Products of finite order rotations and quantum gates universality

Katarzyna Karnas[1] and Adam Sawicki[1]

[1]Center for Theoretical Physics PAS, Al. Lotników 32/46, 02-668, Warszawa, Poland

Abstract

We consider a product of two finite order quantum $SU(2)$-gates U_1, U_2 and ask when $U_1 \cdot U_2$ has an infinite order. Using the fact that $SU(2)$ is a double cover of $SO(3)$ we actually study the product $O(\gamma, \vec{k}_{12})$ of two rotations $O(\phi, \vec{k}_1) \in SO(3)$ and $O(\phi, \vec{k}_2) \in SO(3)$ about axes $\vec{k}_1$, $\vec{k}_2 \in \mathbb{R}^3$. In particular we focus on the case when $\vec{k}_1 \cdot \vec{k}_2 = 0$, and $\phi_1 = \phi = \phi_2$ are rational multiple of π and show that γ is not a rational multiple of π unless $\phi \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$. The proof presented in this paper boils down to finding all pairs $\gamma, \phi \in \{a\pi : a \in \mathbb{Q}\}$ that are solutions of $\cos \frac{\gamma}{2} = \cos^2 \frac{\phi}{2}$.

1 Introduction

A finite subset $\mathcal{S} = \{g_1, \ldots, g_k\}$ of a Lie group G is called a *generating set* if the set

$$< \mathcal{S} >:= \{g_{i_1}^{k_1} \cdot \ldots \cdot g_{i_m}^{k_m} : g_{i_j} \in \mathcal{S}, k_j \in \mathbb{N}, i_j \in \{1, \ldots, n\}\}, \tag{1}$$

consisting of all words built using elements of $\mathcal{S}$ is dense in G. The problem of characterisation of generating sets for various types of Lie groups has recently attracted much more interest, in particular due to its direct connection to the quantum gates universality [4, 6, 16, 17, 18, 20, 21] (c.f. [7, 23] for a similar problem of generating Hamiltonians). In short words the set of quantum gates is universal if and only if it is a generating set for $SU(d)$ or $SO(d)$. It is worth mentioning that for abelian G the smallest generating set consist of one element whereas for nonabelian it is typically enough to use two elements [15].

Although $< \mathcal{S} >$ is closed under group multiplication it might not be a group itself as the inverses of some elements may not be in $< S >$. Nevertheless, its closure has a group structure (see fact 2.6 in [20]). As was shown by Schur in his solution to the Burnside problem (see lemma 36.2 of [8]), infinite but finitely generated groups of matrices over $\mathbb{R}$ or $\mathbb{C}$ always contain infinite order elements. Note that the necessary condition for $\mathcal{S}$ to be universal is that $< \mathcal{S} >$ contains infinite number of elements. Verification of this can be thus accomplished by pointing one infinite order element in $< \mathcal{S} >$. The efficiency of this approach, however, is limited when all generators (elements of $\mathcal{S}$) are of the finite order. In this case one should consider products of elements from $\mathcal{S}$, as the noncommutativity of G implies that the composition of two (or more) finite order elements may be of infinite order. In fact, the main step in the proof contained in [10] of the universality for gates $\{H, T\left(\frac{\pi}{8}\right)\} \subset SU(2)$, where H is the Hadamard gate and $T_{\frac{\pi}{8}}$ is a phase gate (both are elements of finite order), i.e.

$$H = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; T_{\frac{\pi}{8}} = \begin{pmatrix} e^{i\pi/8} & 0 \\ 0 & e^{-i\pi/8} \end{pmatrix}, \tag{2}$$

is showing that $U = H \cdot T_{\frac{\pi}{8}}$ is of infinite order. The method used in the proof boils down to finding the minimal polynomial for $e^{i\phi}$, where the spectrum of U is given by $\{e^{i\phi}, e^{-i\phi}\}$. If this polynomial is not a cyclotomic polynomial then ϕ is not a rational multiple of π and U is of infinite order. Although the application of this method for gates H and $T_{\frac{\pi}{8}}$ is a simple exercise [2] it becomes much more difficult for $\{H, T_\phi\}$, where ϕ is any rational multiple of π or for an arbitrary pair of $SU(2)$ gates. In this short paper we discuss cases when one can efficiently prove that the product of two finite order elements from $SU(2)$ is of infinite order. As the group $SU(2)$ is the double cover of $SO(3)$ we work with matrices belonging to $SO(3)$ rather than to $SU(2)$. In particular we focus on the case when $\vec{k}_1 \cdot \vec{k}_2 = 0$, and $\phi_1 = \phi = \phi_2$ are rational multiples of π and show that γ is not a rational multiple of π unless $\phi \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$. The result obtained for this case is presented as our main theorem whereas, to make our notation clearer, we call all the previously known results as facts and our auxiliary results by lemmas. Our proof boils down

to finding all pairs $\gamma, \phi \in \{a\pi : a \in \mathbb{Q}\}$ that are solutions of $\cos \frac{\gamma}{2} = \cos^2 \frac{\phi}{2}$. In order to show that γ is not a rational multiple of π one can for example find the minimal polynomial for $e^{i\gamma}$ and check if this polynomial is cyclotomic. This approach was studied in [19], where in section 3.1 the author shows that in general the problem is intractable. Another approach that one could follow is finding the minimal polynomial for $\cos^2 \phi$ and showing that its resultant with any of the Chebyshev polynomials in nonzero. This, however, again turns out to be hopeless calculation. Our approach consists of the following steps:

1. Write equation $\cos \frac{\gamma}{2} = \cos^2 \frac{\phi}{2}$ as $2 \cos \frac{\gamma}{2} = 1 + \cos \phi$.

2. For ϕ - a rational multiple of π show that at least one coefficient of the minimal polynomial of $\cos \phi$ is noninteger (see lemma 13).

3. Prove that the minimal polynomial for $2 \cos \frac{\gamma}{2}$ has integer coefficients when γ is rational multiple of π (see lemma 16).

4. Using the companion matrix formalism described in section 3.1 find formulas for coefficients of the minimal polynomial of $1 + \cos \phi$ in terms of the coefficients of the minimal polynomial for $\cos \phi$ (see section 5).

5. Show that coefficients of the minimal polynomial for $1 + \cos \phi$ are not all integers if $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$ (see section 5).

The presented approach is both direct and simple. As we show all the above steps involve easy calculations. In the last section we discuss some cases when the rotation angles are not equal and the rotation axes are not perpendicular.

2 Results

Let $O(\phi, \vec{k})$ be a rotation by ϕ around the axis $\vec{k}$. We will consider three rotations about axes $\vec{k}_x, \vec{k}_y$ and $\vec{k}_z$ all by the same angle ϕ:

$$O(\phi, \vec{k}_x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \phi & \sin \phi \\ 0 & -\sin \phi & \cos \phi \end{pmatrix}, O(\phi, \vec{k}_y) = \begin{pmatrix} \cos \phi & 0 & \sin \phi \\ 0 & 1 & 0 \\ -\sin \phi & 0 & \cos \phi \end{pmatrix}, O(\phi, \vec{k}_z) = \begin{pmatrix} \cos \phi & \sin \phi & 0 \\ -\sin \phi & \cos \phi & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3}$$

The corresponding $SU(2)$ matrices are:

$$U(\frac{\phi}{2}, \vec{k}_x) = \begin{pmatrix} \cos \frac{\phi}{2} & \sin \frac{\phi}{2} \\ -\sin \frac{\phi}{2} & \cos \frac{\phi}{2} \end{pmatrix}, U(\frac{\phi}{2}, \vec{k}_y) = \begin{pmatrix} \cos \frac{\phi}{2} & i \sin \frac{\phi}{2} \\ i \sin \frac{\phi}{2} & \cos \frac{\phi}{2} \end{pmatrix}, U(\frac{\phi}{2}, \vec{k}_z) = \begin{pmatrix} e^{i\frac{\phi}{2}} & 0 \\ 0 & e^{-i\frac{\phi}{2}} \end{pmatrix}. \tag{4}$$

The product of any two of the above three rotations (3) is again a rotation by an angle γ where:

$$2 \cos \gamma + 1 = \cos^2 \phi + 2 \cos \phi. \tag{5}$$

Using trigonometric identities we can write (5) in a simpler form:

$$\pm \cos \frac{\gamma}{2} = \cos^2 \frac{\phi}{2}. \tag{6}$$

Note that the same equation is obtained from the product of any two unitary matrices (4), i.e. the resulting matrix has spectrum $\{e^{-i\frac{\gamma}{2}}, e^{i\frac{\gamma}{2}}\}$, where γ is determined by equation (6). Our main technical result is

Theorem 1. *Assume ϕ is a rational multiple of π. Then γ given by (6) is a rational multiple of π if and only if $\phi \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$.*

Using theorem 1, one easily deduces the following:

Corollary 2. *Assume ϕ is a rational multiple of π and $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$. Let $O(\phi, \vec{k}_1), O(\phi, \vec{k}_2) \in SO(3)$ be rotations around orthogonal axes $\vec{k}_i \perp \vec{k}_j$, by the angle ϕ. Then $O(\gamma, \vec{k}) = O(\phi, \vec{k}_1)O(\phi, \vec{k}_2)$ is the rotation by an angle γ which is an irrational multiple of π. Moreover, the set generated by $\{O(\phi, \vec{k}_1), O(\phi, \vec{k}_2)\}$ or by the corresponding unitary matrices $\{U(\phi/2\vec{k}_1), U(\phi/2, \vec{k}_2)\}$ is infinite if and only if $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$.*

Proof. We only need to verify the case $\phi \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$. But in this case matrices (3) have entries in $\{1, -1\}$ and generate either permutation group S_3 or finite abelian group. $\square$

3 Number fields and minimal polynomials

In this section we present basic facts concerning minimal polynomials. Using the *companion matrix* formalism we explain the relationship between the minimal polynomials of two algebraic numbers and the minimal polynomial of their sum and product.

Recall that $\alpha \in \mathbb{C}$ is an *algebraic number* if it is a root of a polynomial $p \in \mathbb{Q}[x]$, i.e. a polynomial with rational coefficients. The order of α is the order of the monic polynomial $m_\alpha \in \mathbb{Q}[x]$ of the least degree, having α as a root. In other words m_α is irreducible over $\mathbb{Q}$, i.e. it cannot be decomposed into a product of polynomials from $\mathbb{Q}[x]$. This monic polynomial is called the minimal polynomial of α and is uniquely determined by α. If α is not algebraic then it is called *transcendental*. Algebraic numbers form an infinite countable set, $\mathbb{A}$ [3], whereas the set $\mathbb{T}$ of transcendental numbers is uncountable and we have $\mathbb{A} \cup \mathbb{T} = \mathbb{C}$. The examples of algebraic numbers are all integers, rational numbers or the numbers of the form: $\sqrt[k]{n}$, $\cos \frac{2k\pi}{n}$, $e^{2ik\pi/n}$, $\sin \frac{2k\pi}{n}$, where $n, k \in \mathbb{N}$. On the other hand the numbers π, e are known to be transcendental. Obviously if $a \in \mathbb{A} \backslash \{0\}$ and $t \in \mathbb{T}$, then also $a^{-1}, -a$ are algebraic numbers and $t^{-1}, -t$ are transcendental numbers.

Having defined algebraic and transcendental numbers, we introduce the notion of a field extension. Let $\mathbb{L}$ be a field that contains $\mathbb{Q}$ as a subfield and let S be a subset of $\mathbb{L}$. We define the field $\mathbb{Q}(S)$ to be the smallest field that contain both $\mathbb{Q}$ and S. We will call $\mathbb{Q}(S)$ a field extension of $\mathbb{Q}$ obtained by adjoining elements of S. If all elements in $\mathbb{Q}(S)$ are algebraic numbers then the field $\mathbb{Q}(S)$ is called an algebraic field extension. One can view $\mathbb{Q}(S)$ as a vector space over $\mathbb{Q}$. The dimension of this space, denoted by $[\mathbb{Q}(S):\mathbb{Q}]$, will be called a degree of $\mathbb{Q}(S)$ over $\mathbb{Q}$. If $[\mathbb{Q}(S):\mathbb{Q}] < \infty$ the extension is the finite extension. Finite extensions are algebraic as for any $\alpha \in \mathbb{Q}(S)$ numbers $1, \alpha, \alpha^2, \ldots, \alpha^{[\mathbb{Q}(S):\mathbb{Q}]}$ are linearly dependent over $\mathbb{Q}$ which means there is a polynomial $p \in \mathbb{Q}[x]$ which satisfies $p(\alpha) = 0$. The converse is not true.

In this paper we will deal with extensions $Q(S)$, where $S = \{\alpha\}$ and α is an algebraic number of order n whose minimal polynomial is $m_\alpha \in \mathbb{Q}[x]$. For convenience the field $\mathbb{Q}(S)$ will be denoted by $\mathbb{Q}(\alpha)$. Among elements belonging to $\mathbb{Q}(\alpha)$ are all polynomial expressions in α. It turns out that these expressions already form a field which contains α and $\mathbb{Q}$ and therefore they constitute $\mathbb{Q}(\alpha)$. We note that for all $p \in \mathbb{Q}[x]$ satisfying $p(\alpha) = 0$ the corresponding expression is 0. Thus $\mathbb{Q}(\alpha)$ is isomorphic $\mathbb{Q}[x]/(m_\alpha)$, where (m_α) is an ideal of polynomials vanishing on α. Using the polynomial division formula, any element $\beta \in \mathbb{Q}(\alpha)$ can be written as $\beta = m_\alpha(\alpha)f(\alpha) + r(\alpha)$, where $\deg r < \deg m_\alpha = n$. Thus any element of $Q(\alpha)$ is a polynomial in α of degree less than n with coefficients in $\mathbb{Q}$. Therefore $Q(\alpha)$ is a finite extension whose basis is $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and $[\mathbb{Q}(\alpha):\mathbb{Q}] = n$. Hence any element $\beta \in \mathbb{Q}(\alpha)$ is algebraic and $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. One can show that the order of β is a divisor of the order of α, i.e. a divisor of n and is given by

$$\deg m_\beta = [\mathbb{Q}(\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}]/[\mathbb{Q}(\alpha):\mathbb{Q}(\beta)], \tag{7}$$

where m_β is the minimal polynomial for β.

Consider field extension $Q(e^{i\phi})$ where ϕ is a rational multiple of π. As $e^{i\phi}$ is a root of unity, $Q(e^{i\phi})$ is a finite algebraic extension. Next, $\sin \phi, \cos \phi$ depend on $e^{i\phi}$ as $\cos \phi = \frac{e^{i\phi} + e^{-i\phi}}{2}$ and $\sin \phi = \frac{e^{i\phi} - e^{-i\phi}}{2i}$ and therefore $\mathbb{Q}(\cos \phi) \subset \mathbb{Q}(e^{i\phi})$ and $\mathbb{Q}(\sin \phi) \subset \mathbb{Q}(e^{i\phi})$. The minimal polynomials of these functions are characterised by several unique properties. In this paper we place particular emphasis on the minimal polynomials ψ_n for $\cos \frac{2\pi}{n}$ and η_n for $2\cos \frac{\phi}{2}$. Their properties will be crucial in the proof of theorem 1, therefore we describe them at length in section 4.

3.1 Companion matrix formalism

The notion of a minimal polynomial can be generalized to matrices over $\mathbb{Q}$. We say that a square matrix $M \in \mathrm{M}_n(\mathbb{Q})$ is a root of a polynomial $p \in \mathbb{Q}[x]$ if $p(M) = 0$ (in other words p *annihilates* M). Let $\chi_M \in \mathbb{Q}[x]$ be the characteristic polynomial of $M \in \mathrm{M}_n(\mathbb{Q})$. By the Cayley-Hamilton theorem M is a root of its own characteristic polynomial, i.e. $\chi_M(M) = 0$. The monic polynomial $m_M \in \mathbb{Q}[x]$ of the smallest degree that is irreducible over $\mathbb{Q}$ and annihilates M will be called the *minimal polynomial* of M. Conversely, to every minimal polynomial $m_\alpha \in \mathbb{Q}[x]$ we can associate the matrix called a *companion matrix* M_α, defined as follows:

Definition 3. *Let m_α be a minimal polynomial of α of degree* $\deg m_\alpha = d$ *given by* $m_\alpha(x) = x^d + \sum_{k=0}^{d-1} c_k \cdot x^k$.

The companion matrix M_α *is the* $n \times n$ *matrix over* $\mathbb{Q}$ *defined as*

$$M_\alpha = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -c_{d-2} \\ 0 & 0 & 0 & \ldots & 1 & -c_{d-1} \end{pmatrix}. \tag{8}$$

One can show (see [1]) that

$$\chi_{M_\alpha} = m_{M_\alpha} = m_\alpha. \tag{9}$$

Assume $\alpha, \beta \in \mathbb{A}$ and their minimal polynomials are m_α and m_β respectively. Companion matrix formalism allows us to find polynomials that annihilate $\alpha\beta$ and $\alpha + \beta$ knowing polynomials m_α and m_β. To this end we construct matrices

$$M_{\alpha\beta} = M_\alpha \otimes M_\beta, \quad M_{\alpha+\beta} = M_\alpha \otimes I_\beta + I_\alpha \otimes M_\beta. \tag{10}$$

The characteristic polynomials of these matrices annihilate $\alpha\beta$ and $\alpha + \beta$ respectively. We note, however, that $m_{\alpha+\beta}$, $m_{\alpha\beta}$ may not be equal to characteristic polynomials of $M_{\alpha+\beta}$ and $M_{\alpha\beta}$ as these matrices are not companion matrices in the true sense of this word. Nevertheless, the equality holds when either α or β belongs to $\mathbb{Q}$.

Fact 4. *Assume that* $\alpha \in \mathbb{Q}$ *and* $\beta \notin \mathbb{Q}$. *Then* $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}]$ *and the minimal polynomials of* $\alpha\beta$ *and* $\alpha + \beta$ *are given by the characteristic polynomials of*

$$M_{\alpha\beta} = \alpha M_\beta, \quad M_{\alpha+\beta} = \alpha I_\beta + M_\beta, \tag{11}$$

where M_α *and* M_β *are the companion matrices of* α *and* β.

Proof. Note that m_α is the first order polynomial $m_\alpha(x) = x - \alpha$. Thus M_α is a 1×1 matrix $M_\alpha = \alpha$. Using the companion matrix formalism we know that the characteristic polynomials of the matrices (11) annihilate $\alpha\beta$ and $\alpha + \beta$ respectively. We also know that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha\beta)$. Using formula (7) we get that $\deg m_{\alpha+\beta} = \deg m_{\alpha\beta} = [\mathbb{Q}(\beta) : \mathbb{Q}] = \deg(m_\beta)$. But the degrees of $\chi_{M_{\alpha\beta}}$ and $\chi_{M_{\alpha+\beta}}$ are also $\deg m_\beta$. The result follows. $\square$

In general the degrees for $\alpha, \beta \in \mathbb{A}$ are bounded by

$$\max(\deg m_\alpha, \deg m_\beta) \le \deg m_{\alpha+\beta, \alpha\beta} \le \deg m_\alpha \deg m_\beta.$$

The lower bound corresponds to the case when one of the field extensions $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ is a subfield of the second one, e.g. $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$. Then both $\alpha + \beta$ and $\alpha\beta$ belong to the larger field extension. In that case the degrees of the minimal polynomials of $m_{\alpha+\beta}$ and $m_{\alpha\beta}$ are equal to the degree of $\mathbb{Q}(\beta)$ by definition. The other case is when $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ have no common elements different than rational numbers. Then $\mathbb{Q}(\alpha\beta)$ and $Q(\alpha + \beta)$ are the field extensions of the degree at most $[\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}]$. In order to check it, let $\{1, \alpha, \ldots, \alpha^m\}$ be a basis of $\mathbb{Q}(\alpha)$ and $\{1, \beta, \ldots, \beta^n\}$ be a basis of $\mathbb{Q}(\beta)$ such that $\alpha^i \neq \beta^j$ for all $1 \le i \le m$, $1 \le j \le n$. Then the basis of $\mathbb{Q}(\alpha\beta)$ consists of all $\alpha^i\beta^j$'s and the maximal number of such *different* basis elements is $[\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}]$. The same holds for $\mathbb{Q}(\alpha + \beta)$. Thus typically we need to find $\chi_{M_{\alpha\beta}}$ or $\chi_{M_{\alpha+\beta}}$ and factorize it over $\mathbb{Q}$ obtaining $\chi_{M_{\alpha+\beta, \alpha\beta}} = m_{\alpha+\beta, \alpha\beta} \cdot p_1 \cdot \ldots \cdot p_k$.

Polynomials with integer coefficients are characterised by special properties. Particularly important are the *primitive* polynomials for which the greatest common divisor of their coefficients is equal to one. The set of primitive polynomials is closed under multiplication in $\mathbb{Z}[x]$, in other words:

Fact 5. *[11] Let* $f, g \in \mathbb{Z}[x]$ *be primitive polynomials. Then the product* $f \cdot g$ *is also a primitive polynomial.*

Every polynomial with rational coefficients $f \in \mathbb{Q}[x]$ can be associated with a primitive polynomial $\tilde{f}$ such, that

$$f(x) = \alpha\tilde{f}, \ \alpha \in \mathbb{Q}, \tag{12}$$

and the pair $(\tilde{f}, \alpha)$ is unique. This fact allows us to formulate the following theorem that we prove for the reader's convenience.

4

Lemma 6 (Gauss lemma). *[11] Let f be a polynomial with integer coefficients. f is reducible over $\mathbb{Q}$ if and only if it is reducible over $\mathbb{Z}$.*

Proof. The first part of the proof is trivial since $\mathbb{Z} \subset \mathbb{Q}$. Thus it is enough to prove that reducibility over $\mathbb{Q}$ implies reducibility over $\mathbb{Z}$.

Let $f \in \mathbb{Z}[x]$ be a primitive polynomial, reducible over $\mathbb{Q}$ (if not, there is always a pair $(\tilde{f}, \alpha)$ such, that $\tilde{f}$ is primitive and $\alpha \in \mathbb{Z}$). Assume that f decomposes as $f = g \cdot h$, where $g, h \in \mathbb{Q}[x]$. By the identity (12) these polynomials can be expressed as $g = \gamma \tilde{g}$, $h = \chi \tilde{h}$, where $\gamma, \chi \in \mathbb{Q}$ and $\tilde{g}, \tilde{h}$ are primitive polynomials. Therefore we have $f = g \cdot h = \gamma\chi\tilde{g}\tilde{h}$, where $\tilde{g} \cdot \tilde{h}$ is a primitive polynomial.

Let us substitute $\gamma\chi = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$, $\gcd(p, q) = 1$. Hence

$$qf = p\tilde{g} \cdot \tilde{h}. \tag{13}$$

Since f and $\tilde{g} \cdot \tilde{h}$ are primitive, the greatest common divisor of the coefficients of the left and right hand side of (13) are equal q and p respectively. Thus $p = q$, which implies $\gamma\chi = 1$ and $f = \tilde{g} \cdot \tilde{h}$ and $f = \tilde{g}\tilde{h} \in \mathbb{Z}[x]$. This completes the proof. $\qquad\square$

4 Trigonometric minimal polynomials

By trigonometric polynomials we will understand the minimal polynomials for $\cos\phi, \sin\phi, 2\cos\frac{\phi}{2}, \tan\phi$, where ϕ is a rational multiple of π. A detailed description of their properties was given in e.g. [5, 22, 24, 25]. In this paper we will concentrate on minimal polynomials for $\cos\phi$ and $2\cos\frac{\phi}{2}$, that are closely related to Chebyshev polynomials of the first kind.

Definition 7. *Chebyshev polynomials of the first kind $T_k(x)$, $k = 0, 1, \ldots$ are defined by the recurrence formula*

$$T_k(x) = 2xT_{k-1}(x) - T_{k-2}(x), \ T_0(x) = 1, \ T_1(x) = x. \tag{14}$$

Equivalently, $T_k(x)$'s are the polynomials satisfying

$$T_k(\cos\phi) = \cos k\phi. \tag{15}$$

From the formula (14) one can deduce properties of the coefficients of Chebyshev polynomials.

Fact 8. *Let $T_k(x) = \sum_{i=0}^{k} c_i x^i$ be the Chebyshev polynomial of the first kind of the degree k. The coefficients $c_0, \ldots, c_k$ satisfy:*

1. *$c_0, \ldots, c_k$ are integer numbers.*

2. *The leading coefficient c_k is equal to 2^{k-1}.*

3. *$T_k(x)$ is a polynomial of only odd/even powers of x if k is an odd/even number respectively.*

4. *If k is even, then the free term c_0 is given by $c_0 = \pm 1$.*

5. *If k is odd, then the coefficients c_0, c_1 are equal $c_0 = 0$, $c_1 = \pm k$.*

Assume that ϕ is a rational multiple of π. In this case one can express the minimal polynomial of $\cos\phi$ using the Chebyshev polynomials and vice versa. The explicit expressions are given in the following:

Fact 9. *[22, 24] A minimal polynomial $\psi_n(x)$ of $\cos\frac{2\pi}{n}$ is a polynomial defined as*

$$\psi_1(x) = x - \cos 2\pi = x - 1, \quad \psi_2 = x - \cos\pi = x + 1, \tag{16}$$

$$\psi_n(x) = \prod_{\substack{1 \le k \le \lfloor n/2 \rfloor \\ \gcd(k,n) = 1}} \left(x - \cos\frac{2k\pi}{n}\right), \ n \ge 3, \tag{17}$$

$$\deg\psi_n(x) = \begin{cases} 1 & n = 1, 2 \\ \frac{\varphi(n)}{2} & n \ge 3 \end{cases}, \tag{18}$$

where $\varphi(n)$ is the Euler totient function *counting the positive integers $k \leq n$ that are coprime to n. The canonical identity relating $\psi_n(x)$ with Chebyshev polynomials of the first kind is of the form*

$$2^k \prod_{d|n} \psi_d(x) = T_{k+1}(x) - T_k(x), \;\; n = 2k+1, \tag{19}$$

$$2^k \prod_{d|n} \psi_d(x) = T_{k+1}(x) - T_{k-1}(x), \;\; n = 2k. \tag{20}$$

Remark 10. Note that the sum in (17) is over $1 \leq k \leq \lfloor n/2 \rfloor$, $\gcd(k,n) = 1$ instead of $1 \leq k \leq n$. It stems from the symmetry of cosine, *i.e.* $\cos \phi = \cos(-\phi)$. Note that for every $\phi = \frac{2k\pi}{n}$ the opposite angle is defined as $-\phi = -\frac{2k\pi}{n} = \frac{2(n-k)\pi}{n}$. By properties of the greatest common divisor [13], $\gcd(k,n) = 1$ implies $\gcd(n-k,n) = 1$. Thus every root $\cos\frac{2k\pi}{n}$, where $1 \leq k \leq \lfloor n/2 \rfloor$, is equal to the root $\cos\frac{2(n-k)\pi}{n}$ where $\lfloor n/2 \rfloor < n - k < n$. Therefore $\cos\frac{2k\pi}{n}$ for $1 \leq k \leq \lfloor n/2 \rfloor$ are all the possible roots of $\psi_n(x)$.

Before we formulate the lemma describing a important property of $\psi_n(x)$ we will present definition of the Möbius function that allows us to invert (20) and (19) and express $\psi_n(x)$ as a function of Chebyshev polynomials [5].

Definition 11. *Möbius function is an integer function taking three possible values $\mu(n) = \{-1, 0, 1\}$. It depends on the prime factorisation of k (this means a unique representation of n as a product of prime numbers). Let $n = p_1^{n_1} \dots p_m^{n_m}$, then (1) $\mu(n) = 0$ if at least one n_i is larger than one, (2) $\mu(n) = -1$ if m is an odd number and $n_1 = \dots = n_m = 1$ (we say that n is* square free*), (3) $\mu(n) = 1$ if m is even and n is square free.*
The Möbius function satisfies the canonical identity [13]

$$\sum_{d|n} \mu(d) = \begin{cases} 0, & n > 1 \\ 1, & n = 1 \end{cases}. \tag{21}$$

Fact 12. *[5] For $n \geq 3$, odd and $m \geq 1$, $m, n \in \mathbb{N}$ the Möbius inverses of (19) and (20), given by the Möbius inversion formula, are the following*

$$\psi_n(x) = \prod_{d|n} \left[2^{-\lfloor d/2 \rfloor} \left(T_{\lfloor d/2 \rfloor + 1}(x) - T_{\lfloor d/2 \rfloor}(x) \right) \right]^{\mu(n/d)}, \tag{22}$$

$$\psi_{2^m n}(x) = \prod_{d|n} \left[\frac{2^{-\lfloor 2^{m-1}d \rfloor} \left(T_{\lfloor 2^{m-1}d \rfloor + 1}(x) - T_{\lfloor 2^{m-1}d \rfloor - 1}(x) \right)}{2^{-\lfloor 2^{m-2}d \rfloor} \left(T_{\lfloor 2^{m-2}d \rfloor + 1}(x) - T_{\lfloor 2^{m-2}d \rfloor - 1}(x) \right)} \right]^{\mu(n/d)}, \;\; m > 1, \tag{23}$$

$$\psi_{2^m n}(x) = \prod_{d|n} \left[\frac{2^{-d} \left(T_{\lfloor d \rfloor + 1}(x) - T_{\lfloor d \rfloor - 1}(x) \right)}{2^{-\lfloor d/2 \rfloor} \left(T_{\lfloor d/2 \rfloor + 1}(x) - T_{\lfloor d/2 \rfloor}(x) \right)} \right]^{\mu(n/d)}, \;\; m = 1. \tag{24}$$

The following property of $\psi_n(x)$ is crucial in proving theorem 1.

Lemma 13. *At least one coefficient of $\psi_n(x)$ is non-integer if $n \notin \{1, 2, 4\}$.*

Proof. Note that $\cos\frac{2k\pi}{n}$, $\gcd(k,n) = 1$ are integers for $n \in \{1, 2, 4\}$, thus the corresponding minimal polynomials $\psi_n(x)$ belong to $\mathbb{Z}[x]$. In other cases one can distinguish the following situations: 1) n is an odd prime number, 2) n is an odd composite number, 3) n is an even composite number.

1. In the case 1) n has exactly two divisors and the formula (19) simplifies to

   $$\psi_1(x)\psi_n(x) = (x-1)\psi_n(x) = 2^{-\lfloor n/2 \rfloor} \left(T_{\lfloor n/2 \rfloor + 1}(x) - T_{\lfloor n/2 \rfloor}(x) \right). \tag{25}$$

   Note that $T_{\lfloor n/2 \rfloor + 1}(x) - T_{\lfloor n/2 \rfloor}(x)$ is a difference of polynomials of the even and the odd degrees, therefore by fact 8 it has a free term equal ± 1 hence the free term of the right hand side is $\pm\frac{1}{2^{\lfloor n/2 \rfloor}}$. Note that the free term of left hand side is determined by the free term of $\psi_n(x)$. Comparing the left and right side of (25) one can see that the free term of $\psi_n(x)$, *i.e.* $c_0 = \pm\frac{1}{2^{\lfloor n/2 \rfloor}}$, must be a rational number since we consider $n \leq 3$.

2. In the case 2) we will prove that $\psi_n(x)$ has a non-integer free term by applying formula (22) and using properties of the Möbius function. Let $n = p_1^{n_1} \dots p_m^{n_m}$ be the prime factorisation of n. Let $\mathcal{D}_n^+$ and $\mathcal{D}_n^-$ be the sets of all square free (as in definition 11) divisors of n that have even and odd number of prime divisors

respectively. By (21) we have $|\mathcal{D}_n^+| = |\mathcal{D}_n^-|$. Note that the free term of the right hand side of (22) can be written in the form

$$c_0 = \pm \prod_{d|n} \left(\frac{1}{2^{\lfloor d/2 \rfloor}} \right)^{\mu(n/d)} = \pm \prod_{\frac{n}{d} \in \mathcal{D}_n^+ \cup \mathcal{D}_n^-} \left(\frac{1}{2^{\lfloor d/2 \rfloor}} \right)^{\mu(n/d)} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \lfloor d/2 \rfloor}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \lfloor d/2 \rfloor}}. \tag{26}$$

We next raise c_0 to the power $p = 2p_1 \cdot \ldots \cdot p_m$

$$c_0^p = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} p \lfloor d/2 \rfloor}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} p \lfloor d/2 \rfloor}} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} p(d-1)/2}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} p(d-1)/2}} = \frac{2^{-\frac{pk}{2} + \sum_{\frac{n}{d} \in \mathcal{D}_n^-} \frac{pd}{2}}}{2^{-\frac{pk}{2} + \sum_{\frac{n}{d} \in \mathcal{D}_n^+} \frac{pd}{2}}} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \frac{pd}{2}}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \frac{pd}{2}}}. \tag{27}$$

Note that c_0 is non-integer if and only if $c_0^p < 1$. In order to find the appropriate condition we use the fact that if $x = \frac{n}{d}$ belongs to $\mathcal{D}_n^-$ or $\mathcal{D}_n^+$ then

$$p \cdot d = p \frac{n}{x} = 2n \cdot y, \tag{28}$$

where y is the square-free product of such prime divisors of n that do not appear in prime factorisation of x. In particular, if m is an even number and $x \in \mathcal{D}_n^+$, then y must also belong to $\mathcal{D}_n^+$. Similarly $x \in \mathcal{D}_n^-$ implies that $y \in \mathcal{D}_n^-$. When m is odd one easily checks that $x \in \mathcal{D}_n^+$ implies that $y \in \mathcal{D}_n^-$ and *vice versa*.

Let us consider the case when m is an even number. Taking $pd = 2ny$ one can rewrite (27) as

$$c_0^p = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \frac{pd}{2}}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \frac{pd}{2}}} = \frac{2^{\sum_{y \in \mathcal{D}_n^-} ny}}{2^{\sum_{y \in \mathcal{D}_n^+} ny}} = \frac{2^{n \sum_{y \in \mathcal{D}_n^-} y}}{2^{n \sum_{y \in \mathcal{D}_n^+} y}}. \tag{29}$$

As one can easily see $c_0^p < 1$ if the following holds

$$\sum_{y \in \mathcal{D}_n^+} y - \sum_{y \in \mathcal{D}_n^-} y > 0. \tag{30}$$

Note that this expression is equivalent to the product

$$\sum_{y \in \mathcal{D}_n^+} y - \sum_{y \in \mathcal{D}_n^-} y = (1 - p_1) \ldots (1 - p_m), \tag{31}$$

which is always larger than zero if m is even, thus c_0 is non-integer in this case.

Next let us consider n such, that m is an odd number. Doing *mutatis mutandis* to the case when m is even one can transform (27) to the form

$$c_0^p = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} pd}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} pd}} = \frac{2^{\sum_{y \in \mathcal{D}_n^+} ny}}{2^{\sum_{y \in \mathcal{D}_n^-} ny}} = \frac{2^{n \sum_{y \in \mathcal{D}_n^+} y}}{2^{n \sum_{y \in \mathcal{D}_n^-} y}}, \tag{32}$$

thus the condition for $c_0^p < 1$ is given by

$$\sum_{y \in \mathcal{D}_n^+} y - \sum_{y \in \mathcal{D}_n^-} y = (1 - p_1) \ldots (1 - p_m) < 0. \tag{33}$$

Note that this is always satisfied if m is odd, which means that c_0^p is indeed smaller than one. This way we have proven lemma 13 for the case when $n > 1$ and n is odd.

3. In case 3) we will use the similar approach as for case 2). Recall that every even number n can be represented as $n = 2^\eta k$, where k - odd and $\eta \in \mathbb{Z}_+$. This allows us to define $\psi_n(x)$ by the formula (23). Let us define the

7

sets $\mathcal{D}_n^+$ and $\mathcal{D}_n^-$ like previously. Using fact 8 one can extract the free terms from (23) and (24) as

$$c_0 = \prod_{d|k} \left(\frac{2}{2^{2^{\eta-2}d}} \right)^{\mu(k/d)} = \frac{2^{2^{\eta-2}\sum_{\frac{n}{d}\in\mathcal{D}_n^-} d}}{2^{2^{\eta-2}\sum_{\frac{n}{d}\in\mathcal{D}_n^+} d}}, \quad \eta > 1, \tag{34}$$

$$c_0 = \prod_{d|k} \left(\frac{1}{2^{\lfloor d/2 \rfloor}} \right)^{\mu(k/d)} = \frac{2^{\sum_{\frac{n}{d}\in\mathcal{D}_n^-} \lfloor d/2 \rfloor}}{2^{\sum_{\frac{n}{d}\in\mathcal{D}_n^+} \lfloor d/2 \rfloor}}, \quad \eta = 1. \tag{35}$$

By properties of the Möbius function all the sums and products are over the same number of divisors. Note that (35) and (26) are exactly equal, whereas (34) has a very similar form to (26). Using very similar reasoning as in the case 2) we obtain immediately that c_0 is non-integer unless $n = 2, 4$, which completes the proof.

$\square$

Example: In this paragraph we will illustrate the method presented in the proof of lemma 13 with the example for $n = 15$. First, $\mathcal{D}_{15}^+ = \{1, 15\}$ and $\mathcal{D}_{15}^- = \{3, 5\}$. The coefficient c_0 of $\psi_{15}(x)$ is given by

$$c_0 = \frac{2^{\lfloor 5/2 \rfloor + \lfloor 3/2 \rfloor}}{2^{\lfloor 15/2 \rfloor + \lfloor 1/2 \rfloor}}. \tag{36}$$

Using the reasoning presented for the case 2) we raise c_0 to the power $p = 30$ and obtain the condition

$$c_0^{30} = \frac{2^{15(5+3)-15}}{2^{15(15+1)-15}} = \frac{2^{15\sum_{y\in\mathcal{D}_{15}^-} y}}{2^{15\sum_{y\in\mathcal{D}_{15}^+} y}} < 1 \Leftrightarrow \sum_{y\in\mathcal{D}_{15}^+} y - \sum_{y\in\mathcal{D}_{15}^-} y = 16 - 8 > 0.$$

Thus we have shown that $c_0 < 1$. On the other hand one can see immediately from definition (36) than c_0 for $\psi_{15}(x)$ is equal to $2^{-8} \notin \mathbb{Z}$.

The proof of theorem 1 presented in this paper is based also on properties of minimal polynomials for $2\cos\frac{\pi}{n}$. However, before we describe them, we will recall the notion of cyclotomic polynomials. Since $2\cos\frac{k\pi}{n}$ is a sum of two roots of unity $e^{ik\pi/n}$ and $e^{-ik\pi/n}$ one can conclude that properties of minimal polynomials for double cosines depend on properties of cyclotomic polynomials.

Definition 14. *A cyclotomic polynomial $\Phi_n(x)$ is the polynomial with integer coefficients, irreducible over $\mathbb{Q}$, defined as*

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi k/n} \right), \tag{37}$$

and satisfying the identity $1 - x^n = \prod_{d|n} \Phi_d(x)$. $\Phi_n(x)$ is the minimal polynomial of an n-th root of identity.

The basic facts concerning minimal polynomials for double cosines are the following:

Lemma 15. *[5, 25] The minimal polynomial for $2\cos\frac{\pi}{n}$ is a polynomial defined as*

$$\eta_n(x) = 2^{\deg\psi_{2n}(x)}\psi_{2n}\left(\frac{x}{2}\right). \tag{38}$$

Using fact 9 one can write it explicitly as:

$$\eta_1(x) = x + 2, \tag{39}$$

$$\eta_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,2n)=1}} \left(x - 2\cos\frac{k\pi}{n} \right), \quad n \leq 2 \tag{40}$$

Proof. Note that for arbitrary $1 \leq k \leq n$, s.t. $\gcd(k, 2n) = 1$, $\cos\frac{k\pi}{n}$ is a root of the polynomial $\psi_{2n}(x)$ of a degree $d = \deg\psi_{2n}(x) = \frac{\varphi(2n)}{2}$ with the coefficients $c_0, \ldots, c_{d-1}, c_d$. Since $2\cos\frac{\pi}{n}$ is a product of 2 and a root of $\cos\frac{k\pi}{n}$, the

companion matrix $M_{2\cos\frac{k\pi}{n}}$ is given by $M_{2\cos\frac{k\pi}{n}} = 2 \cdot M_{\cos\frac{k\pi}{n}}$ (10) and by fact 4 the minimal polynomial $\eta_n(x)$ is equal to the characteristic polynomial $\chi_{M_{2\cos\frac{k\pi}{n}}}$. Let us write this matrix explicitly. The polynomial $\eta_n(x)$ is given by

$$\eta_n(x) = \chi_{M_{2\cos\frac{k\pi}{n}}} = \det \begin{pmatrix} -x & 0 & \ldots & & -2c_0 \\ 2 & -x & \ldots & & -2c_1 \\ 0 & 2 & \ldots & & -2c_2 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & \ldots & 2 & & -2c_{d-1} - x \end{pmatrix}. \tag{41}$$

The substitution $x \to 2y$ transforms (41) to the form $\eta_n(2y) = \chi_{2M_{\cos\frac{k\pi}{n}}}$. Since $M_{\cos\frac{k\pi}{n}}$ is a $d \times d$ matrix we arrive at

$$\eta_n(2y) = \det 2(M_{\cos\frac{k\pi}{n}} - yI) = 2^d \psi_{2n}(y) = 2^d \psi_{2n}\left(\frac{x}{2}\right), \tag{42}$$

which is exactly (38). The proof is complete $\qquad\square$

Another property of $\eta_n(x)$ that is crucial for the proof of theorem 1 is proven in the following.

Lemma 16. *All the coefficients of $\eta_n(x)$ are integers.*

Proof. In order to prove this fact we use lemma 6 and properties of cyclotomic polynomials. First, note that $2\cos\frac{k\pi}{n} = 2\cos\frac{2k\pi}{2n}$, $\gcd(k, 2n) = 1$ can be written as a sum $e^{ik\pi/n} + e^{-ik\pi/n}$, where both $e^{ik\pi/n}$ and $e^{-ik\pi/n}$ are roots of the cyclotomic polynomial $\Psi_{2n}(x)$, whose companion matrix will be denoted by $M_{\Psi_{2n}(x)}$. Since $\Psi_{2n}(x)$ is a polynomial with integer coefficients, $M_{\Psi_{2n}(x)}$ has only integer entries.

Recall that using (10) $2\cos\frac{\pi}{n}$ is a root of the characteristic polynomial of the matrix defined as

$$M = M_{\Psi_{2n}(x)} \otimes I + I \otimes M_{\Psi_{2n}(x)}, \tag{43}$$

and χ_M belongs obviously to $\mathbb{Z}[x]$. The degree of the minimal polynomial of $2\cos\frac{\pi}{n}$ is smaller than the degree of $\chi_{M_{2\cos\frac{\pi}{n}}}$ as $\mathbb{Q}(2\cos\frac{k\pi}{n}) \subset \mathbb{Q}(e^{ik\pi/n})$. This means, the characteristic polynomial of M can be factorized as a product of at least two polynomials

$$\chi_M = \eta_n(x) \cdot p(x), \text{ where in general } p(x), \eta_n(x) \in \mathbb{Q}[x].$$

Since χ_M belongs to $\mathbb{Z}[x]$, by lemma 6 the polynomials $\eta_n(x)$ and $p(x)$ have integer coefficients. As χ_M is monic, $p(x)$ and $\eta_n(x)$ are also monic and the result follows. $\qquad\square$

5   The proof of theorem 1

The aim of this section is to decide, using the tools presented in previous sections, for which $\phi = \frac{2k\pi}{n}$ the left hand side of the equation

$$2\cos\frac{\gamma}{2} = \cos\phi + 1, \tag{44}$$

is a root of the minimal polynomial $\eta_m(x)$ for some $m \in \mathbb{N}$.

The minimal polynomial $m_{\cos\phi+1}(x)$ can be found using the companion matrix formalism explained in section 3.1. It follows that $\cos\phi + 1$ is a root of the characteristic polynomial of the matrix $M_{\cos\phi+1} = M_{\cos\phi} + I$, where

$$M_{\cos\phi} = \begin{pmatrix} 0 & 0 & \ldots & -c_0 \\ 1 & 0 & \ldots & -c_1 \\ 0 & 1 & \ldots & -c_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & -c_{d-1} \end{pmatrix},$$

Note that the field extensions $\mathbb{Q}(2\cos\frac{\gamma}{2}) = \mathbb{Q}(\cos\phi+1)$ and $\mathbb{Q}(\cos\phi)$ are of the same algebraic degree (see fact 4), therefore the characteristic polynomial of $M_{\cos\phi+1}$ is exactly the minimal polynomial $m_{2\cos\frac{\gamma}{2}}(x)$. One can compute $\chi_{M_{\cos\phi+1}}$ as the determinant of the following matrix:

$$
M_{\cos\phi+1} - Ix = \begin{pmatrix}
1-x & 0 & 0 & \dots & 0 & -c_0 \\
1 & 1-x & 0 & \dots & 0 & -c_1 \\
0 & 1 & 1-x & \dots & 0 & -c_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \dots & 1 & 1-x & -c_{d-2} \\
0 & 0 & \dots & 0 & 1 & 1-c_{d-1}-x
\end{pmatrix}.
\tag{45}
$$

Expansion with respect to the first row gives us to the following expression:

$$
m_{2\cos\frac{\gamma}{2}}(x) = \chi_{M_{\cos\phi+1}}(x) = \det(M_{\cos\phi+1} - Ix) = \sum_{i=0}^{d} \omega_i \cdot x^i =
\tag{46}
$$

$$
= -\left[\sum_{i=0}^{d-3} c_i(-1)^{d+i+1}(1-x)^i\right] + (1-x)^{d-2}[x^2 + x(c_{d-1}-2) + c_{d-2} - c_{d-1} + 1].
\tag{47}
$$

One can simplify (47) using the binomial formula. As a result we obtain the following relations between the coefficients of $\psi_n(x)$ and $\chi_{M_{\cos\phi+1}}$:

$$
\begin{aligned}
\omega_0 &= \sum_{i=0}^{d-3} c_i(-1)^{d+i} + (c_{d-2} - c_{d-1} + 1)(-1)^d, \\
\omega_1 &= \sum_{i=1}^{d-3} c_i(-1)^{d+1+i} + \binom{d-2}{0}(c_{d-1}-2) - \binom{d-2}{1}(c_{d-2} - c_{d-1} + 1), \\
\omega_2 &= \sum_{i=2}^{d-3} c_i(-1)^{d+i+2}\binom{i}{2} + \binom{d-2}{0} - \binom{d-2}{1}(c_{d-2}+1) + \binom{d-2}{2}(c_{d-2} - c_{d-1} + 1), \\
&\quad\vdots \\
\omega_k &= \sum_{i=k}^{d-3} c_i(-1)^{d+i+k}\binom{i}{k} + \binom{d-2}{k}(-1)^k(c_{d-2} - c_{d-1} + 1) + \binom{i}{k-1}(-1)^{k-1}(c_{d-1}-2) + \binom{d-2}{k-2}(-1)^{k-2} \\
&\quad\vdots \\
\omega_{d-3} &= -c_{d-3} + (c-2)(-1)^{d-3}(c_{d-2} - c_{d-1} + 1) + \binom{d-2}{d-4}(-1)^{d-4}(c_{d-1}-2) + (-1)^{d-5}\binom{d-2}{d-5}, \\
\omega_{d-2} &= (-1)^{d-2}(c_{d-2} - c_{d-1} + 1) + (d-2)(-1)^{d-3}(c_{d-1}-2) + (-1)^{d-4}\binom{d-2}{d-4}, \\
\omega_{d-1} &= (-1)^d(c_{d-1}-2) + (d-2)(-1)^{d-1}, \\
\omega_d &= (-1)^d.
\end{aligned}
\tag{48}
$$

Recall that by lemma 15 the coefficients of $m_{2\cos\frac{\gamma}{2}}(x)$ must be all integers if γ is a rational multiple of π. One has to check if this condition is satisfied by all ω_i's starting from ω_{d-1}. For this coefficient we have:

$$
(-1)^{d-2}(c_{d-1}-2) + (d-2)(-1)^{d-3} \in \mathbb{N} \Rightarrow c_{d-1} \in \mathbb{N}.
$$

Note that $\omega_{d-1} \notin \mathbb{N}$ if and only if $c_{d-1} \notin \mathbb{N}$. In this case we are done, however there are polynomials $\psi_n(x)$ for which $c_{d-1} \in \mathbb{N}$. In this case we consider the equation for ω_{d-2}:

$$
\omega_{d-2} = (-1)^{d-2}(c_{d-2} - c_{d-1} + 1) + (d-2)(-1)^{d-3}(c_{d-1}-2) + (-1)^{d-4}\binom{d-2}{d-4} \in \mathbb{N} \Rightarrow c_{d-2} \in \mathbb{N}.
$$

Assuming that $c_{d-1} \in \mathbb{Z}$, the coefficient ω_{d-2} is non-integer only if $c_{d-2} \notin \mathbb{Z}$. One can use the same reasoning for the other ω_i's step by step and notice from (48) that each ω_i depends on the coefficients $c_{d-1}, \dots, c_{i+1}, c_i$, where c_i is multiplied by the factor $(-1)^{d+2i}\binom{i}{i} = \pm 1$. If all of the coefficients $c_{d-1}, \dots, c_{i+1}, c_i$ are integers, then also ω_i belongs to $\mathbb{Z}$. Hence all $\omega_1, \dots, \omega_d$ are integers if and only if $c_1, c_2, \dots, c_{d-1}, c_d \in \mathbb{Z}$. On the other hand we have shown in lemma 13 that $\psi_n(x)$ has always at least one non-integer coefficient if $n \notin \{1, 2, 4\}$. Therefore at least one ω_i does not belong to $\mathbb{Z}$ and $m_{2\cos\frac{\gamma}{2}}$ cannot be the minimal polynomial $\eta_m(x)$ for any $m \in \mathbb{Z}$. This means, γ must be an irrational multiple of π.

Finally we consider what happens in the exceptional cases when $\phi = \{\frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi\}$, i.e. when $n \in \{1, 2, 4\}$.

1. Let $\phi = \pm\frac{\pi}{2}$. The corresponding minimal polynomial and its companion matrix are of the form $\psi_4(x) = x$ and $M_{\cos\frac{\pi}{2}} = 0$. Thus $M_{\cos\phi+1} = 1$ and its minimal polynomial is $m_{M_{\cos\phi+1}}(x) = x - 1$. We have that $x - 1 = \eta_3(x)$, thus $\gamma = \frac{k\pi}{3}$.

10

2. Let $\phi = 2\pi$, then $\psi_1(x) = x - 1$, $M_{\cos 2\pi} = 1$. The companion matrix for $M_{\cos \phi + 1}$ is a 1×1 matrix equal to $M_{\cos \phi + 1} = 1 + 1 = 2$. Thus $m_{M_{\cos \phi + 1}}(x) = x - 2$. This polynomial corresponds to $\gamma = 2\pi$.

3. Assume $\phi = \pi$, then $\psi_2(x) = x + 1$, $M_{\cos \pi} = -1$ and $M_{\cos \phi + 1} = 1 - 1 = 0$. Thus the minimal polynomial of $m_{\cos \phi + 1}(x) = x = \eta_2(x)$ which is the minimal polynomial of $2 \cos \gamma / 2$ for $\gamma = \pi$.

6 More examples

Assume now that we have two finite order $SU(2)$-gates. They can be written as $U(\phi_1, \vec{k}_1)$ and $U_2(\phi_2, \vec{k}_2)$ where

$$U(\phi, \vec{k}) = \cos \phi I + \sin \phi (k_x X + k_y Y + k_z Z), \; \vec{k} = [k_x, k_y, k_z], \; k_x^2 + k_y^2 + k_z^2 = 1, \tag{49}$$

and both ϕ_1 and ϕ_2 are rational multiples of π. Their product is $U(\gamma, \vec{k}_\gamma) = U(\phi_1, \vec{k}_1) U_2(\phi_2, \vec{k}_2)$, where

$$\cos \gamma = \cos \phi_1 \cos \phi_2 + \sin \phi_1 \sin \phi_2 \vec{k}_1 \cdot \vec{k}_2. \tag{50}$$

Under our assumptions $\cos \phi_1$, $\cos \phi_2$ and $\sin \phi_1$, $\sin \phi_2$ are algebraic numbers. It is well known that the sum and the product of an algebraic number and a transcendental number is transcendental. Moreover, if $\cos \phi$ is transcendental then ϕ is an irrational multiple of π. Thus if $\cos \theta = \vec{k}_1 \cdot \vec{k}_2$ is transcendental then $U(\gamma, \vec{k}_\gamma)$ is of infinite order. In the following we show that it can also happen when $\cos \theta$ is an algebraic number.

6.1 Gates H and $T(\phi)$

Let us consider a popular in quantum computation set of unitary gates $\mathcal{S} = \{H, T(\phi)\}$, where $H = U(\frac{\pi}{2}, \frac{1}{\sqrt{2}}(\vec{k}_z + \vec{k}_y))$ is the Hadamard gate, and $T(\phi) = U(\phi, \vec{k}_z)$ is a phase gate. Explicit matrices are given by:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \; T(\phi) = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}. \tag{51}$$

We look for angles ϕ for which the product HT_ϕ is of infinite order. An example value of such ϕ, $\phi = \frac{\pi}{8}$, was given in [2]. A more general answer can be found using the method presented in previous sections. The matrices H and $T(\phi)$ represented as rotation matrices from $SO(3)$ are of the form

$$\text{Ad}_H = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \; \text{Ad}_{T(\phi)} = \begin{pmatrix} \cos 2\phi & \sin 2\phi & 0 \\ -\sin 2\phi & \cos 2\phi & 0 \\ 0 & 0 & 1. \end{pmatrix} \tag{52}$$

The product of Ad_H and $\text{Ad}_{T(\phi)}$ is a rotation by angle γ given by

$$\text{tr} \text{Ad}_H \text{Ad}_{T(\phi)} = \text{tr} O(\gamma, \vec{k}),$$
$$-\cos 2\phi = 2 \cos \gamma + 1 \Rightarrow -2 \cos \gamma = \cos 2\phi + 1,$$

but from trigonometric identities we have that $-\cos \gamma = \cos(\gamma + \pi)$ thus we can write

$$2 \cos \gamma' = \cos 2\phi + 1, \; \gamma' = \gamma + \pi. \tag{53}$$

Note that equation (53) is of the same form as (44), thus by theorem 2 we can say immediately that $\text{Ad}_H \cdot \text{Ad}_{T(\phi)}$ is of infinite order if and only if

$$2\phi \neq \{0, \pi, \pm \frac{\pi}{2}\}. \tag{54}$$

Hence the gate $HT(\phi)$ is of infinite order if and only if

$$\phi \neq \{0, \pi, \pm \frac{\pi}{2}, \frac{\pi}{4}, \frac{3\pi}{4}\}. \tag{55}$$

7 Acknowledgment

References

[1] S. Axler (2015) *Linear algebra done right* (Undergraduate Texts in Mathematics, Springer, 2015).

[2] P. O. Boykin *et. al.*, *On Universal and Fault-Tolerant Quantum Computing*, arXiv:quant-ph/9906054 (1999).

[3] A. Baker, *Transcendental Number Theory* (Cambridge University Press, 1975).

[4] A. Barenco *et al.*, *Elementary gates for quantum computation*, Phys. Rev. **A** 52 (1995), 3457-3467.

[5] A. Bayad, I. N. Cangul, *The minimal polynomial of* $2\cos(p/q)$ *and Dickson polynomials*, Appl. Math. Comp. 218 (2013), 7014-7022.

[6] A. Bouland, S. Aronson, *Generation of Universal Linear Optics by Any Beamsplitter*, Phys. Rev. **A** 89, 062316 (2014).

[7] A. M. Childs *et al.*, *Characterization of universal two-qubit Hamiltonians*, Quantum Info. Comput. 11 (2011), 19-39.

[8] W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras* (Interscience Publishers, John Wiley and sons, 1962).

[9] A. W. Harrow, B. Recht, and I. L. Chuang, *Efficient discrete approximations of quantum gates*, J. Math. Phys. 43:9 (2002), 4445-4451.

[10] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[11] H. M. Edwards, *Galois theory* (Graduate Texts in Mathematics, Springer, 1998).

[12] M. Field, *Generating Sets for compact semisimple Lie Groups*, Proc. Amer. Math. Soc. 127 (1999), 3361-3365.

[13] G. H. Hardy, E. M. Wright, *An introduction to the Theory of Numbers* (Oxford at the Clarendon Press, 1960).

[14] V. Kliuchnikov et. al., *A Framework for Approximating Qubit Unitaries*, arXiv:1510.03888 (2015).

[15] M. Kuranishi, *Two elements generations on semi-simple Lie groups*, Kodai Math. Sem. Rep. 1 (1949), 5-6.

[16] M. Oszmaniec, J. A. Gutt, M. Kuś, *Classical simulation of fermionic linear optics augmented with noisy ancillas* Phys. Rev. **A** 90, 020302 (2014).

[17] A. Politi *et al.*, *Silica-on-Silicon Waveguide Quantum Circuits*, Science 320 (2008), 646-649.

[18] M. Reck *et al.*, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. 73 (1994), 58-61.

[19] A. Sawicki, *Universality of beamsplitters*, Quantum Info. Comput. 16, 3&4 (2016), 0291-0312.

[20] A. Sawicki, K. Karnas, *Universality of single qudit gates*, arXiv:1609.05780 (2016).

[21] A. Sawicki, K. Karnas *Criteria for universality of quantum gates*, arXiv:1610.00547 (2016).

[22] W. Waitkins, J. Zeitlin, *The Minimal Polynomial of* $\cos(2\pi/n)$, The American Mathematical Monthly 100, 5 (1993), 471-474.

[23] Z. Zimborás *et al.*, *Symmetry criteria for quantum simulability of effective interactions*, Phys. Rev. **A** 92, 042309 (2015).

[24] http://oeis.org/A181875.

[25] https://oeis.org/A187360.