Конспект к лекции 6. (Казань, 6 апреля 2017 г.)

15 Экстракторы случайности

В этом параграфе мы обсудим конструкции, позволяющие улучшить «качество» битов, получаемых на выходе случайного генератора. Представим себе, что у нас имеется физическое устройство, по требованию выдающее последовательность из n случайных битов. В идеале нам бы хотелось, чтобы все n битов были независимы и равномерно распределены (т.е., чтобы каждый из 2^n потенциально возможных наборов значений появлялся с вероятностью $1/2^n$). Однако на практике распределение на выходе генератора может немного отличаться от идеального. Значения битов могут быть немного зависимы, вероятности нуля и единицы в каждой из позиций могут немного смещены относительно $1/2$, и т.д. Для некоторых приложений даже небольшое ухудшение качества случайных битов может оказаться критическим. Скажем, если для каждого из n битов, выдаваемых генератором, вероятности появления нуля и единицы равны 0.499 и 0.501 соответственно (вместо ожидаемого симметричного распределения с вероятностями $1/2$), то в последовательности «случайных» битов длиной в неколько миллионов частоты нулей и единиц будут довольно заметно отличаться от ожидаемых 50%. В результате некоторые вероятностные алгоритмы, хорошо работающие на «идеальных» случайных битах, могут давать неожиданно большую вероятность ошибки при использовании «смещённых» случайных битов.

Тем не менее, интуитивно кажется ясным, что даже немного «смещённые» случайные биты содержат в себе большую неопределённость. Нельзя ли каким-то образом выделить полезную случайность и превратить «смещённые» случайные биты в «почти идеальные»? Мы покажем, что в некотором смысле это оказывается возможным. Чтобы уточнить данное утверждение, нам придётся дать некоторые формальные определения. Мы должны пояснить, какие именно распределения вероятностей считаются «не очень сильно смещёнными», и какие распределения можно называть «почти идеальными».

Определение 15.1 *Говорят, что* min-*энтропия случайной величины X равна k, если*

$$\max_a \mathrm{Prob}[X = a] = 2^{-k}$$

(*максимум берётся среди всех значений a случайной велиичны X*).

Именно распределения с большой min-энтропией мы будем считать «несильно смещённым» и «достаточно качественными». Рассмотрим несколько несложных примеров:

- Если случайная величина X равномерно распределена на $\{0,1\}^n$, то min-энтропия X равна n (каждое из 2^n возможных значений имеет вероятность $1/2^n$). Отметим, что у *любого* распределения на $\{0,1\}^n$

min-энтропия не превосходит n, так что равномерное распределение достигает экстремального значения min-энтропии.

- Если случайная величина X равномерно распределена на множестве всех n-битных строк, содержащих чётное число единиц, то min-энтропия X равна $n-1$ (имеется 2^{n-1} возможных значений, и вероятность каждого из них равна $1/2^{-(n-1)}$).

- Если $X = (X^{(1)} \dots X^{(n)})$ есть последовательность независимых одинаково распределённых двоичных случайных величин, и для каждого $i = 1, \dots, n$
$$\begin{cases} \mathrm{Prob}[X^{(i)} = 0] = \frac{1}{2} - \delta, \\ \mathrm{Prob}[X^{(i)} = 1] = \frac{1}{2} + \delta, \end{cases}$$
то min-энтропия X равна
$$\log\left(\frac{1}{(\frac{1}{2}+\delta)^k}\right) = -k\log\left(\frac{1}{2}+\delta\right) = k(1-\Theta(\delta))$$
(среди всех возможных значений максимальную вероятность имеет последовательность $11\dots1$ — последовательность из одних единиц).

Далее мы уточним, какие распредления естественно считать «почти идеальными» (для всевозможных практических применений).

Определение 15.2 *Распределение вероятностей $X = (X_1, \dots, X_n)$ на $\{0,1\}^n$ считается ε-близим к равномерному, если для любого $A \subset \{0,1\}^n$*
$$\left|\mathrm{Prob}[X \in A] - \frac{|A|}{2^n}\right| \leqslant \varepsilon.$$

Упражнение 15.1 *Предположим, что некоторый вероятностный алгоритм $\mathcal{A}$ при использовании набора из n «идеальных» (независимых и равномерно распределённых) случайных битов на каждом входе ошибается с вероятностью не более δ. Докажите, что при использовании неидеального, но ε-близого к равномерному источника случайности, данный алгоритм будет ошибаться с вероятностью не более $\varepsilon + \delta$.*

Упражнение 15.2 *Покажите, что ε-близость к равномерному распределению означает, что распределение X удалено от равномерного распределения на расстояние не более 2ε в смысле l_1-нормы. Другими словами, распредление $X = (X_1, \dots, X_n)$ является ε-близим к равномерному, если и только если*
$$\sum_{(i_1,\dots,i_n)\in\{0,1\}^n} \left|\mathrm{Prob}[X = (i_1, \dots, i_n)] - \frac{1}{2^n}\right| \leqslant 2\varepsilon.$$

Далее мы дадим определения *экстрактора случайности* — схемы, позволяющей превратить набор неидеальных случайных битов с большой min-энтропией в «почти идеальные» биты. При этом экстрактору потребуется в качестве «затравки» небольшое число по-настоящему идеальных случайных битов.

Определение 15.3 *Экстрактором с параметрами* $(n, m, k, t, \varepsilon)$ *называется отображение*

$$Ext \ : \ \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$$

такое, что для всякого распределения $X = (X_1, \ldots, X_n)$ *с* min*-энтропией* $\geqslant k$ *и для равномерно распределенной (независимой с* X*) случайной величины* $Y = (Y_1, \ldots, Y_t)$ *получаемое распределение значений* $Ext(X, Y)$ *оказывается* ε*-близким к равномерному.*

Теорема 15.1 *Для бесконечно многих* n*, для всех* $k \leqslant n$ *и всех* $\varepsilon < 1$ *существует полиномиально вычислимый экстрактор* Ext *с параметрами* $(n, m = n, k, t = O(n - k + \log \frac{1}{\varepsilon}), \varepsilon)$.

Замечание: Предлагаемое ниже доказательство использует спектральный экспандер на 2^n вершинах. Используя конструкцию из лекции 4, мы можем построить такие экспандеры не просто для *бесконечно многих* n, а для некоторой последовательности чисел n, образующих геометрическую прогрессию (см. замечание в конце главы 4).

Доказательство теоремы. Прежде всего опишем конструкцию экстрактора $Ext(X, Y)$. Зафиксируем некоторый спектральный экспандер с параметрами

$$(2^n, d = O(1), \gamma < 1).$$

Отображение Ext будет устроено следующим образом. С помощью случайной величины X (распределённой на наборах из n нулей и единиц, с min-энтропией не менее k) выбираем случайную вершину экспандера. Далее с помощью случайной величины Y организуем случайное блуждание на экспандере, начинающееся в выбранной вершине: t битов «идеально распределённой» величины Y позволяют нам выбрать случайный путь длины

$$T = t/(\log d)$$

по рёбрам графа. Последнюю вершину этого пути (точнее, её n-битный индекс) мы и возвращаем в качестве значения $Ext(X, Y)$.

Покажем, что получаемое в результате распределение достаточно близко к равномерному. Для начала измерим «близость» с помощью l_2-нормы. Обозначим $\mathbf{p}^{(i)}$ распределение вероятностей на вершинах графа после i-го шага блуждания. В частности, $\mathbf{p}^{(0)}$ совпадает с исходным распределением X, а $\mathbf{p}^{(T)}$ есть итоговое распределение $Ext(X, Y)$. Далее, обозначим $\hat{M}$ нормализованную матрицу экспандера.

По определению спектрального экспандера, операторная норма $\hat{M}$ на подпространстве векторов, ортогональных собственному вектору $(1, 1, \ldots, 1)$, равна γ. Это значит, что при каждом умножении на $\hat{M}$ норма разности $\|p^{(i)} - (\frac{1}{2^n}, \frac{1}{2^n}, \ldots, \frac{1}{2^n})\|$ уменьшается не менее, чем в γ раз. Таким образом,

$$\|p^{(T)} - (\frac{1}{2^n}, \ldots, \frac{1}{2^n})\| \leqslant \gamma^T \cdot \|p^{(0)} - (\frac{1}{2^n}, \ldots, \frac{1}{2^n})\| \leqslant \gamma^T \cdot \left(\|p^{(0)}\| + \|(\frac{1}{2^n}, \ldots, \frac{1}{2^n})\| \right).$$

При этом $\|(\frac{1}{2^n}, \ldots, \frac{1}{2^n})\| = 2^{-n/2}$, а

$$\|p^{(0)}\| = \sqrt{\sum_{i=1}^{n} \left(p_i^{(0)}\right)^2} \leqslant \sqrt{\frac{1}{2^k} \cdot \sum_{i=1}^{n} p_i^{(0)}} = 2^{-k/2}$$

(здесь мы воспользовались тем, что исходное распределение X на вершинах графа имеет min-энтропию k). Следовательно,

$$\|p^{(T)} - (\frac{1}{2^n}, \ldots, \frac{1}{2^n})\| \leqslant \gamma^T \cdot (2^{-k/2} + 2^{-n/2}).$$

Остаётся сравнить l_0 и l_1 нормы:

$$\left\|p^{(T)} - (\frac{1}{2^n}, \ldots, \frac{1}{2^n})\right\|_0 \leqslant \sqrt{2^n} \cdot \left\|p^{(T)} - (\frac{1}{2^n}, \ldots, \frac{1}{2^n})\right\| \leqslant \gamma^T \cdot 2^{n/2}(2^{-k/2} + 2^{-n/2}).$$

Теперь подберём такое T, чтобы правая часть неравенства оказалась меньше ε. Легко проверить, что достаточно взять $T = O(n - k + \log \frac{1}{\varepsilon})$. Таким образом, теорема доказана.

16 Надёжные схемы из функциональных элементов

В этом параграфе мы обсуждаем задачу построения надёжных схем из функциональных элементов. Мы предполагаем, что читатель знаком с понятием схемы из функциональных элементов, вычисляющей булеву функцию $f : \mathbb{B}^n \to \mathbb{B}$. Мы будем предполагать, что зафиксирован некоторый конечный *полный базис* булевых функций B, и каждой внутренней вершине схемы сопоставляется некоторая функция $g \in B$, причём арность g совпадает с входной степенью вершины (строго говоря, нужно ещё зафиксировать соответствие между входящими рёбрами и аргументами g). Входным вершинам схемы (вершинам с входной степенью 0) сопоставляются булевы переменные $x_1, \ldots, x_n$ (аргументы функции, которую должна вычислять схема).

Пусть задана схема из N функциональных элементов, вычисляющая некоторую функцию $f : \mathbb{B}^n \to \mathbb{B}$. Рассмотрим работу данной схемы *с ошибками*. Будем предполагать, что каждый из функциональных элементов независимо от других элементов (и от входов схемы) с некоторой вероятностью ε «портится», становится «неисправным». Будем называть данное распределение сбоев *ε-случайным*. При этом мы не предполагаем, что испорченные функциональные элементы *непременно* возвращают неверное значение (т.е., логическое отрицание правильного результата вычислений для заданных аргументов). Мы считаем поведение испорченного элемента непредсказуемым — он может возвращать и правильные, и неправильные значения. Можно полагать, что все неисправные элементы схемы переходят во власть злонамеренного противника, который по своему произволу

определяет их выходы. При этом выходы на остальных (исправных) функциональных элементах определяются по обычным правилам.

Определение 16.1 *Схема из функциональных элементов (ε, δ)-надёжно вычисляет функцию f, если для любого набора входных значений, при ε-случайном выборе элементов, в которых возникает неисправность, с вероятностью не менее $(1-\delta)$ схема выдаёт правильное значение функции, как бы ни действовал противник.*

Теорема 16.1 *Для произвольного полного базиса булевых функций B, для всех достаточно малых ε найдётся $\delta = O(\varepsilon)$ такое, что всякая булева функция может быть вычислена (ε, δ)-надёжной схемой в данном базисе.*

Доказательство: Прежде всего заметим, что если теорема верна для одного полного базиса, то она обязана выполняться и для любого другого базиса, быть может с несколько другим соотношениеммежду ε и δ (поскольку функциональные элементы из первого базиса можно моделировать блоками ограниченного размера, составленными из функциональных элементов второго базиса). Без ограничения общности мы можем считать, что наш базис состоит из всех булевых функций трёх аргументов. Мы покажем, что любую обычную булеву схему можно переделать в (ε, δ)-надёжную. Доказательство проведём индукцией по глубине формулы.

Итак, пусть выход (обычной) булевой схемы вычисляется применением функционального элемента b к тройке значений f_1, f_2, f_3. Каждое из значений f_1, f_2, f_3 в свою очередь вычисляются некоторыми подсхемами (быть может, пересекающимися). Глубина каждой из этих подсхем заведомо меньше, чем глубина всей схемы; поэтому мы можем считать, что для f_1, f_2, f_3 уже имеются (ε, δ)-надёжные схемы T_1, T_2, T_3. Если к выходам схем T_1, T_2, T_3 применить операцию b, то вероятность получить неверный ответ не превосходит $(3\delta + \varepsilon)$ (итоговый результат может оказаться неверным, если хотя бы одно из значений f_i вычислено неправильно или если неисправность возникла в самом элементе b). Назвоём построенную схему R. Чтобы уменьшить вероятность ошибки, мы изготовим три копии схемы R и применим к выходам этих трёх схем функцию большинства. Вероятность того, что и после этого мы получим ошиочный ответ, не превосходит $3(3\delta + \varepsilon)^2 + \varepsilon$ (ошибка должна случиться хотя бы в двух из трех независимых копий схемы R либо в итоговом вычислении большинства). Для малых ε и подходящего $\delta = O(\varepsilon)$ получаем

$$3(3\delta + \varepsilon)^2 + \varepsilon \leqslant \delta,$$

и теорема доказана.

Отметим, что приведённая конструкция может экспоненциально увеличить размер схемы, хотя её глубина увеличивается лишь в константу раз.

Упражнение 16.1 *(а) Докажите,* функцию большинства

$$majority(x_1, \ldots, x_n) = \begin{cases} 1, & \text{если более половины } x_i \text{ равны } 1, \\ 0, & \text{иначе} \end{cases}$$

можно вычислить схемой из функциональных элементов (без случайных ошибок) размера $\mathrm{poly}(n)$ *и глубины* $O(\log n)$.

(б) Докажите, что для всех достаточно малых ε *найдётся* $\delta = O(\varepsilon)$ *такое, что функцию* $majority(x_1, \ldots, x_n)$ *можно вычислить* (ε, δ)*-надёжной схемой размера* $\mathrm{poly}(n)$.

Далее мы докажем более сильный вариант теоремы 16.1:

Теорема 16.2 *Для произвольного полного базиса булевых функций* B*, для всех достаточно малых* ε *найдётся* $\delta = O(\varepsilon)$ *такое, что всякая булева схема* C *из* N *элементов может быть переделана (за время* $\mathrm{poly}(N)$*) в* (ε, δ)*-надёжную схему размера* $O(N \log N)$.

Доказательство: Прежде чем доказывать теорему, введём определение:

Определение 16.2 *Двудольный граф называется* (k, d, α, β)*-компрессором, если*

1. *в левой и правой долях графа содержится по* k *вершин;*
2. *степень каждой вершины равна* d*;*
3. *пусть* A *— произвольное множество вершин левой доли графа, и* $|A| \leqslant \alpha k$*; обозначим* B *множество таких вершин правой доли графа, у которых большинство соседей принадлежат* A*; тогда размер* B *не превосходит* βk.

Лемма 16.1 (о компрессоре) *(а) Если* $4\alpha(\gamma^2 + \alpha) < \beta < 1/2$*, то матрица смежности спектрального* (k, d, γ)*-экспандера задаёт* (k, d, α, β)*-компрессор (двудольный граф с* $2 \times k$ *вершинами также задаётся матрицей* $k \times k$).

(б) Для бесконечно многих[1] k *и для всех достаточно малых* α *существует* (k, d, α, β)*-компрессор для некоторого* $\beta < \alpha/3$*. Более того, такой компрессор может быть построен за полиномиальное время.*

Мы оставим доказательство леммы о компрессоре в качестве упражнения (см. упражнение 16.2 ниже) и покажем, как она помогает доказать теорему. Зафиксируем некоторый параметр k (в последствии мы выберем $k = O(\log N)$). Далее, построим (k, d, α, β)-компрессор такой, что $\beta + Const \cdot \varepsilon < \alpha$ (константа $Const$ не зависит от k и определяется соотношением числа d и базиса, над которым мы строим схему; подробнее значение $Const$ мы обсудим ниже).

[1] На самом деле утверждение верно не просто для *бесконечно многих* k, а для довольно плотного множества занчений k. Чтобы конструкция работала, нам необходимо лишь, чтобы существовал спектральный экспандер на k вершинах. Это означает, в частности, что компрессоры существуют для некоторой последовательности k_i, образующей геометрическую прогрессию (см. замечание в конце главы 4).

Мы преобразовываем заданную нам схему C в эквивалентную ей (ε, δ)-надёжную схему C'. Для этого мы заменим каждый функциональный элемент на некоторый блок из $O(k)$ элементов (устройство такого блока мы сейчас опишем). Если в исходной схеме C выход элемента номер i подавался на вход элементу номер j, то в новой схеме C' от блока номер i к блоку номер j будет идти «кабель» из k проводов. В идеальной ситуации (когда нет ошибок) сигналы во всех проводах этого кабеля будут одинаковы; более того, это будет ровно тот сигнал, который проходил по соответствующему проводу в исходной схеме (при тех же значениях аргументов на входе схемы).

Теперь опишем устройство блока, соответствующего одному из элементов схемы C. Мы объясним конструкцию на простейшем примере: пусть в C присутствовал функциональный элемент конъюнкция; наша задача — построить надёжный блок, успешно моделирующий этот функциональный элемент при *умеренном* количестве ошибок. В этот блок будут входить $2k$ сигналов (два кабеля по k проводов). Мы сводим соответствующие провода из этих кабелей (первый с первым, второй со вторым, и т.д.) и для каждой пары вычисляем конъюнкцию. Получаем k результирующих сигналов. Затем пропускаем эти сигналы через *корректор*: это схема с k входами и k выходами; каждый выход вычисляется как *большинство* среди некоторых d входов; а правило, по которому каждому из выходов сопоставляются d входов, есть (k, d, α, β)-компрессор. Отметим, что блок реализуется схемой глубины $O(1)$ и состоит из $O(k)$ функциональных элементов (константы зависят от выбора базиса).

С помощью оценки вероятности больших уклонений (неравенство Чернова) нетрудно показать, что если $k = \Omega(\log N)$, то с большой вероятностью ни в одном из N описанных блоков не случится больше $Const \cdot \varepsilon k$ (число $Const$ определяется глубиной схемы-корректора, т.е. зависит от выбора базиса). Будем называть такое распределение ошибок «типичным».

Оценим число неправильных значений среди k выходов каждого из блоков при типичном распределении ошибок. Мы утверждаем, что доля ошибочных выходов для каждого блока не превосходит $\alpha/3$, где значение α взято из леммы о компрессоре. (Как мы увидим ниже, деление α на 3 соответствует тому, что в нашем базисе есть функциональные схемы с тремы входами.) Говоря формально, это свойство доказывается индукций по максимальному расстоянию от данного блока до входоы схемы. Чтобы обосновать шаг индукции, мы должны доказать следующее свойство: если каждый из входных кабелей блока несет не более αk «неправильных» сигналов (т.е. сигналов, отличных от значения в соответствующем проводе исходной схемы C), то и среди k выходных сигналов не более αk ошибочных. В самом деле, перед применением *корректора* неправильные сигналы обоих входов складываются — их может стать αk. (Напомним, что мы рассматриваем базис из всех булевых функций трёх аргументов; это значит, что в каждый блок вхоит не более трёх кабелей). Затем мы пропускаем сигналы через корректор, и доля ошибок уменьшается до βk. Наконец, нужно учесть ещё $O(\varepsilon k)$ новых ошибок, которые могли произойти внутри самого блоке (в этом

месте важно, что размера блока ограничен $O(k)$). Всего на выходе имеем долю ошибок $\beta + O(\varepsilon)$. Лемма о компрессоре позволяет нам считать, что $\beta + O(\varepsilon) \leqslant \alpha/3$. Таким образом, на выходе блока мы имеем не более $\alpha k/3$ «неправильных» сигналов.

Чтобы закончить конструкцию, нам нужно вычленить из k-жильного кабеля на выходе последнего блока *один* сингнал с ответом. Для этого нам нужно вычислить *большинство* среди значений этих k сигналов. Для этого можно воспользоваться «экспоненциальной» конструкцией из теоремы 16.1 (для (ε, δ)-надёжного вычисления функции большинства среди $k = O(\log N)$ входных значений данный метод даёт схему размера $\mathrm{poly}(\log N) \ll N \log N$, см. упражнение 16.1).

Упражнение 16.2 (Доказательство леммы о компрессоре) *(а) Обозначим M матрицу спектрального (k, α, γ)-экспандера и $\mathbf{f} = (f_1, \ldots, f_k)$ характеристический вектор множества $A \subset \{1, \ldots, n\}$ ($f_i = 1$ в случае $i \in A$, и $f_i = 0$ иначе). Докажите, что если $|A| \leqslant \alpha n$, то*

$$||M\mathbf{f}^{\perp}||^2 \leqslant (\alpha^2 + \alpha\gamma^2)d^2k.$$

(б) Рассмотрим двудольный граф, задаваемый матрицей (k, α, γ)-экспандера. Пусть A — некоторое множество вершин левой доли графа (состоящее из $\leqslant \alpha k$ вершин), задаваемое характеристическим вектором $\mathbf{f}$. Обозначим B множество вершин правой доли графа, соединённых ребром с $\geqslant d/2$ вершинами из A. Докажите, что

$$|B| \leqslant \frac{||M\mathbf{f}||^2}{(d/2)^2}.$$

(в) Докажите лемму 16.1.

Упражнение 16.3 [о типичном распределении неисправностей] Зафиксируем некоторое $\varepsilon < 1/2$.

(а) Известно, что каждый из m функциональных элементов схемы оказывается «неисправным» с вероятностью ε, причём неисправности в разных функциональных элементах случаются независимо друг от друга. Докажите, что одновременная неисправность $\geqslant 2\varepsilon m$ функциональных элементов схемы просходит с вероятностью не более 2^{-cm}. (Величина c зависит от ε).

(б) Пусть некоторая схема из функциональных элементов состоит из N блоков, по $k = C \log N$ функциональных элементов в каждом блоке. Каждый функциональный элемент схемы оказывается «неисправным» с вероятностью ε, и неисправности в разных функциональных элементах случаются независимо друг от друга. Докажите, что при достаточно большом $C = C(\varepsilon)$ можно утверждать, что с вероятностью $> 0{,}99$ в каждом из блоков неисправно не более $2\varepsilon k$ из k функциональных элементов.

(в) Докажите утверждение пункта (б), заменив границу 0,99 на более сильную оценку $1 - O(1/N)$.