

Protocole E91

Ibrahim Chegrane

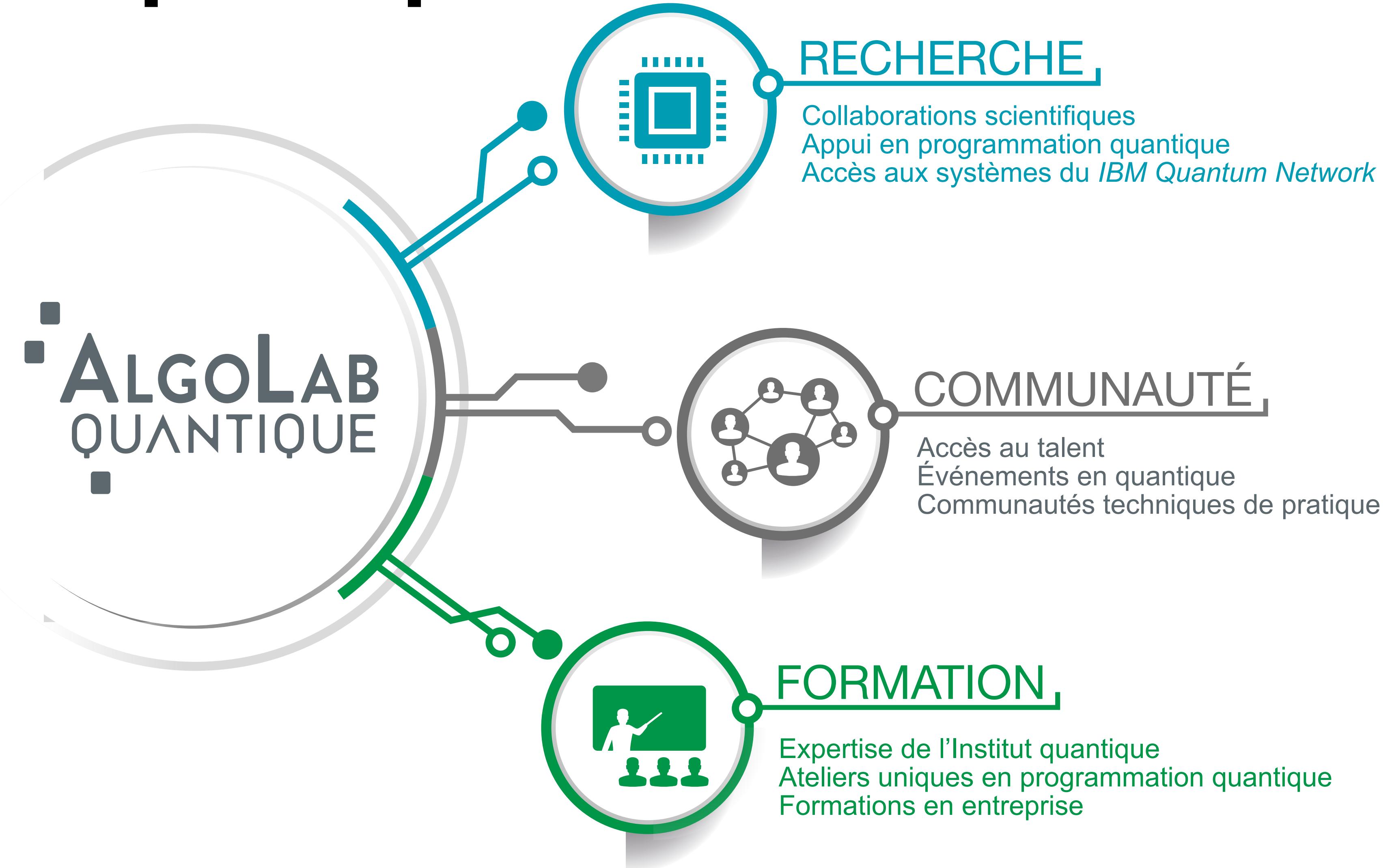
ibrahim.Chegrane@USherbrooke.ca

26 Février 2026

Qui sommes-nous?



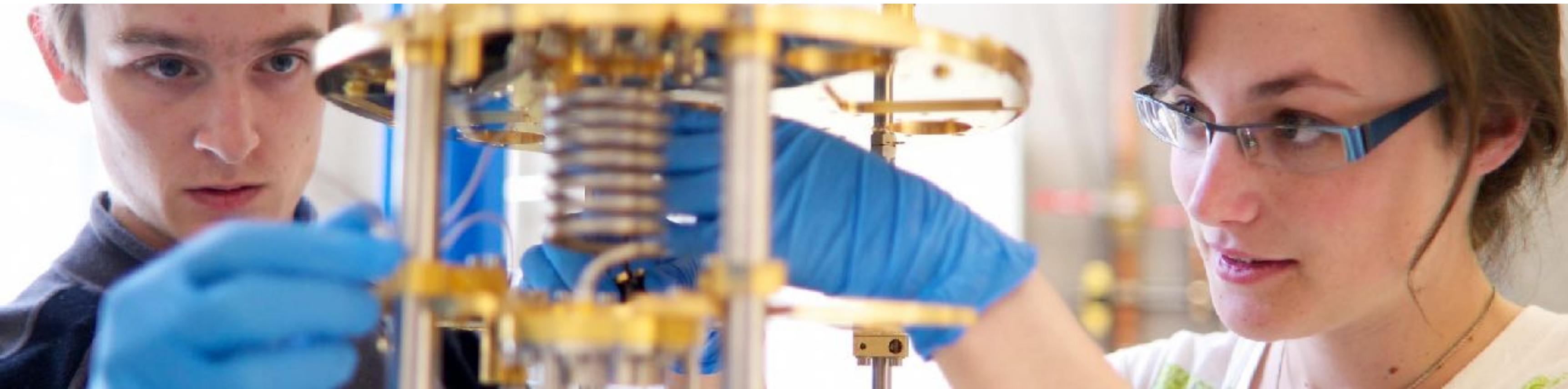
AlgoLab quantique



Nous contacter : AlgoLabquantique@usherbrooke.ca

Institut quantique

Nous plaçons les **250 étudiantes et étudiants** au centre de la recherche dans un environnement ouvert et collaboratif pour **accélérer** le passage **de la science aux technologies quantiques**.



Nos **32 membres du corps professoral** proviennent de 4 facultés et 7 départements
80M\$ investis en 10 ans et un **nouveau bâtiment depuis 2021**

Premier baccalauréat en sciences quantiques au Québec



Nouvelle cohorte à l'automne 2026

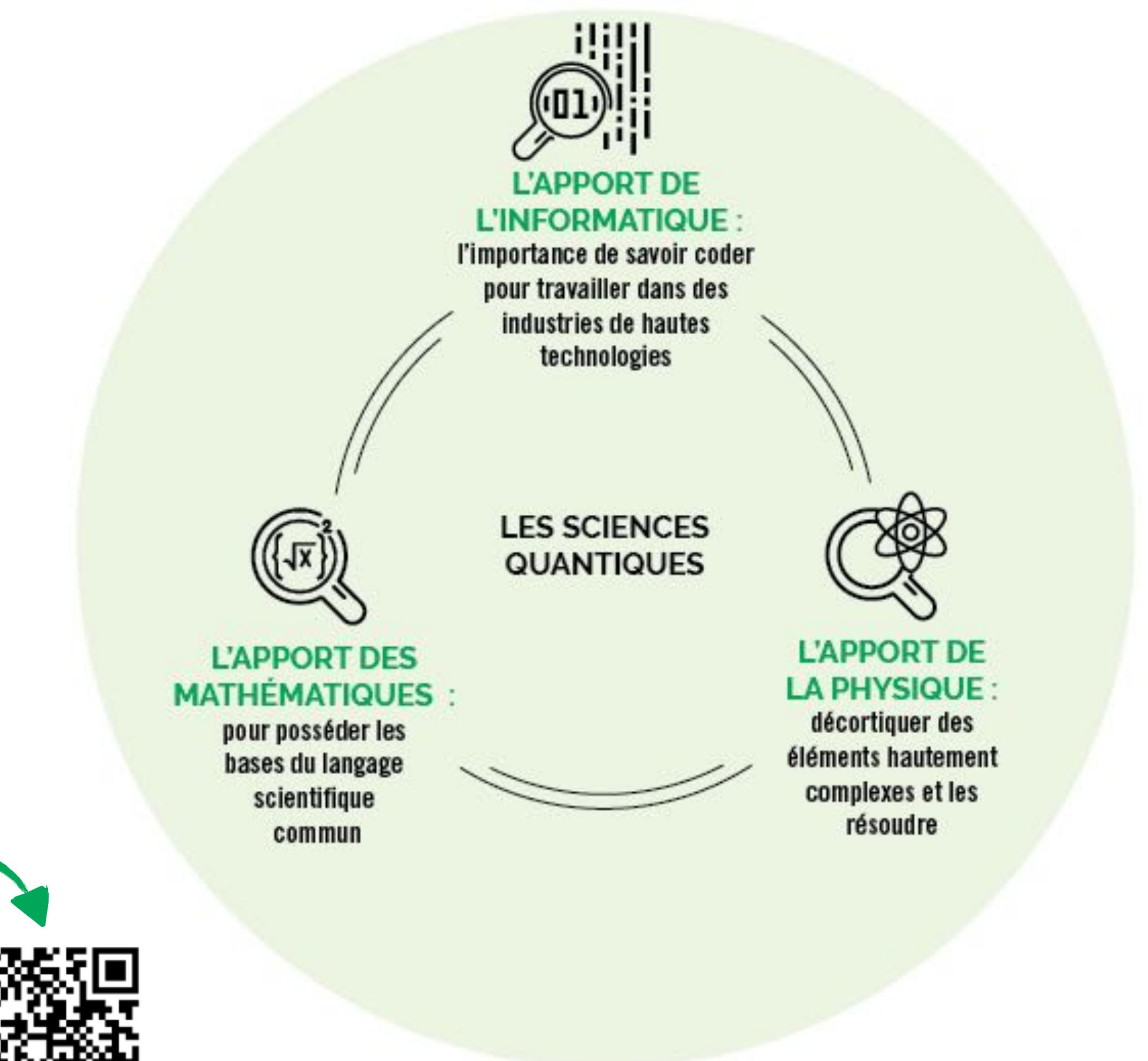
Formation professionnalisante

- Programme interdisciplinaire
- Parcours coop
- Projets intégrateurs

Pour en savoir plus

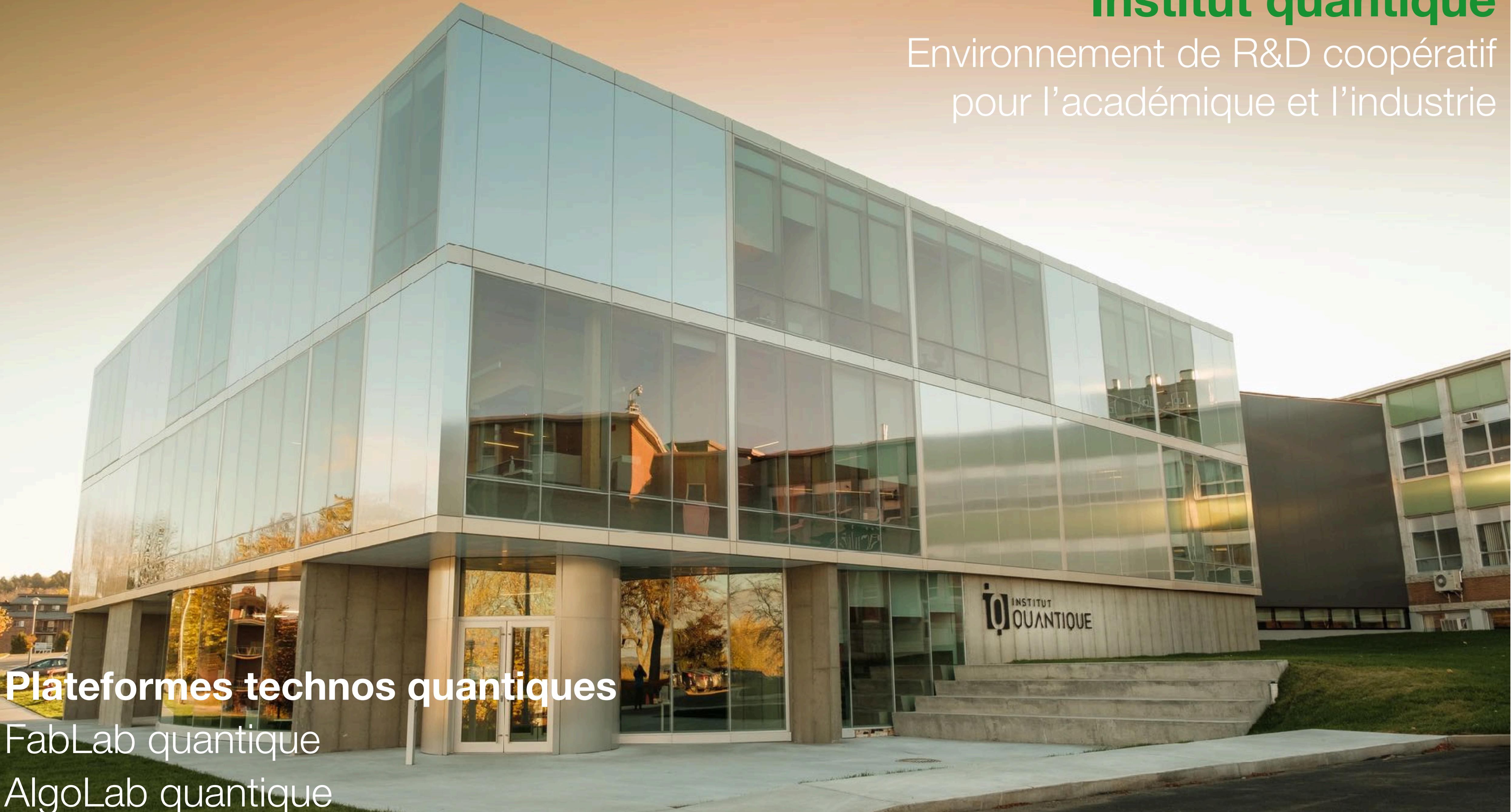


Université de
Sherbrooke



Institut quantique

Environnement de R&D coopératif
pour l'académique et l'industrie



Plateformes technos quantiques

FabLab quantique

AlgoLab quantique

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d'information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- ➊ Présentation
- Cryptographie
- Le qubit
- Le photon: messager d'information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

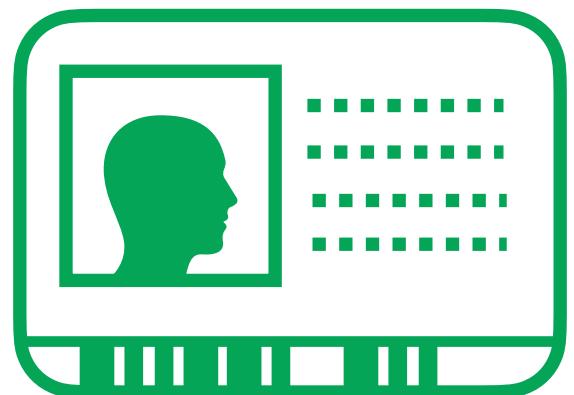
- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

Cryptographie

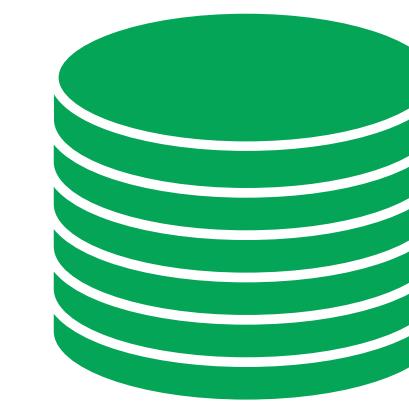
Confidentialité



Authenticité

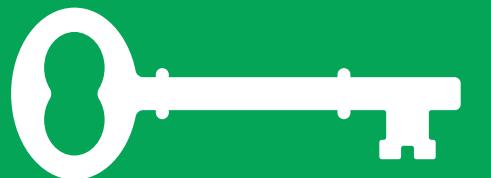


Intégrité

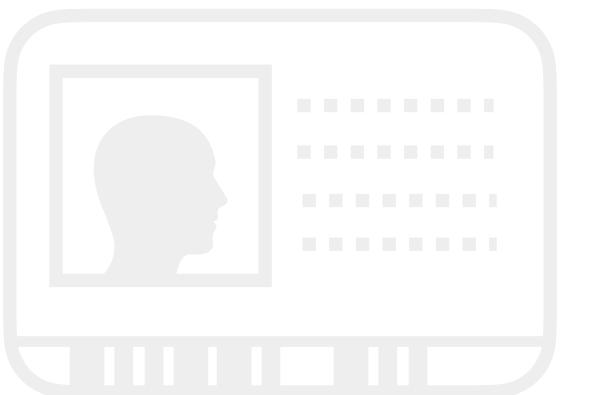


Cryptographie

Confidentialité



Authenticité



Intégrité



Cryptographie

Confidentialité

But: Assurer que le message soit inaccessible à un espion!



Cryptographie

Confidentialité

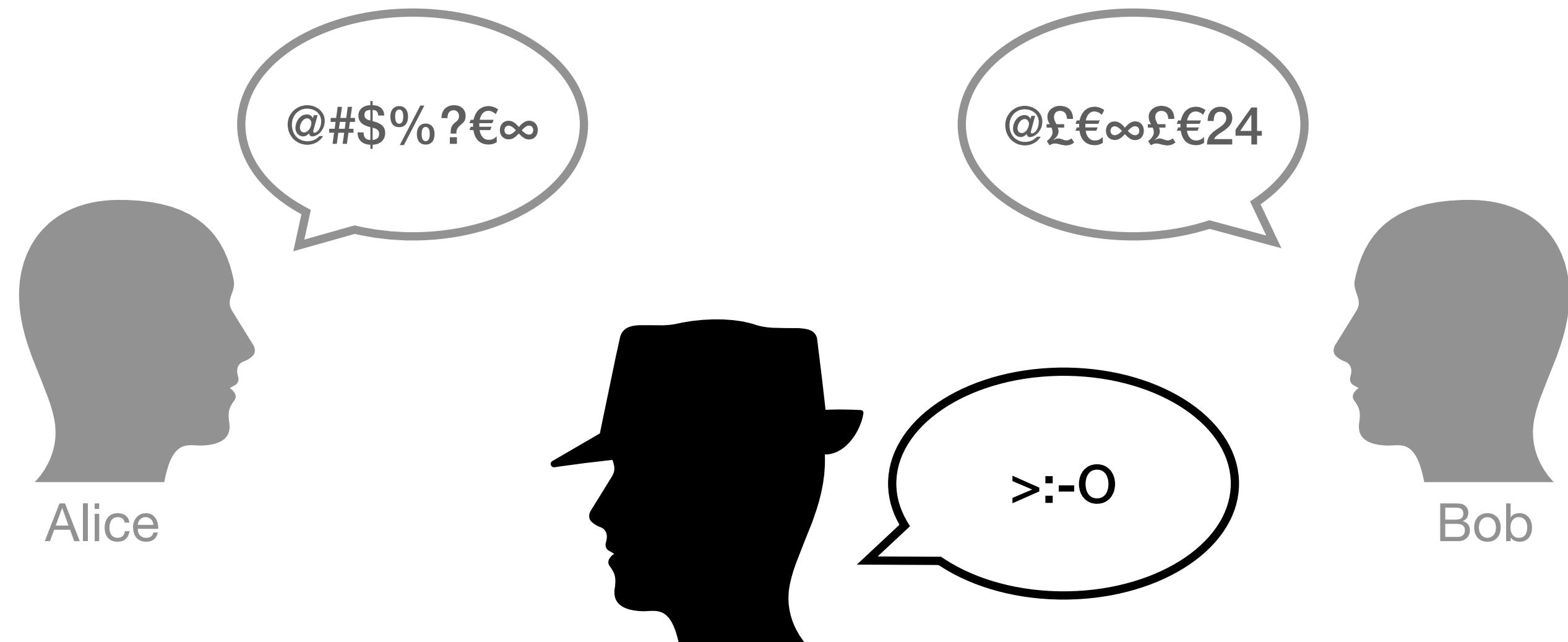
But: Assurer que le message soit inaccessible à un espion!



Cryptographie

Confidentialité

But: Assurer que le message soit inaccessible à un espion!



Clé symétrique



Clé symétrique



Clé symétrique



Clé symétrique



Clé symétrique

Caractéristiques

- une seule clé (privée) pour chiffrer et déchiffrer



Clé symétrique

Caractéristiques

- une seule clé (privée) pour chiffrer et déchiffrer

Avantages

- rapide et nécessite peu de ressource de calcul



Clé symétrique

Caractéristiques

- une seule clé (privée) pour chiffrer et déchiffrer

Avantages

- rapide et nécessite peu de ressource de calcul

Inconvénients

- distribution de la clé



Clé symétrique

Caractéristiques

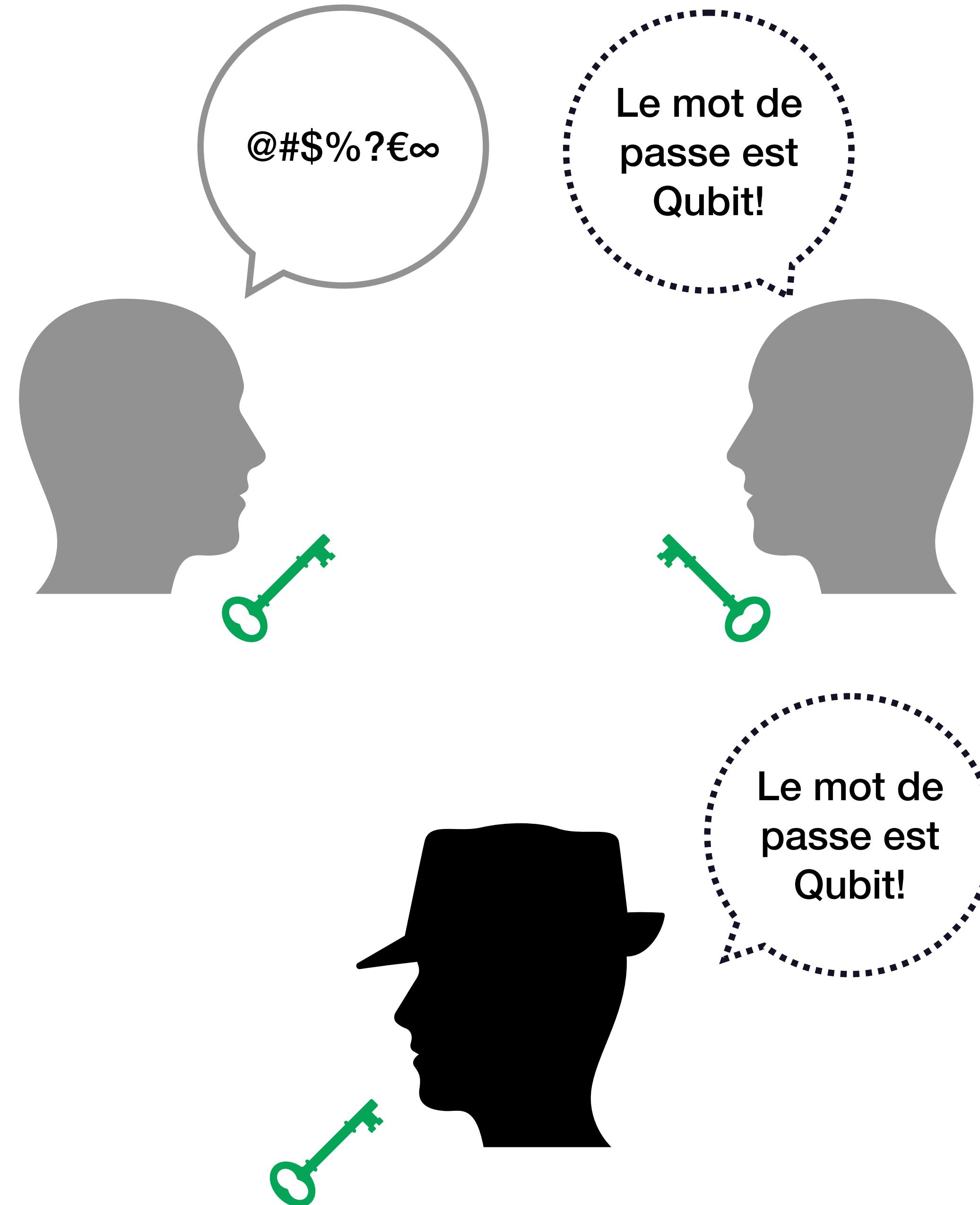
- une seule clé (privée) pour chiffrer et déchiffrer

Avantages

- rapide et nécessite peu de ressource de calcul

Inconvénients

- distribution de la clé



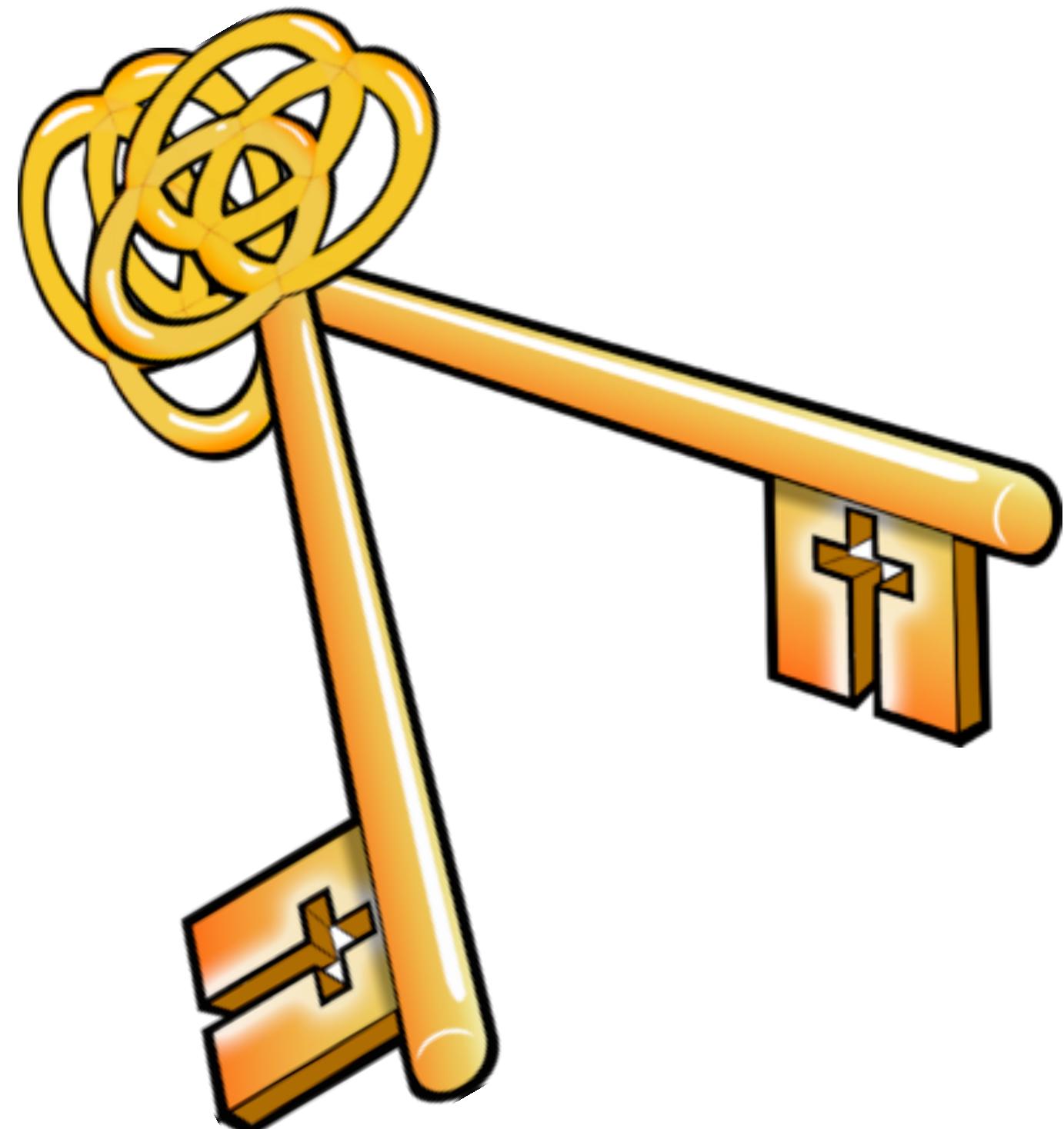
Clé asymétrique

Caractéristiques

- une clé publique pour chiffrer et une clé privée pour déchiffrer



Clé asymétrique



Caractéristiques

- une clé publique pour chiffrer et une clé privée pour déchiffrer

Avantages

- distribution de la clé publique

Clé asymétrique



Caractéristiques

- une clé publique pour chiffrer et une clé privée pour déchiffrer

Avantages

- distribution de la clé publique

Inconvénients

- lent et coûteux en ressources de calcul

Motivation

Cryptographie quantique



Motivation

Cryptographie quantique



Déchiffrer des messages

- Protocole de chiffrement asymétrique (p.e. RSA avec algorithme de Shor)
- Protocole de chiffrement symétrique (p.e. AES avec algorithme de Grover)

Motivation

Cryptographie quantique



Déchiffrer des messages

- Protocole de chiffrement asymétrique (p.e. RSA avec algorithme de Shor)
- Protocole de chiffrement symétrique (p.e. AES avec algorithme de Grover)



Cryptographie quantique

Cryptographie quantique

Méthodes de cryptographie exploitant les propriétés de la mécanique quantique telles que

La superposition

Le théorème de non-clonage

L'intrication



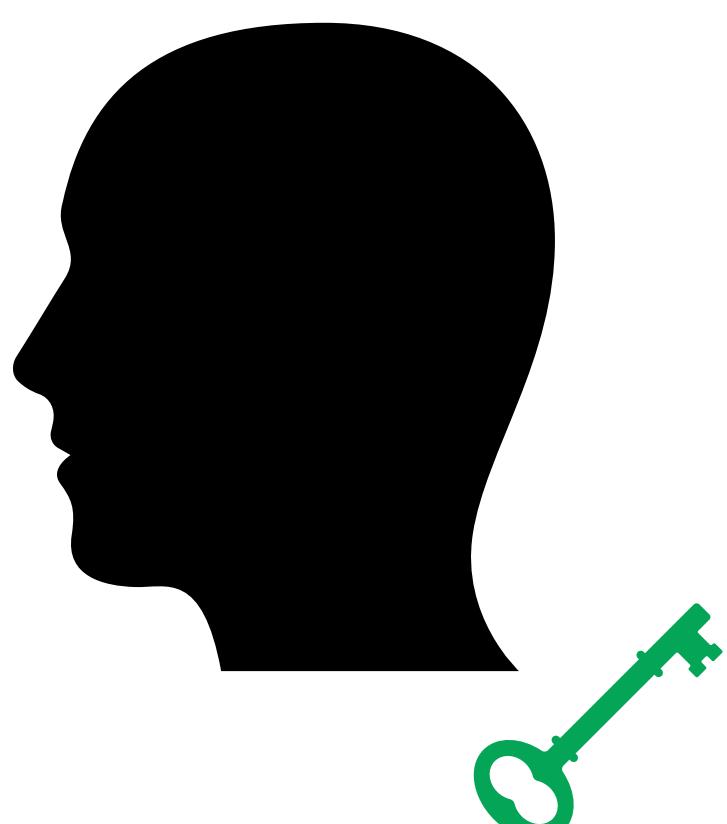
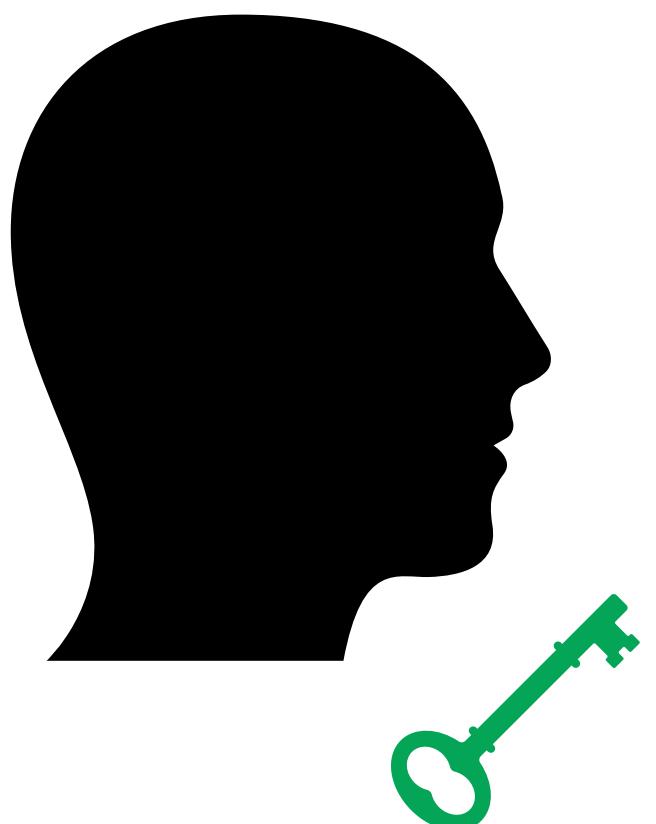
Distribution de clé quantique (QKD)

Distribution de clé quantique (QKD)

Déployer une clé symétrique chez Alice et chez Bob en utilisant les propriétés de la mécanique quantique

Sécurité théorique parfaite

Détection d'espion



Protocole E91



All Journals Physics Magazine

Physical Review Letters

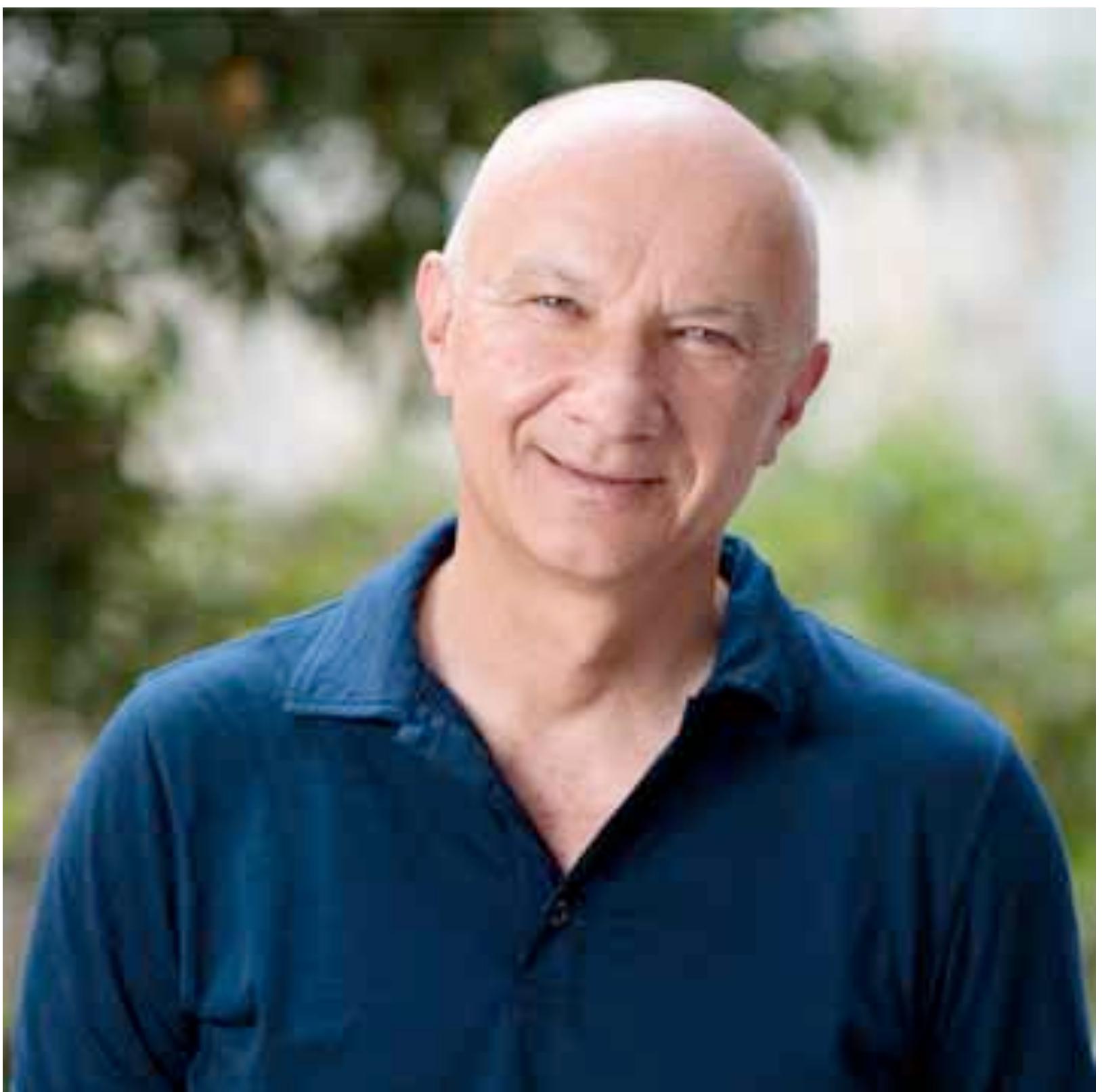
Quantum cryptography based on Bell's theorem

[Artur K. Ekert](#)

Show more ▾

Phys. Rev. Lett. **67**, 661 – Published 5 August, 1991

DOI: <https://doi.org/10.1103/PhysRevLett.67.661>



Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

Le bit

Information classique

- Le bit = unité d'information
0 ou 1

- L'information peut alors être encodée sous la forme de chaines de bits.

00000	[blue]	[blue]	01000	[red]	[red]	10000	[blue]	[blue]	11000	[red]	[red]
00001	[red]	[red]	01001	[blue]	[blue]	10001	[red]	[red]	11001	[blue]	[blue]
00010	[blue]	[blue]	01010	[red]	[red]	10010	[blue]	[blue]	11010	[red]	[red]
00011	[red]	[red]	01011	[blue]	[blue]	10011	[red]	[red]	11011	[blue]	[blue]
00100	[blue]	[blue]	01100	[red]	[red]	10100	[blue]	[blue]	11100	[red]	[red]
00101	[red]	[red]	01101	[blue]	[blue]	10101	[red]	[red]	11101	[blue]	[blue]
00110	[blue]	[blue]	01110	[red]	[red]	10110	[blue]	[blue]	11110	[red]	[red]
00111	[red]	[red]	01111	[blue]	[blue]	10111	[red]	[red]	11111	[blue]	[blue]

Le bit

Information classique

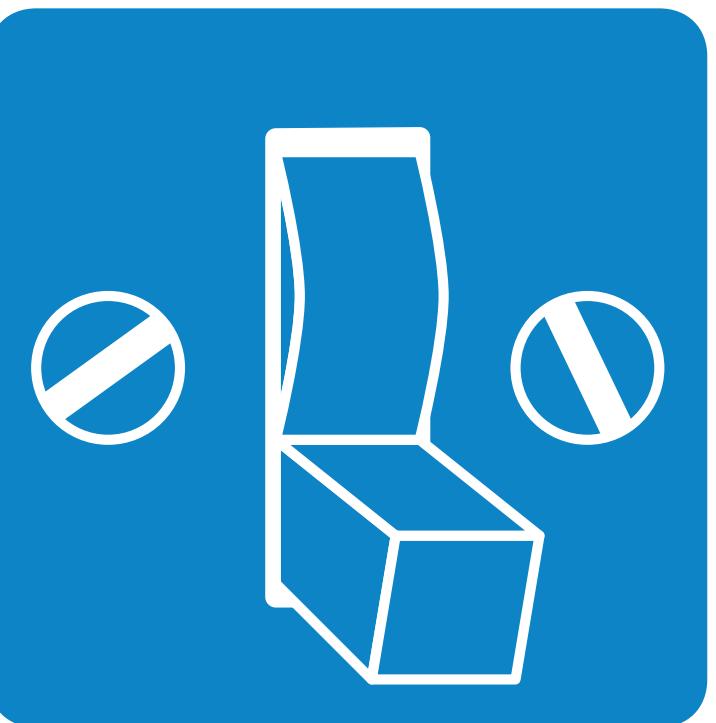
- Le bit = unité d'information
0 ou 1
- L'information peut alors être encodée sous la forme de chaines de bits.
- Avec 5 bits il est possible d'encoder :
 - Les nombres de 0 à 31
 - L'alphabet

00000	0	a	01000	8	i	10000	16	q	11000	24	y
00001	1	b	01001	9	j	10001	17	r	11001	25	z
00010	2	c	01010	10	k	10010	18	s	11010	26	
00011	3	d	01011	11	l	10011	19	t	11011	27	
00100	4	e	01100	12	m	10100	20	u	11100	28	
00101	5	f	01101	13	n	10101	21	v	11101	29	
00110	6	g	01110	14	o	10110	22	w	11110	30	
00111	7	h	01111	15	p	10111	23	x	11111	31	

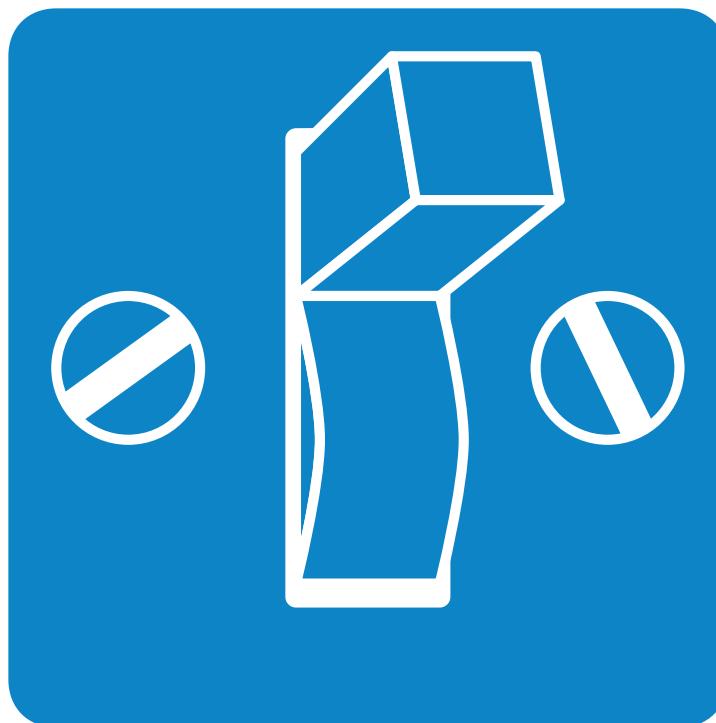
Représentation physique

Information classique

Bit



0

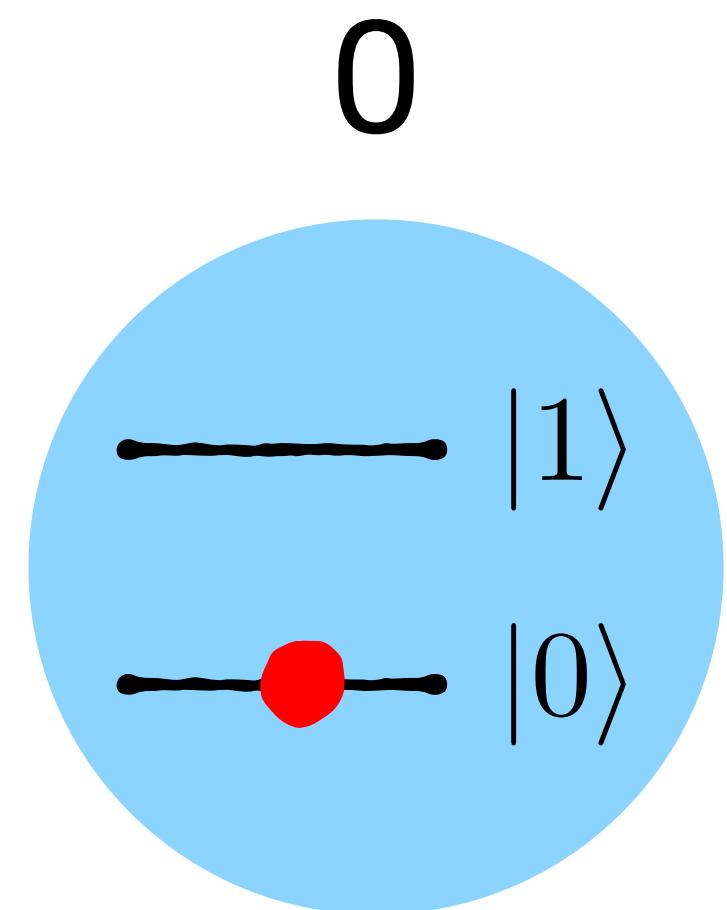


1

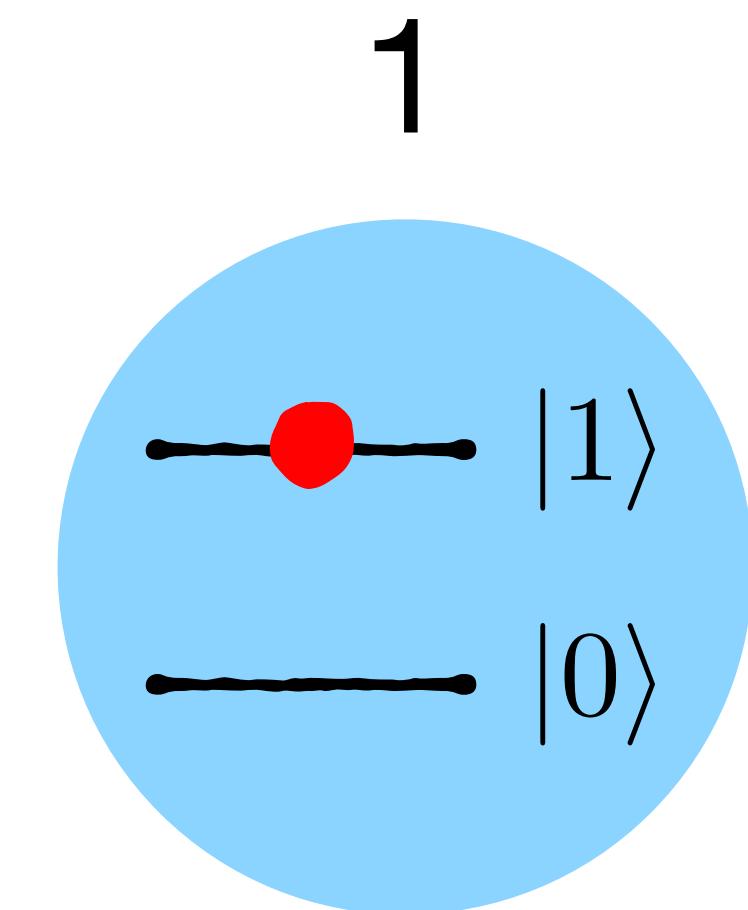
L'information quantique

Le qubit

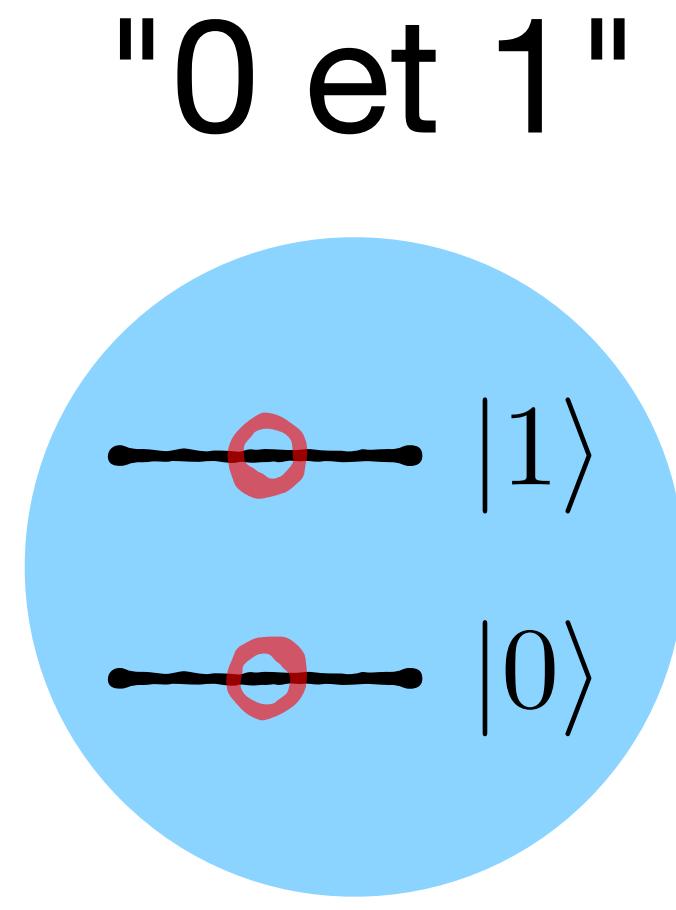
- Le qubit = bit quantique
- Prend un ensemble de valeurs



ou



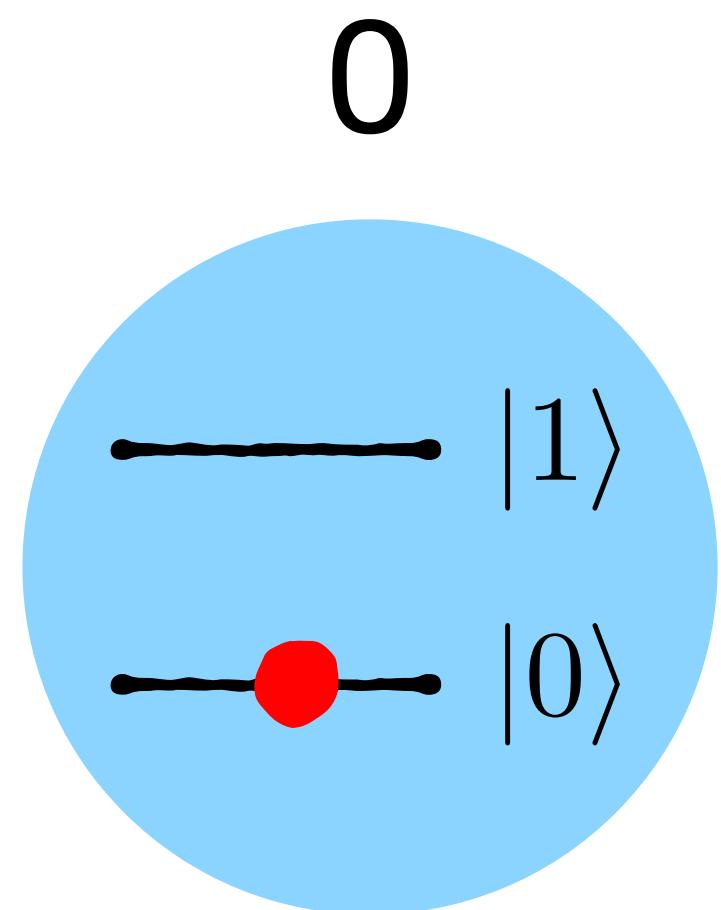
ou



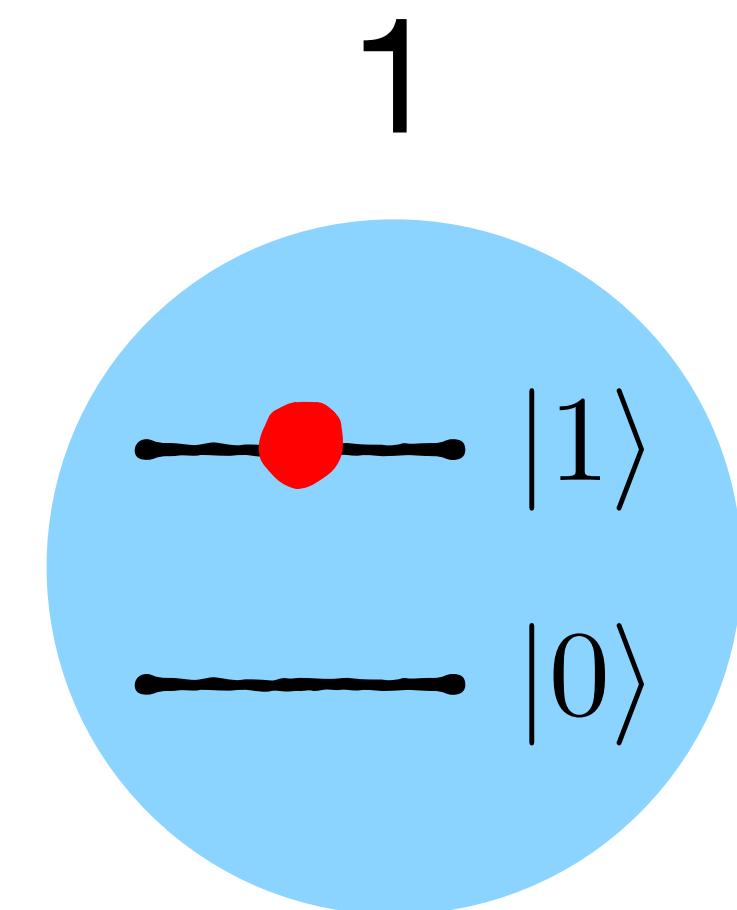
L'information quantique

Le qubit

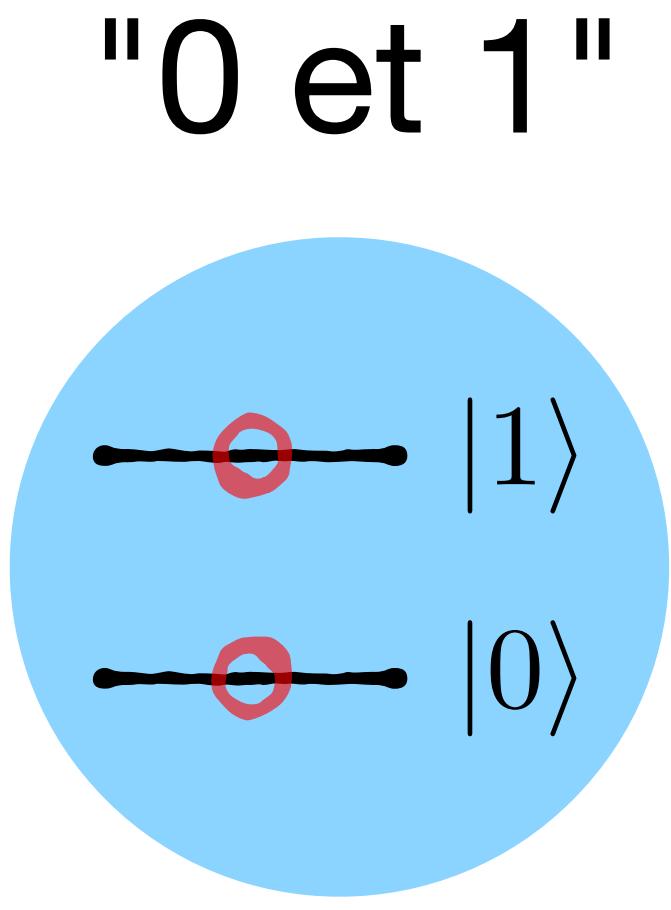
- Le qubit = bit quantique
- Prend un ensemble de valeurs



ou



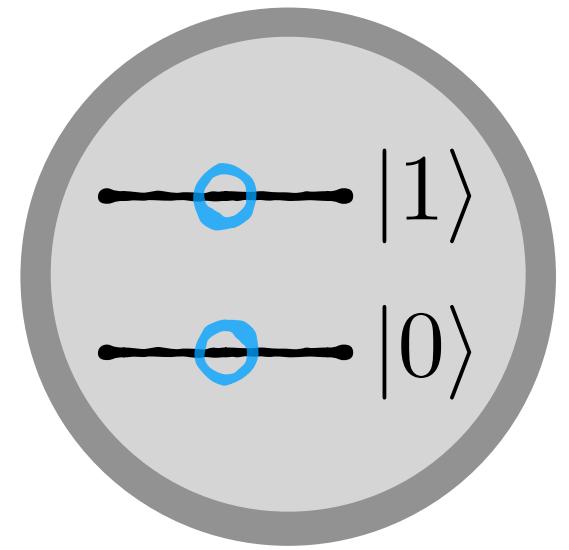
ou



État de
superposition

Notation de Dirac

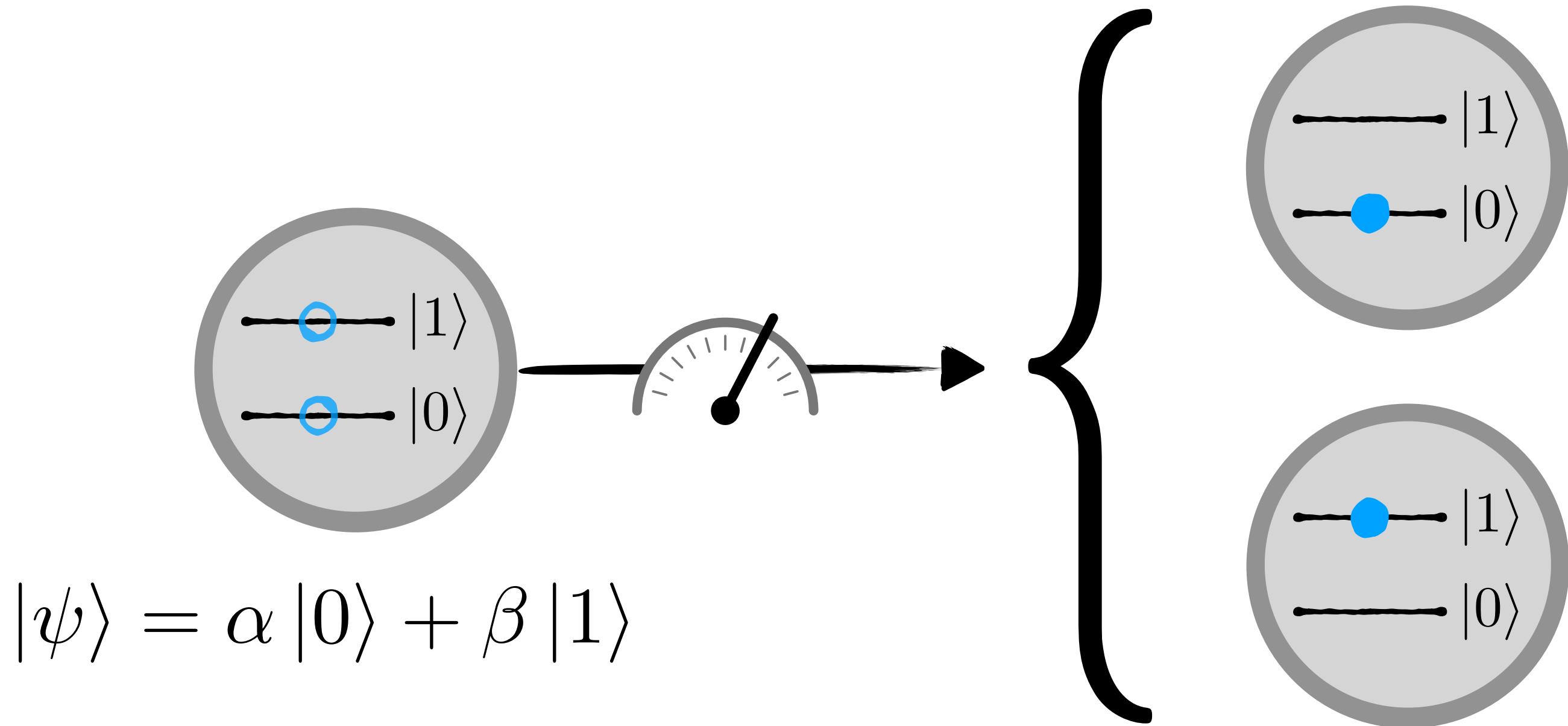
Superposition



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

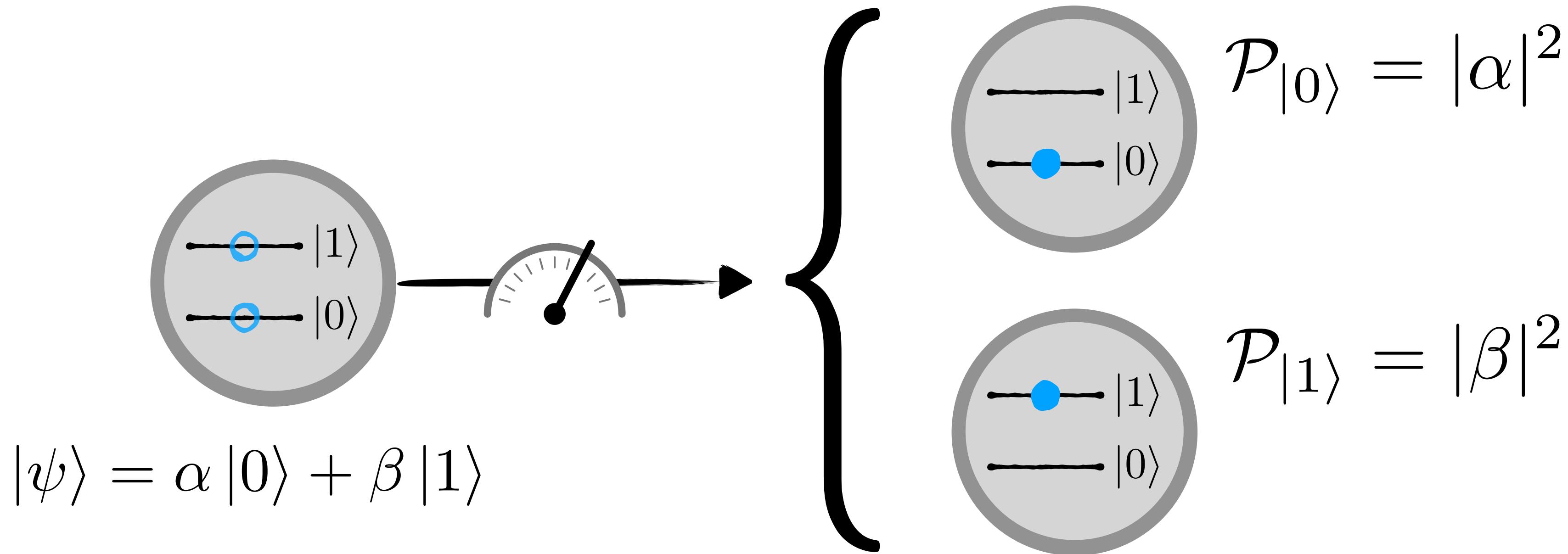
Notation de Dirac

Superposition



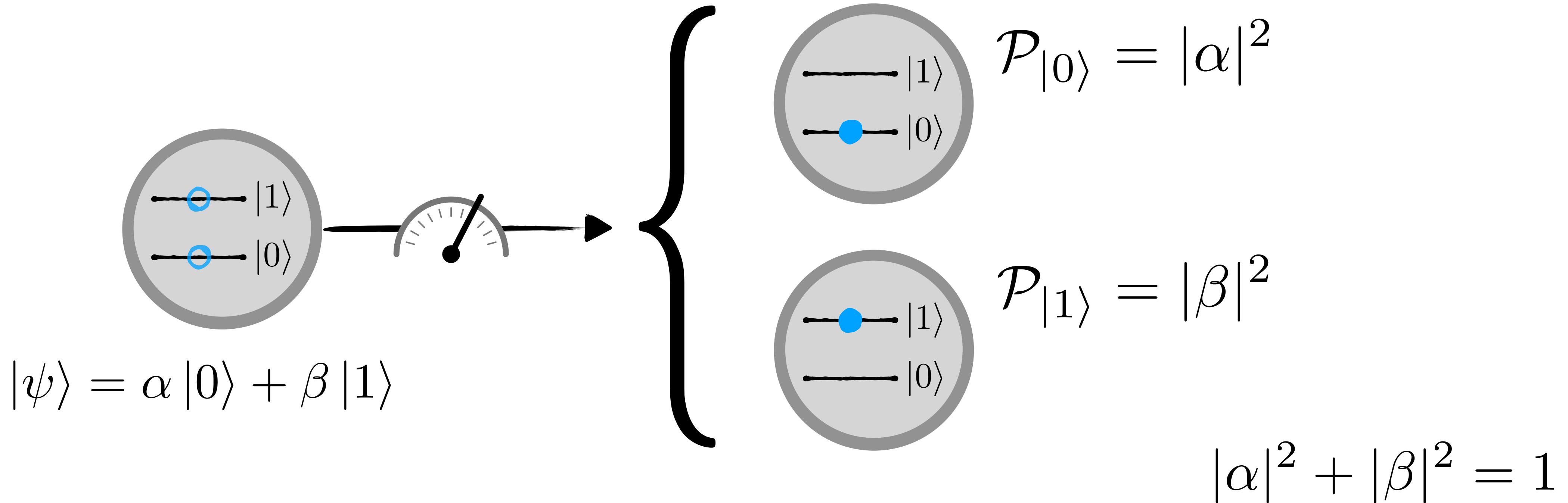
Notation de Dirac

Superposition



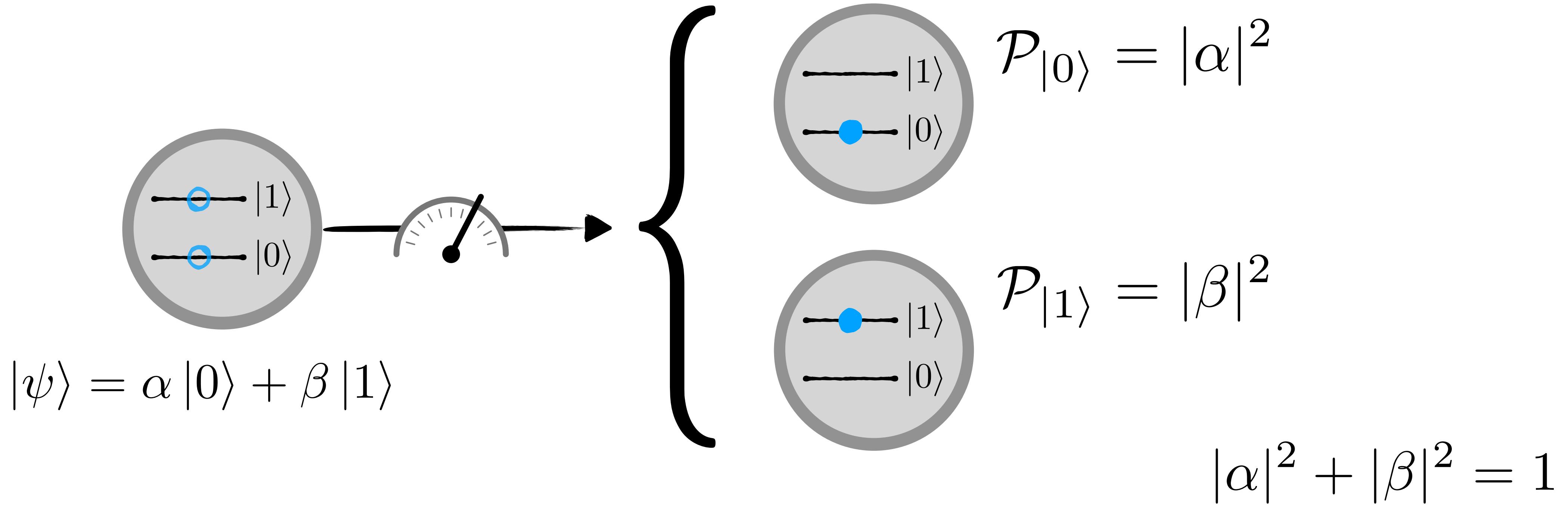
Notation de Dirac

Superposition



Notation de Dirac

Superposition



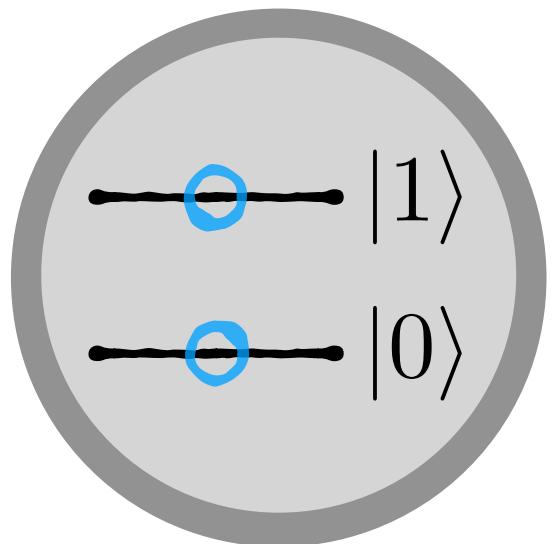
Exemples :

$$|\psi\rangle = 1|0\rangle + 0|1\rangle \quad |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-1}{\sqrt{2}}|1\rangle$$

Représentation physique

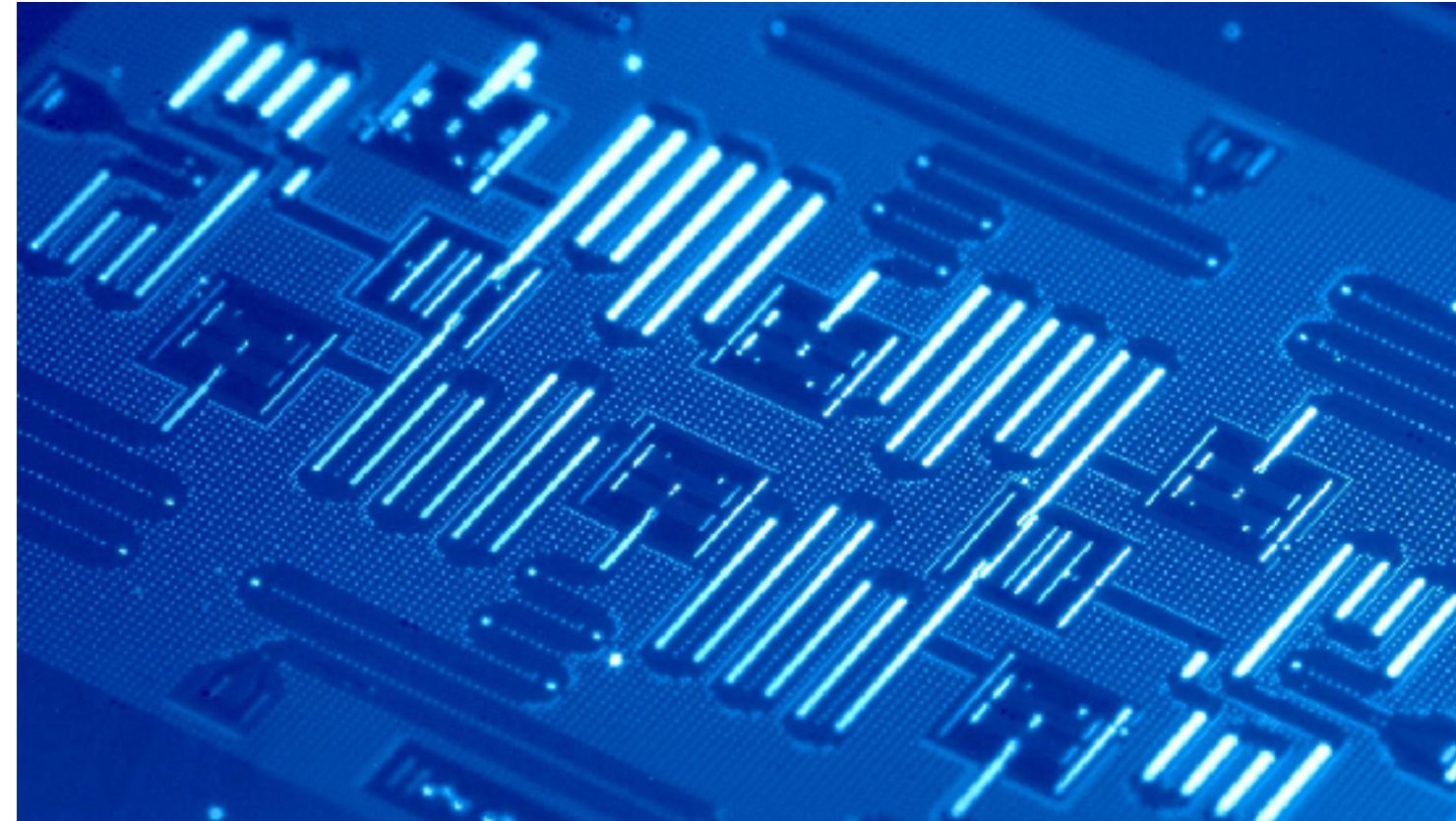
Information quantique

Qubit

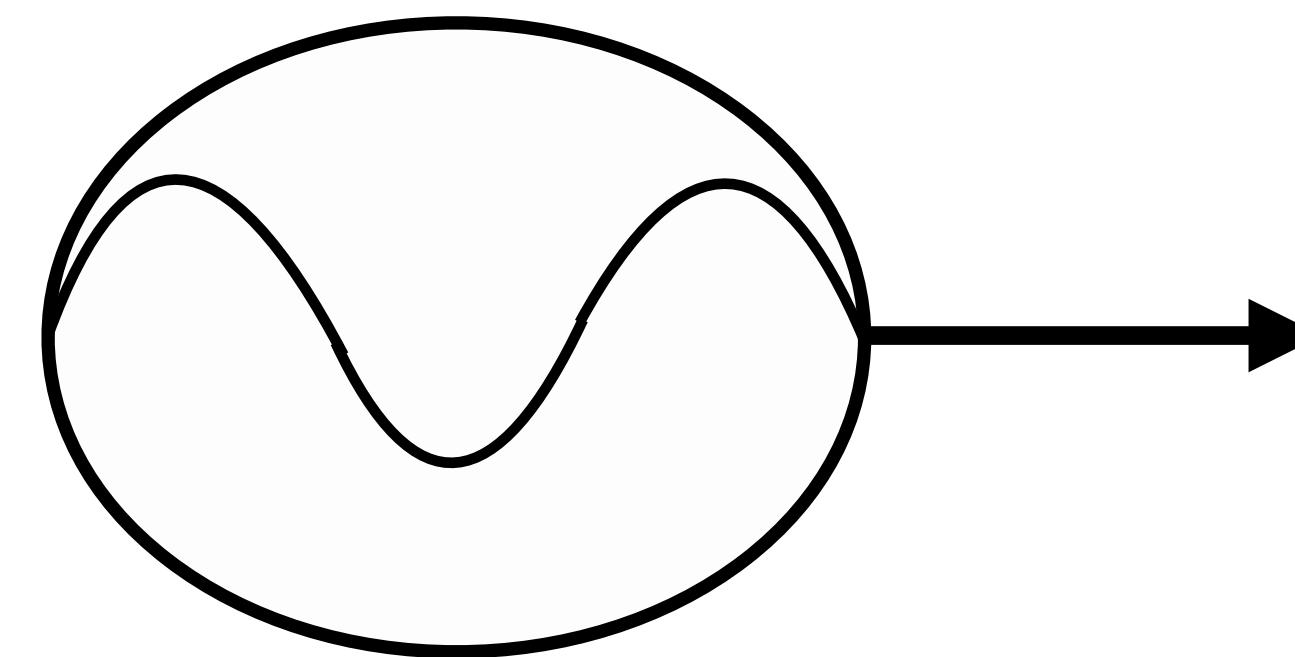


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Qubits supraconducteurs



IBM



Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

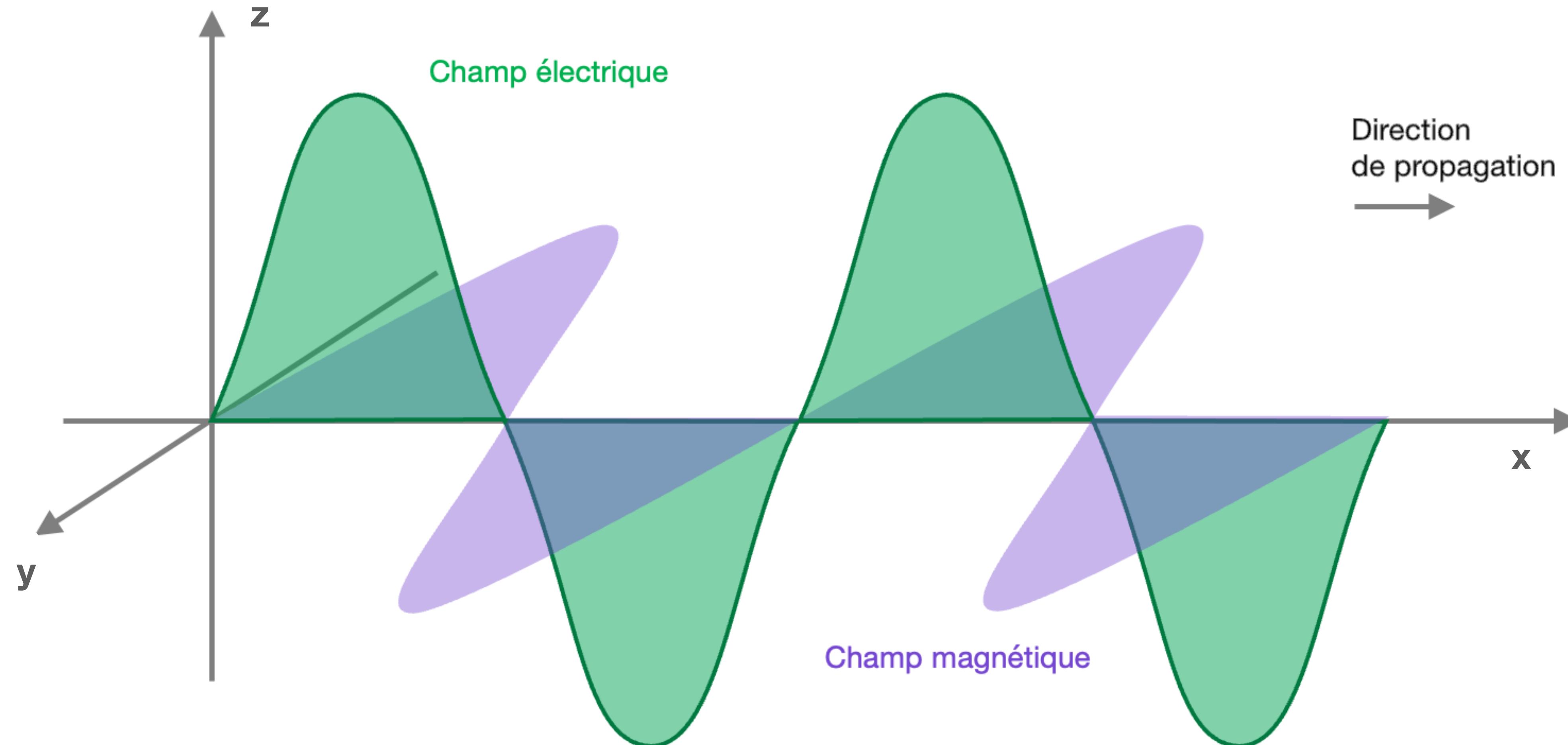
Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

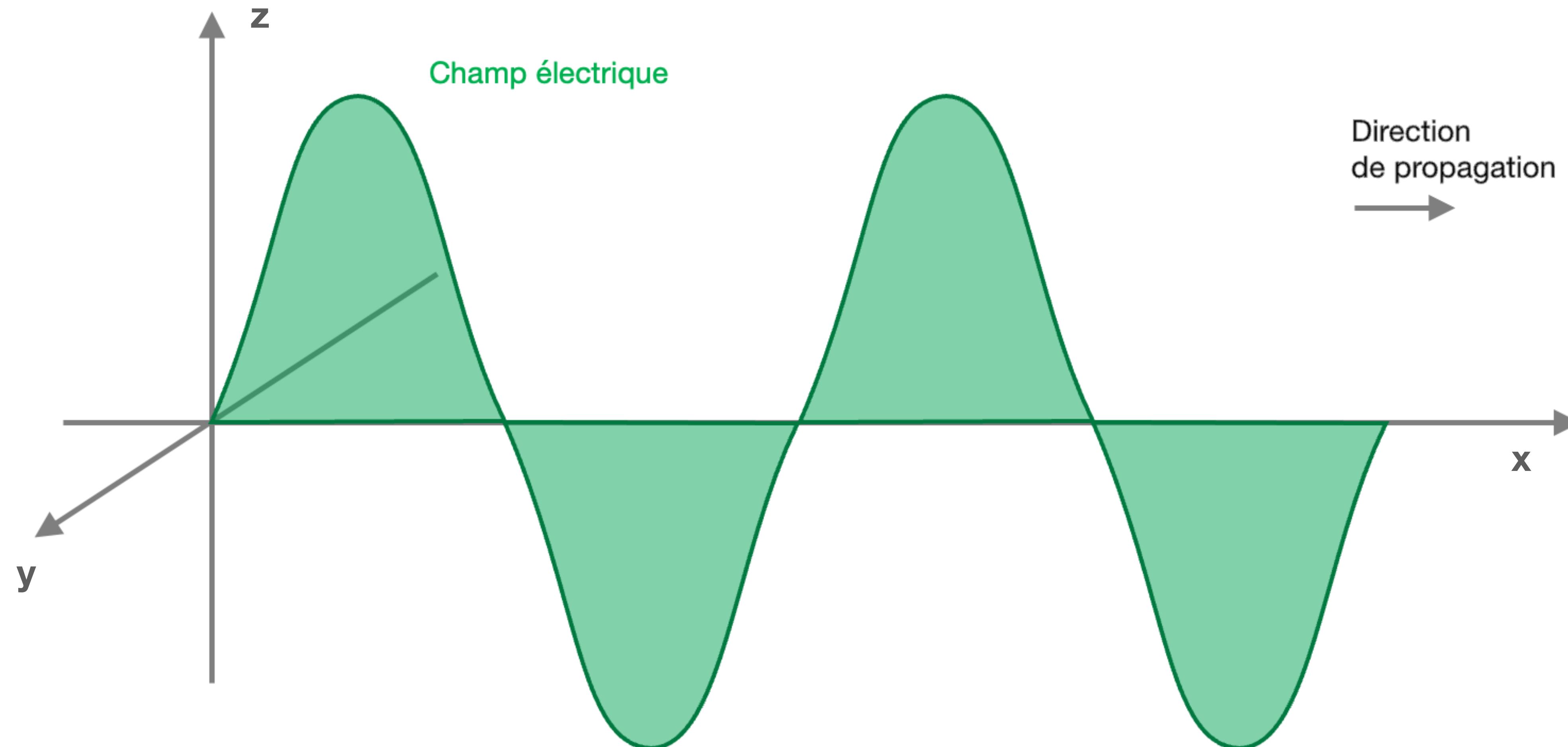
Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

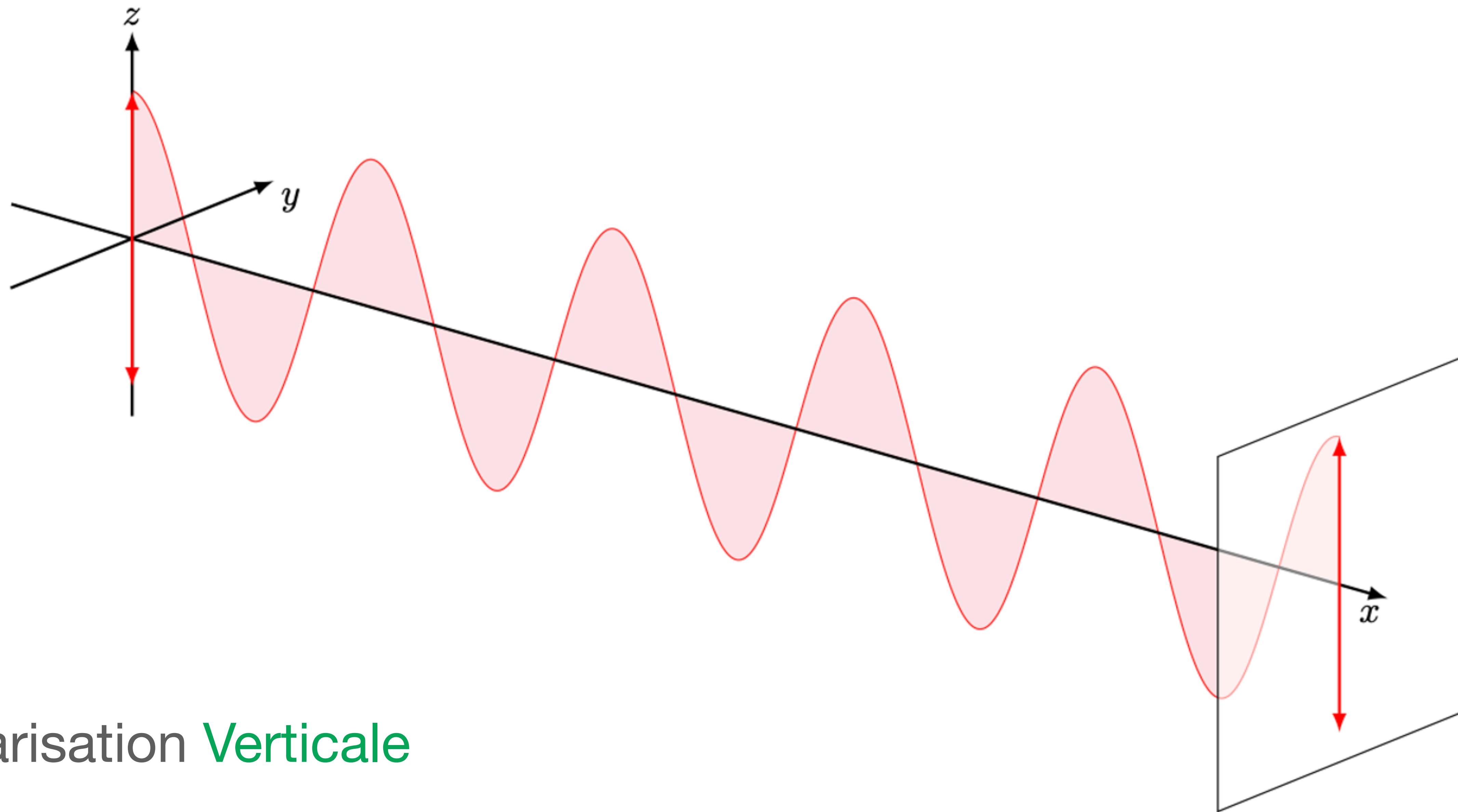
La lumière



La polarisation: propriété quantique

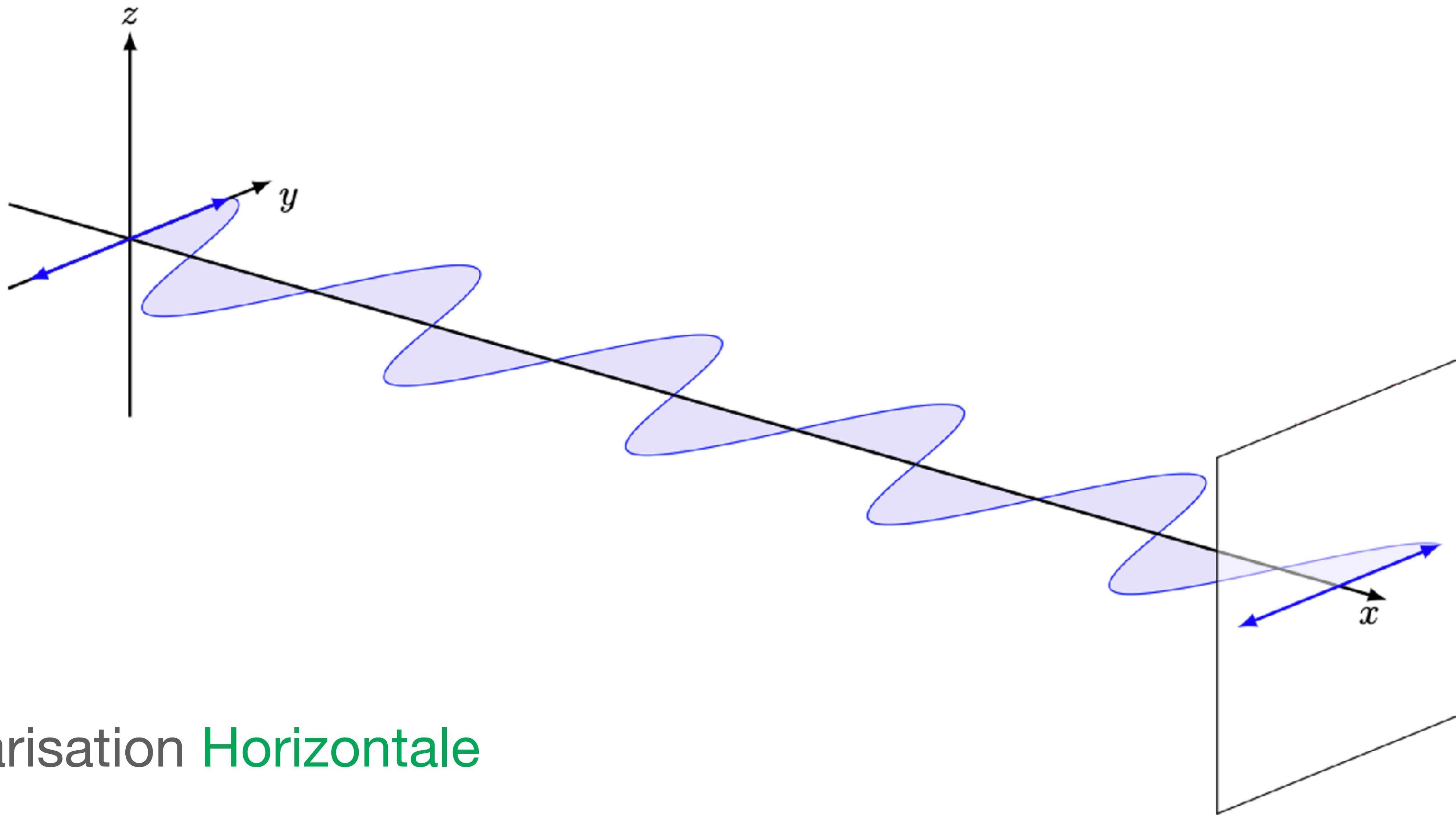


La polarisation: propriété quantique



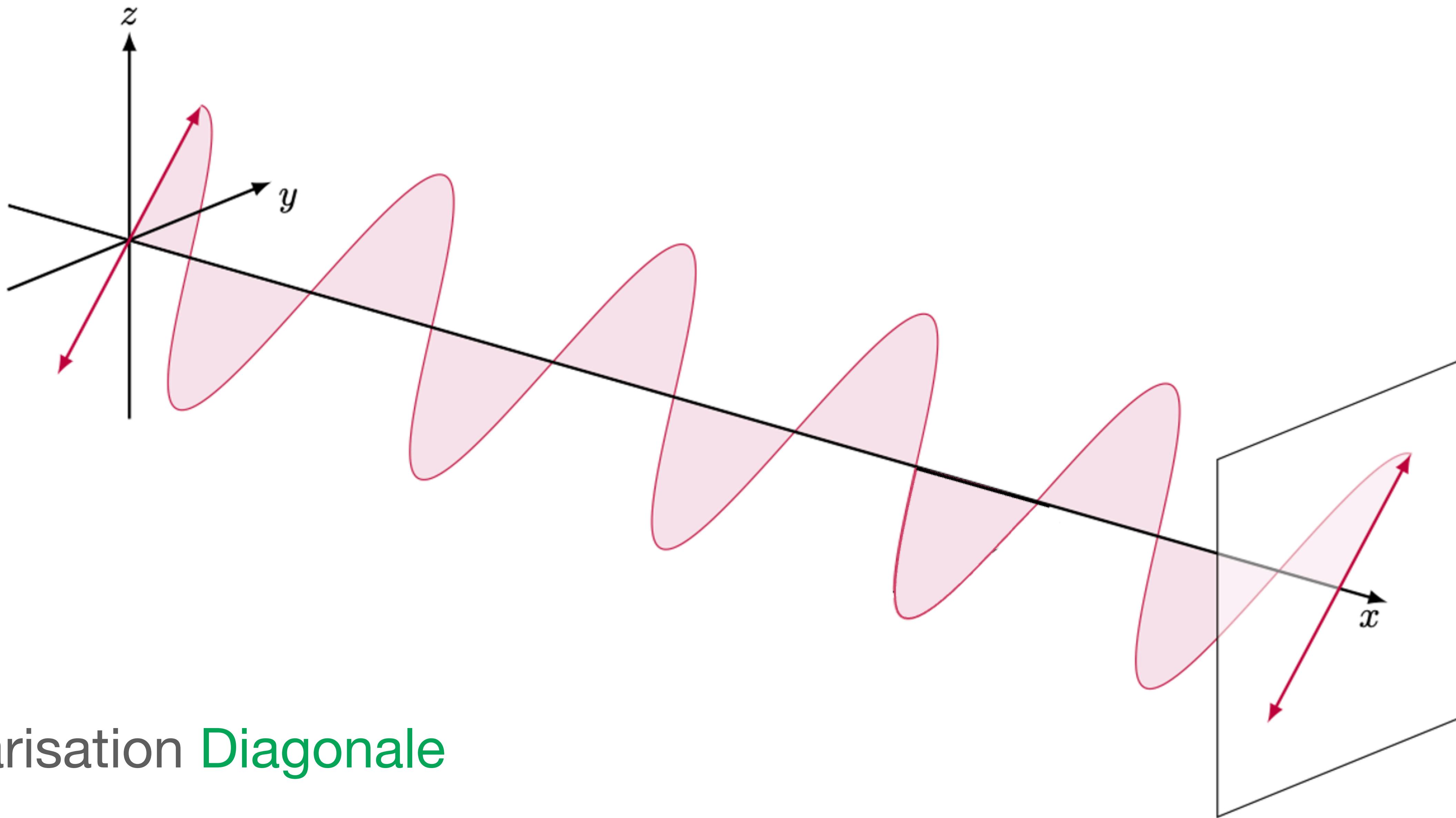
Polarisation Verticale

La polarisation: propriété quantique

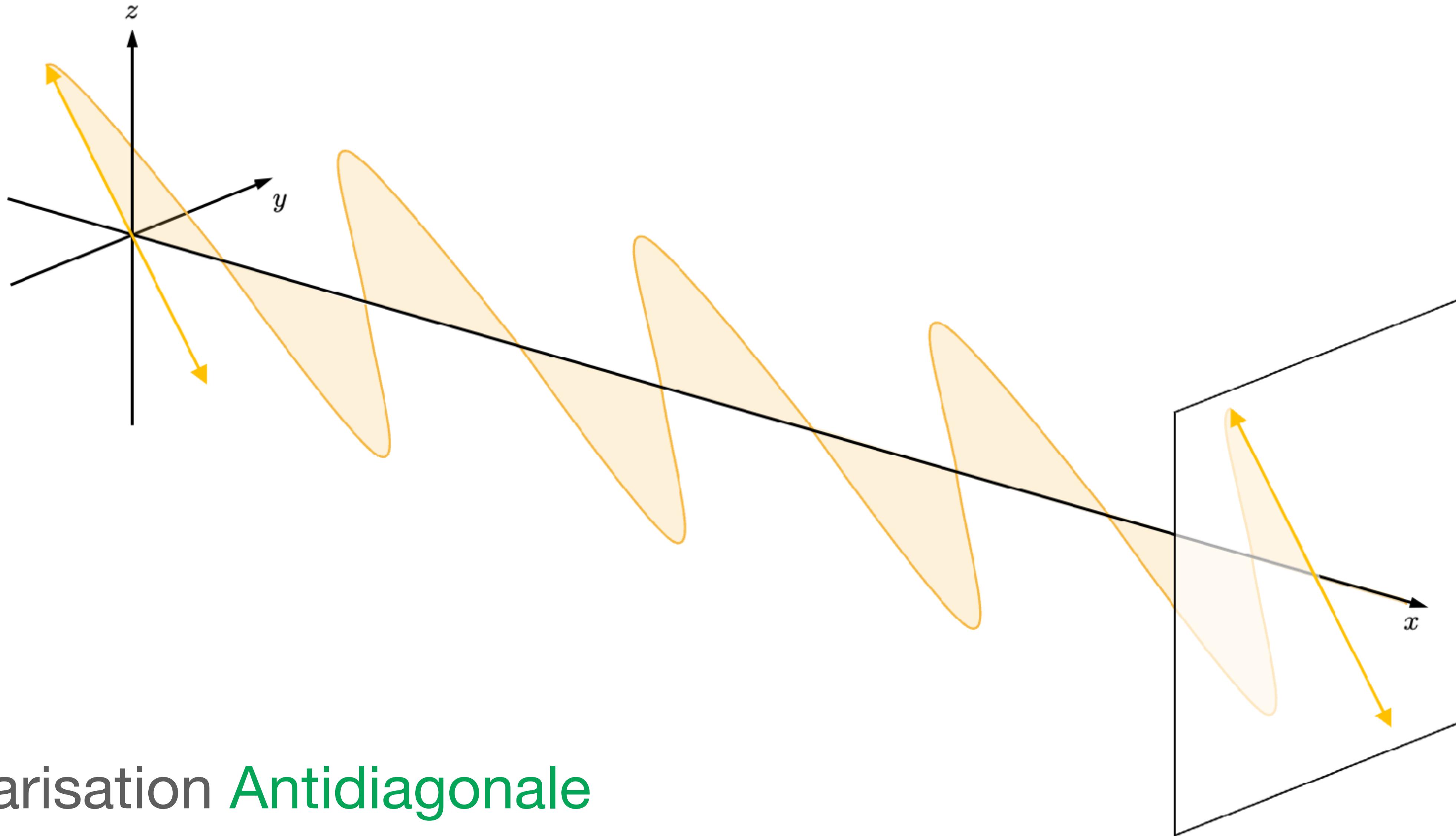


Polarisation Horizontale

La polarisation: propriété quantique



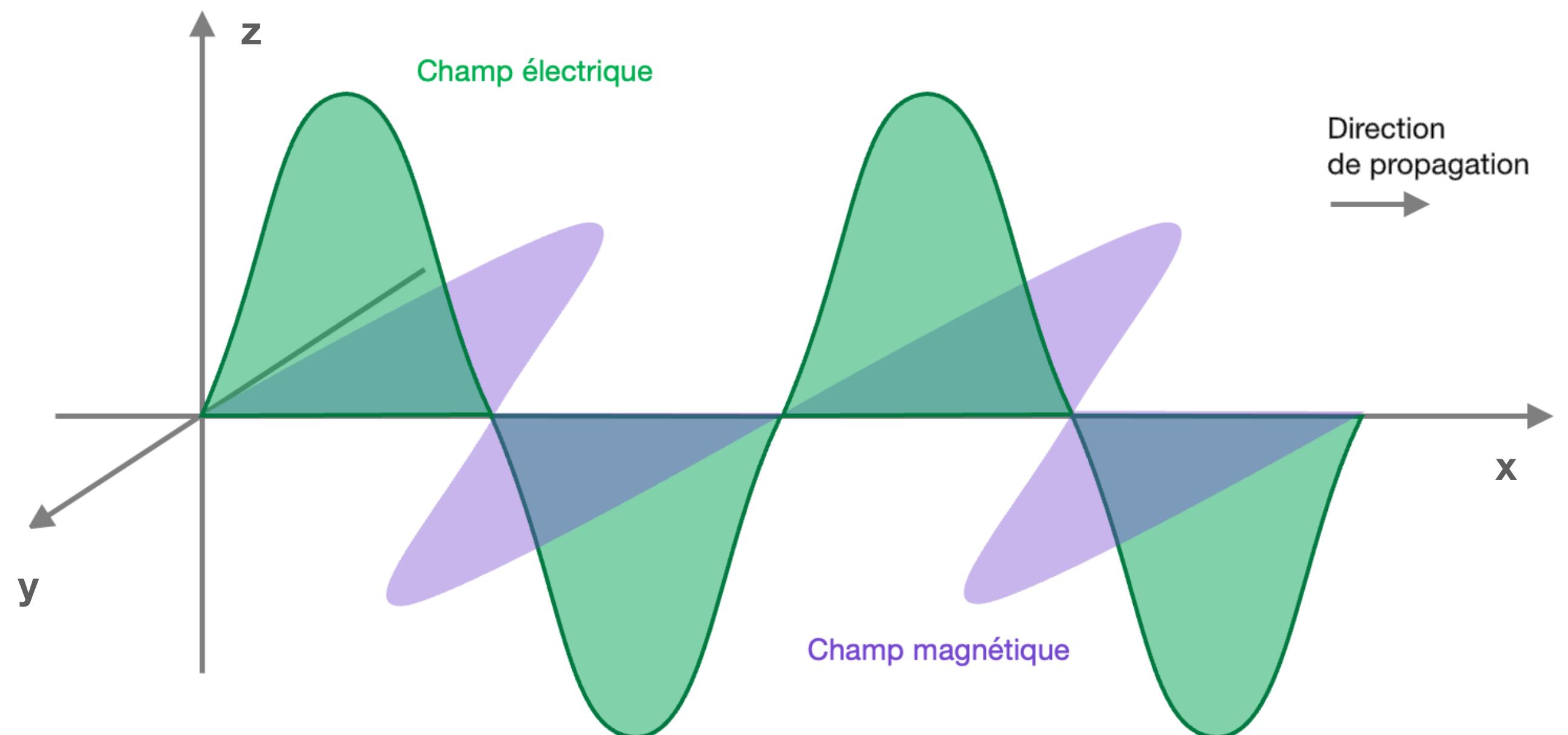
La polarisation: propriété quantique



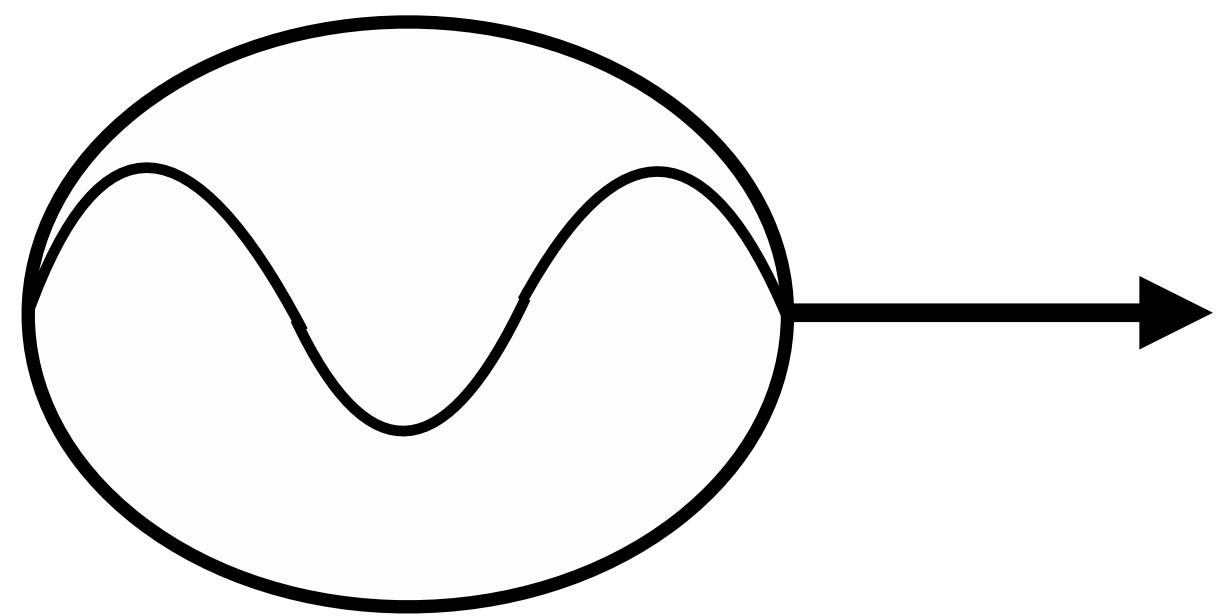
Polarisation Antidiagonale

Dualité onde-particule de la lumière

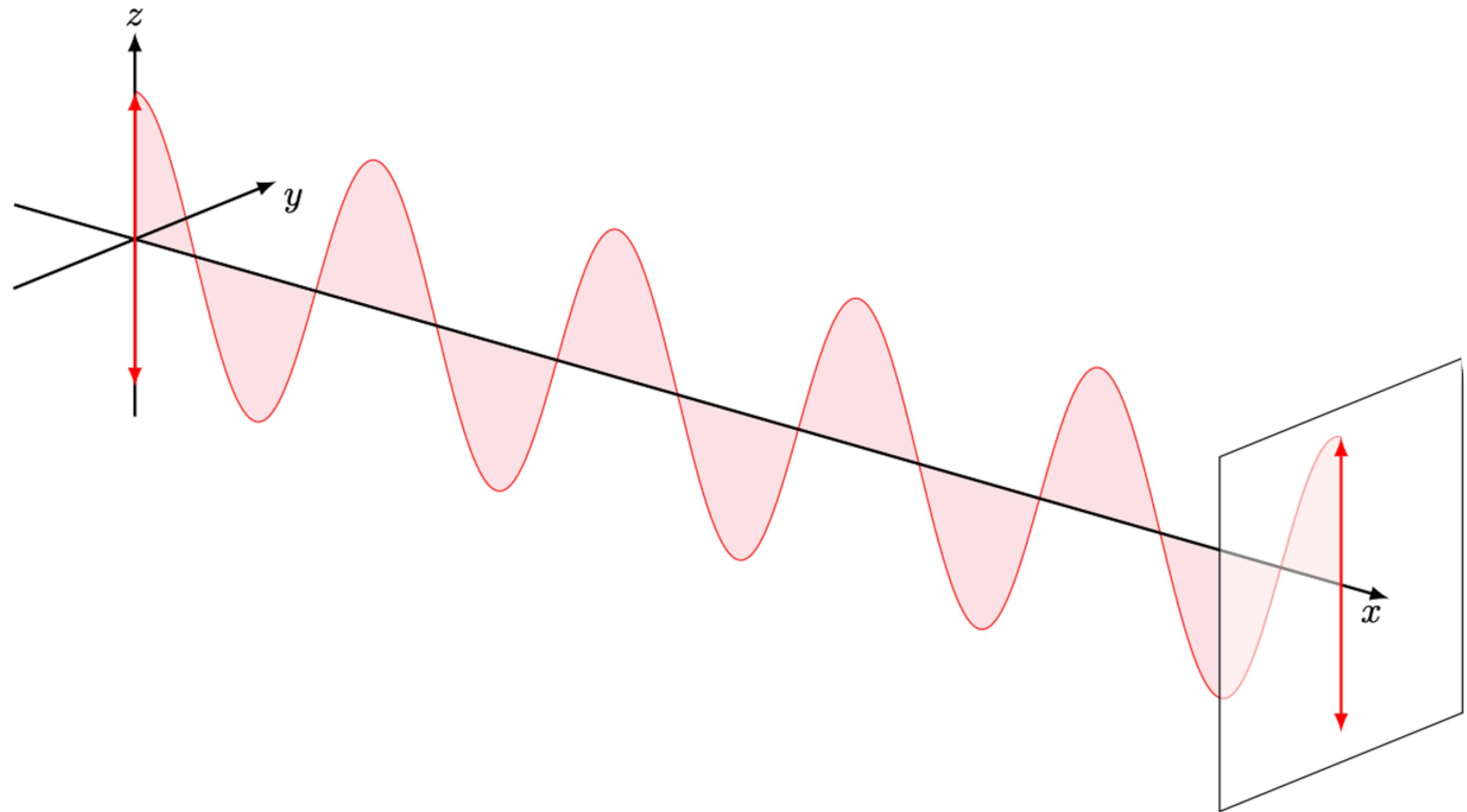
Onde électro-magnétique



Le photon

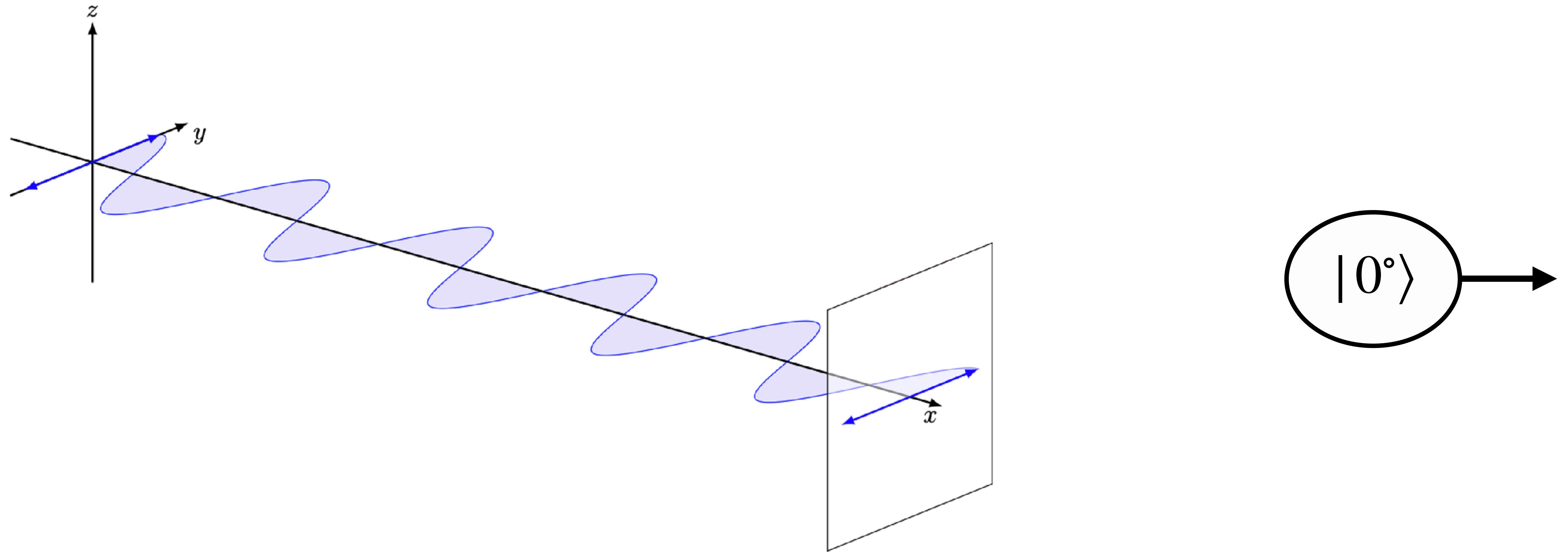


Polarisation Verticale

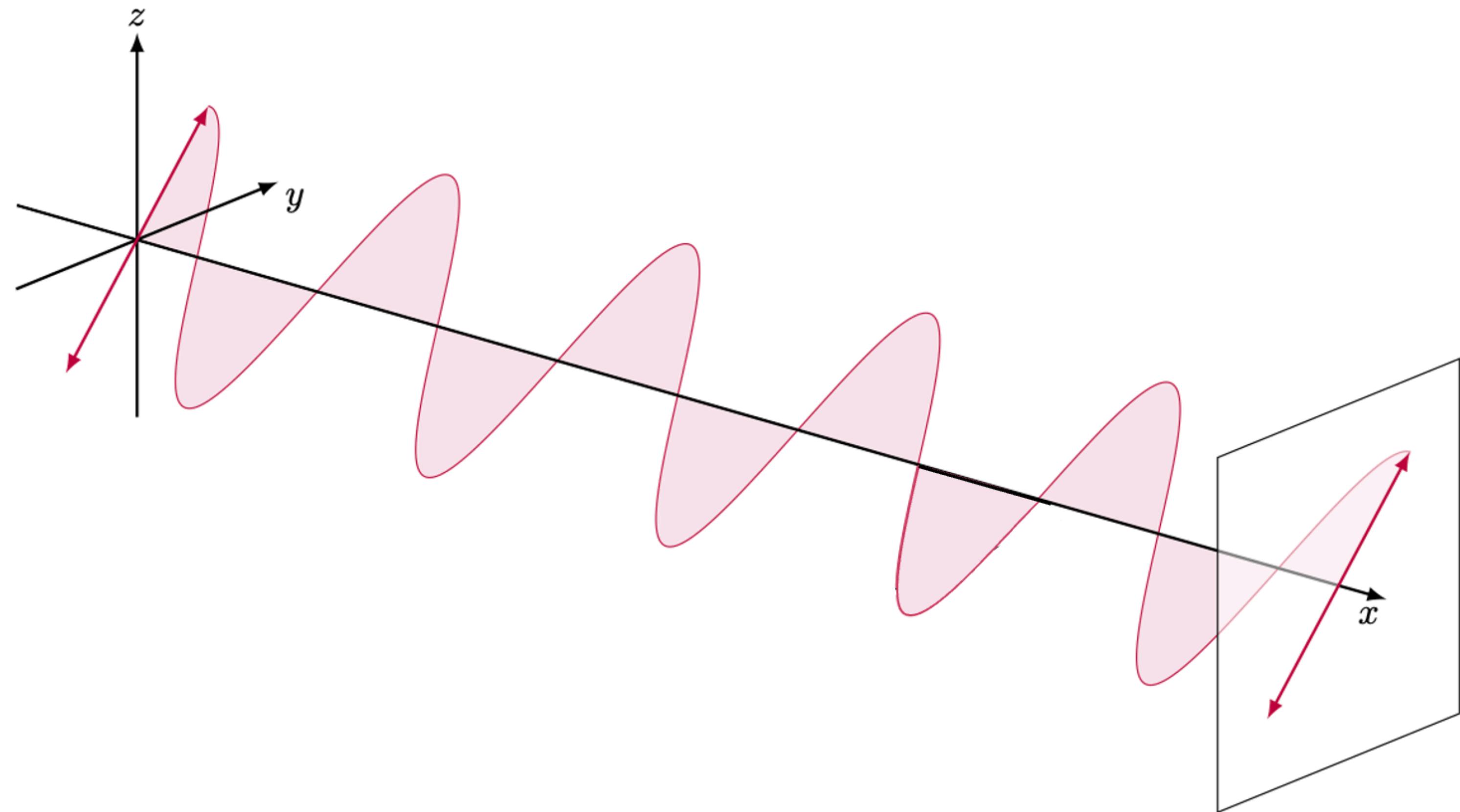


$|90^\circ\rangle$

Polarisation Horizontale

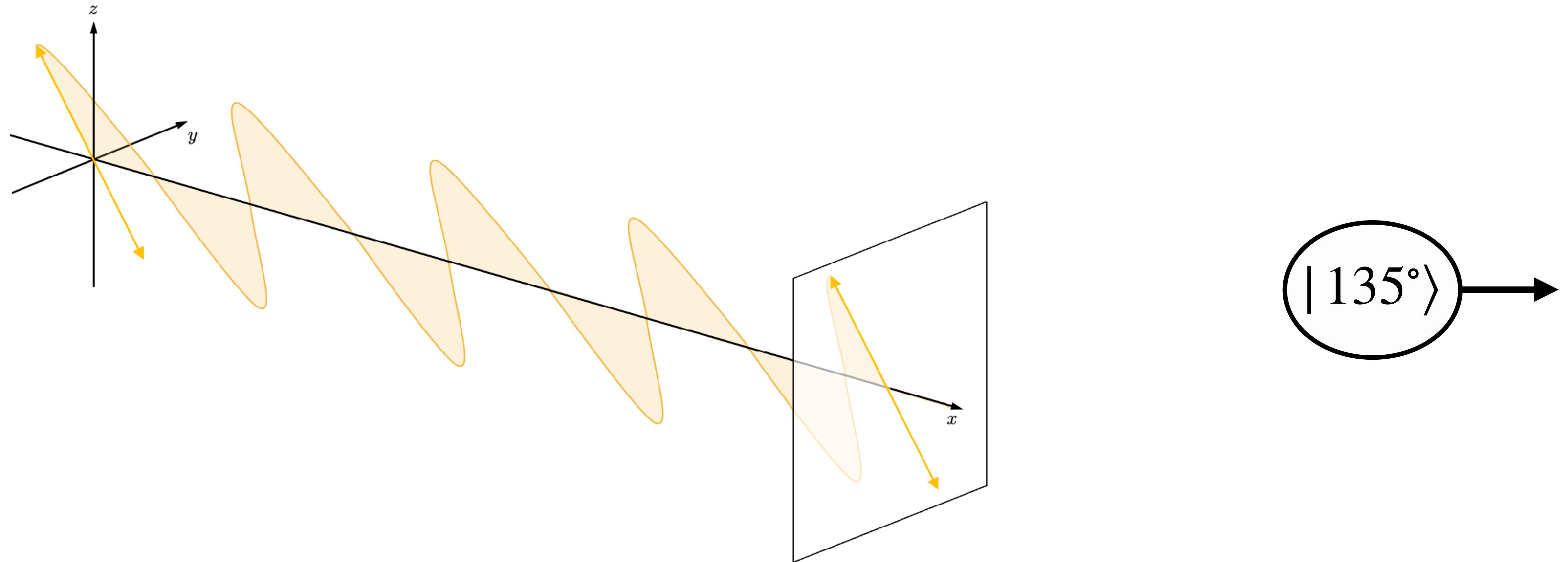


Polarisation Diagonale



$|45^\circ\rangle$

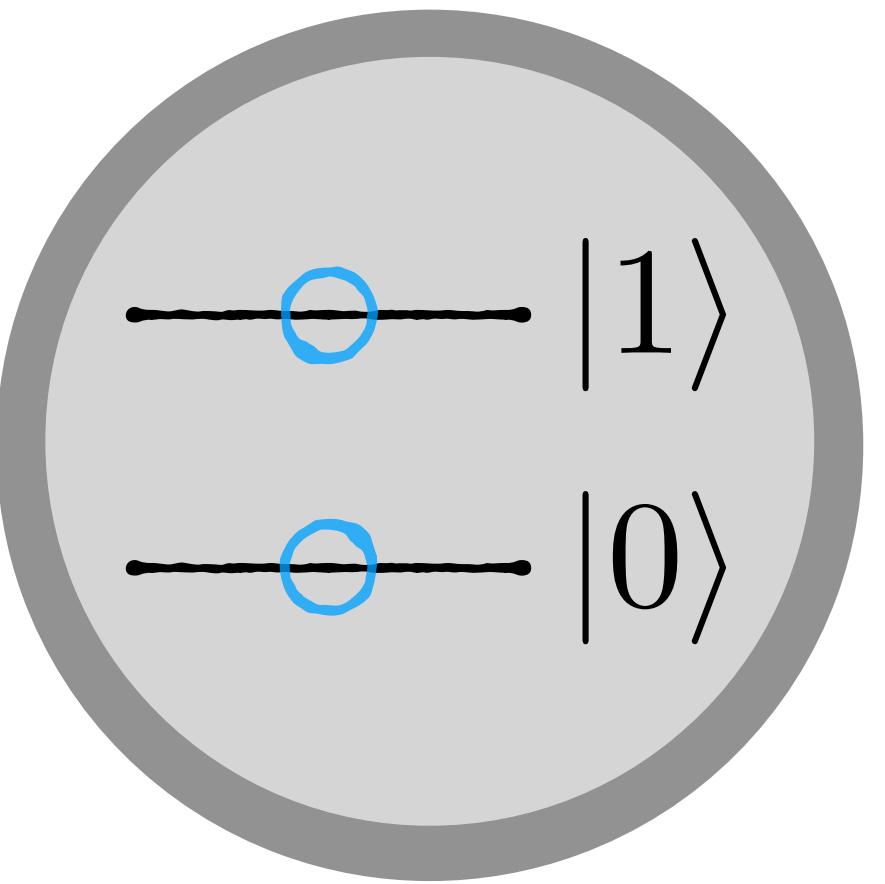
Polarisation Antidiagonale



États de base

États de base

$|0\rangle$ et $|1\rangle$



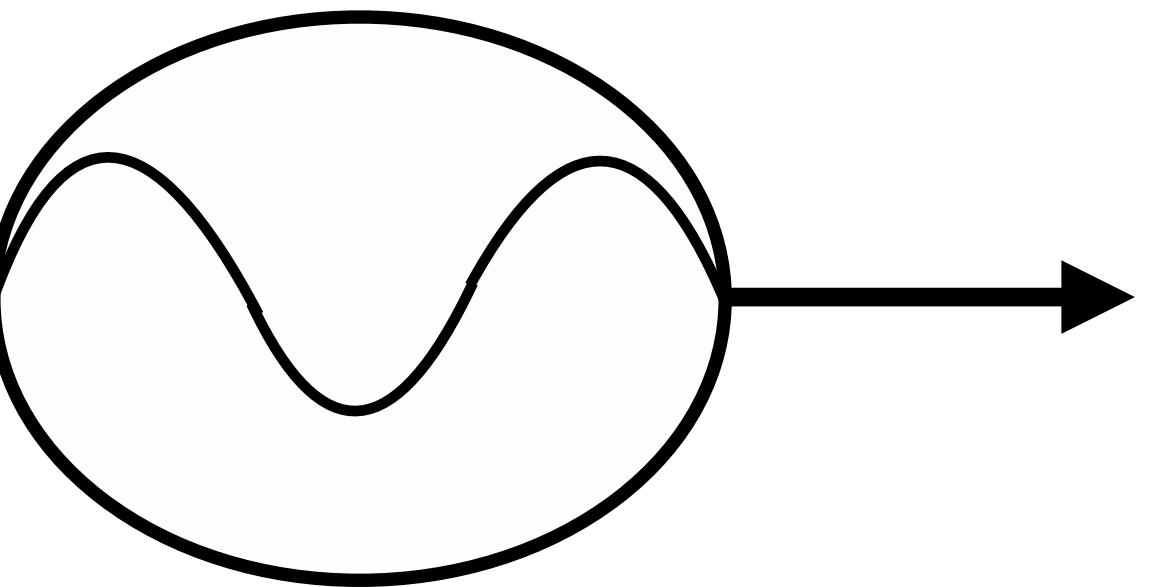
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

États de base

États de base

$|0\rangle$ et $|1\rangle$



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

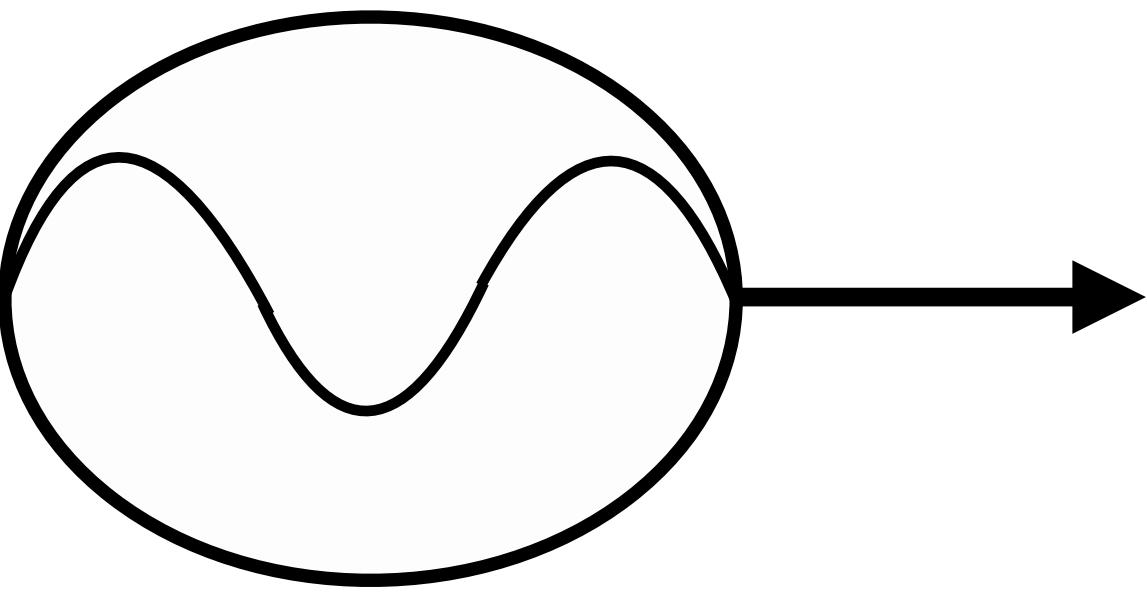
États de base

États de base

$|0\rangle$ et $|1\rangle$

$|90^\circ\rangle$ et $|0^\circ\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



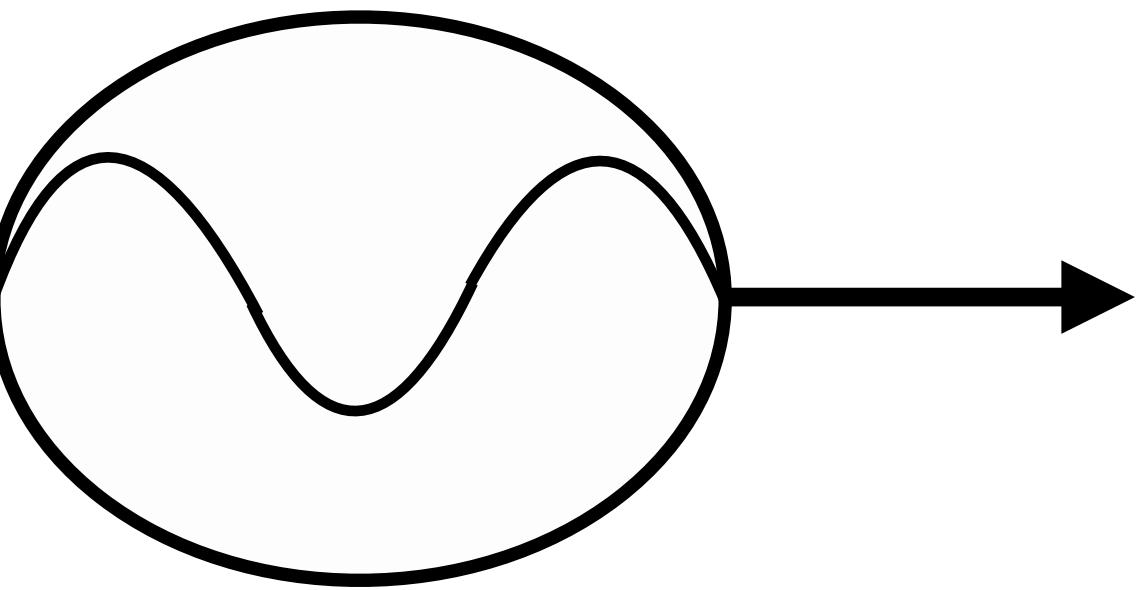
$$|\alpha|^2 + |\beta|^2 = 1$$

États de base

États de base

$|0\rangle$ et $|1\rangle$

$|90^\circ\rangle$ et $|0^\circ\rangle$



$$|\psi\rangle = \alpha|90^\circ\rangle + \beta|0^\circ\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

États de base

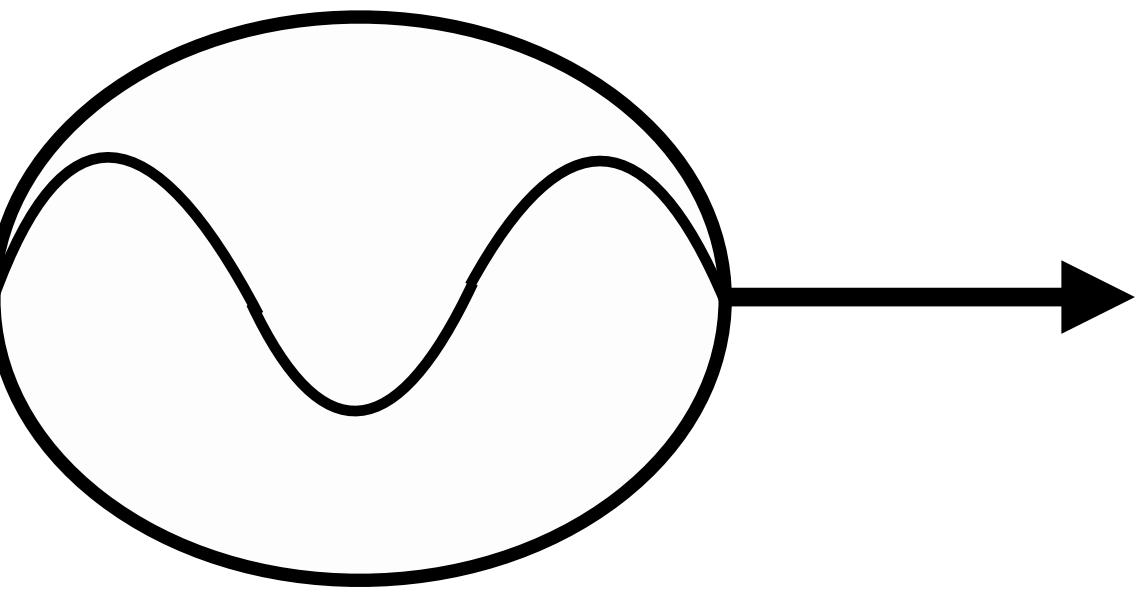
États de base

$|0\rangle$ et $|1\rangle$

$|90^\circ\rangle$ et $|0^\circ\rangle$

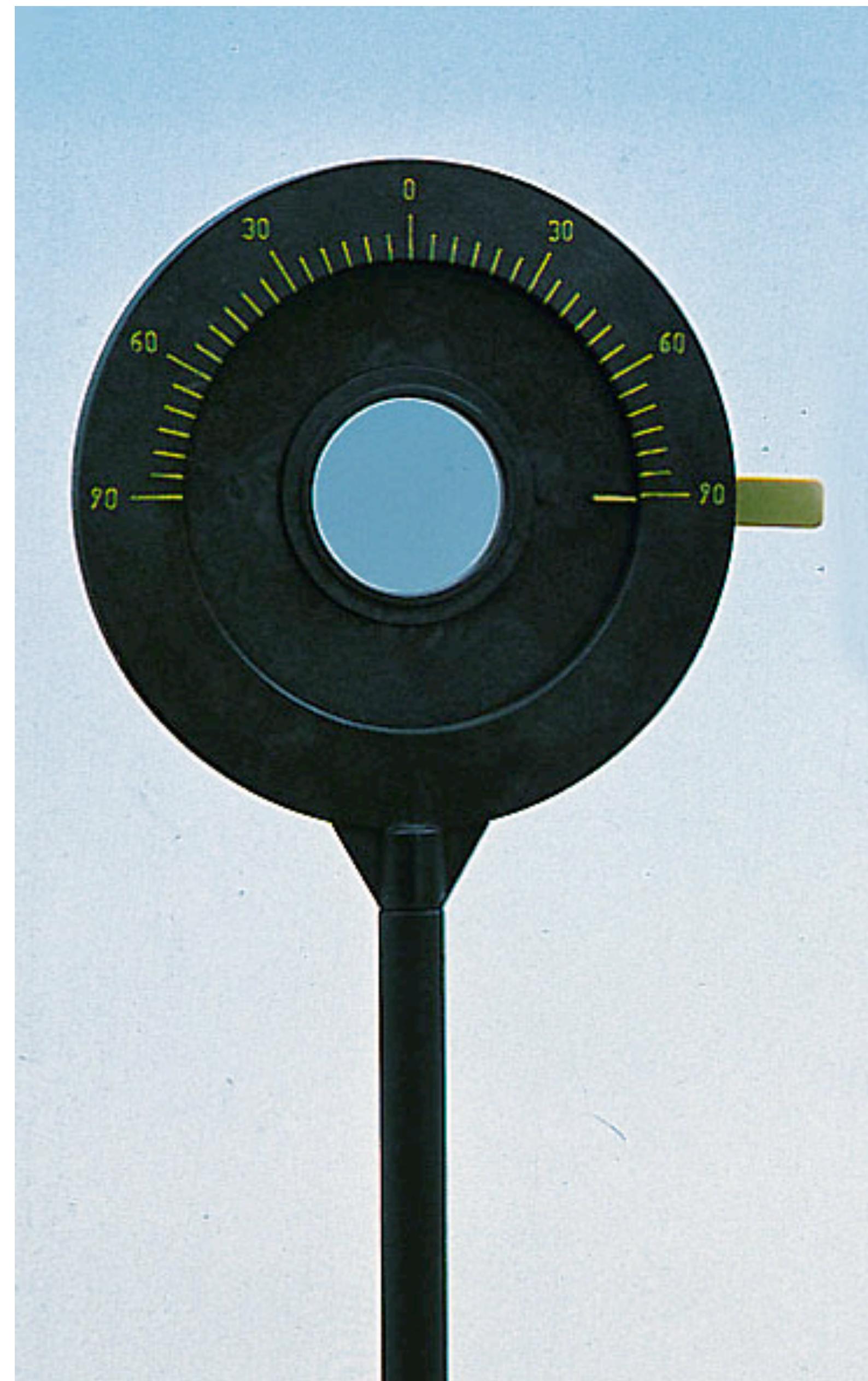
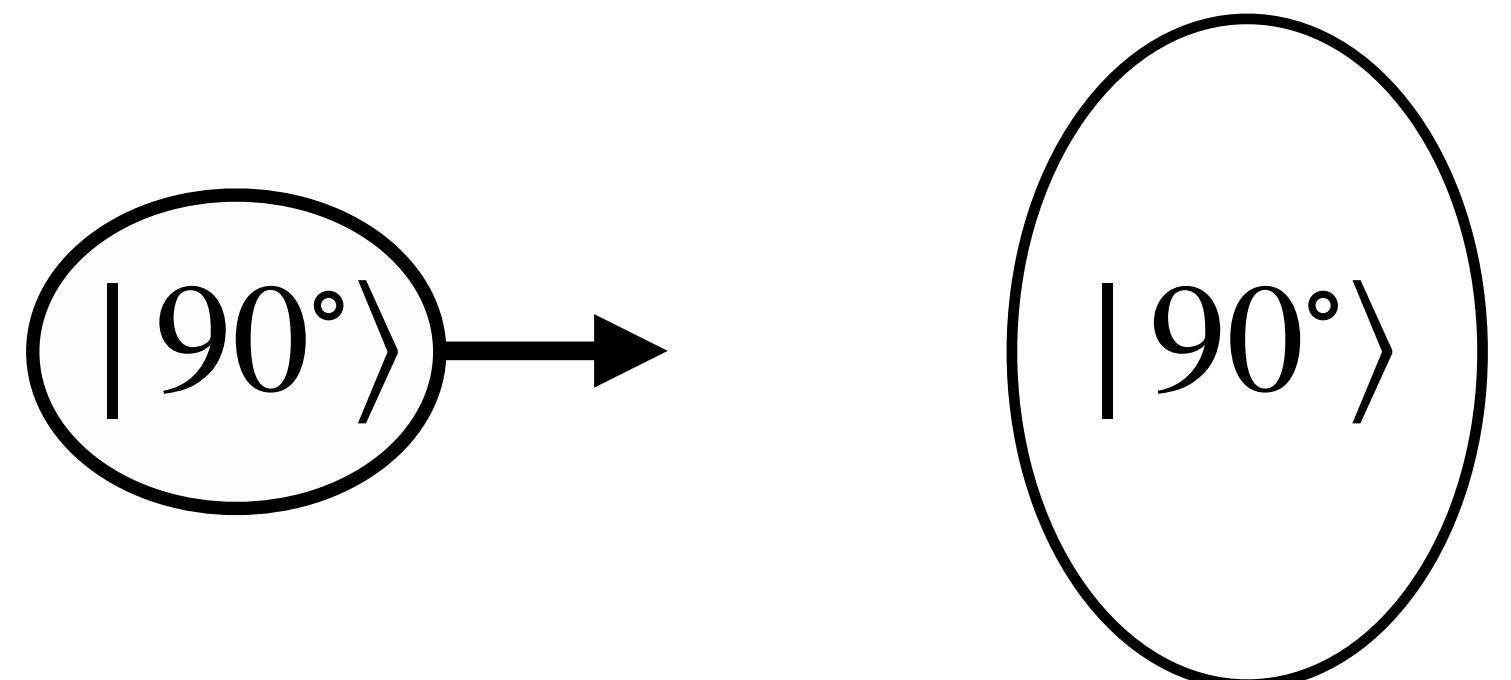
$|45^\circ\rangle$ et $|135^\circ\rangle$

$$|\psi\rangle = \alpha|45^\circ\rangle + \beta|135^\circ\rangle$$

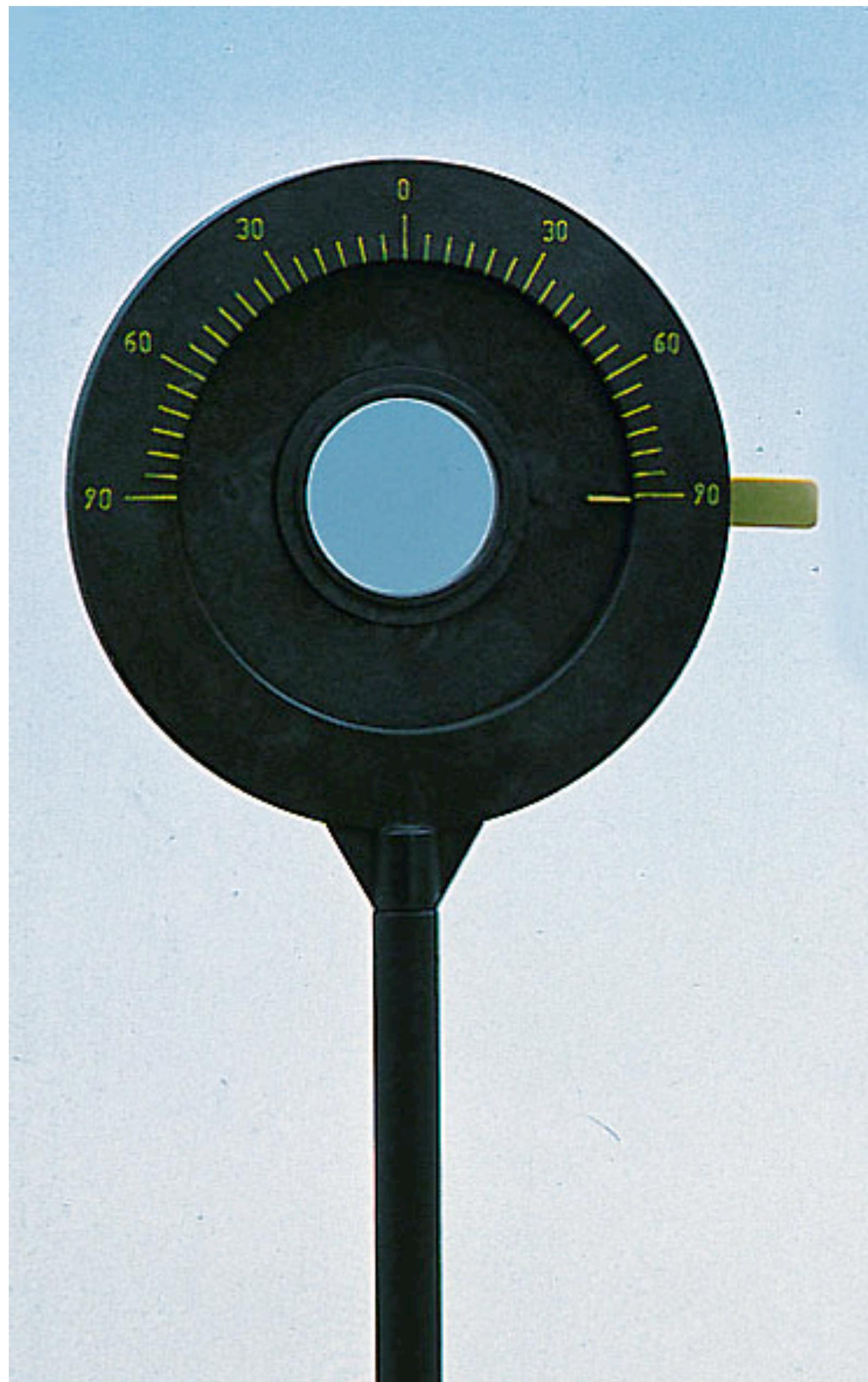
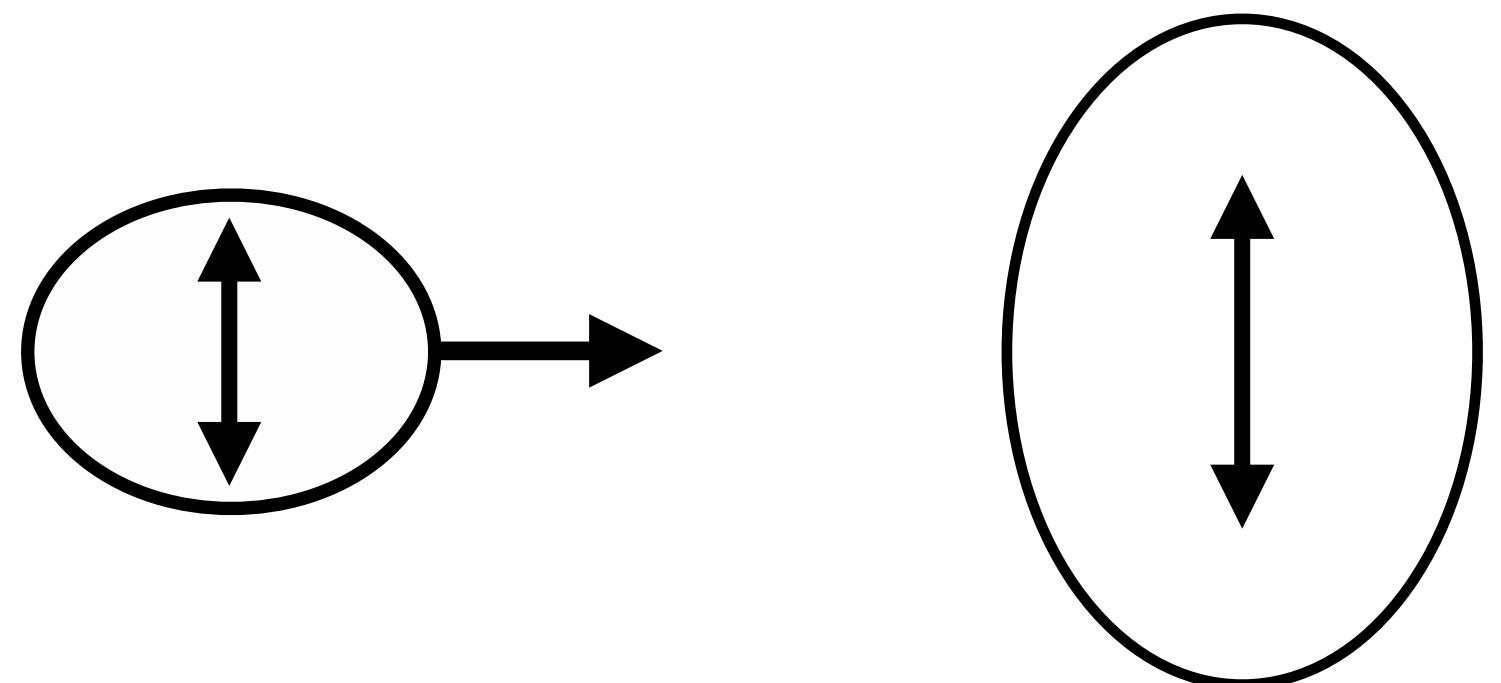


$$|\alpha|^2 + |\beta|^2 = 1$$

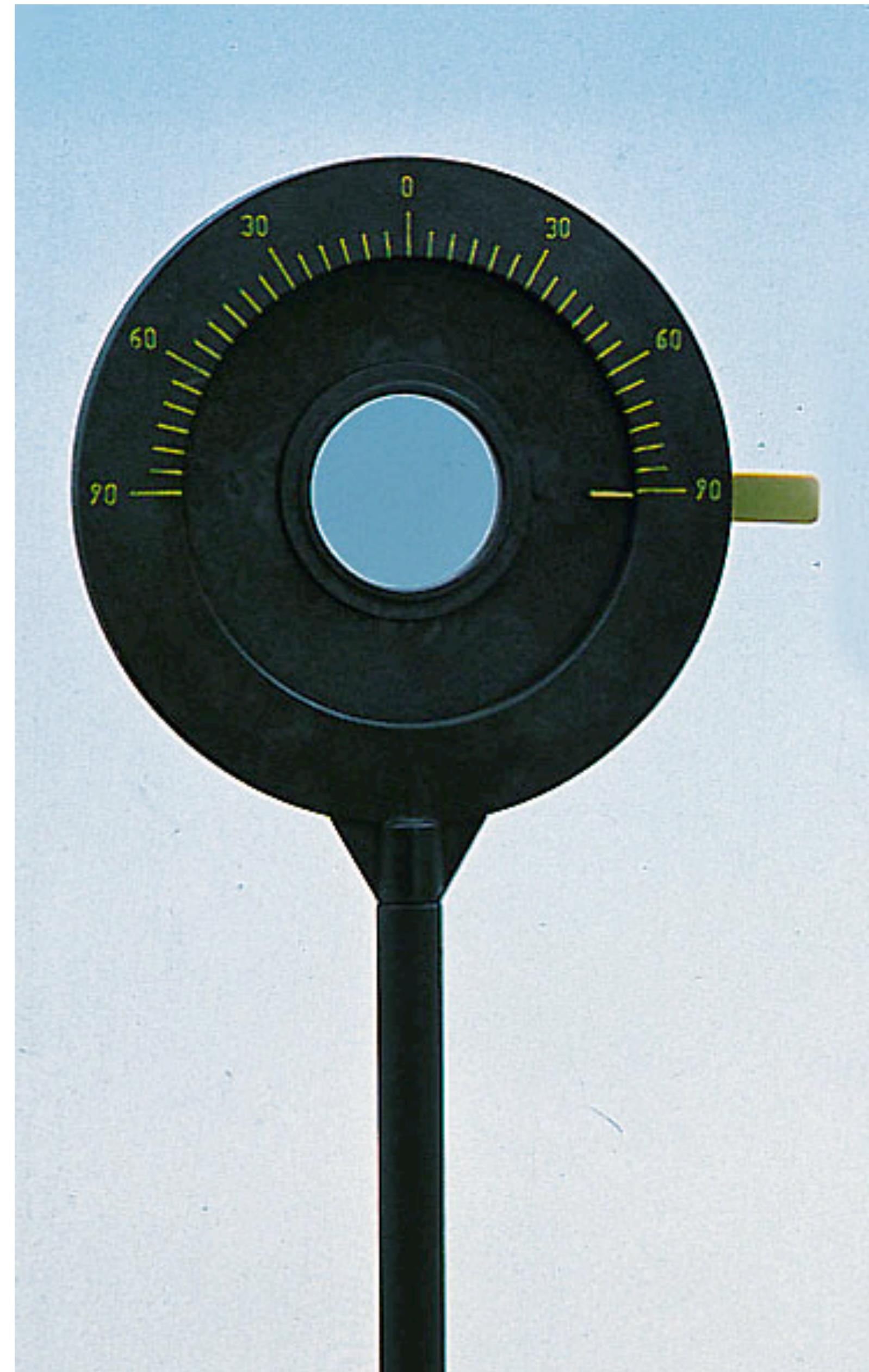
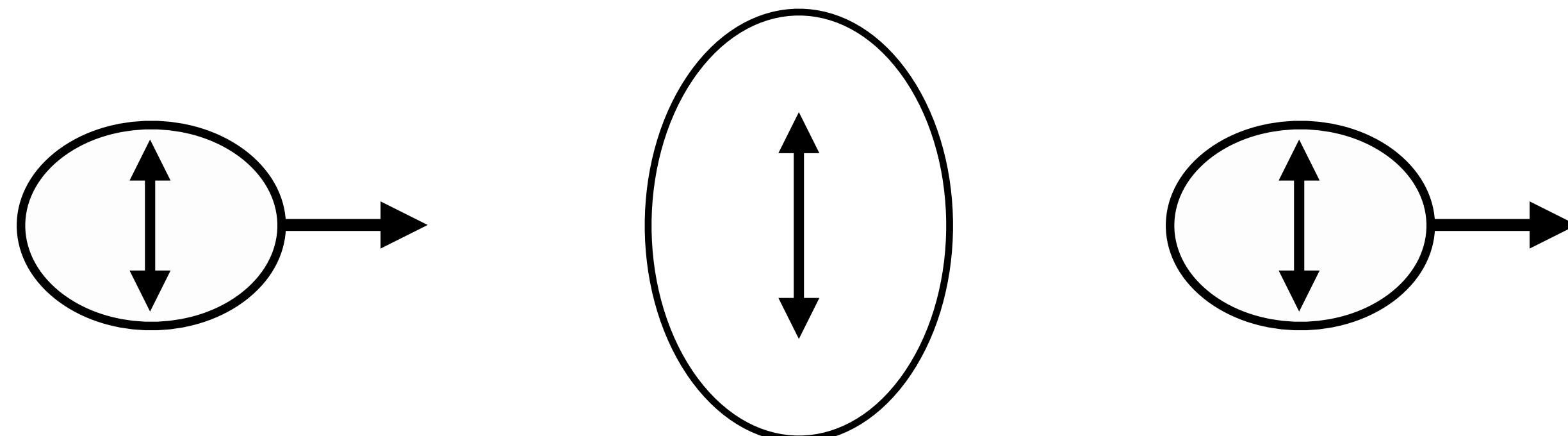
Le polariseur



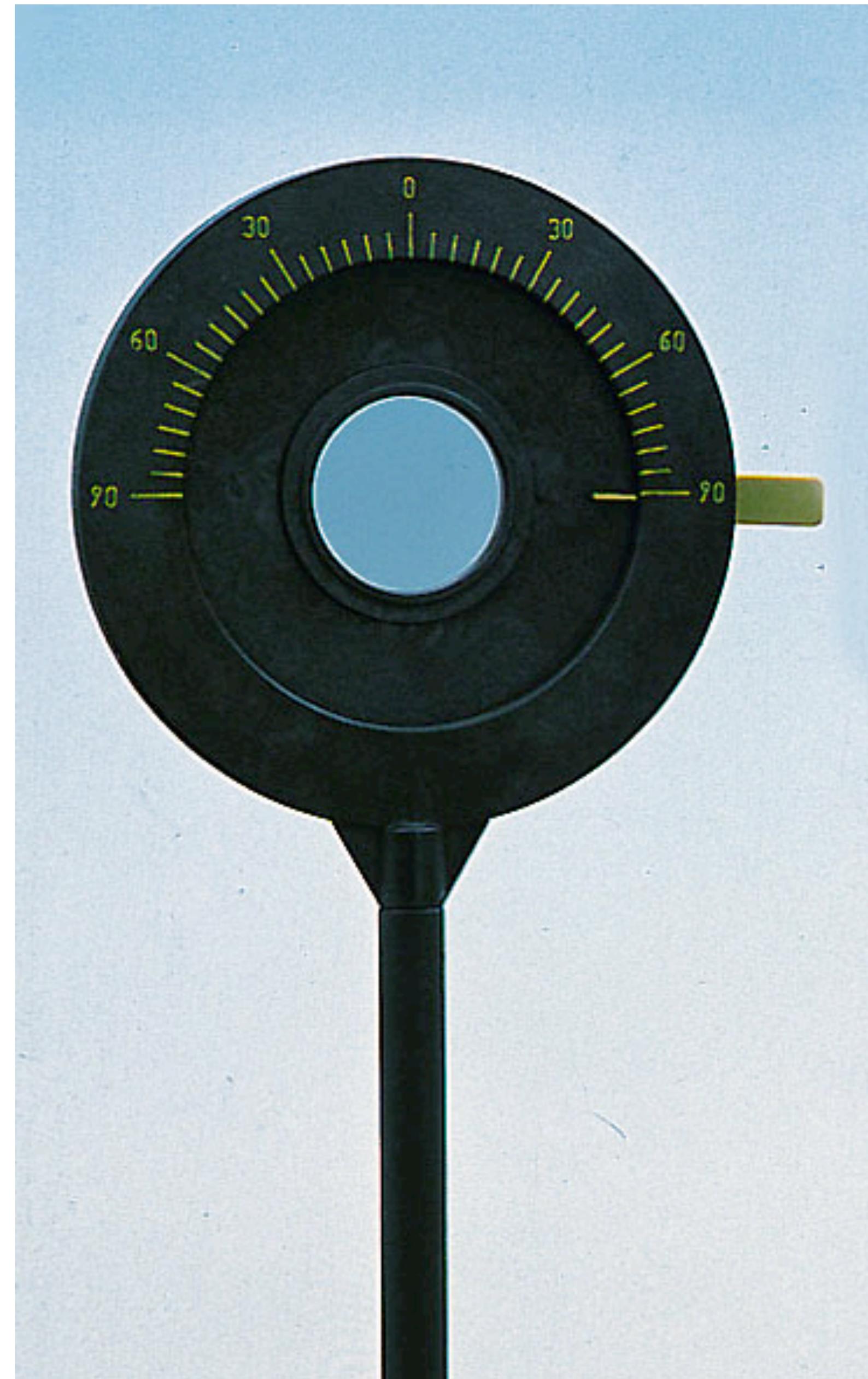
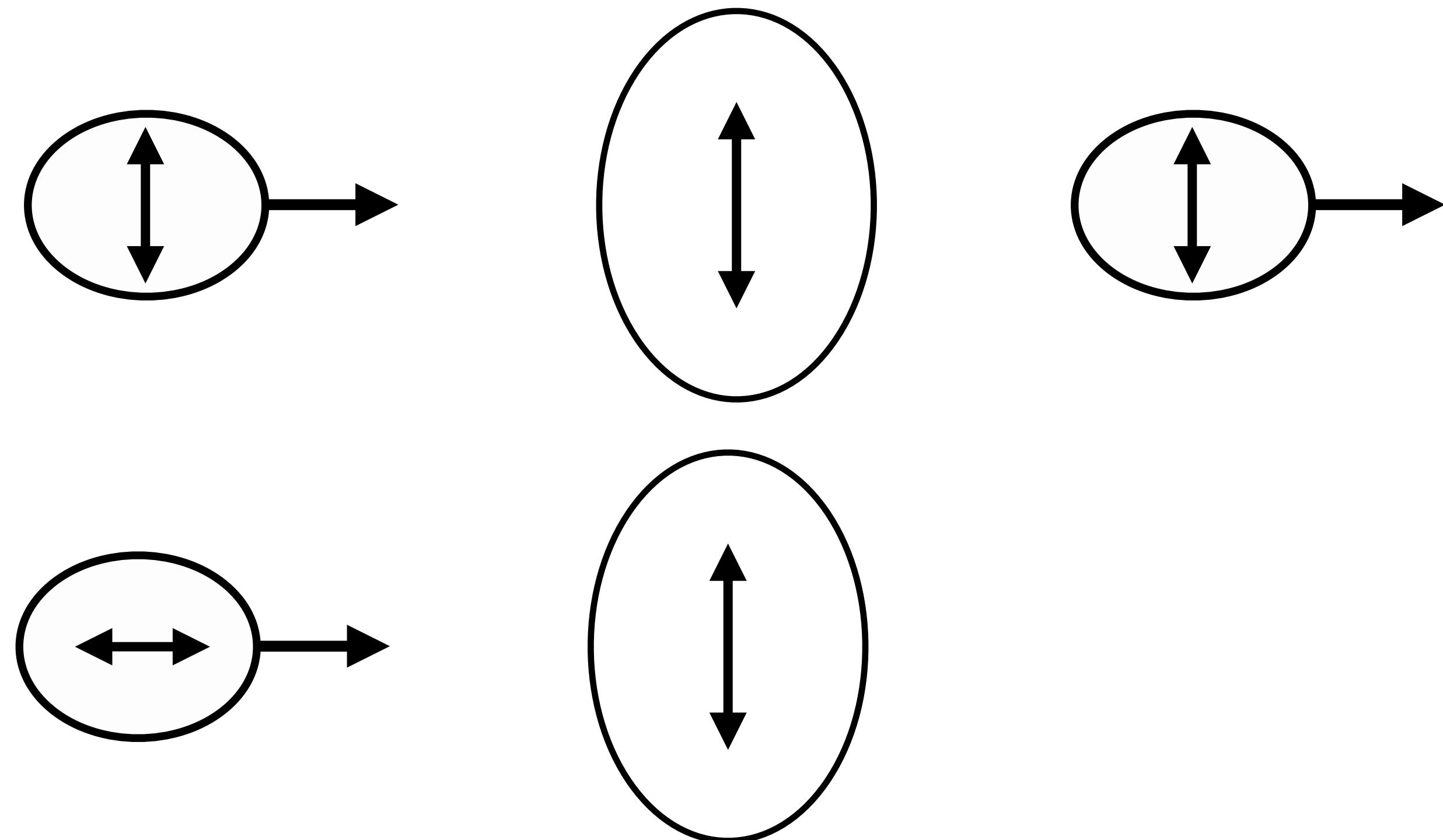
Le polariseur



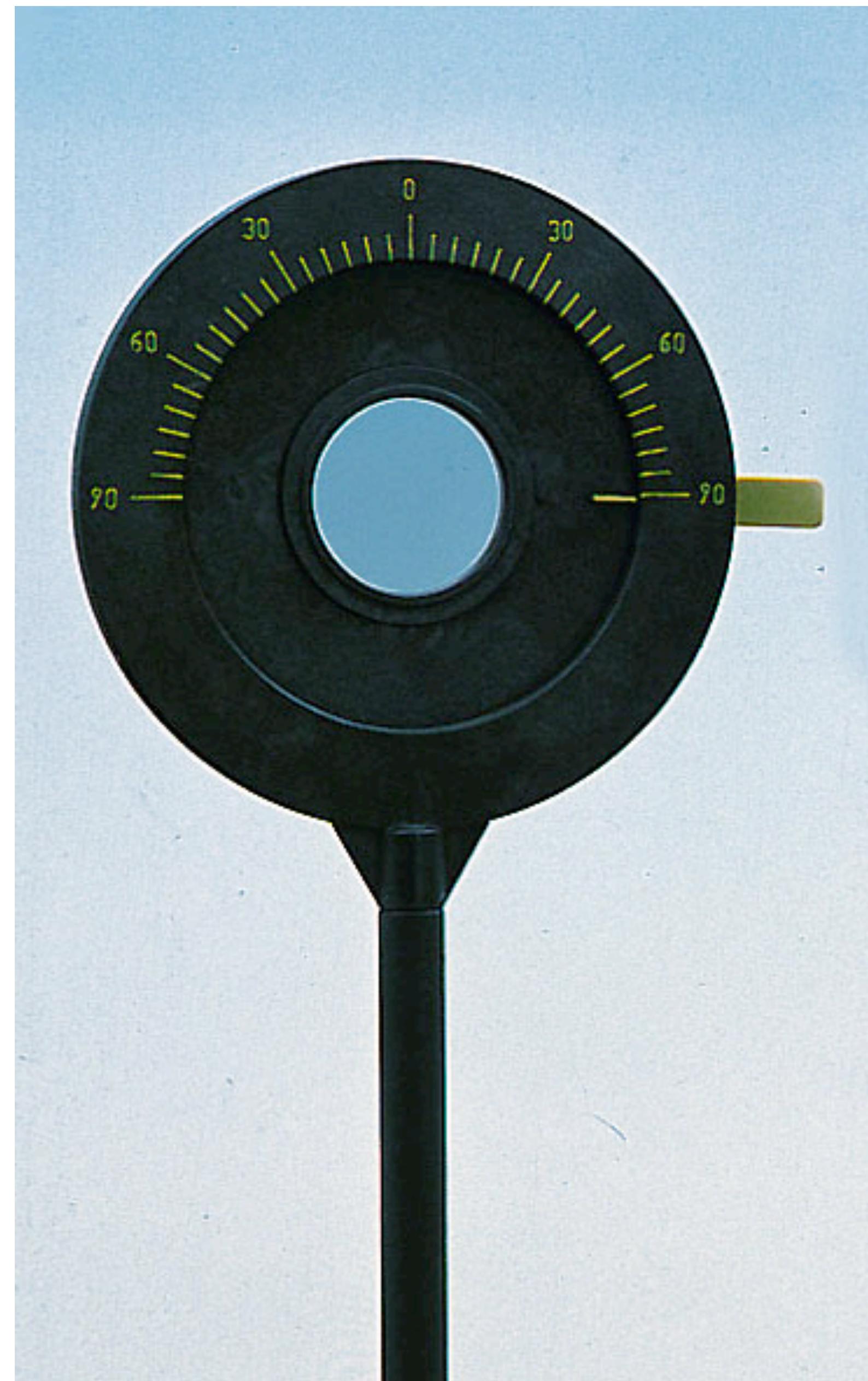
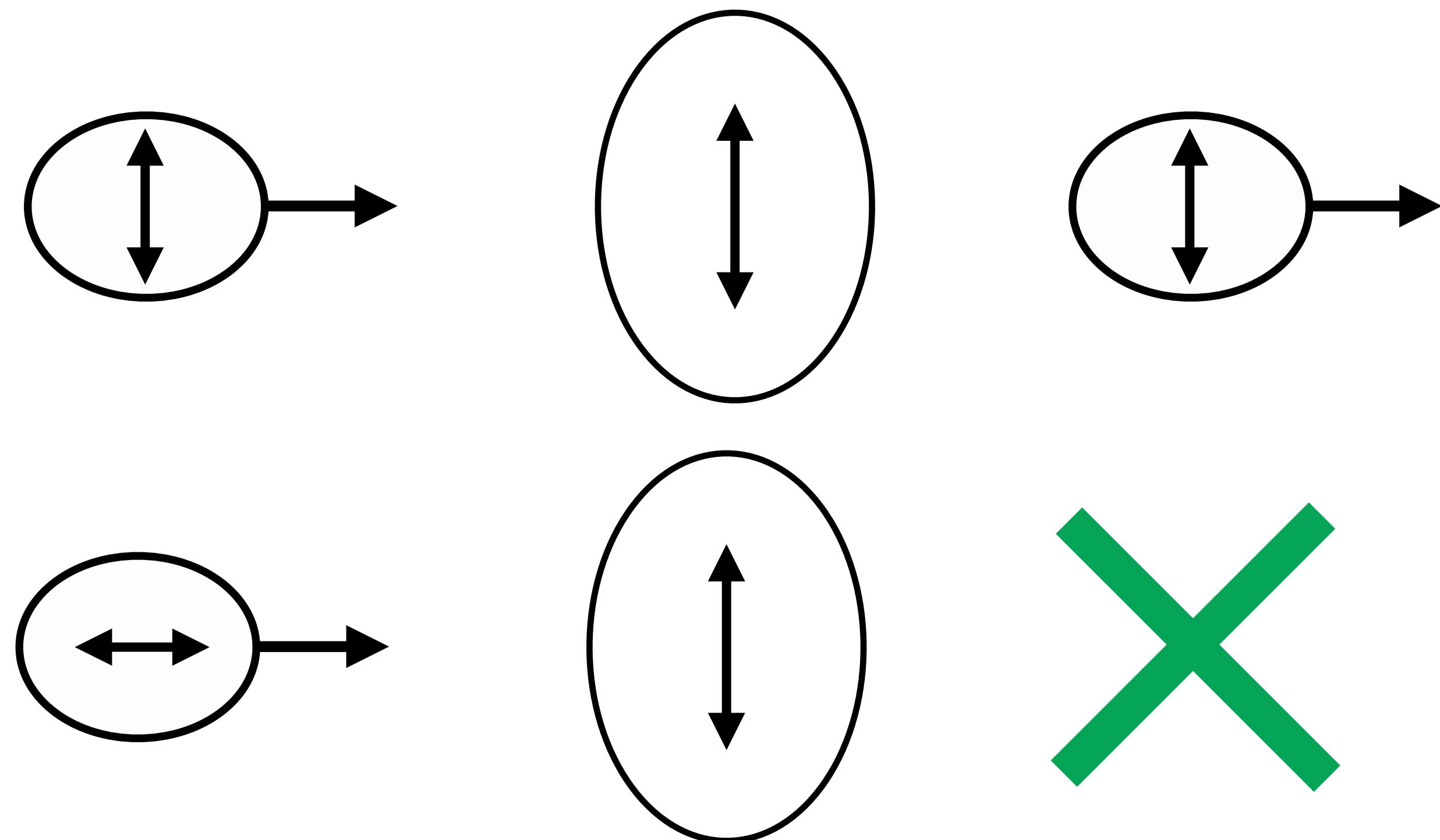
Le polariseur



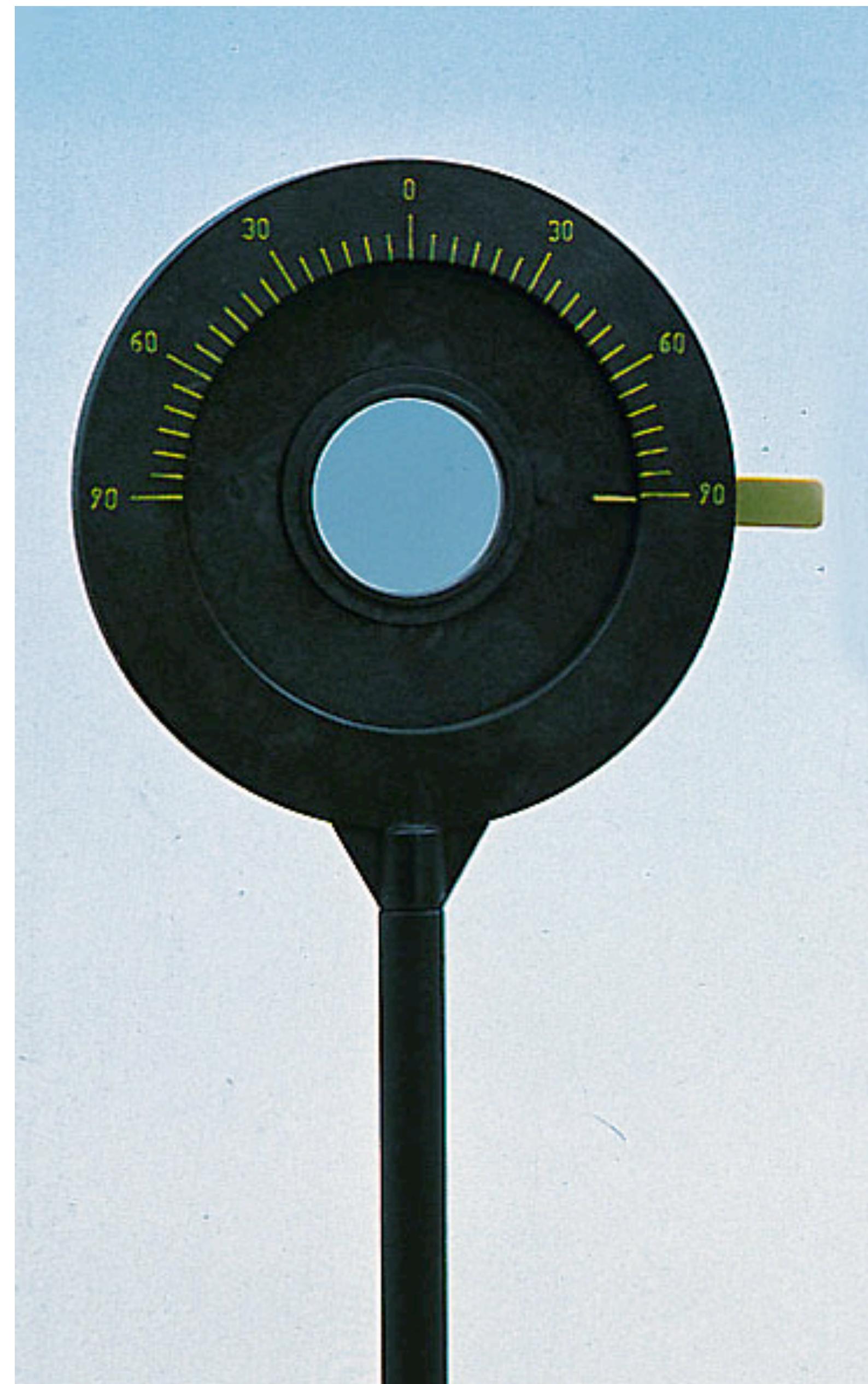
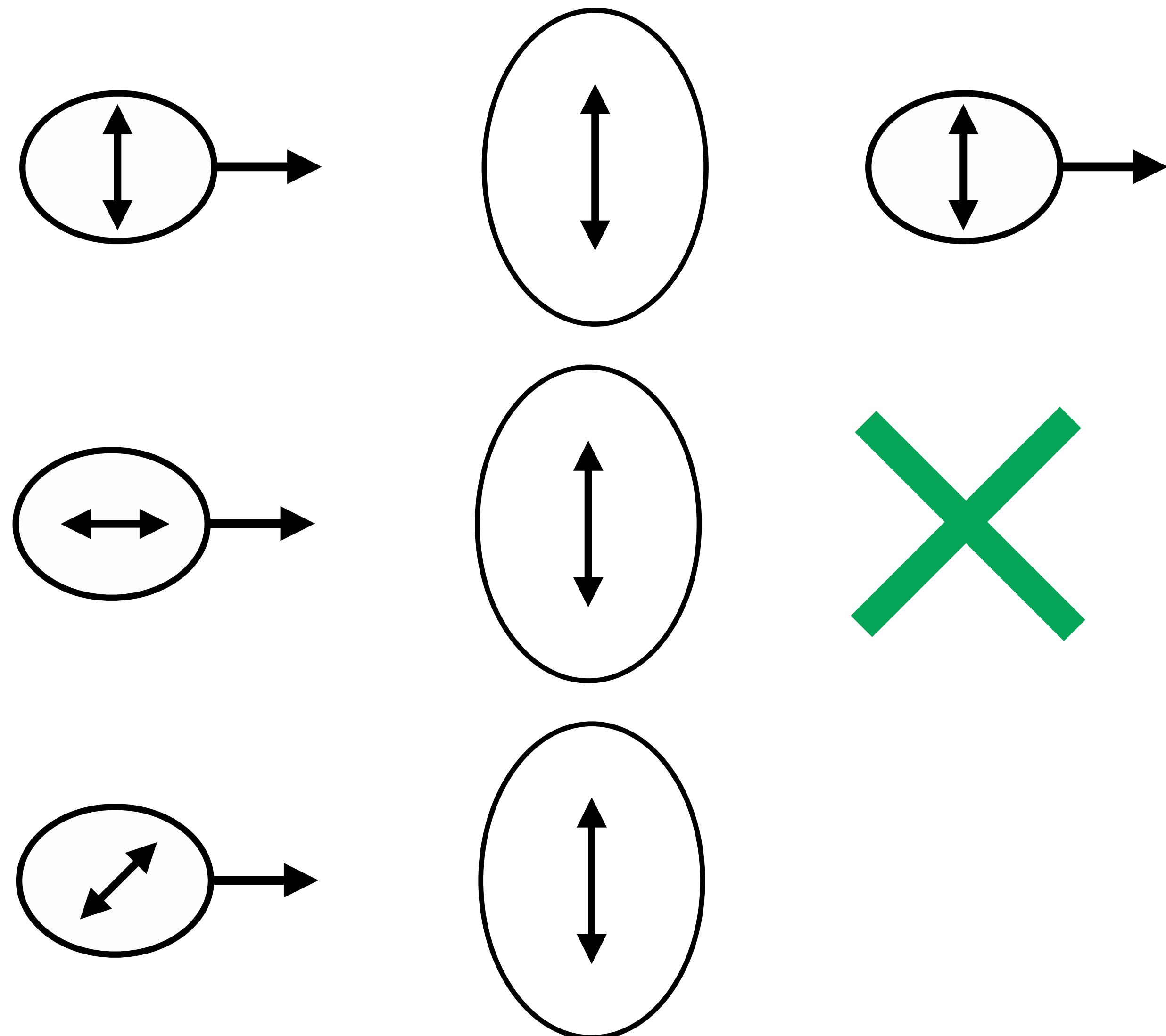
Le polariseur



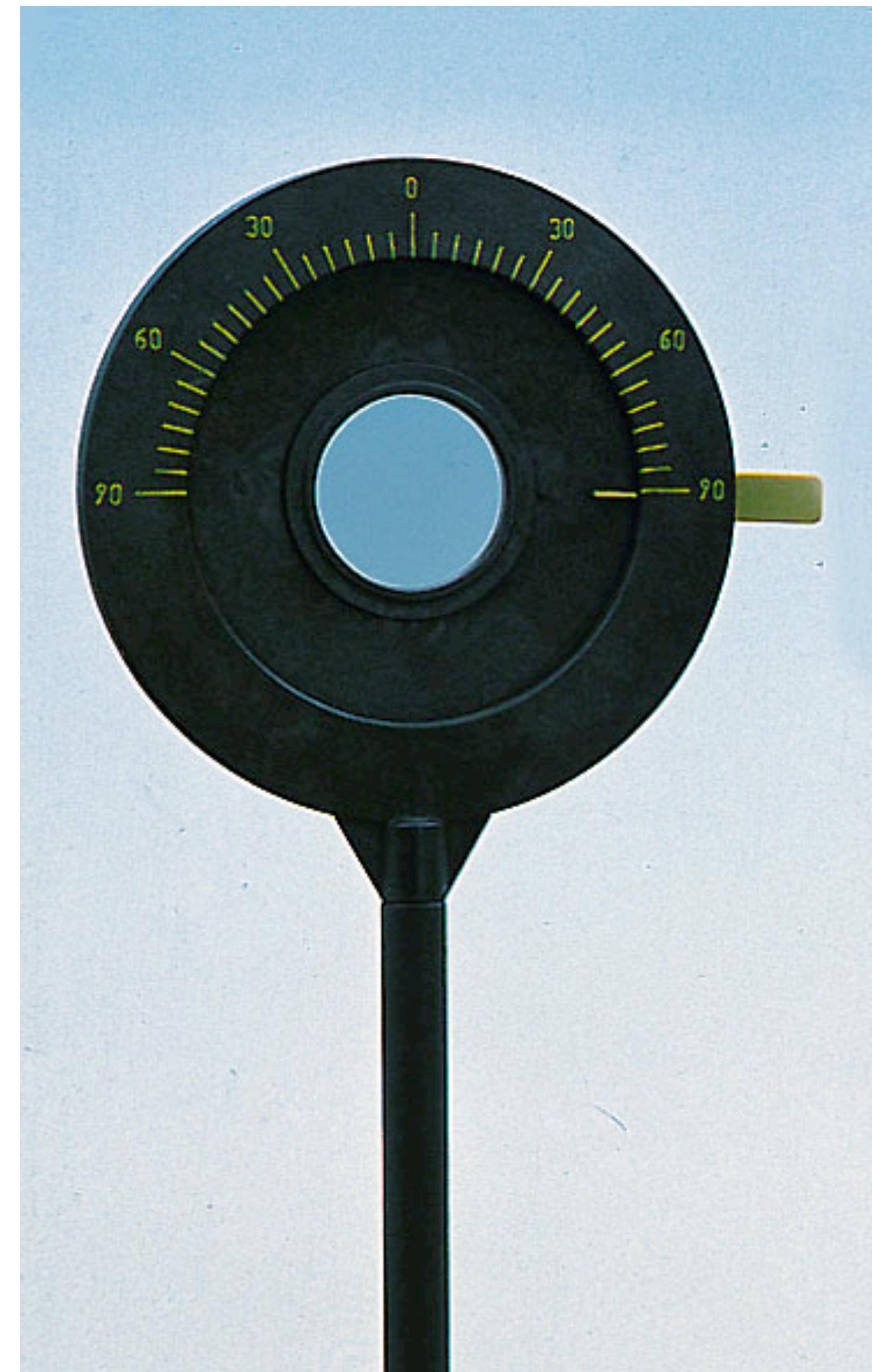
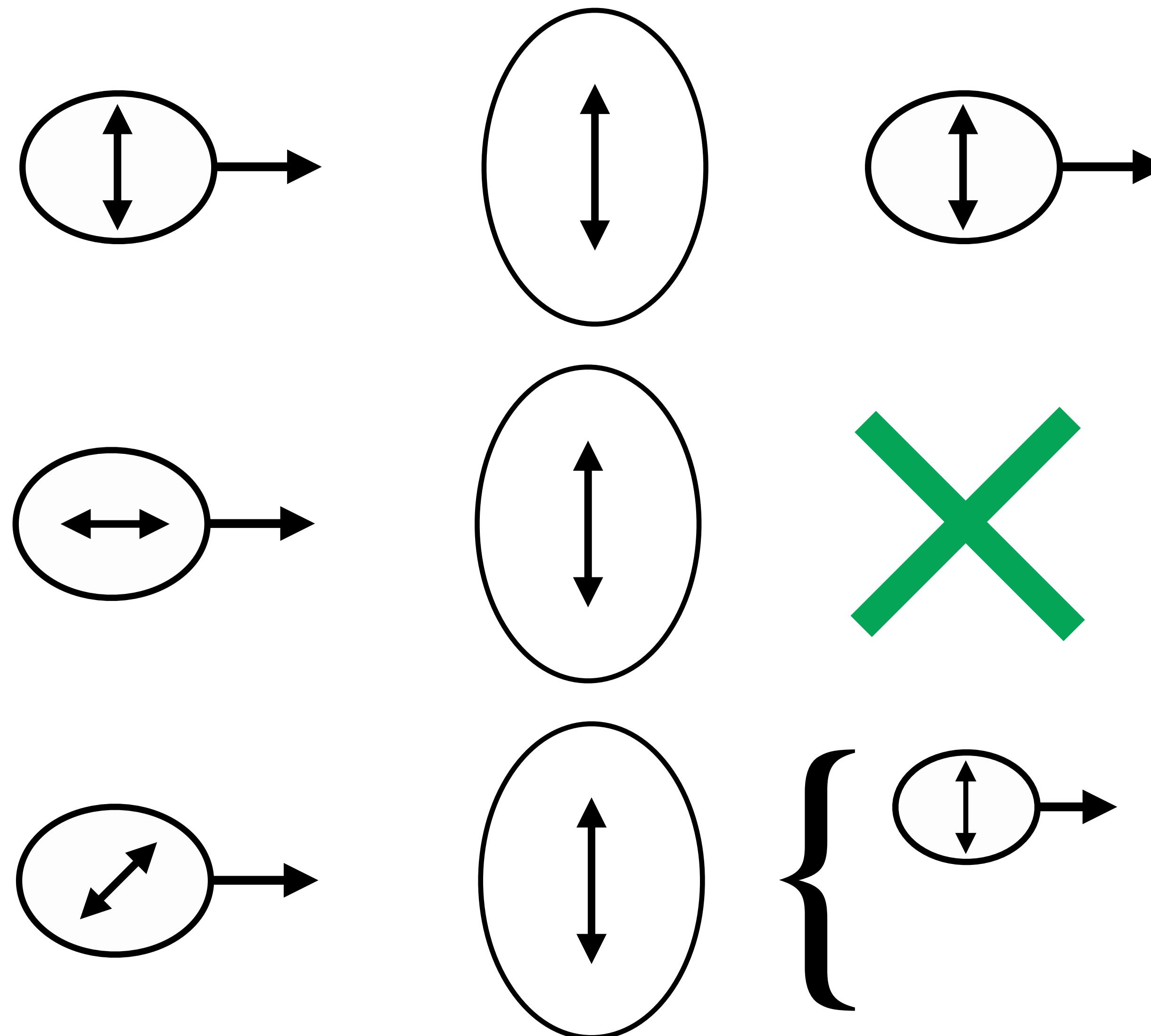
Le polariseur



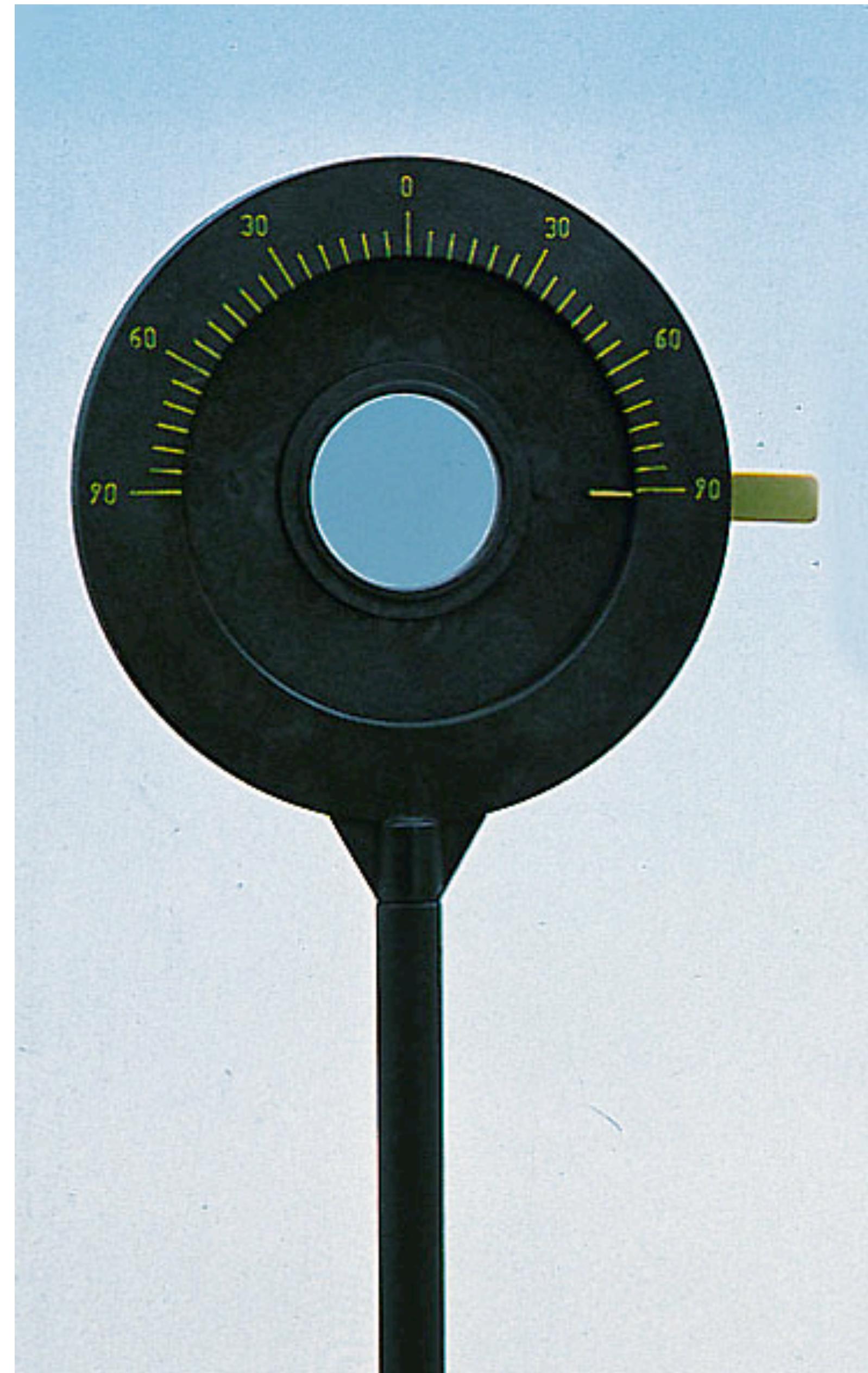
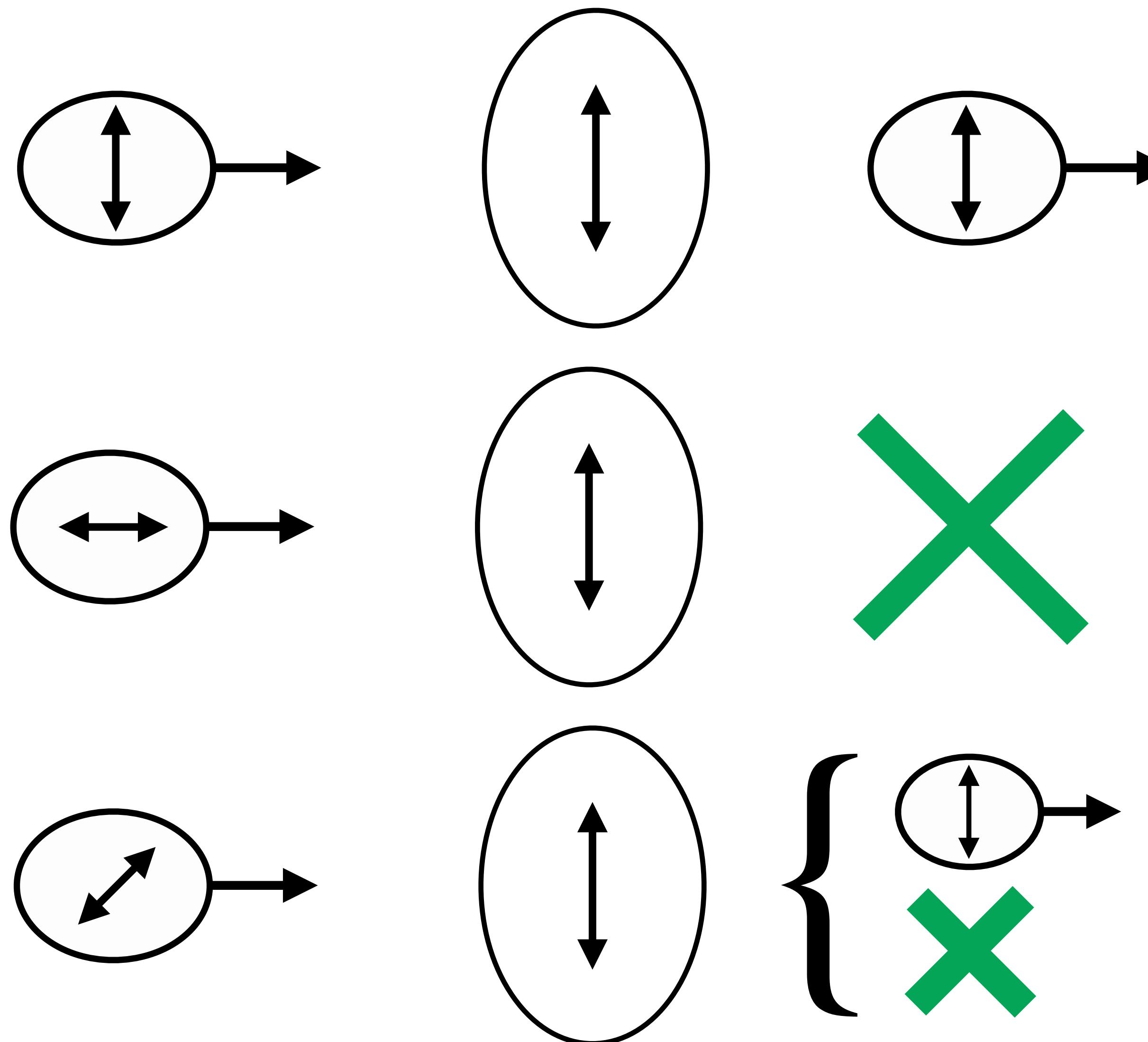
Le polariseur



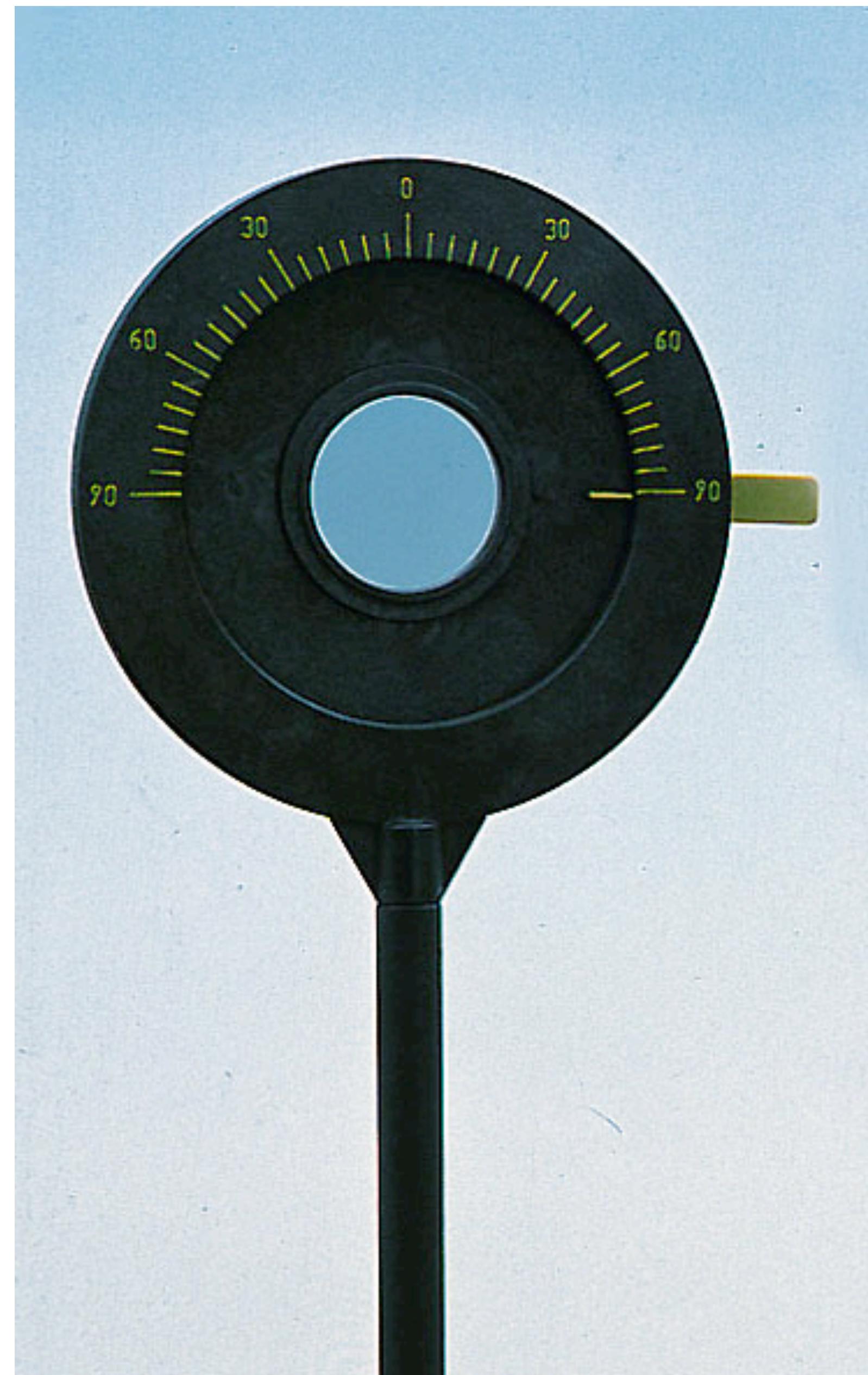
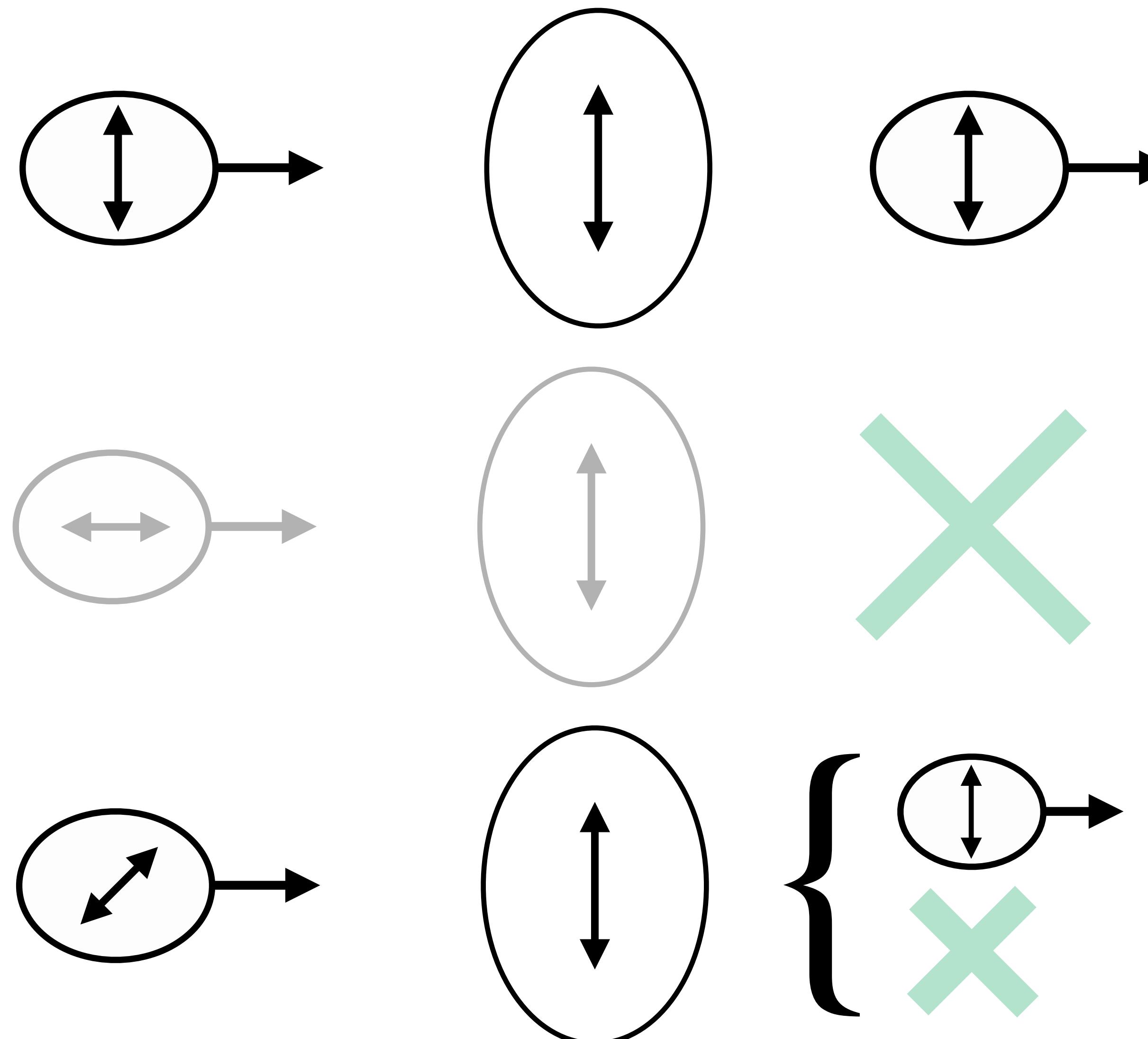
Le polariseur



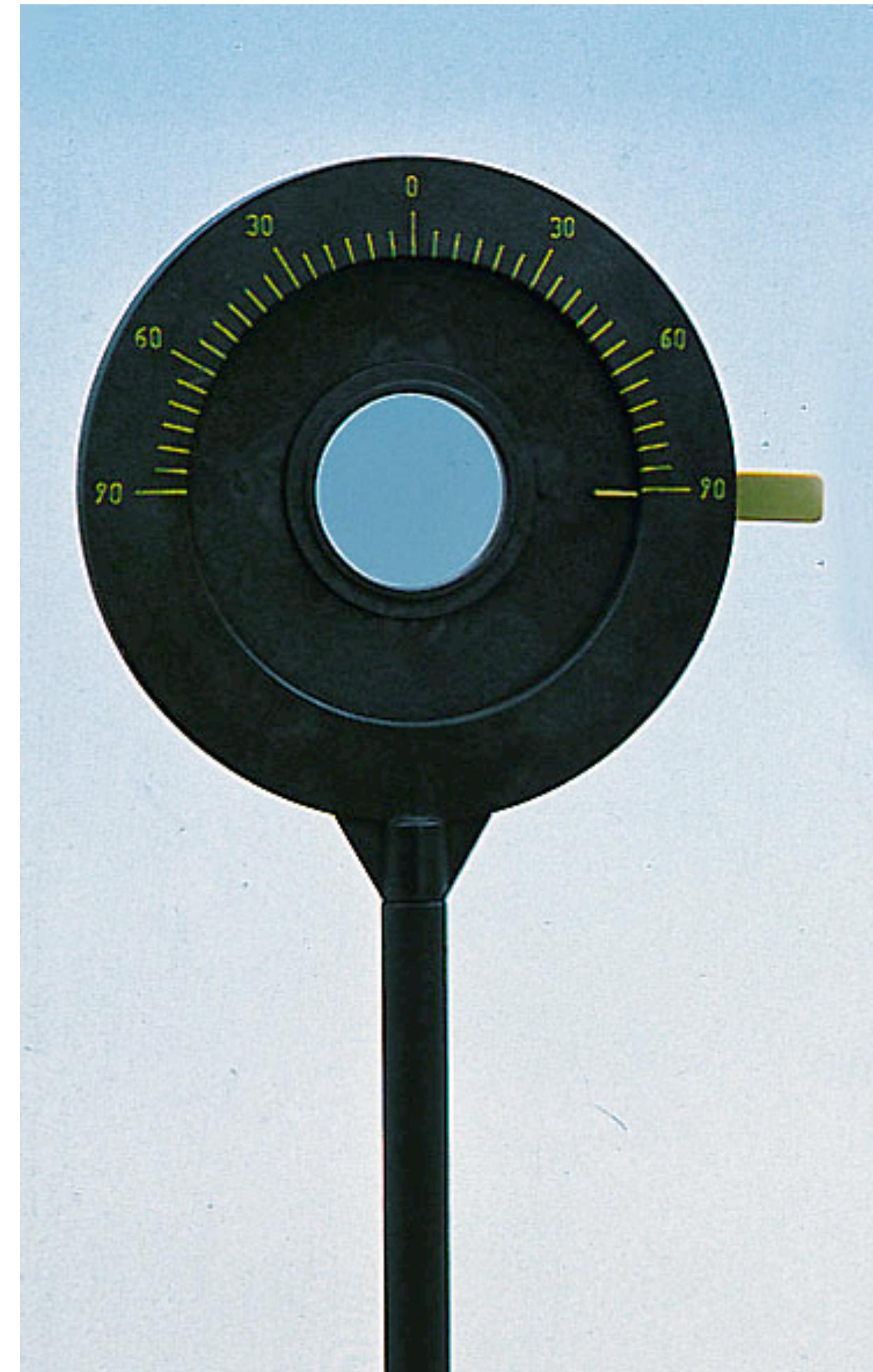
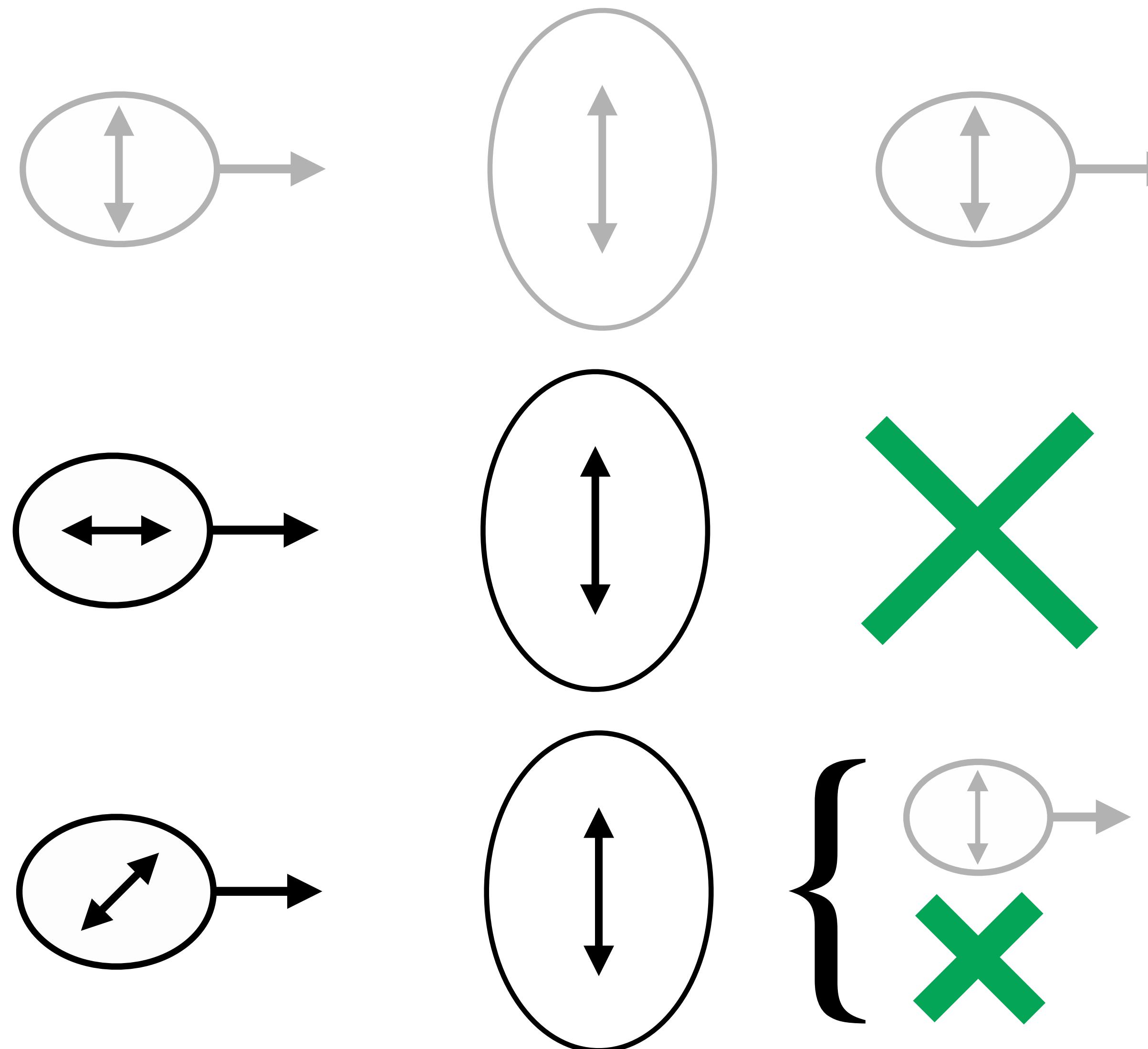
Le polariseur



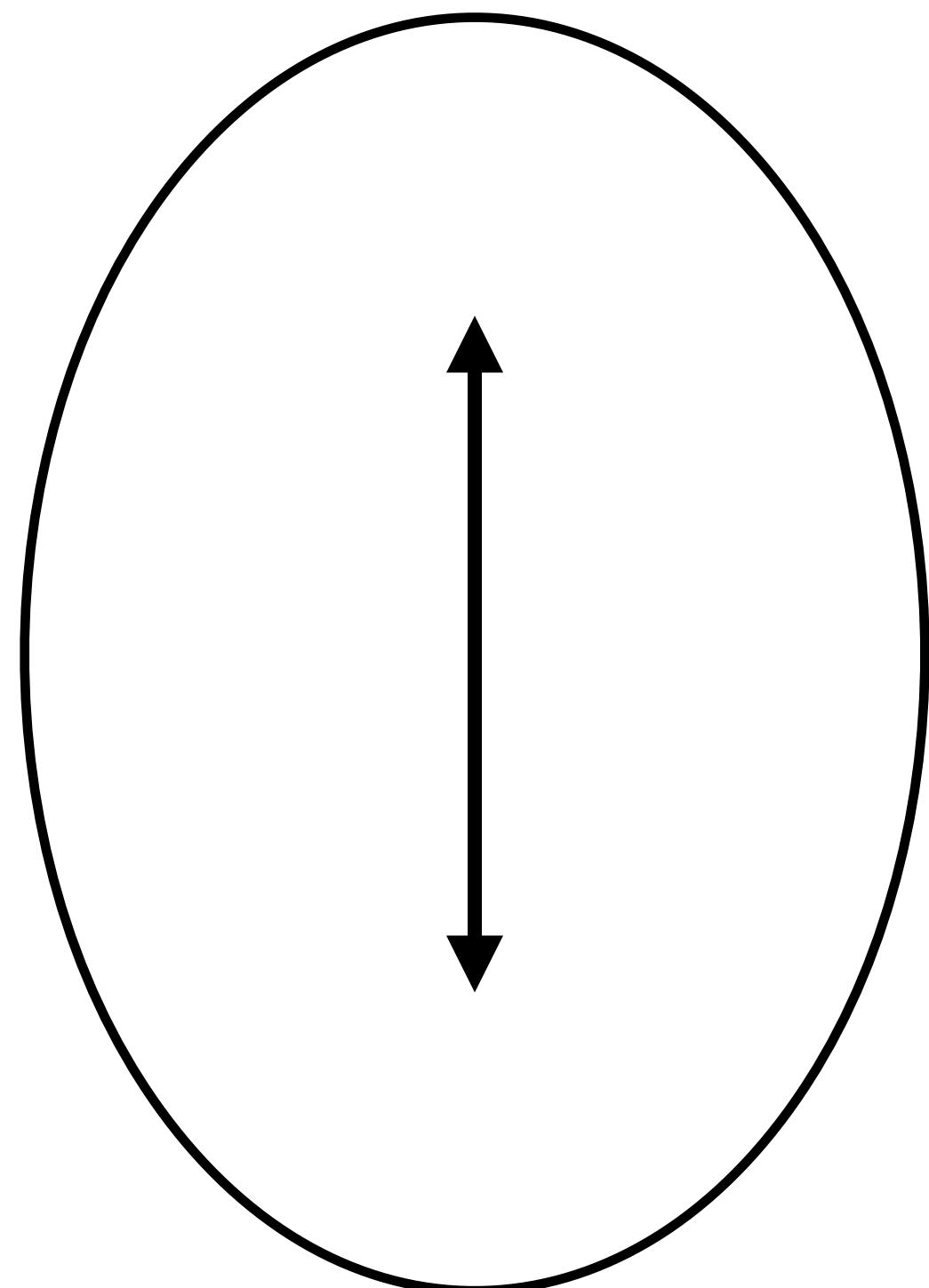
Le polariseur



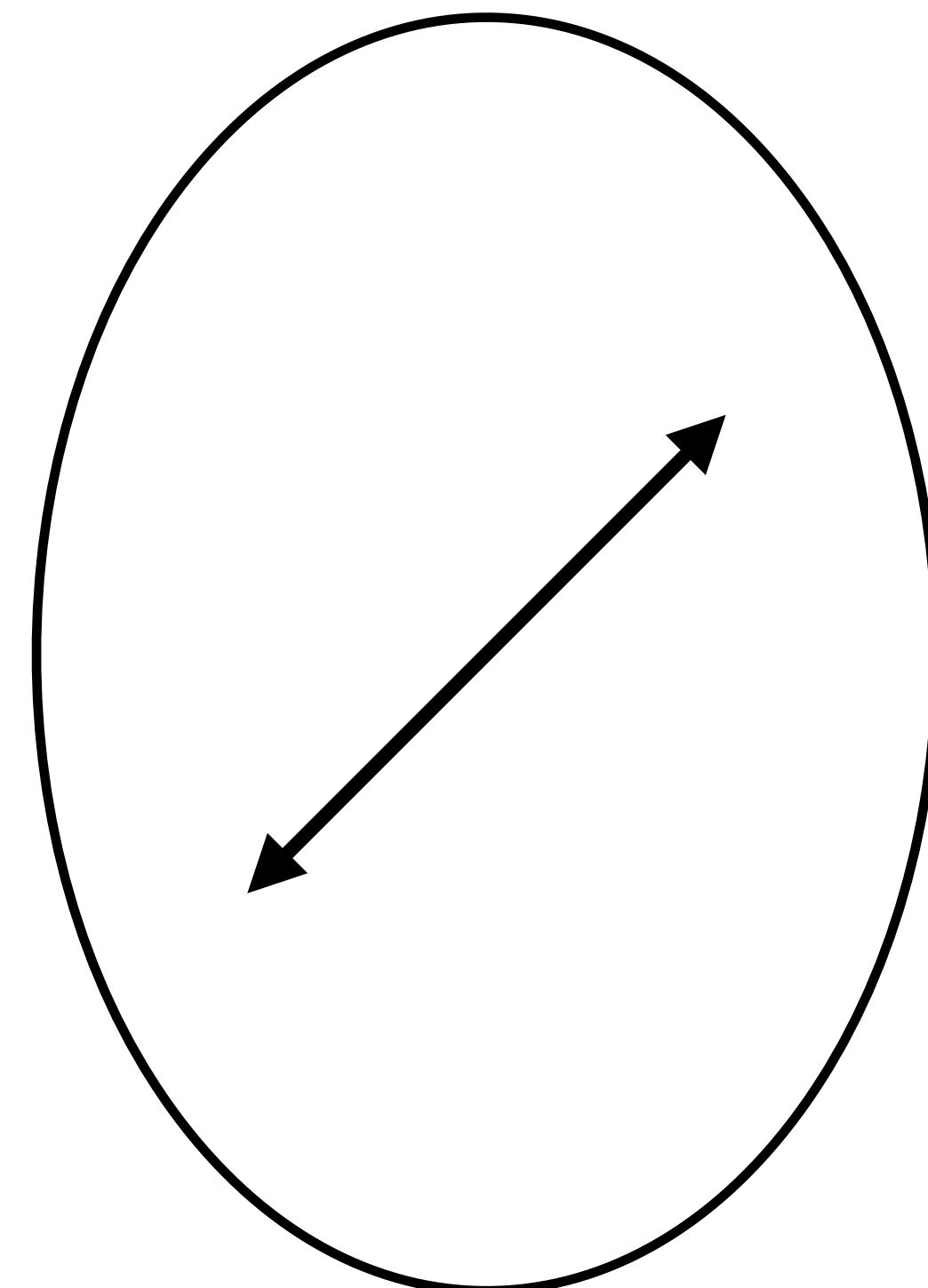
Le polariseur



Base de mesure

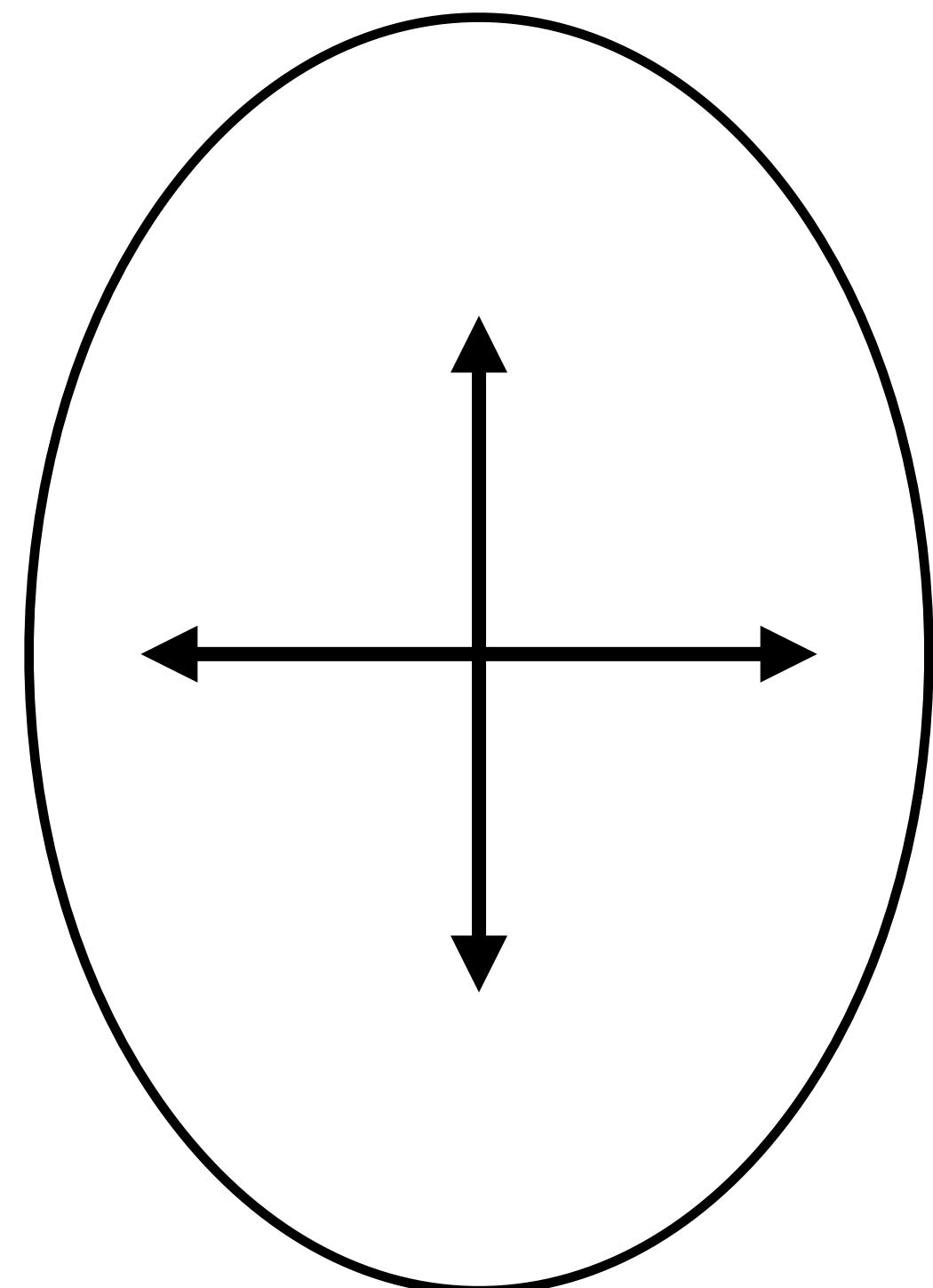


Base Verticale

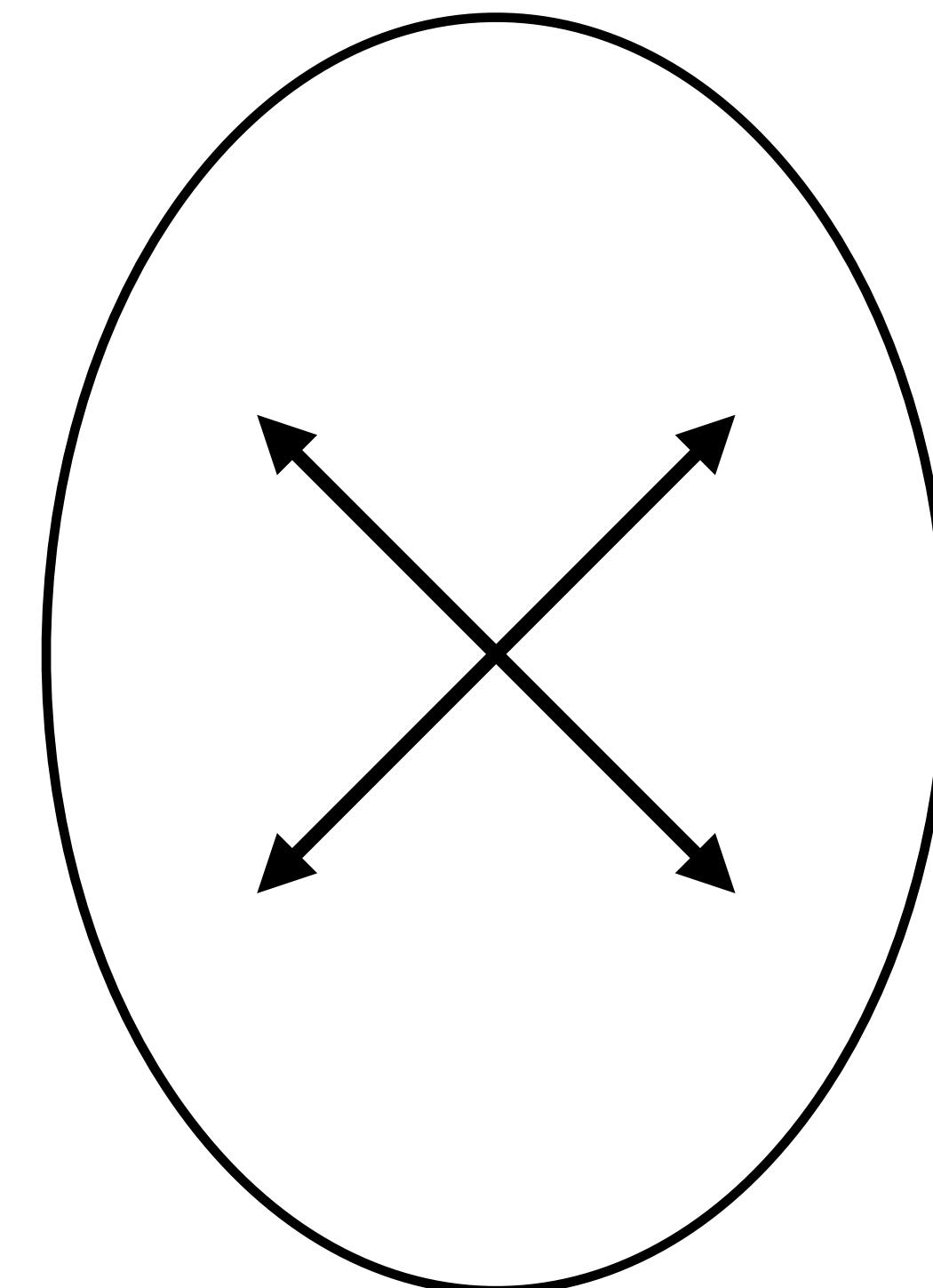


Base Diagonale

Base de mesure

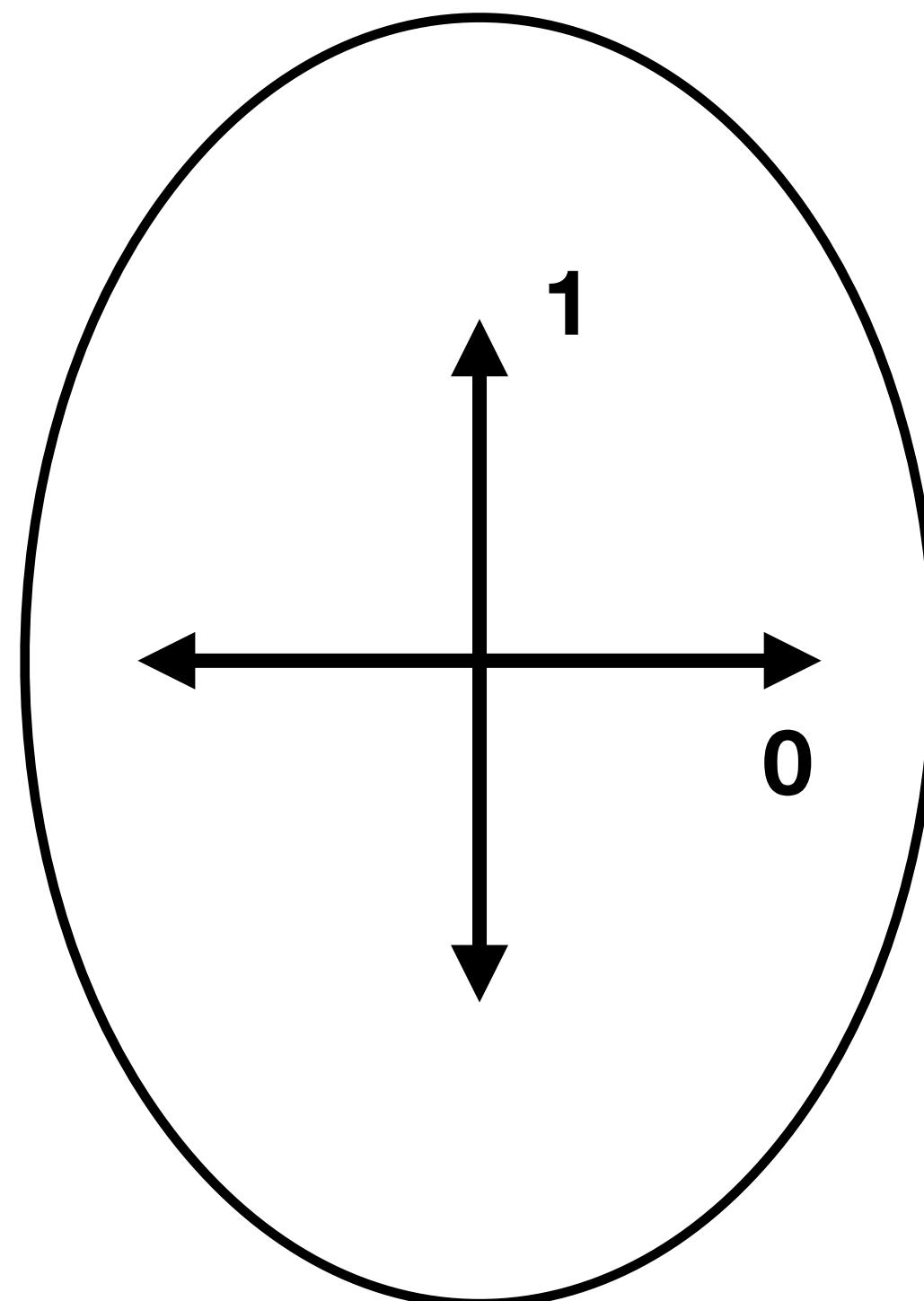


Base Verticale

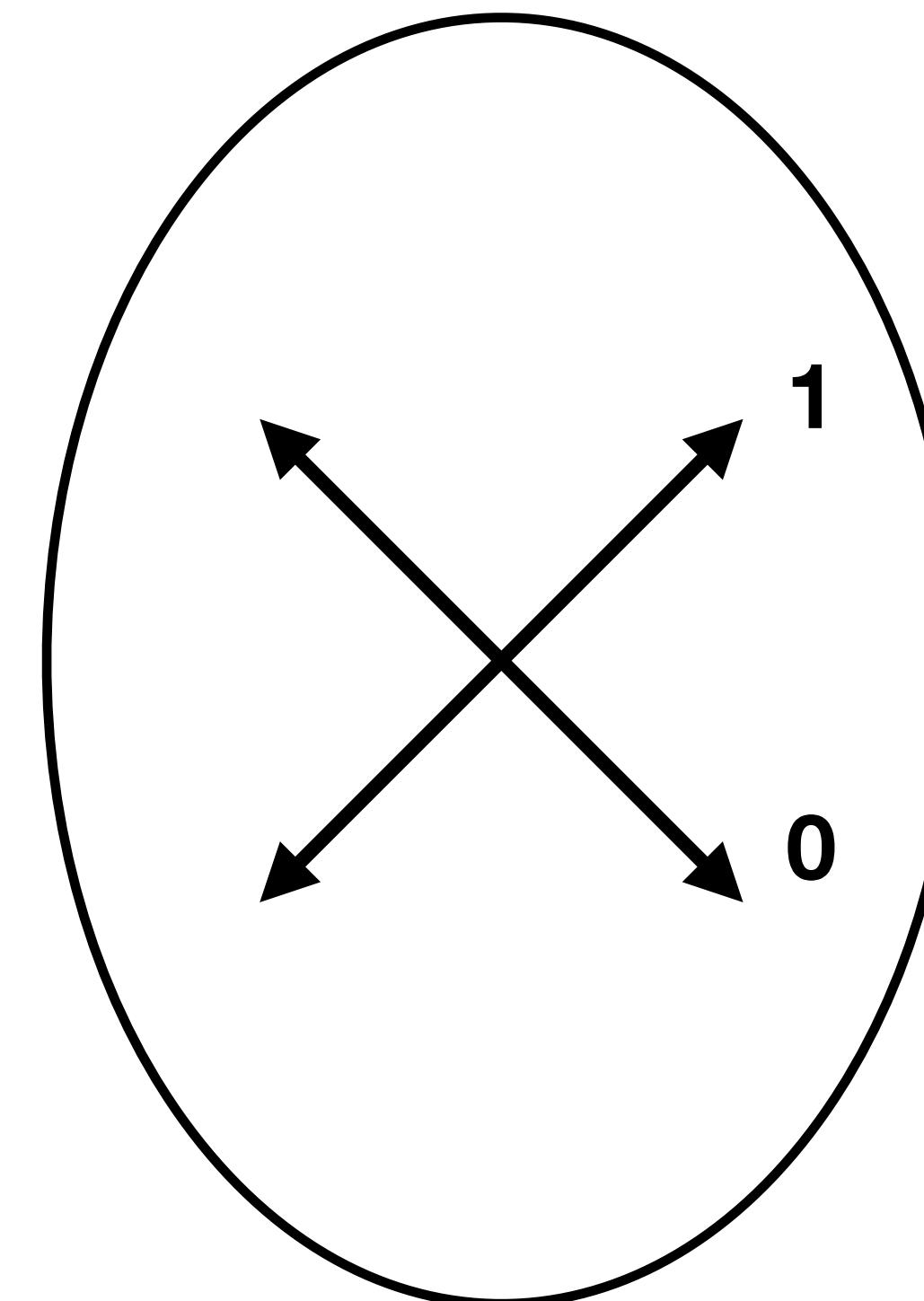


Base Diagonale

Base de mesure

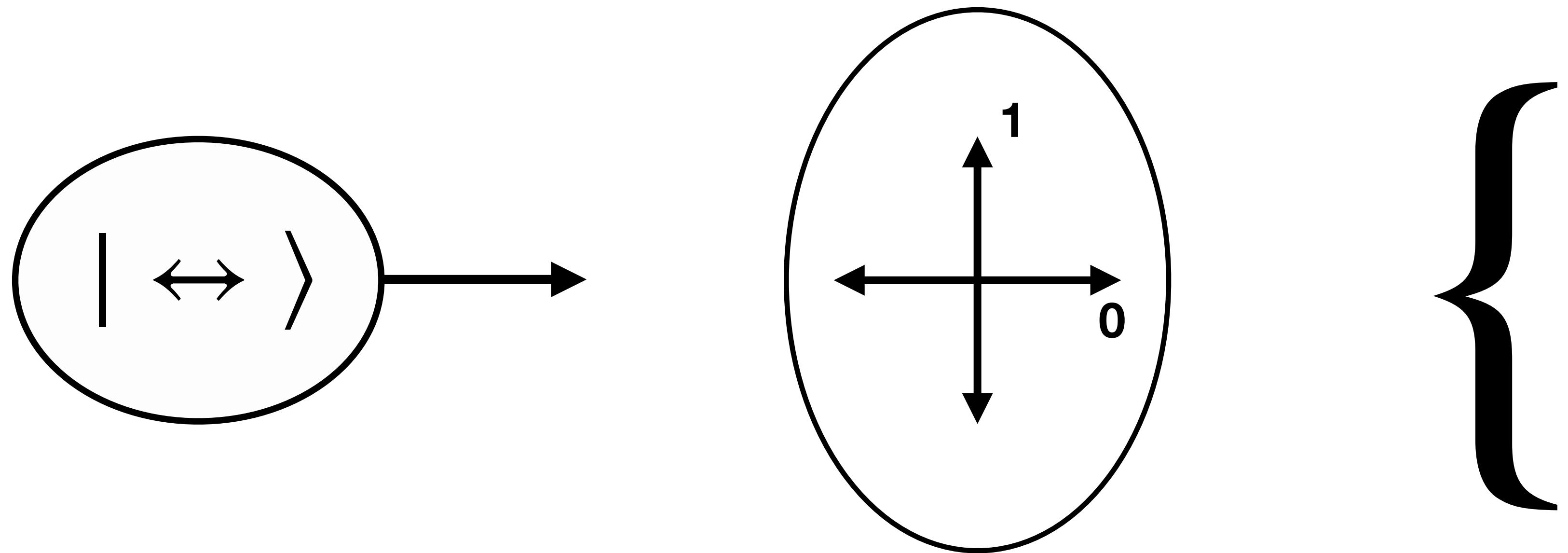


Base Verticale



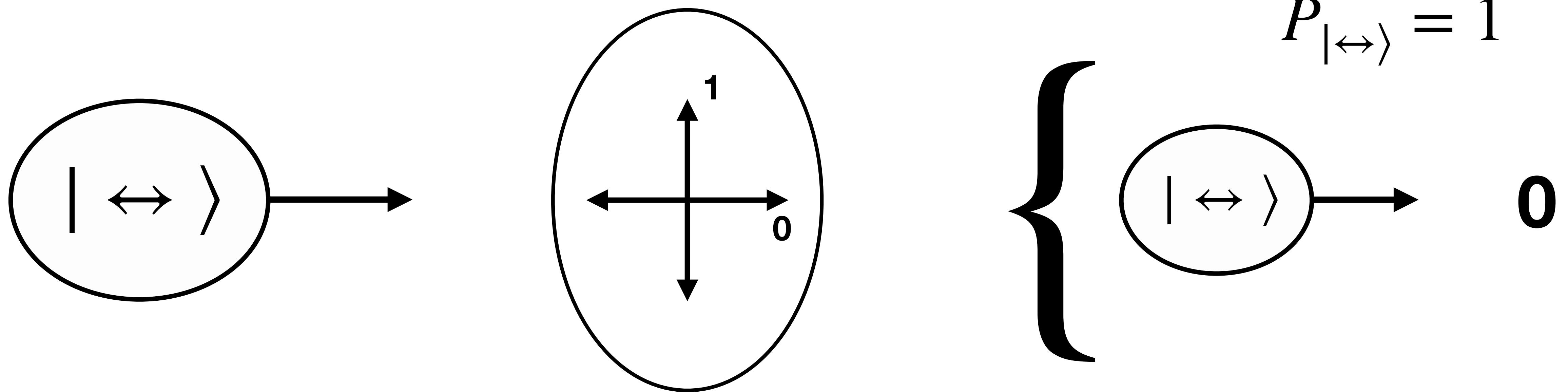
Base Diagonale

Measure



$$\begin{aligned} |90^\circ\rangle &\equiv |\uparrow\downarrow\rangle \\ |0^\circ\rangle &\equiv |\leftrightarrow\rangle \end{aligned}$$

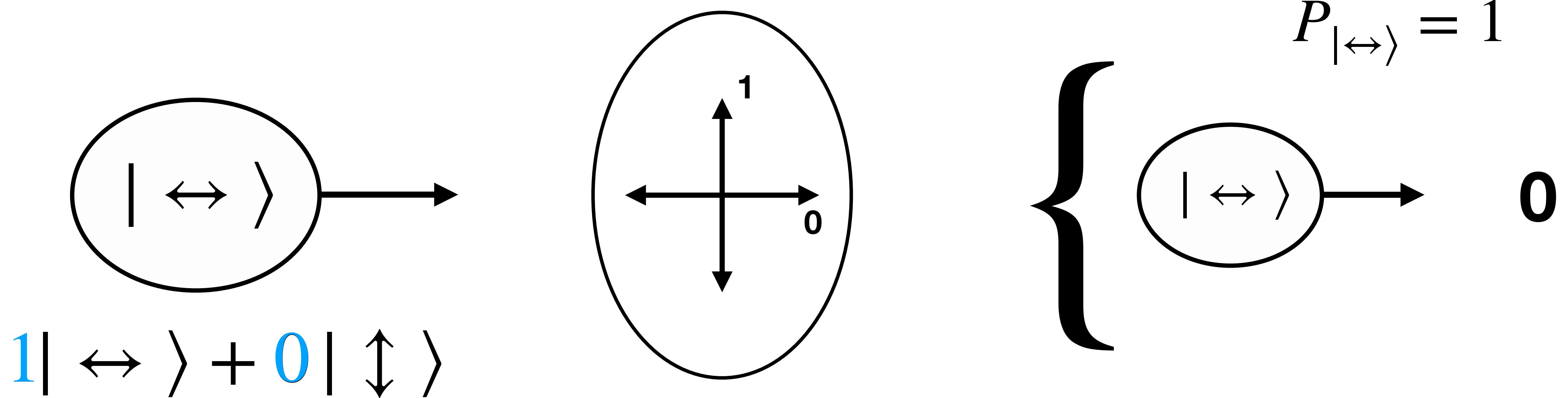
Measure



$$|90^\circ\rangle \equiv | \uparrow \rangle$$

$$|0^\circ\rangle \equiv | \leftrightarrow \rangle$$

Measure

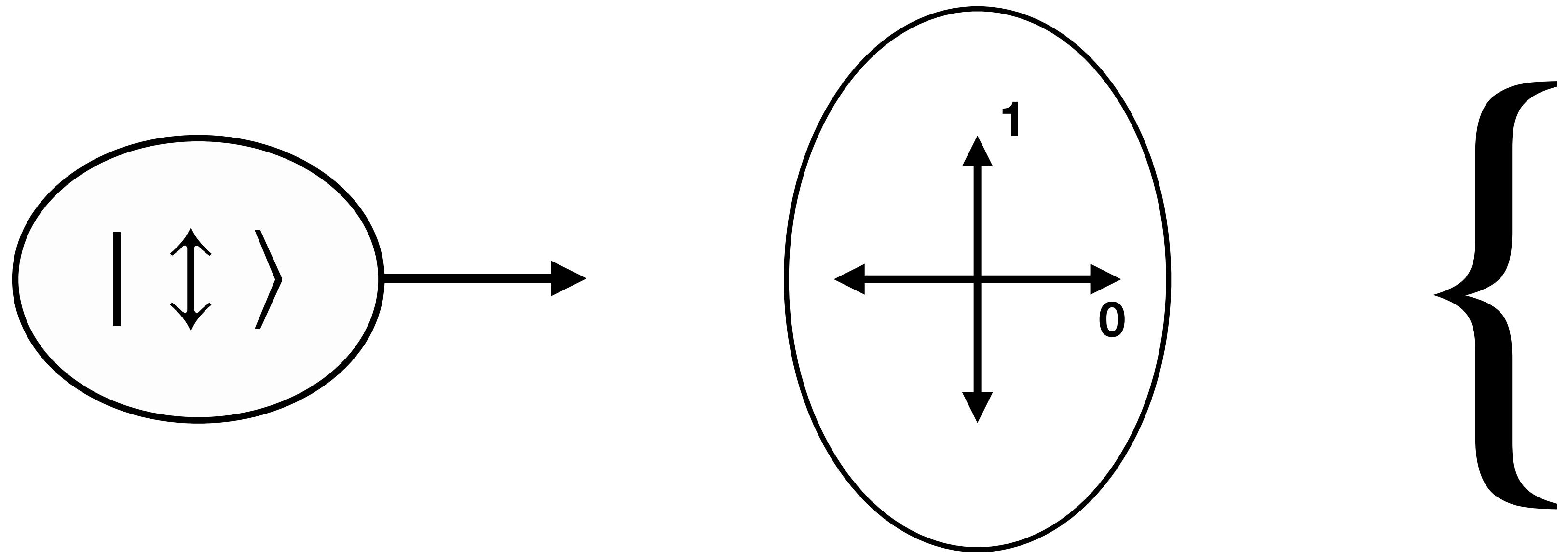


$$\begin{aligned}|90^\circ\rangle &\equiv |\uparrow\downarrow\rangle \\|0^\circ\rangle &\equiv |\leftrightarrow\rangle\end{aligned}$$

$$P_{|\leftrightarrow\rangle} = |1|^2$$

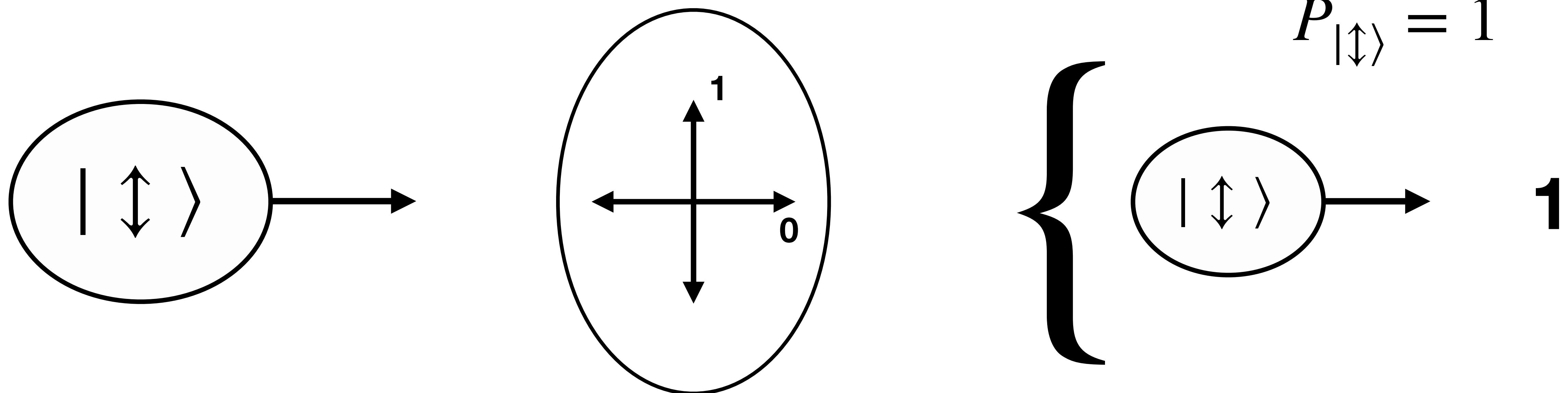
$$P_{|\uparrow\downarrow\rangle} = |0|^2$$

Measure



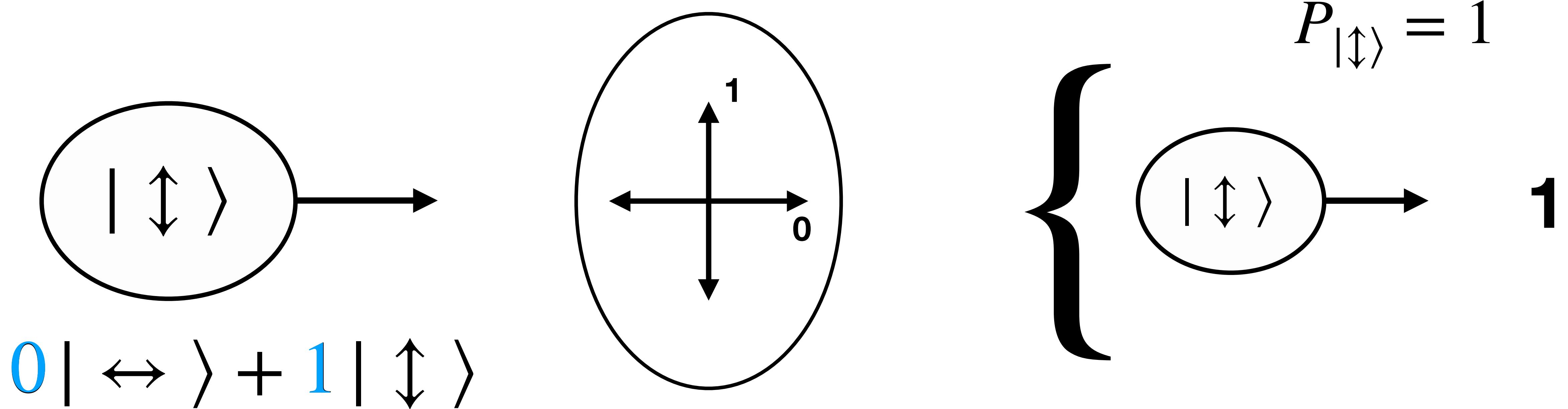
$$|90^\circ\rangle \equiv |\uparrow\rangle$$
$$|0^\circ\rangle \equiv |\leftrightarrow\rangle$$

Measure



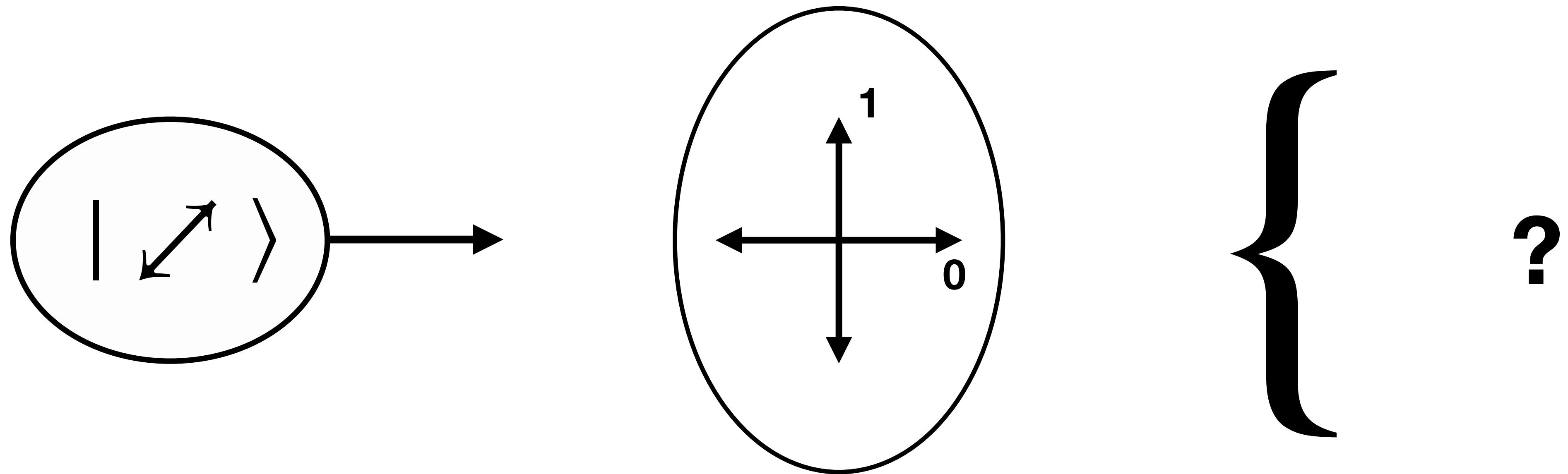
$$\begin{aligned}|90^\circ\rangle &\equiv |\uparrow\downarrow\rangle \\ |0^\circ\rangle &\equiv |\leftrightarrow\rangle\end{aligned}$$

Measure



$$\begin{aligned}|90^\circ\rangle &\equiv |\leftrightarrow\rangle \\|0^\circ\rangle &\equiv |\leftrightarrow\rangle\end{aligned}$$

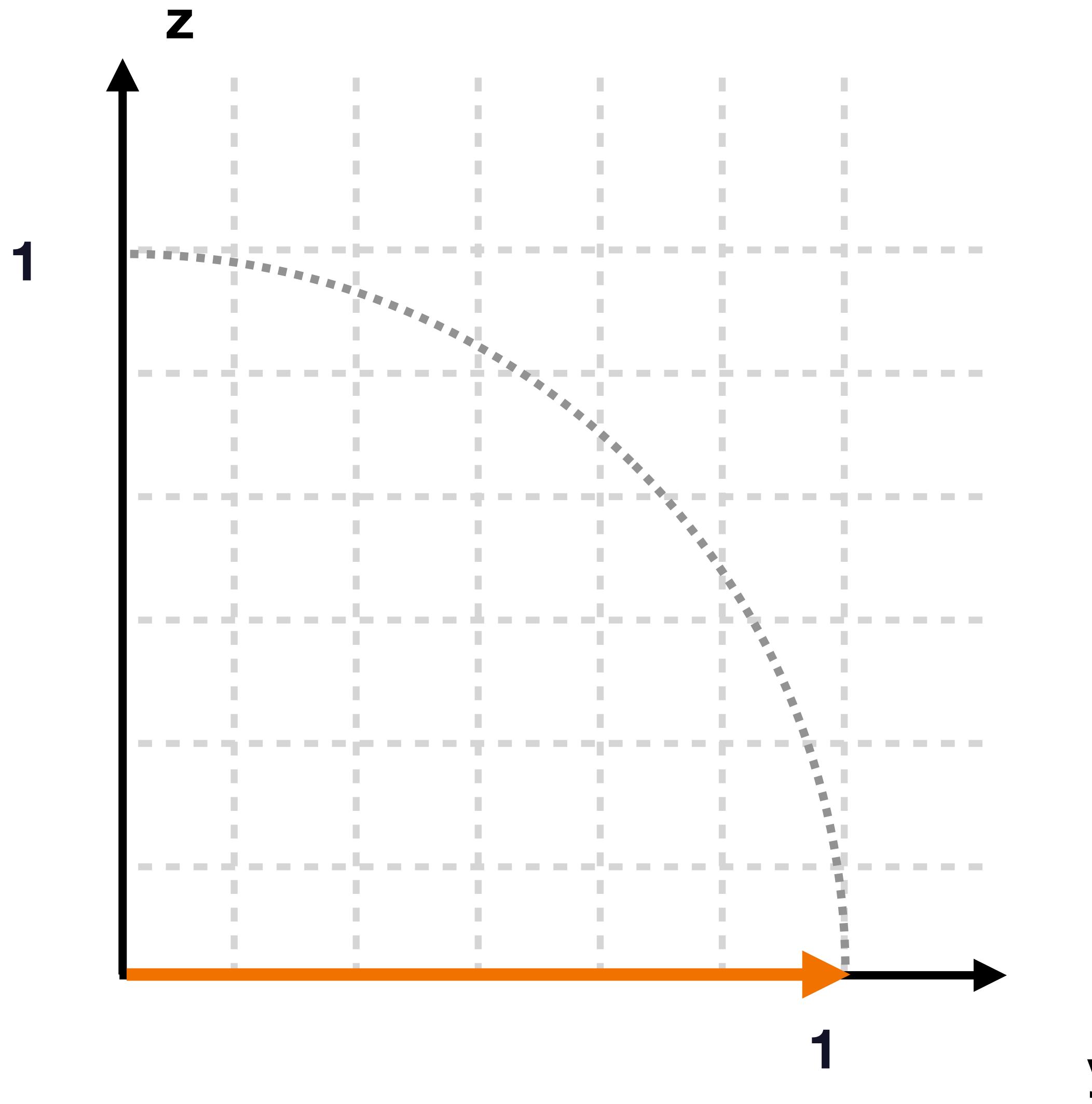
Measure



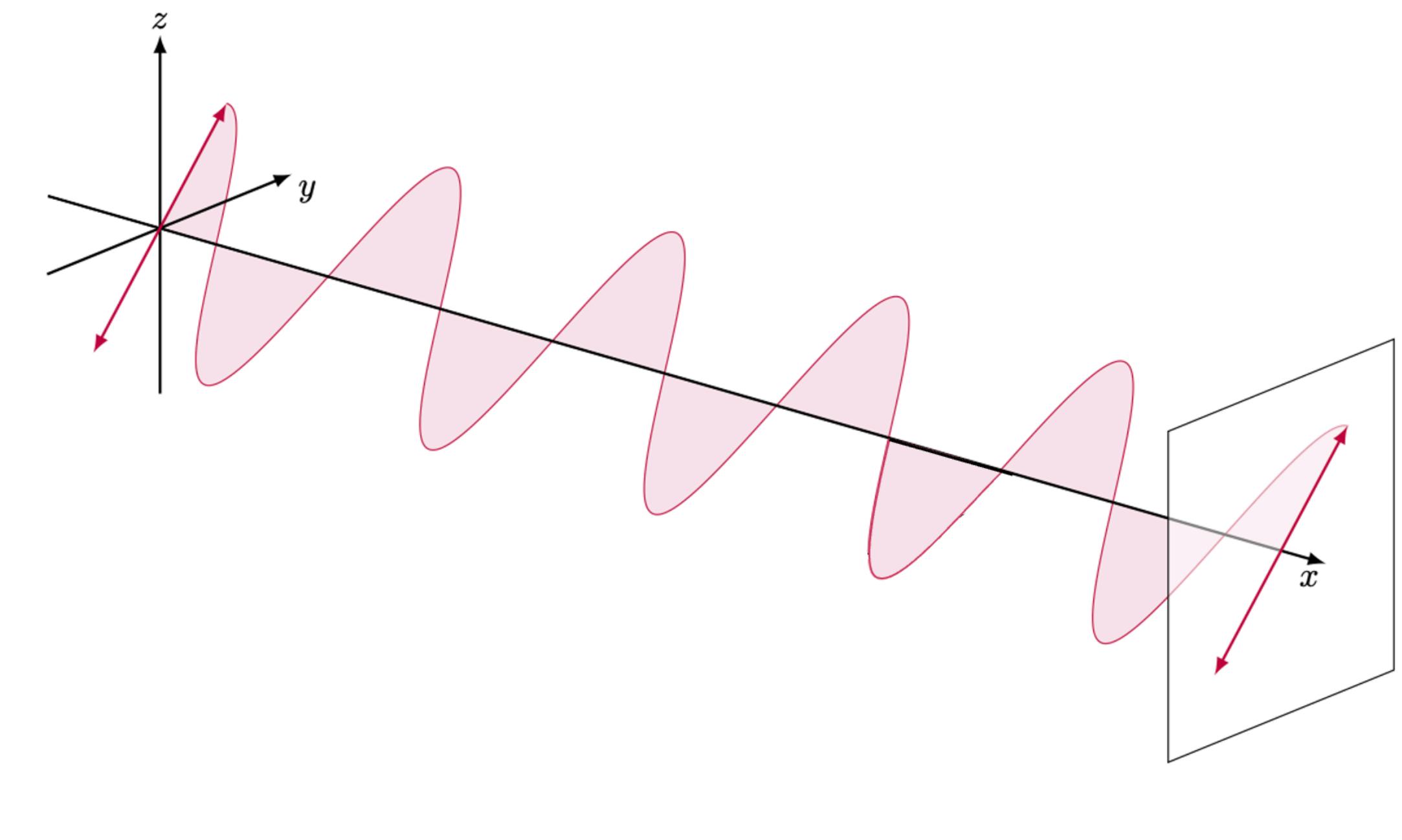
$$|45^\circ\rangle \equiv |\leftrightarrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\rangle$$

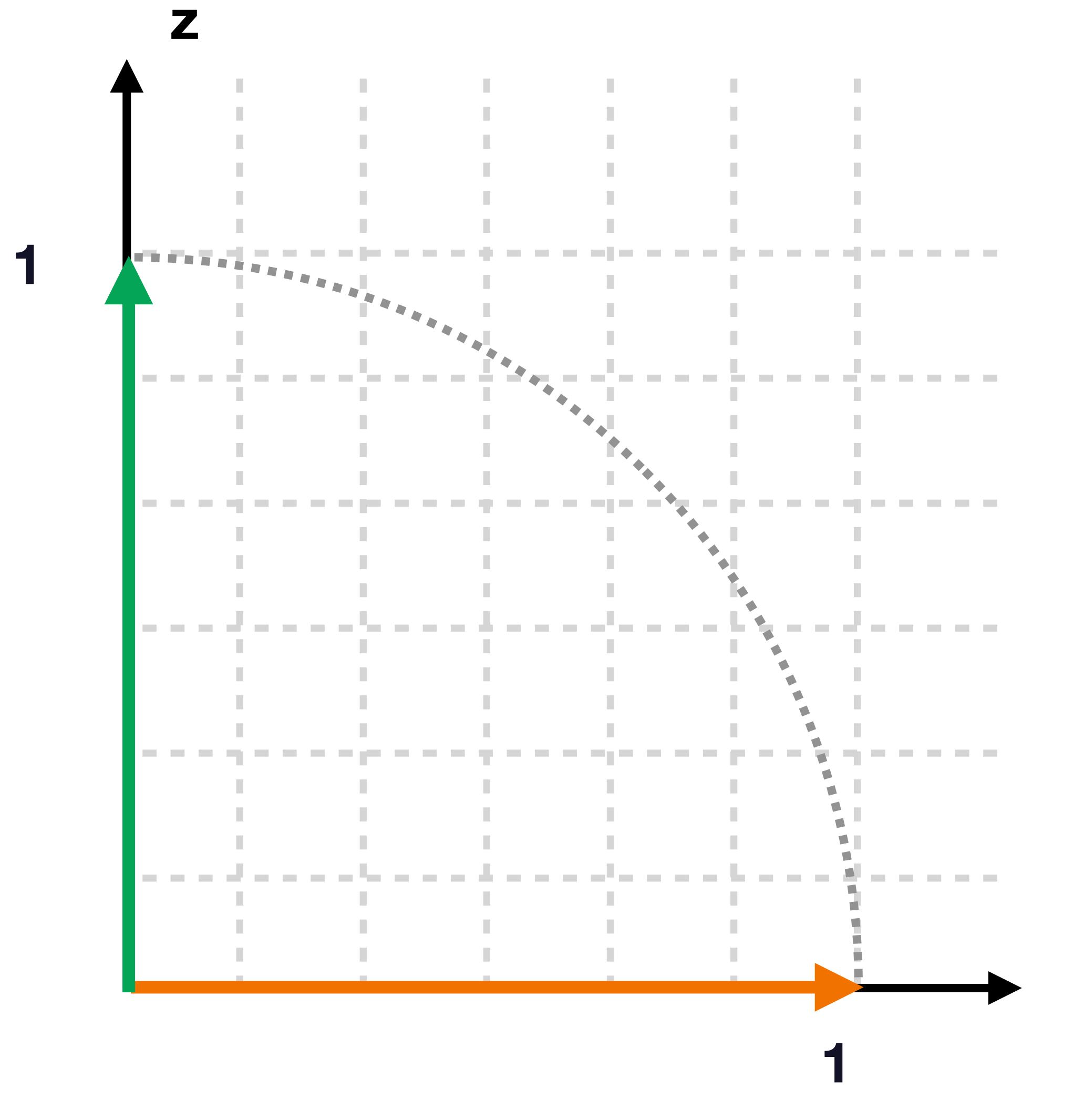
Measure



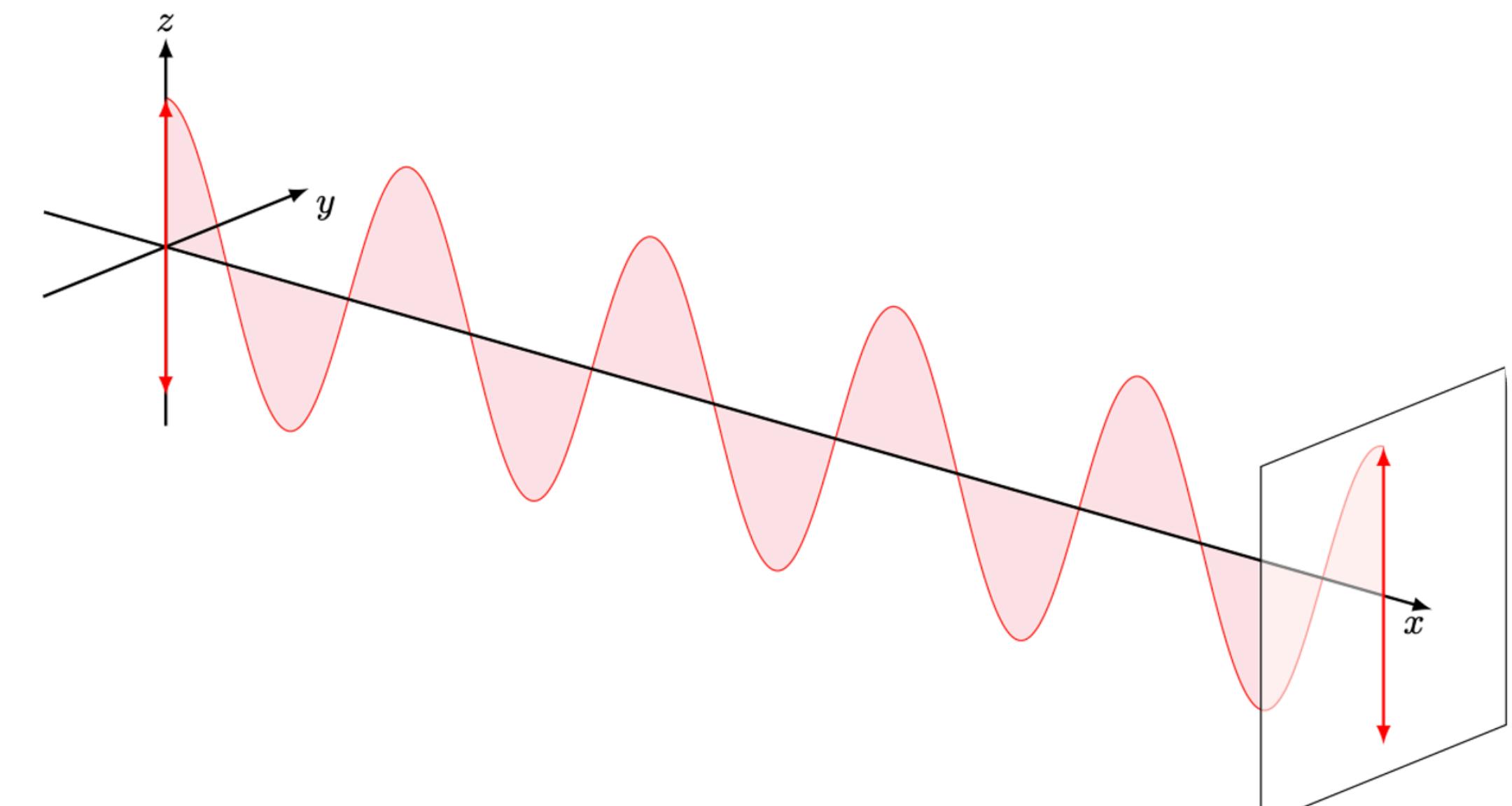
| \leftrightarrow



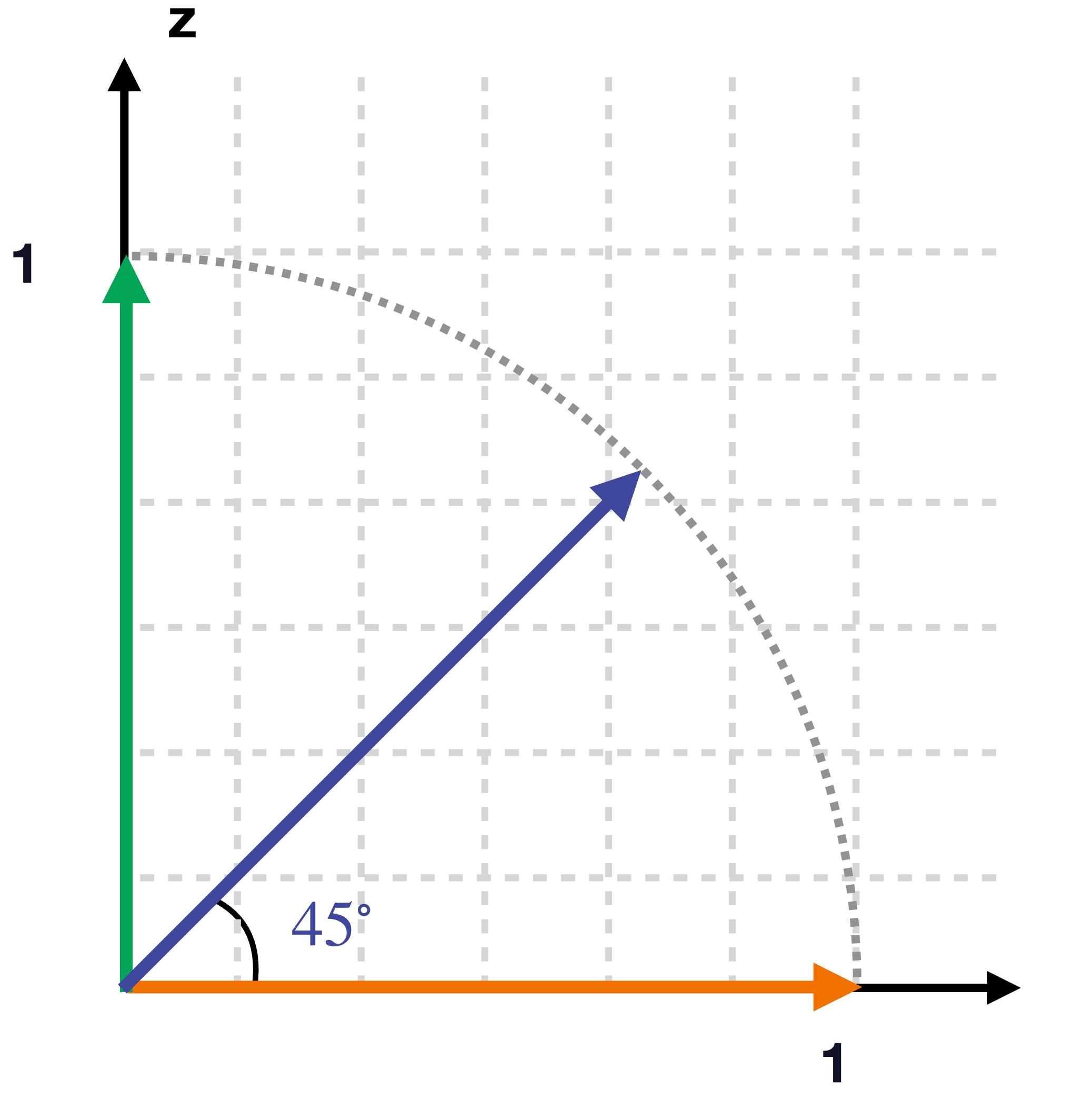
Measure



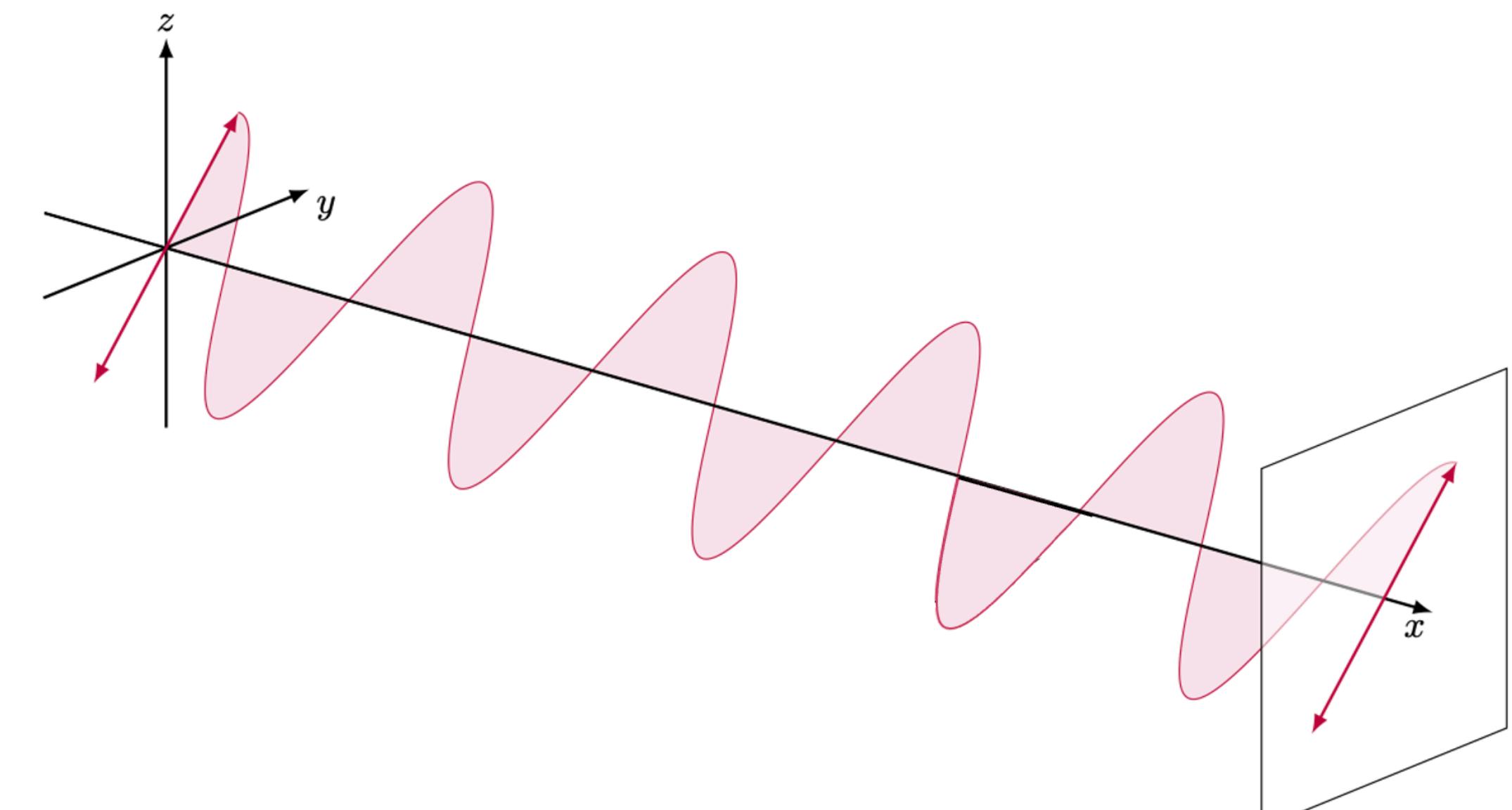
$| \leftrightarrow \rangle$ $| \updownarrow \rangle$



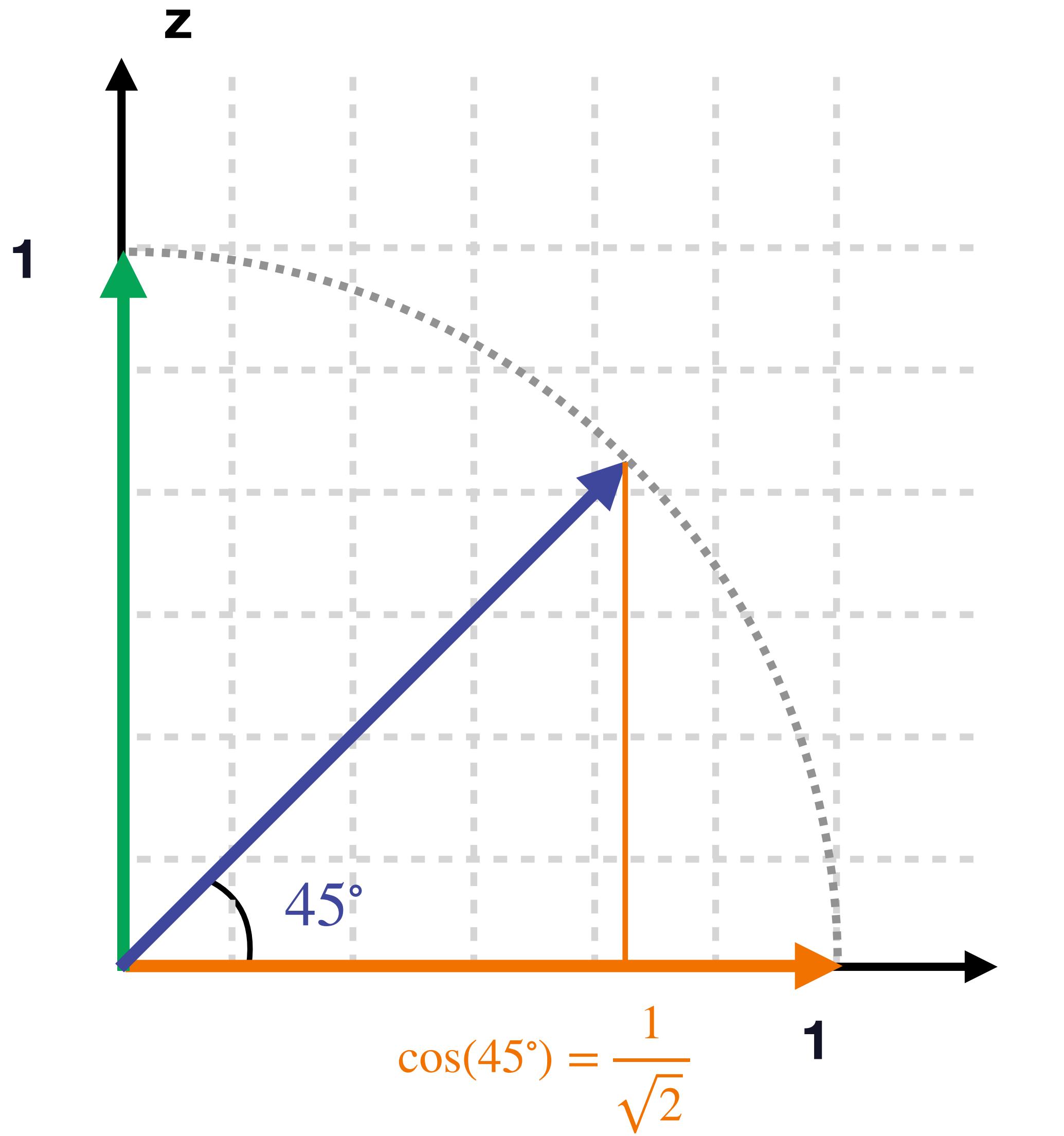
Measure



$| \leftrightarrow \rangle$ $| \updownarrow \rangle$ $| \swarrow \rangle$



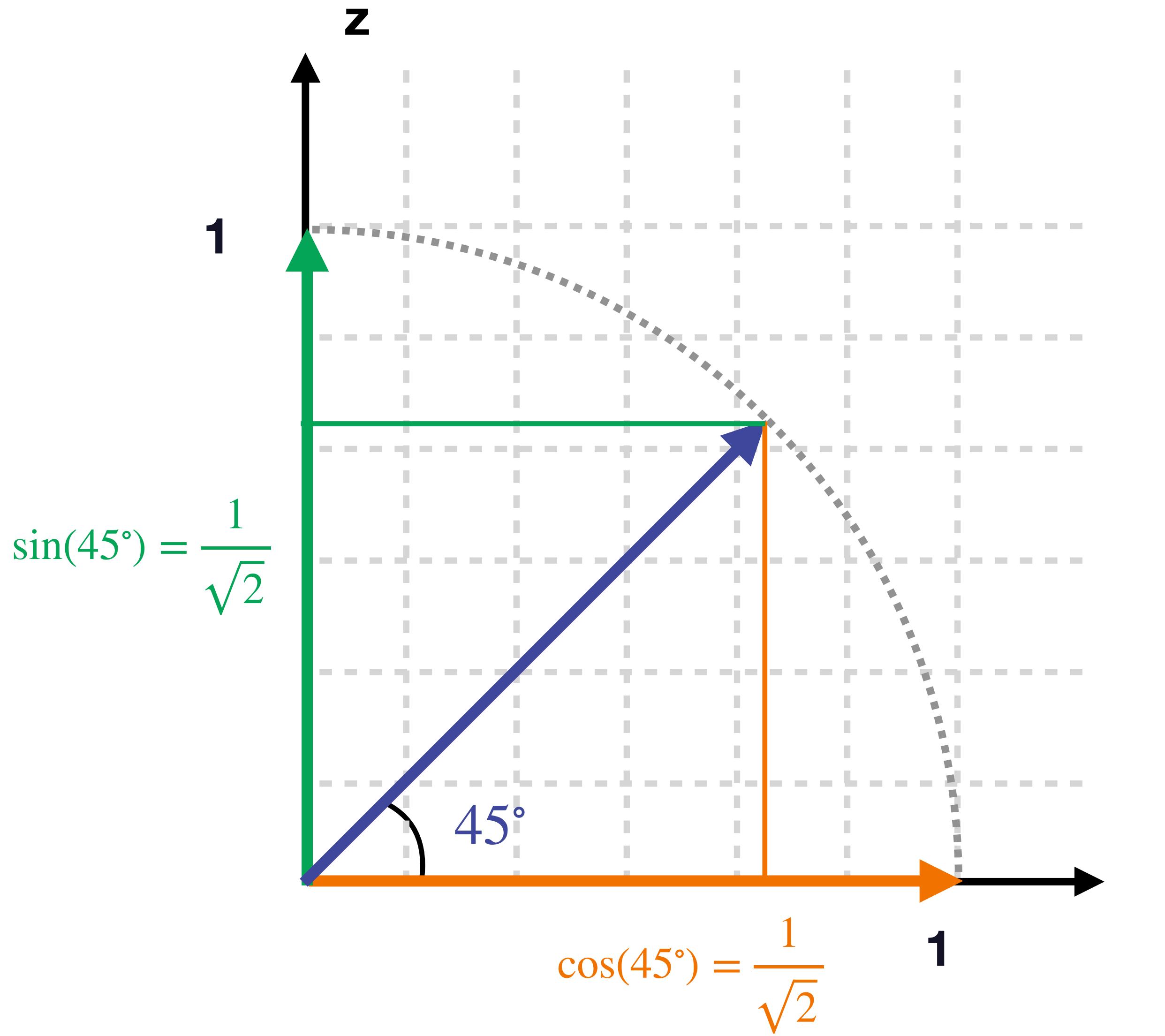
Measure



$| \leftrightarrow \rangle$ $| \updownarrow \rangle$ $| \swarrow \rangle$

$$| \swarrow \rangle = \frac{1}{\sqrt{2}} | \leftrightarrow \rangle +$$

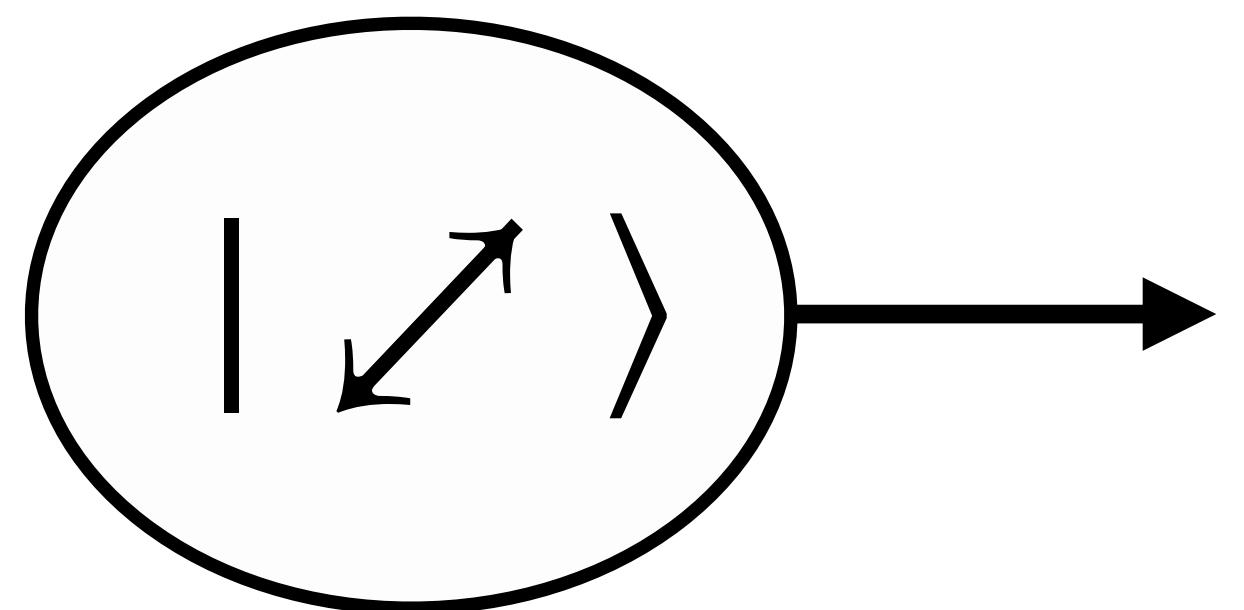
Measure



$| \leftrightarrow \rangle$ $| \uparrow \downarrow \rangle$ $| \downarrow \uparrow \rangle$

$$| \downarrow \uparrow \rangle = \frac{1}{\sqrt{2}} | \leftrightarrow \rangle + \frac{1}{\sqrt{2}} | \uparrow \downarrow \rangle$$

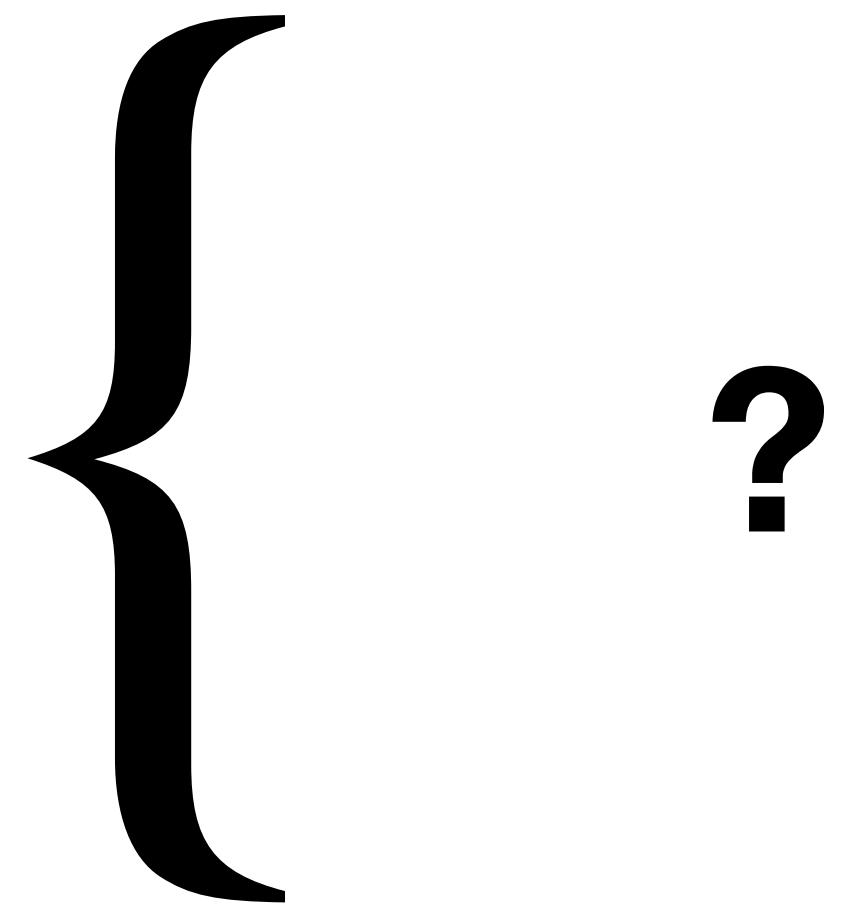
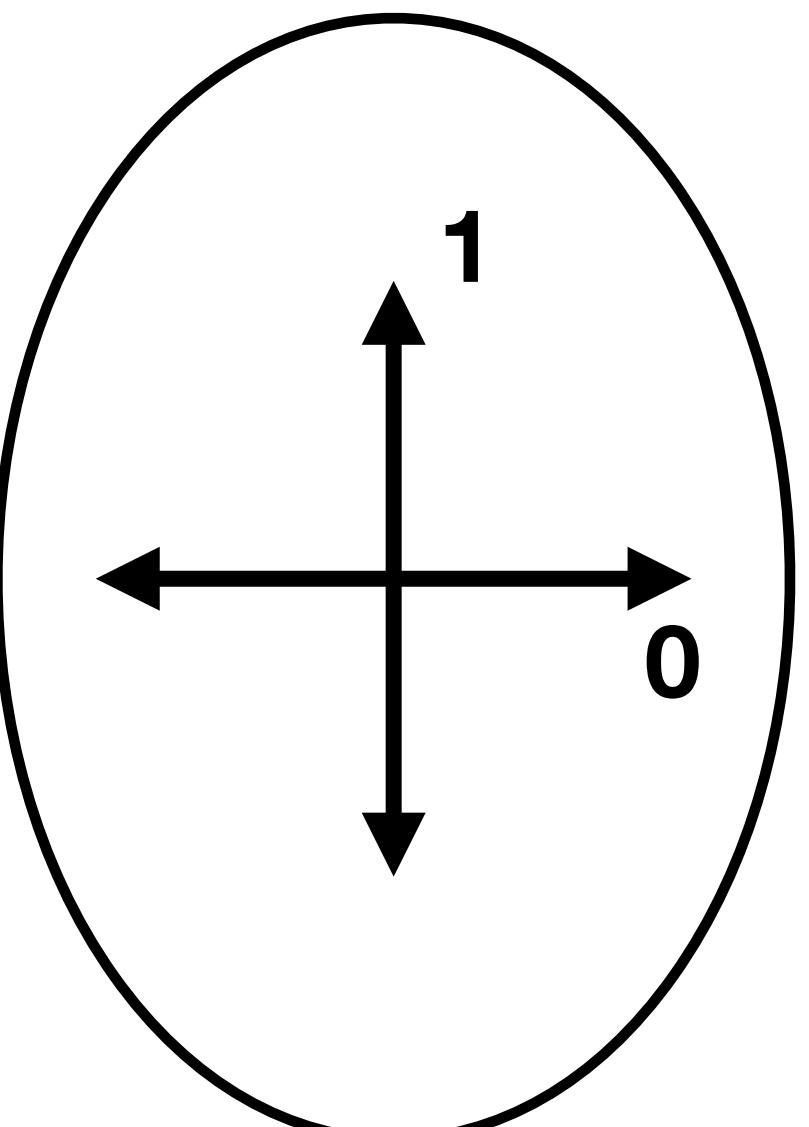
Measure



$$\frac{1}{\sqrt{2}} |\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\rangle$$

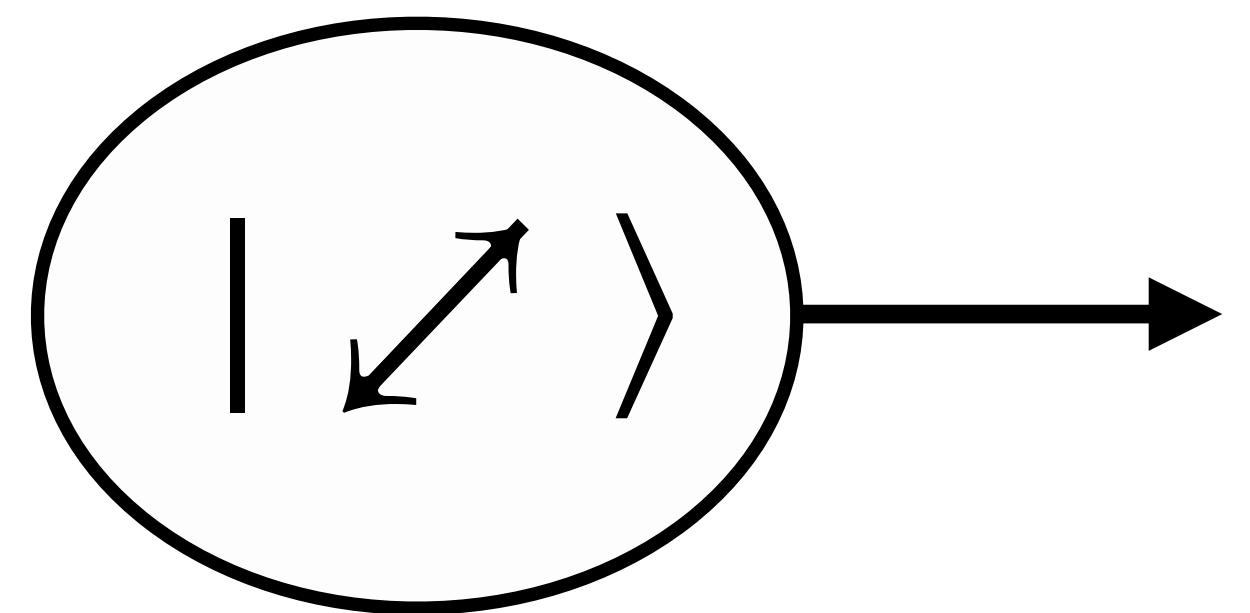
$$|45^\circ\rangle \equiv |\leftrightarrow\rangle$$

$$|135^\circ\rangle \equiv |\uparrow\downarrow\rangle$$



$$|\alpha|^2 + |\beta|^2 = 1$$

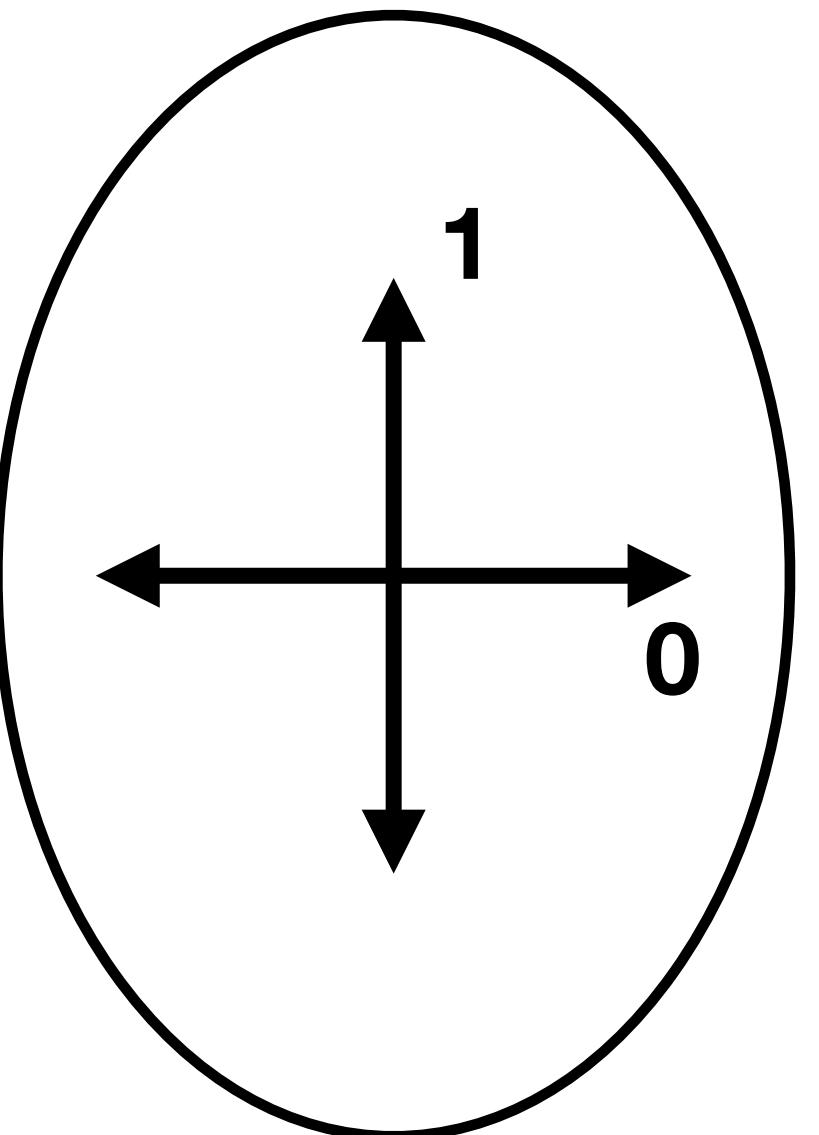
Measure



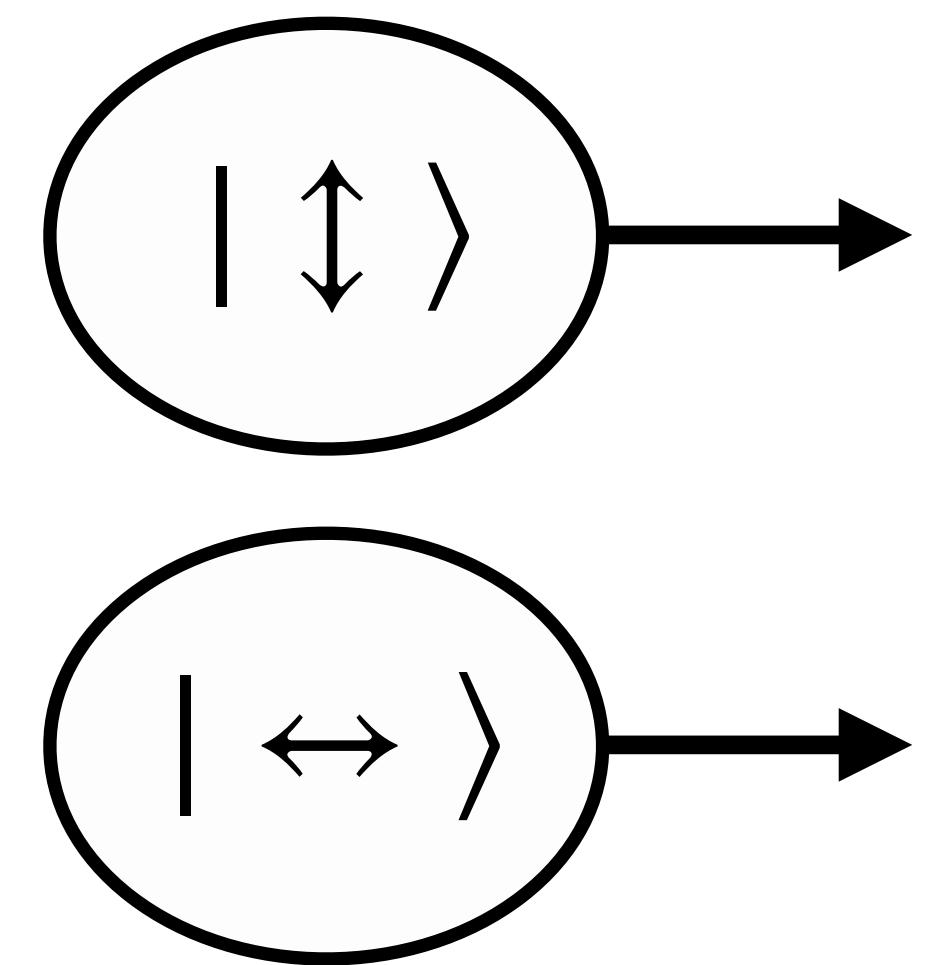
$$\frac{1}{\sqrt{2}} |\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\rangle$$

$$|45^\circ\rangle \equiv |\leftrightarrow\rangle$$

$$|135^\circ\rangle \equiv |\uparrow\downarrow\rangle$$



{

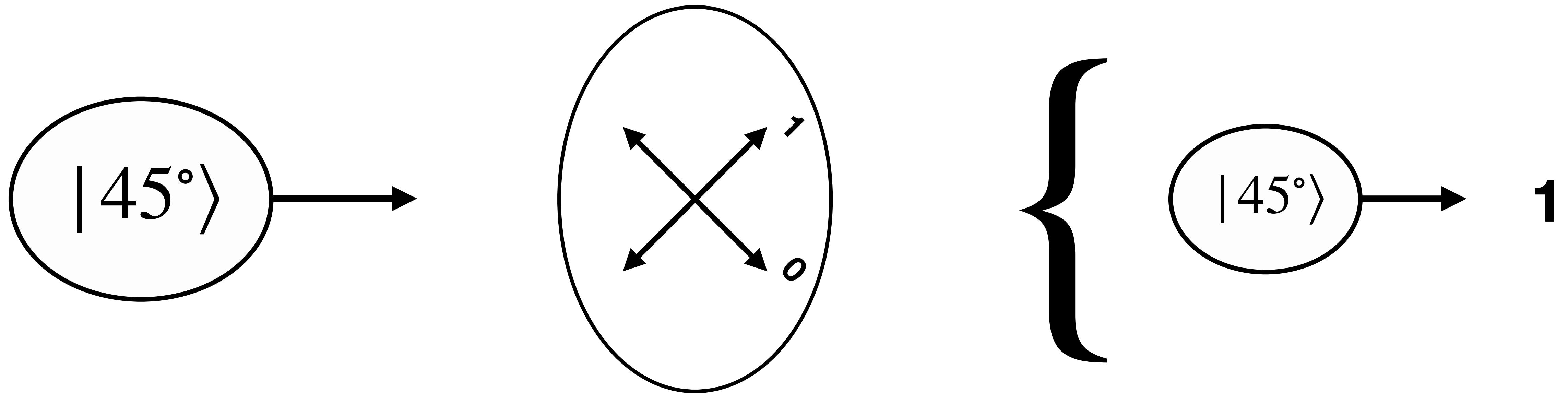


$$P_{|\uparrow\downarrow\rangle} = \frac{1}{2}$$

$$P_{|\leftrightarrow\rangle} = \frac{1}{2}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Measure

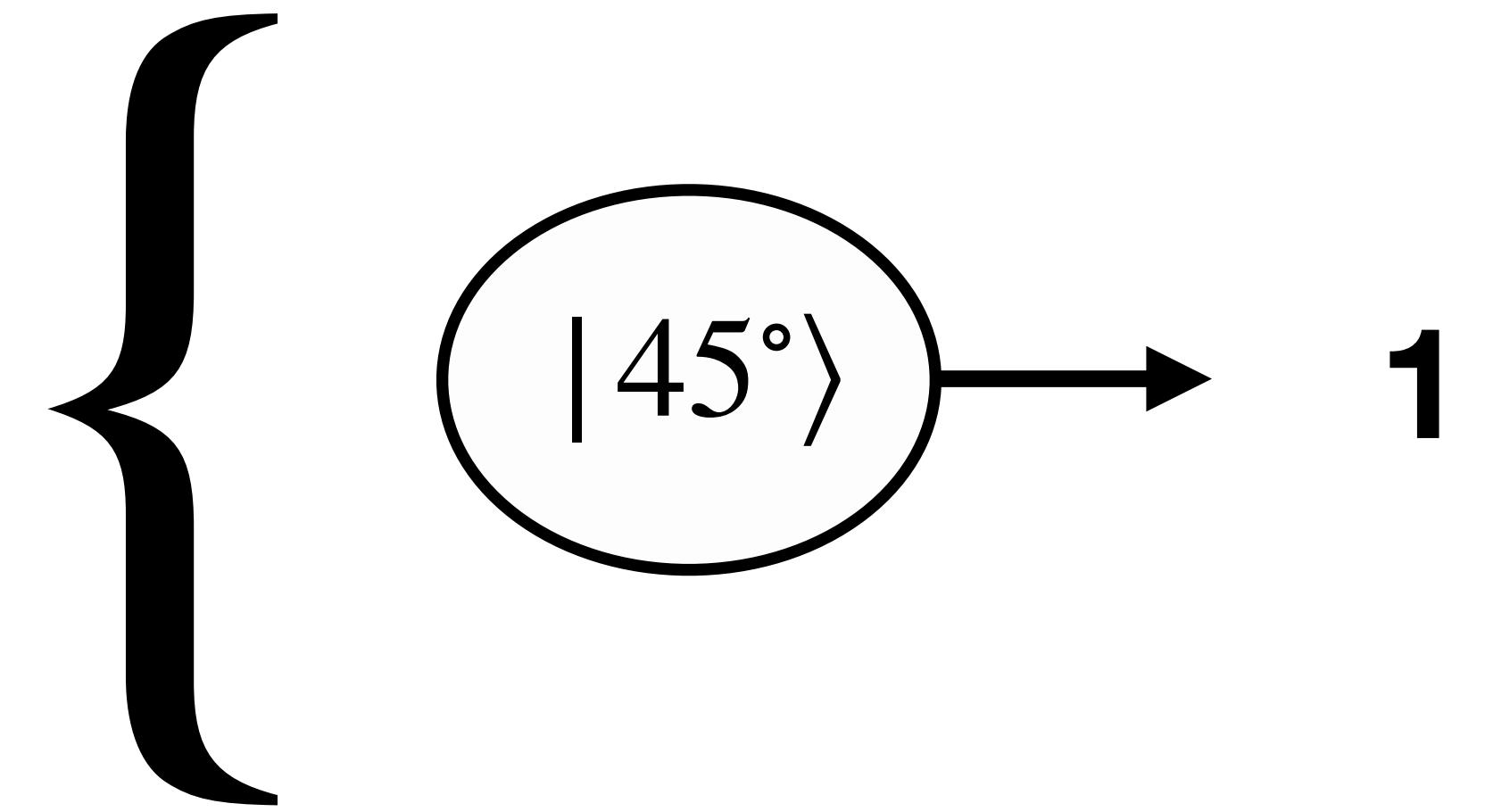
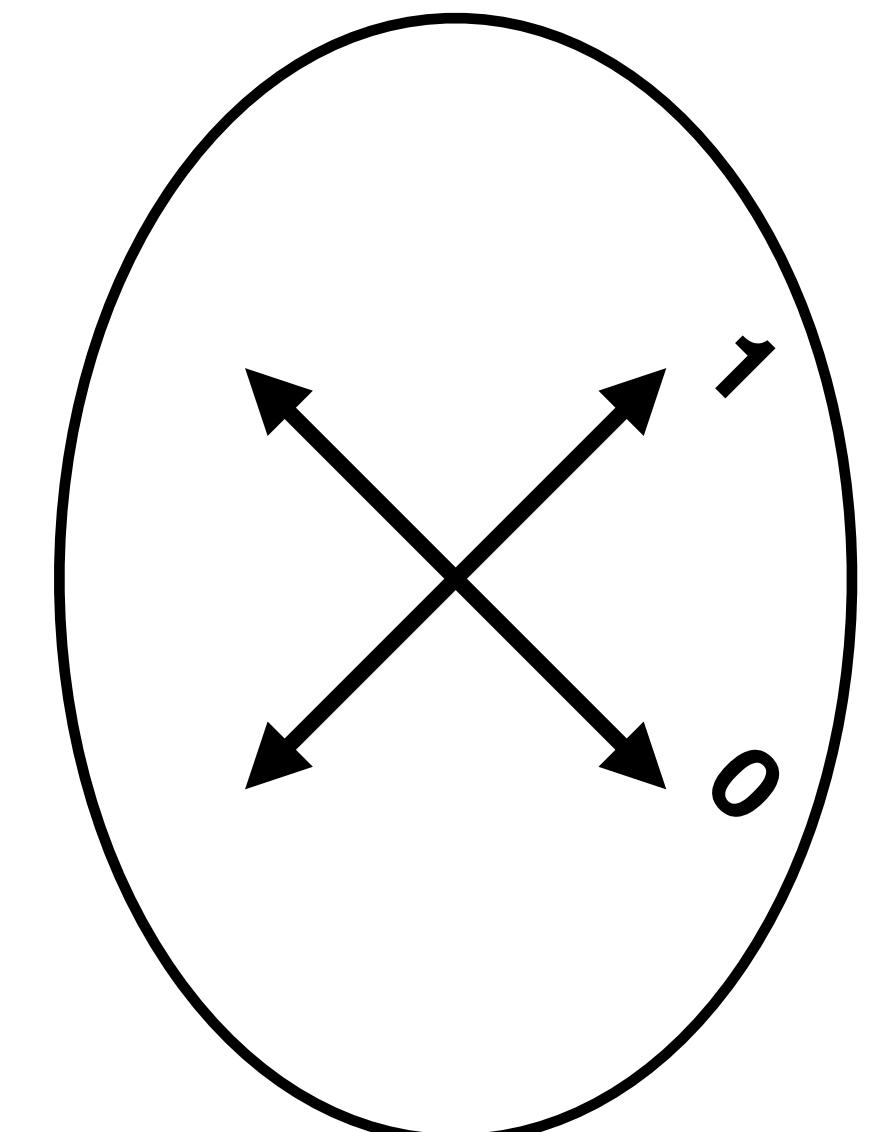


$$|45^\circ\rangle \equiv |\begin{smallmatrix} & + \\ - & \end{smallmatrix}\rangle$$

$$|135^\circ\rangle \equiv |\begin{smallmatrix} + \\ - \end{smallmatrix}\rangle$$

Measure

$$1|45^\circ\rangle + 0|135^\circ\rangle$$

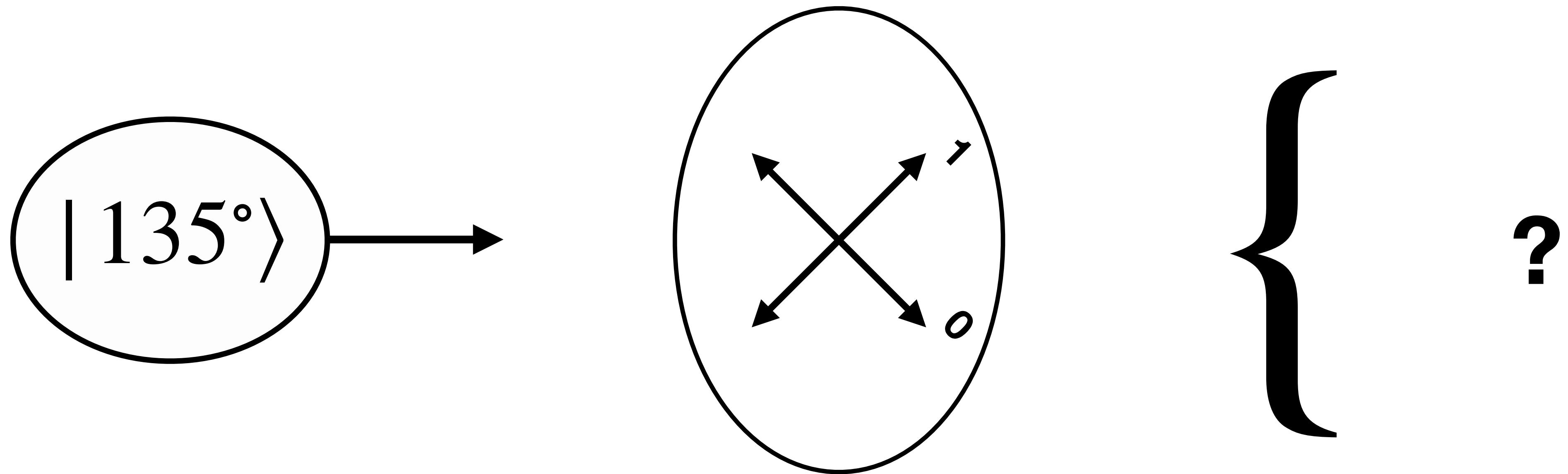


$$|45^\circ\rangle \equiv |\nearrow\rangle$$
$$|135^\circ\rangle \equiv |\nwarrow\rangle$$

$$P_{|45^\circ\rangle} = |1|^2$$

$$P_{|135^\circ\rangle} = |0|^2$$

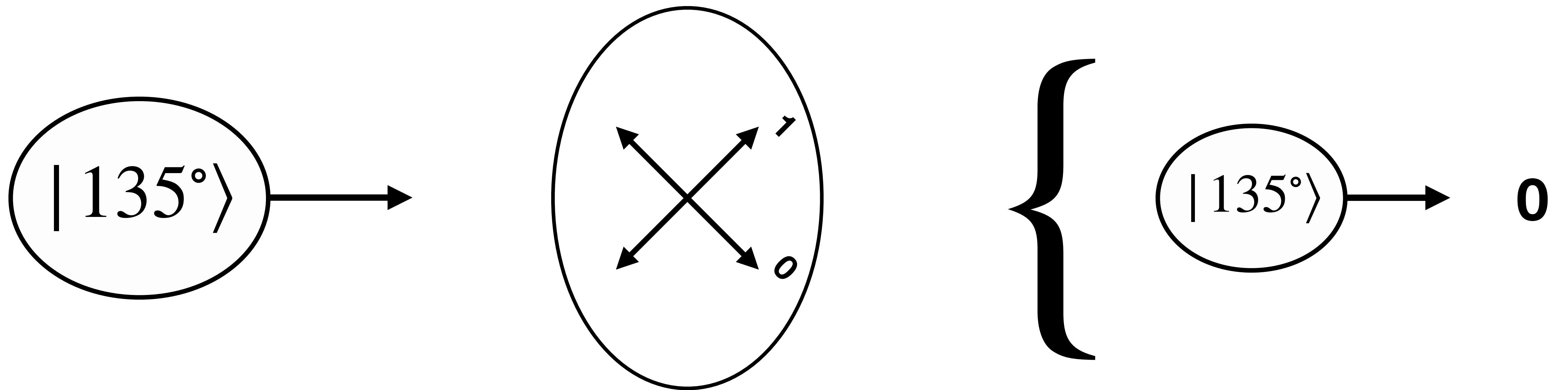
Measure



$$|45^\circ\rangle \equiv |\nearrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\rangle$$

Measure



$$|45^\circ\rangle \equiv |\nearrow\rangle$$

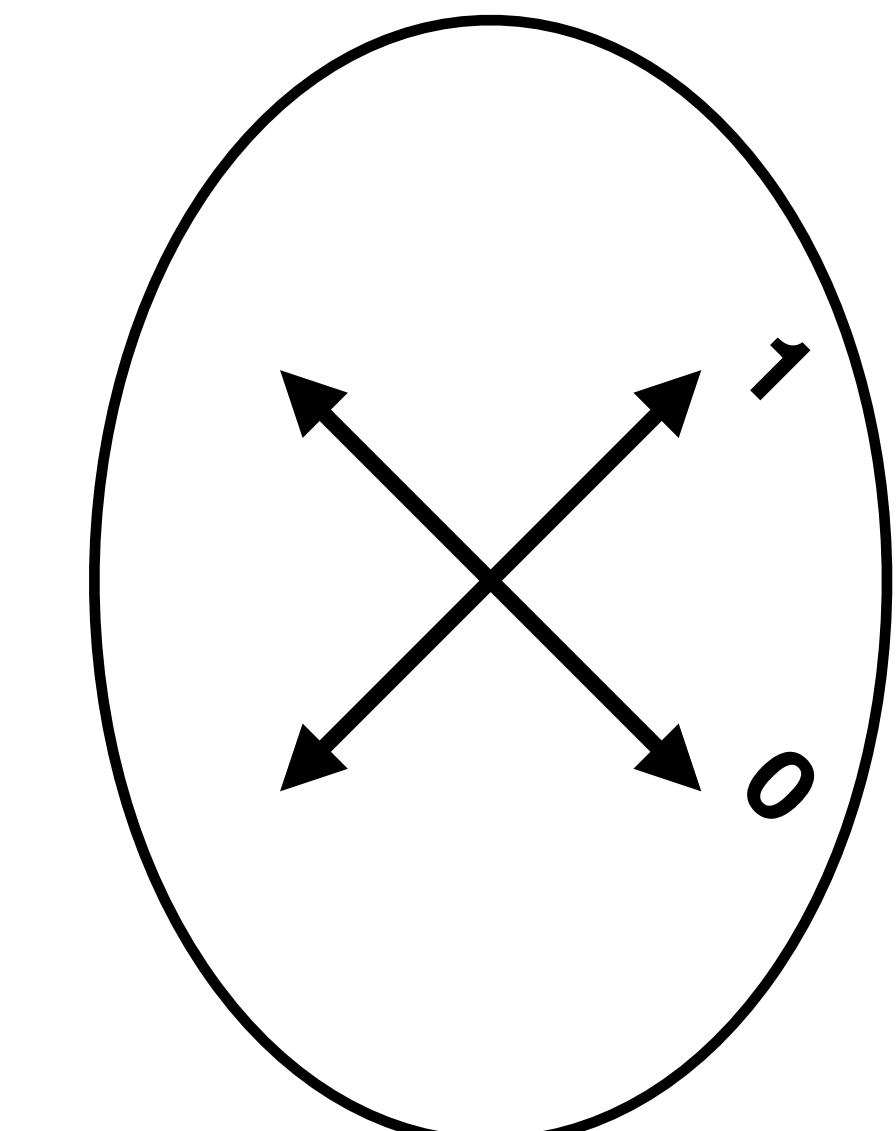
$$|135^\circ\rangle \equiv |\nwarrow\rangle$$

Measure

$|135^\circ\rangle$

$$1|0^\circ\rangle + 0|90^\circ\rangle$$

$$\begin{aligned}|45^\circ\rangle &\equiv |\nearrow\rangle \\ |135^\circ\rangle &\equiv |\nwarrow\rangle\end{aligned}$$

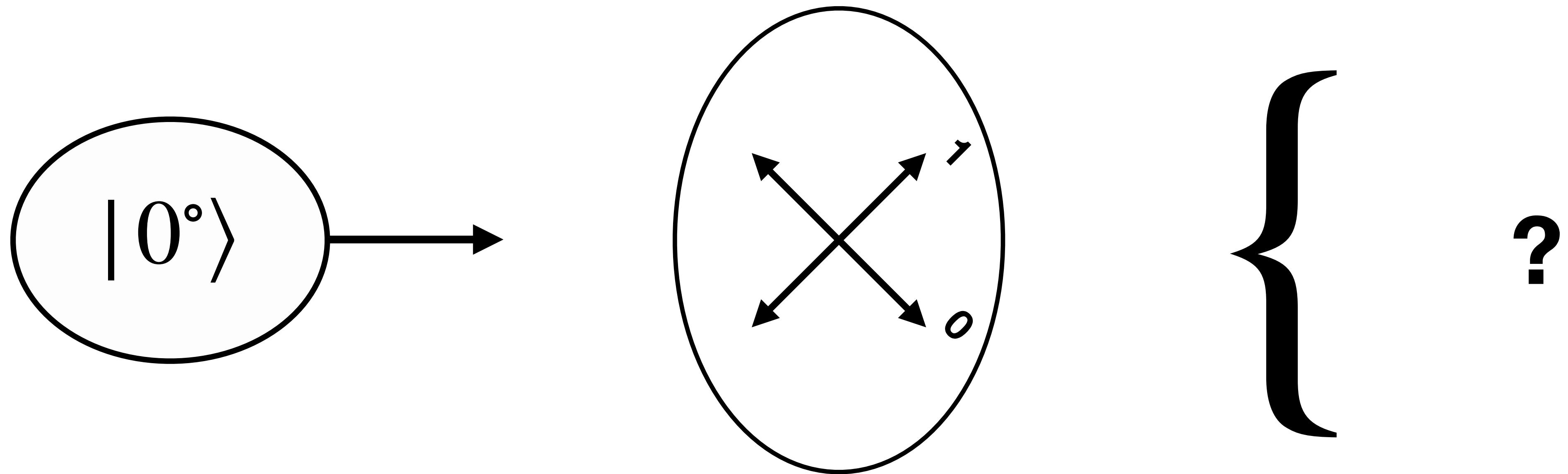


$$P_{|0^\circ\rangle} = |1|^2$$

$\left\{ \begin{array}{l} |135^\circ\rangle \rightarrow 0 \\ \end{array} \right.$

$$P_{|90^\circ\rangle} = |0|^2$$

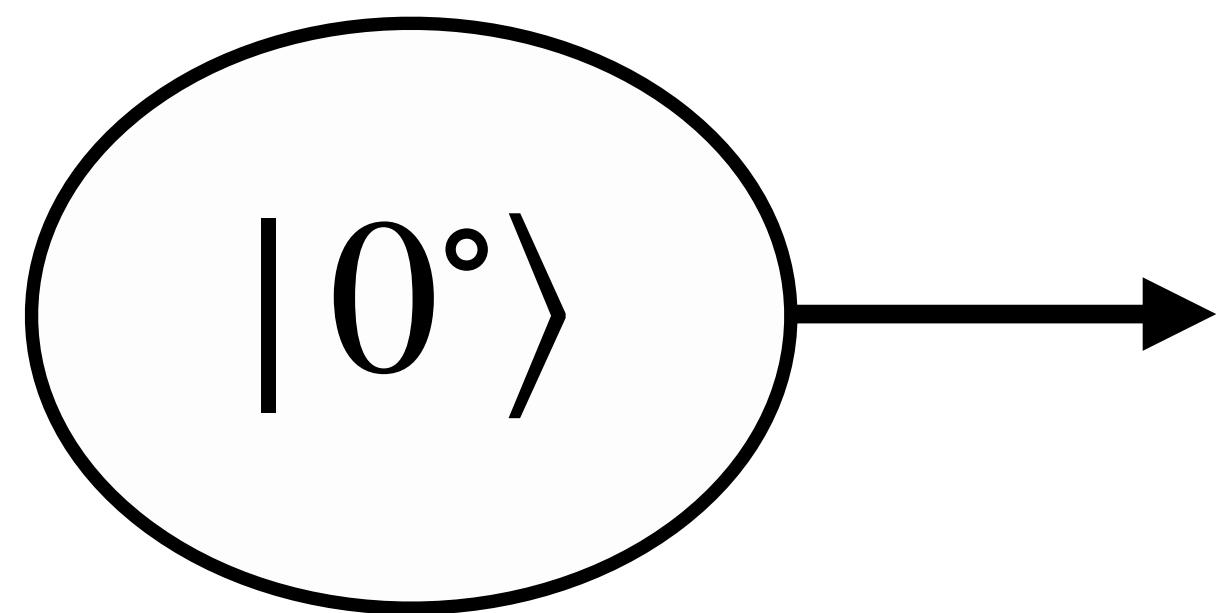
Measure



$$|45^\circ\rangle \equiv | \nearrow \rangle$$

$$|135^\circ\rangle \equiv | \nwarrow \rangle$$

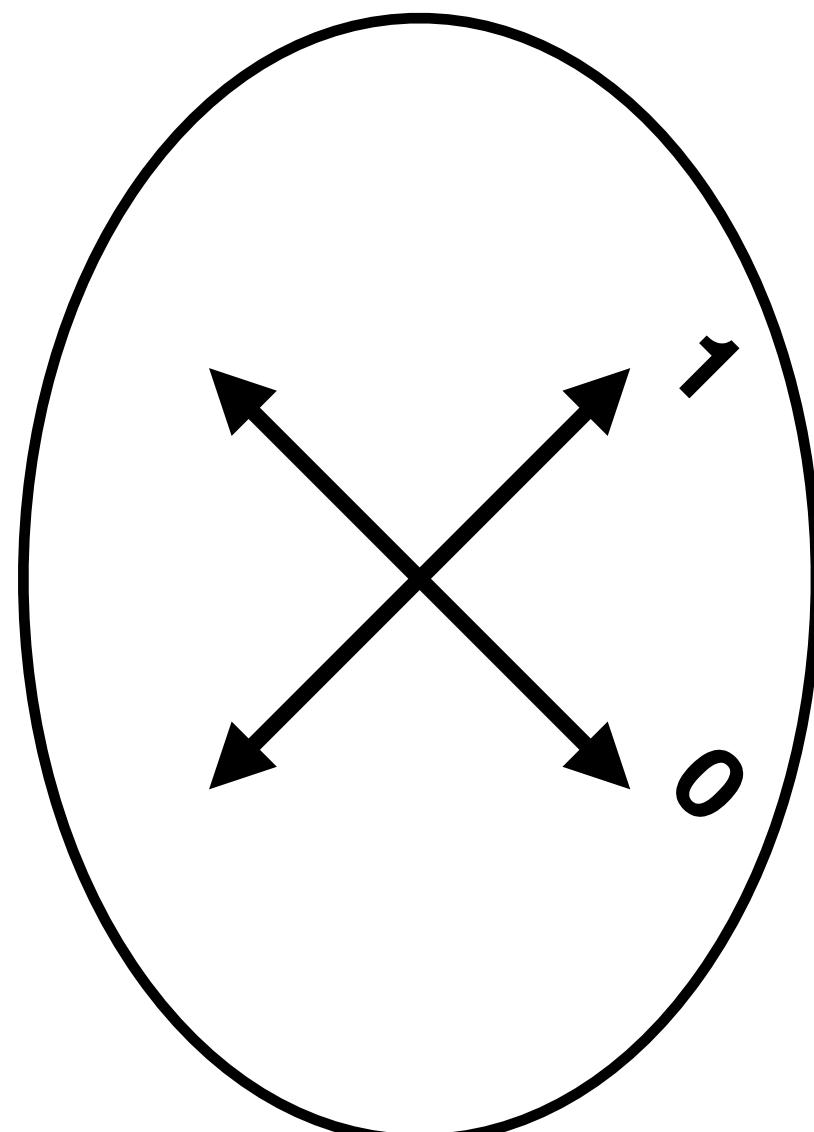
Measure



$$\frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|135^\circ\rangle$$

$$|45^\circ\rangle \equiv |\nearrow\rangle$$

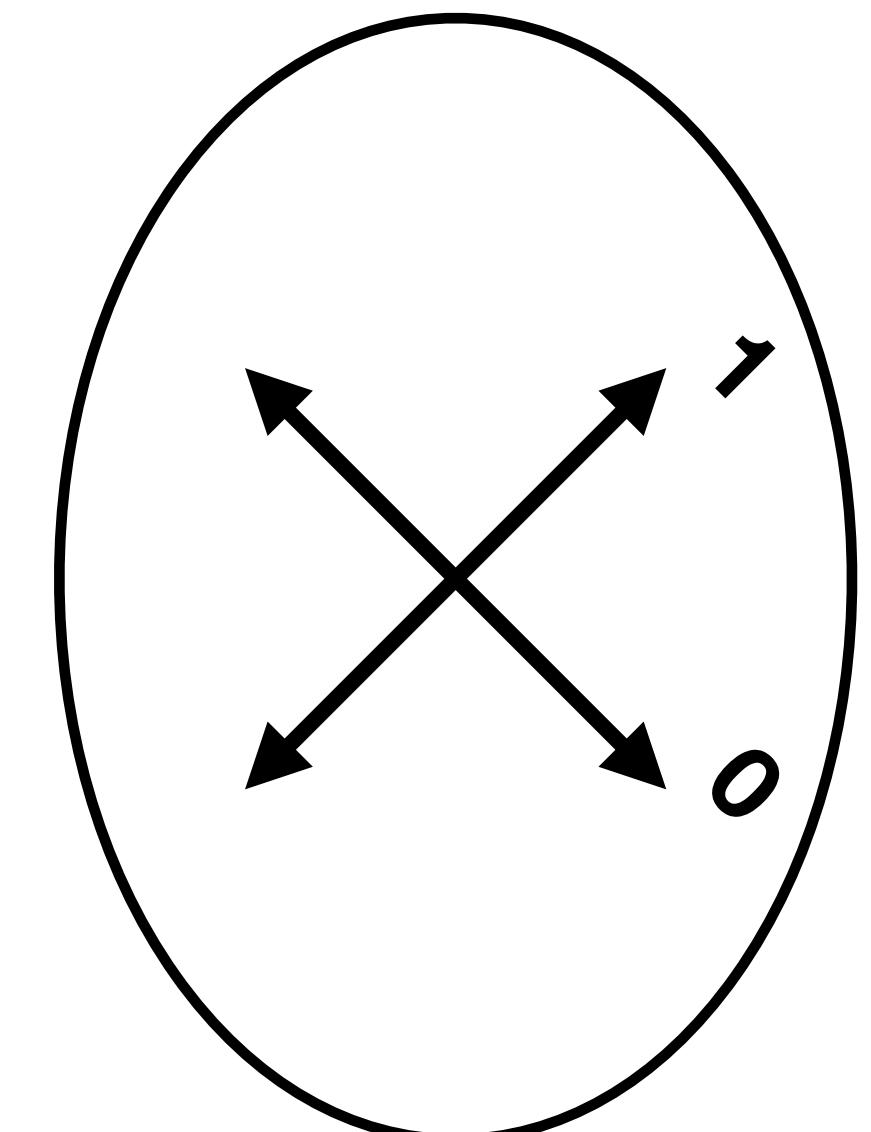
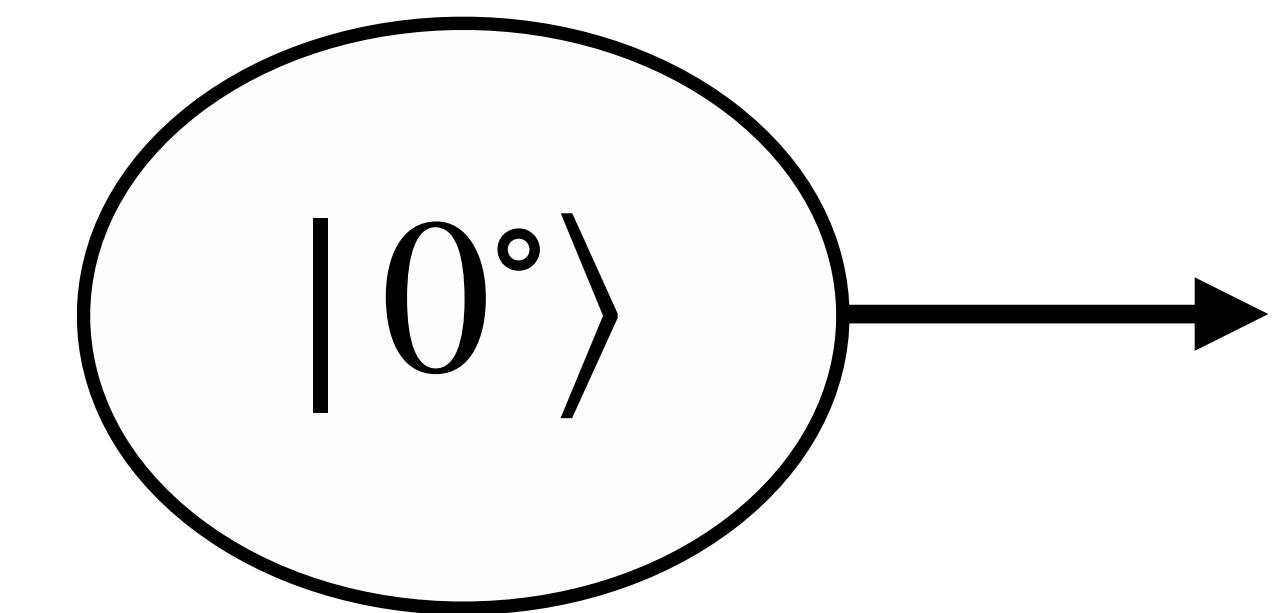
$$|135^\circ\rangle \equiv |\nwarrow\rangle$$



{ ?

Measure

$$\frac{1}{\sqrt{2}} |45^\circ\rangle + \frac{1}{\sqrt{2}} |135^\circ\rangle$$



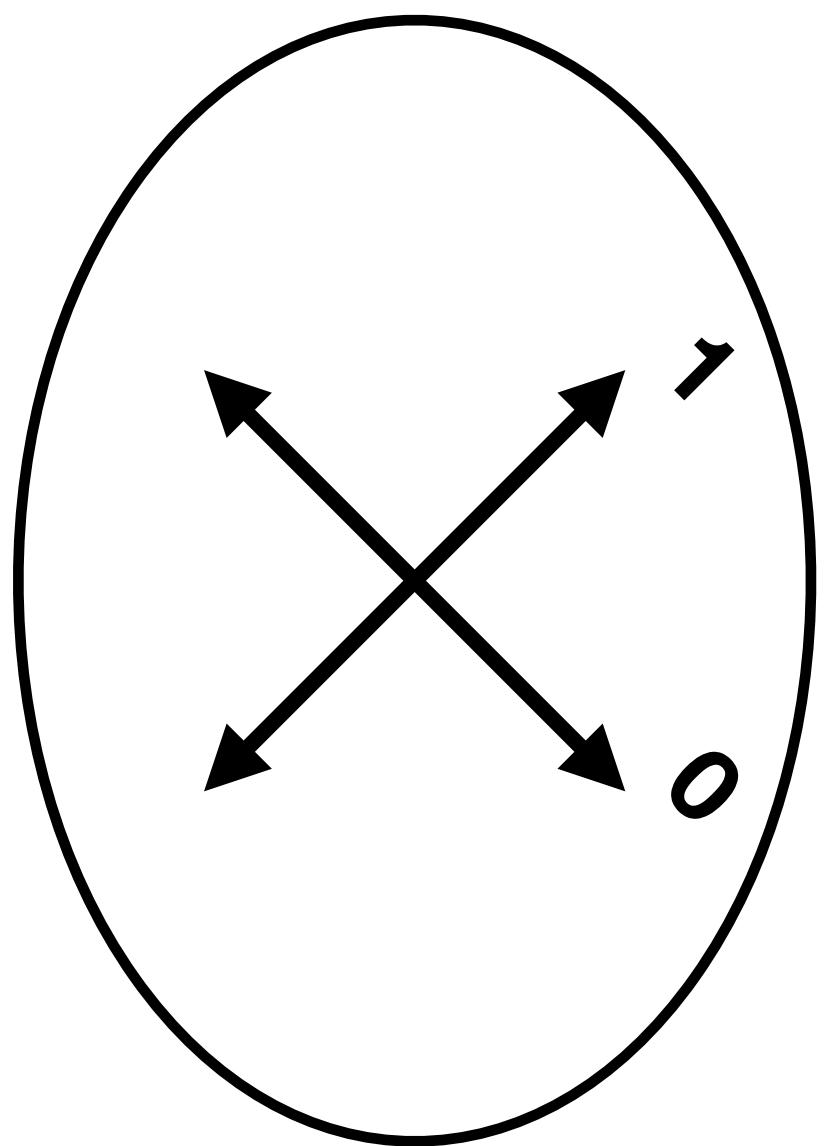
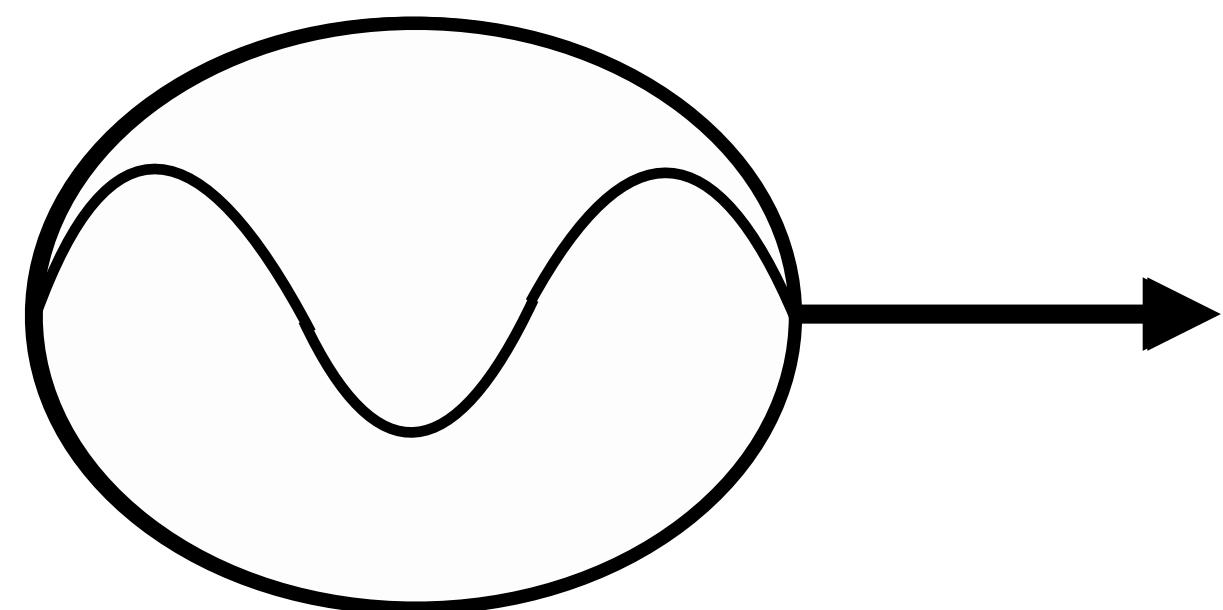
$$|45^\circ\rangle \equiv |\nearrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\rangle$$

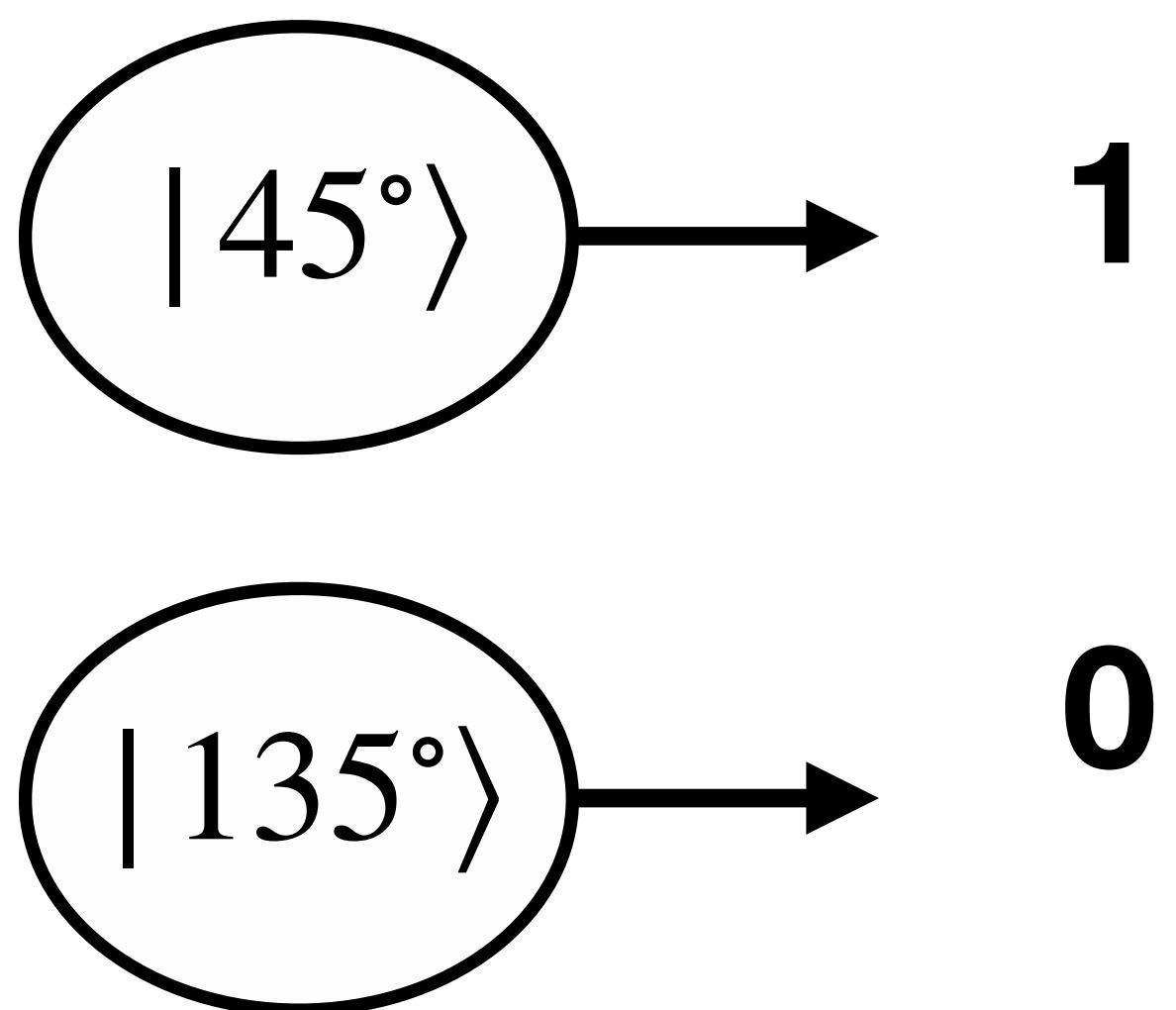
$$P_{|45^\circ\rangle} = \frac{1}{2}$$

$$P_{|135^\circ\rangle} = \frac{1}{2}$$

Measure



$$P_{|45^\circ\rangle} = |\alpha|^2$$



$$|45^\circ\rangle \equiv |\nearrow\rangle$$

$$|135^\circ\rangle \equiv |\nwarrow\rangle$$

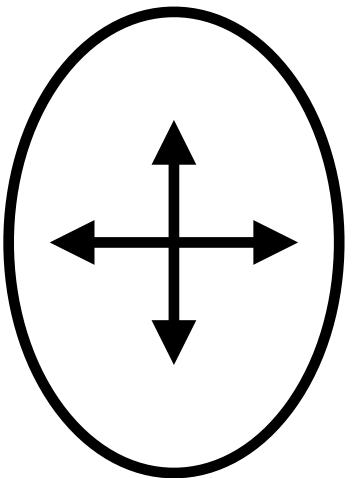
$$P_{|135^\circ\rangle} = |\beta|^2$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Superposition & Mesure quantique

Points clés

- La mesure quantique fait s'effondrer la polarisation dans un des états de base de la base de mesure

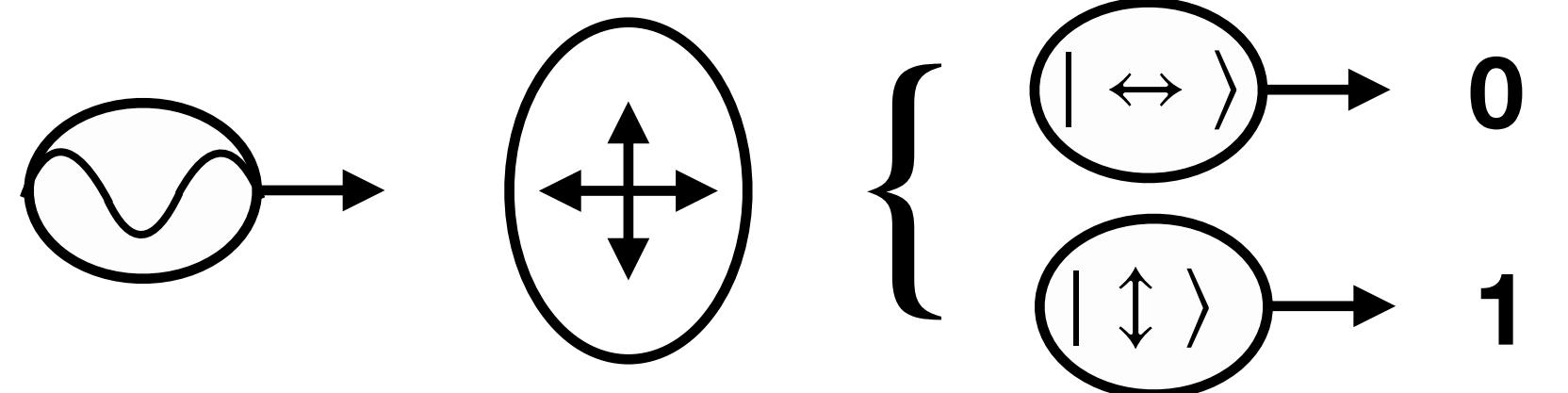


$| \uparrow \downarrow \rangle$ ou $| \leftrightarrow \rangle$

Superposition & Mesure quantique

Points clés

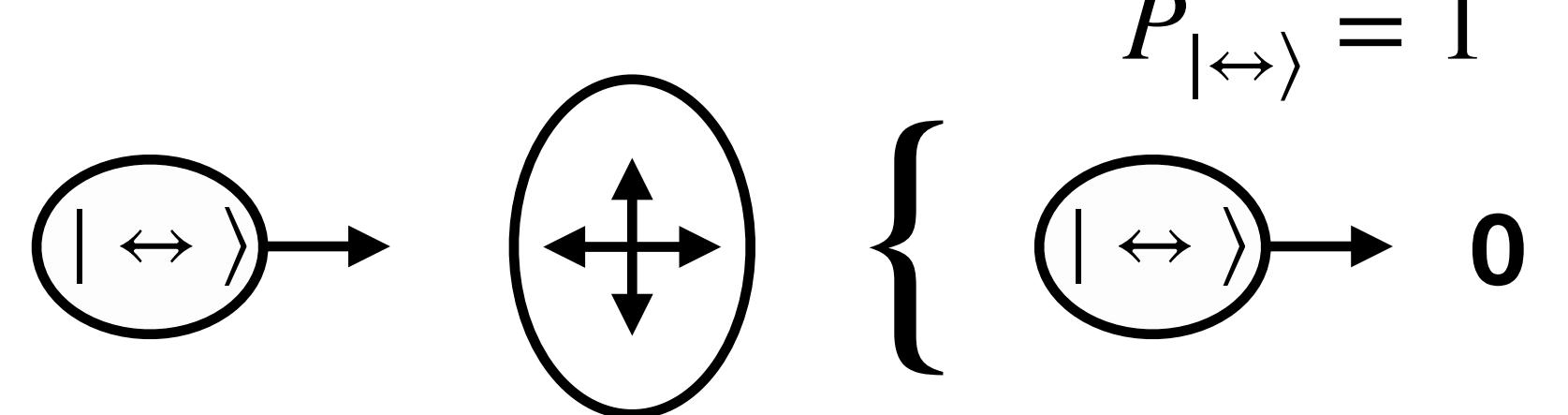
- La mesure quantique fait s'effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire



Superposition & Mesure quantique

Points clés

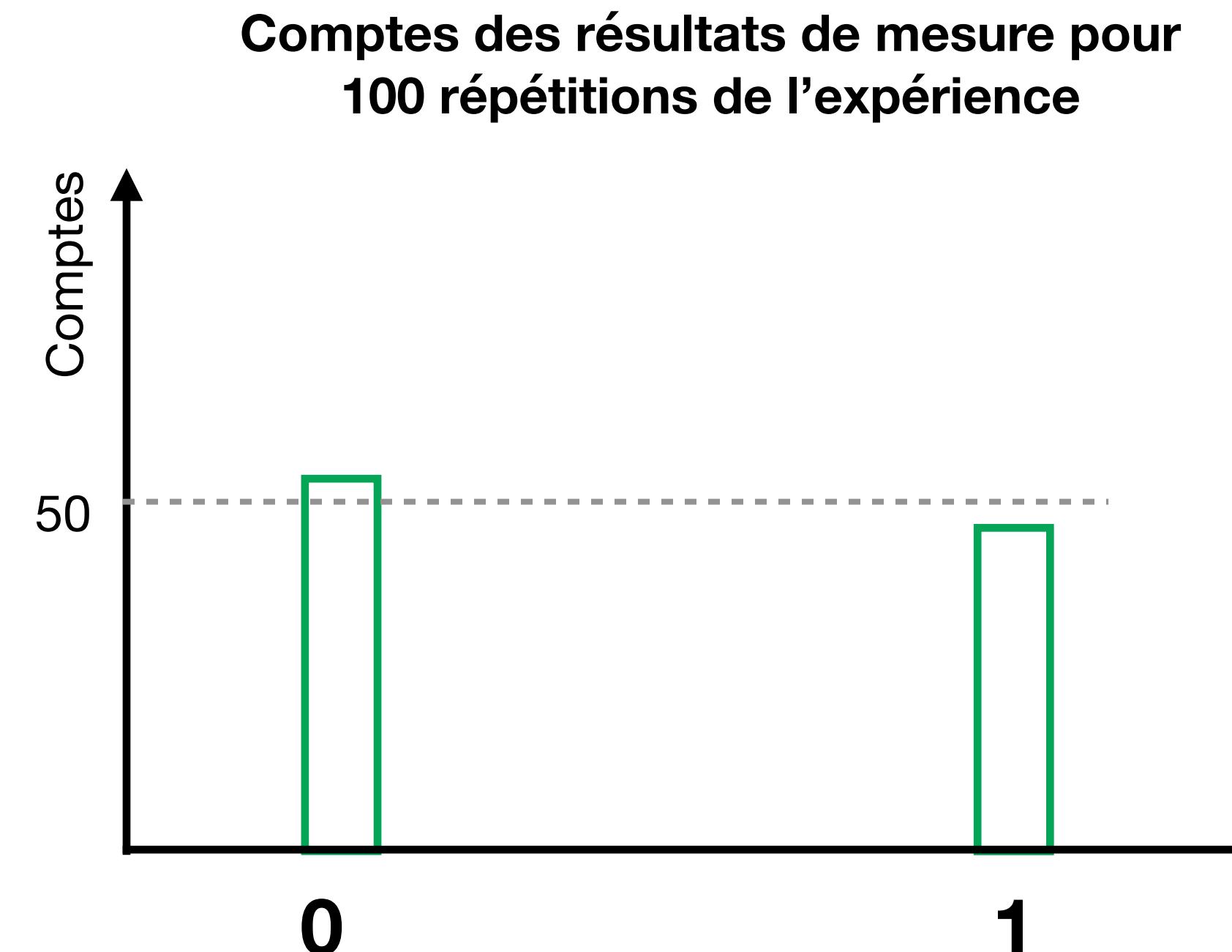
- La mesure quantique fait s'effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire
- Si le photon incident est dans un état de base de la base de mesure, le résultat sera toujours le même



Superposition & Mesure quantique

Points clés

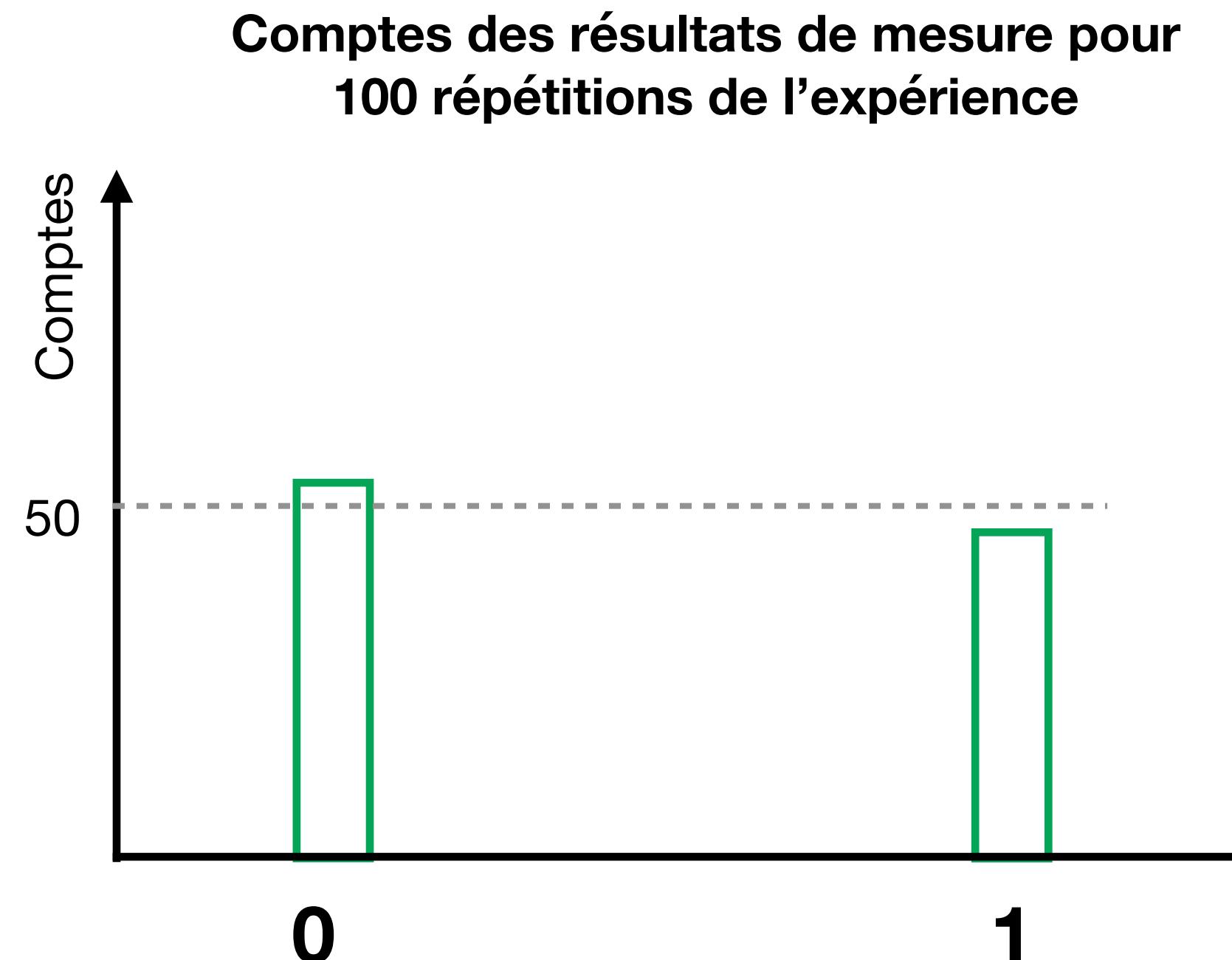
- La mesure quantique fait s'effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire
- Si le photon incident est dans un état de base de la base de mesure, le résultat sera toujours le même
- Pour pouvoir décrire l'état quantique d'un photon incident, il faut répéter plusieurs fois l'expérience de la mesure et compiler des statistiques



Superposition & Mesure quantique

Points clés

- La mesure quantique fait s'effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire
- Si le photon incident est dans un état de base de la base de mesure, le résultat sera toujours le même
- Pour pouvoir décrire l'état quantique d'un photon incident, il faut répéter plusieurs fois l'expérience de la mesure et compiler des statistiques
- Autrement, on ne peut rien dire





Encodage de l'information

Bit à
transmettre

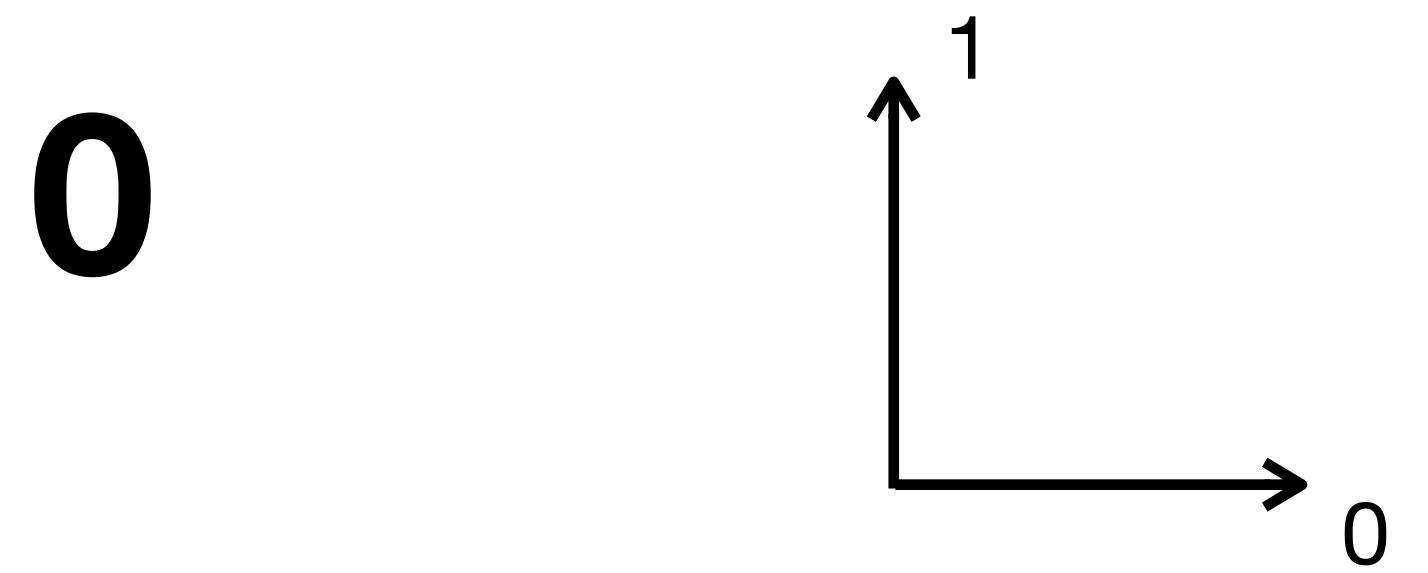
0

1

Encodage de l'information

Bit à
transmettre

Base de
mesure



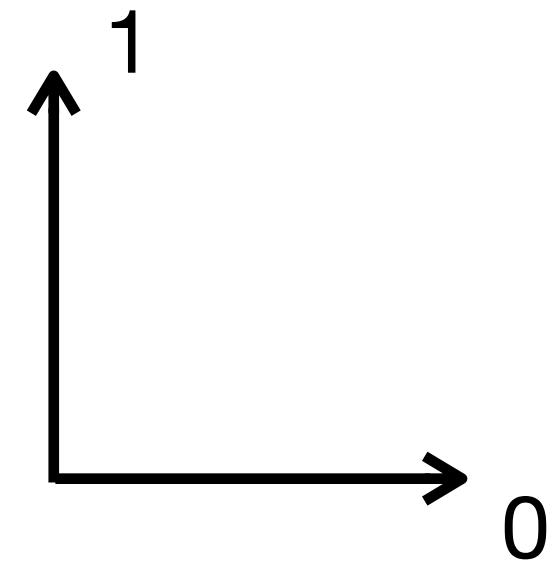
1

Encodage de l'information

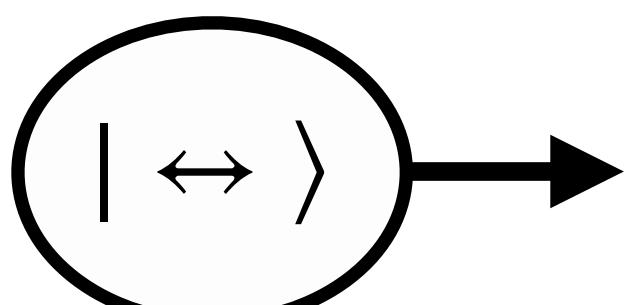
Bit à transmettre

0

Base de mesure



Photon encodé



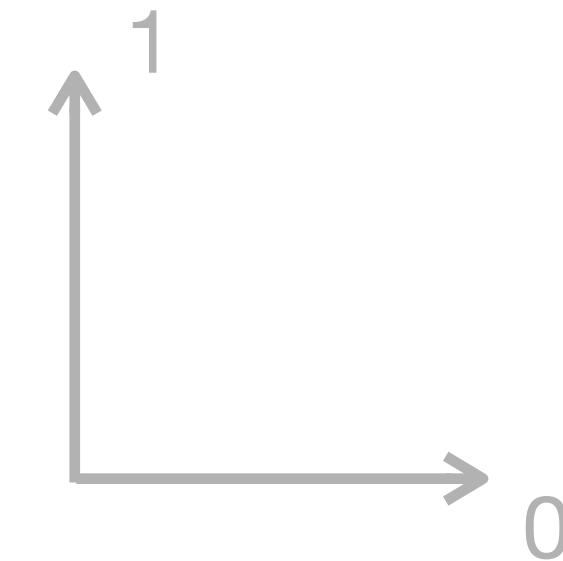
1

Encodage de l'information

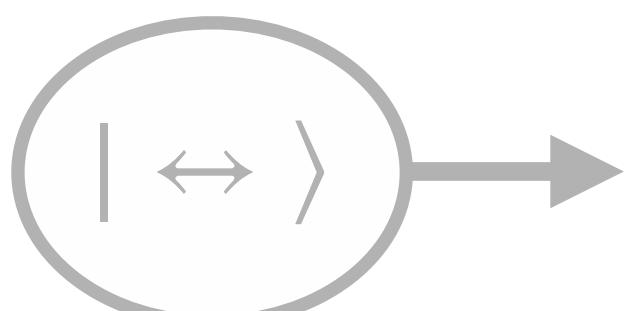
Bit à transmettre

0

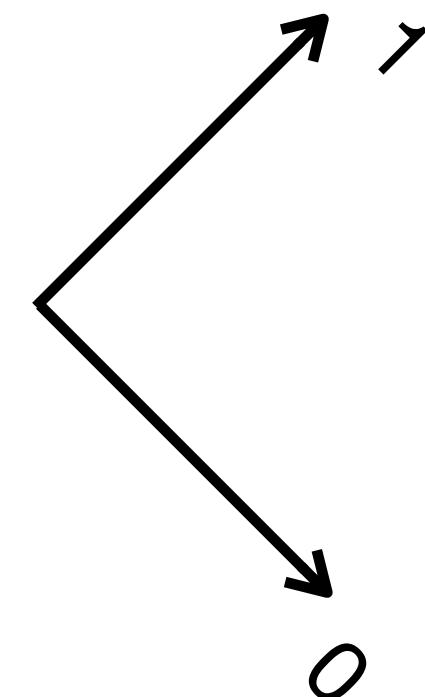
Base de mesure



Photon encodé



1

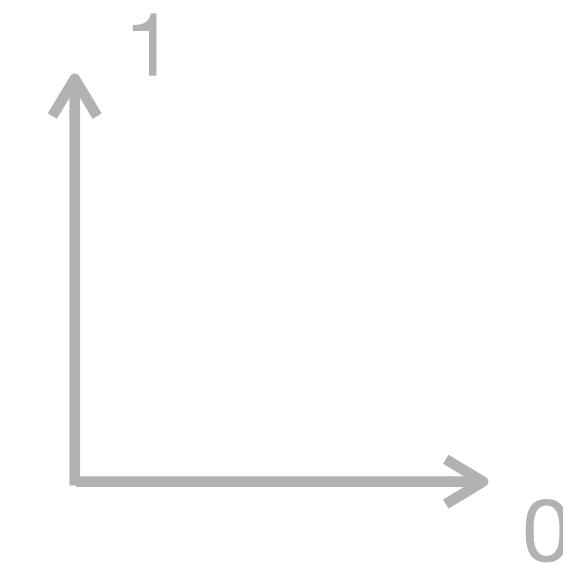


Encodage de l'information

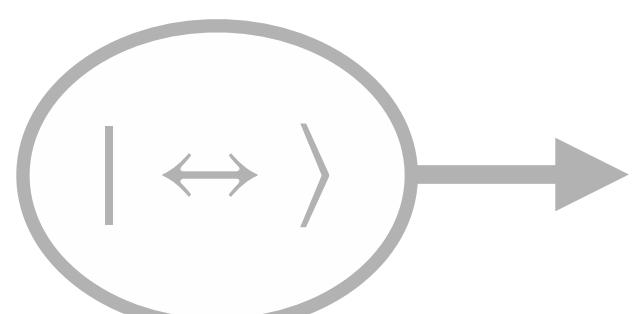
Bit à transmettre

0

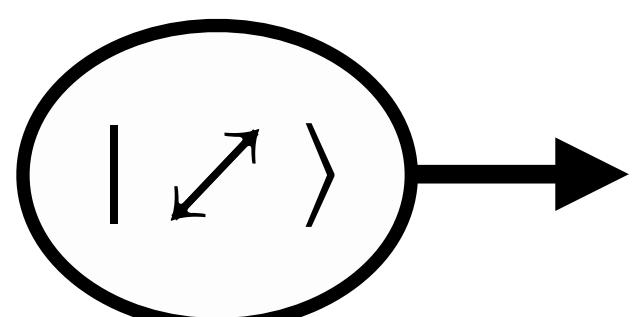
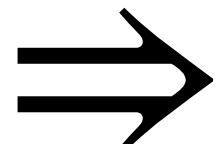
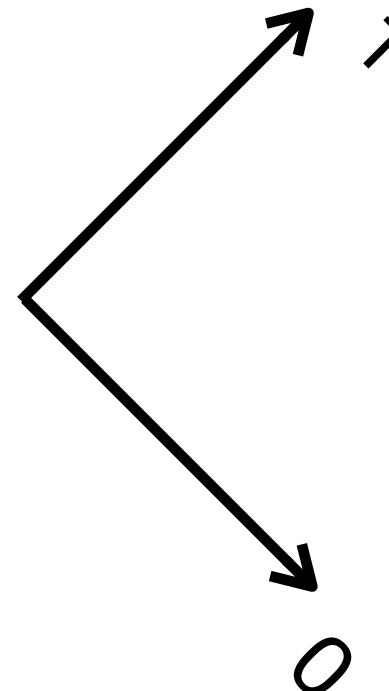
Base de mesure



Photon encodé



1

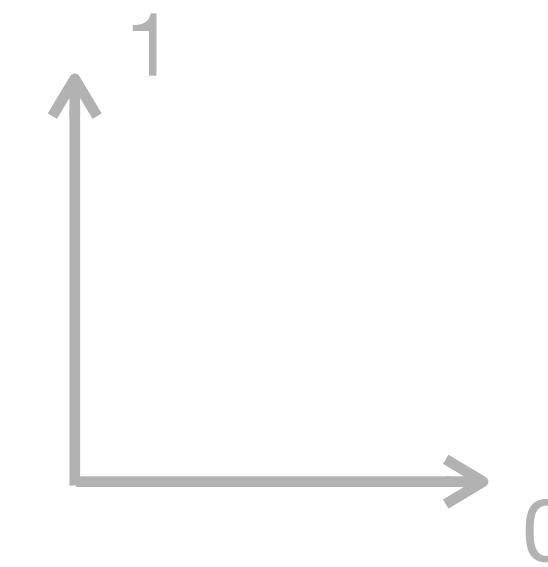


Encodage de l'information

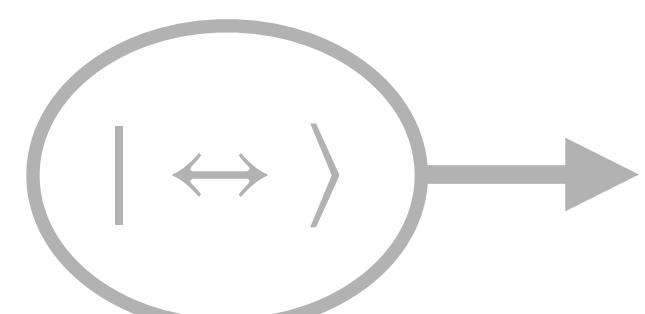
Bit à transmettre

0

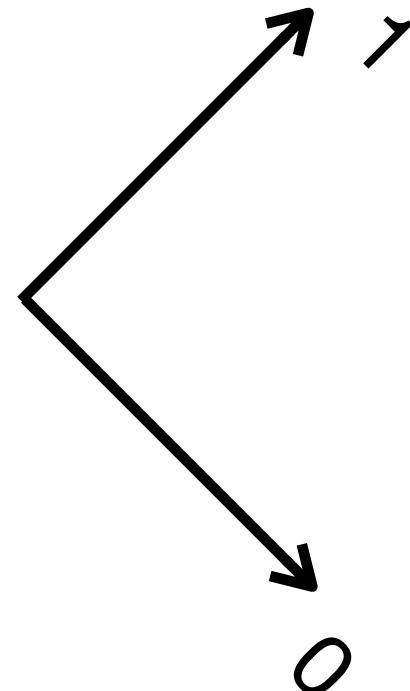
Base de mesure



Photon encodé



1



Bit transmis

$$P_{| \leftrightarrow \rangle} = 1$$

A circle containing the quantum state symbol $| \leftrightarrow \rangle$, with an arrow pointing to the right.

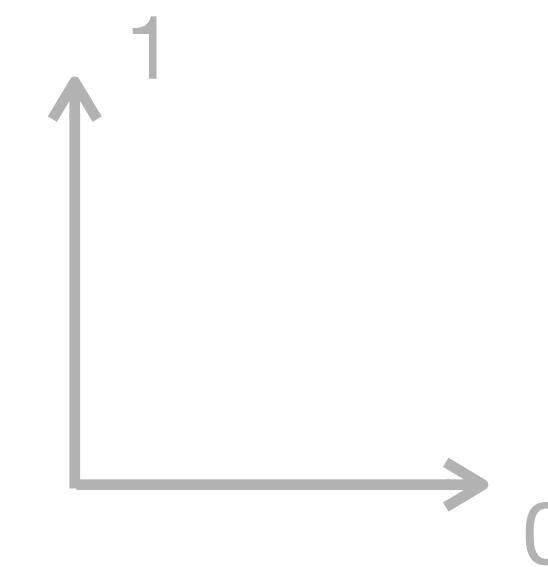
1

Encodage de l'information

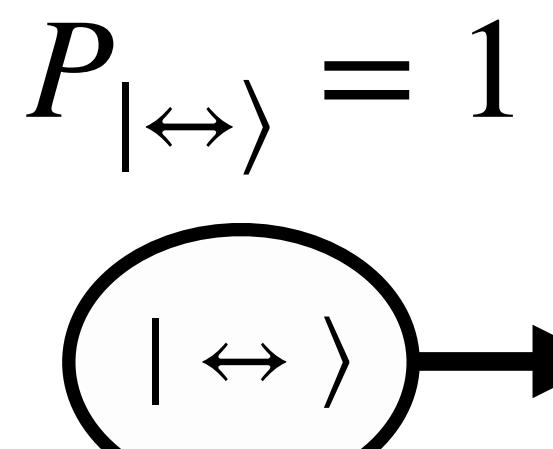
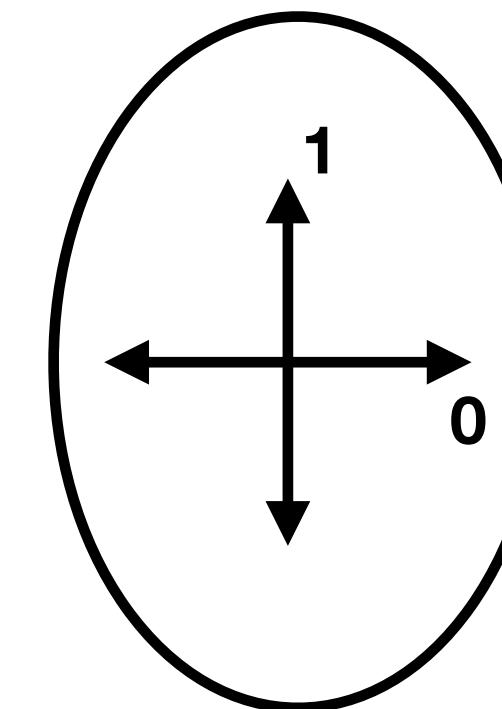
Bit à transmettre

0

Base de mesure



Photon encodé

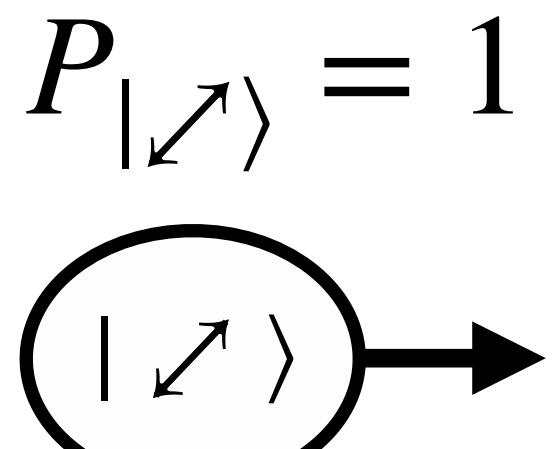
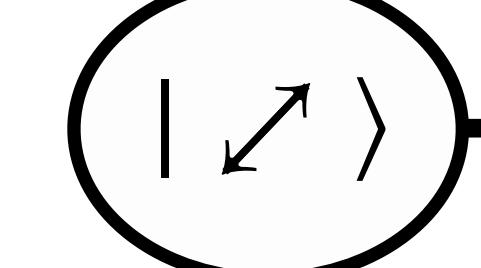
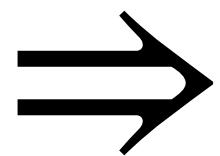
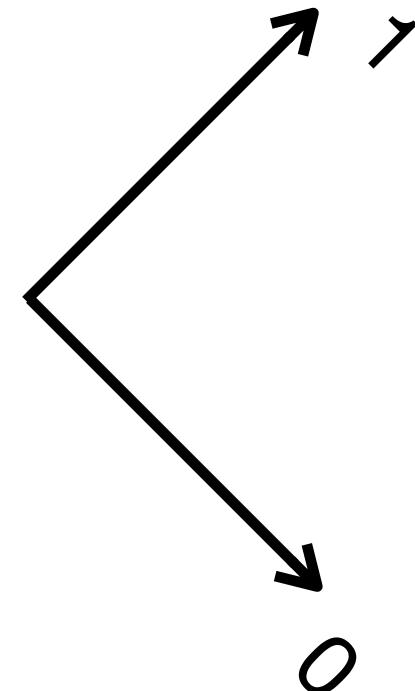


Bit transmis

0

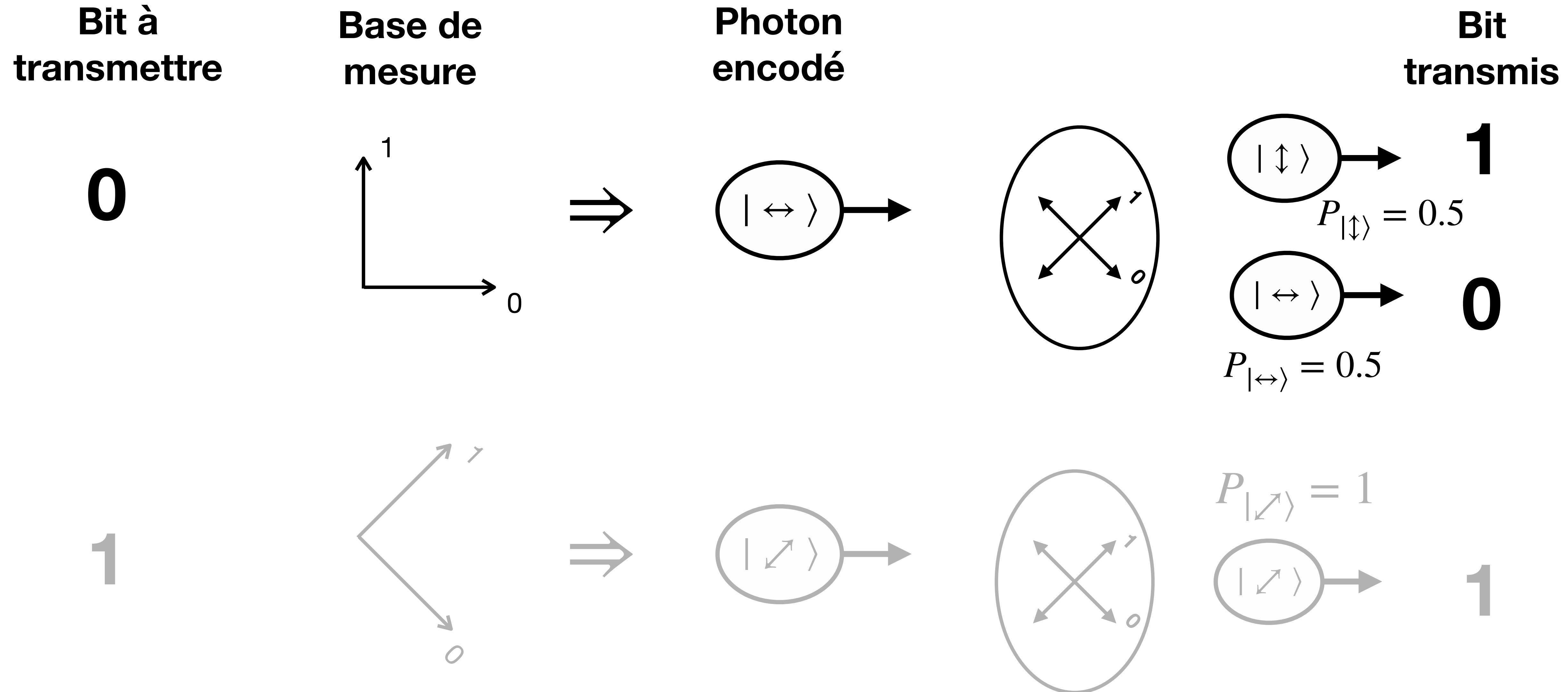


1



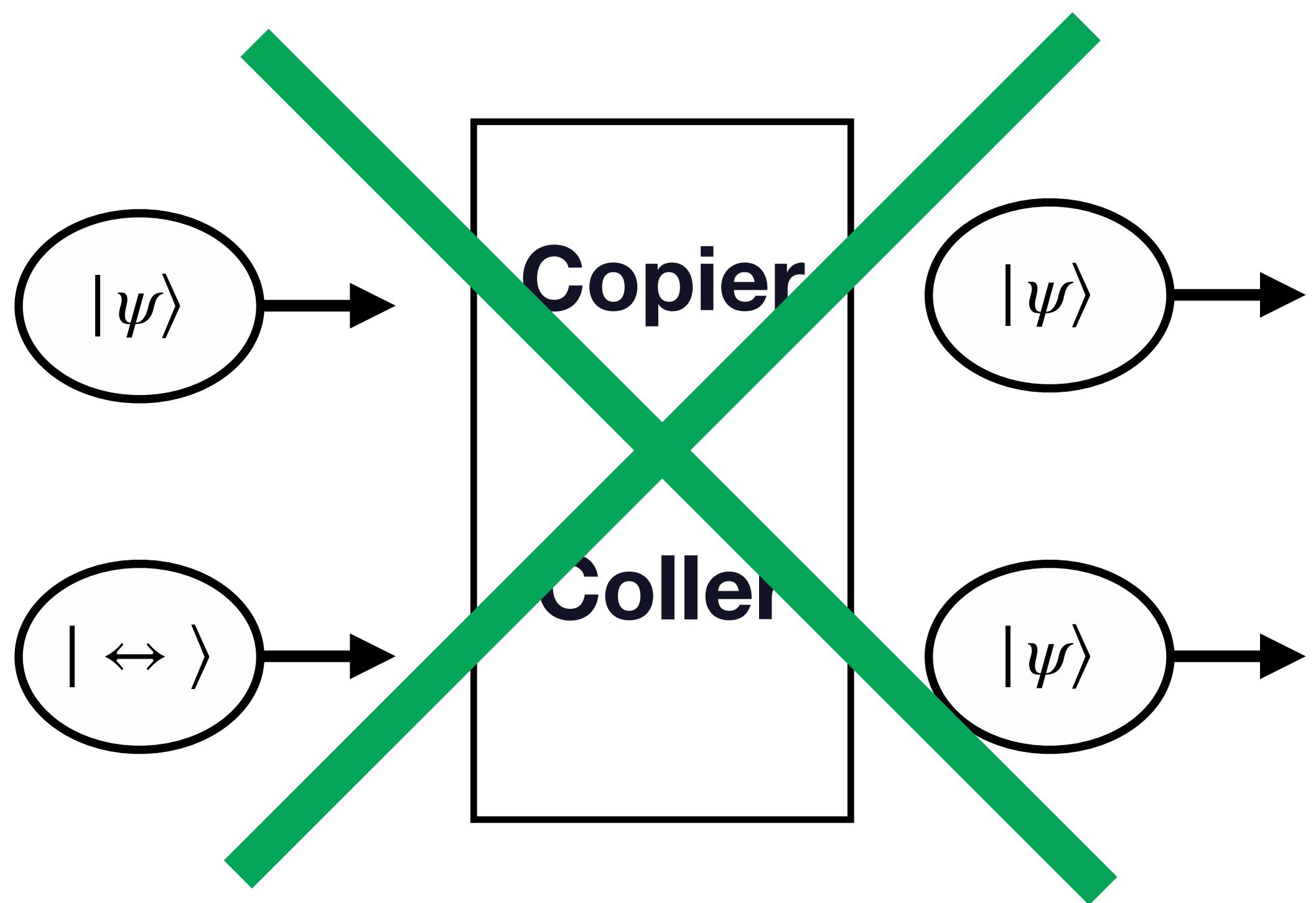
1

Encodage de l'information



Théorème de non-clonage

"Il est impossible de copier l'état quantique d'un photon dans celui d'un deuxième photon"



Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

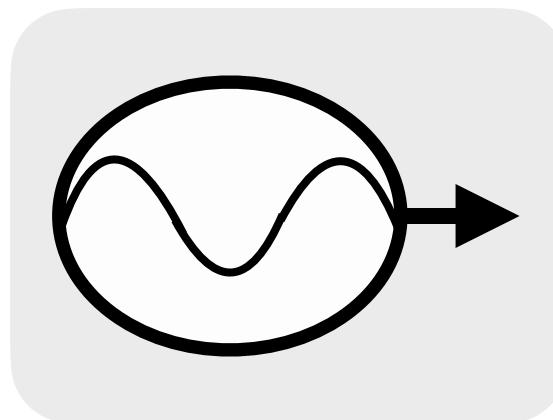
Plan

- ✓ Présentation
- ✓ Cryptographie
- ✓ Le qubit
- ✓ Le photon: messager d'information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

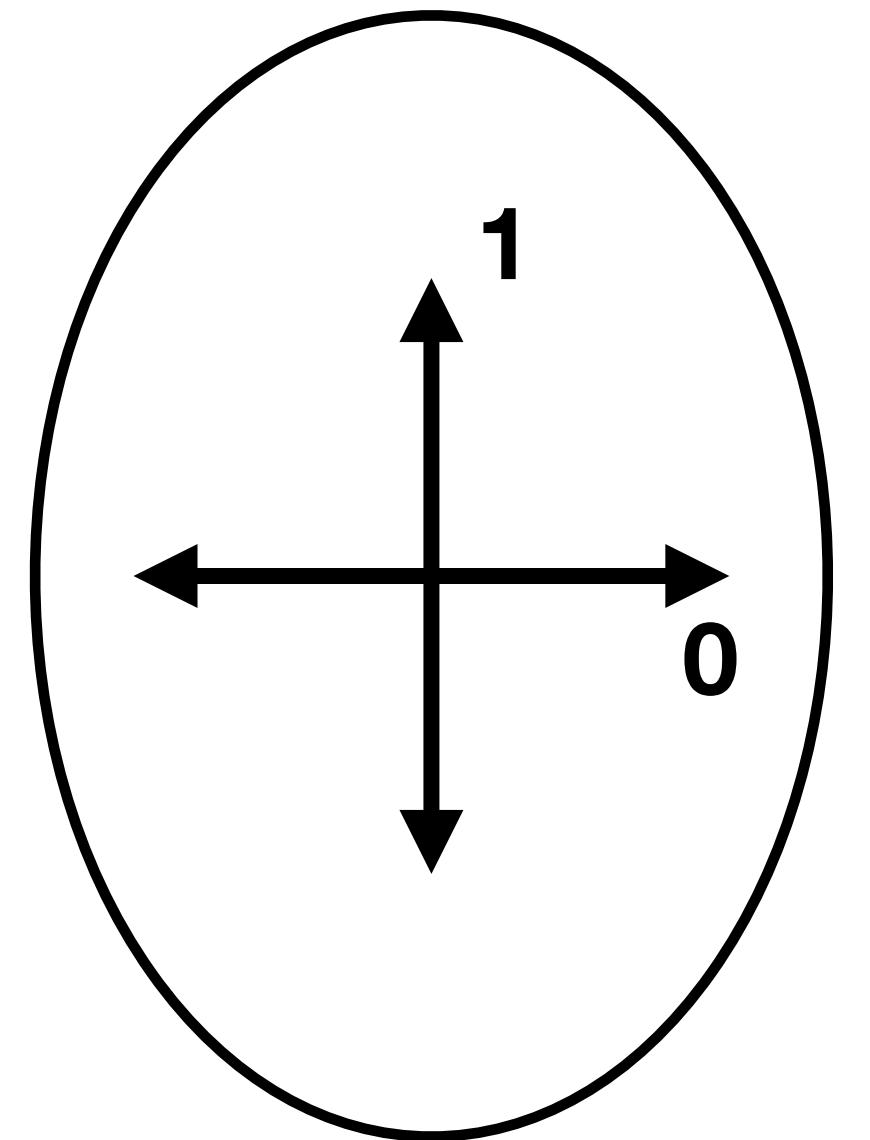
Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

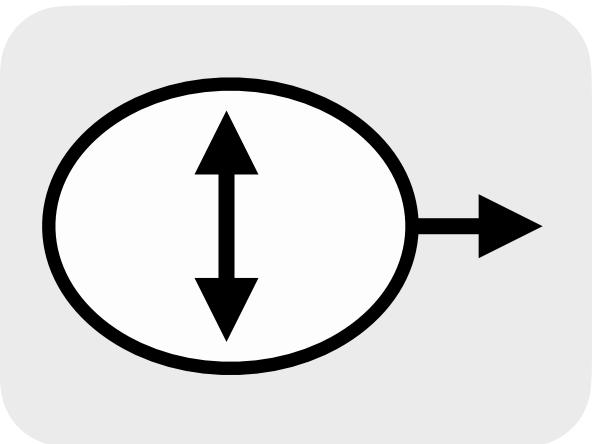
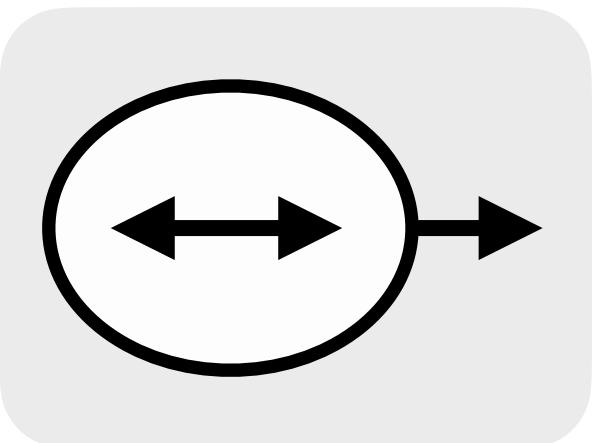
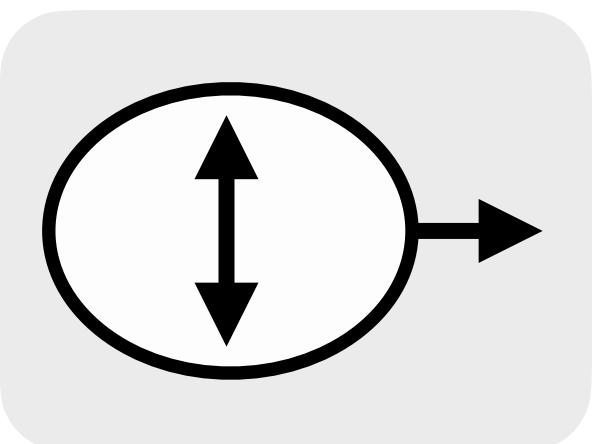
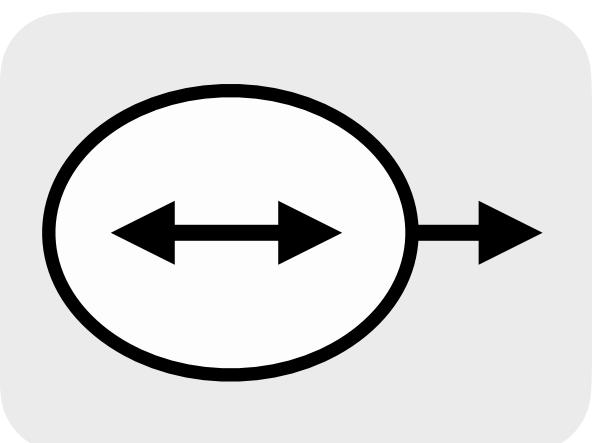
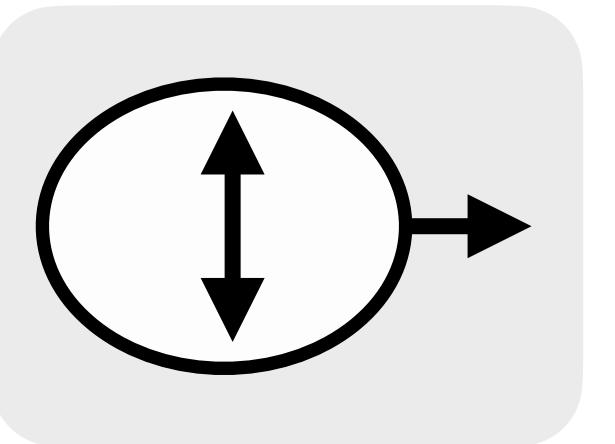
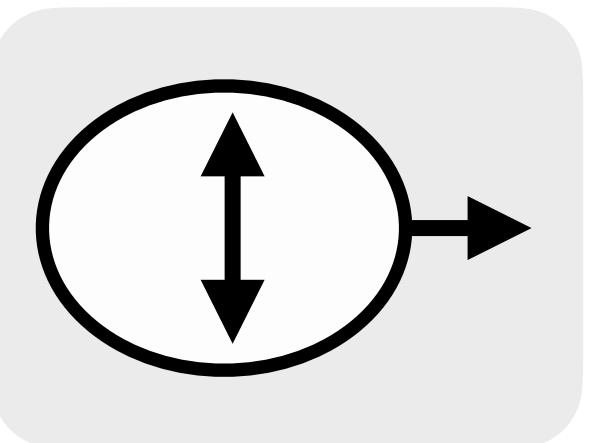
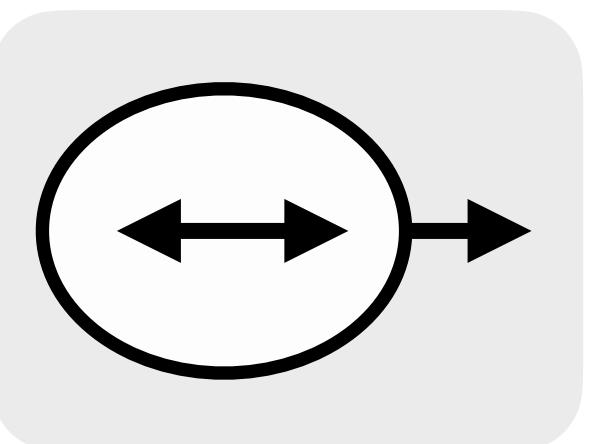
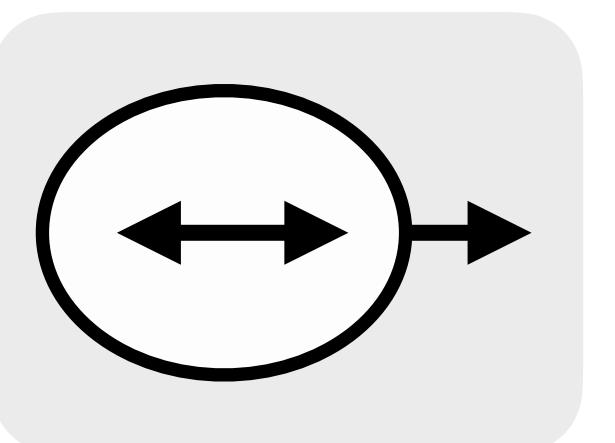
Intrication



$$\alpha | \leftrightarrow \leftrightarrow \rangle + \beta | \leftrightarrow \uparrow \downarrow \rangle \\ + \delta | \uparrow \leftrightarrow \rangle + \gamma | \uparrow \uparrow \downarrow \downarrow \rangle$$



$$|\alpha|^2 + |\beta|^2 + |\delta|^2 + |\gamma|^2 = 1$$



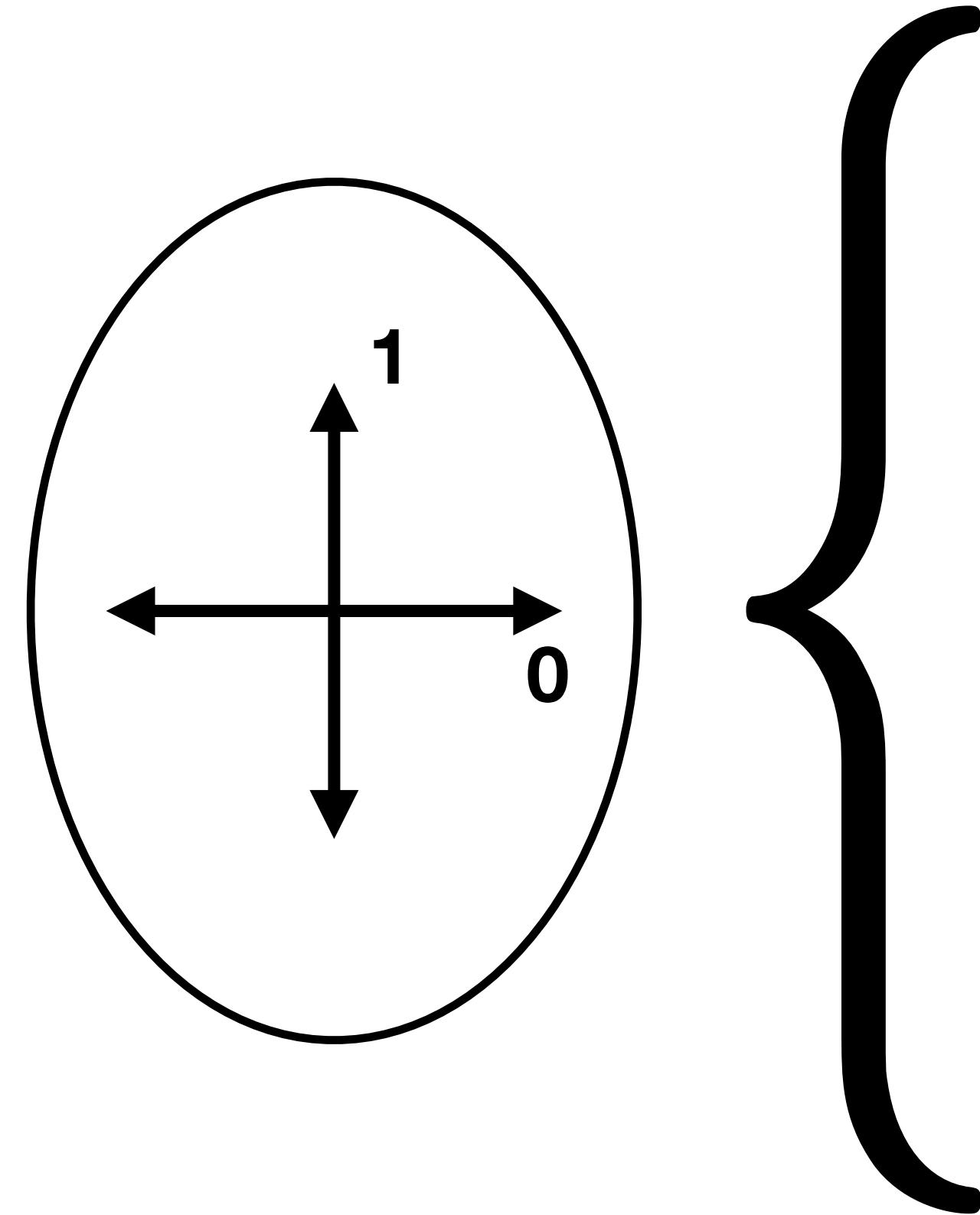
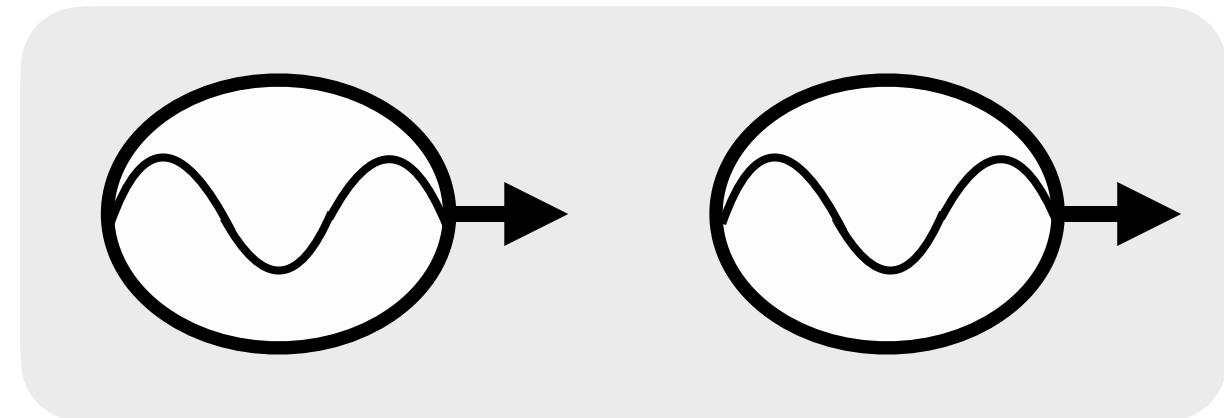
$$P_{| \leftrightarrow \leftrightarrow \rangle} = |\alpha|^2$$

$$P_{| \leftrightarrow \uparrow \downarrow \rangle} = |\beta|^2$$

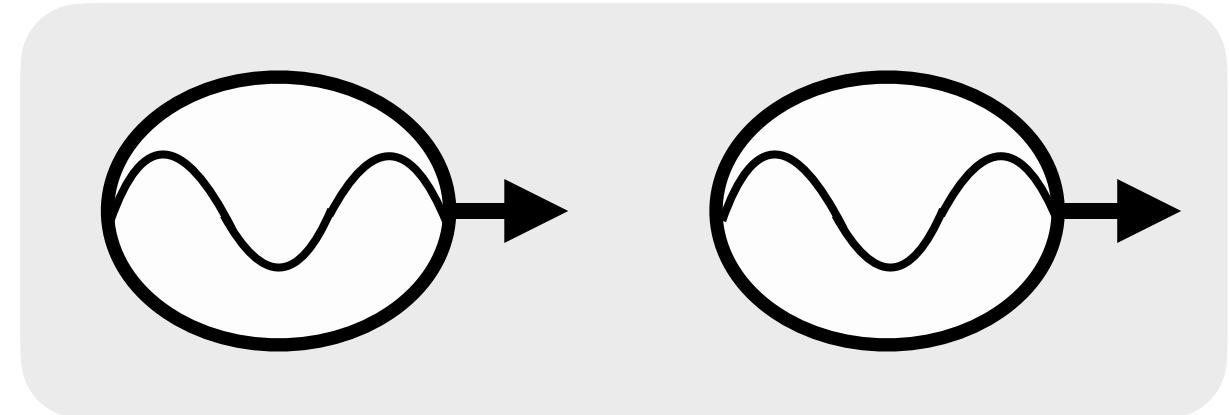
$$P_{| \uparrow \leftrightarrow \rangle} = |\delta|^2$$

$$P_{| \uparrow \uparrow \downarrow \downarrow \rangle} = |\gamma|^2$$

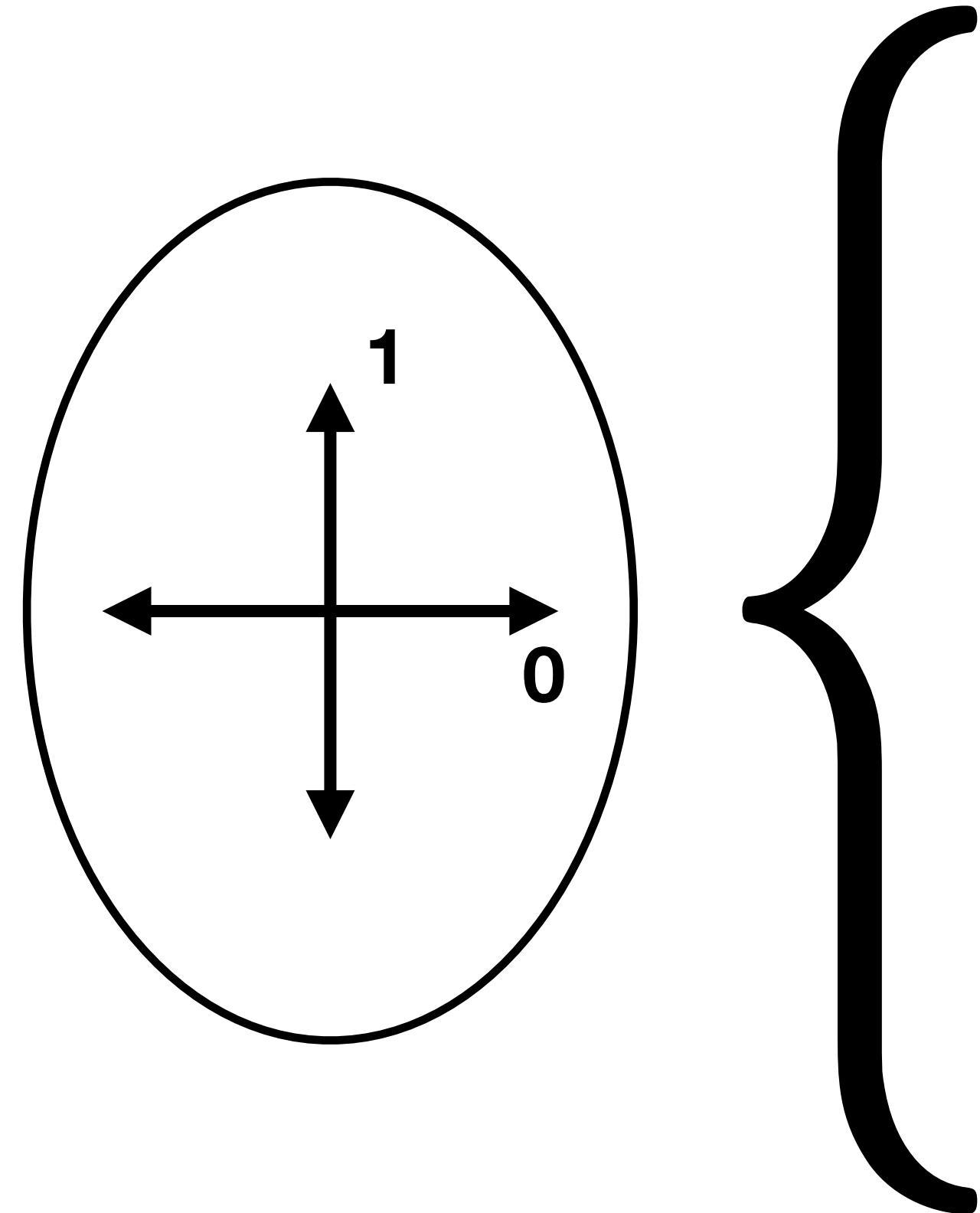
Intrication



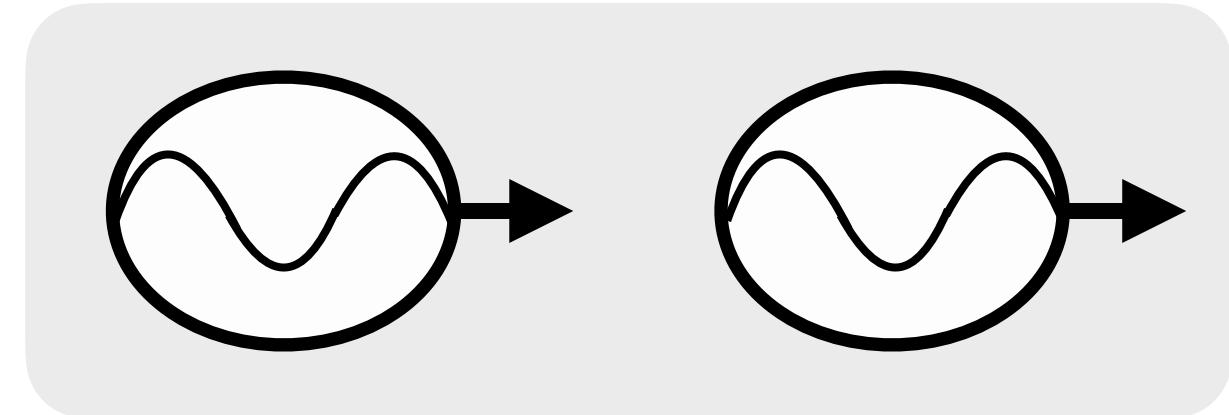
Intrication



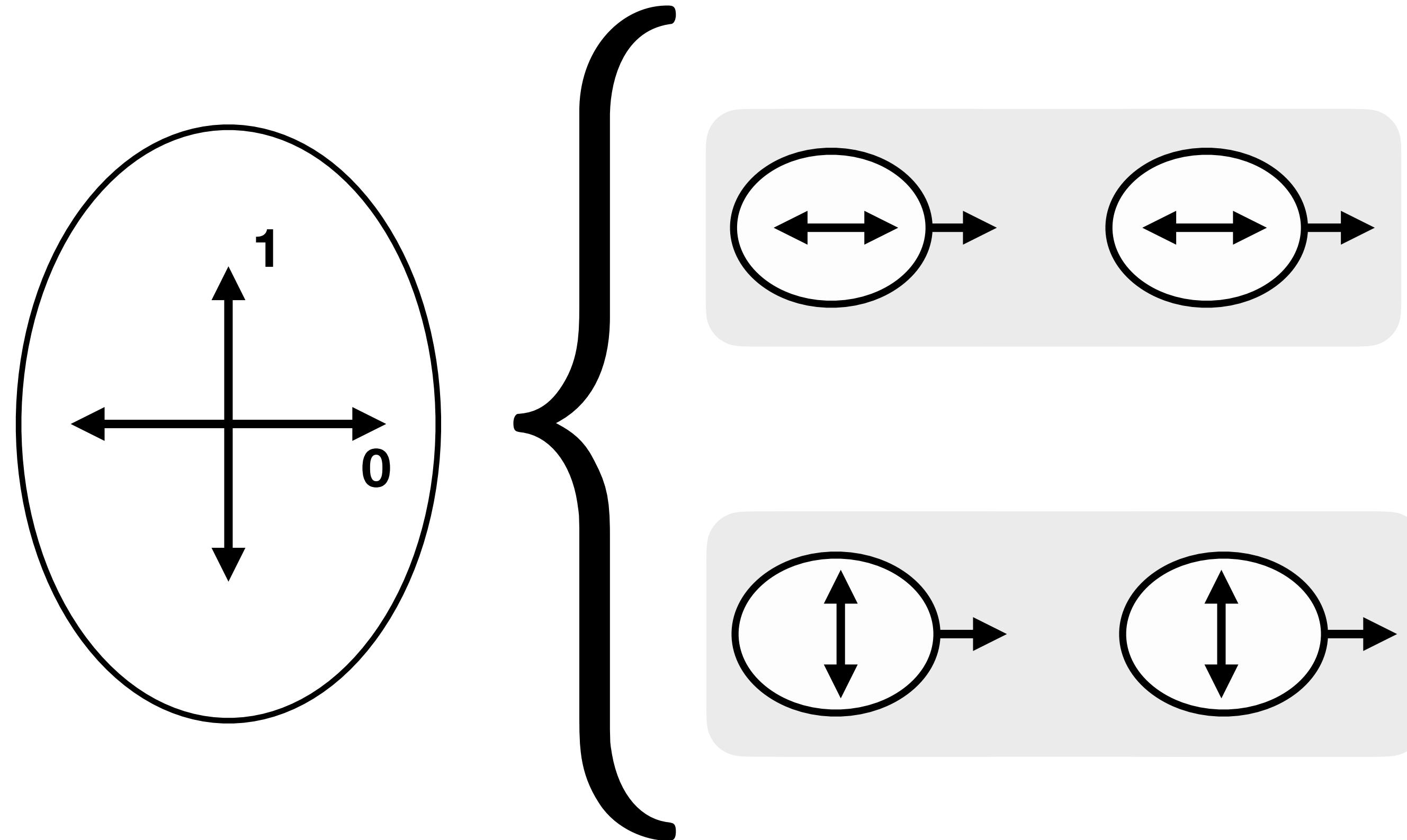
$$\frac{1}{\sqrt{2}} |\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\rangle$$



Intrication



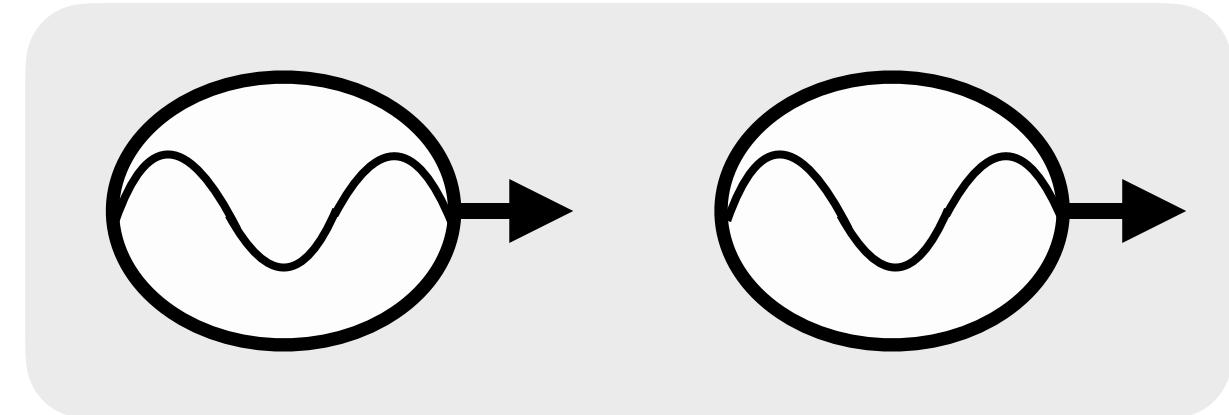
$$\frac{1}{\sqrt{2}} |\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\rangle$$



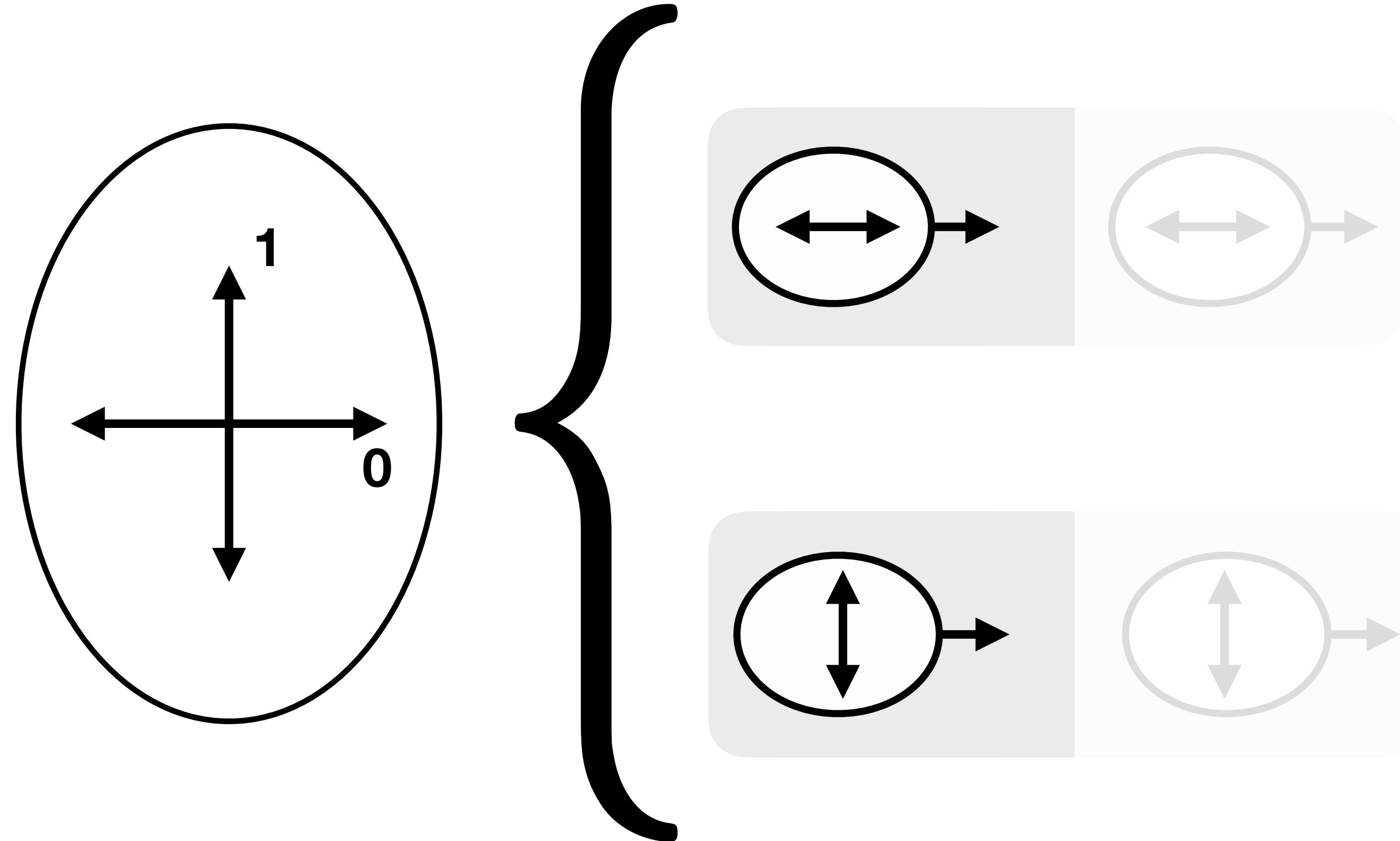
$$P_{|\leftrightarrow\leftrightarrow\rangle} = \frac{1}{2}$$

$$P_{|\uparrow\downarrow\rangle} = \frac{1}{2}$$

Intrication



$$\frac{1}{\sqrt{2}} |\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\rangle$$



$$P_{|\leftrightarrow\leftrightarrow\rangle} = \frac{1}{2}$$

$$P_{|\uparrow\downarrow\rangle} = \frac{1}{2}$$

Paires de Bell

Φ^+

$$\frac{1}{\sqrt{2}} |\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\uparrow\rangle$$

Φ^-

$$\frac{1}{\sqrt{2}} |\leftrightarrow\leftrightarrow\rangle - \frac{1}{\sqrt{2}} |\uparrow\downarrow\uparrow\rangle$$

Ψ^+

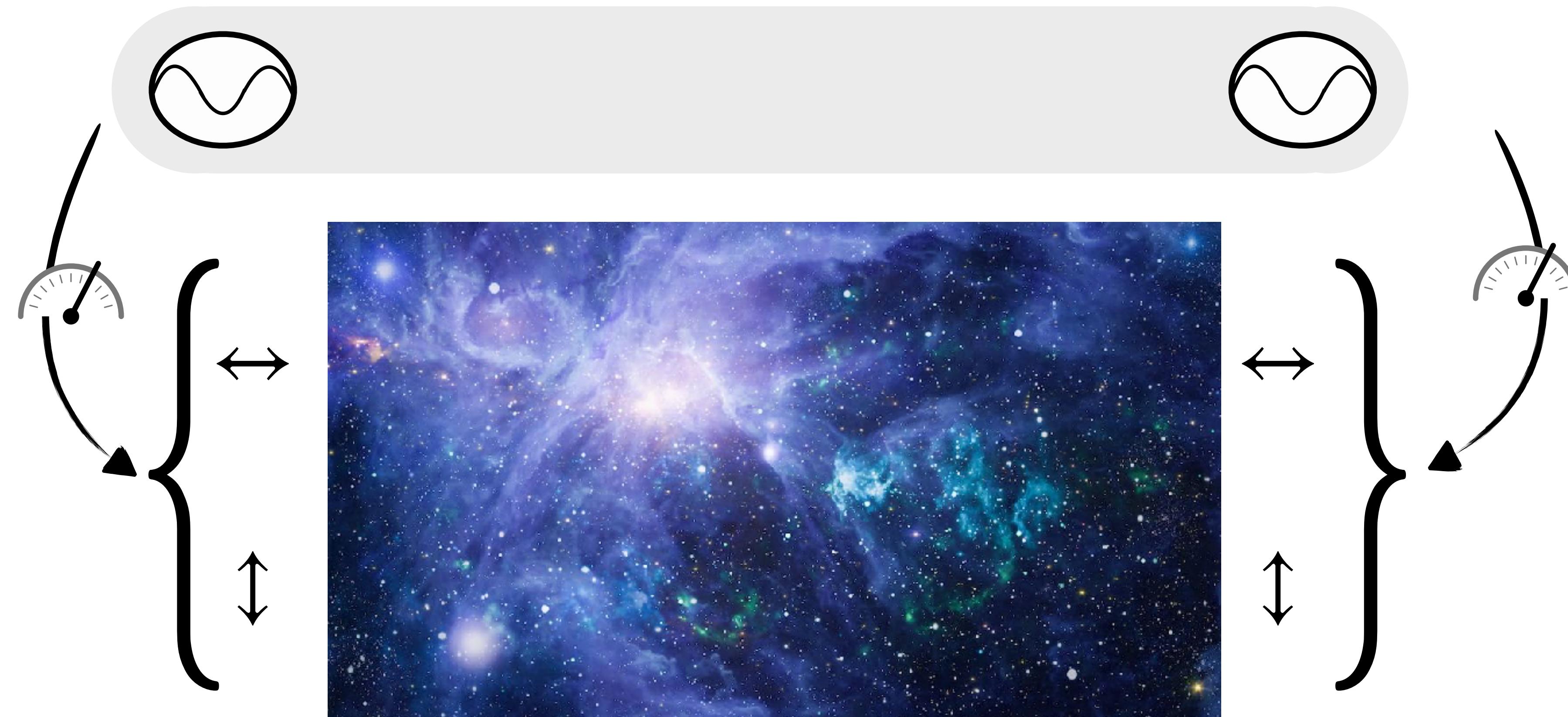
$$\frac{1}{\sqrt{2}} |\leftrightarrow\uparrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\leftrightarrow\rangle$$

Ψ^-

$$\frac{1}{\sqrt{2}} |\leftrightarrow\uparrow\rangle - \frac{1}{\sqrt{2}} |\uparrow\leftrightarrow\rangle$$

Corrélations indépendantes de la distance

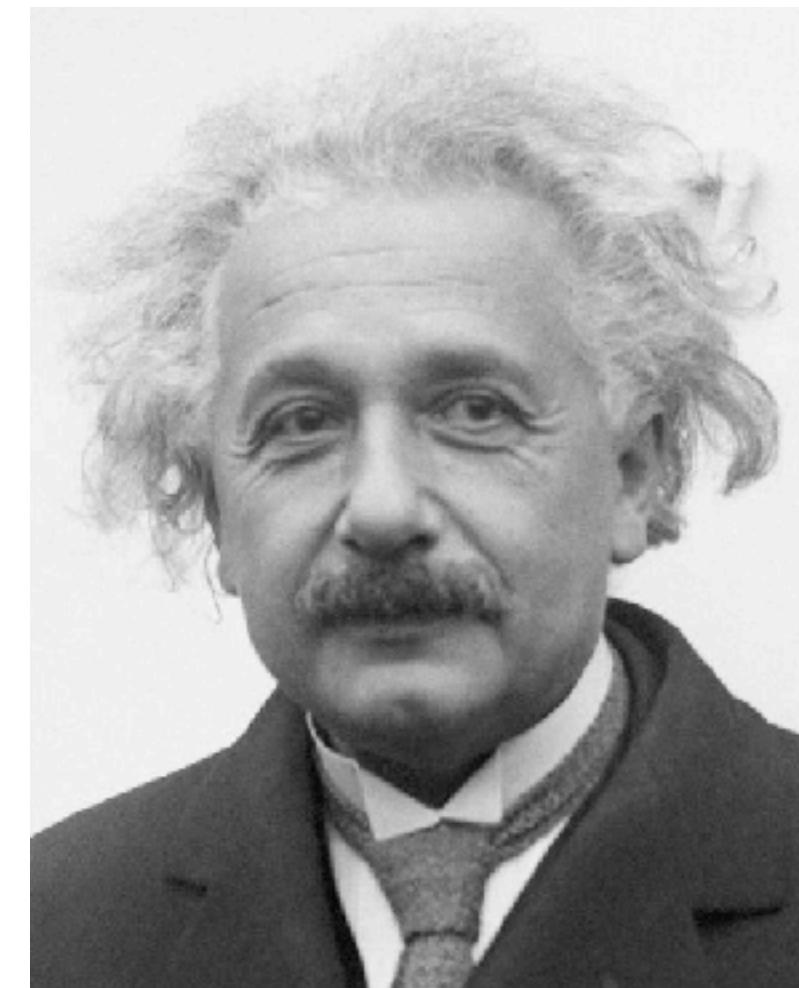
$$\frac{1}{\sqrt{2}} |\leftrightarrow\leftrightarrow\rangle + \frac{1}{\sqrt{2}} |\uparrow\downarrow\uparrow\rangle$$



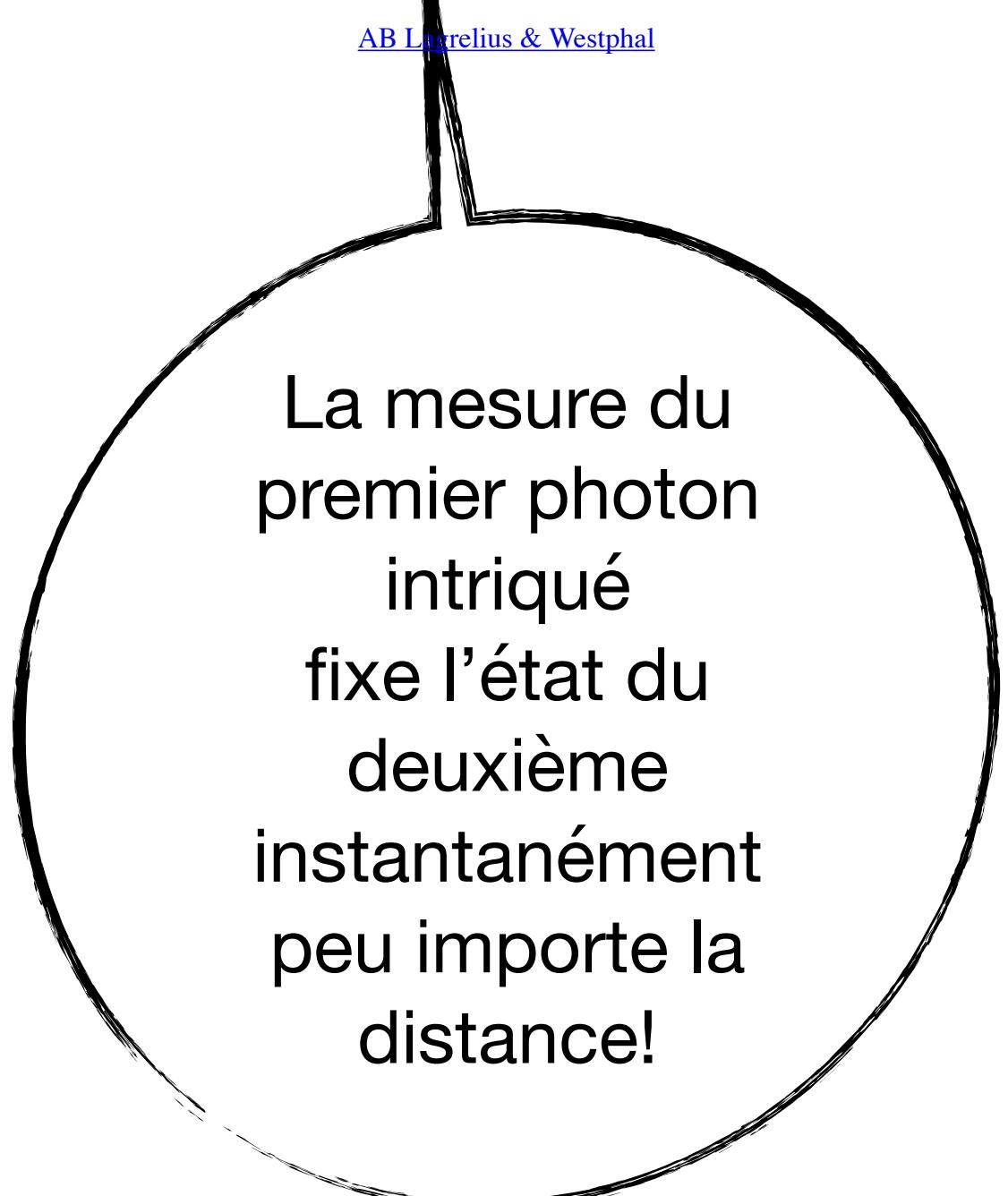
Interprétation de l'intrication



[AB Lægrelius & Westphal](#)



(Image credit: Bettmann / Contributor via Getty Images)



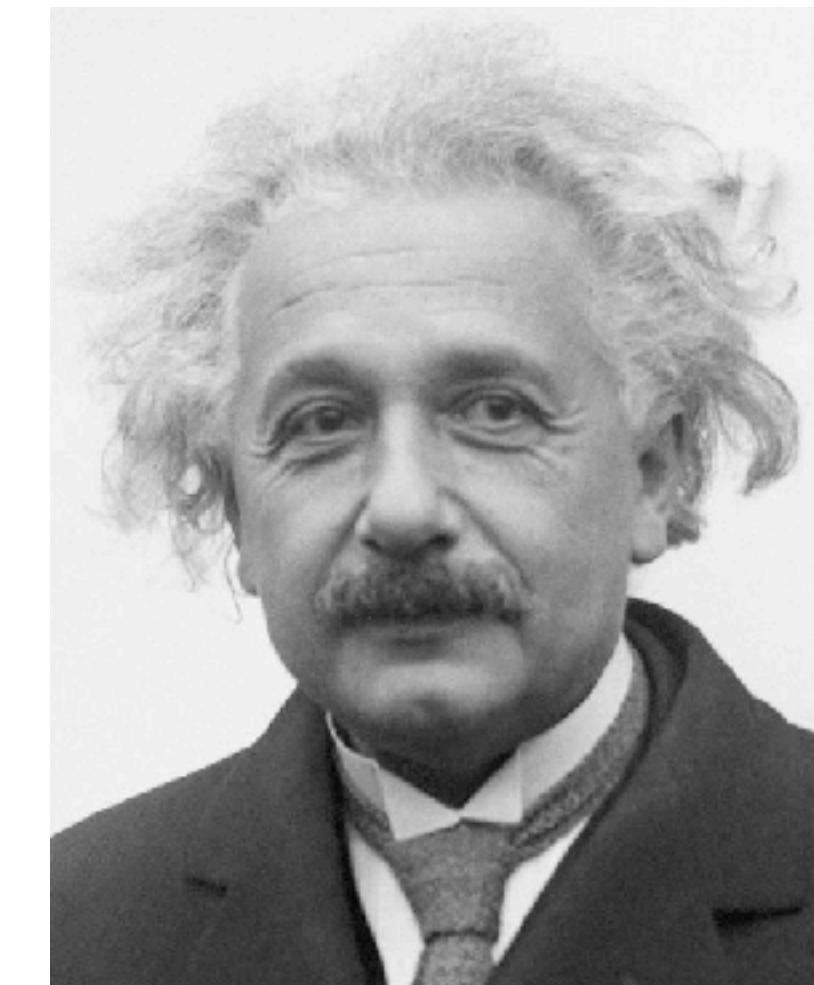
La mesure du
premier photon
intriqué
fixe l'état du
deuxième
instantanément
peu importe la
distance!

Interprétation de l'intrication



[AB Lægrelius & Westphal](#)

La mesure du premier photon intriqué fixe l'état du deuxième instantanément peu importe la distance!



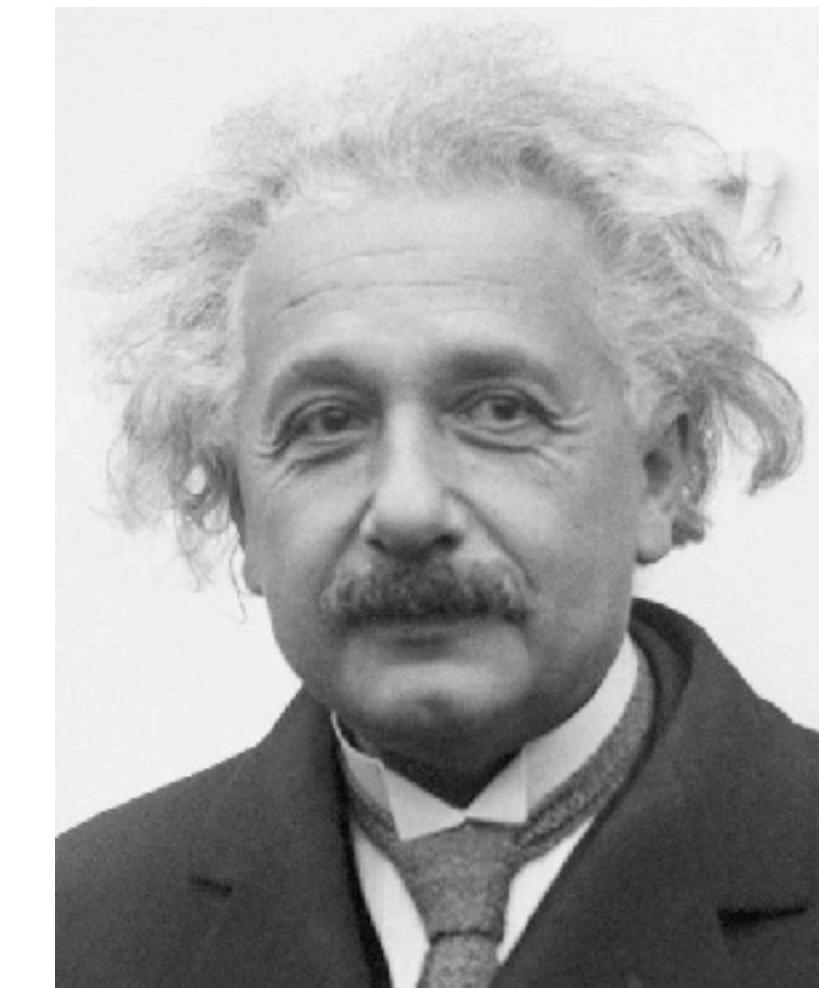
(Image credit: Bettmann / Contributor via Getty Images)

Impossible!
Le choix de l'état doit être déterminé avant la mesure! Il doit y avoir des variables cachées!

Interprétation de l'intrication



[AB Magrelius & Westphal](#)



(Image credit: Bettmann / Contributor via Getty Images)

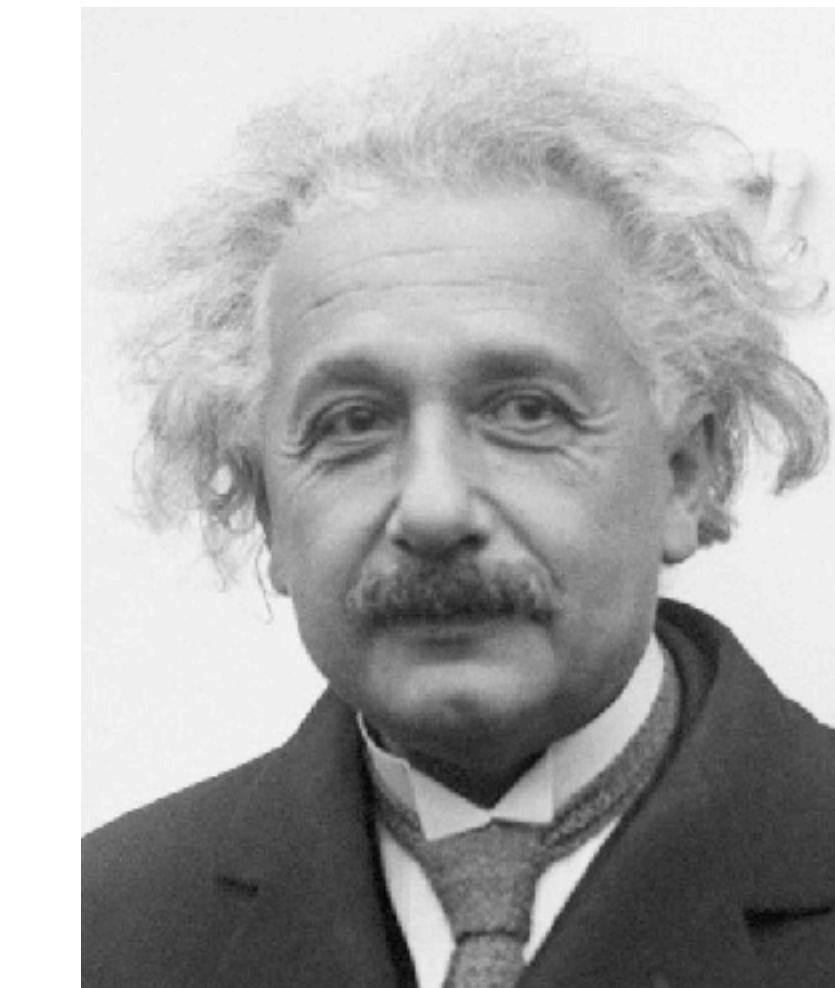
Impossible!
Le choix de l'état
doit être déterminé
avant la mesure! Il
doit y avoir des
variables cachées!

Interprétation de l'intrication



[AB Lægrelius & Westphal](#)

En fait, j'ai une
façon de vérifié
expérimentalement
s'il y a des
variables cachées
ou non!



(Image credit: Bettmann / Contributor via Getty Images)

non localité!



1974, CERN

Impossible!
Le choix de l'état
doit être déterminé
avant la mesure! Il
doit y avoir des
variables cachées!

Interprétation de l'intrication



Inégalité de Bell

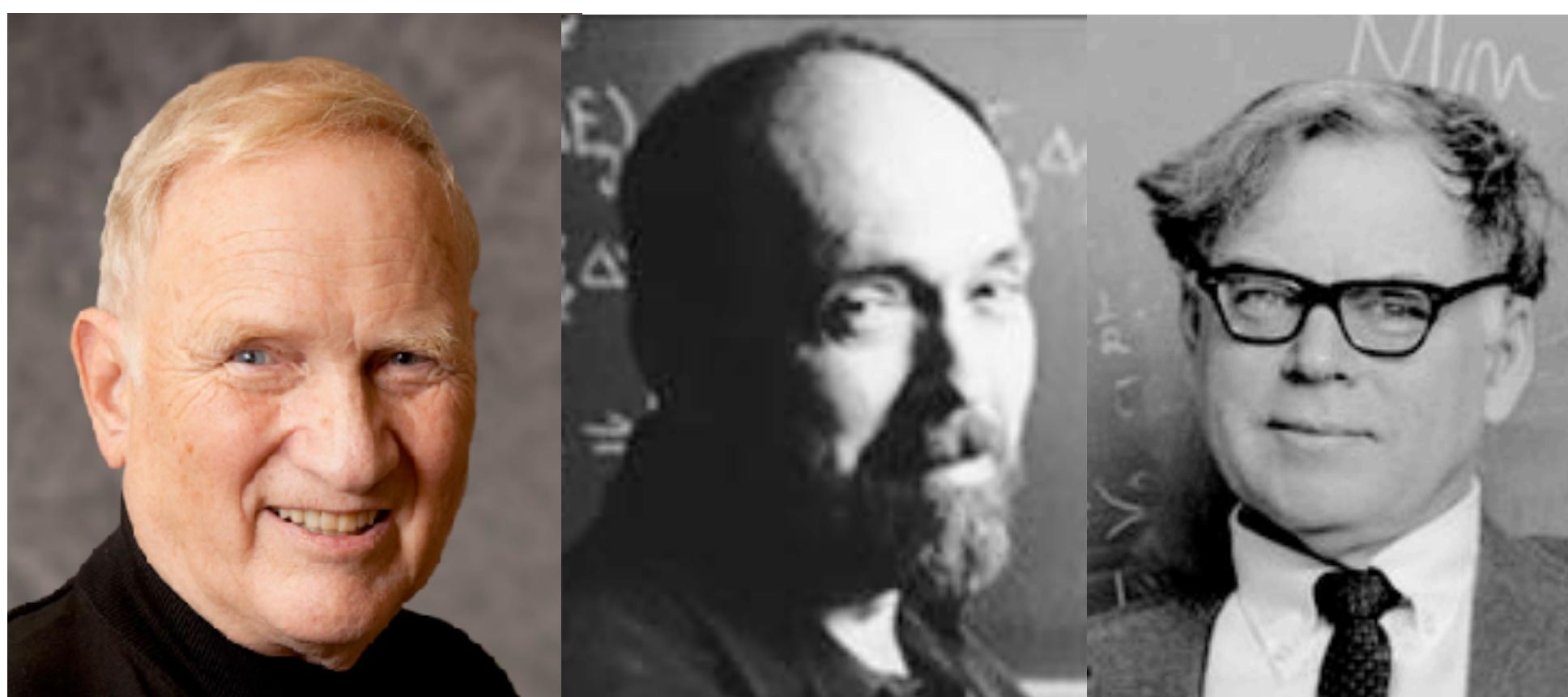
1974, CERN

Interprétation de l'intrication



Inégalité de Bell

1964



1969

John Clauser

Michael Horne

Abner Shimony

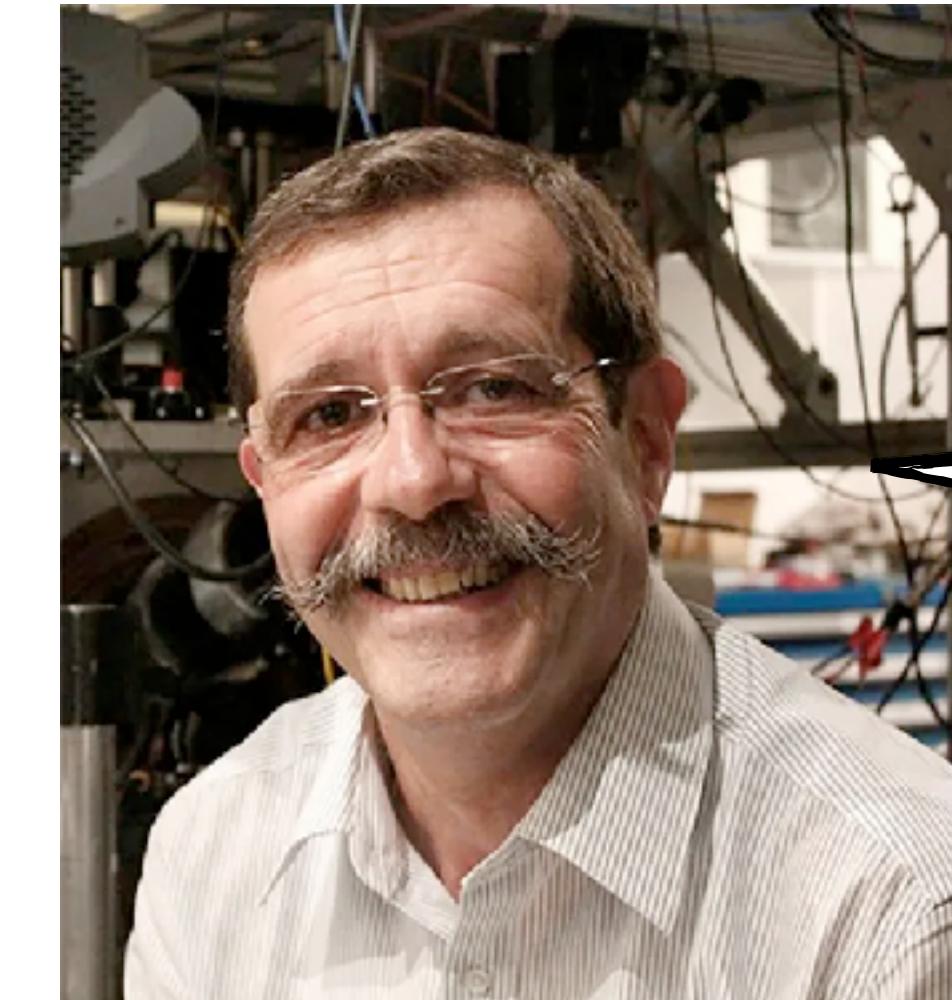
Richard Holt

Inégalité CHSH

Interprétation de l'intrication

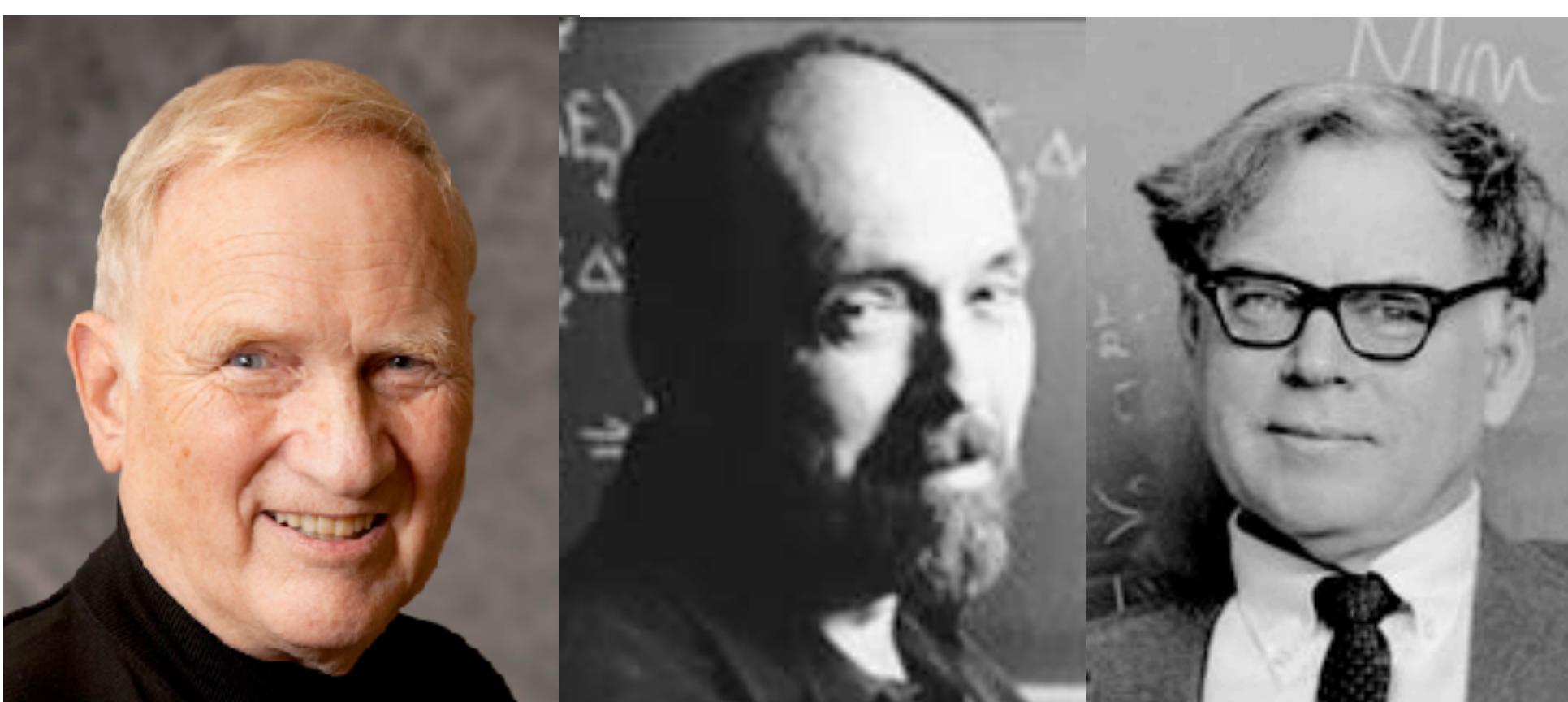


Inégalité de Bell



On ne peut pas expliquer l'intrication par une théorie aux variables cachées!

APPROUVÉ
EXPÉIMENTALEMENT



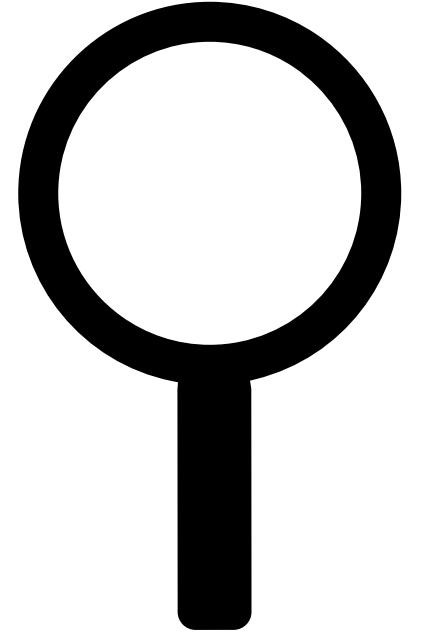
1969

1964

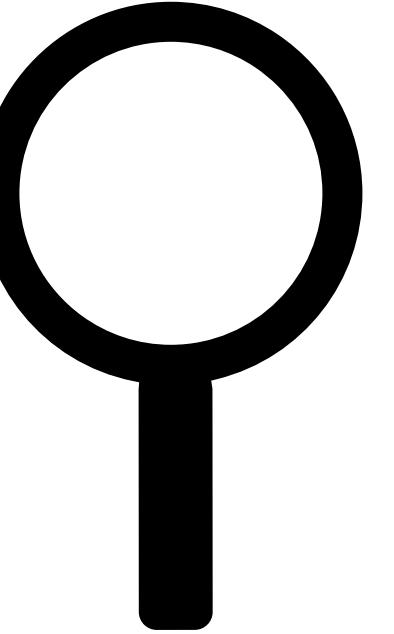
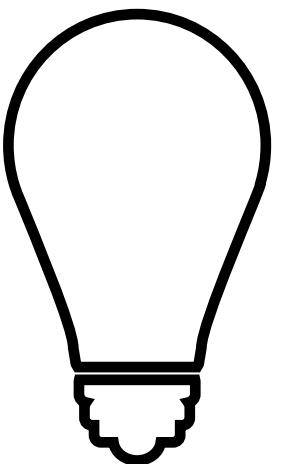
1982

Inégalité CHSH

Test de Bell



A



B

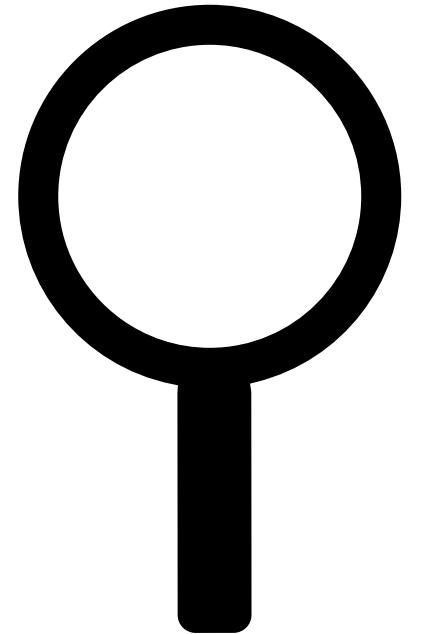
Bases: a_1, a_2

résultats: $\{0, 1\}$

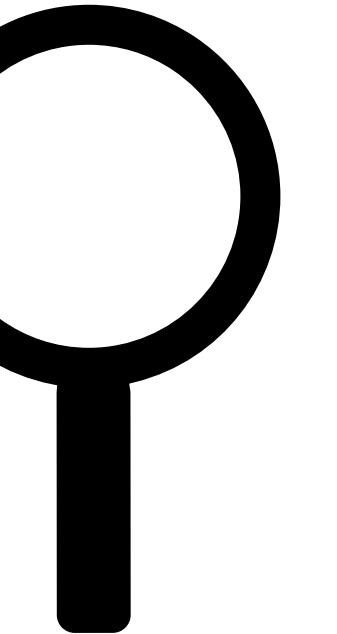
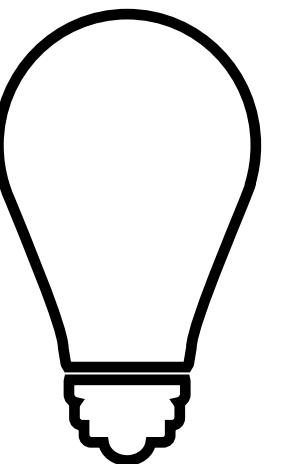
Bases: b_1, b_2

résultats: $\{0, 1\}$

Test de Bell



A



B

Bases: a_1, a_2

résultats: ~~{0, 1}~~

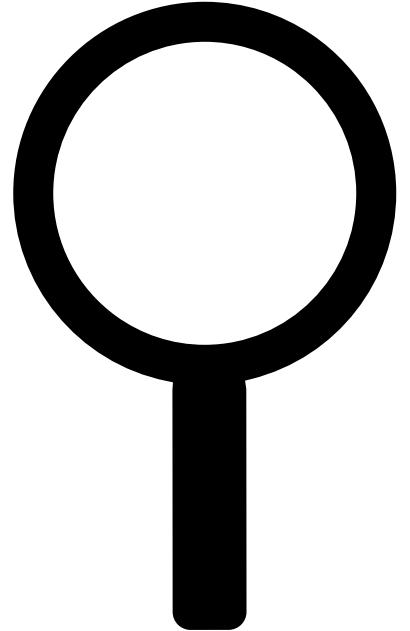
{+1, -1}

Bases: b_1, b_2

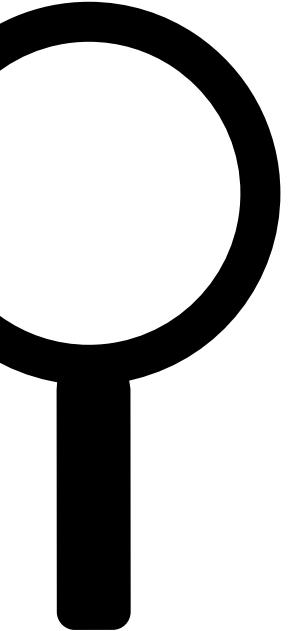
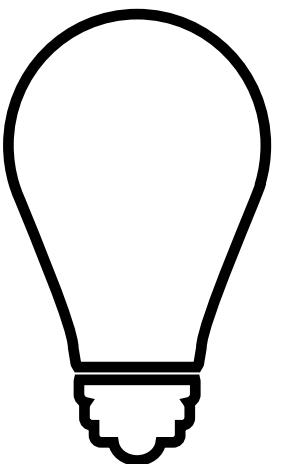
résultats: ~~{0, 1}~~

{+1, -1}

Test de Bell

**A****Bases:** a_1, a_2 **Résultats:** ~~{0, 1}~~

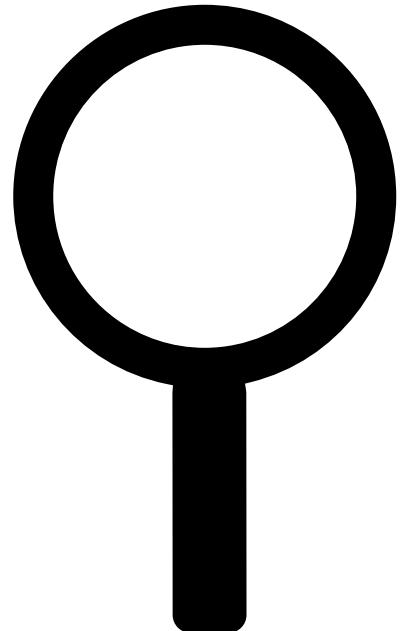
{+1, -1}

**B****Bases:** b_1, b_2 **Résultats:** ~~{0, 1}~~

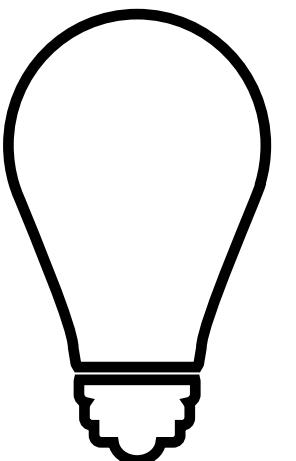
{+1, -1}

a_i	b_j	$a_i b_j$
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

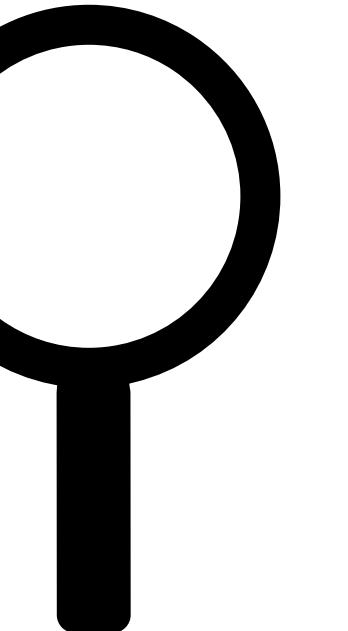
Test de Bell

**A****Bases:** a_1, a_2 **Résultats:** ~~{0, 1}~~

{+1, -1}



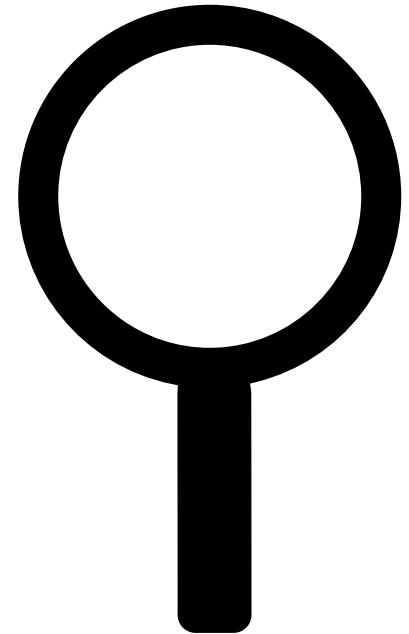
a_i	b_j	$a_i b_j$
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

**B****Bases:** b_1, b_2 **Résultats:** ~~{0, 1}~~

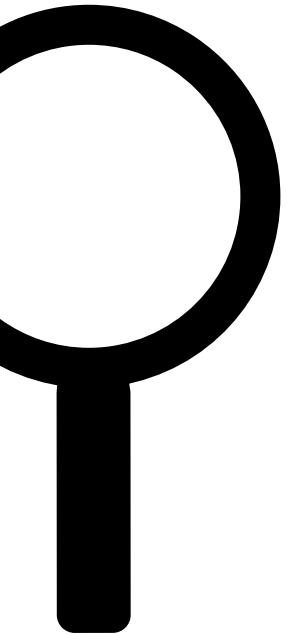
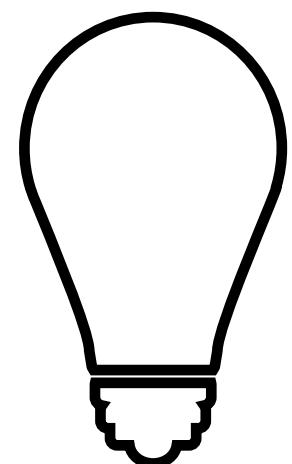
{+1, -1}

Mêmes valeurs
détectées en A et B

Test de Bell

**A****Bases:** a_1, a_2 **Résultats:** ~~{0, 1}~~

{+1, -1}

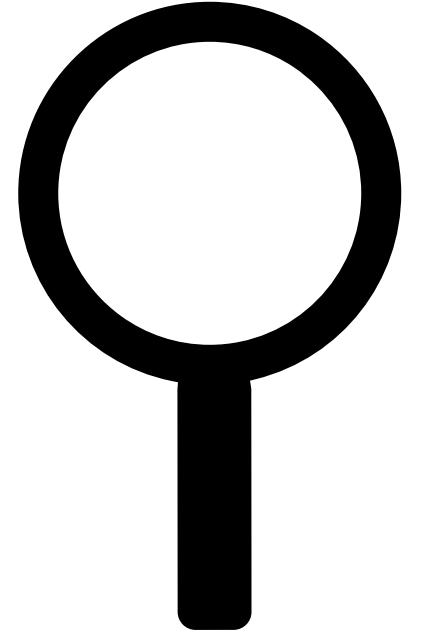
**B****Bases:** b_1, b_2 **Résultats:** ~~{0, 1}~~

{+1, -1}

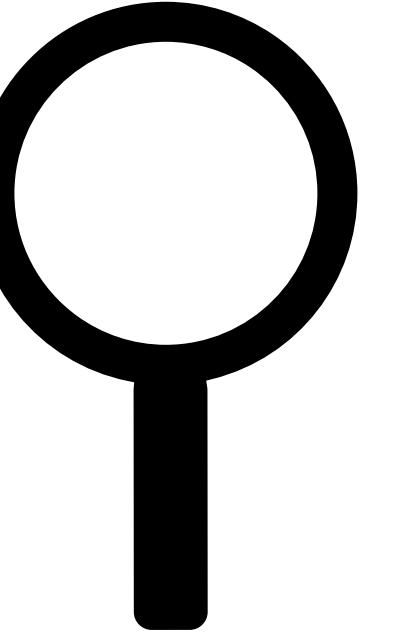
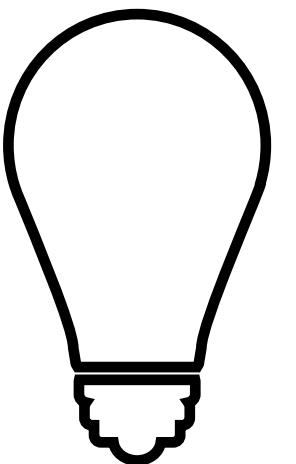
a_i	b_j	$a_i b_j$
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

Différentes valeurs
détectées en A et B

Test de Bell



A



B

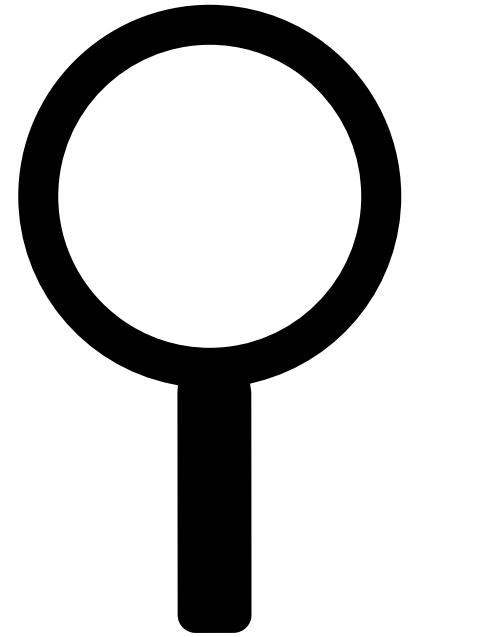
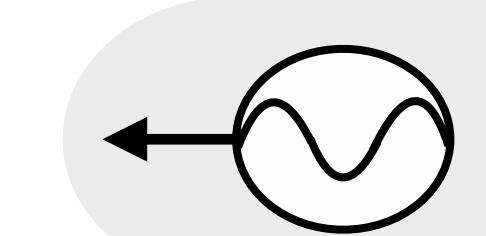
Bases: a_1, a_2

résultats: $\{+1, -1\}$

Bases: b_1, b_2

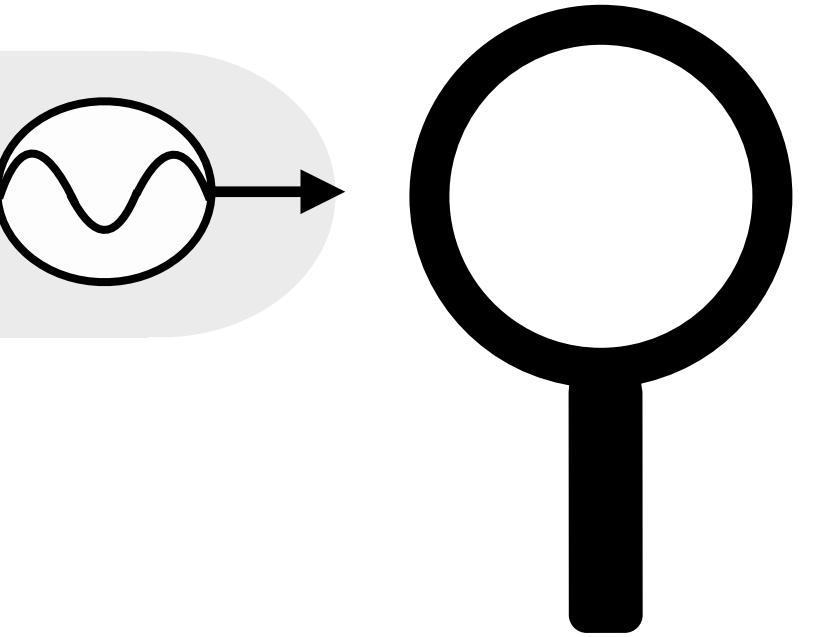
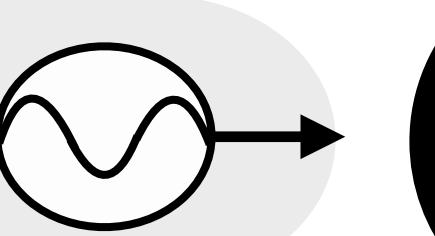
résultats: $\{+1, -1\}$

Test de Bell

**A**

Bases: a_1, a_2

résultats: $\{+1, -1\}$

**B**

Bases: b_1, b_2

résultats: $\{+1, -1\}$

Test de Bell



Bases: a_1, a_2

résultats: $\{+1, -1\}$

Bases: b_1, b_2

résultats: $\{+1, -1\}$

Test de Bell



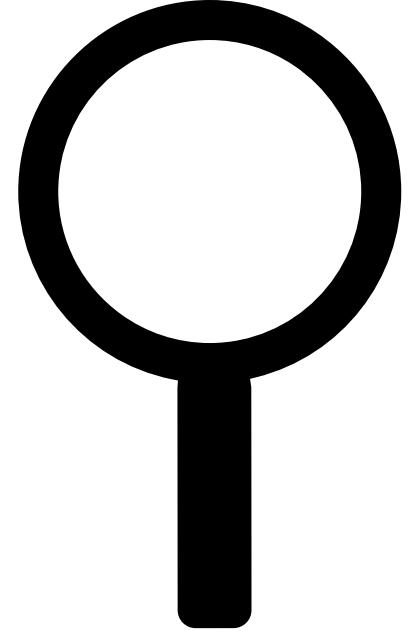
Bases: a_1, a_2

résultats: $\{+1, -1\}$

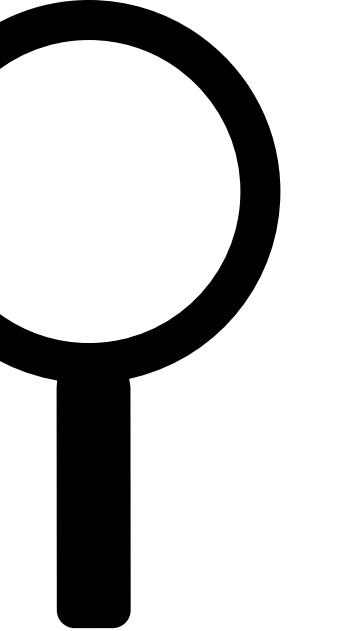
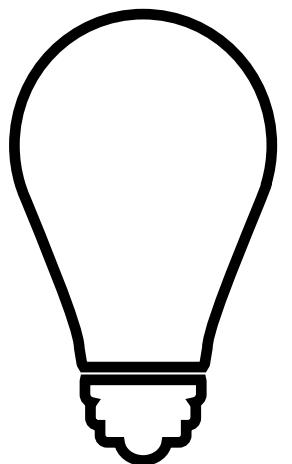
Bases: b_1, b_2

résultats: $\{+1, -1\}$

Test de Bell



A



B

Bases: a_1, a_2

résultats: $\{+1, -1\}$

Bases: b_1, b_2

résultats: $\{+1, -1\}$





Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

E_{a_i, b_j}

Interprétation

1 $a_i = b_j$ est toujours vrai

-1 $a_i = -b_j$ est toujours vrai

0 a_i et b_j sont indépendants l'un de l'autre



Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Les résultats peuvent être expliqués par des variables cachées

Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}|$$

$$E_{a_i, b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Classique

Les résultats peuvent être expliqués par des variables cachées



Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}| \{ \leq 2 \text{ Classique}$$



Inégalité CHSH

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in]2, 2\sqrt{2}] \text{ Avec des} \\ \text{paires de Bell!} \end{array}$$

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

A		B		$a_i \cdot b_j$
Base	résultat	Base	résultat	
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_i,b_j} = \frac{1}{n} \sum_{k=0}^n a_i b_j$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

A		B		$a_i \cdot b_j$
Base	résultat	Base	résultat	
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \left\{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array} \right.$$

A		B		$a_i \cdot b_j$
Base	résultat	Base	résultat	
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

A		B		$a_i \cdot b_j$
Base	résultat	Base	résultat	
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

A		B		$a_i \cdot b_j$
Base	résultat	Base	résultat	
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

$$S = 0.33 + 0 + 1 - 0 = 1.33 \leq 2$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

A		B		$a_i \cdot b_j$
Base	résultat	Base	résultat	
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

$$S = 0.33 + 0 + 1 - 0 = 1.33 \leq 2$$

Pas assez de mesures pour faire émettre une conclusion!

PAUSE

Retour à

00:00

Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

Plan

- ✓ Présentation
- ✓ Cryptographie
- ✓ Le qubit
- ✓ Le photon: messager d'information quantique
- ✓ Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- ➊ Présentation
- ➋ Cryptographie
- ➌ Le qubit
- ➍ Le photon: messager d'information quantique
- ➎ Intrication et inégalité CHSH
- ➏ Protocole E91
- ➐ Atelier pratique

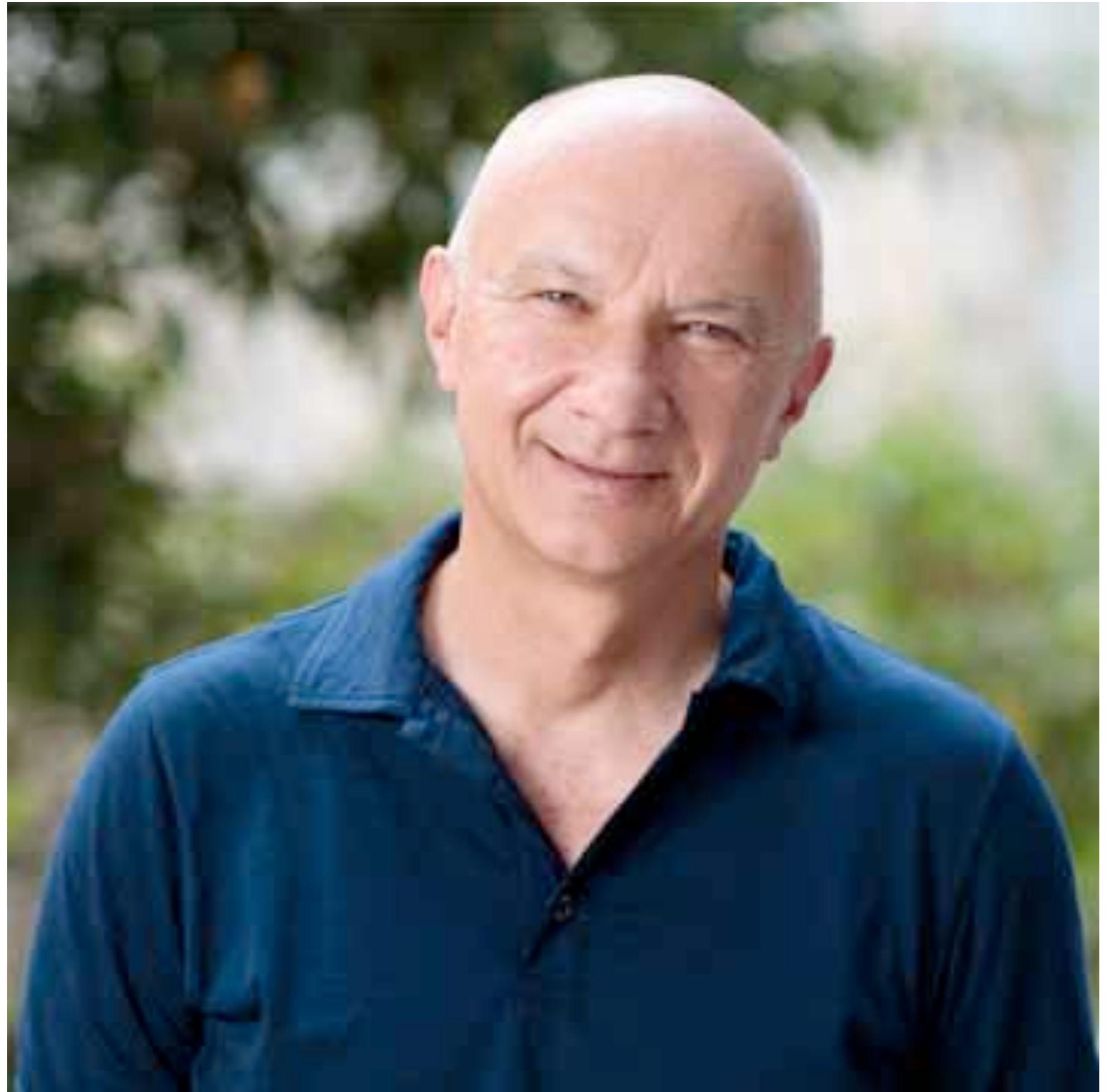
Protocole E91

Créé par **Artur Ekert** en **1991**

Protocole de distribution d'une clé
symétrique quantique (QKD)

Sécurité théorique parfaite

basée sur:



<https://www.cqt.sg/groups/artur-ekert/>



Protocole E91

Créé par **Artur Ekert** en **1991**

Protocole de distribution d'une clé
symétrique quantique (QKD)

Sécurité théorique parfaite

basée sur:

**La mesure
quantique**

Distribution de
la clé symétrique



<https://www.cqt.sg/groups/artur-ekert/>

Protocole E91

Créé par **Artur Ekert** en **1991**

Protocole de distribution d'une clé
symétrique quantique (QKD)

Sécurité théorique parfaite

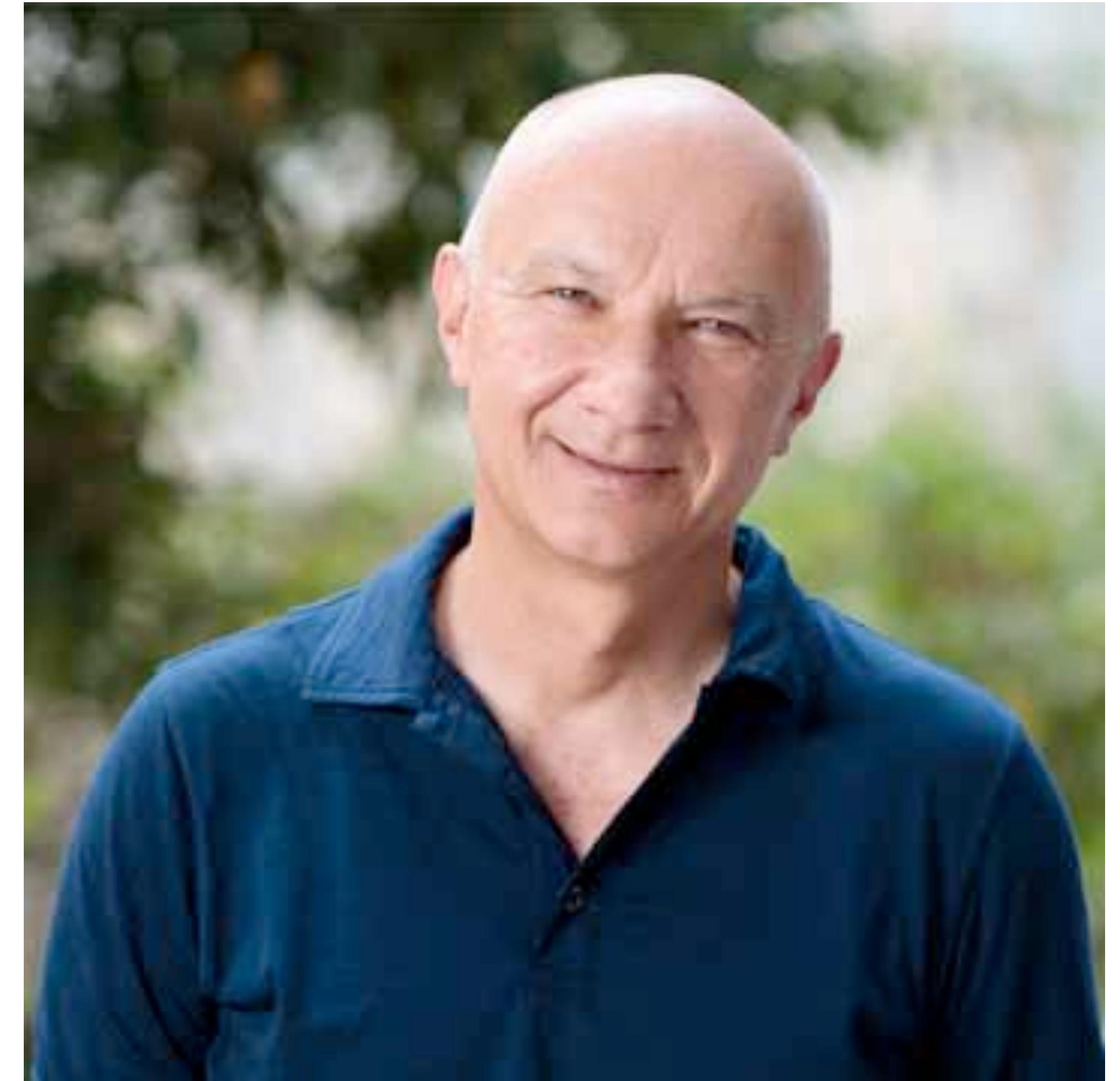
basée sur:

La mesure
quantique

Distribution de
la clé symétrique

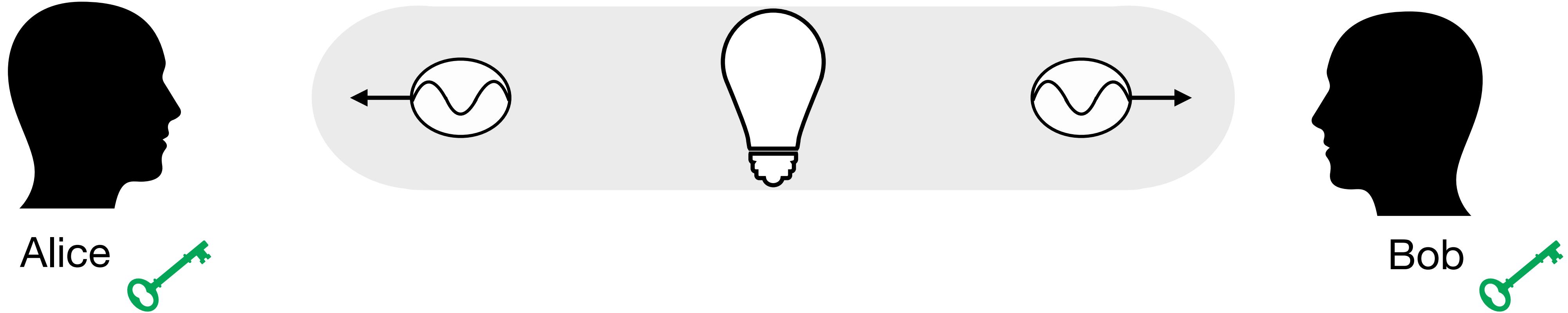
**L'intrication et
l'inégalité CHSH**

Détection
d'espions



<https://www.cqt.sg/groups/artur-ekert/>

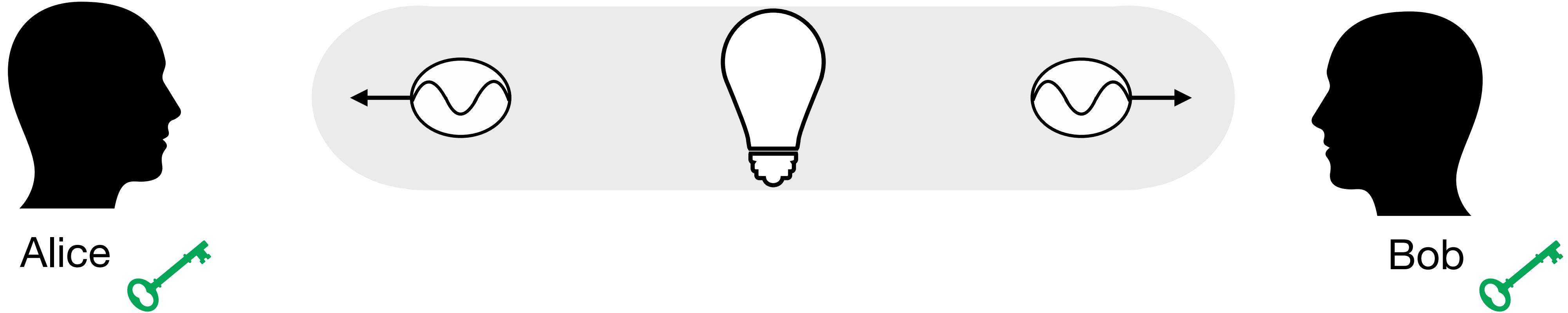
Étapes du protocole



But

Établir une clé symétrique secrète entre Alice et Bob

Étapes du protocole

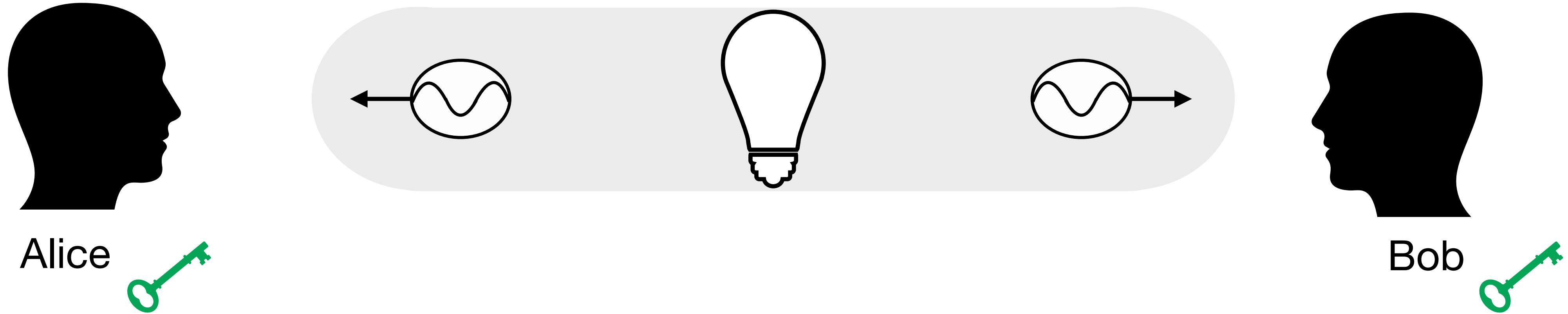


But

Établir une clé symétrique secrète entre Alice et Bob

1. Réception de photons intriqués

Étapes du protocole

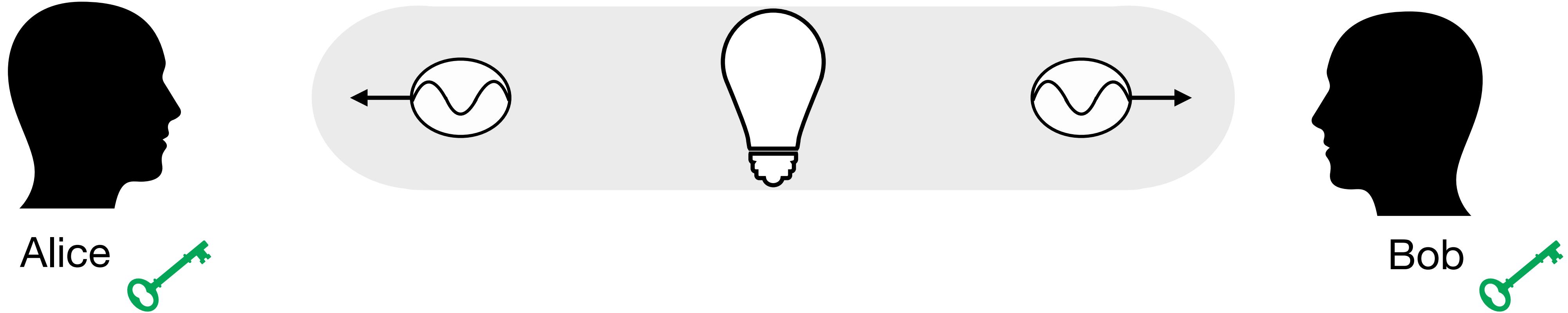


But

Établir une clé symétrique secrète entre Alice et Bob

1. Réception de photons intriqués
2. Annonce des bases de mesures

Étapes du protocole



But

Établir une clé symétrique secrète entre Alice et Bob

1. Réception de photons intriqués
2. Annonce des bases de mesures
3. Détection d'erreur et/ou d'espion

Étape 1: Réception des photons intriqués



Alice et Bob reçoivent chacun un photon d'une paire intriquée



Alice

$(0^\circ, 45^\circ, 90^\circ)$



Bob

$(45^\circ, 90^\circ, 135^\circ)$

Étape 1: Réception des photons intriqués

Alice et Bob reçoivent chacun un photon d'une paire intriquée



Alice

(0° , 45° , 90°)



Bob

(45° , 90° , 135°)

**Choix
aléatoire
d'une base**

0°

90°



Étape 1: Réception des photons intriqués

Alice et Bob reçoivent chacun un photon d'une paire intriquée



Alice

(0° , 45° , 90°)



Bob

(45° , 90° , 135°)

Choix
aléatoire
d'une base

0°

90°



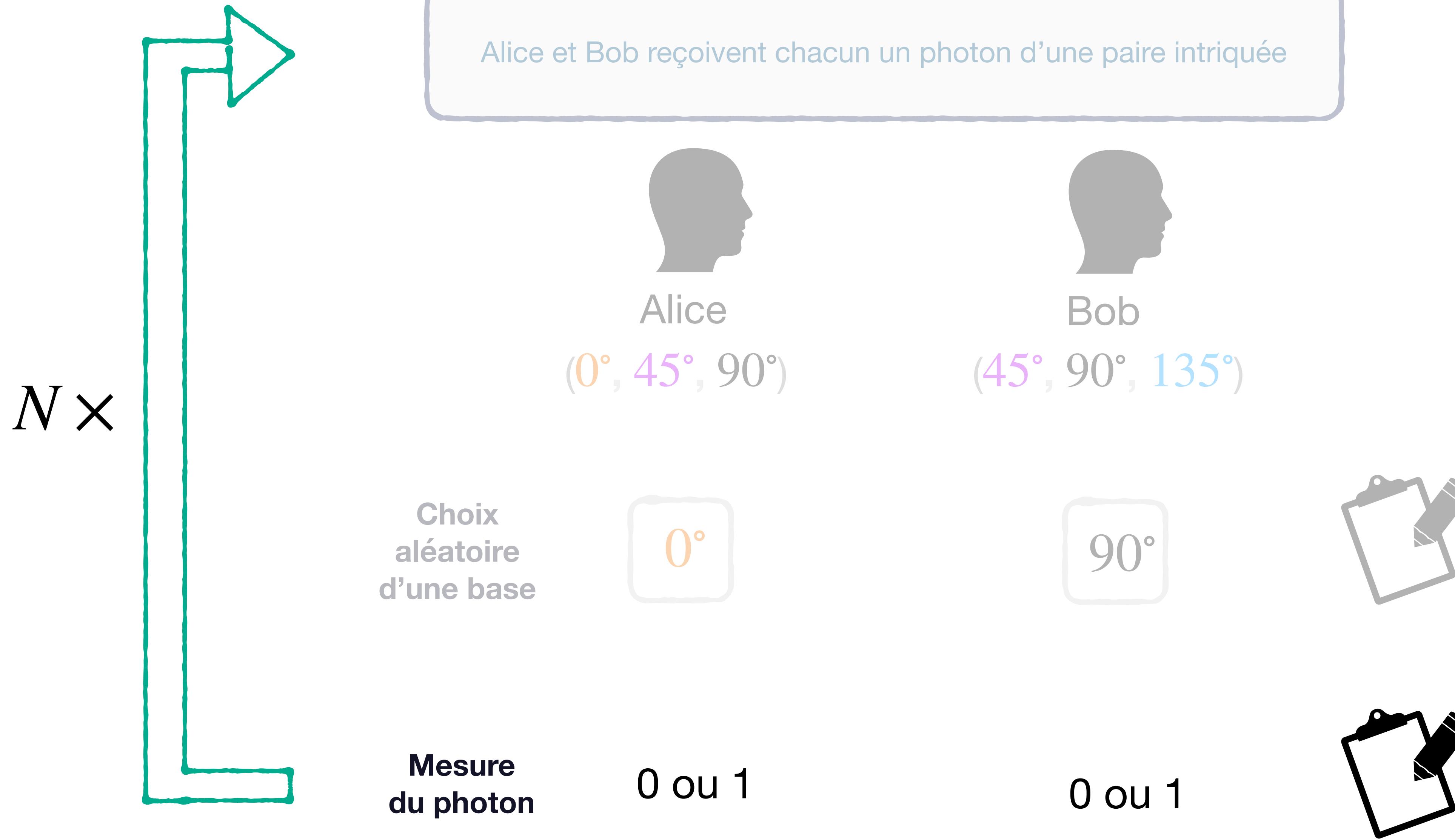
Mesure
du photon

0 ou 1

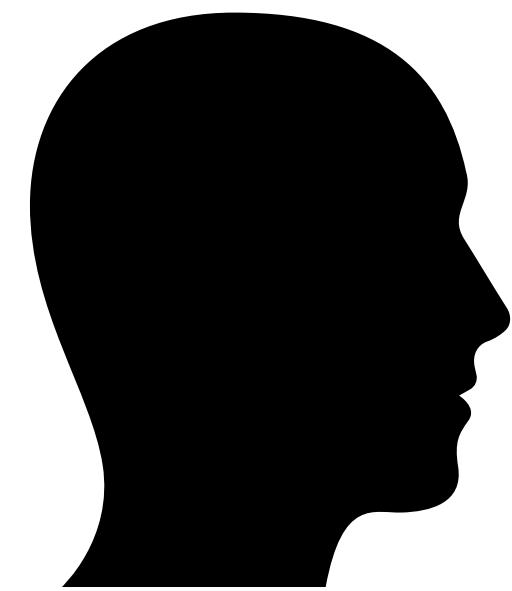
0 ou 1



Étape 1: Réception des photons intriqués

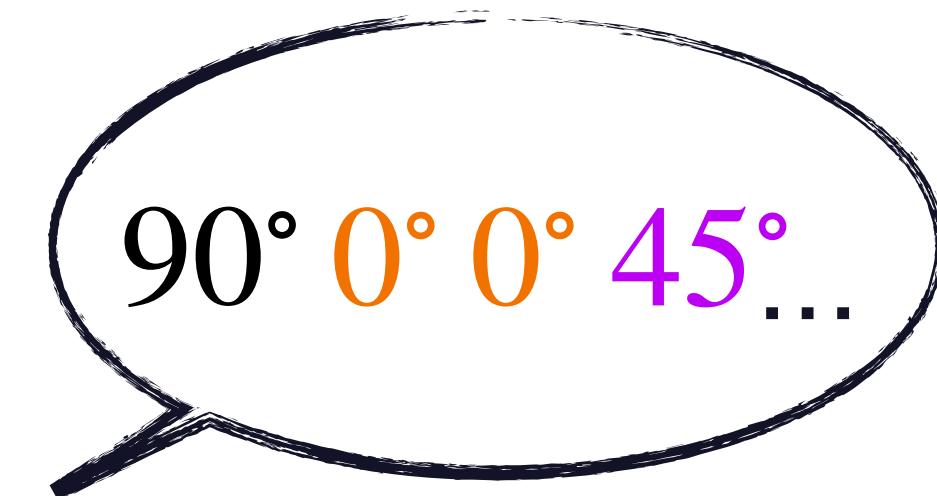


Étape 2: Annonce des bases



Alice

$(0^\circ, 45^\circ, 90^\circ)$

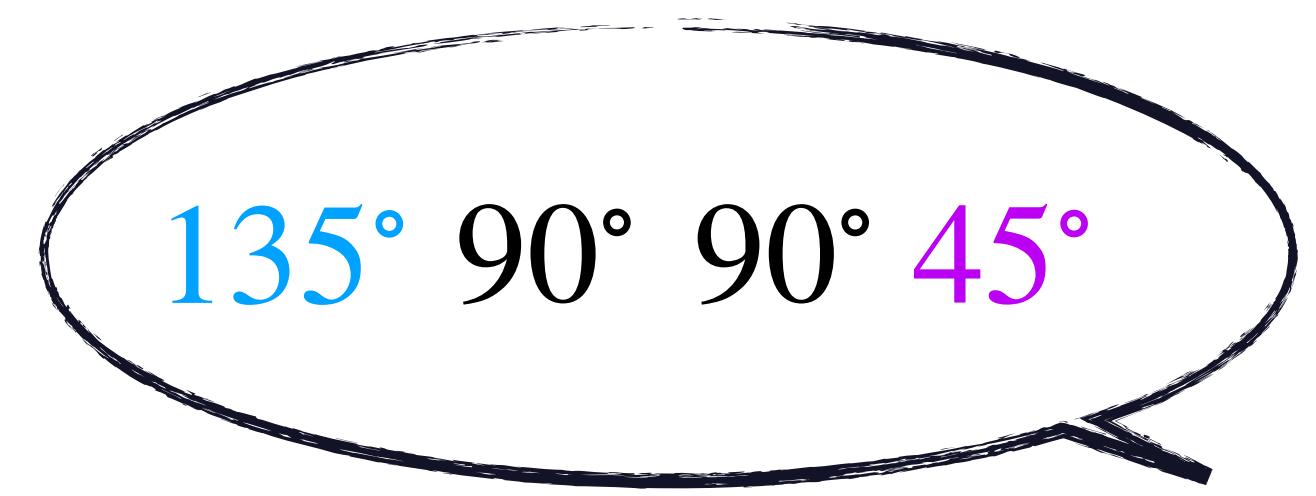


$90^\circ \text{ } 0^\circ \text{ } 0^\circ \text{ } 45^\circ \dots$



Bob

$(45^\circ, 90^\circ, 135^\circ)$



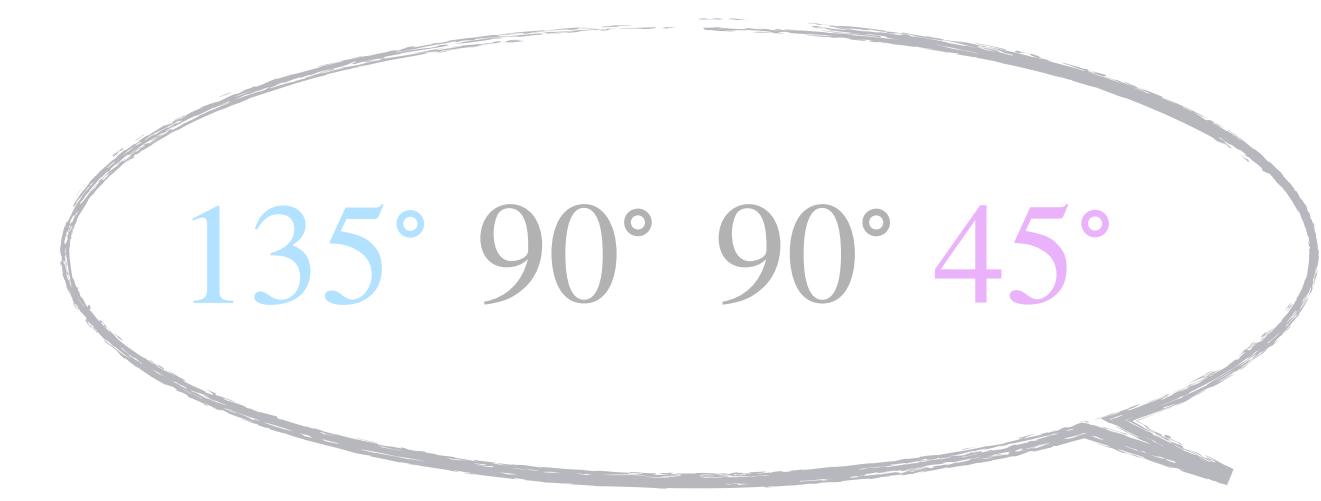
$135^\circ \text{ } 90^\circ \text{ } 90^\circ \text{ } 45^\circ$

Étape 2: Annonce des bases



Alice

$(0^\circ, 45^\circ, 90^\circ)$



Bob

$(45^\circ, 90^\circ, 135^\circ)$

9 combinaisons

$(0^\circ, 45^\circ)(0^\circ, 90^\circ)(0^\circ, 135^\circ)(45^\circ, 45^\circ)(45^\circ, 90^\circ)(45^\circ, 135^\circ)(90^\circ, 45^\circ)(90^\circ, 90^\circ)(90^\circ, 135^\circ)$

Étape 2: Annonce des bases



Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°



Étape 2: Annonce des bases

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Étape 2: Annonce des bases

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

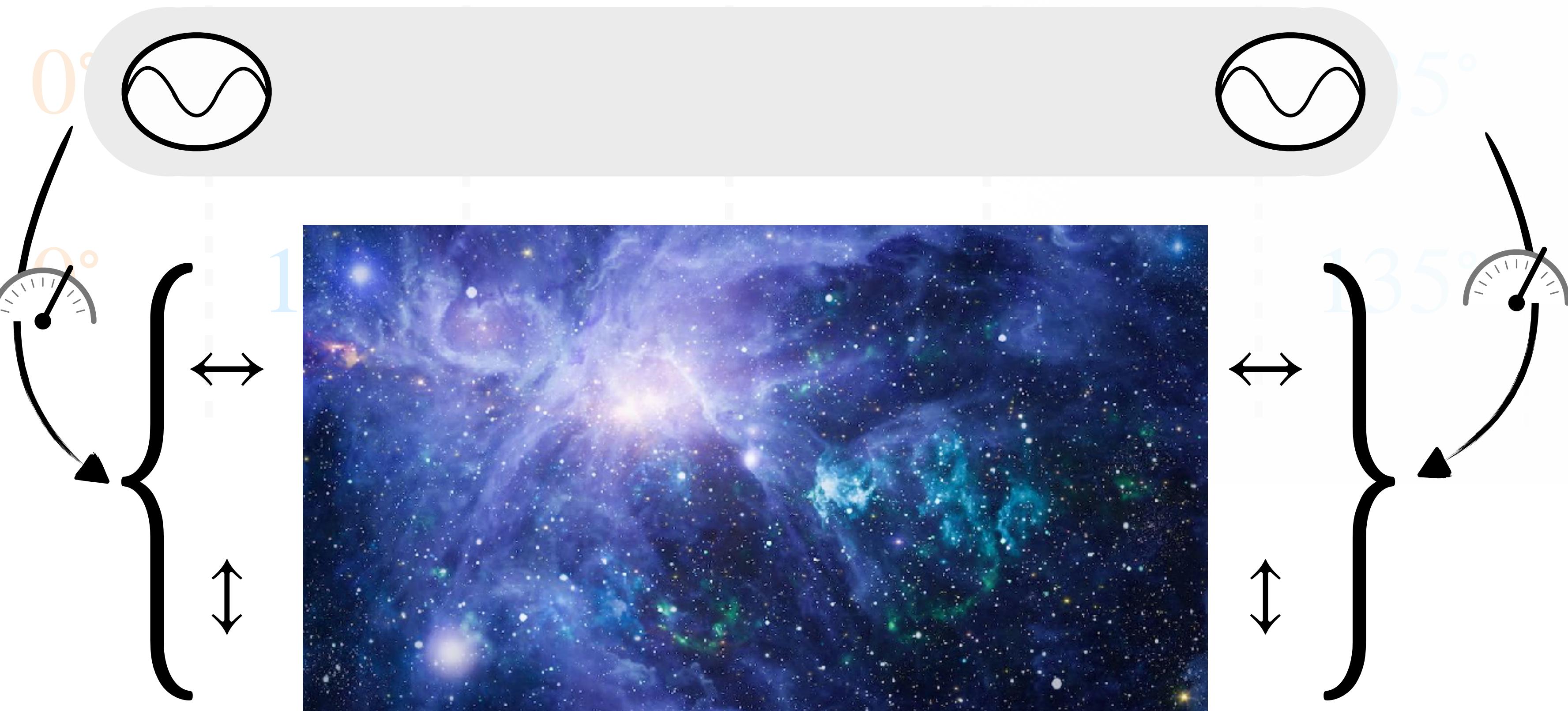
Création de la clé symétrique



	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°

Création de la clé symétrique

$$\frac{1}{\sqrt{2}} | \leftrightarrow \leftrightarrow \rangle + \frac{1}{\sqrt{2}} | \uparrow \downarrow \uparrow \downarrow \rangle$$



Création de la clé symétrique



	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°

Création de la clé symétrique



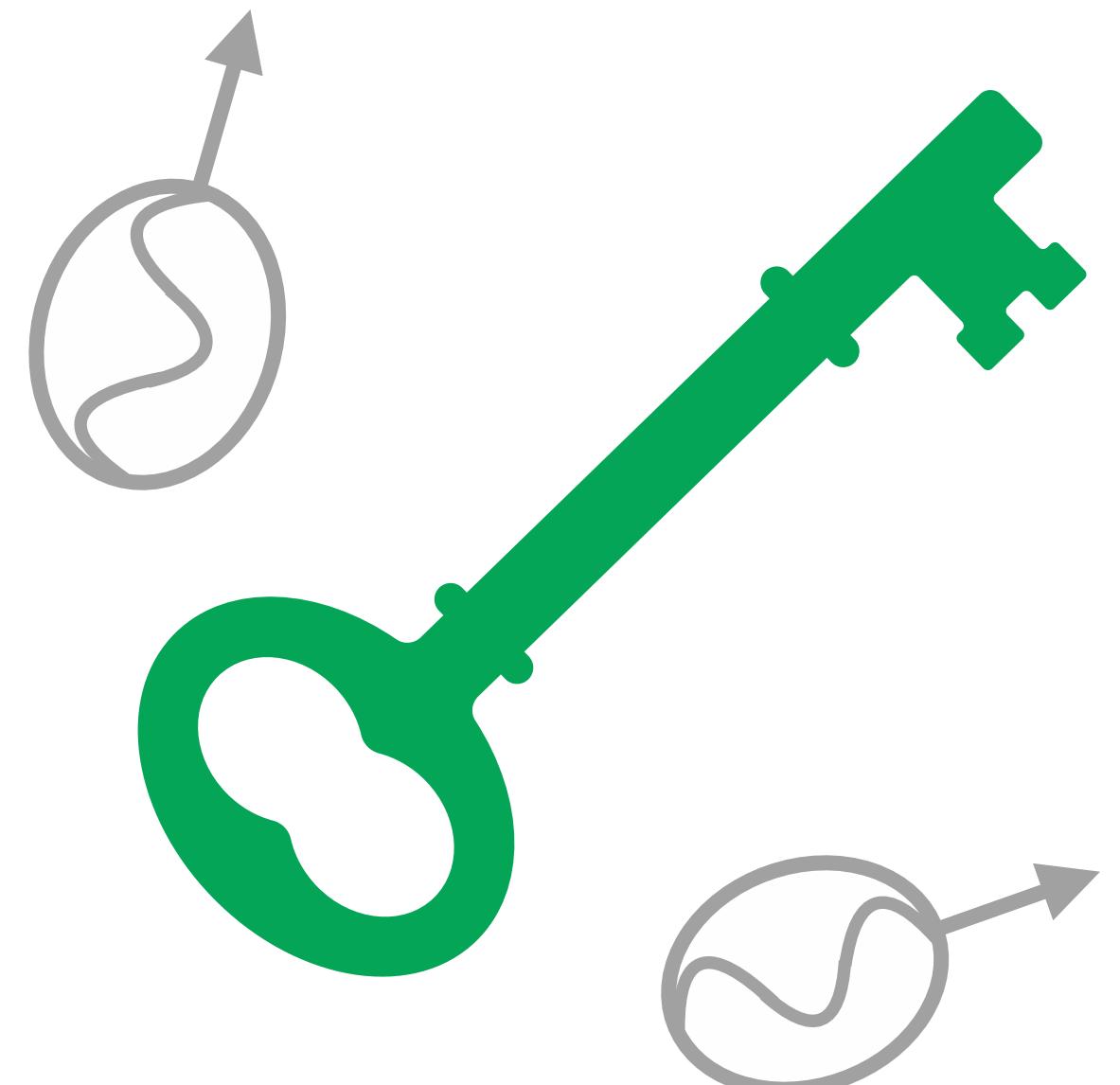
	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°
	1	1	0	0	1	0	0



Propriétés de la clé symétrique quantique

Binaire

Les résultats de mesure quantique sont étiquetés 0 ou 1.



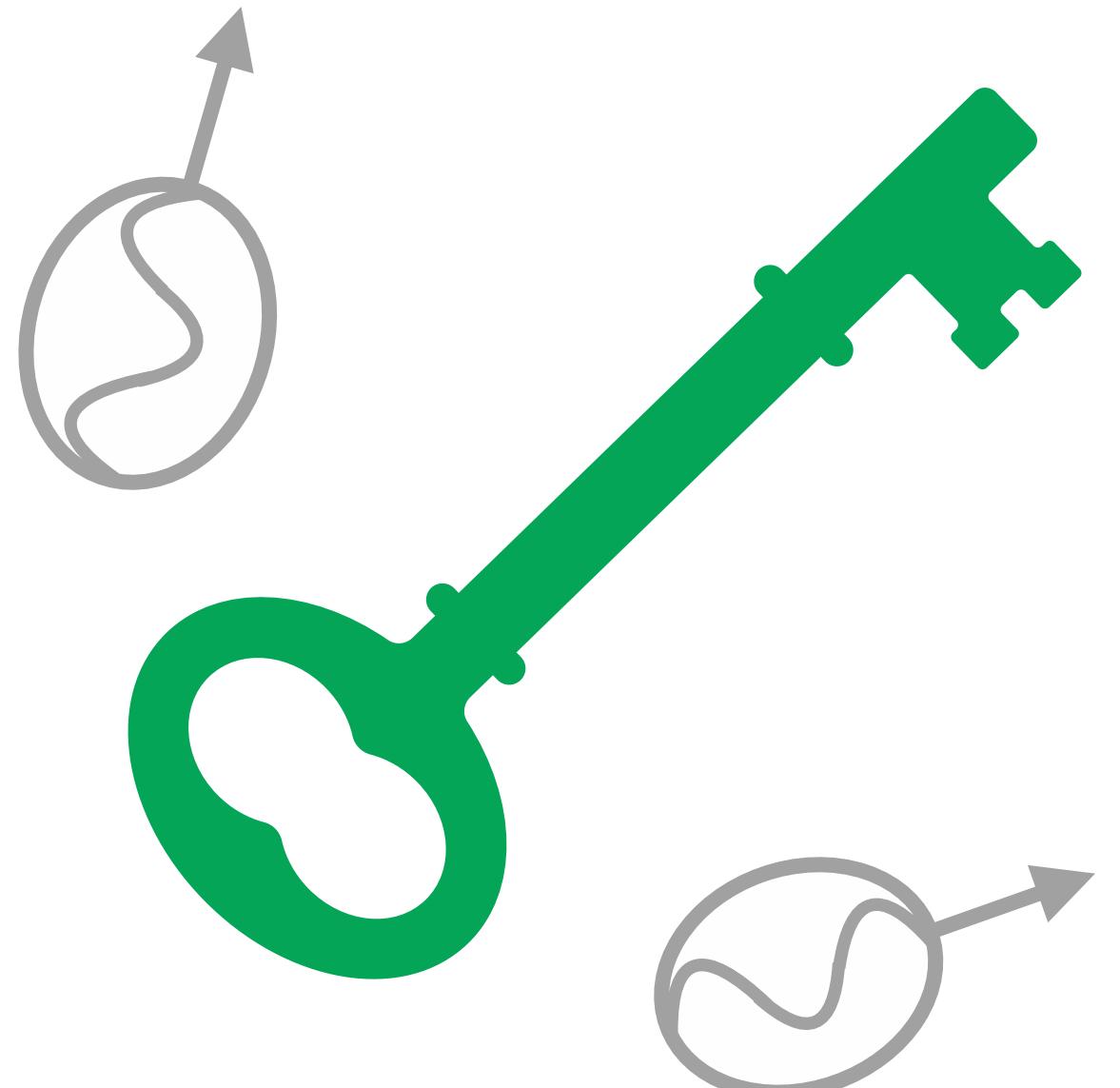
Propriétés de la clé symétrique quantique

Binaire

Les résultats de mesure quantique sont étiquetés 0 ou 1.

Identique

La mesure quantique des photons d'une paire intriquée dans la même base garantie la même mesure chez Alice et Bob.



Propriétés de la clé symétrique quantique



Binaire

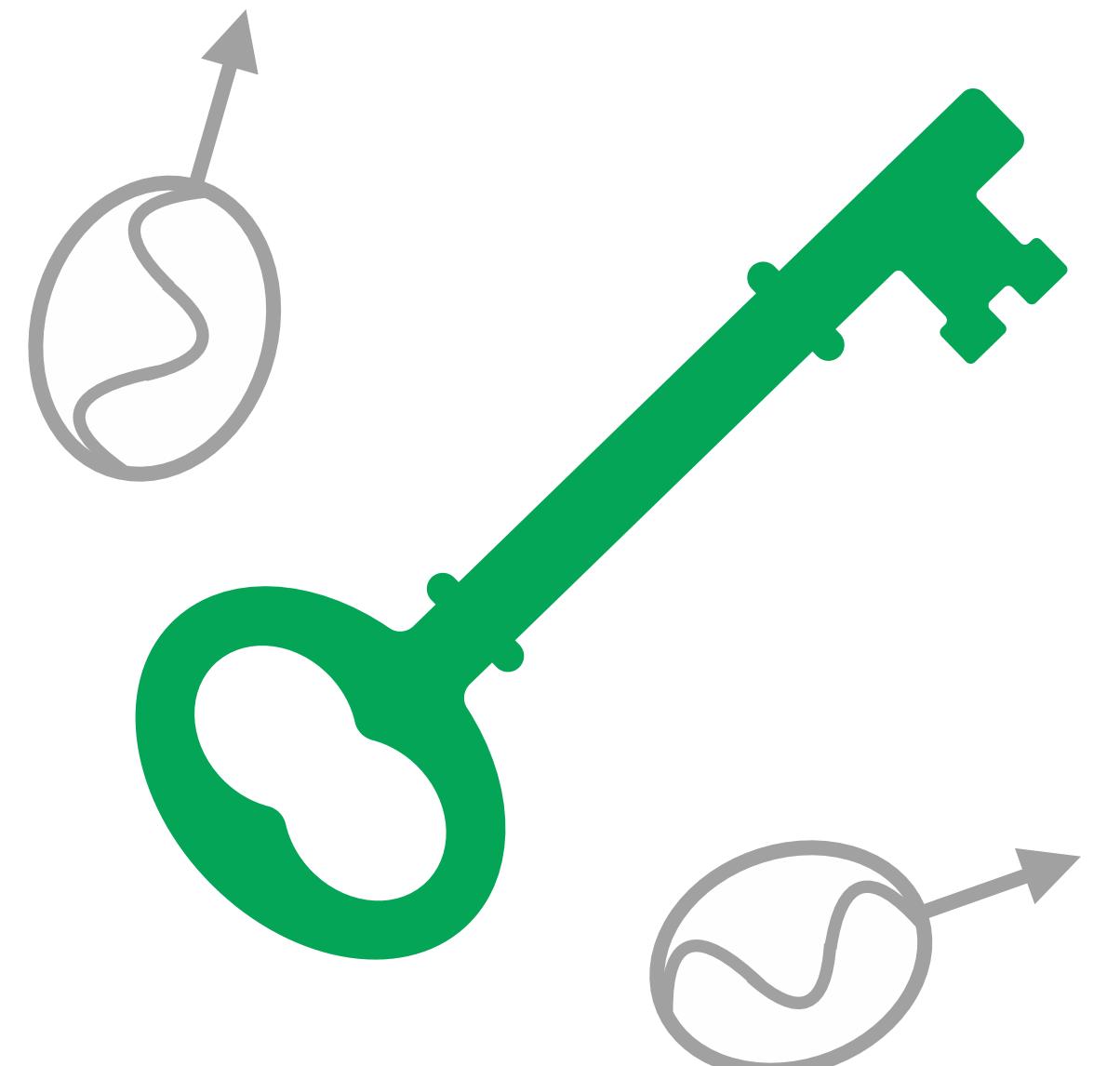
Les résultats de mesure quantique sont étiquetés 0 ou 1.

Identique

La mesure quantique des photons d'une paire intriquée dans la même base garantie la même mesure chez Alice et Bob.

Parfaitement aléatoire

La mesure quantique d'une paire intriquée garantie l'aléatoire.



Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Étape 3: Détection d'erreur et/ou d'espion

Création de la clé
symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°





Étape 3: Détection d'erreur et/ou d'espion

Combinaisons de bases utilisées: (0° , 45°) (0° , 135°) (90° , 45°) (90° , 135°)

Alice { 0° , 90° }

Bob { 45° , 135° }



Étape 3: Détection d'erreur et/ou d'espion

Combinaisons de bases utilisées: $(0^\circ, 45^\circ)$ $(0^\circ, 135^\circ)$ $(90^\circ, 45^\circ)$ $(90^\circ, 135^\circ)$

Alice $\{0^\circ, 90^\circ\}$ $\{a_1, a_2\}$

Bob $\{45^\circ, 135^\circ\}$ $\{b_1, b_2\}$



Étape 3: Détection d'erreur et/ou d'espion

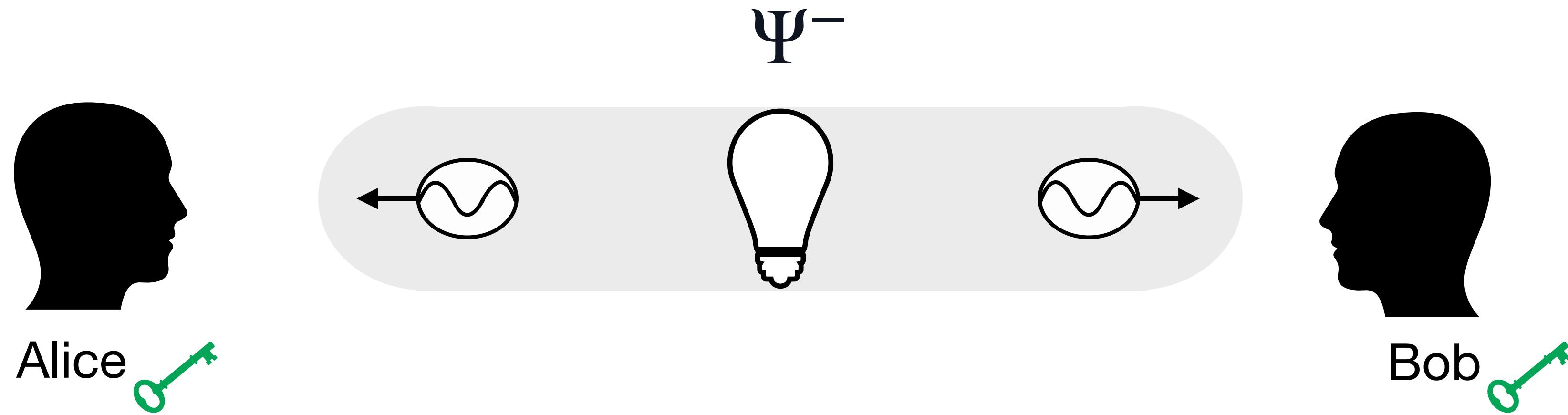
Combinaisons de bases utilisées: $(0^\circ, 45^\circ)$ $(0^\circ, 135^\circ)$ $(90^\circ, 45^\circ)$ $(90^\circ, 135^\circ)$

Alice $\{0^\circ, 90^\circ\}$ $\{a_1, a_2\}$

Bob $\{45^\circ, 135^\circ\}$ $\{b_1, b_2\}$

$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}| \begin{cases} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{cases}$$

Cas 1: Utilisation de paires de Bell



$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

Cas 2: Ève l'espionne écoute la conversation



Cas 2: Ève l'espionne écoute la conversation



Choix de base

45°

135°

90°

Cas 2: Ève l'espionne écoute la conversation



Choix de base

45°

Résultat de mesure

{0 ,1}

135°

{0 ,1}

90°

{0 ,1}

Cas 2: Ève l'espionne écoute la conversation



Choix de base

45°

Résultat de mesure

{0 ,1}

Encodage

{ $| \nwarrow \rangle \rightarrow$, $| \nearrow \rangle \rightarrow$ }

135°

{0 ,1}

{ $| \nwarrow \rangle \rightarrow$, $| \swarrow \rangle \rightarrow$ }

90°

{0 ,1}

{ $| \leftrightarrow \rangle \rightarrow$, $| \updownarrow \rangle \rightarrow$ }

Cas 2: Ève l'espionne écoute la conversation



$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

Cas 2: Ève l'espionne écoute la conversation



$$S = |E_{a_1, b_1} + E_{a_2, b_1} + E_{a_2, b_2} - E_{a_1, b_2}| \{ \begin{array}{l} \leq 2 \text{ Classique} \\ \in [2, 2\sqrt{2}] \text{ Maximum quantique} \end{array}$$

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°



Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

$$\frac{2}{9} \sim 22\% \text{ Cr{\'e}ation de cl{\'e}}$$

D{\'e}tection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°



Enjeux

Longueur de la cl{\'e}

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

$$\frac{2}{9} \sim 22\% \text{ Cr{e}ation de cl{e}}$$

$$\frac{4}{9} \sim 45\% \text{ D{e}tection d'espion}$$

D{e}tection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°



Enjeux

Longueur de la cl{e}

S{e}curit{e} de la cl{e}

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

$\frac{2}{9}$ ~ 22% Crédit de clé

$\frac{4}{9}$ ~ 45% Détection d'espion

$\frac{3}{9}$ ~ 33% Poubelle

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°



Enjeux

Longueur de la clé

Sécurité de la clé

Plan

- ✓ Présentation
- ✓ Cryptographie
- ✓ Le qubit
- ✓ Le photon: messager d'information quantique
- ✓ Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- ✓ Présentation
- ✓ Cryptographie
- ✓ Le qubit
- ✓ Le photon: messager d'information quantique
- ✓ Intrication et inégalité CHSH
- ✓ Protocole E91
- Atelier pratique

Plan

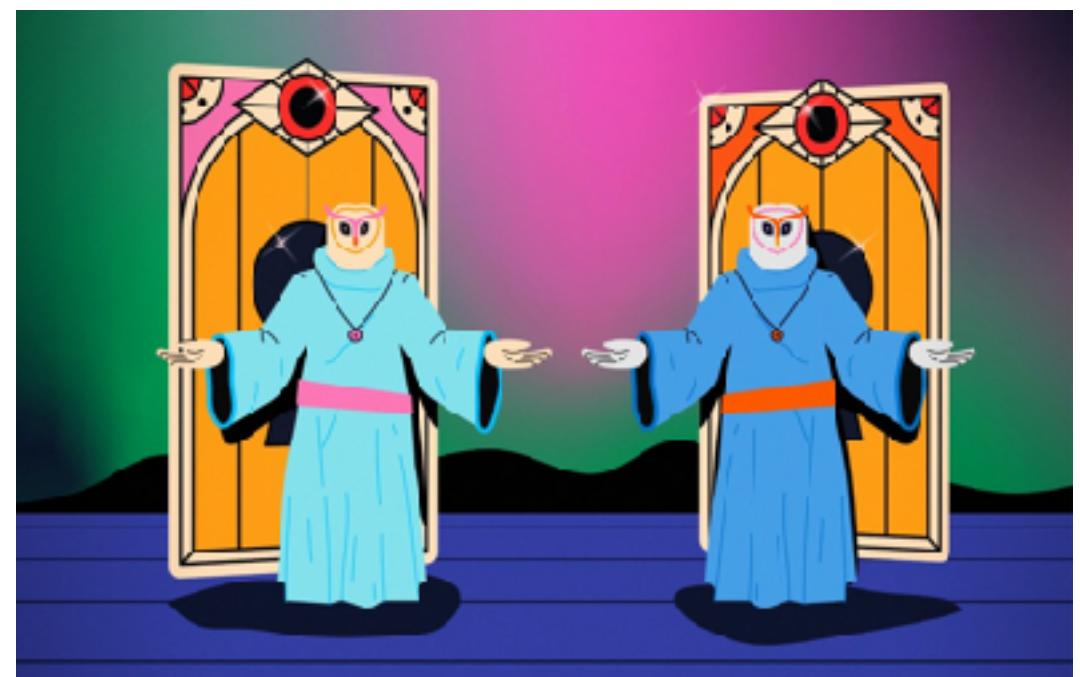
- ✓ Présentation
- ✓ Cryptographie
- ✓ Le qubit
- ✓ Le photon: messager d'information quantique
- ✓ Intrication et inégalité CHSH
- ✓ Protocole E91
- Atelier pratique

Partie pratique

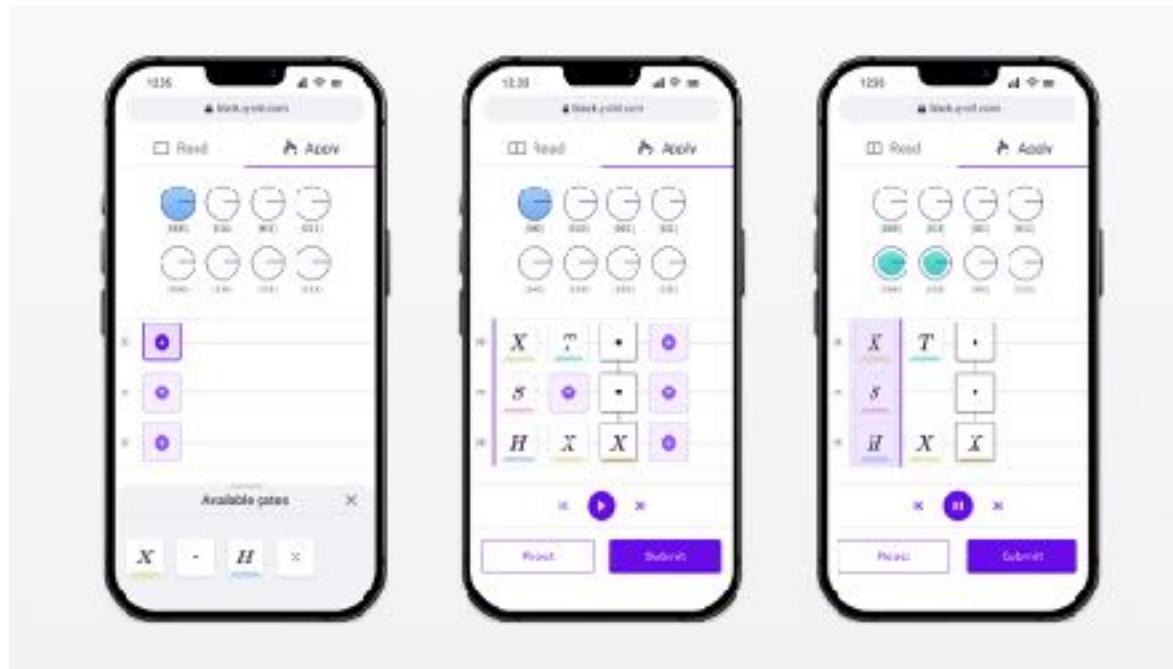
<https://github.com/algolab-quantique/CMAI-E91-Students.git>

Conclusion

Références à consulter



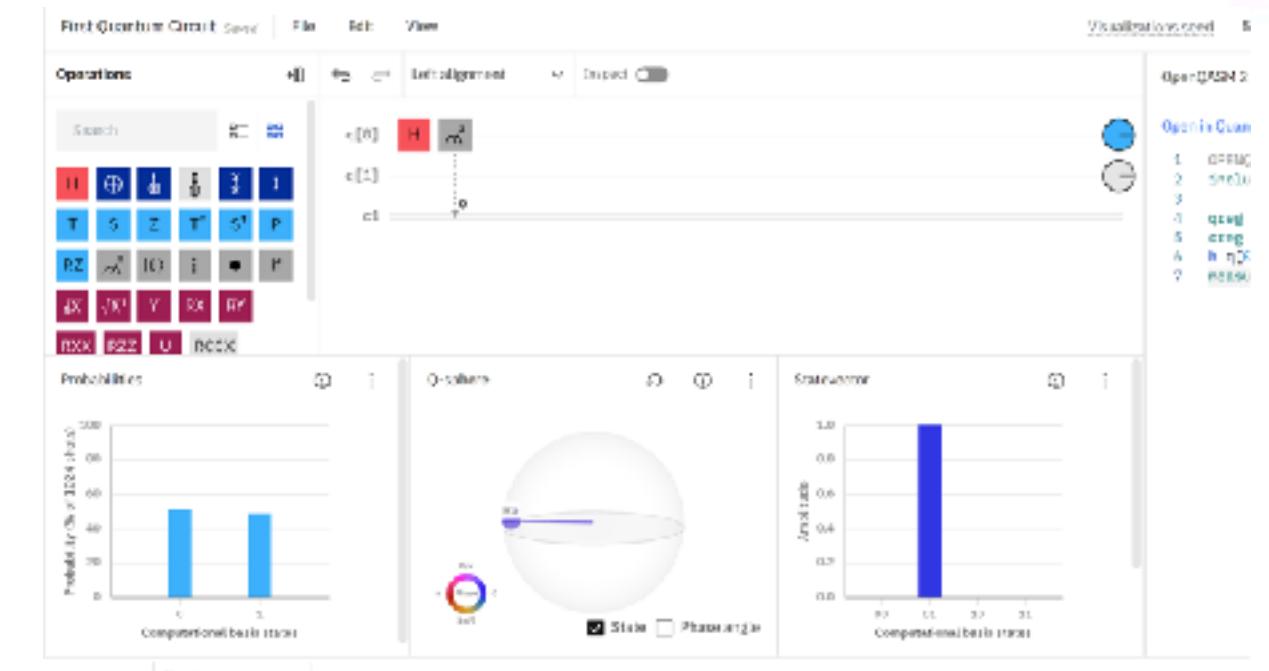
Les Énigmes quantiques ([lien](#))



Black Opal de Q-CTRL ([lien](#))



SkillsBuild ([lien](#))



IBM Quantum learning ([lien](#))



Azure Quantum katas ([lien](#))



Inscription à l'infolettre

Lien du devoir



<https://forms.office.com/r/LshFpNT8nE?origin=lprLink>

Vous avez 24 heures pour compléter le devoir

