Finitely generated bijections of $\{ 0,1 \}^Z$

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE

TECHNOLOGICAL UNIVERSITY EINDHOVEN
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS

Finitely generated bijections of $\{0,1\}^{\mathbb{Z}}$

by

O.P. Lossers, J.H. van Lint and W. Nuij

T.H.-Report 74-WSK-01

February 1974

Abstract

Let $f : \{0,1\}^k \to \{0,1\}$ and let $\Phi_f : \{0,1\}^{\mathbb{Z}} \to \{0,1\}^{\mathbb{Z}}$ be defined by

$$(\Phi_f \underline{s})_n := f(s_n, s_{n+1}, \ldots, s_{n+k-1}) \ .$$

Such a mapping is called finitely generated. This report studies finitely generated bijections of $\{0,1\}^{\mathbb{Z}}$. The main result is a non-trivial example for $k = 4$.

AMS Subject Classifications 54D55, 20E99, 05C20

1. Introduction

In recent research work concerning an Ising model J.M. Beltman encountered a problem on finitely generated bijections of $\{0,1\}^{\mathbb{Z}}$ to itself (for definitions see section 2). The main question was whether there are any non-trivial examples of such mappings. Since we were not able to discover any literature concerning this problem but we did find the required examples and other related results we have combined what we have found in this report. The authors would appreciate receiving information concerning similar results in the literature.

2.

Let $S := \{0,1\}^{\mathbb{Z}}$. Elements of S are denoted by underlined letters, $\underline{s} = (\ldots,s_{-1},s_0,s_1,s_2,\ldots)$. We define

$$(2.1) \qquad \forall_{\underline{s}\in S}\ \forall_{\underline{t}\in S}\ [d(\underline{s},\underline{t}) := \sum_{n=-\infty}^{\infty} |s_n - t_n|.2^{-|n|}] .$$

Then (S,d) is a compact metric space.
We are interested in mappings from S to S. The *translation* T is defined by

$$(2.2) \qquad \forall_{\underline{s}\in S}\ \forall_{n\in\mathbb{Z}}\ [(T\underline{s})_n := s_{n+1}] .$$

Furthermore we define the complement operator C by

$$(2.3) \qquad \forall_{\underline{s}\in S}\ \forall_{n\in\mathbb{Z}}\ [(C\underline{s})_n := s_n + 1] ,$$

where from now on addition is mod 2. We shall also use the symbol $\bar{a}$ for a + 1 (mod 2).

(2.4) Definition. A mapping $\Phi : S \to S$ is called *finitely generated* if there is a $k \in \mathbb{N}$ and a function $f : \{0,1\}^k \to \{0,1\}$ and a $p \in \mathbb{Z}$ such that

$$(2.5) \qquad \forall_{\underline{s}\in S}\ \forall_{n\in\mathbb{Z}}[(\Phi\underline{s})_n := f(s_{n+p},s_{n+p+1},\ldots,s_{n+p+k-1})] .$$

The set of all such mappings is denoted by $\mathcal{F}$ and we denote the subset of bijections in $\mathcal{F}$ by $\hat{\mathcal{F}}$. Clearly $T \in \mathcal{F}$ and all mappings in $\mathcal{F}$ commute with T. We shall use the following notation. If $f : \{0,1\}^k \to \{0,1\}$ then Φ_f denotes the mapping in $\mathcal{F}$ with $(\Phi_f\underline{s})_n := f(s_n,s_{n+1},\ldots,s_{n+k-1})$ for all n, i.e. $T^p\Phi_f$ is the mapping Φ of (2.5).

(2.6) THEOREM. *Let* $\Phi : S \to S$ *be a mapping which commutes with* T. *Then* Φ *is continuous iff* $\Phi \in \mathfrak{F}$.

Proof.

(i) Let $\Phi \in \mathfrak{F}$ and let p, k, i be as in (2.4). If $\varepsilon > 0$ we choose N such that

$$\sum_{n=N-|p|-k}^{\infty} 2^{-n} < \frac{\varepsilon}{2}$$

and then define $\delta := 2^{-N}$. Then clearly

$$\forall_{\underline{s}\in S} \forall_{\underline{t}\in S} [d(\underline{s},\underline{t}) < \delta \Rightarrow d(\Phi(\underline{s}),\Phi(\underline{t})) < \varepsilon] .$$

(ii) Suppose Φ commutes with T and Φ is continuous. Let

$$S_i := \{\underline{s} \in S \mid (\Phi\underline{s})_0 = i\} \quad \text{for } i = 0,1.$$

Since Φ is uniformly continuous because (S,d) is compact, the two sets S_0, S_1 which are clearly both open and closed and furthermore disjoint have positive distance δ. Hence for i = 0,1 it follows that if $\underline{s} \in S_i$, $\underline{t} \in S$ and $d(\underline{s},\underline{t}) < \delta$ then $\underline{t} \in S_i$. In other words $(\Phi\underline{t})_0$ does not depend on the coordinates t_i for which $2^{-|i|} < \delta$. On the remaining coordinates we define f in accordance with $\underline{s} \in S_0$ or $\underline{s} \in S_1$. Since $(\Phi\underline{s})_n = (T^n\Phi\underline{s})_0$ it follows that $\Phi \in \mathfrak{F}$.

Now we observe that the mappings in $\hat{\mathfrak{F}}$ are continuous bijections of a compact metric space to itself. Therefore these mappings are homeomorphisms. Therefore Theorem (2.6) implies that each mapping in $\hat{\mathfrak{F}}$ has an inverse in $\hat{\mathfrak{F}}$, i.e. if a finitely generated function is one to one its inverse is also fi- ely generated.

From our definitions it is obvious that the product of 2 finitely generated functions is again finitely generated. Therefore we have proved:

(2.7) THEOREM. $(\hat{\mathfrak{F}},\circ)$ *is a group.*

We have seen that C and T are elements of this group with order 2 resp. ∞. If $f(x_1,x_2,\dots,x_k) = x_i$ then $\Phi_f \in \hat{\mathfrak{F}}$ because $\Phi_f = T^{i-1}$. In the same way $f(x_1,x_2,\dots,x_k) = \bar{x}_i$ yields a $\Phi_f \in \hat{\mathfrak{F}}$. In the next section we shall consider the question whether $\hat{\mathfrak{F}}$ has any other elements than the elements of the subgroup generated by C and T. Firs state some properties we need in the next section.

(2.8) LEMMA. *Let* $\Phi \in \hat{\mathfrak{F}}$. *If* $\Phi\underline{0} = \underline{0}$ *and* $(\Phi\underline{s})_n = 0$ *for* $n < 0$ *then* $s_n = 0$ *for n small enough.*

<u>Proof</u>. Clearly $\lim\limits_{k\to\infty} T^{-k}\Phi\underline{s} = \underline{0}$. By the continuity of Φ^{-1} we have $d(T^{-k}\underline{s},\underline{0}) < 1$ and hence $s_{-k} = 0$ if k large enough.

(2.9) LEMMA. *If* Φ_f *is in* $\hat{\mathfrak{F}}$ *then* $C\Phi_f C$ *is also in* $\hat{\mathfrak{F}}$ *and it is generated in g where* $g(x_1,x_2,\dots,x_k) := \bar{f}(\bar{x}_1,\dots,\bar{x}_k)$.

<u>Proof</u>. Straightforward substitution.

(2.10) LEMMA. *Let* R *be the bijection on* S *defined by* $(R\underline{s})_n := s_{-n}$. *Then* $\Phi_f \in \hat{\mathfrak{F}}$ *implies* $R\Phi_f R \in \hat{\mathfrak{F}}$, *and* $T^{k-1}R\Phi_f R$ *is generated by* g *where* $g(x_1,\dots,x_k) := f(x_k,\dots,x_1)$.

<u>Proof</u>. Straightforward substitution.

<u>Remark</u>. In Lemma (2.9) and Lemma (2.10) we have $g(0,0,\dots,0) = 0$ if $f(0,0,\dots,0) = 0$.

3. Nontrivial finitely generated bijections

In our search for functions f for which $\Phi_f \in \hat{\mathfrak{F}}$ we shall make use of a number of principles which we list below and number P_i $(i = 1,2,\dots)$.

(P1) W.l.o.g. we may assume $f(0,0,\dots,0) = 0$ because $C \in \hat{\mathfrak{F}}$.

We first describe some more notations. From now on when describing $\underline{s} \in S$ we let s_0 be preceded by a semicolon. Thus we destinguish between the elements $(\dots,0,0,0;1,1,1,\dots)$ and $(\dots,0,0;0,1,1,1,\dots)$. Since periodic sequences often occur we introduce a notation which is obvious, denoting a period by square brackets, e.g.

$$(\dots0,1,0,1,0,1,0,1,1;1,0,1,1,1,1,1,\dots) = ([0,1],1;1,0,[1]) .$$

From P_1 we have $\Phi_f([0]) = ([0])$. Since $\Phi_f([1]) = ([f(1,1,\dots,1)])$ we must have $f(1,1,\dots,1) = 1$. It follows that $f(x_1,x_2) = x_1$ and $f(x_1,x_2) = x_2$ are the only functions of 2 variables which satisfy our conditions because $f(0,1) = f(1,0)$ would imply that $\Phi_f([0,1];) = ([0])$ or $([1])$ and then Φ_f is not a bijection.

Let us use the symbol F_k to denote the set of functions $f : \{0,1\}^k \to \{0,1\}$ with $f(0,0,\dots,0) = 0$, $f(1,1,\dots,1) = 1$ and $\Phi_f \in \hat{\mathfrak{X}}$. We have already seen that F_k contains k functions corresponding to translations.

To illustrate the method (which will become rather complicated for $k = 4$) we now consider $k = 3$. We consider the De Bruijn graph (cf. M. Hall, Combinatorial Theory, Ch. 9, Blaisdell, Waltham, 1967).

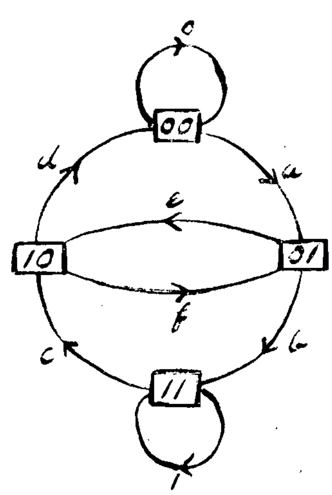

figure 1.

The points of the graph are the pairs $\in \{0,1\}^2$ and (a_1,a_2) is joined by an edge to (b_1,b_2) if $a_2 = b_1$. For arbitrary k the definition is analogous: $(a_1,a_2,\dots,a_{k-1})$ is joined to $(a_2,a_3,\dots,a_{k-1},a_k)$. In figure 1 we place beside the edge from (a_1,a_2) to (a_2,a_3) the number $f(a_1,a_2,a_3)$. In this way figure 1 describes a possible element of F_3.

We then have:

(P2) If $f \in F_k$ then the corresponding De Bruijn graph does not contain a circuit with all values of edges equal to 0, except for the loop on $(0,0,\ldots,0)$. The same holds for the value 1.

(P3) In figure 1 we have $e \neq f$ because $\Phi_f([0,1];) \neq ([0])$ or $([1])$. The same principle holds for $k > 3$.

(P4) The idea of P3 generalizes to periodic sequences with other periods, e.g. in figure 1 $\Phi_f([0,0,1];) = ([a,e,d];)$ and $\Phi_f([0,1,1];) = ([b,c,f];)$ from which it follows that one of the triples (a,e,d), (b,c,f) has 2 zeros and a one, the other has 2 ones and a zero.

(P5) There must be a unique sequence which is mapped by Φ_f into $([0];[1])$. By Lemma (2.8) this implies that in the De Bruijn graph there is a unique path from $(0,0,\ldots,0)$ to $(1,1,\ldots,1)$ such that the values along this path are a number of 0's followed by a number of 1's. E.g. in figure 1 we cannot have $a = 1$, $b = 0$.

(P6) In the De Bruijn graph there must be a path from $(0,0,\ldots,0)$ to $(0,0,\ldots,0)$, i.e. a circuit, with all values along the path equal to 0 except for a single 1. This path is unique. This principle follows from the fact that $([0];1,[0])$ must have an inverse under Φ_f (again using Lemma 2.8).

(P7) If in the De Bruijn graph the edge from $(0,0,\ldots,0)$ to $(0,0,\ldots,0,1)$ has value 1 then in each point the 2 edges pointing out have different value. This is more difficult to see. First observe that a sequence $([0];1,x_1,x_2,\ldots)$ must be $\Phi_f \underline{s}$ where $\underline{s} = ([0];0,0,\ldots,0,1,s_k,s_{k+1},\ldots)$. Since both $x_1 = 0$ and $x_1 = 1$ are possible we must have $f(0,0,\ldots,0,1,0) \neq$ $\neq f(0,0,\ldots,0,1,1)$; etc.

As a consequence we always have $f(0,\ldots,0,1) \neq f(1,1,\ldots,1,0)$ and then by Lemmas 2.9 and 2.10 we have $f(1,0,\ldots,0) \neq f(0,1,\ldots,1)$. The construction of the function g from f, described in these lemmas corresponds in figure 1 and figure 2 to moving the number placed beside the edge to the edge diametrically opposite and taking complements (Lemma 2.9), respectively to moving the number to the mirror image with respect to the axis through 00 and 11 (Lemma 2.10). This symmetry reduces the number of cases to be considered. We shall need more principles but we first finish the discussion for $k = 3$.

(i) If in figure 1 we have $a = 1$ then $b = 1$ by P5 and $e = 0$ by P7. Then $f = 1$ by P3 and $d = 0$ by P7. Also $c = 0$ by P7 and we have $f(x_1,x_2,x_3) = x_3$.

(ii) Let $a = 0$. Then by symmetry $d = 1$. This gives $f(x_1,x_2,x_3) = x_1$. The same solutions turn up when $c = 0$ or $b = 0$.

(iii) Let $a = 0$, $d = 0$, $c = 1$, $b = 1$. Then $e = 1$ by P6 and $f = 0$ by P3 and thus we have $f(x_1,x_2,x_3) = x_2$.

This proves that $|F_3| = 3$, i.e. only trivial functions exist with $\Phi_f \in \hat{\mathfrak{F}}$ if $k \leq 3$.

<u>The case $k = 4$</u>. In figure 2 we consider the De Bruijn graph corresponding to $k = 4$ and label the edges with the function values.

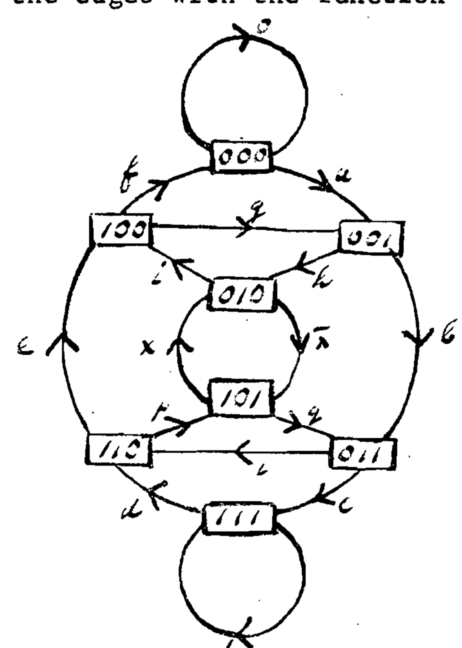

figure 2.

Here we also shall use:

(P8) $b \neq e$. This follows from a consideration of the three 4-cycles in figure 2: ahif, gbre, pqcd. According to P4 these must correspond to 0111, 0011 and 0001. Hence among abcdefghipqr there are 6 zeros. In the same way we see that among ighpqr there are 3 zeros. The result then follows from $a \neq d$ and $c \neq f$.

First we consider the case $a = 1$.
By P7 we have $d = 0$. By P5 we find $c = 1$ and $f = 0$.

(i) $a = 1$, $b = 1$. By P8 we have $e = 0$. Furthermore $h = i = 0$ and $p = q = 1$ by P6. Then $g = 1$ and $r = 0$ by P4 and $x = 0$ by P7 and hence $f(x_1,x_2,x_3,x_4) = x_4$.

(ii) $a = 1$, $b = 0$. Again $d = 0$, $c = 1$, $f = 0$, but now $e = 1$. By P5 we have $h = \bar{x} = q = 1$ and $p = x = i = 0$. This is a contradiction because $qcdp = ahif$.

So we turn to the case $a = 0$: By Lemma 2.10 taking $f = 1$ will give us $f(x_1,x_2,x_3,x_4) = x_1$. Hence we can assume $f = 0$, $c = d = 1$.
By Lemma 2.10 we may assume $b = 0$, $e = 1$.

(i) Suppose $g = 1$. By P6 and P4 we must have $r = 1$ (consider ahif and abref) and $p = q = 0$. If $h = 1$ and $i = 0$ then ([1],d,e;f,[0]) and ([1],d,e,g,h;i,f,[0]) are both ([1];[0]). Therefore $h = 0$, $i = 1$. Then P5 implies that $\bar{x} = 1$ and hence $f(x_1,x_2,x_3,x_4) = x_2 + x_1\bar{x}_3x_4$.

(ii) Suppose $g = 0$. By symmetry $r = 0$ results in $f(x_1,x_2,x_3,x_4) = x_2 + \bar{x}_1x_3\bar{x}_4$. So let $r = 1$. If $h = i = 1$ then ([0],a;h,i,f,[0]) and ([0],a,b;r,e,f,[0]) are the same. If $h = 1$, $i = 0$ then by P5 we have $x = 1$, $p = 0$. This produces the identical sequences ([0],a,b;r,p,x,i,f,[0]) and ([0],a;h,$\bar{x}$,x,i,f,[0]). Hence $h = 0$, $i = 1$ and the other values again follow from P5 and P4. This yields $f(x_1,x_2,x_3,x_4) = x_2$.

The search which we have described yielded the trivial functions and 4 other possibilities which are actually the same by the lemmas 2.9 and 2.10.

<u>The function</u> $f(x_1,x_2,x_3,x_4) = x_2 + x_1\bar{x}_3x_4$.

We shall now show that this function is in F_4. This example was first discovered by W. Nuij. The simplest proof is by considering $(\Phi_f)^2$. Substitution shows that $(\Phi_f)^2 = T^2$ and hence $\Phi_f \in \hat{\mathcal{F}}$. Another way of seeing this is to consider a sequence containing 1 x 01 as a sequence of 4 consecutive symbols, e.g.

. . . . . a b c 1 x 0 1 p q r . . . . . .

Then by definition x is mapped into $\bar{x}$ by $T^{-1}\Phi_f$ but the 1, 0 and 1 are mapped into 1,0,1. A second application then shows that $(T^{-1}\Phi_f)^2 = 1$. The advantage of this second approach is that one easily guesses generalizations of the results we have found.

4. $\underline{F_k \text{ for } k > 4}$

The ideas of section 3 immediately generalize. Let

$$f(x_1,x_2,\ldots,x_n) := x_2 + \bar{x}_1 x_3 x_4 \ldots x_{n-1}\bar{x}_n \qquad (n \geq 4) .$$

By straightforward calculation one finds $(\Phi_f)^2 = T^2$ and hence $f \in F_n$.
To generalize the second point of view in section 3 we define a *good* sequence $(a_1,a_2,\ldots,a_n)$ to be a finite sequence such that for $2 \leq k \leq n-1$.

$$(a_1,a_2,\ldots,a_k) \neq (a_{n-k+1},a_{n-k+2},\ldots,a_n) .$$

We then try to find a sequence $(\varepsilon_1,\ldots,\varepsilon_n)$ such that for some k and ℓ and all choices of $x_1,x_2,\ldots,x_k$ the sequence $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_k,x_1,x_2,\ldots,x_k,\varepsilon_{\ell+1},\ldots$ $\ldots,\varepsilon_n)$ is good. The method is best illustrated by an example. Let

$$f_1 : \{0,1\}^2 \to \{0,1\},\ f_2 : \{0,1\}^2 \to \{0,1\}.$$

We define $g : \{0,1\}^9 \to \{0,1\}$ as follows:

$$g(a_1,1,0,0,0,p,q,1,1) := f_1(p,q) ,$$

$$g(1,0,0,0,p,q,1,1,a) := f_2(p,q) ,$$

$$g(a_1,a_2,\ldots,a_9) = a_6 \quad \text{otherwise.}$$

Consider $T^{-5}\Phi_g$. If for some $\underline{s}$ we have $T^{-5}\Phi_g\underline{s} \neq \underline{s}$, then $\underline{s}$ contains a subsequence $(1,0,0,0,p,q,1,1)$ which is good. It is easily seen that the corresponding coordinates of $T^{-5}\Phi_g\underline{s}$ are $1,0,0,0,f_1(p,q),f_2(p,q),1,1$. If we take $(f_1,f_2) =: \underline{f}$ where $\underline{f}(0,0) = (0,0)$, $\underline{f}(0,1) = (1,1)$, $\underline{f}(1,1) = (1,0)$, $\underline{f}(1,0) = (0,1)$ then $(T^{-s}\Phi_g)^3 = 1$, i.e. $T^{-5}\Phi_g$ is an element of order 3 in $\hat{\mathcal{X}}$.

A natural question is whether there is a function $f \in F_k$ such that $\Phi_f \neq T^i$ and yet Φ_f has infinite order. By section 3 this is not the case for $k = 4$. We give an example for $k = 7$. Let $f(x_1,x_2,x_3,x_4) := x_3 + x_1\bar{x}_2x_4$, $g(x_1,x_2,x_3,x_4) := x_3 + \bar{x}_1x_2\bar{x}_4$, $A := T^{-2}\Phi_f$, $B := T^{-2}\Phi_g$. Then if $\underline{s} := ([0];1,0,1,0,[1,0,0])$ we find $BA\underline{s} = ([0];1,0,1,0,1,0,[1,0,0])$, $(BA)^2\underline{s} = ([0];1,0,1,0,1,0,1,0,[1,0,0])$, etc., i.e. BA has order ∞. Since A en B both have order 2 we see that A and B do not commute.

5. More dimensions

We have not studied this problem extensively for more dimensions but we shall give one example to show that similar results hold. Let $s = (s_{ij};\ i,j \in \mathbb{Z})$ be an element of $S := \{0,1\}^{\mathbb{Z}^2}$. We consider a finitely generated map $\Phi_f S$ defined by

$$(\Phi\underline{s})_{ij} := \bar{s}_{ij} \quad \text{if } s_{i-1,j} = s_{i,j+1} = 1 \text{ and } s_{i+1,j} = s_{i-1,j+1} = 0,$$
$$(\Phi\underline{s})_{ij} := s_{ij} \quad \text{otherwise},$$

i.e. $s_{ij} \to \bar{s}_{ij}$ only if the neighboring coordinates form the configuration

0	1	
1	s_{ij}	0

.

In the same way as before we see that the resulting configuration is

0	1	
1	$\bar{s}_{ij}$	0

, i.e. $\Phi^2 = 1$.

6. Acknowledgements. The authors thank J.M. Beltman for suggesting the problem discussed in this report and mentioning some of his results. Furthermore we thank M.L.J. Hautus, J. Nienhuys and H. van Tilborg for valuable discussions concerning the problem

Notaties:

$\forall_{n \in \mathbb{N}}$ betekent: "Voor ieder natuurlijk getal n".

$\exists_{p \in A}$ betekent: "Er is een element p van de verzameling A waarvoor ......".

$\{x \mid .....\}$ betekent: de verzameling bestaande uit alle x waarvoor ...... geldt. Zo is bijvoorbeeld $\{n \in \mathbb{Z} \mid n < 0\}$ de verzameling der negatieve gehele getallen.