for alle programmer med maksimalt n bit. Og derfor indeholder Omegas første n decimaler informationen om bevisbarheden for alle matematiske sætninger i et formelt system, som er n-bit stort.

Informationsbegrebet

Resultatet af overvejelserne om ufuldstændighed, tilfældighed, uvidenhed, sandsynlighed osv. førte til, at der i løbet af midten af 1900-tallet udvikledes et helt nyt koncept, hvormed man kunne begynde at forstå fysiske og matematiske strukturer. Dette koncept var *information*. I daglig tale defineres information som noget, der har med overførsel af viden at gøre. Dette er en forståelse af ordet, hvor enhver information kun kan forstås, hvis modtageren har en baggrundsviden om det pågældende sprog, om konteksten, de implicitte antagelser osv. Hvis man derimod forestiller sig, at der er kommet et brev fra stjernesystemet Alfa Centauri, kan man næppe gøre sig forhåbninger om at få en forståelse af indholdet, alle populære myter til trods – man kan måske ikke engang være sikker på, at der er tale om et brev.

I semantisk informationsteori taler man her om et referenceproblem: et objekts potentielle vidensindhold vil udefra kun kunne beskrives som en sandsynlighedsfordeling over alle mulige fortolkninger med én og samme sandsynlighed. Uden anden information vil brevet principielt kunne betyde alt mellem himmel og jord. Først når der opstår referentielle begrænsninger for realiseringen af de enkelte alternativer, vil der kunne opstå betydningsbærende elementer, som så igen kan virke tilbage og favorisere bestemte muligheder, og først da bliver brevet forståeligt. Meningsfyldt information (i f.eks. en binær sekvens) er altså ensbetydende med en ændring i sandsynlighedsfordelingen af mulighederne på grundlag af en yderligere indsnævring, som kun kan opstå ved en berøring med en omverden, fælles referencer, symboldannelse osv. Det betyder, at uden referencer kan et virkelig fremmed signal, hvor man intet kender til afsenderen, ikke være andet end et spejl. Et spejl af vores egne tanker. Man bliver offer for en projektion og begynder at lægge sine egne bekymringer og håb i signalets tydninger. Militæret vil sikkert forvente nye våben, videnskabsmanden ny erkendelse, og skønånden vil håbe på forløsning. Men når alt kommer til alt, vil vi mennesker ikke være i stand til at erkende eller forstå signaler fra sådanne verdener, selv hvis de stod med lysende flammer på firmamentet.

Information 1: At tælle bits og bytes

Inden for naturvidenskaberne har man netop udviklet en sådan referenceløs definition af ordet information. Den har derfor heller intet med forståelse at gøre. Den er en ren matematisk øvelse i at tælle bits og i at måle kompleksiteten af en binær sekvens, forstået som længden af det korteste program, der kan frembringe sekvensen. Denne fortolkning af information er rent kvantitativ og har vist sig at have enorm betydning for komprimering af data, krypteringsalgoritmer og for vores erkendelse af, hvordan uvidenhed kan defineres og måles.

Man kan sammenligne denne kvantitative definition af information med opfindelsen af termometret. I slutningen af 1500-tallet begyndte en gruppe af lærde i Venedig, der bl.a. talte Galilei (1564-1642), at definere temperatur som et tal, der kunne aflæses på en skala, uden ellers at beskæftige sig med hvad varme og kulde egentlig var for størrelser. Termometret (eller termoskopet, s. 100) var en pragmatisk løsning på et praktisk problem, og der skulle gå mere end 300 år, før man lærte, at temperaturmåling har at gøre med måling af molekylers hastighed. Det samme gør sig gældende ved måling af information i midten af 1900-tallet.

I løbet af Anden Verdenskrig arbejdede Alan Turing med at bryde tyskernes Enigmakode, hvilket lykkedes for ham og hans hold i den engelske kodeafdeling Bletchley Park i 1943. I løbet af denne tid udviklede Turing også en teoretisk ramme for "graden af tydelighed", hvormed en given mængde information kan transmitteres via et radiosignal. Det førte i 1948 den amerikanske ingeniør og matematiker Claude Elwood Shannon (1916-2001), der også havde arbejdet i Bletchley Park, til at definere information som det, der for modtageren af et signal opfattes som kompleks og dermed tilfældig støj. Et signal bestående af kun et enkelt symbol vil opfattes som meget lidt komplekst, fordi man jo ved, hvad man kan forvente. Men et meget komplekst signal uden synlige mønstre vil opfattes som meget tilfældigt.

Man må huske, at afsenderens intentioner, sproget og budskabets indhold er ting, der er fuldstændig irrelevante i denne her sammenhæng. Det eneste, der tæller, er den mængde af kompleksitet, eller usikkerhed (eller uvidenhed), der transmitteres, set fra en forudsætningsløs modtagers synspunkt. Shannon definerede mængden af output fra en informationskilde som et mål for informationens "entropi". Det er med andre ord et mål for den usikkerhed, der er knyttet til modtagerens tolkning af output. Shannon-

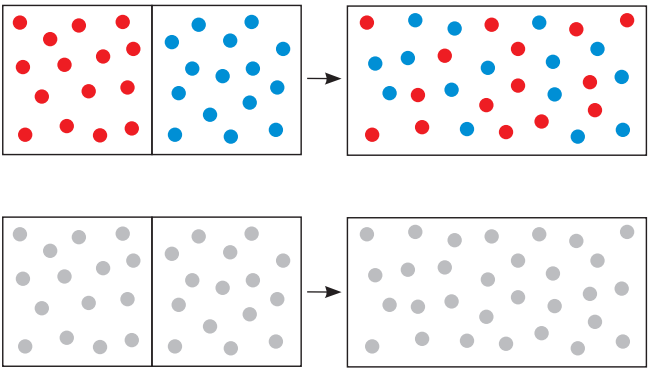
Denne originale Enigma-maskine er udstillet i Bletchley Park · Foto: Oliver Robinson.

entropien fungerer derfor som en tilnærmelse til, hvor stor informationsmængden i et givent budskab er – i modsætning til den forudsigelige del af budskabet. F.eks. bidrager gentagelser og let genkendelige mønstre i daglig talesprog ikke til informationsmængden og dermed ikke til entropien. Det ved enhver, som dagligt sender SMS'er. Det er ikke nødvendigt at skrive besværlige fyldord og selvforklarende bogstaver. Man k nøjs m a skriv så d forstås.

Information 2: Entropi er manglende viden

Shannons og Turings ideer fra 1940'erne og 50'erne indvarslede en ny tid: det var begyndelsen på informationsalderen. På samme måde som den industrielle revolution startede med vores evne til at manipulere og holde regnskab med energi i 1800-tallet, begyndte informationsalderen, da vi lærte, hvordan man manipulerer og holder regnskab med information. Shannons bidrag var bl.a. hans erkendelse af, at det binære talsystem, som kun består af nuller og ettaller, er den mest effektive måde at kommunikere data på. Og Shannon viste, at elektriske afbrydere, som kan skifte mellem strøm/ikke-strøm, var en pålidelig måde at generere disse "bits" på. Og idet bits og bytes kan repræsentere alt, hvad man kan sige med matematik, kan de også repræsentere lyde, billeder og alle mulige andre former for signaler, som kan kodes og afkodes matematisk. Shannon gjorde sig desuden overvejelser om, hvor stor en kapacitet et kommunikationsmedium som f.eks. en telefonlinje skal have for at transmittere signaler, og hvordan støj påvirker dem. Han kunne således udlede en lang række lovmæssigheder for, hvordan information lagres, transporteres og komprimeres via elektriske ledninger – teknikker som i dag ligger til grund for alle digitale datastrømme.

Shannon-entropien er tæt knyttet til den østrigske fysiker Ludwig Boltzmanns (1844-1906) brug af ordet entropi i termodynamikken. Boltzmann



Når man blander to forskellige gasser, vil entropien vokse (øverst). Men "blander" man to identiske gasser, vil entropien forblive den samme (nederst). Det viser, at entropi-begrebet indeholder et element af subjektivitet, da der er forskel på, i hvor høj grad man kan skelne mellem ens og ikke-ens gasser. Den statistiske fortolkning af entropi er derfor et mål for størrelsen af bestemte klasser af mikrotilstande, og ikke for egenskaberne ved disse mikrotilstande.

havde redefineret entropien, og den kunne ikke længere forstås som en absolut egenskab ved en ting, som f.eks. dens vægt, tryk eller volumen. I stedet måtte den tænkes som et mål for antallet af måder, hvorpå komponenterne i systemet kunne arrangeres på – vel at mærke uden at det påvirkede de målelige størrelser.

Et eksempel kunne være et kast med to terninger. Sandsynligheden for at få to seksere er én ud af 36, mens sandsynligheden for at få en syver er seks gange så stor, idet antallet af måder, man kan få syv på, er 1+6, 2+5, 3+4, 4+3, 5+2 og 6+1. Entropi er med andre ord et mål for, hvor mange måder en bestemt tilstand kan fremkomme på. Det samme gælder for store mængder af atomer og molekyler: blander man f.eks. to flasker med henholdsvis varme og kolde gasser, vil molekylerne blandes på en sådan måde, at den makroskopiske måling af temperaturen vil være et sted midt imellem de to tidligere målinger, mens entropien vil vokse uanset hvad, nemlig proportionalt med antallet af de nye kombinationsmuligheder, der kan frembringe den nye makroskopiske tilstand (Boltzmann kaldte dem "komplexioner"). En virkelig forbløffende erkendelse opstår i den situation, hvor man har to identiske flasker med identiske gasmolekyler og identisk tryk, temperatur osv. Her ville en sammenblanding af de to systemer faktisk ikke øge entropien. Men molekylerne blandes vel, kan man spørge? Jo, det gør de sikkert, men man kan hverken se eller måle det. Og det er det, der gør forskellen. Det er som at kaste med en ensidet terning. Du ved, hvad du får.

Denne observation gav Boltzmann et praj om, at den subjektive viden om et systems tilstand på en eller anden måde måtte have en betydning for måleresultatet. Filosoffer ville sige, at termodynamikkens anden hovedsæt-

ning beskriver verden ud fra et epistemologisk niveau og ikke ud fra et ontologisk niveau. Med andre ord er den anden hovedsætning en beskrivelse af *vores viden* om virkeligheden, ikke af virkeligheden selv. Havde der f.eks. – som foreslået af James Clerk Maxwell (1831-79) – været en dæmon i laboratoriet, som kunne se og følge hvert enkelt gasmolekyle, ville dæmonen erklære entropien for at være nul i alle tilfælde. Entropi, defineret af mennesker, er derfor et mål for vores manglende viden om systemet. Og det er i den forstand, at Boltzmanns entropi er tæt forbundet med Shannons information: de er begge et udtryk for den viden, som man *kunne* have om systemet, men ikke har. Shannons information og Boltzmanns entropi er ikke identiske, men de er to forskellige måder at udtrykke den samme ide på.

Information er ifølge Shannon et mål for mængden af viden. Det er ikke denne viden i sig selv. Derfor er informationsbegrebet ligesom energibegrebet – at kende mængden af energi fortæller ikke noget om dens tilstand, dens udbredelse eller dens form. Som en understregning af denne pointe kan man nævne, at Boltzmanns arbejde på mange måder foregreb kvantemekanikkens problemstillinger 50 år senere, idet også Niels Bohrs (1885-1962) fortolkning af kvantemekaniske eksperimenter var strengt epistemologisk. Det vil sige, at de kvantemekaniske ligninger ifølge Bohr fortæller om vores muligheder for at kunne vide noget om virkeligheden, og ikke noget om virkeligheden selv. (Hvilket Einstein som bekendt var stærkt utilfreds med, fordi han mente, at en fysisk teori burde kunne sige noget om virkeligheden og ikke kun noget om, hvad vi ved om virkeligheden; se også s. 294).

Men selvom information er et abstrakt, epistemologisk begreb, har realiseringen af information i form af budskaber naturligvis en fysisk basis. Tænk blot på bøger, aviser og håndskrevne breve. Forsendelsen af information har altid brug for et materielt medium. Kun med opfindelsen af computeren blev omkostningerne ved informationsoverførsel og -lagring så små, at man har tendens til at se bort fra dem. Men omkostningerne er der alligevel, og i 1960 proklamerede fysikeren Rolf Landauer (1927-99), som ligesom Shannon havde arbejdet hos IBM, derfor, at "information er fysisk". Selvom man måske kunne opfinde en kvantecomputer med et uendeligt lille energitab ved hver enkelt beregning, ville det koste en vis mængde entropi, når informationen skulle slettes igen. Derfor er selv kvantemekaniske computere, som man håber en dag vil kunne regne med såkaldte qubits i stedet for bits, underlagt fysikkens love.

Information 3: kvanter og qubits

Siden kvantemekanikkens fødsel har vores viden om atomer været en smule skizofren. Eller sådan opfattes det i hvert fald. Nogle gange opfører atomer sig som partikler, og andre gange som bølger. Desuden viste det sig, at elementarpartiklerne kunne reagere med hinanden på en sådan måde, at de "blandede deres tilstande". Erwin Schrödinger (1887-1961) kaldte dette fænomen for "Verschränkung", dvs. "entanglement" eller "sammenfiltrethed", og uddybede det ved at forklare, at "den maksimale viden om et totalt system ikke nødvendigvis behøver at indbefatte den totale viden om alle systemets dele, selv hvis delene er separerede og langt væk fra hinanden." Denne spøgelsesagtige kvantekorrelation på lange afstande har voldt store kvaler for fysikere og filosoffer.

I 1935 formulerede Albert Einstein og hans kolleger Boris Podolsky (1896-1966) og Nathan Rosen (1909-95) et tankeeksperiment, som skulle modbevise kvantemekanikkens besynderlige vekselvirkninger. At en elektron både kan beskrives som en bølge og som en partikel, var for Einstein ikke det værste problem. Værre var det, at et samtidigt kendskab til forskellige egenskaber ved denne elektron forbød sig på grund af Werner Heisenbergs (1901-76) usikkerhedsrelation. "Gud spiller ikke med terninger", var Einsteins reaktion.

Det såkaldte EPR-tankeeksperiment var designet til det formål. To kvante-korrelerede partikler fra samme kilde bliver skudt af sted i hver sin retning. Venter man længe nok, er de lysår fra hinanden, hvorefter man kan måle forskellige egenskaber hos dem. Hvis man f.eks. måler hastigheden af den første partikel (eller egentlig dens "moment", der er et produkt af dens hastighed og masse), og positionen af den anden, så er ræsonnementet, at fordi dens moment bevares, kan man bestemme både moment og position af den anden partikel, hvilket forbydes af Heisenbergs usikkerhedsrelation. Et problem, der egentlig kun kan forklares i dagligdags forstand, hvis man antager, at partikler kan kommunikere hurtigere end lysets hastighed, hvilket jo er i modstrid med relativitetsteorien.

I mange år var sagen henlagt, indtil den franske fysiker Alain Aspect (f. 1947) udførte et rigtigt EPR-eksperiment i 1982. Hans resultat var, at selv hvis information, der bevæger sig hurtigere end lyset, er nødvendigt, er det ikke muligt på samme tid at bestemme både position og moment af en partikel. De kvantemekaniske ligninger holdt altså vand – men det betød ikke, at

Alain Aspects udstyr fra hans EPR-eksperiment i 1982.

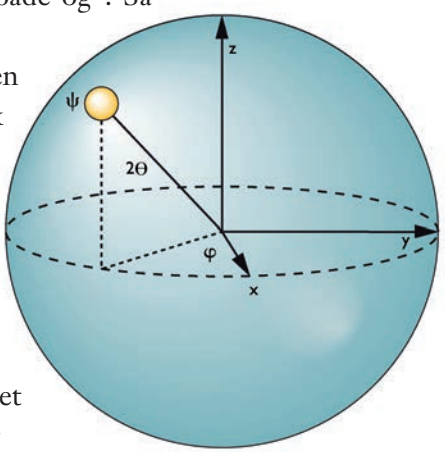
relativitetsteorien var modbevist. Det betød kun, at der ikke blev udvekslet information, samt at de to partikler er i en tilstand af overlejring, eller "entanglement", hvor de så at sige ved, hvad hinanden gør. Eller formuleret på en lidt mere akademisk, men ikke mindre mystisk måde: hvor deres tilstand er kvantekorreleret i form af en informationsoverlejring, således at deres information er indskrevet i deres fælles egenskaber. To partikler, som er i sådan en sammenfiltret tilstand, opfører sig ligesom tvillinger, hvor den ene kun kender sig selv i den andens billede: hvis den ene bliver kildet, griner den anden.

I dag mener mange, at nogle af kvantemekanikkens paradokser skyldes en blanding af to beskrivelsesniveauer – nemlig det epistemologiske niveau, hvor man beskriver, hvad man ved og kan vide, og det ontologiske niveau, hvor man påstår, at sige noget om de faktiske fysiske objekter og deres aktiviteter i verden. Ifølge Bohr forbliver kvantemekanikken på et rent epistemologisk niveau, hvorfor det er utilladeligt at tale om, hvorvidt der faktisk foregår en vekselvirkning på lange afstande eller ej. I moderne kvantemekanik er man således ved at forstå, at alle de spøgelsesagtige fænomener, som man kender fra eksperimenter med entanglement, teleportation og kvantecomputere, skal tolkes epistemologisk – og derfor informationsteoretisk. Det, der

bevæger sig hurtigere end lyset, er vores fantasi, dvs. *ideen* om at vi med et snuptag kan være på Alfa Centauri. Og selv dette er ikke helt korrekt, for selv vores fantasi er determineret af en fysisk hjerne, der også er underlagt lyshastighedens begrænsning. Det, der teleporteres, er en repræsentation af viden og ikke materie. Men det betyder ikke nødvendigvis, at man ikke kan bygge computere, som udnytter denne repræsentation til at lave komplicerede beregninger.

I normale computere bliver bits repræsenteret af mange milliarder elektroner, som er samlede i siliciumtransistorer, der ligger side om side på små computerchips. Om de repræsenterer et 1 eller et 0 i den binære kode afhænger af, om de er til stede eller ej. Men når man først kommer ned til de enkelte elektroner, er det ikke længere muligt at tolke tilstandene entydigt. Elektronerne kan være "enten eller" eller "både og". Så kaldes de qubits.

Oprindelig startede det med fysikeren Richard Feynman (1918-88), der i 1981 fik ideen om kvantecomputere som en teoretisk abstraktion til at diskutere, hvad information er, set fra kvantemekaniske principper. Siden har mange forskere forsøgt at føre de teoretiske diskussioner over i laboratorierne. Men lige meget hvad de prøvede, så ville kvantecomputerne ikke lege med, når det kom til den faktiske implementering i chips og ledninger. Ubestemmeligheden – dvs. deres evne til at indtage en "superposition" – af de enkelte partikler kan ikke bibeholdes, så snart man vil sætte dem i position, hvor man kan begynde at regne med dem. Så selvom man har kunnet melde om fremskridt inden for kvantekryptering, er computere baseret på kvantemekaniske effekter stadig kun en teoretisk ide.



En qubit – i praksis én enkelt elektron – er den basale enhed for en kvantecomputer. Den ligner en almindelig bit i at kunne indtage tilstandene 0 og 1, men den kan også være i en tilstand af superposition (overlejring) af både 0 og 1. En qubit kan tegnes som en "Bloch-sfære", hvor informationen om den kodes via vinkelafstande fra de tre akser X, Y og Z. Når man måler på denne qubit, vil udfaldet enten være 0 eller 1, selvom qubitten er i en tilstand af superposition, dvs. af både-og. Man ville kunne udnytte dette i en hypotetisk kvantecomputer, fordi x-antal qubits ville kunne udføre ikke kun x, men 2^x beregninger samtidigt. En kvantecomputers regnekraft stiger altså eksponentielt med antallet af qubits i modsætning til konventionelle computere, hvor regnekraften stiger lineært med antallet af bits.