Non-Local Games (11/23/2020)

Preface:

- In modern models of computation, hard to prove bounds like P not equal to NP
- Alternative model have good results, like measuring complexity via number of calls to oracle

Multi-Party Computation

- First party computes a function (like oracle), second party implements the main algorithm
    - Only communication via queries
    - Can be extended to 3+ parties (ex: 2 Merlins, 1 Arthur), or have more coordination

Non-Local Game

- Two parties (computers) work together to solve a problem
    - Each only gets a part of the input
    - Have limited coordination
- Ex: two parties, Ava and Benji, compute g(x, y)
    - Ava given x, outputs a
    - Benji given y, outputs b
    - Third party combines a and b
    - Game is won when f(a, b) = g(x, y)
        - f and g both give as input, so up to Ava and Benji to create right outputs

CHSH (Clauser Horne Shimony Holt – authors)

- x, y, a, b are binary bits
- Ava and Benji (the two parties) try to compute AND, g(x,y) = xy given f(a, b) = a XOR b
- Ava knows if their input is 0, then g(0, y) = 0
    - However, doesn't know what Benji's output, b, is, so cannot determine what to output as the f is XOR
- Can calculate probability of success on uniformly random inputs
    - "Dumb Strategy": Ava and Benji always return 0
        - Answer correct ¾ of the time
    - Classical Strategies
        - Limited outputs based on input (4 strategies per Ava/Benji):

Input	0	X	-X	1
0	0	0	1	1
1	0	1	0	1

- So, we end up with 16 combinations of categories and can calculate success
  - Can take advantage of negation property to make calculation easier

Strategy	0	1	x	-x
0	¾	¼	¾	¼
1	¼	¾	¼	¾
y	¾	¼	¼	¾
-y	¼	¾	¾	¼

- So, no random or classical strategy better than ¾ success rate

- Quantum Strategy
  - Ava/Benji would not be able to make use of quantum computers, as strategies easy to implement
  - But, 3rd party could give Ava/Benji halves of the same EPR pair
    - Still can't learn what other partner's input is, but can use it to win with higher probability
    - 3rd party will measure returned qubits to get a and b outputs
  - Strategy:
    - Each applies unitary to their part of EPR Pair
      - Ava: I if x = 0 and ZH if x = 1
        - Note, I = R_0 and ZH = $R_{\pi/4}$
      - Benji: $R_{\pi/8}$ if y = 0 and $R_{-\pi/8}$ if y = 1
        - Recall $R_\theta = \begin{matrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{matrix}$
    - Success Rate = $\frac{1}{\sqrt{2}}(cos(\phi-\theta)|00\rangle + sin(\phi-\theta)|01\rangle - sin(\phi-\theta)|10\rangle + cos(\phi-\theta)|11\rangle$

x	y	θ	ϕ	$\phi-\theta$	Success Rate
0	0	0	$\pi/8$	$\pi/8$	$\cos^2\left(\frac{\pi}{8}\right) \approx 0.854$
0	1	0	$-\pi/8$	$-\pi/8$	$\cos^2\left(\frac{-\pi}{8}\right) \approx 0.854$
1	0	$\pi/4$	$\pi/8$	$-\pi/8$	$\cos^2\left(\frac{-\pi}{8}\right) \approx 0.854$
1	1	$\pi/4$	$-\pi/8$	$-3\pi/8$	$\cos^2\left(\frac{\pi}{8}\right) \approx 0.854$

    - So, we have a better overall success rate as .854 > .75
      - Despite uniformly random outputs (Ava/Benji output 0 half the time, 1 half the time), there is correlation between their outputs
    - This is provably the optimal quantum strategy, as every strategy is applying a unitary on 2 qubits and then measuring, so can optimize over space of tensor products of 4x4 unitaries
      - Corollaries: if Ava and Benji win with 0.854 probability, then they must be using exactly this algorithm, and so their individual outputs are uniformly random. Importantly, gives us way to generate certifiably random numbers