

Decomposing Monomial Representations of Solvable Groups

Markus Püschel

Technical Report DU-MCS-99-02
Department of Mathematics and Computer Science
Drexel University
Philadelphia, PA 19104
October 1999

Abstract

We present an efficient algorithm which decomposes a monomial representation of a solvable group G into its irreducible components. In contradistinction to other approaches we also compute the decomposition matrix A in the form of a product of highly structured, sparse matrices. This factorization can be viewed as a fast algorithm for the multiplication with A . In the special case of a regular representation we hence obtain a fast Fourier transform for G . Our algorithm is based on a *constructive* representation theory that we develop. The term “constructive” signifies that representations are considered and manipulated up to equality and not only up to equivalence as it is done in approaches that are based on characters. Thus, we present some well-known theorems in a constructively refined form and derive some new results on decomposition matrices. All results in this paper have been implemented in the GAP share package AREP.

1 Introduction

Representation theory of finite groups is considered to be one of the most beautiful areas in classical algebra. It deals with homomorphisms $\phi : G \rightarrow \mathrm{GL}_n(\mathbb{K})$ from a group G into the group of invertible $(n \times n)$ -matrices over a field \mathbb{K} . We will consider only “ordinary” representation theory, which means that the characteristic of \mathbb{K} does not divide the group order (Maschke condition). If a certain ϕ is given, then the vector space $V = \mathbb{K}^n$ becomes a (right) G -module through $v \cdot g = v \cdot \phi(g)$. Standard books on representation theory are Curtis and Reiner, [10], and Serre, [28].

Decomposition of a representation ϕ (with Maschke condition) into irreducible representations is a standard problem in representation theory of finite groups. It means that by conjugating $\phi \rightarrow \phi^A$, which corresponds to a change of bases in V , ϕ obtains a block diagonal structure, where all the blocks (which again are representations) cannot be decomposed any further. This decomposition reveals the algebraical structure of ϕ and A is referred to as a “decomposition matrix” for ϕ . Existence and uniqueness of the decomposition are settled in Wedderburn’s theorem.

As usual in algebra, the objects of interest are considered only up to isomorphism, which for representations means up to conjugation with a matrix A . Thus the atomic objects of investigation are not representations but equivalence classes of representations. For this reason usually the character of a representation is considered (character of $\phi = \mathrm{tr} \circ \phi$, $\mathrm{tr} = \text{trace}$) rather than the representation itself. Characters are invariant under conjugation and carry most of the information of the corresponding equivalence class. Moreover, characters can be efficiently represented: a character is determined by its values on the conjugacy classes of the group. The computer-based computation with characters contributed essentially to the classification of the finite simple groups, [7].

Fast Fourier Transforms For some applications, however, computing with characters is not sufficient: concrete matrix representations have to be considered and manipulated. One important example of such an application is the field of generalized Fourier transforms. A Fourier transform for a group G can be viewed as a decomposition matrix for the regular representation (a special permutation representation) of G . For the special case of a cyclic group Z_n one obtains the classical discrete Fourier transform (DFT_n) which is well-known from signal processing. Auslander et. al., [1], and, independently, Beth, [3], showed that the famous Cooley/Tukey factorization [8] of the DFT_n , also referred to as the “fast” Fourier transform (FFT), can be obtained by a stepwise decomposition of the regular representation along a composition series of Z_n . The step-by-step decomposition gives rise to a decomposition matrix that is a product of sparse matrices: the FFT. The FFT computes the DFT_n using $O(n \log n)$ operations, which makes it efficient to satisfy real-time demands in signal processing. Beth also investigated FFTs for the more general case of solvable groups, [2]. Important work in the field of generalized FFTs has been done by Clausen, [4, 6], Diaconis and Rockmore, [11], as well as Rockmore, [26]. For an overview we refer the reader to the book of Clausen and Baum, [6], or the survey article by Maslen and Rockmore, [19]. Applications of generalized FFTs can be found in [27] or [29].

Signal Transforms The connection between representation theory and signal transforms (given as matrices), however, is not restricted to the DFT or regular representations. The “symmetry-based” generation of fast signal transforms as introduced by Minwitz, [20, 21, 23], and further developed by Egner, [14], and Püschel, [24, 25], reveals that decomposition matrices of non-regular permutation representations and, more general, monomial representations occur as

signal transforms. The (monomial) representation associated with the transform is called “symmetry”, and a fast algorithm for the transform can be constructed, as in the case of the DFT, by a stepwise decomposition of this representation along a chain of normal subgroups. The steps in the decomposition determine a factorization of the decomposition matrix and hence a fast algorithm for the transform.

The Problem The application to signal transforms, as sketched above, was the original motivation for considering the problem solved in this paper:

A given monomial representation μ of a solvable group shall be decomposed into a direct sum of irreducible representations. *In parallel*, the corresponding decomposition matrix shall be computed *as a product of highly structured sparse matrices*.

Note that this problem embraces the construction of fast Fourier transforms arising from the special case of regular representations.

In order to solve the problem we are required to deal with representations in a different way than it is done in standard books. Representations have to be considered and manipulated up to *equality*, not only up to *equivalence*. Accordingly, some well-known theorems have to be extended and used to derive results on the structure of decomposition matrices. Our approach for decomposing monomial representations has its root in [20, 21] and is a continuation of the work begun in the authors PhD thesis [24].

All results of this paper have been implemented in the GAP share package AREP [15] which provides the data types and infrastructure for symbolic computation with representations (up to equality) and includes the decomposition algorithm for monomial representations of solvable groups.

The paper is organized as follows:

Section 2 introduces the notation and constructions from representation theory we are going to use. **Section 3** contains the mathematical basis of this paper, which we refer to as “constructive representation theory”. Within constructive representation theory we compute exclusively with representations up to equality. First, some theorems are presented which allow us to manipulate and compute with inductions of representations. Second, it is shown how these theorems can be applied to monomial representations. After a short investigation of intertwining spaces we present the main mathematical results of this paper on the structure of decomposition matrices. These results form the basis for the decomposition algorithm for monomial representations which is presented in detail in **Section 4** including an example and some runtime measurements. The impatient reader can find a sketched version of the decomposition algorithm on page 26. The paper is concluded by **Section 5** where we give a very short overview on the package AREP in which all constructive results presented in this paper as well as the decomposition algorithm are implemented.

2 Notation

A representation ϕ of degree n over a field \mathbb{K} is a homomorphism of a group G into the group $\text{GL}_n(\mathbb{K})$ of invertible $(n \times n)$ -matrices over \mathbb{K} . Throughout the paper the group G is finite and the characteristic of \mathbb{K} does not divide the group order $|G|$ (Maschke condition). In this case, every

representation ϕ can be decomposed with an invertible matrix $A \in \text{GL}_n(\mathbb{K})$ into a direct sum of irreducible representations ρ_i (Maschke's theorem). Every ρ_i is called an irreducible component of ϕ :

$$\phi^A = (g \mapsto A^{-1} \cdot \phi(g) \cdot A) = \bigoplus_{i=1}^r \underbrace{(\rho_i \oplus \dots \oplus \rho_i)}_{n_i}, \text{ where } \rho_i \not\cong \rho_j \text{ for } i \neq j$$

and every $\rho_i \oplus \dots \oplus \rho_i$ is called a homogeneous component of G . We say that ρ_i has multiplicity n_i in ϕ . A representation is called a permutation representation if all images are permutation matrices. A representation is called monomial if all images are monomial matrices. A matrix is called monomial if it contains exactly one non-zero entry in every row and column. Monomial matrices are always invertible.

If ϕ is a representation over \mathbb{K} of degree n , then G operates on the vector space $V = \mathbb{K}^n$ via ϕ by $v \cdot g = v \cdot \phi(g)$, $v \in V$, $g \in G$ making V a right $\mathbb{K}[G]$ -module. We will call V the "representation space" of ϕ . The decomposition of a representation ϕ into irreducible resp. homogeneous components corresponds to the decomposition of the representation space V into irreducible resp. homogeneous components. Whenever possible, we will present results in terms of matrix representations, avoiding the terminology of modules. We use the following conventions for notation:

Matrices: Matrices are denoted by letters A, B, M, P, \dots . A matrix with entries $a_{i,j}$ is written as $[a_{i,j} \mid i \in \{1, \dots, n\}, j \in \{1, \dots, m\}]$ or simpler as $[a_{i,j}]_{i,j}$. A diagonal matrix is written as $\text{diag}(x_1, \dots, x_n)$, a permutation matrix as $[\sigma, n] = [\delta_{i\sigma_j} \mid i, j \in \{1, \dots, n\}]$, where σ is a permutation and n its degree. $[\sigma, (x_1, \dots, x_n)] = [\sigma, n] \cdot \text{diag}(x_1, \dots, x_n)$ is a monomial matrix. A primitive n th root of unity is denoted by ω_n , $\mathbf{1}_n$ is the identity matrix of degree n , $\mathbf{0}_n$ the (square) all-zero matrix of degree n and $\text{DFT}_n = [\omega_n^{ij} \mid i, j \in \{0, \dots, n-1\}]$ the discrete Fourier transform of degree n . The direct sum of matrices A, B is written as $A \oplus B$ and the tensor or Kronecker product as $A \otimes B$ (A determines the coarse structure). A matrix M is called "block-permuted", if $M = P \cdot (B_1 \oplus \dots \oplus B_k) \cdot Q$ with permutation matrices P and Q .

Sets and Lists: A set is written in the usual way as $\{t_1, \dots, t_n\}$ and a list (no multiples, order is crucial) as (t_1, \dots, t_n) . Correspondingly we denote with "U" the union of sets or the concatenation of lists.

Groups: Groups are denoted by letters G, H, N, K, \dots . The set of right cosets of H in G is written as $H \backslash G$. If $H \trianglelefteq G$ is a normal subgroup we write G/H instead. Transversals (= systems of right coset representatives) are denoted by T, S, \dots and are lists. Group elements are written by lower case letters g, h, x, y, s, t, \dots , $\mathbf{E} = \{1\}$ denotes the trivial group and \mathbf{Z}_n a cyclic group of order n .

Representations: Representations are written by Greek letters $\phi, \psi, \rho, \dots, \mu$ denotes a monomial representation, λ a representation of degree 1. Sometimes we put the group represented in the index as in ϕ_G . $1_G : g \mapsto 1$ denotes the trivial representation (of degree 1) of G . The degree of ϕ is $\text{deg}(\phi)$ and the character is written as χ_ϕ .

Constructions for representations:

- $\phi_G^A = g \mapsto A^{-1} \cdot \phi_G(g) \cdot A$ is a conjugated (by $A \in \text{GL}_n(\mathbb{K})$) representation of G . We also write $\phi_G \xrightarrow{A} \phi_G^A$.
- $\phi_G \oplus \psi_G = g \mapsto \phi_G(g) \oplus \psi_G(g)$ is the direct sum of the representations ϕ_G, ψ_G of the same group G .
- $\phi_G^n = \phi_G \oplus \dots \oplus \phi_G$ (n summands).

- $\phi_G \otimes \psi_G = g \mapsto \phi_G(g) \otimes \psi_G(g)$ is the inner tensor product of the representations ϕ_G, ψ_G of the same group G and again is a representation of G .
- $\phi_G \# \psi_H = (g, h) \mapsto \phi_G(g) \otimes \psi_H(h)$ is the outer tensor product of the representations ϕ_G of G and ψ_H of H . The outer tensor product is a representation of the direct product $G \times H$.
- $\lambda_G \cdot \phi_G = g \mapsto \lambda_G(g) \cdot \phi_G(g)$ is the linear multiple of the representation ϕ_G with the representation λ_G of degree 1. It is a special case of an inner tensor product.
- $\phi_G \downarrow H = h \mapsto \phi_G(h)$ is the restriction of the representation ϕ_G of G to the subgroup H .
- $\phi_H \uparrow_T G$ denotes the induction of the representation ϕ_H to G with T where H is a subgroup of G and $T = (t_1, \dots, t_n)$ a transversal of $H \backslash G$ of length $n = (G : H)$. Since the equivalence class of the induction is independent of the choice of transversal we will omit it when calculating only up to equivalence. The degree of the induction is $\deg(\phi_H) \cdot n$. It is defined as

$$\phi_H \uparrow_T G = g \mapsto [\dot{\phi}_H(t_i \cdot g \cdot t_j^{-1}) \mid i, j \in \{1, \dots, n\}], \quad \text{with}$$

$$\dot{\phi}_H(x) = \begin{cases} \phi_H(x), & x \in H \\ \mathbf{0}_{\deg(\phi_H)}, & \text{else} \end{cases}.$$

If ϕ_H is of degree 1, then the induction is monomial. If even $\phi_H = 1_H$, then the induction is a permutation representation.

- A regular representation of a group is a special case of a permutation representation given by any induction $1_{\mathbf{E}} \uparrow G$.
- The extension of a representation ϕ of H to a supergroup G of H is denoted by $\bar{\phi}$. Note that the extension of a representation does not exist in general.
- $\phi_H^t = g \mapsto \phi_H(t \cdot g \cdot t^{-1})$ is the inner conjugate of a representation ϕ_H of H by an element t of a supergroup G of H . ϕ_H^t is a representation of the conjugated subgroup $H^t = t^{-1}Ht$. If in particular H is normal in G then the inner conjugate of any representation of H again is a representation of H , however, in general not equivalent to the original one. The definition implies the following rule:

$$(\phi_H^t)^s = \phi_H^{ts} = g \mapsto \phi_H(tsgs^{-1}t^{-1}),$$

i.e. g first is conjugated by the inverse of the *outer* exponent.

3 Constructive Representation Theory

This section contains the mathematical foundation of the decomposition algorithm. Section 3.1 presents theorems on the interaction of induction and other constructions for representations (direct sum, conjugation etc.) which will serve as a “toolkit” throughout this paper. In Section 3.2 we investigate monomial representations, showing that they are essentially direct sum of inductions which allows us to apply the former results. After the short Section 3.3 on intertwining spaces, we derive formulas for decomposition matrices in Section 3.4, which contains the most important mathematical results in this paper. The theorems presented in this section form the basis for doing symbolic computation with representations and are implemented in the package AREP (cf. Section 5).

3.1 Induction

In this section we will present theorems that explain the interaction of the induction with other constructions for representations (cf. Section 2).

3.1.1 Change of Transversal

It is known that the equivalence class of an induction of a representation ϕ of $H \leq G$ is independent of the choice of transversal, i.e.

$$\phi \uparrow_T G \cong \phi \uparrow_{T'} G.$$

We want to determine the conjugating matrix corresponding to the pair (T, T') which establishes equality. Let ϕ be a representation of H , $n = (G : H)$ and $T = (t_1, \dots, t_n)$ an arbitrary transversal of $H \backslash G$. First we consider two particular cases of change of transversal.

Change of coset representatives in T leads to the transversal

$$T' = (h_1 t_1, \dots, h_n t_n), \quad h_i \in H,$$

and has the following effect on the induction:

$$(\phi \uparrow_{T'} G)(x) = \left[\dot{\phi}(t'_i x t_j'^{-1}) \right]_{i,j} = \left[\dot{\phi}(h_i t_i x t_j^{-1} h_j^{-1}) \right]_{i,j} = \left[\dot{\phi}(t_i x t_j^{-1}) \right]_{i,j}^D,$$

where $D = \bigoplus_{i=1}^n \phi(h_i^{-1})$ is a block diagonal matrix with blocks of size $\deg(\phi)$.

Permutation of T with $\sigma \in S_n$ leads to the transversal

$$T' = T^\sigma = (t_{1\sigma^{-1}}, \dots, t_{n\sigma^{-1}})$$

and the induction with T' can be calculated as

$$\begin{aligned} (\phi \uparrow_{T'} G)(x) &= \left[\dot{\phi}(t'_i x t_j'^{-1}) \right]_{i,j} \\ &= \left[\dot{\phi}(t_{i\sigma^{-1}} x t_{j\sigma^{-1}}^{-1}) \right]_{i,j} \\ &= ([\sigma^{-1}, n] \otimes \mathbf{1}_{\deg(\phi)}) \cdot \left[\dot{\phi}(t_i x t_j^{-1}) \right]_{i,j} \cdot ([\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}) \\ &= (\phi \uparrow_T G)(x)^{[\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}}. \end{aligned}$$

The general case of change of transversal can be composed from these two particular cases.

Theorem 1 *Let $H \leq G$ be a subgroup and ϕ a representation of H and let $T = (t_1, \dots, t_n)$ and $T' = (t'_1, \dots, t'_n)$ be two transversals of $H \backslash G$. Assume that σ is the permutation in S_n mapping the cosets (Ht_1, \dots, Ht_n) on the cosets (Ht'_1, \dots, Ht'_n) . Then*

$$(\phi \uparrow_T G)^M = (\phi \uparrow_{T'} G), \quad \text{where } M = ([\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}) \cdot \bigoplus_{i=1}^n \phi(t_{i\sigma^{-1}} \cdot t_i'^{-1}).$$

We call M the matrix corresponding to the change of transversal $T \rightarrow T'$.

Proof 1 We have $\phi \uparrow_{T^\sigma} G = (\phi \uparrow_T G)^{[\sigma, n] \otimes \mathbf{1}_{\deg(\phi)}}$ according to the calculation above. The transition from T^σ to T' is only a change of coset representatives and hence $\phi \uparrow_{T'} G = (\phi \uparrow_{T^\sigma} G)^D$ with $D = \bigoplus_{i=1}^n \phi(t_{i\sigma^{-1}} \cdot t_i^{-1})$ and the result follows.

The change of transversal is the most important basic routine for the computation with inductions. The following theorems reveal the interaction of the induction with other operations. In most of the cases equality is achieved by choosing a certain transversal which makes Theorem 1 a central tool for manipulating inductions.

3.1.2 Double Induction

Induction is a transitive operation. If ϕ is a representation of H and $H \leq K \leq G$ then

$$\phi \uparrow G \cong (\phi \uparrow K) \uparrow G.$$

Equality is established by appropriate choice of the transversal.

Theorem 2 Let $H \leq K \leq G$ be groups and ϕ a representation of H . Suppose $T = (t_1, \dots, t_n)$ and $S = (s_1, \dots, s_m)$ are transversals of $H \setminus K$ and $K \setminus G$ respectively. Then

$$\phi \uparrow_{TS} G = (\phi \uparrow_T K) \uparrow_S G,$$

where $TS = (t_1 s_1, \dots, t_n s_1, t_1 s_2, \dots, t_n s_2, \dots, t_1 s_m, \dots, t_n s_m)$ denotes the complex product of the transversals S and T .

Proof 2 TS is a transversal of $H \setminus G$ and

$$\begin{aligned} (\phi \uparrow_T K) \uparrow_S G &= \left(x \mapsto \left[\dot{\phi}(t_i x t_j^{-1}) \right]_{i,j} \right) \uparrow_S G = x \mapsto \left[\dot{\phi}(t_i s_k x s_\ell^{-1} t_j^{-1}) \right]_{(k,i),(\ell,j)} \\ &= \phi \uparrow_{TS} G. \end{aligned}$$

The previous theorem allows to decompose an induction into small steps along a chain of subgroups. The only thing to do is a change of transversal according to Theorem 1.

3.1.3 Direct Sum

Induction is additive, i.e. if ϕ_1 and ϕ_2 , are representations of $H \leq G$ then

$$(\phi_1 \oplus \phi_2) \uparrow G \cong (\phi_1 \uparrow G) \oplus (\phi_2 \uparrow G).$$

Equality can be achieved by a permutation matrix.

Theorem 3 Let $H \leq G$ be a subgroup with representations ϕ_1 and ϕ_2 of degrees d_1 and d_2 respectively. Assume T is a transversal of $H \setminus G$ of length n . For brevity let $d = d_1 + d_2$. Denote with σ the permutation mapping the list

$$\bigcup_{k=0}^{n-1} (k \cdot d + 1, \dots, k \cdot d + d_1) \cup \bigcup_{k=0}^{n-1} (k \cdot d + d_1 + 1, \dots, (k+1) \cdot d)$$

onto $(1, \dots, n \cdot d)$. Then

$$((\phi_1 \oplus \phi_2) \uparrow_T G)^{[\sigma, n \cdot d]} = (\phi_1 \uparrow_T G) \oplus (\phi_2 \uparrow_T G).$$

Proof 3 The induction is of degree $n \cdot d$. The first concatenation corresponds to the indices of the base vectors of the representation space of $\phi_1 \uparrow G$ in $(\phi_1 \oplus \phi_2) \uparrow G$, analogous for the second concatenation. The corresponding change of bases decomposes the representation.

3.1.4 Conjugation

Induction of equivalent representations ϕ and $\psi = \phi^A$ leads to equivalent results. The conjugating matrix can be stated immediately.

Theorem 4 *Let $H \leq G$ be a subgroup of index n with representation ϕ over \mathbb{K} of degree d and T a transversal of $H \backslash G$. Assume $A \in \text{GL}_d(\mathbb{K})$, then*

$$(\phi^A \uparrow_T G) = (\phi \uparrow_T G)^{(\mathbf{1}_n \otimes A)}.$$

Proof 4 For $x \in G$ we have

$$(\phi^A \uparrow_T G)(x) = \left[\dot{\phi}^A(t_i x t_j^{-1}) \right]_{i,j} = \left[A^{-1} \cdot \dot{\phi}(t_i x t_j^{-1}) \cdot A \right]_{i,j} = (\phi \uparrow_T G)(x)^{(\mathbf{1}_d \otimes A)},$$

as desired.

If in particular A is a decomposition matrix for ϕ , then we can apply Theorem 3 to compute a permutation matrix P such that $(\mathbf{1}_d \otimes A) \cdot P$ decomposes $\phi \uparrow G$ (however, in general not into irreducibles).

3.1.5 Outer Tensor Product

Assume G_1, G_2 are groups and $H_1 \leq G_1, H_2 \leq G_2$ subgroups with representations ϕ_1, ϕ_2 . A well-known theorem (cf. [9], p. 316) says

$$(\phi_1 \uparrow_{G_1}) \# (\phi_2 \uparrow_{G_2}) \cong (\phi_1 \# \phi_2) \uparrow (G_1 \times G_2).$$

As before we can achieve equality by appropriate choice of transversal. The following theorem is the basis for the constructive decomposition of a monomial representation into an outer tensor product.

Theorem 5 *Let $H_1 \leq G_1$ and $H_2 \leq G_2$ be subgroups with representations ϕ_1 and ϕ_2 . Assume $T_1 = (t_1^{(1)}, \dots, t_n^{(1)})$ and $T_2 = (t_1^{(2)}, \dots, t_m^{(2)})$ are transversals of $H_1 \backslash G_1$ and $H_2 \backslash G_2$ respectively. Then*

$$(\phi_1 \uparrow_{T_1} G_1) \# (\phi_2 \uparrow_{T_2} G_2) = (\phi_1 \# \phi_2) \uparrow_{T_1 \times T_2} (G_1 \times G_2),$$

where $T_1 \times T_2 = \left((t_1^{(1)}, t_1^{(2)}), (t_1^{(1)}, t_2^{(2)}), \dots \right)$ denotes the Cartesian product of the lists T_1 and T_2 .

Proof 5 $T_1 \times T_2$ is a transversal of $(H_1 \times H_2) \backslash (G_1 \times G_2)$ and

$$\begin{aligned} & ((\phi_1 \uparrow_{T_1} G_1) \# (\phi_2 \uparrow_{T_2} G_2))(x_1, x_2) \\ &= \left[\dot{\phi}_1(t_i^{(1)} x_1 t_j^{(1)-1}) \right]_{i,j} \otimes \left[\dot{\phi}_2(t_k^{(2)} x_2 t_\ell^{(2)-1}) \right]_{k,\ell} \\ &= \left[(\phi_1 \# \phi_2) \left((t_i^{(1)} x_1 t_j^{(1)-1}), (t_k^{(2)} x_2 t_\ell^{(2)-1}) \right) \right]_{(i,k),(j,\ell)} \\ &= ((\phi_1 \# \phi_2) \uparrow_{T_1 \times T_2} (G_1 \times G_2))(x_1, x_2), \end{aligned}$$

as desired.

If the products $H_1 \times H_2$ and $G_1 \times G_2$ in Theorem 5 are inner direct products then $T_1 \times T_2 = T_1 T_2$ is just the pointwise product of the transversals. In order to decompose an induction into an outer tensor product, however, it is not sufficient that the represented group is a direct product. In Section 3.2 we will learn a necessary and sufficient criterion for the existence of such a decomposition in the particular case of a monomial representation.

3.1.6 Inner Conjugation

The induction of a representation ϕ of H to a supergroup G can be expressed as an induction of an inner conjugate ϕ^s which is a representation of H^s .

Theorem 6 *Let $H \leq G$ be a subgroup, $s \in G$, ϕ a representation of H , and T a transversal of $H \backslash G$. Then*

$$\phi \uparrow_T G = \phi^s \uparrow_{s^{-1}T} G.$$

Proof 6 Let $T = (t_1, \dots, t_n)$ and $x \in G$:

$$(\phi \uparrow_T G)(x) = \left[\dot{\phi}(t_i x t_j^{-1}) \right]_{i,j} = \left[\dot{\phi}^s(s^{-1} t_i x t_j^{-1} s) \right]_{i,j} = (\phi^s \uparrow_{s^{-1}T} G)(x).$$

Note that $s^{-1}T$ is a transversal of $H^s \backslash G$.

In particular we have $\phi \uparrow G \cong \phi^s \uparrow G$. What happens with the inner conjugate of an induction?

Theorem 7 *Let $H \leq K \leq G$ be subgroups, ϕ a representation of H , T a transversal of $H \backslash K$, and $s \in G$. Then*

$$(\phi \uparrow_T K)^s = \phi^s \uparrow_{T^s} K^s,$$

where $T^s = (s^{-1}t_1s, \dots, s^{-1}t_ns)$ denotes the conjugate of the transversal $T = (t_1, \dots, t_n)$ by s (element-wise).

Proof 7 With $x \in K^s$ we observe

$$\begin{aligned} (\phi \uparrow_T K)^s(x) &= (\phi \uparrow_T K)(sxs^{-1}) = \left[\dot{\phi}(t_i s x s^{-1} t_j^{-1}) \right]_{i,j} = \left[\dot{\phi}^s(t_i^s x (t_j^s)^{-1}) \right]_{i,j} \\ &= (\phi^s \uparrow_{T^s} K^s)(x) \end{aligned}$$

as desired.

3.1.7 Restriction

Mackey's subgroup theorem allows the partial decomposition of the restriction of an induction to an arbitrary subgroup. Assume $H, K \leq G$ are subgroups and ϕ is a representation of H . Then

$$(\phi \uparrow G) \downarrow K \cong \bigoplus_{s \in S} (\phi^s \downarrow (H^s \cap K)) \uparrow K$$

where S denotes a system of representatives of the double cosets $H \backslash G / K = \{HgK \mid g \in G\}$. We will give transversals for the inductions in order to establish equality.

Theorem 8 (Mackey) Let $H, K \leq G$ be subgroups, ϕ a representation of H and $S = (s_1, \dots, s_n)$ a system of representatives of the double cosets $H \backslash G / K$. Assume $T_i = (t_{i,1}, \dots, t_{i,r_i})$, $i = 1 \dots n$ are transversals of $(H^{s_i} \cap K) \backslash K$. Then the concatenation

$$T = \bigcup_{i=1}^n s_i T_i \text{ is a transversal of } H \backslash G$$

and

$$(\phi \uparrow_T G) \downarrow K = \bigoplus_{i=1}^n (\phi^{s_i} \downarrow (H^{s_i} \cap K)) \uparrow_{T_i} K.$$

Proof 8 T is a transversal: T is of correct length because of $(G : H) = \sum_{i=1}^n (K : (H^{s_i} \cap K))$. Suppose further $x, y \in T$, $x \neq y$:

Case 1: $\exists i : x, y \in T_i$, hence $x = s_i t_{i,j}$, $y = s_i t_{i,k}$, $j \neq k$,

$$xy^{-1} \in H \Leftrightarrow s_i t_{i,j} t_{i,k}^{-1} s_i^{-1} \in H \Leftrightarrow t_{i,j} t_{i,k}^{-1} \in H^{s_i}$$

which contradicts the fact that T_i is a transversal of $(H^{s_i} \cap K) \backslash K$.

Case 2: $x = s_i t_{i,k}$, $y = s_j t_{j,\ell}$, $i \neq j$,

$$xy^{-1} \in H \Leftrightarrow s_i t_{i,k} t_{j,\ell}^{-1} s_j^{-1} \in H \Leftrightarrow H s_i \underbrace{t_{i,k} t_{j,\ell}^{-1}}_{\in K} = H s_j,$$

a contradiction to the fact that s_i, s_j are elements of different double cosets.

Let $x \in K$:

$$\begin{aligned} (\phi \uparrow_T G)(x) &= \left[\dot{\phi}(t_i x t_j^{-1}) \mid i, j \in \{1, \dots, \sum_{k=1}^n r_k\} \right] \\ &= \bigoplus_{k=1}^n \left[\dot{\phi}(s_k t_{k,i} x t_{k,j}^{-1} s_k^{-1}) \mid i, j \in \{1, \dots, r_k\} \right] \\ &= \bigoplus_{k=1}^n \left[\dot{\phi}^{s_k}(t_{k,i} x t_{k,j}^{-1}) \mid i, j \in \{1, \dots, r_k\} \right] \\ &= \bigoplus_{k=1}^n ((\phi^{s_k} \downarrow (H^{s_k} \cap K)) \uparrow_{T_k} K)(x). \end{aligned}$$

This completes the proof.

In the particular case that $\phi = 1_H$ is the trivial representation, i.e. $\phi \uparrow G$ is a permutation representation, Mackey's theorem yields exactly the decomposition of $(1_H \uparrow G) \downarrow K$ into its transitive constituents. The following two cases will play an important role.

Corollary 9 If $N \trianglelefteq G$, ϕ a representation of N , and T a transversal of G/N then

$$(\phi \uparrow_T G) \downarrow N = \bigoplus_{t \in T} \phi^t.$$

Proof 9 Follows from $N \backslash G / N = G / N$ and Theorem 8.

Corollary 10 *Let $H \leq G$, $N \trianglelefteq G$ with $HN = G$, ϕ a representation of H and T a transversal of $(N \cap H) \backslash N$. Then T is also a transversal of $H \backslash G$ and*

$$(\phi \uparrow_T G) \downarrow N = (\phi \downarrow (N \cap H)) \uparrow_T N.$$

Proof 10 Because of $H \backslash G / N = HN \backslash G = G \backslash G$ there is only one double coset with representative 1. The rest follows from Theorem 8.

The following theorem deals with the induction of a restriction.

Theorem 11 *Let $H \leq G$ be a subgroup, ϕ a representation of G and $T = (t_1, \dots, t_n)$ a transversal of $H \backslash G$. Then*

$$((\phi \downarrow H) \uparrow_T G)^D = (1_H \uparrow_T G) \otimes \phi, \text{ with } D = \bigoplus_{t \in T} \phi(t).$$

Proof 11 For $x \in G$ we have

$$\begin{aligned} ((\phi \downarrow H) \uparrow_T G)^D(x) &= \left[\phi(t_i)^{-1} (\phi \downarrow H)(t_i x t_j^{-1}) \phi(t_j) \right]_{i,j} = \left[1_H(t_i x t_j^{-1}) \cdot \phi(x) \right]_{i,j} \\ &= (1_H \uparrow_T G)(x) \otimes \phi(x). \end{aligned}$$

On the second “=” we mention that the block $\phi(t_i)^{-1} \cdot (\phi \downarrow H)(t_i x t_j^{-1}) \cdot \phi(t_j) = \phi(x)$ if $t_i x t_j^{-1} \in H$, and the all-zero matrix else.

3.1.8 Kernel

The kernel of an induction can be computed as follows.

Theorem 12 *Let $H \leq G$ be a subgroup with representation ϕ . Then the kernel of the induction, $\ker(\phi \uparrow G)$, does not depend on the transversal and can be computed as*

$$\ker(\phi \uparrow G) = \text{core}_G(\ker(\phi) \cap H),$$

where $\text{core}_G(K) = \bigcap_{g \in G} K^g$, the “core of K in G ”, denotes the largest normal subgroup of G contained in $K \leq G$. In particular we have $\ker(1_H \uparrow G) = \text{core}(H)$.

Proof 12 We choose an arbitrary transversal T of $H \backslash G$ and get $x \in \ker(\phi \uparrow_T G) \Leftrightarrow x^{t^{-1}} \in H$ and $\phi(x^{t^{-1}}) = 1$ for all $t \in T \Leftrightarrow x^{g^{-1}} \in H$ and $\phi(x^{g^{-1}}) = 1$ for all $g \in G \Leftrightarrow x \in H^g \cap \ker(\phi)^g$ for all $g \in G$, as desired.

3.2 Monomial Representations

Monomial representations are a natural generalization of permutation representations. A representation $\phi : G \rightarrow \text{GL}_n(\mathbb{K})$ of a group G is called monomial if every image $\phi(g)$, $g \in G$ is a monomial matrix, i.e. $\phi(g)$ contains in every row and column exactly one non-zero entry. While the set of all permutation matrices in $\text{GL}_n(\mathbb{K})$ is finite (of size $n!$) the same does not hold any longer for the set of monomial matrices (if $|\mathbb{K}| = \infty$), not even for the subset of those of finite order.

Note that questions concerning monomial representations cannot easily be reduced to permutation representations. E.g., monomial representations of degree > 1 can entirely be irreducible whereas the same is impossible for permutation representations. Furthermore, there is a class of groups (so-called M -groups, cf. [9], pp. 357) with the property that every representation is equivalent to a monomial one.

In the following we will present the constructive results concerning monomial representations which we will need for their decomposition. A monomial representation essentially is a direct sum of induction of representations of degree 1 (cf. Theorem 15 and Theorem 16), hence the results of the last section can be applied to their investigation.

First we want to generalize some notions concerning permutation representations to monomial representations. For this purpose we associate with every monomial representation μ a unique permutation representation in the following way.

Definition 13 *Let μ be a monomial representation. Substituting all entries $\neq 0$ by 1 in the images of μ leads to a permutation representation which will be denoted by $\hat{\mu}$ and called the “underlying permutation representation” of μ .*

Using $\hat{\mu}$ allows to transfer many concepts for permutation representations to monomial representations. Standard books on permutation representations/groups are Wielandt, [30], and Dixon and Mortimer, [12].

Definition 14 *A monomial representation μ of a group G is called transitive, if $\hat{\mu}$ is transitive. The orbits of μ on $\{1, \dots, \deg(\mu)\}$ are defined as the orbits of $\hat{\mu}$ on this set. The stabilizer $\text{stab}_\mu(i)$ of a point i under μ is the stabilizer of i under $\hat{\mu}$.*

3.2.1 Orbit Decomposition

Like permutation representations also monomial representations can be decomposed by a permutation into its transitive constituents according to their orbits. To achieve further decomposition it is hence possible to restrict to the transitive case which will be investigated in the next paragraphs. We remind the reader that $\phi \xrightarrow{A} \psi$ means $\phi^A = \psi$.

Theorem 15 *Let μ be a monomial representation of degree n of a group G . Assume the orbits of μ on $\{1, \dots, n\}$ are given as the lists O_1, \dots, O_k . Suppose σ is the permutation mapping $L = (\ell_1, \dots, \ell_n) = O_1 \cup \dots \cup O_k$ onto $(1, \dots, n)$, i.e. $\ell_i^\sigma = i$, $i = 1 \dots n$. Then*

$$\mu \xrightarrow{[\sigma, n]} \bigoplus_{i=1}^k \mu_i,$$

where μ_i are transitive monomial representations.

Proof 13 Trivial.

3.2.2 Decomposition into an Induction

Every transitive monomial representation is equivalent to an induction of a representation λ of degree 1 of a subgroup H . This will now be proved constructively.

Theorem 16 Let μ be a transitive monomial representation of a group G over a field \mathbb{K} with representation space $V = \langle v_1, \dots, v_n \rangle$, i.e.

$$v_i \cdot \mu(g) = v_{i\hat{\mu}(g)} \cdot a_i(g)$$

where $a_i(g) \in \mathbb{K}$ for all $g \in G$. Assume $H = \text{stab}_\mu(1)$ and $T = (t_1, \dots, t_n)$ is a transversal of H in G . Then there exists a representation λ of H of degree 1 such that

$$\mu \xrightarrow{D} \lambda \uparrow_T G, \quad \text{where } D = \text{diag}(a_1(t_i)^{-1} \mid i = 1 \dots n).$$

Proof 14 Assume $H = \text{stab}_\mu(1)$ denotes the stabilizer of 1 under μ . Since μ is transitive we have $(G : H) = \text{deg}(\mu) = n$. Let $T = (t_1, \dots, t_n)$ be a transversal of $H \backslash G$ with $1^{\hat{\mu}(t_i)} = i$. For $h \in H$ we observe $v_1 \mu(h) = v_1 a_1(h)$ and define by $\lambda : h \mapsto a_1(h)$ a representation λ of H of degree 1. The representation space of the induced representation then is given by $V^G = \langle v_1 \otimes t_i \mid i = 1 \dots n \rangle$. Setting $t_i g = h_i t_{i'}$, $h_i \in H$ we deduce

$$(v_1 \otimes t_i)(\lambda \uparrow_T G)(g) = v_1 \lambda(h_i) \otimes t_{i'} = (v_1 \otimes t_{i'}) a_1(h_i).$$

We define $w_i = v_1 \mu(t_i) = v_i a_1(t_i)$ for $i = 1 \dots n$ and calculate

$$w_i \cdot \mu(g) = v_1 \cdot \mu(t_i g) = v_1 \cdot \mu(h_i t_{i'}) = v_1 \cdot a_1(h_i) \mu(t_{i'}) = w_{i'} \cdot a_1(h_i).$$

Hence the change of bases $v_i \rightarrow a_1(t_i) v_i$, $i = 1 \dots n$, describes the transformation of μ to $\lambda \uparrow_T G$. The corresponding matrix is

$$D = \text{diag}(a_1(t_i)^{-1} \mid i = 1 \dots n),$$

since G operates from the *right*.

The case of a permutation representation deserves special attention: here μ is even equal to an induction.

Corollary 17 If under the conditions of Theorem 16 μ is even a permutation representation and $H = \text{stab}_\mu(1)$ then

$$\mu = 1_H \uparrow_T G$$

for every transversal $T = (t_1, \dots, t_n)$ of $H \backslash G$ with the property $1^{\mu(t_i)} = i$, $i = 1 \dots n$.

Proof 15 Since all entries in the images of μ are 1 we obtain 1_H as the representation from which μ is induced. The correction matrix D hence degenerates to the identity.

On the uniqueness of this decomposition we prove the following theorem.

Theorem 18 Let λ_i be a representation of $H_i \leq G$ of degree 1 and T_i a transversal of $H_i \backslash G$ for $i = 1, 2$. Suppose

$$\lambda_1 \uparrow_{T_1} G = \lambda_2 \uparrow_{T_2} G,$$

then H_1 and H_2 are conjugated subgroups in G and λ_1, λ_2 are inner conjugated representations.

Proof 16 Let $\mu = \lambda_1 \uparrow_{T_1} G = \lambda_2 \uparrow_{T_2} G$. First, we apply Theorem 8 to get $(\lambda_1 \uparrow_{T_1} G) \downarrow H_1 = \dots \oplus \lambda_1 \oplus \dots$, where the summand λ_1 arises from the double coset $H_1 \backslash G / H_1$. Hence H_1 stabilizes a point under μ and so does H_2 . Since μ is transitive it follows that $H_1 = H_2^s$ for a certain $s \in G$. Using Theorem 6 we get $\mu = \lambda_2 \uparrow_{T_2} G = \lambda_2^s \uparrow_{s^{-1}T_2} G$ where λ_2^s is a representation of H_1 . We consider the transversal elements $u \in T_1$ and $v \in s^{-1}T_2$ which both are in H_1 , w.l.o.g. at the common position j . Then for $x \in H_1$

$$\lambda_1(uxu^{-1}) = \lambda_2^s(vxv^{-1}) \Leftrightarrow \lambda_1(x) = \lambda_2^s(x)$$

and hence λ_1 and λ_2 are inner conjugates.

The following lemma is obvious.

Lemma 19 *Let $H \leq G$ and λ a representation of H of degree 1. If $\mu = \lambda \uparrow_T G$, then $\hat{\mu} = 1_H \uparrow_T G$.*

3.2.3 Decomposition into an Outer Tensor Product

In this paragraph we will prove a necessary and sufficient criterion which determines whether a transitive monomial representation can be decomposed (using a monomial matrix) into a conjugated, outer tensor product of monomial representations. The criterion has been found by Minkwitz for the special case of a permutation representation and will be presented here for the monomial case with a shorter proof.

Theorem 20 *Let μ be a transitive monomial representation of a group $G = N_1 \times N_2$, which is the direct product of N_1 and N_2 . Then μ is equivalent by a monomial matrix M to an outer tensor product of two representations μ_1 of N_1 and μ_2 of N_2 (which necessarily are also monomial and transitive),*

$$\mu \xrightarrow{M} \mu_1 \# \mu_2,$$

if and only if

$$|H| = |H \cap N_1| \cdot |H \cap N_2|.$$

Assume $\mu \xrightarrow{D} \lambda \uparrow_T G$ with a representation λ of degree 1 of H (cf. Theorem 16) then

$$\mu \xrightarrow{DM} ((\lambda \downarrow H \cap N_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow H \cap N_2) \uparrow_{T_2} N_2),$$

where T_i is a transversal of $(H \cap N_i) \backslash N_i$ for $i = 1, 2$ and M is a monomial matrix corresponding to the change of transversals $T \rightarrow T_1 T_2$ (cf. Theorem 1).

Proof 17 Suppose $\mu \xrightarrow{M} \mu_1 \# \mu_2$ and M is monomial. Assume $\mu^D = \lambda \uparrow_T G$ with a representation λ of H , and $\mu_i^{D_i} = \lambda_i \uparrow_{T_i} N_i$, where λ_i is a representation of H_i , $i = 1, 2$. Then $(\lambda \uparrow_T G)^{D^{-1}M} = ((\lambda_1 \uparrow_{T_1} N_1) \# (\lambda_2 \uparrow_{T_2} N_2))^{D_1^{-1} \otimes D_2^{-1}}$. Switching to the underlying permutation representation on both sides yields (cf. Lemma 19, Theorem 5) $(1_H \uparrow_T G)^P = 1_{H_1 H_2} \uparrow_{T_1 T_2} G$ ($H_1 H_2$ is a direct product) where P is the underlying permutation matrix of M . Theorem 1 allows to write $(1_H \uparrow_T G)^P = 1_H \uparrow_{T'} G$ with an appropriate transversal T' . Using Theorem 18 we get that H and $H_1 H_2$ are conjugated in G , by say $x = x_1 x_2$, $x_i \in N_i$. We get $H = (H_1 H_2)^{x_1 x_2} = H_1^{x_1} H_2^{x_2}$,

which is again a direct product and $|H \cap N_i| = |H_i^{x_i}| = |H_i|$, $i = 1, 2$ and hence $|H| = |H_1| \cdot |H_2| = |H \cap N_1| \cdot |H \cap N_2|$ as desired.

Assume now $H_i = H \cap N_i$, $i = 1, 2$ and $|H| = |H_1| \cdot |H_2|$. Because of $H_i \trianglelefteq H$, $i = 1, 2$ and $H_1 \cap H_2 = \{1\}$ we get $H = H_1 \times H_2 = H_1 H_2$ and hence

$$\lambda \uparrow_T G = ((\lambda \downarrow H_1) \# (\lambda \downarrow H_2)) \uparrow_T G \xrightarrow{M} ((\lambda \downarrow H_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow H_2) \uparrow_{T_2} N_2),$$

where the first equality holds since λ is equal to the outer tensor product of the restrictions to the factors (because it is irreducible and of degree 1, [13], p. 54). The second equality holds because of Theorem 5, where M denotes the conjugating monomial matrix corresponding to the change of transversals $T \rightarrow T_1 T_2$. We get

$$\mu \xrightarrow{DM} \lambda \uparrow_{T_1 T_2} G = ((\lambda \downarrow H_1) \uparrow_{T_1} N_1) \# ((\lambda \downarrow H_2) \uparrow_{T_2} N_2)$$

according to Theorem 5 and DM is monomial as required.

Corollary 21 *If ϕ is a regular representation or a representation of degree 1 then ϕ decomposes into an outer tensor product exactly as the group decomposes into a direct product.*

Proof 18 If ϕ is regular, we have $|S| = 1$, if $\deg(\phi) = 1$ then $S = G$. In both cases the condition $|S| = |S \cap N_1| \cdot |S \cap N_2|$ of Theorem 20 is satisfied.

3.2.4 Abelian Groups

In this section we will classify the monomial representations of abelian groups which will also give rise to an efficient way of decomposing them. First we want to recall in the following lemma the relationship between representations of a group G and representations of a factor group G/N .

Lemma 22 *Let $N \trianglelefteq G$ be a normal subgroup. Then the representations of G/N correspond bijectively to those representations of G for which N is contained in the kernel.*

Proof 19 Let $\kappa : G \rightarrow G/N$, $g \mapsto gN$ denote the canonical homomorphism. Assume ϕ is a representation of G/N , then the composition $\phi \circ \kappa$ is a representation of G containing N in the kernel. If vice-versa ϕ is a representation of G satisfying $N \leq \ker(\phi)$ then $gN \mapsto \phi(g)$ is a (well-defined) representation of G/N .

Sometimes we will identify representations of G/N with the corresponding representation of G . The representation theory of abelian groups is very simple since all irreducibles have degree 1 ([18], p. 81). This implies that any representation ϕ of a subgroup $H \leq G$ has an extension $\bar{\phi}$ to G (follows from Theorem 31). We will show in Lemma 32 how the extension can be done constructively.

Now we are ready to classify monomial representations of abelian groups.

Theorem 23 *Let μ be a transitive monomial representation of an abelian group G with decomposition $\mu^D = \lambda \uparrow_T G$ according to Theorem 16, where λ is a representation of $N \leq G$ with extension $\bar{\lambda}$ to G . Then*

$$\mu^{DD_1} = \bar{\lambda} \cdot (1_N \uparrow_T G) \text{ with } D_1 = \text{diag}(\bar{\lambda}(t) \mid t \in T) \text{ and } \bar{\lambda} \downarrow N = \lambda.$$

In particular μ is equivalent (by a diagonal matrix) to the product of a representation of degree 1 and a regular representation of a factor group of G . Thus the irreducible components of μ are pairwise different.

Proof 20 λ can be extended to a representation $\bar{\lambda}$ of G . Using Theorem 11 we get

$$\mu^{DD_1} = (\lambda \uparrow_T G)^{D_1} = ((\bar{\lambda} \downarrow N) \uparrow_T G)^{D_1} = (1_N \uparrow_T G) \otimes \bar{\lambda} = \bar{\lambda} \cdot (1_N \uparrow_T G).$$

By Lemma 22, $1_N \uparrow_T G$ is a regular representation of the abelian group G/N and hence contains pairwise different irreducibles and thus the same holds for μ .

For an abelian group G , the decomposition problem hence reduces to the case of a regular representation. Using Corollary 21 we can decompose the latter into regular representation of cyclic groups of prime power order. This can even be done without computing the (many) normal subgroups of G .

3.3 Intertwining Space

Definition 24 Assume ϕ, ψ are representations of the group G over the field \mathbb{K} with degrees $\deg(\phi) = n$, $\deg(\psi) = m$ respectively. Then the vector space

$$\text{Int}(\phi, \psi) = \{A \in \mathbb{K}^{n \times m} \mid \forall g \in G : \phi(g) \cdot A = A \cdot \psi(g)\}$$

is called the “intertwining space” of ϕ and ψ . Further we will denote by

$$\langle \phi, \psi \rangle = \dim(\text{Int}(\phi, \psi))$$

the dimension of the intertwining space or “intertwining number” of ϕ and ψ .

It is well-known that the intertwining number of two representations is nothing but the scalar product of the corresponding characters ([10], p. 212) justifying the notation above. The scalar product only depends on the equivalence classes of the arguments. For exploring the algebraic structure of representations it is sufficient to consider the intertwining *number*, the constructivity needed in this paper, however, requires some results on the intertwining *space*.

Theorem 25 Let $\phi, \phi_1, \phi_2 \dots, \psi, \psi_1, \psi_2 \dots$ be representations over \mathbb{K} of the group G with degrees $\deg(\phi) = n, \deg(\psi) = m$. Then the following holds:

i) For $A \in \text{GL}_n(\mathbb{K}), B \in \text{GL}_m(\mathbb{K})$: $\text{Int}(\phi^A, \psi^B) = A^{-1} \cdot \text{Int}(\phi, \psi) \cdot B$.

ii) $\text{Int}(\phi_1 \oplus \phi_2, \psi_1 \oplus \psi_2) = \left\{ \begin{bmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{bmatrix} \mid A_{i,j} \in \text{Int}(\phi_i, \psi_j) \right\}$.

iii) (Schur’s Lemma) If ϕ, ψ are irreducible of degree n , then

$$\text{Int}(\phi, \psi) = \begin{cases} \mathbb{K} \cdot A, & \text{for an } A \in \text{GL}_n(\mathbb{K}), & \phi \cong \psi \\ \mathbf{0}_n, & & \phi \not\cong \psi \end{cases}.$$

iv) Assume $\phi = (\mathbf{1}_{n_1} \otimes \phi_1) \oplus \dots \oplus (\mathbf{1}_{n_k} \otimes \phi_k)$ and $\psi = (\mathbf{1}_{m_1} \otimes \phi_1) \oplus \dots \oplus (\mathbf{1}_{m_k} \otimes \phi_k)$, $n_i, m_j \geq 1$, are two completely decomposed representations with irreducible, pairwise different ϕ_i , then

$$\text{Int}(\phi, \psi) = (\mathbb{K}^{n_1 \times m_1} \otimes \mathbf{1}_{\deg(\phi_1)}) \oplus \dots \oplus (\mathbb{K}^{n_k \times m_k} \otimes \mathbf{1}_{\deg(\phi_k)}).$$

Hence every matrix $\in \text{Int}(\phi, \psi)$ is block-permuted according to the homogeneous components of ϕ and ψ .

Proof 21 i) and ii) is straightforward. For iii) let ϕ, ψ be irreducible of degree n . If $\phi \not\cong \psi$ then $\langle \phi, \psi \rangle = 0$, and hence $\text{Int}(\phi, \psi) = \{\mathbf{0}_n\}$. If $\phi \cong \psi$ then exists an invertible matrix A satisfying $\phi^A = \psi$ which generates the intertwining space because of $\langle \phi, \psi \rangle = 1$. iv) follows from ii) and iii).

Further results on the intertwining space of inductions and restrictions can be found in [24, 25].

Computing the intertwining space is expensive in the general case, however it plays an important role in constructive representation theory. It allows, e.g., the computation of a conjugating matrix for two arbitrary, equivalent representations. The computation requires the solution of a system of linear equations.

Assume ϕ, ψ are representations of the same group $G = \langle g_1, \dots, g_n \rangle$. Obviously, a matrix $A = [a_{i,j}]$ lies in $\text{Int}(\phi, \psi) \subset \mathbb{K}^{\deg(\phi) \times \deg(\psi)}$ if and only if the equations

$$\phi(g_i) \cdot A = A \cdot \psi(g_i) \Leftrightarrow \phi(g_i) \cdot A - A \cdot \psi(g_i) = \mathbf{0}_{\deg(\phi), \deg(\psi)}, \quad i = 1 \dots n,$$

are satisfied. Thus we obtain for every generator g the following $\deg(\phi) \cdot \deg(\psi)$ equations in the same number of unknowns:

$$\sum_{i=1}^{\deg(\phi)} \phi(g)_{k,i} \cdot a_{i,\ell} - \sum_{j=1}^{\deg(\psi)} a_{k,j} \cdot \psi(g)_{j,\ell} = 0, \quad k = 1 \dots \deg(\phi), \quad \ell = 1 \dots \deg(\psi).$$

We put this down in the following theorem.

Theorem 26 *The intertwining space of two representations ϕ, ψ of the group G generated by $\{g_1, \dots, g_n\}$ can be computed by solving a system of $n \cdot \deg(\phi) \cdot \deg(\psi)$ linear equations in $\deg(\phi) \cdot \deg(\psi)$ unknowns.*

The system of equations is sparse if the representations ϕ, ψ are.

3.4 Decomposition Matrices

Let ϕ be a representation of the group G . We will refer to a decomposition matrix of ϕ as any matrix A decomposing ϕ into a direct sum of irreducible representations, i.e.

$$\phi^A = \bigoplus_{i=1}^n \rho_i, \quad \rho_i \text{ irreducible for } i = 1 \dots n.$$

Decomposition matrices play virtually no role in books on representation theory, their mere existence is sufficient for the purposes there. In this paper, however, they are the central object of interest. In this section we will derive the the main results of this paper, allowing to construct recursively a highly structured decomposition matrix for a monomial representation of a solvable group. The algorithm given in Section 4 is based on these results.

The term decomposition matrix can also be formulated in the notion of intertwining spaces.

Definition 27 Let ϕ be a representation of a group G and ρ an arbitrary decomposition of ϕ into irreducibles ρ_i , i.e. $\phi \cong \rho = \bigoplus_{i=1}^n \rho_i$. We will call every invertible matrix $A \in \text{Int}(\phi, \rho)$ a “decomposition matrix” for ϕ .

It would be desirable to have a number of theorems which provide for every construction of representation theory (induction, extension, tensor product, etc.) a corresponding formula for the decomposition matrices. However, this is only possible in some cases which we will derive in the following.

3.4.1 Cyclic Groups

Theorem 28 Let $G = \mathbb{Z}_n = \langle x \mid x^n = 1 \rangle$ be the cyclic group of order n with regular representation $\phi : x \mapsto [(1, \dots, n), n]$. Then ϕ is decomposed by the matrix $\text{DFT}_n = [\omega_n^{ij} \mid i, j \in \{0, \dots, n-1\}]$ into $\bigoplus_{i=0}^{n-1} \lambda_i$, where $\lambda_i : x \mapsto \omega_n^i$.

Proof 22 It is sufficient to show that the j th column of DFT_n , $j = 0 \dots n-1$, is an eigenvector of $[(1, \dots, n), n]$ with eigenvalue ω_n^j .

$$\begin{aligned} [(1, \dots, n), n] \cdot (\omega_n^{0 \cdot j}, \dots, \omega_n^{(n-1) \cdot j})^T &= (\omega_n^{1 \cdot j}, \dots, \omega_n^{(n-1) \cdot j}, \omega_n^{0 \cdot j})^T \\ &= \omega_n^j \cdot (\omega_n^{0 \cdot j}, \dots, \omega_n^{(n-1) \cdot j})^T, \end{aligned}$$

as desired.

The basic building blocks for solvable groups are cyclic groups of prime order p . We will see that correspondingly the DFT_p 's are the basic building blocks for decomposition matrices of inductions.

3.4.2 Direct Sum

Theorem 29 Let ϕ_1, ϕ_2 be representations of G with decomposition matrices A_1, A_2 . Then $A_1 \oplus A_2$ is a decomposition matrix for $\phi_1 \oplus \phi_2$.

Proof 23 Trivial.

3.4.3 Outer Tensor Product

Theorem 30 Let ϕ_1, ϕ_2 be representations of N_1, N_2 with decomposition matrices A_1, A_2 , respectively. Then exists a permutation matrix P such that $(A_1 \otimes A_2) \cdot P$ is a decomposition matrix for $\phi_1 \# \phi_2$.

Proof 24 Follows from the distributivity of “ $\#$ ” and the fact that the outer tensor product of two irreducible representations again is irreducible. The computation of P is an easy combinatorial task, which we will omit here.

Note that the corresponding statement does not hold for the inner tensor product. If ϕ, ψ are irreducible representations then $\phi \otimes \psi$ is in general not irreducible. The decomposition of $\phi \otimes \psi$ is also known as the *Clebsch-Gordan-Problem*, [16].

3.4.4 Induction

Transitivity of induction (cf. Theorem 2)

$$\phi_H \uparrow_{TS} G = (\phi_H \uparrow_T K) \uparrow_S G,$$

gives an immediate idea for a stepwise decomposition of an induction. First, determine a maximal subgroup K between H and G . Second, decompose the lower induction by recursion (divide) and derive a decomposition of the upper induction (conquer). The conquer step requires the answers to the following two questions:

1. How do the irreducible components of $\phi_H \uparrow G$ arise from those of $\phi_H \uparrow K$?
2. How to compute a decomposition matrix of $\phi_H \uparrow G$ from one of $\phi_H \uparrow K$?

Unfortunately, the answers to these questions do not exist in general. In the case that $K \trianglelefteq G$ (and hence of prime index), however, Clifford's theorem provides an exact answer to question 1. An answer to question 2 will be presented in Theorem 33. Clifford's theorem in its most general form (cf. [9], p. 345) deals with the restriction of an irreducible representation of a group G to a normal subgroup $N \trianglelefteq G$ of arbitrary index. For the requirements of this paper we will only consider the case where the index $(G : N)$ is prime and present the theorem in a constructive form.

Theorem 31 (Clifford) *Let $N \trianglelefteq^p G$ be a normal subgroup of prime index p , $T = (t^0, t^1, \dots, t^{p-1})$ a transversal of G/N and ρ an irreducible representation of N . Then exactly one of the two following cases applies:*

1. (cf. Figure 1, Case 1) $\rho \cong \rho^{t^i}$ for $i = 0 \dots p-1$. Then ρ has exactly p pairwise inequivalent extensions to G . Assume $\bar{\rho}$ is one of these and $\lambda_i : t \mapsto \omega_p^i$ a representation of G/N , $i = 0 \dots p-1$, then all extensions are given by $\lambda_i \cdot \bar{\rho}$, $i = 0 \dots p-1$. The induction decomposes into irreducibles according to

$$(\rho \uparrow_T G)^A = \bigoplus_{i=0}^{p-1} \lambda_i \cdot \bar{\rho},$$

where $A = \text{diag}(\bar{\rho}(t)^i \mid i \in \{0, \dots, p-1\}) \cdot (\text{DFT}_p \otimes \mathbf{1}_{n/p})$.

2. (cf. Figure 1, Case 2) $\rho \not\cong \rho^{t^i}$ for $i = 0 \dots p-1$. Then the induction $\rho \uparrow G$ is irreducible,

$$(\rho \uparrow_T G) \downarrow N = \bigoplus_{i=0}^{p-1} \rho^{t^i}$$

and

$$\rho^{t^i} \uparrow_T G = (\rho \uparrow_T G)^B,$$

where $B = ([(1, \dots, p)^{-i}, p] \otimes \mathbf{1}_{\text{deg}(\rho)}) \cdot (\mathbf{1}_{(p-i) \cdot \text{deg}(\rho)} \oplus (\mathbf{1}_i \otimes \rho(t^p)))$.

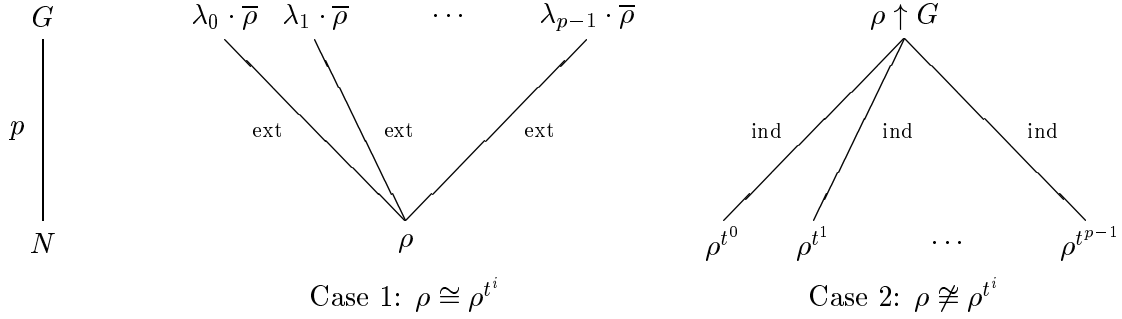


Figure 1: Clifford's Theorem

Proof 25 The proof can be found, e.g., in [6], pp. 88. We will prove only the three equations. Equation in 1.: Using Theorem 11 leads to

$$(\rho \uparrow_T G)^D = (1_N \uparrow_T G) \otimes \bar{\rho}, \quad D = \text{diag}(\bar{\rho}(t)^i \mid i \in \{0, \dots, p-1\}).$$

The representation $1_N \uparrow_T G$ is a regular representation $t \mapsto [(1, \dots, p), p]$ of $G/N \cong \mathbb{Z}_p$ and is decomposed by DFT_p into p representations $t \mapsto \omega_p^i$, $i = 0 \dots p-1$ of degree 1 which gives the first equation.

First equation in 2.: follows from Corollary 9. Second equation in 2.: By Theorem 6 we have $\rho^{t^i} \uparrow_T G = \rho \uparrow_{t^i T} G$. Multiplication of T with t^i permutes the cosets according to $\sigma = (1, \dots, p)^{-i}$. The transition from T^σ to $t^i T$,

$$T^\sigma = (t^i, \dots, t^{(p-1)}, t^0, \dots, t^{(i-1)}) \rightarrow t^i T = (t^i, \dots, t^{(p-1)}, t^p, \dots, t^{(p-i+1)}),$$

is equivalent to a multiplication of the last i transversal elements by t^p . Using Theorem 1 gives the result.

In the case $\rho \cong \rho^t$, ρ has an extension to G . This can for instance be calculated using the Extension Formula of Minkwitz [22, 5]. The formula requires the determination of an extending character and the evaluation of ρ for all $h \in H$. In the particular situation in Clifford's theorem, however, there is also another method which is used in the proof of this theorem in [6] and based on the following lemma.

Lemma 32 *Assume the situation of Theorem 31. In the case $\rho \cong \rho^t$ putting $\rho(t) = A$ defines an extension of ρ to G if and only if $A \in \text{Int}(\rho^t, \rho)$ and $A^p = \rho(t^p)$.*

If the degree of ρ is small and $|N|$ large then this lemma provides a better possibility to compute the extension than Minkwitz' formula. Another advantage is the fact that no extending character has to be computed. Note that $\text{Int}(\rho^t, \rho)$ is of dimension 1, hence any generator differs from $\rho(t)$ only by a scalar multiple.

Clifford's theorem shows how the irreducible representations of G arise from those of N . Accordingly the following theorem shows how a decomposition matrix of a representation ϕ of N gives rise to a decomposition matrix of $\phi \uparrow G$.

Theorem 33 Let $N \stackrel{p}{\trianglelefteq} G$ be a normal subgroup of prime index p and $T = (t^0, t^1, \dots, t^{p-1})$ a transversal of N in G . Assume ϕ is a representation of N of degree n with decomposition matrix A such that $\phi^A = \bigoplus_{i=1}^k \rho_i$, where ρ_1, \dots, ρ_j are exactly those among the ρ_i which have an extension $\bar{\rho}_i$ to G (Theorem 31, Case 1). Denote by $d = \deg(\rho_1) + \dots + \deg(\rho_j)$ the entire degree of the extensible ρ_i and set $\bar{\rho} = \bar{\rho}_1 \oplus \dots \oplus \bar{\rho}_j$. Then exists a permutation matrix P such that

$$M = (\mathbf{1}_p \otimes A) \cdot P \cdot \left(\bigoplus_{t \in T} \bar{\rho}(t) \oplus \mathbf{1}_{p(n-d)} \right) \cdot ((\text{DFT}_p \otimes \mathbf{1}_d) \oplus \mathbf{1}_{p(n-d)})$$

is a decomposition matrix of $\phi \uparrow_T G$. If we denote by $\lambda_i : t \mapsto \omega_p^i$, $i = 0 \dots p-1$, the p one-dimensional representations of G/N then

$$(\phi \uparrow_T G)^M = \bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^j \lambda_i \cdot \bar{\rho}_\ell \oplus \bigoplus_{i=j+1}^k \rho_i \uparrow_T G$$

is the corresponding decomposition into irreducibles.

Proof 26 By Theorem 4 we get

$$(\phi \uparrow_T G)^{(\mathbf{1}_p \otimes A)} = \phi^A \uparrow_T G = \left(\bigoplus_{i=1}^k \rho_i \right) \uparrow_T G.$$

We use Theorem 3 with the block decomposition $\rho_1 \oplus \dots \oplus \rho_j, \rho_{j+1}, \dots, \rho_k$ of ρ to compute a permutation matrix P such that

$$(\phi \uparrow_T G)^{(\mathbf{1}_p \otimes A) \cdot P} = \rho \uparrow_T G \oplus \rho_{j+1} \uparrow_T G \oplus \dots \oplus \rho_k \uparrow_T G.$$

Since ρ has an extension $\bar{\rho}$ to G we get by Theorem 11

$$(\rho \uparrow_T G)^{\bigoplus_{t \in T} \bar{\rho}(t)} = (1_N \uparrow_T G) \otimes \bar{\rho}.$$

The representation $(1_N \uparrow_T G)$ is decomposed by DFT_p into $\bigoplus_{i=0}^{p-1} \lambda_i$ where $\lambda_i : t \mapsto \omega_p^i$. Thus $\bigoplus_{t \in T} \bar{\rho}(t) \cdot (\text{DFT}_p \otimes \mathbf{1}_d)$ is a decomposition matrix for $\rho \uparrow_T G$ with corresponding decomposition $\bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^j \lambda_i \cdot \bar{\rho}_\ell$. The inductions of the ρ_i , $i = j+1 \dots k$, are already irreducible which completes the proof.

3.4.5 Restriction

In the last section we have seen that it is possible to derive a decomposition of $\phi_N \uparrow G$ from a decomposition of ϕ_N , if $N \stackrel{p}{\trianglelefteq} G$. In this section we want to investigate, how to derive in this situation a decomposition of the extension $\bar{\phi}_N$ (if one exists) from a decomposition of ϕ_N . The result will give us a second recursive decomposition method which will allow us to deal with every monomial representation of any solvable group.

Theorem 34 Let $N \stackrel{p}{\trianglelefteq} G$ be a normal subgroup of prime index p and $T = (t^0, t^1, \dots, t^{p-1})$ a transversal of N in G . Let ϕ be a representation of N over the field \mathbb{K} , which has an extension

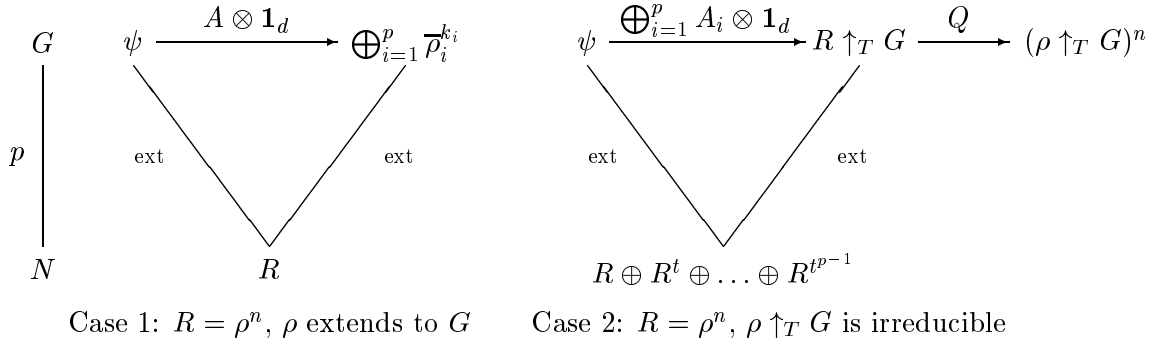


Figure 2: Decomposing the Extension

$\bar{\phi}$ to G . Assume A decomposes ϕ such that equivalent irreducibles are equal and adjacent, $\phi^A = \bigoplus_{i=1}^k R_i$, where $R_i = \rho_i^{n_i}$ is a homogeneous component of multiplicity n_i . We denote $d_i = \deg \rho_i$. Furthermore, we require that whenever $R_i \cong R_j^t$ then even $R_i = R_j^t$ and that these components are adjacent, ordered according to $R_i, R_i^t, \dots, R_i^{t^{p-1}}$. Then exist invertible matrices $A_i \in \mathbb{K}^{n_i \times n_i}$ and a permutation matrix P such that

$$M = A \cdot \left(\bigoplus_{i=1}^k A_i \otimes \mathbf{1}_{d_i} \right) \cdot P$$

is a decomposition matrix of $\bar{\phi}$.

Proof 27 Let ρ be one of the ρ_i with $\rho \not\cong \rho^t$. According to Theorem 31, Case 2, the direct sum $\rho \oplus \rho^t \oplus \dots \oplus \rho^{t^{p-1}}$ extends to $\rho \uparrow_T G$. Since ϕ has an extension to G , the multiplicity of $\rho, \rho^t, \dots, \rho^{t^{p-1}}$ in ϕ is equal.

Now we want to investigate, how far $\bar{\phi}$ is decomposed by A . Obviously, $\bar{\phi}^A$ is an extension of ϕ^A . Extensions of inequivalent extensible ρ_i cannot be equivalent. Also the extension of an extensible ρ_i and the induction of a non-extensible ρ_j cannot be equivalent (follows from Theorem 31). Hence, $\bar{\phi} \xrightarrow{A} \bigoplus_{j=1}^{\ell} \psi_j$ and for each $\psi = \psi_j$, either $\psi \downarrow N = R$ for an extensible homogeneous component R , or $\psi \downarrow N = R \oplus R^t \oplus \dots \oplus R^{t^{p-1}}$ for a non-extensible homogeneous component R .

The remaining task is to decompose the blocks $\psi = \psi_j$ which we will do now for both cases (cf. Figure 2).

Case 1: $\psi \downarrow N = R = \rho^n$ for an extensible ρ . Then ρ has p pairwise inequivalent extensions $\bar{\rho}_i$, $i = 1 \dots p$ and hence ψ decomposes as $\bigoplus_{i=1}^p \bar{\rho}_i^{k_i}$ with certain $k_i \geq 0$, $\sum_{i=1}^p k_i = n$. For the corresponding decomposition matrix B we have $B \in \text{Int}(\psi, \bigoplus_{i=1}^p \bar{\rho}_i^{k_i}) \leq \text{Int}(R, R) = \mathbb{K}^{n \times n} \otimes \mathbf{1}_d$, $d = \deg(\rho)$, according to Theorem 25, iv). Hence $B = A \otimes \mathbf{1}_d$ with an invertible matrix A .

Case 2: $\psi \downarrow N = R \oplus R^t \oplus \dots \oplus R^{t^{p-1}} = R'$, $R = \rho^n$ and $\rho \uparrow_T G$ is irreducible. The direct sum R' can also be extended by $R \uparrow_T G$ (Corollary 9) since all the R^t have the common multiplicity n (see above). For the corresponding conjugation matrix we have $B \in \text{Int}(\psi, R \uparrow_T G) \leq \text{Int}(R', R') = \bigoplus_{i=1}^p \mathbb{K}^{n \times n} \otimes \mathbf{1}_d$, $d = \deg(\rho)$. Hence $B = \bigoplus_{i=1}^p A_i \otimes \mathbf{1}_d$ with invertible matrices A_i . $R \uparrow_T G$ is decomposed into $(\rho \uparrow_T G)^n$ by a permutation matrix Q (using Theorem 3).

Altogether we get that $A \cdot (\bigoplus_{i=1}^k A_i \otimes \mathbf{1}_{d_i}) \cdot P$ is a decomposition matrix for $\bar{\phi}$, where P is the permutation matrix arising from the direct sum of the matrices Q in Case 2. This completes the proof.

Note that the condition $R_i \cong R_j^{t_\ell} \Rightarrow R_i = R_j^{t_\ell}$ in Theorem 34. can be satisfied by a block diagonal matrix, which can be computed block by block using Theorem 26. The requirements concerning the ordering of irreducibles can be established by a suitable permutation matrix.

The problem in Theorem 34 from an algorithmic point of view is the efficient computation of the matrices A_i . In the proof, not the matrices A_i but the matrices $A_i \otimes \mathbf{1}_{d_i}$ have been determined which requires the (expensive) computation of the intertwining space of representations which are a factor of d_i larger than the matrices in which we are actually interested. We will now present efficient methods for the computation of the A_i for both cases (cf. Figure 2) considered in the proof of Theorem 34, following the notation used there. Case 1 will be solved in Theorem 37 and Case 2 in Theorem 38.

Case 1: $\psi \downarrow N = R = \rho^n$ for an extensible ρ . Let $B = A \otimes \mathbf{1}_d$ be the decomposition matrix with $\psi \xrightarrow{B} \bigoplus_{i=1}^p \bar{\rho}_i^{k_i}$. Rather than computing B we want to compute directly A (dealing with smaller matrices). The following definition provides us with the appropriate “shrink operator”.

Definition 35 Let $n, d \geq 1$. We define the “partial trace” operator T_d through

$$T_d: \mathbb{K}^{nd \times nd} \rightarrow \mathbb{K}^{n \times n}, \quad M = [M_{i,j}] \mapsto [\text{tr}(M_{i,j})],$$

where $[M_{i,j}]$ is a division of M into $d \times d$ matrices and $\text{tr}(\cdot)$ denotes the ordinary trace.

We will use the following properties of the operator T_d .

Lemma 36 Let $M \in \mathbb{K}^{nd \times nd}$ and $A \in \mathbb{K}^{n \times n}$. Then

- i) $T_d(M \cdot (A \otimes \mathbf{1}_d)) = T_d(M) \cdot A$.
- ii) $T_d((A \otimes \mathbf{1}_d) \cdot M) = A \cdot T_d(M)$.
- iii) $T_d(M^{A \otimes \mathbf{1}_d}) = T_d(M)^A$.

Proof 28 We proof i), the other statements are shown analogously. Let $A = [a_{i,j}]$ and $M = [M_{i,j}]$ with $d \times d$ matrices $M_{i,j}$, where $i, j = 1 \dots n$. We get $M \cdot (A \otimes \mathbf{1}_d) = [\sum_{k=1}^n M_{i,k} \cdot a_{k,j}]$. Applying T_d yields, using the linearity of the trace, $[\sum_{k=1}^n \text{tr}(M_{i,k}) \cdot a_{k,j}] = T_d(M) \cdot A$ as desired.

The following theorem allows the efficient computation of the matrix $A \otimes \mathbf{1}_d$ in Case 1 (cf. Figure 2).

Theorem 37 We use previous notation. Let $\psi \downarrow N = R = \rho^n$ for an extensible ρ , $d = \deg(\rho)$, and $\bar{R} = \bigoplus_{i=1}^p \bar{\rho}_i^{k_i}$ a decomposition of ψ into irreducibles. $\bar{\rho}_i$ are pairwise inequivalent extensions of ρ . Then exists $g \in G \setminus N$ (set difference) satisfying $\text{tr}(\bar{\rho}_1(g)) \neq 0$ and if $A \in \{A \mid T_d(\psi(g)) \cdot A = A \cdot T_d(\bar{R})\}$ and A is invertible, then $\psi \xrightarrow{A \otimes \mathbf{1}_d} \bar{R}$.

Proof 29 We have

$$\begin{aligned}
\text{Int}(\psi, \overline{R}) &= \{B \mid \psi(g) \cdot B = B \cdot \overline{R}(g), \text{ for all } g \in G\} \\
&= \{A \mid \psi(g) \cdot (A \otimes \mathbf{1}_d) = (A \otimes \mathbf{1}_d) \cdot \overline{R}(g), \text{ for all } g \in G \setminus N\} \\
&= \{A \mid \psi(g) \cdot (A \otimes \mathbf{1}_d) = (A \otimes \mathbf{1}_d) \cdot \overline{R}(g), \text{ for one } g \in G \setminus N\},
\end{aligned}$$

where the first equality holds, since a matrix of structure $B = A \otimes \mathbf{1}_d$ guarantees that B is in the intertwining space of the restrictions to N . The second equality holds since $(G : N)$ is prime. We denote $V_g = \{A \mid \psi(g) \cdot (A \otimes \mathbf{1}_d) = (A \otimes \mathbf{1}_d) \cdot \overline{R}(g)\}$. Mapping the equation defining V_g with T_d yields $W_g = \{A \mid T_d(\psi(g)) \cdot A = A \cdot T_d(\overline{R}(g))\}$ according to Lemma 36, i) and ii). We have to show that $V_g = W_g$. Obviously $V_g \leq W_g$ and $\dim(V_g) = \sum_{i=1}^p k_i^2$. $\psi(g)$ and \overline{R} are conjugated by a matrix $A \otimes \mathbf{1}_d$, hence $T_d(\psi(g))$ and $T_d(\overline{R})$ are conjugated by A (Lemma 36, iii). Thus $W'_g = \{A \mid T_d(\overline{R}(g)) \cdot A = A \cdot T_d(\overline{R}(g))\}$ has the same dimension as W_g . Evaluating T_d yields $T_d(\overline{R}(g)) = \bigoplus_{i=1}^p \text{tr}(\overline{\rho}_1(g)) \cdot a_i \cdot \mathbf{1}_{k_i}$ with pairwise different $a_i \neq 0$ (The a_i are all powers of ω_p , Theorem 31). Since $\text{tr}(\overline{\rho}_1(g)) \neq 0$ by assumption, we get $\dim(W'_g) = \sum_{i=1}^p k_i^2$ and hence $\dim(W'_g) = \dim(W_g) = \dim(V_g)$ as desired.

It remains to show that a $g \in G \setminus N$ with $\text{tr}(\overline{\rho}_1) \neq 0$ exists. Assume $\text{tr}(\overline{\rho}_1(g)) \neq 0$ on all conjugacy classes, which are not in N and let $\overline{\rho}_i$ be another extension of ρ . Then $\overline{\rho}_i = \lambda \cdot \overline{\rho}_1$ with a certain representation of G/N of degree 1 (Theorem 31). Hence $\overline{\rho}_1 \cong \overline{\rho}_i$ which is a contradiction to the fact that ρ has p inequivalent extensions.

Case 2: The following theorem deals with Case 2 (cf. Figure 2), showing that $\bigoplus_{i=1}^p A_i \otimes \mathbf{1}_d$ can be determined without computing an intertwining space.

Theorem 38 *We use previous notation. Let $\psi \downarrow N = R \oplus R^t \oplus \dots \oplus R^{t^{p-1}} = R'$, $R = \rho^n$, $d = \deg(\rho)$ and suppose that $\rho \uparrow_T G$ is irreducible. We evaluate ψ at the transversal $T = (t^0, t^1, \dots, t^{p-1})$ and consider each image to be represented as a $p \times p$ matrix of $nd \times nd$ matrices: $\psi(t^i) = [M_{k,\ell}^{(i)}]_{k,\ell}$. Then each $M_{1,i+1}^{(i)}$, $i = 0 \dots p-1$, has the form $A_i \otimes \mathbf{1}_d$. Furthermore, $\psi \xrightarrow{A} R \uparrow_T G$ with $A = \bigoplus_{i=1}^p A_i^{-1} \otimes \mathbf{1}_d$.*

Proof 30 As in the beginning of the proof of Theorem 37 we have that a matrix $C = \bigoplus_{i=1}^p C_i \otimes \mathbf{1}_d \in \text{Int}(R \uparrow_T G, \psi)$ if and only if $(R \uparrow_T G)(g) \cdot C = C \cdot \psi(g)$ for one $g \in G \setminus N$, e.g. for $g = t$.

Let $R \uparrow_T G \xrightarrow{C} \psi$ with C given as above. We compute

$$(R \uparrow_T G)(t) = \begin{bmatrix} \mathbf{0}_{nd} & \mathbf{1}_n \otimes \mathbf{1}_d & & \\ & & \ddots & \\ & & & \mathbf{1}_n \otimes \mathbf{1}_d \\ \mathbf{1}_n \otimes \rho(t^p) & & & \mathbf{0}_{nd} \end{bmatrix},$$

where omitted blocks are $= \mathbf{0}_{nd}$. In general, the matrix $(R \uparrow_T G)(t^i)$ has in the first block row at position $i+1$ the matrix $\mathbf{1}_{nd}$ and $\mathbf{0}_{nd}$ else ($i = 0 \dots p-1$). Correspondingly, $\psi(t^i) = (R \uparrow_T G)(t^i)^C$ has the matrix $C_1^{-1} C_{i+1} \otimes \mathbf{1}_d$ at position $(1, i+1)$, $i = 0 \dots p-1$. We set $A_j = C_1^{-1} C_j$ and $A' = \bigoplus_{j=1}^p A_j \otimes \mathbf{1}_d$. It remains to show that $R \uparrow_T G \xrightarrow{A'} \psi$ and hence $\psi \xrightarrow{A} R \uparrow_T G$ with $A = A'^{-1}$. Because of the remark at the beginning of this proof, it is sufficient to show it for the image on t . It is $A' = (\mathbf{1}_p \otimes C_1^{-1} \otimes \mathbf{1}_d) \cdot C$. Since the first factor of A' leaves $(R \uparrow_T G)(t)$

(given above) invariant by conjugation, $(R \uparrow_T G)(t)^{A'} = (R \uparrow_T G)(t)^C = \psi(t)$, which completes the proof.

Note that the determination of the conjugating matrix A in Theorem 38 is similar to the determination of the conjugating diagonal matrix D in Theorem 16.

4 Decomposing Monomial Representations

In this section we will present and explain in detail the algorithm for decomposing any monomial representation of any solvable group (with Maschke condition). The crucial point of the derived decompositions is that the decomposition matrix A is determined as a product of highly structured, sparse matrices which can be regarded as a fast algorithm for the multiplication with A . For the special case of a regular representation of a group G we hence obtain a fast Fourier transform for G . A nice feature of the algorithm is the fact that the character table of a group never needs to be computed.

For the algorithm we will use a stronger definition of “decomposition” as in Definition 27. Let μ be a representation of a group G . Decomposing μ means computing a matrix A such that

$$\mu^A = \bigoplus_{i=1}^k \rho_i, \text{ where } \rho_i \text{ is irreducible for } i = 1 \dots k.$$

Furthermore, we require equivalent irreducibles to be equal, i.e. $\rho_i \cong \rho_j \Rightarrow \rho_i = \rho_j$, and adjacent, and all irreducibles shall be (partially) ordered with respect to their degrees.

4.1 The Algorithm

Algorithm 1 Given is a transitive monomial representation μ of degree n of a solvable group G . μ shall be decomposed, i.e.

$$\mu^A = \bigoplus_{i=1}^m \rho_i^{k_i}, \text{ where } \rho_i \text{ is irreducible for } i = 1 \dots m,$$

such that the following conditions hold

1. $i \neq j \Rightarrow \rho_i \not\cong \rho_j$.
2. The ρ_i are ordered by degree.
3. A is a product of highly structured sparse matrices.

For the convenience of the reader we will first give a rough sketch of the recursive algorithm and give the detailed version afterwards. P denotes a permutation matrix and M a monomial matrix.

Sketched:

Case 1: μ is not faithful.

Factor out the kernel and recurse.

Case 2: μ is irreducible.

Nothing to do.

Case 3: μ is not transitive.

$\mu \xrightarrow{P} \mu_1 \oplus \dots \oplus \mu_k$. Recurse with the (transitive) μ_i .

Case 4: μ is a monomial representation of an abelian group.

$\mu \xrightarrow{D} \lambda_G \cdot (1_H \uparrow_T G)$. Recurse with $1_H \uparrow_T G$.

Case 5: μ is a conjugated outer tensor product.

$\mu \xrightarrow{M} \mu_1 \# \dots \# \mu_k$. Recurse with the μ_i .

Case 6: $\mu^D = \lambda_H \uparrow_T G$ and it exists N with $H \leq N \stackrel{p}{\trianglelefteq} G$. (induction recursion)

$\lambda_H \uparrow_T G \xrightarrow{M} (\lambda_H \uparrow_{T_1} N) \uparrow_{T_2} G$. Recurse with $\lambda_H \uparrow_{T_1} N$.

Case 7: Else. (switch recursion)

Compute $N \stackrel{p}{\trianglelefteq} G$. Recurse with $(\lambda_H \uparrow_T G) \downarrow N \xrightarrow{M} \lambda_{H \cap N} \uparrow_{T'} N$.

Detailed:

Case 1: μ is not faithful.

1. Compute the kernel K . If μ is transitive, decompose $\mu \xrightarrow{D} \lambda_H \uparrow_T G$ using Theorem 16 and use Theorem 12.
2. Construct a faithful representation μ' of G/K and decompose $\mu' \xrightarrow{A} \bigoplus_{j=1}^m \rho'_j$ by recursion. We represent G/K (which is solvable) as an ag group to speed up computation (cf. GAP 3 manual, [17], pp. 522).
3. Translate every irreducible ρ'_j of G/K into an irreducible ρ_j of G .

Case 2: μ is irreducible.

The irreducibility is tested with the character of μ ($\langle \chi_\mu, \chi_\mu \rangle \stackrel{?}{=} 1$). $A = \mathbf{1}_n$ is a decomposition matrix with decomposition μ .

Case 3: μ is not transitive.

1. Decompose $\mu \xrightarrow{P_1} \bigoplus_{i=1}^{\ell} \mu_i$ using Theorem 15. The μ_i are transitive and P_1 is a permutation matrix.
2. Decompose $\mu_i \xrightarrow{A_i} \bigoplus_{j=1}^{m_i} \rho_{i,j}^{k_{i,j}}$ for $i = 1 \dots \ell$ by recursion.
3. Compute a block diagonal matrix D which conjugates equivalent irreducibles of different μ_i to be equal. This is done by solving a system of linear equations according to Theorem 26. Note that equivalent irreducibles of the same μ_i are already equal. The blocks in D correspond (in the coarsest case) to the degrees of the $\rho_{i,j}$.

4. Determine a permutation matrix P_2 which sorts the $\rho_{i,j}$ according to their degrees such that equals are adjacent.

$$A = P_1 \cdot \left(\bigoplus_{i=1}^{\ell} A_i \right) \cdot D \cdot P_2 \text{ decomposes } \mu.$$

Case 4: μ is a monomial representation of an abelian group.

1. Decompose $\mu \xrightarrow{D} \lambda_G \cdot (1_H \uparrow_T G)$ using Theorem 23.
2. Decompose $1_H \uparrow_T G \xrightarrow{A} \bigoplus_{j=1}^m \rho_j$ by recursion.

$D \cdot A$ decomposes μ with decomposition $\bigoplus_{j=1}^m \lambda_G \cdot \rho_j$.

Case 5: μ is a conjugated outer tensor product.

1. Decompose $\mu \xrightarrow{M} \mu_1 \# \dots \# \mu_\ell$ using Theorem 30. If G is abelian, then μ is regular (because of Cases 4 and 1) and we can use Corollary 21. M is monomial.
2. Decompose $\mu_i \xrightarrow{A_i} \bigoplus_{j=1}^{m_i} \rho_{i,j}^{k_{i,j}}$ for $i = 1 \dots \ell$ by recursion.
3. Determine a permutation matrix P , such that

$$\left(\bigoplus_{j_1=1}^{m_1} \rho_{1,j_1}^{k_{1,j_1}} \# \dots \# \bigoplus_{j_\ell=1}^{m_\ell} \rho_{\ell,j_\ell}^{k_{\ell,j_\ell}} \right) \xrightarrow{P} \bigoplus_{j_1=1}^{m_1} \dots \bigoplus_{j_\ell=1}^{m_\ell} (\rho_{1,j_1} \# \dots \# \rho_{\ell,j_\ell})^{k_{1,j_1} \dots k_{\ell,j_\ell}}.$$

P is computed from the degrees of the $\rho_{i,j}$.

$$A = M \cdot \left(\bigotimes_{i=1}^k A_i \right) \cdot P \text{ is a decomposition matrix for } \mu \text{ and}$$

$$\mu^A = \bigoplus_{j_1=1}^{m_1} \dots \bigoplus_{j_\ell=1}^{m_\ell} (\rho_{1,j_1} \# \dots \# \rho_{\ell,j_\ell})^{k_{1,j_1} \dots k_{\ell,j_\ell}}.$$

Case 6: If $\mu^D = \lambda_H \uparrow_T G$ then exists N with $H \leq N \trianglelefteq^p G$. (induction recursion)

1. Determine N by building the normal closure \overline{H} of H in G and computing a composition series of G/\overline{H} .
2. Decompose $\lambda_H \uparrow_T G \xrightarrow{M} (\lambda_H \uparrow_{T_1} N) \uparrow_{T_2} G$ using Theorem 1 such that T_2 has the form $T_2 = (t^0, t^1, \dots, t^{p-1})$. M is monomial.
3. Decompose $(\lambda_H \uparrow_{T_1} N) \xrightarrow{B} \bigoplus_{i=1}^m \rho_i^{k_i}$ by recursion.
4. Determine which of the ρ_i have an extension to G (cf. Theorem 31) which is equivalent to $\rho_i^t \cong \rho_i$. We decide this by computing the permutation π_t arising from t permuting the conjugacy classes of N (by conjugation). Then $\rho_i^t \cong \rho_i$ if and only if the list of character values of ρ_i is invariant under π_t . We will denote the extensible representations by σ_ℓ , $\ell = 1 \dots r$ and their direct sum by σ .

5. Conjugate the non-extensible ρ_i such that the following holds: If $\rho_i \cong \rho_j^{t^k}$ then even equality holds. This is done by using Theorem 26 and gives rise to a block diagonal matrix D_1 . We will denote a (complete) direct sum of inner conjugate non-extensibles by $\tau_\ell = \rho \oplus \dots \oplus \rho \oplus \rho^t \oplus \dots \oplus \rho^t \oplus \dots \oplus \rho^{t^{p-1}} \oplus \dots \oplus \rho^{t^{p-1}}$ for $\ell = 1 \dots s$ (Note that the multiplicities of the ρ^{t^k} are not equal in general).
6. Compute a permutation matrix P_1 such that $(\lambda_H \uparrow_{T_1} N) \xrightarrow{B \cdot D_1 \cdot P_1} \sigma \oplus \tau_1 \oplus \dots \oplus \tau_m$. Now we can apply Theorem 33 to obtain the decomposition matrix

$$A' = (\mathbf{1}_p \otimes B \cdot D_1 \cdot P_1) \cdot P \cdot \left(\bigoplus_{i=1}^p \bar{\sigma}(t)^i \oplus \mathbf{1}_{p(n-d)} \right) \cdot ((\text{DFT}_p \otimes \mathbf{1}_d) \oplus \mathbf{1}_{p(n-d)}).$$

for $(\lambda_H \uparrow_{T_1} N) \uparrow_{T_2} G$ Where $d = \deg(\sigma)$ and the extension of σ is computed by extending the its summands σ_ℓ with Lemma 32. The corresponding decomposition into irreducibles can easily be computed using Theorem 33.

7. Consider a summand ρ of τ_ℓ . We conjugate each $\rho^{t^k} \uparrow_{T_2} G$ onto $\rho \uparrow_{T_2} G$ using Theorem 31, Case 2. Altogether this gives rise to a block diagonal matrix D_2 of size $p(n-d)$. Now equivalent irreducibles are equal and we sort them by degree with a permutation matrix P_2 .

$A = D \cdot A' \cdot (\mathbf{1}_{pd} \oplus D_2) \cdot P_2$ is a decomposition matrix for μ with decomposition

$$\mu^A = \left(\bigoplus_{i=0}^{p-1} \bigoplus_{\ell=1}^r \lambda_i \cdot \bar{\sigma}_\ell \oplus \bigoplus_{\ell=1}^s (\tau_{\ell,1} \uparrow_{T_2} G)^{n_\ell} \right)^{P_2},$$

where $\lambda_i = (t \mapsto \omega_p^i)$ and n_ℓ is the number of summands of τ_ℓ .

Case 7: Else. (switch recursion)

1. Decompose $\mu \xrightarrow{D} \lambda_H \uparrow_T G$ using Theorem 16.
2. Determine a normal subgroup $N \stackrel{p}{\leq} G$ using a composition series of G . It is $H \not\leq N$ since Case 4 did not apply and hence $G = HN$.
3. Decompose $(\lambda_H \uparrow_T G) \downarrow N \xrightarrow{M} (\lambda_{H \cap N} \uparrow_{T_1} N)$ by Corollary 10 ($\lambda_{H \cap N} = \lambda_H \downarrow H \cap N$) and $\lambda_{H \cap N} \uparrow_{T_1} N \xrightarrow{B} \bigoplus_{i=1}^m R_i$, $R_i = \rho_i^{k_i}$ by recursion.
4. Determine which of the ρ_i have an extension to G (cf. Theorem 31) which is equivalent to $\rho_i^t \cong \rho_i$. We decide this by computing the permutation π_t arising from t permuting the conjugacy classes of N (through conjugation). Then $\rho_i^t \cong \rho_i$ if and only if the list of character values of ρ_i is invariant under π_t .
5. Conjugate the non-extensible ρ_i such that the following holds: If $\rho_i \cong \rho_j^{t^k}$ then even equality holds. This is done by using Theorem 26 and gives rise to a block diagonal matrix D_1 .
6. Compute a permutation matrix P_1 , which permutes the homogeneous components $R = R_i$ such that non-extensible, inner conjugate components are adjacent, ordered according to $R, R^t, \dots, R^{t^{p-1}}$.

7. Decompose $\lambda_H \uparrow_{T_1} G \xrightarrow{B \cdot D_1 \cdot P_1} \bigoplus_{j=1}^{m'} \psi_j$. For each j , either (1) $\psi_j \downarrow N = R$, $R = \rho^n$ for an extensible ρ or (2) $\psi_j \downarrow N = R \oplus R^t \oplus \dots \oplus R^{t^{p-1}}$, $R = \rho^n$ for a non-extensible $\rho = \rho_i$ (cf. Theorem 34).
8. Case (1), $\psi_i \downarrow N = R$. Extend $R = \rho^n$ by $\bigoplus_{j=1}^p \bar{\rho}_j^{\ell_j} \cong \psi_i$ using Lemma 32. The multiplicities ℓ_i can be determined from the character of ψ_i . Decompose ψ_i with $A_i = C_i \otimes \mathbf{1}_{\deg(\rho)}$ into $\bigoplus_{j=1}^p \bar{\rho}_j^{\ell_j}$ using Theorem 37. Set $Q_i = \mathbf{1}_{\deg(R)}$.
9. Case (2), $\psi_i \downarrow N = R \oplus R^t \oplus \dots \oplus R^{t^{p-1}}$, $R = \rho^n$. Decompose ψ_i with $A_i = (\bigoplus_{j=1}^n C_j \otimes \mathbf{1}_{\deg(\rho)}) \cdot Q_i$ into $(\rho \uparrow_T G)^n$ using Theorem 38. Q_i is a permutation matrix.
10. Order the irreducibles by degree with a permutation matrix P_2 .

$M \cdot B \cdot D_1 \cdot P_1 \cdot \left(\bigoplus_{i=1}^{m'} A_i \right) \cdot Q \cdot P_2$ is a decomposition matrix for μ , where Q is the direct sum of the Q_i .

The first thing to note on the algorithm is that the essential steps are given by the Cases 2, 3, 6, 7. Case 3 reduces to the transitive case in which $\mu \xrightarrow{D} \lambda_H \uparrow G$ can be written as an induction. Since G is solvable, we now find a normal subgroup $N \trianglelefteq G$ of prime index p with either $H \leq N$ and use induction recursion (Case 6) to recurse, or $H \not\leq N$ and use switch recursion (Case 7) to recurse. Induction recursion reduces the degree of the representation and the size of the group, switch recursion reduces only the size of the group. Hence, invoking only these four cases, the algorithm terminates.

Decomposing into an outer tensor product, if possible, yields a simpler decomposition matrix, however requires the computation of all normal subgroups (in the non-abelian case). In the actual implementation, this case can be deactivated on calling the function. We will later (cf. Section 4.3) observe the influence of this on runtime. Reduction to a faithful representation (Case 1) speeds up decomposition by restricting to the smallest possible group represented by a given representation. Abelian groups have a large number of subgroups, which makes the decomposition into an outer tensor product inefficient. Case 4, together with Case 1, reduces the abelian case to regular representations, which decompose into an outer tensor product, as the group into a direct product (Corollary 21). The latter decomposition can be done efficiently (cf. the GAP 3 function `IndependentGeneratorsAbelianPermGroup`). The correctness of the algorithm follows from the theorems on which it is based and we get:

Theorem 39 *Algorithm 1 terminates and is correct.*

Note that by far the most expensive part of the algorithm is the switch recursion, Case 7, because the “conquer part” requires to perform a conjugation (in Step 7). In all other cases, the irreducibles as well as the decomposition matrix are determined by mere construction, dealing only with small matrices (compared to the degree of the representation). Switch recursion is needed for the decomposition of $\lambda_H \uparrow G$ if and only if H is not subnormal in G , i.e. H is not contained in any composition series of G .

The algorithm is implemented in the function `DecompositionMonRep` contained in the package `AREP` (cf. Section 5).

4.2 An Example

As an example we will consider the group $G = \text{SL}(2, 3)$ which is a semidirect product of $Z_3 = \langle r \mid r^3 = 1 \rangle$ with the quaternion group $Q_8 = \langle s, t \mid s^4 = t^4 = 1, s^t = s^{-1} \rangle$ defined by $\text{SL}(2, 3) = \langle r, s, t \mid s^r = t^{-1}, t^r = st \rangle$. Let $\mu = 1_E \uparrow_T G$ be the regular representation with $T = (1, r, r^2, r^2s, s, rs, rt, r^2t, t, sr, s^2t, rsr, rs^2, r^2s^2, s^2, rtr, st, tr, rts, ts, sr^2, s^3, tr^2, str)$. Decomposing μ with Algorithm 1 leads to Case 6 (induction recursion) which we will now work out step by step.

1. The trivial subgroup E is the normal closure of itself and we get $N = Q_8$ as a normal subgroup of index 3 (this is the only possible choice for N).

2. We decompose $1_E \uparrow_T G \xrightarrow{M} (1_E \uparrow_{T_1} N) \uparrow_{T_2} G$ using Theorem 2 with transversals $T_1 = (1, s, t, s^2t, s^2, st, ts, s^3)$, $T_2 = (1, r, r^2)$ and

$$M = [(2, 9, 3, 17, 6, 15, 5)(4, 20, 7, 16, 24, 14, 21, 18, 11)(8, 22)(12, 23, 19), 24].$$

3. We decompose recursively $(1_E \uparrow_{T_1} N) \xrightarrow{B} \rho_1 \oplus \rho_2 \oplus \rho_3 \oplus \rho_4 \oplus \rho_5^2$, where

$$\begin{aligned} B = & [(2, 5, 3)(6, 8, 7), 8] \cdot \\ & (\mathbf{1}_2 \otimes ((\text{DFT}_2 \otimes \mathbf{1}_2) \cdot \text{diag}(1, 1, 1, \omega_4) \cdot (\mathbf{1}_2 \otimes \text{DFT}_2))) \cdot \\ & [(3, 5)(4, 8, 7, 6), (1, 1, 1, 1, 1, 1, -1, 1)] \cdot \\ & ((\text{DFT}_2 \otimes \mathbf{1}_2) \oplus \mathbf{1}_4) \cdot [(2, 4), 8], \end{aligned}$$

$\rho_1 = 1_N$, $\rho_2 : s \mapsto -1, t \mapsto -1$, $\rho_3 : s \mapsto -1, t \mapsto 1$, $\rho_4 : s \mapsto 1, t \mapsto -1$, and $\rho_5 : s \mapsto [(1, 2), (-1, 1)], t \mapsto \text{diag}(\omega_4, -\omega_4)$.

4. A system of representatives of the conjugacy classes of N is given by $C = (1, s, t, s^2, st)$. The permutation induced by r on C is $\pi_r = (2, 3, 5)$. Let χ_i denote the character of ρ_i given by values on C . We have $\chi_1 = (1, 1, 1, 1, 1)$, $\chi_2 = (1, -1, -1, 1, 1)$, $\chi_3 = (1, -1, 1, 1, -1)$, $\chi_4 = (1, 1, -1, 1, -1)$, $\chi_5 = (2, 0, 0, -2, 0)$, and it is easily seen that χ_1 and χ_5 are invariant under π_r and hence have an extension to G . We get $\sigma = \rho_1 \oplus \rho_5^2$.

5. ρ_2, ρ_3, ρ_4 are inner conjugates with $\rho_4 = \rho_2^t, \rho_3 = \rho_2^2$. Equality holds since they are of degree 1. Thus D_1 is the identity.

6. We have to permute the irreducibles into the order $\rho_1 \oplus \rho_5^2 \oplus \rho_2 \oplus \rho_4 \oplus \rho_3$, which is done by $P_1 = [(2, 6, 3, 8, 5)(4, 7), 8]$. The permutation

$$P = [(6, 16, 23, 21, 15, 20, 14, 17, 11, 8, 22, 18, 12, 9)(7, 19, 13, 10), 24]$$

maps $(\sigma \oplus \rho_2 \oplus \rho_4 \oplus \rho_3) \uparrow G$ onto the direct sum of the inductions. An extension of ρ_1 is given by $\bar{\rho}_1 = 1_G$, an extension of ρ_5 by

$$\bar{\rho}_5(r) = \begin{bmatrix} -1/2 - 1/2 \cdot \omega_4 & 1/2 + 1/2 \cdot \omega_4 \\ -1/2 + 1/2 \cdot \omega_4 & -1/2 + 1/2 \cdot \omega_4 \end{bmatrix}$$

which determines $\bar{\sigma} = \bar{\rho}_1 \oplus \bar{\rho}_5^2$ and hence the matrix A' . The 3 irreducible representations arising from the factor group $G/N \cong Z_3$ are given by $\lambda_i : r \mapsto \omega_3^i, i = 0 \dots 2$.

7. We conjugate $\rho_2^{t^i} \uparrow_{T_2} G$ onto $\rho_2 \uparrow_{T_2} G$, $i = 1, 2$ using Theorem 31, Case 2, which gives rise to $D_2 = [(19, 20, 21)(22, 24, 23), 24]$ (note that $\rho_2(r^3) = 1$). The irreducibles are already sorted by degree.

After simplifications we obtain that (with $M = \bar{\rho}_5(r)$)

$$\begin{aligned}
A = & [(2, 9, 6, 15, 3, 17, 5, 4, 24, 13, 11, 8, 21, 20, 7, 10, 12, 23, 22)(14, 19, 16, 18), 24] \cdot \\
& (\mathbf{1}_3 \otimes ((\mathbf{1}_2 \otimes ((\text{DFT}_2 \otimes \mathbf{1}_2) \cdot \text{diag}(1, 1, 1, \omega_4) \cdot (\mathbf{1}_2 \otimes \text{DFT}_2)))) \cdot \\
& [(3, 5)(4, 8, 7, 6), (1, 1, 1, 1, 1, 1, -1, 1)] \cdot ((\text{DFT}_2 \otimes \mathbf{1}_2) \oplus \mathbf{1}_4))) \cdot \\
& [(2, 20, 18, 19, 23, 14, 8, 5)(3, 24, 15, 9, 6)(4, 16, 10, 21, 12, 17, 11, 22, 13, 7), 24] \cdot \\
& (\mathbf{1}_6 \oplus M \oplus M \oplus \mathbf{1}_1 \oplus M^2 \oplus M^2 \oplus \mathbf{1}_9) \cdot ((\text{DFT}_3 \otimes \mathbf{1}_5) \oplus \mathbf{1}_9) \cdot \\
& [(2, 12, 4, 14, 6, 3, 13, 5, 15, 7, 8, 9, 10, 11), 24]
\end{aligned}$$

is a decomposition matrix for μ (and hence a Fourier transform for G) with corresponding decomposition

$$\mu \xrightarrow{A} 1_G \oplus \lambda_1 \oplus \lambda_2 \oplus \bar{\rho}_5^2 \oplus (\lambda_1 \cdot \bar{\rho}_5)^2 \oplus (\lambda_2 \cdot \bar{\rho}_5)^2 \oplus (\rho_2 \uparrow_{T_2} G)^3.$$

$G = \text{SL}(2, 3)$ is the smallest group which is not an M -group, i.e. it has an irreducible representation which cannot be conjugated to be monomial. Decomposing μ with the implemented function `DecompositionMonRep` (cf. Section 5) takes 1.85 sec CPU time on a Pentium II, 233 MHz running Linux. For further timings see the next section.

4.3 Runtimes

Determining the asymptotic runtime of Algorithm 1 is a difficult task, since a lot of high level subroutines are used, as computing the normal closure of a subgroup, a composition series, the stabilizer of a point, the character of a representation (which involves evaluating a homomorphism), etc. In the actual implementation of Algorithm 1 contained in the GAP package AREP (cf. Section 5), these subroutines are provided by standard GAP functions, and their asymptotic runtime is usually not given in the manual.

To get an idea of the asymptotic behavior as well as the order of magnitude of the runtime of the decomposition algorithm, we consider the special case of regular representations, which implies the construction of fast Fourier transforms, however excludes the usage of “switch recursion” (Algorithm 1, Case 7). The experiment is set up as follows. For each number $n = 1 \dots 500$ we consider all groups (up to isomorphism) of order n , or a random sample of 100, if their number is larger than 100. We determine the average runtime for decomposing their regular representations with the function `DecompositionMonRep` implementing Algorithm 1. The machine is a Pentium II, 233 MHz running Linux. Altogether we obtain 500 data points as displayed in Figure 3, a). The abscissa carries the group size n , the ordinate the average runtime in seconds. The outliers of the mainstream correspond to numbers n with a large number of prime factors, e.g. 16, 32, 64, 128, or 48, 96, 192, 384. The fastest runtimes correspond to prime numbers n (in this case only one group exists) and give rise to the vein below the mainstream.

As mentioned at the end of Section 4.1, the decomposition algorithm can be run without invoking the decomposition into an outer tensor product (Case 5), which requires the computation of all normal subgroups. Running the same experiment as above without invoking Case 5 yields the slightly different diagram displayed in Figure 3, b). We observe that, first, as expected, the outliers are less significant and second, the mainstream is slightly slower (the gap to the prime

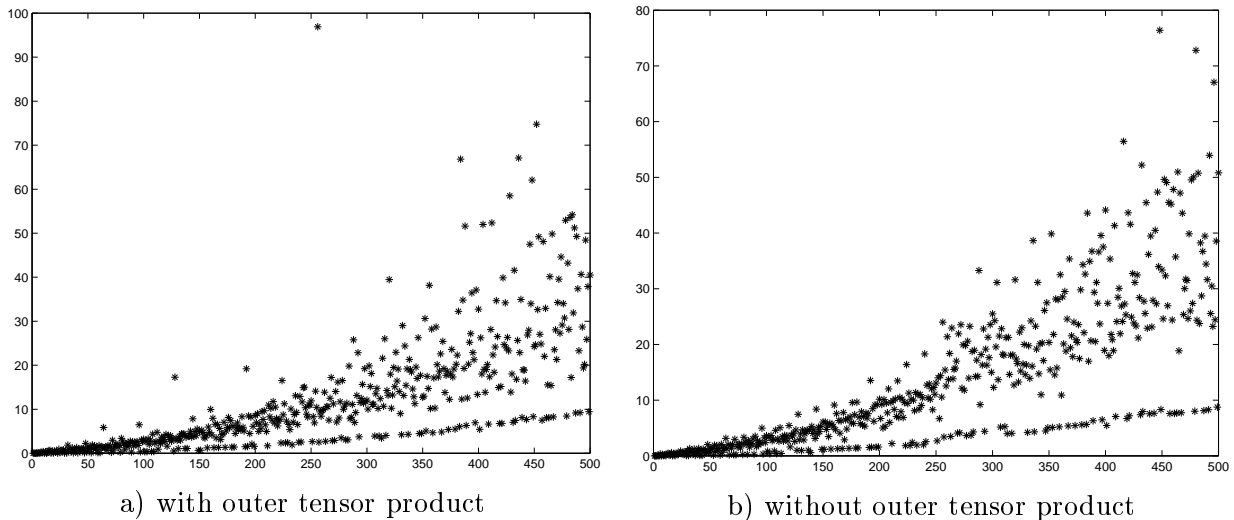


Figure 3: Average runtime (sec) for decomposing a regular representation of group size n

number is larger), which shows that in these cases, decomposing into an outer tensor product even yields a speedup.

Dividing the runtimes by n^2 as shown in Figure 4 gives an idea of the asymptotic behavior. However, we only want to record that the decomposition of a regular representation can be performed in a reasonably short time, considering the mathematical complexity of this task.

5 AREP – a Package for Constructive Representation Theory

The results of this paper and in particular the algorithm for decomposing monomial representations of solvable groups (cf. Section 4) has been realized in the package AREP, [15], by Sebastian Egner and the author. AREP is implemented in the language GAP v3.4.4, a computer algebra system specialized on computational group theory, and has been accepted as a GAP share package. The goal of AREP was to create a general purpose package for computing with group representations up to equality, not only up to equivalence, as it is done by using characters. In this sense, AREP provides the data types and the infrastructure to do efficient symbolic computation with structured matrices and representations.

The central objects in this package are the recursive data types `AREP` and `AMat`. An `AREP` is a GAP record representing a representation. The record contains a number of fields which uniquely characterize a representation up to equality, e.g. degree, characteristic, and the represented group always have to be present.

There are a number of elementary constructors allowing to create an `AREP`, e.g., by specifying the images on a set of generators of the group (`AREPByImages`). Furthermore, there are constructors building a higher structured `AREP` from given `AREPs` (e.g. `DirectSumAREP`, `InductionAREP`). The idea is not to immediately evaluate such a construction, but to build an `AREP` representing it. E.g., an `AREP` representing a direct sum has a field `summands` containing the list of summands. Conversion to an (unstructured) matrix representation is performed by calling the appropriate function. On the other side there are functions converting an unstructured, e.g. monomial `AREP`,

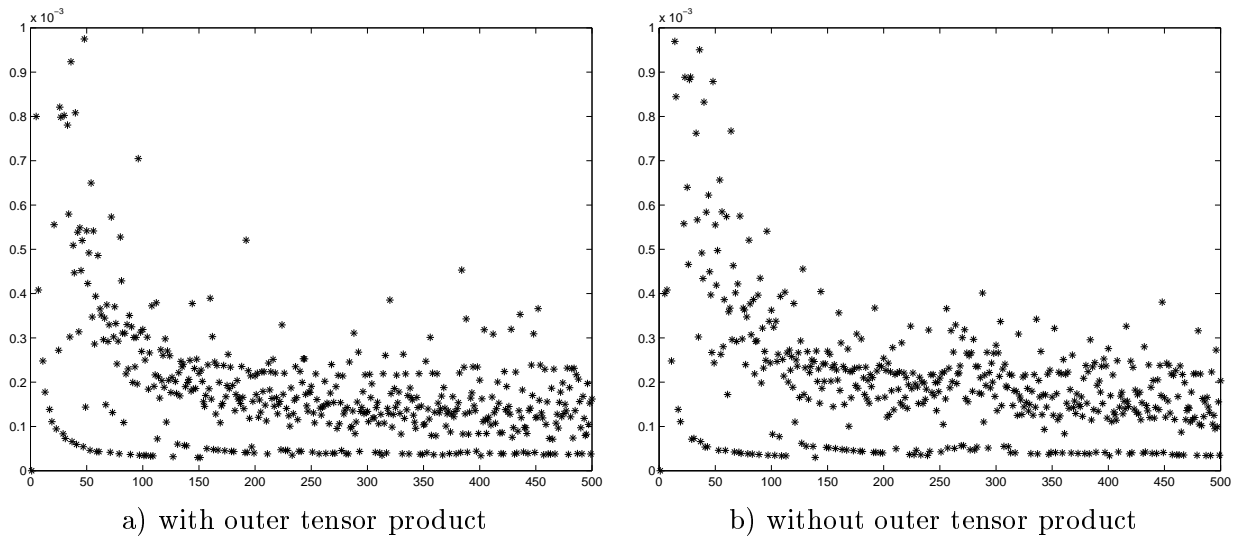


Figure 4: Runtimes from Figure 3 divided by n^2

into a highly structured **AREP**, e.g. a conjugated induction of a representation of degree 1 (cf. Theorem 16), which is mathematical *identical* to the original one. Permutation and monomial representations has been given special attention in the package since they are efficiently to store and to compute with and they were the central object of our interest. The decomposition algorithm in Section 4 is realized in the function `DecompositionMonRep` which takes a monomial representation and returns a conjugated direct sum of irreducibles, which, as before, is mathematical identical to the input. The highly structured decomposition matrix is represented by an **AMat** (explained below).

The data type **AMat** has been created according to the same principle as **AREP**, as a GAP record representing a matrix. Again, there are elementary constructors to create an **AMat**, e.g., `AMatPerm` takes a permutation, a degree, and a characteristic and builds an **AMat** which efficiently represents a permutation matrix. Higher constructors allow to recursively build the product, direct sum, tensor product, etc., of **AMats** and are not evaluated until the appropriate function is invoked. Thus, **AMat** allows to build structured matrices which are more efficient to store and easier to handle than the (mathematical identical) represented matrices, e.g. determinant, trace and inverse can be computed efficiently by using well-known mathematical rules.

For a description of further capabilities of AREP, e.g. symmetry analysis and matrix decomposition, we refer to the AREP manual and web page, [15].

6 Acknowledgements

The main part of the work presented in this paper was developed when the author was with Prof. Beth at the Institute of Algorithms and Cognitive Systems at the University of Karlsruhe, Germany. The author would like to thank Prof. Beth for his full support which made this work possible. The author is particularly indebted to Dr. Sebastian Egner who brought the author's attention to this topic and without whom neither AREP nor this paper would exist. Thanks also to Prof. Johnson for helpful discussions and proofreading.

References

- [1] L Auslander, E. Feig, and S. Winograd. Abelian Semi-simple Algebras and Algorithms for the Discrete Fourier Transform. *Advances in Applied Mathematics*, 5:31–55, 1984.
- [2] T Beth. On the computational complexity of the general discrete Fourier transform. *Theoretical Computer Science*, 51:331–339, 1987.
- [3] Thomas Beth. *Verfahren der Schnellen Fouriertransformation*. Teubner, 1984.
- [4] M. Clausen. *Beiträge zum Entwurf schneller Spektraltransformationen (Habilitationsschrift)*. University of Karlsruhe, 1988.
- [5] M. Clausen. A Direct Proof of Minkwitz’s Extension Theorem. *AAECC*, 8:305–306, 1997.
- [6] M. Clausen and U. Baum. *Fast Fourier Transforms*. BI-Wiss.-Verl., 1993.
- [7] J. H. Conway, R. T. Curtis, S. P. Norton, and R. A. Wilson. *Atlas of Finite Groups*. Clarendon Press, Oxford, 1985.
- [8] James W. Cooley and John W. Tukey. An Algorithm for the Machine Calculation of Complex Fourier Series. *Mathematics of Computation*, 19:297–301, 1965.
- [9] W.C. Curtis and I. Reiner. *Representation Theory of Finite Groups*. Interscience, 1962.
- [10] W.C. Curtis and I. Reiner. *Methods of Representation Theory*, volume 1. Interscience, 1981.
- [11] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups . *Amer. Math. Soc.*, 3(2):297–332, 1990.
- [12] J.D. Dixon and B. Mortimer. *Permutation Groups*. Springer, 1996.
- [13] L. Dornhoff. *Group Representation Theory*. Pure and Applied Mathematics. Dekker New York, 1971.
- [14] S. Egner. *Zur Algorithmischen Zerlegungstheorie Linearer Transformationen mit Symmetrie*. PhD thesis, Universität Karlsruhe, Informatik, 1997.
- [15] S. Egner and M. Püschel. *AREP – A Package for Constructive Representation Theory and Fast Signal Transforms*. GAP share package, 1998.
<http://avalon.ira.uka.de/home/pueschel/arep/arep.html>.
- [16] W. Fulton and J. Harris. *Representation Theory*. Springer, 1991.
- [17] The GAP Team, School of Mathematical and Computational Sciences, U. St. Andrews, Scotland. *GAP – Groups, Algorithms, and Programming*, 1997.
<http://www-gap.dcs.st-and.ac.uk/~gap/>.
- [18] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 1993.

- [19] D. Maslen and D. Rockmore. Generalized FFTs – A survey of some recent results. In *Proceedings of IMACS Workshop in Groups and Computation*, volume 28, pages 182–238, 1995.
- [20] T. Minkwitz. *Algorithmentsynthese für lineare Systeme mit Symmetrie*. PhD thesis, Universität Karlsruhe, Informatik, 1993.
- [21] T. Minkwitz. Algorithms Explained by Symmetry. *Lecture Notes on Computer Science*, 900:157–167, 1995.
- [22] T. Minkwitz. Extension of Irreducible Representations. *AAECC*, 7:391–399, 1996.
- [23] T. Minkwitz. On the generation of algorithms for linear transforms and systems with symmetry. Technical report, EISS, 1997.
- [24] M. Püschel. *Konstruktive Darstellungstheorie und Algorithmengenerierung*. PhD thesis, Universität Karlsruhe, Informatik, 1998. Translated in [25].
- [25] M. Püschel. Constructive Representation Theory and Fast Signal Transforms. Technical Report Drexel-MCS-1999-1, Drexel University, Philadelphia, 1999. Translation of [24].
- [26] D. Rockmore. Efficient computation of Fourier inversion for finite groups. *Assoc. Comp. Mach.*, 41(1):31–66, 1994.
- [27] D. Rockmore. Some applications of generalized FFT's. In *Proceedings of DIMACS Workshop in Groups and Computation*, volume 28, pages 329–370, 1995.
- [28] J.P. Serre. *Linear Representations of Finite Groups*. Springer, 1977.
- [29] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, 1999.
- [30] Helmut Wielandt. *Finite Permutation Groups*. Academic Press, 1964.