Quantum Circuits for Quantum Channels

Raban Iten,‡ Roger Colbeck,† and Matthias Christandl‡‡

1ETH Zürich, 8093 Zürich, Switzerland
2Department of Mathematics, University of York, YO10 5DD, UK
3QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

(Dated: 26th September 2016)

We study the implementation of quantum channels with quantum computers while minimizing the experimental cost, measured in terms of the number of Controlled-NOT (C-NOT) gates required (single qubit gates are free). We consider three different models. In the first, the Quantum Circuit Model (QCM), in addition to the single qubit and C-NOT gates, qubits can be traced out. In the second (RandomQCM), we also allow external classical randomness. In the third (MeasuredQCM) we also allow measurements followed by operations that are classically controlled on the outcomes. We give near-optimal decompositions in almost all cases. Our main result is a MeasuredQCM circuit for any channel from \( m \) qubits to \( n \) qubits that uses at most one ancilla and has a low C-NOT count. We give explicit examples for small numbers of qubits illustrating the improvements offered by our schemes.

I. INTRODUCTION

Quantum channels, mathematically described by completely positive, trace-preserving maps, play an important role in quantum information theory because they are the most general evolutions quantum systems can undergo. Moreover, experimental groups can show their command over quantum systems consisting of a small number of qubits by demonstrating the ability to perform arbitrary quantum channels on them (see for example [1] and references therein). Instead of building a different device for the implementation of each quantum channel, it is convenient to decompose arbitrary channels into a sequence of simple-to-perform operations. In this paper we work with a gate set consisting of C-NOT and single-qubit gates, which is universal [2]. The implementation of a C-NOT gate is usually more prone to errors than the implementation of single-qubit gates. For example, the lowest achieved infidelities are by a factor of more than 10 smaller for single-qubit gates than for two qubit gates [3, 4]. This motivates using the number of C-NOT gates to measure the cost of a quantum circuit.

In this work we consider the construction of universal circuit topologies comprising gates from this universal set. A circuit topology [5, 6] corresponds to a set of quantum channels that have a particular structure but in which some gates may be free or have free parameters. Our aim is to find circuit topologies that minimize the C-NOT count but are universal in the sense that any channel from \( m \) to \( n \) qubits can be obtained by choosing the free parameters appropriately.

In this paper, we work with three different models. In the first we consider the quantum circuit model (QCM), in which we allow a sequence of C-NOT, single-qubit gates and partial trace operations on the qubits and any ancilla. In the second (RandomQCM) we allow the use of classical randomness in addition. In the third (MeasuredQCM), we allow the operations of the QCM as well as measurements and operations that are classically controlled on the measurement outcomes.

A related task is that of minimizing the C-NOT count for a given quantum channel (on a channel-by-channel basis). Although this appears quite different, we will show that it is related in the sense that our lower bounds on the number of C-NOT gates for circuit topologies that are able to generate all quantum channels of Kraus rank \( K \) are also lower bounds for almost all (in a mathematical sense) quantum channels of Kraus rank \( K \) individually, where the Kraus rank of a channel is defined as the smallest number of Kraus operators required to represent the channel and is equal to the rank of the corresponding Choi state [7].

The theory of decomposing operations on an isolated quantum system is quite developed. Considerable effort has been made to reduce the number of C-NOT gates required in the QCM for general unitary gates [8-12] and state preparation [13, 14], which are both special cases of isometries. Recently, it was shown that every isometry from \( m \) to \( n \) qubits can be implemented using about twice the C-NOT count required by a lower bound [13]. However, the task of minimizing the number of required C-NOT gates for the implementation of operations on open quantum systems, i.e., systems that are allowed to interact with the environment, has only been studied carefully in the case of channels on a single qubit [15]. Our work generalizes [16] to arbitrary channels from \( m \) to \( n \) qubits. In fact, we recover a very similar circuit topology (consisting of only one C-NOT gate) for single-qubit channels as given in [16] as a special case of our construction. We also note that Ansatzes for decompositions of arbitrary channels have been considered in [17, 18]. Our results imply that the Ansatz given in [17] (which works
in the RandomQCM) cannot work in general because it doesn’t have enough parameters. Further Ansatzes are given in [18], but it is not proven whether these work. In contrast, our constructive decompositions are proven to always work.

One approach to implement quantum channels is inspired by Stinespring’s theorem [19], which states that every quantum channel from \( m \) to \( n \) qubits can be implemented by an isometry from \( m \) to \( m + 2n \) qubits, followed by tracing out the \( m + n \) ancillas. The isometry can be decomposed into single qubit gates and \( 4^{m+n} \) C-NOTS to leading order [15]. Working in the quantum circuit model this C-NOT count is optimal up to a factor of about four in leading order [15]. However, one can significantly lower this C-NOT count and the required number of ancillas in more general models.

In the following we describe how to construct circuit topologies for quantum channels in the two aforementioned generalizations of the quantum circuit model. Our asymptotic results are summarized in Table I. In contrast to [20], we do not allow there to be a non zero failure probability for the channel implementation. First, we show that in the QCM with additional classical randomness for free the number of required ancillas can be reduced to \( m \) and the C-NOT count to \( 2^{2m+n} \) to leading order. Moreover, we derive a lower bound in this model, which shows that \( m \) ancillas are necessary and that our C-NOT count is optimal up to a factor of about two in leading order.

Second, we show that the MeasuredQCM offers further improvement. Our main result is a constructive decomposition scheme for arbitrary \( m \) to \( n \) channels, which leads to the lowest known C-NOT count of \( m \cdot 2^{m+1} + 2^{m+n} \) if \( m < n \) and of \( n \cdot 2^{m+1} \) if \( m \geq n \) (to leading order). Moreover, our construction allows us to implement \( m \) to \( n \leq m \) channels using only \( m + 1 \) qubits (i.e., one ancilla), and \( m \) to \( n > m \) channels using \( n \) qubits (which is clearly minimal, because the output of the channel is an \( n \)-qubit state). This generalizes the result that one ancilla is enough to perform arbitrary quantum channels on \( m \) qubits [21]. Note that the implementation of a channel decomposed as in [21] requires a lot of interaction and hence C-NOT gates. Indeed, adapting the decomposition scheme of [21] to our model, we find a C-NOT count of \( \Theta(2^{3m}) \) (in the worst case), which is exponentially worse than our C-NOT count of \( \Theta(m \cdot 2^{2m}) \).

Our construction also leads to low-cost implementations of \( m \) to \( n \) channels in the cases where \( 1 \leq m, n \leq 2 \) in Appendix [13]. These circuits are most likely to be of practical relevance for experiments performed in the near future. In particular, they show that every one to two channel can be implemented by 4 C-NOT gates, every two to one channel by 7 C-NOT gates and every two to two channel by 13 C-NOT gates. These counts are lower than those known previously. For example, the best known implementation of a two to two channel in the quantum circuit model requires about 580 C-NOTS.\(^3\) If we also allow classical randomness, this count reduces to 54 C-NOTS,\(^4\) which is over four times our C-NOT count of 13 when measurement and classical control are also allowed.

### II. Decomposition Allowing Classical Randomness

In the following, we consider how classical randomness can help implementing quantum channels. Since the set of all quantum channels from \( m \) to \( n \) qubits is convex, every \( m \) to \( n \) channel \( \mathcal{E} \) can be decomposed into a (finite) convex combination of extreme \( m \) to \( n \) channels \( \mathcal{E}_j \).\(^5\) Physically this means that, allowing classical randomness, the channel \( \mathcal{E} = \sum_{j=1}^{J} p_j \mathcal{E}_j \) can be implemented by performing the channel \( \mathcal{E}_j \) with probability \( p_j \) (and forgetting about the outcome \( j \)).

---

\(^1\) Note that some of the phrasing in [17] gives the impression that this Ansatz is proven to work in all cases; however the authors confirmed that this is not intended.

\(^2\) See Appendix [4] for more details.

| Model | Lower bound | Upper bound | Qubits |
|-------|-------------|-------------|--------|
| 1 [15] | \( \frac{1}{4}4^{m+n} \) | \( 4^{m+n} \) | \( m + 2n \) |
| 2 | \( \frac{1}{2}2^{2m+n} \) | \( 2^{2m+n} \) | \( m + n \) |
| 3 (\( m < n \)) | \( \frac{1}{8}(2^{m+n} - 2^{2m}) \) | \( m \cdot 2^{2m+1} + 2^{m+n} \) | \( n \) |
| 3 (\( m \geq n \)) | \( \frac{1}{2}2^{2m} \) | \( n \cdot 2^{2m+1} \) | \( m + 1 \) |

\(^3\) This is an an upper bound based on the Column-by-Column Decomposition for isometries [15].

\(^4\) This corresponds to the C-NOT count for a two to four isometry [12].

\(^5\) For a bound on the number of channels required see [24].
A. Upper bound

By Remark 6 of [7], every extreme channel from $m$ to $n$ qubits has Kraus rank at most $2^m$. Stinespring's theorem [19] then implies that in order to implement every extreme channel it suffices to be able to implement arbitrary isometries from $m$ to $m+n$ qubits. Decompositions of such isometries use $2^{2m+n}$ C-NOT gates to leading order [15]. In the following section, we derive a lower bound on the number of C-NOT gates and ancillas qubits required for $m$ to $n$ channels allowing classical randomness, which shows that the stated C-NOT count above is optimal up to a factor of two in leading order and optimal in the number of required ancillas.

B. Lower bound

Since classical randomness cannot help implementing extreme channels, a lower bound for extreme channels in the quantum circuit model is also a lower bound for channels in the model where we allow classical randomness. Since the set of extreme channels of Kraus rank $2^m$ is non empty [22], at least $m$ ancillas are required (using fewer ancillas, we could only generate channels of smaller Kraus rank). To find a lower bound on the number of C-NOT gates required for a quantum circuit topology for $m$ to $n$ extreme channels, we can use a parameter counting argument, similar to the argument used to derive a lower bound for unitaries [5, 6] or for channels in the quantum circuit model [13].

First, we count the number of (real) parameters required to describe the set of all extreme channels. Every quantum channel $\mathcal{E}$ from $m$ to $n$ qubits with Kraus rank $K$ can be represented by Kraus operators $A_i \in \text{Mat}_\mathbb{C}(2^m \times 2^m)$ such that $\sum_{i=1}^K A_i^\dagger A_i = I$ and $\mathcal{E}(X) = \sum_{i=1}^K A_i X A_i^\dagger$ (for all $X \in \text{Mat}_\mathbb{C}(2^m \times 2^m)$) [7]. By Theorem 5 of [7], a channel $\mathcal{E}$ is extreme if and only if all elements of the set $\{A_i A_j\}_{i,j \in \{1, 2, \ldots, K\}}$ are linearly independent. Each $m$ to $n$ channel $\mathcal{E}$ of Kraus rank $K = 2^m$ can be described by $K 2^m \times 2^m$ (complex) matrices $A_i$, which satisfy $4^m$ independent (note that the matrix $\sum_{i=1}^K A_i^\dagger A_i$ is Hermitian (conditions over $\mathbb{R}$). However, the Kraus representation is not unique. Two sets of Kraus operators $\{A_i\}_{i \in \{1, 2, \ldots, K\}}$ and $\{B_i\}_{i \in \{1, 2, \ldots, K\}}$ describe the same channel if and only if there exists a unitary $U \in U(2^m)$, such that $A_i = \sum_{j=1}^K (U)_{i,j} B_j$ [7]. Since a $2^m \times 2^m$ unitary matrix is described by $4^m$ parameters, we conclude that the set of all extreme channels form $m$ to $n$ qubits is described by $2^{2m+n+1} - 2^{2m+1}$ parameters. Note that the condition that the elements in $\{A_i A_j\}_{i,j \in \{1, 2, \ldots, K\}}$ must be linearly independent is an open condition for $K = 2^m$ and can therefore be ignored for the parameter counting.

A quantum circuit topology for extreme $m$ to $n$ channels must therefore introduce at least $2^{2m+n+1} - 2^{2m+1}$ parameters. Since C-NOT gates cannot introduce parameters into a circuit topology, all the parameters have to be introduced by the single-qubit gates. We work with the following single-qubit rotation gates

$$R_x(\theta) = \begin{pmatrix} \cos[\theta/2] & -i \sin[\theta/2] \\ -i \sin[\theta/2] & \cos[\theta/2] \end{pmatrix}; \quad (1)$$

$$R_y(\theta) = \begin{pmatrix} \cos[\theta/2] & - \sin[\theta/2] \\ \sin[\theta/2] & \cos[\theta/2] \end{pmatrix}; \quad (2)$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \quad (3)$$

For every unitary operation $U \in U(2)$ acting on a single qubit, there exist real numbers $\alpha, \beta, \gamma$ and $\delta$ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \quad (4)$$

A proof of this decomposition can be found in [23]. Note that (by symmetry) equation (4) holds for any two orthogonal rotation axes. The statement above can be represented as a circuit equivalence as follows.

```
U = R_z(\beta) R_y(\gamma) R_z(\delta)
```

The wire represents a qubit and the time flows from left to right. We ignore the global phase shift, because it is physically undetectable.

Let us consider $l$ qubits, $l - m$ of which start in a fixed (not necessarily product) state. We can act with a single-qubit gate on each qubit at the beginning of the quantum circuit topology (introducing $3l$ parameters). To introduce further (independent) parameters, we have to introduce C-NOT gates. Naively, one would expect that every C-NOT gate can introduce six new parameters by introducing a single-qubit gate after the control and one after the action-part of it. But by the following commutation relation,

```
-R_z R_y R_z = R_z R_y R_z
```

each C-NOT gate can introduce at most four parameters. Since we trace out $l - n$ qubits at the end of the circuit, the single-qubit gates on these qubits can not introduce any parameters into the circuit topology (which removes $3(l - n)$ parameters). We conclude that by using $r$ C-NOT gates we can introduce at most $4r + 3n$ parameters.
into the circuit topology. By the parameter count above, we require \( 4r + 3n \geq 2^{2m+n+1} - 2^{2m+1} \) or equivalently \( r \geq 2^{2m-1}(2^n - 1) - \frac{1}{2}n \) for a quantum circuit topology that is able to perform arbitrary extreme channels from \( m \) to \( n \) qubits.

The derived lower bound can be strengthened and made more general (see [24]): the set of all quantum circuit topologies that have fewer than \([2^{2m-1}(2^n - 1) - \frac{1}{2}n] \) C-NOT gates, together,\(^9\) are not able to approximate every \( m \) to \( n \) extreme channel arbitrarily well. In fact, they can only generate a closed set of measure zero\(^10\) in the smooth manifold of \( m \) to \( n \) extreme channels of Kraus rank \( 2^m \). Therefore, the lower bound holds for almost every \( m \) to \( n \) extreme channel of Kraus rank \( 2^m \) individually.

### III. DECOMPOSITION ALLOWING MEASUREMENT AND CLASSICAL CONTROL

We now move to the consideration of quantum circuit topologies in the model where allowing measurements (of single qubits in the computational basis) and classical control on the measurement results (and an arbitrary number of ancillas). In the following section we describe how to construct circuit topologies for arbitrary \( m \) to \( n \) channels of Kraus rank \( K \). We apply this scheme to extreme channels (which have Kraus rank at most \( 2^m \)), which leads to the C-NOT counts given in Table II.

#### A. Upper bound

Let \( \mathcal{E} \) be a channel from \( m \) to \( n \) qubits with Kraus rank \( K = 2^k \) and Kraus operators \( \{A_i\}_{i=1,2,...,K} \), \( A_i \in \text{Mat}_\mathbb{C}(2^n \times 2^m) \). We define the matrix \( V = [A_1; A_2; \ldots; A_K] \in \text{Mat}_\mathbb{C}(2^{n+k} \times 2^m) \), by stacking the Kraus operators.\(^11\) Since \( V^\dagger V = \sum_{i=1}^{K} A_i^\dagger A_i = I \), we can consider the matrix \( V \) as an isometry from \( m \) to \( n + k \) qubits (which corresponds to a Stinespring dilation of the channel \( \mathcal{E} \)). If \( n + k = m \) or \( k = 0 \), we can perform \( \mathcal{E} \) by implementing \( V \) and tracing out \( k \) qubits afterwards. In all other cases,\(^12\) we consider each half of the matrix \( V \) separately and define \( B_0 = [A_1; A_2; \ldots; A_K/2] \) and \( B_1 = [A_{K/2+1}; A_{K/2+2}; \ldots; A_K] \). By the QR-Decomposition, we can find unitary matrices \( Q_0, Q_1 \in U(2^{n+k-1}) \) and \( R_0, R_1 \in \{[T; 0; \ldots; 0] \in \text{Mat}_\mathbb{C}(2^{n+k-1} \times 2^m) \mid T \in \text{Mat}_\mathbb{C}(2^m \times 2^n) \} \) is upper triangular, such that \( Q_0 R_0 = B_0 \) and \( Q_1 R_1 = B_1 \). Note that \( Q_0 \) and \( Q_1 \) are not unique, indeed only the first \( 2^m \) columns are determined and we are free to choose the other columns (up to orthonormality). We can therefore consider them as isometries from \( m \) to \( n + k - 1 \) qubits. Summarized, we have \((Q_0 \oplus Q_1)[R_0; R_1] = V \) and hence, \( R := [R_0; R_1] = (Q_0 \oplus Q_1)V \) is an isometry. Therefore we can represent this decomposition as an equivalence of circuit topologies on \( n + k \) qubits, where the first \( n + k - m \) start in the state \( |0\rangle \), as follows

\[
\begin{array}{c}
|0\rangle \\
|0\rangle \\
|0\rangle \\
|0\rangle \\
|0\rangle \\
\vdots
\end{array}
\begin{array}{c}
R \\
R \\
R \\
R \\
R
\end{array}
\begin{array}{c}
|0\rangle \\
|0\rangle \\
|0\rangle \\
|0\rangle \\
\vdots
\end{array}
\begin{array}{c}
\tilde{V}
\end{array}
\]

where the backslash stands for a data bus of several (in this case \( m \)) qubits and \( \tilde{V}' \) is an isometry for two isometries in \( \text{Mat}_\mathbb{C}(2^{n+k-1} \times 2^m) \). The unfilled square denotes a uniform control.\(^13\) In the case above, we implement \( Q_0 \) if the most significant qubit is in the state \( |0\rangle \) and \( Q_1 \) if it is in the state \( |1\rangle \). Note that the gate \( R \) only acts non-trivially on the most significant and the \( m \) least significant qubits. In particular, the second to \((n + k - m)\)th qubit are still in the state \( |0\rangle \) after applying \( R \) (the lack of action of a gate on a particular qubit is indicated by use of a dotted line for that qubit). We can apply the same procedure of above to the isometries \( Q_0 \) and \( Q_1 \). We repeat this \( k \) times, until we end up with a quantum circuit topology of the form

\[\text{where each gate } R^i \text{ acts non-trivially only on the } i\text{th and the } m \text{ least significant qubits. If } m < n, \text{ we set } l = n - m \text{ and } k = l \text{ and if } m \geq n, \text{ we set } l = 1 \text{ and } k = n + k - m - 1. \text{ Recall that we can implement the channel } \mathcal{E} \text{ by applying the isometry } V \text{ and tracing out the first } k \text{ qubits afterwards.}\]

\(^9\) By combinatorial arguments, there are only finitely many different quantum circuit topologies consisting of a fixed number of C-NOT gates (w.l.o.g. we can consider circuit topologies in which we perform single-qubit gates on all qubits at the start of the circuit and two after each C-NOT gate).

\(^10\) Nevertheless, many interesting operations lie in this set. This is similar to the case of isometries, where, for example, the operation required to implement Shor’s algorithm lies in (the analogue of) this set \(\text{[12]}\).

\(^11\) For example, we have \([A_1; A_2] := \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}\).

\(^12\) Note that for all channels from \( m \) to \( n \) qubits of Kraus rank \( K = 2^k \) we have that \( n + k \geq m \) (cf. Lemma 6 of [23]).

\(^13\) The notation of ‘uniform control’ was introduced in [11]. Some authors also call these gates ‘multiplexed’ (for example, see [13]).
(which we can think about as performing measurements on them and forgetting the result). Since measurements commute with controls, we conclude that the following MeasuredQCM topology is able to perform all channels from \( m \) to \( n \) qubits of Kraus rank at most \( K \)

\[
\begin{array}{c}
|0\rangle \\
|0\rangle \\
\vdots \\
|0\rangle \\
|0\rangle^{\otimes l} \\
\end{array}

\begin{array}{c}
R^1 \\
\vdots \\
R^k \\
\hat{V} \\
\end{array}

m

\]

where \( m \) is the number of significant qubits. Note that the circuit above can be implemented with only one ancilla qubit by resetting it to the state \( |0\rangle \) after the measurements and saving the measurement outputs in classical registers

\[
\begin{array}{c}
0 \\
0 \\
\vdots \\
0 \\
0 \\
\end{array}

\begin{array}{c}
R^1 \\
\vdots \\
R^k \\
\hat{V} \\
\end{array}

m

\]

where the second symbol means that a \textsc{not} is performed on the first classical register if the output of the first measurement is one.

The construction above can be implemented on a system consisting of \( l + m \) qubits. The number of \	extsc{c-not} gates \( N(m, n, k) \) required for the MeasuredQCM topology above is \( k \cdot N_{\text{iso}}(m, m + 1) + N_{\text{iso}}(m, m + l) \). Working out the different cases, we conclude that the number of \	extsc{c-not} gates required for a quantum channel from \( m \) to \( n \) qubits of Kraus rank \( 2^k \) is \( N(m, n, k) = N_{\text{iso}}(m, n) \) if \( k = 0 \), \( N(m, n, k) = N_{\text{iso}}(m, m) \) if \( n + k = m \) and otherwise

\[
N(m, n, k) \leq \begin{cases} k \cdot N_{\text{iso}}(m, m + 1) + N_{\text{iso}}(m, n) & \text{if } m < n, \\ (k + n - m) \cdot N_{\text{iso}}(m, m + 1) & \text{if } m \geq n \end{cases}
\]

where \( N_{\text{iso}}(m, n) \) denotes the number of \textsc{c-not} gates required for an \( m \) to \( n \) isometry. If \( n \) is large, we have \( N_{\text{iso}}(m, n) \approx 2^m + n \) (for a more precise count, see \cite{13}).

Note that the main idea behind our construction and the requirement of at most one ancilla is general: any decomposition scheme for isometries (including with other universal gate sets, e.g. \cite{14}) can be applied to \( R^1, R^2, \ldots, R^k \) and \( \hat{V} \) arising in the decomposition.

\section{Lower bound}

We expect that allowing measurement and classical controls cannot help implementing isometries. Since isometries are special cases of channels, we expect further that a MeasuredQCM topology for \( m \) to \( n \) channels requires \( \Omega(2^m + n) \) \textsc{c-not} gates if \( m < n \) and \( \Omega(4^n) \) \textsc{c-not} gates if \( m > n \) \cite{13}. Since the proof of this fact is quite technical and uses similar arguments as used to derive the lower bound for extreme channels above, we defer it to Appendix \ref{sec:lower-bound}. The result is summarized in Table \ref{table:kraus-rank}

Note that the lower bound for the case where \( m > n \) is quite weak and it would be interesting to improve it in future work.

\section{Acknowledgements}

We acknowledge financial support from the European Research Council (ERC Grant Agreement no 337603), the Danish Council for Independent Research (Sapere Aude) and VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059). R.C. acknowledges support from the EPSRC’s Quantum Communications Hub. The authors are grateful to Bryan Eastin and Steven T. Flammia, whose package \texttt{Qcircuit.tex} was used to produce the circuit diagrams. We thank Jonathan Home for helpful discussions.

\begin{thebibliography}{99}
\bibitem{1} J. T. Barreiro et al., Nature 470, 486 (2011).
\bibitem{2} A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A 52, 3457 (1995).
\bibitem{3} C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas, Phys. Rev. Lett. 117, 060504 (2016).
\bibitem{4} J. P. Gaebler et al., Phys. Rev. Lett. 117, 060505 (2016).
\bibitem{5} V. V. Shende, I. L. Markov, and S. S. Bullock, Phys. Rev. A 69, 062321 (2004).
\bibitem{6} V. V. Shende, I. L. Markov, and S. S. Bullock, in Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, 2004, p. 980.
\bibitem{7} M.-D. Choi, Linear Algebra and its Applications 10, 285 (1975).
\bibitem{8} E. Knill, LANL report LAUR-95-2225, \texttt{arXiv:quant-ph/9508006} (1995).
\bibitem{9} A. V. Aho and K. M. Svore, \texttt{quant-ph/0311008} (2003).
\bibitem{10} J. J. Vartiainen, M. M"ot"onen, and M. M. Salomaa, Phys. Rev. Lett. 92, 177902 (2004).
\bibitem{11} M. M"ot"onen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Phys. Rev. Lett. 93, 130502 (2004).
\bibitem{12} V. Bergholm, J. J. Vartiainen, M. M"ot"onen, and M. M.
Appendix A: Comparison of our work with the decomposition scheme for channels described in [21]

To compare our decomposition scheme for channels in the MeasuredQCM with the third decomposition scheme introduced in [21], we must adapt the latter to our model. The main aim of [21] was to show that one ancilla is sufficient to implement channels from $m$ to $n = m$ qubits in a model where measurement and classical controls were allowed; a particular universal gate library was not considered. The scheme works by decomposing a quantum channel on $m$ qubits of Kraus rank $K$ into a sequence of (at most) $K - 1$ two-outcome measurements on the $m$ qubits and one unitary operation on them.

In terms of our gate library, the two-outcome measurements can be performed with an isometry from $m$ to $m + 1$ qubits, which requires $2^4m$ C-NOT gates to leading order $12$. Since a unitary on $m$ qubits requires $4^m$ C-NOT gates to leading order $12$, we conclude that an $m$ to $m$ channel requires $\Theta(K \cdot 4^m)$ C-NOT gates using this technique. Therefore, the implementation of extreme channels of Kraus rank $2^m$ requires $\Theta(2^{3m})$ C-NOT gates (in the worst case).

Appendix B: Circuits for $m$ to $n$ channels for $1 \leq m, n \leq 2$

The decomposition scheme in the MeasuredQCM described in Section IIIA also leads to low-cost circuits for extreme $m$ to $n$ channels for small $m$ and $n$. In the following, we demonstrate how to find circuits for $m$ to $n$ channels in the cases where $1 \leq m, n \leq 2$.

1 to 2 channels—An extreme channel from one to one qubit (which is of Kraus rank at most two) can be implemented by performing a one to two isometry followed by tracing out the first qubit. We use the circuit topology for one to two isometries which was derived in Appendix B1 of [15].

![Circuit for 1 to 2 channels]

$$
\begin{array}{c}
|0\rangle \\
U & R_y & U
\end{array}
$$

Since controls commute with measurements, the circuit topology above simplifies to the following.

$$
\begin{array}{c}
|0\rangle \\
U & R_y & U
\end{array}
$$

Therefore, one C-NOT gate is enough to implement one to one channels. A similar circuit topology was first derived in [10].

1 to 2 channels—We do the decomposition exactly as described in the general case in Section IIIA. This leads to a circuit topology of the form

$$
\begin{array}{c}
|0\rangle \\
V & U
\end{array}
$$

where $V$ is a 1 to 3 isometry corresponding to a Stinespring dilation of the implemented channel and $R$ and $V'$ denote 1 to 2 isometries. We use the circuit topology for one to two isometries given in Appendix B1 of [15] (consisting of two C-NOT gates). Therefore, a extreme channels from one to two qubits (of Kraus rank at most two) requires $2 \cdot N_{\text{iso}}(1,2) = 4$ C-NOT gates.

2 to 1 channels—A channel from two qubits to one qubit of Kraus rank at most four can be implemented by an isometry from two to three qubits and tracing out the first two qubits afterwards. We do the first few steps of the decomposition of an two to three isometry as in Appendix B2b of [15]. This leads to the circuit topology

$$
\begin{array}{c}
|0\rangle \\
A_0 & R_y & \bar{B}
\end{array}
$$

where $A_0$ and $\bar{B}$ are two qubit unitaries. We can use a technical trick introduced in Appendix B of [15] to save
By Theorem 14 of [13], we can decompose the gate $A_0$ into a part (which we denote by $\hat{A}_0$) consisting of two C-NOT gates (and single-qubit gates) and a diagonal gate $\Lambda$.

Note that we reversed the gate order of the circuit given in Theorem 14 of [13], such that the diagonal gate is performed after the gate $\hat{A}_0$. We commute the diagonal gate $\Lambda$ to the right and merge it with the gate $\tilde{B}$ (and call the merged gate $\hat{B}$). Therefore, and since controls commute with measurements, the circuit topology given above is equivalent to the following.

We decompose the uniformly controlled $R_y$ gates as described in Theorem 8 of [13]. Noting that 2 C-NOT gates cancel out each other, we get the following circuit topology.

We can further save one C-NOT gate in the decomposition of the gate $\hat{B}$. By [5, 6], we have the following equivalence of circuit topologies.

Substituting this circuit into the second to last one, we find a circuit topology for channels from two qubits to one qubit of Kraus rank at most four to three isometry arising in the decomposition described in Section IIIA as described above in the case of two to one channels, we find the following circuit for (extreme) two to two channels of Kraus rank at most four.

where $\hat{V}$ denotes the second two to three isometry arising in the decomposition described in Section IIIA. We can merge the gate $\hat{B}$ into $\hat{V}$, which leads to

where $\tilde{V}$ is a two to three isometry. Therefore, we can again apply the decomposition scheme described above for two to one channels to $\hat{V}$. Since we do not measure the third qubit at the end of the circuit, we use 8 C-NOT gates to decompose the gate $\hat{V}$. We conclude that we can decompose any channel from two to two qubits of Kraus rank at most four (and hence, in particular, any extreme two to two channel) with at most 13 C-NOT gates.

### Appendix C: Lower bound for isometries in the MeasuredQCM

We give a lower bound on the number of C-NOT gates required for a MeasuredQCM topology that is able to generate all isometries from $m$ to $n$ qubits using the basic gate library comprising arbitrary single qubit unitaries and C-NOT. A lower bound for $m$ to $n$ isometries in the quantum circuit model was already given in [12]. However, here we work in a more general model than that of [12], since we allow measurements and classical controls (and an arbitrary number of ancillas, each of which start in the state $|0\rangle$).

Any MeasuredQCM topology for $m$ to $n$ isometries consisting of $p \geq n$ qubits has the following form

where $k := p - n$ and we can think of $Q_i$ as the set of $(p + 1 - i)$-qubit unitaries that can be generated by the
corresponding quantum circuit topology. In other words, there is a first quantum circuit topology (perhaps with free parameters), followed by a measurement, then a classically controlled quantum circuit topology conditioned on the outcome, followed by a second measurement and so on. Note that the reuse of a qubit after a measurement can be incorporated into the above form by adding an additional ancilla qubit and copying the measurement outcome there.

**Theorem 1 (Lower bound in the MeasuredQCM)**
A MeasuredQCM topology that is able to generate all isometries from $m$ to $n \geq m$ qubits using ancillas initialized in the state $|0\rangle$ has to consist of at least $\lceil \frac{1}{6} (2^{m+n+1} - 2^{2m} - 3m - 1) \rceil$ C-NOT gates.

**Remark 1** The lower bound given in Theorem 1 is by a constant factor of $\frac{7}{8}$ (to leading order) lower than the one for isometries in the quantum circuit model of $\lceil \frac{1}{7} (2^{m+n+1} - 2^{2m} - 2n - m - 1) \rceil$ C-NOT gates [13].

Intuitively, the use of ancillas, measurements and classical controls should not be helpful for implementing isometries. Therefore, we expect that the lower bound given in Theorem 1 can be improved.

Since isometries from $m$ to $n$ qubits are special cases of $m$ to $n \geq m$ channels, we get the following Corollary.

**Corollary 2** A MeasuredQCM topology that is able to generate all channels from $m$ to $n \geq m$ qubits has to consist of at least $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - 3m - 1) \rceil$ C-NOT gates.

Moreover, we find the following lower bound for $m$ to $n < m$ channels.

**Corollary 3** A MeasuredQCM topology that is able to generate all channels from $m$ to $n < m$ qubits has to consist of at least $\lceil \frac{1}{6} (4^n - 3n - 1) \rceil$ C-NOT gates.

**Proof.** Assume to the contrary that there exists a MeasuredQCM topology consisting of fewer than $\lceil \frac{1}{6} (4^n - 3n - 1) \rceil$ C-NOT gates that is able to generate all channels from $m$ to $n < m$ qubits. Such a topology must, in particular, be able to implement all $n$-qubit unitaries from the first $n$ input qubits to the $n$ output qubits (independently of the state of the other $m-n$ input qubits).

We can turn this topology into a MeasuredQCM topology for unitaries on $n$ qubits by fixing the state of the last $m-n$ input qubits to $|0\rangle$. But such a topology cannot exist by Theorem 1.

Before giving the proof of Theorem 1, we sketch the idea. We start with a circuit topology of the form $[C1]$ consisting of $p \geq n$ qubits, where $p - m$ of them are initially in the state $|0\rangle$, and assume that it is able to generate all isometries from $m$ to $n$ qubits. In principle, one would expect that a circuit topology controlled on one (randomized) classical bit can introduce twice as many parameters as the circuit topology itself. Therefore, in general, controlling on the measurement result can help to reduce the C-NOT count (as we saw in Section III A). However, in the special case where we want to implement isometries, the classical control cannot increase the number of introduced parameters. The reason for this is related to the fact that the distribution of the measurement outputs are independent of the input state of the isometry. The precise statement is given in the following Lemma.

**Lemma 4 (Independence of measurement results)**
Assume that the whole circuit in $[C1]$ performs an isometry from $m$ to $n$ qubits for a certain choice of the free parameters of the MeasuredQCM topology. Then the distribution of the measurement outcomes is independent of the input state of the isometry.

**Proof.** It suffices to show this for all non-orthogonal states. Take two non-orthogonal input states $|\psi_0\rangle$ and $|\psi_1\rangle$ and assume to the contrary that there exists a measurement $M$ in $[C1]$, whose output distribution is different depending on which of these states is input. Let $P$ be the distribution over the outcomes for $M$ if we choose the input state $|\psi_0\rangle$, and $Q$ be the analogous probability distribution if we choose the input state $|\psi_1\rangle$.

Since we are implementing an isometry, the output states $|\psi_0'\rangle := V |\psi_0\rangle$ and $|\psi_1'\rangle := V |\psi_1\rangle$ can be turned back into $|\psi_0\rangle$ and $|\psi_1\rangle$. If we repeat this procedure $t$ times, then, the distribution of outcomes for $M$ is either the i.i.d. distribution $P^\times t$ or the i.i.d. distribution $Q^\times t$. Since $Q \neq P$ by assumption, these two distributions can be distinguished arbitrarily well for large $t$. This contradicts the fact that in any measurement procedure the maximum probability of correctly guessing which of these states is given as an input is $\frac{1}{2} [1 + D(|\psi_0'\rangle \langle \psi_0'|, |\psi_1'\rangle \langle \psi_1'|)] < 1$, where $D$ is the trace distance.

To handle the independence of the measurement distributions on the input state, it is useful to introduce the concept of postselection (see also [27]). We introduce the Postselected Quantum Circuit Model (PostQCM for short) as a modification of the QCM to include also single-qubit projectors onto the states $|0\rangle$ and $|1\rangle$ at the end of the circuit. Note that the single-qubit projectors correspond to linear maps that are not unitary. We say that a PostQCM topology with associated total linear map $C$ implements the isometry $V$, if $C = eV$, where $e \neq 0$ is some complex number.

We say that a PostQCM topology corresponds to a MeasuredQCM topology of the form $[C1]$, if it can be obtained from $[C1]$ using the following procedure.

\textbf{14} If all non-orthogonal states have the same distribution, then all states do, since the distribution for two orthogonal states $|\psi_0\rangle$ and $|\psi_1\rangle$ must then agree with that of any third state $|\psi\rangle$ that is not orthogonal with both.

\textbf{15} Note that this is equivalent to a measurement in the $\{|0\rangle, |1\rangle\}$ basis and postselecting on one of the outcomes.
every measurement is replaced by a single-qubit projector (onto either |0⟩ or |1⟩). Then all classical controls are removed. Finally we move the single-qubit projectors to the end of the circuit. Note that the number of single-qubit gates and C-NOTs of a circuit topology of the form (C1) is the same as that of the PostQCM topology formed by making these replacements.

**Lemma 5** The set of isometries that can be generated by a MeasuredQCM topology of the form (C1) is a subset of the set of isometries that can be generated by all the corresponding PostQCM topologies together.

**Proof.** Assume that an isometry V can be generated by a MeasuredQCM topology of the form (C1) for a certain choice of its free parameters. Hence, by Lemma 4 the distribution of the measurement outputs are independent of the input state of the isometry. Therefore, the circuit must perform the isometry independent of the measurement outputs and hence we can choose and fix an arbitrary output which occurs with nonzero probability. In other words, we can replace the measurements in (C1) with single-qubit projectors onto |0⟩ if the probability to measure 0 is nonzero, and with single-qubit projectors on |1⟩ otherwise. Note that this circuit can still perform the isometry V. Removing the classical controls, which does not change the action performed by the whole circuit, we obtain a corresponding PostQCM topology that is able to generate V.

**Lemma 6** A PostQCM topology that has fewer than \(2^{n+m+1} - 2^{2m} - 1\) free parameters can only generate a set of measure zero of the set of all m to n isometries (where we identify isometries that only differ by a global phase).

**Proof.** The argument works similarly to the arguments used in [2] [3] [24]. Let us denote by C the linear map corresponding to the PostQCM topology. We can think of this map as sending a certain choice of d real parameters \((\theta_1, \ldots, \theta_d)\) of the PostQCM topology to the corresponding \(2^n \times 2^n\) matrix \(C(\theta_1, \ldots, \theta_d)\), which describes the whole action of the circuit. We restrict the domain of the free parameters to the set \(D \subset \mathbb{R}^d\), such that for all \((\theta_1, \ldots, \theta_d) \in D\) there exists an isometry V and a complex number \(c \neq 0\), such that \(C(\theta_1, \ldots, \theta_d) = cV\). We denote the set of one dimensional unitaries by \(U(1)\) and define the orbit space \(V_{m,n}/U(1)\), which corresponds to the set of all m to n isometries, after quotienting out the (physically undetectable) global phase. We denote the corresponding (smooth) quotient map by \(\pi : V_{m,n} \mapsto V_{m,n}/U(1)\) (cf. [24] for more details). Then, we define the smooth map \(T(\theta_1, \ldots, \theta_d) := \pi \circ \sqrt{2^{-d+1}C(\theta_1, \ldots, \theta_d)} : D \mapsto V_{m,n}/U(1)\). By Sard’s theorem, \(T(D)\) is of measure zero in \(V_{m,n}/U(1)\) if \(d < \dim(V_{m,n}/U(1)) = 2^{m+n+1} - 2^{2m} - 1\).

**Lemma 7** A PostQCM topology that consists of fewer than \([1/6 (2^{n+m+1} - 2^{2m} - 3m - 1)]\) C-NOT gates (and an arbitrary number of ancilla qubits initialized in the state \(|0⟩\)) can only generate a set of measure zero of the set of all m to n isometries.

**Proof.** We may assume \(n > 1\) (for \(m = n = 1\) the statement of the Lemma is trivial). By Lemma 6 we have left to show that a PostQCM topology consisting of fewer than \([1/6 (2^{n+m+1} - 2^{2m} - 3m - 1)]\) C-NOTs cannot introduce \(2^{m+n+1} - 2^{2m} - 1\) or more (independent) real parameters. Since single-qubit projections do not introduce parameters into the circuit, all parameters must be introduced by single-qubit gates. To relate the number of single-qubit rotations to the number of C-NOT gates, we use similar arguments to those used in Section II B to derive the lower bound for channels allowing classical randomness. We again use the commutation properties of C-NOT gates and single-qubit rotations, which show that a C-NOT can introduce at most four parameters. However, in contrast to Section II B we commute all single-qubit rotations to the left (instead of to the right) and use the fact that the first single-qubit rotation on an ancilla can introduce at most two parameters (because an ancilla qubit always starts in the state |0⟩ and two parameters are enough to describe an arbitrary single-qubit pure state). Note that, in general, the single-qubit rotations performed directly before a single-qubit projection have a non-trivial effect on the operation performed by the whole circuit. Thus, a PostQCM topology with q C-NOT gates and consisting of \(p \geq n\) qubits can introduce at most \(4q + 2(p - m) + 3m\) parameters. Note that we may assume \(q \geq p - m\), since otherwise, there exists a collection of ancilla qubits and output qubits (which are not input qubits) that are not quantum-connected to the m input qubits. Any unconnected output qubits that are not input qubits start in the state |0⟩ and always remain product with the other output qubits. For \(n > 1\), the set of isometries for which the output state always has a product form has fewer parameters than the set of arbitrary isometries, and is hence of measure zero. In the case that all the unconnected qubits are ancilla qubits, they have a trivial effect on the performed circuit and can be removed without affecting the action of the circuit. Therefore, a PostQCM topology with q C-NOT gates can introduce at most \(6q + 3m\) parameters and hence, a circuit topology consisting of fewer than \([1/6 (2^{n+m+1} - 2^{2m} - 3m - 1)]\) C-NOTs cannot introduce \(2^{m+n+1} - 2^{2m} - 1\) or more parameters.

**Proof of Theorem 1** Consider a MeasuredQCM topology of the form (C1) consisting of fewer than

---

16 This follows from a simple statement in graph theory, that a connected graph must have at least \(V - 1\) edges, where \(V\) denotes the number of vertices of the graph.

17 If all output qubits are not quantum connected to the input qubits, the PostQCM topology can generate only a fixed output state independent on the input state, and hence is not able to perform any isometry.
\[ \left( \frac{1}{n} \left( 2^{n+m+1} - 2^{2m} - 3m - 1 \right) \right) \text{ C-NOT gates. Since each of the corresponding PostQCM topologies consists of the same number of C-NOT gates, each can only generate a set of measure zero in the set of all } m \text{ to } n \text{ isometries by Lemma } \#	ext{. Since the MeasuredQCM topology } \text{ has at most } 2^k \text{ corresponding PostQCM topologies, the set of isometries that can be generated by all corresponding PostQCM topologies together is still of measure zero. The theorem then follows from Lemma } \#	ext{ and the fact that a subset of a set of measure zero is again of measure zero.} \]