The Evaluation of Randomness of RPG100 by Using NIST and DIEHARD Tests

FDK CORPORATION
RPG Business Promotion Dept
16/12/2003

Introduction

The RPG100 generated random numbers are tested by means of two popular randomness tests. One is the Special Publication 800-22 issued by the National Institute of Standards and Technology (NIST) [1] and the other is the DIEHARD test provided by Dr. Marsaglia. It is impossible to comment the randomness of a bit sequence with a single bit sample, so we performed the above two tests many times to a 1G bits data with distinct bit samples. The randomness of RPG100 is checked by validity of test passing ratio and uniformity of P-Value of the test samples.

The tested random digits were generated at 250Kbps form a single sample of RPG100 with the conditions of 3.3 Volts at 25 Degrees Celsius.

1． N I S T Special Publication 800-22 Random Number Test

NIST Special Publication 800-22 was issued by National Institute of Standards and Technology [1] in May 15, 2001. A random bit sequence of 1M bits should be considered for the test, so we performed the tests 1000 times with 1M bits distinct samples.

1-1. The sort of test and its parameters

NIST SP800-22 has mentioned 16 tests and their significance levels are considered as 1% as well as some of the test need to be adjusted their parameter settings. The test name and its parameters are shown in the following table. A report, which is issued by the Information-technology Promotion Agency Japan, selects the minimum set from many tests so we mark tests that are in minimum set [2]. There are two tests called Lempel-Ziv Compression Test and Discrete Fourier Transform (Spectral) Test whose statistical distribution is derived from expected ones. So P-Value of this test is not uniform even if the test sequence is perfectly random and the significance level of this test is not 1% ([3], [4] and p40 in [2]), so we ignore results of these two tests.

Test Name (＊ denotes minimum set)	Test Parameter
Frequency (Monobit) Test	—
＊Frequency Test within a Block	m = 20000
Runs Test	—
＊Test for the Longest Run of Ones in a Block	M = 10000
Binary Matrix Rank Test	—

~~Discrete Fourier Transform (Spectral) Test~~	—
Non-overlapping Template Matching Test	m = 9, B = 000000001
Overlapping Template Matching Test	m = 9
Maurer's "Universal Statistical" Test	L = 7, Q = 1280
~~Lempel-Ziv Compression Test~~	—
＊Linear Complexity Test	M = 500
＊Serial Test	m = 5, $\nabla\Psi^2$
Approximate Entropy Test	m = 5
＊Cumulative Sums (Cusum) Test	Forward
Random Excursions Test	X = +3, -3
Random Excursions Variant Test	X = +3, -3

In Random Excursions Test and Random Excursions Variant Test, the test is stopped if the number of cycles in random walk is J < 500. Therefore, lesser frequencies come for these two tests than 1000 times even if NIST SP800-22 is tested 1000 distinct bit samples (Theoretically, probability of stopping the tests is 38 %). For unification of number of test sample to 1000; for these two test P-Value of 500 is used X=+3 together with that of X=-3.

1-2. Passing Ratio of Each Test

The significance level of each test in NIST SP800-22 is set to 1% and it means that 99% of test samples pass the tests if random numbers are truly random. We valuate the passing ratio of test with 1000 samples. When the number of samples are n and the probability of passing each test is p, then the number of samples that pass the test x follows binomial distribution. If n is large (np>>1), x follows normal distribution with the expected value $m = np$ and with the standard deviation $\sigma = \sqrt{np(1-p)}$. Considering $z \equiv (x-m)/\sigma$, z follows standard normal distribution with the expected value zero and the standard deviation one. Expressing x by using z is $x = m + z\sigma$, and divide by n,

$$p' \equiv x/n = p + z\sqrt{p(1-p)/n} \tag{1}$$

Where p' is the observed ratio that pass the test. The range of acceptable ratio that is recommended by NIST is $-3 \leqq z \leqq +3$ and this is the test with significance level 0.27%. The probability is p=0.99 and the number of samples tested are n=1000, then the acceptance region of the passing ratio is

$$p' = 0.99 \pm 3 \times \sqrt{0.99 \times 0.01/1000} = 0.99 \pm 0.0094392 \quad . \tag{2}$$

Test Sample n=1000　Acceptance Region $0.980561 \leqq p' \leqq 0.999439$

Test Name　(＊denotes minimum set)	p'	Result
Frequency (Monobit) Test	0.994	SUCCESS
＊Frequency Test within a Block	0.983	SUCCESS
Runs Test	0.992	SUCCESS
＊Test for the Longest Run of Ones in a Block	0.989	SUCCESS

Binary Matrix Rank Test	0.989	SUCCESS
Non-overlapping Template Matching Test	0.993	SUCCESS
Overlapping Template Matching Test	0.988	SUCCESS
Maurer's "Universal Statistical" Test	0.991	SUCCESS
＊Linear Complexity Test	0.991	SUCCESS
＊Serial Test	0.989	SUCCESS
Approximate Entropy Test	0.991	SUCCESS
＊Cumulative Sums (Cusum) Test	0.985	SUCCESS
Random Excursions Test	0.990	SUCCESS
Random Excursions Variant Test	0.995	SUCCESS

1-3. P-Value's Uniformity of Each Test

If the test sequences are truly random, P-Value is expected to appear uniform in [0,1). NIST recommends to χ^2 test by interval between 0 and 1 is divided into 10 sub-intervals. This is the test of uniformity of P-Value. The degree of freedom is 9 in this case. Define F_i as number of occurrence of P-Value in i th interval, then χ^2 statistics is given as bellow.

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - n/10)^2}{n/10} \tag{3}$$

NIST recommends to set it's significance level as 0.01%, and the acceptance region of statistics is $\chi^2 \le 33.72$.

Acceptance Region $\chi^2 \le 33.72$

Test Name （＊denotes minimum set）	χ^2	Result
Frequency (Monobit) Test	5.20	SUCCESS
＊Frequency Test within a Block	10.51	SUCCESS
Runs Test	2.64	SUCCESS
＊Test for the Longest Run of Ones in a Block	10.33	SUCCESS
Binary Matrix Rank Test	17.84	SUCCESS
Non-overlapping Template Matching Test	5.18	SUCCESS
Overlapping Template Matching Test	9.40	SUCCESS
Maurer's "Universal Statistical" Test	20.53	SUCCESS
＊Linear Complexity Test	13.87	SUCCESS
＊Serial Test	9.978	SUCCESS
Approximate Entropy Test	14.02	SUCCESS
＊Cumulative Sums (Cusum) Test	4.67	SUCCESS
Random Excursions Test	5.64	SUCCESS
Random Excursions Variant Test	6.18	SUCCESS

1-4. Passing ratio of Total Test

This is a valuation of passing ratio of total test samples. The method is same as 1-2 except number of sample that n=14000. From equation (1), the acceptance region of p' is

$$p' = 0.99 \pm 3 \times \sqrt{0.99 \times 0.01 / 14000} = 0.99 \pm 0.0025228 \quad . \tag{4}$$

Test Sample n=14000　Acceptance Region 0.987477≦p'≦0.992523

Test Name	p'	Result
NIST SP800-22	0.990	SUCCESS

1-5. P-Value's Uniformity of Total Test

This is a valuation of P-value's uniformity of total test samples. The method is same as 1-3 except number of samples that n=14000. The statistics is given by equation (3).

Acceptance Region　$\chi^2 \leq 33.72$

Test Name	χ^2	Result
NIST SP800-22	12.85	SUCCESS

２．DIEHARD　Test

This test is provided by Dr. Marsaglia who with the Florida State University [5]. The DIEHARD is composed of 18 tests and that out put P-Value range［０，１）if the test sequence is truly random. This test doesn't have acceptance region but NIST SP800-22. The DIEHARD needs 80Mbit sequence and we test it 12 times.

2-1. The sort of test and number of P-Value

The DIEHARD has 18 tests and each test has some P-value. The number of P-Value is different between each test. The sort of test and its P-value is in following table. There are 220 P-value in a set of DIEHARD so that total number of P-Value is 2640 because we test 12 times.

Test Name　（＊denotes minimum set）	Number of P-Value
＊The Birthday Spacings Test	１０
＊The Overlapping 5-Permutation Test	２
The Binary Rank Test for 31x31 Matrices	１
The Binary Rank Test for 32x32 Matrices	１
The Binary Rank Test for 6x8 Matrices	２６
＊The Bitstream Test	２０
＊The Overlapping-Pairs-Sparse-Occupancy Test	２３

＊The Overlapping-Quadruples-Sparse -Occupancy Test	2 8
The DNA Test	3 1
＊Count-The-1's Test on a Stream of Bytes	2
＊Count-The-1's Test for Specific Bytes	2 5
The Parking Lot Test	1 1
The Minimum Distance Test	1
The 3D-Spheres Test	2 1
The Squeeze Test	1
The Overlapping Sums Test	1 1
The Runs Test	4
The Craps Test	2

2-3. Passing ratio of Total Test

We set the significance level of each test as 1% like NIST and valuate the passing ratio of total test samples. The number of sample is n=2640. The acceptance region of passing ratio p' is from equation (1) then

$$p' = 0.99 \pm 3 \times \sqrt{0.99 \times 0.01 / 2640} = 0.99 \pm 0.0058094 \quad . \tag{5}$$

Test Sample n=2640　Acceptance Region 0.984191≦p'≦0.995809

Test Name	p'	Result
DIEHARD	0.989	SUCCESS

Next, we set the significance level of each test as 5% its acceptance region is 0.025≦P-Value≦0.975. The acceptance region of passing ratio p' is from equation (1) then

$$p' = 0.95 \pm 3 \times \sqrt{0.95 \times 0.05 / 2640} = 0.95 \pm 0.0127252 \quad . \tag{6}$$

Test Sample n=2640　Acceptance Region 0.937275≦p'≦0.962725

Test Name	p'	Result
DIEHARD	0.950	SUCCESS

2-4. P-Value's Uniformity of Total Test

This is a valuation of P-value's uniformity of total test samples. The method is same as 1-3 except number of sample that n=2640. The statistics is given by equation (3).

Acceptance Region　$\chi^2 \leq 33.72$

Test Name	χ^2	Result
DIEHARD	4.57	SUCCESS

３．Summary

We tested 1Gbit random digit sequence by NIST 800-22 and DIEHARD then checked the ratio of passing tests and uniformity of P-value. The significance level of checking passing ratio is 0.27%, and that for uniformity of P-Value is 0.01%. There are no failures in this valuation, so that we conclude about the random digits from RPG100 have good randomness.

REFERENCES

[1] NIST, Special Publication 800-22, "A STASTICAL TEST SUITE FOR RANDOM AND PSEUDO-RANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIC APPLICATIONS", 2001. (http://csrc.nist.gov/rng/)

[2] IPA, 調査報告書,"疑似乱数検証ツールの調査開発", 2003. (http://www.ipa.go.jp/security/fy14/crypto/pseudo_rundum/rundum_inve.pdf)

[3] G. Louchard and W. Szpankowski, "On the average redundancy rate of the Lempel-Ziv code", *IEEE Trans. on Inform. Theory*, Vol. 43, No. 1, 1997.

[4] S. KIM, K. UMENO, A. HASEGAWA, "On the NIST Statistical Test Suite for Randomness" ,IEICE Technical Report,Vol.103, No.449, pp21-27, 2003.

[5] G. Marsaglia, "DIEHARD". (http://stat.fsu.edu/~geo/diehard.html)