11. Appendix A: Combinatorial Designs

In this chapter, we briefly introduce some combinatorial designs that are used in this book, including Galois fields, finite projective p lanes, perfect difference sets, orthogonal Latin squares, and tournament designs.

11.1 Galois fields

In this section, we provide a short introduction of Galois fields. More detailed descriptions and their applications in error control codes can be found in [20].

11.1.1 Prime fields

The notion of *group* is one of the most basic mathematical abstraction of an algebraic structure.

Definition 11.1.1. *(***Group***) A group G is a set of elements with an operation $*$ that satisfies the following four properties:*

(i) Closure*: For all a, b in the set, $c = a * b$ is also in the set.*
(ii) Associativity*: For all a, b, c in the set,*

$$a * (b * c) = (a * b) * c.$$

(iii) Identity*: There is an identity element e that satisfies*

$$a * e = e * a = a.$$

(iv) Inverses*: If a is in the set, then there is some element b in the set, called an inverse of a, such that*

$$a * b = b * a = e.$$

If, furthermore, a group G has the additional property,

(v) Commutativity*: For all a, b in the set,*

$$a * b = b * a,$$

then it is called a commutative group *or* abelian group.

If the number of elements in a group G is finite, then it is called a *finite group* and the number of elements in G is called the order of G.

Definition 11.1.2. *(***Field***) A field F is a set of elements with two operations $+$ (addition) and $*$ (multiplication) that satisfy the following properties:*

(i) The set is an abelian group under addition. The identity element under addition is called the zero element.

(ii) The set is closed under multiplication, and the set of nonzero elements is an abelian group under multiplication. The identity element under multiplication is called the one element.

(iii) Distributivity*: For all a, b, c in the set,*

$$(a + b) * c = (a * c) + (b * c).$$

The set of real numbers is a field. So is the set of rational numbers. These fields have an infinite number of elements. A field with a finite number of elements q is called a finite field or a *Galois field*. It is denoted by $GF(q)$. Denote the q elements in $GF(q)$ as $\{0, 1, 2, \ldots, q-1\}$, where 0 is the zero element (the identity element for addition $+$) and 1 is the one element (the identity element for multiplication $*$). We will use $-a$ to denote the (unique) inverse element of a under $+$, and a^{-1} to denote the (unique) inverse element of a under $*$ for $a \neq 0$. As we can treat these two operations as usual addition and multiplication, it is well-known that $-(a+b) = (-a) + (-b)$, $a * 0 = 0 * a = 0$ and $a * (-b) = (-a) * b = -(a * b)$ for the Galois field $GF(q)$. Loosely speaking, we can add, subtract, multiply and divide in a field as in real numbers.

It is well-known that a Galois field $GF(q)$ exists if and only if q is a prime power. In particular, if $q = 2$, the addition in $GF(2)$ is the exclusive-OR operation and the multiplication in $GF(2)$ is the AND operation as shown in the following two tables:

$+$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

. (11.1)

When q is a prime, the addition is the usual addition with the modulo q operation and the multiplication is the usual multiplication with the modulo q operation, i.e.,

$$(a+b) = ((a+b) \bmod q),$$
$$(a*b) = ((a*b) \bmod q).$$

For example, the field $GF(3) = \{0,1,2\}$ has the following addition and multiplication:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

. (11.2)

A field $GF(q)$ with q being a prime is called a *prime filed*.

For the field $GF(4) = \{0,1,2,3\}$, it has the following addition and multiplication:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

. (11.3)

Note that both addition and multiplication in $GF(4)$ are not modulo operations. Also, $GF(2)$ is contained in $GF(4)$ as the two elements 0 and 1 in $GF(4)$ operate the same way as they do in $GF(2)$.

Definition 11.1.3. *For a field F, a subset of F is called a* subfield *if it is a field under the inherited addition and multiplication. The original field F is called an* extension field *of the subfield.*

In view of (11.3), $GF(2)$ is a subfield of $GF(4)$, and $GF(4)$ is an extension field of $GF(2)$.

11.1.2 Finite fields based on polynomials

One can extend a finite field $GF(q)$ to another finite field $GF(q^n)$ by using polynomials. Specifically, for a finite field $GF(q)$, let $x^2 = x*x$ and $x^h = (x^{h-1})*x$ for $h \geq 3$. A polynomial over a field $GF(q)$ is expressed by

$$f(x) = f_{n-1}*x^{n-1} + f_{n-2}*x^{n-2} + \ldots + f_1*x + f_0,$$

where $f_{n-1}, \ldots, f_0$ are elements in $GF(q)$. A monic polynomial is a polynomial with leading coefficient $f_{n-1} = 1$. Two polynomials are equal if their coefficients are all equal. The degree of a polynomial is the index of the leading coefficient f_{n-1}.

One can easily extend addition and multiplication in $GF(q)$ to polynomial addition and polynomial multiplication as follows:

$$\begin{aligned} f(x) + g(x) &= \sum_{i=0}^{\infty} (f_i + g_i) * x^i, \\ f(x) * g(x) &= \sum_{i=0}^{\infty} (\sum_{j=0}^{i} f_j * g_{i-j}) * x^i. \end{aligned}$$

A polynomial $h(x)$ is divisible by a polynomial $f(x)$ if there exists a polynomial $g(x)$ such that

$$h(x) = f(x) * g(x).$$

Definition 11.1.4. *A polynomial $f(x)$ over a field $GF(q)$ that is divisible only by $\alpha f(x)$ or α, where α is any arbitrary element in $GF(q)$, is called an irreducible polynomial. A monic irreducible polynomial of degree at least 1 is called a* prime polynomial.

Theorem 11.1.5. *For a field F and a monic irreducible polynomial $p(x)$, consider the set of polynomials with degree smaller than that of $p(x)$, together with polynomial addition and polynomial multiplication modulo $p(x)$. Denote such a set of polynomials by $F[x]/p(x)$, Define the addition of two polynomials $f(x)$ and $g(x)$ in $F[x]/p(x)$ by $(f(x) + g(x)) \bmod p(x)$ and the multiplication of two polynomials $f(x)$ and $g(x)$ in $F[x]/p(x)$ by $(f(x) * g(x)) \bmod p(x)$. Then $F[x]/p(x)$ is a finite field if and only if $p(x)$ is a prime polynomial.*

Theorem 11.1.5 allows us to extend a finite field $GF(q)$ to a finite field $GF(q^n)$ by using a prime polynomial of degree n over $GF(q)$. For example, to extend $GF(2)$ to $GF(4)$, we consider the prime polynomial $x^2 + x + 1$. Then the extension field contains the four elements $\{0, 1, x, x+1\}$ with the following addition and multiplication:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

,

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

.

These are exactly the same as those in (11.3) by mapping x to 2 and $x+1$ to 3.

Definition 11.1.6. *A primitive element of a field F is an element λ in F such that every field element except zero can be expressed as a power of λ. A primitive polynomial $p(x)$ over F is a prime polynomial over F with the property that the extension field $F[x]/p(x)$ has the primitive element x.*

That the extension field $F[x]/p(x)$ has the primitive element x means that every polynomial in $F[x]/p(x)$ can be represented by $(x^j \bmod p(x))$ for some j.

Theorem 11.1.7. *For every finite field $GF(q)$ and positive integer n, there exists a primitive polynomial over $GF(q)$ of degree n.*

As a direct consequence of Theorem 11.1.7, every element in the extension field $GF(q^n)$ constructed by the primitive polynomial $p(x)$ can be uniquely represented by

$$(x^j \bmod p(x)) = f_{n-1} * x^{n-1} + f_{n-2} * x^{n-2} + \ldots + f_1 * x + f_0,$$

for some coefficients $f_{n-1}, f_{n-2}, \ldots, f_1, f_0$. The vector

$$(f_{n-1}, f_{n-2}, \ldots, f_1, f_0)$$

can be viewed as the *coordinates* of a field element in $GF(q^n)$. For example, consider $GF(4) = \{0, 1, x, x+1\}$ constructed with the prime polynomial $x^2 + x + 1$. Then x is the primitive element of $GF(4)$ with $x^1 = x$, $(x^2 \bmod x^2+x+1) = x+1$, $(x^3 \bmod x^2+x+1) = 1 = x^0$. The coordinates for these four elements are $(0,0), (0,1), (1,0)$ and $(1,1)$.

11.2 Constructions of finite projective planes $PG(2, q)$

In Section 3.1.4, we discussed the connection between finite projective planes and the synchronous modular clock algorithm constructed from Galois fields. In this section, we show that finite projective planes can be in fact constructed by using projective geometry of Galois fields.

Definition 11.2.1. *A finite projective plane of order N is a collection of $N^2 + N + 1$ lines and $N^2 + N + 1$ points such that*

(P1) every line contains $N + 1$ points,
(P2) every point is on $N + 1$ lines,
(P3) any two distinct lines intersect at exactly one point, and
(P4) any two distinct points lie on exactly one line.

To construct a finite projective plane from a Galois field $GF(q)$, we consider a three-dimensional vector space over a Galois field $GF(q)$. Each point in the three-dimensional space can be represented by the three-dimensional coordinates (x_1, x_2, x_3) with x_i being an element in $GF(q)$, $i = 1, 2$ and 3. A finite projective plane, denoted by $PG(2, q)$, can be constructed by projecting all the points $(k * x_1, k * x_2, k * x_3)$ to the same point for any $k \neq 0$. The parameter 2 in $PG(2, q)$ is the dimension and the parameter q in $PG(2, q)$ is the order. For such a projection, a set of $q - 1$ points are projected to a single point. Excluding the point $(0, 0, 0)$, the projective plane $PG(2, q)$ thus has $(q^3 - 1)/(q - 1) = q^2 + q + 1$ points. A line (u_1, u_2, u_3) in $PG(2, q)$ is the set of points that satisfy

$$u_1 * x_1 + u_2 * x_2 + u_3 * x_3 = 0, \tag{11.4}$$

where u_1, u_2, and u_3 are elements in $GF(q)$, not all zero. Suppose that $u_3 \neq 0$. Then we can write

$$x_3 = -(u_3^{-1}) * (u_1 * x_1 + u_2 * x_2).$$

Note that if $x_2 \neq 0$, then (x_1, x_2, x_3) is projected to the same point as $(x_2^{-1} * x_1, 1, x_2^{-1} * x_3)$. For $x_2 = 0$, the only choice for x_1 is 1. For $x_2 = 1$, x_1 can be any element in $GF(q)$. Thus, there are $q+1$ points in the line (u_1, u_2, u_3). In view of the duality between (x_1, x_2, x_3) and (u_1, u_2, u_3) in (11.4), there are $q^2 + q + 1$ lines. It is straightforward to see that any two distinct lines intersect at exactly at one point. By duality, any two distinct points lie on exactly one line. Thus, $PG(2, q)$ satisfies the four properties (P1)-(P4) of a finite projective plane of order q.

Since $GF(q)$ exists when q is a prime power, a finite projective plane of order q also exists (from the above construction of $PG(2, q)$) when q is a prime power. However, as commented in Section 3.1.4, a finite projective plane may not exist for arbitrary q. It was shown by Bose [21] that there is no projective plane of order 6. Moreover, a much more general theorem by Bruck and Ryser [24] provided a necessary condition for the existence of a

finite projective plane of order q when $q = 4m + 1$ or $4m + 2$ for some nonnegative integer m. The necessary condition requires that q to be a sum of two integer squares. However, such a necessary condition is not sufficient. In particular, when $q = 10 = 1^2 + 3^2$, it was shown in [85] by computer enumeration that there is no projective plane of order 10.

11.3 Singer's construction of perfect difference sets

In Section 4.2, we used difference sets to construct CH sequences that achieve maximum rendezvous diversity. In this section, we show how to construct a perfect difference set from the finite projective plane $PG(2, q)$. Such a construction is known as the Singer's construction [119].

Definition 11.3.1. *Let $Z_n = \{0, 1, 2, \ldots, n-1\}$ be the set of nonnegative integers not larger than n. A set $D = \{a_1, a_2, \ldots, a_m\} \subset Z_n$ is called a* Relaxed Difference Set (RDS) *if for every $(d \ mod \ n) \neq 0$, there exists at least one ordered pair (a_i, a_j) such that $a_i - a_j = (d \ mod \ n)$, where $a_i, a_j \in D$. It is called a perfect difference set if there is exactly one ordered pair with that property.*

As mentioned in Theorem 11.1.7 there exists a primitive polynomial over $GF(q)$ of degree ℓ for any positive integer ℓ. For $\ell = 3$, let

$$p(x) = x^3 - a_3 * x^2 - b_3 * x - c_3 \tag{11.5}$$

be a primitive polynomial over $GF(q)$. Then for the extension field $GF(q^3)$, x is a primitive element, i.e., every nonzero element in $GF(q^3)$ can be expressed as $(x^j \bmod p(x))$ for some $j = 0, 1, \ldots, q^3 - 2$ (with $x^{q^3-1} = x^0 = 1$). Let $(\alpha_j, \beta_j, \gamma_j)$ be the the coordinates for $(x^j \bmod p(x))$, i.e.,

$$(x^j \bmod p(x)) = \alpha_j * x^2 + \beta_j * x + \gamma_j. \tag{11.6}$$

Let $n = q^2 + q + 1$. Since $GF(q)$ is a subfield of $GF(q^3)$, x^{jn} is in $GF(q)$ for $j = 0, 1, \ldots, q - 2$. In other words,

$$(x^{jn} \bmod p(x)) = k, \tag{11.7}$$

for some nonzero element $k \in GF(q)$. Recall that in $PG(2, q)$ we map all the points $(k * x_1, k * x_2, k * x_3)$ to the same point for any $k \neq 0$. Thus, x^u and x^v are projected to the same point when $(u \bmod n) = (v \bmod n)$. In view of this, we know that the n points in $PG(2, q)$ can be

expressed as $(x^j \bmod p(x))$ for $j = 0, 1, \ldots, n-1$. Call these n points, $A_0, A_1, \ldots, A_{n-1}$. Note from (11.6) that

$$\begin{aligned}
&(x^{j+1} \bmod p(x)) \\
&= (x * x^j \bmod p(x)) \\
&= (x * (\alpha_j * x^2 + \beta_j * x + \gamma_j) \bmod p(x)) \\
&= ((a_3 * \alpha_j) + \beta_j) * x^2 + ((b_3 * \alpha_j) + \gamma_j) * x + c_3 * \alpha_j.
\end{aligned}$$

Thus,

$$\begin{pmatrix} \alpha_{j+1} \\ \beta_{j+1} \\ \gamma_{j+1} \end{pmatrix} = \begin{pmatrix} a_3 & 1 & 0 \\ b_3 & 0 & 1 \\ c_3 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_j \\ \beta_j \\ \gamma_j \end{pmatrix}. \tag{11.8}$$

Let

$$T = \begin{pmatrix} a_3 & 1 & 0 \\ b_3 & 0 & 1 \\ c_3 & 0 & 0 \end{pmatrix}. \tag{11.9}$$

The linear transformation T then defines a one-to-one mapping that maps the point A_j to the point A_{j+1} for all $j = 0, 1, \ldots, n-1$ (with $A_n = A_0$). Recall that the line (u_1, u_2, u_3) in $PG(2, q)$ contains the set of points A_j that satisfies

$$u_1 * \alpha_j + u_2 * \beta_j + u_3 * \gamma_j = 0. \tag{11.10}$$

Consider the line (u'_1, u'_2, u'_3) that contains the set of points A_{j+1} that satisfies

$$u'_1 * \alpha_{j+1} + u'_2 * \beta_{j+1} + u'_3 * \gamma_{j+1} = 0. \tag{11.11}$$

Thus, if the j^{th} point $(\alpha_j, \beta_j, \gamma_j)$ is in the line (u_1, u_2, u_3), then the $(j+1)^{th}$ point $(\alpha_{j+1}, \beta_{j+1}, \gamma_{j+1})$ is in the line (u'_1, u'_2, u'_3). Using (11.8) in (11.11), we have from (11.10) that

$$(u_1, u_2, u_3) = (u'_1, u'_2, u'_3) \begin{pmatrix} a_3 & 1 & 0 \\ b_3 & 0 & 1 \\ c_3 & 0 & 0 \end{pmatrix}. \tag{11.12}$$

Note that $c_3 \neq 0$ as otherwise $p(x)$ in (11.5) can be factorized into $x(x^2 - a_3 * x - b_3)$ and it will not be a prime polynomial. Thus, the 3×3 matrix in (11.9) is invertible. It is easy to verify that

$$T^{-1} = \begin{pmatrix} 0 & 0 & c_3^{-1} \\ 1 & 0 & -a_3 * c_3^{-1} \\ 0 & 1 & -b_3 * c_3^{-1} \end{pmatrix}, \tag{11.13}$$

and thus

$$(u_1', u_2', u_3') = (u_1, u_2, u_3) \begin{pmatrix} 0 & 0 & c_3^{-1} \\ 1 & 0 & -a_3 * c_3^{-1} \\ 0 & 1 & -b_3 * c_3^{-1} \end{pmatrix}. \tag{11.14}$$

The linear transformation T^{-1} also defines a one-to-one mapping that maps the line (u_1, u_2, u_3) to another line (u_1', u_2', u_3') that contains the $q+1$ points by shifting the $q+1$ points in the line (u_1, u_2, u_3) by 1. The one-to-one mapping of points T and the one-to-one mapping of lines T^{-1} in a finite projective plane is called a *collineation*.

Now suppose that a line (u_1, u_2, u_3) contains a set of $q+1$ points $\{A_{a_0}, A_{a_1}, \ldots, A_{a_q}\}$. Then it follows from the collineation with the 3×3 matrix in (11.8) that the set of $q+1$ points $\{A_{a_0+1}, A_{a_1+1}, \ldots, A_{a_q+1}\}$ is also a line. Similarly, the set of $q+1$ points $\{A_{a_0+d}, A_{a_1+d}, \ldots, A_{a_q+d}\}$ is also a line for any $0 \leq d \leq n-1$. Consider the array

$$\begin{bmatrix} a_0 & a_0+1 & a_0+2 & \cdots & a_0+n-2 & a_0+n-1 \\ a_1 & a_1+1 & a_1+2 & \cdots & a_1+n-2 & a_1+n-1 \\ a_2 & a_2+1 & a_2+2 & \cdots & a_2+n-2 & a_2+n-1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_q & a_q+1 & a_q+2 & \cdots & a_q+n-2 & a_q+n-1 \end{bmatrix}. \tag{11.15}$$

Then every column of the array corresponds to a line in $PG(2,q)$, and the n columns also correspond to the n *distinct* lines in $PG(2,q)$. Also, every row is a cyclic permutation of $(0, 1, 2 \ldots, n)$ and corresponds to the n points in $PG(2,q)$. Without loss of generality, let us assume that $a_0 = 0$ and consider the columns (resp. lines) that contains 0 (resp. point A_0). As $PG(2,q)$ is a finite projective plane of order q, there are $q+1$ lines that contains point A_0. These $q+1$ lines correspond to the following $q+1$ columns in (11.15):

$$\begin{bmatrix} a_0-a_0 & a_0-a_1 & a_0-a_2 & \cdots & a_0-a_{n-1} \\ a_1-a_0 & a_1-a_1 & a_1-a_2 & \cdots & a_1-a_{n-1} \\ a_2-a_0 & a_2-a_1 & a_2-a_2 & \cdots & a_2-a_{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_q-a_0 & a_q-a_1 & a_q-a_2 & \cdots & a_q-a_{n-1} \end{bmatrix}. \tag{11.16}$$

Note that the $q+1$ diagonal elements in the $(q+1) \times (q+1)$ array in (11.16) are 0. As these $q+1$ lines already contain point A_0, all the other points in

these $q+1$ lines must be distinct. Thus, $(a_i - a_j)$ must be distinct for $i \neq j$, $i, j = 0, 1, \ldots, q$. This shows that $D = \{a_0, a_1, \ldots, a_q\}$ a perfect difference set in Z_n, where $n = q^2 + q + 1$.

In view of (11.16), it is also clear that for a perfect difference set $D = \{a_0, a_1, \ldots, a_q\}$ in Z_n, then $D_i = \{\{a_0 + i, a_1 + i, \ldots, a_q + i\}$, $i = 0, 1, \ldots, n$ are the n lines in a finite projective plane of order n with the n points in Z_n. Also, if t is coprime to n, then the set $\{t*a_0, t*a_1, \ldots, t*a_q\}$ is a perfect difference set in Z_n. This is because $t * (a_i - a_j) \bmod n$ are also distinct for $i \neq j$, $i, j = 0, 1, \ldots, q$ when t is coprime to n. Such a property was used in [122, 130] for searching for disjoint perfect difference sets.

As an illustrating example, we use the following cubic primitive polynomial over $GF(2)$ to construct a perfect different set in Z_7:

$$p(x) = x^3 + x + 1. \tag{11.17}$$

The corresponding collineation mapping T is

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{11.18}$$

Since $T(x^j) = x^{j+1}$ for all j, the coordinates of $x^j = (\alpha_j, \beta_j, \gamma_j)$, $j = 0, 2, \ldots, 6$ are

$$\begin{aligned} x^0 &= (0, 0, 1) \\ x^1 &= (0, 1, 0) \\ x^2 &= (1, 0, 0) \\ x^3 &= (0, 1, 1) \\ x^4 &= (1, 1, 0) \\ x^5 &= (1, 1, 1) \\ x^6 &= (1, 0, 1). \end{aligned} \tag{11.19}$$

As expected, we have $x^7 = x^0 = (0, 0, 1)$.

Consider the line $(u_1, u_2, u_3) = (1, 0, 0)$. Call this line L_0. Then it follows from (11.10) that L_0 contains the three points $\{x^0, x^1, x^3\}$. Note that

$$T^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}. \tag{11.20}$$

Thus, the collineation mapping T^{-1} can be used for constructing L_j, $j = 1, \ldots, 6$, by

$$(u'_1, u'_2, u'_3) = (u_1, u_2, u_3) \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}. \tag{11.21}$$

This leads to

$$\begin{aligned} L_0 &= (1,0,0) = \{x^0, x^1, x^3\} \\ L_1 &= (0,0,1) = \{x^1, x^2, x^4\} \\ L_2 &= (0,1,1) = \{x^2, x^3, x^5\} \\ L_3 &= (1,1,1) = \{x^3, x^4, x^6\} \\ L_4 &= (1,1,0) = \{x^4, x^5, x^0\} \\ L_5 &= (1,0,1) = \{x^5, x^6, x^1\} \\ L_6 &= (0,1,0) = \{x^6, x^0, x^2\}. \end{aligned} \tag{11.22}$$

Note that the seven lines in (11.22) and the seven points in (11.19) form the finite projective plane $PG(2,2)$ (see Figure 11.1). The perfect difference set in Z_7 constructed from using the primitive polynomial in (11.17) is $D = \{0,1,3\}$.

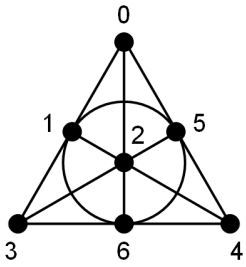

Fig. 11.1. The finite projective plane $PG(2,2)$.

11.4 Constructions of orthogonal Latin squares

In this section, we discuss the connection between orthogonal Latin squares and CH sequences used in this book, including the synchronous modular clock algorithm in a Galois field in Section 3.1.2 and the ORTHO-CH sequence in Section 6.3.1.

Definition 11.4.1. ***(Latin square and orthogonal Latin squares)*** *A Latin square with the set of symbols S is an $|S| \times |S|$ matrix such that every symbol appears exactly once in every row and every column. Two $N \times N$ Latin*

squares $A = (a_{i,j})$ *and* $B = (b_{i,j})$ *are said to be* orthogonal *if the ordered pairs* $(a_{i,j}, b_{i,j})$ *are all different for all* $i, j = 0, 1, \ldots, N-1$.

In the following, we show two 4×4 orthogonal Latin squares with $S = \{0, 1, 2, 3\}$.

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix}. \tag{11.23}$$

Merging these two matrices together yields

$$\begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{bmatrix}. \tag{11.24}$$

Thus, each of the 16 ordered pairs appears exactly once.

The number of mutually orthogonal Latin squares of order N is not greater than $N-1$. If N is a prime power, then there exist $N-1$ mutually orthogonal Latin squares. These $N-1$ mutually orthogonal Latin squares can be constructed by using a Galois filed $GF(N)$ with the N elements $\{0, 1, \ldots, N-1\}$. Specifically, denote the $N-1$ orthogonal Latin squares by $\{C^{(r)} = (c_{i,j}^{(r)}), r = 1, 2, \ldots, N-1\}$. Then for $r = 1, 2, \ldots, N-1$ and $i, j = 0, 1, \ldots, N-1$, let

$$c_{i,j}^{(r)} = (r * i + j),$$

where $+$ and $*$ are the addition and multiplication in $GF(N)$. For $N = 5$, the four orthogonal Latin squares are as follows:

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}, \tag{11.25}$$

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}. \tag{11.26}$$

These four orthogonal Latin squares are also the four orthogonal $(5, 5)$-MACH matrices in Section 6.3.1.

Orthogonal Latin squares also correspond to the CH sequences from the synchronous modular clock algorithm with nonzero slopes. For instance, if $N = 5$, there are four mutually orthogonal Latin squares. The $(b + 1)^{th}$ row ($b = 0, 1, 2, 3, 4$) of the r^{th} ($r = 1, 2, 3, 4$) Latin square is generated by the CH sequence from the synchronous modular clock algorithm with the nonzero slope r and bias b for $t = 1, 2, 3, 4, 5$. This can be seen from (3.4) and (3.5) by removing the first columns of these four matrices. Note that even the matrix generated from $r = 0$ is not a Latin square, it is still orthogonal to the four matrices in the sense that the ordered pairs (i, j) are all different for all $i, j = 1, 2, \ldots, N$.

Remark 11.4.2. The study of the existence of two orthogonal Latin squares (also known as the Graeco-Latin square) was first proposed by L. Euler in 1782 [59]. He was not able to construct two orthogonal Latin squares of order 6 (known as the 36 officers problem) and then conjectured that there do not exist two orthogonal Latin squares of order N for $N = 4m+2$, where m is a nonnegative integer. It was confirmed later by G. Tarry via exhaustive enumeration that there do not exist two orthogonal Latin squares of order 6. However, via extensive computer enumeration, two orthogonal Latin squares of order 10 and order 22 were found and it was later shown that Euler's conjecture is false for all $N \geq 10$. We now know that two orthogonal Latin squares exist for all $N \geq 3$ except $N = 6$.

In the following, we show how to construct two $N \times N$ orthogonal Lain squares for any odd N by using rotators and reflectors.

Definition 11.4.3. ***(Rotator)*** *An* $N \times N$ rotator *is a Latin square with the set of symbols* $S = \{0, 1, 2, \ldots, N - 1\}$*, where symbol* $n = 0, 1, 2, \ldots, N - 1$ *appears at the* $(i, j)^{th}$ *element of the Latin square (with* $i, j = 0, 1, 2, \ldots, N-1$*), when*

$$j = (i + n) \ mod \ N. \tag{11.27}$$

Here is the 3×3 rotator.

$$\begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}. \tag{11.28}$$

Definition 11.4.4. ***(Reflector)*** *An* $N \times N$ reflector *is a Latin square with the set of symbols* $S = \{0, 1, 2, \ldots, N-1\}$*, where symbol* $n = 0, 1, 2, \ldots, N-1$ *appears at the* $(i, j)^{th}$ *element of the Latin square (with* $i, j = 0, 1, 2, \ldots, N-1$*) when*

$$n = (i + j) \text{ mod } N. \tag{11.29}$$

Here is the 3×3 reflector.

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}. \tag{11.30}$$

Lemma 11.4.5. *The* $N \times N$ *rotator and the* $N \times N$ *reflector are orthogonal if* N *is an odd number.*

Proof. It suffices to show that the ordered pair (n_1, n_2) appears exactly once. To see this, we note from (11.27) and (11.29) that the ordered pair (n_1, n_2) appears at the $(i, j)^{th}$ element with

$$j = (i + n_1) \text{ mod } N,$$

and

$$n_2 = (i + j) \text{ mod } N.$$

Thus, we have

$$2j = (n_1 + n_2) \text{ mod } N \tag{11.31}$$

and

$$2i = (n_2 - n_1) \text{ mod } N. \tag{11.32}$$

Since N is an odd number, there is a unique j in $\{0, 1, 2 \ldots, N-1\}$ that satisfies (11.31). Similarly, there is a unique i in $\{0, 1, 2 \ldots, N-1\}$ that satisfies (11.32). ■

As in Section 4.8.1, one can also use the direct product construction to construct larger orthogonal Latin squares [99]. Specifically, if $\{A^{(r)} = (a_{i,j}^{(r)}), r = 1, 2, \ldots, R-1\}$ are $N_1 \times N_1$ orthogonal Latin squares with symbols in $\{0, 1, \ldots, N_1 - 1\}$, and $\{B^{(r)} = (b_{i,j}^{(r)}), r = 1, 2, \ldots, R-1\}$ are $N_2 \times N_2$ orthogonal Latin squares with symbols in $\{0, 1, \ldots, N_2 - 1\}$, then

$\{C^{(r)} = (c_{i,j}^{(r)}), r = 1, 2, \ldots, R-1\}$ are $(N_1 \times N_2) \times (N_1 \times N_2)$ orthogonal Latin squares with symbols in $\{0, 1, \ldots, N_1 N_2 - 1\}$, where

$$\begin{aligned} c_{i,j}^{(r)} &= a_{i_a,j_a}^{(r)} * N_2 + b_{i_b,j_b}^{(r)}, \\ i_a &= \lfloor i/N_2 \rfloor, \\ j_a &= \lfloor j/N_2 \rfloor, \\ i_b &= i - i_a * N_2, \\ j_b &= j - j_b * N_2. \end{aligned}$$

For instance, let $A^{(1)}$ and $A^{(2)}$ be the two 3×3 orthogonal Latin squares in (11.28) and (11.30), and $B^{(1)}$ and $B^{(2)}$ be the two 4×4 orthogonal Latin squares in (11.23). Then we have the following two 12×12 orthogonal Latin squares $C^{(1)}$ and $C^{(2)}$:

$$\left[\begin{array}{cccc|cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 \\ \hline 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 9 & 8 & 11 & 10 & 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\ 10 & 11 & 8 & 9 & 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 11 & 10 & 9 & 8 & 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ \hline 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 \\ 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 & 1 & 0 & 3 & 2 \\ 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 & 2 & 3 & 0 & 1 \\ 7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 & 3 & 2 & 1 & 0 \end{array}\right], \quad (11.33)$$

and

$$\left[\begin{array}{cccc|cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 \\ \hline 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 \\ 7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 & 3 & 2 & 1 & 0 \\ 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 & 1 & 0 & 3 & 2 \\ 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 & 2 & 3 & 0 & 1 \\ \hline 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 11 & 10 & 9 & 8 & 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ 9 & 8 & 11 & 10 & 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\ 10 & 11 & 8 & 9 & 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \end{array}\right]. \quad (11.34)$$

11.5 Constructions of balanced tournament deigns

A tournament design with side N, denoted by $TD(N)$, is to arrange the $N(2N-1)$ distinct unordered pairs $\{\{i,j\} : 0 \leq i \neq j \leq 2N-1\}$ into an $N \times (2N-1)$ array with the following property:

(i) Every element in $\{0, 1, \ldots, 2N-1\}$ is contained in precisely one cell of each column.

In Section 3.1.3, we have shown a simple construction of a $TD(N)$ by using the SYNC-ETCH algorithm (Algorithm 1 in [144]). A *balanced tournament design* with side N, denoted by $BTD(N)$, is a $TD(N)$ that satisfies the following additional property:

(ii) No element in $\{0, 1, \ldots, 2N-1\}$ is contained in more than two cells of any row.

11.5.1 $BTD(N)$ constructions when N is an odd number

In this section, we show how one can apply the *perfect rainbow matching* algorithm in [144] to construct a $BTD(N)$ when N is an odd number. For this, we view the $2N-1$ columns (in the $N(2N-1)$ array) as $2N-1$ time slots, indexed from $0, 1, \ldots, 2N-2$, and the N rows (in the $N(2N-1)$ array) as the N channels, indexed from $0, 1, \ldots, N-1$.

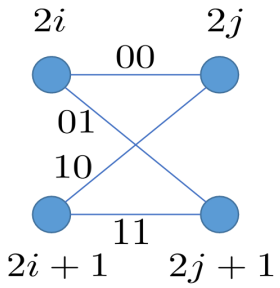

Fig. 11.2. The Monochromatic Complete Bipartite graph $MCB_{i,j}$.

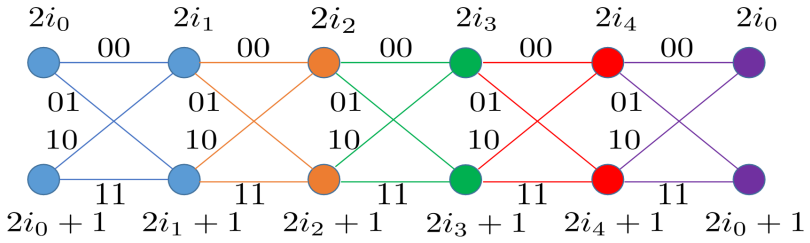

Fig. 11.3. A chain of 5 MCBs.

The detailed steps of the perfect rainbow matching algorithm are shown below:

Step 1. (Initial assignment at time 0) At time 0, assign the N unordered pairs $\{2k, 2k+1\}$ to channel k, $k = 0, 1, \ldots, N-1$. For instance, suppose that $N = 5$ and $2N-1 = 9$. Then after Step 1, $\{0, 1\}$ is assigned to channel 0 at time 0, $\{2, 3\}$ is assigned to channel 1 at time 0, $\{4, 5\}$ is assigned to channel 2 at time 0, $\{6, 7\}$ is assigned to channel 3 at time 0, $\{8, 9\}$ is assigned to channel 4 at time 0.

Step 2. (MCBs) Excluding the N unordered pairs assigned at time 0, there are $N(2N-2)$ unordered pairs remained to be assigned. As N is an odd number, $2N-2$ is an integer multiple of 4. These $N(2N-2)$ unordered pairs can be partitioned into $N(N-1)/2$ groups, each with four unordered pairs. Call the four unordered pairs $\{\{2i, 2j\}, \{2i+1, 2j\}, \{2i, 2j+1\}, \{2i+1, 2j+1\}\}$ the Monochromatic Complete Bipartite (MCB) graph induced from the two unordered pairs $\{2i, 2i+1\}$ and $\{2j, 2j+1\}$ (as the two left-hand side nodes and the two right-hand side nodes of the bipartite graph shown in Figure 11.2). We denote it by $MCB_{i,j}$. Note that $MCB_{i,j} = MCB_{j,i}$ as they both represent the same four unordered pairs $\{\{2i, 2j\}, \{2i+1, 2j\}, \{2i, 2j+1\}, \{2i+1, 2j+1\}\}$. As such, there are $N(N-1)/2$ distinct MCBs. Also, as there are four unordered pairs in an MCB, each MCB needs four time slots (in the $N(2N-1)$ array). For $N = 5$, there are 10 MCBs.

Step 3. (Channel assignments for MCBs) For $k = 0, 1, \ldots, N-1$, and $d = 1, 2, \ldots, (N-1)/2$, assign $MCB_{(k+d) \bmod N, (k-d) \bmod N}$ to channel k for the four consecutive time slots $4(d-1)+1, 4(d-1)+2, 4(d-1)+3$, and $4(d-1)+4$. This ensures that every symbol appears exactly twice in channel k, except symbols $2k$ and $2k+1$ (that appear once at time 0). As such, Property (ii) is satisfied. For $N = 5$, we have $d = 1$ or 2.

For $d = 1$ and $k = 0$, $MCB_{1,4} = \{\{2, 8\}, \{3, 8\}, \{2, 9\}, \{3, 9\}\}$ is assigned to channel 0 for time slots 1,2,3,4.
For $d = 1$ and $k = 1$, $MCB_{2,0} = \{\{4, 0\}, \{5, 0\}, \{4, 1\}, \{5, 1\}\}$ is assigned to channel 1 for time slots 1,2,3,4.
For $d = 1$ and $k = 2$, $MCB_{3,1} = \{\{6, 2\}, \{7, 2\}, \{6, 3\}, \{7, 3\}\}$ is assigned to channel 2 for time slots 1,2,3,4.
For $d = 1$ and $k = 3$, $MCB_{4,2} = \{\{8, 4\}, \{9, 4\}, \{8, 5\}, \{9, 5\}\}$ is assigned to channel 3 for time slots 1,2,3,4.
For $d = 1$ and $k = 4$, $MCB_{0,3} = \{\{0, 6\}, \{1, 6\}, \{0, 7\}, \{1, 7\}\}$ is assigned to channel 4 for time slots 1,2,3,4.
For $d = 2$ and $k = 0$, $MCB_{2,3} = \{\{4, 6\}, \{5, 6\}, \{4, 7\}, \{5, 7\}\}$ is assigned to channel 0 for time slots 5,6,7,8.
For $d = 2$ and $k = 1$, $MCB_{3,4} = \{\{6, 8\}, \{7, 8\}, \{6, 9\}, \{7, 9\}\}$ is assigned to channel 1 for time slots 5,6,7,8.
For $d = 2$ and $k = 2$, $MCB_{4,0} = \{\{8, 0\}, \{9, 0\}, \{8, 1\}, \{9, 1\}\}$ is assigned to channel 2 for time slots 5,6,7,8.
For $d = 2$ and $k = 3$, $MCB_{0,1} = \{\{0, 2\}, \{1, 2\}, \{0, 3\}, \{1, 3\}\}$ is assigned to channel 3 for time slots 5,6,7,8.
For $d = 2$ and $k = 4$, $MCB_{1,2} = \{\{2, 4\}, \{3, 4\}, \{2, 5\}, \{3, 5\}\}$ is assigned to channel 4 for time slots 5,6,7,8.

Step 4. (A chain of MCBs) A set of L MCBs is called a chain of MCBs (CMCBs) if they can be arranged in the way that

$$MCB_{i_0,i_1} \to MCB_{i_1,i_2} \to \dots \quad \to MCB_{i_{L-2},i_{L-1}} \to MCB_{i_{L-1},i_0}. \tag{11.35}$$

In Figure 11.3, we show a chain of 5 MCBs. For a fixed d, if N and d are coprime, then there exists a unique $\ell \in \{0, 1, \dots, N-1\}$ such that $k = (-2\ell d) \bmod N$ for any $k \in \{0, 1, \dots, N-1\}$. Now we can rearrange the N MCBs (for a fixed d) in Step 3 in the order of $MCB_{(d-2\ell d) \bmod N,(-d-2\ell d) \bmod N}$, $\ell = 0, 1, \dots, N-1$. Since

$$(-d - 2\ell d) \bmod N = (d - 2(\ell + 1)d) \bmod N,$$

we have

$$MCB_{d,-d \bmod N} \to MCB_{-d \bmod N,-3d \bmod N} \to \dots$$
$$\to MCB_{5d \bmod N,3d \bmod N} \to MCB_{3d \bmod N,d}.$$

Thus, the N MCBs arranged this way form a chain of N MCBs. For the case that N and d are not coprime, then $MCB_{(d-2\ell d) \bmod N,(-d-2\ell d) \bmod N}$,

$\ell = 0, 1, \ldots, N-1$, can be further partitioned into several smaller CMCBs. For $N = 5$ and $d = 1$, $MCB_{1,4}$, $MCB_{4,2}$, $MCB_{2,0}$, $MCB_{0,3}$, and $MCB_{3,1}$ form a CMCB. Similarly, for $N = 5$ and $d = 2$, $MCB_{2,3}$, $MCB_{3,4}$, $MCB_{4,0}$, $MCB_{0,1}$, and $MCB_{1,2}$ form a CMCB.

Step 5. (Time slot assignments for a chain of MCBs) Call the four unordered pairs $\{2i, 2j\}, \{2i+1, 2j\}, \{2i, 2j+1\}$, and $\{2i+1, 2j+1\}$ in a $MCB_{i,j}$ the *00*, *10*, *01* and *11* pairs of $MCB_{i,j}$. For a chain of L MCBs in (11.35) (with L being an odd number not smaller than 3), let T_0 be the set of pairs consisting of the 00 pair from MCB_{i_0,i_1}, the 11 pair from MCB_{i_{L-1},i_0}, and the 10 pair from the rest of MCBs, i.e.,

$$00 \to 10 \to 10 \to 10 \to \ldots \to 10 \to 10 \to 11.$$

Let T_1 be the set of pairs consisting of the 11 pair from MCB_{i_0,i_1}, the 00 pair from MCB_{i_{L-1},i_0}, and the 01 pair from the rest of MCBs, i.e.,

$$11 \to 01 \to 01 \to 01 \to \ldots \to 01 \to 01 \to 00.$$

Let T_2 be the set of pairs consisting of the 01 pair from MCB_{i_0,i_1}, the 10 pair from MCB_{i_{L-1},i_0}, the 00 pair from $MCB_{i_\ell,i_{\ell+1}}$ for an odd ℓ, and the 11 pair from $MCB_{i_\ell,i_{\ell+1}}$ for an even ℓ, i.e.,

$$01 \to 00 \to 11 \to 00 \to \ldots \to 11 \to 00 \to 10.$$

Let T_3 be the set of pairs consisting of the 10 pair from MCB_{i_0,i_1}, the 01 pair from MCB_{i_{L-1},i_0}, the 11 from $MCB_{i_\ell,i_{\ell+1}}$ for an odd ℓ, and the 00 pair from $MCB_{i_\ell,i_{\ell+1}}$ for an even ℓ, i.e.,

$$10 \to 11 \to 00 \to 11 \to \ldots \to 00 \to 11 \to 01.$$

Assign the set of pairs in T_s, $s = 0, 1, 2, 3$ in the s^{th} time slot. By doing so, we ensure that every symbol in a chain of MCBs appears exactly once in a time slot. In Figure 11.4, we show the assignment of the four time slots, T_0, T_1, T_2 and T_3 for a chain of 5 MCBs.

For $N = 5$ and $d = 1$, the time slot assignments for the CMCB, $MCB_{1,4}$, $MCB_{4,2}$, $MCB_{2,0}$, $MCB_{0,3}$, and $MCB_{3,1}$, are

$$\begin{aligned}
T_0 &= \{\{2,8\},\{9,4\},\{5,0\},\{1,6\},\{7,3\}\},\\
T_1 &= \{\{3,9\},\{8,5\},\{4,1\},\{0,7\},\{6,2\}\},\\
T_2 &= \{\{2,9\},\{8,4\},\{5,1\},\{0,6\},\{7,2\}\},\\
T_3 &= \{\{3,8\},\{9,5\},\{4,0\},\{1,7\},\{6,3\}\}.
\end{aligned}$$

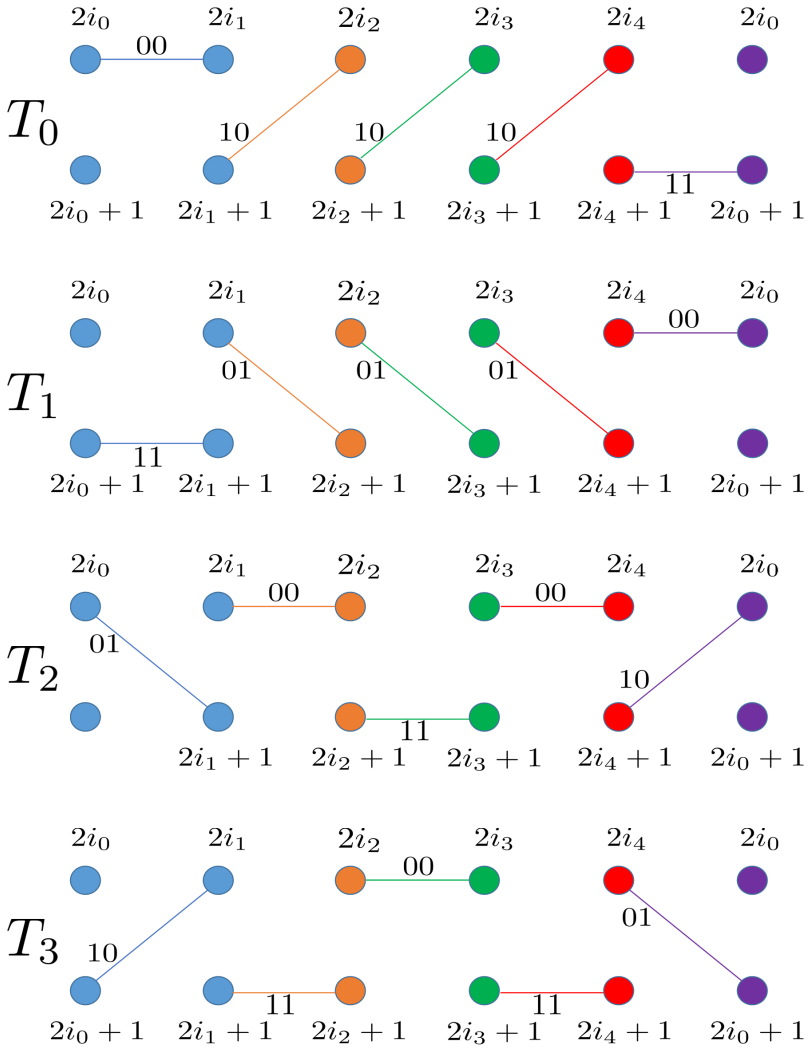

Fig. 11.4. The assignment of the four time slots, T_0, T_1, T_2 and T_3 for a chain of 5 MCBs.

Similarly, for $N = 5$ and $d = 2$, the time slot assignments for the CMCB, $MCB_{2,3}$, $MCB_{3,4}$, $MCB_{4,0}$, $MCB_{0,1}$, and $MCB_{1,2}$, are

$$\begin{aligned} T_0 &= \{\{4,6\},\{7,8\},\{9,0\},\{1,2\},\{3,5\}\}, \\ T_1 &= \{\{5,7\},\{6,9\},\{8,1\},\{0,3\},\{2,4\}\}, \\ T_2 &= \{\{4,7\},\{6,8\},\{9,1\},\{0,2\},\{3,4\}\}, \\ T_3 &= \{\{5,6\},\{7,9\},\{8,0\},\{1,3\},\{2,5\}\}. \end{aligned}$$

This then leads to the BTD(5) shown in Table 11.1.

Table 11.1. A BTD(5) from the perfect rainbow matching algorithm

	0	1	2	3	4	5	6	7	8
0	$\{0,1\}$	$\{2,8\}$	$\{3,9\}$	$\{2,9\}$	$\{3,8\}$	$\{4,6\}$	$\{5,7\}$	$\{4,7\}$	$\{5,6\}$
1	$\{2,3\}$	$\{5,0\}$	$\{4,1\}$	$\{5,1\}$	$\{4,0\}$	$\{7,8\}$	$\{6,9\}$	$\{6,8\}$	$\{7,9\}$
2	$\{4,5\}$	$\{7,3\}$	$\{6,2\}$	$\{7,2\}$	$\{6,3\}$	$\{9,0\}$	$\{8,1\}$	$\{9,1\}$	$\{8,0\}$
3	$\{6,7\}$	$\{9,4\}$	$\{8,5\}$	$\{8,4\}$	$\{9,5\}$	$\{1,2\}$	$\{0,3\}$	$\{0,2\}$	$\{1,3\}$
4	$\{8,9\}$	$\{1,6\}$	$\{0,7\}$	$\{0,6\}$	$\{1,7\}$	$\{3,5\}$	$\{2,4\}$	$\{3,4\}$	$\{2,5\}$

11.5.2 The doubling construction

In this section, we show there exists a $BTD(N)$ for $N \neq 2$. The approach is based on the doubling construction. A factored $BTD(N)$, denoted by $FBTD(N)$, satisfies the following additional property:

(iii) In each row there exist N cells, called a factor, that contain all the $2N$ elements in $\{0, 1, 2, \ldots, 2N-1\}$.

In Table 11.2, we showed an FBTD(4) from [87], where the 4 underlined cells in each row form a factor that contains all the symbols in $\{0, 1, \ldots, 7\}$.

Table 11.2. An FBTD(4) with a factor in each row that contains the underlined cells in that row

	0	1	2	3	4	5	6
0	$\{\underline{3},\underline{4}\}$	$\{\underline{5},\underline{6}\}$	$\{\underline{1},\underline{2}\}$	$\{\underline{0},\underline{7}\}$	$\{4,5\}$	$\{6,7\}$	$\{0,3\}$
1	$\{1,6\}$	$\{2,4\}$	$\{3,5\}$	$\{\underline{4},\underline{6}\}$	$\{\underline{0},\underline{2}\}$	$\{\underline{1},\underline{3}\}$	$\{\underline{5},\underline{7}\}$
2	$\{\underline{2},\underline{7}\}$	$\{0,1\}$	$\{4,7\}$	$\{\underline{1},\underline{5}\}$	$\{\underline{3},\underline{6}\}$	$\{\underline{0},\underline{4}\}$	$\{2,6\}$
3	$\{0,5\}$	$\{\underline{3},\underline{7}\}$	$\{\underline{0},\underline{6}\}$	$\{2,3\}$	$\{1,7\}$	$\{\underline{2},\underline{5}\}$	$\{\underline{1},\underline{4}\}$

Now we argue that a $BTD(N)$ constructed from the perfect rainbow matching algorithm is also an $FBTD(N)$. In Step 3 of the perfect rainbow matching algorithm, $MCB_{(k+d) \bmod N,(k-d) \bmod N}$, $d = 1, 2, \ldots, (N-1)/2$, are assigned to channel k. The two unordered pairs $\{2((k+d) \bmod N), 2((k-d) \bmod N)+1\}$ and $\{2((k+d) \bmod N)+1, 2((k-d) \bmod N)\}$ are assigned to two time slots on channel k for each $d = 1, 2, \ldots, (N-1)/2$. Along with the initial assignment of the unordered pair $\{2k, 2k+1\}$ to channel k at time 0, we know that for each row, there exist N cells that contain all the $2N$ elements in $\{0, 1, 2, \ldots, 2N-1\}$.

The doubling construction can be used to construct an $FBTD(2N)$ if there exists an $FBTD(N)$ and two $2N \times 2N$ orthogonal Latin squares.

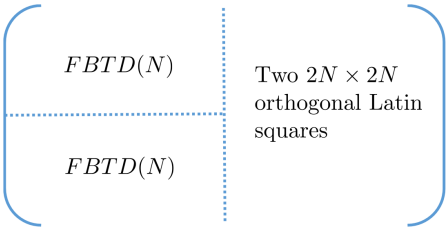

Fig. 11.5. The doubling construction of an $FBTD(2N)$ by stacking two $FBTD(N)$'s and appending two $2N \times 2N$ orthogonal Latin squares.

The idea is to stack two $FBTD(N)$'s in the front and then append two orthogonal Latin squares in the end (see Figure 11.5). The detailed steps are depicted as follows:
Step 1. Partition $\{0, 1, \ldots, 4N-1\}$ into two sets $S_1 = \{0, 1, \ldots, 2N-1\}$ and $S_2 = \{2N, 2N+1, \ldots, 4N-1\}$.

Step 2. (Factor cells and non-factor cells) For the $FBTD(N)$, call the cells in a factor of a row the *factor cells*. The rest of cells are called *non-factor cells*. As such, there are N^2 factor cells and $N(N-1)$ non-factor cells. Since each symbol appears exactly once in the factor cells in a row, and at most twice in a row, it appears at most once in the non-factor cells in a row.

Step 3. (Stacking two $FBTD(N)$'s) Since an $FBTD(N)$ is an $N \times (2N-1)$ array, we stack two $FBTD(N)$'s to form a $2N \times (2N-1)$ array. Call the array that contains the first N rows the *upper* $FBTD(N)$ and the array that contains the last N rows the *lower* $FBTD(N)$.

Step 4. (Interleaving assignments) For the $N(2N-1)$ unordered pairs $\{\{i, j\} : i \in S_1, j \in S_1\}$, we assign them to the factor cells in the upper $FBTD(N)$ and the non-factor cells in the lower $FBTD(N)$. On the other hand, for the $N(2N-1)$ unordered pairs $\{\{i, j\} : i \in S_2, j \in S_2\}$, we assign them to the factor cells in the lower $FBTD(N)$ and the non-factor cells in the upper $FBTD(N)$. By doing so, every element in $\{0, 1, \ldots, 4N-1\}$ is contained in precisely one cell of each column for the first $2N-1$ columns.

Step 5. (Appending two orthogonal Latin squares) Append the two $2N \times 2N$ orthogonal Latin squares to the $2N \times (2N-1)$ array to form a $2N \times (4N-1)$ array. Map S_1 to the symbols in the first Latin square and S_2 to the symbols in the second Latin square. As these two Latin squares are orthogonal, each of the N^2 unordered pairs $\{\{i, j\} : i \in S_1, j \in S_2\}$ appears exactly once.

Moreover, the $2N$ cells in the last $2N$ columns of a row form a factor for the constructed $FBTD(2N)$.

Theorem 11.5.1. *([86]) There exists an $FBTD(N)$ for all $N \neq 2$.*

Proof. We have shown an $FBTD(4)$ in Table 11.2. Using the perfect rainbow matching algorithm, one can construct an $FBTD(N)$ for an odd N. The doubling construction allows us to construct an $FBTD(2N)$ if there exists an $FBTD(N)$ and two $2N \times 2N$ orthogonal Latin squares. Since there exist two $2N \times 2N$ orthogonal Latin squares except for $N = 1$ and $N = 3$, we know that there exists an $FBTD(N)$ except for $N = 2$ and $N = 6$. In Figure 11.6, we show an $FBTD(6)$ from [87]. By an exhaustive enumeration of cases, it is easy to see that there does not exist a $BTD(2)$.

	0	1	2	3	4	5	6	7	8	9	10
0	$\{10,\underline{8}\}$	$\{\underline{4},\underline{6}\}$	$\{6,\underline{2}\}$	$\{\underline{11},\underline{0}\}$	$\{0,\underline{3}\}$	$\{\underline{10},\underline{3}\}$	$\{\underline{9},\underline{1}\}$	$\{1,\underline{7}\}$	$\{11,\underline{5}\}$	$\{\underline{5},\underline{8}\}$	$\{\underline{2},\underline{7}\}$
1	$\{\underline{6},\underline{9}\}$	$\{10,\underline{9}\}$	$\{\underline{5},\underline{7}\}$	$\{7,\underline{3}\}$	$\{\underline{11},\underline{1}\}$	$\{1,\underline{4}\}$	$\{\underline{10},\underline{4}\}$	$\{\underline{0},\underline{2}\}$	$\{2,\underline{8}\}$	$\{11,\underline{6}\}$	$\{\underline{3},\underline{8}\}$
2	$\{11,\underline{7}\}$	$\{\underline{7},\underline{0}\}$	$\{10,\underline{0}\}$	$\{\underline{6},\underline{8}\}$	$\{8,\underline{4}\}$	$\{\underline{11},\underline{2}\}$	$\{2,\underline{5}\}$	$\{\underline{10},\underline{5}\}$	$\{\underline{1},\underline{3}\}$	$\{3,\underline{9}\}$	$\{\underline{4},\underline{9}\}$
3	$\{4,\underline{0}\}$	$\{11,\underline{8}\}$	$\{\underline{8},\underline{1}\}$	$\{10,\underline{1}\}$	$\{\underline{7},\underline{9}\}$	$\{9,\underline{5}\}$	$\{\underline{11},\underline{3}\}$	$\{3,\underline{6}\}$	$\{\underline{10},\underline{6}\}$	$\{\underline{4},\underline{2}\}$	$\{\underline{5},\underline{0}\}$
4	$\{\underline{5},\underline{3}\}$	$\{5,\underline{1}\}$	$\{11,\underline{9}\}$	$\{\underline{9},\underline{2}\}$	$\{10,\underline{2}\}$	$\{\underline{8},\underline{0}\}$	$\{0,\underline{6}\}$	$\{\underline{11},\underline{4}\}$	$\{4,\underline{7}\}$	$\{\underline{10},\underline{7}\}$	$\{\underline{6},\underline{1}\}$
5	$\{\underline{1},\underline{2}\}$	$\{2,\underline{3}\}$	$\{\underline{3},\underline{4}\}$	$\{4,\underline{5}\}$	$\{\underline{5},\underline{6}\}$	$\{6,\underline{7}\}$	$\{\underline{7},\underline{8}\}$	$\{8,\underline{9}\}$	$\{\underline{9},\underline{0}\}$	$\{0,\underline{1}\}$	$\{\underline{11},\underline{10}\}$

Fig. 11.6. An $FBTD(6)$ from [87] (with a factor in each row that contains the underlined cells in that row).

■