$$x_{n+1} = \left(E - \alpha A^2\right)x_n + \alpha A y, \quad x_0 = 0, \tag{2}$$

который в случае приближенной правой части y_δ : $\|y - y_\delta\| \le \delta$ примет вид

$$x_{n+1,\delta} = \left(E - \alpha A^2\right)x_{n,\delta} + \alpha A y_\delta, \quad x_{0,\delta} = 0.$$

Ранее изучен случай единственности решения и в предположении, что точное решение уравнения (1) истокопредставимо, доказана сходимость метода (2) и получены оценки погрешности.

Покажем, что метод (2) пригоден для решения линейных уравнений и тогда, когда его решение неединственно.

Обозначим через $N(A) = \{x \in H \mid Ax = 0\}$, $M(A) = H - N(A)$, т.е. $M(A)$ – ортогональное дополнение ядра $N(A)$ до H.

Пусть $P(A)x$ – проекция $x \in H$ на $N(A)$, а $\Pi(A)x$ – проекция $x \in H$ на $M(A)$. Справедлива

Теорема. Пусть $A \ge 0$, $y \in H$, $0 < \alpha < \frac{2}{\|A\|^2}$. тогда для итеративного процесса (2) верны следующие утверждения:

а) $Ax_n \to \Pi(A)y$, $\|Ax_n - y\| \to I(A,y) = \inf\limits_{x \in H} \|Ax - y\|$,

б) (2) сходится тогда и только тогда, когда уравнение $Ax = \Pi(A)y$ разрешимо.

В последнем случае $x_n \to P(A)x_0 + \tilde{x}$, где $\tilde{x}$ – минимальное решение уравнения (1).

Замечание. Так как у нас $x_0 = 0$, то $x_n \to \tilde{x}$, т.е процесс (2) сходится к нормальному решению, т.е. к решению с минимальной нормой.

О КРИТЕРИИ ПОИСКА НАБОРА "ШАБЛОНОВ" ДЛЯ ТЕСТИРОВАНИЯ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Милованова И.С., БГУ, г. Минск

1. Введение

В настоящее время в информационных системах для защиты информации широко начали использоваться криптографические алгоритмы. Надежность криптографических алгоритмов определяется качеством бинарных последова-

тельностей, используемых для создания ключей алгоритмов: бинарные последовательности должны быть порождены моделью независимых симметричных испытаний Бернулли.

Общепринятым подходом к анализу качества бинарных последовательностей является применение набора статистических критериев [1, 2]. Одним из популярных критериев является критерий серий, построенный по пересекающимся отрезкам [1].

При применении большого количества критериев возникает проблема принятия итогового решения о качестве последовательности. Поэтому было предложено несколько методик принятия решения: методы Бонферрони, Симса и др. [4], однако их нельзя считать эффективными при использовании "зависимых" критериев.

В данной статье вместо критерия серий предлагается использовать "близкий" критерий поиска шаблона [2, 3]. Для учета зависимости между критериями было исследовано совместное распределение статистик критерия поиска шаблона, что позволило построить критерий, использующий множество различных шаблонов.

2. Критерий поиска набора "шаблонов"

В качестве математической модели для анализа бинарных последовательностей $\{X_t\}$ будем использовать симметричную модель Бернулли:

$$\mathbf{H}_0: \quad \{X_t\} \text{ - независимые одинаково распределенные с.в.,} \quad P\{X_t = 1\} = P\{X_t = 0\} = 0.5. \tag{1}$$

Пусть наблюдается выборка $X = (x_1, \ldots, x_n)$ объема n, $x_t \in \{0,1\}$

Рассмотрим задачу проверки гипотезы (1) для выборки X с использованием частот "шаблонов". Пусть $H = (h_1, \ldots, h_m)$ —заданный бинарный вектор-строка длины m, который будем называть шаблоном. Обозначим $W(H)$ — число появлений шаблона H в выборке X:

$$W(H) = \sum_{t=1}^{n-m+1} I\{x_{t+k-1} = h_k, k = \overline{1,m}\}.$$

Обозначим $A_{H_1H_2}(Z)=\sum_{k\in H_1H_2}2^{k-m_1}Z^{m_1-k}$ — корреляционный полином, где H_1H_2 — множество натуральных чисел k таких, что суффикс длины k шаблона H_1 равен префиксу длины k шаблона H_2. В случае $H_1=H_2$ корреляционный полином называется автокорреляционным полиномом.

В [3] было найдено распределение статистики $W(H)$.

Теорема 1. [3] *Если верна гипотеза* $\mathbf{H}_0$, *то в асимптотике* $n\to\infty$ *статистика* $W(H)$ *имеет асимптотически нормальное распределение:*

$$L\{(W(H)-\mu(H))/\sigma(H)\}\to N(0,1),$$

$$\mu(H)=\frac{n-m+1}{2^m},\quad \sigma^2(H)=\frac{n}{2^m}\left(1-\frac{2m-1}{2^m}+\frac{A_{HH}(1)-1}{2}\right)+O(1).$$

Для тестирования бинарных последовательностей следует использовать не один шаблон, а набор шаблонов. Поэтому исследуем совместное распределение частот различных шаблонов. Сначала рассмотрим случай двух шаблонов.

Теорема 2. *В условиях теоремы 1 для двух различных шаблонов* H_1 *и* H_2 *длины* m_1 *и* m_2 $(m_1\ge m_2)$ *вектор частот* $W=(W(H_1),W(H_2))'$ *имеет асимптотически нормальное распределение с вектором математического ожидания* $\mu=(\mu(H_1),\mu(H_2))$ *и ковариационной матрицей* $\Sigma=(\sigma_{ij})$:

$$\sigma_{12}=\sigma_{21}=\frac{-n(m_1+m_2-1)}{2^{m_1+m_2}}+\frac{nA_{H_1H_2}(1)}{2^{m_1}}+\frac{nA_{H_2H_1}(1)}{2^{m_2}}+\frac{nB(H_1,H_2)}{2^{\max(m_1,m_2)}}+O(1),$$

где $\sigma_{ii}=\sigma^2(H_i)$ $(i=1,2)$, $B(H_1,H_2)=\left|\{i,i=\overline{2,m_1-m_2}\mid h_i^1=h_1^2,\ldots,h_{i+m_2}^1=h_{m_2}^2\}\right|$.

Замечание. *Результаты теоремы 2 легко обобщаются на случай любого количества шаблонов.*

Применим утверждение теоремы 2 для построения статистического критерия проверки гипотезы (1).

Теорема 3. *Для выборки* X *и набора различных шаблонов* $H_1,\ldots,H_M$ *принимается гипотеза* $\mathbf{H}_0$, *если*

$$S(H_1,\ldots,H_M)\le\Delta(\alpha) \qquad (2)$$

где $S(H_1,\ldots,H_M)=(W-\mu)'\Sigma^{-1}(W-\mu)$, $W=(W(H_1),\ldots,W(H_M))'$ — *вектор*

частот шаблонов, Δ — $(1-\alpha)$ квантиль распределения χ^2 с M степенями свободы, α — уровень значимости, μ, Σ определены в теореме 2.

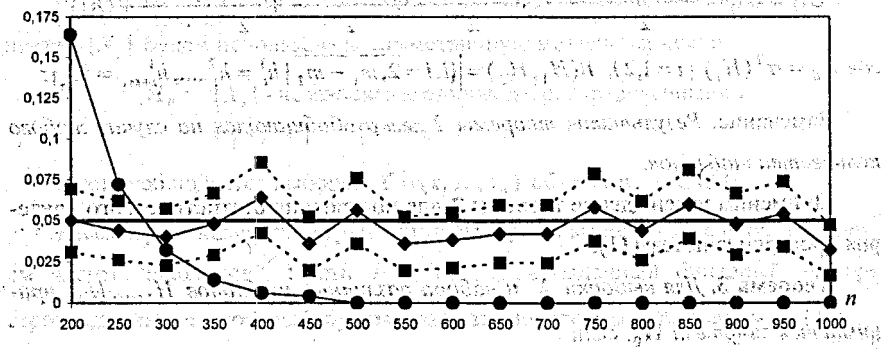
3. Вычислительный эксперимент

Для анализа свойств критерия (2) была проведена серия вычислительных экспериментов по оцениванию вероятностей ошибки первого и второго рода. Для построения критерия (2) использовалось $M=15$ шаблонов различных длин: {010111, 10, 00, 100, 0011, 11000, 0101, 01101, 1110100, 00101, 0110, 001101, 10111, 010, 1110} и α=0.05.

Оценка вероятности ошибки первого рода с 95%-доверительным интервалом вычислялась следующим образом:

$$\hat{\alpha} = N_1 / N,\ \hat{\alpha}_{\pm} = \hat{\alpha} \pm \Phi^{-1}\left((1+\gamma)/2\right)\sqrt{\hat{\alpha}(1-\hat{\alpha})/N},$$

где N_1 — число отклонений гипотезы (1) при тестировании N выборок из равномерного бинарного распределения, γ=0.95. На рисунке приведены значения оценки вероятности ошибки первого рода $\hat{\alpha}$ (обозначение ♦), доверительного интервала $\hat{\alpha}_{\pm}$ (обозначение ■) для различных объемов выборок n. На рисунке также представлена оценка вероятности ошибки второго рода при генерации выборки из несимметричного распределения Бернулли: $P\{X_t = 1\} = 0.65$, $P\{X_t = 0\} = 0.35$ (обозначение ●).



Можно видеть, что теоретическое значение уровня значимости α=0.05 попадает в 95%-доверительный интервал для оценки вероятности ошибки перво-

го родя, а оценка вероятности ошибки второго рода при увеличении длины выборки стремится к нулю.

Литература. 1. Кнут Д. Искусство программирования. Т.2. Получисленные алгоритмы. 3-е изд. – Вильямс, 2000. 2. NIST Special Publication 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000. 3. Régnier M., Szpankowski W. On The Approximate Pattern Occurrences In A Text // 1997, http://citeseer.nj.nec.com/34237.html 4. Tamhane A. C. Multiple Comparisons / Handbook of Statistics — New York: Elsevier Science, 1996.

МЕТОД ИТЕРАЦИЙ РЕШЕНИЯ ОПЕРАТОРНЫХ УРАВНЕНИЙ С АПРИОРНЫМ ВЫБОРОМ ЧИСЛА ИТЕРАЦИЙ

Панцыр В.М., Савчук В.Ф., БрГУ, г. Брест

В действительном гильбертовом пространстве решается уравнение 1 рода

$$Ax = y_\delta, \tag{1}$$

где $\|y - y_\delta\| \le \delta$ и A – ограниченный, положительный, самосопряженный оператор, для которого нуль не является собственным значением. Причем нуль принадлежит спектру оператора A, т.е. задача некорректна. Для отыскания решения уравнения (1) предлагается итеративный метод

$$x_{n+1,\delta} = (E - \alpha A)^2 x_{n,\delta} + 2\alpha y_\delta - \alpha^2 A y_\delta, \quad x_{0,\delta} = 0. \tag{2}$$

Доказана сходимость метода (2). Получены оценки погрешности метода при точной правой части, при приближенной части и погрешность в счете. Доказаны теоремы.

Теорема 1. Итерационный процесс (2) при условии $0 < \alpha < \frac{2}{\|A\|}$ сходится, если число итераций n выбирать в зависимости от δ так, что $n(\delta)\delta \to 0$ при $n \to \infty$, $\delta \to 0$.

Теорема 2. Если выполняется условие $x = A^s z, s > 0$ и $0 < \alpha \le \frac{5}{4\|A\|}$, то общая оценка погрешности для метода (2) имеет вид

$$\|x - x_{n,\delta}\| \le s^s (2n\alpha e)^{-s} \|z\| + 2n\alpha\delta.$$

Теорема 3. Оптимальная оценка погрешности для метода (2) имеет вид $\|x - x_{n,\delta}\|_{опт} \le (1+s) e^{-\frac{s}{s+1}} \|z\|^{\frac{1}{s+1}} \delta^{\frac{s}{s+1}}$ и достигается при