Lie theory of finite simple groups and the Roth property

By J LÓPEZ PEÑA†

University College London,
Department of Mathematics, Gower Street, London WC1E 6BT

S MAJID‡

Queen Mary University of London,
School of Mathematical Sciences, Mile End Rd, London E1 4NS

K RIETSCH§

Kings College London,
Department of Mathematics, The Strand, London

(*Received* * *** ***)

Abstract

In noncommutative geometry a 'Lie algebra' or bidirectional bicovariant differential calculus on a finite group is provided by a choice of an ad-stable generating subset $\mathcal{C}$ stable under inversion. We study the associated Killing form K. For the universal calculus associated to $\mathcal{C} = G\setminus\{e\}$ we show that the magnitude $\mu = \sum_{a,b\in\mathcal{C}}(K^{-1})_{a,b}$ of the Killing form is defined for all finite groups (even when K is not invertible) and that a finite group is Roth, meaning its conjugation representation contains every irreducible, *iff* $\mu \neq \frac{1}{N-1}$ where N is the number of conjugacy classes. We show further that the Killing form is invertible in the Roth case, and that the Killing form restricted to the $(N-1)$-dimensional subspace of invariant vectors is invertible *iff* the finite group is an almost-Roth group (meaning its conjugation representation has at most one missing irreducible). It is known [**9**, **10**] that most nonabelian finite simple groups are Roth and that all are almost Roth. At the other extreme from the universal calculus we prove that the 2-cycles conjugacy class in any S_n has invertible Killing form, and the same for the generating conjugacy classes in the case of the dihedral groups D_{2n} with n odd. We verify invertibility of the Killing forms of all real conjugacy classes in all nonabelian finite simple groups to order $75,000$, by computer, and we conjecture this to extend to all nonabelian finite simple groups.

1. *Introduction*

In this paper we demonstrate the existence of a useful 'Lie theory' of finite groups with a detailed study of the Killing form. We recall that historically the theory of Hopf algebras has unified enveloping algebras of Lie algebras with group algebras. In the same

† EU Marie-Curie fellow PIEF-GA-2008-221519 and MCIM grant MTM2010-20940-C02-01
‡ Senior Leverhulme research fellow
§ EPSRC research fellow EP/D071305/1

way there seems to be a reasonable generalisation of Lie algebras themselves, which comes out of quantum groups and their noncommutative differential geometry and which can nevertheless be specialised to finite groups. Here the 'Lie problem' of finding a finite-dimensional Lie algebra-type object associated to the Drinfeld-Jimbo quantum groups $U_q(\mathfrak{g})$ was solved in [**13**] in the form of a 'braided-Lie algebra', consisting of a coalgebra $\mathcal{L}$ in a braided category and a bracket operation $[\ ,\ ]:\mathcal{L}\otimes\mathcal{L}\to\mathcal{L}$ subject to certain axioms. This will be recalled in the preliminary Section 2 where we will cover the reduction to the finite group case. For a braided Lie algebra there is also a notion of braided Killing form $K:\mathcal{L}\otimes\mathcal{L}\to\underline{1}$ defined as a braided-trace of $[\ ,\ ](\mathrm{id}\otimes[\ ,\ ])$. When the category in which $\mathcal{L}$ lies is Abelian, one has a quadratic braided enveloping algebra $U(\mathcal{L})$ which forms a bialgebra and which in some cases can quotient to a Hopf algebra in the category. Within this framework, for $U_q(\mathfrak{g})$ and at least for generic q we have a certain $\mathcal{L}\subset U_q(\mathfrak{g})$ and $U(\mathcal{L})\twoheadrightarrow B_q(G)$, where the latter is a braided version of a quantum group of which $U_q(\mathfrak{g})$ is a localisation (alternatively one can work over formal power-series). In this context, where $\mathfrak{g}$ is semisimple, the braided-Killing form is nondegenerate as an expression of the factorisability of the quantum group cf. [**13**, **16**]. Just as in Lie theory, the braided-Lie algebras here arise [**8**] from bicovariant differential structures on quantum groups [**26**] but the usual theorem that a topological group has at most one differentiable structure making it a Lie group does not apply and rather there is a known classification theory for the differential structures and hence of braided-Lie algebras, for each $U_q(\mathfrak{g})$. Also the usual theorem that a discrete topology admits only the 0–dimensional differential structure does not apply and this means that we can specialise to finite groups. Many differential constructions still work and in particular one has a notion of noncommutative de Rham cohomology for each choice of calculus.

We will not need the full extent of this theory, being interested in the case where the category is that of vector spaces over a field k with the trivial 'flip' braiding and trivial associator. The general framework, however, provides a bridge

$$\begin{array}{ccc} & \text{Quantum Groups} & \\ \swarrow & & \searrow \\ \text{Lie Algebras} & & \text{Finite Groups} \end{array} \qquad (1{\cdot}1)$$

for the transfer of ideas from Lie theory to finite groups (taking ideas backwards up the left arrow is a loosely defined process of 'quantisation' and we then specialise down by the right arrow).

For the specialisation of structure represented by the first arrow one can look at braided Lie algebras of the form $\mathcal{L}=k\oplus\mathfrak{g}$, a linear map $[\ ,\ ]:\mathfrak{g}\otimes\mathfrak{g}\to\mathfrak{g}$ and a specific form for the remaining structure (see Section 2). The axioms of a braided-Lie algebra then reduce to those of a Leibniz algebra on $\mathfrak{g}$, which includes the case of an ordinary Lie algebra. In the Lie case we obtain $U(\mathcal{L})\twoheadrightarrow U(\mathfrak{g})$ as a quadratic bialgebra extension of the usual enveloping algebra. The braided-Killing form extends the usual Killing form, and is nondegenerate if and only if the usual Killing form is. Other choices of $\mathcal{L}$ can be found from the degree filtration of $U(\mathfrak{g})$.

On the right hand side we can consider braided-Lie algebras of the form $\mathcal{L}=k\mathcal{C}$ where $\mathcal{C}$ is a set and we take the diagonal coalgebra structure. Then the axioms of a regular braided-Lie algebra reduce to a set map $[\ ,\ ]:\mathcal{C}\times\mathcal{C}\to\mathcal{C}$ obeying the axioms of a left-handed rack. A quandle is a rack with a further restriction (see Section 2.1) and arises naturally when $\mathcal{C}$ is an ad-stable generating subset $\mathcal{C}\subseteq G\setminus\{e\}$ in a finite group G. Here

e is the group identity. We consider such a quandle $\mathcal{C}$ as playing the role of a 'Lie algebra' for G. In this setting we also have a quadratic bialgebra $U(\mathcal{L}) \twoheadrightarrow kG$ and a Killing form which looks like

$$K(a,b) = |Z(ab) \cap \mathcal{C}|, \quad \forall a, b \in \mathcal{C}, \tag{1·2}$$

where $Z(g)$ is the centraliser of $g \in G$. Note that $K(a,b)$ is the trace of ab in the conjugation representation of G on $\mathcal{L} = k\mathcal{C}$. We can consider these values as the entries $K_{a,b}$ of a matrix and associate some constants to this Killing form matrix when it is sufficiently invertible, the most important of which is

$$\mu = \sum_{a,b \in \mathcal{C}} K^{-1}_{a,b}$$

the sum of all matrix entries of K^{-1} in our basis $\mathcal{C}$. This is the magnitude of the matrix K in the sense of [**11**] and can be defined even when K is not invertible as long as the vector with all entries 1 is in the image.

In this paper we work over $\mathbb{C}$ and study the Killing form (1·2), particularly the following question motivated by the above transfer of ideas from Lie theory: just as a Lie algebra over $\mathbb{C}$ is semisimple if and only if the Killing form is nondegenerate, *is the Killing form for an ad-stable inversion-stable generating subset $\mathcal{C}$ (as 'Lie algebra') nondegenerate when the group is simple or a product of simple groups?* This is a bit too much to ask in general, as we will see, so we make the following definition.

DEFINITION 1·1. *Let G be a finite group. If the Killing form is nondegenerate*

(1) *for every ad-stable inversion-stable generating subset $\mathcal{C} \subseteq G \setminus \{e\}$, we say that G is* strongly nondegenerate
(2) *for the universal calculus $\mathcal{C} = G \setminus \{e\}$, we say that G is* nondegenerate
(3) *for every nontrivial real generating conjguacy class, we say that G is* class-nondegenerate

Clearly (1) is the most desirable in the absence of a particular choice of $\mathcal{C}$ as 'Lie algebra'. (2) is not very classical (the universal calculus is very far from the classical one on a Lie group, and has the undesirable property of yielding a trivial de Rham cohomology) but is the simplest to look at and we will achieve a more or less complete analysis of this case. (3) is reasonable if we think that a 'Lie algebra' should be in some sense minimal. It is also a proxy for (1) since any $\mathcal{C}$ is a disjoint union of conjugacy classes and one might expect that if (3) holds then (1) will tend to hold as well. Although not part of the classical analogy, we say that a group is *absolutely nondegenerate* if (1) holds for all $\mathcal{C}$ not only generating ones. There is no difference with (1) in the simple case.

Our main results concern G a finite group with what we call the *Roth property* that every irreducible representation is contained in the conjugation representation. We prove (Theorem 4·2) that every Roth property group is nondegenerate. Moreover, we show (Theorem 4·6) that the magnitude μ of the Killing form for the universal calculus is defined for every finite group and completely characterises the Roth property. Namely, we show that a finite group is Roth iff $\mu \neq \frac{1}{N-1}$ where N is the number of conjugacy classes in the group, and in this case we give a formula for μ. The background here is that Roth's conjecture [**21**] in the theory of finite groups asserted that the conjugation representation of the group G on the vector space $\mathbb{C}[G]$ contains every complex irreducible representation of $G/Z(G)$ at least once (where $Z(G)$ is the centre of G). Roth's conjecture turned out to be false in general, but is known to be true for symmetric groups [**4**] and alternating groups [**23**], and, recently, for the sporadic simple groups [**9**] using methods from [**20**]. Indeed, for simple nonabelian groups the exceptions amount to some instances of one classical family of Lie type over finite fields of particular order[**9**] and in these cases the conjugation representation lacks exactly one irreducible representation[**10**]. In this case we do not necessarily have nondegeneracy but a weaker result applies that the Killing form is nondegenerate when restricted to the subspace of invariant vectors (Proposition 4·8). We also show there that if a finite group lacks two or more irreducible representations in its conjugation representation then it is not nondegenerate. Hence if a finite group is nondegenerate and not Roth then it must indeed lack precisely one irreducible representation in its conjugation representation. The non-degeneracy property in our Killing form approach thus provides a new point of view on the Roth property, and may even coincide with it for finite simple groups. The two properties are not equivalent in general however, see below. Meanwhile, the magnitude of the Killing form provides a complete characterisation of whether a finite group is Roth or not.

Let us write $\mathbb{Z}_k$ for the cyclic group $\mathbb{Z}/k\mathbb{Z}$. We first show in Corollary 3·2 that any nondegenerate group of order $|G| > 2$ is centreless while the group $\mathbb{Z}_2$ is exceptional in being nondegenerate and not centreless. Hence we have the following picture

$$\text{Most Nonabelian Simple} \subset \text{Roth property} \subset \text{Nondegenerate} \subset \text{Centreless} \cup \{\mathbb{Z}_2\}$$

where on the left we mean all simple nonabelian groups including sporadics with the possible exceptions identified in [**9**]. All inclusions here are strict. For instance S_n, $n \geq 3$ and D_{2n}, odd $n \geq 3$ are Roth but of course they are not simple. Meanwhile the group

$$(((\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes \mathbb{Z}_4) \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}_2$$

of order 400 (labeled (400, 207) in the Small Groups Library [**1**]) is centreless and nondegenerate but not Roth (indeed we find that it is the smallest such example). The last inclusion is also strict as many centreless groups are not nondegenerate. Of the 680 centreless groups of order $|G| \leq 500$ some 537 are nondegenerate. These results were found using GAP [**7**] and Sage [**24**].

The above results all pertain to the universal calculus and its corresponding class of nondegenerate groups. At the other extreme we have the calculi associated to real, generating conjugacy classes, and the property of class non-degeneracy. All 680 centreless groups of order $|G| \leq 500$ are class-nondegenerate, although this includes 452 of them which do not actually have any real generating conjugacy classes. In this context we make the specific conjecture:

Conjecture 1·2. *All nonabelian finite simple groups are class-nondegenerate.*

This is supported by computer analysis where we have checked this conjecture for all $|G| \leq 75,000$. This was again done using Sage and the methods and tables are collected in the Appendix. Thus

$$\begin{array}{ccccc} \text{Class Nondegenerate} & \supset & \text{Strongly Nondegenerate} & \subset & \text{Nondegenerate} \\ \cup_{\text{conjecture}} & & \cup_{\text{many but not all}} & & \cup_{\text{most but not all}} \\ & & \text{Finite Simple Nonabelian Groups,} & & \end{array}$$

where Conjecture 1·2 is that all finite simple nonabelian groups are included on the left and Theorem 4·2 combined with [**9**] says that most finite simple nonabelian groups are included on the right. Up to order 75,000 the first non-Roth finite simple nonabelian group is $PSU(3,3)$ according to [**10**] and one can check that this is *not* nondegenerate. The only other non-Roth finite simple nonabelian group to this order is $PSU(3,4)$ which at order approximately $62,000$ is well beyond direct verification. With possibly a small number of exceptions it would appear then that most finite simple groups are nondegenerate at the two extremes and indeed that many of them are strongly nondegenerate. Using Sage, we find that of the 15 simple nonabelian groups to order $|G| \leq 8000$ in the tables in the Appendix, the groups A_5, A_6, A_7, $PSL(2,8)$, $PSL(2,13)$, $PSL(2,17)$, $PSL(3,3)$, $PSL(2,16)$, $PSL(2,25)$, and the sporadic Mathieu group M_{11} *are* strongly nondegenerate, whilst $PSL(2,7)$, $PSL(2,11)$, $PSL(2,19)$, $PSU(3,3)$ and $PSL(2,23)$ are not strongly nondegenerate (these are still class-nondegenerate and all but $PSU(3,3)$ are nondegenerate). This explains the above picture and somewhat answers our original question to the extent currently within reach.

We will also prove in Corollary 6·3 that the Killing form for S_n ($n \geq 3$) in the case where $\mathcal{C}$ is taken to be the set of 2-cycles is nondegenerate. This, combined with the Roth property and other data, suggests that S_n for $n \geq 5$ is at least class-nondegenerate. We have verified that in fact it is absolutely non-degenerate up to and including S_8. Likewise, D_{2n} for n odd is nondegenerate, class-nondegenerate (see Proposition 3·3) and is possibly strongly nondegenerate, but is not absolutely nondegenerate. We have checked strong nondegeneracy for odd n dihedral groups D_{2n} up to order 50. Hence there are plenty of groups which are nonsimple but strongly nondegenerate. We also mention S_3, S_4, A_4 as some other examples of groups which are nondegenerate, strongly nondegenerate but not absolutely nondegenerate.

Finally, the product of two Roth groups is clearly Roth, and we see (Proposition 4·5) in our Killing form approach that this characterises Roth groups among all nondegenerate ones. At the other extreme, suppose two groups G_1 and G_2 have 'Lie algebras' with nondegenerate Killing form coming from conjugacy classes $\mathcal{C}_1, \mathcal{C}_2$. Then in Proposition 3·5 we characterize when the direct product $G_2 \times G_2$ has nondegenerate Killing form on its 'Lie algebra' obtained by forming the disjoint union $\mathcal{C}_1 \sqcup \mathcal{C}_2$ in $G_1 \times G_2$.

Among further results we show that when nondegenerate, the matrix K is positive definite precisely when $\mathcal{C}$ consists only of elements of order 2. More generally the index in the sense of positive minus negative eigenvalues is the number of elements of order 2, see Proposition 3·4. By the Feit-Thompson theorem every finite simple group has at least one element of order 2. The corresponding conjugacy class therefore gives us a choice of $\mathcal{C}$ for which the braided-Killing form is positive definite if it is nondegenerate. This is a little reminiscent of usual Lie theory where a complex simple Lie algebra has a compact real form where the Killing form is negative definite.

The Killing form appears to have further properties that are suggested by our data and which deserve further study. The most important such observation is that the Killing form decomposition of $\mathbb{C}\mathcal{C}$ into eigenspaces tends to be a decomposition into irreducibles or conjugate pairs of them. We illustrate this for S_n and the 2-cycles class in Section 6. Another observation is that for simple groups the Killing form appears to be irreducible for all conjugacy classes exactly when the group does not have a strongly embedded subgroup in the sense of Bender (we thank the referee for this observation).

Although the general picture makes sense over any field, all sections after Section 2 will be over $\mathbb{C}$ (or a suitable splitting field for the relevant groups).

2. *From braided-Lie algebras to 'Lie algebras' on finite groups*

In this section we make precise (1·1) and thereby provide the context of braided-Lie algebras which underpins the point of view in the rest of the paper. We derive our point of view of an ad-stable generating subset $\mathcal{C}\subseteq G\setminus\{e\}$ as a 'Lie algebra' and the Killing form in Example 2·4 which is then used in the rest of the paper.

We recall that a braided category means a monoidal category $\otimes$ with unit object $\underline{1}$ and natural isomorphisms $\Psi:\otimes\to\otimes^{op}$, $\Phi:\otimes(\ \otimes\ )\to(\ \otimes\ )\otimes$ subject to standard triangle, hexagon and pentagon identities. The associator Φ can be omitted since by Mac Lane's theorem it can be inserted as needed for brackets to make sense, while the braiding Ψ is denoted by a crossing in a diagrammatic notation in which these and other morphisms are read flowing down the page and $\otimes$ is denoted by juxtaposition [**12**]. Algebra in such a category is done as 'flow charts' except that under and over crossings are significant.

A braided-Lie algebra [**13**] is a quadruple $(\mathcal{L},\Delta,\epsilon,[\ ,\ ])$ where $\mathcal{L}$ is an object on a braided category, $\Delta:\mathcal{L}\to\mathcal{L}\otimes\mathcal{L}$ and $\epsilon:\mathcal{L}\to\underline{1}$ makes it a coalgebra (the axioms are those of a unital algebra but with arrows reversed), and $[\ ,\ ]:\mathcal{L}\otimes\mathcal{L}\to\mathcal{L}$ is a braided coalgebra map obeying the axioms

$$[\ ,\ ]([\ .\ ]\otimes[\ ,\ ])(\mathrm{id}\otimes\Psi\otimes\mathrm{id})(\Delta\otimes\mathrm{id}\otimes\mathrm{id})=[\ ,\ ](\mathrm{id}\otimes[\ ,\ ])$$

$$(\mathrm{id}\otimes[\ ,\ ])(\Psi\otimes\mathrm{id})(\mathrm{id}\otimes\Psi^2)(\Delta\otimes\mathrm{id})=(\mathrm{id}\otimes[\ ,\ ])(\Delta\otimes\mathrm{id}).$$

Here a braided coalgebra map means we are considering the braided tensor product coalgebra structure on $\mathcal{L}\otimes\mathcal{L}$. Since we are only interested in tensor products and sums of one object one can also think of a single braided-Lie algebra as a sextuple $(\mathcal{L},\Delta,\epsilon,[\ ,\ ],\Psi,\Phi)$ where $\Psi:\mathcal{L}\otimes\mathcal{L}\to\mathcal{L}\otimes\mathcal{L}$ and $\Phi:\mathcal{L}\otimes(\mathcal{L}\otimes\mathcal{L})\to(\mathcal{L}\otimes\mathcal{L})\otimes\mathcal{L}$ and subject to similar axioms.

Lemma 2·1. [**14**] *For any braided-Lie algebra $\mathcal{L}$ the morphism $\tilde{\Psi}:\mathcal{L}\otimes\mathcal{L}\to\mathcal{L}\otimes\mathcal{L}$ defined by*

$$\tilde{\Psi}=([\ ,\ ]\otimes\mathrm{id})(\mathrm{id}\otimes\Psi)(\Delta\otimes\mathrm{id})$$

obeys the braid relations on $\mathcal{L}^{\otimes 3}$. We call the braided Lie algebra regular *if $\tilde{\Psi}$ is invertible.*

Associated to any braided Lie algebra $\mathcal{L}$ in an abelian braided category there is a quadratic bialgebra $U(\mathcal{L})$ in the braided category. It is defined as the tensor algebra $T\mathcal{L}$ modulo the relations given by coequalizing the multiplication maps μ and $\mu\circ\tilde{\Psi}$, and with coalgebra structure defined by extending that of $\mathcal{L}$.

Associated to any braided-Lie algebra with (say) a left dual in the braided category (a rigid object), there is a notion of 'braided-Killing form' $K:\mathcal{L}\otimes\mathcal{L}\to\underline{1}$ defined as

$$K=\mathrm{ev}\Psi([\ ,\ ]\otimes\mathrm{id})(\mathrm{id}\otimes[\ ,\ ]\otimes\mathrm{id})(\mathrm{id}\otimes\mathrm{id}\otimes\mathrm{coev})$$

where $\mathrm{ev}:\mathcal{L}^*\otimes\mathcal{L}\to\underline{1}$ and $\mathrm{coev}:\underline{1}\to\mathcal{L}\otimes\mathcal{L}^*$ are the evaluation and coevaluation and here $\Psi:\mathcal{L}\otimes\mathcal{L}^*\to\mathcal{L}^*\otimes\mathcal{L}$. This has the form of a braided trace of $[\ ,[\ ,\ ]]$. Key properties including invariance under the action of $[\ ,\ ]$ and braided-symmetry $K=K\tilde{\Psi}$ are shown in [**13**]. The Killing form K is invertible in a standard categorical sense if there is another morphism $K^{-1}:\underline{1}\to\mathcal{L}\otimes\mathcal{L}$ such that

$$(\mathrm{id}\otimes\mathrm{K})(\mathrm{K}^{-1}\otimes\mathrm{id})=\mathrm{id}=(\mathrm{K}\otimes\mathrm{id})(\mathrm{id}\otimes\mathrm{K}^{-1})$$

where these are morphisms $\mathcal{L}\otimes\mathcal{L}\otimes\mathcal{L}\to\mathcal{L}\otimes\mathcal{L}\otimes\mathcal{L}$.

PROPOSITION 2·2. [**13**] *If K is invertible then*

$$[\ ,\ ](\mathrm{id}\otimes\sigma)\Delta=\mathrm{id}$$

where $\sigma:\mathcal{L}\to\mathcal{L}$ *is* $\sigma=(\mathrm{id}\otimes\mathrm{K})(\Psi\otimes\mathrm{id})(\mathrm{id}\otimes\mathrm{K}^{-1})$

EXAMPLE 2·3. *An actual Lie algebra $\mathfrak{g}$ can be seen as a braided-Lie algebra of the form $\mathcal{L}=k\oplus\mathfrak{g}$ in the category* Vec *of vector spaces over k (so with trivial braiding of the underlying category, although a nontrivial $\tilde\Psi$ even in this case, provided that the Lie bracket is nonzero). Here*

$$[c,v]=v,\quad [v,c]=0,\quad [c,c]=c,\quad \Delta v=v\otimes c+c\otimes v,\quad \Delta c=c\otimes c,\quad \forall v\in\mathfrak{g}$$

where c spans the copy of k. The axioms of a braided-Lie algebra then amount to the bracket $[\ ,\ ]:\mathfrak{g}\otimes\mathfrak{g}\to\mathfrak{g}$ obeying

$$[[v,w],z]+[w,[v,z]]=[v,[w,z]],\quad \forall v,w,z\in\mathfrak{g}$$

while regularity is automatic as is the property $[\ ,\ ]\Delta=\mathrm{id}$. We do not require antisymmetry of the bracket which means that a braided-Lie algebra of this form is the same as $\mathfrak{g}$ a Leibniz algebra (this is a slightly more general notion than that of a Lie algebra). Here $U(k\oplus\mathfrak{g})$ is a quadratic bialgebra associated to any Leibniz algebra with relations $xy-yx=c[x,y]$ and c central. In the Lie algebra case there is a bialgebra homomorphism $U(k\oplus\mathfrak{g})\to U(\mathfrak{g})$ sending c to 1. The Killing form restricts to the usual Killing form and in addition

$$K(c,c)=1,\quad K(c,x)=K(x,c)=0.$$

EXAMPLE 2·4. *Similarly, we can consider $\mathcal{L}=k\mathcal{C}$ where $\mathcal{C}$ is a set, and $\Delta a=a\otimes a$ and $\epsilon(a)=1$ for all $a\in\mathcal{C}$. Writing $[a,b]={}^ab$ as a notation, the axioms boil down in this case to*

$$^{(^ab)}(^ac)={}^a(^bc),\quad \forall a,b,c\in\mathcal{C}.$$

The regularity condition amounts to the requirement that for every a,c there is a unique b such that ${}^ab=c$. Such a structure is called a rack*. A* quandle *as opposed to a rack has the further condition ${}^aa=a$ and this is expressed in braided-Lie algebra terms as the further condition $[\ ,\ ]\Delta=\mathrm{id}$. We assume henceforth that $\mathcal{C}$ is finite. Then the Killing form on basis elements is clearly*

$$K(a,b)=\mathrm{Trace}_{\mathcal{L}}{}^a(^b(\ ))=|\{c\in\mathcal{C}\mid {}^a(^bc)=c\}|,\quad a,b\in\mathcal{C}$$

(the number of fixed points in $\mathcal{C}$ under the iterated action shown). Proposition 2·4 tells us (here $\sigma=\mathrm{id}$) that if a rack has invertible Killing form then it is necessarily a quandle. The quadratic bialgebra $U(k\mathcal{C})$ is generated by $a\in\mathcal{C}$ with relations $(^ab)a=ab$ for all basis elements $a,b\in\mathcal{C}$. If $\mathcal{C}\subseteq G\setminus\{e\}$ is an ad-stable subset of a group G it is well-known that it forms quandle (this point of view apparently goes back to Conway and Wraith), with ${}^ab=aba^{-1}$. In this case there is a bialgebra map $U(\mathcal{L})\to kG$ sending a basis element of $\mathcal{L}$ to the same element viewed in G (if $\mathcal{C}$ generates then this is a surjection). Also in this case

$$K(a,b)=|Z(ab)\cap\mathcal{C}|=\chi_{\mathcal{L}}(ab),\quad \forall a,b\in\mathcal{C} \tag{2·1}$$

where $\chi_{\mathcal{L}}$ is the character of the conjugation representation of G on $\mathcal{L}$ and $Z(g)$ denotes the centralizer of $g\in G$. Clearly K is ad-invariant since $\mathcal{C}$ is and not only $\tilde\Psi$-symmetric *but actually symmetric since* $\chi_{\mathcal{L}}(ba) = \chi_{\mathcal{L}}(a(ba)a^{-1}) = \chi_{\mathcal{L}}(ab)$ *for all* $a, b \in \mathcal{C}$. *It is an interesting question if, starting with a 'Lie algebra'* $\mathcal{C} \subseteq G \setminus \{e\}$ *where* $\mathcal{C}$ *generates, we can recover the group* G. *The answer is in general that one has a covering group* $G_{\mathcal{C}} \twoheadrightarrow G$ [**18**].

We have also made reference in the introduction to the use of 'differential calculus' on quantum groups as one method of construction of braided-Lie algebras. We will not need this explicitly so suffice it to say that a differential structure on a unital algebra A means an $A-A$-bimodule Ω^1 of 'differential 1-forms' equipped with a map $\mathrm{d} : A \to \Omega^1$ obeying the Leibniz rule. We also require that the map $A \otimes A \to \Omega^1$ sending $a \otimes b \mapsto a\,\mathrm{d}b$ is surjective and, optionally (one says that the calculus is connected) that $\ker(\mathrm{d})$ is spanned by 1. When A is a Hopf algebra or 'quantum group' we can require the calculus to be covariant under left or right translation, or both. In the latter case one says that the calculus is bicovariant and these are classified by Ad-stable right ideals I in the augmentation ideal A^+ (cf. [**26**]). The left-invariant 1-forms Λ^1 can be identified with A^+/I and Ω^1 is a free A-module over Λ^1. The classical situation is where $A = \mathbb{C}[G]$, for G an algebraic group, $A^+ = \mathfrak{m}_e$, the functions vanishing at the identity, and $I = \mathfrak{m}_e^2$. Every unital algebra has a universal differential calculus defined as $\Omega^1 = \ker(\cdot : A \otimes A \to A)$ and $\mathrm{d}a = 1 \otimes a - a \otimes 1$ which in the Hopf algebra case is bicovariant (it corresponds to $I = 0$). A calculus is called 'inner' if there is $\theta \in \Omega^1$ such that $[\theta, a] = \mathrm{d}a$ for all $a \in A$. This is a nonclassical concept.

Theorem 2·5. [**8**] *Let* A *be a coquasitriangular Hopf algebra and* Ω^1 *an inner bicovariant differential calculus. Then there is a braided-Lie algebra* $\mathcal{L}$ *associated to* Λ^1 *which lives in the braided category of right* A*-comodules.*

In the case of the algebra of functions on a finite group the bicovariant calculi are classified by ad-stable subsets $\mathcal{C} \subseteq G \setminus \{e\}$ with equality in the case of the universal calculus. The calculus associated to $\mathcal{C}$ is inner with

$$\theta = \sum_{a \in \mathcal{C}} \omega_a$$

where ω_a is the image in A^+/I of the Kronecker δ-function at a. It is connected if $\mathcal{C}$ generates. In general, calculi on finite sets are classified by digraph structures on the given set as the vertices, see [**17**] for some recent work. The calculus is connected in the sense above if and only if the underlying graph is connected. In this context $\mathcal{C}$ stable under inversion corresponds to the digraph being bidirected, i.e. with every edge having arrows in both directions. The graphs here are Cayley graphs and are connected if and only if $\mathcal{C}$ generates. From this point of view:

Lemma 2·6. *A finite group* G *is simple* if and only if *all its nonzero bicovariant calculi are connected.*

Proof. Suppose that G is simple and $\mathcal{C}$ a nonempty ad-stable subset (defining a nonzero bicovariant calculus). Let $N = \langle \mathcal{C} \rangle$ the subgroup generated by $\mathcal{C}$. This is clearly normal and contains more than e (as $\mathcal{C}$ is nonempty), hence $N = G$ and the calculus is connected. Conversely, suppose that all nonempty ad-stable subsets $\mathcal{C}$ generate G. Let $N \subseteq G$ be normal and $\mathcal{C} = N \setminus \{e\}$. This is an ad-stable subset and $\langle \mathcal{C} \rangle = N$ as $N \neq \{e\}$ is a normal subgroup, hence $N = G$. □

Clearly one can further develop the differential geometry of 'finite Lie groups' and notably S_3 has in some sense constant curvature while A_4 is Ricci flat for noncommutative differential structures provided by suitable conjugacy classes and metrics [**16**, **19**]. As far as we know no simple groups have yet been studied at this level of noncommutative Riemannian geometry.

3. *Nondegeneracy of the Killing form for an ad-stable subset*

In this section we will look at the question of non-degeneracy of the Killing form in maximum generality and with miscellaneous results and examples. Then Section 4 will cover the case of the universal calculus and Section 5 the case of conjugacy classes. The analyses of these two extremal cases contain the main results of the paper.

Let G be a finite group and $\mathcal{C} \subseteq G \setminus \{e\}$ be an ad-stable subset with K the associated Killing form (1·2) on $\mathcal{L} = k\mathcal{C}$.

LEMMA 3·1. *If $\mathcal{C} \cap (\mathcal{C}.c) \neq \emptyset$ for some nontrivial $c \in Z(G)$ then K is degenerate. In particular, if $|Z(G) \cap \mathcal{C}| > 1$ then K is degenerate.*

Proof. Looking at K as a matrix with rows and columns labelled by $\mathcal{C}$. If $b = b'c$ where $b, b' \in \mathcal{C}$ and $c \in Z(G) \setminus \{e\}$ then $K(a, b) = |Z(ab) \cap \mathcal{C}| = |Z(ab'c) \cap \mathcal{C}| = |Z(ab') \cap \mathcal{C}| = K(a, b')$ for all $a \in \mathcal{C}$, hence K has a repeated column. If $b, b' \in Z(G) \cap \mathcal{C}$ are distinct then $c = b'^{-1}b$ fits the first part. □

COROLLARY 3·2. *If $|G| > 2$ and $|Z(G)| > 1$ then the Killing form for the universal calculus is degenerate.*

Proof. For the universal calculus $\mathcal{C} = G \setminus \{e\}$ and in the preceding lemma we can take any nontrivial $c \in Z(G)$, any $b' \neq c^{-1}, e$ and $b = b'c$. Then $b \in \mathcal{C} \cap (\mathcal{C}c)$. □

If G has order 2 then K *is* a 1×1 matrix and *is* nondegenerate. We therefore only need to investigate the universal calculus in the case where $|G| > 2$ and $Z(G) = \{e\}$. Even for nonuniversal calculi it will be necessary to avoid too much intersection with $Z(G)$ as Lemma 3·1 shows.

PROPOSITION 3·3. *Let D_{2n} be the dihedral group $\mathbb{Z}_n \rtimes \mathbb{Z}_2 = \langle a, x \rangle$ with relations $x^2 = e$, $a^n = e$, $xa = a^{-1}x$.*

(1) *For odd n, the universal calculus is nondegenerate*

(2) *For odd n, the order 2 conjugacy classes $\mathcal{C}_i = \{a^i, a^{-i}\}$, $i = 1, \cdots, \frac{n-1}{2}$ have degenerate K and we have a single generating conjugacy class $\mathcal{C}_0 = \{a^k x \mid 1 \leq k \leq n\}$ of reflections, which has nondegenerate K.*

(3) *For even n, the universal calculus has degenerate K.*

Hence for odd n, D_{2n} is nondegenerate and class-nondegenerate in the sense of Definition 1·1.

Proof. Part (3) is an application of Corollary 3·2 since when n is even the centre is $\{e, a^{\frac{n}{2}}\}$. Now let us write $\mathbb{Z}_n$ for the cyclic subgroup of rotations in D_{2n}. For part (1) we use that the centralisers are

$$Z(a^i) = \begin{cases} \mathbb{Z}_n & \text{if } i \neq 0 \\ D_{2n} & \text{otherwise,} \end{cases} \qquad Z(a^i x) = \{e, a^i x\}.$$

Hence in the basis $\{a, a^2, \cdots, a^{n-1}, x, ax, \cdots, a^{n-1}x\}$ we have

$$K = \begin{pmatrix} (n-1)\theta_{n-1,n-1} + n\bar{1}_{n-1,n-1} & \theta_{n-1,n} \\ \theta_{n,n-1} & (n-1)\theta_{n,n} + n1_{n,n} \end{pmatrix}$$

where $\theta_{i,j}$ is the matrix with i rows and j columns, and all entries equal to 1, and $1_{j,j}$ is the $j \times j$ identity matrix, and $\bar{1}_{j,j}$ is the permutation matrix which has 1's along the anti-diagonal and 0's elsewhere. The matrix K is straightforwardly seen to be invertible with inverse

$$K^{-1} = \frac{1}{mn} \begin{pmatrix} -(n^2-n-1)\theta_{n-1,n-1} + m\bar{1}_{n-1,n-1} & -\theta_{n-1,n} \\ -\theta_{n,n-1} & -(n-1)^2\theta_{n,n} + m1_{n,n} \end{pmatrix},$$

where $m = 1 - n^2 + n^3$.

Note that (1) also follows later from Theorem 4·2 as one can easily see that D_{2n} for n odd has the Roth property. Namely for $i \neq 0$ the conjugation representation $\mathbb{C}\mathcal{C}_i$ decomposes as $\mathbb{C}\mathcal{C}_i = 1 \oplus \bar{1}$ where $\bar{1}$ is spanned by $a^i - a^{-i}$ so that conjugation by x acts as -1 and a acts trivially, and 1 stands for the trivial representation. Meanwhile $\mathbb{C}\mathcal{C}_0 = \mathbb{C}\theta \oplus (\bigoplus_{k=1}^{\frac{n-1}{2}} V_k)$ where $\theta = \sum_{i=0}^{n-1} a^i x$ is the sum of all the elements in $\mathcal{C}_0$ and the V_k are 2-dimensional irreducible representations spanned by $v_k^{\pm} = \sum_{j=0}^{n-1} e^{\frac{\pi\imath jk}{n}} a^{\mp j} x$, where conjugation by x gives transposition and conjugation by a gives multiplication by a phase factor of $e^{\frac{2\pi\imath k}{n}}$. Hence all $\frac{n+1}{2}$ irreducible representations occur in the conjugation representation of the group D_{2n}.

For (2) on $\mathcal{C}_i$ the entries of K are 2, so these have degenerate K, while $\mathcal{C}_0$ has Killing form $K(a^i x, a^j x) = |\mathcal{C}_0 \cap Z(a^{i-j})| = n\delta_{ij}$ so this is nondegenerate. The $\mathcal{C}_i$ classes do not generate, while $\mathcal{C}_0$ generates so the group is class-nondegenerate. □

Along the same lines it seems likely that D_{2n} is in fact strongly nondegenerate for all n odd, and this has been experimentally confirmed for dihedral groups of small order, but a general proof would be significantly more complicated than the universal case above and is deferred to elsewhere. Clearly it is not absolutely nondegenerate.

Proposition 3·4. *If $\mathcal{C} \subseteq G \setminus \{e\}$ has nondegenerate K then the index of the latter is equal to the number of involutions in $\mathcal{C}$.*

Proof. Let $\pi(a)$ be the matrix of $a \in \mathcal{C}$ in the conjugation representation. As this is a permutation matrix, its inverse is its transpose. Hence if a is an involution $\pi(a)$ is real and symmetric. We may identify $\mathbb{C}\mathcal{C}$ with $\mathbb{C}^{|\mathcal{C}|}$ using $\mathcal{C}$ as a basis. We denote by $\bar{v}$ the complex conjugate of $v \in \mathbb{C}\mathcal{C}$ defined using this identification. We also let $(\ )^\dagger$ denote the associated hermitian transpose. We decompose $\mathbb{C}\mathcal{C}$ into 'symmetric' and 'anti-symmetric' parts, $\mathbb{C}\mathcal{C} = S \oplus A$. Here S has a basis made up of the involutions in $\mathbb{C}$ and the elements $a + a^{-1}$ for all $a \in \mathcal{C}$ not an involution, and A has a basis given by the non-zero elements of the form $a - a^{-1}$, which under π go to real antisymmetric matrices. Consider $v \in S$ and $w \in A$. Then $\pi(\bar{v}) = \pi(v)^\dagger$ because the basis elements go to real symmetric matrices, and therefore $K(\bar{v}, v) = \mathrm{Tr}(\pi(v)^\dagger \pi(v)) \geq 0$. Similarly $\pi(\bar{w}) = -\pi(w)^\dagger$ and $K(\bar{w}, w) = -\mathrm{Tr}(\pi(w)^\dagger \pi(w)) \leq 0$. Finally $K(\bar{v}, w) = 0$ as the trace of the product of a symmetric and an antisymmetric matrix. If K is nondegenerate then $K(\bar{v}, v) = 0$ is not possible for $v \neq 0$ since the underlying real symmetric matrix of K in our basis has no 0-eigenspace. Hence in this case $(\dim(S), \dim(A))$ is the signature of K, their difference is the number of involutions. □

Clearly, one has a similar result over $\mathbb{R}$ without complex conjugation.

Next we associate some auxiliary objects to each ad-stable $\mathcal{C} \subseteq G \setminus \{e\}$, namely

$$\theta = \sum_{a \in \mathcal{C}} a, \quad \theta^*(a) = 1, \quad \lambda^*(a) = |Z(a) \cap \mathcal{C}|, \quad \forall a \in \mathcal{C} \tag{3·1}$$

where θ^*, λ^* are linear functions on $\mathbb{C}\mathcal{C}$ defined on basis elements. In a matrix-vector notation, we also define some numerical constants in $\mathbb{Q}$

$$\mu = \theta \cdot K^{-1}\theta, \quad \nu = \lambda \cdot K^{-1}\theta, \quad \rho = \lambda \cdot K^{-1}\lambda, \tag{3·2}$$

associated to any K for which θ and λ are in the image. Here we are working in our fixed basis $\mathcal{C}$ and $\cdot$ is the dot product of vectors in $\mathbb{C}\mathcal{C}$ or Euclidean inner product in our basis. From elementary linear algebra[**11**] the quantities μ, ν and ρ are well defined independent of the choice of representatives $K^{-1}\theta$ and $K^{-1}\lambda$. For example, if $Kv = \theta$ and $Kw = \lambda$ then

$$\nu := \lambda^t v = w^t K^t v = w^t K v = w^t \theta,$$

which is independent of the choice of v because of its expression in terms of w, and independent of w because of its expression in terms of v. In the case where K is invertible, μ is the sum of all the entries of K^{-1}.

Also note that if G_1, G_2 are groups with $\mathcal{C}_1, \mathcal{C}_2$ ad-stable subsets not containing the identity then

$$\mathcal{C}_1 \times \mathcal{C}_2, \quad \mathcal{C}_1 \sqcup \mathcal{C}_2 = \mathcal{C}_1 \times \{e\} \cup \{e\} \times \mathcal{C}_2 \subseteq (G_1 \times G_2) \setminus \{e\}$$

satisfy the same properties in $G_1 \times G_2$. The first of these has

$$K_{\mathcal{C}_1 \times \mathcal{C}_2}((a,b),(c,d)) = K_1(a,c)K_2(b,d), \quad \forall a, c \in \mathcal{C}_1,\ b, d \in \mathcal{C}_2$$

and this is clearly nondegenerate if K_i are. The second (the disjoint union) is the analogue of the direct sum of Lie algebra structures on the direct product of Lie groups.

PROPOSITION 3·5. *Let $G_1, \mathcal{C}_1$ and $G_2, \mathcal{C}_2$ be two finite groups with ad-stable subsets $\mathcal{C}_1, \mathcal{C}_2$ and K_1, K_2 nondegenerate. Then $K_{\mathcal{C}_1 \sqcup \mathcal{C}_2}$ is nondegenerate if and only if*

$$\det \begin{pmatrix} \rho_1 & d_2\nu_1 & 1 & \nu_1 \\ d_1\nu_2 & \rho_2 & \nu_2 & 1 \\ 1 + d_1\mu_2 & \nu_2 & \mu_2 & 0 \\ \nu_1 & 1 + d_2\mu_2 & 0 & \mu_1 \end{pmatrix} \neq 0$$

where $d_i = |\mathcal{C}_i|$ and μ_i, ν_i, ρ_i are associated to K_i as in (3·2).

Proof. When $a, b \in \mathcal{C}_1$ we have $K(a,b) = |(\mathcal{C}_1 \sqcup \mathcal{C}_2) \cap Z(ab)| = K_1(a,b) + d_2$ as all elements of the form $\{e\} \times \mathcal{C}_2$ commute with (ab, e). Similarly when $a \in \mathcal{C}_1, b \in \mathcal{C}_2$ we will have $K(a,b) = \lambda_1(a) + \lambda_2(b)$. In block matrix form this looks like

$$K_{\mathcal{C}_1 \sqcup \mathcal{C}_2} = \begin{pmatrix} K_1 & 0 \\ 0 & K_2 \end{pmatrix} + \begin{pmatrix} \theta_1 \otimes \theta_1^* d_2 & \lambda_1 \otimes \theta_2^* + \theta_1 \otimes \lambda_2^* \\ \lambda_2 \otimes \theta_1^* + \theta_2 \otimes \lambda_1^* & d_1\theta_2 \otimes \theta_2^* \end{pmatrix}$$

Hence for $v + w \in \mathbb{C}\mathcal{C}_1 \oplus \mathbb{C}\mathcal{C}_2$ as a column vector to be in the kernel means

$$K_1 v + \theta_1(d_2\theta_1 \cdot v + \lambda_2 \cdot w) + \lambda_1\theta_1 \cdot w = 0, \quad K_2 w + \theta_2(d_2\theta_2 \cdot w + \lambda_1 \cdot v) = 0.$$

When the K_i are invertible we write these as

$$v + K_1^{-1}\theta_1(d_2\alpha + \delta) + K_1^{-1}\lambda_1\beta = 0, \quad w + K_2^{-1}\theta_2(d_1\beta + \gamma) + K_2^{-1}\lambda_2\alpha = 0 \tag{3·3}$$

where

$$\alpha = \theta_1 \cdot v, \quad \beta = \theta_2 \cdot w, \quad \gamma = \lambda_1 \cdot v, \quad \delta = \lambda_2 \cdot w.$$

We now apply $\theta_i\cdot$ and $\lambda_i\cdot$ to (3·3) to obtain four equations for these four scalars, described by the displayed matrix. Hence $\alpha, \beta, \gamma, \delta$ are zero and hence v, w are zero by (3·3), unless the stated determinant is not zero. Conversely if the determinant vanishes we may solve for $\alpha, \beta, \gamma, \delta$ hence for v, w and K is degenerate. □

The result suggests that 'generically', i.e. unless the determinant accidentally vanishes, nondegenerate Killing forms remain nondegenerate for the direct sum 'Lie algebra' structure on the direct product of two groups.

Example 3·6. *For D_{2n} with $n \geq 3$ odd and the universal calculus, we have $\lambda = (n-1, \cdots, n-1, 1, \cdots, 1)$ and*

$$d = 2n - 1, \qquad \mu = \frac{3 - 4n + 2n^2}{1 - n^2 + n^3},$$
$$\nu = \frac{1 + n - 2n^2 + n^3}{1 - n^2 + n^3}, \qquad \rho = \frac{-1 + 2n + 2n^2 - 3n^3 + n^4}{1 - n^2 + n^3}$$

from formulae in the proof of Proposition 3·3*. Then any two such $D_{2n}, D_{2n'}$ have nondegenerate $D_{2n} \times D_{2n'}$ with the direct sum 'Lie algebra'. Here the determinant can be checked for small n, n' while for $n, n' \geq 3$ the determinant grows more negative as either n, n' increase and hence is never zero.*

We will study the determinant criterion further in Section 5 in the case where $\mathcal{C}_i$ are conjugacy classes.

4. *Nondegeneracy for the universal calculus*

In this section we will exclusively study the case $\mathcal{C} = G \setminus \{e\}$ where G is a finite group, i.e. the universal calculus and its associated 'Lie algebra' structure on G. We have already seen in Corollary 3·2 that for a group to be nondegenerate in the sense of Definition 1·1 it will at least have to be centreless or $\mathbb{Z}_2$.

In the present setting of the universal calculus we have

$$K(a, b) = |Z(ab)| - 1, \quad \forall a, b \in \mathcal{C}$$

and we similarly have

$$\lambda^*(a) = |Z(a)| - 1, \quad \forall a \in \mathcal{C}$$

which we extend as a linear function on $k\mathcal{C}$. This is the character of the conjugation representation on $\mathcal{C}$ restricted to $\mathcal{C}$. Also in our case the 'inner generator' (3·1) is

$$\theta = \Lambda - e$$

where $\Lambda = \sum_{g \in G} g$ is the integral in the group algebra. Similarly $\theta^*(a) = 1$ for all $a \in \mathcal{C}$ is the integral on the group regarded as a linear function on $\mathbb{C}\mathcal{C}$.

Lemma 4·1. *For the universal calculus on a finite group,*

$$K(\theta, \ ) = -\lambda^* + |G|(N-1)\theta^*$$

where N is the number of conjugacy classes in G including the trivial one. If λ or θ are *in the image of the Killing form then the associated constants μ, ν, ρ in (3·2) are defined and related by*

$$1-\nu = |G|(1-(N-1)\mu), \quad |G|-1-\rho = |G|^2(N-1)(1-(N-1)\mu).$$

Proof. We consider λ^* to be defined on all of G by the formula (the trace of the conjugation representation on $\mathbb{C}\mathcal{C}$). Then for $h \in G$,

$$K(\theta,h) = \sum_{g\neq e} \lambda^*(gh) = \sum_{g\neq h} \lambda^*(g) = -\lambda^*(h) + \sum_{g\in G} \lambda^*(g)$$

so that $K(\theta, \ ) = -\lambda^* + \lambda^*(\Lambda)\theta^*$. Moreover, $\lambda^*(\Lambda) = (\sum_{g\in G} |Z(g)|) - |G| = |G|(N-1)$ by the orbit counting lemma. Also note that $\lambda^*(\theta) = |G|(N-2)+1$. This gives the displayed formula. Clearly then if either θ or λ are in the image of K then so is the other so that μ, ν, ρ are well-defined. Using a vector-matrix notation, we have $\theta = -K^{-1}\lambda + |G|(N-1)K^{-1}\theta + m$ for any choice of inverse elements and some $m \in \ker K$ and applying $\theta\cdot$ and $\lambda\cdot$ to this to give relations

$$d+\nu = |G|\mu(N-1), \quad |G|(N-1)+\rho-d = |G|(N-1)\nu$$

which we write as stated. Here $\theta.m = \lambda.m = 0$ by writing θ, λ as in the image of K and using the symmetry of K to move it over to operate on m. (Note also that $(\nu-1)(\nu+d) = (\rho-d)\mu$ as a consequence). Of course $d := |\mathcal{C}| = |G|-1$ in the present context. □

Our main result of this section is the following theorem.

THEOREM 4·2. *Let G be a finite group such that the conjugation representation on $\mathbb{C}G$ contains every irreducible representation ('Roth property'). Then it is nondegenerate.*

We will prove this by proving a more general result, Proposition 4·3. Here we work with the expression (2·1). We note that this formulation of the Killing form via the character of the conjugation representation $\mathbb{C}\mathcal{C}$ makes sense for any representation W as a bilinear form on $\mathbb{C}G$. Namely we let

$$K_W(a,b) := \chi_W(ab)$$

where $\{a \mid a \in G\}$ is a basis of $\mathbb{C}G$. It is well-known that this symmetric bilinear form on $\mathbb{C}G$ is nondegenerate if and only if W contains every irreducible representation of G with positive multiplicity. This follows from semisimplicity of the group algebra $\mathbb{C}G$ and general facts about semisimple algebras. Namely, if an algebra is semisimple then it is a direct sum of matrix blocks. If $W = \bigoplus_i n_i V_i$ for some multiplicities n_i of irreducible representations V_i then K_W has a block form with n_i times the Euclidean inner product on each matrix block. This is because an element in a matrix block corresponding to a particular irreducible representation acts as zero by left multiplication on any other block and hence in any other irreducible representation. Hence K_W is nondegenerate on $\mathbb{C}G$ if and only if all the $n_i > 0$.

PROPOSITION 4·3. *Let G be a finite group and W be a representation of G for which every irreducible representation appears in W with strictly positive multiplicity. Then the restriction of K_W to $\mathbb{C}.(G \setminus \{e\})$ is nondegenerate.*

Proof. Since the form K_W is nondegenerate on $\mathbb{C}G$ we know that $(\mathbb{C}.(G\setminus\{e\}))^\perp$ is one-dimensional. We will know that K_W is nondegenerate in $\mathbb{C}.(G\setminus\{e\})$ if there is no element in the perpendicular which also lies $\mathbb{C}.(G \setminus \{e\})$. We prove this by determining explicitly a vector spanning the line $(\mathbb{C}.(G \setminus \{e\}))^{\perp}$, and observing that it doesn't lie in $\mathbb{C}.(G \setminus \{e\})$.

Suppose the irreducible representations are $V_1, \cdots, V_n$ say. Define

$$m = \sum_{g \in G} \left(\sum_{i=1}^{n} \frac{\dim(V_i)^2}{\langle \chi_{V_i}, \chi_W \rangle} \overline{\chi_{V_i}(g)} \right) g$$

This is well-defined since $\langle \chi_{V_i}, \chi_W \rangle \neq 0$ for all i by our assumption. We claim that $K_W(a, m) = 0$ for all $a \neq e$. Note that the coefficient of e in m is given by the formula

$$m_e = \sum_{i=1}^{n} \frac{\dim(V_i)^3}{\langle \chi_{V_i}, \chi_W \rangle},$$

so is always strictly positive. Therefore m does not lie in $\mathbb{C}.(G \setminus \{e\})$ and the claim will imply the proposition. We recall the standard orthogonality relations

$$\sum_{g \in G} \overline{\chi_V(g)}\, \chi_{V'}(ga) = \begin{cases} 0 & \text{if } V, V' \text{ are distinct irreducible representations,} \\ \frac{|G|}{\dim V} \chi_V(a) & \text{otherwise,} \end{cases}$$

and

$$\sum_i \overline{\chi_{V_i}(a_1)} \chi_{V_i}(a_2) = 0 \quad \text{if } a_1 \text{ and } a_2 \text{ are not conjugate}$$

and also note that

$$\chi_W(g) = \sum_i \langle \chi_{V_i}, \chi_W \rangle\, \chi_{V_i}(g).$$

Now we can compute, extending linearly,

$$\begin{aligned} K_W(m, a) &= K_W \left(\sum_{g \in G} \left(\sum_{i=1}^{n} \frac{\dim(V_i)^2}{\langle \chi_{V_i}, \chi_W \rangle} \overline{\chi_{V_i}(g)} \right) g, a \right) \\ &= \sum_{g \in G} \left(\sum_{i=1}^{n} \frac{\dim(V_i)^2}{\langle \chi_{V_i}, \chi_W \rangle} \overline{\chi_{V_i}(g)} \right) \chi_W(ga) = \sum_{i=1}^{n} \frac{\dim(V_i)^2}{\langle \chi_{V_i}, \chi_W \rangle} \left(\sum_{g \in G} \overline{\chi_{V_i}(g)} \chi_W(ga) \right) \\ &= \sum_{i=1}^{n} \dim(V_i)^2 \left(\sum_{g \in G} \overline{\chi_{V_i}(g)} \chi_{V_i}(ga) \right) = |G| \sum_i \dim(V_i) \chi_{V_i}(a) \\ &= |G| \sum_i \overline{\chi_{V_i}(e)} \chi_{V_i}(a). \end{aligned}$$

The last expression vanishes whenever $a \neq e$ by orthogonality. □

Proof. (of the theorem) Now suppose that G is a finite group and the conjugation representation on $\mathbb{C}G$ contains every irreducible representation (this is the Roth property in this context). We set $W = \mathbb{C}.(G \setminus \{e\})$ where we remove the group identity. This W still contains a copy of the trivial representation since it is a permutation representation, and for example the element θ is invariant. As $\mathbb{C}G = W \oplus \mathbb{C}.e$ as a G-module, any nontrivial representation contained in $\mathbb{C}G$ must also be in W. Hence W also enjoys the property of containing every irreducible representation. We then apply Proposition 4·3. □

Note that the group will have to be centreless for the Roth property to hold in the form stated. The simplest example where the Roth property holds is $G = S_3$, the group of permutations on three elements. This is elementary enough that we can, instructively, work out everything in our above approach by hand.

EXAMPLE 4·4. *Let G be S_3, with its three irreducible characters χ_{triv}, χ_{sign} and χ_Δ corresponding to the trivial, the sign and the standard representations, $V_{triv}, V_{sign}, V_\Delta$. Then it is easy to see that the conjugation representation $W = \mathbb{C}(G \setminus \{e\})$ decomposes as $V_{triv}^{\oplus 2} \oplus V_{sign} \oplus V_\Delta$, so it contains ever irreducible representation of G. The Killing form on $\mathbb{C}G$ for $W = \mathbb{C}(G \setminus \{e\})$ is*

$$K_W = \begin{pmatrix} 5\,1\,1\,1\,2\,2 \\ 1\,5\,2\,2\,1\,1 \\ 1\,2\,5\,2\,1\,1 \\ 1\,2\,2\,5\,1\,1 \\ 2\,1\,1\,1\,2\,5 \\ 2\,1\,1\,1\,5\,2 \end{pmatrix}$$

in a basis $e, u = (12), v = (23), w = (13) = uvu, uv = (123)$ and $vu = (132)$. This matrix is just obtained by working out $\chi_W(gh) = |Z(gh)| - 1$ for all $g, h \in S_3$. One can then see by direct computation that the lower right 5×5 block in K_W is invertible as required by Theorem 4·2. Or, like in proof of Proposition 4·3, $\mathbb{C}(G \setminus \{e\})^\perp$ is spanned by the single group algebra element,

$$m = \frac{1}{2}\chi_{triv} + \chi_{sgn} + 4\chi_\Delta = \frac{1}{2}(19e - (u + v + w) - 5(uv + vu)).$$

Clearly, since m has a nonzero coefficient of e, it does not lie in $\mathbb{C}.(G \setminus \{e\})$.

Next, the Roth property is manifestly closed under direct products. We see now how this emerges from linear algebra in our Killing form approach and that the converse holds.

PROPOSITION 4·5. *Let G_1, G_2 be two nondegenerate finite groups. Then $G_1 \times G_2$ is nondegenerate* if and only if

$$\mu \neq \frac{1}{N-1}$$

for each group.

Proof. The Killing form for the universal calculus on $G_1 \times G_2$ is

$$\begin{aligned} K((a,b),(c,d)) &= |Z_{G_1 \times G_2}((ac, bd))| - 1 = |Z_{G_1}(ac)||Z_{G_2}(bd)| - 1 \\ &= \tilde{K}_1(a,c)\tilde{K}_2(b,d) + \tilde{K}_1(a,c) + \tilde{K}_2(b,d) \end{aligned}$$

in terms of the extensions of Killing forms K_i of each group to $\mathbb{C}G_i$. We write

$$\mathcal{C} = (G_1 \times G_2) \setminus \{(e,e)\} = (\mathcal{C}_1 \times \mathcal{C}_2) \sqcup \mathcal{C}_1 \sqcup \mathcal{C}_2$$

where $\mathcal{C}_i = G_i \setminus \{e\}$. We have K then in 3×3 block form with

$$\begin{aligned} K((a,b),(c,d)) &= K_1(a,c)K_2(b,d) + K_1(a,c) + K_2(b,d) \\ K((a,b),(c,e)) &= K_1(a,c)(1 + \lambda_2(b)) + \lambda_2(b) \\ K((a,b),(e,d)) &= K_2(b,d)(1 + \lambda_1(a)) + \lambda_1(a) \end{aligned}$$

$$K((a,e),(c,e)) = K_1(a,c)(d_2+1) + d_2$$
$$K((a,e),(e,d)) = \lambda_1(a)\lambda_2(d) + \lambda_1(a) + \lambda_2(d)$$

for $a, c \in \mathcal{C}_1, b, d \in \mathcal{C}_2$, and the other cases by symmetry. In matrix-vector notation, for an element $v + w + z \in \mathbb{C}(\mathcal{C}_1 \times \mathcal{C}_2) \oplus \mathbb{C}\mathcal{C}_1 \oplus \mathbb{C}\mathbb{C}_2$, written as a matrix, a column vector and a row vector respectively, to be in the kernel of K means

$$K_1vK_2 + K_1v\theta_2\theta_2^* + \theta_1\theta_1^*vK_2 + K_1w(\lambda_2^* + \theta_2^*) + \theta_1\theta_1^*w\lambda_2^* + (\lambda_1+\theta_1)zK_2 + \lambda_1z\theta_2\theta_2^* = 0$$

$$K_1v(\theta_2+\lambda_2) + \theta_1\theta_1^*v\lambda_2 + |G_2|K_1w + d_2\theta_1\theta_1^*w + (\lambda_1+\theta_1)z\lambda_2 + \lambda_1z\theta_2 = 0$$

$$(\theta_1^* + \lambda_1^*)vK_2 + \lambda_1^*v\theta_2\theta_2^* + \lambda_1^*w(\lambda_2^*+\theta_2^*) + \theta_1^*w\lambda_2^* + |G_1|zK_2 + d_1z\theta_2\theta_2^* = 0.$$

We will use the notation

$$\phi = \theta_1 \cdot w, \quad \psi = z\theta_2, \quad \sigma = \lambda_1 \cdot w, \quad \tau = z\lambda_2$$

$$\alpha = \theta_1 \cdot v\lambda_2, \quad \beta = \lambda_1 \cdot v\theta_2, \quad \gamma = \theta_1 \cdot v\theta_2, \quad \delta = \lambda_1 v \cdot \lambda_2$$

then applying K_i^{-1} our three equations for the kernel become

$$v + v\theta_2\theta_2^*K_2^{-1} + K_1^{-1}\theta_1\theta_1^*v + w(\lambda_2^*+\theta_2^*)K_2^{-1} + K_1^{-1}\theta_1\phi\lambda_2^*K_2^{-1} + K_1^{-1}(\lambda_1+\theta_1)z + K_1^{-1}\lambda_1\psi\theta_2^*K_2^{-1} = 0$$

$$v(\theta_2+\lambda_2) + K_1^{-1}\theta_1\alpha + |G_2|w + d_2K_1^{-1}\theta_1\phi + K_1^{-1}(\lambda_1+\theta_1)\tau + K_1^{-1}\lambda_1\psi = 0$$

$$(\theta_1^*+\lambda_1^*)v + \beta\theta_2^*K_2^{-1} + \sigma(\lambda_2^*+\theta_2^*)K_2^{-1} + \phi\lambda_2^*K_2^{-1} + |G_1|z + d_1\psi\theta_2^*K_2^{-1} = 0.$$

We now apply evaluation or dot product of the relevant θ_i, λ_i to the two sides of the first equation and to one side of each of the other two, to obtain eight equations for the scalar variables $\phi, \psi, \beta, \alpha, \sigma, \tau, \gamma, \delta$ governed in that basis order by an 8×8 matrix. Specifically, if

$$\begin{pmatrix} d_1\nu_1 & \rho_1 & 1 & \nu_1 & 1+d_2 & \nu_1+\rho_1 & 0 & 1 \\ \rho_2 & d_2\nu_2 & \nu_2 & 1 & \nu_2+\rho_2 & 1+d_1 & 0 & 1 \\ \nu_1\nu_2 & \nu_1+(1+\mu_2)\rho_1 & 1+\mu_2 & 0 & \mu_2+\nu_2 & 0 & \nu_1 & 0 \\ \nu_2+(1+\mu_1)\rho_2 & \nu_1\nu_2 & 0 & 1+\mu_1 & 0 & \mu_1+\nu_1 & \nu_2 & 0 \\ \nu_2 & 1+d_1(1+\mu_2) & 1+\mu_2 & 0 & \mu_2+\nu_2 & 0 & 1 & 0 \\ 1+d_2(1+\mu_1) & \nu_1 & 0 & 1+\mu_1 & 0 & \mu_1+\nu_1 & 1 & 0 \\ \mu_2+(1+\mu_1)\nu_2 & \mu_1+(1+\mu_2)\nu_1 & 0 & 0 & 0 & 0 & 1+\mu_1+\mu_2 & 0 \\ \nu_1\rho_2 & \nu_2\rho_1 & \nu_2 & \nu_1 & \nu_2+\rho_2 & \nu_1+\rho_1 & 0 & 1 \end{pmatrix} \neq 0$$

then these variables are all zero and our three equations for v, w, z simplify to

$$v + v\theta_2\theta_2^*K_2^{-1} + K_1^{-1}\theta_1\theta_1^*v + w(\lambda_2^*+\theta_2^*)K_2^{-1} + K_1^{-1}(\lambda_1+\theta_1)z = 0$$

$$v(\theta_2+\lambda_2) + |G_2|w = 0, \quad (\theta_1^*+\lambda_1^*)v + |G_1|z = 0.$$

The determinant here factorises with degree 2 factors

$$(\rho - d)(1+\mu) - (\nu-1)^2$$

for each group, so we require these not to vanish, which given Lemma 4·1 we write as $\mu \neq 1/(N-1)$ on each group. In this case one can eventually solve the linear system to determine that $v = w = z = 0$ so that $G_1 \times G_2$ is nondegenerate. Details are omitted in view of our later Theorem 4·6 which shows that both groups are Roth and hence so is their direct product, after which we can use Theorem 4·2. Conversely, if G_1 alone obeys $\mu_1(N_1-1)=1$ so $\nu_1=1$ and $\rho_1=d_1$, then the displayed matrix has a 1-dimensional null space spanned by $\alpha=-\tau,\delta=-d_1\tau$ and $\beta=\gamma=\phi=\psi=\sigma=0$. We then solve for the vector variables to find (for example) $x=-z, y=w=0$, $s=-d_1z$, $t=-K_1^{-1}\lambda_1 z$ provided $z\theta_2=0$ and $z\lambda_2=\tau$. Then $v=-K_1^{-1}\lambda_1 z$ from the equation for v. We then check that any z such that $z\theta_2=0$ and w,v as stated reproduce all other vectors and scalars as stated and thereby that the equations to be in the kernel are satisfied. Hence K is degenerate. If both G_1,G_2 obey $\mu(N-1)=1$ then the kernel of the displayed matrix is 2-dimensional but includes the previous one. The solution above still applies and K is degenerate. □

As noted in the proof, we will see in the next theorem that $\mu\neq\frac{1}{N-1}$ is characteristic of a Roth property group. So this proposition says that within the class of non-degenerate groups the Roth property groups form the largest subclass which is closed under direct products. For example $\mathbb{Z}_2$ is nondegenerate and not Roth thence the direct product $\mathbb{Z}_2\times G$ with any nondegenerate group G will be degenerate. This latter result also follows from Corollary 3·2 as $\mathbb{Z}_2\times G$ has a nontrivial center.

One can also compare with Proposition 3·5 for the disjoint union of universal 'Lie algebra' structures on the direct product of two nondegenerate finite groups. Here we find by contrast that if G_1 is non-Roth then $G_1\times G_2$ with the disjoint union structure (as opposed to the universal calculus) has nondegenerate Killing form if and only if G_2 is Roth. Thus for example $\mathbb{Z}_2\times G$ for G any Roth property group and with the disjoint union *will* have nondegenerate Killing form.

We now give our second main result of the section, which is the mentioned complete characterisation of when a finite group is Roth in terms of the Killing form, irrespective of nondegeneracy.

THEOREM 4·6. *Let G be a nontrivial finite group and N the number of conjugacy classes. The constants μ,ν,ρ associated in (3·2) to the Killing form for the universal calculus are well-defined. Moreover, the following are equivalent.*

(1) *G has the Roth property*
(2) $\mu\neq\frac{1}{N-1}$
(3) $\nu\neq 1$
(4) $\rho\neq|G|-1$.

In the Roth case

$$\mu=\frac{1}{n_0}\left(1-\frac{1}{n_0\sum_j\frac{\dim(V_j)^3}{n_j}}\right)$$

where n_j is the multiplicity of irreducible representation V_j in the representation on $W=\mathbb{C}.(G\setminus\{e\})$ and $n_0=N-1$ is the multiplicity of the trivial representation.

Proof. (i) Using the same methods as in the proof of Lemma 4·1, we regard the characters χ_{V_i} by restriction as vectors with entries the $|G|-1$ values at the different points of $\mathcal{C}$. Then

$$K(\overline{\chi_{V_j}},h)=\sum_{g\in\mathcal{C}}\chi_{V_j}(g^{-1})\lambda^*(gh)=-\lambda^*(h)\dim(V_j)+\frac{n_j|G|}{\dim(V_j)}\chi_{V_j}(h)\qquad(4·2)$$

using the orthogonality of characters. We will need this formula.

(ii) If G is missing no irreducible representations in its conjugation representation then we know that K is invertible by Theorem 4·2 so that μ,ν,ρ are defined. Alternatively, suppose G is missing V_1, say. The formula (4·2) tells us that

$$K(\overline{\chi_{V_1}}) = -\dim(V_1)\lambda.$$

so λ is in the image of K in this case. Lemma 4·1 then implies that θ is also in the image of K, namely

$$K(\theta - \frac{\overline{\chi_{V_1}}}{\dim(V_1)}) = |G|(N-1)\theta.$$

Hence Lemma 4·1 applies, μ,ν,ρ are well defined for any finite group and are related by the formulae stated there. This also means that (2)-(4) are all equivalent.

(iii) In the non-Roth case, the vector $-\overline{\chi_{V_1}}/\dim(V_1)$ lies in the inverse image $K^{-1}\lambda$. Here V_1 is as in (ii). We take the dot-product with λ and use orthogonality of characters to find

$$\begin{aligned}\rho &= -\frac{1}{\dim(V_1)}\sum_{g\neq e}\lambda(g)\overline{\chi_{V_1}}(g)\\ &= -\frac{1}{\dim(V_1)}\left(\sum_{g\in G}\chi_{\mathbb{C}G\setminus\{e\}}(g)\overline{\chi_{V_1}}(g)\right) + |G\setminus\{e\}| = |G|-1,\end{aligned}$$

because V_1 does not occur in the conjugation representation on $\mathbb{C}(G\setminus\{e\})$, and where we rewrote $\lambda(g) = \chi_{\mathbb{C}G\setminus\{e\}}(g)$.

(iv) In the Roth case since K is invertible, the formula (4·2) in vector notation gives

$$\overline{\chi_{V_j}} = -\dim(V_j)K^{-1}\lambda + \frac{n_j|G|}{\dim(V_j)}K^{-1}\chi_{V_j}.$$

We multiply both sides by $\dim(V_j)^2/n_j$ and sum over j. Now the right hand summand becomes $|G|\,K^{-1}(\sum_j\dim(V_j)\chi_{V_j})$. But $\sum_j\dim(V_j)\chi_{V_j}$ is the character of the regular representation and has support only on e. Hence regarded by restriction as a vector in $\mathbb{C}\mathcal{C} = \mathbb{C}(G\setminus\{e\})$, this is zero. Now taking the dot product with λ we have

$$-\left(\sum_j\frac{\dim(V_j)^3}{n_j}\right)\rho = \sum_j\frac{\dim(V_j)^2}{n_j}\lambda\cdot\overline{\chi_{V_j}} = \sum_j\frac{\dim(V_j)^2}{n_j}(n_j|G| - |\mathcal{C}|\dim(V_j))$$

which gives $|\mathcal{C}|-\rho = |G|^2/(\sum_j\dim(V_j)^3/n_j)$ and hence the formula for μ using Lemma 4·1. □

Example 4·7. *For the Roth property group S_3 the formula for μ above gives that $\mu = \frac{9}{19}$, which agrees with what we already computed in Example* 3·6 *(since $S_3 \cong D_6$) and can also easily be checked from Example* 4·4.

Theorem 4·6 characterises the Roth property groups among all finite groups in our Killing form approach. All nontrivial finite abelian groups are non-Roth and it is easy to see that $\mu = \frac{1}{N-1}$. The first non-Roth centreless nondegenerate group is the small group with label (400, 207) (cf [**1**]) of order 400 as mentioned in the introduction. The first finite simple nonabelian non-Roth group is $PSU(3,3)$, which is not nondegenerate but where $\mu = \frac{1}{N-1}$ still applies as can be checked. Also, an immediate consequence for the formula for μ is that for Roth property groups

$$\frac{1}{N} < \mu < \frac{1}{N-1}$$

as follows from the observation for all $j \neq 0$ that $0 < \dim(V_j),\ n_j < |G| - 1 = \sum_{j\neq 0} \dim(V_j)^2$. One can do better here, for example these observations actually imply $\mu < 1/(N-1+\frac{1}{(|G|-1)^2})$. In the case of D_{2n} with n odd using the results in Example 3·6 one finds $\mu \to \frac{1}{(N-1)}$ strictly from below as $n \to \infty$.

Going the other way, when the group is not Roth we can still say something about the Killing form.

PROPOSITION 4·8. *Let G be a finite group. K for the universal calculus is nondegenerate on the subspace of invariant vectors inside $\mathbb{C}.(G\setminus\{e\})$ iff the conjugation representation on $\mathbb{C}G$ is missing at most one irreducible representation.*

Proof. (i) Suppose G is missing two distinct irreducible representations, say V_1, V_2. In part (ii) of the proof of Theorem 4·6 we have $-\overline{\chi_{V_1}}/\dim(V_1)$ and now also $-\overline{\chi_{V_2}}/\dim(V_2)$ are in the preimage of λ. As the irreducible representations are non-equivalent their characters are linearly independent and hence K has a kernel, even when restricted to the subspace of invariant vectors.

(ii) We return to the formula (4·2) in vector form and suppose that $v = \sum_{i=1}^{n} v_i \overline{\chi_{V_i}}$ where we omit $\overline{\chi_{V_0}}$ and keep the rest as basis of the 'class vectors' $Z = (\mathbb{C}\mathcal{C})^{Ad}$ of vectors invariant under conjugation. We let $\delta = (\dim(V_i))$ be the vector of dimensions in this basis so $\delta_i = \dim(V_i)$ for $i = 1\cdots N-1$. Then $Kv = 0$ is equivalent to

$$(v\cdot\delta)\lambda = |G|\sum_i v_i \frac{n_i}{\delta_i}\chi_{V_i}$$

but $\lambda = \sum_{i=0}^{N-1} n_i\chi_{V_i} = \sum_{i=1}^{N-1}(n_i - n_0\delta_i)\chi_{V_i}$ so this is equivalent to

$$n_i(|G|v_i - \delta_i(v\cdot\delta)) + n_0\delta_i^2(v\cdot\delta) = 0, \quad \forall i = 1\cdots N-1.$$

Now if $n_1 = 0$ then $v\cdot\delta = 0$. Putting this information into the displayed equation with the assumption $n_i \neq 0$ for $i > 1$ gives $v_i = 0$ for $i > 1$. In this case $v\cdot\delta = 0$ tells us that $v_1 = 0$ as well, i.e. $v = 0$. Hence $K|_Z$ is nondegenerate, but could still be degenerate on all of $\mathbb{C}\mathcal{C}$. □

In summary, if no irreducible representations are missing in the conjugation representation then the group is nondegenerate. If two or more irreducible representations are missing then the group is not nondegenerate as the Killing form for the universal calculus is degenerate. As far as we know the case of one irreducible representation missing can go either way but if the group is nondegenerate but not Roth then it must have precisely one irreducible representation missing. Using the methods of [**20**] one can see that the group $PSU(3,4)$ is indeed missing exactly one irreducible representation and this is now proven [**10**] to hold for all finite simple nonabelian non-Roth groups. So the above proposition applies and we have the immediate corollary:

COROLLARY 4·9. *Let G be a finite simple nonabelian group. Then the Killing form for the universal calculus on G is nondegenerate on the subspace of conjugation-invariant vectors inside $\mathbb{C}.(G\setminus\{e\})$.*

5. *Nondegeneracy, eigenvalues and reducibility of the Killing form for conjugacy classes*

In this section we will be interested in $\mathcal{C}$ a conjugacy class but we start off more generally. Let G be a finite group and $\mathcal{C}\subseteq G\setminus\{e\}$ an ad-stable subset. Since we have a particular basis for $\mathcal{L} = \mathbb{C}\mathcal{C}$ we have already had occasion to regard this for convenience as an operator

$$K : \mathcal{L} \to \mathcal{L}, \quad K(a) = \sum_{b \in \mathcal{C}} K(a,b)b,$$

and we now look at its properties as such in more detail. Note that by construction this operator is ad-invariant and hence its eigenspaces provide a natural decomposition of $\mathbb{C}\mathcal{C}$ into subrepresentations. Nondegeneracy in this language means of course that K has no zero eigenvalues in its spectrum. As K is real and symmetric in our basis it can be diagonalised over $\mathbb{R}$. However, it can also be viewed as a hermitian matrix or self-adjoint operator over $\mathbb{C}$. Moreover, the entries of K are non-negative integers. We give some basic consequences of these properties here.

Proposition 5·1. *Suppose V is an irreducible representation of $\mathbb{C}G$ which is defined over $\mathbb{Q}$. So $V = V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$ for an irreducible representation $V_{\mathbb{Q}}$ of $\mathbb{Q}G$. Furthermore, suppose $\mathcal{C}$ is a conjugacy class in G such that V occurs in the conjugation representation $\mathbb{C}\mathcal{C}$.*

If the isotypical component of V in $\mathbb{C}\mathcal{C}$ is contained in a single eigenspace of the Killing matrix K of $\mathcal{C}$, then the corresponding eigenvalue lies in $\mathbb{Z}$.

Proof. Choose an element $x \in \mathcal{C}$ and consider the map

$$\pi : \mathbb{C}G \to \mathbb{C}\mathcal{C} : g \mapsto gxg^{-1}$$

which is a G-equivariant surjection from the left-regular representation to the conjugation representation of G. Let $A_V \subset \mathbb{C}G$ denote the block of the irreducible representation V. By block decomposition of $\mathbb{C}G$ and Schur's lemma it follows that π restricts to a surjection from A_V to the isotypical component of V in $\mathbb{C}\mathcal{C}$. However, since V was defined over $\mathbb{Q}$ it follows that A_V has a basis that lies inside $\mathbb{Q}G$. Moreover by surjectivity of $\pi|_{A_V}$ onto the isotypical component there exists such a basis element b whose image $\pi(b)$ is nonzero. By the assumptions, b is an eigenvector of the Killing matrix. Moreover b has rational coefficients as a vector in $\mathbb{C}\mathcal{C}$. Since the entries of K are integral and b is rational it follows that the eigenvalue of b lies in $\mathbb{Q}$. On the other hand the integrality of K implies that the eigenvalues are all algebraic integers. So the eigenvalue of b is a rational number and an algebraic integer. Therefore it must lie in $\mathbb{Z}$. □

Note that this proposition implies in particular, that if V is a complex representation of G defined over $\mathbb{Q}$ which occurs in $\mathbb{C}\mathcal{C}$ with multiplicity 1, then it lies in an eigenspace of K with eigenvalue in $\mathbb{Z}$. Since all representations of the symmetric group are defined over $\mathbb{Q}$ (over $\mathbb{Z}$ even), we have the following corollary.

Corollary 5·2. *Let $\mathcal{C}$ be a nontrivial conjugacy class of S_n. If an irreducible representation of S_n occurs in the conjugation representation $\mathbb{C}\mathcal{C}$ with multiplicity one, then it embeds into an eigenspace for the corresponding Killing form with eigenvalue in $\mathbb{Z}$.*

Note that an irreducible representation is rational if all its character values are rational. This is because the matrix entries can be obtained by projection via central idempotents in the group algebra with coefficients defined by the characters. Similarly the character determines whether an irreducible representation is complex in the sense of not real.

Proposition 5·3. *Let $\mathcal{C} \subseteq G \setminus \{e\}$ be an ad-stable subset.*

(1) *If a complex irreducible representation V occurs in $\mathbb{C}\mathcal{C}$ in an eigenspace of the associated Killing form matrix, then so does its dual representation (with complex conjugate character).*
(2) *If we consider the inverse conjugacy class $\mathcal{C}^{-1}$ then the eigenvalues of the Killing form matrix for $\mathcal{C}^{-1}$ are the same as the ones obtained for $\mathcal{C}$, and the decompositions of the respective eigenspaces into irreducible representations are equivalent.*

Proof. The conjugation representation is clearly defined over $\mathbb{R}$, and since K is real and symmetric in the basis $\mathcal{C}$ its eigenspaces are also defined over $\mathbb{R}$, hence real as subrepresentations of the conjugation representation. This implies the first part. For the second part we consider inversion as a bijection between the two ad-stable subsets. Let $a, b, c \in \mathcal{C}$. Clearly c commutes with ab precisely if c^{-1} commutes with $b^{-1}a^{-1}$. But as the Killing forms are symmetric, we see that the Killing forms have the same matrices in their respective bases. If $v \in \mathbb{C}\mathcal{C}$ is expanded in the basis $\mathcal{C}$ we define $\tilde{v}$ to be the corresponding vector in $\mathbb{C}\mathcal{C}^{-1}$ with the same coefficients in the corresponding basis, i.e. $v, \tilde{v}$ are represented by the same column vector in their respective bases. One may readily see that the matrices for the action of an element of g in the two cases are also identical. This implies the second part. □

By a slight abuse of notation, in the following we denote the element $\sum_{a\in\mathcal{C}} a$ by θ (its analogue as a left-invariant 1-form makes the calculus inner). Clearly θ spans a copy of the trivial representation in $\mathbb{C}\mathcal{C}$, and the unique copy if $\mathcal{C}$ is a conjugacy class. We also recall that a matrix with non-negative entries is called *irreducible* if for all indices i, j there exists $m \in \mathbb{N}$ such that the matrix entry $(K^m)_{ij} \neq 0$. This is equivalent to connectedness of the graph on the set of indices defined by an edge whenever the entry $K_{ij} \neq 0$.

PROPOSITION 5·4. *Let G be a finite group and $\mathcal{C} \subseteq G \setminus \{e\}$ a conjugacy class. Then K has a (positive) integral maximal eigenvalue λ_{max}, given by the sum of any column of K. Moreover, K splits onto r irreducible direct summands* if and only if *the eigenspace associated to λ_{max} has dimension r and in this case all other eigenspace dimensions are divisible by r. In particular, if K is irreducible then the eigenspace associated to λ_{max} is 1-dimensional, generated by the eigenvector $\theta = \sum_a a$.*

Proof. $K(\theta) = \sum_{a,b} K(a,b)b = \sum_b c_b b$ where c_b is the sum of the b'th column of the matrix of K. However, $c_{gbg^{-1}} = \sum_a K(a, gbg^{-1}) = \sum_a K(g^{-1}ag, b) = c_b$ after a change of variables. Hence c_b is independent of $b \in \mathcal{C}$ in the case of a conjugacy class. Hence θ is an eigenvector of K with eigenvalue the column sum. Moreover, if K is irreducible then by Perron-Frobenius theory there is a 1-dimensional maximal eigenspace with eigenvalue the column sum of K, i.e. with eigenvector θ. If K is not irreducible then after a reordering of the basis it can be presented as a direct sum. Iterating this, we reduce K to a direct sum of some number $r > 1$ of irreducible blocks. In fact each block will be, after reordering, a copy of the same irreducible matrix. This follows from ad-invariance of K as follows. Consider an element in G that conjugates a corner of the first block to the corresponding corner of another. All the indices relating to the first block belong to the same connected component of the graph and, by assumption, they are not connected to any of the indices for the other blocks, and this notion is ad-invariant, as K is. Hence the indices relating to the conjugated first block must be connected to themselves and not to the first block. Hence the first block maps over to the conjugated block, and all its entries are the same when suitably ordered, again by ad-invariance of K. Once K has been presented as r blocks K_i, its eigenvectors will consist of r parts forming eigenvectors for each block with the same eigenvalue. However, since these blocks are all irreducible and have the same row sum as K, they will each have the same maximal eigenvalue as K, and any other eigenvalues will be strictly lower. This implies the facts stated and justifies the notation λ_{max} for the column sum. Note that the diagonal of K is always nonzero as a commutes with a^2 for all $a \in \mathcal{C}$. Hence K^{m+1} can only have the same or more positive entries as K^m, so in our case irreducible is equivalent to the existence of $m \in \mathbb{N}$ such that all entries of K^m are positive, i.e. to primitivity of the matrix K. □

It appears for finite simple nonabelian groups up to the order 75,000 that we could check that K is always irreducible except for conjugacy classes $\mathcal{C}$ of involutions for certain groups $G = PSL(2, 2^k)$, $G = PSU(3, 2^k)$ or $G = Suz(2^{2k-1})$ for $k \geq 2$. These are the simple groups with the Bender property of possessing a strongly embedded subgroup. S_4 does have a noninvolutive reducible class (the 4-cycles) but for S_n, $n > 4$ we have checked by computer up to $n = 8$ that the conjugacy classes with reducible K are precisely the $\frac{n-1}{2}$-fold 2-cycles for n odd, hence involutive. In this case the maximal eigenvalue has eigenspace decomposition $1 \oplus (n-1)$, where $(n-1)$ means the standard representation.

Lemma 5·5. *Let G be a finite group and $\mathcal{C} \subseteq G \setminus \{e\}$ a conjugacy class. Then μ, ν, ρ in (3·2) are defined and*

$$\mu = \frac{d}{\lambda_{max}} = \frac{1}{\langle K \rangle}, \quad \nu = \chi\mu, \quad \rho = \chi^2\mu, \quad 0 < \lambda_{max} \leq d^2, \quad 1 \leq \chi \leq d$$

where $\langle K \rangle$ denotes the average entry of K, $d = |\mathcal{C}|$ and $\chi = \chi_{\mathcal{C}}(\mathcal{C})$ is the constant value of $\lambda^*(a)$ on $a \in \mathcal{C}$. The upper bound for λ_{max} holds iff K has all entries d.

Proof. By Proposition 5·4 we know that θ is in the image of K and that $\mu = \theta \cdot K^{-1}\theta = \frac{\theta\cdot\theta}{\lambda_{max}} = \frac{d}{\lambda_{max}}$. Since $\lambda = \chi\theta$ we then have ν, ρ as stated. Also since λ_{max} is the column sum of K it is clear that $\lambda_{max}/d = \langle K \rangle$. This is strictly positive since all entries are non-negative and $K(a, a) \geq 1$ for all $a \in \mathcal{C}$. The upper bound for λ_{max}/d is saturated when $\langle K \rangle = d$ which means every entry is d as this is also the maximum of any entry. □

The upper bound for χ is reached precisely when all elements of $\mathcal{C}$ mutually commute, which again implies that all entries of K are d, so apart from this case both upper bounds in the lemma are not reached. If the conjugacy class is real then $\lambda_{max} \geq d$ since for every $a \in \mathcal{C}$ there exists $b \in \mathcal{C}$ with $K(a, b) = d$. Meanwhile, $\chi \geq 2$ if the conjugacy class is real and not one of involutions.

As regards nondegeneracy, we know from computer verification that all finite simple nonabelian groups at least to order 75,000 and with real conjugacy classes have nondegenerate K. In another direction we have the following result:

Proposition 5·6. *Let $G_1, \mathcal{C}_1$ and $G_2, \mathcal{C}_2$ be two finite groups with nontrivial conjugacy classes and K_1, K_2 nondegenerate. Then $K_{\mathcal{C}_1 \sqcup \mathcal{C}_2}$ is nondegenerate if and only if*

$$(\chi_1 + \chi_2)^2 \neq (\langle K_1 \rangle + d_2)(\langle K_2 \rangle + d_1) \tag{5·1}$$

where $\chi_i = \chi_{\mathcal{C}_i}(\mathcal{C}_i)$ and $d_i = |\mathcal{C}_i|$. Sufficient conditions for this are any of

(1) $\chi_i < \langle K_i \rangle$, $i = 1, 2$
(2) $\langle K_1 \rangle \langle K_2 \rangle \notin \mathbb{Z}$
(3) $\max\{\chi_1, \chi_2\} \leq \min\{d_1, d_2\}$

(4) $\max\{\chi_1^2, \chi_2^2\} \leq \frac{d_1 d_2}{2}$

Proof. In the case of a conjugacy class the formula in Proposition 3·5 becomes

$$K_{\mathcal{C}_1 \sqcup \mathcal{C}_2} = \begin{pmatrix} K_1 & 0 \\ 0 & K_2 \end{pmatrix} + \begin{pmatrix} d_2 \theta_1^* \otimes \theta_1^* & (\chi_1 + \chi_2)\theta_1^* \otimes \theta_2^* \\ (\chi_1 + \chi_2)\theta_2^* \otimes \theta_1^* & d_1 \theta_2^* \otimes \theta_2^* \end{pmatrix}$$

as a bilinear form (similarly as a matrix). The formulae in Lemma 5·5 mean that the determinant condition reduces now to the one stated. The listed sufficient conditions are immediate. For (2) note that multiplying out the right hand side of the inequality (5·1) gives cross terms $\lambda_{max,i}$ which are integers. □

Here (1) has the merit of being properties of each group and conjugacy class separately and such groups and classes can be direct producted with the direct sum 'Lie algebra'. However, this is not effective for the simple groups in the Appendix. Rather, (4) provides the following.

COROLLARY 5·7. *At least for finite simple nonabelian groups up to order 75,000 i.e. with reference to the tables in the Appendix, their direct product with the disjoint union of real conjugacy classes gives a nondegenerate Killing form.*

Proof. We apply test (4) in Proposition 5·6. The largest value of $2\chi_{\mathcal{C}}(\mathcal{C})^2/|\mathcal{C}|$ in the tables is for the 2A class of A_8 at about 11.9, when $\chi_{\mathcal{C}}(\mathcal{C})$ is 25. This 11.9 is less than the smallest value of $|\mathcal{C}|$ anywhere else in the tables, as the smallest size of a conjugacy class happens for classes $5A$ and $5B$ in A_5, both with size 12. Any classes with $\chi_{\mathcal{C}}(\mathcal{C}) > 25$ so as to increase the left hand side have a much larger $|\mathcal{C}|$ so that (4) still holds. □

6. *The Killing form and conjugation representations for S_n*

Although Conjecture 1·2 and other points of discussion have been for simple groups, the symmetric groups are sufficiently close that we expect much of the discussion to apply to them as well. Our main result, Proposition 6·2, is for S_n with its 2-cycles class, namely an explicit decomposition of $\mathbb{C}\mathcal{C}$ into irreducible representations in a manner compatible with the eigenspace decomposition under K, and with explicit formulae for the eigenvalues. In particular, we show that the Killing form matrix K for this conjugacy class is nondegenerate. In this case it is necessarily positive definite by Proposition 3·4. At the other extreme we find the maximal eigenvalue λ_{max} for the n-cycles conjugacy class when n is an odd prime.

First we note that in the case of S_n for $n > 4$, with the 2-cycles conjugacy class, one can see from the formulae for the Killing form in [**15**] that K itself has all entries strictly positive. Hence Proposition 5·4 applies in this case and there is a unique maximal eigenvalue, with eigenspace spanned by θ. For S_3 and S_4, K is reducible, and θ is a maximal eigenvector but each eigenvalue has multiplicity 3.

We will need a concrete construction of irreducible subrepresentations inside a conjugation representation. For any partition $\mu = (\mu_1, \cdots, \mu_k)$ of n we have a corresponding conjugacy class $\mathcal{C}_\mu$ in S_n, namely the one with cycle type μ. Explicitly $\mathcal{C}_\mu$ is the conjugacy class containing the element

$$a_\mu = (1, \cdots, \mu_1)(\mu_1 + 1, \cdots, \mu_1 + \mu_2) \cdots (n - \mu_k + 1, \cdots, n).$$

If we let Z_{a_μ} denote the centraliser of a_μ and identify $S_n/Z_{a_\mu} \cong \mathcal{C}_\mu$ via $\sigma Z_{a_\mu} \mapsto \sigma a_\mu \sigma^{-1}$, then we obtain a S_n-equivariant homomorphism from the left regular representation to the conjugation representation,

$$\pi : \mathbb{C}S_n \longrightarrow \mathbb{C}(S_n/Z_{a_\mu}) \cong \mathbb{C}\mathcal{C}_\mu, \tag{6·1}$$

coming from the linear extension of the quotient map $S_n \to S_n/Z_{a_\mu}$. If we interpret $\mathbb{C}S_n$ as the group algebra, then the map π becomes the action of $\mathbb{C}S_n$ on the element $a_\mu \in \mathbb{C}\mathcal{C}_\mu$. The map π is surjective reflecting $\mathbb{C}\mathcal{C}_\mu$ being a cyclic $\mathbb{C}S_n$ module.

For the symmetric groups the irreducible representations are very well known [**5**, **22**, **6**], and we have a concrete decomposition of $\mathbb{C}S_n$ into irreducibles at our disposal. Namely, recall that irreducible representations S^λ of S_n are indexed by partitions $\lambda \vdash n$, and a partition is represented by its *Young diagram* or *shape*. Since S^λ occurs in $\mathbb{C}S_n$ with multiplicity equal to dim S^λ, the construction of a subrepresentation of $\mathbb{C}S_n$ isomorphic to S^λ for given λ must naturally depend on an additional choice, so choose a *tableau* of shape λ, a one-to-one labelling of the boxes by the integers $\{1, \cdots, n\}$. The symmetric group S_n acts on the set of tableaux by permuting the entries, and therefore a tableau T defines a subgroup $R(T)$ of permutations preserving the row sets, and a subgroup $C(T)$ of permutations preserving the column sets. The corresponding irreducible summand in $\mathbb{C}S_n$ is the submodule $S^T := \mathbb{C}S_n\, c_T$, which is generated by the 'Young symmetrizer' $c_T = b_T a_T$ of T, where

$$a_T = \sum_{\sigma \in R(T)} \sigma, \qquad b_T = \sum_{\sigma \in C(T)} \epsilon(\sigma)\sigma,$$

with $\epsilon(\sigma)$ the sign of the permutation σ.

Clearly the right action of S_n on $\mathbb{C}S_n$ provides S_n-equivariant isomorphisms between the modules S^T for varying T making them all equivalent. Note that there are many more tableaux than the multiplicity of S^λ. Let $SYT(\lambda)$ denote the set of *standard Young tableaux*, that is tableaux whose entries are strictly increasing in rows and in columns. Then the isotypic component of S^λ inside $\mathbb{C}S_n$ is precisely the subspace

$$\bigoplus_{T \in SYT(\lambda)} S^T.$$

It is now straightforward to find the irreducible summands of $\mathbb{C}\mathcal{C}_\mu$ using Young symmetrizers, as follows.

Lemma 6·1. *Suppose λ and μ are partitions of n and all notations are as above.*

The Specht module S^λ occurs as a subrepresentation of the conjugation representation $\mathbb{C}\mathcal{C}_\mu$ if and only if there exists a standard Young tableau T of shape λ for which $c_T \cdot a_\mu \neq 0$ in $\mathbb{C}\mathcal{C}_\mu$.

In that case, the subrepresentation is explicitly realized as the subspace $\pi(S^T)$, where π is the projection map from (6·1).

Proof. This is elementary. If there is a tableau T for which $c_T \cdot a_\mu \neq 0$, then the restriction of the map π from (6·1) to the subrepresentation S^T of $\mathbb{C}S_n$ defines a nonzero S_n-equivariant map $S^T \to \mathbb{C}\mathcal{C}_\mu$. Since S^T is irreducible and isomorphic to S^λ it follows that this map must be an isomorphism onto its image. On the other hand, if $c_T \cdot a_\mu = 0$ for all $T \in SYT(\lambda)$, then the entire block of S^λ in $\mathbb{C}S_n$ lies in the kernel of π, and therefore the irreducible representation S^λ does not occur in the image of π. Since π is surjective, this means that S^λ is not a subrepresentation of $\mathbb{C}\mathcal{C}_\mu$. □

6·1. *S_n with the 2-cycles class*

In the example of S_3, the 2-cycles class $\mathcal{C}_{(2,1)}$ has three elements and it is straightforward to see that the conjugation representation, $\mathbb{C}\mathcal{C}_{(2,1)}$, is the (defining) three-dimensional permutation representation of S_3. In terms of Specht modules this representation decomposes as

$$\mathbb{C}\mathcal{C}_{(2,1)} = S^{(3)} \oplus S^{(2,1)}. \tag{6·2}$$

That is, the trivial representation plus the standard 2-dimensional representation. The general case is not much different. We will use the notation $(2, 1^{n-2})$ for the partition $(2, 1, \overset{(n-2)}{\cdots}, 1)$ which represents the 2-cycles class in S_n.

Proposition 6·2. *Consider S_n for $n > 2$ with the 2-cycles class $\mathcal{C} = \mathcal{C}_{(2,1^{n-2})}$. For $n = 3$ the decomposition of $\mathbb{C}\mathcal{C}$ into irreducibles is given in equation (6·2).*

(1) *For $n > 3$ the decomposition of the conjugation representation $\mathbb{C}\mathcal{C}$ into irreducible representations is given by*

$$\mathbb{C}\mathcal{C} \cong S^{(n)} \oplus S^{(n-1,1)} \oplus S^{(n-2,2)}.$$

Here the first two Specht modules $S^{(n)}, S^{(n-1,1)}$ are the trivial representation and the standard $(n-1)$-dimensional representation, respectively.

(2) *Each irreducible submodule of $\mathbb{C}\mathcal{C}$ lies in an eigenspace for the Killing form matrix K with eigenvalues as follows. The eigenvalue of K for the eigenspace containing $S^{(n)}$ (spanned by the element θ) is*

$$\frac{1}{4}(n^4 - 10n^3 + 41n^2 - 72n + 48).$$

The eigenvalue of K in the eigenspace containing $S^{(n-1,1)}$ is

$$n^2 - 6n + 12.$$

Suppose $n > 3$. Then the eigenvalue of K on the eigenspace containing $S^{(n-2,2)}$ is $2n$.

Proof. Part (1) is immediate using character theory. But we will rather define explicit embeddings of the Specht modules, by the method of Lemma 6·1, in order to be able to compute the eigenvalues of K in the later parts of the proof.

Of course the trivial representation embeds into $\mathbb{C}\mathcal{C}_{(2,1^{n-2})}$ as the subspace spanned by the element $\theta = \sum_{a \in \mathcal{C}} a$, and has multiplicity 1.

For the standard representation $S^{(n-1,1)}$ we consider the subspace $\pi(S^{T_1})$ of $\mathbb{C}\mathcal{C}_{(2,1^{n-2})}$ for π from (6·1) corresponding to the tableau

$$T_1 = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & \cdots & n-1 \\ \hline n \\ \cline{1-1} \end{array}$$

This is the submodule of $\mathbb{C}\mathcal{C}$ obtained by applying $\mathbb{C}S_n$ to the vector $c_{T_1} \cdot (12)$. Up to an overall multiple, which we drop, this vector works out to be

$$v_{T_1} = (12) + (13) + \cdots + (1, n-1) - (2, n) - (3, n) - \cdots - (n-1, n).$$

Since $v_{T_1} \neq 0$ we have found a copy of $S^{(n-1,1)}$ in $\mathbb{C}\mathcal{C}$.

For the next representation $S^{(n-2,2)}$ we consider the subspace $\pi(S^{T_2})$ of $\mathbb{C}\mathcal{C}$ for π from

(6·1) and the tableau

$$T_2 = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & \cdots & n-2 \\ \hline n-1 & n \\ \cline{1-2}\end{array}$$

This is the submodule of $\mathbb{C}\mathcal{C}$ obtained by applying $\mathbb{C}S_n$ to the vector $c_{T_2} \cdot (12)$. Up to an overall multiple this vector works out to be

$$v_{T_2} = (12) - (2, n-1) - (1, n) + (n-1, n),$$

and since $v_{T_2} \neq 0$ we have found a copy of $S^{(n-2,2)}$ in $\mathbb{C}\mathcal{C}$.

That we have thereby completely decomposed $\mathbb{C}\mathcal{C}$ follows by dimension count:

$$\dim S^{(n)} + \dim S^{(n-1,1)} + \dim S^{(n-2,2)} = 1 + (n-1) + \frac{n(n-3)}{2} = \binom{n}{2} = \dim \mathbb{C}\mathcal{C},$$

where $\dim (S^{(n-2,2)})$ is computed for example by the hook formula. This concludes the proof of (1).

That the irreducible subrepresentations lie in eigenspaces of K follows immediately from the fact that in the decomposition of $\mathbb{C}\mathcal{C}$ each irreducible representation occurs with multiplicity at most one. We can now compute the eigenvalues.

For the trivial representation we compute the column sum $\sum_a K((12), a)$ over all 2-cycles. In the basis of the 'triangular' listing

$$\begin{array}{c} (12) \\ (13), (23) \\ (14), (24), (34) \\ (15), (25), (35), (45) \\ \vdots \quad \vdots \\ (1n), (2n), (3n), (4n), \cdots, (n-1, n) \end{array}$$

we have for a the choice (12), or a lies in the size $2(n-3)$ region on the left where a has one entry in common with (12), or a lies in the triangle to the right of size $(n-2)(n-3)/2$ where a is disjoint from (12). Using the values of K for these three cases in [**15**], we find

$$\binom{n}{2} + 2(n-2)\binom{n-3}{2} + \frac{(n-2)(n-3)}{2}\left(\binom{n-4}{2} + 2\right)$$

which computes as stated.

For the standard representation we use the vector we constructed in the proof of (1),

$$v_{T_1} = (12) + (13) + \cdots + (1, n-1) - (2, n) - (3, n) - \cdots - (n-1, n),$$

which involves the left and bottom slopes of the triangle leaving out the common vertex. Then the eigenvalue computed as the coefficient of (12) in $K(v_{T_1})$ is

$$K((12),(12)) + (n-3)K((12),(13)) - K((12),(2,n)) - (n-3)K((12),(3,n))$$

$$= \binom{n}{2} + (n-4)\binom{n-3}{2} + (n-3)\left(\binom{n-4}{2} + 2\right)$$

which comes out as stated. Both formulae, although computed for $n > 4$ in the above counting, also give the right answer for $n = 2, 3, 4$, as computed by hand.

For the representation $S^{(n-2,2)}$ we use the vector

$$v_{T_2} = (12) - (2, n-1) - (1, n) + (n-1, n)$$

from the proof of (1) and compute the eigenvalue as the (12) coefficient of $K(v_{T_2})$, i.e. as

$$K((12),(12)) - K((12),(2,n-1)) - K((12),(1,n)) + K((12),(n-1,n))$$

$$= \binom{n}{2} - 2\binom{n-3}{2} + \binom{n-4}{2} + 2 = 2n.$$

□

COROLLARY 6·3. *The Killing form for S_n, $n > 2$ with the 2-cycles conjugacy class $\mathcal{C}$ is non-degenerate and in fact positive definite. Moreover the decomposition of $\mathbb{C}\mathcal{C}$ into irreducible representations consisting of the trivial and the standard representation, and the representation $S^{(n-2,2)}$, coincides for $n > 6$ with the decomposition of K into eigenspaces of respectively the maximal, next to maximal and smallest eigenvalues.*

Proof. Looking at the three expressions for the eigenvalues in the lemmas above it is evident that they have different leading powers of n and hence are distinct for all n bigger than some value. By inspection, the only degeneracies are $n = 3$ when the trivial and the standard representation have the same eigenvalue of K, $n = 4$ when the eigenvalues of the trivial and the $S^{(n-2,2)}$ coincide, being smaller than the eigenvalue of the standard representation, and $n = 6$ when the eigenvalues of the standard representation and of $S^{(n-2,2)}$ coincide. After that, the eigenvalue of the trivial exceeds that of the standard representation which exceeds that of $S^{(n-2,2)}$ as stated. As all the eigenvalues are positive we conclude that K is non-degenerate (and positive definite when extended as a hermitian inner product). □

6·2. *S_n with the n-cycles class*

In this section $\mathcal{C}$ is the class of n-cycles and our first result is a formula for the eigenvalue λ_{max} of the Killing form, with eigenspace the trivial representation in $\mathbb{C}\mathcal{C}$ for n prime, using a result of Zagier[**27**].

PROPOSITION 6·4. *Let n be an odd prime. The maximal eigenvalue of the Killing form matrix on S_n with its n-cycles class is $\lambda_{max} = \frac{(n-1)!}{n+1}(3n-1)$.*

Proof. Suppose a and b are n-cycles for which the product ab is an n-cycle. The centraliser of ab consists in this case of all the powers of ab. Since n is prime, these powers are all n-cycles except for the n-th power which is e. So in this case $K_{a,b} = |Z(ab) \cap \mathcal{C}| = n-1$. If ab is not an n-cycle or the identity, it cannot commute with an n-cycle, and hence $K_{a,b} = 0$ in that case. Finally in the case where $ab = e$ we have $K_{a,b} = |\mathcal{C}| = (n-1)!$. By a result of Zagier's, [**27**], it is known that for each fixed n-cycle a, there are $\frac{2(n-1)!}{n+1}$ many n-cycles b such that ab is again an n-cycle. Hence the eigenvalue λ_{max} which is the row sum of K is $\frac{2(n-1)!}{n+1}(n-1) + (n-1)!$. This simplifies to the formula in the proposition. □

Next we look at the sign representation. As a small digression we first establish precisely which conjugacy class this occurs in. In particular it occurs in the n-cycles class precisely when n is odd, leading us to conjecture a generalisation of Proposition 6·4, see (6·3).

Recall that the overall multiplicity of the sign representation in the conjugation representation $\mathbb{C}S_n$ is easily found by character theory as precisely the number of conjugacy classes consisting of even permutations minus the number of conjugacy classes of odd permutations (the row sum in the character table, for the sign representation). If $s(n)$ denotes the multiplicity of the sign representation in $\mathbb{C}S_n$, then the above description of $s(n)$ implies the product formula

$$1 + t + \sum_{n=2}^{\infty} s(n)t^n = \prod_{k=1}^{\infty} \left(\frac{1}{1 + (-t)^k} \right).$$

By a classical Euler identity which reads (after replacing the usual variable by $-t$ and inverting),

$$\prod_{k=1}^{\infty} \left(\frac{1}{1 + (-t)^k} \right) = \prod_{k=1}^{\infty} (1 + t^{2k-1}),$$

it follows that the multiplicity of the sign representation in the conjugation representation $\mathbb{C}S_n$ is equal to the number of partitions of n into distinct odd parts. The following is surely also known but we have not found a reference and include it here.

Proposition 6·5. *The sign representation ϵ of S_n appears as a subrepresentation of the conjugation representation $\mathbb{C}\mathcal{C}_\mu$ if and only if μ is a partition of n into distinct odd parts. If it appears in $\mathbb{C}\mathcal{C}_\mu$, then it has multiplicity one.*

Proof. Since the sign representation has multiplicity one in in the left-regular representation $\mathbb{C}S_n$ and the conjugation representation $\mathbb{C}\mathcal{C}_\mu$ is a cyclic $\mathbb{C}S_n$-module, it is clear that the sign representation can have multiplicity at most 1 in $\mathbb{C}\mathcal{C}_\mu$.

Let us now write $\sigma \cdot \sigma' = \sigma\sigma'\sigma^{-1}$ for the conjugation action. Fix an element a_μ in the conjugacy class $\mathcal{C}_\mu$. By Lemma 6·1, the sign representation appears in $\mathbb{C}\mathcal{C}_\mu$ if and only if the element

$$v_\mu = \sum_\sigma \epsilon(\sigma)\sigma \cdot a_\mu$$

in $\mathbb{C}\mathcal{C}_\mu$ is nonzero. Moreover if it is nonzero then it spans the sign representation. Now suppose v_μ is nonzero and let τ be an element of the centraliser Z_{a_μ}. Then we see that

$$\tau \cdot v_\mu = \sum_\sigma \epsilon(\sigma)(\tau\sigma\tau^{-1})\tau \cdot a_\mu = \sum_\sigma \epsilon(\sigma)\tau\sigma\tau^{-1} \cdot a_\mu = v_\mu.$$

This implies that τ is even, since v_μ spans the sign representation. Therefore if the sign representation occurs in $\mathbb{C}\mathcal{C}_\mu$ then Z_{a_μ} contains only even permutations.

The converse is true as well. If all elements in Z_μ are even, then the coefficient of a_μ in v_μ comes out to be $|Z_\mu|$, implying that v_μ is nonzero, and the sign representation occurs in $\mathbb{C}C_\mu$.

It remains to prove that Z_{a_μ} contains only even permutations, precisely if μ is a permutation of n into distinct odd parts.

Clearly, if μ has an even part then there is a cycle of even length in a_μ, which gives an element of the centralizer that has odd parity. Also if μ has two parts of size k (we may assume k odd, by above), then there is an element of the centralizer which exchanges the corresponding two k-cycles of a_μ, which is a product of k many 2-cycles. So again there is an element of odd parity in Z_{a_μ}. This shows that for the sign representation to occur inside $\mathbb{C}\mathcal{C}_\mu$, we must have that μ is a partition of n into distinct, odd parts.

Conversely, if μ is a partition of n into distinct odd parts, then the centraliser is generated by the individual cycles in a_μ, and these are all even permutations. □

Remark 6·6. *Another well-known partition identity gains a representation-theoretic interpretation in this context. Namely the block decomposition of $\mathbb{C}S_n$ is also invariant under the conjugation representation, and it is easy to check using character theory that the sign representation occurs, and with multiplicity one, precisely in the blocks of Specht modules corresponding to transpose-symmetric partitions. This gives another explanation of the fact that the number of transpose-symmetric partitions of n agrees with the number of partitions of n into distinct odd parts (a fact which has an easy, not obviously related bijective proof* [**25**]*) .*

Proposition 6·5 implies, as mentioned before, that the sign representation occurs in the class of n-cycles iff n is odd. In this case we define the parity $\pi(a)$ of $a \in \mathcal{C}$ to be $\pi(a) = \epsilon(\sigma)$ where σ is any permutation for which $\sigma a_\mu \sigma^{-1} = a$. Here π is well-defined as any permutation that commutes with an n-cycle has to be a power of an n-cycle and hence even, as n is odd. In this case we let

$$\delta_n = \#\{a \in \mathcal{C} \mid a_\mu a \in \mathcal{C},\ \pi(a) = 1\} - \#\{a \in \mathcal{C} \mid a_\mu a \in \mathcal{C},\ \pi(a) = -1\}$$

where $a_\mu = (1, \cdots, n)$. This δ_n is a signed version of our previous $\#\{a \in \mathcal{C} \mid a_\mu a \in \mathcal{C}\}$ in proof of Proposition 6·4.

LEMMA 6·7. *Let $\mathcal{C}$ be the class of n-cycles in S_n with n an odd prime. The eigenvalue of K on the eigenspace in $\mathbb{C}\mathcal{C}$ containing the sign representation is given by*

$$\lambda_{sign} = \delta_n\,(n-1) + (-1)^{\binom{n}{2}}(n-1)!.$$

Proof. The vector

$$v = \frac{1}{n}\sum_{\sigma \in S_n} \epsilon(\sigma)\sigma a_\mu \sigma^{-1} = \sum_{b \in \mathcal{C}} \pi(b) b,$$

spans the sign representation, and contains a_μ with coefficient 1. Applying K gives

$$K\left(\sum_{b\in\mathcal{C}} \pi(b) b\right) = \sum_{a,b\in\mathcal{C}} \pi(b)|Z(ab)\cap\mathcal{C}|a,$$

and the desired eigenvalue is the new coefficient of a_μ,

$$\lambda_{sign} = \sum_{b\in\mathcal{C}} \pi(b)|Z(a_\mu b)\cap\mathcal{C}|.$$

Since n is prime, as in the proof of Proposition 6·4, an n-cycle can lie in $Z(a_\mu b)$ only if either $a_\mu b$ is itself an n-cycle, or if $a_\mu b = e$. Moreover, the cardinality $|Z(ab)\cap\mathcal{C}|$ is $(n-1)$ in the first case, respectively $(n-1)!$ in the second case. If follows that

$$\lambda_{sign} = \delta_n\,(n-1) + \pi(a_\mu^{-1})\,(n-1)!.$$

Clearly $\pi(a_\mu^{-1})$ is the sign of the longest permutation, which is $(-1)^{\binom{n}{2}}$ and the formula follows. □

Finding the δ_n would seem to require a refinement of Zagier's formula [**27**] for $\#\{a \in \mathcal{C} \mid a_\mu a \in \mathcal{C}\}$ into a sum of 'odd and even' parts. We conjecture for all odd n that

$$\delta_n = (\frac{n-1}{2})!^2, \tag{6·3}$$

which we have verified for all odd $n \leq 9$. This would imply for n an odd prime that

$$\lambda_{sign} = (\frac{n-1}{2})!^2(n-1) + (-1)^{\frac{n-1}{2}}(n-1)!.$$

Appendix A. Computer verifications for simple groups

To provide evidence for our conjectures and get a grip on the behaviour of the Killing forms associated to minimal calculi for finite simple groups we have performed an extensive amount of computational verifications using the open source computer algebra systems Sage and GAP. Code is available from the authors upon request. In the present section we summarize our methods and results. Naming of the conjugacy classes follows the convention in the Atlas of finite simple groups [**3**].

A·1. *Effective calculation of the Killing form*

To compute the Killing form K associated to a conjugacy class $\mathcal{C} = g^G$ we take advantage of the ad-invariance $K(aga^{-1}, h) = K(g, a^{-1}ha)$ by computing a section $s : \mathcal{C} \to G$ satisfying $h = s(h)gs(h)^{-1}$ for all $h \in \mathcal{C}$, and using $K_{ab} = \lambda_g^*(s(a)^{-1}bs(a))$, where $\lambda_g^*(h) := \lambda^*(gh) = |Z(gh) \cap \mathcal{C}|$. This reduces the computation of the Killing form to computing its first row and the permutations that create the remaining rows from that one. Current limiting factor of the implementation is computer memory.

A·2. *Nondegeneracy*

Most of the simple groups are nondegenerate because they are Roth. The only non-Roth groups up to order 75000 are (cf. [**9**]) $PSU(3,3)$ and $PSU(3,4)$. Direct computation shows that $PSU(3,3)$ is **not** nondegenerate, while $PSU(3,4)$ is beyond our reach.

Nondegeneracy of the Killing forms for conjugacy classes is checked directly by computing its rank. Up to order 75,000 the Killing form is nondegenerate in all cases except conjugacy classes 7A and 7B of elements of order 7 in the alternating group A_7, conjugacy classes 4A, 4B, 8A, 8B, 12A, 12B of elements of orders 4, 8 or 12 in the unitary group $PSU(3,3) = G_2(2)'$, and conjugacy classes 7A and 7B of elements of order 7 in $PSL(3,4)$. All the degenerate cases occur in conjugacy classes that are not closed under inversion, with *real* conjugacy classes yielding nondegenerate Killing forms.

A·3. *Irreducibility*

The irreducibility of K is tested by checking connectedness of the graph G_K with vertices indexed by elements of $\mathcal{C}$ and containing an edge (a,b) if and only if $K_{a,b} \neq 0$.

Generically, the tested Killing forms are irreducible, so the Perron-Frobenius theorem applies and the eigenspace associated to the maximal eigenvalue is 1-dimensional; the only observed exceptions are given by the conjugacy classes of involutions in the linear groups $PSL(2,4) = A_5$, $PSL(2,8)$, $PSL(2,16)$, $PSL(2,32)$, the exceptional Suzuki group $Suz(8)$ and the unitary group $PSU(3,4)$. These are precisely the simple Bender groups to the order examined.

A·4. *Eigenspaces and irreducible decompositions*

The computation of the characteristic polynomial and the eigenvalues gets very slow as the size of the conjugacy classes increase. Eigenvalues (with multiplicity) have been computed for all the listed groups, revealing that the Killing form appears to be positive definite whenever it comes from a conjugacy class consisting of involutions plus the (non real) classes 3A and 3B of elements of order 3 and centralizer of size 648 in the unitary group $PSU(4,2)$. The link between involutions and positive definite Killing forms is made clear for the nondegenerate case in Proposition 3·4, with the data showing that neither nondegeneracy nor being closed under inversion can be relaxed.

We have also computed the decomposition into irreducible representations of the adjoint representation on $\mathbb{C}\mathcal{C}$ by means of character theory, looking for some correlation between the two decompositions. The observed behaviour is that as the groups become larger, the dimensions of the eigenspaces coincide with the dimensions of irreducible representations and we expect that each eigenspace contains exactly one irreducible representation. The obvious exceptions to this pattern are the few conjugacy classes yielding reducible Killing forms mentioned in the previous paragraph.

A·5. *Data:*

We summarize some of the obtained data for all finite simple groups up to order 75,000. We list whether a conjugacy class is real, reducibility of the Killing form, and its signature. Naming of the conjugacy classes follows the Atlas, and conjugacy classes of elements with the same centralizer sizes have been amalgamated whenever they show identical behaviour. Listing the actual eigenspace decomposition of the adjoint representation on $\mathbb{C}\mathcal{C}$ would be too lengthy so we shall omit that data here. Whenever the Killing form is reducible we have included in the corresponding column the number of irreducible components. Signature is expressed as (p,n,z) where p, n and z are respectively the number (counted with multiplicities) of positive, negative and zero eigenvalues; in particular, nondegeneracy is given by zero as the last number of this triple. In supplementary information we list the maximal eigenvalue λ_{max} of the Killing form, equal to the row sum. For a real conjugacy class $(\lambda_{max} - |\mathcal{C}|)/|\mathcal{C}|$ is a measure of the typical size of the other entries of the Killing form matrix after the principal entry $|\mathcal{C}|$ in each row. We also list the value $\chi_{\mathcal{C}}(\mathcal{C})$ of the character of the adjoint representation on a typical element of $\mathcal{C}$ as a measure of the degree to which the braided Lie algebra is nonabelian. It counts the number of elements in $\mathcal{C}$ that commute with any given element of $\mathcal{C}$. Note that the last three columns refer to the Killing form.

A_5, order 60

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	15	3	True	False (5)	21	(15, 0, 0)
$3A$	20	2	True	True	34	(10, 10, 0)
$5A-B$	12	2	True	True	24	(6, 6, 0)

$PSL(2,7)$, order 168

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	21	5	True	True	49	(21, 0, 0)
$3A$	56	2	True	True	94	(28, 28, 0)
$4A$	42	2	True	True	76	(21, 21, 0)
$8A-B$	24	3	False	True	30	(16, 8, 0)

A_6, order 360

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	45	5	True	True	73	(45, 0, 0)
$3A-B$	40	4	True	True	88	(20, 20, 0)
$4A$	90	2	True	True	156	(45, 45, 0)
$5A-B$	72	2	True	True	134	(36, 36, 0)

$PSL(2,8)$, order 504

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	63	7	True	False (9)	105	(63, 0, 0)
$3A$	56	2	True	True	112	(28, 28, 0)
$7A-C$	72	2	True	True	130	(36, 36, 0)
$9A-C$	56	2	True	True	112	(28, 28, 0)

$PSL(2,11)$, order 660

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	55	7	True	True	121	(55, 0, 0)
$3A$	110	2	True	True	208	(55, 55, 0)
$5A-B$	132	2	True	True	234	(66, 66, 0)
$6A$	110	2	True	True	208	(55, 55, 0)
$11A-B$	60	5	False	True	80	(36, 24, 0)

$PSL(2,13)$, order 1092

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	91	7	True	True	157	(91, 0, 0)
$3A$	182	2	True	True	328	(91, 91, 0)
$6A$	182	2	True	True	328	(91, 91, 0)
$7A-C$	156	2	True	True	298	(78, 78, 0)
$13A-B$	84	6	True	True	192	(42, 42, 0)

$PSL(2,17)$, order 2448

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	153	9	True	True	273	(153, 0, 0)
$3A$	272	2	True	True	526	(136, 136, 0)
$4A$	306	2	True	True	564	(153, 153, 0)
$8A-B$	306	2	True	True	564	(153, 153, 0)
$9A-C$	272	2	True	True	526	(136, 136, 0)
$17A-B$	144	8	True	True	336	(72, 72, 0)

A_7, order 2520

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	105	9	True	True	273	(105, 0, 0)
$3A$	70	10	True	True	256	(35, 35, 0)
$3B$	280	4	True	True	616	(140, 140, 0)
$4A$	630	2	True	True	1068	(315, 315, 0)
$5A$	504	4	True	True	936	(252, 252, 0)
$6A$	210	6	True	True	528	(105, 105, 0)
$7A-B$	360	3	False	True	324	(171, 140, 49)

$PSL(2,19)$, order 3420

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	171	11	True	True	361	(171, 0, 0)
$3A$	380	2	True	True	706	(190, 190, 0)
$5A-B$	342	2	True	True	664	(171, 171, 0)
$9A-C$	380	2	True	True	664	(190, 190, 0)
$10A-B$	342	2	True	True	706	(171, 171, 0)
$19A-B$	180	9	False	True	252	(100, 80, 0)

$PSL(2,16)$, order 4080

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	255	15	True	False (17)	465	(255, 0, 0)
$3A$	272	2	True	True	514	(136, 136, 0)
$5A-B$	272	2	True	True	514	(136, 136, 0)
$15A-D$	272	2	True	True	514	(136, 136, 0)
$17A-H$	240	2	True	True	480	(120, 120, 0)

$PSL(3,3)$, order 5616

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	117	13	True	True	489	(117, 0, 0)
$3A$	104	14	True	True	412	(52, 52, 0)
$3B$	624	6	True	True	1224	(312, 312, 0)
$4A$	702	2	True	True	1356	(351, 351, 0)
$6A$	936	2	True	True	1848	(468, 468, 0)
$8A-B$	702	2	False	True	600	(337, 365, 0)
$13A-B$	432	3	False	True	399	(224, 208, 0)
$13C-D$	432	3	False	True	399	(236, 196, 0)

$PSU(3,3) \cong G_2^{2'}$, order 6048

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	63	7	True	True	177	(63, 0, 0)
$3A$	56	2	True	True	112	(28, 28, 0)
$3B$	672	6	True	True	1332	(336, 336, 0)
$4A-B$	63	7	False	True	105	(22, 14, 27)
$4C$	378	6	True	True	852	(189, 189, 0)
$6A$	504	2	True	True	1104	(252, 252, 0)
$7A-B$	864	3	False	True	555	(436, 428, 0)
$8A-B$	756	2	False	True	752	(364, 365, 27)
$12A-B$	504	2	False	True	480	(238, 224, 42)

$PSL(2,23)$, order 6072

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	253	13	True	True	529	(253, 0, 0)
$3A$	506	2	True	True	988	(253, 253, 0)
$4A$	506	2	True	True	988	(253, 253, 0)
$6A$	506	2	True	True	988	(253, 253, 0)
$11A-E$	552	2	True	True	1038	(276, 276, 0)
$12A-B$	506	2	True	True	988	(253, 253, 0)
$23A-B$	264	11	False	True	374	(144, 120, 0)

$PSL(2,25)$, order 7800

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	325	13	True	True	601	(325, 0, 0)
$3A$	650	2	True	True	1228	(325, 325, 0)
$4A$	650	2	True	True	1228	(325, 325, 0)
$5A-B$	312	12	True	True	744	(156, 156, 0)
$6A$	650	2	True	True	1228	(325, 325, 0)
$12A-B$	650	2	True	True	1228	(325, 325, 0)
$13A-F$	600	2	True	True	1174	(300, 300, 0)

M_{11}, order 7920

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	165	13	True	True	489	(165, 0, 0)
$3A$	440	8	True	True	946	(220, 220, 0)
$4A$	990	2	True	True	2108	(495, 495, 0)
$5A$	1584	4	True	True	3096	(792, 792, 0)
$6A$	1320	2	True	True	2568	(660, 660, 0)
$8A-B$	990	2	False	True	920	(515, 475, 0)
$11A-B$	720	5	False	True	575	(355, 365, 0)

$PSL(2,27)$, order 9828

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	351	15	True	True	729	(351, 0, 0)
$3A-B$	364	13	False	True	520	(196, 168, 0)
$7A-C$	702	2	True	True	1376	(351, 351, 0)
$13A-F$	756	2	True	True	1434	(378, 378, 0)
$14A-C$	702	2	True	True	1376	(351, 351, 0)

$PSL(2,29)$, order 12180

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	435	15	True	True	813	(435, 0, 0)
$3A$	812	2	True	True	1594	(406, 406, 0)
$5A-B$	812	2	True	True	1594	(406, 406, 0)
$7A-C$	870	2	True	True	1656	(435, 435, 0)
$14A-C$	870	2	True	True	1656	(435, 435, 0)
$15A-D$	812	2	True	True	1594	(406, 406, 0)
$29A-B$	420	14	True	True	1008	(210, 210, 0)

$PSL(2,31)$, order 14880

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	465	17	True	True	961	(465, 0, 0)
$3A$	992	2	True	True	1894	(496, 496, 0)
$4A$	930	2	True	True	1828	(465, 465, 0)
$5A-B$	992	2	True	True	1894	(496, 496, 0)
$8A$	930	2	True	True	1828	(465, 465, 0)
$15A-D$	992	2	True	True	1894	(496, 496, 0)
$16A-E$	930	2	True	True	1828	(465, 465, 0)
$31A-B$	480	15	False	True	690	(256, 224, 0)

A_8, order 20160

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	105	25	True	True	849	(105, 0, 0)
$2B$	210	18	True	True	996	(210, 0, 0)
$3A$	112	22	True	True	784	(56, 56, 0)
$3B$	1120	4	True	True	3028	(560, 560, 0)
$4A$	1260	8	True	True	3280	(630, 630, 0)
$4B$	2520	4	True	True	4736	(1260, 1260, 0)
$5A$	1344	4	True	True	2996	(672, 672, 0)
$6A$	1680	6	True	True	3600	(840, 840, 0)
$6B$	3360	2	True	True	6168	(1680, 1680, 0)
$7A-B$	2880	3	False	True	2466	(1375, 1505, 0)
$15A-B$	1344	4	False	True	1556	(597, 747, 0)

$PSL(3,4)$, order 20160

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	315	27	True	True	1305	(315, 0, 0)
$3A$	2240	8	True	True	4888	(1120, 1120, 0)
$4A-C$	1260	12	True	True	3312	(630, 630, 0)
$5A-B$	4032	2	True	True	7284	(2016, 2016, 0)
$7A-B$	2880	3	False	True	2466	(1398, 1302, 180)

$PSL(2,37)$, order 25308

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	703	19	True	True	1333	(703, 0, 0)
$3A$	1406	2	True	True	2704	(703, 703, 0)
$6A$	1406	2	True	True	2704	(703, 703, 0)
$9A-C$	1406	2	True	True	2704	(703, 703, 0)
$18A-C$	1406	2	True	True	2704	(703, 703, 0)
$19A-I$	1332	2	True	True	2626	(666, 666, 0)
$37A-B$	684	18	True	True	1656	(342, 342, 0)

$PSU(4,2)$, order 25920

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	45	13	True	True	201	(45, 0, 0)
$2B$	270	22	True	True	1188	(270, 0, 0)
$3A-B$	40	13	False	True	196	(40, 0, 0)
$3C$	240	6	True	True	720	(120, 120, 0)
$3D$	480	12	True	True	1548	(240, 240, 0)
$4A$	540	8	True	True	1488	(270, 270, 0)
$4B$	3240	4	True	True	5440	(1620, 1620, 0)
$5A$	5184	4	True	True	9836	(2592, 2592, 0)
$6A-B$	360	5	False	True	708	(231, 129, 0)
$6C-D$	720	4	False	True	1272	(364, 356, 0)
$6E$	1440	2	True	True	3336	(720, 720, 0)
$6F$	2160	2	True	True	4176	(1080, 1080, 0)
$9A-B$	2880	3	False	True	2646	(1595, 1285, 0)
$12A-B$	2160	2	False	True	1824	(1035, 1125, 0)

Suz_8, order 29120

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	455	7	True	False (65)	497	(455, 0, 0)
$4A-B$	1820	4	False	True	2768	(755, 1065, 0)
$5A$	5824	4	True	True	9796	(2912, 2912, 0)
$7A-C$	4160	2	True	True	7690	(2080, 2080, 0)
$13A-C$	2240	4	True	True	4748	(1120, 1120, 0)

$PSL(2,32)$, order 32736

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	1023	31	True	False (33)	1953	(1023, 0, 0)
$3A$	992	2	True	True	1984	(496, 496, 0)
$11A-E$	992	2	True	True	1984	(496, 496, 0)
$31A-O$	1056	2	True	True	2050	(528, 528, 0)
$33A-J$	992	2	True	True	1984	(496, 496, 0)

$PSL(2,41)$, order 34440

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	861	21	True	True	1641	(861, 0, 0)
$3A$	1640	2	True	True	3238	(820, 820, 0)
$4A$	1722	2	True	True	3324	(861, 861, 0)
$5A-B$	1722	2	True	True	3324	(861, 861, 0)
$7A-C$	1640	2	True	True	3238	(820, 820, 0)
$10A-B$	1722	2	True	True	3324	(861, 861, 0)
$20A-D$	1722	2	True	True	3324	(861, 861, 0)
$21A-F$	1640	2	True	True	3238	(820, 820, 0)
$41A-B$	840	20	True	True	2040	(420, 420, 0)

$PSL(2,43)$, order 39732

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	903	23	True	True	1849	(903, 0, 0)
$3A$	1892	2	True	True	3658	(946, 946, 0)
$7A-C$	1892	2	True	True	3658	(946, 946, 0)
$11A-E$	1806	2	True	True	3568	(903, 903, 0)
$21A-F$	1892	2	True	True	3658	(946, 946, 0)
$22A-E$	1806	2	True	True	3568	(903, 903, 0)
$43A-B$	924	21	False	True	1344	(484, 440, 0)

$PSL(2,47)$, order 51888

$\mathcal{C}$	$\|\mathcal{C}\|$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	1081	25	True	True	2209	(1081, 0, 0)
$3A$	2162	2	True	True	4276	(1081, 1081, 0)
$4A$	2162	2	True	True	4276	(1081, 1081, 0)
$6A$	2162	2	True	True	4276	(1081, 1081, 0)
$8A-B$	2162	2	True	True	4276	(1081, 1081, 0)
$12A-B$	2162	2	True	True	4276	(1081, 1081, 0)
$23A-K$	2256	2	True	True	4374	(1128, 1128, 0)
$24A-D$	2162	2	True	True	4276	(1081, 1081, 0)
$47A-B$	1104	23	False	True	1610	(576, 528, 0)

$PSL(2,49)$, order 58800

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	1225	25	True	True	2353	(1225, 0, 0)
$3A$	2450	2	True	True	4756	(1225, 1225, 0)
$4A$	2450	2	True	True	4756	(1225, 1225, 0)
$5A-B$	2352	2	True	True	4654	(1176, 1176, 0)
$6A$	2450	2	True	True	4756	(1225, 1225, 0)
$7A-B$	1200	24	True	True	2928	(600, 600, 0)
$8A-B$	2450	2	True	True	4756	(1225, 1225, 0)
$12A-B$	2450	2	True	True	4756	(1225, 1225, 0)
$24A-D$	2450	2	True	True	4756	(1225, 1225, 0)
$25A-J$	2352	2	True	True	4654	(1176, 1176, 0)

$PSU(3,4)$, order 62400

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	195	3	True	False (65)	201	(195, 0, 0)
$3A$	4160	2	True	True	8134	(2080, 2080, 0)
$4A$	3900	12	True	True	7824	(1950, 1950, 0)
$5A-D$	208	13	False	True	484	(79, 129, 0)
$5E-F$	2496	6	True	True	5436	(1248, 1248, 0)
$10A-D$	3120	3	False	True	3756	(1586, 1534, 0)
$13A-D$	4800	3	False	True	3948	(2310, 2490, 0)
$15A-D$	4160	2	False	True	4054	(2041, 2119, 0)

$PSL(2,53)$, order 74412

$\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{\mathcal{C}}(\mathcal{C})$	Real	Irred	$\lambda_{\max}$	Signature
$2A$	1431	27	True	True	2757	(1431, 0, 0)
$3A$	2756	2	True	True	5458	(1378, 1378, 0)
$9A-C$	2756	2	True	True	5458	(1378, 1378, 0)
$13A-F$	2862	2	True	True	5568	(1431, 1431, 0)
$26A-F$	2862	2	True	True	5568	(1431, 1431, 0)
$27A-I$	2756	2	True	True	5458	(1378, 1378, 0)
$53A-B$	1404	26	True	True	3432	(702, 702, 0)

REFERENCES

[**1**] H. U. Besche, B. Eick and E. O'Brien, *The Small Groups library* `http://www.icm.tu-bs.de/ag_algebra/software/small/`

[**2**] A. Connes, Noncommutative Geometry, Academic Press, 1994

[**3**] J. H. Conway, R. T. Curtis, R. A. Parker, S. P. Norton, and R. A. Wilson, Atlas of finite groups. Clarendon Press, 1985

[**4**] A. Frumkin, Theorem about the conjugacy representation of S_n, Israel J. Math 55 (1986) 121–128

[**5**] W. Fulton, Young tableaux, London Mathematical Society Student Texts, no. 35, Cambridge University Press, 1997

[**6**] W. Fulton, J. Harris, Representation Theory A fist Course, Graduate Texts in Mathematics 129, Springer Verlag, 1991

[**7**] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, `http://www.gap-system.org`

[**8**] X. Gomez and S. Majid, Braided Lie algebras and bicovariant differential calculi over coquasitriangular Hopf algebras, J. Algebra 261 (2003) 334–388

[**9**] G. Heide and A. Zalesski, Passman's problem on adjoint representations. In: Groups, Rings and Algebras (Proc. Conf. in Honour of D.S. Passman), Contemporary Math. 420 (2006) 163 – 176. Amer. Math. Soc.

[**10**] G. Heide, J. Saxl, P. Tiep and A. Zalesski, Conjugacy action, induced representations and the Steinberg square for simple groups of Lie type, Proc. London Math. Soc. 106 (2013) 908–930

[**11**] T. Leinster, The magnitude of metric spaces, Doc. Math. 18 (2013) 857–905

[**12**] S. Majid, *A Quantum Groups Primer*, L.M.S. Lect. Notes no 292, Cambridge University Press, 2002

[**13**] S. Majid, Quantum and braided Lie-algebras, J. Geom. Phys. 13 (1994) 307–356

[**14**] S. Majid, Solutions of the Yang-Baxter Equations from Braided-Lie Algebras and Braided Groups, J. Knot Th. Ramif. 4 (1995) 673-697

[**15**] S. Majid, Noncommutative differentials and Yang-Mills on permutation groups S_N, Lect. Notes Pure Appl. Maths 239 (2004) 189–214, Marcel Dekker

[**16**] S. Majid, Riemannian geometry of quantum groups and finite groups with nonuniversal differentials, Commun. Math. Phys. 225 (2002) 131–170

[**17**] S. Majid, Noncommutative Riemannian geometry of graphs, J. Geom. Phys. 69 (2013) 74–93

[**18**] S. Majid and K. Rietsch, Lie theory and coverings of finite groups, J. Algebra 389 (2013) 137–150

[**19**] F. Ngakeu, S. Majid and D. Lambert, Noncommutative Riemannian geometry of the alternating group A_4, J. Geom. Phys. 42 (2002) 259–282

[**20**] D. S. Passman, The adjoint representation of group algebras and enveloping algebras, Publ. Math. 36 (1992) 861–878

[**21**] R. L. Roth, On the conjugation representation of a finite group, Pacific J. Math. 36 (1971) 515–521

[**22**] B. Sagan, The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions, 2nd edition, Springer-Verlag, New York, 2001

[**23**] T. Scharf, Ein weiterer Beweis, dass die konjugierende Darstellung der symmetrischen Gruppen jede irreduzible Darstellung enthält, Arch. Math. 54 (1990) 427–429

[**24**] W. A. Stein et al., *Sage Mathematics Software (Version 4.8)*. The Sage Development Team, 2011, `http://www.sagemath.org`

[**25**] H. S. Wilf, Lectures on integer partitions, online notes of lectures given at Univ. of Victoria, B.C. Canada in 2000

[**26**] S. L. Woronowicz, Differential calculus on compact matrix pseudogroups (quantum groups), Comm. Math. Phys. 122 (1989) 125–170

[**27**] D. Zagier, On the distribution of the number of cycles of elements in symmetric groups, Nieuw Archief voor Wiskunde 13 (1995) 489–495