Liczby losowe

Sprawozdanie z laboratorium 12 – Łukasz Konieczny, LK4

## 1. Wstęp teoretyczny

Liczby losowe są szeroko wykorzystywane w symulacjach, grach wideo czy kryptografii.

Z założenia, liczba losowa powinna być otrzymywana bez względu na poprzednie liczby w generowanej sekwencji i / lub czynniki zewnętrzne, jednak w praktyce jest to bardzo trudne do osiągnięcia, dlatego często gdy mówimy o liczbach losowych, mamy na myśli liczby pseudolosowe.

Liczby pseudolosowe uzyskuje się wykorzystując opracowane do tego zadania algorytmy co sprawia, że jeśli znamy kilka kolejnych liczb pseudolosowych oraz algorytm je wyznaczający, możemy bez problemu przewidzieć całą następną sekwencję, co w przypadku liczb prawdziwie losowych nie miałoby miejsca.

Podczas zajęć zapoznaliśmy się z „liniowym generatorem kongruentnym”, służącym do generacji sekwencji liczb pseudolosowych.

Jest on dany wzorem:

Gdzie ‘a’, ‘c’ oraz ‘m’ to dowolne współczynniki spełniające podane założenia:

* m > 0
* (a – 1) powinno być wielokrotnością każdego z czynników pierwszych ‘m’
* ‘c’ musi być względnie pierwsze w stosunku do ‘m’, czyli nie powinno mieć z nim żadnych wspólnych czynników pierwszych
* Jeśli ‘m’ jest podzielne przez ‘4’, (a – 1) też musi być podzielne przez ‘4’

Wartość startowa algorytmu, czyli jego ziarno, to , gdzie

## 2. Opis kodu

Moja implementacja powyższego algorytmu dzieli się na dwie funkcje przedstawione poniżej:

vector<int> wyznaczDzielnikiPierwsze(int x, bool wszystkie = false){

    vector<int> czynniki;

    int k = 2;

    int pierwiastek = sqrt(x);

    while(x > 1 && k <= pierwiastek){

        if(x % k == 0){

            czynniki.push\_back(k);

            x /= k;

            while(x % k == 0){

                if(wszystkie)

                    czynniki.push\_back(k);

                x /= k;

            }

        }

        k++;

    }

    return czynniki;

}

Funkcja „wyznaczDzielnikiPierwsze” wyznacza, w zależności od drugiego przyjmowanego parametru, wszystkie dzielniki pierwsze zadanej liczby, lub tylko pojedyncze wystąpienia danego dzielnika (tzn. jeśli liczba jest podzielna przez ‘2’ siedem razy, a parametr ‘wszystkie’ ma wartość ‘false’, w wektorze znajdzie się tylko jedna dwójka).

Zwracaną wartością jest wektor int’ów, ponieważ nie wiemy ile dzielników posiada sprawdzana liczba, więc nie możemy posłużyć się zwykłą tablicą.

vector<int> generuj(int xmax){

    int m = xmax + 1;

    cout << "Wyznaczone \"m\": " << m << endl;

    vector<int> czynniki = wyznaczDzielnikiPierwsze(m);

    int c = 1;

    for(int cz : czynniki)

        c \*= cz;

    c++;

    cout << "Wyznaczone \"c\": " << c << endl;

    int a = 1;

    czynniki = wyznaczDzielnikiPierwsze(m, true);

    for(int cz : czynniki)

        a \*= cz;

    a++;

    cout << "Wyznaczone \"a\": " << a << endl;

    vector<int> wynik;

    int xn = 0;

    do{

        xn = (a\*xn + c) % m;

        wynik.push\_back(xn);

    }

    while(xn != 0);

    return wynik;

}

Funkcja „generuj” wyznacza parametry ‘a’, ‘c’ oraz ‘m’ zgodnie z warunkami zadania, używając do sprawdzenia podzielności funkcji „wyznaczDzielnikiPierwsze”, a następnie z ich pomocą generuje sekwencję liczb pseudolosowych zgodnie z zadanym algorytmem, do momentu napotkania pierwszej powtarzającej się liczby. Zwraca wektor zawierający wygenerowaną sekwencję.

## 3. Wnioski

Podczas zajęć zapoznaliśmy się z definicją liczb losowych oraz pseudolosowych, opisaliśmy różnice między nimi oraz zaimplementowaliśmy algorytm generujący sekwencję liczb pseudolosowych.

## Bibliografia

<https://pl.wikipedia.org/wiki/Liczba_losowa>

<https://eduinf.waw.pl/inf/utils/010_2010/0213.php>

Materiały z wykładów – Zbigniew Kokosiński