

* Изследване на формули
за генериране на
случайни числа с
апарата на генетичните
алгоритми

ас. инж. Тодор Балабанов

Моделиране и оптимизация - ИИКТ - БАН / София -2013

- * Асистент в ИИКТ-БАН
- * Магистър по “Софтуерни технологии в Интернет”
- * Бакалавър по “Информатика”
- * Бакалавър-инженер по “Компютърни системи и технологии”
- * Специалист по “Технология на програмното осигуряване”
- * За контакт:
 - * Имейл: todor.balabanov@gmail.com
 - * Мобилен: 089 8237103
 - * Уеб: <http://tdb.hit.bg/>

*** ас. инж. Тодор Балабанов**

- * Генератори на случайни числа
- * Характеристики на случайните числа (критерии за качество)
- * Изчисления в разпределена среда
- * Кодирание на формули в генетични алгоритми
- * Реализация на научното изследване

Съдържание

- * Действително случайни числа
- * Генерирани на база на физически явления в микро света
 - * Полуразпад на радиоактивни елементи
 - * Спин на фотони
 - * Топлинен шум
- * Генерирани на база на физични явления от макро света
 - * Заснемане на облачно небе
 - * Заснемане на лава лампи

Хардуерни генератори

- * Генериране с помощта на формула
 - * Всяка следващата стойност е в следствие на функционална зависимост от предишните
 - * Инициализиране на генератора със случайно събитие от реалния свят
- * Линеен конгруентен генератор
 - * Един от най-разпространените
$$X_{n+1} = (a * X_n + c) \% m$$
- * Мерсенн туйстър
 - * Един от най-надеждните

Генератори на псевдо-случайни числа

- * Бързодействие
- * Статистически приемливо разпределение
- * Определяне на качеството
 - * Дайхард тестове

Характеристики на PRNG

- * Разделяне на изчислителния ред, така че различни части от пресмятането да се извършват едновременно
- * Изпълнение на програмен код на различни процесори (ядра) в един и същи момент от времето
- * Изпълнение в рамките на една изчислителна машина

Паралелни изчисления

- * Вид паралелни изчисления
- * Кодът се изпълнява на физически различни машини
- * Хетерогенна система
- * Мрежова латентност
- * Акцент над сигурността, когато изчисленията се извършват на машина под чужд контрол

Изчисления в разпределена среда

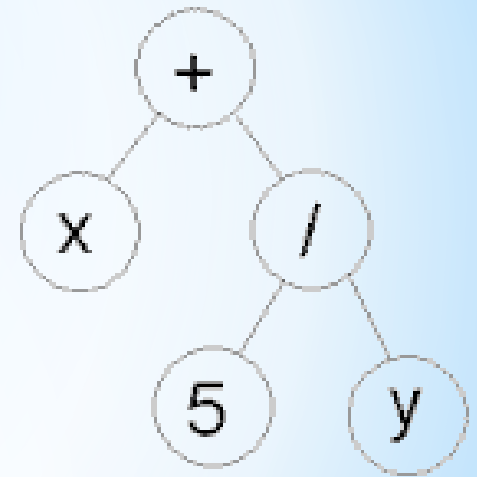
- * Генетични алгоритми
 - * Представяне на информацията в хромозоми (отделни индивиди)
 - * Кръстосване
 - * Мутация
 - * Естествен подбор
- * Математически изрази
 - * Последователност от операнди и операции
- * Представяне на математическите изрази като хромозоми в генетичните алгоритми

Математически изрази част от ГА

- * Аритметичен израз представен като дървовидна структура

$$z = x + (5 / y)$$

- * Кръстосването е “срязване” на дървото в определен възел и размяна
- * Мутацията е модифициране на операнд или операция (на случаен принцип)
- * Естественят подбор е според зададен критерий за качество



Дървовидно представяне в ГА

- * Оптимизират се два основни критерия
 - * Бързодействие за пресмятане на всяка следваща стойност
 - * Статистически приемливо разпределение на числата (максимално наподобяване на случайност)
 - * Оценка с помощта на Дайхард тестовете

Критерии за естествен подбор

- * Стартиране на BOINC сървър
- * Включване на свободно разпространяваща се библиотека за изчисляване на аритметични изрази
- * Включване на свободно разпространяваща се библиотека за проверка по Дайхард тестовете
- * Имплементация на генетичен алгоритъм

Реализиране на изследването

- * Изпробват се формули на различни локални машини
- * Най-добрите резултати, открити локално, се изпращат на отдалечения сървър
- * Ползата от смятането в разпределена среда е, че се изпробват множество формули (междинни резултати), които никога не стават част от окончателното решение

Изследването в разпределена среда

Благодаря за вниманието!

Въпроси и отговори

- * Hardware random number generator -
http://en.wikipedia.org/wiki/Hardware_random_number_generator
- * Linear congruential generator -
http://en.wikipedia.org/wiki/Linear_congruential_generator
- * Mersenne Twister -
http://en.wikipedia.org/wiki/Mersenne_twister
- * Diehard tests - http://en.wikipedia.org/wiki/Diehard_tests
- * Dieharder -
<http://www.phy.duke.edu/~rgb/General/dieharder.php>

Допълнителни информационни източници

Acknowledgement

This research is supported by the project

АComIn "Advanced Computing for Innovation",

grant 316087, funding by FP7 Capacity Programme,
Research Potential of Convergence Regions (2012-2016)