

ARTICLE OPEN



Simulating quantum computations with Tutte polynomials

Ryan L. Mann ^{1,2}

We establish a classical heuristic algorithm for exactly computing quantum probability amplitudes. Our algorithm is based on mapping output probability amplitudes of quantum circuits to evaluations of the Tutte polynomial of graphic matroids. The algorithm evaluates the Tutte polynomial recursively using the deletion–contraction property while attempting to exploit structural properties of the matroid. We consider several variations of our algorithm and present experimental results comparing their performance on two classes of random quantum circuits. Further, we obtain an explicit form for Clifford circuit amplitudes in terms of matroid invariants and an alternative efficient classical algorithm for computing the output probability amplitudes of Clifford circuits.

npj Quantum Information (2021)7:141; <https://doi.org/10.1038/s41534-021-00477-0>

INTRODUCTION

There is a natural relationship between quantum computation and evaluations of Tutte polynomials^{1,2}. In particular, quantum probability amplitudes are proportional to evaluations of the Tutte polynomial of graphic matroids. In this paper, we use this relationship to establish a classical heuristic algorithm for exactly computing quantum probability amplitudes. While this problem is known to be #P-hard in general³, our algorithm focuses on exploiting structural properties of an instance to achieve an improved runtime over traditional methods. Previously it was known that this problem can be solved in time exponential in the treewidth of the underlying graph⁴.

The basis of our algorithm is a mapping between output probability amplitudes of quantum circuits and evaluations of the Tutte polynomial of graphic matroids^{2,5,6}. Our algorithm proceeds to evaluate the Tutte polynomial recursively using the deletion–contraction property. At each step in the recursion, our algorithm computes certain structural properties of the matroid in order to attempt to prune the computational tree. This approach to computing Tutte polynomials was first studied by Haggard et al.⁷. Our algorithm can be seen as an adaption of their work to special points of the Tutte plane where we can exploit additional structural properties.

The performance of algorithms for computing Tutte polynomials based on the deletion–contraction property depends on the heuristic used to decide the ordering of the recursion^{7–9}. We consider several heuristics introduced by Pearce et al.⁸ and an additional heuristic, which is specific to our algorithm. We present some experimental results comparing the performance of these heuristics on two classes of random quantum circuits corresponding to dense and sparse instances.

The correspondence between output probability amplitudes of quantum circuits and evaluations of Tutte polynomials also allows us to obtain an explicit form for Clifford circuit amplitudes in terms of matroid invariants by a theorem of Pendavingh¹⁰. This gives rise to an alternative efficient classical algorithm for computing output probability amplitudes of Clifford circuits.

This paper is structured as follows. We introduce matroid theory in “Matroid theory” and the Tutte polynomial in “The Tutte polynomial.” In “The Potts model partition function,”

“Instantaneous quantum polynomial time,” and “Quantum computation and the Tutte polynomial,” we establish a mapping between output probability amplitudes of quantum circuits and evaluations of the Tutte polynomial of graphic matroids. This is achieved by introducing the Potts model partition function in “The Potts model partition function,” instantaneous quantum polynomial (IQP) time circuits in “Instantaneous quantum polynomial time,” and a class of universal quantum circuits in “Quantum computation and the Tutte polynomial.” In “Efficient classical simulation of Clifford circuits,” we use this mapping to obtain an explicit form for Clifford circuit amplitudes in terms of matroid invariants. We also obtain an efficient classical algorithm for computing the output probability amplitudes of Clifford circuits. We describe our algorithm in “Algorithm overview” and present some experimental results in “Experimental results.” Finally, we conclude in “Discussion.”

RESULTS

Matroid theory

We shall now briefly introduce the theory of matroids. The interested reader is referred to the classic textbooks of Welsh¹¹ and Oxley¹² for a detailed treatment. Matroids were introduced by Whitney¹³ as a structure that generalises the notion of linear dependence. There are many equivalent ways to define a matroid. We shall define a matroid by the independence axioms.

Definition 1 (matroid). A matroid is a pair $M = (S, \mathcal{I})$ consisting of a finite set S , known as the ground set, and a collection \mathcal{I} of subsets of S , known as the independent sets, such that the following axioms are satisfied:

- (1) The empty set is a member of \mathcal{I} .
- (2) Every subset of a member of \mathcal{I} is a member of \mathcal{I} .
- (3) If A and B are members of \mathcal{I} and $|A| > |B|$, then there exists an $x \in A \setminus B$ such that $B \cup \{x\}$ is a member of \mathcal{I} .

The rank of a subset A of S is given by the rank function $r : 2^S \rightarrow \mathbb{N}$ of the matroid defined by $r(A) := \max(|X| \mid X \subseteq A, X \in \mathcal{I})$. The rank of a matroid M , denoted $r(M)$, is the rank of the set S .

¹School of Mathematics, University of Bristol, Bristol BS8 1UG, UK. ²Centre for Quantum Computation and Communication Technology, Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia. email: mail@ryanmann.org

The archetypal class of matroids is vector matroids. A vector matroid $M = (S, \mathcal{I})$ is a matroid whose ground set S is a subset of a vector space over a field \mathbb{F} and whose independent sets \mathcal{I} are the linearly independent subsets of S . The rank of a subset of a vector matroid is the dimension of the subspace spanned by the corresponding vectors. We say that a matroid is \mathbb{F} -representable if it is isomorphic to a vector matroid over the field \mathbb{F} . A matroid is a binary matroid if it is \mathbb{F}_2 -representable and is a ternary matroid if it is \mathbb{F}_3 -representable. A matroid that is representable over every field is called a regular matroid.

Every finite graph $G = (V, E)$ induces a matroid $M(G) = (S, \mathcal{I})$ as follows. Let the ground set S be the set of edges E and let the independent sets \mathcal{I} be the subsets of E that are a forest, i.e., they do not contain a simple cycle. It is easy to check that $M(G)$ satisfies the independence axioms. The rank of a subset A of a cycle matroid is $|V| - \kappa(A)$, where $\kappa(A)$ denotes the number of connected components of the subgraph with edge set A . The rank of the cycle matroid $M(G)$, denoted $r(M(G))$ or simply $r(G)$, is the rank of the set E . The matroid $M(G)$ is called the cycle matroid of G . We say that a matroid is graphic if it is isomorphic to the cycle matroid of a graph.

Graphic matroids are regular. To see this, consider assigning to the graph G an arbitrary orientation $D(G)$, that is, for each edge $e = \{u, v\}$ in G , we choose one of u and v to be the positive end and the other one to be the negative end. Then, construct the oriented incidence matrix of G with respect to the orientation $D(G)$.

Definition 2 (oriented incidence matrix). Let $G = (V, E)$ be a graph and let $D(G)$ be an orientation of G . Then, the oriented incidence matrix of G with respect to $D(G)$ is the $|V| \times |E|$ matrix $A_{D(G)} = (a_{ve})_{|V| \times |E|}$ whose entries are

$$a_{ve} = \begin{cases} +1, & \text{if } v \text{ is the positive end of } e; \\ -1, & \text{if } v \text{ is the negative end of } e; \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

The rows of the oriented incidence matrix $A_{D(G)}$ correspond to the vertices of G and the columns correspond to the edges of G . Each column contains exactly one $+1$ and exactly one -1 representing the positive and negative ends of the corresponding edge. If the column space of $A_{D(G)}$ is the ground set of a vector matroid, then it is easy to see that a subset is independent if and only if it is a forest in G . Hence, the oriented incidence matrix provides a representation of a graphic matroid over every field.

A minor of a matroid M is a matroid that is obtained from M by a sequence of deletion and contraction operations.

Definition 3 (deletion). Let $M = (S, \mathcal{I})$ be a matroid and let e be an element of the ground set. Then, the deletion of M with respect to e is the matroid $M \setminus \{e\} = (S', \mathcal{I}')$ whose ground set is $S' = S \setminus \{e\}$ and whose independent sets are $\mathcal{I}' = \{I \subseteq S \setminus \{e\} \mid I \in \mathcal{I}\}$.

The deletion of an element from the cycle matroid of a graph corresponds to removing an edge from the graph.

Definition 4 (contraction). Let $M = (S, \mathcal{I})$ be a matroid and let e be an element of the ground set. Then, the contraction of M with respect to e is the matroid $M/\{e\} = (S', \mathcal{I}')$ whose ground set is $S' = S \setminus \{e\}$ and whose independent sets are $\mathcal{I}' = \{I \subseteq S \setminus \{e\} \mid I \cup \{e\} \in \mathcal{I}\}$.

The contraction of an element from the cycle matroid of a graph corresponds to removing an edge from the graph and merging its two endpoints.

An element e of a matroid is said to be a loop if $\{e\}$ is not an independent set and said to be a coloop if e is contained in every maximally independent set. If an element e of a matroid is either a loop or a coloop then the deletion and contraction of e are equivalent.

The Tutte polynomial

We shall now briefly introduce the Tutte polynomial, which is a well-known invariant in matroid and graph theory.

Definition 5 (Tutte polynomial of a matroid). Let $M = (S, \mathcal{I})$ be a matroid with rank function $r: 2^S \rightarrow \mathbb{N}$. Then, the Tutte polynomial of M is the bivariate polynomial defined by

$$T(M; x, y) := \sum_{A \subseteq S} (x-1)^{r(M)-r(A)} (y-1)^{|A|-r(A)}. \quad (2)$$

The Tutte polynomial may also be defined recursively by the deletion–contraction property.

Definition 6 (deletion–contraction property). Let $M = (S, \mathcal{I})$ be a matroid. If M is the empty matroid, i.e., $S = \emptyset$, then

$$T(M; x, y) = 1. \quad (3)$$

Otherwise, let e be an element of the ground set. If e is a loop, then

$$T(M; x, y) = yT(M \setminus \{e\}; x, y). \quad (4)$$

If e is a coloop, then

$$T(M; x, y) = xT(M/\{e\}; x, y). \quad (5)$$

Finally, if e is neither a loop nor a coloop, then

$$T(M; x, y) = T(M \setminus \{e\}; x, y) + T(M/\{e\}; x, y). \quad (6)$$

The deletion–contraction property immediately gives an algorithm for recursively computing the Tutte polynomial. This algorithm is in general inefficient, but the performance may be improved by using isomorphism testing to reduce the number of recursive calls¹⁴. The performance of this algorithm depends on the heuristic used to choose elements of the ground set^{7–9}. Björklund et al.¹⁵ showed that the Tutte polynomial can be computed in time exponential in the number of vertices.

The Tutte polynomial of a graph may be recovered by considering the Tutte polynomial of the cycle matroid of a graph and using the fact that the rank of a subset A of a cycle matroid is $|V| - \kappa(A)$, where $\kappa(A)$ denotes the number of connected components of the subgraph with edge set A .

Definition 7 (Tutte polynomial of a graph). Let $G = (V, E)$ be a graph and let $\kappa(A)$ denote the number of connected components of the subgraph with edge set A . Then, the Tutte polynomial of G is a polynomial in x and y , defined by

$$T(G; x, y) := \sum_{A \subseteq E} (x-1)^{\kappa(A)-\kappa(E)} (y-1)^{\kappa(A)+|A|-|V|}. \quad (7)$$

The Tutte polynomial is trivial to evaluate along the hyperbola $(x-1)(y-1) = 1$ for any matroid. In the case of graphic matroids, Jaeger et al.¹⁶ showed that the Tutte polynomial is #P-hard to evaluate, except along this hyperbola and when (x, y) equals one of nine special points.

Theorem 1 (Jaeger et al.¹⁶). The problem of evaluating the Tutte polynomial of a graphic matroid at an algebraic point in the

(x,y) -plane is #P-hard except when $(x-1)(y-1) = 1$ or when (x,y) equals one of $(1,1)$, $(-1,-1)$, $(0,-1)$, $(-1,0)$, $(i,-i)$, $(-i,i)$, (j,j^2) , (j^2,j) , or (j^2,j) , where $j = \exp(2\pi i/3)$. In each of these exceptional cases the evaluation can be done in polynomial time.

Vertigan¹⁷ extended this result to vector matroids.

Theorem 2 (Vertigan¹⁷). The problem of evaluating the Tutte polynomial of a vector matroid over a field \mathbb{F} at an algebraic point in the (x,y) -plane is #P-hard except when $(x-1)(y-1) = 1$, (x,y) equals $(1,1)$, or when

- (1) $|\mathbb{F}| = 2$ and (x,y) equals one of $(-1,-1)$, $(0,-1)$, $(-1,0)$, $(i,-i)$, or $(-i,i)$;
- (2) $|\mathbb{F}| = 3$ and (x,y) equals one of (j,j^2) or (j^2,j) , where $j = \exp(2\pi i/3)$; or
- (3) $|\mathbb{F}| = 4$ and (x,y) equals $(-1,-1)$.

In each of these exceptional cases, except when (x,y) equals $(1,1)$, the evaluation can be done in polynomial time.

Snook¹⁸ showed that when (x,y) equals $(1,1)$ and \mathbb{F} is either a finite field of fixed characteristic or a fixed infinite field, then evaluating the Tutte polynomial is #P-hard. It is an open problem to understand the complexity of evaluating the Tutte polynomial at $(1,1)$ over any fixed field.

The Potts model partition function

The Potts model is a statistical physical model described by an integer $q \in \mathbb{Z}^+$ and a graph $G = (V,E)$, with the vertices representing spins and the edges representing interactions between them. A set of edge weights $\{\omega_e\}_{e \in E}$ characterises the interactions and a set of vertex weights $\{u_v\}_{v \in V}$ characterises the external fields at each spin. A configuration of the model is an assignment σ of each spin to one of q possible states. The Potts model partition function is defined as follows.

Definition 8 (Potts model partition function). Let $q \in \mathbb{Z}^+$ be an integer and let $G = (V,E)$ be a graph with the weights $\Omega = \{\omega_e\}_{e \in E}$ assigned to its edges and the weights $\Upsilon = \{u_v\}_{v \in V}$ assigned to its vertices. Then, the q -state Potts model partition function is defined by

$$Z_{\text{Potts}}(G; q, \Omega, \Upsilon) := \sum_{\sigma \in \mathbb{Z}_q^V} w_G(\sigma), \quad (8)$$

where

$$w_G(\sigma) = \exp\left(\sum_{\{u,v\} \in E} \omega_{\{u,v\}} \delta(\sigma_u, \sigma_v) + \sum_{v \in V} u_v \delta(\sigma_v)\right). \quad (9)$$

The Potts model partition function with an external field is equivalent to the zero-field case on an augmented graph $G' = (V', E')$. To construct G' from G , for each of the connected components $\{C_i\}_{i=1}^{k(E)}$ of G add a new vertex u_i and for every vertex $v \in V(C_i)$ add an edge $e_v = \{u_i, v\}$ with the weight u_v assigned to it. Then, we have the following proposition.

Proposition 3.

$$Z_{\text{Potts}}(G; q, \Omega, \Upsilon) = q^{-k(E)} Z_{\text{Potts}}(G'; q, \Omega \cup \Upsilon, 0). \quad (10)$$

A similar proposition appears in Welsh's monograph¹⁹; we prove Proposition 3 in Supplementary Note 1.

It will be convenient to consider the Potts model with weights that are all positive integer multiples of a complex number θ . We shall implement this model on the augmented graph G' with all

weights equal to θ by replacing each edge with the appropriate number of parallel edges. Let us denote the partition function of this model by $Z_{\text{Potts}}(G'; q, \theta)$. Then, we have the following proposition relating the partition function of this model to the Tutte polynomial of the augmented graph G' .

Proposition 4.

$$Z_{\text{Potts}}(G'; q, \theta) = q^{k(E')} (e^\theta - 1)^{r(G')} T(G'; x, y), \quad (11)$$

where $x = \frac{e^\theta + q - 1}{e^\theta - 1}$ and $y = e^\theta$.

In particular, the q -state Potts model partition function is related to the Tutte polynomial along the hyperbola $(x-1)(y-1) = q$. For a proof of Proposition 4, we refer the reader to Welsh's monograph¹⁹ [Section 4.4].

The two-state Potts model partition function specialises to the Ising model partition function.

Definition 9 (Ising model partition function). Let $G = (V,E)$ be a graph with the weights $\Omega = \{\omega_e\}_{e \in E}$ assigned to its edges and the weights $\Upsilon = \{u_v\}_{v \in V}$ assigned to its vertices. Then, the Ising model partition function is defined by

$$Z_{\text{Ising}}(G; \Omega, \Upsilon) := \sum_{\sigma \in \{-1,+1\}^V} w_G(\sigma), \quad (12)$$

where

$$w_G(\sigma) = \exp\left(\sum_{\{u,v\} \in E} \omega_{\{u,v\}} \sigma_u \sigma_v + \sum_{v \in V} u_v \sigma_v\right). \quad (13)$$

Proposition 5.

$$Z_{\text{Potts}}(G; 2, \Omega, \Upsilon) = w_G Z_{\text{Ising}}\left(G; \frac{\Omega}{2}, \frac{\Upsilon}{2}\right), \quad (14)$$

where $w_G = \exp(\frac{1}{2} \sum_{e \in E} \omega_e + \frac{1}{2} \sum_{v \in V} u_v)$.

Proof. The proof follows from some simple algebra.

Instantaneous quantum polynomial time

We shall now briefly introduce the class of commuting quantum circuits, known as IQP time circuits⁵. These circuits exhibit many interesting mathematical properties. In particular, the output probability amplitudes of IQP circuits are proportional to evaluations of the Tutte polynomial of binary matroids². IQP circuits comprise only gates that are diagonal in the Pauli-X basis and are described by an X-program.

Definition 10 (X-program). An X-program is a pair (P, θ) , where $P = (p_{ij})_{m \times n}$ is a binary matrix and $\theta \in [-\pi, \pi]$ is a real angle. The matrix P is used to construct a Hamiltonian of m commuting terms acting on n qubits, where each term in the Hamiltonian is a product of Pauli-X operators

$$H_{(P, \theta)} := -\theta \sum_{i=1}^m \bigotimes_{j=1}^n X_j^{p_{ij}}. \quad (15)$$

Thus, the columns of P correspond to qubits and the rows of P correspond to interactions in the Hamiltonian.

An X-program induces a probability distribution $\mathcal{P}_{(P, \theta)}$ known as an IQP distribution.

Definition 11 ($\mathcal{P}_{(P, \theta)}$). For an X-program (P, θ) with $P = (p_{ij})_{m \times n}$, we define $\mathcal{P}_{(P, \theta)}$ to be the probability distribution over binary

strings $x \in \{0, 1\}^n$, given by

$$\Pr[x] := |\psi_{(P,\theta)}(x)|^2, \quad (16)$$

where

$$\psi_{(P,\theta)}(x) = \langle x | \exp(-iH_{(P,\theta)}) | 0^n \rangle. \quad (17)$$

The principal probability amplitude $\psi_{(P,\theta)}(0^n)$ of an IQP distribution is directly related to an evaluation of the Tutte polynomial of the binary matroid whose ground set is the row space of P .

Proposition 6. Let (P,θ) be an X-program with $P = (p_{ij})_{m \times n}$. Let $M = (\mathcal{S}, \mathcal{I})$ be the binary matroid whose ground set \mathcal{S} is the row space of P , then

$$\psi_{(P,\theta)}(0) = e^{i\theta(r(M)-m)} (i \sin(\theta))^{r(M)} T(M; x, y), \quad (18)$$

where $x = -i \cot(\theta)$ and $y = e^{2i\theta}$.

A similar result may be obtained for the other probability amplitudes. This can easily be seen when $\theta = \frac{\pi}{2k}$ for $k \in \mathbb{Z}^+$, by firstly letting $P||^k x$ be the matrix obtained from P by appending k rows identical to x , and then observing that $\psi_{(P,\theta)}(x) = -i \psi_{(P||^k x, \theta)}(0^n)$. For a proof of Proposition 6 and a treatment of the general θ case, we refer the reader to ref. ² ["Discussion"].

We shall consider X-programs that are induced by a weighted graph.

Definition 12 (graph-induced X-program). For a graph $G = (V, E)$ with the weights $\{\omega_e \in [-\pi, \pi]\}_{e \in E}$ assigned to its edges and the weights $\{u_v \in [-\pi, \pi]\}_{v \in V}$ assigned to its vertices, we define the X-program induced by G to be an X-program \mathcal{X}_G such that

$$H_{\mathcal{X}_G} = - \sum_{\{u,v\} \in E} \omega_{\{u,v\}} X_u X_v - \sum_{v \in V} u_v X_v. \quad (19)$$

Any X-program can be efficiently represented by a graph-induced X-program⁵. The principal probability amplitude $\psi_{\mathcal{X}_G}(0^n)$ of the IQP distribution generated by a graph-induced X-program is directly related to the Ising model partition function of the graph with imaginary weights.

Proposition 7. Let $G = (V, E)$ be a graph with the weights $\Omega = \{\omega_e \in [-\pi, \pi]\}_{e \in E}$ assigned to its edges and the weights $\Upsilon = \{u_v \in [-\pi, \pi]\}_{v \in V}$ assigned to its vertices, then

$$\psi_{\mathcal{X}_G}(0^{|V|}) = \frac{1}{2^{|V|}} Z_{\text{Ising}}(G; i\Omega, i\Upsilon). \quad (20)$$

Proposition 7 is well known^{20,21}; we provide a proof in Supplementary Note 2. It will be convenient to consider graph-induced X-programs $\mathcal{X}_{G(\theta)}$ with weights that are all positive integer multiples of a real angle θ . As in "Results," this model can be implemented on the augmented graph $G' = (V', E')$ with all weights equal to θ by replacing each edge with the appropriate number of parallel edges. Let us denote the graph-induced X-program of this model by $\mathcal{X}_{G'(\theta)}$. Then, we have the following proposition.

Proposition 8.

$$\psi_{\mathcal{X}_{G(\theta)}}(0^{|V|}) = \psi_{\mathcal{X}_{G'(\theta)}}(0^{|V'|}). \quad (21)$$

We prove Proposition 8 in Supplementary Note 3. We also have the following proposition relating the principal

probability amplitude to the Tutte polynomial of the augmented graph.

Proposition 9.

$$\psi_{\mathcal{X}_{G'(\theta)}}(0^{|V'|}) = e^{i\theta(r(G')-|E'|)} (i \sin(\theta))^{r(G')} T(G'; x, y), \quad (22)$$

where $x = -i \cot(\theta)$ and $y = e^{2i\theta}$.

We prove Proposition 9 in Supplementary Note 4. Note that if we let $M = (\mathcal{S}, \mathcal{I})$ be the binary matroid whose ground set \mathcal{S} is the column space of the orientated incidence matrix $A_{D(G')}$ of G' with an arbitrary orientation $D(G')$ assigned to it, then we can use Proposition 6 to obtain Proposition 9.

Quantum computation and the Tutte polynomial

In this section, we show that quantum probability amplitudes may be expressed in terms of the evaluation of a Tutte polynomial. We achieve this by showing that output probability amplitudes of a class of universal quantum circuits are proportional to the principal probability amplitude of some IQP circuit.

It will be convenient to define the following gate set.

Definition 13 (\mathcal{G}_θ). For a real angle $\theta \in [-\pi, \pi]$, we define \mathcal{G}_θ to be the gate set

$$\mathcal{G}_\theta := \{H, e^{i\theta X}, e^{i\theta XX}\}, \quad (23)$$

where H denotes the Hadamard gate.

It is easy to see that the gate set $\mathcal{G}_{\frac{\pi}{4}}$ generates the Clifford group and the gate set $\mathcal{G}_{\frac{\pi}{8}}$ is universal for quantum computation.

In the IQP model it is easy to implement the gates $e^{i\theta X}$ and $e^{i\theta XX}$. So in order to implement the entire gate set \mathcal{G}_θ , it remains to show that we can implement the Hadamard gate. This can be achieved by the use of postselection when $\theta = \frac{\pi}{4k}$ for $k \in \mathbb{Z}^+$ ⁶. To apply a Hadamard gate to the target state $|a\rangle_t$ consider the following Hadamard gadget. Firstly, introduce an ancilla qubit in the state $|0\rangle_a$ and apply the gate $e^{\frac{i\theta}{4}(1-X)_t(1-X)_a}$ to $|a\rangle_t |0\rangle_a$. Then, measure qubit t in the computational basis and postselect on an outcome of 0. The output state of this gadget is then $H|a\rangle_a$.

We shall consider quantum circuits that comprise gates from the set $\mathcal{G}_{\frac{\pi}{4k}}$ for an integer $k \in \mathbb{Z}^+$. Let $C_{k,n,m}$ denote such a circuit that acts on n qubits and comprises m Hadamard gates. Further let $\mathcal{X}_G(C_{k,n,m})$ denote the graph-induced X-program that implements the circuit $C_{k,n,m}$ by replacing each of the m Hadamard gates with the Hadamard gadget. Then, we have the following proposition.

Proposition 10.

$$\langle 0^n | C_{k,n,m} | 0^n \rangle = \sqrt{2}^m \psi_{\mathcal{X}_G(C_{k,n,m})}(0^{n+m}). \quad (24)$$

Proof. The proof follows immediately from the application of the Hadamard gadgets.

Any quantum amplitude may therefore be expressed as the evaluation of a Tutte polynomial by Propositions 8–10.

Efficient classical simulation of Clifford circuits

In this section, we show how the correspondence between quantum computation and evaluations of the Tutte polynomial provides an explicit form for Clifford circuit amplitudes in terms of matroid invariants, namely, the bicycle dimension and Brown's invariant. This gives rise to an efficient classical algorithm for computing the output probability amplitudes of Clifford circuits. We note that it was first observed by Shepherd² that to compute the probability amplitude of a Clifford circuit, it is sufficient to evaluate the Tutte polynomial of a binary matroid at the point (x, y)

equals $(-i, i)$, which can be efficiently computed by Vertigan's algorithm¹⁷. We proceed with some definitions.

Let V be a linear subspace of \mathbb{F}_2^n . The bicycle dimension and Brown's invariant are defined as follows.

Definition 14 (bicycle dimension). The bicycle dimension of V is defined by

$$d(V) := \dim(V \cap V^\perp). \quad (25)$$

Definition 15 (Brown's invariant). If $|\text{supp}(x)| \equiv 0 \pmod{4}$ for all $x \in V \cap V^\perp$, then Brown's invariant $\sigma(V)$ is defined to be the smallest integer such that

$$\sum_{x \in V} i^{|\text{supp}(x)|} = \sqrt{2}^{d(V) + \dim(V)} e^{\frac{i\pi}{4}\sigma(V)}. \quad (26)$$

The following theorem of Pendavingh¹⁰ provides an explicit form for the Tutte polynomial of a binary matroid at $(-i, i)$ in terms of the bicycle dimension and Brown's invariant.

Theorem 11 (Pendavingh¹⁰). Let V be a linear subspace of \mathbb{F}_2^S and let $M(V)$ be the corresponding binary matroid with ground set S . If $|\text{supp}(x)| \equiv 0 \pmod{4}$ for all $x \in V \cap V^\perp$, then

$$T(M(V); -i, i) = \sqrt{2}^{d(V)} e^{\frac{i\pi}{4}(|S| - 3r(M) - \sigma(V))}. \quad (27)$$

Otherwise, $T(M(V); -i, i) = 0$. Further, $T(M(V); -i, i)$ can be evaluated in polynomial time.

As an immediate consequence of Theorem 11, we obtain an explicit form for Clifford circuit amplitudes in terms the bicycle dimension and Brown's invariant of the corresponding matroid. Furthermore, we obtain an efficient classical algorithm for computing the output probability amplitudes of Clifford circuits. For similar results of this flavour see refs. ^{22,23}.

Algorithm overview

We shall now use the correspondence between quantum computation and evaluations of the Tutte polynomial to establish a heuristic algorithm for computing quantum probability amplitudes. To compute a probability amplitude, it is sufficient to compute the Tutte polynomial of a graphic matroid at $x = -i \cot(\frac{\pi}{4k})$ and $y = e^{\frac{i\pi}{2k}}$ for an integer $k \geq 2$ ^{2,5,6}. Our algorithm will use the deletion–contraction property to recursively compute the Tutte polynomial. At each step in the recursion, the algorithm will compute certain structural properties of the graph in order to attempt to prune the computational tree. Our algorithm can be seen an adaption of the work of Haggard et al.⁷ to special points of the Tutte plane.

We note that our approach differs from tensor network-based methods, which involve the contraction of a graph with tensors assigned to its vertices. These methods have been used to simulate quantum computations while exploiting structural properties of the graph^{4,24–27}. However, our approach allows us to exploit an alternative class of structural properties. We proceed by describing the key aspects of our algorithm.

To improve the performance of our algorithm, we shall use the following deletion–contraction formula for multigraphs.

Proposition 12. Let $G = (V, E)$ be a multigraph and let e be a multiedge of G with multiplicity $|e|$. If e is a loop, then

$$T(G; x, y) = y^{|e|} T(G \setminus \{e\}; x, y). \quad (28)$$

If e is a coloop, then

$$T(G; x, y) = \left(x + \sum_{i=1}^{|e|-1} y^i \right) T(G/\{e\}; x, y). \quad (29)$$

Finally, if e is neither a loop nor a coloop, then

$$T(G; x, y) = T(G \setminus \{e\}; x, y) + \left(\sum_{i=0}^{|e|-1} y^i \right) T(G/\{e\}; x, y). \quad (30)$$

Proposition 12 can easily be proven from the deletion–contraction formula by induction; we omit the proof.

If U is the underlying graph of G , then the number of recursive calls may be bounded by $O(2^{|E(U)|})$. Alternatively, we may bound the number of recursive calls in terms of the number of vertices plus the number of edges $s = |V(U)| + |E(U)|$ in the underlying graph. The number of recursive calls R_s is then bounded by $R_s \leq R_{s-1} + R_{s-2}$, which is precisely the Fibonacci recurrence. Hence, the number of recursive calls is bounded by $O(\phi^{|V(U)| + |E(U)|})$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio²⁸. A careful analysis shows that the number of recursive steps is bounded by $O(\tau(U) \cdot |E(U)|)$, where $\tau(U)$ denotes the number of spanning trees in U ¹⁴.

At each step in the recursion, we use the multigraph deletion–contraction formula to remove all multiedges that correspond to either a loop or a coloop in the underlying graph. This process contributes a multiplicative factor to the proceeding evaluation. Note that when G is a graph whose underlying graph is a looped forest, then every edge in the underlying graph is either a loop or a coloop. Hence, we obtain the following formula for the Tutte polynomial of G .

Corollary 13. Let $G = (V, E)$ be a multigraph whose underlying graph U is a looped forest. Further, for each edge e in U , let $|e|$ denote its multiplicity in G . Then

$$T(G; x, y) = \prod_{\substack{e \in E(U) \\ \text{loop}}} y^{|e|} \prod_{\substack{e \in E(U) \\ \text{coloop}}} \left(x + \sum_{i=1}^{|e|-1} y^i \right). \quad (31)$$

Proof. The proof follows immediately from Proposition 12. \square

There are a number of techniques that we can use to simplify the graph at each step in the recursion. Firstly, we may remove any isolated vertices, since they do not contribute to the evaluation.

Secondly, when $x = -i \cot(\frac{\pi}{4k})$ and $y = e^{\frac{i\pi}{2k}}$ for an integer $k \in \mathbb{Z}^+$, we may replace each multiedge with a multiedge of equal multiplicity modulo $4k$. To account for this, we multiply the proceeding evaluation by a efficiently computable factor. Specifically, we invoke the following proposition.

Proposition 14. Fix $k \in \mathbb{Z}^+$. Let $G = (V, E)$ be a multigraph and let $G' = (V', E')$ be the graph formed from G by taking the multiplicity of each multiedge in G modulo $4k$. Then

$$T(G; x, y) = \left(i e^{\frac{i\pi}{4k}} \sin\left(\frac{\pi}{4k}\right) \right)^{\kappa(E) - \kappa(E')} T(G'; x, y), \quad (32)$$

where $x = -i \cot(\frac{\pi}{4k})$ and $y = e^{\frac{i\pi}{2k}}$.

We prove Proposition 14 in Supplementary Note 5.

The Tutte polynomial of a multigraph whose edge multiplicities are all integer multiples of an integer $k \in \mathbb{Z}^+$ may be evaluated at the point $x = -i \cot(\frac{\pi}{4k})$ and $y = e^{\frac{i\pi}{2k}}$ in polynomial time. This can be seen by the following proposition.

Proposition 15. Fix $k \in \mathbb{Z}^+$. Let $G = (V, E)$ be a multigraph whose edge multiplicities are all integer multiples of k . Further let $G' = (V', E')$ be the graph formed from G by taking the multiplicity of each multiedge in G divided by k . Then

$$T(G; x, y) = \left(\sqrt{2} e^{\frac{i\pi(1-k)}{4k}} \sin\left(\frac{\pi}{4k}\right) \right)^{-r(G)} T(G'; -i, i), \quad (33)$$

where $x = -i \cot\left(\frac{\pi}{4k}\right)$ and $y = e^{\frac{i\pi}{2k}}$.

We prove Proposition 15 in Supplementary Note 6 and note that this is a special consequence of the k -thickening approach of Jaeger et al.¹⁶. The Tutte polynomial may then be efficiently computed by Vertigan's algorithm¹⁷; we call such a multigraph a Vertigan graph. We may therefore prune the computational tree whenever the graph is a Vertigan graph with respect to k . Note that this corresponds to quantum circuits comprising gates from the Clifford group.

The Tutte polynomial factorises over components.

Proposition 16. Let $G = (V, E)$ be a graph with connected components $C = \{C_i\}_{i=1}^k$, then

$$T(G; x, y) = \prod_{i=1}^k T(C_i; x, y). \quad (34)$$

Proposition 16 can easily be proven from the deletion–contraction formula; we omit the proof. At each step in the deletion–contraction recursion, if the graph is disconnected, then we may use this property to prune the computational tree and hence improve performance.

An identical result holds for biconnected components.

Proposition 17 (Tutte²⁹). Let $G = (V, E)$ be a graph with biconnected components $B = \{B_i\}_{i=1}^k$, then

$$T(G; x, y) = \prod_{i=1}^k T(B_i; x, y). \quad (35)$$

Proposition 17 can easily be proven from the deletion–contraction formula. For a proof, we refer the reader to ref. ²⁹ [“Discussion”]. Similarly to the connected component case, we may use this property to prune the computational tree and improve performance. Note that the biconnected components of a graph may be listed in time linear in the number of edges via depth-first search³⁰.

The Tutte polynomial of a multigraph whose underlying graph is a cycle may be computed in polynomial time by invoking the following proposition.

Proposition 18 (Haggard et al.⁷). Let $G = (V, E)$ be a multigraph whose underlying graph U is an n -cycle with edges indexed by the positive integers. Further, for each edge e in U , let $|e|$ denote its multiplicity in G . Then

$$T(G; x, y) = \sum_{k=1}^{n-2} \left(\prod_{j=k+1}^n y_x(|e_j|) \prod_{j=1}^{k-1} y_1(|e_j|) \right) + y_x(|e_n| + |e_{n-1}|) \prod_{j=1}^{n-2} y_1(|e_j|), \quad (36)$$

where $y_x(j) := x + \sum_{i=1}^{j-1} y^i$.

Proposition 18 can easily be proven from the deletion–contraction formula. For a proof, we refer the reader to ref. ⁷ [Theorem 4]. We may use this proposition to prune the computational tree whenever the underlying graph is a cycle.

The Tutte polynomial of a planar graph along the hyperbola $(x-1)(y-1)=2$ may be evaluated in polynomial time via the Fisher–Kasteleyn–Temperley algorithm^{31–33}. We may therefore use this algorithm to prune the computational tree whenever the underlying graph is planar. Note that we may test whether a graph is planar in time linear in the number of vertices³⁴.

The performance of our algorithm depends on the heuristic used to select edges. We shall consider six edge-selection heuristics: vertex order, minimum degree, maximum degree, minimum degree sum, maximum degree sum, and non-Vertigan. These edge-selection heuristics were first studied by Pearce et al.⁸, with the exception of non-Vertigan, which is specific to our algorithm.

Vertex order: The vertices of the graph are assigned an ordering. A multiedge is selected from those incident to the lowest vertex in the ordering and whose other endpoint is also the lowest vertex of any incident in the ordering. For contractions, the vertex inherits the lowest of the positions in the ordering.

Minimum degree: A multiedge is selected from those incident to a vertex with minimal degree in the underlying graph.

Maximum degree: A multiedge is selected from those incident to a vertex with maximal degree in the underlying graph.

Minimum degree sum: A multiedge is selected from those whose sum of degrees of its endpoints is minimal in the underlying graph.

Maximum degree sum: A multiedge is selected from those whose sum of degrees of its endpoints is maximal in the underlying graph.

Non-Vertigan: A multiedge is selected from those whose multiplicity is not an integer multiple of k ; we call such a multiedge non-Vertigan. Using this edge-selection heuristic, the number of recursive calls may be bounded by $O(2^{v(G)})$, where $v(G)$ denotes the number of non-Vertigan multiedges in G . This is due to the fact that both the deletion and contraction operation reduce the number of non-Vertigan multiedges by at least one. We note that this is similar to the sum-over-Cliffords approach studied in refs. ^{35–37}.

There are many other methods that may improve the performance of our algorithm, which we do not study. We shall proceed by discussing some of these.

Isomorphism testing: During the computation the graphs encountered and the evaluation of their Tutte polynomial is stored. At each recursive step, we test whether the graph is isomorphic to one already encountered, and if so, we use the evaluation of the isomorphic graph instead. Haggard et al.⁷ showed that isomorphism testing can lead to an improvement in the performance of computing Tutte polynomials. Note that this may not be as effective when the input is a multigraph.

Almost planar: At each step in the recursion, we may test whether the graph is close to being planar, and if so, select edges in such a way that the deletion and contraction operations give rise to a planar graph. For example, if the graph is apex, that is, it can be made planar by the removal of a single vertex, then we may select a multiedge incident to such a vertex. Similarly, if the underlying graph is edge apex or contraction apex³⁸, then we may select a multiedge such that the deletion or the contraction operation gives rise to a planar graph.

k -connected components: Similarly to the connected and biconnected component case, we may compute the Tutte polynomial in terms of its k -connected components^{39,40}.

Experimental results

In this section, we present some experimental results comparing the performance of the edge-selection heuristics on two classes of random quantum circuits. Our experiments were performed using SageMath 9.0⁴¹. The source code and experimental data are available at ref. ⁴².

The first class we consider corresponds to random instances of IQP circuits induced by dense graphs. Specifically, an instance is

an IQP circuit induced by a complete graph with edge weights chosen uniformly at random from the set $\{\frac{m\pi}{8} | m \in \mathbb{Z}/8\mathbb{Z}\}$. This class of IQP circuits is precisely that was studied in ref. ⁴³, where it is conjectured that approximating the corresponding amplitudes up to a multiplicative error is #P-hard on average.

The second class we consider corresponds to random instances of IQP circuits induced by sparse graphs. Specifically, an instance is an IQP circuit induced by a random graph where each of the possible edges is included independently with probability 1/2 and with edge weights chosen uniformly at random from the set $\{\frac{m\pi}{8} | m \in \mathbb{Z}/8\mathbb{Z}\}$.

We run our algorithm using each of the edge-selection heuristics to compute the principal probability amplitude of 64 random instances of both the dense and sparse class on 12 vertices. The performance of each edge-selection heuristic is measured by counting the number of leaves in the computational tree. Our experimental data are presented in Supplementary Note 7. We find that the non-Vertigan edge-selection heuristic performs particularly well for the dense class and the maximum degree sum edge-selection heuristic performs particularly well for the sparse class.

DISCUSSION

We established a classical heuristic algorithm for exactly computing quantum probability amplitudes. Our algorithm is based on mapping output probability amplitudes of quantum circuits to evaluations of the Tutte polynomial of graphic matroids. The algorithm evaluates the Tutte polynomial recursively using the deletion–contraction property while attempting to exploit structural properties of the matroid. We considered several edge-selection heuristics and presented experimental results comparing their performance on two classes of random quantum circuits. Further, we obtained an explicit form for Clifford circuit amplitudes in terms of matroid invariants and an alternative efficient classical algorithm for computing the output probability amplitudes of Clifford circuits.

DATA AVAILABILITY

Data are available at the University of Bristol Data Repository, data.bris, <https://doi.org/10.5523/bris.kbhgclva863q21tjkkpqr5uvq>.

CODE AVAILABILITY

Source code is available at the University of Bristol Data Repository, data.bris, <https://doi.org/10.5523/bris.kbhgclva863q21tjkkpqr5uvq>.

Received: 18 February 2021; Accepted: 1 September 2021;

Published online: 24 September 2021

REFERENCES

- Aharonov, D., Arad, I., Eban, E. & Landau, Z. Polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane. Preprint at <https://arxiv.org/abs/quant-ph/0702008> (2007).
- Shepherd, D. Binary matroids and quantum probability distributions. Preprint at <https://arxiv.org/abs/1005.1744> (2010).
- Fenner, S., Green, F., Homer, S. & Pruim, R. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proc. Math. Phys. Eng. Sci.* **455**, 3953–3966 (1999).
- Markov, I. L. & Shi, Y. Simulating quantum computation by contracting tensor networks. *SIAM J. Comput.* **38**, 963–981 (2008).
- Shepherd, D. & Bremner, M. J. Temporally unstructured quantum computation. *Proc. Math. Phys. Eng. Sci.* **465**, 1413–1439 (2009).
- Bremner, M. J., Jozsa, R. & Shepherd, D. J. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proc. Math. Phys. Eng. Sci.* 20100301, <https://doi.org/10.1098/rspa.2010.0301> (2010).

- Haggard, G., Pearce, D. J. & Royle, G. Computing Tutte polynomials. *ACM Trans. Math. Softw.* **37**, 24 (2010).
- Pearce, D.J., Haggard, G. & Royle, G. Edge-selection heuristics for computing Tutte polynomials. In *Proc. Fifteenth Australasian Symposium on Computing: The Australasian Theory*, Vol. 94, 153–162 (Australian Computer Society, Inc., 2009).
- Monagan, M. A new edge selection heuristic for computing the Tutte polynomial of an undirected graph. Preprint at <https://arxiv.org/abs/1209.5160> (2012).
- Pendavingh, R. On the evaluation at $(-1, i)$ of the Tutte polynomial of a binary matroid. *J. Algebraic Comb.* **39**, 141–152 (2014).
- Welsh, D. J. *Matroid Theory* (Academic Press, 1976).
- Oxley, J. G. *Matroid Theory*, Vol. 3 (Oxford University Press, 2006).
- Whitney, H. On the abstract properties of linear dependence. *Am. J. Math.* **57**, 509–533 (1935).
- Sekine, K., Imai, H. & Tani, S. Computing the Tutte polynomial of a graph of moderate size. In *Proc. International Symposium on Algorithms and Computation* 224–233 (Springer, 1995).
- Björklund, A., Husfeldt, T., Kaski, P. & Koivisto, M. Computing the Tutte polynomial in vertex-exponential time. In *Proc. 49th Annual IEEE Symposium on Foundations of Computer Science* 677–686 (IEEE, 2008).
- Jaeger, F., Vertigan, D. L. & Welsh, D. J. On the computational complexity of the Jones and Tutte polynomials. In *Proc. Mathematical Proceedings of the Cambridge Philosophical Society*, Vol. 108, 35–53 (Cambridge Univ. Press, 1990).
- Vertigan, D. Bicycle dimension and special points of the Tutte polynomial. *J. Comb. Theory. Ser. B* **74**, 378–396 (1998).
- Snook, M. Counting bases of representable matroids. *Electron. J. Comb.* **19**, 41 (2012).
- Welsh, D. J. *Complexity: Knots, Colourings and Counting (London Mathematical Society Lecture Note Series)*, Vol. 186, 372–390 (Cambridge University Press, 1993).
- Iblisdir, S., Cirio, M., Boada, O. & Brennen, G. Low depth quantum circuits for Ising models. *Ann. Phys.* **340**, 205–251 (2014).
- Fujii, K. & Morimae, T. Commuting quantum circuits and complexity of Ising partition functions. *New J. Phys.* **19**, 033003 (2017).
- Guan, C. & Regan, K. W. Stabilizer circuits, quadratic forms, and computing matrix rank. Preprint at <https://arxiv.org/abs/1904.00101> (2019).
- Gosset, D., Grier, D., Kerzner, A. & Schaeffer, L. Fast simulation of planar Clifford circuits. Preprint at <https://arxiv.org/abs/2009.03218> (2020).
- O’Gorman, B. Parameterization of tensor network contraction. In *Proc. 14th Conference on the Theory of Quantum Computation, Communication and Cryptography* (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019).
- Gray, J. & Kourtis, S. Hyper-optimized tensor network contraction. *Quantum* **5**, 410 (2021).
- Huang, C. et al. Classical simulation of quantum supremacy circuits. Preprint at <https://arxiv.org/abs/2005.06787> (2020).
- Pan, F. & Zhang, P. Simulating the Sycamore quantum supremacy circuits. Preprint at <https://arxiv.org/abs/2103.03074> (2021).
- Wilf, H. S. *Algorithms and Complexity* (AK Peters/CRC Press, 2002).
- Tutte, W. T. A contribution to the theory of chromatic polynomials. *Can. J. Math.* **6**, 80–91 (1954).
- Hopcroft, J. & Tarjan, R. Algorithm 447: efficient algorithms for graph manipulation. *Commun. ACM* **16**, 372–378 (1973).
- Temperley, H. N. & Fisher, M. E. Dimer problem in statistical mechanics—an exact result. *Philos. Mag.* **6**, 1061–1063 (1961).
- Kasteleyn, P. W. Dimer statistics and phase transitions. *J. Math. Phys.* **4**, 287–293 (1963).
- Kasteleyn, P. *Graph Theory and Theoretical Physics*, 43–110 (Academic Press, 1967).
- Hopcroft, J. & Tarjan, R. Efficient planarity testing. *J. ACM* **21**, 549–568 (1974).
- Bravyi, S., Smith, G. & Smolin, J. A. Trading classical and quantum computational resources. *Phys. Rev. X* **6**, 021043 (2016).
- Bravyi, S. & Gosset, D. Improved classical simulation of quantum circuits dominated by Clifford gates. *Phys. Rev. Lett.* **116**, 250501 (2016).
- Bravyi, S. et al. Simulation of quantum circuits by low-rank stabilizer decompositions. *Quantum* **3**, 181 (2019).
- Lipton, M. et al. Six variations on a theme: almost planar graphs. *Involve* **11**, 413–448 (2017).
- Andrzejak, A. Splitting formulas for Tutte polynomials. *J. Comb. Theory, Ser. B* **70**, 346–366 (1997).
- Bonin, J. & De Mier, A. Tutte polynomials of generalized parallel connections. *Adv. Appl. Math.* **32**, 31–43 (2004).
- Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)* (Sage Developers, 2020).
- Mann, R. L. Data from “simulating quantum computations with tutte polynomials”. <https://doi.org/10.5523/bris.kbhgclva863q21tjkkpqr5uvq> (2021).
- Bremner, M. J., Montanaro, A. & Shepherd, D. J. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett.* **117**, 080501 (2016).

ACKNOWLEDGEMENTS

The author thanks Michael Bremner, Adrian Chapman, Iain Moffatt, Ashley Montanaro, Rudi Pendavingh, and Dan Shepherd for helpful discussions. This research was supported by the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme (QuantAlgo project), EPSRC grants EP/L021005/1, EP/R043957/1, and EP/T001062/1, and the ARC Centre of Excellence for Quantum Computation and Communication Technology (CQC2T), project number CE170100012.

COMPETING INTERESTS

The author declares no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41534-021-00477-0>.

Correspondence and requests for materials should be addressed to Ryan L. Mann.

Reprints and permission information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021