Таблица 1

n	5	6	7
Nl	12	26	56

Таблица 2

$\ell \setminus n$	5	6	7
2	2^{36}	2^{55}	2^{78}
4	–	2^{83}	2^{118}
6	–	–	2^{150}
$\geqslant 0$	2^{145}	2^{364}	2^{868}

Известно, что для нечётных n оценка Сидельникова точна на классе AB-функций, причём AB-функции существуют при всех нечётных n. Из табл. 2 видно, что оценка, полученная в теореме 2, применима только к значениям нелинейности, далёким от максимальных. Однако доказательство теоремы 2 конструктивно и может оказаться полезным, поскольку описывает метод построения функций с фиксированной нелинейностью.

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
2. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.
3. *Carlet C.* Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engeneering / eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Ch. 8. P. 257–397. `www.math.univ-paris13.fr/~carlet/`
4. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.

УДК 510.53

ПРОБЛЕМА ДОСТИЖИМОСТИ В НЕПРЕРЫВНЫХ КУСОЧНО-АФФИННЫХ ОТОБРАЖЕНИЯХ ОКРУЖНОСТИ СТЕПЕНИ 2

А. Н. Курганский

На примере непрерывных кусочно-аффинных отображений окружности в себя степени два, для которых в работе доказывается алгоритмическая разрешимость проблемы достижимости из точки точки, обсуждаются некоторые алгоритмические аспекты моделирования дискретных систем непрерывными в контексте криптографического преобразования информации. Все такие кусочно-аффинные отображения топологически сопряжены с хаотическим отображением $E_2(x) = 2x \pmod 1 : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$. Из доказательства основного результата работы следует, что любое другое непрерывное кусочно-аффинное отображение с рациональными коэффициентами и сопряжённое с E_2 показывает хаотическое поведение для некоторых рациональных чисел, что делает их интересными в задачах криптографического преобразования информации.

Ключевые слова: *хаотические системы, криптография, кусочно-аффинные отображения, проблема достижимости.*

Непрерывные хаотические динамические системы привлекают к себе внимание со стороны теории алгоритмов и дискретной математики благодаря полезным аналогиям между их наблюдаемыми свойствами и свойствами, предъявляемым к криптографическим преобразователям информации [1]. В ряде публикаций встречаются исследования непрерывных хаотических систем в качестве прототипов для конечно-автоматных криптографических преобразователей информации [2]. В связи с этим, а также в силу принципиального противопоставления языка непрерывной и дискретной (компьютерной) математики является фундаментальной проблема развития интуитивных аналогий между хаотическими и криптографическими системами до уровня математических взаимосвязей. Отсюда возникает интерес к непрерывным системам с дискретным или непрерывным временем как к моделям вычислений. Это в первую очередь связано с вопросом: можно ли с помощью рассматриваемой непрерывной динамической системы моделировать дискретные системы, в частности универсальную машину Тьюринга? Проблема доказательства вычислительной универсальности тесно связана с проблемой достижимости. Обратим внимание на следующий важный момент при изучении хаотических систем в контексте моделирования с их помощью универсальных вычислений. В [3] приведено следующее замечание: поскольку реальную хаотическую систему физически невозможно установить с бесконечной точностью в заданное состояние, в частности в рациональную точку, то для таких систем идея брать в качестве основы для определения или доказательства вычислительной универсальности проблему достижимости из точки точки ("point-to-point reachability") имеет недостатки в силу чувствительности системы к начальным условиям, из-за которой любые возмущения могут разрушить вычисления. Однако в проблеме моделирования хаотическими системами универсальных вычислений в контексте криптографических задач речь идёт не о реальном физическом моделировании, а о компьютерном моделировании математических нелинейных моделей, и бесконечная точность начальных условий в виде рациональных чисел вполне имеет смысл. В качестве примера можно привести системы, аналогичные кусочно-аффинным, в которых вместе с аффинными отображениями используются функции $\sqrt[3]{x}$, $\sqrt{x}$, x^2, x^3. Для таких кусочно-элементарных отображений было выделено [4] подмножество рациональных точек, орбиты которых остаются рациональными, благодаря чему доказана их вычислительная универсальность.

Будем рассматривать непрерывные кусочно-аффинные отображения $f : S^1 \to S^1$ степени 2 окружности $S^1 = \mathbb{R}/\mathbb{Z}$. Все такие отображения топологически сопряжены с $y = E_2(x) = 2x \pmod 1$ и являются частными случаями кусочно-аффинных отображений с двумя интервалами. Для них доказывается алгоритмическая разрешимость проблемы достижимости, и, следовательно, такие системы не являются вычислительно универсальными. Утверждение практически тривиальное, но тем не менее важное по следующим причинам. Во-первых, проблема достижимости в кусочно-аффинных отображениях с двумя интервалами в общем случае является открытой проблемой [5]. Во-вторых, отображение E_2 является классическим примером хаотической системы, в которой для почти всех точек $x \in S^1$ их орбиты демонстрируют хаотическое поведение. Однако ни одна точка из этих «почти всех» не представима на компьютере, поскольку они являются иррациональными числами, и наоборот, для всех известных в программировании типов данных система E_2 ведёт себя регулярно. Математическая теорема о хаотичности системы E_2 с точки зрения дискретной (компьютерной) ма-

тематики является бессодержательной. И даже если под числом понимать алгоритм, потенциально его порождающий, то теорема о хаотичности E_2 должна принять вид, раскрывающий тот факт, что сложность поведения системы заключается или скрыта не в самом отображении, а в сложности начальной точки x. Вместе с тем, как следует из доказательства ниже, любое другое топологически сопряжённое с E_2 кусочно-аффинное отображение с рациональными коэффициентами показывает хаотическое поведение не только орбит иррациональных чисел, но и некоторого подмножества рациональных чисел. Рациональные числа представимы на компьютере, поэтому такие отображения уже интересны в контексте криптографического преобразования информации.

Пусть $X = \mathbb{R}/\mathbb{Z} \cap \mathbb{Q}$, $f : X \to X$ — непрерывное кусочно-аффинное отображение степени 2, т. е. такое, что $X = X_1 \cup X_2$, $X_1 = \left[0, \frac{m}{n}\right]$ и $X_2 = \left[\frac{m}{n}, 1\right]$, $f(x) = \frac{n}{m}x$ при $x \in X_1$, $f(x) = \frac{n}{n-m}\left(x - \frac{m}{n}\right)$ при $x \in X_2$, $m, n \in \mathbb{N}$. Обозначим через $O(x) = \{f^n(x) : n \in \mathbb{N}\}$ орбиту точки x. Проблема достижимости из точки точки звучит так: существует ли алгоритм, определяющий по произвольным точкам $x_0, x_1 \in X$ принадлежность $x_1 \in O(x_0)$.

Теорема 1. Проблема достижимости в непрерывных кусочно-аффинных отображениях f окружности в себя степени 2 алгоритмически разрешима.

Доказательство. Числа m, n, $n - m$ взаимно простые. Через $|x|_p$ обозначим p-адическую норму x. Если простое $s \in \mathbb{P}$ не делит m и $n-m$, то $|f(x)|_s \leqslant \max\{|x|_s, 0\}$. Если $p \in \mathbb{P}$ делит m, а $q \in \mathbb{P}$ делит $n - m$, то $\left|\frac{n}{m}x\right|_p > |x|_p$, $\left|\frac{n}{m}x\right|_q = |x|_q$. Пусть $|x|_p > \left|\frac{m}{n}\right|_p$ и $|x|_q > \left|\frac{m}{n}\right|_q$, тогда $\left|\frac{n}{n-m}(x - \frac{m}{n})\right|_q > |x|_q$, $\left|\frac{n}{n-m}(x - \frac{m}{n})\right|_p = |x|_p$ и, следовательно, $|f^{i+1}(x)|_p + |f^{i+1}(x)|_q > |f^i(x)|_p + |f^i(x)|_q$, т. е. для проверки $y \in O(x)$ достаточно вычислить начальный отрезок орбиты длины i, такой, что $|f^i(x)|_p + |f^i(x)|_q > |y|_p + |y|_q$.

Пусть условие $\left(|x|_p > \left|\frac{m}{n}\right|_p \text{ и } |x|_q > \left|\frac{m}{n}\right|_q\right)$ не выполняется. Если $|f^i(x)|_p \leqslant |y|_p$, $|f^i(x)|_q \leqslant |y|_q$ для всех i, то последовательность $O(x)$ зацикленная, причём с вычислимого места, поскольку существует лишь конечное множество чисел $0 \leqslant x \leqslant 1$, таких, что $|x|_s \leqslant \max\{0, |y|_r : r \in \mathbb{P}\}$, $s \in \mathbb{P}$. ■

Следствие 1. Если $|x|_p > \left|\frac{m}{n}\right|_p$ и $|x|_q > \left|\frac{m}{n}\right|_q$, то $O(x)$ не зацикливается и рациональное x ведет себя в f как некоторое действительное число в E_2.

ЛИТЕРАТУРА

1. *Птицын Н. В.* Приложение теории детерминированного хаоса в криптографии. М.: Изд-во МГТУ им. Н. Э. Баумана, 2002. 80 с.
2. *Savchenko A. Ya., Kovalev A. M., Kozlovskii V. A., and Scherbak V. F.* Inverse dynamical systems in secure communication and its discrete analogs for information transfer // Proc. NDES. 2003. P. 112–116.
3. *Delvenne J.-C.* What is a universal computing machine? // Appl. Math. Comput. 2009. V. 215. No. 4. P. 1368–1374.
4. *Kurganskyy O., Potapov I., and Sancho-Caparrini F.* Reachability problems in low-dimensional iterative maps // Int. J. Found. Comput. Sci. 2008. No. 19(4). P. 935–951.
5. *Asarin E., Mysore V., Pnueli A., and Schneider G.* Low dimensional hybrid systems — decidable, undecidable, don't know // Inform. Comput. 2012. V. 211. P. 138–159.