Отметим, что не для всех квадратичных функций существует хотя бы одно аффинное подпространство размерности больше чем $\lceil n/2 \rceil$, на котором функция аффинна. Например, если f является бент-функцией (n чётно), то не существует подпространств размерности $n/2+1$, на которых f аффинна. Бент-функция — это булева функция от чётного числа переменных, максимально удаленная от множества всех аффинных функций. Понятие бент-функций ввел О. Ротхаус [1]. Бент-функции представляют интерес в криптографии и теории кодирования, поскольку имеют в этих областях множество различных приложений. Тем не менее до сих пор существует большое количество нерешённых проблем, связанных с бент-функциями [2].

Внесём ограничение на размерность подпространств в условие утверждения 1.

Утверждение 2. Пусть f — квадратичная булева функция от n переменных. Тогда для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ функция f аффинна на L, если и только если f аффинна на любом сдвиге L.

Если f является бент-функцией, то по подпространствам размерности $n/2$, на которых она аффинна, можно строить другие бент-функции.

Утверждение 3 [3]. Пусть f — бент-функция от $2k$ переменных и $L \subseteq \mathbb{Z}_2^{2k}$, $|L| = 2^k$. Тогда $f(x) \oplus Ind_L(x)$ является бент-функцией тогда и только тогда, когда L является аффинным подпространством и f на нём аффинна.

Таким образом, существует взаимно однозначное соответствие между бент-функциями на расстоянии 2^k от f и аффинными подпространствами, на которых f аффинна.

Следующая теорема показывает, для каких функций, помимо квадратичных, справедливо утверждение 2.

Теорема 1. Пусть f — булева функция от n переменных и для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ функция f аффинна на L, если и только если f аффинна на любом сдвиге L. Тогда либо $\deg f \leqslant 2$, либо не существует ни одного аффинного подпространства размерности $\lceil n/2 \rceil$, на котором функция f аффинна.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken: LAP LAMBERT Academic Publishing, 2011.
3. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.

УДК 510.53

ОБ АЛГОРИТМИЧЕСКИХ И ТОПОЛОГИЧЕСКИХ СВОЙСТВАХ ОРБИТ КУСОЧНО-АФФИННЫХ ОТОБРАЖЕНИЙ

А. Н. Курганский

Рассматривается открытая проблема достижимости в одномерных кусочно-аффинных отображениях с двумя интервалами. Найдены частные случаи алгоритмической разрешимости рассматриваемой проблемы, сформулированные на языке топологических свойств орбит в таких системах.

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

При исследовании непрерывных динамических систем наряду с методами теории динамического хаоса, определяющими, например, такие свойства, как эргодичность, перемешивание, топологическая транзитивность и устойчивость, применение методов теории алгоритмов представляется также интересным и, главное, естественным и полезным с точки зрения приложения теории детерминированного хаоса в задачах криптографической защиты информации. Параллели между хаотическими и криптографическими системами мотивируют исследования в области применения дискретных аналогов непрерывных хаотических систем в задачах криптографического преобразования информации [1]. Однако математические связи относящихся к делу свойств дискретных систем и их непрерывных прототипов скорее находятся на уровне взаимосвязи узелков на память и запоминаемых фактов. В связи с этим на стыке теории динамических систем и теории алгоритмов представляет интерес фундаментальная проблема вычислительной универсальности непрерывных динамических систем и тесно с ней связанная проблема достижимости. Динамическая система является вычислительно универсальной, если существует интерпретация поведения системы, при которой моделируется машина Тьюринга. Проблему достижимости можно сформулировать так: существует ли для данной системы алгоритм, определяющий по данным точкам или областям фазового пространства, проходит ли через них одна и та же фазовая кривая.

Непрерывные хаотические динамические системы показывают сложное поведение, позволяющее предполагать для некоторых из них алгоритмическую неразрешимость проблемы достижимости из точки точки. До сих пор единственным способом доказательства алгоритмической неразрешимости является моделирование с помощью изучаемой системы универсальной машины Тьюринга. Публикации показывают в какой-то мере безуспешный поиск таких доказательств для различных непрерывных динамических систем. В связи с этим представляет интерес исследование вычислительной универсальности гибридных дискретно-непрерывных систем и систем с дискретным временем. Примеры таких исследований можно найти в [2]. На практике оказывается, что чем выше размерность фазового пространства, тем проще доказать универсальность системы. Поэтому представляют интерес системы низкой размерности. Например, в [3] для одномерных кусочно-элементарных отображений в базисе функций $\{x^2, x^3, x^{1/2}, x^{1/3}, 2x, x+1, x-1\}$, а также дробно-рациональных функций доказана алгоритмическая неразрешимость достижимости из точки точки. При этом уже долгое время остается открытой проблема достижимости в одномерных кусочно-аффинных отображениях [3] даже в простейшем случае двух интервалов. Настоящая работа посвящена кусочно-аффинным отображениям с двумя интервалами (2-PAM'ам).

Не ясно, влечёт ли сопряжённость двух систем их эквивалентность с точки зрения проблемы достижимости. Во всяком случае, ответ на этот вопрос не очевиден. Поэтому, имея в виду как гипотезу алгоритмическую разрешимость проблемы достижимости в 2-PAM, имеет смысл находить связи топологических и алгоритмических свойств орбит и проводить соответствующую классификацию систем. Например, если для динамической системы доказано свойство перемешивания или эргодичности, то проблема достижимости измеримой области (ненулевой меры) фазового пространства становится, очевидно, тривиальной. Пример менее тривиального утверждения приведён ниже.

Пусть X — отрезок $[0,1]$ с отождествленными концами, т. е. $X = \mathbb{R}/\mathbb{Z}$, и отображение $f : X \to X$ таково, что $X = X_1 \cup X_2$ — разбиение на непересекающиеся интервалы и $f(x) = a_i x + b_i$, если $x \in X_i$; $a_i, b_i \in \mathbb{Q}$, $i = 1, 2$. Обозначим через $f^*(x) = \{f^n(x) : n \in \mathbb{N}\}$ орбиту точки x. Проблема достижимости из точки точ-

ки звучит так: существует ли алгоритм, определяющий по произвольным точкам $x_0, x_1 \in X$ принадлежность $x_1 \in f^*(x_0)$. Ограничимся рассмотрением только рациональных точек X по следующим соображениям. Кусочно-аффинное отображение $f(x) = 2x \pmod 1$ является хаотическим для почти всех $x \in X$. Но ни одно число этого множества почти всех из X не представимо на компьютере, если под числом не понимать алгоритм, его порождающий. Если же под числом понимать произвольный порождающий его алгоритм, проблема достижимости для $f(x)$ оказывается тривиально алгоритмически неразрешимой в общем случае, несмотря на то, что отображение очень простое. Стоит при этом заметить, что некоторые сопряжённые $f(x)$ отображения показывают хаотическое поведение на множестве рациональных точек.

Теорема 1. Если f строго эргодическое, т. е. имеет единственную инвариантную меру, или, другими словами, плотности распределения орбит всех точек совпадают, то проблема достижимости алгоритмически разрешима.

Следствие 1. Если пространство инвариантных мер конечномерно, то проблема достижимости алгоритмически разрешима.

ЛИТЕРАТУРА

1. *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, May 18–22, Scuol/Schuls, Switzerland. P. 112–116.
2. *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.
3. *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.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ ПРОИЗВОЛЬНОЙ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ

О. Л. Мироненко

Доказаны достаточные условия статистической независимости суперпозиции произвольного числа булевых функций от подмножества своих аргументов.

Ключевые слова: *суперпозиция булевых функций, статистическая независимость от подмножества аргументов.*

Определение 1. Для любой булевой функции $f(x)$, где x — переменные со значениями в $\mathbb{Z}_2^n$, и для любого подмножества U её аргументов будем говорить, что $f(x)$ статистически не зависит от переменных множества U, если для любой её подфункции $f'(x')$, полученной фиксированием значений всех переменный в U, имеет место равенство $\Pr[f'(x') = 0] = \Pr[f(x) = 0]$.

В [1] доказано, что если булева функция $f_1(x)$ статистически не зависит от некоторого подмножества своих аргументов, то это свойство сохраняется для произвольной суперпозиции $g(f_1(x), y)$. Для суперпозиции $g(f_1(x), f_2(x), y)$ в [2] доказано более сложное достаточное условие сохранения статистической независимости: этим свойством, помимо f_1 и f_2, должна обладать и их сумма $f_1 \oplus f_2$. В данной работе условие из [2] обобщается на случай произвольного числа внутренних функций суперпозиции.