Canad. Math. Bull. Vol. **64** (3), 2021, pp. 651–666
http://dx.doi.org/10.4153/S0008439520000727

The Clifford-cyclotomic group and Euler–Poincaré characteristics

Colin Ingalls, Bruce W. Jordan, Allan Keeton, Adam Logan, and Yevgeny Zaytman

Abstract. For an integer $n \geq 8$ divisible by 4, let $R_n = \mathbb{Z}[\zeta_n, 1/2]$ and let $\mathrm{U}_2(R_n)$ be the group of 2×2 unitary matrices with entries in R_n. Set $\mathrm{U}_2^\zeta(R_n) = \{\gamma \in \mathrm{U}_2(R_n) \mid \det \gamma \in \langle \zeta_n \rangle\}$. Let $\mathcal{G}_n \subseteq \mathrm{U}_2^\zeta(R_n)$ be the Clifford-cyclotomic group generated by a Hadamard matrix $H = \frac{1}{2}\left[\begin{smallmatrix} 1+i & 1+i \\ 1+i & -1-i \end{smallmatrix}\right]$and the gate $T_n = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_n \end{smallmatrix}\right]$. We prove that $\mathcal{G}_n = \mathrm{U}_2^\zeta(R_n)$ if and only if $n = 8, 12, 16, 24$ and that $[\mathrm{U}_2^\zeta(R_n) : \mathcal{G}_n] = \infty$ if $\mathrm{U}_2^\zeta(R_n) \neq \mathcal{G}_n$. We compute the Euler–Poincaré characteristic of the groups $\mathrm{SU}_2(R_n)$, $\mathrm{PSU}_2(R_n)$, $\mathrm{PU}_2(R_n)$, $\mathrm{PU}_2^\zeta(R_n)$, and $\mathrm{SO}_3(R_n^+)$.

1 Introduction

Let $\mathrm{U}_2 = \{g \in \mathrm{GL}_2(\mathbb{C}) \mid gg^\dagger = 1\}$ be the group of 2×2 unitary matrices stabilizing the standard hermitian form on $\mathbb{C}^2$ with $\dagger$ denoting conjugate-transpose. Let U_2^ζ and SU_2 be its subgroups of matrices whose determinants are roots of unity or 1, respectively. For a subring $R \subseteq \mathbb{C}$, write $\mathrm{U}_2(R) := \mathrm{U}_2 \cap \mathrm{GL}_2(R)$ for the subgroup of U_2 whose matrix entries lie in R; similarly, $\mathrm{U}_2^\zeta(R) := \mathrm{U}_2^\zeta \cap \mathrm{GL}_2(R)$ and $\mathrm{SU}_2(R) := \mathrm{SU}_2 \cap \mathrm{SL}_2(R)$. Let $\mathrm{SO}_3 = \{g \in \mathrm{SL}_3(\mathbb{R}) \mid gg^t = 1\}$. For a subring $R^+ \subseteq \mathbb{R}$, write $\mathrm{SO}_3(R^+)$ for the subgroup of SO_3 whose entries lie in R^+.

Throughout this paper, $n = 2^s d$ is a positive integer with d odd. Unless explicitly stated otherwise, we assume that $s \geq 2$. Let $\zeta_n := e^{2\pi i/n}$, $K_n := \mathbb{Q}(\zeta_n)$, and $R_n = \mathbb{Z}[\zeta_n, 1/2]$. Set $F_n = K_n^+ := \mathbb{Q}(\zeta_n + \overline{\zeta_n})$ and $R_n^+ = \mathbb{Z}[\zeta_n + \overline{\zeta}_n, 1/2]$. Then $i \in R_n$ and $R_n = R_n^+ \oplus R_n^+ i$, since $1/2 \in R_n^+$. The *Clifford group* $\mathcal{C}$ can be defined as $\mathcal{C} = \mathrm{U}_2(R_4)$ [FGKM15, Section 2.1]. Set

$$T_n := \begin{bmatrix} 1 & 0 \\ 0 & \zeta_n \end{bmatrix} \in \mathrm{U}_2(\mathbb{Z}[\zeta_n]) \subseteq \mathrm{U}_2(R_n). \tag{1.1}$$

Define the *Clifford-cyclotomic group* [FGKM15, Section 2.2] (resp., *special* Clifford-cyclotomic group) by

$$\mathcal{G}_n = \langle \mathcal{C}, T_n \rangle \qquad (\text{resp., } \mathrm{S}\mathcal{G}_n = \mathcal{G}_n \cap \mathrm{SU}_2(R_n)); \tag{1.2}$$

Received by the editors March 29, 2019.
Published online on Cambridge Core September 2, 2020.
AMS subject classification: **81P45**, 20G30.
Keywords: Clifford group, T gate, Clifford cyclotomic, Euler–Poincaré characteristics.

we have $\mathcal{G}_n \subseteq \mathrm{U}_2^\zeta(R_n)$. In general, $\mathrm{U}_2^\zeta(R_n) \subsetneq \mathrm{U}_2(R_n)$. For a subgroup $H \leq \mathrm{U}_2(R_n)$, denote by $\mathrm{P}H$ the image of H in $\mathrm{PU}_2(R_n)$. The adjoint map $\mathrm{Ad} : \mathrm{SU}_2(R_n) \to \mathrm{SO}_3(R_n^+)$ induces maps $\pi : \mathrm{U}_2(R_n) \to \mathrm{SO}_3(R_n^+)$ and $\overline{\pi} : \mathrm{PU}_2(R_n) \to \mathrm{SO}_3(R_n^+)$; see Section 5.

Let $G(r,s)$ be the subgroup of $\mathrm{SO}_3(\mathbb{R})$ generated by rotations of order r and order s about chosen perpendicular axes. For an appropriate choice of axes, one has $G(4,n) \subseteq \mathrm{SO}_3(R_n^+)$. In Theorem 5.1, we show that $\pi(\mathcal{G}_n) = G(4,n)$. The subgroup structures

$$\mathcal{G}_n \leq \mathrm{U}_2^\zeta(R_n) \leq \mathrm{U}_2(R_n), \quad G(4,n) \leq \mathrm{SO}_3(R_n^+) \tag{1.3}$$

play a large role in exact synthesis for quantum gates in single-qubit quantum computation. The following results are known.

Theorem 1.1

(i) *We have* $G(4,8) = \mathrm{SO}_3(R_8^+)$ *and* $\mathcal{G}_8 = \mathrm{U}_2(R_8)$ [Ser09, FGKM15], $G(4,12) = \mathrm{SO}_3(R_{12}^+)$ *and* $\mathcal{G}_{12} = \mathrm{U}_2(R_{12})$ [Ser09, BRS15], $G(4,16) = \mathrm{SO}_3(R_{16}^+)$ *and* $\mathcal{G}_{16} = \mathrm{U}_2(R_{16})$ [Ser09], $G(4,24) = \mathrm{SO}_3(R_{24}^+)$ *and* $\mathcal{G}_{24} = \mathrm{U}_2(R_{24})$ [FGKM15].

(ii) *For an integer* n, *we have* $\mathrm{U}_2^\zeta(R_n) = \mathrm{U}_2(R_n)$ *if and only if*

$$-1 \bmod d \in \langle 2 \bmod d\rangle \leq (\mathbb{Z}/d\mathbb{Z})^\times$$

[FGKM15, Theorem 5.3].

(iii) *Let* S_4 *be the symmetric group on 4 letters and let* D_m *be the dihedral group of order* $2m$. *We have* $G(4,n) \cong S_4 *_{D_4} D_n$ [RS99].

(iv) *If* $n = 2^s$, $s \geq 5$, *then* $G(4,n)$ *is of infinite index in* $\mathrm{SO}_3(R_n^+)$ [Ser09].

Serre [Ser09] introduced Euler–Poincaré characteristics to the study of $G(4,n)$ and $\mathcal{G}_n$, as well as observing that $\mathrm{SO}_3(R_n^+)$ for $n = 2^s$ acts on a tree by looking at it over $\mathbb{Q}_2$. Theorem 1.1(iv) follows by computing the Euler–Poincaré characteristic χ of $G(4,n)$ and $\mathrm{SO}_3(R_n^+)$ for $n = 2^s \geq 8$.

Theorem 1.2 (Serre [Ser09]) *Suppose* $n = 2^s \geq 8$.

(i) $\chi(G(4,n)) = -1/12 + 1/2n$.

(ii) $\chi(\mathrm{SO}_3(R_n^+)) = -2^{-2^{s-2}}\zeta_{F_n}(-1)$.

In this paper, we prove the following theorem, settling a conjecture of Sarnak affirmatively [Sar15, p. 15^{IV}].

Theorem 1.3 *Suppose* $4|n$ *with* $n \geq 8$.

(i) *We have* $\mathcal{G}_n = \mathrm{U}_2^\zeta(R_n)$ *if and only if* $n = 8, 12, 16, 24$.

(ii) *We have* $\mathrm{S}\mathcal{G}_n = \mathrm{SU}_2(R_n)$ *if and only if* $n = 8, 12, 16, 24$.

(iii) *We have* $G(4,n) = \mathrm{SO}_3(R_n^+)$ *if and only if* $n = 8, 12, 16, 24$.

In all cases above where equality does not hold, the index is infinite.

We prove Theorem 1.3 by computing Euler–Poincaré characteristics with $4|n$, $n \geq 8$, generalizing Theorem 1.2. We prove that

$$\chi(S\mathcal{G}_n) = \chi\big(G(4,n)\big) = \chi(P\mathcal{G}_n) = -1/12 + 1/2n$$

in Theorem 6.3. Then in Theorem 6.6, we compute χ of $\mathrm{SU}_2(R_n)$, $\mathrm{PSU}_2(R_n)$, $\mathrm{PU}_2(R_n)$, $\mathrm{PU}_2^{\zeta}(R_n)$, and $\mathrm{SO}_3(R_n^+)$. We gain a foothold on these Euler–Poincaré characteristics by considering the group scheme $\mathrm{SU}_2(\mathbb{Z}[1/2])$ over $\mathbb{Z}[1/2]$, denoted A_1^*. We have $A_1^*(\mathbb{R}) = \mathrm{SU}_2(\mathbb{C})$ and $A_1^*(R_n^+) = \mathrm{SU}_2(R_n)$. The results of Serre [Ser71] (which depend on theorems of Harder) apply to compute $\chi(\mathrm{SU}_2(R_n))$, because A_1^* is simply connected and simple. We then deduce χ of the other groups from this using properties of Euler–Poincaré characteristics. The relationship between $\chi(\mathrm{PU}_2(R_n))$ and $\chi(\mathrm{SO}_3(R_n^+))$ is particularly interesting—it involves embedding $\mathrm{PU}_2(R_n)$ in $\mathrm{SO}_3(R_n^+)$ via the adjoint representation with attendant invariant $\overline{c}(R_n)$ defined in Definition 4.10(i).

2 The Special Clifford-cyclotomic Group

For a complex number z of absolute value 1, define the unitary matrix

$$H(z) = \frac{1}{2}\begin{bmatrix} 1+i & z(1+i) \\ \overline{z}(-1+i) & 1-i \end{bmatrix} \tag{2.1}$$

of determinant 1. In particular $H(1) \in \mathcal{C}$. Following [FGKM15, (2)], we take our *Hadamard matrix* to be

$$H := \frac{1}{2}\begin{bmatrix} 1+i & 1+i \\ 1+i & -1-i \end{bmatrix} \in \mathcal{C}. \tag{2.2}$$

We have $H = T_4^{-1}H(1)$ with $T_n \in \mathrm{U}_2(R_n)$ as in (1.1) and $T_n^{-j}H(1)T_n^j = H(\zeta_n^j) \in \mathrm{SU}_2(R_n)$ for integers j if $4|n$. With $4|n$, set

$$\begin{aligned} \mathscr{H}_n &:= \big\langle H(\zeta_n), H(\zeta_n^2), \ldots, H(\zeta_n^{n-1}), H(\zeta_n^n) = H(1)\big\rangle \\ &\leq S\mathcal{G}_n \leq \mathrm{SU}_2(R_n). \end{aligned} \tag{2.3}$$

Proposition 2.1 *Assuming $4|n$, we have*

(i) $[\mathcal{G}_n : S\mathcal{G}_n] = n$,
(ii) $\mathcal{G}_n = \langle H, T_n\rangle = \langle H(1), T_n\rangle$,
(iii) $S\mathcal{G}_n = \mathscr{H}_n$.

Proof (i) follows from the exact sequence

$$1 \longrightarrow \mathrm{SU}_2(R_n) \longrightarrow \mathrm{U}_2^{\zeta}(R_n) \xrightarrow{\det} \langle\zeta_n\rangle \longrightarrow 1, \tag{2.4}$$

since the roots of unity in R_n are $\langle\zeta_n\rangle$ as n is even.

(ii) is shown in [FGKM15, Section 2.2].

For (iii), let w be a word in $H(1)$ and T_n of determinant 1 with k occurrences of $H(1)$. We proceed by induction on k. If $k = 0$, then the word must be 1. If $k = 1$, the

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

word must be $T_n^{-j}H(1)T_n^j = H(\zeta_n^j)$ for some $0 \le j \le n$. Suppose inductively that every word in $H(1)$ and T_n of determinant 1 with at most k_0 occurrences of $H(1)$ is in $\mathscr{H}_n$, and let w be a word in which $H(1)$ appears $k_0 + 1$ times. Choose a with $0 \le a < n$ such that w begins with $T_n^a H(1)$. Then $H(\zeta_n^{-a})^{-1}w \in S\mathcal{G}_n$ has at most k_0 occurrences of $H(1)$, and so is in $\mathscr{H}_n$ by assumption. Hence, $w \in \mathscr{H}_n$ and $S\mathcal{G}_n = \mathscr{H}_n$. ∎

Theorem 2.2 *Assume $4|n$. Then $\mathrm{U}_2^\zeta(R_n) = \mathcal{G}_n$ if and only if $\mathrm{SU}_2(R_n) = S\mathcal{G}_n$.*

Proof First, suppose that $\mathrm{SU}_2(R_n) = \mathscr{H}_n$ and let $\alpha \in \mathrm{U}_2^\zeta(R_n)$. Let $\det\alpha = \zeta_n^j$, where $0 \le j < n$. Then $\alpha = T^j\alpha'$, where $\det\alpha' = 1$ and so $\alpha' \in \mathrm{SU}_2(R_n)$. Since the generators of $\mathrm{SU}_2(R_n)$ belong to $\langle H, T_n\rangle$, it follows that α does too.

The reverse implication follows immediately from the definitions. ∎

3 $\mathrm{SU}_2(R_n)$ and $\mathrm{SO}_3(R_n^+)$

Definition 3.1

(i) Throughout this paper, R^+ is the ring of S-integers in a totally real number field F, where S contains the archimedean places and all places above 2. We put $R = R^+[i]$ and $K = F(i)$. Both R^+ and R are Dedekind domains.

(ii) Define A_1^* to be the group scheme over $\mathbb{Z}[1/2]$ with

$$A_1^*(B) = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} : a^2+b^2+c^2+d^2 = 1;\ a,b,c,d \in B \right\}$$

for any $\mathbb{Z}[1/2]$-algebra B with group operation defined by matrix multiplication. In particular, $A_1^*(B) = \mathrm{SU}_2(B[i])$. For example, $A_1^*(\mathbb{R}) = \mathrm{SU}_2(\mathbb{C})$.

By SO_3, we mean the group of 3×3 matrices of determinant 1 that stabilize the standard inner product on $\mathbb{R}^3$. It is defined as a group scheme over $\mathbb{Z}$ by $\det(g) = 1$ and $gg^t = 1$. There is an exact sequence of group schemes

$$1 \longrightarrow \mu_2 \longrightarrow A_1^* \xrightarrow{\mathrm{Ad}} \mathrm{SO}_3 \longrightarrow 1, \tag{3.1}$$

given by SU_2 acting by conjugation on the three-dimensional real vector space V of trace-0 2×2 hermitian ($m^\dagger = m$) matrices in the *Pauli basis* [NC00]

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

In terms of hermitian matrices, the standard form is $\langle A, B\rangle = \frac{1}{2}\mathrm{Tr}(AB)$:

$$\frac{1}{2}\mathrm{Tr}\left(\begin{bmatrix} z & x-iy \\ x+iy & -z \end{bmatrix}^2 \right) = x^2+y^2+z^2,$$

which is obviously preserved under conjugation by SU_2. This is the adjoint action of SU_2 on its Lie algebra iV of trace-0 skew-hermitian matrices in disguise. Explicitly,

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

we have [Nab11, Appendix A]:

$$\text{(3.2)} \qquad \mathrm{Ad}\left(\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}\right) = \begin{bmatrix} a^2-b^2-c^2+d^2 & 2ab+2cd & -2ac+2bd \\ -2ab+2cd & a^2-b^2+c^2-d^2 & 2ad+2bc \\ 2ac+2bd & -2ad+2bc & a^2+b^2-c^2-d^2 \end{bmatrix}.$$

The map Ad factors as

$$\text{(3.3)} \qquad A_1^*(R^+) = \mathrm{SU}_2(R) \twoheadrightarrow \mathrm{PSU}_2(R) \hookrightarrow \mathrm{SO}_3(R^+).$$

The adjoint action Ad given in (3.2) extends to a group homomorphism $\pi : \mathrm{U}_2(R) \to \mathrm{SO}_3(R^+)$ via conjugation on the 2×2 hermitian matrices of trace 0 in the Pauli basis. We have

$$\pi(g) = \mathrm{Ad}\Big(\frac{1}{\sqrt{\det g}}\, g\Big)$$

for an arbitrary choice of $\sqrt{\det g}$. The map π in turn factors as

$$\text{(3.4)} \qquad \mathrm{U}_2(R) \twoheadrightarrow \mathrm{PU}_2(R) \overset{\overline{\pi}}{\hookrightarrow} \mathrm{SO}_3(R^+).$$

We view $\mathrm{PSU}_2(R)$ as a subgroup of $\mathrm{SO}_3(R^+)$ via (3.3), and we view $\mathrm{PU}_2(R)$ as a subgroup of $\mathrm{SO}_3(R^+)$ via (3.4) with $\mathrm{PSU}_2(R) \leq \mathrm{PU}_2(R) \leq \mathrm{SO}_3(R^+)$.

Remark 3.2 In Section 4, we will define a map ϕ from $\mathrm{SO}_3(R^+)$ into a finite elementary abelian 2-group (the Selmer group $\mathrm{Sel}_2^+(R^+)$) with kernel $\mathrm{PSU}_2(R)$. From this it follows that $\mathrm{PSU}_2(R)$ and $\mathrm{PU}_2(R)$ are *normal* subgroups of $\mathrm{SO}_3(R^+)$; *cf.* Corollary 4.9.

4 $\mathrm{SO}_3(R^+)/\mathrm{PSU}_2(R)$ and $\mathrm{SO}_3(R^+)/\mathrm{PU}_2(R)$

The short exact sequence (3.1) remains short exact on $\mathbb{R}$-points

$$1 \longrightarrow \langle \pm 1 \rangle \longrightarrow A_1^*(\mathbb{R}) \xrightarrow{\mathrm{Ad}} \mathrm{SO}_3(\mathbb{R}) \longrightarrow 1$$

with $A_1^*(\mathbb{R}) = \mathrm{SU}_2(\mathbb{C})$, but in general for R^+ we only have

$$\text{(4.1)} \qquad 1 \longrightarrow \mu_2(R^+) = \langle \pm 1 \rangle \longrightarrow A_1^*(R^+) \xrightarrow{\mathrm{Ad}} \mathrm{SO}_3(R^+)\,.$$

In our situation, $A_1^*(R^+)$ does not surject onto $\mathrm{SO}_3(R^+)$. In particular, the map Ad factors as

$$A_1^*(R^+) = \mathrm{SU}_2(R) \longrightarrow \mathrm{PU}_2(R) \longrightarrow \mathrm{SO}_3(R^+)$$

by (3.3), (3.4), and the map from $\mathrm{SU}_2(R)$ to $\mathrm{PU}_2(R)$ is not surjective. Indeed, for us, R is a localization of an order in a number field, so the group of roots of unity of R is finite, generated by some root of unity ζ. Then ζ is not a square in R, so $\left[\begin{smallmatrix} \zeta & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is an element of $\mathrm{PU}_2(R)$ whose determinant is not a square. Therefore it cannot be

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

the image of any element of $\mathrm{SU}_2(R)$. Since the map $\mathrm{PU}_2(R) \to \mathrm{SO}_3(R^+)$ is injective, this implies that $\mathrm{SU}_2(R) \to \mathrm{SO}_3(R^+)$ is not surjective either, proving the following proposition.

Proposition 4.1 *Let R^+ be the ring of S-integers in a totally real field F, where S contains the archimedean primes and all primes above 2, and let $R = R^+[i]$. Then the group $\mathrm{SO}_3(R^+)/\mathrm{PSU}_2(R)$ is nontrivial.*

Even the map $\mathrm{PU}_2(R) \to \mathrm{SO}_3(R^+)$ may not be surjective.

Example 4.2 The map $\mathrm{PU}_2(\mathbb{Z}[\sqrt{21}, i, 1/2]) \hookrightarrow \mathrm{SO}_3(\mathbb{Z}[\sqrt{21}, 1/2])$ is not surjective.

Let $R^+ = \mathbb{Z}[\sqrt{21}, 1/2]$ and $R = R^+[i]$. Let $u = \frac{5+\sqrt{21}}{2} \in (R^+)^\times$, which is totally positive and *not* the norm of a unit in R. (One checks that $R^\times$ is generated by $u, i, 1+i$ and hence that u is not a norm from $R^\times$.) Choose $q \in \left(\frac{-1,-1}{R^+}\right)$ of norm u, such as $\frac{4+\sqrt{21}+i+j+k}{4}$. The homomorphism from the unit Hamilton quaternions over R^+ to SO_3 takes q to

$$T_q = \begin{bmatrix} \frac{\sqrt{21}+3}{8} & \frac{1}{4} & \frac{-\sqrt{21}+3}{8} \\ \frac{-\sqrt{21}+3}{8} & \frac{\sqrt{21}+3}{8} & \frac{1}{4} \\ \frac{1}{4} & \frac{-\sqrt{21}+3}{8} & \frac{\sqrt{21}+3}{8} \end{bmatrix} \in \mathrm{SO}_3(R^+).$$

The 2×2 matrix M corresponding to q is

$$M_q = \begin{bmatrix} \frac{4+\sqrt{21}+i}{4} & \frac{1+i}{4} \\ \frac{-1+i}{4} & \frac{4+\sqrt{21}-i}{4} \end{bmatrix};$$

it has the property that $MM^\dagger = u\,\mathrm{Id}_{2\times 2}$. The element of $\mathrm{PU}_2(\mathbb{C})$ mapping to T_q is obtained by dividing M_q by an element of $\mathbb{C}$ of norm u. However, lifting this element to an element of $\mathrm{PU}_2(R)$ would require finding an element of R of norm u, which does not exist. Hence, $T_q \in \mathrm{SO}_3(R^+)$ is not the image of any element of $\mathrm{PU}_2(R)$.

In this section, we will prove that $\mathrm{SO}_3(R^+)/\mathrm{PSU}_2(R)$ and $\mathrm{SO}_3(R^+)/\mathrm{PU}_2(R)$ are finite abelian 2-groups, with $\mathrm{SO}_3(R^+)/\mathrm{PSU}_2(R)$ nontrivial by Proposition 4.1. Denote by F_+ the totally positive elements of F. For any subset $S \subseteq F$, denote by $S_+ \subseteq F_+$ the totally positive elements of S.

Definition 4.3 Let $M_x, M_y, M_z \in \mathrm{SO}_3(R^+)$ be the diagonal matrices with entries

$$(1,-1,-1), (-1,1,-1), (-1,-1,1),$$

respectively.

Define the following R^+-valued functions for $M \in \mathrm{SO}_3(R^+)$:

$$\phi_1(M) := (1 + M_{11} + M_{22} + M_{33})/4 = \big(1 + \mathrm{Tr}(M)\big)/4,$$
$$\phi_2(M) := (1 - M_{11} - M_{22} + M_{33})/4 = \big(1 + \mathrm{Tr}(MM_z)\big)/4,$$
$$\phi_3(M) := (1 - M_{11} + M_{22} - M_{33})/4 = \big(1 + \mathrm{Tr}(MM_y)\big)/4,$$

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

$$\phi_4(M) := (1 + M_{11} - M_{22} - M_{33})/4 = \big(1 + \mathrm{Tr}(MM_x)\big)/4$$

and

$$\begin{aligned}\theta_{12}(M) &:= \theta_{21}(M) := (M_{12} - M_{21})/4,\\ \theta_{13}(M) &:= \theta_{31}(M) := (M_{31} - M_{13})/4,\\ \theta_{14}(M) &:= \theta_{41}(M) := (M_{23} - M_{32})/4,\\ \theta_{34}(M) &:= \theta_{43}(M) := (M_{12} + M_{21})/4,\\ \theta_{24}(M) &:= \theta_{42}(M) := (M_{31} + M_{13})/4,\\ \theta_{23}(M) &:= \theta_{32}(M) := (M_{23} + M_{32})/4.\end{aligned}$$

Definition 4.4 Let R be the S-integers in a totally real number field F, where S contains all infinite primes. (Note that the definitions and notation here are different from the standard conventions in Definition 3.1(i).) Define the Selmer group

$$\mathrm{Sel}_2^+(\mathrm{R}) := \{x \in F_+^\times \mid \mathrm{val}_{\mathfrak{p}}\, x \equiv 0 \pmod 2 \text{ for every finite prime } \mathfrak{p} \text{ of } \mathrm{R}\}/(F^\times)^2.$$

We denote by $\mathrm{Cl}(\mathrm{R})$ the class group of R.

It is not difficult to compute $\mathrm{Sel}_2^+(\mathrm{R})$ in examples using the following elementary proposition.

Proposition 4.5 *There is an exact sequence of abelian groups*

$$\mathrm{R}^\times \xrightarrow{2} \mathrm{R}_+^\times \longrightarrow \mathrm{Sel}_2^+(\mathrm{R}) \longrightarrow \mathrm{Cl}(\mathrm{R}) \xrightarrow{2} \mathrm{Cl}(\mathrm{R}).$$

In particular, let $r = [F : \mathbb{Q}]$ and let s be the number of finite primes in S. Then the kernel of the signature map $\mathrm{R}^\times \to (\mathbb{Z}/2\mathbb{Z})^r$ is precisely $\mathrm{R}_+^\times$, while $\mathrm{R}^\times/(\mathrm{R}^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{r+s}$. Thus, if the image of the signature map is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^v$, then $\mathrm{R}_+^\times/(\mathrm{R}^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{r+s-v}$.

This makes it straightforward to compute the following examples.

Proposition 4.6 *Let R_n, R_n^+ be as in the introduction.*

(i) *Suppose $n = 2^s$, $n \geq 8$. Then $\mathrm{Sel}_2^+(R_n^+) \cong \mathbb{Z}/2\mathbb{Z}$.*

(ii) *Suppose $n = 3 \cdot 2^s$, $4|n$. Then $\mathrm{Sel}_2^+(R_n^+) \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof Let $\mathcal{O}_n := \mathbb{Z}[\zeta_n + \overline{\zeta}_n]$, the ring of integers in $F_n := \mathbb{Q}(\zeta_n)^+$. (i): Let $n = 2^s$, $n \geq 8$. Then $\mathcal{O}_n$ has odd class number by [Was82, Theorem 10.4(b)] and so $R_n^+ = \mathcal{O}_n[1/2]$ has odd class number. Every totally positive unit in $\mathcal{O}_n$ is a square by Weber's Theorem [Web99] and there is one prime $\mathfrak{p}$ in F_n above 2. Hence, $(R_n^+)_+/[(R_n^+)^\times]^2 \cong \mathbb{Z}/2\mathbb{Z} \cong \mathrm{Sel}_2^+(R_n^+)$. (ii): Let $n = 3 \cdot 2^s$, $s \geq 3$. Then applying [Was82, Theorem 10.4] to $F_n/\mathbb{Q}(\sqrt{3})$ shows that $\mathcal{O}_n$ has odd class number. We have $(R_n^+)_+^\times/[(R_n^+)^\times]^2 \cong \mathbb{Z}/2\mathbb{Z}$ by [IJK+a, Theorem 3.13(b)]. ■

The functions of Definition 4.3 satisfy the following properties.

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

Lemma 4.7 *For $M \in \mathrm{SO}_3(R^+)$ and*

$$A = \begin{bmatrix} a_1 + a_2 i & a_3 + a_4 i \\ -a_3 + a_4 i & a_1 - a_2 i \end{bmatrix} \in \mathrm{SU}_2(R),$$

we have:

(i) $\phi_i(Ad(A)) = a_i^2, 1 \le i \le 4$;
(ii) $\theta_{ij}(Ad(A)) = a_i a_j, 1 \le i, j \le 4, i \ne j$;
(iii) $\phi_1(M) + \phi_2(M) + \phi_3(M) + \phi_4(M) = 1$;
(iv) $\phi_i(M)\phi_j(M) = \theta_{ij}(M)^2$, $1 \le i, j \le 4$, $i \ne j$, *and* $\theta_{\pi(1)\pi(2)}(M)\theta_{\pi(3)\pi(4)}(M)$ *does not depend on the choice of* $\pi \in \mathcal{S}_4$;
(v) *there exists a unique well-defined function* $\phi : \mathrm{SO}_3(R^+) \to F^\times/(F^\times)^2$ *which agrees with each* ϕ_i, $1 \le i \le 4$, *whenever the latter is nonzero;*
(vi) *the image of* ϕ *lies in* $\mathrm{Sel}_2^+(R^+) \subseteq F^\times/(F^\times)^2$. *In other words* $\phi(M)$ *has even valuation at all primes of* R^+ *and is totally positive;*
(vii) *for* $i \in \{x, y, z\}$, *we have* $\phi(M) = \phi(MM_i) = \phi(M_i M)$.

Proof (iii) follows immediately by summing the definitions of the ϕ_i's. (i) and (ii) follow immediately by plugging in the definition of Ad (3.2).

(iv) is not as trivial but can be derived from the defining equations of SO_3 by a simple Gröbner basis calculation.

To see (v), observe that by (iii) at least one of the $\phi_i(M)$ is always nonzero and by (iv) all the nonzero $\phi_i(M)$ agree modulo squares.

(vi) follows since by (iii) at each prime of R^+ at least one of the $\phi_i(M)$ must have valuation 0. The total positivity follows from the definitions of ϕ_i and the fact that $\mathrm{Tr}(M) \ge -1$ for all $M \in \mathrm{SO}_3(\mathbb{R})$.

Finally, (vii) holds, because the sets $\{\phi_j(M)\}$, $\{\phi_j(MM_i)\}$, $\{\phi_j(M_i M)\}$ for $1 \le j \le 4$ are visibly equal. ∎

Theorem 4.8 *The map* $\phi : \mathrm{SO}_3(R^+) \to \mathrm{Sel}_2^+(R^+)$ *is a group homomorphism and*

$$1 \longrightarrow \mathrm{PSU}_2(R) \xrightarrow{\mathrm{Ad}} \mathrm{SO}_3(R^+) \xrightarrow{\phi} \mathrm{Sel}_2^+(R^+)$$

is an exact sequence.

Proof In view of Lemma 4.7(vii), we can assume that $\phi_1(MN) \ne 0$. It can be checked using a simple Gröbner basis calculation that for $M, N \in \mathrm{SO}_3(R^+)$ and $1 \le i \le 4$, the equation

(4.2)
$$\phi_i(M)\phi_i(N)\phi_1(MN) = \big(\phi_i(M)\phi_i(N) \pm \theta_{ij}(M)\theta_{ij}(N) \pm \theta_{ik}(M)\theta_{ik}(N) \pm \theta_{i\ell}(M)\theta_{i\ell}(N)\big)^2$$

follows from the defining equations of SO_3, where $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$ and the sign is -1 when 1 appears in the subscript and $+1$ otherwise. Hence, $\phi(M)\phi(N) = \phi(MN)$ as long as $\phi_i(M)$, $\phi_i(N)$ are both nonzero for the same i.

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

If three of the $\phi_i(M)$ are 0, then $M \in \{I_3, M_x, M_y, M_z\}$, and it is simple to check that $\phi(MN) = \phi(M)\phi(N)$; similarly, if three of the $\phi_i(N)$ are 0. Otherwise, there is no problem unless two are 0 for M and the other two are 0 for N. Suppose that $\phi_1(M) = \phi_2(M) = \phi_3(N) = \phi_4(N)$ (the other cases are similar). Then we have

$$M = \begin{bmatrix} a & b & 0 \\ b & -a & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad N = \begin{bmatrix} c & d & 0 \\ -d & -c & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

where $a^2 + b^2 = c^2 + d^2 = 1$. In this case, it is easy to check that $\phi_1(MN) = 0$, contradicting our choice of N (and it is also easy to check that $\phi(MN) = \phi(M)\phi(N)$). Thus, ϕ is a group homomorphism.

That $\phi \circ \mathrm{Ad} = 1$ follows from Lemma 4.7(i). Now suppose $M \in \ker \phi$, so that the $\phi_i(M)$ are all squares in R^+. Let $a_i = \sqrt{\phi_i(M)}$ with signs chosen so that $a_i a_j = \theta_{ij}(M)$; we can do this by Lemma 4.7(ii). Now it is again straightforward to check that the equations

$$M = \mathrm{Ad}\left(\begin{bmatrix} a_1 + a_2 i & a_3 + a_4 i \\ -a_3 + a_4 i & a_1 - a_2 i \end{bmatrix}\right)$$

follow from the defining equations of SO_3. ∎

Corollary 4.9 *The subgroups* $\mathrm{PSU}_2(R)$ *and* $\mathrm{PU}_2(R)$ *of* $\mathrm{SO}_3(R^+)$ *are normal.*

Definition 4.10

(i) Set $C(R) = \mathrm{SO}_3(R^+)/\mathrm{PSU}_2(R)$, $\overline{C}(R) = \mathrm{SO}_3(R^+)/\mathrm{PU}_2(R)$, $c(R) = \#C(R)$, and $\overline{c}(R) = \#\overline{C}(R)$. Hence, $c(R), \overline{c}(R)$ are powers of 2 with $c(R) \neq 1$. We have

(4.3) $$c(R) = [\mathrm{PU}_2(R) : \mathrm{PSU}_2(R)]\overline{c}(R).$$

(ii) Let $r(n)$ be the number of primes in $K_n := \mathbb{Q}(\zeta_n)$ above 2 and $r_+(n)$ be the number of primes in $F_n := \mathbb{Q}(\zeta_n)^+$ above 2.

We now state a result from [IJK+b] that we will need.

Proposition 4.11 ([IJK+b, Proposition 2.3]) *Suppose* $n \geq 8$ *and* $4|n$ *with* $r(n)$, $r_+(n)$ *as in Definition* 4.10(ii).

(i) $\mathrm{PU}_2(R_n)/\mathrm{PSU}_2(R_n) \cong (\mathbb{Z}/2\mathbb{Z})^{1+r(n)-r_+(n)}$.

(ii) $\mathrm{PU}_2(R_n)/\mathrm{PU}_2^{\zeta}(R_n) \cong (\mathbb{Z}/2\mathbb{Z})^{r(n)-r_+(n)}$.

(iii) $\mathrm{PU}_2^{\zeta}(R_n)/\mathrm{PSU}_2(R_n) \cong \mathbb{Z}/2\mathbb{Z}$.

Combining Proposition 4.11(i) with (4.3) then gives the following proposition.

Proposition 4.12 *For* $R_n = \mathbb{Z}[\zeta_n, 1/2]$, $4|n$, $n \geq 8$, *we have* $c(R_n) = 2^{1+r(n)-r_+(n)}\overline{c}(R_n)$.

We can compute $c(R)$ and $\overline{c}(R)$ in some important examples with $R = R_n := \mathbb{Z}[\zeta_n, 1/2]$.

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

Theorem 4.13

(i) *Suppose* $n = 2^s$, $n \geq 8$. *Then* $c(R_n) = 2$ *and* $\overline{c}(R_n) = 1$.
(ii) *Suppose* $n = 3 \cdot 2^s$, $s \geq 2$. *Then* $c(R_n) = 2$ *and* $\overline{c}(R_n) = 1$.

Proof Suppose $n = 2^s$ or $n = 3 \cdot 2^s$ with $n \geq 8$. Then there is one prime in $K_n = \mathbb{Q}(\zeta_n)$ above 2 and $r(n) = r_+(n) = 1$. Hence by Proposition 4.12, $c(R_n) = 2\overline{c}(R_n)$. But by Proposition 4.5, $\mathrm{Sel}_2^+(R_n^+) \cong \mathbb{Z}/2\mathbb{Z}$. So $c(R_n) \leq 2$, and therefore $c(R_n) = 2$ and $\overline{c}(R_n) = 1$. ∎

Remark 4.14 In the cyclotomic case $R_n = \mathbb{Z}[\zeta_n, 1/2])$, $4|n$, $n \geq 8$, we do not have an example where $\overline{c}(R_n) \neq 1$. Example 4.2 shows that $\overline{c}(\mathbb{Z}[\sqrt{21}, i, 1/2]) \neq 1$.

5 Amalgamated Products and the Clifford-cyclotomic Group

Set $\overline{\mathcal{G}}_n = \pi(\mathcal{G}_n) \subseteq \mathrm{SO}_3(R_n^+)$ and $\overline{\mathrm{S}\mathcal{G}}_n = \mathrm{Ad}(\mathrm{S}\mathcal{G}_n) \subseteq \mathrm{SO}_3(R_n^+)$.

Theorem 5.1 *Assume* $4|n$, $n \geq 8$. *We have*

$$\mathrm{P}\mathcal{G}_n \cong \overline{\mathcal{G}}_n = G(4, n) \cong S_4 *_{D_4} D_n.$$

Proof By Proposition 2.1(ii) and Theorem 1.1(iii), it suffices to show that $\pi(H_n T^{2m})$ and $\pi(T_n)$ are rotations of order 4 and n about orthogonal axes. Now

$$T^{2m} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \text{so} \quad HT^{2m} = \frac{1}{2}\begin{bmatrix} 1+i & -1-i \\ 1+i & 1+i \end{bmatrix},$$

which has determinant $i = \zeta_8^2$. Define

$$\widetilde{H} = \frac{1}{\zeta_8} HT^{2m} = \frac{1}{2}\begin{bmatrix} \zeta_8 - \zeta_8^3 & \zeta_8^3 - \zeta_8 \\ \zeta_8 - \zeta_8^3 & \zeta_8 - \zeta_8^3 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

We calculate using (3.2):

$$\pi(HT^{2m}) = \mathrm{Ad}(\widetilde{H}) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \cos(\pi/2) & 0 & \sin(\pi/2) \\ 0 & 1 & 0 \\ -\sin(\pi/2) & 0 & \cos(\pi/2) \end{bmatrix},$$

which is a rotation around the y-axis by $\pi/2$, while

$$\begin{aligned} \pi(T_n) &= \mathrm{Ad}\left(\begin{bmatrix} \zeta_{2n}^{-1} & 0 \\ 0 & \zeta_{2n} \end{bmatrix}\right) \\ &= \mathrm{Ad}\left(\begin{bmatrix} \cos(\pi/n) - i\sin(\pi/n) & 0 \\ 0 & \cos(\pi/n) + i\sin(\pi/n) \end{bmatrix}\right) \\ &= \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) & 0 \\ \sin(2\pi/n) & \cos(2\pi/n) & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

is a rotation by $2\pi/n$ about the z-axis. ∎

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

The finite subgroups of $\mathrm{SU}_2(\mathbb{C})$ are well known; see [Vig80, Théorème I.3.7]. Let D_n be the dihedral group of order $2n$. Denote by E_{48} the tetrahedral group, *i.e.*, the degree-2 central extension of S_4, and by Q_{4n} the quaternion group of order $4n$ (called *dicyclique* in [Vig80]). We have $Q_{4n}/\langle \pm 1\rangle \cong D_n$.

Corollary 5.2 *Let $\mathcal{H}$ be the pullback of $\overline{\mathcal{G}}_n$ under the surjective map $\mathrm{SU}_2(\mathbb{C}) \overset{\mathrm{Ad}}{\to} \mathrm{SO}_3(\mathbb{R})$. Then $\mathrm{S}\mathcal{G}_n \subseteq \mathcal{H}$ with $[\mathcal{H} : \mathrm{S}\mathcal{G}_n] = 2$ and*

$$\mathcal{H} \cong E_{48} *_{Q_{16}} Q_{4n}. \tag{5.1}$$

Proof We have $\mathrm{P}\mathcal{G}_n / \mathrm{PS}\mathcal{G}_n \cong \mu_n/\mu_n^2 \cong \mathbb{Z}/2\mathbb{Z}$, since n is even. But

$$\mathrm{P}\mathcal{G}_n \cong \pi(\mathcal{G}_n) = \overline{\mathcal{G}}_n = G(4,n) \cong S_4 *_{D_4} D_n \tag{5.2}$$

and $\mathrm{PS}\mathcal{G}_n \cong \mathrm{Ad}(\mathrm{S}\mathcal{G}_n) = \overline{\mathrm{S}\mathcal{G}}_n$. Hence, $\mathrm{Ad}^{-1}(\overline{\mathcal{G}}_n) := \mathcal{H} \cong E_{48} *_{Q_{16}} Q_{4n}$ and $\mathrm{Ad}^{-1}(\overline{\mathrm{S}\mathcal{G}}_n) = \mathrm{S}\mathcal{G}_n$. Since $[\overline{\mathcal{G}}_n : \overline{\mathrm{S}\mathcal{G}}_n] = 2$, it follows that $[\mathcal{H} : \mathrm{S}\mathcal{G}_n] = 2$. ■

6 Euler–Poincaré Characteristics

In this section, we determine the Euler–Poincaré characteristics of unitary groups over cyclotomic rings and Clifford-cyclotomic groups. These results will then be used in the proof of Theorem 1.3. General references for Euler–Poincaré characteristics are [Bro94, Chapter 9] and [Ser71].

Definition 6.1 ([Bro94, Section IX.6]) A group Γ is of *finite homological type* if Γ has finite virtual cohomological dimension, and, for every Γ-module M that is finitely generated as an abelian group and every natural number i, the homology group $H_i(\Gamma, M)$ is finitely generated.

Proposition 6.2

(i) *Suppose $1 \to \Gamma' \to \Gamma \to \Gamma'' \to 1$ is a short exact sequence of groups with Γ', Γ'' of finite homological type. If Γ is virtually torsion-free, then Γ is of finite homological type and*

$$\chi(\Gamma) = \chi(\Gamma')\chi(\Gamma'').$$

(ii) *Suppose Γ' is a subgroup of Γ of finite index and $\chi(\Gamma)$ is defined. Then $\chi(\Gamma')$ is defined and $\chi(\Gamma') = [\Gamma : \Gamma']\chi(\Gamma)$.*

(iii) *Suppose $\Gamma' \le \Gamma$ with $\chi(\Gamma)$ and $\chi(\Gamma')$ both defined. If $|\chi(\Gamma')|/|\chi(\Gamma)|$ is not a positive integer, then Γ' has infinite index in Γ. In particular, this holds if $|\chi(\Gamma')| < |\chi(\Gamma)|$.*

(iv) *Suppose Γ' and Γ'' are finite groups with $A \le \Gamma'$ and $A \le \Gamma''$. Let $\Gamma = \Gamma' *_A \Gamma''$. Then*

$$\chi(\Gamma) = \frac{1}{\#\Gamma'} + \frac{1}{\#\Gamma''} - \frac{1}{\#A}.$$

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

Proof (i), (ii) are parts (d) and (c) of [Bro94, Proposition 7.3]. To prove (iii), let $C_{\Gamma'}$ be the intersection of the conjugates of Γ' in Γ. If $[\Gamma : \Gamma'] < \infty$ then $[\Gamma : C_{\Gamma'}] < \infty$ as well. Applying (i) to the short exact sequences

$$1 \longrightarrow C_{\Gamma'} \longrightarrow \Gamma \longrightarrow \Gamma/C_{\Gamma'} \longrightarrow 1 \quad \text{and} \quad 1 \longrightarrow C_{\Gamma'} \longrightarrow \Gamma' \longrightarrow \Gamma'/C_{\Gamma'} \longrightarrow 1$$

gives the claimed result. Finally, (iv) is [Ser71, Corollaire 1, p. 104]. ∎

Theorem 6.3 *Assume* $4|n$. *Then* $\chi(S\mathcal{G}_n) = \chi(G(4,n)) = \chi(P\mathcal{G}_n) = -\frac{1}{12} + \frac{1}{2n}$.

Proof Let $\mathcal{H}$ be as in Corollary 5.2. By (5.1) and Proposition 6.2(iv), we have

$$\begin{aligned}\chi(\mathcal{H}) = \chi(E_{48} *_{Q_{16}} Q_{4n}) &= \frac{1}{\#E_{48}} + \frac{1}{\#Q_{4n}} - \frac{1}{\#Q_{16}} \\ &= \frac{1}{48} + \frac{1}{4n} - \frac{1}{16} = -\frac{1}{24} + \frac{1}{4n}.\end{aligned}$$

But $S\mathcal{G}_n$ is an index-2 subgroup of $\mathcal{H}$ from Corollary 5.2, so by Proposition 6.2(ii),

$$\chi(S\mathcal{G}_n) = 2\chi(\mathcal{H}) = -\frac{1}{12} + \frac{1}{2n}.$$

We have $\chi(G(4,n)) = \chi(P\mathcal{G}_n) = -1/12 + 1/2n$ from (5.2) and Proposition 6.2(iv). ∎

We will need the following in the proof of Theorem 6.6.

Remark 6.4 Recall that a connected linear algebraic group G over a perfect field is *reductive* if it admits a representation with finite kernel that is a direct sum of irreducible representations. An alternative definition sufficient for this paper is that G over an algebraically closed field is reductive if and only if every smooth connected unipotent normal subgroup of G is trivial, and if k is perfect, then G is reductive over k if and only if it is over $\bar{k}$.

Definition 6.5 Set

$$M_n := 2^{1-[F_n:\mathbb{Q}]} \left|\zeta_{F_n}(-1)\right| \prod_{\mathfrak{p}|2} \left|1 - \mathrm{N}_{F_n/\mathbb{Q}}(\mathfrak{p})\right|.$$

Theorem 6.6 *Suppose* $n \geq 8$ *and* $4|n$ *with* $r(n)$, $r_+(n)$ *as in Definition 4.10(ii).*

(i) $\chi(\mathrm{SU}_2(R_n)) = -M_n/2$.
(ii) $\chi(\mathrm{PSU}_2(R_n)) = 2\chi(\mathrm{SU}_2(R_n)) = -M_n$.
(iii) $\chi(\mathrm{PU}_2^{\zeta}(R_n)) = \chi(\mathrm{SU}_2(R_n)) = -M_n/2$.
(iv)

$$\chi(\mathrm{PU}_2(R_n)) = \frac{\chi(\mathrm{SU}_2(R_n))}{2^{r(n)-r_+(n)}} = \frac{\chi(\mathrm{PSU}_2(R_n))}{2^{1+r(n)-r_+(n)}} = -\frac{M_n}{2^{1+r(n)-r_+(n)}}.$$

(v) *Put* $c_n = c(R_n)$ *and* $\overline{c}_n = \overline{c}(R_n)$ *as in Definition 4.10. Then*

$$\chi(\mathrm{SO}_3(R_n^+)) = \chi(\mathrm{PU}_2(R_n))/\overline{c}_n = -\frac{M_n}{2^{1+r(n)-r_+(n)}\overline{c}_n}$$

$$= \chi(\mathrm{PSU}_2(R_n))/c_n = -\frac{M_n}{c_n}. \tag{6.1}$$

Proof (i) follows from a result of Harder [Ser71, Section 3.7, $(*)$].

Claims (ii), (iii), (iv), and (v) are obtained by combining this with Proposition 6.2, once we verify that all groups involved are of finite homological type. We start from the fact, due to Borel and Serre [Bro94, p. 218], that a torsion-free reductive S-arithmetic group Γ is of type FL (*i.e.*, that the $\mathbb{Z}\Gamma$-module $\mathbb{Z}$ has a finite free resolution). This is stated for arithmetic groups over $\mathbb{Q}$; however, the result follows more generally by restriction of scalars. The only problem is to verify that restriction of scalars preserves reductivity. As noted in Remark 6.4, in characteristic 0, an algebraic group is reductive over k if and only if it is reductive over $\bar{k}$, and for a finite extension K/F, we have $\mathrm{Res}_{K/F}\, G \otimes_F \bar{F} \equiv (G \otimes_K \bar{F})^{[K:F]}$. A finite direct product of reductive groups is clearly reductive, so it follows that if G is reductive, then so is $\mathrm{Res}_{K/F}\, G$. As SU_2 is a simple group, it is certainly reductive. This shows that our groups are all VFL (as usual, the subgroup of matrices congruent to 1 modulo a large prime is torsion-free).

Since free modules are projective, VFL implies VFP, and groups of type VFP are of finite homological type. This is enough to apply [Bro94, Proposition 7.3].

(ii): Apply Proposition 6.2(i) to

$$1 \longrightarrow \langle \pm 1 \rangle \longrightarrow \mathrm{SU}_2(R_n) \longrightarrow \mathrm{PSU}_2(R_n) \longrightarrow 1,$$

using the fact that $\mathrm{SU}_2(R_n)$ is virtually torsion-free, because it is arithmetic (so a sufficiently small congruence subgroup is torsion-free).

(iii): Apply Proposition 6.2(i) to

$$1 \longrightarrow \mathrm{PSU}_2(R_n) \longrightarrow \mathrm{PU}_2^{\zeta}(R_n) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

from Proposition 4.11(iii). To show that $\mathrm{PU}_2^{\zeta}(R_n)$ is virtually torsion-free, it suffices to show that the finite-index subgroup $\mathrm{PSU}_2(R_n)$ is virtually torsion-free. But $\mathrm{PSU}_2(R_n)$ is virtually torsion-free, since it is a finite quotient $\mathrm{SU}_2(R_n)$, which is virtually torsion-free from (ii).

(iv): Apply Proposition 6.2(i) to

$$1 \longrightarrow \mathrm{PSU}_2(R_n) \longrightarrow \mathrm{PU}_2(R_n) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{1+r(n)-r_+(n)} \longrightarrow 0$$

from Proposition 4.11(i). The group $\mathrm{PU}_2(R_n)$ is virtually torsion-free, because its finite-index subgroup $\mathrm{PSU}_2(R_n)$ is virtually torsion-free from (iii).

(v): Apply Proposition 4.11(i) to

$$1 \longrightarrow \mathrm{PU}_2(R_n) \xrightarrow{\overline{\pi}} \mathrm{SO}_3(R_n^+) \longrightarrow \overline{C}(R_n) \longrightarrow 1 \text{ and}$$

$$1 \longrightarrow \mathrm{PSU}_2(R_n) \xrightarrow{\mathrm{Ad}} \mathrm{SO}_3(R_n^+) \longrightarrow C(R_n) \longrightarrow 1,$$

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

as in Definition 4.10; $\#\overline{C}(R_n) = \overline{c}(R_n) = \overline{c}_n$ and $\#C(R_n) = c(R_n) = c_n$. The group $SO_3(R_n^+)$ is virtually torsion-free, since it is arithmetic. ■

Remark 6.7 Suppose $n = 2^s \geq 8$. Then $r(n) = r_+(n) = 1$. Serre [Ser09, p. 48] uses Tamagawa numbers to show in this case that $\chi(SO_3(R_n^+)) = -M_n/2$ as in Theorem 1.2(ii). Theorem 6.6(v) then shows that $c(R_n) = 2$ and $\overline{c}(R_n) = 1$, giving an independent proof of Theorem 4.13(i).

7 Proof of Theorem 1.3

We first prove Theorem 1.3(ii). It is already known that $S\mathcal{G}_n = SU_2(R_n)$ for $n = 8, 12, 16, 24$ (Theorem 1.1(i)). We will prove that $S\mathcal{G}_n$ is not a finite-index subgroup of $SU_2(R_n)$ otherwise. By Proposition 6.2(ii), to do this, it suffices to show $|\chi(S\mathcal{G}_n)| < |\chi(SU_2(R_n))|$ for $n \notin \{8, 12, 16, 24\}$

Let S be the places of $F_n = K_n^+$ above 2∞ and denote by $\zeta_{F_n,S}(s)$ the Dedekind zeta function of F_n with the Euler factors at finite places in S omitted. Then the Euler–Poincaré characteristic of $\Gamma_n = SU_2(R_n)$ is given in [Ser71, Section 3.7]:

$$\begin{aligned} |\chi(\Gamma_n)| &= 2^{-[F_n:\mathbb{Q}]}|\zeta_{F_n,S}(-1)| \\ &= 2^{-[F_n:\mathbb{Q}]}|\zeta_{F_n}(-1)| \prod_{\mathfrak{p}|2} |1 - N_{F_n/\mathbb{Q}}(\mathfrak{p})| \\ &\geq 2^{-[F_n:\mathbb{Q}]}|\zeta_{F_n}(-1)|. \end{aligned} \tag{7.1}$$

By the functional equation for ζ_{F_n},

$$|\zeta_{F_n}(-1)| = \zeta_{F_n}(2)|\mathrm{Disc}(F_n)|^{3/2}(2\pi^2)^{-[F_n:\mathbb{Q}]},$$

and by [Was82, Proposition 2.7],

$$|\mathrm{Disc}(K_n)| = \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

As for F_n, let $f = \sqrt{|N_{F_n/\mathbb{Q}}\,\mathrm{Disc}(K_n/F_n)|}$. Then $f = 1$ unless n is a power of 2, in which case $f = 2$. Now we have

$$|\mathrm{Disc}(F_n)| = \sqrt{\frac{|\mathrm{Disc}(K_n)|}{|N_{F_n/\mathbb{Q}}\,\mathrm{Disc}(K_n/F_n)|}} = \frac{n^{\phi(n)/2}}{f\prod_{p|n} p^{\phi(n)/(2(p-1))}}$$

using standard properties of the discriminant in towers [Neu99, Corollary 2.10, p. 202].

Hence,

$$\begin{aligned} |\chi(\Gamma_n)| &\geq 2^{-[F_n:\mathbb{Q}]}|\zeta_{F_n}(-1)| = \zeta_{F_n}(2)|\mathrm{Disc}(F_n)|^{3/2}(2\pi)^{-2[F_n:\mathbb{Q}]} \\ &> |\mathrm{Disc}(F_n)|^{3/2}(2\pi)^{-2[F_n:\mathbb{Q}]} \\ &= \left(\frac{n^{\phi(n)/2}}{f\prod_{p|n} p^{\phi(n)/(2(p-1))}}\right)^{3/2}(2\pi)^{-2[F_n:\mathbb{Q}]} \end{aligned}$$

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press

$$= \frac{1}{f^{3/2}}\left(\left(\frac{n}{\prod_{p|n} p^{1/(p-1)}}\right)^{3/2}(2\pi)^{-2}\right)^{[F_n:\mathbb{Q}]}$$
$$> \frac{1}{2^{3/2}}\left(\left(\frac{n}{2\prod_{p|n,\, p>2} p^{1/2}}\right)^{3/2}(2\pi)^{-2}\right)^{[F_n:\mathbb{Q}]}$$
$$> \frac{1}{2^{3/2}}\left(\left(\frac{n}{2(n/4)^{1/2}}\right)^{3/2}(2\pi)^{-2}\right)^{[F_n:\mathbb{Q}]} = \frac{\left(n^{3/4}(2\pi)^{-2}\right)^{[F_n:\mathbb{Q}]}}{2\sqrt{2}},$$

which is greater than $\frac{1}{2\sqrt{2}}$ and hence greater than $\frac{1}{12} - \frac{1}{2n}$ as long as $n > 134.5 > (2\pi)^{8/3}$. If $n \notin \{8,12,16,24\}$, $4|n$, and $8 < n \leq 132$, then it can be manually checked from (7.1) that we still have $|\chi(\Gamma_n)| > \frac{1}{12} - \frac{1}{2n}$. Reassuringly, $\chi(\Gamma_n) = 1/12 - 1/(2n)$ for $n = 8,12,16,24$. Hence, $[\mathrm{SU}_2(R_n) : \mathrm{S}\mathcal{G}_n] = \infty$ for $4|n$, $n \geq 8$, and $n \notin \{8,12,16,24\}$ by Proposition 6.2(ii), proving Theorem 1.3(ii).

To prove Theorem 1.3(i), note that $n = [\mathcal{G}_n : \mathrm{S}\mathcal{G}_n] = [\mathrm{U}_2^{\zeta}(R_n) : \mathrm{SU}_2(R_n)]$ by Proposition 2.1(i) and (2.4). Hence, $[\mathrm{SU}_2(R_n) : \mathrm{S}\mathcal{G}_n] = [\mathrm{U}_2^{\zeta}(R_n) : \mathcal{G}_n]$, and so Theorem 1.3(ii) together with Theorem 1.1(i) implies Theorem 1.3(i).

The proof of Theorem 1.3(iii) is similar: both surjections $\mathcal{G}_n \twoheadrightarrow \mathrm{P}\mathcal{G}_n \cong \overline{\mathcal{G}}_n$ and $\mathrm{U}_2^{\zeta}(R_n) \twoheadrightarrow \mathrm{PU}_2^{\zeta}(R_n)$ have kernel of order n.

Hence, $[\mathrm{U}_2^{\zeta}(R_n) : \mathcal{G}_n] = [\mathrm{PU}_2^{\zeta}(R_n) : \mathrm{P}\mathcal{G}_n]$. But then we have

$$\pi(\mathcal{G}_n) = G(4,n) \cong \mathrm{P}\mathcal{G}_n \subseteq \pi(\mathrm{U}_2^{\zeta}(R_n)) \cong \mathrm{PU}_2^{\zeta}(R_n) \subseteq \mathrm{SO}_3(R_n^+).$$

Hence, $[\mathrm{U}_2^{\zeta}(R_n) : \mathcal{G}_n] = \infty$ implies $[\mathrm{SO}_3(R_n^+) : G(4,n)] = \infty$. Theorem 1.3(iii) then follows from Theorem 1.3(i) and Theorem 1.1(i), completing the proof of Theorem 1.3.

References

[BRS15] A. Bocharov, M. Roetteler, and K. M. Svore, *Efficient synthesis of probabilistic quantum circuits with fallback*. Phys. Rev. A **91**(2015), 052317.

[Bro94] K. S. Brown, *Cohomology of groups*. Graduate Texts in Mathematics, 87, Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.

[FGKM15] S. Forest, D. Gosset, V. Kliuchnikov, and D. McKinnon, *Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets*. J. Math. Phys. **56**(2015), no. 8, 082201. http://arxiv.org/abs/10.1063/1.4927100

[IJK+a] C. Ingalls, B. W. Jordan, A. Keeton, A. Logan, and Y. Zaytman, *The corank of unitary groups over cyclotomic rings*. Preprint, 2019. arXiv:1911:02137.

[IJK+b] C. Ingalls, B. W. Jordan, A. Keeton, A. Logan, and Y. Zaytman, *Quotient graphs and amalgam presentations for unitary groups over cyclotomic rings*. Preprint, 2020. arXiv:2001:01695.

[Nab11] G. L. Naber, *Topology, geometry, and gauge fields*. 2nd ed., Texts in Applied Mathematics, 25, Springer, New York, 2011. http://arxiv.org/abs/10.1007/978-1-4419-7254-5

[Neu99] J. Neukirch, *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften, 322, Springer-Verlag, Berlin, 1999. http://arxiv.org/abs/10.1007/978-3-662-0398-0

[NC00] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[RS99] C. Radin and L. Sadun, *On 2-generator subgroups of* SO(3). Trans. Amer. Math. Soc. **351**(1999), no. 11, 4469–4480. http://arxiv.org/abs/10.1090/S0002-9947-99-02397-1

[Sar15] P. Sarnak, *Letter to Scott Aaronson and Andy Pollington on the Solovay-Kitaev theorem and golden gates*, 2015. http://publications.ias.edu/sarnak/paper/2637

[Ser71] J.-P. Serre, *Cohomologie des groups discrets*. Prospects in Mathematics (Proc. Sympos., Princeton Univ., Princeton, NJ, 1970), Ann. of Math. Studies, 70, 1971, pp. 77–169.
[Ser09] J.-P. Serre, *Le groupe quaquaversal, vu comme groupe S-arithmétique*. Oberwolfach Rep. **6** (2009), no. 2, 1421–1426.
[Vig80] M.-F. Vignéras, *Arithmétique des algébres de quaternions.* Lecture Notes in Mathematics, 800, Springer, Berlin, 1980.
[Was82] L. C. Washington, *Introduction to cyclotomic fields*. Graduate Texts in Mathematics, 83, Springer-Verlag, Berlin, 1982. http://arxiv.org/abs/10.1007/978-1-4684-0133-2
[Web99] H. Weber, *Lehrbuch der Algebra. Vol.* II. *Zweite Auflage*, Vieweg, Braunschweig, 1899.

School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada
e-mail: cingalls@math.carleton.ca

Department of Mathematics, Box B-630, Baruch College, The City University of New York, One Bernard Baruch Way, New York, NY 10010, USA
e-mail: bruce.jordan@baruch.cuny.edu

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540, USA
e-mail: agk@idaccr.org ykzaytm@idaccr.org

The Tutte Institute for Mathematics and Computation, P.O. Box 9703, Terminal, Ottawa, ON K1G 3Z4, Canada

and

School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada
e-mail: adam.m.logan@gmail.com

https://doi.org/10.4153/S0008439520000727 Published online by Cambridge University Press