САНКТ-ПЕТЕРБУРГСКИЙ
АКАДЕМИЧЕСКИЙ УНВЕРСИТЕТ РАН
КАФЕДРА МАТЕМАТИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Д И С С Е Р Т А Ц И Я

НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ

М А Г И С Т Р А

Монахова Ивана Игоревича

Тема: “Трудные задачи для эвристических аксепторов”

Направление: 010600.68 – Прикладные математика и физика

Магистерская программа:
Математические и информационные технологии

Выполнил студент И.И. Монахов

Руководитель: к.ф.-м.н. Д.М. Ицыксон

Рецензент: к.ф.-м.н., доцент Э.А. Гирш

Санкт-Петербург
2010

Содержание

1 Введение

Основными объектами изучения теории сложности доказательств являются *системы доказательств* для некоторого языка L – вычислимые за полиномиальное время функции, отображающие слова заданного алфавита в множество теорем – элементов языка L [20]. Система доказательств для языка пропозициональных тавтологий называется *пропозициональной* системой доказательств. Например, для резолюционной системы доказательств эта функция отображает резолюционный вывод пустого дизъюнкта из заданного множества дизъюнктов в отрицание исходной, являющейся тавтологией в ДНФ. Система доказательств называется *полиномиально ограниченной*, если у каждой теоремы есть доказательства полиномиальной длины. Существование полиномиально ограниченной пропозициональной системы доказательств эквивалентно $\mathbf{NP} = \mathbf{co\text{-}NP}$. Другими словами, если бы оказалось, что абсолютно все пропозициональные системы доказательств не являются полиномиально ограниченными (то есть для них существуют трудные тавтологии, у которых нет коротких доказательств), тогда выполнялось бы $\mathbf{NP} \neq \mathbf{co\text{-}NP}$, из чего, в частности, следует, $\mathbf{P} \neq \mathbf{NP}$.

На сегодняшний день существует очень много различных систем доказательств. Можно разделять две системы доказательств специально построенными наборами теорем (простыми для первой системы доказательств и трудными для второй). Независимый интерес представляет нахождение трудных наборов теорем для всё более сильных систем доказательств. Уже доказаны различные нижние оценки на размер доказательств во многих системах доказательств, например, [22],[14],[12],[17] и пр.

Пусть для каждой теоремы языка L длина кратчайшего доказательства в системе доказательств Π ограничена полиномом от длины любого доказательства в системе доказательств Π', тогда говорят, что первая система доказательств *моделирует* вторую систему доказательств. Если кроме того существует вычислимая за полиномиальное время функция,

которая отображает доказательства в первой системе доказательств в доказательства во второй системе доказательств, тогда первая система доказательств p-моделирует вторую. Оптимальной системой доказательств называется такая система доказательств, которая моделирует все остальные, а p-оптимальная система доказательств p-моделирует все остальные. Однако найти оптимальную пропозициональную систему доказательств пока не удалось (хотя возможно, что какая-нибудь из уже известных систем доказательств является оптимальной, например, такая система доказательств, для которой ещё не доказаны нижние оценки на размер доказательств). Неизвестно также, существует ли p-оптимальная пропозициональная система доказательств.

Даже если оптимальная пропозициональная система доказательств будет найдена, неизвестно, удастся ли доказать для неё нижнюю оценку на размер доказательств.

Система доказательств называется *автоматизируемой*, если существует автоматизирующая процедура, которая по строчке из языка L (теореме) выдаёт её доказательство за время, полиномиальное от длины кратчайшего доказательства и длины теоремы. Такие системы доказательств полиномиально эквивалентны *акцепторам* – процедурам, выдающим 1 на всех строчках из языка L и не заканчивающим работу на других строках. Акцептор для языка L называется оптимальным, если его время работы на строках из L ограничено некоторым полиномом от времени работы всех других акцепторов для L. Вопрос существования оптимальных алгоритмов для задач различных типов был поставлен Левиным в 1970х годах [24], и был дан положительный ответ для задач поиска из класса **NP**. Из этого результата вовсе не следует, что для любого языка из **NP** существует оптимальный акцептор, так как акцепторы решают задачу распознавания, а не задачу поиска, и поэтому могут работать быстрее.

Известно, что существование p-оптимальной системы доказательств для

языка пропозициональных тавтологий эквивалентно существованию оптимального аксептора для языка пропозициональных тавтологий [8]. Эта теорема была обобщена для всех языков, которые замкнуты относительно операции наполнения [13] (говоря неформально, эта операция заключается в приписывании к строчке суффикса достаточно большой длины).

Главной причиной, по которой не удаётся применить идеи Левина для построения оптимальной пропозициональной системы доказательств является отсутствие вычислимой нумерации для пропозициональных систем доказательств. Такие объекты часто называются *семантическими*. Основными структурными свойствами классов задач являются иерархия по времени и полная задача. Для семантических классов задач некоторые структурные свойства удаётся получить, если рассматривать *эвристические* алгоритмы (эвристический алгоритм может выдавать неправильный ответ на небольшой доле входов), или если рассматривать *немного неравномерные* машины Тьюринга – такие машины Тьюринга, которым разрешено использовать при вычислениях произвольную последовательность строк небольшой длины.

- *Вычисления с неравномерной подсказкой.* Сначала были получены теоремы об иерархии по времени для вычислений с несколькими битами неравномерной подсказки [1]. Потом стало известно, что иерархии по времени существует в классах сложности всего с одним битом подсказки $\mathbf{BPP/1}$ [10], зависящим от длины доказательства, и $\mathbf{ZPP/1}, \mathbf{MA/1}$ [4]. (Особенность использования подсказки здесь заключается в том, что с неправильной подсказкой машина Тьюринга может ошибаться с вероятностью, превосходящей допустимую.) Для систем доказательств была получена p-оптимальная система доказательств с одним битом подсказки [21].

- *Эвристические алгоритмы.* Было доказано существование иерархии по времени в $\mathbf{Heur_{1/n^c}BPP}$ – классе задач, которые могут быть ре-

шены эвристическими вероятностными машинами Тьюринга с двусторонне ограниченной допустимой вероятностью ошибки [10], [16]. Доказано существование полной криптосистемы с открытым ключом в классе криптосистем с эвристическим декодирующим алгоритмом [3]. Недавно в классах сложности **HeurBPP** и **AvgBPP** были найдены полные задачи [7].

Неизвестно, существует ли оптимальный аксептор для языка пропозициональных тавтологий, но совсем недавно было доказано, что для любого рекурсивно перечислимого языка L и любого *полиномиально моделируемого* ансамбля распределений S на строчках из $\overline{L}$ (дополнения L) для *распределённой задачи доказательства* (S, L) существует оптимальный эвристический аксептор [5]. Эвристическому аксептору разрешается ошибаться с небольшой вероятностью по входам, взятым с распределением S, то есть утверждать небольшое количество ложных теорем. *Медианное время работы* эвристического аксептора для строчки из языка L – это минимальное число шагов, за которое эвристический аксептор закончит работу с вероятностью хотя бы $1/2$. Оптимальность здесь означает, что для всех строчек из языка L медианное время работы оптимального эвристического аксептора ограничено полиномом от медианного времени работы любого другого эвристического аксептора. Но остаётся неясно, насколько понятие оптимального эвристического аксептора интересно: ведь может оказаться, что существует полиномиально ограниченный эвристический аксептор каждого распределения для языка пропозициональных тавтологий.

1.1 Постановка задачи

Найти необходимые и достаточные условия существования распределённой задачи доказательства, для которой не существует полиномиально ограниченного эвристического аксептора.

1.2 Результаты

1. Из существования трудной распределённой задачи доказательства для эвристических аксепторов следует существование *бесконечно часто* односторонней функции [23] (вычислимая за полиномиальное время функция, которую трудно обратить на некоторой бесконечной последовательности длин входов).

2. Из существования псевдослучайного генератора следует существование трудной распределённой задачи доказательства для эвристических аксепторов.

3. Для любой распределённой задачи доказательства (S, L), такой что язык L рекурсивно перечислимый и ансамбль распределений S полиномиально моделируемый, определяется понятие *эвристического инвертора*. Доказывается, что существование трудной задачи для эвристического инвертора эквивалентно существованию бесконечно часто односторонней функции.

1.3 Структура работы

В главе 2 собраны все необходимые определения и обозначения. Раздел 2.1 содержит все обозначения, относящиеся к распределениям случайных величин и ансамблям; в разделе 2.2 приведены определения эвристических процедур поиска и распознавания и в разделе 2.3 даны определения класса **FAvgBPP**, бесконечно часто односторонней функции и бесконечно часто псевдослучайного генератора.

Основная глава 4 начинается с подробного обсуждения в разделе 3 порядка изложения результатов. Раздел 4.1 содержит конструкцию трудной задачи для эвристических аксепторов из бесконечно часто псевдослучайного генератора. В разделах 4.2, 4.3 рассматривается предположение о существовании бесконечно часто односторонней функции и показывается эк-

вивалентность необходимого и достаточного условия существования трудной задачи доказательства для эвристического инвертора. Это же самое условие оказывается необходимым для существования трудной задачи для эвристического аксептора.

2 Определения и обозначения

2.1 Распределения на строках

Определение 2.1.1. Ансамбль распределений X – это последовательность $\{X_n\}_{n\in\mathbb{N}}$, где X_n – это отображение $\{0,1\}^n \to [0,1]$, такое что $\sum_{y\in\{0,1\}^n} X_n(y) = 1$. Множество $\{y \in \{0,1\}^n \mid X_n(y) > 0\}$ называется носителем X_n.

Обозначение 2.1. Для некоторого полинома p рассмотрим функцию $f : \{0,1\}^{p(n)} \to \{0,1\}^n$ и ансамбль распределений $X = \{X_{p(n)}\}_{n\in\mathbb{N}}$ будем обозначать через X^f ансамбль распределений $\{X^f_n\}_{n\in\mathbb{N}}$, где $X^f_n(y) = \Pr_{r\leftarrow X_{p(n)}}\{f(r) = y\}$ для всех строчек $y \in \{0,1\}^n$.

Определение 2.1.2. Функция $f : \{0,1\}^n \to \{0,1\}^n$ называется сохраняющей длину.

Определение 2.1.3. Ансамбль распределений S называется полиномиально моделируемым, если существует такой полиномиальный вероятностный алгоритм (самплер), который на входе 1^n выдает строчку x с вероятностью $S_n(x)$. Класс таких ансамблей мы будем обозначать **PSamp**.

Обозначение 2.2. Для вероятностной машины M обозначим r_M строку используемых ей случайных битов.

Обозначение 2.3. Обозначим через U_m равномерное распределение на множестве всех строк длины m. Для последовательности натуральных чисел $\{l_n\}_{n\in\mathbb{N}}$ назовём равномерным ансамблем распределений ансамбль $\{U_{l_n}\}_{n\in\mathbb{N}}$. Обозначим $U = \{U_n\}_{n\in\mathbb{N}}$.

2.2 Эвристические процедуры

Определение 2.2.1. Распределенная задача доказательства (S, L) состоит из ансамбля случайных величин S_n с носителем в $\overline{L} \cap \{0,1\}^n$ и языка L.

Мы ограничимся рассмотрением распределенных задач докзательства с полиномиально моделируемым S.

Определение 2.2.2. (λ, ϵ)-корректный аксептор для распределенной задачи доказательства (S, L) – это вероятностный алгоритм A с двумя параметрами $x \in \{0,1\}^*$ и $d \in \mathbb{N}$, который обладает следующими свойствами:

1. A выдает 1 или не заканчивает работу.
2. Для любого $x \in L$ и $d \in \mathbb{N}$, $A(x, d) = 1$.
3. Для любых $n, d \in \mathbb{N}$,

$$\Pr_{r \leftarrow S_n}\Big\{\Pr_{r_A}\{A(r, d) = 1\} > \epsilon\Big\} < \frac{1}{\lambda d}.$$

Здесь $\lambda > 0$ – константа и $\epsilon > 0$ может зависеть от длины первого параметра. Эвристический аксептор – это $(1, \frac{1}{4})$-корректный аксептор.

Сложностной характеристикой эвристического аксептора является медианное время работы.

Определение 2.2.3. Медианное время работы эвристического аксептора A на входе (x, d):

$$t_A(x, d) = \min\Big\{t \in \mathbb{N} \;\Big|\; \Pr_{r_A}\{A(x, d) \text{ останавливается за } t \text{ шагов}\} \geq \frac{1}{2}\Big\}.$$

Эвристический аксептор A называется *полиномиально ограниченным*, если существует такой полином p, что для всех $x \in L$ и $d \in \mathbb{N}$

$$t_A(x, d) \leq p(d \cdot |x|).$$

Определение 2.2.4. Для ансамбля распределений $S \in \mathbf{PSamp}$, рассмотрим самплер M, время работы которого ограничено некоторым полиномом $p(m)$, где m – это длина входа. Будем называть *генератором* ансамбля распределений S_m функцию $f_S : \{0,1\}^{p(m)} \to \{0,1\}^m$, такую что $f_S(x)$ – это выход самплера M на входе 1^m со случайными битами $r_M = x$. Получим $S_m(x) = U_m^{f_S}(x)$.

Определение 2.2.5. Пусть (S, L) – такая распределённая задача доказательства, что $S \in \mathbf{PSamp}$ и для некоторого полинома p обозначим генератор S через $f_S : \{0,1\}^{p(m)} \to \{0,1\}^m$.

(λ, ϵ)-корректный инвертор для распределённой задачи доказательства (S, L) – это вероятностный алгоритм I с параметрами $x \in \{0,1\}^*$ и $d \in \mathbb{N}$, который обладает следующими свойствами:

1. Для любого $x \in L$ и $d \in \mathbb{N}$, $I(x, d) = \perp$.
2. Для любых $n, d \in \mathbb{N}$,
$$\Pr_{x \leftarrow U_n^{f_S}} \Big\{ \Pr_{r_I} \{ I(x, d) = \perp \} > \epsilon \Big\} < \frac{1}{\lambda d}$$
3. Для любых $n, d \in \mathbb{N}$ и $x \in f_S(\{0,1\}^{p(n)})$, $I(x, d) \in f_S^{-1}(x) \cup \{\perp\}$.

Здесь $\lambda > 0$ – константа и $\epsilon > 0$ может зависеть от длины первого параметра. Эвристический инвертор – это $(1, \frac{1}{4})$-корректный инвертор.

Предложение 2.1. *Любой (λ, ϵ)-корректный инвертор для распределённой задачи доказательства (S, L) задаёт (λ, ϵ)-корректный акцептор, достаточно интерпретировать ответ $\perp$, как 1, а для других ответов не заканчивать работу.*

Определение 2.2.6. Медианное время работы эвристического инвертора I на входе (x, d):
$$t_I(x, d) = \min \Big\{ t \in \mathbb{N} \;\Big|\; \Pr_{r_I} \{ I(x, d) \text{ останавливается за } t \text{ шагов} \} \geq \frac{1}{2} \Big\}.$$

Эвристический инвертор I называется *полиномиально ограниченным*, если существует такой полином p, что для всех $n, d \in \mathbb{N}$ и $x \in L \cup f_S(\{0,1\}^n)$, таких что $|x| = n$,

$$t_I(x, d) \leq p(n \cdot d).$$

2.3 Сложность в среднем и криптография

Определим сначала основные необходимые понятия сложности в среднем, следуя [23].

Определение 2.3.1. Функция $f : \{0,1\}^* \to 2^{\{0,1\}^*}$ называется полиномиально проверяемой, если размер любой строчки выхода ограничен полиномом от размера входа и существует такая полиномиально вычислимая функция v, что

$$\forall x, y \in \{0,1\}^* \quad v(x, y) = 1 \Leftrightarrow y \in f(x).$$

Распределенная задача поиска (f, D) состоит из полиномиально проверяемой функции $f : \{0,1\}^* \to 2^{\{0,1\}^*}$ и ансамбля случайных величин D.

Определение 2.3.2. Распределенная задача поиска решается за вероятностное полиномиальное в среднем время с ограниченной ошибкой, если существует такой алгоритм $A(x, \delta)$, что

1. Время работы A полиномиально от $|x|$ и $\frac{1}{\delta}$ для всех x из носителя D и любого положительного δ.
2. Если $f(x) \neq \emptyset$, тогда $\Pr_{r_A}\{A(x, \delta) \notin f(x) \cup \{\perp\}\} \leq \frac{1}{4}$.
3. $\Pr_{x \leftarrow D_n}\{ \Pr_{r_A}\{A(x, \delta) = \perp\} \geq \frac{1}{4} \} \leq \delta$.

Определение 2.3.3. Класс сложности **FAvgBPP** состоит из всех распределенных задач поиска, решаемых за вероятностное полиномиальное в среднем время с ограниченной ошибкой.

Определение 2.3.4. Полиномиально вычислимая функция $f : \{0,1\}^* \to \{0,1\}^*$ является сильной бесконечно часто односторонней функцией, если для любого натурального k и для любого вероятностного полиномиального алгоритма B,

$$\forall N \; \exists n > N \quad \Pr_{\substack{x \leftarrow U_n \\ r_B}} \{B(f(x)) \in f^{-1}(f(x))\} < \frac{1}{n^k}.$$

Сформулируем определение псевдослучайного генератора [6].

Определение 2.3.5. Пусть $X = \{X_n\}_{n \in \mathbb{N}}$ и $Y = \{Y_n\}_{n \in \mathbb{N}}$ – два ансамбля случайных величин, тогда X и Y вычислительно неразличимы, если для любого вероятностного полиномиального алгоритма D и любого натурального k для достаточно больших n

$$\left| \Pr_{\substack{x \leftarrow X_n \\ r_D}} [D(x, 1^n) = 1] - \Pr_{\substack{y \leftarrow Y_n \\ r_D}} [D(y, 1^n) = 1] \right| < \frac{1}{n^k}.$$

Определение 2.3.6. Псевдослучайным генератором называется детерминированная полиномиальная машина Тьюринга G, обладающая двумя свойствами:

1. Существует функция $l : \mathbb{N} \to \mathbb{N}$, такая что $l(n) > n$ для всех $n \in \mathbb{N}$ и $|G(s)| = l(|s|)$ для всех $s \in \{0,1\}^*$.

2. Ансамбли случайных величин $\{U^G_{l(n)}\}_{n \in \mathbb{N}}$ и $\{U_{l(n)}\}_{n \in \mathbb{N}}$ вычислительно неразличимы.

Определение 2.3.7. Пусть $X = \{X_n\}_{n \in \mathbb{N}}$ и $Y = \{Y_n\}_{n \in \mathbb{N}}$ – два ансамбля случайных величин, тогда X и Y бесконечно часто вычислительно неразличимы, если для любого вероятностного полиномиального алгоритма D и любого натурального k для неограниченной последовательности длин входов n_i

$$\left| \Pr_{\substack{x \leftarrow X_{n_i} \\ r_D}} [D(x) = 1] - \Pr_{\substack{y \leftarrow Y_{n_i} \\ r_D}} [D(y) = 1] \right| < \left(\frac{1}{n_i}\right)^k.$$

Определение 2.3.8. Бесконечно часто псевдослучайным генератором называется детерминированная полиномиальная машина Тьюринга G, обладающая двумя свойствами:

1. Существует функция $l : \mathbb{N} \to \mathbb{N}$, такая что $l(n) > n$ для всех $n \in \mathbb{N}$ и $|G(s)| = l(|s|)$ для всех $s \in \{0,1\}^*$.
2. Ансамбли случайных величин $\{U^G_{l(n)}\}_{n\in\mathbb{N}}$ и $\{U_{l(n)}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы.

3 Подробный план

Опишем подробно, как устроена основная часть работы.

В разделах 4.2, 4.3 собраны утверждения о трудной задаче для эвристических инверторов. В теореме 4.3 утверждается, что из трудной задачи для эвристических инверторов можно построить сохраняющую длину одностороннюю в среднем случае функцию (лемма 4.2), а из неё по теореме 4.2 можно построить сохраняющую длину сильную бесконечно часто одностороннюю функцию. По теореме 4.4 из существования сохраняющей длину сильной бесконечно часто односторонней функции следует существование трудной задачи для эвристических инверторов.

Остальная часть работы о существовании трудной задачи для эвристических аксепторов. В теореме 4.1 построена трудная задача для эвристических аксепторов в предположении существования (бесконечно часто) псевдослучайного генератора. Следствие 4.1 показывает, как из трудной задачи для эвристических аксепторов сразу же получается трудная задача для эвристических инверторов (предложение 2.1), а из неё по теореме 4.3 можно построить сохраняющую длину сильную бесконечно часто одностороннюю функцию.

Наконец, доказательству эквивалентности существования бесконечно часто односторонней функции и существования бесконечно часто псевдо-

случайного генератора (следствие 5.2) посвящена вся глава 5.

4 О существовании трудных задач

4.1 Достаточное условие (аксепторы)

Сейчас мы доказываем *условную нижнюю оценку* на медианное время работы эвристического аксептора в предположении существования бесконечно часто псевдослучайного генератора.

Пусть G – бесконечно часто псевдослучайный генератор, такой что $|G(s)| = l(|s|) \geq |s|+3$. Тогда среди всех строчек длины $l(n)$ строчек из носителя $U^G_{l(n)}$ не может быть больше, чем $1/8$. Это доказывается формально в следующей лемме.

Лемма 4.1. *Пусть m – натуральное число, если $\forall n \in \mathbb{N} \;\; l(n) \geq n+3$, тогда*

$$\left|\{x \in \{0,1\}^{l(m)} \mid \exists\, s\; G(s) = x\}\right| \leq 2^{l(m)-3}.$$

Доказательство. Размер образа G на входах длины m не может быть больше, чем 2^m, но $l(m) \geq m+3$, значит среди строк длины $l(m)$ по крайней мере у $7/8$ нет прообраза длины m. □

Теорема 4.1. *Пусть G – бесконечно часто псевдослучайный генератор, тогда не существует полиномиально ограниченного аксептора для распределенной задачи доказательства $(\{U^G_{l(n)}\}_{n\in\mathbb{N}}, L)$, где множество "теорем" $L = \{0,1\}^* \setminus \bigcup_n (G(\{0,1\}^n))$.*

Доказательство. Пусть есть такой полиномиально ограниченный аксептор A, то есть существует некоторый полином p, что для всех $x \in L$

$$t_A(x, 16) \leq p(16 \cdot |x|).$$

Построим следующий вероятностный алгоритм D:

1. На входной ленте написана строчка $x \in \{0,1\}^n$.

2. Запустить алгоритм $A(x, 16)$,
   если он заканчивает работу за $p(16 \cdot |x|)$ шагов,
   тогда выдать его ответ.

3. Иначе выдать 0.

Обозначим через B множество "плохих" строчек:

$$B = \left\{ x \in G(\{0,1\}^n) \mid \Pr_{r_D}\{D(x) = 1\} > \frac{1}{4} \right\}$$

Тогда

$$\Pr_{\substack{x \leftarrow U^G_{l(n)} \\ r_D}} \left\{ D(x) = 1 \right\} = \Pr_{\substack{x \leftarrow U^G_{l(n)} \\ r_D}} \left\{ D(x) = 1 \mid x \in B \right\} \cdot \Pr_{x \leftarrow U^G_{l(n)}} \{x \in B\} +$$

$$+ \Pr_{\substack{x \leftarrow U^G_{l(n)} \\ r_D}} \left\{ D(x) = 1 \mid x \notin B \right\} \cdot \Pr_{x \leftarrow U^G_{l(n)}} \{x \notin B\} \leq$$

$$\leq \Pr_{x \leftarrow U^G_{l(n)}} \left\{ \Pr_{r_A}\{A(x, 16) = 1\} > 1/4 \right\} +$$

$$+ \Pr_{\substack{x \leftarrow U^G_{l(n)} \\ r_D}} \left\{ D(x) = 1 \mid \Pr_{r_D}\{D(x) = 1\} \leq 1/4 \right\} \leq 1/16 + 1/4 = \frac{5}{16}.$$

По лемме 4.1 для распределения $\{U_{l(n)}\}_{n \in \mathbb{N}}$ с вероятностью по крайней мере $\frac{7}{8}$ выданная строчка $x \in L$. Тогда для таких строчек алгоритм G будет выдавать 1 с вероятностью хотя бы $\frac{1}{2}$, так как

$$\Pr_{r_A}\{A(x, 16) \text{ останавливается за время не более } p(16 \cdot |x|)\} \geq \frac{1}{2}.$$

Следовательно,

$$\Pr_{x \leftarrow U_{l(n)}, r_D} \left\{ D(x) = 1 \right\} \geq \frac{7}{8} \cdot \frac{1}{2} = \frac{7}{16}$$

То есть ансамбли $\{U_{l(n)}\}_{n \in \mathbb{N}}$ и $\{U^G_{l(n)}\}_{n \in \mathbb{N}}$ почти везде полиномиально различимы, тогда G не может быть бесконечно часто псевдослучайным генератором – противоречие. $\square$

4.2 Необходимое условие (инверторы и аксепторы)

Теперь покажем, что существование сохраняющей длину сильной бесконечно часто односторонней функции является необходимым условием существования трудной задачи для эвристических инверторов и для эвристических аксепторов. Это условие также эквивалентно условию существования функции, которую сложно обратить в среднем [23].

Лемма 4.2. *Если существует распределённая задача доказательства* (S, L)*, такая что* $S \in \mathbf{PSamp}$*, и для которой никакой эвристический инвертор не будет полиномиально ограниченным, тогда существует такая сохраняющая длину полиномиально вычислимая функция* f*, что задача поиска* $(f^{-1}, U^f) \notin \mathbf{FAvgBPP}$*.*

Доказательство. Возьмём для ансамбля случайных величин S его генератор (определение 2.2.4) $f_S : \{0,1\}^{p(m)} \to \{0,1\}^m$ и построим по нему сохраняющую длину функцию $f : \{0,1\}^n \to \{0,1\}^n$

1. $f(r) = f_S(r)01^{p(m)-m-1}$, если существует такое m, что $n = p(m)$;
2. $f(r) = r$, иначе.

Пусть существует такой вероятностный алгоритм A_f, решающий в среднем задачу (f^{-1}, U^f), и его время работы ограничено некоторым полиномом $g(|x|, \frac{1}{\delta})$ для всех x из носителя $U^f_{|x|}$ и любого положительного δ. Тогда

$$\Pr_{x \leftarrow U^f_n}\{ \Pr_{r_{A_f}}\{A_f(x,\delta) \notin f^{-1}(x)\} \geq \frac{1}{4} \} \leq \delta.$$

Построим эвристический инвертор A для задачи доказательства (S, L):

1. На входе аксептора пара строчек (r, d).
2. Вычислить строку $x = r01^{p(|r|)-|r|-1}$.
3. Промоделировать $g(|x|, 2d)$ шагов алгоритма $A_f(x, \frac{1}{2d})$.
   Пусть r' – строчка на его выходной ленте.

4. Если $f(r') \neq x$, тогда выдать $\perp$.

5. Иначе выдать r'.

Для любых $r \in L$, $d \in \mathbb{N}$ $A(r,d) = \perp$, так как носитель распределения $S_{|r|}$ не пересекается с множеством L, и время работы $A(r,d)$ ограничено некоторым полиномом от $|r|$ и d. Остаётся доказать корректность A, то есть что для любых $m, d \in \mathbb{N}$

$$\Pr_{r \leftarrow S_m}\left\{\Pr_{r_A}\{A(r,d) = \perp\} > \frac{1}{4}\right\} < \frac{1}{d}.$$

Действительно, пусть $\delta = \frac{1}{2d}$, $n = p(m)$

$$\Pr_{r \leftarrow S_m}\left\{\Pr_{r_A}\{A(r,d) = \perp\} > \frac{1}{4}\right\} = \Pr_{x \leftarrow U^f_{p(m)}}\left\{\Pr_{r_{A_f}}\{A_f(x,\delta) \notin f^{-1}(x)\} > \frac{1}{4}\right\} \leq$$

$$\leq \Pr_{x \leftarrow U^f_n}\left\{\Pr_{r_{A_f}}\{A_f(x,\delta) \notin f^{-1}(x)\} \geq \frac{1}{4}\right\} \leq \delta < \frac{1}{d}.$$

Таким образом, построенный алгоритм является полиномиально ограниченным эвристическим инвертором для распределённой задачи доказательства (S, L) – противоречие. □

Теорема 4.2. ([23], *следствие* 3.2) *Если существует сохраняющая длину полиномиально вычислимая функция f, такая что задача поиска $(f^{-1}, U^f) \notin$ **FAvgBPP**, тогда существует сохраняющая длину сильная бесконечно часто односторонняя функция.*

Теперь получим необходимое условие существование трудной задачи доказательства для инверторов. Это же условие будет необходимо для существования трудной задачи для аксепторов.

Теорема 4.3. *Если существует распределённая задача доказательства (S, L), такая что $S \in$ **PSamp** и никакой эвристический инвертор для неё не будет полиномиально ограниченным, тогда существует сохраняющая длину сильная бесконечно часто односторонняя функция.*

Доказательство. По лемме 4.2 существует такая сохраняющая длину полиномиально вычислимая функция f, что задача поиска $(f^{-1}, U^f) \notin$ **FAvgBPP**. Тогда по теореме 4.2 получаем, что существует бесконечно часто односторонняя функция. □

Следствие 4.1. *Пусть существует распределенная задача доказательства (S, L), где $S \in$* **PSamp***, такая что никакой эвристический акцептор для неё не будет полиномиально ограниченным, тогда существует сохраняющая длину сильная бесконечно часто односторонняя функция.*

Доказательство. По предложению 2.1 так как для задачи (S, L) не существует полиномиального ограниченного аксептора, то никакой эвристический инвертор для задачи (S, L) не будет полиномиально ограниченным, тогда по теореме 4.3 существует сохраняющая длину сильная бесконечно часто односторонняя функция. □

4.3 Необходимое и достаточное условие (инверторы)

Необходимое и достаточное условие существования трудной задачи доказательства для эвристических инверторов – это существование бесконечно часто односторонней функции.

Теорема 4.4. *Сохраняющая длину сильная бесконечно часто односторонняя функция f существует тогда и только тогда, когда существует такая распределённая задача доказательства (S, L), где $S \in$* **PSamp***, что никакой эвристический инвертор для неё не будет полиномиально ограниченным.*

Доказательство. Из существования трудной распределённой задачи доказательства для эвристических инверторов следует существование сохраняющей длину сильной бесконечно часто односторонней функции по доказанной теореме 4.3.

Рассмотрим распределенную задачу доказательства (S, L), такую что $S_n(x) = \frac{|f^{-1}(x)|}{2^n}$, и пусть для неё существует эвристический инвертор A, время которого ограничено полиномом $g(d \cdot |x|)$ для всех $n, d \in \mathbb{N}$ и $x \in L \cup f(\{0,1\}^n)$. Построим взломщика D для функции f:

1. На входе алгоритма строчка $x = f(r)$.
2. Запустить алгоритм $A(x, 4)$.
3. Если он заканчивает работу за $g(4 \cdot |x|)$ шагов,
   тогда выдать его ответ.
4. Иначе выдать $\perp$.

Так как мы предположили, что медианное время работы инвертора A, ограничено полиномом $g(d \cdot |x|)$, то для любой строчки r, алгоритм $D(f(r))$ выдает в качестве своего ответа ответ A, вычисленный на шаге 3, с вероятностью по крайней мере $\frac{1}{2}$. Тогда

$$\Pr_{r,r_D}\{D(f(r)) \notin f^{-1}(f(r))\} \leq \left(\frac{1}{2} + \Pr_{r,r_A}\{A(f(r),4) = \perp\}\right) \leq \frac{3}{4},$$

то есть алгоритм D взламывает f почти везде. □

5 Псевдослучайный генератор

Мы покажем, что все промежуточные конструкции [9] позволяют использовать криптографические примитивы с более слабым определением надёжности (надёжные для бесконечной последовательности длин входов), поэтому с их помощью можно построить из бесконечно часто односторонней функции бесконечно часто псевдослучайный генератор.

Разделим всю цепочку конструкций на две части. Сначала из немного неравномерного бесконечно часто ложноэнтропийного генератора построим (немного неравномерный) бесконечно часто псевдослучайный генера-

тор, воспользовавшись универсальной хэш-функцией с некоторыми определёнными длинами параметрами. Потом из (немного неравномерной) бесконечно часто односторонней функции построим немного неравномерный бесконечно часто ложноэнтропийный генератор.

5.1 Необходимые определения

Замечание 5.1. В этой части будет удобнее рассматривать ансамбли распределений, определённые [2].

Будем называть ансамблем распределений последовательность $\{D_n(x)\}_{n=1}^{\infty}$, когда задана последовательность распределений $D_i : \{0,1\}^* \to [0,1]$ и существует такой многочлен p, что

$$\sum_{x \in \{0,1\}^*} D_n(x) = \sum_{|x| \le p(n)} D_n(x) = 1.$$

Множество $\{y \in \{0,1\}^n \mid X_n(y) > 0\}$ называется носителем X_n.

Определение 5.1.1. Для двух случайных величин $x \leftarrow X_n, x' \leftarrow X'_n$ определим статистическое расстояние между ними как

$$\mathrm{L}_1(x, x') = \sum_{r \in \{0,1\}^n} \big|\Pr\{x = r\} - \Pr\{x' = r\}\big|/2.$$

Обозначение 5.1. Из двух случайных величин X_n, X'_n и фиксированной строчки $x' \in \{0,1\}^n$ построим следующую случайную величину $\{0,1\}^n \to [0,1]$

$$[X_n | X'_n = x'](x) = \Pr_{\substack{r \leftarrow X_n \\ r' \leftarrow X'_n}} \Big\{ r = x \;\Big|\; r' = x' \Big\}.$$

Определение 5.1.2. Пусть X_n и X'_n случайные величины.

1. Будем называть энтропией (Шенона [19]) случайной величины X_n число

$$\mathrm{H}(X_n) = \mathop{\mathrm{E}}_{x \leftarrow X_n} \big[-\log(X_n(x)) \big].$$

2. Будем называть условной энтропией случайной величины X_n по отношению к случайной величине X'_n число

$$\mathrm{H}(X_n|X'_n) = \mathop{\mathrm{E}}_{x' \leftarrow X'_n} \Big[\mathrm{H}\left([X_n|X'_n = x'] \right) \Big].$$

Все используемые для доказательства промежуточные конструкции и определения повторяют [9]. Но определение надежности криптографических примитивов отличается тем, что надежность выполняется только для бесконечной последовательности длин входов.

Определение 5.1.3. Пусть $X = \{X_{l_n}\}_{n \in \mathbb{N}}$ и $Y = \{Y_{l_n}\}_{n \in \mathbb{N}}$ – два ансамбля распределений, тогда X и Y бесконечно часто вычислительно неразличимы с небольшими подсказками, если для любого вероятностного полиномиального алгоритма D, любого полинома q, любого натурального k и любой последовательности подсказок $\{\varrho_n\}_{n \in \mathbb{N}}$, где $\varrho_n \in \{0, \ldots, q(n)\}$, для неограниченной последовательности длин входов n_i

$$\left| \Pr_{\substack{x \leftarrow X_{n_i} \\ r_D}} [D(\varrho_{n_i}, x) = 1] - \Pr_{\substack{y \leftarrow Y_{n_i} \\ r_D}} [D(\varrho_{n_i}, y) = 1] \right| < \left(\frac{1}{n_i}\right)^k.$$

Определение 5.1.4. Будем говорить, что функция $f : \{0,1\}^* \to \{0,1\}^*$ вычислима за полиномиальное время с небольшой подсказкой, если существует такая полиномиальная детерминированная машина Тьюринга M и полином q, что для любого $n \in \mathbb{N}$ существует такая последовательность подсказок $\{\varepsilon_n\}_{n \in \mathbb{N}}$, где $\varepsilon_n \in \{0, \ldots, q(n)\}$, что $M(\varepsilon_n, x) = f(x)$ для любой строчки $x \in \{0,1\}^n$.

Определение 5.1.5. Будем называть немного неравномерным бесконечно часто псевдослучайным генератором функцию $g : \{0,1\}^* \to \{0,1\}^*$, обладающую свойствами:

1. Существует функция $l : \mathbb{N} \to \mathbb{N}$, такая что $l(n) > n$ для всех $n \in \mathbb{N}$ и $|g(s)| = l(|s|)$ для всех $s \in \{0,1\}^*$.

2. Ансамбли распределений $\{U^g_{l(n)}\}_{n\in\mathbb{N}}$ и $\{U_{l(n)}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы с небольшими подсказками.

3. g вычислима за полиномиальное время с небольшой подсказкой.

Определение 5.1.6. Мы будем говорить, что последовательность натуральных чисел $\{m_n\}_{n\in\mathbb{N}}$ полиномиально вычислима, если существует такая полиномиальная детерминированная машина Тьюринга M, что $M(1^n) = m_n$.

Определение 5.1.7. Пусть p – некоторый полином, $\{t_n\}_{n\in\mathbb{N}}, \{m_n\}_{n\in\mathbb{N}}$ – полиномиально вычислимые последовательности, такие что $t_n, m_n \in \{0,\dots,p(n)\}$ для любого $n \in \mathbb{N}$.

У вычислимой за полиномиальное время с небольшой подсказкой функции $f : \{0,1\}^{t_n} \to \{0,1\}^{l_n}$ вычислительная энтропия бесконечно часто равна s_n, если существует такая вычислимая за полиномиальное время с небольшой подсказкой функция $f' : \{0,1\}^{m_n} \to \{0,1\}^{l_n}$, что ансамбли распределений $\{U^f_{l_n}\}_{n\in\mathbb{N}}$ и $\{U^{f'}_{l_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы с небольшой подсказкой и $\mathrm{H}(U^{f'}_{l_n}) \geq s_n$.

Определение 5.1.8. Пусть p – полином, $\{t_n\}_{n\in\mathbb{N}}$ – полиномиально вычислимая последовательность, такая что $t_n \in \{0,\dots,p(n)\}$ для любого $n \in \mathbb{N}$. Вычислимая за полиномиальное время с небольшой подсказкой функция $f : \{0,1\}^{t_n} \to \{0,1\}^{l_n}$ называется немного неравномерным бесконечно часто псевдоэнтропийным генератором с псевдоэнтропией s_n, если у f вычислительная энтропия бесконечно часто равна $s_n + t_n$.

Определение 5.1.9. Для полинома p и полиномиально вычислимой последовательности $\{t_n\}_{n\in\mathbb{N}}$, такой что $t_n \in \{0,\dots,p(n)\}$ для любого $n \in \mathbb{N}$. Будем называть вычислимую за полиномиальное время с небольшой подсказкой функцию $f : \{0,1\}^{t_n} \to \{0,1\}^{l_n}$ немного неравномерным бесконечно часто ложноэнтропийным генератором с ложной энтропией s_n, если у f вычислительная энтропия бесконечно часто равна $\mathrm{H}(U^f_{t_n}) + s_n$.

Определение 5.1.10. Пусть q – некоторый полином, для полиномиально вычислимых последовательностей $\{p_n\}_{n\in\mathbb{N}}, \{m_n\}_{n\in\mathbb{N}}$ и $\{j_n\}_{n\in\mathbb{N}}$, таких что $p_n, m_n, j_n \in \{0,\dots,q(n)\}$ для любого $n \in \mathbb{N}$. Мы будем называть полиномиально вычислимую функцию $h : \{0,1\}^{p_n} \times \{0,1\}^{m_n} \to \{0,1\}^{j_n}$ (попарно независимой) универсальной хэш-функцией, если для любой строчки $x \in \{0,1\}^{m_n}$ и любой строчки $x' \in \{0,1\}^{m_n} \setminus \{x\}$, для всех строчек $a, a' \in \{0,1\}^{p_n}$

$$\Pr_{y\leftarrow U_{l_n}}\{h_y(x) = a \wedge h_y(x') = a'\} \leq \frac{1}{2^{2m_n}}.$$

Обозначение 5.2. Для двух строчек $u, v \in \{0,1\}^n$ будем обозначать их внутренее произведение как $u \odot v = \oplus_{i=1}^n u_i v_i$.

Обозначение 5.3. Для двух строчек $u, v \in \{0,1\}^*$ будем обозначать их конкатенацию $u \circ v$; u_i – это i-ый символ строчки u. Будем так же использовать следующее обозначение для подстроки: $u_{\{i,\dots,j\}} = \circ_{k=i}^{j} u_k$.

Обозначение 5.4. Пусть $\{l_n\}_{n\in\mathbb{N}}$, $\{m_n\}_{n\in\mathbb{N}}$, $\{p_n\}_{n\in\mathbb{N}}$ $\{j_n\}_{n\in\mathbb{N}}$ и $\{k_n\}_{n\in\mathbb{N}}$ – последовательности натуральных чисел. Для любого натурального числа n определим для функции $f : \{0,1\}^{m_n} \times \{0,1\}^{p_n} \times \{0,1\}^{j_n} \to \{0,1\}^{l_n}$ и последовательностей строк $\{x_i\}_{i\in\{1,\dots,k_n\}}$ длины m_n, $\{y_i\}_{i\in\{1,\dots,k_n\}}$ длины p_n и $\{z_i\}_{i\in\{1,\dots,k_n\}}$ длины j_n функцию конкатенации k_n применений f:

$$f^{k_n} : \left(\overset{k_n}{\underset{i=1}{\circ}} x_i, \overset{k_n}{\underset{i=1}{\circ}} y_i, \overset{k_n}{\underset{i=1}{\circ}} z_i\right) \mapsto \overset{k_n}{\underset{i=1}{\circ}} f(x_i, y_i, z_i).$$

Обозначение 5.5. Для любых двух последовательностей натуральных чисел $\{l_n\}_{n\in\mathbb{N}}$, $\{k_n\}_{n\in\mathbb{N}}$ и ансамбля распределений $X = \{X_{l_n}\}_{n\in\mathbb{N}}$ определим ансамбль распределений $X^{k_n} = \{X'_{k_n\cdot l_n}\}_{n\in\mathbb{N}}$, полученный конкатенацией последовательности k_n независимых случайных величин $\{x_i\}_{i\in\{1,\dots,k_n\}}$, имеющих распределение X_{l_n}:

$$X'_{k_n\cdot l_n}(\overset{k_n}{\underset{i=1}{\circ}} x_i) = \prod_{i=1}^{k_n} X_{l_n}(x_i).$$

Следующая матричная конструкция универсальной хэш-функции была предложена [11].

Определение 5.1.11. Для любой последовательности натуральных чисел $\{m_n\}_{n\in\mathbb{N}}$ и для любых строчек $x \in \{0,1\}^n$ и $y \in \{0,1\}^{(n+1)m_n}$ определим такую полиномиально вычислимую функцию

$$h : \{0,1\}^{(n+1)m_n} \times \{0,1\}^n \to \{0,1\}^{m_n},$$

такая что $h(y,x)_i = h_y(x)_i = (x \circ 1) \odot y_{\{(n+1)(i-1)+1,\ldots,(n+1)i\}}$, где $i \in \{1,\ldots,m_n\}$. Тогда h – универсальная хэш-функция.

Замечание 5.2. Если q – это некоторый полином, тогда существует такая детерминированная полиномиальная машина Тьюринга H, что для любых полиномиально вычислимых последовательностей $\{m_n\}_{n\in\mathbb{N}}$ и $\{j_n\}_{n\in\mathbb{N}}$, таких что $m_n, j_n \in \{0,\ldots,q(n)\}$ для любого $n \in \mathbb{N}$, выполняется

1. $H(1^{m_n}, 1^{j_n}, 0) = 1^{p_n}$ и
2. $H(y,x,1) = h_y(x)$, где

$h : \{0,1\}^{p_n} \times \{0,1\}^{m_n} \to \{0,1\}^{j_n}$ – это универсальная хэш-функция.

Определение 5.1.12. Для полиномиально вычислимой функции $f : \{0,1\}^n \to \{0,1\}^{l_n}$ и строчки $z \in f(\{0,1\}^n)$ будем называть порядком вырожденности z число $\tilde{D}_f(z) = \lceil \log(|f^{-1}(z)|) \rceil$.

5.2 Промежуточные конструкции

Опишем конструкции, использующие псевдоэнтропийный генератор: его можно построить из ложноэнтропийного генератора g_2, а потом из него построить немного неравномерный псевдослучайный генератор g_1.

Конструкция 1. Пусть $f' : \{0,1\}^n \to \{0,1\}^{m'_n}$ – полиномиально вычислимая функция. По замечанию 5.2 для любых полиномиально вычислимых последовательностей $\{k_n\}_{n\in\mathbb{N}}, \{j_n\}_{n\in\mathbb{N}}$ существует полиномиально

вычислимая последовательность $\{p_n\}_{n\in\mathbb{N}}$ и универсальная хэш-функция $h : \{0,1\}^{p_n} \times \{0,1\}^{m'_n \cdot k_n} \to \{0,1\}^{j_n}$.

Для строчек $u \in \{0,1\}^{nk_n}, y \in \{0,1\}^{p_n}$ определим такую полиномиально вычислимуюх функцию:

$$g_1 : (u, y) \mapsto h_y(f'^{k_n}(u)) \circ y.$$

Конструкция 2. Пусть $\hat{f} : \{0,1\}^n \to \{0,1\}^{\hat{m}_n}$ – полиномиально вычислимая функция и $\{\hat{s}_n\}_{n\in\mathbb{N}}$ полиномиально вычислимая последовательность, такая что $\hat{s}_n \leq 1$ для любых натуральных n. Для последовательности строчек $\{\varepsilon_n\}_{n\in\mathbb{N}}$, такой что $|\varepsilon_n - H(U^{\hat{f}}_{\hat{m}_n})| \leq \frac{\hat{s}_n}{8}$ для всех натуральных n, и двух полиномиально вычислимых с использованием ε_n последовательностей $\{k'_n\}_{n\in\mathbb{N}}, \{j'_n\}_{n\in\mathbb{N}}$ существует полиномиально вычислимая последовательность $\{p'_n\}_{n\in\mathbb{N}}$ и универсальная хэш-функция $h' : \{0,1\}^{p'_n} \times \{0,1\}^{nk'_n} \to \{0,1\}^{j'_n}$.

Для строчек $u \in \{0,1\}^{nk'_n}, r \in \{0,1\}^{p'_n}$ определим такую полиномиально вычислимую функцию:

$$g_2 : (\varepsilon_n, u, r) \mapsto \hat{f}^{k'_n}(u) \circ h'_r(u) \circ r.$$

5.3 Вспомогательные утверждения

Нам потребуются утверждения, которые не зависят от определения понятия вычислительной неразличимости.

Лемма 5.1. ([9], *следствие* 4.10) *Пусть* $\{k_n\}_{n\in\mathbb{N}}$ *– полиномиально вычислимая последовательность.*

1. *Для ансамбля распределений* $\{X_n\}_{n\in\mathbb{N}}$ *и последовательности натуральных чисел* $\{j_n\}_{n\in\mathbb{N}}$, *такой что* $j_n \leq \lfloor k_n H(X_n) - 2nk_n^{2/3} \rfloor$ *для любых натуральных* n, *рассмотрим универсальную хэш-функцию* $h : \{0,1\}^{p_n} \times \{0,1\}^{nk_n} \to \{0,1\}^{j_n}$. *Тогда для случайных величин* $x \leftarrow X_n^{k_n}$, $y \leftarrow U_{p_n}$ *и* $z \leftarrow U_{j_n+p_n}$ *выполняется*

$$\mathrm{L}_1(h_y(x) \circ y, z) \leq 2^{-k_n^{1/3}} \cdot O(2^{-n}).$$

2. *Для двух ансамблей распределений* $\{X_n\}_{n\in\mathbb{N}}, \{X'_n\}_{n\in\mathbb{N}}$ *и последовательности натуральных чисел* $\{j_n\}_{n\in\mathbb{N}}$, *такой что* $j_n \leq \lfloor k_n H(X_n|X'_n) - 2nk_n^{2/3} \rfloor$ *для любых натуральных* n, *рассмотрим универсальную хэш-функцию* $h : \{0,1\}^{p_n} \times \{0,1\}^{nk_n} \to \{0,1\}^{j_n}$. *Тогда для случайных величин* $x \leftarrow X_n^{k_n}$ *и* $x' \leftarrow X_n'^{k_n}$, $y \leftarrow U_{p_n}$ *и* $z \leftarrow U_{j_n+p_n}$ *выполняется*

$$\mathrm{L}_1(h_y(x) \circ y \circ x', z \circ x') \leq 2^{-k_n^{1/3}} \cdot O(2^{-n}).$$

Лемма 5.2. ([9], *утверждение* 4.11) *Пусть* V, W *– два ансамбля распределений и* $f : \{0,1\}^n \to \{0,1\}^{l_n}$ *полиномиально вычислима. Если ансамбли* V *и* W *(бесконечно часто) вычислительно неразличимы (с небольшими подсказками), тогда ансамбли распределений* V^f *и* W^f *(бесконечно часто) вычислительно неразличимы (с небольшими подсказками).*

Лемма 5.3. ([18]) *Пусть* $\{k_n\}_{n\in\mathbb{N}}$ *– полиномиально вычислимая последовательность и* V, W *– два полиномиально моделируемых ансамбля распределений. Если ансамбли* V *и* W *(бесконечно часто) вычислительно неразличимы (с небольшими подсказками), тогда и ансамбли* V^{k_n} *и* W^{k_n} *(бесконечно часто) вычислительно неразличимы (с небольшими подсказками).*

5.4 Псевдоэнтропийный генератор

Предложение 5.1. *Если* $\hat{f}$ *– (немного неравномерный) бесконечно часто ложноэнтропийный генератор с ложной энтропией* $\hat{s}_n = 1$, *тогда существуют такие последовательности параметров* $\{k'_n\}_{n\in\mathbb{N}}, \{j'_n\}_{n\in\mathbb{N}}$, *что* g_2 *из конструкции 2 будет немного неравномерным бесконечно часто псевдоэнтропийным генератором с псевдоэнтропией* 1.

Доказательство. Рассмотрим полиномиально вычислимую функцию $\hat{\phi} : \{0,1\}^{l_n} \to \{0,1\}^{\hat{m}_n}$, такую что $\mathrm{H}(U^{\hat{\phi}}_{\hat{m}_n}) \geq \mathrm{H}(U^{\hat{f}}_{\hat{m}_n}) + 1$ и ансамбли распределений $\{U^{\hat{f}}_{\hat{m}_n}\}_{n\in\mathbb{N}}$ и $\{U^{\hat{\phi}}_{\hat{m}_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы (она существует по определению ложноэнтропийного генератора).

И для строчек $u \in \{0,1\}^{nk'_n}, w \in \{0,1\}^{l_n \cdot k'_n}$ и $z \in \{0,1\}^{j'_n}, r \in \{0,1\}^{p'_n}$ определим следующие полиномиально вычислимые функции:

$$g'_2 : (u, z, r) \mapsto \hat{f}^{k'_n}(u) \circ z \circ r,$$

$$g''_2 : (w, z, r) \mapsto \hat{\phi}^{k'_n}(w) \circ z \circ r.$$

Тогда по лемме 5.3 ансамбли распределений $\{U^{g'_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}\}_{n \in \mathbb{N}}$ и $\{U^{g''_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}\}_{n \in \mathbb{N}}$ бесконечно часто вычислительно неразличимы.

Так как $\mathrm{H}(U_n | U^{\hat{f}}_n) = n - \mathrm{H}(U^{\hat{f}}_n) \geq n - \varepsilon_n$ можно выбрать $k'_n = (4n)^3$, $j'_n = k'_n(n - \varepsilon_n) - 2n(4n)^2$, тогда по лемме 5.1 ансамбли распределений $\{U^{g_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}\}_{n \in \mathbb{N}}$ и $\{U^{g'_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}\}_{n \in \mathbb{N}}$ вычислительно неразличимы.

Следовательно, ансамбли $\{U^{g_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}\}_{n \in \mathbb{N}}$ и $\{U^{g''_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}\}_{n \in \mathbb{N}}$ бесконечно часто вычислительно неразличимы. Наконец,

$$\mathrm{H}(U^{g''_2}_{k'_n \cdot \hat{m}_n + j'_n + p'_n}) - p'_n \geq k'_n \cdot (\mathrm{H}(U^{\hat{f}}_{\hat{m}_n}) + 1) + j'_n \geq k'_n(\varepsilon_n + 7/8) + j'_n \geq nk'_n + 1.$$

□

Предложение 5.2. *Если $f' : \{0,1\}^n \to \{0,1\}^{m'_n}$ – (немного неравномерный) бесконечно часто псевдоэнтропийный генератор с псевдоэнтропией 1, тогда существуют такие последовательности параметров $\{k_n\}_{n \in \mathbb{N}}, \{j_n\}_{n \in \mathbb{N}}$, что g_1 из конструкции 1 будет (немного неравномерным) бесконечно часто псевдослучайным генератором.*

Доказательство. Рассмотрим полиномиально вычислимую функцию $\phi' : \{0,1\}^{l_n} \to \{0,1\}^{m'_n}$, такую что ансамбли распределений $\{U^{f'}_{m'_n}\}_{n \in \mathbb{N}}$ и $\{U^{\phi'}_{m'_n}\}_{n \in \mathbb{N}}$ бесконечно часто вычислительно неразличимы и $\mathrm{H}(U^{\phi'}_{m'_n}) \geq n+1$. Тогда по лемме 5.3 ансамбли распределений $\{U^{f'^{k_n}}_{m'_n}\}_{n \in \mathbb{N}}$ и $\{U^{\phi'^{k_n}}_{m'_n}\}_{n \in \mathbb{N}}$ бесконечно часто вычислительно неразличимы.

Для строчек $w \in \{0,1\}^{l_n \cdot k_n}, y \in \{0,1\}^{p_n}$ определим следующую полиномиально вычислимую функцию:

$$g'_1 : (w, y) \mapsto h_y(\phi'^{k_n}(w)) \circ y.$$

По лемме 5.2 ансамбли распределений $\{U^{g_1}_{j_n+p_n}\}_{n\in\mathbb{N}}$ и $\{U^{g'_1}_{j_n+p_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы.

Так как $\mathrm{H}(U^{\phi'}_{m'_n}) \geq n+1$, и можно выбрать $k_n = (2m'_n+1)^3$, $j_n = k_n(n+1) - 2m'_n(2m'_n+1)^2$, для которых выполнится условие леммы 5.1. Следовательно, ансамбли распределений $\{U^{g'_1}_{j_n+p_n}\}_{n\in\mathbb{N}}$ и $\{U_{j_n+p_n}\}_{n\in\mathbb{N}}$ вычислительно неразличимы. Таким образом, $\{U^{g_1}_{j_n+p_n}\}_{n\in\mathbb{N}}$ и $\{U_{j_n+p_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы. Так как $j_n - nk_n = (2m'_n+1)^2 > 0$, то g_1 – это бесконечно часто псевдослучайный генератор. □

Предложение 5.3. *Если существует немного неравномерный бесконечно часто псевдослучайный генератор, тогда существует бесконечно часто псевдослучайный генератор.*

Доказательство. Доказательство следует из доказательства утверждения 4.17 [9], так как используемая там конструкция сохраняет вероятность успеха противника для фиксированного параметра надежности. □

5.5 Ложноэнтропийный генератор

Остаётся только убедиться в том, что из сильной бесконечно часто односторонней функции можно построить бесконечно часто ложноэнтропийный генератор g_4. Но для этого нам понадобится ещё одна промежуточная конструкция для трудного бита $\hat{g}_3$.

Конструкция 3. Пусть $f : \{0,1\}^n \to \{0,1\}^n$ – полиномиально вычислимая функция и $\hat{h} : \{0,1\}^{\hat{p}_n} \times \{0,1\}^n \to \{0,1\}^{n+\lceil\log(2n)\rceil}$ – универсальная хэш-функция.

Для строчек $x, y \in \{0,1\}^n, i \in \{0,\ldots,\tilde{D}_f(f(x))\}, \hat{r} \in \{0,1\}^{\hat{p}_n}, \beta \in \{0,1\}$ обозначим $\hat{t}_n = n+i+2\lceil\log(n)\rceil+\hat{p}_n+1$ и определим такие полиномиально вычислимые функции:

$$\hat{f}' : (x,i,\hat{r}) \mapsto f(x) \circ \hat{h}_{\hat{r}}(x)_{\{1,\ldots,i+\lceil\log(2n)\rceil\}} \circ i \circ \hat{r},$$

$$\hat{g}_3 : (x, i, r, y) \mapsto \hat{f}'(x, i, r) \circ (x \odot y) \circ y,$$
$$\hat{g}'_3 : (x, i, r, y, \beta) \mapsto \hat{f}'(x, i, r) \circ \beta \circ y.$$

Лемма 5.4. ([15]) *Пусть $f : \{0,1\}^n \to \{0,1\}^n$ – (бесконечно часто) односторонняя функция. Для строчек $x, y \in \{0,1\}^n$ и бита $b \in \{0,1\}$ определим такие полиномиально вычислимые функции:*

$$g : (x, y) \mapsto f(x) \circ (x \odot y) \circ y$$

$$g' : (x, y, b) \mapsto f(x) \circ b \circ y$$

Тогда ансамбли распределений $\{U^g_{2n+1}\}_{n\in\mathbb{N}}$ и $\{U^{g'}_{2n+1}\}_{n\in\mathbb{N}}$ будут (бесконечно часто) вычислительно неразличимы.

Лемма 5.5. ([9], *лемма* 5.1, 1) *Если f – это полиномиально вычислимая функция, сохраняющая длину, и функция $\hat{f}'$ из конструкции 3, тогда для строчек $x \in \{0,1\}^n$, $\hat{r} \in \{0,1\}^{\hat{p}_n}$ определим функцию:*

$$\widetilde{f} : (x, \hat{r}) \mapsto \hat{f}'\Big(x, \tilde{D}_f(f(x)), r\Big).$$

Если f – (бесконечно часто) односторонняя функция, тогда $\widetilde{f}$ (бесконечно часто) односторонняя функция.

Лемма 5.6. ([9], *лемма* 6.1) *Если f – это бесконечно часто односторонняя функция, сохраняющая длину, и функции $\hat{g}_3, \hat{g}'_3$ из конструкции 3, тогда ансамбли распределений $\{U^{\hat{g}_3}_{\hat{t}_n+n+1}\}_{n\in\mathbb{N}}$ и $\{U^{\hat{g}'_3}_{\hat{t}_n+n+1}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы.*

Доказательство. Следствие леммы 5.4 и леммы 5.5. □

Конструкция 4. Пусть $f : \{0,1\}^n \to \{0,1\}^n$ – полиномиально вычислимая функция, сохраняющая длину, и $\hat{f}'$ из конструкции 3. Для последовательности строчек $\{\varrho_n\}_{n\in\mathbb{N}}$ и двух полиномиально вычислимых с использованием ϱ_n последовательностей $\{\hat{k}_n\}_{n\in\mathbb{N}}, \{\hat{j}'_n\}_{n\in\mathbb{N}}$ существует полиномиально вычислимая последовательность $\{\hat{p}'_n\}_{n\in\mathbb{N}}$ и универсальная хэш-функция

$\hat{h}' : \{0,1\}^{\hat{p}'_n} \times \{0,1\}^{\hat{k}_n} \to \{0,1\}^{\hat{j}'_n}$. Пусть последовательность $\{\varrho_n\}_{n\in\mathbb{N}}$ такая, что

$$\varrho_n - \frac{1}{n} \leq \Pr_{\substack{i\leftarrow U_{\lceil \log n\rceil} \\ x\leftarrow U_n}} \Big\{ i \leq \tilde{D}_f(f(x)) \Big\} < \varrho_n + \frac{1}{n}$$

и $\hat{k}_n = (5n)^3$, $\hat{j}'_n = \hat{k}_n\varrho_n - 2(5n)^2$. Обозначим $\hat{s}_n = \hat{j}'_n + \hat{t}_n \cdot \hat{k}_n + \hat{p}'_n + n\hat{k}_n$.

Для строк $\bar{x}, \bar{y} \in \{0,1\}^{n\hat{k}_n}$, $\bar{i} \in \{0,1\}^{\lceil \log(2n)\rceil \hat{k}_n}$, $v \in \{0,1\}^{\hat{p}'_n}$, $\bar{r} \in \{0,1\}^{\hat{p}_n\cdot\hat{k}_n}$ и $z \in \{0,1\}^{\hat{j}'_n}$ определим такие полиномиально вычислимые функции:

$$g_4 : (\varrho_n, \bar{x}, \bar{y}, \bar{i}, v, \bar{r}) \mapsto \hat{h}'_v\Big(\bigcirc_{j=1}^{\hat{k}_n} x_j \odot y_j \Big) \circ \hat{f}'^{\hat{k}_n}(\bar{x}, \bar{i}, \bar{r}) \circ v \circ \bar{y},$$

$$g'_4 : (\varrho_n, z, \bar{x}, \bar{y}, \bar{i}, v, \bar{r}) \mapsto z \circ \hat{f}'^{\hat{k}_n}(\bar{x}, \bar{i}, \bar{r}) \circ v \circ \bar{y}.$$

Лемма 5.7. ([9], *лемма* 6.4) *Для функций* $f : \{0,1\}^n \to \{0,1\}^n$ *и* g_4, g'_4 *из конструкции 4* $\mathrm{H}(U^{g'_4}_{\hat{s}_n}) \geq \mathrm{H}(U^{g_4}_{\hat{s}_n}) + 10n^2$.

Лемма 5.8. ([9], *лемма* 6.5) *Для функций* $f : \{0,1\}^n \to \{0,1\}^n$ *и* g_4, g'_4 *из конструкции 4, а* $\hat{g}_3, \hat{g}'_3$ *из конструкции 3 рассмотрим произвольный немного неравномерный вероятностный взломщик* A*, с вероятностью успеха*

$$\delta_n = \Pr_{x\leftarrow U^{g_4}_{\hat{s}_n}}\{A(x) = 1\} - \Pr_{x'\leftarrow U^{g'_4}_{\hat{s}_n}}\{A(x') = 1\}.$$

Существует немного неравномерная вероятностная полиномиальная оракульная машина Тьюринга M^A*, такая что*

$$\Big| \Pr_{\hat{x}\leftarrow U^{\hat{g}_3}_{\hat{t}_n+n+1}} \{M^A(\hat{x}) = 1\} - \Pr_{\hat{x}'\leftarrow U^{\hat{g}'_3}_{\hat{t}_n+n+1}} \{M^A(\hat{x}') = 1\} \Big| \geq \frac{\delta_n}{16\hat{k}_n}.$$

Замечание 5.3. Первоначальная формулировка леммы 5.8 содержит предположение, что $\delta_n \geq 0$ для всех натуральных n. В случае различимости распределений почти везде это же предположение можно получить за счет использования одного бита $b_n \in \{0,1\}$ небольшой подсказки: если для данного n бит $b_n = 1$, тогда использовать прежний взломщик A, а если $b_n = 0$, тогда инвертировать ответы взломщика A (вместо ответа 1 выдавать 0, иначе выдавать 1).

Следствие 5.1. *Если f – бесконечно часто односторонняя функция, сохраняющая длину, и g_4, g_4' из конструкции 4, тогда ансамбли распределений $\{U^{g_4}_{\hat{s}_n}\}_{n\in\mathbb{N}}$ и $\{U^{g_4'}_{\hat{s}_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы.*

Доказательство. Из леммы 5.6 следует, что ансамбли распределений $\{U^{\hat{g}_3}_{\hat{t}_n+n+1}\}_{n\in\mathbb{N}}$ и $\{U^{\hat{g}_3'}_{\hat{t}_n+n+1}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы, тогда по лемме 5.8 $\{U^{g_4}_{\hat{s}_n}\}_{n\in\mathbb{N}}$ и $\{U^{g_4'}_{\hat{s}_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы. □

Теорема 5.1. *Если f – бесконечно часто односторонняя функция, сохраняющая длину, тогда g_4 из конструкции 4 будет немного неравномерным бесконечно часто ложноэнтропийным генератором с ложной энтропией 1.*

Доказательство. По лемме 5.7 $\mathrm{H}(U^{g_4'}_{\hat{s}_n}) \geq \mathrm{H}(U^{g_4}_{\hat{s}_n}) + 10n^2$, а по следствию 5.1 ансамбли распределений $\{U^{g_4}_{\hat{s}_n}\}_{n\in\mathbb{N}}$ и $\{U^{g_4'}_{\hat{s}_n}\}_{n\in\mathbb{N}}$ бесконечно часто вычислительно неразличимы. Значит, g_4 – это немного неравномерный бесконечно часто ложноэнтропийный генератор с ложной энтропией $10n^2 \geq 1$. □

Наконец, можно объединить все конструкции вместе и построить бесконечно часто псевдослучайный генератор: по теореме 5.1 и предложениям 5.1, 5.2 и 5.3 получаем следствие.

Следствие 5.2. *Если существует бесконечно часто односторонняя функция, сохраняющая длину, тогда существует бесконечно часто псевдослучайный генератор.*

Список литературы

[1] Boaz Barak. A probabilistic-time hierarchy theorem for "slightly non-uniform" algorithms. In *Proceedings of the 6th International Workshop on Randomization and Approximation Techniques (RANDOM '02)*, pages 194–208, London, UK, 2002. Springer-Verlag.

[2] Andrej Bogdanov and Luca Trevisan. Average-case complexity. *CoRR*, abs/cs/0606037, 2006.

[3] Danny Harnik and Joe Kilian and Moni Naor and Omer Reingold and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '05)*, pages 96–113, 2005.

[4] Dieter van Melkebeek and Konstantin Pervyshev. A generic time hierarchy with one bit of advice. *Computational Complexity*, 16(2):139–179, 2007.

[5] Edward A. Hirsch and Dmitry Itsykson. On optimal heuristic randomized semidecision procedures, with application to proof complexity. In *STACS*, pages 453–464, 2010.

[6] Oded Goldreich. Foundations of cryptography - a primer. *Foundations and Trends in Theoretical Computer Science*, 1(1), 2005.

[7] Dmitry Itsykson. Structural complexity of *AvgBPP*. In *Proceedings of CSR*, pages 155–166, 2009.

[8] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[9] Johan Håstad and Russell Impagliazzo and Leonid A. Levin and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[10] Lance Fortnow and Rahul Santhanam. Hierarchy theorems for probabilistic polynomial time. In *Proceedings of the 45th Annual Symposium on Foundations of Computer Science (FOCS 2004)*, pages 316–324, 2004.

[11] Larry Carter and Mark N. Wegman. Universal classes of hash functions. *J. of Comp. and Sys. Sci.*, 18(2):143–154, 1979.

[12] Maria Luisa Bonet and Toniann Pitassi and Ran Raz. On interpolation and automatization for frege systems. *SIAM Journal on Computing*, 29(6):1939–1967, 2000.

[13] Jochen Meßner. On optimal algorithms and optimal proof systems. In *STACS*, pages 541–550, 1999.

[14] Michael Alekhnovich and Eli Ben-Sasson and Alexander A. Razborov and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, 2004.

[15] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, pages 25–32, 1989.

[16] Konstantin Pervyshev. On heuristic time hierarchies. In *Proceedings of the IEEE Conference on Computational Complexity*, pages 347–358, 2007.

[17] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations, 1997.

[18] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. of Comput. and Sys. Sci.*, 28(2):270–299, 1984.

[19] Claude Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[20] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.

[21] Stephen Cook and Jan Krajícek. Consequences of the provability of *NP* subset of or equal to *P/poly*. *Journal of Symbolic Logic*, 72(4):1353–1371, 2007.

[22] Цейтин Г.С. О сложности вывода в исчислении высказываний. *Записки научных семинаров ЛОМИ*, 8:234–259, 1968.

[23] Гирш Э.А., Ицыксон Д.М. Бесконечно часто односторонняя функция, основанная на предположении о сложности в среднем. *Алгебра и анализ*, 21:130–144, 2009.

[24] Левин Л.А. Универсальные задачи перебора. *Проблемы передачи информации*, 9(3):115–116, 1973.