The Complexity of Approximating complex-valued Ising and Tutte partition functions

Citation for published version:
Goldberg, LA & Guo, H 2017, 'The Complexity of Approximating complex-valued Ising and Tutte partition functions' Computational complexity, vol. 26, no. 4, pp. 765–833. DOI: 10.1007/s00037-017-0162-2

Digital Object Identifier (DOI):
10.1007/s00037-017-0162-2

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Computational complexity

THE COMPLEXITY OF APPROXIMATING COMPLEX-VALUED ISING AND TUTTE PARTITION FUNCTIONS

Leslie Ann Goldberg and Heng Guo

February 21, 2017

Abstract. We study the complexity of approximately evaluating the Ising and Tutte partition functions with complex parameters. Our results are partly motivated by the study of the quantum complexity classes **BQP** and **IQP**. Recent results show how to encode quantum computations as evaluations of classical partition functions. These results rely on interesting and deep results about quantum computation in order to obtain hardness results about the difficulty of (classically) evaluating the partition functions for certain fixed parameters.

The motivation for this paper is to study more comprehensively the complexity of (classically) approximating the Ising and Tutte partition functions with complex parameters. Partition functions are combinatorial in nature and quantifying their approximation complexity does not require a detailed understanding of quantum computation. Using combinatorial arguments, we give the first full classification of the complexity of multiplicatively approximating the norm and additively approximating the argument of the Ising partition function for complex edge interactions (as well as of approximating the partition function according to a natural complex metric). We also study the norm approximation problem in the presence of external fields, for which we give a complete dichotomy when the parameters are roots of unity. Previous results were known just for a few such points, and we strengthen these results from **BQP**-hardness to #**P**-hardness. Moreover, we show that computing the sign of the Tutte polynomial is #**P**-hard at certain points related to the simulation of **BQP**. Using our classifications, we then revisit the connections to quantum computation, drawing conclusions that are a little different from (and incomparable to) ones in the quantum literature, but along similar lines.

Keywords. Counting Complexity, Ising model, Tutte polynomial, Approximate Counting

Subject classification. 68Q17 Computational difficulty of problems

1. Introduction

We study the Ising and Tutte partition functions, which are well-known partition functions arising in combinatorics and statistical physics (see, for example, Sokal 2005). Early works which studied the complexity of (exactly) evaluating these partition functions Jaeger *et al.* (1990) considered both real and complex parameters. Applications in statistical mechanics actually require consideration of complex numbers because the possible points of physical phase transitions occur exactly at real limit points of *complex* zeroes of these partition functions (see Sokal's explanation in Section 5 "Complex Zeros of Z_G: Why should we care?" Sokal 2005). However, given the difficulty of completely resolving the complexity of the approximation problem, most works which comprehensively studied the complexity of *approximately* evaluating these partition functions Goldberg & Jerrum (2008, 2014); Jerrum & Sinclair (1993) restricted attention to real parameters. A notable counter-example is the paper of Bordewich *et al.* (2005) which studied normalised additive approximations for #**P** functions including these partition functions. Bordewich et al. were motivated by a result of Freedman *et al.* (2003) showing that an approximate evaluation of the Jones polynomial associated with a particular complex parameter (a 5th root of unity) can be used to simulate the quantum part of any algorithm in the quantum complexity class **BQP**, which is the class of decision problems solvable by a quantum computer in polynomial time with bounded error. The relevance of this result to the partition functions that we study follows from a result of Thistlethwaite (1987), showing that the Jones polynomial is essentially a specialisation of the Tutte partition function.

Recently, there have been several papers showing how to encode quantum computations as evaluations of partition functions. These results rely on interesting and deep results about quantum computation to obtain hardness results about the difficulty of (classically) evaluating Ising and Tutte partition functions. For example, Kuperberg (2015) used three results in quantum computation (a density theorem from Freedman *et al.* (2002), the Solovay-Kitaev theorem (see Nielsen & Chuang 2004), and Post**BQP**=**PP** by Aaronson 2005) to demonstrate the #**P**-hardness of a certain kind of approximation of the Jones polynomial. His theorem is repeated later as Theorem 5.1, where it is discussed in more detail. He also derived related results about multiplicative approximations of the Tutte polynomial for certain real parameters.

IQP stands for "Instantaneous Quantum Polynomial time". It is characterised by a class of quantum circuits introduced by Shepherd & Bremner (2009). Fujii & Morimae (2013) showed how to encode **IQP** circuits as instances of the Ising model. Thus, they were able to use a quantum complexity result of (Bremner *et al.* 2011, Corollary 3.3) (showing that weakly simulating **IQP** with multiplicative error implies that the polynomial hierarchy collapses to the third level) to obtain a result about the approximation of the Ising model — namely that an FPRAS for the Ising model with parameter $y = \exp(\mathrm{i}\pi/8)$ would similarly entail collapse of the polynomial hierarchy. (As they mention, a similar result applies for other parameters that are universal for **IQP**.) This result is further discussed in Section 4.1. Other examples include (De las Cuevas *et al.* 2011, Result 2), (Iblisdir *et al.* 2014, Theorem 6.1), and (Matsuo *et al.* 2014, Theorems 2 and 3) which give **BQP**-hardness of certain Ising model approximations, enabling the conclusion that certain efficient algorithms for approximating these partition function up to additive error are unlikely to exist. Iblisdir *et al.* (2014) point out that some instances that they prove hard *do* have multiplicative approximations, due to Jerrum & Sinclair (1993), emphasising the difference between additive and multiplicative approximation. (Matsuo *et al.* 2014, Theorem 4) also relate the simulation of **IQP** circuits to Ising model approximations with real parameters.

The motivation for our paper is to study more comprehensively the complexity of approximating the Ising partition function at complex parameters, and also to go the other way around, working from the combinatorial model to quantum computation. Partition functions are combinatorial in nature and classifying the difficulty of approximating these partition functions should not require a detailed understanding of quantum mechanics or quantum computation. Hence, we undertake a detailed classification of the complexity of the partition function problems, using combinatorial methods. We focus mainly on the Ising model since this model is particularly relevant in statistical physics (Section 3). This model is also connected to **IQP** (as explained in Section 4.1). We also consider the more general Tutte polynomial at any point (x, y) where $x = -t$ and $y = -t^{-1}$ for a root of unity t (this is connected to **BQP**, as will be explained in Section 5).

Our main result for the Ising model (Theorem 1.2) is a classification of the complexity of approximating the partition function with complex edge interactions. This result is illustrated in Section 1.3. As the figure shows, there are very few parameters (edge interactions) in the complex plane for which the approximation problem is tractable. For most edge interactions, it is extremely intractable (#**P**-hard to approximate the norm within any constant factor and to approximate the argument within $\pm\pi/3$). Theorem 1.3 extends these results to a more relaxed setting in which approximation algorithms are unconstrained (allowed to output any rational number) if the correct output is zero. We emphasise that the goal of our work is to classify the difficulty of the problem for all *fixed* parameters in the complex plane. The proofs of our theorems are elementary and combinatorial. The main idea (see Lemma 3.6) is an extension of a bisection technique of Goldberg & Jerrum (2014) showing how to use an approximation for the norm of a function to get very close to a zero of the function. Our result for the Tutte polynomial (Theorem 1.7) is also proved using bisection. It shows that, for *any* relevant parameters, it is #**P**-hard to determine whether the sign of the polynomial is non-negative or non-positive (with an arbitrary answer being allowed when it is zero).

Using our classifications, we then revisit the connections to quantum computation, drawing conclusions that are a little different from (and incomparable to) the ones in the papers mentioned earlier, but along similar lines, as we now explain. Theorem 1.4 shows that strong simulation of **IQP** within any constant factor is #**P**-hard, even for the restricted class of circuits considered by Bremner *et al.* (2011). Our result is incomparable to their hardness result (Bremner *et al.* 2011, Corollary 3.3). Both results show hardness of multiplicative approximation. However, their result is for weak simulation (sampling from the output distribution of the circuit) whereas ours is for strong simulation (estimating the probability of a given output). In general, hardness results about weak simulation are more desirable, however multiplicative approximation is less appropriate for weak simulation, where total variation distance is more important. Also, our results (unlike those of Bremner *et al.* 2011) are not sensitive to the behaviour of the algorithms when the correct value is zero. Moreover, our complexity assumption (that $\mathbf{FP} \neq \#\mathbf{P}$) is implied by and therefore milder than theirs (that the polynomial hierarchy does not collapse to the third level). These results are discussed further in Section 4.1.

It seems that a result similar to our **IQP** result could also be obtained via Boson sampling Aaronson & Arkhipov (2013). In particular, (Aaronson & Arkhipov 2013, Theorem 4.3) have used a bisection technique similar to the one of Goldberg & Jerrum (2014) to show that approximating the square of the permanent of a real-valued input matrix within a constant factor is #**P**-hard. Any such input (Aaronson & Arkhipov 2013, Lemma 4.4) can be turned into a unitary matrix which can be viewed as a "Boson Sampling" input. The output of the Boson sampling problem is essentially the square of the permanent of the matrix (so is hard to approximate). Furthermore, the Boson sampling problem can be simulated by **BQP** circuits and adaptive **IQP** circuits (in the strong sense). Thus, while it is interesting to see that our Ising-model results have **IQP** applications, the important point concerning our result is the comprehensive classification of the Ising complexity, rather than the particular quantum applications.

As we explain in Section 1.5.2, classical simulation of the complexity class **BQP** is related to (but not directly a consequence of) determining the sign of the Tutte polynomial at a certain point $(-t, -t^{-1})$. Theorem 1.7 shows that this problem is #**P**-hard (even when the algorithm is not required to handle the case in which the output is zero), answering a question raised by Bordewich *et al.* (2005). This is related to (but incomparable to) a result (Theorem 5.1) from Kuperberg (2015). These results are discussed further in Section 5.

Finally, we study Ising models with external fields. (De las Cuevas *et al.* 2011, Result 2) showed that with edge interaction i and external field $e^{\mathrm{i}\pi/4}$ an additive approximation of the partition function is **BQP**-hard. Motivated by such connections, we focus on the problem of (multiplicatively) approximating the norm of the partition function when both the interaction parameter and the external field are roots of unity. We extend our hardness results to show that, for most such parameters, including the one studied by De las Cuevas et al., the approximation problem is #**P**-hard (for an exact statement, see Theorem 1.9). For the remaining parameters, the partition function can be evaluated exactly in polynomial time, and thus we get a complete dichotomy (Theorem 1.9). This extension relies on some lower bounds from transcendental number theory, which allow us to convert additive distances into multiplicative ones. The lower bound results are given in Section 6.1 and our hardness results are in Section 6.2.

As we have already mentioned, there are many papers encoding quantum simulations as Ising models, including especially the result of Fujii & Morimae (2013). We could use this encoding (along with our Theorem 1.3) to derive our quantum application (Theorem 1.4). In order to make the paper self-contained, and to make it accessible to readers from outside the area of quantum computation we instead give our own, more combinatorial, presentation of how to encode **IQP** circuits as Ising instances. This is given in Section 4.1.

1.1. The Ising model. The main partition function that we study is the partition function of the Ising model. Let y (called the edge *interaction*) and λ (called the *external field*) be two parameters. The partition function is defined for a (multi)graph

$G = (V, E)$ as

$$Z_{\text{Ising}}(G; y, \lambda) = \sum_{\sigma: V \to \{0,1\}} y^{m(\sigma)} \lambda^{n_1(\sigma)}, \tag{1.1}$$

where $m(\sigma)$ is the number of monochromatic edges under σ (that is, the number of edges (u, v) with $\sigma(u) = \sigma(v)$) and $n_1(\sigma)$ is the number of vertices v with $\sigma(v) = 1$. We write $Z_{\text{Ising}}(G; y)$ to denote $Z_{\text{Ising}}(G; y, 1)$.

We will consider complex parameters y and λ from the set $\overline{\mathbb{Q}}$ of algebraic numbers. Thus, the real and imaginary parts of y and λ will be algebraic. We use $\arg(z)$ to denote the arg of a complex number z. For fixed y and λ, we study several computational problems. The first of them is approximating the norm of $Z_{\text{Ising}}(G; y, \lambda)$ within a factor $K > 1$.

Name Factor-K-Norm-Ising(y, λ).

Instance A (multi)graph G.

Output A rational number $\widehat{N}$ such that $\widehat{N}/K \leq |Z_{\text{Ising}}(G; y, \lambda)| \leq K\widehat{N}$.

We also consider the problem of approximating the argument of the partition function within an additive distance of $\rho \in (0, 2\pi)$. Here we have to treat the zero case exceptionally since the argument is undefined.

Name Distance-ρ-Arg-Ising(y, λ).

Instance A (multi)graph G.

Output If $Z_{\text{Ising}}(G; y, \lambda) = 0$, then 0. Otherwise, a rational number $\widehat{A}$ such that

$$|\widehat{A} - \arg(Z_{\text{Ising}}(G; y, \lambda))| \leq \rho.$$

We drop the argument λ when it is equal to 1, so Factor-K-Norm-Ising(y) denotes the problem Factor-K-Norm-Ising$(y, 1)$ and Distance-ρ-Arg-Ising(y) denotes Distance-ρ-Arg-Ising$(y, 1)$.

1.2. Approximating Complex Numbers. It makes sense that we approximate the norm of a complex number relatively, whereas we approximate the argument additively. This is natural because multiplying complex numbers multiplies norms and adds arguments, so it preserves the usual property that if you can approximate two numbers, you can approximate the product.

Other notions of approximation have been proposed. Most notably, Ziv (1982) has proposed that the distance between two complex numbers y and y' should be measured as

$$d(y', y) = \frac{|y' - y|}{\max(|y'|, |y|)},$$

where $d(0,0) = 0$. We also study the following approximation problem.

Name Complex-Apx-Ising(y, λ).

Instance A (multi)graph G and a positive integer R, in unary.

Output If $|Z_{\text{Ising}}(G; y, \lambda)| = 0$ then the algorithm should output 0. Otherwise, it should output a complex number y such that $d(y, Z_{\text{Ising}}(G; y, \lambda)) \leq \frac{1}{R}$.

As with the other problems, we use the notation Complex-Apx-Ising(y) for Complex-Apx-Ising$(y, 1)$. We have specified the error R as an input of the problem, rather than as a parameter in order to emphasise the suitability of Complex-Apx-Ising(y, λ) as an appropriate notion of approximation for the Ising partition function when y is complex. The number R is expressed in unary so a polynomial time algorithm for Complex-Apx-Ising(y, λ) would give a so-called "fully polynomial time approximation scheme" for the norm of the partition function. For partition functions, it is well-known that approximating the norm within a factor that is an inverse polynomial in a unary input R is equivalent in difficultly to approximating the norm with any specific factor $K > 1$. We will return to this point later in Lemma 3.2.

1.3. Main results for the Ising model. The following theorem gives our main complexity results about the Ising model.

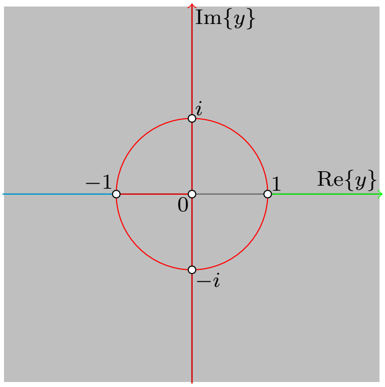

Figure 1.1: An illustration of Theorem 1.2 for Factor-K-Norm-Ising(y). The five white points correspond to the easy evaluations described in Item 1. The green line segment $(1, \infty)$ corresponds to a region where approximation is in **RP**— See Item 2. The blue line segment $(-\infty, -1)$ corresponds to a region where approximation is equivalent to approximately counting perfect matchings. See Item 4. The red points on the axes (the imaginary axis and the segment $(-1, 0)$) and on the unit circle correspond to regions where approximation is #**P**-hard. See Items 5, 6, and 7. Elsewhere the points are coloured grey, and approximation is known to be NP-hard (Items 3, 9 and 10) and sometimes to be #**P**-hard (Item 8, not pictured).

These results classify the problem of approximating the partition function over the entire complex plane. For every value of the parameter y, we either show that the problem is easy, in the sense that both the norm and the arg of the partition function can be well-approximated (and so can the conglomerate problem using the Ziv distance), or we show that approximating at least one these is hard (and so is the conglomerate problem using the Ziv distance). The results for approximation of the norm are illustrated in Section 1.3.

THEOREM 1.2. *Let $y = re^{i\theta}$ be an algebraic complex number with $r \geq 0$ and $\theta \in [0, 2\pi)$. Suppose $K > 1$.*

(i) If $y = 0$ or if $r = 1$ and $\theta \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ then FACTOR-K-NORM-ISING(y), DISTANCE-($\pi/3$)-ARG-ISING(y) *and* COMPLEX-APX-ISING(y) *are in* **FP**.

(ii) If $y > 1$ is a real number then FACTOR-K-NORM-ISING(y) *and* COMPLEX-APX-ISING(y) *are in* **RP** *and* DISTANCE-($\pi/3$)-ARG-ISING(y) *is in* **FP**.

(iii) If y is a real number in $(0, 1)$ then FACTOR-K-NORM-ISING(y) *and* COMPLEX-APX-ISING(y) *are* **NP***-hard and* DISTANCE-($\pi/3$)-ARG-ISING(y) *is in* **FP**.

(iv) If $y < -1$ is a real number then FACTOR-K-NORM-ISING(y) *is equivalent in complexity to the problem of approximately counting perfect matchings in graphs and* COMPLEX-APX-ISING(y) *is as hard. However,* DISTANCE-($\pi/3$)-ARG-ISING(y) *is in* **FP**.

(v) If y is a real number in $(-1, 0)$ then FACTOR-K-NORM-ISING(y), DISTANCE-($\pi/3$)-ARG-ISING(y) *and* COMPLEX-APX-ISING(y) *are* #**P***-hard.*

(vi) If $r = 1$ and $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ then FACTOR-K-NORM-ISING(y), DISTANCE-($\pi/3$)-ARG-ISING(y) *and* COMPLEX-APX-ISING(y) *are* #**P***-hard.*

(vii) If $\theta \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ and $r \notin \{-1,0,1\}$ then Factor-K-Norm-Ising(y), Distance-$(\pi/3)$-Arg-Ising(y) *and* Complex-Apx-Ising(y) *are* #**P**-*hard.*

(viii) If $r > 0$ and $\theta = \frac{a\pi}{2b}$, where a and b are two co-prime positive integers and a is odd then Factor-K-Norm-Ising(y), Distance-$(\pi/3)$-Arg-Ising(y) *and* Complex-Apx-Ising(y) *are* #**P**-*hard.*

(ix) If $r < 1$ and $y \neq 0$ then Factor-K-Norm-Ising(y) *and* Complex-Apx-Ising(y) *are* **NP**-*hard.*

(x) If $r > 1$ and $\theta \notin \{0,\pi\}$ then Factor-K-Norm-Ising(y) *and* Complex-Apx-Ising(y) *are* **NP**-*hard.*

1.4. Relaxed versions of the problems. A polynomial-time algorithm for any of the problems that we have defined is required to output 0 if it is given an input G such that $Z_{\text{Ising}}(G; y, \lambda) = 0$. Theorem 1.2 gives hardness results for these problems. The hardness is not due to special difficulties which arise when the value of the partition function is zero. In order to demonstrate this point, (and in order to make certain reductions easier later on), we also consider the following, more relaxed versions of the problems, where the output is unconstrained if the value of the partition function is zero. As before, the parameter K is greater than 1 and the parameter ρ is in $(0, 2\pi)$.

Name Factor-K-Nonzero-Norm-Ising(y, λ).

Instance A (multi)graph G.

Output If $|Z_{\text{Ising}}(G; y, \lambda)| = 0$ then the algorithm may output any rational number. Otherwise, it must output a rational number $\widehat{N}$ such that $\widehat{N}/K \leq |Z_{\text{Ising}}(G; y, \lambda)| \leq K\widehat{N}$.

Name Distance-ρ-Nonzero-Arg-Ising(y, λ).

Instance A (multi)graph G.

Output If $Z_{\text{Ising}}(G; y, \lambda) = 0$, then the algorithm may output any rational number. Otherwise, it must output a rational number $\widehat{A}$ such that $|\widehat{A} - \arg(Z_{\text{Ising}}(G; y, \lambda))| \leq \rho$.

Name COMPLEX-APX-NONZERO-ISING(y, λ).

Instance A (multi)graph G and a positive integer R, in unary.

Output If $|Z_{\text{Ising}}(G; y, \lambda)| = 0$ then the algorithm may output any complex number. Otherwise, it must output a complex number z such that $d(z, Z_{\text{Ising}}(G; y, \lambda)) \leq \frac{1}{R}$.

As in the un-relaxed versions of the problems, we drop the parameter "λ" from the problem name when it is 1. We give the following generalisation of Theorem 1.2.

THEOREM 1.3. *All of the results in Theorem 1.2 extend to the relaxed case. That is, the results are still true with* FACTOR-K-NORM-ISING(y), DISTANCE-$(\pi/3)$-ARG-ISING(y) *and* COMPLEX-APX-ISING(y) *replaced by* FACTOR-K-NONZERO-NORM-ISING(y), DISTANCE-$(\pi/3)$-NONZERO-ARG-ISING(y) *and* COMPLEX-APX--NONZERO-ISING(y), *respectively.*

1.5. Applications to quantum simulation.

1.5.1. IQP. **IQP** is characterised by a restricted class of quantum circuits Shepherd & Bremner (2009). We will give a formal definition in Section 4.1. There we will also discuss related work by Fujii & Morimae (2013), Bremner *et al.* (2011) and Jozsa & Van den Nest (2014). Here we give an informal description that enables us to state our theorem. Bremner et al. showed a hardness of a certain kind of "weak simulation" of a restricted class of circuits called $\mathbf{IQP}_{1,2}(\theta)$ circuits (see Definition 4.8). The qubits of the circuit travel along "lines" which go into (and out of) quantum gates. The output of such a circuit C is a random variable $\mathbf{Y}$ (over the qubits that get measured in the output). Given as input the string of all zero qubits and an output string $\mathbf{y} \in \{0,1\}^{|I|}$ on a set I — the set of qubits that are measured in the output, $\Pr_{C;I}$ denotes the probability that $\mathbf{Y} = \mathbf{y}$. Strong simulation is the problem of (approximately) computing this probability. We consider the following problem where $K > 1$ is an error parameter.

Name FACTOR-K-STRONG-SIM-IQP$_{1,2}(\theta)$.

Instance An $\mathbf{IQP}_{1,2}(\theta)$ circuit C, a subset $I \subseteq [n]$ of lines, and a string $\mathbf{y} \in \{0,1\}^{|I|}$.

Output A rational number p such that $p/K \leq \Pr_{C;I}(\mathbf{Y} = \mathbf{y}) \leq Kp$.

Our main result regarding this application is the following.

Theorem 1.4. *Suppose $K > 1$ and $\theta \in (0, 2\pi)$. If $e^{i\theta}$ is an algebraic complex number and $e^{i8\theta} \neq 1$ then* Factor-K-Strong-Sim-IQP$_{1,2}(\theta)$ *is* #**P***-hard.*

1.5.2. Connections between the Sign of the Tutte Polynomial and BQP. The partition function $Z_{\text{Ising}}(G; y, \lambda)$ is equivalent to a specialisation of the *Tutte polynomial*, which is a graph polynomial with two parameters, x and y, defined as follows,

$$T(G; x, y) = \sum_{A \subseteq E(G)} (x-1)^{\kappa(A)-\kappa(E(G))}(y-1)^{|A|-n+\kappa(A)}, \tag{1.5}$$

where $n = |V(G)|$ and $\kappa(A)$ is the number of connected components in the subgraph $(V(G), A)$. If the quantity $q = (x-1)(y-1)$ is a positive integer, then the Tutte polynomial with parameters x and y is closely related to the partition function of the Potts model, which includes the Ising model as the special case $q = 2$. In particular, when $q = 2$,

$$T(G; x, y) = (y-1)^{-n}(x-1)^{-\kappa(E(G))} Z_{\text{Ising}}(G; y). \tag{1.6}$$

Bordewich *et al.* (2005) raised the question "of determining whether the Tutte polynomial is greater than or equal to, or less than zero at a given point." As we will see, this question is relevant to the quantum complexity class **BQP**. We consider the following problems.

Name Sign-Real-Tutte(x, y)

Instance A (multi)graph G.

Output Determine whether the sign of the real part of $T(G; x, y)$ is positive, negative, or 0.

Name Sign-Real-Nonzero-Tutte(x, y)

Instance A (multi)graph G.

Output A correct statement of the form "$T(G; x, y) \geq 0$" or "$T(G; x, y) \leq 0$".

BQP is the class of decision problems solvable by a quantum computer in polynomial time with bounded error. The theorem (Bordewich *et al.* 2005, Theorem 6.1) shows that all of the problems in **BQP** can also be solved classically in polynomial time using an oracle that returns the sign of the real part of the Jones polynomial of a link, evaluated at the point $t = \exp(2\pi i/5)$. Thistlethwaite (1987) (see Jaeger *et al.* 1990, (6.1)), showed that this problem is, in turn, related to the problem of evaluating the Tutte polynomial $T(G; -t, -t^{-1})$, for a planar graph G. This inspired the question of Bordewich et al. about the complexity of determining the sign of the Tutte polynomial, particularly for the point $(x, y) = (-t, -t^{-1})$. We show that problem is hard for values of t including the relevant value $t = \exp(2\pi i/5)$. Note that our result does not have direct implications for the simulation of **BQP** because we do not deal with planarity (though it does answer the question of Bordewich et al.). We give the details in Section 5, where we also discuss a related result of Kuperberg (2015). Our theorem is as follows.

Theorem 1.7. *Consider the point* $(x, y) = (\exp(-a\pi\mathrm{i}/b), \exp(a\pi\mathrm{i}/b))$, *where a and b are positive integers satisfying* $0 < a/b < 2$ *and* $a \notin \{b/2, b, 3b/2\}$. *If a is odd and* $\cos(a\pi/b) < 11/27$ *then* Sign-Real-Nonzero-Tutte(x, y) *is* #**P**-*hard. Thus* Sign-Real-Tutte(x, y) *is also* #**P**-*hard.*

The condition $\cos(a\pi/b) < 11/27$ is roughly $0.36643 < a/b < 1.63357$. Since $-\exp(-2\pi\mathrm{i}/5) = \exp(\pi\mathrm{i})\exp(-2\pi\mathrm{i}/5) = \exp(3\pi\mathrm{i}/5)$, we get the relevant corollary by taking $a = 3$ and $b = 5$.

Corollary 1.8. *Let* $y = -\exp(-2\pi\mathrm{i}/5)$. *Then* Sign-Real-Nonzero-Tutte$(1/y, y)$ *is* #**P**-*hard.*

1.6. Results about Ising models with fields. Our results in Section 1.3 are about the complexity of evaluating the Ising partition function in the absence of an external field (when $\lambda = 1$). This is appropriate for the application to **IQP**. Ising models with external fields are important for their own sake. Moreover, (De las Cuevas *et al.* 2011, Result 2) showed that with edge interaction i and external field $e^{\mathrm{i}\pi/4}$ an additive approximation of the partition function is **BQP**-hard. Motivated by such quantum connections, we give the following extension.

THEOREM 1.9. *Let $K > 1$. Let y and z be two roots of unity. Then the following holds:*

(i) If $y = \pm\mathrm{i}$ and $z \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$, or $y = \pm 1$, then $Z_{Ising}(-; y, z)$ can be computed exactly in polynomial time.

(ii) Otherwise FACTOR-K-NONZERO-NORM-ISING(y, z) *is* #**P**-*hard.*

2. Preliminaries

2.1. Facts about Approximating Complex Numbers. We will use the following technical lemma concerning Ziv's distance measure from Section 1.2.

LEMMA 2.1. *If z and z' are two non-zero complex numbers and if $d(z', z) \le \varepsilon$ then $|z'|/|z| \le 1/(1-\varepsilon)$ and $|\arg z - \arg z'| \le \sqrt{36\varepsilon/11}$.*

PROOF. Suppose $d(z', z) \le \varepsilon$ and $|z'| \ge |z|$.

First, by the triangle inequality, $|z| + |z' - z| \ge |z'|$ so

$$\frac{|z'|}{|z|} = 1 + \frac{|z'| - |z|}{|z|} \le 1 + \frac{|z' - z|}{|z|} = 1 + \frac{|z' - z|}{|z'|}\frac{|z'|}{|z|} \le 1 + \varepsilon\frac{|z'|}{|z|},$$

as required.

Second, $|z' - z| \le \varepsilon|z'|$ so $(|z' - z|)^2 \le \varepsilon^2|z'|^2$. Letting $z = r\exp(i\theta)$ and $z' = r'\exp(i\theta')$ we have

$$((r'\cos(\theta') - r\cos(\theta))^2 + ((r'\sin(\theta') - r\sin(\theta))^2 \le \varepsilon^2 r'^2.$$

The left-hand-side is equal to $r^2 + r'^2 - 2rr'\cos(\theta - \theta')$. But we already proved

$$1 \leq \frac{r'}{r} \leq \frac{1}{1-\varepsilon},$$

so

$$r'^2(1-\varepsilon)^2 + r'^2 - 2r'^2\cos(\theta - \theta') \leq \varepsilon^2 r'^2,$$

which implies, by re-arranging the above,

$$\cos(\theta - \theta') \geq 1 - \frac{3\varepsilon}{2} + \frac{\varepsilon^2}{2}.$$

But $\cos(x) = 1 - x^2/2! + x^4/4! - x^6/6! + \cdots$, so

$$\frac{(\theta-\theta')^2}{2!} - \frac{(\theta-\theta')^4}{4!} + \frac{(\theta-\theta')^6}{6!} - \cdots \leq \frac{3\varepsilon}{2} - \frac{\varepsilon^2}{2}.$$

Provided that ε is sufficiently small (so $\theta - \theta' \leq 1$) the left-hand-side is at least $\frac{(\theta-\theta')^2}{2!} - \frac{(\theta-\theta')^4}{4!}$ which is equal to $11(\theta-\theta')^2/24$, so $|\theta - \theta'| \leq \sqrt{36\varepsilon/11}$. □

LEMMA 2.2. *Suppose $K > 1$ and $0 < \rho < 2\pi$. Then the following polynomial-time Turing reductions exist.*

$$\textsc{Factor-}K\textsc{-Norm-Ising}(y,\lambda) \leq_T \textsc{Complex-Apx-Ising}(y,\lambda),$$
$$\textsc{Factor-}K\textsc{-Nonzero-Norm-Ising}(y,\lambda)$$
$$\leq_T \textsc{Complex-Apx-Nonzero-Ising}(y,\lambda),$$
$$\textsc{Distance-}\rho\textsc{-Arg-Ising}(y,\lambda) \leq_T \textsc{Complex-Apx-Ising}(y,\lambda),$$
$$\textsc{Distance-}\rho\textsc{-Nonzero-Arg-Ising}(y,\lambda)$$
$$\leq_T \textsc{Complex-Apx-Nonzero-Ising}(y,\lambda),$$

PROOF. Let R be any (sufficiently large) integer so that $1 - 1/R > 1/K$ and $\sqrt{36/11R} \leq \rho$.

Consider a multigraph G where $|Z_{\text{Ising}}(G; y, \lambda)| \neq 0$. Given input G and R, an oracle for COMPLEX-APX-ISING(y, λ) or COMPLEX-APX-NONZERO-ISING(y, λ) returns a complex number z such that

$$d(z, Z_{\text{Ising}}(G; y, \lambda)) \leq \tfrac{1}{R}.$$

On the other hand, if $|Z_{\text{Ising}}(G;y,\lambda)| = 0$, then the oracle for Complex-Apx-Ising(y,λ) returns the complex number $z = 0$ and the oracle for Complex-Apx-Nonzero-Ising(y,λ) returns any complex number z.

For the first two reductions, suppose first that $|Z_{\text{Ising}}(G;y,\lambda)| \neq 0$. Then by Lemma 2.1, $d(z, Z_{\text{Ising}}(G;y,\lambda)) \leq \frac{1}{R}$ implies

$$\frac{|z|}{K} \leq \left(1 - \frac{1}{R}\right)|z| \leq |Z_{\text{Ising}}(G;y,\lambda)| \leq \frac{|z|}{1-\frac{1}{R}} \leq K|z|,$$

so $|z|$ is a suitable output to Factor-K-Norm-Ising(y,λ) or Factor-K-Nonzero-Norm-Ising(y,λ) with input G. On the other hand, if $|Z_{\text{Ising}}(G;y,\lambda)| = 0$ then $|z|$ is still suitable in both cases.

For the last two reductions, suppose first that $|Z_{\text{Ising}}(G;y,\lambda)| \neq 0$. Then by Lemma 2.1, $d(z, Z_{\text{Ising}}(G;y,\lambda)) \leq \frac{1}{R}$ implies

$$|\arg z - \arg Z_{\text{Ising}}(G;y,\lambda)| \leq \sqrt{36\varepsilon/11} \leq \rho,$$

so $\arg z$ is a suitable output to Distance-ρ-Arg-Ising(y,λ) or Distance-ρ-Nonzero-Arg-Ising(y,λ) with input G. On the other hand, if $|Z_{\text{Ising}}(G;y,\lambda)| = 0$ and $z = 0$ then 0 is a suitable output in both cases. If $|Z_{\text{Ising}}(G;y,\lambda)| = 0$ and $z \neq 0$ then $\arg z$ is suitable (as an output for Distance-ρ-Nonzero-Arg-Ising(y,λ)).

□

2.2. The multivariate Tutte polynomial.

We will require the random cluster formulation of the multivariate Tutte polynomial. Given a (multi) graph G with edge weights $\boldsymbol{\gamma} : E(G) \to \overline{\mathbb{Q}}$ and $q \in \overline{\mathbb{Q}}$, this is defined as

$$Z_{\text{Tutte}}(G;q,\boldsymbol{\gamma}) := \sum_{A \subseteq E(G)} q^{\kappa(A)} \prod_{e \in A} \gamma_e, \tag{2.3}$$

where γ_e is a shorthand for $\boldsymbol{\gamma}(e)$ for an edge $e \in E(G)$.

Suppose x and y satisfy $q = (x-1)(y-1)$. For a graph $G = (V,E)$, let $\boldsymbol{\gamma} : E \to \overline{\mathbb{Q}}$ be the constant function which maps every edge to the value $y-1$. Then (see, for example Sokal 2005, (2.26))

$$T(G;x,y) = (y-1)^{-n}(x-1)^{-\kappa(E(G))} Z_{\text{Tutte}}(G;q,\boldsymbol{\gamma}). \tag{2.4}$$

Obviously from (1.6), this implies that if $q = 2$ then $Z_{\text{Ising}}(G; y) = Z_{\text{Tutte}}(G; q, \boldsymbol{\gamma})$.

To apply a technique from Goldberg & Jerrum (2014) we will require a multivariate version of the problem Factor-K-Nonzero-Norm-Ising(y, λ). We could do this for general q, but we will only use the following version, which is restricted to $q = 2$ and has two complex parameters, γ_1 and γ_2.

Name Factor-K-Nonzero-Norm-2Tutte(γ_1, γ_2).

Instance A (multi)graph $G = (V, E)$ and edge weights $\boldsymbol{\gamma} : E \to \{\gamma_1, \gamma_2\}$.

Output If $|Z_{\text{Tutte}}(G; 2, \boldsymbol{\gamma})| = 0$ then the algorithm may output any rational number. Otherwise, it should output a rational number $\widehat{N}$ such that $\widehat{N}/K \leq |Z_{\text{Tutte}}(G; 2, \boldsymbol{\gamma})| \leq K\widehat{N}$.

Suppose that s and t are two distinguished vertices of G. Let $Z_{st}(G; q, \boldsymbol{\gamma})$ be the contribution to $Z_{\text{Tutte}}(G; q, \boldsymbol{\gamma})$ from subgraphs A where s and t are in the same component of $(V(G), A)$, that is,

$$Z_{st}(G; q, \boldsymbol{\gamma}) := \sum_{\substack{A \subseteq E: \\ s \text{ and } t \text{ in same component}}} q^{\kappa(A)} \prod_{e \in A} \gamma_e.$$

Similarly let $Z_{s|t}$ denote the contribution to $Z_{\text{Tutte}}(G; q, \boldsymbol{\gamma})$ from configurations A in which s and t are in different components.

2.3. Implementing new edge weights, series compositions, and parallel compositions .

Our treatment of implementations, series compositions and parallel compositions is completely standard and is taken from (Goldberg & Jerrum 2012, Section 2.1). The reader who is familiar with this material can skip this section (which is included here for completeness).

Fix $W \subseteq \overline{\mathbb{Q}}$ and $q \in \overline{\mathbb{Q}}$. Let $w^* \in \overline{\mathbb{Q}}$ be a weight (which may not be in W) which we want to "implement". Suppose that there is a graph Υ, with distinguished vertices s and t and a weight function $\widehat{\gamma} : E(\Upsilon) \to W$ such that

$$w^* = qZ_{st}(\Upsilon; q, \widehat{\gamma})/Z_{s|t}(\Upsilon; q, \widehat{\gamma}). \tag{2.5}$$

In this case, we say that Υ and $\widehat{\boldsymbol{\gamma}}$ implement w^* (or even that W implements w^*).

The purpose of "implementing" edge weights is this. Let G be a graph with weight function $\boldsymbol{\gamma}$. Let f be some edge of G with weight $\gamma_f = w^*$. Suppose that W implements w^*. Let Υ be a graph with distinguished vertices s and t with a weight function $\widehat{\boldsymbol{\gamma}} : E(\Upsilon) \to W$ satisfying (2.5). Construct the weighted graph G' by replacing edge f with a copy of Υ (identify s with either endpoint of f (it doesn't matter which one) and identify t with the other endpoint of f and remove edge f). Let the weight function $\boldsymbol{\gamma}'$ of G' inherit weights from $\boldsymbol{\gamma}$ and $\widehat{\boldsymbol{\gamma}}$ (so $\gamma'_e = \hat{\gamma}_e$ if $e \in E(\Upsilon)$ and $\gamma'_e = \gamma_e$ otherwise). Then the definition of the multivariate Tutte polynomial gives

$$Z_{\mathrm{Tutte}}(G'; q, \boldsymbol{\gamma}') = \frac{Z_{s|t}(\Upsilon; q, \widehat{\boldsymbol{\gamma}})}{q^2} Z_{\mathrm{Tutte}}(G; q, \boldsymbol{\gamma}). \tag{2.6}$$

So, as long as $q \neq 0$ and $Z_{s|t}(\Upsilon; q, \widehat{\boldsymbol{\gamma}})$ is easy to evaluate, evaluating the multivariate Tutte polynomial of G' with weight function $\boldsymbol{\gamma}'$ is essentially the same as evaluating the multivariate Tutte polynomial of G with weight function $\boldsymbol{\gamma}$.

Since the norm of the product of two complex numbers is the product of the norms, this reduces computing (or relatively approximating) the norm with weight function $\boldsymbol{\gamma}$ to the problem of computing (or relatively approximating) the norm with weight function $\boldsymbol{\gamma}'$. Also, since the argument of the product of two complex numbers is the sum of the arguments of the numbers, this reduces computing (or additively approximating) the argument with weight function $\boldsymbol{\gamma}$ to the problem of computing (or additively approximating) the argument with weight function γ'.

Two especially useful implementations are series and parallel compositions. Parallel composition is the case in which Υ consists of two parallel edges e_1 and e_2 with endpoints s and t and $\hat{\gamma}_{e_1} = w_1$ and $\hat{\gamma}_{e_2} = w_2$. It is easily checked from Equation (2.5) that $w^* = (1 + w_1)(1 + w_2) - 1$. Also, the extra factor in Equation (2.6) cancels, so in this case $Z_{\mathrm{Tutte}}(G'; q, \boldsymbol{\gamma}') = Z_{\mathrm{Tutte}}(G; q, \boldsymbol{\gamma})$.

Series composition is the case in which Υ is a length-2 path from s to t consisting of edges e_1 and e_2 with $\hat{\gamma}_{e_1} = w_1$ and $\hat{\gamma}_{e_2} = w_2$. It is easily checked from Equation (2.5) that $w^* = w_1w_2/(q + w_1 + w_2)$. Also, the extra factor in Equation (2.6) is $q + w_1 + w_2$, so in this case $Z_{\mathrm{Tutte}}(G'; q, \boldsymbol{\gamma}') = (q + w_1 + w_2)Z_{\mathrm{Tutte}}(G; q, \boldsymbol{\gamma})$. It is helpful to note that w^* satisfies

$$\left(1 + \frac{q}{w^*}\right) = \left(1 + \frac{q}{w_1}\right)\left(1 + \frac{q}{w_2}\right).$$

We say that there is a "shift" from (q, α) to (q, α') if there is an implementation of α' consisting of some Υ and $\widehat{w} : E(\Upsilon) \to W$ where W is the singleton set $W = \{\alpha\}$. Taking $y = \alpha + 1$ and $y' = \alpha' + 1$ and defining x and x' by $q = (x - 1)(y - 1) = (x' - 1)(y' - 1)$ we equivalently refer to this as a shift from (x, y) to (x', y'). It is an easy, but important observation that shifts may be composed to obtain new shifts. So, if we have shifts from (x, y) to (x', y') and from (x', y') to (x'', y''), then we also have a shift from (x, y) to (x'', y'').

The k-thickening of Jaeger *et al.* (1990) is the parallel composition of k edges of weight α. It implements $\alpha' = (1 + \alpha)^k - 1$ and is a shift from (x, y) to (x', y') where $y' = y^k$ (and x' is given by $(x' - 1)(y' - 1) = q$). Similarly, the k-stretch is the series composition of k edges of weight α. It implements an α' satisfying

$$1 + \frac{q}{\alpha'} = \left(1 + \frac{q}{\alpha}\right)^k,$$

It is a shift from (x, y) to (x', y') where $x' = x^k$. (In the classical bivariate (x, y) parameterisation, there is effectively one edge weight, so the stretching or thickening is applied uniformly to every edge of the graph.)

Thus, we have the following observation.

OBSERVATION 2.7. *The k-thickening operation gives the following polynomial-time reductions.*

- $\textsc{Factor-}K\textsc{-Norm-Ising}(y^k) \le \textsc{Factor-}K\textsc{-Norm-Ising}(y)$,
- $\textsc{Distance-}\rho\textsc{-Arg-Ising}(y^k) \le \textsc{Distance-}\rho\textsc{-Arg-Ising}(y)$,
- $\textsc{Sign-Real-Tutte}(1 + (x-1)(y-1)/(y^k - 1), y^k) \le \textsc{Sign-Real-Tutte}(x, y)$, *where* $y^k \neq 1$, *and*

- Complex-Apx-Ising(y^k) $\leq$ Complex-Apx-Ising(y).

Similarly, k-stretching gives the following polynomial-time reductions for $y \neq 1$.

- Factor-K-Norm-Ising($1 + 2/((1 + 2/(y - 1))^k - 1)$) $\leq$ Factor-K-Norm-Ising(y),
- Distance-ρ-Arg-Ising($1+2/((1+2/(y-1))^k-1)$) $\leq$ Distance-ρ-Arg-Ising(y),
- Sign-Real-Tutte($x^k, 1+(x-1)(y-1)/(x^k-1)$) $\leq$ Sign-Real-Tutte(x, y), *where* $x^k \neq 1$, *and*
- Complex-Apx-Ising($1 + 2/((1 + 2/(y - 1))^k - 1)$) $\leq$ Complex-Apx-Ising(y).

Similar statements hold for the relaxed versions of the problems.

3. Hardness results for the Ising model

In this section we prove Theorems Theorem 1.2 and Theorem 1.3.

3.1. Real weights. First we gather some known results regarding approximating the partition function $Z_{\text{Ising}}(G; y)$ of the Ising model when y is an algebraic real number.

If $y \in \{-1, 0, 1\}$, then computing $Z_{\text{Ising}}(G; y)$ is trivial from the definition (1.1). A classical result by Jerrum and Sinclair Jerrum & Sinclair (1993) settles the complexity of approximating $Z_{\text{Ising}}(G; y)$ when $y > 0$. They show that there is a "fully polynomial randomised approximation scheme" (FPRAS) when $y > 1$ and that it is **NP**-hard to approximate the partition function when $0 < y < 1$. The negative case appears to be more complicated. Goldberg and Jerrum Goldberg & Jerrum (2008) showed that if $-1 < y < 0$, it is also **NP**-hard to approximate $Z_{\text{Ising}}(G; y)$, but if $y < -1$, the problem is equivalent to approximating the number of perfect matchings in a graph and it is not known whether there is an FPRAS. Technically, neither Jerrum and Sinclair nor Goldberg and Jerrum worked over the algebraic numbers. In order to avoid issues of real arithmetic, Jerrum and Sinclair used a computational model in which real arithmetic is performed with perfect accuracy, and Goldberg and Jerrum restricted attention to rationals. However, the operations in those papers are easily implemented over the algebraic real numbers. Using our notation, these results are summarised as follows.

Lemma 3.1 (Goldberg & Jerrum 2008; Jerrum & Sinclair 1993). *Suppose* $y \in \overline{\mathbb{Q}}$ *and* $K > 1$. *Then* Factor-K-Norm-Ising(y)

- *is in* **FP** *if* $y \in \{-1, 0, 1\}$*;*
- *is in* **RP** *if* $y > 1$*;*
- *is NP-hard if* $0 < y < 1$ *or* $-1 < y < 0$*; and*
- *is equivalent in difficulty to approximately counting perfect matchings if* $y < -1$*.*

Technically, the results in Goldberg & Jerrum (2008); Jerrum & Sinclair (1993) were not about the problem Factor-K-Norm-Ising(y) with fixed K. Instead, the accuracy parameter was viewed as part of the input as in the following problem.

Name FPRAS-Norm-Ising(y, λ).

Instance A (multi)graph G and a positive integer R, in unary.

Output A rational number $\widehat{N}$ such that

$$\left(1 - \tfrac{1}{R}\right) \widehat{N} \leq |Z_{\text{Ising}}(G; y, \lambda)| \leq \left(1 + \tfrac{1}{R}\right) \widehat{N}.$$

Nevertheless, the hardness results in Lemma 3.1 follow easily from those papers using the following standard powering lemma.

Lemma 3.2. *Let* y *and* λ *be algebraic numbers. For any* $K > 1$*, there are polynomial-time Turing reductions between* Factor-K-Norm-Ising(y, λ) *and* FPRAS-Norm-Ising(y, λ).

Proof. The reduction from Factor-K-Norm-Ising(y, λ) to FPRAS-Norm-Ising(y, λ) is straightforward: Given an input G to Factor-K-Norm-Ising(y, λ), choose R so that $K \geq R/(R -$

1) and run an algorithm for FPRAS-Norm-Ising(y,λ) with inputs G and R, returning the result.

The other direction is almost as easy. Given an input (G,R) to FPRAS-Norm-Ising(y,λ), choose an integer k sufficiently large (which does not depend on the size of G) so that $(1-1/R)^k \leq 1/K$ and $(1+1/R)^k \geq K$. Then form G_k by taking k disjoint copies of G. Run an algorithm for Factor-K-Norm-Ising(y,λ) with input G_k, obtaining a number $\widehat{N}$ such that $\widehat{N}/K \leq |Z_{\text{Ising}}(G_k;y,\lambda)| \leq K\widehat{N}$. Then note that $Z_{\text{Ising}}(G_k;y,\lambda) = Z_{\text{Ising}}(G;y,\lambda)^k$, so

$$\begin{aligned}\left(1-\tfrac{1}{R}\right)\widehat{N}^{1/k} \leq \widehat{N}^{1/k}/K^{1/k} \leq |Z_{\text{Ising}}(G;y,\lambda)| &\leq K^{1/k}\widehat{N}^{1/k}\\ &\leq \widehat{N}^{1/k}\left(1+\tfrac{1}{R}\right),\end{aligned}$$

so $\widehat{N}^{1/k}$ is a suitable output. □

Note that the NP-hardness result for $0<y<1$ in Lemma 3.1 is essentially best possible in the sense that the problem is not much harder than NP. As Goldberg & Jerrum (2008) observed, the problem can be solved in randomised polynomial time using an oracle for an NP predicate by applying the bisection technique of Valiant & Vazirani (1986). The situation is different for $y<0$. (Goldberg & Jerrum 2014, Theorem 1, Region G) showed that it is #**P**-hard to determine the sign of $Z_{\text{Ising}}(G;y)$ if $-1<y<0$. Again, they stated their theorem for the case in which y is rational, but the proof applies equally well when y is an algebraic real number. In terms of our notation, they proved the following lemma.

Lemma 3.3 (Goldberg & Jerrum 2014). *For any algebraic real number $y\in(-1,0)$,* Sign-Real-Tutte(x,y) *is #**P**-hard, where $x = 1+2/(y-1)$.*

If y is real then $Z_{\text{Ising}}(G;y)$ is real. Thus, either $Z_{\text{Ising}}(G;y)=0$, or $\arg(Z_{\text{Ising}}(G;y))\in\{0,\pi\}$. Hence, approximating the argument within ±$\pi/3$ enables one to determine the sign of the real part. Using the connection (1.6) between the Tutte polynomial and the partition function of the Ising model and Lemma 2.2 we immediately obtain the following corollary.

Corollary 3.4. *Suppose y is an algebraic real number in the range $y \in (-1, 0)$. Then the problem* Distance-$(\pi/3)$-Arg-Ising(y) *is* #**P**-*hard and so is* Complex-Apx-Ising(y).

In fact, we can extend Goldberg and Jerrum's #**P**-hardness interval-shrinking technique from Goldberg & Jerrum (2014) to also obtain #**P**-hardness for the relaxed version of the problems. We start with a general discussion of interval shrinking. Suppose that we have a linear function $f(\varepsilon) = -\varepsilon A + B$ for positive A and B and that we wish to find a value $\hat{\varepsilon}$ that is very close to the root $\varepsilon^* = B/A$. Suppose that we also have an interval $[\varepsilon', \varepsilon'']$ such that $f(\varepsilon') > 0$ and $f(\varepsilon'') < 0$. Suppose that $\varepsilon'' - \varepsilon' = \ell$ (so the interval has length ℓ). Roughly, Goldberg and Jerrum had at hand an oracle for computing the sign of $f(\varepsilon)$ (using an oracle for Sign-Real-Tutte(x, y)) and, using this, it is easy to bisect the interval, getting very close to ε^* by binary search.

Using an oracle for the relaxed problem Sign-Real-Nonzero-Tutte(x, y) we can compute the sign whenever it is positive or negative, but we receive an unreliable answer for the sign of $f(\varepsilon)$ if $f(\varepsilon) = 0$. Nevertheless, we observe that having a reliable answer in this case is not important for the progress of the binary search. If the binary search queries the value of $f(\varepsilon)$ and $f(\varepsilon) \neq 0$ then the reply from the oracle is correct. Otherwise, the bisection technique described above recurses into a sub-interval that contains a zero of the function, as required. Thus, we have the following lemma. (We omit the formal proof since the lemma follows immediately from the observation that we have just made.)

Lemma 3.5. *For any algebraic real number $y \in (-1, 0)$,* Sign-Real-Nonzero-Tutte(x, y) *is* #**P**-*hard, where $x = 1 + 2/(y - 1)$. Also, the problems* Distance-$(\pi/3)$-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* #**P**-*hard.*

We next show how to further extend the #**P**-hardness interval-shrinking technique to obtain #**P**-hardness for the problem Factor-K-Nonzero-Norm-Ising(y). This requires new ideas, so we will provide more details. Let us return to the discussion of interval shrinking. Let $\eta = 1/21$ (the exact value of η is not important, but we fix it for concreteness). Instead of having an oracle for the sign of $f(\varepsilon) = -\varepsilon A + B$, we only will be able to assume that we have an oracle that, on input ε, returns a value $\hat{f}(\varepsilon)$ satisfying

$$(1-\eta)|f(\varepsilon)| < \tfrac{21}{22}|f(\varepsilon)| \le \hat{f}(\varepsilon) \le \tfrac{22}{21}|f(\varepsilon)| = (1+\eta)|f(\varepsilon)|,$$

except that again the value $\hat{f}(\varepsilon)$ is completely unreliable if $f(\varepsilon) = 0$. Our strategy will be to divide the interval into 10 equal-length sub-intervals $[\varepsilon_i, \varepsilon_{i+1}]$ for $i \in \{0, \ldots, 9\}$ with $\varepsilon_0 = \varepsilon'$ and $\varepsilon_{10} = \varepsilon''$. (The number 10 is not chosen to be optimal — however, it is easy to see that it suffices. Changing the number of sub-intervals would influence the choice of η above.) We then let s_i be the sign (positive, negative, or zero) of $\hat{f}(\varepsilon_i) - \hat{f}(\varepsilon_{i+1})$, for each $i \in \{0, \ldots, 9\}$. The s_i values can be computed by the oracle. Now recall that ε^* is the root B/A of the function $f(\varepsilon) = -\varepsilon A + B$. Consider next what happens if $\varepsilon_i < \varepsilon_{i+1} < \varepsilon^*$ (so $f(\varepsilon_i) > f(\varepsilon_{i+1}) > 0$) . In this case,

$$\begin{aligned}\hat{f}(\varepsilon_i) - \hat{f}(\varepsilon_{i+1}) &\ge (1-\eta) f(\varepsilon_i) - (1+\eta) f(\varepsilon_{i+1}) \\ &= A(\varepsilon_{i+1} - \varepsilon_i - \eta(2\varepsilon^* - \varepsilon_i - \varepsilon_{i+1})).\end{aligned}$$

Now $\varepsilon_{i+1} - \varepsilon_i \ge \ell/10$. Also $\varepsilon^* - \varepsilon_i$ and $\varepsilon^* - \varepsilon_{i+1}$ are both at most ℓ. So since $\eta < 1/20$, s_i is positive. Similarly, if $\varepsilon^* < \varepsilon_i < \varepsilon_{i+1}$ (so $f(\varepsilon_{i+1}) < f(\varepsilon_i) < 0$) then

$$\begin{aligned}\hat{f}(\varepsilon_i) - \hat{f}(\varepsilon_{i+1}) &\ge (1-\eta)(-f(\varepsilon_i)) - (1+\eta)(-f(\varepsilon_{i+1})) \\ &= -A(\varepsilon_{i+1} - \varepsilon_i - \eta(2\varepsilon^* - \varepsilon_i - \varepsilon_{i+1})),\end{aligned}$$

so s_i is negative. If $\varepsilon_i \le \varepsilon^*$ and $\varepsilon_{i+1} \ge \varepsilon^*$ then we don't know what the value of s_i will be. However, this is true for at most two values of i. So either s_0, s_1, s_2 and s_3 are all positive (in which case $\varepsilon_2 < \varepsilon^*$ and we can recurse on the interval $[\varepsilon_2, \varepsilon_{10}]$) or s_6, s_7, s_8 and s_9 are all negative (in which case $\varepsilon_8 > \varepsilon^*$ and we can recurse on the interval $[\varepsilon_0, \varepsilon_8]$). Either way, the interval shrinks to 4/5 of its original length.

Applying this idea in the proof of (Goldberg & Jerrum 2014, Lemma 1) yields the following.

Lemma 3.6. *Suppose that γ_1 and γ_2 are algebraic reals with $\gamma_1 \in (-2,-1)$ and $\gamma_2 \notin [-2,0]$. Then* Factor-$(\frac{22}{21})$-Nonzero-Norm-2Tutte(γ_1, γ_2) *is #**P**-hard.*

Proof. Apart from the interval shrinking idea discussed above, the proof is similar in structure to the proof of (Goldberg & Jerrum 2014, Lemma 1). We defer some calculations (which are unchanged) to Goldberg & Jerrum (2014) but we provide the rest of the proof to show how to get the stronger result. We use the fact that the following problem is #**P**-complete. This was shown by Provan & Ball (1983).

Name #Minimum Cardinality (s,t)-Cut.

Instance A graph $G=(V,E)$ and distinguished vertices $s,t\in V$.

Output $|\{S\subseteq E : S \text{ is a minimum cardinality } (s,t)\text{-cut in } G\}|$.

We will give a Turing reduction from #Minimum Cardinality (s,t)-Cut to the problem Factor-$(\frac{22}{21})$-Nonzero-Norm-2Tutte(γ_1,γ_2).

Let G,s,t be an instance of #Minimum Cardinality (s,t)-Cut. Assume without loss of generality that G has no edge from s to t. Let $n=|V(G)|$ and $m=|E(G)|$. Assume without loss of generality that G is connected and that $m\geq n$ is sufficiently large. Let k be the size of a minimum cardinality (s,t)-cut in G and let C be the number of size-k (s,t)-cuts.

Let $q=2$ and $M^*=2^{4m}$. Let h be the smallest integer such that $(\gamma_2+1)^h-1>M^*$ and let $M=(\gamma_2+1)^h-1$. Note that we can implement M from γ_2 via an h-thickening, and h is at most a polynomial in m.

Let $\delta=4^m/M$. Let $\boldsymbol{M}$ be the constant weight function which gives every edge weight M. We will use the following facts:

$$qM^m(1-\delta)\leq Z_{st}(G;q,\boldsymbol{M})\leq qM^m(1+\delta) \tag{3.7}$$

and

$$CM^{m-k}q^2(1-\delta)\leq Z_{s|t}(G;q,\boldsymbol{M})\leq CM^{m-k}q^2(1+\delta). \tag{3.8}$$

Fact (3.7) follows from the fact that each of the (at most 2^m) terms in $Z_{st}(G;q,\boldsymbol{M})$, other than the term with all edges in A, has size at most $M^{m-1}q^n$ and $2^mM^{m-1}q^n\leq\delta M^mq$. Fact (3.8) follows from the fact that all terms in $Z_{s|t}(G;q,\boldsymbol{M})$ are complements of

(s,t)-cuts. If more than k edges are cut then the term is at most $M^{m-k-1}q^n$ and

$$2^m M^{m-k-1} q^n \leq \delta C M^{m-k} q^2.$$

For a parameter ε in the open interval $(0,1)$ which we will tune later, let $\gamma' = -1-\varepsilon \in (-2,-1)$. We will discuss the implementation of γ' later. Let G' be the graph formed from G by adding an edge from s to t. Let $\boldsymbol{\gamma}$ be the edge-weight function for G' that assigns weight M to every edge of G and assigns weight γ' to the new edge. Using the definition of the (random cluster) Tutte polynomial, Goldberg and Jerrum noted that

$$\begin{aligned} Z_{\mathrm{Tutte}}(G';2,\boldsymbol{\gamma}) &= Z_{st}(G;2,\boldsymbol{M})(1+\gamma') + Z_{s|t}(G;2,\boldsymbol{M})\left(1+\frac{\gamma'}{2}\right) \\ &= -\varepsilon Z_{st}(G;2,\boldsymbol{M}) + Z_{s|t}(G;2,\boldsymbol{M})\left(1-\frac{1+\varepsilon}{2}\right). \qquad (3.9) \end{aligned}$$

It is easily checked that $Z_{\mathrm{Tutte}}(G';2,\boldsymbol{\gamma})$ is positive if ε is sufficiently small ($\varepsilon = M^{-2m}$ will do) and it is negative at $\varepsilon = 1$. Thus, viewing $Z_{\mathrm{Tutte}}(G';2,\boldsymbol{\gamma})$ as a function of ε, we can perform interval shrinking (as discussed before the statement of the lemma) to find a value of ε for which $Z_{\mathrm{Tutte}}(G';2,\boldsymbol{\gamma})$ is very close to 0. The interval shrinking uses an oracle for Factor-($\frac{22}{21}$)-Nonzero-Norm-2Tutte(γ_1,γ_2).

If we find an ε where $Z_{\mathrm{Tutte}}(G';q,\boldsymbol{\gamma}) = 0$, then for this value of ε, we have $\varepsilon Z_{st}(G;q,\boldsymbol{M}) = Z_{s|t}(G;q,\boldsymbol{M})\left(1-\frac{1+\varepsilon}{2}\right)$. Thus, using ε, we can calculate the fraction $Z_{s|t}(G;q,\boldsymbol{M})/Z_{st}(G;q,\boldsymbol{M})$. Plugging this (known) value into (3.7) and (3.8), we obtain

$$\frac{Cq(1-\delta)}{M^k(1+\delta)} \leq \frac{Z_{s|t}(G;q,\boldsymbol{M})}{Z_{st}(G;q,\boldsymbol{M})} \leq \frac{Cq(1+\delta)}{M^k(1-\delta)}.$$

Now, we don't know k, but C is an integer between 1 and 2^m, whereas $M > 2^{4m}$, so there is only one value of k that gives a solution C in the right range. Using the value of k, we can calculate C exactly.

Technical issues arise both because we are somewhat constrained in what values ε we can implement and because we won't be able to discover the exact value of ε that we need (but we will be able to approximate it closely). These technical issues provide no more difficulty than they did in Goldberg & Jerrum (2014). Suppose first that we are able, for any given $\varepsilon \in (M^{-2m}, 1)$ to implement $\gamma' = -1-\varepsilon$. Then our basic strategy is to do the interval shrinking, repeatedly sub-dividing the current interval $\Theta(\log(M^{m^2}))$ times, so eventually we'll get an interval of width at most M^{-m^2} that contains an ε where $Z_{\mathrm{Tutte}}(G'; 2, \boldsymbol{\gamma}) = 0$. Goldberg & Jerrum (2014) have already shown that knowing such an interval enables the exact calculation of C (so having a small interval is OK — it is not necessary to know ε exactly).

The only issue, then, is implementing the weights $\gamma' = -1-\varepsilon$ during the interval shrinking. As in Goldberg & Jerrum (2014) we cannot expect to implement any particular desired γ' precisely. However, using stretching and thickening, we can implement a value that is within an additive error of $M^{-m^2}/20$ of any desired ε, and this suffices. The fact that we have algebraic, rather than rational, numbers is irrelevant since stretchings and thickenings can be computed on algebraic numbers. □

Using stretching and thickening, we get the following corollary.

Corollary 3.10. *Suppose $K > 1$ and that $y \in (-1, 0)$ is an algebraic real number. Then* Factor-K-Nonzero-Norm-Ising(y) *is* #**P**-*hard.*

Proof. We first show that Factor-(22/21)-Nonzero-Norm-Ising(y) is #**P**-hard. Consider the edge interaction $y \in (-1, 0)$. Using the correspondence from (1.6) and (2.4), this corresponds directly to the quantity $\gamma_1 \in (-2, -1)$ in Lemma 3.6. We now consider how to use y to implement the quantity γ_2. A 2-thickening from (x, y) gives an effective weight (x', y') with $y' = y^2 \in (0, 1)$ and $x' = 2/(y' - 1) + 1 < -1$. Then a 2-stretch from (x', y') gives an effective weight (x'', y'') with $x'' = (x')^2 > 1$ and $y'' = 2/(x'' - 1) + 1 > 1$, corresponding to $\gamma_2 > 0$, as required.

The reduction from Factor-(22/21)-Nonzero-Norm-Ising(y) to Factor-K-Nonzero-Norm-Ising(y) follows from Lemma 3.2. □

Using Lemma 2.2 and the trivial reduction from Factor-K-Nonzero-Norm-Ising(y) to Factor-K-Norm-Ising(y) and from Complex-Apx-Nonzero-Ising(y) to Complex-Apx-Ising(y) we get the following.

Corollary 3.11. *Let $y \in (-1,0)$ be an algebraic real number. Then for any $K > 1$,* Factor-K-Norm-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *and* Complex-Apx-Ising(y) *are* #**P**-*hard.*

3.2. Complex weights.

Lemma 3.12. *Let $\theta \in [0, 2\pi)$ and $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. There is a positive integer k and an integer l such that $k\theta + 2\pi l \in (\frac{\pi}{2}, \pi) \cup (\pi, \frac{3\pi}{2})$.*

Proof. Clearly if $\theta \in (\frac{\pi}{2}, \pi) \cup (\pi, \frac{3\pi}{2})$ then we are done by letting $k = 1$ and $l = 0$. Otherwise $\theta \in (0, \frac{\pi}{2}) \cup (\frac{3\pi}{2}, 2\pi)$. If θ is an irrational fraction of 2π then we can go through the whole unit circle by taking multiple of θ. So assume $\theta = \frac{2\pi a}{b}$ where a and b are co-prime and $b = 3$ or $b \geq 5$ as $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. Moreover $b = 3$ contradicts $\theta \in (0, \frac{\pi}{2}) \cup (\frac{3\pi}{2}, 2\pi)$. Hence $b \geq 5$ and there exists an integer $t \neq b/2$ such that $b < 4t < 3b$. As a and b are relatively prime, there exist integers l_1, l_2 such that $l_1 a + l_2 b = 1$ and $l_1 > 0$. It is easy to see that $tl_1\theta = \frac{2\pi t l_1 a}{b} = -2\pi t l_2 + \frac{2\pi t}{b}$. As $t/b \in (1/4, 1/2) \cup (1/2, 3/4)$ we have that $\frac{2\pi t}{b} \in (\frac{\pi}{2}, \pi) \cup (\pi, \frac{3\pi}{2})$. The lemma follows by taking $k = tl_1$ and $l = tl_2$. □

The following lemma enables us to determine the complexity of evaluating the Ising partition function when the complex edge interaction $y \in \overline{\mathbb{Q}}$ is on the unit circle.

Lemma 3.13. *Let $y = e^{i\theta} \in \mathbb{C}$ be an algebraic complex number such that $\theta \in [0, 2\pi)$ and $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. There exists an algebraic real number $y' \in (-1, 0)$ that can be implemented by a sequence of stretchings and thickenings from y.*

Proof. By Lemma 3.12, there is a positive integer k and an integer l such that $k\theta + 2\pi l \in (\frac{\pi}{2}, \pi) \cup (\pi, \frac{3\pi}{2})$. As a k-thickening realizes $y^k = e^{ik\theta}$, we may assume $\theta \in (\frac{\pi}{2}, \pi) \cup (\pi, \frac{3\pi}{2})$.

Since $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$, we have $\cos\theta \neq 1$ and $\sin\theta\cos\theta \neq 0$. The latter implies that $\sin\theta + \cos\theta \neq 1$. Let $x = \frac{y+1}{y-1}$. Note that $x = \frac{\sin\theta}{\cos\theta - 1}\mathrm{i}$. Moreover $\theta \in (\frac{\pi}{2}, \pi) \cup (\pi, \frac{3\pi}{2})$, implies that $\cos\theta < 0$ and hence $|x| < 1$. We do a 2-stretch and the effective weight is $y' = 1 - \frac{2}{|x|^2+1} \in (-1, 0)$. □

Combining Lemma 3.13 with Observation 2.7, Corollary 3.10, Lemma 3.5 and Corollary 3.11 we get the following corollary, which applies to the problems Factor-K-Nonzero-Norm-Ising(y), Distance-$(\pi/3)$-Nonzero-Arg-Ising(y) and Complex-Apx-Nonzero-Ising(y) and also to the unrelaxed versions Factor-K-Norm-Ising(y), Distance-$(\pi/3)$-Arg-Ising(y) and Complex-Apx-Ising(y).

Corollary 3.14. *Let $y = e^{\mathrm{i}\theta} \in \mathbb{C}$ be an algebraic complex number such that $\theta \in [0, 2\pi)$ and $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. Then for any $K > 1$,* Factor-K-Nonzero-Norm-Ising(y), Distance-$(\pi/3)$-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are #**P**-hard. Hence, so are the un-relaxed versions of all three problems.*

The hardness on the unit circle extends directly to the whole imaginary axis.

Lemma 3.15. *Suppose $y = r\mathrm{i}$ and $r \neq 0, \pm 1$ where r is algebraic. There exists an algebraic real number $y' \in (-1, 0)$ that can be implemented by a sequence of stretchings and thickenings from y.*

Proof. If $0 < |y| < 1$, then a 2-thickening yields effective weight $y^2 = -r^2 \in (-1, 0)$. Let $y' = -r^2$ and the claim holds.

Otherwise suppose $|y| > 1$. We know that a k-stretch yields the weight $z_k = 1+2/(x^k-1)$ where $x = 1+2/(y-1) = (y+1)/(y-1)$. Re-arranging, we find that $z_k = \frac{(y+1)^k+(y-1)^k}{(y+1)^k-(y-1)^k}$. We will now argue that z_k is purely imaginary. To see this, note that monomials in the numerator all have degrees of the same parity as k, whereas those in the denominator have degrees of the same parity as $k-1$. Therefore, it must be the case that the numerator is real and the denominator is purely imaginary, or vice versa. In either case, z_k is purely imaginary. Therefore, if we can find a positive integer k

such that $0 < |z_k| < 1$ then we have reduced our problem to the previous case.

Since y is purely imaginary, we have that $|y+1| = |y-1|$. Since $x = (y+1)/(y-1)$, this implies that $|x| = 1$. It is easy to see that $0 < |z_k| < 1$ if and only if $|x^k + 1| < |x^k - 1|$ and $x^k \neq -1$. This in turn is equivalent to $\arg\left(x^k\right) \in \left(\frac{\pi}{2}, \pi\right) \cup \left(\pi, \frac{3\pi}{2}\right)$. By Lemma 3.12, such a k always exists unless $\arg(x) = \frac{t\pi}{2}$ where $t = 0, 1, 2, 3$. In these cases $y = \pm 1, \pm \mathrm{i}$, which contradicts our assumption. □

Combining Lemma 3.15 with Observation 2.7, Corollary 3.10, Lemma 3.5 and Corollary 3.11, we get the following corollary.

Corollary 3.16. *Let $y = r\mathrm{i}$ where $r \neq 0, \pm 1$ and r is algebraic. Let $K > 1$. Then* Factor-K-Nonzero-Norm-Ising(y),

Distance-($\pi/3$)-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are #**P**-hard. Hence, so are the un-relaxed versions of all three problems.*

Finally, this hardness can be extended to some algebraic complex numbers off of the unit circle.

Lemma 3.17. *Let $y = re^{\mathrm{i}\theta}$ be an algebraic complex number such that $r > 0$ and $\theta = \frac{a\pi}{2b}$, where a and b are two co-prime positive integers and a is odd. There exists an algebraic real number $y' \in (-1, 0)$ that can be implemented by a sequence of stretchings and thickenings from y.*

Proof. If $r = 1$ then we are done by Lemma 3.13. Otherwise $r \neq 1$ and by a b-thickening it reduces to the case of Lemma 3.15. □

Corollary 3.18. *Let $y = re^{\mathrm{i}\theta}$ be an algebraic complex number such that $r > 0$ and $\theta = \frac{a\pi}{2b}$, where a and b are two co-prime positive integers and a is odd. Then for any $K > 1$,* Factor-K-Nonzero-Norm-Ising(y), Distance-($\pi/3$)-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are #**P**-hard. Hence, so are the un-relaxed versions of all three problems.*

To obtain obtain **NP**-hardness results for other values of y, we start with the well-known **NP**-hard problem Max-Cut.

Name MAX-CUT.

Instance A (multi)graph G and a positive integer b.

Output Is there a cut of size at least b.

LEMMA 3.19. *Suppose $K > 1$. Let y be an algebraic complex number such that $|y| < 1$ and $y \neq 0$. Then* FACTOR-K-NONZERO-NORM-ISING(y) *is* **NP**-*hard and so is* COMPLEX-APX-NONZERO-ISING(y).

PROOF. We will reduce MAX-CUT to FACTOR-K-NONZERO-NORM-ISING(y). Given a graph G and a constant b, we want to decide whether G has a cut of size at least b. We do a k-thickening on G, where k is the least positive integer such that $2^m|y|^k < 1/4$. Then the effective edge weight is $y_k = y^k$. Clearly $|y_k| = |y|^k < 1$.

Suppose the maximum cut of G has size c. Now rewrite (1.1) as

$$Z_{\text{Ising}}(G; y_k) = \sum_{i=0}^{c} C_i y_k^{m-i},$$

where m is the number of edges in G and C_i is the number of configurations under which there are exactly i bichromatic edges. Since the maximum cut of G has size c and G has m edges, $\sum_{i=0}^{m-c} C_i = 2^m$. Also, since $2^m|y_k| < 1$, the $i = c$ term dominates the sum, so $Z_{\text{Ising}}(G; y_k)$ is not equal to 0.

If $c \geq b$, then our choice of k together with the triangle inequality implies that

$$\begin{aligned} |Z_{\text{Ising}}(G; y_k)| &= |C_c y_k^{m-c} + \sum_{i=0}^{c-1} C_i y_k^{m-i}| \\ &> C_c|y_k|^{m-c} - 2^m|y_k|^{m-c+1} \\ &> |y_k|^{m-c}|1 - 2^m|y|^k| \;>\; \tfrac{3}{4}|y_k|^{m-b}. \end{aligned}$$

Otherwise we have $c \leq b - 1$ and

$$\begin{aligned} |Z_{\text{Ising}}(G; y_k)| &= |\sum_{i=0}^{c} C_i y_k^{m-i}| \;<\; \sum_{i=0}^{c} C_i |y_k|^{m-i} \\ &\leq 2^m|y_k|^{m-b+1} \;<\; \tfrac{1}{4}|y_k|^{m-b} \end{aligned}$$

again by the triangle inequality and $2^m|y_k| < 1/4$. Therefore we could solve MAX-CUT in polynomial time using an oracle for FACTOR-1.1-NONZERO-NORM-ISING(y_k). By Observation 2.7 it suffices to use an oracle for FACTOR-1.1-NONZERO-NORM-ISING(y). By Lemma 3.2, an oracle for FACTOR-K-NONZERO-NORM-ISING(y) will do. Finally, Lemma 2.2 gives the result for COMPLEX-APX-NONZERO-ISING(y). □

The other case, when the norm of y is larger than 1, can be shown to be NP-hard by reduction from the previous case, unless the edge weight is real.

LEMMA 3.20. *Suppose $K > 1$. Let y be an algebraic complex number such that $|y| > 1$ and $y \notin \mathbb{R}$. Then* FACTOR-K-NONZERO-NORM-ISING(y) *is NP-hard and so is* COMPLEX-APX-NONZERO-ISING(y).

PROOF. We will prove that there exists a positive integer k such that the effective weight y_k of a k-stretch satisfies $|y_k| < 1$. Then we are done by Lemma 3.19.

Recall that $y_k = \frac{x^k+1}{x^k-1}$ where $x = \frac{y+1}{y-1}$. Clearly $|y_k| < 1$ if and only if $|x^k + 1| < |x^k - 1|$. The latter is equivalent to $\arg(x^k) = k \arg(x) \in (\pi/2, 3\pi/2)$ (plus some integer multiple of 2π). Let $\theta = \arg(x) \in [0, 2\pi)$. The fact that $|y| > 1$ implies that $\theta \in [0, \pi/2) \cup (3\pi/2, 2\pi)$. If $\theta = 0$, then $y \in \mathbb{R}$, which is a contradiction. Therefore $\theta \in (0, \pi/2) \cup (3\pi/2, 2\pi)$. By Lemma 3.12, there is a positive integer k and and integer l such that $k\theta + 2\pi l \in (\pi/2, \pi) \cup (\pi, 3\pi/2) \subset (\pi/2, 3\pi/2)$. This is exactly what we need. Moreover, k does not depend on the input G. This finishes our proof. □

3.3. Proof of Theorems Theorem 1.2 and Theorem 1.3.

Theorems Theorem 1.2 and Theorem 1.3 follow from the following combined theorem. The hardness result in Item Theorem 1.2(iii) of Theorem 1.2 (and its counterpart in Theorem 1.3) follows from Item Theorem 3.21(ix) of the combined theorem.

THEOREM 3.21. *Let $y = re^{i\theta}$ be an algebraic complex number with $\theta \in [0, 2\pi)$. Suppose $K > 1$.*

(i) *If* $y = 0$ *or if* $r = 1$ *and* $\theta \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ *then* Factor-K-Norm-Ising(y), Distance-($\pi/3$)-Arg-Ising(y) *and* Complex-Apx-Ising(y) *are in* **FP**.

(ii) *If* $y > 1$ *is a real number then* Factor-K-Norm-Ising(y) *and* Complex-Apx-Ising(y) *are in* **RP** *and* Distance-($\pi/3$)-Arg-Ising(y) *is in* **FP**.

(iii) *If* y *is a real number in* $(0, 1)$ *then* Distance-($\pi/3$)-Arg-Ising(y) *is in* **FP**.

(iv) *If* $y < -1$ *is a real number then* Factor-K-Nonzero-Norm-Ising(y) *is equivalent in complexity to the problem of approximately counting perfect matchings in graphs and* Complex-Apx-Nonzero-Ising(y) *is as hard. However,* Distance-($\pi/3$)-Arg-Ising(y) *is in* **FP**.

(v) *If* y *is a real number in* $(-1, 0)$ *then* Factor-K-Nonzero-Norm-Ising(y), Distance-($\pi/3$)-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* #**P**-*hard.*

(vi) *If* $r = 1$ *and* $\theta \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ *then* Factor-K-Nonzero-Norm-Ising(y), Distance-($\pi/3$)-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* #**P**-*hard.*

(vii) *If* $\theta \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ *and* $r \notin \{-1, 0, 1\}$ *then* Factor-K-Nonzero-Norm-Ising(y), Distance-($\pi/3$)-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* #**P**-*hard.*

(viii) *If* $r > 0$ *and* $\theta = \frac{a\pi}{2b}$, *where* a *and* b *are two co-prime positive integers and* a *is odd then* Factor-K-Nonzero-Norm-Ising(y), Distance-($\pi/3$)-Nonzero-Arg-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* #**P**-*hard.*

(ix) *If* $r < 1$ *and* $y \neq 0$ *then* Factor-K-Nonzero-Norm-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* **NP**-*hard.*

(x) *If* $r > 1$ *and* $\theta \notin \{0, \pi\}$ *then* Factor-K-Nonzero-Norm-Ising(y) *and* Complex-Apx-Nonzero-Ising(y) *are* **NP**-*hard.*

Proof. Item (i) is from Jaeger *et al.* (1990). The randomised algorithm for Factor-K-Norm-Ising(y) referred to in Item (ii) is from Jerrum & Sinclair (1993). See also Lemma 3.1 and the surrounding text for a discussion of algebraic numbers and accuracy parameters. The same algorithm can be used for Complex-Apx-Ising(y) because $Z_{\text{Ising}}(G; y)$ is real and positive so an approximation $\widehat{N}$ satisfing

$$\left(1 - \tfrac{1}{R}\right) \widehat{N} \leq Z_{\text{Ising}}(G; y, \lambda) \leq \left(1 + \tfrac{1}{R}\right) \widehat{N}$$

also satisfies $d(\widehat{N}, Z_{\text{Ising}}(G; y, \lambda)) \leq \frac{1}{R}$. The deterministic algorithm referred to in Items (ii) and (iii) is trivial because the argument of a positive real number is 0. The approximation equivalence in Item (iv) is from Goldberg & Jerrum (2008), since one can decide in polynomial time the existence of perfect matchings to lift the non-zero restriction. The hardness for Complex-Apx-Nonzero-Ising(y) follows from Lemma 2.2. The deterministic sign algorithm in Item (iv) is from Goldberg & Jerrum (2014). Item (v) is from Lemma 3.5 and Corollary 3.10 and Lemma 2.2. Item (vi) is from Corollary 3.14. Item (vii) is from Corollary 3.16. Item (viii) is from Corollary 3.18. Item (ix) is from Lemma 3.19. Finally, item (x) is from Lemma 3.20. □

4. Quantum circuits and counting complexity

In this section we explain the connection between quantum computation and complex weighted Ising models. We begin with some basic notions about quantum circuits. We view qubits $|0\rangle$ and $|1\rangle$ as column vectors $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. Similarly $\langle 0|$ and $\langle 1|$ are row vectors $(1, 0)$ and $(0, 1)$. For $\mathbf{x} \in \{0, 1\}^n$, let $|\mathbf{x}\rangle$ denote the tensor product $\otimes_{j=1}^{n} |x_j\rangle$ and $\langle \mathbf{x}|$ is similar.

Suppose C is a quantum circuit on n qubits and consists of m quantum gates $U_1, \ldots, U_m$ sequentially. A quantum gate is a function taking k input and k output variables and returning a value in $\mathbb{C}$. Such a gate is called k-local and has a natural 2^k by 2^k square unitary matrix representation. In a circuit we also need to specify on which qubits the gate acts upon. To make the notation uniform we view unaffected qubits as simply copied and associate each quantum gate with the following 2^n by 2^n square unitary matrix. Let U be a quantum gate and $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$ two vectors specifying the input and output on all n qubits. Define the 2^n by 2^n matrix M_U corresponding to gate U as $M_{U;\mathbf{x},\mathbf{y}} = U(\mathbf{x}, \mathbf{y})$.

For example, let H be the Hadamard gate $\frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right]$ acting on the first qubit and suppose there are two qubits in total, illustrated as in Figure 4.1. Then the matrix M_H is $\frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right] \otimes \left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right] = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{smallmatrix}\right]$.

Using this notation, given an input $\mathbf{x} \in \{0,1\}^n$, the output of the quantum circuit C is a random variable $\mathbf{Y}$ subject to the distribution

$$\Pr_C(\mathbf{Y} = \mathbf{y}) = \left| \langle \mathbf{y} | \prod_{j=1}^{m} M_{U_{m+1-j}} | \mathbf{x} \rangle \right|^2, \tag{4.1}$$

where $\mathbf{y} \in \{0,1\}^n$. It is not necessary that we measure all qubits in the output. We may measure a subset I of all n qubits. Let $\mathbf{y}' \in \{0,1\}^s$ where $|I| = s$. Then the output is a random variable $\mathbf{Y}'$ subject to the distribution

$$\Pr_{C;I}(\mathbf{Y}' = \mathbf{y}') = \sum_{\mathbf{z} \in \{0,1\}^n \text{ such that } \mathbf{z}|_{\text{I}} = \mathbf{y}'} \Pr_C(\mathbf{Y} = \mathbf{z}). \tag{4.2}$$

Alternatively, we may treat such marginal probability in the counting perspective, as a partition function in the "sum of product" fashion. First let us consider composing two quantum gates, say U_1 and U_2. Let the input variables of U_1 be $x_1, \ldots, x_n$. Let $z_1, \ldots, z_n$ be the variables on the wires between U_1 and U_2. Finally, let $y_1, \ldots, y_n$ be the outputs of U_2. We use $\sigma(\mathbf{x})$ to denote an assignment of values in $\{0,1\}$ to the variables $x_1, \ldots, x_n$. We use $\sigma(\mathbf{y})$ and $\sigma(\mathbf{z})$ similarly. Then the composition U of U_1 followed by U_2 is given by

$$U(\mathbf{x}, \mathbf{y}) = \sum_{\sigma(\mathbf{z})} U_1(\mathbf{x}, \sigma(\mathbf{z})) U_2(\sigma(\mathbf{z}), \mathbf{y}). \tag{4.3}$$

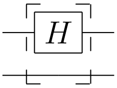

Figure 4.1: Gate H applying only on the first qubit.

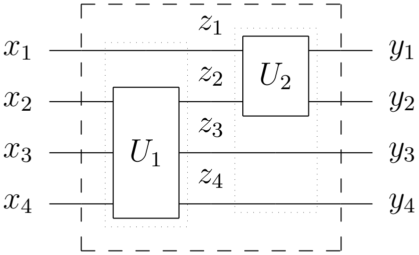

Figure 4.2: Two quantum gates U_1 and U_2 composed together.

Figure 4.2 illustrates the composition of gate U_1 acting upon qubits $2, 3, 4$ followed by U_2 acting upon $1, 2$. In the matrix notation, it is easy to see that $M_U = M_{U_1} M_{U_2}$.

We now associate an intermediate variable $z_{j,k}$ to each edge on qubit k between gate U_j and U_{j+1} for all $2 \leq j \leq m-1$ and $1 \leq k \leq n$. Denote by $\mathbf{z_j}$ the vector $\{z_{j,k} \mid 1 \leq k \leq n\}$ and $\mathbf{z} = \cup_{j=2}^{m-1} \mathbf{z_j}$. As the initial input and output of a quantum circuit are column vectors and row vectors respectively, they may be treated as function/gates with no output variables or no input variables. In particular, on the product input state $|\mathbf{x}\rangle$ input variables are set to $\{x_k\}$ where $\mathbf{x} \in \{0,1\}^n$. Using (4.3) recursively we can rewrite (4.1) as follows:

(4.4)

$$\Pr_C(\mathbf{Y} = \mathbf{y}) = \left| \sum_{\sigma:\mathbf{z} \to \{0,1\}} U_1(\mathbf{x}, \sigma(\mathbf{z_1})) U_m(\sigma(\mathbf{z_{m-1}}), \mathbf{y}) \prod_{j=2}^{m-1} U_j(\sigma(\mathbf{z_{j-1}}), \sigma(\mathbf{z_j})) \right|^2 .$$

To simulate classically a quantum circuit, one can either (approximately) compute the probability $\Pr_C(\mathbf{Y} = \mathbf{y})$ — this is called "strong simulation" — or one can sample from a distribution that is sufficiently close to the one given by (4.1) or (4.4). This is called "weak simulation"

4.1. IQP and the Ising partition function. **IQP**, which stands for "instantaneous quantum polynomial time", is characterised by a restricted class of quantum circuits introduced by Shepherd & Bremner (2009). Bremner *et al.* (2011) showed that if **IQP** can be simulated classically in the sense of "weak simulation" with multiplicative error, then the polynomial hierarchy collapses to the third level. Fujii & Morimae (2013) showed that the marginal probabilities of possible outcomes of **IQP** circuits correspond to partition functions of Ising models with complex edge weights.

The key property of **IQP** is that all gates are diagonal in the $|0\rangle \pm |1\rangle$ basis. Therefore all gates are commutable. In other words, there is no temporal structure and hence it is called "instantaneous". Let H be the Hadamard gate $\frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right]$. If a gate U is diagonal in the $|0\rangle \pm |1\rangle$ basis, there exists a diagonal matrix D such that $M_U = H^{\otimes n} D H^{\otimes n}$. Moreover H is its own inverse; That is, $HH = I_2$. Any two H's between each pair of gates cancel. This leads to an alternative view of **IQP** circuit in which each qubit line starts and ends with an H gate and all gates in between are diagonal.

Definition 4.5. *An* **IQP** *circuit on n qubit lines is a quantum circuit with the following structure: each qubit line starts and ends with an H gate, and all other gates are diagonal.*

We will focus particularly on $1,2$-local **IQP**, which means that every intermediate gate acts on 1 or 2 qubits. It was shown that a classical weak simulation of $1,2$-local **IQP** with multiplicative error implies the polynomial hierarchy collapse to the third level Bremner *et al.* (2011). Let $Z = \left[\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right]$. The hardness of simulation holds even if we restrict gates to the phase gate $e^{\mathrm{i}(\pi/8)Z} = \left[\begin{smallmatrix}e^{\mathrm{i}\pi/8} & 0\\ 0 & e^{-\mathrm{i}\pi/8}\end{smallmatrix}\right]$ and the controlled Z-gate $CZ = \left[\begin{smallmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{smallmatrix}\right]$ other than H gates on two ends of each line. We will show that this class of **IQP** circuits corresponds to Ising models with complex edge interactions and that therefore the strong simulation of these circuits is #**P**-hard, even allowing an error of any factor $K > 1$.

To show the relationship between these circuits and Ising partition functions, it is convenient to use another set of gates. Let

$P_\theta = e^{\mathrm{i}\theta Z} = \begin{bmatrix} e^{\mathrm{i}\theta} & 0 \\ 0 & e^{-\mathrm{i}\theta} \end{bmatrix}$ and $R_\theta = e^{\mathrm{i}\theta Z\otimes Z} = \begin{bmatrix} e^{\mathrm{i}\theta} & 0 & 0 & 0 \\ 0 & e^{-\mathrm{i}\theta} & 0 & 0 \\ 0 & 0 & e^{-\mathrm{i}\theta} & 0 \\ 0 & 0 & 0 & e^{\mathrm{i}\theta} \end{bmatrix}$. Note from (4.1) that we may multiply a gate by any norm 1 constant without affecting the outcome of the gate. By multiplying by $e^{-\mathrm{i}\pi/4}$, we may decompose CZ as:

(4.6)

$$e^{-\mathrm{i}\pi/4}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} e^{\mathrm{i}\pi/8} & 0 & 0 & 0 \\ 0 & e^{-\mathrm{i}\pi/8} & 0 & 0 \\ 0 & 0 & e^{-\mathrm{i}\pi/8} & 0 \\ 0 & 0 & 0 & e^{\mathrm{i}\pi/8} \end{bmatrix}^2 \begin{bmatrix} e^{\mathrm{i}\pi/8} & 0 & 0 & 0 \\ 0 & e^{-\mathrm{i}\pi/8} & 0 & 0 \\ 0 & 0 & e^{\mathrm{i}\pi/8} & 0 \\ 0 & 0 & 0 & e^{-\mathrm{i}\pi/8} \end{bmatrix}^{14}$$

$$\begin{bmatrix} e^{\mathrm{i}\pi/8} & 0 & 0 & 0 \\ 0 & e^{\mathrm{i}\pi/8} & 0 & 0 \\ 0 & 0 & e^{-\mathrm{i}\pi/8} & 0 \\ 0 & 0 & 0 & e^{-\mathrm{i}\pi/8} \end{bmatrix}^{14}$$

(4.7)
$$= \left(R_{\pi/8}\right)^2 \left(P_{\pi/8} \otimes I_2\right)^{14} \left(I_2 \otimes P_{\pi/8}\right)^{14}.$$

Hence we can replace every CZ gate on qubits j, k by 2 copies of $R_{\pi/8}$ on j, k, 14 copies of $P_{\pi/8}$ on qubit j, and 14 $P_{\pi/8}$ on qubit k. It is easy to see that $R_{\pi/8}$ can be replaced by CZ and $P_{\pi/8}$ as well. We may therefore assume every gate is either $P_{\pi/8}$ on 1 qubit or $R_{\pi/8}$ on 2 qubits without changing the computational power of the circuit. In general we give the following definition.

Definition 4.8. *An* $\mathbf{IQP}_{1,2}(\theta)$ *circuit on* n *qubit lines is a quantum circuit with the following structure: each qubit line starts and ends with an* H *gate, and every other gate is either* P_θ *on* 1 *qubit or* R_θ *on* 2 *qubits. We assume the input state is always* $|0^n\rangle$*.*

An example $\mathbf{IQP}_{1,2}(\theta)$ circuit is given in Figure 4.3.

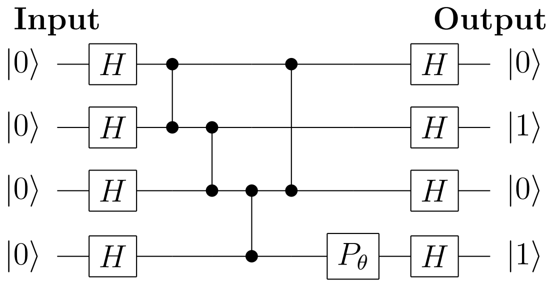

Figure 4.3: An $\mathbf{IQP}_{1,2}(\theta)$ circuit. We use two solid dots to denote R_θ gate as it is diagonal and symmetric.

The relationship between $\mathbf{IQP}_{1,2}(\theta)$ circuits and Ising models was first observed by Fujii & Morimae (2013). These connections will be shown next. For completeness we include our own proofs, which have a more combinatorial flavour than the original ones by Fujii & Morimae (2013). We introduce the following non-uniform Ising model which has been studied previously. See, for example Sokal (2005). Let $G = (V, E)$ be a (multi)graph. The edge interaction is specified by a function $\varphi : E \to \mathbb{C}$ and the external field is specified by a function $\tau : V \to \mathbb{C}$. The partition function is defined as

(4.9)
$$Z_{\text{Ising}}(G; \varphi, \tau) = \sum_{\sigma:V\to\{0,1\}} \prod_{e=(v_j,v_k)\in E} \varphi(e)^{\delta(\sigma(v_j),\sigma(v_k))} \prod_{v\in V} \tau(v)^{\sigma(v)},$$

where $\delta(x, y) = 1$ if $x = y$ and $\delta(x, y) = 0$ if $x \neq y$. We write $Z_{\text{Ising}}(G; y, \tau)$ when $\varphi(e) = y$ is a constant function and similarly $Z_{\text{Ising}}(G; \varphi, \lambda)$ when $\tau(v) = \lambda$. Notice that this notation is consistent with (1.1).

We will show that the following problem is related to Factor-K-Strong-Sim-IQP$_{1,2}(\theta)$ when $e^{\mathrm{i}\theta}$ is a root of unity.

Name Factor-K-Norm-IQP-Ising(θ).

Instance A (multi)graph G with an edge interaction function $\varphi(-)$ taking value $e^{\mathrm{i}\theta}$ or $e^{-\mathrm{i}\theta}$, and an external field function τ so that for each vertex v there are non-negative integers a_v and b_v so that $\tau(v) = (-1)^{a_v} \left(e^{\mathrm{i}\theta}\right)^{b_v}$ or $\tau(v) = (-1)^{a_v} \left(e^{-\mathrm{i}\theta}\right)^{b_v}$.

Output A rational number p such that $|Z_{\text{Ising}}(G; \varphi, \tau)|/K \leq p \leq K|Z_{\text{Ising}}(G; \varphi, \tau)|$.

We will first consider inputs to $\mathbf{IQP}_{1,2}(\theta)$ where $I = [n]$ so all qubits are measured. Given an $\mathbf{IQP}_{1,2}(\theta)$ circuit C on n qubits and a string $\mathbf{y} \in \{0, 1\}^n$, we can construct a non-uniform Ising instance G_C with edge interaction $e^{\mathrm{i}2\theta}$ and external field $\tau_{C;\mathbf{y}}$ such that

$$\Pr_C(\mathbf{Y} = \mathbf{y}) = 2^{-2n} \left|Z_{\text{Ising}}(G_C; e^{\mathrm{i}2\theta}, \tau_{C;\mathbf{y}})\right|^2. \tag{4.10}$$

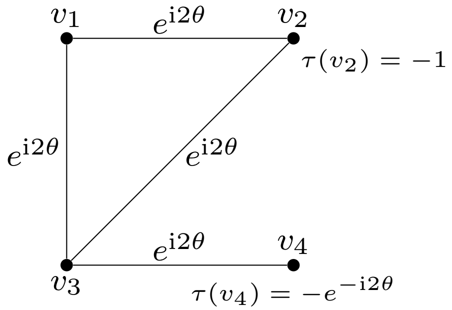

Figure 4.4: The equivalent Ising instance to the circuit in Figure 4.3.

The construction is as follows. The vertex set $\{v_j\}$ contains n vertices and each vertex corresponds to a qubit. For each gate R_θ on two qubits j, k, add an edge (j, k) in G_C. For qubit j, let p_j be the number of gates P_θ acting on qubit j in C. Let $\tau_{C;\mathbf{y}}(v_j) = e^{-\mathrm{i}(2p_j\theta)}(-1)^{y_j}$. An example of the construction is given in Figure 4.4.

Lemma 4.11. *Let C be an $\mathbf{IQP}_{1,2}(\theta)$ circuit on n qubits and $\mathbf{y} \in \{0,1\}^n$ be the output. Let G_C and $\tau_{C;\mathbf{y}}$ be constructed as above. Then (4.10) holds.*

Proof. Suppose C is composed sequentially by $U_1 = H^{\otimes n}$, U_2, ..., U_{m-1}, $U_m = H^{\otimes n}$, where U_j is either P_θ on 1 qubit or R_θ on 2 qubits for $2 \leq j \leq m-1$. Notice that $U_1(\mathbf{x}, \mathbf{x}') = U_m(\mathbf{x}, \mathbf{x}') =$

$2^{-n/2}\prod_{k=1}^{n}(-1)^{x_k x'_k}$. As the input $|\mathbf{x}\rangle = |0^n\rangle$, we can rewrite (4.4):

$$\begin{aligned}
\Pr_C(\mathbf{Y}=\mathbf{y}) &= \Bigg| \sum_{\sigma:\mathbf{z}\to\{0,1\}} U_1(\mathbf{0},\sigma(\mathbf{z_1}))U_m(\sigma(\mathbf{z_{m-1}}),\mathbf{y}) \\
&\qquad\qquad \prod_{j=2}^{m-1} U_j(\sigma(\mathbf{z_{j-1}}),\sigma(\mathbf{z_j}))\Bigg|^2 \\
&= \Bigg| 2^{-n} \sum_{\sigma:\mathbf{z}\to\{0,1\}} \prod_{k=1}^{n}(-1)^{0\cdot\sigma(z_{1,k})} \prod_{k=1}^{n}(-1)^{y_k\sigma(z_{m-1,k})} \\
&\qquad\qquad \prod_{j=2}^{m-1} U_j(\sigma(\mathbf{z_{j-1}}),\sigma(\mathbf{z_j}))\Bigg|^2 \\
&= 2^{-2n}\Bigg|\sum_{\sigma:\mathbf{z}\to\{0,1\}} \prod_{k=1}^{n}(-1)^{y_k\sigma(z_{m-1,k})} \prod_{j=2}^{m-1} U_j(\sigma(\mathbf{z_{j-1}}),\sigma(\mathbf{z_j}))\Bigg|^2 \qquad (4.12)
\end{aligned}$$

Let Q denote the quantity inside the norm, that is,

$$Q := \sum_{\sigma:\mathbf{z}\to\{0,1\}} \prod_{k=1}^{n}(-1)^{y_k\sigma(z_{m-1,k})} \prod_{j=2}^{m-1} U_j(\sigma(\mathbf{z_{j-1}}),\sigma(\mathbf{z_j})).$$

Since U_j's are diagonal for $2 \le j \le m-1$, any configuration σ with a non-zero contribution to Q must satisfy that for any k, $\sigma(z_{1,k}) = \sigma(z_{2,k}) = \cdots = \sigma(z_{m-1,k})$. Therefore we may replace $z_{j,k}$ by a single variable v_k for all $1 \le j \le m-1$ so that

$$Q = \sum_{\sigma:V\to\{0,1\}} \prod_{k=1}^{n}(-1)^{y_k\sigma(v_k)} \prod_{j=2}^{m-1} U_j(\sigma(V),\sigma(V)).$$

Moreover, if U_j is the gate P_θ on qubit k, then $U_j(\sigma(V),\sigma(V)) = e^{\mathrm{i}\theta}\left(e^{-\mathrm{i}2\theta}\right)^{\sigma(v_k)}$. If U_j is the gate R_θ on qubits k_1 and k_2, then $U_j(\sigma(V),\sigma(V)) = e^{-\mathrm{i}\theta}\left(e^{\mathrm{i}2\theta}\right)^{\delta(\sigma(v_{k_1}),\sigma(v_{k_2}))}$, where $\delta(x,y)=1$ if $x=y$ and $\delta(x,y)=0$ if $x\neq y$. Recall that p_k is the number of P_θ gates on qubit k and $\tau_{C;\mathbf{y}}(v_k) = e^{-\mathrm{i}(2p_k\theta)}(-1)^{y_k}$. Collecting all the contributions, we have

$$
\begin{aligned}
Q &= e^{\mathrm{i}(m_1-m_2)\theta} \sum_{\sigma:V\to\{0,1\}} \left(e^{\mathrm{i}2\theta}\right)^{m(\sigma)} \prod_{k=1}^{n} (-1)^{y_k\sigma(v_k)} \left(e^{-\mathrm{i}2\theta}\right)^{p_k\sigma(v_k)} \\
&= e^{\mathrm{i}(m_1-m_2)\theta} \sum_{\sigma:V\to\{0,1\}} \left(e^{\mathrm{i}2\theta}\right)^{m(\sigma)} \prod_{k=1}^{n} \tau_{C;\mathbf{y}}(v_k)^{\sigma(v_k)} \qquad (4.13)\\
&= e^{\mathrm{i}(m_1-m_2)\theta} Z_{\mathrm{Ising}}(G_C; e^{\mathrm{i}2\theta}, \tau_{C;\mathbf{y}}),
\end{aligned}
$$

where m_j is the number of j qubit(s) gates for $j \in \{1,2\}$, and, from (1.1), $m(\sigma)$ is the number of monochromatic edges under σ. We get (4.10) by substituting (4.13) in (4.12). □

Similar results hold when some qubits are not measured. To show it, we need the following fact. It can be viewed as an application of Parsevals's identity on the length-2^n vector $\{C_{\mathbf{z}}\}$ indexed by $\mathbf{z} \in \{0,1\}^n$ over an orthonormal basis $\{e_{\mathbf{z}}\}$ where basis element $e_{\mathbf{z}}$ has value $2^{-\frac{n}{2}}(-1)^{\mathbf{z}\cdot\mathbf{z}'}$ in position $\mathbf{z}'$. We include a proof for completeness.

Claim 4.14. *Let $\{C_{\mathbf{z}}\}$ be 2^n complex numbers where $\mathbf{z}$ runs over $\{0,1\}^n$. Then we have*

$$
\sum_{\mathbf{z}'\in\{0,1\}^n} \left| \sum_{\mathbf{z}\in\{0,1\}^n} C_{\mathbf{z}} (-1)^{\mathbf{z}\cdot\mathbf{z}'} \right|^2 = 2^n \sum_{\mathbf{z}\in\{0,1\}^n} \left|C_{\mathbf{z}}\right|^2 .
$$

Proof. Notice that for two complex numbers A and B,

$$
\begin{aligned}
|A+B|^2 + |A-B|^2 &= \left(|A|^2 + |B|^2 - 2|A||B|\cos\theta\right) \\
&\quad + \left(|A|^2 + |B|^2 + 2|A||B|\cos\theta\right) \\
&= 2\left(|A|^2 + |B|^2\right) \qquad (4.15)
\end{aligned}
$$

where θ is the angle from A to B. Hence we have

$$\begin{aligned}
&\sum_{\mathbf{z}'\in\{0,1\}^n}\left|\sum_{\mathbf{z}\in\{0,1\}^n} C_{\mathbf{z}}(-1)^{\mathbf{z}\cdot\mathbf{z}'}\right|^2\\
&=\sum_{\substack{\mathbf{z}'\in\{0,1\}^n\\ \text{s.t. } \mathrm{z}'_{\mathrm{n}}=0}}\left|\sum_{\mathbf{z}\in\{0,1\}^n} C_{\mathbf{z}}(-1)^{\mathbf{z}\cdot\mathbf{z}'}\right|^2+\sum_{\substack{\mathbf{z}'\in\{0,1\}^n\\ \text{s.t. } \mathrm{z}'_{\mathrm{n}}=1}}\left|\sum_{\mathbf{z}\in\{0,1\}^n} C_{\mathbf{z}}(-1)^{\mathbf{z}\cdot\mathbf{z}'}\right|^2\\
&=\sum_{\mathbf{y}'\in\{0,1\}^{n-1}}\left|\sum_{\mathbf{y}\in\{0,1\}^{n-1}} C_{\mathbf{y}0}(-1)^{\mathbf{y}\cdot\mathbf{y}'}+\sum_{\mathbf{y}\in\{0,1\}^{n-1}} C_{\mathbf{y}1}(-1)^{\mathbf{y}\cdot\mathbf{y}'}\right|^2+\\
&\sum_{\mathbf{y}'\in\{0,1\}^{n-1}}\left|\sum_{\mathbf{y}\in\{0,1\}^{n-1}} C_{\mathbf{y}0}(-1)^{\mathbf{y}\cdot\mathbf{y}'}-\sum_{\mathbf{y}\in\{0,1\}^{n-1}} C_{\mathbf{y}1}(-1)^{\mathbf{y}\cdot\mathbf{y}'}\right|^2\\
&=2\sum_{\mathbf{y}'\in\{0,1\}^{n-1}}\left(\left|\sum_{\mathbf{y}\in\{0,1\}^{n-1}} C_{\mathbf{y}0}(-1)^{\mathbf{y}\cdot\mathbf{y}'}\right|^2+\left|\sum_{\mathbf{y}\in\{0,1\}^{n-1}} C_{\mathbf{y}1}(-1)^{\mathbf{y}\cdot\mathbf{y}'}\right|^2\right),
\end{aligned}$$

where in the last line we apply (4.15). The claim holds by induction. □

We then have the following reduction.

Lemma 4.16. *Let $K > 1$ and $\theta \in [0, 2\pi)$. Then*

$$\text{Factor-}K\text{-Strong-Sim-IQP}_{1,2}(\theta) \le_T \text{Factor-}K^2\text{-Norm-IQP-Ising}(2\theta).$$

Proof. If all qubits in the input to Factor-K-Strong-Sim-IQP$_{1,2}(\theta)$ are measured, then the result follows from Lemma 4.11. Otherwise, without loss of generality we assume the first $n - s$ qubits are measured. Let C, $I = [n - s]$ and $\mathbf{y}' \in \{0, 1\}^{n-s}$ be the input to Factor-K-Strong-Sim-IQP$_{1,2}(\theta)$. We use (4.2), (4.12), and the first line of (4.13):

$$\begin{aligned}\Pr_{C;I}(\mathbf{Y}'=\mathbf{y}') &= \sum_{\mathbf{z}'\in\{0,1\}^s} \Pr_C(\mathbf{Y}=\mathbf{y}'\mathbf{z}')\\ &= 2^{-2n}\sum_{\mathbf{z}'\in\{0,1\}^s}\Bigg|\sum_{\sigma:V\to\{0,1\}}\left(e^{\mathrm{i}2\theta}\right)^{m(\sigma)}\\ &\qquad\left(\prod_{l=n-s+1}^{n}(-1)^{z'_{l-(n-s)}\sigma(v_l)}\left(e^{-\mathrm{i}2\theta}\right)^{p_l\sigma(v_l)}\right)\\ &\qquad\left(\prod_{k=1}^{n-s}(-1)^{y'_k\sigma(v_k)}\left(e^{-\mathrm{i}2\theta}\right)^{p_k\sigma(v_k)}\right)\Bigg|^2\\ &= 2^{-2n}\sum_{\mathbf{z}'\in\{0,1\}^s}\left|\sum_{\mathbf{z}\in\{0,1\}^s}Q_{\mathbf{z}}(-1)^{\mathbf{z}\cdot\mathbf{z}'}\right|^2, \qquad (4.17)\end{aligned}$$

where for $\mathbf{z}\in\{0,1\}^s$, $Q_{\mathbf{z}}$ is the contribution of assigning z_{l-n+s} to v_l without the possible -1 external field, that is,

$$Q_{\mathbf{z}} = \prod_{l=n-s+1}^{n}\left(e^{-\mathrm{i}2\theta}\right)^{z_{l-n+s}p_l}\sum_{\substack{\sigma:V\to\{0,1\}\text{ such that}\\ \text{for } n-s+1\le l\le n,\sigma(v_l)=z_{l-n+s}}}\left(e^{\mathrm{i}2\theta}\right)^{m(\sigma)}\prod_{k=1}^{n-s}(-1)^{y'_k\sigma(v_k)}\left(e^{-\mathrm{i}2\theta}\right)^{p_k\sigma(v_k)}.$$

Apply Claim Claim 4.14 on (4.17):

$$\Pr_{C;I}(\mathbf{Y}'=\mathbf{y}') = 2^{-2n+s}\sum_{\mathbf{z}\in\{0,1\}^s}|Q_{\mathbf{z}}|^2. \qquad (4.18)$$

Moreover we have

$$|Q_{\mathbf{z}}|^2 = \left|\sum_{\substack{\sigma:V\to\{0,1\}\text{ such that}\\ \text{for } n-s+1\le l\le n,\sigma(v_l)=z_{l-n+s}}}\left(e^{\mathrm{i}2\theta}\right)^{m(\sigma)}\prod_{k=1}^{n-s}(-1)^{y'_k\sigma(v_k)}\left(e^{-\mathrm{i}2\theta}\right)^{p_k\sigma(v_k)}\right|^2.$$

We construct the following instance of FACTOR-K^2-NORM-IQP-ISING(2θ). We first construct $G_C=(V,E)$ with edge interaction $e^{\mathrm{i}2\theta}$ as before. The vertex set $\{v_j\}$ contains one vertex

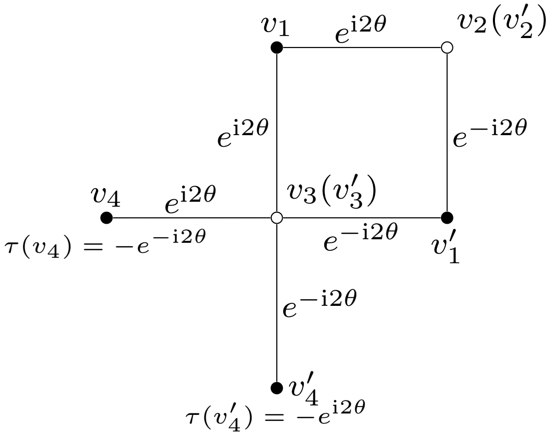

Figure 4.5: The equivalent Ising instance to the circuit in Figure 4.3, if qubits 2 and 3 are unmeasured. The notation $v_2(v_2')$ indicates that vertices v_2 and v_2' have been identified.

for each of the n qubits. For each gate R_θ on two qubits j, k we add edge (j, k) with edge interaction $e^{\mathrm{i}2\theta}$ to G_C. Now make a copy $G_C' = (V', E')$ such that the edge interaction is $\overline{e^{\mathrm{i}2\theta}} = e^{-\mathrm{i}2\theta}$. Let $\varphi_{C;I}$ be this edge interaction function. Then we identify vertices v_l with v_l' for all $n - s + 1 \le l \le n$. Let U be the set of these identified vertices and let $V_1 = V - U$ and $V_1' = V' - U$. The external field $\tau = \tau_{C;I,\mathbf{y}'}$ is defined as follows: for any $v \in U$, $\tau(v) = 1$; for any $v_j \in V_1$, $\tau(v_j) = e^{-\mathrm{i}(2p_j\theta)}(-1)^{y_j'}$; and for any $v_j' \in V_1'$, $\tau(v_j') = \overline{\tau(v_j)} = e^{\mathrm{i}(2p_j\theta)}(-1)^{y_j'}$. Informally, this instance was formed by putting G_C and its complement together and identifying vertices that correspond to unmeasured qubits. Note that if two vertices in U are connected by an edge, then they are actually connected by two edges, and the product of the two edge interactions is 1. We therefore remove all edges with both endpoints in U. Call the resulting graph H_C. One can verify that $(H_C, \varphi_{C;I}, \tau_{C;I,\mathbf{y}'})$ is a valid instance of FACTOR-K^2-NORM-IQP-ISING(2θ). An example of the construction is given in Figure 4.5.

Fix an assignment $\mathbf{z} \in \{0, 1\}^s$ on U. The contribution $Z_{\mathbf{z}}$ to $Z_{\text{Ising}}(H_C; \varphi_{C;I}, \tau_{C;I,\mathbf{y}'})$ can be counted in two independent parts,

V and V'. Hence we have

$$\begin{aligned}Z_{\mathbf{z}} &= \left(\sum_{\sigma_1 : V_1 \to \{0,1\}} \left(e^{\mathrm{i}2\theta}\right)^{m_*(\sigma_1,\mathbf{z})} \prod_{j=1}^{n-s} \tau(v_j)^{\sigma(v_j)} \right) \\ &\quad \cdot \left(\sum_{\sigma_1' : V_1' \to \{0,1\}} \left(e^{-\mathrm{i}2\theta}\right)^{m_*'(\sigma_1',\mathbf{z})} \prod_{j=1}^{n-s} \overline{\tau(v_j)}^{\sigma(v_j')} \right) \\ &= \left| \sum_{\sigma_1 : V_1 \to \{0,1\}} \left(e^{\mathrm{i}2\theta}\right)^{m_*(\sigma_1,\mathbf{z})} \prod_{j=1}^{n-s} \tau(v_j)^{\sigma(v_j)} \right|^2,\end{aligned}$$

where given the configurations σ_1 (or σ_1'), $m_*(\sigma_1, \mathbf{z})$ (or $m_*'(\sigma_1', \mathbf{z})$) is the number of monochromatic edges with at least one endpoint in V (or V'). Recall that $\tau(v_j) = e^{-\mathrm{i}(2p_j\theta)}(-1)^{y_j'}$. Comparing $Z_{\mathbf{z}}$ to $|Q_{\mathbf{z}}|^2$, the only difference is that in $|Q_{\mathbf{z}}|^2$, $e^{\mathrm{i}2\theta}$ is raised to the number of monochromatic edges in the whole V instead of V_1. However for any monochromatic edge in U, its contribution is independent from the configuration σ, and hence can be moved outside of the sum. All such terms are cancelled after taking the norm. This implies $Z_{\mathbf{z}} = |Q_{\mathbf{z}}|^2$. Therefore (4.18) can be rewritten as

$$\begin{aligned}\Pr_{C;I}(\mathbf{Y}' = \mathbf{y}') &= 2^{-2n+s} \sum_{\mathbf{z} \in \{0,1\}^s} Z_{\mathbf{z}} \\ &= 2^{-2n+s} Z_{\mathrm{Ising}}(H_C; \varphi_{C;I}, \tau_{C;I,\mathbf{y}'}) \\ &= 2^{-2n+s} |Z_{\mathrm{Ising}}(H_C; \varphi_{C;I}, \tau_{C;I,\mathbf{y}'})|. \end{aligned} \tag{4.19}$$

The lemma follows from the above equation. □

Remark 4.20. *In fact, the construction of H_C can be further simplified. If $v \in V$ and $v' \in V'$ connect to some $u \in U$, we can replace edges (u, v) and (u, v') by a new edge (v, v') with an Ising interaction $\frac{2}{e^{\mathrm{i}4\theta} + e^{-\mathrm{i}4\theta}}$. (In case $e^{\mathrm{i}4\theta} + e^{-\mathrm{i}4\theta} = 0$ this interaction is equality and we identify v with v'.) Therefore we can reduce an instance of* Factor-K-Strong-Sim-IQP$_{1,2}(\theta)$ *to an Ising model of size linear in $|I|$, the number of measured qubits. If $|I| = O(\log n)$, then the reduced Ising instance is tractable and so is the simulation. This matches the strong simulation result by Shepherd (see*

(Bremner et al. 2011, Theorem 3.4) , the remark following that theorem and also Shepherd 2010.)

The reduction also works in the other direction when $e^{\mathrm{i}\theta}$ is a root of unity.

THEOREM 4.21. *Let $e^{\mathrm{i}\theta}$ be a root of unity and let $K > 1$. Then*

$$\text{FACTOR-}K\text{-NORM-IQP-ISING}(2\theta) \equiv_{\mathrm{T}} \text{FACTOR-}K^{1/2}\text{-STRONG-SIM-IQP}_{1,2}(\theta).$$

PROOF. Lemma 4.16 implies a reduction from the right hand side to the left hand side. In the rest of the proof we show the other direction. As $e^{\mathrm{i}\theta}$ is a root of unity, there exists a positive integer t such that $e^{-\mathrm{i}2\theta} = e^{\mathrm{i}2t\theta}$. Given an instance (G, φ, τ) of FACTOR-K-NORM-IQP-ISING(2θ), we may replace each edge of interaction $e^{-\mathrm{i}2\theta}$ by t parallel edges of weight $e^{\mathrm{i}2\theta}$. Moreover, we may assume the external field is of the form $\tau(v_j) = (-1)^{a_j}\left(e^{-\mathrm{i}2\theta}\right)^{b_j}$ for the same reason.

We construct an $\mathbf{IQP}_{1,2}(\theta)$ circuit C on $n = |V|$ qubits. For each edge $(v_j, v_k) \in E$, we add a quantum gate R_θ on qubits j and k. For each $1 \le j \le n$, we add b_j many quantum gate P_θ on qubits j and let the output $y_j = 1$ on qubit j if a_j is odd. By Lemma 4.11 we see that $2^{2n}\Pr_C(\mathbf{Y} = \mathbf{y}) = \left|Z_{\text{Ising}}(G; e^{\mathrm{i}2\theta}, \tau)\right|^2$. □

Suppose the Ising instance in the proof of Theorem 4.21 has no external field and has a constant edge interaction $e^{\mathrm{i}2\theta}$. Then it is not hard to see that the above construction does not rely on $e^{\mathrm{i}\theta}$ being a root of unity and works for general θ. Hence we have the following lemma.

LEMMA 4.22. *Let $e^{\mathrm{i}\theta} \in \mathbb{C}$ and $K > 1$. Then*

$$\text{FACTOR-}K\text{-NORM-ISING}(e^{\mathrm{i}\theta}) \le_T \text{FACTOR-}K^{1/2}\text{-STRONG-SIM-IQP}_{1,2}(\theta/2).$$

We can now prove our main result about IQP.

THEOREM 1.4. *Suppose $K > 1$ and $\theta \in (0, 2\pi)$. If $e^{\mathrm{i}\theta}$ is an algebraic complex number and $e^{\mathrm{i}8\theta} \neq 1$ then* FACTOR-K-STRONG-SIM-IQP$_{1,2}(\theta)$ *is* $\#\mathbf{P}$*-hard.*

Proof. This follows from Lemma 4.22 and Corollary 3.14. □

We note that if $e^{\mathrm{i}8\theta} = 1$, then Factor-$K$-Strong-Sim-IQP$_{1,2}(\theta)$ has a polynomial time algorithm. By Theorem 4.21, Factor-K-Strong-Sim-IQP$_{1,2}(\theta)$ can be reduced to Factor-K^2-Norm-IQP-Ising(2θ). If $e^{\mathrm{i}8\theta} = 1$, then $e^{\mathrm{i}2\theta}$ is an integer power of i. Therefore both the edge weight and the vertex weight of Factor-K^2-Norm-IQP-Ising(2θ) are powers of i. The algorithm from Cai *et al.* (2014) (affine-type) can be used to solve Factor-K^2-Norm-IQP-Ising(2θ). See also case 1 of Theorem 1.9.

In a related result, (Bremner *et al.* 2011, Corollary 3.3) showed that weakly simulating **IQP** with multiplicative error implies that the polynomial hierarchy collapses to the third level. More precisely, their result is the following. Suppose C is an $\mathbf{IQP}_{1,2}(\pi/8)$ circuit on n qubits. If there exists a classical randomized polynomial time procedure to sample a binary string $\mathbf{Z}$ of length n, such that for every string $\mathbf{y} \in \{0,1\}^n$ and any constant $1 \le K < \sqrt{2}$,

$$\Pr_C(\mathbf{Y} = \mathbf{y})/K \le \Pr(\mathbf{Z} = \mathbf{y}) \le K \Pr_C(\mathbf{Y} = \mathbf{y}),$$

then the polynomial hierarchy collapses to the third level. The usual measure for determining the quality of a sampling procedure is total variation distance. The notion of total variation distances is weaker than "multiplicative error" so the result in Bremner *et al.* (2011) does not rule out weak simulation with small variation distance. To see this, note that, if the multiplicative error is K, then obviously the total variation distance is at most $K-1$. On the other hand, consider two distributions supported by two n-bit Boolean strings. A sample from the first distribution is obtained uniformly choosing each of the n bits. A sample from the second distribution is obtained by uniformly choosing each of the first $n-1$ bits. The last bit is 1 if all other bits are 0, and is chosen uniformly otherwise. The total variation distance is 2^{-n}, but the multiplicative error is infinity at the all 0 string. Note that the complexity implication "polynomial hierarchy collapses to the third level" is apparently weaker than the consequence of strong simulation from Theorem 1.4, which is $\mathbf{FP} = \#\mathbf{P}$.

Strong simulation is also studied with respect to other classes of quantum circuits, see for example Jozsa & Van den Nest (2014).

The allowable error is usually taken to be additive and exponentially small, instead of the constant factors that we have studied here. For example, Jozsa & Van den Nest (2014) requires that the output be computed with k bits of precision in an amount of time that is polynomial in both k and the size of the input. Additive error is quite different from multiplicative error. Also, the amount of accuracy is important. Lemma 3.2 shows that there is no difference between a constant factor and an FPRAS scenario, in which the error is allowed to be a factor of $1 \pm 1/R$ for a unary input R. On the other hand, achieving a multiplicative error of $1 \pm 1/\exp(R)$ is an entirely different matter.

5. BQP and the Tutte polynomial

Bordewich *et al.* (2005) raised the question "of determining whether the Tutte polynomial is greater than or equal to, or less than zero at a given point." Thus, they raised the question of determining the complexity of Sign-Real-Tutte(x, y). In fact, they were especially interested in the case $x = -t$, $y = -t^{-1}$ where $t = \exp(2\pi\mathrm{i}/5)$.

We next show that resolving this case is a simple corollary of our results. After that, we will discuss the motivation for considering this point (x, y) and its connection to the complexity class **BQP**. We will also briefly discuss a relevant general result of Kuperberg (2015), which resolves similar questions by using three results about quantum computation — the Solovay-Kitaev theorem, the FLW density theorem, and a result of Aaronson.

Motivated by connections to quantum computing, we consider the difficulty of the problem Sign-Real-Tutte(x, y) when $xy = 1$. In particular, we study the points

$$(x, y) = (\exp(-a\pi\mathrm{i}/b), \exp(a\pi\mathrm{i}/b)),$$

where a and b are positive integers. If $a \in \{0, b/2, b, 3b/2\}$ then the problem is trivial since (x, y) is one of the so-called "special points" ($(1, 1)$, $(-1, -1)$, $(-i, i)$ and $(i, -i)$) where evaluating the Tutte polynomial is in **FP** Jaeger *et al.* (1990). We can assume without loss of generality that $a < 2b$ since adding 2π to the argument of a complex number doesn't change anything. We can now prove the main result of this section.

Theorem 1.7. *Consider the point* $(x,y) = (\exp(-a\pi\mathrm{i}/b), \exp(a\pi\mathrm{i}/b))$, *where* a *and* b *are positive integers satisfying* $0 < a/b < 2$ *and* $a \notin \{b/2, b, 3b/2\}$. *If* a *is odd and* $\cos(a\pi/b) < 11/27$ *then* Sign-Real-Nonzero-Tutte(x,y) *is* #**P**-*hard. Thus* Sign-Real-Tutte(x,y) *is also* #**P**-*hard.*

Proof. We will use the fact that

$$\begin{aligned} q &= (x-1)(y-1) = 2 - x - y \\ &= 2 - \exp(-a\pi\mathrm{i}/b) - \exp(a\pi\mathrm{i}/b) = 2 - 2\cos(a\pi/b), \end{aligned}$$

which is real. Since $0 < a/b < 2$ and $a \notin \{b/2, b, 3b/2\}$, $q \in (0,4)$ and $q \neq 2$.

We implement (x', y') using a b-thickening from (x,y). Then, since a is an odd positive integer,

$$y' = y^b = \exp(a\pi\mathrm{i}) = -1.$$

So $x' = 1 + q/(y'-1) = 1 - q/2 = \cos(a\pi/b)$.

Now since $x' < 11/27$, (Goldberg & Jerrum 2014, Theorem 1, Region F) shows that computing the sign of $Z_{\mathrm{Tutte}}(-; q, y'-1)$ is #**P**-hard. As we showed in the argument that established Lemma 3.5 (see the paragraph before the statement of the lemma), the same is true if the oracle returns any answer when the value is 0.

Since x' and y' are not 1, (2.4) shows that it is also hard to compute the sign of $T(x',y')$. The result now follows from Observation 2.7. □

Since $-\exp(-2\pi\mathrm{i}/5) = \exp(\pi\mathrm{i})\exp(-2\pi\mathrm{i}/5) = \exp(3\pi\mathrm{i}/5)$, we can take $a = 3$ and $b = 5$ to obtain Corollary 1.8, which says that Sign-Real-Nonzero-Tutte$(1/y, y)$ is #**P**-hard for $y = -\exp(-2\pi\mathrm{i}/5)$.

Theorem 1.7 is very close to a special case of the following result of Kuperberg. A *link* is a collection of smooth simple closed curves embedded in 3-dimensional space. $V_L(t)$ denotes the Jones polynomial of a link L evaluated at point t. We do not need the detailed definition of the Jones polynomial in order to state Kuperberg's theorem.

Theorem 5.1. *(Kuperberg 2015, Theorem 1.2) Let $V(L,t)$ be the Jones polynomial of a link L described by a link diagram, and let t be a principal root of unit other than $\exp(2\pi\mathrm{i}/r)$ where $r \in \{1,2,3,4,5,6\}$. Let $0 < A < B$ be two positive real numbers and assume as a promise that either $|V(L,t)| < A$ or $|V(L,t)| > B$. Then it is $\#\mathbf{P}$-hard to decide which inequality holds. Moreover, it is still $\#\mathbf{P}$-hard when L is a knot.*

The connection is as follows. There is a result of Thistlethwaite (1987) (see Jaeger *et al.* 1990, (6.1)), showing that when L is an alternating link with associated planar graph $G(L)$, then $V_L(t) = f_L(t)T(G; -t, -t^{-1})$, where $f_L(t)$ is an easily-computable factor which is plus or minus a half integer power of t. Thus, the evaluation of Jones polynomial of an alternating link is an easily-computable multiple of an evaluation of the Tutte polynomial along the hyperbola $xy = 1$ (where, for some value t, $x = -t$ and $y = -t^{-1}$), as in Theorem 1.7. The importance of these evaluations is established in (Bordewich *et al.* 2005, Theorem 6.1) which shows that all of the problems in the quantum complexity class **BQP** (consisting of those decisions problems that can be solved by a quantum computer in polynomial time) can also be solved classically in polynomial time using an oracle that returns the sign of the real part of the Jones polynomial of a link, evaluated at the point $t = \exp(2\pi\mathrm{i}/5)$ (the point studied in Corollary 1.8).

Kuperberg's theorem (Theorem 5.1) is incomparable to Theorem 1.7. In some respects, Theorem 5.1 is more general — it does not have the restriction $\cos(a\pi/b) < 11/27$. Also, $G(L)$ is always planar, which is essential for the connection to **BQP**, and it applies to a wide range of A and B. On the other hand, the most relevant case $A = B = 0$ (the one that relates to the **BQP** result of Bordewich *et al.* 2005) is actually excluded from Theorem 5.1 since A and B must be different and positive. We are not sure whether Kuperberg's proof can be adapted to include this case, where the goal would be to determine whether $|V(L,t)| \geq 0$ or $|V(L,t)| \leq 0$. This is covered by Theorem 1.7.

In any case, it seems interesting to note that the proof of Theorem 1.7 is combinatorial (about Tutte polynomials only) whereas the proof of Theorem 5.1 is essentially about quantum computation. (Kuperberg describes it as "a mash-up of three standard theorems in quantum computation".)

We refer the reader to Aharonov & Arad (2011) for more recent results giving **BQP**-hardness of *multiplicative* approximations of the Jones polynomial of the plat closure of a braid at roots of unity. Also, we note that other works such as Geraci & Lidar (2010) have suggested the idea of using tractable planar evaluations of these polynomials to give efficient classical simulations for special cases of quantum circuits.

6. Ising with a field

In Section 6.2, we will extend our Ising hardness results from Theorems Theorem 1.2 and Theorem 1.3 to the situation in which we have an external field $\lambda \neq 1$. To obtain our hardness results, we need a lower bound on the relevant partition functions.

6.1. Lower bounds on partition functions. Suppose we have two edge weights y and y' that are close. It is easy to bound the distance between $Z_{\text{Ising}}(G; y)$ and $Z_{\text{Ising}}(G; y')$ additively, but not multiplicatively. To convert an absolute error into a relative error, one needs some lower bound on the partition function. However, when the edge interaction y is negative or complex, it is possible that the partition function vanishes. Assuming that it doesn't vanish, we would like to know how close to zero could it get. When y is rational, an exponential lower bound is easy to obtain by a simple granularity argument, but the argument is more difficult when y is not rational. In this section we give an exponential lower bound which is valid when y is an algebraic number. The techniques that we use are standard in transcendental number theory, see e.g. Bugeaud (2004).

We begin with some basic definitions from Bugeaud (2004). For a polynomial with complex coefficients

$$P(x) = \sum_{i=0}^{n} a_i x^i = a_n \prod_{i=1}^{n} (x - \alpha_i),$$

the (naive) *height* of $P(x)$ is defined as $\mathrm{H}(P) := \max_i\{|a_i|\}$. A more advanced tool, its *Mahler measure*, is defined as

$$\mathrm{M}(P) := |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}.$$

There is a standard inequality relating these two measures. It is proved for complex polynomials in (Bugeaud 2004, Lemma A.2). For completeness, we include the proof (following Bugeaud 2004) for the case in which $P(x)$ is a real polynomial, which is all that we require.

Lemma 6.1. *Let $P(x)$ be a non-zero real polynomial of degree n. Then $\mathrm{M}(P) \leq \sqrt{n+1}\,\mathrm{H}(P)$.*

Proof. First apply Jensen's formula on $P(x)$ and on the unit circle in the complex plane,

$$\mathrm{M}(P) = \exp\left\{\int_0^1 \log|P(e^{2\mathrm{i}\pi t})|\mathrm{d}t\right\}.$$

The convexity of exponential functions implies

$$\mathrm{M}(P) \leq \int_0^1 |P(e^{2\mathrm{i}\pi t})|\mathrm{d}t \leq \left(\int_0^1 |P(e^{2\mathrm{i}\pi t})|^2\mathrm{d}t\right)^{1/2},$$

where the second inequality follows by the Cauchy-Schwarz inequality writing $P(x)$ as $f(x)g(x)$ where $g(x) = 1$. The inner integral yields

$$\begin{aligned}
&\int_0^1 |P(e^{2\mathrm{i}\pi t})|^2 \mathrm{d}t \\
&= \int_0^1 \left(\left(\sum_{j=0}^n a_j \cos(j \cdot 2\pi t) \right)^2 + \left(\sum_{j=0}^n a_j \sin(j \cdot 2\pi t) \right)^2 \right) \mathrm{d}t \\
&= \sum_{i=0}^n a_i^2 + 2 \int_0^1 \sum_{0 \le j < k \le n} a_j a_k (\cos(j \cdot 2\pi t) \cos(k \cdot 2\pi t) \\
&\qquad\qquad + \sin(j \cdot 2\pi t) \sin(k \cdot 2\pi t)) \mathrm{d}t \\
&= \sum_{i=0}^n a_i^2 + 2 \sum_{0 \le j < k \le n} a_j a_k \int_0^1 \cos((j-k) \cdot 2\pi t) \mathrm{d}t = \sum_{i=0}^n a_i^2 .
\end{aligned}$$

The claim holds as $\mathrm{M}(P) \le \left(\sum_{i=0}^n a_i^2\right)^{1/2} \le \sqrt{n+1}\ \mathrm{H}(P)$. □

Let $y \in \mathbb{C}$ be an algebraic number and its minimal polynomial over $\mathbb{Z}$ is $P_y(x)$. The degree of $P_y(x)$ is called the *degree* of y and $\mathrm{H}(P_y)$ is called the *height* of y, also denoted $\mathrm{H}(y)$.

We also need the following notion of *resultants*.

Definition 6.2. *Let $P(x) = a_n \prod_{i=1}^n (x - \alpha_i)$ and $Q(x) = b_m \prod_{i=1}^m (x - y_i)$ be two non-constant polynomials. The resultant of $P(x)$ and $Q(x)$ is defined as*

$$\mathrm{Res}(P, Q) = a_n^m b_m^n \prod_{1 \le i \le n} \prod_{1 \le i \le m} (\alpha_i - y_j).$$

It is a standard result that $\mathrm{Res}(P, Q)$ is an integer polynomial in the coefficients of $P(x)$ and $Q(x)$. The resultant is also the determinant of the so-called Sylvester matrix. In particular, when $P(x)$ and $Q(x)$ are integer polynomials, $\mathrm{Res}(P, Q)$ is always an integer, as the Sylvester matrix is an integer matrix in this case. Moreover, we can rewrite the resultant as follows:

$$\mathrm{Res}(P, Q) = a_n^m \prod_{1 \le i \le n} Q(\alpha_i) = (-1)^{mn} b_m^n \prod_{1 \le j \le m} P(y_j).$$

Now we are ready to give a lower bound for any integer polynomial evaluated at an algebraic number. It is a standard result in algebraic number theory. For completeness we provide a proof here and the treatment is from (Bugeaud 2004, Theorem A.1).

Lemma 6.3. *Let $P(x)$ be an integer polynomial of degree n, and $y \in \mathbb{C}$ be an algebraic number of degree d. Then either $P(y) = 0$ or*

$$|P(y)| \geq C_y^{-n} \left((n+1)\mathrm{H}(P)\right)^{-d+1}.$$

where $C_y > 1$ is an effectively computable constant that only depends on y.

Proof. Assume $P(y) \neq 0$. Let $Q(x) = b_d \prod_{i=1}^{d}(x - y_i)$ be the minimal polynomial of y over $\mathbb{Z}$ with $y_1 = y$.

Suppose there is an $j \neq 1$ such that $P(y_j) = 0$. As $Q(x)$ is the minimal polynomial of y, none of y_j could be a rational number. Hence there is an automorphism of the splitting field of $Q(x)$ that maps y_j to y. Applying this automorphism on both sides of $P(y_j) = 0$, we get $P(y) = 0$. Contradiction!

Hence we have $P(y_i) \neq 0$ for all i and the resultant of $P(x)$ and $Q(x)$ is non-zero. Since $\mathrm{Res}(P, Q)$ is an integer, we have

$$1 \leq |\mathrm{Res}(P, Q)| = |b_d|^n \prod_{1 \leq i \leq d} |P(y_i)|.$$

Clearly, by triangle inequality we have

$$|P(y_i)| \leq (n+1)\mathrm{H}(P)(\max\{1, |y_i|\})^n.$$

It implies,

$$\begin{aligned} 1 &\leq |P(y)||b_d|^n \left((n+1)\mathrm{H}(P)\right)^{d-1} \prod_{2 \leq i \leq d} (\max\{1, |y_i|\})^n \\ &= |P(y)| \left((n+1)\mathrm{H}(P)\right)^{d-1} \left(\frac{\mathrm{M}(Q)}{\max\{1, |y|\}}\right)^n \\ &\leq |P(y)| \left((n+1)\mathrm{H}(P)\right)^{d-1} \left(\sqrt{d+1}\mathrm{H}(y)\right)^n \end{aligned}$$

where the last inequality follows from Lemma 6.1. Therefore we have

$$|P(y)| \geq ((n+1)\mathrm{H}(P))^{-d+1} \left(\sqrt{d+1}\mathrm{H}(y)\right)^{-n}.$$

Let $C_y = \sqrt{d+1}\mathrm{H}(y)$ and the lemma holds. □

Lemma 6.4. *Let G be a graph and $y \in \mathbb{C}$ a non-zero algebraic number of degree d. There exists a positive constant $C > 1$ depending only on y such that if $Z_{Ising}(G; y) \neq 0$, then $|Z_{Ising}(G; y)| > C^{-m}$, where m is the number of edges in G.*

Proof. Given a graph G, first suppose that G is not connected, G_i's are the components of G. Then $Z_{\text{Ising}}(G; y)= \prod_i Z_{\text{Ising}}(G_i; y)$. It is easy to see that if the claim holds for all components it hold for G as well. Therefore in the following we may assume G is connected. Then $m \geq n - 1$ where n is the number of vertices.

We can rewrite $Z_{\text{Ising}}(G; y)$ as a polynomial in y as follows,

$$P(y) = Z_{\text{Ising}}(G; y) = \sum_{i=0}^{m} C_j y^j,$$

where C_j is the number of configurations such that there are exactly j many monochromatic edges. Notice that $\sum_{j=0}^{m} C_j = 2^n$, we have $\mathrm{H}(P) \leq 2^n$. Assume $P(y) \neq 0$. Apply Lemma 6.3 and we obtain

$$\begin{aligned} |P(y)| &\geq C_y^{-m} ((m+1)\mathrm{H}(P))^{-d+1} \\ &\geq (m+1)^{-d+1} C_y^{-m} 2^{-(d-1)n}, \end{aligned}$$

where $C_y > 1$ is a constant depending only on y. As $m \geq n-1$, the right hand side decays exponentially in m and the lemma follows. □

Lemma 6.5. *Let G be a graph and $y, z \in \mathbb{C}$ two roots of unity. Let n be the number of vertices in G and m the number of edges. There exists a positive constant $C > 1$ depending only on y and z such that if $Z_{Ising}(G; y, z) \neq 0$, then $|Z_{Ising}(G; y, z)| > C^{-m}$.*

Proof. As in the previous lemma we may assume G is connected and $m \geq n-1$. Suppose y is of order d_1 and z order d_2. Let d be the least common multiple of d_1 and d_2. Then there exists a root of unity w of order d such that $y = w^{t_1}$ and $z = w^{t_2}$.

Given a graph G, we can rewrite $Z_{\text{Ising}}(G; y, z)$ as a polynomial in y and z as follows,

$$Z_{\text{Ising}}(G; y, z) = \sum_{k=0}^{n} \sum_{j=0}^{m} C_{j,k} y^j z^k,$$

where $C_{j,k}$ is the number of configurations such that there are exactly j many monochromatic edges and k many 1 vertices. Let

$$P(w) = Z_{\text{Ising}}(G; y, z) = \sum_{k=0}^{n} \sum_{j=0}^{m} C_{j,k} w^{t_1 j + t_2 k} = \sum_{\ell=0}^{t_1 m + t_2 n} C'_\ell w^\ell,$$

where $C'_\ell = \sum_{t_1 j + t_2 k = \ell} C_{j,k}$. Notice that

$$\sum_{\ell=0}^{t_1 m + t_2 n} C'_\ell = \sum_{k=0}^{n} \sum_{j=0}^{m} C_{j,k} = 2^n.$$

We have $\mathrm{H}(P) \leq 2^n$. Assume $P(w) \neq 0$. Apply Lemma 6.3 and we obtain

$$\begin{aligned} |P(w)| &\geq C_w^{-t_1 m - t_2 n} \left((t_1 m + t_2 n + 1)\mathrm{H}(P)\right)^{-d+1} \\ &\geq (t_1 m + t_2 n + 1)^{-d+1} C_w^{-t_1 m - t_2 n} 2^{-(d-1)n}, \end{aligned}$$

where $C_w > 1$ is a constant depending only on w. As $m \geq n-1$, the right hand side decays exponentially in m and the lemma follows. □

6.2. Hardness results. In this section we will show hardness results when both the edge interaction and external field are roots of unity.

We first consider the external field -1. We describe the edge interaction by specifying an interaction matrix $\begin{bmatrix} n_{00} & n_{01} \\ n_{10} & n_{11} \end{bmatrix}$, where

n_{ij} is the weight when the two endpoints have spins i and j, respectively. In this notation, a binary equality is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and an Ising interaction with weight y is $\begin{bmatrix} y & 1 \\ 1 & y \end{bmatrix}$. Given a gadget with two distinguished vertices, we may view it as an edge and compute its effective interaction matrix M. Then we say the gadget *implements* M. Also, recall the definitions of k-stretch and k-thickening (Observation 2.7, for example).

Lemma 6.6. *Let $K > 1$ and $y \in \mathbb{C}$ be an algebraic complex number such that $y \neq \pm 1$. Then we have* Factor-K-Nonzero-Norm-Ising$(y) \leq_T$ Factor-K-Nonzero-Norm-Ising$(y, -1)$.

Proof. We first argue that a binary equality can be implemented. Consider a 2-stretch with the edge interaction y and external field -1. It is easy to calculate that the (effective) interaction matrix is $\begin{bmatrix} y^2-1 & 0 \\ 0 & 1-y^2 \end{bmatrix}$. Then do a 2-thickening. The resulting matrix is $\begin{bmatrix} (y^2-1)^2 & 0 \\ 0 & (1-y^2)^2 \end{bmatrix}$. Up to a constant of $(y^2-1)^2$ this is equality.

Suppose $G = (V, E)$ is an input to Factor-K-Nonzero-Norm-Ising(y). We introduce a new vertex v' for every vertex $v \in V$. Connect v and v' via this equality gadget, that is, first a 2-stretch and then a 2-thickening. Hence the external field on v is cancelled with this construction. The reduction follows. □

Next we consider the case when a real edge interaction can be implemented. If the norm of the interaction is less than 1, then we can cancel out the external field.

Lemma 6.7. *Let $K > 1$ and $K' > 1$. Let y and z be two roots of unity and $z \neq \pm 1$. Suppose some real number $w \in (-1, 1)$ as an edge interaction is implementable for the Ising model with edge interaction y and external field z. Then we have* Factor-K-Nonzero-Norm-Ising$(y) \leq_T$ Factor-(KK')-Nonzero-Norm-Ising(y, z).

Proof. Let $G = (V, E)$ be an input to Factor-K-Nonzero-Norm-Ising(y). Assume $Z_{\text{Ising}}(G; y) \neq 0$ as otherwise we are done. Suppose $|V| = n$, $|E| = m$, and $V = \{v_i | 1 \leq i \leq n\}$.

Suppose $w = 0$, which means we can implement inequality (see the remark above Lemma 6.6). For each vertex v_i, we introduce a new vertex v_i' and connect v_i and v_i' by the inequality. It is easy to verify that if v_i is assigned 0, the weight from v_i and v_i' together is z; when v_i is assigned 1, the weight is also z. Hence the external field is effectively cancelled and the reduction follows.

Otherwise assume $w \neq 0$, that is $w \in (-1, 0) \cup (0, 1)$. For each vertex v_i, we introduce a new vertex v_i', and add $2t$ many new edges between v_i and v_i', where t is a positive integer which we will choose later. By assumption we can implement the edge interaction w and we put it on all new edges. Let $V' = \{v_i' | 1 \leq i \leq n\}$ and we get a new graph $G' = (V \cup V', E')$.

For each vertex v_i, the contribution of v_i and v_i' (to the partition function) together is $w^{2t} + z$ when v_i is assigned 0 and $z(1 + w^{2t} z)$ when v_i is assigned 1. Let $\lambda = \frac{z(1+w^{2t}z)}{w^{2t}+z}$. Notice that $w^{2t} + z \neq 0$ as $|w| < 1 = |z|$. We have

$$Z_{\text{Ising}}(G'; y, z) = (w^{2t} + z)^n \sum_{\sigma : V \to \{0,1\}} y^{m(\sigma)} \lambda^{n_1(\sigma)},$$

where $m(\sigma)$ is the number of monochromatic edges in E under σ and $n_1(\sigma)$ is the number of vertices in V that are assigned 1.

Let $Z := \left| \frac{Z_{\text{Ising}}(G';y,z)}{(w^{2t}+z)^n} - Z_{\text{Ising}}(G; y) \right|$. We want to show that Z is exponentially small. Apply the triangle inequality:

$$|Z| = \left| \sum_{\sigma : V \to \{0,1\}} y^{m(\sigma)} (\lambda^{n_1(\sigma)} - 1) \right| \leq \sum_{\sigma : V \to \{0,1\}} \left| y^{m(\sigma)} (\lambda^{n_1(\sigma)} - 1) \right|$$

$$= \sum_{\sigma : V \to \{0,1\}} \left| \lambda^{n_1(\sigma)} - 1 \right| = \sum_{j=0}^{n} \binom{n}{j} \left| \lambda^j - 1 \right|, \tag{6.8}$$

where we used the fact that $|y| = 1$. Let $\alpha = \lambda - 1 = \frac{z(1+w^{2t}z)}{w^{2t}+z} - 1 = \frac{w^{2t}(z^2-1)}{w^{2t}+z}$. As $z^2 - 1 \neq 0$ and $w^{2t} + z \neq 0$, $|\alpha|$ is decreasing exponentially in t. We may pick a positive integer $t = O(\log n)$ such that $ne|\alpha| < 1$. Applying the triangle inequality again for each $0 \leq j \leq n$, we get

$$\begin{aligned}
|\lambda^j - 1| &= |\sum_{l=1}^{j} \binom{j}{l} \alpha^l| \leq \sum_{l=1}^{j} \binom{j}{l} |\alpha^l| \\
&= (|\alpha| + 1)^j - 1 \leq (|\alpha| + 1)^n - 1 \\
&= \sum_{l=1}^{n} \binom{n}{l} |\alpha|^l \leq \sum_{l=1}^{n} \left(\frac{ne|\alpha|}{l}\right)^l \\
&\leq n^2 e|\alpha|, \qquad (6.9)
\end{aligned}$$

as $\left(\frac{ne|\alpha|}{l}\right)^l$ is decreasing in l. Plugging (6.9) into (6.8) we have

$$|Z| \leq \sum_{j=0}^{n} \binom{n}{j} n^2 e|\alpha| = e2^n n^2 |\alpha|. \qquad (6.10)$$

Since $Z_{\text{Ising}}(G; y) \neq 0$, by Lemma 6.4, there exists a constant $C_y > 1$ such that $|Z_{\text{Ising}}(G; y)| > C_y^{-m}$. Since $|\alpha|$ is decreasing exponentially in t, by (6.10), we may pick an integer t that is polynomial in n (and sufficiently large with respect to K') such that

$$|Z| < \frac{K' - 1}{K'} C_y^{-m} < \frac{K' - 1}{K'} |Z_{\text{Ising}}(G; y)|. \qquad (6.11)$$

By the definition of $|Z|$ and again the triangle inequality we get

$$\frac{1}{K'} = 1 - \frac{K' - 1}{K'} \leq \frac{|Z_{\text{Ising}}(G'; y, z)|}{|w^{2t} + z|^n |Z_{\text{Ising}}(G; y)|} \leq 1 + \frac{K' - 1}{K'} \leq K'.$$

This finishes the proof. □

A similar proof works when the implementable real field has a larger than 1 norm. Basically when this is the case we may power the external field z. If z is a root of unity then we could power it to 1.

Lemma 6.12. *Let $K > 1$ and $K' > 1$. Let y and z be two roots of unity and $z \neq \pm 1$. Suppose some real number $w \in (-\infty, -1) \cup (1, \infty)$ as an edge interaction is implementable for the Ising model with edge interaction y and external field z. Then we have* Factor-K-Nonzero-Norm-Ising$(y, z^r) \leq_T$ Factor-(KK')-Nonzero-Norm-Ising(y, z) *for any positive integer r.*

Proof. Let $G = (V, E)$ be an input to Factor-K-Nonzero-Norm-Ising(y, z^r). Assume that $Z_{\text{Ising}}(G; y, z^r) \neq 0$ as otherwise we are done. Suppose $|V| = n$, $|E| = m$, and $V = \{v_i | 1 \leq i \leq n\}$.

For each vertex v_i, we introduce $r - 1$ many new vertices $v_{i,j}$, and add $2t$ many new edges between v_i and each $v_{i,j}$, where $j \in [r-1]$ and t is a positive integer which we will choose later. By assumption we can implement the edge interaction w and we put it on all new edges. Let $V' = \{v_{i,j} | 1 \leq i \leq n, 1 \leq j \leq r-1\}$ and we get a new graph $G' = (V \cup V', E')$.

For each vertex v_i, the contribution of v_i and all $v_{i,j}$ combined is $\left(w^{2t} + z\right)^{r-1}$ when v_i is assigned 0 and $z\left(1 + w^{2t} z\right)^{r-1}$ when v_i is assigned 1. Let $\lambda = \frac{z\left(1+w^{2t}z\right)^{r-1}}{\left(w^{2t}+z\right)^{r-1}}$. Notice that $w^{2t} + z \neq 0$ as $|w| > 1 = |z|$. We have

$$Z_{\text{Ising}}(G'; y, z) = \left(w^{2t} + z\right)^{n(r-1)} \sum_{\sigma: V \to \{0,1\}} y^{m(\sigma)} \lambda^{n_1(\sigma)},$$

where $m(\sigma)$ is the number of monochromatic edges in E under σ and $n_1(\sigma)$ is the number of vertices in V that are assigned 1.

Let $Z := \left| \frac{Z_{\text{Ising}}(G'; y, z)}{\left(w^{2t}+z\right)^{n(r-1)}} - Z_{\text{Ising}}(G; y, z^r) \right|$. As the previous proof we show that Z is exponentially small. Apply the triangle inequality:

$$\begin{aligned}
|Z| &= \left| \sum_{\sigma: V \to \{0,1\}} y^{m(\sigma)} \left(\lambda^{n_1(\sigma)} - z^{r n_1(\sigma)}\right) \right| \\
&\leq \sum_{\sigma: V \to \{0,1\}} \left| y^{m(\sigma)} \left(\lambda^{n_1(\sigma)} - z^{r n_1(\sigma)}\right) \right| \\
&= \sum_{\sigma: V \to \{0,1\}} \left| \lambda^{n_1(\sigma)} - z^{r n_1(\sigma)} \right| = \sum_{j=0}^{n} \binom{n}{j} \left| \lambda^j - z^{rj} \right|, \qquad (6.13)
\end{aligned}$$

where we used the fact that $|y| = 1$. Let $\alpha = \lambda - z^r = \frac{z\left(1+w^{2t}z\right)^{r-1}}{(w^{2t}+z)^{r-1}} - z^r = z\left((z+\mu)^{r-1} - z^{r-1}\right)$, where $\mu = \frac{1+w^{2t}z}{w^{2t}+z} - z = \frac{1-z^2}{w^{2t}+z} \neq 0$. As $z^2 - 1 \neq 0$ and $|w| > 1$, $|\mu|$ decreases exponentially in t. Pick a large enough integer t so that $|\mu| < 1$. Hence $|\alpha| = |z||(z+\mu)^{r-1} - z^{r-1}| = |\sum_{j=1}^{r-1}\binom{r-1}{j}\mu^j z^{r-1-j}| \leq \sum_{j=1}^{r-1}\binom{r-1}{j}|\mu^j| < |\mu|2^{r-1}$ by the triangle inequality. As $|\mu|$ decreases exponentially in t, so does $|\alpha|$.

Notice that $|\lambda| = |z^r + \alpha| \leq |z|^r + |\alpha| = 1 + |\alpha|$. Pick t large so that $|\alpha| < 1$. Applying the triangle inequality again for each $0 \leq j \leq n$, we get

$$\begin{aligned} |\lambda^j - z^{rj}| &= |\lambda - z^r|\left|\sum_{l=0}^{j-1}\lambda^l z^{r(j-1-l)}\right| \leq |\alpha|\left(\sum_{l=0}^{j-1}\left|\lambda^l z^{r(j-1-l)}\right|\right) \\ &= |\alpha|\left(\sum_{l=0}^{j-1}|\lambda|^l\right) \leq |\alpha|\left(\sum_{l=0}^{j-1}(1+|\alpha|)^l\right) \\ &< |\alpha|\left(\sum_{l=0}^{j-1}2^l\right) < 2^j|\alpha| \leq 2^n|\alpha|, \end{aligned} \tag{6.14}$$

as $|z| = 1$. Plugging (6.14) into (6.13) we have

$$|Z| < \sum_{j=0}^{n}\binom{n}{j}2^n|\alpha| = 4^n|\alpha|. \tag{6.15}$$

Since $Z_{\text{Ising}}(G; y, z^r) \neq 0$, by Lemma 6.5, there exists a constant $C_{y,z^r} > 1$ such that $|Z_{\text{Ising}}(G; y, z^r)| > C_{y,z^r}^{-|E|}$. Since $|\alpha|$ is decreasing exponentially in t, by (6.15), we may pick an integer t that is polynomial in n (and sufficiently large with respect to K') such that

$$|Z| < \frac{K'-1}{K'}C_{y,z^r}^{-|E|} < \frac{K'-1}{K'}|Z_{\text{Ising}}(G; y, z^r)|. \tag{6.16}$$

By the definition of $|Z|$ and again the triangle inequality we get

$$\begin{aligned} \frac{1}{K'} = 1 - \frac{K'-1}{K'} &\leq \frac{|Z_{\text{Ising}}(G'; y, z)|}{|w^{2t}+z|^{n(r-1)}|Z_{\text{Ising}}(G; y, z^r)|} \\ &\leq 1 + \frac{K'-1}{K'} \leq K'. \end{aligned}$$

This finishes the proof. □

We will show how to implement a real edge interaction in the next lemma. Unless the norm of the new interaction is 1, the hardness holds due to the previous two lemmas. The failure cases are indeed polynomial-time computable.

Lemma 6.17. *Let $K > 1$. Let y and z be two roots of unity such that $y \notin \{1, -1, \mathrm{i}, -\mathrm{i}\}$ and $z \notin \{1, -1\}$. Then* Factor-K-Nonzero-Norm-Ising(y, z) *is* #**P***-hard.*

Proof. Let $y = e^{\mathrm{i}\theta}$ and $z = e^{\mathrm{i}\varphi}$ and $\theta, \varphi \in [0, 2\pi)$. Then $\theta \notin \{0, \pi/2, \pi, 3\pi/2\}$ and $\varphi \notin \{0, \pi\}$.

Since y is a root of unity, there exists an integer power of y that equals y^{-1}. Hence we can implement y^{-1} by thickenings. Then we implement a real interaction $w(\theta, \varphi)$ by the following gadget. We replace every edge by two parallel gadgets: one is a 2-stretch with interaction y (on both edges) and the other is also a 2-stretch but with y^{-1}. Then we calculate the effective edge interaction. When both endpoints are assigned 0, the contribution is $(y^2 + z)(1/y^2 + z) = 1 + z^2 + z(y^2 + 1/y^2)$. When both endpoints are assigned 1, the contribution is $(y^2 z + 1)(z/y^2 + 1) = 1 + z^2 + z(y^2 + 1/y^2)$ as well. When one endpoint is assigned 0 and the other 1, the contribution is $y(1 + z) \cdot (1 + z)/y = (1 + z)^2$. Hence effectively on this edge the interaction is of the Ising type and its weight is $w(\theta, \varphi) = \frac{1+z^2+z(y^2+1/y^2)}{(1+z)^2}$.

We claim $w(\theta, \varphi) \in \mathbb{R}$. This is because

$$\begin{aligned} w(\theta, \varphi) &= \frac{1 + z^2 + z(y^2 + 1/y^2)}{(1 + z)^2} = 1 + \frac{z(y^2 + 1/y^2 - 2)}{(1 + z)^2} \\ &= 1 + \frac{(y - 1/y)^2}{z + 1/z + 2} = 1 + \frac{-4 \sin^2 \theta}{2 \cos \varphi + 2} \\ &= 1 - \frac{\sin^2 \theta}{\cos^2 \frac{\varphi}{2}}. \end{aligned}$$

Notice that $\cos \frac{\varphi}{2} \neq 0$ as $\varphi \neq 0, \pi$. If $|w| < 1$, then we are done by combining Lemma 6.7 and Corollary 3.14. Otherwise if $|w| > 1$, the lemma follows from Lemma 6.12 by powering z to 1, and Corollary 3.14.

The failure case is $|w(\theta,\varphi)| = 1$ and hence $\sin^2\theta = 2\cos^2\frac{\varphi}{2}$ or $\sin\theta = 0$. Note that $\sin\theta = 0$ implies $y = \pm 1$ which contradicts our assumption. It is easy to implement y^2, which has argument 2θ. We then repeat the construction. If $|w(2\theta,\varphi)| \neq 1$, then it is reduced to previous cases. Otherwise $|w(2\theta,\varphi)| = 1$, implying that $\sin^2 2\theta = 2\cos^2\frac{\varphi}{2} = \sin^2\theta$ or $\sin 2\theta = 0$. The latter case is impossible as $\theta \notin \{0, \pi/2, \pi, 3\pi/2\}$. Hence $\sin^2 2\theta = \sin^2\theta$. It is easy to show that $\theta \in \{\pi/3, 2\pi/3, 4\pi/3, 5\pi/3\}$ as $\theta \neq 0, \pi$. Therefore $2\cos^2\frac{\varphi}{2} = \sin^2\theta = 3/4$. However $\cos^2\frac{\varphi}{2} = 3/8$ has no solution φ that is a rational fraction of π, which contradicts the fact that z is a root of unity. This finishes the proof. □

LEMMA 6.18. *Let $K > 1$. Let $y = \pm\mathrm{i}$ and z be a root of unity that is not one of $\{1, -1, \mathrm{i}, -\mathrm{i}\}$. Then* FACTOR-$K$-NONZERO-NORM-ISING$(y,z)$ *is* #**P**-*hard.*

PROOF. Let $y = e^{\mathrm{i}\theta}$ and $z = e^{\mathrm{i}\varphi}$ where $\theta, \varphi \in [0, 2\pi)$. As $y = \pm\mathrm{i}$, we have $\theta \in \{\pi/2, 3\pi/2\}$ and $z \notin \{1, -1, \mathrm{i}, -\mathrm{i}\}$ implies $\varphi \notin \{0, \pi/2, \pi, 3\pi/2\}$. We use the same $w(\theta,\varphi) \in \mathbb{R}$ construction as in the proof of Lemma 6.17. If $|w(\theta,\varphi)| = 0$ then $\cos^2\frac{\varphi}{2} = 1$. This implies $\varphi/2 \in \{0, \pi\}$ contradicting $\varphi \notin \{0, \pi/2, \pi, 3\pi/2\}$. If $|w(\theta,\varphi)| = 1$ then $\cos^2\frac{\varphi}{2} = 1/2$. This implies $\varphi/2 \in \{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$ also contradicting $\varphi \notin \{0, \pi/2, \pi, 3\pi/2\}$. Hence we can implement a real edge interaction $w(\theta,\varphi)$ such that $|w(\theta,\varphi)| \neq 0, 1$.

Note that $w(\theta,\varphi) = 1 - \frac{\sin^2\theta}{\cos^2\frac{\varphi}{2}} = 1 - 1/\cos^2\frac{\varphi}{2} < 0$. If $w(\theta,\varphi) \in (-1, 0)$, then we adopt the construction in the proof of Lemma 6.7 to cancel the external field of z. Hence we can reduce FACTOR-K-NONZERO-NORM-ISING$(w(\theta,\varphi))$ to FACTOR-(KK')-NONZERO-NORM-ISING(y,z) for any constant $K' > 1$. The #**P**-hardness follows from Corollary 3.11.

Otherwise $w(\theta,\varphi) \in (-\infty, -1)$, then we use Lemma 6.12 to power up the external field of z. Instead of powering z to 1, we would like to pick a positive integer r such that $w(\theta, r\varphi) \in (-1, 0)$, which reduces to the previous case. This is equivalent to $\frac{1}{2} < \cos^2\frac{r\varphi}{2} < 1$, which, in turn, is equivalent to $r\varphi \in (0, \pi/2) \cup (3/2\pi, 2\pi)$ modulo 2π. Suppose $\varphi = \frac{2a\pi}{b}$ where a, b are two coprime positive integers and $b = 3$ or $b \geq 5$ since $z \notin \{1, -1, \mathrm{i}, -\mathrm{i}\}$.

Assume $b \geq 5$ first. As a, b are co-prime, there exist two integers l_1 and l_2 such that $l_1 a + l_2 b = 1$ and $l_1 > 0$. Let $r = l_1$ and we have $r\varphi/2 = \frac{2al_1\pi}{b} = \frac{2\pi}{b} - 2l_2\pi$. This choice of r meets the requirement since $\frac{2\pi}{b} \in (0, \pi/2)$.

The case left is when $b = 3$, in which case $\varphi \in \{2\pi/3, 4\pi/3\}$. We reduce Factor-$K$-Nonzero-Norm-Ising$(y, -z)$ to Factor-K-Nonzero-Norm-Ising(y, z). This suffices due to $\arg(-z) = \varphi + \pi$, which is one of the previous cases.

Suppose $G = (V, E)$ is an input to Factor-K-Nonzero-Norm-Ising$(y, -z)$. Introduce a new vertex v' for each vertex $v \in V$. Since $y = \pm\mathrm{i}$, there exists a positive integer t such that $y^t = -1$. Connect v and v' by t many new edges. We can calculate that the effective field of v in the new graph (with respect to interaction y and field z) is $\frac{z - z^2}{z - 1} = -z$. This finishes our proof. □

We can now prove our main theorem about this model.

Theorem 1.9. *Let $K > 1$. Let y and z be two roots of unity. Then the following holds:*

(i) If $y = \pm\mathrm{i}$ and $z \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$, or $y = \pm 1$, then $Z_{\mathit{Ising}}(-; y, z)$ can be computed exactly in polynomial time.

(ii) Otherwise Factor-K-Nonzero-Norm-Ising(y, z) *is* #**P**-*hard.*

Proof. If $y = \pm 1$, then we can replace every edge interaction by two unary constraints. Hence the problem is tractable for any external field. Consider next the case where $y = \pm\mathrm{i}$. If $z \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$, the algorithm is from Cai *et al.* (2014). Otherwise, the hardness is from Lemma 6.18. Finally, for the rest of the proof, we consider the case where $y \notin \{1, -1, \mathrm{i}, -\mathrm{i}\}$. For $z = 1$, the hardness follows from Corollary 3.14. For $z = -1$, the hardness is obtained by combining Lemma 6.6 and Corollary 3.14. Otherwise $z \notin \{1, -1\}$, and the hardness follows from Lemma 6.17. □

Acknowledgements

We thank Dan Shepherd and Mark Jerrum for useful discussions.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) ERC grant agreement no. 334828. The paper reflects only the authors' views and not the views of the ERC or the European Commission. The European Union is not liable for any use that may be made of the information contained therein.

Part of the work was done during HG's visit in the University of Oxford. HG is also supported by the EPSRC grant EP/N004221/1.

References

Scott Aaronson (2005). Quantum computing, postselection, and probabilistic polynomial-time. *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **461**(2063), 3473–3482.

Scott Aaronson & Alex Arkhipov (2013). The Computational Complexity of Linear Optics. *Theory of Computing* **9**, 143–252.

Dorit Aharonov & Itai Arad (2011). The BQP-hardness of approximating the Jones polynomial. *New Journal of Physics* **13**(3), 035 019.

M. Bordewich, M. Freedman, L. Lovász & D. Welsh (2005). Approximate Counting and Quantum Computation. *Combin. Probab. Comput.* **14**(5-6), 737–754.

Michael J. Bremner, Richard Jozsa & Dan J. Shepherd (2011). Classical Simulation of Commuting Quantum Computations implies Collapse of the Polynomial Hierarchy. *Proc. R. Soc. A* **467**(2126), 459–472.

Y. Bugeaud (2004). *Approximation by Algebraic Numbers.* Cambridge Tracts in Mathematics. Cambridge University Press. ISBN 9781139455671.

Jin-Yi Cai, Pinyan Lu & Mingji Xia (2014). The complexity of complex weighted Boolean #CSP. *J. Comput. Syst. Sci.* **80**(1), 217–236.

G. De las Cuevas, W. Dür, M. Van den Nest & M. A. Martin-Delgado (2011). Quantum algorithms for classical lattice models. *New Journal of Physics* **13**(9), 093 021.

Michael H. Freedman, Alexei Kitaev, Michael J. Larsen & Zhenghan Wang (2003). Topological quantum computation. *Bull. Amer. Math. Soc. (N.S.)* **40**(1), 31–38.

Michael H. Freedman, Michael Larsen & Zhenghan Wang (2002). A modular functor which is universal for quantum computation. *Comm. Math. Phys.* **227**(3), 605–622.

Keisuke Fujii & Tomoyuki Morimae (2013). Quantum Commuting Circuits and Complexity of Ising Partition Functions. *CoRR* **abs/1311.2128**.

Joseph Geraci & Daniel A Lidar (2010). Classical Ising model test for quantum circuits. *New Journal of Physics* **12**(7), 075 026.

Leslie Ann Goldberg & Mark Jerrum (2008). Inapproximability of the Tutte polynomial. *Inf. Comput.* **206**(7), 908–929.

Leslie Ann Goldberg & Mark Jerrum (2012). Inapproximability of the Tutte polynomial of a planar graph. *Computational Complexity* **21**(4), 605–642.

Leslie Ann Goldberg & Mark Jerrum (2014). The Complexity of Computing the Sign of the Tutte Polynomial. *SIAM J. Comput.* **43**(6), 1921–1952.

S. Iblisdir, M. Cirio, O. Kerans & G. K. Brennen (2014). Low depth quantum circuits for Ising models. *Annals of Physics* **340**(205), 205–251.

F. Jaeger, D. L. Vertigan & D. J. A. Welsh (1990). On the computational complexity of the Jones and Tutte polynomials. *Math. Proc. Cambridge Philos. Soc.* **108**(1), 35–53.

Mark Jerrum & Alistair Sinclair (1993). Polynomial-Time Approximation Algorithms for the Ising Model. *SIAM J. Comput.* **22**(5), 1087–1116.

RICHARD JOZSA & MARRTEN VAN DEN NEST (2014). Classical Simulation Complexity of Extended Clifford Circuits. *Quantum Info. Comput.* **14**(7&8), 633–648.

GREG KUPERBERG (2015). How Hard Is It to Approximate the Jones Polynomial? *Theory of Computing* **11**, 183–219.

A. MATSUO, K. FUJII & N. IMOTO (2014). A quantum algorithm for additive approximation of Ising partition functions. *Phys. Rev. A* **90**, 022 304.

MICHAEL A. NIELSEN & ISAAC L. CHUANG (2004). *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences).* Cambridge University Press, 1st edition. ISBN 0521635039.

J. SCOTT PROVAN & MICHAEL O. BALL (1983). The Complexity of Counting Cuts and of Computing the Probability that a Graph is Connected. *SIAM J. Comput.* **12**(4), 777–788.

DAN SHEPHERD (2010). Binary Matroids and Quantum Probability Distributions. *CoRR* **abs/1005.1744**.

DAN J. SHEPHERD & MICHAEL J. BREMNER (2009). Temporally Unstructured Quantum Computation. *Proc. R. Soc. A* **465**(2105), 1413–1439.

ALAN D. SOKAL (2005). The multivariate Tutte polynomial (alias Potts model) for graphs and matroids. In *Surveys in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, 173–226. Cambridge Univ. Press, Cambridge.

MORWEN B. THISTLETHWAITE (1987). A spanning tree expansion of the Jones polynomial. *Topology* **26**(3), 297–309.

LESLIE G. VALIANT & VIJAY V. VAZIRANI (1986). NP is as Easy as Detecting Unique Solutions. *Theor. Comput. Sci.* **47**(3), 85–93.

ABRAHAM ZIV (1982). Relative distance—an error measure in round-off error analysis. *Math. Comp.* **39**(160), 563–569.

Manuscript received 25 Feburary 2015

Leslie Ann Goldberg
Department of Computer Science,
University of Oxford, UK.

Heng Guo
School of Mathematical Sciences,
Queen Mary, University of London, Mile End Road,
London E1 4NS, UK.