



# On The Efficient Approximation of the Potts Partition Function by Quantum Computers

Joseph Geraci / Daniel Lidar  
UNIVERSITY OF TORONTO/ UNIVERSITY OF SOUTHERN CALIFORNIA



## BACKGROUND

### The Potts Partition Function

- The Potts Partition Function is given by  $Z(\beta) = \sum e^{-\beta H(\sigma)}$  where H is the Hamiltonian.
- The sum is taken over all spin configurations where the number of possible states a spin can be in is  $q$ . When  $q=2$  we have the Ising model. Here we take  $q$  prime.
- It is well known that  $Z$  (over planar graphs) can be written as the product of an easily computed function and the Jones polynomial of an associated knot. More generally we have  $Z_T(\nu) = q^{|T|} T$  where  $T$  is the graph in question and  $T$  is the Tutte polynomial.
- Figure C gives a recent Theorem about approximating the Jones polynomial (2).
- It is also well known that the Tutte polynomial is related to the weight enumerator polynomial from classical coding theory given by  $A(x, y) = \sum_{i=0}^n A_i x^i y^{n-i}$

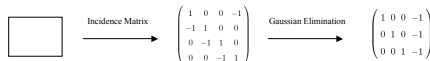
## Some Classical Coding Theory

**Definition** Let  $\mathbb{F}_q$  be a finite field where  $q = q^r$  with  $q$  prime. A linear code  $C$  is a  $k$  dimensional subspace of the vector space  $\mathbb{F}_q^n$  and is referred to as an  $[n, k]$  code. The code is said to be of length  $n$  and of dimension  $k$ .

- A "word" in  $C$  is an  $n$ -tuple  $(c_0, c_1, \dots, c_{n-1})$ . We say that  $C$  is cyclic if when  $(c_0, c_1, \dots, c_{n-1})$  is in  $C$  then so is  $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$ .
- A  $k$  by  $n$  matrix whose rows are a basis for  $C$  is called the generator matrix for the code  $C$ .
- Most cyclic codes have subspaces which are themselves cyclic, but there are those which do not have any cyclic subspace. We call these Irreducible Cyclic Codes and we are particularly interested in these.
- The weight enumerator  $A(x, y)$  mentioned above is very important for the scheme presented here. The coefficients  $A_i$  are equal to the number of words with weight  $i$ , where by the weight we mean the number of non-zero symbols in a word  $(c_0, c_1, \dots, c_{n-1})$ .

## Graph Representation

- The graph over which the Potts model is defined can be associated to a certain matrix which we shall call the Cycle Matroid Matrix (CMM)
- The CMM is constructed as follows: Find the incidence matrix of the graph  $\Gamma(E, V)$  (the  $|V|$  by  $|E|$  matrix with one 1 and one -1 in each column representing the edge-vertex incidence structure). Next use Gaussian elimination to obtain a matrix of the form  $[I|R]$ . This is the CMM.
- Consider the following example with the rectangle graph:



- The columns of the CMM refer to the cycle structure of the graph and the rows generate what is known as the cocycle code in the literature (4). Therefore the CMM is the generator matrix for the cocycle code. In this way every graph has a cocycle code associated with it.

## The Main Theorem

**Theorem** A classical computer with access to a quantum oracle can efficiently approximate the  $q$ -state Potts Partition Function for graphs whose CMM generates either

1. a  $[k + \Delta, \Delta]$  irreducible cyclic code where  $k \geq \frac{k^2-1}{\Delta} - \Delta$  (where  $\Delta$  and  $s \in \mathbb{N}$ ) or
2. a  $[k + \Delta, k]$  cyclic code whose dual code satisfies 1.

- The proof of this theorem relies on a certain representation of the Potts Partition function involving the weight enumerator  $A(x, y)$  given in Note 1.
- Given this, if we are able to find the weight spectrum  $\{A_i\}$  approximately, we would be able to obtain an approximation of  $Z$ .
- Please refer to Note 2. This demonstrates that quantum computers can efficiently (polynomial complexity) estimate the weights of words.
- Note that due to the coding theoretic structure of this scheme we do not have to contend with every word in the code. We have  $nN = q^k - 1$  where  $n$  is the number of repeats of words of the same weight. There are then less than  $N$  words of different weight. Next note that we take the following restriction:  $k \geq \frac{k^2-1}{\Delta} - \Delta$ . This guarantees that the algorithm scales polynomially in the input size  $O(k^2)$ .
- The above restriction affects the types of graphs over which the model is defined. These graphs are intermediate between fully connected and those graphs with vertices only connected to two neighbors. In fact it seems that small world graphs are favored in this scheme.
- We take a tally (a quantum tally offers a quadratic speed up) and once we have this tally we can construct the weight enumerator polynomial and therefore easily construct the approximation to the Potts partition function  $Z$ .

### Note 1

**Theorem 4** Let  $A(x, y)$  be the weight enumerator of the cyclic code of  $\Gamma, C(\Gamma)$  (which is of length  $n$ ), let  $s(E)$  be the number of connected components of  $\Gamma$ , and  $q$  prime where each vertex can be in one of  $q$  possible states. Then

$$Z(\beta) = q^{-s(E)} A(1, q^\beta)$$

This result is outlined and proved in (4). It is not surprising as one should expect this after realizing the relationship between the Potts partition function and the Tutte polynomial. It requires making a change of variables and defining a new Hamiltonian given by

$$H(\sigma) = -J U(\sigma)$$

$U(\sigma)$  is the subset of edges where the vertices have the same spin for a particular spin configuration  $\sigma$ .

It is in general, a hard problem to find the Weight Enumerator  $A(x, y)$ . If one were able however to estimate the weight spectrum  $\{A_i\}$ , then one would be able to construct  $A(1, y)$  and therefore be able to estimate  $Z$ .

### Note 2

#### Gauss Sums and The McElice Theorem

Given the alphabet of the cocycle code comes from a finite field  $F = \mathbb{F}_q$  with  $q$  elements we consider two subgroups of  $F$ . The additive group  $F$  itself and the multiplicative group  $F$  with 0 omitted. Associated with each group is a canonical homomorphism from the group to the complex numbers. We shall call the multiplicative homomorphism  $\chi$  and note that the additive one is parameterized by  $\beta$  in  $F$ . A Gauss sum is given by

$$G(F, \chi, \beta) = \sum_{\alpha \in F} \chi(\alpha) e^{i\pi \beta \alpha^2}$$

Due to (3) we have an efficient quantum algorithm for the approximation of Gauss Sums. This is important here because of the following theorem.

**Theorem 1** (McElice Theorem)

The weight of each word in an irreducible cyclic code is given by

$$w(\alpha) = \frac{q^k(q-1)}{q^k} - \frac{q-1}{q^k} \sum_{\beta \in F} \chi^{-1}(\alpha) G(F, \chi, \beta)$$

where  $\chi^{-1}$  is the inverse of  $\chi$ .

## An Overview of the Proof

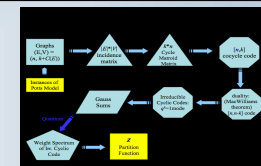


Figure A

A general OWCT/Quantum Oracle Weight Enumerator is of the form  $N(A, B, x, y) = \sum_{i=0}^n (1 + \beta_i x^i y^{n-i})^k$  where  $A$  and  $B$  are  $k$ -matrices with  $k!$  elements in  $\mathbb{F}_q$  and  $\beta_i \in \mathbb{F}_q$ . Weight enumerators are usually found in the theory of error-correcting codes and spin glasses have been considered in this context.

Figure B

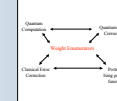


Figure C

There is a recent theorem which can be used to approximate the Jones polynomial. This is a generalization of the Jones polynomial and it is given by  $J(K) = \sum_{\sigma \in S_n} \text{Tr}(R(\sigma))$  where  $R$  is a representation of the braid group  $B_n$ . The theorem states that  $J(K) = \sum_{\sigma \in S_n} \text{Tr}(R(\sigma))$  for a certain representation  $R$  of the braid group  $B_n$ .

## CURRENT RESEARCH AND BEYOND

- We intend to identify the types of graphs that serve as efficient instances which arise naturally in the scheme presented here. Are small world networks one type of graph that naturally arises?
- We wish to use this scheme to begin a classification of the Potts model in terms of instances for which quantum computers will be able to efficiently evaluate approximations of the partition function and those instances which will be too difficult to handle. Is this scheme optimal?
- We are currently working on a characterization of the Ising model which uses a relationship between the Ising partition function and OWCT's (see Figure A). The main theorem can be viewed as an algorithm that accepts a graph and generates an instance of the Ising model (interaction distribution on the edges) which corresponds to a quantum circuit with a relationship to the partition function. The quantum circuit is also returned.

## BIBLIOGRAPHY

- (1) Joseph Geraci and Daniel Lidar, *On the Efficient Approximation of the Potts Partition Function By Quantum Computers* - preprint.
- (2) D. Aharonov, V. Jones and Z. Landau, *On the Quantum Algorithm for Approximating the Jones Polynomial*, preprint.
- (3) Win van Dam and Gadiel Seroussi, *Efficient Quantum Algorithms for Estimating Gauss Sums*, arXiv:quant-ph/0207131 v1, July 23 2002.
- (4) P. Shor and R. Laflamme, *Quantum Mac Williams Identities*, quant-ph/9610040, 1996.
- (5) A. Barg *On Some Polynomials Related to Weight Enumerators of Linear Codes*, SIAM J. Discrete Math., **Vol 15** #2, 155, (2002).
- (6) M. Moiso *Exponential Sums, Gauss Sums, and Cyclic Codes*, www.uwasa.fi/mamo/vaitos.pdf (1997)