О научном вкладе Б. А. Субботовской

А. А. Разборов

Если смотреть на число публикаций, их суммарный объём и т. д., научное наследие Беллы Абрамовны покажется сравнительно небольшим. Оно включает две краткие заметки в «Докладах АН СССР» [1, 2] (составившие, насколько мне известно, основу ее кандидатской диссертации) и пару статей, опубликованных в конце 1960-х уже под фамилией Мучник. Однако, как это часто бывает в математике, ценность работ Субботовской определяется далеко не их количеством.

Моя задача весьма облегчается тем обстоятельством, что о теории вычислительной сложности (к которой и относятся работы Беллы Абрамовны) журнал уже подробно писал в недавнем прошлом [3–5, 9]. Более того, [4, с. 80] содержит краткое изложение главного результата Субботовской, и даже с наброском доказательства. Поэтому я просто постараюсь дать некоторое представление о месте, занимаемом ее научными достижениями в общей картине.

Прежде всего следует напомнить, о чём вообще идет речь. Ввиду наличия вышеупомянутых статей [3–5, 9] я буду предельно краток: почти весь материал, приводимый здесь в сжатой форме, можно найти в этих статьях.

Теория вычислительной сложности занимается изучением алгоритмов для решения алгоритмических задач с точки зрения их эффективности. Большинство этих задач можно без ограничения общности представить как задачу вычисления некоторого отображения $f\colon \{0,1\}^* \longrightarrow \{0,1\}$ из множества конечных двоичных слов в $\{0,1\}$. Всякое такое отображение f можно альтернативным образом рассматривать как последовательность $\{f_n\colon \{0,1\}^n \longrightarrow \{0,1\} \mid n = 1,2,\dots\}$ булевых функций. Вычислительные модели бывают *однородными* (машины Тьюринга, машины с произвольным доступом к памяти (RAM) и т. д.) и *неоднородными*. В однородных моделях одно и то же (конечное) устройство M должно вычислять $f(x)$ для всех слов x вообще, а в неоднородных — для каждого n имеется свое отдельное устройство M_n, вычисляющее булеву функцию f_n. Алгоритмы в однородных и неоднородных моделях настолько хорошо и естественно транслируются друг в друга с сохранением их эффективности, что в большом числе случаев эти два класса моделей можно вообще не различать между собой. С точки зрения такого соответствия наиболее важными неоднородными моделями являются *схемы из функциональных элементов* и *логические формулы*, а наиболее важной мерой эффективности — *размер*, определяемый как число использованных элементов. Схемы отличаются от формул тем, что в них результаты промежуточных вычислений разрешается использовать более одного раза. Важной составной частью определения как схем так и формул является конечное

множество B допустимых в них элементов, называемое *базисом*; базис B полон, если любая булева функция в принципе представима в виде суперпозиции его элементов. *Стандартный базис* — это базис $B_0 = \{\vee, \&, -\}$. От замены одного полного базиса другим минимальный размер $\mathrm{size}_B(f)$ схемы из функциональных элементов в базисе B, вычисляющей булеву функцию f может измениться не более, чем на постоянный множитель [4, теорема 7]. Почти очевидное доказательство этого факта, однако, не проходит для случая логических формул, и для них инвариантность минимального размера представляющей формулы от выбора базиса удается установить лишь с точностью до полинома [4, задача 17], причем доказательство уже далеко не настолько тривиально.

Центральный результат Субботовской [1] как раз и состоит в том, что такое различие в поведении между схемами и формулами неслучайно и с точки зрения представимости формулами одни полные базисы могут быть существенно лучше других (т. е. размер минимального представления одной и той же булевой функции может отличаться более, чем на постоянный множитель). Именно, если добавить к B_0 функцию $x \oplus y$ сложения в поле $\mathbb{F}_2$ (т. е. «по модулю 2»), то тогда, конечно, линейную форму $x_1 \oplus \ldots \oplus x_n$ от n переменных можно вычислить формулой размера $O(n)$. Субботовская доказала, что без расширения базиса ситуация меняется принципиально, и всякая формула в стандартном базисе B_0, вычисляющая $x_1 \oplus \ldots \oplus x_n$, обязана иметь размер $\epsilon n^{3/2}$, где $\epsilon > 0$ — некоторая константа. Развивая эти идеи, в [2] ею был установлен гораздо более общий факт. Именно, Лупанов ранее доказал, что в контексте представимости булевых функций формулами базис B_0 вообще является самым плохим и всякий другой полный базис B либо эквивалентен B_0 либо (как, например, $B \cup \{\oplus\}$) является строго более сильным. Белле Абрамовной удалось получить полную, элегантную и чисто комбинаторную характеризацию тех полных базисов, которые эквивалентны B_0.

Всё, что написано выше про теорию вычислительной сложности, относится к жанру «Взгляд из 21 века». В начале 1960-х годов картина выглядела совсем по-другому. Хотя однородные модели (в основном машины Тьюринга) были известны уже довольно давно, концепция *сложности* алгоритмов только начинала зарождаться, и до работ, в которых были заложены математические основы теории вычислительной сложности, оставалось еще добрых пять лет (а до формулировки ключевой в этой области «проблемы $P \stackrel{?}{=} NP$» — и все десять). Теоретическое значение неоднородных моделей (таких, как схемы, формулы и весьма популярные в то время «контактные схемы») еще не было осознано, и даже сам термин «неоднородные» (non-uniform) появился намного позднее. Схемы и формулы рассматривались в основном с инженерной точки зрения, как прототип реальных устройств, используемых в электронной промышленности.

Тем удивительнее появление на этом фоне в начале и середине 1960-х годов ярких результатов в *теории* сложности булевых функций, по существу заложивших основы для ее бурного развития в 1980-е годы. Работы Субботовской занимают весьма достойное место в ряду этих результатов, и по значимости они вполне сравнимы с классическими результатами Маркова [6] и Нечипорука [7].

В какой-то степени работам Субботовской «повезло» меньше, чем работам Маркова и Нечипорука — ее основной результат был впоследствии усилен Храпченко [8], и сейчас нижняя оценка формульной сложности для функции $x_1 \oplus \ldots \oplus x_n$ ассоциируется в основном с последней работой. Есть, однако, два важных характерных момента, касающихся именно работ Беллы Абрамовны, которыми мне бы и хотелось закончить свою заметку.

Во-первых, следует особо отметить использованный ею способ доказательства, получивший впоследствии название «метод случайных подстановок». Сегодня этот метод является одним из наиболее важных, мощных и широко распространенных в теории сложности булевых функций (а в последние годы — и в родственной теории сложности доказательств). Насколько мне известно, впервые этот метод встретился именно в [1].

Второе и последнее замечание касается всей программы классификации полных базисов с точки зрения их эффективности, начатой Лупановым и сравнительно недавно продолженной Стеценко, Черухиным и Перязевым. Эта программа в какой-то степени предугадала современную тенденцию, когда вместо исследования сложности изолированных алгоритмических задач изучают так называемые *классы сложности* (см., например, [3, 5]) и особое внимание уделяют *структурным* вопросам об этих классах.

Список литературы

[1] Субботовская Б. А. *О реализации линейных функций формулами в базисе* $\vee, \&, -$ // ДАН СССР, 1961. Т. 136, №3. С. 553–555.

[2] Субботовская Б. А. *О сравнении базисов при реализации функций алгебры логики формулами* // ДАН СССР, 1963. Т. 149, №4. С. 784–787.

[3] Разборов А. А. *О сложности вычислений* // Математическое просвещение. Третья серия. Вып. 3. 1999. С. 127–141.

[4] Верещагин Н. К., Шень А. *Логические формулы и схемы* // Математическое просвещение. Третья серия. Вып. 4. 2000. С. 53–80.

[5] Вялый М. Н. *Сложность вычислительных задач* // Математическое просвещение. Третья серия. Вып. 4. 2000. С. 81–114.

[6] Марков А. А. *О минимальных контактно-вентильных двухполюсниках для монотонных симметрических функций* // Проблемы кибернетики. Наука, 1962. Т. 8, С. 117–121.
(Eng. transl.: A. A. Markov, On minimal switching-and-rectifier networks for monotone symmetric functions, *Problems of Cybernetics*, vol. 8, 117–121 (1962).)

[7] Нечипорук Э. И. *Об одной булевской функции* // ДАН СССР, 1966. Т. 169, №4. С. 765–766.
(Eng. transl.: E. I. Nečiporuk, On a Boolean function, *Soviet Mathematics Doklady* 7:4, pages 999–1000.)

[8] Храпченко В. М. *О сложности реализации линейной функции в классе π-схем* // Математические заметки, 1971. Т. 9, №1. С. 35–40.
(Eng. transl.: V.M. Khrapchenko, Complexity of the realization of a linear function in the class of π-circuits, *Math. Notes Acad. Sciences USSR* 9(1971), 21–23.)

[9] Smale S. *О проблемах вычислительной сложности* // Математическое просвещение. Третья серия. Вып. 4. 2000. С. 115–119.