Part XXII

Future of informatics - Chapter 3

Chapter 3: INFORMATION TECHNOLOGIES: EVOLUTION, LAWS and FUTURE

CONTENTS

WISDOMS

- Any sufficiently advanced technology is indistinguishable from magic.

  Arthur C. Clarke's third law

- Any technology distinguishable from magic is insufficiently advanced.

  Barry Gehm

- Technology is still magic even if you know how it's done.

  Terry Pratchell in "A hat full of sky

- No communication technology has ever disappeared,but instead becomes increasingly less important as the technological horizon widens.

  Arthur C. Clarke

- Civilization advances by extending the number of important operations which we can perform without thinking about them.

  Alfread North Whitehead (1911)

- The reasonable man adopts himself to the world; the unreasonable one persists in trying to adopt the world to himself. Therefore all progress depends on unreasonable men.

  George Bernard Shaw

WISDOMS CONCERNING TECHNOLOGY

- First we thought the PC was a calculator. Then we found out how to turn numbers into letters with ASCII - and we thought it was a typewriter. Then we discovered graphics, and we thought it was a television. With the World Wide Web, we have realized it is a brochure..

  Douglas Adams

- There is a proverb which says: "To err is human", but a human error is nothing to what a computer can do, if it tries.

  Agata Christie, Halloween party

VERY SPECIAL WISDOMS

- Computers are useless. They can only give you answers.

  Pablo Picasso

- The production of too many useful things results in too many useless people.

  Karl Marx

- The real danger is not that computers will begin to think like men, but that men will begin to think like computers.

  Sydney J. Harris

- Ethics change with technology.

  Larry Niven: N-Space

- As technology advances in complexity and scope, fear becomes more primitive.

  Don DeLillo

CONVERGENCE of all TECHNOLOGIES to INFORMATION TECHNOLOGIES

- All technologies will essentially become information technologies, including energy.
- Within several decades information based technology will encompass all human knowledge and proficiency, ultimately including pattern-recognition powers, problem-solving skills, and emotional and moral intelligence of the human brain itself.
- One should note that the term "information technology' is encompassing an increasingly broad class of phenomena and will ultimately include the full range of economic activities and cultural endeavour.
- The exponential trends in information technology are far broader than those covered by Moore's law. We see the same type of trends essentially in every technology or measurement that deals with information.
- There were actually four different paradigms - electromechanical, relays, vacuum tubes, and discrete transistors - that showed exponential growth in the price performance of computing long before integrated circuits were even invented,

INCREASE of ORDER and COMPLEXITY as a FEATURE of (TECHNOLOGICAL) EVOLUTION

Two observations seem to play an important role in an understanding, both biological and also technological, evolution: Both concern information technologies.

- Observation 1: Analysis of truly epochal advances (paradigms shifts) in the history of biology and technology have often involved increases in complexity.
- Observation 2: Analysis of truly epochal advances (paradigms shifts) in the history of biology and technology have mostly involved increases in order.

In this context one should understand: information as a sequence of data that is meaningful in a process and order as information that fits a purpose as well as a measure of order as a measure of how well information fits the purpose.

EVOLUTION ADVANCES and PROCESSING INFORMATION

Other deep observations on advances of evolution:

- A primary reason that the evolution speeds up is that it builds on its own increasing order, with ever more sophisticated means of recording and manipulating information.
- In the case of biological evolution, the most notable early example is DNA , which provides a recorded and protected transcription of life's design from which to launch further experiments.
- In the case of technological evolution, ever improving human methods of recording and processing information have fostered always further advances in technology.

The law of accelerating return

and

Moore law

TECHNOLOGICAL PROGRESS

- Exponential growth is a deep feature of any evolutionary progress, of which technology is a prime example.
- History of technology reveals that that technological change is exponential.
- Since technological progress seems to double each decades what is often assumed that will take one hundred years is likely to take only 25 years.
- Ray Kurzweil formulated his discovery that technological progress happens exponentially as the law of accelerating returns.

EXAMPLE

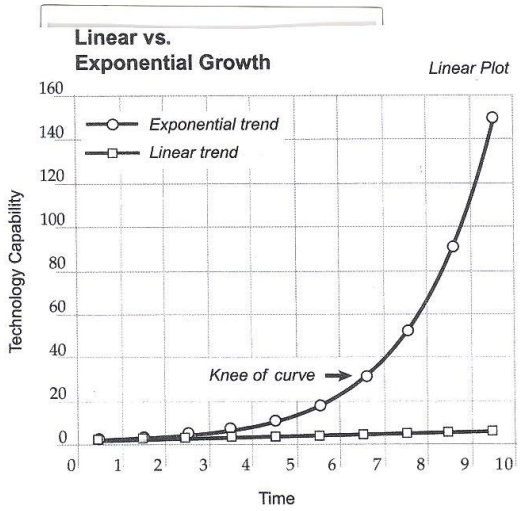
- Biochemists were sceptical in 1990 of the goal of transcribing the entire human genome in a mere fifteen years.
- The reason for pessimism was that at that time they needed whole year to transcribe a mere one ten-thousandth of the genome.
- That was the reason why many expected that to reach the goal will take 100 years.
- However, the goal was reached in just 13 years.
- The main reason behind wrong estimation was that pessimists forgot that techniques and tools for transcription can improve also very fast and pace of transcription will accelerate.

GENERAL GROUNDS for PESSIMISM of SCIENTISTS and ENGINEERS

- They are often so much involved into difficulties and intricate details of their contemporary challenges that they fail to appreciate great long-term impact of their own work and of the whole large field of work in which they operate. They also fail to account for far more powerful tools they are likely to have with each new generation of technology.
- Scientists are trained to be sceptical and to speak cautiously about the potential impacts of their work.
- That could have been an understandable and satisfactory approach when a generation of science and technology lasted longer than a human generation,but this does not serve society's interest now that a generation of a scientific and technology progress often compromises only few years.
- Almost anyone has a linear view of future.That is why people tend to overestimate what can be achieved in short terms (because we tend to leave out necessary details), but underestimate what can be achieved in long terms (because any exponential growth is ignored).

BASIC EXPECTATIONS I

- Computers are getting not only faster and faster they are getting faster faster.
- ICT performance is expected to keep growing exponentially fast in all important aspects. Moreover, we are nowadays only at the beginning of its rapidly fast growing exponential curve for its performance.



Linear versus exponential: Linear growth is steady; exponential growth becomes explosive.

- All that is expected to have enormous impacts.

THE LAW of ACCELERATING RETURNS

- The law of accelerating returns explains why technology, and evolutionary processes in general, progress in an exponential fashion.
- Basic observations: (1) The velocity of computation is proportional to the world knowledge; (2) The rate of change of the world knowledge is proportional to the velocity of computation.

THE PRINCIPLES of THE LAW of ACCELERATING RETURN - I.

- Evolution applies always positive feedbacks: best methods of any stage of the evolution are used to create next stage.
- Each epoch has progressed more rapidly because could use better tools as previous ones.
- Evolution works through "indirection". Evolution created humans; humans created technology; humans in cooperation with very advanced technology create even more advanced technology.
- By the time of Singularity there will not be much difference between humans and technology - because machines will progress to be much as humans and beyond.
- Technology will be metaphorically the "oposable thumb" that enables our next step in evolution.
- Progress will soon occur more and more at the speed close to that of light rather than of very slow electrochemical reactions.
- Each stage of evolution builds on better outcomes/tools that previous stage and the rate of progress of an evolutionary process increases at least exponentially.

MOORE LAW - SEVERAL VERSIONS

Moore's law has now (at least) three forms.

Economic form: Computer power doubles, for constant cost, every two years or so.

Physical form: The number of atoms needed to represent one bit of information should halves every two years or so.

Quantum form: For certain application, quantum computers need to increase in the size only by one qubit every two years or so, in order to keep pace with the classical computers performance increase.

GORDON MOORE and HIS ROAD to HIS LAW

In the mid-1970s Gordon E. Moore, a leading inventor of integrated circuits and later chairman of Intel, observed that we could squeeze twice as many transistors onto an integrated circuits every twenty-four months (in mid-1960s he estimated every twelve months).

Moore also observed that electrons would consequently have less distance to travel, and therefore circuits would also run faster, providing additional boosts to the overall computational power

The result is exponential growth in the price-performance of computation.

Currently, we see that the doubling time for different

MOORE LAW ORIGIN

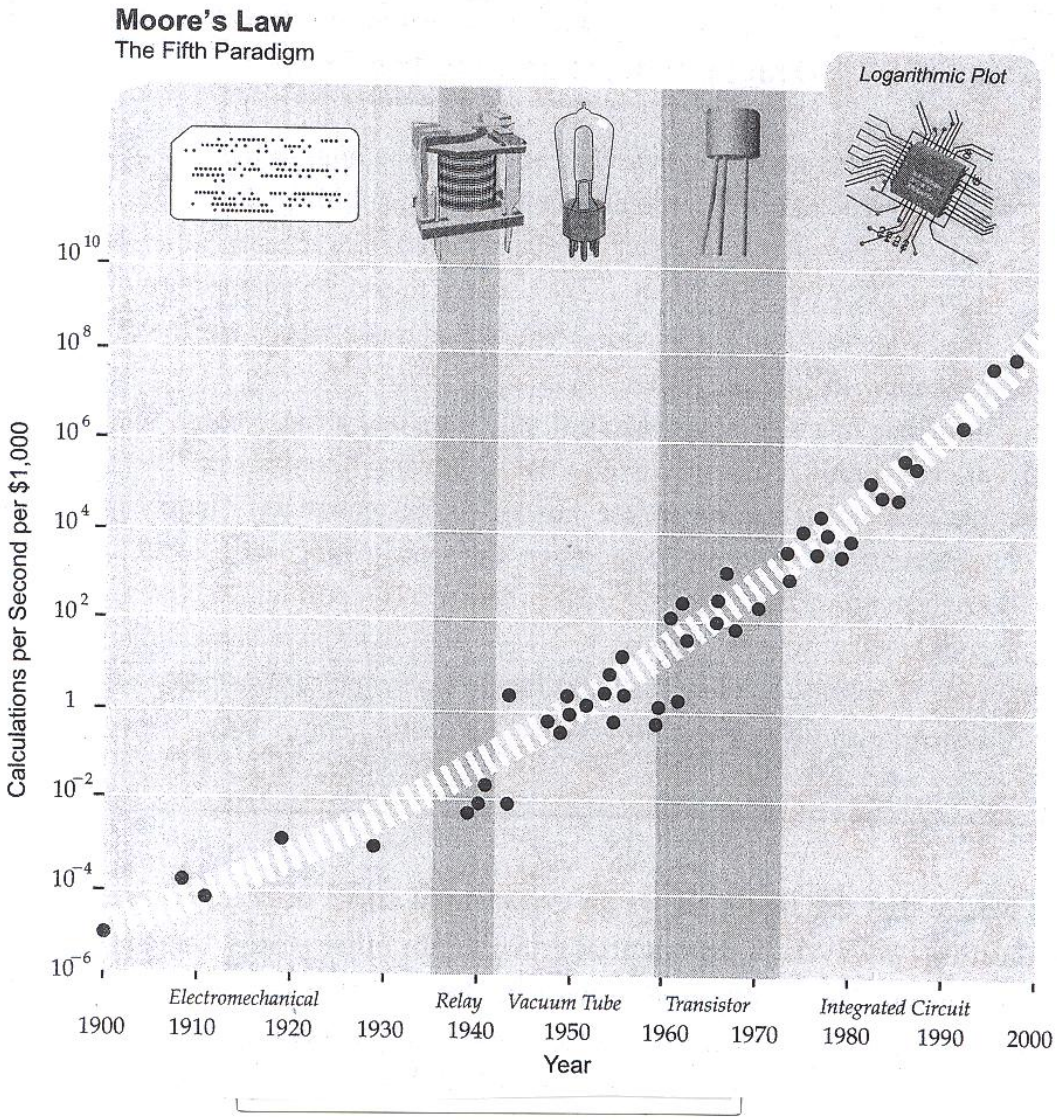
- On April 19, 1965 in *Electronics* Moore wrote "The future of integrated electronics is the future of electronics itself. The advantages of integration will bring about a proliferation of electronic, pushing this science into many new areas."
- Moreover, Moore predicted that "by 1975, economics may dictate squeezing as many as 65, 000 components on a single silicon chip".
- Moore's article described the repeated annual doubling of the number of transistors that could be fitted onto an integrated circuit.
- Moore's initial estimate was incorrect - he revised it a decade later - but the basic idea was valid.

Current situation:

- Top performance chips have 10 millions of transistors per mm^2.
- Top performance CPU have 7 billions of transistors.

Currently, the IPC technology is shrinking by a factor of about four per linear dimension per decade. This miniaturization is a driving force behind Moore's law.

MOORE LAW VISUALLY



General version of the Moore law

Two general observation:

- Exponential growth in the power and price-performance of information-based technologies is not limited to computers but it is true for essentially all information technologies and includes human knowledge - measured in many different ways.
- It is also important to observe that the term "information technology" keeps encompassing an increasingly broad class of phenomena and will ultimately include the full range of economic activities and cultural endeavor.

LIMITATIONS of the MOORE LAW

On the base of quantum mechanics Seth Lloyd determined, in 1999, that an "ultimate laptop" of the mass 1 kg and size 1 l cannot perform more than 2.7×10^{50} bit operations per second.

Calculations of Lloyd were based only on the amount of energy needed to switch from one state to another one.

It seems to be harder to determine the number of bits of such an "ultimate laptop". However, the bound 3.8×10^{126} has been determined for a computer compressed to form a black hole.
It seems to be clear that Moore law cannot hold longer than for another 200 years.

DOUBLE EXPONENTIAL GROWTH

The more effective a particular evolutionary process becomes, the greater are the amount of resources that are deployed toward the further progress of that process and that may result in a double exponential growth.

Example:

- It took three years to double the price-performance of computation at the beginning of the modern computer era (around 1950).
- It took two years around 1980.
- Recently it started to take one year.

A related observation: Not only is each chip doubling in power each year for the same unit cost, but the number of chips being manufactured is also growing exponentially. Consequently, computers research budgets have grown dramatically over the decade.

WISDOM of Gordon E. Moore (2004)

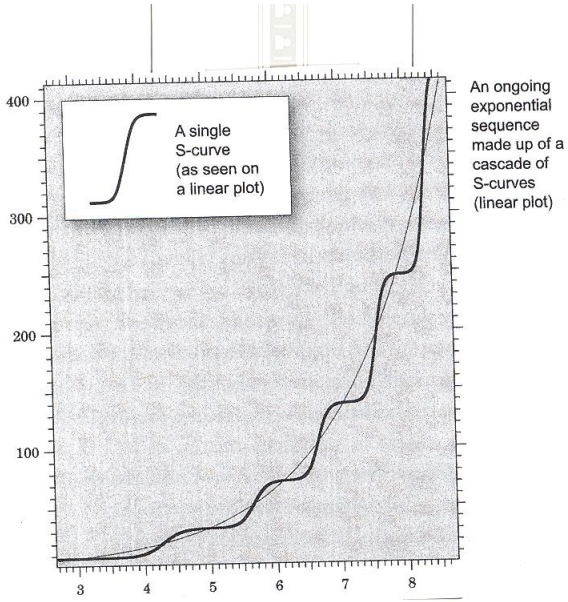
No exponential is forever....but we can delete "forever".

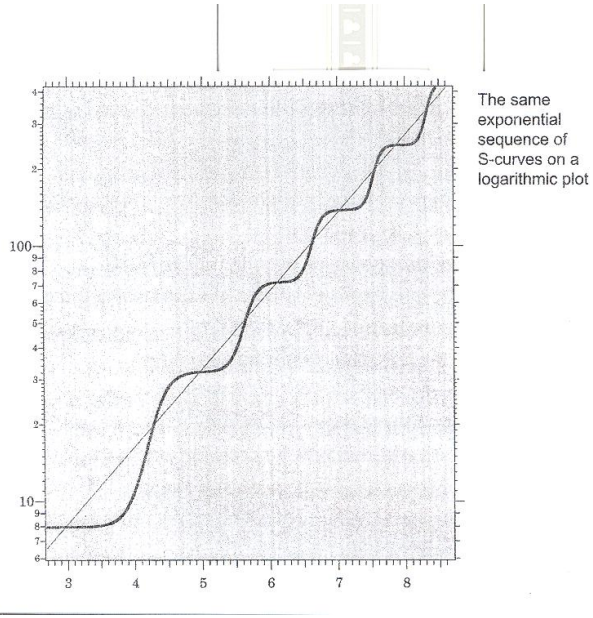
EXAMPLES HOW EVOLUTION SPEEDS UP

- Homo sapience evolved over the course of a few hundred thousands years;
- Early stages of humanoid-created technology (fire, stone-tools, wheel) required for their development tens of thousands years;
- A half millennium ago such products of a paradigm shift as printing press took about a century to be widely deployed.
- Today, the products of major paradigm shifts, such as cell phones or World Wide Web are widely adopted in only few years time.

EVOLUTION as a SEQUENCE of PARADIGMS SHIFTS

Evolution can be seen as a sequence of paradigm shifts, each represented by an "S-curve",as in the following figures showing them in a linear and an exponential plots.



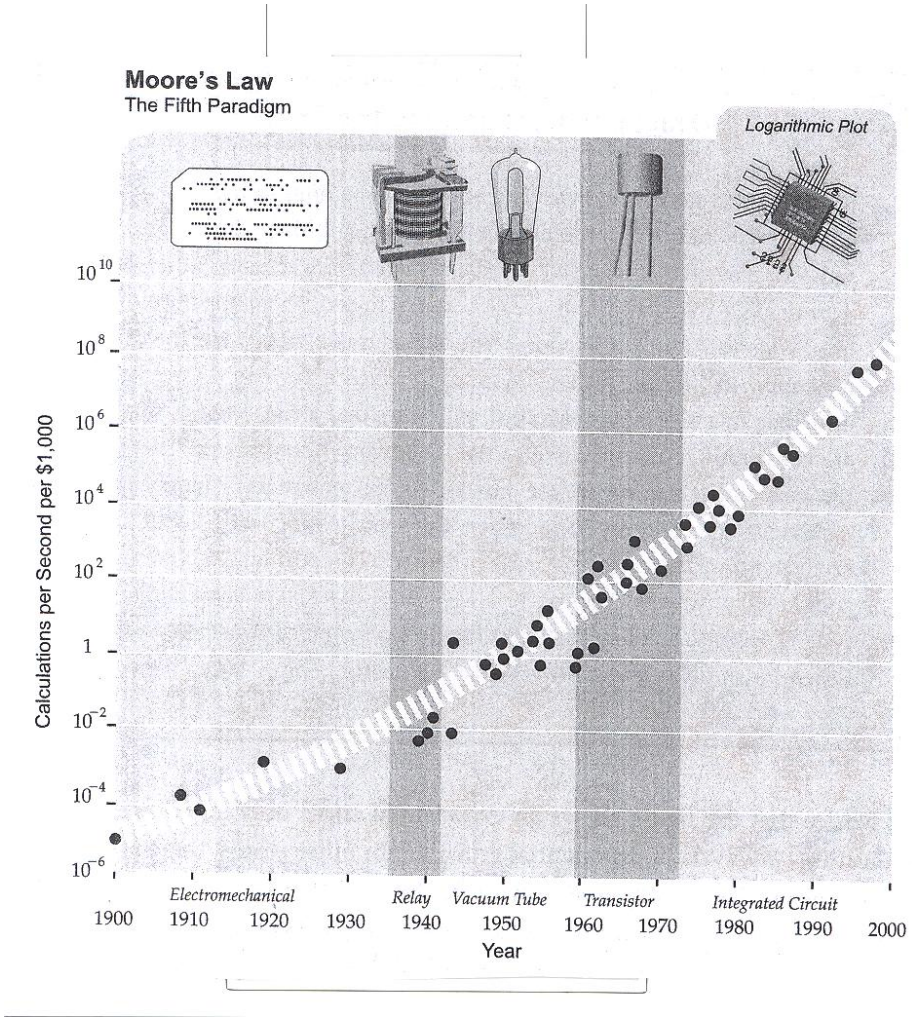


Each paradigm develops in the following three stages:

- Slow growth (as the early stage of exponential growth).
- Explosive stage of the exponential growth
- A leveling off, when the paradigms impact starts to be exhausted and a shift to a new paradigm starts.

The exponential growth of an evolutionary process, therefore, spans multiple S-curves. The most important contemporary example of this phenomenon is the five paradigms of computation discussed later.

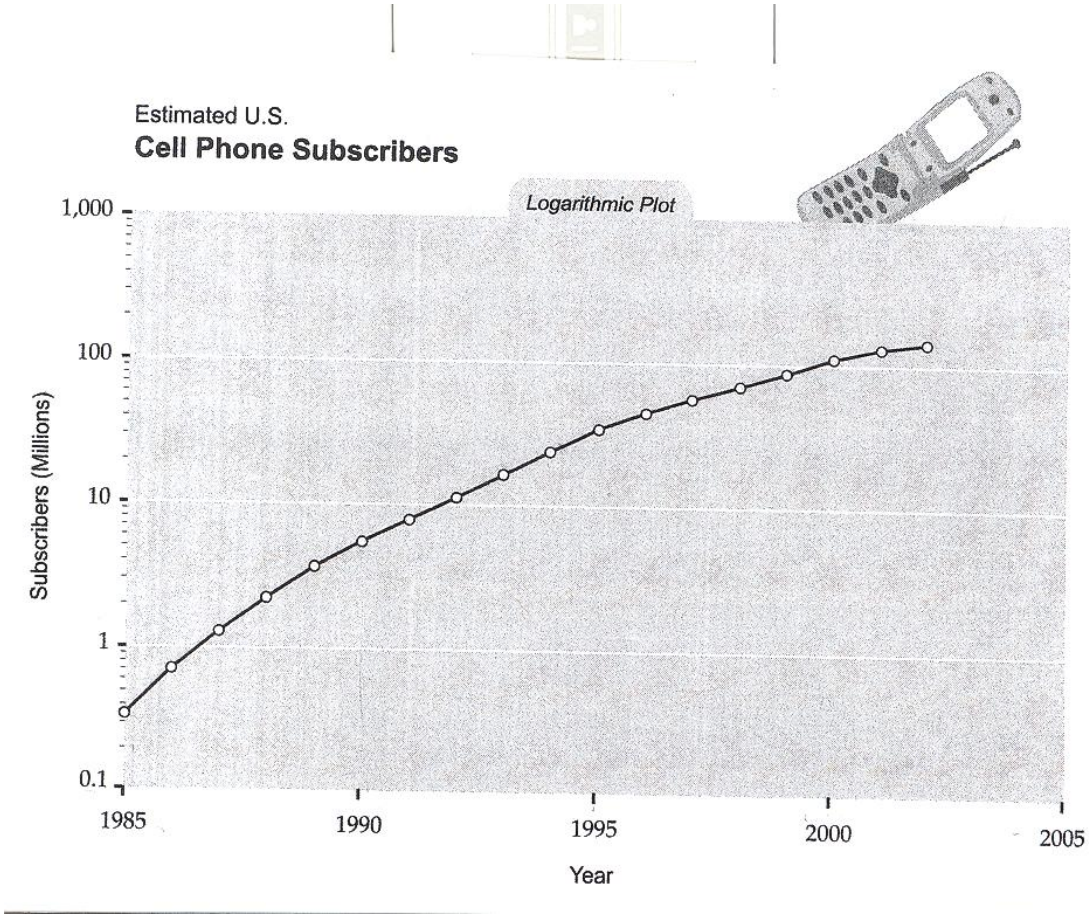
FIVE PARADIGMS BEHIND EXPONENTIAL GROWTH in COMPUTING



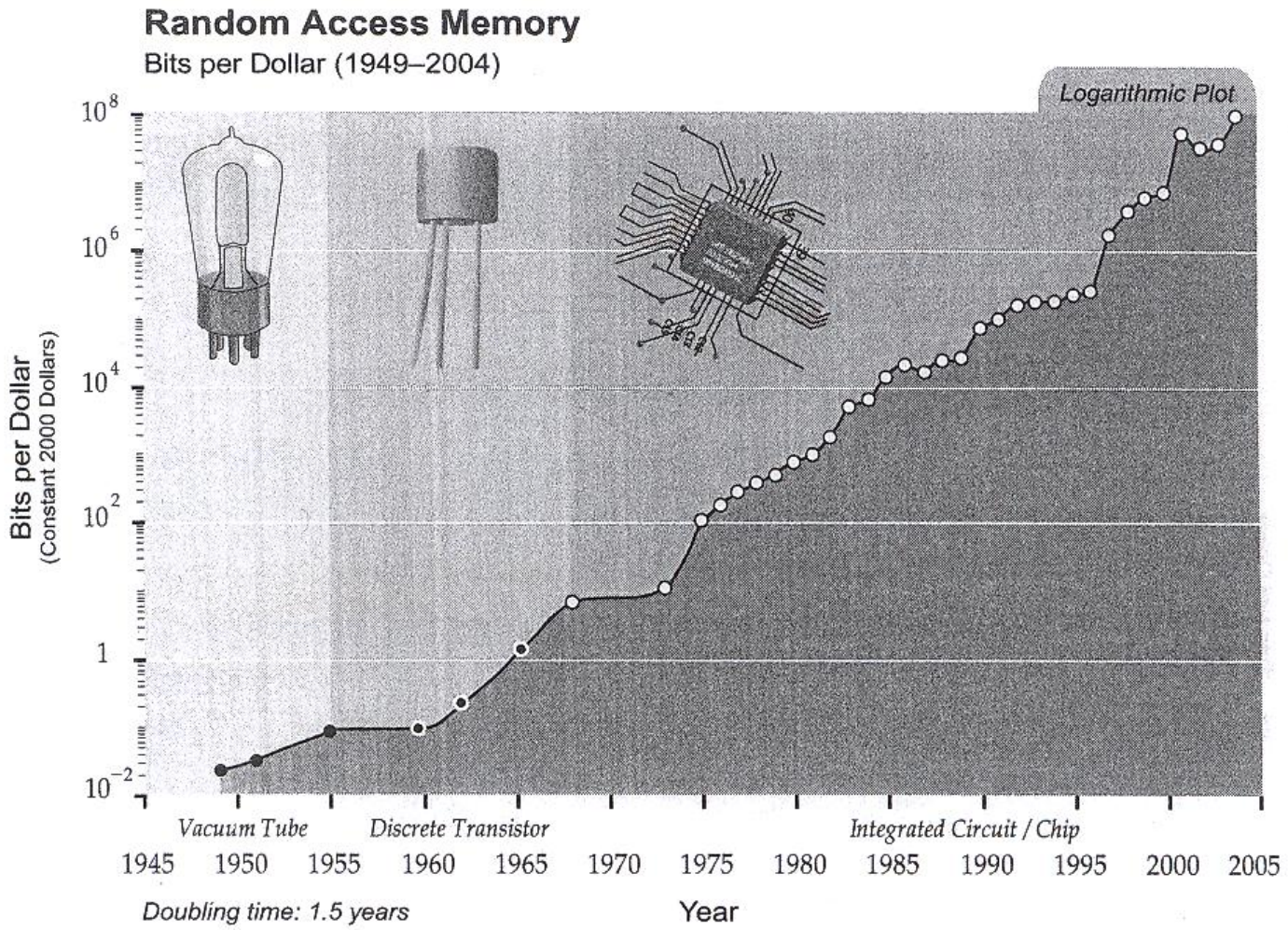
Observe that each time a paradigm "has run out of the steam" another has picked up the pace.It is expected that the three-dimensional molecular computing could be the next paradigm.

Examples of the exponential growth in ICT

An EXAMPLE of the ACCELERATION of PARADIGMS SHIFTS



EXPONENTIAL GROWTH in RAM CAPACITY ACROSS PARADIGM SHIFTS



Exponential growth in RAM capacity across paradigm shifts.

COMMENTS

In case of the technology evolution, we can observe the following situations:

- During the third maturing phase in the life cycle of a paradigm, pressure increases to build/prepare a new paradigm shift and a lot of research money go for that.
- Example: The extensive research is nowadays conducted toward three-dimensional molecular computing - despite the fact that there is still at least a decade left for the paradigm of shifting transistors on flat integrated circuits using photolitography.
- In addition, often when a paradigm starts to reach its saturating phase, a new paradigm is often developed already into such a level that it works in some niche applications.
- Example: In 1950's engineers were working hard to shrink vacuum tubes to provide greater price-performance for computers. At this point, around 1960, transistors had already achieved a strong niche market in portable radios and were subsequently used to replace vacuum tubes in computers.

RESOURCES UNDERLYING EXPONENTIAL GROWTH of EVOLUTIONARY PROCESSES

- Resources are relatively unbounded.
- Resource 1: Each stage of evolution provides more powerful tools for the next one.
- Examples: (1) In biological evolution, the advent of DNA enabled more powerful and faster evolutionary experiments; (2) The advent of computer-assisted design tools allows rapid development of the next generation of computers.
- Resource 2: Impact of (often very diverse/chaotic) environments puts pressure for finding more powerful and more efficient solutions.
- Examples: (1) In biological evolution. one source of diversity is the mixing and matching of gene combinations through sexual reproduction - an evolutionary innovation that accelerated the process of biological adaptation and diversity;(2) In technological evolution, that is human ingenuity combined with variable market conditions that keep the process of innovation going.

EVOLUTION and DESIGN of BIOLOGICAL SYSTEMS

One of key questions of biological evolution and systems is how it is possible for the genome, which contains relatively little information, to produce so much more complex systems as humans.

- There are only eight hundred million bytes of information in the entire human genome, and only 30-100 millions after data compression is applied.
- This is about one hundred million times less information than is represented by inter-neural connections and neurotransmitter concentration patterns in a human brain.

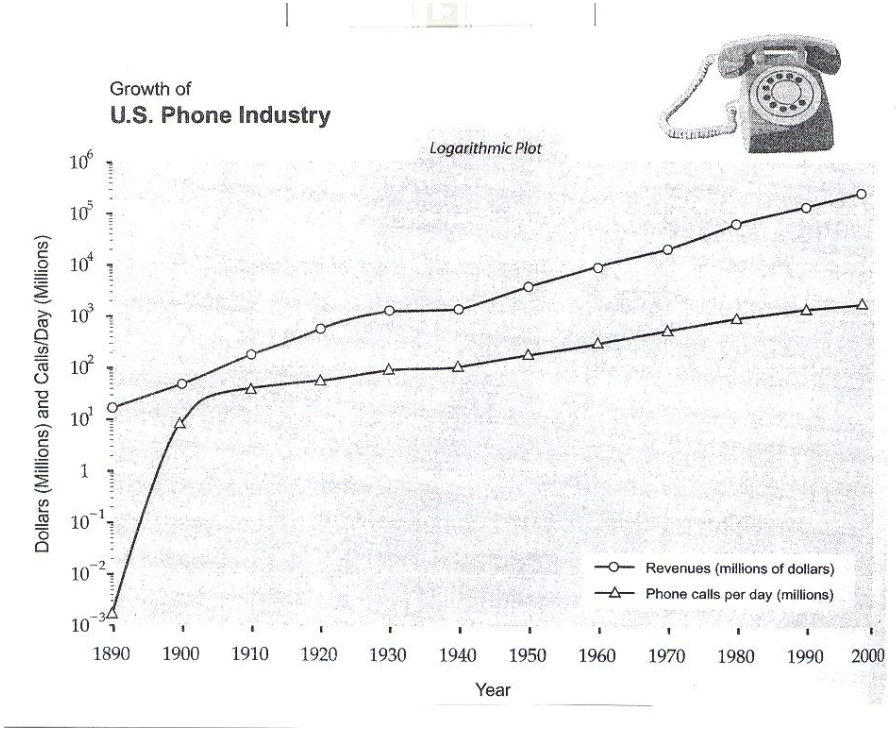
The best answer available seems to be that biological designs are specified through randomized fractals descriptions

APPLICATION of the LAW of ACCELERATING RETURN to SIX EPOCHS

- The combination of amino acids into proteins and of nucleic into strings of RNA established the basic paradigm of biology.
- Strings of RNA (and later DNA) that self-replicated (Epoch Two) provided a digital method to record results of evolutionary experiments.
- The evolution of species that combine rational thought (Epoch Three) with an oposable appendage (the thumb) caused a fundamental paradigm shift from biology to technology (Epoch Four).
- The upcoming primary paradigm shift will be from the biological thinking to a hybrid combining biological and non-biological thinking (epoch Five).

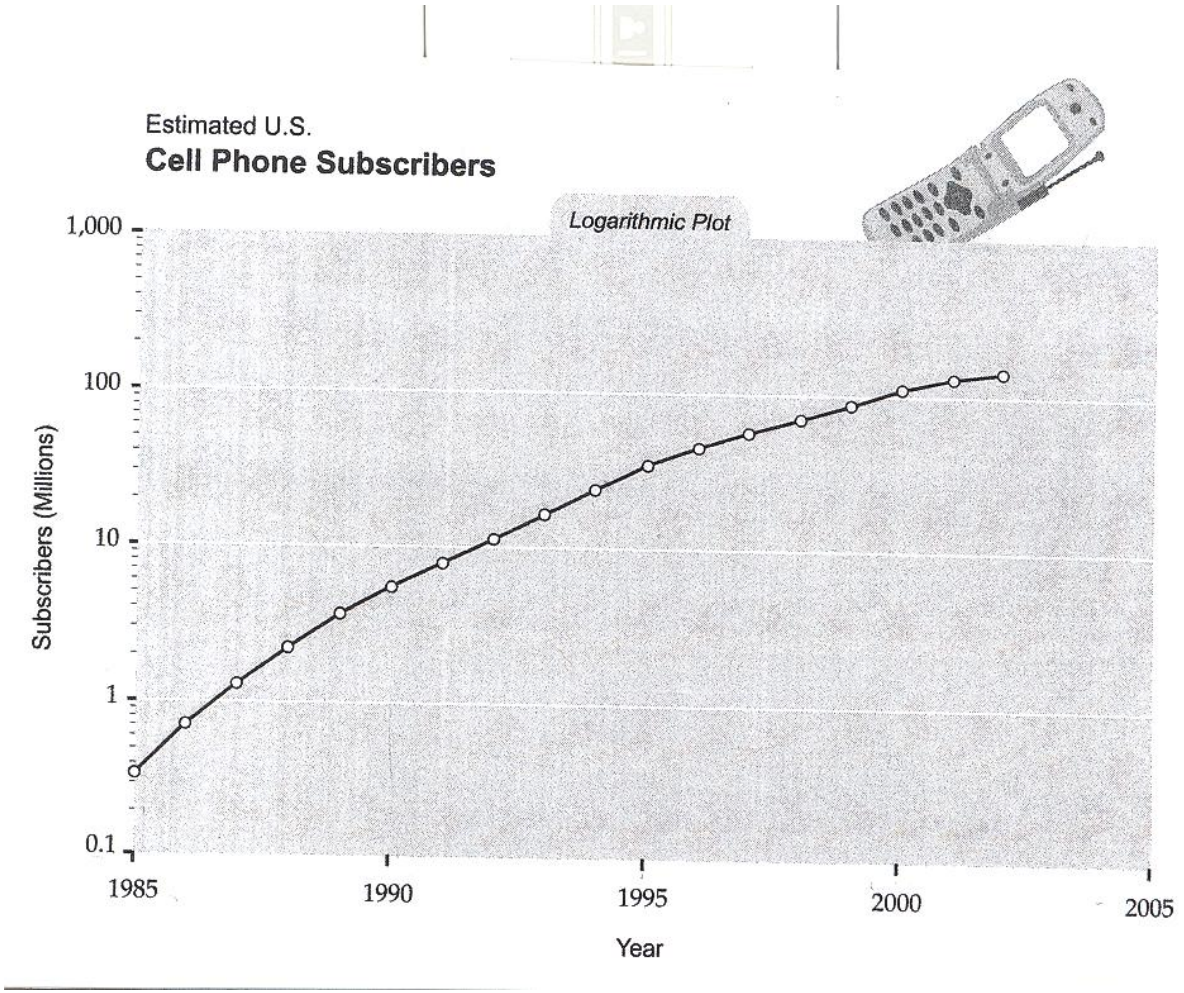
Example 1a: THE ACCELERATION of the TECHNOLOGY PARADIGM SHIFT RATE

The following picture shows how long it took for the late-nineteen century invention - telephone - to reach significant level of usage:



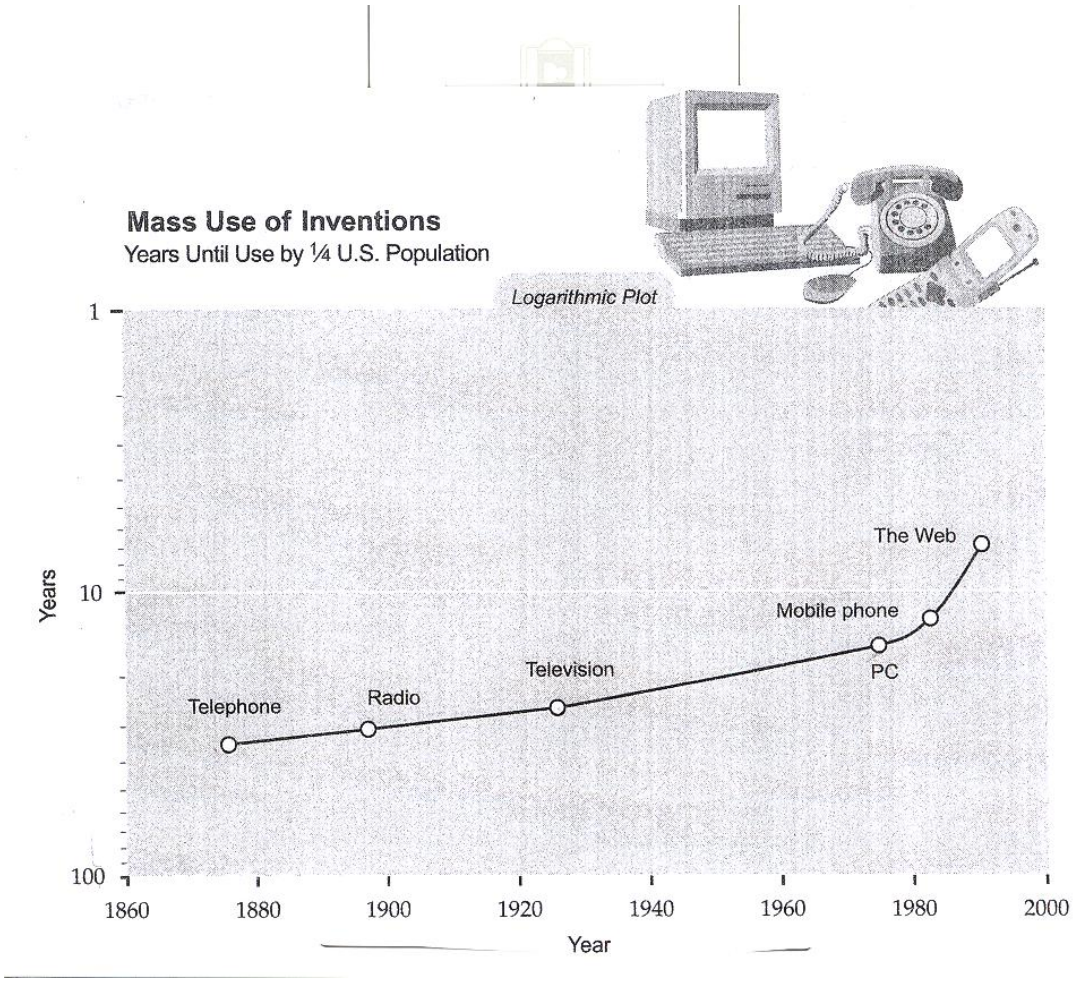
Example 1b: THE ACCELERATION of the TECHNOLOGY PARADIGM SHIFT RATE

The following picture shows that it took only a decade for the late-twentieth-century adoption of cell phones:



AN ACCELERATION of the ADOPTION of COMMUNICATION TECHNOLOGIES

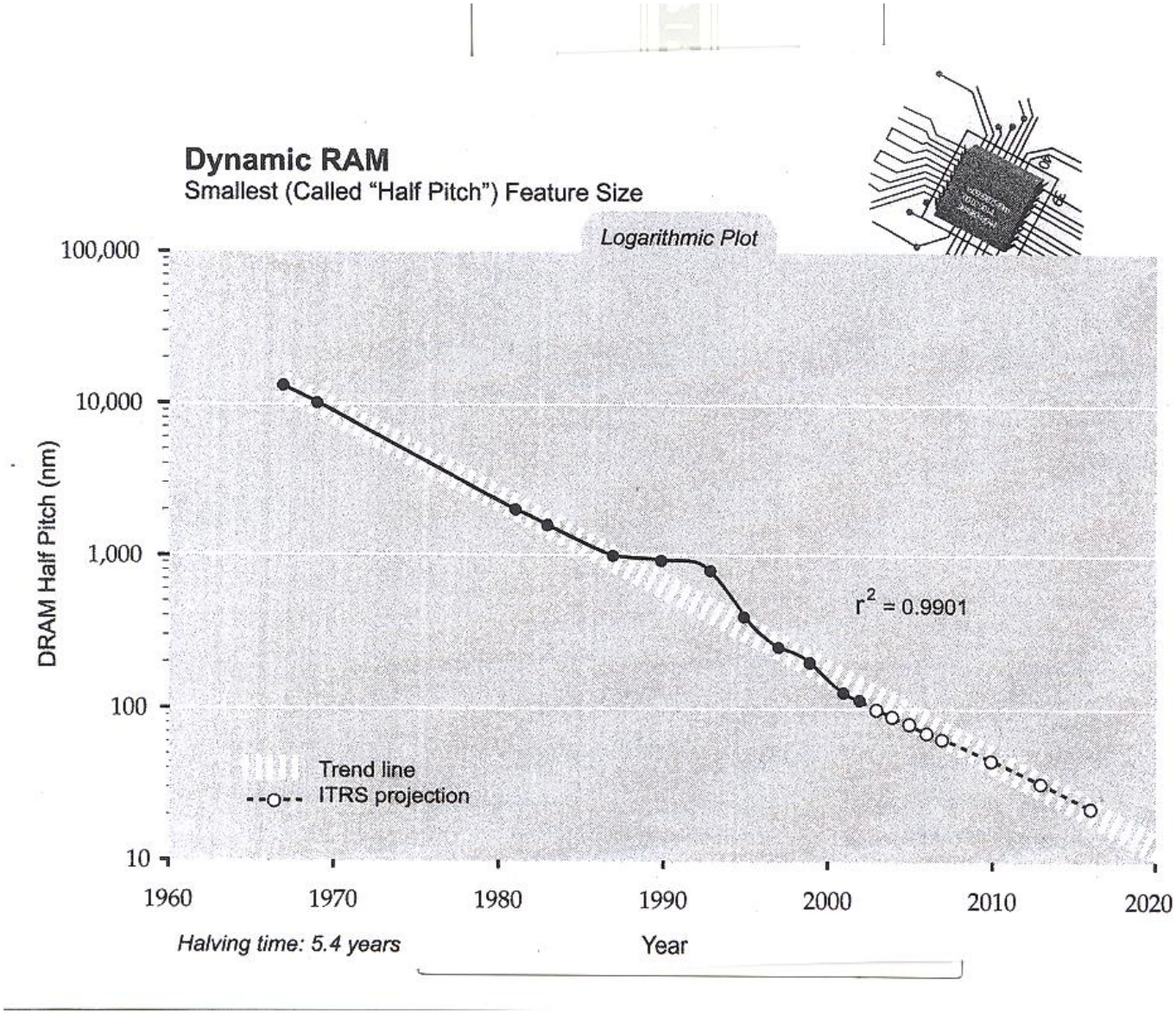
The following figure demonstrates a smooth acceleration in the adoption rates of communication technologies over the past century:



DEVELOPMENTS in SEMICONDUCTOR INDUSTRY

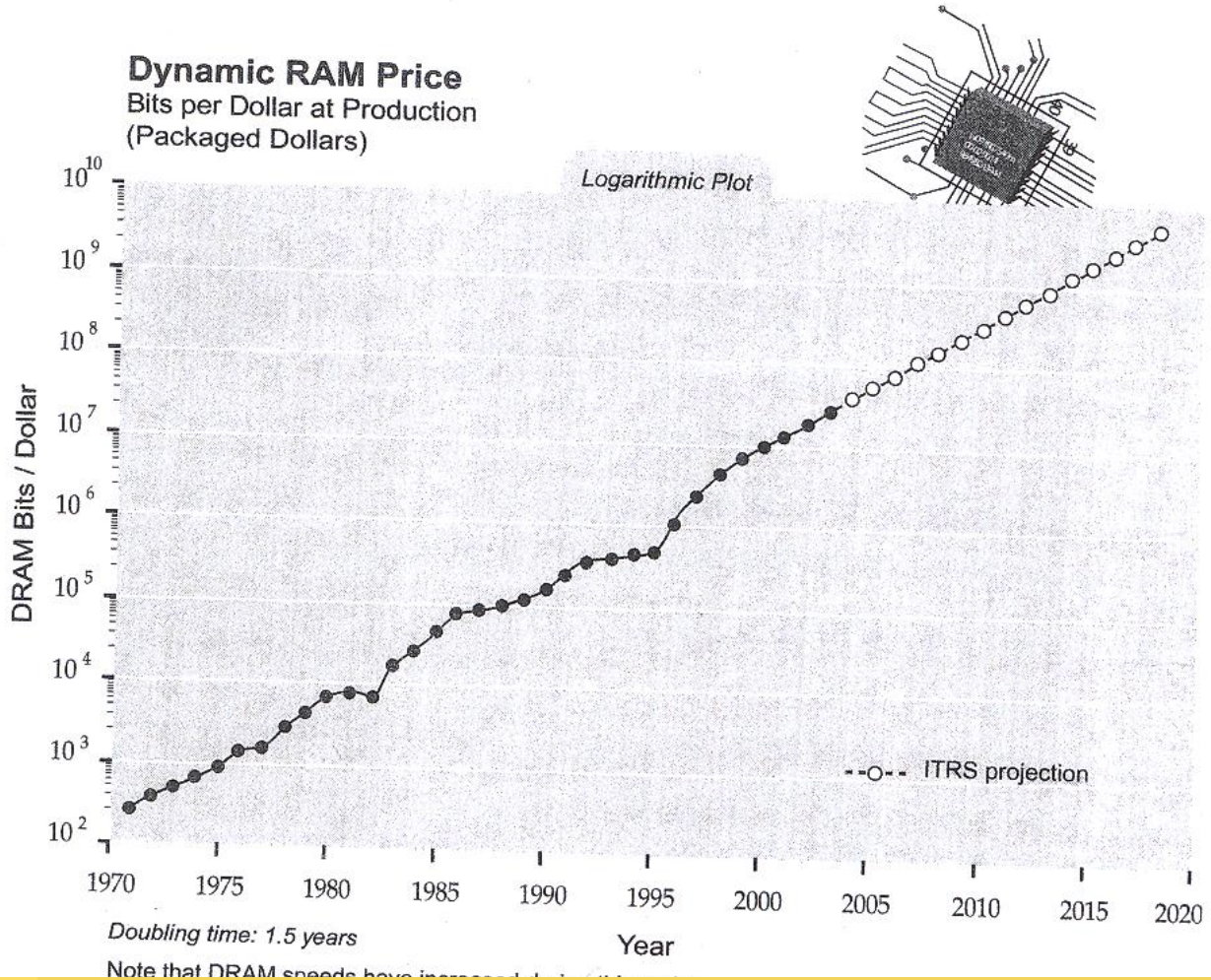
In the following charts various data from the "Semiconductor industry road maps up to 2018' are presented to demonstrate developments according to the Moore law.

DYNAMIC RAM


Dynamic RAM
Smallest (Called "Half Pitch") Feature Size
Logarithmic Plot
100,000
10,000
1,000
100
10
DRAM Half Pitch (nm)
r^2 = 0.9901
Trend line
ITRS projection
1960
1970
1980
1990
2000
2010
2020
Halving time: 5.4 years
Year

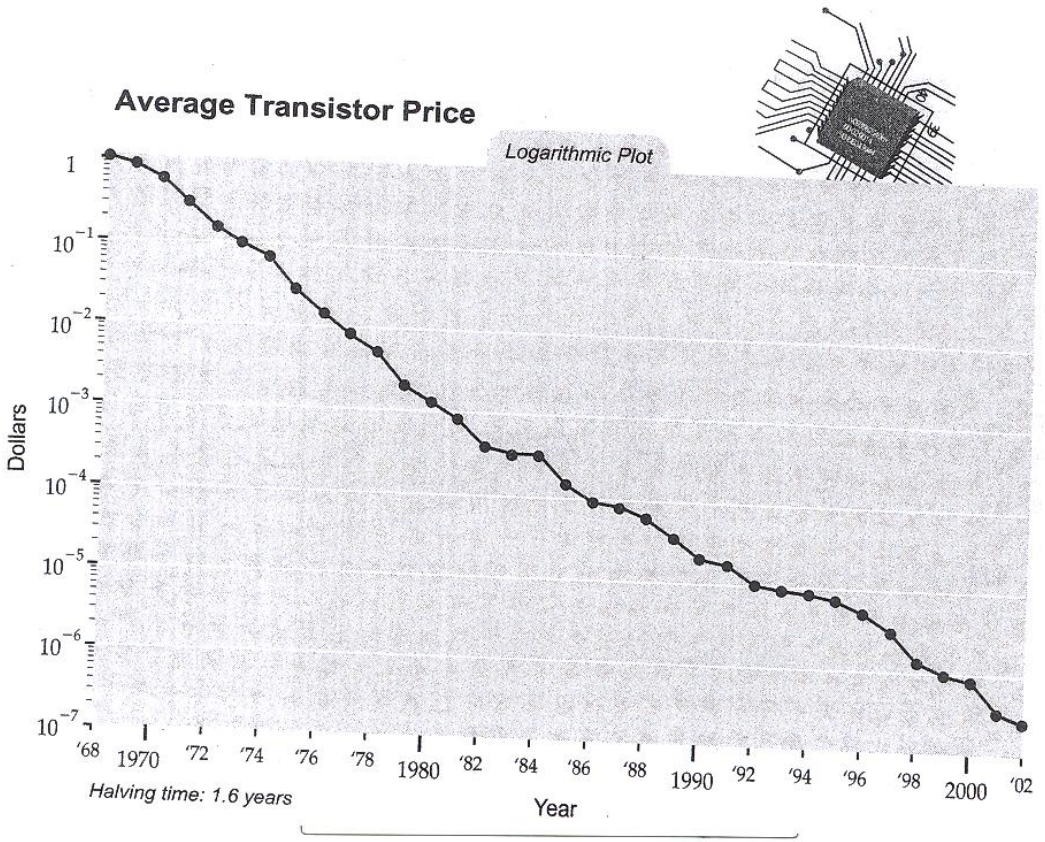
DYNAMIC RAM PRICE

The doubling time for bits of DRAM has been only 1.5 years.



AVERAGE TRANSISTOR PRICE

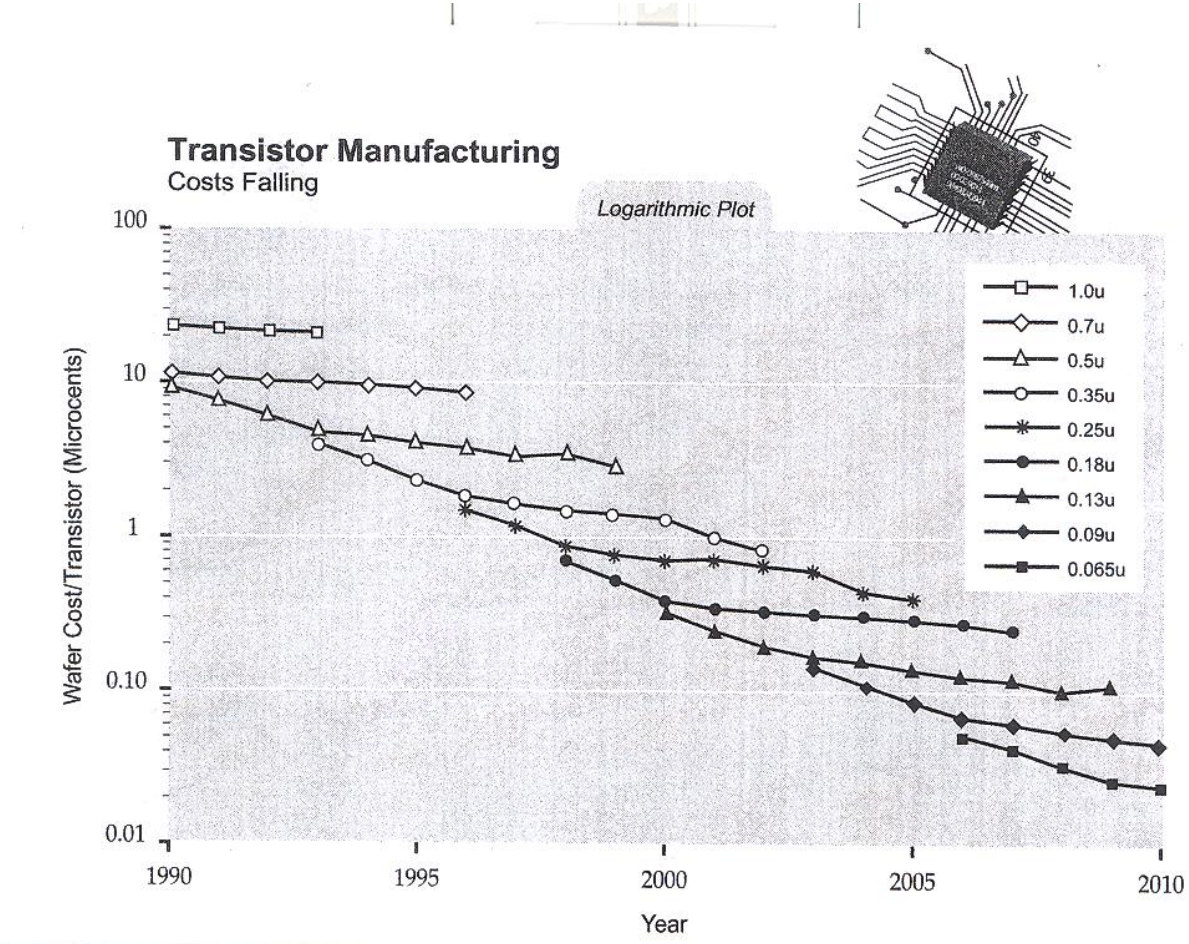
In 1968 one could buy one transistor for a dollar; in 2002 one could get about ten million transistors for a dollar.



Halving time for average transistor price has been about 1.6 years.

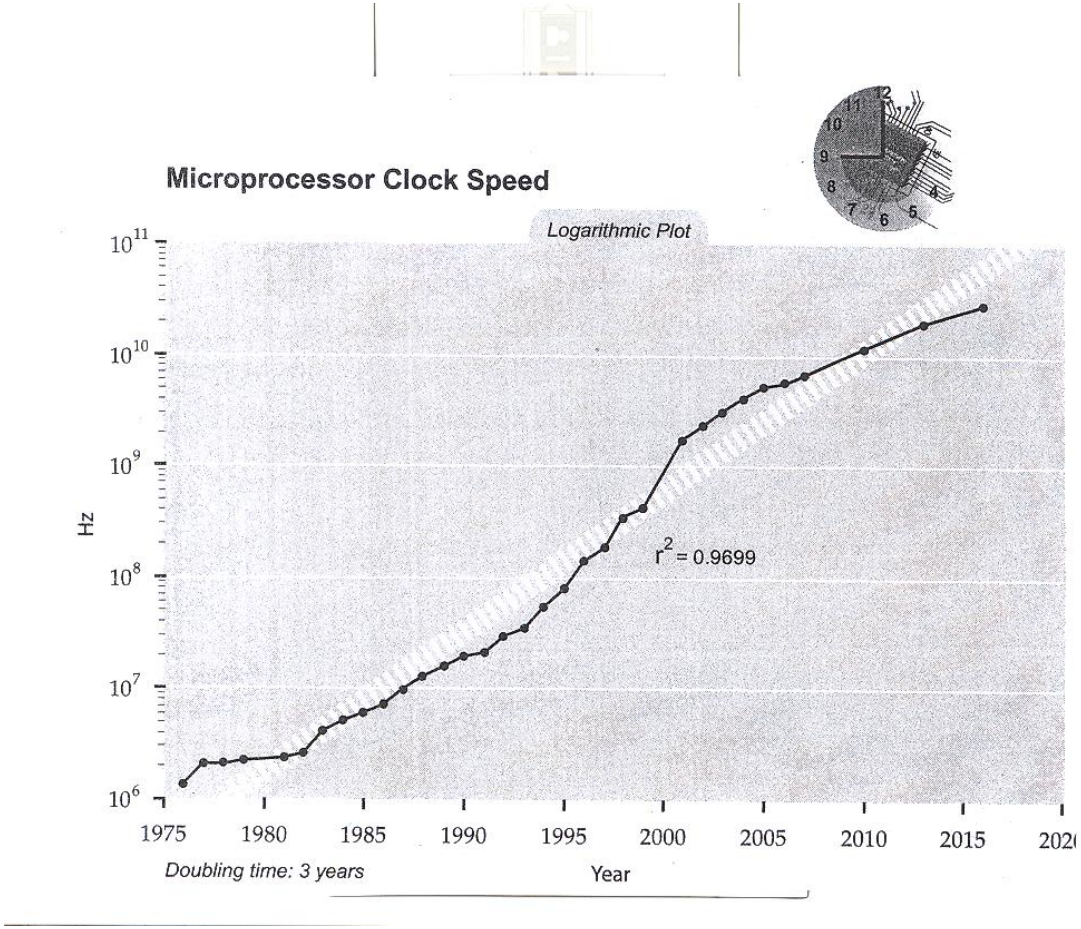
TRANSISTORS MANUFACTURING

Very smooth acceleration in price-performance of semiconductors has progressed through series of stages of process technologies at ever smaller dimension.



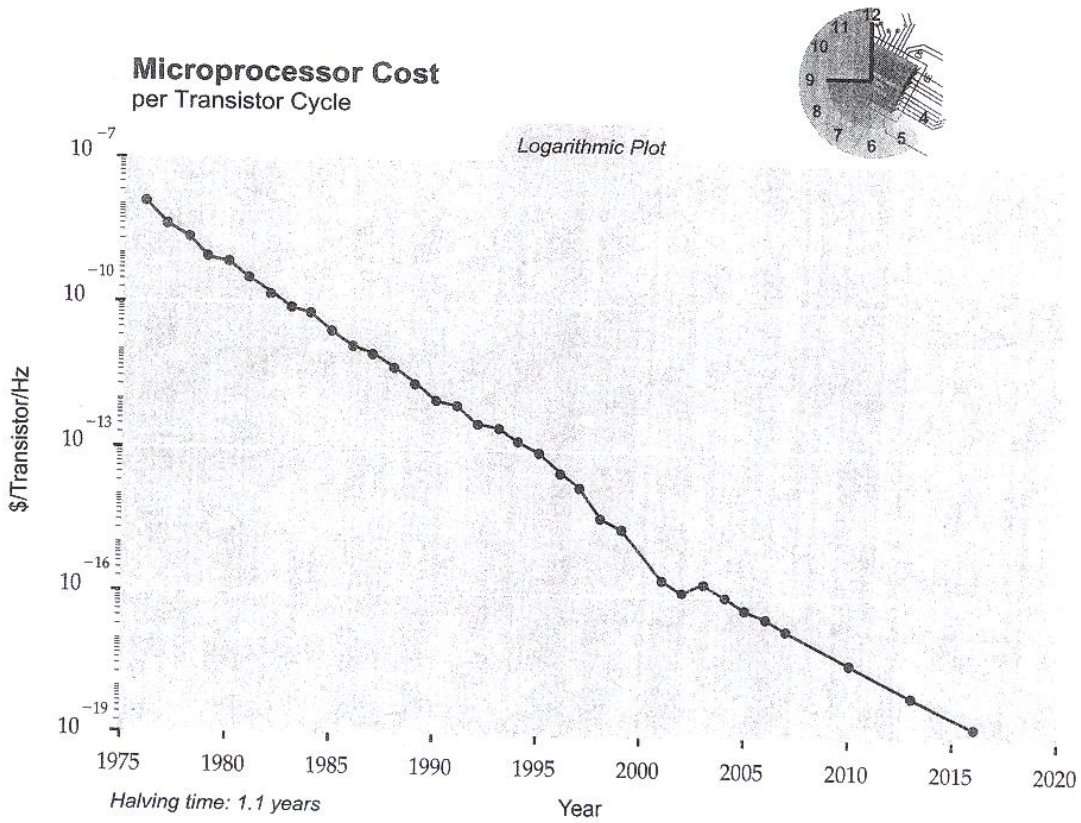
MICROPROCESSOR CLOCK SPEED

As transistors become smaller and less expensive they also become faster, because of less distance electrons had to travel, by about a factor one thousand over the past thirty years.



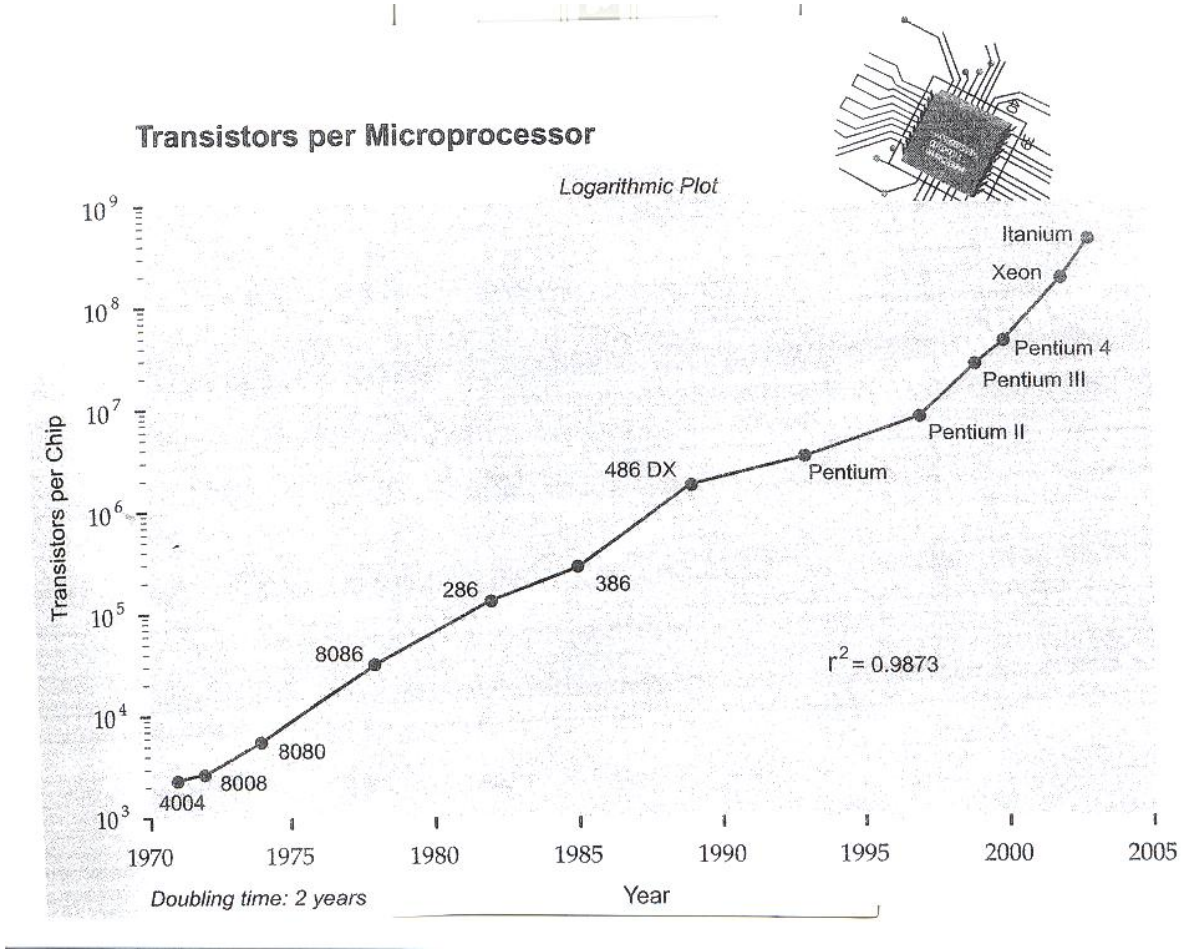
MICROPROCESSOR COST per TRANSISTOR CYCLE

If the exponential trend towards less-expensive transistors and faster cycle times are combined the halving time is 1.1 years in the cost per transistor cycle.



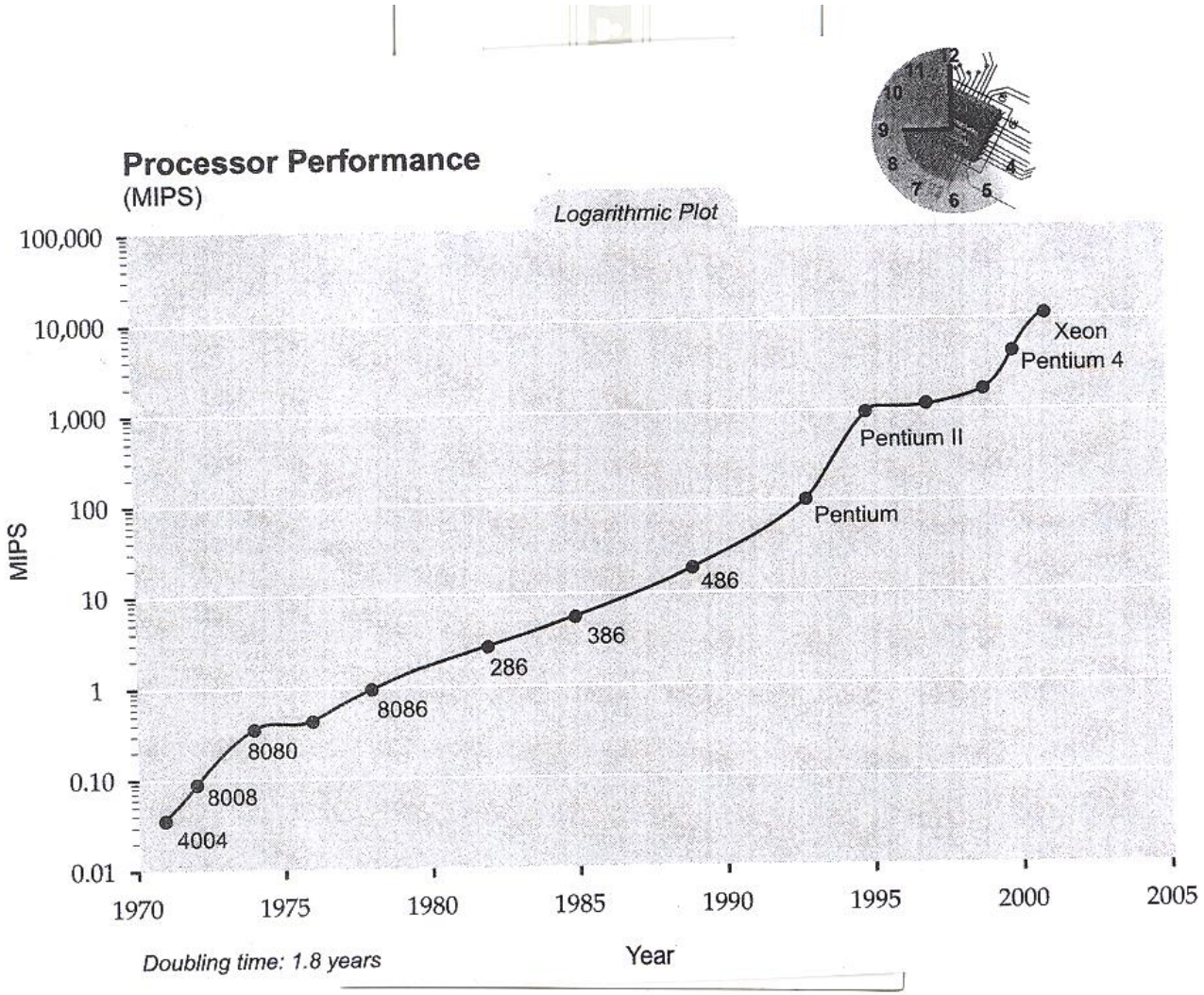
TRANSISTORS per MICROPROCESSORS

The number of transistors in Intel processors has doubled every two years.



PROCESSOR PERFORMANCE

Processor performance in MIPS has doubled every 1.8 years per processor.



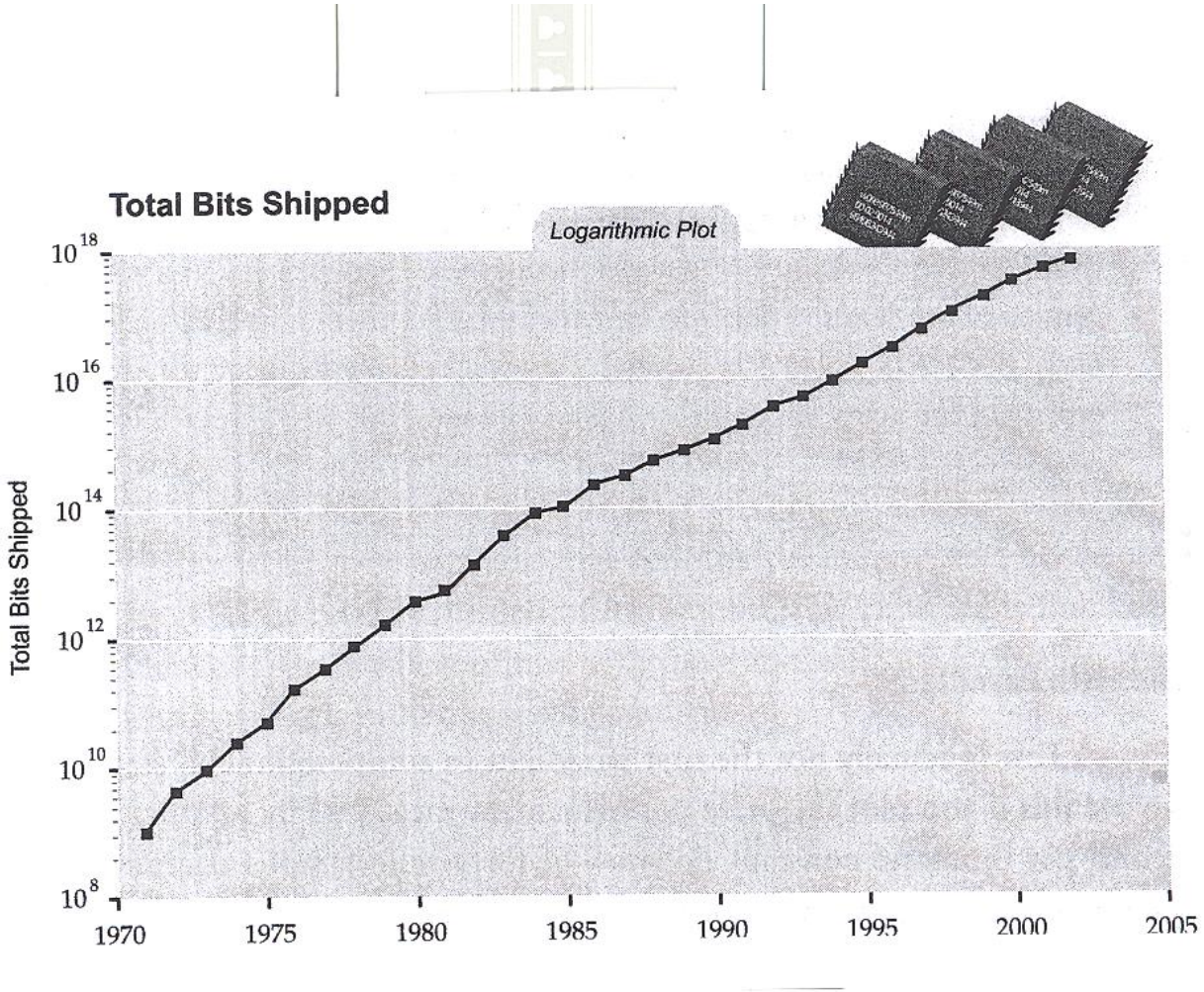
AN EXAMPLE of PERFORMANCE INCREASES

1967 - IBM 7094 : processor speed (MIPS) 0.25; main memory (K Bytes) 144; approximate cost (2003 $) 11, 000, 000.

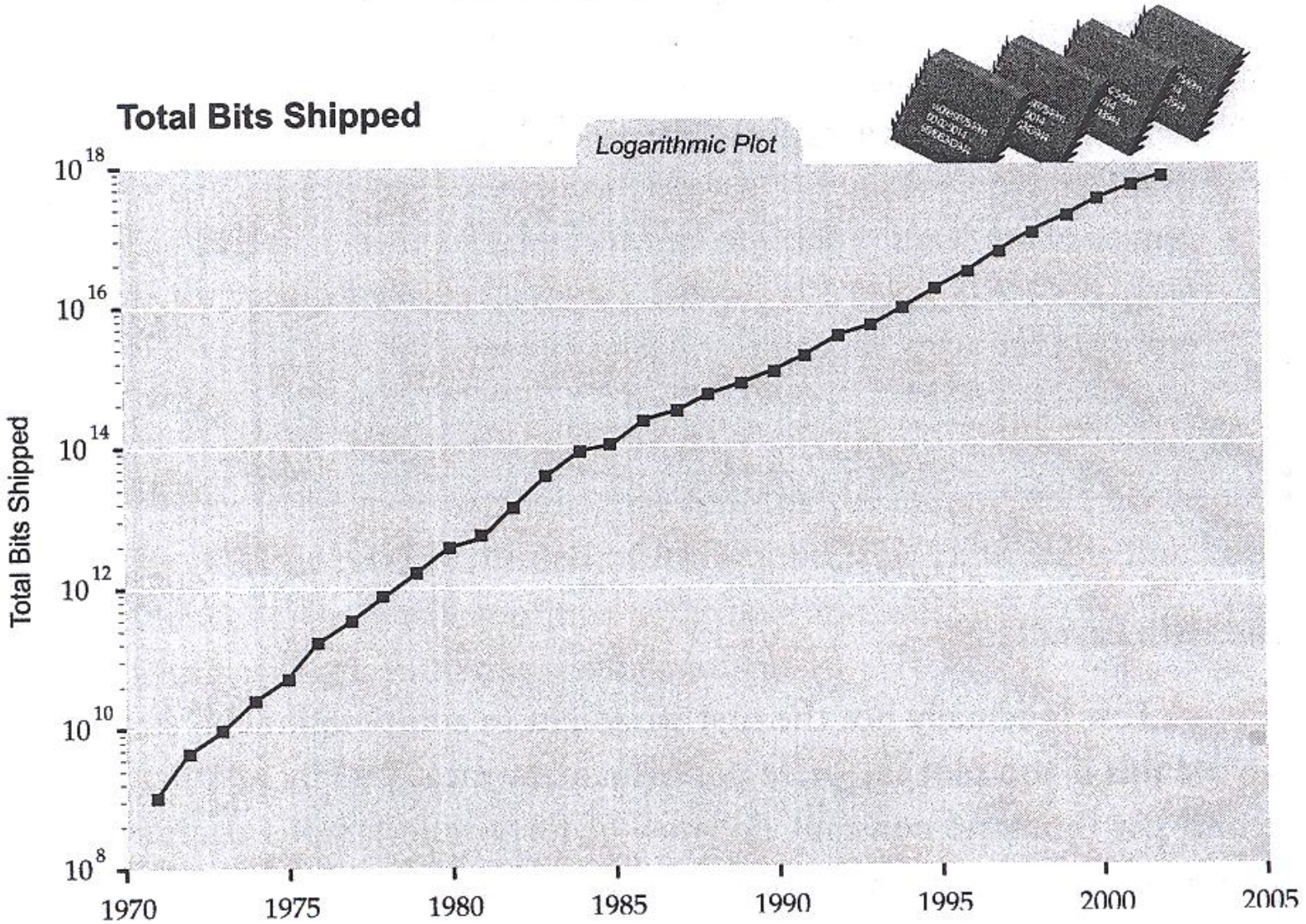
2004- notebook processor speed (MPIS) 2, 000; main memory 256 000; cost 2000

TOTAL BITS SHIPPED

Despite massive deflation in the cost of IT, demands has more than kept up:



TOTAL BITS SHIPPED

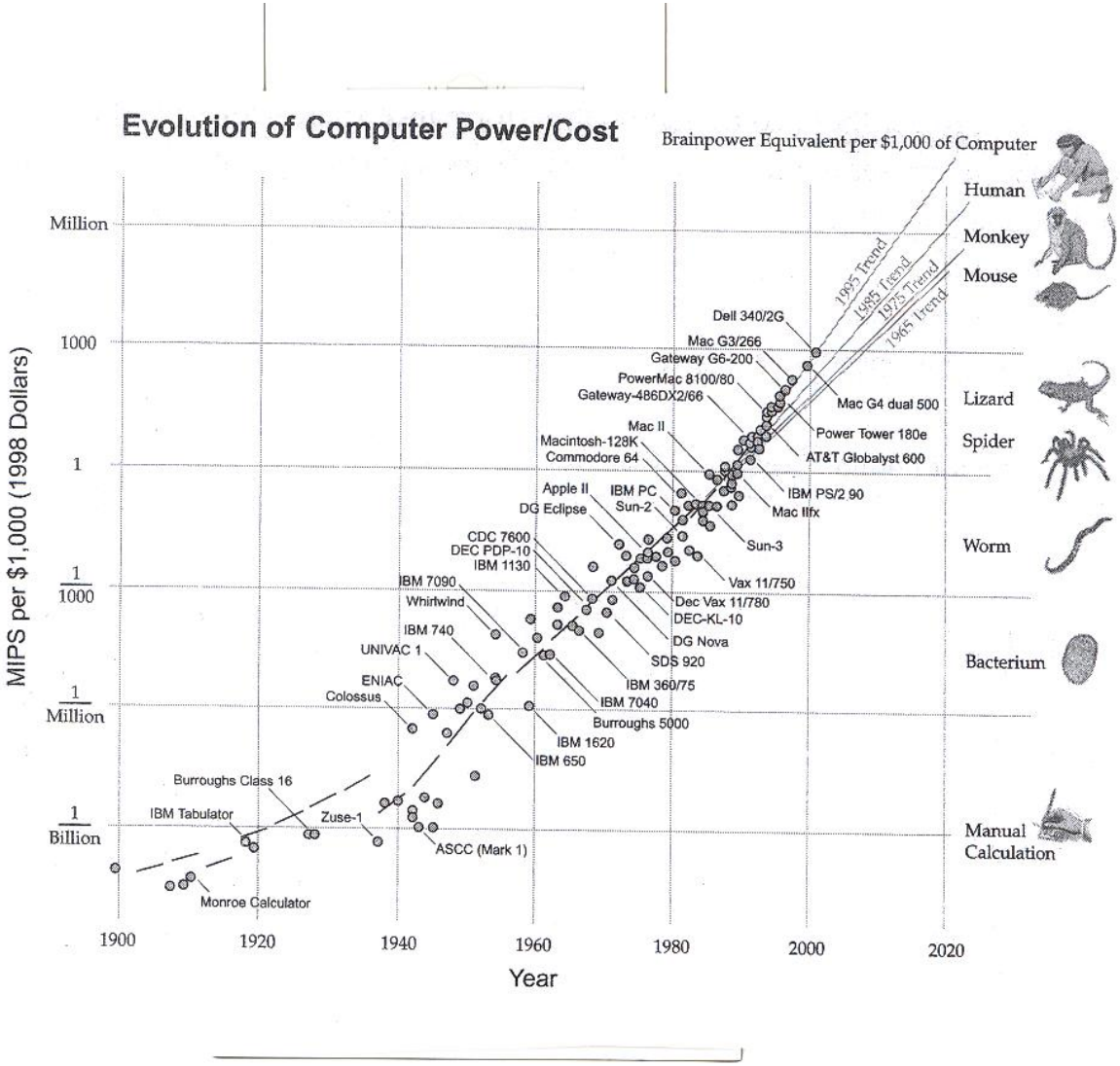


OVERALL IMPACT of IT in US

- The entire IT industry has grown from 4.2% of GDP in 1977 to 8.2% in 1998.
- Semiconductor industry enjoyed 18% annual growth in total revenue from 1958 to 2002.
- IT has become increasingly influential in all economic sectors.
- Even very common manufactured products have significant IT contribution through computers-driven design and manufacturing processes.

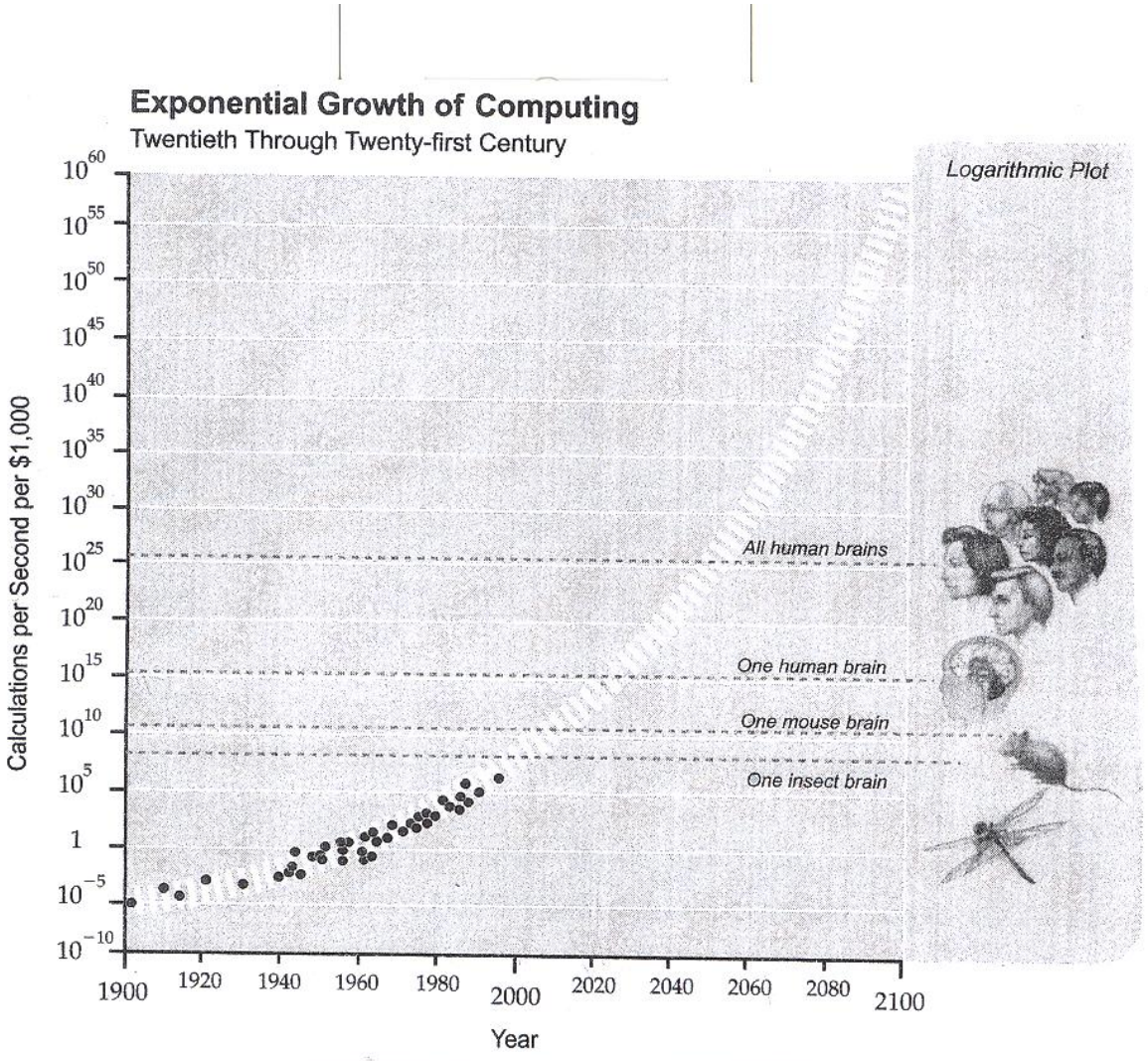
EVOLUTION of COMPUTER-POWER COST

The following chart (H. Moravec) plots the evolution of computer power/cost (brainpower equivalent to $ 1,000 computer, using various historical computers. Observe that slope increases with time demonstrating double-exponential growth.

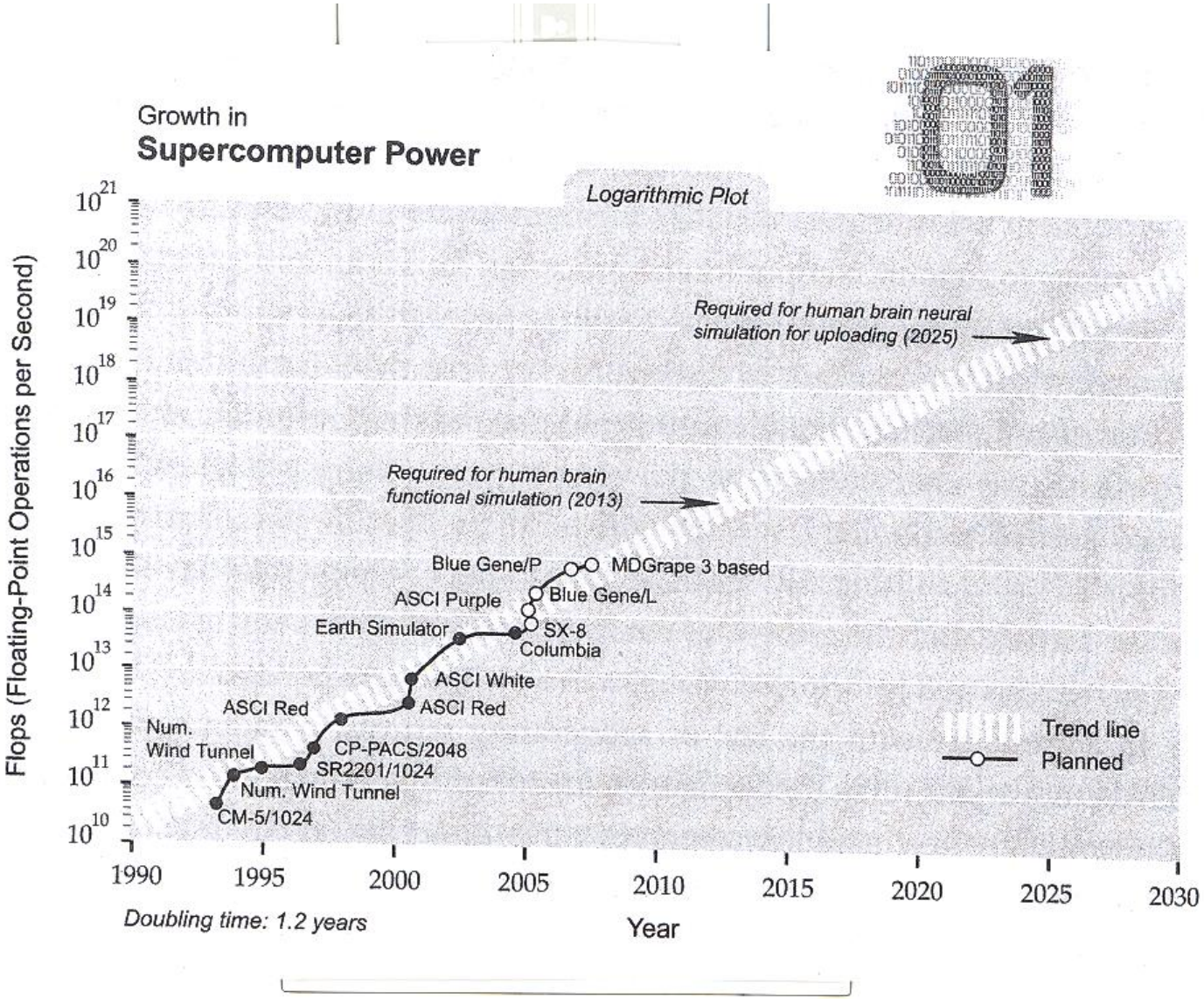


COMPUTER PERFORMANCE TRENDS PROJECTED TO NEXT CENTURY

Next figure predicts that supercomputers will match human brain capabilities by the end of this 2030 an personal computers will do that around 2040.



SUPERCOMPUTER POWER - ESTIMATIONS in 2005



MOST POWERFUL SUPERCOMPUTERS NOWADAYS

1. Titan, Cray XK7, OAK Ridge, 17.6 petaflops, 560,640 processors
2. Sequoia, IBM BlueGene, 16.32 petaflops, 1,472,864 cores
3. K, Fujitsu, 11 petaflops, 705,024 cores
4. Mira, IBM BlueGene/Q Argone National Lab., 10 petaflops, 786,432 cores
5. Juqueen, IBM BlueGene/Q, Juelich, Germany, 5 petaflops, 393,206 cores

In November 2012 there were 23 computer systems with petaflop performance.

Performance of the computer on 100 position increased in six months from 172 to 241 Teraflops

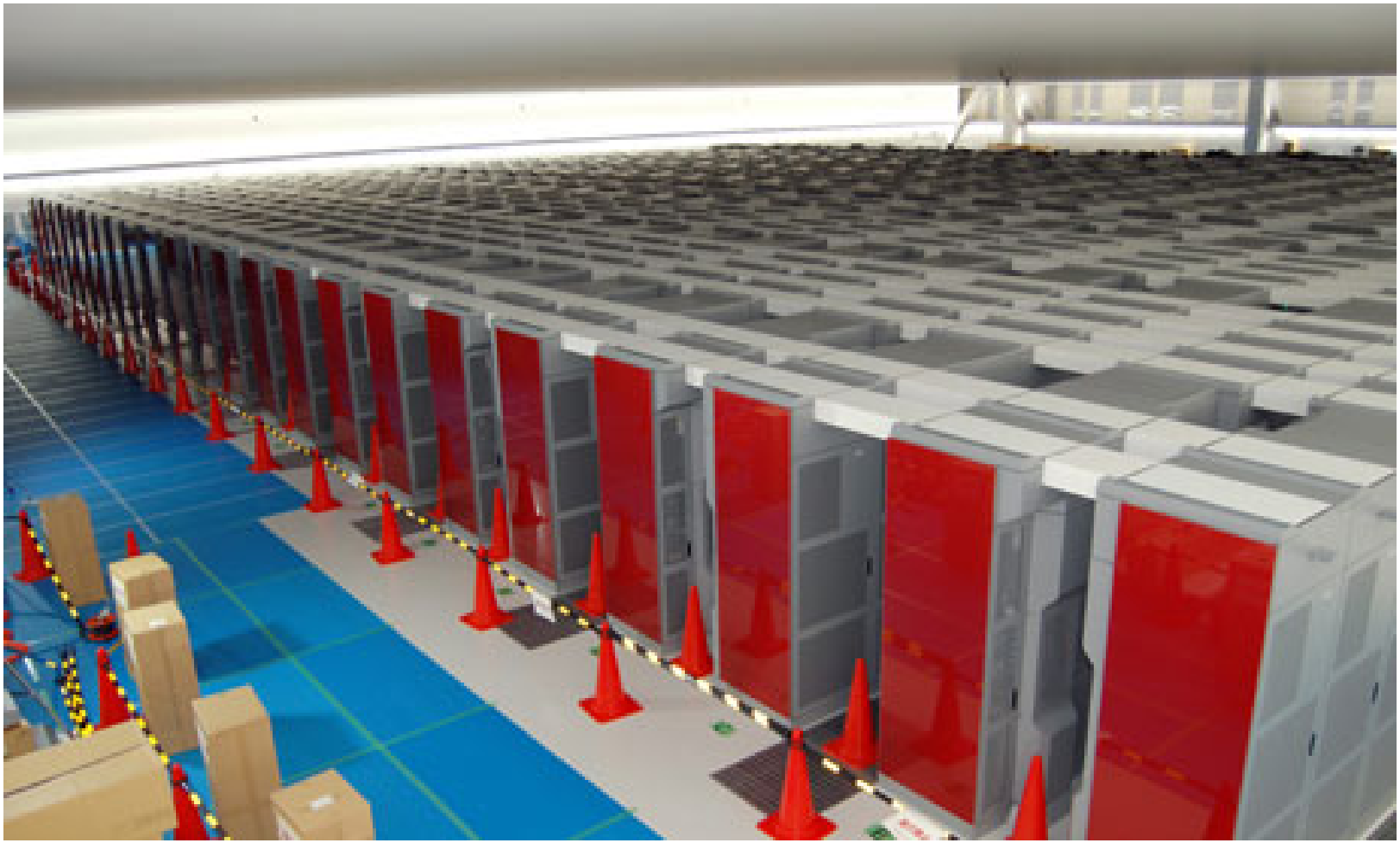
Out of 500 most powerful computer systems, 251 was in US, 123 in Asia, 105 in Europe

Performance of the top computer, in the November lists, in petaflops: 1.7 in 2009, 2.6 in 2010, 10.5 in 2011, 17.6 in 2012 - 10-times increase in 3 years

Exaflops computers (10^{18}) are expected in 2019

Zettaflops computers (10^{21}) are expected in 202?

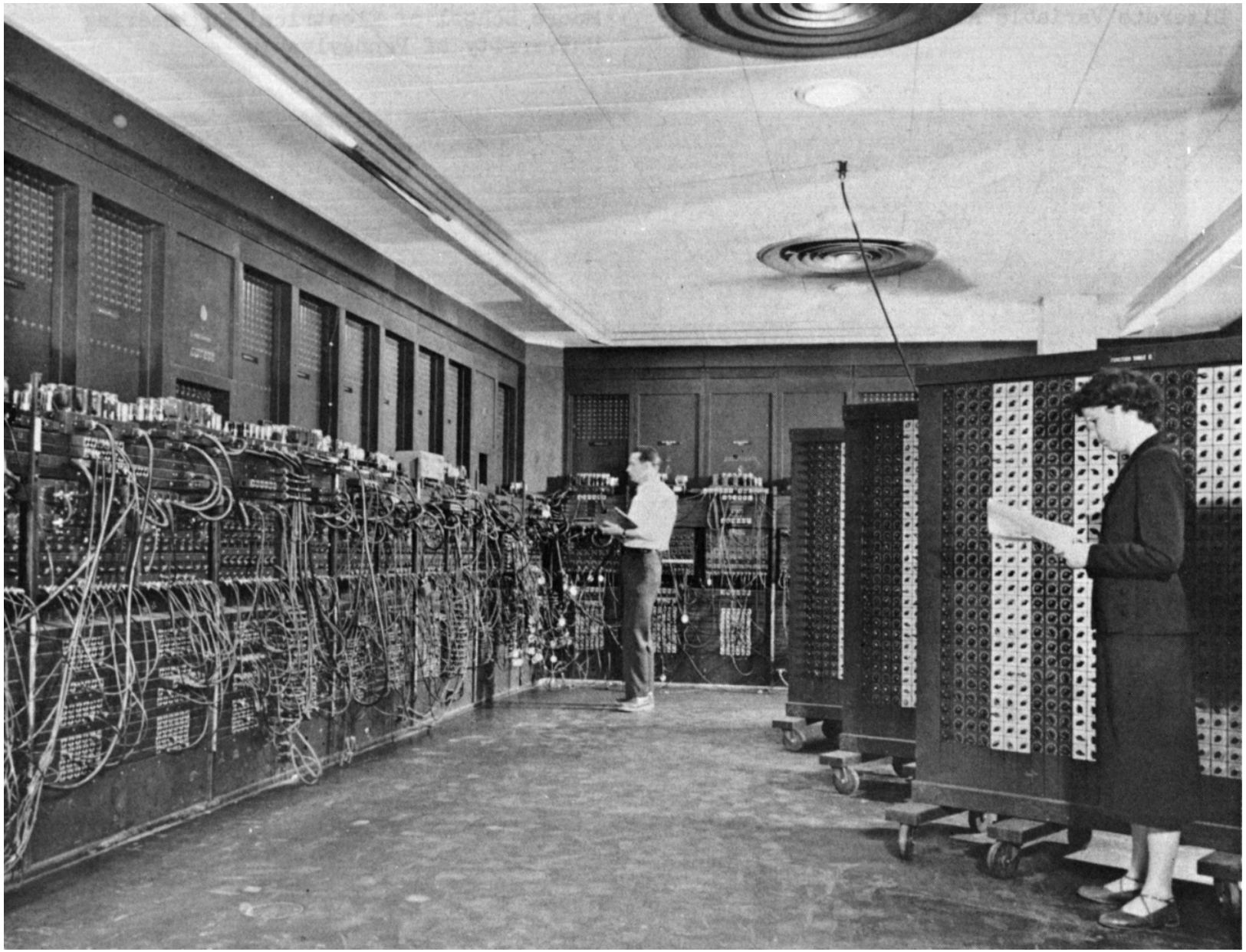
K COMPUTER



K-COMPUTER

TITAN-COMPUTER

ENIAC-COMPUTER



NEXT GOALS in SUPERCOMPUTING

- Axaflop computers (10^{18}) is the next goal that is seen as realistic.
- At this time we have to consider the feasibility of picocomputing (using picotechnology, measured in trillions (10^{-12}) of a meter, and femtocomputing (using femtotechnology measured in (10^{-15}) of a meter, as speculative.
- Supercomputer to be installed in 2015 in Ostrava should have power of 2650 laptops.

COMMUNICATION TECHNOLOGY

- No communication technology has ever disappeared, but instead becomes increasingly less important as the technological horizon widens.

  Arthur C. Clarke

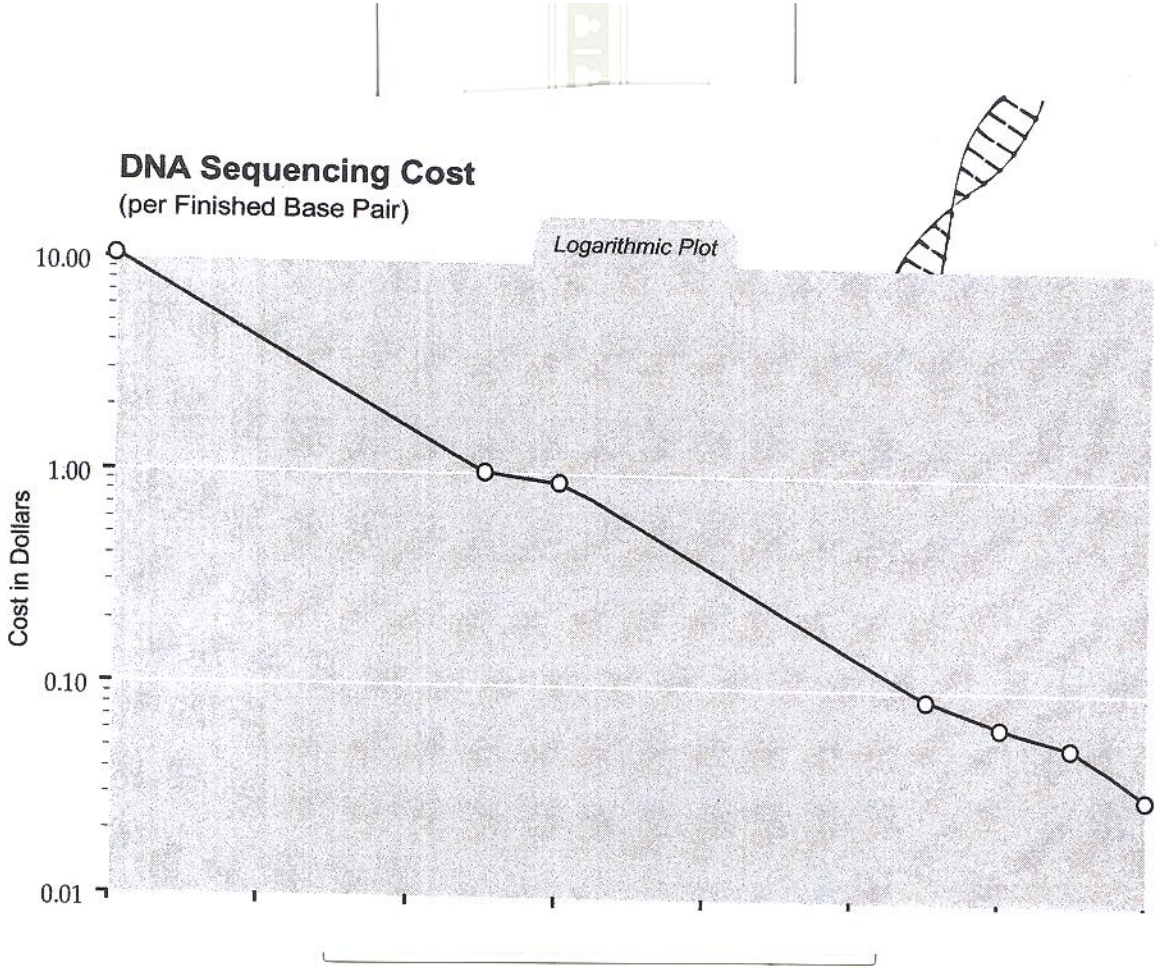
- Exponential growth in communication technology has for many years been even more explosive than in processing and memory measures of computation and is no less significant in its implications.

OTHER EXAMPLES of the LAW of ACCELERATING RETURNS

The law of accelerating returns applies to all technologies.
Some important examples follow.

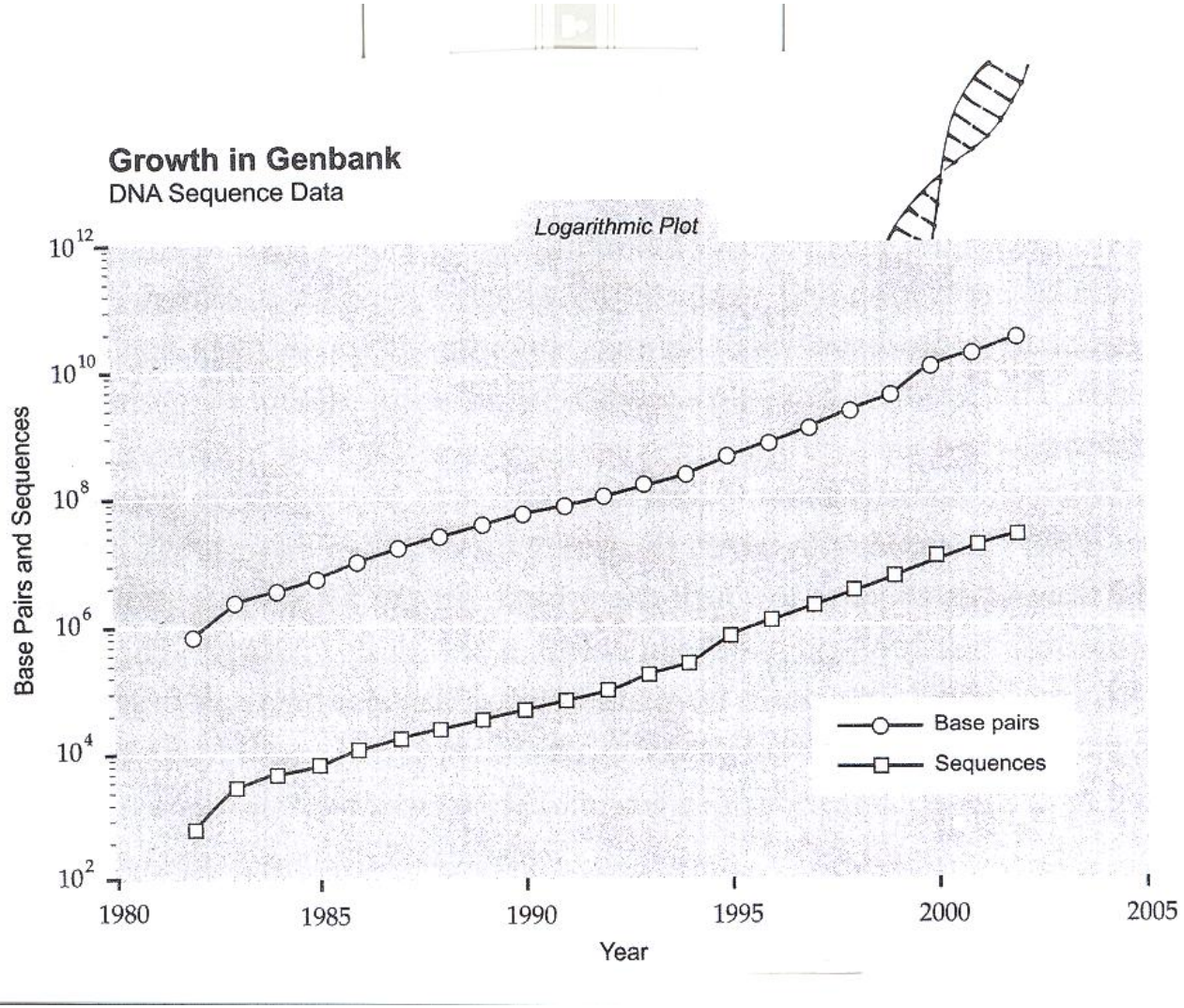
COST of DNA SEQUENCING

When the human genome scan project was launched in 1990, critics expected it will take 1000 years, judging from the scanning speed of that time - finally it took a bit less than 15 years.
The cost of DNA sequencing came down from about 10 $ per base pair in 1990 to a couple of pennies in 2004 and is rapidly falling down.



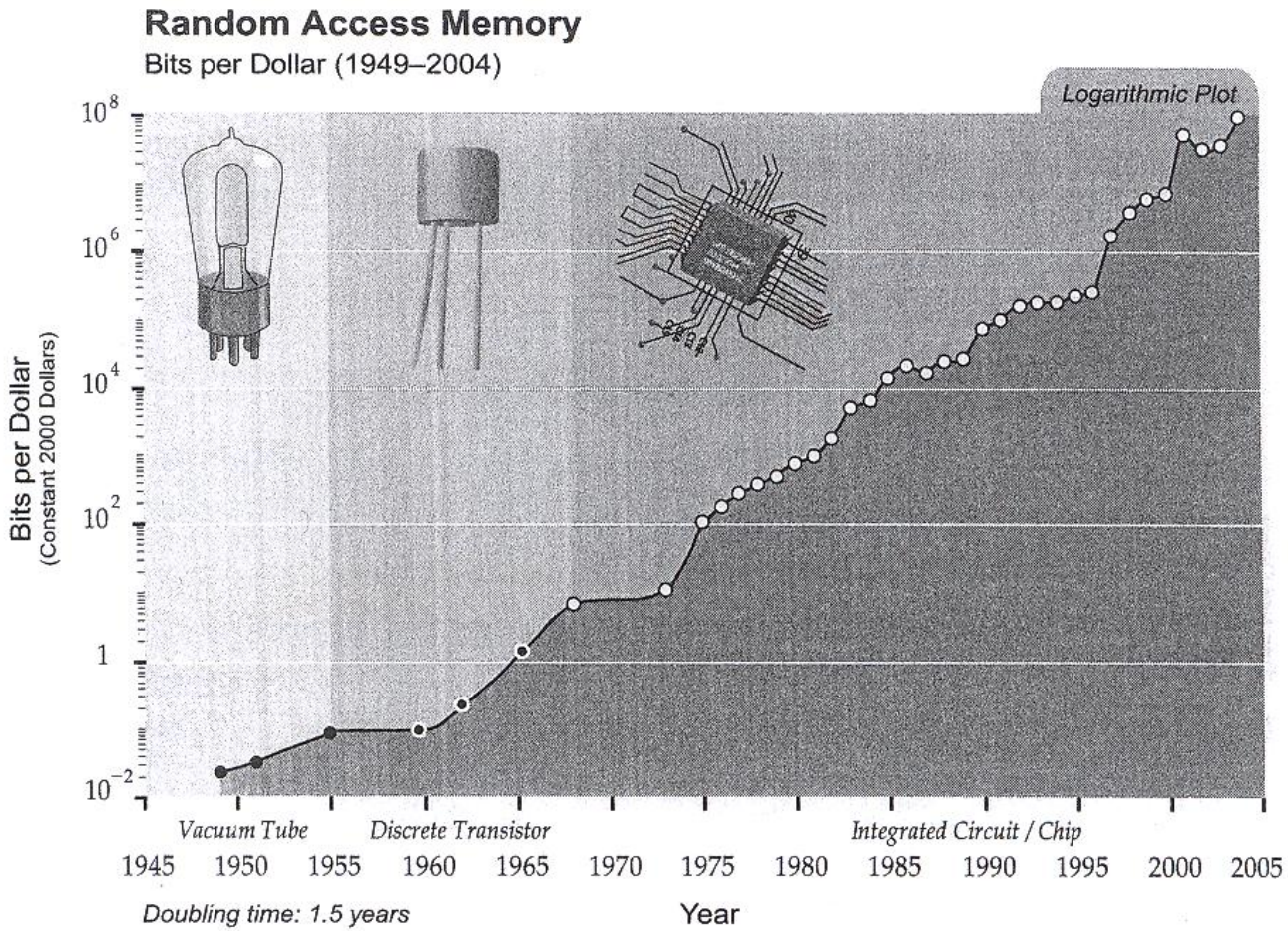
GROWTH in the AMOUNT of DNA SEQUENCE DATA

Exponential growth in in the amount of DNA sequence data is presented in figure bellow. Sequencing of HIV virus took more than 15 years. For SARS virus only 31 days.



RAM

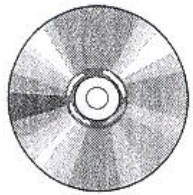
The following picture shows how exponential growth in RAM proceeds smoothly through different technology paradigms.

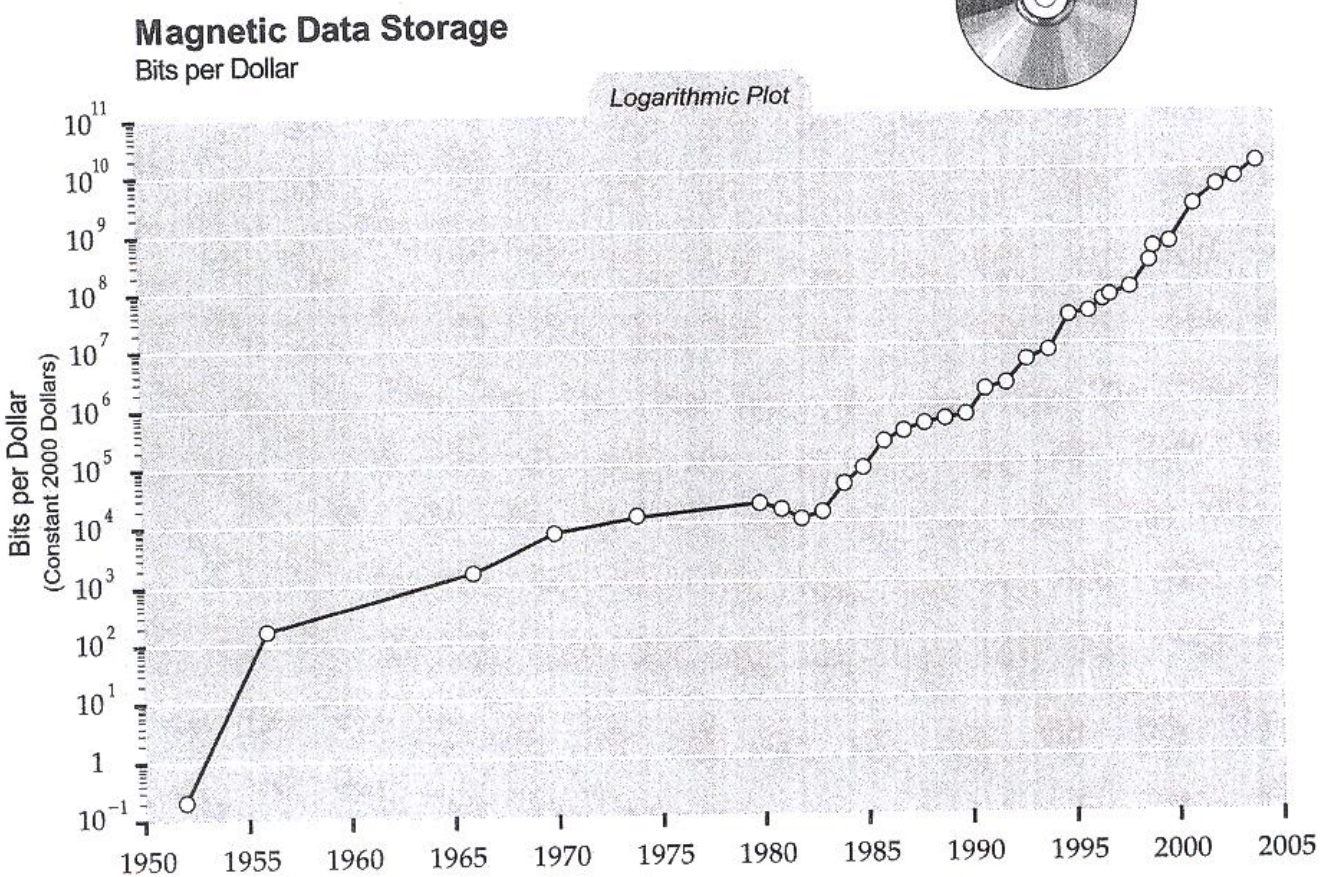


Exponential growth in RAM capacity across paradigm shifts.

MAGNETIC DATA STORAGE

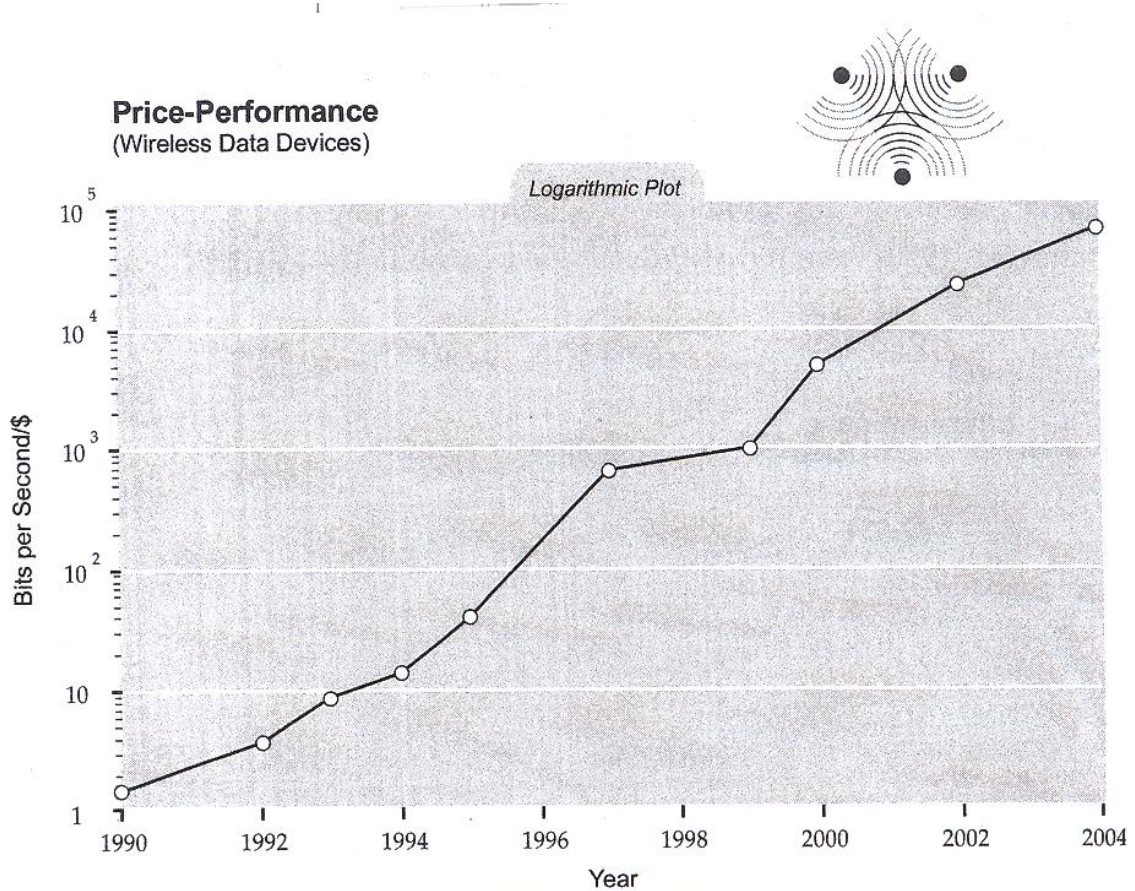
The growth in the price performance of magnetic memory is not a result of Moore's law.This exponential trend of the squeezing of data onto a magnetic substrate, rather than transistors onto an integrated circuit, is a completely different technical challenge pursued by different companies.





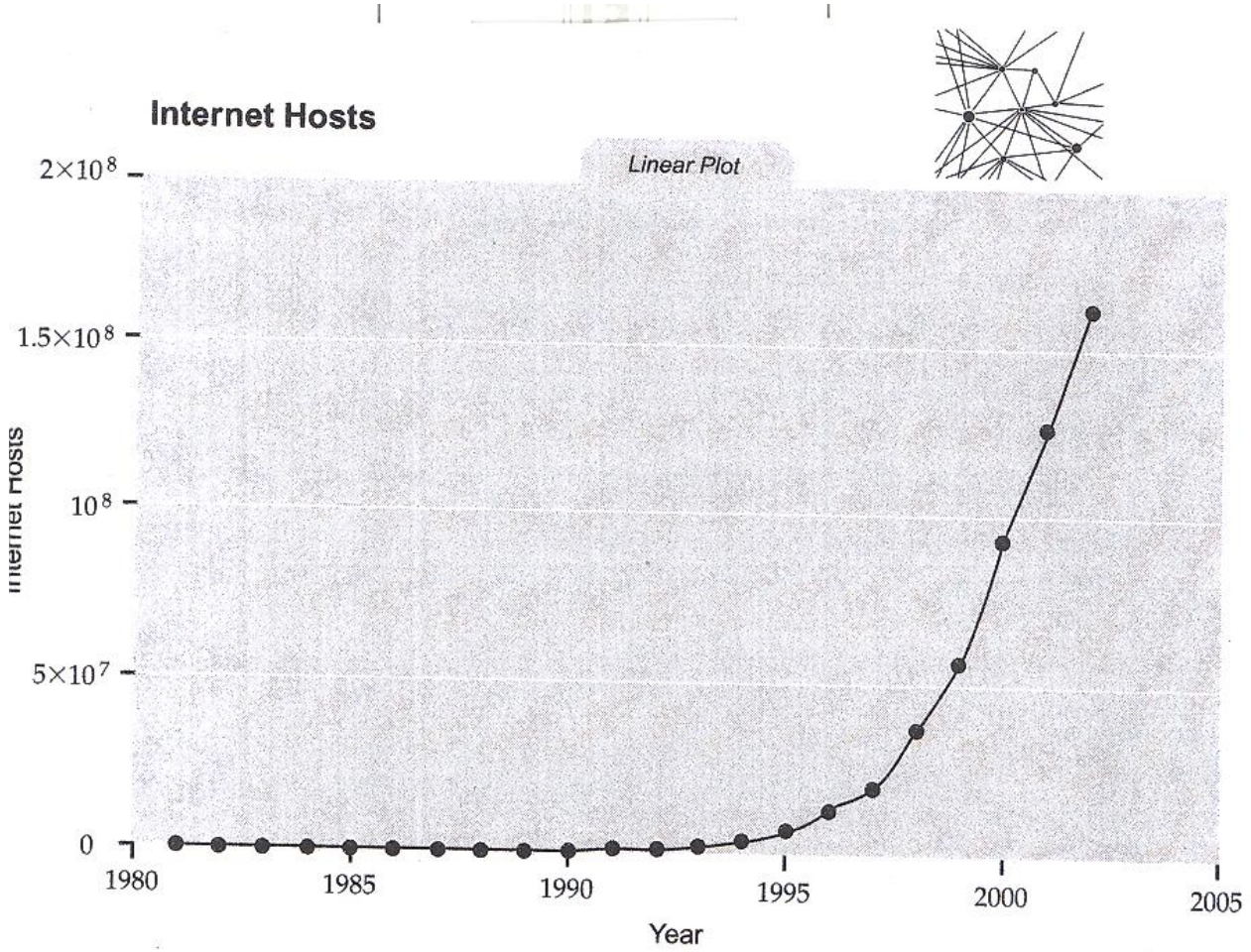
PRICE-PERFORMANCE of WIRELESS DATA DEVICES

Exponential grows concerning communication devices has actually been for many years even more impressive as that of computation devices. First example deals with wireless communication.



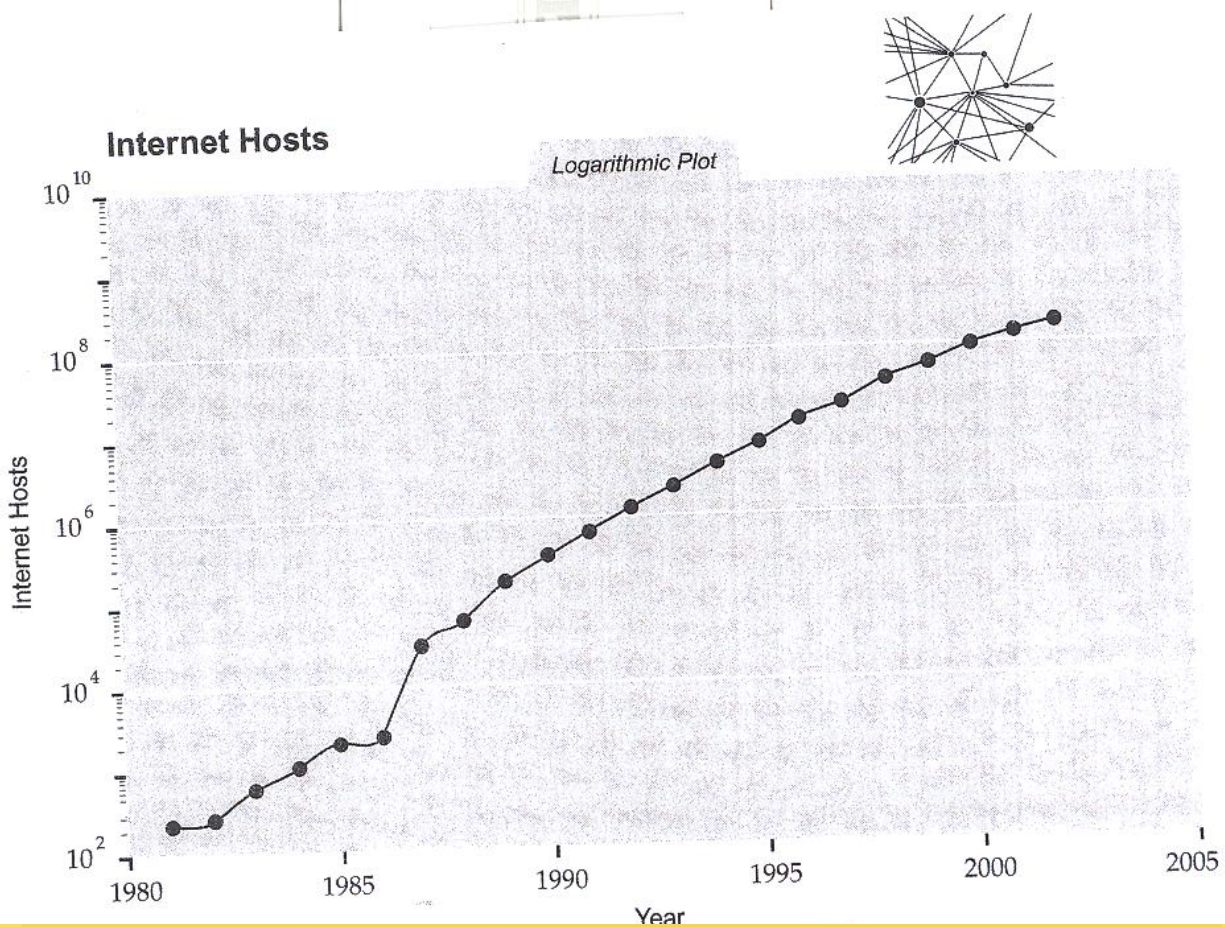
INTERNET HOSTS GROWTH - linear plot

The explosion of the Internet hosts after the mid-1990, when emails and WWW strated to explode, looks as a surprise once linear plot is used.



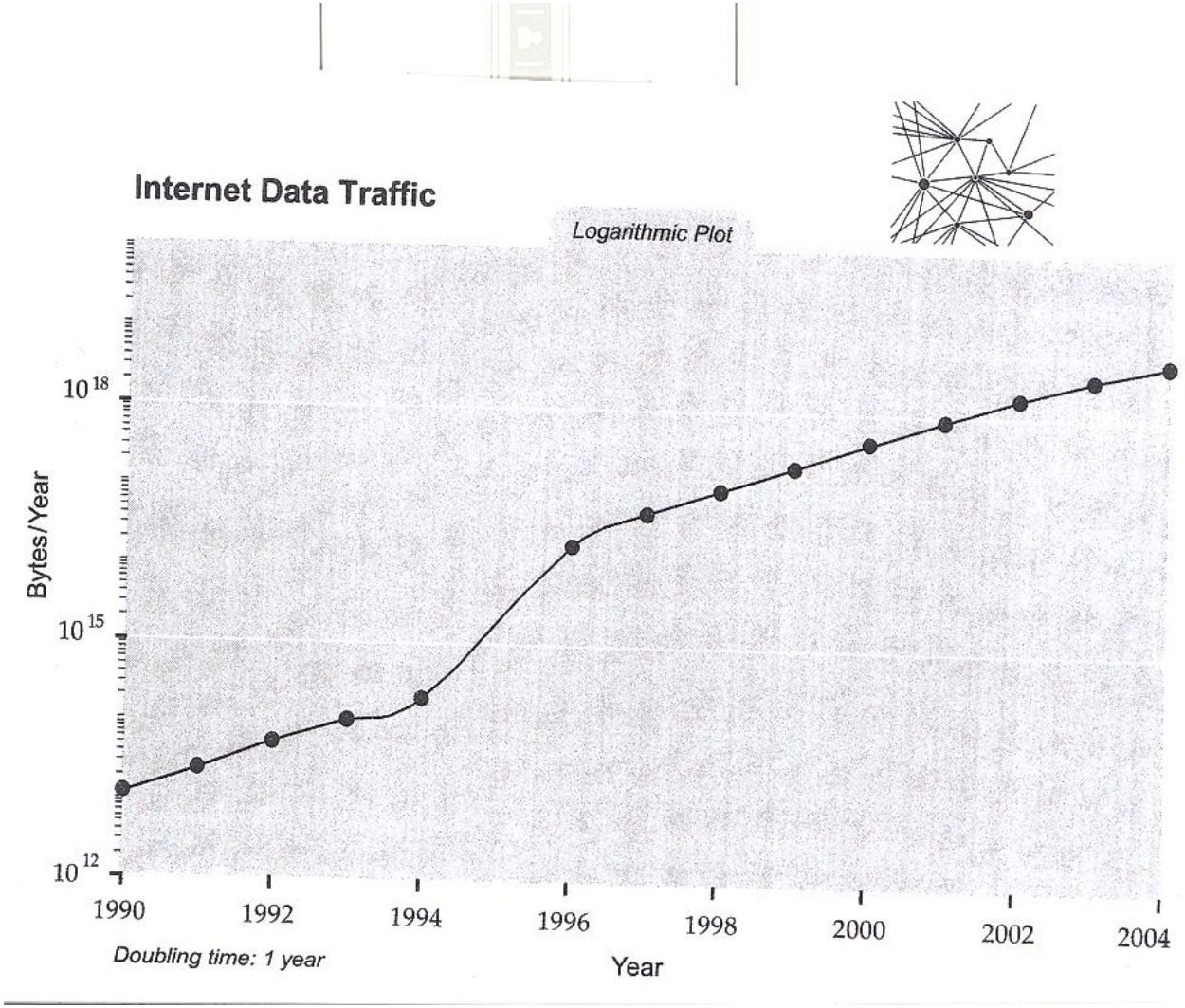
INTERNET HOSTS GROWTH - logarithmic plot

The explosion of the Internet hosts after the mid-1990, when emails and WWW strated to explode, stops to look as a surprise once logarithmic plot is used.



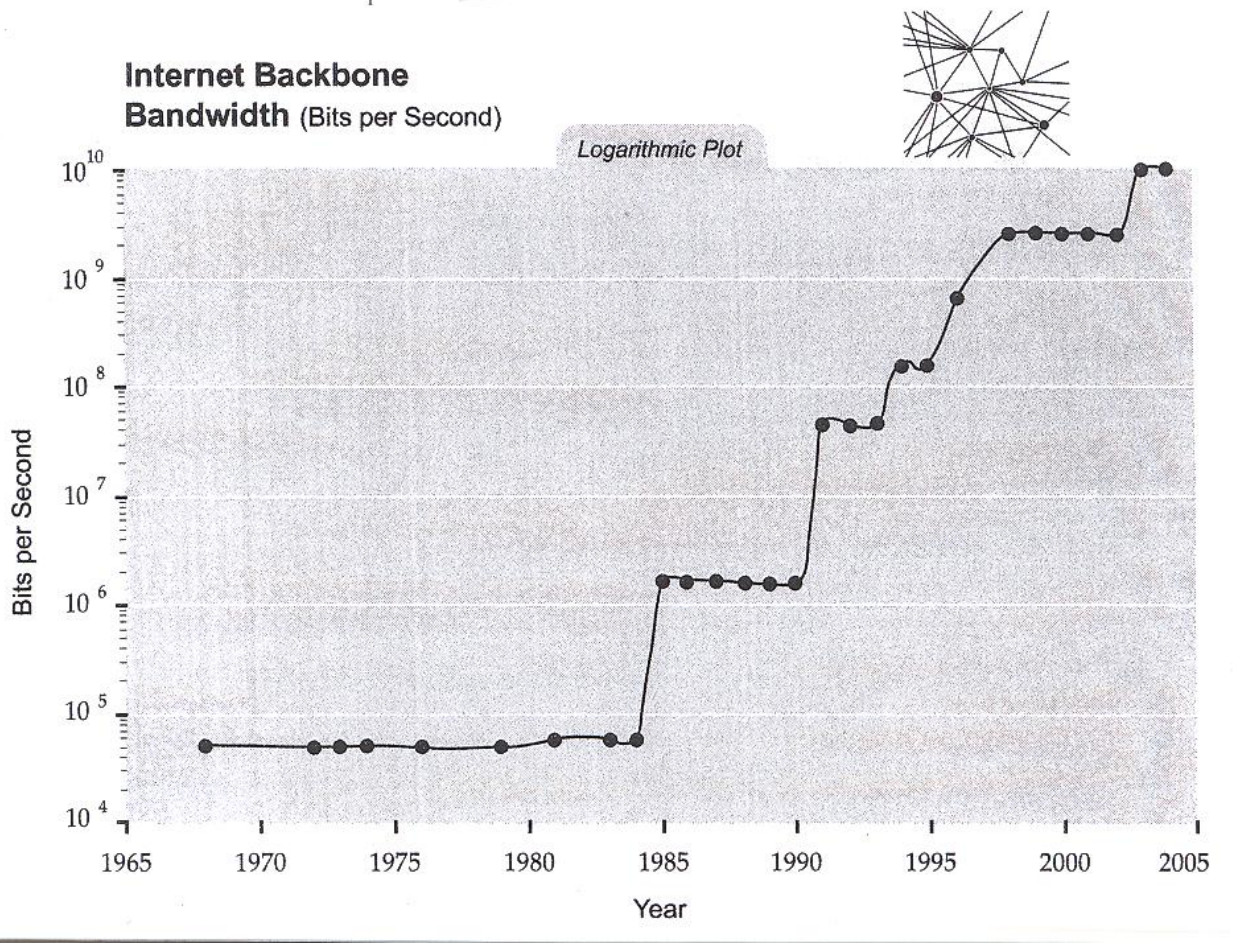
INTERNET DATA TRAFFIC

Data traffic on Internet also doubled every year.



INTERNET BANDWIDTH - BITS for SECOND

To accommodate exponential growth of data traffic on Internet the data transmission speed had also to grow exponentially.
The following figure shows development as a progression of S-curves.



IMPLICATIONS of S-CURVES for PARADIGMS APPLICATIONS

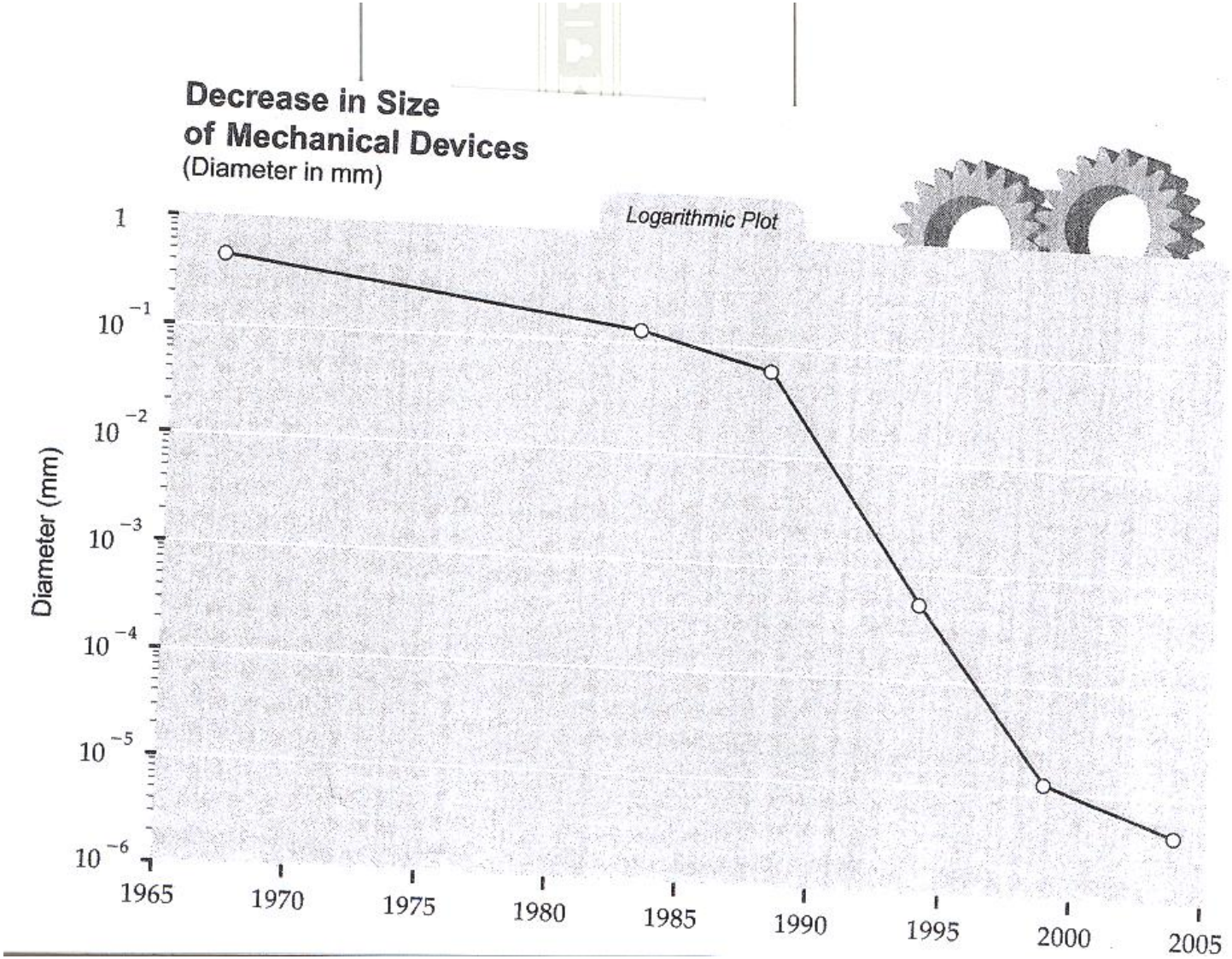
Technology cycle for a paradigm shift - as examples see railroads, AI, Internet, telecommunications,... - typically starts with a period of unrealistic expectations based on small understanding of all enabling factors required.

Although utilization of a new paradigm does increase exponentially, early growth is usually slow until the knee of the exponential curve is realized.

While the general widespread expectations for revolutionary changes are correct, they are usually incorrectly timed and therefore if they do not come early enough a period of disillusionment comes

MINIATURIZATION

Profound impact for future will have also the fact that size is decreasing also in exponential rate for a broad range of mechanical and electronic devices.



BIOLOGY versus TECHNOLOGY

- Biology has inherent limitations.
- Every living organism must be built from proteins that are folded from one-dimensional strings of amino acids. Protein-based mechanisms are lacking in strength and speed.
- We expect to be able to re-engineered all of the organs and systems in our biological bodies and brains to be much more capable.
- Machines are expected to be able to improve their own designs and augment their capabilities without limit.
- Using nanotechnology-based designs, their capabilities are expected to be far greater than that of biological brains - without increasing the size or memory consumption.
- Tomorrow's molecular circuits should be based on devises such as nanotubes - tiny cylinders of carbon atoms that measure about 10 atoms across and are five hundred times smaller than today's silicon-based transistors. They should be able to operate at teraherz speed (trillion of operations per second)

IMPACTS of the TECHNOLOGY DEVELOPMENTS LAW - BASIC EXPECTATIONS II

Impacts of the Moore law and, in general, of the law of accelerating return can be summarized as follows:

- As a first consequence, development of almost all areas of society will speed up so fast that what would happen in the next 1000 (500) years at the current rate od development will actually happen within next 100 (40) years. It is therefore beyond our full understanding how life will look in 30-40 years.However,...
- **Current informatics students are expected to retire at the age 80 ± 10 years, or more, and therefore you can expect that during your life time you can expect what you can hardly imagine.**

MORE SPECIFIC EXPECTATIONS

- It is expected that basic computational resources (10^{19} cps and 10^{18} bits) to simulate the human brain will be available for one thousand dollars in the early 2030s.
- It is expected that around 2050 one will be able to buy for 1000 $ a computer whose information processing power will be greater than all unaided human brains.
- It is expected that, due to the development in nanotechnology and 3D molecular computing, around 2040-50 we can have nanobots - robots of the size of blood cells (7-8 microns or even smaller) that will be able, for example, travel through our body and brain (and to do useful work).
- **This will allow to put before science, technology and medicine many new meta-goals.** For example
  - To fight death definitely or at least to prolong very significantly human (productive) age.
  - To produce non-biological intelligence that will be many (trillion) times faster and more productive in many tasks than biological intelligence.
  - To scan human consciousness into computers so we can live inside them, forever, at least virtually? (It is expected that many people that live today will wind up being functionally immortal.)

ARE RADICALLY MORE POWERFUL COMPUTERS in VISION?

Enormous progress in the potential information processing systems we expected so far was fully in accordance with the laws of classical physics as they are known today?

It is therefore natural to formulate and explore the following problems:

- How much can increase power of computers when we stat to use phenomena of other potential physical worlds?
- In particular, how much more powerful can be computers that make use of quantum phenomena?
- More generally, how powerful can be computers based on the laws of some other physical worlds, especially those that we cannot prove so far as impossible?
- In particular can we beat Church-Turing thesis and barrier that has been seen as major limitation factors of information processing power.?

Quantum information processing and transmission

CLASSICAL versus QUANTUM COMPUTING

The essence of the difference
between
classical computers and **quantum computers**

is in the way information is stored and processed.

In **classical computers**, information is represented on **macroscopic level** by **bits**, which can take one of the two values

0 or 1

In **quantum computers**, information is represented on **microscopic level** using **qubits**, which can take on any from uncountable many values

$$\alpha|0\rangle + \beta|1\rangle$$

where α, β are arbitrary complex numbers such that

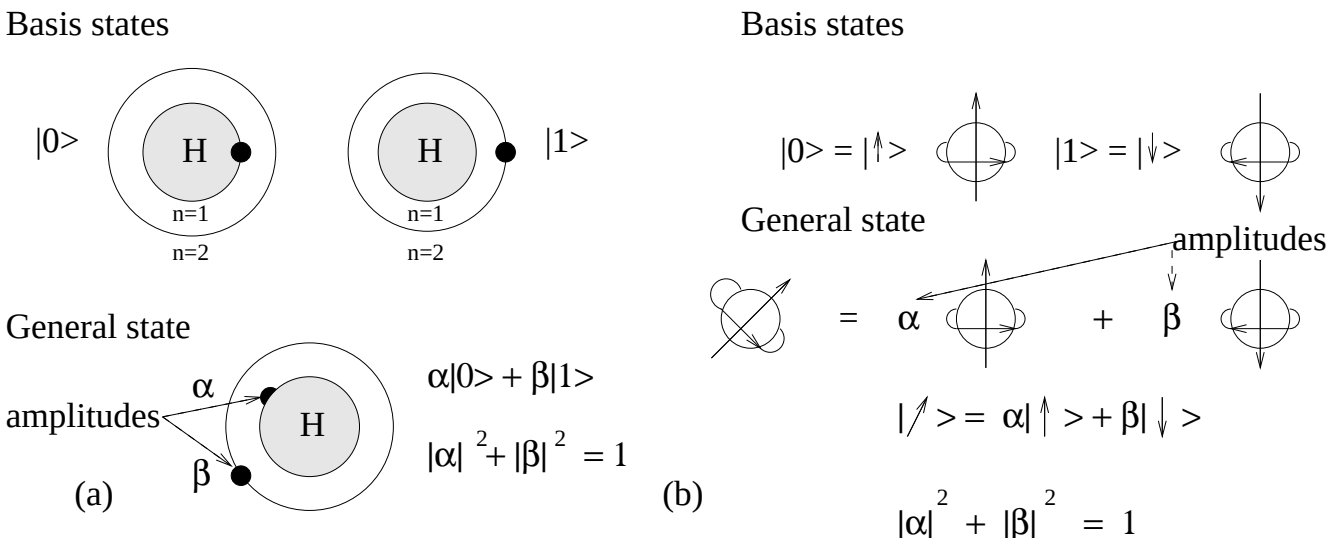
$$|\alpha|^2 + |\beta|^2 = 1.$$

A qubit can be seen as a state in 2-dimensional Hilbert space.

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom

(b) a spin-$\frac{1}{2}$ particle



QUANTUM REGISTERS

For any integer n a quantum system consisting of n qubits forms so called n-qubit quantum register and its states will be states in

$$2^n \text{ - dimensional Hilbert space}$$

For any function $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ it is possible to design, using $O(n)$ of physical resources, a quantum state that "contains" all 2^n values of the function f - a manifestation of so called quantum massive parallelism.

It would seem therefore that using a quantum computer one could compute exponentially faster, using quantum resources, than on classical computers.

HISTORY of QUANTUM COMPUTING - I.

1970 Landauer demonstrated importance of reversibility for minimal energy computation;

1973 Bennett showed the existence of universal reversible Turing machines;

1981 Toffoli-Fredkin designed a universal reversible gate for Boolean logic;

1982 Benioff showed that quantum processes are at least as powerful as Turing machines;

1982 Feynman demonstrated that quantum physics cannot be simulated effectively on classical computers;

1984 Quantum cryptographic protocol BB84 was published, by Bennett and Brassard, for absolutely secure generation of shared secret random classical keys.

1985 Deutsch showed the existence of a universal quantum Turing machine.

1989 First cryptographic experiment for transmission of photons, for distance 32.5cm was performed by Bennett, Brassard and Smolin.

1993 Bernstein-Vazirani-Yao showed the existence of an efficient universal quantum Turing machine;

HISTORY of QUANTUM COMPUTING - II.

1993 Quantum teleportation was discovered, by Bennett et al.

1994 Shor discovered a polynomial time quantum algorithm for factorization;

Cryptographic experiments were performed for the distance of 10km (using fibers).

1994 Quantum cryptography went through an experimental stage;

1995 DiVincenzo designed a universal gate with two inputs and outputs;

1995 Cirac and Zoller demonstrated a chance to build quantum computers using existing technologies.

1995 Shor showed the existence of quantum error-correcting codes.

1996 The existence of quantum fault-tolerant computation was shown by Shor.

CLASSICAL versus QUANTUM TELEPORTATION

The so called **No-teleportation theorem** says that **classical teleportation is impossible**.

This means that there is **no way** to use

classical channels

to transmit faithfully

quantum information.

In contrast to the classical no-teleportation theorem, quantum teleportation is possible.

HOW POWERFUL WOULD BE QUANTUM COMPUTERS

- Known quantum algorithms for some problems are exponentially faster than all known classical algorithms - for example for integer factorization.
- It can be proven for some communication problems that quantum communication can be exponentially more efficient.
- There are problems, for example teleportation, that cannot be done using classical resources but can be done using quantum resources.
- In quantum teleportation one party can teleport an unknown quantum state of its particle to the particle of another party, if they share one special quantum state, without knowing what is being teleported and where another party is located, provided two parties involved can have classical (say email) communication.
- Using quantum tools one can generate classical shared randomness in unconditionally secure way.

COUNTERINTUITIVNESS in QUANTUM WORLD

Quantum physics is full of unexpected or even mysterious and/or counterintuitive phenomena.

For example:

- Unknown quantum information cannot be copied.
- Counterfactual phenomena are possible

COUNTERFACTUAL PHENOMENA

The term **counterfactual** is usually used for things that might have happened, although they did not really happened.

While classical counterfactuals do not have physical consequences, quantum counterfactuals can have surprisingly big consequences because the mere possibility that some quantum event might have happened can change the probabilities of obtaining various experimental outcomes.

A CONSEQUENCE

It can be shown that a quantum computer can provide the result of a computation without performing the computation

provided it would provide the same result of computation

by really performing the computation

Mitchinson and Jozsa, 1999.

HOW DIFFICULT is TO DESIGN a QUANTUM COMPUTER?

Theoretically not so much because it is enough to implement multiplication of quantum states using the following matrices:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4} i} \end{pmatrix}$$

Practically, very difficult -it is even not clear whether it is possible to build very powerful quantum computer.
Two main reasons for that are:

- Destructive impact of environment, so called decoherence, that are almost impossible fully to eliminate.
- Computation has to produce states that exhibits quantum non-locality - a phenomenon that is beyond our understanding.

The world is a dangerous place,

particularly,

if you are a qubit.

UNSCRAMBLING of OMELET

Today we are beginning to realize how much of all physical science is really only *information, organized in a particular way*.

But we are far from unraveling the knotty question: *To what extent does this information reside in us, and to what extent is it a property of nature?*

Our present quantum mechanics formalism is a peculiar mixture describing in part laws of Nature, in part incomplete human information about Nature – all scrambled up together by Bohr into an omelet that nobody has seen how to unscramble,

Yet we think the unscrambling is a prerequisite for any further advances in basic physical theory. .. Edwin T. Jaynes, 1990

APPENDIX I

THE LAW of ACCELERATING RETURNS and ECONOMIC RELATIONS

- It is the economic imperative of a competitive marketplace that is the primary force driving technology forward and fueling the law of the accelerating returns - this is equivalent to survival needs in biological evolution.
- In turn the law of accelerating returns is transforming economical relationships.
- We are moving towards more intelligent and smaller machines as the result of myriad small advances, each with its own particular economic justification. Machines that can better carry out their missions have increased value.

EXPONENTIAL GROWTH and PERIODIC RECESSIONS

- Underlying exponential growth in economy is far more powerful force than periodic recessions.
- Recessions, including depressions, represent only temporary deviations from the underlying exponential curve.
- Finally, economy ends up exactly where it would have been had the recession/depression never occurred.