

С. Ю. К а т ы ш е в, М. С. П р и с м а к о в (Москва, Лаб. ТВП). **Использование алгоритмов поиска ближайших соседей для решения систем нелинейных уравнений.**

УДК 004.056.55

DOI https://doi.org/10.52513/08698325_2022_29_1_1

Резюме: В данной работе предлагается способ решения системы нелинейных уравнений с помощью перехода к системе уравнений с искаженной правой частью специального вида, для решения которой предлагается применить алгоритмы поиска ближайших соседей.

Ключевые слова: системы нелинейных уравнений, системы уравнений с искаженной правой частью, алгоритмы поиска ближайших соседей

Системы нелинейных уравнений встречаются при решении ряда физических задач, в различных краевых задачах, задачах минимизации, а также в криптографии с открытым ключом. В [1] рассматриваются различные методы решения систем нелинейных уравнений. Как известно, решение системы нелинейных уравнений в общем случае является NP-полной задачей и имеет экспоненциальную сложность (см. [2]).

В данной работе предлагается перейти от систем нелинейных уравнений к *системам уравнений (СУ) с искаженной правой частью*. В 1997 в работе [3] было введено это понятие, где для нахождения истинного решения системы булевых уравнений с искаженной правой частью предлагается применить метод максимального правдоподобия (ММП), который сопоставим по трудоемкости с тотальным перебором.

Для решения системы

$$\left\{ f_m(x_1, x_2, \dots, x_n) = a_m, \quad m \in \{1, 2, \dots, t\}, \right. \quad (1)$$

нелинейных булевых уравнений перейдем к системе уравнений с искаженной правой частью специального вида:

$$\left\{ f_m^{(1)}(x_1, x_2, \dots, x_{[n/2]}) + f_m^{(2)}(x_{[n/2]+1}, \dots, x_n) = a_m + \xi_m, \quad m \in \{1, 2, \dots, t\}, \right. \quad (2)$$

где $(\xi_1, \xi_2, \dots, \xi_t)$ — вектор ошибок (искажений). Искажение ξ_m в каждом уравнении системы (2) будет появляться за счет удаления из уравнения таких мономов

$$x_{i_1} x_{i_2} \dots x_{i_k}, \quad \text{что существует} \quad (3)$$

$$\text{хотя бы одна пара } i_{j_1} \in \left\{ 1, 2, \dots, \left\lfloor \frac{n}{2} \right\rfloor \right\} \text{ и } i_{j_2} \in \left\{ \left\lfloor \frac{n}{2} \right\rfloor + 1, \dots, n \right\}.$$

Если $\varphi_m(x_{i_1}, x_{i_2}, \dots, x_{i_l})$ — функция, которая содержит все мономы вида (3), то

$$\mathbf{P}\{\xi_m = 1\} = \frac{\|\varphi_m(\mathbf{x})\|}{2^l}. \quad (4)$$

Если вероятности $\mathbf{P}\{\xi_r = 1\}$ малы, то можно воспользоваться идеей метода согласования. А именно, перебрав всевозможные значения переменных $x_{[n/2]+1}, \dots, x_n$, запишем в память векторы

$$(f_1^{(2)}(x_{[n/2]+1}, \dots, x_n) + a_1, \dots, f_t^{(2)}(x_{[n/2]+1}, \dots, x_n) + a_t).$$

Полученное множество обозначим S . После этого на всевозможных значениях переменных $x_1, \dots, x_{[n/2]}$ для векторов

$$(f_1^{(1)}(x_1, x_2, \dots, x_{[n/2]}), \dots, f_t^{(1)}(x_1, x_2, \dots, x_{[n/2]}))$$

найдем ближайшего соседа в множестве S . Остается подставить потенциальное решение $(x_1^k, x_2^k, \dots, x_n^k)$ в систему (1).

В работе [4] доказано, что в предварительно обработанном множестве из N элементов можно найти k ближайших соседей к запросу q за время, равное $O(\max\{k, \log N\})$. Здесь под предварительной обработкой подразумевается построение диаграммы Вороного, что происходит за время $O(N \log N)$.

В итоге предложенный метод решения систем из t уравнений с n неизвестными на предварительном этапе требует времени, равного $O(2^{n/2})$, а на оперативном этапе — $O(2^{n/2})$. При этом используется $O(t \cdot 2^{n/2})$ ячеек памяти.

По итогам анализа данной темы остаются открытыми такие вопросы, как правильный и эффективный способ разделения переменных, в том числе для минимизации вероятностей $\mathbf{P}\{\xi_m = 1\}$, а также выбор эффективных алгоритмов поиска ближайших соседей.

СПИСОК ЛИТЕРАТУРЫ

1. Ортега Дж., Рейнболдт В. Итерационные методы решения нелинейных систем уравнений со многими неизвестными. Пер. с англ. Э.В. Вершкова и др. Под ред. И.В. Коновальцева. М.: Мир, 1988, 560 с. // *Ortega J. M., Rheinboldt W. C. Iterative Solution of Nonlinear Equations in Several Variables*. San Diego, CA: Academic Press, 1970, 572 p. (Ser. Compute Sci. Appl. Math.)
2. Wolf C. Hidden Field Equations (HFE) — Variations and Attacks. Diplomarbeit. Ulm: Universität Ulm, 2002, 87 p.
3. Балакин Г.В. Введение в теорию случайных систем уравнений. В кн.: Труды по дискретной математике. Т. 1./Под общей ред. В.Н. Сачкова. М.: ТВП, 1997, с. 1–18. // *Balakin G. V. Introduction to the theory of systems of random equations*. In: *Proceedings in Discrete Mathematics*. / Ed. by V.N. Sachkov et al. Moscow: TVP Sci. Publ., 1997, p. 1–18. (In Russian.)
4. Shamov M.I., Hoey D. Closest-point problems. In: 16th Annual Symposium on Foundations of Computer Science — SFCS'1975. (Berkeley, October 13–15, 1975.) Piscataway, NJ: IEEE, 1975, p. 151–162.

Дата поступления в редакцию:
24.IX.2022

UDC 004.056.55

***Katyshev S. Y., Prismakov M. S.* (Moscow). Using nearest neighbor search algorithms to solve systems of nonlinear equations.**

Abstract: In this paper, we propose a method for solving a system of nonlinear equations by transformation it into a system of equations with a distorted right-hand side of a special form, nearest neighbor search algorithms being proposed to solve such a system.

Keywords: nearest neighbor search algorithm, systems of equations with distorted right-hand side, systems of nonlinear equations.