# 10. Physics from Quantum Information

## I. The Clifton-Bub-Halvorson (CBH) Theorem

Clifton, Bub, Halvorson (2003)

*Motivation*: Can quantum physics be reduced to information-theoretic principles?

*CBH Theorem*: A theory is a quantum theory *if and only if* the following information-theoretic constraints are satisfied:

(i) No superluminal information transmission between systems by measurement on one of them.

(ii) No broadcasting of the information contained in an unknown state.

(iii) No unconditionally secure bit commitment.

*Strategy:*

- *First*: What is a quantum theory? Three essential characteristics.
- *Then*: Show that these characteristics are equivalent to the three information-theoretic constraints.

*Three Essential Characteristics of a Quantum Theory*

(1) *If $A$ and $B$ are distinct physical systems, then the observables of $A$ commute with those of $B$.*

- *What this means*: If $A$ and $B$ are *distinct*, then a measurement of a property (observable) of $A$ should not influence a measurement of a property of $B$.

  *More precisely*: Suppose we represent properties by operators.
  - Two operators $O_A$, $O_B$ *commute* just when $O_A O_B = O_B O_A$.
  - *Or*: Just when the order in which you apply them doesn't matter.
  - *Which is one way to say they are independent of each other.*

- *Recall*: Some quantum properties (*Hardness*, *Color*) are *not* independent in this sense.

  - *So*: The operators representing *Hardness* and *Color* do *not* commute.
  - *Note*: For a *classical* theory, *all* observables commute.

- *Thus*: What (1) says is that if we're dealing with two *distinct* quantum systems (and not just one), then how we measure the properties of one should be independent of how we measure the properties of the other.

*Three Essential Characteristics of a Quantum Theory*

(1) *If A and B are distinct physical systems, then the observables of A commute with those of B.*

- *CBH prove*: A necessary and sufficient condition for (1) is:

  *No superluminal information transmission between systems by measurement on one of them.*

- *Motivation*: A prohibition on superluminal signaling is equivalent to a prohibition on instantaneous signaling (according to Special Relativity).
  - *And*: A prohibition on instantaneous signaling is a way of enforcing independence.

*Alice and Bob are independent if:*

*any measurement Alice does here...*

*...cannot instantaneously affect the outcomes of measurements Bob does here.*

(2) *The observables of an individual system do not all commute with each other.*

- *What this means*: Just that there are quantum properties that cannot be simultaneously measured (like *Hardness* and *Color*).
- *CBH prove*: A necessary and sufficient condition for (2) is:

  *No broadcasting of the information contained in an unknown state.*
- *What **this** means*: Broadcasting is the generalization of cloning.

  - A state $\rho$ of a system $A$ can be *cloned* just when there is a ready state $\sigma$ of a system $B$ and an operator $U$ on states of the joint system $A$ & $B$ such that $U(\rho \otimes \sigma) = \rho \otimes \rho$.
  - A state $\rho$ of a system $A$ can be *broadcast* just when there is a ready state $\sigma$ of a system $B$ and an operator $T$ on states of the joint system $A$ & $B$ such that $T(\rho \otimes \sigma)|_A = T(\rho \otimes \sigma)|_B = \rho$.

  *The restriction of the joint state $T(\rho \otimes \sigma)$ to the system $A$.*
- *So*: CBH show that the impossibility of cloning/broadcasting quantum info entails (and is entailed by) the noncommutativity of quantum observables.

(3) *There are physically realizable nonlocal entangled states.*

- *Recall*: If we use a product vector space to represent the state space of a composite quantum system, then some states can be entangled in the mathematical sense of not being factorizable into a product with terms in the subspaces of each subsystem.
- (3) requires that this part of the mathematical formalism is *not surplus*: there are actual physical composite systems that can be in entangled states.
- *CBH prove*: A necessary and sufficient condition for (3) is:

  *No unconditionally secure bit commitment.*

*What does this mean... ?*

*Bit Commitment Protocol*

- A protocol in which two distrustful parties can exchange information with no cheating.

*Steps*:

1. Alice commits to a message by encoding it in an encrypted bit and sending the encryption to Bob.
2. Alice announces her commitment after an appropriate time interval.
3. The encryption should:
   (a) Not allow Bob to determine Alice's commitment before she announces it.
   (b) Not allow Alice to change her commitment after she announces it.

*Example*: Alice the Quant claims she can predict the stock market.

- On Day 1, Alice makes a stock prediction for Day 2, encodes it as a single bit (0 for "up", 1 for "down"), and seals it in a safe and gives Boss Bob the key.
- On Day 2 (after stocks close), Alice announces her prediction.
- Bob checks to see if it's accurate (and then either fires her or gives her a bonus).


*Bit Commitment Protocol*: (Bennett and Brassard 1984)

1. (a) Alice randomly choses either *Hardness* or *Color* to represent her bit. She then encodes the bit by measuring a sequence of electrons for that property, recording their values by means of an encryption chart.

   (b) Alice then generates a list of bits associated with her electrons.

   (c) Alice then sends her electrons to Bob.

**Encryption chart**

| *Hardness* | | *Color* | |
|---|---|---|---|
| $\|hard\rangle$ | $\Leftrightarrow 0$ | $\|black\rangle$ | $\Leftrightarrow 0$ |
| $\|soft\rangle$ | $\Leftrightarrow 1$ | $\|white\rangle$ | $\Leftrightarrow 1$ |

**Alice's list**

$H$: 1 0 1 0 0 1 1 1 0 1 0 1 1 0 0...


*Bit Commitment Protocol*: (Bennet and Brassard 1984)

2. (a) Upon reception of an electron, Bob *randomly* picks a *Hardness* box or a *Color* box to send it through.

   (b) Bob then generates two lists, one for the values of electrons measured for *Hardness*, the other for the values of electrons measured for *Color*.

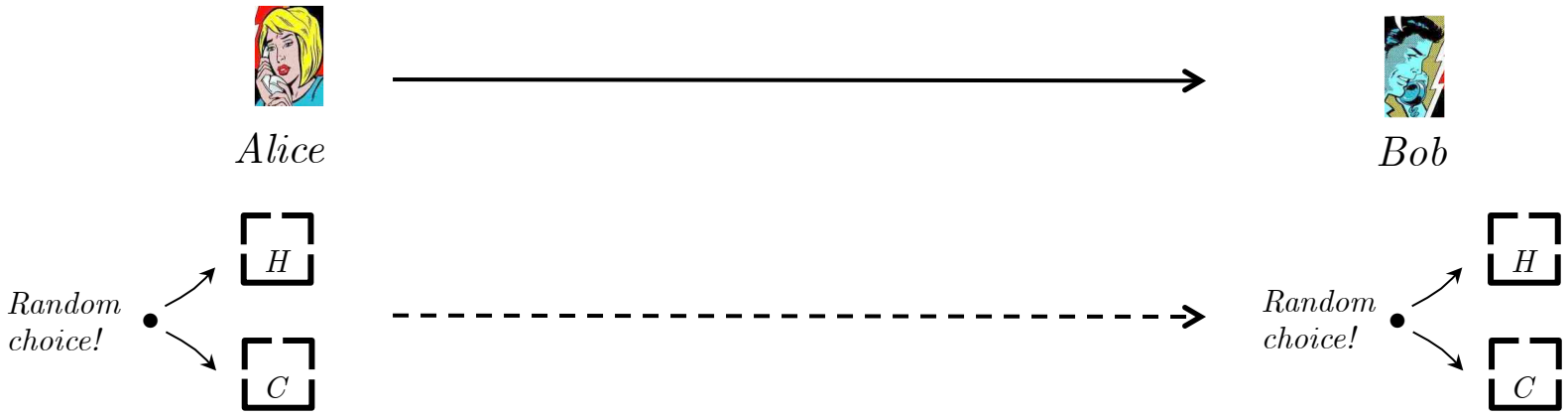
**Encryption chart**

| *Hardness* | | | *Color* | | |
|---|---|---|---|---|---|
| $\|hard\rangle$ | $\Leftrightarrow$ | 0 | $\|black\rangle$ | $\Leftrightarrow$ | 0 |
| $\|soft\rangle$ | $\Leftrightarrow$ | 1 | $\|white\rangle$ | $\Leftrightarrow$ | 1 |

**Bob's lists**

*H*: 1 - - 0 - - 1 - 0 1 - - 1 - 0...

*C*:- 0 0 - 0 1 - 1 - - 1 0 - 1...




*Bit Commitment Protocol*: (Bennet and Brassard 1984)

3. (a) After the appropriate time interval, Alice announces her commitment (encoded as either "*Hardness*" or "*Color*"), and certifies it by sending Bob her bit list.

   (b) Bob verifies Alice's commitment by comparing her list with his. There should be perfect correlation between one of his lists and Alice's, and no correlation between the other of his lists and Alice's.

**Encryption chart**

| *Hardness* | | | *Color* | | |
|---|---|---|---|---|---|
| $\|hard\rangle$ | $\Leftrightarrow$ | 0 | $\|black\rangle$ | $\Leftrightarrow$ | 0 |
| $\|soft\rangle$ | $\Leftrightarrow$ | 1 | $\|white\rangle$ | $\Leftrightarrow$ | 1 |

**Alice's list**

*H*: 1 0 1 0 0 1 1 1 0 1 0 1 1 0 0...

**Bob's lists**

*H*: 1 - - 0 - - 1 - 0 1 - - 1 - 0...

*C*:- 0 0 - 0 1 - 1 - - 1 0 - 1...

*How Alice Can't Cheat:*


- Alice cannot cheat by announcing her commitment after the fact (*i.e.*, if she originally committed to *Hardness*, she cannot, at Step #3, announce *Color*).
- *Why*? This requires Alice to reproduce Bob's "incorrect" list (his *Color* list in this case). And she cannot know with certainty the values of *Color* of any of the electrons she already measured for *Hardness*!

*How Alice Can Cheat:*


- Alice can *entangle* each electron she sends Bob with another electron.
- She can then wait and announce her commitment after the fact and hide this by measuring her electrons for the correct property *after* Bob has done his measurements.
- The bit list she then constructs will then be perfectly correlated with Bob's correct list, and uncorrelated with Bob's incorrect list.

*Example*:

- At Step #1, Alice prepares two electrons in an entangled state, say
  $\frac{1}{\sqrt{2}}(|hard\rangle_{A1}|soft\rangle_{B1} + |soft\rangle_{A1}|hard\rangle_{B1}) = \frac{1}{\sqrt{2}}(|white\rangle_{A1}|black\rangle_{B1} + |black\rangle_{A1}|white\rangle_{B1})$
- Alice then sends Bob electron $B1$ and keeps electron $A1$.
- If Bob then measures his electron $B1$ for *Color* and gets the value *black*, the entangled state collapses to $|white\rangle_{A1}|black\rangle_{B1}$.
- If Bob measures electron $B1$ for *Color* and gets the value *white*, the entangled state collapses to $|black\rangle_{A1}|white\rangle_{B1}$.
- Suppose Alice now discovers the correct prediction is *Color*.
- She can then measure her electron $A1$ for *Color*: if she gets the value *white*, she knows Bob got *black*, and if she gets *black*, she knows Bob got *white*.
- So she can reconstruct Bob's correct *Color* list.
- (And similarly if *Hardness* was the correct prediction.)

# II. Implications.

*General Claim*: (Bub 2004)
A quantum theory is a theory about the representation and manipulation of *information*.

- *Not* a theory about particles or waves...
- Information = "a new sort of physical entity".
- An entangled state = "a nonclassical communication channel".

*Why this is potentially significant*

- There is no general consensus on how to *interpret* quantum mechanics!

$$\left(\begin{array}{l}\text{An } \textit{interpretation} \\ \text{of a theory } T.\end{array}\right) = \left(\begin{array}{l}\text{A description of what the world} \\ \text{would be like if } T \text{ were true.}\end{array}\right)$$

*What would the world be like if quantum mechanics were true?*

*The Measurement Problem*

According to the *standard formulation*, there are two ways the state of a quantum system can change:

(a) *In the presence of a measurement*: Indeterministic, instantaneous collapse (Projection Postulate).

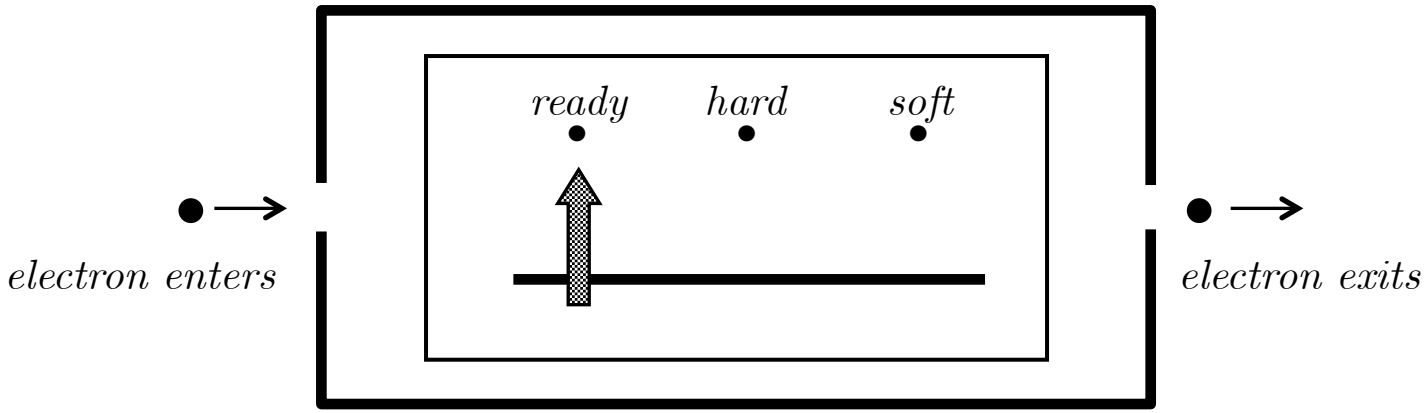
- Suppose the state of our system is given by $|Q\rangle = \frac{1}{\sqrt{2}}(|white\rangle + |black\rangle)$.
- Suppose we measure our system for *Color* and get the value *white*.
- Then the state collpases to $|white\rangle$.

(b) *In the absence of a measurement*: Deterministic, temporal evolution *via* the Schrödinger equation.

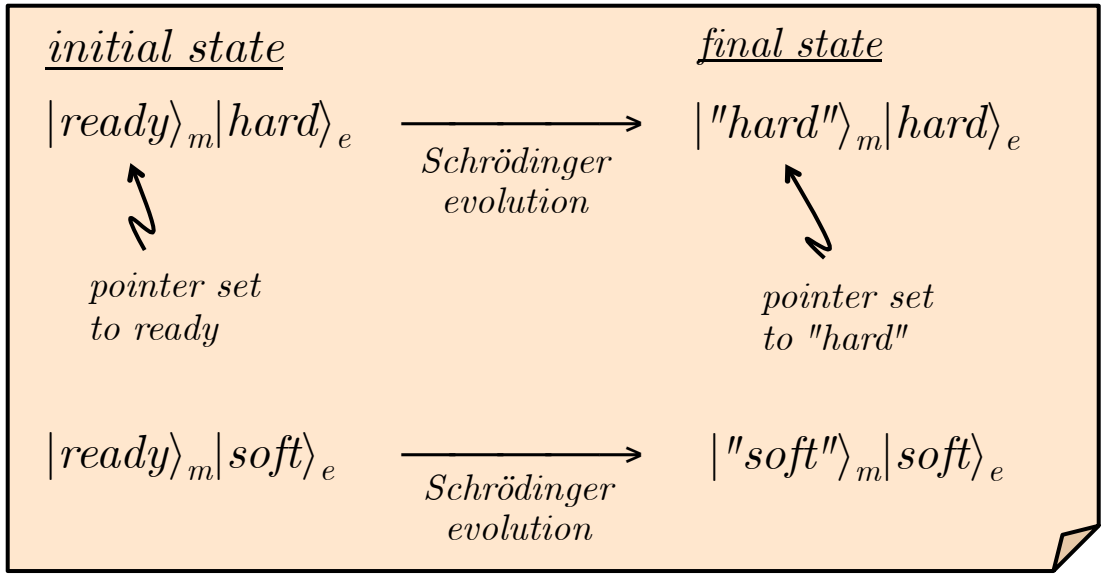
- Suppose the state of our system at $t_i$ is given by $|Q\rangle$.
- Then the state of our system at $t_f > t_i$ is given by $U|Q\rangle$, where $U = e^{-iHt_f/\hbar}$ is a linear operator (and $H$ is the Schrödinger Hamiltonian operator).

*These accounts of state evolution are inconsistent:*
*They make distinct predictions!*

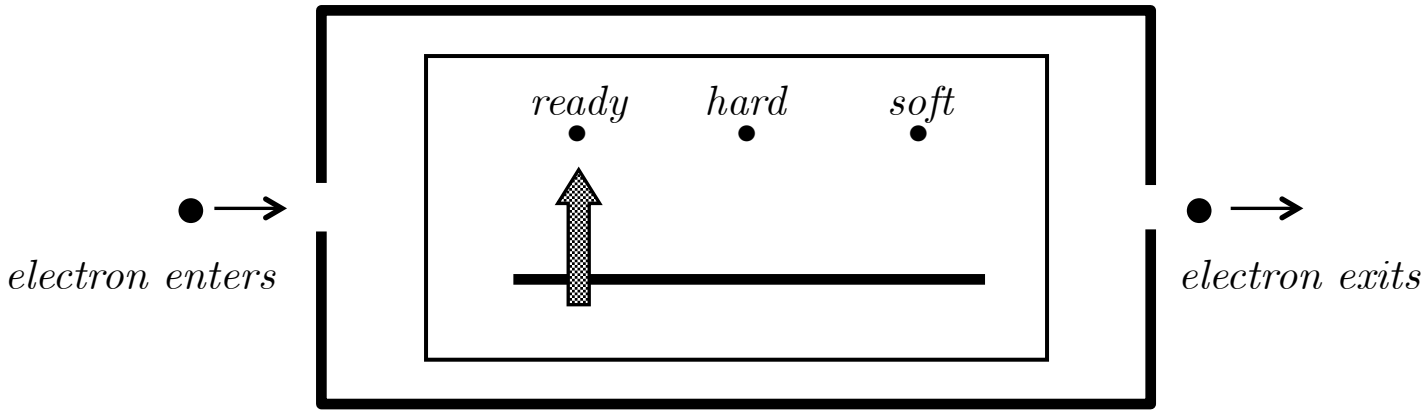
*How to Model a Measurement Process:*




- Consider composite system of measuring device and electron: $m + e$.
- The Schrödinger equation tells us how the state of this composite system evolves in time.



*How to Model a Measurement Process:*




- *Now*: Suppose a *black* electron is measured for *Hardness*.

*initial state* $\xrightarrow[\text{evolution}]{\text{Schrödinger}}$ *final state*

$|ready\rangle_m|black\rangle_e$

$= \sqrt{\frac{1}{2}}\left(|ready\rangle_m|hard\rangle_e + |ready\rangle_m|soft\rangle_e\right)$ $\quad\sqrt{\frac{1}{2}}\left(|"hard"\rangle_m|hard\rangle_e + |"soft"\rangle_m|soft\rangle_e\right)$

- *But*: According to the *Projection Postulate*,

*initial state* $\xrightarrow{\text{collapse}}$ *final state*

$|ready\rangle_m|black\rangle_e$

$= \sqrt{\frac{1}{2}}\left(|ready\rangle_m|hard\rangle_e + |ready\rangle_m|soft\rangle_e\right)$

*either* $|"hard"\rangle_m|hard\rangle_e$ with prob $= 1/2$

*or* $|"soft"\rangle_m|soft\rangle_e$ with prob $= 1/2$

*final state*

$\sqrt{\frac{1}{2}}\left(|"hard"\rangle_m|hard\rangle_e + |"soft"\rangle_m|soft\rangle_e\right)$ *according to Schrödinger evolution*

| | | | |
|---|---|---|---|
| *either* | $|"hard"\rangle_m|hard\rangle_e$ | with prob = 1/2 | *according to Projection Postulate* |
| *or* | $|"soft"\rangle_m|soft\rangle_e$ | with prob = 1/2 | |

- According to the EE Rule, these represent *different* states!

*Initial response*:

- According the standard formulation, the Projection Postulate is supposed to take over during a measurement.
- So just ignore what the Schrödinger dynamics predicts when measurements occur.

- *But*: What exactly is a *measurement*? *When* is the Projection Postulate supposed to take over from the Schrödinger dynamics?

*Some Attempts to Solve the Measurement Problem*

(a) Dynamical Collapse Interpretations

- Keep the Projection Postulate and modify the Schrödinger dynamics so that superpositions will *not* occur after measurements.

(b) Many Worlds Interpretations

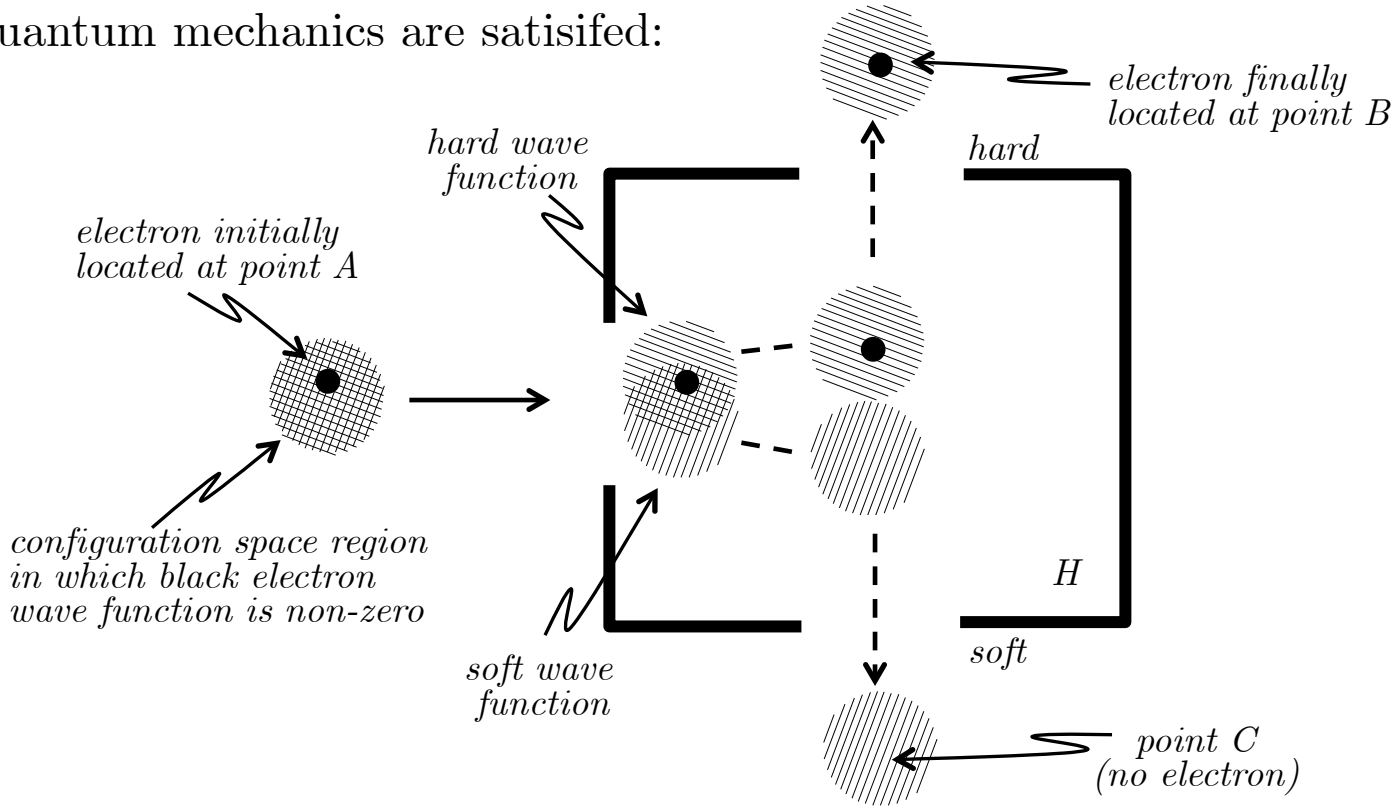
- Keep the Schrödinger dynamics and give up the Projection Postulate.
- Claim that each term in a superposition represents a distinct possible world.
- *In particular*: When a measurement (or, in general, interaction) occurs, all possible outcomes are generated, one per possible world.

(c) Modal Interpretations.

- Keep the Schrödinger dynamics and the Projection Postulate, but give up the Eigenvalue/Eigenvector Rule.
- Claim that there is some set of always-determinate properties for any given quantum system, and that this set uniquely determines measurement outcomes.

*Example of Modal Interpretation*: Bohm's Theory.

- Particle positions always have determinate values.
- The dynamics of such particle positions is defined in terms of a "guiding wavefunction" in configuration space that guarantees that the statistical predictions of quantum mechanics are satisifed:




- Inside *Hardness* box, *black* wave function "splits" into *soft* and *hard* wave functions.
- Depending on where electron is initially located, it will either be "carried" up with the *hard* wave function, or down with the *soft* wave function.

$$|black\rangle|\psi_A(x)\rangle \longrightarrow \frac{1}{\sqrt{2}}\left(|hard\rangle|\psi(x)\rangle + |soft\rangle|\psi_C(x)\rangle\right)$$

*So*: Does the CBH Theorem really contribute to an understanding of the Measurement Problem?

> *General Claim*: (Bub 2004)
> A quantum theory is a theory about the representation and manipulation of *information*.

- In what sense is this an interpretation of quantum mechanics that addresses the Measurement Problem?

- *Also*: Recall Timpson (2008):

> *Information* = What is produced by an information source that is required to be reproducible at the receiver if the transmission is to be counted a success.

- *In particular*: Information (in the technical sense) is an "abstract noun".
- "Information" does not refer to a substance (*token*); rather, it refers to a *type*.