электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0421100025. ISSN 1994-0408

Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей

77-30569/241308
10, октябрь 2011
Ключарёв П. Г.
УДК 519.713.1; 519.177; 004.056.55

МГТУ им. Н.Э. Баумана
pk.iu8@yandex.ru

1. Введение

В задачах вычислительной математики, криптографии, математического моделирования часто применяются псевдослучайные последовательности. Причем такие последовательности должны быть неотличимы от истинно случайных последовательностей по своим статистическим свойствам. Для выработки таких последовательностей используют специальные алгоритмы – генераторы псевдослучайных последовательностей (ГПСП). В работах [3, 4] предлагается использовать клеточные автоматы в качестве элементов таких генераторов. Этот подход является многообещающим, так как ГПСП, основанные на клеточных автоматах, имеют очень высокую скорость работы, как при программной, так и при аппаратной реализации. Однако остается открытым вопрос о явном детерминируемом построении обобщенных клеточных автоматов для таких генераторов. Решению этого вопроса и посвящена настоящая статья.

2. Обобщенные клеточные автоматы

Классические клеточные автоматы впервые были предложены Дж. Фон Нейманом в работе [20]. Они активно исследовались (см. работы [15, 21-24]), в том числе и в контексте выработки псевдослучайных последовательностей. Недавно, в работах [3, 4], было предложено и исследовано обобщение клеточных автоматов – неоднородные клеточные автоматы. Такие автоматы мы будем называть обобщенными.

Назовем *обобщенным клеточным автоматом* пару (G, f), где $G = (V, E)$ – ориентированный регулярный мультиграф (V – множество вершин, а E – мультимножество ребер) размера n, с каждой вершиной которого ассоциирована булева переменная,

причем все вершины пронумерованы числами $0...(n-1)$. Переменную, ассоциированную с *i*-ой вершиной, будем обозначать m_i. Такие переменные мы будем называть *ячейками*. Для каждой вершины входящие в нее ребра пронумерованы числами $0...(k-1)$.

Функция $f:\{0;1\}^k \to \{0;1\}$ – локальная функция связи.

Обобщенный клеточный автомат работает следующим образом:

в начальный момент времени, каждая ячейка памяти m_i, $i=0...(n-1)$ имеет некоторое начальное значение $m_i(0)$. Далее автомат работает по шагам. На шаге с номером *t* с помощью локальной функции связи вычисляются новые значения переменных:

$$m_i(t) = f\left(m_{\eta(i,0)}(t-1), m_{\eta(i,1)}(t-1), ..., m_{\eta(i,k-1)}(t-1)\right), \quad (1)$$

где $\eta(i,j)$ – номер вершины, из которой исходит ребро, входящее в вершину i и имеющее номер j.

Выходом обобщенного клеточного автомата на шаге с номером *t* являются значения первых *r* ячеек: $m_0(t), m_1(t), ..., m_{r-1}(t)$. Соответственно, последовательность $m_0(t_0), m_1(t_0), ..., m_{r-1}(t_0), m_0(t_0+1), m_1(t_0+1), ..., m_{r-1}(t_0+1), m_0(t_0+2), ...$ будем называть *выходной последовательностью клеточного автомата*.

Поскольку клеточный автомат, очевидно, является конечным автоматом, выходная последовательность является периодической.

Рассмотрим частный случай обобщенных клеточных автоматов – неориентированный обобщенный клеточный автомат.

Назовем *неориентированным обобщенным клеточным автоматом* обобщённый клеточный автомат (G, f), где граф $G=(V,E)$ такой, что для любого $(u,v)\in E$ существует $(v,u)\in E$.

Граф неориентированного обобщённого клеточного автомата можно рассматривать как неориентированный мультиграф, если каждую пару ребер вида $(u,v)\in E$ и $(v,u)\in E$ заменить на одно неориентированное ребро $\{u,v\}$. Такой автомат можно рассматривать как тройку (G, f, η), где *G* – неориентированный мультиграф, f – локальная функция связи, а $\eta: \mathbb{Z}_n \times \mathbb{Z}_d \to \mathbb{Z}_n$ – функция нумерации ребер, определенная выше.

Одними из важных криптографических характеристик клеточного автомата являются характеристики лавинного эффекта. Лавинный эффект представляет собой способ-

ность динамической системы существенно изменять выходную последовательность при небольших изменениях входных данных.

Рассмотрим два идентичных неориентированных обобщенных клеточных автомата A_1 и A_2. Будем обозначать векторы их ячеек соответственно $\vec{m}^{(1)} = (m_0^{(1)},...,m_{n-1}^{(1)})$ и $\vec{m}^{(2)} = (m_0^{(2)},...,m_{n-1}^{(2)})$. Начальное заполнение отличается только в одной ячейке. Для определенности будем считать, что номер такой ячейки равен нулю (это не нарушает общности, поскольку перенумеровать переменные можно как угодно):

$$m_i^{(2)}(0) = \begin{cases} m_i^{(1)}(0), & i \neq 0 \\ \neg m_i^{(1)}(0), & i = 0 \end{cases}. \quad (2)$$

Будем рассматривать две характеристики лавинного эффекта: интегральную и пространственную.

Интегральной характеристикой лавинного эффекта [3] назовем зависимость доли несовпадающих ячеек у двух конечных автоматов от номера такта:

$$\omega(t) = \frac{1}{n}\sum_{j=0}^{n-1}\left(m_j^{(1)}(t) \oplus m_j^{(2)}(t)\right). \quad (3)$$

Пространственной характеристикой лавинного эффекта назовем зависимость отношения расстояния от вершины с номером 0 до самой дальней вершины, ячейка которой у двух автоматов не совпадает, к эксцентриситету вершины с номером 0:

$$\mu(t) = \frac{1}{e(0)} \cdot \max_{j \in \mathbb{Z}_n}\left(\left(m_j^{(1)}(t) \oplus m_j^{(2)}(t)\right) \cdot \Delta(0, j)\right), \quad (4)$$

где $\Delta(i, j)$ – длина минимального пути из вершины i в вершину j, а $e(i)$ – эксцентриситет вершины i.

Как показано в работе [4], для того, чтобы вероятности нулей и единиц в выходной последовательности обобщенного клеточного автомата совпадали, необходимо и достаточно, чтобы локальная функция связи являлась равновесной. Мы будем полагать ее таковой.

Мы будем рассматривать усредненные по достаточно большому количеству начальных заполнений интегральную и пространственную характеристику лавинного эффекта: $\hat{\omega}(t)$ и $\hat{\mu}(t)$.

Начиная с некоторого t_n, выполняется $\hat{\omega}(t) = \omega_n$ и $\hat{\mu}(t) = \mu_n$ при $t \geq t_n$. Для обеспечений хороших статистических характеристик выходной последовательности необходимо, чтобы $\omega_n = 0.5$, а $\mu_n = 1$.

Для обеспечения хороших статистических свойств граф клеточного автомата должен быть таким, чтобы t_n было как можно меньшим. Чтобы уменьшить эту величину следует использовать клеточный автомат, граф которого имеет возможно меньший диаметр.

Диаметр D регулярного графа размера n степени k имеет следующую нижнюю оценку (граница Мура [8, 13]):

$$D \geq \log_{k-1} n + 1 - \log_{k-1} k . \tag{5}$$

Учитывая тот очевидный факт, что $t_n \geq D$, по-видимому, следует выбрать граф с диаметром, не слишком превосходящим границу Мура. Кроме того, для реализации лавинного эффекта граф должен быть таким, чтобы изменения одной ячейки клеточного автомата приводило к изменению все большего и большего числа ячеек с каждым шагом. Этим требованиям отвечают так называемые расширяющие графы (expander graphs).

3. Расширяющие графы

Теория расширяющих графов – сравнительно молодая область дискретной математики, нашедшая много приложений в математике и информатике. Этой теории посвящено большое количество литературы. Не задаваясь целью дать полный ее обзор, приведем здесь ссылки лишь на основные источники: [5, 7, 9, 10, 14, 17, 18]. Расширяющие графы применяются в ряде прикладных областей, в том числе, в задачах дерандомизации [18, 19] и для построения кодов, исправляющих ошибки [1]. Приведем здесь основные определения из этой теории.

Коэффициентом расширения неориентированного регулярного мультиграфа $G = (V, E)$ называется величина:

$$h(G) = \min_{\left\{S \subset V \,\middle|\, 0 < |S| \leq \frac{|V|}{2}\right\}} \frac{|\partial(S)|}{|S|}, \tag{6}$$

где ∂S – множество ребер, каждое из которых инцидентно ровно одной вершине из множества *S*.

Расширяющим графом (expander graph) называется неориентированный регулярный мультиграф *G*, такой, что $h(G) \geq c$, где *c* – некоторая константа.

Коэффициент расширения графа связан с его спектральными свойствами. Так, рассмотрим отсортированный по убыванию спектр графа (то есть собственные числа его матрицы смежности):

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n. \quad (7)$$

Как известно из спектральной теории графов [5], $\lambda_1 = k$, где k – степень графа G и справедливо следующее соотношение, называемое *неравенством Чигера*:

$$\frac{1}{2}(k - \lambda_2) \leq h(G) \leq \sqrt{2k(k - \lambda_2)}. \quad (8)$$

Для того, чтобы улучшить характеристики лавинного эффекта неориентированного клеточного автомата, основанного на расширяющем графе, следует, по-видимому, выбрать граф с возможно большим коэффициентом расширения графа. Учитывая то, что задача определения коэффициента расширения является вычислительно сложной, удовлетворимся выбором графа с величиной λ_2 близкой к минимальной.

Согласно теореме Нили, нижняя граница для этой величины:

$$\lambda_2 \geq 2\sqrt{k-1} - \frac{2\sqrt{k-1}-1}{D}, \quad (9)$$

где D – диаметр графа.

К этой границе приближаются *графы Рамануджана*, то есть такие расширяющие графы, для которых справедливо неравенство

$$\lambda_2 \leq 2\sqrt{k-1}. \quad (10)$$

Для диаметра графов Рамануджана справедливо соотношение:

$$D = 2\log_{k-1} n + O(1). \quad (11)$$

Другими словами, диаметр графа Рамануджана всего в два раза больше границы Мура (5).

Учитывая близость графов Рамануджана к случайным графам по целому ряду свойств, можно ожидать, что для конечных автоматов, основанных на таких графах, t_n будет близка к диаметру.

Все это позволяет высказать гипотезу о том, что графы Рамануджана позволят обеспечить хорошие характеристики лавинного эффекта для основанных на них клеточных автоматах.

Одно из семейств графов Рамануджана – графы Любоцкого-Филипса-Сарнака (*LPS*-графы) [2, 11]. Одним из вариантов явных конструкций таких графов является конструкция, приведенная в книге [17]. Опишем ее здесь.

Выберем простые числа *p* и *q*, для которых выполняются условия:

$$\begin{cases} p = 1 \pmod 4 \\ q = 1 \pmod 4 \\ p \neq q \\ \left(\frac{q}{p}\right) = 1 \end{cases} \tag{12}$$

Мы будем строить неориентированный мультиграф $G = (V, E)$. Множеством вершин мультиграфа *V* является проективная прямая над конечным полем $\mathbb{F}_q$, другими словами, $V = \mathbb{F}_q \cup \{\infty\}$. Мультимножество ребер *E* состоит из всех пар (u, v), для которых выполняется:

$$v = \begin{cases} ((a_0 + ia_1)u + (a_2 + ia_3)) \cdot \\ \quad \cdot ((-a_2 + ia_3)z + (a_0 - ia_1))^{-1}, & при\ (a_2 - ia_3)z \neq a_0 - ia_1,\ z \neq \infty \\ \quad \infty, & при\ (a_2 - ia_3)z = a_0 - ia_1,\ z \neq \infty \\ (a_0 + ia_1)(-a_2 + ia_3)^{-1}, & при\ a_2 \neq ia_3,\ z = \infty \\ \quad \infty, & при\ a_2 = ia_3,\ z = \infty \end{cases} \tag{13}$$

для всех четверок $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, таких что:

- a_0 – нечетное положительное;
- a_1, a_2, a_3 – четные положительные;
- Выполняется условие:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p \tag{14}$$

В построенном таким образом графе могут быть кратные ребра (в том случае, когда (13) выполняется и для (u, v) и для (v, u)) и петли. Степенью графа является количество решений уравнения (14), равное $p + 1$.

В книге [17] доказано, что этот граф является графом Рамануджана.

4. Применение графов Рамануджана в клеточных автоматах

Как было указано выше, для построения неориентированного обобщенного клеточного автомата достаточно задать его граф и локальную функцию связи, которая должна быть равновесной. Для обеспечения хороших криптографических свойств клеточного автомата, его локальная функция связи должна быть как можно более нелинейной. Способы построения равновесных булевых функций, нелинейность которых близка к максимальной, описаны, например, в книге [6].

Вычислительные эксперименты показали, что статистические свойства выходной последовательности лишь несущественно зависят от вида локальной функции связи, если она является равновесной и имеет близкую к максимальной нелинейность.

В качестве графа обобщенного клеточного автомата, мы будем использовать LPS-граф, конструкция которого приведена в предыдущем разделе. У полученного таким образом клеточного автомата имеется $q+1$ ячейка, а его граф имеет степень $p+1$. Числа *p* и *q* являются простыми. На них накладываются приведенные в предыдущем разделе ограничения (12).

Были проведены вычислительные эксперименты по определению характеристик лавинного эффекта построенных таким образом клеточных автоматов, при параметрах $268 < q < 500$ и $p \in \{5,13\}$, удовлетворяющих ограничениям (12). Во всех случаях, характеристики лавинного эффекта были близки к лучшим возможным теоретически: параметр t_n был близок к диаметру графа, $\omega_n = 0.5$ и $\mu_n = 1$.

Были произведены исследования статистических свойств выходных последовательностей, при помощи тестов, рекомендованных NIST [16], по стандартной методике. При $p = 5$ выходные последовательности автоматов проходили большинство тестов, в том числе такие важные тесты, как универсальный тест Маурера [12]. При $p = 13$ последовательности проходили все тесты.

В качестве примера рассмотрим *LPS*-граф размера 270 и степени 6 ($q = 269$, $p = 5$), вид которого показан на Рис. 1, а характеристики лавинного эффекта соответствующего обобщенного клеточного автомата приведены на Рис. 2 и Рис. 3. У этого графа параметр $\lambda_2 = 4.4281$, а диаметр равен 5. Этот диаметр близок к минимально возможному для регулярных графов такой степени и такого размера диаметру, равному, согласно границе Мура (5), четырем. Из графиков видно, что $t_n = 6$, что близко к диаметру графа.

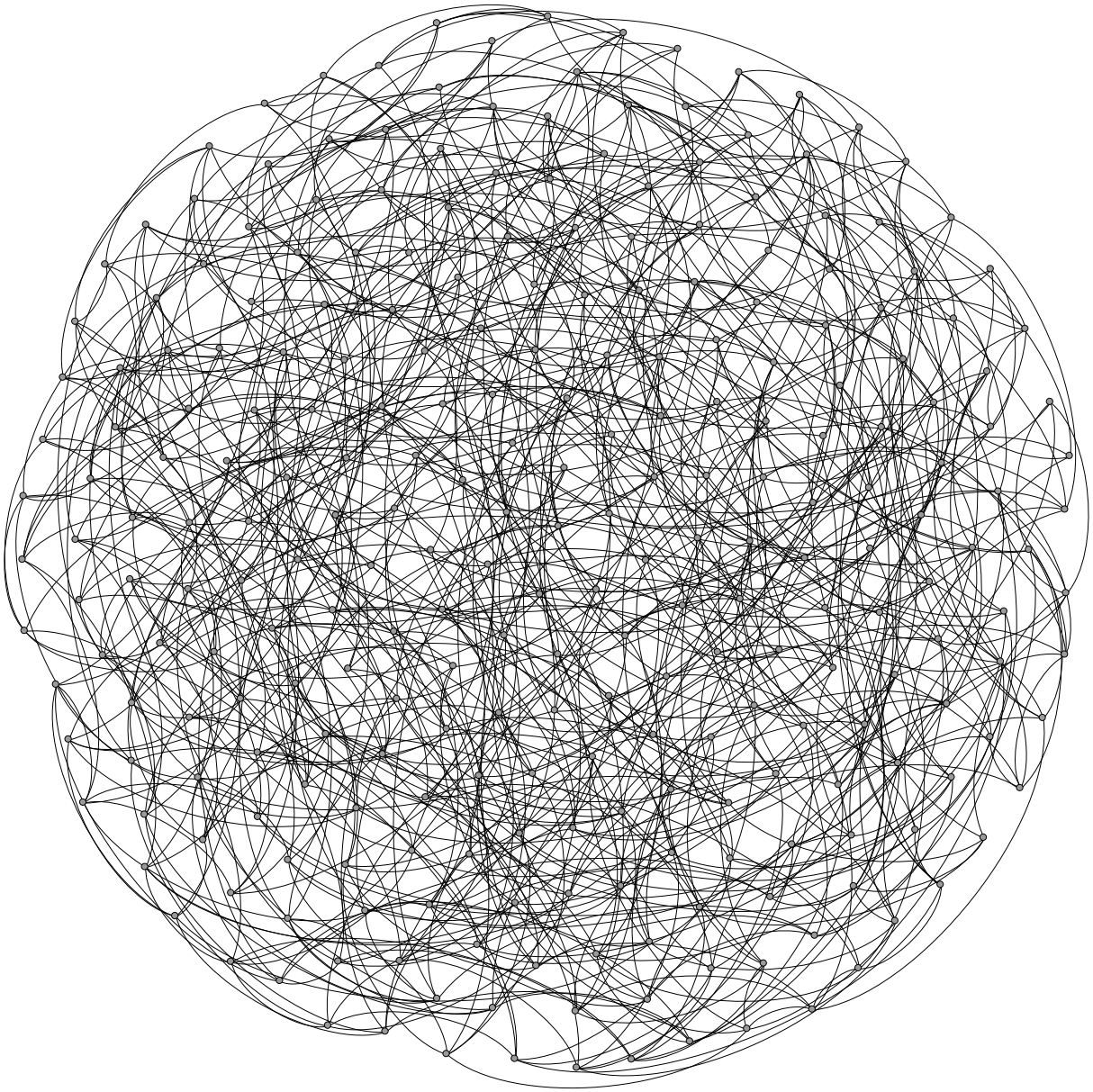

Рис. 1. LPS-граф размера 270, степени 6.

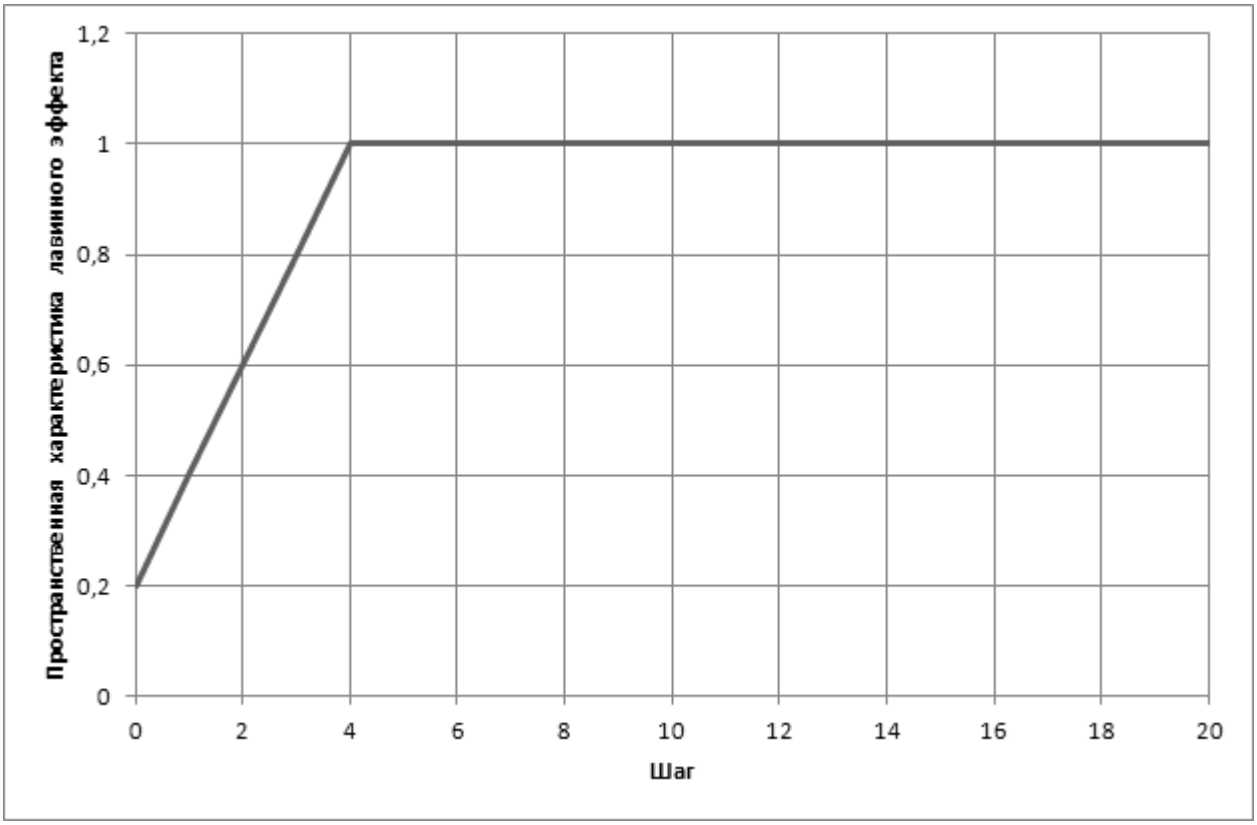

Рис. 2. Усредненная пространственная характеристика лавинного эффекта.

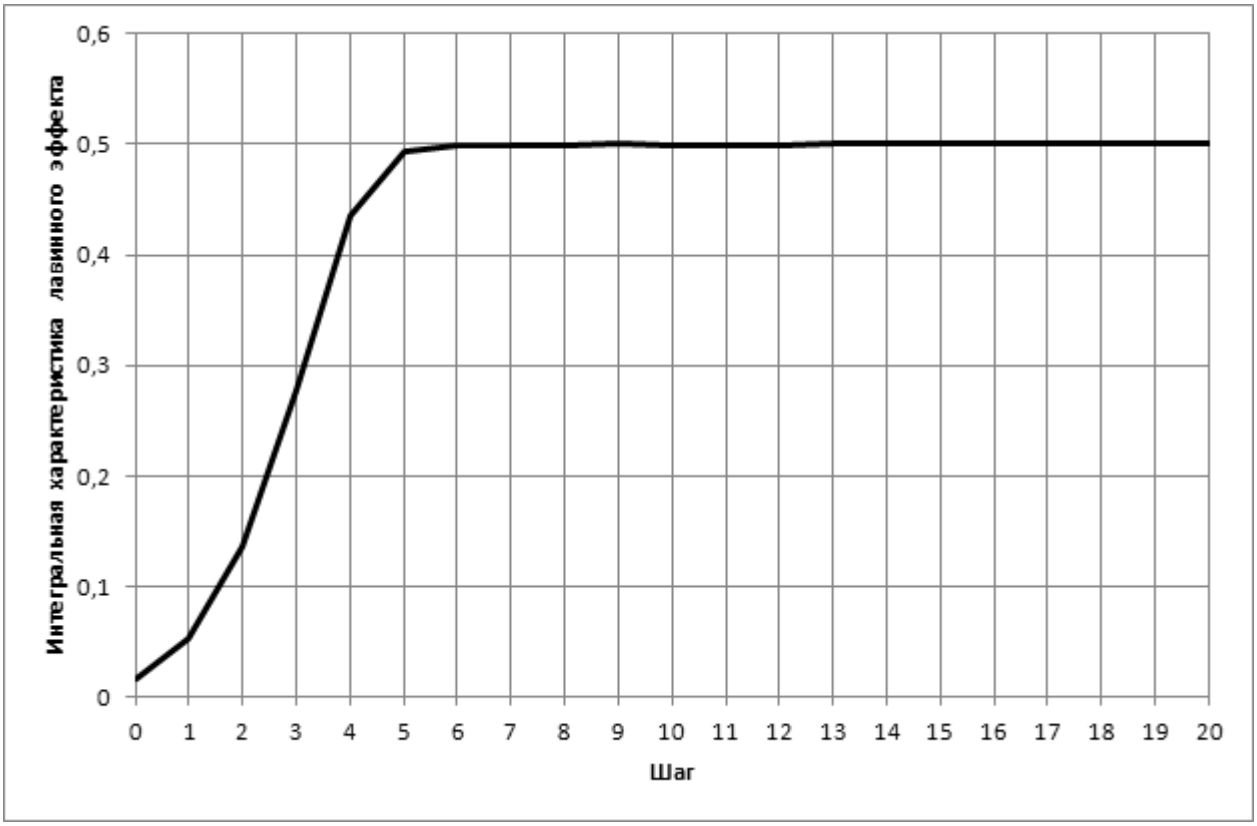

Рис. 3. Усредненная интегральная характеристика лавинного эффекта.

Использование одного автомата не обеспечивает непредсказуемости. Поэтому, мы, основываясь на схеме, предложенной в работе [4], будем использовать два обобщенных клеточных автомата A_1 и A_2 разного размера с различными локальными функциями связи: f_1 и f_2. Выходные последовательности этих автоматов поразрядно складываются по модулю два (выбор именно сложения по модулю два связан с тем, что эта функция является корреляционно-иммунной). Функции f_1 и f_2, судя по результатам экспериментов, могут быть почти любыми равновесными, с нелинейностью, близкой к максимальной. Единственное условие, которое на них следует, по-видимому, наложить, это $f_1 \neq f_2 \oplus 1$. Такая схема также существенно улучшает статистические свойства последовательности.

В качестве примера удачного сочетания параметров, для длины выхода $r = 256$, можно использовать размеры клеточных автоматов 270 и 282, как наиболее близкие к *r*. Для повышения эффективности реализации, степень графов должна быть наименьшей возможной, то есть равной 6.

Построенный таким образом ГПСП, при $p = 5$ генерирует случайные последовательности, которые успешно проходят все статистические тесты, рекомендованные NIST.

5. Заключение

Предложен способ детерминированного построения обобщенных клеточных автоматов, имеющих близкие к оптимальным характеристики лавинного эффекта. Генераторы псевдослучайных последовательностей, основанные на таких клеточных автоматах, вырабатывают последовательности, имеющие статистические свойства криптографического качества, что подтверждается успешным прохождением тестов, рекомендованных NIST. Такие генераторы могут найти применения как в криптографии и стеганографии, так и в различных областях математического моделирования.

Литература

1. Жуков Д.А. Асимптотически хорошие коды с линейной сложностью кодирования и декодирования // Дискретная математика и её приложения. – 2009. – №5. – С. 23-25.
2. Маргулис Г.А. Явные теоретико-групповые конструкции комбинаторных схем и их применения в построении расширителей и концентраторов // Пробл. передачи информ. – 1988. – Vol. 24, №1. – С. 51-60.

3. Сухинин Б.М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование: электронное научно-техническое издание. – 2010. – №8. – http://technomag.edu.ru/doc/159565.html.
4. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование: электронное научно-техническое издание. – 2010. – №9. – http://technomag.edu.ru/doc/159714.html.
5. Chung F.R.K. Regional conference series in mathematics,. Spectral graph theory. – Providence, R.I.: Published for the Conference Board of the mathematical sciences by the American Mathematical Society, 1997. – 207 p.
6. Cusick T.W., Stanica P. Cryptographic Boolean functions and applications. Academic Press, 2009.
7. Davidoff G.P., Sarnak P., Valette A. London Mathematical Society student texts. Elementary number theory, group theory, and Ramanujan graphs. – New York: Cambridge University Press, 2003. – 144 p.
8. Hoffman A., Singleton R. On Moore graphs with diameter 2 and 3, IBM Res // Develop. – 1960. – Vol. 4, P. 497–504.
9. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // Bulletin-American Mathematical Society. – 2006. – Vol. 43, №4. – 439 p.
10. Krebs M., Shaheen A. Expander families and Cayley graphs. – Oxford ; New York: Oxford University Press, 2011.
11. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. – 1988. – Vol. 8, №3. – P. 261-277.
12. Maurer U.M. A universal statistical test for random bit generators // Journal of cryptology. – 1992. – Vol. 5, №2. – P. 89-105.
13. Miller M., Širán J. Moore graphs and beyond: A survey of the degree/diameter problem // Electronic Journal of Combinatorics. – 2005. – Vol. 61, P. 1-63
14. Morgenstern M. Existence and explicit constructions of q+ 1 regular Ramanujan graphs for every prime power q // Journal of Combinatorial Theory, Series B. – 1994. – Vol. 62, №1. – P.44-62.
15. Packard N.H., Wolfram S. Two-dimensional cellular automata // Journal of Statistical Physics. – 1985. – Vol. 38, №5. – P.901-946.
16. Rukhin A., и др. A statistical test suite for random and pseudorandom number generators for cryptographic applications (SP 800-22). NIST, 2010.
17. Sarnak P. Cambridge tracts in mathematics. Some applications of modular forms. – Cambridge ; New York: Cambridge University Press, 1990. – 111 p.
18. Vadhan S. The unified theory of pseudorandomness // ACM SIGACT News. – 2007. – Vol. 38, №3. – P. 39-54.
19. Vadhan S.P. Pseudorandomness // Foundations and Trends in Theoretical Computer Science. – 2010. – 200 p.

20. Von Neumann J. The general and logical theory of automata // Cerebral mechanisms in behavior. – 1951. – P. 1–41.
21. Wolfram S. Cryptography with cellular automata //: Springer, 1986. - P. 429-432.
22. Wolfram S. Statistical mechanics of cellular automata // Reviews of Modern Physics. – 1983. – Vol. 55, №3. – 601 p.
23. Wolfram S. Theory and applications of cellular automata // Advanced Series on Complex Systems, Singapore: World Scientific Publication, 1986. – 1986. – Vol. 1.
24. Wolfram S. Universality and complexity in cellular automata // Physica D: Nonlinear Phenomena. – 1984. – Vol. 10, №1-2. – P. 1-35.

electronic scientific and technical periodical
SCIENCE and EDUCATION
EL № FS 77 - 30569. №0421100025. ISSN 1994-0408

Cellular automations based on Ramanujan graphs in the field of the generation of pseudorandom sequences.

77-30569/241308

10, October 2011

Klyucharev P.G.

Bauman Moscow State Technical University
pgkl@yandex.ru

The problems of an explicit construction of generalized cellular automations for the generation of pseudorandom sequences are considered in this article. It is theoretically approved and empirically confirmed that the avalanche effect parameters of the generalized cellular automations based on Ramanujan graphs are nearly optimal. The pseudorandom sequence generator of the cryptographic quality based on these cellular automations is introduced in the article.

Publications with keywords: cryptography, cellular automata, expander graph, pseudorandom sequence generator

Publications with words: cryptography, cellular automata, expander graph, pseudorandom sequence generator

Reference

1. Zhukov D.A., Diskretnaia matematika i ee prilozheniia 5 (2009) 23-25.
2. Margulis G.A., Problemy peredachi informatsii 24 (1) (1988) 51-60.
3. Sukhinin B.M., Nauka i obrazovanie - Science and Education 8 (2010) <http://technomag.edu.ru/doc/159565.html>.
4. Sukhinin B.M., Nauka i obrazovanie - Science and Education 9 (2010) <http://technomag.edu.ru/doc/159714.html>.
5. Chung F.R.K., Regional conference series in mathematics,. Spectral graph theory. – Providence, R.I.: Published for the Conference Board of the mathematical sciences by the American Mathematical Society, 1997, 207 p.

6. Cusick T.W., Stanica P., Cryptographic Boolean functions and applications, Academic Press, 2009.
7. Davidoff G.P., Sarnak P., Valette A., London Mathematical Society student texts, Elementary number theory, group theory, and Ramanujan graphs, New York: Cambridge University Press, 2003, 144 p.
8. Hoffman A., Singleton R. On Moore graphs with diameter 2 and 3, IBM Res, Develop., 1960, Vol. 4, pp. 497–504.
9. Hoory S., Linial N., Wigderson A., Expander graphs and their applications, Bulletin-American Mathematical Society 43 (4) (2006) 439.
10. Krebs M., Shaheen A., Expander families and Cayley graphs, Oxford, New York, Oxford University Press, 2011.
11. Lubotzky A., Phillips R., Sarnak P., Ramanujan graphs, Combinatorica 8 (3) (1988) 261-277.
12. Maurer U.M., A universal statistical test for random bit generators, Journal of cryptology 5 (2) (1992) 89-105.
13. Miller M., Širán J., Moore graphs and beyond: A survey of the degree/diameter problem, Electronic Journal of Combinatorics 61 (2005) 1-63.
14. Morgenstern M., Existence and explicit constructions of q+ 1 regular Ramanujan graphs for every prime power q, Journal of Combinatorial Theory, Series B 62 (1) (1994) 44-62.
15. Packard N.H., Wolfram S., Two-dimensional cellular automata, Journal of Statistical Physics 38 (5) (1985) 901-946.
16. Rukhin A., et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications (SP 800-22), NIST, 2010.
17. Sarnak P., Cambridge tracts in mathematics. Some applications of modular forms, Cambridge, New York, Cambridge University Press, 1990, 111 p.
18. Vadhan S., The unified theory of pseudorandomness, ACM SIGACT News 38 (3) (2007) 39-54.
19. Vadhan S.P., Pseudorandomness, Foundations and Trends in Theoretical Computer Science, 2010, 200 p.
20. Von Neumann J., The general and logical theory of automata, Cerebral mechanisms in behavior, 1951, pp. 1–41.
21. Wolfram S., Cryptography with cellular automata , Springer, 1986, pp. 429-432.
22. Wolfram S., Statistical mechanics of cellular automata, Reviews of Modern Physics 55 (3) (1983) 601.

23. Wolfram S., Theory and applications of cellular automata, Advanced Series on Complex Systems, Singapore, World Scientific Publication, 1986, Vol. 1.
24. Wolfram S., Universality and complexity in cellular automata, Physica D: Nonlinear Phenomena 10 (1-2) (1984) 1-35.