

Diehard-Test PRG260 XOR3 (PTG.2)

IBB, 14.04.2014

```

BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA= 2.0000
  xor3.rnd      using bits 1 to 24 p-value= .782865
  xor3.rnd      using bits 2 to 25 p-value= .948424
  xor3.rnd      using bits 3 to 26 p-value= .763257
  xor3.rnd      using bits 4 to 27 p-value= .943083
  xor3.rnd      using bits 5 to 28 p-value= .856005
  xor3.rnd      using bits 6 to 29 p-value= .293713
  xor3.rnd      using bits 7 to 30 p-value= .767240
  xor3.rnd      using bits 8 to 31 p-value= .156810
  xor3.rnd      using bits 9 to 32 p-value= .604901

```

```

The 9 p-values were
.782865 .948424 .763257 .943083 .856005
.293713 .767240 .156810 .604901
A KSTEST for the 9 p-values yields .919124

```

```

-----
      OPERM5 test for file xor3.rnd
chisquare for 99 degrees of freedom= 87.126; p-value= .202511
      OPERM5 test for file xor3.rnd
chisquare for 99 degrees of freedom= 90.988; p-value= .295247
-----

```

```

Binary rank test for xor3.rnd
  Rank test for 31x31 binary matrices:
  rows from leftmost 31 bits of each 32-bit integer
  rank  observed  expected (o-e)^2/e  sum
  28      223      211.4   .634489   .634
  29     5149     5134.0  .043765   .678
  30     23169    23103.0  .188279   .867
  31     11459    11551.5  .741094   1.608
chisquare= 1.608 for 3 d. of f.; p-value= .444752

```

```

Binary rank test for xor3.rnd
  Rank test for 32x32 binary matrices:
  rows from leftmost 32 bits of each 32-bit integer
  rank  observed  expected (o-e)^2/e  sum
  29      172      211.4  7.349326   7.349
  30     5062     5134.0  1.010025   8.359
  31     23268    23103.0  1.177747   9.537
  32     11498    11551.5  .248007   9.785
chisquare= 9.785 for 3 d. of f.; p-value= .980396

```

```

-----
b-rank test for bits 1 to 8 p=1-exp(-SUM/2)= .68073
b-rank test for bits 2 to 9 p=1-exp(-SUM/2)= .09026
b-rank test for bits 3 to 10 p=1-exp(-SUM/2)= .80664
b-rank test for bits 4 to 11 p=1-exp(-SUM/2)= .45924
b-rank test for bits 5 to 12 p=1-exp(-SUM/2)= .81253
b-rank test for bits 6 to 13 p=1-exp(-SUM/2)= .04599
b-rank test for bits 7 to 14 p=1-exp(-SUM/2)= .35635
b-rank test for bits 8 to 15 p=1-exp(-SUM/2)= .35788
b-rank test for bits 9 to 16 p=1-exp(-SUM/2)= .67752
b-rank test for bits 10 to 17 p=1-exp(-SUM/2)= .90244
b-rank test for bits 11 to 18 p=1-exp(-SUM/2)= .33720
b-rank test for bits 12 to 19 p=1-exp(-SUM/2)= .51250
b-rank test for bits 13 to 20 p=1-exp(-SUM/2)= .02023
b-rank test for bits 14 to 21 p=1-exp(-SUM/2)= .81882
b-rank test for bits 15 to 22 p=1-exp(-SUM/2)= .83130
b-rank test for bits 16 to 23 p=1-exp(-SUM/2)= .94930
b-rank test for bits 17 to 24 p=1-exp(-SUM/2)= .07186
b-rank test for bits 18 to 25 p=1-exp(-SUM/2)= .04845
b-rank test for bits 19 to 26 p=1-exp(-SUM/2)= .36940
b-rank test for bits 20 to 27 p=1-exp(-SUM/2)= .11713
b-rank test for bits 21 to 28 p=1-exp(-SUM/2)= .41560
b-rank test for bits 22 to 29 p=1-exp(-SUM/2)= .60440
b-rank test for bits 23 to 30 p=1-exp(-SUM/2)= .52466
b-rank test for bits 24 to 31 p=1-exp(-SUM/2)= .44173
b-rank test for bits 25 to 32 p=1-exp(-SUM/2)= .31446
TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices

```

These should be 25 uniform [0,1] random variables:

| | | | | |
|---------|---------|---------|---------|---------|
| .680725 | .090263 | .806643 | .459244 | .812533 |
| .045995 | .356352 | .357875 | .677525 | .902439 |
| .337200 | .512501 | .020225 | .818821 | .831303 |
| .949304 | .071855 | .048446 | .369401 | .117126 |
| .415605 | .604400 | .524656 | .441734 | .314457 |

brank test summary for xor3.rnd

The KS test for those 25 supposed UNI's yields

KS p-value= .325421

No. missing words should average 141909. with sigma=428.

| | | | |
|------------|-----------------------|-------------------------|-----------------|
| tst no 1: | 141741 missing words, | -.39 sigmas from mean, | p-value= .34705 |
| tst no 2: | 142212 missing words, | .71 sigmas from mean, | p-value= .76027 |
| tst no 3: | 142559 missing words, | 1.52 sigmas from mean, | p-value= .93548 |
| tst no 4: | 142286 missing words, | .88 sigmas from mean, | p-value= .81059 |
| tst no 5: | 141541 missing words, | -.86 sigmas from mean, | p-value= .19473 |
| tst no 6: | 141650 missing words, | -.61 sigmas from mean, | p-value= .27229 |
| tst no 7: | 141817 missing words, | -.22 sigmas from mean, | p-value= .41460 |
| tst no 8: | 141589 missing words, | -.75 sigmas from mean, | p-value= .22710 |
| tst no 9: | 142091 missing words, | .42 sigmas from mean, | p-value= .66439 |
| tst no 10: | 142063 missing words, | .36 sigmas from mean, | p-value= .64022 |
| tst no 11: | 141647 missing words, | -.61 sigmas from mean, | p-value= .26997 |
| tst no 12: | 140925 missing words, | -2.30 sigmas from mean, | p-value= .01073 |
| tst no 13: | 142293 missing words, | .90 sigmas from mean, | p-value= .81499 |
| tst no 14: | 142315 missing words, | .95 sigmas from mean, | p-value= .82839 |
| tst no 15: | 141087 missing words, | -1.92 sigmas from mean, | p-value= .02735 |
| tst no 16: | 141997 missing words, | .20 sigmas from mean, | p-value= .58115 |
| tst no 17: | 141223 missing words, | -1.60 sigmas from mean, | p-value= .05440 |
| tst no 18: | 141794 missing words, | -.27 sigmas from mean, | p-value= .39379 |
| tst no 19: | 141748 missing words, | -.38 sigmas from mean, | p-value= .35311 |
| tst no 20: | 141632 missing words, | -.65 sigmas from mean, | p-value= .25850 |

| | | | | |
|-------------------|---------------------|--------|--------|-------|
| OPSO for xor3.rnd | using bits 23 to 32 | 141886 | -.080 | .4679 |
| OPSO for xor3.rnd | using bits 22 to 31 | 141572 | -1.163 | .1224 |
| OPSO for xor3.rnd | using bits 21 to 30 | 142179 | .930 | .8238 |
| OPSO for xor3.rnd | using bits 20 to 29 | 142193 | .978 | .8360 |
| OPSO for xor3.rnd | using bits 19 to 28 | 141761 | -.511 | .3045 |
| OPSO for xor3.rnd | using bits 18 to 27 | 142181 | .937 | .8256 |
| OPSO for xor3.rnd | using bits 17 to 26 | 142179 | .930 | .8238 |
| OPSO for xor3.rnd | using bits 16 to 25 | 142022 | .389 | .6512 |
| OPSO for xor3.rnd | using bits 15 to 24 | 142386 | 1.644 | .9499 |
| OPSO for xor3.rnd | using bits 14 to 23 | 142353 | 1.530 | .9370 |
| OPSO for xor3.rnd | using bits 13 to 22 | 141779 | -.449 | .3266 |
| OPSO for xor3.rnd | using bits 12 to 21 | 142388 | 1.651 | .9506 |
| OPSO for xor3.rnd | using bits 11 to 20 | 141795 | -.394 | .3467 |
| OPSO for xor3.rnd | using bits 10 to 19 | 141509 | -1.380 | .0837 |
| OPSO for xor3.rnd | using bits 9 to 18 | 142015 | .364 | .6422 |
| OPSO for xor3.rnd | using bits 8 to 17 | 142133 | .771 | .7797 |
| OPSO for xor3.rnd | using bits 7 to 16 | 141636 | -.943 | .1730 |
| OPSO for xor3.rnd | using bits 6 to 15 | 142353 | 1.530 | .9370 |
| OPSO for xor3.rnd | using bits 5 to 14 | 142109 | .689 | .7544 |
| OPSO for xor3.rnd | using bits 4 to 13 | 141876 | -.115 | .4543 |
| OPSO for xor3.rnd | using bits 3 to 12 | 141477 | -1.491 | .0680 |
| OPSO for xor3.rnd | using bits 2 to 11 | 142562 | 2.251 | .9878 |
| OPSO for xor3.rnd | using bits 1 to 10 | 142399 | 1.689 | .9543 |
| QOSO for xor3.rnd | using bits 28 to 32 | 142329 | 1.423 | .9226 |
| QOSO for xor3.rnd | using bits 27 to 31 | 141381 | -1.791 | .0367 |
| QOSO for xor3.rnd | using bits 26 to 30 | 141841 | -.232 | .4084 |
| QOSO for xor3.rnd | using bits 25 to 29 | 142204 | .999 | .8411 |
| QOSO for xor3.rnd | using bits 24 to 28 | 141800 | -.371 | .3555 |
| QOSO for xor3.rnd | using bits 23 to 27 | 142334 | 1.440 | .9250 |
| QOSO for xor3.rnd | using bits 22 to 26 | 142405 | 1.680 | .9535 |
| QOSO for xor3.rnd | using bits 21 to 25 | 142088 | .606 | .7276 |
| QOSO for xor3.rnd | using bits 20 to 24 | 141965 | .189 | .5748 |
| QOSO for xor3.rnd | using bits 19 to 23 | 142128 | .741 | .7707 |
| QOSO for xor3.rnd | using bits 18 to 22 | 141598 | -1.055 | .1456 |
| QOSO for xor3.rnd | using bits 17 to 21 | 141885 | -.082 | .4671 |
| QOSO for xor3.rnd | using bits 16 to 20 | 141264 | -2.188 | .0144 |

| | | | | |
|-------------------|---------------------|--------|--------|-------|
| OQSO for xor3.rnd | using bits 15 to 19 | 141816 | -.316 | .3759 |
| OQSO for xor3.rnd | using bits 14 to 18 | 142341 | 1.463 | .9283 |
| OQSO for xor3.rnd | using bits 13 to 17 | 141835 | -.252 | .4005 |
| OQSO for xor3.rnd | using bits 12 to 16 | 141682 | -.771 | .2205 |
| OQSO for xor3.rnd | using bits 11 to 15 | 141739 | -.577 | .2818 |
| OQSO for xor3.rnd | using bits 10 to 14 | 142577 | 2.263 | .9882 |
| OQSO for xor3.rnd | using bits 9 to 13 | 141715 | -.659 | .2550 |
| OQSO for xor3.rnd | using bits 8 to 12 | 141803 | -.360 | .3593 |
| OQSO for xor3.rnd | using bits 7 to 11 | 141420 | -1.659 | .0486 |
| OQSO for xor3.rnd | using bits 6 to 10 | 141843 | -.225 | .4111 |
| OQSO for xor3.rnd | using bits 5 to 9 | 142184 | .931 | .8241 |
| OQSO for xor3.rnd | using bits 4 to 8 | 141340 | -1.930 | .0268 |
| OQSO for xor3.rnd | using bits 3 to 7 | 141753 | -.530 | .2981 |
| OQSO for xor3.rnd | using bits 2 to 6 | 141833 | -.259 | .3979 |
| OQSO for xor3.rnd | using bits 1 to 5 | 142502 | 2.009 | .9777 |
| DNA for xor3.rnd | using bits 31 to 32 | 141811 | -.290 | .3859 |
| DNA for xor3.rnd | using bits 30 to 31 | 141874 | -.104 | .4585 |
| DNA for xor3.rnd | using bits 29 to 30 | 142556 | 1.908 | .9718 |
| DNA for xor3.rnd | using bits 28 to 29 | 141254 | -1.933 | .0266 |
| DNA for xor3.rnd | using bits 27 to 28 | 141377 | -1.570 | .0582 |
| DNA for xor3.rnd | using bits 26 to 27 | 141950 | .120 | .5477 |
| DNA for xor3.rnd | using bits 25 to 26 | 141885 | -.072 | .4714 |
| DNA for xor3.rnd | using bits 24 to 25 | 141682 | -.671 | .2512 |
| DNA for xor3.rnd | using bits 23 to 24 | 142150 | .710 | .7611 |
| DNA for xor3.rnd | using bits 22 to 23 | 142809 | 2.654 | .9960 |
| DNA for xor3.rnd | using bits 21 to 22 | 142746 | 2.468 | .9932 |
| DNA for xor3.rnd | using bits 20 to 21 | 141625 | -.839 | .2008 |
| DNA for xor3.rnd | using bits 19 to 20 | 142148 | .704 | .7593 |
| DNA for xor3.rnd | using bits 18 to 19 | 142112 | .598 | .7250 |
| DNA for xor3.rnd | using bits 17 to 18 | 142364 | 1.341 | .9101 |
| DNA for xor3.rnd | using bits 16 to 17 | 142030 | .356 | .6391 |
| DNA for xor3.rnd | using bits 15 to 16 | 142302 | 1.158 | .8766 |
| DNA for xor3.rnd | using bits 14 to 15 | 142035 | .371 | .6446 |
| DNA for xor3.rnd | using bits 13 to 14 | 141978 | .203 | .5803 |
| DNA for xor3.rnd | using bits 12 to 13 | 141851 | -.172 | .4317 |
| DNA for xor3.rnd | using bits 11 to 12 | 142140 | .680 | .7519 |
| DNA for xor3.rnd | using bits 10 to 11 | 141808 | -.299 | .3825 |
| DNA for xor3.rnd | using bits 9 to 10 | 141131 | -2.296 | .0108 |
| DNA for xor3.rnd | using bits 8 to 9 | 142081 | .506 | .6937 |
| DNA for xor3.rnd | using bits 7 to 8 | 141574 | -.989 | .1613 |
| DNA for xor3.rnd | using bits 6 to 7 | 141369 | -1.594 | .0555 |
| DNA for xor3.rnd | using bits 5 to 6 | 142149 | .707 | .7602 |
| DNA for xor3.rnd | using bits 4 to 5 | 141761 | -.438 | .3309 |
| DNA for xor3.rnd | using bits 3 to 4 | 142255 | 1.020 | .8461 |
| DNA for xor3.rnd | using bits 2 to 3 | 141969 | .176 | .5699 |
| DNA for xor3.rnd | using bits 1 to 2 | 141174 | -2.169 | .0150 |

Test results for xor3.rnd

Chi-square with $5^5-5^4=2500$ d.of f. for sample size:2560000

chisquare equiv normal p-value

Results fo COUNT-THE-1's in successive bytes:

| | | | |
|--------------------------|---------|--------|---------|
| byte stream for xor3.rnd | 2345.17 | -2.190 | .014273 |
| byte stream for xor3.rnd | 2483.39 | -.235 | .407140 |

Chi-square with $5^5-5^4=2500$ d.of f. for sample size: 256000

chisquare equiv normal p value

Results for COUNT-THE-1's in specified bytes:

| | | | |
|---------------|---------|--------|---------|
| bits 1 to 8 | 2567.73 | .958 | .830946 |
| bits 2 to 9 | 2500.55 | .008 | .503085 |
| bits 3 to 10 | 2521.35 | .302 | .618637 |
| bits 4 to 11 | 2339.02 | -2.277 | .011406 |
| bits 5 to 12 | 2605.25 | 1.488 | .931677 |
| bits 6 to 13 | 2411.55 | -1.251 | .105492 |
| bits 7 to 14 | 2369.63 | -1.844 | .032616 |
| bits 8 to 15 | 2521.54 | .305 | .619666 |
| bits 9 to 16 | 2450.32 | -.703 | .241171 |
| bits 10 to 17 | 2451.48 | -.686 | .246295 |
| bits 11 to 18 | 2555.11 | .779 | .782121 |

| | | | |
|---------------|---------|--------|---------|
| bits 12 to 19 | 2575.46 | 1.067 | .857042 |
| bits 13 to 20 | 2509.11 | .129 | .551253 |
| bits 14 to 21 | 2563.67 | .900 | .816058 |
| bits 15 to 22 | 2548.82 | .690 | .755016 |
| bits 16 to 23 | 2548.70 | .689 | .754522 |
| bits 17 to 24 | 2485.27 | -.208 | .417510 |
| bits 18 to 25 | 2577.01 | 1.089 | .861936 |
| bits 19 to 26 | 2603.73 | 1.467 | .928813 |
| bits 20 to 27 | 2455.60 | -.628 | .265048 |
| bits 21 to 28 | 2530.48 | .431 | .666776 |
| bits 22 to 29 | 2329.31 | -2.414 | .007889 |
| bits 23 to 30 | 2447.01 | -.749 | .226822 |
| bits 24 to 31 | 2487.50 | -.177 | .429851 |
| bits 25 to 32 | 2615.64 | 1.635 | .949022 |

CDPARK: result of ten tests on file xor3.rnd
 Of 12,000 tries, the average no. of successes
 should be 3523 with sigma=21.9

| | | |
|-----------------|-----------------|------------------|
| Successes: 3541 | z-score: .822 | p-value: .794438 |
| Successes: 3511 | z-score: -.548 | p-value: .291865 |
| Successes: 3534 | z-score: .502 | p-value: .692266 |
| Successes: 3546 | z-score: 1.050 | p-value: .853193 |
| Successes: 3505 | z-score: -.822 | p-value: .205562 |
| Successes: 3511 | z-score: -.548 | p-value: .291865 |
| Successes: 3519 | z-score: -.183 | p-value: .427537 |
| Successes: 3495 | z-score: -1.279 | p-value: .100530 |
| Successes: 3496 | z-score: -1.233 | p-value: .108811 |
| Successes: 3520 | z-score: -.137 | p-value: .445521 |

| square size | avg. no. parked | sample sigma |
|-------------|-----------------|--------------|
| 100. | 3517.800 | 16.899 |

KSTEST for the above 10: p= .378127

This is the MINIMUM DISTANCE test
 for random integers in the file xor3.rnd

| Sample no. | d^2 | avg | equiv uni |
|------------|--------|--------|-----------|
| 5 | .2184 | .7871 | .197039 |
| 10 | .0676 | 1.0243 | .065709 |
| 15 | .0137 | .7468 | .013710 |
| 20 | .6077 | 1.0030 | .457048 |
| 25 | 1.5755 | .9915 | .794728 |
| 30 | .1295 | .9745 | .122059 |
| 35 | .4798 | .9535 | .382582 |
| 40 | .4045 | 1.0033 | .334040 |
| 45 | .7264 | .9769 | .518093 |
| 50 | .1599 | .9588 | .148470 |
| 55 | .4602 | 1.0015 | .370283 |
| 60 | .2730 | 1.0153 | .239921 |
| 65 | .8683 | 1.0583 | .582155 |
| 70 | .7038 | 1.0209 | .507046 |
| 75 | .9092 | 1.0148 | .599006 |
| 80 | .4489 | 1.0617 | .363089 |
| 85 | 1.8546 | 1.0591 | .844931 |
| 90 | .8708 | 1.1001 | .583218 |
| 95 | 3.0456 | 1.1475 | .953156 |
| 100 | 1.1423 | 1.1309 | .682743 |

MINIMUM DISTANCE TEST for xor3.rnd

Result of KS test on 20 transformed mindist^2's:
 p-value= .424779

The 3DSPHERES test for file xor3.rnd

| | | |
|--------------|-------------|-----------------|
| sample no: 1 | r^3= 13.546 | p-value= .36334 |
| sample no: 2 | r^3= 8.797 | p-value= .25416 |
| sample no: 3 | r^3= 37.868 | p-value= .71698 |
| sample no: 4 | r^3= 8.189 | p-value= .23889 |
| sample no: 5 | r^3= 35.475 | p-value= .69349 |
| sample no: 6 | r^3= 10.660 | p-value= .29905 |
| sample no: 7 | r^3= 61.646 | p-value= .87189 |

| | | |
|---------------|-------------|-----------------|
| sample no: 8 | r^3= 17.041 | p-value= .43336 |
| sample no: 9 | r^3= 84.072 | p-value= .93934 |
| sample no: 10 | r^3= 14.544 | p-value= .38419 |
| sample no: 11 | r^3= 52.186 | p-value= .82440 |
| sample no: 12 | r^3= 39.753 | p-value= .73422 |
| sample no: 13 | r^3= 20.489 | p-value= .49489 |
| sample no: 14 | r^3= 84.198 | p-value= .93959 |
| sample no: 15 | r^3= 14.106 | p-value= .37512 |
| sample no: 16 | r^3= 4.563 | p-value= .14109 |
| sample no: 17 | r^3= 70.607 | p-value= .90497 |
| sample no: 18 | r^3= 56.385 | p-value= .84733 |
| sample no: 19 | r^3= 33.331 | p-value= .67078 |
| sample no: 20 | r^3= 3.296 | p-value= .10406 |

3DSPHERES test for file xor3.rnd p-value= .473301

RESULTS OF SQUEEZE TEST FOR xor3.rnd
Table of standardized frequency counts
((obs-exp)/sqrt(exp))^2
for j taking values <=6,7,8,...,47,>=48:

| | | | | | |
|-----|------|------|-----|-----|------|
| -.8 | -.7 | -.6 | -.5 | .0 | -1.4 |
| .4 | .7 | .8 | -.1 | .0 | .9 |
| -.1 | .0 | -.5 | .2 | .0 | 1.7 |
| -.7 | -.7 | -1.6 | -.1 | .1 | .6 |
| 2.0 | -2.1 | -.1 | 1.4 | -.8 | .2 |
| -.3 | -1.8 | 1.2 | -.1 | .8 | -.1 |
| -.7 | 1.1 | .1 | 1.0 | .1 | -1.0 |
| -.1 | | | | | |

Chi-square with 42 degrees of freedom: 32.976
z-score= -.985 p-value= .160545

| | | |
|-------------|---------|---------|
| Test no. 1 | p-value | .547889 |
| Test no. 2 | p-value | .425635 |
| Test no. 3 | p-value | .249063 |
| Test no. 4 | p-value | .436784 |
| Test no. 5 | p-value | .461082 |
| Test no. 6 | p-value | .588325 |
| Test no. 7 | p-value | .786673 |
| Test no. 8 | p-value | .111705 |
| Test no. 9 | p-value | .518395 |
| Test no. 10 | p-value | .013106 |

Results of the OSUM test for xor3.rnd
KSTEST on the above 10 p-values: .637148

The RUNS test for file xor3.rnd
Up and down runs in a sample of 10000

| | |
|--------------------------------|---------|
| Run test for xor3.rnd | : |
| runs up; ks test for 10 p's: | .618383 |
| runs down; ks test for 10 p's: | .846326 |
| Run test for xor3.rnd | : |
| runs up; ks test for 10 p's: | .442940 |
| runs down; ks test for 10 p's: | .152234 |

Results of craps test for xor3.rnd

| | | | | |
|--------------|----------|----------|--|--|
| No. of wins: | Observed | Expected | | |
| | 98830 | 98585.86 | | |

Chisq= 13.95 for 20 degrees of freedom, p= .16691

| | | | | |
|--------|----------|----------|-------|-----|
| Throws | Observed | Expected | Chisq | Sum |
|--------|----------|----------|-------|-----|

SUMMARY FOR xor3.rnd

| | |
|--------------------------|---------|
| p-value for no. of wins: | .862570 |
| p-value for throws/game: | .166911 |

Test completed. File xor3.rnd

::