

ГЕНЕТИЧЕСКИЙ АЛГОРИТМ ФАКТОРИЗАЦИИ НАТУРАЛЬНЫХ ЧИСЕЛ С МІLP-ФУНКЦИЕЙ ПРИСПОСОБЛЕННОСТИ

Антонов Николай Андреевич

Аспирант 4 курса

Институт ВМиИТ (ВМК) КФУ, Казань, Россия

E-mail: nikoljaany@mail.ru

Научный руководитель — Ишмухаметов Шамиль Талгатович

Метаэвристики широко применяются в дискретной оптимизации и комбинаторике [1]. Одним из актуальных направлений этих исследований является факторизация натуральных чисел генетическими алгоритмами [2, 3]. Однако существующие методы ограничены отсутствием эффективной функции приспособленности, что снижает их применимость для чисел свыше 40-50 бит. В настоящем исследовании предложена новая функция, позволяющая факторизовать числа до 100 бит.

Функция приспособленности. Рассмотрим задачу факторизации полупростого числа $n = (n_0, \dots, n_{2k-1})$ длиной $2k$ бит на два простых множителя длиной k бит, используя генетический алгоритм. Популяция представлена бинарными векторами $a = (a_0, \dots, a_{k-1})$. Функция приспособленности формулируется как задача смешанно-целочисленного программирования (MILP):

$$\min \sum_{i=0}^{2k-1} (2k - i)(n_i(1 - y_i) + (1 - n_i)y_i),$$

при условиях:

$$q_0 = 0, \quad q_{2k-1} = y_{2k-1},$$

$$q_i + \sum_{j, i-j < k} a_j x_{i-j} = 2q_{i+1} + y_i, \quad i = 0, \dots, 2k - 2,$$

$$x = (x_0, \dots, x_{k-1}) \in \{0, 1\}^{2k}, y = (y_0, \dots, y_{2k-1}) \in [0, 1]^{2k}$$

$$q = (q_0, \dots, q_{2k-1}) \in \mathbb{Z}_+^{2k}$$

Модель вычисляет взвешенную сумму позиций, в которых двоичные представления произведения $y = ax$ и числа n не совпадают. Значение целевой функции используется в качестве функции приспособленности, оценивая точность разложения.

Предложенная MILP-модель была интегрирована в генетический алгоритм BRKGA (Biased Random Key Genetic Algorithm) [4] с локальным поиском. В Таблице 1 представлены результаты факторизации чисел длиной 20-100 бит.

Делитель (бит)	BRKGA&MILP		SOTA	
	% реш	Время (с)	% реш	Время (с)
10	100	0.1	100	0.05
20	100	5	100	0.13
30	90	5	0	0.24
40	60	5	0	0.4
50	20	5	0	0.61

Таблица 1: Сравнение методов по числу найденных решений и времени выполнения. **% реш** — процент чисел, для которых найден делитель. **Время (с)** — время вычисления функции приспособленности для одного элемента. **BRKGA&MILP/SOTA** — сравнение предложенного алгоритма с методами из [2, 3]. Выборка: 50 чисел. BRKGA: 200 элит, 700 потомков, 100 мутантов. Таймаут MILP – 5 с.

Литература

1. Rajwar, K., Deep, K., & Das, S. (2023). An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges. Artificial Intelligence Review, pp.1–71
2. E. Rutkowski and S. Houghten, "Cryptanalysis of RSA: Integer Prime Factorization Using Genetic Algorithms," 2020 IEEE Congress on Evolutionary Computation (CEC), Glasgow, UK, 2020, pp.1-8
3. A. V. Shoshina, G. I. Borzunov and E. Y. Ivanova, "Application of Bio-inspired Algorithms to the Cryptanalysis of Asymmetric Ciphers on the Basis of Composite Number," 2021 IEEE Conference, Moscow, Russia, 2021, pp. 2399-2403
4. Katoch, S., Chauhan, S.S. & Kumar, V. A review on genetic algorithm: past, present, and future. Multimed Tools Appl 80, 8091–8126 (2021)