Санкт-Петербургский Государственный Университет
математико-механический факультет

кафедра Математического Обеспечения ЭВМ

ДИПЛОМНАЯ РАБОТА

ПО ТЕМЕ

Преобразование доказательств в арифметике с правилом случайной подстановки

студента 57 группы Гребинского Владимира Александровича

научный руководитель канд.физ.-мат. наук Данцин Е.Я.

рецензент докт.физ.-мат. наук Оревков В.П.

Санкт-Петербург

1995

ОГЛАВЛЕНИЕ

Введение 2

Краткое содержание 2

Глава 1. Система ARS. Арифметика с правилом случайной подстановки. 4

1. Обозначения 4

2. Доказательства в системе ARS 4

3. Доказывающие деревья 5

4. Интерактивные системы 5

5. Доказывающее дерево — другой вид доказательства 6

6. Ошибка в доказательстве. Вероятность ошибки доказательства. 7

7. Оценка вероятности ошибки доказательства. 8

Глава 2. Доказательства полиномиальной длины. 10

Доказательства с экспоненциально малой вероятностью ошибки. 10

Система ARS_n 10

Верхняя оценка длины доказательства 11

Глава 3. Каноническая форма доказательств. 13

Заключение 19

Литература *Error! Bookmark not defined.*

Введение

Краткое содержание

В дипломной работе представлены новые результаты об Арифметике с правилом случайной подстановки (ARS). В работе [Да] поставлен ряд вопросов, на некоторые из которых удалось получить ответ.

В Главе 1 описана формальная система ARS, вводится понятие доказывающего дерева и вероятность ошибки. При таком подходе, удается сформулировать основные идеи в терминах доказывающих деревьев. Интересным наблюдение является то, что доказывающие деревья -- другой способ записи доказательства.

В Главе 2 вводится множество формул и класс языков с “приемлемой” (полиномиальной) длиной и экспоненциально маленькой вероятностью ошибки. Без каких-то бы ни было предположений доказана теорема:

Теорема Пусть Ф имеет доказывающее дерево Тф длины l, тогда Ф имеет доказательство в арифметике длины $< 2^{poly(l)}$ - полином зависящий от k -параметра в правиле $\forall^{-k}_{x<N} : F(x)$).

Эта теорема существенно улучшает верхнюю оценку длины доказательства при элиминации правила случайной подстановки. Новая оценка -- экспонента от длины дерева, старая -- дважды экспоненциальная. Эта оценка не улучшаема, если доказательство принадлежности PSPACE языку не может быть короче экспоненты от длины входного слова.

Результат Главы 3 показывает, что в сущности, с точностью до полиномиального увеличения длины доказывающего дерева, существует правило случайной подстановки ровно **одного** вида: $\frac{\forall_{x<N}^{-1} : F(x)}{F(r)}$. Этот результат не улучшаем и может быть полезен для получения доказывающих деревьев стандартного вида, получения отрицательных результатов о доказуемости в ARS. Применяемая техника, видимо, не имеет переложения в технику связанную с интерполяцией полиномов, и, следовательно, является специфической для ARS, но поскольку доказательства в ARS можно рассматривать в рамках интерактивных систем, то она может быть применена и в интерактивных доказательствах.

Глава 1.
Система ARS.
Арифметика с правилом случайной подстановки.

1. Обозначения

Арифметика с правилом случайной подстановки является расширением обычной арифметики, за счет введения в нее черт отражающих существенные особенности интерактивных систем, а именно, взаимодействие и случайность.

Под арифметикой мы будем подразумевать одну из ее стандартных формализаций (например, см. [Kleene]). Ограниченные кванторы $\forall x_{<a} F$ и $\exists x_{<a} F$ определяются обычным образом, т.е. как сокращения для формул $\forall x\ (x < a) \supset F$ и $\exists x\ (x < a) \& F$, где x<a является сокращением для $\exists y\ (y' + x = a)$

Пусть F(x) — арифметическая формула с одной свободной переменной x, а все остальные переменные встречающиеся в F(x) — связаны ограниченными кванторами. Рассмотрим следующее высказывание о формуле F(x) и натуральных числах N и k:

Формула F(x) истинна для всех значений x, меньших N, за исключением не более k каких-то значений.

Это высказывание можно записать в виде

(*) $$\exists x_1 x_2 \cdots x_k \forall x < N\ (x = x_1 \vee x = x_2 \cdots \vee x = x_k) \vee F(x),$$

где N—терм без переменных. Формулу (*) мы будем сокращенно записывать как $\forall^{-k}_{x<N} F(x)$

Всюду далее всякое упоминание о некоторой формуле F(x) в контексте $\forall^{-k}_{x<N} F(x)$ будет означать требование связывания всех переменных отличных от x, ограниченными кванторами. Основным случаем нашего рассмотрения в дальнейшем будет ситуация $N>2^k$, тогда доля чисел x, для которых F(**x**) не доказуема — экспоненциально мала и формулу (*) можно читать как “для почти всех **x**, F(x)“. Введем термин: если F(n) не доказуема, то назовем натуральное число n **контрпримером.** Тогда (*) может быть прочитана как: “F(x) имеет не более k контрпримеров при x<N“. Заметим, что в случае ограниченности кванторов, истинность и доказуемость замкнутой формулы F(r) — совпадают.

Правилом случайной подстановки называется схема

(1) $$\frac{\forall^{-k}_{x<N} F(x)}{F(r)},$$

где r—равномерно распределенное случайное число из интервала (0,1,...,N-1).

Под арифметикой с правилом случайной подстановки мы понимаем аксиомы и правила вывода формальной арифметики, к которым добавлена схема правил (1). Для краткости будем обозначать эту систему ARS (Arithmetic with Random Substitution).

2. Доказательства в системе ARS

Проводя аналогию с выводом в исчислении, мы говорим, что доказательство в ARS—это **порождающий процесс**, состоящий из шагов, суть которых состоит в получении нового объекта из уже полученных к началу этого шага объектов; получение нового объекта получается путем применения произвольного “разрешительного” правила. Эти правила суть

следующие: нульпосылочные—аксиомы, двухпосылочные—modus ponens, однопосылочные—схема правил (1) (правила случайной подстановки) и схемы однопосылочных правил арифметики. Допустимые объекты такого “исчисления” и будут предметом нашего изучения. Определение понятия допустимого объекта индуктивное—если объект B получается из $A_1,..,A_k$ применением одного из разрешительных правил и если $A_1,...,A_k$ являются допустимыми объектами, то и B объявляется допустимым. При этом мы подразумеваем, что шаг, связанный с применением правила случайной подстановки включает в себя упоминание о некоторой ленте со случайными числами, или другом элементе достаточно большого вероятностного пространства (что понимать под достаточно большим будет уточнено в одной из Лемм; неформально говоря, от пространства требуется возможность определить на нем достаточно (счетно) много независимых случайных величин). Таким образом, множество допустимых объектов в исчислении ARS будет зависеть от случайной ленты. А значит корректно говорить о том, что объект допустим с некоторой вероятностью. (Стоит напомнить, что в нашей ситуации, все объекты—это арифметические формулы). Замети что шаг порождения объекта по правилу (1) подразумевает вычисление некоторой случайной величины (т.е. измеримой функции Ω->**N**) $r=\xi(N, \text{лента})$ и на эту величину наложено условие равномерного распределения на множестве (0,1,...,N-1).

3. Доказывающие деревья

Доказывающее дерево для формулы Ф—это конечное дерево, устроенное следующим образом:

- Корню дерева приписана аксиома арифметики.
- Вершина имеет степень ветвления больше 1 тогда и только тогда, когда формула ей приписанная имеет вид $\forall^{-k}_{x<N} F(x)$ и N>1, а все ее потомки—это вершины помеченные формулами $F(0), F(1), \ldots, F(N-1)$.
- Формулы приписанные вершинам степени 1 получаются по правилам порождения объектов, из формул приписанных вершинам находящимся выше по пути к корню дерева.
- Всем листьям приписаны формулы полученые по правилу порождения объектов из вышестоящих на пути к корню и все эти формулы должны совпадать с формулой Ф.

Определение: доказывающее дерево, все листья которого помечены формулой Ф называется *доказывающим деревом* формулы Ф и обозначается $T_Ф$.

4. Интерактивные системы

Вывод объекта в нашем исчислении можно рассматривать как коммуникацию двух машин P (Prover) и V (Verifier), где V снабжен доступом к ленте со случайными числами. P и V обмениваются сообщениями и имеют выходную ленту, куда могут только писать. Шаг общения состоит в том, что P производит шаг, порождая допустимый объект не применяя правило случайной подстановки, или просит V применить шаг порождения нового объекта с помощью правила случайной подстановки исходя из последнего выписанного объекта вида $\forall^{-k}_{x<N} F(x)$. После чего V записывает на выходную ленту некоторую формулу F(r), где r—случайное число, из интервала 0...N-1. Как только порождена формула Ф — V допускает.

Утверждение: Детерминированный P может вынудить V принять формулу Ф при любых случайных числах тогда и только тогда, когда существует доказывающее дерево.

Доказательство: Иначе существует бесконечная ветвь в доказывающем дереве.

5. Доказывающее дерево — другой вид доказательства

Следующее утверждение столь важно для дальнейшего, что сформулировано в виде теоремы:
Теорема 1: Для следующих высказываний о Ф имеет место 1⇔2

1.PA|—Ф, т.е. Ф доказуемо в арифметике

2.Существует доказывающее дерево для Ф

Доказательство:

1=>2: PA|—Ф, следовательно, существует классическое доказательство формулы Ф; все формулы этого доказательства, записанные в виде дерева (в нашем случае—в виде цепи) —- образуют доказывающее дерево для Ф.

2=>1: Существует $T_Ф$ => PA|—Ф ?

<u>Первое доказательство</u> ([Да]):

Рассмотрим правило $\dfrac{\forall^{-k}_{x<N} F(x)}{F(r)}$

Поскольку F(r) — замкнутая формула с ограниченными кванторами, то либо |—F(r), либо |— **not** F(r). Выберем в дереве $T_Ф$ путь проходящий только через формулы F(r), для которых |—F(r). Это можно сделать всегда при k<N. Тогда дописав вывод всех встретившихся формул вида F(r), мы получим обычное доказательство Ф в PA.

<u>Второе доказательство</u>: Основное препятствие на пути считать формулы стоящие вдоль пути доказательством Ф состоит в том, что F(r) *не доказаны* (в обычном смысле), более того они могут быть и **не**доказуемы (ложны). Рассмотрим, однако, последнее “препятствие" - последнюю формулу F(r), на некотором пути из корня в лист, полученную по правилу случайной подстановки $\dfrac{\forall^{-k}_{x<N} F(x)}{F(r)}$. Мы не знаем *a priori* доказуемость F(r), но мы знаем, что от r в сущности ничего не зависит. И в силу конечности дерева, мы можем считать, что выбранный путь обладает тем свойством, что все F(0),F(1),...,F(N-1) — суть последние формулы полученные по правилу случайной подстановки (каждая на своем пути). Значит $F_1(r_1), F_2(r_2), \ldots, F_n(r_n)$, $F(i)$ |— $Ф$, для всех i, поскольку:

1.Проведению обычного доказательства мешают лишь формулы полученные по правилу случайной подстановки.

2.Все рассматриваемые пути при i=0...N-1 имеют общий префикс содержащий в качестве препятствий $F_1(r_1), F_2(r_2), \ldots, F_n(r_n)$

По теореме о дедукции получаем

(*) $F_1(r_1), F_2(r_2), \ldots, F_n(r_n) \vdash F(i) \supset \Phi$, при i=0...k,

где k — число “контрпримеров” в правиле.

Из k+1 формулы (*) получаем

(**) $F_1(r_1), F_2(r_2), \ldots, F_n(r_n) \vdash (F(0) \vee F(1) \vee \ldots \vee F(k)) \supset \Phi$

Далее, выводима импликация

(***) $\vdash \forall^{-k}_{x<N} F(x) \supset (F(0) \vee F(1) \vee \ldots \vee F(k))$

(Принцип Дирихле: k+1 формула, не более k ложных, значит хоть одна истинна).

И наконец, поскольку формула F(x) стоит на пути содержащем лишь препятствия $F_1(r_1), F_2(r_2), \ldots, F_n(r_n)$, значит

(****) $F_1(r_1), F_2(r_2), \ldots, F_n(r_n) \vdash \forall^{-k}_{x<N} F(x)$

Теперь имеем вывод:

(****) , (***)

———————————————————————————————————————

$F_1(r_1), F_2(r_2), \ldots, F_n(r_n) \vdash F(0) \vee \ldots \vee F(k)$, (**)

———————————————————————————————————————-

$F_1(r_1), F_2(r_2), \ldots, F_n(r_n) \vdash \Phi$

И мы показали, что Ф доказуема в предположении с числом препятствий на единицу меньшим. Теперь простое индуктивное рассуждение покажет, что ⊢ Ф. Это будет сделано позже, когда нас будет интересовать увеличение длины такого преобразования.

Анализ вышеописанной процедуры показывает:

1.Доказывающее дерево, это в сущности доказательство, записанное несколько необычным способом.

2.Предположение об ограниченности кванторов нигде в сущности не использовалось. От вида Ф и F ничего не зависит.

6. Ошибка в доказательстве. Вероятность ошибки доказательства.

Далее мы всегда будем предполагать, что процесс порождения формулы Ф при всех случайных лентах, соответствует некоторому доказывающему дереву. Путь в этом дереве, соответствующий процессу порождения Ф при данной случайной ленте будем называть **доказательством** Ф при данной случайной ленте. Заметим, что в силу результатов предыдущего параграфа, мы имеем дело теперь только с доказуемыми формулами (т.е. PA⊢Ф).

При данной случайной ленте, рассмотрим процесс порождения Ф, пусть это будут формулы $\hat{O}_1, \hat{O}_2, \ldots, \hat{O}_n$, часть которых получена в результате применения правила случайной подстановки.

Определение: *Ошибкой в правиле случайной подстановки* называется ситуация, когда для формулы $\forall^{-k}_{x<N} F(x)$ и F(r) выполнено: PA|— $\forall^{-k}_{x<N} F(x)$ и PA|-/-F(r), то есть F(r) не доказуема в арифметике.

Определение: Говорят, что доказательство *не содержит ошибки* тогда и только тогда, когда оно не содержит ошибки в применениях правила случайной подстановки.

Таким образом, каждой ленте соответствует доказательство содержащее или не содержащее ошибки, а значит можно говорить о вероятности ошибки доказательства.

Поскольку основным объектом дальнейшего изучения будут доказывающие деревья, посчитаем вероятность ошибки доказательства в терминах доказывающего дерева

1. На множестве путей проходящих от корня до листа дерева $T_Ф$ есть естественная мера, а именно, пути проходящему через вершины со степенями N_1, N_2,..., N_k—ставится в соответствие вероятность $1/(N_1*N_2*...*N_k)$.
2. Следующая Лемма показывает, что мера лент, соответствующая некоторому пути в дереве равна естественной вероятности этого пути.

Лемма 1. Пусть $\xi^{r_1 r_2 \ldots r_k}_{N_1 N_2 \ldots N_k}(N_{k+1})$ — обозначает случайную величину из диапазона $(0,1,...,N_{k+1}-1)$— которая будет получена, если со случайной ленты уже считаны числа r_1 из диапазона $0...N_1-1$, ..., r_k из $0...N_k-1$. Если при всех i=0...k, случайные величины $\xi^{r_1 r_2 \ldots r_i}_{N_1 N_2 \ldots N_i}(N_{i+1})$ — независимы и равномерно распределены, то

$$\Pr(\forall_{0 \le j \le k} \xi^{r_1 r_2 \ldots r_j}_{N_1 N_2 \ldots N_j}(N_{j+1}) = r_{j+1}) = \frac{1}{N_1 N_2 \ldots N_{k+1}}$$

Доказательство: непосредственно следует из независимости.

Утверждение: На отрезке [0,1] существует набор случайных величин, удовлетворяющих условиям леммы 1.

Следствие: Вероятность ошибки доказательства равна мере всех путей в дереве содержащих ошибку. Обозначим эту величину **e**($T_Ф$). Такой подход сводит почти все вопросы об ARS к вопросу о деревьях.

7. Оценка вероятности ошибки доказательства.

Рассмотрим доказывающее дерево $T_Ф$ для формулы Ф, на которое наложены следующие ограничения:

1. Во всех правилах случайной подстановки $k \le log\ N$
2. k и N—фиксированы во всем дереве

Пусть h равно наибольшему числу применения правил случайной подстановки вдоль путей дерева $T_Ф$. Тогда мера путей, не содержащих ошибки > *(1-k/N)^h*, а значит вероятность ошибки $e(T_Ф) < 1-(1-k/N)^h < k*h/N$.

Определим **длину** доказательства, как *суммарное число символов* в записи всех формул входящих в доказательство. <u>*Максимальная длина пути дерева*</u> $l(T_Ф)$ равна максимуму длин его путей из корня. Заметим, что

$$e(T_Ф) < k*h/N < l(T_Ф)/N$$

Действительно, формула записывающая $\forall^{-k}_{x<N} F(x)$ имеет по крайней мере k кванторов, а значит $h < l/k$.

Мы будем считать приемлемыми доказывающие деревья с вероятностью ошибки $e(\mathrm{T}_{\Phi})<2^{-|\Phi|}$, т.е. с экспоненциально маленькой вероятностью ошибки. Напомним, что доказательство формулы Ф, выписанное по случайной ленте, может быть дополнено до доказательства в арифметике с вероятностью $> 1-e(\mathrm{T}_{\Phi})$. Отметим, что вышеприведенная оценка основывается не на специфике формулы Ф, а лишь на специфике доказывающего дерева. При $N>l(\mathrm{T}_{\Phi})*2^{|\Phi|}$, мы имеем $e(\mathrm{T}_{\Phi})<2^{-|\Phi|}$.

Глава 2.
Доказательства полиномиальной длины.

Доказательства с экспоненциально малой вероятностью ошибки.

Определение: Обозначим через $ARS(x^n)$ множество формул удовлетворяющих следующим условиям: $\Phi \in ARS(x^n) \Leftrightarrow$

1. Ф имеет доказывающее дерево T_Φ, длина максимального пути $T_\Phi < |\Phi|^n$

2. Все правила случайной подстановки имеют вид

$$\frac{\forall^{-k}_{x<N} F(x)}{F(r)} \quad и \quad k \le log\ N, \quad N > l(T_\Phi) * 2^{|\Phi|} ,$$

т.е. $ARS(x^n)$ состоит из формул, заведомо имеющих полиномиальные доказательства и экспоненциально малую вероятность ошибки доказательства.

Легко проверяются следующие утверждения:

1. $\bigcup_n ARS(x^n) = \{\Phi: \ \vdash_{PA} \Phi\}$

2. $\forall n\ ARS(x^n) \in PSPACE$

3. $ARS(x^1) \subseteq ARS(x^2) \subseteq \ldots \subseteq ARS(x^n) \subseteq \ldots$ è $\forall i\ \exists j\ ARS(x^i) \neq ARS(x^j)$

Доказательство

1. $\Phi \in ARS \Rightarrow \exists T_\Phi \Rightarrow \Phi$ —- доказуема (см. ранее)

   Ф — доказуема в PA => Ф ∈ ARS(длина доказательства Ф)

2. При данном n можно построить PSPACE машину, пытающуюся построить необходимое T_Φ путем перебора деревьев доказательств и следящую за ограничениями на степени ветвления и прочими ограничениями. Эта машина должна чередовать работу в экзистенциональном и альтернирующем режимах. В первом она угадывает вывод формулы без применения правила случайной подстановки, а во втором проверяет, что всевозможные разветвления приводят к доказательству Ф.

3. Ясно что $ARS(x^n) \subseteq ARS(x^{n+1})$. Если с некоторого места все включения — равенства, то множество доказуемых формул лежит в PSPACE, что не верно (т.к. оно не рекурсивно).

Система ARS_n

Мы говорим, что язык L арифметических формул принадлежит $\boldsymbol{ARS_n}$, если $L \subseteq ARS(x^n)$, для некоторого n. То есть $ARS(x^n)$ — множество формул, а $\boldsymbol{ARS_n}$ — множество языков.

Интерес к системе $\boldsymbol{ARS_n}$ объясняется следующим фактом: как показано в [Да], существует язык L, такой что:

1. $L \in \boldsymbol{ARS_n}$, при некотором n

2.Задача принадлежности к PSPACE языку полиномиально сводится к задаче доказуемости некоторой $\Phi \in L$.

Таким образом, вопросы о принадлежности к PSPACE языкам (таким как булевы формулы с кванторами) можно сводить к вопросу доказуемости некоторой формулы Ф, которая, если доказуема имеет короткое доказательство в ARS (и очень малую вероятность ошибки). Доказательство этой теоремы существенным образом использовало методы интерактивных систем и технику разработанную в [Ba], [Sh] и [LFKN].

Вопрос о том, какие языки арифметических формул лежат в $\boldsymbol{ARS_n}$ — является одним из основных открытых вопросов.

Верхняя оценка длины доказательства

В Теореме 1 Главы 1 было показано, что всякая формула, имеющая конечное доказывающее дерево — доказуема и в арифметике. Сейчас мы извлечем оценку изменения длины в ходе получения по доказывающему дереву доказательства в PA.

Теорема Пусть Ф имеет доказывающее дерево T_Φ длины l, тогда Ф имеет доказательство в арифметике длины < $2^{poly(l)}$ - полином зависящий от k -параметра в правиле $\forall^{-k}_{x<N} F(x)$. Для удобства мы предполагаем k фиксированным в доказывающем дереве.

Доказательство:

Обозначения

1. $p = \{F_1(r_1), F_2(r_2), \ldots, F_k(r_k)\}$— обозначает путь в дереве, идущий из корня, проходящий последовательно через вершины $\{F_1(r_1), F_2(r_2), \ldots, F_k(r_k)\}$ (и содержащий все промежуточные вершины). Таким образом, p — префикс некоторого пути из корня в лист.

Мы говорим $p_1 < p_2$, если p_1 — собственный префикс p_2.

2. Мы пишем p|— Ф, если в предположении формул входящих в p, Ф доказуема в арифметике.

3. Пусть {} — "пустой" путь. Считаем, что $\forall p \neq \{\}: \{\} < p$

{}|—Ф — трактуется как PA|—Ф

Лемма 1 ("Индукционный переход")

$\forall p_1: (\forall p_2 : (p_1 < p_2) \supset \vdash \Phi)) \supset p_1 \vdash \Phi$

(т.е. если все пути, большие чем p, доказывают Ф, то и p доказывает Ф)

Доказательство: Пусть $p = \{F_1(r_1), F_2(r_2), \ldots, F_n(r_n)\}$, поскольку дерево конечно, рассмотрим все пути p_i для которых p — непосредственный предшественник. Если таковых не нашлось, то p — путь от корня до листа и p|—Ф, т.к. вывод Ф в предположении формул из p повторяет вывод Ф в дереве. Иначе, пусть $p_0, p_1, \ldots, p_{N-1}$ — все такие вершины. Действительно, они должны соответствовать применению правила случайной подстановки, причем в силу минимальности, одному и тому же.

Таким образом p |— $\forall^{-k}_{x<N} F(x)$ (*)

$p_i=\{F_1,...,F_n,\ F(i)\}$

Следуя доказательству Теоремы 1 Главы 1 получаем

поскольку $p_i=F_1,...,F_n,F(i)\vdash\Phi$, имеем $F_1,...,F_n\vdash F(i)\supset\Phi$ для всех i,

то есть $p\vdash F(i)\supset\Phi$, значит $p\vdash(\vee_{0\le i\le k}F(i))\supset\Phi$, но
$\vdash(\forall^{-k}_{x<N}F(x))\supset(\vee_{0\le i\le k}F(i))$ (принцип Дирихле) и $p\vdash\forall^{-k}_{x<N}F(x)$.
Комбинируя последние три формулы получаем $p\vdash\Phi$, что и требовалось доказать.

Посчитаем длину доказательства $p\vdash\Phi$

1. Доказательство $F_1,...,F_n\vdash F(i)\supset\Phi$ получается переписыванием доказательства $F_1,...,F_n,F(i)\vdash\Phi$ (теорема о дедукции) и его длина линейно зависит от исходной.

2. $\vdash(\forall^{-k}_{x<N}F(x)\ \supset\ \bigvee_{0\le i\le k}F(i))$ — выражает тот факт, что если F(x) ложно при не более чем k значениях, то хоть при одном из k+1-го она истинна. Доказательство может быть длинным по k, но линейно по |F(x)|, так как от F — ничего не зависит.

3. $p\vdash\forall^{-k}_{x<N}F(x)$ имеет длину доказательства меньшую l, так как все эти формулы лежат на одном пути из корня, длина которого $\le l$.

Таким образом, $длина(p\vdash\Phi)<a*(k+1)*MAX_i\ (длина(p_i\vdash\Phi))\ +\ b*l\ +\ l$, где a — коэффициент удлинения из теоремы о дедукции, b — коэффициент из пункта 2, оценивая $|F(x)|<l$

Доказательство Теоремы

из Леммы 1 получаем:

$\{\}\vdash\Phi$, *то есть* $\vdash\Phi$

Оценим длина($\vdash\Phi$)

$длина(\vdash\Phi)<\ ((a+b)(k+l))^l\ <\ 2^{(c*l^2)}$, так как $k<l$, где c может зависеть от k.

Замечание 1. Эта теорема показывает, что безнадежно искать в ARS короткие доказательства для языков, нижние оценки длин доказательств которых растут быстрее экспоненты от полинома.

Замечание 2. Рассуждение проходит и в самой сильной системе, когда k=N-1; тогда правило $\dfrac{\forall^{-k}_{x<N}F(x)}{F(r)}$, может быть записано гораздо компактней: $\dfrac{\exists_{x<N}F(x)}{F(r)}$. Анализ показывает, что заключение теоремы сохраняет силу и в этом случае.

Глава 3.
Каноническая форма доказательств.

Один из первых вопросов возникших в связи с ARS, заключался в том, насколько в действительности важен параметр k в правиле случайной подстановки $\forall^{-k}_{x<N}$? Действительно, при k=0 правило случайной подстановки заменяется обычным правилом арифметики, и надеяться на полиномиально короткие доказательства не приходится, если только NP≠PSPACE. Интересно, что техника интерактивных доказательств обычно приводит к правилу с k=2 ([Ba]) или k=3 ([Sh]). Существенное использование техники работы с полиномами, кажется, не оставляет пути для уменьшения k.

Однако, ниже будет доказана теорема, показывающая, что k можно сделать равным 1. Следует отметить несколько важных моментов, следующих из этой теоремы: во-первых, для правила случайной подстановки важен факт случайности подставляемого числа, а не число контрпримеров — характерная черта интерактивных систем, во-вторых появляется возможность рассматривать системы лишь с k=1, что может быть полезно при установлении отрицательных результатов об ARS.

Определение: Обозначим через $\mathrm{ARS}^*(x^n)$ множество формул Φ имеющих доказывающее дерево T_Φ со следующими ограничениями:

1. Всякое применение правила случайной подстановки соответствует схеме с k=1, то есть имеет вид $\dfrac{\forall^{-1}_{x<N}:F(x)}{F(r)}$.

2. Максимальная длина пути дерева T_Φ не превосходит $|\Phi|^n$

Доказательства в такой системе будем называть *приведенными*.

Теорема 1. Для любой формулы Φ: $\Phi\in\mathrm{ARS}(x^n) \Rightarrow \Phi\in\mathrm{ARS}^*(x^{cn})$, где c зависит лишь от k -- числа контрпримеров в правиле случайной подстановки, дла которого $\Phi\in\mathrm{ARS}(x^n)$.

Если обозначить за T_Φ *и* T_Φ' соответственно доказывающие деревья формулы Φ в системах $\mathrm{ARS}(x^n)$ и $\mathrm{ARS}^*(x^{cn})$, то верны следующие утверждения:

1. $e(T_\Phi')=e(T_\Phi)$ (вероятность ошибки не изменяется)

2. $l(T_\Phi') < p(l(T_\Phi),k)$, где $p(.,.)$ — некоторый полином. В частности, поскольку $k<l(T_\Phi)$, длина увеличивается полиномиально.

Доказательство будет непосредственно следовать из Теоремы 2:

Теорема 2: Правило $\dfrac{\forall^{-k}_{x<N}:F(x)}{F(r)}$ моделируется правилом $\dfrac{\forall^{-1}_{x<N}:F(x)}{F(r)}$, в том смысле, что если $F_0=\forall^{-k}_{x<N}:P(x)$, $H=P(r)$ (*)
то существует последовательность формул $F_1, F_2,\ldots,F_n$ содержащих применение только правила $\dfrac{\forall^{-1}_{x<N}:F(x)}{F(r)}$, такая что результирующая формула F_n имеет вид $P(r)$, где величина r распределена как и в (*) --- равномерно.

При этом оказывается, что:

1. Длина $(F_0,\ldots,F_n) < p(|F_0|\ ,k)$ для некоторого полинома, не зависящего от F_0.

2. Переход $\dfrac{\forall^{-k}_{x<N}:F(x)}{F(r)}$ содержит ошибку тогда и только тогда, когда ее содержит последовательность $F_0=\forall^{-k}_{x<N}:P(x),\ F_1,\ldots,F_n=P(r)$.

Из Теоремы 2 немедленно следует Теорема 1. Первое утверждение следует из того, что вероятность получить ошибку при переходе от $\forall^{-k}_{x<N}:F(x)$ к $F(r)$ — не изменилась. Второе утверждение следует из того, что оставив в p(l,k) лишь положительные слагаемые имеем:

$p(|F|,k)+p(|G|,k) \le p(|F|+|G|,k)$, а значит и

$l(T_\Phi') \le p(|F_1|+|F_2|+\ldots+|F_n|,k) \le p(l(T_\Phi),k)$

Доказательство Теоремы 2

Сначала докажем несколько технических лемм.

Лемма 1. Предикат $C(a,b,n)$<—> $(a<b)\ \&\ (n=b*(b-1)/2+a)$ нумерует все упорядоченные пары { <a,b> | a<b }, и задает биекцию таких пар на натуральные числа.

```
<0,1>—><0,2>  <0,3>   <0,4>...
                 |     /    |          /  |
          <1,2>  <1,3>   /  .
                 |     /   .
               <2,3>    .
```

Доказуемы следующие формулы:

1. $\forall a,b\ \ \exists!\ n\ \ (a<b)\supset C(a,b,n)$
2. $\forall n\ \exists!\ a,b\ \ C(a,b,n)$
3. $\forall N\ \forall\ a,b,n\ C(a,b,n) \supset (n < N*(N-1)/2 \Leftrightarrow a<b<N)$ *(то есть все пары <a,b> вида a<b<N биективно отображаются на отрезок 0...N*(N-1)/2-1)*

Эти формулы носят ясный интуитивный смысл и могут быть доказаны по индукции.

Обозначение: $n=<a,b>$ обозначает $C(a,b,n)$.

Лемма 2. Для любой F(x)

$\vdash\forall N>1[\exists x_1\exists x_2\forall y_{<N}\ \ x_1=y \vee x_2=y \vee F(y)\Leftrightarrow\exists x_1<_N\exists x_2<_N(x_1<x_2)\&\forall y_{<N}(x_1=y \vee x_2=y) \vee F(y)\ ]$

Доказывается индукцией по N. Длина доказательства — линейна по |F(x)|.

Лемма показывает, что про те два числа, при которых F(x) может быть ложна, можно считать, что они различны и одно больше другого.

Лемма 3.

$$\forall\ x_1,x_2<N :\forall\ z<_{N(N-1)/2}:(x_1<x_2\ \&\ C(a,b,z)) \supset$$

$$((x_1=a\ \&\ x_2=b) \vee \exists\ c<2:(c=0\ \&\ a\neq x_1\ \&\ a\neq x_2 \vee c=1\ \&\ b \neq x_1\ \&\ b \neq x_2))$$

То есть если код пары z отличен от кода $<x_1,x_2>$, то хоть одно из двух закодированных z чисел не совпадает ни с x_1 ни с x_2. Действительно, ложность второго члена дизъюнкции в

заключении влечет $(x_1=a \vee x_2=a)\&(b=x_1 \vee b=x_2)$, но так как $x_1<x_2$, $a<b \supset x_1=a\&x_2=b$, значит истинен первый член дизъюнкции. Мы используем лишь то, что $x<y$ (посылка импликации) и $a<b$ (существование и упорядочение a и b — следствие Леммы 1).

Лемма 4.

$\vdash(\exists x_1<N\ \exists x_2<N\ \forall z<N(z=x_1 \vee z=x_2) \vee F(z)) \supset (\exists x \forall z_{<N(N-1)/2}\ \ z=x \vee \exists c_{<2} G(c,z))$, где $G(c,z) = \exists\ a,b\ C(a,b,z)\&(c=0\&F(a) \vee c=1\&F(b))$

Действительно, если

$(\exists x_1,x_2,z<N\ \ (z\neq x_1)\&(z\neq x_2)\&\mathbf{not}F(z))$, то можно показать, что доказуемо **not** $\forall^{-2}_{x<N}:F(x)$.

Значит, применяя Лемму 3, можно показать

$\forall^{-2}_{x<N}:F(x)\ \vdash\ \exists\ x_1,x_{2<N}\ \forall\ z_{<N(N-1)/2}(x_1<x_2)\ \&\ C(a,b,z) \supset [\ x_1=a\&x_2=b \vee \exists c_{<2}:(c=0\&a\neq x_1\&a\neq x_2\&F(a) \vee c=1\&b\neq x_1\&b\neq x_2\&F(b))\ ]$,

добиваясь с помощью Леммы 2, что бы $x_1<x_2<N$, получим:

$\forall^{-2}_{x<N}:F(x)\vdash\exists\ x_{<N(N-1)/2}\ \forall\ z_{<N(N-1)/2}\ \ x=z \vee G(c,z)$

Следствие 1: лемма 4 показывает, что

$\vdash\forall^{-2}_{x<N}:F(x)\supset \forall^{-1}_{y<N(N-1)/2}:G'(y)$,

где $G`(y)==\exists\ c_{<2}\ \ G(c,y)$

Лемма 5

$\vdash(\exists\ x_{<2}F(x)) \Leftrightarrow\forall^{-1}_{x<2}:F(x)$

Доказательство

$\forall^{-1}_{x<2}:F(x)==\ \exists\ y_{<2}\ \ \forall\ x_{<2}\ \ x=y \vee F(x) \Leftrightarrow \exists\ y_{<2}\ (0=y \vee F(0))\&(1=y \vee F(1)) \Leftrightarrow\exists y_{<2}F(0)\&(y=1) \vee F(1)\&(y=0) \vee F(0)\&F(1)) \Leftrightarrow F(0) \vee F(1) \Leftrightarrow \exists x_{<2}\ F(x)$

Длина доказательства — линейна по $|F(x)|$

Продолжение доказательства Теоремы 2.

Рассмотрим случай k=2

Смоделируем
$$\frac{\forall^{-2}_{x<N}:F(x)}{F(r_x)}\quad r_x \in 0...N-1$$

По следствию 1
$$\frac{\forall^{-2}_{x<N}:F(x)}{\forall^{-1}_{y<N(N-1)/2}:G'(y)}$$

Правило случайной подстановки
$0<=r_y<N(N-1)/2$
$$\frac{\forall^{-1}_{y<N(N-1)/2}:G'(y)}{G`(r_y)}$$

$G`$-сокращение
$$\frac{G`(r_y)}{\exists\ c_{<2}\ G(c,r_y)}$$

По лемме 5

$$\frac{}{\forall^{-1}\ c_{<2}\ G(c,r_y)}$$

Правило случайной подстановки

$$\frac{0<=r_c<=1 \qquad \forall^{-1}\ c_{<2}\ G(c,r_y)}{G(r_c,r_y)}$$

Но $G(r_c,r_y)==\exists\ a,b_{<N}\ r_y=<a,b>\ \&(r_c=0\&F(a)\ \vee\ r_c=1\&F(b))$

Пусть для определенности $r_c=0$

$$\frac{}{G(0,r_y)}$$

$$\frac{G(0,r_y)}{\exists\ a,b\ r_y=<a,b>\ \&\ F(a)}$$

$$\frac{\exists\ a,b\ r_y=<a,b>\ \&\ F(a)}{F(a) \qquad (*)}$$

где a — то единственное число, для которого $\exists$ b C(a,b,r_y).

Возможность последнего перехода обосновывается тем, что r_y — число, а про спаривающую функцию доказано, что$\forall$z $\exists!$ a,b z=<a,b>.

Итак, в случае k=2, мы заменили одно применение правила в системе

$\forall^{-2}$ двумя правилами в системе $\forall^{-1}$.

Покажем, что так получаемое число a в формуле (*) — равномерно распределено на интервале 0...N-1. Действительно, вероятностное пространство r_y=0,1,...,N(N-1)/2-1 r_c=0,1. То есть имеем N(N-1) пар вида (r_c,r_y). Но каждое число r $\in$ 0...N-1 можно получить ровно из N-1 пары вида (r_c,r_y), а именно

(1,<0,r>) (1,<1,r>) ... (1,<r-1,r>) r-пар такого вида

(0,<r,r+1>) (0,<r,r+2>) ... (0,<r,N-1>) N-1-r-пар такого вида

(так как r_c выбирает правый или левый элемент r_y соответственно).

Тем самым, из случайных величин (r_c,r_y) мы можем получить любое число из промежутка 0..N-1 с равной вероятностью — что и требовалось доказать.

Покажем, что переходы (1) и (2) (см. ниже) содержат или не содержат ошибку одновременно.

$$* \ \frac{\forall^{-2}_{x<N}:F(x)}{F(r_x)} \ (1) \qquad \frac{\forall^{-2}_{x<N}:F(x)}{\forall^{-1}_{y<N(N-1)/2}:G'(y)} \ (2)$$

$$* \ \frac{\forall^{-1}_{y<N(N-1)/2}:G'(y)}{G`(r_y)}$$

$$\frac{G`(r_y)}{\forall^{-1}c_{<2}\ G(c,r_y)}$$

$$* \ \frac{\forall^{-1}c_{<2}\ G(c,r_y)}{G(r_c,r_y)}$$

$$\frac{G(r_c,r_y)}{F(r_x)}$$

* — отмечены места вывода, где может появиться ошибка

r_x — одинаково в обоих переходах.

a. (2) не содержит ошибки => (1) не содержит ошибки

Доказательство: Если $\vdash \forall^{-2}_{x<N} : F(x)$, то по определению ошибки в доказательстве, все формулы (2) — доказуемы, то есть $\vdash F(r_x)$, и поэтому (1) не содержит ошибки.

в. (1) не содержит ошибки => (2) не содержит ошибки

Доказательство: Если $\vdash \forall^{-2}_{x<N} : F(x)$ и $\vdash F(r_x)$, то r_y

необходимо имеет вид $<r, r_x>$ или $<r_x, r>$, а значит $\vdash G`(r_y)$, но $G(r_c, r_y) <-> F(r_x)$ и следовательно оба перехода не содержат ошибки.

Тем самым, мы доказали, что в случае k=2 данная процедура преобразует доказывающее дерево Тф при k=2 в доказывающее дерево Тф' при k=1, при этом вероятность ошибки не изменилась, а увеличение длины доказательства происходит лишь за счет формул внутри участка моделирования (где на каждом участке увеличение оценивается некоторым полиномом от |F|, не зависящим от F — это видно из того, что конкретный вид F — нигде не использовался, а все вспомогательные леммы вносят константную или линейную от |F| добавку к доказательству).

Для доказательства теоремы при k>2 рекурсивно повторим проделанное преобразование. Для данного k будем рассматривать упорядоченные наборы из k различных чисел. Тогда если формула Ф верна для всех значений x кроме может быть k, то о произвольном наборе чисел $[x_1 < x_2 <\ldots< x_k]$, можно сказать, что он либо совпадает с набором контрпримеров к Ф, либо хоть одно из чисел входящих в него не является контрпримером к Ф. Индекс i числа в нашем наборе, которое не является контрпримером можно соотнести с log(i) чисел $c_j<2$, кодирующих двоичную запись i.

Пусть формула G(c,y) выражает утверждение: y — кодирует набор чисел, в котором при c=0 левая часть, а при c=1 — правая, содержит число x, такое что $\vdash F(x)$.

Напишем последовательность формул

$G_0(c_0,y) == \exists\, a,b_{<=y}\ \ y=<a,b> \ \&\ (c_0=0\&F(a) \vee c_0=1\&F(b))$ $G_{j+1}(c_{j+1},y) == \exists\, a,b<=y+1$ $y=<a,b> \ \&\ \exists\, c_{j<2}\ (c_{j+1}=0\&G_j(c_j,a) \vee c_{j+1}=1\&G_j(c_j,b))$

Тогда $G_{\log(k)}$ — то, что нам нужно.

Доказательство Теоремы 2 состоит в доказательстве следующих выводов:

$\forall^{-k}_{x<N} : F(x)$ $\qquad (k=2^j)$

$\forall^{-1} x_{<poly(N)}\ \exists\, c_j <2\ G_j(c_j,x)$

$\exists\, c_{j<2}\ \ G_j(c_j,r_x)$, x — код набора из к чисел

$\forall^{-1} c_{j<2}\ \ G_j(c_j,r_x)$

$G_j(r_{cj},r_x)$

$\exists\, c_{j-1}\ G_{j-1}(c_{j-1},r_{1x})$, r_{1x} -правая или левая половина списка r_x

---

.

. $F(r)$

Всего log(k)+1 применения правила случайной подстановки.

Аналогичное рассуждение показывает, что F(r) — формула, где r -равномерно распределенная случайная величина. Аналогично случаю k=2 показывается, что данное преобразование не изменяет ошибки доказательства.

Примечания

1. Нам было существенно необходимо, чтобы $x_1 < ... < x_k$ (строгие неравенства). Тогда если a и b — коды списков из t элементов, то <a,b> может оказаться неправильным кодом списка из 2t элементов (нам нужно, чтобы все числа списка a были меньше чисел списка b). $a=\{x_1<...<x_t\}$ $b=\{y_1,...,y_t\}$ и $x_t<y_1$. Этого можно добиться введя не одну спаривающую функцию C(a,b,n), а log(k), так чтобы помимо конкатенации они еще и проверяли правильность упорядочения в объединяемых списках. При фиксированном k доказательство всех соответствующих теорем об этих log(k) предикатах $C_j(a,b,n)$ займет константное место, и значит не отразится на полиномиальности увеличения общего доказательства от |Φ|.

2. В вышеприведенном доказательстве было использовано порядка log(k) формул длины порядка $|\forall^{-k}_{x<N}:F(x)|$, то есть хотя $|r_x|$~k|N|, так как это код k чисел длины ~|N|, но и формулы $\forall^{-k}_{x<N}:F(x)$ требуют столько же места из-за k кванторов $\exists x_i<N$. Таким образом общее увеличение длины --- не более чем в c*log(k) раз, при некотором c. Таким образом Теорема 2 и Теорема 1 доказаны.

Заключение

В заключении хотелось бы упомянуть о результатах не вошедших в работу и об открытых вопросах. Основной нерешенной проблемой остается характеризация выразительной силы ARS, или более точно, иерархии $ARS(x^n)$:

Проблема: Пусть язык $L \in PSPACE$ и состоит из доказуемых арифметических формул, что можно сказать о сложности доказательства формул из L в ARS ?

Имеются примеры, основанные на диагональной конструкции, показывающие, что некоторые очень простые языки (из PTIME) не имеют коротких доказательств в $ARS(x^n)$.

Утверждение: Существует $L \in PTIME$: L состоит только из доказуемых формул и $\forall n\ L \notin ARS(x^n)$.

Следует отметить, однако, что доказуемость формул из L показывается метаматематически.

Другой открытый вопрос касается того, на сколько точна иерархия $ARS(x^n)$: Гипотеза: Существует константа c>1, такая что $ARS(x^n) \neq ARS(x^{cn})$.

Эта гипотеза, как кажется, тесно связана со следующим вопросом:

Пусть P(x) - предикат, определяющий язык L (то есть $n \in L$ <=> P(n)), и пусть $L \in PSPACE$. Верно ли, что тогда существует арифметизация P(x), скажем A(n), такая что $P(n) \Leftrightarrow \vdash A(n)$ и при некотором m: $\{A(n) \mid n \in N \ \&\ \vdash A(n)\} \in ARS(x^m)$, то есть предикат P—равномерно “быстро” доказуем ?

Следующий вопрос тесно связан с получением через доказательства в ARS верхних оценок для языков арифметических формул:

“принцип рефлексии”

Пусть A([ф]) -- арифметическая формула, такая что $\vdash A([ф]) \Rightarrow \vdash Prov([ф])$. Пусть мы знаем, что $\vdash ф$. В каких ситуациях можно быстро доказать в ARS $(A([ф]) \supset ф)$?

Ответ на этот вопрос дал бы возможность устанавливать верхние оценки сложности доказательства.

Литература

[Ba] L.Babai, L.Fortnow, *Acharacterization of #P by Arithmetic Straight Line Programs.* Proceedings of the 31st Annual Simposium on Foundation of Computer Science, 1990, pp26-34.

[Да] Е.Я. Данцин, *Доказательства в арифметике, использующие случайные числа*, сборник ПОМИ РАН 1994.

[Kleene] S.Kleene, *Introduction to Metamathematics*: North Holland, 1952

[LFKN] C.Lund, L.Fortnow, H.Karloff anf N.Nisan, *Algebraic Methods for for Interactive Proof Systems.* Proceedings of the 31st Annual Simposium on Foundation of Computer Science, 1990, pp2-10.

[Sh] A.Shamir, *IP=PSPACE.* Proceedings of the 31st Annual Simposium on Foundation of Computer Science, 1990, pp11-15.