IMPLEMENTATION OF QUADRATIC SIEVE ALGORITHM USING MPI

By Kiran Kumar

CSE 633 Parallel Computing Fall 2011

About Quadratic Sieve

- Quadratic sieve algorithm is used for factoring large composite numbers.
- The mains steps in the algorithm :
  1. Generating the factor base.
  2. Generating polynomial
  3. Sieving
  4. Gaussian Elimination

Generating Factor Base

- Factor base consists of sets of numbers which is quadratic residue modulo of the number which is to be factored i.e., which satisfies the below equation.

$$n \equiv r^2 \pmod{p},$$

where r= floor(sqrt(n)) + k

k= 1,2,…

n→ integer to be factored

p→ a prime number below a bound B

Generating Polynomial

- We chose polynomial of type

  $f(x) = Ax^2+Bx+c$

  Where we chose A to be a square

  we chose B $0<=B<A$ such that B^2 is congruent to n mod(A)

  And finally we chose C which satisfies $B^2-AC=n$

- We can generate different polynomials by changing the values for A,B,C.

Sieving

- This is the most time consuming step in the algorithm.
- We solve the the polynomial f(x) for each value of the factor base.
- We loop through each element in factor base and check if f(x) completely factors using the prime numbers within the bound.
- If we find the f(x) which completely factors, we save the exponents of the factors in a matrix and continue the loop. We need to find many relation because most of the times we get trivial solutions.
- And finally Gaussian row reduction is applied on the exponent matrix and first non-trivial solution is given back as output.

Parallel Implementation

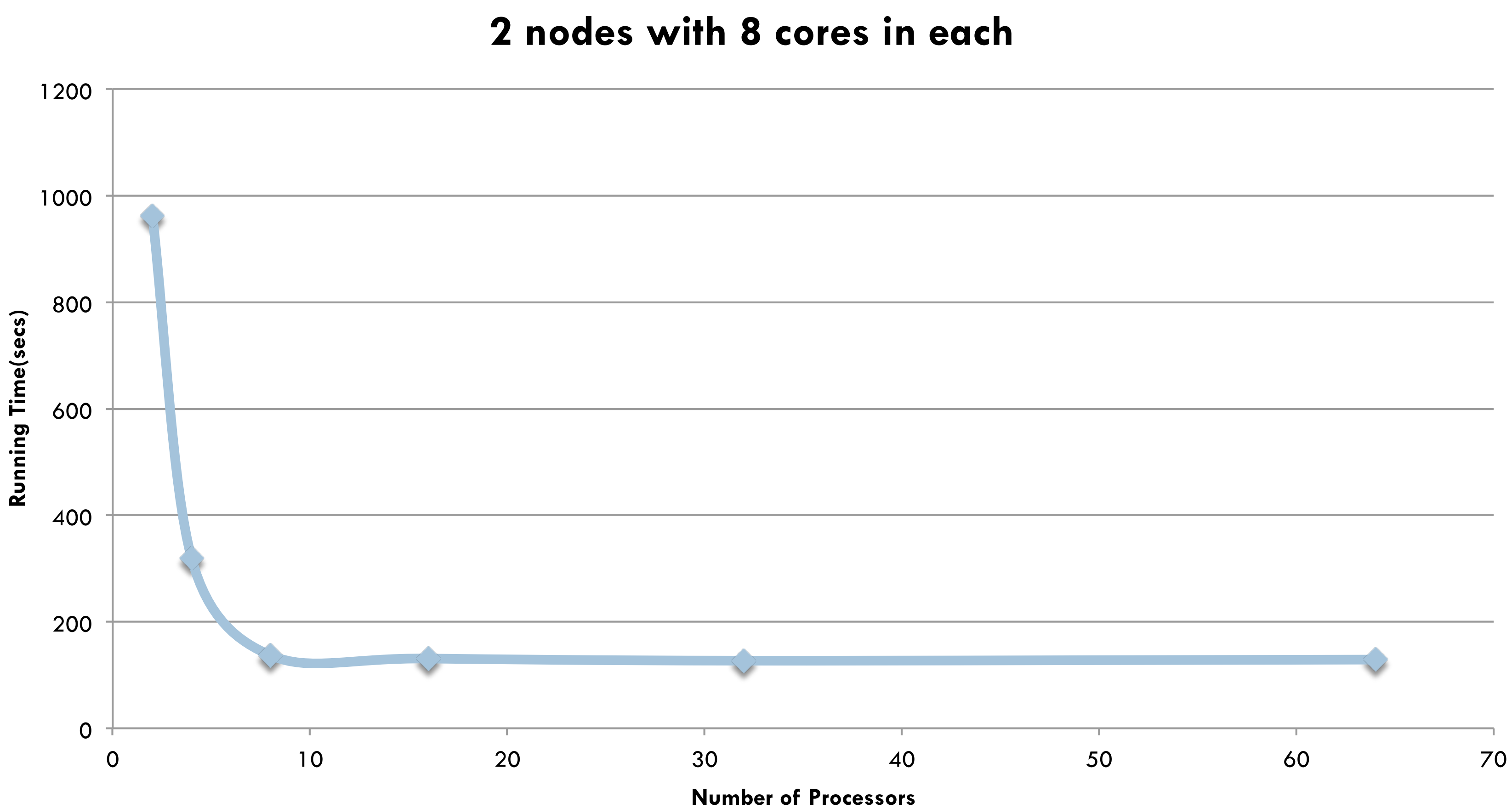
- The master the nodes initializes the variables and waits for the clients to request for job.
- The client node requests for n(the number to be factored) and then generates the factor base. Calculates the exponents A,B,C and generate the polynomial and starts sieving over the sieving interval.
- If the client node finds a solution, it sends the value back to master node
- After gathering the enough relations, the master node performs the Gaussian elimination and prints out the result and terminates the clients.

Results

- 2 nodes with 8 cores in each node.
- Input is 60 digit number

No Of Processors	Running Time(secs)
2	962
4	319
8	137
16	131
32	127
64	129

Results Contd..

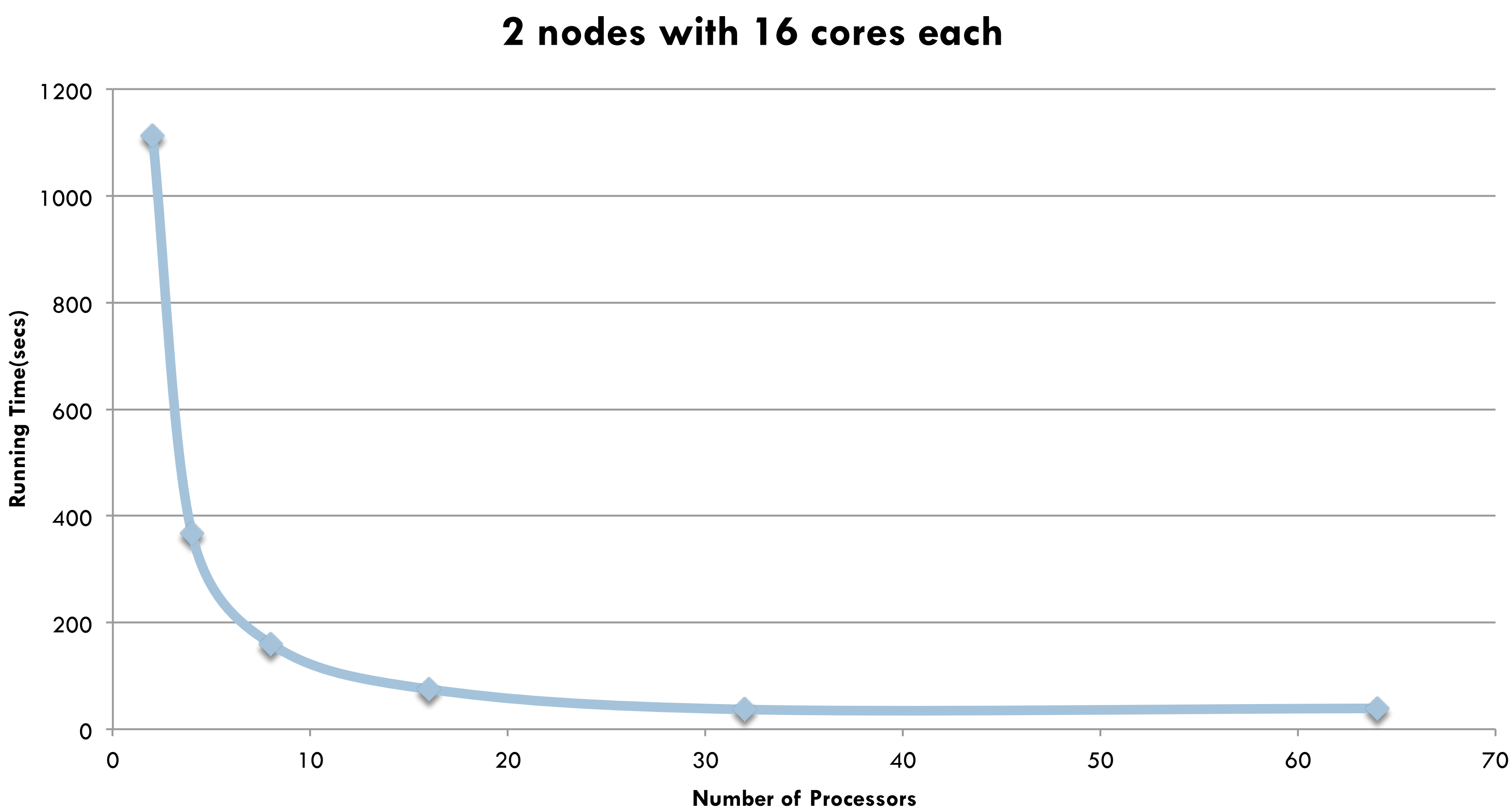


Results contd..

- 2 nodes with 16 cores each on one node.
- Input is 60 digit number.

No Of Processors	Running Time(secs)
2	1113
4	367
8	160
16	75
32	37
64	39

Results contd…

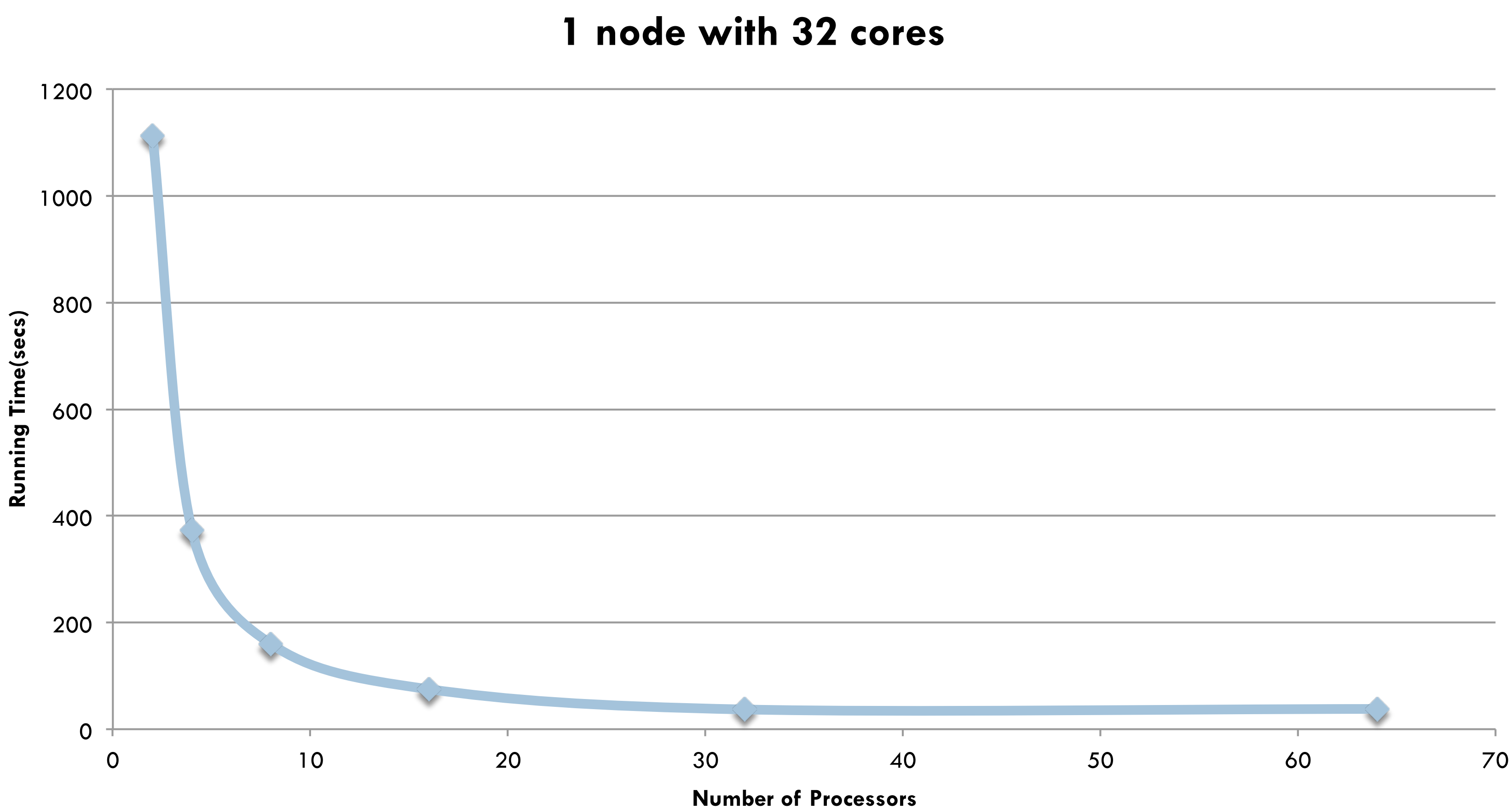


Results contd..

- 1 node with 32 cores on it.
- Input is 60 digit number

No Of Processors	Running Time(secs)
2	1113
4	373
8	160
16	75
32	37
64	38

Results cond…



References

- http://www.cs.virginia.edu/crab/QFS_Simple.pdf
- http://www.math.leidenuniv.nl/~reinier/ant/sieving.pdf

Questions?