Claudio Bonechi (clavicordo)

IL VERO CUORE DELLE TELECOMUNICAZIONI

27 January 2017

Premessa

Questa volta, invece di tradurre articoli, ho la fortuna di avere in dono dal suo autore, che mi ha autorizzato a pubblicarla, una trattazione sintetica ma molto pregnante dei fondamenti tecnologici di ciò che quotidianamente ci accompagna; ho pensato allora di trascriverla qui. L'autore è **Valentino Castellani**, che alcuni di noi (sicuramente IsidoroKZ, per esempio) già conoscono sia come professore emerito del Politecnico di Torino sia come sindaco della stessa città dal 1993 al 2001. Avendo studiato con lui, tesi compresa, ne ho una grande e incondizionata stima su tutti i piani. La trattazione che segue è la sua *Prolusione generale al Congresso Annuale della Società Scientifica e Tecnologica Friulana*, presentata il 30 ottobre 2010 ed ha il seguente titolo:

LA SOCIETA' DELL'INFORMAZIONE: ALLA RICERCA DELLE ORIGINI di *Valentino Castellani*

Nell'era che stiamo vivendo le reti di comunicazione sono una parte vitale delle infrastrutture della società.

La domanda sempre crescente di scambiare informazione, la necessità di condividere risorse di calcolo e di accedere ai grandi archivi di dati disseminati nelle biblioteche del mondo richiedono capacità di trasmissione e reti di telecomunicazione sempre più complesse e dotate dei più svariati supporti fisici (rame, fibre ottiche, satelliti, reti radiomobili …). Un World Wide Web, una ragnatela globale avvolge la terra, quasi fosse l'infrastruttura fisica di quella Noosfera che Pierre Teilhard de Chardin ha intravisto come sviluppo evolutivo della vita sul nostro pianeta. Internet sta per compiere trentadue anni se si assume come data di nascita la tecnologia che consentì l'interconnessione tra le reti informatiche a livello mondiale. Il Web, cioè la tecnologia che ha permesso l'accumulazione del patrimonio di documenti d'ogni genere a cui Internet consente l'accesso è più giovane di circa un decennio ed è stato donato a tutti, compresa quindi l'industria privata, da un ente di ricerca pubblico, il CERN di Ginevra, presso il quale la tecnologia era stata sviluppata e collaudata. Le stime dicono che i documenti presenti nel Web sono cresciuti dai pochi milioni dei primi anni '90 alle parecchie centinaia di miliardi di oggi.

La forma più comune di comunicazione consiste oggi in persone poste a dei terminali sempre più vari e complessi (PC, telefono fisso o mobile, iPod, iPad, televisore…) che comunicano con altri terminali o con grossi elaboratori attraverso la connessione in reti locali (LAN) o reti geografiche (WAN). Lo scambio di informazioni su queste reti è governato da una architettura stratificata,

tanto affascinante quanto complessa, di protocolli che controllano i flussi, gli instradamenti e gli accessi.

Il supporto dell'informazione, la "materia prima" che deve essere convogliata su queste reti sono miliardi e miliardi di simboli binari ("zeri" e "uni"). Ogni sorgente di informazione immette nell'oceano della rete la sua quantità, le sue sequenze di simboli, e questi devono raggiungere l'utente situato in un punto qualunque del pianeta (o anche nello spazio cosmico che è stato raggiunto dall'uomo), e lo deve raggiungere in buono stato di salute, cioè senza errori (gli "zeri" devono essere restituiti come "zeri" e gli "uni" come "uni").

In questa mia prolusione mi propongo di andare alle origini di questo scenario e di individuarne i presupposti scientifici e tecnologici che lo hanno reso possibile con una dinamica evolutiva travolgente.

L'evoluzione della scienza e della tecnologia procede normalmente con gradualità ed ogni ricercatore o tecnologo fa tesoro dell'accumulo di conoscenze che lo hanno preceduto fino a che, di tanto in tanto, si crea una "rottura" con il passato, si determina un nuovo inizio che non sempre viene subito riconosciuto per la buona ragione che bisognerebbe poterne vedere gli sviluppi per riconoscerne la nascita. Si torna allora indietro nel tempo e si prova a riconoscere questo momento magico.

Due sono i **momenti magici** che secondo me hanno caratterizzato l'inizio della nostra storia, entrambi accaduti nel biennio 1947-48. Uno fa riferimento a Shannon, che ha posto le basi scientifiche della **Teoria dell'Informazione**[1] e l'altro è la **scoperta del Transistor** avvenuta nei Laboratori della Bell nel 1947 ad opera di Bardeen, Brattain e Shockley, che per questo ottennero il Nobel per la fisica nel 1956. Dalla loro scoperta ha avuto inizio l'era della microelettronica.

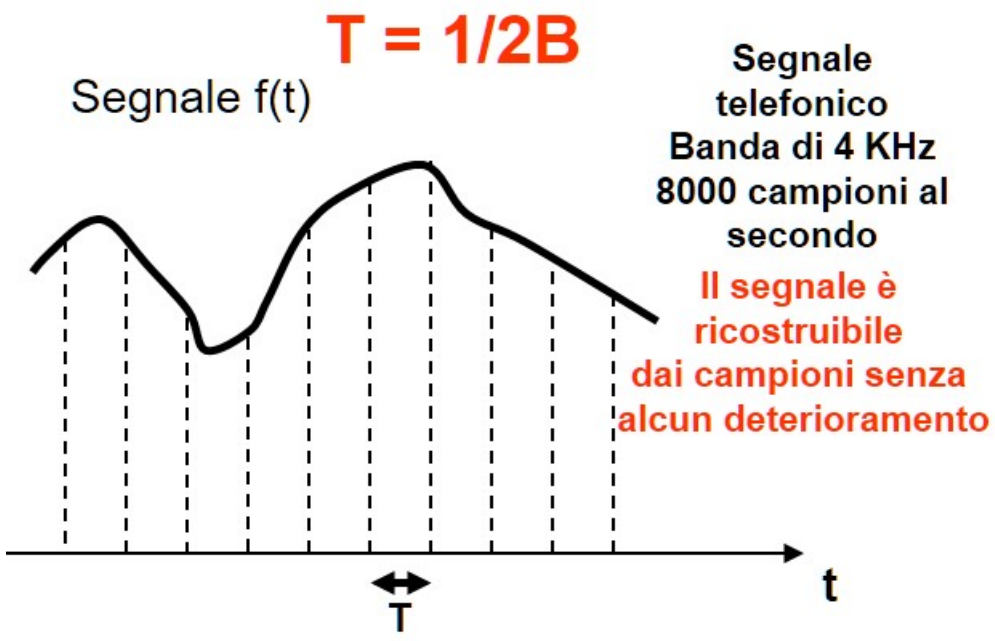
Visiteremo alcuni concetti fondamentali della teoria di Shannon per poi vedere come essi hanno trovato pieno sviluppo ed applicazione sposando le tecnologie della microelettronica e costruendo poco a poco lo scenario nel quale oggi, più o meno consapevolmente, operiamo quando accediamo anche noi al Web.

La prima fondamentale assunzione di Shannon fu che **ogni sorgente di informazione** è una **sorgente discreta**, cioè una sorgente che si può rappresentare con un alfabeto costituito da un **numero finito di simboli**.

Vi sono ovviamente sorgenti che sono discrete per loro natura come ad esempio i segnali generati dalle tastiere dei nostri terminali. Non così appaiono a prima vista i segnali elettrici a valle dei trasduttori che li generano, come ad esempio il segnale telefonico che rappresenta la voce dell'utente o il segnale video all'uscita di una telecamera. Essi appaiono come funzioni continue del tempo e coprono una dinamica continua di possibili ampiezze.

Anche questi segnali però possono essere rappresentati come una sorgente discreta, cioè un dispositivo che genera informazione mediante sequenze di simboli scelti da un alfabeto finito. Vediamo quali ne sono i presupposti.

Ogni segnale fisico ha una banda di frequenze limitata e pertanto può essere rappresentato in modo perfetto anche solo con una successione di campioni prelevati ad intervalli di tempo uguali (teorema del campionamento). Il segnale telefonico, ad esempio, ha una banda convenzionale di 4 KHz e quindi bastano 8000 campioni al secondo per rappresentarlo in maniera fedele. Se poi volessimo aumentare la fedeltà di un segnale acustico, dovremmo tenere conto che il nostro orecchio non percepisce suoni oltre i 15 KHz e quindi sarebbe inutile prelevare più di 30000 campioni al secondo da un segnale il cui utilizzatore finale fosse l'orecchio umano. Questo fenomeno è ben noto anche ai bambini quando scoprono che si può simulare il movimento facendo scorrere tra le dita un pacchetto di immagini fisse, una leggermente diversa dall'altra. E' il "gioco" del cinematografo. Il nostro occhio infatti non è in grado di percepire come separate nel tempo immagini che si susseguono a velocità troppo elevata (è un filtro passa-basso) ed infatti i quadri del televisore cambiano ad una frequenza di 25 al secondo. Il movimento viene ricostruito con una sequenza di immagini fisse, di "campioni" del movimento.



Ora abbiamo un campione del segnale che può coprire con continuità un intervallo di ampiezze. Anche qui operiamo, questa sì, una approssimazione. Suddividiamo l'intervallo in N parti uguali e numeriamole da 0 ad (N-1). Il campione del segnale cade in uno di questi intervalli e noi possiamo sostituirlo con il numero dell'intervallo. Abbiamo trasformato il segnale in una sequenza di numeri (digits, in inglese, da cui digital transmission). Tanto più numerosi gli intervalli, tanto migliore l'approssimazione. Anche in questo caso il criterio di quantizzazione sarà guidato dalle

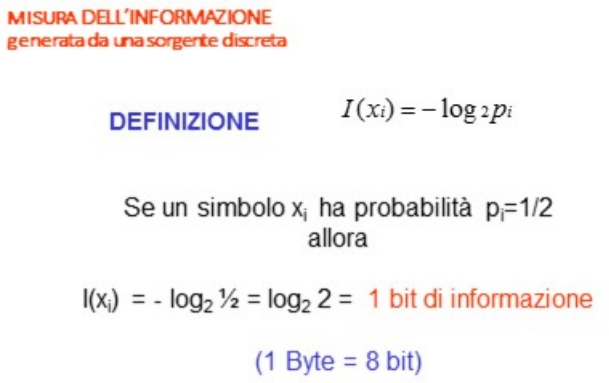
esigenze dell'utente. Ad esempio, nel caso del segnale telefonico 256 intervalli di quantizzazione garantiscono una qualità ottima nella riproduzione del segnale.

Misurare l'informazione

Il primo passo importante fatto da Shannon è stato quello di definire matematicamente la **misura dell'informazione**. La definizione è la conseguenza di **due assiomi di assoluto buon senso**.

Il **primo** è che un evento fornisce **tanta più informazione quanto meno è probabile**;

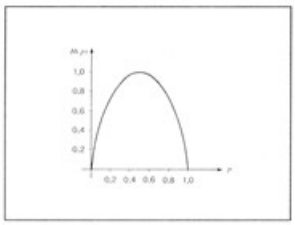
il **secondo**, che d**ue eventi indipendenti danno quantità di informazione che si sommano**. Il **bit** è **l'unità** per misurare l'**informazione** e corrisponde all'informazione prodotta quando si verifica uno tra due eventi equiprobabili.



Una sorgente è caratterizzata dalla quantità media di **informazione generata per ogni simbolo**. A questa media Shannon ha dato il nome di **Entropia della sorgente**. Nel caso della sorgente binaria si vede che l'entropia al massimo vale 1 bit quando i simboli sono **equiprobabili** ed in caso contrario si dice che la sorgente è **ridondante**, cioè ogni simbolo binario prodotto fornisce meno informazione di quanto potrebbe.

Quantità media di informazione
(Entropia) generata da una sorgente

$$H(X) = \sum_i p_i I(x_i) = -\sum_i p_i \log_2 p_i$$



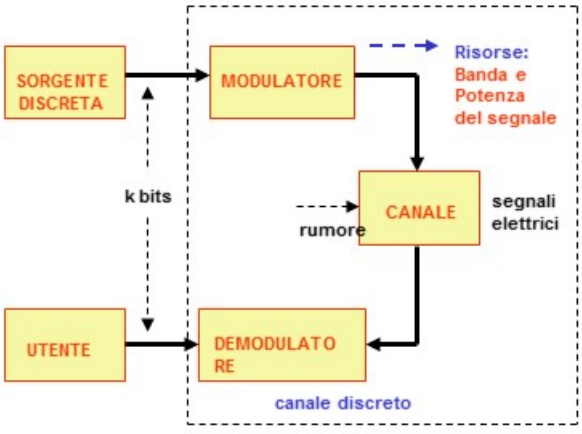
Entropia H(X) di una sorgente binaria con simboli di probabilità p e (1-p)
Il massimo si ha per p=1/2

Quando p è diversa da 1/2 si dice che la sorgente ha ridondanza

Una osservazione importante da fare subito è che l**a ridondanza non è inutile**. Essa aiuta l'utente a contrastare la perdita di informazione che ci sarà sul canale di trasmissione. Ad esempio, ogni linguaggio è ridondante, ma questo aiuta a capire un discorso in un ambiente molto rumoroso, nel quale si fa molta fatica a capire se chi parla lo fa in una lingua straniera.

Trasmettere l'informazione a un utente lontano

Facciamo ora un passo avanti e guardiamo al problema della trasmissione dell'informazione ad un utente lontano,

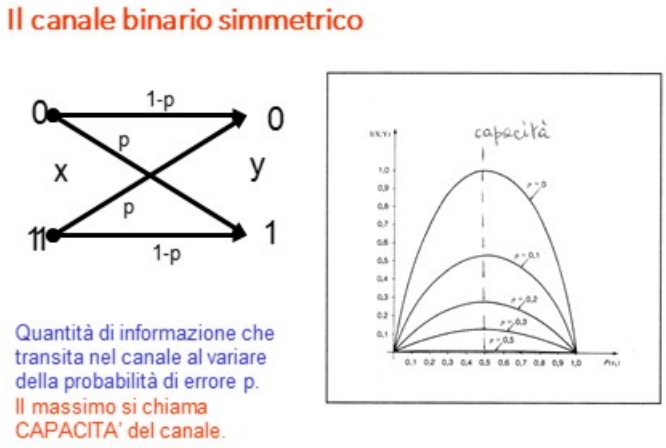


modem

I bit generati dalla sorgente vengono "affidati" in **blocchi di k** a segnali elettrici che sono generati da un modulatore, trasmessi sul canale fisico di comunicazione e restituiti all'utente dal demodulatore che compie l'operazione inversa fatta dal modulatore (la coppia è il **modem**). Il canale di trasmissione degrada i segnali trasmessi per effetto dei disturbi, delle distorsioni, delle interferenze. Chiamiamo **rumore**, per estrema semplificazione, l'insieme di questi fenomeni. Il risultato sarà che dalla parte dell'utente non tutti i k bit trasmessi saranno ricevuti correttamente ed il sistema presenta una **probabilità di errore**. Le **risorse** a disposizione degli ingegneri per trasmettere sul canale sono sempre state la **banda di frequenza dei segnali** e la **potenza elettrica dei segnali trasmessi**. Vedremo più avanti che proprio su questo punto specifico Shannon ha dato il suo contributo fondamentale di innovazione.

Quanto è capace il canale?

Il **canale di trasmissione** può essere rappresentato con un modello molto semplice e non è difficile calcolare la **quantità media di informazione** che esce dal canale. Se i simboli di sorgente sono **equiprobabili** ed il canale non sbaglia abbiamo come ovvio **1 bit per ogni simbolo ricevuto**. Si noti che basta una probabilità di errore del 10% per perdere la metà dell'informazione. Infatti, è vero che noi sappiamo che il 10% dei simboli sono sbagliati, ma non sappiamo quali sono se volessimo correggerli. Shannon ha definito la capacità del canale come il massimo dell'informazione che riusciamo a ricevere, dato un valore della **probabilità di errore p**.

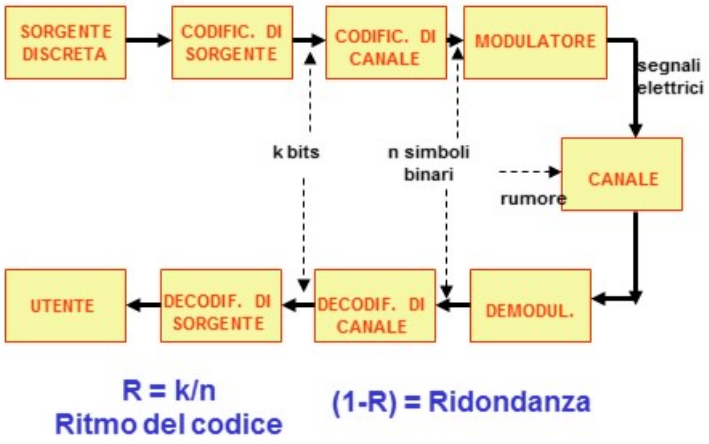


Torniamo ora al nostro schema generale e vediamo di renderlo più completo.

Abbiamo detto che le sorgenti di solito sono ridondanti. Il problema è che la loro ridondanza è fuori dal nostro controllo perché non ne conosciamo bene la struttura matematica. Conviene allora eliminarla con il **codificatore di sorgente**. Il suo compito è quello di sostituire, mediante opportuni algoritmi, la sequenza di simboli binari non equiprobabili della sorgente con un'altra

sequenza nella quale i simboli siano il più possibile equiprobabili (nel caso ideale lo saranno). Sarà compito del decodificatore di sorgente, al terminale di ricezione, di ricostruire la sequenza originaria perché naturalmente gli è noto l'algoritmo di codifica. In tal modo però la sequenza dei k simboli di informazione da trasmettere sono molto vulnerabili a causa degli errori del canale; ma noi **sostituiamo la sequenza di k simboli con una più lunga, di n simboli binari** (abbiamo aggiunto una **ridondanza pari a 1-k/n**), usando il codificatore di canale.

Questa ridondanza la possiamo aggiungere mediante sofisticati algoritmi matematici che dal lato del decodificatore di canale ci potranno consentire di individuare eventuali errori e di correggerli. Quanto più grande è n rispetto a k tanto più saremo capaci di **rivelare e correggere gli errori** e restituire una sequenza esatta di k simboli al decodificatore di sorgente. Lascio alla vostra immaginazione intuire quanta matematica sofisticata è stata inglobata dentro i moderni codificatori di sorgente e di canale.



Codifica di Sorgente e di Canale

Aggiungo anche un'altra considerazione molto importante che riguarda la segretezza dei k bit di informazione che si vogliono trasmettere sul canale. In molte applicazioni (si pensi alle transazioni finanziarie) l'utente vuole evitare che un intruso possa accedere ai suoi dati e quindi rubare il contenuto di informazione associato. Avendo a disposizione l'informazione rappresentata da una sequenza di numeri binari, si possono operare su questi numeri delle operazioni matematiche sofisticate che li trasformano in una nuova sequenza apparentemente casuale e quindi apparentemente priva di alcun contenuto informativo. **Il codificatore di sorgente può cioè inglobare anche un algoritmo che consente di crittografare l'informazione** rendendola così accessibile solo all'utente designato, perché solo lui conosce l'algoritmo, cioè la chiave, per interpretarla. La matematica della crittografia è basata sui numeri primi ed è un esempio molto suggestivo di come capitoli di matematica teorica apparentemente senza alcuna implicazione pratica possano ad un certo momento diventare di grande interesse applicativo. E' anche

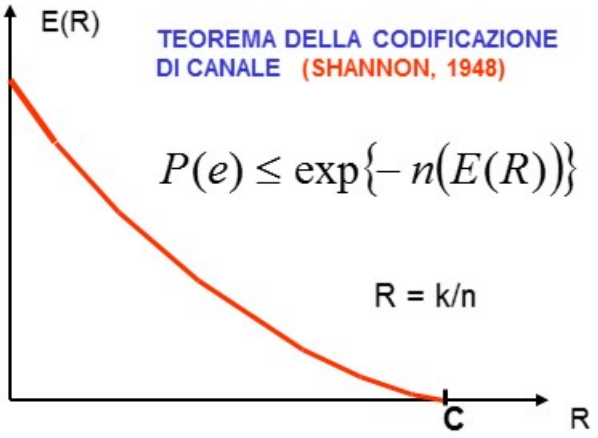
opportuno ricordare il fondamentale contributo dato da Shannon alla crittografia con un lavoro pubblicato nel 1949[2].

La codificazione di canale

In questo modo siamo pronti per descrivere uno dei risultati più importanti della teoria di Shannon: **il teorema della codificazione di canale.**

La probabilità di errore del sistema diminuisce esponenzialmente per l'effetto di **due fattori**: la **lunghezza del codice di canale n** ed una **funzione E(R)** il cui andamento tipico si vede nella figura,

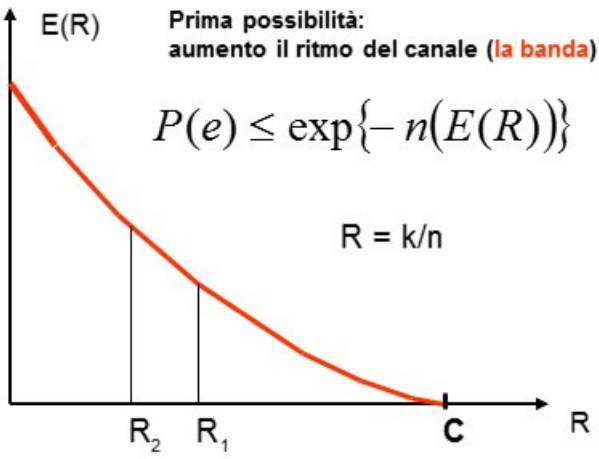
ciò **nell'ipotesi** che il ritmo di trasmissione **R = k/n** sia **inferiore alla capacità del canale**.



Questo elegante risultato è quello che ha consentito alla teoria delle telecomunicazioni di incontrarsi con lo sviluppo della microelettronica per determinare gli scenari che abbiamo descritto all'inizio. Vediamo come e perché.

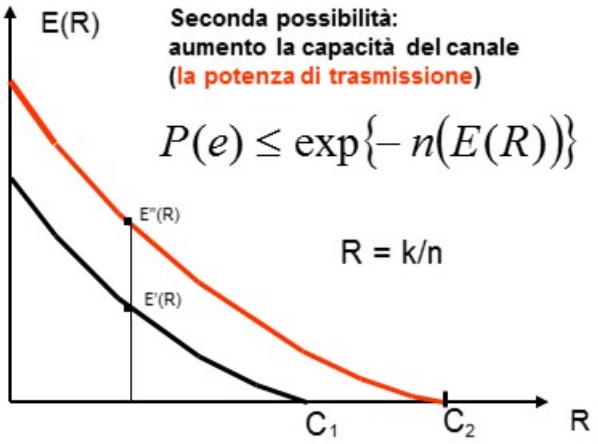
Per migliorare le prestazioni del sistema (cioè diminuire la probabilità di errore) possiamo innanzitutto cercare di **aumentare E(R)**, e ciò può essere fatto in **due modi**.

Prima possibilità. Usiamo un ritmo di trasmissione R2 minore di R1 e siccome k è dato, ciò significa aumentare n, cioè usare il canale con una frequenza maggiore. Stiamo aumentando la banda di trasmissione e con questo possiamo migliorare le prestazioni.



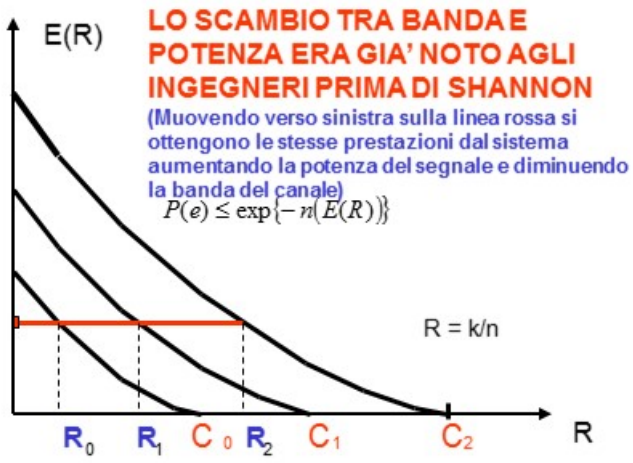
Prima Possibilità

Seconda possibilità. Posso aumentare la potenza del segnale trasmesso, con ciò riduco la probabilità di errore sul canale e ne aumento la capacità ottenendo un valore maggiore per E(R).



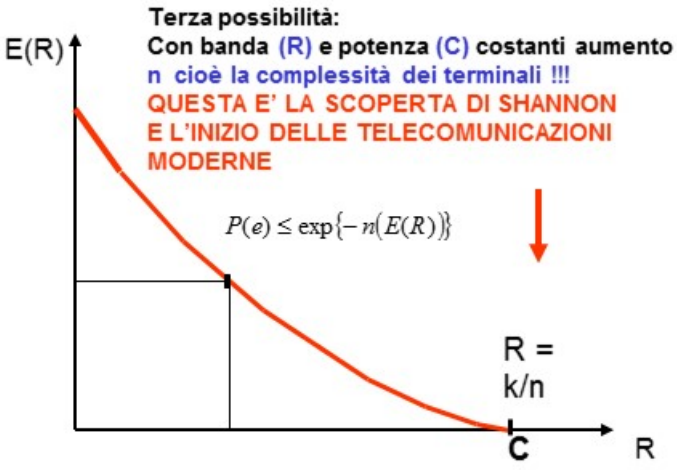
Seconda Possibilità

Queste due possibilità, come abbiamo già accennato, erano ben note a tutti gli ingegneri delle telecomunicazioni. La funzione E(R) descrive il meccanismo già noto dell'uso della banda e della potenza del segnale come risorse trasmissive ed eventualmente del loro scambio.



La terza via

Ora però arriva la **grande novità**. **Terza possibilità**. Senza cambiare la banda (k/n resta costante) o la potenza del segnale possiamo migliorare le prestazioni facendo **n sempre più grande**. Abbiamo a disposizione una nuova risorsa: **la complessità dei terminali**. E' evidente che se n è molto grande gli algoritmi di codificazione (e di decodificazione) devono operare su **sequenze di dati molto lunghe** e quindi sono **sempre più complessi**.



Terza Possibilità

Come capita spesso per le scoperte scientifiche, la portata rivoluzionaria di questo risultato fu apprezzata solo più tardi, quando la microelettronica ha reso disponibili grandi potenze e velocità di calcolo e grandi capacità di memorizzare i dati.

Lo ha scritto molto bene, nel 1981, un editoriale delle IEEE Transactions on Communications: " Ci troviamo all'alba di una nuova era, quella in cui gli ingegneri possono scambiare banda e potenza per una terza risorsa, la complessità di elaborazione. Nel passato, quando i dispositivi attivi costavano cinque dollari l'uno, la parola complessità era gravida di connotazioni negative. Adesso una nuova economia ha capovolto la situazione: l'integrazione a larga scala ha ridotto il costo dei dispositivi di un milione di volte e molteplici nuovi dispositivi sono in attesa dietro le quinte. Pertanto questa complessità, opportunamente progettata ed introdotta nei sistemi, diventerà una necessità economica".

La nuova era di cui si parla è quella che ormai chiamiamo la società dell'informazione.

Percorrere la strada, dalle origini ai giorni nostri, e riconoscere i passi critici delle scoperte che hanno reso possibile lo scenario nel quale viviamo sarebbe un'avventura affascinante, che però esula dai limiti di questa conversazione. Non provo nemmeno a cominciare... mi limito ad enunciare le principali tendenze che ormai si sono consolidate.

Nel campo della microelettronica, a partire dal 1971, la potenza dei microprocessori in media è raddoppiata ogni 18 mesi, dimezzando contemporaneamente il costo per bit (legge di Moore). Questo è il motore che spinge continuamente in avanti il progresso tecnologico, trasformando con altrettanta continuità costi, rendimenti, modi di produrre e di consumare.

Per quanto riguarda le tecnologie della connessione, le telecomunicazioni, la riduzione dei costi è dovuta allo sviluppo dei mezzi di trasmissione: cavi, fibre, banda larga ... La larghezza di banda disponibile, a parità di costo, triplica ogni 12 mesi (legge di Gilder).

Per quanto riguarda le reti, il processo di riduzione dei costi e di aumento del valore della connessione è dovuto alla affermazione di standard universali, che consentono di sommare una domanda di connessione sempre più vasta; se molti utenti usano lo stesso standard e si connettono alla stessa rete, il costo della connessione diminuisce e, contemporaneamente cresce esponenzialmente il valore generato per gli utenti della rete. Le reti, infatti, accrescono il loro valore al crescere del numero delle persone connesse e al conseguente aumento del flusso delle loro comunicazioni (legge di Metcalfe)[3].

Questo scenario conferma il risultato che **Shannon** aveva enunciato con il suo elegante teorema, cioè che **la complessità è una potente risorsa di sistema** se gli scienziati e gli ingegneri la sanno utilizzare.

Conclusione

Voglio concludere sottolineando una distinzione per nulla scontata e fonte perciò di equivoci e di semplificazioni pericolose: la distinzione tra informazione e conoscenza. Sono usati spesso come

sinonimi (società dell'informazione e società della conoscenza, ad esempio), ma sono invece entità diverse e come tali vanno definite e riconosciute. Al concetto di informazione possiamo associare quantità discrete e misurabili (i bit di informazione) cosa che non possiamo fare con il concetto di conoscenza. **La conoscenza non è "mera informazione"**[4], non può essere associata ad un numero, non è fisicamente misurabile.

La conoscenza è una risorsa necessaria per interpretare ed elaborare l'informazione. Una quantità di informazione anche grande non è ancora, in quanto tale, conoscenza.

La conoscenza è dunque un processo culturale e sociale molto complesso: nell'economia della conoscenza la capacità di aggiungere valore ai beni prodotti non è determinata tanto dal trasferimento di pacchetti di informazione (ad esempio dalle università alle imprese) ma soprattutto dall'esistenza di un ambiente complessivo difficile da definire nei contorni, caratterizzato da una forte cultura dell'innovazione e basato principalmente sul capitale umano.

Una conoscenza critica e consapevole richiama la grande responsabilità del sistema educativo di una comunità, di un Paese e noi tutti siamo consapevoli di quanto impegno richieda il sistema educativo del nostro Paese: alla politica nazionale e locale, agli insegnati, agli adulti nei confronti dei più giovani. Di una conoscenza critica e consapevole si nutre anche la democrazia, e l'impegno è dunque a tutto campo.

Quando vedo i miei nipotini muoversi con disinvoltura ormai superiore alla mia davanti ad un terminale, mi trovo spesso a riflettere sul fatto che stanno compiendo solo il primo passo, importante fin che si vuole, ma non ancora quello decisivo, quello per il quale la nostra attenzione educativa è determinante affinchè non si verifichi la suggestiva quanto inquietante premonizione di Jorge Louis Borges che, nella Biblioteca de Babel, scrive: "Yo conozco distritos en que los jovenes se prosternan ante los libros y besan con barbarie las paginas, pero no saben descifrar una sola letra". Che questo non succeda ai nostri figli e nipoti seduti davanti ad un terminale connesso con la rete è il compito che spetta alla nostra generazione.

Valentino Castellani

Bibliografia

[1] Claude E. Shannon,"A Mathematical Theory of Communication", The Bell System Technical Journal, 1948[2] C.E. Shannon, "Communication Theory of Secrecy Systems",BSTJ 1949[3] F: Vespasiano, "La società della conoscenza comemetafora dello sviluppo", Franco Angeli 2005[4] A. Cerroni, "Scienza e società della conoscenza",Utet, Torino 2007