

# Quadratic Form Expansions for Unitaries

Niel de Beaudrap<sup>1</sup>, Vincent Danos<sup>2</sup>, Elham Kashefi<sup>3</sup>, Martin Roetteler<sup>4</sup>

<sup>1</sup> IQC, University of Waterloo

<sup>2</sup> CNRS, Université Paris 7

<sup>3</sup> Christ Church College, University of Oxford

<sup>4</sup> 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 [4, 5]. 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

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

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

Quadratic form expansions are closely related to the sum-over-paths description of unitary embeddings described in [6]: the details of this relation, and an

equivalent description of quadratic form expansions in terms of the formula for individual matrix coefficients, can be found in Appendix A.

Given such an expression for a unitary  $U$ , we can obtain a decomposition of  $U$  in terms of operations closely related to the entangling procedure of the one-way measurement model. Using this connection, we demonstrate various techniques involving quadratic form expansions to efficiently implement unitary operators under various conditions, including an  $O(n^3)$  algorithm to obtain a reduced measurement pattern for Clifford group operations from a description of how they transform the Pauli group.

## 2 Connection to measurement patterns

Note that in a quadratic form expansion,  $Q(\mathbf{x})$  can be expressed as an expectation value  $\langle \mathbf{x} | H | \mathbf{x} \rangle$ , where  $H$  is a 2-local diagonal Hamiltonian:

$$H = \sum_{\substack{\{u,v\} \subseteq V \\ u \neq v}} \theta_{uv} \left[ |1\rangle\langle 1|_u \otimes |1\rangle\langle 1|_v \right] + \sum_{v \in V} \theta_{vv} |1\rangle\langle 1|_v . \quad (2)$$

Then, given a quadratic form expansion for a unitary embedding  $U$  as in (1), we may decompose  $U$  as follows:

$$\begin{aligned} U &\propto \sum_{\mathbf{x} \in \{0,1\}^V} |\mathbf{x}_O\rangle\langle \mathbf{x}| e^{iH} |\mathbf{x}\rangle\langle \mathbf{x}_I| = \left[ \sum_{\mathbf{y} \in \{0,1\}^V} |\mathbf{y}_O\rangle\langle \mathbf{y}| \right] e^{iH} \left[ \sum_{\mathbf{x} \in \{0,1\}^V} |\mathbf{x}\rangle\langle \mathbf{x}_I| \right] \\ &\propto R_O e^{iH} P_I , \end{aligned} \quad (3)$$

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

We can express this in terms of a process of postselecting observables, as follows. Decompose  $H$  into terms  $H_O$ ,  $H_1$ , and  $H_2$ , where  $H_O$  is the 1-local term on the qubits of  $O$ ,  $H_1$  is the 1-local term on the remaining qubits, and  $H_2$  are the remaining terms from (2). We then have  $U \propto R_O e^{iH_O} e^{iH_1} e^{iH_2} P_I$ . Note that  $e^{iH_O}$  and  $e^{iH_1}$  are simply single-qubit  $Z$  rotations applied to the elements of  $O$  and  $O^c = V \setminus O$  respectively, where in each case the qubits  $v$  in those sets are rotated by an angle  $\theta_{vv}$ . The composite map  $\tilde{R}_O = R_O e^{iH_1}$  projects each the state of each qubit  $v \in O^c$  onto the vector  $|0\rangle + e^{-i\theta_{vv}} |1\rangle$  for each  $v \in O^c$ . Then, we have  $U = e^{iH_O} \tilde{R}_O e^{iH_2} P_I$ , 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  $v \in O^c$ , 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 which performs measurements  $M(\alpha_v) = \cos(\alpha_v)X + \sin(\alpha_v)Y$ , in the case where all measurements result in the  $+1$  eigenvalue. If this can be extended to a complete measurement algorithm, including the feedforward mechanism, we obtain a measurement-based algorithm for  $U$ . 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  $-\pi < \theta_{vv} \leq \pi$  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 [7] (and using the notation of that article), the measurement pattern  $X_v^{s_u} M_u^{-\alpha} E_{uv} N_v$  performs the unitary transformation  $J(\alpha) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{bmatrix}$  for  $\alpha \in \mathbb{R}$ , from the state space of a qubit  $u$  to that of a “fresh” qubit  $v$ . These operations generate  $SU(2)$ , and generate a group dense in  $SU(2)$  if we restrict to  $\alpha \in \frac{\pi}{4}\mathbb{Z}$ , by [8].

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 [4], in this measurement pattern, the probability of every measurement resulting in the  $+1$  eigenvalue (i.e.  $s_v = 0$  for all  $v \in O^c$ ) is non-zero. Then,  $U \propto R_O e^{iH} P_I$ , where

$$H = \sum_{uv \in E(G)} \pi \left[ |1\rangle\langle 1|_u \otimes |1\rangle\langle 1|_v \right] - \sum_{v \in O^c} \alpha_v |1\rangle\langle 1|_v . \quad (4)$$

By (3), this yields a quadratic form expansion for  $U$ , with

$$Q(\mathbf{x}) = \sum_{uv \in E(G)} \pi x_u x_v - \sum_{v \in O^c} \alpha_v x_v^2 . \quad (5)$$

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

To exploit the connection between quadratic form expansions and the one-way measurement model to actually obtain an implementation of a unitary  $U$ , we must be able to determine a suitable feed-forward mechanism to determine how to adapt measurements and correct the state of the output.

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 its  $+1$  eigenvalue the *positive branch* of the measurement pattern. 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 graph of entanglement operations performed, and  $I, O \subseteq V(G)$  are the sets of qubits defining the input/output space of the pattern), and the angles  $\mathbf{a} = \{\alpha_v\}_{v \in O^c}$  defining the measurements to be performed.

In order to better consider the analogies between quadratic form expansions and the one-way measurement model, we will define the following:

**Definition 2.** *For a quadratic form expansion*

$$\frac{1}{C} \sum_{\mathbf{x} \in \{0,1\}^V} e^{iQ(\mathbf{x})} |\mathbf{x}_O\rangle \langle \mathbf{x}_I| \quad \text{where} \quad Q(\mathbf{x}) = \sum_{\{u,v\} \subseteq V} \theta_{uv} x_u x_v, \quad (6)$$

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  $-\pi < \theta_{uv} \leq \pi$  for all  $u, v \in V$ , we may without loss of generality restrict  $G$  to have edge-weights  $-1 < W_G(uv) \leq 1$ . 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 the remaining sections, we consider the problem of synthesizing an efficient implementation of  $U$ , either from a quadratic form expansion for  $U$  whose geometry meets some condition, or by constructing a quadratic form expansion which can be directly translated into a measurement pattern for  $U$ .

### 3 Synthesis via measurement pattern interpolation

The following problem is what we are most generally interested in:

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

This problem may be quite difficult in general. We may attempt to make the problem easier by considering a more restricted problem:

**Generic Measurement Pattern Interpolation (GMPI).** *Given  $(G, I, O)$ , are there measurement patterns  $\mathfrak{P}(\mathbf{a})$ , each with geometry  $(G, I, O)$ , parameterized by the choice of measurement angles  $\mathbf{a}$ , 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. There is a notable special case which has been solved: those geometries  $(G, I, O)$  which have a *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 [5]. The following is the definition of gflows in [9], for measurements restricted to the  $XY$  plane:

**Definition 3.** *Given a geometry  $(G, I, O)$  for a measurement pattern, a gflow is a pair  $(g, \preceq)$ , where  $g$  is a function from  $O^c$  to subsets of  $I^c$  and  $\preceq$  is a partial order, such that the following conditions hold for all  $u$  and  $v$  in the graph  $G$ :*

$$v \in g(u) \implies u \prec v, \quad (7a)$$

$$v \in \text{odd}(g(u)) \implies u \preceq v, \quad (7b)$$

$$u \in \text{odd}(g(u)), \quad (7c)$$

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

In this section, we discuss polynomial time algorithms for synthesizing  $U$  in terms of measurement pattern interpolation, under different constraints on the geometry of a quadratic form expansion for  $U$ .

### 3.1 Measurement pattern synthesis via gflows

Consider a geometry  $(G, I, O)$  arising from 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 is then sufficient to find a gflow for  $(G, I, O)$ : because in that case, for any choice of measurement angles  $\mathbf{a} = \{\alpha_v\}_{v \in O^c}$ , we may consider the pattern

$$\left[ \prod_{u \in O^c}^{\succ} \left( \bigotimes_{\substack{v \in \text{odd}(g(u)) \\ v \neq u}} Z_v \right) \left( \bigotimes_{v \in g(u)} X_v \right) M_u^{\alpha_u} \right] \left[ \prod_{u \sim v} E_{uv} \right] \left[ \prod_{u \in I^c} N_u \right] \quad (8)$$

where the left-hand product may be ordered right-to-left in any linear extension of the order  $\preceq$ . It is straightforward to see that any correction operation on a

qubit  $u$  will occur on the right of any measurement made on  $u$ , and that the correction operations consist of a product of operators  $K(v)$  for  $v \in g(v)$ , where  $K(v) = X_v \prod_{w \sim v} Z_w$  is a stabilizer generator of the family of states described by preparing all the qubits of  $I^c$  in the state  $|+\rangle$ , and performing the entanglement operations described by the edges of  $G$ . (Here,  $\sim$  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 [9], an  $O(n^4)$  algorithm is provided to determine whether or not a geometry  $(G, I, O)$  has a gflow, and obtain one in the case that one exists, where  $n = |V(G)|$ . The measurement pattern of (8) can be constructed in time  $O(nm)$ , where  $m = |E(G)|$ , and the number of operations in the pattern will also be  $O(nm)$ . Thus:

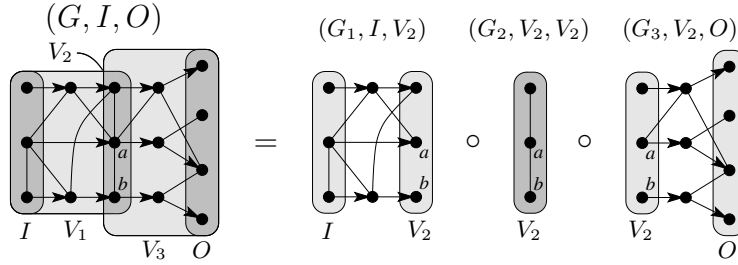
**Theorem 2.** *For a unitary embedding  $U$  given as a quadratic form expansion with geometry  $(G, I, O)$  with unit edge-weights, there is an  $O(n^4)$  algorithm which either determines that  $(G, I, O)$  has no gflow, or constructs a measurement pattern consisting of  $O(nm)$  operations<sup>1</sup> implementing  $U$  (using measurement angles of arbitrary precision), where  $n = |V(G)|$  and  $m = |E(G)|$ .*

### 3.2 Circuit synthesis via flows

A geometry  $(G, I, O)$  which has fractional edges lies 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  $v \in O^c$  to a singleton set: we may say  $(f, \preceq)$  is a flow if and only if  $(g_f, \preceq)$  is a gflow, where  $g_f(v) = \{f(v)\}$ . The positive branch of a measurement pattern whose geometry has a flow can be represented by a circuit with the following characteristics [4]:

- edges of the form  $v f(v)$  for  $v \in O^c$  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  $v$ ;

<sup>1</sup> These operations may involve measurement angles of arbitrary precision. A corresponding approximate measurement pattern may use  $O(nm + n \text{ polylog}(n/\varepsilon))$  operations by the Solovay-Kitaev Theorem [10], where  $\varepsilon$  is the precision of the coefficients of  $Q$ .



**Fig. 1.** Illustration of the decomposition of a quadratic form expansion, 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  $\preceq$  associated with a fractional-edge flow. Arrows represent the action of the corresponding fractional-edge flow function,  $f$ .

- wires whose initial segments are labelled by vertices of  $I$  accept arbitrary input states, while those labelled by vertices  $I^c \setminus \text{img}(f)$  take input  $|+\rangle$ .

Suppose  $(G, I, O)$  is a geometry of a quadratic form expansion for a unitary transformation  $U$ . We may say that  $(f, \preceq)$  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 for  $U$  given by such a quadratic form expansion 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  $b$ . We can show this by induction on the number of edges of fractional weight, as follows. We may use the following Lemma to consider how to compose/decompose, quadratic form expansions:

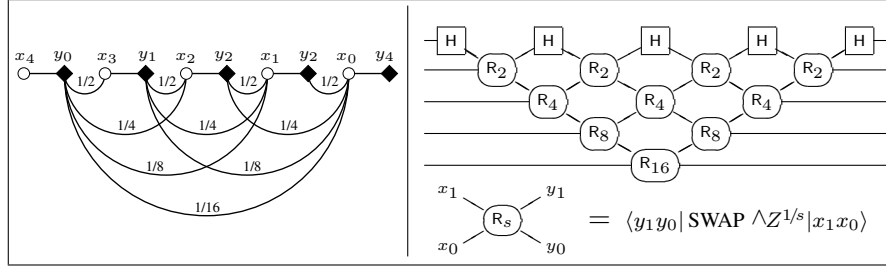
**Lemma 1.** *Let  $U_1, U_2$  be matrices given by quadratic form expansions*

$$U_j = \frac{1}{C_j} \sum_{\mathbf{x} \in \{0,1\}^{V_j}} e^{iQ_j(\mathbf{x})} |\mathbf{x}_{O_j}\rangle \langle \mathbf{x}_{I_j}|. \quad (9)$$

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

Consider an arbitrary edge  $ab$  of fractional weight: we will decompose the quadratic form expansion into three parts, as illustrated in Figure 1, induced by “sub-geometries” of  $(G, I, O)$ . Let  $V_2$  be the set of maximal vertices in  $\preceq$  which are bounded above by either  $a$  or  $b$ . Let  $V_1$  and  $V_3$  be the sets of vertices bounded above/below (respectively) by  $V_2$ . Let  $Q_2(\mathbf{x}_{V_2})$  contain all terms  $x_u x_v$



**Fig. 2.** The geometry for the quadratic form expansion of the QFT for  $\mathbb{Z}_{32}$ , and the corresponding circuit due to [17]. 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  $x_u, x_v \in V_2$  but  $x_u \neq x_v$ , and divide the remaining terms of  $Q$  into quadratic forms  $Q_1$  and  $Q_3$  on  $\{0, 1\}^{V_1}$  and  $\{0, 1\}^{V_3}$ . This induces three quadratic form expansions for unitary embeddings  $U_1$ ,  $U_2$ , and  $U_3$ , all of which have circuit decompositions as described; therefore, their composite  $U$  does as well. More details of this proof can be found in Appendix B.

In [9], 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  $[u \neq f(v) \text{ and } v \neq f(u)]$  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  $\preceq$ , 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 [11], any geometry with a flow has  $m \leq kn$ : 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; 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<sup>2</sup> implementing  $U$ , where  $n = |V(G)|$  and  $k = |O|$ .*

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

$$\mathcal{F}_n = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}, \mathbf{y} \in \{0, 1\}^n} e^{2\pi i \left[ \sum_{h=0}^{n-1} 2^h x_h \right] \left[ \sum_{j=0}^{n-1} 2^j y_j \right] / 2^n} |\mathbf{y}\rangle \langle \mathbf{x}|, \quad (10)$$

<sup>2</sup> 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  $O(kn \text{ polylog}(kn/\varepsilon))$  by the Solovay-Kitaev Theorem [10], where  $\varepsilon$  is the precision of the coefficients of  $Q$ .

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

$$Q(\mathbf{x}, \mathbf{y}) = \sum_{h=0}^{n-1} \sum_{j=0}^{n-1-h} 2^{(h+j)-(n-1)} x_h y_j. \quad (11)$$

This has a fractional-edge flow for all  $n$ . Figure 2 illustrates this geometry for  $n = 5$ , and the circuit (due to [17]) which may be synthesized from it.

#### 4 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 result of [13] then allows us to synthesize reduced measurement patterns for Clifford group operations in time  $O(n^3)$ .

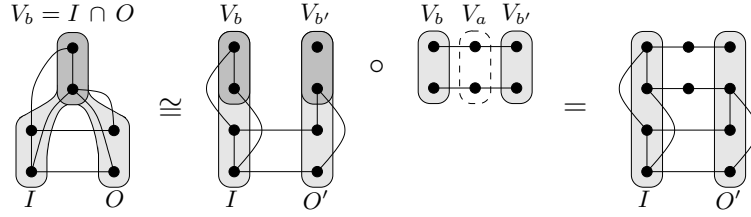
Suppose we are given a Clifford group operation  $U$  on  $n$  qubits in terms of how it transforms the operations  $X_j$  and  $Z_j$  for  $1 \leq j \leq n$ . Dehaene and de Moor [13] then provide the following matrix formula for  $U$ ,

$$U = \frac{1}{\sqrt{2^r}} \sum_{\substack{\mathbf{x}_b \in \{0,1\}^{n-r} \\ \mathbf{x}_c, \mathbf{x}_r \in \{0,1\}^r}} \left[ \begin{array}{l} (-1)^{(\mathbf{x}_{br}^\top L_{br} \mathbf{x}_{br} + \mathbf{x}_r^\top \mathbf{x}_c + \mathbf{x}_{bc}^\top L_{bc} \mathbf{x}_{bc} + \mathbf{h}_{bc}^\top \mathbf{x}_{bc})} \times \\ (-i)^{(\mathbf{d}_{br}^\top \mathbf{x}_{br} + \mathbf{d}_{bc}^\top \mathbf{x}_{bc})} |R_1 \mathbf{x}_{br}\rangle \langle R_2^{-1} \mathbf{x}_{bc} + \mathbf{t}| \end{array} \right], \quad (12)$$

where  $\mathbf{x}_{br} = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_r \end{bmatrix}$  and  $\mathbf{x}_{bc} = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_c \end{bmatrix}$  are  $n$  bit boolean vectors, and where the matrices above can be computed in  $O(n^3)$  time from the representation of  $U$  in terms of a transformation of the Pauli group. (A detailed account is in Appendix C.) We can use this to obtain a reduced pattern for  $U$ , as follows:

- Produce an equivalent formula to (23) with independent summation indices  $\mathbf{x}_I$  and  $\mathbf{x}_O$  by introducing auxiliary vertices of degree 2 (as illustrated in Figure 3): these represent Kronecker delta terms in the larger expansion.
- Perform the appropriate change of variables on  $\mathbf{x}_I$  and  $\mathbf{x}_O$  to obtain a quadratic form expansion; and use this to obtain a measurement pattern on  $n$  inputs,  $n$  outputs, and  $n - r$  auxiliary vertices (using the stabilizer formalism to determine byproduct operations).
- Obtain a pattern on  $n$  inputs and  $n$  outputs, using the vertex removal operations described in [14] on the  $n - r$  auxiliary variables.

This yields an  $O(n^3)$  algorithm to obtain a reduced pattern for  $U$ , as compared with  $O(n^4 / \log n)$  for the direct approach of obtaining a circuit (e.g. using the algorithm of [15]) and converting it into a reduced measurement pattern.



**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.

## 5 Conclusions

In this paper, we introduced quadratic form expansions, and provided examples to 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. We hope that, by identifying the existence of this structure, other useful instances of quadratic form expansions may be recognized.

## References

1. R. Raussendorf and H. Briegel. *Physical Review Letters*, 86 (5188), 2001.
2. R. Raussendorf and H. Briegel. *Quantum Information & Computation*, 2(6):443–486, 2002.
3. A. Broadbent and E. Kashefi. arXiv:0704.1736, 2007.
4. V. Danos and E. Kashefi. *Physical Review A*, 74 (052310), 2006.
5. D.E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. arXiv:quant-ph/0702212, 2007.
6. C. M. Dawson, H. L. Haselgrove, A. P. Hines, D. Mortimer, M. A. Nielsen, and T. J. Osborne. *Quantum Information & Computation*, 5(2):102 – 112, 2004.
7. V. Danos, E. Kashefi, and P. Panangaden. arXiv:quant-ph/0412135, 2004.
8. V. Danos, E. Kashefi, and P. Panangaden. *Physical Review A*, 72 (064301), 2005.
9. M. Mhalla and S. Perdrix. arXiv:0709.2670, 2007.
10. A. Kitaev, A. Shen, and M. Vylalyi. Graduate Texts in Mathematics, vol 47, American Mathematical Society, Providence RI, 2002.
11. N. de Beaudrap and M. Pei. arXiv:quant-ph/0702229, 2007.
12. D. Gottesman. PhD thesis, Caltech, 1997. arXiv:quant-ph/9705052.
13. J. Dehaene and B. De Moor. *Physical Review A*, 68 (042318), 2003.
14. M. Hein, J. Eisert, and H. J. Briegel. *Physical Review A*, 69 (62311), 2004.
15. S. Aaronson and D. Gottesman. *Physical Review A*, 70 (052328), 2004.
16. N. de Beaudrap. arXiv:quant-ph/0611284, 2006.
17. A. Fowler, S. Devitt, and L. Hollenberg. *Quantum Information & Computation*, 4(4):237 – 251, 2004.
18. K. N. Patel, I. L. Markov, and J. P Hayes. arXiv:quant-ph/0302002, 2003.

## A Quadratic form expansions as sums over paths

It is easy to verify that if  $U$  is a matrix with a quadratic form expansion as in (1), the columns of  $U$  are indexed by vectors  $\mathbf{a} \in \{0, 1\}^I$  and the rows by  $\mathbf{b} \in \{0, 1\}^O$ , and the coefficient  $U_{\mathbf{b}, \mathbf{a}}$  is given by

$$U_{\mathbf{b}, \mathbf{a}} = \frac{1}{C} \sum_{\mathbf{x} \simeq \mathbf{a}, \mathbf{b}} e^{iQ(\mathbf{x})}, \quad (13)$$

where the sum is taken over all vectors  $\mathbf{x} \in \{0, 1\}^V$  whose bit-values are consistent with both  $\mathbf{a}$  and  $\mathbf{b}$ .<sup>3</sup> This resembles a formulation of  $U$  as a sum over paths from  $\mathbf{a}$  to  $\mathbf{b}$ , where the terms  $e^{iQ(\mathbf{x})}$  represent the phase contributions of various paths parameterized by  $\mathbf{x} \in \{0, 1\}^V$ .

Let  $(G, I, O)$  be the geometry of a quadratic form expansion, as defined on page 4. 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 [6], 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 [6]. 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  $1 \leq j \leq k$ , 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  $I = \{1, \dots, k\}$ . 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:

<sup>3</sup> If  $I$  and  $O$  are non-disjoint and  $a_v \neq b_v$  for some  $v \in I \cap O$ , there are no such vectors  $\mathbf{x}$ , and therefore  $U_{\mathbf{b}, \mathbf{a}} = 0$ .

- (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  $-1 < t \leq 1$ . The phase of a given path, described by a bit-string  $\mathbf{x} \in \{0, 1\}^n$ , is then given by  $(-1)^{\varphi(\mathbf{x})} = e^{i\pi\varphi(\mathbf{x})}$ . Each path also has an associated amplitude of  $2^{-r/2}$ , where  $r = n - k$  is the number of Hadamard gates in the circuit.<sup>4</sup>

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  $\mathbf{b} \in \{0, 1\}^O$ . We can then describe the coefficients  $U_{\mathbf{b}, \mathbf{a}}$  as the sum of the contributions of all paths beginning at  $\mathbf{x}_I = \mathbf{a}$  and ending at  $\mathbf{x}_O = \mathbf{b}$ . That is:

$$U_{\mathbf{b}, \mathbf{a}} = \frac{1}{\sqrt{2^r}} \sum_{\substack{\mathbf{x} \in \{0, 1\}^n \\ \mathbf{x}_I = \mathbf{a} \\ \mathbf{x}_O = \mathbf{b}}} e^{i\pi\varphi(\mathbf{x})}, \quad (14)$$

which is an expression of  $U$  as a quadratic form expansion as in (13).

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  $\frac{1}{4}$ .  $\square$

<sup>4</sup> Although it is quite reasonable to consider  $\varphi$  to be simply a polynomial over  $\mathbb{R}$ , in terms of the descriptions used in Section VI of [6], one may consider  $\varphi$  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  $-1$ .

## B Proof of circuit synthesis algorithm for geometries $(G, I, O)$ with fractional-edge flow

In this section, we provide a more detailed proof that any quadratic form expansion whose geometry has a fractional-edge flow  $(f, \preceq)$  has an equivalent circuit representation of the following form:

- (i) The wires of the circuit are divided into segments labelled with the indices  $v \in V$ , which are separated by  $J(\theta_{vv})$  gates (where  $\theta_{vv}$  are coefficients in the quadratic form for the terms  $x_v^2$ );
- (ii) Every edge  $v f(v)$  for  $v \in O^c$  corresponds to a gate  $J(\theta_{vv})$  on a single wire, separating segments labelled by  $v$  and  $f(v)$ ;
- (iii) Every edge  $uv \in E(G)$  where  $u \neq f(v)$  and  $v \neq f(u)$  corresponds to a  $\wedge Z^{W_G(uv)}$  gate on the wire segments labelled with  $u$  and  $v$ ;
- (iv) Wires whose initial segments are labelled by vertices of  $I$  accept arbitrary input states, while those labelled by vertices  $I^c \setminus \text{img}(f)$  take input  $|+\rangle$ .

(Note that this is almost the opposite process to the construction of quadratic form expansions given in Appendix A.)

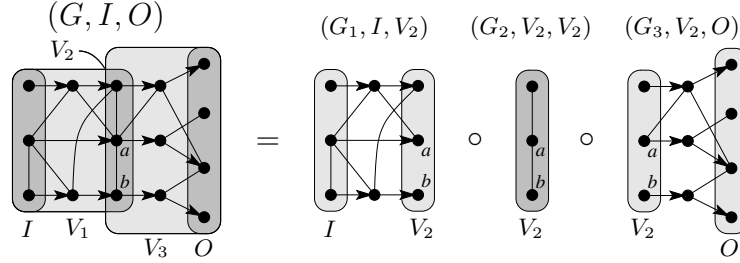
First, note that if  $(G, I, O)$  has no fractional-weight edges, then we may synthesize a circuit for  $U$  as above, as it corresponds to a normal measurement pattern with a flow, and so falls under the analysis of [4]. We may then proceed by induction for geometries with fractional edge-weights by showing we can decompose the geometry into ones with fewer fractional edge-weights.

For any arbitrary fractional edge  $ab \in E(G)$  and each  $z \in O$ , we may define  $m(ab, z)$  to be the maximal vertex  $v \in V(G)$  in the ordering  $\preceq$  subject to  $z = f^\ell(v)$  for some  $\ell \geq 0$ , such that at least one of  $v \preceq a$  or  $v \preceq b$  holds.

- Let  $V_2$  be the set of vertices  $m(ab, z)$  for each  $z \in O^c$ : 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  $u \preceq v$  for some  $v \in V_2$ ; let  $G_1 = G[V_1] \setminus \{uv \mid u, v \in V_2\}$ ; and let  $\mathcal{G}_1 = (G_1, I, V_2)$ .
- Let  $V_3$  be the set of vertices  $u \in V(G)$  such that  $u \succ v$  for some  $v \in V_2$ ; let  $G_3 = G[V_3] \setminus \{uv \mid u, v \in V_2\}$ ; 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 4 (which is a reprinting of 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).



**Fig. 4.** Illustration of the decomposition of a quadratic form expansion, 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  $\preceq$  associated with a fractional-edge flow. Arrows represent the action of the corresponding fractional-edge flow function,  $f$ .

- $U_2$  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  $u \in V_2$ , each with one wire segment, with the fractional controlled- $Z$  gates as described.
- 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  $\theta_v$  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 for  $U_2$ . The composite circuit for  $U_3 U_2 U_1$  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  $U_3 U_2 U_1$  can differ from  $U$  by at most a scalar factor by Lemma 1; so the circuit obtained implements the operation  $U$ .  $\square$

## C Derivation of quadratic form expansions for Clifford group operations

Define the following notation for bit-flip and phase-flip operators on a qubit  $t$  out of a collection  $\{1, \dots, n\}$ :

$$P_t = X_t, \quad P_{n+t} = Z_t. \quad (15)$$

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

matrix  $M$  over  $\mathbb{Z}_2$ . Then, we may represent a  $n$  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

$$UP_tU^\dagger = i^{d_t(C)} (-1)^{h_t} \bigotimes_{j=1}^n \left[ Z_h^{C_{(n+j)t}} X_h^{C_{jt}} \right] \quad (16)$$

for each  $1 \leq t \leq 2n$ . (Note that the factor of  $i^{d_t(C)}$  is only necessary to map Hermitian Pauli operators to other Hermitian operators, 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 (16).<sup>5</sup>

Provided a Leuven tableau  $(C, \mathbf{h})$  for a Clifford group operation  $U$ , [13] provides a matrix formula for  $U$  which we may obtain for  $U$ , as follows. Decompose  $C$  as a block matrix  $C = \begin{bmatrix} E & F \\ G & H \end{bmatrix}$  with  $n \times n$  blocks, and then find invertible matrices  $\tilde{R}_1, \tilde{R}_2$  over  $\mathbb{Z}_2$  such that  $\tilde{R}_1^{-1}G\tilde{R}_2 = \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{1}_r \end{bmatrix}$  for some  $r < n$  (using *e.g.* the decomposition algorithm of [18] to obtain  $\tilde{R}_1$  and  $\tilde{R}_2$  in terms of elementary row operations). Then, define the matrices

$$\begin{bmatrix} \tilde{E}_{11} & \tilde{E}_{12} \\ \tilde{E}_{21} & \tilde{E}_{22} \end{bmatrix} = \tilde{R}_1^\top E \tilde{R}_2, \quad R_1 = \tilde{R}_1, \quad R_2 = \begin{bmatrix} \tilde{E}_{11}^{-1} & 0 \\ 0 & \mathbb{1}_r \end{bmatrix}^\top \tilde{R}_2^\top, \quad (17)$$

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

$$\begin{bmatrix} \mathbb{1}_{n-r} & E_{12} & F_{11} & F_{12} \\ E_{21} & E_{22} & F_{21} & F_{22} \\ 0 & 0 & H_{11} & H_{12} \\ 0 & \mathbb{1}_r & H_{21} & H_{22} \end{bmatrix} = \begin{bmatrix} R_1^\top & 0 \\ 0 & R_1^{-1} \end{bmatrix} C \begin{bmatrix} R_2^\top & 0 \\ 0 & R_2^{-1} \end{bmatrix}, \quad (18)$$

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

$$M_{br} = \begin{bmatrix} F_{11} + E_{12}H_{21} & E_{12} \\ E_{12}^\top & E_{22} \end{bmatrix}, \quad M_{bc} = \begin{bmatrix} 0 & H_{21}^\top \\ H_{21} & H_{22} \end{bmatrix}. \quad (19)$$

Next, define

$$\begin{aligned} \mathbf{d}_{br} &= \text{diag}(M_{br}), & \mathbf{d}_{bc} &= \text{diag}(M_{bc}), \\ L_{br} &= \text{lower}(M_{br} + \mathbf{d}_{br}\mathbf{d}_{br}^\top), & L_{bc} &= \text{lower}(M_{bc} + \mathbf{d}_{bc}\mathbf{d}_{bc}^\top), \end{aligned} \quad (20)$$

<sup>5</sup> Note that the block matrix  $[C^\top \mathbf{h}]$  is similar to a *destabilizer tableau* as defined by Aaronson and Gottesman [15]. The characterization in (16) of Clifford group operations in terms of a matrix  $C$  and vector  $\mathbf{h}$  follows [13].

where  $\text{lower}(M)$  is the strictly lower-triangular part of a square matrix  $M$  (with all other coefficients set to 0). Finally, define  $\Pi_r = \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{1}_r \end{bmatrix}$  and  $\Pi_r^\perp = \mathbb{1}_n - \Pi_r$  for the sake of brevity, and let<sup>6</sup>

$$\mathbf{t} = [\mathbb{1}_n \ 0] \mathbf{h} + \text{diag} \left( [R_2^{-1} \Pi_r] L_{br} [R_2^{-1} \Pi_r]^\top \right), \quad (21)$$

$$\begin{aligned} \mathbf{h}_{bc} = [0 \ R_2^{-\top}] \mathbf{h} + R_2^{-\top} \text{diag} \left( R_2^\top [L_{bc} + \Pi_r M_{bc} \right. \\ \left. + (\Pi_r^\perp + \Pi_r M_{bc}) L_{br} (\Pi_r^\perp + M_{bc} \Pi_r)] R_2 \right). \end{aligned} \quad (22)$$

Then Theorem 6 of [13] states that the unitary operation  $U$  for the Clifford operation characterized by  $(C, \mathbf{h})$  is given by the matrix formula

$$U = \frac{1}{\sqrt{2^r}} \sum_{\substack{\mathbf{x}_b \in \{0,1\}^{n-r} \\ \mathbf{x}_c, \mathbf{x}_r \in \{0,1\}^r}} \left[ \begin{aligned} & (-1)^{(\mathbf{x}_{br}^\top L_{br} \mathbf{x}_{br} + \mathbf{x}_r^\top \mathbf{x}_c + \mathbf{x}_{bc}^\top L_{bc} \mathbf{x}_{bc} + \mathbf{h}_{bc}^\top \mathbf{x}_{bc})} \times \\ & (-i)^{(\mathbf{d}_{br}^\top \mathbf{x}_{br} + \mathbf{d}_{bc}^\top \mathbf{x}_{bc})} |R_1 \mathbf{x}_{br}\rangle \langle R_2^{-1} \mathbf{x}_{bc} + \mathbf{t}| \end{aligned} \right], \quad (23)$$

where  $\mathbf{x}_{br} = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_r \end{bmatrix}$  and  $\mathbf{x}_{bc} = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_c \end{bmatrix}$  are  $n$  bit boolean vectors.

The formula in (23) shows strong similarities to a quadratic form expansion. In particular, consider disjoint sets  $V_b$ ,  $V_r$ , 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 for  $\mathbf{x} \in \{0, 1\}^V$ :

$$\mathbf{x}_I = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_c \end{bmatrix} = \begin{bmatrix} \mathbf{x}_{V_b} \\ \mathbf{x}_{V_c} \end{bmatrix} \in \{0, 1\}^I, \quad \mathbf{x}_O = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_r \end{bmatrix} = \begin{bmatrix} \mathbf{x}_{V_b} \\ \mathbf{x}_{V_r} \end{bmatrix} \in \{0, 1\}^O, \quad (24)$$

$$\begin{aligned} Q(\mathbf{x}) = \pi \left( \mathbf{x}_O^\top L_{br} \mathbf{x}_O + \mathbf{x}_O^\top \Pi_r \mathbf{x}_I + \mathbf{x}_I^\top L_{bc} \mathbf{x}_I + \mathbf{x}_I^\top \mathbf{h}_{bc} \mathbf{h}_{bc}^\top \mathbf{x}_I \right) \\ - \frac{\pi}{2} \left( \mathbf{x}_O^\top \mathbf{d}_{br} \mathbf{d}_{br}^\top \mathbf{x}_O + \mathbf{x}_I^\top \mathbf{d}_{bc} \mathbf{d}_{bc}^\top \mathbf{x}_I \right). \end{aligned} \quad (25)$$

Then, (23) is equivalent to

$$U = \frac{1}{\sqrt{2^r}} \sum_{\mathbf{x} \in \{0,1\}^V} e^{iQ(\mathbf{x})} |R_1 \mathbf{x}_O\rangle \langle R_2^{-1} \mathbf{x}_I + \mathbf{t}|. \quad (26)$$

To obtain a 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

<sup>6</sup> The vector formulas given here for  $\mathbf{t}$  and  $\mathbf{h}_{bc}$  may be obtained by repeated application of Theorem 2 of [13].

the changes of variables do not 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

$$\mathbb{1}_2 = \sum_{\mathbf{x} \in \{0,1\}^2} \delta_{x_1, x_2} |x_2\rangle \langle x_1| = \frac{1}{2} \sum_{\mathbf{x} \in \{0,1\}^3} (-1)^{x_1 x_3 + x_2 x_3} |x_2\rangle \langle x_1| \quad (27)$$

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

$$\mathbf{x}_I = \begin{bmatrix} \mathbf{x}_b \\ \mathbf{x}_c \end{bmatrix} \in \{0,1\}^I, \quad \mathbf{x}_{O'} = \begin{bmatrix} \mathbf{x}_{b'} \\ \mathbf{x}_r \end{bmatrix} \in \{0,1\}^{O'}, \quad (28)$$

$$\begin{aligned} Q'(\mathbf{x}_I, \mathbf{x}_a, \mathbf{x}_{O'}) &= \pi \left( \mathbf{x}_{O'}^\top L_{br} \mathbf{x}_{O'} + \mathbf{x}_{O'}^\top \Pi_r \mathbf{x}_I + \mathbf{x}_I^\top L_{bc} \mathbf{x}_I + \mathbf{h}_{bc}^\top \mathbf{x}_I \right) \\ &\quad + \pi \mathbf{x}_I^\top \begin{bmatrix} \mathbb{1}_{n-r} \\ 0 \end{bmatrix} \mathbf{x}_a + \pi \mathbf{x}_{O'}^\top \begin{bmatrix} \mathbb{1}_{n-r} \\ 0 \end{bmatrix} \mathbf{x}_a \\ &\quad - \frac{\pi}{2} \left( \mathbf{d}_{br}^\top \mathbf{x}_{O'} + \mathbf{d}_{bc}^\top \mathbf{x}_I \right). \quad (29) \end{aligned}$$

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  $\mathbf{x}_a$ .

We therefore have

$$\begin{aligned} &\sum_{\mathbf{x} \in \{0,1\}^V} e^{iQ(\mathbf{x})} |R_1 \mathbf{x}_O\rangle \langle R_2^{-1} \mathbf{x}_I + \mathbf{t}| \\ &= \sum_{\mathbf{x}_I, \mathbf{x}_{O'}} \delta_{\mathbf{x}_b, \mathbf{x}_{b'}} e^{iQ'(\mathbf{x}_I, \mathbf{0}, \mathbf{x}_{O'})} |R_1 \mathbf{x}_{O'}\rangle \langle R_2^{-1} \mathbf{x}_I + \mathbf{t}| \\ &= \frac{1}{2^{n-r}} \sum_{\mathbf{x} \in \{0,1\}^{V'}} e^{iQ'(\mathbf{x}_I, \mathbf{x}_a, \mathbf{x}_{O'})} |R_1 \mathbf{x}_{O'}\rangle \langle R_2^{-1} \mathbf{x}_I + \mathbf{t}|. \quad (30) \end{aligned}$$

Substituting the final expression of (30) into (26) and performing the appropriate change of variables, we have

$$U = \frac{\sqrt{2^r}}{2^n} \sum_{\mathbf{x} \in \{0,1\}^{V'}} e^{iQ'(R_2[\mathbf{x}_I + \mathbf{t}], \mathbf{x}_a, R_1^{-1} \mathbf{x}_{O'})} |\mathbf{x}_{O'}\rangle \langle \mathbf{x}_I|. \quad (31)$$

Note that the quadratic form of the expansion in (31) has only angles  $\theta_{uv}$  which are multiples of  $\frac{\pi}{2}$ , with  $\theta_{uv} \in \{0, \pi\}$  for  $u \neq v$ . Using the analysis of

Section 2, this represents the positive branch of a one-way measurement pattern on the geometry  $(G', I, O')$  of the quadratic form expansion of 31, using only  $X$  or  $Y$  basis measurements and having only  $n-r$  auxiliary vertices. These observables all commute or anti-commute with the operators  $K(v) = X_v \prod_{v \sim w} Z_w$  for  $v \in I^c$  (where  $\sim$  is the adjacency relation of  $G$ ), which are the stabilizer generators of the family of entangled states which is prepared by the entanglement operations of the measurement pattern. Precisely because the measurement pattern performs a unitary operation in the positive branch, none of the measurements commute with *all* of the generators  $K(v)$  for  $v \in I^c$ ; otherwise, the space of output states would have smaller dimension than the input. Then, we know that the stabilizer formalism will produce some by-product operations for each of the measurements to be made. This allows us to obtain a measurement pattern on  $n$  inputs,  $n$  outputs, and  $n-r$  auxiliary vertices performing the unitary  $U$ . A reduced measurement pattern can then be obtained using the transformations described in [14], which will require  $O(n)$  local complementation operations.

The ability to obtain a quadratic form expansion representing an almost completely reduced measurement pattern allows us to obtain a more efficient algorithm to find totally reduced Clifford patterns from descriptions of how it transforms the Pauli group. The quadratic form of (31) 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  $R_2$ . The local complementations required to remove the  $n-r$  auxiliary qubits of  $V_a$  can each be performed in time  $O(n^2)$ , so that the total running time to obtain a reduced pattern is  $O(n^3)$ . 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 [15]. To obtain a measurement pattern from such a circuit by composing the patterns for each gate, removing vertices opportunistically, takes 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.