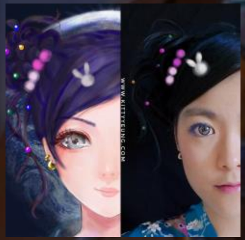
Introduction to Quantum Computing



Kitty Yeung, Ph.D. in Applied Physics

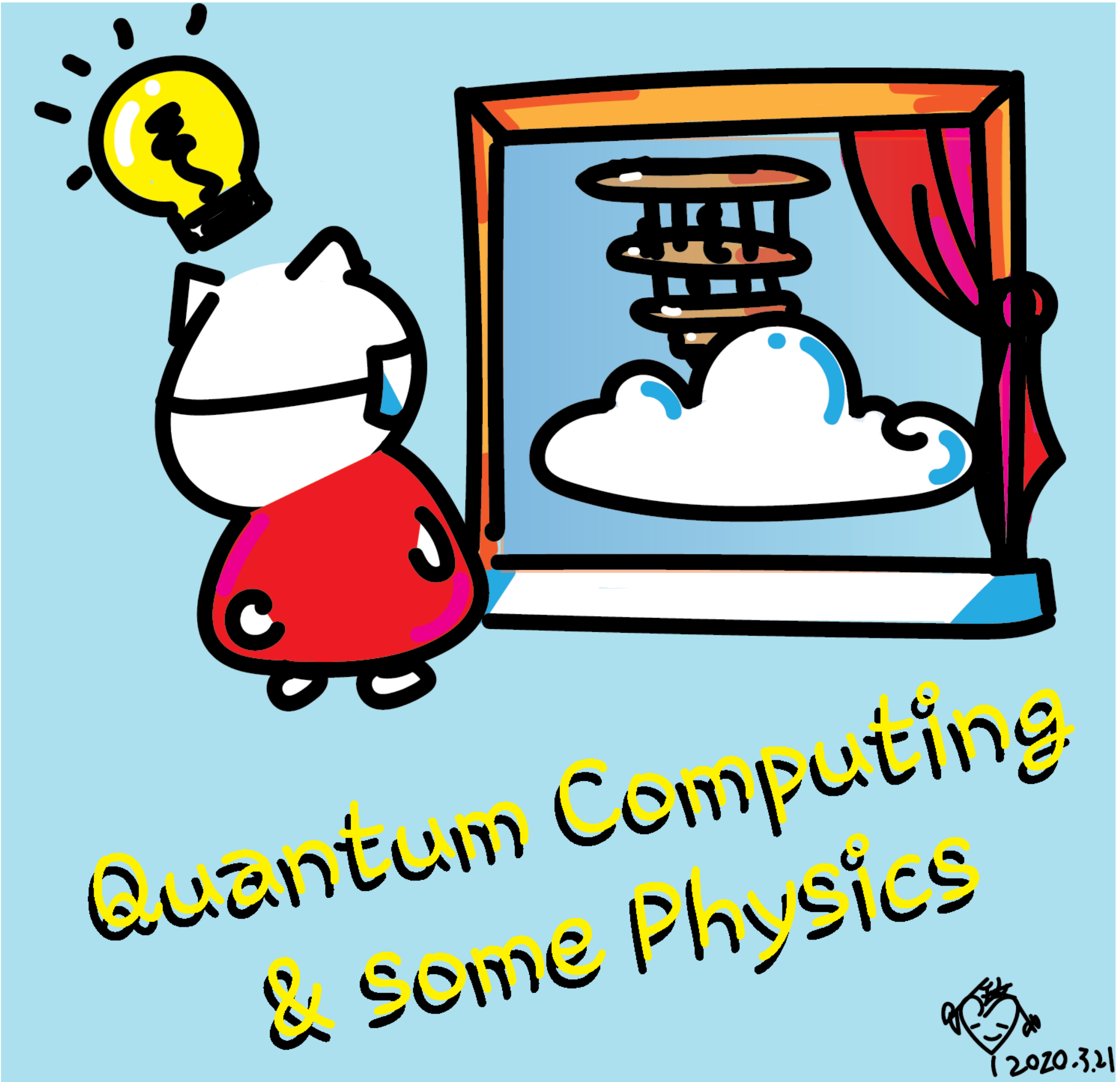
Creative Technologist + Sr. PM
Microsoft

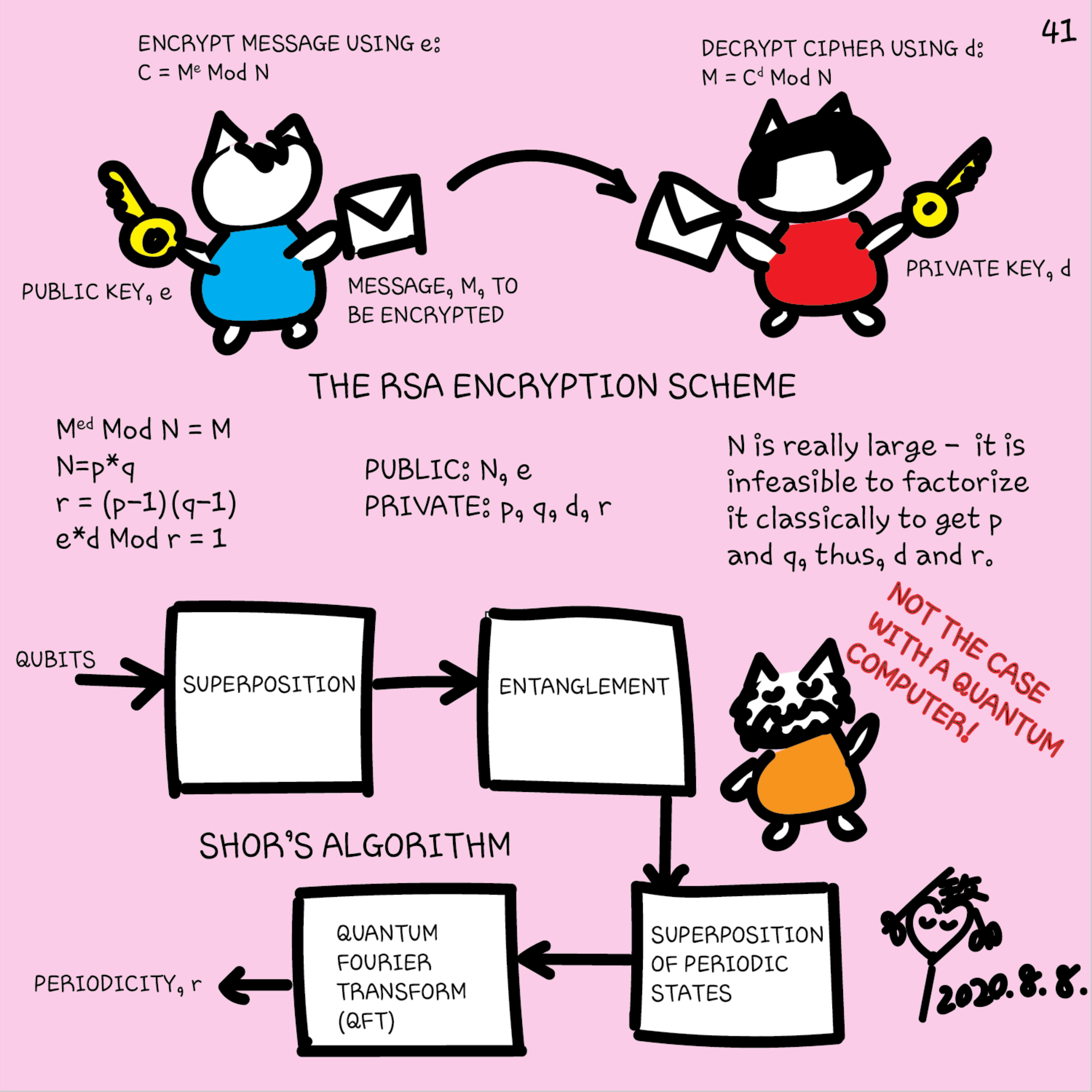
www.artbyphysicistkittyyeung.com
@KittyArtPhysics
@artbyphysicistkittyyeung

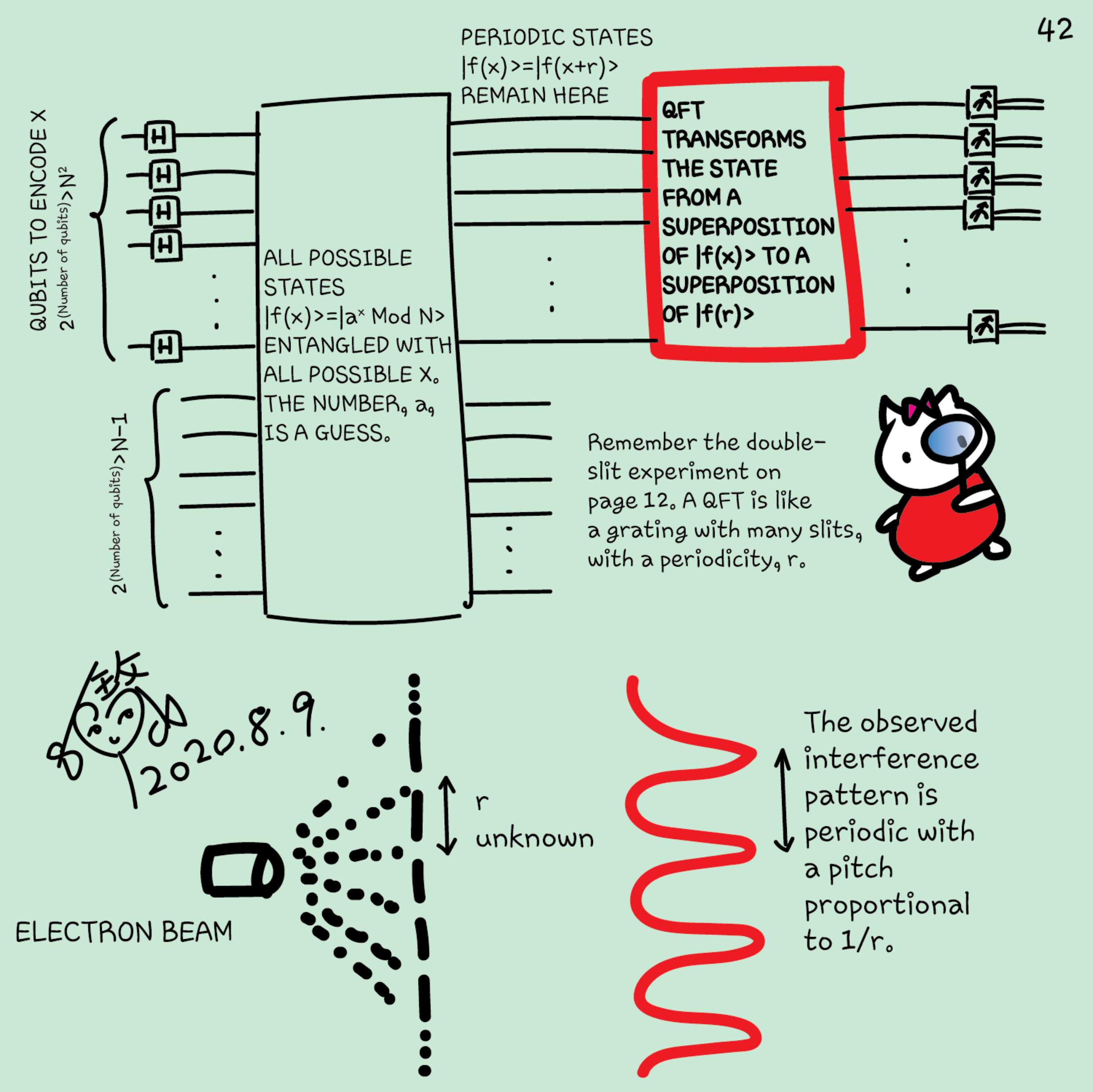
August 16, 2020
Hackaday, session 18
Other communities, session 10

Class structure

- Comics on Hackaday – Quantum Computing through Comics every Sun
- 30 mins – 1 hour every Sun, one concept (theory, hardware, programming), Q&A
- Contribute to Q# documentation http://docs.microsoft.com/quantum
- Coding through Quantum Katas https://github.com/Microsoft/QuantumKatas/
- Discuss in Hackaday project comments throughout the week
- Take notes




ENCRYPT MESSAGE USING e:
C = M^e Mod N
DECRYPT CIPHER USING d:
M = C^d Mod N
PUBLIC KEY, e
MESSAGE, M, TO BE ENCRYPTED
PRIVATE KEY, d
THE RSA ENCRYPTION SCHEME
M^ed Mod N = M
N=p*q
r = (p−1)(q−1)
e*d Mod r = 1
PUBLIC: N, e
PRIVATE: p, q, d, r
N is really large – it is infeasible to factorize it classically to get p and q, thus, d and r.
NOT THE CASE WITH A QUANTUM COMPUTER!
QUBITS
SUPERPOSITION
ENTANGLEMENT
SHOR'S ALGORITHM
SUPERPOSITION OF PERIODIC STATES
QUANTUM FOURIER TRANSFORM (QFT)
PERIODICITY, r
2020.8.8.


42
QUBITS TO ENCODE X
2(Number of qubits) > N²
H
2(Number of qubits) > N−1
ALL POSSIBLE STATES |f(x)>=|aˣ Mod N> ENTANGLED WITH ALL POSSIBLE X. THE NUMBER, a, IS A GUESS.
PERIODIC STATES |f(x)>=|f(x+r)> REMAIN HERE
QFT TRANSFORMS THE STATE FROM A SUPERPOSITION OF |f(x)> TO A SUPERPOSITION OF |f(r)>
Remember the double-slit experiment on page 12. A QFT is like a grating with many slits, with a periodicity, r.
2020.8.9.
ELECTRON BEAM
r unknown
The observed interference pattern is periodic with a pitch proportional to 1/r.

RSA Numbers

- https://en.wikipedia.org/wiki/RSA_numbers
- RSA-100 has 100 decimal digits (330 bits). Its factorization was announced on April 1, 1991 by Arjen K. Lenstra. Reportedly, the factorization took a few days using the multiple-polynomial quadratic sieve algorithm on a MasPar parallel computer.

- RSA-100 = N = 1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139
- RSA-100 = p x q=

37975227936943673922808872755445627854565536638199

× 40094690950920881030683735292761468389214899724061

- Number of qubits needed ~ 659 + 329 = 988

(not considering error-correction qubits)

Let’s use a (much) smaller number

- N = 35 = p * q
- Number of qubits needed = 11, so that

$2^{11} = 2048 > N^2 = 35^2 = 1225$

x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17

Let's use a (much) smaller number

- N = 35 = p * q
- Number of qubits needed = 11, so that

$2^{11} = 2048 > N^2 = 35^2 = 1225$

Periodicity $r = 12$

$a^0\ Mod\ N = 3^0\ Mod\ 35 = a^r Mod\ N = 3^{12} Mod\ 35 = 1$

a^r -1 should be divisible by N

x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17

Pure math

- Rearrange: $(a^{r/2})^2$ -1 should be divisible by N
- ($a^{r/2}$ -1) ($a^{r/2}$ +1) should be divisible by N
- r needs to be even, ($a^{r/2}$ +1) and ($a^{r/2}$ -1) are not individually divisible by N
- p divides ($a^{r/2}$ -1) = 728, q divides ($a^{r/2}$ +1) = 730

- p = GCD(N, ($a^{r/2}$ -1)) = GCD(35,728) = 7
- q = GCD(N, ($a^{r/2}$ +1)) = GCD(35,730) = 5

A different proof: How Quantum Computers Break Encryption | Shor's Algorithm Explained https://www.youtube.com/watch?v=lvTqbM5Dq4Q

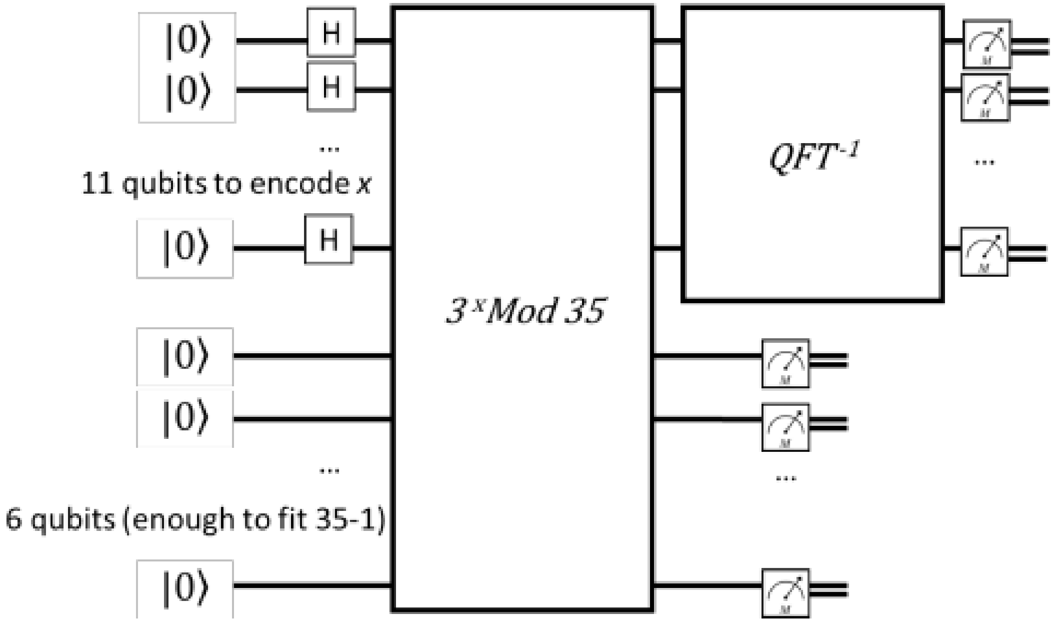
Euclidean algorithm

- p = GCD(N, ($a^{r/2}$ -1)) = GCD(35,728) = 7
- q = GCD(N, ($a^{r/2}$ +1)) = GCD(35,730) = 5

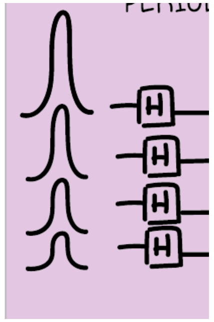
- 728-35 = 693 divisible by 7
- 693-35 = 658 divisible by 7
- …
- 63-35 = 28 divisible by 7

Quantum part

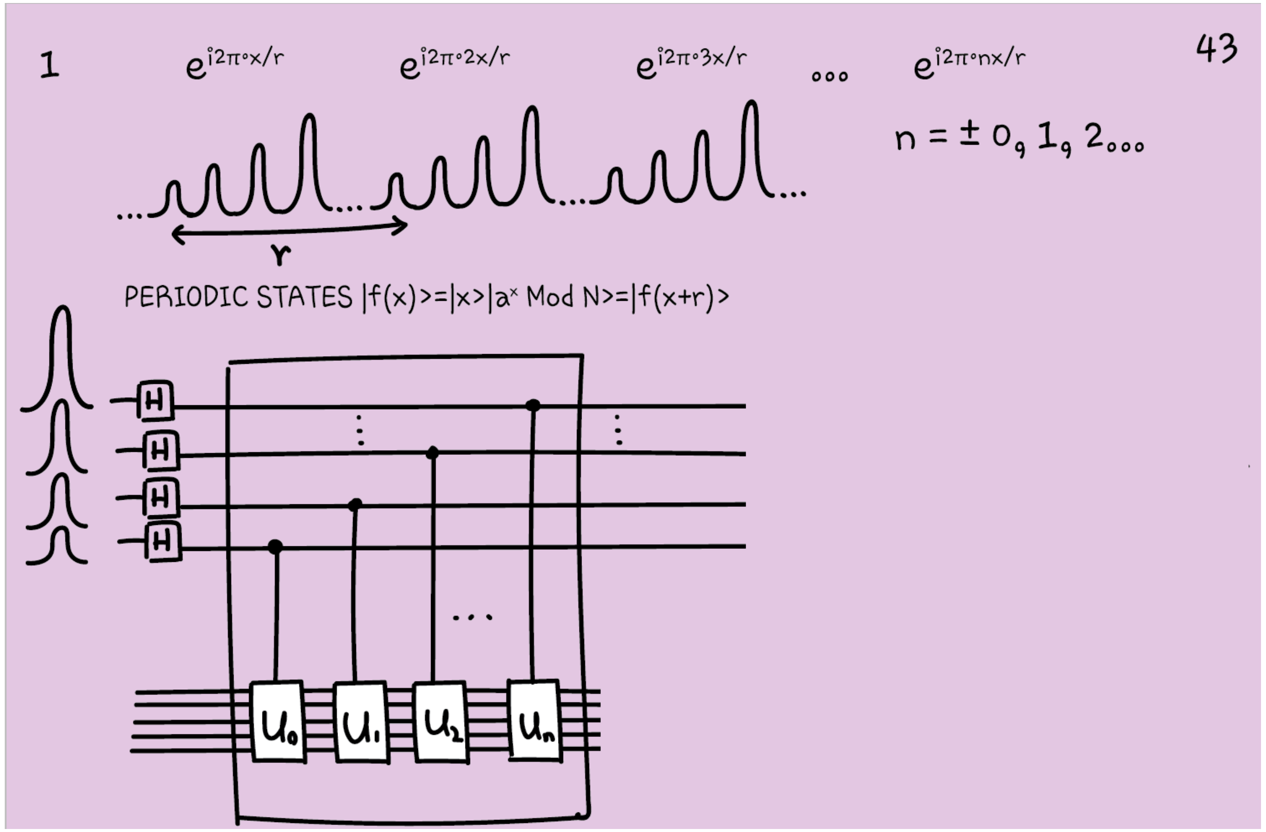
- Hard step is finding r for large N



x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17

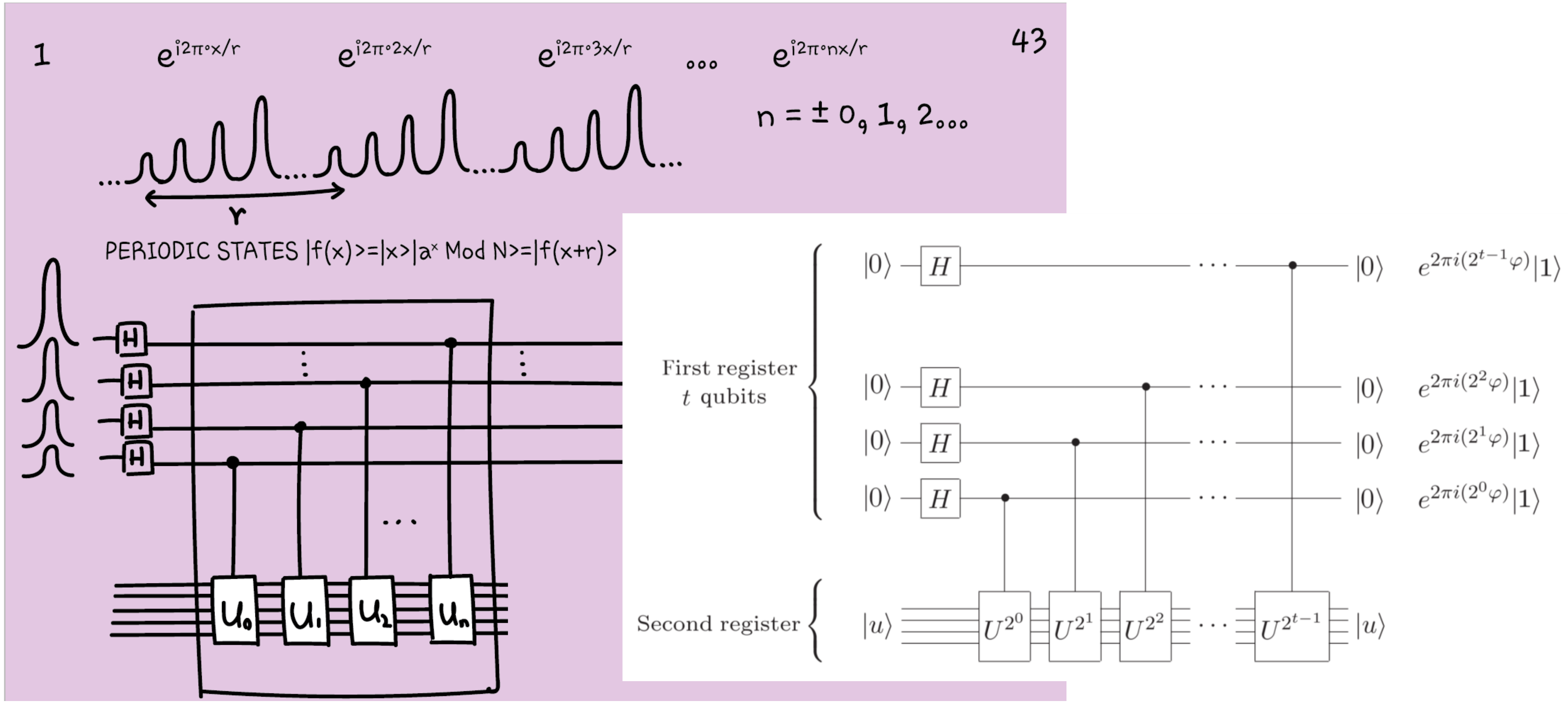


x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17



$|0\rangle|a^0\ Mod\ N\rangle + |1\rangle|a^1\ Mod\ N\rangle + \ |2\rangle|a^2\ Mod\ N\rangle \ldots\ |Q-1\rangle|a^{Q-1}\ Mod\ N\rangle$

x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17

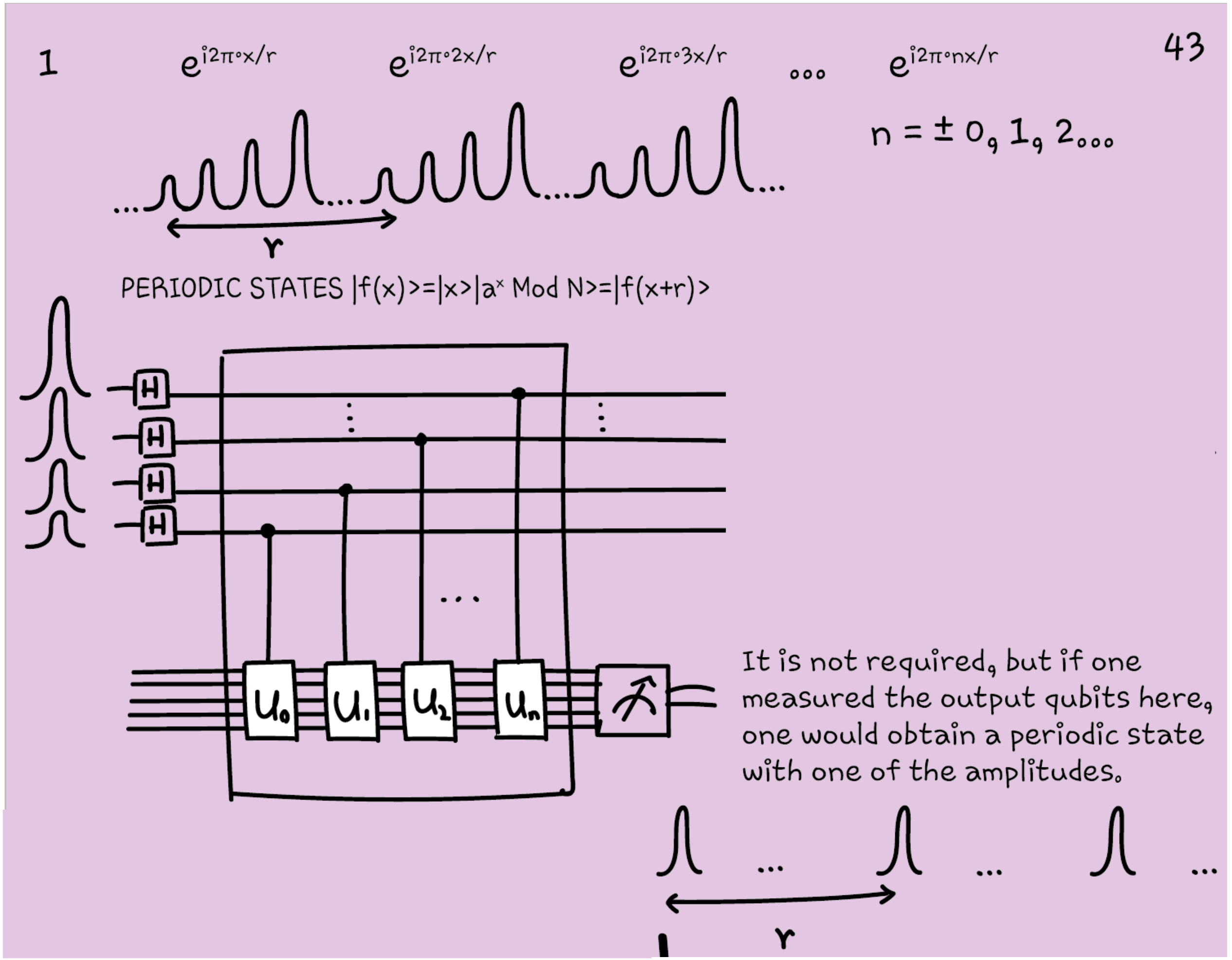


$|0\rangle|a^0\ Mod\ N\rangle + |1\rangle|a^1\ Mod\ N\rangle + |2\rangle|a^2\ Mod\ N\rangle \ldots |Q-1\rangle|a^{Q-1}\ Mod\ N\rangle$

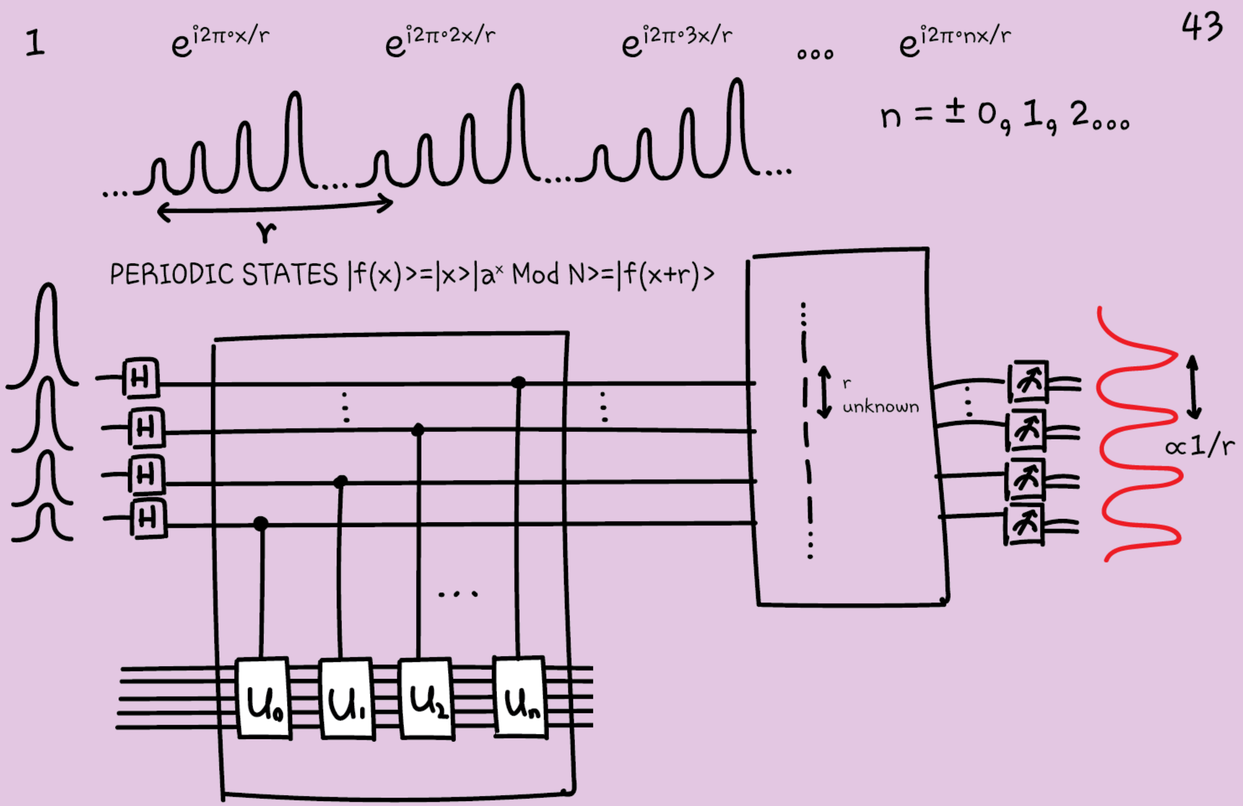
x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17

1. Quantum Computation and Quantum Information - 10th Anniversary Edition, Nielsen and Chuang
2. https://github.com/Michaelvll/myQShor

CS251 Quantum Information Science, 2018
@ ACM Honors Class, SJTU

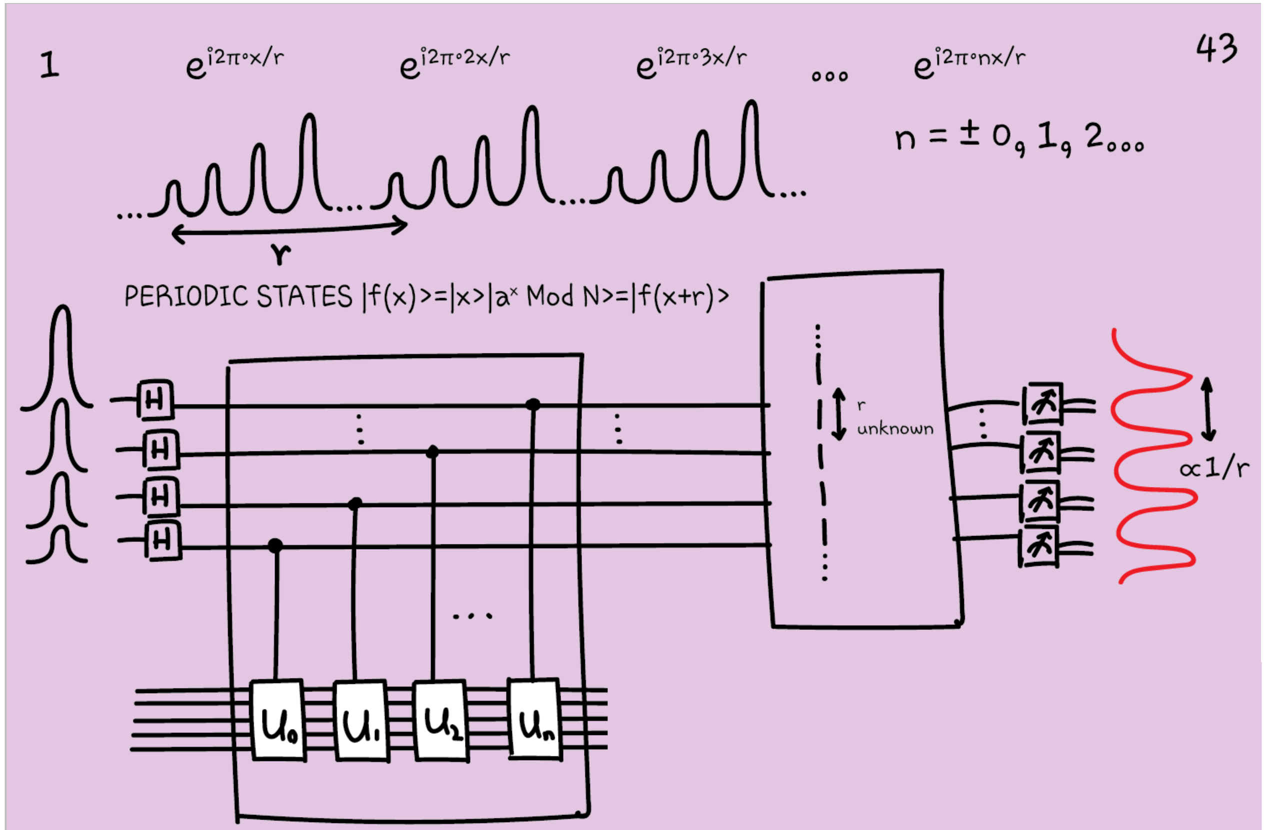


x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17



The oracle in Shor's algorithm arranges all the data into a format that can utilize the QFT.

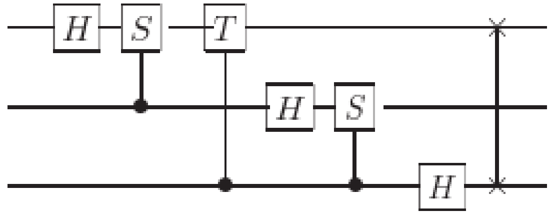
x	$3^x Mod\ 35$
0	1
1	3
2	9
3	27
4	11
5	33
6	29
7	17
8	16
9	13
10	4
11	12
12	1
13	3
14	9
15	27
16	11
17	33
18	29
19	17
20	16
21	13
22	4
23	12
24	1
25	3
26	9
.	.
.	.
.	.
2047	17



The oracle in Shor's algorithm arranges all the data into a format that can utilize the QFT.

Box 5.1: Three qubit quantum Fourier transform

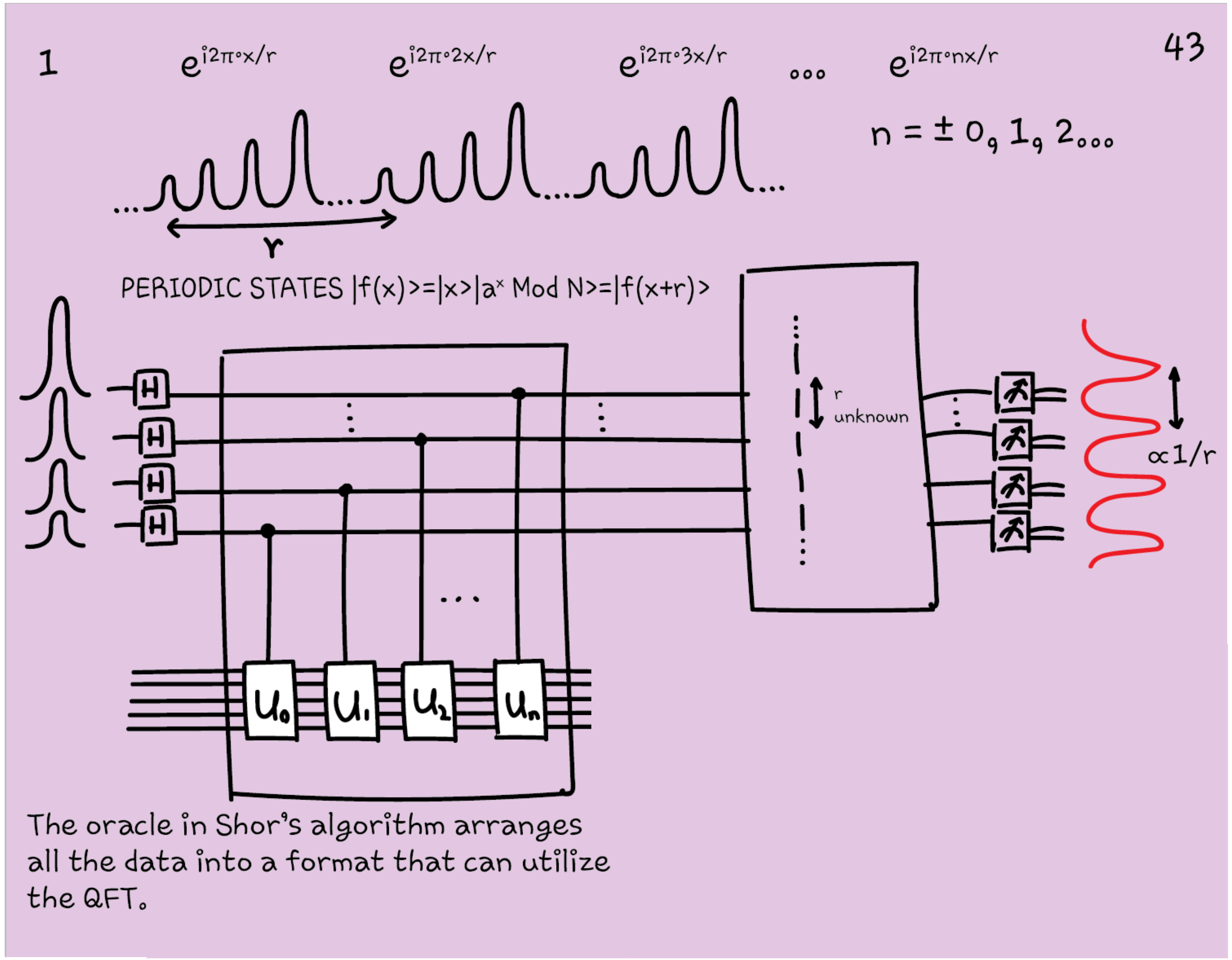
For concreteness it may help to look at the explicit circuit for the three qubit quantum Fourier transform:

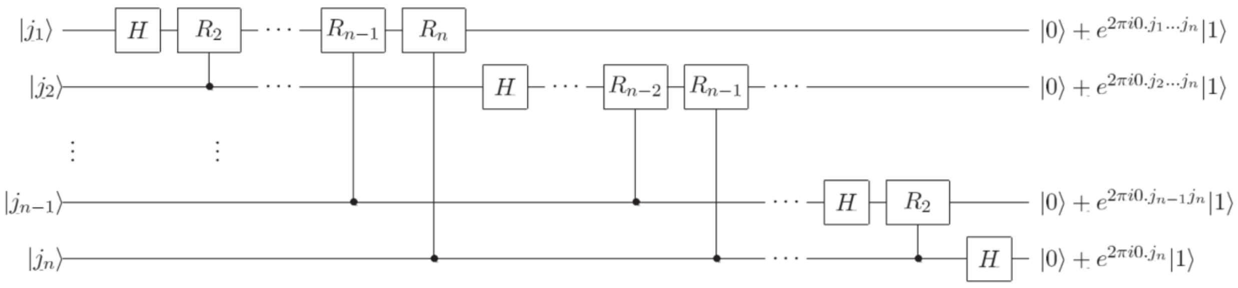


Recall that S and T are the phase and $\pi/8$ gates (see page xxiii). As a matrix the quantum Fourier transform in this instance may be written out explicitly, using $\omega = e^{2\pi i/8} = \sqrt{i}$, as

$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}. \qquad (5.19)$$

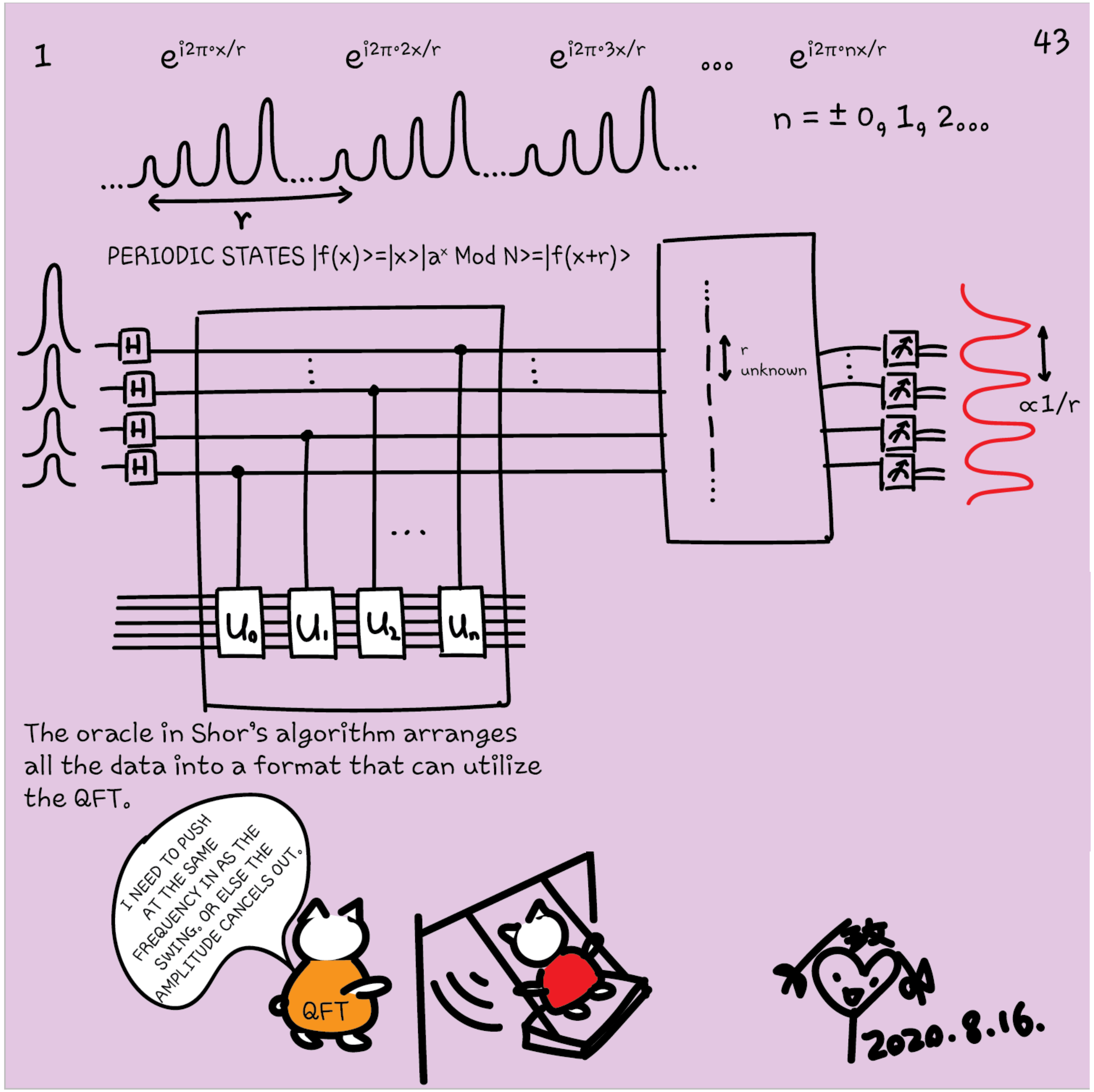
Quantum Computation and Quantum Information - 10th Anniversary Edition, Nielsen and Chuang





1.	$\|0\rangle\|0\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}\|x\rangle\|0\rangle$	create superposition
3.	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}\|x\rangle\|f(x)\rangle$	apply U
	$\approx \frac{1}{\sqrt{r2^t}}\sum_{\ell=0}^{r-1}\sum_{x=0}^{2^t-1} e^{2\pi i \ell x/r}\|x\rangle\|\hat{f}(\ell)\rangle$	
4.	$\rightarrow \frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1}\|\widetilde{\ell/r}\rangle\|\hat{f}(\ell)\rangle$	apply inverse Fourier transform to first register
5.	$\rightarrow \widetilde{\ell/r}$	measure first register
6.	$\rightarrow r$	apply continued fractions algorithm

Quantum Computation and Quantum Information - 10th Anniversary Edition, Nielsen and Chuang



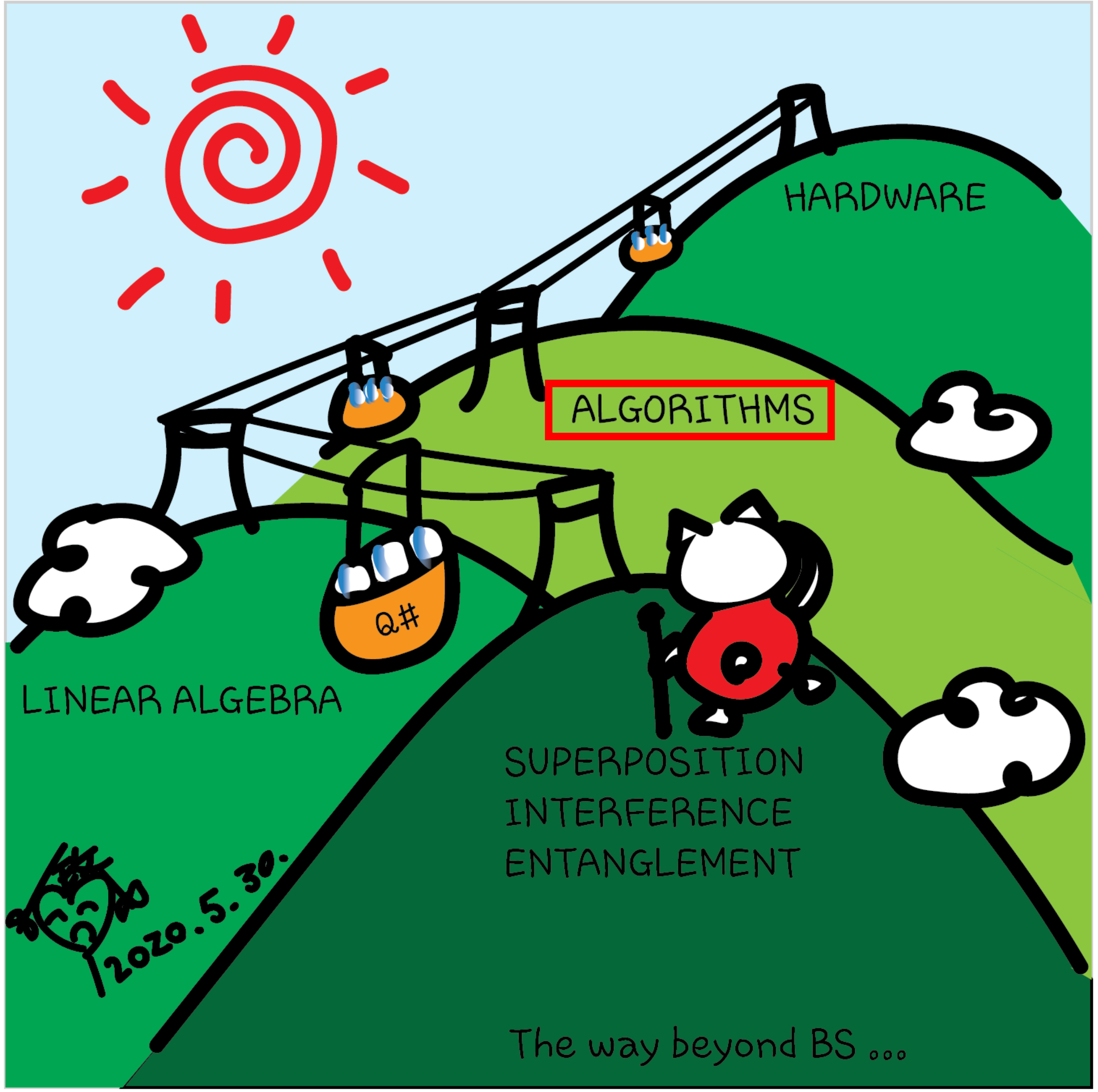
43
1
$e^{i2\pi\cdot x/r}$
$e^{i2\pi\cdot 2x/r}$
$e^{i2\pi\cdot 3x/r}$
...
$e^{i2\pi\cdot nx/r}$
$n = \pm 0, 1, 2...$
r
PERIODIC STATES |f(x)>=|x>|a^x Mod N>=|f(x+r)>
H
H
H
H
U_0
U_1
U_2
U_n
r unknown
∝1/r
The oracle in Shor's algorithm arranges all the data into a format that can utilize the QFT.
I NEED TO PUSH AT THE SAME FREQUENCY AS THE SWING, OR ELSE THE AMPLITUDE CANCELS OUT.
QFT
2020.8.16.

Q# sample

- **microsoft/Quantum**: Samples and tools to help get started with the Quantum Development Kit.
- Samples>algorithms>integer-factorization
- Numerics Library: Microsoft.Quantum.Arithmetic;
- QFT: Microsoft.Quantum.Canon

Questions

- Post in chat or on Hackaday project
  https://hackaday.io/project/168554-quantum-computing-through-comics
- FAQ: Past Recordings on Hackaday project or my YouTube https://www.youtube.com/c/DrKittyYeung
- Next Sunday: quantum career Q&A session


HARDWARE
ALGORITHMS
Q#
LINEAR ALGEBRA
SUPERPOSITION
INTERFERENCE
ENTANGLEMENT
2020.5.30.
The way beyond BS ...