Discrete Mathematics & Mathematical Reasoning
Chapter 7 (continued): Examples in probability: Ramsey numbers and the probabilistic method

Kousha Etessami

U. of Edinburgh, UK

Frank Ramsey (1903-1930)

A brilliant logician/mathematician.

He studied and lectured at Cambridge University.

He died tragically young, at age 26.

Despite his early death,
he did hugely influential work in several fields:
logic, combinatorics, and economics.

Friends and Enemies

Theorem: Suppose that in a group of 6 people every pair are either friends or enemies.

Then, there are either 3 mutual friends or 3 mutual enemies.

Proof: Let $\{A, B, C, D, E, F\}$ be the 6 people.

Consider A's friends & enemies. A has 5 relationships, so A must either have 3 friends or 3 enemies.

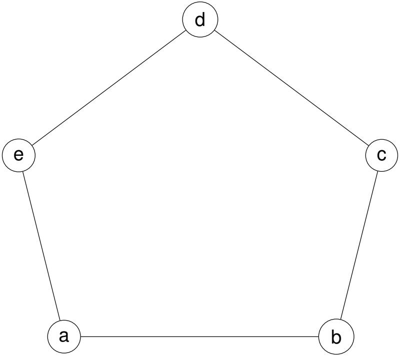
Suppose, for example, that $\{B, C, D\}$ are all friends of A.

If some pair in $\{B, C, D\}$ are friends, for example $\{B, C\}$, then $\{A, B, C\}$ are 3 mutual friends. Otherwise, $\{B, C, D\}$ are 3 mutual enemies.

The same argument clearly works if A had 3 enemies instead of 3 friends. $\square$

Remarks on “Friends and Enemies”: 6 is the smallest number possible for finding 3 friends or 3 enemies

Note that it is possible to have 5 people, where every pair of them are either friends or enemies, such that there does not exist 3 of them who are all mutual friends or all mutual enemies:



Graphs and Ramsey's Theorem

Ramsey's Theorem (a special case, for graphs)

Theorem: For any positive integer, k, there is a positive integer, n, such that in any undirected graph with n or more vertices:

either there are k vertices that are all mutually adjacent, meaning they form a k-clique,

or, there are k vertices that are all mutually non-adjacent, meaning they form a k-independent-set.

For each integer $k \geq 1$, let $R(k)$ be the smallest integer $n \geq 1$ such that every undirected graph with n or more vertices has either a k-clique or a k-independent-set as an induced subgraph.

The numbers $R(k)$ are called diagonal Ramsey numbers.

Proof of Ramsey's Theorem: Consider any integer $k \geq 1$, and any graph, $G_1 = (V_1, E_1)$ with at least 2^{2k} vertices.

> Initialize: $S_{Friends} := \{\}$; $S_{Enemies} := \{\}$;
> **for** $i := 1$ to $2k - 1$ **do**
>   Pick any vertex $v_i \in V_i$;
>   **if** (v_i has at least 2^{2k-i} friends in G_i) **then**
> $S_{Friends} := S_{Friends} \cup \{v_i\}$; $V_{i+1} := \{\text{friends of } v_i\}$;
>   **else** (* in this case v_i has at least 2^{2k-i} enemies in G_i *)
> $S_{Enemies} := S_{Enemies} \cup \{v_i\}$; $V_{i+1} := \{\text{enemies of } v_i\}$;
>   **end if**
>   Let $G_{i+1} = (V_{i+1}, E_{i+1})$ be the subgraph of G_i induced by V_{i+1};
> **end for**

At the end, all vertices in $S_{Friends}$ are mutual friends, and all vertices in $S_{Enemies}$ are mutual enemies. Since $|S_{Friends} \cup S_{Enemies}| = 2k - 1$, either $|S_{Friends}| \geq k$ or $|S_{Enemies}| \geq k$. Done. $\square$

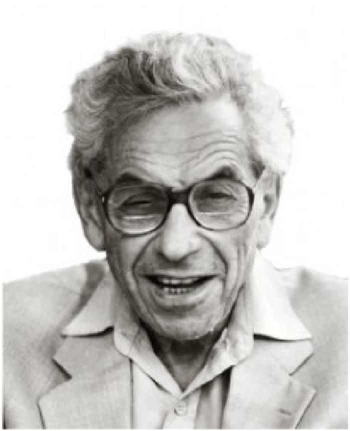
Remarks on the proof, and on Ramsey numbers

- The proof establishes that $R(k) \leq 2^{2k} = 4^k$.

  (A more careful look at this proof shows that $R(k) \leq 2^{2k-1}$.)

- **Question:** Can we give a better upper bound on $R(k)$?

- **Question:** Can we give a good lower bound on $R(k)$?



Paul Erdös (1913-1996)

Immensely prolific mathematician,
eccentric nomad,
father of the probabilistic method in combinatorics.

Lower bounds on Ramsey numbers, and the Probabilistic Method

Theorem (Erdös,1947)

For all $k \geq 3$,

$$R(k) > 2^{k/2}$$

The proof uses the probabilistic method:

General idea of "the probabilistic method": To show the existence of a hard-to-find object with a desired property, Q, try to construct a probability distribution over a sample space Ω of objects, and show that with positive probability a randomly chosen object in Ω has the property Q.

Proof that $R(k) > 2^{k/2}$ using the probabilistic method:

Let Ω be the set of all graphs on the vertex set $V = \{v_1, \ldots, v_n\}$. (We will later determine that $n \leq 2^{k/2}$ suffices.)

There are $2^{\binom{n}{2}}$ such graphs. Let $P : \Omega \rightarrow [0, 1]$, be the uniform probability distribution on such graphs.

So, every graph on V is equally likely. This implies for all $i \neq j$:

$$P(\{v_i, v_j\} \text{ is an edge of the graph}) = 1/2. \qquad (1)$$

We could also define the distribution P by saying it satisfies (1), and the events "$\{v_i, v_j\}$ is an edge of the graph" are *mutually independent*, for all $i \neq j$.

There are $\binom{n}{k}$ subsets of V of size k.
Let $S_1, S_2, \ldots, S_{\binom{n}{k}}$ be an enumeration of these subsets of V.

For $i = 1, \ldots, \binom{n}{k}$, let E_i be the event that S_i forms either a k-clique or a k-independent-set in the graph. Note that:

$$P(E_i) = 2 \cdot 2^{-\binom{k}{2}} = 2^{-\binom{k}{2}+1}$$

Proof of $R(k) > 2^{k/2}$ (continued):

Note that $E = \bigcup_{i=1}^{\binom{n}{k}} E_i$ is the event that there exists either a k-clique or a k-independent-set in the graph. But:

$$P(E) = P(\bigcup_{i=1}^{\binom{n}{k}} E_i) \leq \sum_{i=1}^{\binom{n}{k}} P(E_i) = \binom{n}{k} \cdot 2^{-\binom{k}{2}+1}$$

Question: How small must n be so that $\binom{n}{k} \cdot 2^{-\binom{k}{2}+1} < 1$?

For $k \geq 2$: $$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} < \frac{n^k}{2^{k-1}}$$

Thus, if $n \leq 2^{k/2}$, then

$$\binom{n}{k} \cdot 2^{-\binom{k}{2}+1} < \frac{(2^{k/2})^k}{2^{k-1}} \cdot 2^{-\binom{k}{2}+1} = \frac{2^{k^2/2}}{2^{k-1}} \cdot 2^{-k(k-1)/2+1} = 2^{2-\frac{k}{2}}$$

Completion of the proof that $R(k) > 2^{k/2}$:

For $k \geq 4$, $2^{2-(k/2)} \leq 1$.

So, for $k \geq 4$, $P(E) < 1$, and thus $P(\Omega - E) = 1 - P(E) > 0$.

But note that $P(\Omega - E)$ is the probability that in a random graph of size $n \leq 2^{k/2}$, there is no k-clique and no k-independent-set.

Thus, since $P(\Omega - E) > 0$, such a graph must exist for any $n \leq 2^{k/2}$.

Note that we earlier argued that $R(3) = 6$, and clearly $6 > 2^{3/2} = 2.828\ldots$.

Thus, we have established that for all $k \geq 3$,

$$R(k) > 2^{k/2}. \qquad \square$$

A Remark

In the proof, we used the following trivial but often useful fact:

Union bound

Theorem: For any (finite or countable) sequence of events $E_1, E_2, E_3, \ldots$

$$P(\bigcup_i E_i) \leq \sum_i P(E_i)$$

Proof (trivial):

$$P(\bigcup_i E_i) = \sum_{s \in \bigcup_i E_i} P(s) \leq \sum_i \sum_{s \in E_i} P(s) = \sum_i P(E_i). \quad \square$$

Remarks on Ramsey numbers

- We have shown that

$$2^{k/2} = (\sqrt{2})^k \; < \; R(k) \; \leq \; 4^k = 2^{2k}$$

[1] See [Conlon,2009] for state-of-the-art upper bounds.

Remarks on Ramsey numbers

- We have shown that

$$2^{k/2} = (\sqrt{2})^k \; < \; R(k) \; \leq \; 4^k = 2^{2k}$$

- Despite decades of research by many combinatorists, nothing significantly better is known![1] In particular:

  no constant $c > \sqrt{2}$ is known such that $c^k \leq R(k)$, and no constant $c' < 4$ is known such that $R(k) \leq (c')^k$.

- For specific small k, more is known:

$$R(1) = 1 \quad ; \quad R(2) = 2 \quad ; \quad R(3) = 6 \quad ; \quad R(4) = 18$$

$$43 \leq R(5) \leq 49$$

$$102 \leq R(6) \leq 165$$

$$\cdots$$

[1] See [Conlon,2009] for state-of-the-art upper bounds.

Why can't we just compute $R(k)$ exactly, for small k?

For each k, we know that $2^{k/2} < R(k) < 2^{2k}$,

So, we could try to check, exhaustively, for each r such that $2^{k/2} < r < 2^{2k}$, whether there is a graph G with r vertices such that G has no k-clique and no k-independent set.

Question: How many graphs on r vertices are there?

There are $2^{\binom{r}{2}} = 2^{r(r-1)/2}$ (labeled) graphs on r vertices.

So, for $r = 2^k$, we would have to check $2^{2^k(2^k-1)/2}$ graphs!!

So for $k = 5$, just for $r = 2^5$, we have to check 2^{496} graphs !!

Quote attributed to Paul Erdös:

Suppose an alien force, vastly more powerful than us, landed on Earth demanding to know the value of $R(5)$*, or else they would destroy our planet.*

Quote attributed to Paul Erdös:

Suppose an alien force, vastly more powerful than us, landed on Earth demanding to know the value of $R(5)$, or else they would destroy our planet.

In that case, I believe we should marshal all our computers, and all our mathematicians, in an attempt to find the value.

Quote attributed to Paul Erdös:

Suppose an alien force, vastly more powerful than us, landed on Earth demanding to know the value of $R(5)$, or else they would destroy our planet.

In that case, I believe we should marshal all our computers, and all our mathematicians, in an attempt to find the value.

But suppose instead they asked us for $R(6)$.

Quote attributed to Paul Erdös:

Suppose an alien force, vastly more powerful than us, landed on Earth demanding to know the value of $R(5)$, or else they would destroy our planet.

In that case, I believe we should marshal all our computers, and all our mathematicians, in an attempt to find the value.

But suppose instead they asked us for $R(6)$.

In that case, I believe we should attempt to destroy the aliens.