Лабораторна робота № 4

Тема: *АНАЛІЗ АЛГОРИТМІВ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ*

Базові статистичні ймовірнісні тести

Як базові рекомендується використовувати п'ять тестів:

- частотний (монобітний) тест;
- тест двох бітових серій;
- тест Поккера;
- тест серій (загальний);
- автокореляційний тест.

Монобітний тест.

Метою монобітного тесту є перевірка того, чи є число двійкових символів "0" та "1" в послідовності $a = a_0, a_1, \ldots, a_n$ приблизно таким, як у випадкової послідовності. Якщо n_0 є число символів "0" в послідовності, а n_1 – символів "1", то параметр ПВП

$$\chi_1 = \frac{(n_0 - n_1)^2}{n}$$

підпорядковується χ^2 розподілу з одним ступенем свободи (якщо $n > 10$).

Тест двобітових серій.

Метою тесту двобітових серій є перевірка того, чи є число з'явлень серій "00" – n_{00}, "01" – n_{01}, "10" – n_{10}, "11" – n_{11} такою, як і у випадковій послідовності. Параметр ПВП

$$\chi_2 = \frac{4}{n-1}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1$$

підпорядковується χ^2 розподілу з двома ступенями свободи (якщо $n \geq 21$).

Тест Поккера.

Нехай m – додатне ціле число, таке що

$$\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot (2^m); \;\; k = \left\lfloor \frac{n}{m} \right\rfloor.$$

Розділимо послідовність Y на k не перекриваючих частин, кожна довжиною m, нехай і буде число з'явлення послідовності довжиною m. Тест Поккера дозволяє визначити, чи дійсно послідовності довжиною m кожна приблизно з'являються стільки ж разів, скільки очікується у випадковій послідовності. Параметр

$$\chi_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k$$

підпорядковується χ^2 розподілу з $2^m - 1$ ступенями свободи.

Зазначимо, що тест Поккера є узагальненням частотного тесту – при $m = 1$ співпадає з частотним.

Тест серій.

Тест серій дозволяє визначити, чи дійсно число нулів або одиниць (серії) різної довжини в послідовності Y такі ж як і у випадковій послідовності. Бажане число інтервалів довжиною i у випадковій послідовності n є

$$l_i = (n - i + 3)/2^{i+2}.$$

Нехай k буде рівним найбільшому цілому числу i, для якого $l_i \geq 5$. Нехай також B та G буде числом блоків та інтервалів відповідно довжиною i в Y для кожного i, $1 \leq i \leq k$. Тоді параметр

$$\chi_4 = \sum_{i=1}^{k} \frac{(B_i - l_i)^2}{l_i} + \sum_{i=1}^{k} \frac{(G_i - l_i)^2}{l_i}$$

підпорядковується χ^2 розподілу з $2k-2$ ступенями свободи.

Автокореляційний тест.

Метою автокореляційного тесту є перевірка ступеня зв'язку між Y_v і її зсувами. Нехай d фіксоване ціле число, $1 \leq d \leq \lfloor n/2 \rfloor$. Число бітів у Y послідовності дорівнює

$$R(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d}.$$

Статистика параметра $\chi_5 = 2\left(R(d) - \frac{n-d}{2} \right) \Big/ \sqrt{n-d}$ приблизно підпорядковується $N(0,1)$ нормальному розподілу, якщо $n - d \geq 10$. Автокореляційний метод має бути двостороннім, щоб розглядати його як для малих значень $R(d)$, так і для великих.

4.3 Приклади розв'язку задач

Задача 1.

Розглянемо послідовність Y довжиною n=160, яку сформуємо із чотирьох 40 бітових послідовностей Y_0.

Y_0=11100 01100 01000 10100 11101 11100 10010 01001.

1. Частотний (монобітний тест)

$$n_0 = 21 \cdot 4 = 84, \qquad n_1 = 19 \cdot 4 = 76.$$

$$\chi_1 = \frac{(84 - 76)^2}{160} = 0{,}4.$$

2. Двобітовий тест

$$n_{00}=44;\ \ n_{01}=40;\ \ n_{10}=40;\ \ n_{11}=35.$$

$$\chi_2=\frac{4}{159}(44^2+40^2+40^2+35^2)-\frac{2}{160}(84^2+76^2)+1=0{,}62.$$

3. Тест Поккера

Нехай m=3 і k=53. Блоки 000, 001, 010, 011, 100, 101, 110, 111 з'являються відповідно 5, 10, 6, 4, 12, 3, 6 та 7 разів. Значення параметра

$$\chi_3=\frac{2^3}{53}\left(5^2+10^2+6^2+4^2+12^2+3^2+6^2+7^2\right)-53=9{,}6415.$$

4. Тест серій

$$l_i=(n-i+3)/2^{i+2};$$

$$l_1=(160-1+3)/2^3=20{,}25;$$

$$l_2=(160-2+3)/2^4=10{,}0625;$$

$$l_3=(160-3+3)/2^5=5.$$

Є 25, 4 та 5 блоків довжиною 1, 2, 3 відповідно, 8, 20 та 12 інтервалів довжиною 1, 2 та 3 відповідно. Параметр χ_4 приймає значення $\chi_4=31{,}7913$.

5. Автокореляційний тест.

Якщо d=8, то $R(8)$=100.

Значення статистичного параметра

$$\chi_5=\left(2\left(100-\frac{160-8}{2}\right)\right)\Big/\sqrt{160-8}=3{,}8933.$$

Для рівня значущості $\alpha=0{,}05$ порогові значення χ_1, χ_2, χ_3, χ_4 та χ_5 дорівнюють 3.8415, 5.9915, 14.0671, 9.4877, 1.96 відповідно.

Бачимо, що послідовність проходить частотний (монобітний) тест, двобітовий тест та тест Поккера, але не проходить тест серій та автокореляційний тест.

Задачі для самостійного розв'язання

1. Федеральним стандартом США FIPS – 140 – 1, 140 – 2 використовуються 4 статистичні тести на випадковість. Замість вибору користувачами потрібних рівнів значущості задаються реальні границі. Довжина бітової послідовності 20000 бітів. Проведіть аналіз цього стандарту.

Монобітний тест. Кількість n_0 та n_1, $9654<n_i<10346$.

Тест Поккера. Статистичний параметр χ_3 обчислюється для m=4; тест виконується, якщо $1{,}03<\chi_3<57{,}4$.

Тест серій. Тести проходять, якщо кожний із 12 номерів B_i та G_i, $1\le i\le 6$, знаходиться в інтервалі згідно з табл. 4.1.

Таблиця 4.1 – Значення інтервалів

Довжина серії	Відповідний інтервал
1	2267 – 2733
2	1079 – 1421
3	502 – 748
4	223 – 402
5	90 – 223
6	90 – 223

Тест довжин серій. Цей тест проходить, якщо не існує ніяких серій довжиною 34 або більше. Для високозахищених застосувань FIPS – 140 – 1 зобов'язує, щоб 4 тести виконувалися при кожній ініціалізації генератора випадкових бітів. В FIPS-140-2 максимальна довжина серії збільшена до 36 бітів.

2. Необхідно розробити такі процедури мовою С++ або іншою мовою:

а) генерація псевдовипадкової послідовності довільної довжини з використанням лінійного рекурентного регістру, закон генерації якої визначається відповідно до примітивних поліномів, наведених в табл. 4.2;

Таблиця 4.2 – Примітивні поліноми

№ п/п	1	2	3	4	5
1	$x^{31}+x^3+1$	$x^{61}+x+1$	$x^{95}+x^{11}+1$	$x^{127}+x^{63}+1$	$x^{31}+x^3+1$
2	x^6+x+1	x^7+x+1	x^9+x^4+1	$x^{10}+x^3+1$	x^5+x^2+1
№ п/п	6	7	8	9	10
1	$x^{168}+x^{15}+1$	$x^{63}+x^5+1$	$x^{47}+x^5+1$	$x^{257}+x^{52}+1$	$x^{52}+x^{21}+1$
2	x^9+x^5+1	x^7+x^3+1	$x^{10}+x^7+1$	x^6+x^5+1	x^5+x^3+1

б) реалізація монобітного тесту згідно з вищесказаною теорією для довільної довжини послідовності;

в) реалізація тесту Поккера згідно з вищесказаною теорією для довільної довжини послідовності;

г) реалізація тесту серій згідно з вищесказаною теорією для довільної довжини послідовності;

д) реалізація тесту довгих серій згідно з вищесказаною теорією для довільної довжини послідовності.

3. Розв'язати задачі 2 (а-д) з використанням ЕОМ при довжині послідовності $l = 2 \cdot 10^4$ бітів.

4. Розв'яжіть задачу 1 пункту 1.10.2, якщо псевдовипадкова послідовність довжиною n=128 бітів побудована шляхом чотириразового повторення такої 32-бітової послідовності:

$$S=\{0110\ 0100\ 0111\ 1010\ 1100\ 1000\ 1111\ 0101\}.$$

Відповідь: (χ_1=0,5; χ_2=2,295; χ_3=1,048; χ_4=5,99; χ_5=0,18).

Контрольні запитання та завдання

1. Поясніть алгоритм функціонування генератора псевдовипадкових послідовностей

2. Назвіть основні показники оцінки властивостей генератора псевдовипадкових послідовностей.

3. Визначте період повторення лінійної рекурентної послідовності, якщо m={7, 10, 12, 19, 31, 63, 89, 127, 257, 52}.

4. Визначте структурну скритність лінійної рекурентної послідовності періоду $L = 2^m - 1$.

5. Визначте значення безпечного часу, якщо в генератор псевдовипадкової послідовності може бути введено N_k (10^{20}, 10^{25}, 10^{30}, 10^{35}, 10^{40}, 10^{50}, 10^{70}, 10^{80}, 10^{90}, 10^{100}, 10^{127}) ключів.

6. Визначте структурну скритність лінійної рекурентної послідовності періоду $L = 2^m - 1$, m=20, 25, 30, 35, 40, 61, 63, 85, 89, 127, 257, 507.

7. Поясніть сутність:
- монобітного тесту;
- тесту двобітових серій;
- тесту Поккера;
- тесту серій;
- автокореляційного тесту.

8. Поясніть вихідний код процедури реалізації:
- монобітного тесту;
- тесту двобітових серій;
- тесту Поккера;
- тесту серій;
- автокореляційного тесту.

9. Дайте визначення лінійного конгруентного генератора.

10. Які вимоги висуваються до коефіцієнтів a та b рекурентного співвідношення, що визначає алгоритм функціонування лінійного конгруентного генератора.

11. За яких умов лінійний конгруентний генератор забезпечує максимальний період формувальної послідовності.

12. Зробіть пропозиції щодо реалізації та виберіть параметри конгруентного генератора, що забезпечує максимальний період послідовності.

13. Зробіть пропозиції щодо реалізації та виберіть параметри конгруентного генератора, що забезпечує максимальний період послідовності.