Reiknirit, rökfræði og reiknanleiki

Magni Þór Birgisson

skil 10

1 Exercise 7.8 bls 272

Show that primality testing is solvable in plynomail time if we use a unary encoding rather than a binary encoding for numbers. In other words, show that the language UNARY-PRIMES = $\{1^n | n$ is prime$\}$ is in P.

Við getum prófað hvort p sé prímtala með að deila 2 til $\sqrt{n}$ og athugað hvort það gangi upp í p. Deilunin er hægt að framkvæma í margliðutíma.

Einnig er búið að finna lokaða formúlu fyrir prímtölur.

2 Exercise 7.19 bls 272

Let DOUBLE-SAT = $\{< \phi > | \phi$ has at least two satisfying assignments $\}$. Show that DOUBLE-SAT is NP-complete.

SAT $\leq$ DOUBLE-SAT
SAT er NP-complete

Við búum til vörpun úr SAT yfir í DOUBLE-SAT með að bæta að $\phi' = \phi \wedge (x \vee \bar{x})$ ϕ' það mun hafa mynsta lægi tvær lausnir og hægt er að búa til vörpunina í margliðutíma.

3 Exercise 7.25 bls 274

Let $U = \{< M, x, 1^t > | M$ is an NTM that accepts input x within t steps $\}$. Show that U is NP-complete.

SAT $\leq$ U

NP er það sem tekur briðgeng turing vél að finna lausn á margliðutíma og venjulega turingvél að fara yfir á margliðutíma.
Þannig að það er hægt að leysa þetta á NP-complete. Því keyrslu tíminn er ekki meiri en lengdin á inputinu sinnum fasti. Hægt er að sannreyna svarið á margliðutíma.

4 Exercise 7.29 bls 274

Show that, if P = NP, we can factor integers in plynomial time. (Note: NP is a class of languages and factoring problem if a function. Thus simply saying that, "becuse factoring is in NP, you are done" ins't enough.)

Factor er hjartað í RSA tulkóðun. Bankarnir yrðu hræddir ef það tæki margliðutíma að brjóta lásanna þeirra.
Ekki er búið að sanna að P = NP eða P $\neq$ NP

5 Exercise 7.30 bls 274

Let MAX-CLIQUE = $\{< G, k > \mid$ the largest clique of G has k vertices $\}$. Whether MAX-CLIQUE is in NP in unknown. Show that if P = NP, then MAX-CLIQUE is in P, and a plynomial time algoritm exist thatm for a graph G , finds one of its larges cliques.

Samkvæmt theorem 7.20 (bls 246) nota hana svo með fjölda punkta í hnitakerfinu. Fáum við þá að þetta er NP vandamál.

6 Exercise 7.33 bls 274

Describe the error in following gallacius "proof" that P $\neq$ NP. Consider an algorithm for SAT: "On input ϕ."This algorithm clearly requires exponential time. Thus SAT has exponential time complexity. Therefore SAT is not in P. Because SAT is in NP, it must be true that P is not equal to NP.

Til er betri algrím fyrir SAT sem þarf ekki "exponential time".
Sjá bls 254 í Sipser