Application: factoring

Given a positive composite integer N, what prime numbers when multiplied together equal it?

$$N = p_1 \cdot p_2 \cdots p_m \quad , \quad p_i \text{ prime}$$

$\longrightarrow$ "factoring problem"

Will make use of two theorems:

Theorem 1:

Suppose N is an L bit composite number, and x is a non-trivial solution to the equation $x^2 = 1 \pmod N$ in the range $1 \le x \le N$, that is, neither $x = 1 \pmod N$ nor $x = N-1 = -1 \pmod N$. Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N that can be computed using $O(L^3)$ operations.

Theorem 2:

Suppose $N = p_1^{\alpha_1} \cdots p_2^{\alpha_m}$ is the prime factorization of an odd composite positive integer. Let y be an integer chosen uniformely at random, subject to the requirements that $1 \leq y \leq N-1$ and y is co-prime to N. Let r be the order of y modulo N. Then

$$p\left(r \text{ is even and } y^{r/2} \not\equiv -1 \pmod{N}\right) \geq 1 - \frac{1}{2^m}$$

→ setting $x \equiv y^{\frac{r}{2}} \pmod{N}$, where y is from Th. 2, gives nontrivial solution to $x^2 = 1 \pmod{N}$

→ use Th. 1.

Schematics of factoring algorithm:

- Inputs : A composite number N
- Outputs : A non-trivial factor of N
- Runtime: $O((\log N)^3)$ operations. Succeeds with probability $O(1)$.

- Procedure:

1) If is even, return the factor 2.
2) Determine whether $N = a^b$ for integers $a \geqslant 1$ and $b \geqslant 2$, and if so return the factor a (classical)
3) Randomely choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.
4) Use the order-finding subroutine to find the order r of x modulo N.
5) If r is even and $x^{r/2} \neq -1 \pmod N$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so.

Example: Factoring 15 quantum-mechanically

choose $N = 15$

→ choose random number which has no common factors with N:

$x = 7$

→ compute order of $x = 7 \pmod{15}$:

$$|0\rangle|0\rangle$$

$$\downarrow \quad \text{set } t = 11$$

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle|0\rangle = \frac{1}{\sqrt{2^t}} \left[|0\rangle + |1\rangle + |2\rangle + \dots + |2^t-1\rangle \right] |0\rangle$$

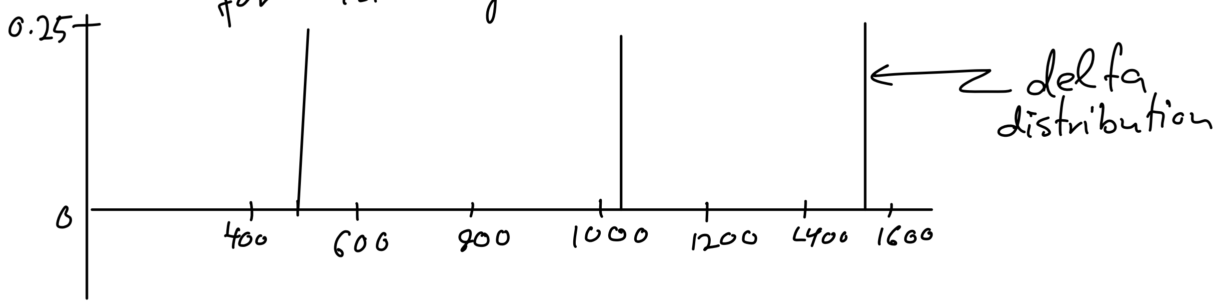
$$\downarrow \quad \text{compute } f(k) = x^k \bmod N \to \text{2nd register}$$

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |x^k \bmod N\rangle$$

$$= \frac{1}{\sqrt{2^t}} \Big[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + |6\rangle|4\rangle + \cdots \Big]$$

$$\downarrow \quad FT^\dagger$$

measure 2nd register → probability distr. for 1st register:



$\downarrow$ measure first register

suppose we get $l = 1536$ $\left(p = \frac{1}{4}\right)$

$\downarrow$ continued fractions

$$\frac{1536}{2048} = \frac{1}{1 + \frac{1}{3}} = \frac{3}{4}$$

$\downarrow$

$r = 4$, is even and $x^{\frac{r}{2}} \bmod N = 4 = -1$
$7^2 \bmod 15$

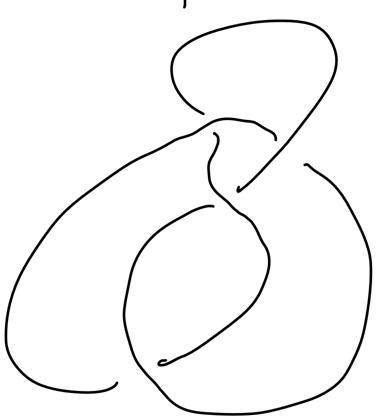
$\downarrow$

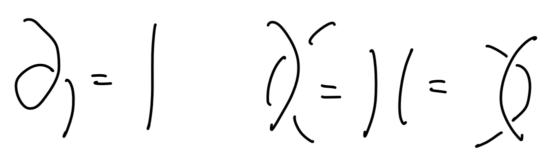
$\gcd(x^2 - 1, 15) = 3$ and $\gcd(x^2 + 1, 15) = 5$

$\longrightarrow 15 = 3 \times 5$

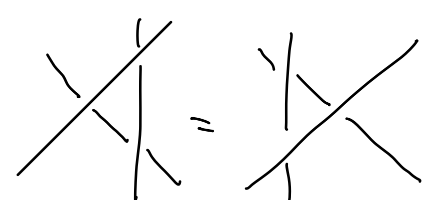
A Quantum Algorithm to approximate the Jones polynomial

Jones polynomial is link invariant (of links in 3d):

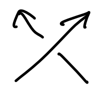
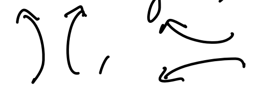




where

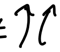
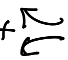


$\rightarrow$ reflect continuous def. in 3d algorithm:

(i) smooth each crossing 
in two ways $\{$  $\}$

$\longrightarrow$ denote resulting diagram with closed loops and no crossings by s (state)

(ii) For each state s, assign a weight

$$W(s) = A^{s^+ - s^-} d^{|s|-1}, \quad s^+ = \#$$  $,\ s^- = \#$ 

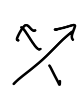
where $d = -(A^2 + A^{-2})$

$\longrightarrow$ summation over all states gives Kauffman bracket $\langle L \rangle$ defined as:

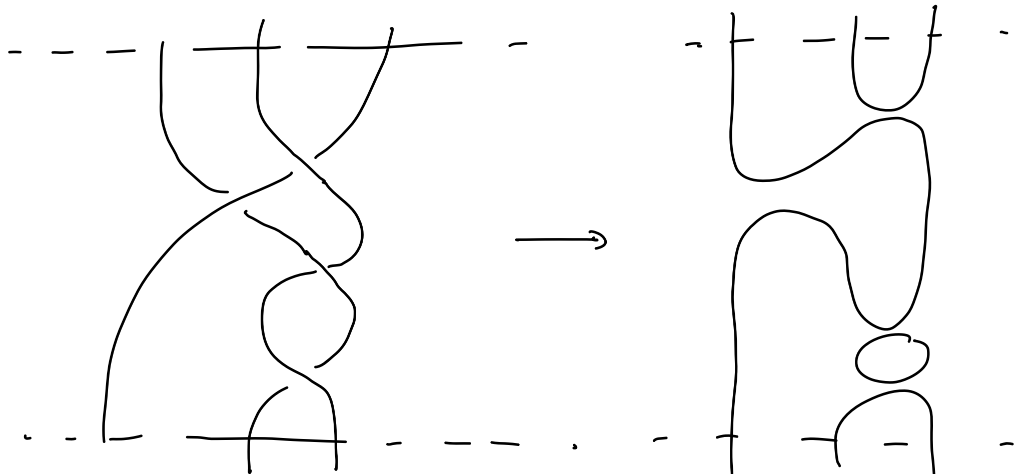
$$\langle L \rangle = \sum_s W(s)$$

$\longrightarrow$ the Jones polynomial is defined as a function of $t = A^{-4}$:

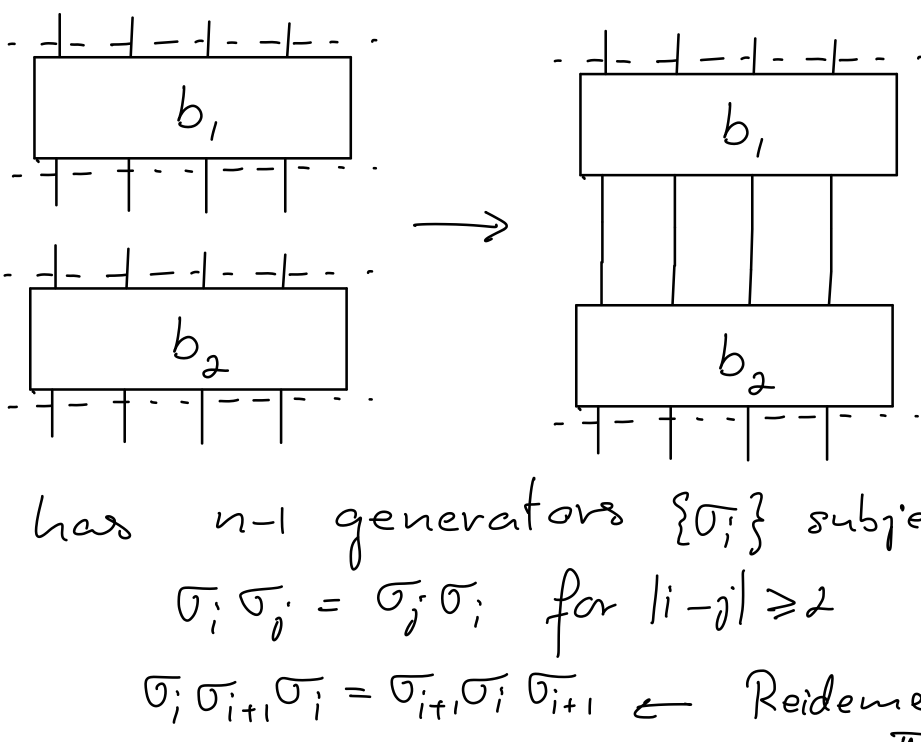
$$V_L(t) = (-A)^{3w(L)} \langle L \rangle,$$

where $w(L) = \#$  $- \#$ 

Let B_n be a braid group consisting of the braid diagrams of n strands



multiplication of two braid diagrams b_1 and b_2 is defined by

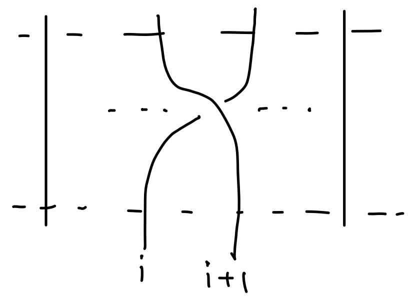


B_n has $n-1$ generators $\{\sigma_i\}$ subject to:

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{for } |i-j| \geq 2$$

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \leftarrow \text{Reidemeister move } \underline{III}$$

σ_i :



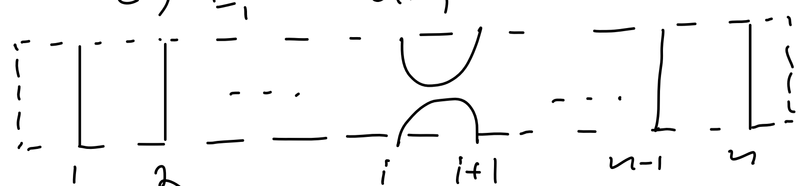
Embed B_n into $TL_n(d)$ (Temperly-Lieb algebra)

generators $TL_n(d)$: $\{E_1, \dots, E_{n-1}\}$

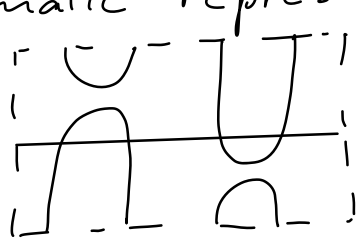
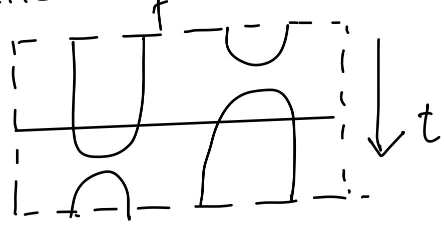
relations : (a) $E_i E_j = E_j E_i$, $|i-j| \geq 2$

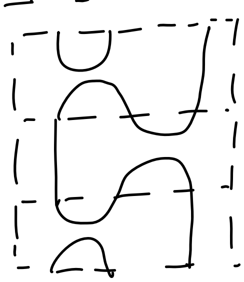
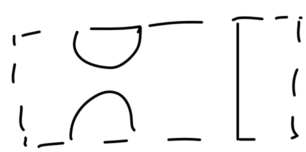
(b) $E_i E_{i\pm 1} E_i = E_i$,

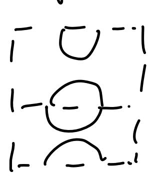
(c) $E_i^2 = d E_i$

where $E_i =$ 

diagramatic representation of relations :

(a)  = 

(b)  = 

(c)  $= d$