От тритов к битам в солвере z3: ускорение трипликации сильных стартеров

О. С. Оганджанянц*, С. Ю. Садов‡

Для построения сильных стартеров в циклических группах $\mathbb{Z}_{3m}$ методом трипликации с использованием SAT/SMT солвера z3 ранее использовалась система условий с неизвестными из множества $\{0,1,2\}$. Эмуляция её системой с булевыми неизвестными привела к повышению производительности на несколько порядков.

Ключевые слова: сильный стартер, трипликация, солвер z3.

1. Сильные стартеры и метод трипликации

Сильный стартер в циклической группе $\mathbb{Z}_n$, $n = 2q+1$, — это разбиение множества $\{1,\dots,n-1\}$ на q пар $\{x_i, y_i\}$, такое, что все разности $\pm(x_i - y_i)$ по модулю n различны и не равны 0 и то же верно для сумм $x_i + y_i$. Например, $\{\{2,3\},\{4,6\},\{5,1\}\}$ — сильный стартер в $\mathbb{Z}_7$.

Приведем новую интерпретацию сильных стартеров как **расстановок неатакующих ферзей** на шахматной доске специального вида.

Горизонтали доски — окружности $C_j = \{|z| = \cos\frac{j\pi}{n}\}$ на комплексной плоскости ($j = 0,\dots,q$). Для $0 \le k \le n-1$, *вертикаль* V_k — диаметр окружности C_0, проходящий через корень из единицы $\omega^k = e^{2\pi ik/n}$, а *диагональ* D_k — окружность радиуса $1/2$, касающаяся C_0 внутренним образом в точке ω^k. Точка 0 исключается из V_k и D_k. Точки $Q_{k,\ell} = D_k \cap D_\ell$ ($k \ne \ell$) назовем *внутренними*, а $Q_{k,k} = \omega^k$ — *внешними полями* доски. Имеем $Q_{k,\ell} \in V_s \cap C_d$, где $d = \min\{|k-\ell|, n-|k-\ell|\}$, $2s \equiv k+\ell \pmod n$. *Ферзь* атакует поля на своей горизонтали, вертикали и диагоналях.

Предложение. *Разбиение $\{(x_j,y_j)\}_{j=1,\dots,q}$ множества $\{1,\dots,n-1\}$ является сильным стартером тогда и только тогда, когда ферзи, расположенные на полях Q_{x_j,y_j} и на $Q_{0,0}$, не атакуют друг друга* (рис. 1).

При этом, если внутренние ферзи имеют массу 2, а внешний — массу 1, то центр масс системы $q+1$ ферзей находится в центре доски.

* *Оганджанянц Олег Сергеевич* — Ph.D., ст. преподаватель, С.-Петербургский Педагогический ун-т им. А.И. Герцена, e-mail: oo4706@mun.ca, ORCID: 0000-0001-8476-9113.

Ogandzhanyants Oleg Sergeevich — Ph.D., Senior Lecturer, S.-Petersburg Herzen Pedagogical University.

‡ *Садов Сергей Юрьевич* — канд. физ.-мат. наук, частный преподаватель, г. Москва, e-mail: serge.sadov@gmail.com, ORCID: 0000-0002-9069-6894.

Sadov Sergey Yurievich — Candidate of Physical and Mathematical Sciences, Private tutor, Moscow.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

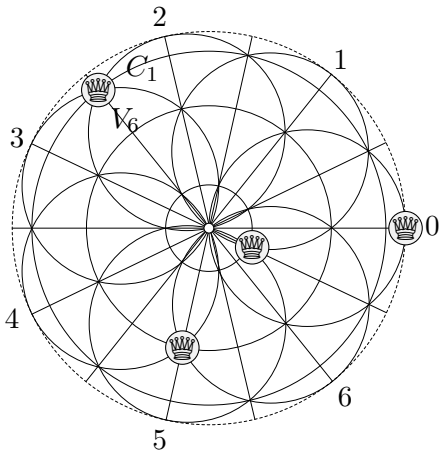


Рис. 1: Расстановка ферзей на полях $Q_{0,0}, Q_{2,3}, Q_{4,6}, Q_{5,1}$, соответствующая сильному стартеру $\{(2,3),(4,6),(5,1)\}$ в $\mathbb{Z}_7$

Эксперты уверены, что сильные стартеры существуют в $\mathbb{Z}_n$ при $n = 7$ и всех нечетных $n \geq 11$, но это доказано лишь для n, не кратных 3.

Метод трипликации для построения сильных стартеров в циклических группах порядка $3m$ предложен в [1] и развит в [2],[3]. В простейшем случае $m \not\vdots 3$ строятся две таблицы одинаковой структуры — Σ_m с элементами из $\mathbb{Z}_m$ и Σ_3 с элементами из $\mathbb{Z}_3$. По китайской теореме об остатках из них строится сильный стартер в $\mathbb{Z}_{3m}$ в форме таблицы Σ_{3m}.

Таблица Σ_m формируется из пар выбранного сильного стартера в $\mathbb{Z}_m$ с использованием параметра — ключа трипликации t. Пара в неполной строке имеет вид (t, t). Каждая полная строка содержит пару (x, y) исходного стартера и пары $(x + t, y + t)$ и $(t - y, t - x)$, см. Табл. 1.

Заполнение таблицы Σ_3 сводится к системе линейных неравенств по модулю 3. В примерах, рассмотренных в [1], эта задача, названная *модульным Судоку*, решалась вручную, а в [2],[3] использовался солвер z3 [4]. Условия модульного Судоку формулировались в терминах целочисленной арифметики. Здесь мы изучаем эффект перевода условий на булев язык.

Σ_7		
	4, 4	
2, 3	6, 0	1, 2
4, 6	1, 3	5, 0
5, 1	2, 5	3, 6

$+$

Σ_3		
	2, 0	
0, 2	1, 2	2, 2
1, 2	0, 0	2, 1
0, 1	1, 1	1, 0

$\Rightarrow$

Σ_{21}		
	11, 18	
9, 17	13, 14	8, 2
4, 20	15, 3	5, 7
12, 1	16, 19	10, 6

Таблица 1: Трипликация сильного стартера, как на рис. 1; ключ $t = 4$

2. Булева эмуляция троичной задачи и её эффект

Для перевода условий с неизвестными из области $T = \mathbb{Z}_3$ в систему с неизвестными из области $B = \{\texttt{True}, \texttt{False}\}$ использована кодировка: $0 \to 00$, $1 \to 01$, $2 \to 10$. Каждой неизвестной x из T ставим в соответствие две неизвестных x_1, x_2 из B, добавляя условие $\neg(x_1 \wedge x_2)$ (код 11 запрещен).

Все условия в формулировке задачи для z3 выражаются через арифметические операции $+, -\pmod 3$ и тернарный предикат `Distinct(x,y,z)`, то есть условие $\{x, y, z\} = \{0, 1, 2\}$. Приведем короткие выражения для эмулирующих операторов в функциональном базисе $\{\wedge, =\}$.

Операция	формула над T	формула над B
Сложение	$z = x + y \pmod 3$	$z_1 = (x_2 = y_2) \wedge ((x_1 = x_2) = y_1)$ $z_2 = (x_1 = y_1) \wedge ((y_1 = y_2) = x_2)$
Вычитание	$z = x - y \pmod 3$	$z_1 = (x_2 = y_1) \wedge ((x_1 = x_2) = y_2)$ $z_2 = (x_1 = y_2) \wedge ((x_1 = x_2) = y_1)$
Различие	$\{x, y, z\} = \{0, 1, 2\}$	$(x_1 = (y_1 = z_1)) \wedge (x_2 = (y_2 = z_2))$

Эмулирующие вставки непосредственно внедрены в опубликованную программу-трипликатор на Python [3, Appendix 3] без прочих изменений.

Результаты численного эксперимента

Использовался тот же компьютер, что и в работе [2]: fanless mini PC, процессор 11th Gen Intel(R) Core(TM) i7-1165G7 2.80GHz, 32 GB, ОС Windows 11, солвер z3py версии 5.3.3. Базовые стартеры трипликации предварительно сгенерированы методом hill-climbing with restarts.

Для базовых стартеров порядков $m \leq 599$ результаты показаны на рис. 2. Трипликация выполнялась при всех $(m-1)/2$ допустимых (см. [2]) значениях ключа t и вычислялось среднее время, как в [2, §8.4].

По сравнению с прежней версией время решения одного Судоку снизилось примерно в 10^2–10^4 раз. Например, $m = 19$: 1.4/0.07 сек; $m = 97$: 90/0.3 сек; $m = 251$: 2750/0.83 сек; $m = 499$: 17962/1.4 сек. Вычисления в [2] доведены до $m_{\max} = 499$; новая текущая граница: $m_{\max} = 8001$.

Отметим сильную зависимость времени решения от внешних по отношению к солверу факторов: загрузки процессора, ресурса памяти, авторегулировки тактовой частоты. Нерегулярность и немонотонность по порядку заметнее при больших порядках. Вот данные (порядок/время в сек.) для пяти испробованных порядков между 6000 и 7000 (ключ выбирался случайно): 6001/17170, 6201/2439, 6401/919, 6601/1244, 6801/672.

Вычисления в новой версии подтверждают тезис (не формализованный) [2, p. 332] о низкой асимптотической сложности задачи трипликации.

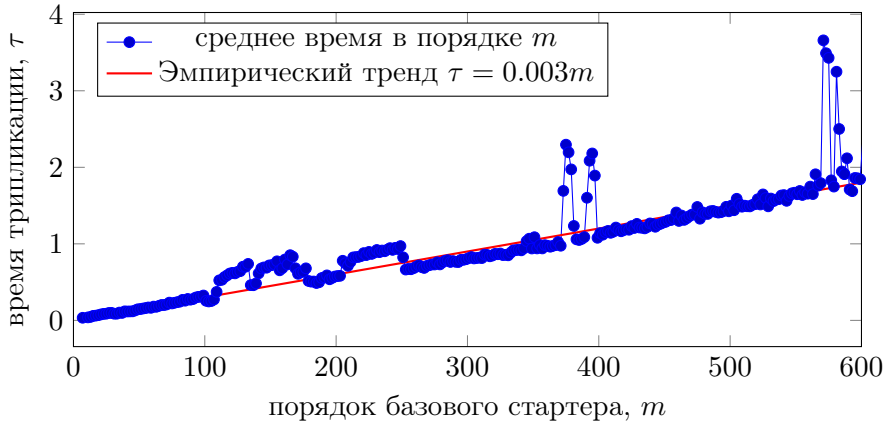


Рис. 2: Среднее время решения (сек.) для порядков $m < 600$

Список литературы

[1] O. Ogandzhanyants, *New constructions of strong and Skolem starters*, PhD thesis, Memorial University of Newfoundland, St. John's, 2025, 145 pp.

[2] O. Ogandzhanyants, S. Sadov, M. Kondratieva, "Constructing strong starters of orders $3p$: triplication with SAT solver", *J. Combin. Math. Combin. Comput.*, **126** (2025), 317–338. DOI: 10.61091/jcmcc126-23.

[3] O. Ogandzhanyants, S. Sadov, M. Kondratieva, "The triplication method for constructing strong starters", *J. Combin. Math. Combin. Comput.*, **131** (2026), 115–160. DOI: 10.61091/jcmcc131-08.

[4] Microsoft Corp., *z3 Official Guide*, https://microsoft.github.io/z3guide/docs.

Статья поступила 10 ноября 2026 г.

From trits to bits in z3 solver: a high-performance triplication of strong starters

O. S. Ogandzhanyants, S. Y. Sadov

The triplication method for constructing strong starters in cyclic groups $\mathbb{Z}_{3m}$ was earlier implemented with SAT/SMT solver z3 using constraints for unknowns with values in $\{0, 1, 2\}$. Emulation by Boolean constraints boosted performance by several orders of magnitude.

Keywords: strong starter, triplication, SAT solver z3.

Received on November 10, 2026