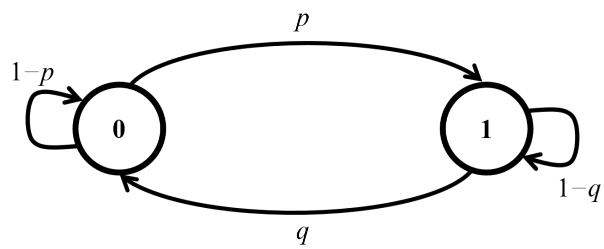
CMU 15-252 **Spring 2018**

HOMEWORK 11
DUE MAY 4TH IN CLASS

---

1. **(SOLO)** Below is a Markov chain with two states $\{0, 1\}$ and not-fully-specified transition probabilities, defined in terms of parameters $0 < p, q < 1$.



   (a) Write the transition matrix K for this chain. (The "first" row/column should correspond to state 0, the "second" row/column to state 1.)

   (b) Determine the invariant distribution π for this chain.

   (c) In this part of the problem we consider what happens when p or q can be 0 or 1.

   For the case of $p = q = 1$, the resulting chain is "periodic" (don't worry about what that formally means) and the rows of K^t do not converge to a limit as $t \to \infty$. Still, the chain does have an invariant distribution, $\pi = [\frac{1}{2}\ \frac{1}{2}]$.

   When one (or both) of p, q is 0, the resulting chain is not even strongly connected. The Fundamental Theorem does not tell us anything about this case. Nevertheless, please answer the following questions: Does the chain have an invariant distribution π satisfying $\pi = \pi K$? If so, is it unique? If so, do the rows of K^t converge to it as $t \to \infty$? (When answering these questions, distinguish the case when $p = q = 0$ from the case when only one of them is 0.)

2. **(OPEN)** True story: The laws of physics, as we know them, do not definitely rule out time-travel. True story 2: The first person to mathematically prove this (that time-travel is consistent with the laws of physics) was Kurt Gödel. Specifically, it is possible that there exist spacetime "wormholes" with the following properties: (i) the two endpoints of the wormhole have the same position in space; (ii) the two endpoints of the wormhole have different positions in time; (iii) the state of the universe at the two endpoints of the wormhole is, by definition, the same. We have never found such a wormhole, but it is *possible* that they exist. If by some amazing miracle they do exist, it's probable that their spacial extent is not very large, maybe like the size of one electron.

   For the purposes of this question, you can think of such a wormhole like a magic microwave. One endpoint is in the microwave at 9am and one endpoint in the microwave at 5pm. The microwave is just large enough to hold a single electron, and we can use this electron's spin to encode a single logical *bit*, either 0 or 1. By definition, whatever the state of the bit inside the microwave is at 9am, that's also the state of the bit inside the microwave at 5pm. It's kind of like the bit is sent back in time from 5pm to 9am.

Actually, Stephen Hawking and George Ellis once argued that time travel is *impossible*, for the following "grandfather paradox"-type reason. Suppose you operate the microwave as follows. At 9am you open it up and take out the bit b inside. Then during the day, you apply a NOT gate to b, and put it back in the microwave. Hawking and Ellis then argued as follows: Suppose that b is 0 at time 9am; then your NOT gate causes it to be 1 at time 5pm, a contradiction. On the other hand, suppose that b is 1 at time 9am; then your NOT gate causes it to be 0 at time 5pm, a contradiction. Gödel would love this argument.

Not so fast, said David Deutsch (founder of quantum computation). The laws of physics are actually probabilistic, so there's no reason to assume that the state of b is deterministic. And indeed, suppose the "state of b at time 9am" is "probability $\frac{1}{2}$ of being 0, probability $\frac{1}{2}$ of being 1". Then after you apply the NOT gate during the day, the resulting state of b at time 5pm will be "probability $\frac{1}{2}$ of being 0, probability $\frac{1}{2}$ of being 1". Same as at 9am, no contradiction.

David Deutsch proposed the following model of how this magic microwave could not only be possible, it could be useful computationally! In Deutsch's model, instead of just a single NOT gate, you can have *any randomized* polynomial-time algorithm A. This algorithm should have two inputs: a "real" n-bit input string x, and a single "time-traveling input bit" b_0. Furthermore, A should have two separate outputs: ACCEPT/REJECT, plus a "time-traveling output bit" b_1. The model is now as follows: The algorithm gets a real input x (from the user) and gets the time-traveling input bit b_0 out of the microwave at 9am. Then it runs for a day (polynomial-time), puts b_1 back in the microwave at 5pm, and at the same time ACCEPTS/REJECTS. Note that the microwave can only be used once.

Notice that if you *fix* an input string x, the behavior of algorithm A is *like a 2-state Markov chain* with respect to the time-traveling bit. I.e., it's just like the above problem for some values p and q (that depend on x and A). Let us call that resulting Markov chain A_x. Now Deutsch's model is that once you decide you'll use algorithm A during the day, the universe automagically sets the (probabilistic) state of b_0 (and hence b_1) to be the[1] invariant distribution π_x of A_x.

Basically, the situation is the following: Once you define the randomized algorithm A, it implicitly defines a 2-state Markov chain for each possible real input x; then when the algorithm runs on x, it also gets access to one bit b_0 drawn from the invariant distribution π_x.

Finally the problem: In this model, show that there is a Monte Carlo randomized polynomial-time algorithm A solving SAT (with error probability $\leq 1\%$)! (Tip: Reread the problem statement multiple times. It has many hints along the way.)

(Note: In fact, it turns out that in the above model, one can efficiently solve all problems in PSPACE, which if you recall, contains the whole polynomial hierarchy, and probably much more.)

[1] Actually, to be very careful, we should say "some" rather than "the", for reasons you'll understand when you do the $p = q = 0$ case of Question 1.