Quantum Information and Computation, Vol. 16, No. 3&4 (2016) 0291–0312

UNIVERSALITY OF BEAMSPLITTERS

ADAM SAWICKI
Center for Theoretical Physics, Massachusetts Institute of Technology
77 Massachusetts Ave, Cambridge, MA 02139, USA

School of Mathematics, University of Bristol, University Walk
Bristol BS8 1TW, UK

Center for Theoretical Physics, Polish Academy of Sciences
Al. Lotników 32/46, 02-668 Warszawa, Poland

Received August 9, 2015
Revised December 16, 2015

We consider the problem of building an arbitrary $N \times N$ real orthogonal operator using a finite set, S, of elementary quantum optics gates operating on $m \leq N$ modes - the problem of universality of S on N modes. In particular, we focus on the universality problem of an m-mode beamsplitter. Using methods of control theory and some properties of rotations in three dimensions, we prove that any nontrivial real 2-mode and 'almost' any nontrivial real 3-mode beamsplitter is universal on $m \geq 3$ modes.

Keywords: linear optics, beamsplitters, universality, orthogonal group, control theory, Lie algebras
Communicated by: R Cleve & J Eisert

1 Introduction

Around twenty years ago Reck *et al.* [16] considered the problem of building an arbitrary $N \times N$ unitary operator using the set of elementary quantum optics gates. They gave a recursive algorithm which transforms an $N \times N$ unitary matrix into an arrangement of 2-mode beamsplitters, phase shifters, and mirrors. If one wants to implement any $N \times N$ unitary, however, then one needs to have access to all possible beamsplitters and phase shifters. This makes the results of [16] not particularly useful in a real experimental setting. Recently, Bouland and Aaronson [1] considered the same problem albeit with a finite set of optical gates available. They showed that actually any single 2-mode beamsplitter that nontrivially acts on two modes densely generates unitary transformations $U(3)$ (or orthogonal transformations $O(3)$, in the real case). Combining their result with the arguments from [16] they concluded that any nontrivial 2-mode beamsplitter densely generates $U(m)$ for $m \geq 3$ modes. For example, a real 2-mode beamsplitter is given by one rotation angle $\theta \in [0, 2\pi]$. Having such a beamsplitter we let it operate on pairs of three available modes. This way we get operators which effectively mix 3 modes. The resulting operators are dense in $O(3)$. As a direct consequence, for building orthogonal (unitary) transformation one does not need tunable beamsplitters - those whose θ can be changed. In fact any 2-mode beamsplitter with a fixed $\theta \notin \{0, \pi/2, \pi, 3\pi/2\}$ is universal for generation of quantum linear optics. They left the problem of classifying optical gates that act on three or more modes open. This kind of gates

can be easily built experimentally using coupled optical waveguides [12, 2]. We also note that there are some interesting developments in models of fermionic linear optics [13, 18]. In this paper we address the open problem given in [1] using methods that are orthogonal to those used in [1]. In a generic case, our approach can be used to obtain the desired classification for any number of modes which is impossible using representation theory arguments of [1]. We also give another proof of a 2-mode real beamsplitter universality which is entirely based on our method and does not make any use of the results of [16, 1].

Mathematically, a real m-mode beamsplitter is represented by an orthogonal $m \times m$ matrix. Throughout this paper we will follow convention of Nielsen and Chuang [10] and assume that this matrix has a determinant equal to one (some authors use a convention with -1 [1]). Under this assumption the set of m-mode beamsplitters forms the group $SO(m)$.

We say that a finite set of beamsplitters $S \subset SO(m)$ is universal on m modes if and only if it generates $SO(m)$, i.e. any m-mode beamsplitter can be approximated by a sequence of elements form S (or their inverses) with an arbitrary precision. This definition is analogous to the one for quantum gate universality. For example the famous set consisting of H and T gates is universal for one qubit as it generates any operation from $SU(2)$ with an arbitrary precision [11]. In this paper we consider the problem of m-mode universality when the set S is constructed (in some natural way which we explain in the subsequent sections) from a single 2- or 3-mode beamsplitter and show that:

1. Any nontrivial 2-mode beamsplitter is universal on $m \geq 3$ modes.

2. Almost any nontrivial 3-mode beamsplitter is universal on $m \geq 3$ modes.

We also make several interesting statements for m-mode beamsplitters for an arbitrary m. They concern universality on $k > m$ provided universality on m modes. The method we use to obtain the result is a combination of the fundamental theorem of control theory (see Theorem 1) and some algebraic properties of the rotation group in three dimensions. Recently, Bouland and Aaronson [1] gave a proof of universality of a 2-mode beamsplitter (also for the case when $SO(2)$ is replaced by $SU(2)$). Their approach is based on representation theory and classification of subgroups of $SU(3)$. As the authors of [1] point out, such classification is missing starting from $SU(5)$ and therefore their approach has clear limitations. The method presented in this paper is complementary to [1] and attacks the problem from a different direction. It divides the problem into two. For $O_m \in SO(m)$ with the spectrum $\sigma(O_m) = \left\{e^{i\phi_1}, e^{-i\phi_1}, \ldots, e^{i\phi_{m/2}}, e^{-i\phi_{m/2}}\right\}$, where each ϕ_i is an irrational multiple of π it boils down to proving that some particular elements generate the special orthogonal Lie algebra. This can be fully handled. For O_m with at least one $\phi_i = a\pi$, where $a \in \mathbb{Q}$ the subtle techniques to show that the product of two group elements that have finite order can have infinite order are required. We discuss this by considering an example with two rotations about the x and z axes by rational angle θ whose $\cos(\theta)$ is algebraic of degree 2 in Section 3.1. The techniques used in this section are based on cyclotomic polynomials and they were used in the similar context in [11]. They, however, do not generalise easily for an arbitrary rational angle. Therefore in the general case we use the recent results of Conway, Radin and Sadun concerning products of rotations [3, 4, 14, 15].

Our method reveals the importance of mode permutations for m-mode beamsplitters, $m \geq 3$. The central role is played by the set $S(O_m) = \{P_\sigma^t O_m P_\sigma : \sigma \in S_m\}$ where P_σ are

$m \times m$ matrices that permute modes of the considered beamsplitter. In particular we show that in a great number of cases universality of an m-mode beamsplitter O_m on $k \geq m$ modes reduces to showing that the set $S(O_m)$ is universal on m-modes (rather than on $m+1$ modes). Moreover, we show that already on 3-modes there is a beamsplitter that is not universal on 3 and 4 modes. It corresponds to what we call the trivial action of permutation group, that is, to $S(O_3) = \left\{O_3, O_3^{-1}\right\}$.

The paper is organized as follows. In Section 2 we discuss general aspects of the method we use in this paper. Next, in Section 3 we prove universality of a nontrivial 2-mode beamsplitter on $m \geq 3$ modes. The proof is divided into two parts. The first one is an elegant Lie-algebra calculation. The second is showing that the product of two finite order orthogonal rotations is a rotation by an angle which is an irrational multiple of π. In the subsequent section we discuss some aspects of beamsplitters operating on higher number of modes, introduce $S(O_m)$ and prove general results concerning $S(O_m)$. Finally in Section 5 the 3-mode beamsplitters are discussed in details.

2 The method

In this section we sketch the method we will use throughout the paper.

Let G be a connected Lie group and $\mathfrak{g}$ its Lie algebra. We say that elements $\{g_1, \ldots, g_k\} \subset G$ generate G, if and only if the set

$$< g_1, \ldots, g_k >:= \{g_{a_1}^{k_1} \cdot g_{a_2}^{k_2} \cdots g_{a_n}^{k_n} : a_i \in \{1, \ldots, k\}, k_i \in \mathbb{Z}, n \in \mathbb{N}\},$$

is dense in G that is $G = \overline{< g_{1,}, \ldots, g_k >}$. Similarly we say that subgroups $\{H_1, \ldots, H_k\}$ of G generate G iff the set

$$< H_1, \ldots, H_k >:= \{g_{a_1}^{k_1} \cdot g_{a_2}^{k_2} \cdots g_{a_n}^{k_n} : a_i \in \{1, \ldots, k\}, g_{a_i} \in H_{a_i}, k_i \in \mathbb{Z}, n \in \mathbb{N}\},$$

is dense in G. Finally, let $S = \{X_1, \ldots, X_k\} \subset \mathfrak{g}$ be a subset of Lie algebra $\mathfrak{g}$. We say that S generates $\mathfrak{g}$ iff any element X of $\mathfrak{g}$ can be expressed as a linear combination of X_i's and arbitrarily nested commutators of X_i's:

$$X = \sum_j \alpha_i X_i + \sum_{i,j} \alpha_{ij} [X_i, X_j] + \sum_{i,j,k} \alpha_{ijk} [X_i, [X_j, X_k]] + \ldots$$

The following theorem [8] will be of the great importance in this paper.

Theorem 1. *Let G be a connected Lie group and $\mathfrak{g}$ its Lie algebra. G is generated by one-parameter subgroups $\{e^{tX} : t \in \mathbb{R}\}$, $X \in S$ where S is a finite subset of $\mathfrak{g}$ if and only if S generates $\mathfrak{g}$ as a Lie algebra.*

The problem which we are going to deal with is the following one:

Problem 1. *Let $A = \{a_1, \ldots, a_k\} \subset G$ be a finite subset of G. We want to show that A generates G, that is, the group generated by A is dense in G.*

We make use of Theorem 1 to solve Problem 1. To this end we note that one can always write

$$a_i = e^{X_i}, X_i \in \mathfrak{g}.$$

We consider two cases:

1. Assume that for all $i \in \{1, \ldots, k\}$ we have that $< a_i >$ is dense in $\{e^{tX_i} : t \in \mathbb{R}\}$, i.e. $\overline{< a_i >} = \{e^{tX_i} : t \in \mathbb{R}\}$. Under this assumption, by Theorem 1 we get that A generates G if and only if $\{X_1, \ldots, X_k\}$ generates $\mathfrak{g}$.

2. Assume that for some a_i the group $< a_i >$ is not dense in $\{e^{tX_i} : t \in \mathbb{R}\}$ but $\{X_1, \ldots, X_k\}$ generate $\mathfrak{g}$. In this case we cannot directly apply Theorem 1. What we can do however is to replace a_i by some element $b_i = e^{Y_i}$ that belong to $< A >$ and is such that $< b_i >$ is dense in $\{e^{tY_i} : t \in \mathbb{R}\}$ and $\{X_1, \ldots, Y_i, \ldots, X_k\}$ generate $\mathfrak{g}$. If this kind of manipulation can be done for each "bad" $a_i \in A$ then the problem is solved by means of Theorem 1.

In the following we will show that this is the case for beamsplitters.

3 Universality of a real 2-mode beamsplitter

A 2-mode beamsplitter is given by a matrix $g_\theta \in SO(2)$ of the form

$$g_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix},$$

where $\theta \in [0,\, 2\pi[$. Let us first look at the spectrum of g_θ. The characteristic equation reads:

$$\lambda^2 - 2\lambda\cos(\theta) + 1 = 0.$$

And therefore spectrum is given by $\{e^{i\theta},\, e^{-i\theta}\}$. We want to show that three matrices:

$$O_{1,2} = \begin{pmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix},\ O_{1,3} = \begin{pmatrix} \cos(\theta) & 0 & \sin(\theta) \\ 0 & 1 & 0 \\ -\sin(\theta) & 0 & \cos(\theta) \end{pmatrix}, \qquad (1)$$
$$O_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & \sin(\theta) \\ 0 & -\sin(\theta) & \cos(\theta) \end{pmatrix},$$

for a given and fixed $\theta \in [0, 2\pi[\backslash\{0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi\}$ generate $SO(3)$.[a] Following the reasoning explained in Section 2 we note that $O_{i,j} = e^{X_{i,j}}$, where

$$X_{1,2} = \begin{pmatrix} 0 & \theta & 0 \\ -\theta & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ X_{1,3} = \begin{pmatrix} 0 & 0 & \theta \\ 0 & 0 & 0 \\ -\theta & 0 & 0 \end{pmatrix},\ X_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \theta \\ 0 & -\theta & 0 \end{pmatrix}.$$

It is obvious that $\{X_{1,2},\, X_{1,3}, X_{2,3}\}$ generate Lie algebra $\mathfrak{so}(3)$ iff $\theta \neq 0$, as matrices

$$E_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ E_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix},\ E_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

form a standard basis of $\mathfrak{so}(3)$. We also note that for $\theta = a\pi$ where a is irrational we have that $< O_{ij} >$ is dense in $\{e^{tX_{ij}} : t \in \mathbb{R}\}$. Therefore using Theorem 1 we have that

[a] The excluded angles correspond to either permutation of modes or $\pm$ identity operation.

$\{O_{1,2}, O_{1,3}, O_{2,3}\}$ generate $SO(3)$ for $\theta = a\pi$ with irrational a. We still need to examine the case when $a \in \mathbb{Q}$ that is the case when for all three groups $\overline{< O_{i,j} >} \neq \{e^{tX_{i,j}} : t \in \mathbb{R}\}$. To this end we choose three new matrices that belong to $< O_{1,2}, O_{1,3}, O_{2,3} >$, i.e.:

$$O_{1,2}O_{1,3},\ O_{1,2}O_{2,3},\ O_{1,3}O_{2,3}.$$

Our goal is to show:

Statement 1. The Lie algebra elements corresponding to $\{O_{1,2}O_{1,3}, O_{1,2}O_{2,3}, O_{1,3}O_{2,3}\}$ form a basis of $\mathfrak{so}(3)$.

Statement 2. The elements $\{O_{1,2}O_{1,3}, O_{1,2}O_{2,3}, O_{1,3}O_{2,3}\}$ are rotations by angles that are not rational multiples of π, or equivalently there is no power $k \in \mathbb{N}$ for which they become identity matrix.

The proofs of these two statements are given in the next three subsections.

3.1 Finite and infinite order elements - examples.

In this section we consider examples showing that the product of two orthogonal rotations by an angle θ which is a rational multiple of π can be a rotation by an angle α which is not a rational multiple of π. In particular we show that this is the case for all θ's whose $\cos(\theta)$ is algebraic of degree two. Our approach makes a heavy use of cyclotomic polynomials as they are useful in showing that for a complex number $e^{i\alpha}$ its argument α in not a rational multiple of π. These techniques were also used in [11] to show that gates H and T generate $SU(2)$, where the product of two specific rotation was considered. Here we provide much more general discussion which reveals the natural limitations of this method. The main purpose of this section is to provide some hands on examples and explicit calculations. For an arbitrary θ we will use a different approach (see section 3.3).

3.1.1 Cyclotomic ploynomials

The method we use is based on some properties of cyclotomic polynomials and therefore we start with their discussion (see [5] for more details).

Definition 1. *The n-th cyclotomic polynomial for $n \in \mathbb{N}$ is given by*

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

where $\gcd(k, n)$ *is the greatest common divisor of n and k.*

Cyclotomic polynomials have several useful properties. In the following we will use three of them: (1) cyclotomic polynomials are monic and irreducible over $\mathbb{Q}$, (2) Coefficients of cyclotomic polynomials are integers, (3) For any $q \in \mathbb{N}$ we have

$$x^q - 1 = \prod_{d|q} \Phi_d(x). \tag{2}$$

The first property is actually a nontrivial result due to Gauss (it can be however easily proved for prime n using Eisenstein criterion for irreducibility) [5]. The second one is a direct result

of

$$x^q - 1 = \prod_{1 \le k \le q} \left(x - e^{2i\pi \frac{k}{q}} \right),$$

and the definition of a cyclotomic polynomial. For $\alpha \in \mathbb{C}$ we say that the monic irreducible polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial for α over $\mathbb{Q}$ iff $m_\alpha(\alpha) = 0$. If $\alpha \in \mathbb{C}$ has a minimal polynomial over $\mathbb{Q}$ then we call it algebraic. Otherwise it is transcendental. The algebraic degree of α is a degree of its minimal polynomial. Now we can state the main theorem (cf. lemma 3.4 of [17]):

Theorem 2. *The following two are equivalent: (1) $a \in \mathbb{Q}$, (2) the minimal polynomial for $\alpha = e^{i2\pi a}$ over $\mathbb{Q}$ exists and is cyclotomic.*

Proof. If $a = p/q$ then $(e^{i2\pi a})^q = 1$ and therefore the minimal polynomial $m_\alpha(x)$ exists as α satisfies $x^q - 1 = 0$. By (2) we know that α is a root of some $\Phi_d(x)$ where $d|q$. But $\Phi_d(x)$ is irreducible and monic hence it is the minimal polynomial for α over $\mathbb{Q}$. Conversely, assume m_α exists and is cyclotomic. Then we have

$$0 = m_\alpha(\alpha) = \Phi_n(\alpha) = \Pi_{d|n} \Phi_d(\alpha) = \alpha^n - 1. \tag{3}$$

By (3) we get $e^{2i\pi cn} = 1$ and hence $c \in \mathbb{Q}$. □

3.1.2 Products of rotations

Theorem 2 can be used in particular for showing that for a given complex number $e^{i\alpha}$ the angle α is not a rational multiple of π. In this case it is enough to prove that either the minimal polynomial does not exist or it exists and is not cyclotomic. In the following we use it to study the composition of two rotations about orthogonal axes by an angle θ which is a rational multiple of π. Let $O_{1,2}$ and $O_{2,3}$ be as in (1). We have

$$\mathrm{tr} O_{1,2} O_{2,3} = 2\cos(\theta) + \cos^2(\theta).$$

From the other hand $O_{1,2}O_{2,3}$ is a rotation by an angle α and hence $\mathrm{tr} O_{1,2} O_{2,3} = 1 + 2\cos(\alpha)$. As a result we get the equation which relates θ and α:

$$2\cos(\alpha) = 2\cos(\theta) + \cos^2(\theta) - 1. \tag{4}$$

We first determine if $e^{i\alpha}$ is algebraic or transcendental.

Fact 1. *For α given by (4) $e^{i\alpha}$ is an algebraic number.*

Proof. As θ is a rational multiple of π, using De Moivre's formula we get that $\cos(\theta)$ is an algebraic number. Next, it is known [17], that the sum and product of two algebraic numbers is again algebraic number. Applying this to (4) we get that $\cos(\alpha)$ is an algebraic number. A complex number is algebraic iff its both real and imaginary parts are algebraic. To show that $\sin(\alpha)$ is algebraic note that the field extensions $\mathbb{Q}[\cos(\alpha)] : \mathbb{Q}$ and $\mathbb{Q}[\cos(\alpha), \sin(\alpha)] : \mathbb{Q}[\cos(\alpha)]$ are both algebraic and consequently by the chain rule $\mathbb{Q}[\sin(\alpha)] : \mathbb{Q}$ is algebraic. Hence $e^{i\alpha} = \cos\alpha + i\sin\alpha$ is algebraic. □

Note that by Fact 3.1.2 $e^{i\alpha}$ is never transcendental so in order to use Theorem 2 we need to determine its minimal polynomial. Putting $x = e^{i\alpha} = \cos(\alpha) + i\sqrt{1-\cos^2(\alpha)}$ we get

$$x^2 - 2\cos(\alpha)x + 1 = 0, \tag{5}$$

where $\cos(\alpha)$ is determined by $\cos(\theta)$.

Fact 2. *The algebraic degree of* $\cos(\alpha)$ *divides the algebraic degree of* $\cos(\theta)$ *and the algebraic degree of* $e^{i\alpha}$ *is twice the algebraic degree of* $\cos(\alpha)$.

Proof. It is easy to see that the field extensions satisfy $\mathbb{Q}[\cos(\alpha)] \subset \mathbb{Q}[\cos(\theta)]$. Using the chain rule for fields [17] we get

$$[\mathbb{Q}[\cos(\theta)] : \mathbb{Q}] = [\mathbb{Q}[\cos(\theta)] : \mathbb{Q}[\cos(\alpha)][\mathbb{Q}[\cos(\alpha)] : \mathbb{Q}] \tag{6}$$

As $[\mathbb{Q}[\cos(\theta)] : \mathbb{Q}]$ and $[\mathbb{Q}[\cos(\alpha)] : \mathbb{Q}]$ are algebraic degrees of $\cos(\theta)$ and $\cos(\alpha)$ respectively we get the conclusion. The relation between algebraic degrees $e^{i\alpha}$ and $\cos(\alpha)$ comes from equation (5). □

Note that $\cos(\theta)$ can have arbitrary large algebraic degree and therefore minimal polynomial for $e^{i\alpha}$ can have any order. In the following we consider example when degree of $\cos(\theta)$ is 2 which by Fact 2 means the algebraic degree of $e^{i\alpha}$ can be either 2 or 4. As by our assumption $\cos(\theta) = a + b\sqrt{C}$ we get $cos(\alpha) = A + B\sqrt{C}$, where A and B are given in terms of a, b, c. The minimal polynomial of $e^{i\alpha}$ is:

$$x^4 - 4Ax^3 + (4A^2 + 2)x^2 - 4Ax - 4B^2C + 1 = 0 \tag{7}$$

We next determine possible values of a and b. Using De Moivre's formula one can easily see that roots x_1 and x_2 with $|x_1| < 2$ and $|x_2| < 2$ of

$$x^2 + ax + b = 0, \tag{8}$$

where $a, b \in \mathbb{Z}$ are only possible values of $2\cos(\theta)$ of algebraic degree two. Direct calculation leads to: (1) $\cos(\theta) = \pm\frac{1}{\sqrt{2}}$, (2) $\cos(\theta) = \pm\frac{\sqrt{3}}{2}$, (3) $\cos(\theta) = \pm\frac{1}{4} \pm \frac{\sqrt{5}}{4}$. The corresponding angles are: $\cos(\pi/4) = 1/\sqrt{2}$, $\cos(\pi/3) = \sqrt{3}/2$, $\cos(\pi/5) = 1/4 + 1/4\sqrt{5}$, $\cos(2\pi/5) = -1/4 + 1/4\sqrt{5}$, $\cos(3\pi/5) = 1/4 - 1/4\sqrt{5}$, $\cos(4\pi/5) = -1/4 - 1/4\sqrt{5}$, $\cos(3\pi/4) = -1/\sqrt{2}$, $\cos(2\pi/3) = -\sqrt{3}/2$. One explicitly checks that in all case polynomial (7) is not cyclotomic. This way we showed that the product of two rotations about orthogonal axes by rational angle θ, whose $\cos\theta$ is algebraic of degree two, is a rotation by an angle which is an irrational multiple of π.

3.2 The proof of Statement 1

We will make use of a compact form of Baker-Campbell-Hausdorff (BCH) formula for the group $SO(3)$. For the detailed derivation see [6] (cf. [7]). Let us first recall the definition of the BCH formula for an arbitrary compact semisimple matrix Lie algebra $\mathfrak{g}$. For $X, Y \in \mathfrak{g}$ we define $\mathrm{BCH}(X, Y)$ in the following way:

$$e^{\mathrm{BCH}(X,Y)} = e^X e^Y.$$

It is known that $\mathrm{BCH}(X,Y)$ is given by an infinite sum. In the case of $\mathfrak{so}(3)$, however, there is a particularly nice compact formula for $\mathrm{BCH}(X,Y)$. This is due to the following two facts:

1. For $X \in \mathfrak{so}(3)$ the characteristic polynomial is given by $p(\lambda) = -\lambda^3 - ||X||^2\lambda$, where $||X||^2 = \frac{1}{2}\mathrm{tr}(X^tX)$. Therefore by the Cayley-Hamilton theorem $X^3 = -\theta^2 X$, where $\theta = ||X||$.

$$\begin{aligned} e^X = I + X + \frac{1}{2!}X^2 + \frac{1}{3!}X^3 + \ldots + \frac{1}{n!}X^n + \ldots = \\ = I + X\left(1 - \frac{\theta^2}{3!} + \frac{\theta^4}{5!} - \frac{\theta^6}{7!} + \ldots\right) + X^2\left(\frac{1}{2!} - \frac{\theta^2}{4!} + \frac{\theta^4}{6!} - \ldots\right) = \\ = I + \frac{\sin\theta}{\theta}X + 2\frac{\sin^2(\theta/2)}{\theta^2}X^2. \end{aligned} \tag{9}$$

2. Let $O = e^X$ be a rotation matrix from $SO(3)$ and let $Z = \frac{O-O^t}{2}$. Using formula (9) we see that $Z = \frac{\sin\theta}{\theta}X$. Therefore:

$$\log(O) := X = \frac{\sin^{-1}(||Z||)}{||Z||}Z. \tag{10}$$

Having these the BCH formula for $\mathfrak{so}(3)$ can be easily calculated. One simply writes down the expression for e^Xe^Y using (9) and then calculates the logarithm using (10). Details can be found in [6]. In the case where X and Y are orthogonal $\mathrm{tr}(X^tY) = 0$ the formula reads:

$$\mathrm{BCH}(X,Y) = \alpha X + \beta Y + \gamma[X,Y], \tag{11}$$

where

$$\begin{gathered} \alpha = \frac{\sin^{-1}(d)}{d}\frac{a}{\theta},\ \beta = \frac{\sin^{-1}(d)}{d}\frac{b}{\phi},\ \gamma = \frac{\sin^{-1}(d)}{d}\frac{c}{\theta\phi}, \\ a = \sin\theta\cos^2(\phi/2)\,,\ b = \sin\phi\cdot\cos^2(\theta/2)\,,\ c = \frac{1}{2}\sin\theta\sin\phi, \\ d = \sqrt{a^2+b^2+c^2},\ \theta = ||X||,\ \phi = ||Y||. \end{gathered} \tag{12}$$

We need to show that

$$\{\mathrm{BCH}(X_{1,2},X_{1,3}),\ \mathrm{BCH}(X_{1,2},X_{2,3}),\ \mathrm{BCH}(X_{1,3},X_{2,3})\}\,, \tag{13}$$

form a basis of $\mathfrak{so}(3)$. Using (11) and (12) we easily find:

$$\begin{aligned} \mathrm{BCH}(X_{1,2},X_{1,3}) &= \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\left(\cos^2\frac{\theta}{2}X_{1,2} + \cos^2\frac{\theta}{2}X_{1,3} - \frac{1}{2}\sin\theta X_{2,3}\right), \\ \mathrm{BCH}(X_{1,2},X_{2,3}) &= \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\left(\cos^2\frac{\theta}{2}X_{1,2} + \cos^2\frac{\theta}{2}X_{2,3} + \frac{1}{2}\sin\theta X_{1,3}\right), \\ \mathrm{BCH}(X_{1,3},X_{2,3}) &= \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\left(\cos^2\frac{\theta}{2}X_{1,3} + \cos^2\frac{\theta}{2}X_{2,3} - \frac{1}{2}\sin\theta X_{1,2}\right). \end{aligned} \tag{14}$$

where $d = \sin\theta\sqrt{2\cos^4(\theta/2) + 1/4\sin^2\theta}$. Next we write down matrices (14) in the standard basis of $\mathfrak{so}(3)$ and get the following change of basis matrix

$$M = \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\cdot A_{SO(3)} = \frac{\sin^{-1}(d)}{d}\sin\theta\begin{pmatrix} \cos^2\frac{\theta}{2} & \cos^2\frac{\theta}{2} & -\frac{1}{2}\sin\theta \\ \cos^2\frac{\theta}{2} & \frac{1}{2}\sin\theta & \cos^2\frac{\theta}{2} \\ -\frac{1}{2}\sin\theta & \cos^2\frac{\theta}{2} & \cos^2\frac{\theta}{2} \end{pmatrix}. \tag{15}$$

The determinant of (15) is given by:

$$\left(\frac{\sin^{-1}(d)}{d}\sin\theta\right)^3\left(-2\cos^6(\theta/2) + \frac{1}{2}\cos^4(\theta/2)\sin(\theta) + \frac{1}{8}\sin^3(\theta)\right) \tag{16}$$

To find its zeros of (16) one can for example write down all functions in terms of $t = \tan(\frac{\theta}{4})$ and solve the polynomial equations with respect to t.The relevant part of (16) reads:

$$-2\cos^6(\theta/2) + \frac{1}{2}\cos^4(\theta/2)\sin(\theta) + \frac{1}{8}\sin^3(\theta) = 0. \tag{17}$$

using $\sin\theta = 2\sin\frac{\theta}{2}\cos\frac{\theta}{2}$ one gets:

$$\cos^3(\theta/2)\left(-2\cos^3(\theta/2) + \cos^2(\theta/2)\sin(\theta/2) + \sin^3(\theta/2)\right) = 0\ . \tag{18}$$

The first factor of (18) gives $\theta = \pi$. Using $\cos\theta/2 = \frac{1-t^2}{1+t^2}$ and $\sin\theta/2 = \frac{2t}{1+t^2}$, for the second factor of (18) one gets polynomial equation that has only one positive real root $t = \sqrt{2}-1$ (the remaining roots are $t = -\sqrt{2}-1$ and four complex roots). That means $\theta = \pi/2$. Therefore the determinant (16) vanishes iff $\theta = 0$, $\theta = \pi$ or $\theta = \pi/2$. Hence (13) form a basis of $\mathfrak{so}(3)$ in all cases we are interested in.

Remark 1. *Using isomorphism $SO(3) = SU(2)/\mathbb{Z}_2$ one can also prove this result working with $SU(2)$ matrices.*

3.3 The proof of Statement 2

For the proof we use the following result of [14]:

Lemma 1. *Let A and B be rotations about orthogonal axes by $2\pi/p$ and $2\pi/q$ respectively. Consider the word:*

$$A^{a_1}B^{b_1}\cdots A^{a_n}B^{b_n},$$

where none of a_i's are multiple of $p/2$ and none of b_i's are multiple of $q/2$. If no two consecutive terms represent rotations by $\pi/2$ and if the word is nonempty, then the word is not equal to identity.

Corollary 1. *Let $O_1, O_2 \in SO(3)$ be rotations about orthogonal axes by $2\pi\frac{a}{p}$ and $2\pi\frac{b}{q}$, respectively, where $a < p$ and $b < q$ and fractions a/p and b/q are not equal $\{1, \frac{1}{2}, \frac{1}{4}, \frac{3}{4}\}$. Then for any $n \in \mathbb{N}$ we have $(O_1O_2)^n \neq I$. Thus the product of two finite order orthogonal rotations is a rotation by an angle which is not a rational multiple of π.*

Proof. Let A and B be orthogonal rotations by $\frac{2\pi}{p}$ and $\frac{2\pi}{q}$ respectively. We put $O_1 = A^a$ and $O_2 = B^b$. Then $(O_1O_2)^n = \left(A^aB^b\right)^n$. By the assumptions $a \neq \frac{p}{2}$ and $b \neq \frac{q}{2}$. Moreover, neither O_1 nor O_2 is a rotation by $\pi/2$. Therefore, using Lemma 1 we get $\left(A^aB^b\right)^n \neq 1$. □

Combining corollary 1 with the results of Section 3.2 we get:

Theorem 3. *Assume* $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi\}$. *Let*

$$S = \{O_{k,l} : O_{k,l} \in SO(3),\, k,l \in \{1,\, 2,\, 3\}\,,\, k < l\}\,,$$

where $O_{k,l}$ *are given by (1). The set* S *generates* $SO(3)$ *and hence a real 2-mode beamsplitter is universal on 3-modes.*

3.4 A real 2-mode beamsplitter is universal on m *modes,* $m \geq 3$

In the previous section we discussed the first non-trivial case, that is, $SO(3)$. It turns out that having the result for $SO(3)$ is almost enough to state the corresponding one for $SO(N)$. To this end let us denote by $\{|i\rangle\}_{i=1}^{N}$ a basis of $\mathbb{C}^N$. In this section we will consider the following set

$$S = \{O_{k,l} : O_{k,l} \in SO(N),\, k,l \in \{1,\ldots,N\}\,,\, k < l\}\,, \tag{19}$$

where $O_{k,l}$ represent the matrix of a beamsplitter acting on modes k, l:

$$O_{kl} = \cos\theta\,(|k\rangle\langle k| + |l\rangle\langle l|) + \sin\theta\,(|k\rangle\langle l| - |l\rangle\langle k|)\,.$$

The number of these matrices is $N(N-1)/2$. The Lie algebra elements satisfying $e^{X_{kl}} = O_{kl}$ are given by

$$X_{kl} = \theta\,(|k\rangle\langle l| - |l\rangle\langle k|) = \theta E_{kl}, \tag{20}$$

where $\{E_{kl}\}_{k<l}$ is a standard basis of $\mathfrak{so}(N)$ and we have the following commutation relations:

$$[X_{k,l}, X_{k,m}] = -\theta X_{l,m},\;\; [X_{k,l}, X_{l,m}] = \theta X_{k,m}, [X_{k,m}, X_{l,m}] = -\theta X_{k,m},$$

where we assumed $k < l$, $l < m$, $k < m$.

We first, in section 3.4.1 give an argument based purely on Theorem 1 which shows that generation of $SO(3)$ by $\{O_{1,2}, O_{2,3}, O_{1,3}\}$ implies generation of $SO(N)$ by S (defined as in (19)). This reasoning is then extended in section 4 to state some general facts about universality of m-mode beamsplitters, where $m > 2$. In section 3.4.2 we give another argument which is tailored specifically for 2-mode beamsplitters. It has an interesting advantage over the general argument which we discuss in section 3.4.1.

3.4.1 General argument

Fact 3. *Assume that* $\{O_{1,2}, O_{2,3}, O_{1,3}\}$ *generates* $SO(3)$. *Then*

$$\{O_{k,l} : O_{k,l} \in SO(N),\, k,l \in \{1,\ldots,N\}\,,\, k < l\} \tag{21}$$

generates $SO(N)$.

Proof. Assume that $\{O_{1,2}, O_{2,3}, O_{1,3}\}$ generates $SO(3)$. In particular, it means that after closure one can obtain any 2-mode beamsplitter $O \in SO(2) \subset SO(3)$ acting on any pair of available 3 modes. Therefore we have (at least in the limit) access to elements $e^{E_{12}}$, $e^{E_{13}}$, $e^{E_{23}}$.

Repeating that argument for any three out of N modes we obtain all possible elements $e^{E_{kl}}$ with $1 \leq k < l \leq N$- some are obtained more than once. Note that set $\{E_{kl}\}_{k<l}$ is a standard basis of $\mathfrak{so}(N)$ and the rotation angle of $e^{E_{kl}}$ is 1 which is clearly not a rational multiple of π. Therefore, by Theorem 1, we get the desired result. □

In the proof of Fact 3 we used that certain elements are available after closure. It is not clear, and in general may not be true, that they are available before closing set $< S >$. In the situation when the dense set generated by $\{O_{1,2}, O_{2,3}, O_{1,3}\}$ does not contain elements $e^{E_{12}}$, $e^{E_{13}}$, $e^{E_{23}}$ the argument described above uses elements that are available only in the approximate sense to show generation of $SO(N)$. From the mathematical point of view this is not a problem. One can also say that perhaps other elements $e^{\phi_{12}E_{12}}$, $e^{\phi_{13}E_{13}}$, $e^{\phi_{23}E_{23}}$ with ϕ_{ij} not rational multiples of π are in fact available in $< O_{1,2}, O_{2,3}, O_{1,3} >$. This can be true, however, it is not clear which ϕ_{ij}'s are possible and which are not. Therefore, the proof does not give any insight into how elements of $SO(N)$ are generated. Form the practical point of view one would like to know at least one example of a small number of elements that belong to $< S >$, that can be constructed in a simple way from the available beamsplitter and that enable generation of any element of $SO(N)$. In section 3.4.2 we show an exemplary construction which provides the set of elements $S^{(N)}$ that generates a dense set in $SO(N)$ and satisfies the assumptions of theorem 1. Moreover these elements are available in $< S >$ before any closure and they are given by products of the original beamsplitter acting on selected triplets of modes. The construction can be viewed as an alternative proof of Fact 3.

3.4.2 The example

If $\theta \neq 0$ then $\{X_{kl}\}_{k<l}$,where X_{kl} is given by (20), spans Lie algebra $\mathfrak{so}(3)$. Moreover when $\theta = a\pi$, $a \notin \mathbb{Q}$ then $< O_{k,l} >$ is dense in $\left\{e^{tX_{k,l}} : t \in R\right\}$. Therefore we can use Theorem 1 and obtain that $\{O_{kl}\}_{k<l}$ generates dense subset of $SO(N)$. What is left is to consider the case when $a \in \mathbb{Q}$. Note that for $k < l$ and $m < n$, we have $O_{k,l}O_{m,n} = O_{m,n}O_{k,l}$ iff $\{k,l\} \cap \{m,n\} = \emptyset$. In this case non-trivial elements of the spectrum (i.e. those different from 1) of $O_{k,l}O_{m,n}$ are nontrivial elements of spectra of $O_{k,l}$ and $O_{m,n}$ and hence if a is rational they are rational multiples of π. Thus we are interested only in the case when $\{k,l\} \cap \{m,n\} \neq 0$. Without any loss of generality we can assume that $k \leq m$. We have three possibilities:

$$\begin{aligned} k = m &: \ O_{k,l}O_{k,n}, \\ l = m &: \ O_{k,l}O_{l,n}, \\ l = n &: \ O_{k,l}O_{m,l}. \end{aligned} \tag{22}$$

Consider now the isomorphism: $|k\rangle \mapsto |1\rangle$, $|l\rangle \mapsto |2\rangle$, $|m\rangle \mapsto |3\rangle$($|n\rangle \mapsto |3\rangle$) between the 3-dimensional spaces: $\mathrm{Span}_{\mathbb{C}}\{|k\rangle, |l\rangle, |m\rangle(|n\rangle)\}$ and $\mathbb{C}^3$. Under this isomorphism we can apply Theorem 1 and obtain that spectra of matrices (22) are irrational multiples of π. Moreover,

we can use formulas (12) to find the corresponding BCH elements belonging to $\mathfrak{so}(N)$:

$$\mathrm{BCH}(X_{k,l}, X_{k,n}) = \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\left(\cos^2\frac{\theta}{2}X_{k,l} + \cos^2\frac{\theta}{2}X_{k,n} - \frac{1}{2}\sin\theta X_{l,n}\right),$$

$$\mathrm{BCH}(X_{k,l}, X_{l,n}) = \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\left(\cos^2\frac{\theta}{2}X_{k,l} + \cos^2\frac{\theta}{2}X_{l,n} + \frac{1}{2}\sin\theta X_{k,n}\right),$$

$$\mathrm{BCH}(X_{k,m}, X_{l,m}) = \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta\left(\cos^2\frac{\theta}{2}X_{k,m} + \cos^2\frac{\theta}{2}X_{k,m} - \frac{1}{2}\sin\theta X_{k,m}\right),$$

where $d = \sin\theta\sqrt{2\cos^4(\theta/2) + 1/4\sin^2\theta}$. Next we explain how to chose indices $\{k,l\}$ and $\{m,n\}$ so that the corresponding BCH elements generate $\mathfrak{so}(N)$. This is in fact the nontrivial part of the extension from $\mathfrak{so}(3)$ to $\mathfrak{so}(N)$, $N > 3$.

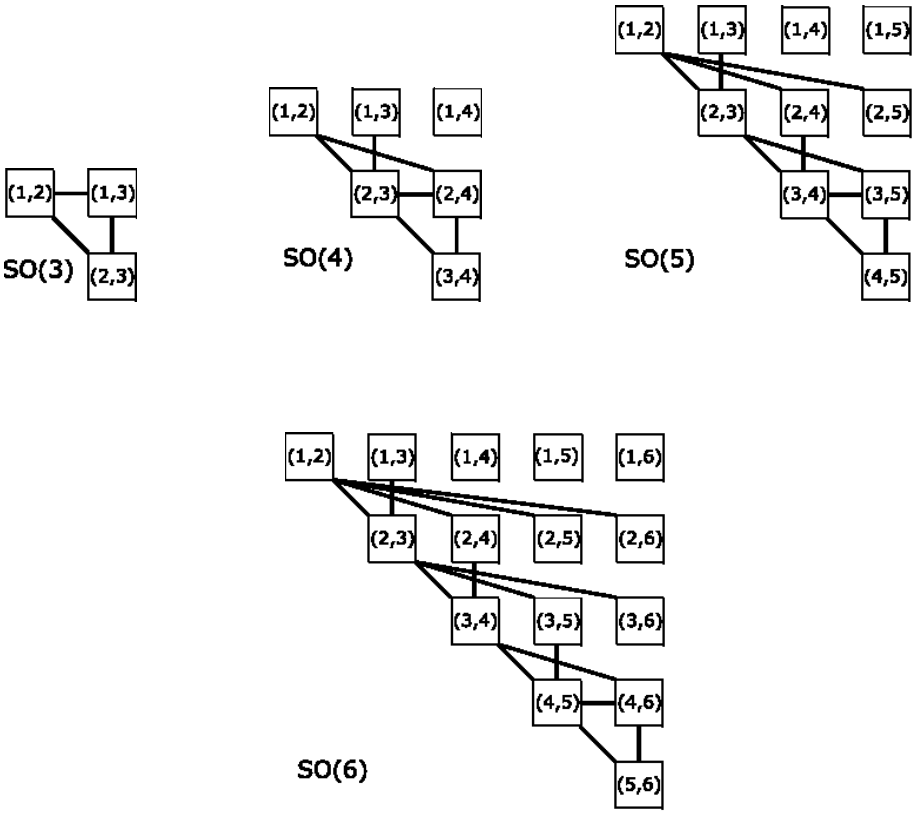

Fig. 1. The pictorial representation of the rules for choosing elements $O_{k,l}O_{m,n}$. An index (k,l) represent the matrix $O_{k,l}$. If indices (k,l) and (m,n) are connected by a line then matrix $O_{k,l}O_{m,n}$ is chosen as an element of a new generating set for $SO(N)$.

In case of $SO(3)$ we chosen as a new generating set

$$S^{(3)} = \{O_{12}O_{13},\, O_{12}O_{23},\, O_{13}O_{23}\},$$

and showed that corresponding BCH elements form the basis of $\mathfrak{so}(3)$. The construction of the basis for $N > 3$ is presented pictorially in figure 1. Each "box" with an index (i,j)

represents the matrix $O_{i,j}$. If there is a line between two boxes (k,l) and (m,n), where $k \leq m$ the product $O_{k,l}O_{m,n}$ is a member of a new generating set for $SO(N)$. For example in case of $SO(4)$ we have:

$$S^{(4)} = \{O_{2,3}O_{2,4},\, O_{2,3}O_{3,4},\, O_{2,4}O_{3,4}\} \cup \{O_{1,2}O_{2,3},\, O_{1,2}O_{2,4}, O_{1,3}O_{2,3}\} \simeq \\ \simeq S^{(3)} \cup R^{(4)},$$

where $R^{(4)} = \{O_{1,2}O_{2,3},\, O_{1,2}O_{2,4}, O_{1,3}O_{2,3}\}$. The first set, $S^{(3)}$, is isomorphic to the one we used for $SO(3)$ (under isomorphism $|1\rangle \mapsto |2\rangle$, $|2\rangle \mapsto |3\rangle$, $|3\rangle \mapsto |4\rangle$). We need to show that BCH elements

$$\{\mathrm{BCH}(X_{2,3}X_{2,4}),\, \mathrm{BCH}(X_{2,3}X_{3,4}),\, \mathrm{BCH}(X_{2,4}X_{3,4})\} \cup \\ \cup \{\mathrm{BCH}(X_{1,2}X_{2,3}),\, \mathrm{BCH}(O_{1,2}O_{2,4}),\, \mathrm{BCH}(O_{1,3}O_{2,3})\}\,,$$

are linearly independent. To this end we write them in the standard basis $\{E_{k,l}\}_{k<l}$ of $\mathfrak{so}(4)$. The corresponding coefficients form columns of the change of basis matrix. We use the ordering of the basis elements that reflects the structure of $S^{(4)}$ that is $\{E_{2,3},\, E_{2,4},\, E_{3,4}\} \cup \{E_{12},\, E_{13},\, E_{14}\}$. Under these assumption the change of basis matrix has the following structure:

$$\frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta \cdot A_{SO(4)} = \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta \begin{pmatrix} A_{SO(3)} & N \\ 0_{3\times 3} & P_{SO(4)} \end{pmatrix},$$

where

$$N = \begin{pmatrix} \cos^2\frac{\theta}{2} & 0 & \cos^2\frac{\theta}{2} \\ 0 & \cos^2\frac{\theta}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix},\; P_{SO(4)} = \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos^2\frac{\theta}{2} & -\frac{1}{2}\sin\theta \\ \frac{1}{2}\sin\theta & 0 & \cos^2\frac{\theta}{2} \\ 0 & \frac{1}{2}\sin\theta & 0 \end{pmatrix}.$$

Since we are interested in the determinant only, the matrix N is irrelevant for calculation of $\det(A_{SO(4)}) = \det(A_{SO(3)}) \cdot \det(P_{SO(4)})$. But $\det(P_{SO(4)}) = -\frac{1}{2}\sin\theta\left(\frac{1}{4}\sin^2\theta + \cos^4\frac{\theta}{2}\right)$ and hence vanishes iff $\theta = 0$ or $\theta = \pi$.

General N To prove that BCH elements corresponding to products of rotations chosen according to the rules explained in figure 1 form the basis of $\mathfrak{so}(N)$ we proceed by induction. Assume that $\det(A_{SO(N-1)})$ is nontrivial except for $\theta \in \{0,\, \frac{\pi}{2},\, \pi,\, \frac{3}{2}\pi\}$. Next note that $S^{(N)} \simeq S^{(N-1)} \cup R^{(N)}$ where

$$R^{(N)} = \{O_{1,2}O_{2,3},\, O_{1,2}O_{2,4}, \ldots,\, O_{1,2}O_{2,N},\, O_{1,3}O_{2,3}\}\,.$$

Therefore the change of basis matrix has a structure

$$\frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta \cdot A_{SO(N)} = \frac{\sin^{-1}(d)}{d\cdot\theta}\sin\theta \begin{pmatrix} A_{SO(N-1)} & N \\ 0 & P_{SO(N)} \end{pmatrix},$$

where

$$P_{SO(N)} = \begin{pmatrix} -\frac{1}{2}\sin\theta & \cos^2\frac{\theta}{2} & \cos^2\frac{\theta}{2} & & \cos^2\frac{\theta}{2} \\ \cos^2\frac{\theta}{2} & \frac{1}{2}\sin\theta & 0 & & 0 \\ & & \frac{1}{2}\sin\theta & & \vdots \\ & & & \ddots & 0 \\ & & & & \frac{1}{2}\sin\theta \end{pmatrix}.$$

Therefore $\det P_{SO(N)} = \left(-\frac{1}{2}\right)^N \sin^N\theta - \cos^2\frac{\theta}{2}\det P'_{SO(N)}$ where

$$P'_{SO(N)} = \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos^2\frac{\theta}{2} & \cos^2\frac{\theta}{2} & & \cos^2\frac{\theta}{2} \\ 0 & \frac{1}{2}\sin\theta & 0 & & 0 \\ 0 & 0 & \frac{1}{2}\sin\theta & & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & & & \frac{1}{2}\sin\theta \end{pmatrix},$$

and is $N-1\times N-1$ matrix. Hence

$$\det P_{SO(N)} = -\left(\frac{1}{2}\right)^N \sin^N\theta - \left(\frac{1}{2}\right)^{N-2}\sin^{N-2}\theta\cos^4\frac{\theta}{2} = \\ = -\left(\frac{1}{2}\right)^{N-2}\sin^{N-2}\theta\left(\frac{1}{4}\sin^2\theta + \cos^4\frac{\theta}{2}\right),$$

and $\det P_{SO(N)} = 0$ iff $\theta = 0$ or $\theta = \pi$ which finishes the induction step of the proof.

Theorem 4. *Assume* $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. *Let*

$$S = \{O_{k,l} : O_{k,l} \in SO(N),\, k,l \in \{1,\ldots,N\},\, k<l\},$$

where $O_{k,l}$ *represent the matrix of a beamsplitter acting on modes k,l:*

$$O_{kl} = \cos\theta\,(|k\rangle\langle k| + |l\rangle\langle l|) + \sin\theta\,(|k\rangle\langle l| - |l\rangle\langle k|).$$

The set S generates $SO(N)$.

Remark 2. *In [19] it was shown that one can not make arbitrary unitary transformations using only beam splitters when acting on two qubits. This result is not in contradiction with the fact that a 2-mode beamsplitter generates* $SO(4)$. *The point is that in the setting of [19] 'modes' are divided into two pairs and the beamsplitters can only act separately on these pairs. In our setting they are allowed to act on any pair of modes and therefore they can generate more than* $SO(2)\times SO(2)$ *which happens to be entire* $SO(4)$.

4 m-mode beamsplitters

In case of a 2-mode beamsplitter the freedom stemming from mode permutations was not significant since it was changing O_2 into O_2^{-1}. For m-mode beamsplitters with $m \geq 3$ we have two situations which should be treated differently.

Let $\mathrm{Sym}(m)$ be a permutation group of m elements, $|\mathrm{Sym}(m)| = m!$. We consider an m-mode beamsplitter $O_m = e^{A_m} \in SO(m)$, $m \geq 3$. Taking into account all possible mode

permutations the starting point is not a single beamsplitter but rather a set of beamsplitters given by matrices:

$$S(O_m) := \{P_\sigma^T O_m P_\sigma : \sigma \in \mathrm{Sym}(m)\},$$

where P_σ is an $m \times m$ permutation matrix corresponding to $\sigma \in \mathrm{Sym}(m)$. Note that by Schur's lemma $S(O_m)$ has always at least two elements as the only permutation invariant matrix in $SO(m)$ is the identity matrix. However, we still can have two cases:

1. Trivial action of $\mathrm{Sym}(m)$: $S(O_m)$ consists of O_m and O_m^{-1}. In this case the action of permutation group is exactly as for a 2-mode beamsplitter.

2. Nontrivial action of $\mathrm{Sym}(m)$: $S(O_m)$ has at least two non-commuting elements. Combining this with a standard result of Kuranishi [9] saying that the set of pairs that generate a semisimple Lie group G is open and dense in $G \times G$ then is a good chance set $S(O_m)$ generates $SO(m)$.

From now on we will say that O_m is universal on $k \geq m$ modes iff the set $S(O_m)$ is universal on $k \geq m$ modes.

Remark 3. *If a beamsplitter O_m falls into the first case then it cannot be universal on m-modes if only m of them are at our disposal. On the other hand, if O_m belongs to the second case it can be universal on m-modes without usage of any additional modes.*

Having $X \in \mathfrak{so}(m)$ we can embed it into $\mathfrak{so}(m+k)$ in $\binom{m+k}{m}$ natural ways and similarly having $O \in SO(m)$ we can embed it into $SO(m+k)$ in $\binom{m+k}{m}$ natural ways by choosing m out of $m+k$ modes and letting X or O operate on them. For example in case when $m = 3$ and $k = 1$ we have

$$\mathfrak{so}(3) \hookrightarrow \mathfrak{so}(4) : \begin{pmatrix} * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} * & * & 0 & * \\ * & * & 0 & * \\ 0 & 0 & 0 & 0 \\ * & * & 0 & * \end{pmatrix}, \begin{pmatrix} * & 0 & * & * \\ 0 & 0 & 0 & 0 \\ * & 0 & * & * \\ * & 0 & * & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix},$$

$$SO(3) \hookrightarrow SO(4) : \begin{pmatrix} * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} * & * & 0 & * \\ * & * & 0 & * \\ 0 & 0 & 1 & 0 \\ * & * & 0 & * \end{pmatrix}, \begin{pmatrix} * & 0 & * & * \\ 0 & 1 & 0 & 0 \\ * & 0 & * & * \\ * & 0 & * & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}.$$

We start with the following simple fact:

Fact 4. *Let $X = \{X_1, \ldots, X_k\} \subset \mathfrak{so}(m)$. Consider $\binom{m+k}{k}$ natural embedding of X into $\mathfrak{so}(m+k)$. If X generates $\mathfrak{so}(m)$ then the $\binom{m+k}{k}$ natural embedding of X into $\mathfrak{so}(m+k)$ generate $\mathfrak{so}(m+k)$.*

Proof. As X generates $\mathfrak{so}(m)$ we have a basis of $\mathfrak{so}(m)$ at our disposal. In particular we can chose it to be a standard basis $\{E_{i,j}\}_{i<j}$, where $1 \leq i, j \leq m$. By definition of standard basis, it is obvious that $\binom{m+k}{k}$ natural embeddings of this basis into $\mathfrak{so}(m+k)$ gives a set which is an overcomplete basis of $\mathfrak{so}(m+k)$. Therefore the result follows. □

Fact 5. *The group $< e^{A_m} >$ with $A_m \in \mathfrak{so}(m)$ is dense in $\{e^{tA_m} : t \in \mathbb{R}\}$ iff spectrum of e^{A_m} is given by $\{e^{i\phi_k} : k \in \{1, \ldots, m\}\}$ with all ϕ_i's being irrational multiples of π.*

Proof. A direct generalization of 2-mode case. □

Theorem 5. *(Non-trivial action* $\mathrm{Sym}(m)$*) Assume that for an* m*-mode beamsplitter* $< S(O_m) >$ *is dense in* $SO(m)$*. Then* O_m *is universal on* k *modes for any* $k \geq m$*.*

Proof. As the set generated by $< S(O_m) >$ is dense in $SO(m)$ we have access to any matrix from $SO(m)$ (at least after closure). Having arbitrary $SO(m)$ matrix we choose the set $B = \{e^{X_i} : X_i \in \mathfrak{so}(m),\, i \in \{1, ..., k\}\}$, where $X = \{X_1, \ldots, X_k\}$ generate $\mathfrak{so}(m)$ and spectra of X_i's are as in Fact 5. By Fact 4 the $\binom{m+k}{k}$ natural embedding of X into $\mathfrak{so}(m+k)$ generate $\mathfrak{so}(m+k)$. As the assumptions of Fact 5 are satisfied we can use Theorem 1 and get the desired result. □

Theorem 6. *(Trivial action of* $\mathrm{Sym}(m)$*) Assume that for an* m*-mode beamsplitter* $S(O_m) = \left\{O_m, O_m^{-1}\right\}$ *and the* $\binom{m+k}{k}$ *natural embeddings of* $S(O_m)$ *into* $SO(m+k)$ *generate dense set in* $SO(m+k)$ *for some* k*. Then* O_m *is universal on* l *modes for any* $l \geq m+k$*.*

Proof. The analogous to the proof of Theorem 5. □

Remark 4. *(1) All the statements of this section remain true if we substitute* $SO(k)$, $\mathfrak{so}(k)$ *with* $SU(k)$, $\mathfrak{su}(k)$*. (2) Theorem 5 can be used to prove Theorem 4. We however found the calculation using only the BCH formula elegant and worth presenting.*

5 3-mode beamsplitter

In this section we present the full discussion for $S(O_3)$.

The Lie Algebra $\mathfrak{so}(3)$ is generated by $\{E_{12}, E_{13}, E_{23}\}$. Let $O_3 = e^{A_3}$ where

$$A_3 = \theta \begin{pmatrix} 0 & a_{12} & a_{13} \\ -a_{12} & 0 & a_{23} \\ -a_{13} & -a_{23} & 0 \end{pmatrix} = \theta \sum_{ij} a_{ij} E_{ij},$$

$a_{ij} \in \mathbb{R}$ and $\sum |a_{ij}|^2 = 1$. The permutation group consists of six elements

$$\mathrm{Sym}(3) = \{e,\, (1,2),\, (1,3),\, (2,3),\, (1,2,3),\, (1,3,2)\}.$$

We want to consider set $S(O_3) = \{P_\sigma^t O_3 P_\sigma : \sigma \in \mathrm{Sym}(3)\}$. Making use of $P_\sigma^t O_3 P_\sigma = e^{P_\sigma^t A_3 P_\sigma}$, we have the following $S(A_3)$ set of Lie algebra elements

$$A_3 = a_{12}E_{12} + a_{13}E_{13} + a_{23}E_{23},\; P_{(1,2)}^T A_3 P_{(1,2)} = -a_{12}E_{12} + a_{23}E_{13} + a_{13}E_{23},$$
$$P_{(1,3)}^T A_3 P_{(1,3)} = -a_{23}E_{12} - a_{13}E_{13} - a_{12}E_{23},\; P_{(2,3)}^T A_3 P_{(2,3)} = a_{13}E_{12} + a_{12}E_{13} - a_{23}E_{23},$$
$$P_{(1,2,3)}^T A_3 P_{(1,2,3)} = -a_{13}E_{12} - a_{23}E_{13} + a_{12}E_{23},\; P_{(1,3,2)}^T A_3 P_{(1,3,2)} = a_{23}E_{12} - a_{12}E_{13} - a_{13}E_{23}.$$

Note that if $S(O_3) = \{O_3, O_3^{-1}\}$ then $P_\sigma^t A_3 P_\sigma = \pm A_3$ for any $\sigma \in \mathrm{Sym}(3)$. It happens when $a_{12} = -a_{13} = a_{23}$, i.e. when

$$A_3 = \frac{\theta}{\sqrt{3}} \left(E_{12} - E_{13} + E_{23}\right).$$

In the following we divide our discussion of 3-mode beamsplitters into two cases according to the behavior under mode permutations.

5.1 *Nontrivial action of* Sym(3)

In this section we consider those beamsplitters whose $A_3 \neq \frac{\theta}{\sqrt{3}}(E_{12} - E_{13} + E_{23})$. Our goal is to first show that in such a case $S(A_3)$ generate the Lie algebra $\mathfrak{so}(3)$. Let us start with the following simple lemma.

Lemma 2. *Let $X, Y \in \mathfrak{so}(3)$ be linearly independent. Then X, Y generate $\mathfrak{so}(3)$.*

Proof. Let $\{X_{12}, X_{13}, X_{23}\}$ be a basis of $\mathfrak{so}(3)$, where $X_{ij} = |i\rangle\langle j| - |j\rangle\langle i|$. We have:

$$\begin{gathered} X = \alpha_1 X_{12} + \beta_1 X_{13} + \gamma_1 X_{23}, \\ Y = \alpha_2 X_{12} + \beta_2 X_{13} + \gamma_2 X_{23}, \\ [X,Y] = (\gamma_1\beta_2 - \beta_1\gamma_2) X_{12} + (\alpha_1\gamma_2 - \gamma_1\alpha_2) X_{13} + (\beta_1\alpha_2 - \alpha_1\beta_2) = \\ = -M_{31} X_{12} + M_{32} X_{13} - M_{33} X_{23} \end{gathered}$$

We need to show that X, Y and $[X,Y]$ form a basis of $\mathfrak{so}(3)$. To this end we calculate

$$\det \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ -M_{31} & M_{32} & M_{33} \end{pmatrix} = -\left(M_{31}^2 + M_{32}^2 + M_{33}^2\right) \neq 0, \tag{23}$$

since X and Y are linearly independent (at least one of $M_{ij} \neq 0$). □

Next we proceed with the proof that $S(A_3)$ generates $\mathfrak{so}(3)$. There are a few cases to consider.

1. Exactly one of a_{ij} is non-zero. Without loss of generality assume that $a_{12} \neq 0$ and $a_{13} = 0 = a_{23}$. In this case elements

$$A_3 = a_{12}E_{12},\ P_{(1,3)}^T A_3 P_{(1,3)} = -a_{12}E_{23},\ P_{(2,3)}^T A_3 P_{(2,3)} = a_{12}E_{13}, \tag{24}$$

   form the basis of $\mathfrak{so}(3)$ and therefore matrices $\{P_\sigma^T A_3 P_\sigma : \sigma \in S_3\}$ generate $\mathfrak{so}(3)$.

2. There are exactly two non-zero a_{ij}'s. Assume for example that $a_{12} = 0$. Then

$$A_3 = a_{13}E_{13} + a_{23}E_{23},\ P_{(1,3)}^T A_3 P_{(1,3)} = -a_{23}E_{12} - a_{13}E_{13},$$

   are clearly linearly independent and by Lemma 2 they generate $\mathfrak{so}(3)$.

3. All a_{ij}'s are non-vanishing. We need to consider two cases: (a) $a_{12} \neq -a_{13} \neq a_{23}$ or $a_{12} = -a_{13} \neq a_{23}$ or $a_{12} = a_{23} \neq -a_{13}$ then A_3 and $P_{(1,2)}^T A_3 P_{(1,2)}$ are linearly independent and by Lemma 2 they generate $\mathfrak{so}(3)$, (b) $a_{12} \neq -a_{13} = a_{23}$ then A_3 and $P_{(2,3)}^T A_3 P_{(2,3)}$ are linearly independent and by Lemma 2 they generate $\mathfrak{so}(3)$.

Therefore we have

Fact 6. *Let $O_3 = e^{A_3}$ be a beamsplitter which admits nontrivial action of* Sym(3)*. Then $S(A_3)$ generates $\mathfrak{so}(3)$.*

5.1.1 The case when θ is an irrational multiple of π

Combining Fact 6 with theorems 1 and 5 we obtain:

Theorem 7. *Let $O_3 = e^{A_3}$ be a 3-mode beamsplitter which admits nontrivial action of* Sym(3) *and whose spectrum is given by $\{e^{i\theta}, e^{-i\theta}, 1\}$ where θ is not a rational multiple of π. Then $S(O_3)$ generates $SO(3)$ and O_3 is universal on $k \geq 3$ modes.*

Remark 5. *Similar reasoning, however with more cases to consider, can be carried out for m-mode beamsplitters with $m > 3$. We will discuss generation of $\mathfrak{so}(m)$ by $S(A_m)$ for $m > 3$ in a subsequent publication including analogous calculations for $\mathfrak{su}(m)$.*

5.1.2 The case when θ is a rational multiple of π

We start with a review of some important and relatively new facts concerning compositions of rotations in $\mathbb{R}^3$.

Let O_1 and O_2 be two finite order rotations about axes separated by an angle α. In the series of papers [3, 4, 15, 14] Conway Radin and Sadun studied the group generated by O_1 and O_2 for large class of α's. This group is characterized by relations that involve generators O_1 and O_2. In order to discuss these relations we recall some basic definitions from algebraic number theory.

Definition 2. *A complex number $z \in \mathbb{C}$ is algebraic iff it is a root of some nonzero polynomial with rational coefficients. If z is not algebraic then it is called transcendental.*

Note that the set of algebraic numbers is countable. This can be easily inferred from the fact that there are countably many coefficients of polynomials in $\mathbb{Q}[x]$ and each polynomial contributes finitely many algebraic numbers. Therefore the set of transcendental numbers is uncountable.

Theorem 8. *[3] Assume that for $\alpha \in [0, 2\pi[$ there are nontrivial relations between O_1 and O_2. Then $e^{i2\alpha}$ is algebraic.*

As an immediate consequence we get:

Corollary 2. *Assume $e^{i2\alpha}$ is transcendental. Then there are no nontrivial relations between O_1 and O_2 and in particular the group generated by O_1 and O_2 is infinite and dense in $SO(3)$*

As $e^{i2\alpha}$ is generically transcendental the above corollary covers almost all cases. What is left is the countable set of these $\alpha \in [0, 2\pi[$ for which $e^{i2\alpha}$ is algebraic. Note that if α is a rational multiple of π then $e^{2i\alpha}$ is algebraic as it is a root of unity (it satisfies $x^q - 1 = 0$ for some $q \in \mathbb{N}$).

Theorem 9. *[14] Let O_1 and O_2 be two finite order rotations about axes separated by an angle α which is a rational multiple of π. A group generated by O_1 and O_2 is infinite and dense in $SO(3)$ with the following three exceptions: (a) Either $O_1 = I$ or $O_2 = I$, (b) $O_1^2 = I$ or $O_2^2 = I$ and $\alpha = \pi/2$, (c)$O_1^4 = I = O_2^4$.*

The exceptions to Theorem 9 correspond to O_i being rotations by: 0, $\pi/2$, π or $3\pi/2$ that we exclude. It is well known that when α is a rational multiple of π the algebraic order of $e^{i2\alpha}$ can be arbitrary large. It is therefore interesting to understand better those angles for which $e^{i2\alpha}$ has, for example, order two. Authors of [3] do this for the so-called geodetic angles, that is angles whose squared trigonometric functions are rational. For this kind of angle they prove relations between O_1 and O_2 can occur only for finite number of α's. The full understanding of all angles for which $e^{i2\alpha}$ is algebraic is however still non-complete.

Let us return to our problem. We assume $O_3 = e^{A_3}$ is nontrivial with respect to mode

permutations. Then the set $S(O_3)$ contains at least two rotations about axes separated by an angle α which is determined by coefficients of A_3. Making use of the facts discussed above we have the following:

Lemma 3. *Assume α is a rational multiple of π or is such that $e^{i2\alpha}$ is transcendental. Then $S(O_3)$ generates $SO(3)$.*

Combining this with Fact 6 and Theorems 1 and 5 we get:

Theorem 10. *Let $O_3 = e^{A_3}$ be a beamsplitter which admits nontrivial action of* Sym(3) *and whose spectrum is given by $\{e^{i\theta}, e^{-i\theta}, 1\}$ where θ is a rational multiple of π. Let α be the angle between rotation axes of two different elements from $S(O_3)$. Assume α is a rational multiple of π or is such that $e^{i2\alpha}$ is transcendental. Then O_3 is universal on $k \geq 3$ modes.*

5.2 Trivial action of Sym(3)

In this section we show that when $S(O_3) = \left\{O_3, O_3^{-1}\right\}$ that is for $O_3 = e^{A_3}$ with

$$A_3 = \frac{\theta}{\sqrt{3}} \left(E_{12} - E_{13} + E_{23}\right),$$

the group generated by the four natural embedding of O_3 into $SO(4)$ is exactly $SO(3)$. Therefore the beamsplitter given by O_3 is not universal on 3 or 4 modes. The four embedding of O_3 into $SO(4)$ are given by $O_{ijk} = e^{\frac{\theta}{\sqrt{3}} A_{ijk}}$ where

$$A_{123} = E_{12} - E_{13} + E_{23},\ A_{234} = E_{23} - E_{24} + E_{34},$$
$$A_{134} = E_{13} - E_{14} + E_{34},\ A_{124} = E_{12} - E_{14} + E_{24}.$$

Elements A_{ijk} are not linearly independent ($A_{123} + A_{134} = A_{124} + A_{234}$) and one can easily verify that they span the 3-dimensional subspace

$$\mathrm{Span}_{\mathbb{R}} \{A_{123}, A_{234}, A_{134}, A_{124}\} \subset \mathfrak{so}(4).$$

Lemma 4. *The space* $\mathrm{Span}_{\mathbb{R}} \{A_{123}, A_{234}, A_{134}, A_{124}\}$ *is a 3-dimensional Lie subalgebra of* $\mathfrak{so}(4)$.

Proof. It is enough to show that $\mathrm{Span}_{\mathbb{R}} \{A_{123}, A_{234}, A_{134}, A_{124}\}$ is closed under Lie bracket. The result follows from the commutations relations

$$[A_{123}, A_{234}] = A_{134} + A_{124},\ [A_{123}, A_{134}] = A_{124} - A_{234},$$
$$[A_{123}, A_{124}] = -A_{234} - A_{134},\ [A_{234}, A_{134}] = A_{123} + A_{124},$$
$$[A_{234}, A_{124}] = A_{123} - A_{134},\ [A_{134}, A_{124}] = A_{123} + A_{234}.$$

□

Let us remind that $\mathfrak{so}(4) \simeq \mathfrak{so}(3) \oplus \mathfrak{so}(3)$. It is therefore natural to suspect that

$$\mathrm{Span}_{\mathbb{R}} \{A_{123}, A_{234}, A_{134}, A_{124}\} \simeq \mathfrak{so}(3). \tag{25}$$

Lemma 5. *The space* $\mathrm{Span}_{\mathbb{R}} \{A_{123}, A_{234}, A_{134}, A_{124}\}$ *is isomorphic to* $\mathfrak{so}(3)$.

Proof. Let

$$X = \frac{1}{4}\left(A_{123} + A_{234} + A_{134} + A_{124}\right),$$
$$Y = \frac{1}{4}\left(A_{123} + A_{234} - A_{134} - A_{124}\right),$$
$$Z = -\frac{1}{4}\left(A_{123} - A_{234} - A_{134} + A_{124}\right).$$

It is easy to verify that $\mathrm{Span}_{\mathbb{R}}\{X, Y, Z\} = \mathrm{Span}_{\mathbb{R}}\{A_{123}, A_{234}, A_{134}, A_{124}\}$. On the other hand we have:

$$[X, Y] = Z,\ [Z, X] = Y,\ [Y, Z] = X,$$

which are commutation relations of $\mathfrak{so}(3)$. □

Combining Lemma 5 with Theorem 1 we get

Theorem 11. *Let θ be an irrational multiple of π. The group generated by four natural embeddings of $O_3 = e^{A_3}$ into $SO(4)$ where*

$$A_3 = \frac{\theta}{\sqrt{3}}\left(E_{12} - E_{13} + E_{23}\right),$$

is isomorphic to $SO(3)$ and therefore O_3 is not universal on 4 modes.

We are left with the case of θ which is a rational multiple of π. By Lemma 5 the rotation matrices O_{ijk} act on some 3-dimensional subspace of $\mathbb{R}^4 = \mathrm{Span}_{\mathbb{R}}\{e_1, e_2, e_3, e_4\}$. Note that, for example, O_{123} and O_{234} are rotations by θ about axes given by:

$$\vec{n}_{123} = -\frac{1}{\sqrt{3}}e_1 + \frac{1}{\sqrt{3}}e_2 - \frac{1}{\sqrt{3}}e_3,$$
$$\vec{n}_{234} = -\frac{1}{\sqrt{3}}e_2 + \frac{1}{\sqrt{3}}e_3 - \frac{1}{\sqrt{3}}e_4.$$

Let α be the angle between $\vec{n}_{123}$ and $\vec{n}_{234}$. One has $\cos(\alpha) = -\frac{2}{3}$ and therefore α is an geodetic angle - an angle whose squared trigonometric functions are rational. The Primordial Theorem (Theorem 2 of [3]) lists all geodetic angles $\alpha = \sin^{-1}\left(\sqrt{\frac{p}{q}}\right)$ with p and q coprime that support nontrivial relations between two finite order rotations about axes separated by α. In our case $\sin(\alpha) = \sqrt{\frac{5}{9}}$ and it does not belong to the list given in [3]. Therefore

Theorem 12. *Let θ be a rational multiple of π. The group generated by four natural embeddings of $O_3 = e^{A_3}$ into $SO(4)$ where*

$$A_3 = \frac{\theta}{\sqrt{3}}\left(E_{12} - E_{13} + E_{23}\right),$$

is isomorphic to $SO(3)$ and therefore O_3 is not universal on 4-modes.

Remark 6. *One can also show that O_3 is not universal on 5-modes - the natural ten embeddings of O_3 into $SO(5)$ generate the group isomorphic to $SO(4)$. We conjecture that on k-modes where $k \geq 4$ the $\binom{k}{3}$ natural embeddings of O_3 generate $SO(k-1)$.*

6 Summary and outlook

In this paper we discussed the universality problem of m-mode real beamsplitters for $m = 2, 3$ from the perspective of control theory using some nice properties of the $SO(3)$ group. We also pointed out the importance of the set $S(O_m)$ which is the orbit of adjoint action of permutation group through O_m. In particular we showed that when $S(O_3) = \{O_3, O_3^{-1}\}$ the beamsplitter O_3 is not universal on both 3 and 4 modes (we also know it is the case for 5-modes). The study of similar phenomena in higher dimensions is a natural direction we want to explore. The other problem would be extension of the result presented here to complex beamsplitters. This requires proving several nontrivial results that we plan to discuss elsewhere.

Acknowledgments

I would like to thank Jan Gutt for the inspiring email correspondence concerning finite generation of Lie groups and Lorenzo Sadun for referring me to papers [3, 4, 14, 15]. Moreover, I thank Scott Aaronson, Adam Bouland, Aram Harrow, Jon Keating, Marek Kuś, John Mackay, Jonathan Robbins, Cyril Stark for discussions, Nick Jones for reading the manuscript and the anonymous referee for suggestions that led to improving the contents of this paper. The author is supported by the Marie Curie International Outgoing Fellowship.

References

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

[2] Y. Bromberg, Y. Lahini, R. Morandotti, and Y. Silberberg, Quantum and Classical Correlations in Waveguide Lattices, Phys. Rev. Lett. 102, 253904, 2009.

[3] J. Conway, C. Radin, L. Sadun, Relations in SO(3) Supported by Geodetic Angles, Discrete Comput. Geom. 23, 453-463, 2000.

[4] J. Conway, C. Radin, L. Sadun, On Angles Whose Squared Trigonometric Functions are Rational, Discrete Comput. Geom. 22, 321-332, 1999.

[5] D. S. Dummit and R. M. Foote, Abstract Algebra, Prentice-Hall, Inc., 1991.

[6] K. Eng On the BCH-formula in so(3) BIT, 41 (3) pp. 629–63, 2001.

[7] W. R. Hamilton Lectures on Quaternions, Hodges and Smith, Dublin, 1853.

[8] V. Jurdjevic, Geometric control theory, Cambridge studies in advanced mathematics 51, Cambridge University Press, New York, 1997.

[9] M. Kuranishi. Two element generations on semi-simple Lie groups, Kodai math. Sem. Report, 9-10, 1949.

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

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

[12] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, Silica-on-Silicon Waveguide Quantum Circuits, Science 320, 646, 2008.

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

[14] C. Radin and L. Sadun, On 2-generator subgroups of SO(3), Trans. Amer. Math. Soc. 351, 4469-4480, 1999.

[15] C. Radin and L. Sadun, Subgroups of SO(3) Associated with Tilings, J. Algebra. 202, 611-633, 1998.

[16] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. Physical Review Letters, 73(1):58–61, 1994.

[17] I. Stewart and D. Tall Algebraic Number Theory and Fermat's last theorem, Natick Massachusetts: A K Peters, 2002.

[18] B. M. Terhal and D. P. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits, Physical Review A 65, 032325, 2002.

[19] L. Vaidman and N. Yoran Methods for reliable teleportation, Phys. Rev. A 59, 116, 1999.