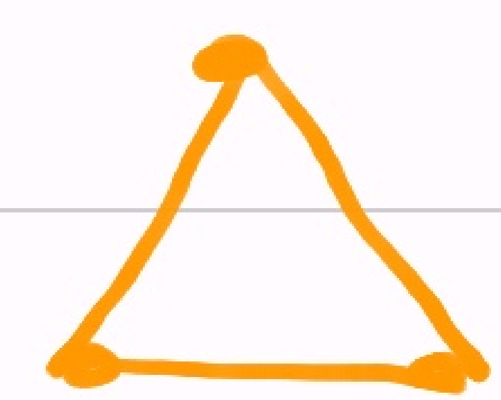
Probabilistic Methods

- Prob. can be used to prove the existence of important mathematical objects; whose definition had nothing to do with probability!

1) Ramsey number (or Graph coloring)

- Let K_n := complete, undirected graph on n vertices.

e.g. K_3 = 

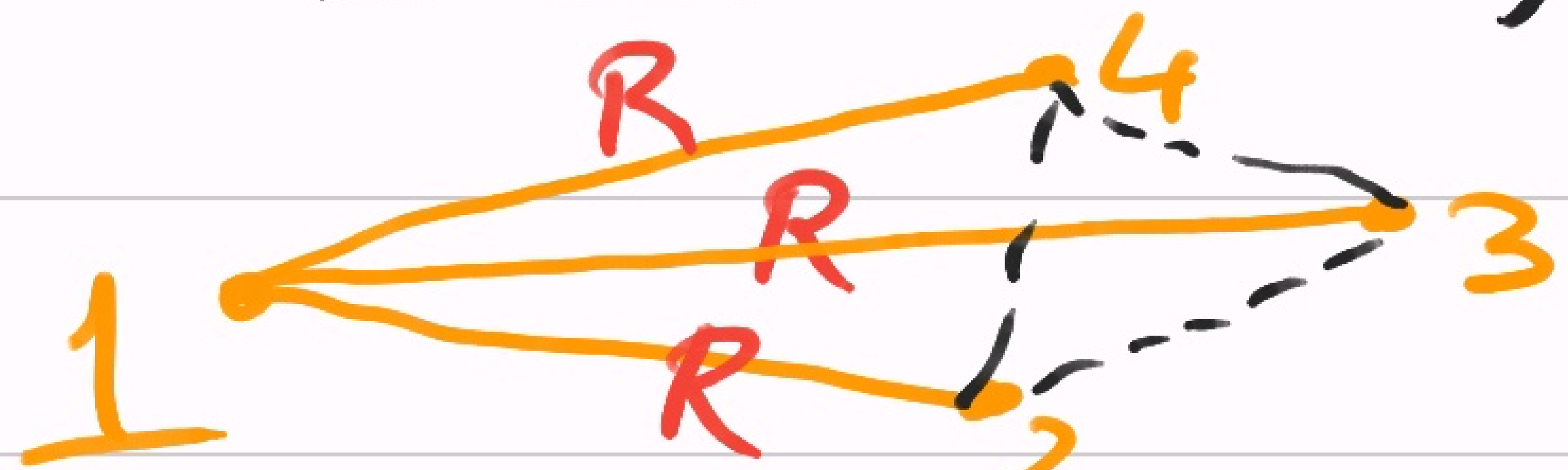
K_1 = • K_2 = 

- Suppose we color the edges of a given K_n by R(ed) & B(lue).

↳ Interesting facts about monochromatic complete subgraphs could be shown:

- Exercise: Color K_6. There is either a Red Triangle (K_3) or a Blue Triangle (K_3)!

[Hint:



$\Rightarrow$ either R Δ or B Δ exists!]

- We want K_n to have either a Red K_k, or a Blue K_ℓ ; for any coloring.

- Defn: Smallest such n is called Ramsey number $R(k,\ell)$.

- Qn: Does $R(k,\ell)$ exist? How large?

  ▷ $R(3,3) \le 6$. $= 6$.

- Let's study $n := R(k,k)$ first.

Analyse:

- Randomly color the edges in $K_n =: G = (V, E)$.
- Let's estimate $P(G \text{ has monochromatic } K_k) = ?$

▷ $\forall S \in \binom{V}{k}$, $P(S \text{ is monochromatic}) = 2/2^{\binom{k}{2}}$.

$\Rightarrow$ (by union bound) $P(\exists S \text{ monochromatic}) \leq \binom{n}{k} \cdot 2^{1-\binom{k}{2}}$.

$\Rightarrow$ If RHS < 1, then $\exists$ bad coloring (s.t. G has no monochromatic K_k).

▷ In particular, $n := \lceil 2^{\frac{k-1}{2}} \rceil \Rightarrow \binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$

$\Rightarrow K_n$ has a coloring to avoid K_k.

▷ $R(k,k) > \lceil 2^{\frac{k-1}{2}} \rceil$. ⇝ exponential-growth

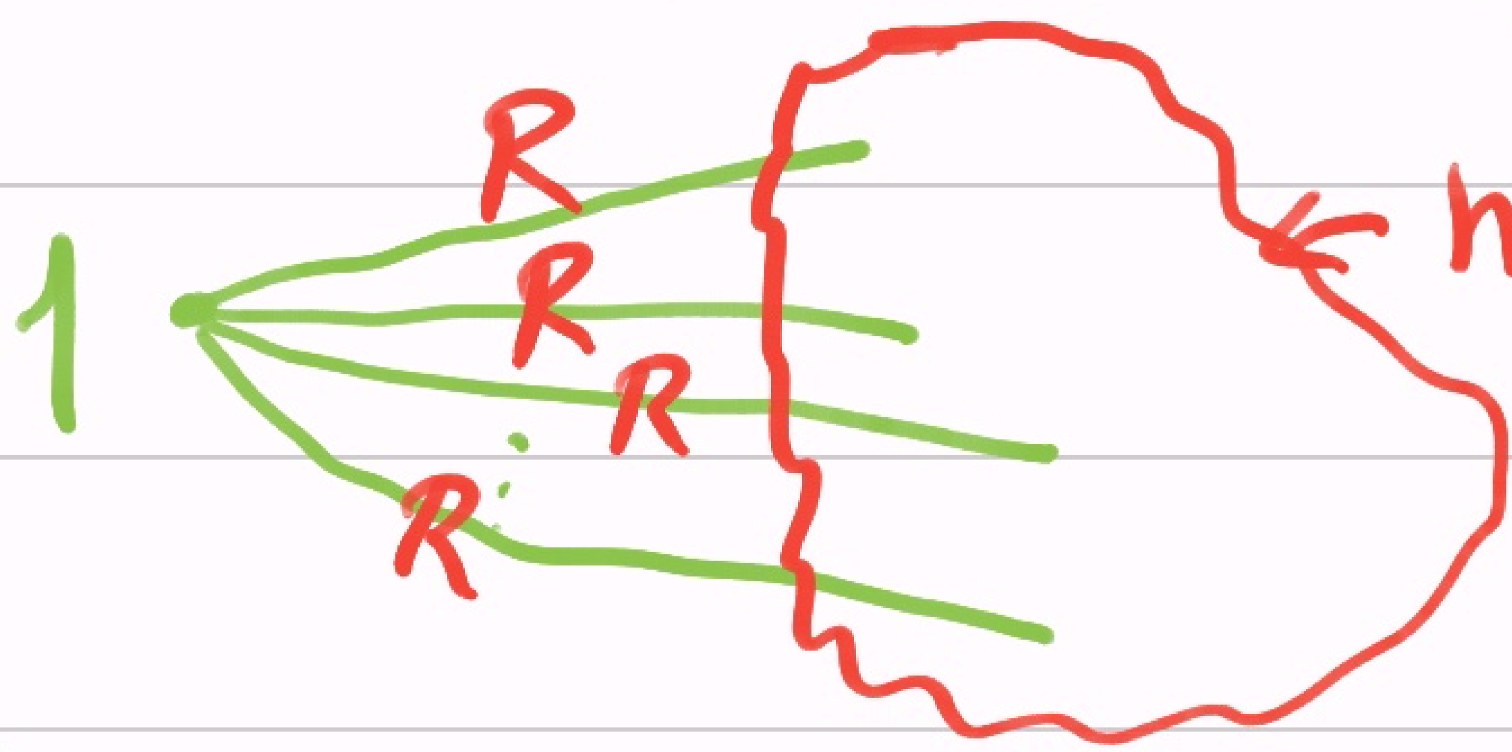
- In fact, this a randomized algo. to find bad colorings if $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} \ll 1$. ⇝ time = poly(n).

[# colorings $= 2^{|E|} = 2^{\binom{n}{2}} \approx 2^{n^2/2}$.]

Exercise: $R(k,\ell) \le \binom{k+\ell-2}{k-1}$.

$R(k,\ell) \geq R(k-1,\ell) + R(k,\ell-1)$

[Hint:



neighbor(1) =: G'

▷ If $|V(G')| \geq R(k-1,\ell)$, then G' has K_{k-1}-RED or K_ℓ-Blue]

Use induction!

Theorem 1: $\lceil 2^{\frac{k-1}{2}} \rceil < R(k,k) \le \binom{2k-2}{k-1} \approx 2^{k-1}$.

2) Large Cut in a graph

- Let $G=(V,E)$ be an undirected graph. For $A \subseteq V$, define $\text{cut}(A) := \{(u,v) \in E \mid (u \in A, v \in \bar{A}) \vee (u \in \bar{A}, v \in A)\}$

  undirected subgraph of G.

- Qn: How large is $\text{cut}(A)$, as A varies?
- Max. Cut is an important CS problem.

  ↳ $\#(A \subseteq V) = 2^n$; so exp. many!

- Let's try a heuristic: (rnd. A ?)

Algo: 0) $A \leftarrow \phi$;

1) For each $v \in V$ {

2) Add v in A with probability $= 1/2$;

}

3) Return $cut(A)$;

Analyse: $X := |cut(A)|$. For $e \in E$, $X_e := \begin{cases} 1, & \text{if } e \in cut(A) \\ 0, & \text{else.} \end{cases}$

▷ $X = \sum_{e \in E} X_e$.

▷ $E[X] = \sum_e E[X_e] = \sum_e P(e \in cut(A)) = \sum_e 2 \times \frac{1}{2} \cdot \frac{1}{2}$

$= |E|/2$.

Theorem 2: Given $G=(V,E)$, a cut of size $\geq |E|/2$ can be found efficiently (randomized algo.).

↳ it proves existence of A: $|cut(A)| \geq |E|/2$.

3) Sum-Free Subset

- For subset $S \subseteq \mathbb{Z}$, define $S+S := \{s_1+s_2 \mid s_1, s_2 \in S\}$.
- Defn: S is sum-free if $S \cap (S+S) = \phi$.

▷ $0 \in S \Rightarrow S$ is not sum-free!

- Eg. • $\{1,2\}$ is not sum-free.
  • $\{1, 3, 3^2, \ldots\}$ is sum-free. (base-3 no.?)

Theorem 3: For any set S of n nonzero integers, there is a subset $S' \subseteq S$: (i) S' is sum-free, & (ii) $|S'| > n/3$.

Exercise: Is $n/3$ optimal?

Pf of Thm 3: Idea — Note that $T := \{k+1, k+2, \ldots, 2k+1\}$ is sum-free if $k > 0$.

- Try to map S to $[3k+1] \supset T$.
- Pick prime $p := 3k+2$, for $k > \max(S)$, & map S to $(r \cdot S \bmod p)$.

Does r exist?

- Note: $T \bmod p$ remains sum-free! (Why?)

- Pick p & random $r \in [p-1]$.

▷ $\forall s, s' \in S$: $r \cdot s \equiv r \cdot s' \pmod p$ iff
$s \equiv s' \pmod p$ iff $s = s'$.

▷ $|r \cdot S \bmod p| = |S| = n$.

- Define rnd. variable $Y := |\underbrace{(r \cdot S \bmod p)}_{\text{image}} \cap \underbrace{T}_{\text{sum-free}}|$.

▷ $Y = \sum_s Y_s$

▷ $E[Y] \overset{\text{linearity}}{=} \sum_{s \in S} E[\underbrace{(r \cdot s \bmod p) \in T}_{Y_s := 1, \text{ if true; } 0, \text{ else}}] \overset{\text{partition}}{=} \sum_{\substack{s \in S \\ t \in T}} P(rs \equiv t \bmod p)$

$= \sum_{s,t} P(r \equiv t/s \bmod p) = \sum_{s,t} \frac{1}{p-1} = \frac{|S| \cdot |T|}{p-1}$

$= n \cdot \frac{k+1}{3k+1} > n/3$.

$\Rightarrow \exists\, r \in [p-1]$, $|(r \cdot S \bmod p) \cap T| > n/3$ & $(r \cdot S \bmod p) \cap T$ is sum-free.

$\Rightarrow$ $S \cap (r^{-1} \cdot T \bmod p) =: S'$ is a sum-free subset of S of size $> n/3$. $\square$

▷ This gives a fast, randomized algorithm to find a large sum-free subset of input S.