Circuits + Cryptomorphism

Last time: A matroid is a pair $M = (E, \mathcal{I})$, where
where

- E is a finite set
- $\mathcal{I} \subseteq 2^E$ satisfies

 (I1) $\emptyset \in \mathcal{I}$.

 (I2) If $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$.

[Augmentation] (I3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then thee exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

There are several equivalent-but-not-obviously-equivalent ("cryptomorphic") ways to define a matroid.

Exercise 3 Last time:

Thm: A collection $\mathcal{B} \subseteq 2^E$ is the set of bases of a matroid on E if and only if $\mathcal{B}$ satisfies

 (B1) $\mathcal{B} \neq \emptyset$.

[Exchange] (B2) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then there exists $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Def: A minimal dependent set of a matroid M is a **circuit**. The set of all circuits is denoted $\mathcal{C}(M)$.

$C \in \mathcal{C}(M) \iff C \notin \mathcal{I}(M)$ but every proper subset of C is in $\mathcal{I}(M)$.

Thm: Let E be a finite set. A collection of subsets $\mathcal{C} \subseteq 2^E$ is the set of circuits of a matroid on E if and only if $\mathcal{C}$ satisfies

(C1) $\emptyset \notin \mathcal{C}$

(C2) If $C_1, C_2 \in \mathcal{C}$ with $C_1 \subseteq C_2$, then $C_1 = C_2$.

[Elimination] (C3) If $C_1, C_2 \in \mathcal{C}$ are distinct and $e \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ with

$$C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$$

Proof: ($\Rightarrow$) Let $M = (E, \mathcal{I})$ be a matroid and $\mathcal{C} = \mathcal{C}(M)$ its set of circuits.

(C1): Circuits are dependent and $\emptyset \in \mathcal{I}$ by (I1). So $\emptyset \notin \mathcal{C}$.

(C2): By minimality, every proper subset of a circuit is independent, so cannot be a circuit.

(C3): Let $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$, $e \in C_1 \cap C_2$.

<u>Want</u>: $(C_1 \cup C_2) \setminus e$ is dependent.

Suppose it's independent.

Since $C_1 \neq C_2$, $C_1 \cap C_2$ is independent also.

By (I3), we may repeatedly augment $C_1 \cap C_2$ by $(C_1 \cup C_2) \setminus e$ until we get

$$C_1 \cap C_2 \subseteq I \subseteq (C_1 \cup C_2)$$

where $I \in \mathcal{I}(M)$

$$|I| = |(C_1 \cup C_2) \setminus e| = |C_1 \cup C_2| - 1.$$

So $I = (C_1 \cup C_2) \setminus f$ for some $f \in C_1 \cup C_2$.

But $f \notin C_1 \cap C_2$, so either

- $f \in C_1 \setminus C_2 \Rightarrow C_2 \subseteq I$
- $f \in C_2 \setminus C_1 \Rightarrow C_1 \subseteq I$

This contradicts the independence of I.

Conclude $(C_1 \cup C_2) \setminus e$ is dependent, so it contains a circuit.

✓