Two-Qubit Circuit Depth and the Monodromy Polytope

Eric C. Peterson, Gavin E. Crooks, and Robert S. Smith

Rigetti Quantum Computing, 2919 Seventh St, Berkeley, CA 94710

For a native gate set which includes all single-qubit gates, we apply results from symplectic geometry to analyze the spaces of two-qubit programs accessible within a fixed number of gates. These techniques yield an explicit description of this subspace as a convex polytope, presented by a family of linear inequalities themselves accessible via a finite calculation. We completely describe this family of inequalities in a variety of familiar example cases, and as a consequence we highlight a certain member of the "XY–family" for which this subspace is particularly large, i.e., for which many two-qubit programs admit expression as low-depth circuits.

1 Introduction

Compilers for quantum computers have two primary tasks. One is to convert a hardware-agnostic description of an algorithm to a hardware-aware description suitable for execution on a particular physical device. This is an involved process, owing both to the idiosyncratic limitations of quantum computational devices and to the extremely large space of quantum programs. Ideal, "pure" quantum programs, which do not interact with the outside world until termination, can be interpreted as points in the projective unitary group $PU(2^q)$ (i.e., unitaries neglecting the effects of global phase), where q is the number of qubits in the system. For all $q > 0$, the group $PU(2^q)$ is infinite, and so quantum compilers must draw on methods from continuous mathematics to accomplish their task.

Optimized expression of a program, a compiler's second task, is of particular interest to programmers of quantum devices which do not yet enjoy fault tolerance. If each instruction has the potential to introduce error into the computation, then after sufficiently many instructions are enacted, the state of the quantum device will no longer even approximate the programmer's intent. Correspondingly, optimization passes in a quantum compiler which lower circuit depth provide a form of noise mitigation, and hence they contribute not just to expedience but to correctness.

In light of this, optimality results for decompositions are of interest to quantum compiler designers. In the presence of recursive compilation schemes (e.g., Quantum Shannon Decomposition [44, Theorem 13]), such results for low numbers of qubits are particularly interesting, as they improve the overall output of the compilation routine by a scalar factor. Some of the most advanced such results to date include: Shende, Bullock, and Markov [43] showed (using an existing framework, see e.g. [31]) that all two-qubit programs can be expressed using three applications of the CZ–gate,[1] interleaved with single-qubit rotations; Zhang, Vala, Sastry, and Whaley [50] showed that all two-qubit programs can be expressed using two applications of the B–gate, interleaved with single-qubit rotations; and the same group showed that a wide class of exponential families of two-qubit gates can be used to implement an arbitrary two-qubit program, using three applications interleaved with single-qubit rotations [49].

This first set of results has two particularly interesting features. First, the methods they describe are computationally tractable: one can actually construct their circuits by using standard algorithms in linear algebra. Second, they use the same techniques in a follow-up paper [45] to analyze the subspace of programs which take no more than two CZs to implement, and they conclude that "almost all" two-qubit programs take three invocations of CZ to implement. Comparing this with the results of the other authors suggests an interesting quality metric on native gate sets: let $\mathcal{L}_{\mathcal{S}}(U)$ be the minimum number of two-qubit gates needed to implement U as a circuit with gates drawn from $\mathcal{S}$. We then conclude that

[1] Equivalently: three applications of CNOT gates.

the expected values satisfy $\langle \mathcal{L}_{\mathrm{CZ}} \rangle = 3$, $\langle \mathcal{L}_{\mathrm{B}} \rangle = 2$, and $\langle \mathcal{L}_{\mathcal{H}} \rangle \leq 3$ for most gate sets of the form $\mathcal{H} = \{H_t = \exp(th) \mid t \in \mathbb{R}\}$ with h a fixed anti-Hermitian matrix.

Although physical devices with native multi-qubit operations other than CZ have been implemented, optimality results and expected gate counts for these other native gate sets have not yet appeared. In this paper, we offer tools for the analysis of these problems at the following level of generality:

Theorem (Corollary 26)**.** *For $\mathcal{S}$ a finite set[2] of two-qubit operations and for $n \geq 0$, let $P^n_{\mathcal{S}} \subseteq PU(4)$ be the following set of two-qubit programs*

$$P^n_{\mathcal{S}} = \left\{ \begin{array}{l} \cdots A_n \; S_n \; \cdots A_1 \; S_1 \; A_0 \cdots \\ \cdots B_n \; \;\; \cdots B_1 \;\;\; B_0 \cdots \end{array} \right\}$$

for $S_j \in \mathcal{S}$ and $A_j, B_j \in PU(2)$. In a certain coordinate system to be described below, $P^n_{\mathcal{S}}$ can be expressed as a union of $(2|\mathcal{S}|)^n$ convex polytopes, each described by a (typically highly redundant) family of linear inequalities of size exponential in n.

We use these results to explore the space of possible choices for the native gate set, with an emphasis on those appearing via Rigetti's choice of interaction Hamiltonian [10] (cf. also [42]): the gates CZ, iSWAP, CPHASE, and XY, where by XY we intend the unitary family

$$\begin{aligned} \mathrm{XY}_\alpha &= \exp\left(-i\alpha(\sigma_X^{\otimes 2} + \sigma_Y^{\otimes 2})\right) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\left(\frac{\alpha}{2}\right) & -i\sin\left(\frac{\alpha}{2}\right) & 0 \\ 0 & -i\sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Our methods in the case of $\mathcal{S} = \{\mathrm{CZ}\}$ recover results of Shende, Bullock, and Markov [43, 45]. In the other cases, we make the following conclusions:

Corollary (Remark 38)**.** *The sets $P^2_{i\mathrm{SWAP}}$ and $P^3_{i\mathrm{SWAP}}$ are the same as the corresponding sets for $\mathcal{S} = \{\mathrm{CZ}\}$. Hence, $P^2_{i\mathrm{SWAP}}$ occupies 0% of the volume of all two-qubit programs, and $\langle \mathcal{L}_{i\mathrm{SWAP}} \rangle = 3$.*

[2]The finiteness assumption on S may be relaxed to account for such families as CPHASE_α.

Corollary (Lemma 46)**.** *Allowing the parameter of* CPHASE *to range freely in $0 \leq \alpha \leq 2\pi$, the sets P^2_{CPHASE} and P^3_{CPHASE} are the same as the corresponding sets for $\mathcal{S} = \{\mathrm{CZ}\}$. Hence, P^2_{CPHASE} occupies 0% of the volume of all two-qubit programs, and $\langle \mathcal{L}_{\mathrm{CPHASE}} \rangle = 3$.*

We find the situation to be quite different for XY:

Corollary (Somewhat informal[3]; Corollary 53, Remark 57)**.** *As a function of α, the volume of the set $P^2_{\mathrm{XY}_\alpha}$ is maximized at $\alpha = 3\pi/4$, where it contains 75% of randomly sampled two-qubit programs. Correspondingly, $\langle \mathcal{L}_{\mathrm{XY}_\alpha} \rangle$ is minimized as $\langle \mathcal{L}_{\mathrm{XY}_\alpha} \rangle = 9/4$. Allowing the parameter of* XY *to range freely, the set P^2_{XY} contains ≈96% of randomly sampled all two-qubit programs, with corresponding value $\langle \mathcal{L}_{\mathrm{XY}} \rangle \approx 2.04$.*

The two most interesting features of this result are that the availability of gates in the XY–family can have a dramatic effect on the optimal gate depth of a generic two-qubit program, and that the bulk of this effect is seen from a *single* gate from this family. At the magic value of $\alpha = 3\pi/4$, we provide an explicit routine for checking membership in this preferred subspace.

Our methods also lend themselves to an analysis of problems in approximate compilation. Each of the sets $P^n_{\mathcal{S}}$ described above is a proper subset of the space of all two-qubit programs, and for a two-qubit program U it is natural to search for the two-qubit program within $P^n_{\mathcal{S}}$ "closest" to U and to give a precise expression for this distance. We give a protocol describing the use of our techniques in this situation, and we give explicit computations of the best approximant and its minimum distance for certain interesting gates (e.g., SWAP) and interesting gate sets (e.g., $\mathrm{XY}_{\frac{3\pi}{4}}$).

We include as appendices an introduction to the mathematics underpinning these results as well as a simpler viewpoint that yields similar qualitative results but is quantitatively inexplicit.

2 The geometry of two-qubit programs and the canonical decomposition

As motivation, we include a brief treatment of the Euler decomposition of single-qubit programs

[3]In particular, the notion of "volume" is different from the usual Haar volume, and so "randomly sampled" also changes meaning.

into triples of rotations. We begin by fixing notation:[4]

$$\mathrm{X}_\alpha = \exp\left(-i\alpha\sigma_X\right) = \begin{pmatrix} \cos\frac{\alpha}{2} & -i\sin\frac{\alpha}{2} \\ -i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix},$$

$$\mathrm{Y}_\alpha = \exp\left(-i\alpha\sigma_Y\right) = \begin{pmatrix} \cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix},$$

$$\mathrm{Z}_\alpha = \exp\left(-i\alpha\sigma_Z\right) = \begin{pmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{pmatrix}.$$

Theorem 1 (YZY–Euler decomposition, [15, pg. 189–207])**.** *Any single-qubit program $U \in PU(2)$ can be expressed as a triple of rotations:*

$$U = \mathrm{Y}_\alpha \cdot \mathrm{Z}_\beta \cdot \mathrm{Y}_\delta,$$

where $0 \leq \beta \leq \pi$. (Moreover, for $0 < \beta < \pi$, the values $0 \leq \alpha, \delta \leq 2\pi$ are essentially unique.)

Proof. This follows as a special case of the *Cartan decomposition*, which we briefly recount for a generic Lie group G. Such a decomposition rests on the choice of an involution θ on G, referred to as a *Cartan involution* on G. The function θ breaks the Lie algebra $\mathfrak{g}$ of G into two parts: the derivative $D_1\theta$ has nontrivial eigenspaces of weights 1 and -1, denoted $\mathfrak{e}$ and $\mathfrak{o}$ respectively, and $\mathfrak{g} = \mathfrak{e} \oplus \mathfrak{o}$. The Cartan decomposition refers to a corresponding decomposition at the level of Lie *groups*: by selecting a maximal abelian subalgebra $\mathfrak{t} \leq \mathfrak{e}$ and exponentiating $\mathfrak{t}$ and $\mathfrak{o}$ to the Lie subgroups T and O, one has

$$G = O \cdot T \cdot O = \{o_1 \cdot t \cdot o_2 \mid o_1, o_2 \in E, t \in T\}.$$

In this context, "abelian" means $[t_1, t_2] = 0$ for any $t_1, t_2 \in \mathfrak{t}$.

Rather than simply remit this decomposition to the literature, we make wholly concrete its application to $PU(2)$. Begin by selecting the involution $\theta_1(U) = U^T$, whose associated eigenspaces $\mathfrak{e}$ and $\mathfrak{o}$ are given by

$$\mathfrak{e} = \langle\sigma_\mathrm{Z}\rangle \oplus \langle\sigma_\mathrm{X}\rangle, \qquad \mathfrak{o} = \langle\sigma_\mathrm{Y}\rangle.$$

Further selecting the maximal abelian subalgebra $\mathfrak{t} = \langle\sigma_\mathrm{Z}\rangle$, the Cartan decomposition associated to this data asserts that any $U \in PU(2)$ can be decomposed as

$$U = \mathrm{Y}_\alpha \cdot \mathrm{Z}_\beta \cdot \mathrm{Y}_\delta.$$

[4] N.B.: This normalization of the Pauli matrices is nonstandard.

Finally, we turn to the algorithmic determination of these parameter values. Inspired by this product form, we consider the *Cartan double* of U:

$$\gamma_1(U) = U \cdot \theta_1(U) = UU^T.$$

In terms of the decomposition, this gives

$$\gamma_1(\mathrm{Y}_\alpha \cdot \mathrm{Z}_\beta \cdot \mathrm{Y}_\delta) = \mathrm{Y}_\alpha \cdot \mathrm{Z}_{2\beta} \cdot \mathrm{Y}_{-\alpha}.$$

Indeed, UU^T is a symmetric unitary matrix and hence admits a basis of real eigenvectors. These can be used to determine the value of α, and the eigenvalues of $\gamma_1(U)$ can be used to determine the value of 2β (and hence β); and the value of the parameter δ can then be determined from $\mathrm{Y}_\delta = \mathrm{Z}_{-\beta} \cdot \mathrm{Y}_{-\alpha} \cdot U$. The claim $0 \leq \beta \leq \pi$ can be guaranteed by beginning with $-\pi \leq \beta \leq \pi$ and, in the case $\beta \leq 0$ is negative, commuting Y_π through the expression. □

Before continuing on to the two-qubit case, we remark on some variations on this result which are specifically useful to quantum computing.

Remark 2. In the practice of microwave-driven superconducting qubits, there is some preferred rotation—say, Z_t—which is a "virtual" operation, implemented as a frame shift, and hence is both instantaneous and immune to device error. Because of this, it would be preferable to have a variant of the decomposition of Theorem 1 in which Z_t appears twice, as it would produce circuits with superior execution properties. One can accomplish this by *conjugation*: given an operator U, its conjugation by Q is defined by $U^Q = Q^\dagger UQ$. This operation enjoys the following properties:

- $(UV)^Q = U^Q V^Q$ and $(U^Q)^\dagger = (U^\dagger)^Q$.
- $(U^Q)^V = U^{QV}$ and $U = (U^Q)^{Q^\dagger}$.
- A *torus* is a connected abelian subgroup of a compact Lie group (e.g., $PU(n)$), and a torus is *maximal* when no larger torus contains it. For any two maximal tori T_1 and T_2, there exists an operator Q such that $T_1^Q = T_2$ [22, Lemma 11.2].[5]

For example, the families Y_t and Z_t are both maximal tori in $PU(2)$, and they are conjugate

[5] However, for maximal tori of higher dimension, one may *not* have element-wise control over how conjugation carries one maximal torus into another.

by the operator $Q_1 = \mathrm{X}_{\frac{\pi}{2}}$:

$$\mathrm{Y}_t^{Q_1} = \mathrm{Z}_t, \qquad \mathrm{Z}_t^{Q_1} = \mathrm{Y}_{-t}.$$

One can then use Q_1 to transform the outer components of Theorem 1 from Y_t to Z_t, which gives the desired decomposition:

$$U = (U^{Q_1^\dagger})^{Q_1} = (\mathrm{Y}_\alpha \mathrm{Z}_\beta \mathrm{Y}_\delta)^{Q_1} = \mathrm{Z}_\alpha \mathrm{Y}_{-\beta} \mathrm{Z}_\delta.$$

Remark 3. Alternatively, one can apply Q_1–conjugation to the set-up of the theorem, rather than its inputs, to reach the same conclusion. Starting with the Cartan involution $\theta(U) = U^T$, we define a new involution[6]

$$\begin{aligned}\theta_1^{Q_1}(U) &= ((U^{Q_1})^T)^{Q_1^\dagger} = Q_1((Q_1^\dagger U Q_1)^T)Q_1^\dagger \\ &= Q_1 Q_1^T U^T (Q_1 Q_1^T)^\dagger = \mathrm{X}_\pi U^T \mathrm{X}_{-\pi}\end{aligned}$$

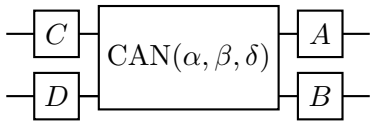
and its associated doubling

$$\gamma_1^{Q_1}(U) = U \cdot \theta^{Q_1}(U) = U \mathrm{X}_\pi U^T \mathrm{X}_{-\pi}.$$

We now turn to the analogous structure theorem for two-qubit operators:

Theorem 4 ("Canonical decomposition", [31, Section III], [33, Theorem 2], [49, Section III.A.1])**.** *Any two-qubit unitary operator U admits an expression as*

$$U = \quad ,$$



where A, B, C, and D are single-qubit operators, where $\pi/2 \geq \alpha \geq \beta \geq |\delta|$ are certain parameters, and where

$$\mathrm{CAN}(\alpha, \beta, \delta) = \exp\left(-i(\alpha \sigma_X^{\otimes 2} + \beta \sigma_Y^{\otimes 2} + \delta \sigma_Z^{\otimes 2})\right).$$

The parameter values are unique, and for generic parameter values the local gates are also unique.

Proof. As before, the Cartan involution $\theta(U) = U^T$ and associated Cartan doubling $\gamma(U) = UU^T$ give a decomposition of an operator V into a product $O_L D O_R$, where these factors satisfy

$$O_L^T = O_L^{-1}, \qquad O_R^T = O_R^{-1}, \qquad D^T = D,$$

hence O_L and O_R are orthogonal and D is symmetric, hence diagonal. As in Remark 2, the theorem as stated arises by conjugating this decomposition by a particular operator Q,

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix},$$

which satisfies

$$(PU(2)^{\otimes 2})^Q = PO(4), \qquad \mathrm{CAN}^Q = \Delta$$

for $\Delta \leq PU(4)$ the diagonal matrices.[7]

To see the constraints on the parameters α, β, and δ, we require an explicit formula for CAN^Q:

$$\mathrm{CAN}(\alpha, \beta, \delta)^Q = \exp\left(i \,\mathrm{diag}\begin{pmatrix} \alpha - \beta + \delta \\ \alpha + \beta - \delta \\ -(\alpha + \beta + \delta) \\ -\alpha + \beta + \delta \end{pmatrix} \right).$$

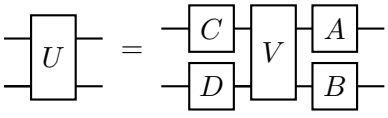
This linear system can be solved for any diagonal matrix $\mathrm{diag}(d_1, d_2, d_3, d_4)$ satisfying $d_+ = 0$, and the resulting parameters can furthermore be taken to lie in the range $[-\pi, \pi]$. Since diagonal operators are stable under conjugation by signed permutation matrices, which are themselves members of $PO(4)$, one may insert such operators into the expression to obtain several equivalent decompositions. One checks that the effects of these signed permutation matrices are generated by permutations and the operator

$$(\alpha, \beta, \delta) \mapsto (\pi - \alpha, \pi - \beta, \delta).$$

It follows that there is a unique representative satisfying the indicated inequality. □

Corollary 5. *If Theorem 4 yields the same canonical parameters for a pair of two-qubit operators U and V, then there exist single-qubit operators A, B, C, and D satisfying*

$$\quad = \quad .$$

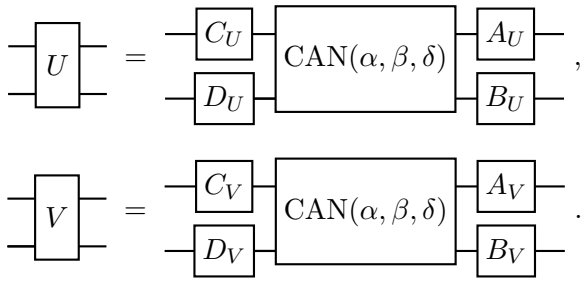


(In this case, U and V are said to be locally equivalent.)

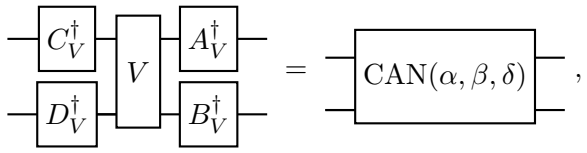
[6] There is a similarity relation $\gamma_1^{Q_1}(U) = \gamma_1(U^{Q_1})^{Q_1^\dagger}$.

[7] Identifying a useful analogue of Q and of $PU(2)^{\otimes 2}$ is the primary inhibitor of generalizing this to higher qubit counts. See [45, Proposition IV.3] for a list of references concerning the provenance of this operator Q.

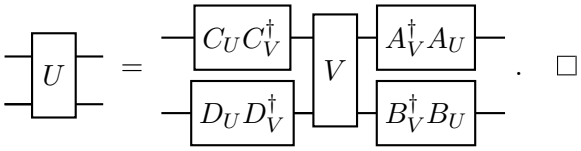
Proof. Apply the Theorem to produce



Solving the second equation for the canonical gate gives



and substituting it into the first yields



□

Remark 6. As in the single-qubit case, this decomposition is algorithmically effective: given a two-qubit gate U, by selecting angle values α, β, and δ the operator spectrum of $\gamma(U^Q)$ can be made to agree with that of $\mathrm{CAN}(\alpha, \beta, \delta)$; a special-orthogonal matrix diagonalizing $\gamma(U^Q)$ recovers A and B; and, from this, one can then solve for C and D [45, Proposition IV.3]. The keystone of Shende, Bullock, and Markov is a process for manufacturing circuits with low CNOT–count for realizing particular values of $\mathrm{CAN}(\alpha, \beta, \delta)$. In general, they show that this requires three applications of CNOT, and they moreover show which gates are accessible within two (resp. one, resp. zero) applications of CNOTs: these are those gates whose canonical parameter δ is fixed at zero (resp. both β and δ are zero, resp. all parameters are zero). With these circuits in hand, they then apply Corollary 5.

Remark 7. In the current practice of quantum computing, single qubit operators typically experience device errors at a rate 1–2 orders of magnitude less than multi-qubit operators, which underscores a compiler designer's desire for decompositions that use two-qubit gates as sparingly as possible. From this perspective, the canonical decomposition neatly cleaves any two-qubit interaction into outer pieces, which are completely assailable by decomposition into single-qubit gates and which hence are representable with good fidelity, and an inner piece, which is completely unassailable by single-qubit gates, for which a general theory of decomposition into native interactions is not known, and which is especially prone to poor fidelity if a decomposition is inefficient. In reaction to this, we will focus all of our attention on the manufacture of families of canonical gates with the shortest circuits possible.

canonical decomp.	$G = \mathrm{Z}_\alpha \mathrm{Y}_\beta \mathrm{Z}_\delta$
orthogonal decomp.	$G^{Q_1} = \mathrm{Y}_{-\alpha} \mathrm{Z}_\beta \mathrm{Y}_{-\delta}$
diagonalized Cartan double	$\gamma^{Q_1}(G) = \mathrm{Y}_{-\alpha} \mathrm{Z}_{2\beta} \mathrm{Y}_\alpha$
canonical parameter	β

Figure 1: Summary of the one-qubit invariants of Section 2 and their interrelations

canonical decomp.	$G = L_1 \cdot \mathrm{CAN} \cdot L_2$, with L_1, L_2 local.
orthogonal decomp.	$G^Q = O_1 D O_2$, with $O_j = L_j^Q$ ortho., $D = \mathrm{CAN}^Q$ diagonal.
diagonalized Cartan double	$\gamma^Q(G) = O_1 D^2 O_1^T$, with $O_1 = L_1^Q$ ortho., $D = \mathrm{CAN}^Q$ diagonal.
canonical parameter	spectrum of D, or spectrum of $\gamma^Q(G)$, or arguments to CAN.

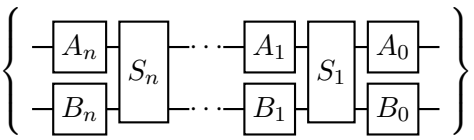
Figure 2: Summary of the two-qubit invariants of Section 2 and their interrelations

3 The multiplicative eigenvalue problem and the monodromy polytope

Shende, Bullock, and Markov's description of those two-qubit programs accessible within a fixed number of applications of CNOT relies on specific commutation relations and explicit computation (cf. Appendix B). We will study a more general version of this same question:

Problem 8. Let $\mathcal{S}$ be a set of two-qubit gates.

1. Describe the subspace $P_{\mathcal{S}}^n$,



for $S_j \in \mathcal{S}$ and $A_j, B_j \in PU(2)$.

2. Given $G \in P_{\mathcal{S}}^n$, algorithmically produce local gates A_j, B_j which realize G as such a circuit.

A solution to the entirety of Problem 8 would yield a depth-optimal compilation algorithm targeting $\mathcal{S}$: given a two-qubit program U, one could compute its canonical parameters, use Problem 8.1 to discern the minimal $P_{\mathcal{S}}^n$ to which they belong, use Problem 8.2 to manufacture a circuit of the prescribed depth and with the prescribed canonical parameters, and finally use Corollary 5 to produce a circuit modeling U. A solution only to Problem 8.1 would yield a method for computing the following interesting value:

Definition 9. Let $\mathcal{L}_{\mathcal{S}}(U)$ be the minimum number of two-qubit gates appearing in any circuit implementation of U using the gate set $\mathcal{S}$. We define the *expected circuit depth of* $\mathcal{S}$ to be

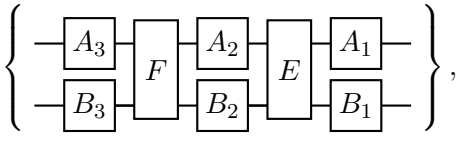
$$\begin{aligned}\langle \mathcal{L}_{\mathcal{S}} \rangle^{\text{Haar}} &= \int_{U \in PU(4)} \mathcal{L}_{\mathcal{S}}(U) d\mu \\ &= \sum_{n=0}^{\infty} n \cdot \text{vol}^{\text{Haar}} \left(\mathcal{L}_{\mathcal{S}}^{-1}(n) \right) \\ &= \sum_{n=0}^{\infty} n \cdot \text{vol}^{\text{Haar}} \left(P_{\mathcal{S}}^n \setminus \bigcup_{j=0}^{n-1} P_{\mathcal{S}}^j \right).\end{aligned}$$

This value measures the efficiency of the gate set $\mathcal{S}$: the smaller $\langle \mathcal{L}_{\mathcal{S}} \rangle^{\text{Haar}}$, the more efficient $\mathcal{S}$ is at encoding programs into circuits.

Sufficiently enticed, we begin with the first nontrivial case where $n = 2$ and where S_1 and S_2 are fixed:

Problem 10. Let E and F be fixed two-qubit gates.

1. Describe the subspace $P \subseteq PU(4)$,



for A_1, A_2, A_3, B_1, B_2, $B_3 \in PU(2)$.

2. Given $G \in P$, algorithmically produce local gates A_1, A_2, A_3, B_1, B_2, and B_3 which realize G as such a circuit.

In this section, we show that this reduces to a well-known problem in representation theory, the *multiplicative eigenvalue problem*, whose solution comes in the form of the *monodromy polytope*.

Using Corollary 5, we can discern whether a given program G belongs to P by computing all of the canonical parameters of the programs in P and checking whether that set includes those of G. In order to make use of this, one would require a compact description of this set of parameters. To begin exploring whether this is feasible, let us go through the motions of computing the canonical parameters of $G \in P$—or, equivalently, computing the spectrum of the Cartan double $\gamma(G^Q)$. Begin by applying Q–conjugation to the supposed decomposition of G to get $G^Q = O_1 E^Q O_2 F^Q O_3$, where each O_j is the orthogonal matrix Q–conjugate to the local gate $(A_j \otimes B_j)$. In turn, E^Q and F^Q have orthogonal decompositions:

$$E^Q = O_{E,L} D_E O_{E,R}, \quad F^Q = O_{F,L} D_F O_{F,R},$$

where D_E and D_F are diagonal and $O_{E,L}$, $O_{E,R}$, $O_{F,L}$, and $O_{F,R}$ are all orthogonal. Combining these decompositions yields

$$G^Q = O_1 O_{E,L} D_E O_{E,R} O_2 O_{F,L} D_F O_{F,R} O_3,$$

from which we compute

$$\begin{aligned}\gamma(G^Q) &= O_1 O_{E,L} D_E O_{E,R} O_2 O_{F,L} D_F O_{F,R} O_3 \cdot \\ &\qquad (O_1 O_{E,L} D_E O_{E,R} O_2 O_{F,L} D_F O_{F,R} O_3)^T \\ &= O_1 O_{E,L} D_E O_{E,R} O_2 O_{F,L} D_F^2 \cdot \\ &\qquad O_{F,L}^T O_2^T O_{E,R}^T D_E O_{E,L}^T O_1^T \\ &\sim D_E^2 O D_F^2 O^T,\end{aligned}$$

where $O = O_{E,R} O_2 O_{F,L}$ is an orthogonal operator and $\sim$ denotes unitary similarity. Altogether, this reduces Problem 10 to the following:

Problem 11. Let D_E and D_F be fixed diagonal special unitary matrices.

1. Calculate the possible spectra of operators of the form $D_E^2 O D_F^2 O^T$ as O ranges over orthogonal matrices.

2. Given a particular such operator spectrum D_G, calculate an orthogonal matrix O such that $D_E^2 O D_F^2 O^T$ diagonalizes to give D_G^2.

Description of reduction. The canonical parameters of G are equivalent data to the spectrum of $\gamma(G^Q)$. Because $\gamma(G^Q)$ is similar to $D_E^2 O D_F^2 O^T$ and because operator similarity preserves spectra, it is equivalent to compute the spectrum of $D_E^2 O D_F^2 O^T$. As G ranges over P (i.e., as the local gates in the circuit vary), the terms O range over $PO(4)$.

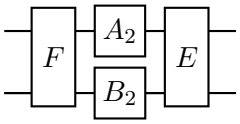
For the second part, suppose that we can construct an O so that $D_E^2 O D_F^2 O^T$ has a prescribed operator spectrum. We may then work backward:

$$\begin{aligned}
&D_E^2 O D_F^2 O^T \\
&\sim D_E O D_F^2 O^T D_E \\
&\sim O_{E,L} D_E O D_F^2 O^T D_E O_{E,L}^T \\
&= O_{E,L} D_E O_{E,R} (O_{E,R}^T O O_{F,R}^T) O_{F,R} D_F O_{F,L} \cdot \\
&\qquad (O_{E,L} D_E O_{E,R} (O_{E,R}^T O O_{F,R}^T) O_{F,R} D_F O_{F,L})^T \\
&= \gamma(O_{E,L} D_E O_{E,R} (O_{E,R}^T O O_{F,R}^T) O_{F,R} D_F O_{F,L}) \\
&= \gamma^Q((1 \otimes 1) E (A_2 \otimes B_2) F (1 \otimes 1)),
\end{aligned}$$

where the local gate $A_2 \otimes B_2$ is determined by the formula

$$(A_2 \otimes B_2)^Q = O_{E,R}^T O O_{F,R}^T.$$

The circuit



then has the prescribed canonical parameters. □

Problem 11 is a restricted instance of the multiplicative eigenvalue problem:

Problem 12 ([1])**.** Let U_1, U_2, and U_3 be unitary operators.

1. *Multiplicative eigenvalue problem*: Describe the possible spectra of all triples U_1, U_2, U_3 satisfying $U_1 U_2 U_3 = 1$.[8]

2. *Effective saturation problem*: Given a triple of operator spectra satisfying the conditions of Problem 12.1, algorithmically produce U_1, U_2, and U_3 realizing these spectra and satisfying $U_1 U_2 U_3 = 1$.

[8]There are also variants of the multiplicative eigenvalue problem concerning products of any fixed length $k \geq 0$.

What is immediately clear is that the collection of spectral quadruples satisfying Problem 11.1 can be converted to satisfy Problem 12.1. Supposing that we have suitable operators D_E, D_F, D_G, and O satisfying the similarity relation above, there must exist a unitary U satisfying

$$\begin{aligned}
\gamma^Q(G) = O_{G,L} D_G^2 O_{G,L}^T &\sim D_E^2 O D_F^2 O^T \\
U^\dagger D_G^2 U &= D_E^2 O D_F^2 O^T,
\end{aligned}$$

which can be rewritten as

$$\begin{aligned}
1 &= D_E^2 (O D_F^2 O^T)(U^\dagger (D_G^2)^\dagger U) \\
&= U_1 U_2 U_3.
\end{aligned}$$

This shows that the spectra of D_E^2 and D_F^2 agree with those of U_1 and U_2, and the spectrum of D_G^2 agrees with that of $U_3^\dagger$. What is not obvious is that the reverse implication is also true: given U_1, U_2, U_3 satisfying $1 = U_1 U_2 U_3$, we would like to know whether it is always possible to factor out orthogonal matrices and rearrange terms to produce a sentence of the form

$$O_{G,L} D_G^2 O_{G,L}^T \sim D_E^2 O D_F^2 O^T.$$

This turns out to be so, which is a nontrivial result in symplectic geometry:

Theorem 13 ([16, Theorem 3])**.** *Suppose that D_1, D_2, D_3 are diagonal operators which satisfy the conditions of Problem 12.1.*[9] *Then there exist operators V_1, V_2, V_3 which diagonalize to D_1, D_2, D_3, which satisfy $V_1 V_2 V_3 = 1$, and for which V_1 and V_2 are orthogonally diagonalizable, i.e.,*

$$V_1 = O_1^T D_1 O_1, \qquad V_2 = O_2^T D_2 O_2,$$

for some orthogonal matrices O_1, O_2. □

Corollary 14. *For U_1, U_2, and U_3 unitaries satisfying $U_1 U_2 U_3 = 1$ and with diagonalizations D_E^2, D_F^2, and $(D_G^2)^\dagger$ respectively, there exists an orthogonal O and a unitary U such that*

$$U^\dagger D_G^2 U = D_E^2 O D_F^2 O^T,$$

i.e., solutions to Problem 12 give rise to solutions to Problem 11.

[9]That is, they appear as the diagonalizations of unitaries U_1, U_2, U_3 satisfying $U_1 U_2 U_3 = 1$.

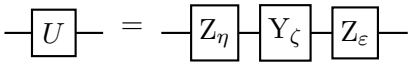
Proof. Start by applying the Theorem:

$$\begin{aligned} 1 &= V_1 V_2 V_3 \\ &= (O_1^T D_E^2 O_1)(O_2^T D_F^2 O_2) V_3 \\ O_1 V_3^\dagger O_1^T &= D_E^2 O_1 O_2^T D_F^2 O_2 O_1^T \\ U^\dagger D_G^2 U &= D_E^2 O D_F^2 O^T, \end{aligned}$$

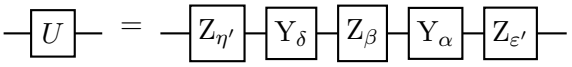
where we have written $O = O_1 O_2^T$ and $U = E O_1^T$ for E a matrix with columns an eigenbasis of $V_3^\dagger$. □

Problem 12.1 has been completely resolved by Agnihotri, Meinrenken, and Woodward. Because even the statement of their result is quite technical, the newcomer may find it too opaque, and so we pause to first investigate some simple cases by hand. We hope that this serves to motivate the full statement of Theorem 23 to follow.

Example 15 ([26, Proposition 3.1]). Let us return to the setting of Remark 2, where we we hypothesized that Z–rotations were less expensive to implement in hardware than Y–rotations, and were thus led to study a decomposition of a single-qubit operator U into the form $U = \mathrm{Z}_\varepsilon \mathrm{Y}_\zeta \mathrm{Z}_\eta$. Let us now further suppose that the supply of Y–rotations is limited: we are only able to implement those whose parameters are drawn from a fixed set. We would then be interested to know, given a program U with canonical decomposition



what are the conditions on ζ such that U admits expression as



with α and δ drawn from the fixed set of parameters? To address this, we study the characteristic polynomial of the Cartan double $\gamma^{Q_1}(U)$, as computed from the canonical decomposition of U and from its putative expression as a circuit with constrained Ys:

$$\begin{aligned} &\chi(\gamma^{Q_1}(U)) = z^2 - \mathrm{tr}(\gamma^{Q_1}(U))z + 1, \\ &\mathrm{tr}(\gamma^{Q_1}(U)) = 2(\cos\alpha\cos\delta - \cos\beta\sin\alpha\sin\delta), \\ &\mathrm{tr}(\gamma^{Q_1}(U)) = 2\cos\zeta, \end{aligned}$$

hence

$$\zeta = \cos^{-1}\left(\cos\alpha\cos\delta - \cos\beta\sin\alpha\sin\delta\right).$$

The role of β is thus to modulate the interference of α and δ, and it imposes the following linear inequality on ε:

$$|\alpha - \delta| \leq \zeta \leq \pi - |\alpha + \delta - \pi|.$$

However, the precise dependence of ζ on β is decidedly nonlinear.[10]

Example 16. In extremely favorable situations, the two-qubit case can also be manually analyzed. Let us consider the gate family

$$\mathrm{SWAP}_t = \exp\left(-2\pi i t(\sigma_{\mathrm{X}}^{\otimes 2} + \sigma_{\mathrm{Y}}^{\otimes 2} + \sigma_{\mathrm{Z}}^{\otimes 2})\right),$$

for which $\gamma^Q(\mathrm{SWAP}_t)$ has spectrum

$$\left(e^{-i\frac{t}{4}}, e^{-i\frac{t}{4}}, e^{-i\frac{t}{4}}, e^{i\frac{3t}{4}}\right),$$

and let us consider the instance of Problem 10.1 for $E = \mathrm{SWAP}_{t_1}$ and $F = \mathrm{SWAP}_{t_2}$. Using the reduction to Problem 12, we will describe the possible spectra for operators of the form

$$U_1 = V^\dagger D_{t_1}^2 V, \quad U_2 = D_{t_2}^2, \quad U_3 = U_1 U_2,$$

where $D_{t_j}^2$ is the diagonal matrix formed from the spectrum of $\gamma^Q(\mathrm{SWAP}_{t_j})$ and V is an arbitrary unitary.

Our first observation is that the eigenspace of weight $\exp(-i\frac{t_j}{4})$ of U_j is 3–dimensional, and hence the intersection of these two eigenspaces for U_1 and U_2 is at least 2–dimensional. It follows that there exists an orthonormal 2–frame $\{b_1, b_2\}$ of eigenvectors for U_3:

$$U_3 b_i = U_1 U_2 b_i = U_1 e^{-i\frac{t_2}{4}} b_i = e^{-i\frac{t_1+t_2}{4}} b_i =: \lambda b_i.$$

In particular, we find U_3 to be block-diagonal in this partial basis: no matter what full orthonormal basis $\{b_1, b_2, b_3, b_4\}$ is chosen, we have

$$U_3 = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & * & * \\ & & * & * \end{pmatrix}$$

in this basis.

It will be convenient to choose the full orthonormal basis so that b_3 spans the complement of $\{b_1, b_2\}$ in the 3–dimensional eigenspace for U_2

[10] As a consequence, we recover the familiar fact that $\alpha = \delta = \pi/2$ generates all rotations with such a circuit.

and b_4 spans the 1–dimensional eigenspace. In this basis, the subblock governing the action of U_3 on $B = \mathrm{span}\{b_3, b_4\}$ becomes

$$(U_3)|_B = \begin{pmatrix} e^{-i\frac{t_1}{4}} & 0 \\ 0 & e^{i\frac{3t_1}{4}} \end{pmatrix} W \begin{pmatrix} e^{-i\frac{t_2}{4}} & 0 \\ 0 & e^{i\frac{3t_2}{4}} \end{pmatrix}$$
$$= \lambda^{-1} \begin{pmatrix} e^{-i\frac{t_1}{2}} & 0 \\ 0 & e^{i\frac{t_1}{2}} \end{pmatrix} W \begin{pmatrix} e^{-i\frac{t_2}{2}} & 0 \\ 0 & e^{i\frac{t_2}{2}} \end{pmatrix}$$

for some auxiliary unitary matrix W. The resulting operator spectra are shifts by λ^{-1} of those those studied in Example 15, hence subject to the same inequalities also shifted by λ^{-1}.[11]

We now turn to the vocabulary needed to enunciate the full solution to Problem 12.1 given by Agnihotri, Meinrenken, and Woodward. Based on our experience with the linear inequality families above, there is a particular presentation of operator spectra which we are likely to find useful:

Definition 17 (cf. [25, Chapter 4])**.** For a special unitary matrix U, we may uniquely present its spectrum

$$\mathrm{Spec}\, U = (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n})$$

as

$$\mathrm{LogSpec}\, U = (a_1, \ldots, a_n),$$

where

$$a_1 \leq \cdots \leq a_n \leq a_1 + 1, \quad a_+ := \sum_j a_j = 0.$$

We refer to the collection of all such n–tuples as $\mathfrak{A}$, the *fundamental alcove* of $SU(n)$, and we will write $\mathrm{LogSpec}\, U$ for the associated point in $\mathfrak{A}$.

The above definition is standard for special unitary matrices, but we will also require the following nonstandard modification:

Definition 18. Let $C_2 \leq SU(4)$ be the finite central subgroup $\{\pm 1\}$,[12] and let $U \in SU(4)/C_2$ be a member of the quotient group, which we may present as a coset

$$\{\tilde{U}, -\tilde{U}\} \subset SU(4).$$

[11] We leave it to the reader to imagine how complex the elementary analysis of the generic case (i.e., without degenerate eigenspaces) can become.

[12] One could make a similar definition for $SU(n)/C_m$ with $m \mid n$, but we will need only this particular case.

The logarithmic spectra of these matrices

$$a_* = \mathrm{LogSpec}\, \tilde{U}, \qquad b_* = \mathrm{LogSpec}(-\tilde{U})$$

are related by a form of rotation:

$$a_* = \rho(b_*)$$
$$:= \left(b_3 - \frac{1}{2}, b_4 - \frac{1}{2}, b_1 + \frac{1}{2}, b_2 + \frac{1}{2}\right).$$

By appropriately picking either $\mathrm{LogSpec}\, U = \mathrm{LogSpec}\, \tilde{U}$ or $\mathrm{LogSpec}\, -\tilde{U}$, we see that we may uniquely specify a sequence $\mathrm{LogSpec}\, U$ which further satisfies either

$$(\mathrm{LogSpec}\, U)_2 + 1/2 > (\mathrm{LogSpec}\, U)_4$$

or

$$\left\{ \begin{array}{c} (\mathrm{LogSpec}\, U)_2 + 1/2 = (\mathrm{LogSpec}\, U)_4 \\ \text{and} \\ (\mathrm{LogSpec}\, U)_1 + 1/2 \leq (\mathrm{LogSpec}\, U)_3 \end{array} \right\},$$

where $(\mathrm{LogSpec}\, U)_j$ denotes the j^{th} component of the quadruple $\mathrm{LogSpec}\, U$. We similarly refer to the collection of all such quadruples as $\mathfrak{A}_{C_2}$, the fundamental alcove of $SU(4)/C_2$.

Remark 19. Definition 17 is the natural target of the logarithmic spectrum of a special unitary operator, and it forms a convex polytope. Definition 18 is useful because it is the natural target of the logarithmic spectrum of the Cartan double of a *projective* unitary operator:

$$\mathrm{LogSpec}\, \gamma(-)\colon\ PU(4) \to \mathfrak{A}_{C_2}.$$

However, it does not quite form a convex polytope: the closure $\overline{\mathfrak{A}_{C_2}}$ is a convex polytope, but the values a_* satisfying $a_2 + 1/2 = a_4$ and $a_1 + 1/2 > a_3$, which constitute half a face of $\overline{\mathfrak{A}_{C_2}}$, are missing from $\mathfrak{A}_{C_2}$.

Definition 20. In line with the program outlined above, we will be especially interested in the assignment

$$\Pi\colon\ PU(4) \to \mathfrak{A}_{C_2},$$
$$U \mapsto \mathrm{LogSpec}\, \gamma(U^Q),$$

which we abbreviate to $\Pi(U)$.

Definition 21. The extremal points of the polytope $\overline{\mathfrak{A}_{C_2}}$ lie at the following coordinates:

$$\begin{aligned}
\Pi(I) &= e_1 = (0,0,0,0)\,,\\
\Pi(\mathrm{CZ}) &= e_2 = \left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\\
\Pi(i\mathrm{SWAP}) &= e_3 = \left(-\frac{1}{2},0,0,\frac{1}{2}\right),\\
\Pi(\mathrm{SWAP}) &= e_4 = \left(-\frac{3}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\\
\Pi(\sqrt{\mathrm{SWAP}}) &= e_5 = \left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\\
\rho(e_5) &= e_6 = \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right).
\end{aligned}$$

The subspace $\mathfrak{A}_{C_2}$ of $\overline{\mathfrak{A}_{C_2}}$ is given by deleting the subspace of convex combinations of e_2, e_3, and e_6 in which e_6 carries a nonzero coefficient.

Definition 22. For $r, k > 0$ be positive integers, let $\mathcal{P}_{r,k}$ denote the set of partitions of k into r parts:

$$\mathcal{P}_{r,k} = \{(I_1, \ldots, I_r) \in \mathbb{Z}^r \mid 0 \leq I_1 \leq \cdots \leq I_r \leq k\}.$$

We are now in a position to state the solution to Problem 12.1. We will give a more complete exposition of this result, its context, and its proof in Appendix A, but for our intended application we need only the following statement:

Theorem 23 (see Theorem 86)**.** *Let U_1, U_2, $U_3 \in SU(n)$ satisfy $U_1U_2 = U_3$, and let*

$$\begin{aligned}
\alpha_* &= \mathrm{LogSpec}\, U_1,\\
\beta_* &= \mathrm{LogSpec}\, U_2,\\
\delta_* &= \mathrm{LogSpec}\, U_3
\end{aligned}$$

be the associated logarithmic spectra.

Select $r, k > 0$ satisfying $r + k = n$, select $a, b, c \in \mathcal{P}_{r,k}$, and take $d \geq 0$ so that the associated quantum Littlewood–Richardson coefficient $N_{ab}^{c,d}(r,k)$ (see Figure 14, Figure 3) satisfies $N_{ab}^{c,d}(r,k) = 1$. The following inequality then holds:

$$d - \sum_{i=1}^{r} \alpha_{k+i-a_i} - \sum_{i=1}^{r} \beta_{k+i-b_i} + \sum_{i=1}^{r} \delta_{k+i-c_i} \geq 0. \quad (*)$$

We define the monodromy polytope (for $SU(n)$) to be the polytope determined by all such inequalities.

Conversely, given alcove sequences α_*, β_*, δ_* which belong to the monodromy polytope, then there must exist U_1, U_2, U_3 satisfying $U_1U_2 = U_3$ and

$$\begin{aligned}
\alpha_* &= \mathrm{LogSpec}\, U_1,\\
\beta_* &= \mathrm{LogSpec}\, U_2,\\
\delta_* &= \mathrm{LogSpec}\, U_3. \quad \square
\end{aligned}$$

r	k	a	b	c	d	$N_{ab}^{c,d}(r,k)$
1	1	(0)	(0)	(0)	0	1
		(1)	(0)	(1)	0	1
			(1)	(0)	1	1

Figure 3: Structure constants in $qH^*\mathrm{Gr}(1,1)$. There is a further symmetry relation $N_{ab}^{c,d}(r,k) = N_{ba}^{c,d}(r,k)$.

Before proceeding to use this result in any complex way, we show how it can be used to recover the contents of Example 15.[13]

Example 24 (cf. Example 15). In Figure 3, we provide a table of quantum Littlewood–Richardson coefficients relevant for $PU(2)$. Coupling these to Theorem 23 then gives the following family of inequalities:

$$\begin{aligned}
\alpha_1 + \beta_1 &\leq \delta_1, & \alpha_2 + \beta_1 &\leq \delta_2,\\
\alpha_2 + \beta_2 &\leq \delta_1 + 1, & \alpha_1 + \beta_2 &\leq \delta_2,
\end{aligned}$$

or, in terms of $\alpha_2, \beta_2, \delta_2 \geq 0$ alone,

$$\begin{aligned}
-\alpha_2 + -\beta_2 &\leq -\delta_2, & \alpha_2 + -\beta_2 &\leq \delta_2,\\
\alpha_2 + \beta_2 &\leq -\delta_2 + 1, & -\alpha_2 + \beta_2 &\leq \delta_2.
\end{aligned}$$

The resulting polytope is portrayed in Figure 4. Isolating δ_2—or, equivalently, studying a vertical ray in the Figure above a particular choice of (α_2, β_2)—yields

$$|\alpha_2 - \beta_2| \leq \delta_2 \leq \frac{1}{2} - |\alpha_2 + \beta_2 - \frac{1}{2}|.$$

A geometrical interpretation of this restriction is shown in Figure 5.

In our study of two-qubit programs, we have already announced the importance of the composite

$$\Pi\colon\ PU(4) \xrightarrow{\gamma^Q} SU(4)/C_2 \xrightarrow{\mathrm{LogSpec}} \mathfrak{A}_{C_2},$$

and we will accordingly want to employ a variant of Theorem 23 that applies to $SU(4)/C_2$.

[13] We will re-do Example 16 as part of Section 4.3.

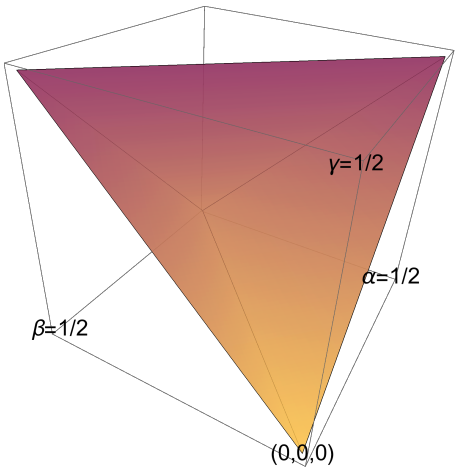


Figure 4: Full monodromy polytope for $SU(2)$, shaded along the coordinate δ.

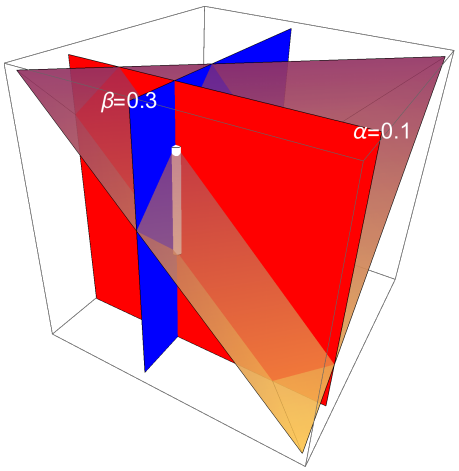


Figure 5: The polytope intersected with the planes $\alpha = 0.1$, shaded red, and $\beta = 0.3$, shaded blue, resulting in restrictions on δ, shaded white.

Corollary 25 (cf. Remark 80)**.** *Theorem 23 holds for $SU(4)/C_2$, under the condition that the indicated family of inequalities all simultaneously hold either for $\delta = \operatorname{LogSpec} U_3$ or for $\delta = \rho(\operatorname{LogSpec} U_3)$.*

Proof. If U_1, U_2, and U_3 are elements of $SU(4)$ such that $U_1 U_2 \equiv U_3$ in $SU(4)/C_2$, then there is some j so that $U_1 U_2 = (-1)^j U_3$ as elements of $SU(4)$. If j is even, then Theorem 23 applies directly to give the same statement. If j is odd, then Theorem 23 applies with U_3 replaced by $-U_3$, which has the effect of replacing δ by $\operatorname{LogSpec}(-U_3) = \rho(\operatorname{LogSpec} U_3)$. □

Additionally, not only do Theorem 23 and Corollary 25 resolve Problem 10.1, but its form is sufficiently polite that we can also bootstrap it into a solution to Problem 8.1:

Corollary 26. *Let $\mathcal{S}$ be a gate set whose image through Π is a (finite) union of convex polytopes. The image of $P_{\mathcal{S}}^n$ through Π is then also a (finite) union of convex polytopes.*

Proof. We have assumed the base case: $\Pi(P_{\mathcal{S}}^1)$ is a union of convex polytopes. Assuming that $\Pi(P_{\mathcal{S}}^{n-1})$ is a union of convex polytopes, each constituent polytope is described by a finite collection of linear inequalities. The monodromy polytope is itself also described by a finite collection of linear inequalities. Select a polytope constituent of $\Pi(P_{\mathcal{S}}^1)$ and of $\Pi(P_{\mathcal{S}}^{n-1})$. By imposing those linear inequalities describing the constituent of $\Pi(P_{\mathcal{S}}^1)$ on the first coordinate, imposing those linear inequalities describing the constituent of $\Pi(P_{\mathcal{S}}^{n-1})$ on the second coordinate, and using Fourier–Motzkin elimination to project to the final coordinate, we produce a subset of $\Pi(P_{\mathcal{S}}^n)$ which is described by a finite collection of linear inequalities. It follows that this too is a convex polytope, and the entire set $\Pi(P_{\mathcal{S}}^n)$ is the union of the convex polytopes formed in this way. □

Remark 27. For gate sets $\mathcal{S}$ of interest to us, it is often the case that $\mathcal{S}$ appears as a subset of $P_{\mathcal{S}}^2$. This condition entails the nesting properties $P_{\mathcal{S}}^n \subseteq P_{\mathcal{S}}^{n+1}$ and $\Pi(P_{\mathcal{S}}^n) \subseteq \Pi(P_{\mathcal{S}}^{n+1})$ for $n \geq 2$.

Definition 28. Recall from Definition 9 the gate set quality metric $\langle \mathcal{L}_{\mathcal{S}} \rangle^{\text{Haar}}$. By Corollary 26, we now know the sets $\Pi(P_{\mathcal{S}}^n)$ to all be unions of polytopes, which have easily calculable volumes. Inspired by this, and using the fact that $\mathcal{L}_{\mathcal{S}}$ is

constant on fibers of Π (i.e., Corollary 5), we propose the following alternative definition:

$$\begin{aligned}\langle \mathcal{L}_{\mathcal{S}} \rangle^{\mathfrak{A}_{C_2}} &= \int_{x \in \mathfrak{A}_{C_2}} \mathcal{L}_{\mathcal{S}}(\Pi^{-1}(x))\, dx \\ &= \sum_{n=0}^{\infty} n \cdot \mathrm{vol}^{\mathfrak{A}_{C_2}} \left(\Pi \left(\mathcal{L}_{\mathcal{S}}^{-1}(n) \right) \right) \\ &= \sum_{n=0}^{\infty} n \cdot \mathrm{vol}^{\mathfrak{A}_{C_2}} \left(\Pi(P_{\mathcal{S}}^n) \setminus \bigcup_{j=0}^{n-1} \Pi(P_{\mathcal{S}}^j) \right),\end{aligned}$$

where $\mathrm{vol}^{\mathfrak{A}_{C_2}}$ indicates the Euclidean volume as a subset of the polytope $\mathfrak{A}_{C_2}$, normalized so that $\mathfrak{A}_{C_2}$ itself has unit volume. These are not generally equal: their difference is mediated by the Jacobian of Π, considered as a function on the subset of canonical gates, as well as the sizes of the fibers of Π. The quantity $\langle \mathcal{L}_{\mathcal{S}} \rangle^{\mathrm{Haar}}$ has the advantage of capturing a more traditional notion of average, but $\langle \mathcal{L}_{\mathcal{S}} \rangle^{\mathfrak{A}_{C_2}}$ has the advantage of being reliably computable by finite means.

Due to their similar definitions, it is often the case that we can make claims about both quantities simultaneously. In these situations where we intend to make a statement about both, we will omit the superscript.

4 Monodromy polytope slices for the standard gates

In this section, we consider the "standard gates" that appear in the paper of Smith, Curtis, and Zeng [46, Appendix A] and their effect as members of a native gate set. Each of these gates or gate families specify via Π either a particular point in $\mathfrak{A}_{C_2}$ or a line segment in $\mathfrak{A}_{C_2}$, which in either case can be specified via a family of linear inequalities. By consequence of Remark 27, the space of programs which are accessible via circuits of native gates of a fixed depth then appears as a projection of linear slice of the monodromy polytope. Our goal is to give descriptions of these projections.

4.1 The CZ gate

The sets $\Pi(P_{\mathrm{CZ}}^0)$ and $\Pi(P_{\mathrm{CZ}}^1)$ are singletons and hence automatically convex polytopes:

$$\Pi(P_{\mathrm{CZ}}^0) = e_1, \qquad \Pi(P_{\mathrm{CZ}}^1) = e_2.$$

In order to compute $\Pi(P_{\mathrm{CZ}}^2)$, we intersect the polytope described in Theorem 23 with the six hyperplanes describing the conditions $\alpha_* = e_2$ and $\beta_* = e_2$:

Lemma 29 (cf. [43, Proposition III.3])**.** *The convex polytope $\Pi(P_{\mathrm{CZ}}^2)$ is described by*

$$\left\{ (\delta_1, \delta_2, \delta_3, \delta_4) \in \mathfrak{A}_{C_2} \;\middle|\; \begin{array}{l} \delta_1 = -\delta_4, \\ \delta_2 = -\delta_3 \end{array} \right\}.$$

The extremal points of $\Pi(P_{\mathrm{CZ}}^2)$ are $\{e_1, e_2, e_3\}$, with circuit realizations given in Figure 16.

Proof. Using the quantum Littlewood–Richardson coefficients

$$N_{(1,0)(1,0)}^{(2,0),0}(2,2) = 1, \qquad N_{(1,0)(1,0)}^{(1,1),0}(2,2) = 1$$

we apply Theorem 23 to deduce the inequalities

$$\begin{aligned} 0 - (\alpha_{2+1-1} + \alpha_{2+2-0}) - (\beta_{2+1-1} + \beta_{2+2-0}) \\ + \delta_{2+1-2} + \delta_{2+2-0} \geq 0, \\ 0 - (\alpha_{2+1-1} + \alpha_{2+2-0}) - (\beta_{2+1-1} + \beta_{2+2-0}) \\ + \delta_{2+1-1} + \delta_{2+2-1} \geq 0, \end{aligned}$$

i.e.,

$$\begin{aligned} 0 - (1/4 + -1/4) - (1/4 + -1/4) + \delta_1 + \delta_4 \geq 0, \\ 0 - (1/4 + -1/4) - (1/4 + -1/4) + \delta_2 + \delta_3 \geq 0. \end{aligned}$$

Because of the additional constraint $\delta_+ = 0$, we learn that these nonnegative quantities are in fact exactly zero:

$$\delta_1 = -\delta_4, \qquad \delta_2 = -\delta_3.$$

This plane passes through three of the extremal vertices of $\mathfrak{A}_{C_2}$, hence $\Pi(P_{\mathrm{CZ}}^2)$ is contained inside of the triangle formed as the convex hull of those three vertices. In order to show that this inclusion is actually an equality, we need only produce witnesses that these three points have preimages in P_{CZ}^2. One checks that the circuits described in Figure 16 do the job: not only do they image to the appropriate vertex under $\Pi(-)$, but the mirroring value j in Theorem 23 is not used, so that these vertices belong to the same polytope. Hence, their convex hull is as claimed. □

Remark 30. One can avoid divine inspiration by instead producing the entire family of inequalities of Theorem 23, adding the equalities coming from our selection of $\alpha_* = \beta_* = \Pi(\mathrm{CZ})$, optionally pre-reducing the system, calculating all of the points of triple intersection, and throwing

out those points which do not satisfy the original family of inequalities. This will, ultimately, produce the same set of extremal points. While this has the benefit of being mechanical, it is quite arduous—and it does not produce the realizations of the extremal points as circuits.

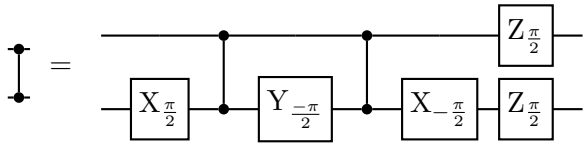
The briefest method for accessing P^3_{CZ} follows along identical lines: if we can show that the extremal vertices of $\mathfrak{A}_{C_2}$ have realizations within $\Pi(P^3_{\mathrm{CZ}})$ and we are allowed to apply convexity, then we can conclude the following equality:

Lemma 31 (cf. [45, Section V])**.** $\Pi(P^3_{\mathrm{CZ}}) = \mathfrak{A}_{C_2}$, *with circuits realizing the extremal points given in Figure 17.*

Proof. It is automatic that we have $\Pi(P^3_{\mathrm{CZ}}) \subseteq \mathfrak{A}_{C_2}$. In order to show the opposite inclusion, we need to supply the necessary realizations (with the necessary mirroring property, as in the proof of Lemma 29). One may check directly that the circuits above will do. □

Remark 32. There is also the following alternative approach that mimics the alternative approach to P^2_{CZ}. By intersecting the full polytope described by Theorem 23 with the family of inequalities which constrain $\alpha_* \in \Pi(P^2_{\mathrm{CZ}})$ and with the equality which constrains $\beta_* = \Pi(\mathrm{CZ})$, we arrive at a convex polytope contained in $\mathfrak{A}_{C_2} \times * \times \mathfrak{A}_{C_2}$. Using Fourier–Motzkin elimination to delete the first factor yields $\Pi(P^3_{\mathrm{CZ}})$ by projection to the last factor. This, too, is completely mechanical but is even more arduous.

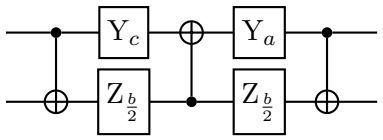
Remark 33. In order to explain the provenance of the first three circuits in the Lemma statement, we remark that Lemma 29 shows that $\mathrm{CZ} \in P^2_{\mathrm{CZ}}$, and hence we are led to the method suggested by Remark 27. Beginning with the realization of the extremal vertex $e_2 \in \Pi(P^2_{\mathrm{CZ}})$, we need only solve for the outer local gates to realize CZ exactly, as in:



Using this formula, we may inflate the other realizations of the extremal vertices of $\Pi(P^2_{\mathrm{CZ}})$ into realizations in $\Pi(P^3_{\mathrm{CZ}})$ by substituting the above circuit for CZ in for, say, the left-hand CZ supplied in Lemma 29. The realization supplied for the fourth extremal vertex is a rephrasing of the usual expression of SWAP as a triple of alternating CNOTs, and the fifth we produced by numerical search.

Remark 34 ([45, Proposition V.1]). Critically for quantum compilation, a circuit realization for any point within $\Pi(P^3_{\mathrm{CZ}})$ can be exactly produced algorithmically. The circuit proposed by Shende, Markov, and Bullock is

$\mathrm{CAN}(\alpha, \beta, \delta) =$



,

where a, b, and c are certain linear functions of α, β, and δ. In general, exact decompositions do not seem to exist (cf. Remark 62 for a basic such result), and even numerical methods pose a challenge (cf. Section 7).

Corollary 35 (cf. [43])**.** *The expected circuit depth for* CZ *is* $\langle \mathcal{L}_{\mathrm{CZ}} \rangle = 3$. □

4.2 The iSWAP gate

Now we prove analogous results for the gate set $S = \{i\mathrm{SWAP}\}$. We will be briefer in the aspects that exactly mimic those for the gate CZ.

The sets $\Pi(P^0_{i\mathrm{SWAP}})$ and $\Pi(P^1_{i\mathrm{SWAP}})$ are again singletons:

$$\Pi(P^0_{i\mathrm{SWAP}}) = e_1, \qquad \Pi(P^1_{i\mathrm{SWAP}}) = e_3.$$

Lemma 36. $\Pi(P^2_{i\mathrm{SWAP}})$ *is described by*

$$\Pi(P^2_{i\mathrm{SWAP}}) = \left\{ \delta_* \in \mathfrak{A}_{C_2} \;\middle|\; \begin{array}{l} \delta_1 = -\delta_4, \\ \delta_2 = -\delta_3 \end{array} \right\}.$$

The extremal points of $\Pi(P^2_{i\mathrm{SWAP}})$ *are* $\{e_1, e_2, e_3\}$, *with circuit realizations given as in Figure 18.*

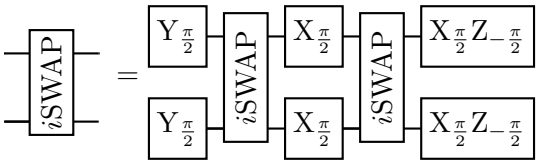
Proof. This proof entirely mimics that of Lemma 29, but this time the relevant quantum Littlewood–Richardson coefficients are

$$N^{(2,0),0}_{(0,0)(2,0)}(2,2) = 1, \quad N^{(1,1),0}_{(1,0)(2,1)}(2,2) = 1. \ \square$$

Moving on to $P^3_{i\mathrm{SWAP}}$, we have

Lemma 37. $\Pi(P^3_{i\mathrm{SWAP}}) = \mathfrak{A}_{C_2}$, *with realizations of the extremal vertices as circuits given in Figure 19.*

Proof. Again, the proof is almost identical to that of Lemma 31, beginning with an exact realization of $i\mathrm{SWAP} \in P^2_{i\mathrm{SWAP}}$ by solving for the outer local gates in the realization of $e_3 \in \Pi(P^2_{i\mathrm{SWAP}})$:



Using this, we can inflate the left-hand iSWAP in the realizations of the extremal vertices in Lemma 36 to produce realizations of those same vertices in $\Pi(P^3_{i\mathrm{SWAP}})$. What remains is to produce realizations of the extremal points SWAP and $\sqrt{\mathrm{SWAP}}$, where we rely on a standard decomposition. □

Remark 38. Combining the results above with those from the previous subsection, we conclude

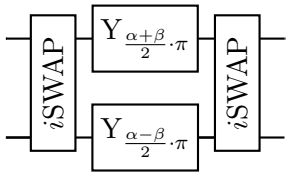
$$P^2_{\mathrm{CZ}} = P^2_{i\mathrm{SWAP}}, \qquad P^3_{\mathrm{CZ}} = P^3_{i\mathrm{SWAP}}.$$

Corollary 39. *The expected circuit depth for* iSWAP *is* $\langle \mathcal{L}_{i\mathrm{SWAP}} \rangle = 3$. □

As in the case of CZ, the compilation problem for iSWAP (i.e., Problem 10.2 and its depth-three variant) admits exact solutions. This does not appear to be in the literature, and so we include an analysis here:

Corollary 40. *For* $1/2 \geq \alpha \geq \beta \geq 0$*, the operator*

$$U(\alpha, \beta) =$$



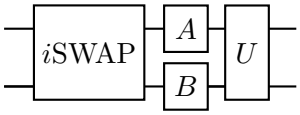
satisfies

$$\Pi(U(\alpha, \beta)) = (-\alpha, -\beta, \beta, \alpha).$$

Proof. This is checked by direct computation. One may ease the computation somewhat by noticing that conjugation by $\mathrm{X}_{\frac{\pi}{2}} \otimes \mathrm{X}_{\frac{\pi}{2}}$ diagonalizes the operator. □

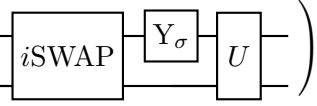
Remark 41 (cf. [43, Proposition V.2]). Our strategy for algorithmically producing circuits for points in $P^3_{i\mathrm{SWAP}}$ will be to isolate the troublesome extremal vertex e_4. Once this vertex does not contribute to the remaining convex linear combination, the remainder is solved by Corollary 40. Selecting a gate $U \in PU(4)$, we seek local gates A and B so that

$$V(U, A, B) :=$$



satisfies $\Pi(V(U, A, B)) \in \Pi(P^2_{i\mathrm{SWAP}})$. We apply Lemma 36 to see that this is accomplished by finding values of A and B so that $\operatorname{tr} \gamma^Q (V(U, A, B))$ is real. It turns out that we may take $A = \mathrm{Y}_\sigma$ and $B = 1$, which we see by manual calculation:

$$-\frac{1}{2} \operatorname{tr} \gamma^Q \left(\quad \right)$$



$$= \left(\sum_{j=1}^{4} U_{2j} U_{3(j+(-1)^j)} - \sum_{k=1}^{4} U_{4k} U_{1(k+(-1)^k)} \right) \cos\sigma + \left(\sum_{j=1}^{2} \sum_{k=1}^{4} U_{(2j)k} U_{(2j+1)(k-2)} (-1)^{(j-1)+k} \right) \sin\sigma,$$

where we have interpreted the indices modulo 4. In particular, this summation formula enables us to solve the equation

$$\operatorname{Im}\left(\operatorname{tr} \gamma^Q \left(V(U, \sigma) \right) \right) = 0$$

by picking a value of σ so that $\tan\sigma$ agrees with

$$\frac{-\operatorname{Im}\left(\sum_j U_{2j} U_{3(j+(-1)^j)} - \sum_k U_{4k} U_{1(k+(-1)^k)} \right)}{\operatorname{Im}\left(\sum_{j=1}^{2} \sum_k U_{(2j)k} U_{(2j+1)(k-2)} (-1)^{(j-1)+k} \right)}.$$

Because the tangent function is surjective, there is always such a value.

As one remaining case of interest, we can also describe the collection of gates accessible to a gate set that has *both* CZ and iSWAP available:

Lemma 42. *The set* $\Pi(P^2_{i\mathrm{SWAP},\mathrm{CZ}})$ *is the union of* $\Pi(P^2_{i\mathrm{SWAP}})$ *and the convex polytope*

$$\left\{ \delta_* = (\delta_1, \delta_2, \delta_3, \delta_4) \in \mathfrak{A}_{C_2} \;\middle|\; \begin{array}{c} \delta_4 = 1/2 - \delta_3, \\ \delta_1 = -1/2 - \delta_2 \end{array} \right\},$$

which has extremal vertices $\{e_2, e_3, e_4\}$. □

Corollary 43. *The expected depth for the gate set with* CZ *and* iSWAP *is* $\langle \mathcal{L}_{\mathrm{CZ},i\mathrm{SWAP}} \rangle = 3$. □

Remark 44. The metrics $\langle \mathcal{L}_{\mathcal{S}} \rangle$ capture the efficacy of $\mathcal{S}$ at encoding *random* two-qubit programs, but programs appearing "in the wild" (as

well as sub-programs appearing as components in decompositions) are not random: the program SWAP $\in PU(4)$ is a prime example of an uncommonly important two-qubit interaction. Although the equation

$$\langle \mathcal{L}_{\mathrm{CZ}} \rangle = \langle \mathcal{L}_{i\mathrm{SWAP}} \rangle = \langle \mathcal{L}_{\mathrm{CZ},i\mathrm{SWAP}} \rangle$$

indicates that there is no salient difference between these different gate sets from the perspective of random programs,

$$\mathrm{SWAP} \in P^2_{\mathrm{CZ},i\mathrm{SWAP}} \setminus P^2_{\mathrm{CZ}}$$

indicates that there is an important difference from the perspective of structured programs.

This gate set also admits algorithmic decomposition, which one may verify by direct calculation:

Lemma 45. *For a point*

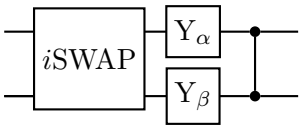
$$\delta_* \in \Pi(P^2_{i\mathrm{SWAP},\mathrm{CZ}}) \setminus \Pi(P^2_{i\mathrm{SWAP}}),$$

there are two entries satisfying

$$-1/4 \leq \delta_i \leq \delta_j \leq 1/4.$$

Setting $\alpha = (\delta_i + \delta_j)\pi$ *and* $\beta = (\delta_i - \delta_j)\pi$*, we then have*

$$\delta_* = \Pi \left(\begin{array}{c} \\ \\ \end{array} \right.$$



$$\left. \begin{array}{c} \\ \\ \end{array} \right) . \qquad \square$$

4.3 The CPHASE and PSWAP gate families

As further demonstration of these techniques, we also consider some combinations of the parametric two-qubit gates which appear in the Quil standard gate set [46].

Lemma 46. *The convex polytope* $\Pi(P^2_{\mathrm{CPHASE}})$ *agrees with* $\Pi(P^2_{\mathrm{CZ}})$ *and with* $\Pi(P^2_{i\mathrm{SWAP}})$.

Proof. The proof is identical to that given for Lemma 29: the same quantum Littlewood–Richardson coefficients impose the same symmetry relation on $\Pi(P^2_{\mathrm{CPHASE}})$, and the reverse inclusion then follows from $P^2_{\mathrm{CZ}} \subseteq P^2_{\mathrm{CPHASE}}$. $\square$

Corollary 47. *The expected circuit depth for* CPHASE *is* $\langle \mathcal{L}_{\mathrm{CPHASE}} \rangle = 3$. $\square$

Similarly, there is no substantial gain from mixing CPHASE with *i*SWAP over CZ with *i*SWAP.

Lemma 48. $P^2_{\mathrm{CZ},i\mathrm{SWAP}} = P^2_{\mathrm{CPHASE},i\mathrm{SWAP}}$*, and* $\langle \mathcal{L}_{\mathrm{CPHASE},i\mathrm{SWAP}} \rangle = 3$. $\square$

Example 49. As an exercise in the application of these methods, we provide an analysis of the polytopes associated to $\sqrt{\mathrm{CZ}} = \mathrm{CPHASE}_{\frac{\pi}{2}}$. Since $\sqrt{\mathrm{CZ}} \cdot \sqrt{\mathrm{CZ}} = \mathrm{CZ}$, we can deduce immediately from Corollary 35 (i.e., from previously known methods) that $\langle \mathcal{L}_{\sqrt{\mathrm{CZ}}} \rangle \leq 6$. Coupling our methods to the software `lrs` [4, 5], we enumerate the vertices of the sets $\Pi(P^n_{\sqrt{\mathrm{CZ}}})$ for $n \leq 5$ in Figure 20, as displayed in graphical form in Figure 6. These yield the exact calculation

$$\langle \mathcal{L}_{\sqrt{\mathrm{CZ}}} \rangle^{\mathfrak{A}_{C_2}} = 3 \cdot \frac{1}{2} + 4 \cdot \frac{19}{48} + 5 \cdot \frac{5}{48} = 3.6041\overline{6},$$

a considerable improvement over the naive estimate.

The gate PSWAP is not natively available on charge-coupled superconducting hardware, so we do not explore it very thoroughly here, but for completeness we at least include a calculation of P^2_{PSWAP}.

Lemma 50. P^2_{PSWAP} *agrees with the other depth-two sets studied so far:*

$$P^2_{\mathrm{PSWAP}} = P^2_{\mathrm{CZ}} = P^2_{i\mathrm{SWAP}} = P^2_{\mathrm{CPHASE}}.$$

Proof. This proof proceeds similarly to that of Lemma 36. This time the relevant quantum Littlewood–Richardson coefficients are

$$N^{(2,0),1}_{(2,1)(2,1)}(2,2) = 1, \qquad N^{(1,1),1}_{(2,1)(2,1)}(2,2) = 1,$$

and $\Pi(\mathrm{PSWAP}_{2\pi t})$ is calculated to be

$$\left(-\frac{1}{4} - \frac{t}{2}, -\frac{1}{4} + \frac{t}{2}, -\frac{1}{4} + \frac{t}{2}, \frac{3}{4} - \frac{t}{2} \right).$$

An application of Theorem 23 yields inequalities which enforce the same symmetry conditions on $\Pi(P^2_{\mathrm{PSWAP}})$ as in the previous Lemmas. Because we have $P^2_{i\mathrm{SWAP}} \subseteq P^2_{\mathrm{PSWAP}}$, we may conclude equality. $\square$

Corollary 51. *The expected circuit depth for* PSWAP *is* $\langle \mathcal{L}_{\mathrm{PSWAP}} \rangle = 3$. $\square$

5 Monodromy polytope slices for the XY–family

Combining the ideas which motivated *i*SWAP and CPHASE, we are also motivated to con-

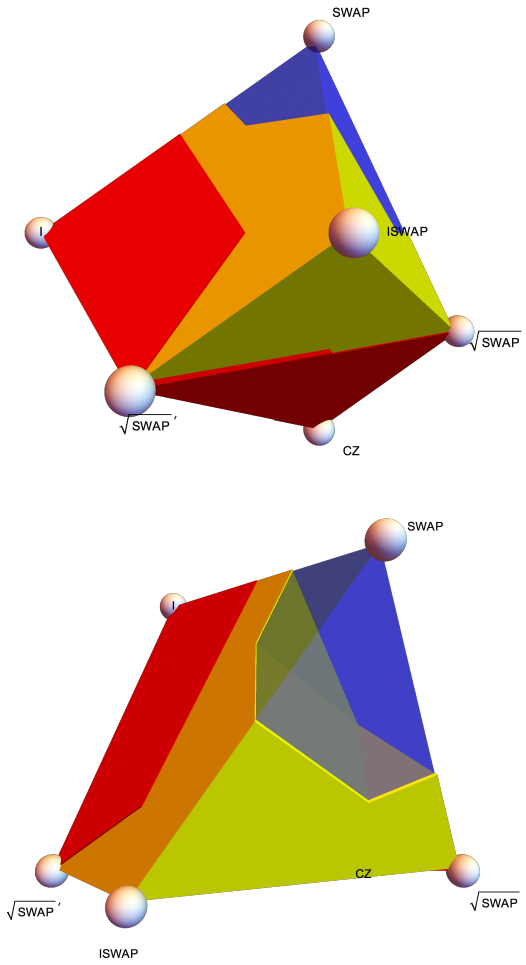


Figure 6: The regions $\Pi(P^n_{\sqrt{\mathrm{CZ}}})$ within $\mathfrak{A}_{C_2}$: red denotes $P^3_{\sqrt{\mathrm{CZ}}}$, yellow denotes $P^4_{\sqrt{\mathrm{CZ}}}$, and blue denotes $P^5_{\sqrt{\mathrm{CZ}}}$. Not pictured are $P^0_{\sqrt{\mathrm{CZ}}}$ and $P^1_{\sqrt{\mathrm{CZ}}}$, each a point, and $P^2_{\sqrt{\mathrm{CZ}}}$, a flat triangle.

sider the one-parameter family of native two-qubit gates given by

$$\begin{aligned}\mathrm{XY}_\alpha &= \exp\left(-i\alpha\cdot(\sigma_X^{\otimes 2}+\sigma_Y^{\otimes 2})\right)\\ &= \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & \cos(\alpha/2) & -i\sin(\alpha/2) & 0\\ 0 & -i\sin(\alpha/2) & \cos(\alpha/2) & 0\\ 0 & 0 & 0 & 1\end{pmatrix}.\end{aligned}$$

This family is interesting for a few reasons: it is one of the only[14] remaining "edges" of $\mathfrak{A}$; it can arise naturally as a gate natively available to systems where iSWAP is available, as in [10]; and it itself belongs to the canonical family.

Having noted that XY_α belongs to the canonical family, we may compute its associated diagonal coordinates to be

$$\begin{aligned}\mathrm{XY}^Q_\alpha &= \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & e^{i\alpha/2} & 0 & 0\\ 0 & 0 & e^{-i\alpha/2} & 0\\ 0 & 0 & 0 & 1\end{pmatrix},\\ \Pi(\mathrm{XY}_\alpha) &= \left(-\frac{\alpha}{2\pi}, 0, 0, \frac{\alpha}{2\pi}\right).\end{aligned}$$

In pursuit of an analogue of the results of Section 4.3, we can perform an analysis of the polytope $\Pi(P^2_{\mathrm{XY}})$. The computation is much more involved, but we are rewarded with the following theorem:

Theorem 52. *The set $\Pi(P^2_{\mathrm{XY}})$ is the union of the polytopes with extremal coordinates as specified in Figure 21. The set $\Pi(P^3_{\mathrm{XY}})$ is the entire solid $\mathfrak{A}_{C_2}$.*

Proof. We compute along the lines of Remark 30: we intersect the monodromy polytope with the hyperplane equations specifying that the first coordinate take the form $(\alpha_1, 0, 0, -\alpha_1)$ and that the second coordinate take the form $(\beta_1, 0, 0, -\beta_1)$; then we apply Fourier-Motzkin elimination to project to the third coordinate; and finally we feed the resulting system to the software package `lrc` [4, 5]. Altogether, this results in the vertex sets listed above. □

[14] The other remaining edge is the ray connecting I to SWAP, but we addressed this in Example 16.

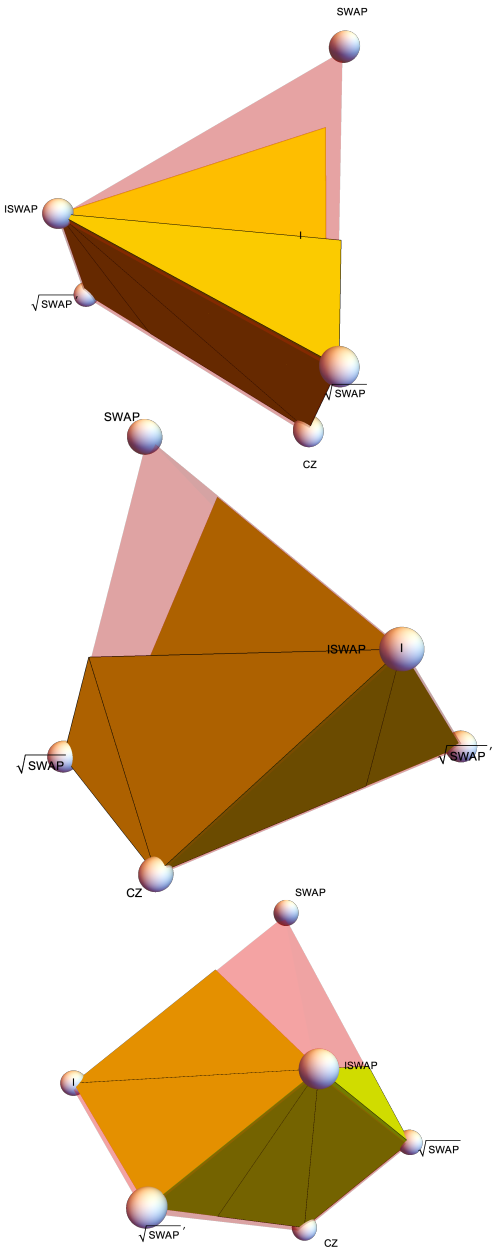


Figure 7: Three views of $\Pi(P^2_{\mathrm{XY}})$

Corollary 53. *In particular,* $\Pi(P^2_{\mathrm{XY}})$ *is of positive volume. More precisely, we compute the expected gate depth for* XY *to be*[15]

$$\langle \mathcal{L}_{\mathrm{XY}} \rangle^{\mathfrak{A}_{C_2}} = 2 \cdot \frac{5}{6} + 3 \cdot \frac{1}{6} = \frac{13}{6}. \quad \square$$

Remark 54. As an interesting aside, SWAP lies outside of this polytope.

Our main observation is that XY enjoys a property that none of the other gate sets have thus far: P^2_{XY} is top-dimensional or, said otherwise, has positive volume. In the CPHASE family, we found in Lemma 46 that P^2_{CPHASE} had zero volume, from which we can also conclude that $P^2_{\mathrm{CPHASE}_\alpha}$ has zero volume for every fixed of α, including $\mathrm{CPHASE}_\pi = \mathrm{CZ}$ (cf. Lemma 29). We here pursue the corresponding question of whether there are any fixed values of α for which $P^2_{\mathrm{XY}_\alpha}$ has nonzero volume.[16] In the event that such slices exist, we can ask an additional question: which particular values of α maximize the volume of the slice?

Fix $0 \leq \alpha < \pi$ with corresponding value $t = \alpha/\pi$ satisfying $0 \leq t \leq 1$. The fundamental alcove sequences under consideration are then

$$\begin{aligned} \alpha_* &= (-t/2, 0, 0, t/2), \\ \beta_* &= (-t/2, 0, 0, t/2), \\ \delta_* &= (\delta_1 \leq \delta_2 \leq \delta_3 \leq \delta_4), \end{aligned}$$

and the inequalities given by combining Theorem 23 with Figure 14 and the above alcove sequences are

$$\begin{aligned} \delta_1 + t &\geq 0, & \delta_1 + \delta_2 + t &\geq 0, \\ -\delta_4 + t &\geq 0, & \delta_2 + t/2 &\geq 0, \\ \delta_1 + \delta_4 + t/2 &\geq 0, & -\delta_3 + t/2 &\geq 0, \\ \delta_3 &\geq 0, & \delta_1 + \delta_4 - t &\geq -1, \\ -\delta_2 &\geq 0, & \delta_1 - t/2 &\geq -1, \\ \delta_2 + \delta_3 - t &\geq -1, & -\delta_4 - t/2 &\geq -1. \end{aligned}$$

From these inequalities, we may draw the following consequence:

[15] As mentioned in Section 1, we can approximate $\mathrm{vol}^{\mathrm{Haar}}(P^2_{\mathrm{XY}})$ to be ≈ 0.96, which is quite different from 5/6. The skew in these two values comes from the commentary in Definition 28: the remaining sixth of $\mathfrak{A}_{C_2}$ is underdense for $\Pi_* \mu^{\mathrm{Haar}}$.

[16] Of course, this is not automatically true: these subpolytopes could form something like a "foliation" of $\Pi(P^2_{\mathrm{XY}})$.

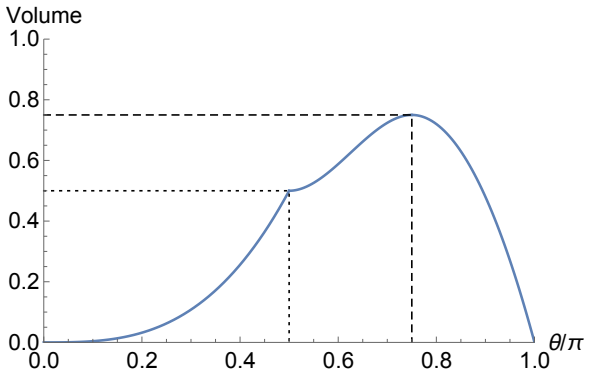


Figure 8: Volume of $\Pi(P^2_{\mathrm{XY}_\alpha})$, plotted as a fraction of the volume of $\mathfrak{A}_{C_2}$ against α/π.

Theorem 55. *The volume of* $\Pi(P^2_{\mathrm{XY}_\alpha})$ *is maximized at* $\alpha = 3\pi/4$.

Proof. Because the finite family of inequalities determining $\Pi(P^2_{\mathrm{XY}_\alpha})$ are linearly dependent in α, the curve $\operatorname{vol}\Pi(P^2_{\mathrm{XY}_\alpha})$ is piecewise cubic in α. One can use this fact, together with sampling [32] and interpolation techniques, to determine a formula for $\operatorname{vol}\Pi(P^2_{\mathrm{XY}_\alpha})$:

$$\operatorname{vol}\Pi(P^2_{\mathrm{XY}_\alpha}) = \begin{cases} 4t^3 & 0 \le t \le \frac{1}{2}, \\ \frac{15}{2} - 36t + 60t^2 - 32t^3 & \frac{1}{2} \le t \le \frac{3}{4}, \\ -6 + 18t - 12t^2 & \frac{3}{4} \le t \le 1, \end{cases}$$

as depicted in Figure 8. From this curve, we may directly determine its maximum value. □

Definition 56. Motivated by Theorem 55, we also refer to $\mathrm{XY}_{\frac{3\pi}{4}}$ by the briefer synonym DB.[17]

Remark 57. Similarly, one may compute $\Pi(P^3_{\mathrm{DB}}) = \mathfrak{A}_{C_2}$, from which we conclude

$$\langle \mathcal{L}_{\mathrm{DB}} \rangle^{\mathfrak{A}_{C_2}} = 2 \cdot \frac{3}{4} + 3 \cdot \frac{1}{4} = \frac{9}{4}.$$

In fact, $\Pi(P^2_{\mathrm{XY}_{\pi/2}}) \cup \Pi(P^3_{\mathrm{XY}_{\pi/2}}) = \mathfrak{A}_{C_2}$, so that

$$\langle \mathcal{L}_{\mathrm{XY}_{\pi/2}} \rangle^{\mathfrak{A}_{C_2}} = 2 \cdot \frac{1}{2} + 3 \cdot \frac{1}{2} = \frac{5}{2}.$$

Remark 58. In Figure 9, Figure 10, and Figure 11, we illustrate the solids $\Pi(P^2_{\mathrm{XY}_\alpha})$ for varying values of α, where we have projected onto the last three coordinates and shaded $\mathfrak{A}_{C_2}$ red. We record here (but do not prove) some interesting observations about the solids. First, for

[17] Dagwood Bumstead is a comic strip character famous for making really big sandwiches.

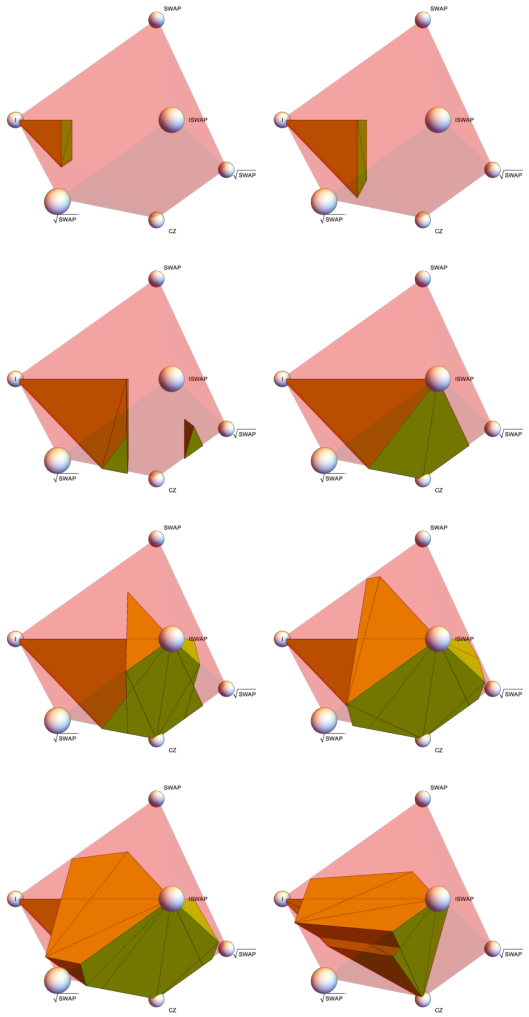


Figure 9: The solids $\Pi(P^2_{\mathrm{XY}_{\pi t}})$ for differing values of t: $2/10, 3/10, \ldots, 9/10$.

$0 \le \alpha \le \alpha' \le 3\pi/4$, there is an inclusion of solids $\Pi(P^2_{\mathrm{XY}_\alpha}) \subseteq \Pi(P^2_{\mathrm{XY}_{\alpha'}})$, from which it follows that $\operatorname{vol}\Pi(P^2_{\mathrm{DB}}) \ge \operatorname{vol}\Pi(P^2_{\mathrm{XY}_\alpha})$ for any $0 \le \alpha \le 3\pi/4$ as in the Theorem. However, for $3\pi/4 \le \alpha < \alpha' \le \pi$, neither of $\Pi(P^2_{\mathrm{XY}_\alpha})$ and $\Pi(P^2_{\mathrm{XY}_{\alpha'}})$ is contained in the other: although $\Pi(P^2_{\mathrm{XY}_\alpha})$ continues to lose volume as α approaches π from the left, the solid also continues to pick up "new" two-qubit programs as it shrinks.

It is then of further interest to give a precise description of the polytope $\Pi(P^2_{\mathrm{DB}})$.

Lemma 59. $\Pi(P^2_{\mathrm{DB}})$ *is a union of two convex polytopes, respectively described the following two families of inequalities:*

$$\left\{ \delta_3 \ge 0, \;\; \frac{1}{4} \ge |\delta_2 + \delta_3|, \;\; 0 \ge \delta_2 \right\},$$

$$\left\{ \frac{1}{2} \ge \delta_2 + \delta_3 + \delta_4, \;\; -\frac{1}{4} + \delta_3 + \delta_4 \ge 0, \right.$$

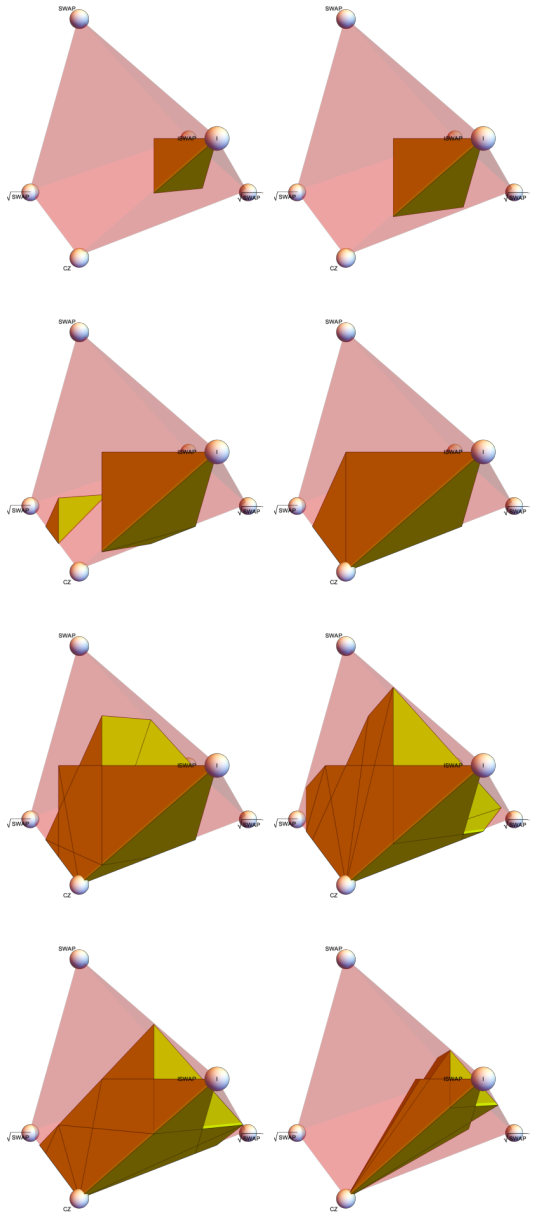


Figure 10: The solids $\Pi(P^2_{\mathrm{XY}_{\pi t}})$, as shown from a second perspective, for differing values of t: $2/10$, $3/10$, $\ldots$, $9/10$.

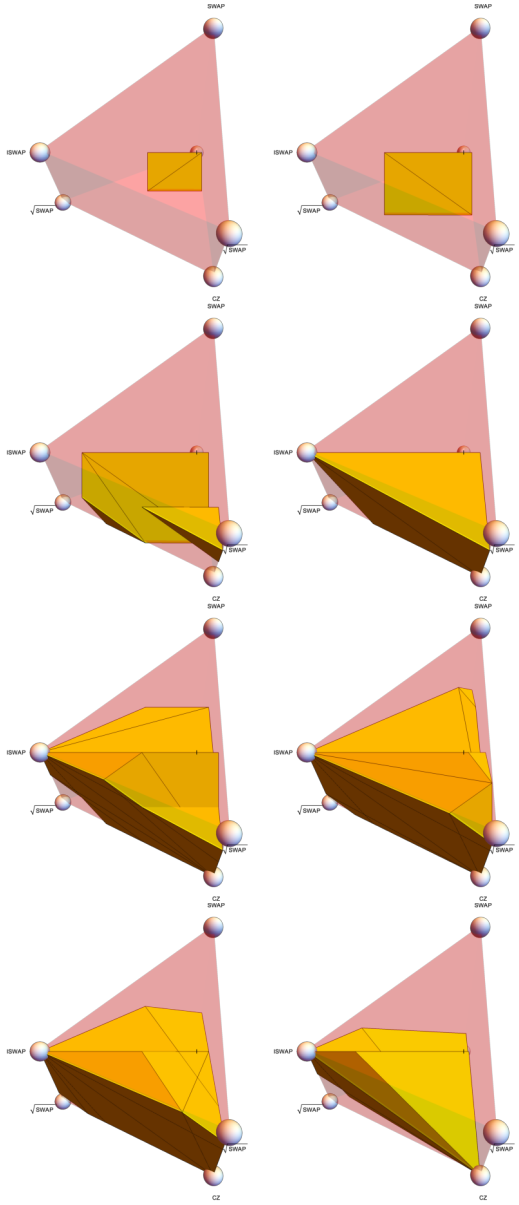


Figure 11: The solids $\Pi(P^2_{\mathrm{XY}_{\pi t}})$, as shown from a third perspective, for differing values of t: $2/10$, $3/10$, $\ldots$, $9/10$.

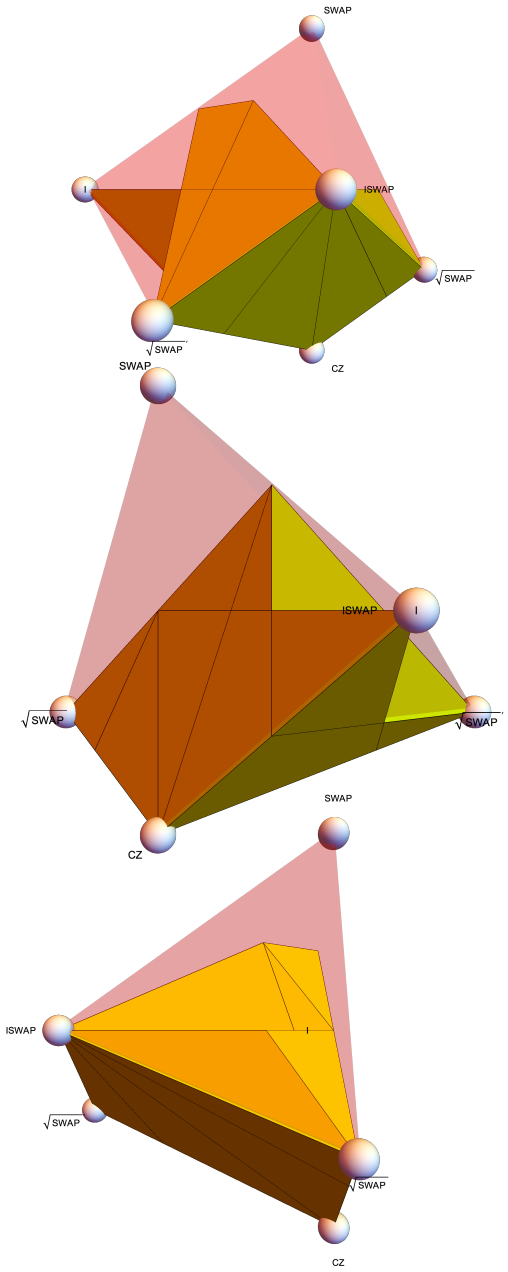


Figure 12: Three views of $\Pi(P^2_{\mathrm{DB}})$

$$\frac{1}{4} \geq |\delta_2 + \delta_3| \Big\}$$

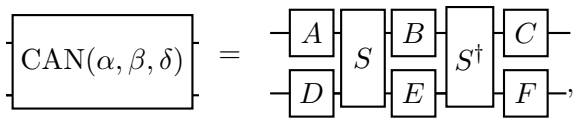
intersected with the fundamental alcove. The extremal points can be found in Figure 22.

Proof. Here we follow the method espoused by Remark 30. The family of inequalities comes directly from reducing the family supplied by Theorem 23. After calculating all of the points of intersection of the associated equalities and discarding those intersection points which do not satisfy all of the inequalities, the remainder is the set of extremal vertices, as listed above. □

Remark 60. The polytope $\Pi(P^2_{\mathrm{DB}})$ is pictured from three angles in Figure 12.

Remark 61. For the interested reader, we also include as Figure 13 a depiction a numerical sampling of $\operatorname{vol}\Pi(P^2_X)$ as X ranges over (the facets of) the entire monodromy polytope. Points shaded black correspond to those values of X for which $\operatorname{vol}\Pi(P^2_X)$ is at 0% of the total volume, and points shaded white correspond to 100% of the total volume. In the middle figure, the heat values along the line connecting the westernmost point, labeled I, to the center point, labeled iSWAP, correspond to the graph depicted in Figure 8.

Remark 62. In the course of our analysis of $\langle \mathcal{L}_{\mathrm{XY}} \rangle^{\mathfrak{A}_{C_2}}$, we have avoided giving an effective compilation routine for P^2_{XY} along the lines of Remark 34 for P^3_{CZ}. Indeed, one can show under mild hypotheses that such a formula cannot exist. The canonical family forms a 3–dimensional maximal torus in $PU(4)$, but the maximal tori in $PU(2)^{\otimes 2}$ are merely 2–dimensional. It is therefore impossible for any gate $S \in PU(4)$ to conjugate a family of local gates onto the canonical family. If $S^\dagger$ is additionally locally equivalent to S, then this means that any analogue of Remark 34 for P^2_S must instead be of the form



where the outer gates A, C, D, and F are *not all constant* in the parameters α, β, δ. In practice, it seems that B and E cannot be made linearly dependent on the canonical parameters either, though we do not presently have a proof of this to offer.

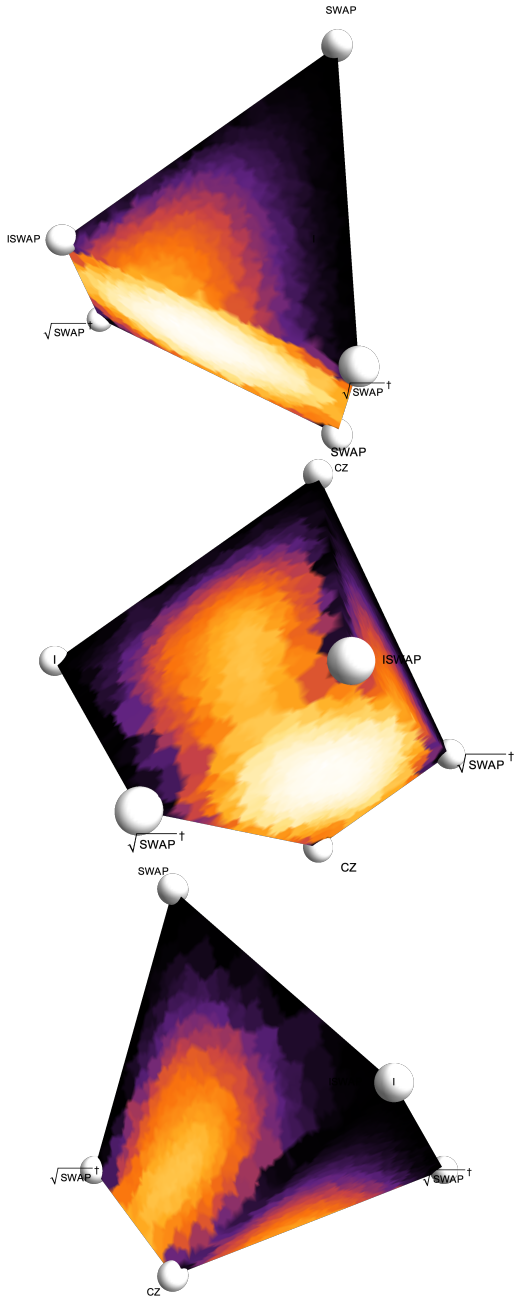


Figure 13: An approximate heat map of volumes of symmetric monodromy polytope slices. The vertices of the figures are labeled I, CZ, iSWAP, SWAP, and $\sqrt{\text{SWAP}}$. A gate U is shaded according to the volume of $\Pi(P_U^2)$: black is 0% of the total volume of $\mathfrak{A}_{C_2}$, and white is 100%.

6 Approximate compilation

We now use the above descriptions of the polytopes $\Pi(P_{\mathcal{S}}^n)$ to address the problem of *approximate compilation*:

Problem 63. Given a two-qubit program U and a gate set $\mathcal{S}$ whose members $S \in \mathcal{S}$ have associated fidelity estimates f_S, what circuit drawn from $\mathcal{S}$ gives the greatest fidelity approximation to U?

For instance, in this specific setting of $\mathcal{S} = \{\text{CZ}\}$, Lemma 31 shows that every such U can be written as a circuit involving three applications of CZ, whereas Lemma 29 shows that almost no U can be decomposed exactly using just two applications of CZ. Nonetheless, if there is an associated cost to each application of CZ, it may be preferable to deliberately "miss" U (and thereby incur deliberate error) if it affords an opportunity to avoid applying CZ a third time (and thereby avoid indeliberate error). This idea of approximate compilation is not a new one [11, Appendix B], and we begin by recalling some useful results.

Definition 64 ([38], see also [39])**.** Given a pair of two-qubit programs G and G', we define their *average gate fidelity* to be

$$\begin{aligned} F_{\text{avg}}(G, G') &= \int_{\psi \in \mathbb{P}(V)} |\langle \psi | G^\dagger G' | \psi \rangle|^2 \\ &= \frac{4 + |\operatorname{tr}(G^\dagger G')|^2}{4 \cdot 5} \in [1/5, 1]. \end{aligned}$$

Because this comes down to a trace calculation, this value is especially easy to calculate for simultaneously diagonalizable gates, which includes pairs of canonical gates after conjugation by Q:

Lemma 65 ([11, Equation B.8d])**.** *Let* $G = \text{CAN}(\alpha, \beta, \delta)$ *and* $G' = \text{CAN}(\alpha', \beta', \delta')$ *be two canonical gates with parameter differences*

$$\Delta_\alpha = \frac{\alpha' - \alpha}{2}, \quad \Delta_\beta = \frac{\beta' - \beta}{2}, \quad \Delta_\delta = \frac{\delta' - \delta}{2}.$$

Their average gate fidelity is given by

$$20 F_{\text{avg}}(G, G') = 4 + 16 \left| \begin{array}{c} \cos \Delta_\alpha \cos \Delta_\beta \cos \Delta_\delta \\ + \\ i \sin \Delta_\alpha \sin \Delta_\beta \sin \Delta_\delta \end{array} \right|.$$

□

In pursuit of Problem 63, we are also interested in the effect of local gates on Lemma 65. Rewriting the trace in terms of Q–conjugates, we have

$$\begin{aligned} |\operatorname{tr} G^\dagger G'|^2 &= |\operatorname{tr} L_2^\dagger C^\dagger L_1^\dagger \cdot L_1' C' L_2'|^2 \\ &= |\operatorname{tr} D_1 O_1 D_2 O_2|^2, \end{aligned}$$

where $D_1 = (C^\dagger)^Q$ and $D_2 = (C')^Q$ are diagonal gates and $O_1 = (L_1^\dagger L_1')^Q$ and $O_2 = (L_2' L_2^\dagger)^Q$ are orthogonal gates. Letting L_2 and L_2' range, we see from Corollary 14 that we are maximizing a quadratic functional over the monodromy polytope slice associated to D_1 and D_2. Mercifully, one need not employ this heavy machinery to solve this optimization problem:

Lemma 66 ([47, Section III.A])**.** *Suppose that C_1, C_2 are fixed canonical gates and that L_1, L_1' are fixed local gates. Letting L_2 and L_2' range over all local gates, the value $F_{\text{avg}}(L_1 C_1 L_1', L_2 C_2 L_2')$ is maximized when taking $L_2 = L_1$ and $L_2' = L_1'$.* □

Corollary 67. *The spectrum of the gate which gives the best approximation to a two-qubit unitary U depends only on $\Pi(U)$.* □

By combining these results to our descriptions of $\Pi(P_{\mathcal{S}}^n)$ for our preferred gate sets $\mathcal{S}$, we produce the following protocol for approximate compilation. In the following, we take $\mathcal{S}$ to be a gate-set with the nesting property of Remark 27 and U to be a two-qubit program to be compiled.

1. Calculate the canonical decomposition associated to U: $U = LCL'$.
2. Let $n = 1$.
3. Use $\Pi(U)$ to calculate the point $\delta_*^n \in \Pi(P_{\mathcal{S}}^n)$ which maximizes $F_{\text{avg}}(U, -)$. Multiply this maximum value by f_S^n.[18]
4. Is this fidelity value smaller than the previous fidelity value? If not, increment n and try Step 3 again. Otherwise, proceed to Step 5.
5. Find a realization R of δ_*^{n-1} with canonical decomposition
$$R = L_{\text{approx}} \cdot C_{\text{approx}} \cdot L'_{\text{approx}}.$$
6. Return
$$L L_{\text{approx}}^\dagger \cdot R \cdot (L'_{\text{approx}})^\dagger L'.$$

[18] We are using f_S^n as an *approximation* for the fidelity of the depth n circuit. However, as fidelity is not multiplicative, there is considerable room for the implementer to express their own preference here.

The first half of the protocol depends only on the structure of the polytopes $\Pi(P_{\mathcal{S}}^n)$, from which we may conclude the following result:

Corollary 68. *The two-qubit gate sets* {CZ}*,* {iSWAP}*,* {CPHASE}*, and* {PSWAP} *all do an equally effective job of approximating an arbitrary two-qubit program by a circuit with a pair of two-qubit gates.*

Proof. This is a direct consequence of coupling the above ideas to Lemma 50. □

Remark 69 ([11, Appendix B])*.* Finding the nearest point in $P_{\mathcal{S}}^n$ to an arbitrary outside point is numerically accessible, but it does not seem to admit a closed-form solution in general. An exception is the case of P_{CZ}^2, where the nearest canonical gate to $\text{CAN}(\alpha, \beta, \delta)$ is $\text{CAN}(\alpha, \beta, 0)$.

Example 70*.* The SWAP gate is of particular interest, and so we provide an analysis of its approximants as an example of these methods. The nearest point to SWAP within $\Pi(P_{\text{XY}}^2)$ is $(-2/3, 0, 1/3, 1/3)$, with an average gate infidelity of $3/20$. The nearest point to SWAP within $\Pi(P_{\text{DB}}^2)$ is only slightly further: $(-1/2, 1/8, 1/8, 1/4)$, with average gate infidelity of $1/6$. For contrast, the nearest point to $\text{SWAP} \equiv \text{CAN}(\pi/2, \pi/2, \pi/2)$ within $\Pi(P_{\text{CZ}}^2)$ is given by $\text{CAN}(\pi/2, \pi/2, 0)$, with an average gate infidelity of $2/5$.

7 Open questions

In closing the main thread of the paper, we list some follow-on projects where one would expect to find interesting results.

7.1 Algorithmic effectiveness and circuit realization

The single most important avenue left open by this work is the actual manufacture of a circuit in $P_{\mathcal{S}}^2$ from a point in $\Pi(P_{\mathcal{S}}^2)$ (i.e., Problem 8.2), which we refer to as the *realization problem*.

Edelman et al. have presented a specialization of Newton's method on a curved Riemannian manifold to the orthogonal group with its natural

metric [14]. If one were able to provide approximate solutions to the realization problem, such an algorithm could be used to rapidly increase the accuracy of such a solution—but without approximate solutions, such methods have no guarantee of convergence.[19] Additionally, this method would require foreknowledge of the gates D_E and D_F in Problem 11, limiting its applicability in parametric settings such as P^2_{XY}.

From the perspective of Appendix A, a solution to the monodromy problem corresponds to a flat connection on the trivial $PU(4)$–bundle over a punctured Riemann sphere with prescribed monodromy values. The data of an *arbitrary* connection is easier to describe: it assigns to each path an element of $PU(4)$ via parallel transport, perhaps with some further smoothness conditions. Rade's thesis [40] analyzes the Yang–Mills flow from an arbitrary such connection (with boundary conditions) to a flat representative, and for generic connections its convergence is rapid. One might therefore try to discretize the punctured Riemann sphere and apply a numerical variant of Rade's method. It is not immediately clear, however, how one would introduce the orthogonality constraints present in Problem 11 [16].

Cole Franks et al. [17, 9] have described effective numerical methods for solving the *additive* analogue of the eigenvalue problem. One might explore multiplicative variations on their methods (especially those with the orthogonality constraint kept in mind) which would then adapt to solve the problem posed here.

A separate concern of algorithmic effectiveness is the taming of the exponential upper bound on the size of the family of inequalities coming from Corollary 26. In practice, this bound appears to be a gross overestimate, and we are optimistic that a polynomial bound is possible. As an aside, one of the advantages of Belkale's analysis of the monodromy polytope [6] over that of Agnihotri and Woodward [1] is that his set of inequalities is minimal—so similar considerations have already been taken up by the progenitors of the results shown here.

[19] In the particular case of P^2_{XY}, M. Scheer has pointed out to us the commutation relation $[\mathrm{XX}+\mathrm{YY}, \mathrm{ZI}+\mathrm{IZ}] = 0$, from which it follows that the group of interest can be reduced from $PO(4)$ to a particular four-dimensional subset. However, this subset is not closed under multiplication, which hinders the translation of the methods of Edelman et al.

7.2 Alternative interpretations of "optimum"

The particular metric by which we measured the utility of DB over other instances of XY_α was the volume of the polytope $\Pi(P^2_{\mathrm{DB}})$. It is not clear that this is the best such metric (nor that there is a best). Here we list some alternative metrics that seem worth exploring.

Firstly, is there a value of α for which the average (or worst) value of average gate infidelity is minimized? Against this metric, an "elliptical" polytope may be more valuable than a "spherical" one. This analysis may also change when considering other approximation metrics than average gate infidelity, e.g., diamond distance.

The Haar volume (or, indeed, most any other natural volume) of a subset of $PU(4)$ is not perfectly related to the volume of its image as a subset of $\mathfrak{A}_{C_2}$. For any such volume vol' on $PU(4)$, it would also be of interest to maximize the analogous function $\mathrm{vol}' P^2_{\mathrm{XY}_t}$ over t. (For the Haar volume, it appears that the maximum remains at $\alpha = 3\pi/4$, but we do not have a proof that this is so.) Another discrepancy that is worth illuminating is the change-of-coordinates formula comparing $\langle \mathcal{L}_{\mathcal{S}} \rangle^{\mathrm{Haar}}$ and $\langle \mathcal{L}_{\mathcal{S}} \rangle^{\mathfrak{A}_{C_2}}$. These integrals vary at least by the Jacobian of Π, considered as a function on the canonical subgroup, which would already be worth computing.

It would also be of interest to understand the local behavior of any of these metrics with respect to small distances in $PU(4)$. This is the domain of *coherent unitary error*, and one might hope to leverage some of the results of this paper to tailor a compilation method for a coherently error-prone device. Preliminary inspection of this for P^2_{CZ} indicates that derivatives conspire so that only large coherent unitary error gives rise to significant gain in volume.

Any more nuanced tracking of error has the potential to alter the analysis in Section 6. In particular, separate tracking of unitary and nonunitary error is very likely to affect the outcome of the protocol described there.

C. Iancu has observed that potential native gate-sets are typically not uniform in quality: for instance, on certain hardware architectures it could be the case that $\sqrt{\mathrm{CZ}}$ takes half as long (and hence suffers half as much performance degradation) as CZ, so that the "performance metric" of expected gate depth ought to be reweighted by an appropriate factor coming

from the performances of the gates involved. Indeed, in this toy example, one finds

$$\frac{1}{2}\langle \mathcal{L}_{\sqrt{\mathrm{CZ}}} \rangle^{\mathfrak{A}_{C_2}} = 1.802083 < 3 = \langle \mathcal{L}_{\mathrm{CZ}} \rangle^{\mathfrak{A}_{C_2}},$$

contrary to the apparent loss in gateset quality considered in Example 49.

7.3 Unexplored polytopes

The material presented here amounts to a toolkit for analyzing the space of programs available to a given native gate set. We have used this as incentive to investigate a particular native gate set because of its depth-two behavior and its relevance to a particular sort of hardware, but this is hardly the only option.

As part of the project of exploring the structure of the space of gatesets, it would be of interest to describe those native gate sets $\mathcal{S}$ which enjoy $\Pi(P_{\mathcal{S}}^2) = \mathfrak{A}_{C_2}$. This set is nonempty, as the B–gate has this property. Are there other singletons? Other finite sets? Other exponential families?

Figure 13 could probably be smoothed using the same interpolation techniques as in Theorem 55, yieliding an explicit piecewise formula for $\mathrm{vol}^{\mathfrak{A}_{C_2}}(P_S^2)$ as S ranges over the entire solid.

The hardware employed by Rigetti is not the only option, and one could re-run this same analysis for other designs. As an example, calculating the subspace of programs efficiently available to Google's fSim gate would likely be a pleasant exercise in these techniques.

The methods of this paper may also bear indirect fruit at higher qubit counts. For example, Wei and Di [48] have given a CZ–based circuit decomposition for operators in the subgroup $PO(8)$ which improves over the best known general such circuit decomposition for operators in $PU(8)$. They leave open the full reach of their result: namely, the local equivalence class of $PO(8)$ within $PU(8)$ belongs in the middle of the chain of inclusions

$$PO(8) \subseteq PU(2)^{\otimes 3} \cdot PO(8) \cdot PU(2)^{\otimes 3} \subseteq PU(8),$$

and their techniques continue to apply to this middle term. However, its structure is unknown, save that $PO(8)$ is generically of codimension 12 within it. Preliminary application of our techniques in this context shows that this local equivalence class is detected within $PU(8)$ by a set of linear constraints on the logarithmic spectrum, as well as some further constraint phenomena for which we are unable to account. Giving concrete descriptions these remaining constraints would greatly widen the applicability of the techniques of Wei and Di.

Recent work by Glaudell, Ross, and Taylor leverages the accidental isomorphism $SU(4) \cong \mathrm{Spin}(6)$ to produce circuit decompositions into a certain discrete gate set [19]. One might wonder whether the methods described here interact usefully with this alternative presentation of two-qubit operations.

7.4 Leakiness

The analysis of "leaky gates" in Appendix B is not as thorough as it might be. Here are some open questions and problems concerning that property:

- In Remark 89, we argue that within the local equivalence class of a leaky entangler, there is one where the single-qubit gates involved in the leakiness relation are all Z–gates. However, their parameters may depend on each other in a nontrivial way. Give a description of the possible ways this can happen. The exponential family SWAP_α (i.e., the $(\alpha/\pi)^{\mathrm{th}}$ root of SWAP) is probably of interest here.
- Every given example of a leaky gate is leaky on both coordinates. Is this always the case?
- Every given example of a leaky gate has a representative in its local equivalence class with it transpose-symmetric. Is this always the case?
- Our best guess is that the subspace of leaky entanglers coincides exactly with the edges of $\mathfrak{A}_{C_2}$. Is this true?

Acknowledgements

We would like to thank Rigetti Computing for providing such a stimulating workplace, with difficult problems to solve and wonderful peers to work alongside. In particular, M. Appleby, J. Combes, E. Davis, C. Hadfield, P. Karalekas, A. Papageorge, N. Rubin, C. Ryan, M. Scheer, M. P. da Silva, M. Skilbeck, and N. Tezak contributed a lot to our momentum, whether through pointers, proofreading, or generalized enthusiasm. E.

Davis deserves special credit, as he finally put us on the right path to move from numerical experiment to mathematical proof, and this project might not have come together if not for his crucial advice. Although W. Zeng had been suggesting that we think about approximate compilation for some time, Section 6 is a direct result of A. Javadi-Abhari's very pleasant talk at IWQC 2018. We additionally had the pleasure of speaking with the mathematicians W. C. Franks, B. Gammage, S. Kumar, E. Lerman, S. Lichak, P. Solis, C. Teleman, R. Wentworth, and C. Woodward, who freely offered their consultation and expertise on matters related to the monodromy polytope. The first author would like to note the indirect but invaluable role that his PhD adviser, C. Teleman, played in this project: the material presented here is *much* closer to Teleman's domain than the first author's thesis ever was, and acquiring the working knowledge to complete this project would have been much harder without a steady exposure to these ideas over the years. An additional hearty thank you goes to R. Bryant for teaching the first author most of what he knows about Lie theory (and from the second author to the first for the same reason). Finally, the anonymous referees enormously improved the quality of this paper and kindly pointed out a goodly number of errors, for which we are very grateful.

References

[1] S. Agnihotri and C. Woodward. Eigenvalues of products of unitary matrices and quantum Schubert calculus. *Math. Res. Lett.*, 5(6):817–836, 1998. doi:10.4310/MRL.1998.v5.n6.a10.

[2] M. F. Atiyah. Convexity and commuting Hamiltonians. *Bull. London Math. Soc.*, 14(1):1–15, 1982. doi:10.1112/blms/14.1.1.

[3] M. F. Atiyah and R. Bott. The Yang-Mills equations over Riemann surfaces. *Philos. Trans. Roy. Soc. London Ser. A*, 308(1505):523–615, 1983. doi:10.1098/rsta.1983.0017.

[4] D. Avis. Living with lrs. In *Discrete and computational geometry (Tokyo, 1998)*, volume 1763 of *Lecture Notes in Comput. Sci.*, pages 47–56. Springer, Berlin, 2000. doi:10.1007/978-3-540-46515-7_4.

[5] D. Avis and K. Fukuda. Reverse search for enumeration. volume 65, pages 21–46. 1996. doi:10.1016/0166-218X(95)00026-N. First International Colloquium on Graphs and Optimization (GOI), 1992 (Grimentz).

[6] P. Belkale. Local systems on $\mathbb{P}^1 - S$ for S a finite set. *Compositio Math.*, 129(1):67–86, 2001. doi:10.1023/A:1013195625868.

[7] A. Bertram, I. Ciocan-Fontanine, and W. Fulton. Quantum multiplication of Schur polynomials. *J. Algebra*, 219(2):728–746, 1999. doi:10.1006/jabr.1999.7960.

[8] A. Buch. Littlewood–Richardson calculator. `http://sites.math.rutgers.edu/~asbuch/lrcalc/`, 1999-2014.

[9] P. Bürgisser, C. Franks, A. Garg, R. M. de Oliveira, M. Walter, and A. Wigderson. Efficient algorithms for tensor scaling, quantum marginals, and moment polytopes. In M. Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 883–897. IEEE Computer Society, 2018. doi:10.1109/FOCS.2018.00088.

[10] S. A. Caldwell, N. Didier, C. A. Ryan, E. A. Sete, A. Hudson, P. Karalekas, R. Manenti, M. P. da Silva, R. Sinclair, E. Acala, N. Alidoust, J. Angeles, A. Bestwick, M. Block, B. Bloom, A. Bradley, C. Bui, L. Capelluto, R. Chilcott, J. Cordova, G. Crossman, M. Curtis, S. Deshpande, T. E. Bouayadi, D. Girshovich, S. Hong, K. Kuang, M. Lenihan, T. Manning, A. Marchenkov, J. Marshall, R. Maydra, Y. Mohan, W. O'Brien, C. Osborn, J. Otterbach, A. Papageorge, J. P. Paquette, M. Pelstring, A. Polloreno, G. Prawiroatmodjo, V. Rawat, M. Reagor, R. Renzas, N. Rubin, D. Russell, M. Rust, D. Scarabelli, M. Scheer, M. Selvanayagam, R. Smith, A. Staley, M. Suska, N. Tezak, D. C. Thompson, T. W. To, M. Vahidpour, N. Vodrahalli, T. Whyland, K. Yadav, W. Zeng, and C. Rigetti. Parametrically Activated Entangling Gates Using Transmon Qubits. *Physical Review Applied*, 10:034050, Sep 2018, 1706.06562. doi:10.1103/PhysRevApplied.10.034050.

[11] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta. Validating quantum comput-

ers using randomized model circuits. *Phys. Rev. A*, 100:032328, Sep 2019. doi:10.1103/PhysRevA.100.032328.

[12] S. K. Donaldson. A new proof of a theorem of narasimhan and seshadri. *J. Differential Geom.*, 18(2):269–277, 1983. doi:10.4310/jdg/1214437664.

[13] S. K. Donaldson. Boundary value problems for Yang-Mills fields. *J. Geom. Phys.*, 8(1-4):89–122, 1992. doi:10.1016/0393-0440(92)90044-2.

[14] A. Edelman, T. A. Arias, and S. T. Smith. The geometry of algorithms with orthogonality constraints. *SIAM J. Matrix Anal. Appl.*, 20(2):303–353, 1999. doi:10.1137/S0895479895290954.

[15] L. Euler. *Novi commentarii Academiae Scientiarum Imperialis Petropolitanae*, volume t.20. Petropolis, Typis Academiae Scientarum, 1775.

[16] E. Falbel and R. A. Wentworth. Eigenvalues of products of unitary matrices and Lagrangian involutions. *Topology*, 45(1):65–99, 2006. doi:10.1016/j.top.2005.06.003.

[17] C. Franks. Operator scaling with specified marginals. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, page 190–203, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3188745.3188932.

[18] W. Fulton and R. Pandharipande. Notes on stable maps and quantum cohomology. In *Algebraic geometry—Santa Cruz 1995*, volume 62 of *Proc. Sympos. Pure Math.*, pages 45–96. Amer. Math. Soc., Providence, RI, 1997. doi:10.1090/pspum/062.2/1492534.

[19] A. N. Glaudell, N. J. Ross, and J. M. Taylor. Optimal Two-Qubit Circuits for Universal Fault-Tolerant Quantum Computation. *arXiv e-prints*, page arXiv:2001.05997, Jan. 2020, 2001.05997.

[20] V. Guillemin and S. Sternberg. Convexity properties of the moment mapping. *Invent. Math.*, 67(3):491–513, 1982. doi:10.1007/BF01398933.

[21] V. Guillemin and S. Sternberg. Convexity properties of the moment mapping. II. *Invent. Math.*, 77(3):533–546, 1984. doi:10.1007/BF01388837.

[22] B. Hall. *Lie groups, Lie algebras, and representations*, volume 222 of *Graduate Texts in Mathematics*. Springer, Cham, second edition, 2015. doi:10.1007/978-3-319-13467-3. An elementary introduction.

[23] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. doi:https://doi.org/10.1007/978-1-4757-3849-0. Graduate Texts in Mathematics, No. 52.

[24] A. Horn. Eigenvalues of sums of Hermitian matrices. *Pacific J. Math.*, 12:225–241, 1962. URL http://projecteuclid.org/euclid.pjm/1103036720.

[25] J. E. Humphreys. *Reflection groups and Coxeter groups*, volume 29 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990. doi:10.1017/CBO9780511623646.

[26] L. C. Jeffrey and J. Weitsman. Bohr-Sommerfeld orbits in the moduli space of flat connections and the Verlinde dimension formula. *Communications in Mathematical Physics*, 150(3):593–630, Dec. 1992. doi:10.1007/BF02096964.

[27] F. Kirwan. Convexity properties of the moment mapping. III. *Invent. Math.*, 77(3):547–552, 1984. doi:10.1007/BF01388838.

[28] A. A. Klyachko. Stable bundles, representation theory and Hermitian operators. *Selecta Math. (N.S.)*, 4(3):419–445, 1998. doi:10.1007/s000290050037.

[29] A. Knutson. The symplectic and algebraic geometry of horn's problem. *Linear Algebra and its Applications*, 319(1):61 – 81, 2000. doi:https://doi.org/10.1016/S0024-3795(00)00220-2.

[30] M. Kontsevich and Y. Manin. Gromov-Witten classes, quantum cohomology, and enumerative geometry. *Comm. Math. Phys.*, 164(3):525–562, 1994. URL http://projecteuclid.org/euclid.cmp/1104270948.

[31] B. Kraus and J. I. Cirac. Optimal creation of entanglement using a two-qubit gate. *Physical Review A*,

63:062309, Jun 2001, quant-ph/0011050. doi:10.1103/PhysRevA.63.062309.

[32] J. Lawrence. Polytope volume computation. *Math. Comp.*, 57(195):259–271, 1991. doi:10.2307/2938672.

[33] Y. Makhlin. Nonlocal properties of two-qubit gates and mixed states, and the optimization of quantum computations. *Quantum Information Processing*, 1(4):243–252, Aug. 2002. doi:10.1023/A:1022144002391.

[34] V. B. Mehta and C. S. Seshadri. Moduli of vector bundles on curves with parabolic structures. *Math. Ann.*, 248(3):205–239, 1980. doi:10.1007/BF01420526.

[35] E. Meinrenken and C. Woodward. A symplectic proof of Verlinde factorization. *eprint arXiv:dg-ga/961201*, Dec. 1996, dg-ga/9612018.

[36] E. Meinrenken and C. Woodward. Hamiltonian loop group actions and verlinde factorization. *J. Differential Geom.*, 50(3):417–469, 1998. doi:10.4310/jdg/1214424966.

[37] M. S. Narasimhan and C. S. Seshadri. Stable and unitary vector bundles on a compact Riemann surface. *Ann. of Math. (2)*, 82:540–567, 1965. doi:10.2307/1970710.

[38] M. A. Nielsen. A simple formula for the average gate fidelity of a quantum dynamical operation. *Physics Letters A*, 303(4):249 – 252, 2002. doi:https://doi.org/10.1016/S0375-9601(02)01272-0.

[39] L. H. Pedersen, N. M. Møller, and K. Mølmer. Fidelity of quantum operations. *Phys. Lett. A*, 367:47–51, July 2007, quant-ph/0701138. doi:10.1016/j.physleta.2007.02.069.

[40] J. Rå de. On the Yang-Mills heat equation in two and three dimensions. *J. Reine Angew. Math.*, 431:123–163, 1992. doi:10.1515/crll.1992.431.123.

[41] A. Sard. The measure of the critical values of differentiable maps. *Bull. Amer. Math. Soc.*, 48:883–890, 1942. doi:10.1090/S0002-9904-1942-07811-6.

[42] N. Schuch and J. Siewert. Natural two-qubit gate for quantum computation using the XY interaction. *Physical Review A*, 67:032301, Mar 2003, quant-ph/0209035. doi:10.1103/PhysRevA.67.032301.

[43] V. V. Shende, S. S. Bullock, and I. L. Markov. Recognizing small-circuit structure in two-qubit operators. *Physical Review A*, 70:012310, July 2004, quant-ph/0308045. doi:10.1103/PhysRevA.70.012310.

[44] V. V. Shende, S. S. Bullock, and I. L. Markov. Synthesis of quantum-logic circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(6):1000–1010, 2006. doi:10.1109/TCAD.2005.855930.

[45] V. V. Shende, I. L. Markov, and S. S. Bullock. Minimal universal two-qubit controlled-NOT-based circuits. *Phys. Rev. A*, 69:062321, 2004. doi:10.1103/PhysRevA.69.062321.

[46] R. S. Smith, M. J. Curtis, and W. J. Zeng. A Practical Quantum Instruction Set Architecture. *arXiv e-prints*, page arXiv:1608.03355, Aug. 2016, 1608.03355.

[47] P. Watts, J. Vala, M. M. Müller, T. Calarco, K. B. Whaley, D. M. Reich, M. H. Goerz, and C. P. Koch. Optimizing for an arbitrary perfect entangler. i. functionals. *Phys. Rev. A*, 91:062306, Jun 2015. doi:10.1103/PhysRevA.91.062306.

[48] H.-R. Wei and Y.-M. Di. Decomposition of orthogonal matrix and synthesis of two-qubit and three-qubit orthogonal gates. *Quantum Info. Comput.*, 12(3–4):262–270, Mar. 2012.

[49] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley. Geometric theory of nonlocal two-qubit operations. *Phys. Rev. A*, 67:042313, 2003. doi:10.1103/PhysRevA.67.042313.

[50] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley. Minimum Construction of Two-Qubit Quantum Operations. *Phys. Rev. Lett.* , 93:020502, Jul 2004, quant-ph/0312193. doi:10.1103/PhysRevLett.93.020502.

A The mathematics of the monodromy polytope

In this appendix, we produce some of the details (or, failing that, some soothing exposition) of the mathematics underlying our results in the main text. This effort cleaves into two parts: some generic convexity results in symplectic geometry that give the qualitative solution to the multiplicative eigenvalue problem (and which merit the name "monodromy polytope"), followed by some results around quantum cohomology that give the quantitative solution.

A.1 Qualitative results

Before getting involved with the multiplicative eigenvalue problem directly, we first give a slightly ahistorical account[20] of a generic qualitative result found in symplectic geometry.

Definition 71. A *symplectic manifold* M is an oriented $2n$–manifold equipped with a choice of *symplectic form* ω, i.e., an n^{th} root of the volume form (or, equivalently, an everywhere nondegenerate 2–form).

Example 72. Examples of such objects are rife in physics: all phase spaces are instances of symplectic manifolds. For an ultra-simple but ultra-concrete example, we might take $M = T^*\mathbb{R} = \mathbb{R}^2$ with the symplectic form $\omega = dp \wedge dq$, or more generally $M = T^*\mathbb{R}^d = \mathbb{R}^{2d}$ with $\omega = \sum_j dp_j \wedge dq_j$. These arise as the phase spaces associated to d many non-interacting simple harmonic oscillators. In general, a symplectic manifold has this as its local form.

Definition 73. Given an action on a symplectic manifold M by a Lie group G (so that $\tau_g^*\omega = \omega$), a *moment map* is a G–equivariant function $\Phi\colon M \to \mathfrak{g}^*$, where the target carries the coadjoint action.

Example 74. Again, examples of such objects are rife in physics: a nontrivial gauge group gives rise to a G–action on a phase space, and a moment map can be used to describe a G–invariant physical quantity, such as the total energy of a system. In the above example, $G = S^1$ acts on $\mathbb{R}^2$ by rotation, and the associated Lie algebra $\mathfrak{g}^*$ can be identified with $\mathbb{R}$ in such a way that a moment map is given by $\Phi(v) = \frac{1}{2}|v|^2$. Similarly, the d–torus $G = (S^1)^{\times d}$ acts on $\mathbb{R}^{2d}$ by rotations of the component planes, and there is an associated moment map $\mathbb{R}^{2d} \to \mathfrak{g}^* \cong \mathbb{R}^d$ which sends each particle to its total energy.

A useful tool for manufacturing these objects comes in the form of the following theorem:

Theorem 75 (Symplectic reduction)**.** *Let M be a symplectic G–manifold with associated proper moment map Φ_G, and let $H \leq G$ be a normal subgroup. When $M/\!\!/H := \Phi_G^{-1}(0)/H$ is a manifold, it inherits both a symplectic form $\omega_{M/\!\!/H}$ (which pulls back to $\Phi_G^{-1}(0)$ to agree with the restriction of ω_M), a compatible action by G/H, and a moment map $\Phi_{G/H}$.* □

Our interest in these objects stems from the following family of convexity results:

Theorem 76. *Let M be a connected symplectic manifold with an action by a Lie group G through symplectomorphisms and a proper moment map $\Phi\colon M \to \mathfrak{g}^*$.*

- *(Atiyah [2], Guillemin–Sternberg [20, 21]:) Suppose that $G = T$ is a compact torus, and let $\mathfrak{A}$ be a choice of fundamental alcove within $\mathfrak{t}^*$. The restriction of the image of Φ to $\mathfrak{A}$ then forms a convex polytope.*
- *(Kirwan [27]:) Suppose that G is compact, let $T \leq G$ be a choice of maximal torus with corresponding dual Cartan subalgebra $\pi\colon \mathfrak{g}^* \to \mathfrak{t}^*$, and let $\mathfrak{A}$ again be a fundamental alcove within $\mathfrak{t}^*$. The restricted set $\mathfrak{A} \cap \operatorname{im}(\pi \circ \Phi)$ is a convex polytope.*

[20] The solution to this problem is strongly coupled to the solution of the corresponding "linearized" problem: given Hermitian matrices H_1 and H_2, what spectra can possibly arise as that of $\operatorname{Ad}_{U_1} H_1 + \operatorname{Ad}_{U_2} H_2$ for unitary operators U_1 and U_2? A conjectural solution to this problem was set out by Horn [24], which spurred the development of a great many results in symplectic geometry and representation theory in an effort to explain his findings, and these tools were ultimately used by Klyachko [28] to settle the matter. Knutson [29] gives a very pleasant overview of this body of work and its surroundings, and although he does not address the multiplicative problem, (generalizations of) these same tools reappear in this context. We intend the word "ahistorical" only in the sense that the tools were developed *in response to* the visible behavior of the (additive) eigenvalue problem, whereas our exposition presents the tools as generic ideas which we then apply *post facto* to the eigenvalue problem—a significant misrepresentation of history.

- *(Meinrenken–Woodward [35, Theorem 3.13]:) For G' a Lie group, its loop group is the infinite-dimensional Lie group $LG' = (G')^{S^1}$ of loops in G' with pointwise multiplication.*[21] *Suppose that $G = LG'$ for G' a compact, connected, simply connected Lie group, let T' be a choice of maximal torus within G', and let $\mathfrak{A}'$ be a choice of fundamental alcove within $(\mathfrak{t}')^*$. The intersection $\mathfrak{A}' \cap (\pi \circ \Phi)(M)$ is then a convex polytope.* □

Remark 77. The most basic of this chain of results is somewhat believable: in Example 74, the image of the moment map is the positive orthant in $\mathfrak{t}^*$. Since a general symplectic manifold is constructed locally from that example, the image of a general moment map is constructed locally out of such "corners"—though amplifying this to an equivariant statement (and then to the nonabelian setting) is no trivial feat. The final form of the theorem is *considerably* harder to visualize, but it is the version that will concern us chiefly.

Example 78 ([3, p. 587], [13]). We focus our attention on an example that physicists will recognize as an instance of Yang–Mills theory. Let G be a compact, connected, simply-connected Lie group (e.g., $SU(4)$), let Σ be Riemann sphere with b disks excised, and let P be the trivial principal G–bundle over Σ. The space $\mathcal{A}(\Sigma;\mathfrak{g})$ of $\mathfrak{g}$–valued connections on P may be identified with $\Omega^1(\Sigma;\mathfrak{g})$, and it can be shown to carry the structure of a symplectic manifold using the Atiyah–Bott symplectic form

$$\omega_{AB}(A_1, A_2) = \int_\Sigma A_1 \wedge A_2.$$

This carries a compatible action by the gauge group $\mathcal{G}(\Sigma)$ of sections of P (i.e., G–valued continuous functions on Σ), which has Lie algebra $\Omega^0(\Sigma;\mathfrak{g})$, and this action moreover admits a moment map Φ_{AB} determined by

$$\langle \Phi_{AB}(A), \xi \rangle = \int_\Sigma F_A \cdot \xi + \int_{\partial\Sigma} \iota^*(A \cdot \xi),$$

where F_A is the curvature form associated to A and $\iota\colon \partial\Sigma \to \Sigma$ is the inclusion of the boundary components. Writing $\mathcal{G}_\partial(\Sigma)$ for the term in the kernel sequence

$$1 \to \mathcal{G}_\partial(\Sigma) \to \mathcal{G}(\Sigma) \xrightarrow{\iota^*} \mathcal{G}(\partial\Sigma) \to 1,$$

the restricted action on $\mathcal{A}(\Sigma;\mathfrak{g})$ inherits the moment map $\Phi_\partial(A) = F_A$, and so the symplectic reduction

$$\mathcal{M}^\flat(\Sigma;\mathfrak{g}) = \mathcal{A}(\Sigma;\mathfrak{g}) /\!\!/ \mathcal{G}_\partial(\Sigma) = \mathcal{A}^\flat(\Sigma;\mathfrak{g})/\mathcal{G}_\partial(\Sigma),$$

called the *moduli of flat connections*, inherits an action by $\mathcal{G}(\partial\Sigma) \cong LG^b$ and a $\mathcal{G}(\partial\Sigma)$–equivariant moment map $\Phi^\flat(A) = \iota^* A$.

Corollary 79 ([36, Theorem 3.2], [35, Theorem 3.16])**.** *The set*

$$\mathrm{LogSpec}\{U_1, U_2, U_3 \in SU(4) \mid U_1 U_2 = U_3\} \subset \mathfrak{A}^{\times 3}$$

is a convex polytope.

Construction. We set $\Sigma = \mathbb{C}\mathrm{P}^1 \setminus \{1, 2, 3\}$ and $G = SU(4)$, then apply Example 78 to conclude that $\mathcal{M}^\flat(\Sigma)$ is a symplectic G–manifold with associated moment map $A \mapsto \iota^* A$. Fix the following auxiliary data:

- Parametrizations $B_j\colon S^1 \to \Sigma$ of the j^{th} boundary component.
- Paths $\gamma_j\colon B_1(0) \to B_j(0)$ begetting loops $b_j = \gamma_j^{-1} B_j \gamma_j$ which have the property

$$\pi_1\Sigma = \left\langle \begin{array}{c} b_1 = B_1, \\ b_2 = \gamma_2^{-1} B_2 \gamma_2, \\ b_3 = \gamma_3^{-2} B_3 \gamma_3 \end{array} \middle| 1 = b_1 b_2 b_3 \right\rangle.$$

[21] The loops are commonly assumed to have a further technical property—for instance, some degree of differentiability.

To these data, a connection A associates elements $B_j^* A \in L\mathfrak{g}^*$, the local behavior of A near B_j, and elements $\Gamma(A, \gamma_j)_0^1 \in G$, the action of parallel transport along γ_j from the (trivialized) fiber over $\gamma_j(0)$ to the (trivialized) fiber over $\gamma_j(1)$.

It is well-known that the moduli space of flat connections on a trivial G–bundle over a suitable Riemann surface Σ is weakly equivalent to the space of G–representations of $\pi_1\Sigma$. The procedure for extracting such a representation is by sending a loop in the base to the monodromy of the connection around the loop. One may promote this idea from a weak equivalence into a commuting square with horizontal arrows *equivariant symplectomorphisms*:

$$\begin{array}{ccc} \mathcal{M}^\flat(\Sigma;\mathfrak{g}) & \longrightarrow & \left\{ \begin{array}{c} c_* \in \{1\} \times G^2 \\ \xi_* \in (L\mathfrak{g}^*)^{\times 3} \end{array} \middle| 1 = \prod_{j=1}^{3} \mathrm{Ad}_{c_j} \mathrm{Mon}(\xi_j) \right\} \\ \downarrow \Phi & & \downarrow \Phi \\ (\mathrm{Lie}\, \mathcal{G}(\partial\Sigma))^* & \longrightarrow & \{(\xi_*) \in (L\mathfrak{g}^*)^{\times 3}\}, \end{array}$$

where the first horizontal arrow is defined by

$$c_j(A) = \Gamma(A, \gamma_j)_0^1, \qquad \xi_j(A) = B_j^*(A),$$

the monodromy operator is defined by

$$\mathrm{Mon}(\xi_j) = \int_{S^1} B_j^*(A) \in G,$$

and the action of $\mathcal{G}(\partial\Sigma) \cong LG^3$ on the top-right corner is given by

$$g \cdot c_j = g_j(0)^{-1} c_j g_1(0), \qquad g \cdot \xi_j = \mathrm{Ad}_{g_j} \xi_j - g_j^{-1} dg_j.$$

Granting this, we find ourselves at the doorstep of the multiplicative eigenvalue problem. Note first that the operator Mon enjoys two pleasant properties:

1. After using the Killing form to identify $\mathfrak{g}^*$ with the subspace $\mathfrak{g} \subseteq L\mathfrak{g}$ of constant loops, for $h \in \mathfrak{g}$ we have $\mathrm{Mon}(h) = \exp(h)$, the usual Lie exponential.
2. The G–action on ξ_j is then arranged so that the following formula holds:

$$\mathrm{Mon}(g \cdot \xi_j) = \mathrm{Ad}_{g_j(0)} \mathrm{Mon}(\xi_j).$$

These properties combine to give the required link. We apply Theorem 76: take $\mathfrak{A} \subset \mathfrak{t}^*$ to be real diagonal matrices whose entries obey the criteria set out by Definition 17. The image of the moment map then becomes those triples of diagonal matrices $(\xi_1, \xi_2, \xi_3) \in \mathfrak{A}^{\times 3}$ for which there exist unitary operators c_2, c_3 satisfying

$$e^{-2\pi i \xi_1} = c_2^{-1} e^{2\pi i \xi_2} c_2 \cdot c_3^{-1} e^{2\pi i \xi_3} c_3. \qquad \square$$

Remark 80. Throughout the paper, there are two Lie groups of interest: $PU(4) = U(4)/\mathbb{C}^\times$, which participates in a nontrivial central extension

$$1 \to C_4 \to SU(4) \to PU(4) \to 1,$$

and the double cover $SU(4)/C_2$ of $PU(4)$, which also participates in a nontrivial central extension

$$1 \to C_2 \to SU(4) \to SU(4)/C_2 \to 1.$$

Neither is simply connected, a necessary hypothesis of Corollary 79, which we redress as follows. In general, we may consider compact connected Lie groups G whose universal cover $\widetilde{G}$ participates in a finite central extension

$$1 \to F \to \widetilde{G} \xrightarrow{\pi} G \to 1.$$

The Lie algebras of $\widetilde{G}$ and G may be identified by π, and the image of the moment map Φ_G considered in Corollary 79 is then given by the union over $f \in F$ of the images of the moment maps $\Phi_{\widetilde{G},f}$, constructed analogously so as to detect products of the form $U_1 U_2 = f U_3$ with $U_1, U_2, U_3 \in \widetilde{G}$.

A.2 Quantitative results

We now turn to quantitative results: given that the solution set to the multiplicative eigenvalue problem forms a convex polytope, what polytope is it? As in the additive case, this problem passes through representation theory, and in the exposition about the qualitative problem we have already begun to make this contact: a flat connection on a trivial vector bundle is equivalent data to a representation of the fundamental group of the base, and flat connections modulo gauge equivalence correspond to representations up to choice of basis. Theorems of Narasimhan and Seshadri and of Donaldson show that this has a kind of converse: unitary representations of the fundamental group of a compact Riemann surface correspond to "stable" holomorphic vector bundles over the surface [37], and such bundles can be shown to admit a unique flat unitary connection [12]. A vector bundle V is said to be stable when its slope, $\mu(V) = \deg(V)/\operatorname{rank}(V)$, decreases when passing to any subbundle. Informally, a stable bundle is "more ample" than any of its subbundles.

However, our surface of interest, $\Sigma = \mathbb{C}\mathrm{P}^1 \setminus \{1, 2, 3\}$, is a *noncompact* Riemann surface.[22] Work of Mehta and Seshadri extends the above correspondence to the noncompact case: a *parabolic bundle* (on $\mathbb{C}\mathrm{P}^1$) is a holomorphic vector bundle E, a choice of finite set $S \subset \mathbb{C}\mathrm{P}^1$, a choice of flag $\{E_{s,i}\}$ for each $s \in S$, and a family of weights $\lambda_{s,i}$ satisfying the strings of inequalities

$$\lambda_{s,1} \geq \cdots \geq \lambda_{s,n} > \lambda_{s,1} - 1$$

as well as the equality $\deg E = -\sum_{s,i} \lambda_{s,i}$. A parabolic bundle is additionally said to be *semistable* when its *parabolic slope*, a modification of the slope that is offset by the choice of parabolic weights, decreases when passing to any subbundle (and appropriately restricting the parabolic structure). They then show the following result:

Theorem 81 ([34])**.** *Fix a set S and a family of parabolic weights $\lambda_{s,i}$.*[23] *The moduli space of semistable parabolic bundles on $\mathbb{C}\mathrm{P}^1$ with these weights is a normal, projective variety, homeomorphic to the moduli space of flat unitary connections on the trivial bundle over $\mathbb{C}\mathrm{P}^1 \setminus S$ such that the monodromy operator U_s at s has $\operatorname{LogSpec} U_s = (\lambda_{s,i})_i$.* □

What this theorem conspicuously does not assert is when the moduli of semistable parabolic bundles is *nonempty*. In order to assess this, Agnihotri and Woodward give a geometric interpretation of the semistability condition, then connect it to a complicated form of intersection theory known as *quantum cohomology*. Their ultimate theorem statement is as follows:

Definition 82. We make the following definitions:

- For $r, k > 0$ be positive integers with $r + k = n$, let $\mathcal{P}_{r,k}$ be the set of partitions
$$\mathcal{P}_{r,k} = \{(I_1, \ldots, I_r) \in \mathbb{Z}^r \mid 0 \leq I_1 \leq \cdots \leq I_r \leq k\}.$$
- Let $\mathrm{Gr}(r, k)$ be the Grassmannian of k–planes in $\mathbb{C}^n$.
- Let $\mathbb{C}^n = F_n \supset F_{n-1} \supset \cdots \supset F_0 = \{0\}$ be a complete flag in $\mathbb{C}^n$.
- For a partition $I \in \mathcal{P}_{r,k}$, its *Schubert variety* is $\sigma_I = \left\{W \in \mathrm{Gr}(r, k) \mid \dim(W \cap F_{I_j}) \geq j\right\}$.
- The *Schubert cell* $C_I \subset \sigma_I$ is the complement of all lower-dimensional Schubert varieties contained in σ_I: $C_I = \bigcap_{\sigma_J \subset \sigma_I} \sigma_I \setminus \sigma_J$.
- From these, we define Schubert cycles $[\sigma_I]$ and $[C_I]$ in $H_*\mathrm{Gr}(r, k)$, as well as cohomology classes $T_I \in H^*\mathrm{Gr}(r, k)$ Poincaré dual to $[\sigma_I]$.

[22] In fact, the fundamental groups of compact Riemann surfaces are all known: the surface Σ_g of genus g has fundamental group the free group on letters $a_1, b_1, \ldots, a_g, b_g$ subject to the relation $1 = [a_1, b_1] \cdots [a_g, b_g]$. There is no g for which this looks like our desired free group on generators a, b, c subject to $abc = 1$.

[23] In fact, they assume that $\lambda_{s,i}$ are rational because they work with tools from algebraic geometry. Since we are concerned with complex geometry, we may drop this assumption by interpolation.

Theorem 83 ([1, Theorem 5.3, Lemma 5.5])**.** *The moduli of semistable parabolic bundles with prescribed weights $\lambda_{s,i}$ is non-empty if and only if, for all subsets I_s and integers d such that there exists a degree d map sending $s \in S$ to a general translate of the Schubert cell C_{I_s},*

$$\sum_{s\in S}\sum_{i\in I_s}\lambda_{s,i} \leq d.$$

Moreover, the minimum such value d is computable: for d the lowest degree of any map

$$\mu\colon \mathbb{C}\mathrm{P}^1 \to \mathrm{Gr}(r,k)$$

sending $s \in S$ to a general translate of σ_{I_s}, q^d is the maximal power of q dividing $\prod_{s\in S} T_{I_s}$ in the "small quantum cohomology ring" of $\mathrm{Gr}(r,k)$. □

We now endeavor to explain the contents of this theorem and the connection to the ideas above. The first half is relatively easy to see: suppose that we have a semistable parabolic structure on the trivial bundle over $\mathbb{C}\mathrm{P}^1$. A subbundle of rank k is then classified by a map $\mu\colon \mathbb{C}\mathrm{P}^1 \to \mathrm{Gr}(r,k)$, and the inequality imposed by semistability on the parabolic weights is given by

$$\sum_{s\in S}\sum_{i\leq I_s}\lambda_{s,i} \leq \deg(\mu),$$

where here I_s is the position of the subspace $\mu(s)$ inside of the parabolic flag at $s \in S$. Taking the intersection of all such inequality families imposed by all such maps then gives the proposed description of the moduli.

The meat of the theorem is in the connection with quantum cohomology, which requires a much more elaborate explanation. We follow a set of summary lectures by Fulton and Pandharipande [18]. Beginning with a sufficiently nice[24] space X and for a choice of class $\beta \in H_2(X)$, one may construct a *moduli space of nodal curves* $\mathcal{M}_{g,S}(X,\beta)$ populated by triples (C,Σ,μ) consisting of a projective connective nodal curve C of genus g, a marking $\Sigma\colon S \to C$ in the nonsingular locus, and a map $\mu\colon C \to X$ such that $\mu_*[C] = \beta$ and such that μ admits finitely many automorphisms. This moduli turns out to have a compactification $\overline{\mathcal{M}_{g,S}}(X,\beta)$, and hence its rational cohomology acquires Poincaré duality and an intersection form [30].

Our interest in this construction stems from setting $X = \mathrm{Gr}(r,k)$ and $g = 0$, so that $\overline{\mathcal{M}_{0,S}}(\mathrm{Gr}(r,k),\beta)$ carries information about the available maps μ in Theorem 83. If we try to simultaneously prescribe the positions I_s of $\mu(s)$ inside of the parabolic flag at $s \in S$, we will be further led to consider the classes

$$[\mathrm{ev}_s^{-1}(\sigma_{I_s})] \in H_*\overline{\mathcal{M}_{0,S}}(\mathrm{Gr}(r,k),\beta)$$

as well as their intersections. To capture these intersections, we define the *Gromov–Witten invariant* I_β associated to an S–labled family of cohomology classes $(\gamma_s)_{s\in S} \in H^{2*}(X)$:

$$I_\beta\left(\gamma_s\right)_{s\in S} := \int_{\overline{\mathcal{M}_{0,S}(X,\beta)}} \prod_{s\in S} \mathrm{ev}_s^*(\gamma_s).$$

Example 84 ([18, Equation 44])*.* This definition contains the following special case: writing g^{ef} for the inverse of the permutation operator $g_{ef} = \int_{\mathrm{Gr}(r,k)}(T_eT_f)$, we have

$$T_iT_j = \sum_{e,f}\left(\int_{\mathrm{Gr}(r,k)} T_iT_jT_e\right) g^{ef}T_f = \sum_{e,f} I_0(T_iT_jT_e)g^{ef}T_f,$$

i.e., $I_0(T_iT_jT_e)g^{ef}$ records the structure constants for the cup product. These values are recognized in the literature as *Littlewood–Richardson coefficients*.

[24] The key property is called "convexity" [18, Equation 2, Sections 1–6]. Any homogeneous variety $X = G/P$ with P a parabolic subgroup will do [18, pg. 6], which includes Grassmannians.

Motivated by this, we use nontrivial classes β to define the following "deformed product":

Theorem 85 ([18, Equation 66])**.** *There is a commutative $\mathbb{Z}[\![q]\!]$–bilinear product on $\mathbb{Z}[\![q]\!] \otimes H^*\mathrm{Gr}(r,k)$ given by the formula*

$$T_i * T_j = \left(\sum_{\substack{\beta \in H^2(\mathrm{Gr}(r,k)) \\ \beta \text{ ``effective''}}} I_\beta(T_i T_j T_e) q^{\int_\beta T_1} \right) g^{ef} T_f =: \sum_{d,f} N_{ij}^{f,d}(r,k) \cdot q^d T_f.$$

The structure coefficients $N_{ij}^{f,d}(r,k)$ are called quantum Littlewood–Richardson coefficients. □

We now reconnect with the multiplicative eigenvalue problem: if the classes $[\mathrm{ev}_s^{-1}(\sigma_{I_s})]$ intersect the subspace of $\overline{\mathcal{M}_{0,S}}(\mathrm{Gr}(r,k),\beta)$ of curves of degree d to produce a nontrivial homology class, they will induce a corresponding q^i–divisible cohomology class to appear in the quantum cohomology product of the classes T_{I_s} for some $i \leq d$. In the case where d is minimal, they show that the corresponding cohomology class is degree 0, so that the q^d–divisibility is exact, and also conversely that a minimally q–divisible cohomology class belongs to such an intersection [1, Lemma 5.5].

Finally, we may actually check this condition in cases of interest because the quantum Littlewood–Richardson coefficients are computable: they are connected to enumerative geometry [18, Section 9], and one can use this to calculate them directly in small-index cases; they are connected to cohomology and so obey associativity-type relations [18, Theorem 4]; and it is possible to assemble both of these sources of information into an algorithm which recursively computes them [7, 8]. Since we are specifically interested in the cases of $SU(2)$ and $SU(4)$, we produce a table of the quantum Littlewood–Richardson coefficients appearing in the products on the small quantum cohomology rings for $\mathrm{Gr}(1,1)$ in Figure 3 and for $\mathrm{Gr}(1,3)$, $\mathrm{Gr}(2,2)$, and $\mathrm{Gr}(3,1)$ in Figure 14.

Altogether, these results assemble into the following summary theorem, with form presented here due to Belkale:[25]

Theorem 86 ([1, Theorem 3.1], [6, Theorem 7])**.** *Let U_1, U_2, $U_3 \in SU(n)$ satisfy $U_1 U_2 = U_3$, and let α_*, β_*, δ_* be the fundamental alcove sequence respectively associated to these unitaries through* LogSpec*. Select $r,k > 0$ satisfying $r+k=n$, select $a,b,c \in \mathcal{P}_{r,k}$, and take $d \geq 0$; then if $N_{ab}^{c,d}(r,k) = 1$, the following inequality must hold:*

$$d - \sum_{i=1}^{r} \alpha_{k+i-a_i} - \sum_{i=1}^{r} \beta_{k+i-b_i} + \sum_{i=1}^{r} \delta_{k+i-c_i} \geq 0. \tag{*}$$

Conversely, given alcove sequences α_*, β_*, δ_* for which $N_{ab}^{c,d}(r,k) = 1$ implies Equation (*), there exist U_1, U_2, U_3 with $U_1 U_2 = U_3$ and

$$\alpha_* = \mathrm{LogSpec}\, U_1, \qquad \beta_* = \mathrm{LogSpec}\, U_2, \qquad \delta_* = \mathrm{LogSpec}\, U_3.$$

B Leaky entanglers

There is also a differential-geometric proof that $\Pi(P_{\mathrm{CZ}}^2)$ has vanishing volume which does not rely on first knowing the precise region. The gate CZ commutes with Z–rotations:

[25] The original Mehta–Seshadri theorem concerns unitary flat connections. Belkale also produced an alternative form of their theorem appropriate for flat connections which are special unitary [6, Appendix].

r	k	a	b	c	d	$N_{ab}^{c,d}(r,k)$
1	3	(0)	(0)	(0)	0	1
			(1)	(1)	0	1
			(2)	(2)	0	1
			(3)	(3)	0	1
		(1)	(1)	(2)	0	1
			(2)	(3)	0	1
			(3)	(0)	1	1
		(2)	(2)	(0)	1	1
			(3)	(1)	1	1
		(3)	(3)	(2)	1	1
3	1	(0,0,0)	(0,0,0)	(0,0,0)	0	1
			(1,0,0)	(1,0,0)	0	1
			(1,1,0)	(1,1,0)	0	1
			(1,1,1)	(1,1,1)	0	1
		(1,0,0)	(1,0,0)	(1,1,0)	0	1
			(1,1,0)	(1,1,1)	0	1
			(1,1,1)	(0,0,0)	1	1
		(1,1,0)	(1,1,0)	(0,0,0)	1	1
			(1,1,1)	(1,0,0)	1	1
		(1,1,1)	(1,1,1)	(1,1,0)	1	1

r	k	a	b	c	d	$N_{ab}^{c,d}(r,k)$
2	2	(0,0)	(0,0)	(0,0)	0	1
			(1,0)	(1,0)	0	1
			(1,1)	(1,1)	0	1
			(2,0)	(2,0)	0	1
			(2,1)	(2,1)	0	1
			(2,2)	(2,2)	0	1
		(1,0)	(1,0)	(2,0)	0	1
				(1,1)	0	1
			(1,1)	(2,1)	0	1
			(2,0)	(2,1)	0	1
			(2,1)	(0,0)	1	1
				(1,1)	0	1
		(1,0)	(2,1)	(2,2)	0	1
			(2,2)	(1,0)	1	1
		(1,1)	(1,1)	(2,2)	0	1
			(2,0)	(0,0)	1	1
			(2,1)	(1,0)	1	1
			(2,2)	(2,0)	1	1
		(2,0)	(2,0)	(2,2)	0	1
			(2,1)	(1,0)	1	1
			(2,2)	(1,1)	1	1
		(2,1)	(2,1)	(2,0)	1	1
			(2,1)	(1,1)	1	1
			(2,2)	(2,1)	1	1
		(2,2)	(2,2)	(0,0)	2	1

Figure 14: Structure constants in $qH^*\mathrm{Gr}(r,k)$ for $r+k=4$. Note $N_{ab}^{c,d}(r,k) = N_{ba}^{c,d}(r,k)$.

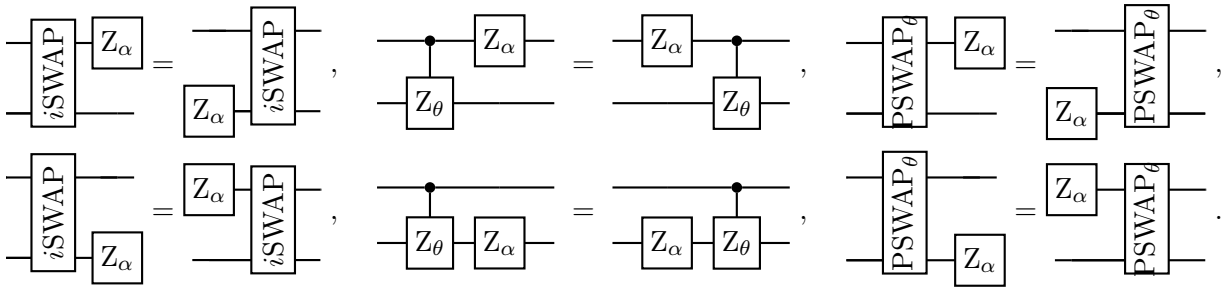
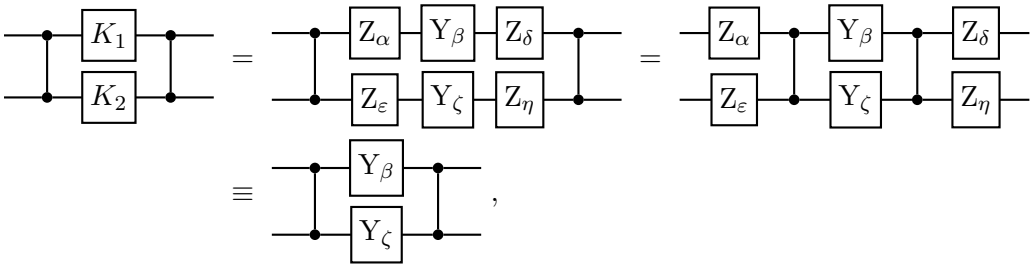


Figure 15: Leakiness relations for the other standard Quil gates

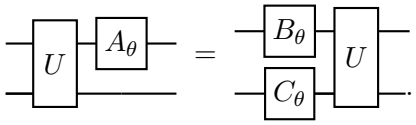
from which we may conclude the following for a generic pair of one-qubit gates K_1 and K_2:



where by $\equiv$ we intend local equivalence. This circuit therefore traces out at most a two-parameter subfamily of gates within $\mathfrak{A}_{C_2}$, which cannot be the image of a top dimensional set in $PU(4)$ and hence cannot have positive Haar volume.

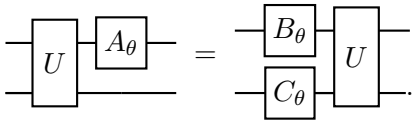
This kind of argument turns out to be flexible enough that the commutation property powering it deserves its own name:

Definition 87. A two-qubit gate U is said to *leak (on the first qubit wire)* when there are exponential families A_θ, B_θ, and C_θ such that

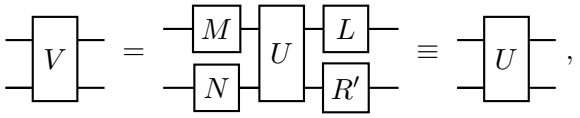


In fact, the other two-qubit gates in the Quil standard library are also leaky, as portrayed in Figure 15. This table has two remarkable features: first, that there are so many such relations, and second, that the single-qubit rotation is always a Z. We now show that at least the second of these is to be expected:

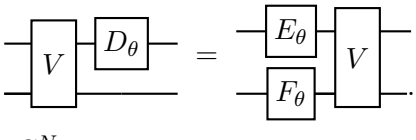
Lemma 88. *Leakiness is invariant under $\equiv_L$. Specifically, if U satisfies*



for some single-qubit exponential families A, B, C, and if V is given by

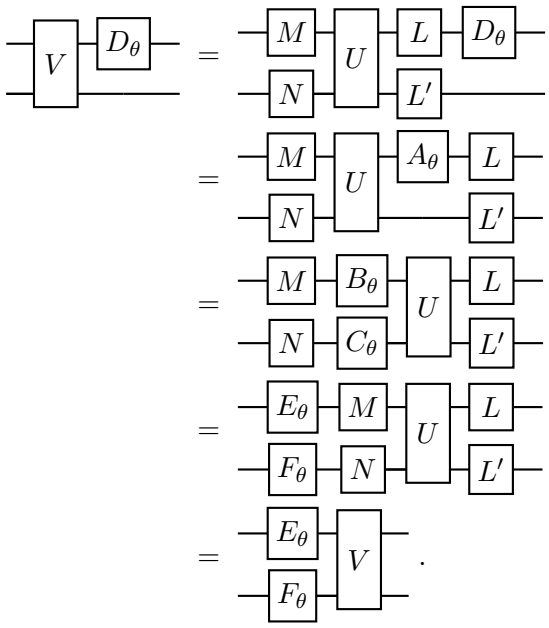


then we also have



for $D_\theta = A_\theta^L$, $E_\theta = B_\theta^M$, and $F_\theta = C_\theta^N$.

Proof. This is a direct calculation:

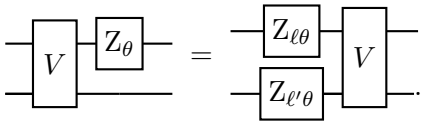


□

Remark 89. Suppose U is as in Lemma 88. By picking single-qubit operators L, M, and N with

$$A^L_{k\theta} = \mathrm{Z}_\theta, \qquad B^M_{k\theta} = \mathrm{Z}_{\ell\theta}, \qquad C^N_{k\theta} = \mathrm{Z}_{\ell'\theta},$$

we may replace U by V, also as in Lemma 88, for which we then have



In fact, if U has a second leakiness relation on the other qubit wire, transforming the single-qubit gate A'_θ into the local operator $B'_\theta \otimes C'_\theta$, one may reuse M and N: because $A \otimes 1$ and $1 \otimes A'$ commute, $B \otimes C$ and $B' \otimes C'$ must also commute, which forces B and B' (hence $B^M = \mathrm{Z}$ and $(B')^M$) to lie in the same one-parameter family and the same for C and C' (hence $C^N = \mathrm{Z}$ and $(C')^N$).

However, the first observation—that Smith, Curtis, and Zeng's standard library contains so many leaky gates—is much more of an accident.

Lemma 90. *A generic two-qubit gate does not leak.*

Proof. At the level of Lie algebras, a leaky gate U satisfies

$$(\mathfrak{su}(2) \oplus \mathfrak{su}(2)) \cap \mathrm{Ad}_U(\mathfrak{su}(2) \oplus 0) \neq \emptyset,$$

witnessed by anti-Hermitian matrices

$$h = \begin{pmatrix} c & a+bi \\ -a+bi & d \end{pmatrix},$$

and

$$h' \otimes h'' = \begin{pmatrix} (c_0+c_1)i & a_0+b_0i & a_0+b_1i & 0 \\ -a_0+b_0i & (-c_0+c_1)i & 0 & a_1+b_1i \\ -a_1+b_1i & 0 & (c_0-c_1)i & a_0+b_0i \\ 0 & -a_1+b_1i & -a_0+b_0i & -(c_0+c_1)i \end{pmatrix}$$

which in particular satisfy

$$h' \otimes h'' = U^\dagger \left(\begin{array}{c|c} h & 0 \\ \hline 0 & h \end{array}\right) U.$$

Elements of this product are computed by

$$(h' \otimes h'')_{i\ell} = \sum_{p=0}^{1} \sum_{j,k=1}^{2} \overline{U_{(2p+j)i}} h_{(2p+j)(2p+k)} U_{(2p+k)\ell},$$

which for a fixed value of U gives a linear system of *real* equations in the *real* unknowns specifying the elements of $\mathfrak{su}(2) \otimes 1$ and $\mathfrak{su}(2) \otimes \mathfrak{su}(2)$.

We claim that this system is generically of full rank, i.e., there is no solution but the trivial one. This system drops rank only when all determinants of all maximal subminors of the system vanish. As each determinant is an algebraic function on the real algebraic variety determined by $SU(4)$, if these do not all simultaneously vanish everywhere, then they generically do not simultaneously vanish. We therefore need only exhibit a point where the system has full rank for the conclusion to follow. Selecting $g = \sqrt{i\mathrm{SWAP}}$, we make the manual calculation that the above system of equations is satisfied only for $h = 0$, $h' = h'' = 0$.[26] □

Remark 91. The above mode of proof can be adapted to show that a generic entangler U has associated set P_U^2 of positive volume. We rely on the following pair of geometric facts:

Lemma 92 (Sard's theorem, [41]). *Let $U \subseteq \mathbb{R}^n$ be an open set, and let $f\colon U \to \mathbb{R}^m$ be differentiable. The image of f contains an open ball (hence is of positive volume) if and only if there exists a point $u \in U$ so that the derivative $D_u f$ is surjective.* □

Lemma 93 ([23, Section I.1]). *Let $f\colon V \to W$ be an algebraic morphism of connected algebraic varieties. For $w \in W$ in the image of f, the set $f^{-1}(w)$ is either all of W or of positive codimension (hence of zero volume in the real case).* □

We use these tools to analyze the algebraic function

$$\begin{aligned} \mathrm{cov}\colon\ SU(4) \times (SU(2)^{\otimes 2})^{\times 3} &\to SU(4) \\ (U, A, B, C) &\mapsto AU^{-1}BUC. \end{aligned}$$

Fixing U to be the B–gate, it is known that $\mathrm{cov}|_{U=\mathrm{B}}$ is surjective [50], hence Lemma 92 shows that there is a point (X, Y, Z) in the domain at which the derivative $D_{(X,Y,Z)}\mathrm{cov}|_{U=\mathrm{B}}$ is surjective. This is equivalent to the claim that the family of determinants $\det M_i D_{(X,Y,Z)}\mathrm{cov}|_{U=\mathrm{B}}$ do not all simultaneously vanish, where M_i ranges over the $\binom{18}{15}$ different (15×15)–minors. Each of these determinants can be thought of as an algebraic function in the gate used to restrict cov:

$$f_i(V) = \det M_i D_{(X,Y,Z)}\mathrm{cov}|_{U=V},$$

and the above claim becomes the claim that $(f_i)|_{V=\mathrm{B}}$ is not equal to the origin in $\mathbb{R}^{\binom{18}{15}}$. In turn, Lemma 93 says that $(f_i)^{-1}(0)$ has zero volume, so that $(f_i)(V)$ is nonvanishing generically in V, $D_{(X,Y,Z)}\mathrm{cov}|_{U=V}$ is surjective generically in V, and the image of $\mathrm{cov}|_{U=V}$ has positive volume generically in V.

Remark 94. On the other hand, leakiness is an essential part of quantum error correction codes: the very definition of a nonleaky multi-qubit gate means that a locally correctable error becomes a locally uncorrectable error after application of the entangler. This can severely dampen the functionality of stabilizer-type codes which rely on an understanding of the rate of error propagation.

[26] Alternatively, using Theorem 55, $\Pi(P_{\mathrm{DB}}^2)$ has positive volume, hence DB cannot be leaky, hence the linear system studied here has no solutions.

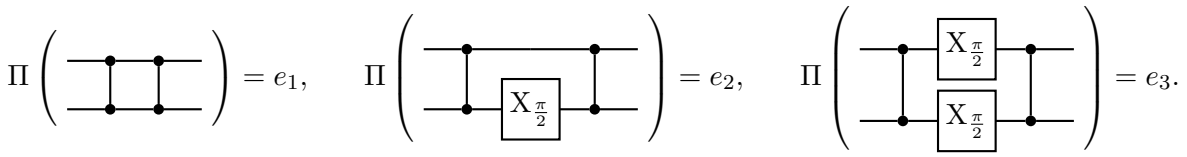


Figure 16: Realizations for the extremal vertices of $\Pi(P^2_{\mathrm{CZ}})$ as circuits.

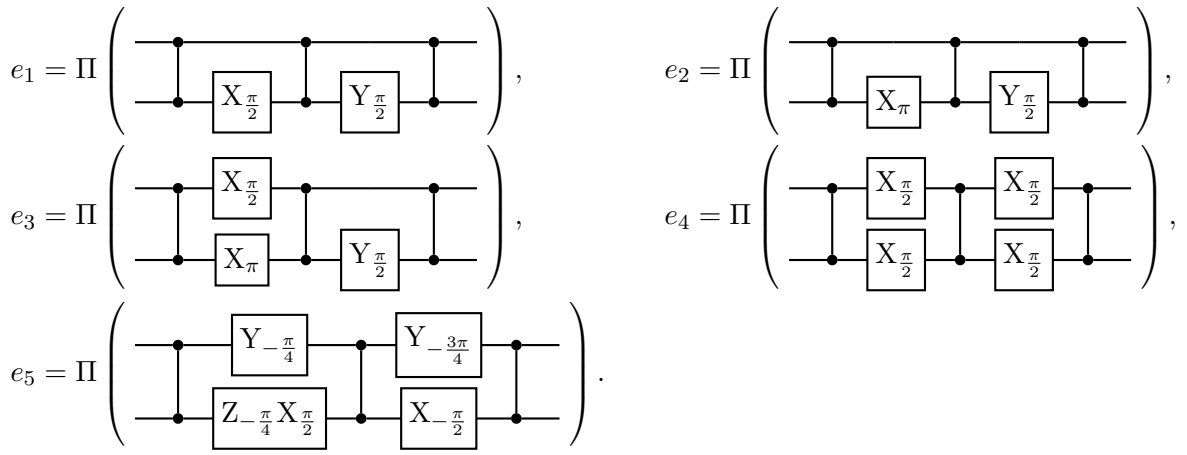


Figure 17: Realizations for the extremal vertices of $\Pi(P^3_{\mathrm{CZ}})$ as circuits.

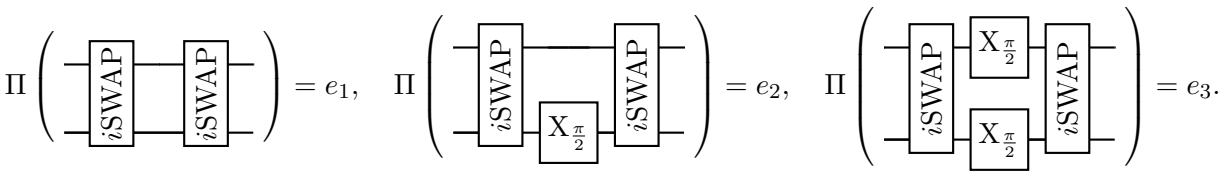


Figure 18: Realizations for the extremal vertices of $\Pi(P^2_{i\mathrm{SWAP}})$ as circuits.

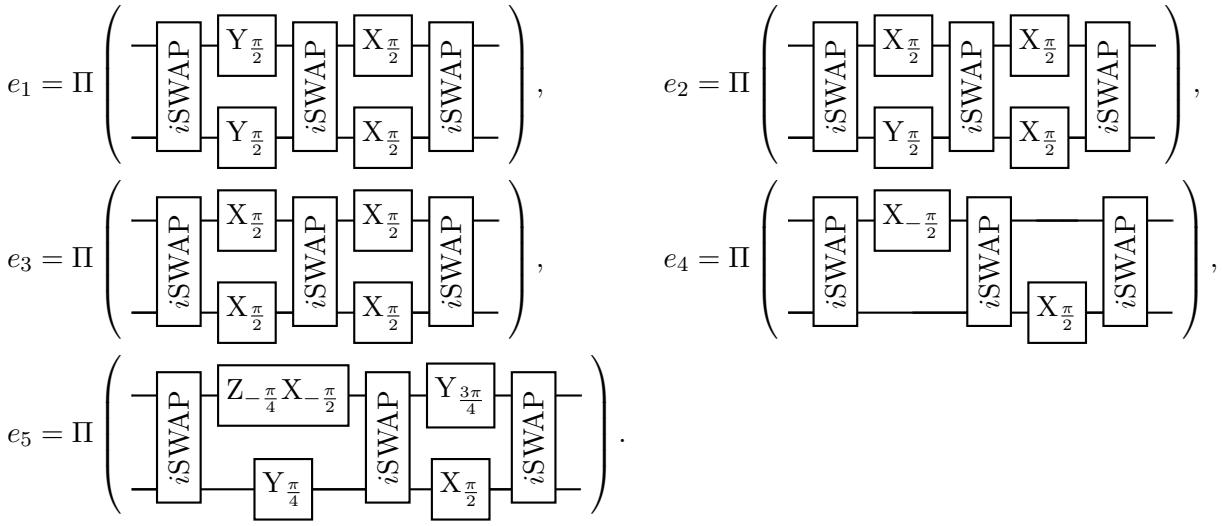


Figure 19: Realizations for the extremal vertices of $\Pi(P^3_{i\mathrm{SWAP}})$ as circuits.

$n = 0$:

$$\{(0,0,0,0)\}.$$

$n = 1$:

$$\left\{\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right)\right\}.$$

$n = 2$:

$$\left\{\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\quad (0,0,0,0),\quad \left(-\frac{1}{4},0,0,\frac{1}{4}\right)\right\}.$$

$n = 3$:

$$\left\{\left(-\frac{3}{8},-\frac{1}{8},\frac{1}{8},\frac{3}{8}\right),\quad \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right),\quad (0,0,0,0),\quad \left(-\frac{9}{24},-\frac{5}{24},\frac{7}{24},\frac{7}{24}\right),\right.$$
$$\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{3}{8},\frac{1}{8},\frac{1}{8},\frac{1}{8}\right),\quad \left.\left(-\frac{3}{8},0,0,\frac{3}{8}\right)\right\},$$

$$\left\{\left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\quad \left(-\frac{3}{8},-\frac{1}{8},\frac{1}{8},\frac{3}{8}\right),\quad \left(-\frac{5}{24},-\frac{5}{24},\frac{3}{24},\frac{7}{24}\right),\quad \left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\right.$$
$$\left.\left(-\frac{1}{8},-\frac{1}{8},\frac{1}{8},\frac{1}{8}\right)\right\}.$$

$n = 4$:

$$\left\{\left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left(-\frac{1}{2},\frac{1}{6},\frac{1}{6},\frac{1}{6}\right),\quad \left(-\frac{1}{2},-\frac{1}{6},\frac{1}{3},\frac{1}{3}\right),\quad \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right),\right.$$
$$(0,0,0,0),\quad \left.\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right)\right\},$$

$$\left\{\left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left(-\frac{2}{3},0,\frac{1}{3},\frac{1}{3}\right),\quad \left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\quad \left(-\frac{1}{6},-\frac{1}{6},0,\frac{1}{3}\right),\right.$$
$$\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{4},0,0,\frac{1}{4}\right),\quad \left(-\frac{1}{4},0,\frac{1}{8},\frac{1}{8}\right),\quad \left(-\frac{1}{12},-\frac{1}{12},0,\frac{1}{6}\right),$$
$$\left.\left(-\frac{1}{12},-\frac{1}{12},\frac{1}{12},\frac{1}{12}\right)\right\},$$

$$\left\{\left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\quad \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right),\quad \left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\right.$$
$$(0,0,0,0),\quad \left(-\frac{5}{8},\frac{1}{8},\frac{1}{8},\frac{3}{8}\right),\quad \left.\left(-\frac{3}{8},\frac{1}{8},\frac{1}{8},\frac{1}{8}\right)\right\},$$

$$\left\{\left(-\frac{5}{8},0,\frac{1}{4},\frac{3}{8}\right),\quad \left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right),\quad \left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\right.$$
$$\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{2},0,\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{8},0,\frac{1}{16},\frac{1}{16}\right),\quad \left(-\frac{1}{8},0,0,\frac{1}{8}\right),$$
$$\left(-\frac{1}{16},-\frac{1}{16},\frac{1}{16},\frac{1}{16}\right),\quad \left.\left(-\frac{1}{16},-\frac{1}{16},-\frac{1}{16},\frac{3}{16}\right)\right\}.$$

Figure 20: The extermal vertices of the polytopes making up the sets $P^n_{\sqrt{\mathrm{CZ}}}$, $n \leq 4$. The set $P^5_{\sqrt{\mathrm{CZ}}}$ exhausts the complement.

$$\left\{\left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\quad \left(-\frac{2}{3},0,\frac{1}{3},\frac{1}{3}\right),\quad \left(-\frac{1}{6},-\frac{1}{6},0,\frac{1}{3}\right),\right.$$
$$\left.(0,0,0,0),\quad \left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right)\right\},$$

$$\left\{\left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right),\quad \left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{2},\frac{1}{6},\frac{1}{6},\frac{1}{6}\right),\right.$$
$$\left.(0,0,0,0),\quad \left(-\frac{1}{2},-\frac{1}{6},\frac{1}{3},\frac{1}{3}\right)\right\}.$$

Figure 21: The extremal points of the two polytopes comprising $\Pi(P^2_{\mathrm{XY}})$.

$$\left\{\left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{6},-\frac{1}{6},0,\frac{1}{3}\right),\quad (0,0,0,0),\quad \left(-\frac{5}{8},-\frac{1}{8},\frac{3}{8},\frac{3}{8}\right),\right.$$
$$\left(-\frac{1}{2},0,\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{2},0,0,\frac{1}{2}\right),\quad \left.\left(-\frac{5}{8},0,\frac{1}{4},\frac{3}{8}\right)\right\},$$

$$\left\{\left(-\frac{1}{8},-\frac{1}{8},\frac{1}{8},\frac{1}{8}\right),\quad \left(-\frac{3}{8},\frac{1}{8},\frac{1}{8},\frac{1}{8}\right),\quad \left(-\frac{1}{2},\frac{1}{8},\frac{1}{8},\frac{1}{4}\right),\quad \left(-\frac{1}{4},-\frac{1}{4},\frac{1}{4},\frac{1}{4}\right),\right.$$
$$\left(-\frac{1}{2},0,\frac{1}{4},\frac{1}{4}\right),\quad \left(-\frac{1}{2},-\frac{1}{6},\frac{1}{3},\frac{1}{3}\right),\quad \left(-\frac{1}{8},-\frac{1}{8},-\frac{1}{8},\frac{3}{8}\right),\quad \left.\left(-\frac{1}{2},0,0,\frac{1}{2}\right)\right\}.$$

Figure 22: The extremal points of the two polytopes comprising $\Pi(P^2_{\mathrm{DB}})$.