Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Realizacja szyfru „bezkluczowego" c80k395 do kryptograficznej ochrony załączników poczty elektronicznej w środowisku Maple

Maple implementation of „Keyless" Cipher c80k395 for cryptographic protection of e-mail enclosures

Czesław Kościelny

Treść. Opisano przykład aplikacji typu workhsheet, uruchamianej w środowisku Maple i realizującej procedury „bezkluczowego" szyfrowania i deszyfrowana plików za pomocą symetrycznego szyfru plikowego c80k395. Aplikacja posiada prosty graficzny interfejs użytkownika i przeznaczona jest głównie do kryptograficznej ochrony załączników poczty elektronicznej.
Słowa kluczowe: kodowanie transportowe, funkcja Maple convert/base, szyfrowanie symetryczne plików.

Abstract. An example of a Maple worksheet application which performs the „keyless" file encryption or decryption by means of the symmetric cipher c80k395 has been presented. The application has a simple graphical user interface and may be used mainly for cryptographic protection of e-mail enclosures.
Keywords: Base 64 Encoding Scheme, Maple convert/base built-in function, Symmetric File Encryption.

Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Operacyjne i analityczne bazy danych wspomagające procesy decyzyjne w zarządzaniu uczelnią wyższą

Transactional and analytical databases to support decision-making in the management of a university

Swietłana Lebiediewa

Treść. Przedstawiono charakterystykę użytkowników bazy danych i potrzeby różnych grup użytkowników. Omówiono zawartość informacyjną bazy danych. Omówiono rolę bazy danych w zarządzaniu szkołą wyższa dotyczącą dwóch aspektów: zarządzania operacyjnego i podejmowania decyzji strategicznych. Przytoczono przykłady informacji potrzebnej do podejmowania decyzji operacyjnych i strategicznych.
Słowa kluczowe: baza danych, zarządzanie, wyższa szkoła niepaństwowa

Abstract. The characteristics of database users and the needs of different user groups are presented. The information content of the database is discussed. Database role in the management of university on two aspects: operational and strategic decision-making is discussed. Examples of information needed to make operational and strategic decisions are quoted.
Keywords: database, management, non-public university

Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Application of Monte Carlo method in the computer system for valuation of exotic option contracts

Zastosowanie metody Monte Carlo w informatycznym systemie wyceny egzotycznych kontraktów opcyjnych

Hubert Zarzycki

Treść. W artykule prezentowana jest propozycja komputerowego systemu obliczania finansowych instrumentów pochodnych – opcji egzotycznych i hybrydowych. Handel takimi produktami odbywa się na rynku pozagiełdowym (OTC) i często są to produkty tworzone na zlecenie. Wartości pewnych rodzajów opcji egzotycznych i hybrydowych nie można wyliczyć tradycyjnymi analitycznymi i numerycznymi metodami. W takich przypadkach warto użyć metody Monte-Carlo do wyceny rzeczywistej wartości instrumentów finansowych. W artykule przedstawiony został sposób obliczania ceny przykładowej opcji egzotycznej za pomocą metody MC. System komputerowy oparty o MC mógłby służyć do wspomagania decyzji inwestycyjnych dotyczących egzotycznych kontraktów opcyjnych.
Słowa kluczowe: metody Monte-Carlo, systemy wspomagania decyzji, opcje egzotyczne i hybrydowe, inżynieria fi-nansowa, wycena kontraktów opcyjnych

Abstract. This paper presents a proposal for a computer system of calculation of financial derivatives - exotic and hy-brid options. The trade of such products takes place on the OTC market and these products are often made and tailored on demand. The values of certain types of exotic and hybrid options cannot be calculated with traditional analytical and numerical methods. In such cases, it is worth to use the Monte-Carlo method for the valuation of the real value of financial instruments. This paper presents an example of calculating the price of exotic options using the MC method. The computer system based on MC could be used to support investment decisions regarding exotic option contracts.
Keywords: Monte-Carlo methods, decision support systems, exotic and hybrid options, financial engineering, valu-ation of option contracts

Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Nowa implementacja algorytmu mrówkowego wykorzystująca technologię przetwarzania wieloprocesorowego i rozproszonego w systemie nawigacji

A new implementation of an ant algorithm using multiprocessor and distributed computing technologies in navigation system

Daniel Komar

Treść. Artykuł ma na celu przybliżenie czytelnikowi problemu wyboru najlepszej trasy podróży pomiędzy dwoma punktami, która będzie minimalizowała liczbę negatywnych czynników wpływających na osobę kierującą pojazdem. Zaprezentowany zostanie nowo zaimplementowany algorytm mrówkowy, który został przystosowany do wykorzystania w pełni możliwości obliczeniowych współczesnych systemów wieloprocesorowych i rozproszonych. Autor przeprowadzając eksperyment w warunkach rzeczywistych, ukaże wyższość opracowanego rozwiązania nad stosowanym obecnie tradycyjnym systemem nawigacji. Przeprowadzone badania wykazały, że wykorzystywana nowa implementacja algorytmu w znacznym stopniu zmniejsza czas przejazdu i liczbę czynników zakłócających mających bezpośredni wpływ na osobę kierującą pojazdem.
Słowa kluczowe: algorytm mrówkowy, nawigacja, czas podróży, warunki drogowe

Abstract. The purpose of this paper is to give reader an understanding of the problem of the best itinerary selection between two points which will minimize the number of negative factors affecting the person driving a vehicle. The author will present an entirely new implementation of an ant algorithm that was adapted in order to make the most of computational capabilities of modern multiprocessor and distributed systems. Having performed experiments in real-world conditions, the author demonstrates, that the new solution is superior to the traditional navigation system which is still used today. The conducted research showed that the new implementation of the algorithm significantly contributed to reduction of journey times and the number of confounding factors which have a direct impact on the person driving a vehicle.
Keywords: ant algorithm, navigation, journey times, driving conditio

Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Hybrydowy algorytm mrówkowy wykorzystujący algorytm genetyczny do wyznaczania trasy w systemie nawigacji

A hybrid ant algorithm using genetic algorithm to determine the route in navigation system

Daniel Komar

Treść. Artykuł ma na celu zaprezentowanie nowej implementacji hybrydowego algorytmu mrówkowego, który do rozwiązywania postawionego problemu wyznaczenia optymalnej trasy przejazdu będzie wykorzystywał również algorytm genetyczny. Autor przedstawi wyniki symulacji przeprowadzonej na podstawie rzeczywistych danych, ukazując znaczny wzrost efektywności rozwiązywania problemu. Otrzymane wyniki wykazały, że nowy algorytm wyznaczał w większej liczbie przypadków znacznie krótszy czas przejazdu, a tym samym redukował występujące czynniki zakłócające i negatywnie wpływające na osobę kierującą pojazdem.
Słowa kluczowe: algorytm mrówkowy, algorytm genetyczny, system nawigacji

Abstract. The purpose of this paper is to present the new implementation of a hybrid ant algorithm that will also use a genetic algorithm in order to solve the problem consisting in optimal route calculation. The author will present results of simulations that were performed based on real data and showed a significant increase of problem solution effectiveness. The obtained results proved that the new algorithm determined in more number of cases a significantly shorter journey time and in consequence reduced the occurring confounding factors which had a negative impact on the person driving a vehicle.
Keywords: ant algorithm, genetic algorithm, navigation system

Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Weryfikacja „słabej" hipotezy Goldbacha do 1031

Verifying the „weak" Goldbach conjecture up to 1031

Łukasz Świerczewski

Treść. Praca prezentuje aspekt numerycznej weryfikacji „słabej" hipotezy Goldbacha dla wartości mniejszych niż 1031. Do obliczeń, które zajęły w sumie ok. 50 000 godzin czasu pojedynczego CPU wykorzystano klaster wydajnościowy złożony z procesorów AMD Opteron 4284. Podczas sprawdzania pierwszości zastosowano test Millera-Rabina. Przetestowano także możliwe zastosowanie testu ECPP. Jak się okazało przy założeniu dodatkowych warunków poprawności testu Millera-Rabina „słaba" hipoteza Goldbacha w badanym zakresie jest prawidłowa.
Słowa kluczowe: teoria liczb, hipoteza Goldbacha, liczby pierwsze

Abstrackt. This paper presents aspect of the numerical verification a „weak" Goldbach's conjecture for values less than 1031. For calculations, that took about 50 000 hours of a single CPU performance, there was used an performance cluster consisting of the AMD Opteron 4284 processors. During the primality check, there was used Miller-Rabin test. There was also tested the possiblity of ECPP test usage. As it turned out, when there were added some additional conditions of correctness of Miller-Rabin test, the „weak" Goldbach's conjecture occurs correct in researched range.
Key words: number theory, Goldbach conjecture, primes

Biuletyn Naukowy Wrocławskiej Wyższej Szkoły Informatyki Stosowanej
Informatyka nr 3 2013

Intel Manycore Testing Lab - środowisko sprzętowo-programowe do dydaktyki tworzenia i testowania efektywności równoleglizacji oprogramowania

Intel Manycore Testing Lab - hardware and software environment focused on didactic of development and efficiency testing in software paralleling

Łukasz Świerczewski

Treść. Współczesny proces dydaktyczny technik programowania często wymaga dostępu zarówno do nowoczesnego sprzętu, jak i oprogramowania. W szczególnej mierze odnosi się to do algorytmów równoległych, których odpowiednie właściwości w dużo większym stopniu można zaobserwować na wydajnych procesorach nowej generacji. Aby stworzyć międzynarodową społeczność akademicką związaną z tą specjalizacją firma Intel udostępniła wirtualne laboratorium testowe (Manycore Testing Lab - MTL). Artykuł przedstawia aspekt architektury oraz praktycznego zastosowania MTL w pracy wieloużytkowej i skupia się na empirycznym potwierdzeniu wzrostu wydajności uzyskanej dzięki programowaniu równoległemu i10-rdzeniowym procesorom Westmere-EX. Badaniom objęto cztery klasy algorytmów: czysto matematyczny dotyczący problemu Collatza, kryptograficzny 3DES, kwantowy algorytm Grovera oraz klasyczny algorytm genetyczny. Dla zastosowań edukacyjnych dostęp do laboratorium jest bezpłatny, a udostępniane platformy wspierają wszelkie zaawansowane technologie.
Słowa kluczowe: wirtualne labolatorium, wirtualny eksperyment, programowanie równoległe, Manycore Testing Lab

Abstract. The modern didactic process of programming techniques often requires access to the modern hardware and software. In a particular part applies to parallel algorithms, where appropriate properties to a much greater extent can be seen in the new generation of high-performance processors. To create an international academic community associated with this specialization, Intel released a virtual test lab (Manycore Testing Lab - MTL). The paper presents the architectural aspect and the practical application of MTL at work reusable and focuses on empirical confirmation gains obtained through parallel programming and 10-core Westmere-EX processors. The study consisted of four classes of algorithms: for a purely mathematical problem Collatz, 3DES cryptography, quantum Grover algorithm and the classic genetic algorithm. For educational access to the laboratory is free and available to all platforms support advanced technologies.
Key words: virtual labolatory, virtual experiments, parallel programming, Manycore Testing Lab