СИНТЕЗ И АНАЛИЗ АСИММЕТРИЧНЫХ КРИПТОПРИМИТИВОВ

УДК 004.032.26

Е.А. ВИНОКУРОВА, д-р техн. наук

ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МОДИФИЦИРОВАННОЙ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

Введение

Генераторы псевдослучайных последовательностей являются важным блоком в областях науки, а именно в информатике, прикладной математике, тестировании программных средств, криптографических системах шифрования [1 – 3].

Генераторы псевдослучайных последовательностей должны обладать такими преимуществами как непрогнозируемость сгенерированной последовательности чисел по некоторой ее части, повышенной скоростью генерации, а также удовлетворять требованиям, описанным в стандартах [4 – 7].

Большинство генераторов псевдослучайных последовательностей основываются на детерминистических алгоритмах. На данный момент существуют различные методы генерации псевдослучайных последовательностей, среди которых метод Блюма – Блюма – Шуба [8], метод Блюма и Микали [9], алгоритм Mersenne Twister [10, 11] и др. Существующие генераторы имеют ряд недостатков, таких как невозможность использования в on-line режиме.

Для решения этой проблемы в последнее время широкое использование получили генераторы псевдослучайных последовательностей на основе гибридных нейронных сетей, которые являются существенно нелинейными системами [12 – 15], а также обладают свойствами обучаемости и обработкой данных в on-line режиме. Большинство таких генераторов основывается на многослойных нейронных сетях с громоздкими методами обучения с параметрами, которые необходимо выбирать вручную.

В статье предлагается генератор псевдослучайных последовательностей на основе модифицированной рекуррентной нейронной сети, а также ее метод обучения для работы в последовательном режиме обработки данных.

1. Модифицированная рекуррентная нейронная сеть

Важный класс искусственных нейронных сетей – рекуррентные нейронные сети, имеющие замкнутые петли обратной связи в своей топологии. В этих сетях на первый план выступает фактор времени: входные сигналы в искусственных нейронных сетях должны быть заданы в форме временной последовательности, автокорреляционные свойства которой выявляются и анализируются в процессе обработки.

В рекуррентных сетях в основном используется два способа организации обратной связи: локальная обратная связь на уровне отдельных нейронов и глобальная, охватывающая сеть в целом, хотя возможны и промежуточные варианты. Так, если в качестве базового строительного блока рекуррентной сети принять многослойный персептрон, то локальная обратная связь организуется на уровне отдельного слоя, глобальная – связывает нейроны выходного слоя со входами сети, однако при этом возможны варианты связи от скрытого слоя ко входному или от скрытого к предыдущему скрытому слою.

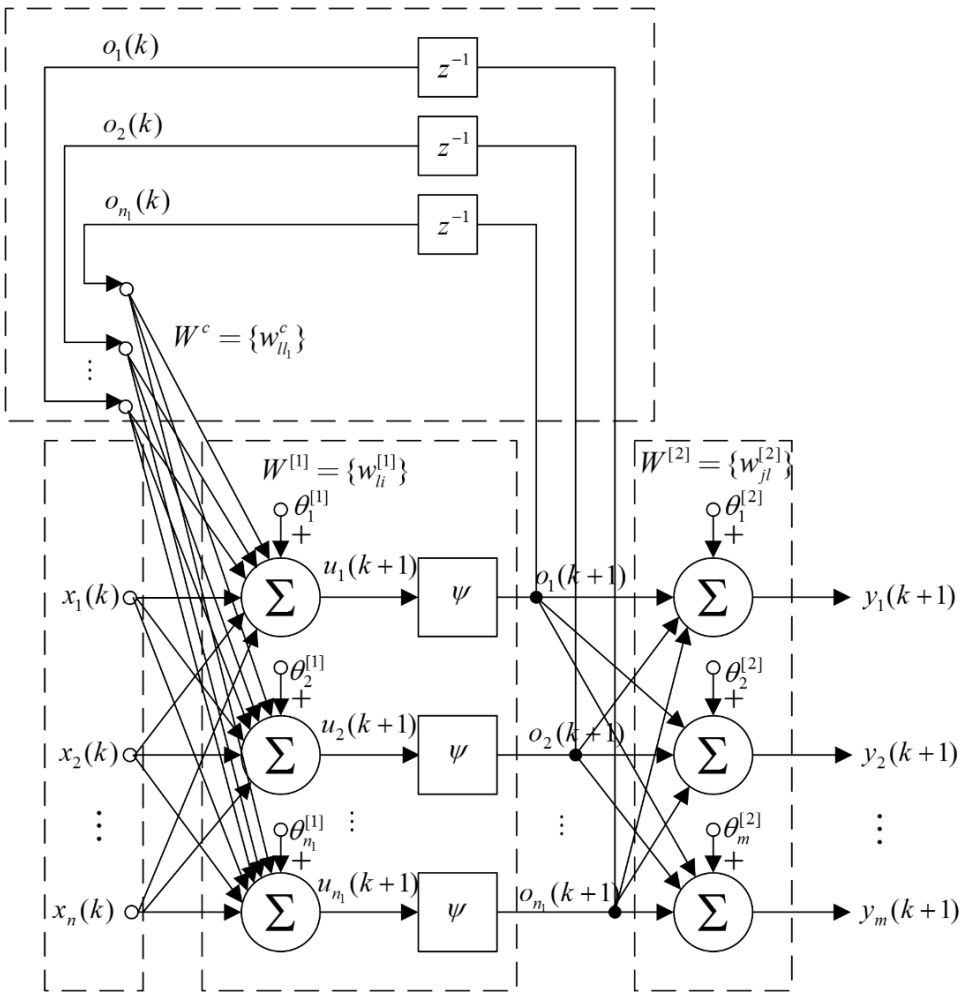
В настоящее время сформировалось два больших класса рекуррентных сетей: сети, реализующие отображение «вход-выход» с учетом временного фактора, и сети ассоциативной памяти. Последние будут рассмотрены в следующем разделе, а здесь подробно остановимся на сетях первого класса, широко применяемых для решения задач оптимизации, идентификации, эмуляции, прогнозирования, управления, диагностики и т.п., словом там, где фактор времени имеет существенное значение.

С точки зрения нейродинамики рекуррентные сети рассматриваются как многосвязные динамические нелинейные стохастические диссипативные системы с большим числом степеней свободы, для анализа устойчивости которых неприменимы традиционные инженерные критерии устойчивости [16].

В связи с этим основные подходы к разработке и анализу рекуррентных сетей связаны с аппаратом функций Ляпунова [17], идентификацией устойчивых состояний (аттракторов) и минимизацией тех или иных форм энергетических функций.

Введем в рассмотрение многослойную рекуррентную нейронную сеть, предназначенную для генерации псевдослучайных последовательностей, архитектура которой приведена на рисунке. В дополнение к традиционным скрытому и выходному слоям в сеть введен специальный слой обратной связи, называемый контекстным или слоем состояний. Этот слой получает сигналы с выхода скрытого слоя и через элементы задержки подает их на входной слой, сохраняя таким образом обрабатываемую информацию в течение одного временного такта.

«Строительными блоками» модифицированной рекуррентной нейронной сети являются стандартные нейроны со специализированными активационными сигмоидальными функциями, адаптивные линейные ассоциаторы и элементы задержки z^{-1}.



Архитектура модифицированной рекуррентной нейронной сети

Функционирование модифицированной рекуррентной нейронной сети описывается системой рекуррентных соотношений

$$y_j(k+1) = \sum_{l=1}^{n_1} w_{jl}^{[2]} o_l(k+1) + \theta_j^{[2]},\ j = 1,2,\ldots m, \tag{1}$$

$$\begin{cases} u_l(k+1) = \sum\limits_{i=1}^{n} w_{li}^{[1]} x_i(k) + \sum\limits_{i=1}^{n} w_{ll_1}^{c} o_{l_1}(k) + \theta_l^{[1]}, \\ o_l(k+1) = \psi(u_l(k+1)) = \dfrac{1}{1+\exp(-\gamma u_l(k+1))},\ l = 1,2,\ldots,n_1, \end{cases} \tag{2}$$

где γ – параметр крутизны сигмоидальной функции активации.

Для упрощения описания структуры рекуррентной нейронной сети предлагается использовать матричную форму

$$o(k+1) = \Psi(W^{[1]} x(k) + W^c o(k) + \theta^{[1]}), \tag{3}$$

$$y(k+1) = W^{[2]} o(k) + \theta^{[2]}, \tag{4}$$

где $W^{[1]} = \{w_{li}\} - (n_1 \times n)$ – матрица настраиваемых синаптических весов входного слоя; $W^c = \{w_{ll_1}\} - (n_1 \times n_1)$ – матрица настраиваемых синаптических весов контекстного слоя; $W^{[2]} = \{w_{jl}\} - (m \times n_1)$ – матрица настраиваемых синаптических весов выходного второго слоя;

$x(k) = (x_1(k), x_2(k), \ldots, x_n(k))^T - (n \times 1)$ – вектор входов первого слоя;

$o(k) = (o_1(k), o_2(k), \ldots, o_{n_1}(k))^T - (n_1 \times 1)$ – вектор входов второго слоя;

$\theta^{[1]}(k) = (\theta_1^{[1]}(k), \theta_2^{[1]}(k), \ldots, \theta_{n_1}^{[1]}(k))^T - (n_1 \times 1)$;

$\theta^{[2]}(k) = (\theta_1^{[2]}(k), \theta_2^{[2]}(k), \ldots, \theta_m^{[2]}(k))^T - (m \times 1)$ – векторы смещений первого и второго слоя соответственно.

2. Метод обучения модифицированной рекуррентной нейронной сети

Рассмотрим метод обучения модифицированной рекуррентной нейронной сети на основе алгоритма обратного распространения ошибок.

Исходная информация должна быть задана в виде последовательности пар образов «вход/выход», образующих обучающую выборку. Обучение состоит в адаптации параметров всех слоев таким образом, чтобы расхождение между выходным сигналом сети и внешним обучающим сигналом в среднем было бы минимальным. Из этого следует, что алгоритм обучения представляет собой по сути процедуру поиска экстремума специально синтезированной целевой функции ошибок.

Введем обозначения: n – количество входов, n_1 количество нейронов в первом скрытом слое и m – количество выходов. Каждый входной образ представляет собой $(n \times 1)$-вектор $x = (x_1, \ldots, x_i, \ldots, x_n)^T$, выходной образ – $(m \times 1)$-вектор $y = (y_1, \ldots, y_j, \ldots, y_m)^T$ и обучающий образ $-(m \times 1)$-вектор $d = (d_1, \ldots, d_j, \ldots, d_m)^T$. Необходимо в процессе обучения обеспечить минимальное рассогласование между текущими значениями выходных $y_j(k)$ и желаемых

$d_j(k)$ сигналов для всех $j = 1,2,\ldots,m$ и k. Обычно в качестве функции ошибок используется локальный критерий качества

$$E(k) = \frac{1}{2}\sum_{j=1}^{m}(d_j(k) - y_j(k))^2 = \frac{1}{2}\sum_{j=1}^{m} e_j^2(k) = \frac{1}{2}\sum_{j=1}^{m}\left(d_j(k) - \left[\sum_{l=1}^{n_1} w_{jl}^{[2]} o_l(k+1) + \theta_j^{[2]}\right]\right)^2 =$$
$$= \frac{1}{2}\sum_{j=1}^{m}\left(d_j(k) - \left[\sum_{l=1}^{n_1} w_{jl}^{[2]}\psi_l(u_l(k+1)) + \theta_j^{[2]}\right]\right)^2. \quad (5)$$

Рассмотрим алгоритм обучения реального времени, связанный с минимизацией на каждом шаге локальной функции $E(k)$. Очевидно, что для синаптических весов выходного слоя $w_{jl}^{[2]}$ справедливо соотношение типа

$$w_{jl}^{[2]}(k+1) = w_{jl}^{[2]}(k) - \eta(k)\frac{\partial E(k)}{\partial w_{jl}^{[2]}(k)} = w_{jl}^{[2]}(k) - \eta(k)\frac{\partial E(k)}{\partial e_j(k)}\frac{\partial e_j(k)}{\partial y_j(k)}\frac{\partial y_j(k)}{\partial w_{jl}^{[2]}(k)} =$$
$$= w_{jl}^{[2]}(k) + \eta(k)e_j(k)o_l(k+1). \quad (6)$$

Аналогично можно записать формулу настройки весов первого скрытого слоя

$$w_{li}^{[1]}(k+1) = w_{li}^{[1]}(k) - \eta(k)\frac{\partial E(k)}{\partial w_{li}^{[1]}(k)} =$$
$$= w_{li}^{[1]}(k) - \eta(k)\frac{\partial E(k)}{\partial e_j(k)}\frac{\partial e_j(k)}{\partial y_j(k)}\frac{\partial y_j(k)}{\partial \psi_l(u_l(k+1))}\frac{\partial \psi_l(u_l(k+1))}{\partial u_l(k+1)}\frac{\partial u_l(k+1)}{\partial w_{li}^{[1]}(k)} =$$
$$= w_{li}^{[1]}(k) + \eta(k)e_j(k)w_{jl}^{[2]}(k)x_i(k)\frac{\partial \psi_l(u_l(k+1))}{\partial u_l(k+1)} =$$
$$= w_{li}^{[1]}(k) + \eta(k)e_j(k)w_{jl}^{[2]}(k)x_i(k)\gamma\psi_l(u_l(k+1))(1-\psi_l(u_l(k+1))) \quad (7)$$

и алгоритм настройки синаптических весов контекстного слоя

$$w_{ll_1}^{c}(k+1) = w_{ll_1}^{c}(k) - \eta(k)\frac{\partial E(k)}{\partial w_{ll_1}^{c}(k)} =$$
$$= w_{ll_1}^{c}(k) - \eta(k)\frac{\partial E(k)}{\partial e_j(k)}\frac{\partial e_j(k)}{\partial y_j(k)}\frac{\partial y_j(k)}{\partial \psi_l(u_l(k+1))}\frac{\partial \psi_l(u_l(k+1))}{\partial u_l(k+1)}\frac{\partial u_l(k+1)}{\partial w_{ll_1}^{c}(k)} =$$
$$= w_{ll_1}^{c}(k) + \eta(k)e_j(k)w_{ll_1}^{c}(k)x_i(k)\frac{\partial \psi_l(u_l(k+1))}{\partial u_l(k+1)} =$$
$$= w_{ll_1}^{c}(k) + \eta(k)e_j(k)w_{jl}^{[2]}(k)o_{l_1}(k)\gamma\psi_l(u_l(k+1))(1-\psi_l(u_l(k+1))) \quad (8)$$

Работу алгоритма обратного распространения ошибок удобно описать в виде последовательности следующих шагов:

- задание начальных условий для всех синаптических весов сети в виде достаточно малых случайных чисел (обычно $--0.5/n_{s-1} < w_{ji}^{[s]} < 0.5/n_{s-1}$) с тем, чтобы активационные функции нейронов не вошли в режим насыщения на начальных стадиях обучения (защита от «паралича» сети);
- подача на вход сети образа x и вычисление выходов всех нейронов при заданных значениях $w_{ji}^{[s]}$;
- по заданному обучающему вектору d и вычисленным промежуточным выходам $o_j^{[s]}$ расчет локальных ошибок $\delta_j^{[s]}$ для всех слоев;
- уточнение всех синаптических весов;
- подача на вход сети следующего образа x и т.д.

Процесс обучения продолжается до тех пор, пока ошибка на выходе ИНС не станет достаточно малой, а веса стабилизируются на некотором уровне. После обучения нейронная сеть приобретает способности к обобщению, т.е. начинает правильно классифицировать образы, не представленные в обучающей выборке. Это самая главная черта многослойных сетей, осуществляющих после обучения произвольное нелинейное отображение пространства входов в пространство выходов на основе аппроксимации сложных многомерных нелинейных функций.

Свойства рассмотренной выше процедуры обучения существенно зависят от выбора параметра шага $\eta(k)$. С одной стороны, он должен быть достаточно малым, чтобы обеспечить оптимизацию глобальной целевой функции, с другой – малый шаговый коэффициент резко снижает скорость сходимости, а следовательно, увеличивает время обучения.

3. Метод генерации псевдослучайных последовательностей

Метод генерации псевдослучайной последовательности основывается на матрице синаптических весов скрытого (контекстного) слоя $W^c = \{w_{ll_1}^c\}$, размерностью $(n \times n)$. Для обучения сети используется входное уникальное ключевое слово (последовательность) x и выходная последовательность y и обучающий сигнал d. На основе обучающей выборки производится обучение модифицированной рекуррентной нейронной сети до достижения заданного уровня среднеквадратичной ошибки.

Таким образом, генератор псевдослучайных последовательностей можно записать в виде

$$PRNGnn = f\left(\left|W^c\right| - I \cdot W_{mean}^c\right), \tag{9}$$

где $PRNGnn$ – сгенерированная псевдослучайная последовательность на основе модифицированной рекуррентной нейронной сети, f – функция преобразования матрицы в вектор, $|\bullet|$ – абсолютное значение матрицы W^c, W_{mean}^c – вектор строка средних значений по каждому столбцу матрицы W^c, I – единичный вектор столбец.

Тестирование генерируемой псевдослучайной последовательности может быть проверена, используя методики такие как NIST STS, FIPS PUB 140-1, AIS 20 та AIS 31 [4 – 7].

Методика FIPS PUB 140-1 – применяется как средство оперативного контроля. Ее применение обусловлено высокой скоростью выполнения статистического тестирования и позволяет проводить статистический контроль в on-line режиме.

Методика NIST STS – применяется как способ комплексного контроля. Выбор этой методики обусловлен тем, что она содержит необходимый набор статистических тестов, совокупность которых обусловлена, и предлагает критерии принятия решений относительно не только последовательности, а и относительно всего генератора псевдослучайных последовательностей.

Методика AIS 20 – используется для тестирования детерминированных псевдослучайных последовательностей. Может применяться как в реальном времени, так и в процессе исследования, а также для технологического тестирования.

Методика AIS 31 – также является надежным способом тестирования последовательностей. Методика может быть использована в реальном времени, а также в процессе исследований и технологического тестирования. В AIS 31 учтены требования качественной проверки на случайность и возможность оперативного тестирования [18].

Выводы

В качестве генератора псевдослучайных последовательностей предложено использовать модифицированную рекуррентную нейронную сеть. Такой подход позволяет получить метод генерации последовательностей в последовательном режиме. Синтезирован метод обучения модифицированной рекуррентной нейронной сети. Результаты экспериментов подтверждают эффективность предложенного подхода.

Список литературы: 1. *Agnew G.B.* Random Source for Cryptographic Systems / Agnew G.B. // Advances in Cryptology. EUROCRYPT '87 Proceedings, Springer-Verlag. – 1988. – P. 77-81. 2. *Eastlake D.* Randomness Requirements for Security // Eastlake D., Crocker S.D., Schiller J.I. RFC 1750, Internet Engineering Task Force, Dec. 2005. 3. *L'Ecuyer P.* Random Number Generation and Quasi-Monte Carlo // in Encyclopedia of Actuarial Science, J. Teugels and B. Sundt Eds., John Wiley, Chichester, UK. – 2004. – 3. – P. 1363-1369. 4. *NIST* SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: April 2000. Режим доступа: http://csrc.nist.gov/publications /nistpubs/SP800-22rev1a.pdf 5. *Federal* Information Processing Standarts Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994. 6. *Aplication* Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for Deterministic random number generators. 1999. 7. *Aplication* Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. 2001. 8. *Blum L.* A simple unpredictable pseudo random number generator / Blum L., Blum M., Shub M. // SIAM Journal on Computing. – 1986. – 15(2). – P. 364-383. 9. *Blum L.* Howto generate cryptographically strong sequences of pseudo random bits / Blum L., Micali S. // SIAM Journal on Computing. – 1984. – P. 850-863. 10. *Matsumotora* Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator / Matsumoto, Nishimura // ACM Transactions on Modelling and Computer Simulation. – 1998. – 8(1). – P. 3-30. 11. *Abdi H.* A neural network primer // Journal of Biological Systems, 1994. – 2. – P. 247-281. 12. *Kauffman S.* Understanding genetic regulatory networks // Int. J. of Astrobiology, 2003. – P. 234-237. 13. *Desai V.V.* S-box design for DES using neural networks for bent function approximation // Desai V.V., Rao D. H. // Proc. of IEEE, INDICON-07, Bangalore, India. – P. 223-227. 14. *Schneier B.* Applied Cryptrography / Schneier B. – John Wiley & Sons, 1996. – 758 p. 15. *Plumb C.* Truly Random Numbers / Plumb C. // Dr. Dobbs Journal. – 1994. – 19 (13) – P. 113-115. 16. *Первозванский А. А.* Курс теории автоматического управления. – М. : Наука, 1986. – 616 с. 17. *Справочник* по теории автоматического управления ; под. ред. А. А. Красовского. – М. : Наука, 1987. – 712 с. 18. *Горбенко І.Д.* Прикладна криптологія. Теорія. Практика. Застосування / Горбенко І.Д., Горбенко Ю.І. – Харків : Форт, 2012. – 870 с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.01.2014