Chapter II

CHAPTER II

GENERATION OF QUASIGROUPS

There are different schemes for generating quasigroups of large order which will be useful for Cryptographical applications. In this chapter eight different schemes for generating quasigroups are illustrated with examples.

SECTION - 2.1

GENERATION USING ISOTOPIES

Definition: 2.1.1

Let $(Q_1, \cdot)$ and $(Q_2, *)$ be two quasigroups. Q_1 and Q_2 are **isotopic** if there are bijections $f, g, h : Q_1 \to Q_2$ so that $f(x \cdot y) = g(x) * h(y)$ for all $x, y \in Q_1$. The ordered triple (f, g, h) is called an **isotopy.**

An isotopy can be used to create a quasigroup $(Q, *)$ from another quasigroup $(Q, \cdot)$ by defining,

$$x * y = f^{-1}(g(x) \cdot h(y)) \qquad \text{for } x, y \in Q.$$

Example: 2.1.2

Let $(Q, \cdot) = (Z_4, +)$ where $Z_4 = \{0, 1, 2, 3\}$ and addition is computed modulo 4, so that the Cayley table for $(Q, \cdot)$ is given in Table 2.1.1. Let the isotopy (f, g, h) be as shown in Table 2.1.2.

.	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 2.1.1
The Cayley table for $(Q, \cdot)$

x	f(x)	g(x)	h(x)
0	1	2	3
1	0	3	1
2	3	1	0
3	2	0	2

Table 2.1.2

The isotopy (f, g, h)

Then the quasigroup $(Q, *)$ is created by $x * y = f^{-1}(g(x) \cdot h(y))$. The quasigroup $(Q, *)$ is produced and its Cayley table is given in Table 2.1.3.

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

Table 2.1.3

The Cayley table for $(Q, *)$

We find that although $(Q, \cdot)$ is a group, $(Q, *)$ is neither associative nor commutative and has no identity element.

Note: 2.1.3

Normally when we are working with isotopies, we will choose f to be the identity map, so that a quasigroup operation is defined by $x * y = g(x) \cdot h(y)$.

SECTION -2.2

GENERATION USING AFFINE ISOTOPIES

Definition: 2.2.1

Let $(Q,+)$ be a group and for $f:Q\to Q$. f is an **affine map** if $f(x+y) = f(x)+f(y)-f(0)$, where $0\in Q$ denotes the identity element under $+$.

Note: 2.2.2

An affine map requires both an identity element and inverse elements, so we must start with a group in order to have the concept of an affine map well-defined.

Example: 2.2.3

Let $Q = Z_8 = \{0,1,2,3,4,5,6,7\}$ and let the group operation be addition modulo 8. Then we can create a quasigroup $(Q,\cdot)$ from $(Z_8,+)$ by isotopy, with $f(x) = 3x+4$ and $g(x) = 5x+1$.

The maps f and g are affine maps, because

$$\begin{aligned} f(x+y) &= 3(x+y)+4 \\ &= 3x+3y+4 \\ &= (3x+4)+(3x+4)-4 \\ &= f(x)+f(y)-f(0) \end{aligned}$$

and

$$\begin{aligned} g(x+y) &= 5(x+y)+1 \\ &= 5x+5y+1 \\ &= (5x+1)+(3y+1)-1 \\ &= g(x)+g(y)-g(0) \end{aligned}$$

Since we are creating $(Q,\cdot)$ by isotopy, we will define $x \cdot y = f(x) + g(y)$ for $x, y \in Z_8$. Then $(Q,\cdot)$ is shown in Table 2.2.1, where $Q = Z_8$.

.	0	1	2	3	4	5	6	7
0	5	2	7	4	1	6	3	0
1	0	5	2	7	4	1	6	3
2	3	0	5	2	7	4	1	6
3	6	3	0	5	2	7	4	1
4	1	6	3	0	5	2	7	4
5	4	1	6	3	0	5	2	7
6	7	4	1	6	3	0	5	2
7	2	7	4	1	6	3	0	5

Table 2.2.1

The Cayley table for $(Q,\cdot)$

We find that $(Q,\cdot)$ is not associative, because $(0\cdot 4)\cdot 5 = 1\cdot 5 = 1$ but $0\cdot(4\cdot 5) = 0\cdot 2 = 7$. It is not commutative, because $0\cdot 1 = 2$ and $1\cdot 0 = 0$. There is no identity element and hence no inverses.

However, $(Q,\cdot)$ is still quite structured – the elements in each row always appear in the same order, and the elements in each column are also arranged in the same order.

SECTION - 2.3

GENERATION USING NON AFFINE ISOTOPIES

Definition: 2.3.1

Let $(Q, +)$ be a group and let $f : Q \to Q$. f is an **non-affine map** if, $f(x+y) \neq f(x)+f(y)-f(0)$, where $0 \in Q$ denotes the identity element under $+$.

Example: 2.3.2

Let $Q = Z_8 = \{0,1,2,3,4,5,6,7\}$ and let the group operation on Q be addition modulo 8. Let $f, g : Q \to Q$ be as in Table 2.3.1.

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
f(x)	1	4	6	3	2	7	0	5
g(x)	4	2	1	0	6	5	7	3

Table 2.3.1

Non- affine isotopies f and g

Both f and g are non-affine maps, because

$$f(2+3) = f(5) = 7 \text{ but } f(2) + f(3) - f(0) = 6 + 3 - 1 = 8$$

and

$$g(4+3) = g(7) = 3 \text{ but } g(4) + g(3) - g(0) = 6 + 0 - 4 = 2$$

If a quasigroup $(Q, \cdot)$ is created by isotopy from f and g by defining $x \cdot y = f(x) + g(y)$, then $(Q, \cdot)$ is shown in Table 2.3.2.

.	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	5	3	2	1	7	6	0	4
1	0	6	5	4	2	1	3	7
2	2	0	7	6	4	3	5	1
3	7	5	4	3	1	0	2	6
4	6	4	3	2	0	7	1	5
5	3	1	0	7	5	4	6	2
6	4	2	1	0	6	5	7	2
7	1	7	6	5	3	2	4	0

Table 2.3.2

The Cayley table for $(Q, \cdot)$

SECTION - 2.4

GENERATION USING LINEAR MAPPING

Using this scheme, we generate two linear functions f and g and then elements associated with each function is stored in one dimensional array of size equal to size of the permutation. Now, in order to generate the $(i, j)^{th}$ element of the huge Latin square, the i^{th} element of the first function is added to the j^{th} element of the second function and modulus operation with respect to the size of the Latin square to be generated is applied to the addition of i^{th} element of 1^{st} function and j^{th} element of 2^{nd} function. In this way we get a huge Latin square with elements in the range 0 to the size of Latin square.

Definition: 2.4.1

Let $(Q, +)$ be a group and let $f : Q \to Q$. f is a **linear map** if

$$f(x + y) = f(x) + f(y)$$

for all $x, y \in Q$.

Let $Q = Z_n = \{0, 1, \ldots, n-1\}$ and let the group operation be addition modulo n. Then we can create a Quasigroup $(Q, \cdot)$ from $(Z_n, +)$ by defining

$$f(x) = px + a,$$

$$g(x) = qx + b,$$

where p and q are relatively prime with respect to the order of the quasigroup and a, b are positive integers less than the size of quasigroup, and then further defining,

$$h(x, y) = (f(x) + g(y)) \% n.$$

Example: 2.4.2

Let $Q = Z_8 = \{0,1,2,3,4,5,6,7\}$ and let the group operation be addition modulo 8. Then we can create a quasigroup $(Q,\cdot)$ from $(Z_8,+)$ by defining $f(x) = 5x + 6$ and $g(x) = 3x + 7$, where a = 6 & b = 7 and p = 5 & q = 3. Since we are creating $(Q,\cdot)$ by linear mapping, we will define

$$h(x,y) = (f(x) + g(y))\%8.$$

Then $(Q,\cdot)$ is as shown in Table 2.4.1.

.	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	5	0	3	6	1	4	7	2
1	2	5	0	3	6	1	4	7
2	7	2	5	0	3	6	1	4
3	4	7	2	5	0	3	6	1
4	1	4	7	2	5	0	3	6
5	6	1	4	7	2	5	0	3
6	3	6	1	4	7	2	5	0
7	0	3	6	1	4	7	2	5

Table 2.4.1

Quasigroup using linear mapping.

We find that $(Q,\cdot)$ is not associative, because $h(h(0,2),4) = h(3,4) = 0$ but $h(0,h(2,4)) = h(0,3) = 6$.

It is not commutative, because $h(0,1) = 0$ but $h(1,0) = 2$. There is no identity element and hence no inverses.

Limitations of the above method:

The problem with this scheme is that $(Q,\cdot)$ is still quite structured. The elements in each row always appear in the same order. Similarly, the

elements in each column are also arranged in the same order. In addition, each row is a copy of the previous row, shifted one space to the right. Each column is a copy of the previous column, shifted one space down. As we see in Example **2.4.2**: 1^{st} and 2^{nd} row are (5 2 7 4 1 6 3 0) and (0 5 2 7 4 1 6 3) respectively. Hence by determining any of the rows, one can guess the entire Latin square.

SECTION – 2.5

GENERATION USING KEYED PERMUTATION

In the previous scheme, one row could be easily derived from the other row. We remove this problem by using nonlinear mapping. In this scheme two random permutations f and g are generated and then each permutation is stored in one dimensional array of size equal to size of permutation. Now, in order to generate the $(i, j)^{th}$ element of the huge Latin square, the i^{th} element of the first permutation is added to the j^{th} element of the second permutation and modulus operation with respect to the size of the Latin square to be generated is applied to the addition of i^{th} element of 1^{st} permutation and j^{th} element 2^{nd} permutation. In this way we get a huge Latin square with elements in the range 0 to the size of Latin square.

Let $Q = Z_n = \{0, 1, \ldots, n-1\}$ and let the group operation be addition modulo n. Then we can create a quasigroup $(Q, \cdot)$ from $(Z_n, +)$ by supposing

$f(x)$ = any random permutation $\{6, 2, 8\ldots\}$

$g(x)$ = any random permutation $\{5, 3, 9\ldots\}$

then defining $h(x, y) = (f(x) + g(y))\,\%\,n$.

Example: 2.5.1

Let $Q = Z_8 = \{0,1,2,3,4,5,6,7\}$ and let the group operation be addition modulo 8. Then we can create a quasigroup $(Q,\cdot)$ from $(Z_8,+)$ by generate two permutation f and g and then apply $h(x,y) = (f(x)+g(y))\ \%\ 8$ for x and y ranging from 0 to 7.

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
f(x)	2	5	0	4	6	7	1	3
g(x)	7	4	3	2	1	0	6	5

Table 2.5.1

Then the quasigroup $(Q,\cdot)$ is created from f and g by using the equation $h(x,y) = (f(x)+g(y))\ \%\ 8$ is as shown in Table 2.5.2

.	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	1	6	5	4	3	2	0	7
1	4	1	0	7	6	5	3	2
2	7	4	3	2	1	0	6	5
3	3	0	7	6	5	4	2	1
4	5	2	1	0	7	6	4	3
5	6	3	2	1	0	7	5	4
6	0	5	4	3	2	1	7	6
7	2	7	6	5	4	3	1	0

Table 2.5.2

Generation using keyed permutation

We find that $(Q,\cdot)$ is not associative, because $h(h(0,2),4) = h(5,4) = 0$ but $h(0,h(2,4)) = h(0,1) = 6$.

It is not commutative, because $h(0,1) = 6$ but $h(1,0) = 4$. There is no identity element and hence no inverses.

SECTION - 2.6

GENERATION USING COMPLETE MAPPING

Definition: 2.6.1

Let $(G,+)$ be a group and let $i: G \to G$ denote the identity map on G. $\theta: G \to G$ is a **Complete Mapping** if

1. θ is a bijection.
2. $i-\theta$ is a bijection, where $(i-\theta)(x) = x - \theta(x)$.

Example: 2.6.2

Let $(G,+) = (Z_9,+)$, where $Z_9 = \{0,1,2,3,4,5,6,7,8\}$ and addition is performed modulo 9. Then $\theta(x) = 5x+3$ is a complete mapping as seen in Table 2.6.1, because both θ and $i-\theta$ are bijections.

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
$\theta(x)$	3	8	4	0	5	1	8	2	7
$(i-\theta)(x)$	6	2	7	3	8	4	0	5	1

Table 2.6.1

A Complete Mapping on Z_9

Before using complete maps to generate quasigroups, it would be helpful to know whether or not a group G has a complete map.

Definition: 2.6.3

Let G be a group. G is **admissible** if there is a complete map $\theta: G \to G$.

Preposition: 2.6.4 [48]

If G has exactly one element of order 2, then G is not admissible, but there is some $\theta : G \to G$ so that the number of distinct elements is n - 1. If G does not have exactly one element of order 2, then G is admissible.

Creating Quasigroups Using Complete Map: [54]

A quasigroup $(Q, \cdot)$ is created from an admissible group $(Q, +)$ and a complete mapping θ by defining $x \cdot y = \theta(x - y) + y$ for $x, y \in Q$.

Example: 2.6.5

Let $Q = Z_5 = \{0, 1, 2, 3, 4\}$ be the additive group of five elements, where x + y is computed modulo 5 for $x, y \in Q$. By Preposition 2.6.4, Q is admissible because it is a finite abelian group which does not have exactly one element of order 2. Let $\theta : Q \to Q$ be given by θ (x) = 2x.

To Prove: θ is a Complete mapping

Given $\theta(x) = 2x$

$$\begin{aligned}(i - \theta)(x) &= x - \theta(x) \\ &= x - 2 \\ &= -x \\ &= 4x\end{aligned}$$

x	**0**	**1**	**2**	**3**	**4**
θ(x)	0	2	4	6	8
$(i - \theta)$(x)	0	4	8	12	16

Table 2.6.2

So θ is a complete mapping, as shown in Table 2.6.2, because both θ and $i - \theta$ are bijections. If a quasigroup $(Q, \cdot)$ is created by

$$x \cdot y = \theta(x - y) + y,$$

then the Cayley table for $(Q, \cdot)$ is shown in Table 2.6.3.

.	0	1	2	3	4
0	0	4	3	2	1
1	2	1	0	4	3
2	4	3	2	1	0
3	1	0	4	3	2
4	3	2	1	0	4

Table 2.6.3

The Cayley table for $(Q,\cdot)$.

We find that $(Q,\cdot)$ is not associative, because $(0\cdot 1)\cdot 4 = 4\cdot 4 = 4$ but $0\cdot(1\cdot 4) = 0\cdot 3 = 2$.

It is not commutative, because $0\cdot 3 = 2$ but $3\cdot 0 = 1$. There is no identity element and hence no inverses.

SECTION - 2.7

GENERATION USING AFFINE COMPLETE MAPPING

As with isotopies, we could choose our complete mapping to have special properties. If we choose θ to be an affine complete map and create $(Q,\cdot)$ by $x\cdot y = \theta(x-y)+y$, then $(Q,\cdot)$ is again isotopic to $(Q,+)$.

That is, creating a quasigroup by using an affine complete map is simply a special case of creating a quasigroup by isotopy.

In this case, the isotopy is given by

$f(x) = \theta(x)$ and $g(x) = \theta(-x)+\theta(0)+x$, because

$$\begin{aligned} x\cdot y &= \theta(x-y)+y \\ &= \theta(x+(-y))+y \\ &= \theta(x)+\theta(-y)-\theta(0)+y \qquad \text{(because } \theta \text{ is affine)} \\ &= f(x)+g(y) \end{aligned}$$

Because both θ and $i-\theta$ are bijections, f and g are bijections, so this is indeed an isotopy.

Example: 2.7.1

Let $Q = Z_2^4$ and define $\theta : Q \to Q$ by,

$$\theta(\langle x_3, x_2, x_1, x_0 \rangle) = \langle x_3 \oplus x_2, x_1, x_0, x_3 \rangle.$$

That is, θ is defined by rotating the bits of $x \in Q$ one bit to the left and exclusive or-ing the "new" first component of x with the "old" first component of x. In order to prove that $(Q, \cdot)$ is a quasigroup, we need to show that θ is a complete map. We also need to show that is θ an affine map.

Claim:

θ is an affine map.

Proof:

In order to show that θ is affine, we need to show that

$$\theta(x \oplus y) = \theta(x) \oplus \theta(y) \oplus \theta(0) \qquad \text{for all } x, y \in Q$$

Consider,

$$\begin{aligned}
\theta(\langle x_3, x_2, x_1, x_0 \rangle \oplus \langle y_3, y_2, y_1, y_0 \rangle) &= \theta(\langle x_3 \oplus y_3, x_2 \oplus y_2, x_1 \oplus y_1, x_0 \oplus y_0 \rangle) \\
&= \langle x_3 \oplus y_3 \oplus x_2 \oplus y_2, x_1 \oplus y_1, x_0 \oplus y_0, x_3 \oplus y_3 \rangle \\
&= \langle x_3 \oplus x_2, x_1, x_0, x_3 \rangle \oplus \langle y_3 \oplus y_2, y_1, y_0, y_3 \rangle \\
&= \theta(x) \oplus \theta(y) \oplus \theta(0) \qquad (\because \theta(0) = 0)
\end{aligned}$$

Therefore, θ is an affine map.

To see that θ is a complete map, notice that Table 2.7.1 demonstrates that both θ and $i \oplus \theta$ are bijections. This can also be seen in Table 2.7.2, which shows how θ and $i \oplus \theta$ act on the integer representations of the elements of $(Q, \cdot)$.

x	θ(x)	x ⊕ θ(x)
<0,0,0,0>	<0,0,0,0>	<0,0,0,0>
<0,0,0,1>	<0,0,1,0>	<0,0,1,1>
<0,0,1,0>	<0,1,0,0>	<0,1,1,0>
<0,0,1,1>	<0,1,1,0>	<0,1,0,1>
<0,1,0,0>	<1,0,0,0>	<1,1,0,0>
<0,1,0,1>	<1,0,1,0>	<1,1,1,1>
<0,1,1,0>	<1,1,0,0>	<1,0,1,0>
<0,1,1,1>	<1,1,1,0>	<1,0,0,1>
<1,0,0,0>	<1,0,0,1>	<0,0,0,1>
<1,0,0,1>	<1,0,1,1>	<0,0,1,0>
<1,0,1,0>	<1,1,0,1>	<0,1,1,1>
<1,0,1,1>	<1,1,1,1>	<0,1,0,0>
<1,1,0,0>	<0,0,0,1>	<1,1,0,1>
<1,1,0,1>	<0,0,1,1>	<1,1,1,0>
<1,1,1,0>	<0,1,0,1>	<1,1,0,1>
<1,1,1,1>	<0,1,1,1>	<1,0,0,0>

Table 2.7.1

θ and i ⊕ θ on Z_2^4.

X	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
θ(x)	0	2	4	6	8	10	12	14	9	11	13	15	1	3	5	7
x ⊕ θ(x)	0	8	6	5	12	15	10	9	1	2	7	4	13	14	11	8

Table 2.7.2

θ and i ⊕ θ on integers corresponding to elements of Z_2^4.

The quasigroup $(Q,\cdot)$ created from θ by $x \cdot y = \theta(x \oplus y) \oplus y$ is shown in Table 2.7.3.

.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	3	6	5	12	15	10	9	1	2	7	4	13	14	11	8
1	2	1	4	7	14	13	8	11	3	0	5	6	15	12	9	10
2	4	7	2	1	8	11	4	13	5	6	3	0	9	10	15	12
3	6	5	0	3	10	9	12	15	7	4	1	2	11	8	13	14
4	8	11	14	13	4	7	2	1	9	10	15	12	5	6	3	0
5	10	9	12	15	6	5	0	3	11	8	13	14	7	4	1	2
6	12	15	10	9	0	3	6	5	13	14	11	8	1	2	7	4
7	14	13	8	11	2	1	4	7	15	12	9	10	3	0	5	6
8	9	10	15	12	5	6	3	0	8	11	14	13	4	7	2	1
9	11	8	13	14	7	4	1	2	10	9	12	15	6	5	0	3
10	13	14	11	8	1	2	7	4	12	15	10	9	0	3	6	5
11	15	12	9	10	3	0	5	6	14	13	8	11	2	1	4	7
12	1	2	7	4	13	14	11	8	0	3	6	5	12	15	10	9
13	3	0	5	6	15	12	9	10	2	1	4	7	14	13	8	11
14	5	6	3	0	9	10	15	12	4	7	2	1	8	11	14	13
15	7	4	1	2	11	8	13	14	6	5	0	3	10	9	12	15

Table 2.7.3

The quasigroup $(Q,\cdot)$ created using the map θ.

SECTION – 2.8

GENERATION USING NON AFFINE COMPLETE MAPPING

It is also possible to create a quasigroup using complete mapping that are not affine map.

Example: 2.8.1

Let $\theta : Z_2^4 \to Z_2^4$ be as shown in Table 2.8.1. Then the action of θ on the binary representations of the group elements is shown in Table 2.8.2. The quasigroup $(Q,\cdot)$ created from θ is shown in Table 2.8.3.

x	θ(x)	x ⊕ θ(x)
<0,0,0,0>	<1,1,1,0>	<1,1,1,0>
<0,0,0,1>	<1,0,1,0>	<1,0,1,1>
<0,0,1,0>	<1,0,0,0>	<1,0,1,0>
<0,0,1,1>	<1,1,1,0>	<1,1,1,1>
<0,1,0,0>	<0,1,0,0>	<0,0,0,0>
<0,1,0,1>	<0,0,0,0>	<0,1,0,1>
<0,1,1,0>	<0,0,0,1>	<0,1,1,1>
<0,1,1,1>	<0,1,0,1>	<0,0,1,0>
<1,0,0,0>	<1,0,1,1>	<0,0,1,1>
<1,0,0,1>	<1,1,1,1>	<0,1,1,0>
<1,0,1,0>	<0,0,1,1>	<1,0,0,1>
<1,0,1,1>	<0,1,1,1>	<1,1,1,0>
<1,1,0,0>	<1,1,0,1>	<0,0,0,1>
<1,1,0,1>	<1,0,0,1>	<0,1,0,0>
<1,1,1,0>	<0,1,1,0>	<1,0,0,0>
<1,1,1,1>	<0,1,1,0>	<1,1,0,1>

Table 2.8.1

A non-affine complete map θ and i ⊕ θ on Z_2^4

First, notice that θ is not affine, because

$$\theta(2 \oplus 4) = \theta(6) = 1 \quad \text{but}$$

$$\theta(2) \oplus \theta(4) \oplus \theta(0) = 8 \oplus 4 \oplus 14 = 2.$$

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
θ(x)	14	10	8	12	4	0	1	5	11	15	3	7	13	9	6	2
x ⊕ θ(x)	14	11	10	15	0	5	7	2	3	6	9	12	1	4	8	13

Table 2.8.2

θ and i ⊕ θ on integers corresponding to elements of Z_2^4.

.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	11	10	15	0	5	7	2	3	6	9	12	1	4	8	13
1	10	15	14	11	4	1	3	6	7	2	13	8	5	0	12	9
2	8	13	12	9	5	0	2	7	11	14	1	4	10	15	3	6
3	12	9	8	13	1	4	6	3	15	10	5	0	14	11	7	2
4	4	1	3	6	10	15	14	11	5	0	12	9	7	2	13	8
5	0	5	7	2	14	11	10	15	1	4	8	13	3	6	9	12
6	1	4	6	3	12	9	8	13	14	11	7	2	15	10	5	0
7	5	0	2	7	8	13	12	9	10	15	3	6	11	14	1	4
8	11	14	1	4	9	12	0	5	6	3	2	7	8	13	15	10
9	15	10	5	0	13	8	4	1	2	7	6	3	12	9	11	14
10	3	6	9	12	2	7	11	14	0	5	4	1	13	8	10	15
11	7	2	13	8	6	3	15	10	4	1	0	5	9	12	14	11
12	13	8	4	1	15	10	5	0	12	9	11	14	2	7	6	3
13	9	12	0	5	11	14	1	4	8	13	15	10	6	3	2	7
14	6	3	15	10	7	2	13	8	9	12	14	11	4	1	0	5
15	2	7	11	14	3	6	9	12	13	8	10	15	0	5	4	1

Table 2.8.3

The quasigroup $(Q,\cdot)$ created using the non-affine complete map θ.