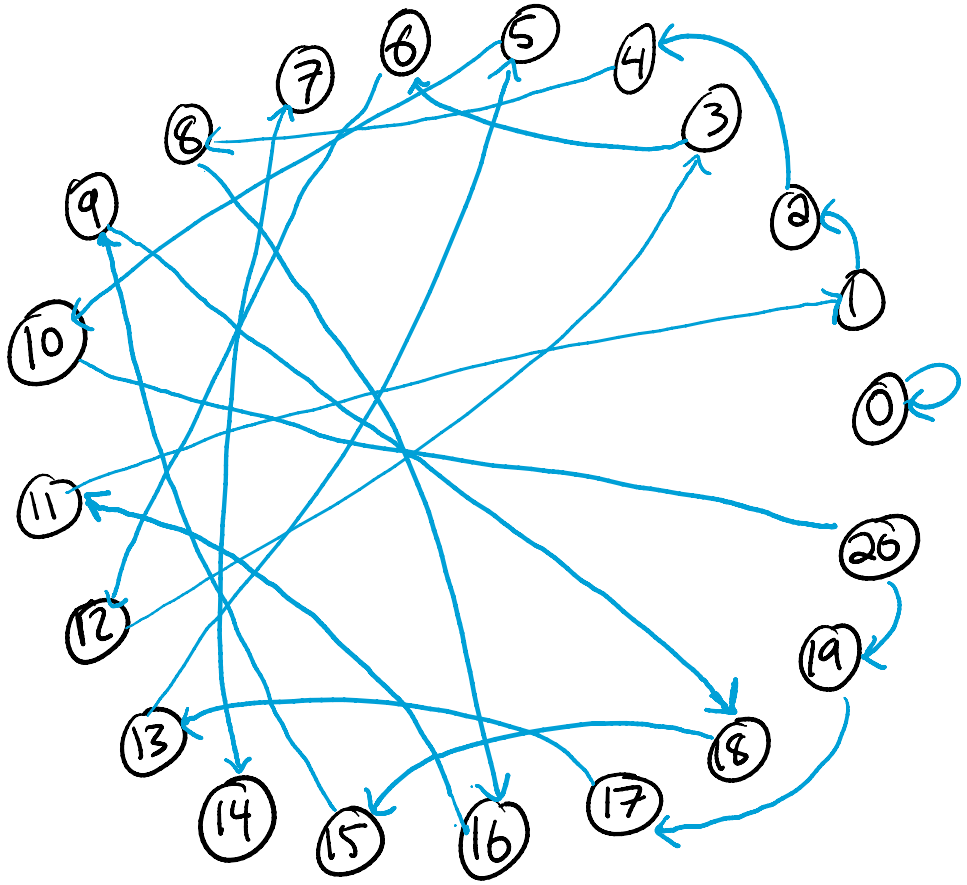
Lecture 19 – Quantum Factoring pt. 1



[[This is the graph]] $G_{21,2}$ [[for trying to factor 21 using "multiplier" 2]] $x \mapsto 2 \cdot x \bmod 21$.

[[Next time we'll explain why...]]

knowing L = length of cycle (1) is on (here: $L = 6$) lets you factor 21.

[[I'll give you a quick sneak preview...]]

[Say you work very hard and discover that....]

$2^6 \equiv 1 \pmod{21}$. Compute $R = 2^{L/2} \pmod{21}$

$= 2^3 \pmod{21} = 8$.

Then $R^2 \equiv (2^{L/2})^2 \equiv 2^L \equiv 1 \pmod{21}$

$\Rightarrow R^2 - 1 \equiv 0$

$\Rightarrow (R-1)(R+1) =$ multiple of $21 = 3 \cdot 7$

↑ ↑ "mystery" factors

$\Rightarrow$ 3, 7 in prime factorization of $R-1, R+1$ (or v.v.)

Find using GCDs: $GCD(R-1, 21) = GCD(7, 21) = 7$

$GCD(R+1, 21) = GCD(9, 21) = 3$

[There's some details to go over here! Next time...

Also, you should imagine all these concrete #'s like 21, 6, etc. have hundreds of digits.

So the odd thing is you know how to walk around — even "warp around" — $G_{21,2}$, but the names of the vertices on the 6-cycle containing ① are all weird...]

[[For analysis purposes, let's give "pseudonyms" to the vertices on this cycle...]]

Real names	"Pseudonyms"
1	"0"
2	"1"
4	"2"
8	"3"
16	"4"
11	"5"
⋮	⋮

[[Yes, initially they start 1, 2, 4, ... but for 100-digit values of "21", you wrap around to weird #'s after a few hundred steps. Yet "L" might have 100's of digits itself...]]

[[Now actually since we're using small #'s, this "5" is the last vertex in cycle of len. L = 6.]]

Can easily classically compute the Adjacency function $x \mapsto 2 \cdot x \bmod 21$.

this is # of bits in number to factor, a few hundred

this 5 has nothing to do with the fact that our last pseudonym is "5"

this is L−1, which is a multi-hundred digit #, usually

[[suffices to store using 5 bits, because $21 \leq 32 = 2^5$]]

Can quantumize the Adjacency code to get a quantum operation "U" mapping $|x\rangle \mapsto |2x \bmod 21\rangle$.

[[there's a small subtlety I'll address next time]]

[[on 5 qubits in our example]]

Actual names (in base 2)

$U|00001\rangle = |00010\rangle$ (one → two)

$U|00010\rangle = |00100\rangle$ (two → four)

⋮

$U|10000\rangle = |01011\rangle$ (sixteen → eleven)

$U|01011\rangle = |00001\rangle$ (eleven → one)

"Pseudonyms"

$U|"0"\rangle = |"1"\rangle$

$U|"1"\rangle = |"2"\rangle$

⋮

$U|"4"\rangle = |"5"\rangle$

$U|"5"\rangle = |"0"\rangle$

[U acts like "Increment mod L" on pseudonyms]

[We know that if you start at $|0\ldots01\rangle = |"0"\rangle$ and repeatedly do U, you hang around in some (mystery) L-dim. subspace. But how does U "rotate" in this space?]

L=3 intuition

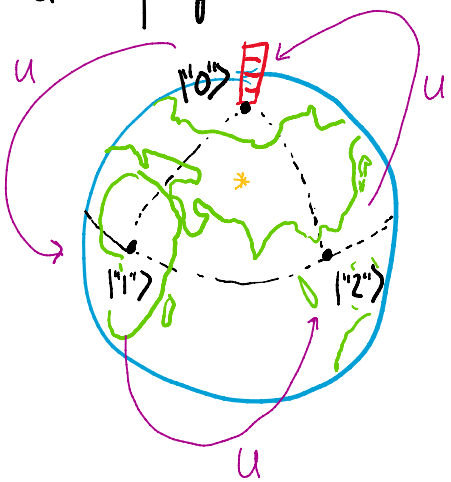
$|"0"\rangle, |"1"\rangle, |"2"\rangle$ are perpendicular unit vecs in some 3-d space.

Picture:

$|"0"\rangle$ = North Pole

$|"1"\rangle$ = Gabon

$|"2"\rangle$ = Singapore



U acts like rotation by $120° = \frac{1}{3}$ Circle around axis thru ✳ = Ufa, Russia, in dir. of $|"0"\rangle + |"1"\rangle + |"2"\rangle$

Fact: Let Q be a unitary op on $\mathbb{R}^N$. Then:

[[proof uses eigenvecs/eigenvals and complex numbers!]]

- $\exists$ some orthogonal 2-d subspaces $P_1, P_2, \ldots$ on which Q rotates by angles $\theta_1, \theta_2, \ldots$
- $\exists$ some other orthogonal 1-d subspaces ("axes") which Q fixes [[like $Rot_{0°}$]]
- $\exists$ remaining orthogonal 1-d subspaces which Q negates (reflects) [[like $Rot_{180°}$]]

[[ok to have no subspaces in some categories]]

[[We won't actually need this fact; just telling you for the sake of culture]]

Goal: Understand these for our U = "Increm. mod L".

[[Not too hard. However, I know a "bookkeeping trick that makes the work a bit cleaner..."]]

Bookkeeping trick: Add in another qubit B.

Dim. of space now $2 \cdot L$.

Let U' = "Do nothing on B, Increm. mod L on other qubits."

Before

$$U: c_0|"0"\rangle + c_1|"1"\rangle + \cdots + c_{L-1}|"L-1"\rangle \longmapsto c_{L-1}|"0"\rangle + c_0|"1"\rangle + \cdots + c_{L-2}|"L-1"\rangle$$

$$(c_0, c_1, c_2, \ldots, c_{L-1}) \longmapsto (c_{L-1}, c_0, c_1, \ldots, c_{L-2})$$

After

$$U': |"0"\rangle_B \otimes |v_0\rangle \text{ (in } \mathbb{R}^2) + |"1"\rangle \otimes |v_1\rangle + \cdots + |"L-1"\rangle \otimes |v_{L-1}\rangle \longmapsto |"0"\rangle \otimes |v_{L-1}\rangle + |"1"\rangle \otimes |v_0\rangle + |"2"\rangle \otimes |v_1\rangle + \cdots$$

⟦Now check out this new...⟧ "Steering Wheel"-type state:

e.g. if $L=5$

$$|SW_1\rangle = \sqrt{\tfrac{1}{5}}\Big(|\text{"0"}\rangle_A \otimes |\rightarrow\rangle_B + |\text{"1"}\rangle_A \otimes |\nearrow\rangle_B + |\text{"2"}\rangle_A \otimes |\nwarrow\rangle_B + |\text{"3"}\rangle_A \otimes |\swarrow\rangle_B + |\text{"4"}\rangle_A \otimes |\searrow\rangle_B \Big)$$

$|\rightarrow\rangle = \text{Rot}_{0\cdot\theta_1}|0\rangle$

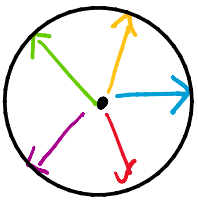
$\text{Rot}_{1\cdot\theta_1}|0\rangle$

$\text{Rot}_{2\theta_1}|0\rangle$

$\text{Rot}_{3\theta_1}|0\rangle$

$\text{Rot}_{4\theta_1}|0\rangle$

$\mathbb{R}^2$



⟦equally spaced by angle

$\theta_1 := \frac{1}{5}\text{Circle} = 72°$

Can also write $|SW_1\rangle \in \mathbb{R}^{10}$ $(10 = 2\cdot L = 2\cdot 5)$ as...

$$|SW_1\rangle = \sqrt{\tfrac{1}{5}}\Big(\underbrace{1,0}_{\text{"0" slot}}, \underbrace{\cos\theta_1, \sin\theta_1}_{\text{"1" slot}}, \underbrace{\cos 2\theta_1, \sin 2\theta_1}_{\text{"2" slot}}, \underbrace{\cos 3\theta_1, \sin 3\theta_1}_{\text{"3" slot}}, \underbrace{\cos 4\theta_1, \sin 4\theta_1}_{\text{"4" slot}} \Big)$$

Fact: Unit length: $\langle SW_1|SW_1\rangle = \frac{1}{5}\left(\|\rightarrow\|^2 + \|\nearrow\|^2 + \|\nwarrow\|^2 + \|\swarrow\|^2 + \|\searrow\|^2 \right) = 1.$

⟦Key point: Imagine doing U', meaning doing just U = "Incr. mod L" on "A" qubits.
It effectively cycles the B-vectors, so...⟧

$$U'|sw_1\rangle = \sqrt{\tfrac{1}{5}}\Big(|\text{"0"}\rangle_A \otimes |\downarrow\rangle_B + |\text{"1"}\rangle_A \otimes |\rightarrow\rangle_B + |\text{"2"}\rangle_A \otimes |\nearrow\rangle_B + |\text{"3"}\rangle_A \otimes |\nwarrow\rangle_B + |\text{"4"}\rangle_A \otimes |\swarrow\rangle_B \Big)$$

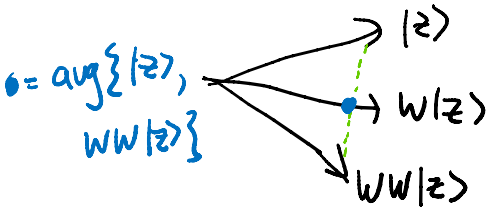
["B-vectors" get "cycled down", which is equivalent to Rotation (clockwise) by $\frac{1}{5}$ Circle $= \theta_1$.]

[Similar to MEP...] U on "A" $\equiv$ $Rot_{-\theta_1}$ on "B" !

Fact: U' rotates $|sw_1\rangle \in \mathbb{R}^{2\cdot L}$ in a 2-dim. subspace (i) by amount θ_1 (ii)

Proof: [Is it "obvious"? Maybe? It's definitely doing this to the B part, but... does that prove it? Anyway...]

To check (i): Abstractly: W rotates $|z\rangle$ in 2d-subsp. iff $W|z\rangle$ is in direction of $\text{avg}\{|z\rangle, W|z\rangle\}$



True for $W = U'$, $|z\rangle = |sw_1\rangle$, because for all "j", avg of "j^{th}" & "$(j+2)^{th}$" B-vector is in direction of $(j+1)^{th}$.

To check (ii): Repeating U' brings $|sw_1\rangle$ back to itself after L steps (and not fewer).

Putting $|SW_1\rangle$ into Revolver Resolver (with U_1) will give output "$\theta \approx \frac{1}{2\pi} \cdot 0.200000\ldots$" [[with high confidence]]

$\frac{1}{L}$ in general.

[[Should be enough to figure out L, if we get a few hundred digits accuracy — which as we'll see next time, we can do efficiently!]]

[[But.... we don't know $|SW_1\rangle$! So how does this help?]]

[[Meanwhile, we only found one 2-d plane where U rotates. Others? Why yes, check out...]]

$$|SW_2\rangle = \frac{1}{\sqrt{5}}\Big(|\text{"0"}\rangle \otimes |\ \rightarrow\ \rangle + |\text{"1"}\rangle \otimes |\ \nwarrow\ \rangle + |\text{"2"}\rangle \otimes |\ \downarrow\ \rangle + |\text{"3"}\rangle \otimes |\ \nearrow\ \rangle + |\text{"4"}\rangle \otimes |\ \swarrow\ \rangle \Big)$$

("A" = $|\text{"0"}\rangle$, $|\text{"1"}\rangle$, $|\text{"2"}\rangle$, $|\text{"3"}\rangle$, $|\text{"4"}\rangle$; "B" = $|\rightarrow\rangle$, $|\nwarrow\rangle$, $|\downarrow\rangle$, $|\nearrow\rangle$, $|\swarrow\rangle$)

- $|\text{"0"}\rangle \otimes |\rightarrow\rangle$ ← $\text{Rot}_{0\cdot\theta_1}|0\rangle$
- $|\text{"1"}\rangle \otimes |\nwarrow\rangle$ ← $\text{Rot}_{2\theta_1}|0\rangle$ ($\frac{2}{L}$ of Circle)
- $|\text{"2"}\rangle \otimes |\downarrow\rangle$ ← $\text{Rot}_{4\theta_1}|0\rangle$ ($\frac{4}{L}$ of Circle)
- $|\text{"3"}\rangle \otimes |\nearrow\rangle$ ← $\text{Rot}_{6\theta_1}|0\rangle$ ($\frac{6}{L}$ of Circle)
- $|\text{"4"}\rangle \otimes |\swarrow\rangle$ ← $\text{Rot}_{8\theta_1}|0\rangle$ ($\frac{8}{L}$ of Circle)

(Wraps to $\frac{10}{L} = \frac{10}{5}$ Circles, which is 0 again)

Same story! RevRes($|SW_2\rangle$) would give "$\theta \approx \frac{1}{2\pi} \cdot 0.4000\ldots$" ($\frac{2}{L}$ in general)

Can similarly define $|SW_3\rangle$: "B-vectors" rotate by $3\theta_1 = \frac{3}{L}$ of circle,

and $|SW_4\rangle, \ldots, |SW_{L-1}\rangle$, last of which is rotation by $\frac{L-1}{L}$ of a circle.

Throw in "$|SW_0\rangle$" $= \sqrt{\frac{1}{L}}\left(|\text{"0"}\rangle\otimes|0\rangle + |\text{"1"}\rangle\otimes|0\rangle + \cdots + |\text{"L-1"}\rangle\otimes|0\rangle\right)$,

which is fixed by U' (Rotation by 0, if you will)

Fact: Putting $|SW_k\rangle$ into Revolver Resolver yields output "$\frac{1}{2\pi}\cdot$(digits of $\frac{k}{L}$)" [[with high confidence]]

[[This should be pretty great for learning L — we'll get to that next time.
Still, we don't know how to make any of these (except for we could approximately make $|SW_0\rangle$, but that's useless as Revkes would just tell us 0 — no clue for L.

There's going to be a deus ex machina, tho.

First, let's establish that these 2-d rotation planes (and 1-d axis) we found are perpendicular...]]

Fact: $|SW_k\rangle$'s are orthonormal; i.e., $\langle SW_k | SW_j \rangle = 0$ for $j \neq k$.

Proof by example:

$$|SW_5\rangle = \sqrt{\tfrac{1}{L}}\left(|0\rangle, \text{Rot}_{5\theta_1}|0\rangle, \text{Rot}_{10\theta_1}|0\rangle, \text{Rot}_{15\theta_1}|0\rangle, \ldots, \text{Rot}_{(L-1)\cdot 5\theta_1}|0\rangle \right)$$

$$|SW_8\rangle = \sqrt{\tfrac{1}{L}}\left(|0\rangle, \text{Rot}_{8\theta_1}|0\rangle, \text{Rot}_{16\theta_1}|0\rangle, \text{Rot}_{24\theta_1}|0\rangle, \ldots \text{Rot}_{(L-1)\cdot 8\theta_1}|0\rangle \right)$$

$$\text{Inner product} = \frac{1}{L}\left(1 + \cos(3\theta_1) + \cos(6\theta_1) + \cos(9\theta_1) + \cdots + \cos((L-1)\cdot 3\theta_1) \right)$$

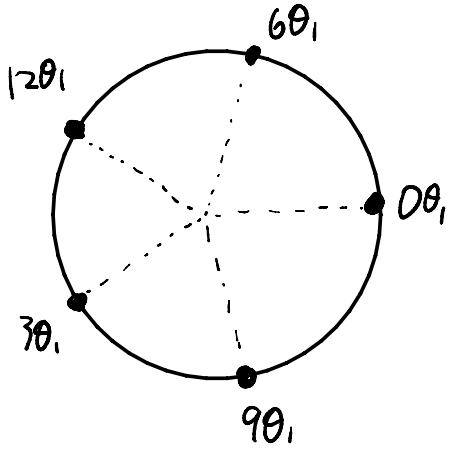
since $\text{Rot}_{5\theta_1}|0\rangle$ & $\text{Rot}_{8\theta_1}|0\rangle$ are unit vecs at angle $3\theta_1$

Recall $\theta_1 = \frac{1}{L}$ Circle $= \frac{2\pi}{L}$

So: want to show $\text{avg}\{\cos(0\theta_1), \cos(3\theta_1), \cos(6\theta_1), \ldots, \cos((L-1)\theta_1)\} = 0$

Look at $\text{avg}\left\{ \begin{bmatrix}\cos(0\theta_1)\\ \sin(0\theta_1)\end{bmatrix}, \begin{bmatrix}\cos(3\theta_1)\\ \sin(3\theta_1)\end{bmatrix}, \begin{bmatrix}\cos(6\theta_1)\\ \sin(6\theta_1)\end{bmatrix}, \ldots \begin{bmatrix}\cos((L-1)\theta_1)\\ \sin((L-1)\theta_1)\end{bmatrix} \right\}$

It's the average (center of mass) of L points around unit circle, spaced out by $3\theta_1 = \frac{3}{L}\cdot 2\pi$:



By symmetry, center of mass is $\begin{bmatrix}0\\0\end{bmatrix}$.

$\therefore$ the cos-average is 0. ✓

(so would be the sin-average).

∎

The Deus Ex Machina

[We have orthonormal states $|SW_0\rangle, |SW_1\rangle, \ldots, |SW_{L-1}\rangle$. Would be happy to get (almost) any of them (maybe not $|SW_0\rangle$): if you had $|SW_k\rangle$ and ran it through Revolver Resolver, would get "$\frac{1}{2\pi} \cdot$ (many digits of k/L)", which is hopefully good enough to get L. Idea: put a random state into Rev.Res... maybe you'll get out the k/L answer for a random k? Actually this works, but there's an even slicker method: we know the unif. superpos. over all $|SW_k\rangle$'s ....]

Q: What is $|start\rangle := \sqrt{\frac{1}{L}}\left(|SW_0\rangle + |SW_1\rangle + \cdots + |SW_{L-1}\rangle\right)$?

A: Some unit vec., by Pythagoras, since $|SW_k\rangle$'s orthonormal.

It's $\sqrt{\frac{1}{L}} \cdot \Big(\sqrt{\frac{1}{L}}(1, 0, \ 1, 0, \ 1, 0, \ \ldots)\ |SW_0\rangle$

$+ \sqrt{\frac{1}{L}}(1, 0, \cos\theta_1, \sin\theta_1, \cos 2\theta_1, \sin 2\theta_1, \ldots)\ |SW_1\rangle$

$+ \sqrt{\frac{1}{L}}(1, 0, \cos 2\theta_1, \sin 2\theta_1 \ldots \ldots)\ |SW_2\rangle$

$+ \sqrt{\frac{1}{L}}(1, 0, \ldots \ldots \ldots)$

$\ldots \ldots \ldots$

$+ \sqrt{\frac{1}{L}}(1, 0, \ldots \ldots \ldots)\ \Big)\ |SW_{L-1}\rangle$

$= (1, 0, \ldots$ wait, that's already len. 1, remaining entries must be all-0's!

$|\text{start}\rangle$ = unif superpos of $|SW_0\rangle, |SW_1\rangle, \ldots, |SW_{L-1}\rangle$

$= (1,0,\ 0,0,\ \ldots\ldots\ 0,0)$
("0" "1" "L-1")

$= |\text{"0"}\rangle_A \otimes |0\rangle_0$

$= |000\ldots01\rangle \otimes |0\rangle$ ← the real name of |"0"⟩ is vertex ①

We can make this!

Then putting $|\text{start}\rangle$ into Revolver Resolver indeed (cf. HW#8.3, next lecture) yields output "$\frac{1}{2\pi}\cdot$(digits of K/L)" for uniformly random $K \in \{0,1,2,\ldots,L-1\}$.

[This is going to let us efficiently find L & hence factor!]