Nobel A. Aspect: des inégalités de Bell à la communication quantique

Jean Orloff

Menu

Menu

- Lois de Copenhague

Menu

- Lois de Copenhague
- Photon et polarisation

Menu

- Lois de Copenhague
- Photon et polarisation
- Paradoxe EPR

Menu

- Lois de Copenhague
- Photon et polarisation
- Paradoxe EPR
- Inégalités de Bell

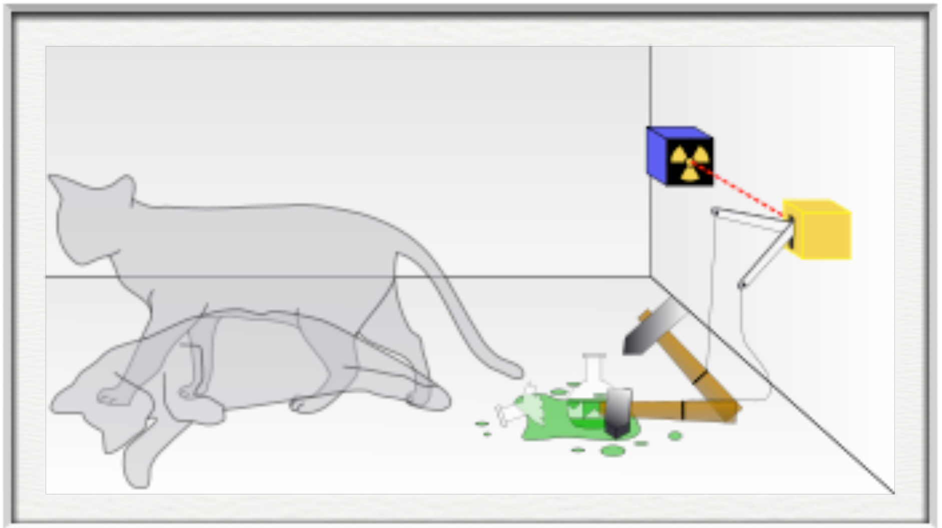
Menu

- Lois de Copenhague
- Photon et polarisation
- Paradoxe EPR
- Inégalités de Bell
- Test expérimentaux d’Aspect et al.

Etat intriqué célèbre:
le chat de Schrödinger

Etat intriqué célèbre: le chat de Schrödinger

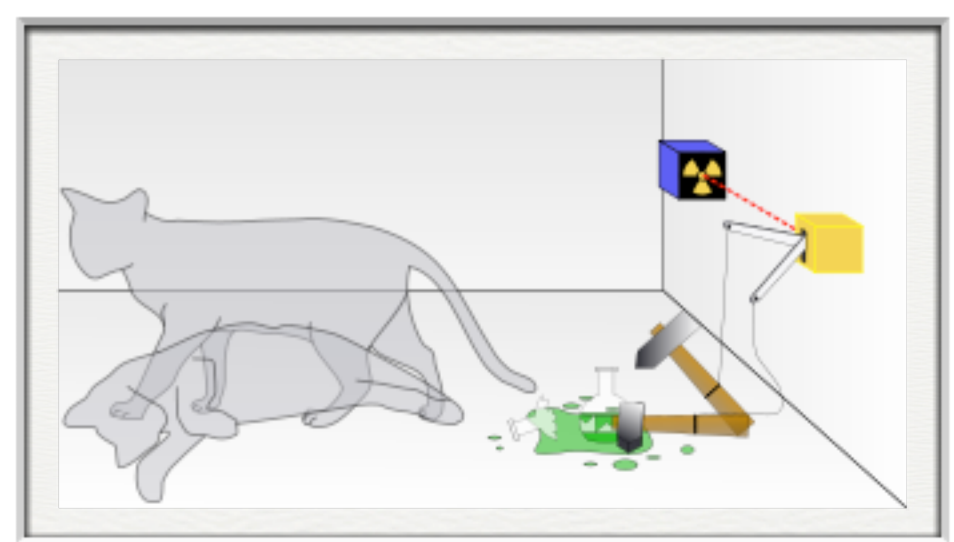
Dans un coffre-fort: chat + noyau instable(1/2vie=1h) + marteau + fiole d'acide cyanhydrique



Etat intriqué célèbre: le chat de Schrödinger

Dans un coffre-fort: chat + noyau instable(1/2vie=1h) + marteau + fiole d'acide cyanhydrique

L'état d'un noyau instable $|N^*\rangle$ qui se désintègre en $|n\rangle$ stable est une superposition $c\,|N^*\rangle + s\,|n\rangle$ tant que le coffre reste fermé (i.e. pas de mesure)

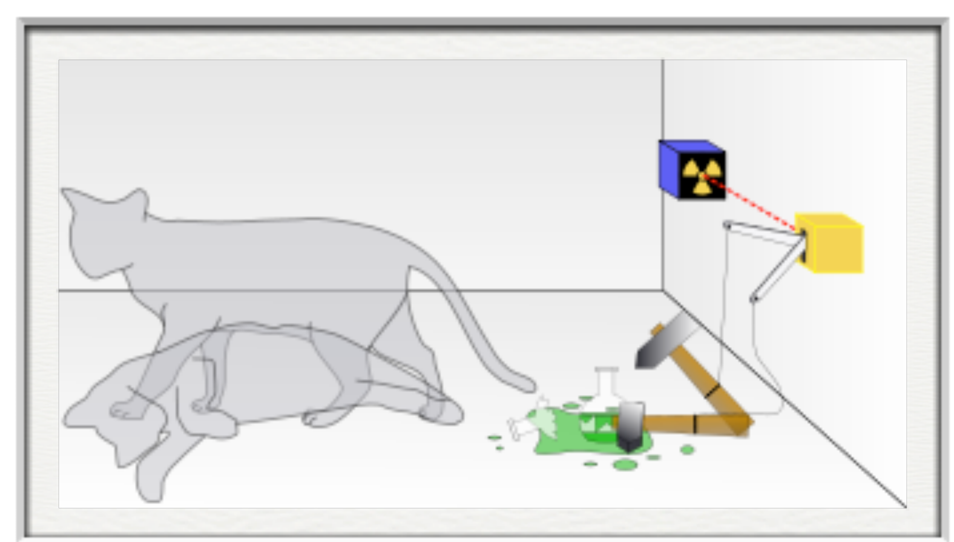


Etat intriqué célèbre: le chat de Schrödinger

Dans un coffre-fort: chat + noyau instable(1/2vie=1h) + marteau + fiole d'acide cyanhydrique

L'état d'un noyau instable $|N^*\rangle$ qui se désintègre en $|n\rangle$ stable est une <u>superposition</u> $c\,|N^*\rangle + s\,|n\rangle$ tant que le coffre reste fermé (i.e. pas de mesure)

Si le noyau se désintègre, il libère le marteau, casse la fiole et tue le chat: les états noyau - chat sont liés (ou **<u>intriqués</u>**)



Etat intriqué célèbre: le chat de Schrödinger

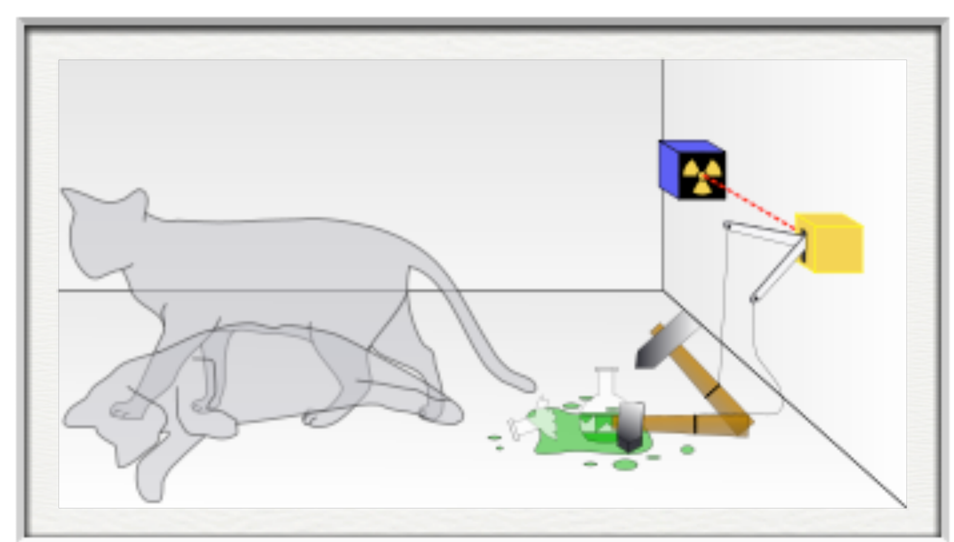
Dans un coffre-fort: chat + noyau instable(1/2vie=1h) + marteau + fiole d′acide cyanhydrique

L'état d'un noyau instable $|N^*\rangle$ qui se désintègre en $|n\rangle$ stable est une <u>superposition</u> $c\,|N^*\rangle + s\,|n\rangle$ tant que le coffre reste fermé (i.e. pas de mesure)

Si le noyau se désintègre, il libère le marteau, casse la fiole et tue le chat: les états noyau - chat sont liés (ou <u>**intriqués**</u>)

$$c\,|\text{Noyau}^*\rangle\,|\text{Chat vivant}\rangle + s\,|\text{noyau}\rangle\,|\text{chat mort}\rangle$$

Dans ce cas pendant ±1h, le chat aussi n′est tout à fait ni vivant ni mort!… (Schrödinger, 1935)



Etat intriqué célèbre: le chat de Schrödinger

Dans un coffre-fort: chat + noyau instable(1/2vie=1h) + marteau + fiole d'acide cyanhydrique

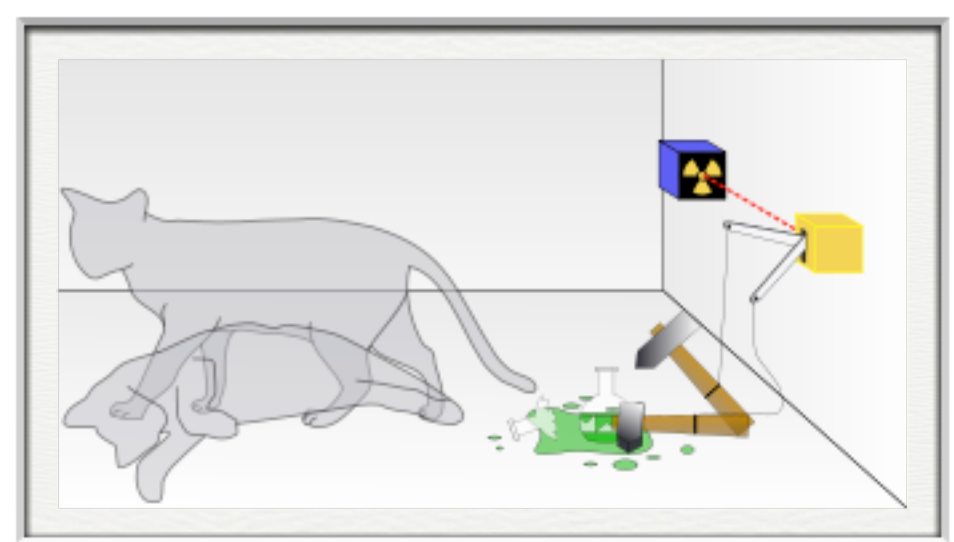
L'état d'un noyau instable $|N^*\rangle$ qui se désintègre en $|n\rangle$ stable est une <u>superposition</u> $c\,|N^*\rangle + s\,|n\rangle$ tant que le coffre reste fermé (i.e. pas de mesure)

Si le noyau se désintègre, il libère le marteau, casse la fiole et tue le chat: les états noyau - chat sont liés (ou <u>**intriqués**</u>)

$$c\,|\text{Noyau}^*\rangle\,|\text{Chat vivant}\rangle$$
$$+\,s\,|\text{noyau}\rangle\,|\text{chat mort}\rangle$$

Dans ce cas pendant ±1h, le chat aussi n'est tout à fait ni vivant ni mort!… (Schrödinger, 1935)

Réalité objective d'un tel état quantique???



Lois de Copenhague

Bohr, Born,… 1926-27

Désespoir du gendarme quantique

Désespoir du gendarme quantique

Gendarme: Notre radar vous a flashé dans le village à 68km/h.

Désespoir du gendarme quantique

Gendarme: Notre radar vous a flashé dans le village à 68km/h.

Conducteur Quantique: ma vitesse était indéfinie avant votre mesure: c′est **vous** qui m′avez fait commettre l′infraction!

Désespoir du gendarme quantique

Gendarme: Notre radar vous a flashé dans le village à 68km/h.

Conducteur Quantique: ma vitesse était indéfinie avant votre mesure: c′est **vous** qui m′avez fait commettre l′infraction!

G.: Il vous appartient de contrôler votre vitesse de façon à ne pas dépasser la limite en cas de mesure.

Désespoir du gendarme quantique

Gendarme: Notre radar vous a flashé dans le village à 68km/h.

Conducteur Quantique: ma vitesse était indéfinie avant votre mesure: c′est **vous** qui m′avez fait commettre l′infraction!

G.: Il vous appartient de contrôler votre vitesse de façon à ne pas dépasser la limite en cas de mesure.

C.Q.: j′avais bien vérifié que j'avais v<50km/h, mais votre radar m'a localisé dans le village avant de mesurer ma vitesse.

Désespoir du gendarme quantique

<u>Gendarme:</u> Notre radar vous a flashé dans le village à 68km/h.

<u>Conducteur Quantique:</u> ma vitesse était indéfinie avant votre mesure: c′est **vous** qui m′avez fait commettre l′infraction!

<u>G.:</u> Il vous appartient de contrôler votre vitesse de façon à ne pas dépasser la limite en cas de mesure.

<u>C.Q.:</u> j′avais bien vérifié que j'avais v<50km/h, mais votre radar m'a localisé dans le village avant de mesurer ma vitesse.

Selon les lois de la mécanique quantique et le principe d′incertitude, cela m′a fait perdre le contrôle de ma vitesse.

Désespoir du gendarme quantique

Gendarme: Notre radar vous a flashé dans le village à 68km/h.

Conducteur Quantique: ma vitesse était indéfinie avant votre mesure: c′est **vous** qui m′avez fait commettre l′infraction!

G.: Il vous appartient de contrôler votre vitesse de façon à ne pas dépasser la limite en cas de mesure.

C.Q.: j′avais bien vérifié que j'avais v<50km/h, mais votre radar m'a localisé dans le village avant de mesurer ma vitesse.

Selon les lois de la mécanique quantique et le principe d′incertitude, cela m′a fait perdre le contrôle de ma vitesse.

G.: Votre cas n′est pas clair, et d′abord quelles sont ces lois?

Loi quantique 1: **états**

Loi quantique 1: **états**

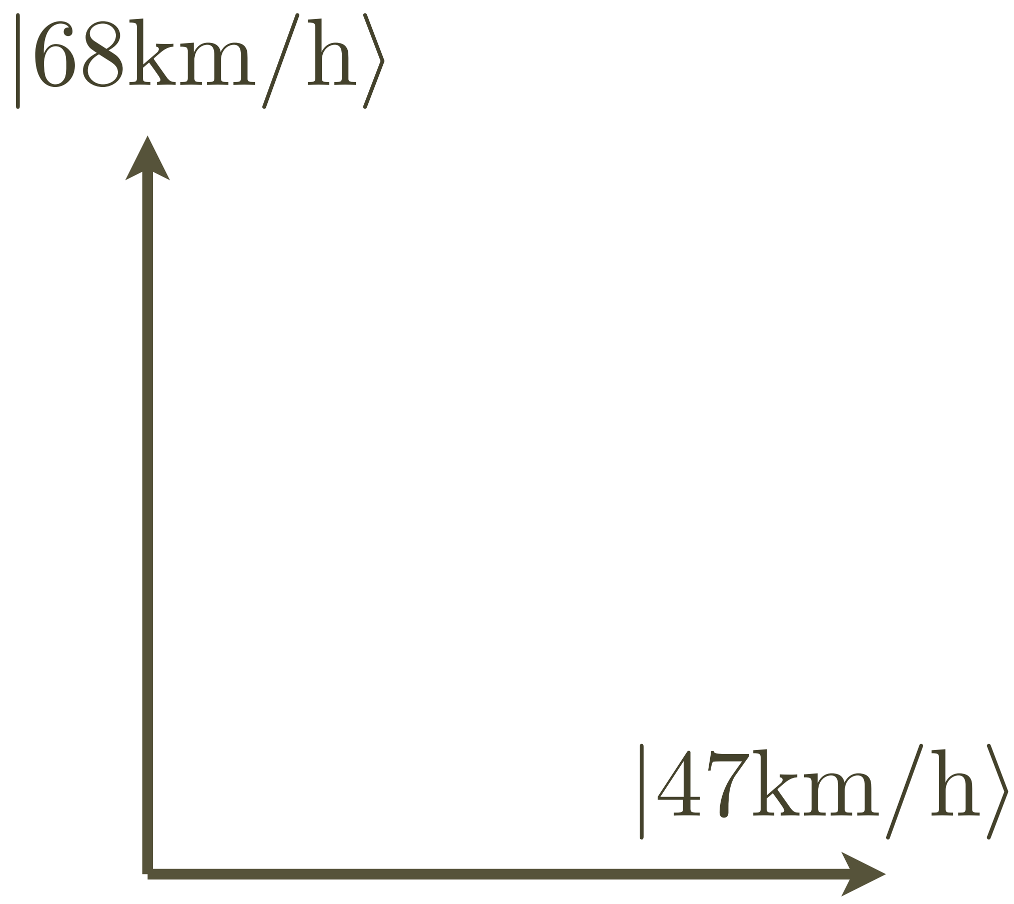
- **L′état d′un système quantique est entièrement déterminé par un vecteur.**

Loi quantique 1: **états**

- **L′état d′un système quantique est entièrement déterminé par un vecteur.**
- À chaque vecteur correspond un état possible.

Loi quantique 1: **états**

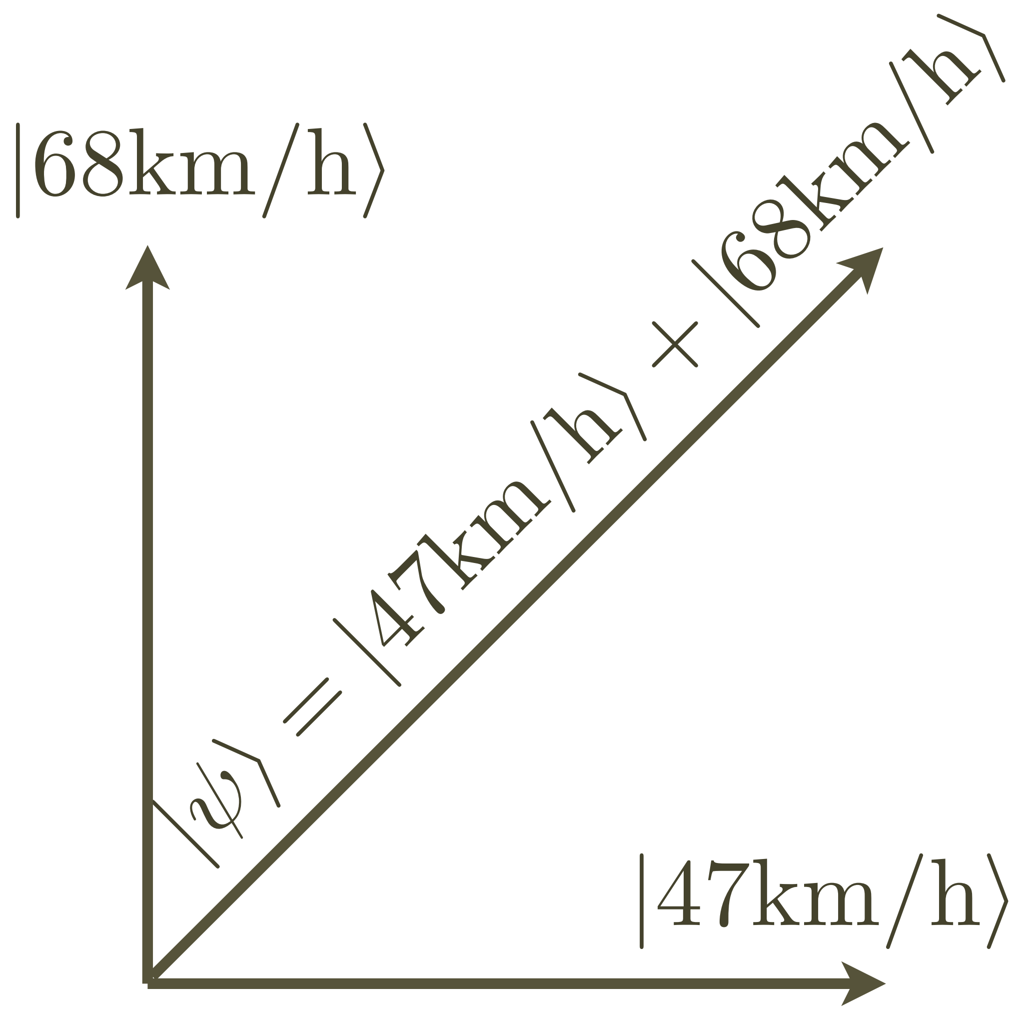
- **L′état d′un système quantique est entièrement déterminé par un vecteur.**
- À chaque vecteur correspond un état possible.
- Si les états *"rouler à 47km/h"* et *"rouler à 68km/h"* existent,



Loi quantique 1: **états**

- **L'état d'un système quantique est entièrement déterminé par un vecteur.**
- À chaque vecteur correspond un état possible.
- Si les états *"rouler à 47km/h"* et *"rouler à 68km/h"* existent,

alors leur somme vectorielle définit un état possible.

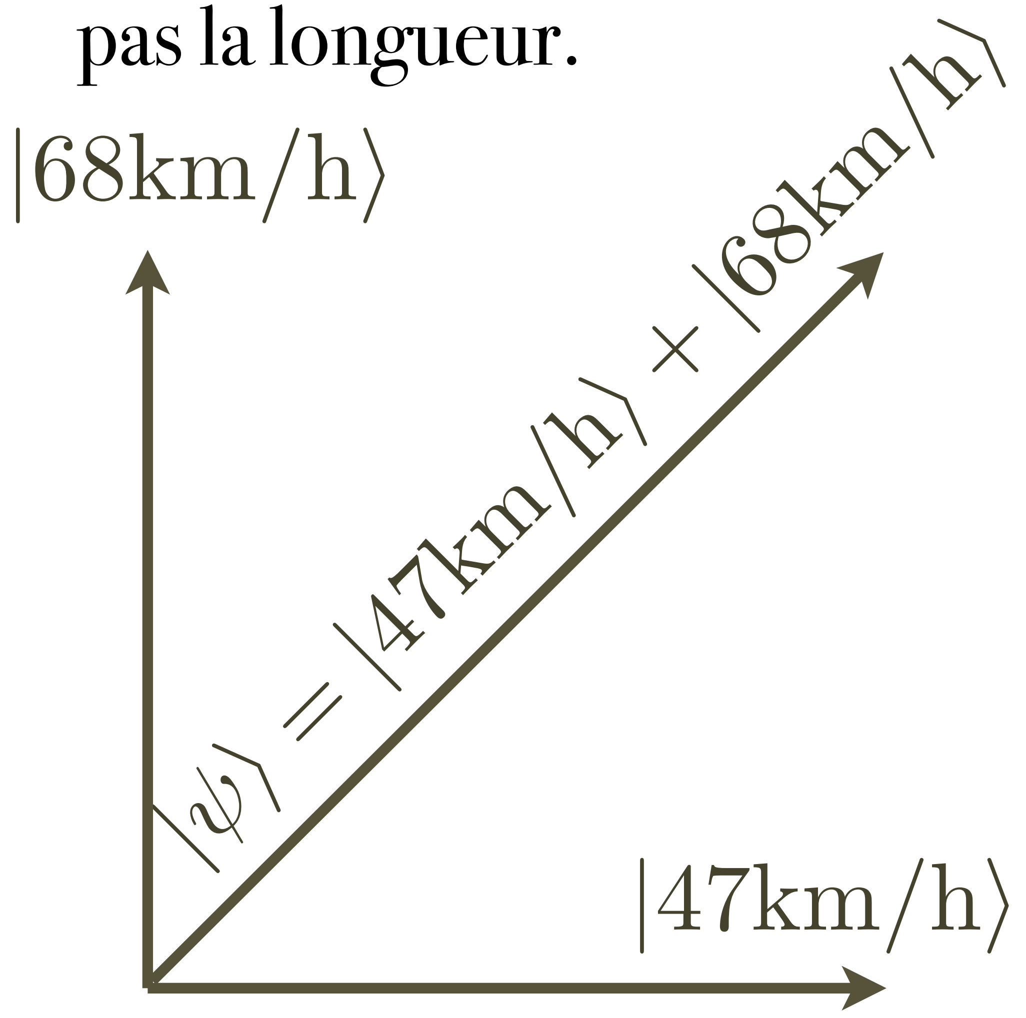


Loi quantique 1: **états**

- **L'état d'un système quantique est entièrement déterminé par un vecteur.**
- À chaque vecteur correspond un état possible.
- Si les états *"rouler à 47km/h"* et *"rouler à 68km/h"* existent,

  alors leur somme vectorielle définit un état possible.

- Deux vecteurs proportionnels définissent le même état: la direction compte, pas la longueur.

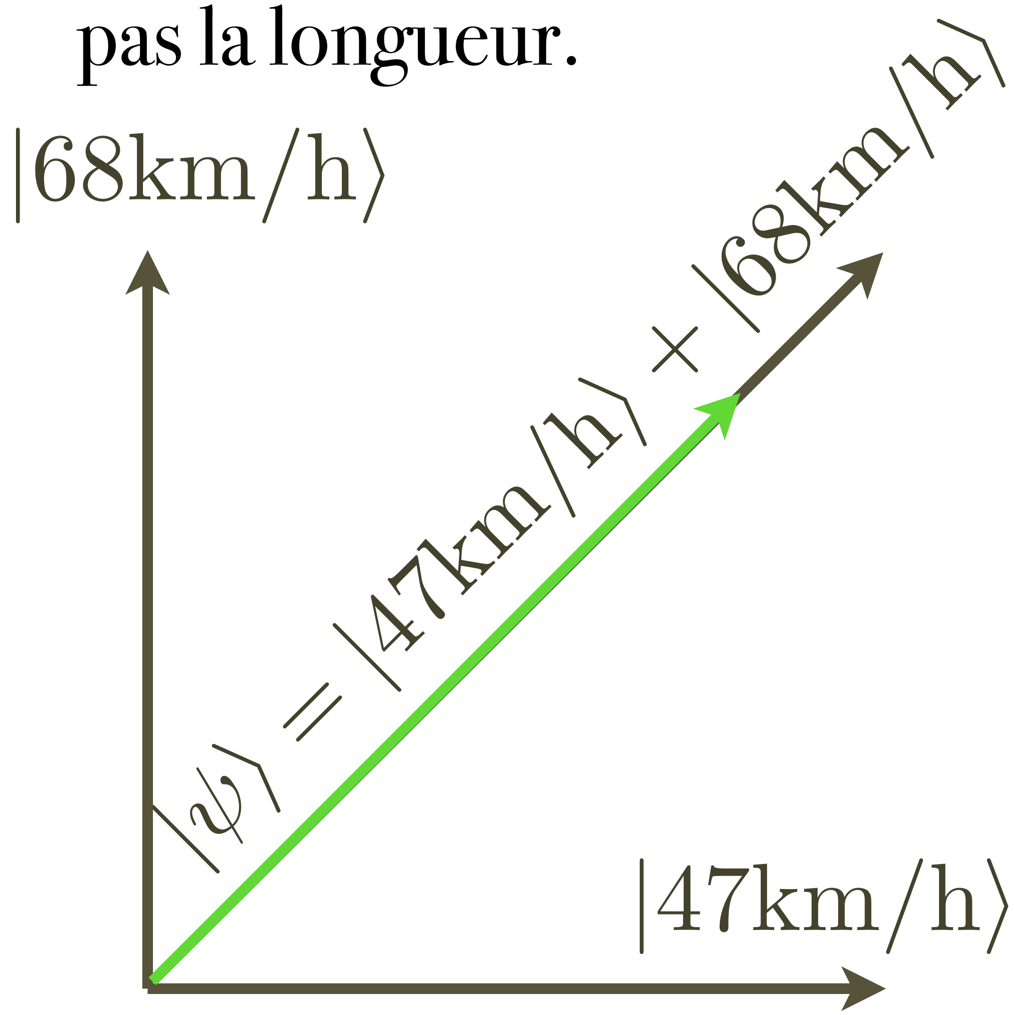


Loi quantique 1: **états**

- **L′état d′un système quantique est entièrement déterminé par un vecteur.**
- À chaque vecteur correspond un état possible.
- Si les états *"rouler à 47km/h"* et *"rouler à 68km/h"* existent,

  alors leur somme vectorielle définit un état possible.

- Deux vecteurs proportionnels définissent le même état: la direction compte, pas la longueur.

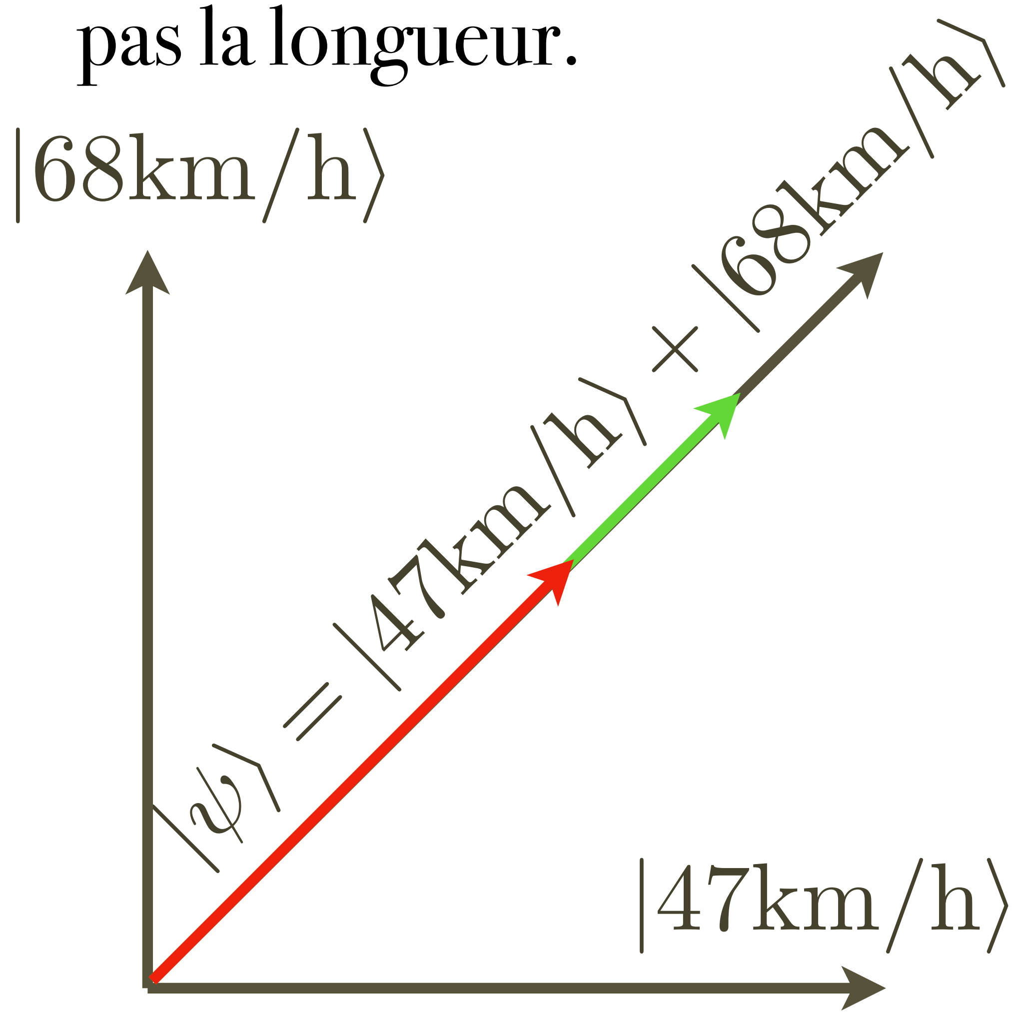


Loi quantique 1: **états**

- **L'état d'un système quantique est entièrement déterminé par un vecteur.**
- À chaque vecteur correspond un état possible.
- Si les états *"rouler à 47km/h"* et *"rouler à 68km/h"* existent,

  alors leur somme vectorielle définit un état possible.

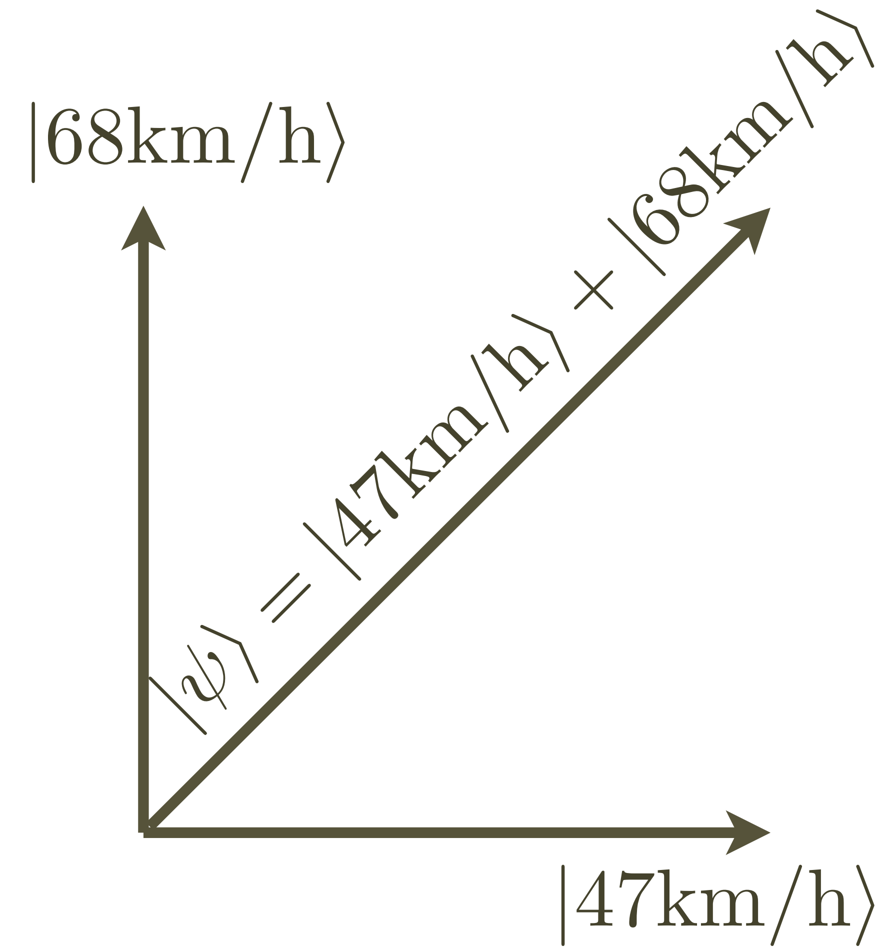
- Deux vecteurs proportionnels définissent le même état: la direction compte, pas la longueur.



Loi quantique 2: **amplitudes**

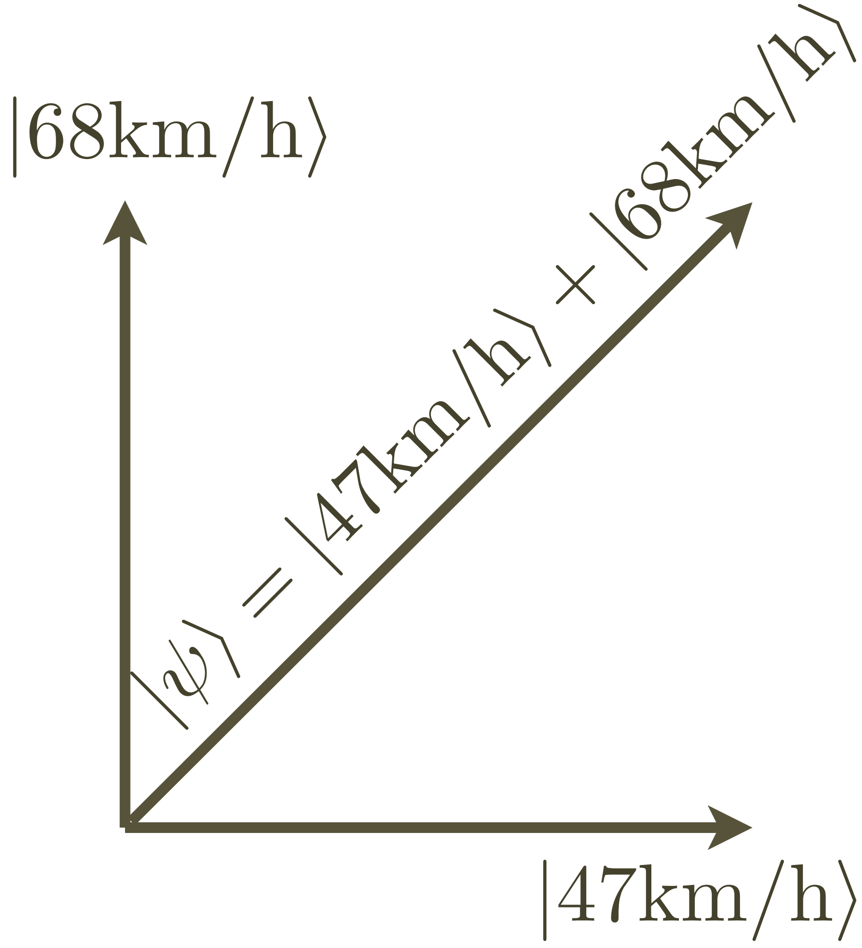
Loi quantique 2: **amplitudes**

- Si on note $\langle 47|\psi\rangle(= 1)$ le **produit scalaire** de 2 vecteurs, la longueur s′écrit



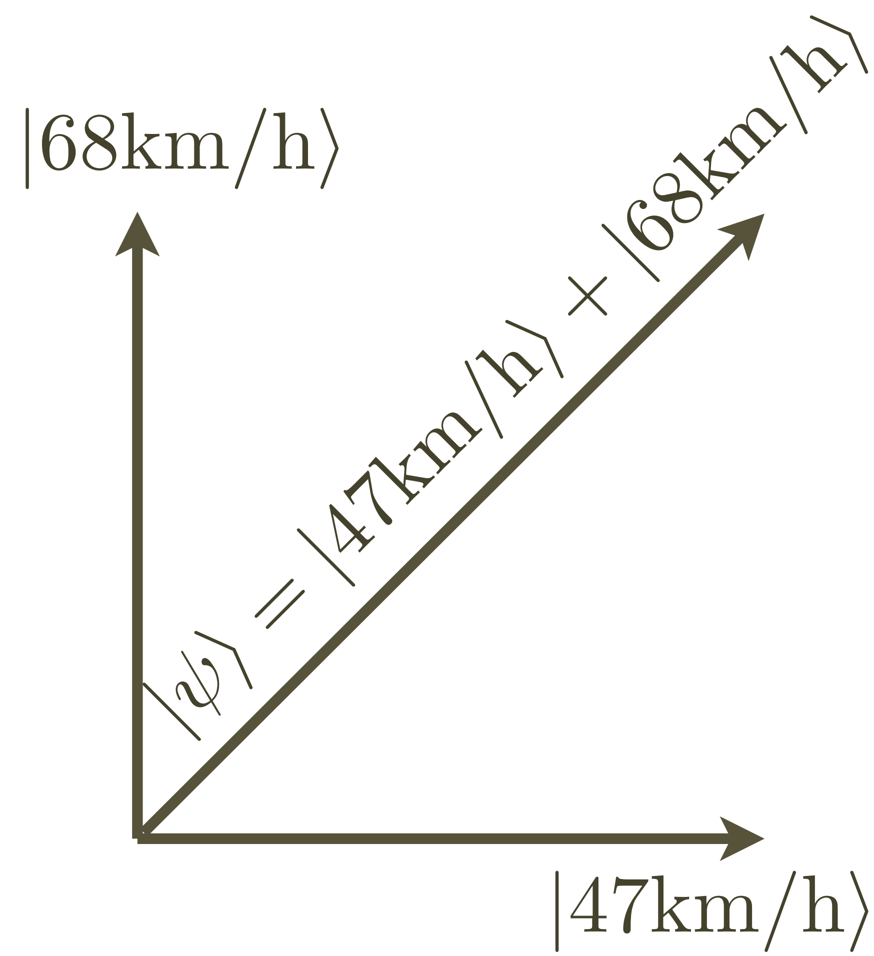
Loi quantique 2: **amplitudes**

- Si on note $\langle 47|\psi\rangle (= 1)$ le **produit scalaire** de 2 vecteurs, la longueur s'écrit
$$l_\psi = \sqrt{\langle\psi|\psi\rangle} (= \sqrt{2})$$



Loi quantique 2: **amplitudes**

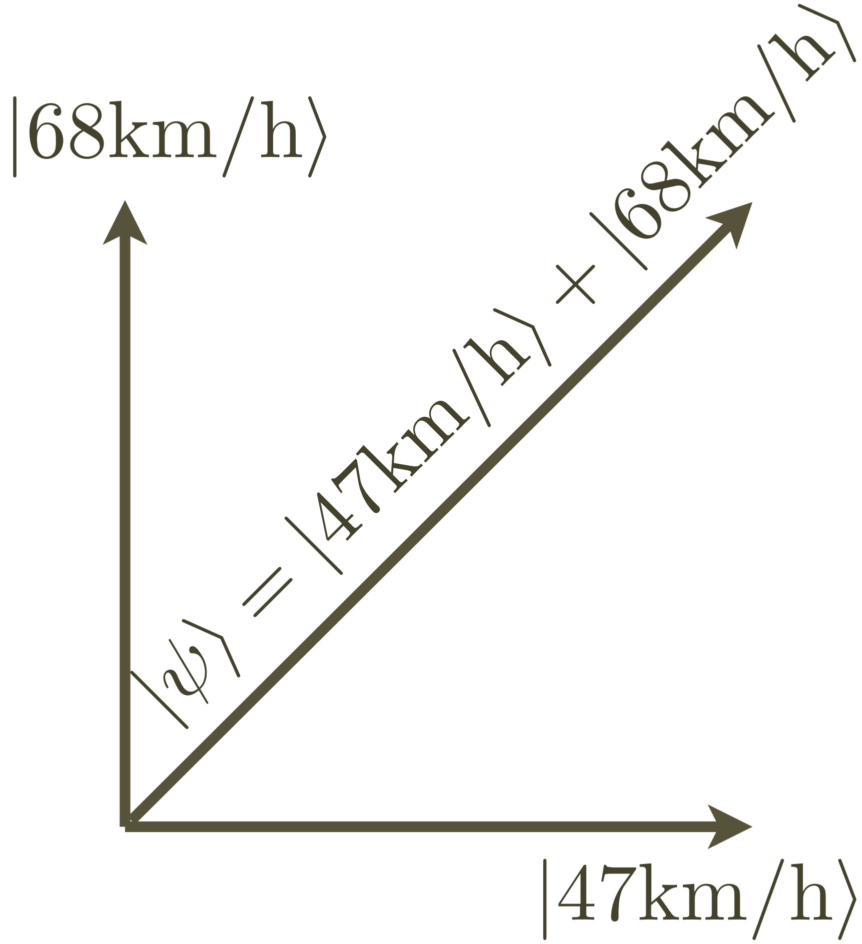
- Si on note $\langle 47|\psi\rangle(=1)$ le **produit scalaire** de 2 vecteurs, la longueur s′écrit
  $$l_\psi = \sqrt{\langle\psi|\psi\rangle}(=\sqrt{2})$$
- On définit l′**amplitude** de trouver 47 dans le vecteur ψ :



Loi quantique 2: **amplitudes**

- Si on note $\langle 47|\psi\rangle$ $(=1)$ le **produit scalaire** de 2 vecteurs, la longueur s'écrit
  $$l_\psi = \sqrt{\langle\psi|\psi\rangle}(=\sqrt{2})$$
- On définit l'**amplitude** de trouver 47 dans le vecteur ψ :

$$A(\psi \to 47) = \frac{\langle 47|\psi\rangle}{l_\psi l_{47}}$$
$$= \cos\theta_{\psi-47} (= 1/\sqrt{2})$$

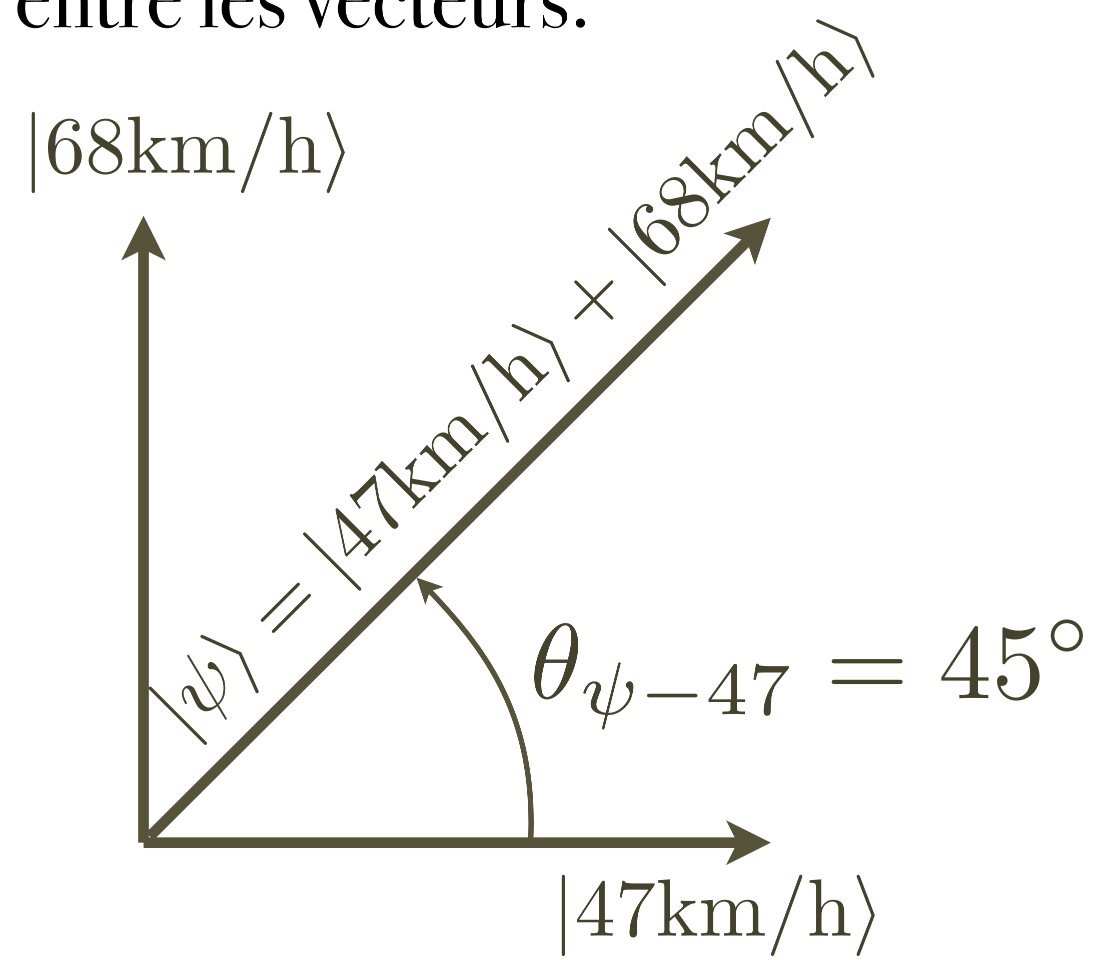


Loi quantique 2: **amplitudes**

- Si on note $\langle 47|\psi\rangle$ $(= 1)$ le **produit scalaire** de 2 vecteurs, la longueur s′écrit
  $$l_\psi = \sqrt{\langle\psi|\psi\rangle} (= \sqrt{2})$$
- On définit l′**amplitude** de trouver 47 dans le vecteur ψ :

$$A(\psi \to 47) = \frac{\langle 47|\psi\rangle}{l_\psi l_{47}}$$
$$= \cos\theta_{\psi-47} (= 1/\sqrt{2})$$

- Elle est fixée par **l′angle** entre les vecteurs:

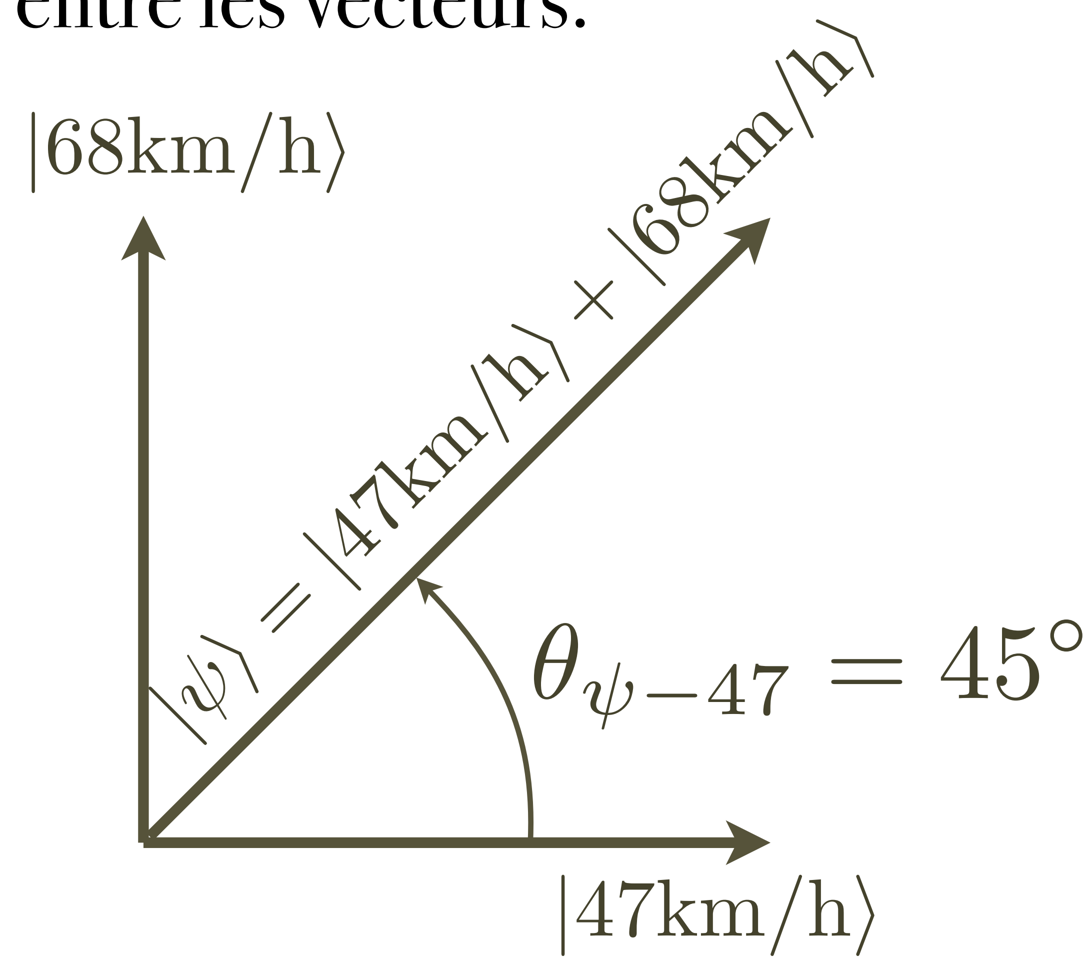


Loi quantique 2: **amplitudes**

- Si on note $\langle 47|\psi\rangle (= 1)$ le **produit scalaire** de 2 vecteurs, la longueur s′écrit
  $l_\psi = \sqrt{\langle\psi|\psi\rangle} (= \sqrt{2})$
- On définit l′**amplitude** de trouver 47 dans le vecteur ψ :

$$A(\psi \to 47) = \frac{\langle 47|\psi\rangle}{l_\psi l_{47}}$$
$$= \cos\theta_{\psi-47} (= 1/\sqrt{2})$$

- Elle est fixée par **l′angle** entre les vecteurs:



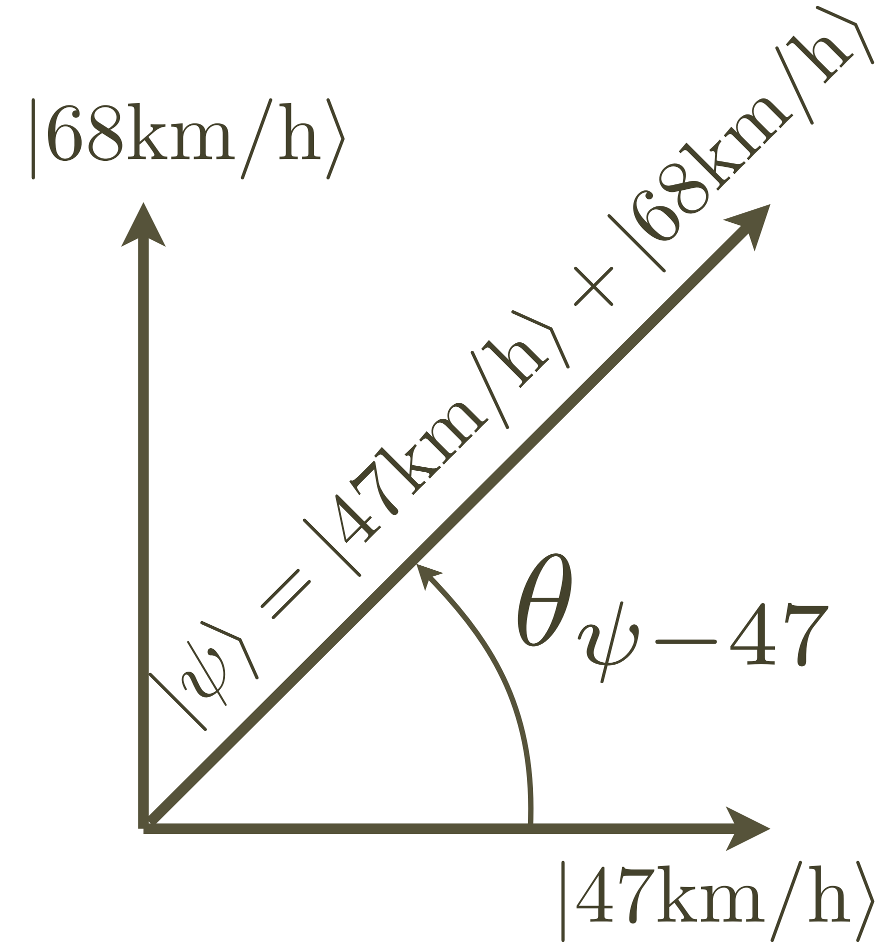
⇒ Deux états différents ($\theta \neq 0°$) ne sont **pas** “séparés” (sauf si $\theta = 90°$)

Loi quantique 2: **probabilités**

Loi quantique 2: **probabilités**

- La **probabilité** de trouver 47 dans un vecteur <u>superposition</u> ψ est le **carré de l'amplitude**:

$$P(\psi \to 47) = |A(\psi \to 47)|^2$$
$$= \cos^2\theta (= 1/2)$$



Loi quantique 2: **probabilités**

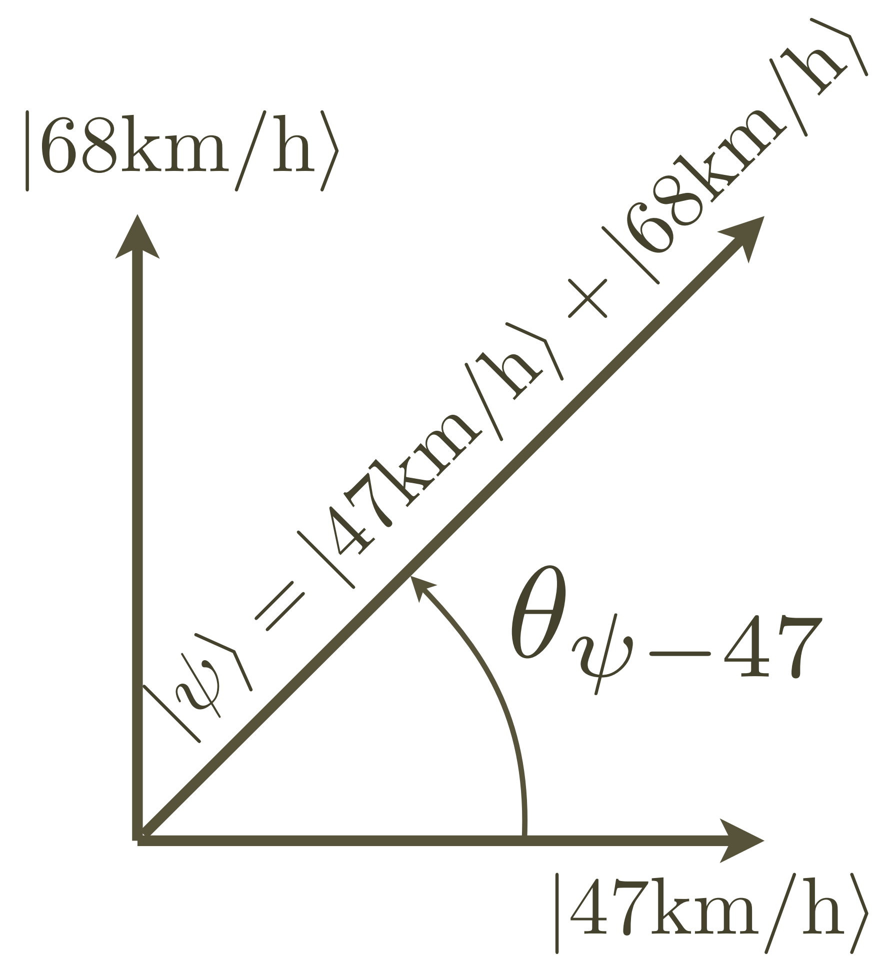
- La **probabilité** de trouver 47 dans un vecteur superposition ψ est le **carré de l'amplitude**:

$$P(\psi \to 47) = |A(\psi \to 47)|^2$$
$$= \cos^2\theta (= 1/2)$$

- La probabilité de trouver 68 est complémentaire:

$$P(\psi \to 68) = \sin^2\theta (= 1/2)$$

Dans notre exemple, on a 50-50% de trouver l'une ou l'autre vitesse



Loi quantique 2: **probabilités**

- La **probabilité** de trouver 47 dans un vecteur <u>superposition</u> ψ est le **carré de l'amplitude**:

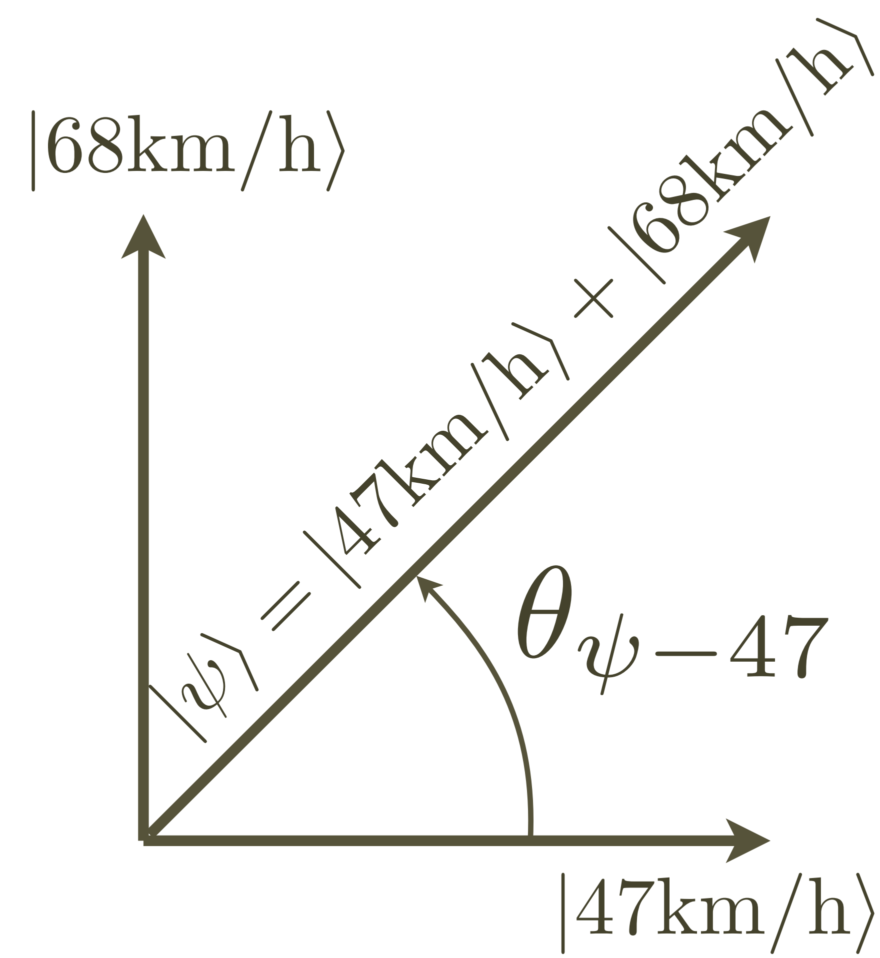
  $$P(\psi \to 47) = |A(\psi \to 47)|^2$$
  $$= \cos^2\theta (= 1/2)$$

- La probabilité de trouver 68 est complémentaire:

  $$P(\psi \to 68) = \sin^2\theta (= 1/2)$$

  Dans notre exemple, on a 50-50% de trouver l'une ou l'autre vitesse

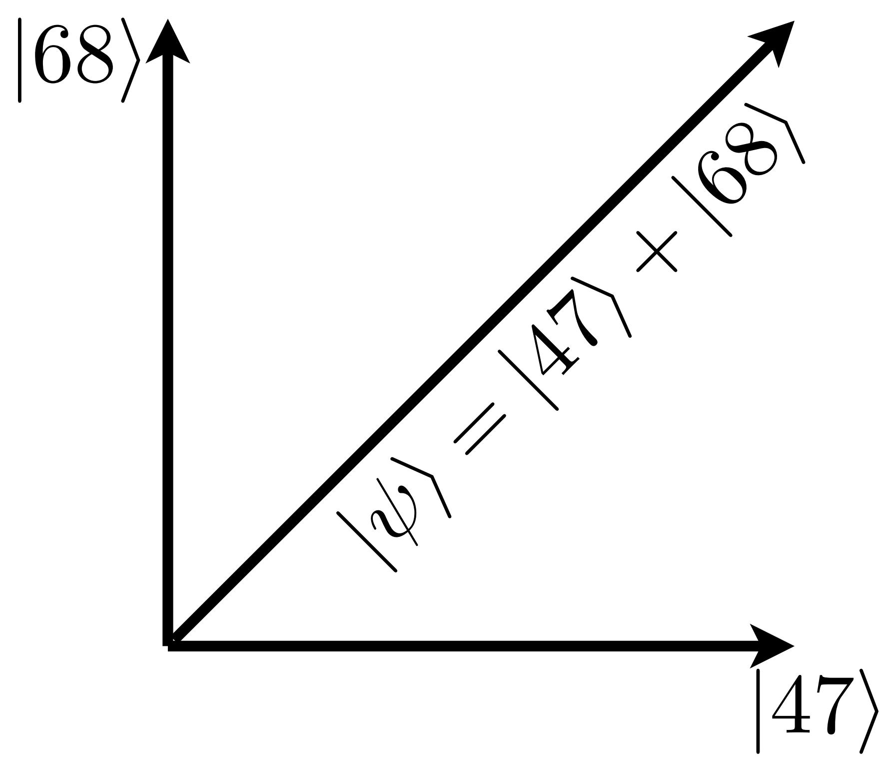
- La vitesse moyenne varie continument avec θ , p.ex: $47\cos^2\theta + 68\sin^2\theta$ (= 57,5)



Loi quantique 3:
grandeurs physiques

Loi quantique 3: **grandeurs physiques**

- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.

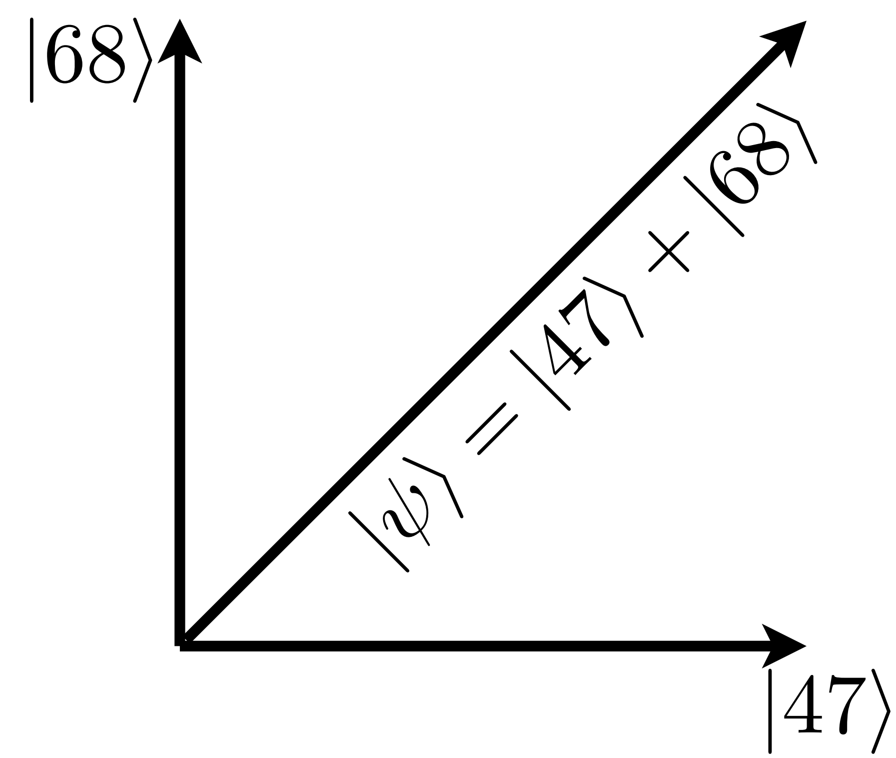


Loi quantique 3: **grandeurs physiques**

- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.

- À la **vitesse V** correspond l′opérateur-matrice

$$V = \begin{pmatrix} 47 & 0 \\ 0 & 68 \end{pmatrix}$$

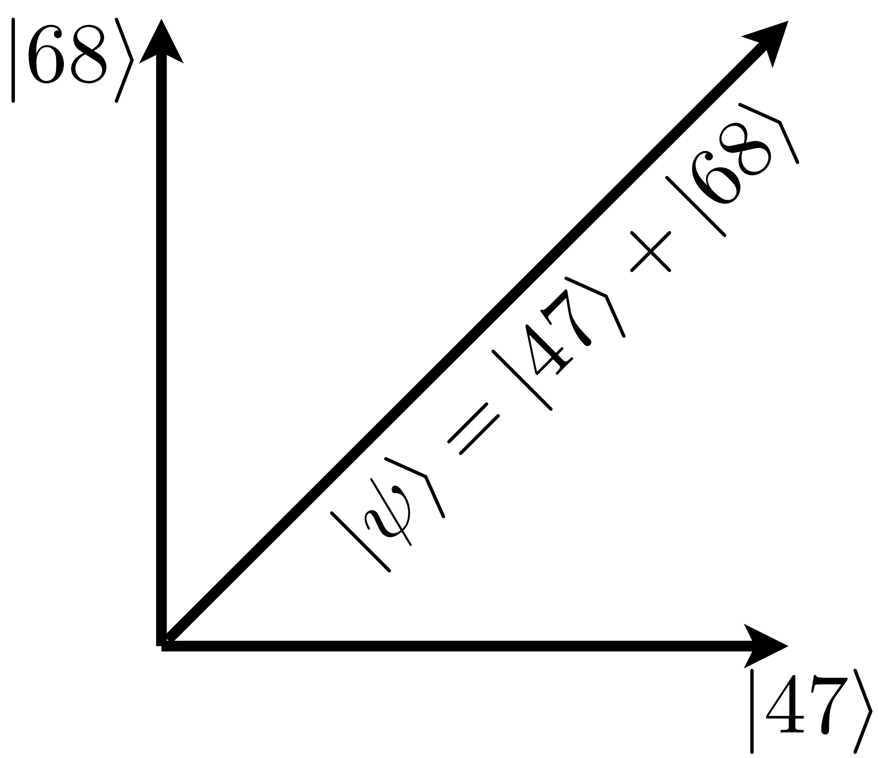


Loi quantique 3: **grandeurs physiques**

- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.
- À la **vitesse V** correspond l′opérateur-matrice

$$V = \begin{pmatrix} 47 & 0 \\ 0 & 68 \end{pmatrix}$$

- Il multiplie chaque vecteur (**propre**) par sa vitesse (**valeur propre**).

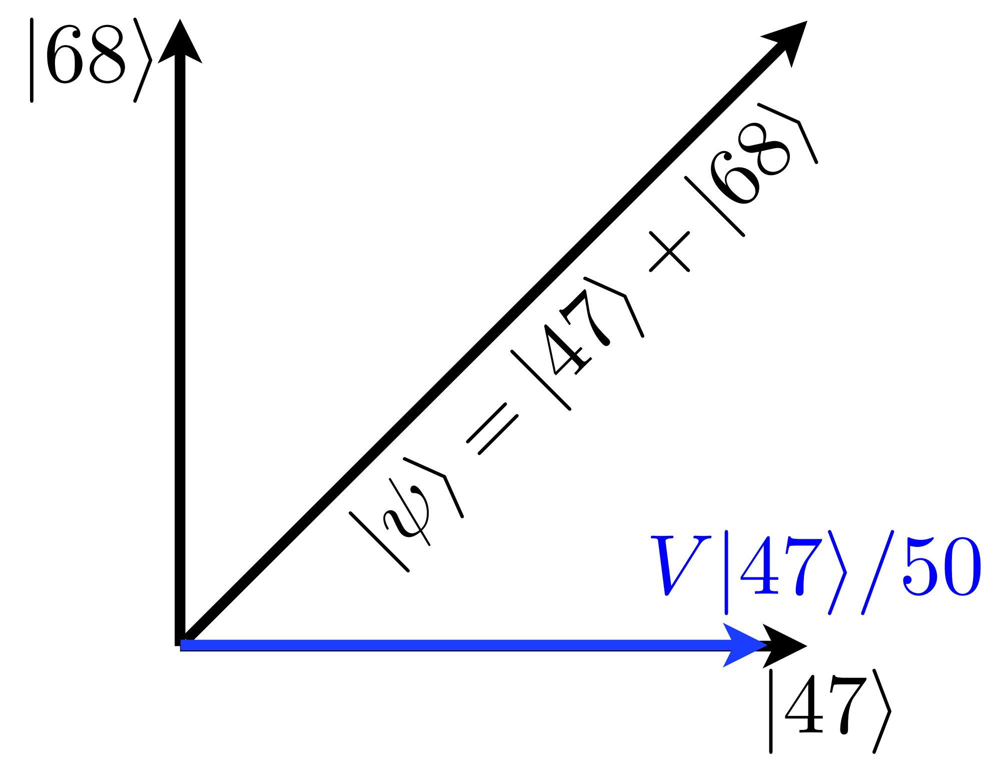


Loi quantique 3: **grandeurs physiques**

- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.
- À la **vitesse V** correspond l′opérateur-matrice

$$V = \begin{pmatrix} 47 & 0 \\ 0 & 68 \end{pmatrix}$$

- Il multiplie chaque vecteur (**propre**) par sa vitesse (**valeur propre**).

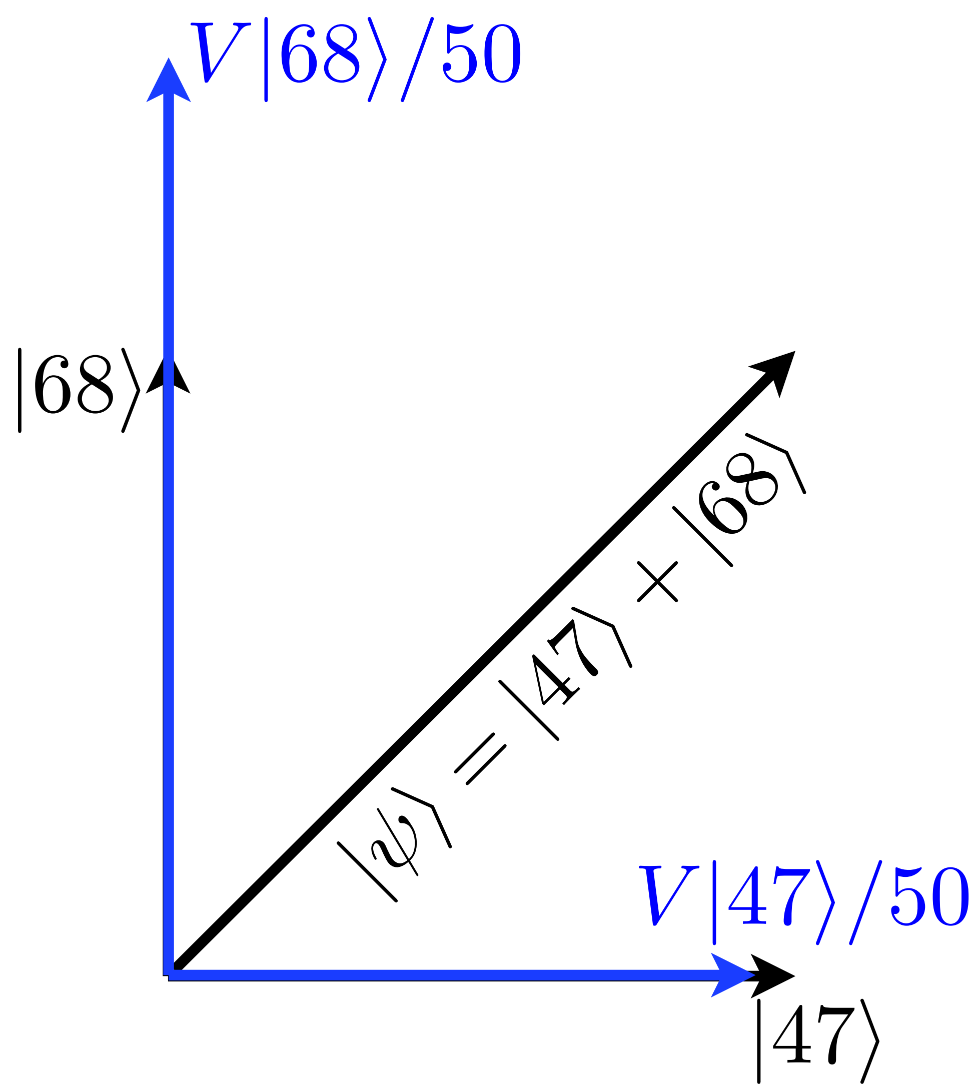


Loi quantique 3: **grandeurs physiques**

- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.
- À la **vitesse V** correspond l′opérateur-matrice

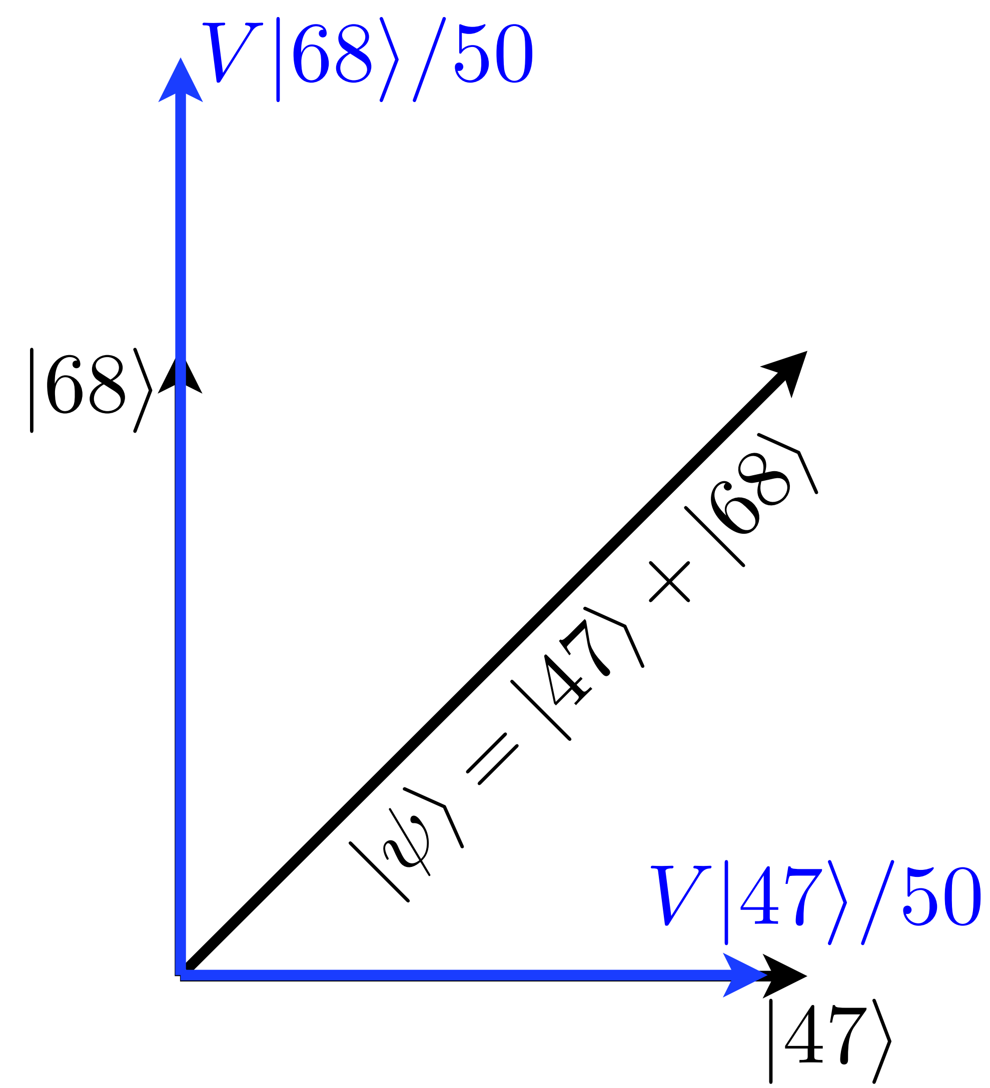
$$V = \begin{pmatrix} 47 & 0 \\ 0 & 68 \end{pmatrix}$$

- Il multiplie chaque vecteur (**propre**) par sa vitesse (**valeur propre**).



Loi quantique 3: **grandeurs physiques**

- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.
- À la **vitesse V** correspond l'opérateur-matrice
$$V = \begin{pmatrix} 47 & 0 \\ 0 & 68 \end{pmatrix}$$
- Il multiplie chaque vecteur (**propre**) par sa vitesse (**valeur propre**).
- Pour les autres vecteurs (non-propres) l'action de V n'est pas multiplicative:

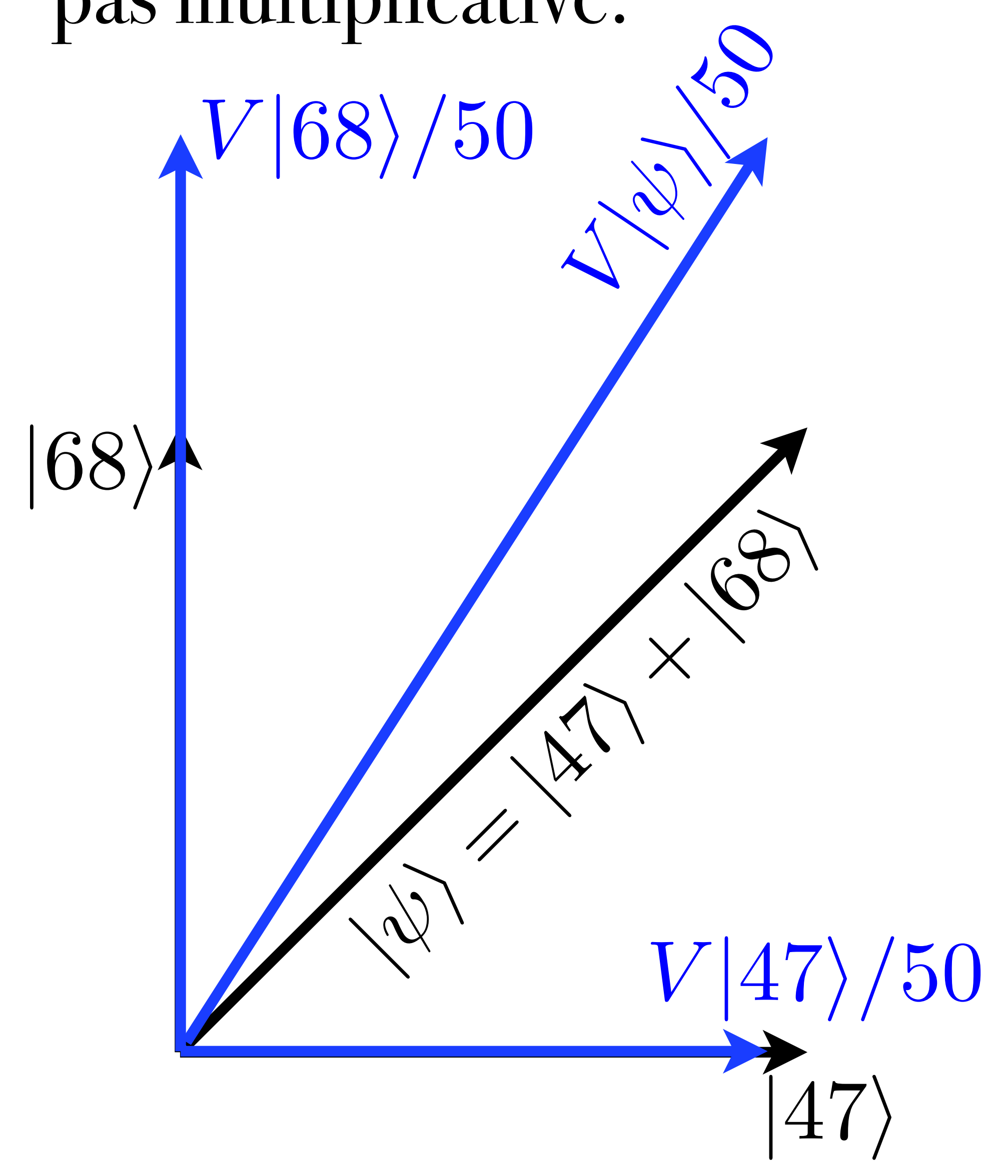


Loi quantique 3: **grandeurs physiques**

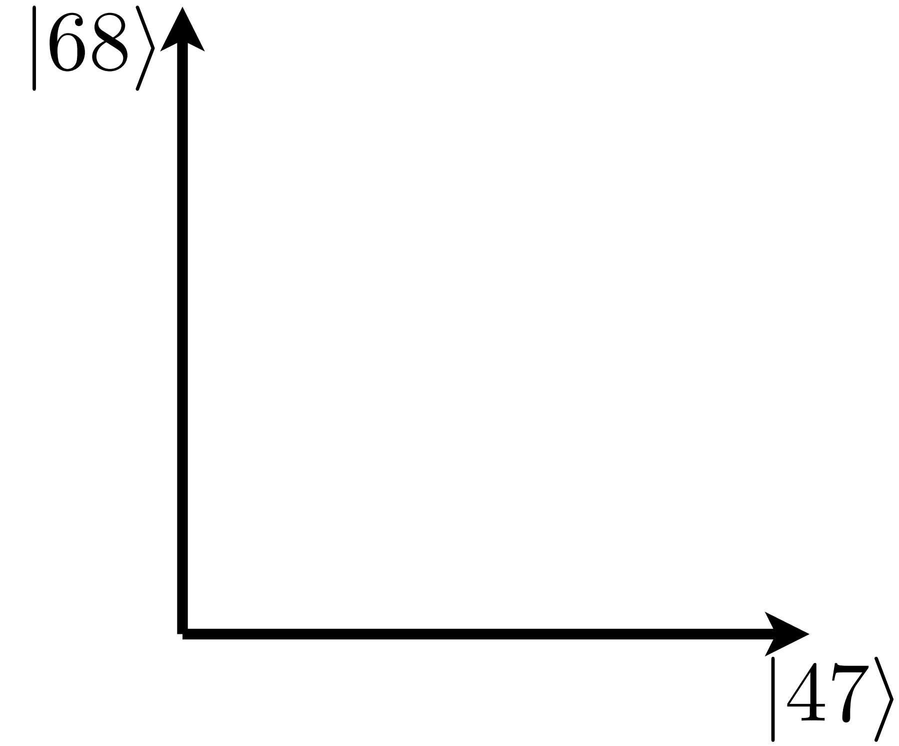
- À toute **grandeur physique** est associée un **opérateur** (matrice) agissant sur les vecteurs.
- À la **vitesse V** correspond l'opérateur-matrice

$$V = \begin{pmatrix} 47 & 0 \\ 0 & 68 \end{pmatrix}$$

- Il multiplie chaque vecteur (**propre**) par sa vitesse (**valeur propre**).
- Pour les autres vecteurs (non-propres) l'action de V n'est pas multiplicative:

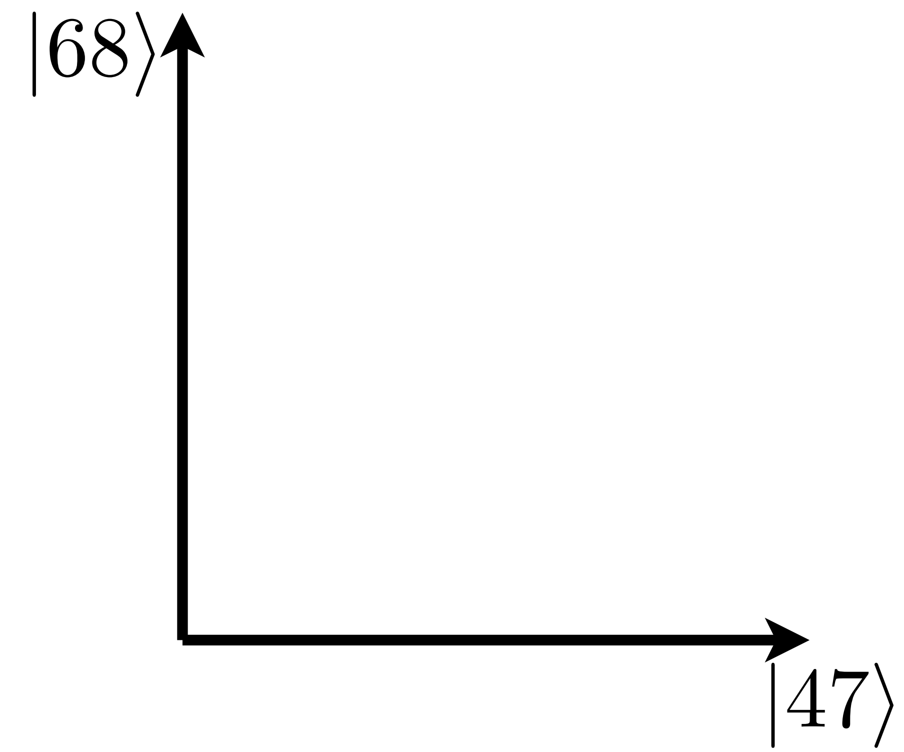


Grandeurs incompatibles



Grandeurs incompatibles

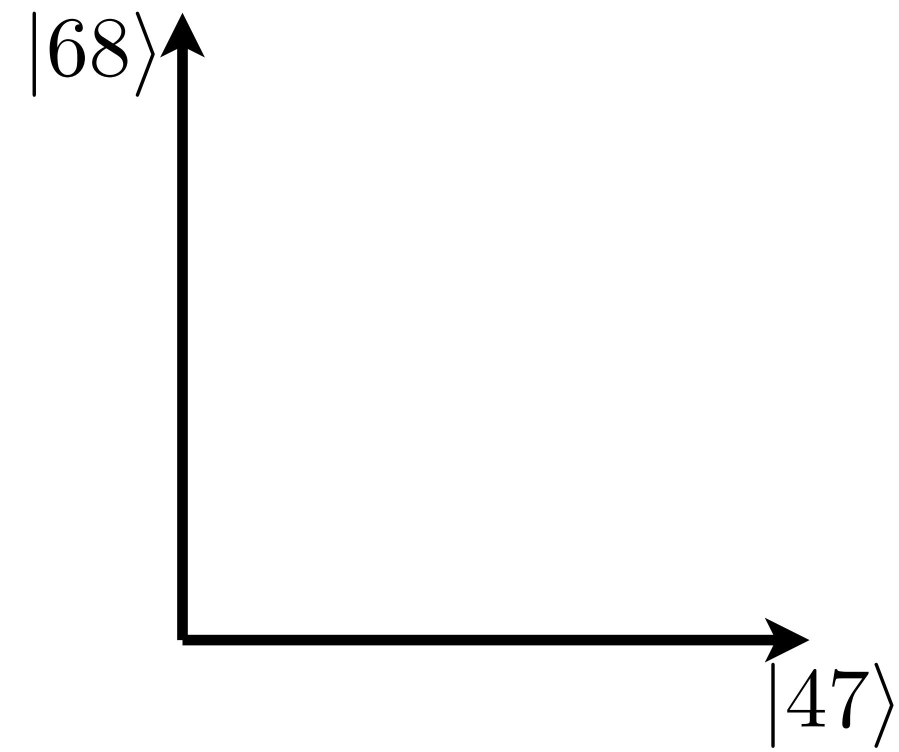
- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.



Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

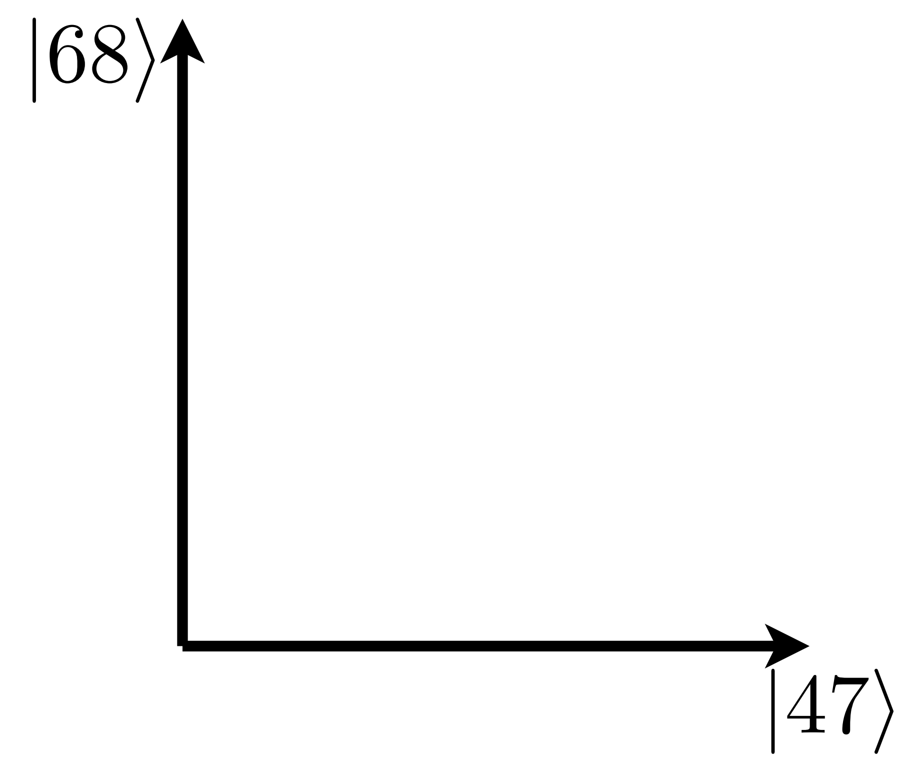


Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:



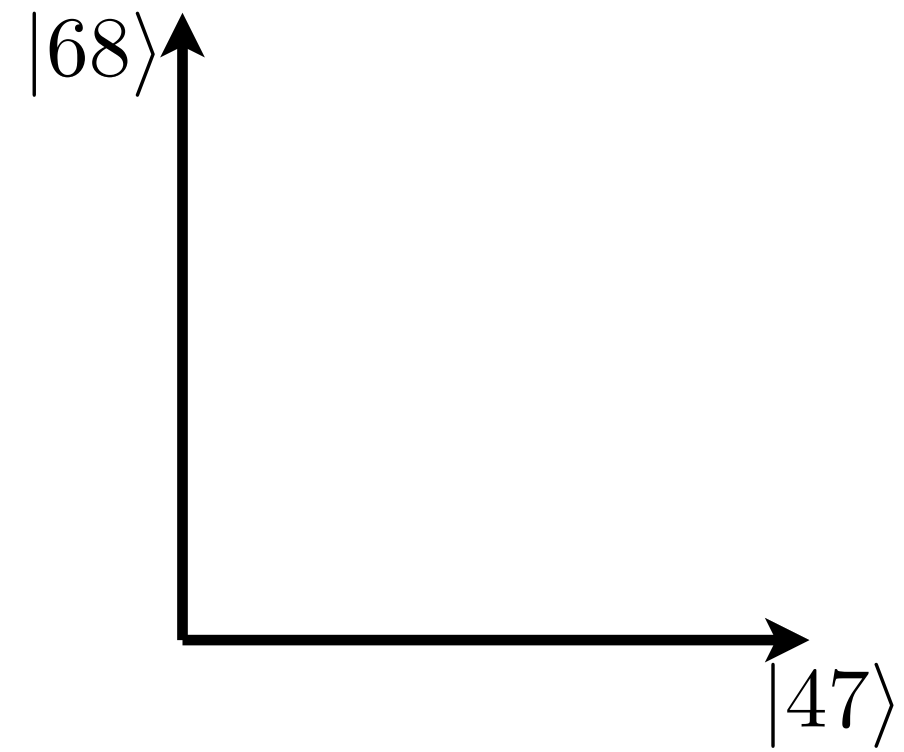
Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X = 2\rangle = |47\rangle + |68\rangle$$



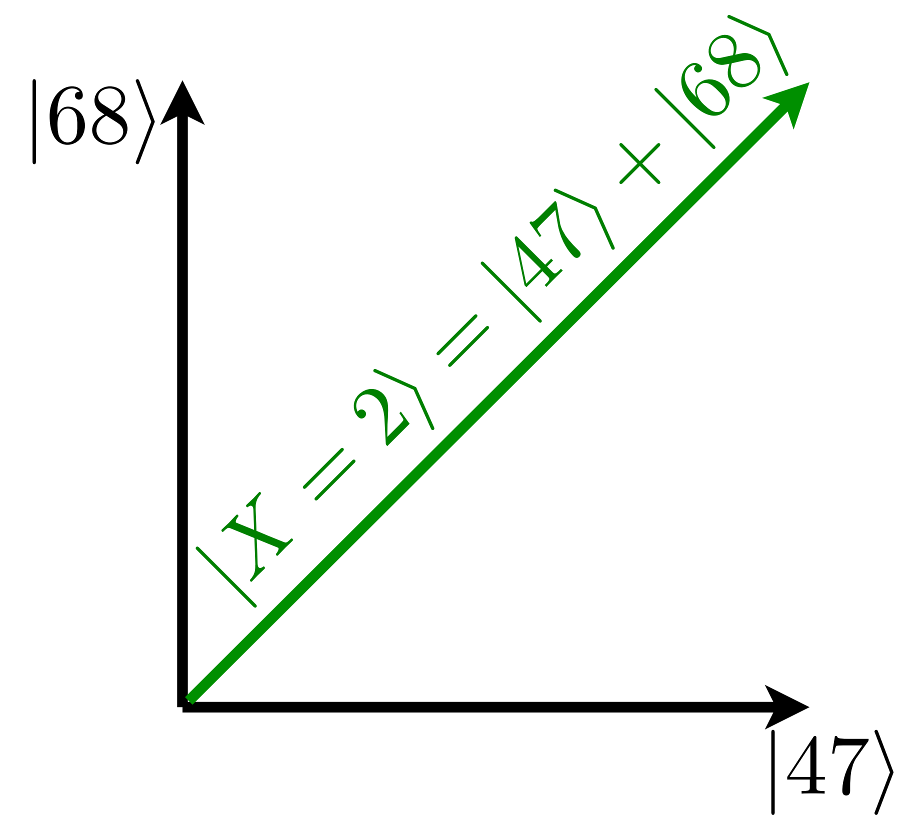
Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X=2\rangle = |47\rangle + |68\rangle$$



Grandeurs incompatibles

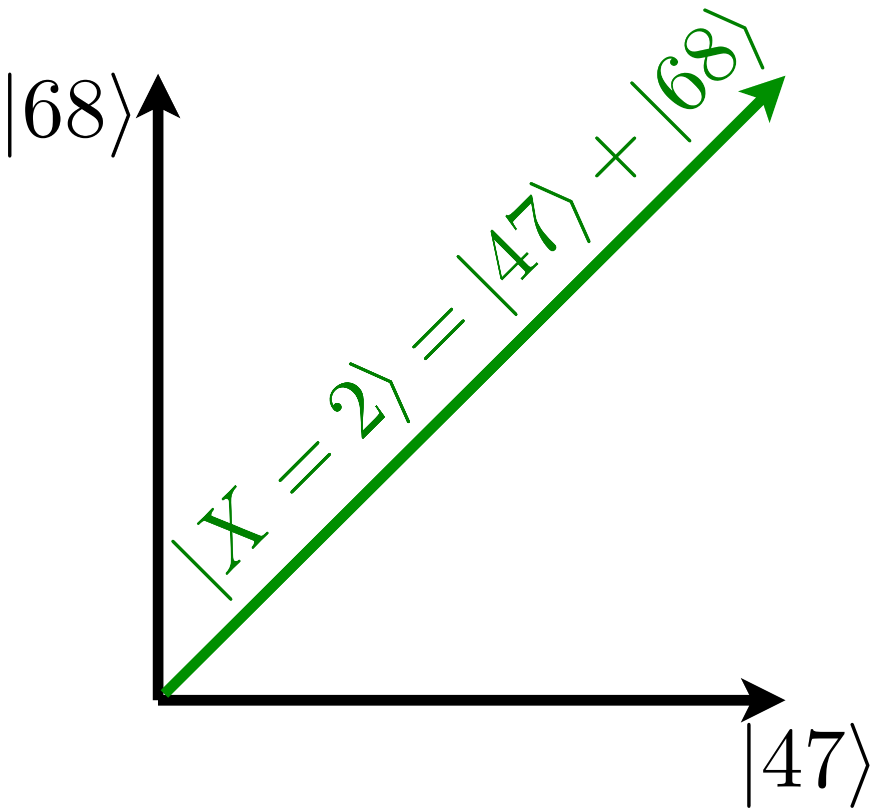
- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X=2\rangle = |47\rangle + |68\rangle$$

$$|X=0\rangle = -|47\rangle + |68\rangle$$



Grandeurs incompatibles

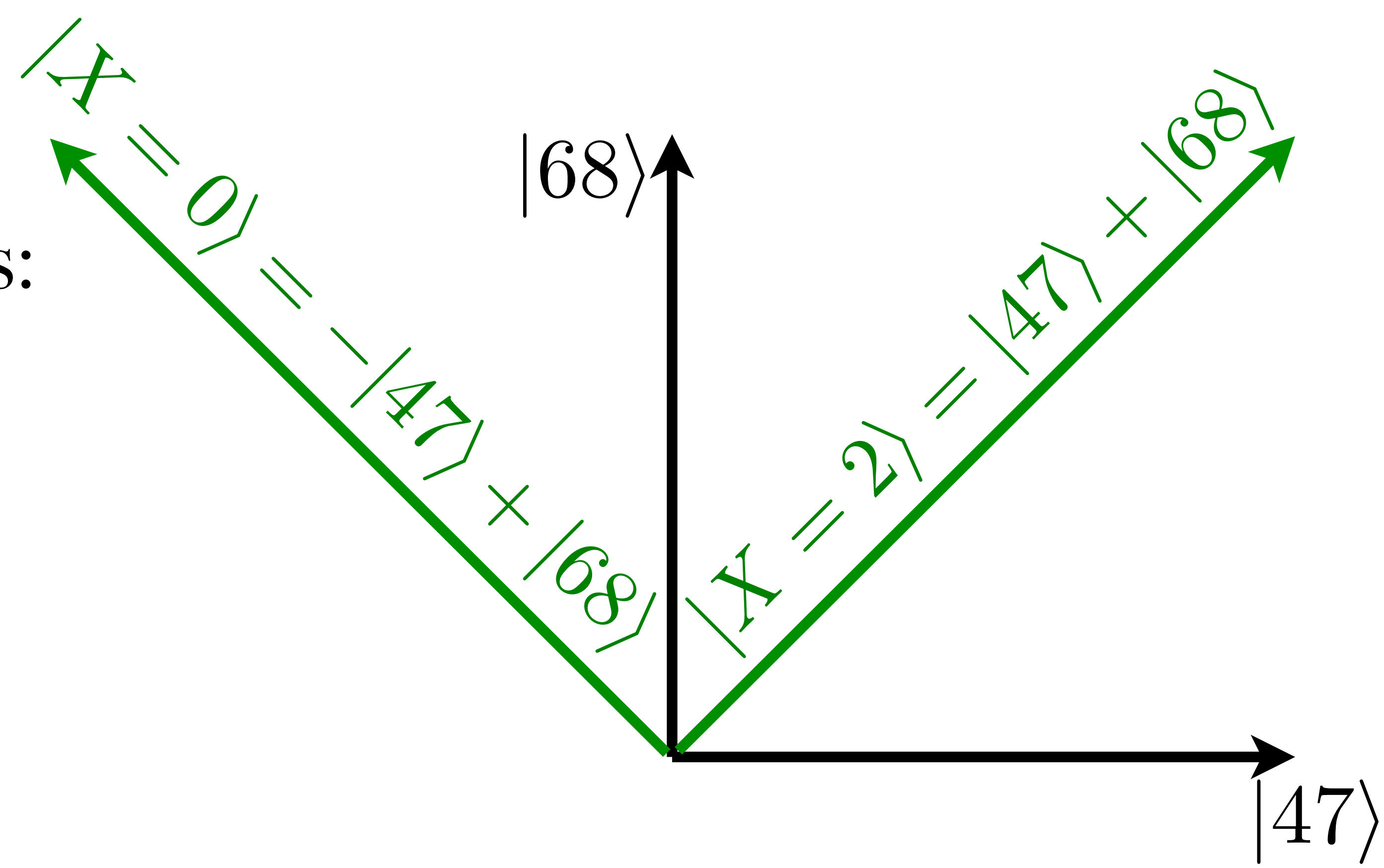
- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X=2\rangle = |47\rangle + |68\rangle$$

$$|X=0\rangle = -|47\rangle + |68\rangle$$



Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

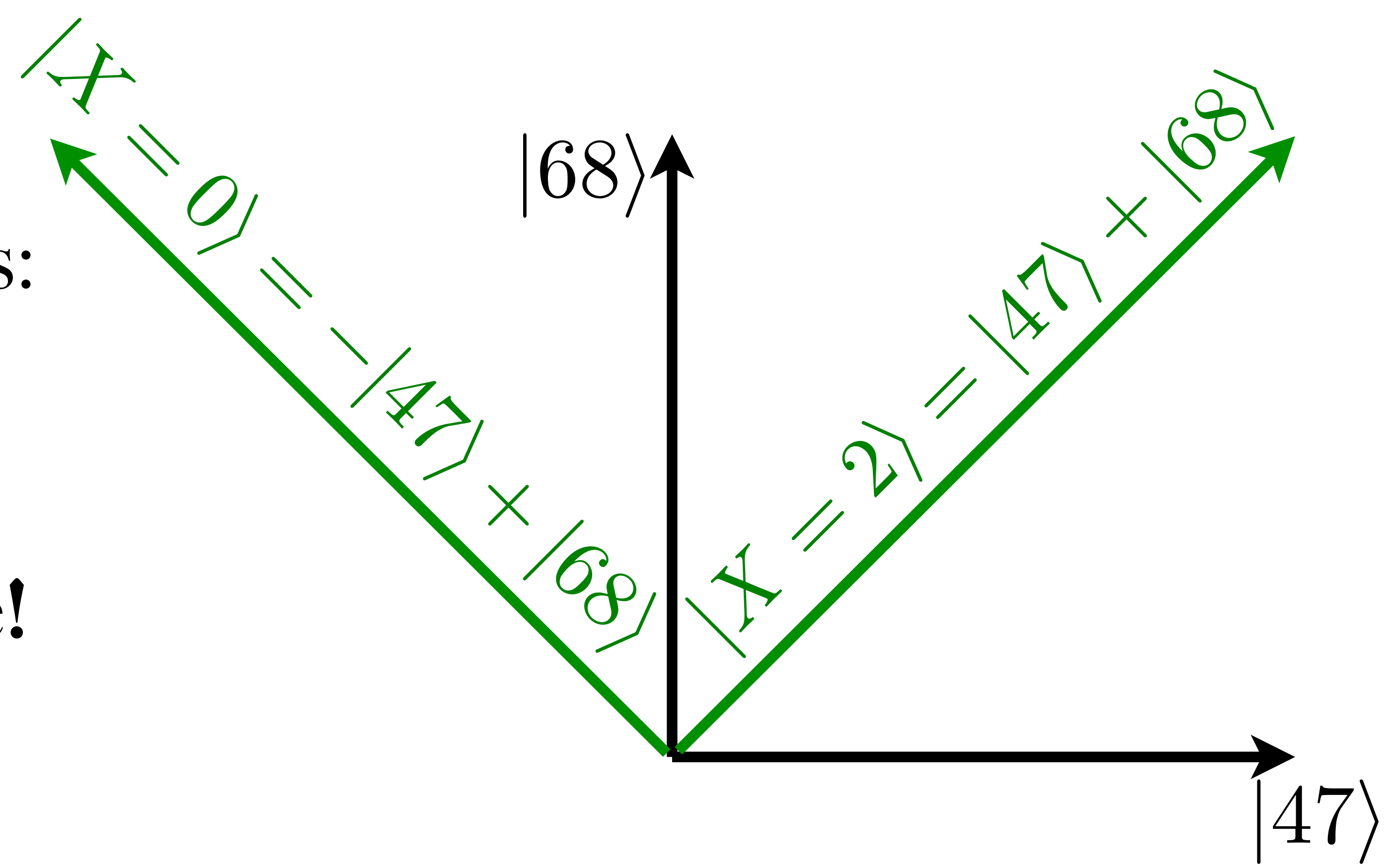
$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X=2\rangle = |47\rangle + |68\rangle$$

$$|X=0\rangle = -|47\rangle + |68\rangle$$

$\rightarrow$ **incertitude sur la vitesse!**



Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

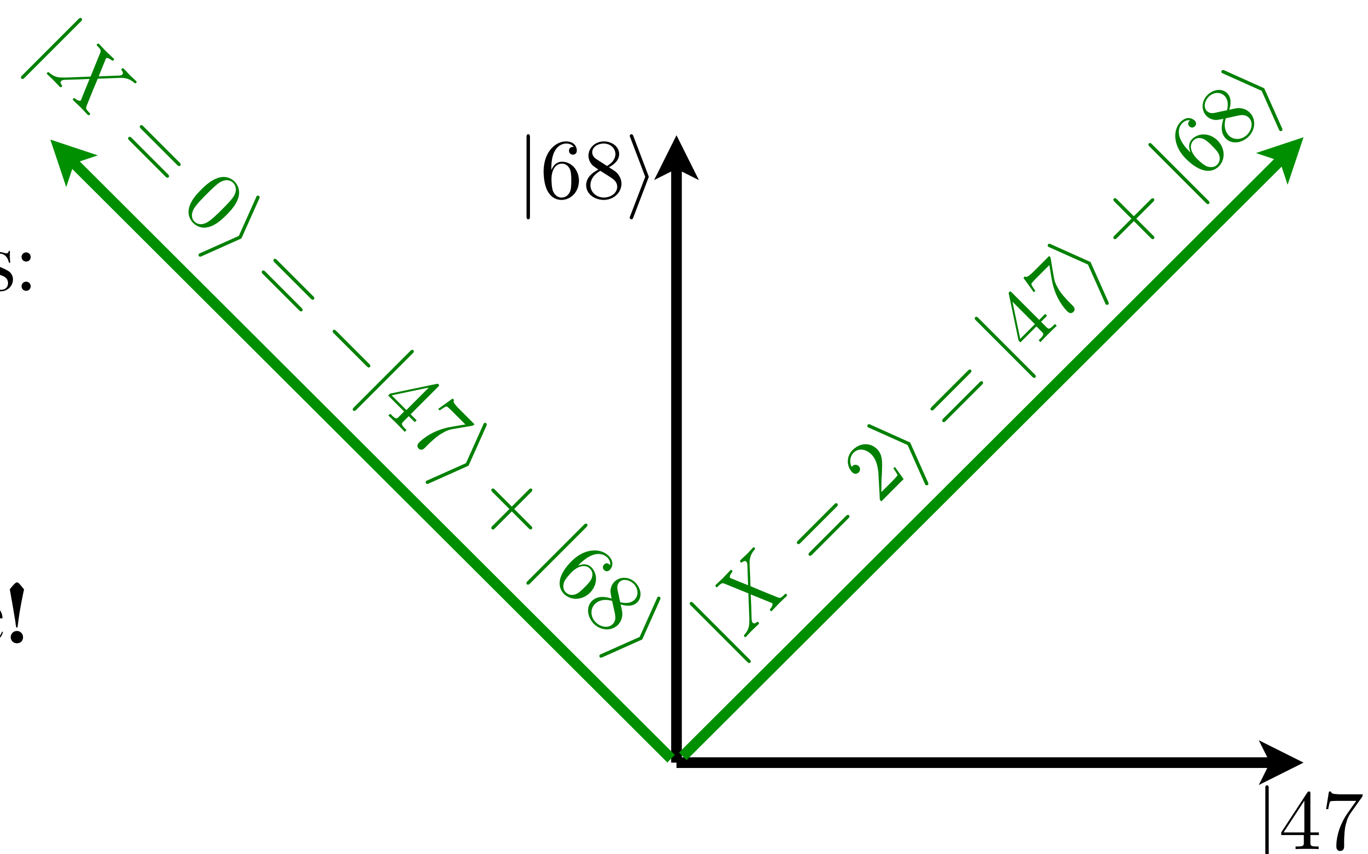
- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X = 2\rangle = |47\rangle + |68\rangle$$

$$|X = 0\rangle = -|47\rangle + |68\rangle$$

$\rightarrow$ **incertitude sur la vitesse!**

- Ce problème se produit chaque fois que
  $[X, V] = XV - VX \neq 0$



Grandeurs incompatibles

- À une autre grandeur comme la position X, correspond un autre opérateur-matrice, p.ex.

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

- Les états avec une position bien définie sont des états qui contiennent les 2 vitesses:

$$|X=2\rangle = |47\rangle + |68\rangle$$

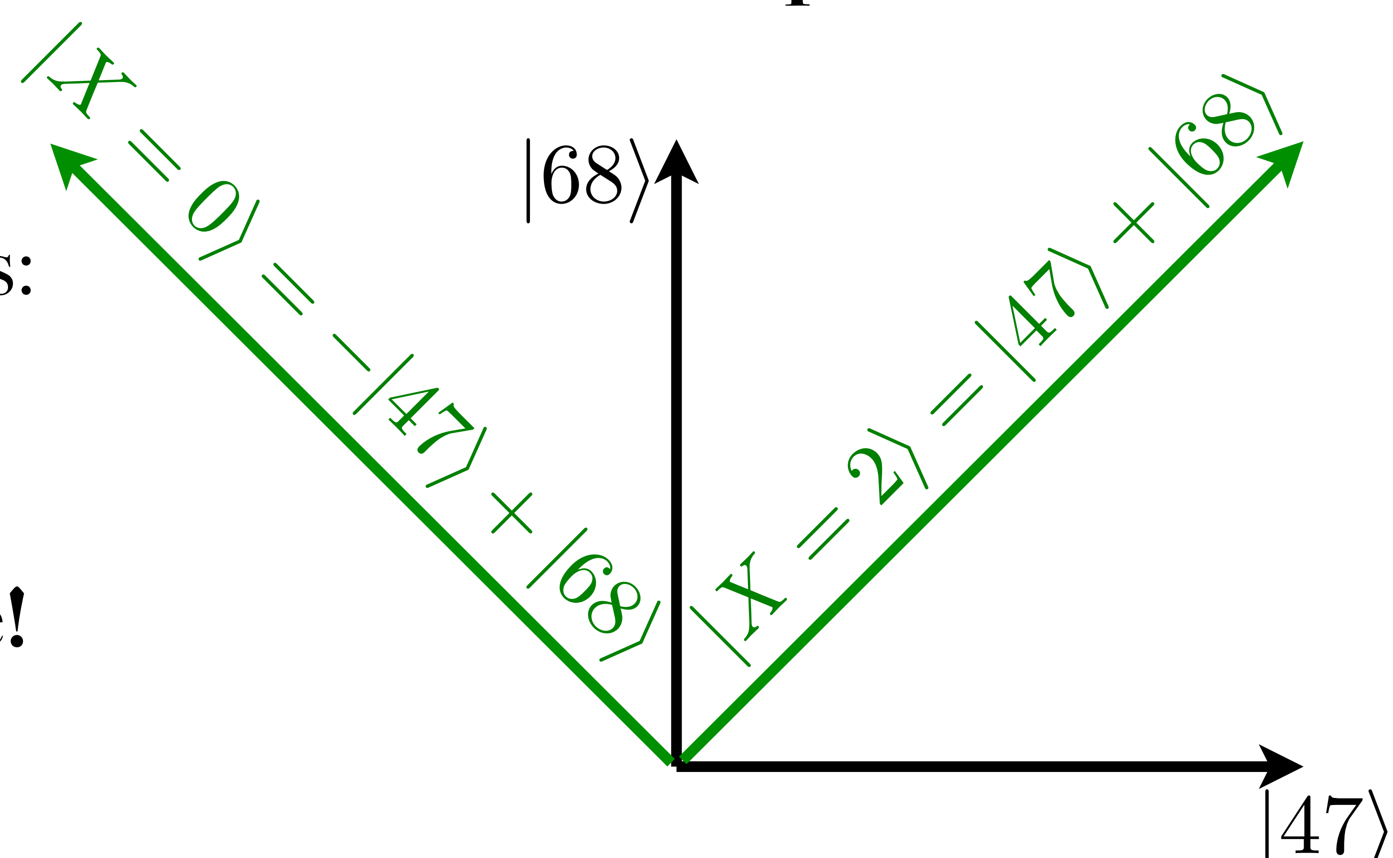
$$|X=0\rangle = -|47\rangle + |68\rangle$$

$\rightarrow$ **incertitude sur la vitesse!**

- Ce problème se produit chaque fois que

$$[X, V] = XV - VX \neq 0$$

- Les grandeurs X et V sont alors dites **incompatibles**



Loi quantique 4: **mesures (!!!)**

Loi quantique 4: **mesures (!!!)**

a) La mesure d′une grandeur V ne peut donner comme résultat qu′une des **valeurs propres** v de l'opérateur-matrice
→ discontinuités naturelles

Loi quantique 4: **mesures (!!!)**

a) La mesure d'une grandeur V ne peut donner comme résultat qu'une des **valeurs propres** v de l'opérateur-matrice
$\longrightarrow$ discontinuités naturelles

b) Connaissant **complètement** l'état $|\psi\rangle$ du système, **on ne peut prédire que (!!) la probabilité** de trouver la valeur v :
$P(\psi \rightarrow v) = |\langle v | \psi \rangle|^2$
$= 50\%$ pour $v=47$ ou 68

Loi quantique 4: **mesures (!!!)**

a) La mesure d'une grandeur V ne peut donner comme résultat qu'une des **valeurs propres** v de l'opérateur-matrice
$\rightarrow$ discontinuités naturelles

b) Connaissant **complètement** l'état $|\psi\rangle$ du système, **on ne peut prédire que (!!) la probabilité** de trouver la valeur v :
$P(\psi \rightarrow v) = |\langle v|\psi\rangle|^2$
$= 50\%$ pour $v=47$ ou 68

Déterminisme?

Loi quantique 4: **mesures (!!!)**

a) La mesure d'une grandeur V ne peut donner comme résultat qu'une des **valeurs propres** v de l'opérateur-matrice
→ discontinuités naturelles

b) Connaissant **complètement** l'état $|\psi\rangle$ du système, **on ne peut prédire que (!!) la probabilité** de trouver la valeur v :
$P(\psi \to v) = |\langle v|\psi\rangle|^2$
$= 50\%$ pour v=47 ou 68

Déterminisme?

c) L'état du système passe **instantanément** de $|\psi\rangle$ avant → $|v\rangle$ après la mesure.
L'état final dépend donc du résultat (aléatoire!) v de la mesure !!!!

Loi quantique 4: **mesures (!!!)**

a) La mesure d'une grandeur V ne peut donner comme résultat qu'une des **valeurs propres** v de l'opérateur-matrice
→ discontinuités naturelles

b) Connaissant **complètement** l'état $|\psi\rangle$ du système, **on ne peut prédire que (!!) la probabilité** de trouver la valeur v :
$P(\psi \to v) = |\langle v|\psi\rangle|^2$
$= 50\%$ pour v=47 ou 68

Déterminisme?

c) L'état du système passe **instantanément** de $|\psi\rangle$ avant → $|v\rangle$ après la mesure.
L'état final dépend donc du résultat (aléatoire!) v de la mesure !!!!

G.: c'est donc bien moi qui, par ma mesure, vous ai poussé hors la loi… et vous y ai laissé par la suite!

Loi quantique 4: **mesures (!!!)**

a) La mesure d′une grandeur V ne peut donner comme résultat qu′une des **valeurs propres** v de l'opérateur-matrice
→ discontinuités naturelles

b) Connaissant **complètement** l′état $|\psi\rangle$ du système, **on ne peut prédire que (!!) la probabilité** de trouver la valeur v :
$P(\psi \rightarrow v) = |\langle v|\psi\rangle|^2$
= 50% pour v=47 ou 68

Déterminisme?

c) L′état du système passe **instantanément** de $|\psi\rangle$ avant → $|v\rangle$ après la mesure.
L′état final dépend donc du résultat (aléatoire!) v de la mesure !!!!

G.: c′est donc bien moi qui, par ma mesure, vous ai poussé hors la loi… et vous y ai laissé par la suite!

C.Q.: d′autant plus que pour l′évolution temporelle…

Loi quantique 5:
évolution dans le temps

Loi quantique 5: **évolution dans le temps**

L'évolution au cours du temps d'un vecteur d'état $|\psi(t)\rangle$ est dictée par **l'équation de Schrödinger :**

$$i\hbar\, \partial_t |\psi(t)\rangle = H\,|\psi(t)\rangle$$

où l'opérateur H correspond à l'énergie E du système; et $\hbar$=1.05 10^{-34} J.s

est la constante de Planck.

Loi quantique 5:
évolution dans le temps

L′évolution au cours du temps d′un vecteur d′état $|\psi(t)\rangle$ est dictée par **l′équation de Schrödinger :**

$$i\hbar\,\partial_t|\psi(t)\rangle = H\,|\psi(t)\rangle$$

où l′opérateur H correspond à l′énergie E du système; et $\hbar$=1.05 10^{-34} J.s

est la constante de Planck.

‣Rem. 1: Les amplitudes sont en fait complexes

Loi quantique 5:
évolution dans le temps

L'évolution au cours du temps d'un vecteur d'état $|\psi(t)\rangle$ est dictée par **l'équation de Schrödinger :**

$$i\hbar\, \partial_t |\psi(t)\rangle = H\,|\psi(t)\rangle$$

où l'opérateur H correspond à l'énergie E du système;
et $\hbar = 1.05\ 10^{-34}$ J.s

est la constante de Planck.

‣ Rem. 1: Les amplitudes sont en fait complexes

‣ Rem. 2: si l'énergie $H = H(v)$ est fixée par la seule vitesse,

$$|68(t)\rangle = e^{-\frac{i}{\hbar}E_{68}t}|68(0)\rangle$$

décrit toujours le même état.

Loi quantique 5: **évolution dans le temps**

L′évolution au cours du temps d′un vecteur d′état $|\psi(t)\rangle$ est dictée par **l′équation de Schrödinger :**

$$i\hbar\,\partial_t|\psi(t)\rangle = H\,|\psi(t)\rangle$$

où l′opérateur H correspond à l′énergie E du système; et $\hbar$=1.05 10^{-34} J.s

est la constante de Planck.

‣Rem.1: Les amplitudes sont en fait complexes

‣Rem.2: si l′énergie H=$H(v)$ est fixée par la seule vitesse,

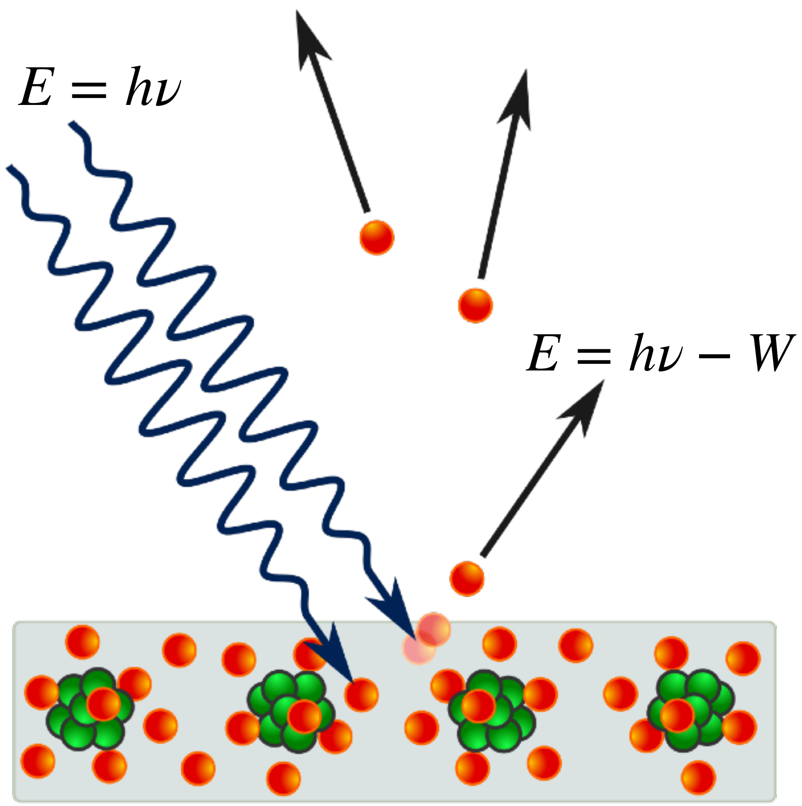
$$|68(t)\rangle = e^{-\frac{i}{\hbar}E_{68}t}|68(0)\rangle$$

décrit toujours le même état.

‣Rem.3: ceci décrit l′évolution d′un système isolé (coffre-fort); en plus, il peut y avoir une évolution discontinue par des mesures.

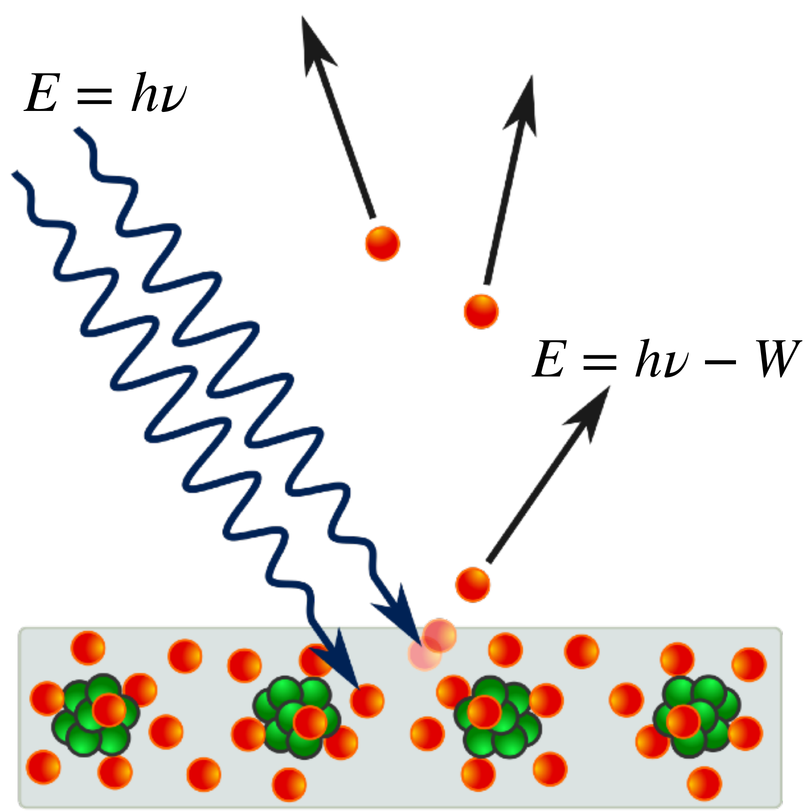
Photons et polarisation

Effet photo-électrique et photons



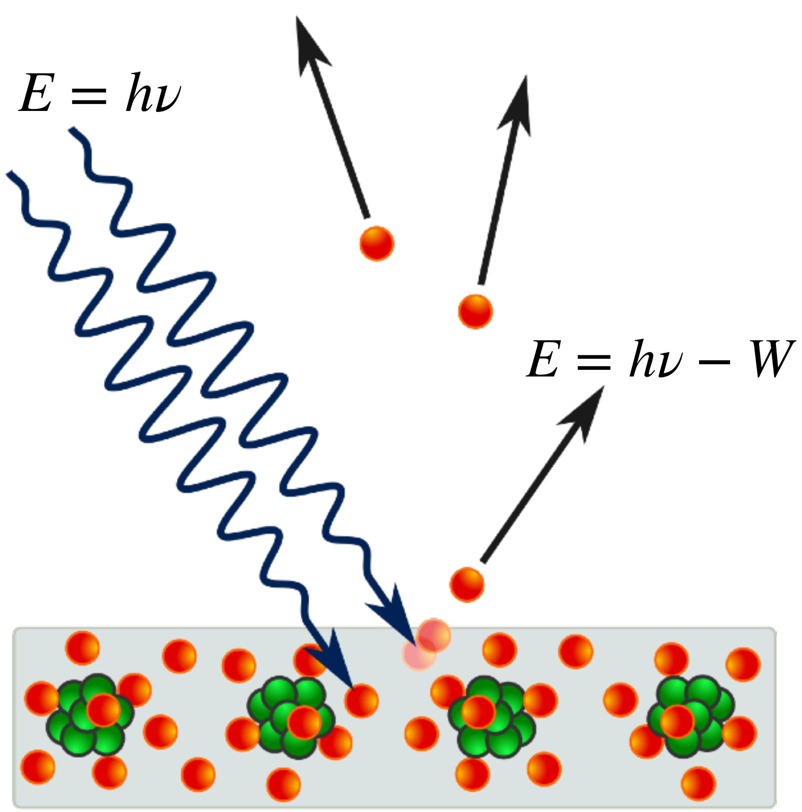
Effet photo-électrique et photons

- Dans panneaux solaires, lumière captée comme des **photons** = grains d'énergie $E = h\nu$ éjectant chacun un électron (Einstein, 1905)



Effet photo-électrique et photons

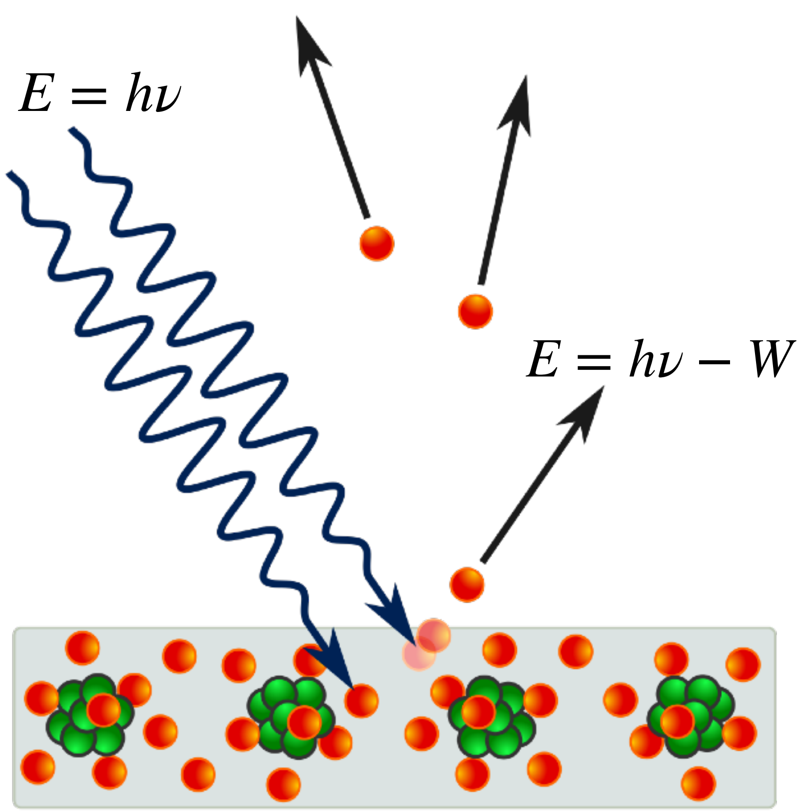
- Dans panneaux solaires, lumière captée comme des **photons** = grains d'énergie $E = h\nu$ éjectant chacun un électron (Einstein, 1905)



- On détecte toujours un **photon entier** ici **ou** là, jamais 1/2 photon ici **et** 1/2 là

Effet photo-électrique et photons

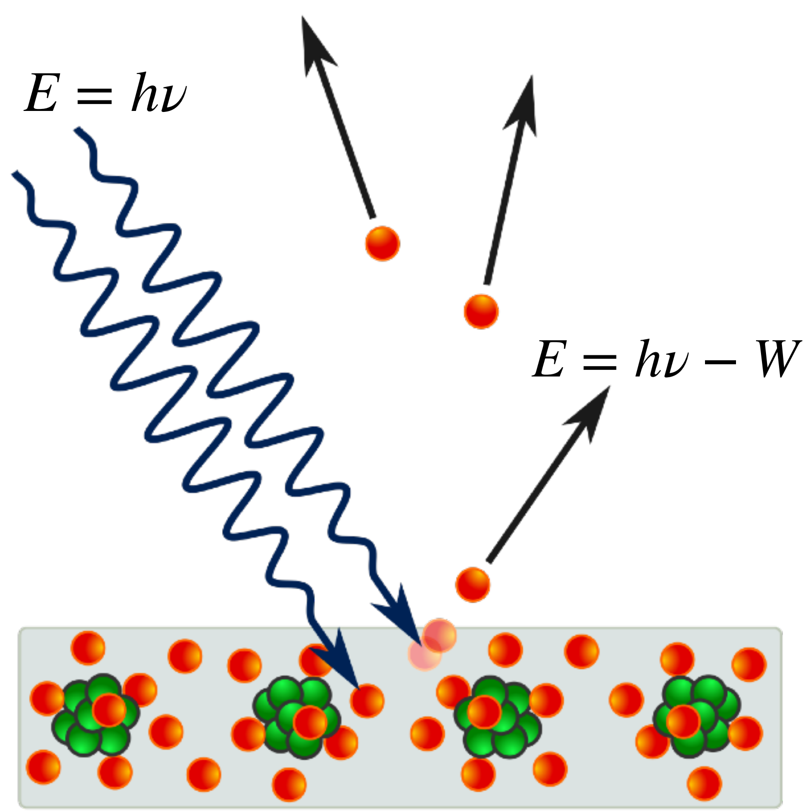
- Dans panneaux solaires, lumière captée comme des **photons** = grains d'énergie $E = h\nu$ éjectant chacun un électron (Einstein, 1905)



- On détecte toujours un **photon entier** ici **ou** là, jamais 1/2 photon ici **et** 1/2 là
- Lieu exact est imprévisible ($\Leftrightarrow$ quel électron?); **probabilité** plus élevée là où forte intensité lumineuse.

Effet photo-électrique et photons

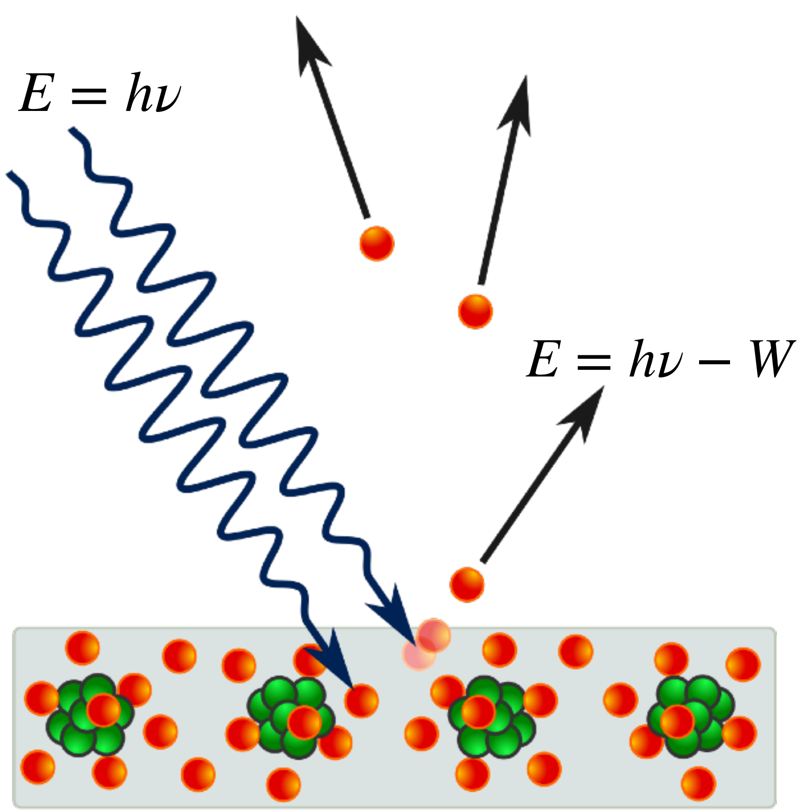
- Dans panneaux solaires, lumière captée comme des **photons** = grains d'énergie $E = h\nu$ éjectant chacun un électron (Einstein, 1905)



- On détecte toujours un **photon entier** ici **ou** là, jamais 1/2 photon ici **et** 1/2 là
- Lieu exact est imprévisible (⇔ quel électron?); **probabilité** plus élevée là où forte intensité lumineuse.
- Faisceau divergent: intensité (et probabilité) se dilue. Détecter ici empêche de détecter ailleurs? (à l'autre bout de l'univers???)

Effet photo-électrique et photons

- Dans panneaux solaires, lumière captée comme des **photons** = grains d'énergie $E = h\nu$ éjectant chacun un électron (Einstein, 1905)

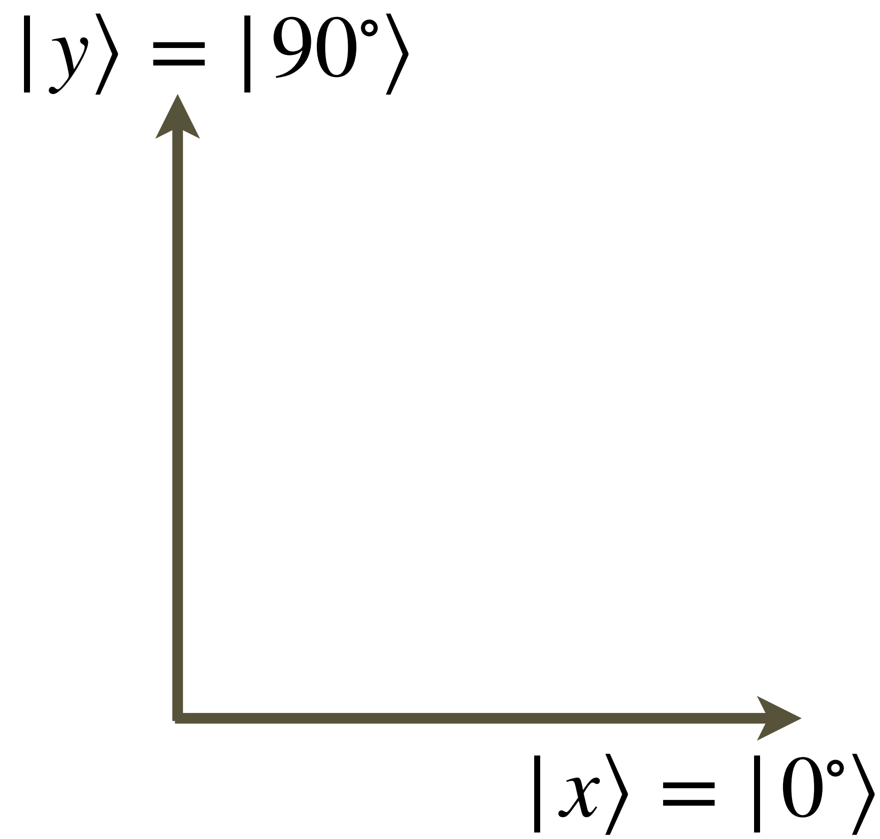


- On détecte toujours un **photon entier** ici **ou** là, jamais 1/2 photon ici **et** 1/2 là
- Lieu exact est imprévisible (⇔ quel électron?); **probabilité** plus élevée là où forte intensité lumineuse.
- Faisceau divergent: intensité (et probabilité) se dilue. Détecter ici empêche de détecter ailleurs? (à l'autre bout de l'univers???)
- Copenhague répond oui!

États de polarisation d'un photon

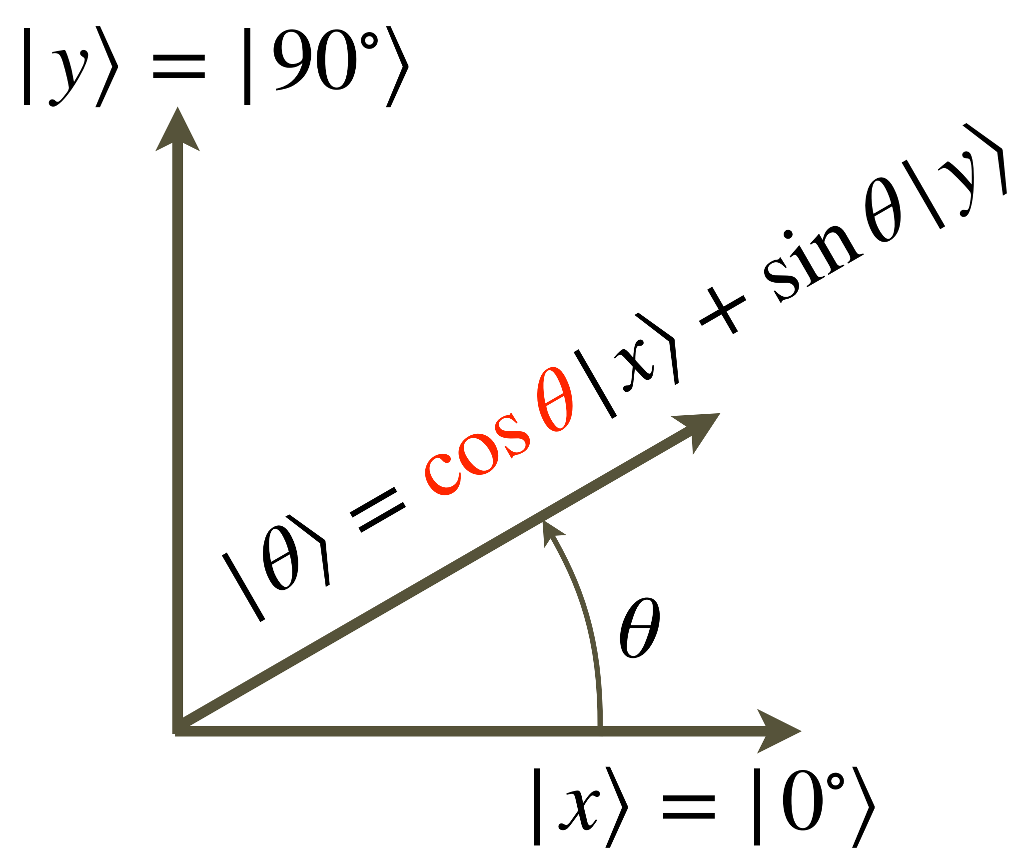
États de polarisation d'un photon

- Chaque photon peut avoir 2 états de polarisation disjoints: $|x\rangle$ ou $|y\rangle$, avec $\langle x|y\rangle = 0$



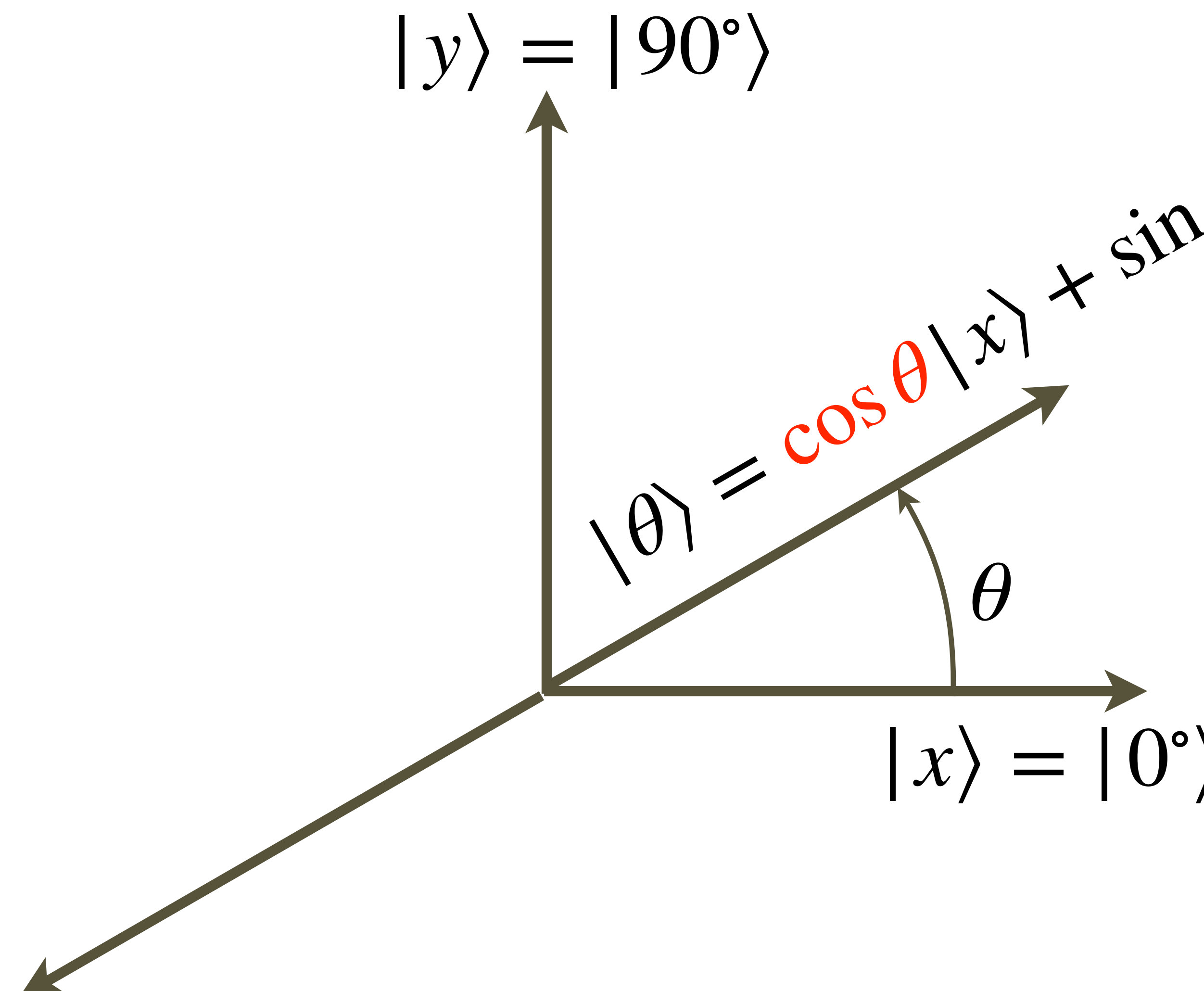
États de polarisation d'un photon

- Chaque photon peut avoir 2 états de polarisation disjoints: $|x\rangle$ ou $|y\rangle$, avec $\langle x|y\rangle = 0$
- Un état général est donc une superposition des 2: $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$



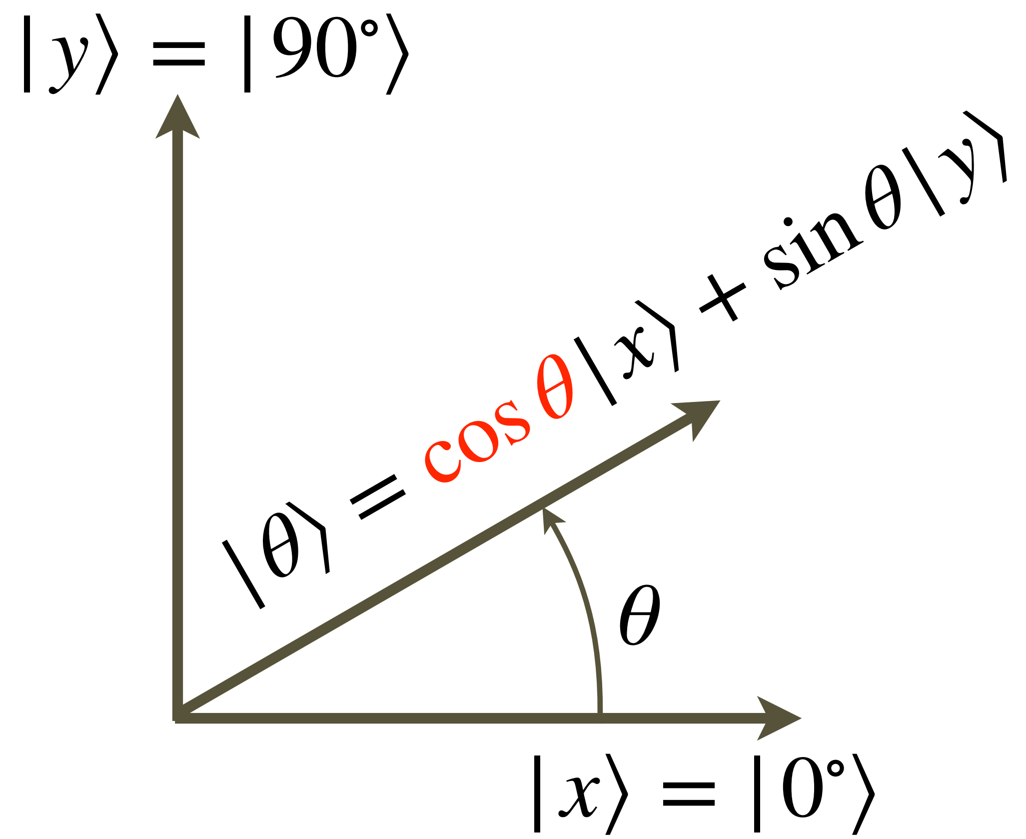
États de polarisation d'un photon

- Chaque photon peut avoir 2 états de polarisation disjoints: $|x\rangle$ ou $|y\rangle$, avec $\langle x|y\rangle = 0$
- Un état général est donc une superposition des 2: $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$
- $|\theta + 180°\rangle = -|\theta\rangle$ décrit le même état



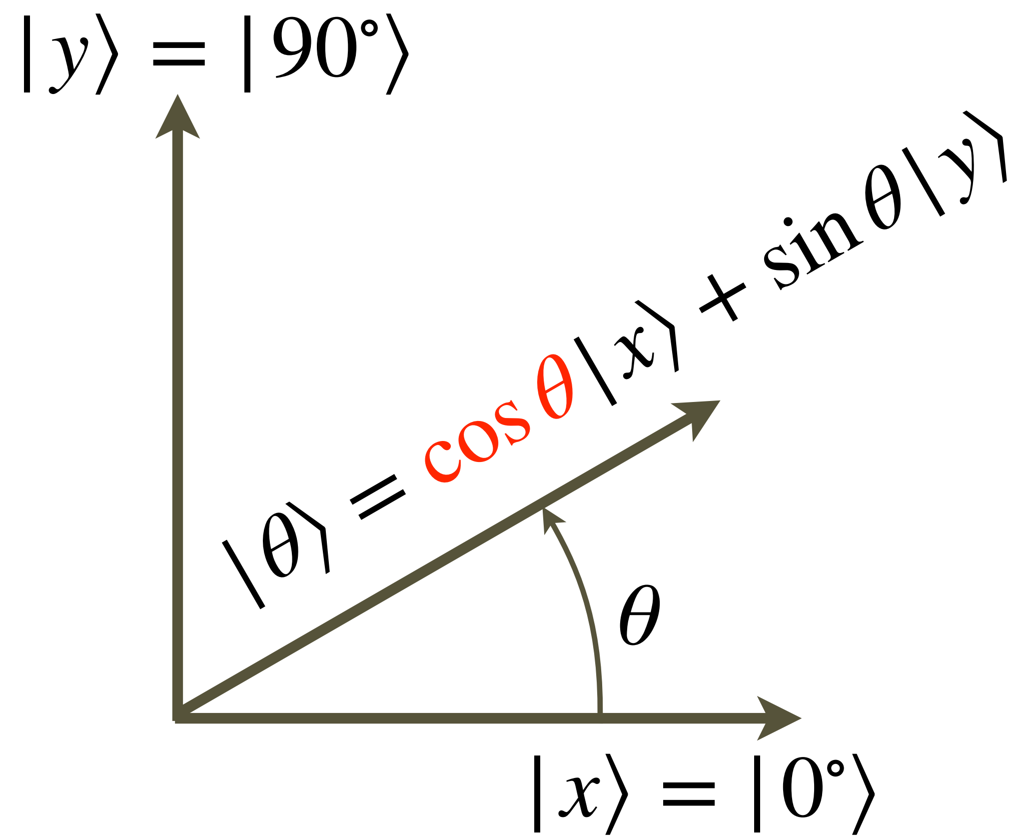
États de polarisation d'un photon

- Chaque photon peut avoir 2 états de polarisation disjoints: $|x\rangle$ ou $|y\rangle$, avec $\langle x|y\rangle = 0$
- Un état général est donc une superposition des 2: $|\theta\rangle = \cos\theta\,|x\rangle + \sin\theta\,|y\rangle$
- $|\theta + 180°\rangle = -|\theta\rangle$ décrit le même état
- $\cos(\theta)^2 = \langle x|\theta\rangle^2 = P(\theta \to x)$ est la probabilité de trouver $|x\rangle$ dans $|\theta\rangle$



États de polarisation d'un photon

- Chaque photon peut avoir 2 états de polarisation disjoints: $|x\rangle$ ou $|y\rangle$, avec $\langle x|y\rangle = 0$
- Un état général est donc une superposition des 2: $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$
- $|\theta + 180°\rangle = -|\theta\rangle$ décrit le même état
- $\cos(\theta)^2 = \langle x|\theta\rangle^2 = P(\theta \to x)$ est la probabilité de trouver $|x\rangle$ dans $|\theta\rangle$
- C'est aussi la probabilité de passer un polariseur Π_x quand on est dans l'état $|\theta\rangle$, ou Π_θ quand on est dans l'état $|x\rangle$

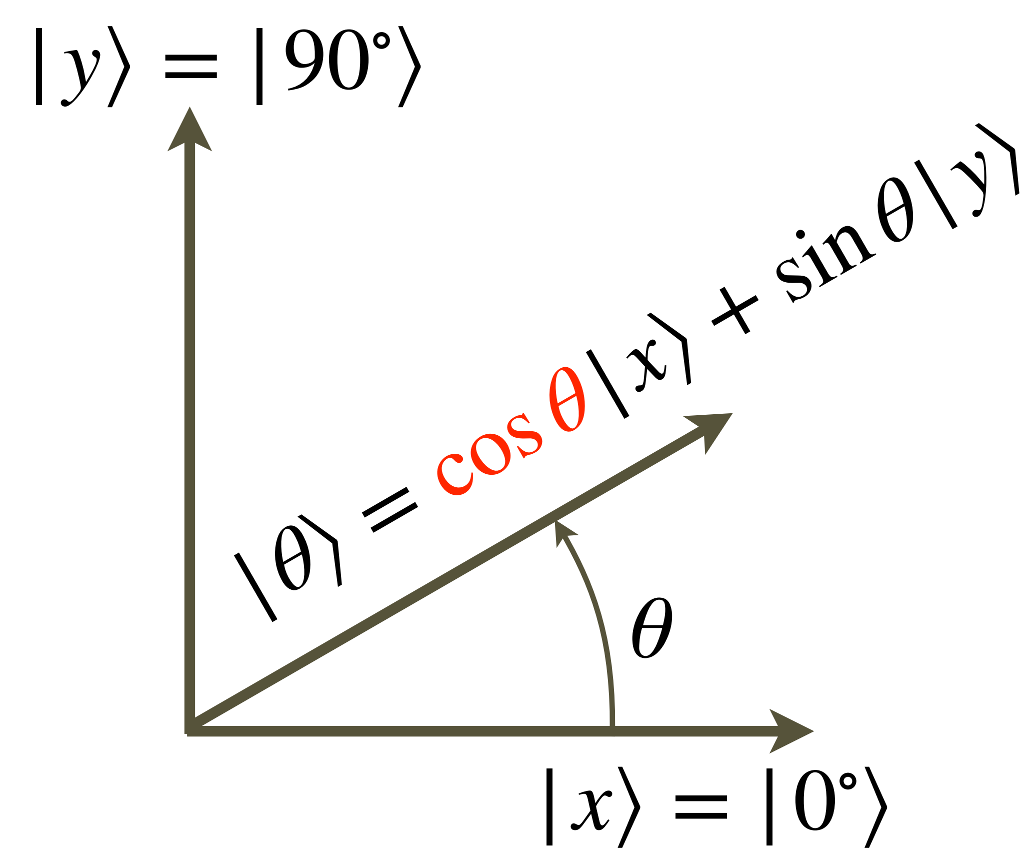


États de polarisation d'un photon

- Chaque photon peut avoir 2 états de polarisation disjoints: $|x\rangle$ ou $|y\rangle$, avec $\langle x|y\rangle = 0$
- Un état général est donc une superposition des 2: $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$
- $|\theta + 180°\rangle = -|\theta\rangle$
  décrit le même état
- $\cos(\theta)^2 = \langle x|\theta\rangle^2 = P(\theta \to x)$ est la probabilité de trouver $|x\rangle$ dans $|\theta\rangle$
- C'est aussi la probabilité de passer un polariseur Π_x quand on est dans l'état $|\theta\rangle$, ou Π_θ quand on est dans l'état $|x\rangle$

- Donc aussi le rapport des nombres de photons N_{apres}/N_{avant} , et d'intensité

$I_{apres}/I_{avant} = \cos(\theta)^2$ (loi de Malus)



Mesure de polarisation: mieux vaut un séparateur

Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :

Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$ inchangé $\rightarrow$ valeur propre 1

Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$
    inchangé → valeur propre 1
  - envoie $|y\rangle$ sur 0
    → valeur propre 0
    mais on a plus de photon!

Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$ inchangé $\rightarrow$ valeur propre 1
  - envoie $|y\rangle$ sur 0 $\rightarrow$ valeur propre 0 **mais on a plus de photon!**
- Préférer $\Sigma_0 = \Pi_x - \Pi_y$ avec valeurs propres et probas

Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$
    inchangé → valeur propre 1
  - envoie $|y\rangle$ sur 0
    → valeur propre 0
    mais on a plus de photon!
- Préférer $\Sigma_0 = \Pi_x - \Pi_y$
  avec valeurs propres et probas
  - $+1 \rightarrow |x\rangle : P_+ = \cos^2\theta$

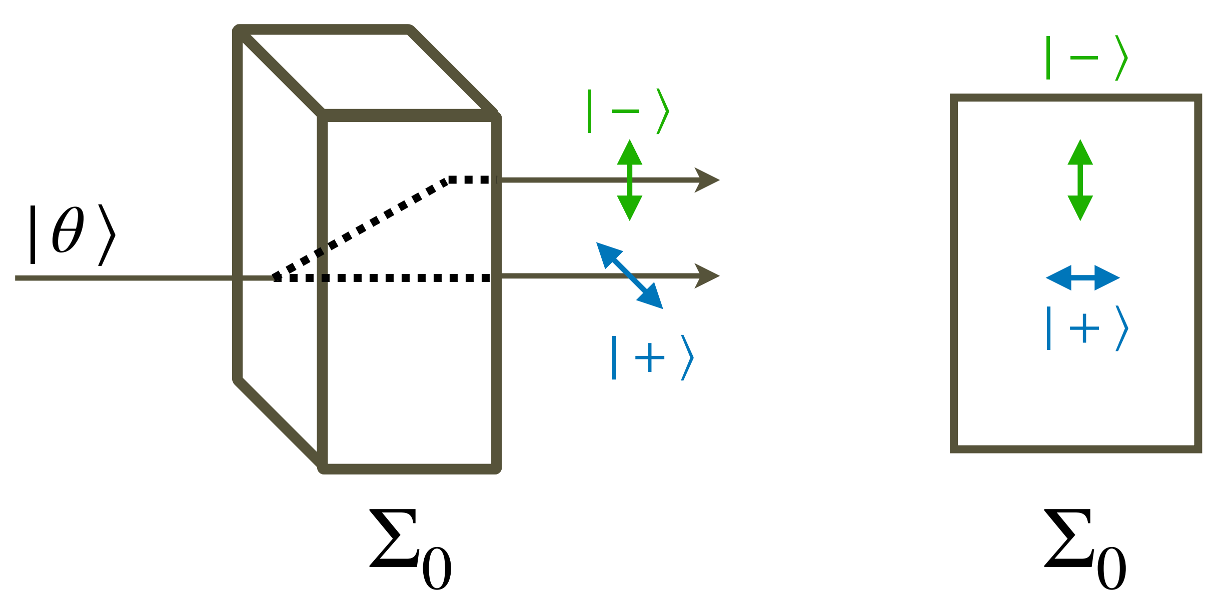
Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$
    inchangé $\rightarrow$ valeur propre 1
  - envoie $|y\rangle$ sur 0
    $\rightarrow$ valeur propre 0
    mais on a plus de photon!
- Préférer $\Sigma_0 = \Pi_x - \Pi_y$
  avec valeurs propres et probas
  - $+1 \rightarrow |x\rangle : P_+ = \cos^2\theta$
  - $-1 \rightarrow |y\rangle : P_- = \sin^2\theta$

Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$ inchangé → valeur propre 1
  - envoie $|y\rangle$ sur 0 → valeur propre 0 **mais on a plus de photon!**
- Préférer $\Sigma_0 = \Pi_x - \Pi_y$ avec valeurs propres et probas
  - $+1 \rightarrow |x\rangle : P_+ = \cos^2\theta$
  - $-1 \rightarrow |y\rangle : P_- = \sin^2\theta$

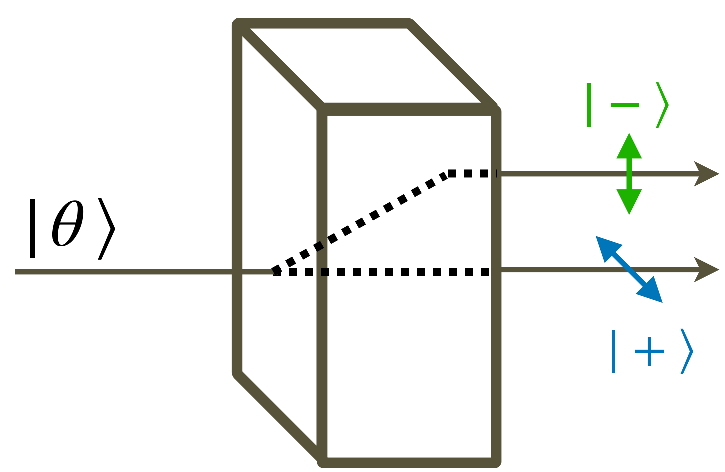
- Calcite (biréfringente) sépare les polarisations:
$|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle \rightarrow \cos\theta|x\rangle|\text{bas}\rangle + \sin\theta|y\rangle|\text{haut}\rangle$



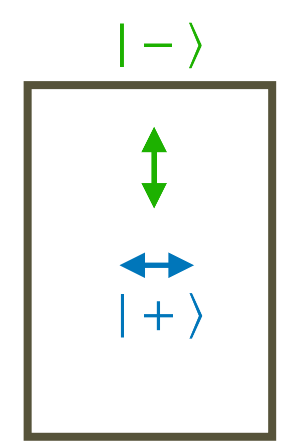
Mesure de polarisation: mieux vaut un séparateur

- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$ inchangé → valeur propre 1
  - envoie $|y\rangle$ sur 0 → valeur propre 0 **mais on a plus de photon!**
- Préférer $\Sigma_0 = \Pi_x - \Pi_y$ avec valeurs propres et probas
  - $+1 \rightarrow |x\rangle : P_+ = \cos^2\theta$
  - $-1 \rightarrow |y\rangle : P_- = \sin^2\theta$

- Calcite (biréfringente) sépare les polarisations: $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle \rightarrow \cos\theta|x\rangle|\text{bas}\rangle + \sin\theta|y\rangle|\text{haut}\rangle$
- état <u>**intriqué**</u>: mesure de position (bas/haut) donne la polarisation (+ ou -) sans détruire le photon



Σ_0



Σ_0

Mesure de polarisation: mieux vaut un séparateur

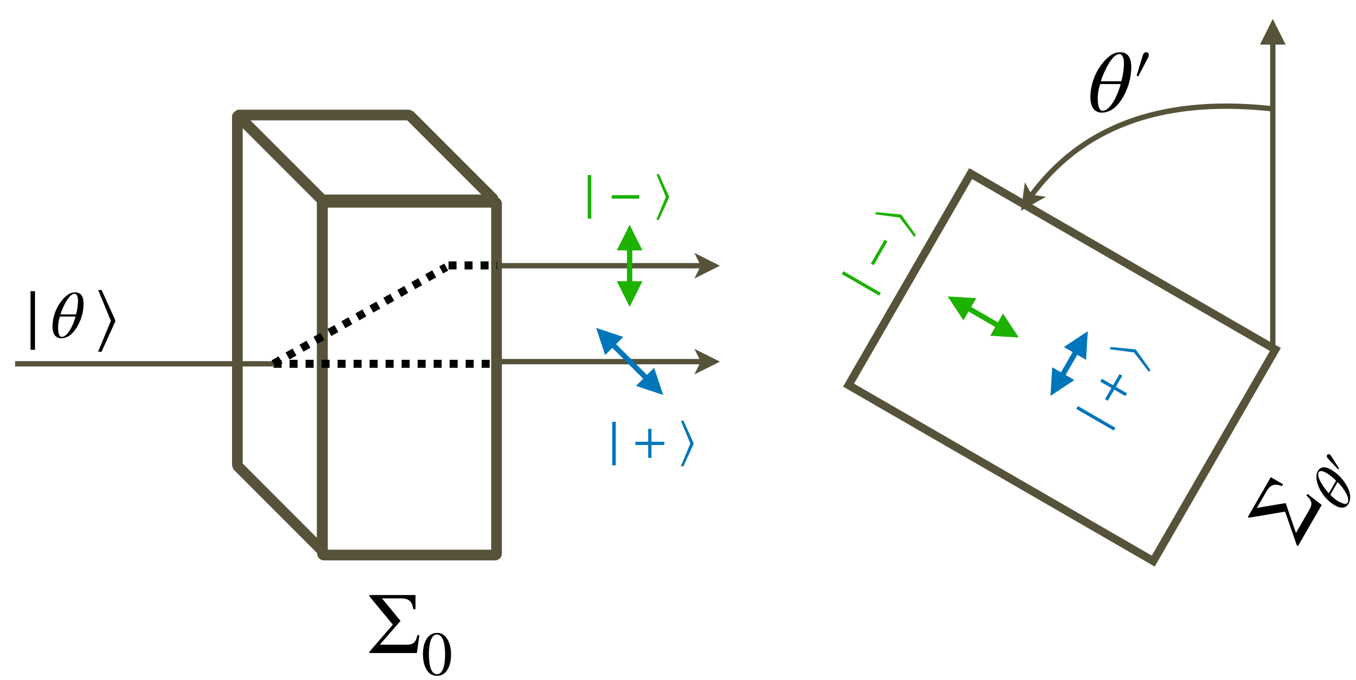
- Polariseur Π_x :
  - envoie $|x\rangle$ sur $|x\rangle$ inchangé → valeur propre 1
  - envoie $|y\rangle$ sur 0 → valeur propre 0 **mais on a plus de photon!**
- Préférer $\Sigma_0 = \Pi_x - \Pi_y$ avec valeurs propres et probas
  - $+1 \rightarrow |x\rangle : P_+ = \cos^2\theta$
  - $-1 \rightarrow |y\rangle : P_- = \sin^2\theta$

En général: $\Sigma_{\theta'} = \Pi_{\theta'} - \Pi_{\theta'+90^\circ}$

$P_+(\theta') = \cos(\theta' - \theta)^2$

$P_-(\theta') = \sin(\theta' - \theta)^2$

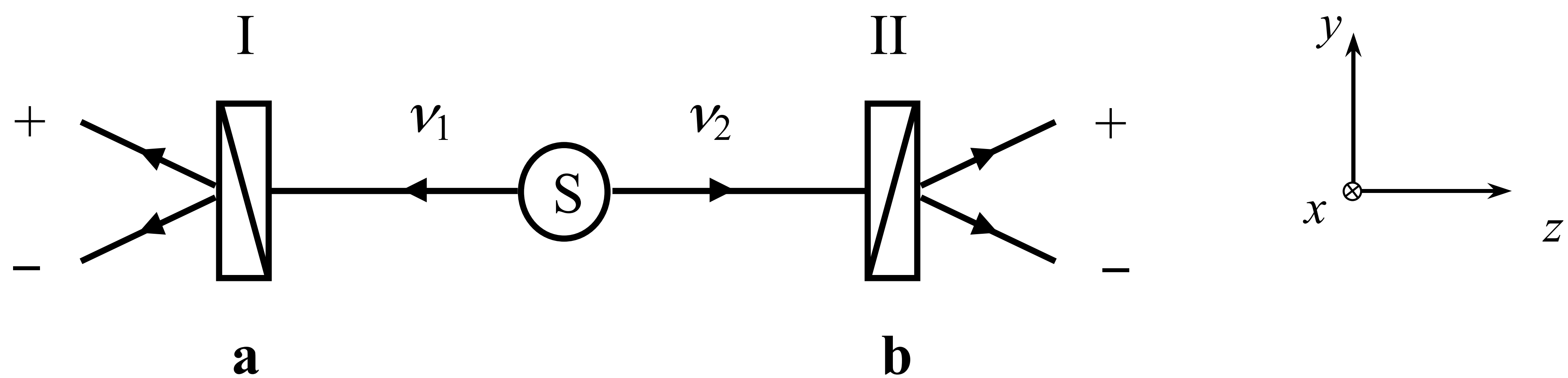
- Calcite (biréfringente) sépare les polarisations: $|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle \rightarrow \cos\theta|x\rangle|\text{bas}\rangle + \sin\theta|y\rangle|\text{haut}\rangle$
- état <u>**intriqué**</u>: mesure de position (bas/haut) donne la polarisation (+ ou -) sans détruire le photon



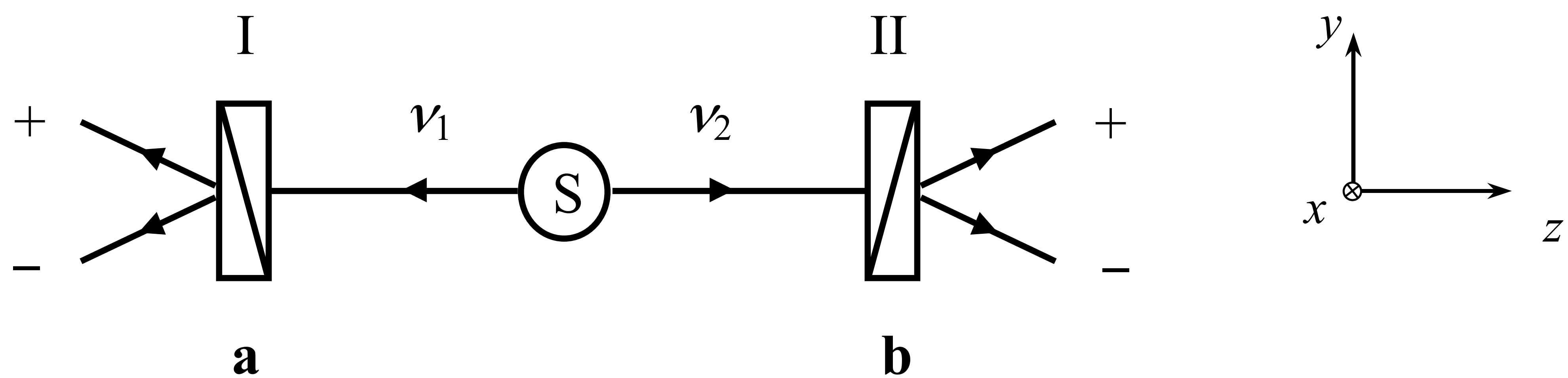
Paradoxe EPR

(Einstein, Podolski, Rosen, 1935)

Paradoxe EPR: expérience de pensée

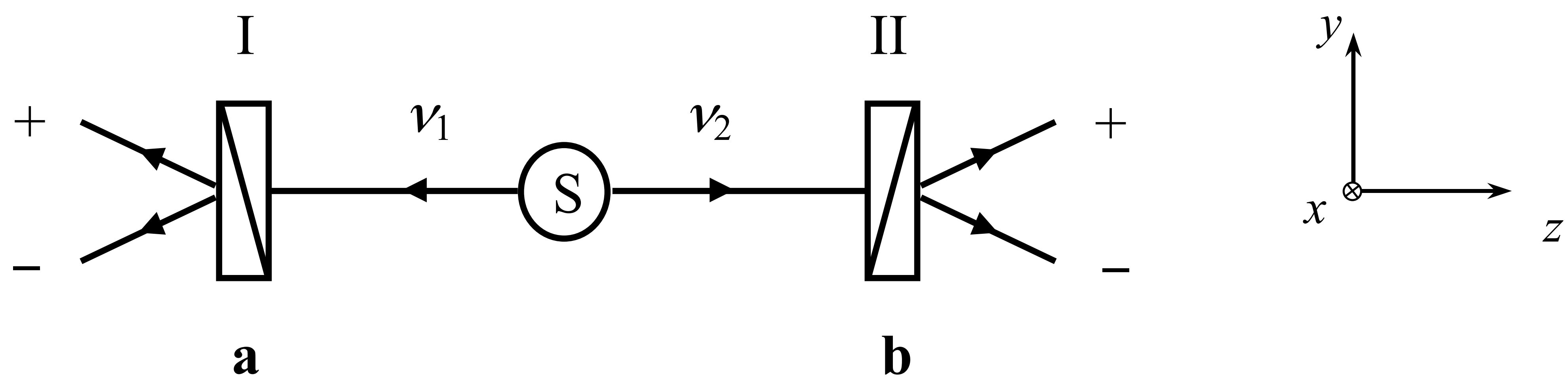


Paradoxe EPR: expérience de pensée



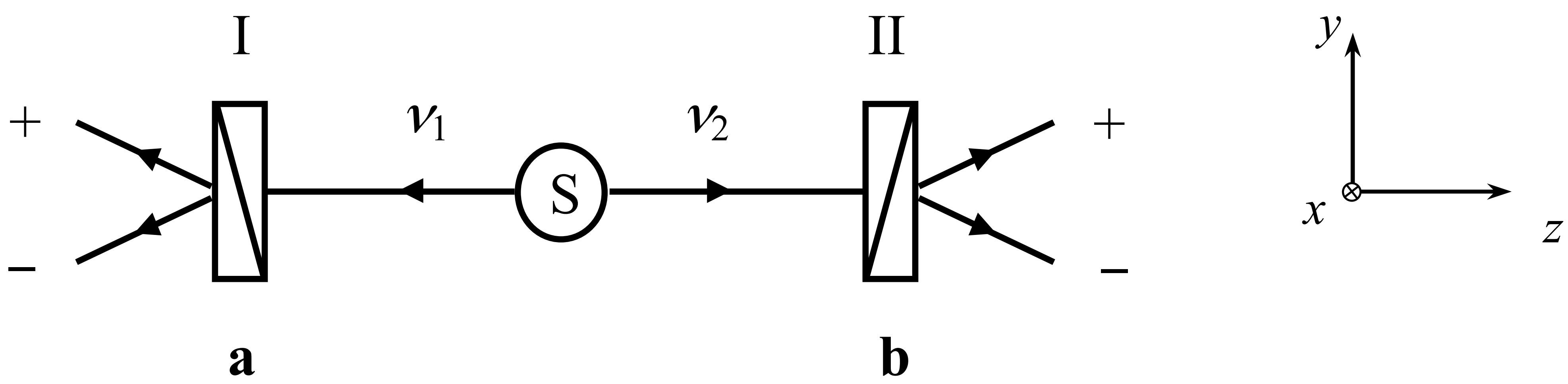
- Source S envoie vers A et B 2 photons **intriqués**
  $| +, + \rangle + | -, - \rangle = | +_a, +_a \rangle + | -_a, -_a \rangle$

Paradoxe EPR: expérience de pensée



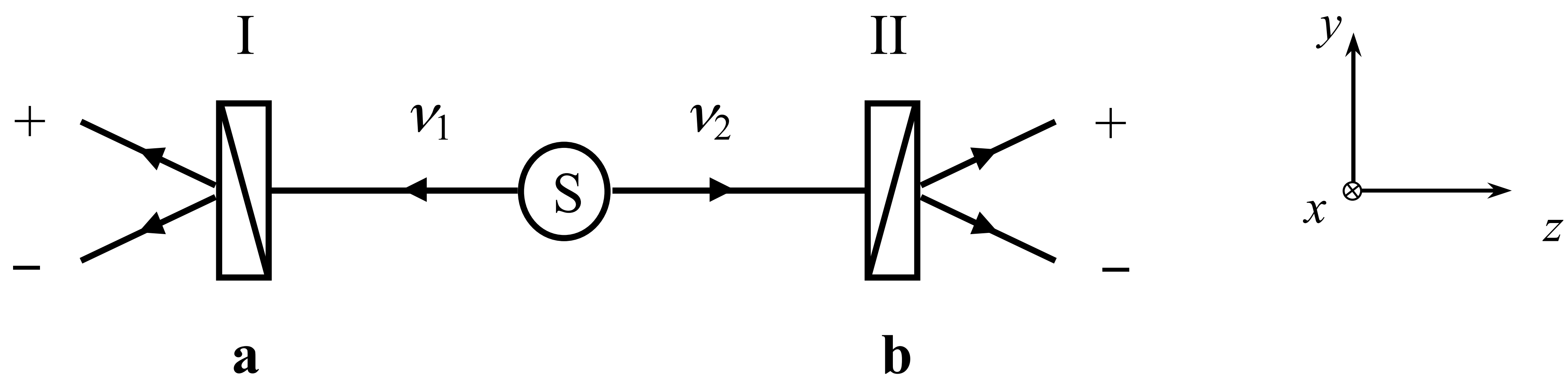
- Source S envoie vers A et B 2 photons **intriqués**
  $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec
  $P_+(a) = P_-(a) = 50\,\%$

Paradoxe EPR: expérience de pensée



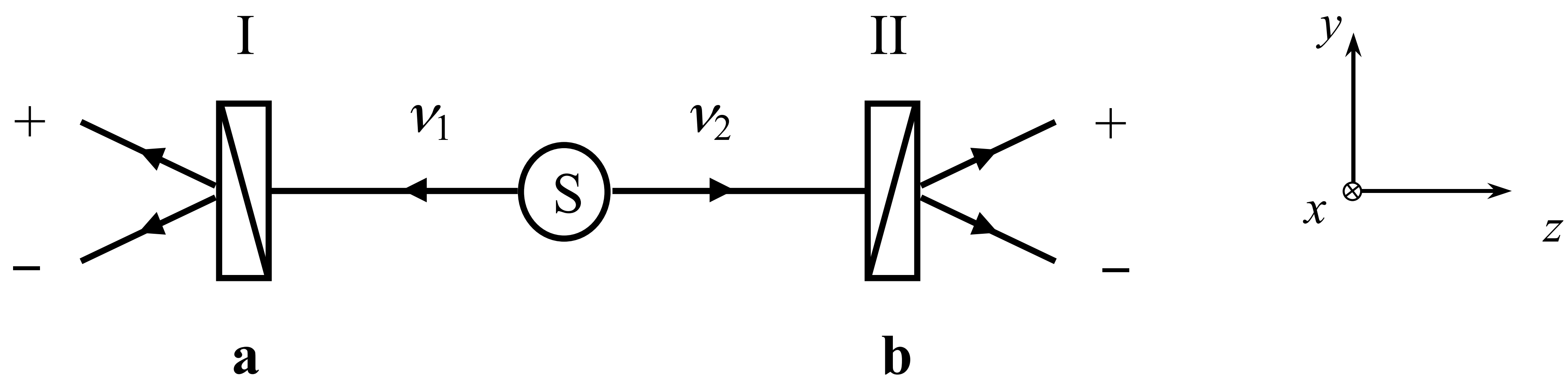
- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$

Paradoxe EPR: expérience de pensée



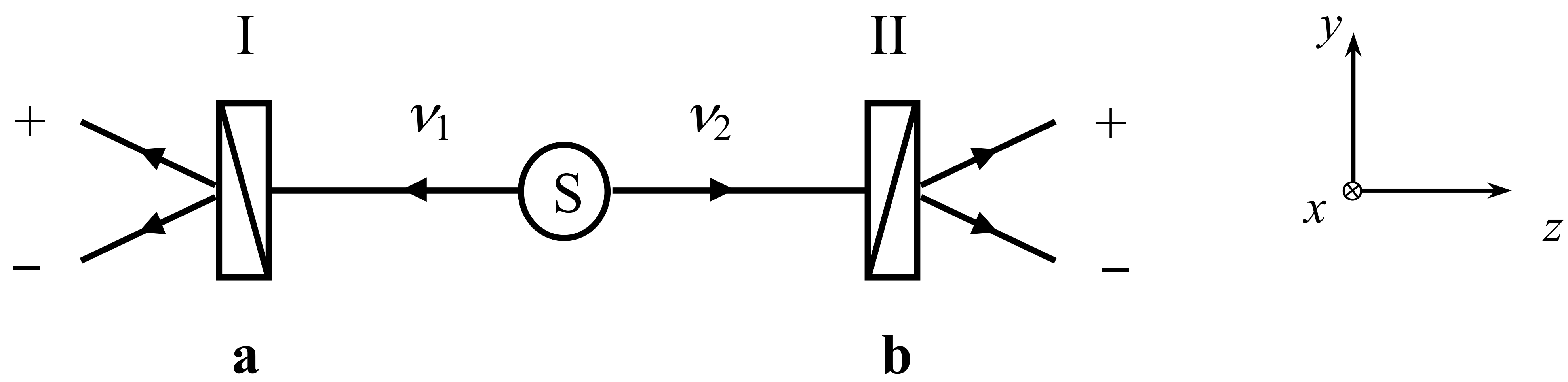
- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +

Paradoxe EPR: expérience de pensée



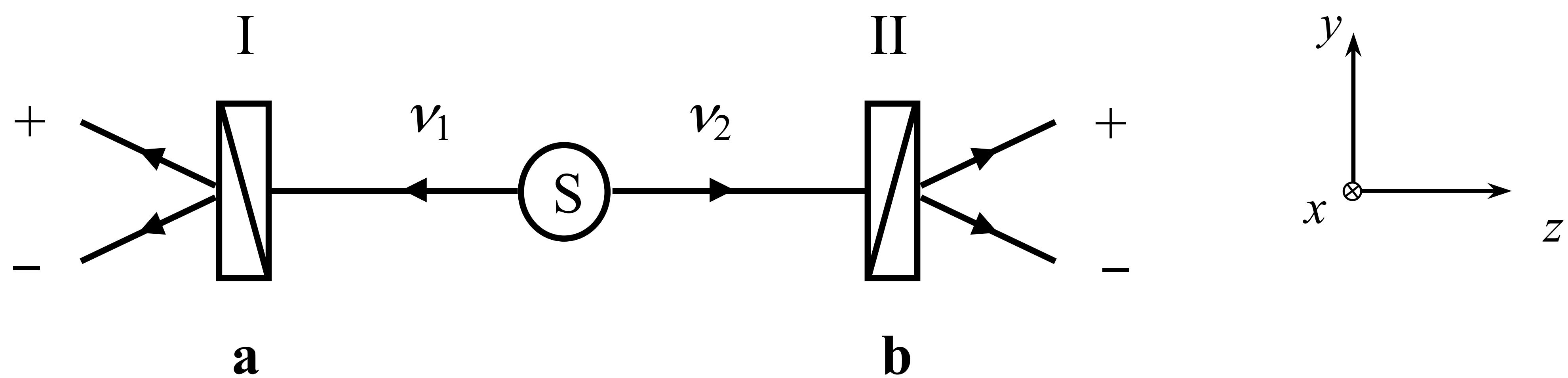
- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +
- En général, si $\theta_{ab} = \theta_a - \theta_b$ $P_{++}(a,b) = P_{--}(a,b) = \cos(\theta_{ab})^2/2$ $P_{+-}(a,b) = P_{-+}(a,b) = \sin(\theta_{ab})^2/2$

Paradoxe EPR: expérience de pensée



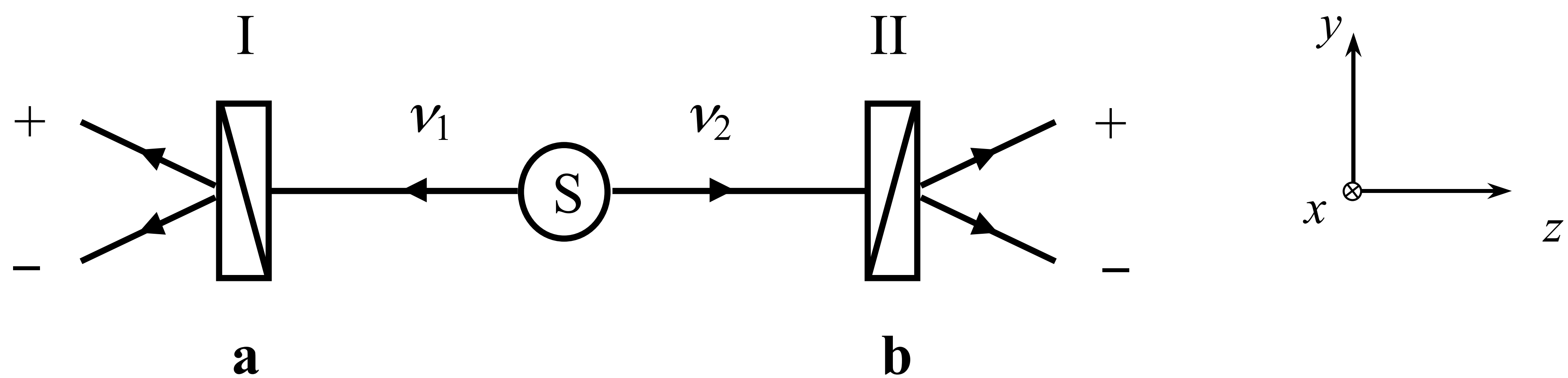
- Source S envoie vers A et B 2 photons **intriqués**
  $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec
  $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +
- En général, si $\theta_{ab} = \theta_a - \theta_b$
  $P_{++}(a,b) = P_{--}(a,b) = \cos(\theta_{ab})^2/2$
  $P_{+-}(a,b) = P_{-+}(a,b) = \sin(\theta_{ab})^2/2$
- Même la moyenne
  $E_((a,b) = P_{++} + P_{--} - P_{+-} - P_{-+} = \cos(2\theta_{ab})$
  dépend des choix indépendants de $\theta_{a,b}$

Paradoxe EPR: expérience de pensée



- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +
- En général, si $\theta_{ab} = \theta_a - \theta_b$ $P_{++}(a,b) = P_{--}(a,b) = \cos(\theta_{ab})^2/2$ $P_{+-}(a,b) = P_{-+}(a,b) = \sin(\theta_{ab})^2/2$
- Même la moyenne $E_((a,b) = P_{++} + P_{--} - P_{+-} - P_{-+} = \cos(2\theta_{ab})$ dépend des choix indépendants de $\theta_{a,b}$
- Or B est aussi loin qu'on veut… **comment peut-il savoir le choix en A?**

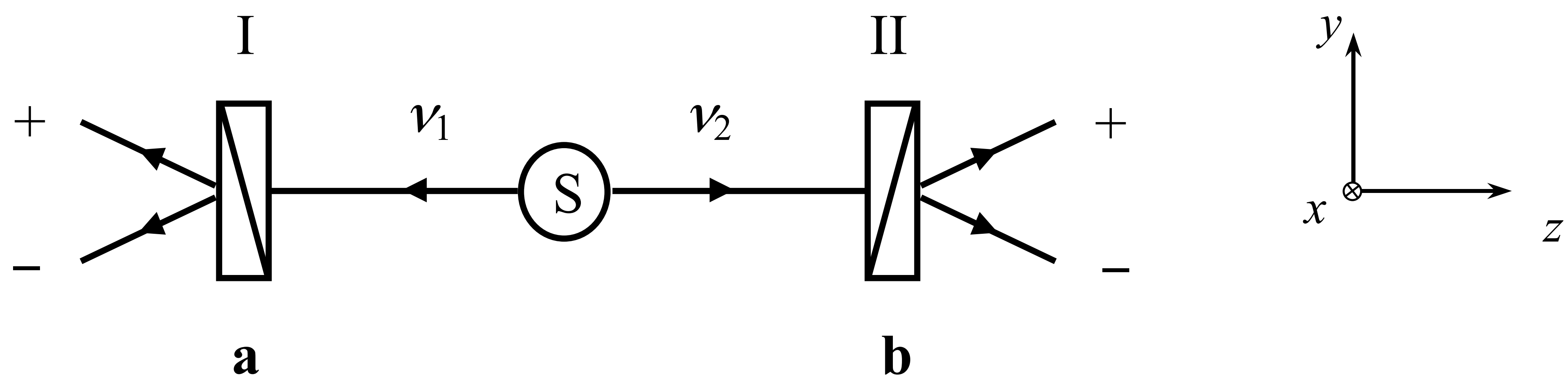
Paradoxe EPR: expérience de pensée



- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer $+$ ou $-$ avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +
- En général, si $\theta_{ab} = \theta_a - \theta_b$ $P_{++}(a,b) = P_{--}(a,b) = \cos(\theta_{ab})^2/2$ $P_{+-}(a,b) = P_{-+}(a,b) = \sin(\theta_{ab})^2/2$
- Même la moyenne $E_{(}a,b) = P_{++} + P_{--} - P_{+-} - P_{-+} = \cos(2\theta_{ab})$ dépend des choix indépendants de $\theta_{a,b}$
- Or B est aussi loin qu′on veut… **comment peut-il savoir le choix en A?**

$\Rightarrow$ Ou bien:

Paradoxe EPR: expérience de pensée

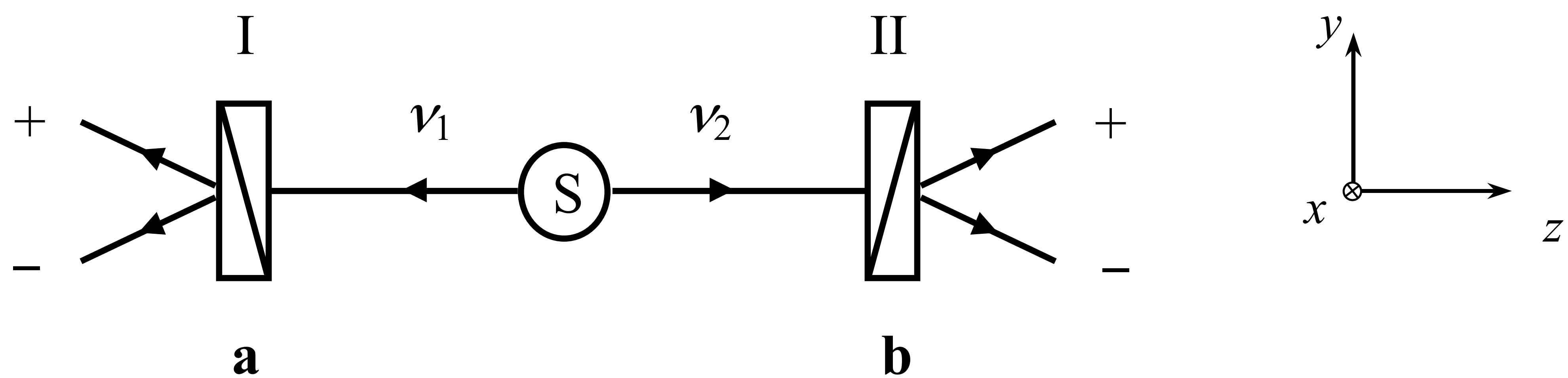


- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +
- En général, si $\theta_{ab} = \theta_a - \theta_b$ $P_{++}(a,b) = P_{--}(a,b) = \cos(\theta_{ab})^2/2$ $P_{+-}(a,b) = P_{-+}(a,b) = \sin(\theta_{ab})^2/2$
- Même la moyenne $E_((a,b) = P_{++} + P_{--} - P_{+-} - P_{-+} = \cos(2\theta_{ab})$ dépend des choix indépendants de $\theta_{a,b}$
- Or B est aussi loin qu′on veut… **comment peut-il savoir le choix en A?**

$\Rightarrow$ Ou bien:

1. il y a des effets à distance plus rapide que la lumière (loi 4 de Copenhague)

Paradoxe EPR: expérience de pensée



- Source S envoie vers A et B 2 photons **intriqués** $|+,+\rangle + |-,-\rangle = |+_a,+_a\rangle + |-_a,-_a\rangle$
- Quelque soit l'angle θ_a de sa calcite, A doit mesurer + ou − avec $P_+(a) = P_-(a) = 50\,\%$
- Après sa mesure, p.ex. de +, état devient **instantanément** $|+_a,+_a\rangle$
- Donc si $\theta_b = \theta_a$, la mesure de B sera **certainement** +
- En général, si $\theta_{ab} = \theta_a - \theta_b$ $P_{++}(a,b) = P_{--}(a,b) = \cos(\theta_{ab})^2/2$ $P_{+-}(a,b) = P_{-+}(a,b) = \sin(\theta_{ab})^2/2$

- Même la moyenne $E_{(}a,b) = P_{++} + P_{--} - P_{+-} - P_{-+} = \cos(2\theta_{ab})$ dépend des choix indépendants de $\theta_{a,b}$
- Or B est aussi loin qu'on veut… **comment peut-il savoir le choix en A?**

$\Rightarrow$ Ou bien:

1. il y a des effets à distance plus rapide que la lumière (loi 4 de Copenhague)
2. la description de l'état initial est incomplète (p.ex. il y a des variables cachées prédéterminant localement les résultats).

Variables cachées

Variables cachées

- Depuis Born ('26), les lois 2 et 4 sont les seules introduisant un hasard de principe en physique

≠ tirer une carte *au hasard* provient de l'ignorance de l'ordre!...

Variables cachées

- Depuis Born ('26), les lois 2 et 4 sont les seules introduisant un hasard de principe en physique

≠ tirer une carte *au hasard* provient de l'ignorance de l'ordre!...

- Pour éviter ce hasard de principe, il faudrait un état quantique augmenté "**réel**", **avec variables cachées** dont l'ignorance engendre le hasard

Variables cachées

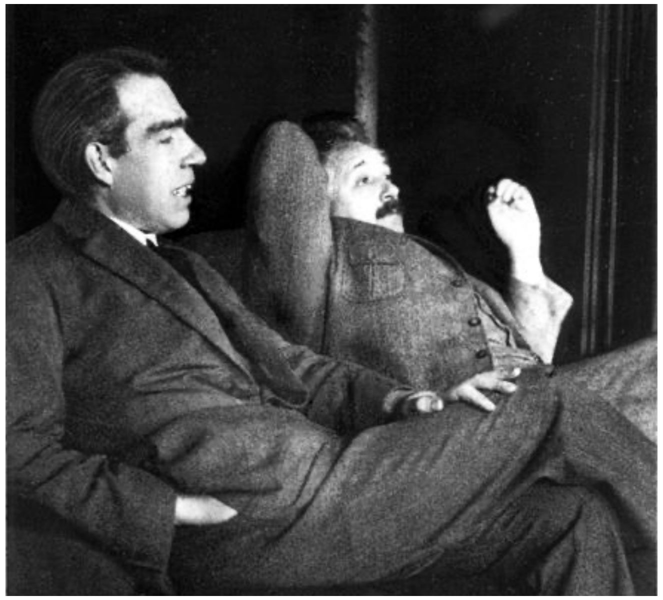
- Depuis Born ('26), les lois 2 et 4 sont les seules introduisant un hasard de principe en physique

≠ tirer une carte *au hasard* provient de l'ignorance de l'ordre!…

- Pour éviter ce hasard de principe, il faudrait un état quantique augmenté "**réel**", **avec variables cachées** dont l'ignorance engendre le hasard

- Einstein: God doesn't play dices!

(Bohr: stop telling God what to do!)



Variables cachées

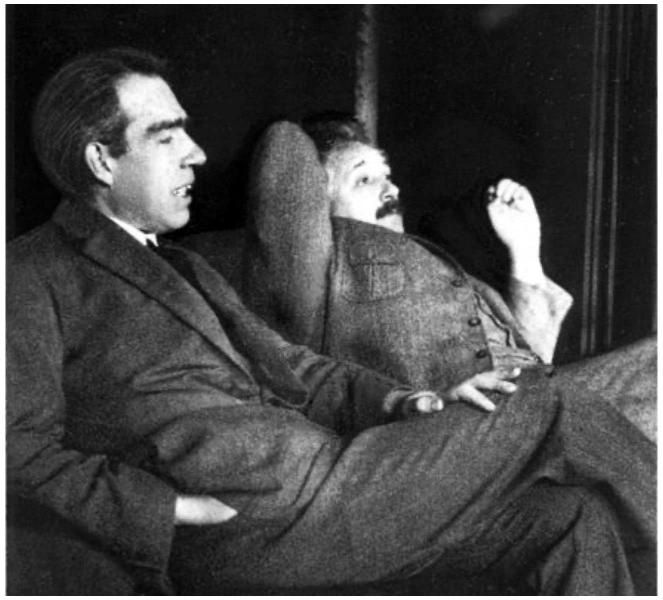
- Depuis Born ('26), les lois 2 et 4 sont les seules introduisant un hasard de principe en physique

≠ tirer une carte *au hasard* provient de l'ignorance de l'ordre!…

- Pour éviter ce hasard de principe, il faudrait un état quantique augmenté "**réel**", **avec variables cachées** dont l'ignorance engendre le hasard

- Einstein: God doesn't play dices! (Bohr: stop telling God what to do!)

- Tentative simple pour EPR: une "couleur" (réelle, mais inconnue) des photons dicterait localement leur polarisation



Variables cachées

- Depuis Born ('26), les lois 2 et 4 sont les seules introduisant un hasard de principe en physique

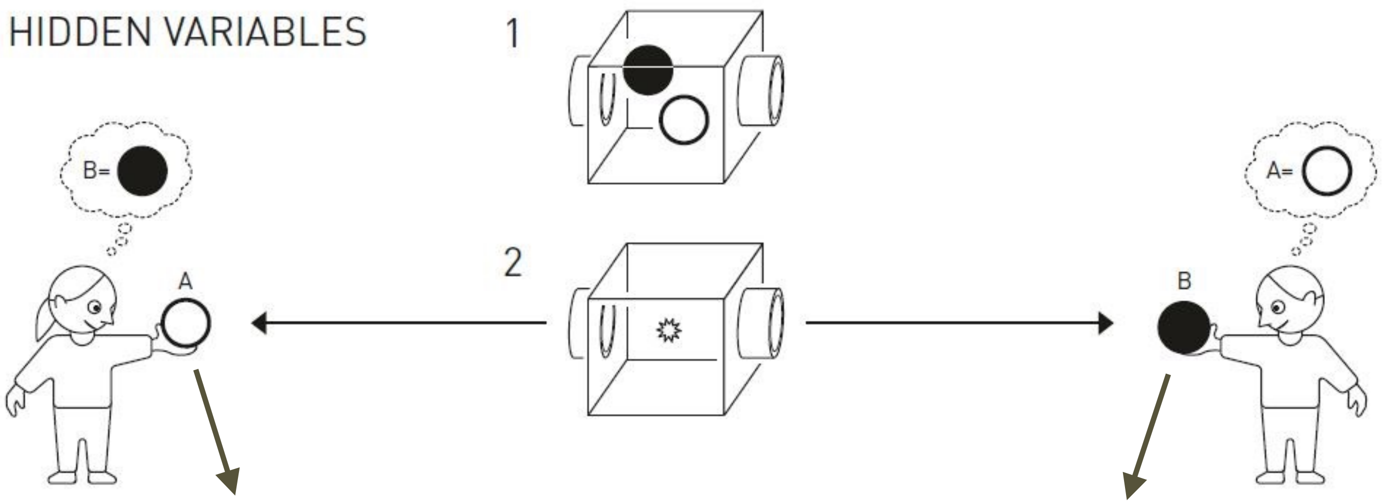
$\neq$ tirer une carte *au hasard* provient de l'ignorance de l'ordre!...

- Pour éviter ce hasard de principe, il faudrait un état quantique augmenté "**réel**", **avec variables cachées** dont l'ignorance engendre le hasard

- Einstein: God doesn't play dices! (Bohr: stop telling God what to do!)

- Tentative simple pour EPR: une "couleur" (réelle, mais inconnue) des photons dicterait localement leur polarisation

- Cela peut-il marcher?



$| +_a \rangle$ $\qquad$ $| +_a \rangle$

Inégalités de Bell

Bell1964, Clauser-Horne-Shimony-Holt 1969

Théorème de Bell

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
    - variables cachées λ

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
  - variables cachées λ
  - l'orientation θ_a de A

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
  - variables cachées λ
  - l'orientation θ_a de A
  - **pas** de θ_b (localité)

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
  - variables cachées λ
  - l'orientation θ_a de A
  - **pas** de θ_b (localité)
  - et vice-versa pour $b(\theta_b, \lambda) = \pm 1$

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
  - variables cachées λ
  - l'orientation θ_a de A
  - **pas** de θ_b (localité)
  - et vice-versa pour $b(\theta_b, \lambda) = \pm 1$
- si les moyennes quantiques sont données par la probabilité $P(\lambda)$ d'avoir différentes λ
  $E(a, b)_{VC} = \sum_{\lambda} P(\lambda) a(\theta_a, \lambda) b(\theta_b, \lambda)$

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
  - variables cachées λ
  - l'orientation θ_a de A
  - **pas** de θ_b (localité)
  - et vice-versa pour $b(\theta_b, \lambda) = \pm 1$
- si les moyennes quantiques sont données par la probabilité $P(\lambda)$ d'avoir différentes λ $E(a, b)_{VC} = \sum_{\lambda} P(\lambda)a(\theta_a, \lambda)b(\theta_b, \lambda)$
- Alors (Bell 1964) montre une inégalité pour **3 paires** d'orientation θ_{ab}, θ_{bc} et θ_{ac} qui est violée pour petit $|\theta_{bc}|$ par le résultat quantique $E(a, b)_{MQ} = \cos(2\theta_{ab})$

Théorème de Bell

- Si mesure de A entièrement fixée par $a(\theta_a, \lambda) = \pm 1$, fonction de
  - variables cachées λ
  - l'orientation θ_a de A
  - **pas** de θ_b (localité)
  - et vice-versa pour $b(\theta_b, \lambda) = \pm 1$
- si les moyennes quantiques sont données par la probabilité $P(\lambda)$ d'avoir différentes λ $E(a, b)_{VC} = \sum_{\lambda} P(\lambda) a(\theta_a, \lambda) b(\theta_b, \lambda)$
- Alors (Bell 1964) montre une inégalité pour **3 paires** d'orientation θ_{ab}, θ_{bc} et θ_{ac} qui est violée pour petit $|\theta_{bc}|$ par le résultat quantique $E(a, b)_{MQ} = \cos(2\theta_{ab})$
- $\Rightarrow$ on peut choisir en principe des configurations réalisant un **test expérimental** des variables cachées locales!!!

Inégalité de Clauser-Horn-Shimony-Holt

Inégalité de Clauser-Horn-Shimony-Holt

- Pour chaque λ fixé, la combinaison de **4 paires** de directions:
  $$S(a, a', b, b') = E(a, b) - E(a, b') + E(a', b) + E(a', b')$$
  se factorise en
  $$a(b - b') + a'(b + b')$$

Inégalité de Clauser-Horn-Shimony-Holt

- Pour chaque λ fixé, la combinaison de **4 paires** de directions:
  $$S(a, a', b, b') = E(a, b) - E(a, b') + E(a', b) + E(a', b')$$
  se factorise en
  $a(b - b') + a'(b + b')$
- Si $b - b' = 0$, alors $b + b' = \pm 2$ et vice versa

Inégalité de Clauser-Horn-Shimony-Holt

- Pour chaque λ fixé, la combinaison de **4 paires** de directions:
$$S(a, a', b, b') = E(a, b) - E(a, b') + E(a', b) + E(a', b')$$
se factorise en
$a(b - b') + a'(b + b')$

- Si $b - b' = 0$, alors
$b + b' = \pm 2$ et vice versa

- Comme a et $a' = \pm 1$

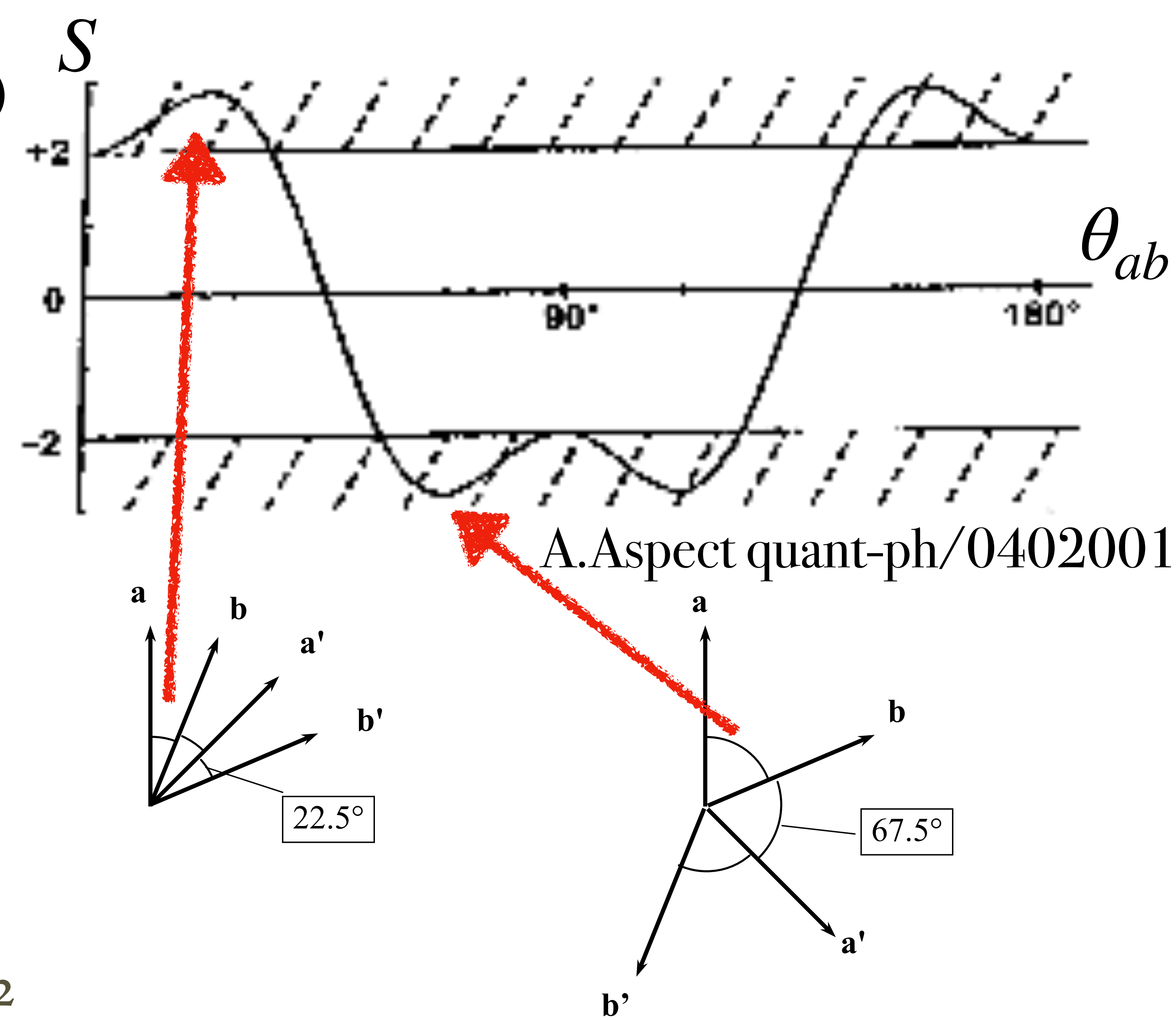
$$-2 \leq S_{VC} \leq 2$$

Inégalité de Clauser-Horn-Shimony-Holt

- Pour chaque λ fixé, la combinaison de **4 paires** de directions:
  $$S(a, a', b, b') = E(a, b) - E(a, b') + E(a', b) + E(a', b')$$
  se factorise en
  $$a(b - b') + a'(b + b')$$
- Si $b - b' = 0$, alors $b + b' = \pm 2$ et vice versa
- Comme a et $a' = \pm 1$

$$-2 \leq S_{VC} \leq 2$$

- On montre que S_{MQ} est extrême pour $\theta_{ab} = \theta_{ba'} = \theta_{a'b'} = \theta_{ab'}/3$

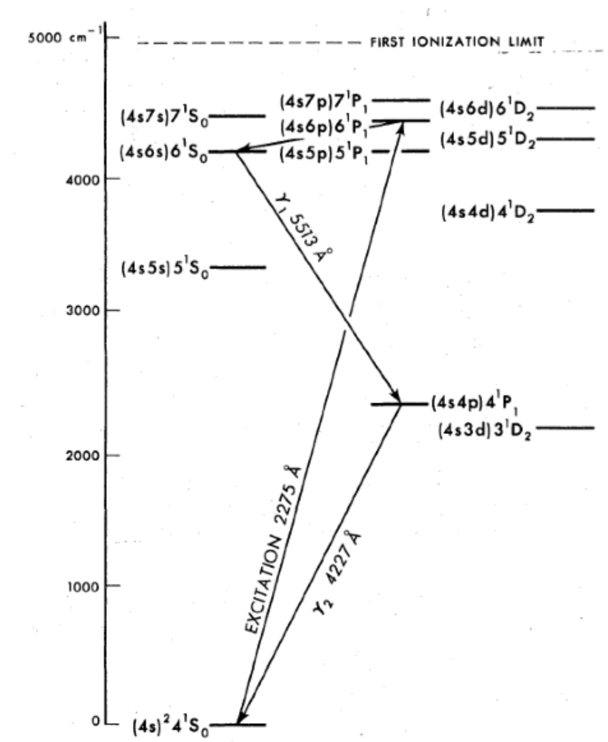


A.Aspect quant-ph/0402001

Tests expérimentaux

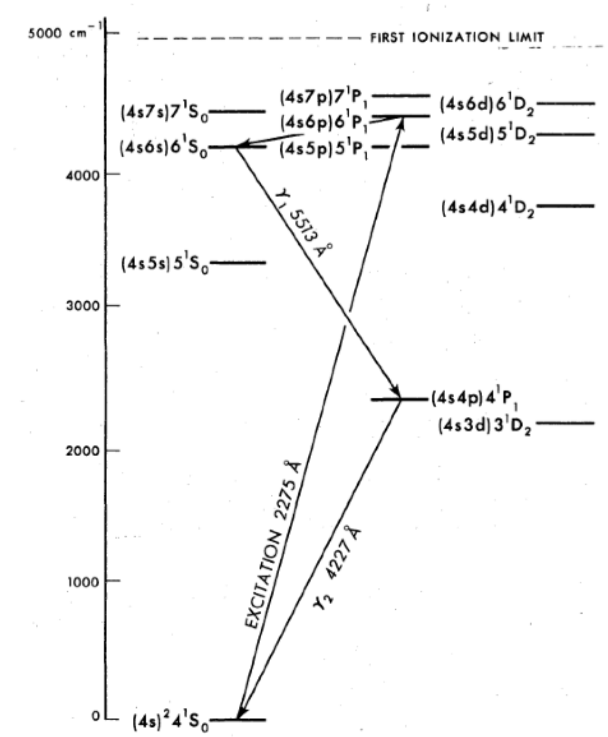
Freedman-Clauser 1972, Aspect-Grangier-Roger 1982

Freedman & Clauser ('72)



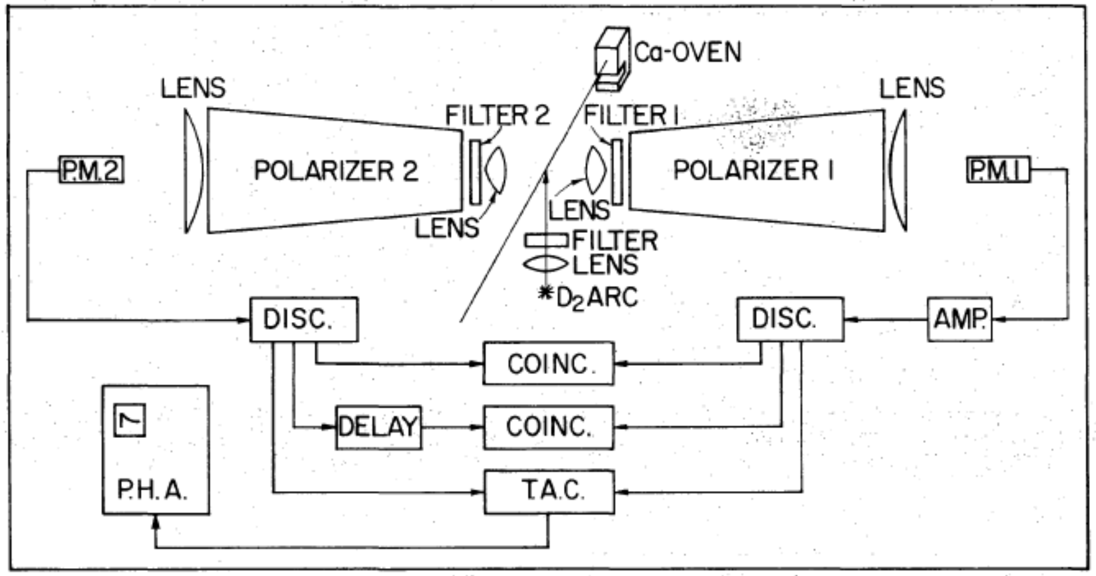
Freedman & Clauser ('72)

- Double désexcitation d'un atome de Calcium
→ paire intriquée



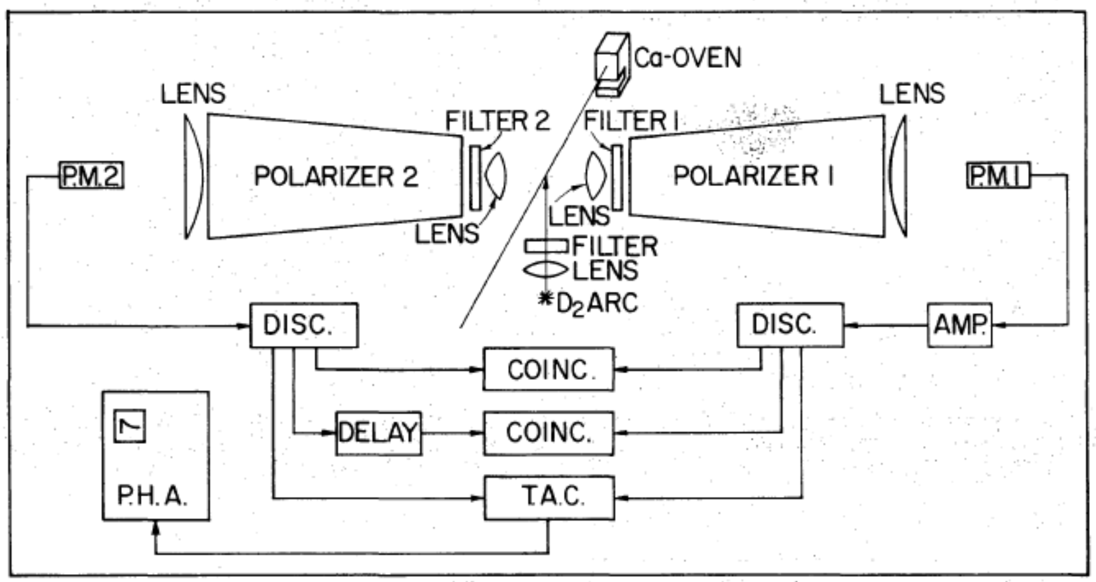
Freedman & Clauser ('72)

- Double désexcitation d'un atome de Calcium → paire intriquée
- Mesurent la variation du taux de coincidence $R(\theta_{ab})/R_0$ pour différents angles



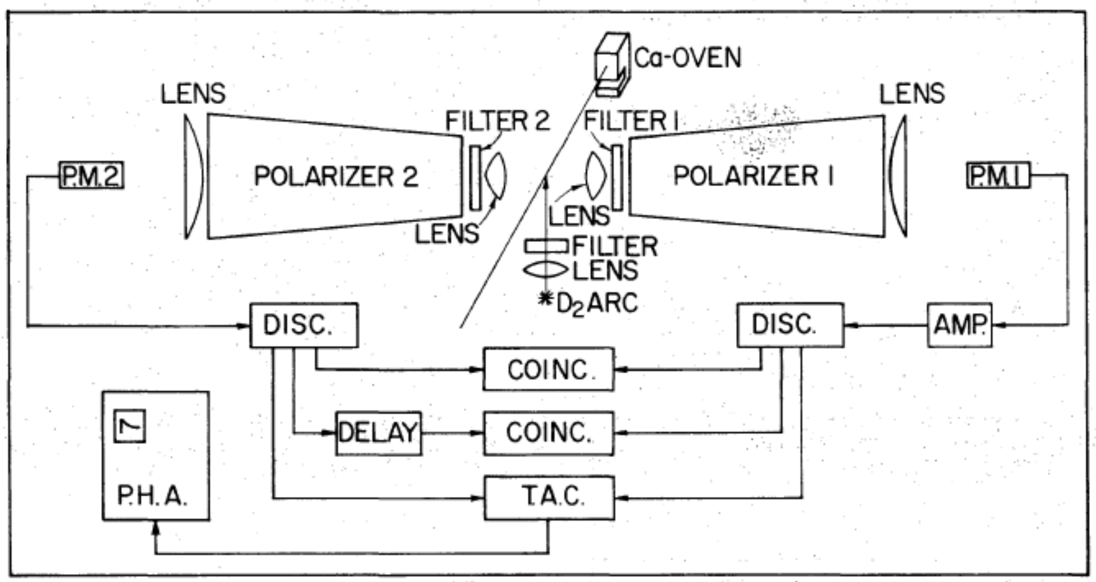
Freedman & Clauser ('72)

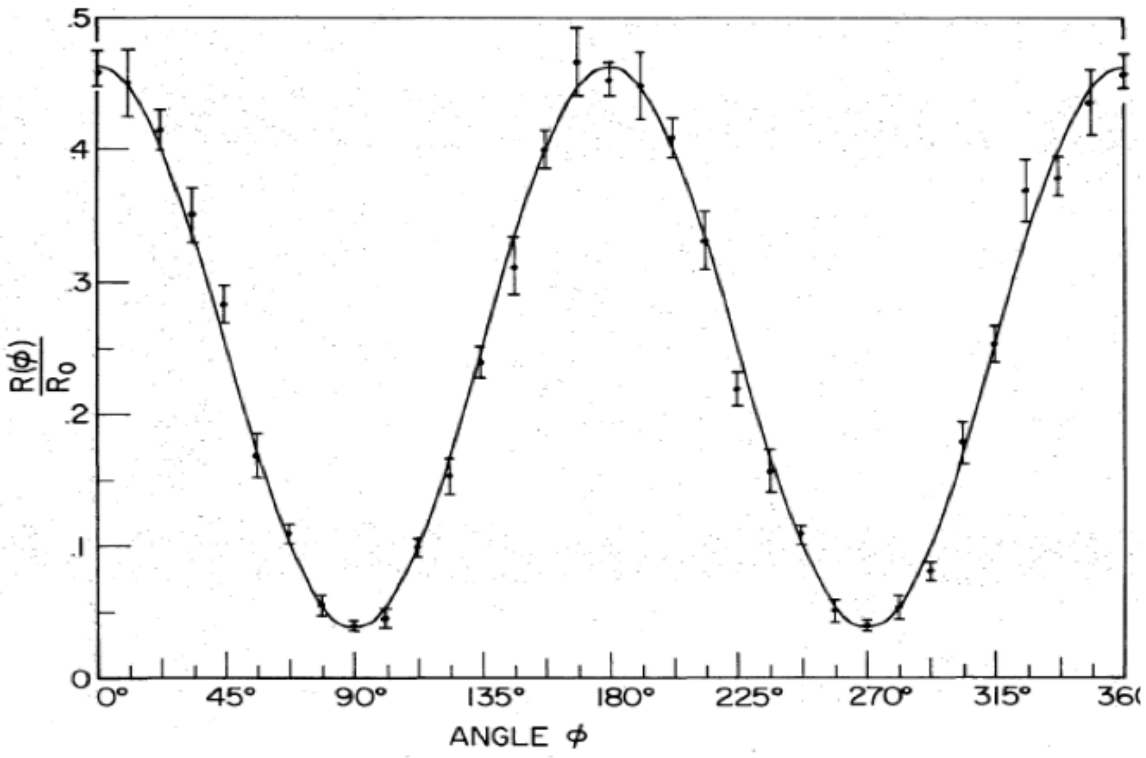
- Double désexcitation d'un atome de Calcium
  → paire intriquée
- Mesurent la variation du taux de coincidence $R(\theta_{ab})/R_0$ pour différents angles
- Vérifient (200h) la violation d'une variante des inégalités:
  $|R(22{,}5) - R(67{,}5)|/R_0 - 1/4 \leq 0$
  à 6 écarts standard



Freedman & Clauser ('72)

- Double désexcitation d'un atome de Calcium $\rightarrow$ paire intriquée
- Mesurent la variation du taux de coincidence $R(\theta_{ab})/R_0$ pour différents angles
- Vérifient (200h) la violation d'une variante des inégalités: $|R(22,5) - R(67,5)|/R_0 - 1/4 \leq 0$ à 6 écarts standard

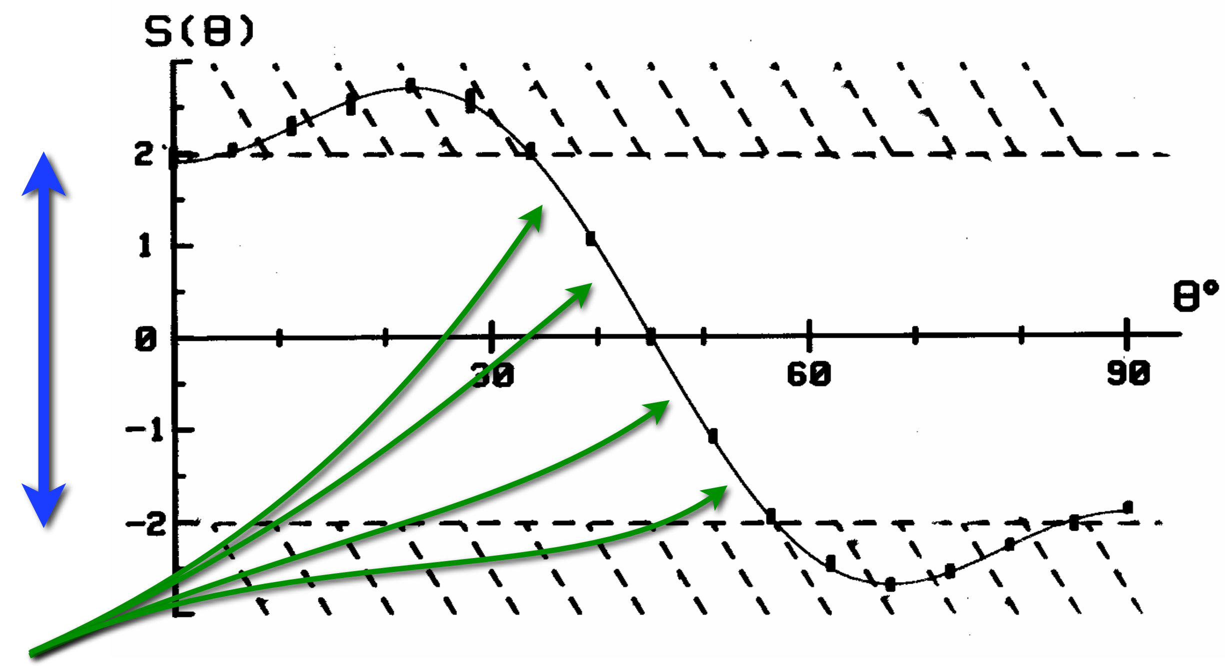




Aspect, Grangier, Roger & Dalibard ('81-82)

Aspect, Grangier, Roger & Dalibard ('81-82)

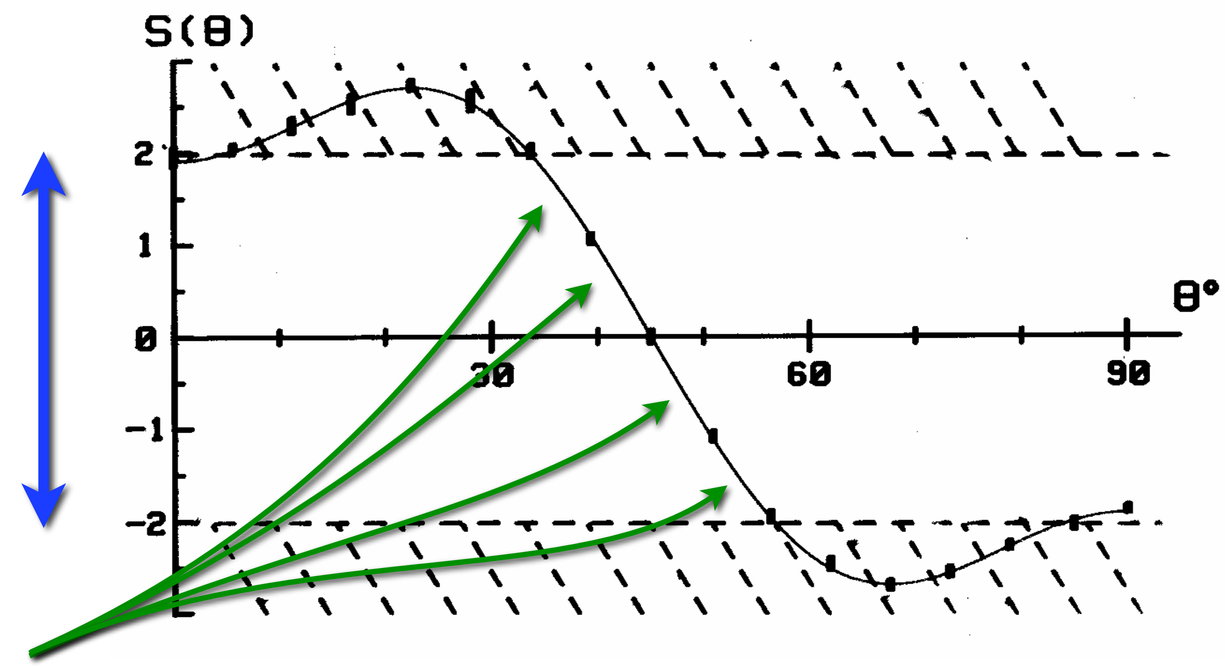
- Vérifient la violation de l'inégalité à 40 déviations standard, grâce à meilleure statistique



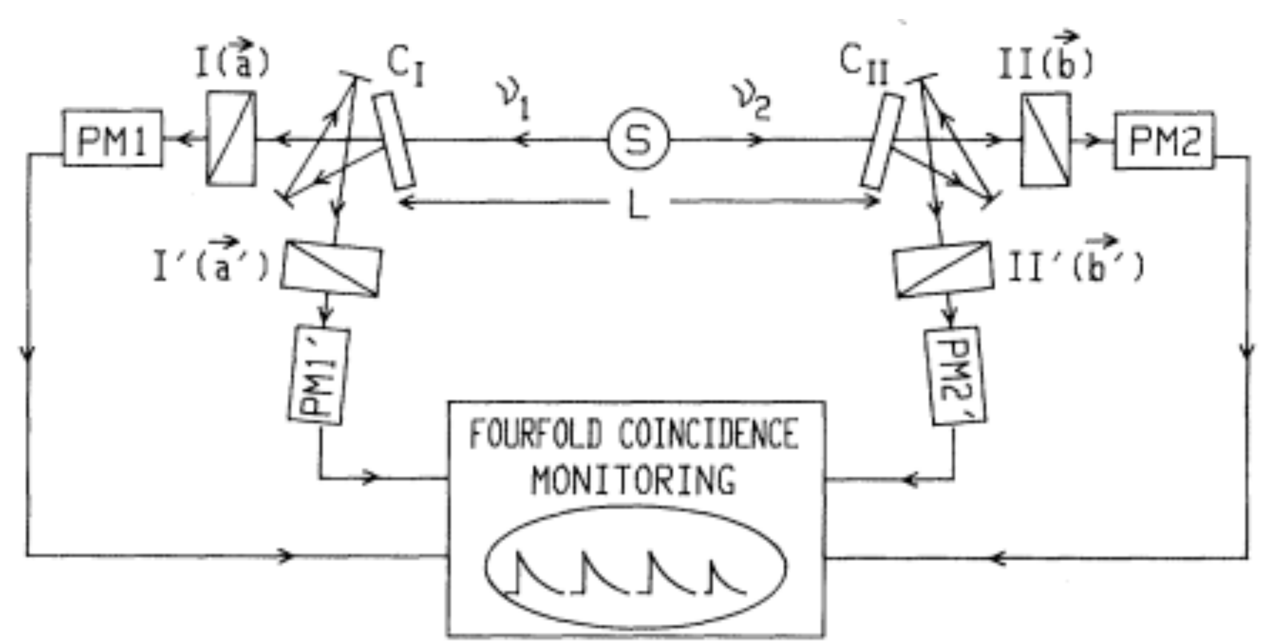
quant-ph/0402001

Aspect, Grangier, Roger & Dalibard ('81-82)

- Vérifient la violation de l'inégalité à 40 déviations standard, grâce à meilleure statistique
- Ecartent la possibilité de communication entre A et B (dist. 6m) en changeant les orientations en moins 20ns, grâce à switch opto-acoustiques: violation à 5 déviations standards



quant-ph/0402001



Nobel A. Aspect 2022

Conclusions

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)
- Bien que surprenantes, elles ne sont pas contradictoires

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)
- Bien que surprenantes, elles ne sont pas contradictoires
- Recherches d'Aspect, Clauser et Zeilinger ont fondé

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)
- Bien que surprenantes, elles ne sont pas contradictoires
- Recherches d'Aspect, Clauser et Zeilinger ont fondé
  - le caractère intrinsèquement aléatoire

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)
- Bien que surprenantes, elles ne sont pas contradictoires
- Recherches d'Aspect, Clauser et Zeilinger ont fondé
  - le caractère intrinsèquement aléatoire
  - l'effet inévitable de la mesure (+: cryptographie et communication)

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)
- Bien que surprenantes, elles ne sont pas contradictoires
- Recherches d'Aspect, Clauser et Zeilinger ont fondé
  - le caractère intrinsèquement aléatoire
  - l'effet inévitable de la mesure (+: cryptographie et communication)
  - intrication (+: calcul quantique)

Conclusions

- Théorie quantique forme un corpus de lois validées expérimentalement
- Utilisées quotidiennement (électronique)
- Bien que surprenantes, elles ne sont pas contradictoires
- Recherches d'Aspect, Clauser et Zeilinger ont fondé
  - le caractère intrinsèquement aléatoire
  - l'effet inévitable de la mesure (+: cryptographie et communication)
  - intrication (+: calcul quantique)
- Théorie alternative:
  toujours désirable, notamment pour le mariage avec la gravitation.
  Mais de plus en plus contrainte!

Références

Références

- *Le monde quantique: une introduction*, M. Le Bellac, EDP Sciences: très bonne introduction physique; quelques mathématiques

Références

- *Le monde quantique: une introduction*, M. Le Bellac, EDP Sciences: très bonne introduction physique; quelques mathématiques
- *Le réel voilé*, B. D'Espagnat, Fayard: pour les aspects plus philosophiques

Références

- *Le monde quantique: une introduction*, M. Le Bellac, EDP Sciences: très bonne introduction physique; quelques mathématiques
- *Le réel voilé*, B. D'Espagnat, Fayard: pour les aspects plus philosophiques
- *Speakable and Unspeakable in Quantum Mechanics,* J. S. Bell, Cambridge U. Press'87

Références

- *Le monde quantique: une introduction*, M. Le Bellac, EDP Sciences: très bonne introduction physique; quelques mathématiques
- *Le réel voilé*, B. D′Espagnat, Fayard: pour les aspects plus philosophiques
- *Speakable and Unspeakable in Quantum Mechanics,* J. S. Bell, Cambridge U. Press′87

- *From Einstein's Theorem to Bell's Theorem: A History of Quantum Nonlocality*, H. M. Wiseman, quant-ph/0509061

Références

- *Le monde quantique: une introduction*, M. Le Bellac, EDP Sciences: très bonne introduction physique; quelques mathématiques
- *Le réel voilé*, B. D'Espagnat, Fayard: pour les aspects plus philosophiques
- *Speakable and Unspeakable in Quantum Mechanics,* J. S. Bell, Cambridge U. Press'87
- *From Einstein's Theorem to Bell's Theorem: A History of Quantum Nonlocality*, H. M. Wiseman, quant-ph/ 0509061
- www.futura-sciences.com

Nécessité des lois quantiques

Pourquoi ces 5 lois "de Copenhague" ?

Pourquoi ces 5 lois ″de Copenhague″ ?

5 lois (ou postulats) énoncés par Bohr-Heisenberg
= cadre opérationnel décrivant toutes expériences quantiques à ce jour; permet de séparer

Pourquoi ces 5 lois ″de Copenhague″ ?

5 lois (ou postulats) énoncés par Bohr-Heisenberg = cadre opérationnel décrivant toutes expériences quantiques à ce jour; permet de séparer

- <u>questions métaphysiques</u> d′interprétation comme la recherche de systèmes équivalents plus satisfaisants

Pourquoi ces 5 lois "de Copenhague" ?

5 lois (ou postulats) énoncés par Bohr-Heisenberg = cadre opérationnel décrivant toutes expériences quantiques à ce jour; permet de séparer

- questions métaphysiques d'interprétation comme la recherche de systèmes équivalents plus satisfaisants
- de l'exploitation de résultats concrets découlant de ces lois, quand on les admet (loi 4.b,c ???)

Nécessité loi 3: quanta

Planck, Bohr

Nécessité loi 3: quanta
Planck, Bohr

- Incohérence théorique dans le traitement du rayonnement électromagnétique à l'équilibre thermique
  → Planck (1899) introduit **niveaux d'énergie** é-magn.

  $\Delta E = h\nu$

  $h = 6.63\ 10^{-34}$ J.s

Nécessité loi 3: quanta

Planck, Bohr

- Incohérence théorique dans le traitement du rayonnement électromagnétique à l'équilibre thermique → Planck (1899) introduit **niveaux d'énergie** é-magn.

  $\Delta E = h\nu$

  $h = 6.63\ 10^{-34}$ J.s

- Spectres d'émission atomique → Bohr ('13): hypothèse du **moment cinétique discret de l'électron**

  $L = \hbar\, n$

Nécessité loi 3: quanta
Planck, Bohr

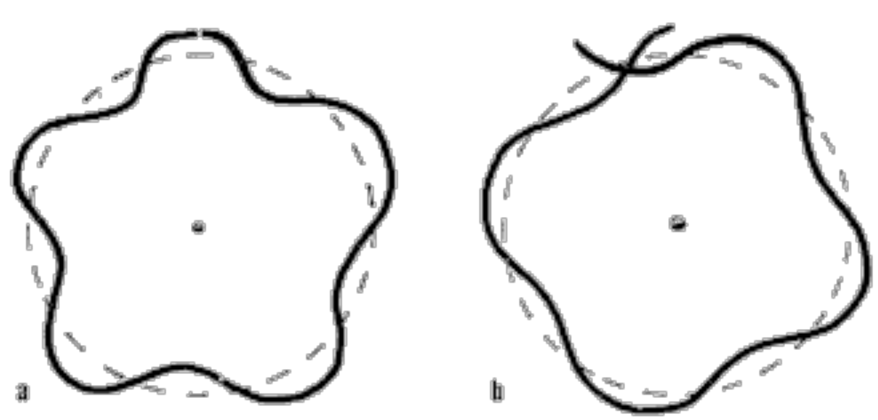
- Incohérence théorique dans le traitement du rayonnement électromagnétique à l′équilibre thermique → Planck (1899) introduit **niveaux d′énergie** é-magn.
  $\Delta E = h\nu$
  $h = 6.63\ 10^{-34}$ J.s

- Spectres d′émission atomique → Bohr (′13): hypothèse du **moment cinétique discret de l′électron**
  $L = \hbar\, n$

- Comment en rendre compte sans un opérateur-matrice pour chaque grandeur discrète?

Nécessité lois 1&2: superposition

de Broglie, Davisson & Germer



Nécessité lois 1&2: superposition

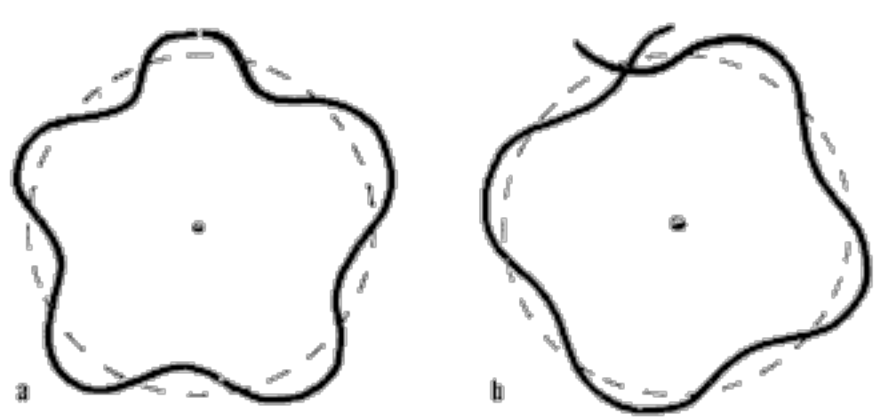
de Broglie, Davisson & Germer

- de Broglie ('24) rend compte de la quantification de Bohr de L par argument d'**interférence constructive d'une onde** de longueur

  $\lambda = h/(m\,v)$

  Incertitude

  $\Delta X > \lambda \leftrightarrow \Delta X \Delta V > \hbar/m$



Nécessité lois 1&2: superposition

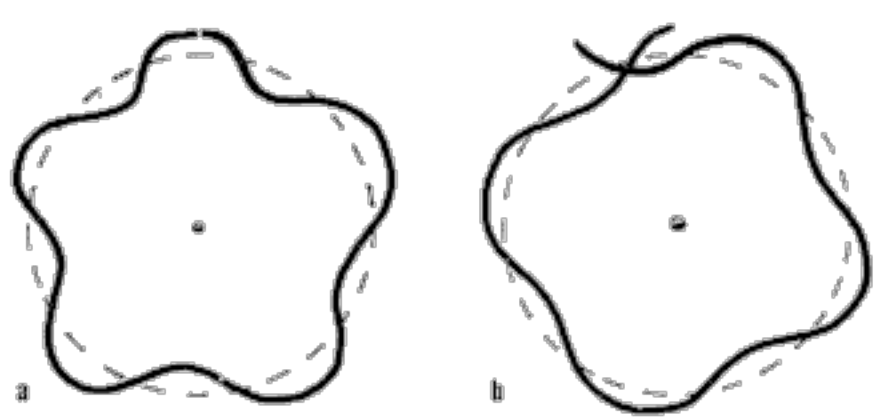
de Broglie, Davisson & Germer

- de Broglie ('24) rend compte de la quantification de Bohr de L par argument d'**interférence constructive d'une onde** de longueur

  $\lambda = h/(m\,v)$

  Incertitude

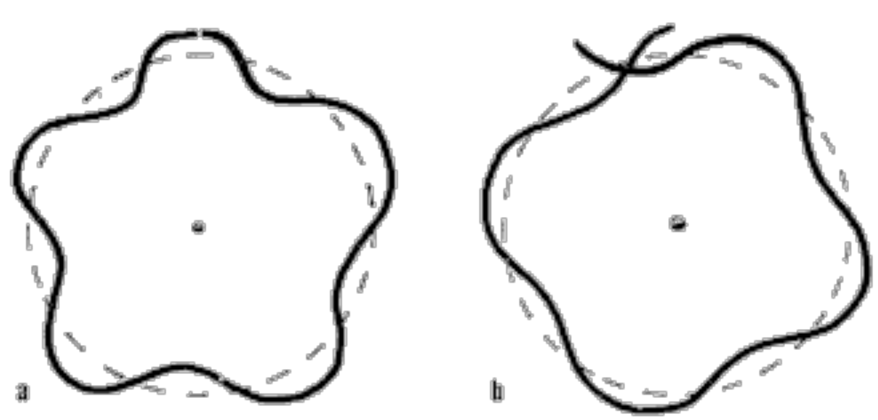
  $\Delta X > \lambda \Leftrightarrow \Delta X\,\Delta V > \hbar/m$



- Pour interférences il faut :

Nécessité lois 1&2: superposition
de Broglie, Davisson & Germer

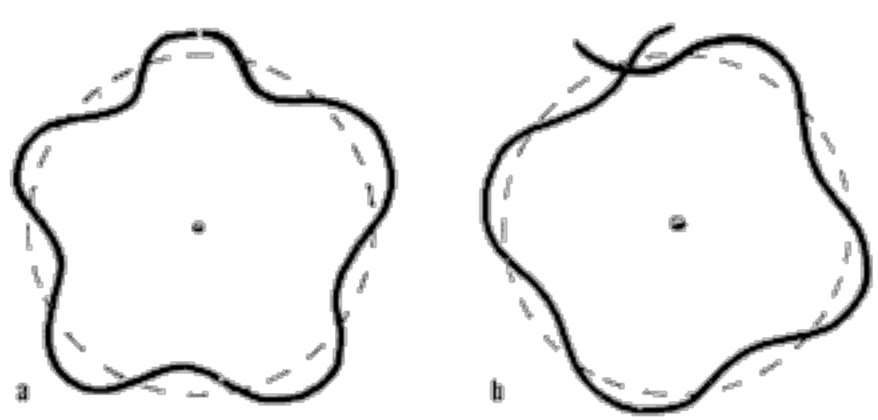
- de Broglie ('24) rend compte de la quantification de Bohr de L par argument d'**interférence constructive d'une onde** de longueur
  $$\lambda = h/(m\,v)$$
  Incertitude
  $\Delta X > \lambda \Leftrightarrow \Delta X \, \Delta V > \hbar/m$



- Pour interférences il faut :
  - une onde associée à l'électron

Nécessité lois 1&2: superposition
de Broglie, Davisson & Germer

- de Broglie ('24) rend compte de la quantification de Bohr de L par argument d'**interférence constructive d'une onde** de longueur
  $$\lambda = h/(m\,v)$$
  Incertitude
  $\Delta X > \lambda \Leftrightarrow \Delta X\,\Delta V > \hbar/m$

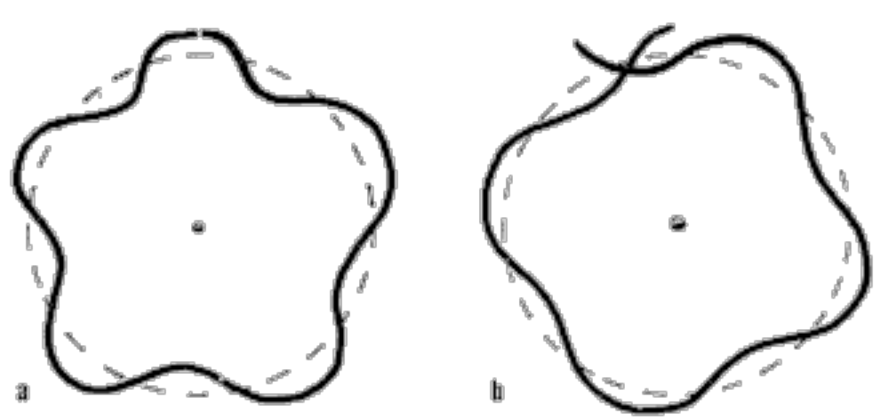


- Pour interférences il faut :
  - une onde associée à l'électron
  - pouvoir superposer ces ondes, comme les produits scalaires de vecteurs

Nécessité lois 1&2: superposition

de Broglie, Davisson & Germer

- de Broglie ('24) rend compte de la quantification de Bohr de L par argument d'**interférence constructive d'une onde** de longueur
  $$\lambda = h/(m\,v)$$
  Incertitude
  $\Delta X > \lambda \Leftrightarrow \Delta X\,\Delta V > \hbar/m$



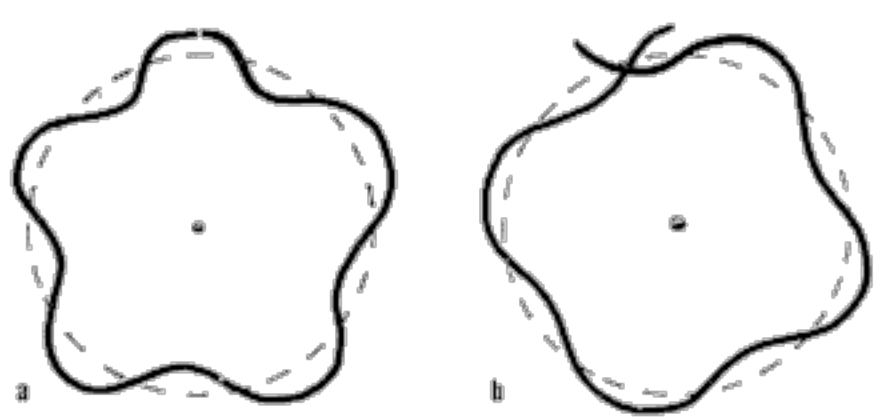
- Pour interférences il faut :
  - une onde associée à l'électron
  - pouvoir superposer ces ondes, comme les produits scalaires de vecteurs

➡ lois 1 & 2

Nécessité lois 1&2: superposition

de Broglie, Davisson & Germer

- de Broglie ('24) rend compte de la quantification de Bohr de L par argument d'**interférence constructive d'une onde** de longueur
  $\lambda = h/(m\,v)$
  Incertitude
  $\Delta X > \lambda \leftrightarrow \Delta X\,\Delta V > \hbar/m$



- Pour interférences il faut :
  - une onde associée à l'électron
  - pouvoir superposer ces ondes, comme les produits scalaires de vecteurs

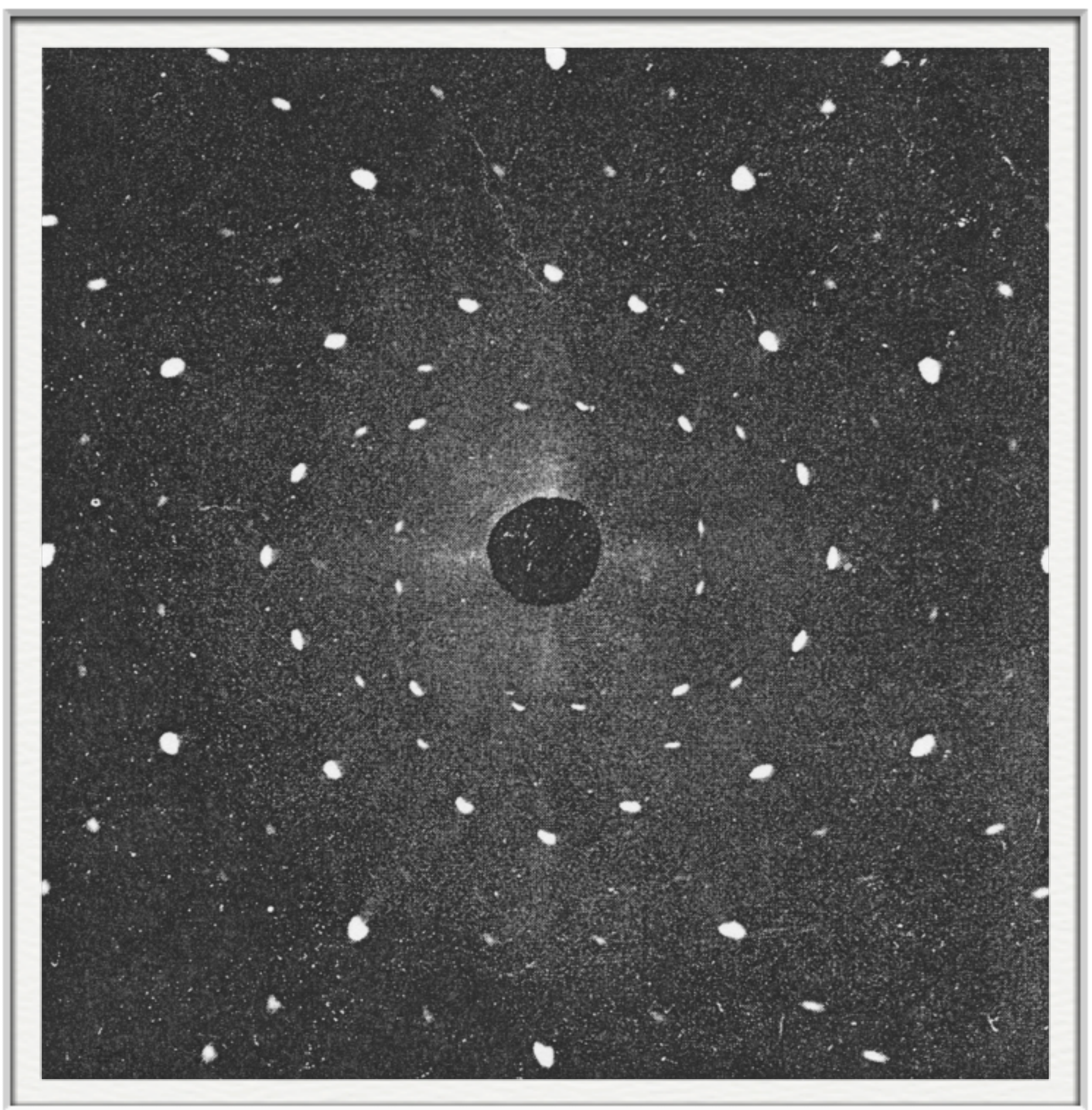
➡ lois 1 & 2

- Vérification: diffractions d'ondes d'électrons ('27), ou de neutrons…

Les neutrons sont des ondes

Diffraction d'un cristal de sel par:

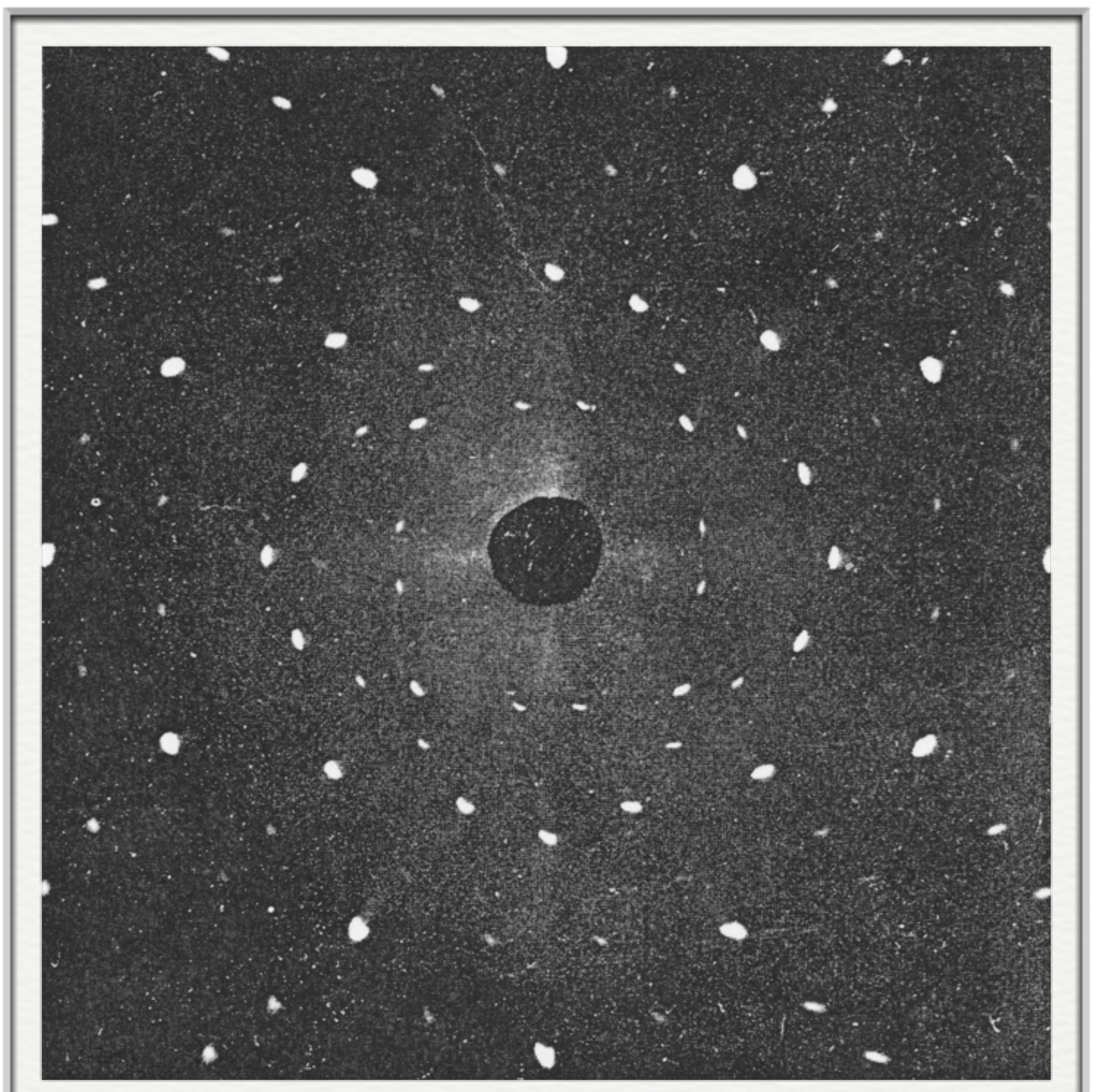
Rayons X



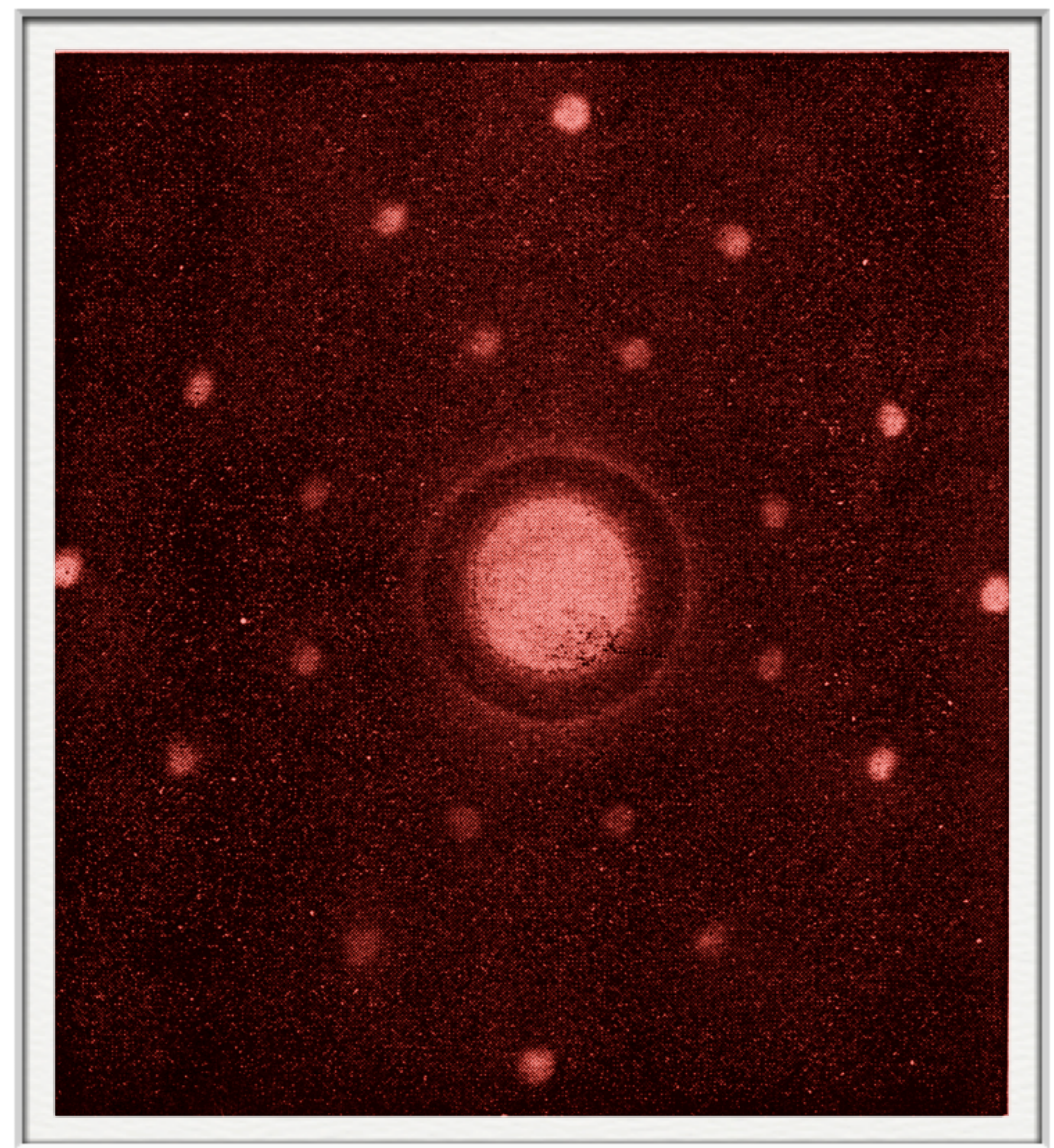
Les neutrons sont des ondes

Diffraction d'un cristal de sel par:

Rayons X



Faisceau de neutrons

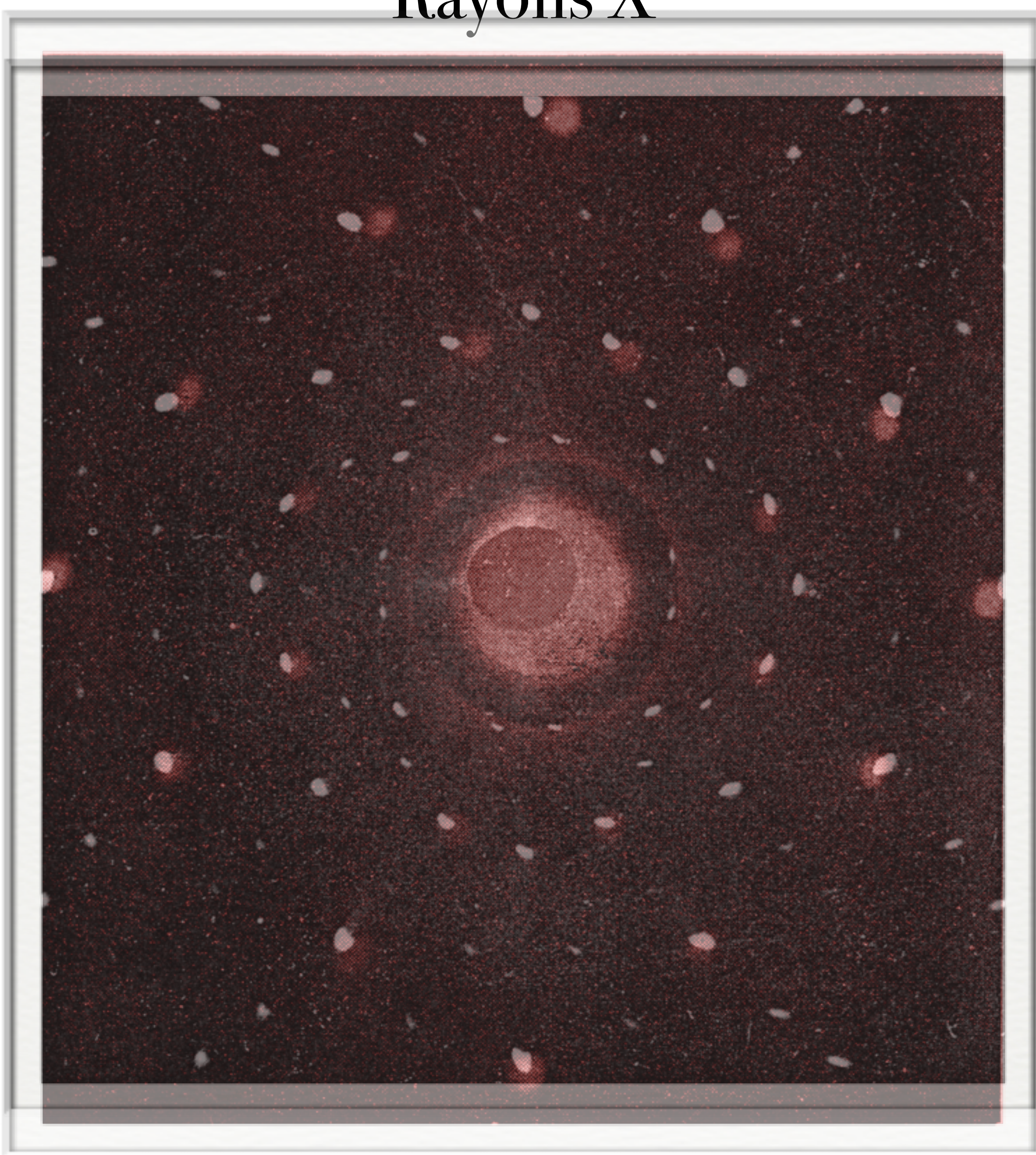


Les neutrons sont des ondes

Diffraction d’un cristal de sel par:

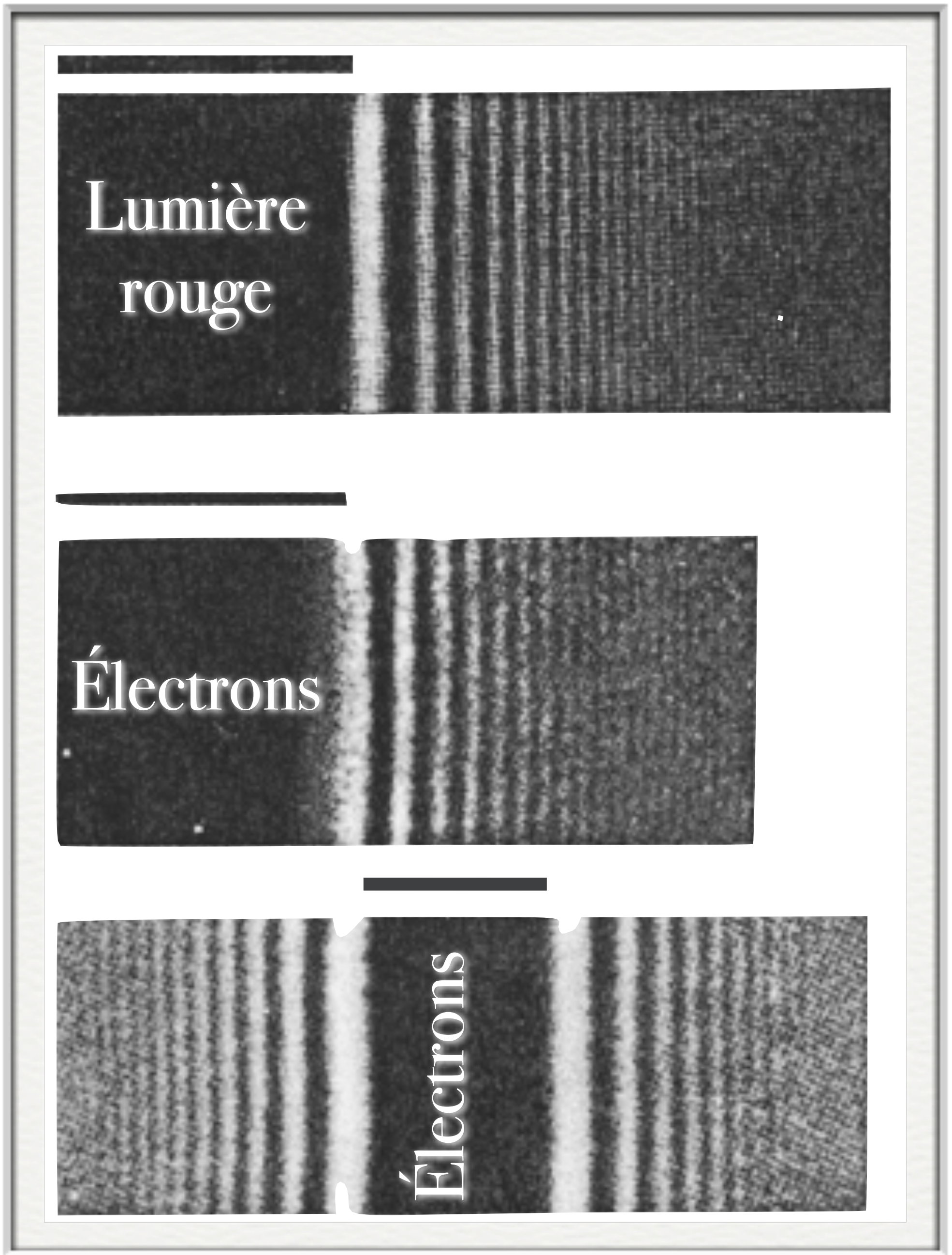
Rayons X

Faisceau de neutrons

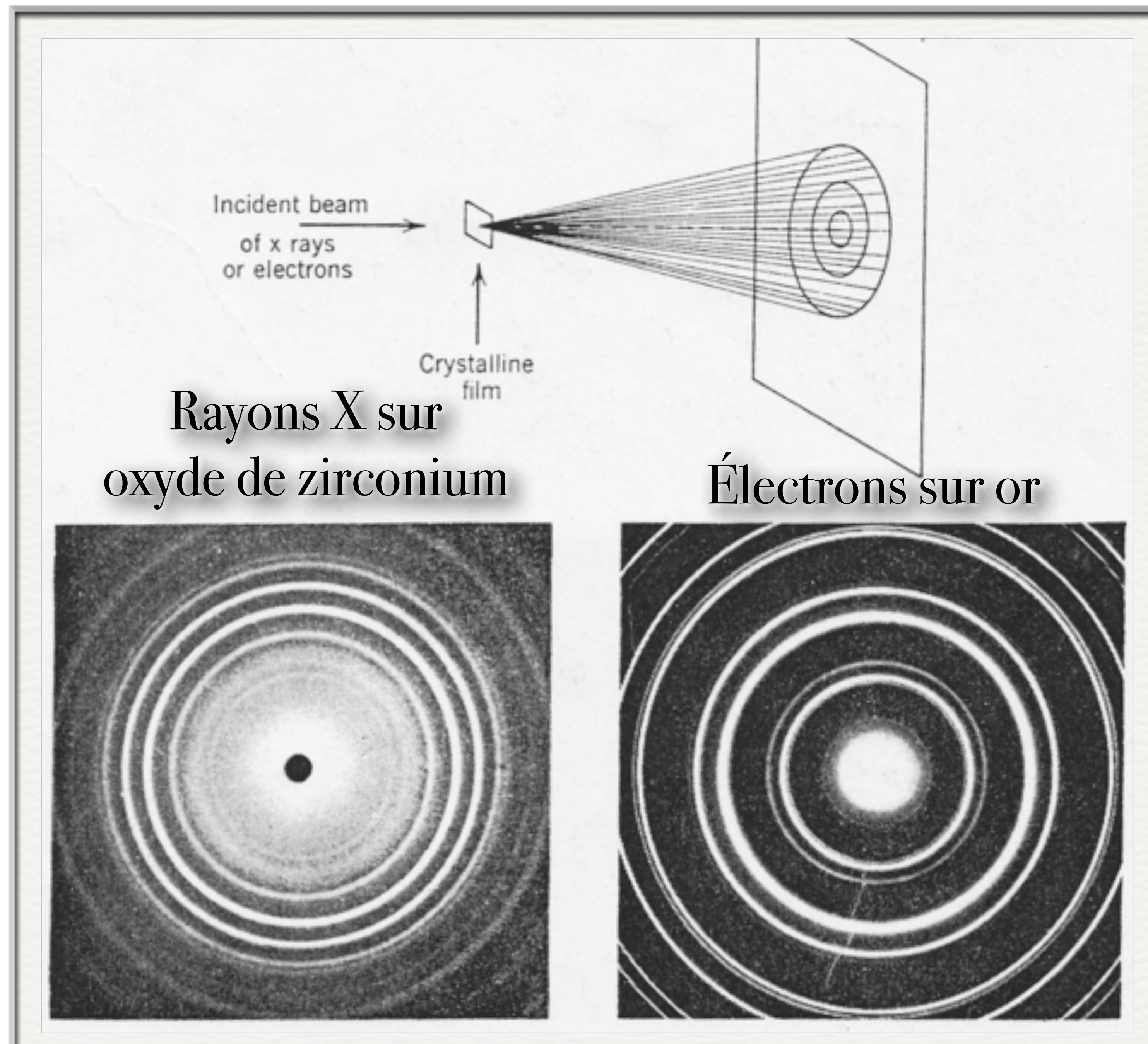


Les électrons sont des ondes

Franges d'interférence
au bord de
l'ombre géométrique

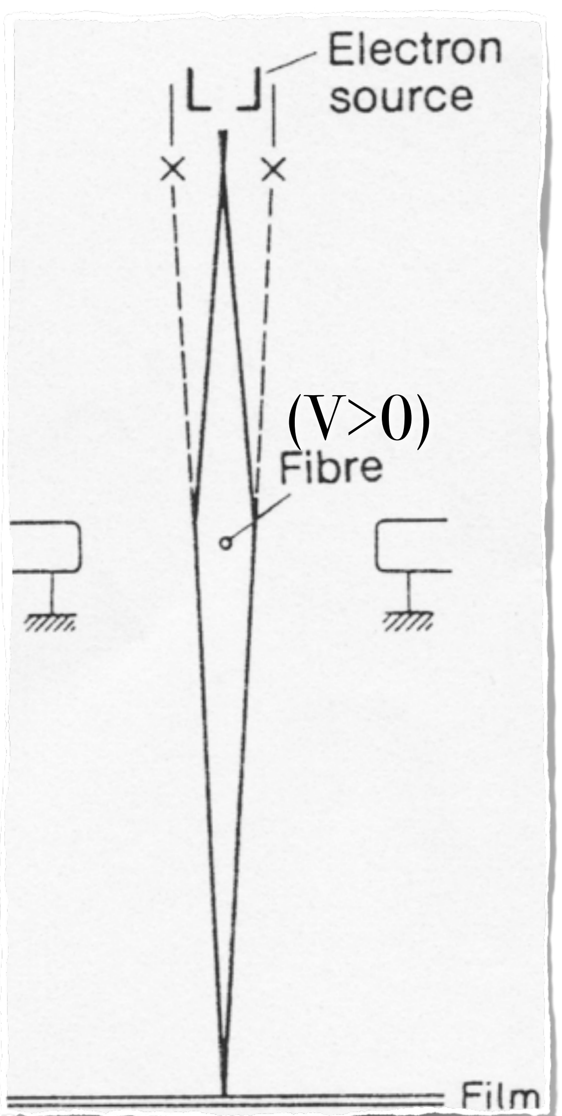


Diffraction Debye-Scherrer



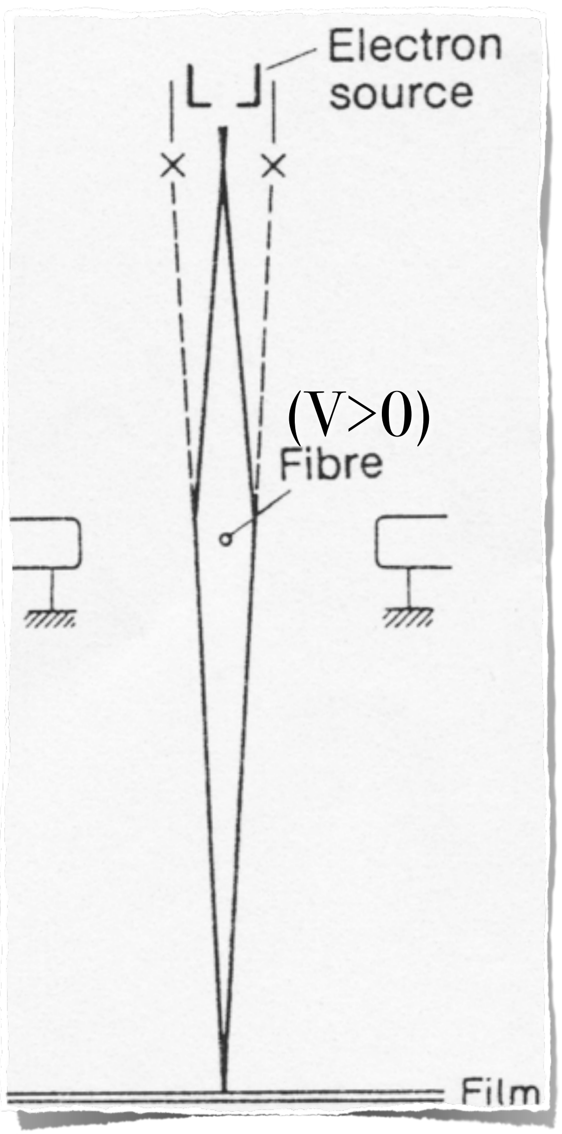
Interférence d'électrons suivant de 2 chemins classiques

Expérience de Jönsson (1961)



Interférence d'électrons suivant de 2 chemins classiques

Expérience de Jönsson (1961)



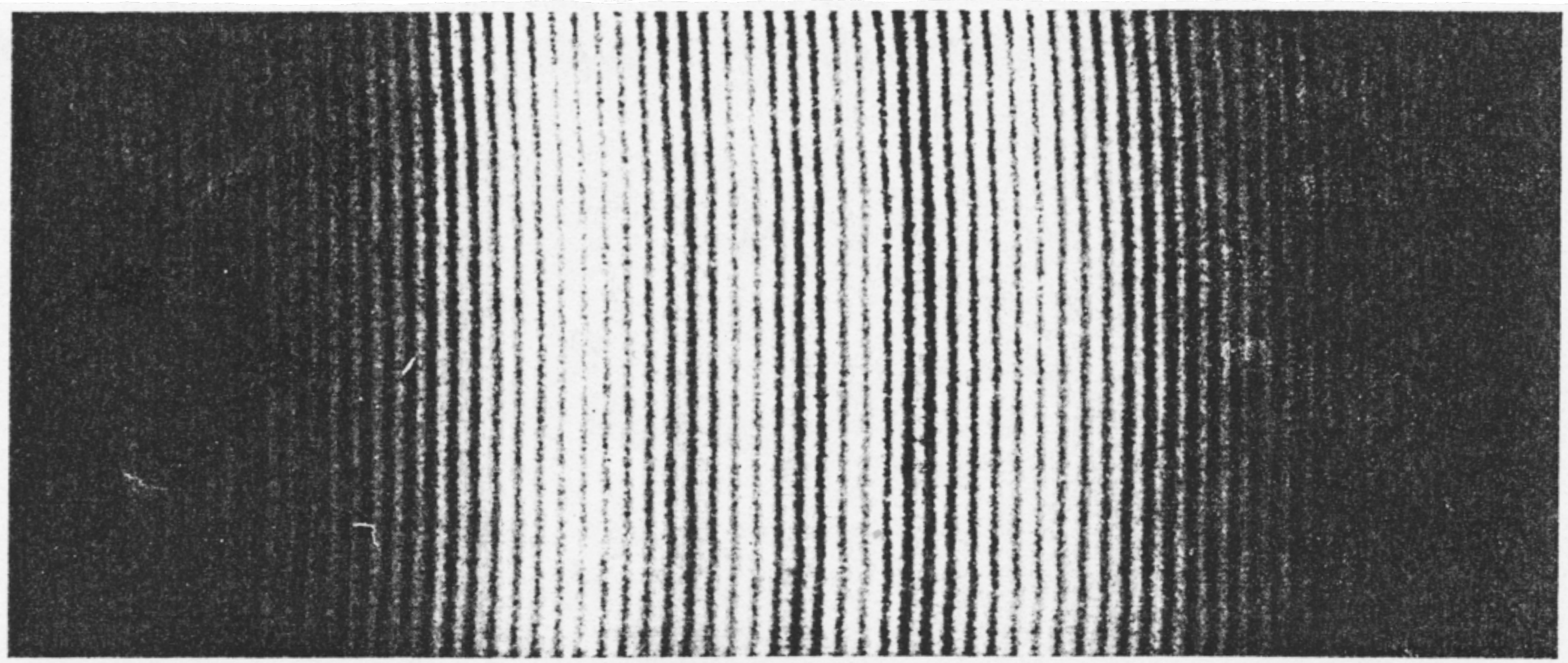
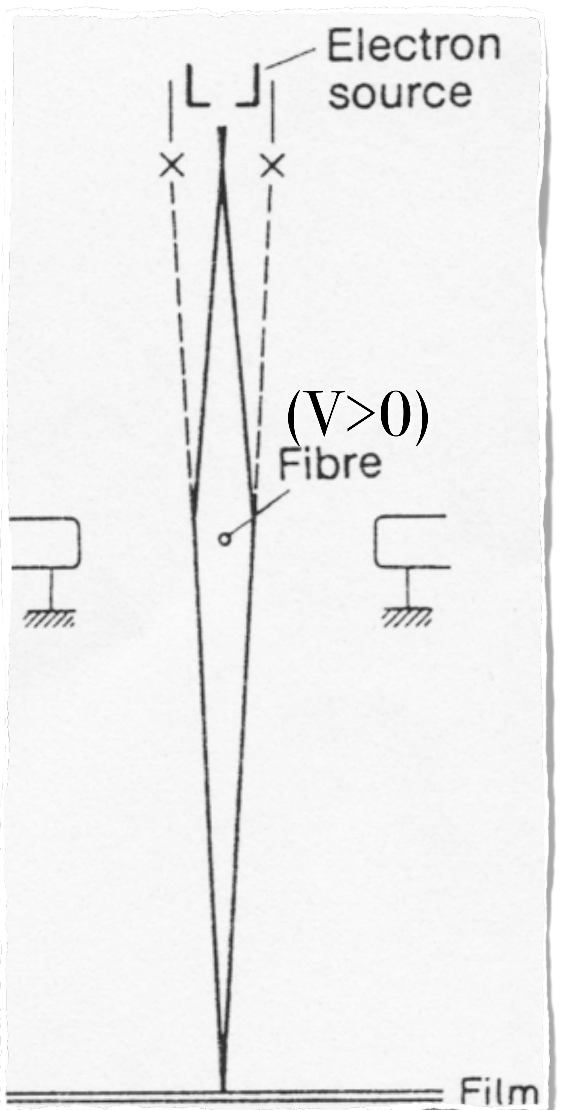


Fig. 6.10. Electron interference from the electrostatic double prism according to *Möllenstedt* and *Düker*. Data from Gerthsen, Kneser, Vogel: *Physik*, 13th ed. (Springer, Berlin, Heidelberg, New York 1977) Fig. 10.69

Interférence d'électrons suivant de 2 chemins classiques

Expérience de Jönsson (1961)



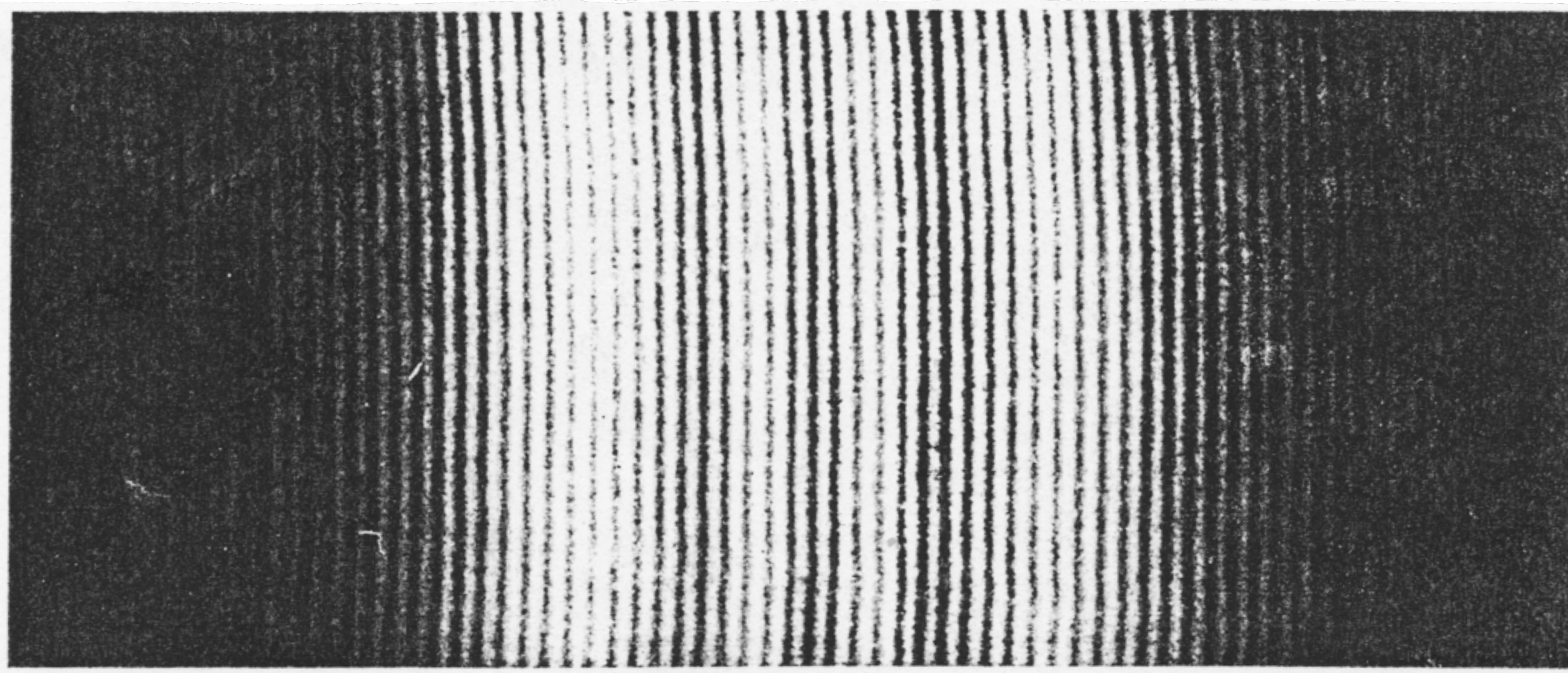


Fig. 6.10. Electron interference from the electrostatic double prism according to *Möllenstedt* and *Düker*. Data from Gerthsen, Kneser, Vogel: *Physik*, 13th ed. (Springer, Berlin, Heidelberg, New York 1977) Fig. 10.69

⇒ électrons se comportent comme ondes !

Mais alors ...

Nécessité lois 2&4: logique

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu′est-ce qui s′étend quand on a une onde d′électron divergente ?

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu′est-ce qui s′étend quand on a une onde d′électron divergente ?
- Ce ne peut être que la probabilité de trouver l′électron.

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu′est-ce qui s′étend quand on a une onde d′électron divergente ?
- Ce ne peut être que la probabilité de trouver l′électron.
- Mais probabilités > 0 : interférence destructives???

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu'est-ce qui s'étend quand on a une onde d'électron divergente ?
- Ce ne peut être que la probabilité de trouver l'électron.
- Mais probabilités > 0 : interférence destructives???

➡ Probabilité = |Amplitude|^2 (Loi 2) + addition amplitudes

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu′est-ce qui s′étend quand on a une onde d′électron divergente ?
- Ce ne peut être que la probabilité de trouver l′électron.
- Mais probabilités > 0 : interférence destructives???

➡ Probabilité = |Amplitude|^2 (Loi 2) + addition amplitudes

- Par extension, toutes mesures probabilistes, pour lisser entre valeurs discrètes (4.b)

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu'est-ce qui s'étend quand on a une onde d'électron divergente ?
- Ce ne peut être que la probabilité de trouver l'électron.
- Mais probabilités > 0 : interférence destructives???

➡ Probabilité = |Amplitude|^2 (Loi 2) + addition amplitudes

- Par extension, toutes mesures probabilistes, pour lisser entre valeurs discrètes (4.b)
- Après la mesure, il peut être cohérent de réduire l'état à la composante mesurée (4.c?)

Nécessité lois 2&4: logique

- On ne trouve jamais de 1/2 électron!
- Qu'est-ce qui s'étend quand on a une onde d'électron divergente ?
- Ce ne peut être que la probabilité de trouver l'électron.
- Mais probabilités > 0 : interférence destructives???

➡ Probabilité = |Amplitude|² (Loi 2) + addition amplitudes

- Par extension, toutes mesures probabilistes, pour lisser entre valeurs discrètes (4.b)
- Après la mesure, il peut être cohérent de réduire l'état à la composante mesurée (4.c?)
- Permet la préparation d'un état bien défini!

Franges de Young particule par particule

Tonomura *et al.* (Hitashi-1989)

Franges de Young particule par particule

Tonomura *et al.* (Hitashi-1989)

Interprétations

″Mondes multiples″ ou Multi-vers d′Everett

"Mondes multiples" ou Multi-vers d'Everett

(Reprise des *mondes possibles*
de Leibniz, si chers à Voltaire…)

″Mondes multiples″ ou Multi-vers d′Everett

(Reprise des *mondes possibles* de Leibniz, si chers à Voltaire…)

- Lors d′une mesure, que deviennent les possibilités non-mesurées?

"Mondes multiples" ou Multi-vers d'Everett

(Reprise des *mondes possibles* de Leibniz, si chers à Voltaire…)

- Lors d'une mesure, que deviennent les possibilités non-mesurées?

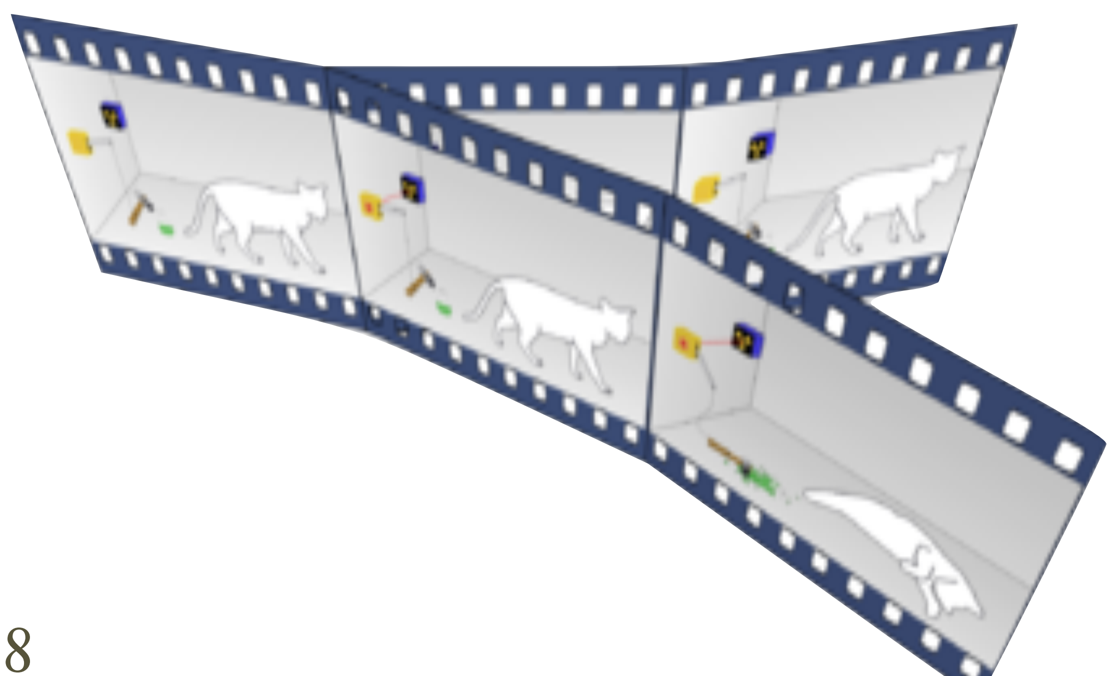
- Au lieu de les détruire (loi 4), Everett voit chaque mesure comme une bifurcation entre des mondes possibles où chaque possibilité se réalise

"Mondes multiples" ou Multi-vers d'Everett

(Reprise des *mondes possibles* de Leibniz, si chers à Voltaire…)

- Lors d'une mesure, que deviennent les possibilités non-mesurées?

- Au lieu de les détruire (loi 4), Everett voit chaque mesure comme une bifurcation entre des mondes possibles où chaque possibilité se réalise

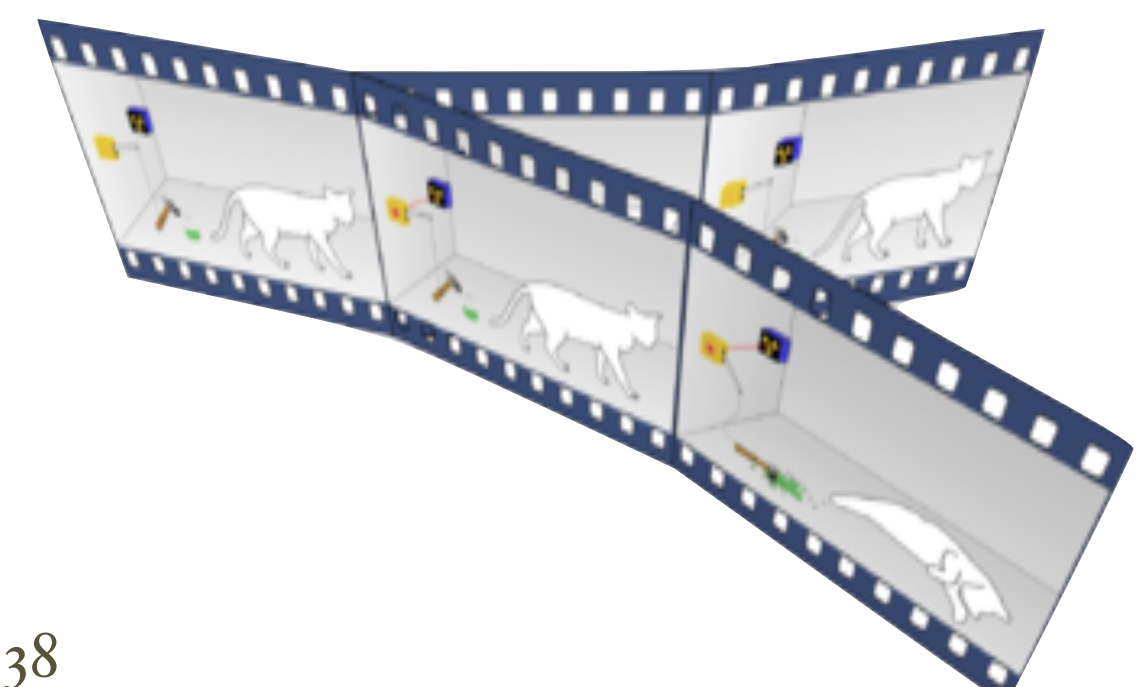


"Mondes multiples" ou Multi-vers d'Everett

(Reprise des *mondes possibles* de Leibniz, si chers à Voltaire…)

- Lors d'une mesure, que deviennent les possibilités non-mesurées?
- Au lieu de les détruire (loi 4), Everett voit chaque mesure comme une bifurcation entre des mondes possibles où chaque possibilité se réalise

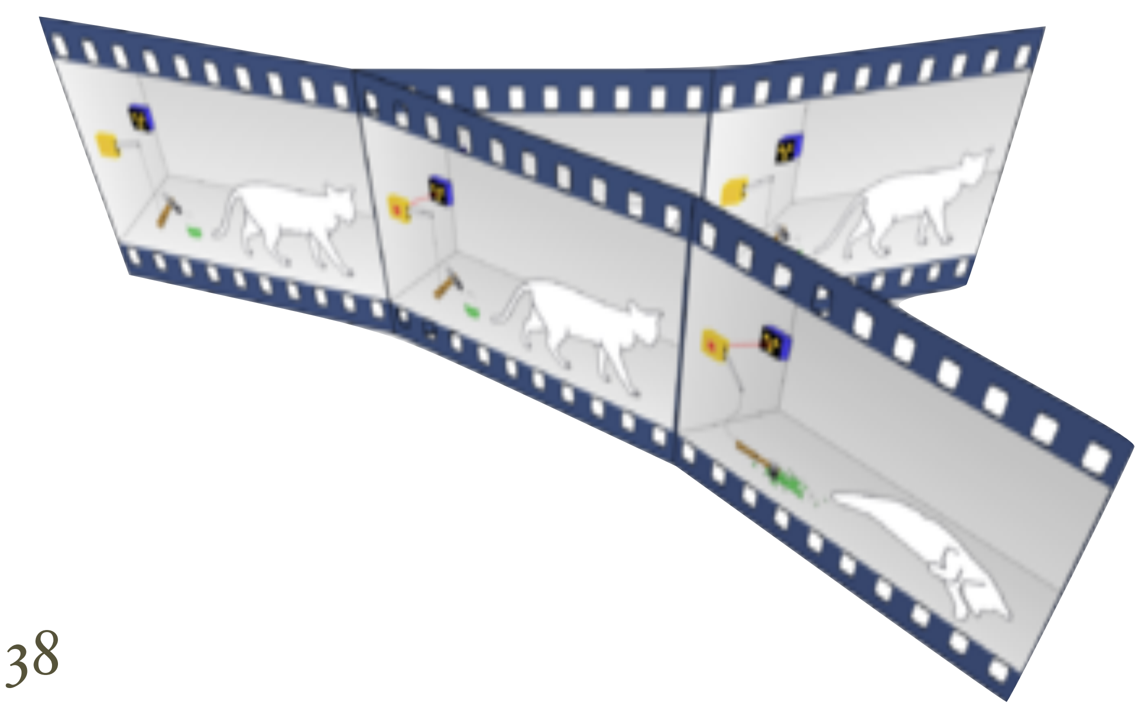
- Ensuite, chaque monde n'interagit plus avec ses copies



"Mondes multiples" ou Multi-vers d'Everett

(Reprise des *mondes possibles* de Leibniz, si chers à Voltaire…)

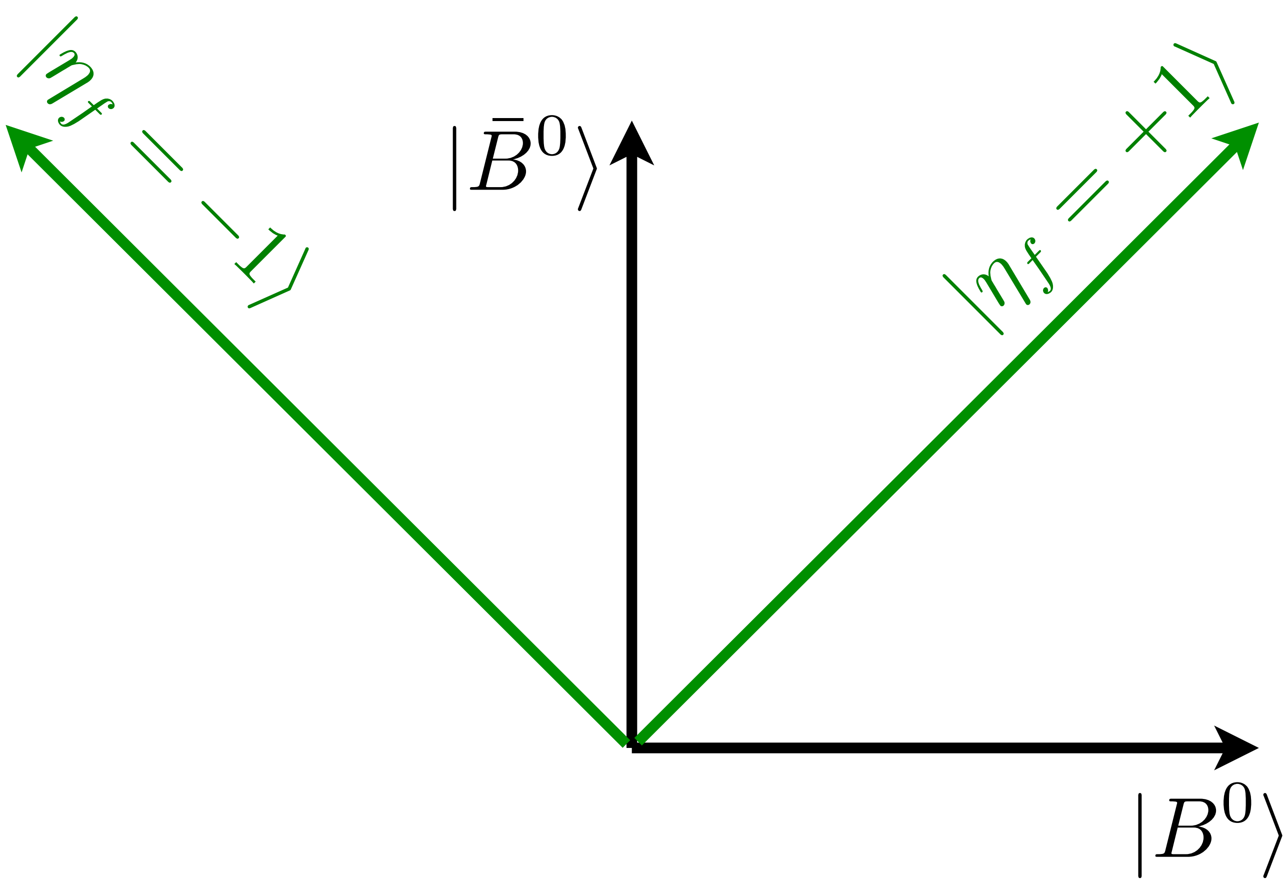
- Lors d'une mesure, que deviennent les possibilités non-mesurées?
- Au lieu de les détruire (loi 4), Everett voit chaque mesure comme une bifurcation entre des mondes possibles où chaque possibilité se réalise
- Ensuite, chaque monde n'interagit plus avec ses copies
- Intéressante, mais ré-interprétation sans effet mesurable nouveau (sauf si état cohérent macroscopique)

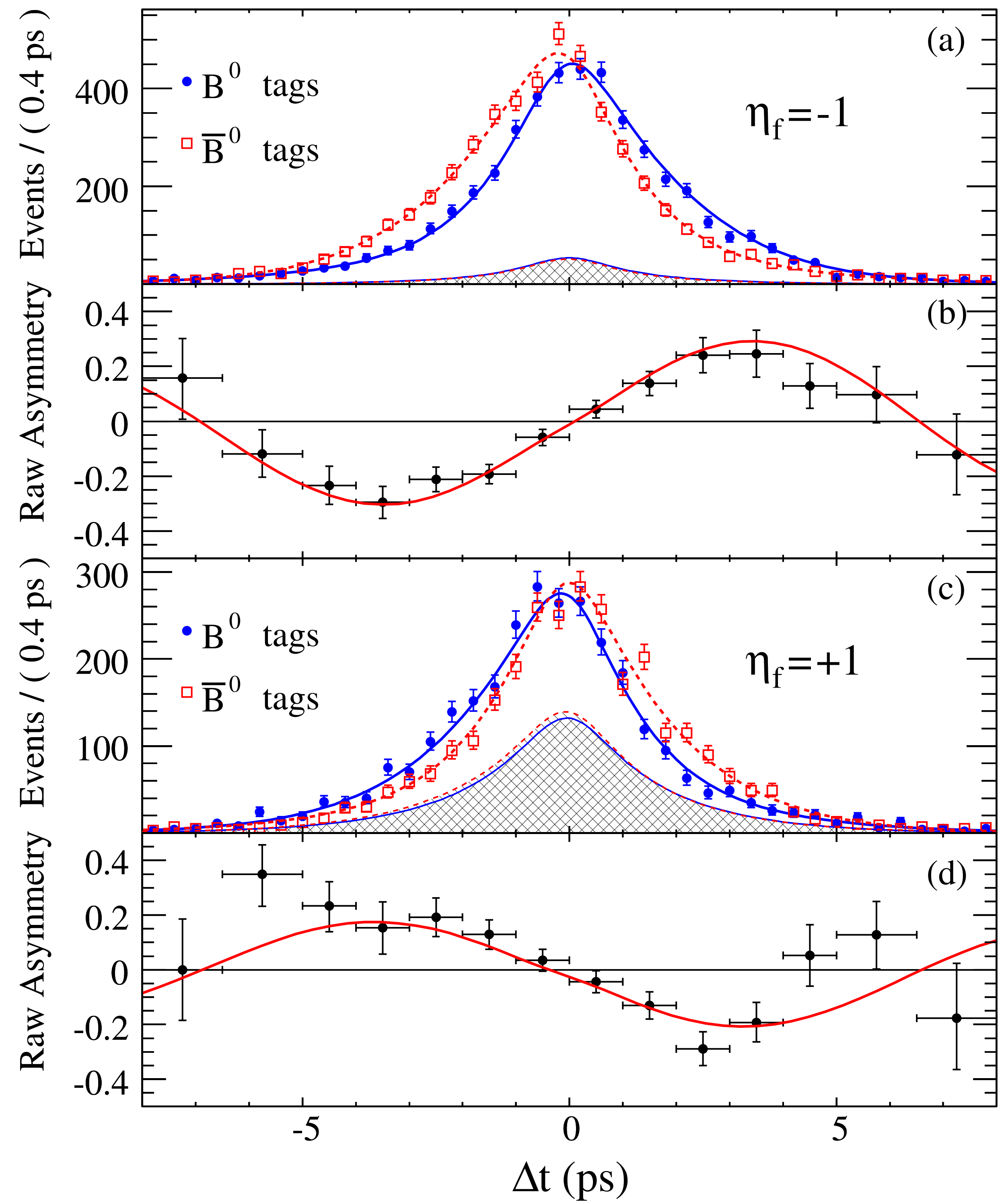


Utilisation et développements récents - futurs

EPR et Violation de CP dans le mélange $B_0 - \bar{B}_0$.

BaBar ′09: produit 465M de paires EPR de quarks b anti-b:





Cryptographie quantique
(Bennett, Brassard′84)

Cryptographie quantique
(Bennett, Brassard'84)

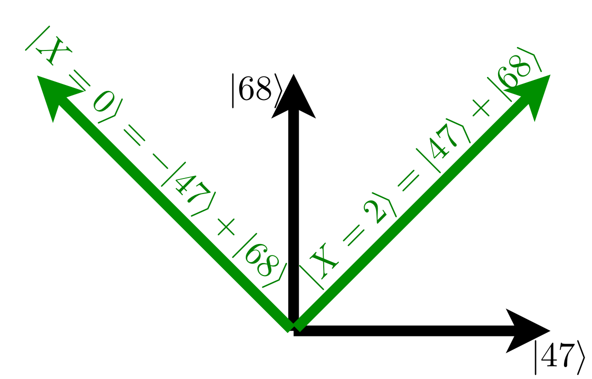
- Si mesure perturbe système, interception d'un message détectable

Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x = 2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x = 0\rangle$

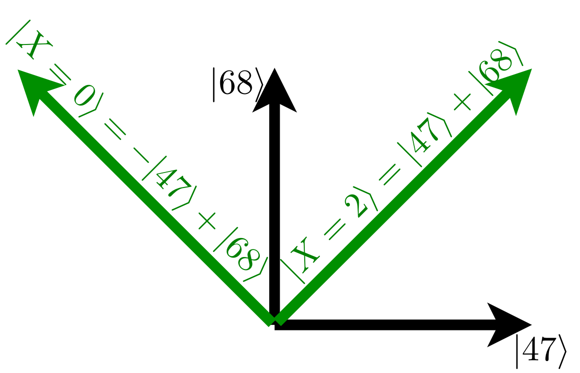
Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |\,68\rangle$ ou $|x = 2\rangle$
  $0 \Leftrightarrow |\,47\rangle$ ou $|x = 0\rangle$



Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x=2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x=0\rangle$
- Roger (ou espion) reçoit un à un et mesure au hasard V ou X



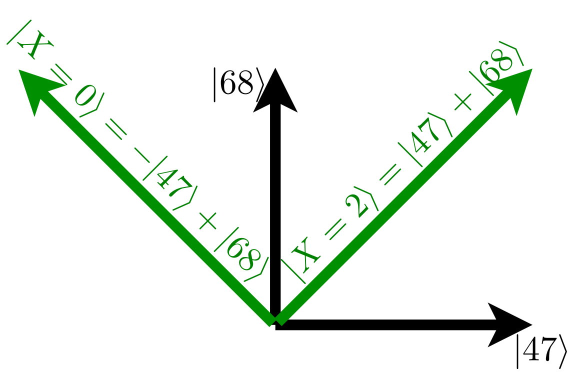
Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable

- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x=2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x=0\rangle$

- Roger (ou espion) reçoit un à un et mesure au hasard V ou X

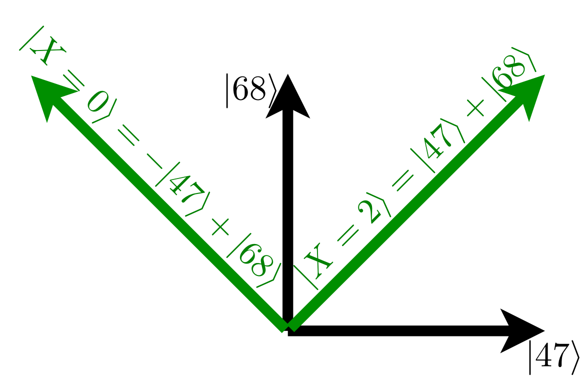
- (L′espion ré-émet l′état qu′il a mesuré, ≠ initial 50% des fois, mesuré ≠ par Roger 25% des fois)



Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x=2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x=0\rangle$
- Roger (ou espion) reçoit un à un et mesure au hasard V ou X
- (L′espion ré-émet l′état qu′il a mesuré, ≠ initial 50% des fois, mesuré ≠ par Roger 25% des fois)

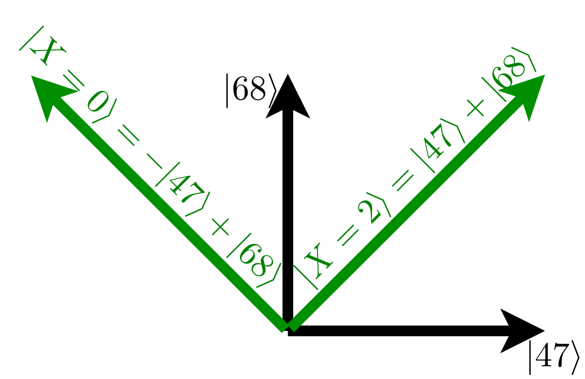
- Emile envoie en clair la liste des 2N codages utilisés: $VXVVXXXV$...



Cryptographie quantique

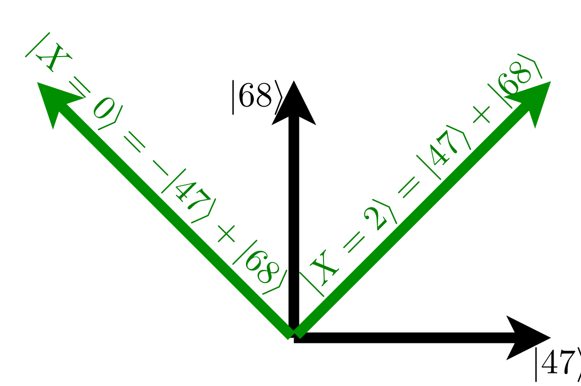
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x = 2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x = 0\rangle$
- Roger (ou espion) reçoit un à un et mesure au hasard V ou X
- (L′espion ré-émet l′état qu′il a mesuré, ≠ initial 50% des fois, mesuré ≠ par Roger 25% des fois)
- Emile envoie en clair la liste des 2N codages utilisés: $VXVVXXXV$...
- Roger garde en moyenne N bonnes mesures, et les communique en clair.



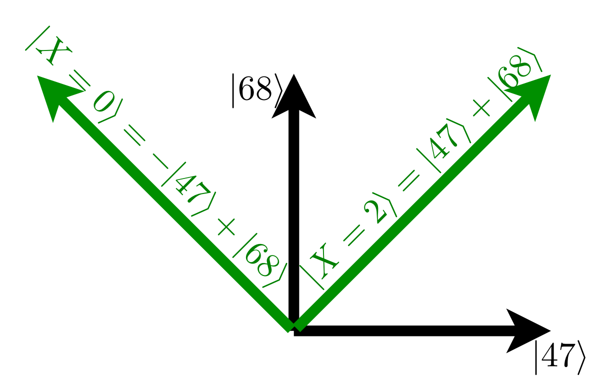
Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x = 2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x = 0\rangle$
- Roger (ou espion) reçoit un à un et mesure au hasard V ou X
- (L′espion ré-émet l′état qu′il a mesuré, ≠ initial 50% des fois, mesuré ≠ par Roger 25% des fois)
- Emile envoie en clair la liste des 2N codages utilisés: $VXVVXXXV$...
- Roger garde en moyenne N bonnes mesures, et les communique en clair.
- Emile renvoie en clair un sous-ensemble de n bits



Cryptographie quantique
(Bennett, Brassard′84)

- Si mesure perturbe système, interception d′un message détectable
- Emile émet 2N bits codés aléatoirement:
  $1 \Leftrightarrow |68\rangle$ ou $|x=2\rangle$
  $0 \Leftrightarrow |47\rangle$ ou $|x=0\rangle$
- Roger (ou espion) reçoit un à un et mesure au hasard V ou X
- (L′espion ré-émet l′état qu′il a mesuré, ≠ initial 50% des fois, mesuré ≠ par Roger 25% des fois)
- Emile envoie en clair la liste des 2N codages utilisés: $VXVVXXXV$...
- Roger garde en moyenne N bonnes mesures, et les communique en clair.
- Emile renvoie en clair un sous-ensemble de n bits
- Un espion n′a que 3^n chances sur 4^n d′intercepter sans être détecté



Les promesses d'un ordinateur quantique

Les promesses d'un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1

Les promesses d'un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1
- un seul calcul avec superp. quantique de **n q-bits** peut couvrir 2^n possibilités *à la fois*

Les promesses d'un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1
- un seul calcul avec superp. quantique de **n q-bits** peut couvrir 2^n possibilités *à la fois*
- Problèmes de complexité N ″non-résolus″ si $t_{calcul} \sim e^N$

Les promesses d'un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1
- un seul calcul avec superp. quantique de **n q-bits** peut couvrir 2^n possibilités *à la fois*
- Problèmes de complexité N "non-résolus" si $t_{calcul} \sim e^N$
- **Résolus avec n=N q-bits !!!**

Les promesses d′un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1
- un seul calcul avec superp. quantique de **n q-bits** peut couvrir 2^n possibilités *à la fois*
- Problèmes de complexité N ″non-résolus″ si $t_{calcul} \sim e^N$
- **Résolus avec n=N q-bits !!!**

- Les algorithmes quantiques existent! Reste l′ordinateur.

Les promesses d'un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1
- un seul calcul avec superp. quantique de **n q-bits** peut couvrir 2^n possibilités *à la fois*
- Problèmes de complexité N "non-résolus" si $t_{calcul} \sim e^N$
- **Résolus avec n=N q-bits !!!**

- Les algorithmes quantiques existent! Reste l'ordinateur.
- Problèmes actuels:

Les promesses d'un ordinateur quantique

- 1 état quantique binaire **q-bit** peut être *à la fois* dans une superposition de 0 et 1
- un seul calcul avec superp. quantique de **n q-bits** peut couvrir 2^n possibilités *à la fois*
- Problèmes de complexité N "non-résolus" si $t_{calcul} \sim e^N$
- **Résolus avec n=N q-bits !!!**

- Les algorithmes quantiques existent! Reste l'ordinateur.
- Problèmes actuels:
  - on arrive à maintenir la cohérence quantique entre n q-bits que pendant $t_{coh} \sim e^{-n}$ (chat de Schrödinger...)