Irreducible Decomposition of Representations of Finite Groups via Polynomial Computer Algebra

Vladimir V. Kornyak

Abstract. An algorithm for splitting permutation representations of finite group over fields of characteristic zero into irreducible components is described. The algorithm is based on the fact that the components of the invariant inner product in invariant subspaces are operators of projection into these subspaces. An important part of the algorithm is the solution of systems of quadratic equations. A preliminary implementation of the algorithm splits representations up to hundreds of thousands of dimensions. Examples of computations are given.

1. Introduction. One of the central problems of group theory and its applications in physics is the decomposition of linear representations of groups into irreducible components. In general, the problem of splitting a module over an associative algebra into irreducible submodules is quite nontrivial. An overview of the algorithmic aspects of this problem can be found in [1]. For vector spaces over finite fields, the most efficient is the Las Vegas type algorithm called *MeatAxe*. This algorithm played an important role in solving the problem of classifying finite simple groups. However, the approach used in the *MeatAxe* is ineffective in characteristic zero, whereas quantum-mechanical problems are formulated just in Hilbert spaces over fields of characteristic zero. Our algorithm deals with representations over such fields, and its implementation copes with dimensions up to hundreds of thousands that is not less than the dimensions achievable for the *MeatAxe*. The algorithm requires knowledge of the centralizer ring of the considered group representation. In the general case, the calculation of the centralizer ring is a problem of linear algebra, namely, solving matrix equations of the form $AX = XA$. In the case of permutation representations, there is an efficient algorithm for computing the centralizer ring — it is reduced to constructing the set of orbitals. In addition, permutation representations are fundamental in the sense that any linear representation of a finite group is a subrepresentation of some permutation representation, and we use this fact in some quantum mechanical considerations [2, 3]. Therefore, we consider here only permutation representations.

2. Mathematical preliminaries. Let G be a *transitive* permutation group on the set $\Omega \cong \{1, \ldots, \mathsf{N}\}$. The action of $g \in \mathsf{G}$ on $i \in \Omega$ is denoted by i^g. A representation of G in an N-dimensional vector space over a field $\mathcal{F}$ by the matrices $\mathrm{P}(g)$ with the entries $\mathrm{P}(g)_{ij} = \delta_{i^g j}$, where δ_{ij} is the Kronecker delta, is called a *permutation representation*. We assume that the permutation representation space is a Hilbert space $\mathcal{H}_\mathsf{N}$. From a constructive point of view it is sufficient to assume that the base field $\mathcal{F}$ is a *minimal splitting field* of the group G. Such field is a subfield of an m-th cyclotomic field, where m is a divisor of the *exponent* of G. The field $\mathcal{F}$, being an abelian extension of $\mathbb{Q}$, is a constructive dense subfield of $\mathbb{R}$ or $\mathbb{C}$.

An orbit of G on the Cartesian square $\Omega \times \Omega$ is called an *orbital* [5]. The number of orbitals, R, is called the *rank* of G on Ω. Among the orbitals of a transitive group there is one *diagonal* orbital, $\Delta_1 = \{(i,i) \mid i \in \Omega\}$, which will always be fixed as the first element in the list of orbitals $\Delta_1, \ldots, \Delta_{\mathrm{R}}$. For a transitive action of G there is a natural one-to-one correspondence between the orbitals of G and the orbits of a point stabilizer G_i: $\Delta \longleftrightarrow \Sigma_i = \{j \in \Omega \mid (i,j) \in \Delta\}$. The G_i-orbits are called *suborbits* and their cardinalities are called the *suborbit lengths*.

The invariance condition for a bilinear form A in the Hilbert space $\mathcal{H}_{\mathsf{N}}$ can be written as the system of equations $A = \mathrm{P}(g)\, A \mathrm{P}\left(g^{-1}\right),\ g \in \mathsf{G}$. It is easy to verify that in terms of the entries the equations of this system have the form $(A)_{ij} = (A)_{i^g j^g}$. Thus, the matrices $\mathcal{A}_1, \ldots, \mathcal{A}_{\mathrm{R}}$, where $\mathcal{A}_r$ is the characteristic function of the orbital Δ_r on the set $\Omega \times \Omega$, form a *basis* of the *centralizer ring* of the representation P. The *multiplication table* for this basis has the form $\mathcal{A}_p \mathcal{A}_q = \sum_{r=1}^{\mathrm{R}} C_{pq}^r \mathcal{A}_r$, where C_{pq}^r are non-negative integers. The commutativity of the centralizer ring indicates that the representation P is *multiplicity-free*.

3. Algorithm and its implementation. Let T be a transformation (we can assume that T is unitary) that splits the permutation representation P into M irreducible components:

$$T^{-1}\mathrm{P}(g)\, T = 1 \oplus \mathsf{U}_{d_2}(g) \oplus \cdots \oplus \mathsf{U}_{d_m}(g) \oplus \cdots \oplus \mathsf{U}_{d_M}(g)\,,$$

where U_{d_m} is a d_m-dimensional irreducible subrepresentation, $\oplus$ denotes the direct sum of matrices, i.e., $A \oplus B = \mathrm{diag}(A, B)$.

The matrix $\mathbb{1}_{\mathsf{N}}$ is the *standard inner product* in any orthonormal basis. In the splitting basis we have the following decomposition of the standard inner product

$$\mathbb{1}_{\mathsf{N}} = \mathbb{1}_{d_1=1} \oplus \cdots \oplus \mathbb{1}_{d_m} \oplus \cdots \oplus \mathbb{1}_{d_M}\,.$$

The *inverse image* of this decomposition in the original permutation basis is

$$\mathbb{1}_{\mathsf{N}} = \mathcal{B}_1 + \cdots + \mathcal{B}_m + \cdots + \mathcal{B}_M\,,$$

where $\mathcal{B}_m$ is defined by

$$T^{-1}\mathcal{B}_m T = \mathbb{0}_{1+d_2+\cdots+d_{m-1}} \oplus \mathbb{1}_{d_m} \oplus \mathbb{0}_{d_{m+1}+\cdots+d_M}\,.$$

The main idea of the algorithm is based on the fact that $\mathcal{B}_m$'s form a complete set of *orthogonal projectors*, i.e., they are *idempotent*, $\mathcal{B}_m^2 = \mathcal{B}_m$, and mutually *orthogonal*, $\mathcal{B}_m \mathcal{B}_{m'} = \mathbb{0}_{\mathsf{N}}$ if $m \neq m'$. We see that all $\mathcal{B}_m$'s can be obtained as solutions of the *idempotency equation* $X^2 - X = \mathbb{0}_{\mathsf{N}}$ for the generic invariant form $X = x_1\mathcal{A}_1 + \cdots + x_{\mathrm{R}}\mathcal{A}_{\mathrm{R}}$. This is a system of quadratic polynomial equations in the indeterminates $x_1, x_2, \ldots, x_{\mathrm{R}}$. The polynomial system can be computed by using the multiplication table. Let us write the projector in the basis of invariant forms: $\mathcal{B}_m = b_{m,1}\mathcal{A}_1 + b_{m,2}\mathcal{A}_2 + \cdots + b_{m,\mathrm{R}}\mathcal{A}_{\mathrm{R}}$. It is easy to show that $b_{m,1} = d_m/\mathsf{N}$. Thus, any solution of the idempotency system has the form $\left[x_1^* = d/\mathsf{N}, x_2^*, \ldots, x_{\mathrm{R}}^*\right]$, where $d \in [1..\mathsf{N}-1]$ is either an irreducible dimension or a sum of such dimensions.

The core part of the algorithm is constructed as follows.

We set initially $E(x_1, x_2, \ldots, x_{\mathrm{R}}) \leftarrow \left\{X^2 - X = \mathbb{0}_{\mathsf{N}}\right\}$.

Then we perform a loop on dimensions that starts with $d = 1$ and ends when the sum of irreducible dimensions becomes equal to N.

For the current d we solve the system of equations $E(d/\mathsf{N}, x_2, \ldots, x_{\mathrm{R}})$. All solutions belong to abelian extensions of $\mathbb{Q}$, so their getting is always algorithmically realizable.

If the system is incompatible, then go to the next d.

If $E(d/\mathsf{N}, x_2, \ldots, x_{\mathrm{R}})$ describes a zero-dimensional ideal, then we have k (including the case $k = 1$) different d-dimensional irreducible subrepresentations.

If the polynomial ideal has dimension $h > 0$, then we encounter an irreducible component with a multiplicity k, where $\left\lfloor k^2/2 \right\rfloor = h$. In this case we select, by a somewhat arbitrary procedure, k convenient mutually orthogonal representatives in the family of equivalent subrepresentations.

In any case, if at the moment we have a solution $\mathcal{B}_m$, we append $\mathcal{B}_m$ to the list of irreducible projectors, and exclude from the further consideration the corresponding invariant subspace by adding the linear *orthogonality condition* $\mathcal{B}_m X = \mathbb{0}_{\mathsf{N}}$ to the polynomial system:

$$E(x_1, x_2, \ldots, x_{\mathrm{R}}) \leftarrow E(x_1, x_2, \ldots, x_{\mathrm{R}}) \cup \{\mathcal{B}_m X = \mathbb{0}_{\mathsf{N}}\}.$$

After processing all $\mathcal{B}_m$'s of dimension d, go to the next d.

The complete algorithm is implemented by two procedures:

1. The procedure `PreparePolynomialData` is a program written in **C**. The input data for this program is a set of permutations of Ω that generates the group G. The program computes the basis of the centralizer ring and its multiplication table, constructs the idempotency and orthogonality polynomials, and generates the code of the procedure `SplitRepresentation` that processes the polynomial data. The implementation is able to cope with dimensions (dimension$= |\Omega|$) up to several hundred thousand on a PC within a reasonable time.
2. The procedure `SplitRepresentation` implements the above described loop on dimensions that splits the representation of the group into irreducible components. It is generated by the **C** program `PreparePolynomialData`. Currently, the code is generated in the **Maple** language, and the polynomial equations are processed by the **Maple** implementation of the Gröbner bases algorithms.

Comparison with the **Magma** implementation of the *MeatAxe*.

The **Magma** database contains a 3906-dimensional representation of the exceptional group of Lie type $G_2(5)$. This representation (over the field $\mathrm{GF}(2)$) is used in [4] as an illustration of the capabilities of the *MeatAxe*.

The application of our algorithm to this problem — the calculation showed that the splitting field in this case is $\mathbb{Q}$ — produces the following data.

Rank: 4. Suborbit lengths: $1, 30, 750, 3125$.

$$\underline{\mathbf{3906}} \cong \mathbf{1} \oplus \mathbf{930} \oplus \mathbf{1085} \oplus \mathbf{1890}$$

$$\mathcal{B}_{\mathbf{1}} = \frac{1}{3906}\sum_{k=1}^{4}\mathcal{A}_k$$

$$\mathcal{B}_{\mathbf{930}} = \frac{5}{21}\left(\mathcal{A}_1 + \frac{3}{10}\mathcal{A}_2 + \frac{1}{50}\mathcal{A}_3 - \frac{1}{125}\mathcal{A}_4\right)$$

$$\mathcal{B}_{\mathbf{1085}} = \frac{5}{18}\left(\mathcal{A}_1 - \frac{1}{5}\mathcal{A}_2 + \frac{1}{25}\mathcal{A}_3 - \frac{1}{125}\mathcal{A}_4\right)$$

$$\mathcal{B}_{\mathbf{1890}} = \frac{15}{31}\left(\mathcal{A}_1 - \frac{1}{30}\mathcal{A}_2 - \frac{1}{30}\mathcal{A}_3 + \frac{1}{125}\mathcal{A}_4\right)$$

Time **C**: 1.14 sec. Time **Maple**: 0.8 sec.

The **Magma** fails to split the 3906-dimensional representation over the field $\mathbb{Q}$, but we can model to some extent the case of characteristic zero, using a field of characteristic not dividing $|G_2(5)|$. The smallest such field is $\mathrm{GF}(11)$.

Below is the session of the corresponding **Magma** computation on a computer with two Intel Xeon E5410 2.33GHz CPUs (time is given in seconds).

```
> load "g25";
Loading "/opt/magma.21-1/libs/pergps/g25"
The Lie group G( 2, 5 ) represented as a permutation
group of degree 3906.
Order: 5 859 000 000 = 2^6 * 3^3 * 5^6 * 7 * 31.
Group: G
> time Constituents(PermutationModule(G,GF(11)));
[
    GModule of dimension 1 over GF(11),
    GModule of dimension 930 over GF(11),
    GModule of dimension 1085 over GF(11),
    GModule of dimension 1890 over GF(11)
]
Time: 282.060
```

4. Some decompositions for sporadic simple groups.

Generators of representations are taken from the section “Sporadic groups” of the Atlas [6].

Representations are denoted by their dimensions in bold (possibly with some signs added to distinguish different representations of the same dimension).

Permutation representations are underlined.

Multiple subrepresentations are underbraced in the decompositions.

All timing data were obtained on a PC with 3.30GHz Intel Core i3 2120 CPU.

- 1980-dimensional representation of the Mathieu group cover $6.M_{22}$
  Rank: 17. Suborbit lengths: $1^6, 14^3, 84^3, 336^5$.

$$\underline{\mathbf{1980}} \cong \mathbf{1} \oplus \mathbf{21}_\alpha \oplus \mathbf{21}_\beta \oplus \overline{\mathbf{21}_\beta} \oplus \mathbf{55} \oplus \mathbf{99}_\alpha \oplus \mathbf{99}_\beta \oplus \overline{\mathbf{99}_\beta} \oplus \mathbf{105}_+ \oplus \overline{\mathbf{105}_+} \oplus \mathbf{105}_- \oplus \overline{\mathbf{105}_-} \oplus \mathbf{120} \oplus \mathbf{154} \oplus \mathbf{210} \oplus \mathbf{330} \oplus \overline{\mathbf{330}}$$

  Time **C**: 2 sec. Time **Maple**: 8 h 41 min 1 sec.
- 29155-dimensional representation of the Held group He
  Rank:12.Suborbit lengths: $1, 90, 120, 384, 960^2, 1440, 2160, 2880^2, 5760, 11520$.

$$\underline{\mathbf{29155}} \cong \mathbf{1} \oplus \mathbf{51} \oplus \overline{\mathbf{51}} \oplus \mathbf{680} \oplus \underbrace{\mathbf{1275} \oplus \mathbf{1275}} \oplus \mathbf{1920} \oplus \mathbf{4352} \oplus \mathbf{7650} \oplus \mathbf{11900}$$

  Time **C**: 5 min 41 sec. Time **Maple**: 15 sec.
- 66825-dimensional representation of the McLaughlin group cover $3.McL$
  Rank: 14. Suborbit lengths: $1^3, 630, 2240^3, 5040^3, 8064^3, 20160$.

$$\underline{\mathbf{66825}} \cong \mathbf{1} \oplus \mathbf{252} \oplus \mathbf{1750} \oplus \mathbf{2772} \oplus \overline{\mathbf{2772}} \oplus \mathbf{5103}_\alpha \oplus \mathbf{5103}_\beta \oplus \overline{\mathbf{5103}_\beta} \oplus \mathbf{5544} \oplus \mathbf{6336} \oplus \overline{\mathbf{6336}} \oplus \mathbf{8064} \oplus \overline{\mathbf{8064}} \oplus \mathbf{9625}$$

  Time **C**: 39 min 36 sec. Time **Maple**: 14 min 11 sec.
- 98280-dimensional representation of the Suzuki group cover $3.Suz$
  Rank: 14. Suborbit lengths: $1^3, 891^3, 2816^3, 5940, 19008, 20736^3$.

$$\underline{\mathbf{98280}} \cong \mathbf{1} \oplus \mathbf{78} \oplus \overline{\mathbf{78}} \oplus \mathbf{143} \oplus \mathbf{364} \oplus \mathbf{1365} \oplus \overline{\mathbf{1365}} \oplus \mathbf{4290} \oplus \overline{\mathbf{4290}} \oplus \mathbf{5940} \oplus \mathbf{12012} \oplus \mathbf{14300} \oplus \mathbf{27027} \oplus \overline{\mathbf{27027}}$$

  Time **C**: 2 h 36 min 29 sec. Time **Maple**: 7 min 41 sec.

References

[1] Holt, D. F., Eick, B., O'Brien, E. A. *Handbook of Computational Group Theory.* Chapman & Hall/CRC, 2005.

[2] Kornyak V. V. Quantum models based on finite groups. *J. Phys.: Conf. Ser.* **965** 012023, 2018. http://stacks.iop.org/1742-6596/965/i=1/a=012023

[3] Kornyak V. V. Modeling Quantum Behavior in the Framework of Permutation Groups. *EPJ Web of Conferences* **173** 01007, 2018. https://doi.org/10.1051/epjconf/201817301007

[4] Bosma, W., Cannon, J., Playoust, C., Steel, A. *Solving Problems with Magma.* University of Sydney. http://magma.maths.usyd.edu.au/magma/pdf/examples.pdf

[5] Cameron P. J. *Permutation Groups.* Cambridge University Press, 1999.

[6] Wilson, R. A., et al., Atlas *of finite group representations.* http://brauer.maths.qmul.ac.uk/Atlas/v3.

Vladimir V. Kornyak
Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
e-mail: `vkornyak@gmail.com`