Two-Channel Perfect Reconstruction Filter Banks over Commutative Rings

Andreas Klappenecker, Matthias Holschneider, and Kristin Flornes

Universität Karlsruhe, IAKS,
Am Fasanengarten 5,
D-76128 Karlsruhe, Germany.
klappi@ira.uka.de

CNRS CPT Luminy, Case 907,
F-13288 Marseille, France.
Matthias.Holschneider
@cpt.univ-mrs.fr

Department of Math. Sciences,
Norwegian University
of Science and Technology,
N-7034 Trondheim, Norway.
flornes@math.ntnu.no

October 6, 1997

List of Symbols

$\mathbf{C}$	complex numbers
$\mathbf{N}$	natural numbers
$\mathbf{Q}$	rational numbers
$\mathbf{R}$	real numbers
$\mathbf{Z}$	integers
$\mathbf{Z}/N\mathbf{Z}$	integers modulo N
$\mathrm{GF}(q)$	finite field with q elements
A	commutative ring with identity
$A[z, z^{-1}]$	Laurent polynomial ring over the commutative ring A
$U(A)$	group of units of the ring A
M	module of finitely supported sequences with values in A
$\mathrm{supp} f$	support of the function or sequence f
$\mathrm{Aut}_A(M)$	group of A-module automorphisms
$\mathrm{GL}(n, R)$	general linear group over the ring R
$\mathrm{SL}(n, R)$	special linear group over the ring R
$\delta_k(x)$	delta sequence $\delta_k(x) = 1$ for $k = x$, $\delta_k(x) = 0$ otherwise
$[\downarrow 2]$	decimation by two
$[\uparrow 2]$	upsampling operation
$a * b$	convolution of sequences a and b
$\mathrm{ldeg} f$	degree of the Laurent polynomial f
$\mathrm{lc} f$	leading coefficient of the (Laurent) polynomial f
T_n	translation of sequence s: $T_n s(k) = s(k-n)$
P_e	projection of sequence s on subsequence $P_e s = s_e$ with even indices
P_o	projection of sequence s on subsequence $P_o s = s_o$ with odd indices
O_W	local rotation operator (explained in the text)
$O_{W,F}$	local rotation operator for fundamental domain F (explained in the text)
O^F_{spr}	spreading operator (explained in the text)

Running Head: Filter Banks over Commutative Rings

Contact Address:
Andreas Klappenecker
Universität Karlsruhe, IAKS,
Am Fasanengarten 5,
D-76128 Karlsruhe, Germany.
klappi@ira.uka.de

Abstract

We develop a theory of perfect reconstructing filter banks over commutative rings A with identity. The filter bank viewpoint is complemented by interpreting the signals as elements of the free A-module of finitely supported sequences with values in A. It is shown that bases of this module can be obtained by the even translates of the two synthesis filter sequences of a perfect reconstructing filter bank. We associate a group structure with these bases and thereby obtain a parametrization of synthesis filter pairs. It is proved that this parametrization is complete when A is an arbitrary field. As a special case we derive a complete parametrization of biorthogonal real-valued filter pairs. We discuss lifting techniques and their use to reduce the computational complexity of implementations.

1 Introduction

Perfect reconstructing two-channel filter banks were introduced by Mintzer [27] and by Smith and Barnwell [34] in the mid eighties. The connection of wavelets with filter banks was established by Mallat soon afterwards [26]. Since then, a lot of research has been devoted to the structural analysis of orthogonal solutions [10, 16, 29, 30, 41, 42, 44, 51, 52] and biorthogonal solutions [3, 9, 12, 18, 19, 46, 47, 48, 50]. Almost all work was confined to real or complex filter coefficients. For an overview of these results the reader may consult [1, 11, 15, 43, 49]. Several authors started to investigate filter banks with finite field coefficients [5, 17, 28, 31, 32, 35, 36, 37, 40, 47]. The proposed applications of these filter banks include lossless compression of images [17, 35, 36, 37] and multilevel error protection (an error control coding application) [31, 32]. There is also a potential for applications in cryptography.

We treat filter banks over arbitrary fields and even over arbitrary commutative rings. Many results are known in the special case when the filter coefficients are assumed to be real or complex. Often it is fairly easy to generalize these results to other fields of characteristic zero. However, some extra care is necessary when the fields or rings have non-zero characteristic. For example, convenient tools such as modulation matrices are useless when the filter coefficients are elements of a field of characteristic two!

Implementations often suggest to consider rings and fields that differ from the real or complex numbers. For example, in integrated circuit implementations it is much more desirable to use fixed-point arithmetic rather than floating point arithmetic regarding costly chip area. A natural choice for fixed-point implementations are filters with dyadic rational or integer coefficients (although this is not the only possibility, cf. [6, 20]). The dyadic rationals and the integers are commutative rings but neither is a field.

A serious disadvantage of filter banks over rings of characteristic zero is that more and more bits are necessary to represent the signal values in successive decomposition steps, a phenomenon known in computer algebra as *intermediate coefficient swell* [45]. This problem is nonexistent for filter banks over finite rings. Examples of such rings are the integers modulo some natural number $\mathbf{Z}/N\mathbf{Z}$ or the finite fields $\mathrm{GF}(q)$.

The preceding discussion shows that it is quite natural to study filter banks over commutative rings in full generality. This includes then as special cases the filter banks over integers $\mathbf{Z}$, over dyadic rationals, over finite fields $\mathrm{GF}(q)$, over integers modulo some natural number $\mathbf{Z}/N\mathbf{Z}$, over algebraic number fields, over polynomial rings, etc. Although this abstract approach has the advantage that we can deal with various different arithmetic situations using a single formulation, we are very well aware of the fact that the language used here might not be familiar to every reader. If this is the case, we suggest to think of vector spaces instead of more general modules. The algebraic terminology used is standard and can be found in almost any treatise on algebra, see for example [2, 25, 33].

The first author [21] and the last two authors [13] worked independently on characterizations of wavelet filters over arbitrary fields. Our approaches were quite different and complemented each other. We decided to join forces and this paper is the compositum of our results. Fortunately, we unified [13] and [21] while both works were in their infancies, leading to the present coherent approach.

This paper is organized as follows. In the next section we fix notations and briefly discuss the analysis and synthesis steps of a two-channel filter bank. It turns out that the perfect reconstruction condition is equivalent to the invertibility of the polyphase matrix, as in the case of biorthogonal filter banks with real coefficients. The module theoretic viewpoint is expounded in §§3 and 4. We show that the even translates of the synthesis filters constitute a basis of the module of all finitely supported signal sequences; this parallels the situation of QMFs with complex coefficients as explained in Holschneider [14]. In §§6 and 7 we derive a parametrization of synthesis filters and prove its completeness for arbitrary fields. We then give some examples in §8. We discuss lifting techniques and their use to reduce the computational complexity of a filter bank implementation in §9.

Since the manuscript of this paper was first circulated, one of us applied the ideas explained here to lossless image compression. Filter banks over the finite ring $\mathbf{Z}/256\mathbf{Z}$ were successfully used to derive particularly area efficient VLSI layouts, cf. [22].

2 Perfect Reconstructing Filter Banks

Let A be a commutative ring with identity. We analyse finitely supported signal sequences with values in A; these signals are elements of the set

$$M = \{f : \mathbf{Z} \to A \mid |\,\mathrm{supp}(f)\,| < \infty\}.$$

The set M can be interpreted as an A-module under componentwise addition and scalar multiplication. Note that M is a *free* A-module with basis $B = \{\,\delta_k \mid k \in \mathbf{Z}\}$ defined by

$$\delta_k(x) = \begin{cases} 1 & \text{if } x = k, \\ 0 & \text{if } x \neq k. \end{cases}$$

The z-transform of a signal $s \in M$ is given by the A-module isomorphism between M and the A-module of Laurent polynomials $A[z, z^{-1}]$, which is induced by the mapping $\delta_k \mapsto z^{-k}$.

Before going any further, we introduce some convenient notation. We denote by $U(A)$ the set of units of the ring A. We will assume throughout that A is non-trivial, i. e., that $0 \neq 1$ holds in A. We write $a * b$ for the convolution of two sequences $a, b \in M$. The sign T_n is used for the translation operation $T_n\, s(k) = s(k - n)$. The projection of a signal onto its even subsequence is given by

$$P_e\, s(k) = \begin{cases} s(k) & \text{for even } k, \\ 0 & \text{otherwise.} \end{cases}$$

The corresponding projection onto the odd subsequence is $P_o := T_{-1} P_e T_1$. Closely related to these projection operations are the decimation operation defined by $[\downarrow 2] s\,(k) = s(2k)$, as well as the upsampling operation given by $[\uparrow 2]\, s(2k) = s(k)$, and $[\uparrow 2]\, s(2k+1) = 0$. Clearly, the projection operation P_e is the composition of decimation followed by upsampling $P_e = [\uparrow 2][\downarrow 2]$.

We also use the language of z-transforms whenever this is convenient. The convolution is given in the z-domain by the product $a(z)b(z)$ in the algebra $A[z, z^{-1}]$. If we write a signal $s(z)$ in its polyphase form $s(z) = s_e(z^2) + z s_o(z^2)$, then the downsampling can be described by $[\downarrow 2]\, s(z) = s_e(z)$. This operation is defined more explicitly by

$$[\downarrow 2]\, z^m = \begin{cases} z^{m/2} & \text{for even } m, \\ 0 & \text{otherwise.} \end{cases}$$

The upsampling operation acts as $[\uparrow 2]\, s(z) = s(z^2)$.

We recall briefly the analysis and synthesis steps of a two-channel filter bank. It turns out that the situation does not differ much from the case of real numbers, except that we avoid formulations such as $P_e\, s(z) = (s(z) + s(-z))/2$, since 2 might not be a unit in the ring A.

Let $s(z)$ be a signal that is written in polyphase form $s(z) = s_e(z^2) + z s_o(z^2)$. In the decomposition step this signal is convolved with the analysis filters $\widetilde{\alpha}, \widetilde{\beta}$ followed by a decimation. We thus obtain the two signals $d_\alpha(z) = [\downarrow 2]\, \widetilde{\alpha}(z)s(z)$ and $d_\beta(z) = [\downarrow 2]\, \widetilde{\beta}(z)s(z)$. If we express the analysis filters as $\widetilde{\alpha}(z) = \widetilde{\alpha}_e(z^2) + z^{-1}\widetilde{\alpha}_o(z^2)$ and $\widetilde{\beta}(z) = \widetilde{\beta}_e(z^2) + z^{-1}\widetilde{\beta}_o(z^2)$, then the decomposition step can be written in polyphase form as follows:

$$(s_e(z), s_o(z))\, H_p(z) = (d_\alpha(z), d_\beta(z)), \quad \text{where} \quad H_p(z) = \begin{pmatrix} \widetilde{\alpha}_e & \widetilde{\beta}_e \\ \widetilde{\alpha}_o & \widetilde{\beta}_o \end{pmatrix}. \tag{1}$$

The two signals d_α, d_β are then upsampled and convolved with the synthesis filters α and β respectively. The reconstruction step thus yields a signal $\hat{s}$ given by

$$\hat{s}(z) = \alpha(z)\, d_\alpha(z^2) + \beta(z)\, d_\beta(z^2). \tag{2}$$

Expressing the synthesis filters α, β and the signal $\hat{s}$ as

$$\alpha(z) = \alpha_e(z^2) + z\alpha_o(z^2), \qquad \beta(z) = \beta_e(z^2) + z\beta_o(z^2), \tag{3}$$

and $\hat{s}(z) = \hat{s}_e(z^2) + z\hat{s}_o(z^2)$, then equation (2) can be written as follows:

$$\begin{aligned} \hat{s}_e(z^2) + z\hat{s}_o(z^2) \quad &= \quad \left(\alpha_e(z^2)d_\alpha(z^2) + \beta_e(z^2)d_\beta(z^2)\right) \\ &\quad +z\left(\alpha_o(z^2)d_\alpha(z^2) + \beta_o(z^2)d_\beta(z^2)\right). \end{aligned}$$

Comparing coefficients on the left and right hand side thus yields the following description of the synthesis filter bank in polyphase form:

$$(d_\alpha(z), d_\beta(z))\, G_p^t(z) = (\hat{s}_e(z), \hat{s}_o(z)), \quad \text{where} \quad G_p(z) = \begin{pmatrix} \alpha_e(z) & \beta_e(z) \\ \alpha_o(z) & \beta_o(z) \end{pmatrix}. \tag{4}$$

If we combine the equations (1) and (4), then the perfect reconstruction requirement $\hat{s}(z) = s(z)$ for all signals $s \in A[z, z^{-1}]$ is equivalent to

$$H_p(z)G_p^t(z) = I.$$

Since $A[z, z^{-1}]$ is a commutative ring, this equation already implies that $H_p(z)$ and $G_p^t(z)$ are elements of $\mathrm{GL}(2, A[z, z^{-1}])$. In particular we have $H_p^{-1}(z) = G_p^t(z)$.

The results of this section may now be summed up as follows:

Proposition 1 *A pair of analysis (or synthesis) filters allows perfect reconstruction in a filter bank if and only if the corresponding polyphase matrix is invertible.*

3 Modules, Filter Pairs, and Groups

The reconstruction filter bank may be regarded as a simple device that allows to construct all sequences of M by means of even shifts of the synthesis filter sequences (α, β). It follows from the perfect reconstruction property that $\{T_{2k}\alpha, T_{2k}\beta \mid k \in \mathbf{Z}\}$ has to be a generating set of M, since otherwise we could not compose all signals $s \in M$. Moreover, we show in the next section that this set is free, hence a basis of the module M. This motivates the following definition:

Definition 2 *A pair of sequences $(\alpha, \beta) \in M \times M$ is called a* filter pair *if and only if the set $\{\alpha(\cdot - 2k), \beta(\cdot - 2k) \mid k \in \mathbf{Z}\}$ is a basis of the A-module M.*

A simple example of such a basis is given by the filter pair (δ_0, δ_1). The next proposition shows how new filter pairs can be obtained from old ones.

Proposition 3 *Let $(\alpha, \beta) \in M \times M$ be a filter pair, and let B be an A-module automorphisms of M that commutes with translations by two, i. e., $BT_2 = T_2B$. Then $(B\alpha, B\beta)$ is again a filter pair.*

Proof. An A-module automorphism maps a basis of M again onto a basis, cf. [33, §36]. Consequently, the set $S = \{B\,T_{2k}\,\alpha, B\,T_{2k}\,\beta \mid k \in \mathbf{Z}\}$ is a basis. Since B commutes with translations by two, the set S can be written in the form $\{T_{2k}B\,\alpha, T_{2k}B\,\beta \mid k \in \mathbf{Z}\}$. Therefore, we can conclude that $(B\alpha, B\beta)$ is indeed a filter pair. □

Lemma 4 *Denote by G the set of A-module automorphisms of M that commute with translations by two. Then G is a subgroup of the group $\mathrm{Aut}_A(M)$ of all A-module automorphisms of M.*

Proof. By definition, $G \subset \mathrm{Aut}_A(M)$. The composition of two automorphisms $B, C \in G$ is again an automorphism commuting with translations by two, hence $BC \in G$. All operators $B \in G$ satisfy $T_2 = B^{-1}BT_2 = B^{-1}T_2B$, which implies $T_2B^{-1} = B^{-1}T_2$. Thereby we have shown that $B^{-1} \in G$ for all $B \in G$. Hence, G is a subgroup of $\mathrm{Aut}_A(M)$, which proves our claim. □

The next theorem tells us that the set of all filter pairs is endowed with a group structure. In fact, the following theorem shows that there exists a canonic bijection between filter pairs and elements of the group G.

Theorem 5 *Denote by G the group of all A-module automorphisms in M that commute with even translations. Let $(\alpha, \beta) \in M \times M$ be a pair of filters, then there exists a unique operator $B \in G$ such that $(\alpha, \beta) = (B\delta_0, B\delta_1)$.*

Proof. An A-module automorphism of M is completely determined by the image of a generating set, cf. [33, §36]. Hence, any A-module automorphism B of the free module M commuting with translations by two is completely determined by its image of (δ_0, δ_1). This proves uniqueness of such an operator. The existence of such an operator is proved by defining B as

$$Bs = \alpha * (P_e\, s) + (T_{-1}\, \beta) * (P_o\, s).$$

This operator is indeed an A-module endomorphism of M that commutes with translations by two. Since B maps the basis $\{T_{2k}\, \delta_0, T_{2k}\, \delta_1 \mid k \in \mathbf{Z}\}$ onto the basis $\{T_{2k}\alpha, T_{2k}\, \beta \mid k \in \mathbf{Z}\}$ of M, the mapping B is bijective, hence an automorphism. Therefore, we can conclude that $B \in G \subset \mathrm{Aut}_A(M)$. □

4 Bases and Filter Banks

The connection between filter pairs and synthesis filters of perfect reconstruction filter banks is established in this section. In the following proposition we show that a pair of *synthesis filters* of a perfect reconstruction filter bank is a filter pair. A similar result was proved for vector spaces by Chen and Vaidyanathan in [8].

Proposition 6 *Denote by α, β the synthesis filters of a perfect reconstruction filter bank. Then $B = \{T_{2k}\alpha, T_{2k}\beta \mid k \in \mathbf{Z}\}$ is a basis of the free A-module M.*

Proof. It is clear that B is a generating set of M. Suppose that B is not free, meaning that there exists a non-trivial linear combination

$$\sum_{k \in \mathbf{Z}} a_k\, T_{2k}\alpha + \sum_{k \in \mathbf{Z}} b_k\, T_{2k}\beta = 0 \tag{5}$$

with a finite number of non-zero coefficients $a_k, b_k \in A$. Writing this relation in the z-domain, we obtain:

$$\sum_{k \in \mathbf{Z}} a_k z^{-2k} \alpha(z) + \sum_{k \in \mathbf{Z}} b_k z^{-2k} \beta(z) = 0. \tag{6}$$

Denote by $a(z), b(z)$ the Laurent polynomials $\sum_{k\in\mathbf{Z}} a_k z^{-k}$ and $\sum_{k\in\mathbf{Z}} b_k z^{-k}$ respectively. Then equation (6) can be written more briefly as $a(z^2)\alpha(z) + b(z^2)\beta(z) = 0$. Using the polyphase decompositions (3), we deduce the following relation:

$$(a(z), b(z)) \begin{pmatrix} \alpha_e(z) & \alpha_o(z) \\ \beta_e(z) & \beta_o(z) \end{pmatrix} = (a(z), b(z))\, G_p^t(z) = (0, 0).$$

Since α, β are synthesis filters of a perfect reconstruction filter bank, the matrix $G_p^t(z)$ is an element of $\mathrm{GL}(2, A[z, z^{-1}])$. Therefore, we can conclude that both $a(z)$ and $b(z)$ are identically zero. Thus there can not exist a non-trivial linear combination (5). □

The next proposition shows the other direction, namely that any *filter pair* in the sense of Definition 2 can be used as a pair of synthesis filters of a perfect reconstructing filter bank.

Proposition 7 *Let (α, β) be a filter pair. Then the corresponding polyphase matrix $G_p(z)$ is an element of* $\mathrm{GL}(2, A[z, z^{-1}])$.

Proof. Suppose that there exists a non-trivial linear combination of the columns of $G_p(z)$:

$$a(z) \begin{pmatrix} \alpha_e(z) \\ \alpha_o(z) \end{pmatrix} + b(z) \begin{pmatrix} \beta_e(z) \\ \beta_o(z) \end{pmatrix} = 0,$$

with non-zero $a(z), b(z) \in A[z, z^{-1}]$. It follows that

$$\left(a(z^2)\alpha_e(z^2) + b(z^2)\beta_e(z^2)\right) + z\left(a(z^2)\alpha_o(z^2) + b(z^2)\beta_o(z^2)\right) = 0,$$

which implies $a(z^2)\alpha(z) + b(z^2)\beta(z) = 0$. Expanding the Laurent polynomials $a(z) = \sum_k a_k z^{-k}$ and $b(z) = \sum_k b_k z^{-k}$, then this equation may be formulated more explicitly as follows:

$$\sum_{k\in\mathbf{Z}} a_k z^{-2k}\alpha(z) + \sum_{k\in\mathbf{Z}} b_k z^{-2k}\beta(z) = 0.$$

This implies that there exists a non-trivial linear combination $\sum_{k\in\mathbf{Z}} a_k T_{2k}\alpha + \sum_{k\in\mathbf{Z}} b_k T_{2k}\beta = 0$, contradicting the basis property of the even translates of α, β. Therefore, the columns of $G_p(z)$ are linearly independent.

Similarly, if the columns of $G_p(z)$ do not generate the free $A[z, z^{-1}]$-module of column vectors, then it follows that there exists a sequence in M that can not be generated by the even translates of (α, β). This is again a contradiction to the basis property of $T_{2k}\alpha, T_{2k}\beta$.

Therefore, we have shown that the columns of $G_p(z)$ are a basis of the free $A[z, z^{-1}]$-module of column vectors with entries in $A[z, z^{-1}]$. It follows that the determinant of $G_p(z)$ is a unit, hence $G_p(z) \in \mathrm{GL}(2, A[z, z^{-1}])$, cf. [33, Korollar 48.4]. This concludes our proof. □

5 Properties of Filter Pairs

In this section we derive several properties of filter pairs that turn out to be useful in later sections. A question of intrinsic interest is the following: Given a filter pair (α, β), what can be said about other filters γ complementing α to a new filter pair (α, γ)? This question was answered by Sweldens [39] and by Vetterli and Herley [48] for filters which have real or complex coefficients. For filter pairs over arbitrary commutative rings A the answer is given by the following proposition:

Proposition 8 (Lifting) *Let $(\alpha, \beta) \in M \times M$ be a filter pair. Then a filter $\gamma \in M$ complements $\alpha \in M$ to a filter pair (α, γ) if and only if it can be written in the following form:*

$$\gamma(z) = \beta(z)\nu(z^2) + \alpha(z)\lambda(z^2),$$

where $\lambda(z)$ is an element of $A[z, z^{-1}]$ and $\nu(z)$ is a unit in $A[z, z^{-1}]$.

Proof. The polyphase matrices of (α, β) and (α, γ) are given by

$$G_p^1(z) = \begin{pmatrix} \alpha_e(z) & \beta_e(z) \\ \alpha_o(z) & \beta_o(z) \end{pmatrix}, \quad G_p^2(z) = \begin{pmatrix} \alpha_e(z) & \gamma_e(z) \\ \alpha_o(z) & \gamma_o(z) \end{pmatrix},$$

where $\alpha(z) = \alpha_e(z^2) + z\alpha_o(z^2)$, $\beta(z) = \beta_e(z^2) + z\beta_o(z^2)$, and $\gamma(z) = \gamma_e(z^2) + z\gamma_o(z^2)$. Suppose that (α, β) and (α, γ) are filter pairs, then it follows from Proposition 7 that $G_p^1(z)$ and $G_p^2(z)$ are elements of the group $\mathrm{GL}(2, A[z, z^{-1}])$. Hence, there exists a matrix $T \in \mathrm{GL}(2, A[z, z^{-1}])$ satisfying $G_p^1(z)T = G_p^2(z)$, namely T is the product of the inverse of $G_p^1(z)$ and of $G_p^2(z)$. This matrix is of the following form:

$$T = \begin{pmatrix} 1 & \lambda(z) \\ 0 & \nu(z) \end{pmatrix}, \qquad \lambda(z) \in A[z, z^{-1}], \quad \nu(z) \in U(A[z, z^{-1}]),$$

as can be verified directly by expanding the expression $T = [G_p^1(z)]^{-1}G_p^2(z)$. Thus, the polyphase components of γ can be written in the form:

$$\gamma_e(z) = \alpha_e(z)\lambda(z) + \beta_e(z)\nu(z), \qquad \gamma_o(z) = \alpha_o(z)\lambda(z) + \beta_o(z)\nu(z).$$

Consequently, $\gamma(z)$ is of the desired form $\gamma(z) = \alpha(z)\lambda(z^2) + \beta(z)\nu(z^2)$.

Conversely, assume that we are given a filter γ of this form. Then the polyphase matrix corresponding to the pair (α, γ) can be factored as follows:

$$G_p^2(z) = \begin{pmatrix} \alpha_e(z) & \gamma_e(z) \\ \alpha_o(z) & \gamma_o(z) \end{pmatrix} = \begin{pmatrix} \alpha_e(z) & \beta_e(z) \\ \alpha_o(z) & \beta_o(z) \end{pmatrix} \begin{pmatrix} 1 & \lambda(z) \\ 0 & \nu(z) \end{pmatrix} = G_p^1(z)T.$$

Since ν is a unit, the determinant of T is a unit, implying $T \in \mathrm{GL}(2, A[z, z^{-1}])$. Therefore, $G_p^2(z)$ is in $\mathrm{GL}(2, A[z, z^{-1}])$, since it is the product of two invertible matrices. It follows from Proposition 6 that (α, γ) is a filter pair. □

A similar reasoning proves the following proposition:

Proposition 9 (Dual-Lifting) *Let $(\alpha, \beta) \in M \times M$ be a filter pair. Then a filter $\gamma \in M$ complements $\beta \in M$ to a filter pair (γ, β) if and only if it can be written in the following form:*

$$\gamma(z) = \alpha(z)\nu(z^2) + \beta(z)\lambda(z^2),$$

where $\lambda(z)$ is an element of $A[z, z^{-1}]$ and $\nu(z)$ is a unit in $A[z, z^{-1}]$.

Note that this is equivalent to say that the polyphase matrix of (γ, β) factors as follows:

$$\begin{pmatrix} \gamma_e(z) & \beta_e(z) \\ \gamma_o(z) & \beta_o(z) \end{pmatrix} = \begin{pmatrix} \alpha_e(z) & \beta_e(z) \\ \alpha_o(z) & \beta_o(z) \end{pmatrix} \begin{pmatrix} \nu(z) & 0 \\ \lambda(z) & 1 \end{pmatrix}.$$

We show later that the polyphase matrix can be factored in lifting and dual lifting steps if A is a field. For later use in §9 we remark here that if both polyphase matrices are elements of the group $\mathrm{SL}(2, A[z, z^{-1}])$ then the unit $\nu(z)$ is necessarily 1 in the lifting and dual lifting matrix.

Assume now that A is an integral domain, that is, a non-trivial commutative ring with identity in which zero is the only zero-divisor. It follows that $A[z, z^{-1}]$ is again an integral domain. Moreover, all units of $A[z, z^{-1}]$ are of the form uz^k, where u is a unit in A and k is an integer, cf. [23, p. 95]. For integral domains we get the following consequence of the lifting proposition, which will be essential in the parametrization of filter pairs:

Corollary 10 (Dirac-Lifting) *Let A be an integral domain. If $(\delta_0, \gamma) \in M \times M$ is a filter pair, then γ is of the form $P_o\gamma = b\delta_{2k+1}$ for some unit $b \in U(A)$ and some $k \in \mathbf{Z}$.*

Proof. Since (δ_0, δ_1) is a filter pair, the filter γ can be written in the form $\gamma(z) = z^{-1}\nu(z^2) + \lambda(z^2)$, where $\nu(z)$ is a unit in $A[z, z^{-1}]$. We assumed that A is an integral domain, therefore $\nu(z)$ is of the form $\nu(z) = bz^{-k}$, $b \in U(A)$. It follows that $\gamma(z) = bz^{-(2k+1)} + \lambda(z^2)$. Hence, $P_o\gamma = bz^{-(2k+1)}$. □

Lemma 11 *Let A be an integral domain. Let (α, β) be a filter pair, and assume that α satisfies $\alpha = P_e \alpha$, that is, all samples with odd index are zero in α. Then α is of the form $b\delta_{2m}$, where b is a unit in A and m is an integer.*

Proof. The z-transform of α is of the form $\alpha(z) = \alpha_e(z^2)$. The polyphase matrix corresponding to (α, β) is of the following form:

$$G_p(z) = \begin{pmatrix} \alpha_e(z) & \beta_e(z) \\ 0 & \beta_o(z) \end{pmatrix}.$$

Since (α, β) is a filter pair, it follows from Proposition 7 that the polyphase matrix $G_p(z)$ is an element of $\mathrm{GL}(2, A[z, z^{-1}])$. This means that the determinant of $G_p(z)$ is a unit in $A[z, z^{-1}]$, i. e., the product $\alpha_e(z)\beta_o(z)$ is of the form az^k, where $a \in U(A)$, and $k \in \mathbf{Z}$. Since in a commutative ring the product of two elements is a unit if and only if the elements are units, it follows that $\alpha_e(z)$ is of the form bz^m, with $b \in U(A)$, and $m \in \mathbf{Z}$. □

6 The Factorization Algorithm

Given a fundamental domain $F = (2n, 2m+1)$ of $\mathbf{Z}/2\mathbf{Z}$ and a matrix $W \in \mathrm{GL}(2, A)$, we define an operator $O_{W,F} \in G$ by

$$O_{W,F}\delta_{2n} = a\delta_{2n} + b\delta_{2m+1}, \quad O_{W,F}\delta_{2m+1} = c\delta_{2n} + d\delta_{2m+1}, \quad W = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, A).$$

The action of $O_{W,F}$ on the other basis elements δ_k is determined by the commutation relation $[O_{W,F}, T_2] = O_{W,F}T_2 - T_2 O_{W,F} = 0$. In other words, the action of the operator $O_{W,F}$ on the basis δ_n can be described by

$$O_{W,F}\delta_{2n+2k} = a\delta_{2n+2k} + b\delta_{2m+1+2k}, \quad O_{W,F}\delta_{2m+1+2k} = c\delta_{2n+2k} + d\delta_{2m+1+2k}.$$

We abbreviate $O_{W,F}$ with $F = (0, 1)$ by O_W.

The purpose of this section is to prove the following theorem, which shows that every element $B \in G$ can be factored into a chain of operators of the form $O_{W,F}$ or T_k. The proof is constructive and in fact an algorithm if A is a computable field.

Theorem 12 *Let A be a field. Then any filter pair $(\alpha, \beta) \in M \times M$ can be written in the form $(B\delta_0, B\delta_1)$, where B is a composition of a finite number of operators of the form $O_{W,F}$ or T_k, with $W \in \mathrm{GL}(2, A)$, $F = (2n, 2m+1)$, and $n, m, k \in \mathbf{Z}$.*

We prove this theorem in three steps. In the first step we reduce the filter pair (α, β) to the form (δ_0, γ). We observed in Corollary 10 that γ is then of a special form, namely $P_o\gamma = b\delta_{2k+1}$, where b is a unit in A. In a second step we show that filter pairs of this particular form (δ_0, γ) can reduced to a filter pair of the form $(\delta_0, \delta_{2k+1})$ by applying operators $O_{W,F}$. In the final step we map this filter pair to (δ_0, δ_1).

Definition 13 *Let α be a sequence in M, $l := \min(\mathrm{supp}(\alpha))$, and $r := \max(\mathrm{supp}(\alpha))$. We define the length of this sequence α by $r - l + 1$.*

Lemma 14 (Reduction I) *Let A be a field. A filter pair $(\alpha, \beta) \in M \times M$ can be mapped to a pair of the form (δ_0, γ) by applying a finite number of operators of the form T_k or $O_{W,F}$, where $k \in \mathbf{Z}$, $W \in \mathrm{GL}(2, A)$, and F is a fundamental domain of $\mathbf{Z}/2\mathbf{Z}$.*

Proof. We prove this lemma by induction on the length N of α. Without loss of generality we may always assume that the support of $\alpha \in M$ is contained in the interval $[0, N-1]$, which can be achieved by a translation T_k.

In case of length $N = 1$ we apply the operator O_D, with $D = \mathrm{diag}(a^{-1}, 1)$, to the filter pair $(\alpha, \beta) = (a\delta_0, \beta)$, which leads immediately to a filter pair of the form (δ_0, γ).

For $N > 1$ we see by Lemma 11 that $P_o\alpha$ can not be the zero sequence, since this would force α to be of length one. Denote by $l := \min(\mathrm{supp}(P_o\,\alpha))$ the smallest odd index l with non-zero sample $\alpha(\,l\,) \neq 0$. We use the abbreviations $a := \alpha(0)$ and $b := \alpha(l)$. Consider the operator $O_{W,F} \in G$ associated to the fundamental domain $F := (0, l)$ and the matrix

$$W := \begin{pmatrix} b & 0 \\ -a & 1 \end{pmatrix} \in \mathrm{GL}(2, A).$$

We apply this operator to (α, β) and obtain the filter pair $(\alpha', \beta') := (O_{W,F}\alpha, O_{W,F}\beta)$. Since W satisfies the relations $(a, b)W = (0, b)$ and $(c, 0)W = (b\,c, 0)$, the coefficient $\alpha'(0)$ is zero and the support of α' is contained in $[1, N-1]$. It follows that the length of the sequence α' is less than N. $\square$

Lemma 15 (Reduction II) *Suppose that* $(\delta_0, \gamma) \in M \times M$ *is a filter pair and assume that* γ *is a sequence of the form* $P_o\gamma = u\delta_{2k+1}$, *where* $u \in U(A)$ *and* $k \in \mathbf{Z}$ *(recall that Corollary 10 assures that this assumption on* γ *is always satisfied if* A *is a field or an integral domain). Then* (δ_0, γ) *can be mapped to* $(\delta_0, \delta_{2k+1})$ *by applying a finite number of operators of the form* $O_{W,F}$, *where* $W \in \mathrm{GL}(2, A)$ *and* F *is a fundamental domain of* $\mathbf{Z}/2\mathbf{Z}$.

Proof. Suppose that γ has a non-zero sample at the position $2n$, where $n \neq 0$ (the other case is discussed below). The idea is to apply an operator of the group G that fixes the sequence δ_0 (up to a multiplication with a unit) and that maps γ to a sequence which has a support that is strictly included in the support of the sequence γ.

Denote by b the value $b = \gamma(2n)$. Let W be the following matrix $W = \left(\begin{smallmatrix} u & 0 \\ -b & 1 \end{smallmatrix}\right)$, where u is a unit according to our hypothesis. This matrix is an element of $\mathrm{GL}(2, A)$ and satisfies the relations $(b, u)\, W = (0, u)$ and $(c, 0)\, W = (uc, 0)$. If we take the fundamental domain $F = (2n, 2k+1)$, then we claim that the operator $O_{W,F}$ has the desired properties.

Indeed, the operator $O_{W,F}$ maps the sequence δ_0 onto $u\delta_0$. We note that

$$O_{W,F}\left(\gamma(2n)\delta_{2n} + \gamma(2k+1)\delta_{2k+1}\right) = u\delta_{2k+1}\,,$$

since $(\gamma(2n), \gamma(2k+1)) = (b, u)$. Furthermore, we have by hypothesis $(\gamma(2n+m), \gamma(2k+1+m)) = (*\,, 0)$ on all even translates of the fundamental domain with $m \in 2\mathbf{Z}$, $m \neq 0$. It follows from the relations satisfied by the matrix W that

$$O_{W,F}\left(\gamma(2n+m)\delta_{2n+m} + \underbrace{\gamma(2k+1+m)}_{=0}\delta_{2k+1+m}\right) = u\,\gamma(2n+m)\delta_{2n+m}$$

holds for all $m \in 2\mathbf{Z}$, $m \neq 0$.

The support of the resulting sequence $O_{W,F}\,\gamma$ is thus strictly contained in the support of γ. Using these operators, we can reduce successively the filter pair (δ_0, γ) to a filter pair of the form $B := (u^i\delta_0, d\delta_0 + u\delta_{2k+1})$, where $d \in A$ and $i \in \mathbf{Z}$. Finally, we apply the operator $O_{V,F}$ associated to the fundamental domain $F = (0, 2k+1)$ and the matrix

$$V = \begin{pmatrix} u^{-i} & 0 \\ -u^{-(1+i)}d & u^{-1} \end{pmatrix} \in \mathrm{GL}(2, A).$$

This operator $O_{V,F}$ maps B to the desired form. □

Let now F be the fundamental domain $F = (0, 2k+1)$ where k is some integer. Denote by $O^F_{spr} \in G$ the "spreading operator" that maps (δ_0, δ_1) to $(\delta_0, \delta_{2k+1})$. The next lemma tells us that this operator can be expressed with the help of the operators T_1, T_{-1}, and O_S with $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Consequently, the inverse of O^F_{spr} can also be expressed by these operators. This proves the final step of our theorem, since the inverse of the spreading operator maps $(\delta_0, \delta_{2k+1})$ to (δ_0, δ_1).

Lemma 16 *Let $F = (0, 2k+1)$, $k \in \mathbf{Z}$. Then the spreading operator O^F_{spr} can be expressed by*

(a) composing k-times $O_S T_{-1}$, if k is non-negative.

(b) composing $(-k)$-times $T_1 O_S$, if k is negative.

Proof. (a) If k is zero, then there is nothing to prove. Let now k be positive and assume that our claim holds for $k-1$. We notice that $O^{(0,2k+1)}_{spr}$ is equal to $O_S T_{-1} \, O^{(0,2k-1)}_{spr}$, which proves part (a).

(b) The case $k = -1$ follows from the identity $O^{(0,-1)}_{spr} = T_1 O_S$. Let now k be smaller than -1 and assume that the claim holds for $k+1$. It is easy to see that $O^{(0,2k+1)}_{spr}$ equals $T_1 O_S \, O^{(0,2k+3)}_{spr}$. Therefore, part (b) follows by induction on $-k$. □

To summarize, we have seen that a given filter pair (α, β) can be reduced to the filter pair (δ_0, δ_1). The necessary reduction steps required only a finite number of operators of the form $O_{W,F}$ or T_k. Denote the composition of these operators by B^{-1}, that is, $(B^{-1}\alpha, B^{-1}\beta) = (\delta_0, \delta_1)$. Notice that the inverse operators of $O_{W,F}$ and T_k are given by $O_{W^{-1},F}$ and T_{-k} respectively. Consequently, the operator B with $(\alpha, \beta) = (B\delta_0, B\delta_1)$ is also a composition of operators $O_{W,F}$ and T_k, which concludes our proof of Theorem 12. □

A worked example illustrating these reduction steps can be found in §8.

7 Generating the Group G

Recall that there exists a bijection between filter pairs and elements of the group G. This allows us to deduce from Theorem 12 that all operators $B \in G$ can be composed by a finite number of operators of the form T_k or $O_{W,F}$, provided A is a field. In other words, the group G is generated by these operators. In this section we want to derive a reduced set of generators for the group G. More precisely, we want to prove the following theorem:

Theorem 17 *Let A be a field. The group G of all A-module automorphisms commuting with even translations is generated by T_1, and operators of the form O_W, $W \in \mathrm{GL}(2, A)$. Moreover, all operators $B \in G$ can be expressed as*

$$T_n O_{W_1} T_1 O_{W_2} \cdots T_1 O_{W_m}, \qquad \textit{where} \quad W_i \in \mathrm{GL}(2, A),\ W_i \neq I,\ n \in \mathbf{Z}, m \in \mathbf{N}.$$

Proof. We observe that each operator $O_{W,F}$ with fundamental domain $F = (2n, 2m+1)$ can be expressed as $O_{W,F} = O_{W,F^0}$, where $F^0 = (0, 2m - 2n + 1)$. Let now F be the fundamental domain $F = (0, 2k+1)$ where k is some integer. We note that all operators $O_{W,F}$ with $F = (0, 2k+1)$ can be written as follows:

$$O_{W,F} = O^F_{spr} O_W.$$

It follows from Lemma 16 that O^F_{spr} can be expressed by means of the translations T_1, T_{-1}, and the swap O_S with $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which proves the first part of the theorem.

It remains to show that each operator B can be expressed in the form given in the theorem. We note that B can be written as an alternating composition of T_k and O_W, since we have the identities $T_m T_n = T_{n+m}$ and $O_W O_V = O_{VW}$. Furthermore, since T_2 is in the center of G, we can bring this alternating product to one of the following forms:

$$T_n O_{W_1} T_1 O_{W_2} \cdots T_1 O_{W_m} \quad \text{or as} \quad T_n O_{W_1} T_1 O_{W_2} \cdots T_1 O_{W_m} T_1,$$

where $W_i \in \mathrm{GL}(2, A)$ and $n, m \in \mathbf{Z}$, $m > 0$. Clearly, we may assume without loss of generality that all matrices W_i differ from the identity matrix.

The second form is a special case of the first form, since we can write T_1 more complicated as $T_1 = T_{-2} O_V T_1 O_W T_1 O_X T_1 O_Y$, where V, W, X, and Y are the following elements of $\mathrm{GL}(2, A)$:

$$V := \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad W := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad X := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad Y := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

It follows that

$$T_n O_{W_1} T_1 O_{W_2} \cdots T_1 O_{W_m} T_1 = T_{n-2} O_{W_1} T_1 O_{W_2} \cdots T_1 O_{V W_m} T_1 O_W T_1 O_X T_1 O_Y,$$

which concludes the proof of the theorem. □

The second part of the theorem gives a convenient (non-unique) parametrization of all filter pairs. Clearly, the theorem does imply the following parametrization of filter pairs over integral domains:

Corollary 18 *Let A be an integral domain and denote by* $\mathrm{Quot}(A)$ *its quotient field. Then every filter pair $(\alpha,\beta) \in M \times M$ can be obtained by applying some operator of the form*

$$T_n O_{W_1} T_1 O_{W_2} \cdots T_1 O_{W_m}, \qquad \textit{where} \quad W_i \in \mathrm{GL}(2, \mathrm{Quot}(A)),\ W_i \neq I,\ n \in \mathbf{Z}, m \in \mathbf{N},$$

to the filter pair (δ_0, δ_1).

The claim of this corollary does not hold in general, if we restrict the matrices W_i to be elements of $\mathrm{GL}(2, A)$.

As a further consequence of the proof of the theorem we note the following fact:

Corollary 19 *Let A be an arbitrary commutative ring with identity. Denote by G the group of all A-module automorphisms commuting with the even translations. Let H be the subgroup of G generated by the operators T_k, and $O_{W,F}$, where $k \in \mathbf{Z}$, $W \in \mathrm{GL}(2, A)$, and F is a fundamental domain of $\mathbf{Z}/2\mathbf{Z}$. Then H is already generated by the operators T_1 and O_W, $W \in \mathrm{GL}(2, A)$. Moreover, all operators in H can be expressed as*

$$T_n O_{W_1} T_1 O_{W_2} \cdots T_1 O_{W_m}, \qquad \textit{where} \quad W_i \in \mathrm{GL}(2, A),\ W_i \neq I,\ n \in \mathbf{Z}, m \in \mathbf{N}.$$

Theorem 17 assures that the group H coincides with G provided A is a field, thereby we obtain a complete parametrization of filter pairs; for other rings A we obtain at least a rich family of filter pairs by applying the elements of H to the filter pair (δ_0, δ_1).

8 Examples

We give three examples in this section. The first one is meant to illustrate the reduction steps in the proof of Theorem 12. The second example gives a parametrization of real-valued biorthogonal filters; and the third example is concerned with the construction of filter pairs over the finite field GF(2).

Worked Example. Consider the following filter pair [9] with values in the dyadic rationals:

$$\alpha = \frac{1}{2}\delta_0 - \delta_1 + \frac{1}{2}\delta_2, \qquad \beta = -\frac{1}{4}\delta_0 + \frac{1}{2}\delta_1 + \frac{3}{2}\delta_2 + \frac{1}{2}\delta_3 - \frac{1}{4}\delta_4.$$

The first reduction step sets out to map the filter pair (α, β) to a filter pair of the form (δ_0, γ). Following the algorithm described in the proof of Lemma 14 (Reduction I), we derive the operator

$O_{W_3}T_1O_{W_2}T_1O_{W_1}$, where the matrices $W_i \in \mathrm{GL}(2,\mathbf{Q})$ are given by

$$W_1 = \begin{pmatrix} -1 & 0 \\ -1/2 & 1 \end{pmatrix}, \quad W_2 = \begin{pmatrix} -1/2 & 0 \\ 1 & 1 \end{pmatrix}, \quad W_3 = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}.$$

It is easy to check that this operator maps (α, β) to the filter pair (δ_0, γ) with

$$\gamma = -2\delta_{-1} + \frac{7}{2}\delta_0 - \frac{1}{2}\delta_2.$$

According to the second reduction step (Lemma 15), we have to apply first the operator O_{W_4,F_4} and then O_{W_5,F_5}, which correspond the the fundamental domains $F_4 = (2,-1)$ and $F_5 = (0,-1)$ of $\mathbf{Z}/2\mathbf{Z}$ and the matrices

$$W_4 = \begin{pmatrix} -2 & 0 \\ 1/2 & 1 \end{pmatrix}, \quad W_5 = \begin{pmatrix} -1/2 & 0 \\ 7/4 & -1/2 \end{pmatrix}.$$

The result of this second reduction is

$$(O_{W_5,F_5}\, O_{W_4,F_4}\delta_0, O_{W_5,F_5}\, O_{W_4,F_4}\gamma) = (\delta_0, \delta_{-1}).$$

The final reduction uses the inverse of the spreading operator $O_{spr}^{(0,-1)} = T_1 O_S$, i.e., the operator $O_S T_{-1}$, to map (δ_0, δ_{-1}) to the filter pair (δ_0, δ_1). Upon inverting all operators and reversing the order of composition, we finally obtain the operator B which maps (δ_0, δ_1) to (α, β) :

$$B = O_{W_1^{-1}}\, T_{-1}\, O_{W_2^{-1}}\, T_{-1}\, O_{W_3^{-1}}\, O_{W_4^{-1},F_4}\, O_{W_5^{-1},F_5}\, T_1\, O_S.$$

The Real Numbers R. Recall that all elements of the special linear group $\mathrm{SL}(2,\mathbf{R})$ can be expressed as a product $u(x)s(a)r(\theta)$ of the following matrices, cf. Lang [24, p. 238] or Segal [7]:

$$u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \qquad s(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \qquad r(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix},$$

where $x, a, \theta \in \mathbf{R}$, $a > 0$.

Let $W_i \in \mathrm{SL}(2,\mathbf{R})$ be the matrix $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$. Then we have

$$O_{W_1}\delta_0 = a_1\delta_0 + b_1\delta_1, \qquad O_{W_1}\delta_1 = c_1\delta_0 + d_1\delta_1.$$

Thus the matrix $W(x,a,\theta) = u(x)s(a)r(\theta)$ leads to a three parameter family of filter pairs $(O_{W(x,a,\theta)}\delta_0, O_{W(x,a,\theta)}\delta_1)$, where an easy calculation shows that

$$\begin{aligned} O_{W(x,a,\theta)}\,\delta_0 &= (a\cos\theta - (x/a)\sin\theta)\delta_0 + (a\sin\theta + (x/a)\cos\theta)\delta_1, \\ O_{W(x,a,\theta)}\,\delta_1 &= (-a^{-1}\sin\theta)\,\delta_0 + (a^{-1}\cos\theta)\delta_1. \end{aligned}$$

If we apply the operator $O_{W_2}T_1O_{W_1}$ to the filter pair (δ_0, δ_1), then we obtain:

$$\begin{aligned} O_{W_2}T_1O_{W_1}\delta_0 &= a_1c_2\,\delta_{-2} + a_1d_2\,\delta_{-1} + b_1a_2\,\delta_0 + b_1b_2\,\delta_1, \\ O_{W_2}T_1O_{W_1}\delta_1 &= c_1c_2\,\delta_{-2} + c_1d_2\,\delta_{-1} + d_1a_2\,\delta_0 + d_1b_2\,\delta_1. \end{aligned}$$

Using the parametrized matrices $W(x_i, a_i, \theta_i)$, with $i = 1, 2$, then a simple substitution yields the following six parameter family of filter pairs:

$$\begin{aligned} O_{W(x_2,a_2,\theta_2)}T_1O_{W(x_1,a_1,\theta_1)}\delta_0 &= \alpha_{-2}\,\delta_{-2} + \alpha_{-1}\,\delta_{-1} + \alpha_0\,\delta_0 + \alpha_1\,\delta_1, \\ O_{W(x_2,a_2,\theta_2)}T_1O_{W(x_1,a_1,\theta_1)}\delta_1 &= \beta_{-2}\,\delta_{-2} + \beta_{-1}\,\delta_{-1} + \beta_0\,\delta_0 + \beta_1\,\delta_1, \end{aligned}$$

with

$$\begin{aligned} \alpha_{-2} &= \frac{(-a_1^2\cos\theta_1 + x_1\sin\theta_1)\sin\theta_2}{a_1a_2}, & \beta_{-2} &= \frac{\sin\theta_1\sin\theta_2}{a_1a_2}, \\ \alpha_{-1} &= -\frac{(-a_1^2\cos\theta_1 + x_1\sin\theta_1)\cos\theta_2}{a_1a_2}, & \beta_{-1} &= -\frac{\sin\theta_1\cos\theta_2}{a_1a_2}, \\ \alpha_0 &= -\frac{(a_1^2\sin\theta_1 + x_1\cos\theta_1)(-a_2^2\cos\theta_2 + x_2\sin\theta_2)}{a_1a_2}, & \beta_0 &= -\frac{\cos\theta_1(-a_2^2\cos\theta_2 + x_2\sin\theta_2)}{a_1a_2}, \\ \alpha_1 &= \frac{(a_1^2\sin\theta_1 + x_1\cos\theta_1)(a_2^2\sin\theta_2 + x_2\cos\theta_2)}{a_1a_2}, & \beta_1 &= \frac{\cos\theta_1(a_2^2\sin\theta_2 + x_2\cos\theta_2)}{a_1a2}. \end{aligned}$$

This gives a convenient parametrization of biorthogonal real-valued filter pairs. For the sake of simplicity we restricted ourselves to matrices with determinant one, ignoring a further scaling factor. The submanifold obtained by fixing the parameters $x_i = 0$ and $a_i = 1$ parametrizes the real-valued QMFs, see for example [14, 15].

The Finite Field GF(2). The finite field with two elements GF(2) is very attractive from a computational point of view, since the addition in this field can be realized by an '*exclusive-or*' gate and the multiplication by an '*and*' gate. Furthermore, the storage of one field element requires only a single one-bit register. Therefore, this arithmetic is particularly suitable for digital circuit or binary computer implementations.

The general linear group over GF(2) is of order six; its elements are given by the following matrices:

$$M_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad M_3 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$
$$M_4 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_5 := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_6 := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

If we apply the operator $O_{M_2}T_1O_{M_3}$ to the filter pair (δ_0, δ_1), then we obtain

$$\begin{aligned} \alpha &= O_{M_2}T_1O_{M_3}\delta_0 = O_{M_2}T_1\delta_0 = O_{M_2}\delta_{-1} = \delta_{-1}, \\ \beta &= O_{M_2}T_1O_{M_3}\delta_1 = O_{M_2}T_1(\delta_0 + \delta_1) = O_{M_2}(\delta_{-1} + \delta_0) = \delta_{-1} + \delta_0 + \delta_1. \end{aligned}$$

Clearly, a sequence over GF(2) is completely determined by its support. For example, the filter pair $(T_1\alpha, T_1\beta)$ is determined by $\operatorname{supp}(T_1\alpha) = \{-2\}$ and $\operatorname{supp}(T_1\beta) = \{-2, -1, 0\}$. We give in Appendix A a table of filter pairs (α, β) with small support; this table lists analysis and synthesis filters for several operators. The interested reader may check that our calculation of $T_1\alpha = T_1O_{M_2}T_1O_{M_3}\delta_0$ and $T_1\beta = T_1O_{M_2}T_1O_{M_3}\delta_1$ coincides with the tabulated sequences.

9 Lifting Steps and Euclid's Algorithm

There exist numerous techniques to reduce the computational complexity of a filter bank. We discuss only one technique here, namely the factorization of filters into lifting (or ladder) steps. Lifting techniques were advocated by Sweldens [39, 38] and others [3, 18]. The basic idea is to avoid convolutions with lengthy filters using a network of small length filters.

Daubechies and Sweldens showed in a recent paper [12] that all real-valued filter pairs can be factored into lifting and dual lifting steps. We extend their approach to arbitrary fields and show that it can not be generalized further to integral domains which fail to be fields.

Assume that we are given a Laurent polynomial $f \in A[z, z^{-1}]$ of the form $f(z) = \sum_{k=m}^{n} a_k z^k$, where both a_n and a_m are non-zero. Then a_n is called the leading coefficient of f and is denoted by $\operatorname{lc}(f)$; the corresponding exponent n is denoted by $\operatorname{lcdeg}(f)$. We define the degree of a Laurent polynomial f by

$$\operatorname{ldeg}(f) := \operatorname{lcdeg} f(z) + \operatorname{lcdeg} f(1/z).$$

If A is a field, then $A[z,z^{-1}]$ is an Euclidean domain, that is, for all $f,g \in A[z,z^{-1}]$, $g \neq 0$, there exist elements $q,r \in A[z,z^{-1}]$ with the property $f = q\,g + r$ and either $r = 0$ or $\operatorname{ldeg}(r) < \operatorname{ldeg}(g)$. Thus, the greatest common divisor of two elements $x_0, x_1 \in A[z,z^{-1}]$ exists and can be determined by the well-known Euclidean algorithm by successive application of division with remainder:

$$\begin{array}{rcll} x_0 &=& q_1\,x_1 + x_2, & \operatorname{ldeg}(x_2) < \operatorname{ldeg}(x_1) \\ x_1 &=& q_2\,x_2 + x_3, & \operatorname{ldeg}(x_3) < \operatorname{ldeg}(x_2) \\ &\vdots&& \\ x_{n-2} &=& q_{n-1}\,x_{n-1} + x_n, & \operatorname{ldeg}(x_n) < \operatorname{ldeg}(x_{n-1}) \\ x_{n-1} &=& q_n\,x_n. & \end{array}$$

It is easily seen that $x_n = \gcd(x_0, x_1)$. Let us rewrite the equations $x_i = q_{i+1}\,x_{i+1} + x_{i+2}$ in terms of matrices. Denote by E_i the matrix $\begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ and let $x_{n+1} := 0$, then the Euclidean remainder scheme yields:

$$\begin{pmatrix} x_j \\ x_{j+1} \end{pmatrix} = E_j \cdots E_1 \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \qquad \text{for} \quad 1 \leq j \leq n,$$

and in particular

$$\begin{pmatrix} x_n \\ 0 \end{pmatrix} = E_n \cdots E_1 \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}. \tag{7}$$

The Euclidean algorithm is the main tool in the constructive proof of the following theorem:

Theorem 20 *Let A be a field, let $(\alpha,\beta) \in M \times M$ be a filter pair with polyphase matrix $H_p(z)$. Then there exist Laurent polynomials $\lambda_i(z) \in A[z,z^{-1}]$ such that $H_p(z)$ can be written as an alternating product of lifting and dual lifting matrices, followed by a diagonal matrix:*

$$H_p(z) = \prod_{i=1}^{m} \left[\begin{pmatrix} 1 & \lambda_{2i}(z) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda_{2i+1}(z) & 1 \end{pmatrix} \right] \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \tag{8}$$

where $d = \det H_p(z)$.

Proof. Multiplication of the polyphase matrix $H_p(z)$ with the diagonal matrix $\operatorname{diag}(1, d^{-1})$, $d = \det H_p(z)$, yields an element of the special linear group $\mathrm{SL}(2, A[z,z^{-1}])$. Therefore, we may assume from now on that the polyphase matrices are elements of $\mathrm{SL}(2, A[z,z^{-1}])$. We proceed to show how the Euclidean algorithm allows us to factor the polyphase matrix $H_p(z)$ in lifting and dual lifting steps.

The polyphase components $\alpha_e(z)$ and $\alpha_o(z)$ of α are coprime, since a common factor would divide the determinant of the polyphase matrix. Let $x_0 := \alpha_e(z)$ and $x_1 := \alpha_o(z)$. Then the Euclidean algorithm (7) allows us to write the vector $(\alpha_e(z), \alpha_o(z))^t$ in the following form:

$$E_1^{-1} \cdots E_n^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_e(z) \\ \alpha_o(z) \end{pmatrix}, \quad \text{where} \quad E_i^{-1} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}. \tag{9}$$

The matrices E_i^{-1} can be written as

$$E_i^{-1} \overset{a.}{=} \begin{pmatrix} 1 & q_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \overset{b.}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_i & 1 \end{pmatrix}. \tag{10}$$

Suppose that n is even, then we can extend (9) to a matrix in $\mathrm{SL}(2, A[z, z^{-1}])$ upon setting

$$H_p^0(z) = E_1^{-1} \cdots E_n^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

If we subsitute the matrices E_i^{-1} with even index i by the factored form given in (10, a.) and replace the matrices E_i^{-1} with odd index i by the factored form (10, b.), then we obtain a factorization of $H_p^0(z)$ in lifting and dual lifting matrices. A single lifting from $H_p^0(z)$ to $H_p(z)$ then leads to the desired factorization of $H_p(z)$.

Suppose that n is odd, then we can extend (9) to a matrix in $\mathrm{SL}(2, A[z, z^{-1}])$ upon setting

$$H_p^0(z) = E_1^{-1} \cdots E_n^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If we replace E_i^{-1} with even index i by the factored form (10, a.), substitute all E_i^{-1} with odd index $i < n$ by the factored form (10, b.), and write

$$E_n^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} q_n & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & q_n - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$

then we obtain a factorization of $H_p^0(z)$ in lifting and dual lifting steps. Again, a single lifting step is necessary to recover $H_p(z)$ from $H_p^0(z)$. This completes the proof. □

The theorem essentially comes down to saying that the group $\mathrm{SL}(2, A[z, z^{-1}])$ is generated by elementary matrices, i. e., matrices that differ from the identity matrix by at most one non-zero off-diagonal entry. It is well-known that the special linear group over any Euclidean domain is generated by elementary matrices, see e.g. [33, Satz VI.B.6]. We gave the full proof, since it yields a simple algorithm to construct a network of small length filters. The above proof differs only in detail from the proof given in [12] for the special linear group with entries in $\mathbf{R}[z, z^{-1}]$.

We discuss briefly the benefit of the factorization in lifting steps. A single decomposition step amounts to convolve the even and odd part of the signal with the filters $\alpha_e(z)$, $\beta_e(z)$ and $\alpha_o(z)$, $\beta_o(z)$ respectively. Thus, the standard algorithm requires at most

$$\operatorname{ldeg} \alpha_e(z) + \operatorname{ldeg} \alpha_o(z) + \operatorname{ldeg} \beta_e(z) + \operatorname{ldeg} \beta_o(z) + 4$$

multiplications.

The Euclidean representation of x_0, x_1 is given by the sequence of quotients q_i and the greatest common divisor: $(q_1, \ldots, q_n, x_n)$. The sequence

$$(d_1, \ldots, d_n, g) := (\operatorname{ldeg} q_1, \ldots, \operatorname{ldeg} q_n, \operatorname{ldeg} x_n)$$

is the corresponding degree pattern. Denote by N_0 and N_1 the degrees of the Laurent polynomials x_0, x_1. It can be shown that the "typical" degree pattern of two elements $x_0, x_1 \in A[z, z^{-1}]$ with $N_0 > N_1$ is of the form $(N_0 - N_1, 1, \ldots, 1, 0)$, provided that A is a field, cf. [4].

Assume now that $\operatorname{ldeg} \alpha \leq \operatorname{ldeg} \beta$ (otherwise exchange the rôle of α and β). Consider a filter pair (α, β) with $\operatorname{ldeg} \alpha(z) = 2N$ and $\operatorname{ldeg} \beta = 2M$ and assume that their polyphase components have the degrees $\operatorname{ldeg} \alpha_e(z) = N$, $\operatorname{ldeg} \alpha_o(z) = N - 1$, $\operatorname{ldeg} \beta_e(z) = M$, and $\operatorname{ldeg} \beta_o(z) = M - 1$. Thus, the Euclidean algorithm applied to $\alpha_e(z), \alpha_o(z)$ usually will need N steps. Consequently, the convolutions with the filters q_i, $1 \leq i \leq N$, typically need $2N$ multiplications. The final lifting step is realized with a filter of degree $M - N$ and therefore can be implemented with at most $M - N + 1$ multiplications. The diagonal matrix yields a futher multiplication. In summary, we typically need $M + N + 2$ multiplications for the lifting implementation which compares favourably with the $2M + 2N + 2$ multiplications for the standard implementation!

10 Conclusion

We presented a parametrization of filter pairs. We proved that this parametrization allows to generate all filter pairs with values in a field A by applying to (δ_0, δ_1) a finite number of translation operators or operators O_W associated to matrices of the general linear group $W \in \mathrm{GL}(2, A)$.

This result extends to integral domains A, provided that we allow operators O_W associated to matrices of the general linear group over the quotient field $W \in \mathrm{GL}(2, \mathrm{Quot}(A))$. A complete parametrization of all real-valued biorthogonal filters was obtained as a special case. We showed that in general it is possible to reduce the computational complexity of a two-channel filter bank by a factorization into lifting steps, assuming that A is a field.

Acknowledgements. Kristin Flornes greatfully acknowledges support by the Norwegian Research Council 100552/410. Andreas Klappenecker thanks DFG for support through SFB 414 "Informationstechnik in der Medizin – Rechner- und sensorgestützte Chirurgie".

A Filter Pairs over GF(2)

Table 1 lists operators, analysis filters $(\widetilde{\alpha}, \widetilde{\beta})$, and synthesis filters (α, β) for sequences over GF(2). The operator B is given in the first column. The last two columns list the support of the synthesis filters $(\alpha, \beta) = (B\delta_0, B\delta_1)$. The corresponding analysis filters $(\widetilde{\alpha}, \widetilde{\beta})$ are given in the second and third column of the table.

References

[1] A. N. Akansu and R. A. Haddad. *Multiresolution Signal Decomposition – Transforms, Subbands, and Wavelets.* Academic Press, Inc., 1992.

[2] N. Bourbaki. *Algebra I, Chap. 1-3.* Springer-Verlag, 1989.

[3] F. A. Brueckers and A. W. van den Enden. New networks for perfect inversion and perfect reconstruction. *IEEE J. on Selected Areas in Communications*, 10(1):130–137, 1992.

[4] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory.* Springer-Verlag, 1997.

[5] G. Caire, R. L. Grossman, and H. V. Poor. Wavelet transforms associated with finite cyclic groups. *IEEE Trans. on Information Theory,* 39(4):1157–1166, 1993.

[6] A. R. Calderbank, I. Daubechies, W. Sweldens, and B. L. Yeo. Wavelet transforms that map integer to integers. Preprint, 1996.

[7] R. Carter, G. Segal, and I. MacDonald. *Lectures on Lie Groups and Lie Algebras.* Cambridge University Press, Cambridge, Great Britain, 1995.

[8] T. Chen and P. P. Vaidyanathan. Vector space framework for unification of one- and multidimensional filter bank theory. *IEEE Trans. on Signal Processing*, 42(8):2006–2021, 1994.

[9] A. Cohen, I. Daubechies, and J.-C. Feauveau. Biorthogonal bases of compactly supported wavelets. *Comm. Pure Appl. Math.*, 45:485–560, 1992.

[10] I. Daubechies. Orthonormal bases of compactly supported wavelets. *Comm. Pure Appl. Math.*, 41:909–996, 1988.

[11] I. Daubechies. *Ten Lectures on Wavelets.* CBMS-NSF Reg. Conf. Series Appl. Math. SIAM, 1992.

[12] I. Daubechies and W. Sweldens. Factoring wavelet transforms into lifting steps. Preprint[1], 1996.

[13] K. Flornes and M. Holschneider. Finite filters. Unpublished manuscript, 1995.

[14] M. Holschneider. Wavelet analysis over abelian groups. *Applied and Computational Harmonic Analysis*, 2:52–60, 1995.

[15] M. Holschneider. *Wavelets – An Analysis Tool.* Oxford University Press, 1995.

[16] M. Holschneider and U. Pinkall. Quadratic mirror filters and loop groups. Preprint, TU-Berlin, 1993.

[17] C. P. Johnston. The lifting scheme and finite-precision-error-free filter banks. In M. Unser, A. Aldroubi, and A. Laine, editors, *Wavelet Applications in Signal and Image Processing IV*, volume 2825, pages 307–316. SPIE, 1996.

[18] T. Kalker and I. Shah. On ladder structures and linear phase conditions for multidimensional biorthogonal filter banks. Preprint, Philips research laboratories, Eindhoven.

[19] M. R. Kansari and E. Dubois. Padé table, continued fraction expansion, and perfect reconstruction filter banks. *IEEE Trans. on SP*, 44(8):1955–1963, 1996.

[20] A. Klappenecker. Algebraic wavelet filters. *International Journal of Imaging Systems and Technology*, 7(3):166–169, 1996.

[21] A. Klappenecker. Two-channel perfect reconstruction filter banks over arbitrary fields. Unpublished manuscript, 1996.

[22] A. Klappenecker, A. Nückel, and F. U. May. Lossless image compression using wavelets over finite rings and related architectures. In M. A. Unser, A. Aldroubi, and A. F. Laine, editors, *Wavelet Applications in Signal and Image Processing V*, volume 3169. SPIE, 1997.

[23] T. Y. Lam. *A First Course in Noncommutative Rings.* Springer-Verlag, 1991.

[24] S. Lang. *Undergraduate Algebra.* Springer-Verlag, 2nd edition, 1990.

[1] `http://cm.bell-labs.com/who/wim/papers/`

[25] S. Lang. *Algebra.* Addison-Wesley, 3rd edition, 1993.

[26] S. Mallat. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Trans. Pattern Anal. Mach. Intell.*, 11(7):674–693, Juli 1989.

[27] F. Mintzer. Filters for distortion-free two-band multirate filter banks. *IEEE Acoust., Speech, and Signal Proc.*, 33(3):626–630, 1985.

[28] S.-M. Phoong and P. P. Vaidyanathan. Paraunitary filter banks over finite fields. Preprint, submitted to *IEEE Trans. on SP.*

[29] D. Pollen. Parametrization of compactly supported wavelets. Technical Report AD890503.1.4, Aware Inc., 1989.

[30] D. Pollen. $SU_I(2, F[z, 1/z])$ for F a subfield of C. *JAMS*, 3, 1990.

[31] H. V. Poor. Finite-field wavelet transforms. In J.Y. Chouinard, P. Fortier, and T. A. Gulliver, editors, *Information Theory and Applications II*, LNCS 1133, pages 225–238. Springer Verlag, 1996.

[32] S. Sarkar and H. V. Poor. Finite field wavelet transforms and multilevel error protection. In *Proc. 1995 Intl. Symp. on Information Theory*, page 428, Whistler, BC, Canada, 1995. IEEE.

[33] G. Scheja and U. Storch. *Lehrbuch der Algebra*, volume 1. B. G. Teubner Verlag, Stuttgart, 2nd edition, 1994.

[34] M. J. T. Smith and T. P. Barnwell. Exact reconstruction techniques for tree structured subband coders. *IEEE ASSP*, 34:434–441, 1986.

[35] M. D. Swanson and A. H. Tewfik. Wavelet decomposition of binary finite images. In *Proc. IEEE Int. Conf. on Image Proc.*, pages 61–65. IEEE, 1994.

[36] M. D. Swanson and A. H. Tewfik. A binary wavelet decomposition of binary images. Preprint, To appear in IEEE Trans. on Image Processing, 1995.

[37] M. D. Swanson and A. H. Tewfik. A binary wavelet decomposition of binary images. *IEEE Trans. on Image Processing*, 5(6), 1996.

[38] W. Sweldens. The lifting scheme: A construction of second generation wavelets. Technical report, Dept. of Math., University of South Carolina, 1995.

[39] W. Sweldens. The lifting scheme: a custom-design construction of biorthogonal wavelets. *Appl. Comp. Harmon. Anal.*, 3(2):186–200, 1996.

[40] P. Vaidyanathan. Unitary and paraunitary systems in finite fields. In *Proc. 1990 IEEE Int. Symp. on Circuits and Systems*, pages 1189–1192. IEEE, 1990.

[41] P. Vaidyanathan, T. Truong, Z. Doğanatha, and T. Saramäki. Improved technique for design of perfect reconstruction FIR QMF banks with lossless polyphase matrices. *IEEE Trans. on ASSP*, 37(7):1042–1056, 1989.

[42] P. P. Vaidyanathan. Quadrature mirror filter banks, M-band extensions and perfect-reconstruction techniques. *IEEE ASSP Magazine*, pages 4–20, 1987.

[43] P. P. Vaidyanathan. *Multirate Systems and Filter Banks.* Prentice Hall, 1993.

[44] P. P. Vaidyanathan and P. Q. Hoang. Lattice structures for optimal design and robust implementation of two-channel perfect reconstruction filter banks. *IEEE Trans. Acoust., Speech, Signal Processing*, 36:81–94, 1988.

[45] J. A. van Hulzen and J. Calmet. Computer algebra systems. In B. Buchberger, G. E. Collins, and R. Loos, editors, *Computer Algebra – Symbolic and Algebraic Computation*, pages 221–243. Springer Verlag, 1983.

[46] M. Vetterli. Filter banks allowing perfect reconstruction. *Signal Processing*, 10:219–244, 1986.

[47] M. Vetterli. A theory of multirate filter banks. *IEEE Trans. Acoust., Speech, Signal Processing*, 35(3):356–372, 1987.

[48] M. Vetterli and C. Herley. Wavelets and filter banks: Theory and design. *IEEE Trans. on Signal Processing*, 40:2207–2232, Sept. 92.

[49] M. Vetterli and J. Kovačević. *Wavelets and Subband Coding.* Prentice Hall, 1995.

[50] M. Vetterli and D. Le Gall. Perfect reconstruction FIR filter banks: some properties and factorizations. *IEEE Trans. on ASSP*, 37(7):1057–1071, 1989.

[51] R. O. Wells. Parametrizing smooth compactly supported wavelets. *Trans. Amer. Math. Soc.*, 338(2):919–931, 1993.

[52] H. Zou and A. H. Tewfik. Parametrization of compactly supported orthonormal wavelets. *IEEE Trans. Signal Processing*, 41(3):1428–1431, 1993. *Errata, ibid.,* 42(1):208-209, 1994.

Table 1: Table of some analysis and synthesis filter sequences over GF(2).

Operator	supp($\widetilde{\alpha}$)	supp($\widetilde{\beta}$)	supp(α)	supp(β)
$T_1O_{M_2}$	1	$0, 1$	$-1, 0$	0
$T_1O_{M_3}$	$0, 1$	0	-1	$-1, 0$
$T_1O_{M_4}$	0	1	0	-1
$T_1O_{M_5}$	$0, 1$	1	0	$-1, 0$
$T_1O_{M_6}$	0	$0, 1$	$-1, 0$	-1
$T_1O_{M_2}T_1O_{M_2}$	$2, 3$	$1, 2, 3$	$-2, -1, 0$	$-1, 0$
$T_1O_{M_2}T_1O_{M_3}$	$1, 2, 3$	1	-2	$-2, -1, 0$
$T_1O_{M_2}T_1O_{M_4}$	1	$2, 3$	$-1, 0$	-2
$T_1O_{M_2}T_1O_{M_5}$	$1, 2, 3$	$2, 3$	$-1, 0$	$-2, -1, 0$
$T_1O_{M_2}T_1O_{M_6}$	1	$1, 2, 3$	$-2, -1, 0$	-2
$T_1O_{M_3}T_1O_{M_2}$	2	$0, 1, 2$	$-3, -2, -1$	-1
$T_1O_{M_3}T_1O_{M_3}$	$0, 1, 2$	$0, 1$	$-3, -2$	$-3, -2, -1$
$T_1O_{M_3}T_1O_{M_4}$	$0, 1$	2	-1	$-3, -2$
$T_1O_{M_3}T_1O_{M_5}$	$0, 1, 2$	2	-1	$-3, -2, -1$
$T_1O_{M_3}T_1O_{M_6}$	$0, 1$	$0, 1, 2$	$-3, -2, -1$	$-3, -2$
$T_1O_{M_4}T_1O_{M_2}$	3	$0, 3$	$-3, 0$	0
$T_1O_{M_4}T_1O_{M_3}$	$0, 3$	0	-3	$-3, 0$
$T_1O_{M_4}T_1O_{M_4}$	0	3	0	-3
$T_1O_{M_4}T_1O_{M_5}$	$0, 3$	3	0	$-3, 0$
$T_1O_{M_4}T_1O_{M_6}$	0	$0, 3$	$-3, 0$	-3
$T_1O_{M_5}T_1O_{M_2}$	3	$0, 1, 3$	$-3, -2, 0$	0
$T_1O_{M_5}T_1O_{M_3}$	$0, 1, 3$	$0, 1$	$-3, -2$	$-3, -2, 0$
$T_1O_{M_5}T_1O_{M_4}$	$0, 1$	3	0	$-3, -2$
$T_1O_{M_5}T_1O_{M_5}$	$0, 1, 3$	3	0	$-3, -2, 0$
$T_1O_{M_5}T_1O_{M_6}$	$0, 1$	$0, 1, 3$	$-3, -2, 0$	$-3, -2$
$T_1O_{M_6}T_1O_{M_2}$	$2, 3$	$0, 2, 3$	$-3, -1, 0$	$-1, 0$
$T_1O_{M_6}T_1O_{M_3}$	$0, 2, 3$	0	-3	$-3, -1, 0$
$T_1O_{M_6}T_1O_{M_4}$	0	$2, 3$	$-1, 0$	-3
$T_1O_{M_6}T_1O_{M_5}$	$0, 2, 3$	$2, 3$	$-1, 0$	$-3, -1, 0$
$T_1O_{M_6}T_1O_{M_6}$	0	$0, 2, 3$	$-3, -1, 0$	-3