Statement of Research

Ka.Shrinivaasan, M.Sc(CS), Chennai Mathematical Institute (CMI)
(shrinivas@cmi.ac.in)

May 29, 2010

1 Research interests

Computational number theory, Graph and Combinatorial Algorithms (problems in http://www2.research.att.com/ dsj/nsflist.html), Program analysis and Verification, Distributed Algorithms and Complexity

2 Factorization

2.1 Description

This problem talks about factoring a composite integer z into two integers x and y (both possibly primes).

2.2 Relevance and Current status

All known algorithms for factorization take exponential time in the length of input integer. This problem is a good example of search vs decision paradox. Deciding whether a number is prime is in P by AKS algorithm (polynomial in length of input bits) but searching for the factors is still elusive and no polynomial algorithm has been found yet except for Shor's algorithm for Quantum computers (in Bounded Quantum Error Polynomial - BQP). Decision version of Factorization lies in intersection of P and coNP. Best known algorithm for factorization is the General number field sieve algorithm which takes time

$$O(exp[(64/9 * logn)^a * (loglogn)^b]) \tag{1}$$

where a = 0.33 and b = 0.66

2.3 Methodologies that might be required to find a polytime algorithm

Randomization might help in finding a polynomial time algorithm though not better - Since factorization is in BQP, it will be reasonable to ask if it is in BPP (Bounded error probabilistic polynomial).Victor Shoup's book discusses one such probabilistic polytime algorithm. Since it is widely believed that BPP = P (i.e randomization does not achieve extensive speed up), if factoring is in BPP then it should be in P.

3 Edge partitioning a planar graph into two outerplanar graphs

3.1 Description

This problem talks about edge partitioning a planar graph into two outerplanar graphs

3.2 Relevance and Current status

Partitioning a graph has many applications in electronics. This problem was discussed as part of Graph Theory course in M.Sc and an algorithmic solution for the dual of the above problem was tried out in endsem exam (sketch given below). Best known result is discussed in paper "Edge Partition of Planar Graphs into Two Outerplanar Graphs" by Daniel GonÃğalves (LaBRI, U.M.R. 5800, UniversitÃľ Bordeaux 1, 351, cours de la LibÃľration 33405 Talence Cedex, France)

3.3 Methodologies that might be required

Given the dual (3-regular face graph of triangulated planar graph)

- Given the edge set E of the graph G, partition E into two sets E1 and E2 of size n and n if $|E|$ is even or two sets of size $n-1$ and $n+1$ if $|E|$ is odd such that each vertex is listed in both sets.
- Merge two paths in Ei if one of the endpoints of paths match and no cycle is formed.
- Repeat previous step till no new path is formed by the merger