*mgr inż. Krzysztof Mańk*
*Wojskowa Akademia Techniczna*
*Wydział Cybernetyki*
*Instytut Matematyki i Kryptologii*

## Testy losowości dla nakładających się wektorów

W testowaniu generatorów ciągów losowych i pseudolosowych zawsze niemałą rolę odgrywały i wciąż odgrywają pieniądze, dające się w miarę liniowo wymieniać na czas. Oczywistym jest, że im większa próbka zostanie przebadana przy użyciu możliwie najpełniejszego zestawu testów, tym bardziej wiarygodny będzie końcowy werdykt. W przypadku użytych testów rzecz leży bardziej po stronie teoretyków i programistów, których zadaniem jest odpowiedni dobór i implementacja realizowanych testów, co również, ale już nietrywialnie, przekłada się na czas i pieniądze. Jeśli chodzi o objętość badanej próbki, nowy kierunek został wskazany przez zespół George'a Marsagli w opublikowanym w 1995 roku pakiecie testów DIEHARD. Pokazali oni, że rozpatrując badaną sekwencję liczb (bloków bitów) jako ciąg nakładających się $t$-elementowych wektorów, w którym dwa kolejne mają po $t-1$ wspólnych elementów, można uzyskać informację zbliżoną do przebadania $t$-krotnie dłuższej sekwencji, którą podzielono by na nienakładające się wektory. Testy losowości budowane w taki sposób mają jeden tylko, ale bardzo poważny mankament — bardzo trudno określić rozkład uzyskiwanej statystyki testowej, co więcej poważne kłopoty sprawia wyznaczenie wartości parametrów nawet dla rozkładów asymptotycznych. Widać to dobrze w oryginalnym pakiecie DIEHARD, gdzie w przypadku wielu testów znaleźć można informację, iż podane wartości wyznaczone zostały symulacyjnie. Jak pokazał czas, w niektórych przypadkach wyniki te były dalekie od prawdy.

W referacie zaprezentujemy zarówno obecny stan wiedzy, jak i własne wyniki.

Praca naukowa finansowana ze środków na naukę w latach 2010–2012 jako projekt rozwojowy Nr O R00 0111 12.