GROUP FILTERS AND IMAGE PROCESSING

Richard Tolimieri and Myoung An
Prometheus Inc.
Newport, Rhode Island U.S.A.
myoung@prometheus-inc.com

Abstract Abelian group DSP can be completely described in terms of a special class of signals, the characters, defined by their relationship to the translations defined by abelian group multiplication. The first problem to be faced in extending classical DSP theory is to decide on what is meant by a translation. We have selected certain classes of nonabelian groups and defined translations in terms of left nonabelian group multiplications.

The main distinction between abelian and nonabelian group DSP centers around the problem of character extensions. For abelian groups the solution of the character extension problem is simple. Every character of a subgroup of an abelian group A extends to a character of A. We will see that character extensions lie at the heart of several fast Fourier transform (FFT) algorithms.

The nonabelian groups presented in this work will be among the simplest generalizations of abelian groups. A complete description of the DSP of an abelian by abelian semidirect product will be given. For such a group G, there exists an abelian normal subgroup A. A basis for signals indexed by G can be constructed by extending the characters of A and then by forming certain (left-) translations of these characters. The crucial point is that some of these characters of A cannot be extended to characters of G, but only to proper subgroups of G. In contrast to abelian group DSP expansions, expansions in nonabelian group DSP reflect local signal domain information over these proper subgroups. These expansions can be viewed as combined, local image-spectral image domain expansions in analogy to time-frequency expansions.

This DSP leads to the definition of a certain class of group filters whose properties will be explored on simulated and recorded images. Through examples we will compare nonabelian group filters with classical abelian group filters. The main observation is that in contrast to abelian group filters, nonabelian group filters can localize in the image domain. This advantage has been used for detecting and localizing the position of geometric objects in image data sets.

The works of R. Holmes M. Karpovski and E. Trachtenberg are the basis of much of the research in the application of nonabelian group harmonic analysis to DSP, especially in the construction of group transforms and group filters. Similar ideas in coding theory have been introduced by F. J. MacWilliams.

During the last ten years considerable effort has taken place to extend the range of applicability of nonabelian group methods to the design of new filters and spectral analysis methodologies, as an image processing tool. Accompanying these application efforts, there has been extensive development of algorithms for computing Fourier transforms over nonabelian groups generalizing the classical FFT.

Keywords: finite group harmonic analysis, group filters, image domain locality.

1. Introduction: Classical Digital Signal Processing

There are two disjoint themes in this work: the fundamental role played by translations of data in all aspects of digital signal processing (DSP) and the role of group structures on data indexing sets in defining these translations.

The set of integers paired with addition modulo N is the simplest finite abelian group. The term *abelian* refers to the fact that addition modulo N is a commutative binary operation. We denote this group by $\mathbf{Z}/N$ and call it the *group* of integers *modulo* N.

Denote by $\mathcal{L}(\mathbf{Z}/N)$ the space of all complex valued functions on $\mathbf{Z}/N$. $\mathcal{L}(\mathbf{Z}/N)$ is the space of N-point data sets.

For $y \in \mathbf{Z}/N$, the mapping $T(y)$ of $\mathcal{L}(\mathbf{Z}/N)$ defined by

$$(T(y)f)(x) = f(x-y), \qquad f \in \mathcal{L}(\mathbf{Z}/N),\ x \in \mathbf{Z}/N,$$

is a linear operator of $\mathcal{L}(\mathbf{Z}/N)$ called *translation* by y.

For $g \in \mathcal{L}(\mathbf{Z}/N)$, the mapping $C(g)$ of $\mathcal{L}(\mathbf{Z}/N)$ defined by

$$C(g) = \sum_{y \in \mathbf{Z}/N} g(y)T(y)$$

is a linear operator of $\mathcal{L}(\mathbf{Z}/N)$ called *convolution* by g. If $f \in \mathcal{L}(\mathbf{Z}/N)$, then

$$(C(g)f)(x) = \sum_{y \in \mathbf{Z}/N} f(x-y)g(y), \qquad x \in \mathbf{Z}/N.$$

1.1 Fourier Analysis

Fourier analysis provides the tools for the detailed analysis and construction of translation-invariant subspaces of $\mathcal{L}(\mathbf{Z}/N)$.

For $y \in \mathbf{Z}/N$, define $\chi_y \in \mathcal{L}(\mathbf{Z}/N)$ by

$$\chi_y(x) = e^{2\pi i \frac{yx}{N}}, \qquad x \in \mathbf{Z}/N.$$

The collection

$$\{\chi_y : y \in \mathbf{Z}/N\}$$

is a basis of $\mathcal{L}(\mathbf{Z}/N)$ called the *exponential basis*.

A mapping $\chi : \mathbf{Z}/N \longrightarrow \mathbf{C}^\times$ is called a *character* of $\mathbf{Z}/N$ if χ satisfies

$$\chi(x+y) = \chi(x)\chi(y), \qquad x,\, y \in \mathbf{Z}/N.$$

$\mathbf{C}^\times$ denotes the set of nonzero complex numbers. Direct computation shows that every exponential function is a character of $\mathbf{Z}/N$. Eventually, we will show that the collection of characters and exponential functions of $\mathbf{Z}/N$ coincide.

We want to show that the characters of $\mathbf{Z}/N$ can be defined in terms of the translations of $\mathcal{L}(\mathbf{Z}/N)$.

Suppose $\mathcal{M}$ is a collection of linear operators of a vector space V. For $M \in \mathcal{M}$, a nonzero vector v in V is called an *M-eigen vector* if there exists $\alpha \in \mathbf{C}$ such that

$$Mv = \alpha v.$$

We call α the *eigen value* of M corresponding to the eigen vector v. A nonzero vector v in V is called an $\mathcal{M}$-eigen vector if v is an M-eigen vector for all $M \in \mathcal{M}$. In this case, there exists a mapping $\alpha : \mathcal{M} \longrightarrow \mathbf{C}$ such that

$$Mv = \alpha(M)v, \qquad M \in \mathcal{M}.$$

A basis of V is called an *$\mathcal{M}$-eigen vector basis* if every vector in the basis is an $\mathcal{M}$-eigen vector. Equivalently, a basis for V is an $\mathcal{M}$-eigen vector basis if and only if the matrix of every $M \in \mathcal{M}$ with respect to the basis is a diagonal matrix.

THEOREM 1 *If χ is a character of $\mathbf{Z}/N$, then χ is a $T(\mathbf{Z}/N)$-eigen vector.*

THEOREM 2 *If f is a $T(\mathbf{Z}/N)$-eigen vector and*

$$T(y)f = \alpha(y)f, \qquad y \in \mathbf{Z}/N,$$

then α is a character of $\mathbf{Z}/N$ and

$$f(y) = \alpha(-y)f(0) = \alpha(y)^* f(0), \qquad y \in \mathbf{Z}/N.$$

Proof

$$f(x-y) = \alpha(y)f(x), \qquad x,\, y \in \mathbf{Z}/N.$$

Setting $y = 0$,

$$f(x) = \alpha(0)f(x), \qquad x \in \mathbf{Z}/N.$$

Since $f \neq 0$, $\alpha(0) = 1$, α is a character of $\mathbf{Z}/N$. Setting $x = 0$ and replacing $-y$ by y completes the proof.

THEOREM 3 *If χ is a $T(\mathbf{Z}/N)$-eigen vector and $\chi(0) = 1$, then χ is a character of $\mathbf{Z}/N$.*

By Theorems 1 and 3 the characters of $\mathbf{Z}/N$ are uniquely characterized as the $T(\mathbf{Z}/N)$-eigen vectors taking the value 1 at the origin of $\mathbf{Z}/N$.

We will now complete the picture and show that the characters of $\mathbf{Z}/N$ form a $T(\mathbf{Z}/N)$-eigen vector basis.

> **Linear algebra theorem** *If $\mathcal{M}$ is a commuting family of linear operators of a vector space V and each $M \in \mathcal{M}$ has finite order, then there exists an $\mathcal{M}$-eigen vector basis.*

THEOREM 4 *The set of characters of $\mathbf{Z}/N$ is a $T(\mathbf{Z}/N)$-eigen vector basis.*

Proof Choose a $T(\mathbf{Z}/N)$-eigen vector basis

$$\{\chi_0, \dots, \chi_{N-1}\}$$

consisting of characters of $\mathbf{Z}/N$. We will show that if χ is character of $\mathbf{Z}/N$, then $\chi = \chi_n$, for some n, $0 \leq n \leq N-1$. Write

$$\chi = \sum_{n=0}^{N-1} \alpha(n)\chi_n, \qquad \alpha(n) \in \mathbf{C},\ 0 \leq n \leq N-1.$$

Without loss of generality, assume $\alpha(0) \neq 0$. For $y \in \mathbf{Z}/N$, since

$$T(y)\chi = \chi(-y)\chi = \sum_{n=0}^{N-1} \alpha(n)\chi_n(-y)\chi_n,$$

we have

$$\chi(-y)\alpha(n) = \chi_n(-y)\alpha(n), \qquad 0 \leq n \leq N-1.$$

Setting $n = 0$, for $y \in \mathbf{Z}/N$,

$$\chi(-y) = \chi_0(-y)$$

implying $\chi = \chi_0$, completing the proof.

2. Abelian Group DSP

Suppose A is an abelian group and $\mathcal{L}(A)$ is the space of all complex valued functions on A.

2.1 Translations

For $y \in A$, the mapping $T(y)$ of $\mathcal{L}(A)$ defined by

$$(T(y)f)(x) = f(y^{-1}x), \quad x \in A,\ f \in \mathcal{L}(A),$$

is a linear operator of $\mathcal{L}(A)$ called *translation* by y.

For $g \in \mathcal{L}(A)$, the mapping $C(g)$ of $\mathcal{L}(A)$ defined by

$$C(g) = \sum_{y \in A} g(y)T(y)$$

is a linear operator of $\mathcal{L}(A)$, called *convolution* by g.

By definition

$$f * g(x) = \sum_{y \in A} f(y)g(y^{-1}x), \quad x \in A.$$

THEOREM 5 *Convolution is a commutative algebra product on $\mathcal{L}(A)$.*

The algebra formed by $\mathcal{L}(A)$ paired with convolution product is called the *convolution algebra* over A.

2.2 Fourier Analysis

Suppose $\mathbf{C}A$ is the group algebra of A.

A mapping $\chi : A \longrightarrow \mathbf{C}^{\times}$ is called a *character* of A if χ satisfies

$$\chi(xy) = \chi(x)\chi(y), \quad x, y \in A.$$

A character of A is simply a group homomorphism from A into $\mathbf{C}^{\times}$.

Denote the set of all characters of A by A^*. Under the identification between $\mathcal{L}(A)$ and $\mathbf{C}A$, every character τ of A can be viewed as a formal sum in $\mathbf{C}A$

$$\tau = \sum_{x \in A} \tau(x)x.$$

Multiplication of characters will always be taken in $\mathbf{C}A$.

EXAMPLE 6 As elements in $\mathbf{C}(C_2 \times C_2)$, the characters of $C_2 \times C_2$ are the formal sums

$$\begin{aligned}
\phi_{0,0} &= 1 + x_1 + x_2 + x_1x_2, \\
\phi_{1,0} &= 1 - x_1 + x_2 - x_1x_2, \\
\phi_{0,1} &= 1 + x_1 - x_2 - x_1x_2, \\
\phi_{1,1} &= 1 - x_1 - x_2 + x_1x_2.
\end{aligned}$$

The mapping $\tau_0 : A \longrightarrow \mathbf{C}^\times$ defined by $\tau_0(x) = 1$, $x \in A$, is a character called the *trivial character* of A. As an element in $\mathbf{C}A$,

$$\tau_0 = \sum_{x \in A} x.$$

The importance of characters in DSP is a result of their invariance under left multiplication as stated in the following theorem.

THEOREM 7 *If $y \in A$ and τ is a character of A, then*

$$y\tau = \tau(y^{-1})\tau.$$

EXAMPLE 8 In $\mathbf{C}C_N$, if

$$\phi_n = \sum_{m=0}^{N-1} v^{nm} x^m, \qquad v = e^{2\pi i \frac{1}{N}},$$

then

$$x^r \phi_n = \sum_{m=0}^{N-1} v^{nm} x^{m+r} = \sum_{m=0}^{N-1} v^{n(m-r)} x^m = v^{-nr} \phi_n.$$

COROLLARY 1.1 *If $f \in \mathbf{C}A$ and τ is a character of A, then*

$$f\tau = \widehat{f}(\tau)\tau,$$

where

$$\widehat{f}(\tau) = \sum_{y \in A} f(y)\tau(y^{-1}).$$

Theorem 7 implies every character τ of A is an $L(A)$-eigen vector,

$$L(y)\tau = y\tau = \tau(y^{-1})\tau, \qquad y \in A.$$

The eigen value of the eigen vector τ of $L(y)$ is $\tau(y^{-1})$.

THEOREM 9 *A^* is the unique $L(A)$-eigen vector basis of $\mathbf{C}A$ satisfying the condition that the value of each basis element is 1 at the identity element 1 of A.*

The Fourier analysis over A will be developed in terms of the properties of the characters of A in $\mathbf{C}A$.

THEOREM 10 *If τ and λ are characters of A, then*

$$\tau\lambda = \begin{cases} N\tau, & \tau = \lambda, \\ 0, & \tau \neq \lambda. \end{cases}$$

A nonzero element e in $\mathbf{C}A$ is called an *idempotent* if $e^2 = e$. Two idempotents e_1 and e_2 in $\mathbf{C}A$ are called *orthogonal* if $e_1e_2 = e_2e_1 = 0$. In the language of idempotent theory Theorem 10 says that the set

$$\left\{ \frac{1}{N}\tau : \tau \in A^* \right\}$$

is a set of pairwise orthogonal idempotents.

Since A^* is a basis of the space $\mathbf{C}A$, we can write

$$1 = \sum_{\tau \in A^*} \alpha(\tau)\tau, \qquad \alpha(\tau) \in \mathbf{C}.$$

For any $\lambda \in A^*$,

$$\lambda = \lambda \cdot 1 = \sum_{\tau \in A^*} \alpha(\tau)\lambda\tau = N\alpha(\lambda)\lambda$$

and $\alpha(\lambda) = \frac{1}{N}$, proving the following.

THEOREM 11

$$1 = \frac{1}{N} \sum_{\tau \in A^*} \tau.$$

A set of pairwise orthogonal idempotents $\mathcal{I}$ in $\mathbf{C}A$ is called *complete* if

$$1 = \sum_{e \in \mathcal{I}} e.$$

In the language of idempotent theory Theorems 10 and 11 say that the set

$$\left\{ \frac{1}{N}\tau : \tau \in A^* \right\}$$

is a complete set of pairwise orthogonal idempotents.

COROLLARY 1.2

$$\frac{1}{N} \sum_{\tau \in A^*} \tau(x) = \begin{cases} 1, & x = 1, \\ 0, & x \neq 1, \end{cases} \quad x \in A.$$

By Corollary 1.1 and completeness every $f \in \mathbf{C}A$ can be written as

$$f = \frac{1}{N} \sum_{\tau \in A^*} f\tau = \frac{1}{N} \sum_{\tau \in A^*} \widehat{f}(\tau)\tau.$$

We call this expansion of f the *Fourier expansion* of f.

$$\widehat{f}(\tau) = \sum_{y \in A} f(y)\tau(y^{-1}), \qquad \tau \in A^*,$$

is called the *Fourier coefficient* of f at τ.

2.3 Character Extensions I

In this chapter we will show that every character of a direct product $A = B \times C$ of abelian groups B and C can be represented as a product in $\mathbf{C}A$ of a character of B with a character of C.

More generally, we will relate the characters of a subgroup of an abelian group to the characters of the group through a construction called *character extensions*. The generalization of this construction to nonabelian groups will occupy a great deal of the later chapters. A is an abelian group throughout this chapter.

2.4 Direct Products

Suppose B is a subgroup of A and ρ is a character of A. The mapping $\rho_B : B \longrightarrow \mathbf{C}^{\times}$ defined by

$$\rho_B(x) = \rho(x), \qquad x \in B,$$

is a character of B called the *restriction* of ρ to B. As an element in $\mathbf{C}A$,

$$\rho_B = \sum_{x \in B} \rho(x)x.$$

THEOREM 12 *Suppose $A = B \times C$. If ρ is a character of A, then $\rho = \rho_B\rho_C$, the product in $\mathbf{C}A$ of the characters ρ_B and ρ_C of B and C defined by the restrictions of ρ.*

By Theorem 12 the character ρ of $A = B \times C$ is represented as a product in $\mathbf{C}A$ of a character of B with a character of C. The representation is unique.

Theorem 12 easily extends to direct product factorizations of A having any number of factors.

EXAMPLE 13 The character

$$1 + x_1 - x_2 - x_1x_2 - x_3 - x_1x_3 + x_2x_3 + x_1x_2x_3$$

of $C_2(x_1) \times C_2(x_2) \times C_2(x_3)$ is the product

$$(1 + x_1)(1 - x_2)(1 - x_3)$$

of the characters $1 + x_1$, $1 - x_2$, $1 - x_3$ of $C_2(x_1)$, $C_2(x_2)$, $C_2(x_3)$.

THEOREM 14 *Suppose $A = B \times C$. If τ and λ are characters of B and C, then the product $\rho = \tau\lambda$ in $\mathbf{C}A$ is a character of A.*

Proof By Theorem 7 if $x = uv$, $u \in B$, $v \in C$, then

$$x\rho = (u\tau)(v\lambda) = \tau(u^{-1})\lambda(v^{-1})\tau\lambda = \rho(x^{-1})\rho,$$

implying ρ is a character of A, completing the proof.

2.5 Character Extensions

Suppose B is a subgroup of A and τ is a character of B. A character ρ of A is called an *extension* of τ if τ is the restriction of ρ to B.

Consider a complete system of B-coset representatives in A,

$$\{y_s : 1 \leq s \leq S\}.$$

Every $x \in A$ can be written uniquely as $x = y_s z$, $1 \leq s \leq S$, $z \in B$. Suppose ρ is an extension of τ. Then

$$\rho = \sum_{x \in A} \rho(x)x = \sum_{s=1}^{S} \sum_{z \in B} \rho(y_s z) y_s z.$$

Since $\rho(y_s z) = \rho(y_s)\rho(z) = \rho(y_s)\tau(z)$,

$$\rho = \left(\sum_{s=1}^{S} \rho(y_s) y_s \right) \left(\sum_{z \in B} \tau(z) z \right) = \left(\sum_{s=1}^{S} \rho(y_s) y_s \right) \tau,$$

proving the following result.

THEOREM 15 *Suppose B is a subgroup of A and τ is a character of B. If ρ is a character of A extending τ, then*

$$\rho = \left(\sum_{s=1}^{S} \rho(y_s) y_s \right) \tau.$$

We can use Theorem 15 to characterize the characters extending τ.

THEOREM 16 *Suppose B is a subgroup of A and τ is a character of B. A character ρ of A is an extension of τ if and only if*

$$\rho = \frac{1}{|B|}\tau\rho.$$

Assume for the rest of this section that B is a subgroup of A. For a character τ of B denote by

$$ext_\tau(A)$$

the collection of all characters of A extending the character τ of B. We will show that there always exists a character of A extending τ and describe $ext_\tau(A)$. If $A = B \times C$, then by Theorems 12 and 14 $ext_\tau(A)$ is the set of all products in $\mathbf{C}A$ of the form $\tau\lambda$, where λ is a character of C.

EXAMPLE 17 The characters of $C_{12}(x)$ extending the character

$$\tau = \sum_{n=0}^{3} v^n x^{3n}, \qquad v = e^{2\pi i \frac{1}{4}},$$

of $C_{12}(x^3)$ have the form

$$\rho_w = \sum_{n=0}^{11} w^n x^n, \qquad w^3 = v.$$

This will be the case if and only if

$$w = e^{2\pi i \frac{1}{12}},\ e^{2\pi i \frac{1}{12}} e^{2\pi i \frac{1}{3}},\ e^{2\pi i \frac{1}{12}} e^{2\pi i \frac{2}{3}}.$$

For each such w we can write the corresponding extension ρ_w as

$$\rho_w = \tau(1 + wx + w^2x^2),$$

which is the factorization of ρ_w given in Theorem 15. In this case we also have the direct product factorization,

$$C_{12}(x) = C_{12}(x^3) \times C_{12}(x^4)$$

and can write

$$\rho_w = \tau(1 + ux^4 + u^2x^8),$$

where

$$1 + ux^4 + u^2x^8$$

is the character of $C_{12}(x^4)$ defined by $u = w^4$.

3. Nonabelian Groups

EXAMPLE 18 The 3×3 cyclic shift matrix

$$S_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

and the 3×3 time-reversal matrix

$$R_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

satisfy the relations

$$S_3^2 = S_3^{-1} \neq I_3, \quad , S_3^3 = I_3 = R_3^2, \quad R_3 S_3 R_3^{-1} = S_3^{-1}.$$

Denote by $\mathcal{D}_6(S_3, R_3)$ the collection of all matrices

$$\{I_3,\ S_3,\ S_3^2;\ R_3,\ S_3R_3,\ S_3^2R_3\}.$$

By the above relations $\mathcal{D}_6(S_3, R_3)$ is closed under matrix multiplication. For example

$$R_3S_3 = S_3^{-1}R_3 = S_3^2R_3.$$

Since $R_3S_3 \neq S_3R_3$, $\mathcal{D}_6(S_3, R_3)$ is a nonabelian group of order 6.

In general we have the following result. Assume $N \geq 3$.

THEOREM 19 *The $N \times N$ cyclic shift matrix S_N and the $N \times N$ time-reversal matrix R_N satisfy the relations $S_N^n \neq I_N$, $0 < n < N$, and*

$$S_N^N = I_N = R_N^2, \quad R_N S_N R_N = S_N^{-1}.$$

The set of all products $\mathcal{D}_{2N}(S_N, R_N)$ of the form

$$\{S_N^n R_N^j : 0 \leq n < N,\ 0 \leq j < 2\}$$

is a nonabelian group of order $2N$.

The group $\mathcal{D}_{2N}(S_N, R_N)$ is a matrix representation of the *dihedral group* of order $2N$.

3.1 Normal Subgroups

Abelian group constructions do not automatically extend to nonabelian groups. The identification of a distinguished class of subgroups, the normal subgroups, is one of the most significant insights in the development of nonabelian group theory.

The concept of a normal subgroup of a nonabelian group G is closely related to a certain class of automorphisms, the inner automorphisms of G. We will discuss these concepts in this section.

Suppose H and K are subgroups of G. We say that K *normalizes* H if

$$yHy^{-1} = H, \quad y \in K.$$

H is a *normal* subgroup of G if G normalizes H.

3.2 Quotient Groups

Suppose, to begin with, that H is any subgroup of G.

For $y \in G$, the set

$$yH = \{yx : x \in H\}$$

is called the *left* H*-coset in* G at y. Right H-cosets can be defined in an analogous manner.

THEOREM 20 *Two left H-cosets are either equal or disjoint.*

The collection of left H-cosets in G forms a partition of G. Denote this collection by G/H and call G/H the *quotient space* of left H-cosets in G.

THEOREM 21 *If y, $z \in G$, then $yH = zH$ if and only if $z^{-1}y \in H$.*

A set

$$\{y_1, \dots, y_R\},$$

formed by choosing exactly one element in each left H-coset is called a *complete system of* left *H-coset representatives* in G.

THEOREM 22 *If H is a normal subgroup of G, then the product*

$$(yH)(zH) = yzH, \quad y,\ z \in G,$$

is a group product on G/H with H as identity element and

$$(yH)^{-1} = y^{-1}H, \quad y \in G.$$

The group G/H is called the *quotient group* of left H-cosets in G.

3.3 Semidirect Product

Suppose H is a normal subgroup of G. We say that G *splits* over H with *complement* K if $G = HK$ and $H \cap K = \{1\}$. If G splits over H with complement K, then we say that G is the *internal semidirect product* $H \triangleleft K$. The usual argument shows that $G = H \triangleleft K$ if and only if every $x \in G$ has a *unique representation* of the form $x = yz$, $y \in H$, $z \in K$. In general, the complement K is not uniquely determined.

If $G = H \triangleleft K$ and K is a normal subgroup of G then $[H, K] = \{1\}$ and G is the direct product $H \times K$. What is new in the internal semidirect product is the possibility that K acts nontrivially on H.

Suppose H and K are groups and

$$\Psi : K \longrightarrow Aut(H)$$

is a group homomorphism. The *semidirect product* $H \triangleleft_{\Psi} K$ is the pair consisting of the cartesian product $H \times K$ and the binary operation

$$(y_1, z_1)(y_2, z_2) = (y_1 \Psi_{z_1}(y_2), z_1 z_2)\,, \qquad y_1,\, y_2 \in H,\; z_1, z_2 \in K.$$

The semidirect product $H \triangleleft_{\Psi} K$ is a group having identity $(1, 1)$ and inverse

$$x^{-1} = \left(\Psi_{z^{-1}}(y^{-1}), z^{-1}\right), \qquad x = (y, z) \in H \triangleleft_{\Psi} K.$$

3.4 Examples: Semidirect product constructions

DSP algorithms will be designed for nonabelian group indexing sets formed mainly by semidirect product constructions. The groups will have the form $A \triangleleft H$, where A is an abelian group.

Consider the ring $\mathbf{Z}/N$ of integers modulo N. An $m \in \mathbf{Z}/N$ is called a *unit* if there exists an $n \in \mathbf{Z}/N$ such that $mn = 1$ in $\mathbf{Z}/N$. A unit in $\mathbf{Z}/N$ is an invertible element relative to multiplication in $\mathbf{Z}/N$. The unit group $U(N)$ can be characterized as the set of all integers $0 < m < N$ such that m and N are relatively prime.

Theorem 23 *The mapping*

$$u \longrightarrow \Psi_u, \qquad u \in U(N),$$

is a group isomorphism from $U(N)$ *onto* $Aut(C_N(x))$.

The group isomorphism in Theorem 23 establishes a one-to-one correspondence between the subgroups of $U(N)$ and those of $Aut(C_N(x))$. Under this identification, we can form $C_N(x) \triangleleft K$ for any subgroup K of $U(N)$ by the group isomorphism throughout this work. A typical point in $C_N(x) \lhd K$ is denoted by (x^m, u), $0 \le m < N$, $u \in K$ with multiplication given by

$$(x^m, u)(x^n, v) = (x^{m+un}, uv), \quad 0 \le m,\, n < N,\, u,\, v \in K,$$

where $m + un$ is taken modulo N. Identifying $C_N(x)$ with the normal subgroup $C_N(x) \times \{1\}$ of $C_N(x) \lhd K$ and K with the subgroup $\{1\} \times K$ of $C_N(x) \lhd K$, we can write

$$x^m u = (x^m, u), \quad 0 \le m < N,\, u \in K. \tag{1}$$

Groups of the form $C_N(x) \lhd K$ will be used in many examples as several DSP concepts are introduced in the following chapters. Although the identification in (1) is unambiguous as a description of an abstract group, we will use the modification,

$$x^m k_u = (x^m, u), \quad 0 \le m < N,\, u \in U(N),$$

with $x^m k_u^j = (x^m, u^j)$.

The reason for this modification is to avoid any confusion or awkward notation in viewing $C_N(x) \lhd K$ as a subset of the group algebra

$$\mathbf{C}(C_N(x) \lhd K).$$

For a prime p the unit group $U(p)$ of $\mathbf{Z}/p$ is a cyclic group of order $p-1$ under multiplication modulo p. Choosing a generator y for $U(p)$, we can write the elements of $U(p)$ as successive powers of y,

$$1,\, y,\, \ldots,\, y^{p-2},$$

with $y^{p-1} = 1$.

A typical point in $G = C_p(x) \lhd U(p)$ can be written as

$$x^m k_y^j, \quad 0 \le m < p,\, 0 \le j < p-1,$$

with y a generator of $U(p)$. Multiplication in G is subject to the relations

$$x^p = 1 = k_y^{p-1}, \quad k_y x = x^y k_y.$$

Other semidirect products can be constructed replacing $U(p)$ by any subgroup of $U(p)$.

Suppose $N = p_1 p_2$, with p_1 and p_2 distinct primes. A number theoretic result asserts that $U(N) = U(p_1) \times U(p_2)$. There exist $y_1,\, y_2 \in U(N)$ such that every $y \in U(N)$ can be written uniquely as

$$y = y_1^{j_1} y_2^{j_2}, \quad 0 \le j_1 < p_1 - 1,\, 0 \le j_2 < p_2 - 1,$$

with $y_1^{p_1-1} = 1 = y_2^{p_2-1}$ and $y_1 y_2 = y_2 y_1$.

EXAMPLE 24 An arbitrary element in the group $C_N(x) \lhd U(N)$, $N = p_1 p_2$, can be written uniquely as

$$x^m k_{y_1}^{j_1} k_{y_2}^{j_2}, \quad 0 \leq m < N,\ 0 \leq j_1 < p_1 - 1,\ 0 \leq j_2 < p_2 - 1,$$

with group multiplication subject to the relations

$$x^N = 1 = k_{y_1}^{p_1-1} = k_{y_2}^{p_2-1},$$

$$k_{y_1} x = x^{y_1} k_{y_1}, \quad k_{y_2} x = x^{y_2} k_{y_2}, \quad k_{y_1} k_{y_2} = k_{y_2} k_{y_1}.$$

Consider the abelian group $C_N(x) \times C_N(y)$. Under the usual identifications, we can write a typical point as $x^m y^n$, $0 \leq m,\ n < N$, subject to the relations $x^N = 1 = y^N$ and $xy = yx$. We begin our discussion of $Aut(C_N(x) \times C_N(y))$ by extending the concept of a unit group to matrices.

The set $M(2, \mathbf{Z}/N)$ of all 2×2 matrices over $\mathbf{Z}/N$ is a ring with respect to matrix addition and matrix multiplication. The arithmetic required for the matrix addition and multiplication is taken in $\mathbf{Z}/N$. I_2 denotes the identity matrix in $M(2, \mathbf{Z}/N)$. A matrix $L \in M(2, \mathbf{Z}/N)$ is called a *unit* if there exists $L' \in M(2, \mathbf{Z}/N)$ such that $LL' = I_2 = L'L$. L' is called the inverse of L in $M(2, \mathbf{Z}/N)$ and is uniquely determined when it exists. If L is a unit in $M(2, \mathbf{Z}/N)$, we denote by L^{-1} the inverse of L. If L_1 and L_2 are units, then

$$(L_1 L_2)(L_2^{-1} L_1^{-1}) = I_2 = (L_2^{-1} L_1^{-1}) L_1 L_2$$

and $L_1 L_2$ is a unit with inverse $L_2^{-1} L_1^{-1}$. The set $GL(2, \mathbf{Z}/N)$ of all units in $M(2, \mathbf{Z}/N)$ is a group under matrix multiplication in $M(2, \mathbf{Z}/N)$. We call $GL(2, \mathbf{Z}/N)$ the *unit group* in $M(2, \mathbf{Z}/N)$. $GL(2, \mathbf{Z}/N)$ can be characterized as the set of all $L \in M(2, \mathbf{Z}/N)$ such that $det(L) \in U(N)$. $det(L)$ is defined by the same formula for complex matrices but with arithmetic operations taken in $\mathbf{Z}/N$.

For

$$L = \begin{bmatrix} L_1 & L_2 \\ L_3 & L_4 \end{bmatrix} \in M(2, \mathbf{Z}/N),$$

define $\Psi_L : C_N(x) \times C_N(y) \longrightarrow C_N(x) \times C_N(y)$ by

$$\Psi_L(x^m y^n) = x^{L_1 m + L_2 n} y^{L_3 m + L_4 n}, \quad 0 \leq m,\ n < N.$$

Ψ_L is uniquely determined by its values on the generators x and y,

$$\Psi_L(x) = x^{L_1} y^{L_3}, \quad \Psi_L(y) = x^{L_2} y^{L_4}.$$

THEOREM 25 *The mapping*

$$L \longrightarrow \Psi_L, \quad L \in GL(2, \mathbf{Z}/N),$$

is a group isomorphism from $GL(2, \mathbf{Z}/N)$ *onto* $Aut(C_N(x) \times C_N(y))$.

Under the group isomorphism in Theorem 25, there is a one-to-one correspondence between the subgroups of $GL(2, \mathbf{Z}/N)$ and the subgroups of $Aut(C_N(x) \times C_N(y))$ and we can form

$$(C_N(x) \times C_N(y)) \triangleleft K,$$

for any subgroup K of $GL(2, \mathbf{Z}/N)$. A typical point is denoted by $(x^m y^n, L)$, $0 \leq m,\ n < N$, $L \in K$ with multiplication given by

$$(x^m y^n, L)(x^{m'} y^{n'}, L') = (x^{m''} y^{n''}, L''),$$

where

$$m'' = m + L_1 m' + L_2 n', \quad n'' = n + L_3 m' + L_4 n',\ L = \begin{bmatrix} L_1 & L_2 \\ L_3 & L_4 \end{bmatrix},$$

and $L'' = LL'$. Under the usual identifications, we can write

$$x^m y^n L = (x^m y^n, L), \quad 0 \leq m,\ n < N,\ L \in K.$$

As before, to avoid awkward notation in the group algebra setting, we will use the modified identification,

$$x^m y^n k_L = (x^m, y^n, L), \quad 0 \leq m,\ n < N,\ L \in GL(2, \mathbf{Z}/N).$$

The discussion extends to any number of cyclic group factors as long as each factor has the same order.

3.5 Nonabelian Group DSP

The new problem raised by noncommutativity is that the characters no longer form a basis of nonabelian group algebras. As a result, there exist multidimensional irreducible ideals. Throughout G is an arbitrary nonabelian group of order N and $\mathbf{C}G$ is its group algebra.

EXAMPLE 26 The dihedral group $\mathcal{D}_{2N} = \mathcal{D}_{2N}(x, k_{N-1})$ is the set of products $x^m k_{N-1}^j$, $0 \leq m < N$, $0 \leq j < 2$, with multiplication subject to the relations

$$x^N = 1 = k_{N-1}^2, \quad k_{N-1} x = x^{-1} k_{N-1}.$$

The group algebra $\mathbf{C}\mathcal{D}_{2N}$ is the set of polynomials of the form

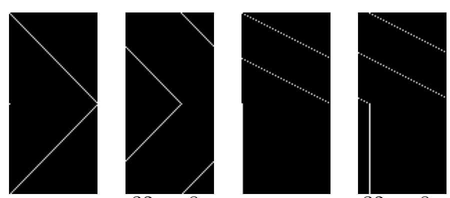
$$\sum_{m=0}^{N-1}\sum_{j=0}^{1} a_{m,j}x^m k_{N-1}^j, \qquad a_{m,j} \in \mathbf{C},$$

with polynomial multiplication subject to the relations given for the group $\mathcal{D}_{2N}$.

EXAMPLE 27 Set $A = C_N(x) \times C_N(y)$, $G = A \rtimes C_2(k_c)$, where $c = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$.

In Figure 1 we display lines indexed by G and their translations under multiplications by elements from G.

Figure 1. An image and its translates in $\mathbf{C}G_4$, $N = 64$



$\mathbf{f}$ $\quad x^{32}y^{-8}\mathbf{f}$ $\quad k_c\mathbf{f}$ $\quad x^{32}y^{-8}k_c\mathbf{f}$

In the following figures, we show the effects of replacing k_c by other elements of $GL(2, \mathbf{Z}/N)$ of order 2.

Set

$$b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The first image in Figure 2 is the same as in Figure 1. The remaining images are its translates by left multiplications of elements of $A \rtimes C_2(k_b)$.

Figure 2. An image and its translates in $\mathbf{C}(A \rtimes C_2(k_b))$, $N = 64$

$\mathbf{f}$ $\quad x^{32}y^{-8}\mathbf{f}$ $\quad k_b\mathbf{f}$ $\quad x^{32}y^{-8}k_b\mathbf{f}$

$G_5 = A \triangleleft C_6(k_d)$, where $A = C_N(x) \times C_N(y)$, $N = 3 \cdot 2^K$ for an integer $K \geq 2$. Set $M = 2^K$.

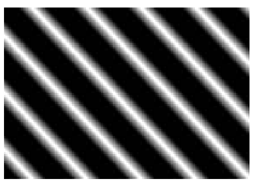
$$d = \begin{bmatrix} -1 & M+1 \\ M-1 & M \end{bmatrix}.$$

Order G_5 by

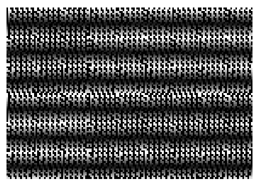
$$\begin{bmatrix} A & Ak_d^2 & Ak_d^4 \\ Ak_d^3 & Ak_d^5 & Ak_d \end{bmatrix},$$

where A is ordered as before. Figure 3 is an example of translations of data indexed by G_5, $M = 16$. Starting with the top left image as an element in $\mathbf{C}G_5$, the remaining 5 images are obtained by left multiplication by successive powers of k_d.

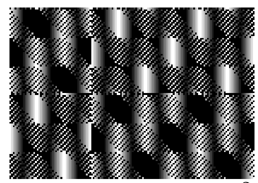
Figure 3. Translations by $C_6(k_d)$



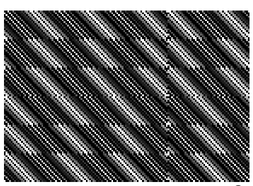
original image



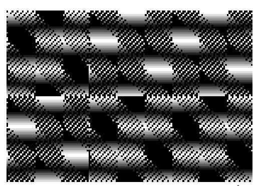
translation by k_d



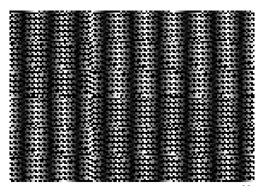
translation by k_d^2



translation by k_d^3



translation by k_d^4

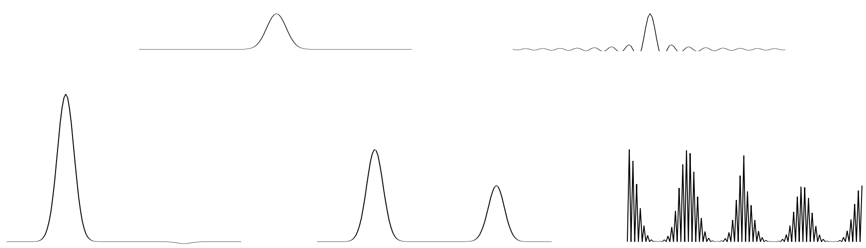


translation by k_d^5

Example 28 Varying group structures are placed on an indexing set of data, and products are computed corresponding to the group algebra. G_1 is the abelian group $C_{2N}(x)$, where G_1 is indexed by the successive powers of x. G_2 is the dihedral group $\mathcal{D}_{2N}(x, k_{N-1})$. G_3 is constructed as follows: For $N = 2^M$, $M \in \mathbf{Z}$, $M \geq 2$, $(\frac{N}{2}+1)^2 \equiv 1 \bmod N$; $\frac{N}{2}+1$ generates a subgroup of $U(N)$ of order 2. Set $G_3 = C_N(x) \triangleleft \{1, k_{\frac{N}{2}+1}\}$, $\frac{N}{2}+1 \in U(N)$. The product in $\mathbf{C}G_3$ is governed by the relations

$$x^N = k_{\frac{N}{2}+1} = 1, \qquad k_{\frac{N}{2}+1} x = x^{\frac{N}{2}+1} k_{\frac{N}{2}+1}.$$

Figure 4. Group algebra products



G_3 is indexed by

$$1, x, \ldots, x^{N-1};\ k_{\frac{N}{2}+1}, xk_{\frac{N}{2}+1}, \ldots, x^{N-1}k_{\frac{N}{2}+1}.$$

Note that G_2 and G_3 are isomorphic groups.

For $N = 64$, the first two plots in Figure 4 are those of 128 points of data. The product in G_1 is the usual cyclic convolution of two sets of data and displayed in the third plot. The 4th and 5th plots are those of group algebra products in $\mathbf{C}G_2$ and $\mathbf{C}G_3$.

For $N = 128$, each of the groups determines an indexing of data of size 256. The first plots in 5 are those of 256 points of data. The product in G_1 is the usual cyclic convolution of two sets of data and displayed in the third plot. The remaining plots are those of group algebra products in $\mathbf{C}G_2$ and $\mathbf{C}G_3$.

Example 29 Varying group structures are placed on the indexing set of two-dimensional data, and products are computed corresponding to the group algebra. For $0 \leq m, n < N$, place the lexicographic ordering on the pair (m, n). G_1 is the abelian group $C_N(x) \times C_{2N}(y)$ with two-dimensional ordering given by

$$(x^m, y^n);\ (x^m, y^{n+N}).$$

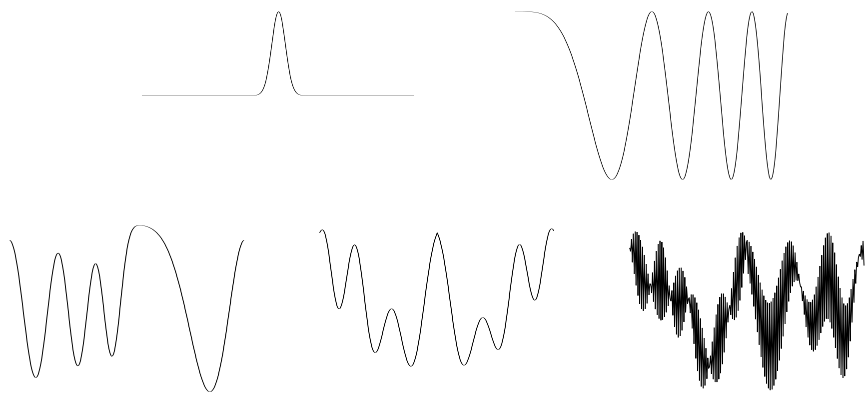
G_2 is the abelian group $(C_N(x) \times C_N(y)) \times C_2(z)$ with two-dimensional ordering given by

$$(x^m, y^n);\ (x^m, y^n z).$$

$G_3 = (C_N(x) \times C_N(y)) \triangleleft \{I_2, k_z\},\ z = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. The ordering of G_3 is the two-dimensional ordering given by

$$(x^m, y^n);\ (x^m, y^n k_z).$$

Figure 5. Group algebra products



G_4 is the nonabelian group $(C_N(x) \times C_N(y)) \triangleleft \{I_2, k_u\}$, $u = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2, \mathbf{Z}/N)$. The ordering of G_4 is the two-dimensional ordering given by

$$(x^m, y^n);\ (x^m, y^n k_u).$$

For $N = 32$, each of the groups determines indexing of data of size 32×64. Images in Figure 6 are log scaled intensity plots of data of size 32×64. Images in Figure 7 are convolutions of images in Figure 6 in $\mathbf{C}G_1$, $\mathbf{C}G_2$, $\mathbf{C}G_3$ and $\mathbf{C}G_4$.

3.6 Fourier Analysis

A mapping $\rho : G \longrightarrow \mathbf{C}^{\times}$ is called a *character* of G if it satisfies

$$\rho(xy) = \rho(x)\rho(y), \qquad x,\ y \in G. \tag{2}$$

A character of G is simply a group homomorphism of G into $\mathbf{C}^{\times}$. In group representation theory the more general concept of a character of a group representation of G is defined and characters as defined in (2) are called *one-dimensional characters.* We will not use this general concept.

Figure 6. Images of size 32×64

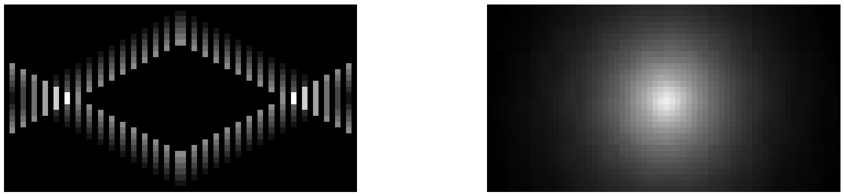
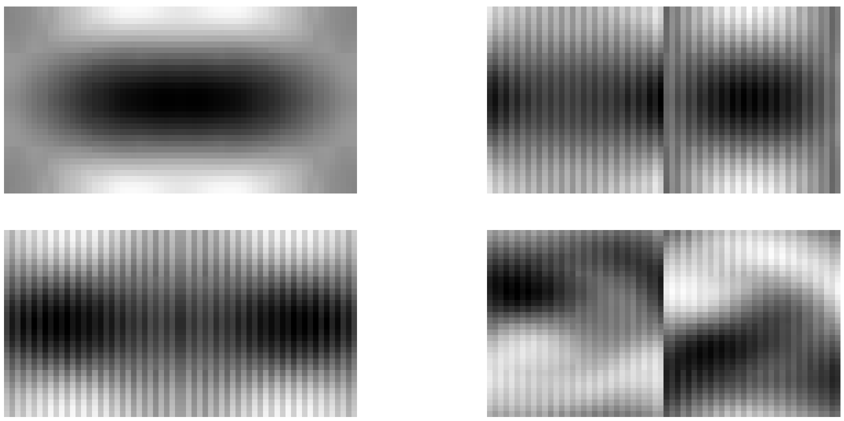


Figure 7. Group algebra products



Characters of nonabelian groups are more difficult to describe than in the abelian group case. There always exists a character, the *trivial character* of G, which takes on the value 1 at all points of G.

Denote the collection of all characters of G by G^*. We can view a character ρ of G as a formal sum in $\mathbf{C}G$,

$$\rho = \sum_{x \in G} \rho(x)x,$$

and G^* as a subset of $\mathbf{C}G$.

THEOREM 30 *Suppose ρ is a character of G. If $t \in G$,*

$$t\rho = \rho t = \rho(t^{-1})\rho.$$

COROLLARY 1.3 *Suppose ρ is a character of G. If $f \in \mathbf{C}G$, then*

$$f\rho = \rho f = \widehat{f}(\rho)\rho,$$

where $\widehat{f}(\rho) = \sum_{t\in G} f(t)\rho(t^{-1})$.

Theorem 30 leads to an important formula for the product of two characters in $\mathbf{C}G$.

THEOREM 31 *For characters* ρ *and* λ *of* G,

$$\rho\lambda = \begin{cases} N\rho, & \rho = \lambda, \\ 0 & \rho \neq \lambda. \end{cases}$$

3.7 Character Extensions II

Methods will be developed for constructing characters of nonabelian groups having semidirect product representations. For a group $G = H \lhd K$, the strategy is to begin with a character τ of H, determine if τ has an extension to a character of G and if it does, construct the collection of all characters of G extending τ.

An arbitrary character τ of H does not necessarily extend to a character of $G = H \lhd K$.

We assume that H is a normal subgroup of G throughout this paper. In Section 3.9, when required, we will explicitly assume that H splits in G and $G = H \lhd K$.

3.8 Group Action

For $y \in G$ and $f \in \mathbf{C}G$, define $f^y \in \mathbf{C}G$ by

$$f^y = yfy^{-1} = \sum_{x\in G} f(x)yxy^{-1}.$$

Two characters τ_1 and τ_2 of H are said to be *conjugate* in G if there exists $y \in G$ such that $\tau_2 = \tau_1^y$. Conjugacy is an equivalence relation on the set H^* of all characters of H.

Suppose τ is a character of H and $G(\tau)$ its centralizer in G. Choose a complete system of left $G(\tau)$-coset representatives in G,

$$\{y_s : 1 \leq s \leq S\}.$$

Every $y \in G$ can be uniquely written as

$$y = y_s z, \quad 1 \leq s \leq S,\ z \in G(\tau).$$

Define the conjugates τ_s, $1 \leq s \leq S$, of τ by

$$\tau_s = y_s \tau y_s^{-1}, \quad 1 \leq s \leq S. \tag{3}$$

THEOREM 32 *If τ is a character of H, the conjugates τ_s, $1 \leq s \leq S$, of τ defined by (3) are distinct characters of H and the set*

$$\{\tau_s : 1 \leq s \leq S\}$$

is the collection of all conjugates of τ in G.

Proof Suppose $y \in G$ and write $y = y_s z$, $1 \leq s \leq S$, $z \in G(\tau)$. Since $G(\tau)$ centralizes τ,

$$y\tau y^{-1} = y_s z\tau z^{-1} y_s^{-1} = y_s \tau y_s^{-1} = \tau_s$$

and every conjugate of τ in G is of the form τ_s, $1 \leq s \leq S$. If $\tau_s = \tau_t$, $1 \leq s,\, t \leq S$, then

$$\tau = y_s^{-1} y_t \tau y_t^{-1} y_s.$$

This implies $y_s^{-1} y_t \in G(\tau)$ and $y_s = y_t$, completing the proof.

By Theorem 31 we have the following corollary.

COROLLARY 1.4 *If $1 \leq s,\, t \leq S$ and $s \neq t$, then $\tau_s\tau_t = \tau_t\tau_s = 0$.*

The characters ϕ_n, $0 \leq n < M$, of $C_M(x)$ are defined by

$$\phi_n(x^m) = v^{nm}, \quad 0 \leq m < M,\, v = e^{2\pi i \frac{1}{M}}.$$

If $0 \leq n < N$ and $m \in U(M)$, then since

$$\phi_n^{k_m}(x) = \phi_n(x^m) = \phi_{nm}(x),$$

the set

$$\{\phi_{nm} : m \in U(M)\} \tag{4}$$

is the set of conjugates of ϕ_n in $C_M(x) \lhd U(M)$. The product nm is taken modulo M. (4) is called the *conjugacy class* of ϕ_n in $C_M \lhd U(M)$.

3.9 Character Extension

Throughout this section H is a normal subgroup of G and K is an arbitrary subgroup of G. Following Corollary 1.5, we assume $G = H \lhd K$. The main results on character extensions will be proved under this assumption.

Suppose ρ is a character of K. We say that ρ *extends to a character* of G if there exists a character γ of G such that ρ is the restriction of γ to K. Generally, even if K is a normal subgroup of G, a character ρ of

K will not necessarily extend to a character of G. This obstruction is a major difference between the abelian and the nonabelian group cases.

The following result establishes a necessary condition for a character τ of the normal subgroup H of G to have an extension to a character of G. For groups of the form $G = H \triangleleft K$, it is also a sufficient condition.

THEOREM 33 *If a character τ of H extends to a character of G, then G centralizes τ.*

THEOREM 34 *If τ is a character of H and G_1 is a subgroup of G containing H such that τ extends to a character of G_1, then $G_1 \subset G(\tau)$.*

As a special case, we have the following corollary.

COROLLARY 1.5 *If τ is a character of H and $H = G(\tau)$, then τ cannot be extended to a character of any subgroup of G strictly containing H.*

In the language introduced below, if τ is a character of H such that $H = G(\tau)$, then τ is a maximal character in G.

Assume $G = H \triangleleft K$ for the rest of this chapter. A typical point $x \in G$ will be written uniquely as

$$x = uv, \qquad u \in H,\ v \in K,$$

with the understanding that $u = u \cdot 1$ and $v = 1 \cdot v$.

THEOREM 35 *If τ is a character of H centralized by K, then every product $\tau\lambda$, where λ is a character of K, is a character of G extending τ.*

Proof Choose any character λ of K and form the product $\rho = \tau\lambda$. We must show ρ is a character of G. Since $v\tau = \tau v$, $v \in K$, we have

$$x\rho = uv\tau\lambda = (u\tau)(v\lambda), \qquad x = uv,\ u \in H, v \in K.$$

By Theorem 30

$$x\rho = \tau(u^{-1})\lambda(v^{-1})\tau\lambda = \rho(x^{-1})\rho,$$

and ρ is an $L(G)$-eigen vector. Since $\rho(1) = 1$, ρ is a character of G, completing the proof.

COROLLARY 1.6 *If τ is a character of H, then τ extends to a character of G if and only if K centralizes τ.*

Theorem 35 describes a procedure for constructing characters of G extending a character τ of H centralized by K. In fact all the characters of G extending τ are constructed in this way. For each character τ of H centralized by K denote by

$$ext_\tau(G)$$

the collection of all characters of G extending τ.

THEOREM 36 *If τ is a character of H centralized by K, then $ext_\tau(G)$ is the collection of all products $\tau\lambda$, where λ is a character of K.*

The collection G^* of all characters of G is the disjoint union of the sets

$$ext_\tau(G), \qquad \tau \in H^* \text{ and } \tau \text{ centralized by } K.$$

EXAMPLE 37 If p is prime, there are $p-1$ characters of the group $C_p(x) \rtimes U(p)$. The only character of $C_p(x)$ which extends to $C_p(x) \rtimes U(p)$ is the trivial character ϕ_0. Since $U(p)$ has order $p-1$, there are $p-1$ characters λ_j, $0 \le j < p-2$, of $U(p)$. The group algebra products

$$\phi_0\lambda_j, \qquad 0 \le j < p-2,$$

are the $p-1$ characters of $C(p) \rtimes U(p)$.

EXAMPLE 38 For $N \ge 2$, the characters of the normal subgroup

$$C_N(x) = \{x^m : 0 \le m < N\}$$

of the dihedral group $\mathcal{D}_{2N} = \mathcal{D}_{2N}(x, k_{N-1})$ are given by $\phi_n : C_N(x) \longrightarrow U_N$, $0 \le n < N$,

$$\phi_n(x^m) = v^{nm}, \qquad 0 \le m < N,\ v = e^{2\pi i \frac{1}{N}}.$$

Since $\mathcal{D}_{2N} = C_N(x) \rtimes K$, where $K = \{1, k_{N-1}\}$ and

$$k_{N-1} x k_{N-1}^{-1} = x^{-1},$$

ϕ_n is centralized by K if and only if $v^n = e^{2\pi i \frac{n}{N}}$ is real. For N odd, we must have $n = 0$ and the trivial character ϕ_0 is the only character of $C_N(x)$ centralized by K. If N is odd, $\mathcal{D}_{2N}$ has two characters, the trivial character and the character ρ_1 defined by

$$\rho_1(x^m k_{N-1}^j) = (-1)^j, \qquad 0 \le m < N,\ 0 \le j < 2.$$

For N even, we must have $n = 0$ or $n = \frac{N}{2}$ and the trivial character ϕ_0 and the character $\phi_{\frac{N}{2}}$ are the only characters of $C_N(x)$ centralized by

K. If N is even, $\mathcal{D}_{2N}$ has four characters, the trivial character ρ_0 and the three characters defined by

$$\rho_1(x^m k_{N-1}^j) = (-1)^j,\ \rho_2(x^m k_{N-1}^j) = (-1)^m,\ \rho_3(x^m k_{N-1}^j) = (-1)^{m+j},$$
$$0 \le m < N,\ 0 \le j < 2.$$

3.10 Maximal Extensions

We continue to assume that $G = H \triangleleft K$. If a character τ of H is *not* centralized by K, then τ cannot be extended to a character of G. Since H is a subgroup of $G(\tau)$, $G(\tau)$ has the form

$$G(\tau) = H \triangleleft K(\tau),$$

where $K(\tau)$ is the centralizer of τ in K,

$$K(\tau) = \{v \in K : v\tau v^{-1} = \tau\}.$$

THEOREM 39 *If τ is a character of H, then τ extends to a character of $G(\tau) = H \triangleleft K(\tau)$.*

Denote by

$$ext_\tau(G(\tau))$$

the collection of all characters of $G(\tau)$ extending τ.

THEOREM 40 *If τ is a character of H, then $ext_\tau(G(\tau))$ is the collection of all products in $\mathbf{C}G$ of the form $\tau\lambda$, where λ is a character of $K(\tau)$.*

For future use we have the following corollary.

COROLLARY 1.7 *If τ is a character of H, then*

$$\sum_{\rho \in ext_\tau(G(\tau))} \rho = \tau \sum_{\lambda \in K(\tau)^*} \lambda.$$

Suppose G_1 is an arbitrary group and K_1 is a subgroup of G_1. A character γ of K_1 is called a *maximal character* in G_1 if γ has no extension to a character of a subgroup of G_1 strictly containing K_1. Any extension of a character γ of K_1 to a maximal character in G_1 is called a *maximal extension* of γ in G_1.

THEOREM 41 *If τ is a character of H then $ext_\tau(G(\tau))$ is a collection of maximal extensions of τ in G.*

We will show that the left ideal generated by a maximal character is irreducible.

Suppose τ is a character of H and ρ is a character of $G(\tau)$ extending τ. $G(\tau)$ is not necessarily a normal subgroup of G. Consider the centralizer $G(\rho)$ of ρ in G. Since the support of ρ is $G(\tau)$, $G(\rho)$ normalizes $G(\tau)$,

$$yzy^{-1} \in G(\tau), \quad z \in G(\tau),\ y \in G(\rho).$$

$G(\tau)$ centralizes ρ implying $G(\tau)$ is a normal subgroup of $G(\rho)$.

THEOREM 42 *If τ is a character of H and ρ is a character of $G(\tau)$ extending τ, then $G(\rho) = G(\tau)$.*

3.11 Abelian by Abelian Semidirect Products

Groups of the form $G = A \triangleleft B$ with A and B abelian groups are perhaps the simplest generalizations of abelian groups. Not surprisingly, the DSP of this class of groups closely resembles that of abelian groups.

We proved that each character τ of A extends to a character of the centralizer $G(\tau) = A \triangleleft B(\tau)$ and that the set $ext_\tau(G(\tau))$ of all characters of $G(\tau)$ extending τ consists of maximal characters in G.

3.12 $EXT(G, A)$

Suppose τ is a character of A. The centralizer of τ in G is $G(\tau) = A \triangleleft B(\tau)$. Denote by

$$ext_\tau(G(\tau))$$

the collection of all extensions of τ to characters of $G(\tau)$.

Denote by

$$EXT(G, A)$$

the union of the sets $ext_\tau(G(\tau))$ as τ runs over all characters of A. By Theorem 41 every character γ in $ext_\tau(G(\tau))$ is a maximal extension of τ and $EXT(G, A)$ consists of maximal characters in G.

EXAMPLE 43 If $G = C_p(x) \triangleleft U(p)$, p a prime, $EXT(G, C_p(x))$ has order $2(p-1)$. The characters ϕ_n, $0 < n < p$, of $C_p(x)$ are maximal characters in G. The trivial character ϕ_0 extends to $p - 1$ characters of G.

EXAMPLE 44 If $G = C_8(x) \triangleleft U(8)$, $EXT(G, C_8(x))$ has order 16. The characters ϕ_1, ϕ_3, ϕ_5 and ϕ_7 of $C_8(x)$ are maximal characters in G. As elements of $\mathbf{C}G$ they can be written explicitly as

$$\begin{bmatrix} \phi_1 \\ \phi_3 \\ \phi_5 \\ \phi_7 \end{bmatrix} = \begin{bmatrix} 1 & v & v^2 & v^3 & v^4 & v^5 & v^6 & v^7 \\ 1 & v^3 & v^6 & v & v^4 & v^7 & v^2 & v^5 \\ 1 & v^5 & v^2 & v^7 & v^4 & v & v^6 & v^3 \\ 1 & v^7 & v^6 & v^5 & v^4 & v^3 & v^2 & v \end{bmatrix} \begin{bmatrix} 1 \\ x \\ \vdots \\ x^7 \end{bmatrix}.$$

The character ϕ_2 of $C_8(x)$ has two maximal extensions in G to characters of $C_8(x) \lhd K_2$, $K_2 = \{1, 5\}$. A similar remark can be made for the character ϕ_6. The characters ϕ_0 and ϕ_4 of $C_8(x)$ extend to eight characters of G.

The first result extends, to the characters in $EXT(G, A)$, the product formula of Theorem 9 for characters of abelian groups.

For $f \in \mathbf{C}G$ set $|f|$ equal to the order of the support of f.

Theorem 45 *If* γ_1, $\gamma_2 \in EXT(G, A)$, *then*

$$\gamma_1\gamma_2 = \begin{cases} |\gamma_1|\gamma_1, & \gamma_1 = \gamma_2, \\ 0, & \gamma_1 \neq \gamma_2. \end{cases}$$

In the language of idempotent theory a nonzero element $e \in \mathbf{C}G$ is called an *idempotent* if $e^2 = e$. Two idempotents e_1 and e_2 in $\mathbf{C}G$ are called *orthogonal* if $e_1e_2 = e_2e_1 = 0$. Theorem 45 says that

$$\left\{ \frac{1}{|\gamma|}\gamma \in EXT(G, A) \right\}$$

is a set of pairwise orthogonal idempotents. Using the language of idempotents, we call $EXT(G, A)$ a *set of pairwise orthogonal characters* in G.

The next result extends Theorem 11 to $EXT(G, A)$.

Theorem 46

$$1 = \sum_{\gamma \in EXT(G,A)} \frac{1}{|\gamma|}\gamma.$$

A set $\mathcal{I}$ of pairwise orthogonal idempotents is said to be *complete* if

$$1 = \sum_{e \in \mathcal{I}} e.$$

Theorems 45 and 46 say that the set

$$\left\{ \frac{1}{|\gamma|}\gamma : \gamma \in EXT(G, A) \right\}$$

is a complete set of pairwise orthogonal idempotents. Using the language of idempotents, we call $EXT(G, A)$ a *complete set of pairwise orthogonal characters* in G.

Arguing as before, we have the following result.

Theorem 47

$$\mathbf{C}G = \bigoplus_{\gamma \in EXT(G,A)} \mathbf{C}G\gamma.$$

3.13 A Basis of $\mathbf{C}G\gamma$

Suppose $\gamma \in EXT(G, A)$. We will show that $\mathbf{C}G\gamma$ can be multidimensional, determine the dimension of $\mathbf{C}G\gamma$ and construct a basis of $\mathbf{C}G\gamma$. In the next section we will show $\mathbf{C}G\gamma$ is irreducible.

Choose a complete system of left $G(\gamma)$-coset representatives in G,

$$\{y_s : 1 \le s \le S\}. \tag{5}$$

In general this system depends on γ. Since $G(\gamma)$ is a normal subgroup of G, by Theorem 32

$$\gamma_s = y_s \gamma y_s^{-1}, \quad 1 \le s \le S,$$

is the set of all conjugates of γ in G and

$$\gamma_{s_1}\gamma_{s_2} = 0, \quad 1 \le s_1,\ s_2 \le S,\ s_1 \ne s_2.$$

THEOREM 48 *If $\gamma \in EXT(G, A)$, then*

$$\{y_s\gamma : 1 \le s \le S\}$$

is a basis of the space $\mathbf{C}G\gamma$.

Proof Suppose $x \in G$ and write $x = y_s z$, $1 \le s \le S$, $z \in G(\gamma)$. By Theorem 30

$$x\gamma = y_s z\gamma = \gamma(z^{-1}) y_s \gamma.$$

Since the elements $x\gamma$, $x \in G$, span $\mathbf{C}G\gamma$, the elements $y_s\gamma$, $1 \le s \le S$, span $\mathbf{C}G\gamma$.

To prove linear independence, suppose

$$0 = \sum_{s=1}^{S} \alpha(s) y_s \gamma, \quad \alpha(s) \in \mathbf{C}.$$

For any t, $1 \le t \le S$,

$$0 = \gamma_t\, 0 = \sum_{s=1}^{S} \alpha(s)\gamma_t\gamma_s y_s = |\gamma|\alpha(t) y_t \gamma$$

implying

$$\alpha(t) = 0, \quad 1 \le t \le S,$$

completing the proof.

The basis of $\mathbf{C}G\gamma$

$$\{y_s\gamma : 1 \le s \le S\}$$

will be denoted by $BAS(\gamma)$. It consists of the left multiplications of γ by the system (5). The basis of $\mathbf{C}G$ formed by the union of the sets $BAS(\gamma)$, $\gamma \in EXT(G, A)$, will be denoted by $BAS(G, A)$.

3.14 Irreducibility of $\mathbf{C}G\gamma$

THEOREM 49 *If $\gamma \in EXT(G,A)$, then $\mathbf{C}G\gamma$ is an irreducible left ideal.*

Proof We continue to assume that $\{y_s : 1 \leq s \leq S\}$ is a complete system of left $G(\gamma)$-coset representatives in G. Suppose V is a nonzero left ideal in $\mathbf{C}G\gamma$ and $f \in V$, $f \neq 0$. By Theorem 48

$$f = \sum_{s=1}^{S} \alpha(s) y_s \gamma,$$

where $\alpha(s_1) \neq 0$ for some $1 \leq s_1 \leq S$. Theorems 45 and 31 imply

$$\gamma_{s_1} f = \sum_{s=1}^{S} \alpha(s) \gamma_{s_1} y_s \gamma = \sum_{s=1}^{S} \alpha(s) \gamma_{s_1} \gamma_s y_s = \alpha(s_1)|\gamma| \gamma_{s_1} y_{s_1}.$$

Since V is a left ideal and $f \in V$, $\gamma_{s_1} y_{s_1} \in V$ and

$$\gamma = y_{s_1}^{-1} \gamma_{s_1} y_{s_1} \in V$$

implying $V = \mathbf{C}G\gamma$, completing the proof.

3.15 Expansion Coefficients

A formula will be derived for the expansion coefficients of $f \in \mathbf{C}G$ relative to the basis $BAS(G,A)$. An algorithm implementing this formula will be constructed by making explicit the relationship between the characters of A and $EXT(G,A)$.

Suppose $\gamma \in EXT(G,A)$. Choose a complete system of left $G(\gamma)$-coset representatives in G,

$$y_s(\gamma), \quad 1 \leq s \leq S(\gamma).$$

The dependence of the system on γ is now explicitly expressed. The basis $BAS(G,A)$ of $\mathbf{C}G$ consists of all elements of the form

$$y_s(\gamma)\gamma, \quad \gamma \in EXT(G,A),\ 1 \leq s \leq S(\gamma).$$

The expansion of $f \in \mathbf{C}G$ relative to this basis will be written as

$$f = \sum_{\gamma \in EXT(G,A)} \sum_{s=1}^{S(\gamma)} f_\gamma(s) y_s(\gamma)\gamma.$$

In this section we derive a formula for the expansion coefficients

$$f_\gamma(s), \quad \gamma \in EXT(G,A),\ 1 \leq s \leq S(\gamma).$$

In the next section we will use this formula to derive a fast Fourier-like algorithm to compute these expansion coefficients.

By Theorem 45 if $f \in \mathbf{C}G$ and $\gamma \in EXT(G, A)$, then

$$f\gamma = |\gamma| \sum_{s=1}^{S(\gamma)} f_\gamma(s) y_s(\gamma)\gamma. \tag{6}$$

The expansion coefficients of the component of f in $\mathbf{C}G\gamma$ relative to the basis $BAS(\gamma)$ are given by $f_\gamma(s)$, $1 \le s \le S(\gamma)$.

THEOREM 50 *If* $f \in \mathbf{C}G$ *and* $\gamma \in EXT(G, A)$, *then*

$$f_\gamma(s) = \frac{1}{|\gamma|} \sum_{z \in G(\gamma)} f(y_s(\gamma)z)\gamma(z^{-1}), \qquad 1 \le s \le S(\gamma).$$

Proof Set $y_s = y_s(\gamma)$ and $S = S(\gamma)$ throughout the proof. For $x \in G$, write $x = y_s z$, $1 \le s \le S$, $z \in G(\gamma)$, and

$$f = \sum_{x \in G} f(x)x = \sum_{s=1}^{S} \sum_{z \in G(\gamma)} f(y_s z) y_s z.$$

Since by Theorem 30, $y_s z\gamma = \gamma(z^{-1}) y_s \gamma$, we have

$$f\gamma = \sum_{s=1}^{S} \left(\sum_{z \in G(\gamma)} f(y_s z)\gamma(z^{-1}) \right) y_s \gamma.$$

Comparing with (6) completes the proof.

4. Examples

We will compute $EXT(G, A)$ and $BAS(G, A)$ for the groups $G = A \triangleleft B$, where $A = C_N(x) \times C_N(y)$ and $B = C_2(k_a) \times C_2(k_b)$ with

$$a = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The fixed points in A under actions by the elements of B depend on whether N is even or odd.

Fixed points

	N even	N odd
k_a	$(0,0)$, $(\frac{N}{2},0)$, $(0,\frac{N}{2})$, $(\frac{N}{2},\frac{N}{2})$	$(0,0)$
k_b	$(0,0)$, $(1,1)$, $\ldots$, $(N-1,N-1)$	$(0,0)$, $(1,1)$, $\ldots$, $(N-1,N-1)$
$k_a k_b$	$(0,0)$, $(1,N-1)$, $\ldots$, $(N-1,1)$	$(0,0)$, $(1,N-1)$, $\ldots$, $(N-1,1)$

Apart from the difference in the first row, it is important to note that for N even, $\left(\frac{N}{2}, \frac{N}{2}\right)$ is a fixed point for k_b and $k_a k_b$, but is not in the indexing set if N is odd.

Centralizer in B

	character index	
Centralizer	N even	N odd
B	$(0,0)$, $\left(\frac{N}{2}, \frac{N}{2}\right)$	$(0,0)$
B_1	$\left(\frac{N}{2}, 0\right)$, $\left(0, \frac{N}{2}\right)$	None
B_2	(l,l), $1 \leq l < N$, $l \neq \frac{N}{2}$	(l,l), $1 \leq l < N$
B_3	$(l, N-l)$, $1 \leq l < N$, $l \neq \frac{N}{2}$	$(l, N-l)$, $1 \leq l < N$

4.1 $EXT(G_1, A)$

$Ext(G_1, A)$ can be computed from the fixed points and centralizers and the characters of the subgroups of B. If the subgroup C of B is the centralizer of the point (k,l), then the collection of products in $\mathbf{C}G_1$,

$$\tau_{k,l}\lambda, \qquad \lambda \in C^*$$

is the collection of all characters in $EXT(G_1, A)$ extending $\tau_{k,l}$.

The characters of B are

$$\begin{aligned}
\lambda_{0,0} &= 1 + k_a + k_b + k_a k_b, \qquad \text{(trivial character)}.\\
\lambda_{0,1} &= 1 + k_a - k_b - k_a k_b,\\
\lambda_{1,0} &= 1 - k_a + k_b - k_a k_b,\\
\lambda_{1,1} &= 1 - k_a - k_b + k_a k_b.
\end{aligned}$$

The characters of the subgroups of B are given by restriction.

Characters of subgroups of B.

Subgroups	characters
B_0	1
B_1	$1 + k_a$, $1 - k_a$
B_2	$1 + k_b$, $1 - k_b$
B_3	$1 + k_a k_b$, $1 - k_a k_b$

The following table describes $EXT(G_1, A)$, for even N, by describing the subsets $ext_\tau(G_1(\tau))$ of characters in $EXT(G_1, A)$ extending $\tau \in A^*$.

$EXT(G_1, A)$, N even.

τ	$ext_\tau(G_1(\tau))$	$G_1(\tau)$
$\tau_{0,0}$, $\tau_{\frac{N}{2},\frac{N}{2}}$	$\tau\lambda_{0,0}$, $\tau\lambda_{0,1}$, $\tau\lambda_{1,0}$, $\tau\lambda_{1,1}$	G_1
$\tau_{0,\frac{N}{2}}$, $\tau_{\frac{N}{2},0}$	$\tau(1+k_a)$, $\tau(1-k_a)$	$A \rtimes B_1$
$\tau_{l,l}$	$\tau(1+k_b)$, $\tau(1-k_b)$ $1 \le l < N$, $l \ne \frac{N}{2}$	$A \rtimes B_2$
$\tau_{l,N-l}$	$\tau(1+k_a k_b)$, $\tau(1-k_a k_b)$ $1 \le l < N$, $l \ne \frac{N}{2}$	$A \rtimes B_3$

Characters τ of A not listed above have $B_0 = \{1\}$ as their centralizer and are maximal characters in $EXT(G_1, A)$.

$EXT(G_1, A)$, N odd.

τ	$ext_\tau(G_1(\tau))$	$G_1(\tau)$
$\tau_{0,0}$	$\tau_{0,0}\lambda_{0,0}$, $\tau_{0,0}\lambda_{0,1}$, $\tau_{0,0}\lambda_{1,0}$, $\tau_{0,0}\lambda_{1,1}$	G_1
$\tau_{l,l}$	$\tau_{l,l}(1+k_b)$, $\tau_{l,l}(1-k_b)$, $\quad 1 \le l < N$	$A \rtimes B_2$
$\tau_{l,N-l}$	$\tau_{l,N-l}(1+k_a k_b)$, $\tau_{l,N-l}(1-k_a k_b)$, $\quad 1 \le l < N$	$A \rtimes B_3$

Characters τ of A not of the form given above are maximal characters in $EXT(G_1, A)$.

The basis $BAS(G_1, A)$ is the disjoint union of the bases $BAS(\gamma)$ of the irreducible left ideals $\mathbf{C}G_1\gamma$, $\gamma \in EXT(G_1, A)$. $BAS(\gamma)$ is the set given by the left multiplications of γ by the elements in the complete system of left $B(\gamma)$-coset representatives in B.

We will define an ordering on $BAS(G_1, A)$ which is compatible with the direct sum decomposition of $\mathbf{C}G_1$ into the irreducible left ideals $\mathbf{C}G_1\gamma$, $\gamma \in EXT(G_1, A)$. The elements in each basis $BAS(\gamma)$ of $\mathbf{C}G_1\gamma$ occur as contiguous elements.

$EXT(G_1, A)$ consists of all elements of the form

$$\gamma = \tau_{k,l}\lambda, \quad 0 \le k,\ l < N,\ \lambda \in B(\tau_{k,l})^*.$$

Order the characters of B as defined and order the characters of subgroups. Order $EXT(G_1, A)$ by ordering (k, l, λ), lexicographically. In this ordering λ is the fastest running parameter, followed by l and then by k.

The ordering in $EXT(G_1, A)$ induces an ordering on the collection of all bases $BAS(\gamma)$, $\gamma \in EXT(G_1, A)$. Ordering the elements in each of these bases, we have ordered $BAS(G_1, A)$ with the required compatibility condition with respect to the direct sum decomposition.

$BAS(\gamma)$, $N = 3$

$B(\gamma)$	$BAS(\gamma)$
B	$\tau_{0,0}\lambda_{0,0}$, $\tau_{0,0}\lambda_{0,1}$, $\tau_{0,0}\lambda_{1,0}$, $\tau_{0,0}\lambda_{1,1}$
B_1	None
B_2	$\tau_{1,1}(1+k_b)$, $k_a\tau_{1,1}(1+k_b)$, $\tau_{1,1}(1-k_b)$, $k_a\tau_{1,1}(1-k_b)$, $\tau_{2,2}(1+k_b)$, $k_a\tau_{2,2}(1+k_b)$, $\tau_{2,2}(1-k_b)$, $k_a\tau_{2,2}(1-k_b)$,
B_3	$\tau_{1,2}(1+k_ak_b)$, $k_a\tau_{1,2}(1+k_ak_b)$, $\tau_{1,2}(1-k_ak_b)$, $k_a\tau_{1,2}(1-k_ak_b)$, $\tau_{2,1}(1+k_ak_b)$, $k_a\tau_{2,1}(1+k_ak_b)$, $\tau_{2,1}(1-k_ak_b)$, $k_a\tau_{2,1}(1-k_ak_b)$,
B_0	$\tau_{0,1}$, $k_b\tau_{0,1}$, $k_a\tau_{0,1}$, $k_ak_b\tau_{0,1}$ $\tau_{0,2}$, $k_b\tau_{0,2}$, $k_a\tau_{0,2}$, $k_ak_b\tau_{0,2}$ $\tau_{1,0}$, $k_b\tau_{1,0}$, $k_a\tau_{1,0}$, $k_ak_b\tau_{1,0}$ $\tau_{2,0}$, $k_b\tau_{2,0}$, $k_a\tau_{2,0}$, $k_ak_b\tau_{2,0}$

Figure 8. Normalized basis of $\mathbf{C}\left((C_3 \times C_3) \rtimes (C_2 \times C_2)\right)$

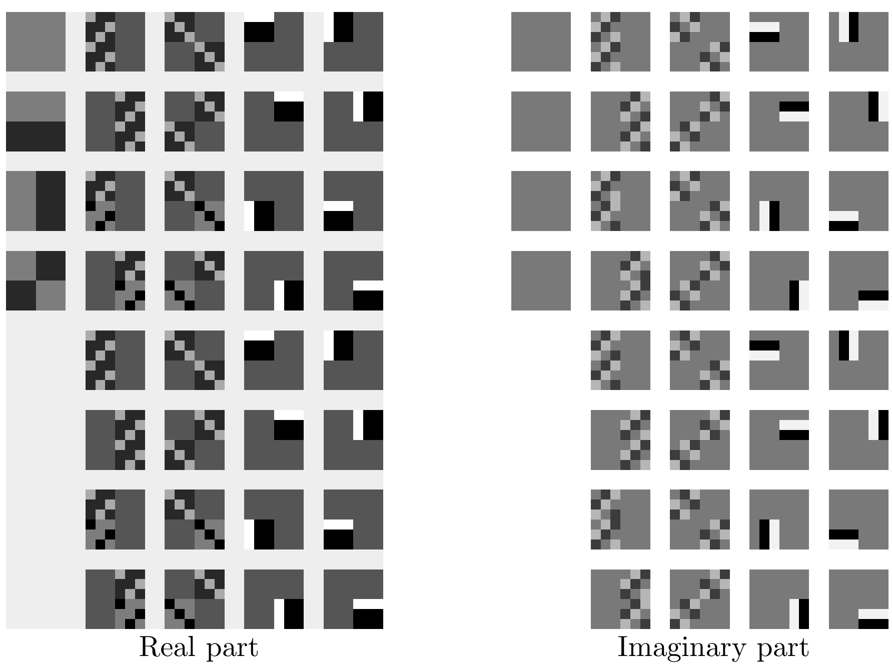


Figure 9. Normalized basis of $\mathbf{C}\left((C_4 \times C_4) \rtimes (C_2 \times C_2)\right)$

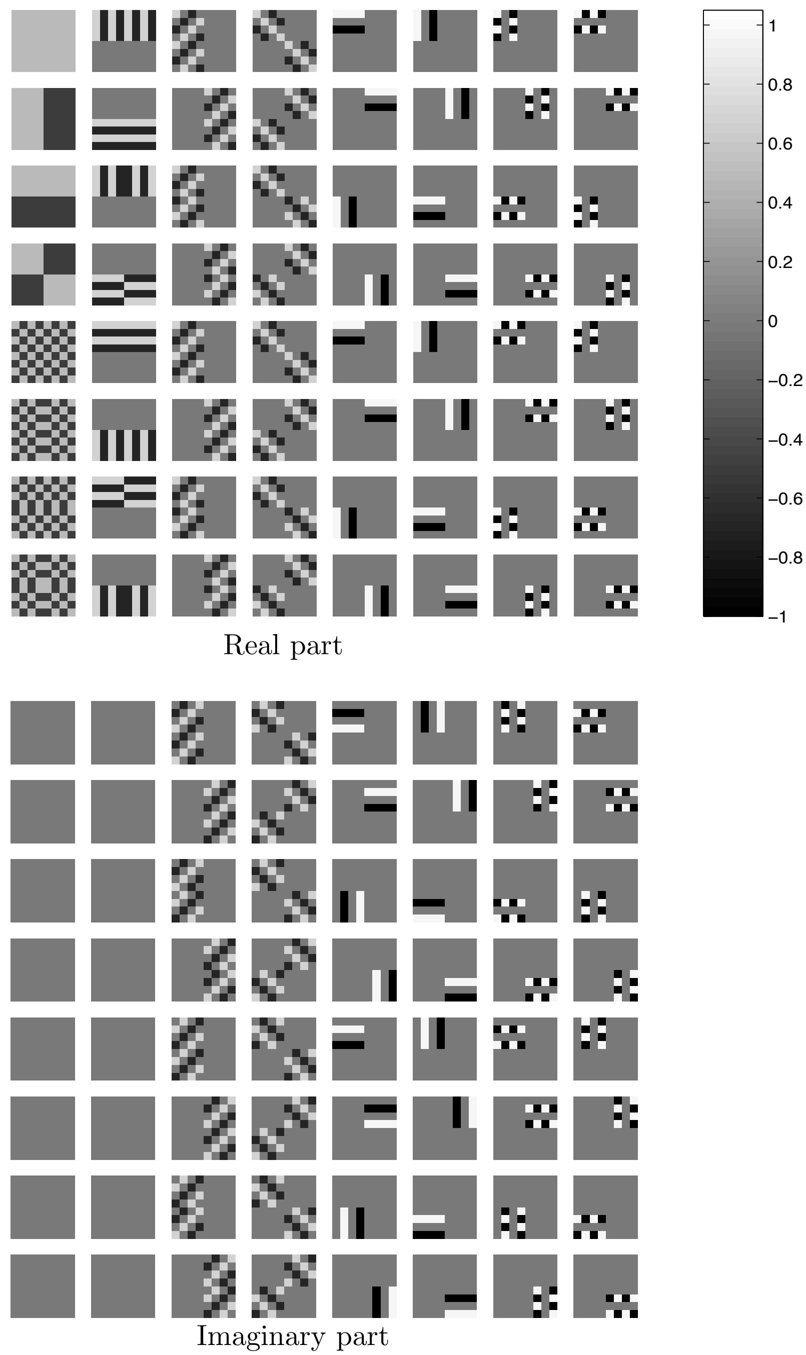
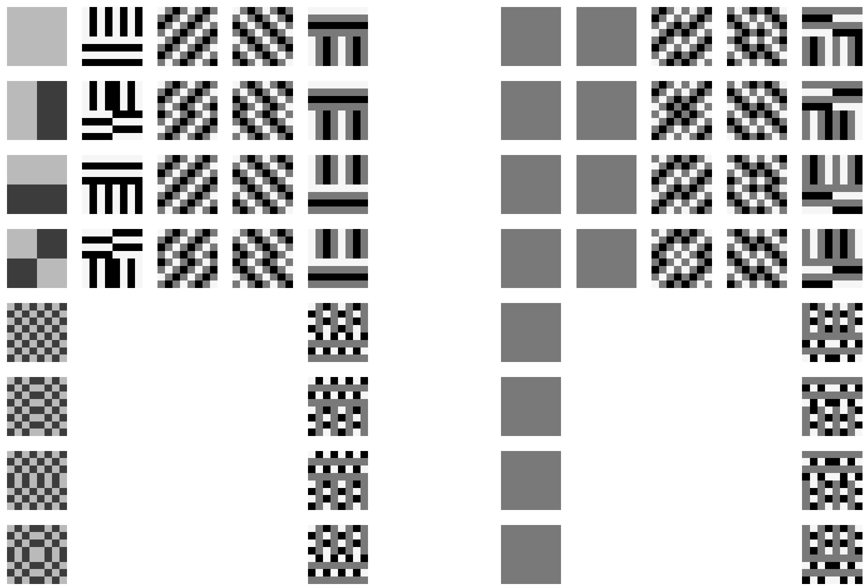


Figure 10. Generators of invariant subspaces of $\mathbf{C}\left((C_4 \times C_4) \triangleleft (C_2 \times C_2)\right)$



Real part Imaginary part

In Figure 8, the coefficients of the basis of G_1, for $N = 3$, are displayed as log-scaled intensity plots, with respect to this 2-dimensional indexing. The first column of 4 images corresponds to the characters of G_1, scaled by $|G_1| = 36$. Each of these elements generates a 1-dimensional $\mathcal{L}G_1$-invariant subspace. The imaginary parts of the images in the first column are identically zero. The second column of 8 images, in pairs, corresponds to the basis of 2-dimensional invariant subspaces generated by the maximal extensions to $A \triangleleft B_2$, scaled by 18. The third column of 8 images, in pairs, corresponds to the basis of 2-dimensional invariant subspaces generated by the maximal extensions to $A \triangleleft B_3$, scaled by 18. The remaining two columns of images, 4 images at a time, correspond to the basis of 4-dimensional invariant subspaces generated by the characters of A which are maximal in G_1, scaled by 9.

An index matrix of G_1, for $N = 4$, is defined in an analogous way. In Figure 9, the coefficients of the basis of G_1, for $N = 4$, are displayed as log-scaled intensity plots, with respect to this 2-dimensional indexing.

An intensity scale bar is appended on the right for reference, and applies to all image plots in this chapter.

The first column of 8 images corresponds to the characters of G_1, scaled by $|G_1| = 64$. Each of these elements generates a 1-dimensional $\mathcal{L}G_1$-invariant subspace. The second column of 8 images, in pairs, corresponds to the basis of 2-dimensional invariant subspaces generated by maximal extensions to $A \lhd B_1$, scaled by $|A \lhd B_1| = 32$. The imaginary parts of the images in the first two columns are identically zero. The third column of 8 images, in pairs, corresponds to the basis of 2-dimensional invariant subspaces generated by the maximal extensions to $A \lhd B_2$, scaled by 32. The fourth column of 8 images, in pairs, corresponds to the basis of 2-dimensional invariant subspaces generated by the maximal extensions to $A \lhd B_3$, scaled by 32. The remaining columns of images, 4 images at a time, correspond to the basis of 4-dimensional invariant subspaces generated by the characters of A which are maximal in G_1, scaled by 16.

In Figure 10, the 28 generators of invariant subspaces are displayed. These are the results of adding the basis elements belonging to an invariant subspace.

5. Group Transforms

Suppose G is an arbitrary group and Δ is a complete system of primitive, pairwise orthogonal idempotents in $\mathbf{C}G$. The *G-group transform* or simply G-transform is the collection of right multiplications of $\mathbf{C}G$

$$\{R(e) : e \in \Delta\}. \tag{7}$$

Reference to Δ will always be suppressed. Each right multiplication in (7) is a *G-component filter*. Any G-component filter or sum of G-component filters is a *G-filter*.

The G-transform of $f \in \mathbf{C}G$ is the collection

$$\{R(e)f : e \in \Delta\}. \tag{8}$$

Each product in (8) is a *G-spectral component* of f. Any G-spectral component or sum of G-spectral components of f is a *G-filtering* of f.

For an abelian group A we always take $\Delta = \Delta(A)$. Abelian group transforms are probably well-known to the reader. Since each *filter space* of the A-transform

$$\mathbf{C}Ae, \quad e \in \Delta(A),$$

is one-dimensional, the A-spectral component

$$fe = \widehat{f}(\tau)e, \quad e = \frac{1}{N}\tau,$$

can be represented by $\widehat{f}(\tau)$. The *A-spectral image* of f is the collection

$$\left\{\widehat{f}(\tau) : \tau \in A^*\right\}.$$

For any abelian by abelian semidirect product $G = A \lhd B$ we always take $\Delta = \Delta(G)$. The *filter spaces* of the G-transform

$$\mathbf{C}Ge, \quad e \in \Delta(G),$$

are not necessarily one-dimensional. The *G-spectral image* of f is the collection of expansion coefficients of f relative to the basis $BAS(G, A)$.

A *G-filter* is a linear operator $P : \mathbf{C}G \longrightarrow \mathbf{C}G$ satisfying

$$P(yf) = yP(f), \quad f \in \mathbf{C}G,\ y \in G.$$

By linearity if P is a G-filter, then

$$P(gf) = gP(f), \quad f,\ g \in \mathbf{C}G.$$

Every $f \in \mathbf{C}G$ defines a G-filter $R(f)$ by

$$R(f)g = gf, \quad g \in \mathbf{C}G.$$

$R(f)$ is called *right multiplication* by f. In general $L(f)$ is not a G-filter.

THEOREM 51 *If P is a G-filter, then there exists $f \in \mathbf{C}G$ such that $P = R(f)$.*

The image of the G-filter $R(f)$ is the left ideal $\mathbf{C}Gf$. We call $\mathbf{C}Gf$ the *filter space* of $R(f)$. Since we can have $\mathbf{C}Gf_1 = \mathbf{C}Gf_2$, for distinct $f_1,\ f_2 \in \mathbf{C}G$, distinct G-filters can have the same filter space.

5.1 Matched Filtering

Suppose G is an arbitrary group and Δ is a complete system of primitive, pairwise orthogonal idempotents in $\mathbf{C}G$. For $f \in \mathbf{C}G$, the *G-matched filter* of f is the G-filter

$$e_f = \sum_{fe \neq 0} e. \tag{9}$$

The summation in (9) runs over all idempotents $e \in \Delta$ such that $fe \neq 0$. The G-matched filter of f satisfies

$$fe_f = f.$$

In a typical image processing application an image $f \in \mathbf{C}G$ is contained in noise and background. The problem is to separate the target f from the noise and background. The image data has the form

$$g = f + \eta,$$

where $\eta \in \mathbf{C}G$ represents the noise and background. The G-matched filtering

$$ge_f = f + \eta e_f$$

is usually the optimal G-filtering for separating f from η. Examples of G-matched filtering will be given in the following sections.

The concept of a G-matched filter is a major tool in both abelian and nonabelian group filter design. As defined, the formal structure of a G-matched filter does not change with different choices of group G. However, the choice of indexing group is a critical parameter affecting several important characteristics of the resulting matched filters. We have distinguished two properties which can vary as the indexing group varies: invariance under left group actions and the extent and form of image domain locality. The first will be discussed in this section. Image domain locality is the topic addressed in the next section.

For an image $f \in \mathbf{C}G$, the *G-equivalence class of images* containing f is the equivalence class of images in the set

$$\{xf : x \in G\}\,.$$

The G-equivalence class containing f depends on the actions of the left multiplications from G on f and can vary as G varies.

The G-matched filter of f satisfies

$$xfe_f = xf, \qquad x \in G.$$

This implies that the G-matched filter of f is the G-matched filter of every image G-equivalent to f. In applications this means that the G-matched filter constructed for an image f will be the optimal filtering not only for f, but also for all G-equivalent images.

5.2 Image Domain Locality

Image domain locality is a key component of nonabelian group filters not available with abelian group filters. To understand where this property comes from and how it can be controlled at the group level, we will show that the expansion coefficients in nonabelian group DSP can encode local image space information.

The explanation is related to the character extension problem. If A is an abelian group, then this is straightforward. The basis for Fourier representation is the collection of characters. Relative to this basis, each expansion coefficient contains image information across the image plane. These coefficients are sensitive to all local changes. The placing of a geometric structure in an image data set affects all expansion coefficients.

The character extension problem is more complicated for an abelian by abelian semidirect product $G = A \triangleleft B$. As we have pointed out there exist characters of A, which can not be extended to characters of G. The characters defining $\Delta(G)$ are maximal characters in G, but some have proper subgroups of G as their supports.

Suppose $e \in \Delta(G)$ and

$$e = \frac{1}{|\gamma|}\gamma,$$

where γ is a character of the subgroup $G(\gamma)$ of G. For the discussion assume $G(\gamma)$ is a proper subgroup of G. If

$$\{y_s : 1 \leq s \leq S\}$$

is a complete system of left $G(\gamma)$-coset representatives in G, then

$$\{y_s e : 1 \leq s \leq S\} \tag{10}$$

is a basis for the irreducible left ideal $\mathbf{C}Ge$. The key point is that $G(\gamma)$ is a proper subgroup of G and the basis (10) is supported on pairwise disjoint left-cosets. For each s, $1 \leq s \leq S$, the basis element $y_s e$ is localized in the image domain to the left coset $y_s G(\gamma)$.

Suppose $f \in \mathbf{C}G$. We can write

$$fe = \sum_{s=1}^{S} \alpha(s) y_s e.$$

If $g \in \mathbf{C}G$ is supported in $y_t G(\gamma)$ for some $1 \leq t \leq S$, then

$$(f+g)e = \sum_{s \neq t} \alpha(s) y_s e + \alpha'(t) y_t e.$$

The effect of the local image domain change on the expansion coefficients of the filtered image, resulting from the addition of g, is to change exactly one coefficient. The sensitivity to the local image domain depends on the relative orders of G and $G(\gamma)$.

For a fixed character τ of A, the left ideal $\mathbf{C}G\tau$ can be written as

$$\mathbf{C}G\tau = \bigoplus_{\lambda \in B(\tau)^*} \mathbf{C}G\tau\lambda.$$

$\mathbf{C}G\tau$ is not necessarily irreducible. We can write

$$f\tau = \frac{1}{|B(\tau)|} \sum_{\lambda \in B(\tau)^*} \sum_{s=1}^{S} \alpha_\lambda(s) y_s \tau\lambda.$$

This expansion shifts the basis in both the image and spectral image domains and can be viewed as a localized image-spectral image domain expansion in analogy to time-frequency expansions. Local image domain changes affect a set of prescribed coefficients and these changes describe the local image domain change in both image and spectral image domains.

6. Group Filters

In this section we study and compare properties of abelian and non-abelian group filters by illustrating their effects on lines and line segments. These examples will concentrate on the image domain locality and the left group multiplication invariance of the filters.

6.1 Abelian group filtering

For $N = 64$, set

$$A_0 = \sum_{k=0}^{N-1} \tau_{0,k} \in \mathbf{C}A.$$

A_0 is the matched filter of the vertical line and all its abelian group translates.

The following examples show detection and location by A_0 of a vertical line and several of its abelian group translates. Varying levels of noise are added to generate the images in Figure 12. The noise is modeled as Gaussian with zero-mean. Levels of noise are indicated by the standard deviation (sd). Images in Figure 13 are the results of filtering by A_0. Even in severe noise, the location of maximum intensity yields the positions of the translates of a vertical line.

Figure 11. Images containing a vertical line

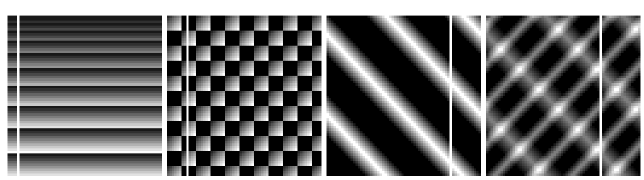
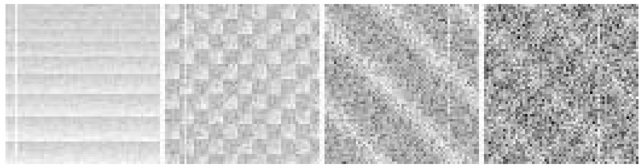
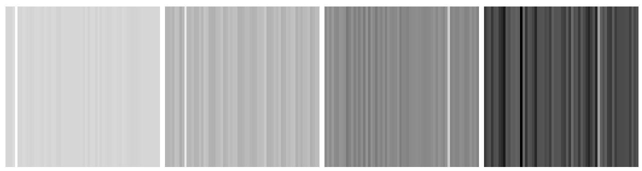


Figure 12. Noisy images containing a vertical line



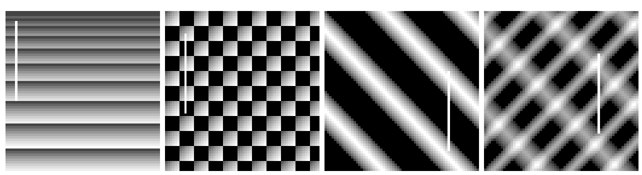
sd=.5 sd=1.0 sd=2.0 sd=3.0

Figure 13. Results of Filtering by A_0



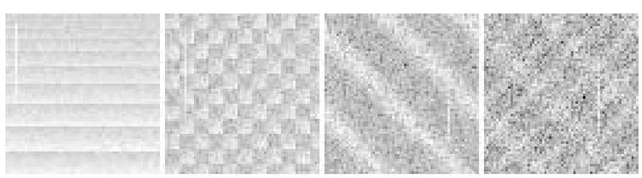
In Figures 14 and 15 the translates of a vertical line are replaced by line segments of one half the length. The placement of the vertical line segment is given by the coordinate of the starting position.

Figure 14. Images containing a vertical line segment



(4,4) (9,8) (24,51) (17,47)

Figure 15. Noisy images containing a vertical line segment



sd=.5 sd=1.0 sd=1.5 sd=2.0

The last example shows that as the length of the line diminishes, the performance of the filter A_0 for detecting line segments worsens.

Figure 16. Results of Filtering by A_0

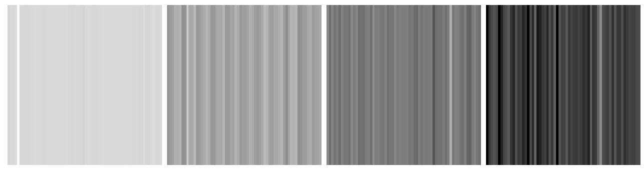
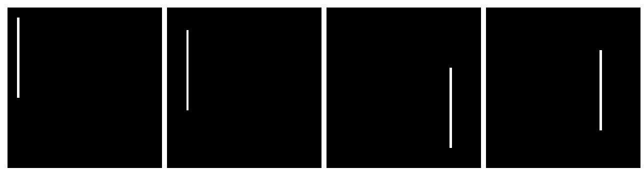
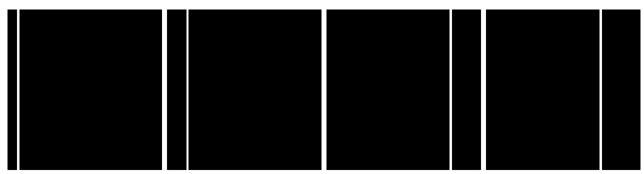


Figure 17. Images of vertical line segments



(4,4) (9,8) (24,51) (17,47)

Figure 18. Results of Filtering by A_0



Moreover, the vertical position of the line segment cannot be detected, even without any noise as shown in Figure 18.

The preceding examples show one of the major deficiencies of abelian group filtering, the lack of image domain locality.

6.2 Nonabelian group filtering

Consider the group

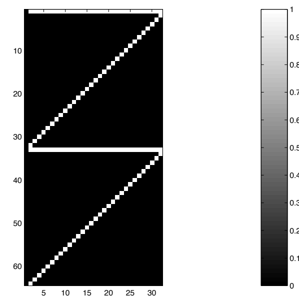
$$G_4 = A \rtimes C_2(k_c)$$

and the group filter defined by

$$P_0 = \frac{1}{N} \sum_{k=1}^{N-1} \tau_{0,k} + k_c \tau_{0,k}.$$

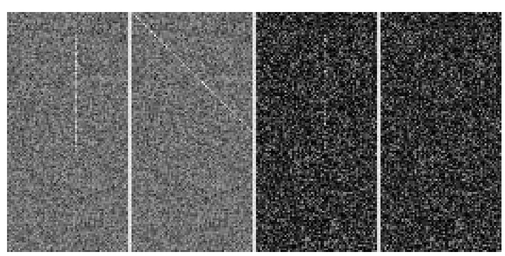
The choice of P_0 was made for its simplicity, and because it is *symmetric* or real valued. An intensity plot of the filter is shown below for $N = 32$ along with the intensity color scheme.

Figure 19. Intensity plot of the filter P_0, $N = 32$.



The following example shows the importance of matching the filter to the targeted image. The first test image contains a vertical line segment, while the second test image contains a line segment of slope 1. In Figure 20, the first and third images contain a vertical line segment, while the second and fourth images contain a line segment of slope 1. Noise levels are indicated by the standard deviation (sd). Figure 21 displays the results of applying P_0.

Figure 20. Test images in noise



$sd = 2.0$ $sd = 2.0$ $sd = 5.0$ $sd = 5.0$

The filter P_0 is matched to the vertical line and to all left multiplications of the vertical line by the elements of G_4. Since the line segment of slope 1 is not contained in the collection of G_4-equivalent images, it cannot be detected by P_0.

Invariance of P_0 with respect to left multiplication by the elements from G_4 implies that these left actions do not affect filter performance. The previous figure shows this for left multiplications by $x^m y^n$, $0 \leq m$, $n < N$.

Figure 21. Results of applying P_0

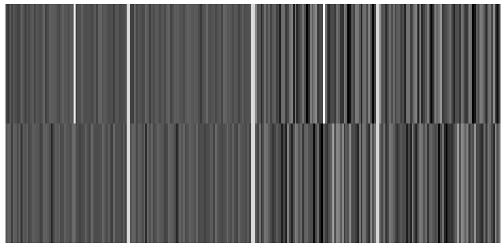


Figure 22. k_c-translates of the images in Figure 20

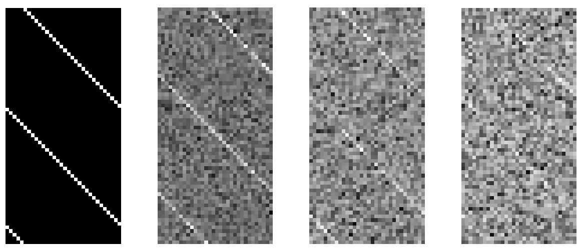
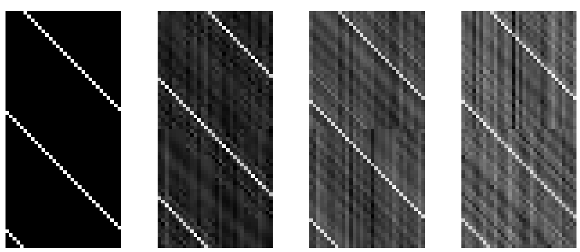


Figure 23. Results of filtering by P_0



Each frame in Figure 22 displays the k_c-translate of the corresponding frame in Figure 20. Figure 23 displays the results of filtering the images in Figure 22 by P_0.

The next pair of figures show the implications of invariance and image domain locality. In Figure 24 a vertical line segment of length 32 is placed arbitrarily, and the horizontal position is recorded. The problem is to determine the position using the filter P_0. Figure 25 shows the results of this filtering by P_0.

Figure 24. x^m-translates of an image containing line segment of length 32

$m = 11$ $m = 5$ $m = 6$ $m = 28$

Figure 25. Results of filtering by P_0

$(u, l) =$ $(.585, .382)$ $(.761, .207)$ $(.732, .236)$ $(.117, .851)$

The pair of numbers (u, l) in Figure 23 are the intensities of the upper and lower half of the line segments. Note the close relationship between the intensities of the line segment and its position. (The intensity of the input line segment in Figure 25 is 1.0, but this information is only relative.) The relationship between the difference of intensities and position is given by

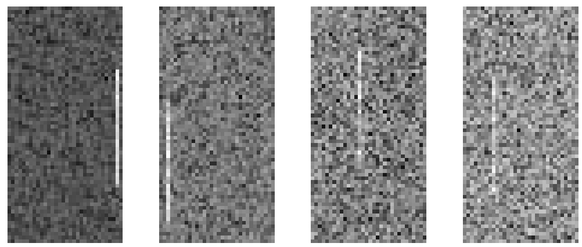
$$m \sim N - \frac{uN}{u + l}. \tag{11}$$

Accuracy of the relationship (11) depends on N, up to $\frac{N}{16}$ pixels. Thus the smaller N is the more accurate the relationship (11).

The same experiment is repeated with varying levels of noise. The position of the line segment is estimated from the filtered image using (11), and denoted by m' in Figure 27.

In the presence of noise, the intensity is not uniform through the upper or lower half of the line segment, but the variance is very small. Estimate of location in (11) is derived using the intensity at position

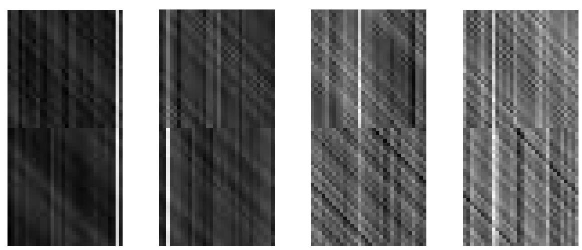
Figure 26. x^m-translates of an image containing line segment of length 32



$sd = 0.5$ $\quad$ $sd = 1.0$ $\quad$ $sd = 1.5$ $\quad$ $sd = 2.0$

$m = 16$ $\quad$ $m = 25$ $\quad$ $m = 10$ $\quad$ $m = 18$

Figure 27. Results of filtering by P_0



$(u, l) =$ $(.489, .499)$ $\quad$ $(.302, .851)$ $\quad$ $(.538, .171)$ $\quad$ $(.264, .357)$

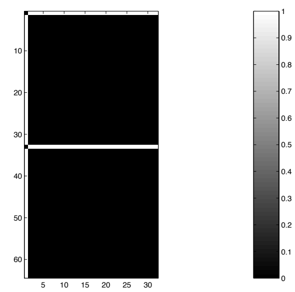
$m' = 16.1$ $\quad$ $m' = 23.6$ $\quad$ $m' = 7.7$ $\quad$ $m' = 18.3$

$(0, y)$ and (N, y), where y is the horizontal position of the line segment. A better estimate than (11) can be derived, especially in cases where noise characteristics are known.

As these experiments show, detection and location of vertical lines of uniform intensity of known lengths can be implemented using P_0. Using similar analysis, a relationship can be derived and the same implementation can be used to locate diagonal lines shown in Figure 22. Since $k_c x^m y^n k_c^{-1} = x^m y^{m-n}$, the x-intercept is equivalent to the horizontal location of the vertical line.

Note that the length of a line segment must be at least N for exploiting the localization property consistently. More specifically, if the length of the line segment is less than N, in the case where the line segment lies entirely in lower or the upper of the two planes, we can localize the line segment only up to one of the two planes. This provides one major parameter determining the design of groups and filters in detection/localization applications: For consistent detection/localization

Figure 28. Intensity plot of the filter P_1, $N = 32$.



of, for example, a vertical line segment of length N in an image of size $K_1N \times K_2N$, the following two approaches can be used.

1 Starting with a group $G = (C_N \times C_N) \lhd C_2$, we can apply P_0 to subimages of size $2N \times N$, overlapped by at least N.

2 Design filters associated to a group of the form $G = (C_N \times C_N) \lhd (C_{K_1} \times C_{K_2})$. (Groups of the form $(C_N \lhd C_{K_1}) \times (C_N \times C_{K_2})$ will work as well for detection/localization of vertical or horizontal lines, but groups of the form $(C_N \times C_N) \lhd (C_{K_1} \times C_{K_2})$ provide more flexibility in shapes.)

The filter performance degrades as the noise level increases. This is particularly true with no prior knowledge of the noise characteristics. One method that will improve filter performance is to use a similar filter based on a different group of the same size. Consider the group

$$G = (C_N(x) \times C_N(y)) \lhd C_2(k_e),$$

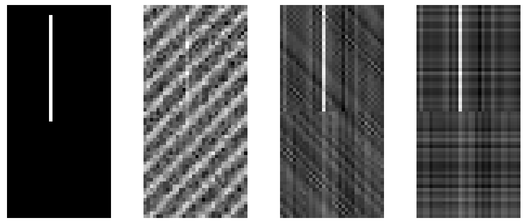
where $e = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Construct the G-filter

$$P_1 = \frac{1}{N} \sum_{n=1}^{N-1} \tau_{0,k} + k_e \tau_{0,k}.$$

P_1 is also real-valued. An intensity plot of P_1 is shown in Figure 28.

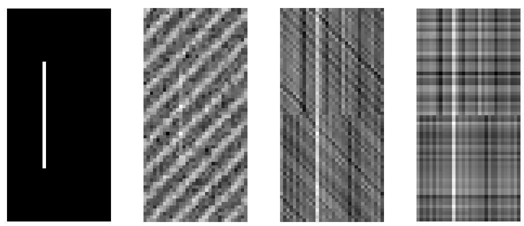
In Figures 29 − 31, results of applying P_0 and P_1 are shown in the third and fourth frames along with estimates of the location of the line segment. The first frame displays the line segment and the second frame displays the line segment embedded in background and noise.

Figure 29. Results of applying P_0 and P_1



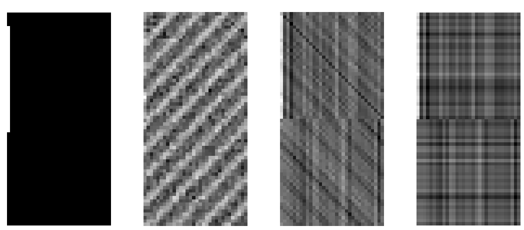
$m = 3$ $sd = 2.0$ $m' = 5.0$ $m'' = 5.6$

Figure 30. Results of applying P_0 and P_1



$m = 16$ $sd = 2.0$ $m' = 14.8$ $m'' = 16.7$

Figure 31. Results of applying P_0 and P_1



$m = 4$ $sd = 2.0$ $m' = 5.5$ $m'' = 2.2$

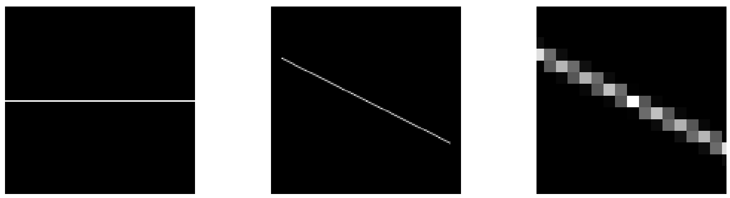
The accuracy of the estimate (11) differs between the filters P_0 and P_1 as the noise is *filtered out* in two distinct ways by the distinct convolutions defined by the two groups. This is another parameter determining design of a detection/location application. By applying several distinct groups, detection and location can be made more accurate. A trade-off is clearly the cost of processing.

7. Line-like Images

In this section the performance of groups filters on non-digital, line-like objects is illustrated. Generally, filter performances are better due to the fact that non-digital lines have more than one pixel width.

In Figure 32 the first image is the digital line of slope 0. The second image is generated by rotating the horizontal line by 27° clockwise about the center of the image. Rotation is implemented using bilinear interpolation. The third image displays a portion of the rotated line near the center of rotation.

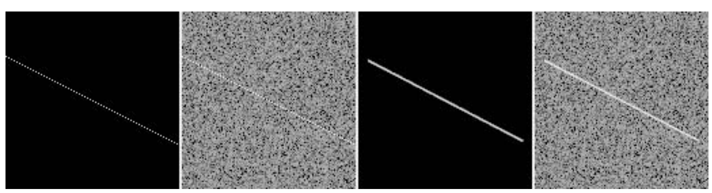
Figure 32. Result of rotating a line



horizontal line through $(64, 64)$ | result of rotating the horizontal line | detail around center of rotation

The following example compares the results of filtering a digital test image and a rotated test image in varying levels of noise.

Figure 33. Test images in noise, $sd = .5$



(a1) (b1) (c1) (d1)

Images in Figure 33 are as follows.

(a1) digital line segment of slope $-\frac{1}{2}$, (b1) digital line in noise,
(c1) rotated line, (d1) rotated line in noise

The next example illustrates the performance of matched filters in detecting and locating a *line-like* object in recorded data.

Figure 34. Results of filtering in noise, $sd = .5$

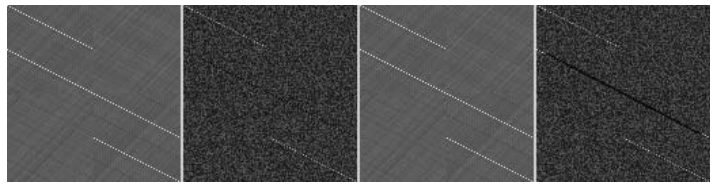
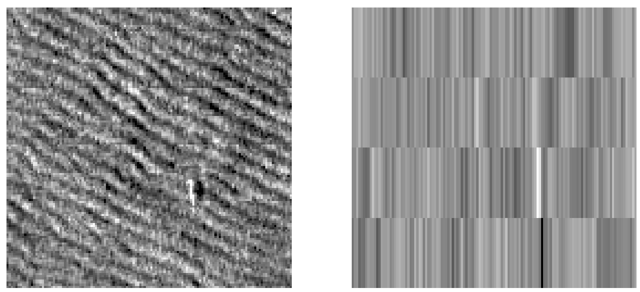


Figure 35. Sonar image of size 128×128 and result of filtering



The next collection of examples are included to illustrate:

1 the diversity of images which can be created by composition of parallel lines of varying orientations,

2 the sensitivity of the matched filters to changes in orientations,

3 design strategy for matched filters whose properties vary with image size.

For a positive integer K and $N = 16K$, consider the groups

$$G_6 = A \lhd C_4(k_a), \qquad G_7 = A \lhd C_4(k_b),$$

where $A = C_N(x) \times C_N(y)$ and

$$a = \begin{bmatrix} \frac{N}{2} & \frac{N}{4}+1 \\ \frac{N}{4}+1 & 0 \end{bmatrix}, \qquad b = \begin{bmatrix} \frac{N}{2} & \frac{N}{4}-1 \\ \frac{N}{4}-1 & 0 \end{bmatrix}.$$

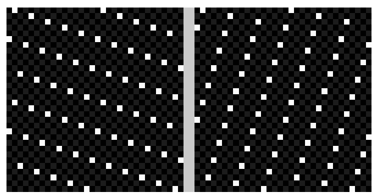
The sum of 1-dimensional idempotents in $\mathbf{C}G_6$ and in $\mathbf{C}G_7$ define matched filters

$$P_6 = \sum_{k=0}^{N-1} \sum_{j=0}^{3} \tau_{k,(M+1)k} \lambda_j \in \mathbf{C}G_6,$$

$$P_7 = \sum_{k=0}^{N-1} \sum_{j=0}^{3} \tau_{k,(M-1)k} \mu_j \in \mathbf{C}G_7.$$

Figures 36 and 37 display the filters P_6 and P_7. Unlike the matched filters we have previously described, properties of P_6 and P_7 depend on N which determines the image size.

Figure 36. Matched filters, $N = 16$.



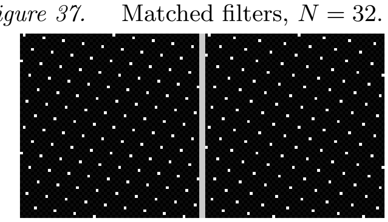
$P_6 \in \mathbf{C}G_6$ $P_7 \in \mathbf{C}G_7$

The first image in Figure 38 is a composition of two sets of intensities along parallel lines of slopes 3 and 4. The results of applying P_6 and P_7 in noise are displayed. Noise is simulated as Gaussian of zero mean with varying values of standard deviation.

The last image in Figure 38 is not an algebraic object in that it belongs neither to $\mathbf{C}G_6$ nor $\mathbf{C}G_7$. It is simply the sum of two intensities defined on an array of size $2N \times 2N$.

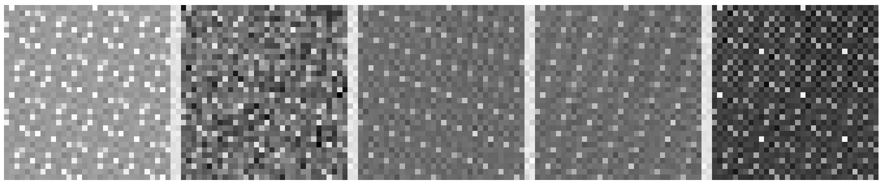
In Figure 40, $\mathbf{g}$ is viewed as an element of $\mathbf{C}G_7$. The last image is again simply the sum of two intensities.

Figure 37. Matched filters, $N = 32$.



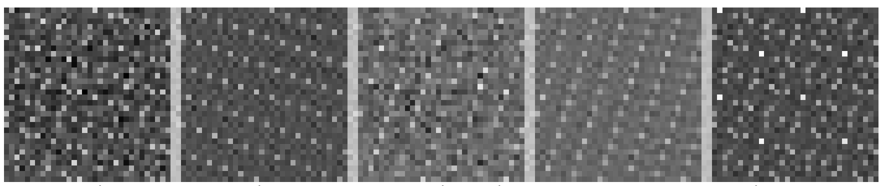
$P_6 \in \mathbf{C}G_6$ $P_7 \in \mathbf{C}G_7$

Figure 38. Results of filtering in noise



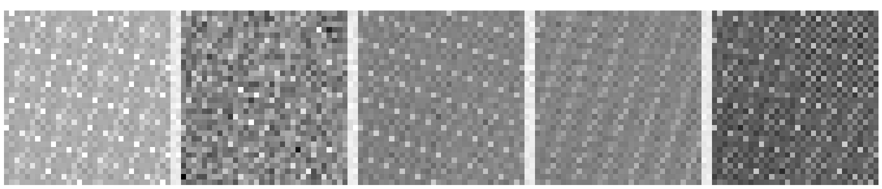
test image $\mathbf{f}$ | $\mathbf{f}$ in noise | P_6 | P_7 | $P_6 + P_7$

Figure 39. Results of filtering in noise



$\mathbf{f}'$ | $\mathbf{f}'P_6$ | $\mathbf{g} = \mathbf{f}' - \mathbf{f}'P_6$ | $\mathbf{g}P_7$ | $\mathbf{f}'P_6 + \mathbf{g}P_7$

Figure 40. Results of filtering in noise

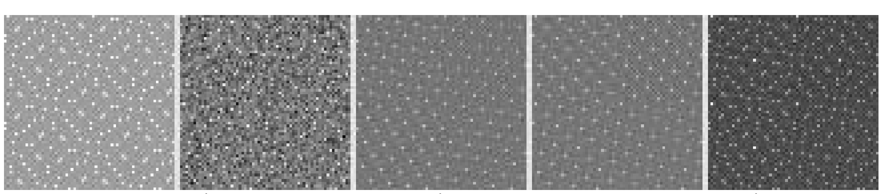


$\mathbf{g} = \mathbf{f} + k_b\mathbf{f}$ | $\mathbf{g}' = \mathbf{g}+$ noise | $\mathbf{g}'P_6$ | $\mathbf{g}'P_7$ | $\mathbf{g}'P_6 + \mathbf{g}'P_7$

The first image in Figure 40 is generated by adding to $\mathbf{f}$ its translation by k_b.

The results of applying P_6 and P_7 in noise are displayed.

Figure 41. Results of filtering in noise, $N = 32$



$\mathbf{f}$ | $\mathbf{f}' = \mathbf{f}+$ noise | $\mathbf{f}'P_6$ | $\mathbf{g}P_7$ | $\mathbf{f}'P_6 + \mathbf{g}P_7$

References

All the material presented in this paper has been reproduced from the text *Group Filters and Image Processing*, M. An and R. Tolimieri, Psypher Press, 2003, with explicit permissions from the authors and the publisher.

1 M. An, R. Tolimieri, B. York, Technical report, AF #F49620-98-C-0043, May, 2002.

2 P. Diaconis, D. Rockmore, "Efficient computation of the Fourier transform on finite groups," *J. of AMS* **3**(2), 297-332, 1990.

3 R. Foote, D. Healy, G. Mirchandani, T. Olson and D. Rockmore, "A wreath product group approach to signal and image processing: Part I Multiresolution analysis," *IEEE Trans. in SP*, **48**(1), 2000, pp. 102–132.

4 R. Holmes, "Signal processing on finite groups," *Technical Report 873*, MIT Lincoln Laboratory, 1990.

5 M. Karpovski and E. Trachtenberg, "Filtering in a communication channel by Fourier transforms over finite groups," *Spectral techniques and fault detection*, M. Karpovski, ed., Academic Press, 1985.

6 F.J. MacWilliams, "Codes and ideals in group algebras," *Combinatorial mathematics and its applications*, 317-328, R.C. Bose and T.A. Dowlin, eds., University of North Carolina Press, 1969.

7 D. Maslen and D. Rockmore, "Generalized FFTs'" *DIMACS Ser. in Disc. Math. and Theor. Comp. Sci.,* **28**, 183-237, L. Finkelstein and W. Kantor, eds., 1997.

8 R. Tolimieri, M. An, *Time-Frequency Representaions*, Birkhauser, 1998.