INTISARI

AKSELERASI ALGORITMA AKS DENGAN MPI DAN OPENMP PADA PERMASALAHAN PENGUJIAN BILANGAN PRIMA

Ardhi Wiratama Baskara Yudha

12/334773/PA/15003

Bilangan prima yang sangat besar banyak digunakan oleh algoritma kriptografi untuk melakukan enkripsi dan dekripsi. Salah satu di antaranya adalah algoritma RSA yang saat ini banyak digunakan untuk mengamankan transaksi perbankan. Namun sampai saat ini belum ada algoritma deterministik yang efisien untuk menentukan primalitas sebuah bilangan. Algoritma deterministik yang terbaik di dunia saat ini adalah algoritma AKS yang memiliki asimtotik polinomial namun belum dapat digunakan secara praktik.

Pada penelitian ini diimplementasikan algoritma AKS secara paralel dalam 1 dan 2 tingkat paralelisasi dengan MPI dan OPENMP yang lebih *load balance*. Terdapat 3 strategi paralelisasi dan 3 teknik *load balancing* yang diusulkan. Untuk menangani masukan bilangan yang besar digunakan pustaka GMP yang dapat menangani berapa pun panjang masukan yang diberikan. Untuk menangani struktur data polinomial dan fungsi pemangkatan polinomial modular yang cepat digunakan pustaka NTL. Program ini dijalankan pada sebuah HPC.

Pada penelitian ini diperoleh hasil bahwa teknik paralelisasi 1 tingkat MPI dengan 1 *core* 1 proses lebih cepat dari pada teknik paralelisasi MPI dengan 1 *node* 1 proses dan teknik paralelisasi 2 tingkat dengan MPI dan OPENMP. Selain itu teknik *load balancing* 2 lebih baik dari 2 teknik lainnya yang diusulkan. Dengan demikian teknik paralelisasi 1 *core* 1 proses dengan menggunakan teknik *load balancing* 2 menjadi yang tercepat. Diperoleh *speed up* sebesar 39 kali lipat ketika dijalankan pada 23 *node*.

Kata kunci: algoritma AKS, pengujian bilangan prima, implementasi hibrid MPI dan OPENMP

ABSTRACT

ACCELERATING AKS ALGORITHM WITH MPI AND OPENMP ON PRIMALITY TESTING PROBLEM

Ardhi Wiratama Baskara Yudha

12/334773/PA/15003

Big prime used in various cryptographic algorithms for doing encryption and decryption. For example RSA algorithm used big prime for encryption and decryption. RSA now widely used to secure banking transaction. Nowadays there is no efficient deterministic algorithm for primality proving. The best deterministic algorithm for primality proving is AKS algorithm asymptotically running in polynomial time although impractical used.

In this research AKS algorithm have been implemented on 1 and 2 level parallelization using MPI and OPENMP. Three different parallelization strategies and load balancing strategies have been implemented. GMP library used to handle big arbitrarily large integer and NTL library used to handle polynomial data structure and modular exponentiation operation. These implementations run on HPC.

In this research show experimentally that 1 level parallelization strategy with 1 core 1 process faster than 1 level parallelization with 1 node 1 process and 2 level parallelization with MPI and OPENMP. Furthermore load balancing strategy 2 better than the others two proposed strategy. Therefore parallelization strategy 1 core 1 process and load balancing strategy 2 become the fastest. Obtained 39 times speed up runs on 23 node.

Keyword: algoritma AKS, primality proving, hybrid MPI and OPENMP implementation