NOTE ON AN INEQUALITY OF BURNSIDE

E. KOWALSKI

A well-known property of irreducible characters of finite groups is the fact, proved by Burnside, that if G is a finite group and

$$\varrho : G \longrightarrow \mathrm{GL}(E)$$

is an irreducible complex representation of dimension $\dim(\varrho) \geqslant 2$, then there exists some $g \in G$ such that $\chi_\varrho(g) = \operatorname{Tr} \varrho(g)$ is zero.

A common argument to prove this relies on the following result (also due to Burnside) on representations of finite *cyclic* groups:

Theorem 1 (Burnside)**.** *Let $G = \mathbf{Z}/m\mathbf{Z}$ with $m \geqslant 2$ be a finite cyclic group, and let*

$$G^* = \{x \in G \mid x \text{ generates } G\} = \{x \in \mathbf{Z}/m\mathbf{Z} \mid (x, m) = 1\}$$

be the set of generators of G. If

$$\varrho : G \longrightarrow \mathrm{GL}(E)$$

is a representation of G, not necessarily irreducible, such that $\chi_\varrho(x) \neq 0$ for all $x \in G^*$, then we have

$$\sum_{x \in G^*} |\chi_\varrho(x)|^2 \geqslant |G^*| = \varphi(m), \tag{1}$$

the Euler function.

The simplest proof of this relies on the arithmetic-geometric mean inequality and the remark that

$$\prod_{x \in G^*} |\chi_\varrho(x)|^2$$

is an algebraic integer which, by Galois invariance, is in fact in $\mathbf{Z}$, and non-negative; if non-zero, it must be $\geqslant 1$, and the arithmetic-geometric inequality implies that

$$\frac{1}{|G^*|} \sum_{x \in G^*} |\chi_\varrho(x)|^2 \geqslant \Big(\prod_{x \in G^*} |\chi_\varrho(x)|^2 \Big)^{1/|G^*|} \geqslant 1.$$

This is a nice argument, but since this result is, after all, a true fact about representations of the simplest possible groups (finite cyclic groups!), one may ask if one couldn't just prove it straight without knowing anything about Galois theory. We explain here one way to do this – it is a scenic road, but surprisingly involved.

The key to this approach is to see the left-hand side of (1) as a quadratic form in the m integral variables which are the multiplicities $n(a) \in \mathbf{Z}$ of the irreducible characters

$$x \mapsto e\Big(\frac{ax}{m}\Big), \qquad a \in \mathbf{Z}/m\mathbf{Z}$$

in ϱ. Indeed, we have

$$\chi_\varrho(x) = \sum_{a \,(\mathrm{mod}\, m)} n(a) e\Big(\frac{ax}{m}\Big),$$

and hence

$$\sum_{x\in G^*}|\chi_\varrho(x)|^2=\sum_{(x,m)=1}\Big|\sum_{a\,(\mathrm{mod}\,m)}n(a)e\Big(\frac{ax}{m}\Big)\Big|^2,$$

which is, as function of $\boldsymbol{n}=(n(a))\in\mathbf{Z}^m$, a quadratic form

$$Q_m\,:\,\mathbf{Z}^m\longrightarrow\mathbf{Z}$$

(the integrality is clear by Galois invariance, though we will also recover it directly later – since we do all this to avoid appealing to Galois theory!) In other words, we see Q_m as a quadratic form on the integral representation ring $K(\mathbf{Z}/m\mathbf{Z})$ of virtual characters of $\mathbf{Z}/m\mathbf{Z}$.

The goal is then to prove that the minimum non-zero value of the quadratic form Q_m on $\mathbf{Z}^m$ is $\varphi(m)$ for $m\geqslant 1$, i.e., denoting

$$s(Q)=\min_{\substack{x\in\mathbf{Z}^d\\ Q(x)\neq 0}}Q(x)$$

for any integral quadratic form Q, that $s(Q_m)=\varphi(m)$.

We can assume of course that $m\geqslant 2$; the strategy is then the following:

- First step: writing
$$m=\prod_{p|m}p^{k_p}$$
the factorization of m, we have a tensor product decomposition
$$Q_m=\bigotimes_{p|m}Q_{p^{k_p}}.$$
- Second step: for p prime and $k\geqslant 1$, we have
$$s(Q_{p^k})=p^k-p^{k-1}=\varphi(p^k),$$
- Third step: as a general rule, the minimum of a tensor product does *not* satisfy $s(Q_1\otimes Q_2)=s(Q_1)s(Q_2)$ (see Remark 2 below for examples about this). However, for any prime p and $k\geqslant 1$, the following is true: for any integral quadratic form Q', we have
$$s(Q_{p^k}\otimes Q')=s(Q_{p^k})s(Q')=\varphi(p^k)s(Q').$$

By induction on the number of prime factors of $m\geqslant 2$, the properties (1), (2) and (3) imply that

$$s(Q_m)=s\Big(\bigotimes_{p|m}Q_{p^{k_p}}\Big)=\prod_{p|m}\varphi(p^{k_p})=\varphi(m),$$

as desired.

We now prove (1), (2) and (3). First of all, (1) is a formal fact, coming from the Chinese Remainder Theorem. As for (2), it follows from (3) applied to the "trivial" quadratic form $Q(x)=x^2$ on $\mathbf{Z}$, for which $s(Q)=1$. Thus we proceed to prove (3), using arguments adapted from Kitaoka's in [2, §7.1]. For this, it should be noted at the outset that the upper-bound

$$s(Q_m)\leqslant\varphi(m)$$

is always easy: it is obtained when $n(a)$ is 0 except for a single a, in which case it is 1, i.e., it corresponds to taking an irreducible representation ϱ in the original problem.

We now work towards the converse lower bound, and we start with $k = 1$, i.e., with Q_p where p is prime. Then we compute Q_p explicitly for $\boldsymbol{n} = (n(a))_{a\in\mathbf{Z}/p\mathbf{Z}}$:

$$Q_p(\boldsymbol{n}) = \sum_{a,b} n(a)n(b) \sum_{(x,p)=1} e\Big(\frac{x(a-b)}{p}\Big) \tag{2}$$

and the inner sum, by orthogonality of characters, is either $p-1$ or -1, depending on whether $a = b$ or $a \neq b$. Hence

$$Q_p(\boldsymbol{n}) = p\sum_a n(a)^2 - \Big(\sum_b n(b)\Big)^2.$$

We interpret this as essentially the "variance" of the values $n(a)$ as a runs over $\mathbf{Z}/p\mathbf{Z}$, precisely it is p^2 times the variance:

$$Q_p(\boldsymbol{n}) = p^2\Big\{\frac{1}{p}\sum_a n(a)^2 - \Big(\frac{1}{p}\sum_b n(b)\Big)^2\Big\}.$$

The variance has two alternate expressions: the first one is very well-known, and states that

$$Q_p(\boldsymbol{n}) = p\sum_a \Big\{n(a) - \frac{1}{p}\sum_b n(b)\Big\}^2. \tag{3}$$

The second is maybe not so well known, and gives

$$Q_p(\boldsymbol{n}) = \frac{1}{2}\sum_{a,b}(n(a) - n(b))^2, \tag{4}$$

which displays clearly the integrality of Q_p (the factor $1/2$ is innocuous since the pairs (a, b) and (b, a) have the same contributions if $a \neq b$, and the diagonal terms $a = b$ are zero). In probabilistic terms, these identities say that

$$\mathbf{V}(X) = \mathbf{E}((X - \mathbf{E}(X))^2),$$

and that

$$\mathbf{V}(X) = \frac{1}{2}\mathbf{E}((X - Y)^2),$$

respectively, where Y is a random variable with the same law as X and independent of X: indeed, we have

$$\mathbf{E}((X-Y)^2) = \mathbf{E}(X^2) + \mathbf{E}(Y^2) - 2\mathbf{E}(XY) = 2\mathbf{E}(X^2) - 2\mathbf{E}(X)\mathbf{E}(Y) = 2\mathbf{V}(X).$$

We must show that, unless $Q_p(\boldsymbol{n}) = 0$, we have $Q_p(\boldsymbol{n}) \geqslant p - 1$. This can be proved using (3), but (4) gives a much nicer argument. First, this formula makes it clear that $Q_p(n)$ is non-zero if and only if there exist $a \neq b$ such that $n(a) \neq n(b)$. If this is the case, fix one such pair (a, b). Let

$$I = \{x \in \mathbf{Z}/p\mathbf{Z} \mid n(x) = n(a)\}, \qquad J = \mathbf{Z}/p\mathbf{Z} - I.$$

Then observe that the $2|I|$ pairs

$$(n(b), n(x)), \quad (n(x), n(b)), \qquad x \in I,$$

are distinct, and the $2|J|$ pairs

$$(n(a), n(y)), \quad (n(y), n(a)), \qquad y \in J,$$

also are. The only pairs appearing in both sets are $(n(b), n(a))$ and $(n(a), n(b))$. Thus we have at least $2(|I| + |J|) - 2 = 2(p-1)$ pairs of distinct integers in the sum appearing in (4), and therefore

$$Q_p(\boldsymbol{n}) \geqslant \frac{2(p-1)}{2} = p - 1.$$

As we saw early on, the converse inequality is easy, and hence we obtain the first step

$$s(Q_p) = p - 1.$$

Although the argument was applied to Q_p itself, it is "natural", and hence extends to any tensor product $Q' = Q_p \otimes Q$: indeed, if Q is of rank $m \geqslant 1$, the quadratic form Q' can be seen as acting on vectors $\boldsymbol{n} = (n(a))_{a\in\mathbf{Z}}$ with $n(a) \in \mathbf{Z}^m$, using the *same* formula (4) with Q replacing the quadratic form $n \mapsto n^2$ on $\mathbf{Z}$:

$$Q'(\boldsymbol{n}) = \frac{1}{2} \sum_{a,b\in\mathbf{Z}/p\mathbf{Z}} Q(n(a) - n(b)).$$

If not all $n(a)$ are equal, which corresponds to $Q'(\boldsymbol{n}) = 0$, we get by the same argument as above

$$Q'(\boldsymbol{n}) \geqslant (p-1)s(Q).$$

Again the corresponding upper bound is clear (take $n(a) = 0$ except for a single a, and for this select any $n(a) \in \mathbf{Z}^m$ which achieves $s(Q)$), and therefore

$$s(Q \otimes Q_p) = (p-1)s(Q) \tag{5}$$

for any integral quadratic form Q.

This fact about the case $k = 1$, it turns out, is enough for our purposes, because for $k \geqslant 2$, there is an integral quadratic form Q of rank p^{k-1} with $s(Q) = p^{k-1}$ such that

$$Q_{p^k} = Q_p \otimes Q,$$

and hence, by (5), we have

$$s(Q_{p^k}) = s(Q_p)s(Q) = (p-1)p^{k-1} = \varphi(p^k),$$

as desired. To see this, we compute Q_{p^k} as before using (2), which now gives

$$Q_p(n) = \sum_{a,b\in\mathbf{Z}/p^k\mathbf{Z}} n(a)n(b) \sum_{x\in(\mathbf{Z}/p^k\mathbf{Z})^\times} e\Big(\frac{x(a-b)}{p^k}\Big)$$

and the inner sum is now

$$\sum_{x\in(\mathbf{Z}/p^k\mathbf{Z})^\times} e\Big(\frac{x(a-b)}{p^k}\Big) = \begin{cases} p^k - p^{k-1}, & \text{if } a = b \\ -p^{k-1}, & \text{if } a \neq b \text{ but } a \equiv b \,(\mathrm{mod}\, p^{k-1}) \\ 0 & \text{othwerwise,} \end{cases}$$

by orthogonality (and inclusion-exclusion; this is a special case of evaluation of a Ramanujan sum). Using this, one is lead by a simple computation to the formula

$$Q_{p^k}(\boldsymbol{n}) = p^k \sum_{a\in\mathbf{Z}/p^k\mathbf{Z}} \Big\{ n(a) - \frac{1}{p} \sum_{b\equiv a \,(\mathrm{mod}\, p^{k-1})} n(b) \Big\}^2.$$

We can rewrite this as follows, in order to bring the factorization of Q_{p^k} in focus:

$$Q_{p^k}(\boldsymbol{n}) = p^{k-1} \sum_{c \in \mathbf{Z}/p^{k-1}\mathbf{Z}} p \sum_{\substack{a \in \mathbf{Z}/p^k\mathbf{Z} \\ a \equiv c \,(\mathrm{mod}\, p^{k-1})}} \Big\{ n(a) - \frac{1}{p} \sum_{b \equiv c \,(\mathrm{mod}\, p^{k-1})} n(b) \Big\}^2.$$

Indeed, in view of (3) and the fact that the $a \in \mathbf{Z}/p^k\mathbf{Z}$ congruent to $c \,(\mathrm{mod}\, p^{k-1})$ are those of the form

$$c + a' p^{k-1}$$

with $a' \in \mathbf{Z}/p\mathbf{Z}$, this can be interpreted as the statement that

$$Q_{p^k} = Q \otimes Q_p$$

where, for $\boldsymbol{n} \in \mathbf{Z}^{p^{k-1}}$, we have

$$Q(\boldsymbol{n}) = p^{k-1} \sum_{c \in \mathbf{Z}/p^{k-1}\mathbf{Z}} n(c)^2.$$

This quadratic form satisfies $s(Q) = p^{k-1}$, obviously (!), and therefore we have obtained the desired factorization.

Remark 2 (Multiplicativity, where art thou?). As already mentioned, it is not true, in general that

$$s(Q_1 \otimes Q_2) = s(Q_1)s(Q_2)$$

for integral quadratic forms Q_1 and Q_2. Indeed, following an argument of Steinberg based on Siegel's Mass formula, Milnor and Husemoller explain in [3, §9.6] that for any n large enough, there exists self-dual lattices L_1 and L_2 of rank n such that

$$s(L_1 \otimes L_2) < s(L_1)s(L_2).$$

The idea of the construction is that, for any lattice L with dual L', we have an a priori inequality $s(L \otimes L') \leqslant n$, which comes from the vector $v \in L \otimes L'$ that corresponds to the identity under the canonical isomorphism $\mathrm{Hom}(L, L) \simeq L \otimes L'$. Thus, if L is self-dual with $s(L) > \sqrt{n}$, we have

$$s(L)s(L') > n \geqslant s(L \otimes L').$$

Now, using Siegel's formula, Conway and Thompson have shown (see [3, Th. 9.5]) that for all n large enough, there exists some self-dual lattice L of rank n with $s(L) > \sqrt{n}$, in fact, with $s(L) \gg n$.

In [2], a quadratic form Q such that $s(Q \otimes Q') = s(Q)s(Q')$ for all Q' is said to be "type E", and a number of examples and properties of these are given. Amusingly, although the definition would not be so interesting without examples of lattices which are *not* of "type E", Kitaoka does not seem to provide any reference or hint to such examples as those of Steinberg!

Remark 3 (More formulas). For a general $m \geqslant 1$, one can express Q_m "directly" as follows, generalizing the cases $m = p$ or p^k: we have

$$\begin{aligned} Q_m(\boldsymbol{n}) &= \sum_{(x,m)=1} \Big| \sum_{a \in \mathbf{Z}/m\mathbf{Z}} n(a) e\Big(\frac{ax}{m}\Big) \Big|^2 \\ &= m \sum_{a \in \mathbf{Z}/m\mathbf{Z}} \Big\{ \sum_{d \mid m} \frac{d}{m} \mu\Big(\frac{m}{d}\Big) \sum_{\substack{b \,(\mathrm{mod}\, m) \\ b \equiv a \,(\mathrm{mod}\, d)}} n(b) \Big\}^2. \end{aligned}$$

Some identities which are close to this appear in some forms of the (arithmetic) large sieve inequalities. It is not clear to me if one can prove $s(Q_m) \geqslant \varphi(m)$ directly using this expression (i.e., without using the multiplicative structure to reduce to the case of m a power of a prime.)

References

[1] I.M. Isaacs: *Character theory of finite groups*, Academic Press (1976).
[2] Y. Kitaoka: *Arithmetic of quadratic forms*, Cambridge Tracts in Math. 106, Cambridge Univ. Press (1993).
[3] J. Milnor and D. Husemoller: *Symmetric bilinear forms*, Ergebnisse der Math. 73, Springer-Verlag (1973).

ETH Zürich – DMATH, Rämistrasse 101, 8092 Zürich, Switzerland
E-mail address: kowalski@math.ethz.ch