Bounding the number of characters in a block of a finite group

Benjamin Sambale*

October 17, 2019

Abstract

We present a strong upper bound on the number $k(B)$ of irreducible characters of a p-block B of a finite group G in terms of local invariants. More precisely, the bound depends on a chosen major B-subsection (u,b), its normalizer $\mathrm{N}_G(\langle u\rangle, b)$ in the fusion system and a weighted sum of the Cartan invariants of b. In this way we strengthen and unify previous bounds given by Brauer, Wada, Külshammer–Wada, Héthelyi–Külshammer–Sambale and the present author.

Keywords: number of characters in a block, Cartan matrix, Brauer's $k(B)$-Conjecture
AMS classification: 20C15, 20C20

1 Introduction

Let B be a p-block of a finite group G with defect d. Since Richard Brauer [4] conjectured that the number of irreducible characters $k(B)$ in B is at most p^d, there has been great interest in bounding $k(B)$ in terms of local invariants. Brauer and Feit [6] used some properties of the Cartan matrix $C = (c_{ij}) \in \mathbb{Z}^{l(B)\times l(B)}$ of B to prove their celebrated bound $k(B) \le p^{2d}$ (here and in the following $l(B)$ denotes the number of irreducible Brauer characters of B). In the present paper we investigate stronger bounds by making use of further local invariants. By elementary facts on decomposition numbers, it is easy to see that

$$k(B) \le \mathrm{tr}(C) \tag{1}$$

where $\mathrm{tr}(C)$ denotes the trace of C. However, it is not true in general that $\mathrm{tr}(C) \le p^d$. In fact, there are examples with $\mathrm{tr}(C) > l(B)p^d$ (see [11]) although Brauer already knew that $k(B) \le l(B)p^d$ (see Corollary 15 below) and this was subsequently improved by Olsson [12, Theorem 4]. For this reason, some authors strengthened (1) in a number of ways. Brandt [3, Proposition 4.2] proved

$$k(B) \le \mathrm{tr}(C) - l(B) + 1$$

and this was generalized by the present author in [17, Proposition 8] to

$$k(B) \le \sum_{i=1}^{m} \det(C_i) - m + 1$$

*Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany, sambale@math.uni-hannover.de

where $S_1, \ldots, S_m$ is a partition of $\{1, \ldots, l(B)\}$ and $C_i := (c_{st})_{s,t \in S_i}$. Using different methods, Wada [20] observed that

$$k(B) \le \operatorname{tr}(C) - \sum_{i=1}^{l(B)-1} c_{i,i+1}. \tag{2}$$

In Külshammer–Wada [10], the authors noted that (2) is a special case of

$$k(B) \le \sum_{1 \le i \le j \le l(B)} q_{ij} c_{ij} \tag{3}$$

where $q(x) = \sum_{1 \le i \le j \le l(B)} q_{ij} x_i x_j$ is a (weakly) positive definite integral quadratic form.

Since C is often harder to compute than $k(B)$, it is desirable to replace C by the Cartan matrix of a Brauer correspondent of B in a proper subgroup. For this purpose let D be a defect group of B and choose $u \in \mathrm{Z}(D)$. Then a Brauer correspondent b of B in $\mathrm{C}_G(u)$ has defect group D as well. The present author replaced c_{ij} in (3) by the corresponding entries of the Cartan matrix C_u of b (see [15, Lemma 1]).

In Héthelyi–Külshammer–Sambale [9, Theorem 2.4] we have invoked Galois actions to obtain stronger bounds although only in the special cases $p = 2$ and $l(b) = 1$ (see [9, Theorems 3.1 and 4.10]). More precisely, in the latter case we proved

$$k(B) \le \sum_{i=1}^{\infty} p^{2i} k_i(B) \le \Big(n + \frac{|\langle u \rangle| - 1}{n}\Big) \frac{p^d}{|\langle u \rangle|} \le p^d = \operatorname{tr}(C_u) \tag{4}$$

where $n := |\mathrm{N}_G(\langle u \rangle, b) : \mathrm{C}_G(u)|$ and $k_i(B)$ is the number of irreducible characters of height $i \ge 0$ in B. This is a refinement of a result of Robinson [13, Theorem 3.4.3]. In [18, Theorem 2.6], the present author relaxed the condition $l(b) = 1$ to the weaker requirement that $\mathcal{N} := \mathrm{N}_G(\langle u \rangle, b)/\mathrm{C}_G(u)$ acts trivially on the set $\mathrm{IBr}(b)$ of irreducible Brauer characters of b.

In this paper we replace integral quadratic forms by real matrices W describing weighted sums of Cartan invariants. This allows us to drop all restrictions imposed above. We prove the following general result which incorporates the previous special cases (see Section 3 for details).

Theorem A. *Let B be a block of a finite group G with defect group D. Let $u \in \mathrm{Z}(D)$ and let b be a Brauer correspondent of B in $\mathrm{C}_G(u)$. Let $\mathcal{N} := \mathrm{N}_G(\langle u \rangle, b)/\mathrm{C}_G(u)$ and let C be the Cartan matrix of the block $\overline{b}$ of $\mathrm{C}_G(u)/\langle u \rangle$ dominated by b. Let $W \in \mathbb{R}^{l(b) \times l(b)}$ such that $xWx^t \ge 1$ for every $x \in \mathbb{Z}^{l(b)} \setminus \{0\}$. Then*

$$\boxed{k(B) \le \Big(|\mathcal{N}| + \frac{|\langle u \rangle| - 1}{|\mathcal{N}|}\Big) \operatorname{tr}(WC) \le |\langle u \rangle| \operatorname{tr}(WC).}$$

The first inequality is strict if $\mathcal{N}$ acts non-trivially on $\mathrm{IBr}(b)$ and the second inequality is strict if and only if $1 < |\mathcal{N}| < |\langle u \rangle| - 1$.

In contrast to (4), we cannot replace $k(B)$ by $\sum p^{2i} k_i(B)$ in Theorem A (the principal 2-block of $\mathrm{SL}(2,3)$ is a counterexample with $u = 1$). By a classical fusion argument of Burnside, the automorphism group $\mathcal{N}$ of $\langle u \rangle$ in Theorem A is the restriction of the inertial quotient $\mathrm{N}_G(D, b_D)/D\mathrm{C}_G(D) \le \mathrm{Aut}(D)$ where b_D is a Brauer correspondent of B in $\mathrm{C}_G(D)$ (see [1, Corollary 4.18]). In particular, $\mathcal{N}$ is a p'-group and $|\mathcal{N}|$ divides $p - 1$.

As noted in previous papers, if $u \in D \setminus \mathrm{Z}(D)$, one still gets upper bounds on the number of height 0 characters and this is of interest with respect to Olsson's Conjecture $k_0(B) \le |D : D'|$ where D' denotes the commutator subgroup of D. In fact, we will deduce Theorem A from our second main theorem:

Theorem B. *Let B be a block of a finite group G with defect group D. Let $u \in D$ and let b be a Brauer correspondent of B in $\mathrm{C}_G(u)$. Let $\mathcal{N} := \mathrm{N}_G(\langle u\rangle, b)/\mathrm{C}_G(u)$ and let C be the Cartan matrix of the block $\overline{b}$ of $\mathrm{C}_G(u)/\langle u\rangle$ dominated by b. Let $W \in \mathbb{R}^{l(b)\times l(b)}$ such that $xWx^t \ge 1$ for every $x \in \mathbb{Z}^{l(b)} \setminus \{0\}$. Then*

$$\boxed{k_0(B) \le k_0\big(\langle u\rangle \rtimes \mathcal{N}\big)\operatorname{tr}(WC) \le |\langle u\rangle| \operatorname{tr}(WC).}$$

The first inequality is strict if $\mathcal{N}$ acts non-trivially on $\mathrm{IBr}(b)$.

In the situation of Theorem B we may assume, after conjugation, that $\mathrm{N}_D(\langle u\rangle)/\mathrm{C}_D(u)$ is a Sylow p-subgroup of $\mathcal{N}$ (see [2, Proposition 2.5]). In particular, $\mathcal{N} = \mathrm{N}_D(\langle u\rangle)/\mathrm{C}_D(u)$ whenever $p = 2$.

If $\mathcal{N}$ acts trivially on $\mathrm{IBr}(b)$, then our bounds cannot be improved in general. To see this, let $\langle u\rangle$ be any cyclic p-group, and let $\mathcal{N} \le \mathrm{Aut}(\langle u\rangle)$. Then $G := \langle u\rangle \rtimes \mathcal{N}$ has only one p-block B. In this situation $l(b) = 1$ and $C = (1)$. Hence, $k_0(B) = k_0(G) = k_0(\langle u\rangle \rtimes \mathcal{N})\operatorname{tr}(WC)$ for $W = (1)$. Similarly, if $\mathcal{N}$ is a p'-group, then $k(B) = k(G) = |\mathcal{N}| + \frac{|\langle u\rangle|-1}{|\mathcal{N}|}$.

It is known that the ordinary character table of $\mathrm{C}_G(u)/\langle u\rangle$ determines C up to basic sets, i. e. up to transformations of the form $S^{\mathrm{t}}CS$ where $S \in \mathrm{GL}(l(b), \mathbb{Z})$ and S^{t} is the transpose of S. Then $\widetilde{W} := S^{-1}WS^{-\mathrm{t}}$ still satisfies $x\widetilde{W}x^{\mathrm{t}} \ge 1$ for every $x \in \mathbb{Z}^{l(b)} \setminus \{0\}$ and

$$\operatorname{tr}(\widetilde{W}S^{\mathrm{t}}CS) = \operatorname{tr}(S^{-1}WCS) = \operatorname{tr}(WC).$$

Hence, our results do not depend on the chosen basic set.

2 Proofs

First we outline the proof of Theorem B: For sake of simplicity suppose first that $u = 1$. Then every row d_χ of the decomposition matrix Q of B is non-zero and $Q^{\mathrm{t}}Q = C$. Hence,

$$k(B) \le \sum_{\chi \in \mathrm{Irr}(B)} d_\chi W d_\chi^{\mathrm{t}} = \operatorname{tr}(QWQ^{\mathrm{t}}) = \operatorname{tr}(WQ^{\mathrm{t}}Q) = \operatorname{tr}(WC).$$

In the general case we replace Q be the generalized decomposition matrix with respect to the subsection (u, b). Then Q consists of algebraic integers in the cyclotomic field of degree $q := |\langle u\rangle|$. We apply a discrete Fourier transformation to turn Q into an integral matrix with the same number of rows, but with more columns. At the same time we need to blow up W to a larger matrix with similar properties. Afterwards we use the fact that the rows of Q corresponding to height 0 characters are non-zero and fulfill a certain p-adic valuation. For $p = 2$ the proof can be completed directly, while for $p > 2$ we argue by induction on q. Additional arguments are required to handle the case where $|\mathcal{N}|$ is divisible by p. These calculations make use of sophisticated matrix analysis.

We fix the following matrix notation. For $n \in \mathbb{N}$ let 1_n be the identity matrix of size $n \times n$ and similarly let 0_n be the zero matrix of the same size. Moreover, let

$$U_n := \frac{1}{2}\begin{pmatrix} 2 & -1 & & 0 \\ -1 & \ddots & \ddots & \\ & \ddots & \ddots & -1 \\ 0 & & -1 & 2 \end{pmatrix} \in \mathbb{Q}^{n\times n}.$$

For $d \in \mathbb{N}$ let $d^{n\times n}$ be the $n\times n$ matrix which has every entry equal to d. For $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{m\times m}$ we construct the direct sum $A \oplus B \in \mathbb{R}^{(n+m)\times(n+m)}$ and the Kronecker product $A \otimes B \in \mathbb{R}^{nm\times nm}$

in the usual manner. Note that $\mathrm{tr}(A \oplus B) = \mathrm{tr}(A) + \mathrm{tr}(B)$ and $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\,\mathrm{tr}(B)$. Finally, let δ_{ij} be the Kronecker delta. We assume that every positive (semi)definite matrix is symmetric. Moreover, we call a symmetric matrix $A \in \mathbb{R}^{n\times n}$ *integral positive definite*, if $xAx^{\mathrm{t}} \geq 1$ for every $x \in \mathbb{Z}^n \setminus \{0\}$.

The proof of Theorem B is deduced from a series of lemmas and propositions.

Lemma 1. *Every integral positive definite matrix is positive definite.*

Proof. Let $W \in \mathbb{R}^{n\times n}$ be integral positive definite. By way of contradiction, suppose that there exists an eigenvector $v \in \mathbb{R}^n$ of W with eigenvalue $\lambda \leq 0$ and (euclidean) norm 1. If $\lambda < 0$, choose $x \in \mathbb{Q}^n$ such that $\|x\| \leq \|v\| = 1$ and $\|x - v\| < -\frac{\lambda}{2\|W\|}$ where $\|W\|$ denotes the Frobenius matrix norm of W. Then

$$xWx^{\mathrm{t}} = (x - v)W(x + v)^{\mathrm{t}} + vWv^{\mathrm{t}} \leq \|x - v\|\|W\|\|x + v\| + \lambda < 0.$$

However, there exists $m \in \mathbb{N}$ such that $mx \in \mathbb{Z}^n$ and $(mx)W(mx)^{\mathrm{t}} < 0$. This contradiction implies $\lambda = 0$. By Dirichlet's approximation theorem (see [8, Theorem 200]) there exist infinitely many integers m and $x \in \mathbb{Z}^n$ such that

$$\|x - mv\| < \frac{\sqrt{n}}{\sqrt[n]{m}}.$$

It follows that

$$xWx^{\mathrm{t}} = (x - mv)W(x - mv)^{\mathrm{t}} \leq \|x - mv\|^2\|W\| < 1$$

if m is sufficiently large. Again we have a contradiction. $\square$

Conversely, every positive definite matrix can be scaled to an integral positive definite matrix. The next lemma is a key argument when dealing with non-trivial actions of $\mathcal{N}$ on $\mathrm{IBr}(b)$.

Lemma 2. *Let $A, B \in \mathbb{R}^{n\times n}$ positive semidefinite matrices such that A commutes with a permutation matrix $P \in \mathbb{R}^{n\times n}$. Then $\mathrm{tr}(ABP) \leq \mathrm{tr}(AB)$. If A and B are positive definite, then $\mathrm{tr}(ABP) = \mathrm{tr}(AB)$ if and only if $P = 1_n$.*

Proof. By the spectral theorem, A and P are diagonalizable. Since they commute, they are simultaneously diagonalizable. Since A has real, non-negative eigenvalues, there exists a positive semidefinite matrix $A^{1/2} \in \mathbb{R}^{n\times n}$ such that $A^{1/2}A^{1/2} = A$ and $A^{1/2}P = PA^{1/2}$. Then $M := (m_{ij}) = A^{1/2}BA^{1/2}$ is also positive semidefinite. In particular $m_{ij} \leq (m_{ii} + m_{jj})/2$ for $i, j \in \{1, \ldots, n\}$. If σ denotes the permutation corresponding to P, then we obtain

$$\mathrm{tr}(ABP) = \mathrm{tr}(A^{1/2}BPA^{1/2}) = \mathrm{tr}(MP) = \sum_{i=1}^{n} m_{i\sigma(i)} \leq \sum_{i=1}^{n} \frac{m_{ii} + m_{\sigma(i)\sigma(i)}}{2} = \mathrm{tr}(M) = \mathrm{tr}(AB).$$

If A and B are positive definite, then so is M and we have $m_{ij} < (m_{ii} + m_{jj})/2$ whenever $i \neq j$. This implies the last claim. $\square$

Lemma 3. *Let $W \in \mathbb{R}^{n\times n}$ be integral positive definite and suppose that W commutes with a permutation matrix P. Let*

$$W_m := \frac{1}{2}\begin{pmatrix} 2W & -PW & & 0 \\ -P^tW & \ddots & \ddots & \\ & \ddots & \ddots & -PW \\ 0 & & -P^tW & 2W \end{pmatrix} \in \mathbb{R}^{mn\times mn}.$$

Then W_m is integral positive definite. In particular, $U_m \otimes W$ is integral positive definite.

Proof. Let $x = (x_1, \ldots, x_m)$ with $x_i \in \mathbb{Z}^n$. Since $WP = PW$ we have

$$\begin{aligned} xW_m x^{\mathrm{t}} &= \sum_{i=1}^{m} x_i W x_i^{\mathrm{t}} - \sum_{i=1}^{m-1} x_i P W x_{i+1}^{\mathrm{t}} \\ &= \frac{1}{2} x_1 W x_1^{\mathrm{t}} + \frac{1}{2} x_m W x_m^{\mathrm{t}} + \frac{1}{2} \sum_{i=1}^{m-1} (x_i P - x_{i+1}) W (x_i P - x_{i+1})^{\mathrm{t}}. \end{aligned}$$

We may assume that $x_i \neq 0$ for some $i \in \{1, \ldots, m\}$. If $i = 1$, then $x_m \neq 0$ or $x_j P \neq x_{j+1}$ for some j. In any case $xW_m x^{\mathrm{t}} \geq 1$. If $i > 1$, then the claim can be seen in a similar fashion. The last claim follows with $P = 1_n$. □

Now assume the notation of Theorem B. In addition, let p be the characteristic of B such that $q := |\langle u \rangle|$ is a power of p. Let $k := k(B)$, $l := l(b)$ and $\zeta := e^{2\pi i/q} \in \mathbb{C}$. Then the generalized decomposition matrix $Q = (d^u_{\chi\varphi})$ of B with respect to the subsection (u, b) has size $k \times l$ and entries in $\mathbb{Z}[\zeta]$ (see [16, Definition 1.19] for instance). By the orthogonality relations of generalized decomposition numbers, we have $Q^{\mathrm{t}}\overline{Q} = qC$ where qC is the Cartan matrix of b (see [16, Theorems 1.14 and 1.22]). Recall that C is positive definite and has non-negative integer entries.

The first part of the next lemma is a result of Broué [7] while the second part was known to Brauer [5, (5H)].

Lemma 4 ([16, Proposition 1.36])**.** *Let d_χ be a row of Q corresponding to a character $\chi \in \mathrm{Irr}(B)$ of height* 0*. Let d be the defect of $\overline{b}$ and let $\widetilde{C} := p^d C^{-1} \in \mathbb{Z}^{l \times l}$. Then the p-adic valuation of $d_\chi \widetilde{C} \overline{d_\chi}^{\mathrm{t}}$ is* 0*. In particular, $d_\chi \neq 0$. Now assume that $u \in \mathrm{Z}(D)$ and $\chi \in \mathrm{Irr}(B)$ is arbitrary. Then $d_\chi \neq 0$.*

We identify the Galois group $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ with $\mathrm{Aut}(\langle u \rangle) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ such that $\gamma(\zeta) = \zeta^\gamma$ for $\gamma \in \mathcal{G}$. In this way we regard $\mathcal{N}$ as a subgroup of $\mathcal{G}$. Let $n := |\mathcal{N}|$. For any $\gamma \in \mathcal{G}$, $\gamma(Q)$ is the generalized decomposition matrix with respect to (u^γ, b). If the subsections (u, b) and (u^γ, b) are not conjugate in G, then $\gamma \notin \mathcal{N}$ and $\gamma(Q)^{\mathrm{t}}\overline{Q} = 0$. On the other hand, if they are conjugate, then $\gamma \in \mathcal{N}$ and

$$\gamma(d^u_{\chi\varphi}) = d^{u^\gamma}_{\chi\varphi} = d^u_{\chi\varphi^\gamma} \tag{5}$$

for $\chi \in \mathrm{Irr}(B)$ and $\varphi \in \mathrm{IBr}(b)$. Hence, in this case, γ acts on the columns of Q and there exists a permutation matrix P_γ such that $\gamma(Q) = QP_\gamma$. Recall that permutation matrices are orthogonal, i. e. $P_{\gamma^{-1}} = P_\gamma^{-1} = P_\gamma^{\mathrm{t}}$. Since $\mathcal{G}$ is abelian, we obtain

$$CP_\gamma = Q^{\mathrm{t}}\gamma(\overline{Q}) = \gamma^{-1}(Q)^{\mathrm{t}}\overline{Q} = P^{\mathrm{t}}_{\gamma^{-1}}C = P_\gamma C \tag{6}$$

for every $\gamma \in \mathcal{N}$ and

$$\gamma(Q)^{\mathrm{t}}\overline{\delta(Q)} = \begin{cases} CP_{\gamma^{-1}\delta} & \text{if } \gamma \equiv \delta \pmod{\mathcal{N}} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

for $\gamma, \delta \in \mathcal{G}$. For any subset $\mathcal{S} \subseteq \mathcal{N}$ we write $P_{\mathcal{S}} := \sum_{\delta \in \mathcal{S}} P_\delta$.

Lemma 5. *In the situation of Theorem B we may assume that W is (integral) positive definite and commutes with P_γ for every $\gamma \in \mathcal{N}$.*

Proof. Let

$$\mathcal{W} := \frac{1}{2n} \sum_{\delta \in \mathcal{N}} P_\delta (W + W^{\mathrm{t}}) P_\delta^{\mathrm{t}}.$$

Then $\mathcal{W}$ is symmetric and commutes with P_δ for every $\delta \in \mathcal{N}$. Moreover, $\mathcal{W}$ is integral positive definite and by Lemma 1, $\mathcal{W}$ is positive definite. Finally,

$$\operatorname{tr}(\mathcal{W}C) = \frac{1}{2n}\sum_{\delta\in\mathcal{N}} \operatorname{tr}(P_\delta W C P_\delta^{\mathrm{t}}) + \operatorname{tr}(P_\delta W^{\mathrm{t}} C P_\delta^{\mathrm{t}}) = \operatorname{tr}(WC),$$

since P_δ commutes with C. Hence, we may replace W by $\mathcal{W}$. □

In the following we revisit some arguments from [16, Section 5.2]. Write $Q = \sum_{i=1}^{\varphi(q)} A_i\zeta^i$ where $A_i \in \mathbb{Z}^{k\times l}$ for $i = 1,\ldots,\varphi(q)$ and $\varphi(q) = q - q/p$ is Euler's function. Let

$$\mathcal{A}_q = \big(A_i : i = 1,\ldots,\varphi(q)\big) \in \mathbb{Z}^{k\times\varphi(q)l}.$$

Lemma 6. *The matrix $\mathcal{A}_q$ has rank $l\varphi(q)/n$.*

Proof. It is well-known that the Vandermonde matrix $V := (\zeta^{i\gamma} : 1 \le i \le \varphi(q), \gamma \in \mathcal{G})$ is invertible. Since Q has full rank, the facts stated above show that $(\gamma(Q) : \gamma \in \mathcal{G})$ has rank $l|\mathcal{G} : \mathcal{N}| = l\varphi(q)/n$. Then also $\mathcal{A}_q = (\gamma(Q) : \gamma \in \mathcal{G})(V \otimes 1_l)^{-1}$ has rank $l\varphi(q)/n$. □

Let T_q be the trace of $\mathbb{Q}(\zeta)$ with respect to $\mathbb{Q}$. Recall that

$$T_q(\zeta^i) = \begin{cases} \varphi(q) & \text{if } q \mid i, \\ -q/p & \text{if } q \nmid i \text{ and } \frac{q}{p} \mid i, \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$T_q(Q\zeta^{-i}) = \sum_{j=1}^{\varphi(q)} A_j T_q(\zeta^{j-i}) = \frac{q}{p}\Big(pA_i - \sum_{j\equiv i \pmod{q/p}} A_j\Big).$$

Definition 7. For $1 \le i \le \varphi(q)$ let i' be the unique integer such that $0 \le i' < q/p$ and $i' \equiv -i \pmod{q/p}$.

Then $q/p \le i + i' \le \varphi(q)$ and $\sum_{j\equiv i \pmod{q/p}} \zeta^{-j} = -\zeta^{i'}$ where we consider only those summands with $1 \le j \le \varphi(q)$. With this convention we obtain

$$\begin{aligned} T_q\big(Q(\zeta^{-i} - \zeta^{i'})\big) &= \frac{q}{p}\Big(pA_i - \sum_{j\equiv i \pmod{q/p}} A_j + \sum_{j\equiv i \pmod{q/p}} \big(pA_j - \sum_{s\equiv j \pmod{q/p}} A_s\big)\Big) \\ &= \frac{q}{p}\Big(pA_i + (p-1)\sum_{j\equiv i \pmod{q/p}} A_j - (p-1)\sum_{s\equiv i \pmod{q/p}} A_s\Big) = qA_i \end{aligned}$$

and (7) yields

$$\begin{aligned} q^2 A_i^{\mathrm{t}} A_j &= \sum_{\gamma,\delta\in\mathcal{G}} (\zeta^{-i\gamma} - \zeta^{i'\gamma})(\zeta^{j\delta} - \zeta^{-j'\delta})\gamma(Q)^{\mathrm{t}}\delta(\overline{Q}) \\ &= \sum_{\delta\in\mathcal{N}}\sum_{\gamma\in\mathcal{G}} (\zeta^{-i\gamma} - \zeta^{i'\gamma})(\zeta^{j\gamma\delta} - \zeta^{-j'\gamma\delta}) qCP_\delta \\ &= qC\sum_{\delta\in\mathcal{N}} P_\delta T_q\big(\zeta^{j\delta-i} - \zeta^{j\delta+i'} - \zeta^{-j'\delta-i} + \zeta^{-j'\delta+i'}\big) \end{aligned}$$

for $1 \le i, j \le \varphi(q)$. Note that

$$j\delta - i \equiv j\delta + i' \equiv -j'\delta - i \equiv -j'\delta + i' \pmod{q/p}.$$

Moreover, if $j\delta - i \equiv 0 \pmod q$, then $j\delta + i' \not\equiv 0 \pmod q$. In this case $T_q(\zeta^{j\delta-i} - \zeta^{j\delta+i'}) = \varphi(q) + q/p = q$. In a similar way we obtain

$$\boxed{A_i^{\mathrm{t}} A_j = C \sum_{\delta \in \mathcal{N}} P_\delta \big([j\delta \equiv i] - [j\delta \equiv -i'] + [j'\delta \equiv i'] - [j'\delta \equiv -i]\big)} \tag{8}$$

where all congruences are modulo q and $[. \equiv .]$ evaluates to 1 if the congruence is fulfilled and to 0 otherwise.

By Lemma 4, $\mathcal{A}_q$ has non-zero rows $a_1, \ldots, a_{k_0(B)}$. If $\mathcal{W} \in \mathbb{R}^{l\varphi(q) \times l\varphi(q)}$ is integral positive definite, then

$$k_0(B) \le \sum_{i=1}^{k_0(B)} a_i \mathcal{W} a_i^{\mathrm{t}} \le \operatorname{tr}(\mathcal{A}_q \mathcal{W} \mathcal{A}_q^{\mathrm{t}}) = \operatorname{tr}(\mathcal{W} \mathcal{A}_q^{\mathrm{t}} \mathcal{A}_q)$$

and this is what we are going to show. We need to discuss the case $p = 2$ separately.

Proposition 8. *Theorem B holds for $p = 2$.*

Proof. If $q \le 2$, then $Q = A_1 = \mathcal{A}_q$, $n = 1$ and

$$k_0(B) \le \operatorname{tr}(WQ^{\mathrm{t}}Q) = \operatorname{tr}(WqC) = q \operatorname{tr}(WC) = k_0(\langle u \rangle \rtimes \mathcal{N}) \operatorname{tr}(WC).$$

Hence, we will assume for the remainder of the proof that $q \ge 4$. Then $i' = q/2 - i$ for every $1 \le i \le \varphi(q) = q/2$. Hence, (8) simplifies to

$$A_i^{\mathrm{t}} A_j = 2C \sum_{\delta \in \mathcal{N}} P_\delta \big([j\delta \equiv i] - [j\delta \equiv i + q/2]\big). \tag{9}$$

It is well-known that

$$\mathcal{G} = \langle -1 + q\mathbb{Z} \rangle \times \langle 5 + q\mathbb{Z} \rangle \cong C_2 \times C_{q/4}.$$

In particular, $\mathcal{N}$ is a 2-group and so is $U := \langle u \rangle \rtimes \mathcal{N}$. Therefore, $k_0(U) = |U : U'|$ where U' denotes the commutator subgroup of U.

Case 1: $\mathcal{N} = \langle 5^{2^m} + q\mathbb{Z} \rangle$ for some $m \ge 0$.
Then $q = |\mathcal{N}| 2^{m+2} = n 2^{m+2}$ and U' is generated by $u^{5^{2^m} - 1}$. Since $5^{2^m} - 1 \equiv 2^{m+2} \pmod{2^{m+3}}$, we conclude that $|U'| = n$ and $k_0(U) = |U : U'| = q$.

For any given $\delta \in \mathcal{N} \setminus \{1\}$ both congruences $i\delta \equiv i \pmod q$ and $i\delta \equiv i + q/2 \pmod q$ have solutions $i \in \{1, \ldots, q/2\}$. Moreover, the number of solutions is the same, since they both form residue classes modulo a common integer. On the other hand, $i\delta \equiv i + q/2 \pmod q$ has no solution for $\delta = 1$. An application of (9) yields

$$\sum_{i=1}^{q/2} A_i^{\mathrm{t}} A_i = 2C \sum_{\delta \in \mathcal{N}} P_\delta \sum_{i=1}^{q/2} [i\delta \equiv i] - [i\delta \equiv i + q/2] = qCP_1 = qC.$$

The matrix $\mathcal{W} := 1_{q/2} \otimes W$ is certainly integral positive definite. Moreover,

$$k_0(B) \le \operatorname{tr}(\mathcal{W} \mathcal{A}_q^{\mathrm{t}} \mathcal{A}_q) = \operatorname{tr}\Big(\sum_{i=1}^{q/2} W A_i^{\mathrm{t}} A_i\Big) = q \operatorname{tr}(WC) = k_0(U) \operatorname{tr}(WC). \tag{10}$$

It remains to check when this bound is sharp. If $k_0(B) = \operatorname{tr}(\mathcal{W}\mathcal{A}_q^{\mathrm{t}}\mathcal{A}_q)$, then every row of $\mathcal{A}_q$ vanishes in all but (possibly) one A_i. Moreover, characters of positive height vanish completely in $\mathcal{A}_q$. By way of contradiction, suppose that $\mathcal{N}$ acts non-trivially on $\operatorname{IBr}(b)$. Using (5), it follows that there exists a character $\chi \in \operatorname{Irr}(B)$ of height 0 such that the corresponding row $d_\chi = a\zeta^i$ of Q satisfies $aP_\delta = -a$ for some $\delta \in \mathcal{N}$. We write $a = (\alpha_1, \ldots, \alpha_s, -\alpha_1, \ldots, -\alpha_s, 0, \ldots, 0)$ with non-zero $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}$. With the notation of Lemma 4 let $\widetilde{C} = (\widetilde{c}_{ij})$. By (6), we have $P_\delta\widetilde{C} = \widetilde{C}P_\delta$. Now Lemma 4 leads to the contradiction

$$0 \not\equiv d_\chi\widetilde{C}\overline{d_\chi}^{\mathrm{t}} = a\widetilde{C}a^{\mathrm{t}} \equiv \sum_{i=1}^{s} 2\alpha_i^2\widetilde{c}_{ii} \equiv 0 \pmod 2,$$

since the diagonal of $\widetilde{C}$ is constant on the orbits of $\mathcal{N}$. Therefore, equality in (10) can only hold if $\mathcal{N}$ acts trivially on $\operatorname{IBr}(b)$.

Case 2: $\delta := -5^m + q\mathbb{Z} \in \mathcal{N} \setminus \{1\}$ for some $m \ge 0$.
Since $1 + 5^m \equiv 2 \pmod 4$, we have $U' = \langle u^{1+5^m}\rangle = \langle u^2\rangle$ and $k_0(U) = |U : U'| = 2n$. We show that every row of $A_{q/2}$ corresponding to a height 0 character $\chi \in \operatorname{Irr}(B)$ is non-zero. Let $d_\chi = \sum_{i=1}^{q/2} a_i\zeta^i$ be the corresponding row of Q where a_i is a row of A_i. Let ν be the p-adic valuation. By Lemma 4,

$$0 = \nu(d_\chi\widetilde{C}\overline{d_\chi}^{\mathrm{t}}) = \nu\Big(\sum_{1\le i,j\le q/2} a_i\widetilde{C}a_j^{\mathrm{t}}\zeta^{i-j}\Big) = \nu\Big(\sum_{i=1}^{q/2} a_i\widetilde{C}a_i^{\mathrm{t}}\Big),$$

i. e.

$$\sum_{i=1}^{q/2} a_i\widetilde{C}a_i^{\mathrm{t}} \equiv 1 \pmod 2. \tag{11}$$

On the other hand,

$$\sum_{i=1}^{q/2} a_iP_\delta\zeta^i = d_\chi P_\delta = \delta(d_\chi) = \sum_{i=1}^{q/2} a_i\zeta^{i\delta}.$$

Now $i\delta \equiv i \pmod q$ implies $-5^m \equiv \delta \equiv 1 \pmod{q/\gcd(q,i)}$ and $i = q/2$. Similarly $i\delta \equiv i + q/2 \pmod q$ implies $i = q/4$. Then $A_{q/4}P_\delta = -A_{q/4}$. As in Case 1, it follows that $a_{q/4}\widetilde{C}a_{q/4}^{\mathrm{t}} \equiv 0 \pmod 2$. For $i \notin \{q/2, q/4\}$ we have $A_iP_\delta = \pm A_j$ for some $j \in \{1, \ldots, q/2\} \setminus \{i\}$. Then, using (6),

$$a_j\widetilde{C}a_j^{\mathrm{t}} = a_iP_\delta\widetilde{C}P_\delta^{\mathrm{t}}a_i^{\mathrm{t}} = a_i\widetilde{C}a_i^{\mathrm{t}}.$$

Now (11) yields $a_{q/2}\widetilde{C}a_{q/2}^{\mathrm{t}} \equiv 1 \pmod 2$ and $a_{q/2} \ne 0$. Therefore, $A_{q/2}$ has non-zero rows for height 0 characters.

By (9), $A_{d/2}^{\mathrm{t}}A_{d/2} = 2CP_{\mathcal{N}}$ and Lemma 2 implies

$$k_0(B) \le \operatorname{tr}(WA_{d/2}^{\mathrm{t}}A_{d/2}) = 2\operatorname{tr}(WCP_{\mathcal{N}}) = 2\sum_{\gamma\in\mathcal{N}} \operatorname{tr}(WCP_\gamma) \le 2n\operatorname{tr}(WC) = k_0(U)\operatorname{tr}(WC)$$

with strict inequality if $\mathcal{N}$ acts non-trivially on $\operatorname{IBr}(b)$. □

We are left with the case $p > 2$. Here $\mathcal{G}$ is cyclic and $\mathcal{N}$ is uniquely determined by n. Let n_p be the p-part of n and $n_{p'}$ the p'-part. Then $n_p \mid \frac{q}{p}$ and $n_{p'} \mid p - 1$.

Lemma 9. *We have* $k_0\big(\langle u\rangle \rtimes \mathcal{N}\big) = n + \frac{q-n_p}{n_{p'}}$ *for* $p > 2$.

Proof. The inflations from $\mathcal{N}$ yield n linear characters in $U := \langle u\rangle \rtimes \mathcal{N}$, since $\mathcal{N}$ is cyclic. Now let $1 \ne \lambda \in \mathrm{Irr}(\langle u\rangle)$. If the orbit size of λ under $\mathcal{N}$ is divisible by p, then the irreducible characters of U lying over λ all have positive height. Hence, we may assume that $\lambda^{q/n_p} = 1$. Then, by Clifford theory, λ extends in n_p many ways to $\langle u\rangle \rtimes \mathcal{N}_p$ where $\mathcal{N}_p$ is the Sylow p-subgroup of $\mathcal{N}$. All these extensions induce to irreducible characters of U of height 0. We have $\frac{q/n_p-1}{n_{p'}}$ choices for λ. Thus, in total we obtain

$$k_0(U) = n + n_p\frac{q/n_p - 1}{n_{p'}} = n + \frac{q - n_p}{n_{p'}}. \qquad \square$$

The following settles Theorem B in the special case $n_p = 1$ (use Lemma 9).

Proposition 10. *Let $p > 2$ and $n_p = 1$. With the notation above there exists an integral positive definite matrix $\mathcal{W} \in \mathbb{R}^{\varphi(q)l\times\varphi(q)l}$ such that*

$$\mathrm{tr}(\mathcal{W}\mathcal{A}_q^t\mathcal{A}_q) \le \big(n + \frac{q-1}{n}\big)\,\mathrm{tr}(WC)$$

with equality if and only if $\mathcal{N}$ acts trivially on $\mathrm{IBr}(b)$.

Proof. We argue by induction on q. If $q = 1$, then $\mathcal{A}_q = A_1 = Q$, $n = 1$ and the claim holds with $\mathcal{W} = W$ (Lemma 5). The next case requires special treatment as well.

Case 1: $q = p$.
Then $i' = 0$ for all i and (8) simplifies to

$$A_i^{\mathrm{t}}A_j = C\sum_{\delta\in\mathcal{N}} P_\delta\big([j\delta \equiv i] + [0\delta \equiv 0]\big) = \begin{cases} CP_{\mathcal{N}} & \text{if } i \not\equiv j \pmod{\mathcal{N}},\\ C(P_{\mathcal{N}} + P_{j^{-1}i}) & \text{if } i \equiv j \pmod{\mathcal{N}}.\end{cases}$$

After permuting the columns of $\mathcal{A}_q$ if necessary, we obtain

$$\mathcal{A}_q^{\mathrm{t}}\mathcal{A}_q = 1^{\varphi(q)\times\varphi(q)} \otimes P_{\mathcal{N}}C + 1_{n'} \otimes (P_{\gamma^{-1}\delta}C)_{\gamma,\delta\in\mathcal{N}}$$

where $n' := (p-1)/n$. We fix a generator ρ of $\mathcal{N}$. Then we may write $(P_{\gamma^{-1}\delta}C)_{\gamma,\delta\in\mathcal{N}} = (P_\rho^{j-i}C)_{i,j=1}^n$.
By Lemma 5, we may assume that W is (integral) positive definite and commutes with P_ρ. Let W_n as in Lemma 3 where we use P_ρ instead of P. A repeated application of that lemma shows that the matrix $\mathcal{W} := U_{n'} \otimes W_n$ is integral positive definite. Moreover, since $P_{\mathcal{N}}P_\rho = P_{\mathcal{N}} = P_{\mathcal{N}}P_\rho^{\mathrm{t}}$, we have

$$\begin{aligned}
\mathrm{tr}(\mathcal{W}\mathcal{A}_q^{\mathrm{t}}\mathcal{A}_q) &= \mathrm{tr}\big((U_{n'} \otimes W_n)(1^{\varphi(q)\times\varphi(q)} \otimes P_{\mathcal{N}}C)\big) + \mathrm{tr}\big((U_{n'} \otimes W_n)(1_{n'} \otimes (P_\rho^{j-i}C))\big)\\
&= \mathrm{tr}\big((U_{n'} \otimes W_n)(1^{n'\times n'} \otimes 1^{n\times n} \otimes P_{\mathcal{N}}C)\big) + \mathrm{tr}\big(U_{n'} \otimes W_n(P_\rho^{j-i}C)\big)\\
&= \mathrm{tr}\big(U_{n'}1^{n'\times n'}\big)\,\mathrm{tr}\big(W_n(1^{n\times n} \otimes P_{\mathcal{N}}C)\big) + \mathrm{tr}(U_{n'})\,\mathrm{tr}\big(W_n(P_\rho^{j-i}C)\big)\\
&= \mathrm{tr}\big(W_n(1^{n\times n} \otimes P_{\mathcal{N}}C)\big) + n'\,\mathrm{tr}\big(W_n(P_\rho^{j-i}C)\big)\\
&= \sum_{i=1}^{n}\mathrm{tr}(WCP_{\mathcal{N}}) - \sum_{i=1}^{n-1}\mathrm{tr}(WCP_{\mathcal{N}}P_\rho) + n'\Big(\sum_{i=1}^{n}\mathrm{tr}(WC) - \sum_{i=1}^{n-1}\mathrm{tr}(WCP_\rho P_\rho^{\mathrm{t}})\Big)\\
&= \mathrm{tr}(WCP_{\mathcal{N}}) + n'\,\mathrm{tr}(WC).
\end{aligned}$$

Finally, Lemma 2 implies

$$\mathrm{tr}(WCP_{\mathcal{N}}) = \sum_{\delta\in\mathcal{N}}\mathrm{tr}(WCP_\delta) \le n\,\mathrm{tr}(WC)$$

with equality if and only if $\mathcal{N}$ acts trivially on $\mathrm{IBr}(b)$. This completes the proof in the case $q = p$.

Case 2: $q > p$.
Let

$$I_p := \{1 \le i \le \varphi(q) : p \mid i\}, \qquad\qquad I_{p'} := \{1 \le i \le \varphi(q) : p \nmid i\}.$$

Then $|I_p| = \varphi(q)/p = \varphi(q/p)$ and $|I_{p'}| = \varphi(q) - \varphi(q/p) = \varphi(q/p)(p-1)$. If $i \in I_p$ and $j \in I_{p'}$, then $j\delta - i \not\equiv 0 \pmod{q/p}$ for every $\delta \in \mathcal{N}$ and $A_i^{\mathrm{t}}A_j = 0$ by (8). Hence, after relabeling the columns of $\mathcal{A}_q$, we obtain

$$\mathcal{A}_q^{\mathrm{t}}\mathcal{A}_q = \begin{pmatrix} \Delta_p & 0 \\ 0 & \Delta_{p'} \end{pmatrix}$$

where Δ_p corresponds to the indices in I_p. Since $n \mid p-1$, we may regard $\mathcal{N}$ as a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta^p)|\mathbb{Q})$. For $i \in I_p$ let $j = i/p$. Then $i' \equiv -i \pmod{q/p}$ implies $i'/p \equiv -j \pmod{q/p^2}$ and $0 \le i'/p < q/p^2$. Hence, $j' = i'/p$ where the left hand side refers to q/p. It follows from (8) that $\Delta_p = \mathcal{A}_{q/p}^{\mathrm{t}}\mathcal{A}_{q/p}$. By induction on q there exists an integral positive definite $\mathcal{W}_p$ such that

$$\mathrm{tr}(\mathcal{W}_p\Delta_p) \le \Bigl(n + \frac{q/p - 1}{n}\Bigr)\,\mathrm{tr}(WC)$$

with equality if and only if $\mathcal{N}$ acts trivially on $\mathrm{IBr}(b)$.

It remains to consider $\Delta_{p'}$. By Lemma 6, $\mathcal{A}_{q/p}$ and Δ_p have rank $l\varphi(q/p)/n$ and therefore $\Delta_{p'}$ has rank

$$l(\varphi(q) - \varphi(q/p))/n = l\varphi(q/p)(p-1)/n.$$

We define a subset $J \subseteq I_{p'}$ such that $|J| = \varphi(q/p)(p-1)/n$ and the matrix $(A_i : i \in J)$ has full rank. Let R be a set of representatives for the orbits of $\{i \in I_{p'} : 1 \le i \le q/p\}$ under the multiplication action of $\mathcal{N}$ modulo q/p. Note that every orbit has size n. For $r \in R$ let

$$J_r := \{r + jq/p : j = 0, \ldots, p-2\} \subseteq I_{p'}$$

and $J := \bigcup_{r \in R} J_r$. Since $J_r \cap J_s = \varnothing$ for $r \ne s$, we have $|J| = \varphi(q/p)(p-1)/n$. If $i \in J_r$ and $j \in J_s$ with $r \ne s$, then $j\delta \not\equiv i \pmod{q/p}$ for every $\delta \in \mathcal{N}$. Consequently, $A_i^{\mathrm{t}}A_j = 0$. Now let $i, j \in J_r$. Then (8) implies

$$A_i^{\mathrm{t}}A_j = C(1 + \delta_{ij}).$$

After relabeling we obtain

$$(A_i : i \in J)^{\mathrm{t}}(A_i : i \in J) = 1_{\varphi(q/p)/n} \otimes (1 + \delta_{ij})_{i,j=1}^{p-1} \otimes C.$$

In particular, $(A_i : i \in J)$ has full rank. Since $\Delta_{p'}$ has the same rank, there exists an integral matrix $S \in \mathrm{GL}(l\varphi(q/p)(p-1), \mathbb{Q})$ such that

$$S^{\mathrm{t}}\Delta_{p'}S = 1_{\varphi(q/p)/n} \otimes (1 + \delta_{ij}) \otimes C \oplus 0_s$$

where $s := l\varphi(q/p)(p-1)(n-1)/n$. Let

$$\mathcal{W}_{p'} := S\bigl(1_{\varphi(q/p)/n} \otimes U_{p-1} \otimes W \oplus 1_s\bigr)S^{\mathrm{t}}.$$

Then $\mathcal{W}_{p'}$ is integral positive definite by Lemma 3. Moreover,

$$\begin{aligned}\mathrm{tr}(\mathcal{W}_{p'}\Delta_{p'}) &= \mathrm{tr}\bigl((1_{\varphi(q/p)/n} \otimes U_{p-1} \otimes W)(1_{\varphi(q/p)/n} \otimes (1 + \delta_{ij}) \otimes C)\bigr) + \mathrm{tr}(1_s 0_s) \\ &= \frac{\varphi(q/p)}{n}\,\mathrm{tr}\bigl(U_{p-1}(1 + \delta_{ij})\bigr)\,\mathrm{tr}(WC) = \frac{\varphi(q/p)p}{n}\,\mathrm{tr}(WC) = \frac{\varphi(q)}{n}\,\mathrm{tr}(WC).\end{aligned}$$

Finally, we set $\mathcal{W} := \mathcal{W}_p \oplus \mathcal{W}_{p'}$. Then $\mathcal{W}$ is integral positive definite and

$$\begin{aligned}\operatorname{tr}(\mathcal{W}\mathcal{A}_q^{\mathrm{t}}\mathcal{A}_q) &= \operatorname{tr}(\mathcal{W}_p\Delta_p) + \operatorname{tr}(\mathcal{W}_{p'}\Delta_{p'}) \le \Big(n + \frac{q/p-1}{n}\Big)\operatorname{tr}(WC) + \frac{\varphi(q)}{n}\operatorname{tr}(WC)\\ &= \Big(n + \frac{q-1}{n}\Big)\operatorname{tr}(WC)\end{aligned}$$

with equality if and only if $\mathcal{N}$ acts trivially on $\operatorname{IBr}(b)$. □

To complete the proof of Theorem B it remains to show the following.

Proposition 11. *Theorem B holds in the case $p > 2$ and $n_p > 1$.*

Proof. Let

$$I_1 := \{1 \le i \le \varphi(q) : n_p \mid i\}, \qquad I_2 := \{1 \le i \le \varphi(q) : n_p \nmid i\}.$$

As in the proof of Proposition 10 we have

$$\mathcal{A}_q^{\mathrm{t}}\mathcal{A}_q = \begin{pmatrix}\Delta_1 & 0\\ 0 & \Delta_2\end{pmatrix}$$

where Δ_1 corresponds to the indices in I_1. Let $\mathcal{N} = \mathcal{N}_p \times \mathcal{N}_{p'}$ where $\mathcal{N}_p := \langle 1 + q/n_p + q\mathbb{Z}\rangle$ is the unique Sylow p-subgroup of $\mathcal{N}$. Then $\delta i \equiv i \pmod q$ for $\delta \in \mathcal{N}_p$ and $i \in I_1$. Hence, for $i, j \in I_1$ we have

$$\begin{aligned}A_i^{\mathrm{t}}A_j &= C\sum_{\delta\in\mathcal{N}} P_\delta\big([j\delta \equiv i] - [j\delta \equiv -i'] + [j'\delta \equiv i'] - [j'\delta \equiv -i]\big)\\ &= CP_{\mathcal{N}_p}\sum_{\delta\in\mathcal{N}_{p'}} P_\delta\big([j\delta \equiv i] - [j\delta \equiv -i'] + [j'\delta \equiv i'] - [j'\delta \equiv -i]\big).\end{aligned}$$

For $i \in I_1$ it is easy to see that $i'/n_p = (i/n_p)'$ when the right hand side is considered with respect to q/n_p (see proof of Proposition 10). It follows that

$$\Delta_1 = (1_{\varphi(q/n_p)} \otimes P_{\mathcal{N}_p})\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p}$$

where we consider $\mathcal{A}_{q/n_p}$ with respect to the p'-group $\mathcal{N}_{p'}$. By Proposition 10, there exists an integral positive definite $\mathcal{W}_1$ such that

$$\operatorname{tr}(\mathcal{W}_1\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p}) \le \Big(n_{p'} + \frac{q/n_p - 1}{n_{p'}}\Big)\operatorname{tr}(WC). \tag{12}$$

Moreover, equality holds if and only if $\mathcal{N}_{p'}$ acts trivially on $\operatorname{IBr}(b)$. By construction, $\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p}$ is positive semidefinite. By (6) and (8), $\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p}$ commutes with $1_{\varphi(q/n_p)} \otimes P_\delta$ for $\delta \in \mathcal{N}_p$. Hence, Lemma 2 implies

$$\begin{aligned}\operatorname{tr}(\mathcal{W}_1\Delta_1) &= \operatorname{tr}\big(\mathcal{W}_1(1_{\varphi(q/n_p)} \otimes P_{\mathcal{N}_p})\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p}\big)\\ &\le n_p\operatorname{tr}(\mathcal{W}_1\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p}) \le \Big(n + \frac{q-n_p}{n_{p'}}\Big)\operatorname{tr}(WC).\end{aligned} \tag{13}$$

Suppose that $\operatorname{tr}(\mathcal{W}_1\Delta_1) = \big(n + \frac{q-n_p}{n_{p'}}\big)\operatorname{tr}(WC)$. Then, by (12), $\mathcal{N}_{p'}$ acts trivially on $\operatorname{IBr}(b)$ and the matrices $A_i^{\mathrm{t}}A_j$ with $i, j \in I_1$ are scalar multiples of $CP_{\mathcal{N}_p}$. We write $\mathcal{A}_{q/n_p}^{\mathrm{t}}\mathcal{A}_{q/n_p} = (A_{ij})$ such that

$A^{\mathrm{t}}_{in_p}A_{jn_p} = P_{\mathcal{N}_p}A_{ij}$. Note that $A_{11} = 2C$ is positive definite. As in the proof of Lemma 2, we construct a positive semidefinite matrix $M = (m_{ij}) := A^{1/2}\mathcal{W}_1A^{1/2}$ where $A^{1/2}A^{1/2} = (A_{ij})_{i,j}$. By way of contradiction, suppose that $P_\delta \ne 1_l$ for some $\delta \in \mathcal{N}_p$. Let $1 \le i \le l$ such that $\delta(i) \ne i$, and let $x = (x_j) \in \mathbb{Z}^{\varphi(q/n_p)l}$ with $x_i = -x_{\delta(i)} = 1$ and zero elsewhere. Then $x(A_{ij})x^{\mathrm{t}} > 0$ since A_{11} is positive definite. Thus, $A^{1/2}x^{\mathrm{t}} \ne 0$. Since $\mathcal{W}_1$ is positive definite (Lemma 1), it follows that $xMx^{\mathrm{t}} > 0$ and $m_{i\delta(i)} < (m_{ii} + m_{\delta(i)\delta(i)})/2$. Hence, the proof of Lemma 2 leads to

$$\begin{aligned}\operatorname{tr}\big(\mathcal{W}_1(1_{\varphi(q/n_p)} \otimes P_\delta)\mathcal{A}^{\mathrm{t}}_{q/n_p}\mathcal{A}_{q/n_p}\big) &= \operatorname{tr}(A^{1/2}\mathcal{W}_1(1_{\varphi(q/n_p)} \otimes P_\delta)A^{1/2})\\ &= \operatorname{tr}(M(1_{\varphi(q/n_p)} \otimes P_\delta)) < \operatorname{tr}(M) = \operatorname{tr}(\mathcal{W}_1\mathcal{A}^{\mathrm{t}}_{q/n_p}\mathcal{A}_{q/n_p})\end{aligned}$$

and we derive the contradiction $\operatorname{tr}(\mathcal{W}_1\Delta_1) < n_p \operatorname{tr}(\mathcal{W}_1\mathcal{A}^{\mathrm{t}}_{q/n_p}\mathcal{A}_{q/n_p})$. Thus, we have shown that equality in (13) can only hold if $\mathcal{N}$ acts trivially on $\operatorname{IBr}(b)$.

Now we use the argument from Proposition 8 to deal with Δ_2. Let $\chi \in \operatorname{Irr}(B)$ of height 0, and let $d_\chi = \sum_{i=1}^{\varphi(q)} a_i\zeta^i$ be the corresponding row of Q. By Lemma 4, we have

$$0 = \nu(d_\chi\widetilde{C}\overline{d_\chi}^{\mathrm{t}}) = \nu\Big(\sum_{i,j=1}^{\varphi(q)} a_i\widetilde{C}a_j^{\mathrm{t}}\Big)$$

where ν is the p-adic valuation. In order to show that $a_i \ne 0$ for some $i \in I_1$, it suffices to show that

$$\sum_{i,j\in I_2} a_i\widetilde{C}a_j^{\mathrm{t}} \equiv 0 \pmod p. \tag{14}$$

For any $\delta \in \mathcal{N}_p$ we have

$$\sum_{i=1}^{\varphi(q)} A_iP_\delta\zeta^i = QP_\delta = \delta(Q) = \sum_{i=1}^{\varphi(q)} A_i\zeta^{i\delta}.$$

Restricting to the indices $i \in I_2$ and taking the valuation yields

$$\sum_{i\in I_2} A_iP_\delta \equiv \sum_{i\in I_2} A_i \pmod p.$$

Let $i \in I_2$ be arbitrary and choose $\delta \in \mathcal{N}_p$ such that $\gcd(q,i)p = |\langle\delta\rangle|$. Let

$$\{i_1,\ldots,i_{p-1}\} = \big\{j \in I_2 : j \equiv i \pmod{q/p}\big\}.$$

We may assume that $i_1\delta \equiv -i' \pmod q$ and $i_j\delta \equiv i_{j-1} \pmod q$ for $j = 2,\ldots,p-1$. Since $\zeta^{-i'} = -\zeta^{i_1} - \ldots - \zeta^{i_{p-1}}$, we obtain $A_{i_{p-1}}P_\delta = -A_{i_1}$ and $A_{i_j}P_\delta = A_{i_{j+1}} - A_{i_1}$ for $j = 1,\ldots,p-2$. Hence,

$$\begin{aligned}\Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}a_{i_1}^{\mathrm{t}} &= \Big(\sum_{j\in I_2} a_j\Big)P_\delta\widetilde{C}P_\delta^{\mathrm{t}}a_{i_1}^{\mathrm{t}} \equiv \Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}(a_{i_2} - a_{i_1})^{\mathrm{t}} \equiv \Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}(a_{i_3} - a_{i_2})^{\mathrm{t}}\\ &\equiv \ldots \equiv \Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}(a_{i_{p-1}} - a_{i_{p-2}})^{\mathrm{t}} \equiv -\Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}a_{i_{p-1}}^{\mathrm{t}} \pmod p.\end{aligned}$$

Now it is easy to see that

$$\Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}(a_{i_1} + \ldots + a_{i_{p-1}})^{\mathrm{t}} \equiv \frac{p(p-1)}{2}\Big(\sum_{j\in I_2} a_j\Big)\widetilde{C}a_{i_1}^{\mathrm{t}} \equiv 0 \pmod p$$

and (14) follows. Thus, we have shown that every height 0 character has a non-vanishing part in A_i for some $i \in I_1$. Hence by (13),

$$k_0(B) \le \operatorname{tr}(\mathcal{W}_1\Delta_1) \le \Bigl(n + \frac{q - n_p}{n_{p'}}\Bigr) \operatorname{tr}(WC)$$

with strict inequality if $\mathcal{N}$ acts non-trivially on $\operatorname{IBr}(b)$. By Lemma 9, the proof is complete. □

Now it is time to derive Theorem A from Theorem B. For the convenience of the reader we restate it as follows.

Proposition 12. *If $u \in \mathrm{Z}(D)$ in the situation above, then*

$$k(B) \le \Bigl(n + \frac{q-1}{n}\Bigr) \operatorname{tr}(WC) \le q \operatorname{tr}(WC).$$

The first inequality is strict if $\mathcal{N}$ acts non-trivially on $\operatorname{IBr}(b)$ and the second inequality is strict if and only if $1 < n < q - 1$.

Proof. As mentioned in the introduction, the inertial quotient $\mathrm{N}_G(D, b_D)/D\mathrm{C}_G(D)$ restricts to $\mathcal{N}$ and therefore $\mathcal{N}$ is a p'-group. As a subgroup of $\operatorname{Aut}(\langle u\rangle)$, its order n must divide $p - 1$. For $p = 2$ we obtain $n = 1$ and $k_0(\langle u\rangle \rtimes \mathcal{N}) = q$. For $p > 2$, Lemma 9 gives $k_0(\langle u\rangle \rtimes \mathcal{N}) = n + \frac{q-1}{n}$. By Lemma 4, all rows of Q are non-zero. Hence, the proofs of Propositions 8 and 10 actually show that $k(B) \le k_0(\langle u\rangle \rtimes \mathcal{N}) \operatorname{tr}(WC)$ with strict inequality if $\mathcal{N}$ acts non-trivially on $\operatorname{IBr}(b)$ (note that only Case 1 in the proof of Proposition 8 is relevant). This implies the first two claims. The last claim follows, since $n + \frac{q-1}{n}$ is a convex function in n and $1 \le n \le q - 1$. □

If the action of $\mathcal{N}$ on $\operatorname{IBr}(b)$ is known, a careful analysis of the proofs above leads to even stronger estimates. For instance, in Proposition 10 we have actually shown that

$$k_0(B) \le \operatorname{tr}(WCP_{\mathcal{N}}) + \frac{q-1}{n} \operatorname{tr}(WC)$$

for $p > 2$ and $n_p = 1$. If $\bar{b}$ has cyclic defect groups, then $P_{\mathcal{N}}$ is a direct sum of equal blocks of the form $d^{n/d \times n/d}$ (see [18, Proposition 3.2]). This can be used to give a simpler proof of [18, Theorem 3.1].

3 Consequences

In this section we deduce some of the results stated in the introduction.

Corollary 13 (Sambale [14, Lemma 1])**.** *Let $C = (c_{ij})_{i,j=1}^{l}$ be the Cartan matrix of a Brauer correspondent of B in $\mathrm{C}_G(u)$ where $u \in \mathrm{Z}(D)$. Then for every positive definite, integral quadratic form $q(x_1, \ldots, x_l) = \sum_{1 \le i \le j \le l} q_{ij} x_i x_j$ we have*

$$k(B) \le \sum_{1 \le i \le j \le l} q_{ij} c_{ij}.$$

Proof. Let $t := |\langle u\rangle|$. Then $t^{-1}C$ is the Cartan matrix of the block $\overline{b}$ in Theorem A (see [16, Theorem 1.22]). Taking $W := \frac{1}{2}(q_{ij}(1+\delta_{ij}))$ with $q_{ij} = q_{ji}$ we obtain

$$xWx^{\mathrm{t}} = \frac{1}{2}\sum_{1\le i,j\le l} q_{ij}(1+\delta_{ij})x_ix_j = \sum_{1\le i\le j\le l} q_{ij}x_ix_j = q(x) \ge 1$$

for every $x = (x_1,\ldots,x_l) \in \mathbb{Z}^l \setminus \{0\}$ and

$$k(B) \le t\,\mathrm{tr}(Wt^{-1}C) = \mathrm{tr}(WC) = \sum_{1\le i\le j\le l} q_{ij}c_{ij}.$$ □

Wada's inequality (2) follows from Corollary 13 with $q(x) = \sum_{i=1}^{l} x_i^2 - \sum_{i=1}^{l-1} x_ix_{i+1}$ (or $W = U_l$ in Theorem A).

Corollary 14 (Héthelyi–Külshammer–Sambale [9, Theorem 4.10])**.** *Suppose $p > 2$. Let b be a Brauer correspondent of B in $\mathrm{C}_G(u)$ where $u \in D$ and $l(b) = 1$. Let $|\mathrm{N}_G(\langle u\rangle, b) : \mathrm{C}_G(u)| = p^sr$ with $s \ge 0$ and $p \nmid r$. Then*

$$k_0(B) \le \frac{|\langle u\rangle| + p^s(r^2-1)}{|\langle u\rangle| r} p^d$$

where d is the defect of b.

Proof. Setting $q := |\langle u\rangle|$ we obtain $C = (p^d/q)$ in the situation of Theorem B. By Lemma 9, $k_0(\langle u\rangle \rtimes \mathcal{N}) = (q + p^s(r^2-1))/r$ and the claim follows with $W = (1)$. □

The following result of Brauer cannot be seen in the framework of integral quadratic forms. It was a crucial ingredient in the proof of the $k(GV)$-Problem (see [19, Theorem 2.5d]).

Corollary 15 (Brauer [5, 5D])**.** *Let B be a p-block with defect d, and let C be the Cartan matrix of a Brauer correspondent b of B in $\mathrm{C}_G(u)$ where $u \in \mathrm{Z}(D)$. Then $k(B) \le l(b)/m \le l(b)p^d$ where*

$$m := \min\bigl\{xC^{-1}x^{\mathrm{t}} : x \in \mathbb{Z}^{l(b)} \setminus \{0\}\bigr\}.$$

Proof. By the definition of m, the matrix $W := \frac{1}{m}C^{-1}$ is integral positive definite. Theorem A gives $k(B) \le \mathrm{tr}(WC) = l(b)/m$. For the second inequality we recall that the elementary divisors of C divide p^d. Hence, p^dC^{-1} has integral entries and $m \ge p^{-d}$. □

In [16], we referred to the *Cartan method* and the *inverse Cartan method* when applying Corollary 13 and Corollary 15 respectively. Now we know that both methods are special cases of a single theorem. In fact, the following examples show that Theorem A is stronger than Corollary 13 and Corollary 15:

(i) Let B be the principal 2-block of the affine semilinear group $G = \mathrm{A\Gamma L}(1,8)$, and let $u = 1$. Then

$$C = \begin{pmatrix} 2 & . & . & 1 & 1\\ . & 2 & . & 1 & 1\\ . & . & 2 & 1 & 1\\ 1 & 1 & 1 & 4 & 3\\ 1 & 1 & 1 & 3 & 4 \end{pmatrix}$$

and $m = \frac{1}{2}$ with the notation of Corollary 15. This implies $k(B) \le 10$. On the other hand, $q(x_1,\ldots,x_5) = x_1^2 + \ldots + x_5^2 + x_1x_2 - x_1x_5 - x_2x_5 - x_3x_5 - x_4x_5$ in Corollary 13 gives $k(B) \le 8$ and in fact equality holds (cf. [10, p. 84]).

(ii) Let B be the principal 2-block of $G = A_4 \times A_4$ where A_4 denotes the alternating group of degree 4. Let $u = 1$. Then

$$C = (1 + \delta_{ij})_{i,j=1}^3 \otimes (1 + \delta_{ij})_{i,j=1}^3$$

and $m = 9/16$ with the notation of Corollary 15. Hence, we obtain $k(B) \le 16$ and equality holds. On the other hand, it has been shown in [15, Section 3] that there is no positive definite, integral quadratic form q such that $k(B) \le 16$ in Corollary 13.

We give a final application where the Cartan matrix C is known up to basic sets. It reveals an interesting symmetry in the formula.

Proposition 16. *Let B be a block of a finite group with abelian defect group D and inertial quotient $E \le \mathrm{Aut}(D)$. Suppose that $u \in D$ such that $D/\langle u\rangle$ is cyclic. Then*

$$k(B) \le \Bigl(|\mathrm{N}_E(\langle u\rangle)/\mathrm{C}_E(u)| + \frac{|\langle u\rangle| - 1}{|\mathrm{N}_E(\langle u\rangle)/\mathrm{C}_E(u)|}\Bigr)\Bigl(|\mathrm{C}_E(u)| + \frac{|D/\langle u\rangle| - 1}{|\mathrm{C}_E(u)|}\Bigr) \le |D|.$$

Proof. With the notation of Theorem A we have $\mathcal{N} = \mathrm{N}_E(\langle u\rangle)/\mathrm{C}_E(u)$. Moreover, $\overline{b}$ has defect group $D/\langle u\rangle$ and inertial quotient $\mathrm{C}_E(u)$. By Dade's theorem on blocks with cyclic defect groups, $l(b) = |\mathrm{C}_E(u)|$ and $C = (m + \delta_{ij})$ up to basic sets where $m := (|D/\langle u\rangle| - 1)/l(b)$ (see [16, Theorem 8.6]). With $W = U_{l(b)}$ we obtain

$$\begin{aligned} k(B) &\le \Bigl(|\mathcal{N}| + \frac{|\langle u\rangle - 1}{|\mathcal{N}|}\Bigr)\operatorname{tr}(WC) \\ &= \Bigl(|\mathrm{N}_E(\langle u\rangle)/\mathrm{C}_E(u)| + \frac{|\langle u\rangle| - 1}{|\mathrm{N}_E(\langle u\rangle)/\mathrm{C}_E(u)|}\Bigr)\Bigl(|\mathrm{C}_E(u)| + \frac{|D/\langle u\rangle| - 1}{|\mathrm{C}_E(u)|}\Bigr). \end{aligned}$$

The first factor is at most $|\langle u\rangle|$ and the second factor is bounded by $|D/\langle u\rangle|$. This implies the second inequality. □

Coming back to the initial motivation of this paper, we remark that Theorem A implies Brauer's Conjecture $k(B) \le |D|$ in all examples we have considered.

Acknowledgment

I have been pursuing these formulas since my PhD in 2010 and it has always remained a challenge to prove the most general. The work on this paper was initiated in February 2018 when I received an invitation by Christine Bessenrodt to the representation theory days in Hanover. I thank her for this invitation. The paper was written in summer 2018 while I was an interim professor at the University of Jena. I like to thank the mathematical institute for the hospitality and also my sister's family for letting me stay at their place. Moreover, I appreciate some comments on algebraic number theory by Tommy Hofmann. The work is supported by the German Research Foundation (projects SA 2864/1-1 and SA 2864/3-1).

References

[1] J. L. Alperin and M. Broué, *Local methods in block theory*, Ann. of Math. (2) **110** (1979), 143–157.

[2] M. Aschbacher, R. Kessar and B. Oliver, *Fusion systems in algebra and topology*, London Mathematical Society Lecture Note Series, Vol. 391, Cambridge University Press, Cambridge, 2011.

[3] J. Brandt, *A lower bound for the number of irreducible characters in a block*, J. Algebra **74** (1982), 509–515.

[4] R. Brauer, *On blocks of characters of groups of finite order. II*, Proc. Nat. Acad. Sci. U.S.A. **32** (1946), 215–219.

[5] R. Brauer, *On blocks and sections in finite groups. II*, Amer. J. Math. **90** (1968), 895–925.

[6] R. Brauer and W. Feit, *On the number of irreducible characters of finite groups in a given block*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 361–365.

[7] M. Broué, *On characters of height zero*, in: The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), 393–396, Proc. Sympos. Pure Math., Vol. 37, Amer. Math. Soc., Providence, RI, 1980.

[8] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Sixth edition, Oxford University Press, Oxford, 2008.

[9] L. Héthelyi, B. Külshammer and B. Sambale, *A note on Olsson's Conjecture*, J. Algebra **398** (2014), 364–385.

[10] B. Külshammer and T. Wada, *Some inequalities between invariants of blocks*, Arch. Math. (Basel) **79** (2002), 81–86.

[11] G. Navarro and B. Sambale, *A counterexample to Feit's Problem VIII on decomposition numbers*, J. Algebra **477** (2017), 494–495.

[12] J. B. Olsson, *Inequalities for block-theoretic invariants*, in: Representations of algebras (Puebla, 1980), 270–284, Lecture Notes in Math., Vol. 903, Springer-Verlag, Berlin, 1981.

[13] G. R. Robinson, *On the number of characters in a block*, J. Algebra **138** (1991), 515–521, Corrigendum: J. Algebra **144** (1991), 266–267.

[14] B. Sambale, *Cartan matrices and Brauer's $k(B)$-conjecture*, J. Algebra **331** (2011), 416–427.

[15] B. Sambale, *Cartan matrices and Brauer's $k(B)$-conjecture II*, J. Algebra **337** (2011), 345–362.

[16] B. Sambale, *Blocks of finite groups and their invariants*, Springer Lecture Notes in Math., Vol. 2127, Springer-Verlag, Cham, 2014.

[17] B. Sambale, *Cartan matrices and Brauer's $k(B)$-Conjecture III*, Manuscripta Math. **146** (2015), 505–518.

[18] B. Sambale, *Refinements of the orthogonality relations for blocks*, Algebr. Represent. Theory **20** (2017), 1109–1131.

[19] P. Schmid, *Some remarks on the $k(GV)$ theorem*, J. Group Theory **8** (2005), 589–604.

[20] T. Wada, *A lower bound of the Perron-Frobenius eigenvalue of the Cartan matrix of a finite group*, Arch. Math. (Basel) **73** (1999), 407–413.