CHAPTER 2 REPRESENTATIONS OF BASIC BOOLEAN TRANSFORMATIONS

ABSTRACT. Orthogonal transformations of $\{-1,1\}^n$ are restrictions to $\{-1,1\}^n$ of orthogonal transformations of the real n-dimensional space $\mathbf{R}^n$ that map $\{-1,1\}^n$ onto itself. Corresponding equivalent transformations of $\{0,1\}^n$, that is, Boolean transformations, are called Boolean isometries. A minimal Boolean transformation is a one which has the minimum number of coordinates changed under it among isometrically equivalent transformations. A self-dual Boolean transformation is a one that commutes with the complementation of all coordinates. The possible graphs of one-to-one self-dual transformations are completely determined. Any self-dual Boolean transformation can be expressed by Boolean functions which are concerned with only those points whose coordinates are changed by the transformation. A circular transformation is a one which commutes with rotations of coordinates, and if it is self-dual, then only one Boolean function can represent it. A skew-circular transformation is similarly defined and represented.

2.1 BOOLEAN ISOMETRIES

Boolean transformations of $\mathbf{Q}^n$ are simplest transformations and play a fundamental role in computer systems. They are ubiquitous in computer science and discrete mathematics. However, a general theory that supports various results in different branches has not been established. In this chapter, we describe representations of Boolean transformations belonging to some basic classes. These representations are used in the following chapters as basic devices for the present study of threshold transformations and neural networks.

A simple Boolean transformation is a permutation of coordinates. If τ is a permutation of $\mathbf{N}$, i.e. an element of SYM($\mathbf{N}$), then τ defines the permutation $H\tau$ of the coordinates of $\mathbf{Q}^n$ by the Pólya action H, as described in Chapter 1.3, by

$$(H\tau)(x_1, x_2, .., x_n) = (x_{\tau^{-1}1}, x_{\tau^{-1}2}, .., x_{\tau^{-1}n})$$

We omit the Pólya action H hereafter and write τx in place of $(H\tau)x$ for an element x of $\mathbf{Q}^n$. Another simple transformation of $\mathbf{Q}^n$ is a complementation of coordinates. Let J^- for $J = \{s, t, .., w\} \subseteq \mathbf{N}$ denote the complementation of the sth, tth,..,wth coordinates defined by

$$J^-x = (x_1, .., \neg x_s, .., \neg x_t, .., \neg x_w, .., x_n).$$

If J is a one element-set $\{s\}$, then J^- is denoted by s^-. Also $\mathbf{N}^-$ is denoted by $\bar{\neg}$.

For the composition of a permutation of coordinates τ and a complementation J^-, we have

$$\begin{aligned} J^-\tau(x_1, x_2, .., x_n) &= J^-(x_{\tau^{-1}1}, x_{\tau^{-1}2}, .., x_{\tau^{-1}n}) \\ &= (x_{\tau^{-1}1}, .., \neg x_{\tau^{-1}s}, .., \neg x_{\tau^{-1}t}, .., \neg x_{\tau^{-1}w}, .., x_{\tau^{-1}n}) \\ &= \tau(\{\tau^{-1}s, \tau^{-1}t, .., \tau^{-1}w\}^-(x_1, x_2, .., x_n)). \end{aligned}$$

Therefore,

$$J^-\tau = \tau(\tau^{-1}J)^-, \text{ i.e. } \tau K^- = (\tau K)^-\tau \ , \tag{2.1.1}$$

The inverse of τJ^- is, therefore,

$$\begin{aligned} (\tau J^-)^{-1} &= (J^-)^{-1}\tau^{-1} = J^-\tau^{-1} \\ &= \tau^{-1}(\tau J)^-. \end{aligned} \tag{2.1.2}$$

For the composition of σJ^- and τK^-, we have

$$\begin{aligned} \sigma J^- \circ \tau K^- &= \sigma\tau(\tau^{-1}J)^- K^- \\ &= \sigma\tau(\tau^{-1}J\dot{+}K)^-. \end{aligned} \tag{2.1.3}$$

We have also obtained:

Proposition 2.1.1 The set $O(\mathbf{Q}^n)$ of all products of a finite number of permutations and complementations of coordinates of $\mathbf{Q}^n$ consists of $n!2^n$ elements, each uniquely expressed as a product τJ^-, where τ is a permutation of $\mathbf{N}$, and J^- is a complementation. Further, $O(\mathbf{Q}^n)$ is a transformation group for $\mathbf{Q}^n$.

The identity transformation of $\mathbf{Q}^n$ will be denoted by I. Clearly $(\bar{\neg})^{-1} = \bar{\neg}$. If $x = (x_1, x_2, .., x_n) \in \mathbf{Q}^n$, then $\bar{\neg}x$ is called the complement of x. Then we have

$$\bar{\neg}T = T\bar{\neg} \text{ for every } T \text{ of } O(\mathbf{Q}^n).$$

Let $\mathbf{B}$ the set of all Boolean functions from $\mathbf{Q}^n$ to $\mathbf{Q}$. The group $O(\mathbf{Q}^n)$ further defines the Pólya action on $\mathbf{B}$ by

$$(Tf)x = f(T^{-1}x),$$

for each $T \in O(\mathbf{Q}^n)$ and $f \in \mathbf{B}$. It is clear from the definition that $x \in f$ if and only if $Tx \in Tf$. In other words, $(Tf)^{-1}1 = T(f^{-1}1)$, so that the application of T to a function f is equivalent to the application of T to the set f through the Pólya action on $\mathbf{Q}^n$. For example, the set $\bar{\neg}f$ is the set of complements of all points of $f^{-1}1$, while the set $\neg f = f^{-1}0$.

Sometimes it is more convenient to use the set $\{-1,1\}^n$ in place of $\mathbf{Q}^n = \{0,1\}^n$ and to consider a corresponding transformation of $\{-1,1\}^n$ for a transformation of $\mathbf{Q}^n$. This is made possible by the bijection between $\{-1,1\}^n$ and $\mathbf{Q}^n$ obtained by the function Sgn from the *real n-dimensional space* $\mathbf{R}^n$ onto $\{-1,1\}^n$ defined by

$$(\mathrm{Sgn}(y))_i = \begin{cases} 1 & \text{if } y_i > 0, \\ -1 & \text{if } y_i \le 0, \end{cases}$$

or the function *Bool* from $\mathbf{R}^n$ onto $\mathbf{Q}^n$ defined by

$$(\mathrm{Bool}(x))_i = \begin{cases} 1 & \text{if } x_i > 0, \\ 0 & \text{if } x_i \le 0, \end{cases}$$

The *Hamming distance* d_H is defined on both $\mathbf{Q}^n$ and $\{-1,1\}^n$ as

$$d_H(x,y) = |\{i \mid x_i \ne y_i\}|.$$

When both $\mathbf{Q}^n$ and $\{-1,1\}^n$ are imbedded in $\mathbf{R}^n$, they represent geometric *n-dimensional cubes* or *n-cubes* with each element being their vertex and each pair (x,y) of elements such that $d_H(x,y) = 1$ being their edge.

If Sgn is restricted to $\mathbf{Q}^n$ and Bool is restricted to $\{-1,1\}^n$, then

$$\mathrm{Bool} = \mathrm{Sgn}^{-1}.$$

A transformation F of $\mathbf{Q}^n$ and a transformation G of $\{-1,1\}^n$ is *equivalent* if

$$G = \mathrm{Sgn} \circ F \circ \mathrm{Sgn}^{-1},$$

that is, the following diagram is *commutative.*

$$\begin{tikzcd}
\mathbf{Q}^n \arrow[r, "F"] \arrow[d, "\mathrm{Sgn}"'] & \mathbf{Q}^n \arrow[d, "\mathrm{Sgn}"] \\
\{-1,1\}^n \arrow[r, "G"'] & \{-1,1\}^n.
\end{tikzcd}$$

The transformation of $\{-1,1\}^n$ corresponding to the transformation $J^- = \{s,t,..,w\}^-$ of $\mathbf{Q}^n$ is the inversion of corresponding coordinates. We will use the same symbols for these operations in $\{-1,1\}^n$. Threfore,

$$\begin{aligned} J^- y &= \{s,t,..,w\}^-(y_1, y_2, .., y_n) \\ &= (y_1, .., -y_s, .., -y_t, .., -y_w, .., y_n). \end{aligned}$$

However, $\mathbf{N}^-$ is the scalar multiplication by -1 in $\mathbf{R}^n$, so that it is denoted by $-$ when no confusion occurs. Applying a permutation τ to a point $y \in \{-1,1\}^n$ by the Pólya action is made by multiplying y by a particular $n \times n$ orthogonal matrix P over $\mathbf{R}$ such that each row has only one non-zero element, which is 1, and each column has only one non-zero element, which is 1. Also applying an inversion J^- to y is made by multiplying y by a diagonal matrix D such that $D_{ii} = -1$ if $i \in J$, and $D_{ii} = 1$ if $i \notin J$. Therefore, PD is a matrix representing an orthogonal transformation of $\mathbf{R}^n$ with respect to the basis $\{10 \cdot \cdot 0, 010 \cdot \cdot 0, ..., 0 \cdot \cdot 01\}$ that maps $\{-1,1\}^n$ onto itself. Conversely, let T be an orthogonal transformation of $\mathbf{R}^n$ that maps $\{-1,1\}^n$ onto itself. If a point $c \in \mathbf{R}^n$ is the center of a face of the n-cube $\{-1,1\}^n$, then $c_i = 1$ or -1 for some i and $c_i = 0$ for every other i, and c must be sent into the center of a face by T. Also since the set of n centers $\{10 \cdot \cdot 0, 010 \cdot \cdot 0, .., 0 \cdot \cdot 01\}$ constitutes an orthogonal basis of $\mathbf{R}^n$, the matrix representing T with respect to this basis is PD for some P and D described above. Thus we have obtained:

Proposition 2.1.2 The set $O(\{-1,1\}^n)$ of transformations of $\{-1,1\}^n$ that are equivalent to elements of $O(\mathbf{Q}^n)$ is the set of all orthogonal transformations of $\mathbf{R}^n$ that map $\{-1,1\}^n$ onto itself, each transformation being expressed by a multiplication by an orthogonal matrix such that each row has only one non-zero element, which is 1 or -1, and each column has only one non-zero element, which is 1 or -1.

By the above proposition, an element of $O(\mathbf{Q}^n)$ is called a (*Boolean*) *isometry* of $\mathbf{Q}^n$ hereafter; an element of $O(\{-1,1\}^n)$ is called an *orthogonal transformation.* Note that $O(\{-1,1\}^n)$ is the same as $O(\mathbf{Q}^n)$ as a group and well known as a finite reflection subgroup of $O(\mathbf{R}^n)$, the group of orthogonal transformations of $\mathbf{R}^n$ (see e.g. Grove & Benson, 1985). Further, the following Proposition 2.1.4 shows $O(\{-1,1\}^n)$ is the set of all one-to-one linear transformations that map $\{-1,1\}^n$ onto itself.

Lemma 2.1.3 $v \in \{-1,1\}^n$ and $v = (v^{(1)} + ... + v^{(n)})/(n-2)$ for linearly independent vectors $v^{(i)} \in \{-1,1\}^n$, then $d_H(v, v^{(i)}) = 1$ for every $i = 1, ..., n$.

Proof. Let $v \in \{-1,1\}^n$ and $v = (v^{(1)} + ... + v^{(n)})/(n-2)$ for linearly independent vectors $v^{(i)} \in \{-1,1\}^n$. Let $v = 11 \cdots 1$ without loss of generality. Then $(v_1^{(i)} + ... + v_n^{(i)}) \cdot (n-2) = 1$ for every $i = 1,..,n$. Let the number of -1s in $\{v_j^{(1)},...,v_j^{(n)}\}$ be k. Then $(n-k)-k = n-2$, so that $k = 1$ for every j. Suppose the number of -1s in $v^{(i)}$ is more than 1 for some i. Then there exists some l such that $v^{(l)} = 11 \cdots 1 = v$. Let $l = 1$ without loss of generality. Then $(1 - 1/(n-2))v^{(1)} = (v^{(2)} + ... + v^{(n)})/(n-2)$ contrary to the linear independence of $v^{(1)},...,v^{(n)}$. Therefore, $d_H(v, v^{(i)}) = 1$ for every $i = 1,...,n$. □

Proposition 2.1.4 If T is a one-to-one linear transformation of $\mathbf{R}^n$ that maps $\{-1,1\}^n$ onto itself, then T is an orthogonal transformation.

Proof. This proposition is clear for $n \leq 2$. Let T be a one-to-one linear transformation of $\mathbf{R}^n$ that maps $\{-1,1\}^n$ onto itself for $n \geq 3$. Let $v = 1 \cdots 1, v^{(1)} = -11 \cdot \cdot 1, v^{(2)} = 1-11 \cdot \cdot 1, ..., v^{(n)} = 1 \cdot \cdot 1-1$. Since $v = (v^{(1)} + ... + v^{(n)})/(n-2)$, and T is linear, $Tv = (Tv^{(1)} + ... + Tv^{(n)})/(n-2)$. Tv and $Tv^{(i)}$ are elements of $\{-1,1\}^n$ for every i. Since T is one-to-one, and $v^{(i)}$ are linearly independent, $Tv^{(i)}$ are also linearly independent. Therefore, by Lemma 2.1.3, $d_H(Tv, Tv^{(i)}) = 1$ for every $i = 1,...,n$ and $Tv^{(i)} \neq Tv^{(j)}$ for every $i \neq j$. Therefore, $(Tv^{(i)}, Tv^{(i)}) = n = (v^{(i)}, v^{(i)})$ for every i and $(Tv^{(i)}, Tv^{(j)}) = n-4 = (v^{(i)}, v^{(j)})$ for every $i \neq j$. On the other hand, $\{v^{(1)},...,v^{(n)}\}$ is a basis of $\mathbf{R}^n$. Therefore, T is an orthogonal transformation. □

Proposition 2.1.5 Any isometry $T \in O(\mathbf{Q}^n)$ can be decomposed as a disjoint composition

$$T = \sigma_1 J_1^- \odot ... \odot \sigma_k J_k^- \odot \iota J_{k+1}^-,$$

where σ_i is a cyclic permutation, $J_i \subseteq \mathrm{Car}\sigma_i$ for each $i = 1,...,k$, and $J_{k+1} \subseteq \mathbf{N} \backslash \bigcup_i \mathrm{Car}\sigma_i$, and ι is the identity on $\mathbf{N} \backslash \bigcap_i \mathrm{Car}\sigma_i$.

Proof. Let T be an isometry of $\mathbf{Q}^n$. Then T is expressed as $T = \tau J^-$ by Proposition 2.1.1, where $\tau \in \mathrm{SYM}(\mathbf{N})$ and $J \subseteq \mathbf{N}$. If τ is not the identity permutation, then, by Proposition 1.2.2 of Chapter 1, $\tau = \sigma_1 \odot ... \odot \sigma_k$, where σ_i is a cyclic permutation of length at least 2, and $\mathrm{Car}\sigma_i$ and $\mathrm{Car}\sigma_j$ are disjoint if $i \neq j$. Let $J_i = J \cap \mathrm{Car}\sigma_i$ for each $i = 1,..,k$, and $J_{k+1} = J \cap (\mathbf{N} \backslash \bigcup_i \mathrm{Car}\sigma_i)$. Then T can be expressed by the disjoint composition shown above. □

As a group, $O(\mathbf{Q}^n)$ is also the wreath product of $\mathrm{SYM}(\mathbf{N})$ by the $\mathrm{SYM}(\{-1,1\})$ (see Krishnamurthy, 1986 or Williamson, 1985 for the definition of the wreath product). In this case, $O(\mathbf{Q}^n)$ can be regarded as a transformation group on the $2n$-point set $\{1,-1,2,-2,..,n,-n\}$. The transformation is defined by $\tau J^- x = (\mathrm{Sgn} x)\tau|x|$ if $|x| \notin J$, and $\tau J^- x = -(\mathrm{Sgn} x)\tau|x|$ if $|x| \in J$. However, we are always concerned with transformations on $\mathbf{Q}^n$ or $\{-1,1\}^n$, so that reducing the domain of transformations in this way will not help us.

2.2 Minimal and maximal transformations

In the present study, we are mainly concerned with threshold transformations that are not isometries of $\mathbf{Q}^n$. However, in order to characterize non- isometrical transformations, we investigate their relations to isometries.

Transformations F and G of $\mathbf{Q}^n$ are called *isometrically equivalent* if there exist isometries S and T of $\mathbf{Q}^n$ such that $G = SFT$. Clearly, a transformation is an isometry if and only if it is isometrically equivalent to the identity. If $G = T^{-1}FT$ for an isometry T, then G is called *isometrically similar* to F. In this case, the graphs of F and G are not only isomorphic under the isomorphism induced by T, but also T preserves the Euclidean distance and hence the Hamming distance between every pair of points. If $G = SFT$ for isometries S and T, then $G = T^{-1}(TSF)T$. Therefore, the graph of any transformation isometrically equivalent to F is obtained from F by applying an isometry after F, if we regard two isomorphic graphs induced by an isometry T as the same. If F and G are transformations of $\{-1,1\}^n$, and if $G = SFT$ for some orthogonal transformations S and T of $\{-1,1\}^n$, then G is called *orthogonally equivalent* to F. If $G = T^{-1}FT$ for some orthogonal transformation T of $\{-1,1\}^n$, then G is called *orthogonally similar* to F.

As shown by Proposition 2.1.4, orthogonal transformations of $\{-1,1\}^n$ are the only one-to-one linear transformations of $\mathbf{R}^n$ that map $\{-1,1\}^n$ onto itself. Therefore, by reducing non-isometrical transformations to the isometrically equivalent simplest forms, we may be able to extract some nonlinear aspects, such as reflected in their graphs, that are unique to the non-isometrical transformations.

First we introduce the *variation* of F denoted by $\mathrm{Var}(F)$ for a transformation F of $\mathbf{Q}^n$ as the total number of coordinates that change under F. That is,

$$\mathrm{Var}(F) = \sum_{x \in \mathbf{Q}^n} d_H(x, Fx).$$

Example 2.2.1 $Var(I) = 0$, $Var(\neg) = n \cdot 2^n$.

Proposition 2.2.2 If F and G are isometrically similar, then $\mathrm{Var}(F) = \mathrm{Var}(G)$.

Proof. If T is an isometry, then

$$\begin{aligned}\mathrm{Var}(T^{-1}FT) &= \sum_{x \in \mathbf{Q}^n} d_H(x, (T^{-1}FT)x) \\ &= \sum_{x \in \mathbf{Q}^n} d_H(Tx, T(T^{-1}FT)x) \\ &= \sum_{x \in \mathbf{Q}^n} d_H(Tx, F(Tx)) \\ &= \sum_{y \in \mathbf{Q}^n} d_H(y, Fy) = \mathrm{Var}(F)\end{aligned}$$

□

We call a Boolean transformation F *minimal*, if $\mathrm{Var}(F) \leq \mathrm{Var}(TF)$ for every isometry T. We call a minimal transformation F *uniquely minimal*, if TF is not minimal for any non-identity isometry T. Similarly, we call a Boolean transformation F *maximal*, if $\mathrm{Var}(F) \geq \mathrm{Var}(TF)$ for every isometry T. We call a maximal transformation F *uniquely maximal*, if TF is not maximal for any non-identity isometry T.

Let F and G be isometrically equivalent and uniquely minimal; then $G = SFT$ for some isometries S and T. Therefore, $G = T^{-1}TSFT$. Since G is minimal, TSF is minimal. Since F is uniquely minimal, $TS = I$. Therefore $G = T^{-1}FT$. The discussion above is summarized in the following theorem.

Theorem 2.2.3 If F is a Boolean transformation, then there exists an isometry S such that SF is minimal. If F and G are uniquely minimal and isometrically equivalent, then F and G are isometrically similar.

Example 2.2.4 If T is an isometry, then T is isometrically equivalent to the identity transformation I, which is uniquely minimal, and T is isometrically equivalent to the uniquely maximal transformation $\bar{\neg}$.

Proposition 2.2.5 F is minimal if and only if $\bar{\neg}F$ is maximal. F is uniquely minimal if and only if $\bar{\neg}F$ is uniquely maximal.

Proof. We have $d_H(x, \bar{\neg}y) = n - d_H(x, y)$ for every $x, y \in \mathbf{Q}^n$. Therefore, the proof is clear from $\mathrm{Var}(\bar{\neg}F) = n \cdot 2^n - \mathrm{Var}(F)$. □

2.3 Self-dual transformations

A Boolean function f defined on $\mathbf{Q}^n$ is called *self-dual*, if $\bar{\neg}f = \neg f$. Similarly, a transformation F of $\mathbf{Q}^n$ is called *self-dual*, if $F\bar{\neg} = \bar{\neg}F$. The transformation G of $\{-1, 1\}^n$ equivalent to a self-dual transformation of $\mathbf{Q}^n$ satisfies $-G = G-$ and is also called *self-dual*. Let F be expressed as $F = (F_1, ..., F_n)$, where $F_i = p_i F$. Then, F is self-dual if and only if F_i is self-dual for every i.

Example 2.3.1 If τ is a permutation of $\mathbf{N}$, then τ and $\bar{\neg}\tau (= \tau\bar{\neg})$ are self-dual. Conversely, if T is a self-dual isometry of $\mathbf{Q}^n$, then $T = \tau$ or $\bar{\neg}\tau$ for a permutation τ of $\mathbf{N}$.

If F and G are self-dual, then FG is clearly self-dual. Further, by the following proposition, the set of all self-dual one-to-one transformations of $\mathbf{Q}^n$ is a transformation group.

Proposition 2.3.2 If F is a one-to-one self-dual transformation, then $(\bar{\neg}F)^{-1} = \bar{\neg}F^{-1}$, and F^{-1} is also self-dual.

Proof. Let F be one-to-one and self-dual. Then $\bar{\neg}F\bar{\neg}F^{-1} = FF^{-1} = I$. Therefore, $(\bar{\neg}F)^{-1} = \bar{\neg}F^{-1}$. On the other hand, $(\bar{\neg}F)^{-1} = F^{-1}\bar{\neg}^{-1} = F^{-1}\bar{\neg}$, so that $\bar{\neg}F^{-1} = F^{-1}\bar{\neg}$. □

Now, we shall describe graphs of one-to-one self-dual transformations, though they are rather obvious and partly described in Ishii (1970). We call a self-dual transformation H *elementary*, when if $H = F \odot G$, and both F and G are self-dual, then F or G is the identity I. From these definitions the following proposition is clear.

Proposition 2.3.3 Any self-dual transformation is a disjoint composition of one or several elementary self-dual transformations.

The graph of any one-to-one transformation of a finite set consists of a set of disjoint cycles. In general, let $A = \{(s_1, t_1), ..., (s_k, t_k)\}$, where $s_i \geq 1$ and $t_i \geq 1$ are integers for every i, $t_i \neq t_j$ for $i \neq j$, and $s_1 \cdot t_1 + ... + s_k \cdot t_k = 2^n$. We call A a *cycle* *structure* for $\mathbf{Q}^n$. We say that the cycle structure A is *realized* by a transformation F of $\mathbf{Q}^n$, or that the cycle structure $\mathrm{CS}(F)$ of F is A, and write $\mathrm{CS}(F) = A$, if the set of all cycles of GRAPH(F) consists of s_1 t_1-cycles, ... , and s_k t_k-cycles. A subset C of $\mathbf{Q}^n$ such that $^\urcorner C = C$ is called a *complete set.*

Proposition 2.3.4 If F is an elementary one-to-one self-dual transformation which is not the identity, then $\mathrm{CS}(F) = \{(1,t),(2^n - t, 1)\}$ for some even $t \geq 2$,or $\mathrm{CS}(F) = \{(2,t),(2^n - 2t, 1)\}$ for some $t \geq 2$. Conversely, the cycle structure $\{(1,t),(2^n - t, 1)\}$ for some even $s \geq 2$, and the cycle structure $\{(2,t),(2^n - 2t, 1)\}$ for some $t \geq 2$ are realized by some elementary self-dual transformations of $\mathbf{Q}^n$.

Proof. Let q be a point on a t-cycle such that $t \geq 2$ of an elementary one-to-one self-dual transformation F. If $^\urcorner q$ is in the same cycle, then $^\urcorner(Fq) = F(^\urcorner q)$ and Fq are in the same cycle. Inductively, if x is any point on this cycle, then $^\urcorner x$ is also on the same cycle. Therefore, in this case, t is even, and this cycle and loops form GRAPH(F). If $^\urcorner q$ is on another cycle, then $F^m q$ is on the first cycle and $^\urcorner(F^m q) = F^m(^\urcorner q)$ is on the second cycle for every m. The two cycles and loops form GRAPH(F). Conversely, if t is a positive integer, consider a complete set $C \subseteq \mathbf{Q}^n$ such that $|C| = 2t$, and let $C = A \cup B$ such that $A \cap B = \emptyset$ and if $x \in A$ then $^\urcorner x \in B$ and if $x \in B$ then $^\urcorner x \in A$. Construct a transformation F composed of fixed points and one t-cycle ranging over A. $G = F \odot {}^\urcorner F^\urcorner$ is elementary and self-dual, and $\mathrm{CS}(G) = \{(2,t),(2^n - 2t, 1)\}$. If t is even, consider G defined above for a complete set C such that $|C| = t$. For a point q in C, define H as $Hq = G(^\urcorner q)$, and $H(^\urcorner q) = Gq$ and $Hx = Gx$ for every other x. H is elementary and self-dual and $\mathrm{CS}(H) = \{(1,t),(2^n - t, 1)\}$. □

Theorem 2.3.5 The necessary and sufficient condition for a cycle structure $\{(s_1,t_1),...,(s_k,t_k)\}$ such that $s_1 \cdot t_1 + ... + s_k \cdot t_k = 2^n$ to be realized by a self-dual transformation of $\mathbf{Q}^n$ is that $t_i s_i$ is even for every i.

Proof. By decomposing one-to-one self-dual transformations into elementary self-dual transformations we obtain the necessary part. For the sufficiency, express $\mathbf{Q}^n$ as a mutually disjoint union of s_i complete sets with t_I elements for even t_i and $s_i/2$ complete sets with $2t_i$ elements for odd t_i and the rest of $\mathbf{Q}^n$. Following the proof of Proposition 2.3.4, construct self-dual elementary transformations composed of fixed points and one t_i-cycle for even t_i and two t_i-cycles for odd t_i ranging over each complete set. The disjoint composition of these elementary transformations realizes the given cycle structure. □

2.4 [ ]-REPRESENTATIONS

Assume that the transformation $F = (F_1, ..., F_n)$ of $\mathbf{Q}^n$, where $F_i = p_i F$, is self-dual. A necessary and sufficient condition for $x \in \mathbf{Q}^n$ to be a point such that $x_i = 1$ and $(Fx)_i = 0$ is that $x \in p_i \cdot \neg F_i$. Let f_i be defined as

$$f_i = p_i \cdot \neg F_i \tag{2.4.1}$$

for every i. Then $\neg f_i = \neg(p_i \cdot \neg F_i) = \neg p_i \vee F_i$, so that $p_i \cdot \neg f_i = p_i \cdot F_i$. Also $^\urcorner f_i = (p_i \cdot \neg F_i)^\urcorner = (p_i{}^\urcorner) \cdot (\neg F_i{}^\urcorner) = \neg p_i \cdot F_i$. Since $F_i = p_i \cdot F_i \vee \neg p_i \cdot F_i$, we obtain

$$F_i = p_i \cdot \neg f_i \vee {}^\urcorner f_i. \tag{2.4.2}$$

Conversely, for any Boolean function f_i such that $f_i = p_i \cdot f_i$ for every i, let F_i be defined by (2.4.2). Then

$$\begin{aligned} \neg\bar{\neg}F_i &= \neg((p_i\bar{\neg}) \cdot (\neg f_i\bar{\neg}) \vee f_i) \\ &= (\neg((p_i\bar{\neg}) \cdot (\neg f_i\bar{\neg}))) \cdot \neg f_i \\ &= (p_i \vee f_i\bar{\neg}) \cdot \neg f_i = p_i \cdot \neg f_i \vee (f_i\bar{\neg}) \cdot \neg f_i. \end{aligned}$$

However, $(f_i\bar{\neg}) \cdot f_i = ((p_i \cdot f_i)\bar{\neg}) \cdot p_i \cdot f_i = \neg p_i \cdot (f_i\bar{\neg}) \cdot p_i \cdot f_i = \emptyset$. Therefore,

$$\neg\bar{\neg}F_i = F_i,$$

so that $F = (F_1, ..., F_n)$ is a self-dual transformation. Further,

$$\begin{aligned} p_i \cdot \neg F_i &= p_i \cdot \neg(p_i \cdot \neg f_i \vee f_i\bar{\neg}) = p_i \cdot \neg(p_i \cdot \neg f_i) \cdot (\neg f_i\bar{\neg}) \\ &= p_i \cdot (\neg p_i \vee f_i) \cdot (\neg(p_i \cdot f_i)\bar{\neg}) = p_i \cdot f_i \cdot (p_i \vee (\neg f_i\bar{\neg}) \\ &= f_i \vee f_i \cdot \neg f_i\bar{\neg} = f_i. \end{aligned}$$

Therefore, (2.4.1) is satisfied.

Consequently, any self-dual transformation F such that $F = (F_1, ..., F_n)$ will be represented by a [ ]-representation as

$$F = [f_1, ..., f_n], \tag{2.4.3}$$

where if $x = (x_1, ..., x_n) \in f_i$ then $x_i = 1$, and the relations between F_i and f_i are given above by (2.4.1) and (2.4.2).

Example 2.4.1 Let $F = [p_1 \cdot p_2 \cdot p_3, \neg p_1 \cdot p_2, \neg p_1 \cdot \neg p_2 \cdot p_3]$ be a transformation of $\mathbf{Q}^3$. We express F in the following tables.

$$\begin{array}{c|c} f_1 & \bar{\neg}f_1 \\ \hline f_2 & \bar{\neg}f_2 \\ \hline f_3 & \bar{\neg}f_3 \end{array} = \begin{array}{l|l} 1 \cdot 2 \cdot 3 & \neg 1 \cdot \neg 2 \cdot \neg 3 \\ \hline \neg 1 \cdot 2 & 1 \cdot \neg 2 \\ \hline \neg 1 \cdot \neg 2 \cdot 3 & 1 \cdot 2 \cdot \neg 3 \end{array} = \begin{array}{c|c} 111 & 000 \\ \hline 011 & 100 \\ 010 & 101 \\ \hline 001 & 110 \end{array}$$

Then we obtain GRAPH(F):

$$\begin{tikzcd} 101 \arrow[r] & 111 \arrow[r] & 011 \arrow[r] & 001 \arrow[d] & \\ & 110 \arrow[u] & 100 \arrow[l] & 000 \arrow[l] & 010 \arrow[l] \end{tikzcd}$$

The advantage of the form (2.4.3) is not only its absorption of F_i's self-duality. We have clearly

$$\mathrm{Car}F = \bigcup_{I=1}^{n} (f_i \cup \bar{\neg}f_i).$$

In fact, the points of f_i, whose ith coordinate is 1, are transformed into points whose ith coordinate is 0, while the points of $\bar{\neg}f_i$, whose ith coordinate is 0, are transformed into points whose ith coordinate is 1. And these are all the changes on $\mathbf{Q}^n$ when F is applied. Therefore, if F is self-dual and represented as $[f_1, ..., f_n]$, then clearly

$$\mathrm{Var}(F) = 2\sum_{i=1}^{n} |f_i|. \tag{2.4.4}$$

Further, if $F = [f_1, ..., f_n]$, $G = [g_1, ..., g_n]$, and Car$F$ and Car$G$ are disjoint, then $F + G = [f_1 \vee g_1, ..., f_n \vee g_n]$. Now, let F_i be a Boolean function expressed as

$$F_i = p_i \cdot g_i \vee (\neg p_i) \cdot h_i, \tag{2.4.5}$$

for some $g_i, h_i : \mathbf{Q}^{\mathbf{N}\setminus i} \to \mathbf{Q}$. Then

$$\begin{aligned} f_i &= p_i \cdot \neg F_i \\ &= p_i \cdot \neg g_i. \end{aligned} \tag{2.4.6}$$

Further,

$$\begin{aligned} \neg\bar{\neg}F_i &= \neg(\neg p_i \cdot (g_i \bar{\neg}) \vee p_i \cdot (h_i \bar{\neg})) \\ &= (p_i \vee \neg g_i \bar{\neg}) \cdot (\neg p_i \vee \neg h_i \bar{\neg}) \\ &= p_i \cdot (\neg h_i \bar{\neg}) \vee \neg p_i \cdot (\neg g_i \bar{\neg}) \vee (\neg h_i \bar{\neg}) \cdot (\neg g_i \bar{\neg}) \\ &= p_i \cdot (\neg h_i \bar{\neg}) \vee \neg p_i \cdot (\neg g_i \bar{\neg}) \vee p_i \cdot (\neg h_i \bar{\neg}) \cdot (\neg g_i \bar{\neg}) \vee \neg p_i \cdot (\neg h_i \bar{\neg}) \cdot (\neg g_i \bar{\neg}) \\ &= p_i \cdot (\neg h_i \bar{\neg}) \vee \neg p_i \cdot (\neg g_i \bar{\neg}). \end{aligned}$$

Therefore, $\neg\bar{\neg}F_i = F_i$, if and only if $h_i = \neg g_i \bar{\neg}$, that is,

$$F_i = p_i \cdot g_i \vee \neg p_i \cdot (\neg\bar{\neg} g_i). \tag{2.4.7}$$

Proposition 2.4.2 If $F = [f_1, ..., f_n]$ then

$$k^- F = [f_1, .., f_{k-1}, p_k \cdot \neg f_k, f_{k+1}, .., f_n].$$

Proof. Let $k^- F = [g_1, .., g_k, .., g_n]$. Then $g_k = p_k \cdot \neg(\neg F_k) = p_k \cdot F_k$ by (2.4.1), so that $g_k = p_k \cdot (p_k \cdot \neg f_k \vee \bar{\neg} f_k) = p_k \cdot \neg f_k \vee p_k \cdot (\bar{\neg} f_k)$ by (2.4.2). Since $(\bar{\neg} f_k)x = 1$ implies $(\bar{\neg} x)_k = 1$, i.e. $x_k = 0$, we have $p_k \cdot (\bar{\neg} f_k) = 0$. Therefore, $g_k = p_k \cdot \neg f_k$. Clearly $g_i = f_i$ for any other i. □

Notation If $F = [f_1, ..., f_n]$, then $f_i|1$ is the function from $\mathbf{Q}^{\mathbf{N}\setminus i}$ to $\mathbf{Q}$ defined by

$$(f_i|1)x = f_i(x, 1),$$

where $(x, 1)$ is the point of $\mathbf{Q}^{\mathbf{N}}$ obtained by adding the ith coordinate 1 to x, i.e.

$$P_M(x, 1) = x \quad \text{and} \quad p_i(x, 1) = 1.$$

Proposition 2.4.3 If $F = [f_1, ..., f_n]$ then

$$Fk^- = [k^- f_1, .., p_k \cdot (\neg\bar{\neg}(f_k|1)), .., k^- f_n].$$

Proof. Let $Fk- = [g_1, .., g_k, .., g_n]$. If $i \neq k$, then

$$\begin{aligned} g_i &= p_i \cdot \neg(Fk^-)_i \\ &= p_i \cdot \neg p_i(Fk^-) \\ &= (p_i \cdot \neg(p_i F))k^- \\ &= f_i k^- && \text{by (2.4.1)} \\ &= k^- f_i. && \text{Polya action} \\ g_k &= p_k \cdot \neg(Fk^-)_k \\ &= p_k \cdot (\neg p_k(Fk^-)) \\ &= p_k \cdot (\neg(p_k \cdot \neg f_k \vee \bar{\neg} f_k)k^-) && \text{by (2.4.2)} \\ &= p_k \cdot ((\neg(p_k \cdot \neg f_k) \cdot \neg\bar{\neg} f_k)k^-) \\ &= p_k \cdot (((\neg p_k \vee f_k) \cdot \neg\bar{\neg} f_k)k^-) \\ &= p_k \cdot ((\neg p_k \cdot \neg\bar{\neg} f_k \vee f_k \cdot \neg\bar{\neg} f_k)k^-). \end{aligned}$$

Since

$$p_k \cdot (f_k k^-) = p_k \cdot ((p_k \cdot f_k)k^-) = p_k \cdot (p_k k^-) \cdot (f_k k^-) = p_k \cdot (\neg p_k) \cdot (f_k k^-) = 0,$$

$$\begin{array}{rcll}
g_k & = & p_k \cdot ((\neg p_k \cdot \neg\bar{\neg} f_k)k^-) & \\
& = & p_k \cdot p_k \cdot ((\neg\bar{\neg} f_k)k^-) & \\
& = & p_k \cdot (\neg f_k \bar{\neg})k^-) & \text{Polya action} \\
& = & p_k \cdot (\neg f_k(\mathbf{N}\backslash k)^-) & \\
& = & p_k \cdot (\neg(p_k \cdot (f_k|1))(\mathbf{N}\backslash k)^-) & \\
& = & p_k \cdot ((\neg p_k \vee \cdot(\neg(f_k|1)))(\mathbf{N}\backslash k)^-) & \\
& = & p_k \cdot (\neg p_k \vee \neg(f_k|1)\bar{\neg}) & \\
& = & p_k \cdot (\neg(f_k|1)\bar{\neg}) & \\
& = & p_k \cdot (\neg\bar{\neg}(f_k|1)). & \text{Polya action}
\end{array}$$

□

If $F = [f_1, ..., f_n]$ then

$$Fk^- = [k^- f_1, .., p_k \cdot (\neg\bar{\neg}(f_k|1), .., k^- f_n].$$

Proof. Let $Fk^- = [g_1, .., g_k, .., g_n]$. If $i \neq k$, then

$$\begin{array}{rcl}
g_i & = & p_i \cdot \neg(Fk^-)_i \\
& = & p_i \cdot \neg p_i Fk^- \\
& = & (p_i \cdot \neg p_i F)k^- \\
& = & f_i k^- \\
& = & k^- f_i. \\
g_k & = & p_k \cdot \neg(Fk^-)_k \\
& = & p_k \cdot (\neg p_k Fk^-) \\
& = & p_k \cdot (\neg(p_K \cdot \neg f_k \vee \bar{\neg} f_k)k^-) \\
& = & p_k \cdot ((\neg(p_K \cdot \neg f_k) \cdot \neg\bar{\neg} f_k)k^-) \\
& = & p_k \cdot (((\neg p_K \vee f_k) \cdot \neg\bar{\neg} f_k)k^-) \\
& = & p_k \cdot ((\neg p_K \cdot \neg\bar{\neg} f_k \vee f_k \cdot \neg\bar{\neg} f_k)k^-).
\end{array}$$

If $g_k x = 1$ then $x_k = 1$. But if $x_k = 1$ then $f_k k^- x = 0$, since $f_k y = 1$ implies $y_k = 1$. Therefore,

$$\begin{array}{rcl}
g_k & = & p_k \cdot ((\neg p_K \cdot \neg\bar{\neg} f_k)k^-) = p_k \cdot p_K \cdot ((\neg\bar{\neg} f_k)k^-) \\
& = & p_k \cdot (\neg f_k \bar{\neg})k^-) = p_k \cdot (\neg f_k(N\backslash k)^-) \\
& = & p_k \cdot (\neg(p_k \cdot (f_k|1))(N\backslash k)^-) \\
& = & p_k \cdot ((\neg p_k \vee \cdot(\neg(f_k|1)))(N\backslash k)^-) \\
& = & p_k \cdot (\neg p_k \vee \neg(f_k|1)\bar{\neg}) = p_k \cdot (\neg(f_k|1)\bar{\neg}) \\
& = & p_k \cdot (\neg\bar{\neg}(f_k|1)).
\end{array}$$

□

Let $F = [f_1, .., f_m]$ and $G = [g_{n+1}, .., g_{m+n}]$ be respectively self-dual transformations of $\mathbf{Q}^M$ and $\mathbf{Q}^N$, where $M = \{1, ..., m\}$ and $N = \{m+1, .., m+n\}$. Then the direct product $F \times G$, which is the transformation of $\mathbf{Q}^{M \cup N}$, is also self-dual and represented by

$$F \times G = [f_1 \circ P_M, .., f_m \circ P_M, g_{m+1} \circ P_N, .., g_{m+n} \circ P_N]. \tag{2.4.8}$$

Example 2.4.4 Let $F = [p_1 \cdot p_2 \cdot p_3, \neg p_1 \cdot p_2, \neg p_1 \cdot \neg p_2 \cdot p_3]$ and and $G = [p_4 \cdot p_5, \neg p_4 \cdot p_5]$ be respectively transformations of $\mathbf{Q}^{\{1,2,3\}}$ and $\mathbf{Q}^{\{4,5\}}$.

GRAPH(F) is illustrated in Example 2.4.1. GRAPH(G) is

$$\begin{tikzcd}
11 \arrow[r] & 01 \arrow[d] \\
10 \arrow[u] & 00 \arrow[l]
\end{tikzcd}$$

Then

$$F \times G = [p_1 \cdot p_2 \cdot p_3, \neg p_1 \cdot p_2, \neg p_1 \cdot \neg p_2 \cdot p_3, p_4 \cdot p_5, \neg p_4 \cdot p_5.$$

GRAPH($F \times G$) is

$$\begin{tikzcd}
10110 \arrow[r] & 11111 \arrow[r] & 01101 \arrow[r] & 00100 \arrow[r] & 00010 \arrow[d] & 01000 \arrow[l] \\
 & 11010 \arrow[u] & & & 10011 \arrow[d] & \\
 & 10000 \arrow[u] & & & 11001 \arrow[d] & \\
01011 \arrow[r] & 00001 \arrow[u] & 00111 \arrow[l] & 01110 \arrow[l] & 11100 \arrow[l] & 10101, \arrow[l] \\
01001 \arrow[r] & 00000 \arrow[r] & 10010 \arrow[r] & 11011 \arrow[r] & 11101 \arrow[d] & 10111 \arrow[l] \\
 & 00101 \arrow[u] & & & 01100 \arrow[d] & \\
 & 01111 \arrow[u] & & & 00110 \arrow[d] & \\
10100 \arrow[r] & 11110 \arrow[u] & 11000 \arrow[l] & 10001 \arrow[l] & 00011 \arrow[l] & 01010. \arrow[l]
\end{tikzcd}$$

2.5 Circular and skew-circular transformations

Let ρ be the cyclic permutation $(1, 2, .., n)$ of $\mathbf{N}$. The transformation ρ defined by the Pólya action on $\mathbf{Q}^n$ is the right rotation of coordinates of $\mathbf{Q}^n$, that is, $\rho(x_1, x_2, .., x_n) = (x_n, x_1, .., x_{n-1})$ for every $x = (x_1, x_2, .., x_n) \in \mathbf{Q}^n$. A transformation F of $\mathbf{Q}^n$ is called *circular*, if $F\rho = \rho F$. A transformation G is isometrically similar to a circular transformation, if and only if G satisfies $G\sigma = \sigma G$ for some n-cyclic permutation $\sigma = (s_1, s_2, .., s_n)$.

If F and G are circular, then clearly FG is also circular. If F is circular and one-to-one, then $F\rho = \rho F$ i.e. $\rho^{-1}F^{-1} = F^{-1}\rho^{-1}$. By applying ρ to the left and right of each side of the last equation, we obtain $F^{-1}\rho = \rho F^{-1}$, so that F^{-1} is also circular.

Let $F = (F_1, ..., F_n)$ be a transformation of $\mathbf{Q}^n$, where $F_i = p_i F$. Then $\rho F = (F_n, F_1, ..., F_{n-1})$, while $F\rho = (F_1\rho, F_2\rho, ..., F_n\rho) = (\rho^{-1}F_1, \rho^{-1}F_2, ..., \rho^{-1}F_n)$ Therefore, F is circular if and only if $F_i = \rho F_{i-1}$ for every i, that is,

$$F_i = \rho^{i-1} F_1 \tag{2.5.1}$$

for every i. Further,

Proposition 2.5.1 A self-dual transformation $F = [f_1, ..., f_n]$, where $f_i = p_i \cdot \neg F_i$, is circular if and only if

$$f_i = \rho^{i-1} f_1. \tag{2.5.2}$$

Proof. From (2.5.1) it follows that F is circular and self-dual, if and only if

$$\begin{aligned} F &= [p_1 \cdot \neg F_1, p_2 \cdot \neg(\rho F_1), .., p_i \cdot \neg(\rho^{i-1} F_1, .., p_n \cdot \neg(\rho^{n-1} F_1)] \\ &= [p_1 \cdot \neg F_1, \rho(p_1 \cdot \neg F_1), .., \rho^{i-1}(p_1 \cdot \neg F_1), .., \rho^{n-1}(p_1 \cdot \neg F_1)] \end{aligned}$$

Therefore, F is circular and self-dual if and only if (2.5.2) holds. □

We briefly write

$$F = \langle f \rangle$$

for $F = [f, .., \rho^{i-1} f, ..., \rho^{n-1} f]$, where $p_1 \cdot f = f$. From (2.4.4),

$$\mathrm{Var}(F) = 2n|f|. \qquad (2.5.3)$$

Theorem 2.5.2 Let $F = \langle f \rangle$ be a circular self-dual transformation. Then (i) F is isometrically equivalent to a circular minimal self-dual transformation. (ii) If $|f| \le 2^{n-3}$ then F is minimal. (iii) If $|f| < 2^{n-3}$, then F is uniquely minimal.

Proof. Let $F = (F_1, ..., F_n)$, where $F_i = p_i F$. (i) Suppose $|p_1 \cdot \neg F_j| < |p_1 \cdot \neg F_1|$. If $\sigma = \rho^{-j+1}$, then σF is circular, and $(\sigma F)_1 = F_j$, so that $|p_1 \cdot \neg(\sigma F)_1| = |p_1 \cdot \neg F_j| < |p_1 \cdot \neg F_1|$. Therefore, by (2.5.3) we have $\mathrm{Var}(\sigma F) < \mathrm{Var}(F)$. Let a new F be the σF. Similarly, if $|p_1 \cdot F_j| < |p_1 \cdot \neg F_1|$, then $(\sigma \bar{\neg})F$ is circular, and $\mathrm{Var}((\sigma \bar{\neg})F) < \mathrm{Var}(F)$. Then let a new F be the $(\sigma \bar{\neg})F$. Repeat the above procedure until there is no such j as above. Then we obtain a transformation that is isometrically equivalent to F, circular, and minimal.
(ii) Let $j \neq 1$. We have

$$\begin{aligned} |p_1 \cdot \neg F_j| &= |p_1 \cdot p_j \cdot \neg F_j| + |p_1 \cdot \neg p_j \cdot \neg F_j| \\ &= |\bar{\neg}(p_1 \cdot p_j \cdot \neg F_j)| + |p_1 \cdot \neg p_j \cdot \neg F_j| \\ &= |\neg p_1 \cdot \neg p_j \cdot F_j| + (|p_1 \cdot \neg p_j| - |p_1 \cdot \neg p_j \cdot F_j|), \end{aligned}$$

because F_j is self-dual. Therefore,

$$|p_1 \cdot \neg F_j| \ge 2^{n-2} - |f|,$$

since $|p_1 \cdot \neg p_j| = 2^{n-2}$ and $|\neg p_1 \cdot \neg p_j \cdot F_j| + |p_1 \cdot \neg p_j \cdot F_j| = |\neg p_j \cdot F_j| = |f|$. Similarly $|p_1 \cdot F_j| \ge 2^{n-2} - |f|$ and $|p_1 \cdot F_1| = 2^{n-1} - |f|$. By (i), there exists an isometry T such that TF is minimal, circular, and self-dual. Therefore, if $|f| \le 2^{n-3}$, then $\mathrm{Var}(TF) \ge 2n \cdot (2^{n-2} - |f|) \ge 2n \cdot (2^{n-2} - 2^{n-3}) = 2n \cdot 2^{n-3} \ge 2n|f| = \mathrm{Var}(F)$, so that F is minimal.
(iii) is clear from the proof of (ii). □

Example 2.5.3 n is even ($n = 2m$). $F = \langle f \rangle$,

$$f = p_1 \cdots p_m \cdot \neg p_{m+1} \cdots \neg p_{2m}.$$

GRAPH(F) consists of loops and one n-cycle, which is

$$1 \cdots 10 \cdots 0 \to 01 \cdots 10 \cdots 0 \to ... \to 1 \cdots 10 \cdots 01 \to 1 \cdots 10 \cdots 0.$$

F is uniquely minimal for $n \ge 4$.

In later chapters we will encounter some self-dual transformations F of $\mathbf{Q}^n$ which are not circular but commutative with ρn^-, that is, $F \rho n^- = \rho n^- F$. We call such a transformation skew-circular. Skew-circular transformations are self-dual, since $(\rho n^-)^n = \bar{\neg}$.

Proposition 2.5.4 A self-dual transformation $F = [f_1, ..., f_n]$, where $f_i = p_i \cdot \neg F_i$, is skew-circular if and only if

$$f_i = (\rho n^-)^{i-1} f_1 \text{ for every } i.$$

Proof. Let $F = (F_1, ..., F_n)$ be a self-dual transforma-tion, where $F_i = p_i F$. Then $\rho n^- F = (\neg F_n, F_1, ..., F_{n-1})$, while $F \rho n^- = (F_1 \rho n^-, F_2 \rho n^-, ..., F_n \rho n^-)$. Therefore, F is commutative with ρn^- if and only if

$$\begin{array}{rcl}
F_1 & = & \neg F_n (\rho n^-)^{-1} = \neg \rho n^- F_n, \\
F_2 & = & F_1 (\rho n^-)^{-1} = \rho n^- F_1, \\
F_3 & = & F_2 (\rho n^-)^{-1} = (\rho n^-)^2 F_1, \\
 & & \ldots\ldots \\
F_n & = & F_{n-1} (\rho n^-)^{-1} = (\rho n^-)^{n-1} F_1,
\end{array}$$

From the last equation, it follows that $\rho n^- F_n = (\rho n^-)^n F_1 = \bar{\neg} F_1 = \neg F_1$, which is the first equation. Therefore, F is commutative with ρn^- if and only if $F_i = (\rho n^-)^{i-1} F_1$ for every i. If F is represented as $F = [f_1, ..., f_n]$, then this is equivalent to

$$\begin{array}{rcl}
f_i & = & p_i \cdot \neg F_i = p_i \cdot \neg (\rho n^-)^{i-1} F_1 \\
 & = & (\rho n^-)^{i-1} p_1 \cdot (\rho n^-)^{i-1} (\neg F_1) \\
 & = & (\rho n^-)^{i-1} (p_1 \cdot \neg F_1) \\
 & = & (\rho n^-)^{i-1} f_1.
\end{array}$$

□

$F = [f, .., (\rho n^-)^{i-1} f, ..., (\rho n^-)^{n-1} f]$, where $p_1 \cdot f = f$, is hereafter briefly denoted by

$$F = \langle\langle f \rangle\rangle.$$

Then (2.5.3) also holds.

Example 2.5.5 $F = \langle\langle f \rangle\rangle$,

$$f = p_1 \cdots p_i \cdots p_n.$$

GRAPH(F) consists of loops and one $2n$-cycle, for example, for $n = 4$,

$$\begin{array}{ccccccc}
1111 & \rightarrow & 0111 & \rightarrow & 0011 & \rightarrow & 0001 \\
\uparrow & & & & & & \downarrow \\
1110 & \rightarrow & 1100 & \rightarrow & 1000 & \rightarrow & 0000 \\
1101\partial, & & 1011\partial, & & 1001\partial, & & 1010\partial, \\
0101\partial, & & 0110\partial, & & 0010\partial, & & 0100\partial.
\end{array}$$

A transformation isometrically similar to this transformation was first given by Masters and Mattson (1966).

Let T be an isometry of $\mathbf{Q}^n$. As described in Section 2.1, T is uniquely expressed as a product $T = \tau J^-$ of a permutation τ and a complementation J^-. Let T be circular, then, by definition, $\tau J^- \rho = \rho \tau J^-$. Therefore, by (2.1.1), $\tau \rho (\rho^{-1} J)^- = \rho \tau J^-$, so that $\tau \rho = \rho \tau$ and $\rho^{-1} J = J$. The first equation implies τ is a linear permutation of slope 1, i.e. $\tau = \rho^k$ for some $k \in \mathbf{Z}_n$. From the second equation follows $J = \mathbf{N}$ or $\emptyset$. Therefore

$$T = \rho^k \text{ or } T = \rho^k\bar{\neg} \text{ for some } k. \tag{2.5.4}$$

Conversely, it is clear that any T that satisfies (2.5.4) is a circular transformation. Next, we determine skew-circular isometries. First, if τ is a permutation of $\mathbf{N}$, and if L and M are subsets of $\mathbf{N}$, then it is clear that

$$\tau(L\dot{+}M) = \tau(L)\dot{+}\tau(M). \tag{2.5.5}$$

Lemma 2.5.6 Let $\rho = (1, 2, .., m)$ and $i \neq j$ are elements of $\mathbf{N}_m$. Then

$$X\dot{+}\rho^{-1}X = \{i, j\}, \tag{2.5.6}$$

if and only if $X = \{i+1, ..., j\}$ or $X = \{j+1, ..., i\}$.

Proof. The if part is clear. To prove the only if part, suppose that both X and Y are solutions of (2.5.6). Then $X\dot{+}\rho^{-1}X = Y\dot{+}\rho^{-1}Y$, so that $(X\dot{+}\rho^{-1}X)\dot{+}(Y\dot{+}\rho^{-1}Y) = \emptyset$, i.e. $(X\dot{+}Y)\dot{+}\rho^{-1}(X\dot{+}Y) = \emptyset$ by (2.5.5). Therefore, $X\dot{+}Y = \emptyset$ or $X\dot{+}Y = \mathbf{N}_m$, i.e. $Y = X$ or $Y = X^c$. □

Let $T = \tau J^-$ be a skew-circular isometry of $\mathbf{Q}^n$. Then, by definition, $\tau J^- \rho n^- = \rho n^- \tau J^-$. Therefore, by (2.1.1), $\tau\rho\rho^{-1}J\dot{+}n^{-} = \rho\tau J\dot{+}\tau^{-1}n^{-}$, so that $\tau\rho = \rho\tau$ and $\rho^{-1}J\dot{+}n = J\dot{+}\tau^{-1}n$. From the first equation follows $\tau = \rho^k$ for some $k \in \mathbf{Z}_n$. Then, from the second equation follows $J\dot{+}\rho^{-1}J = \{n-k\}\dot{+}\{n\}$. Therefore, by Lemma 2.5.6, $J = \{n-k+1, ..., n\}$ or $J = \{1, ..., n-k\}$, so that

$$T = \rho^k\{n-k+1, ..., n\}^- \text{ or } T = \rho^k\{1, ..., n-k\}^- \text{ for some } k. \tag{2.5.7}$$

Conversely, it is clear that any T satisfies (2.5.7) is a skew-circular transformation. Thus we have obtained the following proposition.

Proposition 2.5.7 Let T be an isometry of $\mathbf{Q}^n$. Then (i) T is circular if and only if $T = \rho^k$ or $T = \rho^k\bar{\neg}$ for some k. (ii) T is skew-circular if and only if $T = \rho^k\{n-k+1, ..., n\}^-$ or $T = \rho^k\{1, ..., n-k\}^-$ for some k.

2.6. Flow graphs

Let a transformation F of $\mathbf{Q}^n$ be commutative with any element τ of a group $\mathbf{G}$ acting on $\mathbf{Q}^n$. For a subset S of $\mathbf{Q}^n$, let $[S]$ denote $\mathrm{Orb}_{\mathbf{G}}S$. Then, a transformation $F^\sim$ of the orbit set $\{[x] \mid x \in \mathbf{Q}^n\}$ is naturally defined by $F^\sim[x] = [Fx]$. We call $F^\sim$ the *flow* of F. For example, if F is self-dual and circular, then $\mathbf{G}$ is $\langle\rho, \bar{\neg}\rangle$, that is, the group generated by the rotation ρ and complementation $\bar{\neg}$.

An outline of the flow $F^\sim$ can be described by a *flow graph* with an arc set A such that (i) If $(X, Y) \in A$, then X and Y are orbits, that is, $X = [C]$ and $Y = [D]$ for some C and D, and $X \subseteq \mathrm{Car}F$ and $FX \cap Y \neq \emptyset$; (ii) If $x \in \mathrm{Car}F$, then there exists an arc $(X, Y) \in A$ such that $x \in X$ and $Fx \in Y$; (iii) Any cycle $X \to ... \to Z \to X$ (including a loop) of GRAPH($F^\sim$) is a subgraph of the flow graph. (iv) Any cycle $X \to ... \to Z \to X$ (including a loop) of the flow graph is a cycle of GRAPH($F^\sim$).

Note that all cycles and loops as well as some asymptotic properties of $F^\sim$ are described by this flow graph. In particular, if F is one-to-one, then $F^\sim$ is completely represented. In the following example, a Boolean function is expressed with skipped p; for example, $1\cdot 2\cdot(\neg 3\vee 4)$ denotes $p_1\cdot p_2\cdot(\neg p_3\vee p_4)$. A Boolean function f also denotes the set $f^{-1}(1)$, and $\sim$ denotes $\sim_{\langle\rho,\bar{\neg}\rangle}$.

Example 2.6.1 Let $F=\langle f\rangle$, $f=1\cdot 2\cdot 3\neg 6$, be a transforma-tion of $\mathbf{Q}^6$. Since F is circular self-dual, $\mathrm{Car}F=[f]$. We have

$$\begin{array}{rcl}
f=1\cdot 2\cdot 3\neg 6 & = & 1\cdot 2\cdot 3\cdot(4\vee 5)\cdot\neg 6\cup 1\cdot 2\cdot 3\cdot\neg 4\cdot\neg 5\cdot\neg 6,\\
1\cdot 2\cdot 3\cdot(4\vee 5)\cdot\neg 6) & \to_F & \neg 1\cdot 2\cdot 3\cdot(4\vee 5)\cdot\neg 6,\\
1\cdot 2\cdot 3\cdot\neg 4\cdot\neg 5\cdot\neg 6) & \to_F & \neg 1\cdot 2\cdot 3\cdot 4\cdot\neg 5\cdot\neg 6\sim 1\cdot 2\cdot 3\cdot\neg 4\cdot\neg 5\cdot\neg 6,\\
\neg 1\cdot 2\cdot 3\cdot(4\vee 5)\cdot\neg 6 & = & \neg 1\cdot 2\cdot 3\cdot 4\cdot\neg 5\cdot\neg 6\cup\neg 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot\neg 6\cup\neg 1\cdot 2\cdot 3\cdot\neg 4\cdot 5\cdot\neg 6,\\
\neg 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot\neg 6 & \to_F & \neg 1\cdot\neg 2\cdot 3\cdot 4\cdot 5\cdot\neg 6\sim 1\cdot 2\cdot 3\cdot\neg 4\cdot\neg 5\cdot\neg 6,\\
\neg 1\cdot 2\cdot 3\cdot\neg 4\cdot 5\cdot\neg 6 & \notin & \mathrm{Car}F.
\end{array}$$

Therefore, a flow graph of F is

$$\begin{tikzcd}
 & {[1\cdot 2\cdot 3\cdot\neg 4\cdot\neg 5\cdot\neg 6]\partial} \\
{[1\cdot 2\cdot 3\cdot(4\vee 5)\neg 6]} \arrow[ur] \arrow[r] \arrow[dr] & {[\neg 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot\neg 6]} \arrow[u] \\
 & {[\neg 1\cdot 2\cdot 3\cdot\neg 4\cdot 5\cdot\neg 6],}
\end{tikzcd}$$

that is,

$$\begin{tikzcd}
 & {[1\cdot 2\cdot 3\cdot\neg 4\cdot\neg 5\cdot\neg 6]\partial} \\
{[1\cdot 2\cdot 3\cdot(4\vee 5)\neg 6]} \arrow[ur] \arrow[r] \arrow[dr] & {[1\cdot 2\cdot 3\cdot 4\cdot\neg 5\cdot\neg 6]} \arrow[u] \\
 & {[1\cdot 2\cdot\neg 3\cdot 4\cdot\neg 5\cdot\neg 6].}
\end{tikzcd}$$