Случайный шум увеличивает колмогоровскую сложность

alexander.shen@lirmm.fr, www.lirmm.fr/~ashen,
Глеб Пособин
(и Петер Гач)

LIRMM CNRS & University of Montpellier, supported by ANR RaCAF

13 ноября 2019, семинар кафедры

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ

  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) \colon d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Уменьшение сложности при изменении битов

- пусть дано $x \in \mathbb{B}^n$ сложности $\mathrm{KS}(x) < n$
- $\mathrm{KS}(x) = \alpha n$
- изменим небольшую часть битов x
- что будет с $\mathrm{KS}(x)$?
- насколько может уменьшиться или вырасти?
- уменьшение: $\min\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$ как функция τ
  $d(x,y)$: расстояние Хемминга (число изменённых битов)
- τn-шары: минимальная сложность элементов
- зависит не только $\mathrm{KS}(x)$, но и от других свойств x
- алгоритмическая статистика для ограниченных семейств описаний (Верещагин, Витаньи)
- два случая:
  - [случайные биты]$000\ldots000$
  - случайное слово кода с исправлением ошибок

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x, y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x, y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Увеличение сложности при изменении битов

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем τ-долю битов: $d(x,y) \leqslant \tau n$
- всегда ли можно увеличить сложность?
- $\tau \mapsto \max\{\mathrm{KS}(y) : d(x,y) \leqslant \tau n\}$
- Buhrman, Fortnow, Newman, Vereshchagin: $\Omega(n)$ да, всегда
- гарантированно возможное увеличение зависит от x
- открытый вопрос: какие функции тут возможны?
- максимально возможное увеличение: кодовые слова
- BFNV: минимально возможное увеличение (для бернуллиевых слов)
- комбинаторная сущность: теорема Харпера о минимальной окрестности для шаров Хемминга

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- “случайный шум” понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ — распределение Бернулли
- “случайный шум” понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Случайный шум: как влияет на сложность?

- $x \in \mathbb{B}^n$, $\mathrm{KS}(x) = \alpha n$
- изменяем случайную τ-долю битов
- лучше: меняем каждый бит с вероятностью τ (независимо)
- $N_\tau(x)$: шум с параметром τ добавлен к x
  $N_\tau(x) = x \oplus B_\tau$, где B_τ – распределение Бернулли
- "случайный шум" понимаем вероятностно
- $\mathrm{KS}(N_\tau(x))$: случайная величина
- concentration inequalities: для каждого x эта величина близка к некоторому типичному значению
- сложность с большой вероятностью увеличивается
- точная нижняя оценка этого увеличения

Сложность увеличивается почти наверняка

Теорема

Пусть $\alpha \in (0,1)$ *и* $\tau \in (0,1/2)$. *Существует* $\beta > \alpha$, *для которого*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n] \geqslant 1 - \frac{1}{n}$$

при любом достаточно большом n *и любом* x *длины* n.

режим: α, β, τ фиксированы, $n \to \infty$

β зависит от α и τ

есть разные комбинаторные рассуждения но они не дают оптимальной оценки для β

$1/n$ можно заменить на $1/n^d$ для любой константы d

Сложность увеличивается почти наверняка

Теорема

Пусть $\alpha \in (0,1)$ *и* $\tau \in (0,1/2)$. *Существует* $\beta > \alpha$, *для которого*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n] \geqslant 1 - \frac{1}{n}$$

при любом достаточно большом n *и любом* x *длины* n.

режим: α, β, τ фиксированы, $n \to \infty$

β зависит от α и τ

есть разные комбинаторные рассуждения но они не дают оптимальной оценки для β

$1/n$ можно заменить на $1/n^d$ для любой константы d

Сложность увеличивается почти наверняка

Теорема

Пусть $\alpha \in (0,1)$ *и* $\tau \in (0,1/2)$. *Существует* $\beta > \alpha$, *для которого*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n] \geqslant 1 - \frac{1}{n}$$

при любом достаточно большом n *и любом* x *длины* n.

режим: α, β, τ фиксированы, $n \to \infty$

β зависит от α и τ

есть разные комбинаторные рассуждения но они не дают оптимальной оценки для β

$1/n$ можно заменить на $1/n^d$ для любой константы d

Сложность увеличивается почти наверняка

Теорема

Пусть $\alpha \in (0,1)$ *и* $\tau \in (0,1/2)$. *Существует* $\beta > \alpha$, *для которого*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n] \geqslant 1 - \frac{1}{n}$$

при любом достаточно большом n *и любом* x *длины* n.

режим: α, β, τ фиксированы, $n \to \infty$

β зависит от α и τ

есть разные комбинаторные рассуждения но они не дают оптимальной оценки для β

$1/n$ можно заменить на $1/n^d$ для любой константы d

Сложность увеличивается почти наверняка

Теорема

Пусть $\alpha \in (0,1)$ и $\tau \in (0,1/2)$. Существует $\beta > \alpha$, для которого

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n] \geqslant 1 - \frac{1}{n}$$

при любом достаточно большом n и любом x длины n.

режим: α, β, τ фиксированы, $n \to \infty$

β зависит от α и τ

есть разные комбинаторные рассуждения но они не дают оптимальной оценки для β

$1/n$ можно заменить на $1/n^d$ для любой константы d

Сложность увеличивается почти наверняка

Теорема

Пусть $\alpha \in (0,1)$ *и* $\tau \in (0,1/2)$. *Существует* $\beta > \alpha$, *для которого*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n] \geqslant 1 - \frac{1}{n}$$

при любом достаточно большом n *и любом* x *длины* n.

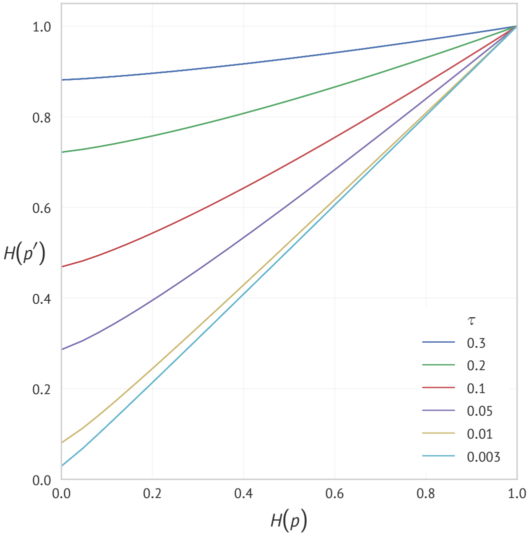
режим: α, β, τ фиксированы, $n \to \infty$

β зависит от α и τ

есть разные комбинаторные рассуждения но они не дают оптимальной оценки для β

$1/n$ можно заменить на $1/n^d$ для любой константы d

Оптимальная оценка



Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- log(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$$

  – энтропия Шеннона для распределения $(p, 1-p)$

- если B_p – распределение Бернулли с вероятностью p, то
  $N_\tau(B_p) = B_{N(p,\tau)}$
  $N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- $\log$(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$$

  – энтропия Шеннона для распределения $(p, 1-p)$
- если B_p – распределение Бернулли с вероятностью p, то
  $N_\tau(B_p) = B_{N(p,\tau)}$
  $N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- log(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$$

  – энтропия Шеннона для распределения $(p, 1-p)$
- если B_p – распределение Бернулли с вероятностью p, то
  $N_\tau(B_p) = B_{N(p,\tau)}$
  $N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- log(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p \log \frac{1}{p} + (1-p)\log \frac{1}{1-p}$$

  – энтропия Шеннона для распределения $(p, 1-p)$
- если B_p – распределение Бернулли с вероятностью p, то
  $N_\tau(B_p) = B_{N(p,\tau)}$
  $N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- log(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$$

– энтропия Шеннона для распределения $(p, 1-p)$

- если B_p – распределение Бернулли с вероятностью p, то
$N_\tau(B_p) = B_{N(p,\tau)}$
$N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- $\log$(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$$

  – энтропия Шеннона для распределения $(p, 1-p)$
- если B_p – распределение Бернулли с вероятностью p, то
  $N_\tau(B_p) = B_{N(p,\tau)}$
  $N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Типичная сложность B_τ

- $N_\tau(0^n) = B_\tau$
- $\approx$ сложность случайного слова длины n с τn единиц
- log(количество таких слов)
- $\log_n : \tau n = 2^{H(\tau)n}$, где

$$H(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$$

  – энтропия Шеннона для распределения$(p, 1-p)$
- если B_p – распределение Бернулли с вероятностью p, то
  $N_\tau(B_p) = B_{N(p,\tau)}$
  $N(p,\tau) = p(1-\tau) + (1-p)\tau$
- увеличение сложности $H(p) \mapsto H(N(p,\tau))$

Оптимальная оценка

Теорема

Пусть $p \in (0, 1/2)$ *и* $\tau \in (0, 1/2)$.
Пусть $\alpha = H(p)$ *и* $\beta = H(N(\tau, p))$. *Then*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n - o(n)] \geqslant 1 - \frac{1}{n}$$

при $n \to \infty$ *и при любом* x *длины* n. *Эта оценка неулучшаема*

(нельзя улучшить сразу для всех x; для некоторых сложность увеличивается сильнее)

Оптимальная оценка

Теорема

Пусть $p \in (0,1/2)$ *и* $\tau \in (0,1/2)$.
Пусть $\alpha = H(p)$ *и* $\beta = H(N(\tau,p))$. *Then*

$$\mathrm{KS}(x) \geqslant \alpha n \Rightarrow \Pr[\mathrm{KS}(N_\tau(x)) \geqslant \beta n - o(n)] \geqslant 1 - \frac{1}{n}$$

при $n \to \infty$ *и при любом* x *длины* n. *Эта оценка неулучшаема*

(нельзя улучшить сразу для всех x; для некоторых сложность увеличивается сильнее)

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Три подхода

- Колмогоров (1965): комбинаторный, алгоритмический, вероятностный
- комбинаторный: указание элемента среди N требует $\log N$ битов
- алгоритмический: $\mathrm{KS}(x)$, минимальная длина программы для x
- вероятностный: энтропия Шеннона
- измеряют разное и по-разному, но тесно связаны
- BFNV: связь между комбинаторным и вероятностным
- нам пригодятся все три

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

Подробнее о BFNV

- (сложностной) если слово длины n имеет сложность $\geqslant \alpha n$, то можно изменить не более τn битов и получить слово сложности $\geqslant \beta n$
- (комбинаторный) для всякого множеств из $2^{\beta n}$ слов длины n его τn-внутренность имеет не более $2^{\alpha n}$ элементов
  (вариант:) любое множество размера не меньше $2^{\alpha n}$ имеет τn-окрестность не меньше $2^{\beta n}$.
- d-окрестность X: все слова на расстоянии не больше d от X (объединение d-шаров)
- d-внутренность X: все слова y, содержащиеся в X вместе с d-шаром
- теорема Харпера: минимальная окрестность и максимальная внутренность у шаров Хемминга

комбинаторный ⇒ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит ...
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный ⇒ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит …
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный ⇒ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит ...
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный $\Rightarrow$ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит …
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный $\Rightarrow$ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит …
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный ⇒ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит …
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный $\Rightarrow$ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит ...
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный $\Rightarrow$ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит …
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

комбинаторный $\Rightarrow$ сложностной

- пусть мы знаем, что множества размера $\leqslant 2^{\beta n}$ всегда имеют внутренность не больше $2^{\alpha n}$
- применим к множеству X слов длины n и сложности не больше βn
- $|X| \leqslant 2^{\beta n}$
- поэтому τn-внутренность содержит не более $2^{\alpha n}$ элементов
- и перечислима по n, βn, τn
- поэтому все её элементы сложности не больше $\alpha n + O(\log n)$ (с логарифмической точностью)
- поэтому слово сложности $> \alpha n + O(\log n)$ в ней *не* лежит ...
- то есть может быть изменено не более чем в τn местах и выйдет из X, сложность станет больше βn

сложностной $\Rightarrow$ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

сложностной $\Rightarrow$ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

сложностной $\Rightarrow$ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

сложностной $\Rightarrow$ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

сложностной ⇒ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

сложностной ⇒ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

сложностной $\Rightarrow$ комбинаторный

- пусть мы знаем, что всякое слово сложности $\geqslant \alpha n$ может быть изменено в $\leqslant \tau n$ и получится слово сложности $\geqslant \beta n$
- а комбинаторное утверждение неверно: есть множество X из $2^{\beta n}$ слов длины n с τn-внутренностью сильно больше $2^{\alpha n}$
- пусть X первое такое множество
- все его элементы имеют сложность не больше βn (с логарифмической точностью)
- и потому все элементы его внутренности имеют сложность не больше αn
- но их слишком много: противоречие

Случайный шум

- (шенноновский) пусть P — распределение вероятностей на словах длины n. Если $H(P) \geqslant \alpha n$, то $H(N_\tau(P)) \geqslant \beta n$.
- (сложностной) если $\mathrm{KS}(x) \geqslant \alpha n$, то $\mathrm{KS}(N_\tau(x)) \geqslant \beta n$ с вероятностью не меньше $1 - \frac{1}{n}$
- (комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $\frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$
- (слабый комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $1 - \frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$

Все варианты эквивалентны (с $o(n)$-точностью для границ сложности и логарифма размера)

Случайный шум

- (шенноновский) пусть P – распределение вероятностей на словах длины n. Если $H(P) \geqslant \alpha n$, то $H(N_\tau(P)) \geqslant \beta n$.
- (сложностной) если $\mathrm{KS}(x) \geqslant \alpha n$, то $\mathrm{KS}(N_\tau(x)) \geqslant \beta n$ с вероятностью не меньше $1 - \frac{1}{n}$
- (комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $\frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$
- (слабый комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $1 - \frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$

Все варианты эквивалентны (с $o(n)$-точностью для границ сложности и логарифма размера)

Случайный шум

- (шенноновский) пусть P — распределение вероятностей на словах длины n. Если $H(P) \geqslant \alpha n$, то $H(N_\tau(P)) \geqslant \beta n$.
- (сложностной) если $\mathrm{KS}(x) \geqslant \alpha n$, то $\mathrm{KS}(N_\tau(x)) \geqslant \beta n$ с вероятностью не меньше $1 - \frac{1}{n}$
- (комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $\frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$
- (слабый комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $1 - \frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$

Все варианты эквивалентны (с $o(n)$-точностью для границ сложности и логарифма размера)

Случайный шум

- (шенноновский) пусть P — распределение вероятностей на словах длины n. Если $H(P) \geqslant \alpha n$, то $H(N_\tau(P)) \geqslant \beta n$.
- (сложностной) если $\mathrm{KS}(x) \geqslant \alpha n$, то $\mathrm{KS}(N_\tau(x)) \geqslant \beta n$ с вероятностью не меньше $1 - \frac{1}{n}$
- (комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $\frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$
- (слабый комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $1 - \frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$

Все варианты эквивалентны (с $o(n)$-точностью для границ сложности и логарифма размера)

Случайный шум

- (шенноновский) пусть P — распределение вероятностей на словах длины n. Если $H(P) \geqslant \alpha n$, то $H(N_\tau(P)) \geqslant \beta n$.
- (сложностной) если $\mathrm{KS}(x) \geqslant \alpha n$, то $\mathrm{KS}(N_\tau(x)) \geqslant \beta n$ с вероятностью не меньше $1 - \frac{1}{n}$
- (комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $\frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$
- (слабый комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $1 - \frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$

Все варианты эквивалентны (с $o(n)$-точностью для границ сложности и логарифма размера)

Случайный шум

- (шенноновский) пусть P — распределение вероятностей на словах длины n. Если $H(P) \geqslant \alpha n$, то $H(N_\tau(P)) \geqslant \beta n$.
- (сложностной) если $\mathrm{KS}(x) \geqslant \alpha n$, то $\mathrm{KS}(N_\tau(x)) \geqslant \beta n$ с вероятностью не меньше $1 - \frac{1}{n}$
- (комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $\frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$
- (слабый комбинаторный) если $|B| \leqslant 2^{\beta n}$, и всякий элемент A имеет вероятность попасть в B после τ-шума не меньше $1 - \frac{1}{n}$, то $|A| \leqslant 2^{\alpha n}$

Все варианты эквивалентны (с $o(n)$-точностью для границ сложности и логарифма размера)

Доказательство эквивалентности

- сложностной $\Longleftrightarrow$ комбинаторный: как раньше
- сложностной $\Rightarrow$ вероятностный: случайные независимые копии почти наверняка имеют сложность, близкую к шенноновской энтропии
- вероятностный $\Rightarrow$ слабый комбинаторный: энтропия не больше средней длины кода, а предположение даёт эффективное кодирование
- слабый комбинаторный $\Rightarrow$ комбинаторный: concentration inequalities (неравенство МакДиармида, следствие неравенства Азумы – Хёфдинга)

Доказательство эквивалентности

- сложностной $\Leftrightarrow$ комбинаторный: как раньше
- сложностной $\Rightarrow$ вероятностный: случайные независимые копии почти наверняка имеют сложность, близкую к шенноновской энтропии
- вероятностный $\Rightarrow$ слабый комбинаторный: энтропия не больше средней длины кода, а предположение даёт эффективное кодирование
- слабый комбинаторный $\Rightarrow$ комбинаторный: concentration inequalities (неравенство МакДиармида, следствие неравенства Азумы – Хёфдинга)

Доказательство эквивалентности

- сложностной $\Leftrightarrow$ комбинаторный: как раньше
- сложностной $\Rightarrow$ вероятностный: случайные независимые копии почти наверняка имеют сложность, близкую к шенноновской энтропии
- вероятностный $\Rightarrow$ слабый комбинаторный: энтропия не больше средней длины кода, а предположение даёт эффективное кодирование
- слабый комбинаторный $\Rightarrow$ комбинаторный: concentration inequalities (неравенство МакДиармида, следствие неравенства Азумы – Хёфдинга)

Доказательство эквивалентности

- сложностной $\Leftrightarrow$ комбинаторный: как раньше
- сложностной $\Rightarrow$ вероятностный: случайные независимые копии почти наверняка имеют сложность, близкую к шенноновской энтропии
- вероятностный $\Rightarrow$ слабый комбинаторный: энтропия не больше средней длины кода, а предположение даёт эффективное кодирование
- слабый комбинаторный $\Rightarrow$ комбинаторный: concentration inequalities (неравенство МакДиармида, следствие неравенства Азумы – Хёфдинга)

Доказательство эквивалентности

- сложностной $\Leftrightarrow$ комбинаторный: как раньше
- сложностной $\Rightarrow$ вероятностный: случайные независимые копии почти наверняка имеют сложность, близкую к шенноновской энтропии
- вероятностный $\Rightarrow$ слабый комбинаторный: энтропия не больше средней длины кода, а предположение даёт эффективное кодирование
- слабый комбинаторный $\Rightarrow$ комбинаторный: concentration inequalities (неравенство МакДиармида, следствие неравенства Азумы – Хёфдинга)

Как доказать неравенство для энтропий

- при $n = 1$ это определение:
- $P = B_p$ for some p
- $H(P) = H(p)$
- $H(N_\tau(P)) = H(N(p, \tau))$
- общий случай ("тензоризация" плюс выпуклость)

Как доказать неравенство для энтропий

- при $n = 1$ это определение:
- $P = B_p$ for some p
- $H(P) = H(p)$
- $H(N_\tau(P)) = H(N(p, \tau))$
- общий случай ("тензоризация" плюс выпуклость)

Как доказать неравенство для энтропий

- при $n = 1$ это определение:
- $P = B_p$ for some p
- $H(P) = H(p)$
- $H(N_\tau(P)) = H(N(p, \tau))$
- общий случай ("тензоризация" плюс выпуклость)

Как доказать неравенство для энтропий

- при $n = 1$ это определение:
- $P = B_p$ for some p
- $H(P) = H(p)$
- $H(N_\tau(P)) = H(N(p, \tau))$
- общий случай ("тензоризация" плюс выпуклость)

Как доказать неравенство для энтропий

- при $n = 1$ это определение:
- $P = B_p$ for some p
- $H(P) = H(p)$
- $H(N_\tau(P)) = H(N(p,\tau))$
- общий случай ("тензоризация" плюс выпуклость)

Как доказать неравенство для энтропий

- при $n = 1$ это определение:
- $P = B_p$ for some p
- $H(P) = H(p)$
- $H(N_\tau(P)) = H(N(p, \tau))$
- общий случай ("тензоризация" плюс выпуклость)

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0,n] \times [0,n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0,n] \times [0,n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского

correction: точнее: выше выпуклой оболочки $S_n + S_m$

(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Тензоризация

- пусть P распределение на словах длины n
- $(H(P), H(N_\tau(P))$: какие пары возможны?
- $S_n \subset [0, n] \times [0, n]$

Лемма: $S_{n+m} \subset S_n + S_m$ сумма Минковского
correction: точнее: выше выпуклой оболочки $S_n + S_m$
(базовые неравенства для энтропии)

выпуклость можно проверить для степенных рядов

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1X_2\ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p,\tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1 X_2 \ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p,\tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1 X_2 \ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p, \tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1 X_2 \ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p, \tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1X_2\ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p,\tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1 X_2 \ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p,\tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Следствия для бесконечных последовательностей

- эффективная размерность Хаусдорфа:

$$\dim(X) = \liminf_n \frac{\mathrm{KS}(X_1 X_2 \ldots X_n)}{n}$$

- возрастает, если каждый бит изменить независимо с вероятностью τ:
- если $\dim(X) \geqslant \alpha = H(p)$ то $\dim(N_p(X)) \geqslant H(N(p,\tau))$ с вероятностью 1
- та же самая оптимальная нижняя оценка
- шум может зависеть от позиции, тогда получаем следствие:
- всякая последовательность размерность α может быть изменена в стремящейся к нулю доле позиций так, чтобы получилась α-случайная последовательность. [для слабой случайности: Greenberg et al.]

Спасибо!