概率计数

刘正阳 zhengyang@bit.edu.cn

概率方法

证明事件的存在性

- 想法: 构造概率空间,证明事件发生的概率非零
- 与平均值原理类似
- 关注简单例子,看上去可以等同于计数问题

概率论复习

离散概率

- 概率空间,概率分布 $\Pr: \Omega \to [0,1]$,满足 $\sum_{x \in \Omega} \Pr[x] = 1$
- 事件 $A \subseteq \Omega$, $\Pr[A] := \sum_{x \in A} \Pr[x]$
 - 1. $\Pr[\Omega] = 1$, $\Pr[\emptyset] = 0$ and $\Pr[A] \ge 0$ for all $A \subseteq \Omega$;
 - 2. $\Pr[A \cup B] = \Pr[A] + \Pr[B] \Pr[A \cap B] \le \Pr[A] + \Pr[B]$;
 - 3. $Pr[A \cup B] = Pr[A] + Pr[B]$ if A and B are disjoint;
 - 4. $\Pr[A] = 1 \Pr[A];$
 - 5. $\Pr[A \setminus B] = \Pr[A] \Pr[A \cap B];$
 - 6. $\Pr[A \cap B] \ge \Pr[A] \Pr[\overline{B}];$
 - 7. If B_1, \ldots, B_m is a partition of Ω then $\Pr[A] = \sum_{i=1}^m \Pr[A \cap B_i]$.

离散概率Ⅱ

- 条件概率 $\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}$
- 独立事件 $Pr[A \cap B] = Pr[A] \cdot Pr[B]$
- 随机变量 $X: \Omega \to \mathbb{R}$, 特例: 示性变量 (indicator)
- 期望 $\mathrm{E}\left[X\right] := \sum_{i=1}^{m} s_i \cdot \Pr\left[X = s_i\right] = \sum_{x \in \Omega} X(x) \cdot \Pr\left[x\right]$ $\mathrm{E}\left[a_1 X_1 + \dots + a_n X_n\right] = a_1 \mathrm{E}\left[X_1\right] + \dots + a_n \mathrm{E}\left[X_n\right]$
- 联合界 (union bound)

$$\Pr\left[A_1 \cup A_2 \cup \dots \cup A_n\right] \leq \Pr\left[A_1\right] + \Pr\left[A_2\right] + \dots + \Pr\left[A_n\right]$$

如果 A_i 都是坏事件且 $\sum \Pr[A_i] < 1$,所有坏事件可能均不发生。

Ex 3.2
$$\Pr[A_1 \cap \dots \cap A_n] \ge \Pr[A_1] + \dots + \Pr[A_n] - n + 1$$

概率方法的一般框架

- 集合 M 和函数 $f: M \to \mathbb{R}$
 - E.g. M是满足特定性质的图的集合,f(x) 表示图中最大团的大小。然后证明 $\max_{x \in M} f(x) \ge t$

概率方法的一般框架

- 集合 M 和函数 $f: M \to \mathbb{R}$
 - E.g. M是满足特定性质的图的集合,f(x) 表示图中最大团的大小。然后证明 $\max_{x \in M} f(x) \ge t$
- 概率空间 $Pr: M \rightarrow [0,1]$,此时 f 是随机变量

概率方法的一般框架

- 集合 M 和函数 $f: M \to \mathbb{R}$
 - E.g. *M*是满足特定性质的图的集合, f(x) 表示图中最大团的大小。然后证明 $\max_{x \in M} f(x) \ge t$
- 概率空间 $Pr: M \rightarrow [0,1]$,此时 f 是随机变量
- 证明 $\mathbb{E}[f] \ge t$ 或 $\Pr[f(x) \ge t] \ne 0$

有向图,任意两点间有边

来源:循环赛

• 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y, x) \in E$ 。

有向图,任意两点间有边

来源:循环赛

• 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y,x) \in E$ 。

有向图,任意两点间有边

来源:循环赛

• 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y,x) \in E$ 。

Theorem 3.1 (Erdős 1963a). If $n \ge k^2 2^{k+1}$, then there is a tournament of n players that has the property P_k .

• 建立概率分布?

有向图,任意两点间有边

- 来源:循环赛
- 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y,x) \in E$ 。

- 建立概率分布? 等概率朝向
- 令 A_S 记对集合 S 不满足 P_k ,所以 $\Pr[A_S] = ?$

有向图,任意两点间有边

- 来源:循环赛
- 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y,x) \in E$ 。

- 建立概率分布? 等概率朝向
- $\Diamond A_S$ 记对集合 S 不满足 P_k , 所以 $\Pr[A_S] = (1 2^{-k})^{n-k}$

有向图,任意两点间有边

- 来源:循环赛
- 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y,x) \in E$ 。

- 建立概率分布? 等概率朝向
- 令 A_S 记对集合 S 不满足 P_k , 所以 $\Pr[A_S] = (1 2^{-k})^{n-k}$

$$\Pr\left[\bigcup A_S\right] \le \binom{n}{k} (1 - 2^{-k})^{n-k} < \frac{n^k}{k!} e^{-(n-k)/2^k} \le n^k e^{-n/2^k}$$

有向图,任意两点间有边

- 来源:循环赛
- 性质 P_k : 对任意 k-元素子集 $S \subseteq V$,存在 $y \notin S$,使得对于任意 $x \in S$,有 $(y,x) \in E$ 。

- 建立概率分布? 等概率朝向
- 令 A_S 记对集合 S 不满足 P_k , 所以 $\Pr[A_S] = (1 2^{-k})^{n-k}$

$$\Pr\left[\bigcup A_S\right] \le \binom{n}{k} (1 - 2^{-k})^{n-k} < \frac{n^k}{k!} e^{-(n-k)/2^k} \le n^k e^{-n/2^k}$$

联合界 组合数上界

A set of 0-1 strings of length n is (n,k)-universal if, for any subset of k coordinates $S = \{i_1, \ldots, i_k\}$, the projection

$$A \upharpoonright_S := \{(a_{i_1}, \dots, a_{i_k}) : (a_1, \dots, a_n) \in A\}$$

of A onto the coordinates in S contains all possible 2^k configurations.

A set of 0-1 strings of length n is (n,k)-universal if, for any subset of k coordinates $S = \{i_1, \ldots, i_k\}$, the projection

$$A \upharpoonright_S := \{(a_{i_1}, \dots, a_{i_k}) : (a_1, \dots, a_n) \in A\}$$

of A onto the coordinates in S contains all possible 2^k configurations.

• {1010} 是 (4,2)-universal, {101, 010} 是 (3,2)-universal

A set of 0-1 strings of length n is (n,k)-universal if, for any subset of k coordinates $S = \{i_1, \ldots, i_k\}$, the projection

$$A \upharpoonright_S := \{(a_{i_1}, \dots, a_{i_k}) : (a_1, \dots, a_n) \in A\}$$

of A onto the coordinates in S contains all possible 2^k configurations.

• {1010} 是 (4,2)-universal, {101, 010} 是 (3,2)-universal

Theorem 3.2 (Kleitman–Spencer 1973). If $\binom{n}{k} 2^k (1 - 2^{-k})^r < 1$, then there is an (n, k)-universal set of size r.

A set of 0-1 strings of length n is (n,k)-universal if, for any subset of k coordinates $S = \{i_1, \ldots, i_k\}$, the projection

$$A \upharpoonright_S := \{(a_{i_1}, \dots, a_{i_k}) : (a_1, \dots, a_n) \in A\}$$

of A onto the coordinates in S contains all possible 2^k configurations.

• {1010} 是 (4,2)-universal, {101, 010} 是 (3,2)-universal

Theorem 3.2 (Kleitman–Spencer 1973). If $\binom{n}{k} 2^k (1 - 2^{-k})^r < 1$, then there is an (n, k)-universal set of size r.

固定 k-元素的集合 S 和某个 $v \in \{0,1\}^k$,我们有

A set of 0-1 strings of length n is (n,k)-universal if, for any subset of k coordinates $S = \{i_1, \ldots, i_k\}$, the projection

$$A \upharpoonright_S := \{(a_{i_1}, \dots, a_{i_k}) : (a_1, \dots, a_n) \in A\}$$

of A onto the coordinates in S contains all possible 2^k configurations.

• {1010} 是 (4,2)-universal, {101, 010} 是 (3,2)-universal

Theorem 3.2 (Kleitman–Spencer 1973). If $\binom{n}{k} 2^k (1 - 2^{-k})^r < 1$, then there is an (n, k)-universal set of size r.

固定 k-元素的集合 S 和某个 $v \in \{0,1\}^k$,我们有

$$\Pr\left[v \not\in \mathbf{A} \upharpoonright_{S}\right] = \prod_{a \in \mathbf{A}} \Pr\left[v \neq a \upharpoonright_{S}\right] = \prod_{a \in \mathbf{A}} \left(1 - 2^{-|S|}\right) = \left(1 - 2^{-k}\right)^{r}$$

二分团覆盖(Biclique Covering)

- 二分团,也称二分完全图,即任意两个不同边的点均有边相连。
- 图G的一个二分团覆盖:一组二分团 $H_1, ..., H_t$,使得G中所有边均属于某一个二分团 H_i
 - 一个覆盖的权重: $\sum_{i=1}^{t} |V(H_i)|$
 - bc(G) := G的二分图覆盖中的权重最小值

二分团覆盖(Biclique Covering)

- 二分团,也称二分完全图,即任意两个不同边的点均有边相连。
- 图G的一个二分团覆盖:一组二分团 $H_1, ..., H_t$,使得G中所有边均属于某一个二分团 H_i
 - 一个覆盖的权重: $\sum_{i=1}^{l} |V(H_i)|$
 - bc(G) := G的二分图覆盖中的权重最小值

Theorem 3.3. If n is a power of two, then $bc(K_n) = n \log_2 n$.

n个点的团(完全图)

• 组合极值:证明分两部分,证明极值&构造极值

- 组合极值:证明分两部分,证明极值&构造极值
- 令一个覆盖为 $A_1 \times B_1, ..., A_t \times B_t$, 因此 $\sum_{i=1}^t (|A_i| + |B_i|) = \sum_{v=1}^n m_v$
 - 其中 m_v 表示包含点 v 的二分团个数

- 组合极值:证明分两部分,证明极值&构造极值
- 令一个覆盖为 $A_1 \times B_1, ..., A_t \times B_t$, 因此 $\sum_{i=1}^t (|A_i| + |B_i|) = \sum_{v=1}^n m_v$
 - 其中 m_v 表示包含点 v 的二分团个数
- 根据定义,每条边均属于某个二分团 $A_i \times B_i$,如果删掉 A_i 或 B_i ,该边就不存在了。

- 组合极值:证明分两部分,证明极值&构造极值
- 令一个覆盖为 $A_1 \times B_1, ..., A_t \times B_t$, 因此 $\sum_{i=1}^t (|A_i| + |B_i|) = \sum_{v=1}^n m_v$
 - 其中 m_v 表示包含点 v 的二分团个数
- 根据定义,每条边均属于某个二分团 $A_i \times B_i$,如果删掉 A_i 或 B_i ,该边就不存在了。
 - 对 $i \in [t]$,等概率删掉 A_i 或 B_i !

- 组合极值:证明分两部分,证明极值&构造极值
- 令一个覆盖为 $A_1 \times B_1, ..., A_t \times B_t$, 因此 $\sum_{i=1}^t (|A_i| + |B_i|) = \sum_{v=1}^n m_v$
 - 其中 m_v 表示包含点 v 的二分团个数
- 根据定义,每条边均属于某个二分团 $A_i \times B_i$,如果删掉 A_i 或 B_i ,该边就不存在了。
 - 对 $i \in [t]$,等概率删掉 A_i 或 B_i !
- 考虑 $X = \sum X_i$, $\mathbb{E}[X] \le 1$, X_i 为 i 最终存活的示性变量

- 组合极值:证明分两部分,证明极值&构造极值
- 令一个覆盖为 $A_1 \times B_1, ..., A_t \times B_t$, 因此 $\sum_{i=1}^t (|A_i| + |B_i|) = \sum_{v=1}^t m_v$
 - 其中 m_v 表示包含点 v 的二分团个数
- 根据定义,每条边均属于某个二分团 $A_i \times B_i$,如果删掉 A_i 或 B_i ,该边就不存在了。
 - 对 $i \in [t]$,等概率删掉 A_i 或 B_i !
- 考虑 $X = \sum X_i$, $\mathbb{E}[X] \le 1$, X_i 为 i 最终存活的示性变量
- 另一方面,如何利用 m_v 表示 $\mathbb{E}[X]$?

- 组合极值:证明分两部分,证明极值&构造极值
- 令一个覆盖为 $A_1 \times B_1, ..., A_t \times B_t$, 因此 $\sum_{i=1}^t (|A_i| + |B_i|) = \sum_{v=1}^n m_v$
 - 其中 m_v 表示包含点 v 的二分团个数
- 根据定义,每条边均属于某个二分团 $A_i \times B_i$,如果删掉 A_i 或 B_i ,该边就不存在了。
 - 对 $i \in [t]$,等概率删掉 A_i 或 B_i !
- 考虑 $X = \sum X_i$, $\mathbb{E}[X] \le 1$, X_i 为 i 最终存活的示性变量
- 另一方面,如何利用 m_v 表示 $\mathbb{E}[X]$?

$$\sum_{v=1}^{n} 2^{-m_v} = \sum_{v=1}^{n} \Pr[v \text{ survives}] = \sum_{v=1}^{n} E[X_v] = E[X] \le 1$$

- 族 $\mathcal{F} \subseteq 2^X$,对 X 的元素进行**2-染色**,使得 \mathcal{F} 中的成员(即 X 的一个子集)均不同色!
- 一个族是k-均匀(uniform),如果 \mathcal{F} 中的每个成员包含k个元素。

Theorem 3.4 (Erdős 1963b). Every k-uniform family with fewer than 2^{k-1} members is 2-colorable.

- 族 $\mathcal{F} \subseteq 2^X$,对 X 的元素进行**2-染色**,使得 \mathcal{F} 中的成员(即 X 的一个子集)均不同色!
- 一个族是k-均匀 (uniform) ,如果爭中的每个成员包含k个元素。 **Theorem 3.4** (Erdős 1963b). Every k-uniform family with fewer than 2^{k-1} members is 2-colorable.
- 概率空间?

- 族 $\mathcal{F} \subseteq 2^X$,对 X 的元素进行**2-染色**,使得 \mathcal{F} 中的成员(即 X 的一个子集)均不同色!
- 一个族是k-均匀 (uniform) ,如果爭中的每个成员包含k个元素。

 Theorem 3.4 (Erdős 1963b). Every k-uniform family with fewer than 2^{k-1}

 members is 2-colorable.
- 概率空间? 对每个元素随机染色!
- 坏事件?

- 族 $\mathcal{F} \subseteq 2^X$,对 X 的元素进行**2-染色**,使得 \mathcal{F} 中的成员(即 X 的一个子集)均不同色!
- 一个族是*k*-均匀(uniform),如果ℱ中的每个成员包含*k*个元素。
 Theorem 3.4 (Erdős 1963b). Every k-uniform family with fewer than 2^{k-1}
 members is 2-colorable.
- 概率空间?对每个元素随机染色!
- 坏事件? X_A 表示集合 A 中元素同色, $X = \sum_{A \in \mathcal{F}} X_A$
- 要证明?

- 族 $\mathcal{F} \subseteq 2^X$,对 X 的元素进行**2-染色**,使得 \mathcal{F} 中的成员(即 X 的一个子集)均不同色!
- 一个族是k-均匀 (uniform) ,如果爭中的每个成员包含k个元素。
 Theorem 3.4 (Erdős 1963b). Every k-uniform family with fewer than 2^{k-1} members is 2-colorable.
- 概率空间? 对每个元素随机染色!
- 坏事件? X_A 表示集合 A 中元素同色, $X = \sum_{A \in \mathcal{F}} X_A$
- 要证明? E[X] < 1

- 族 $\mathcal{F} \subseteq 2^X$,对 X 的元素进行**2-染色**,使得 \mathcal{F} 中的成员(即 X 的一个子集)均不同色!
- 一个族是k-均匀(uniform),如果爭中的每个成员包含k个元素。 **Theorem 3.4** (Erdős 1963b). Every k-uniform family with fewer than 2^{k-1} members is 2-colorable.
- 概率空间?对每个元素随机染色!
- 坏事件? X_A 表示集合 A 中元素同色, $X = \sum_{A \in \mathcal{F}} X_A$
- 要证明? E[X] < 1
- | F | 能再大一点吗?

Theorem 3.5 (Erdős 1964a). If k is sufficiently large, then there exists a k-uniform family \mathcal{F} such that $|\mathcal{F}| \leq k^2 2^k$ and \mathcal{F} is not 2-colorable.

鸽笼原理

一个简单的事实

鸽子多,笼子少

- 反证法的应用
- 证明存在性的方法,非构造性
- 简单蕴含着不简单!
- 什么是鸽子? 什么是笼子?

一些例子

• 任意图存在两个点度数相等

一些例子

• 任意图存在两个点度数相等

If G is a finite graph, the *independence number* $\alpha(G)$ is the maximum number of pairwise nonadjacent vertices of G. The *chromatic number* $\chi(G)$ of G is the minimum number of colors in a coloring of the vertices of G with the property that no two adjacent vertices have the same color.

Proposition 4.2. In any graph G with n vertices, $n \leq \alpha(G) \cdot \chi(G)$.

一些例子

• 任意图存在两个点度数相等

If G is a finite graph, the *independence number* $\alpha(G)$ is the maximum number of pairwise nonadjacent vertices of G. The *chromatic number* $\chi(G)$ of G is the minimum number of colors in a coloring of the vertices of G with the property that no two adjacent vertices have the same color.

Proposition 4.2. In any graph G with n vertices, $n \leq \alpha(G) \cdot \chi(G)$.

Proposition 4.3. Let G be an n-vertex graph. If every vertex has a degree of at least (n-1)/2 then G is connected.

序列中的递增和递减,一种对偶?

Theorem 4.5 (Erdős–Szekeres 1935). Let $A = (a_1, \ldots, a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of s + 1 terms or a decreasing subsequence of r + 1 terms (or both).

序列中的递增和递减,一种对偶?

Theorem 4.5 (Erdős–Szekeres 1935). Let $A = (a_1, \ldots, a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of s + 1 terms or a decreasing subsequence of r + 1 terms (or both).

$$a_i \rightarrow (x_i, y_i)$$

序列中的递增和递减,一种对偶?

Theorem 4.5 (Erdős–Szekeres 1935). Let $A = (a_1, \ldots, a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of s + 1 terms or a decreasing subsequence of r + 1 terms (or both).

$$a_i \rightarrow (x_i, y_i)$$

其中 x_i 是以 a_i 终止的最长递增序列长度, y_i 是以 a_i 起始的最长递减序列长度。

序列中的递增和递减,一种对偶?

Theorem 4.5 (Erdős–Szekeres 1935). Let $A = (a_1, \ldots, a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of s + 1 terms or a decreasing subsequence of r + 1 terms (or both).

$$a_i \rightarrow (x_i, y_i)$$

其中 x_i 是以 a_i 终止的最长递增序列长度, y_i 是以 a_i 起始的最长递减序列长度。

所有元素的 (x_i, y_i) 均不相等

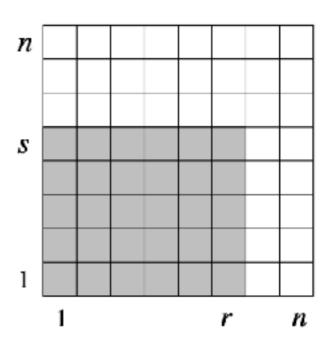
序列中的递增和递减,一种对偶?

Theorem 4.5 (Erdős–Szekeres 1935). Let $A = (a_1, \ldots, a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of s + 1 terms or a decreasing subsequence of r + 1 terms (or both).

$$a_i \rightarrow (x_i, y_i)$$

其中 x_i 是以 a_i 终止的最长递增序列长度, y_i 是以 a_i 起始的最长递减序列长度。

所有元素的 (x_i, y_i) 均不相等



无三角形(triangle-free)的图最多有多少边?

Theorem 4.7 (Mantel 1907). If a graph G on n vertices contains more than $n^2/4$ edges, then G contains a triangle.

无三角形(triangle-free)的图最多有多少边?

Theorem 4.7 (Mantel 1907). If a graph G on n vertices contains more than $n^2/4$ edges, then G contains a triangle.

• 算两次: 没有三角形->相邻两点不存在公共邻居, $d(x) + d(y) \le n$, 对于 $(x, y) \in E$

无三角形(triangle-free)的图最多有多少边?

Theorem 4.7 (Mantel 1907). If a graph G on n vertices contains more than $n^2/4$ edges, then G contains a triangle.

- 算两次: 没有三角形->相邻两点不存在公共邻居, $d(x) + d(y) \le n$, 对于 $(x, y) \in E$
- 均值不等式: 令 $A \subseteq V$ 为一个最大独立集,那么 $B = V \setminus A$?

无三角形(triangle-free)的图最多有多少边?

Theorem 4.7 (Mantel 1907). If a graph G on n vertices contains more than $n^2/4$ edges, then G contains a triangle.

- 算两次: 没有三角形->相邻两点不存在公共邻居, $d(x) + d(y) \le n$, 对于 $(x, y) \in E$
- 均值不等式: 令 $A \subseteq V$ 为一个最大独立集,那么 $B = V \setminus A$?
- 鸽笼原理+数学归纳法