Simultaneous Block Diagonalization of Matrices of Finite Order

Ingolf Bischer, a) Christian Döring, b) and Andreas Trautner c)
Max-Planck-Institut für Kernphysik, Saupfercheckweg 1, 69117 Heidelberg, Germany

Abstract. It is well known that a set of non-defect matrices can be simultaneously diagonalized if and only if the matrices commute. In the case of non-commuting matrices, the best that can be achieved is simultaneous block diagonalization. Here we give an efficient algorithm to explicitly compute a transfer matrix which realizes the simultaneous block diagonalization of unitary matrices whose decomposition in irreducible blocks (common invariant subspaces) is known from elsewhere. Our main motivation lies in particle physics, where the resulting transfer matrix must be known explicitly in order to unequivocally determine the action of outer automorphisms such as parity, charge conjugation, or time reversal on the particle spectrum.

I. INTRODUCTION

A standard problem in group theory is the decomposition of matrix representations into their irreducible invariant subspaces (irreps). Given an explicit matrix representation of a group, the well-known character analysis, see e.g. [1] for finite groups, serves to determine the number and minimal size of blocks that can be achieved in a simultaneous block diagonalization of all representation matrices. However, it is in general a very different problem to perform such a simultaneous block diagonalization explicitly. In this note we introduce an algorithm that solves this problem. Given a set of original input matrices in an arbitrary basis, as well as their decomposition into irreducible blocks (i.e. the number and dimension of the blocks), the algorithm gives the transfer (basis-transformation) matrix that rotates all matrices simultaneously to their block diagonal form.

The algorithm presented here applies to any finite set of equal-dimension unitary matrices for which the decomposition into minimal common invariant subspaces is explicitly known. The problem of finding such common invariant subspaces and their explicit representations seems to be generally solved only if the matrices obey a group structure, and it is particularly tractable if the corresponding group is finite. Nonetheless, a method to find the number of $d$-dimensional common invariant subspaces of a finite set of square matrices for arbitrary $d$ was presented in [2]. The existence of a similarity transformation that performs the simultaneous block diagonalization of matrices with blocks of dimension one or two has been addressed in [3] and [4], while here we seek for an explicit derivation of this transformation, also for blocks of arbitrary dimensions. Our algorithm partly benefits from ideas set forth in [5].

Applications of our algorithm and the resulting transfer matrix are manifold. First and foremost, our algorithm can be used to explicitly find a simultaneously block diagonal basis for a finite group. This problem is, for example, commonly encountered in the breaking of continuous groups to their finite subgroups [6–9]. But applications reach far beyond that. For instance, it may occur that there exist matrix operators living in the same space as the group matrices, but which are themselves not part of the group. If the action of the group is diagonalized it is often very important to know how these operators transform, and this requires explicit knowledge of the basis transformation matrix. In the continuous→discrete example above, this would be operators that live in the coset of the continuous group with respect to the finite subgroup. These operators correspond to non-linearly realized symmetries, implying that knowing their action on the physical fields, which can be derived by our algorithm, is instrumental in constructing the low-energy effective field theory [10, 11], see also [12] for a recent example.

Other examples for operators that act on the same space as the group, but which are themselves not part of the group, are representations of outer automorphisms. For instance, knowing the transfer matrix is strictly required in order to compute the action of outer automorphisms on non-product representations such as, for example, the regular representation of a finite group. This will be investigated in more detail by the present authors in a forthcoming publication [13]. This is of particular physical interest, because parity (P), charge conjugation (C), and time reversal (T) transformations are all known to correspond to outer automorphisms [14–16], which is specifically true for finite groups [17]. For these, physically very interesting situations can arise where CP is explicitly violated by the Clebsch-Gordan coefficients of a finite group [18, 19] or CP transformations may be forced to be of order larger than two for specific groups [19] (see also [20] for a brief introduction, and [21] for a specific phenomenological model). While standard bases for such general CP transformations [22] exist, see [23] and also [24, Ch.2, App.C], such bases may typically not be attained while keeping the linear symmetry (block) diagonal. Our algorithm, here can be used to derive the

---

1 While our algorithm does apply to product representations, for them the problem of explicitly decomposing a representation into irreducible blocks is solved, in general, by knowledge of the Clebsch-Gordan coefficients.
action of a general CP transformation on the physical spectrum, which is obtained after diagonalizing the action of the linearly realized symmetry group. Finally, the above examples also appear in combination: Breaking a continuous group to a finite subgroup while tracking the effect of the physical CP transformation on the physical spectrum requires knowledge of the transfer matrix that diagonalizes the action of the linearly realized group [25].

In many of the above examples, the explicit block diagonalization has been done manually which is not a real challenge for a small number of generators or small dimensional representations. However, the problem becomes more complicated and quickly grows out of hand for more complicated situations with larger groups and/or larger representations. The benefit of our algorithm is that it seamlessly extends to such situations.

We will now present the algorithm in form of a proposition and subsequently prove it. In App. A we give an example based on the regular representation of the group $D_8$.

II. SIMULTANEOUS MATRIX TRANSFORMATION

Consider a collection of $N$, $D$-dimensional unitary matrices $G_g \in U(D)$, where $g = 1, \ldots, N$. We assume that there exists a unitary (hence, invertible) $S \in U(D)$ such that

$$S^{-1} G_g S = B_g \quad \forall g \in \{1, \ldots, N\}, \quad (1)$$

where $B_g$ is a collection of unitary block diagonal matrices. Further, we assume that the $B_g$’s here are composed of blocks of minimal size, i.e. $S$ realizes a decomposition of linear transformations $G_g$ into their minimal common invariant subspaces. In this work we give a fast constructive algorithm to explicitly obtain a matrix $S$ satisfying the above requirements.

Let us first establish a standard form of the matrices $B_g$. Each $B_g$ can be written as a direct sum of blocks $B$,

$$B_g = B^l_g \oplus B^2_g \cdots \quad \forall g. \quad (2)$$

In general, it may occur that the $k$-th and $l$-th block in $B_g$ are identical. If such a degeneracy extends over all $g$ (for some fixed indices $k$ and $l$), that is, if

$$B^k_g = B^l_g \quad \forall g, \quad (3)$$

we speak of degenerate blocks. Note that we may use (3) without loss of generality even if the blocks are only identical up to a global (i.e. $g$-independent) similarity transformation, since such a transformation can always be absorbed in $S$. We introduce $b = 1, \ldots, n$ which runs over the blocks, counting degenerate blocks only once, and the numbers $q_b$ and $d_b$ for the multiplicity (i.e. the degeneracy) and dimensionality of a given block $b$, respectively. Hence, by definition

$$\sum_{b=1}^n q_b d_b = D. \quad (4)$$

In our standard form, we order the direct sum (2) such that degenerate blocks appear in direct succession, i.e.

$$B_g = \bigoplus_{b=1}^n \bigoplus_{q=1}^{q_b} B^b_g \equiv \bigoplus_{b=1}^n (B^b_g)^{\oplus q_b} = B^1_g \oplus \cdots \oplus B^1_g \oplus \cdots \oplus B^n_g \oplus \cdots \oplus B^n_g \quad \forall g. \quad (5)$$

We now state the construction of $S$ in the form of a proposition and subsequently prove it.

Proposition 1. Define

$$\mathcal{M}^b_g := \left[ (\mathbb{1}_{d_b} \otimes G_g) - (B^b_g)^T \otimes \mathbb{1}_D \right], \quad (6)$$

and

$$\mathcal{M}^b := \begin{pmatrix} \mathcal{M}^1_g \\ \vdots \\ \mathcal{M}^n_g \end{pmatrix}. \quad (7)$$

The kernel $\ker \mathcal{M}^b$ is $q_b$-dimensional, i.e. it can be spanned by $q_b$ orthogonal $(D \cdot d_b)$-dimensional vectors $\vec{w}_q = (\vec{w}_{q_b})$. A solution to (1) then is given by

$$S = \text{vec}^{-1}_{D^m} \begin{pmatrix} \vec{w}_1 \\ \vdots \\ \vec{w}_{q_1} \\ \vec{w}_2 \\ \vdots \\ \vec{w}_{q_2} \\ \vdots \\ \vec{w}_n \\ \vdots \\ \vec{w}_{q_n} \end{pmatrix}. \quad (8)$$

$S$ is invertible with pairwise orthogonal columns, such that we can always normalize them in order to promote $S$ to a unitary matrix.

To prove our proposition, let us first reformulate Eq. (1). We use the vectorization operation, which transforms an $n \times m$ matrix $A$ into an $nm \times 1$ vector vec$(A)$ by stacking the columns of the matrix $A$ on top of each other. Given two matrices $X \in \mathbb{C}^{a \times b}$ and $Y \in \mathbb{C}^{b \times c}$ the vectorization of the product of the matrices fulfills the identities

$$\text{vec}(XY) = (\mathbb{1}_c \otimes X)\text{vec}(Y) = (Y^T \otimes \mathbb{1}_a)\text{vec}(X). \quad (9)$$

$^2 \text{vec}^{-1}_{D^m}$ converts a $D \cdot k$ dimensional vector into a $D \times k$ matrix by taking the first $D$ components as the first column, the second $D$ components as the second column and so forth.
Using these, we reformulate Eq. (1) as

$$ (\mathbb{1}_D \otimes G_g)\text{vec}(S) = (B^g_T \otimes \mathbb{1}_D)\text{vec}(S) \quad \forall g. \quad (10) $$

Note that Eq. (10) holds even if $S$ is not invertible. The required invertibility of $S$ is kept in mind as additional information. We then use (5) to decompose the matrix on the r.h.s. of Eq. (10) as

$$ [B^g_T \otimes \mathbb{1}_D] = \left[ \bigoplus_{b=1}^n (B^b_g \otimes \mathbb{1}_D)^{\oplus q_b} \right]. \quad (11) $$

With regard to this, it makes sense to also write the matrix on the l.h.s. of Eq. (10) as a direct sum,

$$ (\mathbb{1}_D \otimes G_g) = \left[ \bigoplus_{b=1}^n (\mathcal{M}^b_g)^{\oplus q_b} \right]. \quad (12) $$

In this way, Eq. (10) decomposes into blocks, with the smallest commensurable blocks of both sides being of size $(d_b \cdot D) \times (d_b \cdot D)$, and those blocks appear with a multiplicity $q_b$. Using this decomposition, we can rewrite (10) as

$$ \left[ \bigoplus_{b=1}^n (\mathcal{M}^b_g)^{\oplus q_b} \right] \text{vec}(S) = \vec{0}_{D^2} \quad \forall g, \quad (13) $$

with $\mathcal{M}^b_g$ as defined in (6), and $\vec{0}_{D^2}$ being the $D^2$-dimensional null vector. Due to the $q_b$ fold degeneracy in (13) one actually just has to solve the equations

$$ \mathcal{M}^b_g \vec{w}^b = \vec{0}_{(D \cdot d_b)} \quad \forall g, \quad (no \; sum) \quad (14) $$

for a $(D \cdot d_b)$-dimensional vector $\vec{w}^b$. That is, for each block $b$ one has to find the intersection of the kernels of $\mathcal{M}^b_g = 1, \ldots, N$, i.e. the kernel of $\mathcal{M}^b$ as defined in (7). This kernel is $q_b$-dimensional, because it is in a one-to-one correspondence with the according invariant subspaces of $G_1, \ldots, N$, of which we have assumed there exist $q_b$ copies. A more detailed proof of $\dim \ker \mathcal{M}^b = q_b$ is given in App. B. Therefore, for each block $b$ there are exactly $q_b$ non-trivial linearly independent solutions to (14). We choose a basis for these solutions, spanned by $q_b$ orthogonal vectors $\vec{w}^b_{q,1} = \ldots = q_b$. Put together as in (8), these form a non-trivial solution of (10) and, for invertible $S$, also a solution of (1). We now discuss the conditions that $S$ obtained by our construction is invertible, which turns out to be always the case given our assumptions. The requirement that $S$ is invertible puts a stronger condition on the solution of (14) than just the existence of $q_b$ linearly independent solutions. In order to formulate this, let us partition each $(D \cdot d_b)$-dimensional vector $\vec{w}^b_q$ into $d_b \cdot D$-dimensional vectors as

$$ \vec{w}^b_q = \left( \begin{array}{c} \vec{v}^b_{q,1} \\ \vdots \\ \vec{v}^b_{q,d_b} \end{array} \right). \quad (15) $$

Invertibility of $S$ now requires not only the $\vec{w}^b_q$’s to be linearly independent, but in fact, it requires that all of the $\vec{v}^b_{q,\beta}$’s in $\mathbb{C}^D$ ($b = 1, \ldots, n$, $q = 1, \ldots, q_b$, $\beta = 1, \ldots, d_b$) must be linearly independent, and, in particular, none of them can be zero. Clearly, if an invertible $S$ exists, we must be able to find such a solution.

First, note that all non-trivial solutions to (14) have the feature that the according $\vec{v}^b_{q,\beta}$ are orthogonal. To see this, define a $(D \times d_b)$-dimensional matrix $W := \text{vec}_D^{-1}(\vec{w}^b_q)$ and rewrite (14), using (9) in reverse, as

$$ G_g W = W B^b_g \quad \forall g. \quad (16) $$

From invertibility of $G_g$ and $B^b_g$, and irreducibility of $B^b_g$, we find that $\ker W = 0$ (another solution would be $W$ being the zero matrix, which is excluded by our desire to discuss a non-trivial solution of (14)). Consequently, $W$ is left-invertible, implying that the $d_b \cdot D$ dimensional vectors within $W$ are linearly independent. This is analogous to the representation theoretic proof of Schur’s lemma. Furthermore, using the unitarity of $G_g$ and $B^b_g$ we derive from (16) by multiplying each side of the equation with its conjugate transpose that

$$ B^b_g (W^\dagger W) = (W^\dagger W) B^b_g \quad \forall g. \quad (17) $$

By Schur’s lemma this implies $W^\dagger W \propto \mathbb{1}_{d_b}$ (since $\text{rank}(W^\dagger W) = \text{rank}(W) = d_b = 0$), confirming that indeed all vectors $v^b_{q,\beta}$ are pairwise orthogonal. This also shows that $\vec{w}^b_q \neq \vec{0}$ for all non-trivial solutions to (14).

Finally, we show that all $v^b_{q,\beta}$’s from within one solution $w^b_q$ are orthogonal to all $v^p_{\beta',d_b}$’s from within a distinct solution $w^p_q$ for any $\beta_1, \beta_2$. Defining the according matrices $W_g := \text{vec}_D^{-1}(\vec{w}^b_q)$ and $W_p := \text{vec}_D^{-1}(\vec{w}^p_q)$ and following the same steps that led to Eq. (17) one can show that

$$ B^b_g (W^\dagger_p W_g) = (W^\dagger_p W_g) B^b_g \quad \forall g. \quad (18) $$

For non-identical solutions $w^b_q \neq w^p_q$ the only possible solution to this is (again by Schur’s lemma) $W_g^\dagger W_g = 0_{d_b \times d_b}$. Altogether this shows the orthogonality of all the $v^b_{q,\beta}$’s, and thereby the invertibility (and, after appropriate normalization, the unitarity) of $S$.

### III. FINAL REMARKS

We have implemented the presented algorithm in a short MATHEMATICA package for convenience. The package provides the function SED that finds a unitary solution for $S$ (provided that it exists) given as input two ordered sets of matrices, $\{G_1, \ldots, G_N\} \cup \{B_1, \ldots, B_N\}$, where the $B^b_g$’s are assumed to be block diagonal with irreducible blocks.
Appendix A: Example $D_8$

As an example we discuss the regular representation of the Dihedral group $D_8$. This finite group has eight elements and is generated by two elements $a$ and $b$ that fulfill the relations

$$ a^4 = e, \quad b^2 = e, \quad abab = e. \quad (A1) $$

The character table is shown in Tab. 1. Generators for the irreducible two-dimensional (2D) representation can be chosen as

$$ \rho_2(a) = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \quad \text{and} \quad \rho_2(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (A2) $$

The (left-)regular representation acts as

$$ \text{reg}_a : g \mapsto ag \quad \forall g \in D_8, \quad (A3) $$

$$ \text{reg}_b : g \mapsto bg \quad \forall g \in D_8. \quad (A4) $$

These act as permutations on the group elements. In a basis $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ those are represented by

$$ G_a = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (A5) $$

$$ G_b = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (A6) $$

The regular representation decomposes into irreducible representations as

$$ \text{reg} = \mathbf{1}_0 \oplus \mathbf{1}_1 \oplus \mathbf{1}_2 \oplus \mathbf{1}_3 \oplus \mathbf{2} \oplus \mathbf{2}. \quad (A7) $$

Hence, there must be a basis in which $G_a$ and $G_b$ are block diagonal and given by

$$ B_a = \rho_{1_0}(a) \oplus \rho_{1_1}(a) \oplus \rho_{1_2}(a) \oplus \rho_{1_3}(a) \oplus \rho_{2}(a), $$

$$ B_b = \rho_{1_0}(b) \oplus \rho_{1_1}(b) \oplus \rho_{1_2}(b) \oplus \rho_{1_3}(b) \oplus \rho_{2}(b), $$

with 2D representation matrices given in (A2) and 1D representations that can be read off from Tab. 1.

Our algorithm finds a transformation matrix $S$ which simultaneously transforms $G_a$ to $B_a$, and $G_b$ to $B_b$. Of course, this is not a real challenge here as for a small number of generators and small dimensional representations this problem could straightforwardly be solved by a manual computation. However, our algorithm seamlessly extends to much more complicated situations.

The number of generators is $N = 2$ and the number of non-identical blocks is $n = 5$ with degeneracies $q_{b=1,\ldots,5} = \{1, 1, 1, 1, 2\}$. For the 1D blocks (commutative part), this reduces to the usual problem of finding common eigenvectors, which is simple to solve see e.g. [5]. In our approach this part of $S$ is determined by finding

$$ \ker(M^b) = \ker \left( G_a - \rho_{1_b}(a) \cdot \mathbb{I}_8 \right), \quad (A8) $$

for $b = 1, \ldots, 4$. These kernels are one-dimensional (as warranted by $q_{b=1,2,3,4} = 1$) and spanned by the orthogonal vectors

$$ w^1 = (1, 1, 1, 1, 1, 1, 1, 1)^T, \quad (A9) $$

$$ w^2 = (1, 1, 1, -1, -1, -1, -1, -1)^T, \quad (A10) $$

$$ w^3 = (-1, 1, -1, 1, -1, 1, -1, -1)^T, \quad (A11) $$

$$ w^4 = (1, -1, -1, 1, 1, -1, 1, -1)^T. \quad (A12) $$

For the twofold degenerate 2D blocks ($b = 5, q_5 = 2$) one has to find

$$ \ker(M^b) = \ker \left( \mathbb{I}_2 \otimes G_a - \rho_{2}(a) \cdot \mathbb{I}_8 \right), \quad (A13) $$

In agreement with $q_5 = 2$, this kernel is two-dimensional and can be spanned by the two $(D \cdot d_5 = 8 \cdot 2)$-dimensional orthogonal vectors

$$ w^5_1 = (-i, 1, i, -1, 0, 0, 0, 0, 0, i, -1, -i, i, i, i, -1, -i, 1, -i, 1, 0, 0, 0)^T, $$

$$ w^5_2 = (0, 0, 0, 0, -i, i, -1, -1, -i, -1, i, 0, 0, 0, 0)^T. $$

According to Proposition 1, we then find the unitary matrix $S$ by joining the vectors $w^b$, applying the inverse vectorization to them, and normalizing each column of the

| $D_8$ | $\{e\}$ | $\{a^2\}$ | $\{a, a^3\}$ | $\{b, a^2b\}$ | $\{ab, a^3b\}$ |
|-------|--------|----------|-------------|-------------|-------------|
| $\mathbf{1}_0$ | 1 | 1 | 1 | 1 | 1 |
| $\mathbf{1}_1$ | 1 | 1 | 1 | -1 | -1 |
| $\mathbf{1}_2$ | 1 | 1 | -1 | 1 | -1 |
| $\mathbf{1}_3$ | 1 | 1 | -1 | -1 | 1 |
| $\mathbf{2}$ | 2 | -2 | 0 | 0 | 0 |
resulting matrix. The result is given by

$$
S = \frac{1}{\sqrt{8}} \begin{pmatrix}
1 & 1 & -1 & 1 & -i\sqrt{2} & 0 & 0 & -i\sqrt{2} \\
1 & 1 & 1 & -1 & \sqrt{2} & 0 & 0 & -\sqrt{2} \\
1 & 1 & -1 & 1 & i\sqrt{2} & 0 & 0 & i\sqrt{2} \\
1 & 1 & 1 & -1 & -\sqrt{2} & 0 & 0 & i\sqrt{2} \\
1 & -1 & -1 & -1 & 0 & -i\sqrt{2} & -i\sqrt{2} & 0 \\
1 & 1 & 1 & 1 & 0 & -\sqrt{2} & i\sqrt{2} & 0 \\
1 & -1 & -1 & -1 & 0 & i\sqrt{2} & i\sqrt{2} & 0 \\
1 & 1 & 1 & 1 & 0 & \sqrt{2} & -\sqrt{2} & 0
\end{pmatrix}
$$

(A14)

It is straightforward to check that this matrix is unitary and satisfies (1) for \(G_{a,b}\) and \(B_{a,b}\).

**Appendix B: Details on \(\text{dim ker} \ M^b = q_b\)**

Here we demonstrate that \(\text{dim ker} \ M^b = q_b\). We first show \(\text{dim ker} \ M^b \geq q_b\), and then \(\text{dim ker} \ M^b \leq q_b\).

Part 1: \(\text{dim ker} \ M^b \geq q_b\). Let \(V\) denote the space on which the matrices \(G_b\) act. By assumption, there are \(q_b\) copies of the common invariant subspace \(V^b\), associated with the blocks \(B^b\), within \(V\). That is

\[
V \supset V^b \oplus \cdots \oplus V^q_b .
\]  

(B1)

We now establish that each of these \(q_b\) invariant subspaces defines a non-trivial vector in \(\text{ker} \ M^b\), and that those \(q_b\) vectors are pair-wise orthogonal.

Each invariant subspace is spanned by a set of basis vectors \(\{v^b_{q,\beta=1,\ldots,d_b}\}\). Then, per definition of an invariant subspace,

\[
G^b v^b_{q,1} = \left[\tilde{B}^b\right]_{11} v^b_{q,1} + \cdots + \left[\tilde{B}^b\right]_{d_b} v^b_{q,d_b} ,
\]

\[
G^b v^b_{q,d_b} = \left[\tilde{B}^b\right]_{d_b} v^b_{q,1} + \cdots + \left[\tilde{B}^b\right]_{d_b} v^b_{q,d_b} ,
\]  

(B2)

where the \(\left[\tilde{B}^b\right]_{\alpha,\beta}\) are arbitrary expansion coefficients. Clearly, we can always choose a basis for \(V^b\) in which \(\tilde{B}^b = B^b\) of Eq. (2). Working in such a basis and arranging \(\{v^b_{q,\beta=1,\ldots,d_b}\}\) into a \(w^b_q\) according to Eq. (15), one finds that Eq. (B2) is nothing but the spelled-out version of Eq. (14). Thus, \(w^b_q \in \text{ker} \ M^b\) by construction. Furthermore, \(w^b_{q,1} \perp w^b_{q,2}\) for \(q_1 \neq q_2\), since

\[
\langle w^b_{q,1}, w^b_{q,2} \rangle = \sum_{\alpha=1}^{d_b} \langle v^b_{q,1,\alpha}, v^b_{q,2,\alpha} \rangle = \sum_{\alpha=1}^{d_b} 0 = 0 ,
\]

(B3)

where we have used that \(V^b_{q_1} \perp V^b_{q_2}, q_1 \neq q_2\), by assumption. Hence, each copy of the invariant subspace provides an independent solution to (14), implying that there are at least \(q_b\) orthogonal vectors in \(\text{ker} \ M^b\).

Part 2: \(\text{dim ker} \ M^b \leq q_b\). Assume \(\text{dim ker} \ M^b = Q\). Then we can find \(Q\) linearly independent solutions to (14). Each of those can be transformed to a \((D \times d_b)\)-dimensional left-invertible matrix \(W^b_Q := \text{vec}_B(v^b_Q)\) (see the discussion around Eq. (16)). Furthermore, since all columns of all \(W^b_{Q=1,\ldots,Q}\) are pair-wise orthogonal these matrices can straightforwardly be combined to a \((D \times d_b, Q)\)-dimensional left-invertible matrix \(W^b_Q\) that fulfills the equation

\[
(W^b_Q)^{-1} G^b W^b_Q = (B^b)^{\perp Q} \forall g .
\]

Hence, \(Q \leq q_b\), as there are, by assumption, exactly \(q_b\) copies of \(B^b\) in \(G^b\).
19 M.-C. Chen, M. Fallbacher, K. Mahanthappa, M. Ratz, and A. Trautner, “CP Violation from Finite Groups,” Nucl. Phys. B 883, 267–305 (2014), arXiv:1402.0507 [hep-ph].

20 M.-C. Chen and M. Ratz, “Group-theoretical origin of CP violation,” (2019), 10.31526/lhep.1.2019.125, arXiv:1903.00792 [hep-ph].

21 I. P. Ivanov and J. P. Silva, “CP-conserving multi-Higgs model with irremovable complex coefficients,” Phys. Rev. D93, 095014 (2016), arXiv:1512.09276 [hep-ph].

22 T. D. Lee and G. C. Wick, “Space Inversion, Time Reversal, and Other Discrete Symmetries in Local Field Theories,” Phys. Rev. 148, 1385–1404 (1966).

23 G. Ecker, W. Grimus, and H. Neufeld, “A Standard Form for Generalized CP Transformations,” J.Phys. A20, L807 (1987).

24 S. Weinberg, “The quantum theory of fields. vol. 1: Foundations,” Cambridge, UK: Univ. Pr. (1995) 609 p.

25 M. Ratz and A. Trautner, “CP violation with an unbroken CP transformation,” JHEP 02, 103 (2017), arXiv:1612.08984 [hep-ph].