12 / 7 / 20

Victoria Liu

Ma 6 Final.

Problem 1 (Page 1)

Proof:

Since p is prime, it will be relatively prime for every element a in $\{2, 3, \dots, p-2\}$, and the $GCD(p, a) = 1$. By theorem from lecture 2, $\exists\ s, b \in \mathbb{Z}$ such that

$$s \cdot p + ab = GCD(p, a) = 1.$$

In other words, for every a in $\{2, 3, \dots, p-2\}$:

$$ab \equiv 1 \pmod p$$

Now, we show that the pairs $\{a, b\}$ are distinct. from each other and that there are no "repeat" elements across the pairs.

By Latin Square property of mod multiplication, there is a unique $b \pmod p$ such that $ab \equiv 1 \pmod p$, so a given "a" will only be paired with one "b," modulo p.

We also know that $a \neq b$. We can prove this via contradiction. Suppose that $a \equiv b \pmod p$, so that:

$$a \cdot a \overset{?}{\equiv} 1 \pmod p.$$

$$a^2 - 1 \overset{?}{\equiv} 0 \pmod p$$

$$(a-1)(a+1) \overset{?}{\equiv} 0 \pmod p.$$

Victoria Li 12/7/20

Ma 6 Final

Problem 2 (Page 2)

This suggests that $p \mid a-1$ or $p \mid a+1$. However, this is impossible for the set $\{2, 3, \ldots, p-2\}$. The only solutions (mod p) are $1 \pmod p$ and $(p-1) \pmod p$. Hence, $a \not\equiv b \pmod p$.

Now, for every $a \in \{2, 3, \ldots, p-2\}$, we can find one "b" such that $ab \equiv 1 \pmod p$. However, this method "double counts" every "a" and "b" b/c each "b" will also be counted as an "a." This is an easy fix — if a number has been found as a "b" for a previous number "a," we just don't add it to a partition again, since it would already be in a partition. Now, we've successfully partitioned $\{2, 3, \ldots, p-2\}$ into pairs $\{a, b\}$ of distinct elements. ■

Proof:
Note that this partition creates an equal partition between "a" and "b" b/c the Latin Square property creates a bijection from every "a" to a "b." As an additional sanity check, the set $\{2, 3, \ldots, p-2\}$ also has an even number of elements, for odd primes.

Now, this means that $\frac{(p-2)!}{1} \equiv 1 \pmod p$ because the partition will create $\frac{p-3}{2}$ pairs that multiply to be equivalent to $1 \pmod p$.

12 / 7

Victoria Liu

Ma 6 Final

Problem 1 (Page 3)

Now, we have:

$(p-1)\cdot(p-2)! \equiv (p-1)(1) \pmod{p}$

$(p-1)! \equiv -1 \pmod{p}$

No, this is not true if p is composite. For example, take $p=8$.

$(p-1)! \overset{?}{\equiv} -1 \pmod{8}$

$7\cdot 6\cdot 5\cdot \underline{4}\cdot 3\cdot \underline{2}\cdot 1 \overset{?}{\equiv} -1 \pmod{8}$

$0 \not\equiv -1 \pmod{8}$

4×2 makes LHS divisible by 8.

The $\{a\ b\}$ partition is also impossible to have distinct elements b/c we would have 5 elements, an odd number, to partition.

12 / 7 / 20

Victoria Liu

Ma 6 Final

Problem 2.

Use definition for positive integers for combinations: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$

$$\binom{n}{k}\binom{k}{l} \overset{?}{=} \binom{n}{l}\binom{n-l}{k-l}$$

$$\left[\frac{n!}{\cancel{k!}(n-k)!}\right]\left[\frac{\cancel{k!}}{l!(k-l)!}\right] \overset{?}{=} \left[\frac{n!}{l!\cancel{(n-l)!}}\right]\left[\frac{\cancel{(n-l)}!}{(n\cancel{-l}-k\cancel{+l})!(k-l)!}\right]$$

$\Downarrow$ cancelling ..

$$\frac{n!}{(n-k)!l!(k-l)!} \overset{?}{=} \frac{n!}{l!(n-k)!(k-l)!}$$

$\Downarrow$ Rearrange

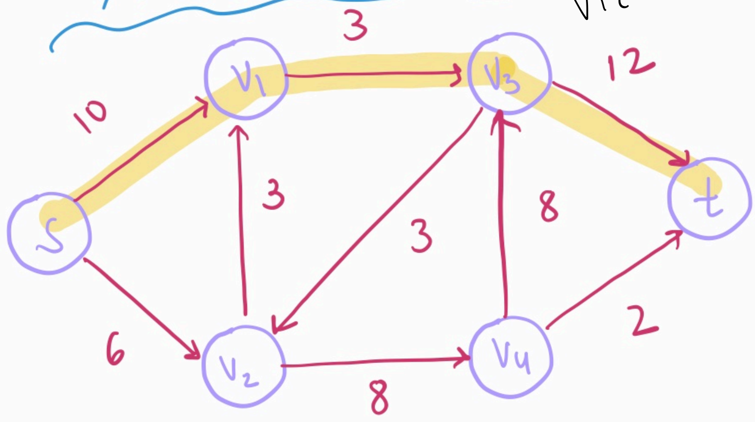
$$\frac{n!}{(n-k)!l!(k-l)!} \overset{\checkmark}{=} \frac{n!}{(n-k)!l!(k-l)!}$$

$\blacksquare$

Residual Network:

Problem 3
Victoria Liu

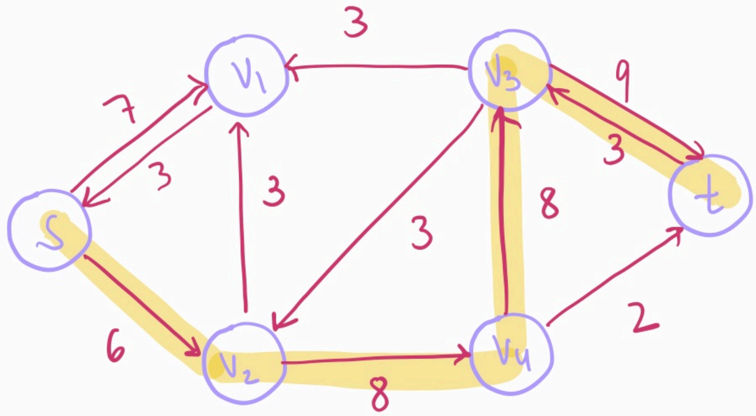
Flow:



Initially, $|f| = 0$

In the path we've chosen,

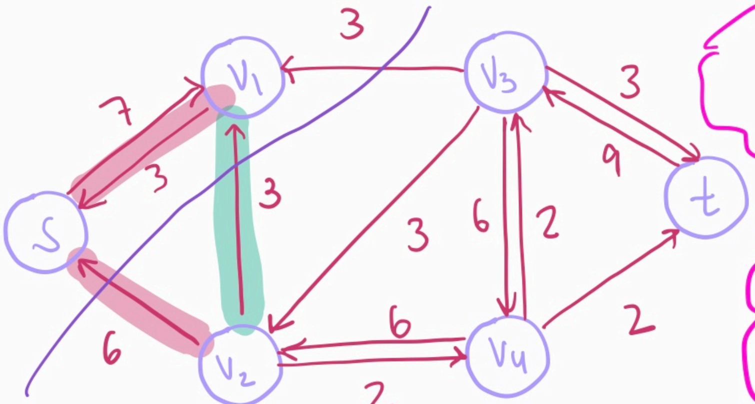
$$d = \min_{e \in P} c(e) = 3$$



Now, $|f| = 3$

In the path we've chosen,

$$d = \min_{e \in P} c(e) = 6$$



$|f| = 9$

There are no more s-t paths, so the maximum flow is 9.

min. cut.

Let $S = \{s, v_1\}$ and $T = \{t, v_2, v_3, v_4\}$

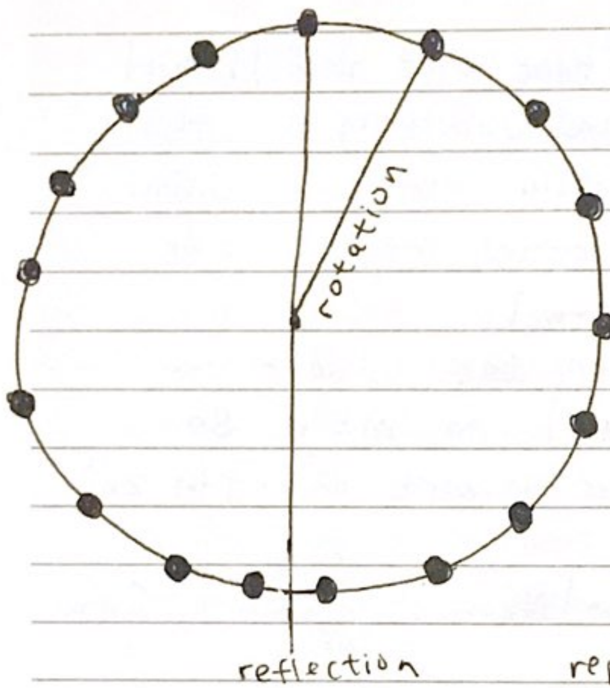
Interestingly, our max flow is less than the min. cut, which is 12. However, even when the min. cut splits our nodes into S and T, our residual diagram still satisfies that 1) all edges (u,v) where $u \in S$ and $v \in T$ are saturated; and 2) all edges (v,u), where $v \in T$ and $u \in S$ have no flow. Thus, I'm comfortable w/ a max. flow of 9. Incidentaley, we can think of the edge in green as being "wrongly oriented"

12 / 7 /20

Victoria Lin

Ma 6 Final

Problem 4 (four):



Important formula:

$$\#\text{ orbits} = \frac{1}{|G|}\sum_{g\in G} F(g)$$

where

$$F(g) = \left|\{x \in X \mid g(x) = x\}\right|$$

In other words, find F(g) for each permutation. We draw / represent the necklace as a 17-gon that is regular.

We use Lecture 21 for inspiration:

Total configurations: $\binom{17}{4} = 2380$

Symmetry:	F(g)
Identity	2380
16 Rotations by $\frac{2\pi i}{17}$, $1 \le i \le 16$	0
17 reflections across lines that go between center & a bead	$17 \times \underbrace{\binom{8}{2}}$

$\binom{8}{2}$ since the beads need to be symmetric wrt. reflection axis.

Taken all together.

$|G| = 34$

$$\#\text{ orbits} = \frac{1}{|34|}(2380 + 476)$$

$\#$ orbits $= 84$

84 unique necklaces

12/7/20

Victoria Liu

Ma 6 Final

Problem 5 (five): (Page 1)

The starting letter always has to be X, and the ending letter always has to be Y. Let's write out the actual 2n-length "words" to see if we can detect a pattern. We set $C_0 = 1$, in the spirit of matching the definition of Catalan numbers.

Catalan: Words:

$C_0 = 1$ } W_0

$C_1 = 1$ XY } W_1

$C_2 = 2$ XXYY XYXY } W_2

$C_3 = 5$ XYXXYY XYXYXY
XXYYXY
XXXYYY XXYXYY } W_3

$C_4 = 14$ XYXYXXYY XYXYXYXY
XYXXYYXY XYXXXYYY
XYXXYXYY

XXYYXYXY XXYYXXYY

XXXYYYXY XXYXYYXY

XXYXXYYY XXYXYXYY
XXXYYXYY XXXXYYYY
XXXYXYYY } W_4

etc...

12/7/20

victoriaLiu

Ma6 Final

Problem 5: (Page 2)

Let W_n be the set of $2n$-length words containing n X's & n Y's such that no initial substring contains more Y's than X's. As shown in the diagram, $C_1 = |W_1|$, $C_2 = |W_2|$, and so on.

Like the triangulation definition of catalan numbers, we partition our words into two substrings that can be related to previous (Catalan) numbers. Scanning each word from left to right, we place our divider, which looks like ⦚, after the first substring that is an element of W_m, where $m \leq n$, and $2n$ is the length of the entire word.

For example, take:

$$\underbrace{\underbrace{XXYY}_{\text{element of } W_2} ⦚ \underbrace{XYXY}_{\text{element of } W_2}}_{\text{element of } W_4}$$

$m = 2$

$n = 4$

$2n = 8$

Note that because the initial substring is a member of W_m, the remaining substring must have equal amounts of X & Y, begin w/ X, and end in Y. This means the second substring is a member of W_{n-m}.

Victoria Liu

12/7/20

Ma 6 Final

Problem 5 (page 3)

We know there will be $|W_{n-m}|$ different substring options for the second substring. However, there aren't $|W_m|$ different options for the first substring. For example, going back to C_4, if our divider is placed after 4 characters (i.e. the initial substring $\in W_2$), we actually only have 2 possibilities, rather than 5. This is because if we included all 5, we would be double-counting from words we've already seen, when the partition was placed earlier. For example,

XYXY | XYXY

doesn't work, because it would've been tabulated as:

XY | XYXYXY.

Instead of having $|W_m|$ different options for the first substring, we only have $|W_{m-1}|$. We can justify this b/c the first letter always has to be X and the last letter Y, so we're really only concerned with the $2m-2$ letters in between ?????? Sorry, this is prob. not rigorous at all, but ran out of time before I could think thru this part!

12 / 7 / 20

Victoria Liu

Math Final

Problem 5: (Page 4)

Anyway, if we can accept that there are $|W_{m-1}|$ possibilities for the initial substring (i.e. the part before our divider), then given the divider is present after $2m$ letters, there would be:

$$|W_{m-1}| \times |W_{n-m}|$$

combinations. As we've seen, the divider can take on values from $m=1$ to $m=n$. So we sum to get: (btw, this is for words of length $2n$):

$$C_n = \sum_{m=1}^{n} |W_{m-1}| \times |W_{n-m}| = \sum_{m=1}^{n} C_{m-1} \times C_{n-m}$$

The definition of Catalan numbers from lecture was:

$$C_{n-2} = \sum_{i=0}^{n-3} c_i \, c_{n-3-i}$$

Adjusting our bounds, we get:

$$C_n = \sum_{m=0}^{n-1} C_m C_{n-m-1}$$

Adjusting our indices, we get:

$$C_{n-2} = \sum_{m=0}^{n-3} C_m C_{n-2-m-1} = \sum_{m=0}^{n-3} C_m C_{n-3-m}$$

The same recurrence relation as the Catalan numbers!