Statistické testy NIST

V technické praxi se můžeme více či méně často setkat se statistickým testováním různých vlastností či výsledků funkcí nebo testováním náhodnosti jimi produkovaných binárních posloupností. Význam statistických testů náhodnosti je natolik důležitý, že tyto testy byly standardizovány v normě amerického úřadu pro standardy a technologie NIST. V minulém čísle ST jsme se o tomto balíku testů zmínili, a sice v souvislosti s objevem nových účinných postupů tureckých

Tabuľka 1 Sada testů NIST

číslo	Název testu
1	Frekvenční test (test rozdělení nul a jedniček)
2	Rozdělení jedniček a nul uvnitř bloků stejné dané délky
3	Test runů (tj. test počtů a délek úseků typu 1111..11 nebo 0...000)
4	Test nejdelšího runu v bloku (délka nejdelšího řetězce 1..11 při rozdělení posloupnosti do bloků stejné dané délky)
5	Test na hodnost binární matice
6	Spektrální test (diskrétní Fourierova transformace)
7	Nepřekrývající se vzorové řetězce (template)
8	Překrývající se vzorové řetězce
9	Maurerův univerzální statistický test
10	Test lineární složitosti
11	Test sérií
12	Test přibližné entropie
13	Test kumulativních součtů
14	Test náhodné procházky
15	Variantní test náhodné procházky

matematiků při testování kryptografických funkcí. Ti (kromě několika zvláštních testů) ve své podstatě udělali dvě věci – navrhli v první řadě strukturovaná vstupní data pro zkoumané funkce, aby se na jejich výstupu mohli odhalit nechtěné závislosti, a v druhé řadě způsob zpracování odpovídajících výstupních dat. Suma sumárum (kromě zmíněných několika zvláštních testů) však jejich výsledkem byla vždy nějaká posloupnost binárních dat. K jejímu testování se jim pak hodila standardizovaná sada NISTu.

Pochopitelně, na internetu je možné najít i konkurenční sady, např. SW balík Diehard. I když se zdá, že na statistických testech není nic zvláštního, neboť statistika je dost stará matematická věda, tyto balíky testů nejsou triviální a příroda nás v otázce náhodnosti stále vodí za nos. Na testovacím standardu NIST pracovali podle očekávání špičkoví američtí matematici i statistici, a přesto v nich byla nalezena řada drobných chyb, a dokonce jedna závažnější. Test rychlé Fourierovy transformace musel být dokonce z tohoto důvodu z balíku vyřazen. Původní standard z roku 2001 byl tak před několika měsíci nahrazen novou verzí [1], s kterou se nyní seznámíme.

Pozor na klasickou chybu při vyhodnocování

Ještě si neodpustíme malou realizační poznámku. Pokud máte jeden test a dostanete milion testových hodnot, jak se rozhodnete, že daná posloupnost je náhodná nebo ne? Prostě porovnáte obdržené hodnoty (resp. jejich rozdělení) s hodnotami, které byste očekávali, že dostanete při zkoumání kvalitní náhodné funkce. Toto jsme tedy zvládli a v rámci jednoho testu to umíme udělat. Pokud máme několik testů (N), téměř jistě budou tyto testy nějak závislé. To se projeví tak, že pokud nevyjde jeden test, z důvodu závislosti nevyjde i nějaký další. Typicky pokud nevyjde test rozdělení jedniček a nul, „vybouchnou“ velice pravděpodobně i jemnější testy, třeba rozdělení dvojic bitů. Proto není teoreticky správné aplikovat na jednu posloupnost všechny testy najednou. A přesto je to naprosto běžná věc a chyba, kterou se dopouští 99 % výzkumníků. Často si lámou hlavu nad tím, že jim nevychází testy dokonalé náhodné posloupnosti, protože součet všech překročení limitních hodnot u všech testů je vyšší, než by měl být. Není to tím, že by jejich funkce byly špatné, ale v tom, že testy jsou závislé a jedno „vybouchnutí“ je započteno vlastně několikrát. Přitom postačí jednoduše (ovšem N-krát pomaleji) aplikovat každý z testů na jinou (nezávislou) posloupnost.

Sada NIST

Tato sada obsahuje 15 základních testů, z nichž některé mají ještě tzv. podtesty. Například test, v němž se vyhledává určitý vzorový řetězec (template) ve zkoumané posloupnosti, má mnoho doporučených hodnot vzoru, čili pro každou hodnotu tohoto řetězce dostáváme tzv. podtest. Testovací sadu můžeme použít na binární posloupnost jakékoliv délky a pocházející z kryptografického hardwarového nebo softwarového zdroje náhodnosti. Pochopitelně je můžeme použít i pro nekryptografické účely! Sada testů je totiž velmi dobře popsána a zpracována a po deseti letech existence snad i bez chyb. K minulé sadě existoval odkaz, kde se na stránkách NIST dal stáhnout celý SW balík, dnes je velice nešťastně zastrčen na webu NISTu na linku http://csrc.nist.gov/groups/ST/toolkit/rng/batteries_stats_test.html..

Každý z testů je ve standardu [1] podrobně popsán jak na vyšší úrovni, tak na detailní technické úrovni ve zvláštní kapitole.

Parametry

NIST upozorňuje, že nejprve by měl být prováděn test rozdělení četností jedniček a nul, neboť když nevyhoví, pravděpodobnost, že nevyhoví ostatní testy, je vysoká. Dále se uvádí, že časově nejnáročnější je test lineární složitosti. V tomto případě se doporučuje nastavit si nízké parametry testu a změřit dobu skutečného běhu v konkrétním výpočetním prostředí a na základě časové kalkulace zadat parametry vyšší. Ostatně nasta-

$$z = \frac{x - \mu}{\sigma}$$

Obr. 1 Normované normální rozdělení

$$\chi^2 = \sum_{i=1}^{N} \frac{(x_i - n_i)^2}{n_i}$$

Obr. 2 Hodnota testu chí-kvadrát

vování a významu parametrů je ve standardu věnována celá kapitola.

Naproti tomu uživatelé nebudou muset věnovat příliš velkou pozornost teorii, neboť velká většina testů končí tím, že daná veličina daná vzorcem a realizovaná v daném SW má normované normální rozdělení. Pokud se jedná o málo diskrétních hodnot, jsou většinou roztříděny do intervalů a je na ně aplikován test chí-kvadrát, což je druhé a poslední rozdělení, se kterým se uživatel setká.

Ještě poslední poznámka předtím, než se na testy vrhnete, je k délce zkoumané posloupnosti. I když v teoretické části jsou použity příklady pro počet bitů např. $n = 10$, pamatujte, že dobré výsledky dostanete pro velmi dlouhé posloupnosti (megabajty, gigabajty apod.). Doporučené délky jsou vždy u každého testu popsány jako doporučovaná velikost hodnoty volitelného parametru (n) a je dobré je respektovat. Při nižších hodnotách se totiž neprojeví Zákon velkých čísel tak dokonale, jak nám ho příroda může poskytnout.

Vlastimil Klíma,
vlastimil.klima@knzsro.cz

LITERATURA:

[1] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo: NIST Special Publication 800-22, Revision 1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Revised: April 2010, Lawrence E Bassham, http://csrc.nist.gov/publications/ pubsSPs.html.