электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0420900025. ISSN 1994-0408

Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов

№ 08, август 2010 г.

Автор: Б. М. Сухинин

УДК 519.713.4

МГТУ им. Н. Э. Баумана, Россия, г. Москва

E-mail: b.sukhinin@gmail.com

1. Основные определения

Рассмотрим множество $M = \{m_0, m_1, \ldots, m_{X-1}\}$, состоящее из X двоичных ячеек памяти. Каждая ячейка характеризуется ее индексом — натуральным числом $x \in [0; X-1]$ — и способна хранить значение из множества $\{0; 1\}$.

Сопоставим каждой ячейке $m_x \in M$ упорядоченный набор

$$\Psi(m_x) = [m_{x_1}, m_{x_2}, \ldots, m_{x_k}], \quad m_{x_i} \in M,$$

где мощность (или длина) набора — число k — не зависит от выбора ячейки m_x, а элементы m_{x_i} выбираются из M произвольным образом для каждой ячейки m_x. Полученный набор $\Psi(m_x)$ назовем *окрестностью ячейки* m_x; кроме того, под окрестностью Ψ (без указания конкретной ячейки) будем подразумевать правило, по которому каждой ячейке $m_x \in M$ сопоставляется ее окрестность $\Psi(m_x)$. Отметим, что такое правило может быть задано в произвольной форме (например, таблицей).

Обозначим через $m_x^{(t)}$ значение ячейки x в момент времени t, а через $\Psi^{(t)}(m_x)$ — набор, составленный из значений ячеек, входящих в окрестность m_x, в момент времени t:

$$\Psi^{(t)}(m_x) = \left[m_{x_1}^{(t)}, m_{x_2}^{(t)}, \ldots, m_{x_k}^{(t)}\right].$$

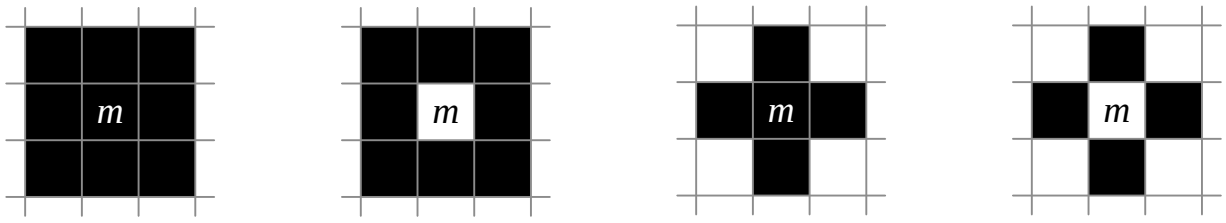
Тогда *неоднородным двоичным клеточным автоматом* размера X с окрестностью Ψ и функцией переходов f будем называть автономный конечный автомат, состояние которого в каждый момент времени определяется текущими значениями ячеек из набора M ($|M| = X$). Время такого автомата изменяется дискретными шагами, а смена значений всех ячеек происходит синхронно в момент увеличения номера такта в соответствии с зависимостью

$$m_x^{(t+1)} = f\left(\Psi^{(t)}(m_x)\right),$$

где f является булевой функцией от k переменных (k — мощность окрестности) и не зависит от выбора ячейки.

Классические двоичные клеточные автоматы [1,2] являются частным случаем неоднородных, и все сказанное выше для них также справедливо. Мы рассматриваем только двумерные классические клеточные автоматы, в которых множество M представляется в виде геометрически упорядоченного набора: ячейки памяти располагаются в узлах двумерной решетки размера $X \times Y$. Очевидно, что каждая ячейка в таком случае характеризуется вектором своих координат (x, y), а мощность множества M составляет $|M| = X \cdot Y$.

В окрестность каждой ячейки памяти входят только ячейки, непосредственно смежные с данной и, возможно, она сама. В зависимости от мощности и состава мы выделяем *полные*, *квазиполные* и *неполные* окрестности (см. рис. 1). Отметим, что полные окрестности также называются окрестностями Мура, а неполные мощности 4 — окрестностями фон Неймана.



(а) (б) (в) (г)

Рис. 1. Типы окрестности двумерных классических клеточных автоматов: (а) — полная окрестность, (б) — квазиполная окрестность, (в) — неполная окрестность (мощность 5), (г) — неполная окрестность (мощность 4).

Все ячейки памяти классического клеточного автомата являются неразличимыми по своим свойствам, т. е. для них используется один и тот же тип окрестности. Для реше-

ния проблемы граничных клеток противоположные края решетки отождествляются, что эквивалентно выполнению всех действий над координатами ячеек по модулю соответствующего линейного размера решетки.

Принимая во внимание геометрическую интерпретацию множества M можно ввести понятие расстояния $\delta(m_{x_1,y_1}, m_{x_2,y_2})$ между ячейками m_{x_1,y_1} и m_{x_2,y_2} классического клеточного автомата как максимальную по абсолютной величине разницу между соответствующими координатами с учетом отождествления краев решетки:

$$\delta(m_{x_1,y_1},m_{x_2,y_2}) = \max\big(\min\left(|x_1 - x_2|, X - |x_1 - x_2|\right), \\ \min\left(|y_1 - y_2|, Y - |y_1 - y_2|\right)\big).$$

Максимально возможное расстояние между двумя произвольными ячейками m_{x_1,y_1} и m_{x_2,y_2} в таком случае равно

$$\delta_{max} = \max_{\substack{m_{x_1,y_1}\in M \\ m_{x_2,y_2}\in M}} \delta(m_{x_1,y_1}, m_{x_2,y_2}) = \max\left(\left\lceil\frac{X-1}{2}\right\rceil, \left\lceil\frac{Y-1}{2}\right\rceil\right).$$

2. Постановка задачи

Понятие *лавинного эффекта* было введено Х. Фейстелем [3] и обычно применяется в криптографии для анализа блочных шифров и хеш-функций. «Хорошим» считается [4] такой лавинный эффект, при котором малые изменения входных данных ведут к значительным изменениям выходных.

Более формально, преобразование $\varphi : \{0;1\}^n \to \{0;1\}^n$ удовлетворяет критерию лавинного эффекта, если для всех $i \in \{1, 2, \ldots, n\}$

$$\frac{1}{2^n}\sum_{\boldsymbol{a}\in\{0;1\}^n} \big\|\varphi(\boldsymbol{a}) \oplus \varphi(\boldsymbol{a} \oplus \boldsymbol{e}_i)\big\| = \frac{n}{2},$$

где $\boldsymbol{e}_i \in \{0;1\}^n$ — единичный вектор, все компоненты которого, за исключением i-го, равны нулю, $\|\boldsymbol{x}\|$ — вес вектора $\boldsymbol{x}$, т. е. количество его ненулевых компонентов, а символ $\oplus$ здесь и далее обозначает операцию сложения по модулю 2.

Мы рассматриваем клеточный автомат как блочный преобразователь информации (см. рис. 2), состоящий из множества ячеек памяти M и функции $F : \{0;1\}^{|M|} \to \{0;1\}^{|M|}$, заключающейся в вычислении $f\left(\Psi(m)\right)$ для всех ячеек $m \in M$ клеточного автомата (фак-

тически функция F является S-блоком большой размерности, итеративно применяемым к входным данным). Мультиплексор mux позволяет записывать в ячейки памяти либо данные со входа клеточного автомата, либо значение функции F.

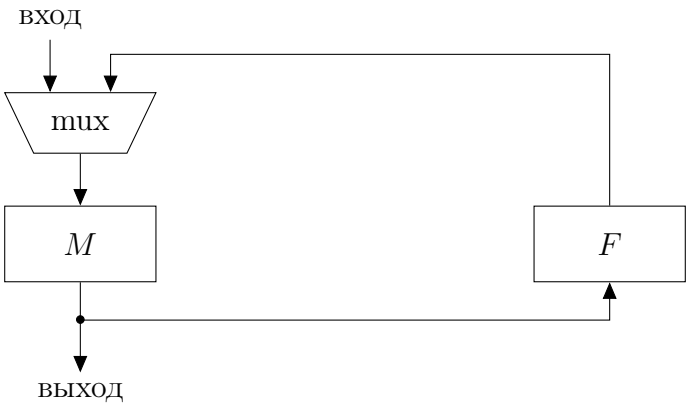


Рис. 2. Модель клеточного автомата как блочного преобразователя информации.

В работе ставится задача оценить лавинный эффект в классических и неоднородных клеточных автоматах в зависимости от выбора преобразования F, а точнее — от выбора типа (для классических) или мощности (для неоднородных клеточных автоматов) окрестности при условии использования равновесных функций перехода f.

С целью количественного описания лавинного эффекта вводятся две его числовые характеристики: *интегральная* и *пространственная*. Интегральная характеристика $\eta(t)$ отражает временну́ю зависимость отношения числа изменившихся ячеек к размеру (т. е. общему количеству ячеек) клеточного автомата. Пространственная характеристика $\mu(t)$ рассматривается только для классических клеточных автоматов и отражает линейную скорость, с которой изменения распространяются по решетке клеточного автомата.

Также мы определяем понятие *оптимальˊного лавинного эффекта* как лавинный эффект, при котором изменения распространяются с максимально возможной скоростью, и при этом изменяется значение в среднем половины ячеек.

3. Лавинный эффект в классических клеточных автоматах

Рассмотрим два идентичных двоичных двумерных классических клеточных автомата, т. е. автоматы с одинаковыми размерами решетки $X \times Y$ (для определенности будем считать, что $X \geqslant Y$), функциями перехода f и окрестностями Ψ. Обозначим через $m_{x,y}^{(t)}$

значение ячейки первого клеточного автомата с координатами (x, y) в момент времени t; для аналогичной ячейки второго клеточного автомата будем использовать обозначение $\widehat{m}_{x,y}^{(t)}$.

Пусть в начальный момент времени $t = 0$ совпадают значения всех ячеек первого и второго клеточных автоматов с соответствующими координатами, кроме нулевой:

$$m_{x,y}^{(0)} \neq \widehat{m}_{x,y}^{(0)} \Leftrightarrow (x,y) = (0,0)$$

(отметим, что, поскольку все ячейки классического клеточного автомата неразличимы по своим свойствам, выбор конкретной ячейки не имеет значения).

Тогда интегральная характеристика лавинного эффекта описывается выражением

$$\eta(t) = \frac{1}{XY} \sum_{(x,y)} \left(m_{x,y}^{(t)} \oplus \widehat{m}_{x,y}^{(t)} \right),$$

где сумма берется по всем координатным векторам (x,y). Если лавинный эффект является оптимальным, интегральная характеристика имеет вид

$$\eta_{opt}(t) = \begin{cases} (2t+1)^2/(2 \cdot X \cdot Y), & 2t+1 \leqslant Y, \\ (2t+1)/(2 \cdot X), & Y < 2t+1 \leqslant X, \\ 1/2, & X < 2t+1. \end{cases}$$

Пространственная характеристика лавинного эффекта равна отношению максимального расстояния, на котором проявились изменения, к максимально возможному расстоянию между ячейками:

$$\mu(t) = \frac{\max\limits_{(x,y)} \left\{ \left(m_{x,y}^{(t)} \oplus \widehat{m}_{x,y}^{(t)} \right) \cdot \delta \left(m_{0,0}, m_{x,y} \right) \right\}}{\lceil (X-1)/2 \rceil}.$$

Пространственная характеристика оптимального лавинного эффекта имеет вид

$$\mu_{opt}(t) = \begin{cases} \dfrac{t}{\lceil (X-1)/2 \rceil}, & t \leqslant \lceil (X-1)/2 \rceil, \\ 1, & t > \lceil (X-1)/2 \rceil. \end{cases}$$

На рис. 3 и 4 приведены графики интегральных и пространственных характеристик лавинного эффекта в двумерных классических клеточных автоматах для различных

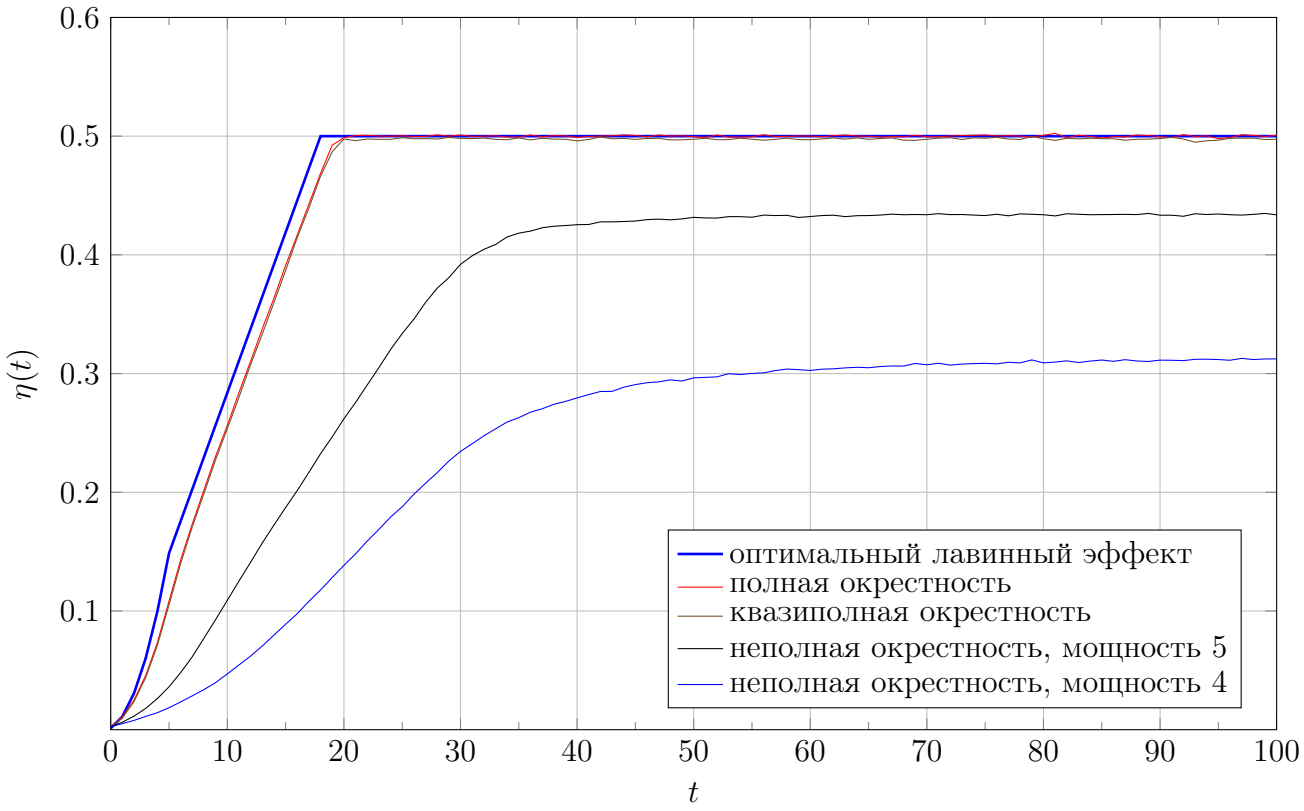


Рис. 3. Интегральные характеристики лавинного эффекта в классических двумерных клеточных автоматах.

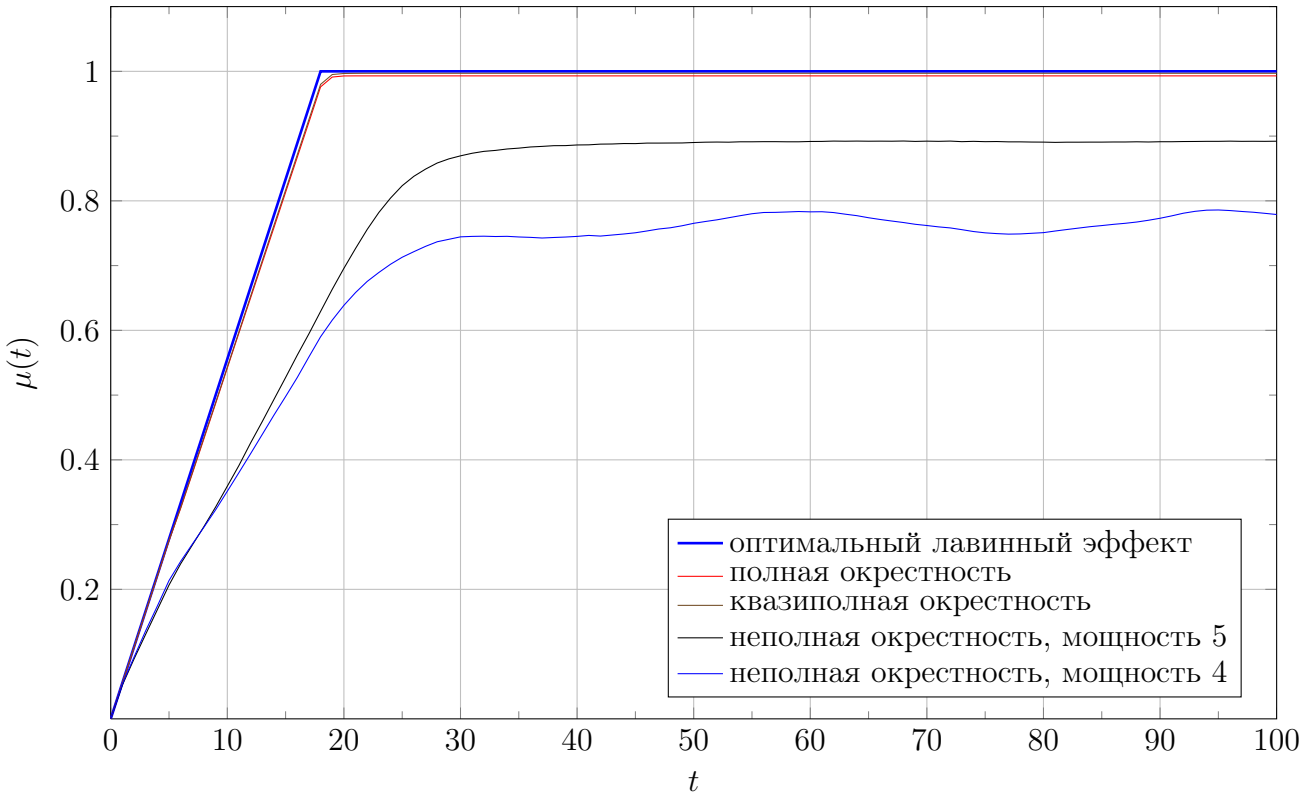


Рис. 4. Пространственные характеристики лавинного эффекта в классических двумерных клеточных автоматах.

вариантов выбора окрестности (см. рис. 1). Каждый график (за исключением графика оптимального лавинного эффекта) отражает усредненные показатели, полученные в результате проведения численных экспериментов с 1 000 различных клеточных автоматов. Размер автоматов составлял 37×11 ячеек, а равновесная функция переходов и начальные значения ячеек выбирались случайным равновероятным образом в каждом эксперименте.

На графиках хорошо видно, что характеристики быстро приближаются к некоторому установившемуся значению, причем для полных и квазиполных типов окрестности лавинный эффект практически совпадает с оптимальным. Следует отметить, что с уменьшением мощности окрестности возрастает вероятность отсутствия лавинного эффекта при определенном сочетании начальных значений ячеек и выбранной функции переходов. Этим объясняются наблюдаемые различия между характеристиками оптимального лавинного эффекта и лавинного эффекта в клеточных автоматах с неполными окрестностями.

4. Лавинный эффект в неоднородных клеточных автоматах

Для описания лавинного эффекта в неоднородных клеточных автоматах мы будем действовать по той же схеме, что и в классическом случае. При этом, поскольку в неоднородных клеточных автоматах отсутствует упорядоченная структура ячеек, мы не вводим для них определение расстояния и используем для описания лавинного эффекта единственную характеристику — интегральную.

Рассмотрим два двоичных неоднородных клеточных автомата размера X с одинаковыми функциями переходов f и окрестностями Ψ. Через $m_x^{(t)}$ и $\widehat{m}_x^{(t)}$ обозначим значения ячеек с индексом x в момент времени t первого и второго автоматов соответственно. Пусть в начальный момент времени для обоих клеточных автоматов совпадают значения всех ячеек с соответствующими индексами, за исключением ячеек с индексом ноль:

$$m_x^{(0)} \neq \widehat{m}_x^{(0)} \Leftrightarrow x = 0.$$

Интегральная характеристика $\eta(t)$ лавинного эффекта в неоднородных клеточных

автоматах описывается соотношением

$$\eta(t) = \frac{1}{X} \sum_{0 \leqslant x < X} \left(m_x^{(t)} \oplus \widehat{m}_x^{(t)} \right).$$

Поскольку лавинный эффект в неоднородных клеточных автоматах существенно зависит от структуры связей между ячейками (т. е. от выбора окрестности для каждой ячейки), для оптимального лавинного эффекта была получена только верхняя оценка:

$$\eta_{opt}(t) \leqslant \begin{cases} \dfrac{1}{2X} \sum\limits_{i=0}^{t} k^i, & \sum\limits_{i=0}^{t} k^i \leqslant X, \\ \dfrac{1}{2}, & \sum\limits_{i=0}^{t} k^i > X, \end{cases}$$

где k — мощность окрестности. Следует отметить, что, в отличие от оптимального лавинного эффекта в классических клеточных автоматах, описываемого полиномиальным по t соотношением, в неоднородных клеточных автоматах зависимость носит экспоненциальный характер.

Графики интегральных характеристик лавинного эффекта приведены на рис. 5. Как и ранее, каждый график отражает усредненные показатели по 1 000 клеточных автоматов. Размер автоматов составлял 257 ячеек, а равновесные функции переходов, начальные значения ячеек и окрестности каждой ячейки выбирались случайным равновероятным образом для каждого эксперимента. Мы не приводим графики для оптимального лавинного эффекта, поскольку в неоднородных клеточных автоматах интегральная характеристика зависит от выбранной мощности окрестности.

Как и в классическом случае, каждому значению мощности окрестности соответствует установившееся значение характеристики; при этом ни один из приведенных графиков не достигает оптимального уровня $\eta(t) = 1/2$. Тем не менее, сравнение характеристик показывает, что при равномощных окрестностях лавинный эффект в неоднородных клеточных автоматах проявляется лучше. Кроме того, в неоднородных клеточных автоматах лавинный эффект нарастает значительно более резко, что согласуется с экспоненциальным характером зависимости, отмеченным выше.

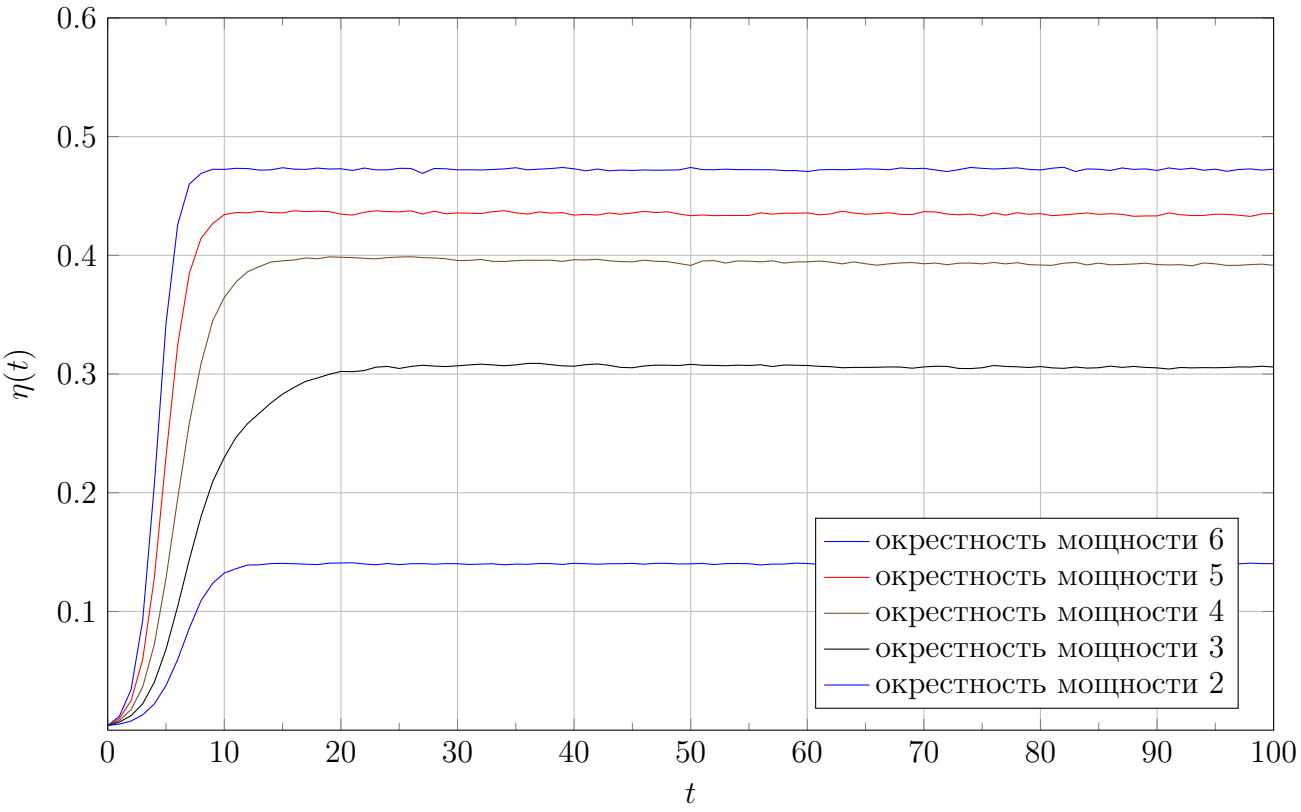


Рис. 5. Интегральные характеристики лавинного эффекта в неоднородных клеточных автоматах.

Заключение

Итак, мы рассмотрели лавинный эффект в клеточных автоматах. Для его количественного описания были введены две числовые характеристики — пространственная и интегральная, отражающие различные аспекты проявления лавинного эффекта.

Проведенные исследования показали, что лавинный эффект существенно зависит от выбора окрестностей ячеек клеточных автоматов, причем с увеличением мощности окрестности характеристики лавинного эффекта приближаются к оптимальным.

Сравнивая лавинный эффект в классических и неоднородных клеточных автоматах можно отметить, что в неоднородных клеточных автоматах он проявляется более сильно при тех же значениях мощности окрестности, т. е. такие автоматы потенциально обладают лучшими свойствами.

Полученные результаты могут использоваться для выбора параметров клеточных автоматов при построении на их основе алгоритмов блочного преобразования информации, таких как блочные шифры, хеш-функции или генераторы псевдослучайных последовательностей.

Автор благодарит Жукова Алексея Евгеньевича за внимание к настоящей работе.

Список литературы

1. Farmer D., Toffoli T., Wolfram S. Preface to Cellular Automata // Proceedings of an Interdisciplinary Workshop, 1984. Pp. vii – xii.

2. Тоффоли Т., Марголус Н. Машины клеточных автоматов: Пер. с англ. М.: Мир, 1991. 280 с.

3. Feistel H. Cryptography and Computer Privacy // Scientific American, vol. 228, no. 5, 1973. Pp. 15 – 23.

4. Vergili I., Yücel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen $n \times n$ S-Boxes // Turk J Elec Engin, vol. 9, no. 2, 2001. Pp. 137 – 145.