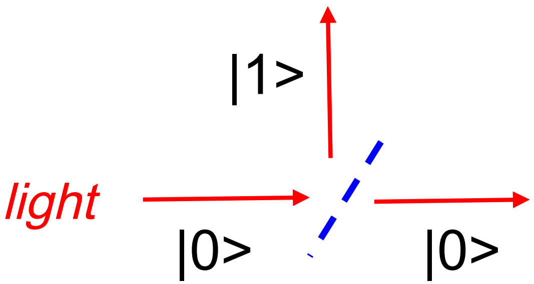
Counterfactual quantum computation

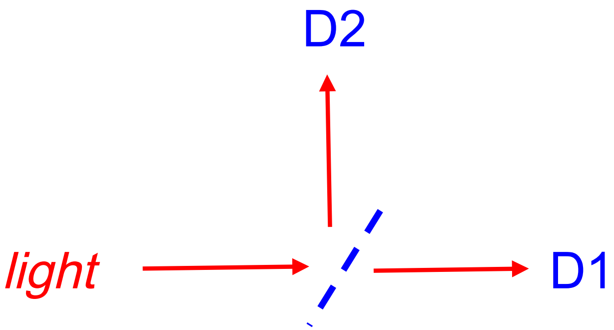
Richard Jozsa
DAMTP, University of Cambridge

Photons and half-silvered mirrors (beamsplitters)



Now make light weaker and weaker.

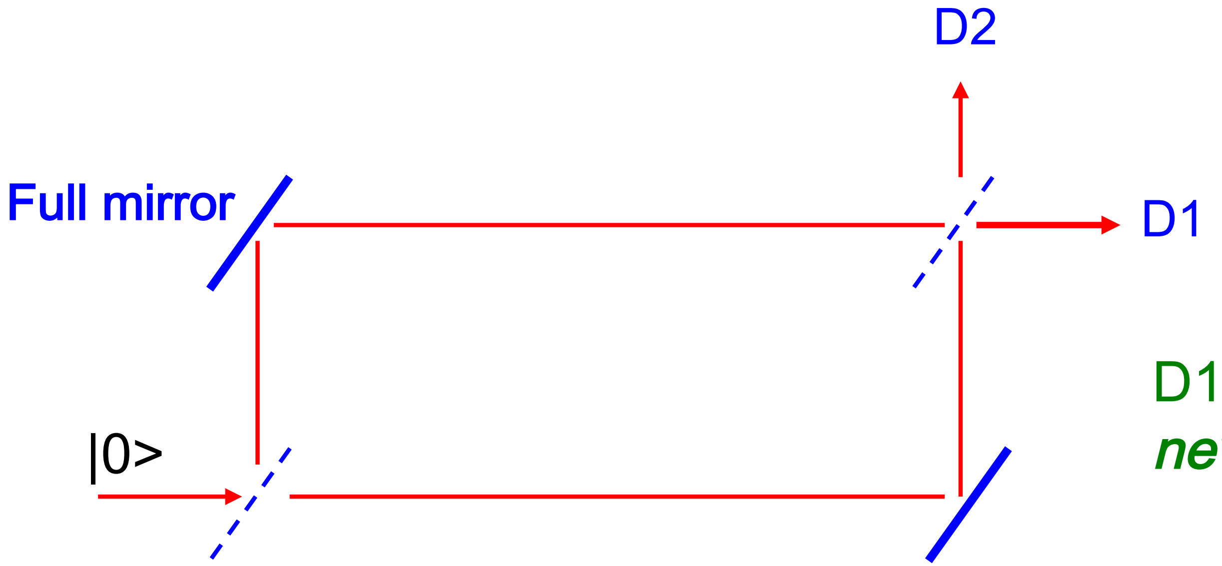
Put detectors in the two arms: *we see corpuscular behaviour (photons)*



Exactly one of D1, D2 *fires,*
at random, probabilities ½ each.
Afterwards photon is in |0> or |1> state
as seen (if non-destructive detection).

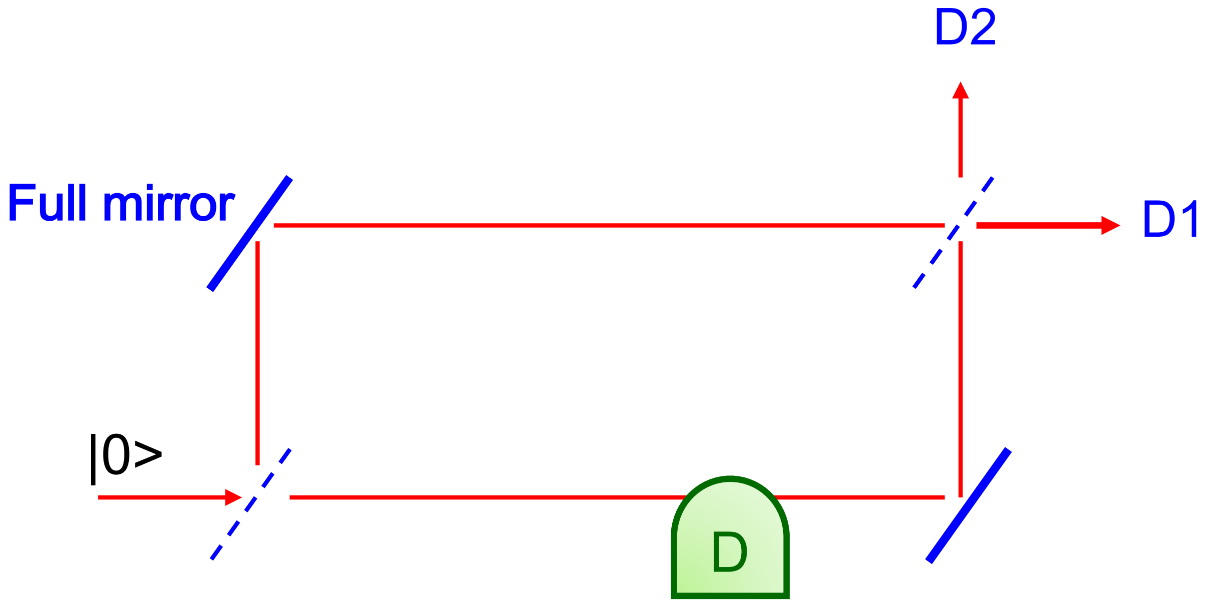
(!) Further experiments show: each photon goes *both* ways!
If we look to see "which way" we get a definite answer and
photon state changes to be in only that arm.

Why say "*both ways*"? - Interferometer



D1 *always fires* –
never D2!

Why say "*both ways*"? - Interferometer



Any device able to detect photon
(non-destructively)

*If D absent, photon always registers at D1

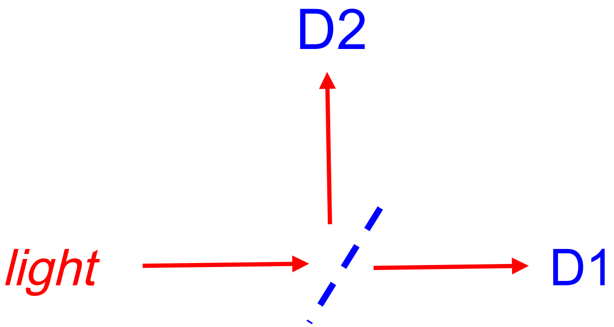
*If D present, photon registers at D2 (or at D1) with probability half (and D may or may not detect a photon).

So can sometimes get:

Photon seen at D2 but D remains "untouched" (no detection).

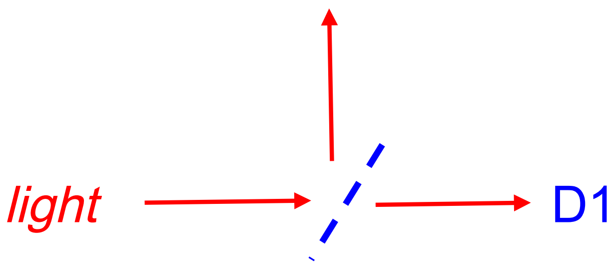
This can only happen if D could have detected the photon.

The basic "counterfactual" (CF) effect



* *Photon emerges from half-mirror going "both ways".*
* *Exactly one detector always fires -- never both!*

The basic "counterfactual" (CF) effect



* *Photon emerges from half-mirror going "both ways".*

* *Exactly one detector always fires -- never both!*

Now remove D2

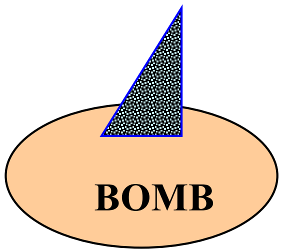
If D1 does not fire then photon is fully in vertical path
i.e. photon state is changed even though the agent (D1) has been unaffected (photon found *absent* in horizontal path!)

"State change caused by fact that D1 *could* have detected the photon even though it, in fact, *did not*."

Can use this to learn *whether* a proposed detector *can* function *without actually using the detector* !

CF quantum effects

* Elizur-Vaidman (1993) bomb testing problem
* Interaction-free imaging
* Computational applications (G. Mitchison & R. Jozsa 2000)

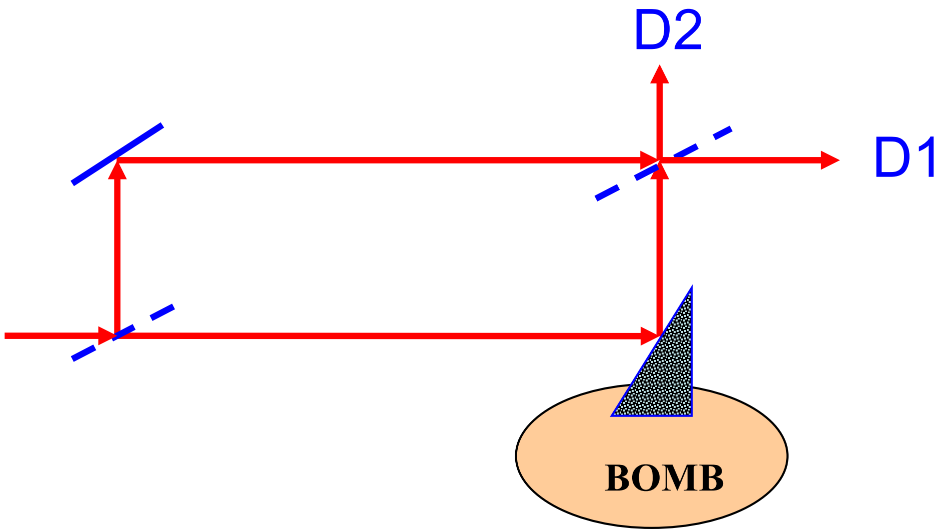


Have many bombs.
Trigger so sensitive that any disturbance will set bomb off!
But bomb may be a dud - trigger jammed.

Problem:
How can we tell if a bomb is good without setting it off ?

No classical solution!
There is a quantum solution!

Photon interferometer (again)



Solution of bomb testing problem:

D is bomb trigger (e.g. as a mirror). Photon deflects off it at lower corner.

Dud bomb -- cannot register photon, photon never seen at D2.

Good bomb -- able to register presence of photon.

Sometimes photon seen at D2 but bomb unexploded.
Then it must then be a good bomb !
(Half the time, photon will be seen absent by bomb, and half of those times it will register at D2.)

Interaction-free Imaging

D is presence or absence of an opaque object.

Absence: just empty space! -- photon passes through and always registers at D1.

Presence: path blocked! -- photon seen at D2 *half the time, and half these times photon not registered to go along lower path! i.e. then no photon hits object! (All this works with prob ¼.)*

Improved set-up: probability ¼ improved to 1- ε (any ε > 0).
Example: photographic film at D2: with raster scan, can get silhouette image of object without shining any light on it!

Experimental demonstration *(S. Inoue & G. Björk 2000):*
"…here we present experimental results where a photographic film's shape is imaged on an identical piece of film without exposing the first film."

Application: silhouette X-ray imaging without radiation damage!

Counterfactual quantum computation

Imagine replacing bomb by a (quantum) computer QC of following kind:

* QC has on/off switch, initially off (switch settings: off = 0, on = 1);
* QC programmed ready to solve a yes/no problem if switched on,
  for time *T* (denote answers *r* by *r* = 0 for 'yes' and *r* = 1 for 'no';
* QC has output register initially set to 0, that will contain the answer *r*.

So initially we have $|0\rangle \; |0\rangle \; |R\rangle$ and in time T get:

switch output prog

$$|0\rangle \quad |j\rangle \quad |R\rangle \quad \longrightarrow \quad |0\rangle \quad |j\rangle \quad |R\rangle \qquad \text{(computer off)}$$

$$|1\rangle \quad |j\rangle \quad |R\rangle \quad \longrightarrow \quad |1\rangle \; |j \oplus r\rangle \; |R\rangle \qquad \text{(computer on)}$$

For the two possible (unknown) answers *r* = 0 or 1 we have unitary operations U_0 or U_1 on switch and output registers, with

U_0 = Identity operation $\qquad$ U_1 = CNOT quantum operation

when the computer is run.

In the interferometer: replace bomb by computer with photon being the agent capable of switching it on.

If $r = 1$: computer works as a photon detector i.e. wait time T
and look at output register (*like "good bomb exploding".)*

If $r = 0$: computer does nothing i.e. output register unchanged
(whether it ran or not, cannot be a photon detector)
(*like "bomb with jammed trigger remaining unchanged".)*

So as before:
if we see photon at D2 we can be sure that $r = 1$, and then
if also the output register shows value 0 we know the computer was not run *("good bomb that remains unexploded".)*
These two things viz. CF computation of answer *when it is 1*, happen with probability ¼.

If instead we see photon at D1: this always occurs if $r = 0$ but sometimes occurs for $r = 1$; and then sometimes computer is run too *("bomb is exploded") .* Thus if photon seen at D1 we cannot deduce r.

Improving the ¼ : not running the computer *many times!*

Look just at switch and output registers initially in $|0\rangle\ |0\rangle$

Choose *N* (largish), write $\theta = (\frac{\pi}{2})/N$

Rotate switch to $\cos\theta|0\rangle + \sin\theta|1\rangle$

Wait for time *T*, get $\cos\theta|0\rangle|0\rangle + \sin\theta|1\rangle|r\rangle$

Measure the output register (only):

if r is actually 1:

we see 0, prob. $\cos^2\theta$ *and state becomes* $|0\rangle\ |0\rangle$ *(computer not run)*

or see 1, prob. $\sin^2\theta$ *... ... ...* $|1\rangle\ |1\rangle$ *(computer has run)*

(and latter are also the new states of switch/output registers).

If see 1 we know r = 1 but abort (as computer has run too!)

if r is actually 0:

we see 0 always and state becomes $\cos\theta|0\rangle|0\rangle + \sin\theta|1\rangle|0\rangle$

Repeat the above *N* times (each time rotating the switch by θ and measuring output register).

After *N* repeats, finally measure switch to see if it is 0 or 1.

If $r = 0$:
state will have rotated to $|1\rangle\ |0\rangle$ so switch will certainly show 1 *(and computer will have been run)*.
If $r = 1$:
with prob $(\cos\frac{\pi}{2N})^N$ state will be $|0\rangle\ |0\rangle$ and switch will certainly show 0. In this case all intermediate measurements are 0 too, *so the computer has not run yet we learn that r = 1!*

And note: $(\cos\frac{\pi}{2N})^N \to 1$ as $N \to \infty$.

For ***any*** protocol write
P_r = probability or learning result r (if it is r)
without running the computer.

In the *above* protocol we have
$P_0 = 0$ and $P_1 \to 1$ as $N \to \infty$.

Can we have ***both*** P_0 *and* P_1 *nonzero, and* ***both*** $\to 1$??

G. Mitchison and R. Jozsa "Counterfactual computation", *Proc. Roy. Soc. (Lond.)* A457, *p1175-1193 (2001)*

Formulated notion of a general protocol with insertions of the computer.

Defined a precise mathematical notion of the feature that we learn the result *r* "without running the computer".

Proved:

THEOREM

(i) It is possible to have both P_0 and P_1 nonzero, but

(ii) We always have $P_0 + P_1 \leq 1$ (rather than 2!)

(iii) If either of P_0 or P_1 approach 1, then number N of insertions of the computer must have $N \to \infty$.

i.e. we then need to not run the computer unboundedly many times.