Title: Introduction to Quantum Information

Date: Dec 03, 2007 10:45 AM

URL: http://pirsa.org/07120016

Abstract:

The last conference we held…

Quantum Information & Quantum Computation

Robin Blume-Kohout
Perimeter Institute

Quantum Information & Quantum Computation

Robin Blume-Kohout
Perimeter Institute

Part I: Foundations

Information

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

Information

a physical system

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

Information

another system → "Something"; a physical system → "something else"

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

Information

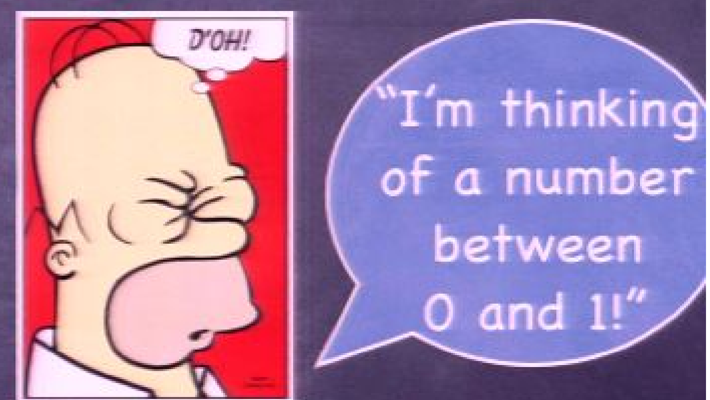
another system → "Something"; predictive power → "something"; a physical system → "something else"

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

Information

another system — predictive power — a physical system

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"



Information

another system → "Something"

predictive power → "something"

a physical system → "something else"

- "Something that tells you something about something else"

- "Information is physical" (Landauer)

- "A resource to reduce uncertainty"

- "Correlation"

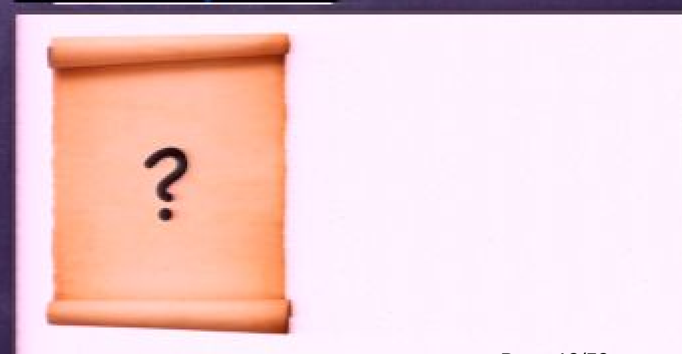
"I'm thinking of a number between 0 and 1!"

Information

another system → predictive power → a physical system

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

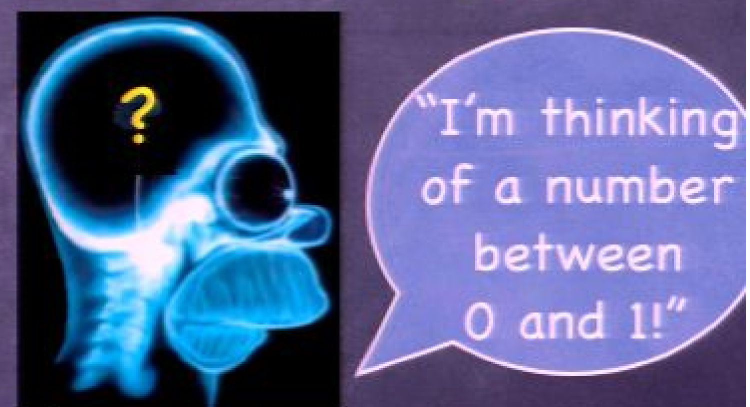
"I'm thinking of a number between 0 and 1!"



Information

another system — predictive power — a physical system

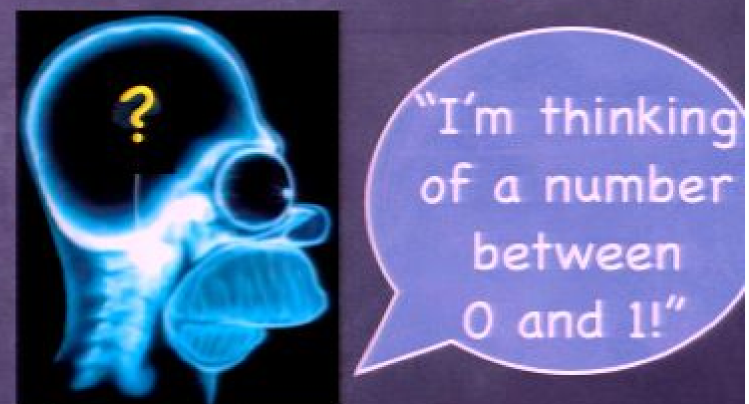
- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

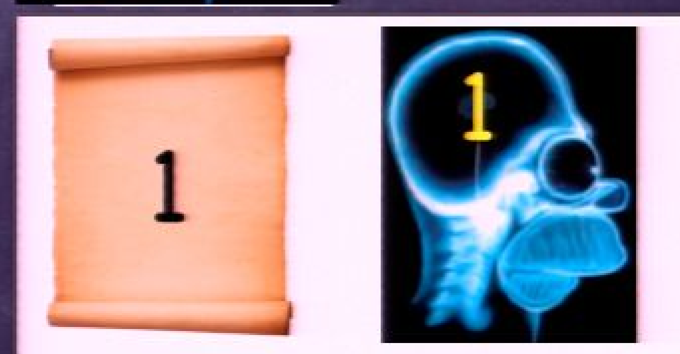


Information

another system → "Something" · predictive power → "something" · a physical system → "something else"

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"





	"0"	"1"
"0"	$\frac{1}{2}$	0
"1"	0	$\frac{1}{2}$

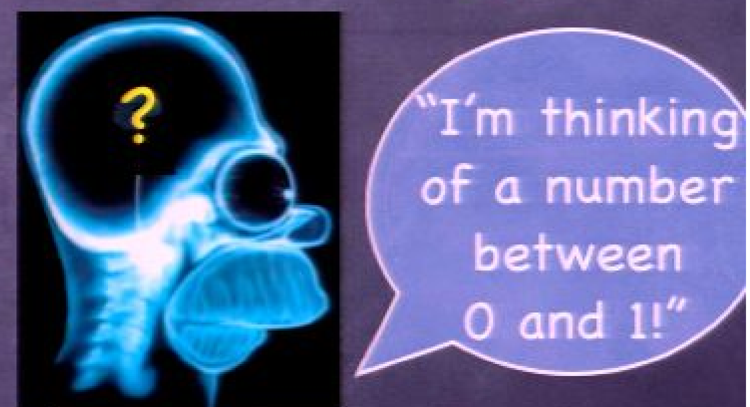
Information

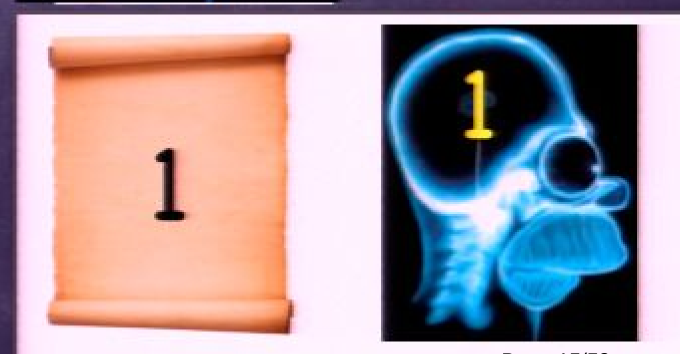
another system → "Something"; predictive power → "something"; a physical system → "something else"

- "Something that tells you something about something else"
- "Information is physical" (Landauer)
- "A resource to reduce uncertainty"
- "Correlation"

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

P_{paper} \ P_{brain}	"0"	"1"
"0"	$\frac{1}{2}$	0
"1"	0	$\frac{1}{2}$





Classical Information

- Information about classical systems
  = correlation between classical systems (A & B).
  $\Rrightarrow$ probability distributions.... $p\left(\vec{x}_A, \vec{x}_B\right)$

- Kinematics: the possible states of classical systems
  Dynamics: possible maps on classical systems

- Focus: "What correlations can be achieved?"
  ...between different subsystems (spacelike).
  ...between input & output of processes (timelike).

What do we care about?

It's all about **transforming** information (correlations)!

- Information in a large system into information in a small system: **compression**
- My information into your information: **communication**
- Alice's information into Bob's information but **not** Eve's information too! **cryptography**
- No transformation: **error correction**
- One representation (e.g. "{a, b}") into a different representation (e.g. "a+b"): **computation**

Quantum Information (I)

- Information about quantum systems
  = correlations between quantum systems.
  $\Rightarrow$ joint quantum states... $|\psi_{A,B}\rangle$

- Kinematics: possible states of quantum systems
  - Finite-dimensional Hilbert spaces: $|\psi_A\rangle = \sum_{i=1}^{D} c_i |i\rangle$
  - Combination = tensor product: $|\psi_A\rangle \otimes |\psi_B\rangle = \sum_{i,j} c_i d_j |i,j\rangle$
  - Correlation = non-"product states": $|\psi_{A,B}\rangle = \sum_{i,j} \alpha_{ij} |i,j\rangle$
  - Uncertainty = mixed states: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
  - State of a subsystem: $\rho_A = \mathrm{Tr}_B [\rho_{A,B}] = \mathrm{Tr}_B [|\psi_{A,B}\rangle\langle\psi_{A,B}|]$

Quantum Information (II)

- **Dynamics:** possible maps on quantum systems
  - Unitary dynamics: $|\psi(t)\rangle = U\,|\psi_0\rangle\,;\quad \rho(t) = U\rho_0 U^\dagger$
  - Extension: $|\psi(t)\rangle = |\psi_0\rangle\,|0\rangle\,;\quad \rho(t) = \rho_0 \otimes |0\rangle\langle 0|$
  - Isometry: $|\psi(t)\rangle = U\,(|\psi_0\rangle\,|0\rangle)\,;\quad \rho(t) = U\,(\rho_0 \otimes |0\rangle\langle 0|)\,U^\dagger$
  - Reduction: $\rho_A(t) = \mathrm{Tr}_B\left[\rho_{AB}(0)\right]$
  - Most general: $\rho(t) = \mathrm{Tr}_\varepsilon\left[U\,(\rho_0 \otimes |0\rangle\langle 0|)\,U^\dagger\right]$
    (Completely Positive Trace-Preserving linear map)

$$\rho = \begin{pmatrix} p_1 & & & \\ & p_2 & & \\ & & \ddots & \\ & & & p_D \end{pmatrix}$$

- **Entropy:** $H(\rho) \equiv -\mathrm{Tr}\left[\rho\,\log\rho\right] = \sum_i p_i \log\left(\frac{1}{p_i}\right)$ ⟷

$H(\rho_A \otimes \rho_B) = H(\rho_A) + H(\rho_B)$

$H(\rho_A) = 0 \Longleftrightarrow \rho_{AB} = |\psi_A\rangle\langle\psi_A| \otimes \rho_B$

Two kinds of questions

QUESTION: Given certain resources...

- ...what kind of correlations can be established between two **quantum** systems?

OR

- ...what kind of correlations can be established between two **classical** systems?
  ... using quantum intermediaries!

  - 1st may be more fundamental
  - 2nd is more useful (**we** are classical!)

Bits: a basic tool

- "Bit" = classical system with 2 states
- Two bits have 4 states... N bits have 2^N states
- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...
    - ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

Bits: a basic tool

- "Bit" = classical system with 2 states

- Two bits have 4 states... N bits have 2^N states
- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...
    - ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

Bits: a basic tool

- "Bit" = classical system with 2 states

- Two bits have 4 states... N bits have 2^N states

- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...
    - ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

Bits: a basic tool

- "Bit" = classical system with 2 states

- Two bits have 4 states... N bits have 2^N states

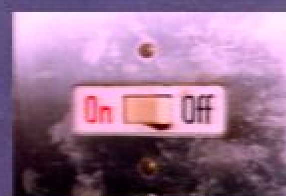
- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...
    - ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

Bits: a basic tool

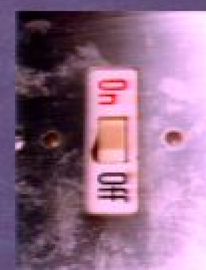
- "Bit" = classical system with 2 states

- Two bits have 4 states... N bits have 2^N states

=



x



- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...

$\leq$

- ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

Bits: a basic tool

- "Bit" = classical system with 2 states

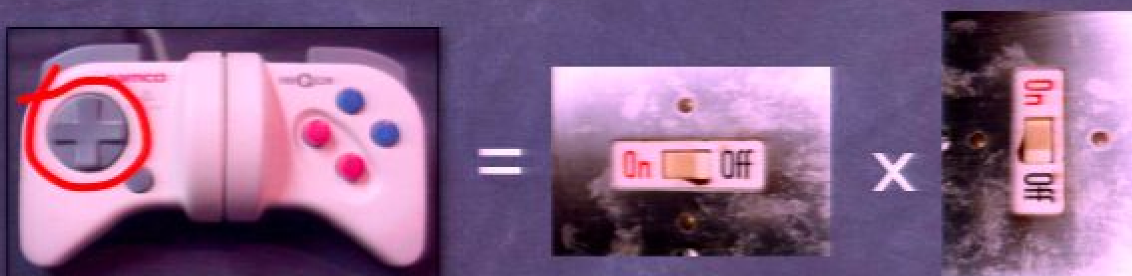
- Two bits have 4 states... N bits have 2^N states

- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...
    - ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

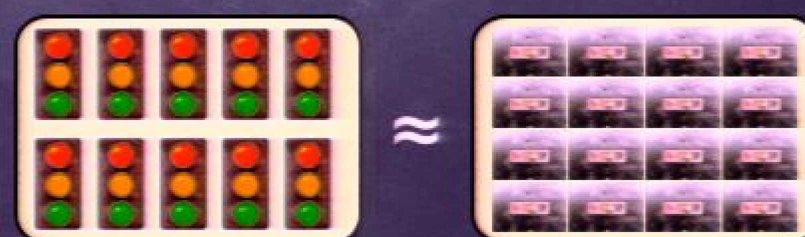
Bits: a basic tool

- "Bit" = classical system with 2 states

- Two bits have 4 states... N bits have 2^N states



- One "trit" fits in 2 bits...
  - ...10 trits fit in 16 bits...



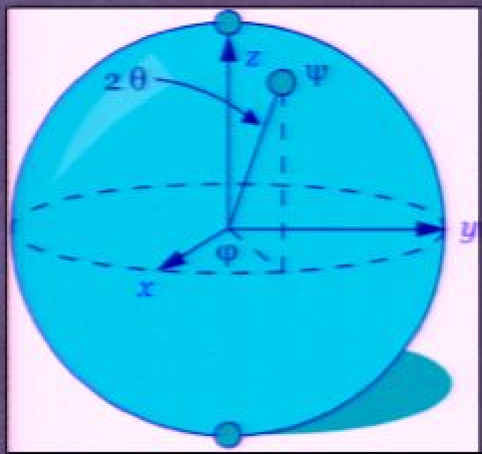
  - ...asymptotically, 1 trit = $\log_2(3) \approx 1.58$ bits

Qubits (you knew this was coming...)

- Qubit: quantum system w/ 2 distinguishable states: $\{|0\rangle, |1\rangle\}$
  - photon ($\{|H\rangle, |V\rangle\}$)
  - spin-1/2 fermion ($\{|\uparrow\rangle, |\downarrow\rangle\}$)
  - 2-state atom ($\{|g\rangle, |e\rangle\}$)
- Superpositions => 2-dimensional Hilbert space
- As w/bits, any system fits in N qubits (for some N)
- Pauli operators:

Qubits (you knew this was coming...)

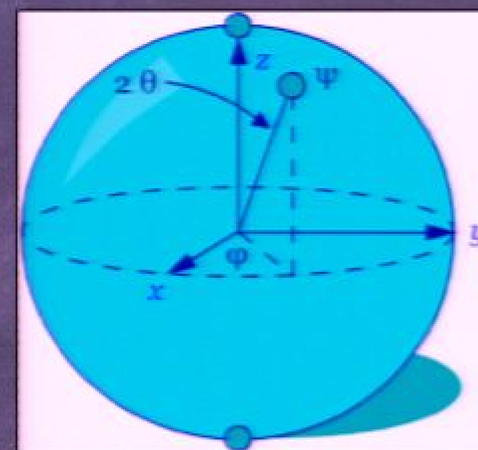
- Qubit: quantum system w/ 2 distinguishable states: $\{|0\rangle, |1\rangle\}$
  - photon ($\{|H\rangle, |V\rangle\}$)
  - spin-1/2 fermion ($\{|\uparrow\rangle, |\downarrow\rangle\}$)
  - 2-state atom ($\{|g\rangle, |e\rangle\}$)



- Superpositions => 2-dimensional Hilbert space
- As w/bits, any system fits in N qubits (for some N)
- Pauli operators:

Qubits (you knew this was coming...)

- **Qubit**: quantum system w/ 2 distinguishable states: $\{|0\rangle, |1\rangle\}$
  - photon ($\{|H\rangle, |V\rangle\}$)
  - spin-1/2 fermion ($\{|\uparrow\rangle, |\downarrow\rangle\}$)
  - 2-state atom ($\{|g\rangle, |e\rangle\}$)



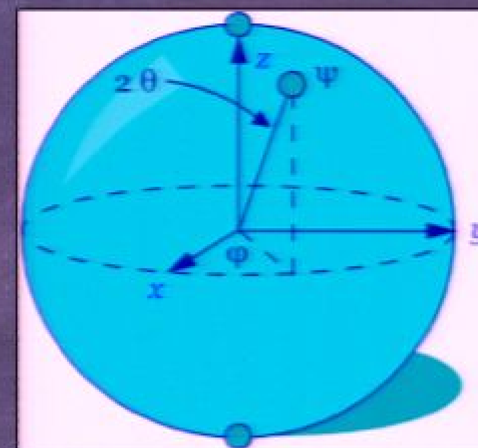
- **Superpositions** => 2-dimensional Hilbert space

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix};\ |1\rangle = \begin{pmatrix}0\\1\end{pmatrix};\ |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix};\ |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix};\ |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix};\ |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$$

- As w/bits, any system fits in N qubits (for some N)
- Pauli operators:

Qubits (you knew this was coming...)

- **Qubit**: quantum system w/ 2 distinguishable states: $\{|0\rangle\,,\,|1\rangle\}$
  - photon ($\{|H\rangle, |V\rangle\}$)
  - spin-1/2 fermion ($\{|\uparrow\rangle, |\downarrow\rangle\}$)
  - 2-state atom ($\{|g\rangle, |e\rangle\}$)



- **Superpositions** => 2-dimensional Hilbert space

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix};\ |1\rangle = \begin{pmatrix}0\\1\end{pmatrix};\ |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix};\ |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix};\ |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix};\ |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$$

- As w/bits, any system fits in N qubits (for some N)
- Pauli operators: $\sigma_z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix};\ \sigma_x = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix};\ \sigma_y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}$

Part IIa: Information

Entanglement

- Nonclassical correlation -- e.g. EPR pair:

$$|EPR\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \text{ or } \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

- Pure states: Entangled = not a product state
- Mixed states: Entangled = not separable
  - Separable => $\rho = \sum |\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|$
  - Example: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ vs $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$
- LOCC: "Local Operations & Classical Communication"
  - Entanglement never increases under LOCC.
- Distillable ($\rho^{\otimes N} \rightarrow |EPR\rangle\langle EPR|$) vs. bound entanglement

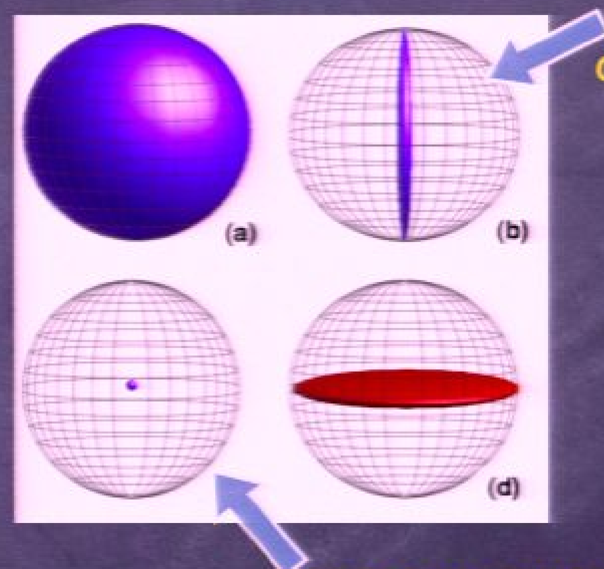
Multiparty Entanglement...

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|W\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}$$

Decoherence & Classicality

- Decoherence: interaction with environment destroys quantumness (coherence).



- Ideally, pointer basis & classical physics emerge.
  (bad for quantum info processing, though!)
- Also destroys classical info.
- Goal #1: characterize decoherence
  - e.g., T_2 = dephasing time; T_1 = depolarization time
- Goal #2: counteract decoherence
  - e.g. error correction, refocusing, noiseless subsystems

Quantum Cryptography

- Cryptography: Transfer information from Alice to Bob… and keep Eve in the dark!
  - "HELLO" => "IFMMP" … insecure
  - 1-time pad … absolutely secure
  - RSA public key … computationally secure
- Quantum crypto:
  - Establish a secret key w/quantum communication.
  - Use measurement disturbance to detect eavesdropping
- BB84: Alice sends each bit as $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$; Bob measures randomly => perfect correlation 1/2 the time.
  - Eavesdropping causes detectable errors.

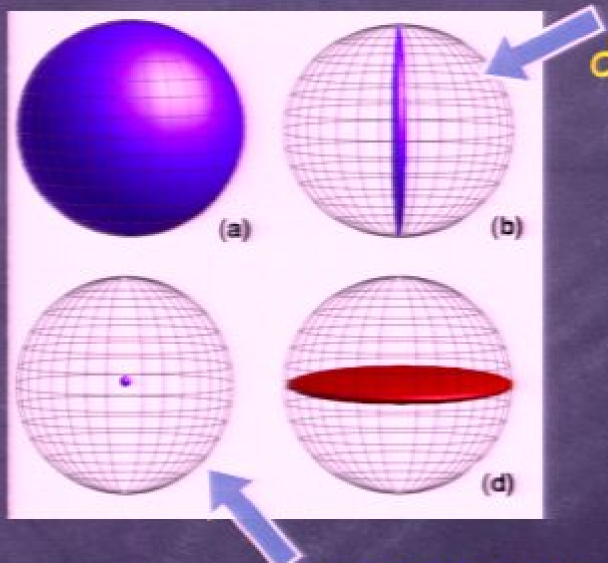
Quantum Cryptography

- Cryptography: Transfer information from Alice to Bob… and keep Eve in the dark!
  - "HELLO" => "IFMMP" … insecure
  - 1-time pad … absolutely secure
  - RSA public key … computationally secure
- Quantum crypto:
  - Establish a secret key w/quantum communication.
  - Use measurement disturbance to detect eavesdropping
- BB84: Alice sends each bit as $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$; Bob measures randomly => perfect correlation 1/2 the time.
  - Eavesdropping causes detectable errors.

QUANTUM COMMUNICATION IS USEFUL!

Decoherence & Classicality

- Decoherence: interaction with environment destroys quantumness (coherence).
- Ideally, pointer basis & classical physics emerge.
  (bad for quantum info processing, though!)
- Also destroys classical info.



- Goal #1: characterize decoherence
  - e.g., T_2 = dephasing time; T_1 = depolarization time
- Goal #2: counteract decoherence
  - e.g. error correction, refocusing, noiseless subsystems

Entanglement

- Nonclassical correlation -- e.g. EPR pair:

$$|EPR\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \text{ or } \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

- Pure states: Entangled = not a product state
- Mixed states: Entangled = not separable
  - Separable => $\rho = \sum |\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|$
  - Example: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ vs $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$
- LOCC: "Local Operations & Classical Communication"
  - Entanglement never increases under LOCC.
- Distillable ($\rho^{\otimes N} \rightarrow |EPR\rangle\langle EPR|$) vs. bound entanglement

Multiparty Entanglement...

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|W\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}$$

Quantum Cryptography

- Cryptography: Transfer information from Alice to Bob... and keep Eve in the dark!
  - "HELLO" => "IFMMP" ... insecure
  - 1-time pad ... absolutely secure
  - RSA public key ... computationally secure
- Quantum crypto:
  - Establish a secret key w/quantum communication.
  - Use measurement disturbance to detect eavesdropping
- BB84: Alice sends each bit as $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$; Bob measures randomly => perfect correlation 1/2 the time.
  - Eavesdropping causes detectable errors.

Quantum Cryptography

- Cryptography: Transfer information from Alice to Bob... and keep Eve in the dark!
  - "HELLO" => "IFMMP" ... insecure
  - 1-time pad ... absolutely secure
  - RSA public key ... computationally secure
- Quantum crypto:
  - Establish a secret key w/quantum communication.
  - Use measurement disturbance to detect eavesdropping
- BB84: Alice sends each bit as $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$; Bob measures randomly => perfect correlation 1/2 the time.
  - Eavesdropping causes detectable errors.

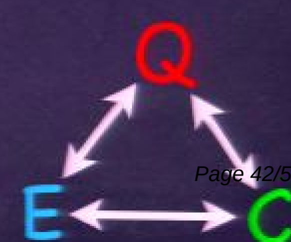
QUANTUM COMMUNICATION IS USEFUL!

Communication Capacity (I)

- How much correlation between Alice & Bob can N uses of a quantum channel create?
  - Classical capacity: how much classical correlation?
  - Quantum capacity: how much entanglement?
- Transmission rate depends on what code is used:
  - Capacity = correlation established by best code.
  - Code states can be entangled over multiple uses
  - Open question: can the classical capacity be reached with non-entangled codes?

Communication Capacity (II)

- Pre-existing entanglement plays an interesting role!
  - Shared EPR pairs (alone) can transmit **no** info.
  - A qubit channel (alone) can only transmit 1 c-bit.
  - A c-bit channel (alone) can transmit **no** qubits.
- Surprising results!
  - 1 EPR + 1 qubit ==> 2 c-bits! (superdense coding)
  - 1 EPR + 1 c-bit ==> 1 qubit! (teleportation)
- Result: Quantum communication as a resource theory.



Part IIb: Computation

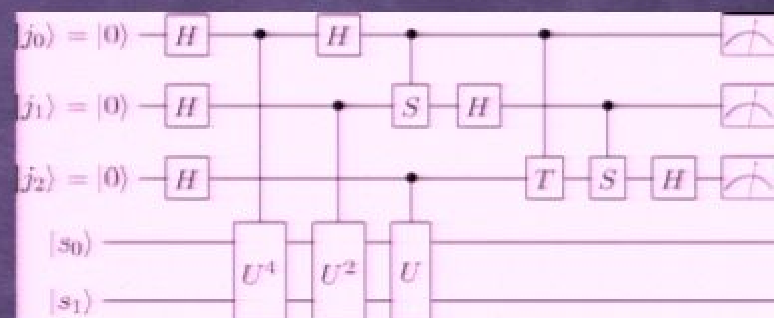
Quantum Computers

- **Computer**: A bunch of bits, on which you can perform 1- and 2-bit **logic gates**, e.g:

NOT:
0→1
1→0

CNOT:
00→00
01→01
10→11
11→10

- **Quantum computer**: A bunch of qubits, on which you can perform 1- and 2-qubit **unitary gates**:



- **Algorithm**: A function from N-bit strings to M-bit strings, implemented by [relatively few] gates:
  - "Multiply X and Y": f: $\{0,1\}^{2N} \rightarrow \{0,1\}^{2N}$
  - "Is X prime?": f: $\{0,1\}^{N} \rightarrow \{0,1\}$

Quantum Algorithms

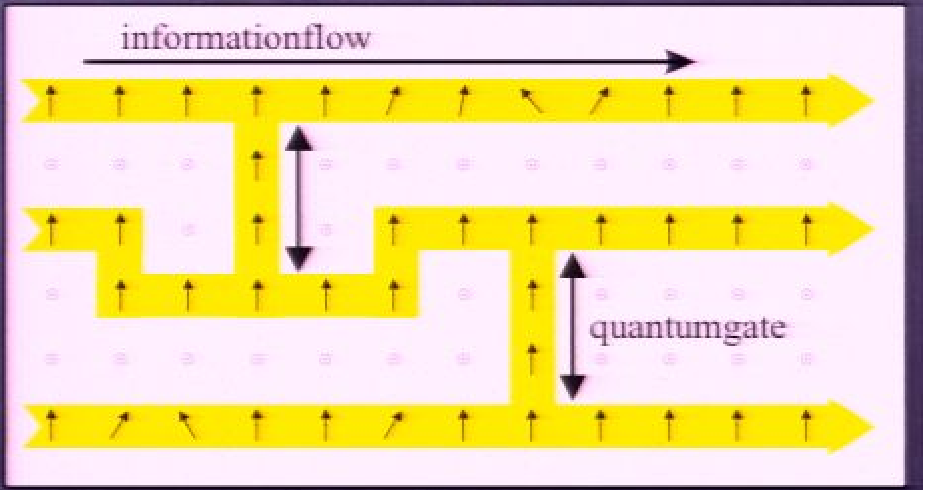
- Shor's Algorithm: given an N-bit number, the product of two large primes, find its factors.
  - Takes $O(N_3)$ time, vs. $O(e^{\sqrt[3]{n}})$ classically
  - Based on the quantum Fourier transform.
- Grover's Algorithm: given N-bit X and a function f(Y), find Y such that f(Y) = X.
  - Requires $O(N^{1/2})$ queries, vs. O(N) classically
- Quantum Simulation: for a given Hamiltonian, predict a measurement on the evolved state.

Error Correction

- **The point:** protect information against noise.
- **Classical:** use redundant coding; check to see if an error happened. "0" -> 000 "1" -> 111
- **Quantum:** observing the code states will collapse them! Seems impossible.
- **Solution:** tailor the code to the expected errors so we can measure the error -- but not the info.
  - N-qubit Hilbert space = {Code} $\otimes$ {Syndrome}
  - The **syndrome** measurement "collapses" a continuous manifold of possible errors to one of a discrete set

Models of Computation

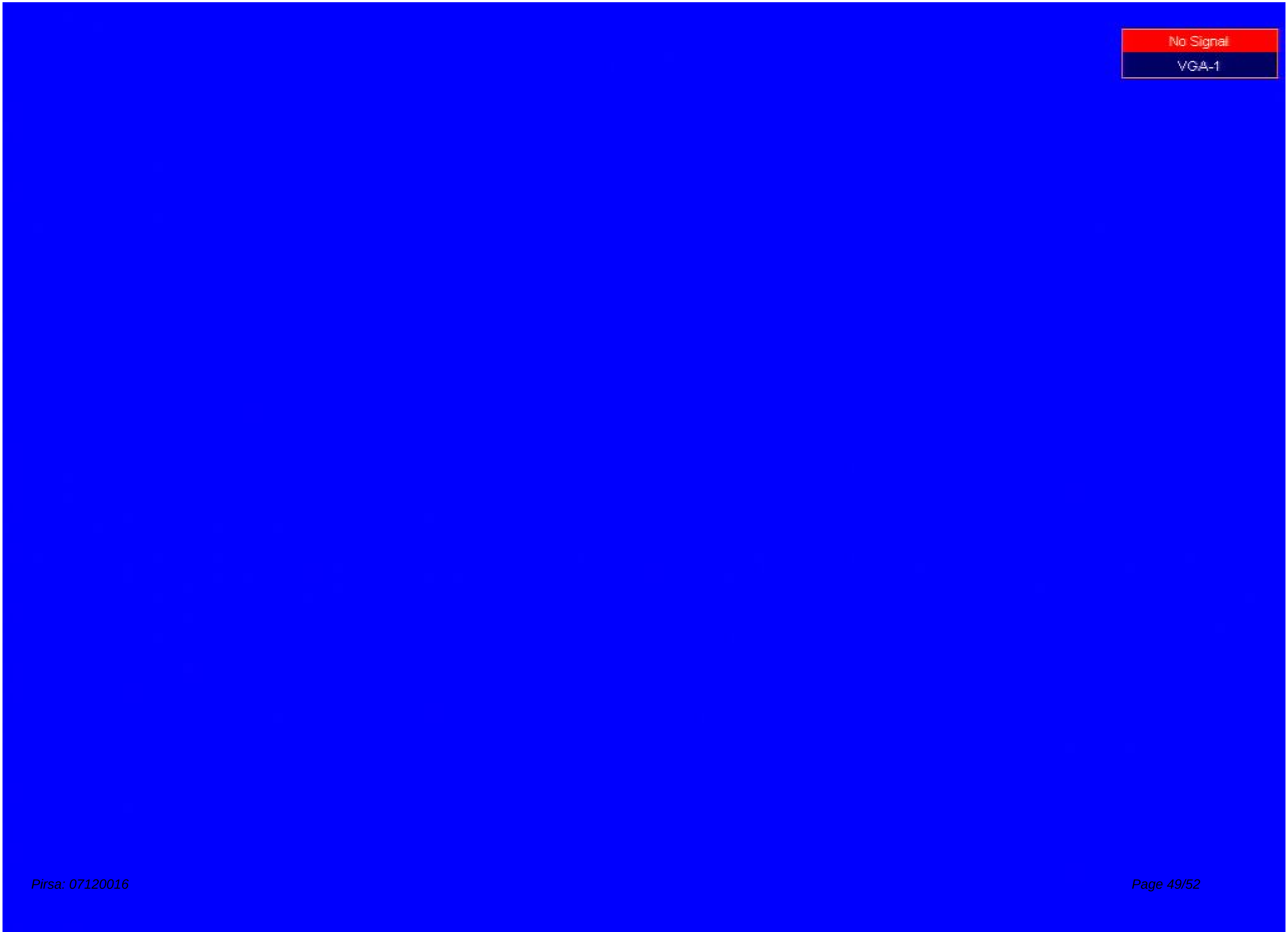
- Where does a quantum computer get its power?
  - Entanglement? Unitary gates? Parallelism?
- Standard (circuit) model is not the only way!
  - Adiabatic Q.C. doesn't use gates.
  - Measurement-based Q.C. has no unitaries at all:



  - A "one clean qubit Q.C." still seems to provide an advantage -- despite negligible entanglement

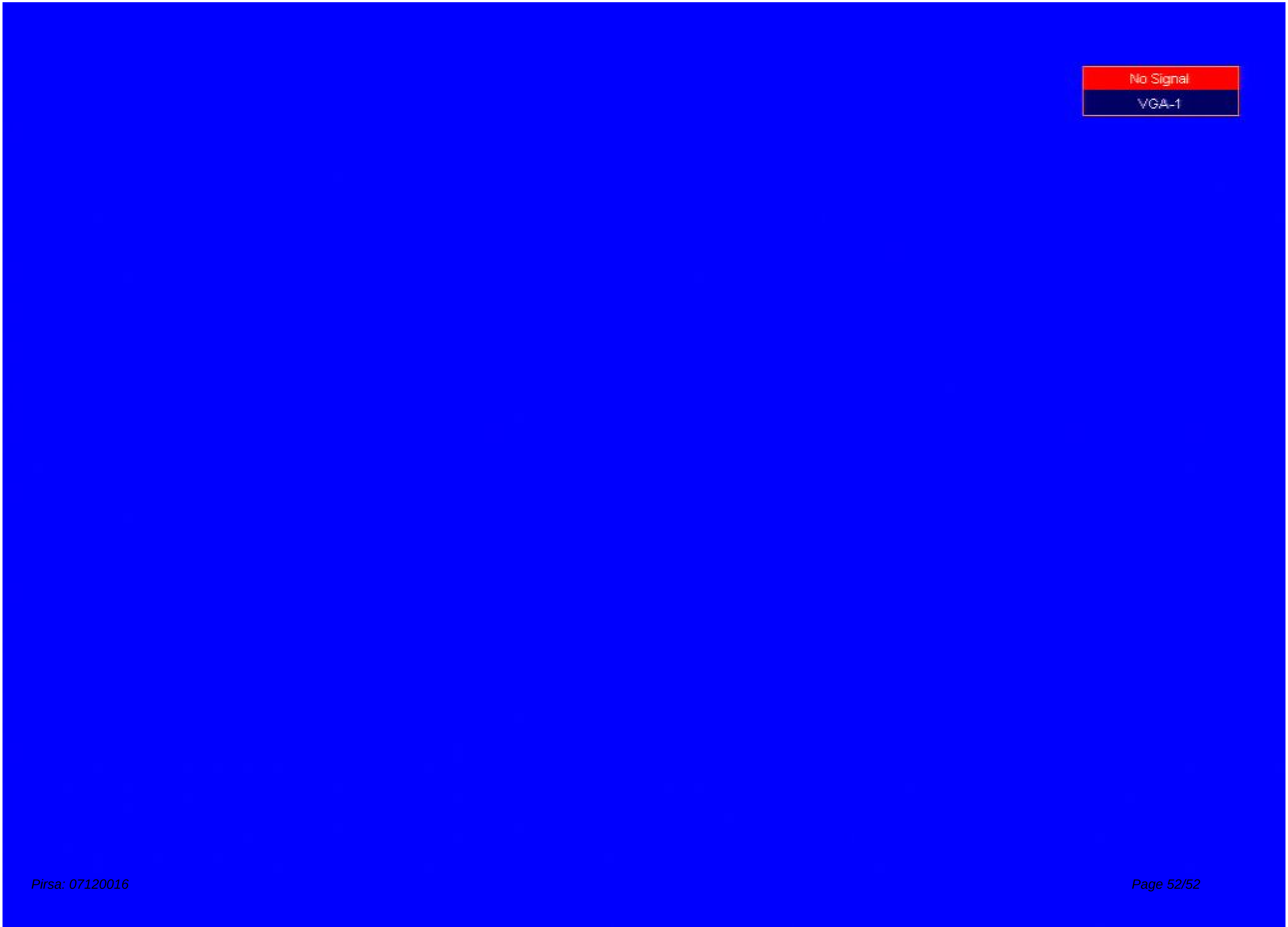
No Signal

VGA-1


No Signal
VGA-1

No Signal
VGA-1

No Signal
VGA-1


No Signal
VGA-1