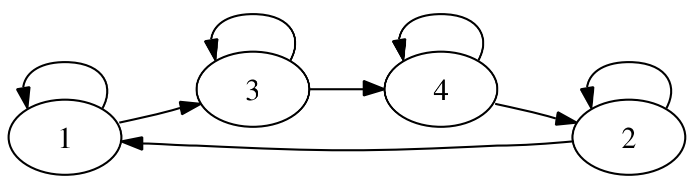
Midterm 1 review problems, part 2

(try to solve before coming to the review session, 03/02 5-7pm, 306 Soda)

7. Let $K_{m,n}$ be a *complete* (m,n) *bipartite graph* – a graph which has two groups of nodes, one with m nodes, the other with n nodes, with each of the former connected to each of the latter, and no edges between nodes in the same group. You can think about the nodes of $K_{m,n}$ as a group of (heterosexual) men and women, and each edge corresponding to a possible couple. For what value of m and n is there an Eulerian path in $K_{m,n}$?

8. Let p be a prime. The "Cayley graph of $\mathbb{Z}_p$ with respect to some set S of numbers between 1 and $p-1$" is a directed graph defined as follows: the vertices are the non-zero elements of $\mathbb{Z}_p$ (numbers from 1 to $p-1$); an edge (a,b) is in the graph if there is some $c \in S$ such that $b \equiv ac \pmod{p}$.

   For example, the Cayley graph of Z_5 with respect to the set $\{1,3\}$ is the following graph:



   (a) For which sets S does the Caykey graph with respect to $\mathbb{Z}_p$ have an Eulerian tour?

   (b) What about a variation on the Cayley graph which also has 0 as a node (and S may include 0)?

9. We want to prove that if the undirected graph $G = (V,E)$ is connected, then $|E| \geq |V| - 1$.

   (a) What false implication is assumed in with the following proof by induction on $|V|$?:
   Base: If there's one vertex, $|V| - 1 = 0$, so of course G can't have less than zero edges.
   Inductive step: Suppose all connected graphs with $n-1$ vertices have at least $n-2$ edges. For any connected graph G with $n-1$ vertices, add a new vertex v and connect it to any subset of the vertices of G to form G'. If v doesn't connected to any vertex, there'll be no paths to v, so G' will not be connected. If at least one edge is introduced, G' will have at least $n-2+1 = n-1$ edges.

   (b) Give a correct proof of the above statement. *Hint*: Fix the number of vertices, and use induction on the number of edges. You'll find it useful to think about "connected components". A *connected component* of an undirected graph is a subset of the vertices $V' \subseteq V$ such that there's a path from any $u \in V'$ to any $v \in V'$, and no path from from $u \in V'$ to any $w \in V \backslash V'$ (the set of vertices outside V').

10. **Stable marriage**

   (a) Consider the following situation. After we find the pairing using the male-optimal algorithm we described in class, one of the men m, who got paired up with some woman w, becomes more fond of w, that is, he changes his preference by moving w higher up in his list. Is the pairing is still boy-optimal?

   (b) Consider an instance of the stable matching problem in which there exists a man m and a woman w such that m is ranked first on the prefrence list of w and w is ranked first on the prefrence list of m. Does every stable matching S for this instance have to contain the pair (m,w)?

(c) In a large group of n men and n women, Bob, one of the men, gets tipped off that he's the second-highest preference on every woman's list. Bob is pretty happy to hear this. Assuming the traditional (male-optimal) algorithm, might Bob be in for a disappointment? In particular, is it possible that he will end up with the woman he prefers the least of all?

11. **Linear systems**
Solve in $\mathbb{Z}_{11}$:

(a) $\begin{cases} 5a + 6b = 0 \\ 7a + 2b = 2 \end{cases}$

(b) $\begin{cases} 3a + 2b = 7 \\ 4a + 10b = 1 \end{cases}$

12. **Root access sold separately**
While we've shown at class that a degree-d polynomial over $GF(p)$ has *at most* d roots, we didn't claim there are always d roots. Show that, for all primes p, there's a non-constant polynomial over $GF(p)$ which has no roots. Given a p, what is the lowest degree d such that there exists a zero-less polynomial of degree d?

13. **Polynomial interpolation busywork**

(a) Find a 2nd-degree polynomial over $\mathbb{Z}_7$ that goes through $(1, 3)$,$(2, 3)$, and $(3, 1)$.

(b) What if we change the third point to $(3, 3)$?

(c) What if we instead change the second point to $(2, 2)$?

14. **Secret-sharing**
Suppose you want to share a secret number ($s = 6$), there are $n = 3$ people, and we want any 2 of them to be able to discover the secret.

(a) Pick some appropriate prime q and polynomial P over $GF(q)$.

(b) Find the 3 values to hand out to the three people.

(c) Check that person 1 and person 2 can discover s.

15. **Secret-sharing, Stanford-style**
A Stanford student asks, "Why bother with this whole polynomial mes for secret sharing? For the problem above, why don't you just write your secret as a 3-digit binary number (110), tell everyone that the secret is some binary number between 000 (0) and 111 (7), and then give bits 1&2 to person 1, bits 1&3 to person 2, and bits 2&3 to person 3? That way, none of them will know the code without talking to at least one other person." Why is this approach worse?

16. **Article I and Secret Sharing**
In the year 2150 AD, the US Constitution is still, remarkably, intact, though, with the rainforests gone, all legal-documents have been digitized and stored on a fileserver buried under Washington, DC. Thus, any legislation is just a matter of logging into the fileserver and updating `US-laws.txt`. Of course, there's the little matter of access control.

Recall that, per Article I, Section 7, of the Constitution, in order for legislation to be passed into law, it must be approved either (i) by the majority of the Senate, the majority of the House, and the President; or, if the President vetoes it, by (ii) 2/3rds of the Senate and 2/3rds of the House.

Conveniently enough, the country has been reorganized into just 3 states — Jesusland, the United States of Canada, and The People's Republic of Berkeley, so there are only 6 senators in the Senate and 12 congressmen in the House.

Design a secret-sharing scheme that distributes the write-access password to `US-laws.txt` between the 18 legislators and the president in such a way that the file can only be modified by (i) the president, at least 3 senators, and at least 6 congressmen, or (ii) at least 4 senators and at least 8 congressmen.

17. **Error correction**
    How can we encode a 11-byte message to protect against up to 3 errors in unknown positions?

18. **Error detection**
    An error *detection* code detects that errors were introduced somewhere into the message but can't necessarily pinpoint and correct them.

    (a) Naturally, a Berlekamp-Welsch error correction code that transmits n packets and can correct up to k errors can also detect it when k errors happenned (why?). What's the highest number of errors that can happen using this code so that the receiver will still definitely be able to detect that some error occured?

    (b) What about an erasure code that corrects up to k erasures in a message of n packets?