Quadratic Form Expansions for Unitaries

Quadratic Form Expansions for Unitaries

Niel de Beaudrap[1], Vincent Danos[2], Elham Kashefi[3], Martin Roetteler[4]

[1] IQC, University of Waterloo
[2] School of Informatics, University of Edinburgh
[3] Laboratoire d'Informatique de Grenoble
[4] NEC Laboratories America, Inc.

Abstract. We introduce techniques to analyze unitary operations in terms of *quadratic form expansions*, a form similar to a sum over paths in the computational basis when the phase contributed by each path is described by a quadratic form over $\mathbb{R}$. We show how to relate such a form to an entangled resource akin to that of the one-way measurement model of quantum computing. Using this, we describe various conditions under which it is possible to efficiently implement a unitary operation U, either when provided a quadratic form expansion for U as input, or by finding a quadratic form expansion for U from other input data.

1 Introduction

In the one-way measurement model [1,2], quantum states are transformed using single-qubit measurements on an entangled state, which is prepared from an input state by performing controlled-Z operations on pairs of qubits, including the input system and ancillas prepared in the $|+\rangle$ state. This model lends itself to ways of analyzing quantum computation which do not naturally arise in the circuit model, *e.g.* with respect to depth complexity [3] and discrete structures underlying unitary operations [6,8]. In this article, we present another result of this variety, by introducing *quadratic form expansions*.

Definition 1. *Let V be a set of n elements, and $I, O \subseteq V$ be (possibly intersecting) subsets. For a binary string $\mathbf{x} \in \{0,1\}^V$, let $\mathbf{x}_I$ and $\mathbf{x}_O$ be the restriction of $\mathbf{x}$ to those bit-positions indexed by elements of I and O, respectively. Then a* quadratic form expansion *is a matrix-valued expression of the form*

$$U \;=\; \frac{1}{C} \sum_{\mathbf{x} \in \{0,1\}^V} \mathrm{e}^{iQ(\mathbf{x})} \; |\mathbf{x}_O\rangle\langle\mathbf{x}_I| \,, \tag{1}$$

$U : \mathcal{H}_2^{\otimes I} \to \mathcal{H}_2^{\otimes O}$, where Q is a real-valued quadratic form on $\mathbf{x}$, and $C \in \mathbb{C}$.

Quadratic form expansions bear a formal similarity to a representation of a propagator of a quantum system in terms of a sum over paths. For a unitary U given as in (1), the outer product $|\mathbf{x}_O\rangle\langle\mathbf{x}_I|$ essentially specifies a particular coefficient, in the row indexed by the substring $\mathbf{x}_I$ and the column indexed by $\mathbf{x}_O$:

the amplitude of the transition between these standard basis states is proportional to a sum of complex units specified by $\mathbf{x}_I$, $\mathbf{x}_O$, and the auxiliary variables $v \in V \setminus (I \cup O)$.

Representations of unitary transformations as sums over paths is a well-developed subject in theoretical physics (see e.g. [4,5]); and a representation of unitaries as a sum over paths was used in [9] to provide a simple proof of $\mathsf{BQP} \subseteq \mathsf{PP}$.[1] However, there are also examples of quadratic form expansions which arise without explicitly seeking to represent unitaries in terms of path integrals: the quantum Fourier Transform over $\mathbb{Z}_{2^n}$ can readily be expressed in such a form, and quadratic form expansions for Clifford group operations are implicit in the work of Dehaene and de Moor [17], as we will describe in Section 3.3.

Given such an expression for a unitary U, we show how to obtain a decomposition of U in terms of operations similar to those used in the one-way measurement model. Using this connection, we demonstrate techniques involving quadratic form expansions to efficiently implement a unitary operator, when the coefficients of the quadratic form satisfies certain constraints related to "generalized flows" (or *gflows*) [8] or Clifford group operations. In particular, we exhibit an $O(n^3/\log n)$ algorithm to obtain a reduced *measurement pattern* (an algorithm in the one-way model) for Clifford group operations from a description of how they transform the Pauli group, based on the results of [17].

2 Connection to the one-way model

2.1 Review of the one-way model

We can formulate the one-way measurement model as a way of transforming quantum states in the following way. Given a state $|\psi\rangle$ on a set of qubits I (the *input system*), we embed I in a larger system V, where the qubits of $V \setminus I$ are prepared in the $|+\rangle \propto |0\rangle + |1\rangle$ state. We then perform entangling operations on the qubits of V, by performing controlled-Z (denoted $\wedge Z$) operations on some sets of pairs of qubits. (These operations are symmetric and commute with each other, and so we may characterize the entangling stage by a simple graph G whose vertices are the qubits of V: we call this the *entanglement graph* of the procedure.) We then measure each of the qubits of V in some sequence, except for some set of qubits $O \subseteq V$ (the *output subsystem*) which will support a final quantum state. We may represent the measurement result for each qubit v by a

[1] Unitaries were expressed in [9] in terms of paths whose phase contributions are described by cubic polynomials over $\mathbb{Z}_2$; comments made in Section VI of that paper essentially anticipate quadratic form expansions with discretized coefficients. We describe how their techniques provide a means of constructing quadratic form expansions from circuits in Appendix A.

bit $\mathsf{s}_v \in \{0,1\}$ which indexes the orthonormal basis states of the measurement. The measurement basis for each qubit may depend on the results of previous measurements, but without loss of generality may be expressed in terms of a "default" basis which is used when all preceding measurements yield the result 0. Depending on the measurement results, a final Pauli operator may be applied to the qubits in the output subsystem O.[2]

In the original formulation of the one-way measurement model, the measurement bases were described by some axis of the Bloch sphere lying on the XY plane, which is sufficient for universal quantum computation. It is also easy to prove that restricting this to states which are an angle $\theta \in \frac{\pi}{4}\mathbb{Z}$ from the X axis is sufficient for approximately universal quantum computation [12]. While it is reasonable to extend beyond this for choices of measurement bases [7], we will only need to consider measurement bases from the XY plane.

2.2 Phase map decompositions from quadratic form expansions

Consider a unitary U given by a quadratic form expansion as in (1), where the quadratic form Q is given by

$$Q(\mathbf{x}) \;=\; \sum_{\{u,v\}\subseteq V} \theta_{uv} x_u x_v \;, \tag{2}$$

for some angles $\{\theta_{uv}\}_{u,v\in V}$, and where the sum includes terms for $u = v$. Note that $Q(\mathbf{x})$ can be expressed as an expectation value $\langle \mathbf{x}| \, H \, |\mathbf{x}\rangle$, where H is a 2-local diagonal operator:

$$H \;=\; \sum_{\substack{\{u,v\}\subseteq V \\ u\neq v}} \theta_{uv} \Big[|1\rangle\langle 1|_u \otimes |1\rangle\langle 1|_v \Big] \;+\; \sum_{v\in V} \theta_{vv} \, |1\rangle\langle 1|_v \;. \tag{3}$$

Then we may decompose U as follows:

$$\begin{aligned} U \;\propto \sum_{\mathbf{x}\in\{0,1\}^V} |\mathbf{x}_O\rangle\langle \mathbf{x}| \, \mathrm{e}^{iH} \, |\mathbf{x}\rangle\langle \mathbf{x}_I| \;&=\; \left[\sum_{\mathbf{y}\in\{0,1\}^V} |\mathbf{y}_O\rangle\langle \mathbf{y}| \right] \mathrm{e}^{iH} \left[\sum_{\mathbf{x}\in\{0,1\}^V} |\mathbf{x}\rangle\langle \mathbf{x}_I| \right] \\ &\propto \; R_O \, \mathrm{e}^{iH} \, P_I \;, \end{aligned} \tag{4}$$

where P_I is a unitary embedding which introduces fresh ancillas (indexed by $v \in I^{\mathsf{c}} = V \setminus I$) initialized to the $|+\rangle$ state, and R_O is a map projecting onto the $|+\rangle$ state for all qubits in $O^{\mathsf{c}} = V \setminus O$ (tracing those qubits out afterwards).

[2] The reason for using the same variables V, I, and O for these sets of (labels for) qubits as for the sets in Definition 1 will become apparent in the next section.

Equation (4) is a *phase map decomposition* [10] for U: that is, it expresses U in terms of a process of postselecting observables, as follows. Decompose H into terms H_O, H_1, and H_2, where H_O consists of the 1-local terms on the qubits of O, H_1 consists of the 1-local term on the remaining qubits, and H_2 contains the remaining terms from (3). We then have $U \propto R_O \, \mathrm{e}^{iH_O} \mathrm{e}^{iH_1} \mathrm{e}^{iH_2} P_I$. Note that e^{iH_O} and e^{iH_1} are simply single-qubit Z rotations applied to the elements of O and O^{c} respectively, where in each case the qubits v in those sets are rotated by an angle θ_{vv}. Then, the composite map $\tilde{R}_O = R_O \mathrm{e}^{iH_1}$ projects each the state of each qubit $v \in O^{\mathsf{c}}$ onto the vector $|0\rangle + \mathrm{e}^{-i\theta_{vv}} |1\rangle$ for each $v \in O^{\mathsf{c}}$. We then have $U = \mathrm{e}^{iH_O} \tilde{R}_O \, \mathrm{e}^{iH_2} P_I$, which is a decomposition of U into the preparation of some number of $|+\rangle$ states, followed by a diagonal unitary operator consisting of two-qubit (fractional) controlled-Z operations, followed by post-selection of states on the Bloch equator for $v \in O^{\mathsf{c}}$, and (unconditionally applied) single-qubit Z rotations on the remaining qubits. If $\theta_{uv} \in \{0, \pi\}$ for all distinct $u, v \in V$ and for $u = v \in O$, the above describes precisely the action of a measurement-based computation in which the qubits $v \in O^{\mathsf{c}}$ are measured in the eigenbases of observables of the form $M(-\theta_{vv}) = \cos(\theta_{vv}) X - \sin(\theta_{vv}) Y$, in the special case where all measurements result in the $+1$ eigenstate (which we may label with the bit $\mathsf{s}_v = 0$).

If we are able to extend the above into a complete measurement algorithm, with defined behavior when not all measurements yield a specific outcome, we obtain a measurement-based algorithm for U: we discuss this problem in the next section. Conversely, from every measurement based algorithm, we may obtain a quadratic form expansion:

Theorem 1. *Every unitary operator on n qubits may be expressed by a quadratic form expansion with $|I| = |O| = n$, and where the quadratic form has coefficients $\theta_{uv} \in \{0, \pi\}$ for all cross-terms $x_u x_v$ and $-\pi < \theta_{vv} \leqslant \pi$ for all terms x_v^2. Furthermore, any unitary can be approximated to arbitrary precision by such an expansion where we further require $\theta_{vv} \in \frac{\pi}{4}\mathbb{Z}$.*

Proof. From [11] (and using the notation of that article), the measurement pattern $X_v^{\mathsf{s}_u} M_u^{-\alpha} E_{uv} N_v$ performs the unitary transformation $J(\alpha) = \frac{1}{\sqrt{2}} \left[\begin{smallmatrix} 1 & \mathrm{e}^{i\alpha} \\ 1 & -\mathrm{e}^{i\alpha} \end{smallmatrix}\right]$ for $\alpha \in \mathbb{R}$, from the state space of a qubit u to that of a "fresh" qubit v. These operations generate $\mathsf{SU}(2)$, and generate a group dense in $\mathsf{SU}(2)$ if we restrict to $\alpha \in \frac{\pi}{4}\mathbb{Z}$, by [12].

For any n qubit unitary U, there exists a measurement pattern composed of such patterns together with two-qubit controlled-Z operations (which we denote $\wedge Z$) which implements U. Let G be the entanglement graph of this pattern, and I and O be the qubits defining the input space and output space (respectively) of the measurement pattern. By [6], in this measurement pattern, the probability of

every measurement resulting in the $+1$ eigenvalue (i.e. $\mathsf{s}_v = 0$ for all $v \in O^{\mathsf{c}}$) is non-zero. Then, $U \propto R_O \, \mathrm{e}^{iH} P_I$, where

$$H \;=\; \sum_{uv \in E(G)} \pi \Big[\, |1\rangle\langle 1|_u \otimes |1\rangle\langle 1|_v \, \Big] \;-\; \sum_{v \in O^{\mathsf{c}}} \alpha_v \, |1\rangle\langle 1|_v \;\; . \tag{5}$$

By (4), this yields a quadratic form expansion for U, with

$$Q(\mathbf{x}) \;=\; \sum_{uv \in E(G)} \pi x_u x_v \;-\; \sum_{v \in O^{\mathsf{c}}} \alpha_v x_v^2 \;\; . \tag{6}$$

For a quadratic form expansion approximating U, it is sufficient to consider measurement patterns approximating U using angles $\alpha_v \in \frac{\pi}{4}\mathbb{Z}$. □

2.3 Measurement Pattern Interpolation

As we remarked above, the connection from quadratic form expansions to phase map decompositions may allow us to obtain an implementation for U, provided we can determine how to adapt measurements in case the measurements for qubits $v \in O^{\mathsf{c}}$ do not all yield the result $\mathsf{s}_v = 0$.

In a measurement pattern performing N measurements, the computation may follow any of 2^N branches, corresponding to the different combinations of measurement results. Let us call the branch in which every measurement produces the result $\mathsf{s}_v = 0$ the *positive branch* of the measurement pattern.[3] Without loss of generality, we may restrict our attention to patterns where no classical feed-forward is required in the positive branch: then, the positive branch of a measurement pattern is characterized by the *geometry* (G, I, O) of the pattern (where G is the entanglement graph of the measurement algorithm, and $I, O \subseteq V(G)$ are the sets of qubits defining the input/output space of the pattern), and the angles $\mathbf{a} = \{\alpha_v\}_{v \in O^{\mathsf{c}}}$ defining the measurements to be performed.

To extend the description of the positive branch of a measurement algorithm into a *complete* measurement algorithm performing a unitary is the subject of the following problem:

Measurement Pattern Interpolation (MPI). *For input data* $(G, I, O, \mathbf{a})$*, describing a unitary embedding* U *as* the positive branch *of a measurement pattern with geometry* (G, I, O) *and performing measurements* $\mathbf{a}$*, determine if there a measurement pattern* $\mathfrak{P}$ *with geometry* (G, I, O) *which performs the transformation* U*.*

[3] This choice of terminology refers to all measurements yielding the $+1$ eigenvalues of their respective observables $M(-\theta_{vv})$.

This problem is open, and seems to be difficult in general. We may attempt to make the problem easier by considering a more restricted problem:

Generic Measurement Pattern Interpolation (GMPI). *For an input geometry (G, I, O), determine if there exist measurement patterns $\mathfrak{P}(\mathbf{a})$ parameterized by a choice $\mathbf{a}$ of measurement angles, each with geometry (G, I, O), such that the pattern $\mathfrak{P}(\mathbf{a})$ performs a unitary embedding for all $\mathbf{a}$.*

GMPI addresses, in an *angle-independent* manner, the subject of the structure of measurement patterns which perform unitary transformations. A special case of the GMPI which has been solved are those geometries (G, I, O) which have a "generalized flow" (or *gflow*), which are the "*yes*" instances of GMPI such that the patterns $\mathfrak{P}(\mathbf{a})$ yield maximally random outcomes on all of their measurements [8]. The following is the definition of gflows in [13], for measurements restricted to the XY plane:[4]

Definition 2. *Given a geometry (G, I, O) for a measurement pattern, a* gflow *is a pair $(g, \preccurlyeq)$, where g is a function from O^c to subsets of I^c and $\preccurlyeq$ is a partial order, such that the following conditions hold for all u and v in the graph G:*

$$v \in g(u) \implies u \prec v\,, \tag{7a}$$

$$v \in \mathrm{odd}(g(u)) \implies u \preccurlyeq v\,, \tag{7b}$$

$$u \in \mathrm{odd}(g(u))\,, \tag{7c}$$

where $\mathrm{odd}(S)$ is the set of vertices adjacent to an odd number of elements of S.

Here, $u \preccurlyeq v$ essentially represents, for two qubits u and v, that v is measured no earlier than u; a gflow then specifies an ordering in which the qubits are to be measured (with the function g providing a description of how to adapt later measurements). Mhalla and Perdrix [13] present an algorithm which determines if a geometry has a gflow in this sense in polynomial time, which in turn yields a polynomial time solution to the GMPI for that case. As a result, any instance of the MPI where the geometry (G, I, O) has a gflow can be efficiently solved.

A different special case of the Measurement Pattern Interpolation problem which has been solved is that where the measurement angles are restricted to multiples of $\frac{\pi}{2}$ (or slightly more generally, where the measurement observables are Pauli operations). In this case, as noted in [7], no measurement adaptations are necessary, and the corrections can be determined via the stabilizer formalism [16].

In the following section, we apply these solutions to special cases of the MPI to describe how to synthesize implementations for a unitary U given by a quadratic form expansion.

[4] The original definition of gflows in [8] also allows for YZ plane and XZ plane measurements, which do not play a role either in our analysis or in [13].

3 Synthesis via measurement pattern interpolation

In order to apply the partial solutions to the MPI described above, it will be useful to define the following:

Definition 3. *For a quadratic form expansion*

$$\frac{1}{C} \sum_{\mathbf{x} \in \{0,1\}^V} \mathrm{e}^{iQ(\mathbf{x})} \; |\mathbf{x}_O\rangle\langle \mathbf{x}_I| \quad \textit{where} \quad Q(\mathbf{x}) \; = \sum_{\{u,v\} \subseteq V} \theta_{uv} x_u x_v \;\; , \tag{8}$$

the geometry induced by the quadratic form *is a triple* (G, I, O)*, where* G *is a* weighted *graph with vertex-set* V*, edge-set* $\{uv \mid u \neq v \text{ and } \theta_{uv} \neq 0\}$*, and edge-weights* $W_G(uv) = \theta_{uv}/\pi$.

Because we can require $-\pi < \theta_{uv} \leqslant \pi$ for all $u, v \in V$, we may without loss of generality restrict G to have edge-weights $-1 < W_G(uv) \leqslant 1$. We will assume that this holds for the remainder of the article, and speak of edges being either of *unit weight* or *fractional weight*.

In this section, we consider the problem of synthesizing an efficient implementation of unitaries U in terms of the geometry induced by a quadratic form expansion for U by reduction to the solved cases of the Measurement Pattern Interpolation problem discussed in the previous section.

3.1 Measurement pattern synthesis via gflows

Consider a geometry (G, I, O) induced by a quadratic form expansion for a unitary embedding U, where G has only edges of unit weight: then (G, I, O) is also a geometry for a measurement pattern. To obtain a measurement pattern for U, it suffices to find a gflow for (G, I, O): in that case, by Theorem 2 of [8], for any choice of measurement angles $\mathbf{a} = \{\alpha_v\}_{v \in O^{\mathsf{c}}}$, we may consider the pattern

$$\left[\prod_{u \in O^{\mathsf{c}}}^{\succcurlyeq} \left(\bigotimes_{\substack{v \in \mathrm{odd}(g(u)) \\ v \neq u}} Z_v \right) \left(\bigotimes_{v \in g(u)} X_v \right) M_u^{\alpha_u} \right] \left[\prod_{u \sim v} E_{uv} \right] \left[\prod_{u \in I^{\mathsf{c}}} N_u \right] \tag{9}$$

where the left-hand product may be ordered right-to-left in any linear extension of the order $\preccurlyeq$, and $\sim$ denotes the adjacency relation of G. This pattern thus steers the reduced state after every measurement to the state which would occur if the result had been the $+1$ eigenvalue. Every branch of the pattern then performs the same operation as the positive branch, and so the pattern implements a unitary operation U. To obtain a pattern in standard form (with corrections

only on output qubits), it is sufficient to propagate the corrections to the left, absorbing them into the measurement bases.

In [13], an $O(n^4)$ algorithm is provided to determine whether or not a geometry (G, I, O) has a gflow where every qubit is to be measured in the XY plane (and obtain one in the case that one exists), where $n = |V(G)|$. The measurement pattern of (9) can be constructed in time $O(n^2)$ by first producing a pattern where corrections undo byproduct operations after each measurement, commuting these corrections to the end, and simplifying; the resulting pattern will have $O(n)$ operations each with complexity $O(n)$. Thus:

Theorem 2. *For a unitary embedding U given as a quadratic form expansion with geometry (G, I, O) with unit edge-weights, there is an $O(n^4)$ algorithm which either determines that (G, I, O) has no gflow, or constructs a measurement pattern consisting of $O(n^2)$ operations*[5] *implementing U (using measurement angles of arbitrary precision), where $n = |V(G)|$.*

3.2 Circuit synthesis via flows

A geometry (G, I, O) which has fractional edges lies, at first glance, outside of the domain of the Measurement Interpolation Problems described above. However, given a quadratic form expansion with such a geometry, we may still be able to synthesize a circuit for a unitary U represented by that expansion by considering *flows*, which correspond to gflows where the function g maps each vertex $v \in O^{\mathsf{c}}$ to a singleton set: we may say $(f, \preccurlyeq)$ is a flow if and only if $(g_f, \preccurlyeq)$ is a gflow, where $g_f(v) = \{f(v)\}$.

Geometries which have flows are a solvable special case of the GMPI, where the resulting measurement patterns are very "circuit-like". Specifically, the positive branch of a measurement pattern whose geometry has a flow can be represented by a circuit with the following characteristics [6]:

- edges of the form $v\, f(v)$ for $v \in O^{\mathsf{c}}$ correspond to $J(-\alpha_v)$ gates on some wire, separating two wire segments which we label v and $f(v)$;
- edges $uv \in E(G)$ for $u \neq f(v)$ and $v \neq f(u)$ correspond to $\wedge Z$ operations acting on the wire segments labelled by u and v;
- wires whose initial segments are labelled by vertices of I accept arbitrary input states, while those labelled by vertices $I^{\mathsf{c}} \setminus \mathrm{img}(f)$ take input $|+\rangle$.

In the above formulation, the edges of the form $v\, f(v)$ can be interpreted as implementing single-qubit teleportation, in which case a fully entangling unitary

[5] These operations may involve measurement angles of arbitrary precision. A corresponding approximate measurement pattern may use $O(n^2 + n\,\mathrm{polylog}(n/\varepsilon))$ operations by the Solovay-Kitaev Theorem [14], where ε is the precision of the coefficients of Q.

is important in order to transfer the information of the "source" qubit to the "target" qubit upon measurement. However, considering the analysis of [6], it is not important that the edges of the second kind above be fully entangling operations: using such edges to represent fractional powers of $\wedge Z$ will also yield unitary circuits. This motivates the following definition:

Definition 4. *Suppose (G, I, O) is a geometry of a quadratic form expansion for a unitary transformation U. We may say that $(f, \preccurlyeq)$ is a* fractional-edge flow *for (G, I, O) if it is a flow for that geometry, and for all $ab \in E(G)$ with $W_G(ab) < 1$, we have $f(a) \neq b$ and $f(b) \neq a$.*

If (G, I, O) has a fractional-edge flow, we may synthesize a circuit from a quadratic form expansion for U using the description above, where edges ab of fractional weight correspond to $\wedge Z^{W_G(ab)}$ gates on the wire segments labelled by a and b rather than simple $\wedge Z$ gates. We will make use the following easily verified Lemma to consider how to compose/decompose quadratic form expansions:

Lemma 1. *Let U_1, U_2 be matrices given by quadratic form expansions*

$$U_j \;=\; \frac{1}{C_j} \sum_{\mathbf{x} \in \{0,1\}^{V_j}} \mathrm{e}^{iQ_j(\mathbf{x})} \; \left|\mathbf{x}_{O_j}\right\rangle\!\left\langle \mathbf{x}_{I_j}\right| \; . \tag{10}$$

In the following, $C = C_1 C_2$, and sums are over $\{0,1\}^{V_1 \cup V_2}$.

(*i*) *If $V_1 \cap V_2 = I_2 = O_1$, then $U_2 U_1 \;=\; \frac{1}{C} \sum_{\mathbf{x}} \; \mathrm{e}^{\,iQ_1(\mathbf{x}) + iQ_2(\mathbf{x})} \; \left|\mathbf{x}_{O_2}\right\rangle\!\left\langle \mathbf{x}_{I_1}\right|$.*

(*ii*) *If V_1 and V_2 are disjoint, then $U_1 \otimes U_2 \;=\; \frac{1}{C} \sum_{\mathbf{x}} \; \mathrm{e}^{\,iQ_1(\mathbf{x}) + iQ_2(\mathbf{x})} \; \left|\mathbf{x}_{O}\right\rangle\!\left\langle \mathbf{x}_{I}\right|$, where $I = I_1 \cup I_2$ and $O = O_1 \cup O_2$.*

We prove the circuit construction given by inducting on the number of edges of fractional weight. For the base case, if (G, I, O) has no fractional-weight edges at all, we may synthesize a circuit for U as above, as it corresponds to a normal measurement pattern with a flow, and so falls under the analysis of [6]. We may then induct for geometries with fractional edge-weights if we can show we can decompose the geometry into ones with fewer fractional edge-weights.

For any arbitrary fractional edge $ab \in E(G)$ and each each $z \in O$, we may define $m(ab, z)$ to be the maximal vertex $v \in V(G)$ in the ordering $\preccurlyeq$ subject to z being in the orbit of v under f (that is, $z = f^{\ell}(v)$ for some $\ell \geqslant 0$), such that at least one of $v \preccurlyeq a$ or $v \preccurlyeq b$ holds. For a set $S \subseteq V(G)$, let $G[S]$ represent the subgraph of G induced by S (i.e. by deleting all vertices in G not in S). Then, define the following subgraphs of G, and corresponding geometries:

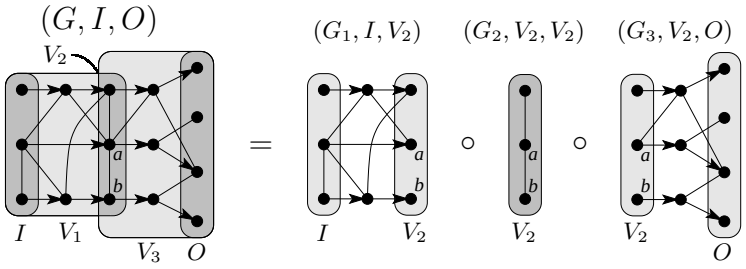

Fig. 1. Illustration of the decomposion of a quadratic form expansion about an edge ab, expressed in terms of geometries. V_2 is a set of maximal vertices under the constraint of being bounded from above, by the vertices a and b, in a partial order $\preccurlyeq$ associated with a fractional-edge flow. Arrows represent the action of the corresponding fractional-edge flow function, f.

- Let V_2 be the set of vertices $m(ab, z)$ for each $z \in O^{\mathsf{c}}$: it is easy to show that $a, b \in V_2$. Let $G_2 = G[V_2]$, and let $\mathcal{G}_2 = (G_2, V_2, V_2)$.
- Let V_1 be the set of vertices $u \in V(G)$ such that $u \preccurlyeq v$ for some $v \in V_2$; let $G_1 = G[V_1] \setminus \left\{uv \,\middle|\, u, v \in V_2\right\}$; and let $\mathcal{G}_1 = (G_1, I, V_2)$.
- Let V_3 be the set of vertices $u \in V(G)$ such that $u \succcurlyeq v$ for some $v \in V_2$; let $G_3 = G[V_3] \setminus \left\{uv \,\middle|\, u, v \in V_2\right\}$; and let $\mathcal{G}_3 = (G_3, V_2, O)$.

This decomposes the geometry (G, I, O) into three geometries with fractional-edge flows, as illustrated in Figure 1.

Let Q_1 be a quadratic form on $\{0,1\}^{V_1}$ consisting of the terms $x_u x_v$ of Q for $u \in V_1$ or $v \in V_1$, but not both; Q_2 be a quadratic form on $\{0,1\}^{V_2}$ consisting of the terms $x_u x_v$ of Q for *distinct* $u, v \in V_2$; and similarly let Q_3 be defined on $\{0,1\}^{V_3}$, and consist of the remaining terms of Q. Then Q_1, Q_2, and Q_3 define quadratic form expansions for some operations U_1, U_2, and U_3 (respectively) with geometries $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ (respectively).

- U_2 in particular will be a product of operations $\wedge Z^{W_G(uv)}$ for distinct $u, v \in V_2$, as it is a quadratic form expansion whose input and output indices coincide. Then U_2 can be represented as a circuit with a wire for each $u \in V_2$, with fractional controlled-Z gates $\wedge Z^{W_G(uv)}$ for each edge $uv \in E(G)$.
- Both $\mathcal{G}_1$ and $\mathcal{G}_3$ have fractional-edge flows, but fewer fractional edges than (G, I, O). By induction, U_1 and U_3 are also unitary embeddings, and have circuits with wire-segments connected by $J(\theta_v)$ gates (where θ_v are the coefficients of the terms x_v^2 in each quadratic form) and possibly fractional $\wedge Z$ gates (as in the case for U_2).
- In the circuits described above, the terminal wire-segments for U_1 and (a subset of) the initial wire-segments for U_3 have the same labels as the wires

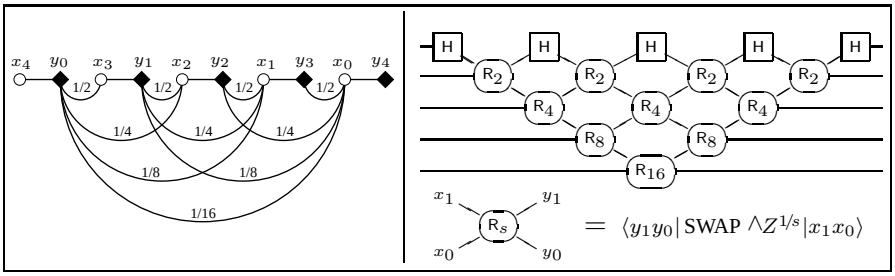

Fig. 2. The geometry for the quadratic form expansion of the QFT for $\mathbb{Z}_{32}$, and the corresponding circuit due to [21]. In the geometry (on the left), input vertices are labelled by circles, output vertices by lozenges, and fractional edges are labelled with their edge-weights.

for U_2 . The composite circuit for $U_3U_2U_1$ can then use these labels to arrive at a unified labelling of its' wire-segments.

Because $Q_1(\mathbf{x}_{V_1}) + Q_2(\mathbf{x}_{V_2}) + Q_3(\mathbf{x}_{V_3}) = Q(\mathbf{x})$ for all $\mathbf{x} \in \{0,1\}^V$ by construction, the composite operation $U_3U_2U_1$ can differ from U by at most a scalar factor by Lemma 1; so the circuit obtained implements the operation U.

In [13], an $O(kn)$ algorithm is provided to determine whether or not a geometry (G, I, O) has a flow, and obtain one if it exists, where $n = |V(G)|$ and $k = |O|$. For each edge uv, we may check whether one of $W_G(uv) = 1$ or $\big[u \neq f(v)$ and $v \neq f(u)\big]$ holds: if all edges satisfy this constraint, the circuit described above is well-defined. By iterating through the vertices of $V(G)$ in an arbitrary linear extension of $\preccurlyeq$, we may construct the circuit described above can be constructed in time $O(m)$, and the size of the resulting circuit will also be $O(m)$, where $m = |E(G)|$. By an extremal result [15], any geometry with a flow has $m \leqslant kn$: thus, the total running time of this algorithm is $O(kn)$.

In the case $|I| = |O|$, a flow function f is unique if it exists, by [20]; so in this case, if (G, I, O) has a flow but there is an edge $v\, f(v)$ of fractional weight, there is no fractional-weight flow for (G, I, O). We then have:

Theorem 3. *For a unitary transformation U given as a quadratic form expansion with geometry (G, I, O), there is an $O(kn)$ algorithm which either determines that (G, I, O) has no fractional-edge flow, or constructs a circuit consisting of $O(kn)$ operations*[6] *implementing U, where $n = |V(G)|$ and $k = |O|$.*

[6] These operations may consist of $J(\alpha)$ gates and fractional $\wedge Z$ gates of arbitrary precision. A corresponding circuit using a finite elementary gate set may be of size $O(kn\,\mathrm{polylog}(kn/\varepsilon))$ by the Solovay-Kitaev Theorem [14], where ε is the precision of the coefficients of Q.

Example. The Fourier Transform over $\mathbb{Z}_{2^n}$ is given by the matrix formula

$$\mathcal{F}_n \;=\; \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x},\mathbf{y}\in\{0,1\}^n} \mathrm{e}^{2\pi i \left[\sum_{h=0}^{n-1} 2^h x_h\right]\left[\sum_{j=0}^{n-1} 2^j y_j\right]/2^n} \,|\mathbf{y}\rangle\langle\mathbf{x}|\,, \qquad (11)$$

which is a quadratic form expansion; its quadratic form can be given by

$$Q(\mathbf{x},\mathbf{y}) \;=\; \sum_{h=0}^{n-1} \sum_{j=0}^{n-1-h} \frac{2^{(h+j)}}{2^{n-1}}\, \pi x_h y_j \;. \qquad (12)$$

This has a fractional-edge flow for all n. Figure 2 illustrates this geometry for $n = 5$, and the circuit (due to [21]) which may be synthesized from it.

3.3 Synthesizing measurement patterns for the Clifford group

If a quadratic form expansion has a geometry whose edges all have unit weight, and its' other coefficients are multiples of $\frac{\pi}{2}$, then it corresponds to the positive branch of a measurement pattern which measures only X or Y observables. A measurement pattern of this sort, if it performs a unitary operation, performs a Clifford group operation in particular.

An algorithm of Aaronson and Gottesman [19] can produce a circuit of size $O(n^2/\log n)$ in classical deterministic time $O(n^3/\log n)$ for a Clifford group operation U acting on n qubits, from a description of how U transforms Pauli operators by conjugation. By converting the circuit into a measurement-based algorithm, and performing the graph transformations of [18] to remove auxiliary qubits, we may obtain a pattern of at most $3n$ qubits[7] in time $O(n^4/\log n)$. Building on the results of [17], we show how to classically compute such a minimal pattern in time $O(n^3/\log n)$ by solving the MPI for a quadratic form expansion for U.

Obtaining a quadratic form expansion. For the sake of completeness, we outline the relevant results of [17]. Define the following notation for bit-flip and phase-flip operators on a qubit t out of a collection $\{1,\ldots,n\}$:

$$P_t \;=\; X_t\,, \qquad\qquad P_{n+t} \;=\; Z_t\,. \qquad (13)$$

Let $\mathrm{diag}(M) \in \mathbb{Z}_2^m$ represent the vector of the diagonal elements of any square boolean matrix M; and let $\mathbf{d}(M) = \mathrm{diag}\left(M^\top \left[\begin{smallmatrix} 0 & \mathbb{1}_n \\ 0 & 0 \end{smallmatrix}\right] M\right) \in \mathbb{Z}_2^{2n}$ for a $2n \times 2n$

[7] In [7], Clifford operations on n qubits are described as having minimal patterns for are described as requiring at most $2n$ qubits; however, this only holds up to local Clifford operations on the output qubits.

matrix M over $\mathbb{Z}_2$. Then, we may represent an n qubit unitary U by a $2n \times 2n$ boolean matrix C and a vector $\mathbf{h} \in \{0,1\}^{2n}$, whose coefficients are jointly given by

$$UP_tU^\dagger \;=\; i^{d_t(C)}\big(-1\big)^{h_t}\bigotimes_{j=1}^{n}\Big[Z_j^{C_{(n+j)t}}X_j^{C_{jt}}\Big] \tag{14}$$

for each $1 \leqslant t \leqslant 2n$. (Note that the factor of $i^{d_t(C)}$ is only necessary to ensure that the image of P_t is Hermitian, and does not serve as a constraint on the value of C as a matrix.) We will call an ordered pair $(C, \mathbf{h})$ a *Leuven tableau* for a Clifford group element U if it satisfies (14).[8]

Provided a Leuven tableau $(C, \mathbf{h})$ for a Clifford group operation U, [17] provides a matrix formula for U which we may obtain for U, as follows. Decompose C as a block matrix $C = \left[\begin{smallmatrix} E & F \\ G & H \end{smallmatrix}\right]$ with $n \times n$ blocks, and then find invertible matrices $\tilde{R}_1, \tilde{R}_2$ over $\mathbb{Z}_2$ such that $\tilde{R}_1^{-1}G\tilde{R}_2 = \left[\begin{smallmatrix} 0 & 0 \\ 0 & \mathbb{1}_r \end{smallmatrix}\right]$ for some $r < n$ (using *e.g.* the decomposition algorithm of [22] to obtain $\tilde{R}_1$ and $\tilde{R}_2$ in terms of elementary row operations). Then, define the matrices

$$\begin{bmatrix} \tilde{E}_{11} & \tilde{E}_{12} \\ \tilde{E}_{21} & \tilde{E}_{22} \end{bmatrix} \;=\; \tilde{R}_1^\top E \tilde{R}_2\,, \quad R_1 \;=\; \tilde{R}_1\,, \quad R_2 \;=\; \begin{bmatrix} \tilde{E}_{11}^{-1} & 0 \\ 0 & \mathbb{1}_r \end{bmatrix}^\top \tilde{R}_2^\top\,, \tag{15}$$

where $\tilde{E}_{11}$ is taken to be a block of size $(n-r) \times (n-r)$. We may then obtain the block matrices

$$\begin{bmatrix} \mathbb{1}_{n-r} & E_{12} & F_{11} & F_{12} \\ E_{21} & E_{22} & F_{21} & F_{22} \\ 0 & 0 & H_{11} & H_{12} \\ 0 & \mathbb{1}_r & H_{21} & H_{22} \end{bmatrix} \;=\; \begin{bmatrix} R_1^\top & 0 \\ 0 & R_1^{-1} \end{bmatrix} C \begin{bmatrix} R_2^\top & 0 \\ 0 & R_2^{-1} \end{bmatrix}\,, \tag{16}$$

and use these to construct the $n \times n$ boolean matrices

$$M_{br} \;=\; \begin{bmatrix} F_{11} + E_{12}H_{21} & E_{12} \\ E_{12}^\top & E_{22} \end{bmatrix}\,, \qquad M_{bc} \;=\; \begin{bmatrix} 0 & H_{21}^\top \\ H_{21} & H_{22} \end{bmatrix}\,. \tag{17}$$

Next, define

$$\begin{aligned} \mathbf{d}_{br} &= \operatorname{diag}(M_{br})\,, & \mathbf{d}_{bc} &= \operatorname{diag}(M_{bc})\,, \\ L_{br} &= \operatorname{lower}\big(M_{br} + \mathbf{d}_{br}\mathbf{d}_{br}^\top\big)\,, & L_{bc} &= \operatorname{lower}\big(M_{bc} + \mathbf{d}_{bc}\mathbf{d}_{bc}^\top\big)\,, \end{aligned} \tag{18}$$

[8] Note that the block matrix $\big[C^\top \;\mathbf{h}\big]$ is similar to a *destabilizer tableau* as defined in [19].

where $\mathrm{lower}(M)$ is the strictly lower-triangular part of a square matrix M (with all other coefficients set to 0). Finally, define $\Pi_r = \left[\begin{smallmatrix} 0 & 0 \\ 0 & \mathbb{1}_r \end{smallmatrix}\right]$ and $\Pi_r^\perp = \mathbb{1}_n - \Pi_r$ for the sake of brevity, and let[9]

$$\mathbf{t} \;=\; \left[\begin{smallmatrix} \mathbb{1}_n & 0 \end{smallmatrix}\right] \mathbf{h} \;+\; \mathrm{diag}\Big(\left[R_2^{-1}\Pi_r\right] L_{br} \left[R_2^{-1}\Pi_r\right]^\top \Big) \,, \tag{19}$$

$$\begin{aligned} \mathbf{h}_{bc} \;=\; \left[\begin{smallmatrix} 0 & R_2^{-\top} \end{smallmatrix}\right] \mathbf{h} \;+\; R_2^{-\top}\, \mathrm{diag}\Big(R_2^\top \Big[L_{bc} \;+\; \Pi_r M_{bc} \\ +\; \Big(\Pi_r^\perp + \Pi_r M_{bc}\Big) L_{br} \Big(\Pi_r^\perp + M_{bc}\Pi_r\Big) \Big] R_2 \Big) \,. \end{aligned} \tag{20}$$

Then Theorem 6 of [17] states that the unitary operation U for the Clifford operation characterized by $(C, \mathbf{h})$ is given by the matrix formula

$$U \;=\; \frac{1}{\sqrt{2^r}} \sum_{\substack{\mathbf{x}_b \in \{0,1\}^{n-r} \\ \mathbf{x}_c, \mathbf{x}_r \in \{0,1\}^r}} \Big[\begin{array}{l} (-1)^{\left(\mathbf{x}_{br}^\top L_{br} \mathbf{x}_{br} + \mathbf{x}_r^\top \mathbf{x}_c + \mathbf{x}_{bc}^\top L_{bc} \mathbf{x}_{bc} + \mathbf{h}_{bc}^\top \mathbf{x}_{bc}\right)} \times \\ \qquad (-i)^{\left(\mathbf{d}_{br}^\top \mathbf{x}_{br} + \mathbf{d}_{bc}^\top \mathbf{x}_{bc}\right)} \; \big| R_1 \mathbf{x}_{br} \big\rangle \big\langle R_2^{-1} \mathbf{x}_{bc} + \mathbf{t} \big| \end{array} \Big] \,, \tag{21}$$

where $\mathbf{x}_{br} = \left[\begin{smallmatrix} \mathbf{x}_b \\ \mathbf{x}_r \end{smallmatrix}\right]$ and $\mathbf{x}_{bc} = \left[\begin{smallmatrix} \mathbf{x}_b \\ \mathbf{x}_c \end{smallmatrix}\right]$ are n bit boolean vectors.

The formula in (21) shows strong similarities to a quadratic form expansion. In particular, consider disjoint sets of indices V_b, V_r, and V_c, with $|V_b| = n - r$ and $|V_r| = |V_c| = r$. Let $V = V_b \cup V_c \cup V_r$, $I = V_b \cup V_c$, and $O = V_b \cup V_r$, and define the following notation for $\mathbf{x} \in \{0,1\}^V$:

$$\mathbf{x}_I \;=\; \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_c \end{bmatrix} \;=\; \begin{bmatrix} \mathbf{x}_{V_b} \\ \mathbf{x}_{V_c} \end{bmatrix} \in \{0,1\}^I \;\;, \quad \mathbf{x}_O \;=\; \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_r \end{bmatrix} \;=\; \begin{bmatrix} \mathbf{x}_{V_b} \\ \mathbf{x}_{V_r} \end{bmatrix} \in \{0,1\}^O \;\;, \tag{22}$$

$$\begin{aligned} Q(\mathbf{x}) \;=\; \pi \Big(\mathbf{x}_O^\top L_{br} \mathbf{x}_O \;+\; \mathbf{x}_O^\top \Pi_r \mathbf{x}_I \;+\; \mathbf{x}_I^\top L_{bc} \mathbf{x}_I \;+\; \mathbf{x}_I^\top \mathbf{h}_{bc} \mathbf{h}_{bc}^\top \mathbf{x}_I \Big) \\ -\; \frac{\pi}{2} \Big(\mathbf{x}_O^\top \mathbf{d}_{br} \mathbf{d}_{br}^\top \mathbf{x}_O \;+\; \mathbf{x}_I^\top \mathbf{d}_{bc} \mathbf{d}_{bc}^\top \mathbf{x}_I \Big) \,. \end{aligned} \tag{23}$$

Then, (21) is equivalent to

$$U \;=\; \frac{1}{\sqrt{2^r}} \sum_{\mathbf{x} \in \{0,1\}^V} \mathrm{e}^{iQ(\mathbf{x})} \; \big| R_1 \mathbf{x}_O \big\rangle \big\langle R_2^{-1} \mathbf{x}_I + \mathbf{t} \big| \;\;, \tag{24}$$

which is essentially a quadratic form expansion sandwiched between two networks of controlled-not and X gates. To obtain a simple quadratic form expansion, we would like to perform a change of variables on $\mathbf{x}_I$ and $\mathbf{x}_O$; but this cannot be done as I and O intersect at V_b, and the changes of variables do not

[9] The vector formulas given here for $\mathbf{t}$ and $\mathbf{h}_{bc}$ may be obtained by repeated application of Theorem 2 of [17].

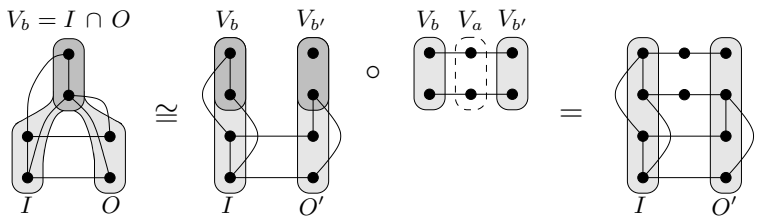

Fig. 3. Illustration of geometries arising from quadratic form expansions yielding the same matrix. On the left is a geometry whose inputs and output intersect; on the right is a geometry from an equivalent quadratic form expansion, constructed so that the input and output indices are disjoint.

necessarily respect the partitioning of I and O with respect to this intersection. However, we may add auxiliary variables in order to produce an expansion with disjoint input and output indices. Note that

$$\mathbb{1}_2 \;=\; \sum_{\mathbf{x}\in\{0,1\}^2} \delta_{x_1,x_2}\,|x_2\rangle\langle x_1| \;=\; \frac{1}{2}\sum_{\mathbf{x}\in\{0,1\}^3} (-1)^{x_1x_3+x_2x_3}\,|x_2\rangle\langle x_1| \quad (25)$$

where $\delta_{x,y}$ is the Kronecker delta. Let V_a and $V_{b'}$ be disjoint copies of V_b, and set $V' = V \cup V_a \cup V_{b'}$ and $O' = V_{b'} \cup V_r$. Writing $\mathbf{x}_a$ and $\mathbf{x}_{b'}$ for the restriction of $\mathbf{x} \in \{0,1\}^{V'}$ to V_a and $V_{b'}$, we then define

$$\mathbf{x}_I \;=\; \begin{bmatrix}\mathbf{x}_b\\ \mathbf{x}_c\end{bmatrix} \in \{0,1\}^{\,I}\;, \qquad\qquad \mathbf{x}_{O'} \;=\; \begin{bmatrix}\mathbf{x}_{b'}\\ \mathbf{x}_r\end{bmatrix} \in \{0,1\}^{\,O'}\;, \quad (26)$$

$$\begin{aligned} Q'(\mathbf{x}_I\,,\,\mathbf{x}_a\,,\,\mathbf{x}_{O'}) \;=\; \pi\Big(\mathbf{x}_{O'}^\top L_{br}\mathbf{x}_{O'} \;+\; \mathbf{x}_{O'}^\top \Pi_r \mathbf{x}_I \;+\; \mathbf{x}_I^\top L_{bc}\mathbf{x}_I \;+\; \mathbf{h}_{bc}^\top \mathbf{x}_I\Big) \\ +\; \pi\mathbf{x}_I^\top \begin{bmatrix}\mathbb{1}_{n-r}\\ 0\end{bmatrix}\mathbf{x}_a \;+\; \pi\mathbf{x}_{O'}^\top \begin{bmatrix}\mathbb{1}_{n-r}\\ 0\end{bmatrix}\mathbf{x}_a \\ -\; \frac{\pi}{2}\Big(\mathbf{d}_{br}^\top \mathbf{x}_{O'} \;+\; \mathbf{d}_{bc}^\top \mathbf{x}_I\Big)\,. \end{aligned} \quad (27)$$

Note that the difference between the expressions for Q' and Q is essentially that all instances of $\mathbf{x}_O$ have been replaced with $\mathbf{x}_{O'}$ (which is independent from $\mathbf{x}_I$), and the presence of the terms involving $\mathbf{x}_a$. (This manipulation is illustrated in Figure 3 as a transformation of geometries.) We therefore have

$$\begin{aligned} &\sum_{\mathbf{x}\in\{0,1\}^V} \mathrm{e}^{iQ(\mathbf{x})}\,\big|R_1\mathbf{x}_O\big\rangle\big\langle R_2^{-1}\mathbf{x}_I + \mathbf{t}\big| \\ &\qquad = \sum_{\mathbf{x}_I,\,\mathbf{x}_{O'}} \delta_{\mathbf{x}_b,\mathbf{x}_{b'}}\,\mathrm{e}^{iQ'(\mathbf{x}_I,\,\mathbf{0},\,\mathbf{x}_{O'})}\,\big|R_1\mathbf{x}_{O'}\big\rangle\big\langle R_2^{-1}\mathbf{x}_I + \mathbf{t}\big| \\ &\qquad = \frac{1}{2^{n-r}} \sum_{\mathbf{x}\in\{0,1\}^{V'}} \mathrm{e}^{iQ'(\mathbf{x}_I,\,\mathbf{x}_a,\,\mathbf{x}_{O'})}\,\big|R_1\mathbf{x}_{O'}\big\rangle\big\langle R_2^{-1}\mathbf{x}_I + \mathbf{t}\big|\,. \end{aligned} \quad (28)$$

Substituting the final expression of (28) into (24) and performing the appropriate change of variables, we have

$$U \;=\; \frac{\sqrt{2^r}}{2^n} \sum_{\mathbf{x}\in\{0,1\}^{V'}} \mathrm{e}^{iQ'(R_2(\mathbf{x}_I+\mathbf{t}),\, \mathbf{x}_a,\, R_1^{-1}\mathbf{x}_{O'})} \, |\mathbf{x}_{O'}\rangle\langle\mathbf{x}_I| \;. \qquad (29)$$

Note that the quadratic form of the expansion in (29) has only angles θ_{uv} which are multiples of $\frac{\pi}{2}$, with $\theta_{uv} \in \{0, \pi\}$ for $u \neq v$. This then represents the positive branch of a one-way measurement pattern on the geometry (G', I, O') of the quadratic form expansion of 29, using only X or Y basis measurements, and having only $n - r$ auxiliary vertices.

Interpolating the measurement pattern. We can augment this to a measurement pattern by applying the techniques of the stabilizer formalism [16] to the stabilizer code generated by the operators $K(v) = X_v \prod_{v\sim w} Z_w$ for $v \in I^{\mathsf{c}}$ (where again $\sim$ is the adjacency relation of G), as follows. To obtain the final correction, we do classical pre-processing simulating the evolution of the *state space* when we perform one measurement at a time. For each measured qubit u, there is an associated correction σ_v which we may perform immediately after the measurement if we obtain the result $\mathsf{s}_u = 1$. We store for each qubit v two boolean formulas β_v and γ_v, representing the X and Z components of the accumulated corrections to be performed on v. When v is measured, the pending X corrections will affect the result of any Y measurement, and the pending Z corrections will affect the result of any X or Y measurement, in each case by exchanging the significance of the two measurement outcomes.[10] Just prior to the (simulated) measurement of δ_v, let $\delta_v = \gamma_v$ if v is to be measured with an X observable, and $\delta_v = \beta_v + \gamma_v$ if v is to be measured with a Y observable. Thus, upon measuring v, the following operations are accumulated into the corrections which must be performed:

- For every qubit w where σ_v acts with an X or Y operation, we must add $\mathsf{s}_v + \delta_v$ to β_w;
- For every qubit w where σ_v acts with a Y or Z operation, we must add $\mathsf{s}_v + \delta_v$ to γ_w.

This accounts for the accumulated corrections due to the measurement of v and every preceding measurement which affects it. By simulating measurement for all of the qubits in O^{c} in this way, we obtain boolean formulae for the corrections on O in terms of the results of the measurements: the correction to be

[10] This can be described in terms of *signal shifting*, as described in [11].

performed for some $w \in O$ is $X^{\beta_w} Z^{\gamma_w}$, for β_w and γ_w constructed after all of the (simulated) measurements. To obtain β_w and γ_w for all $w \in O$ in this way takes time $O(n^2)$.

It is easy to show that the resulting measurement pattern is irreducible by the techniques of [18], by the following argument. Let A denote the set of auxiliary vertices corresponding to the bit positions of $\mathbf{x}_a$: note that in the measurement pattern, these are all to be measured with the observable X, and are adjacent only to the input/output variables $\mathbf{x}_I$ and $\mathbf{x}_O$.[11] To eliminate a vertex $v \in A$ using the methods of [18] on the geometry induced by the quadratic form expansion, we would have to identify an output variable $b_0 \in O$ adjacent to x, and apply the graph transformation in [18, Proposition 1]. This would result in a geometry where b_0 has the former neighbors of v in G (and in particular is not adjacent to any more removable vertices), and where a local Clifford (which is not a Pauli operator) must be applied to b_0 after the entangling procedure. Because b_0 is not adjacent to any other auxiliary qubit after this transformation, the local Clifford cannot be undone or made into a Pauli operator by e.g. another vertex removal; then, except by extending the computational model to allow for corrections which are local Clifford operations, performing the local Clifford can only be done by introducing an auxiliary qubit (or rather, a new output qubit following b_0, making the latter an auxiliary qubit). Thus:

Theorem 4. *For an n-qubit Clifford group operation U given in the form of a Leuven tableau, there is an $O(n^3/\log n)$ algorithm which produces a minimal one-way measurement pattern for U.*

The ability to obtain a quadratic form expansion representing a reduced measurement pattern yields a more efficient algorithm to find totally reduced Clifford patterns than from using existing techniques to obtain one via the circuit model. The quadratic form of (29) can be found from a Leuven tableau $(C, \mathbf{h})$ in time $O(n^3/\log n)$, which is dominated by the time required to compute R_1 and R_2. To contrast, an approximately optimal quantum circuit for a Clifford group operation (*i.e.* consisting of $O(n^2/\log n)$ gates) can be found from a Leuven tableau in time $O(n^3/\log n)$ by transforming it into a destabilizer tableau, and then applying the algorithm of [19]. To obtain a measurement pattern from such a circuit by composing the patterns for each gate, removing vertices opportunistically (with each removal taking time $O(n^2)$), requires time $O(n^4/\log n)$. Thus, making use of quadratic form expansions provides us with a faster algorithm to obtain reduced measurement patterns for Clifford group operations.

[11] There are no square terms x_v^2 for $v \in A$ or cross-term $x_u x_v$ for $u, v \in A$ before the change of variables in (28)), and the change of variables itself does not introduce any.

4 Conclusions and Open Problems

We have introduced quadratic form expansions, and developed techniques which suggest that they may be useful for synthesizing efficient implementations for unitary operations. We described conditions under which implementations may be efficiently found for unitaries specified by quadratic form expansions; and we showed how quadratic form expansions leads to more efficient algorithms for obtaining reduced patterns for Clifford operations in the one way measurement model.

In the introduction, we mentioned that quadratic form expansions are similar in form to a sum-over-paths representation of unitary operations, which is a well-developed subject in theoretical physics. This raises the question of whether the techniques developed here are useful e.g. for developing algorithms to simulate physical systems. It is not known whether the solved cases of the Measurement Pattern Interpolation problem correspond to *natural* (in the more literal sense) unitaries expressed as sums over paths: this question, and how to extend the solved cases of the MPI to include propagators for interesting physical systems, remain open.

References

1. R. Raussendorf and H. Briegel. *A one-way quantum computer*. Physical Review Letters 86 (5188), 2001.
2. R. Raussendorf and H. Briegel. *Computational model underlying the one-way quantum computer*. Quantum Information & Computation, vol 2 #6 (443) 2002.
3. A. Broadbent and E. Kashefi. *Parallelizing quantum circuits*. arXiv:0704.1736, 2007.
4. R. P. Feynmann, A. R. Hibbs. *Quantum Mechanics and Path Integrals*. McGraw-Hill, New York, 1965.
5. L. S. Schulman. *Techniques and Application of Path Integration*. Wiley-Interscience, New York, 1981.
6. V. Danos and E. Kashefi. *Determinism in the one-way model*. Physical Review A 74 (052310), 2006. arXiv:quant-ph/0506062.
7. D. E. Browne and H. J. Briegel. *One-way Quantum Computation — a tutorial introduction*. arXiv:quant-ph/0603226 (2006).
8. D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. *Generalized flow and determinism in measurement-based quantum computation*. New J. Physics vol. 9 (250), 2007. arXiv:quant-ph/0702212
9. C. M. Dawson, H. L. Haselgrove, A. P. Hines, D. Mortimer, M. A. Nielsen, and T. J. Osborne. *Quantum computing and polynomial equations over* $\mathbb{Z}_2$. Quantum Information & Computation vol 5 #2 (102), 2004. arXiv:quant-ph/0408129
10. N. de Beaudrap, V. Danos, and E. Kashefi. *Phase map decompositions for unitaries*. arXiv:quant-ph/0603266, 2006.
11. V. Danos, E. Kashefi, and P. Panangaden. *The measurement calculus*. J. ACM vol. 54, 8 (2007). arXiv:quant-ph/0412135

12. V. Danos, E. Kashefi, and P. Panangaden. *Parsimonious and robust realizations of unitary maps in the one-way model*. Physical Review A vol 72 (064301), 2005. arXiv:quant-ph/0411071
13. M. Mhalla and S. Perdrix. Finding optimal flows efficiently. arXiv:0709.2670, 2007.
14. A. Kitaev, A. Shen, and M. Vylalyi. *Classical and quantum computation*. Graduate Texts in Mathematics, vol 47, American Mathematical Society, Providence RI, 2002.
15. N. de Beaudrap and M. Pei. *An extremal result for geometries in the one-way measurement model*. To appear in Quantum Information and Computation, vol. 8 #5 (430), 2008. arXiv:quant-ph/0702229
16. D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, Caltech, 1997. arXiv:quant-ph/9705052.
17. J. Dehaene and B. De Moor. *Clifford group, stabilizer states, and linear and quadratic operations over GF(2)*. Physical Review A vol 68 (042318), 2003. arXiv:quant-ph/0304125
18. M. Hein, J. Eisert, and H. J. Briegel. *Multi-party entanglement in graph states*. Physical Review A vol 69 (62311), 2004. arXiv:quant-ph/0307130
19. S. Aaronson and D. Gottesman. *Improved simulation of stabilizer circuits*. Physical Review A vol 70 (052328), 2004. arXiv:quant-ph/0406196
20. N. de Beaudrap. Finding flows in the one-way measurement model. arXiv:quant-ph/0611284, 2006.
21. A. Fowler, S. Devitt, and L. Hollenberg. *Implementation of Shor's algorithm on a linear nearest neighbor qubit array*. Quantum Information & Computation vol 4 #4 (237), 2004.
22. K. N. Patel, I. L. Markov, and J. P Hayes. Efficient synthesis of linear reversible circuits. To appear in Quantum Information & Computation vol 8, 2008. arXiv:quant-ph/0302002

A Quadratic form expansions as sums over paths

Let (G, I, O) be the geometry of a quadratic form expansion, as defined on page 7. In the special case when (G, I, O) has a fractional-edge flow as defined in Section 3.2, the quadratic form expansion corresponds exactly to a sum over paths as described in [9], for the elementary gate set of H, Z^t, and $\wedge Z^t$, where $t \in R$ (*i.e.* admitting arbitrary Z rotations and fractional controlled-Z gates). In order to demonstrate the sense in which quadratic form expansions are sums over paths in this case, and because it represents a reasonably simple algorithm for converting quantum circuits into quadratic form expansions, we now present an alternate proof of Theorem 1 based on the techniques of [9]. That any quadratic form expansion with geometry with a fractional-edge flow can be constructed in this way follows by reversing the construction below.

Proof of Theorem 1. Consider a quantum circuit implementing U exactly, using the operations H, $\wedge Z^t$, and Z^t. Enumerate the wires of the circuit from 1 to k, and for each wire $1 \leqslant j \leqslant k$, introduce a *path label* x_j for the input end of the wire, corresponding to an input bit $x_j \in \{0, 1\}$. We set $I = \{1, \ldots, k\}$. Divide each wire into *segments*, bounded on each end by either a Hadamard gate, the input terminal of the wire, or the output terminal. We label the wire segments with path variables: for the segments at the inputs, we apply the labels

x_j for $j \in I$, and we introduce new path variables to label the remaining wire segments. Computational paths in the circuit are then described by setting all of the the path variables $x_1 \cdots x_n$ collectively to some particular binary string in $\{0,1\}^n$. The phase contribution of each paths, governing how they interfere to produce an output state for any given input state, is described by a function $\varphi(\mathbf{x})$ depending the gates of the circuit as follows:

(*i*) For every Hadamard gate on a single wire, with a path variable x_h labelling the segment preceding the Hadamard and a path variable x_j labelling the segment following the Hadamard, we add a term $x_h x_j$.

(*ii*) For every $\wedge Z^t$ operation between two wires, with a path variable x_h labelling the segment of one wire and x_j labelling the segment of the other wire in which the $\wedge Z^t$ operation is performed, we add a term $t x_h x_j$.

(*iii*) For every Z^t operation on a wire segment labelled with a path variable x_j , we add a term $t x_j^2$. (Because the path variable x_j ranges over $\{0,1\}$, the extra power of 2 has no effect.)

In particular, the function $\varphi(\mathbf{x})$ is a quadratic form, where without loss of generality the coefficients may be constrained to $-1 < t \leqslant 1$. The phase of a given path, described by a bit-string $\mathbf{x} \in \{0,1\}^n$, is then given by $(-1)^{\varphi(\mathbf{x})} = \mathrm{e}^{i\pi\varphi(\mathbf{x})}$. Each path also has an associated amplitude of $2^{-r/2}$, where $r = n - k$ is the number of Hadamard gates in the circuit.[12]

Let O be the set of indices j such that some wire is labelled by the path-variable x_j at its' output end. Then, the initial points of computational paths are described by bit-vectors $\mathbf{a} \in \{0,1\}^I$, and the terminal points of paths are described by $\mathbf{b} \in \{0,1\}^O$. The coefficients $U_{\mathbf{b},\mathbf{a}}$ can then be given as the sum of the contributions of all paths beginning at $\mathbf{x}_I = \mathbf{a}$ and ending at $\mathbf{x}_O = \mathbf{b}$:

$$U_{\mathbf{b},\mathbf{a}} \;=\; \frac{1}{\sqrt{2^r}} \sum_{\substack{\mathbf{x}\in\{0,1\}^n \\ \mathbf{x}_I=\mathbf{a} \\ \mathbf{x}_O=\mathbf{b}}} \mathrm{e}^{i\pi\varphi(\mathbf{x})} \;, \tag{30}$$

which is an expression of the coefficients of U as a quadratic form expansion.

To obtain a proof of Theorem 1, it is sufficient to note that without loss of generality we may restrict ourselves to using $\wedge Z^t$ gates only for $t = 1$ to implement U exactly; and that to implement U to arbitrary precision, it suffices to use Z^t gates where t is restricted to multiples of $\frac{1}{4}$. □

[12] Although it is quite reasonable to consider φ to be simply a polynomial over $\mathbb{R}$, in terms of the descriptions used in Section VI of [9], one may consider φ to be a polynomial over the ring $\mathbb{R}/2\mathbb{Z}$. If we restrict to $t \in \frac{\pi}{4}\mathbb{Z}$, we may simplify this to the finite ring $\mathbb{Z}_8$ by multiplying all of the coefficients by 4, and using it to describe powers of $\sqrt{i}$ rather than of -1.