Centrum voor Wiskunde en Informatica
REPORT*RAPPORT*

Discrete wavelet transforms over finite sets which are translation invariant

L. Kamstra

Probability, Networks and Algorithms (PNA)

PNA-R0112 July 31, 2001

Report PNA-R0112
ISSN 1386-3711

CWI
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

CWI is the National Research Institute for Mathematics and Computer Science. CWI is part of the Stichting Mathematisch Centrum (SMC), the Dutch foundation for promotion of mathematics and computer science and their applications.
SMC is sponsored by the Netherlands Organization for Scientific Research (NWO). CWI is a member of ERCIM, the European Research Consortium for Informatics and Mathematics.

Copyright © Stichting Mathematisch Centrum
P.O. Box 94079, 1090 GB Amsterdam (NL)
Kruislaan 413, 1098 SJ Amsterdam (NL)
Telephone +31 20 592 9333
Telefax +31 20 592 4199

Discrete Wavelet Transforms over Finite Sets which are Translation Invariant

Lute Kamstra
CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

ABSTRACT

The discrete wavelet transform was originally a linear operator that works on signals that are modeled as functions from the integers into the real or complex numbers. However, many signals have discrete function values. This paper builds on two recent developments: the extension of the discrete wavelet transform to finite valued signals and the research of nonlinear wavelet transforms triggered by the introduction of the lifting scheme by Sweldens. It defines an essentially nonlinear translation invariant discrete wavelet transform that works on signals that are functions from the integers into any finite set. Such transforms can be calculated very time efficiently since only discrete arithmetic is needed. Properties of these generalized discrete wavelet transforms are given along with an elaborate example of such a transform. In addition, an upper bound is given for the number of certain kinds of discrete wavelet transforms over finite sets and it is shown that, in case the finite set is a ring, there are much more nonlinear transforms than linear transforms. Finally the paper presents some ideas to find explicit examples of discrete wavelet transforms over finite sets.

2000 Mathematics Subject Classification: 42C40, 68U10, 94A12.
Keywords and Phrases: Signal processing, Nonlinear discrete wavelet transforms over finite sets, Second generation wavelets, Perfect reconstruction filter banks.
Note: This work was carried out under project PNA4.2 "Wavelets and Morphology". The research is sponsored (grant no. 613.006.570) by the Dutch Science Foundation (NWO).

1. Introduction

The discrete wavelet transform has proved to be a useful tool for both signal processing and signal analysis. The classic discrete wavelet transform is a linear operator that works on signals that are modeled as functions from (an interval of) the integers into the real or complex numbers. However, a lot of signals are in fact finite valued. In the past ten years, some researchers have constructed extensions of the discrete wavelet transform to resolve this problem.

In 1993 Caire, Grossman and Poor [1] introduced a linear discrete wavelet transform that works on signals that are functions from an interval of the integers to a finite field. In 1996, Swanson and Tewfik [2] used filters over the finite field with two elements to define a linear discrete wavelet transform of binary images. More recently, Klappenecker, May and Nückel [3] have generalized this concept by introducing a linear discrete wavelet transform of signals over finite commutative rings.

Parallel to this development, the lifting scheme as proposed by Sweldens [4] has triggered the research of nonlinear wavelet transforms. These so called second generation wavelets do not require the function values of the signals to be elements of a ring or a field. It is sufficient to have a '+' operator on the signals that can be negated by a corresponding '−' operator. A drawback of the lifting scheme is that it is not known if every discrete wavelet transform can be factored into lifting steps. Of some types of linear discrete wavelet transforms, it is known that they can be factored into linear lifting steps [5]. Of others types it is know that they cannot be factored into linear lifting steps in general [6]. An example of the latter are linear integer to integer transforms [7]. However, which discrete wavelet transforms can be generated by means of the lifting scheme if nonlinear lifting steps are allowed is an open question. An even more general definition of a wavelet transform, where no '+'

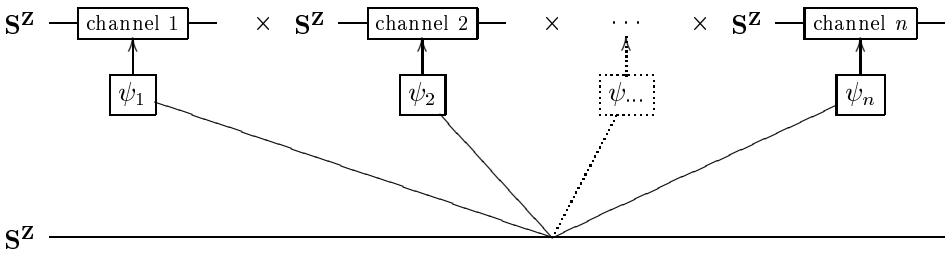


Figure 1: The analysis part of the discrete wavelet transform scheme.

and '$-$' operators on the signals are needed, has recently been introduced by Heijmans and Goutsias [8].

This paper combines these two ideas and proposes a discrete wavelet transform of signals that are functions from the integers into a finite set. Such a transform is in essence not linear since the underlying finite set need not be a ring (or a field); however, if the finite set can be considered a ring then the linear transforms are included. The investigation is restricted to transforms that are translation invariant. Some researchers have already investigated examples of such wavelet transforms [9, 10], but a general theoretical framework was never developed.

The advantage of this extension to the discrete wavelet transform is twofold. On the one hand, since the functions values are taken from a finite set, only discrete arithmetic is needed. This is much more efficient than calculations involving real or complex numbers. On the other hand, the transforms are not restricted to the linear case. Thus, a lot of freedom in choosing a particular transform is gained.

This paper is organized as follows. In Section 2, the concept of a discrete wavelet transform over a finite set is introduced, along with an idea of identifying multi-channel transforms with one-channel transforms. Section 3 derives some general properties of the collection of discrete wavelet transform over a finite set and Section 4 gives an elaborate example of a discrete wavelet transform over a set with two elements. Section 5 introduces translation invariant equivalence classes of signals and explains how the discrete wavelet transform behaves on these classes. This behavior is exploited in Section 6 to produce an upper bound for the number of certain kinds of discrete wavelet transforms over finite sets. Section 6 gives some ideas for producing explicit examples of transforms over finite sets as well.

2. The Discrete Wavelet Transform Scheme

This section describes the discrete wavelet transform scheme that is studied in this paper. It also demonstrates a technique to simplify this scheme.

2.1 The Multi-Channel Scheme

Discrete wavelet transforms work on a signal space. To describe the signal space that is used in this paper, we first choose a nonempty *finite* set $\mathbf{S}$. We will not assume any structure on $\mathbf{S}$. As is explained in the introduction, this is noteworthy, because most texts on wavelets do assume that $\mathbf{S}$ has a certain structure. Frequently, $\mathbf{S}$ is assumed to be a field or a ring and sometimes $\mathbf{S}$ is assumed to be a lattice. By using $\mathbf{S}$, we define the *signal space* $\mathrm{Fun}(\mathbf{Z}, \mathbf{S}) = \mathbf{S}^{\mathbf{Z}}$, that is the set of functions from the domain $\mathbf{Z}$ into $\mathbf{S}$. The elements of the signal space are called *signals*. For a signal $x \in \mathbf{S}^{\mathbf{Z}}$, we use $x[i] \in \mathbf{S}$ to denote the function value of x at position $i \in \mathbf{Z}$.

Consider the discrete wavelet transform scheme as is depicted in Figure 1. It comprises a set of n operators

$$\psi_j : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}, \qquad 1 \leq j \leq n \tag{2.1}$$

that decompose a signal x into n different channels: $\psi_1(x)$ through $\psi_n(x)$. Often, one of these channels, say channel 1, is referred to as the *approximation* of x and the others are called *details* of x.

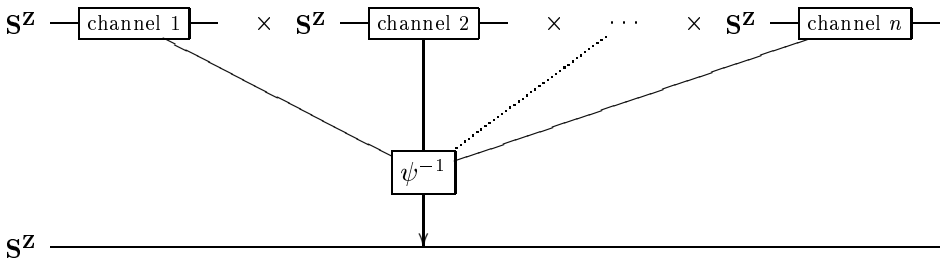


Figure 2: The synthesis part of the discrete wavelet transform scheme.

We want the discrete wavelet transform scheme to be *non-redundant*, therefore we demand that the operator

$$\psi := (\psi_1,\ \psi_2,\ \ldots,\ \psi_n) : \mathbf{S}^{\mathbf{Z}} \to \underbrace{\mathbf{S}^{\mathbf{Z}} \times \cdots \times \mathbf{S}^{\mathbf{Z}}}_{n \text{ times}} \tag{2.2}$$

is surjective. In addition, we want to *perfectly reconstruct* the signal x from the n channels $\psi(x)$. So we demand that ψ is injective as well. Figure 2 shows how the inverse

$$\psi^{-1} : \underbrace{\mathbf{S}^{\mathbf{Z}} \times \cdots \times \mathbf{S}^{\mathbf{Z}}}_{n \text{ times}} \to \mathbf{S}^{\mathbf{Z}} \tag{2.3}$$

can be used to reconstruct a signal form the n channels.

Let us summarize the above in a definition.

Definition 2.1. Let $n \in \mathbf{N}$ and let $\mathbf{S}$ be a finite set. We define the *signal space (over* $\mathbf{S}$*)* to be the set of functions $\mathbf{S}^{\mathbf{Z}}$. The elements of the signal space are called *signals*. An *n-channel discrete wavelet transform over* $\mathbf{S}$ is an operator $\psi : \mathbf{S}^{\mathbf{Z}} \to (\mathbf{S}^{\mathbf{Z}})^n$ that is bijective.

We can use the approximation (channel 1) of a signal as input for yet another discrete wavelet transform (not necessarily the same). This can be repeated any number of times. The scheme thus constructed is called a *multiresolution analysis* of the signal. See Figure 3(a) for an example. By using the appropriate inverses, the signal can be reconstructed from all the details from every stage and the last approximation. This is shown in Figure 3(b).

This paper focuses on translation invariant discrete wavelet transforms. The translation of a signal over a distance t is defined in the usual way.

Definition 2.2. For any $t \in \mathbf{Z}$, the operator $\tau_t : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ defined by

$$\tau_t(x)[i] := x[i - t], \qquad \forall i \in \mathbf{Z} \tag{2.4}$$

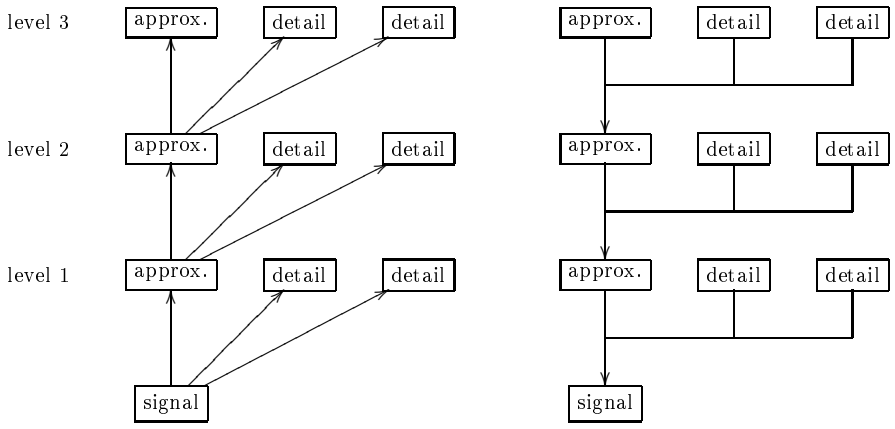
is called a *translation operator*.

Now we can define translation invariance of any operator (not necessarily bijective) from the domain $\mathbf{S}^{\mathbf{Z}}$ into $(\mathbf{S}^{\mathbf{Z}})^n$.

Definition 2.3. Let $n \in \mathbf{N}$. An operator $\phi : \mathbf{S}^{\mathbf{Z}} \to (\mathbf{S}^{\mathbf{Z}})^n$ is said to be *translation invariant* if for every (channel) $1 \leq j \leq n$

$$\phi_j \circ \tau_{nt} = \tau_t \circ \phi_j, \qquad \forall t \in \mathbf{Z}. \tag{2.5}$$

In other words, translation invariance means that translating each of the n channels over a distance 1 corresponds to translating the signal by n.



(a) Analysis. (b) Synthesis.

Figure 3: A three level multiresolution analysis with three channels at each level.

2.2 A New Scheme

This section will demonstrate that an n-channel discrete wavelet transform over a set $\mathbf{S}$ corresponds to a one-channel discrete wavelet transform over the set $\mathbf{F} := \mathbf{S}^n$. As a result, we only have to consider the one-channel case. For the theory we are about to develop, this is more convenient than the multi-channel case.

The general idea is as follows. We identify a signal in $\mathbf{S}^{\mathbf{Z}}$ on which we want to apply an n-channel discrete wavelet transform with a signal in $\mathbf{F}^{\mathbf{Z}}$ by taking n consecutive function values (in $\mathbf{S}$) together to form an element of $\mathbf{F}$. Similarly, we identify the n channels (in $(\mathbf{S}^{\mathbf{Z}})^n$) with one element of $\mathbf{F}^{\mathbf{Z}}$ by taking one function value (in $\mathbf{S}$) of each channel to form an element of $\mathbf{F}$. As a result we can identify an n-channel discrete wavelet transform with a one-channel discrete wavelet transform.

To describe this process in more detail, we introduce some operators that allow us to identify elements in $\mathbf{S}^{\mathbf{Z}}$ or $(\mathbf{S}^{\mathbf{Z}})^n$ with elements in $\mathbf{F}^{\mathbf{Z}}$.

Definition 2.4. Let $\mathbf{S}$ be a finite set and let $\mathbf{F} := \mathbf{S}^n$ for some $n \in \mathbf{N}$. We define a *signal merge operator* $\mathrm{sm}^n : \mathbf{S}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ and a *signal split operator* $\mathrm{ss}^n : \mathbf{F}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ by

$$\mathrm{sm}^n(x)[i] := (x[ni],\ x[ni+1],\ \ldots,\ x[ni+n-1]) \tag{2.6}$$

and

$$\mathrm{ss}^n(x)[ni+k] := (x[i])_k, \qquad 0 \le k < n. \tag{2.7}$$

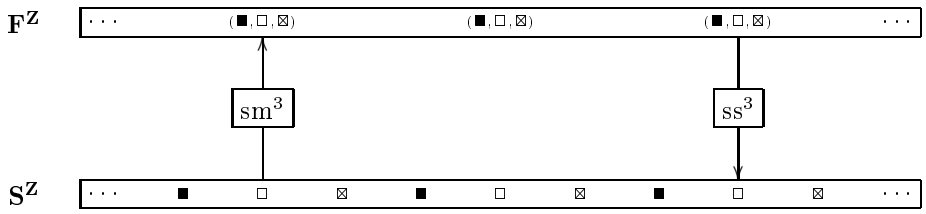
In addition, we define a *channel merge operator* $\mathrm{cm}^n : (\mathbf{S}^{\mathbf{Z}})^n \to \mathbf{F}^{\mathbf{Z}}$ and a *channel split operator* $\mathrm{cs}^n : \mathbf{F}^{\mathbf{Z}} \to (\mathbf{S}^{\mathbf{Z}})^n$ by

$$\mathrm{cm}^n(y_1,\ y_2,\ \ldots,\ y_n)[i] := (y_1[i],\ y_2[i],\ \ldots,\ y_n[i]) \tag{2.8}$$

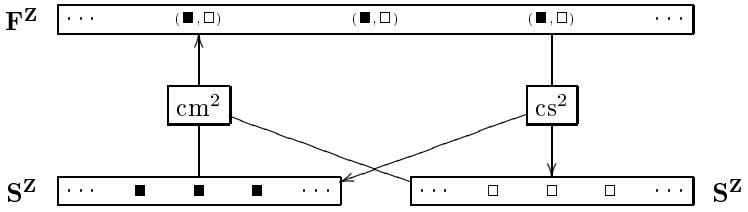
and

$$\mathrm{cs}^n_j(y)[i] := (y[i])_j, \qquad 1 \le j \le n. \tag{2.9}$$

Observe that signal merge operator sm^n is the inverse of the signal split operator ss^n and that the channel merge operator cm^n is the inverse of the channel split operator cs^n. This is illustrated by Figure 4. In case $n = 1$, all the operators sm^1, ss^1, cm^1 and cs^1 equal the identity operator.



(a) The signal merge and split operators for $n = 3$.



(b) The channel merge and split operators for $n = 2$.

Figure 4: The merge and split operators.

Theorem 2.1. *Let* $\mathbf{S}$ *be a finite set and let* $\mathbf{F} := \mathbf{S}^n$ *for some* $n \in \mathbf{N}$. *Then the mapping* $c : \mathrm{Fun}(\mathbf{S}^{\mathbf{Z}}, (\mathbf{S}^{\mathbf{Z}})^n) \to \mathrm{Fun}(\mathbf{F}^{\mathbf{Z}}, \mathbf{F}^{\mathbf{Z}})$ *defined by* $c(\psi) := \mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n$ *is a one-to-one correspondence. Moreover, if* $\omega = c(\psi)$, *then*

1. ω *is injective if and only if* ψ *is injective,*
2. ω *is surjective if and only if* ψ *is surjective and*
3. ω *is translation invariant if and only if* ψ *is translation invariant.*

Proof. We easily verify that c has an inverse given by $c^{-1}(\omega) = \mathrm{cs}^n \circ \omega \circ \mathrm{sm}^n$.

If ψ is injective, then $\omega = \mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n$ is a composition of three injective functions and therefore injective itself. The converse is proved analogously.

Similarly, if ψ is surjective, then $\omega = \mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n$ is a composition of three surjective functions and therefore surjective itself. Again, the converse is proved analogously.

By definition, ω is translation invariant if and only if

$$\omega \circ \tau_t = \tau_t \circ \omega, \qquad \forall t \in \mathbf{Z}.$$

Since $\omega = \mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n$, this is equivalent to

$$\mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n \circ \tau_t = \tau_t \circ \mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n, \qquad \forall t \in \mathbf{Z}. \tag{$*$}$$

We verify that $\mathrm{ss}^n \circ \tau_t = \tau_{nt} \circ \mathrm{ss}^n$ and

$$\tau_t(\mathrm{cm}^n(y_1,\ y_2,\ \ldots,\ y_n)) = \mathrm{cm}^n(\tau_t(y_1),\ \tau_t(y_2),\ \ldots,\ \tau_t(y_n)), \qquad \forall (y_1,\ y_2,\ \ldots,\ y_n) \in (\mathbf{S}^{\mathbf{Z}})^n.$$

Note that in both these equations, the translations on either side of the equal sign work on *different* signal spaces. We conclude that Equation $(*)$ is equivalent to

$$\psi_j \circ \tau_{nt} = \tau_t \circ \psi_j, \qquad \forall t \in \mathbf{Z}, \quad \forall 1 \le j \le n,$$

which is the definition of translation invariance of ψ. □

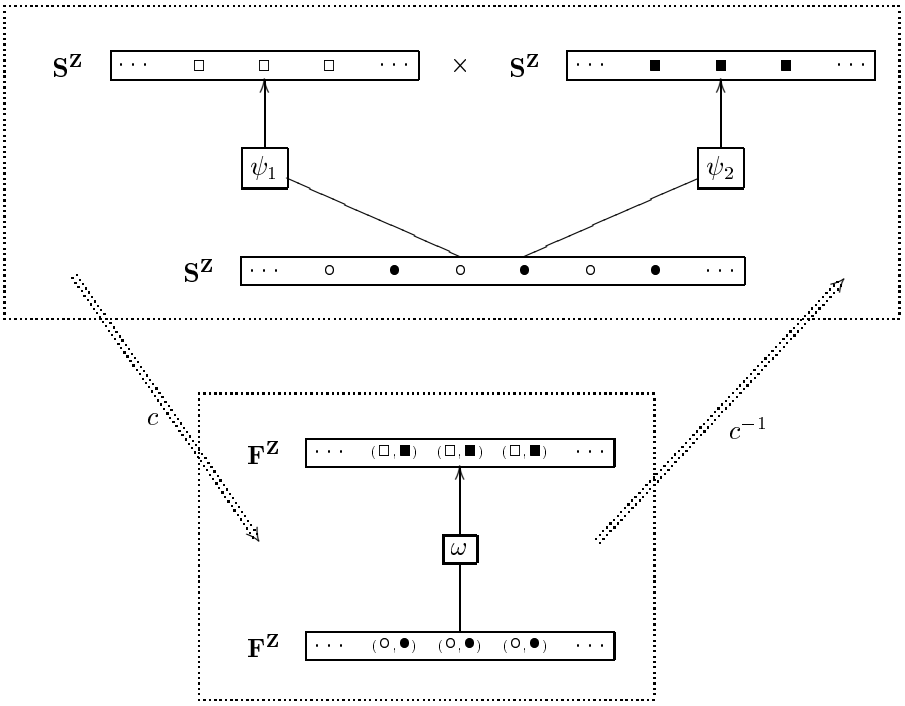


Figure 5: The relation between the classic two-channel and the new one-channel discrete wavelet transform scheme.

The relation between the classic n-channel discrete wavelet transform scheme with operator ψ and the new one-channel discrete wavelet transform scheme with operator $\omega = \mathrm{cm}^n \circ \psi \circ \mathrm{ss}^n$ is depicted in Figure 5.

In conclusion, Theorem 2.1 shows how we can identify translation invariant multi-channel discrete wavelet transforms over a finite set $\mathbf{S}$ with translation invariant one-channel discrete wavelet transforms over the finite set $\mathbf{F} := \mathbf{S}^n$. In the sequel, we will therefore study only these discrete wavelet transforms over $\mathbf{F}$ and 'forget' that $\mathbf{F} = \mathbf{S}^n$. Since we did not assume any structure on $\mathbf{S}$, we do not lose any information by doing this. Later on, for the cases where the number of elements of $\mathbf{F}$ is s^n for some $s, n \in \mathbf{N}$, we can always 'remember' that $\mathbf{F} = \mathbf{S}^n$ for some set $\mathbf{S}$ with s elements.

3. Translation Invariance

In this section, we will derive some basic properties of translation invariant operators on the signal space $\mathbf{F}^{\mathbf{Z}}$ in general and of bijective operators in particular.

This paper frequently manipulates subsets of the integers, so we will develop some notation to facilitate this. Let $A, B \subseteq \mathbf{Z}$ and $t \in \mathbf{Z}$. We use $t + A$ to denote the translation of A by t, that is

$$t + A := \{t + a |\ a \in A\}. \tag{3.1}$$

The Minkowski addition of A and B will be denoted by $A + B$:

$$A + B := \{a + b |\ a \in A \text{ and } b \in B\}. \tag{3.2}$$

The notation $-A$ is used to denote the reflection of A, that is

$$-A := \{-a |\ a \in A\}, \tag{3.3}$$

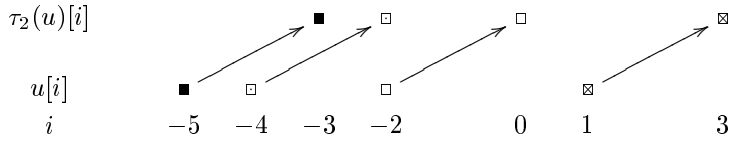


Figure 6: The translation by two of a function $u : \{-5, -4, -2, 1\} \to \mathbf{F}$, resulting in the function $\tau_2(u) : \{-3, -2, 0, 3\} \to \mathbf{F}$.

and $A - B$ denotes $A + (-B)$:

$$A - B := \{a - b |\ a \in A \text{ and } b \in B\}. \tag{3.4}$$

In addition to functions in $\mathbf{F}^{\mathbf{Z}}$, we will frequently use functions in $\mathbf{F}^A$, where A is a subset of $\mathbf{Z}$. In such cases, we will implicitly assume that A is *not empty*. To denote the restriction of a function $u \in \mathbf{F}^A$ to the domain $B \subset A \subseteq \mathbf{Z}$, we use the usual notation $u|_B$. So $u|_B$ is the function in $\mathbf{F}^B$, defined by

$$u|_B[i] := u[i], \qquad \forall i \in B. \tag{3.5}$$

When we consider a function f from a set X into a set Y and A is a subset of X, we will use the notation $f(A)$ to denote the set

$$\{f(x) |\ x \in A\}, \tag{3.6}$$

which is a subset of Y.

3.1 Constructing Translation Invariant Operators

Any translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ can be constructed from a single function $\alpha : \mathbf{F}^A \to \mathbf{F}$, where A is a certain subset of the integers. Vice versa any function $\alpha : \mathbf{F}^A \to \mathbf{F}$ can be used to construct a translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$. Such a function α is the analogue of a convolution filter in the linear case. We will now describe this construction.

The first tool we need is a translation on functions in $\mathbf{F}^A$, when A is a proper subset of the integers. We obtain this by generalizing the translation operator, as defined in Definition 2.2.

Definition 3.1. For any $t \in \mathbf{Z}$, the *translation by* t is an operator $\tau_t : \bigcup_{A \subseteq \mathbf{Z}} \mathbf{F}^A \to \bigcup_{A \subseteq \mathbf{Z}} \mathbf{F}^A$. If $u \in \mathbf{F}^A$, then $\tau_t(u)$ is the element of $\mathbf{F}^{t+A}$ defined by

$$\tau_t(u)[i] := u[i - t], \qquad \forall i \in t + A. \tag{3.7}$$

Observe that for signals in $\mathbf{F}^{\mathbf{Z}}$, this new definition of the translation operator equals the previous definition. Under the new definition, the translation operator τ_t remains bijective and $\tau_t^{-1} = \tau_{-t}$. We extended the translation operator is such a way that

$$\tau_t(x)|_A = \tau_t(x|_{-t+A}), \qquad \forall x \in \mathbf{F}^{\mathbf{Z}}, \quad \forall A \subseteq \mathbf{Z}, \quad \forall t \in \mathbf{Z}. \tag{3.8}$$

To illustrate this extension of the translation operator, let $A = \{-5, -4, -2, 1\}$. If we translate a function $u \in \mathbf{F}^A$ by $t = 2$, we obtain a function in $\mathbf{F}^{2+A} = \mathbf{F}^{\{-3,-2,0,3\}}$. This is depicted in Figure 6.

We can use the translation operator on functions in $\mathbf{F}^A$, $A \subseteq \mathbf{Z}$ to construct an operator $\overline{\alpha} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ from a function $\alpha : \mathbf{F}^A \to \mathbf{F}$.

Definition 3.2. Let A be a nonempty subset of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be any function. For all $i \in \mathbf{Z}$, we define the function $\alpha^i : \mathbf{F}^{i+A} \to \mathbf{F}$ by

$$\alpha^i := \alpha \circ \tau_{-i}. \tag{3.9}$$

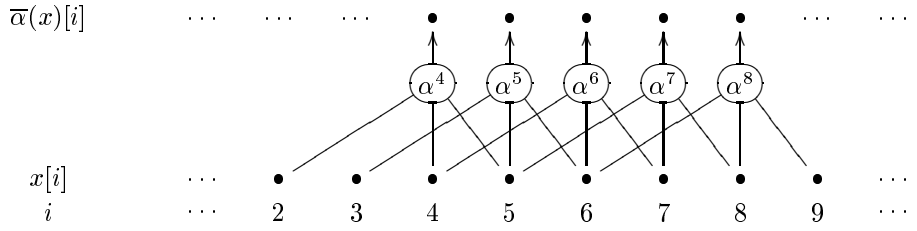


Figure 7: The construction of $\overline{\alpha} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ from $\alpha : \mathbf{F}^A \to \mathbf{F}$ where $A = \{-2, 0, 1\}$.

Furthermore, we define the operator $\overline{\alpha} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ by

$$\overline{\alpha}(x)[i] := \alpha^i(x|_{i+A}), \qquad \forall i \in \mathbf{Z}. \tag{3.10}$$

Consider as an example the function $\alpha : \mathbf{F}^A \to \mathbf{F}$, where $A = \{-2, 0, 1\}$. If we want to construct $\overline{\alpha} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$, we first have to generate the operators $\alpha^i : \mathbf{F}^{i+A} \to \mathbf{F}$ for all $i \in \mathbf{Z}$. E.g., α^7 is an operator that assigns an element of $\mathbf{F}$ to a function u from the domain $7 + A = \{5, 7, 8\}$ into $\mathbf{F}$. Then we can use α^i to calculate $\overline{\alpha}(x)[i]$. This construction is illustrated by Figure 7.

We now state the theorem that justifies the construction of $\overline{\alpha} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ from $\alpha : \mathbf{F}^A \to \mathbf{F}$.

Theorem 3.1. *An operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ is translation invariant if and only if there exists a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $A \subseteq \mathbf{Z}$, such that $\omega = \overline{\alpha}$.*

Proof. Suppose that ω is translation invariant. We define the function $\alpha : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}$ by $\alpha(x) := \omega(x)[0]$. Since ω is translation invariant we have for all $x \in \mathbf{F}^{\mathbf{Z}}$ and all $i \in \mathbf{Z}$

$$\begin{aligned}
\omega(x)[i] &= \tau_{-i}(\omega(x))[0] && \{\text{By Definition 3.1.}\} \\
&= \omega(\tau_{-i}(x))[0] && \{\omega \text{ is translation invariant}\} \\
&= \alpha(\tau_{-i}(x)) && \{\text{By definition of } \alpha\} \\
&= \alpha^i(x) && \{\text{By Definition 3.2.}\} \\
&= \overline{\alpha}(x)[i]. && \{\text{By Definition 3.2.}\}
\end{aligned}$$

Conversely, consider any function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $A \subseteq \mathbf{Z}$. We have

$$\begin{aligned}
\overline{\alpha}(\tau_t(x))[i] &= \alpha^i(\tau_t(x)|_{i+A}) && \{\text{By Definition 3.2.}\} \\
&= \alpha^i(\tau_t(x|_{i-t+A})) && \{\text{By Equation (3.8).}\} \\
&= \alpha(\tau_{-i}(\tau_t(x|_{i-t+A}))) && \{\text{By Definition 3.2.}\} \\
&= \alpha(\tau_{t-i}(x|_{i-t+A})) && \{\text{By Definition 3.1.}\} \\
&= \alpha^{i-t}(x|_{i-t+A}) && \{\text{By Definition 3.2.}\} \\
&= \overline{\alpha}(x)[i-t] && \{\text{By Definition 3.2.}\} \\
&= \tau_t(\overline{\alpha}(x))[i] && \{\text{By Definition 3.1.}\}
\end{aligned}$$

for all $x \in \mathbf{F}^{\mathbf{Z}}$ and all $t, i \in \mathbf{Z}$. Hence $\omega := \overline{\alpha}$ is translation invariant. □

In the sequel, it is important that we make a distinction between translation invariant operators that are finitely supported and translation invariant operators that are not. We define this property as follows.

Definition 3.3. A translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ is called *finitely supported* if there exists at least one nonempty *finite* subset A of $\mathbf{Z}$ and a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ such that $\omega = \overline{\alpha}$.

We can verify that for any nonempty subset $A \subseteq \mathbf{Z}$ and two functions $\alpha : \mathbf{F}^A \to \mathbf{F}$ and $\alpha' : \mathbf{F}^A \to \mathbf{F}$ we have that $\overline{\alpha} = \overline{\alpha'}$ if and only if $\alpha = \alpha'$. However, for two functions $\alpha : \mathbf{F}^A \to \mathbf{F}$ and $\beta : \mathbf{F}^B \to \mathbf{F}$ with $A, B \subseteq \mathbf{Z}$ and $A \neq B$, we could have $\overline{\alpha} = \overline{\beta}$. As an example, consider the sets $A = \{0\}$ and $B = \{0, 1\}$. We define a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ by $\alpha(u) = u[0]$ for all elements u in $\mathbf{F}^A$ and we define a function $\beta : \mathbf{F}^B \to \mathbf{F}$ by $\beta(v) = v[0]$ for all $v \in \mathbf{F}^B$. Both $\overline{\alpha}$ and $\overline{\beta}$ equal the identity operator. However α is not equal to β; their domains are different. The following theorem describes how this problem can be circumvented in case $\overline{\alpha}$ and $\overline{\beta}$ are finitely supported.

Theorem 3.2. *Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a finitely supported translation invariant operator. Then there exists a* unique smallest *nonempty set $A \subseteq \mathbf{Z}$ such that a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $\omega = \overline{\alpha}$ exists.*

Proof. Let $\mathcal{A}_\omega$ be the collection of nonempty sets $A \subseteq \mathbf{Z}$ for which there exists a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $\omega = \overline{\alpha}$:

$$\mathcal{A}_\omega := \big\{ A \subseteq \mathbf{Z} \,\big|\, \exists \alpha \in \mathrm{Fun}\big(\mathbf{F}^A, \mathbf{F}\big) \text{ such that } \omega = \overline{\alpha} \big\}.$$

The intersection of this collection of sets, $\bigcap \mathcal{A}_\omega$, is unique and clearly contained in every set in $\mathcal{A}_\omega$. We will show that $\bigcap \mathcal{A}_\omega \in \mathcal{A}_\omega$ and hence prove that there indeed exists a unique smallest set $A \subseteq \mathbf{Z}$ such that a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $\omega = \overline{\alpha}$ exists.

We will first prove that $A, B \in \mathcal{A}_\omega$ implies that $A \cap B \in \mathcal{A}_\omega$. So we choose two arbitrary sets $A, B \in \mathcal{A}_\omega$. This means that there exist two functions $\alpha : \mathbf{F}^A \to \mathbf{F}$ and $\beta : \mathbf{F}^B \to \mathbf{F}$ such that $\overline{\alpha} = \omega = \overline{\beta}$. Since $\overline{\alpha} = \overline{\beta}$, we know that $\alpha(u|_A) = \beta(u|_B)$ for all $u \in \mathbf{F}^{A \cup B}$. Now consider two elements $p, q \in \mathbf{F}^A$ with $p|_{A\cap B} = q|_{A\cap B}$. Since $p|_{A\cap B} = q|_{A\cap B}$, we can find two elements u, v of $\mathbf{F}^{A\cup B}$ with $u|_A = p$, $v|_A = q$ and $u|_B = v|_B$. We conclude that $\alpha(p) = \alpha(q)$. So $\alpha(p) = \alpha(q)$ for all $p, q \in \mathbf{F}^A$ with $p|_{A\cap B} = q|_{A\cap B}$. This allows us to define the function $\gamma : \mathbf{F}^{A\cap B} \to \mathbf{F}$ by setting $\gamma(r) := \alpha(p)$ for some $p \in \mathbf{F}^A$ with $p|_{A\cap B} = r$. From this, it follows as well that $\overline{\gamma} = \overline{\alpha}$. Hence $A \cap B \in \mathcal{A}_\omega$.

We now know that the intersection of any *finite* subcollection of $\mathcal{A}_\omega$ is contained in $\mathcal{A}_\omega$. Due to the fact that ω is finitely supported, at least one set A^* in $\mathcal{A}_\omega$ is finite. We use it to define the *finite* collection of sets

$$\mathcal{A}^*_\omega := \big\{ A^* \cap A \,\big|\, A \in \mathcal{A}_\omega \big\}.$$

Clearly $\mathcal{A}^*_\omega$ is contained in $\mathcal{A}_\omega$ *and* $\bigcap \mathcal{A}^*_\omega = \bigcap \mathcal{A}_\omega$. Since the collection of sets $\mathcal{A}^*_\omega$ is finite, we have that $\bigcap \mathcal{A}^*_\omega \in \mathcal{A}_\omega$ and therefore that $\bigcap \mathcal{A}_\omega \in \mathcal{A}_\omega$. □

Using this result, we make the following definition.

Definition 3.4. Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a translation invariant operator. If ω is finitely supported then the *support* of ω is the smallest nonempty subset A of $\mathbf{Z}$ such that there exists a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $\overline{\alpha} = \omega$. We call the number of elements of this smallest set the *support size* of ω.

So for a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $A \subset \mathbf{Z}$ finite, the operator $\overline{\alpha}$ has a support that is included in A.

This paper will make some comparisons between discrete wavelet transforms over finite sets and linear discrete wavelet transforms. To be precise, we will give an explicit definition of linearity. It is based on the definition given in [6]. For more background information on linear algebra, we refer the reader to [11].

We will assume that $\mathbf{S}$ is a *commutative ring with unit element*. The set $\mathbf{F} := \mathbf{S}^n$ then becomes an $\mathbf{S}$-module. Furthermore, the set $\mathbf{F}^A$, where $A \subseteq \mathbf{Z}$, is an $\mathbf{S}$-module as well.

Definition 3.5. Let the set $\mathbf{S}$ be a commutative ring with unit element and let $\mathbf{F} := \mathbf{S}^n$. An operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ is called *linear* if

$$\omega(x + y) = \omega(x) + \omega(y) \qquad \text{and} \qquad \omega(a \cdot x) = a \cdot \omega(x) \tag{3.11}$$

for all $x, y \in \mathbf{F}^{\mathbf{Z}}$ and all $a \in \mathbf{S}$.

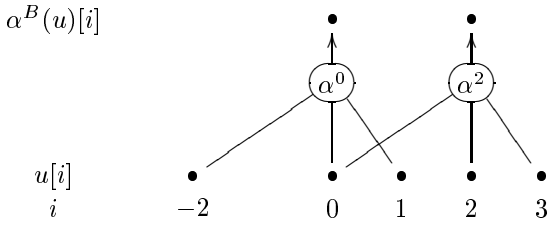


Figure 8: The construction of $\alpha^B : \mathbf{F}^{A+B} \to \mathbf{F}^B$ from $\alpha : \mathbf{F}^A \to \mathbf{F}$ when $A = \{-2, 0, 1\}$ and $B = \{0, 2\}$.

If ω is a translation invariant operator and $\omega = \overline{\alpha}$ for a certain $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $A \subseteq \mathbf{Z}$, then ω is linear if and only if

$$\alpha(u + v) = \alpha(u) + \alpha(v) \qquad \text{and} \qquad \alpha(a \cdot u) = a \cdot \alpha(u) \tag{3.12}$$

for all $u, v \in \mathbf{F}^A$ and all $a \in \mathbf{S}$. So ω is linear if and only if α is linear.

3.2 Composition of Translation Invariant Operators

Two translation invariant operators on $\mathbf{F}^{\mathbf{Z}}$ can be composed to obtain a third, which will be translation invariant as well. If we interpret –as is described in Section 2– two operators on $\mathbf{F}^{\mathbf{Z}}$ as n-channel transforms from $\mathbf{S}^{\mathbf{Z}}$ into $(\mathbf{S}^{\mathbf{Z}})^n$ ($\mathbf{F} = \mathbf{S}^n$), then composition of two such operators has no natural interpretation. This is due to the fact that a signal in $\mathbf{F}^{\mathbf{Z}}$ is interpreted differently before the transform than after applying the the transform. However, if we do not consider this interpretation beforehand, we can use composition to construct new translation invariant operators on $\mathbf{F}^{\mathbf{Z}}$, and any such operator *can* be interpreted as an n-channel transform.

To describe the composite operator effectively, we make the following definition.

Definition 3.6. Let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be any function with $A \subseteq \mathbf{Z}$. For any nonempty $B \subseteq \mathbf{Z}$, we define the function $\alpha^B : \mathbf{F}^{A+B} \to \mathbf{F}^B$ by

$$\alpha^B(u)[i] = \alpha^i(u|_{i+A}), \qquad \forall u \in \mathbf{F}^{A+B}, \quad \forall i \in B. \tag{3.13}$$

The idea behind Definition 3.6 is that we have

$$\overline{\alpha}(x)|_B = \alpha^B(x|_{A+B}), \qquad \forall x \in \mathbf{F}^{\mathbf{Z}}. \tag{3.14}$$

In other words, to be able to determine $\overline{\alpha}(x)|_B$, we need to know only $x|_{A+B}$. As a consequence we have

$$\tau_t(\alpha^B(u)) = \alpha^{t+B}(\tau_t(u)), \qquad \forall u \in \mathbf{F}^{A+B}, \quad \forall t \in \mathbf{Z}. \tag{3.15}$$

Please note that the functions α^i and $\alpha^{\{i\}}$ are formally not equal. While α^i is a function from the domain $\mathbf{F}^{i+A}$ into $\mathbf{F}$, $\alpha^{\{i\}}$ is a function from the domain $\mathbf{F}^{i+A}$ into $\mathbf{F}^{\{i\}}$. However, we do have $\alpha^{\{i\}}(u)[i] = \alpha^i(u)$ for all $u \in \mathbf{F}^{i+A}$. Note as well that $\alpha^{\mathbf{Z}}$ is the same as $\overline{\alpha}$.

Let us expand on the example that is illustrated by Figure 7. We have a function $\alpha : \mathbf{F}^A \to \mathbf{F}$ and $A = \{-2, 0, 1\}$. If we choose $B = \{0, 2\}$, then $A + B$ equals $\{-2, 0, 1, 2, 3\}$ and $\alpha^B : \mathbf{F}^{A+B} \to \mathbf{F}^B$ satisfies

$$\alpha^B(u)[0] = \alpha^0(u|_{\{-2,0,1\}})$$
$$\alpha^B(u)[2] = \alpha^2(u|_{\{0,2,3\}})$$

for all $u \in \mathbf{F}^{A+B}$. This is depicted in Figure 8.

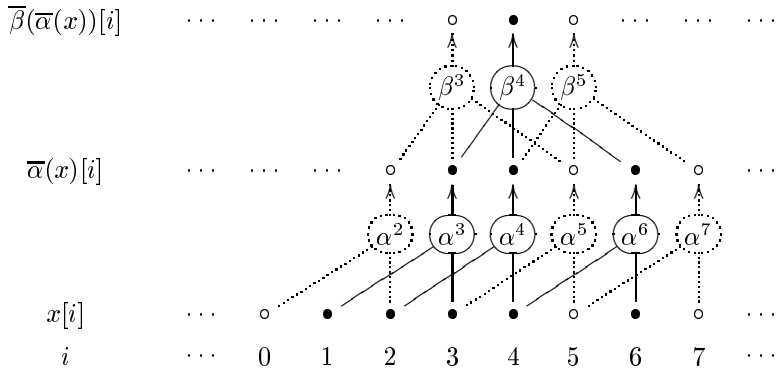


Figure 9: The composition $\overline{\beta} \circ \overline{\alpha}$ for $\alpha : \mathbf{F}^{\{-2,0\}} \to \mathbf{F}$ and $\beta : \mathbf{F}^{\{-1,0,2\}} \to \mathbf{F}$.

Theorem 3.3. *Let $A, B \subseteq \mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ and $\beta : \mathbf{F}^B \to \mathbf{F}$ be two functions. Then we have that $\overline{\beta} \circ \overline{\alpha} = \overline{\gamma}$, where $\gamma : \mathbf{F}^{A+B} \to \mathbf{F}$ is defined by $\gamma := \beta \circ \alpha^B$.*

Proof. By using the respective definitions, Equation (3.14) and Equation (3.15), we obtain

$$\begin{aligned}
\overline{\beta}(\overline{\alpha}(x))[i] &= \beta^i(\overline{\alpha}(x)|_{i+B}) && \{\text{By Definition 3.2.}\}\\
&= \beta^i(\alpha^{i+B}(x|_{i+A+B})) && \{\text{By Equation (3.14).}\}\\
&= \beta(\tau_{-i}(\alpha^{i+B}(x|_{i+A+B}))) && \{\text{By Definition 3.2.}\}\\
&= \beta(\alpha^B(\tau_{-i}(x|_{i+A+B}))) && \{\text{By Equation (3.15).}\}\\
&= \gamma(\tau_{-i}(x|_{i+A+B})) && \{\text{By definition of } \gamma.\}\\
&= \gamma^i(x|_{i+A+B}) && \{\text{By Definition 3.2.}\}\\
&= \overline{\gamma}(x)[i] && \{\text{By Definition 3.2.}\}
\end{aligned}$$

for all signals $x \in \mathbf{F}^{\mathbf{Z}}$ and all $i \in \mathbf{Z}$. □

Consider two operators $\omega, \psi : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ that are translation invariant and have support A and B respectively. According to the above theorem, the support C of their composition $\psi \circ \omega$ is included in $A + B$; however, it might be smaller. For example, if $|A|, |B| > 1$ and $\psi = \omega^{-1}$, then $|A + B| > 1$, while $|C| = |\{0\}| = 1$.

To illustrate Theorem 3.3, let $\alpha : \mathbf{F}^{\{-2,0\}} \to \mathbf{F}$ and $\beta : \mathbf{F}^{\{-1,0,2\}} \to \mathbf{F}$ be two functions. Figure 9 shows how the composition $\overline{\beta} \circ \overline{\alpha}$ is constructed. The calculation of $\overline{\beta}(\overline{\alpha}(x))[4]$ is highlighted. We start by evaluating

$$\alpha^3(x|_{\{1,3\}}), \quad \alpha^4(x|_{\{2,4\}}) \quad \text{and} \quad \alpha^6(x|_{\{4,6\}}),$$

which are the function values of $\alpha^{\{3,4,6\}}(x|_{\{1,2,3,4,6\}})$. Then we calculate

$$\overline{\beta}(\overline{\alpha}(x))[4] = \beta^4(\overline{\alpha}(x)|_{\{3,4,6\}}) = \beta^4(\alpha^{\{3,4,6\}}(x|_{\{1,2,3,4,6\}})).$$

3.3 Bijective Translation Invariant Operators

Until now, we have merely given a definition of a translation invariant wavelet transform. To be able to find explicit examples, we need to provide the proper tools. Since the framework we work in is very general, this is difficult without any further assumptions. We cannot, for example, exploit a ring structure on the function values of signals. What remains are primarily techniques from combinatorial

theory and group algebra. They are used in this subsection to state some strong necessary, but not sufficient, conditions on translation invariant bijective operators.

As we have seen, every translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ can be constructed from a function $\alpha : \mathbf{F}^A \to \mathbf{F}$. Since we are interested in translation invariant bijective operators, it is natural to ask for which functions $\alpha : \mathbf{F}^A \to \mathbf{F}$ the operator $\overline{\alpha}$ is bijective. This subsection will look at a property of α that can be used to identify a large group of functions α for which $\overline{\alpha}$ is *not* bijective.

Let A be a nonempty subset of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be a function. In addition, we choose another nonempty subset B of $\mathbf{Z}$ and consider the function $\alpha^B : \mathbf{F}^{A+B} \to \mathbf{F}^B$ as defined in the previous subsection. The function α^B decomposes its domain $\mathbf{F}^{A+B}$ into a number of (possibly empty) subsets

$$U_v := \big\{ u \in \mathbf{F}^{A+B} \big|\ \alpha^B(u) = v \big\}, \qquad v \in \mathbf{F}^B.$$

If every set U_v is nonempty then the collection of sets $\{U_v\}_{v \in \mathbf{F}^B}$ is a partition of $\mathbf{F}^{A+B}$. If every set in this partition has the same cardinality then we say that α satisfies the equipartition condition for the set B.

Definition 3.7. Let A be a nonempty subset of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be a function. The function α is said to satisfy the *equipartition condition for a nonempty subset B of $\mathbf{Z}$* if the sets

$$U_v := \big\{ u \in \mathbf{F}^{A+B} \big|\ \alpha^B(u) = v \big\}, \qquad v \in \mathbf{F}^B \tag{3.16}$$

all have the same cardinality.

We will prove that every $\alpha : \mathbf{F}^A \to \mathbf{F}$, for which $\overline{\alpha}$ is bijective, satisfies the equipartition condition for any nonempty subset B of $\mathbf{Z}$. The following technical lemma will be used in this proof.

Lemma 3.4. *Let the collection of sets $\{A_i |\ i \in I\}$ be a partition of the set A and let $\{B_j |\ j \in J\}$ be a partition of B. Furthermore, suppose that for all $i \in I$ and $j \in J$, the cardinality of A_i and B_j are equal. Then the cardinality of A and B are equal if and only if the cardinality of I and J are equal.*

Proof. Suppose that the cardinality of A and B are equal. Because A_i and B_j also have the same cardinality, there exists a bijection $f : A \to B$ such that for all $i \in I$ we have $f(A_i) = B_j$ for a unique $j \in J$ depending on i. This means that $g : I \to J$, (well) defined by

$$g(i) = j \qquad \Longleftrightarrow \qquad f(A_i) = B_j,$$

is bijective as well. Thus the cardinality of I and J are the same.

Conversely, suppose that the cardinality of I and J are equal. Then there exists a bijection $g : I \to J$. Since the cardinality of A_i and $B_{g(i)}$ are the same, there exists a bijection $f_i : A_i \to B_{g(i)}$ as well. It follows that function $f : A \to B$, (well) defined by $f|_{A_i} := f_i$, is bijective. Thus A and B have the same cardinality. □

The following theorem states that the equipartition condition for a set B is stronger when the set B is larger.

Theorem 3.5. *Let A and B be nonempty subsets of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be a function. If α satisfies the equipartition condition for B then*

1. *α satisfies the equipartition condition for any nonempty subset of B and*
2. *α satisfies the equipartition condition for any translation of B.*

Proof of 1. Let C be a nonempty subset of B. In this proof, we will use the letter u for elements in $\mathbf{F}^{A+B}$, v for elements in $\mathbf{F}^B$, p for elements in $\mathbf{F}^{A+C}$ and the letter q for elements in $\mathbf{F}^C$. Let the

collection of sets $\{U_v\}_{v\in\mathbf{F}^B}$ be defined as is Definition 3.7 and let the collection of sets $\{P_q\}_{q\in\mathbf{F}^C}$ be defined by

$$P_q := \{p \in \mathbf{F}^{A+C} \mid \alpha^C(p) = q\}.$$

In order to prove the first part of the theorem, we assume that the sets U_v, $v \in \mathbf{F}^B$ all have the same cardinality and we will show that the sets P_q, $q \in \mathbf{F}^C$ have the same cardinality as well.

For any $q \in \mathbf{F}^C$, the collection of sets $\{U_v \mid v \in \mathbf{F}^B \text{ and } v|_C = q\}$ is a partition of the set

$$U'_q := \{u \in \mathbf{F}^{A+B} \mid \alpha^B(u)|_C = q\}.$$

Since all the sets U_v have equal cardinality and for every $q \in \mathbf{F}^C$ the index set $\{v \in \mathbf{F}^B \mid v|_C = q\}$ has the same cardinality, it follows from Lemma 3.4 that all the sets U'_q have equal cardinality as well.

Observe that $u \in U'_q$ if and only if $u|_{A+C} \in P_q$. Hence the collection of sets

$$\left\{\{u \in \mathbf{F}^{A+B} \mid u|_{A+C} = p\} \,\middle|\, p \in P_q\right\}$$

is a partition of U'_q. Every class in the partition has equal cardinality (independent of q), so it follows from Lemma 3.4 that all the sets P_q have equal cardinality. □

Proof of 2. Let C be a translation of B: $t + C = B$ for some $t \in \mathbf{Z}$. Again, we will use the letter u for elements in $\mathbf{F}^{A+B}$, v for elements in $\mathbf{F}^B$, p for elements in $\mathbf{F}^{A+C}$ and the letter q for elements in $\mathbf{F}^C$. We define the collection of sets $\{U_v\}_{v\in\mathbf{F}^B}$ and $\{P_q\}_{q\in\mathbf{F}^C}$ as previously. To prove the second part of the theorem, we assume that the sets U_v, $v \in \mathbf{F}^B$ all have the same cardinality and we will show that the sets P_q, $q \in \mathbf{F}^C$ have the same cardinality as well.

We accomplish this by proving that every set P_q is in one-to-one correspondence with some set U_v, namely $U_{\tau_t(q)}$. Note that $q \in \mathbf{F}^C$ implies $\tau_t(q) \in \mathbf{F}^{t+C} = \mathbf{F}^B$. We claim that the aforementioned correspondence is given by τ_t. Since τ_t is bijective, we need only prove that $\tau_t(P_q) = U_{\tau_t(q)}$.

First, we show that $\tau_t(P_q) \subseteq U_{\tau_t(q)}$. So let $p \in P_q$. Obviously $\tau_t(p) \in \mathbf{F}^{t+A+C} = \mathbf{F}^{A+B}$. Furthermore, we have that

$$\alpha^B(\tau_t(p)) = \alpha^{t+C}(\tau_t(p)).$$

By Equation (3.15) we have

$$\alpha^{t+C}(\tau_t(p)) = \tau_t(\alpha^C(p)) = \tau_t(q).$$

In other words, $\tau_t(p) \in U_{\tau_t(q)}$. Second, to show that $\tau_t(P_q) \supseteq U_{\tau_t(q)}$, we can prove that $P_{\tau_{-t}(q)} \supseteq \tau_{-t}(U_q)$. This is done analogously. □

As a consequence of Theorem 3.5 we have the following.

Corollary 3.6. *Let A be a nonempty subset of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be a function. If $\overline{\alpha}$ is bijective, then α satisfies the equipartition condition for every nonempty subset of $\mathbf{Z}$.*

Proof. Note that $\overline{\alpha}$ equals $\alpha^{\mathbf{Z}}$. The result follows directly from Theorem 3.5 and the fact that the sets

$$\{x \in \mathbf{F}^{\mathbf{Z}} \mid \alpha^{\mathbf{Z}}(x) = y\}$$

have cardinality 1 for all $y \in \mathbf{F}^{\mathbf{Z}}$. □

It is noteworthy that there exist functions $\alpha : \mathbf{F}^A \to \mathbf{F}$ which satisfy the equipartition condition for every nonempty subset of $\mathbf{Z}$, but for which $\overline{\alpha}$ is *not* bijective. An example is the case $\mathbf{F} = \{0, 1\}$,

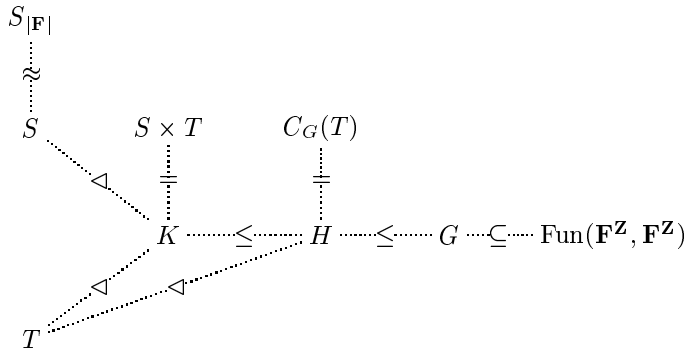


Figure 10: The relations between various subgroups of G. The symbol '$\lhd$' is used to denote 'is a normal subgroup of', the symbol '$\leq$' means 'is a subgroup of' and '$\approx$' is used to denote 'is isomorphic to'. In addition, $S \times T$ stands for the internal direct product of S and T and the notation $C_G(T)$ is used for the centralizer of T in G.

the field with two elements, and the function $\alpha : \mathbf{F}^{\{0,1\}} \to \mathbf{F}$, defined by $\alpha(u)[0] = u[0] + u[1]$ for all $u \in \mathbf{F}^{\{0,1\}}$. The operator $\overline{\alpha}$ is surjective, but not injective. It can be shown that

$$\left|\left\{x \in \mathbf{F}^{\mathbf{Z}} \,\middle|\, \overline{\alpha}(x) = y\right\}\right| = 2 \tag{3.17}$$

for all $y \in \mathbf{F}^{\mathbf{Z}}$.

An interesting question about translation invariant bijective operators is how their support is related to the support of their inverse. A first naive guess is that if the support of a translation invariant bijective operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{Z}$ is A then the support of ω^{-1} is $-A$. However, this is not true. A counterexample is given in the next section. Even an attempt to prove that the inverse of a finitely supported translation invariant bijective operator is finitely supported was unsuccessful. So this remains an open question. A trivial relation between the support of a translation invariant bijective operator and the support of its inverse is given by the following theorem.

Theorem 3.7. *Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a translation invariant bijective operator with support A. Then the inverse ω^{-1} is translation invariant and its support has at least one element in common with $-A$.*

Proof. The translation invariance of ω^{-1} is trivially proved. We have for all $t \in \mathbf{Z}$

$$\omega^{-1} \circ \tau_t = (\tau_{-t} \circ \omega)^{-1} = (\omega \circ \tau_{-t})^{-1} = \tau_t \circ \omega^{-1}.$$

Let B be the support of ω^{-1}. It follows from Theorem 3.3 that the support of $\omega^{-1} \circ \omega$ is included in $A + B$. Since $\omega^{-1} \circ \omega$ is the identity mapping on $\mathbf{F}^{\mathbf{Z}}$, it has support $\{0\}$. We easily verify that $0 \in A + B$ if and only if $-A \cap B$ is nonempty. □

We could also look at translation invariant bijective operators from a group theoretical point of view. This is not relevant for the remainder of this paper, but might still be interesting. The bijective operators in $\mathrm{Fun}(\mathbf{F}^{\mathbf{Z}}, \mathbf{F}^{\mathbf{Z}})$ form a group G under composition. We can identify the following subgroups of G.

1. The set H of translation invariant bijective operators.
2. The set K of translation invariant bijective operators with support size one.
3. The set S of translation invariant bijective operators with support $\{0\}$.

4. The set T of translations.

The subgroup S is isomorphic to $S_{|\mathbf{F}|}$, the symmetric group of degree $|\mathbf{F}|$. Both S and T are normal subgroups of K and K is the internal direct product of S and T. The subgroup K is in turn a subgroup of H. In addition T is a normal subgroup of H and H is the centralizer of T in G. These relations are shown if Figure 10. For an introduction to these algebraic concepts, we refer the reader to [12].

These assertions are not difficult to prove. It is obvious that the set of bijective operators $G \subseteq \mathrm{Fun}(\mathbf{F}^{\mathbf{Z}}, \mathbf{F}^{\mathbf{Z}})$ together with the composition operator forms a group. It is easily verified that T is a subgroup of G. By definition, H is the centralizer of T in G. Hence T is a normal subgroup of H and H is a subgroup of G.

Let us prove that the set of translation invariant bijective operators with support one $K \subseteq H$ is a subgroup of H. We choose two elements $\omega, \psi \in K$. Since the supports of both ω and ψ has size one, there exist functions $\alpha : \mathbf{F}^{\{a\}} \to \mathbf{F}$ and $\beta : \mathbf{F}^{\{b\}} \to \mathbf{F}$ with $a, b \in \mathbf{Z}$, such that $\omega = \overline{\alpha}$ and $\psi = \overline{\beta}$. Using Theorem 3.3, we conclude that $\psi \circ \omega$ has support $\{a + b\}$ and thus that it contained in K. So K is closed under composition. To prove that the inverse of ω is contained in K is conceptually not difficult, but notationally a bit awkward. First, note that for any function $\alpha : \mathbf{F}^{\{a\}} \to \mathbf{F}$, we have that $\overline{\alpha}$ is bijective if and only if α is bijective. Furthermore, we can rewrite the the function $\alpha : \mathbf{F}^{\{a\}} \to \mathbf{F}$ into a function $f : \mathbf{F} \to \mathbf{F}$ by identifying an element u of $\mathbf{F}^{\{a\}}$ with the element $u[a]$ of $\mathbf{F}$:

$$f(u[a]) := \alpha(u), \qquad \forall u \in \mathbf{F}^{\{a\}}.$$

This function f is bijective as well. Now we define the function $\alpha^* : \mathbf{F}^{\{-a\}} \to \mathbf{F}$ by

$$\alpha^*(v) = f^{-1}(v[-a]), \qquad \forall v \in \mathbf{F}^{\{-a\}}.$$

We have that $\overline{\alpha^*}$ is the inverse of $\overline{\alpha}$.

We now show that S and T are normal subgroups of K. It is readily verified that both the set $S \subseteq K$ of translation invariant bijective operators with support $\{0\}$ and the set of translations $T \subseteq K$ are subgroups of K. Since T is a normal subgroup of H and K is a subgroup of H, T is also a normal subgroup of K. Now choose an element σ of S and an element ω of K. Observe that the support of $\omega \circ \sigma \circ \omega^{-1}$ is $\{0\}$. Hence $\omega S \omega^{-1} \subseteq S$ for all $\omega \in K$ and we proved that S is a normal subgroup of K.

To prove that K is the internal direct product of its normal subgroups S and T, we verify that the intersection of S and T contains only the identity element. What remains it showing that the set $ST := \{\sigma \circ \tau |\ \sigma \in S \text{ and } \tau \in T\}$ equals K. We easily verify that $ST \subseteq K$. Conversely any element $\omega \in K$ with support $\{a\}$ satisfies $\omega = \omega \circ \tau_{-a} \circ \tau_a$. Since the support of $\omega \circ \tau_{-a}$ is $\{0\}$, it is a member of S and consequently $K \subseteq ST$.

Finally, we prove that the group S of translation invariant bijective operators with support $\{0\}$ is in isomorphic to the symmetric group of degree $|\mathbf{F}|$. We trivially have that the group S^* of bijections on $\mathbf{F}$ is isomorphic to $S_{|\mathbf{F}|}$. So we define a mapping $\Phi : S^* \to S$ by

$$\Phi(\sigma)(x)[i] = \sigma(x[i]), \qquad \forall \sigma \in S^*, \quad \forall x \in \mathbf{F}^{\mathbf{Z}}, \quad \forall i \in \mathbf{Z}.$$

We have that $\Phi(\sigma \circ \pi) = \Phi(\sigma) \circ \Phi(\pi)$ for all $\sigma, \pi \in S^*$, hence Φ is a homomorphism. In addition, we can verify that Φ is injective as well as surjective. This means that Φ is an isomorphism, which is what we wanted to show.

4. Example

This section will study two translation invariant bijective operators in detail. It is an example of the theory presented in the previous two sections. The two operators will be applied to the rows and columns of an image to obtain a two dimensional decomposition.

In this example we consider a two-channel binary wavelet transform and its inverse. This means that we have $\mathbf{S} = \{0, 1\}$ and $\mathbf{F} = \mathbf{S}^2 = \{(0, 0),\ (0, 1),\ (1, 0),\ (1, 1)\}$. Furthermore, we define the

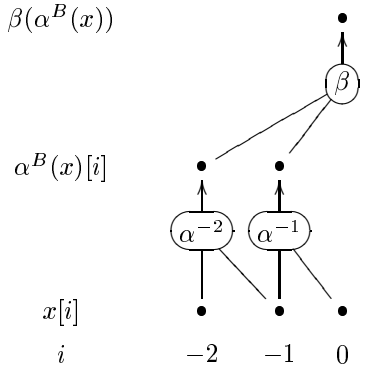
$u[0]$	$u[1]$	$\alpha(u)$
(0,0)	(0,0)	(0,0)
(0,0)	(0,1)	(1,0)
(0,0)	(1,0)	(0,1)
(0,0)	(1,1)	(1,1)

$u[0]$	$u[1]$	$\alpha(u)$
(0,1)	(0,0)	(0,0)
(0,1)	(0,1)	(0,1)
(0,1)	(1,0)	(1,1)
(0,1)	(1,1)	(1,0)

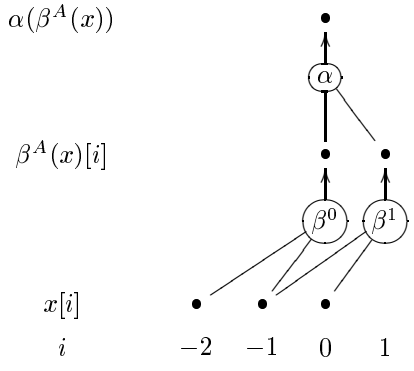
$u[0]$	$u[1]$	$\alpha(u)$
(1,0)	(0,0)	(0,0)
(1,0)	(0,1)	(0,1)
(1,0)	(1,0)	(1,1)
(1,0)	(1,1)	(1,0)

$u[0]$	$u[1]$	$\alpha(u)$
(1,1)	(0,0)	(0,0)
(1,1)	(0,1)	(0,1)
(1,1)	(1,0)	(1,1)
(1,1)	(1,1)	(1,0)

Table 1: The definition of the function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $A = \{0,1\}$. For each element $u \in \mathbf{F}^A$, the value of $\alpha(u) \in \mathbf{F}$ is given.



(a) First α, then β.



(b) First β, then α.

Figure 11: The construction of the functions $\beta \circ \alpha^B : \mathbf{F}^{A+B} \to \mathbf{F}$ and $\alpha \circ \beta^A : \mathbf{F}^{A+B} \to \mathbf{F}$.

function $\alpha : \mathbf{F}^A \to \mathbf{F}$ with $A = \{0,1\}$ by giving a list of its function values. This is done in Table 1. The function $\beta : \mathbf{F}^B \to \mathbf{F}$ with $B = \{-2,-1\}$ is defined as a translation of α: $\beta = \alpha \circ \tau_2$.

From the function α and β, we can construct the translation invariant operators $\overline{\alpha} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ and $\overline{\beta} : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$. Because $\beta = \alpha \circ \tau_2$ we have $\overline{\alpha} = \overline{\beta} \circ \tau_2$. We claim that both these operators are bijective and that $\overline{\alpha}^{-1} = \overline{\beta}$. To verify this, we must demonstrate that both $\overline{\beta} \circ \overline{\alpha}$ and $\overline{\alpha} \circ \overline{\beta}$ equal the identity operator. Theorem 3.3 shows that

$$\overline{\beta} \circ \overline{\alpha} = \overline{\beta \circ \alpha^B},$$
$$\overline{\alpha} \circ \overline{\beta} = \overline{\alpha \circ \beta^A}.$$

In other words, we have to show that the functions $\beta \circ \alpha^B : \mathbf{F}^{A+B} \to \mathbf{F}$ and $\alpha \circ \beta^A : \mathbf{F}^{A+B} \to \mathbf{F}$ as depicted in Figure 11 satisfy

$$\beta(\alpha^B(u)) = u[0], \qquad \forall u \in \mathbf{F}^{A+B},$$
$$\alpha(\beta^A(v)) = v[0], \qquad \forall v \in \mathbf{F}^{A+B}.$$

We can do this by simply verifying these two equations for every element $u \in \mathbf{F}^{A+B}$ and every element $v \in \mathbf{F}^{A+B}$. As an example for the first equation, suppose $u \in \mathbf{F}^{A+B}$ is given by $u[-2] = (0,0)$, $u[-1] = (0,1)$ and $u[0] = (0,0)$. Then $\alpha^B(u)[-2] = (1,0)$ and $\alpha^B(u)[-1] = (0,0)$ and subsequently $\beta(\alpha^B(u)) = (0,0)$, which is equal to $u[0]$. For the second equation, consider $v \in \mathbf{F}^{A+B}$ given by $v[-2] = (1,1)$, $v[-1] = (1,1)$ and $v[0] = (0,1)$. Now $\beta^A(v)[0] = (1,0)$ and $\beta^A(v)[1] = (0,1)$ and $\alpha(\beta^A(v)) = (0,1)$, which is equal to $v[0]$.

Table 1 gives a nice demonstration of Corollary 3.6 as well. We easily check that the set

$$\{u \in \mathbf{F}^A \mid \alpha(u) = v\}$$

has four elements for every $v \in \mathbf{F}$. Since β is a translation of α, we see as well that the set

$$\{v \in \mathbf{F}^B \mid \beta(v) = u\}$$

also has four elements for every $u \in \mathbf{F}$.

It is noteworthy that neither of the operators $\overline{\alpha}$ and $\overline{\beta}$ is linear. In this example we have that $\mathbf{S} = \{0, 1\}$. So if we use modulo 2 arithmetic on $\mathbf{S}$, then $\mathbf{S}$ certainly is a commutative ring with unit element; it even is a field. To show that, for example, the operator $\overline{\alpha}$ is not linear, we can consider the elements $u, v \in \mathbf{F}^A$ given by

$$u[0] = (0,0) \qquad u[1] = (0,1)$$
$$v[0] = (0,1) \qquad v[1] = (0,0).$$

We observe that one the one hand we have

$$\alpha(u) + \alpha(v) = (1,0) + (0,0) = (1+0,\ 0+0) = (1,0).$$

On the other hand, since

$$(u+v)[0] = u[0] + v[0] = (0,0) + (0,1) = (0+0,\ 0+1) = (0,1) \qquad \text{and}$$
$$(u+v)[1] = u[1] + v[1] = (0,1) + (0,0) = (0+0,\ 1+0) = (0,1),$$

we have $\alpha(u+v) = (0,1)$. A similar observation can be made for the operator $\overline{\beta}$.

If we want to use the operators $\overline{\alpha}$ or $\overline{\beta}$ on binary images, we have to overcome some problems. First of all, images are two dimensional, while our operators work on one dimensional signals. We solve this by applying the operators first on every row and then on every column. This is a common technique in signal processing. In wavelet literature, such a two dimensional transform is usually called a separable wavelet transform [13]. Secondly, the function values of binary images are elements of $\mathbf{S}$, while $\overline{\alpha}$ and $\overline{\beta}$ work on signals with function values in $\mathbf{F}$. This is solved as described in Section 2, by 'preprocessing' with the signal merge operator $\mathrm{sm}^2 : \mathbf{S}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ or the channel merge operator $\mathrm{cm}^2 : (\mathbf{S}^{\mathbf{Z}})^2 \to \mathbf{F}^{\mathbf{Z}}$ and 'post processing' with the signal split operator $\mathrm{ss}^2 : \mathbf{F}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ or the channel split operator $\mathrm{cs}^2 : \mathbf{F}^{\mathbf{Z}} \to (\mathbf{S}^{\mathbf{Z}})^2$. Lastly, both the rows and columns of an image are only defined on an interval of $\mathbf{Z}$ while all the operators work on signals that are defined on $\mathbf{Z}$. We work around this problem by extending the image periodically so that it is defined on $\mathbf{Z}$. As will be explained in Section 5, this a valid approach since translation invariant operators map p-periodic signals to q-periodic signals, where q is a divisor of p.

Figure 12 shows the application of the operator $\overline{\alpha}$ to the rows of a binary image. The top left shows the original image (that is, one period of the original image). Black pixels denote function values $0 \in \mathbf{S}$, white pixels denote $1 \in \mathbf{S}$. First, the signal merge operator is applied to the rows to make the rows signals in $\mathbf{F}^{\mathbf{Z}}$. The result is shown in the top right in Figure 12. Here $(0,0) \in \mathbf{F}$ is represented by black, $(0,1) \in \mathbf{F}$ by dark gray, $(1,0) \in \mathbf{F}$ by light gray and $(1,1) \in \mathbf{F}$ is represented by white pixels. Then, the operator $\overline{\alpha}$ is applied to the rows of the image. The result is in the lower right of the figure. The four gray levels refer to the same elements of $\mathbf{F}$ as previously. Last, the channel split operator is applied to the rows to obtain two binary images. The lower left of Figure 12 shows the result. The left image is the approximation channel, the right is the detail. As can be expected, white pixels denote $1 \in \mathbf{S}$, black pixels denote $0 \in \mathbf{S}$. We can duplicate this entire procedure for the columns of both the approximation image and the detail image thus obtained. This process is depicted in Figure 13.

Since $\overline{\alpha}$ is a bijective operator, we can reverse this decomposition of the binary image into an approximation image and three detail images. This is also shown in Figure 12 and Figure 13. We

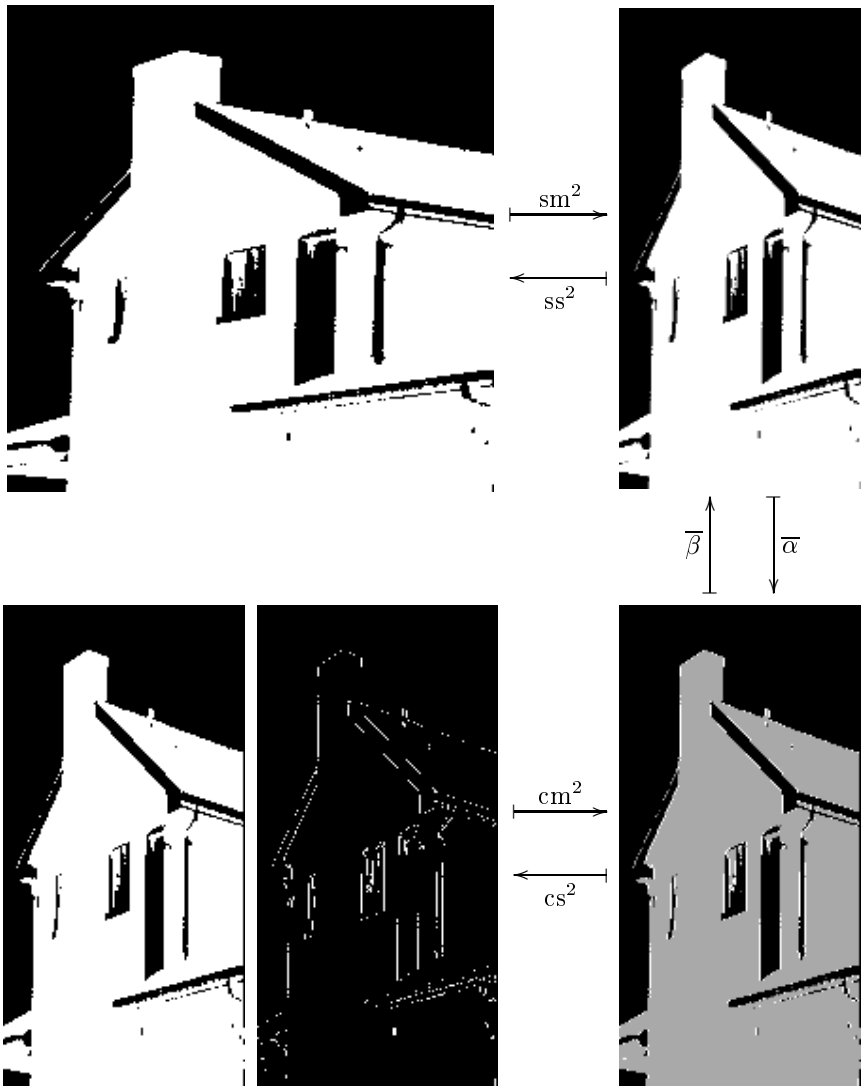


Figure 12: The application of the operator $\mathrm{cs}^2 \circ \overline{\alpha} \circ \mathrm{sm}^2 : \mathbf{S}^{\mathbf{Z}} \to (\mathbf{S}^{\mathbf{Z}})^2$ on the rows of a binary image to obtain a two-channel decomposition. The original image can be reconstructed by applying the operator $\mathrm{ss}^2 \circ \overline{\beta} \circ \mathrm{cm}^2 : (\mathbf{S}^{\mathbf{Z}})^2 \to \mathbf{S}^{\mathbf{Z}}$ on every pair of rows of the decomposition.

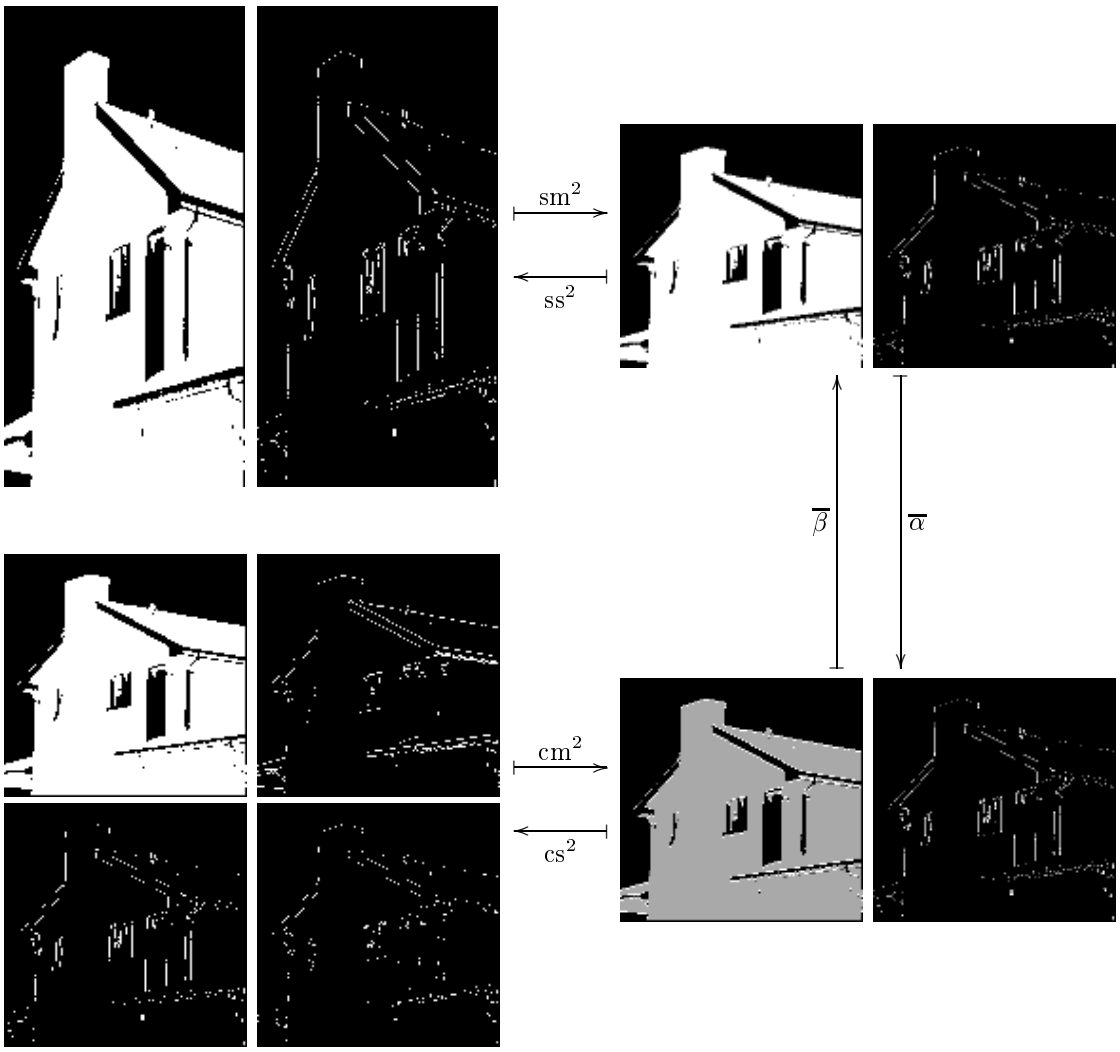


Figure 13: The application of the operator $\mathrm{cs}^2 \circ \overline{\alpha} \circ \mathrm{sm}^2 : \mathbf{S}^{\mathbf{Z}} \to (\mathbf{S}^{\mathbf{Z}})^2$ on the columns of two binary images to obtain a two-channel decomposition of each. The original images can be reconstructed by applying the operator $\mathrm{ss}^2 \circ \overline{\beta} \circ \mathrm{cm}^2 : (\mathbf{S}^{\mathbf{Z}})^2 \to \mathbf{S}^{\mathbf{Z}}$ on every pair of columns of each decomposition.

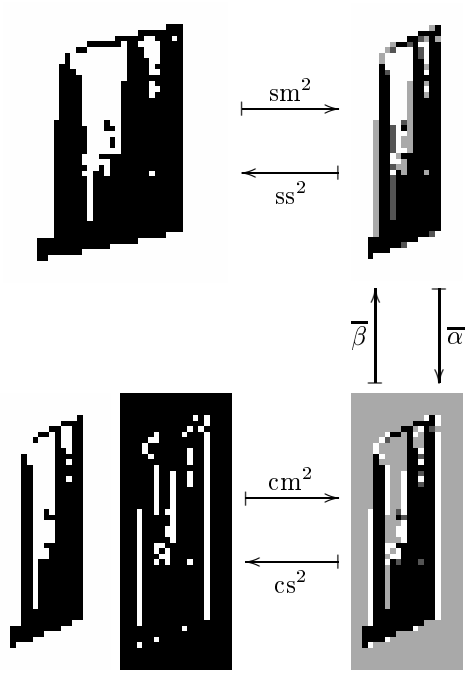


Figure 14: The same as Figure 12, but zoomed in on a part of the image.

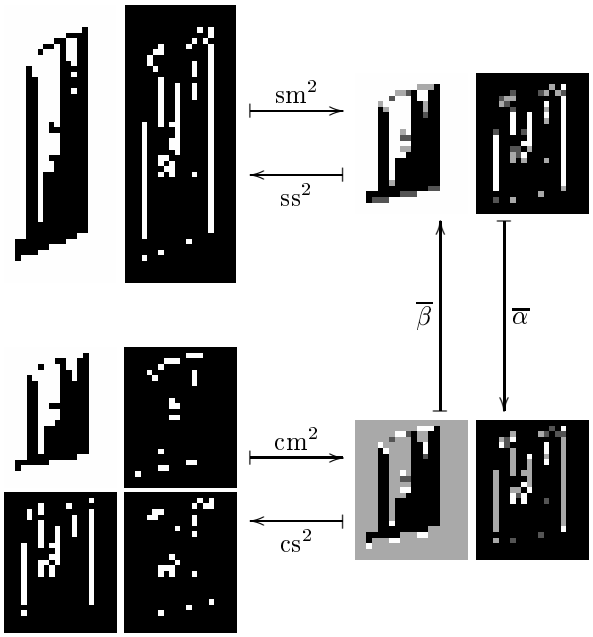


Figure 15: The same as Figure 13, but zoomed in on a part of the image.

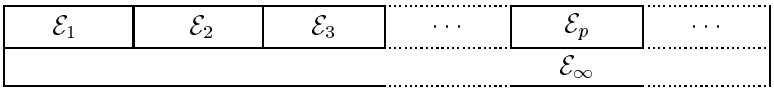


Figure 16: The partition of the collection of equivalence classes $\mathcal{E}$.

have to start by vertically merging the images into two images by using the channel merge operator on the columns, then use the inverse of $\overline{\alpha}$, that is $\overline{\beta}$, on the columns and subsequently apply the signal split operator on the columns. We then merge the two binary images thus obtained by using the channel merge operator on the rows, continue by applying $\overline{\beta}$ on the rows and finish by using the signal split operator on the rows. The image thus obtained is equal to the original image. For a more detailed view of this process, we refer to Figure 14 and Figure 15, that show a part of the image of the house, namely the window.

5. Equivalence Classes of Signals

This section studies the way translation invariant operators act on translation invariant equivalence classes of signals. As a result, we will be able to derive an upper bound for the number of translation invariant bijective operators. Our starting point is the definition of an equivalence relation on the signal space $\mathbf{F}^{\mathbf{Z}}$.

Definition 5.1. We define the relation $\sim$ on $\mathbf{F}^{\mathbf{Z}}$ by

$$x \sim y \quad \Longleftrightarrow \quad \exists t \in \mathbf{Z} \text{ such that } \tau_t(x) = y. \tag{5.1}$$

In other words, two signals are related through $\sim$ if one is a translation of the other. It is obvious that this defines an equivalence relation. The collection of equivalence classes of the equivalence relation $\sim$ on $\mathbf{F}^{\mathbf{Z}}$ is denoted by $\mathcal{E}$. This collection forms a partition of the signal space. An equivalence class $E \in \mathcal{E}$ comprises all translates $\tau_t(x)$ of some element x of the signal space. If x is periodic with period p, then E contains p elements. Otherwise, if x is aperiodic, E is infinite.

Definition 5.2. For all $p \in \mathbf{N}$, we define the collection $\mathcal{E}_p \subseteq \mathcal{E}$ by

$$\mathcal{E}_p := \{E \in \mathcal{E} |\ E \text{ has } p \text{ elements}\}. \tag{5.2}$$

The collection $\mathcal{E}_\infty \subset \mathcal{E}$ is defined by

$$\mathcal{E}_\infty := \{E \in \mathcal{E} |\ E \text{ is not finite}\}. \tag{5.3}$$

Note that the collections $\mathcal{E}_p$, $p \in \mathbf{N}$, together with the collection $\mathcal{E}_\infty$ form a partition of the collection $\mathcal{E}$. This is depicted in Figure 16. By definition, for $p \in \mathbf{N}$ all the equivalence classes in $\mathcal{E}_p$, have the same cardinality (namely p). Likewise for the equivalence classes in $\mathcal{E}_\infty$. We easily verify that every equivalence class in $\mathcal{E}_\infty$ has the same cardinality as $\mathbf{Z}$.

Translation invariant operators on the signal space map equivalence classes to equivalence classes. Moreover, a p-periodic equivalence class is mapped to a q-periodic equivalence class, where q is a divisor of p (notation $q \mid p$).

Theorem 5.1. *Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a translation invariant operator. If $E \in \mathcal{E}$, then $\omega(E) \in \mathcal{E}$. Moreover, if $E \in \mathcal{E}_p$ with $p \in \mathbf{N}$, then there exists a $q \mid p$ such that $\omega(E) \in \mathcal{E}_q$.*

Proof. Suppose that $E \in \mathcal{E}$ and choose a signal $x \in E$. Since $\mathcal{E}$ is a partition of the signal space, there exists an $F \in \mathcal{E}$ such that $y := \omega(x) \in F$. For every $x' \in E$ there exists a $t \in \mathbf{Z}$ such that $x' = \tau_t(x)$. This means that $\omega(x') = \omega(\tau_t(x)) = \tau_t(\omega(x)) = \tau_t(y) \in F$. So $\omega(E) \subseteq F$. On the other hand, for every $y' \in F$ there exists a $t \in \mathbf{Z}$ such that $y' = \tau_t(y)$. This means that there exists an element $x' \in E$ such that $\omega(x') = y'$, namely $x' = \tau_t(x)$. Thus $\omega(E) \supseteq F$.

Now suppose that $E \in \mathcal{E}_p$ for some $p \in \mathbf{N}$ and let y be a signal in $F := \omega(E) \in \mathcal{E}$. There exists an $x \in E$ such that $\omega(x) = y$. Since x is p-periodic, we have $\tau_p(x) = x$. It follows that $\tau_p(y) = y$. So y is periodic and its period q is a divisor of p. Hence $F \in \mathcal{E}_q$ for a divisor q of p. □

It follows from the above proposition that we can make the following definition.

Definition 5.3. For a translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{Z}$, we define $\widetilde{\omega} : \mathcal{E} \to \mathcal{E}$ by

$$\widetilde{\omega}(E) = \omega(E). \tag{5.4}$$

The next theorem shows that we can more or less reverse the last statement of Theorem 5.1.

Theorem 5.2. *Let $\lambda : \mathcal{E} \to \mathcal{E}$ have the property that if $E \in \mathcal{E}_p$ with $p \in \mathbf{N}$, then $\lambda(E) \in \mathcal{E}_q$ for a certain $q \mid p$. Then there exists a translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ with $\widetilde{\omega} = \lambda$.*

Proof. We define an operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ by specifying $\omega|_E$ for each $E \in \mathcal{E}$. This is a valid approach since $\mathcal{E}$ is a partition of the domain $\mathbf{F}^{\mathbf{Z}}$ of ω. The Axiom of Choice states that for each $E \in \mathcal{E}$ we can choose one $x \in E$ and one $y \in \lambda(E)$. Next, we define $\omega(\tau(x)) := \tau(y)$ for all translations τ. This indeed defines $\omega|_E$ since $E = \{\tau_t(x) |\ t \in \mathbf{Z}\}$. Moreover, the definition is not ambiguous because if x is p-periodic, then y is q-periodic for some divisor q of p. It is readily verified that ω thus defined is translation invariant and satisfies $\widetilde{\omega} = \lambda$. □

We will now prove some properties of the function $\widetilde{\omega}$ associated with a translation invariant operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$.

Theorem 5.3. *Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a translation invariant operator. If $\widetilde{\omega}$ is injective, then $\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p$ for all $p \in \mathbf{N}$ and $\widetilde{\omega}(\mathcal{E}_\infty) \subseteq \mathcal{E}_\infty$.*

Proof. To have a convenient notation, we define the collection of equivalence classes

$$\mathcal{E}_p^* := \bigcup_{i=1}^{p} \mathcal{E}_i = \{E \in \mathcal{E} |\ |E| \leq p\}.$$

Since $|\omega(E)| \leq |E|$ for all $E \in \mathcal{E}$, we know that $\widetilde{\omega}(\mathcal{E}_p^*) \subseteq \mathcal{E}_p^*$. Every set $\mathcal{E}_p^*$ is finite and $\widetilde{\omega}$ is injective, thus $\widetilde{\omega}(\mathcal{E}_p^*) = \mathcal{E}_p^*$. Because the sets $\mathcal{E}_{p-1}^*$ and $\mathcal{E}_p$ are disjoint and $\widetilde{\omega}$ is injective, the sets $\widetilde{\omega}(\mathcal{E}_{p-1}^*) = \mathcal{E}_{p-1}^*$ and $\widetilde{\omega}(\mathcal{E}_p)$ are disjoint. Thus $\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p^* \setminus \mathcal{E}_{p-1}^* = \mathcal{E}_p$. The sets $\mathcal{E}_\infty$ and $\mathcal{E}_p$ are disjoint for every $p \in \mathbf{N}$ and $\widetilde{\omega}$ is injective, thus $\widetilde{\omega}(\mathcal{E}_\infty) \subseteq \mathcal{E}_\infty$. □

It is important to realize that the proof of Theorem 5.3 uses the fact that the set $\mathbf{F}$ is finite. One of the consequences of Theorem 5.3 is the next theorem. It tells us that the all the information about injectivity and surjectivity of a translation invariant operator ω on the signal space is contained in $\widetilde{\omega}$. A second application of the theorem will be described in the next section.

Theorem 5.4. *Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a translation invariant operator. Then the following statements hold:*

1. *ω is injective if and only if $\widetilde{\omega}$ is injective.*
2. *ω is surjective if and only if $\widetilde{\omega}$ is surjective.*

Proof of 1. Suppose that ω is injective. Any injective function maps two disjoint subsets of its domain to two disjoint subsets of its range. So ω maps two distinct equivalence classes E and E' to two distinct equivalence classes $\omega(E)$ and $\omega(E')$. This means that $\widetilde{\omega}(E) \neq \widetilde{\omega}(E')$ if $E \neq E'$.

Conversely, suppose that $\widetilde{\omega}$ is injective. We consider a pair of signals x and x' with $\omega(x) = \omega(x')$. We first show that both signals are in the same equivalence class. Recall that the collection of equivalence classes $\mathcal{E}$ forms a partition of the signal space, so both x and x' are a member of some equivalence

class. Say $x \in E$ and $x' \in E'$. Since $\omega(x) = \omega(x')$, we know $\omega(E) = \omega(E')$. Since $\widetilde{\omega}$ is injective, we must have $E = E'$.

We will now show that $x = x'$. To that end, we distinguish between two cases. The first case is that $x, x' \in E \in \mathcal{E}_p$ for some $p \in \mathbf{N}$. We learn from Theorem 5.3 that $\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p$. Hence $|\omega(E)| = |E| < \infty$. So $\omega|_E$ is injective and $x = x'$. The second case is $x, x' \in E \in \mathcal{E}_\infty$. Since x and x' are in the same equivalence class, there exists a $t \in \mathbf{Z}$ with $x' = \tau_t(x)$. It follows that $\omega(x) = \tau_t(\omega(x))$. By Theorem 5.3, $\widetilde{\omega}(\mathcal{E}_\infty) \subseteq \mathcal{E}_\infty$. This means that $\omega(x)$ is aperiodic. We conclude that $t = 0$ and $x = x'$. □

Proof of 2. Suppose that ω is surjective and choose any $F \in \mathcal{E}$. Now choose some element $y \in F$. Since ω is surjective, there exists an $x \in \mathbf{F}^{\mathbf{Z}}$ such that $\omega(x) = y$. This x belongs to some equivalence class, say E. We know that $\omega(E) = F$, thus $\widetilde{\omega}(E) = F$.

Conversely, suppose that $\widetilde{\omega}$ is surjective and choose any $y \in \mathbf{F}^{\mathbf{Z}}$. This signal y belongs to some equivalence class, say F. Since $\widetilde{\omega}$ is surjective, there exists an equivalence class E such that $\widetilde{\omega}(E) = F$. It follows that there exists an $x \in E$ such that $\omega(x) = y$. □

In general, a function is injective if and only if it has (at least) one left inverse. Similarly, a function is surjective if and only if it has (at least) one right inverse. The latter statement is equivalent to the Axiom of Choice. In the case of translation invariant operators on $\mathbf{F}^{\mathbf{Z}}$, the following theorem states when injective and surjective operators have *translation invariant* left and right inverses, respectively.

Theorem 5.5. *Let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be a translation invariant operator. Then the following statements hold:*

1. *If ω is injective then it has a translation invariant left inverse.*
2. *If ω is surjective then it has a translation invariant right inverse if and only if $\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p$ for all $p \in \mathbf{N}$ and $\mathcal{E}_\infty \subseteq \widetilde{\omega}(\mathcal{E}_\infty)$.*

Proof. To prove the first statement, let $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ be an injective translation invariant operator. We can restrict the codomain of ω to its image and obtain $\omega_* : \mathbf{F}^{\mathbf{Z}} \to \omega(\mathbf{F}^{\mathbf{Z}})$. This is a (translation invariant) bijective function and we will refer to its inverse by $\omega_*^{-1} : \omega(\mathbf{F}^{\mathbf{Z}}) \to \mathbf{F}^{\mathbf{Z}}$, which is translation invariant as well. We now define the operator $\psi : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ by

$$\psi(y) = \begin{cases} \omega_*^{-1}(y) & \text{if } y \in \omega(\mathbf{F}^{\mathbf{Z}}) \\ y & \text{if } y \notin \omega(\mathbf{F}^{\mathbf{Z}}). \end{cases}$$

It is clear that $\psi \circ \omega$ is the identity operator, so ψ is a left inverse of ω. Moreover, it can be easily verified that ψ is translation invariant.

To prove the second statement, we assume that $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ is a surjective translation invariant operator. Suppose in addition that ω has a translation invariant right inverse $\psi : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$. So $\omega \circ \psi$ is the identity operator on $\mathbf{F}^{\mathbf{Z}}$. Moreover $\widetilde{\omega} \circ \widetilde{\psi}$ is the identity operator on $\mathcal{E}$. Since $\widetilde{\psi}$ has a left inverse, namely $\widetilde{\omega}$, it is injective. Thus it follows from Theorem 5.3 that $\widetilde{\psi}(\mathcal{E}_p) = \mathcal{E}_p$ for all $p \in \mathbf{N}$. We conclude that $\mathcal{E}_p = \widetilde{\omega}(\widetilde{\psi}(\mathcal{E}_p)) = \widetilde{\omega}(\mathcal{E}_p)$ for all $p \in \mathbf{N}$. Since $\widetilde{\omega}$ is surjective, we also have $\mathcal{E}_\infty \subseteq \widetilde{\omega}(\mathcal{E}_\infty)$.

Conversely, suppose in addition to that fact that $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ is a surjective translation invariant operator, that $\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p$ for all $p \in \mathbf{N}$ and $\mathcal{E}_\infty \subseteq \widetilde{\omega}(\mathcal{E}_\infty)$. We must show that ω has a translation invariant right inverse. We define an operator $\psi : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$ by first specifying ψ on the periodic signals and then specifying ψ on every aperiodic equivalence class $E \in \mathcal{E}_\infty$. For ease of notation, let us define the set of p-periodic signals $P_p := \bigcup \mathcal{E}_p$ and the set of all periodic signals $P := \bigcup_{p \in \mathbf{N}} P_p$.

Since $\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p$ for all $p \in \mathbf{N}$, we know that $\omega(P_p) = P_p$ for all $p \in \mathbf{N}$. The set of signals P_p is finite, so ω is a one-to-one-correspondence between P_p and P_p. Consequently, since $\{P_p\}_{p \in \mathbf{N}}$ is a partition of P, ω is also a one-to-one-correspondence between P and P. This allows us to define $\psi|_P := (\omega|_P)^{-1}$. Now choose any aperiodic equivalence class $E \in \mathcal{E}_\infty$. Since $\widetilde{\omega}(\mathcal{E}_\infty)$ contains $\mathcal{E}_\infty$, there

exists at least one $E^* \in \mathcal{E}_\infty$ such that $\widetilde{\omega}(E^*) = E$. Using the Axiom of Choice, we choose such a set E^*. Since both E^* and E are aperiodic and ω is translation invariant, we know that ω is a one-to-one correspondence between the sets E^* and E. So we can define $\psi|_E := (\omega|_{E^*})^{-1}$. It it clear that ψ thus defined is a right inverse of ω and that ψ is translation invariant. □

We have seen that for any translation invariant bijective operator $\omega : \mathbf{F}^{\mathbf{Z}} \to \mathbf{F}^{\mathbf{Z}}$, we have that

$$\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p, \qquad \forall p \in \mathbf{N}.$$

We can relate this property to the equipartition condition as defined in Section 3. To that end we define the permutation condition.

Definition 5.4. Let A be a nonempty finite subset of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be a function. The function α satisfies the *permutation condition* for a nonempty finite subset B of $\mathbf{Z}$ if

$$\widetilde{\overline{\alpha}}(\mathcal{E}_p) = \mathcal{E}_p, \qquad \forall p \mid c, \tag{5.5}$$

where c is the size of the smallest interval that contains $A + B$.

We immediately see from the definition that if a function α satisfies the permutation condition for a particular set B, it also satisfies the permutation condition for any translate $t + B$ of B. We will prove that the permutation condition implies the equipartition condition and to that end we need the following technical lemma.

Lemma 5.6. *Let $A \subset \mathbf{Z}$ be a finite interval with $a := |A|$ elements. Let $D_a \subset \mathbf{F}^Z$ be the set of p-periodic signals whose period p divides a. Then the mapping*

$$\Phi : D_a \to \mathbf{F}^A, \qquad \Phi(x) := x|_A \tag{5.6}$$

is a one-to-one correspondence between the set D_a and the set $\mathbf{F}^A$.

Proof. We choose two periodic signals $x, y \in \mathbf{F}^{\mathbf{Z}}$, with both periods a divisor of a. Then $\tau_{ka}(x) = x$ and $\tau_{ka}(y) = y$ for all $k \in \mathbf{Z}$. Now we assume that $\Phi(x) = x|_A = y|_A = \Phi(y)$. This implies that $x|_{ka+A} = y|_{ka+A}$ for all $k \in \mathbf{Z}$. Because A is an interval, this means $x = y$ and we have proved that Φ is injective.

To prove that the mapping is surjective, we choose any $u \in \mathbf{F}^A$. We now define $x \in \mathbf{F}^{\mathbf{Z}}$ by $x[ka + i] := u[i]$, for all $i \in A$ and $k \in \mathbf{Z}$. Due to the fact that A is an interval with a elements, x is well defined. We have that $\tau_{ka}(x) = x$ for all $k \in \mathbf{Z}$. Hence x is an q-periodic signal for a certain divisor q of a. By definition of x, we have $\Phi(x) = x|_A = u$, thus Φ is surjective. □

Theorem 5.7. *Let A and B be two nonempty finite subsets of $\mathbf{Z}$ and let $\alpha : \mathbf{F}^A \to \mathbf{F}$ be a function. If α satisfies the permutation condition for B then α satisfies the equipartition condition for B.*

Proof. The first three steps of this proof are very similar. Their general idea is as follows. Suppose we have two sets X and Y and a bijective mapping $f : X \to Y$. If $\{X_i\}_{i \in I}$ is a partition of X with subsets X_i of equal cardinality, then $\{f(X_i)\}_{i \in I}$ is a partition of Y with equally sized subsets.

We first construct a set and a partition of that set with subsets of equal cardinality. Observe that, since A and B are both finite, $A + B$ is finite. Let C the smallest interval that contains $A + B$. The interval C is finite as well and we define $c := |C|$. Now we choose an integer $t \in A$. Since the Minkowski addition of A and B is contained in C, we have that $B \subseteq t + C$. Let $\{W_v\}_{v \in \mathbf{F}^B}$ be the collection of subsets of $\mathbf{F}^{t+C}$ defined by

$$W_v := \left\{ w \in \mathbf{F}^{t+C} \,\middle|\, w|_B = v \right\}, \qquad v \in \mathbf{F}^B.$$

This collection of sets forms a partition of $\mathbf{F}^{t+C}$. Moreover, all the sets in the collection have the same cardinality.

Let $D_c \subset \mathbf{F}^Z$ be the set of p-periodic signals whose period p divides c. Consider the mapping $\Phi_{t+C} : D_c \to \mathbf{F}^{t+C}$ defined by $\Phi_{t+C}(y) := y|_{t+C}$. Lemma 5.6 shows that this mapping is a one-to-one correspondence. Hence we can use Φ_{t+C} to construct the partition $\{\Phi_{t+C}^{-1}(W_v)\}_{v\in\mathbf{F}^B}$ of D_c from the partition $\{W_v\}_{v\in\mathbf{F}^B}$ of $\mathbf{F}^{t+C}$. In addition, the sets in this partition all have the same cardinality. Observe that, if we define

$$Y_v := \big\{y \in D_c \big|\ y|_B = v\big\}, \qquad v \in \mathbf{F}^B,$$

we have $\Phi_{t+C}(Y_v) = W_v$. Hence $\{Y_v\}_{v\in\mathbf{F}^B}$ is a partition of D_c with equally sized parts.

Since α satisfies the permutation condition for B, we have that $\overline{\alpha}(D_c) = D_c$. The set of signals D_c is finite, so the operator $\phi : D_c \to D_c$ defined by $\phi(x) = \overline{\alpha}(x)$ is bijective. We use ϕ to create the partition $\{\phi^{-1}(Y_v)\}_{v\in\mathbf{F}^B}$ of D_c. The sets in this partition have equal cardinality as well. Now we define

$$X_v := \big\{x \in D_c \big|\ \overline{\alpha}(x)|_B = v\big\}, \qquad v \in \mathbf{F}^B.$$

Since $\phi(X_v) = Y_v$, the collection of sets $\{X_v\}_{v\in\mathbf{F}^B}$ is a partition of D_c with the property that all the sets in the collection have the same cardinality.

Now consider the mapping $\Phi_C : D_c \to \mathbf{F}^C$ defined by $\Phi_C(x) := x|_C$. Lemma 5.6 proves that this mapping is bijective. So we can use Φ_C to form the partition $\{\Phi_C(X_v)\}_{v\in\mathbf{F}^B}$ of $\mathbf{F}^C$ from the partition $\{X_v\}_{v\in\mathbf{F}^B}$ of D_c. Again, the sets in this partition all have the same cardinality. We proceed by defining

$$U_v := \big\{u \in \mathbf{F}^C \big|\ \alpha^B(u|_{A+B}) = v\big\}, \qquad v \in \mathbf{F}^B.$$

Because $\overline{\alpha}(x)|_B = \alpha^B(x|_{A+B})$ (Equation (3.14)), we have $\Phi_C(X_v) = U_v$. Consequently, $\{U_v\}_{v\in\mathbf{F}^B}$ is a partition of F^C with equally sized parts.

For the final step, we define the collection of sets $\{U'_v\}_{v\in\mathbf{F}^B}$ by

$$U'_v := \big\{u' \in \mathbf{F}^{A+B} \big|\ \alpha^B(u') = v\big\}, \qquad v \in \mathbf{F}^B.$$

Observe that $u \in U_v$ if and only if $u|_{A+B} \in U'_v$. In addition, for any $u' \in \mathbf{F}^{A+B}$, the number of elements of $\{u \in \mathbf{F}^C|\ u|_{A+B} = u'\}$ is $|\mathbf{F}^C|$ divided by $|\mathbf{F}^{A+B}|$. This number, which we will denote by d, does not depend on u. We conclude that $d\,|U'_v| = |U_v|$ for all $v \in \mathbf{F}^B$. As a result every set in the collection $\{U'_v\}_{v\in\mathbf{F}^B}$ has the same cardinality. In other words, we have proved that α satisfies the equipartition condition for B. □

6. Enumerating Translation Invariant Operators

With the theory developed so far, it is not feasible to enumerate translation invariant bijective operators on $\mathbf{F}^{\mathbf{Z}}$ directly. However, this section will establish some upper bounds for their number. Both Corollary 3.6 and Theorem 5.3 will be used for accomplishing this. Furthermore, the computation of upper bounds suggests a method for the construction of translation invariant bijective operators.

We start by fixing some *finite* subset A of $\mathbf{Z}$ and consider only translation invariant operators with support included in A. For this section we define four sets of operators.

Definition 6.1. Let A be a nonempty finite subset of $\mathbf{Z}$.

1. The set $T(A)$ is the set of translation invariant operators on $\mathbf{F}^{\mathbf{Z}}$ with support included in A:

$$T(A) := \big\{\overline{\alpha} \big|\ \alpha \in \mathrm{Fun}\big(\mathbf{F}^A, \mathbf{F}\big)\big\}. \tag{6.1}$$

2. The set $T_{\mathrm{e}}(A)$ consists of those operators $\overline{\alpha} \in T(A)$ for which $\alpha \in \mathrm{Fun}(\mathbf{F}^A, \mathbf{F})$ satisfies the equipartition condition for $\{0\}$.

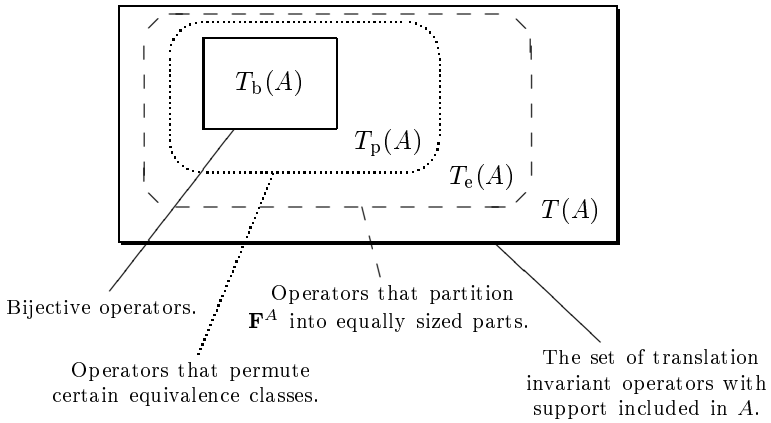


Figure 17: Venn diagram of the sets $T(A)$, $T_{\mathrm{e}}(A)$, $T_{\mathrm{p}}(A)$ and $T_{\mathrm{b}}(A)$.

3. The set $T_{\mathrm{p}}(A)$ contains those operators $\overline{\alpha} \in T(A)$ for which $\alpha \in \mathrm{Fun}(\mathbf{F}^A, \mathbf{F})$ satisfies the permutation condition for $\{0\}$.

4. The set $T_{\mathrm{b}}(A)$ contains the bijective elements of $T(A)$.

We are primarily interested in the set $T_{\mathrm{b}}(A)$. We defined the sets $T_{\mathrm{e}}(A)$ and $T_{\mathrm{p}}(A)$ simply because they both contain $T_{\mathrm{b}}(A)$ and we can count them. Indeed, Corollary 3.6 shows that $T_{\mathrm{b}}(A) \subseteq T_{\mathrm{e}}(A)$ and Theorem 5.3 shows that $T_{\mathrm{b}}(A) \subseteq T_{\mathrm{p}}(A)$. Furthermore, Theorem 5.7 learns that $T_{\mathrm{p}}(A) \subseteq T_{\mathrm{e}}(A)$. We conclude that

$$T_{\mathrm{b}}(A) \subseteq T_{\mathrm{p}}(A) \subseteq T_{\mathrm{e}}(A) \subseteq T(A), \tag{6.2}$$

which is depicted in Figure 17.

6.1 Enumerations
It follows Equation (6.2) that

$$|T_{\mathrm{b}}(A)| \leq |T_{\mathrm{p}}(A)| \leq |T_{\mathrm{e}}(A)| \leq |T(A)|. \tag{6.3}$$

Thus $|T_{\mathrm{p}}(A)|$ gives us a better upper bound for the number of translation invariant bijective operators, i.e. $|T_{\mathrm{b}}(A)|$, than $|T_{\mathrm{e}}(A)|$. However, we can only calculate $|T_{\mathrm{p}}(A)|$ in case A is an interval. So if A is not an interval, we can use $|T_{\mathrm{e}}(A)|$. The following three theorems count $T(A)$, $T_{\mathrm{e}}(A)$ and $T_{\mathrm{p}}(A)$.

Theorem 6.1. *Let $A \subset \mathbf{Z}$ be a finite set with $a := |A|$ elements. Then*

$$|T(A)| = |\mathbf{F}|^{|\mathbf{F}|^a}. \tag{6.4}$$

Proof. An obvious bijective mapping between the set of functions $\mathrm{Fun}(\mathbf{F}^A, \mathbf{F})$ and the set of operators $T(A)$ is given by $\alpha \mapsto \overline{\alpha}$. Therefore

$$|T(A)| = |\,\mathrm{Fun}(\mathbf{F}^A, \mathbf{F})| = |\mathbf{F}|^{|\mathbf{F}^A|} = |\mathbf{F}|^{|\mathbf{F}|^a}. \qquad \square$$

Theorem 6.2. *Let $A \subset \mathbf{Z}$ be a finite set with $a := |A|$ elements. Then*

$$|T_{\mathrm{e}}(A)| = \frac{(|\mathbf{F}|^a)!}{((|\mathbf{F}|^{a-1})!)^{|\mathbf{F}|}}. \tag{6.5}$$

p \ $\lvert\mathbf{F}\rvert$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	0	1	3	6	10	15	21
3	0	2	8	20	40	70	112
4	0	3	18	60	150	315	588
5	0	6	48	204	624	1554	3360
6	0	9	116	670	2580	7735	19544
7	0	18	312	2340	11160	39990	117648
8	0	30	810	8160	48750	209790	720300
9	0	56	2184	29120	217000	1119720	4483696
10	0	99	5880	104754	976248	6045837	28245840

Table 2: The number $|\mathcal{E}_p|$ for several sizes of the set $\mathbf{F}$.

Proof. The mapping $\alpha \mapsto \overline{\alpha}$ is a one to one correspondence between the set of functions

$$\{\alpha \in \mathrm{Fun}(\mathbf{F}^A, \mathbf{F}) |\ \alpha \text{ satisfies the equipartition condition for } \{0\}\}$$

and the set of operators $T_{\mathrm{e}}(A)$. The number of such functions α equals the number of ways to partition the domain $\mathbf{F}^A$ into $|\mathbf{F}|$ distinguishable groups with each $|\mathbf{F}|^{a-1}$ elements. It is well know in combinatorial theory that this number is given by the multinomial coefficient

$$\binom{|\mathbf{F}|^a}{|\mathbf{F}|^{a-1},\ |\mathbf{F}|^{a-1},\ \ldots,\ |\mathbf{F}|^{a-1}} = \frac{(|\mathbf{F}|^a)!}{((|\mathbf{F}|^{a-1})!)^{|\mathbf{F}|}}.$$ □

The next theorem counts $T_{\mathrm{p}}(A)$ in case A is an interval. It depends on knowledge of the number of equivalence classes of a certain period. This number is given by the following lemma. See [14] for more information on the classic Möbius function.

Lemma 6.3. *The number of equivalence classes of p-periodic elements of* $\mathbf{F}^{\mathbf{Z}}$ *is given by*

$$|\mathcal{E}_p| = \frac{1}{p} \sum_{i|p} \mu\left(\frac{p}{i}\right) |\mathbf{F}|^i, \tag{6.6}$$

where μ *is the classic Möbius function.*

Proof. Let us denote the number of p-periodic signals in $\mathbf{F}^{\mathbf{Z}}$ by $N(p)$. We have that

$$\sum_{p|n} N(p) = |\mathbf{F}|^n.$$

Therefore we can use classic Möbius inversion to obtain

$$N(p) = \sum_{i|p} \mu\left(\frac{p}{i}\right) |\mathbf{F}|^i.$$

Since $N(p) = p\,|\mathcal{E}_p|$, we have proved the lemma. □

To get some idea of the number of p-periodic equivalence classes, Table 2 evaluates Equation (6.6) for some periods p and several sizes of the set $\mathbf{F}$. In a subsequent example, we will focus on the two channel binary case, where

$$\mathbf{F} = \big\{(0,0),\ (0,1),\ (1,0),\ (1,1)\big\}.$$

So pay special attention to the column $|\mathbf{F}| = 4$.

Theorem 6.4. *Let $A \subset \mathbf{Z}$ be a finite interval with $a := |A|$ elements. Then*

$$|T_{\mathrm{p}}(A)| = \prod_{p|a} |\mathcal{E}_p|!\, p^{|\mathcal{E}_p|}. \tag{6.7}$$

Proof. Recall that $T_{\mathrm{p}}(A)$ is the set of operators $\overline{\alpha}$ with $\alpha \in \mathrm{Fun}(\mathbf{F}^A, \mathbf{F})$ that satisfy

$$\widetilde{\overline{\alpha}}(\mathcal{E}_p) = \mathcal{E}_p, \qquad \forall p \mid a.$$

For convenience, we define $D_a := \bigcup_{p|a} \bigcup \mathcal{E}_p$ as the set of all p-periodic signals with $p \mid a$. In addition we let $\Delta(A)$ be the set of all translation invariant operators $\delta : D_a \to D_a$ that satisfy

$$\widetilde{\delta}(\mathcal{E}_p) = \mathcal{E}_p, \qquad \forall p \mid a.$$

We claim that $T_{\mathrm{p}}(A)$ and $\Delta(A)$ have the same cardinality. We will prove this by demonstrating a bijective mapping between the two sets.

Let us define $\Psi : T_{\mathrm{p}}(A) \to \Delta(A)$ by $\Psi(\omega) = \omega|_{D_a}$. We have for each $\omega \in T_{\mathrm{p}}(A)$ that $\omega|_{D_a} \in \Delta(A)$, so Ψ is well defined. First, we show that Ψ is surjective. Remember that Lemma 5.6 states that $\Phi : D_a \to \mathbf{F}^A$ defined by $\Phi(x) := x|_A$ is bijective. We choose any $\delta \in \Delta(A)$ and define $\alpha : \mathbf{F}^A \to \mathbf{F}$ by $\alpha(u) := \delta(\Phi^{-1}(u))[0]$. For all $x \in D_a$ we have

$$\overline{\alpha}(x)[0] = \alpha(x|_A) = \alpha(\Phi(x)) = \delta(\Phi^{-1}(\Phi(x)))[0] = \delta(x)[0].$$

Moreover, because $\overline{\alpha}$ and δ are translation invariant, we have that $\overline{\alpha}(x) = \delta(x)$ for all $x \in D_a$. We conclude that $\overline{\alpha} \in T_{\mathrm{b}}(A)$ and that $\Psi(\overline{\alpha}) = \delta$. Hence Ψ is surjective.

To show that Ψ is injective, we choose a pair $\alpha, \beta \in \mathrm{Fun}(\mathbf{F}^A, \mathbf{F})$ such that $\overline{\alpha}, \overline{\beta} \in T_{\mathrm{b}}(A)$. Suppose that $\Psi(\overline{\alpha}) = \Psi(\overline{\beta})$. Then we have that $\overline{\alpha}(x) = \overline{\beta}(x)$ for all $x \in D_a$. This implies that $\alpha(x|_A) = \beta(x|_A)$ for all $x \in D_a$ and because $\Phi : D_a \to \mathbf{F}^A$ is bijective we have $\alpha(u) = \beta(u)$ for all $u \in \mathbf{F}^A$. So $\alpha = \beta$, which means that Ψ is injective.

We will now count the number of operators in $\Delta(A)$. To facilitate this, we make a partition of $\Delta(A)$ and count the subsets individually. This partition is created by looking at the behavior of the operators in $\Delta(A)$ on the equivalence classes of signals in $\mathcal{D}_a := \bigcup_{p|a} \mathcal{E}_p$. Notice that $\bigcup \mathcal{D}_a$ equals the domain D_a of every operator in $\Delta(A)$. We let Γ be the set of functions $\gamma : \mathcal{D}_a \to \mathcal{D}_a$ that satisfy $\gamma(\mathcal{E}_p) = \mathcal{E}_p$ for all $p \mid a$. For every $\gamma \in \Gamma$, we define the subset $\Delta_\gamma(A)$ of $\Delta(A)$ comprising those operators $\delta \in \Delta(A)$ for which $\widetilde{\delta} = \gamma$. By definition, $\{\Delta_\gamma(A)\}_{\gamma \in \Gamma}$ forms a partition of $\Delta(A)$. Observe that $|\Gamma|$, the number of subsets in this partition, equals $\prod_{p|a} |\mathcal{E}_p|!$.

To count one of the subsets in the partition, we choose a $\gamma \in \Gamma$ and consider an element δ of $\Delta_\gamma(A)$. We know that for every $E \in \mathcal{E}_p$ we have $\delta(E) \in \mathcal{E}_p$. Due to the translation invariance of δ, this means that we have p possibilities for $\delta|_E$. Hence $|\Delta_\gamma(A)| = \prod_{p|a} p^{|\mathcal{E}_p|}$. We see that this number does not depend on γ, so we have

$$|\Delta(A)| = |\Gamma|\, |\Delta_\gamma(A)| = \prod_{p|a} |\mathcal{E}_p|!\, p^{|\mathcal{E}_p|}. \qquad \square$$

As an example, we look at the two channel binary case where

$$\mathbf{F} = \big\{(0,0),\ (0,1),\ (1,0),\ (1,1)\big\}.$$

So $|\mathbf{F}| = 4$. Table 3 lists the cardinality of the sets $T(A)$, $T_{\mathrm{e}}(A)$ and $T_{\mathrm{p}}(A)$ for several sizes of an interval $A \subset \mathbf{Z}$. The values for $|T_{\mathrm{b}}(A)|$ have been calculated by means of a brute force algorithm, with which calculation for $|A| > 2$ are not feasible. This algorithm will be described in Subsection 6.2. The set $\mathbf{F}$ is the Cartesian product of $\mathbf{S} = \{0, 1\}$ with itself and $\mathbf{S}$ can be identified with the binary field. Hence we can check, like we did in Section 4, each operator for linearity. As it turns out, there are

$\lvert A\rvert$	$\lvert T_{\mathrm{b}}(A)\rvert$	$\lvert T_{\mathrm{p}}(A)\rvert$	$\lvert T_{\mathrm{e}}(A)\rvert$	$\lvert T(A)\rvert$
1	24	24	24	256
2	5,904	1,105,920	63,063,000	4,294,967,296
3	-	$2.036{\cdot}10^{29}$	$6.621{\cdot}10^{35}$	$3.403{\cdot}10^{38}$
4	-	$1.223{\cdot}10^{124}$	$3.309{\cdot}10^{150}$	$1.341{\cdot}10^{154}$
5	-	$1.238{\cdot}10^{528}$	$1.001{\cdot}10^{612}$	$3.232{\cdot}10^{616}$
6	-	$4.351{\cdot}10^{2,159}$	$4.226{\cdot}10^{2,460}$	$1.091{\cdot}10^{2,466}$
7	-	$5.121{\cdot}10^{8,848}$	$6.856{\cdot}10^{9,857}$	$1.415{\cdot}10^{9,864}$
8	-	$1.605{\cdot}10^{35,871}$	$2.431{\cdot}10^{39,449}$	$4.014{\cdot}10^{39,456}$
9	-	$1.200{\cdot}10^{145,170}$	$1.965{\cdot}10^{157,818}$	$2.596{\cdot}10^{157,826}$
10	-	$3.418{\cdot}10^{585,678}$	$4.299{\cdot}10^{631,296}$	$4.544{\cdot}10^{631,305}$

Table 3: The cardinality of the sets $T(A)$, $T_{\mathrm{e}}(A)$ and $T_{\mathrm{p}}(A)$ for several sizes of an interval $A \subseteq \mathbf{Z}$ when $\mathbf{F}$ has 4 elements. For $|A| \geq 3$, the numbers are approximations. The cardinality of the set $T_{\mathrm{b}}(A)$ has been calculated by means of a brute force algorithm for the cases where $|A| = 1$ or $|A| = 2$.

substantially less linear operators in $T_{\mathrm{b}}(A)$ in this case. For example, if $|A| = 2$, then 84 out of the 5,904 operators in $T_{\mathrm{b}}(A)$ are linear.

In spite of our inability to count $T_{\mathrm{b}}(A)$ directly, we can prove that $|\mathbf{F}|!$ is a divisor of $|T_{\mathrm{b}}(A)|$. As was observed in Subsection 3.3, the set S of translation invariant bijective operators with support $\{0\}$ is a subgroup of the group of translation invariant bijective operators H. The collection $\{\omega S\}_{\omega \in H}$ of left cosets of S is a partition of H. Moreover, every coset has $|S| = |\mathbf{F}|!$ elements. We can easily verify that $\omega S \subset T_{\mathrm{b}}(A)$ if $\omega \in T_{\mathrm{b}}(A)$. So $T_{\mathrm{b}}(A)$ is the union of a finite number of cosets and hence divisible by $|\mathbf{F}|!$.

6.2 The Generation of Translation Invariant Bijective Operators

So far, we have been concerned with (combinatorial) properties of translation invariant operators. However, finding explicit examples is equally important. We will now describe one method for finding translation invariant bijective operators with support included in a given finite interval $A \subset \mathbf{Z}$ with $a := |A|$ elements. In other words, we are going to generate operators in the set $T_{\mathrm{b}}(A)$. For the sake of brevity, we merely give an outline of the algorithm.

The basic idea comprises two steps: (i) find all operators in the set $T_{\mathrm{p}}(A)$ and (ii) check each operator for bijectivity. So we must implement a loop over all elements of $T_{\mathrm{p}}(A)$ and we need an algorithm to check if a given operator in $T_{\mathrm{p}}(A)$ is bijective. Note that an element $\omega \in T_{\mathrm{p}}(A)$ can be efficiently stored by means of the function $\alpha : \mathbf{F}^A \to \mathbf{F}$ for which $\overline{\alpha} = \omega$.

The loop over all elements of $T_{\mathrm{p}}(A)$ can be implemented by using the idea of the proof of Theorem 6.4. Using the notation of this proof: we can create all the elements of $\Delta(A)$ and then use Ψ^{-1} to obtain the corresponding elements of $T_{\mathrm{p}}(A)$. This is feasible, since all the operators in $\Delta(A)$ have a finite domain.

An element $\omega \in T_{\mathrm{p}}(A)$ will be tested for bijectivity in two steps. The first step involves the permutation condition. Since $\omega \in T_{\mathrm{p}}(A)$ and A is an interval, we know that

$$\widetilde{\omega}(\mathcal{E}_p) = \mathcal{E}_p \qquad (*)$$

for all $p \mid a$. We can also test this condition for other values of p, say for all $1 \leq p \leq p_{\max}$ with $p \nmid a$, a procedure which we will dub '`PermutesEp?`$(\omega, p_{\max})$'. For a certain value of p, such a test would require $|\mathcal{E}_p|$ evaluations of ω. If ω fails condition $(*)$ for any p, we know that ω is not bijective. However if ω does satisfies $(*)$ for all $1 \leq p \leq p_{\max}$, then ω might be bijective. In such a case we have to take a second step.

Algorithm 1 Generating operators in the set $T_{\mathrm{b}}(A)$.

```
for all ω ∈ T_p(A) do
  if PermutesEp?(ω, p_max) then
    if HasInverse?(ω, B) then
      AddToBijectiveList!(ω)
    else
      AddToUnknownList!(ω)
    end if
  end if
end for
```

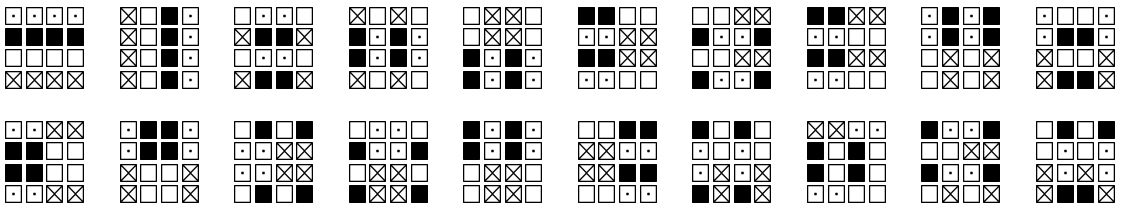


Figure 18: Plots of twenty functions $\alpha_j : \mathbf{F}^{\{0,1\}} \to \mathbf{F}$. Each operator $\overline{\alpha_j}$ is bijective and $\overline{\alpha_j}^{-1}$ has a support that is included in $\{-1, 0\}$. In each of the plots, the horizontal axis is used for the value of $u[0]$ and the vertical axis is used for the value of $u[1]$ ($u \in \mathbf{F}^{\{0,1\}}$). The symbols ⊡, ■, □ and ⊠ are used to denote the value of α_j at u.

The second step tries to find the inverse of ω. The idea is to choose a set $B \subset \mathbf{Z}$ and then verify if there exists a function $\beta : \mathbf{F}^B \to \mathbf{F}$ such that $\overline{\beta} = \omega^{-1}$. A candidate for such a function β can be found by observing that $\beta(\alpha^B(u)) = u[0]$ for all $u \in \mathbf{F}^{A+B}$. It must then be verified that $\alpha(\beta^A(v)) = v[0]$ for all $v \in \mathbf{F}^{A+B}$. This procedure, which we dub '`HasInverse?`(ω, B)', will find the inverse of a bijective ω if the support of ω^{-1} is included in B. We learn from Theorem 3.7, that a set B which has $-A$ as a subset is a good candidate. A problem is, that if we do not find an inverse, we do not know whether ω is bijective or not. It might be bijective and have a support that is larger that B, or it might not be bijective. However, for the case that $|\mathbf{F}| = 4$ and $A = \{0, 1\}$, it turns out that every ω that satisfies `PermutesEp?`$(\omega, 4)$ is bijective and has an inverse with support included in the relatively small set $\{-3, -2, -1, 0, 1, 2\}$. So this case allows us to find all translation invariant bijective operators in the set $T_{\mathrm{b}}(A)$. Algorithm 1 summarizes the operator generating algorithm.

As an example, we consider the case where $A = \{0, 1\}$ and $\mathbf{F}$ has four elements. We use the algorithm to find functions $\alpha : \mathbf{F}^A \to \mathbf{F}$ for which $\overline{\alpha}$ is bijective. As we have seen (Table 3), there exist 5,904 such functions. To restrict ourselves, we look only for those functions α for which the inverse of $\overline{\alpha}$ has a support included in $B = -A = \{-1, 0\}$. The number of such functions is 480. Twenty of these, $\{\alpha_j\}_{1 \le j \le 20}$, are depicted by the twenty plots in Figure 18. The remaining functions can be obtained by permuting the four different function values of each function α_j. There are $4! = 24$ different permutations on $\mathbf{F}$ which we can denote by $\{\sigma_k\}_{1 \le k \le 24}$. So $\{\sigma_k \circ \alpha_j\}_{1 \le j \le 20, 1 \le k \le 24}$ forms the complete set of 480.

A major disadvantage of this algorithm to generate operators in $T_{\mathrm{b}}(A)$ is its time complexity. Even if we assume that the test for bijectivity is a constant time operation, the complexity has the same order as the number of elements in $T_{\mathrm{p}}(A)$. Experimental results (see Table 3) show that this number is substantially higher than the number of elements of $T_{\mathrm{b}}(A)$ itself. Given $f := |\mathbf{F}|$ and $a := |A|$, the

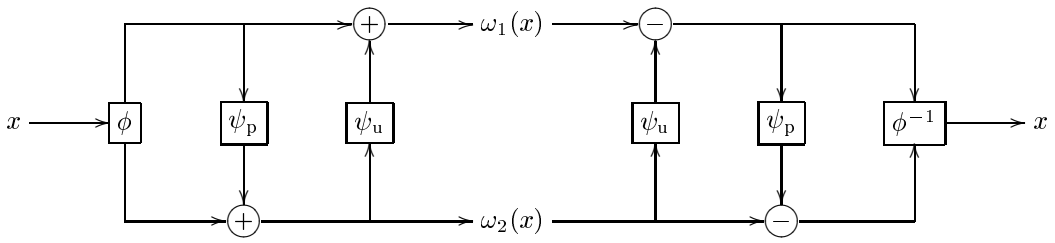


Figure 19: The construction of a translation invariant discrete wavelet transform $\omega : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}} \times \mathbf{S}^{\mathbf{Z}}$ by means of the lifting scheme.

complexity (by Theorem 6.4 and Lemma 6.3) is of order

$$\prod_{p|a} e[f,p]!\, p^{e[f,p]}, \tag{6.8}$$

where $e[f,p] = \frac{1}{p}\sum_{i|p} \mu(\frac{p}{i}) f^i$. In case a is prime, Equation (6.8) equals

$$f!\, \left(\frac{f^a - f}{a}\right)!\, a^{\left(\frac{f^a - f}{a}\right)}, \tag{6.9}$$

so it is obvious that the time complexity grows extremely fast when f or a grow. This makes the algorithm only suitable for very small values of f and a. Fortunately, there are other ways of creating explicit examples of translation invariant bijective operators with finite support. One method, composition, was already discussed in Subsection 3.2. Another method is using Sweldens' lifting scheme [4].

To understand how the lifting scheme can be used to construct wavelet transforms, we examine the construction of a translation invariant discrete wavelet transform $\omega : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}} \times \mathbf{S}^{\mathbf{Z}}$. The construction is shown in Figure 19. The pair of operators $+ : \mathbf{S}^{\mathbf{Z}} \times \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ and $- : \mathbf{S}^{\mathbf{Z}} \times \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ have the property that

$$(x+y) - y = x \quad \text{and} \quad (x-y) + y = x, \qquad \forall x, y \in \mathbf{S}^{\mathbf{Z}}. \tag{6.10}$$

The first equation guarantees that ω will be injective and the second equation is to guarantee that ω will be surjective. To ensure that the constructed transform will be translation invariant, we demand that these two operators are also translation invariant in the sense that

$$\tau_t(x) + \tau_t(y) = \tau_t(x+y) \quad \text{and} \quad \tau_t(x) - \tau_t(y) = \tau_t(x-y), \qquad \forall x, y \in \mathbf{S}^{\mathbf{Z}}, \quad \forall t \in \mathbf{Z}. \tag{6.11}$$

The operator $\phi : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}} \times \mathbf{S}^{\mathbf{Z}}$ is an initial wavelet transform. It should be translation invariant as well. Usually, ϕ is defined as the so called lazy wavelet transform which splits a signal into its odd and even samples. It is defined by $\phi := (\phi_{\mathrm{e}}, \phi_{\mathrm{o}})$, where

$$\phi_{\mathrm{e}}(x)[i] := x[2i], \tag{6.12}$$
$$\phi_{\mathrm{o}}(x)[i] := x[2i+1]. \tag{6.13}$$

The operators $\psi_{\mathrm{p}} : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ and $\psi_{\mathrm{u}} : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}}$ are the so called prediction and update operators. To make sure that ω is translation invariant, we demand that these operators are translation invariant as well. Note that it is *not* necessary that ψ_{p} or ψ_{u} is bijective. The application of an prediction or update operator to one side and then adding the result to the other side is called a lifting step.

The operator $\omega : \mathbf{S}^{\mathbf{Z}} \to \mathbf{S}^{\mathbf{Z}} \times \mathbf{S}^{\mathbf{Z}}$ is now constructed as follows:

$$\omega_1(x) = \phi_{\mathrm{e}}(x) + \psi_{\mathrm{u}}\big(\phi_{\mathrm{o}}(x) + \psi_{\mathrm{p}}(\phi_{\mathrm{e}}(x))\big), \tag{6.14}$$

$$\omega_2(x) = \phi_{\mathrm{o}}(x) + \psi_{\mathrm{p}}(\phi_{\mathrm{e}}(x)). \tag{6.15}$$

It can be verified that ω is bijective and translation invariant; its inverse is given by

$$\omega^{-1}(y_1, y_2) = \phi^{-1}\Big(y_1 - \psi_{\mathrm{u}}(y_2),\ y_2 - \psi_{\mathrm{p}}\big(y_1 - \psi_{\mathrm{u}}(y_2)\big)\Big). \tag{6.16}$$

Note that any number of lifting steps may be added to this scheme; the resulting operator ω will remain bijective and translation invariant.

We see that it is quite easy to construct translation invariant discrete wavelet transforms over a finite set $\mathbf{S}$ by using the lifting scheme. It is worth further study to investigate how the scheme can be applied to construct discrete wavelet transforms with certain desirable properties. See [8] for some examples in this direction. As was said in the introduction of this paper, it is an open question if the lifting scheme in this form (with ϕ being the lazy wavelet) can be used to create all discrete wavelet transforms.

7. Conclusion

We have defined an extension of the discrete wavelet transform that is translation invariant and works on signals that are functions from the integers into any finite set. This is potentially useful since a large quantity of real world signals are finite valued and the defined transform can be calculated very time efficiently, using only discrete arithmetic.

The discrete wavelet transform over finite sets includes nonlinear transforms and is as such a generalization of previous work of other authors that defined a linear discrete wavelet transform over finite commutative rings. We have seen that, by using the more general definition, the number of transforms increases drastically thus giving more freedom in choosing a particular transform.

On the down side, no efficient method for systematically finding explicit examples of discrete wavelet transforms over finite sets was presented. The crude algorithm given is very time consuming, usable only for finding simple (but nontrivial) transforms.

Our treatment of the subject was of a rather theoretical nature. Starting from the most general definition, we derived some general properties of discrete wavelet transforms over finite sets. We especially investigated means to recognize bijective transforms. We found that looking at the behavior of transforms on translation invariant equivalence classes of signals was useful in that respect. In addition, an effort was made to enumerate the set of transforms with finite support, which resulted in an upper bound.

Although the paper is restricted to the definition of the discrete wavelet transform over finite sets to transforms on one dimensional signals only, generalization to signals defined on any finite Cartesian product of the integers, e.g. images, is straightforward. In addition most of the results for the one dimensional case, may be easily extended to the higher dimensional case. For images, examples of transforms over finite sets can be found by constructing a tensor-like product of two one dimensional transforms. The paper explains this in detail in an example.

The paper did not investigate possible applications of the discrete wavelet transform over finite sets. However, some possibilities quickly jump to mind. Since the transform can be calculated extremely time efficiently, it may be useful for real time systems that rely on fast computations. Also, the gained freedom in choosing a particular transform suggests possible application of the discrete wavelet transform over finite sets to compression using transform coding.

References

1. Giuseppe Caire, Robert L. Grossman, and H. Vincent Poor. Wavelet transforms associated with finite cyclic groups. *IEEE Transactions on Information Theory*, 39(4):1157–1166, July 1993.

2. Mitchell D. Swanson and Ahmed H. Tewfik. A binary wavelet decomposition of binary images. *IEEE Transactions on Image Processing*, 5(12):1637–1650, December 1996.
3. A. Klappenecker, F.U. May, and A. Nückel. Lossless image compression using wavelets over finite rings and related architectures. In Akram Aldroubi, Andrew F. Laine, and Michael A. Unser, editors, *Wavelet Applications in Signal and Image Processing V*, volume 3169, pages 139–147. SPIE, October 1997.
4. W. Sweldens. The lifting scheme: A construction of second generation wavelets. *SIAM Journal on Mathematical Analysis*, 29(2):511–546, 1997.
5. I. Daubechies and W. Sweldens. Factoring wavelet transforms into lifting steps. *Journal of Fourier Analysis and Applications*, 4(3):245–267, 1998.
6. Andreas Klappenecker, Matthias Holschneider, and Kristin Flornes. Two-channel perfect reconstruction FIR filter banks over commutative rings. *Applied and Computational Harmonic Analysis*, 8:113–121, 2000.
7. R. Calderbank, I. Daubechies, W. Sweldens, and B.-L. Yeo. Wavelet transforms that map integers to integers. *Applied and Computational Harmonic Analysis*, 5(3):332–369, 1998.
8. Henk J.A.M. Heijmans and John Goutsias. Nonlinear multiresolution signal decomposition schemes–Part II: Morphological wavelets. *IEEE Transactions on Image Processing*, 9(11):1897–1913, November 2000.
9. O.N. Gerek, M.N. Gürcan, and A.E. Çetin. Binary morphological subband decomposition for image coding. In *International Symposium on Time-Frequency and Time-Scale Analysis*. IEEE, 1996.
10. Ömer N. Gerek, A. Enis Çetin, Ahmed Tewfik, and Volkan Atalay. Subband domain coding of binary textual images for document archiving. *IEEE Transactions on Image Processing*, 8(10):1438–1446, October 1999.
11. Saunders MacLane and Garrett Birkhoff. *Algebra*. MacMillan, New York, second edition, 1979.
12. Joseph J. Rothman. *An Introduction to the Theory of Groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.
13. Stéphane Mallat. *A Wavelet Tour of Signal Processing*. Academic Press, San Diego, second edition, 1999.
14. Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.