Vijfde Serie Opgaven

1. Dit is een programmeeropgave. Op veel plaatsen, bijvoorbeeld www.prime-numbers.org kunnen priemgetallen van beperkte grootte worden gevonden. Als $n = pq$ met p en q priemgetallen, e relatief priem is met $\phi(n) = (p-1)(q-1)$ en d de inverse is van e in $\mathbb{Z} \bmod \phi(n)$, dan kan een bericht $M < n$ gecodeerd worden als $C = M^e \bmod n$ en C kan weer gedecodeerd worden als $C^d = (M^e)^d \bmod n = M$ (zie syllabus p80). Neem twee priemgetallen, kies een geschikte e, bereken d m.b.v. de uitgebreide Euclidische algoritme en codeer en decodeer "Hello World". (Merk op: voor $M < n$ moet uw bericht misschien in gedeelten worden verzonden). Om uw programma te testen, zal ik priemgetallen in de buurt van 9929802349 gebruiken.

2. Voor het gemak beschouwen we alleen Turing machines met één band en bandalfabet $\{0, 1\}$. Het geheugen dat een Turingmachine in een berekening gebruikt is het aantal bandcellen dat beschreven wordt. Ook het geheugengebruik is een functie van de lengte van de invoer, en de lengte van de invoer is het aantal niet blanco bancellen aan het begin van de berekening.

   Laat zien dat er een taal bestaat die geaccepteerd wordt door een Turingmachine die $O(n^2)$ geheugen gebruikt, die door geen enkele Turingmachine die $O(n)$ geheugengebruik geaccepteerd kan worden. (Kijk naar het bewijs voor P en EXP.)

3. Laat zien dat er geen Turingmachine M_0 kan bestaan die van elk ander Turingmachineprogramma p kan zeggen of p ooit een 0 zal afdrukken als p gestart wordt op blanco invoer.

4. Waarom zitten de volgende problemen in NP?

   (a) SAUCIJSJES Gegeven een verzameling van k snackbars en een verzameling van j klanten. Gevraagd: als snackbar i een capaciteit van $c(i)$ saucijsjes per uur heeft, en iedere klant $h(i)$ saucijsjes per uur kan opeten. Kunnen de klanten dan zo over de snackbars verdeeld worden dat niemand honger krijgt?

   (b) MAXFLOW Gegeven een gerichte graaf N met capaciteiten langs de kanten, en een getal k. Gevraagd: is de maximale stroom in N groter dan k?

   (c) CELLPHONE CAPACITY. Gegeven is een aantal personen, elk op een vaste plaats. Twee personen kunnen met elkaar praten als ze in elkaars bereik zijn. Iedereen die dan ook in het bereik van één van deze twee is, moet dan stil zijn, anders is er interferentie. Gegeven N personen en hun posities en een getal k. Gevraagd, kunnen er tenminste k gesprekken tegelijk gevoerd worden?