

Vijfde serie sommen.

1. Alice en Bob wisselen sleutels uit met de Diffie-Hellman-methode uit de syllabus. De getallen Y_A en Y_B worden over een open kanaal uitgewisseld en zijn dus voor iedereen zichtbaar.
 - (a) Zoek op of bedenk, en leg uit. Waarom heeft Claire, die de uitwisseling van informatie kan zien daar niet veel aan om achter X_A of X_B te komen?
 - (b) Zou Claire misschien toch wat kunnen leren waarmee ze de boodschappen van Alice en Bob die met de uitgewisselde sleutel K verzonden worden zou kunnen lezen? Zo nee, waarom niet, zo ja, hoe?
2. Een Turingmachine M begint met x en y geschreven in binair op de band (er is maar één band), met tussen x en y een $\#$. Per definitie is de rest van de band gevuld met blanco symbolen (B). De lees-schrijfkop staat op het eerste bit van x en de toestand is q_0 . Een Random Access Machine R begint met dezelfde x en y in binair in de eerste $|x| + |y| + 1$ registers met in elk register één bit van x of van y en een $\#$ in het midden. Omdat registers van R alleen getallen kunnen bevatten (definitie) wordt $\#$ gerepresenteerd door 2. Ook is het aantal registers onbegrensd, daarom staat in het register na (boven) het laatste bit van y (register $|x| + |y| + 2$) ook 2. De programmateller van R staat aan het begin op 0. Geef voor beide machines een programma dat x en y optelt. Machine laat $x + y$ in binair op de band achter aan het einde van de berekening, terwijl machine R aan het einde van de berekening $x + y$ als één enkel getal in register 0 achterlaat.
3. Er bestaat geen machine M_H die voor een gegeven Turingmachine M en een invoer x beslist of M op invoer x stopt. Dat is bekend als het “haltingprobleem.”
 - (a) Laat zien dat er ook geen Turingmachine M_E bestaat die voor een gegeven Turingmachine M beslist of (a) M stopt en (b) de invoer een even getal is. (Dus M_E antwoord 1 dan en slechts dan als zowel (a) als (b) waar is.) Je bewijs is van de vorm “Als M_E bestaat, dan bestaat M_H ook.” Dit noemen we een (many-one) reductie.
 - (b) Anders dan bij NP-volledigheidsbewijzen, hoeft dit type reducties niet polynomiaal begrensd te zijn. Waarom niet? Is de reductie die je bij het vorige onderdeel gevonden hebt tijd/geheugen begrensd?
4. Voor het gemak beschouwen we alleen Turingmachines 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 bandcellen aan het begin van de berekening.
 - (a) Als M precies 10 toestanden heeft waarin q_0 de begintoestand is en q_F de (enige) accepterende toestand is, en M voor een zekere berekening 35 bandcellen mag gebruiken, hoeveel stappen kan M dan maximaal doen voordat je weet dat M de invoer niet zal accepteren.
 - (b) Toon met behulp van diagonalisatie aan dat er een taal is die kan worden geaccepteerd met gebruik van n^2 bandcellen, maar die niet wordt geaccepteerd als maar $\log n$ bandcellen mogen worden gebruikt, waarbij n de lengte van de invoer is. (Ter herinnering: een diagonalisatie is een bewijs waar een Turingmachine een andere Turingmachine en diens invoer als invoer gebruikt en dan iets doet op de diagonaal, de i -de machine op invoer i .)