Pi seems a good random number generator - but not always the best

April 27 2005

If you wanted a random number, historically you could do worse than to pick a sequence from the string of digits in pi. But Purdue University scientists now say other sources might be better.
Physicists including Purdue's Ephraim Fischbach have completed a study comparing the "randomness" in pi to that produced by 30 software random number generators and one chaos-generating physical machine. After conducting several tests, they have found that while sequences of digits from pi are indeed an acceptable source of randomness – often an important factor in data encryption and in solving certain physics problems – pi's digit string does not always produce randomness as effectively as manufactured generators do.

"We do not believe these results imply anything about a pattern existing in pi's number set," said Fischbach, who is a professor of physics in Purdue's College of Science. "However, it may imply that if your livelihood depends on a reliable source of random numbers, as a cryptographer's might, then some commercially available random number generators might serve you better."

Fischbach conducted the study with Shu-Ju Tu, a former graduate student who has since moved to a postdoctoral fellowship at the University of Texas M.D. Anderson Cancer Center. Their research paper appears in the International Journal of Modern Physics C, vol. 16, no. 2.

Pi, the ratio between a circle's diameter and circumference, has fascinated mathematicians for centuries. A bit larger than the number 3,

pi cannot be expressed as a ratio of two whole numbers, and its apparently endless string of digits is sometimes expressed as 3.14159… Modern computers have enabled mathematicians to calculate the value of pi to more than 200 billion digits to the right of the decimal point. But no one has ever found evidence that calculating finer and finer values of pi will ever reveal an end to the string or that there is any regular pattern to be found within it.

Tu and Fischbach decided to test pi's randomness against the outputs of 31 commercially available random number generators (RNGs) that are frequently used for encrypting confidential information before it is stored or sent electronically. To produce numbers, many of these RNGs use an algorithm – a short set of instructions that can be repeated quickly – and it is the quality of the algorithm that makes one RNG more valuable than another.

"Strictly speaking, an algorithm does not produce a truly random number," Fischbach said. "Because its instructions are fixed, an RNG's output could, in theory, be predicted, if you knew what the algorithm was. Of course, anyone using a particular RNG will want to keep its algorithm secret, and for the most part RNGs are cleverly designed enough that they produce numbers that are 'sufficiently random' for encryption purposes."

The scientists took approximately the first 100 million digits of pi, broke the string up into 10-digit segments, and gave the segments a form that defines a point somewhere within a cube with sides one unit long. To specify each point, three such segments are necessary – one for each dimension. For example, the sequence 1415926535 was given the form 0.1415926535, which specifies the point's distance along the x-axis. Similarly, the two subsequent sequences give the point's y and z coordinates. All of the sequences thus became coordinates between zero and one, giving millions of points that lay within the imaginary cube.

"Each point within a cube lies at some distance from the cube's center – some are close, some farther away," Fischbach said. "If you graph their distribution from the center, what you get resembles a familiar bell-shaped probability curve. What we wanted to find out, in essence, was whether the points derived from pi's digits generate an identical curve, and also whether the commercially available RNGs do."

In addition to checking these curves against the predicted ideal, the scientists created a computer program that was able to test randomness even further. It also took groups of points, formed angles from the lines between them, and compared the measure of those angles. The program even took groups of coordinates and tested their randomness within imaginary cubes of six dimensions.

"This was our attempt to leave fewer stones unturned," Tu said. "We hoped additional tests might reveal hidden correlations between number sets that a single test might not have shown."

From the tests Tu and Fischbach ran, each RNG was given a letter grade according to how great its standard deviation, or sigma, was from the expected value. Pi's scores were consistently high across all the experiments, but what surprised them was that some of the RNGs performed even better in some situations.

"Our work showed no correlations or patterns in pi's number set – in short, pi is indeed a good source of randomness," Fischbach said. "However, there were times when pi's performance was outdone by the RNGs."

Pi never scored less than a B on the tests, and in one case outperformed all the RNGs, which in addition to mathematical algorithms included a device that uses turbulence in a fluid as its source of randomness. But in most cases, pi lost out to at least one RNG, and in several it finished

decidedly in the middle of the pack. Fischbach emphasized that the results do not imply the existence of any patterns in pi's digit string, though he said would like to see more tests done.

"This study probably says more about our commercially available random number generators than the nature of pi," Fischbach said. "Some of them failed our tests outright. But they, and pi as well, might perform differently if the tests were run under different circumstances."

Fischbach mentioned that less than 1 percent of pi's known digits were used in the tests, and that cubes of dimensions other than 3 and 6 could be imagined.

"These tests are simple to reproduce with a desktop computer. All you need is time," he said. "It took us almost a year of work to crunch these numbers. We have included the program we used in the paper if anyone would like to try doing the analysis with a larger number set. I hope someone will because pi shows up in security systems, cryptography and other places that have nothing to do with circles. That's part of what gives it a fascination that will not go away."

Source: Purdue University (by Chad Boutin)