Вероятностные методы и параметризованные алгоритмы

*St. Petersburg Academic University of the Russian Academy of Sciences

14 Октября, 2015

(n,k,l)-splitter

Definition

(n,k,l)-разделитель ((n,k,l)-splitter) $\mathcal{F}$ — это семейство функций действующих из $\{1,2,\dots n\}$ в $\{1,2,\dots,l\}$ так, что для любого множества $S \subseteq \{1,2,\dots,n\}$ размера k, существует $f \in \mathcal{F}$, которая "разделяет" множество S равномерно. То есть для любых $1 \le i,j \le l$:

$$|f^{-1}(i) \cap S| - |f^{-1}(j) \cap S| \in \{-1,0,1\}.$$

Если $l > k$, то требование равномерного разделения эквивалетно инъективности.

(n,k,l)-splitter

Definition

(n,k,l)-разделитель ((n,k,l)-splitter) $\mathcal{F}$ — это семейство функций действующих из $\{1,2,\dots n\}$ в $\{1,2,\dots,l\}$ так, что для любого множества $S \subseteq \{1,2,\dots,n\}$ размера k, существует $f \in \mathcal{F}$, которая "разделяет" множество S равномерно. То есть для любых $1 \le i,j \le l$:

$$|f^{-1}(i) \cap S| - |f^{-1}(j) \cap S| \in \{-1,0,1\}.$$

Если $l > k$, то требование равномерного разделения эквивалетно инъективности.

Размер разделителя

Theorem

Для любых $n, k \geq 1$ можно построить (n, k, k^2)-разделитель размера $k^{O(1)} \log n$ за время $k^{O(1)} n \log n$.

Definition

(n, k, k)-разделитель называется (n, k)-совершенным хэш семейством ((n, k)-perfect hash family).

Theorem

Для любых $n, k \geq 1$ можно построить (n, k)-совершенное хэш семейство размера $e^k k^{O(\log k)} \log n$ за время $e^k k^{O(\log k)} n \log n$

Размер разделителя

Theorem

Для любых $n, k \geq 1$ можно построить (n, k, k^2)-разделитель размера $k^{O(1)} \log n$ за время $k^{O(1)} n \log n$.

Definition

(n, k, k)-разделитель называется (n, k)-совершенным хэш семейством ((n, k)-perfect hash family).

Theorem

Для любых $n, k \geq 1$ можно построить (n, k)-совершенное хэш семейство размера $e^k k^{O(\log k)} \log n$ за время $e^k k^{O(\log k)} n \log n$

Размер разделителя

Theorem

Для любых $n, k \geq 1$ *можно построить* (n, k, k^2)*-разделитель размера* $k^{O(1)} \log n$ *за время* $k^{O(1)} n \log n$*.*

Definition

(n, k, k)-разделитель называется (n, k)-совершенным хэш семейством ((n, k)-perfect hash family).

Theorem

Для любых $n, k \geq 1$ *можно построить* (n, k)*-совершенное хэш семейство размера* $e^k k^{O(\log k)} \log n$ *за время* $e^k k^{O(\log k)} n \log n$

Совершенное хэш семейство

Theorem

Для любых $n, k \geq 1$ можно построить (n, k)-совершенное хэш семейство размера $e^k k^{O(\log k)} \log n$ за время $e^k k^{O(\log k)} n \log n$.

Доказательство теоремы получается применением композиции (n, k, k^2)-разделителя $\mathcal{F}_1$ и явной конструкцией (k^2, k, k)-разделителя $\mathcal{F}_2$.

Совершенное хэш семейство

Theorem

Для любых $n, k \geq 1$ можно построить (n, k)-совершенное хэш семейство размера $e^k k^{O(\log k)} \log n$ за время $e^k k^{O(\log k)} n \log n$.

Доказательство теоремы получается применением композиции (n, k, k^2)-разделителя $\mathcal{F}_1$ и явной конструкцией (k^2, k, k)-разделителя $\mathcal{F}_2$.

k-путь

Theorem

Задача k-пути может быть решена за время $(2e)^k k^{O(\log k)} n^{O(1)}$.

(n,k)-универсальные множества

Definition

(n,k)-универсальное множество — это семейство $\mathcal{U}$ подмножеств $[n] = \{1, 2, \ldots, n\}$, такое что для любого $S \subseteq [n]$ размера k, семейство $\{A \cap S | A \in \mathcal{U}\}$ содержит все 2^k подмножеств S.

Theorem

Для любых $n, k \geq 1$ можно построить (n,k)-универсальное множество размера $2^k k^{O(\log k)} n \log n$

Problem

Дерандомизировать алгоритм для Изоморфизма Подграфов.

(n, k)-универсальные множества

Definition

(n, k)-универсальное множество — это семейство $\mathcal{U}$ подмножеств $[n] = \{1, 2, \ldots, n\}$, такое что для любого $S \subseteq [n]$ размера k, семейство $\{A \cap S | A \in \mathcal{U}\}$ содержит все 2^k подмножеств S.

Theorem

Для любых $n, k \geq 1$ можно построить (n, k)-универсальное множество размера $2^k k^{O(\log k)} n \log n$

Problem

Дерандомизировать алгоритм для Изоморфизма Подграфов.

(n,k)-универсальные множества

Definition

(n,k)-универсальное множество — это семейство $\mathcal{U}$ подмножеств $[n] = \{1, 2, \dots, n\}$, такое что для любого $S \subseteq [n]$ размера k, семейство $\{A \cap S | A \in \mathcal{U}\}$ содержит все 2^k подмножеств S.

Theorem

Для любых $n, k \geq 1$ можно построить (n,k)-универсальное множество размера $2^k k^{O(\log k)} n \log n$

Problem

Дерандомизировать алгоритм для Изоморфизма Подграфов.

k-независимость

Definition

Семейство $H_{n,k,q}$ функций из $[n] = \{1, 2, \ldots, n\}$ в $[q] = \{1, 2, \ldots, q\}$ называется *k-независимым (k-wise independent sample space)*, если для любых $1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n$ и набора $\alpha \in [q]^k$, выполняется:

$$Pr((f(i_1), f(i_2), \ldots, f(i_k)) = \alpha) = q^{-k},$$

где функция $f \in H_{n,k,q}$ выбирается случайно (равновероятно).

Theorem

Существует k-независимое семейство $H_{n,k,q}$ размера $O(n^k)$ и оно может быть сгенерировано за линейное время от размера выхода.

k-независимость

Definition

Семейство $H_{n,k,q}$ функций из $[n] = \{1, 2, \ldots, n\}$ в $[q] = \{1, 2, \ldots, q\}$ называется *k-независимым (k-wise independent sample space)*, если для любых $1 \le i_1 \le i_2 \le \cdots \le i_k \le n$ и набора $\alpha \in [q]^k$, выполняется:

$$Pr((f(i_1), f(i_2), \ldots, f(i_k)) = \alpha) = q^{-k},$$

где функция $f \in H_{n,k,q}$ выбирается случайно (равновероятно).

Theorem

Существует k-независимое семейство $H_{n,k,q}$ размера $O(n^k)$ и оно может быть сгенерировано за линейное время от размера выхода.

Цветное семейство

Definition

(n, k, q)-цветное семейство (coloring family) — это семейство $\mathcal{F}$ функций из $[n]$ в $[k]$ со следующим свойством: для любого графа G с множеством вершин $[n]$, с не более k вершинами, существует функция $f \in \mathcal{F}$ которая правильно красит $E(G)$.

Для решения задачи о d-кластеризации, достаточно построить цветное семейство.

Theorem

Для любоых $n, k \geq 1$ существует $(n, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно посторить за линейное время от его размера.

Цветное семейство

Definition

(n,k,q)-цветное семейство (coloring family) — это семейство $\mathcal{F}$ функций из $[n]$ в $[k]$ со следующим свойством: для любого графа G с множеством вершин $[n]$, с не более k вершинами, существует функция $f \in \mathcal{F}$ которая правильно красит $E(G)$.

Для решения задачи о d-кластеризации, достаточно построить цветное семейство.

Theorem

Для любоых $n, k \geq 1$ существует $(n, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно посторить за линейное время от его размера.

Цветное семейство

Definition

(n,k,q)-цветное семейство (coloring family) — это семейство $\mathcal{F}$ функций из $[n]$ в $[k]$ со следующим свойством: для любого графа G с множеством вершин $[n]$, с не более k вершинами, существует функция $f \in \mathcal{F}$ которая правильно красит $E(G)$.

Для решения задачи о d-кластеризации, достаточно построить цветное семейство.

Theorem

Для любоых $n, k \geq 1$ существует $(n, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно посторопить за линейное время от его размера.

Доказательство

Theorem

Для любого $k \geq 1$ *существует* $(k^2, k, 2\sqrt{k})$*-цветное семейство* $\mathcal{F}$ *размера* $2^{O(\sqrt{k}\log k)}$. *Более того такое семейство можно постороить за линейное время от его размера.*

Доказательство.

- Положим $q = \sqrt{k}$.
- Рассмотрим 2-независимое семейство функций $\mathcal{G} := H_{k^2,2,q}$.
- Размер $\mathcal{G}$ равен $O(k^4)$, $\forall g \in \mathcal{G}$, $g : [k^2] \to [q]$.
- Для любого $T \subseteq [k^2]$ размера q построим функцию перекрашивающую элементы T.
- $\binom{k^2}{q} = 2^{O(\sqrt{k}\log k)}$.

$\square$

Доказательство

Theorem

Для любого $k \geq 1$ существует $(k^2, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно постороить за линейное время от его размера.

Доказательство.

- Положим $q = \sqrt{k}$.
- Рассмотрим 2-независимое семейство функций $\mathcal{G} := H_{k^2,2,q}$.
- Размер $\mathcal{G}$ равен $O(k^4)$, $\forall g \in \mathcal{G}$, $g : [k^2] \to [q]$.
- Для любого $T \subseteq [k^2]$ размера q построим функцию перекрашивающую элементы T.
- $\binom{k^2}{q} = 2^{O(\sqrt{k}\log k)}$.

□

Доказательство

Theorem

Для любого $k \geq 1$ существует $(k^2, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно посторoить за линейное время от его размера.

Доказательство.

- Положим $q = \sqrt{k}$.
- Рассмотрим 2-независимое семейство функций $\mathcal{G} := H_{k^2,2,q}$.
- Размер $\mathcal{G}$ равен $O(k^4)$, $\forall g \in \mathcal{G}$, $g : [k^2] \to [q]$.
- Для любого $T \subseteq [k^2]$ размера q построим функцию перекрашивающую элементы T.
- $\binom{k^2}{q} = 2^{O(\sqrt{k}\log k)}$.

Доказательство

Theorem

Для любого $k \geq 1$ существует $(k^2, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно постороить за линейное время от его размера.

Доказательство.

- Положим $q = \sqrt{k}$.
- Рассмотрим 2-независимое семейство функций $\mathcal{G} := H_{k^2,2,q}$.
- Размер $\mathcal{G}$ равен $O(k^4)$, $\forall g \in \mathcal{G}$, $g : [k^2] \to [q]$.
- Для любого $T \subseteq [k^2]$ размера q построим функцию перекрашивающую элементы T.
- $\binom{k^2}{q} = 2^{O(\sqrt{k}\log k)}$.

Доказательство

Theorem

Для любого $k \geq 1$ существует $(k^2, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно постороить за линейное время от его размера.

Доказательство.

- Положим $q = \sqrt{k}$.
- Рассмотрим 2-независимое семейство функций $\mathcal{G} := H_{k^2,2,q}$.
- Размер $\mathcal{G}$ равен $O(k^4)$, $\forall g \in \mathcal{G}$, $g : [k^2] \to [q]$.
- Для любого $T \subseteq [k^2]$ размера q построим функцию перекрашивающую элементы T.
- $\binom{k^2}{q} = 2^{O(\sqrt{k}\log k)}$.

□

Доказательство

Theorem

Для любого $k \geq 1$ существует $(k^2, k, 2\sqrt{k})$-цветное семейство $\mathcal{F}$ размера $2^{O(\sqrt{k}\log k)}$. Более того такое семейство можно постороить за линейное время от его размера.

Доказательство.

- Положим $q = \sqrt{k}$.
- Рассмотрим 2-независимое семейство функций $\mathcal{G} := H_{k^2,2,q}$.
- Размер $\mathcal{G}$ равен $O(k^4)$, $\forall g \in \mathcal{G}$, $g : [k^2] \to [q]$.
- Для любого $T \subseteq [k^2]$ размера q построим функцию перекрашивающую элементы T.
- $\binom{k^2}{q} = 2^{O(\sqrt{k}\log k)}$.

$\square$

Thank you for your attention!