GENEROWANIE ROZDAŃ: TEORIA I PRAKTYKA

MICHAŁ KLICHOWICZ

KRAJOWA KURSOKONFERENCJA SĘDZIÓW IT

PZBS, GRUDZIEŃ 2018

JAK WYGENEROWAĆ ROZKŁAD? METODY INTUICYJNE

- „mieszanie” uporządkowanej talii (przez wielokrotną zamianę kart miejscami)
- losowanie ręki N/E/S/W, dla każdej karty, kolejno
- ???

Problemy:

- czasochłonne, niewydajne obliczeniowo
- często trudno skontrolować poprawność
- losowanie dużo większej liczby losowych danych niż potrzeba

ODROBINA …KRYPTOGRAFII

Liczby losowe w oprogramowaniu:

- komputery są deterministyczne, bardzo źle znoszą „losowość”
- „prawdziwe” (sprzętowe) źródła losowych danych nie są powszechne
- zamiast tego używa się tzw. PRNG

PRNG – *PSEUDO-RANDOM NUMER GENERATOR*

- potrzebują niewielkiej porcji „prawdziwie” losowych danych – tzw. ziarna
- z ziarna generują w deterministyczny sposób ciąg liczb
- ten ciąg na potrzeby oprogramowania jest nieodróżnialny od „prawdziwie” losowego ciągu liczb
- równomierny – wszystkie liczby mają równe prawdopodobieństwo wystąpienia
- nieprzewidywalny – z poprzednich liczb ciągu nie da się przewidzieć kolejnych
- PRNG po określonej liczbie wyrazów ciągu **traci** tę własność (staje się przewidywalny)

ODEJŚCIE OD INTUICYJNYCH METOD LOSOWANIA

- niepotrzebne „zużycie” losowych danych
- liczba wszystkich możliwych rozkładów rozdań:

$$\binom{52}{13} \times \binom{39}{13} \times \binom{26}{13} \approx 5.36 \times 10^{28} \approx 1.35 \times 2^{95}$$

- wystarczy wylosować **jedną** liczbę z przedziału $(0; 1.35 \times 2^{95})$
- w intuicyjnym sposobie #2 losowaliśmy 52 liczby z przedziału $(0; 2^2)$, czyli liczbę z przedziału $(0; 2^{104})$ - tylko jedno losowanie na **512** było prawidłowe!

BIGDEAL

- dla każdego rozdania losuje jedną liczbę o minimalnej niezbędnej długości (nie „marnuje” losowych danych)
- losuje od razu, w jednej operacji 96-bitową liczbę
- taka liczba przekształcana jest jednoznacznie w rozkład rozdania przy pomocy magii
- magia zapewnia przy okazji, że procedura nie oddaje ewentualnej „słabej” losowości w sposób mający brydżowe znaczenie

„SŁABA” LOSOWOŚĆ

A♠ K♠ Q♠ J♠ 10♠ 9♠ 8♠ 7♠ 6♠ 5♠ 4♠ 3♠ 2♠

00 00 01 10 11 11 01 10 10 00 01 10 11

N N E S W W E S S N E S W

00 00 01 10 11 11 01 10 10 00 01 10 11

Rozdanie nr 1825307

A♠ K♠ Q♠ J♠ 10♠ 9♠ 8♠ 7♠ 6♠ 5♠ 4♠ 3♠ 2♠

00 00 **00** 10 11 11 01 10 10 **01** 01 10 11

N N **N** S W W E S S **E** E S W

00 00 **00** 10 11 11 01 10 10 **01** 01 10 11

Rozdanie nr 776795

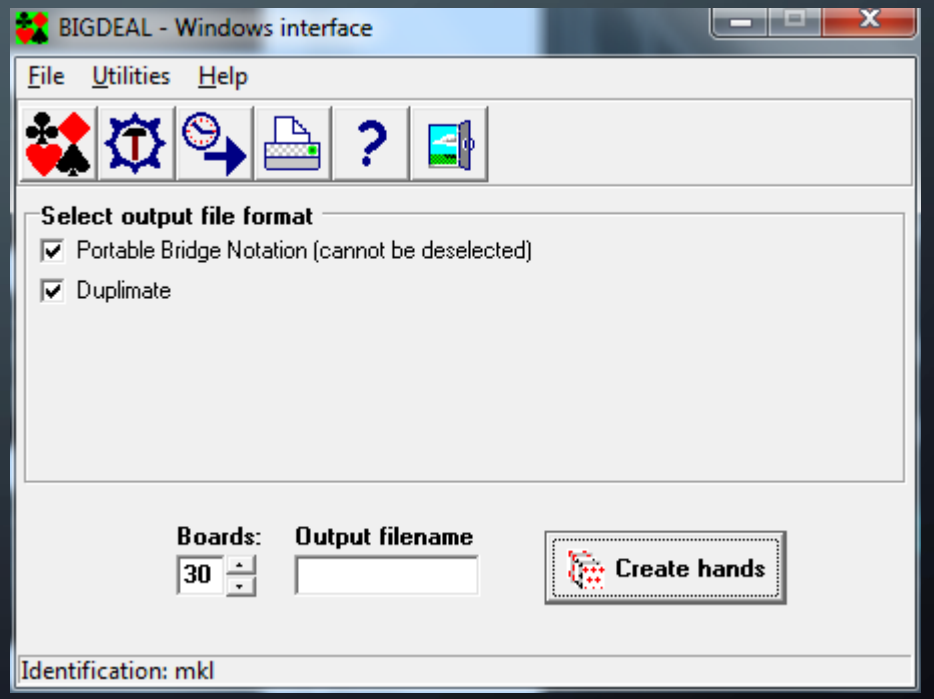
Zamieniliśmy miejscami jedynie dwie karty.

Kompletnie inne rozdanie!

BIGDEAL

Nakładka z interfejsem graficznym, umożliwiającym wydruk i archiwizację rozkładów, autorstwa Jasia Romańskiego:

http://jfr.pzbs.pl/bigden.htm



NIE UŻYWAMY INNEGO OPROGRAMOWANIA

- nie używamy oprogramowania przestarzałego
  na przykład: modułu „Rozdawaczka” w KoPSie
- nie używamy oprogramowania dostarczanego z maszynami powielającymi karty
- nie używamy jakiegokolwiek oprogramowania umożliwiającego ustawienie parametrów generowanych rozdań (Dealer, Analizator9000)

INGERENCJA W GENEROWANE ROZKŁADY

- przy używaniu BigDeala – jedynie „ręczna”
  - poprzez zmianę wygenerowanych rozkładów – czyli tak naprawdę nieużycie BigDeala
  - poprzez selekcję całych plików zestawów rozkładów
- kwestia zaufania i autorytetu organizatora i sędziego komputerowego
- istnieją sposoby, żeby poprawić (lub wręcz zagwarantować) wiarygodność wygenerowanych rozkładów

WIARYGODNOŚĆ GENEROWANYCH ROZKŁADY

- generować rozdania w obecności zawodników, np. po poprzednim turnieju
  - jak zagwarantować, że nie zostały podmienione?
- wygenerować wiele zestawów rozdań, pozwolić uczestnikom wybrać zestaw
  - powszechne np. w wyjazdowych meczach barażowych Drużynowych Mistrzostw Polski
- rozwiązanie kryptograficzne – SquareDeal
  - wprowadzone i używane w WBF
  - od bieżącego sezonu – również w Drużynowych Mistrzostwach Polski