which is tailored for rings, in the sense that there is a duality (correspondence) between the finite geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$ (discussed in Sect. 5.1) and weak mutually unbiased bases in $H[\mathbb{Z}(d)]$. This is a strong motivation for their study.

As the name indicates, the weak mutually unbiased bases are weaker structures than mutually unbiased bases, and this is related to the fact that rings are weaker structures than fields. Roughly speaking, we replace the requirement $|\langle X; m|Y; n\rangle|^2 = \frac{1}{d}$ in Eq. (5.25), with the requirement that $|\langle X; m|Y; n\rangle|^2$ is $\frac{1}{e_i}$ where e_i is a divisor of the dimension d. In the case of prime dimension there are no non-trivial divisors, and the weak mutually unbiased bases are mutually unbiased bases.

The number of weak mutually unbiased bases is shown to be $\psi(d)$ (the Dedekind psi function). For non-prime d we have $\psi(d) > d+1$, and measurements with the weak mutually unbiased bases provide $(d-1)\psi(d)$ probabilities, which is greater than the d^2-1 degrees of freedom in a density matrix. Therefore weak mutually unbiased bases do not provide independent information, and Eq. (5.27) does not hold.

As above, we consider the case where the dimension d is the product of two odd prime numbers $d = p_1 p_2$, which are different from each other.

Definition 5.2 A set of orthonormal bases in $H[\mathbb{Z}(p_1 p_2)]$ is weakly mutually unbiased, if the vectors in any two of these bases $|X; m\rangle$ and $|Y; n\rangle$, obey the relations in one of the following three categories:

(1)

$$|\langle X; m|Y; n\rangle|^2 = \frac{1}{p_1}; \quad \text{if} \quad n = m \pmod{p_2}$$
$$|\langle X; m|Y; n\rangle|^2 = 0; \quad \text{otherwise} \tag{5.44}$$

(2)

$$|\langle X; m|Y; n\rangle|^2 = \frac{1}{p_2}; \quad \text{if} \quad n = m \pmod{p_1}$$
$$|\langle X; m|Y; n\rangle|^2 = 0; \quad \text{otherwise} \tag{5.45}$$

(3)

$$|\langle X;m|Y;n\rangle|^2=\frac{1}{p_1p_2}. \tag{5.46}$$

Apart from the third option which is the standard definition of mutually unbiased bases, we have here two more options. Therefore any set of mutually unbiased bases in $H[\mathbb{Z}(p_1p_2)]$, can be regarded as a subset of a bigger set of weak mutually unbiased bases.

Proposition 5.7 *We factorize the system $\Sigma[\mathbb{Z}(p_1p_2)]$ as $\Sigma[\mathbb{Z}(p_1)]\otimes\Sigma[\mathbb{Z}(p_2)]$, as discussed in Sect. 4.9. For any set $S_{\rm WMUB}$ of weak mutually unbiased bases in $H[\mathbb{Z}(p_1p_2)]$, there exists a set $|\mathscr{X}_1(\nu_1);\overline{m}_1\rangle$ of mutually unbiased bases in $H[\mathbb{Z}(p_1)]$, and a set $|\mathscr{X}_2(\nu_2);\overline{m}_2\rangle$, of mutually unbiased bases in $H[\mathbb{Z}(p_2)]$, such that the*

$$\begin{aligned}&S_{\rm WMUB}^{\rm max}=\{|\mathscr{X}_1(\nu_1);\overline{m}_1\rangle\otimes|\mathscr{X}_2(\nu_2);\overline{m}_2\rangle\}\\&\nu_1=-1,\ldots,p_1-1;\quad \nu_2=-1,\ldots,p_2-1\end{aligned} \tag{5.47}$$

is a set of weak mutually unbiased bases, and $S_{\rm WMUB}\subseteq S_{\rm WMUB}^{\rm max}$. The cardinality of $S_{\rm WMUB}^{\rm max}$ is $\psi(p_1p_2)$.

Proof Let $|X;m\rangle$ and $|Y;n\rangle$ be two bases in $H[\mathbb{Z}(p_1p_2)]$, which are factorized as

$$\begin{aligned}&|X;m\rangle=|X_1;\overline{m}_1\rangle\otimes|X_2;\overline{m}_2\rangle;\quad |Y;n\rangle=|X_1;\overline{n}_1\rangle\otimes|X_2;\overline{n}_2\rangle\\&\overline{m}_1,\overline{n}_1\in\mathbb{Z}(p_1);\quad \overline{m}_2,\overline{n}_2\in\mathbb{Z}(p_2).\end{aligned} \tag{5.48}$$

We assume that the relations in the Definition 5.2 hold, and we will construct the corresponding set $S_{\rm WMUB}^{\rm max}$ of weak mutually unbiased bases. We consider the following three cases:

(1) In the case that Eq. (5.44) holds, we get

$$|\langle X_1;\overline{m}_1|Y_1;\overline{n}_1\rangle||\langle X_2;\overline{m}_2|Y_2;\overline{n}_2\rangle|^2=\frac{1}{p_1}. \tag{5.49}$$

The condition $n=m\pmod{p_2}$ gives $\overline{n}_2=\overline{m}_2$. As (n,m) take all values in $\mathbb{Z}(p_1p_2)\times\mathbb{Z}(p_1p_2)$ such that $n=m\pmod{p_2}$, the $(\overline{n}_1,\overline{m}_1)$ take all values in $\mathbb{Z}(p_1)\times\mathbb{Z}(p_1)$. From Eq. (5.49), it follows that

$$|\langle X_1;\overline{m}_1|Y_1;\overline{n}_1\rangle|^2\geq\frac{1}{p_1};\qquad \sum_{\overline{m}_1}|\langle X_1;\overline{m}_1|Y_1;\overline{n}_1\rangle|^2=1 \tag{5.50}$$

The first of these relations follows from Eq. (5.49). From this we conclude that

$$|\langle X_1;\overline{m}_1|Y_1;\overline{n}_1\rangle|^2=\frac{1}{p_1};\quad |\langle X_2;\overline{m}_2|Y_2;\overline{m}_2\rangle|=1. \tag{5.51}$$

Therefore the $|X_1; \overline{m}_1\rangle$, $|Y_1; \overline{n}_1\rangle$, ..., are mutually unbiased bases in $H[\mathbb{Z}(p_1)]$. In this case the $|X_2; \overline{m}_2\rangle$ is the same basis as $|Y_2; \overline{n}_2\rangle$, so we have the tensor product of mutually unbiased bases in $H[\mathbb{Z}(p_1)]$, with one basis in $H[\mathbb{Z}(p_2)]$.

(2) The case where Eq. (5.45) holds, is similar to the above case.

(3) In the case that Eq. (5.46) holds, we get

$$|\langle X_1; \overline{m}_1 | Y_1; \overline{n}_1\rangle|^2 |\langle X_2; \overline{m}_2 | Y_2; \overline{n}_2\rangle|^2 = \frac{1}{p_1 p_2} \tag{5.52}$$

We also consider the overlap of $|X; m\rangle$ with another vector $|Y; n'\rangle$ in the second basis, such that $n = n' \pmod{p_1}$. Then $\overline{n}_1 = \overline{n}'_1$ and as n' takes all values in $\mathbb{Z}(p_1 p_2)$ subject to the constraint $n = n' \pmod{p_1}$, the $\overline{n}'_2$ takes all values in $\mathbb{Z}(p_2)$. We get

$$|\langle X_1; \overline{m}_1 | Y_1; \overline{n}_1\rangle|^2 |\langle X_2; \overline{m}_2 | Y_2; \overline{n}'_2\rangle|^2 = \frac{1}{p_1 p_2} \tag{5.53}$$

From Eqs. (5.52), (5.53) we see that $|\langle X_2; \overline{m}_2 | Y_2; \overline{n}_2\rangle|$ is constant for all $\overline{n}_2 \in \mathbb{Z}(p_2)$. This and the relation

$$\sum_{\overline{n}_2 \in \mathbb{Z}(p_2)} |\langle X_2; \overline{m}_2 | Y_2; \overline{n}_2\rangle|^2 = 1 \tag{5.54}$$

prove that $|\langle X_2; \overline{m}_2 | Y_2; \overline{n}_2\rangle|^2 = \frac{1}{p_2}$. Therefore the $|X_2; \overline{m}_2\rangle$, $|Y_2; \overline{n}_2\rangle$ are mutually unbiased bases in $H[\mathbb{Z}(p_2)]$.

In a 'dual' way we prove that $|\langle X_1; \overline{m}_1 | Y_1; \overline{n}_1\rangle|^2 = \frac{1}{p_1}$, and therefore the $|X_1; \overline{n}_1\rangle$, $|Y_1; \overline{m}_1\rangle$ are mutually unbiased bases in $H[\mathbb{Z}(p_1)]$.

The number of mutually unbiased bases in $H[\mathbb{Z}(p_1)]$ is $p_1 + 1$, and in $H[\mathbb{Z}(p_2)]$ is $p_2 + 1$. Therefore the maximum number of weak mutually unbiased bases in $H[\mathbb{Z}(p_1 p_2)]$ is $\psi(p_1 p_2) = (p_1 + 1)(p_2 + 1)$.

Notation 5.3 *We use an alternative 'factorized notation' for the states in Eq. (5.47), which is analogous to the 'factorized notation' for lines*

$$\begin{aligned}
|\mathscr{X}(\nu_1, \nu_2); \overline{m}_1, \overline{m}_2\rangle &= |\mathscr{X}_1(\nu_1); \overline{m}_1\rangle \otimes |\mathscr{X}_2(\nu_2); \overline{m}_2\rangle \\
|\mathscr{X}(-1, \nu_2); \overline{m}_1, \overline{m}_2\rangle &= |X_1; \overline{m}_1\rangle \otimes |\mathscr{X}_2(\nu_2); \overline{m}_2\rangle \\
|\mathscr{X}(\nu_1, -1); \overline{m}_1, \overline{m}_2\rangle &= |\mathscr{X}_1(\nu_1); \overline{m}_1\rangle \otimes |X_2; \overline{m}_2\rangle \\
|\mathscr{X}(-1, -1); \overline{m}_1, \overline{m}_2\rangle &= |X_1; \overline{m}_1\rangle \otimes |X_2; \overline{m}_2\rangle .
\end{aligned} \tag{5.55}$$

In order to establish a correspondence between the factorized and unfactorized notations for the weak mutually unbiased bases, we need the following corollary, which is analogous to Corollary 3.1.

Corollary 5.1 *Let S_1, S_2, S be symplectic transformations in $H[\mathbb{Z}(p_1)]$, $H[\mathbb{Z}(p_2)]$ and $H[\mathbb{Z}(p_1p_2)]$, correspondingly. Then*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$

$$\begin{aligned} &S_1(0, -1|1, \nu_1) \otimes S_2(0, -1|1, \nu_2) \\ &= S(0, -s_1t_1 - s_2t_2|p_1 + p_2, \nu_1s_1 + \nu_2s_2) \end{aligned} \tag{5.56}$$

(2) If $\nu_2 \in \mathbb{Z}(p_2)$

$$\mathbf{1} \otimes S_2(0, -1|1, \nu_2) = S(s_1, -s_2t_2|p_1, s_1 + \nu_2s_2) \tag{5.57}$$

(3) If $\nu_1 \in \mathbb{Z}(p_1)$

$$S_1(0, -1|1, \nu_1) \otimes \mathbf{1} = S(s_2, -s_1t_1|p_2, \nu_1s_1 + s_2) \tag{5.58}$$

(4)

$$\mathbf{1} \otimes \mathbf{1} = \mathbf{1}. \tag{5.59}$$

Proof The proof is analogous to the one in Corollary 3.1, because the matrices g and S are different representations of the same group (the symplectic group).

The following proposition gives the relation between the factorized and unfactorized notation, for the weak mutually unbiased bases in $H[\mathbb{Z}(p_1p_2)]$.

Proposition 5.8 *The correspondence between the factorized notation for weak mutually unbiased bases, and the unfactorized one (for which the notation in Eq. (4.53) is used), is as follows.*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$, then

$$\begin{aligned} &|\mathscr{X}(\nu_1, \nu_2); \overline{m}_1, \overline{m}_2\rangle = |X(\alpha, \beta); m\rangle \\ &\alpha = p_1 + p_2; \quad \beta = \nu_1s_1 + \nu_2s_2; \quad m = \overline{m}_1p_2 + \overline{m}_2p_1. \end{aligned} \tag{5.60}$$

(2) If $\nu_2 \in \mathbb{Z}(p_2)$, then

$$\begin{aligned} &|\mathscr{X}(-1, \nu_2); \overline{m}_1, \overline{m}_2\rangle = |X(\alpha, \beta); m\rangle \\ &\alpha = p_1; \quad \beta = s_1 + \nu_2s_2; \quad m = \overline{m}_1p_2 + \overline{m}_2p_1 \end{aligned} \tag{5.61}$$

(3) If $\nu_1 \in \mathbb{Z}(p_1)$, then

$$\begin{aligned} &|\mathscr{X}(\nu_1, -1); \overline{m}_1, \overline{m}_2\rangle = |X(\alpha, \beta); m\rangle \\ &\alpha = p_2; \quad \beta = \nu_1s_1 + s_2; \quad m = \overline{m}_1p_2 + \overline{m}_2p_1 \end{aligned} \tag{5.62}$$

(4)

$$\begin{aligned}
&|\mathscr{X}(-1,-1);\overline{m}_1,\overline{m}_2\rangle = |X;m\rangle \\
&m = \overline{m}_1 p_2 + \overline{m}_2 p_1
\end{aligned} \tag{5.63}$$

Proof The proof follows immediately from Corollary 5.1.

Our notation and terminology so far, aimed to show the existence of duality between maximal lines in $\mathbb{Z}(p_1p_2)\times\mathbb{Z}(p_1p_2)$ and weak mutually unbiased bases in the Hilbert space $H[\mathbb{Z}(p_1p_2)]$. This is formalized in the proposition below.

Proposition 5.9 *There is a duality between the $\psi(p_1p_2)$ maximal lines through the origin in the non-near-linear finite geometry $\mathbb{Z}(p_1p_2)\times\mathbb{Z}(p_1p_2)$ and the $\psi(p_1p_2)$ weak mutually unbiased bases in the Hilbert space $H[\mathbb{Z}(p_1p_2)]$, where*

$$\begin{aligned}
&\mathscr{L}(\nu_1,\nu_2) \quad \leftrightarrow \quad \{|\mathscr{X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle\} \\
&\nu_1 = -1, ..., p_1-1; \quad \nu_2 = -1, ..., p_2-1.
\end{aligned} \tag{5.64}$$

The $d = p_1p_2$ points in the maximal line $\mathscr{L}(\nu_1,\nu_2)$ correspond to the $d = p_1p_2$ vectors in the basis $\{|\mathscr{X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle\}$.

Proof For the proof we compare and contrast Propositions 5.3, 5.8, using the correspondence

$$\begin{aligned}
&L(0,1) \quad \leftrightarrow \quad |X;m\rangle \\
&g(\kappa,\lambda|\mu,\nu) \quad \leftrightarrow \quad S(\kappa,\lambda|\mu,\nu).
\end{aligned} \tag{5.65}$$

For $\nu_1 = -1$ and $\nu_2 = -1$, we get

$$\begin{aligned}
&\mathscr{L}(-1,-1) = L_1(0,1)\times L_2(0,1) \quad \leftrightarrow \\
&|\mathscr{X}(-1,-1);\overline{m}_1,\overline{m}_2\rangle = |X_1;\overline{m}_1\rangle\otimes|X_2;\overline{m}_2\rangle.
\end{aligned} \tag{5.66}$$

For $\nu_1 = 0, ..., p_1-1$ and $\nu_2 = -1$, we get

$$\begin{aligned}
&\mathscr{L}(\nu_1,-1) = [g_1(0,-1|1,\nu_1)\circ L_1(0,1)]\times L_2(0,1) \quad \leftrightarrow \\
&|\mathscr{X}(\nu_1,-1);\overline{m}_1,\overline{m}_2\rangle = [S_1(0,-1|1,\nu_1)|X_1;\overline{m}_1\rangle]\otimes|X_2;\overline{m}_2\rangle.
\end{aligned} \tag{5.67}$$

For $\nu_1 = -1$ and $\nu_2 = 0, ..., p_2-1$, we get

$$\begin{aligned}
&\mathscr{L}(-1,\nu_2) = L_1(0,1)\times[g_2(0,-1|1,\nu_2)\circ L_2(0,1)] \quad \leftrightarrow \\
&|\mathscr{X}(-1,\nu_2);\overline{m}_1,\overline{m}_2\rangle = |X_1;\overline{m}_1\rangle\otimes[S_2(0,-1|1,\nu_2)|X_2;\overline{m}_2\rangle].
\end{aligned} \tag{5.68}$$

For $\nu_1 = 0, ..., p_1-1$ and $\nu_2 = 0, ..., p_2-1$, we get

$$\begin{aligned}&{\mathscr L}(\nu_1,\nu_2)=[g_1(0,-1|1,\nu_1)\circ L_1(0,1)]\times[g_2(0,-1|1,\nu_2)\circ L_2(0,1)]\quad\leftrightarrow\\&|{\mathscr X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle=[S_1(0,-1|1,\nu_1)|X_1;\overline{m}_1\rangle]\\&\qquad\qquad\qquad\otimes[S_2(0,-1|1,\nu_2)|X_2;\overline{m}_2\rangle].\end{aligned}\tag{5.69}$$

These equations show the exact analogy between maximal lines through the origin in the finite geometry and weak mutuall unbiased bases, and prove the proposition.

Example 5.5 In $\mathbb{Z}(15)\times\mathbb{Z}(15)$ there are $\psi(15)=24$ maximal lines through the origin. The dual statement is that in $H[\mathbb{Z}(15)]$ there are $\psi(15)=24$ weak mutually unbiased bases. In the factorized notation for both lines and bases, the duality between them is

$$\begin{aligned}&{\mathscr L}(\nu_1,\nu_2)\quad\leftrightarrow\quad\{|{\mathscr X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle\mid\overline{m}_1\in\mathbb{Z}(3);\quad\overline{m}_2\in\mathbb{Z}(5)\}\\&\nu_1=-1,...,2;\quad\nu_2=-1,...,4.\end{aligned}\tag{5.70}$$

This is shown in Table 5.3. Both the factorized and unfactorized notations are used (the correspondence is given in Proposition 5.3 for the lines, and in Proposition 5.8 for the bases).

We conclude this section with a brief summary on weak mutually unbiased bases and their duality to the finite geometries. In the case of prime dimension $d=p$, the weak mutually unbiased bases, are the same as mutually unbiased bases (prime numbers have only trivial divisors). In this case:

- Measurements with the $\psi(p)=p+1$ mutually unbiased bases in $H[\mathbb{Z}(p)]$ provide independent information. Each basis is associated with $p-1$ independent probabilities. The total number of independent probabilities is $(p-1)\psi(p)=p^2-1$, and is equal to the number of degrees of freedom in a density matrix.
- The $\psi(p)=p+1$ lines through the origin in the finite geometry $\mathbb{Z}(p)\times\mathbb{Z}(p)$, have no points in common, apart from the origin. Each line consists of $p-1$ points, in addition to the origin. The total number of points is $(p-1)\psi(p)=p^2-1$, plus the origin.

In the case of non-prime dimension d, the weak mutually unbiased bases, are different from mutually unbiased bases (non-prime numbers have non-trivial divisors). In this case:

- Measurements with the $\psi(d)$ weak mutually unbiased bases in $H[\mathbb{Z}(d)]$, provide $\psi(d)(d-1)$ probabilities. Since $\psi(d)(d-1)$ is greater than d^2-1 (which is the number of degrees of freedom in a density matrix), these probabilities are not independent.
- The $\psi(d)$ maximal lines through the origin in the finite geometry $\mathbb{Z}(d)\times\mathbb{Z}(d)$, have a total of $\psi(d)(d-1)$ points, apart from the origin. Since $\psi(d)(d-1)$ is greater than d^2-1 (which is the number of points in $\mathbb{Z}(d)\times\mathbb{Z}(d)$ apart from the origin), two lines might have more points in common apart from the origin.

Table 5.3 The 24 maximal lines through the origin in the finite geometry $\mathbb{Z}(15) \times \mathbb{Z}(15)$ and the corresponding weak mutually unbiased bases in $H[\mathbb{Z}(15)]$. Both the factorized and unfactorized notation, are used

Lines in $\mathbb{Z}(15) \times \mathbb{Z}(15)$	Bases in $H[\mathbb{Z}(15)]$
$\mathscr{L}(-1,-1) = L(0,1)$	$\vert\mathscr{X}(-1,-1); \overline{m}_1, \overline{m}_2\rangle = \vert X(0,1); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,0) = L(3,10)$	$\vert\mathscr{X}(-1,0); \overline{m}_1, \overline{m}_2\rangle = \vert X(3,10); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,1) = L(3,1)$	$\vert\mathscr{X}(-1,1); \overline{m}_1, \overline{m}_2\rangle = \vert X(3,1); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,2) = L(3,7)$	$\vert\mathscr{X}(-1,2); \overline{m}_1, \overline{m}_2\rangle = \vert X(3,7); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,3) = L(3,13)$	$\vert\mathscr{X}(-1,3); \overline{m}_1, \overline{m}_2\rangle = \vert X(3,13); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,4) = L(3,4)$	$\vert\mathscr{X}(-1,4); \overline{m}_1, \overline{m}_2\rangle = \vert X(3,4); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,-1) = L(5,6)$	$\vert\mathscr{X}(0,-1); \overline{m}_1, \overline{m}_2\rangle = \vert X(5,6); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,0) = L(8,0)$	$\vert\mathscr{X}(0,0); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,0); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,1) = L(8,6)$	$\vert\mathscr{X}(0,1); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,6); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,2) = L(8,12)$	$\vert\mathscr{X}(0,2); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,12); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,3) = L(8,3)$	$\vert\mathscr{X}(0,3); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,3); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,4) = L(8,9)$	$\vert\mathscr{X}(0,4); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,9); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,-1) = L(5,1)$	$\vert\mathscr{X}(1,-1); \overline{m}_1, \overline{m}_2\rangle = \vert X(5,1); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,0) = L(8,10)$	$\vert\mathscr{X}(1,0); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,10); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,1) = L(8,1)$	$\vert\mathscr{X}(1,1); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,1); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,2) = L(8,7)$	$\vert\mathscr{X}(1,2); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,7); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,3) = L(8,13)$	$\vert\mathscr{X}(1,3); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,13); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,4) = L(8,4)$	$\vert\mathscr{X}(1,4); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,4); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,-1) = L(5,11)$	$\vert\mathscr{X}(2,-1); \overline{m}_1, \overline{m}_2\rangle = \vert X(5,11); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,0) = L(8,5)$	$\vert\mathscr{X}(2,0); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,5); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,1) = L(8,11)$	$\vert\mathscr{X}(2,1); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,11); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,2) = L(8,2)$	$\vert\mathscr{X}(2,2); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,2); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,3) = L(8,8)$	$\vert\mathscr{X}(2,3); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,8); 5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,4) = L(8,14)$	$\vert\mathscr{X}(2,4); \overline{m}_1, \overline{m}_2\rangle = \vert X(8,14); 5\overline{m}_1+3\overline{m}_2\rangle$

5.4 Other Topics

There has been an enormous amount of work on various aspects of mutually unbiased bases. We summarize some problems, which are not discussed here:

(1) The problem of finding the maximum number of mutually unbiased bases, in a system with dimension which is not a power of a prime number. This is a difficult problem even in the simple case of dimension $d = 6$ [27–31].

(2) The study of various finite geometries, related to finite quantum systems [32–38].

(3) Related to mutually unbiased bases is the so-called ‘King’s problem’ [39–41].

(4) Acting with a unitary transformation on a set of mutually unbiased bases, we get another set of mutually unbiased bases. But there are unitarily inequivalent mutually unbiased bases which have been discussed in [42].

(5) There are links between mutually unbiased bases and latin squares [43] which have been studied in [44–47].

(6) There are links between mutually unbiased bases and designs [48] which have been studied in [49, 50].

(7) We can approach mutually unbiased bases, and also weak mutually unbiased bases, using the formalism of analytic representations discussed in Sect. 4.10. In particular it is interesting to study the zeros of the analytic functions that represent the vectors in mutually unbiased bases, and also in weak mutually unbiased bases. It has been shown in [26], that the duality discussed above is extended to a triality, that involves

- the maximal lines in the finite geometry
- the weak mutually unbiased bases
- the zeros of the analytic functions that represent the vectors in weak mutually unbiased bases.

(8) There is a partial order in the set of all finite geometries $\mathbb{Z}(d) \times \mathbb{Z}(d)$, where $\mathbb{Z}(e) \times \mathbb{Z}(e)$ is a subgeometry of $\mathbb{Z}(d) \times \mathbb{Z}(d)$, when e is a divisor of d. Through duality, there is also a partial order in the set of all weak mutually unbiased bases [51].

(9) Mutually unbiased bases in systems with dimension $d = 2^N$ have been studied in [52, 53].

(10) Deep links between mutually unbiased bases and path integrals, have been studied in [54].

(11) Symmetric informationally complete positive operator valued measures, have been studied in [55–58].

References

1. Batten, L. M. (1997). *Combinatorics of finite geometries*. Cambridge: Cambridge University Press.
2. Hirchfeld, J. W. P. (1979). *Projective geometries over finite fields*. Oxford: Oxford University Press.
3. Hirchfeld, J. W. P., & Thas, J. A. (1991). *General Galois geometries*. Oxford: Oxford University Press.
4. Ivanovic, I. D. (1981). *Journal of Physics A*, *14*, 3241.
5. Wootters, W. K., & Fields, B. D. (1989). *Annals of Physics (N.Y)*, *191*, 363.
6. Bandyopadhyay, S., Boykin, P. O., Roychowdhury, V., & Vatan, F. (2002). *Algorithmica*, *34*, 512.
7. Kibler, M. (2006). *International Journal of Modern Physics B*, *20*, 1792.
8. Kibler, M., & Planat, M. (2006). *International Journal of Modern Physics B*, *20*, 1802.
9. Sulc, P., & Tolar, J. (2007). *Journal of Physics A*, *40*, 15099.
10. Aschbachev, M., Childs, A. M., & Wocjan, P. (2007). *Journal of Algebraic Combinatorics*, *25*, 111.
11. Klimov, A., Romero, J. L., Bjork, G., & Sanchez-Soto, L. L. (2007). *Journal of Physics A*, *40*, 9177.
12. Albouy, O. (2009). *Journal of Physics A*, *42*, 072001.

13. Kibler, M. (2009). *Journal of Physics A*, *42*, 353001.
14. Godsil, C., & Roy, A. (2009). *European Journal of Combinatorics*, *30*, 246.
15. Klimov, A., Romero, J. L., Bjork, G., & Sanchez-Soto, L. L. (2009). *Annals of Physics*, *324*, 53.
16. Durt, T., Englert, B. G., Bengtsson, I., & Zyczkowski, K. (2010). *International Journal of Quantum Computation*, *8*, 535.
17. Daoud, M., & Kibler, M. (2010). *Journal of Physics A*, *43*, 115303.
18. Mandayam, P., Bandyopadhyay, S., Grassl, M., & Wootters, W. K. (2014). *Quantum Information and Computation*, *14*, 823.
19. Seyfarth, U., Sanchez-Soto, L. L., & Leuchs, G. (2014). *Journal of Physics A*, *47*, 455303.
20. Blanchfield, K. (2014). *Journal of Physics A*, *47*, 135303.
21. Kalev, A., & Gour, G. (2014). *New Journal of Physics*, *16*, 053038.
22. Fillipov, S. N., & Man'ko, V. I. (2011). *Physica Scripta*, *2011*, 014010.
23. Shalaby, M., & Vourdas, A. (2011). *Journal of Physics A*, *44*, 345303.
24. Shalaby, M., & Vourdas, A. (2012). *Journal of Physics A*, *45*, 052001.
25. Shalaby, M., & Vourdas, A. (2013). *Annals of Physics*, *337*, 208.
26. Olupitan, T., Lei, C., & Vourdas, A. (2016). *Annals of Physics*, *371*, 1.
27. M. Grassl, arXiv, quant-phys/0406175
28. Brierley, S., & Weigert, S. (2008). *Physical Review A*, *78*, 042312.
29. Brierley, S., & Weigert, S. (2009). *Physical Review A*, *79*, 052316.
30. Jaming, P., Matolcsi, M., Mora, P., Szollosi, F., & Weiner, M. (2009). *Journal of Physics A*, *42*, 245305.
31. Goyeneche, D. (2013). *Journal of Physics A*, *46*, 105301.
32. Calderbank, A. R., Cameron, P. J., Kantor, W. M., & Seidel, J. J. (1997). *Proceedings of the London Mathematical Society*, *75*, 436.
33. Planat, M., Saniga, M., & Kibler, M. (2006). *SIGMA*, *2*, 066.
34. Saniga, M., & Planat, M. (2006). *Journal of Physics A*, *39*, 435.
35. Saniga, M., Planat, M., Kibler, M., & Pracna, P. (2007). *Chaos, Solitons, Fractals*, *33*, 1095.
36. Planat, M., & Baboin, A. C. (2007). *Journal of Physics A*, *40*, F1005.
37. Havlicek, H., & Saniga, M. (2008). *Journal of Physics A*, *41*, 015302.
38. Saniga, M., Levay, P., & Pracna, P. (2012). *Journal of Physics A*, *45*, 295304.
39. Englert, B. G., & Aharanov, Y. (2001). *Physics Letter A*, *284*, 1.
40. Vaidman, L., Aharanov, Y., & Albert, D. Z. (1987). *Physical Review Letters*, *58*, 1385.
41. Kalev, A., Mann, A., & Revzen, M. (2013). *Europhysics Letters*, *104*, 50008.
42. Kantor, W. (2012). *Journal of Mathematical Physics*, *53*, 032204.
43. Denes, J., & Keedwell, A. D. (1974). *Latin squares and their applications*. New York: Academic.
44. Patarek, T., Dikic, B., & Brukner, C. (2009). *Physical Review A*, *79*, 01209.
45. Patarek, T., Pawlowski, M., Grassl, M., & Brukner, C. (2009). *Physical Review A*, *79*, 01209.
46. Hall, J. L., & Rao, A. (2010). *Journal of Physics A*, *43*, 135302.
47. Gaeta, M., di Mateo, O., Klimov, A. B., & de Guise, H. (2014). *Journal of Physics A*, *47*, 435303.
48. Beth, T., Jungnickel, D., & Lenz, H. (1993). *Design theory*. Cambridge: Cambridge University Press.
49. Zauner, G. (2011). *International Journal of Quantum Information*, *1*, 445.
50. Graydon, M., & Appleby, D. M. (2016). *Journal of Physics A*, *49*, 085301.
51. Oladejo, S., Lei, C., & Vourdas, A. (2014). *Journal of Physics A*, *47*, 485204.
52. Durt, T. (2005). *Journal of Physics A*, *38*, 5267.
53. Kern, O., Ranade, K. S., & Seyfarth, U. (2010). *Journal of Physics A*, *43*, 275305.
54. Tolar, J., & Hadzitaskos, G. (2009). *Journal of Physics A*, *42*, 245306.
55. Renes, J. M., Blume-Kohut, R., Scott, A. J., & Caves, C. M. (2004). *Journal of Mathematical Physics*, *45*, 2171.
56. Scott, A. J., & Grassl, M. (2010). *Journal of Mathematical Physics*, *51*, 042203.
57. Appleby, D. M. (2005). *Journal of Mathematical Physics*, *46*, 052107.
58. Appleby, D. M., Flammia, S. T., & Fuchs, C. A. (2011). *Journal of Mathematical Physics*, *52*, 022202.