Quantum Money from Knots

with
David Gosset
Avinatan Hassidim
Andrew Lutomirski
Peter Shor

Good Currency

* Hard to Copy
* Verifiable
* Verifiable without contacting a third party

Bills or information stored on a computer

$$\boxed{i \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle}$$

Schrödinger Equation

$$|\psi(t)\rangle = U(t, t_0) |\psi(t_0)\rangle$$

Quantum Mechanics is Linear

Do not ask about measurements!

$$|\psi_1(0)\rangle \longrightarrow |\psi_1(t)\rangle$$

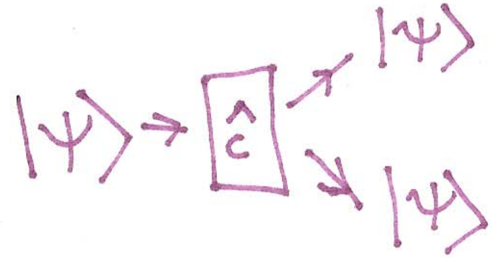
$$|\psi_2(0)\rangle \longrightarrow |\psi_2(t)\rangle$$

$$\alpha |\psi_1(0)\rangle + \beta |\psi_1(0)\rangle \longrightarrow \alpha |\psi_1(t)\rangle + \beta |\psi_2(t)\rangle$$

Can we copy an unknown state $|\psi\rangle$?

Want a Quantum Cloner, $\hat{C}$.

$$\boxed{\hat{C}\left(|\psi\rangle|b\rangle\right) = |\psi\rangle|\psi\rangle}$$



Not Linear, Not Possible. !!

Illustrate: Two levels $|\uparrow\rangle, |\downarrow\rangle$

Good U

$$U\left(|\uparrow\rangle|b\rangle\right) = |\uparrow\rangle|\uparrow\rangle$$

$$U\left(|\downarrow\rangle|b\rangle\right) = |\downarrow\rangle|\downarrow\rangle$$

Linear: $U\left(\left(\alpha|\uparrow\rangle + \beta|\downarrow\rangle\right)|b\rangle\right) = \alpha|\uparrow\rangle|\uparrow\rangle + \beta|\downarrow\rangle|\downarrow\rangle$

But the cloner should have

$$\hat{C}\left(\left(\alpha|\uparrow\rangle + \beta|\downarrow\rangle\right)|b\rangle\right) = \left(\alpha|\uparrow\rangle + \beta|\downarrow\rangle\right)\left(\alpha|\uparrow\rangle + \beta|\downarrow\rangle\right)$$

$$= \alpha^2|\uparrow\rangle|\uparrow\rangle + \ldots$$

$\boxed{\text{Quantum Money}}$

Stephen Weisner (1970, 1983)

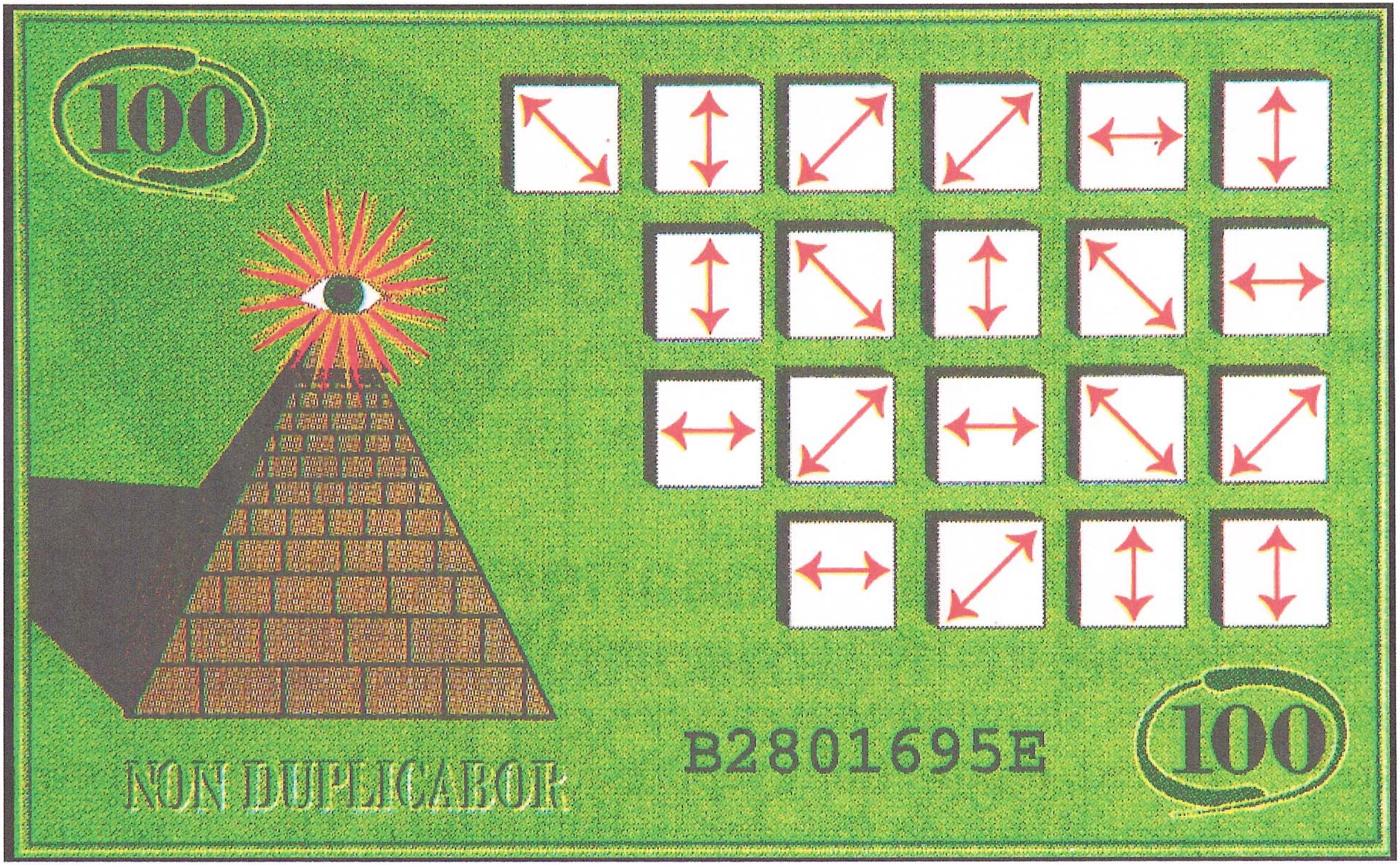
Money is an n-qubit product state

$$\boxed{|\$\rangle = |+\rangle|\uparrow\rangle|\downarrow\rangle|-\rangle \ldots |-\rangle}$$

No cloning Theorem prevents copying the bill.

The mint that made the money knows, for each qubit, if it is an eigenstate of σ_x or σ_z with eigenvalue 1 or −1.

If $|\$\rangle$ is sent back to the mint, the mint can verify that it is good.


100
NON DUPLICABOR
B2801695E
100

We want the merchant to be able to verify the bill without sending it back to the mint. If the merchant knows the quantization axis and the eigenvalue of each qubit then the merchant can verify the money.

However he could also make new bills exactly like the one he got.

We seek a verification procedure that does not allow the merchant to make fresh bills.

Quantum Money

Each bill has a serial number p and an associated quantum state $|\$_p\rangle$.

1. The mint can produce pairs $(p, |\$_p\rangle)$.
2. A merchant is handed a bill $(p, |\$_p\rangle)$. He/She can run a verification algorithm on $|\$_p\rangle$ that outputs "good money" and leaves $|\$_p\rangle$ undamaged.
3. Given $(p, |\$_p\rangle)$ it is hard to make two states $|\psi\rangle$ and $|\psi'\rangle$ each of which passes the verification algorithm.

Blue Print for Quantum Money

Big Set B example $B = \{\text{integers from } 1 \text{ to } 2^n\}$

$n \sim 1000$

$|B|$ = number of elements in B is 2^n

Function $f : B \to T$ $|T|$ is big, say $2^{n/2}$

$|f^{-1}(t)|$ is big for $t \in T$

Many things map to each target value

f is easy to compute

Now go quantum!

Mint makes

$$|\text{initial}\rangle = \frac{1}{\sqrt{|B|}} \sum_{b \in B} |b\rangle |0\rangle$$

Mint computes f into the second register

$$\longrightarrow \frac{1}{\sqrt{|B|}} \sum_{b \in B} |b\rangle |f(b)\rangle$$

Mint measures the second register. Call the observed value p. The state is now

$$\frac{1}{\sqrt{N}} \sum_{\substack{b \in B \\ f(b)=p}} |b\rangle |p\rangle \quad \text{where} \quad N = |f^{-1}(p)|$$

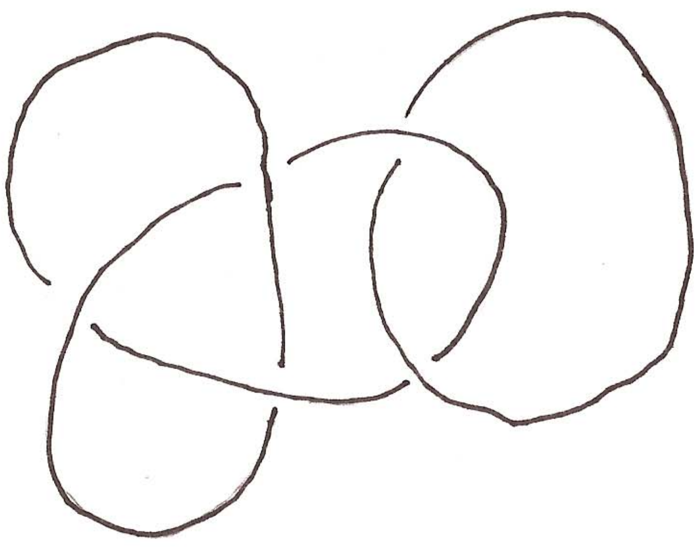
So take $\boxed{|\$_p\rangle = \frac{1}{\sqrt{N}} \sum_{\substack{b \in B \\ f(b)=p}} |b\rangle}$

Knots, Links, Grid Diagrams

A **Knot** is a loop of string in 3 dimensions.
i.e. a map from S^1 into $\mathbb{R}^3$

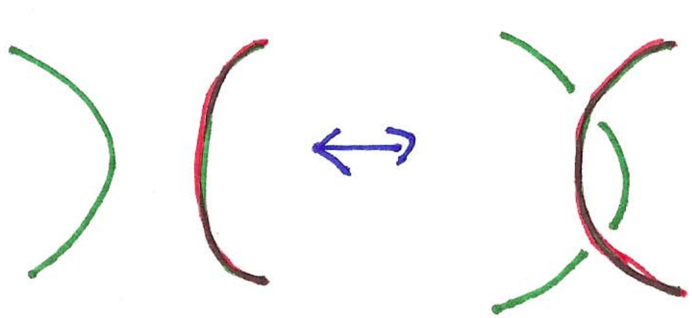
A **link** is a bunch of intertwined knots.

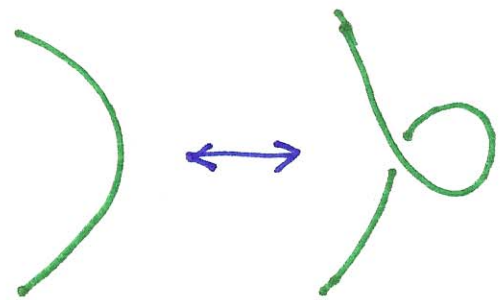
A **link diagram** is a projection into two dimensions. At each crossing it is indicated which strand passes above and which below.

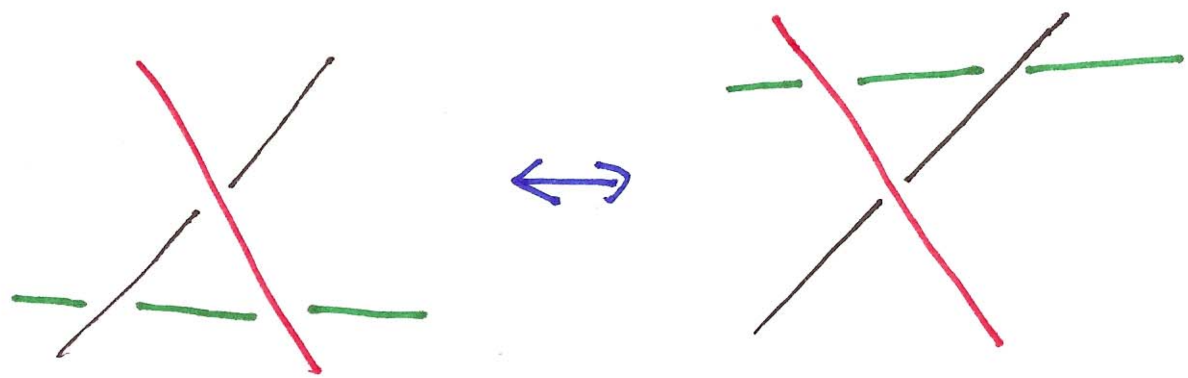


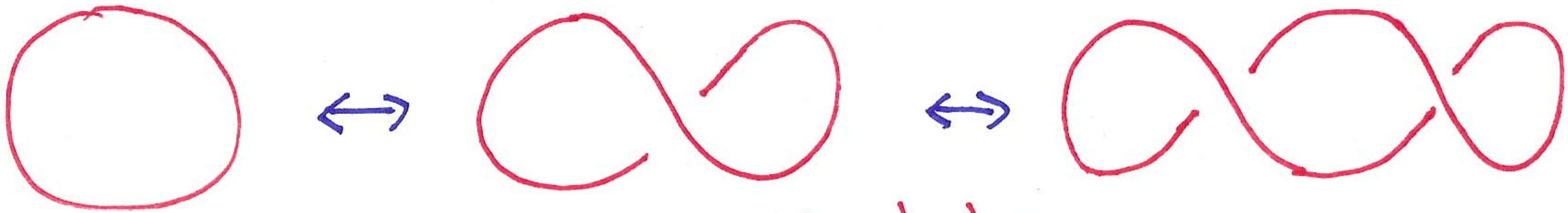
Two links are <u>equivalent</u> if one can be smoothly morphed into the other without cutting the string.

Two links L_1 and L_2 are equivalent <u>if and only if</u> the associated diagrams D_1 and D_2 can be transformed into each other using <u>Reidemeister moves</u>









$\leftrightarrow$ very complicated looking

Given two link diagrams, there is no known procedure for determining if the associated links are equivalent.

Given two equivalent links with different link diagrams there is no known procedure for finding the Reidemeister moves that take one diagram to the other.*

The security of our quantum money scheme is based on the computational difficulty of these problems.

* It is not known if this problem is in NP

A Knot Invariant

There are functions of link diagrams which are invariant under Reidemeister moves.
An example is the Alexander Polynomial which can be efficiently determined from a link diagram.
Given a link diagram D there is a polynomial

$$\left[\ \Delta(x) = p_0 + p_1 X + p_2 X^2 + \cdots p_k X^k\ \right]$$

The list of coefficients p is what we mean by the polynomial.

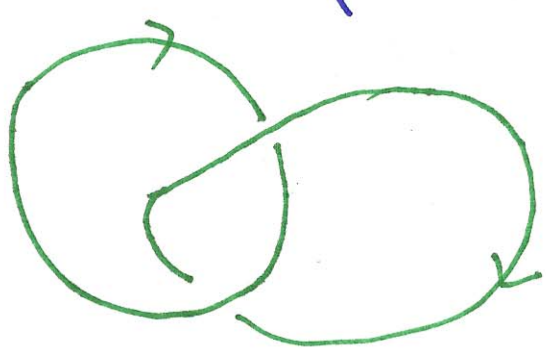
$$\boxed{p = A(D)}$$

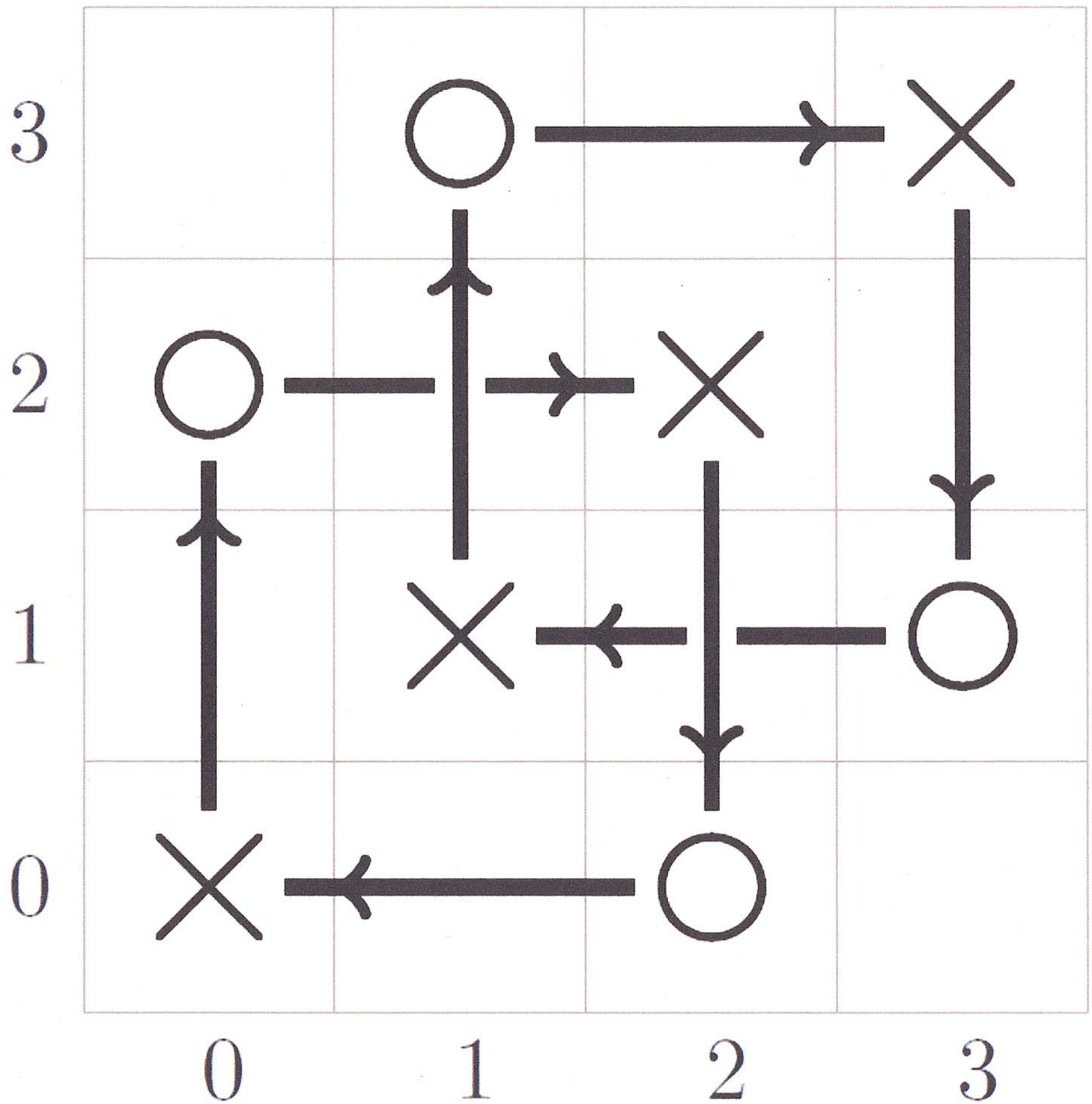
Two link diagrams coming from two equivalent knots have the same Alexander polynomials.
The converse is not true.

Grid Diagrams

We work in a finite dimensional Hilbert space.

We need some discrete way of representing link diagrams so we can encode them as bit strings. A Grid Diagram is a d by d square with d X's and d O's, one of each in each column and row with lines connecting the O's and X's in each column and row. These can be used to represent links.





3
2
1
0
0
1
2
3

Grid diagrams are discrete representations of links.
Reidemeister moves can be formulated as grid moves.
Reidemeister moves can change the number of crossings.
Grid moves can also change the dimension of the grid.

$$P_s(G) = G'$$

$$s \in S = \{\text{a finite list of grid moves}\}$$

$$\dim(G') = \dim(G),\ \dim(G) \pm 1$$

Start is $\tilde{G}$. Apply $P_{s_1}, P_{s_2}, P_{s_3} \ldots$
where $s_1, s_2, s_3 \ldots$ are randomly picked from S.
You will end up with a random grid diagram equivalent to $\tilde{G}$.

Quantum Money from Knots

$$|\text{initial}\rangle = \frac{1}{N} \sum_{\substack{\text{grid diagrams} \\ G}} \rho(G)\,|G\rangle|0\rangle$$

$\rho(G)$ is a weight which depends only on $\dim(G)$.

(The number of grid diagrams of dimension d grows like $[d!]^2$ so we want to cut this off.)

Compute the Alexander Polynomial into the second register.

$$\longrightarrow \frac{1}{N} \sum_{G} \rho(G)\,|G\rangle|A(G)\rangle$$

Measure the second register and get the result p.

Now

$$\boxed{|\$_p\rangle = \frac{1}{N'} \sum_{G:A(G)=p} \varrho(G)\,|G\rangle}$$

This is a massive sum over grid diagrams with the same Alexander Polynomial.

Merchant Verification

Recall $P_s(G) = G'$

For each s, this is one to one, (invertible)

$$\hat{P}_s |G\rangle = |G'\rangle$$

is a quantum operator.

For simplicity Let's take $\varrho \equiv 1$

$$|\tilde{\$}_p\rangle = \sum_{G : A(G) = p} |G\rangle \qquad \text{(normalization?)}$$

Then $\hat{P}_s |\tilde{\$}_p\rangle = |\tilde{\$}_p\rangle$

The state $|\tilde{\$}_p\rangle$ is invariant under all the grid moves.

This is because it contains all Grid diagrams with $A(G) = p$.

The merchant verifies the quantum state by checking that it is invariant under all $\hat{P}_s$.

In fact the merchant can check all grid moves at once!

Append an extra register.

Let

$$\hat{V} = \sum_s \hat{P}_s \otimes |s\rangle\langle s|$$

act on

$$\underbrace{|\tilde{\$}_p\rangle \frac{1}{|S|} \sum_{s'} |s'\rangle}$$

get

$$\sum_s \hat{P}_s |\tilde{\$}_p\rangle \frac{1}{|S|} \sum_s |s\rangle$$

$$= \underbrace{|\tilde{\$}_p\rangle \frac{1}{|S|} \sum_{s'} |s'\rangle}$$

So $\underbrace{\qquad}$ is an eigenstate of $\hat{V}$ with eigenvalue 1.

Measure, get the result 1, and the state is undamaged!

Our Money Scheme:

1. Mint can produce pairs $(P, |\$_P\rangle)$

   Each serial number is different. A rogue mint can not produce the same serial numbers.

2. Tendered Money can be Verified.

3. We do not know how to counterfeit bills.

Our Security is based on the inability to tell if two link diagrams represent equivalent links.

$|\$\rangle$