Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЗВІТ ДО КОМП’ЮТЕРНОГО ПРАКТИКУМУ № 1

Побудова тестів для перевірки якості випадкових та псевдовипадкових послідовностей

Виконали:
студенти ФІ-94
Музиченко О.
Скоробагатько М.

Перевірив:
Якимчук О.

Київ – 2022

1.Мета роботи

Вивчення критеріїв згоди і набуття навичок у побудові та застосуванні тестів для перевірки статистичних властивостей бінарних випадкових і псевдовипадкових послідовностей, ознайомлення з поняттям *M*-послідовності.

2. Постановка задачі:

1. Написати програми, які реалізують генератори псевдовипадкових бітів, наведені у розділі 2.3 теоретичних відомостей, а саме:
1) вбудований генератор вашої мови програмування;
2) генератор LehmerLow;
3) генератор LehmerHigh;
4) генератор L20;
5) генератор L89;
6) генератор Джиффі (Geffe);
7) генератор «Бібліотекар»;
8) генератор Вольфрама;
9) генератор Блюма-Мікалі BM;
10) генератор BM_bytes (байтова модифікація генератору Блюма-Мікалі);
11) генератор BBS;
12) генератор BBS_bytes (байтова модифікація генератору BBS).
2. Розробити програми для реалізації трьох тестів перевірки якості двійкових послідовностей: про рівноімовірність розподілу, про незалежність і про однорідність (див. розділ 2.4 теоретичних відомостей). Програми повинні враховувати можливості введення випробовуваної послідовності різної довжини із зазначених датчиків, а також із зовні заданого файлу, можливості задавати різні значення рівня значимості α (обов’язково: 0,01;0,05;0,1 , інші значення за бажанням).
У програмі повинне бути передбачене відображення на екрані комп'ютера результатів обробки послідовності, що перевіряється тестами, із зазначенням вхідних даних послідовності (її довжини, датчиків, що її генерують чи зовнішнього файлу), обраних значень α, обчислених та теоретичних значень χ^2 і висновку (у яких випадках послідовності відкидаються чи приймаються зазначеними критеріями).

3. Провести обробку трьома побудованими тестами прикладів послідовностей, згенерованих зазначеними датчиками, для значень $\alpha = 0{,}01; 0{,}05; 0{,}1$. Пам’ятайте, що для одержання статистично достовірних даних ваша послідовність повинна містити щонайменше мільйон бітів (краще декілька мільонів).

Хід роботи:

1) Написали класи генераторів. Кожен з генераторів має функцію generate_byte(), тому незалежно від того, що саме генерує генератор (біти чи байти), повертаються все одно байти.
2) Написали реалізацію кожного з 3 зазначених тестів.
3) Провели обробку послідовностей, отриманих з кожного з генераторів кожним з трьох тестів для трьох рівнів значущості (значень $\alpha = 0{,}01; 0{,}05; 0{,}1$)
4) Для тестів використовували послідовності довжиною 2^{20} байт (1048576) або ж 8388608 біт.
   Труднощі виникали із пошуком тексту з потрібним кодуванням для шифру Бібліотекар. Оскільки більшість текстів все одно містили символи, які виходять за один байт, було принято рішення брати кодування усіх символів за модулем 256

Результати досліджень:

Python_default

```
PythonGen
test_check_equlity  0.01    True    298.47340400000013  307.53633180797567
test_check_equlity  0.05    False   298.47340400000013  292.14602484235235
test_check_equlity  0.1 False   298.47340400000013  283.94150914735457
test_check_independ 0.01    True    -2509623265.540261  65077.536331807976
test_check_independ 0.05    True    -2509623265.540261  65062.146024842354
test_check_independ 0.1 True    -2509623265.540261  65053.94150914736
test_check_homog    0.01    True    -8447784719.365603  90067.53633180798
test_check_homog    0.05    True    -8447784719.365603  90052.14602484235
test_check_homog    0.1 True    -8447784719.365603  90043.94150914735
```

LehmerLow

```
LehmerLowGen
test_check_equlity  0.01    False   124254.55276399996  307.53633180797567
test_check_equlity  0.05    False   124254.55276399996  292.14602484235235
test_check_equlity  0.1 False   124254.55276399996  283.94150914735457
test_check_independ 0.01    True    -1001296044.8463132 65077.536331807976
test_check_independ 0.05    True    -1001296044.8463132 65062.146024842354
test_check_independ 0.1 True    -1001296044.8463132 65053.94150914736
test_check_homog    0.01    True    -5313705301.726484  90067.53633180798
test_check_homog    0.05    True    -5313705301.726484  90052.14602484235
test_check_homog    0.1 True    -5313705301.726484  90043.94150914735
```

LehmerHigh

```
LehmerHighGen
test_check_equlity  0.01    False   124245.12876399998  307.53633180797567
test_check_equlity  0.05    False   124245.12876399998  292.14602484235235
test_check_equlity  0.1 False   124245.12876399998  283.94150914735457
test_check_independ 0.01    True    -1001921272.7267088 65077.536331807976
test_check_independ 0.05    True    -1001921272.7267088 65062.146024842354
test_check_independ 0.1 True    -1001921272.7267088 65053.94150914736
test_check_homog    0.01    True    -5303705230.927832  90067.53633180798
test_check_homog    0.05    True    -5303705230.927832  90052.14602484235
test_check_homog    0.1 True    -5303705230.927832  90043.94150914735
```

L20

```
L20Gen
test_check_equlity  0.01    True    253.78578800000048  307.53633180797567
test_check_equlity  0.05    True    253.78578800000048  292.14602484235235
test_check_equlity  0.1 True    253.78578800000048  283.94150914735457
test_check_independ 0.01    True    -2560438672.2947345 65077.536331807976
test_check_independ 0.05    True    -2560438672.2947345 65077.536331807976
test_check_independ 0.1 True    -2560438672.2947345 65053.94150914736
test_check_homog    0.01    True    -8464909865.840063  90067.53633180798
test_check_homog    0.05    True    -8464909865.840063  90052.14602484235
test_check_homog    0.1 True    -8464909865.840063  90043.94150914735
```

L89

```
L89Gen
test_check_equlity  0.01    True    232.1980760000002   307.53633180797567
test_check_equlity  0.05    True    232.1980760000002   292.14602484235235
test_check_equlity  0.1 True    232.1980760000002   283.94150914735457
test_check_independ 0.01    True    -2522435055.4425025 65077.536331807976
test_check_independ 0.05    True    -2522435055.4425025 65062.146024842354
test_check_independ 0.1 True    -2522435055.4425025 65053.94150914736
test_check_homog    0.01    True    -8485285012.411412  90067.53633180798
test_check_homog    0.05    True    -8485285012.411412  90052.14602484235
test_check_homog    0.1 True    -8485285012.411412  90043.94150914735
```

Geffe

```
GeffeGen
test_check_equlity  0.01    False   56755.91046000001   307.53633180797567
test_check_equlity  0.05    False   56755.91046000001   292.14602484235235
test_check_equlity  0.1 False   56755.91046000001   283.94150914735457
test_check_independ 0.01    True    -182747695.51968867 65077.536331807976
test_check_independ 0.05    True    -182747695.51968867 65062.146024842354
test_check_independ 0.1 True    -182747695.51968867 65053.94150914736
test_check_homog    0.01    True    -7784926953.273764  90067.53633180798
test_check_homog    0.05    True    -7784926953.273764  90052.14602484235
test_check_homog    0.1 True    -7784926953.273764  90043.94150914735
```

Librarian

```
LibGen
test_check_equlity  0.01    False   1679081.1004760007  307.53633180797567
test_check_equlity  0.05    False   1679081.1004760007  292.14602484235235
test_check_equlity  0.1 False   1679081.1004760007  283.94150914735457
test_check_independ 0.01    True    -99110531.53616562  65077.536331807976
test_check_independ 0.05    True    -99110531.53616562  65062.146024842354
test_check_independ 0.1 True    -99110531.53616562  65053.94150914736
test_check_homog    0.01    True    -1597201667.6594684 90067.53633180798
test_check_homog    0.05    True    -1597201667.6594684 90052.14602484235
test_check_homog    0.1 True    -1597201667.6594684 90043.94150914735
```

Wolfram

```
WolframGen
test_check_equlity  0.01    False   7067897.679291999   307.53633180797567
test_check_equlity  0.05    False   7067897.679291999   292.14602484235235
test_check_equlity  0.1 False   7067897.679291999   283.94150914735457
test_check_independ 0.01    True    -125005.99966400847 65077.536331807976
test_check_independ 0.05    True    -125005.99966400847 65062.146024842354
test_check_independ 0.1 True    -125005.99966400847 65053.94150914736
test_check_homog    0.01    True    -133123623.51969133 90067.53633180798
test_check_homog    0.05    True    -133123623.51969133 90052.14602484235
test_check_homog    0.1 True    -133123623.51969133 90043.94150914735
```

BM

```
BMGen
test_check_equlity  0.01    True    286.3388760000001   307.53633180797567
test_check_equlity  0.05    True    286.3388760000001   292.14602484235235
test_check_equlity  0.1 False   286.3388760000001   283.94150914735457
test_check_independ 0.01    True    -2515935143.9814925 65077.536331807976
test_check_independ 0.05    True    -2515935143.9814925 65062.146024842354
test_check_independ 0.1 True    -2515935143.9814925 65053.94150914736
test_check_homog    0.01    True    -8485660323.684333  90067.53633180798
test_check_homog    0.05    True    -8485660323.684333  90052.14602484235
test_check_homog    0.1 True    -8485660323.684333  90043.94150914735
```

BBS

```
BBSGen
test_check_equlity  0.01    True    254.70342000000036  307.53633180797567
test_check_equlity  0.05    True    254.70342000000036  292.14602484235235
test_check_equlity  0.1 True    254.70342000000036  283.94150914735457
test_check_independ 0.01    True    -2514434788.000359  65077.536331807976
test_check_independ 0.05    True    -2514434788.000359  65062.146024842354
test_check_independ 0.1 True    -2514434788.000359  65053.94150914736
test_check_homog    0.01    True    -8488410471.029903  90067.53633180798
test_check_homog    0.05    True    -8488410471.029903  90052.14602484235
test_check_homog    0.1 True    -8488410471.029903  90043.94150914735
```

Таблиці результатів:

Generator	Test	Alpha	Passed	χ^2	Critical χ^2
Python default	check_equlity	0.01	+	298.47340400000013	307.53633180797567
		0.05	-	298.47340400000013	307.53633180797567

		0.1	-	298.47340400000013	283.94150914735457
	check_independ	0.01	+	-2509623265.540261	65077.536331807976
		0.05	+	-2509623265.540261	65062.146024842354
		0.1	+	-2509623265.540261	65053.94150914736
	check_homog	0.01	+	-8447784719.365603	90067.53633180798
		0.05	+	-8447784719.365603	90052.14602484235
		0.1	+	-8447784719.365603	90043.94150914735
LehmerLow	check_equlity	0.01	-	124254.55276399996	307.53633180797567
		0.05	-	124254.55276399996	292.14602484235235
		0.1	-	124254.55276399996	283.94150914735457
	check_independ	0.01	+	-1001296044.8463132	65077.536331807976
		0.05	+	-1001296044.8463132	65062.146024842354
		0.1	+	-1001296044.8463132	65053.94150914736
	check_homog	0.01	+	-5313705301.726484	90067.53633180798
		0.05	+	-5313705301.726484	90052.14602484235
		0.1	+	-5313705301.726484	90043.94150914735
LehmerHigh	check_equlity	0.01	-	124245.12876399998	307.53633180797567
		0.05	-	124245.12876399998	292.14602484235235
		0.1	-	124245.12876399998	283.94150914735457
	check_independ	0.01	+	-1001921272.7267088	65077.536331807976
		0.05	+	-1001921272.7267088	65062.146024842354
		0.1	+	-1001921272.7267088	65053.94150914736
	check_homog	0.01	+	-5303705230.927832	90067.53633180798

		0.05	+	-5303705230.927832	90052.14602484235
		0.1	+	-5303705230.927832	90043.94150914735
L20	check_equlity	0.01	+	253.78578800000048	307.53633180797567
		0.05	+	253.78578800000048	292.14602484235235
		0.1	+	253.78578800000048	283.94150914735457
	check_independ	0.01	+	-2560438672.2947345	65077.536331807976
		0.05	+	-2560438672.2947345	65077.536331807976
		0.1	+	-2560438672.2947345	65053.94150914736
	check_homog	0.01	+	-8464909865.840063	90067.53633180798
		0.05	+	-8464909865.840063	90052.14602484235
		0.1	+	-8464909865.840063	90043.94150914735
L89	check_equlity	0.01	+	232.1980760000002	307.53633180797567
		0.05	+	232.1980760000002	292.14602484235235
		0.1	+	232.1980760000002	283.94150914735457
	check_independ	0.01	+	-2522435055.4425025	65077.536331807976
		0.05	+	-2522435055.4425025	65062.146024842354
		0.1	+	-2522435055.4425025	65053.94150914736
	check_homog	0.01	+	-8485285012.411412	90067.53633180798
		0.05	+	-8485285012.411412	90052.14602484235
		0.1	+	-8485285012.411412	90043.94150914735
	check_equlity	0.01	-	56755.91046000001	307.53633180797567
		0.05	-	56755.91046000001	292.14602484235235

Geffe					
		0.1	-	56755.91046000001	283.94150914735457
	check_independ	0.01	+	-182747695.51968867	65077.536331807976
		0.05	+	-182747695.51968867	65062.146024842354
		0.1	+	-182747695.51968867	65053.94150914736
	check_homog	0.01	+	-7784926953.273764	90067.53633180798
		0.05	+	-7784926953.273764	90052.14602484235
		0.1	+	-7784926953.273764	90043.94150914735
Librarian	check_equlity	0.01	-	1679081.1004760007	307.53633180797567
		0.05	-	1679081.1004760007	292.14602484235235
		0.1	-	1679081.1004760007	283.94150914735457
	check_independ	0.01	+	-99110531.53616562	65077.536331807976
		0.05	+	-99110531.53616562	65062.146024842354
		0.1	+	-99110531.53616562	65053.94150914736
	check_homog	0.01	+	-1597201667.6594684	90067.53633180798
		0.05	+	-1597201667.6594684	90052.14602484235
		0.1	+	-1597201667.6594684	90043.94150914735
Wolfram	check_equlity	0.01	-	7067897.679291999	307.53633180797567
		0.05	-	7067897.679291999	292.14602484235235
		0.1	-	7067897.679291999	283.94150914735457
	check_independ	0.01	+	-125005.99966400847	65077.536331807976
		0.05	+	-125005.99966400847	65062.146024842354
		0.1	+	-125005.99966400847	65053.94150914736

	check_homog	0.01	+	-133123623.51969133	90067.53633180798
		0.05	+	-133123623.51969133	90052.14602484235
		0.1	+	-133123623.51969133	90043.94150914735
BM	check_equlity	0.01	+	286.3388760000001	307.53633180797567
		0.05	+	286.3388760000001	292.14602484235235
		0.1	-	286.3388760000001	283.94150914735457
	check_independ	0.01	+	-2515935143.9814925	65077.536331807976
		0.05	+	-2515935143.9814925	65062.146024842354
		0.1	+	-2515935143.9814925	65053.94150914736
	check_homog	0.01	+	-8485660323.684333	90067.53633180798
		0.05	+	-8485660323.684333	90052.14602484235
		0.1	+	-8485660323.684333	90043.94150914735
BBS	check_equlity	0.01	+	254.70342000000036	307.53633180797567
		0.05	+	254.70342000000036	292.14602484235235
		0.1	+	254.70342000000036	283.94150914735457
	check_independ	0.01	+	-2514434788.000359	65077.536331807976
		0.05	+	-2514434788.000359	65062.146024842354
		0.1	+	-2514434788.000359	65053.94150914736
	check_homog	0.01	+	-8488410471.029903	90067.53633180798
		0.05	+	-8488410471.029903	90052.14602484235
		0.1	+	-8488410471.029903	90043.94150914735

Висновки:

У даній лабораторній роботі ми запрограмували генератор LehmerLow, генератор LehmerHigh, генератор L20, генератор L89, генератор Geffe , генератор «Бібліотекар» , генератор Вольфрама, генератор BM, генератор BM_bytes, генератор BBS, генератор BBS_bytes та перевірили їх на послідовностях довжини довжиною 2^{20} байт (1048576) або ж 8388608 біт. По таблиці можемо побачити, що такі генератори як PythonDefault, LehmerHigh, GeneratorL20, GeneratorL89, GeneratorBM, а також GeneratorBM(bits) можна рекомендувати для використання у криптографії.

Вихідний код програми виконання можна знайти за посиланням.