

COMPUTERIZED LOTTERY DRAWINGS

mindtab

Location: California

I usually play the 5-number lotto, which is automated. Yes, I would rather have the big payouts of the SuperLotto. But considering my lack of funds, and that the odds of winning the Fantasy5 lotto are 1 in 575,000 or such (against the 27million or more in the SuperLotto), I decided to spend my little money on a more modest goal.

The problem that comes into play is the draws being automated. Yet, it presents me with an intriguing quest---to find the ticker.

The draw is selected from two machines--one uses a PRNG (pseudo-random generator), while the other uses an algorithm, at approximately 6:35pm each day.

Thus the data file is a mixture of two separate outputs. The stats are dubious overall, yet when dissected, one can spot many interesting things (I've been 'dreaming' of reverse engineering, and common algorithms). There have been many draws which have duplicated (period of the PRNG?). Some Quads which repeat after about the same amount of time. Triples which come around the same time together. Next draws also. But, since the inputs are from two different sources, the output is mixed in analysis. Some fare no pattern, while some do.

The type of draw conducted each night is randomly chosen (not by machine) --whether by PRNG or algorithm---which means, one machine or the other.

We use machines to try to find patterns in a random universe which may be localized at a certain time and place (at the time when a non-automated draw occurs in your state).

Automated draws are already confined within their own FINITE universe. A pattern is still at play, yet this time it is predetermined by an initial state. And every state afterwards, intermingled together in a dance of numbers.

Could the lottery be using 'Scientific games' machines? John Koza was one of the initial contributions (the father of genetic programming).

Ah, the quest has been on for years now, but only now have had time to spend on it.

Why do some of the patterns (as mentioned above) show a really interesting correlation? Could it be that the PRNG is really a simple LCG? (linear congruential generator) based on the time when the program is run? Could the other machine implemented to use an algorithm use an off the wall algorithm, or rather, it would use something that's been tested and implemented already (i.e. Mersenne Twister, or others)?

Working on a few programs to test some more data. Will post results if anyone is interested. I am using both mine and of course, Ion's excellent programs. Mine are meager little programs, and don't do as much, but enough for me to test a few of my hypothesis.

Moreover, I want to test the data in unsorted fashion, as the numbers have been generated (since in PRNG's, the next number usually depends on the previous number in output). The list of previous

numbers on the Cali site are not all in drawn order. I think it goes in drawn order only until Oct 10, 2004. Then it is shown sorted.

I do have a list from its beginning (July 1, 1998---when the automated draws started) until Apr 2, 2002. Question that I ponder on is: have those machines changed since then? Searching on the internet, it seems Cali did have a contract with Gtech for several new machines in 2005, yet I do not know if that affected the original draw machines implemented.

Camelia Sacui

Nanhajir

Location: Hic et ubique

Posted: Jun 05, 2009 08:02 Post subject: Re: Automated draws type of lottery

mindtab wrote:

The draw is selected from two machines--one uses a PRNG (pseudo-random generator), while the other uses an algorithm, at approximately 6:35pm each day.

Why do some of the patterns (as mentioned above) show a really interesting correlation? Could it be that the PRNG is really a simple LCG? (linear congruential generator) based on the time when the program is run? Could the other machine implemented to use an algorithm use an off the wall algorithm, or rather, it would use something that's been tested and implemented already (ie Mersenne Twister, or others)?

Hello, mindtab!

Part of my work is related to cryptography and applications of randomness and pseudorandomness, so I could add my two cents.

First of all I don't think that any lottery is ran on simple PRNGs, like mentioned one of LCG type. Using just two-dimensional plot of consecutive states of LCG PRNG can reveal visible patterns. Such generators are no-no in area of gambling.

Mersenne Twister is another type of PRNG - actually it is a large array of LFSR (Linear Feedback Shift Register) states, aggregated and mixed to produce single output. It is tested statistically thoroughly - yet is predictable and unsuitable for lottery applications. Predictable means that knowing some part of its output you could calculate its internal state (the seed). Being lottery manager I would never risk using such engine for draws. There is plenty of methods dedicated to analysing and "breaking" LCG and LFSR-based PRNGs.

The most reasonable choice for lottery owner is to use hardware non-algorithmic random number generator. You have mentioned G-Tech as company involved in running this particular lotto game. This company has partnership with idQuantique, company developing quantum phenomena-based hardware random number generators.

On their website (<http://www.idquantique.com/products/quantis.htm>) this partnership is described:

Quote:

Quantis-PCI has been approved by GTECH

GTech, the leading gaming technology company based in the United States, has subjected the Quantis-PCI product to an in-depth evaluation procedure. The Quantis-PCI product is now "ES Approved", meaning that it meets its demanding reliability and quality requirements and is compatible with the world's leading lottery solutions.

Other gambling companies are mentioned as partners, too.

So, if G-Tech is now a technology provider to your lotto, probably it will be ran on idQuantique technology. As I know, few computerized lotto games, like Keno in some countries, are already using idQuantique technology to generate draws.

Of course I don't exclude possibility that draws generated before partnership with G-Tech was generated using simpler methods. So, IF PRNG states was not changed between consecutive draws, then all draws in sequence was generated using consecutive states of PRNG. This could be very risky for lottery owner. More likely is that PRNG was reseeded before every draw. If the source of seed was computer internal clock, then we have probably less than

$18,2 * \text{NumberOfSecondsInDay}$

possible seeds.

This could be beautiful, because you could check ALL possible states in short time. Of course you still need to know the exact draw generating routine. If you know the range of time, when PRNG was seeded, you could reduce number of possible seeds to check.

If the source of seed was RTDSC timestamp instruction from Intel CPU, then we have MUCH more possible seeds. Brute-forcing probably is infeasible for ordinary person.

It is possible that lotto owner switched to G-Tech/idQuantique technology because of detected flaws in previously used methods. So you can discover many patterns in historical results. But how to extrapolate those results to make them usable in predicting new draws, when technology is probably switched to another one?

Is so-called quantum randomness harder to beat? I don't think so. Many statistical features of draws will change, but you still have lot of possibilities to attack.

Good luck!

Nanhajir

Uyzsudoi joigof ouk aoyjs.

mindtab

Nanhajir,

My hope is the 'what if not'.

The automated draws started before Gtech's work with Quantis, or other mergers. From looking around the net, it seems that CA Lottery has purchased Gtech machines to run terminals in stores. Are they using a GTech machine for the official draw? I don't know. CA has gravity-pick machines from Smartplay as well (again, according to net reading). Or they could be using 'Scientific Games' related stuff.

As a 'lottery owner' I don't think they have much say in what goes in the machine, but simply who has been awarded the contract to deal with them. So you are stuck with what your contractor has at the time put in the machine. There are only so many companies dealing with lottery contracts.

Now, just because there is new technology, has the state lottery immediately run over and change their equipment? Maybe yes, if the budget allows. Maybe not, if they think 'don't fix what is not broken'.

Now if I would have started testing the seeds way back in 98, I would be far better off, without the question of 'what if they did' [change the machines]. I could have left one computer (even running for years) to keep on testing. Twenty-one years later now, without even a start, I am left at guessing. Geesh! 21! Where did time fly? I thought of this back then. Why I didn't start I have no idea.

But, I can still start. Better off than asking that same question 10 years From NOW.

Today I am left looking at data comprised of two outputs from two different methods not related to each other. As my previous post response concerning the non-automated draw of Superlotto---where each draw has a fair shake regardless---I think that in the Fantasy5 it is a different situation of 'fairness'. I could be wrong, again.

Camelia Sacui

The topic of true random number generating is hot! It's been so for many years, since the inception of personal computers. I was posed with this type of questions way-back-when I opened a message board at Saliu.com. I did write about the subject in a manner of most merit. I also provided the source code for software to generate truly random numbers (directly applicable to a 6-number lotto game). The main articles on randomness as in probability theory:

[True random numbers generator: BASIC programming source code, algorithm](#)

"True random numbers generator: BASIC programming source code, algorithm";

[Randomness, true random numbers generators, degree of randomness](#)

"Randomness, true random numbers generators, degree of randomness".

When they say randomness in computer software, many pundits say it is pseudo-randomness. They actually refer to software written for the original IBM PC and Microsoft BASIC. The software generates "random" numbers based on a "seed", usually the timer. The timer counts the number of seconds since midnight. There are only 86,400 seconds in a day. The variation in randomness is just too low, not only by computer standards. If the random generator is started exactly at the same second of the day, the same sequence of numbers is generated.

I heard stories of a state lottery being ripped-off by Keno players. The Keno numbers were generated by a computer precisely every 15 minutes: The same times of the day! The bare-bone timer was used as

the randomizing seed. Thus, the Keno drawing of 9:00 PM yesterday will be the same today at 9:00 PM! The state lottery does not go bankrupt because they allocate to prizes only 50% of ticket sales.

The midnight was the most interesting case, as the timer was equal to zero. A randomizing seed equal to zero always generates the same sequence of numbers. I don't know if they allowed playing Keno that late. But it was the most sure-fire method of winning huge amounts of money with a \$1 ticket!

There are easy and sure-fire ways to verify the "randomness" of random number generators. One of them has been done thousands, if not millions of times, running my software. My software makes it very easy to analyze past random results, be it lottery, or roulette, or anything that most people perceive as "truly random". But ask them back: "Is there anything that is NOT random?" Some might get mad at you in no time!

Everything is random and the Universe itself is ruled by randomness. The variation is in the degree of certainty (or probability of appearance). Randomness is the fairest form of being and not-being. And all that is possible to comprehend by means of mathematics.

The Keno case above (as implemented by idiotic bureaucrats) would show blatant defiance of randomness and probability theory. Just check 100 or 200 of past Keno results in that game. The analysis as done by my software would have shown way too many repeats of the same Keno drawings! And we talkin' here 20-number Keno drawings! Make no mistake: The lotto drawings will repeat, BUT according to mathematics only. Ion Saliu's Paradox or Birthday Paradox show that there will be at least one lotto draw repeated... after thousands of drawings.

I run `[color=red][b]Collisions.exe[/b][/color]` for a 6/49 lotto game. If 4406 lotto drawings are considered, the degree of certainty is 50% that at least one lotto draw is a duplicate. If 100000 lotto drawings are considered, the degree of certainty is very, very, very close to 100% that at least one lotto draw is a duplicate. In the case of a 20-number Keno draw, we would need billions of drawings to have a 50-50 chance for a duplicate. The bonehead Keno game with the flawed random generator would have shown lots of drawings being duplicated several times in just one month!

Some say that only hardware-based generating can be truly random. I don't think so. Yes, I was puzzled for many years why my cheap Atari of the 1980's was more successful than the much more expensive PCs in generating truly random numbers. I am referring here to lotto, for I used both Atari and PCs to generate random lotto combinations. Atari had a hardware-based random number generator. The degree of randomness was higher when using an Atari. The randomization seed Atari used was the quartz frequency of the CPU. Even if the frequency was just up to one million, the range 1 to 1000000 was randomly variable and offered a higher variation than 1 to 86400. The quartz frequency is never dependent on the time of the day, or the date. No wonder why my old, cheap Atari 800XL generated so many winning lotto combinations for me, including the astounding lotto jackpot with a number of combinations I was unable to play.

The Intel CPU chips are so fast now that they measure the frequency in gigahertz (GHz = billions of hertz)! What an extraordinary random seed! Too bad, Windows does not allow direct hardware access by the software.

Several years ago I made public a randomization function that is no longer dependent on the time of the day (timer). The function generates variable randomization seeds between millions and trillions. The

variation is the widest, compared to any other attempts to date. My software generates SIMulated random data files for lotto. Millions of analyses performed by my lotto software have not shown any bias whatsoever. The combinations generated are truly random. That is, the results prove a high degree of randomness. Nobody will be able to see unwarranted repeats even if checking millions of combinations.

I prefer my software-based randomization to any hardware based random number generation. The variation reaches in the range of trillions — far higher than any hardware generator. Also, a processor might be stuck at the same frequency for seconds. It depends a lot on the processes the operating system deals with.

The lottery commissions have no experts in mathematics. They might rely on the type of mediocrities such as those who write articles for Wikipedia. I was shocked what I discovered in the Wiki article on the [Birthday Paradox](#) ("Birthday Problem"). I was led there by a Google search and some input. The Wiki article was at the top of the search results list. That article represents blatant plagiarism — and that on top of horrendous mathematics. Similar articles are on combinatorics, lexicographic order — and, yes, randomness and random number generation!

The link to California lottery is also proof of happy marriage between bureaucracy and mediocrity. The state lottery commission does not require any proof, as in reviews or analyses by third parties. The state governments don't care a bit about fairness. They build casinos to improve revenues (a normal policy). But they don't give a damn that the chips in all slot machines are NOT fairly random. The chips are PROGRAMMED to improve the bottom line of the gambling operators. That translates to higher revenue for the casino operators, therefore higher revenues from taxes for the state governments. Who gives a damn about fairness and that cuckoo-speak concept of randomness? The taxpayers are hurting — the governments need money no matter in what ways, shapes, or forms the monies come in!

By the way: The players who won several times were not prosecuted — rightfully so! With one... blatant exception. What if the winners had insider information? You know, the state employees are not permitted to play the lotteries. But they might have "friends" who would play for them and share the profits! "Hey, bud! The Keno drawing of 8 p.m. today will be exactly the same tomorrow at 8PM."

Ion Saliu