"Year 2020"-Topics in Information The ory for Further Studies


## Comprestimation



## Comprestimation

- rosy compression of "non-natural" images (regular lossy compression uses MS E)
- compression of images so that the statistical inferences on the compressed images remain valid
- Egg. compression of microarray images


## Microarray images



Comprestimation cont.

- also Known as "Multi-terminal data compression"
- T. Han \& S.Amari; R. Iörnsten \&B. $\mathscr{A} u$;


Three Concepts: Information '02


## Algorithmic Information The ory



## Algorithmic Information The ory

- ..as used by Chaitin for "me tamathematics"
- incomple teness theorems
$\checkmark$ Gödel(logic)
$\checkmark$ Turing (algorithm)
$\checkmark$ The Halting Probability Omega (information, randomness)
http://www.umcs.maine.edu/~chaitin/


## Pfysics, information and games



## e system has ha automatic parameter whirb increasus the advantage from; " $15-30 \%$ " to $20.40 \%$.

Tan earchng for an urvestor to financially back a tour of casnos usng thus computer. Tur project has my filest attenton and has taken some 5 yerrs to comp nuncine into thousiads of dolars of investement Thave theceforse foond it necessary to adverkes. A financial and personal cormontroent to thais project is therfore required. The intensl progrem uses some 4000 insucticas, 8000 equaticas and over 100 sub-roucines in order to predect accurately the outcome of roulette sod has been tested against a reguation size roulette wheel over many thousand of spins. This computer can be put aganct any roulette whiel with marg variable intial condtions. I beliere this to be the mest poaverfija and adeptable device of it's kind
All legalites have been irvestigated and the use of such a device as still legal in most countries
Applicanss should hase a sola backeround of informsticu reger ding the tsble Lageut of numbert, abiky to leam bacic copcept send applicstion together with an understanding of the fiture potertial of this concept, and a wilingress to progress in this drectico will be requred The rewards involved have a greater meaning than just foones. You should also be of stable and fresidy persanality. Travel is unvolued sed so time is of importance. If you are betting weth scared mones please do not reply.
The advactage stated of $15-30 \%$ is of a broical nature. Therefore it is probable that some fluctuations uall occax before the pastive rewards can be fillp realised Any
e] |l|| itemet

## 2020: Quantum Odyssey

"On Quantum Computing and information transmission"


## Motivation

- Computers as physical systems
- Technological issues
$\checkmark$ miniaturization and speedup - Moore's Law $\checkmark$ need for energy efficiency


Fig. 1.1 The number of atoms needed to represent one bit of information as a functon of calendar year. As the vertical axis is on a logarithmic scale, the straight line fit suggests the trend is exponential. Extrapolation of the trend suggests that the one-atom-per-bit level is reached in about the year 2020. Adapted from [Keyes88].

Why would we bother?

- Cryptography: QC can breakRSA codes
- Communication of messages that betray the presence of eavesdropping
- Teleportation: moving quits around without having them ever being transmitted over an insecure channel


## Centralconcepts

- Superposition: $a$ " $b$ lend" of 0 and 1 simultane ously, i.e., quantum parallel mode
- Reversible computing: logical irreversibility implies thermodynamic irreversibility (i.e., heat dissipation)



Charles Bennett

## The Capabilities of Computers

(Deterministic)
Turing Machine


## Probabilistic <br> Turing Machine

## Quantum <br> Turing Machine



Fig. 2.2 In a probabilistic classical Turing machine there are multiple possible successor states, only one of which is actually selected. Unselected paths are terminated $(x)$. The probabilities of transitioning between various states are shown. Notice that the sum of the probabilities on all the paths emanating from a state is 1 .

Proving vs . providing proof

- $Q \mathcal{T M}$ can simulate a $\mathcal{T M}-Q \mathcal{T M}$ universal
- TM provides a proof as the sequence of steps performed
- QTM can provide an answer without a proof trace (worse: if you try to "peek"
$Q \mathcal{T M}$ that would disrupt the proof!)


## Bits and Qubits

- Each bit is represented by the state of a simple 2-state quantum system e.g., spin state)
- We need finite dimensional Hilbert space
"Complex linear vector space"


## BraCKet

- For a simple two-state system you can write the state as a "Ket (vector)"

$$
|\psi\rangle=\omega_{0}\left|\psi_{0}\right\rangle+\omega_{1}\left|\psi_{1}\right\rangle \equiv\binom{\omega_{0}}{\omega_{1}}
$$

- Probability interpretation

$$
P\left(\text { system in state }\left|\psi_{i}\right\rangle\right)=\frac{\left|\omega_{i}\right|^{2}}{\left.\sum_{i=0}^{n-1} \omega_{i}\right|^{2}}
$$



## Unitary operators

- 2-state system has 2 eigenstates called $\mid \psi_{0}>$ and $\mid \psi_{1}>$ (6asis)

$$
\begin{aligned}
& |0\rangle=\binom{1}{0}|1\rangle=\binom{0}{1} \\
& |\psi\rangle=\omega_{0}\binom{1}{0}+\omega_{1}\binom{0}{1}=\binom{\omega_{0}}{\omega_{1}}
\end{aligned}
$$

## Unitary operators continued

- To change the quantum world one needs an operator, egg. NOT

$$
\text { NOT }|0\rangle=\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right)\binom{1}{0}=\binom{0}{1}=|1\rangle, \quad \text { NOT is reversible! }
$$

$$
\operatorname{NOT}|1\rangle=\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right)\binom{0}{1}=\binom{1}{0}=|0\rangle
$$

- One can also fave non-classicalgates such as $\sqrt{\mathrm{NOT}}$


## Unive rsality

- In classic al computation $\mathfrak{A N} \mathcal{D}$ and $\mathfrak{N O}(\mathcal{T}$ are enough to build any circuit
- In quantum computing it is enough to use a 2-qubit gate (Barenco et al)

$$
\hat{A}(\phi, \alpha, \theta)=\left(\begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & e^{i \alpha} \cos (\theta) & -i e^{i(\alpha-\theta)} \sin (\theta) \\
0 & 0 & -i e^{i(\alpha+\theta)} \sin (\theta) & e^{i \alpha} \cos (\theta)
\end{array}\right)
$$

## Fundamentals

- One can have quantum interference whenever there is more than one way of obtaining a particular result
- measuring a quantum system:
$\checkmark$ if the system is in eigenstate the outcome is one of the eigenvalues
$\checkmark$ if the system is in superposition state the result is given by

$$
P\left(\text { system in state }\left|\psi_{i}\right\rangle\right)=\frac{\left|\omega_{i}\right|^{2}}{\left.\sum_{i=0}^{n-1} \omega_{i}\right|^{2}}
$$

## "A good quantum calculation"

- Create a superposition of register elements
- Calculate in "one shot" all function values $\mathcal{F}(j)$
- Do something clever with all the $\mathcal{F}(j)$ values
(Use interference to increase the amplitudes and thus probabilities of the solution states)

Quantum entanglement (EPR)

- If two systems (particles) are "Quantum correlated" one talks about entanglement
- For entangled particles their joint state is not factorizable as the direct product of two simpler states
- Produced by conservation of some attribute


## Teleportation


-dissociation
-information transmission
-reconstitution

## Well, at le ast a qubit ...

Bob takes the result of Alice's measurement and performs a rotation of his EPR particle to
Classical message from Alice to Bob describing the result of her measurement on particles 1 and 2 .

Alice performs a joint measurement on the state of particles 1 and 2 which destroys the state of particle 1 .

Alice wishes to teleport)

$$
|\phi\rangle=a\left|\uparrow_{1}\right\rangle+b\left|\downarrow_{1}\right\rangle
$$

EPR entangled state (particles 2 and $\frac{1}{\sqrt{2}}\left(\left|\uparrow_{2}\right\rangle \otimes\left|\downarrow_{3}\right\rangle-\left|\downarrow_{2}\right\rangle \otimes\left|\uparrow_{3}\right\rangle\right)$

Fig. 9.5 Schematic view of quantum teleportation using EPR.

