О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Т о м 21 М А Т Е М А Т И К И В ы п у с к 4
2014

Г. В. Б а л а к и н, **В. Г. Н и к о н о в** (Москва, ТВП). **Псевдобулевы методы решения систем нелинейных булевых уравнений.**

В настоящем докладе авторами рассмотрены возможности применения в задачах дискретной математики при анализе систем дискретных уравнений псевдобулевых или пороговых методов, основанных на сведении исходных задач в область вещественных значений, показать возможные преимущества этого замысла и проследить ожидаемые перспективы его дальнейшего развития.

Исходная идея псевдобулевых методов известна уже примерно 50 лет, благодаря работам таких авторов, как Иванеску, Рудеану (см. [3, 5]) и уже докладывалась авторами на осенней сессии нашего симпозиума в 2012 году [20]. Первоначально эта идея ставила целью использовать для решения дискретных задач хорошо развитый аппарат математики в действительной области. Для обоснования возможности сведения булевых задач в действительную область и был разработан аппарат псевдобулевых функций, заданных на множестве булевых неизвестных и принимающих действительные значения. Псевдобулевы ограничения представляют собой неравенства, сравнивающие значения псевдобулевой функции с некоторым действительным числом и имеют множество решений, по своей природе соответствующее множеству единичных вершин некоторой булевой функции или системы булевых функций.

На использовании этой связи и построено все множество псевдобулевых методов, с достаточной полнотой рассмотренное в работах [13–15]. В частности, если псевдобулевы функции — линейные, то каждое булево уравнение требует замены на систему линейных неравенств или в геометрическом смысле — разделяющих плоскостей. Так строится метод разделяющих плоскостей, предназначенный для решения систем булевых уравнений, включающий как проблему представления произвольного булевого уравнения в виде системы линейных неравенств и минимизации их числа, так и разработку алгоритмов решения результирующих систем неравенств.

Развитию различных аспектов этого метода было посвящено большое количество работ, а сам метод разделяющих плоскостей можно рассматривать в качестве первого псевдобулевого метода, разработанного непосредственно для анализа и решения систем булевых уравнений. Упомянутые работы, связанные с данным методом, условно можно разделить на две группы. К первой относятся исследования, связанные со сведением произвольного булевого уравнения к равносильной системе линейных неравенств. Одно линейное неравенство с булевыми неизвестными, как известно, задает пороговую булеву функцию, а задание произвольной булевой функции в виде системы линейных неравенств можно трактовать как представление ее в базисе пороговых функций, или в пороговом базисе.

В дискретной математике изучение свойств пороговых функций, факта принадлежности функций классу пороговых и способов представления произвольных булевых функций в пороговом базисе составили целое направление, получившее название «пороговая логика» (см. [4]). Особый интерес это направление получило после экспериментального обнаружения того факта, что нейроны живых организмов в первом приближении работают как пороговые элементы [1, 11]. Развитие этого обстоятельства привело к построению особого вида ЭВМ — нейрокомпьютеров, моделирующих работу нейронных сетей живых организмов и обладающих способностью к обучению.

На современном этапе интерес к пороговой логике подогревается потенциальной возможностью реализации базовой операции пороговой функции — скалярного произведения непосредственно в среде — носителе сигнала, т. е. в случае оптической реализации — со скоростью света. Перечисленные предпосылки привел к появлению большого числа публикаций как в области основ пороговой логики, так и в части указанных приложений. Широкую известность получили монографии [4] и [9], в которых значительное внимание было уделено изучению свойств пороговых булевых функций (например, свойства полной монотонности) и распознаванию принадлежности функции классу пороговых с нахождением коэффициентов задающей ее линейной формы и значения порога.

Задача распознавания и сама по себе носит прикладной характер, так как сводится к нахождению параметров преобразования автомата. Несмотря на простоту постановки решение этой задач оказалось достаточно сложным и достигалось с помощью итеративного алгоритма, изложенного, например, в работе [4]. Алгоритм базировался на подсчете некоторых параметров роста (убывания) функции по направлению каждой переменной, принимаемых в качестве первого приближения коэффициентов линейной формы и, в общем случае, требовал итеративной корректировки. Забегая вперед и переходя к пороговым k-значным функциям необходимо отметить, что построение подобного алгоритма сопряжено уже с очень большими трудностями, начиная с неоднозначности характеризации параметров роста в k-значном случае. Вместе с тем, рассматривая эту задачу с современных позиций, подчеркнем, что ее формулировка и в булевом, и в k-значном случаях вкладывается в условия применимости полиномиального алгоритма Л. Г. Хачияна. Такое сведение, правда, почти всегда приводит к существенно большим алгоритмическим затратам, нежели упомянутый итеративный путь, но тем не менее в теоретическом плане дает четкую характеризацию этой задачи.

Значительно более сложной является вторая выделенная задача пороговой логики — задача представления произвольной булевой функции (лучше сказать — булевого уравнения) в пороговом базисе. Для метода разделяющих плоскостей она является важнейшей, так как непосредственно связана со сведением произвольного булевого уравнения к системе линейных неравенств, желательно минимальной. Со сложностной точки зрения эта задача занимает единую нишу с хорошо известной задачей минимизации ДНФ, точнее, с построением кратчайшей ДНФ, содержащей минимальное число элементарных конъюнкций.

Серьезное продвижение в этой проблематике сопряжено непосредственно с развитием метода разделяющих плоскостей в работах В. Г. Никонова (см. [14–16]). В этих работах автор указал способ построения искомых неравенств и оригинальный геометрический подход к доказательству минимальности полученных систем неравенств. Этот подход основах на выделении в n-мерном единичном кубе таких пар вершин, подлежащих отсечению, которые не могут быть отсечены одновременно. Наибольшее число вершин, попарно неотсекаемых, дает оценку снизу числа неравенств в минимальной системе, а в случае совпадения этих чисел — доказывает минимальность. Важным достижением автора явилось составление каталога минимальных систем неравенств (разделяющих плоскостей) для всех булевых функций 4-х-переменных, разбитых на 402 типа, с приведением не только самих систем неравенств, но и доказательств их минимальности указанным способом. Таким образом была создана теоретическая основа сведения произвольной системы булевых уравнений к равносильной относительно булевых решений системе линейных неравенств.

Вторая самостоятельная группа исследований в рамках метода разделяющих плоскостей посвящена проблеме решения систем линейных неравенств, получающихся после описанной процедуры сведения. Для того чтобы дать общую характеристику этой проблемы и путей ее разрешения, целесообразно рассмотреть два взаимосвязанных свойства систем линейных неравенств, а именно, взглянуть на них с аналитической и с геометрической точек зрения.

Как аналитический объект система линейных неравенств состоит из простых, арифметических по своей природе, неравенств, в которых можно переносить слагаемые из одной части неравенства в другую, которые можно складывать, умножать и в общем случае из которых можно формировать различные новые неравенства — следствия в виде линейных комбинаций исходных. По ряду своих свойств системы линейных неравенств близки системам линейных уравнений (см. [2, 6, 7, 8]).

Геометрический подход исключительно полезен для описания множества решений системы линейных неравенств, которое образует некоторый, в общем случае, многогранник в n-мерном пространстве. Действительно, каждое неравенство делит n-мерное пространство на два полупространства — решений и не решений, а формирование системы неравенств приведет к пересечению этих полупространств с образованием многогранника, возможно пустого многогранника, если система неравенств несовместна. Взаимное пересечение плоскостей при образовании этого многогранника приводит к образованию вершин или узлов, ребер и т. д., а сам многогранник является выпуклым.

Некоторые методы анализа и решения линейных псевдобулевых равенств и неравенств предложены в работах Г. В. Балакина [10, 12, 17, 18, 19, 21, 22].

В докладе будут проиллюстрированы прикладные возможности этих методов, например, для изучения запретов функций k-значной логики [23, 24], решения задач дискретной оптимизации и проч. В развернутом виде доклад представлен к публикации в одном из ближайших выпусков журнала «Обозрение прикладной и промышленной математики».

СПИСОК ЛИТЕРАТУРЫ

1. *McCulloch W.*, *Pitts W.* A logical calculus of the ideas immanent in nervous activity. — Bull. Math., Biophys, 1943, № 5, p. 115–133.
2. *Черникова Н. В.* Алгоритм для нахождения общей формулы неотрицательных решений системы линейных неравенств. — Вычисл. матем. физ., 1965, т. 5, № 2, с. 34–337.
3. *Ivanescu P. L.*, *Rudeanu S.* Pseudoboolean methods for bivalent programming. — Lect. Notes. Math., 1966, v. 23.
4. *Дертоузос М.* Пороговая логика. М.: Мир, 1967, 462 с.
5. *Hammer* (*Ivanescu*) *P. L.*, *Rudeanu S.* Boolean Methods in Operations Research and Related Areas. Berlin etc.: Springer, 1968.
6. *Черников С. Н.* Линейные неравенства. М.: Наука, 1968.
7. *Рыбашов Н. В.*, *Дудников Е. Е.* Градиентные методы решения линейных равенств, неравенств и задач линейного программирования на ЭВМ. М.: Советское радио, 1970.
8. *Корбут А. А.*, *Финкельштейн Ю. Ю.* Дискретное программирование М.: Наука, 1970.
9. *Бутаков Е. А.* Методы синтеза релейных устройств на пороговых элементах. М.: Энергия, 1970.
10. *Balakin G. V.* On the number of solutions of systems of pseudo-Boolean random equations. — В кн.: Вероятностные методы дискретной математики. М./Утрехт: ТВП/VSP, 1993, p. 71–98.
11. *Вальцев В. Б.*, *Григорьев В. Р.*, *Никонов В. Г.* Некоторые структурные принципы организации высших функций мозга. — В кн.: Нейрокомпьютер как основа мыслящих ЭВМ, РАН, отд. физиологии. М.: Наука, 1993, с. 38–46.

12. *Балакин Г. В.* О возможности решения систем линейных целочисленных уравнений методом выделения и оценки отдельных неизвестных. — Дискретн. матем., 1994, т. 6, в. 1, с. 116–126.
13. *Балакин Г. В.*, *Никонов В. Г.* Методы сведения булевых уравнений к системам пороговых соотношений. — Обозрение прикл. промышл. матем., 1994, т. 1, в. 3, с. 389–401.
14. *Никонов В. Г.* Пороговые представления булевых функций. — Обозрение прикл. промышл. матем., 1994, т. 1, в. 3, с. 402–457.
15. *Никонов В. Г.* Классификация минимальных базисных представлений всех булевых функций от четырех переменных. — Обозрение прикл. промышл. матем., 1994, т. 1, в. 3, с. 458–545.
16. *Никонов В. Г.* Покрытия булевых графов. – Дискретн. матем., 1994, т. 6, в. 4, с. 21–34.
17. *Балакин Г. В.* О вероятностном подходе к решению систем уравнений с целочисленными неизвестными. — Дискретн. матем., 1995, т. 7, в. 1, с. 88–98.
18. *Балакин Г. В.* Линейные псевдобулевые неравенства. — Матем. вопросы криптографии, 2010, т. 1, в. 3, с. 5–18.
19. *Балакин Г. В.* О структуре решений системы из линейных псевдобулевых неравенств. — Матем. вопросы криптографии, 2012, т. 3, в. 3, с. 5–20.
20. *Балакин Г. В.*, *Никонов В. Г.* Псевдобулево направление в дискретной математике. — Обозрение прикл. промышл. матем., 2012, т. 19, в. 6.
21. *Балакин Г. В.* О решении некоторых классов систем булевых уравнений рекуррентного типа. — Матем. вопросы криптографии, 2013, т. 4, в. 1, с. 5–25.
22. *Балакин Г. В.* О возможности частичного восстановления некоторых последовательностей по наблюдениям. — Матем. вопросы криптографии, 2013, т. 4, в. 4.
23. *Никонов В. Г.*, *Никонов Н. В.* Запреты k-значных функций и их связь с проблемой разрешимости систем уравнений специального вида. — Вестник РУДН. Сер. прикл. и компьют. матем., 2003, т. 2, №1, с. 77–93.
24. *Никонов Н. В.* Полиэдральные классы функций kзначной логики с обобщенными запретами и полузапретами. — Матем. вопросы криптографии, 2012, т. 3, в. 1, с. 53–69.