

A photograph of a Foucault pendulum in a museum. The pendulum consists of a large, dark, spherical bob suspended from a high ceiling by a thin wire. The bob is positioned in the center of a circular platform. The platform is surrounded by a series of parallel, light-colored wooden or metal bars that form a spiral pattern, likely representing the path of the pendulum's swing. The background shows a large window with a view of a cityscape. The text "Fizyka dla wszystkich" is overlaid in a bold, yellow font across the center of the image.

Fizyka dla wszystkich

Wykład popularny
dla młodzieży szkół średnich

Splątane kubity

czyli
rzecz o informatyce kwantowej

Ryszard Tanaś

<http://zon8.physd.amu.edu.pl/~tanas>

21 kwietnia 2004

Spis treści

1	Rozwój komputerów	6
1.1	Początki	6
1.2	Obwody scalone — miniaturyzacja	7
1.3	„Prawo Moore'a”	7
1.4	Zasada Landauera	11
2	Od bitu do kubit	13
2.1	Superpozycja	13
2.2	Sfera Blocha	25
2.3	Algebra kubitów w pigułce	35
3	Ewolucja kubitów	37
3.1	Pomiar kwantowy	37

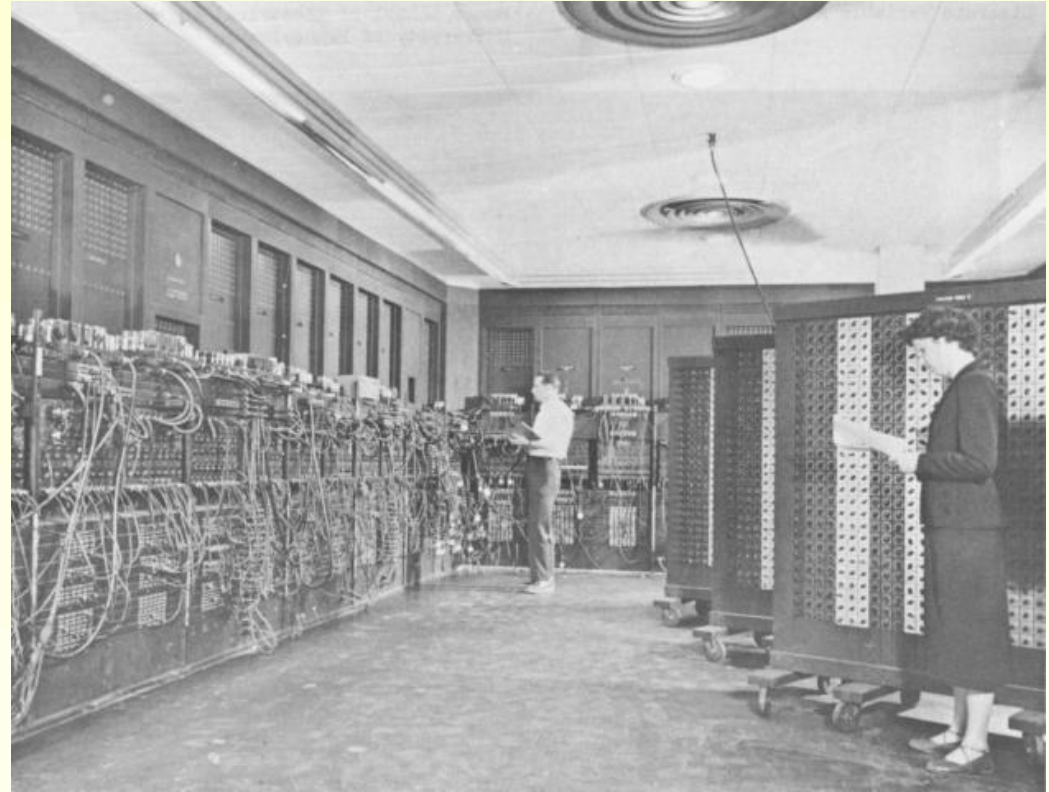
3.2	Reguła Feynmana	53
3.3	Kwantowe, czyli nielogiczne bramki lo- giczne	77
3.4	Zakaz klonowania	91
4	Rejestry kwantowe	93
4.1	Dwa kubity	93
4.2	Kwantowy paralelizm	95
4.3	Splątane kubity	96
4.4	Stany Bella	98
5	Kwantowe przesyłanie informacji	108
5.1	Gęste kodowanie	108
5.2	Teleportacja kwantowa	119

1 Rozwój komputerów

1.1 Początki

ENIAC, luty 1946

(Electronic Numerical
Integrator and Computer)
17468 lamp elektronowych
5000 dodawań/s
357 mnożeń/s
175 kW energii



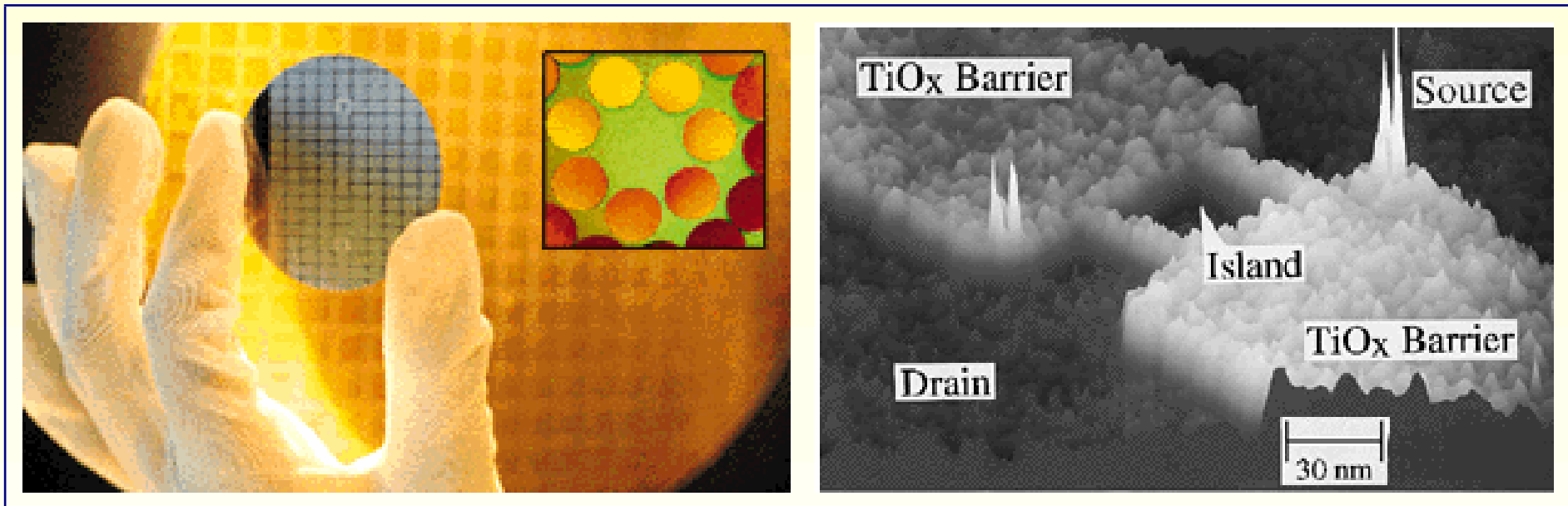
1.2 Obwody scalone — miniaturyzacja

Komputery stają się coraz

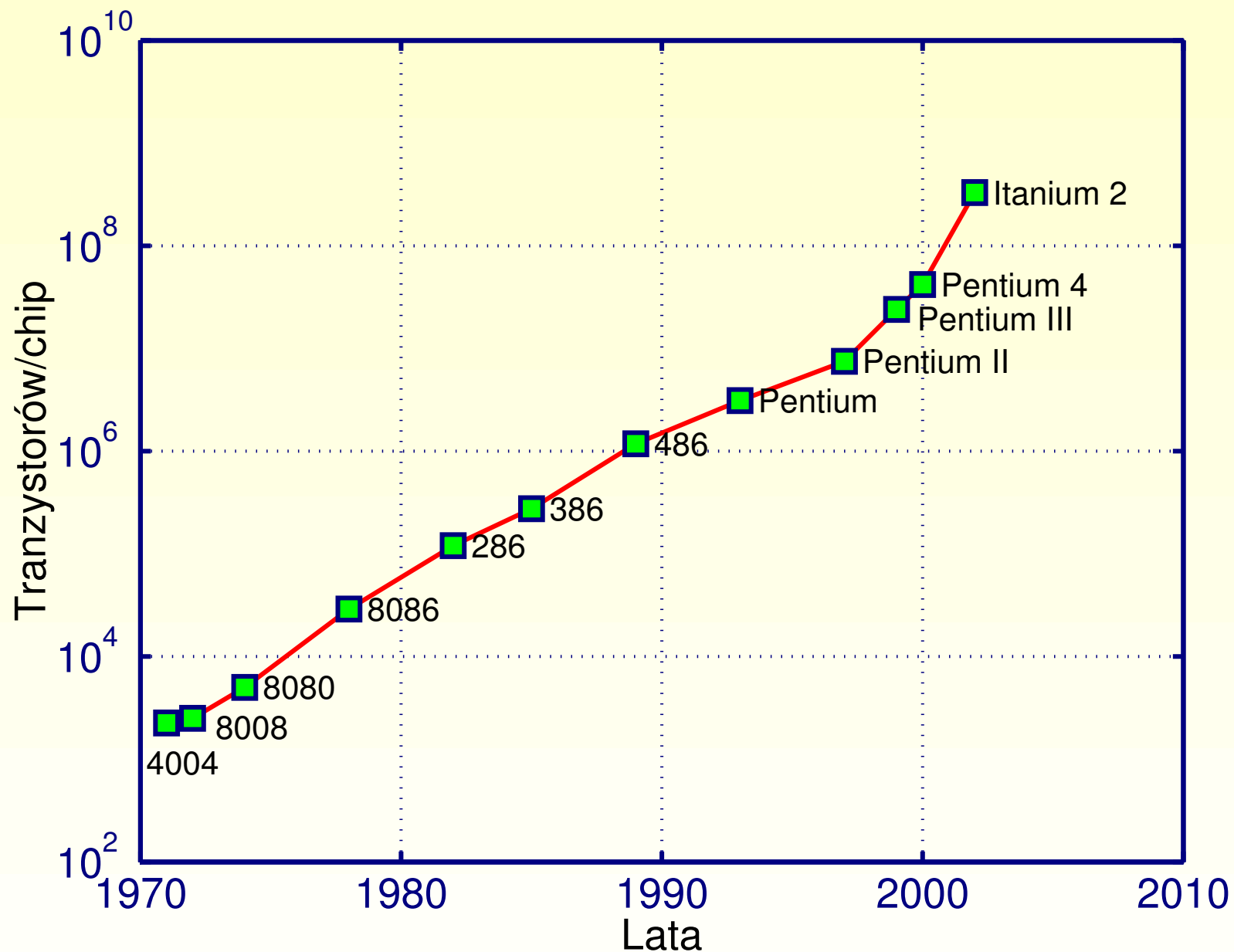
mniejsze

szybsze

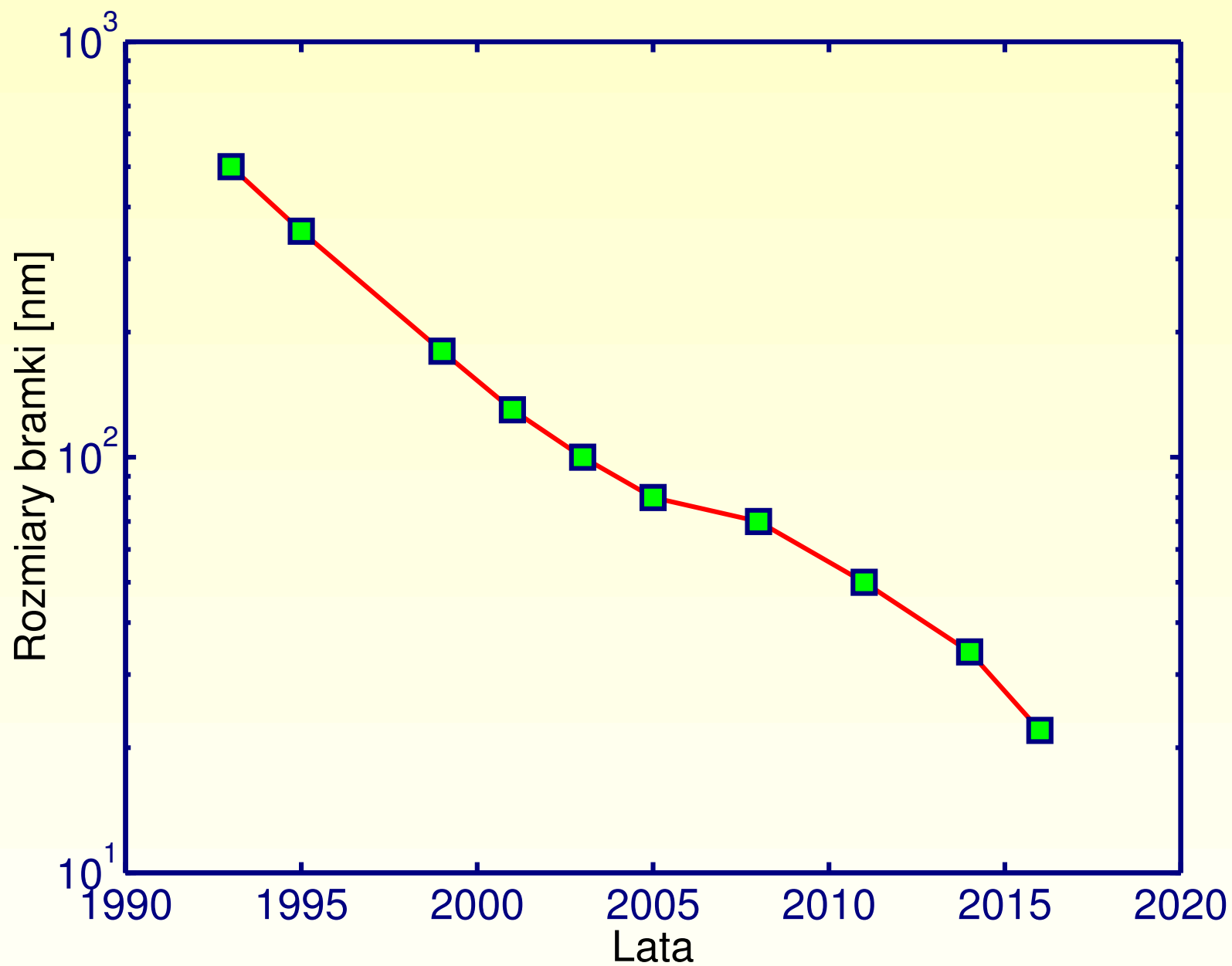
tańsze



1.3 „Prawo Moore'a”



Rozwój układów scalonych (Intel)



Rozmiary elementów obwodu scalonego
(SIA Roadmap 2000/2001)

**Jak długo „prawo Moore'a” będzie jeszcze
obowiązywać?**

Jak długo „prawo Moore’a” będzie jeszcze obowiązywać?

Obecna technologia to $90\text{ nm} = 0.09\text{ }\mu\text{m}$

Już obecnie na jedną bramkę logiczną potrzeba mniej niż 1000 elektronów.

Jak długo „prawo Moore’a” będzie jeszcze obowiązywać?

Obecna technologia to $90\text{ nm} = 0.09\ \mu\text{m}$

Już obecnie na jedną bramkę logiczną potrzeba mniej niż 1000 elektronów.

Czy istnieją fizyczne granice miniaturyzacji?

Jak długo „prawo Moore’a” będzie jeszcze obowiązywać?

Obecna technologia to $90\text{ nm} = 0.09\text{ }\mu\text{m}$

Już obecnie na jedną bramkę logiczną potrzeba mniej niż 1000 elektronów.

Czy istnieją fizyczne granice miniaturyzacji?

Przewiduje się, że około roku 2020 technologia zejdzie do rozmiarów, przy których niezbędne jest uwzględnienie praw fizyki obowiązujących w mikroświecie, czyli mechaniki kwantowej.



Earth Simulator

marzec 2002, Yokohama

5120 procesorów, $0.15\mu m$

500 MHz NEC

640 węzłów po 8 CPU

40 TFLOPS, tera = 10^{12}

wysokość szafy $2m$

miniaturyzacja?

1.4 Zasada Landauera



Rolf Landauer (1927-1999)

Wymazanie jednego bitu informacji wymaga straty energii (wydzielenia ciepła) o wartości co najmniej $kT \ln 2$

Informacja jest wielkością fizyczną!

2 Od bitu do kubit

2.1 Superpozycja

Klasyczny bit może przyjmować tylko dwie wartości $\{0, 1\}$ ($\{\text{orzeł}, \text{reszka}\}$, $\{\text{TAK}, \text{NIE}\}$).

2 Od bitu do kubit

2.1 Superpozycja

Klasyczny bit może przyjmować tylko dwie wartości $\{0, 1\}$ ($\{\text{orzeł}, \text{reszka}\}$, $\{\text{TAK}, \text{NIE}\}$).

Układ fizyczny reprezentujący bit znajduje się w jednym z dwóch możliwych stanów: albo w stanie 0 (orzeł, TAK) albo w stanie 1 (reszka, NIE).

2 Od bitu do kubit

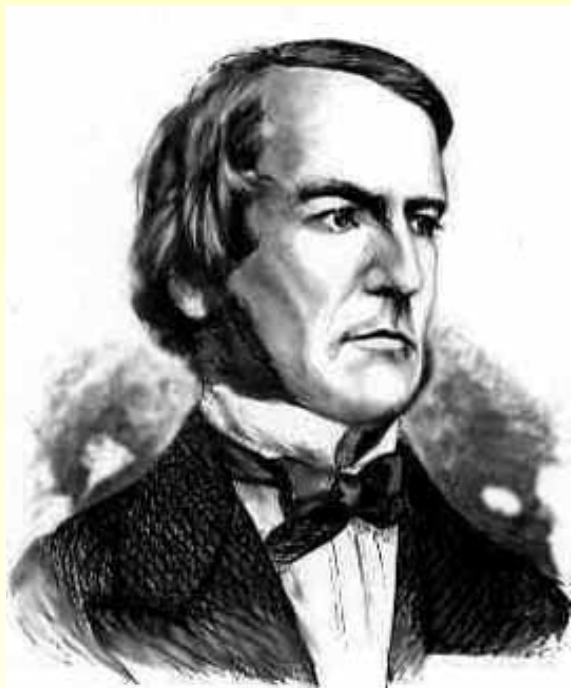
2.1 Superpozycja

Klasyczny bit może przyjmować tylko dwie wartości $\{0, 1\}$ ($\{\text{orzeł}, \text{reszka}\}$, $\{\text{TAK}, \text{NIE}\}$).

Układ fizyczny reprezentujący bit znajduje się w jednym z dwóch możliwych stanów: albo w stanie 0 (orzeł, TAK) albo w stanie 1 (reszka, NIE).

Dowolną informację można zapisać w postaci ciągu bitów, np.

bit = 011000100110100101110100



George Boole (1815-1864)

pokazał, że logikę i matematykę można sprowadzić do ciągu odpowiedzi: **TAK, NIE**



Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:

Kwantowym odpowiednikiem klasycznego bitu jest
dowolny układ dwustanowy:
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$,

Kwantowym odpowiednikiem klasycznego bitu jest
dowolny układ dwustanowy:
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$,
spin elektronu $\{|\uparrow\rangle, |\downarrow\rangle\}$,

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$,
spin elektronu $\{|\uparrow\rangle, |\downarrow\rangle\}$,
foton o dwóch wzajemnie ortogonalnych stanach polaryzacji $\{|\uparrow\rangle, |\rightarrow\rangle\}$,

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$,
spin elektronu $\{|\uparrow\rangle, |\downarrow\rangle\}$,
foton o dwóch wzajemnie ortogonalnych stanach polaryzacji $\{|\uparrow\rangle, |\rightarrow\rangle\}$,
itp.

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$,
spin elektronu $\{|\uparrow\rangle, |\downarrow\rangle\}$,
foton o dwóch wzajemnie ortogonalnych stanach polaryzacji $\{|\uparrow\rangle, |\rightarrow\rangle\}$,
itp.

Taki układ to qubit (quantum bit); po polsku kubit.

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$,
spin elektronu $\{|\uparrow\rangle, |\downarrow\rangle\}$,
foton o dwóch wzajemnie ortogonalnych stanach polaryzacji $\{|\uparrow\rangle, |\rightarrow\rangle\}$,
itp.

Taki układ to qubit (quantum bit); po polsku kubit.

Dwa stany układu, które możemy nazwać $|0\rangle$ i $|1\rangle$, przez analogię do klasycznego bitu, $\{0, 1\}$, tworzą bazę standardową albo obliczeniową — $\{|0\rangle, |1\rangle\}$.

Kubit to jednak nie klasyczny bit, dla podkreślenia tego faktu stosujemy specjalny, wprowadzony przez Diraca, zapis dla określenia kubitów, $|?\rangle$.

Kubit to jednak nie klasyczny bit, dla podkreślenia tego faktu stosujemy specjalny, wprowadzony przez Diraca, zapis dla określenia kubitów, $|\psi\rangle$.

Kubit, w przeciwieństwie do klasycznego bitu, może być dowolną superpozycją stanów bazowych!

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

Kubit to jednak nie klasyczny bit, dla podkreślenia tego faktu stosujemy specjalny, wprowadzony przez Diraca, zapis dla określenia kubitów, $|?\rangle$.

Kubit, w przeciwieństwie do klasycznego bitu, może być dowolną superpozycją stanów bazowych!

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

Kubit reprezentuje obydwa stany:

stan $|0\rangle$ z amplitudą A_0

stan $|1\rangle$ z amplitudą A_1

Kubit to jednak nie klasyczny bit, dla podkreślenia tego faktu stosujemy specjalny, wprowadzony przez Diraca, zapis dla określenia kubitów, $|\psi\rangle$.

Kubit, w przeciwieństwie do klasycznego bitu, może być dowolną superpozycją stanów bazowych!

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

Kubit reprezentuje obydwa stany:

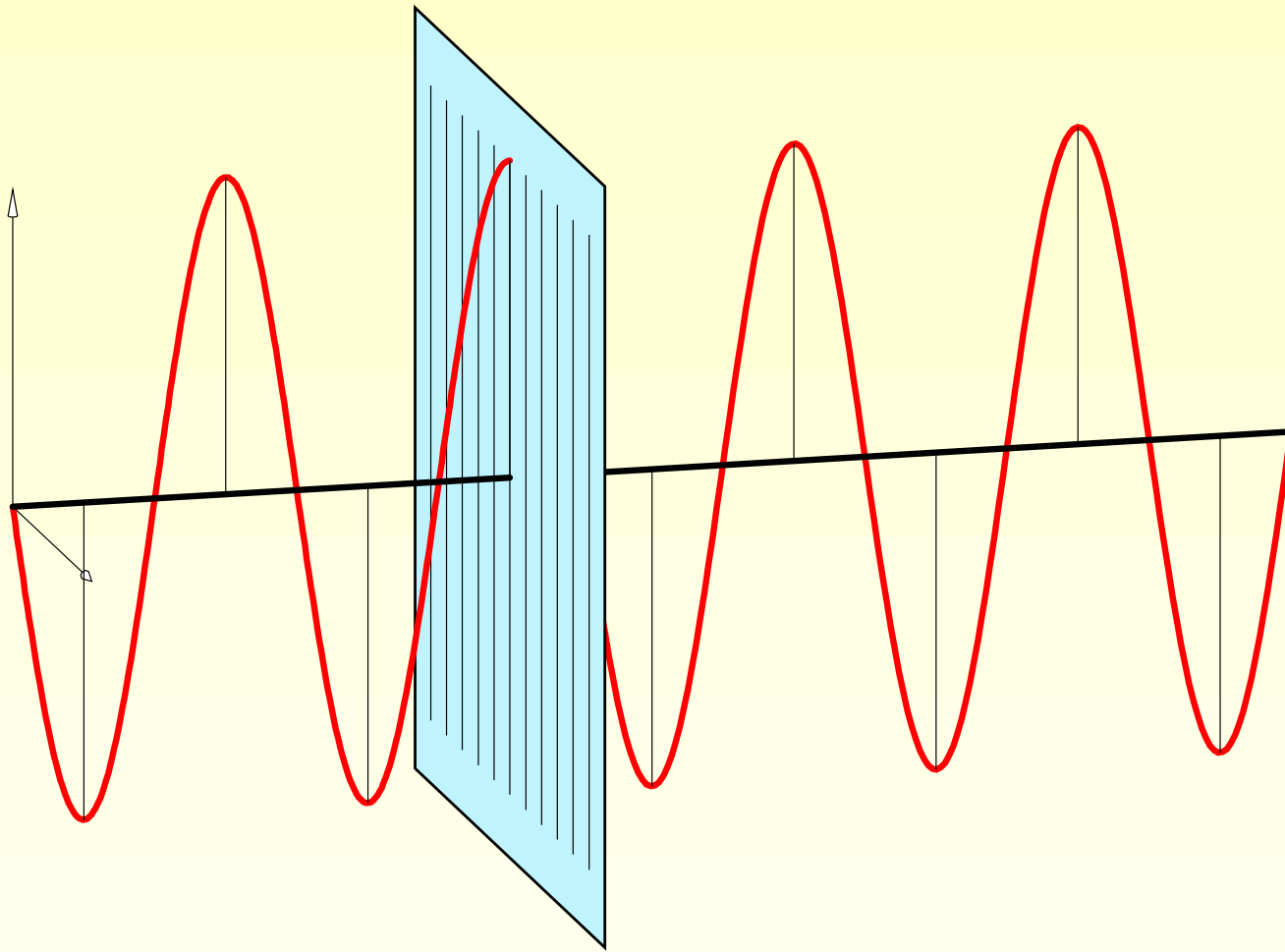
stan $|0\rangle$ z amplitudą A_0

stan $|1\rangle$ z amplitudą A_1

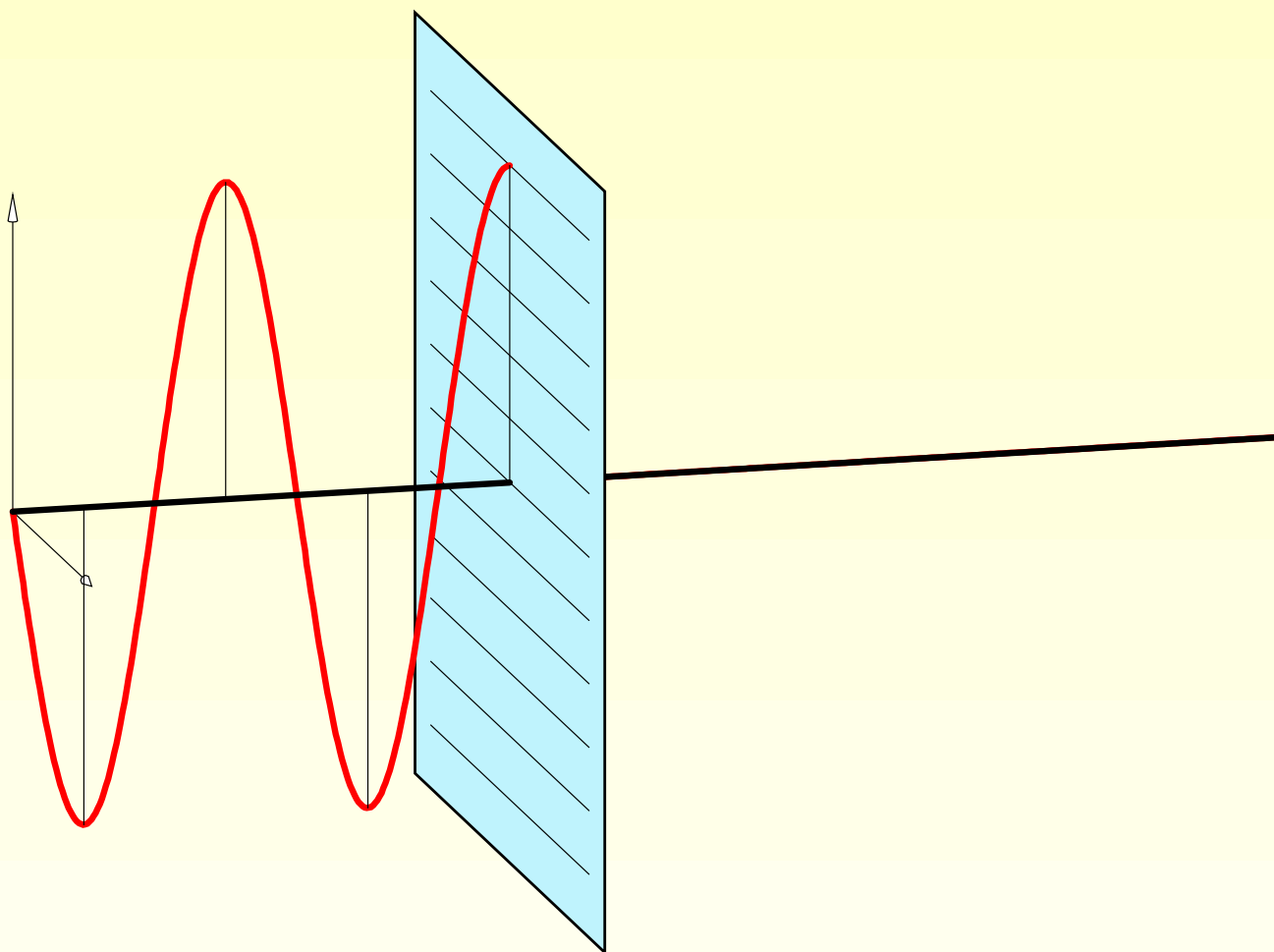
Pomiar w bazie $\{|0\rangle, |1\rangle\}$ daje:

stan $|0\rangle$ z prawdopodobieństwem $|A_0|^2$

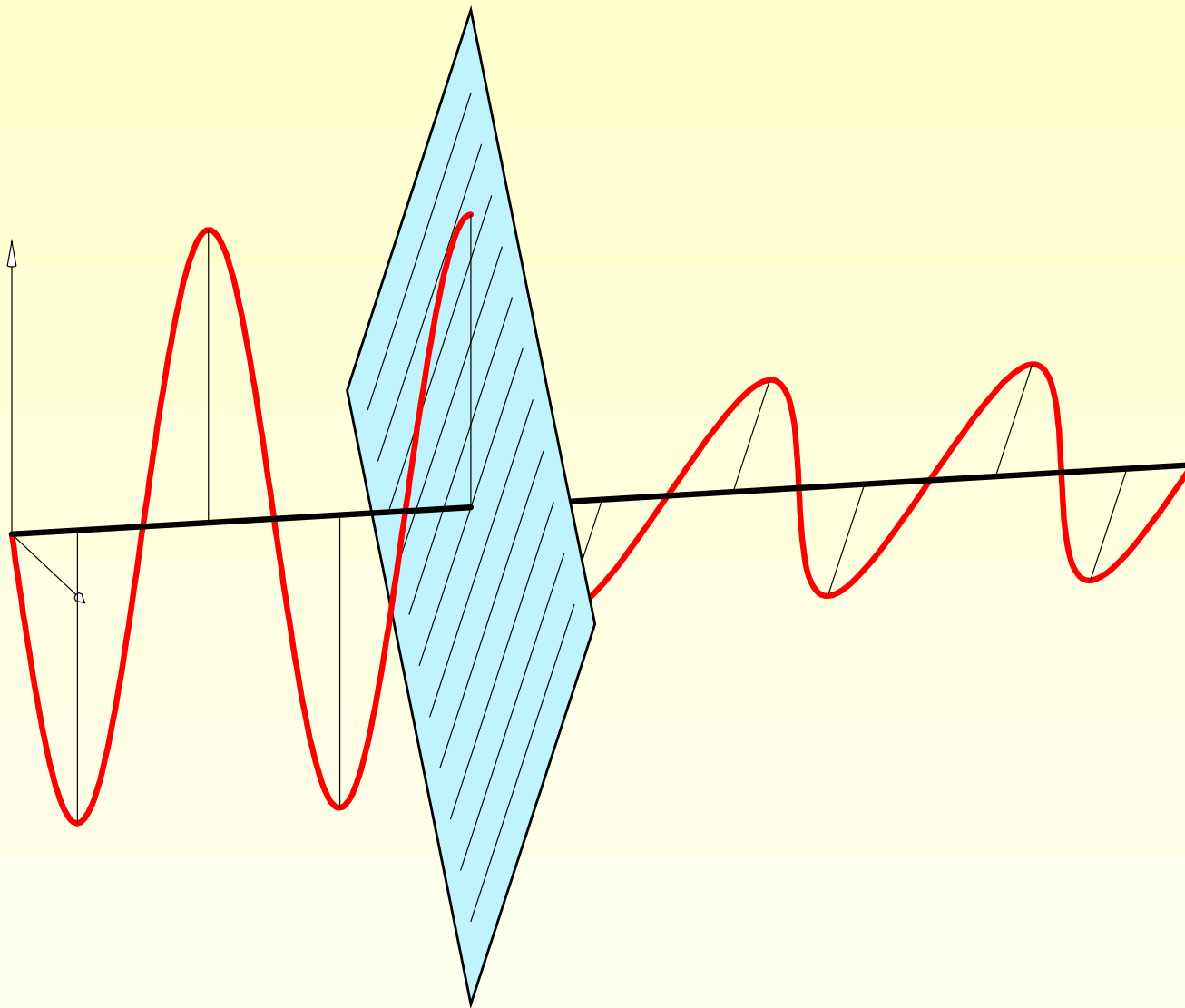
stan $|1\rangle$ z prawdopodobieństwem $|A_1|^2$



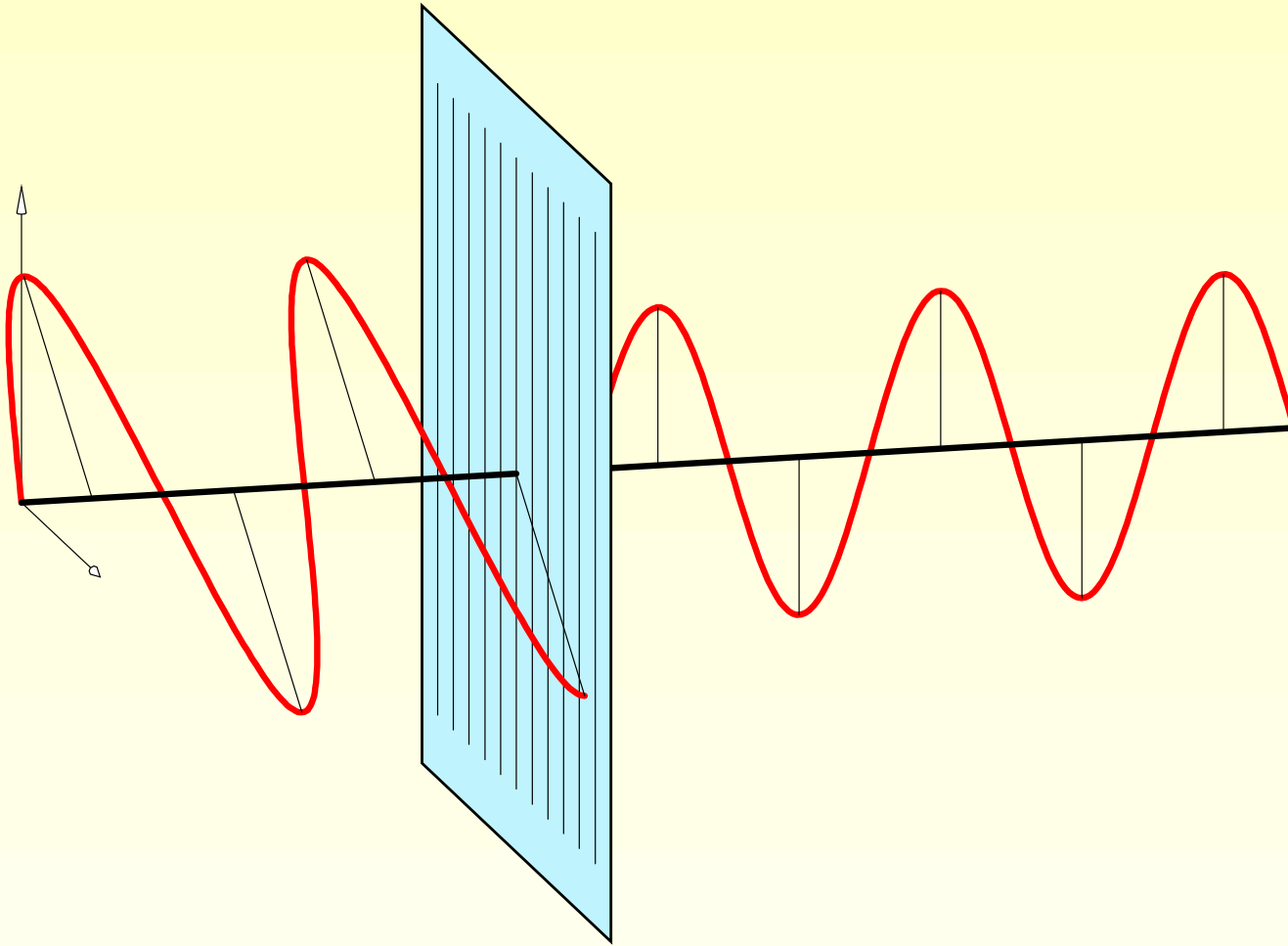
Polaryzator ustawiony pionowo przepuszcza światło spolaryzowane pionowo.



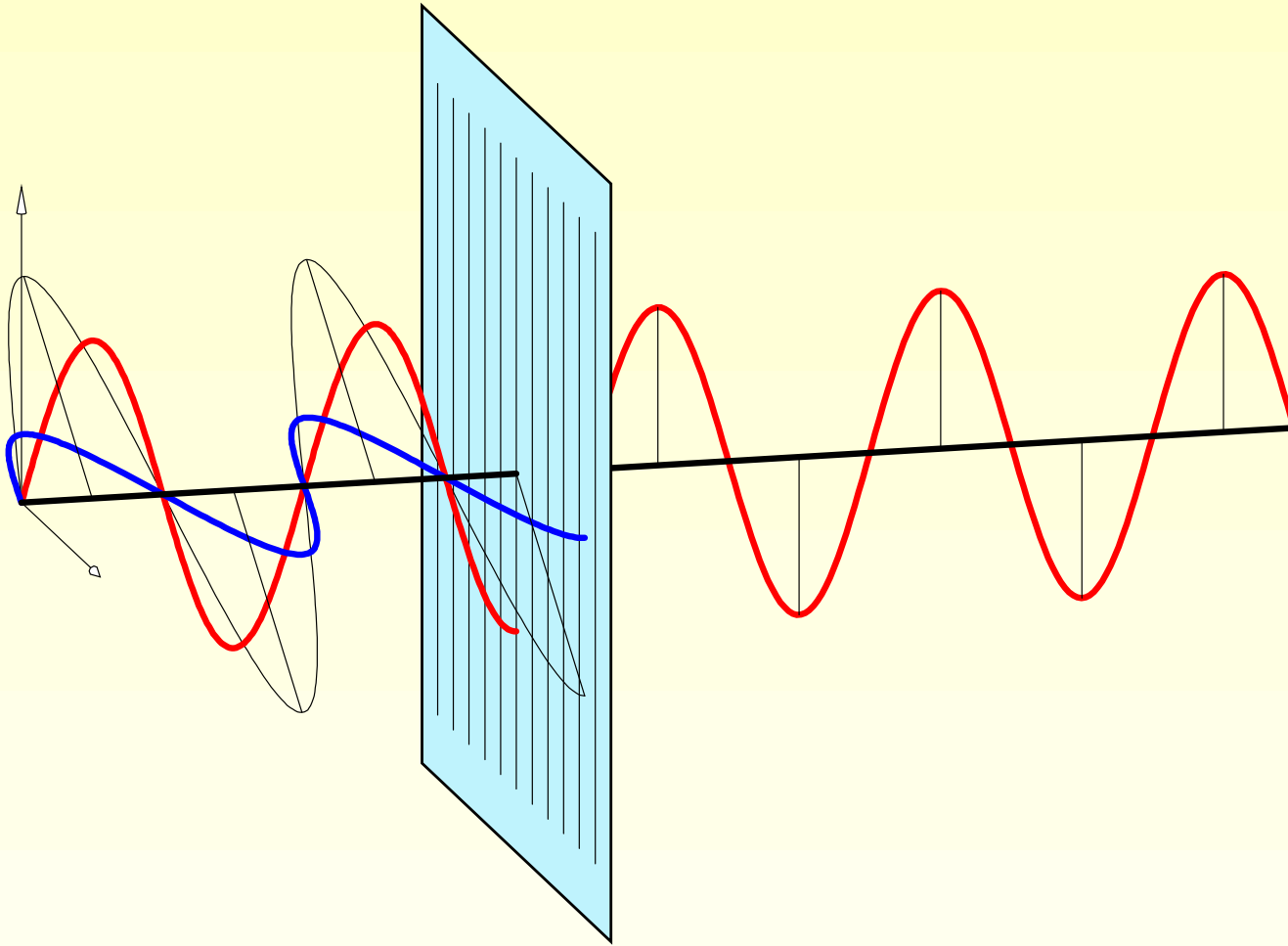
Polaryzator ustawiony **poziomo** zatrzymuje światło spolaryzowane **pionowo**.



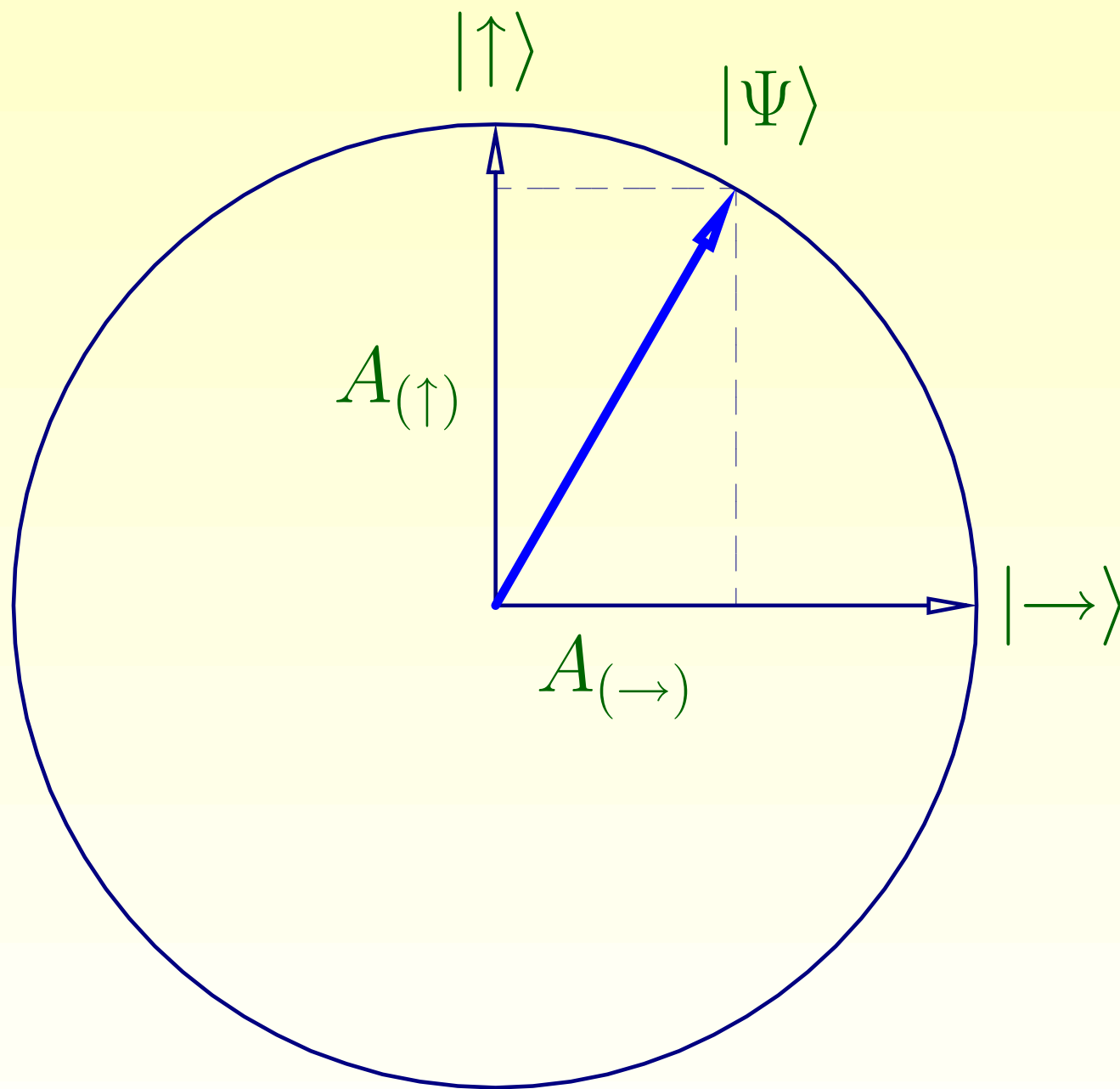
Polaryzator ustawiony **ukośnie** przepuszcza światło spolaryzowane **ukośnie**. Skąd się wzięło światło spolaryzowane **ukośnie**?



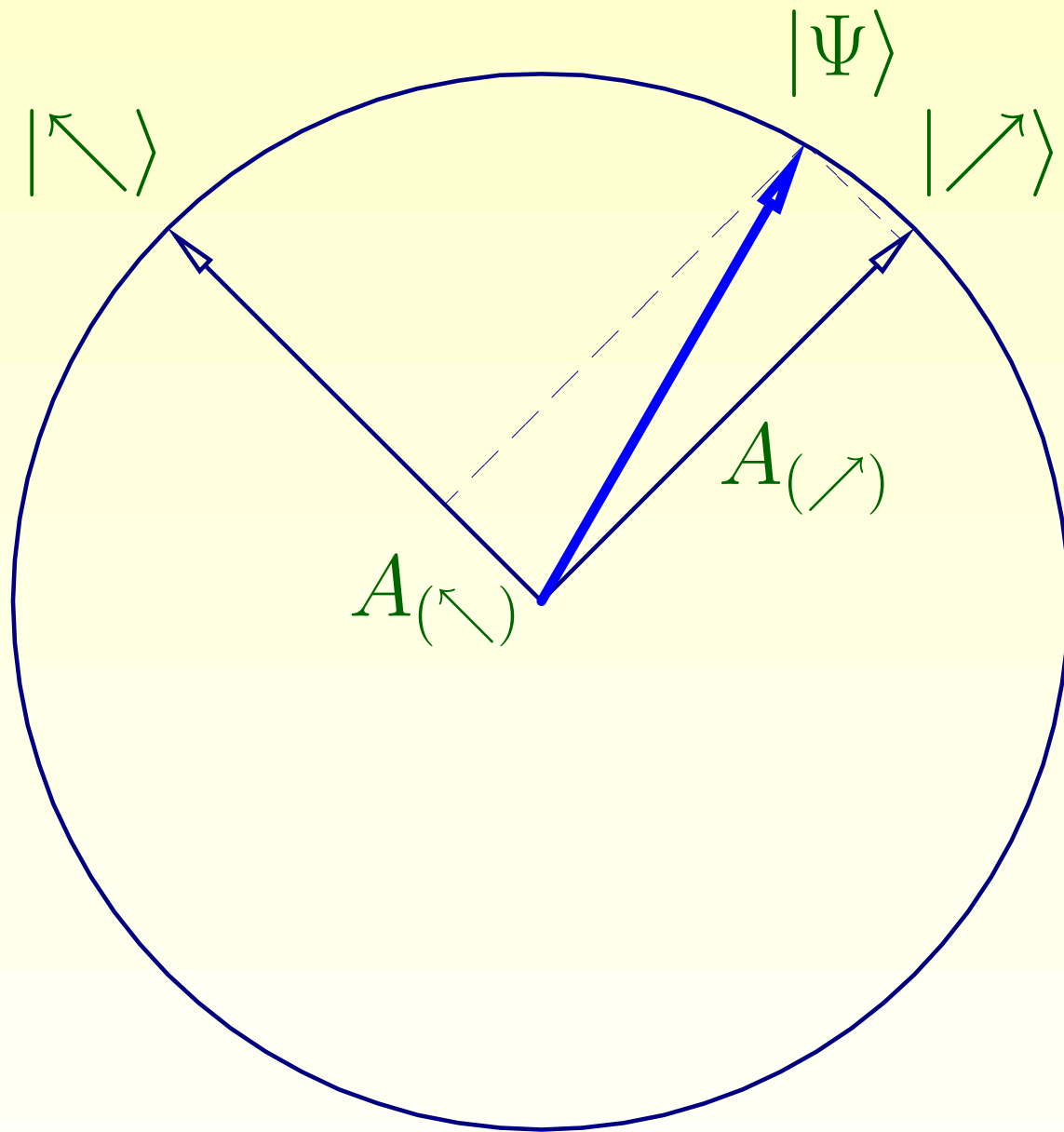
Pada światło spolaryzowane **ukośnie**, polaryzator ustawiony **pionowo** przepuszcza światło spolaryzowane **pionowo**.



Polaryzacja ukośna jest superpozycją polaryzacji pionowej i poziomej. Polaryzator przepuszcza tylko składową pionową!



Polaryzacja fotonu: $|\Psi\rangle = A_{(\uparrow)} |\uparrow\rangle + A_{(\rightarrow)} |\rightarrow\rangle$



Baza ukośna: $|\Psi\rangle = A_{(\nearrow)} |\nearrow\rangle + A_{(\nwarrow)} |\nwarrow\rangle$

Ustawienie polaryzatora określa **bazę pomiarową**.

Zmieniając ustawienie polaryzatora zmieniamy bazę.

Ustawienie polaryzatora określa **bazę pomiarową**.

Zmieniając ustawienie polaryzatora zmieniamy bazę.

Matematycznie wygląda to tak!

$$|\nearrow\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle + |\rightarrow\rangle)$$

$$|\uparrow\rangle = \frac{1}{\sqrt{2}} (|\nearrow\rangle + |\nwarrow\rangle)$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle - |\rightarrow\rangle)$$

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}} (|\nearrow\rangle - |\nwarrow\rangle)$$

$$A_{(\nearrow)} = \frac{1}{\sqrt{2}} (A_{(\uparrow)} + A_{(\rightarrow)})$$

$$A_{(\uparrow)} = \frac{1}{\sqrt{2}} (A_{(\nearrow)} + A_{(\nwarrow)})$$

$$A_{(\nwarrow)} = \frac{1}{\sqrt{2}} (A_{(\uparrow)} - A_{(\rightarrow)})$$

$$A_{(\rightarrow)} = \frac{1}{\sqrt{2}} (A_{(\nearrow)} - A_{(\nwarrow)})$$

2.2 Sfera Blocha

Kubitem jest też spin połówkowy, który w stałym polu magnetycznym może ustawić się zgodnie z kierunkiem pola lub przeciwnie do tego kierunku. Mamy więc dwa stany $|\uparrow\rangle$ i $|\downarrow\rangle$, które możemy też nazwać $|0\rangle$ i $|1\rangle$.

Ewolucja takiego spinu to ruch jego końca po sferze o jednostkowym promieniu, zwanej **sferą Blocha**.

2.2 Sfera Blocha

Kubitem jest też spin połówkowy, który w stałym polu magnetycznym może ustawić się zgodnie z kierunkiem pola lub przeciwnie do tego kierunku. Mamy więc dwa stany $|\uparrow\rangle$ i $|\downarrow\rangle$, które możemy też nazwać $|0\rangle$ i $|1\rangle$.

Ewolucja takiego spinu to ruch jego końca po sferze o jednostkowym promieniu, zwanej **sferą Blocha**.

Ale nie tylko spin połówkowy, lecz **dowolny kubit** może graficznie być reprezentowany jako punkt na takiej sferze. Ewolucja kubitów to ruch punktu po sferze Blocha.

2.2 Sfera Blocha

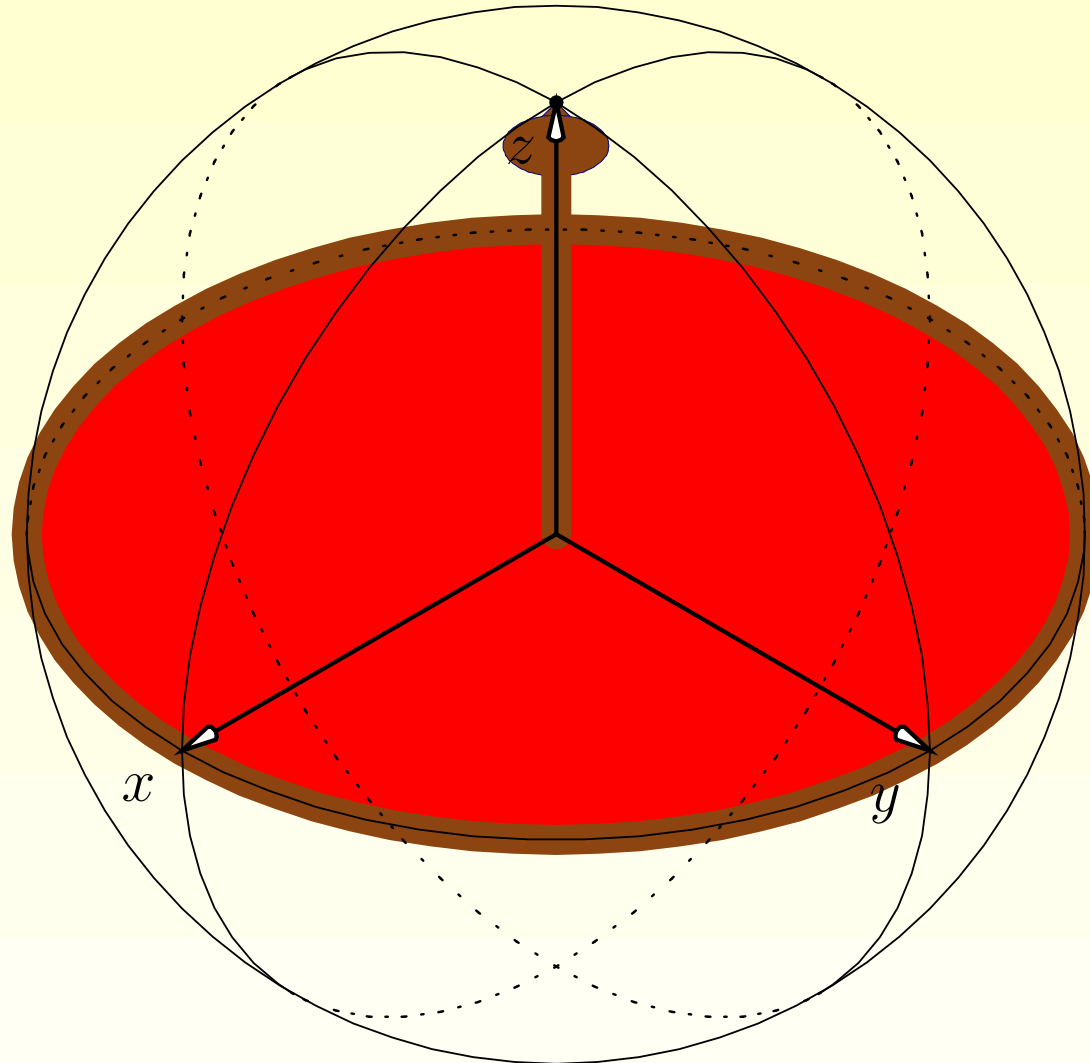
Kubitem jest też spin połówkowy, który w stałym polu magnetycznym może ustawić się zgodnie z kierunkiem pola lub przeciwnie do tego kierunku. Mamy więc dwa stany $|\uparrow\rangle$ i $|\downarrow\rangle$, które możemy też nazwać $|0\rangle$ i $|1\rangle$.

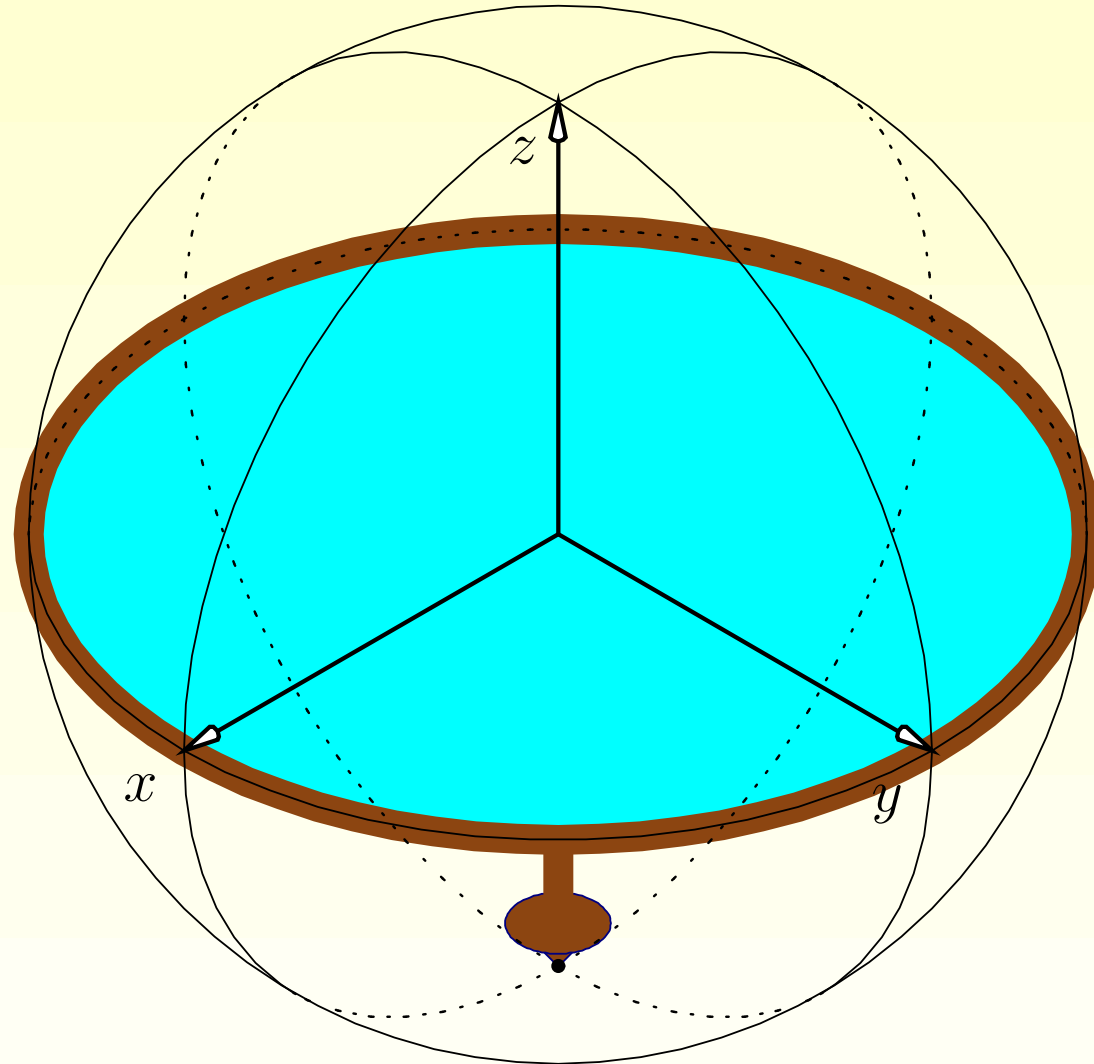
Ewolucja takiego spinu to ruch jego końca po sferze o jednostkowym promieniu, zwanej **sferą Blocha**.

Ale nie tylko spin połówkowy, lecz **dowolny kubit** może graficznie być reprezentowany jako punkt na takiej sferze. Ewolucja kubitów to ruch punktu po sferze Blocha.

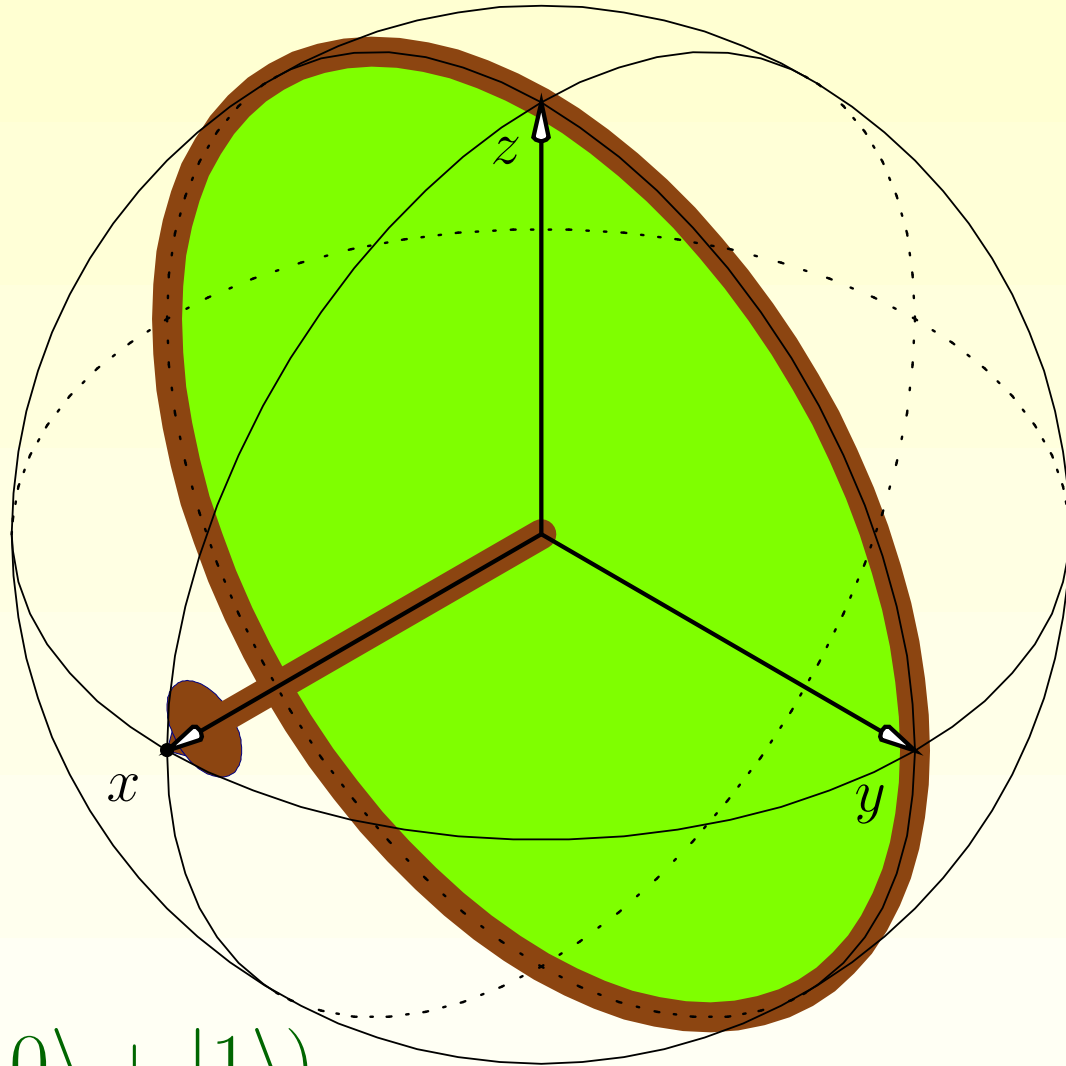
A wygląda to tak ...

$|0\rangle$



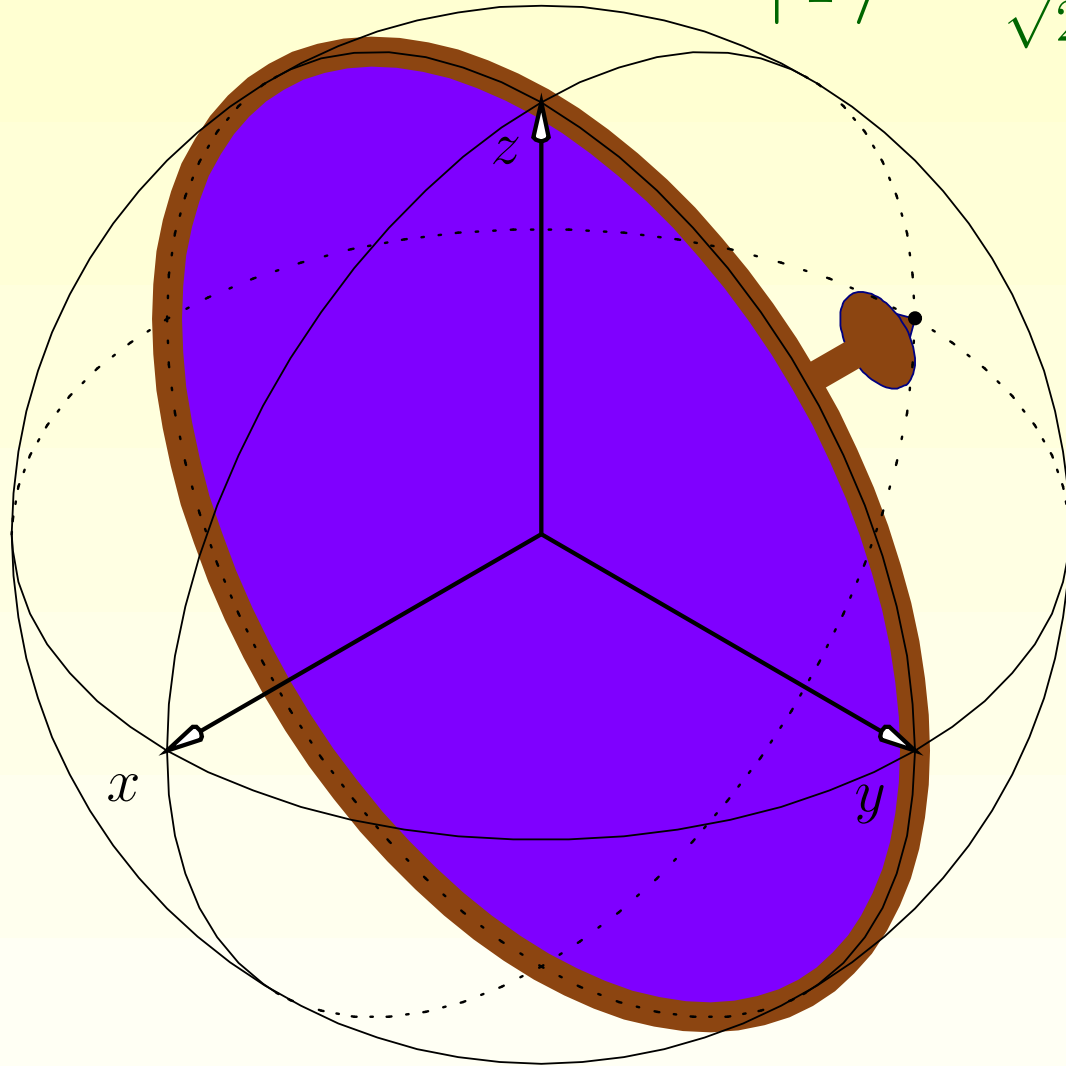


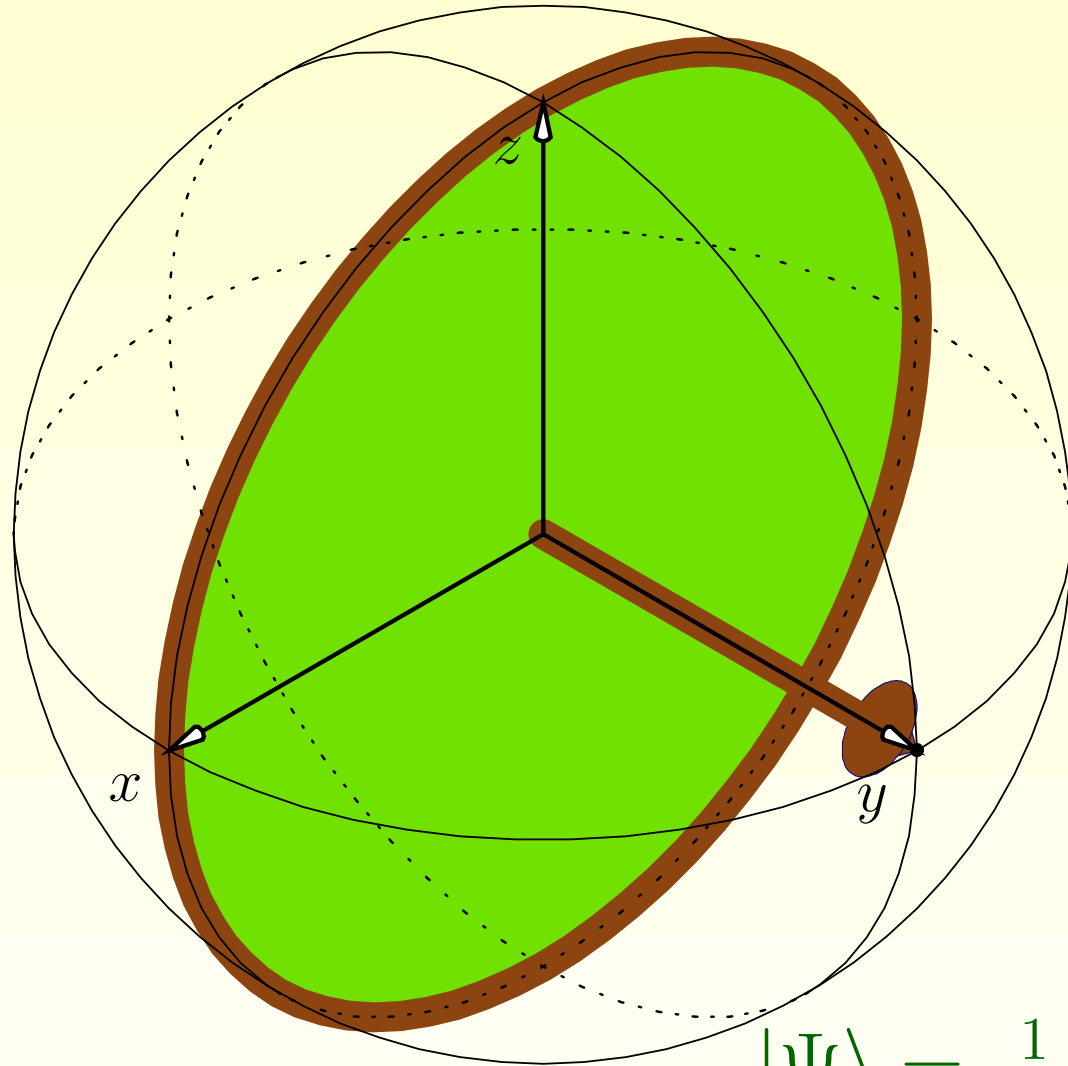
$|1\rangle$



$$|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

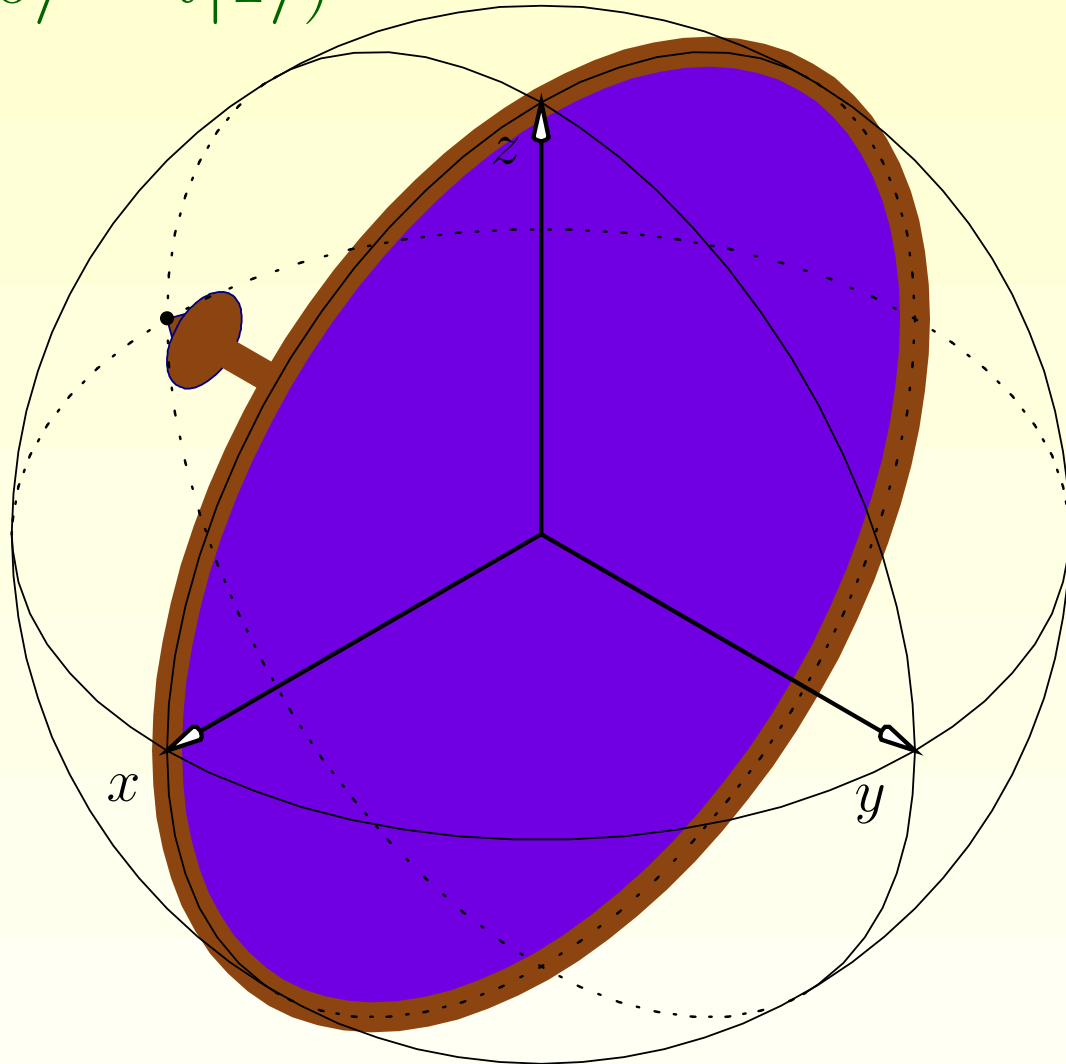
$$|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$



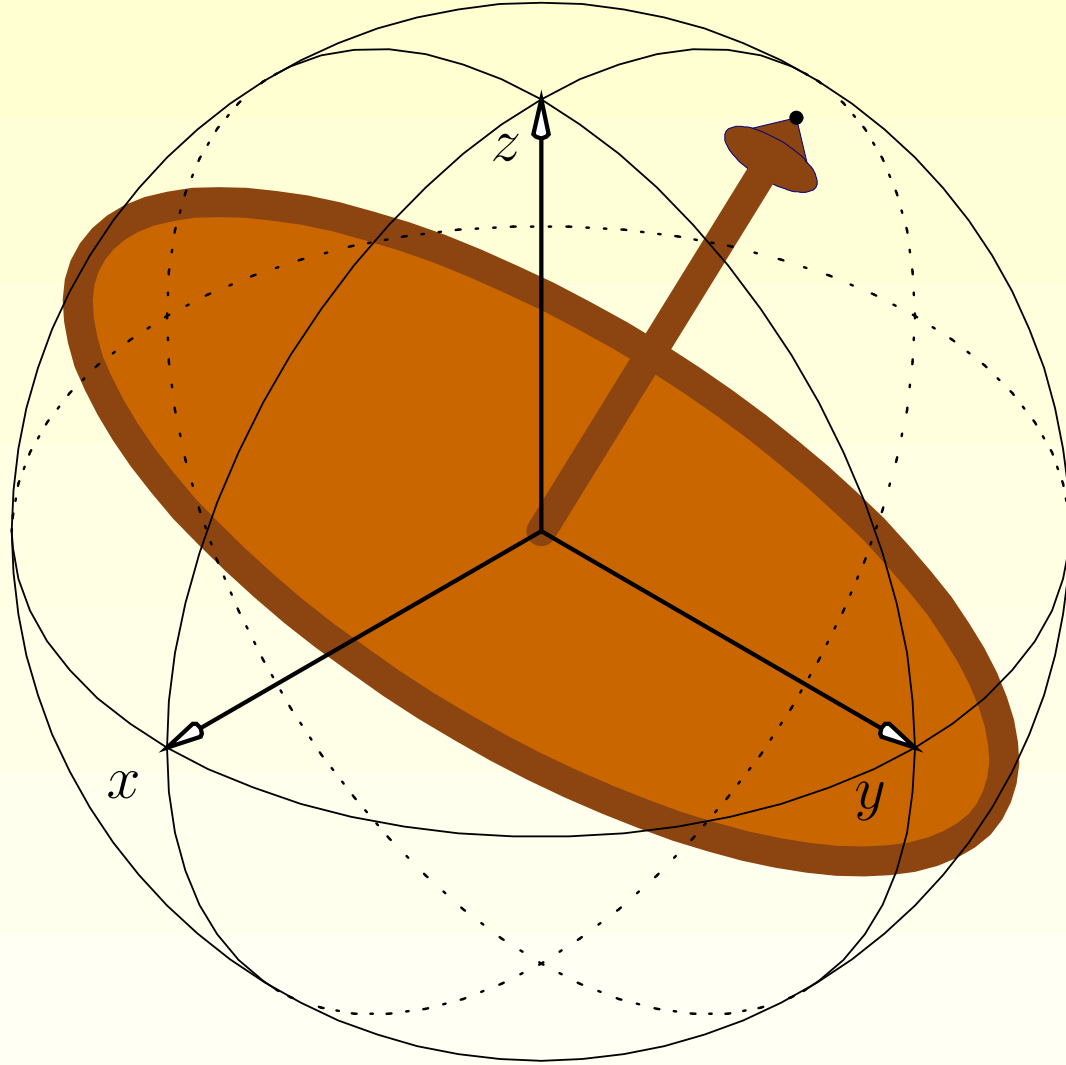


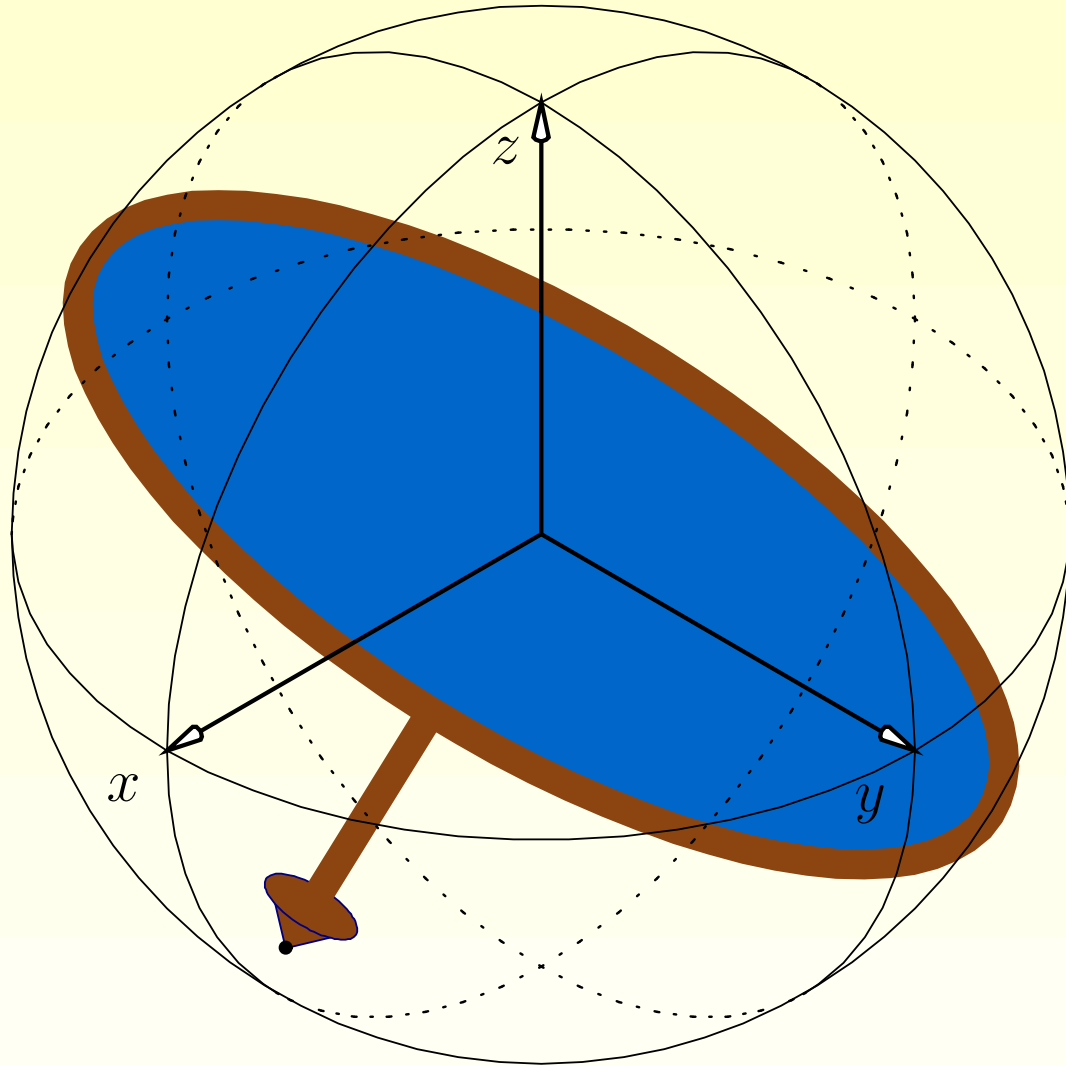
$$|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle)$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle - i|1\rangle)$$



$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$





$$|\Psi\rangle = \sin \frac{\theta}{2} |0\rangle - e^{i\varphi} \cos \frac{\theta}{2} |1\rangle$$

Przyjeliśmy tutaj następującą konwencję dotyczącą
kolorowania kubitów:

Przyjeliśmy tutaj następującą konwencję dotyczącą kolorowania kubitów:

- Każdy kubit (punkt na sferze) ma własny kolor

Przyjęliśmy tutaj następującą konwencję dotyczącą kolorowania kubitów:

- Każdy kubit (punkt na sferze) ma własny kolor
- Dwa ortogonalne kubity (punkty na antypodach) mają kolory dopełniające (ich zmieszanie daje kolor biały lub odcień szarości)

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

$$\langle 0|A_0^* + \langle 1|A_1^* = \langle \Psi|$$

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

$$\langle 0|A_0^* + \langle 1|A_1^* = \langle \Psi|$$

$$\langle \Psi|\Psi\rangle = (\langle 0|A_0^* + \langle 1|A_1^*)(A_0|0\rangle + A_1|1\rangle)$$

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

$$\langle 0|A_0^* + \langle 1|A_1^* = \langle \Psi|$$

$$\begin{aligned}\langle \Psi|\Psi\rangle &= (\langle 0|A_0^* + \langle 1|A_1^*)(A_0|0\rangle + A_1|1\rangle) \\ &= A_0^*A_0 \langle 0|0\rangle + A_1^*A_1 \langle 1|1\rangle \\ &\quad + A_0^*A_1 \langle 0|1\rangle + A_1^*A_0 \langle 1|0\rangle\end{aligned}$$

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

$$\langle 0|A_0^* + \langle 1|A_1^* = \langle \Psi|$$

$$\begin{aligned}\langle \Psi|\Psi\rangle &= (\langle 0|A_0^* + \langle 1|A_1^*)(A_0|0\rangle + A_1|1\rangle) \\ &= A_0^*A_0 \langle 0|0\rangle + A_1^*A_1 \langle 1|1\rangle \\ &\quad + A_0^*A_1 \langle 0|1\rangle + A_1^*A_0 \langle 1|0\rangle \\ &= |A_0|^2 + |A_1|^2\end{aligned}$$

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

$$\langle 0|A_0^* + \langle 1|A_1^* = \langle \Psi|$$

$$\begin{aligned}\langle \Psi|\Psi\rangle &= (\langle 0|A_0^* + \langle 1|A_1^*)(A_0|0\rangle + A_1|1\rangle) \\ &= A_0^*A_0 \langle 0|0\rangle + A_1^*A_1 \langle 1|1\rangle \\ &\quad + A_0^*A_1 \langle 0|1\rangle + A_1^*A_0 \langle 1|0\rangle \\ &= |A_0|^2 + |A_1|^2 \\ &= 1\end{aligned}$$

2.3 Algebra kubitów w pigułce

$$|\Psi\rangle = A_0|0\rangle + A_1|1\rangle$$

$$\langle 0|A_0^* + \langle 1|A_1^* = \langle \Psi|$$

$$\begin{aligned}\langle \Psi|\Psi\rangle &= (\langle 0|A_0^* + \langle 1|A_1^*)(A_0|0\rangle + A_1|1\rangle) \\ &= A_0^*A_0 \langle 0|0\rangle + A_1^*A_1 \langle 1|1\rangle \\ &\quad + A_0^*A_1 \langle 0|1\rangle + A_1^*A_0 \langle 1|0\rangle \\ &= |A_0|^2 + |A_1|^2 \\ &= 1\end{aligned}$$

$$\langle 0|0\rangle = \langle 1|1\rangle = 1$$

$$\langle 0|1\rangle = \langle 1|0\rangle = 0$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$|\Psi\rangle\langle\Psi| = (A_0|0\rangle + A_1|1\rangle)(\langle 0|A_0^* + \langle 1|A_1^*)$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$\begin{aligned} |\Psi\rangle\langle\Psi| &= (A_0|0\rangle + A_1|1\rangle)(\langle 0|A_0^* + \langle 1|A_1^*) \\ &= A_0A_0^* |0\rangle\langle 0| + A_1A_1^* |1\rangle\langle 1| \\ &\quad + A_0A_1^* |0\rangle\langle 1| + A_1A_0^* |1\rangle\langle 0| \end{aligned}$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$\begin{aligned} |\Psi\rangle\langle\Psi| &= (A_0|0\rangle + A_1|1\rangle)(\langle 0|A_0^* + \langle 1|A_1^*) \\ &= A_0A_0^* |0\rangle\langle 0| + A_1A_1^* |1\rangle\langle 1| \\ &\quad + A_0A_1^* |0\rangle\langle 1| + A_1A_0^* |1\rangle\langle 0| \end{aligned}$$

$$|0\rangle\langle 0||0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle$$

$$|0\rangle\langle 0||1\rangle = |0\rangle\langle 0|1\rangle = 0$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$\begin{aligned} |\Psi\rangle\langle\Psi| &= (A_0|0\rangle + A_1|1\rangle)(\langle 0|A_0^* + \langle 1|A_1^*) \\ &= A_0A_0^* |0\rangle\langle 0| + A_1A_1^* |1\rangle\langle 1| \\ &\quad + A_0A_1^* |0\rangle\langle 1| + A_1A_0^* |1\rangle\langle 0| \end{aligned}$$

$$|0\rangle\langle 0||0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle$$

$$|0\rangle\langle 0||1\rangle = |0\rangle\langle 0|1\rangle = 0$$

$$|1\rangle\langle 1||1\rangle = |1\rangle\langle 1|1\rangle = |1\rangle$$

$$|1\rangle\langle 1||0\rangle = |1\rangle\langle 1|0\rangle = 0$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$\begin{aligned} |\Psi\rangle\langle\Psi| &= (A_0|0\rangle + A_1|1\rangle)(\langle 0|A_0^* + \langle 1|A_1^*) \\ &= A_0A_0^* |0\rangle\langle 0| + A_1A_1^* |1\rangle\langle 1| \\ &\quad + A_0A_1^* |0\rangle\langle 1| + A_1A_0^* |1\rangle\langle 0| \end{aligned}$$

$$|0\rangle\langle 0||0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle$$

$$|0\rangle\langle 0||1\rangle = |0\rangle\langle 0|1\rangle = 0$$

$$|1\rangle\langle 1||1\rangle = |1\rangle\langle 1|1\rangle = |1\rangle$$

$$|1\rangle\langle 1||0\rangle = |1\rangle\langle 1|0\rangle = 0$$

$$|0\rangle\langle 1||1\rangle = |0\rangle\langle 1|1\rangle = |0\rangle$$

$$|0\rangle\langle 1||0\rangle = |0\rangle\langle 1|0\rangle = 0$$

$$A_0|0\rangle + A_1|1\rangle = |\Psi\rangle$$

$$\langle\Psi| = \langle 0|A_0^* + \langle 1|A_1^*$$

$$\begin{aligned} |\Psi\rangle\langle\Psi| &= (A_0|0\rangle + A_1|1\rangle)(\langle 0|A_0^* + \langle 1|A_1^*) \\ &= A_0A_0^* |0\rangle\langle 0| + A_1A_1^* |1\rangle\langle 1| \\ &\quad + A_0A_1^* |0\rangle\langle 1| + A_1A_0^* |1\rangle\langle 0| \end{aligned}$$

$$|0\rangle\langle 0||0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle$$

$$|0\rangle\langle 0||1\rangle = |0\rangle\langle 0|1\rangle = 0$$

$$|1\rangle\langle 1||1\rangle = |1\rangle\langle 1|1\rangle = |1\rangle$$

$$|1\rangle\langle 1||0\rangle = |1\rangle\langle 1|0\rangle = 0$$

$$|0\rangle\langle 1||1\rangle = |0\rangle\langle 1|1\rangle = |0\rangle$$

$$|0\rangle\langle 1||0\rangle = |0\rangle\langle 1|0\rangle = 0$$

$$|1\rangle\langle 0||0\rangle = |1\rangle\langle 0|0\rangle = |1\rangle$$

$$|1\rangle\langle 0||1\rangle = |1\rangle\langle 0|1\rangle = 0$$

3 Ewolucja kubitów

3.1 Pomiar kwantowy

Kubit, $|\Psi(t)\rangle = A_0(t)|0\rangle + A_1(t)|1\rangle$, ewoluując w czasie reprezentuje jednocześnie **obydwa** stany bazy, $|0\rangle$ i $|1\rangle$.

3 Ewolucja kubitów

3.1 Pomiar kwantowy

Kubit, $|\Psi(t)\rangle = A_0(t)|0\rangle + A_1(t)|1\rangle$, ewoluując w czasie reprezentuje jednocześnie **obydwa** stany bazy, $|0\rangle$ i $|1\rangle$.

Pomiar kwantowy w bazie $\{|0\rangle, |1\rangle\}$ powoduje przejście kubitów do **jednego** ze stanów bazowych. Następuje, jak mówimy, **redukcja stanu kwantowego**.

3 Ewolucja kubitów

3.1 Pomiar kwantowy

Kubit, $|\Psi(t)\rangle = A_0(t)|0\rangle + A_1(t)|1\rangle$, ewoluując w czasie reprezentuje jednocześnie **obydwa** stany bazy, $|0\rangle$ i $|1\rangle$.

Pomiar kwantowy w bazie $\{|0\rangle, |1\rangle\}$ powoduje przejście kubit do **jednego** ze stanów bazowych. Następuje, jak mówimy, **redukcja stanu kwantowego**.

Pomiar $M_0 = |0\rangle\langle 0|$: $|\Psi(t_m)\rangle \mapsto |0\rangle$, $P_0 = |A_0(t_m)|^2$

3 Ewolucja kubitów

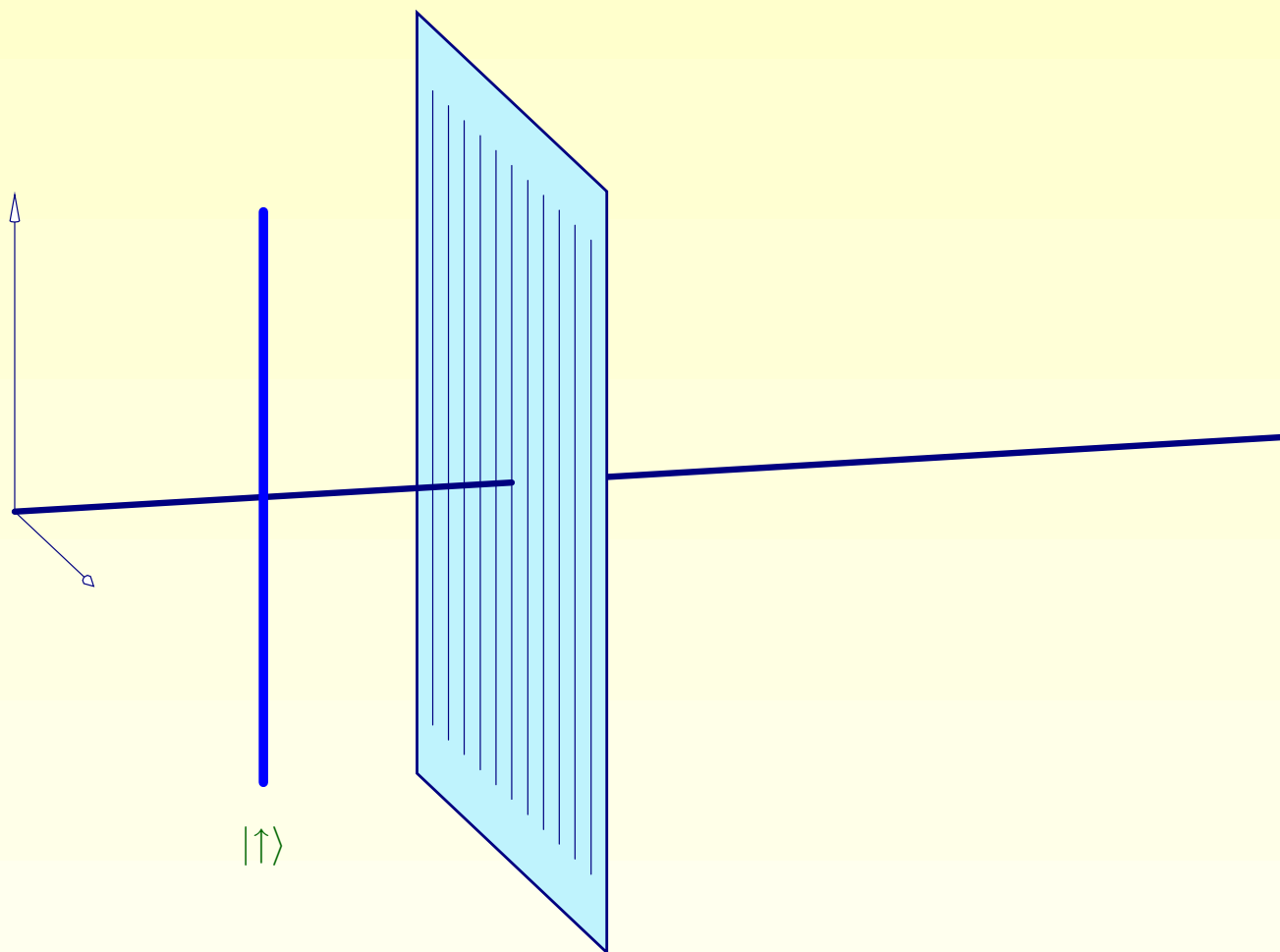
3.1 Pomiar kwantowy

Kubit, $|\Psi(t)\rangle = A_0(t)|0\rangle + A_1(t)|1\rangle$, ewoluując w czasie reprezentuje jednocześnie **obydwa** stany bazy, $|0\rangle$ i $|1\rangle$.

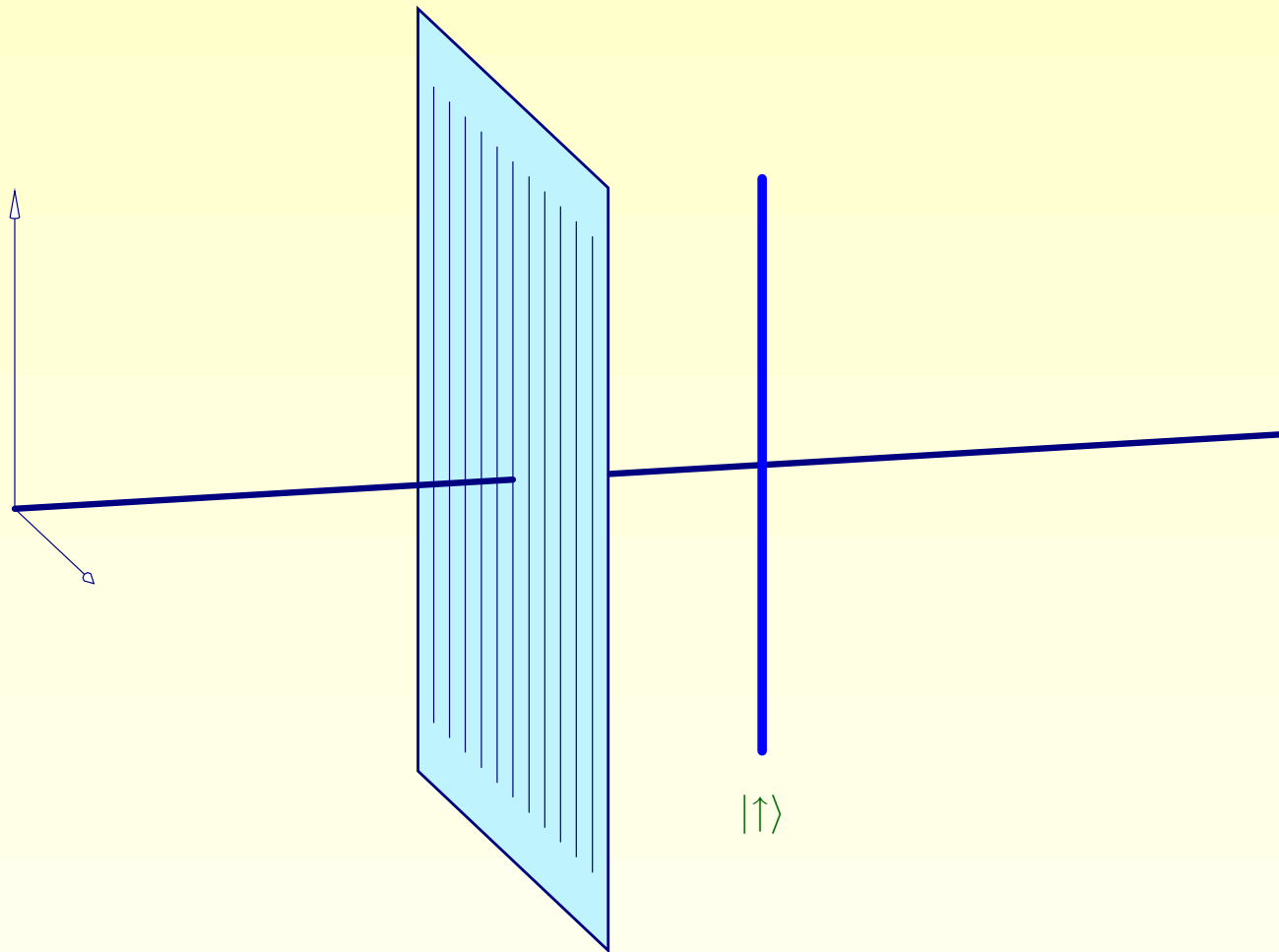
Pomiar kwantowy w bazie $\{|0\rangle, |1\rangle\}$ powoduje przejście kubit do **jednego** ze stanów bazowych. Następuje, jak mówimy, **redukcja stanu kwantowego**.

Pomiar $M_0 = |0\rangle\langle 0|$: $|\Psi(t_m)\rangle \mapsto |0\rangle$, $P_0 = |A_0(t_m)|^2$

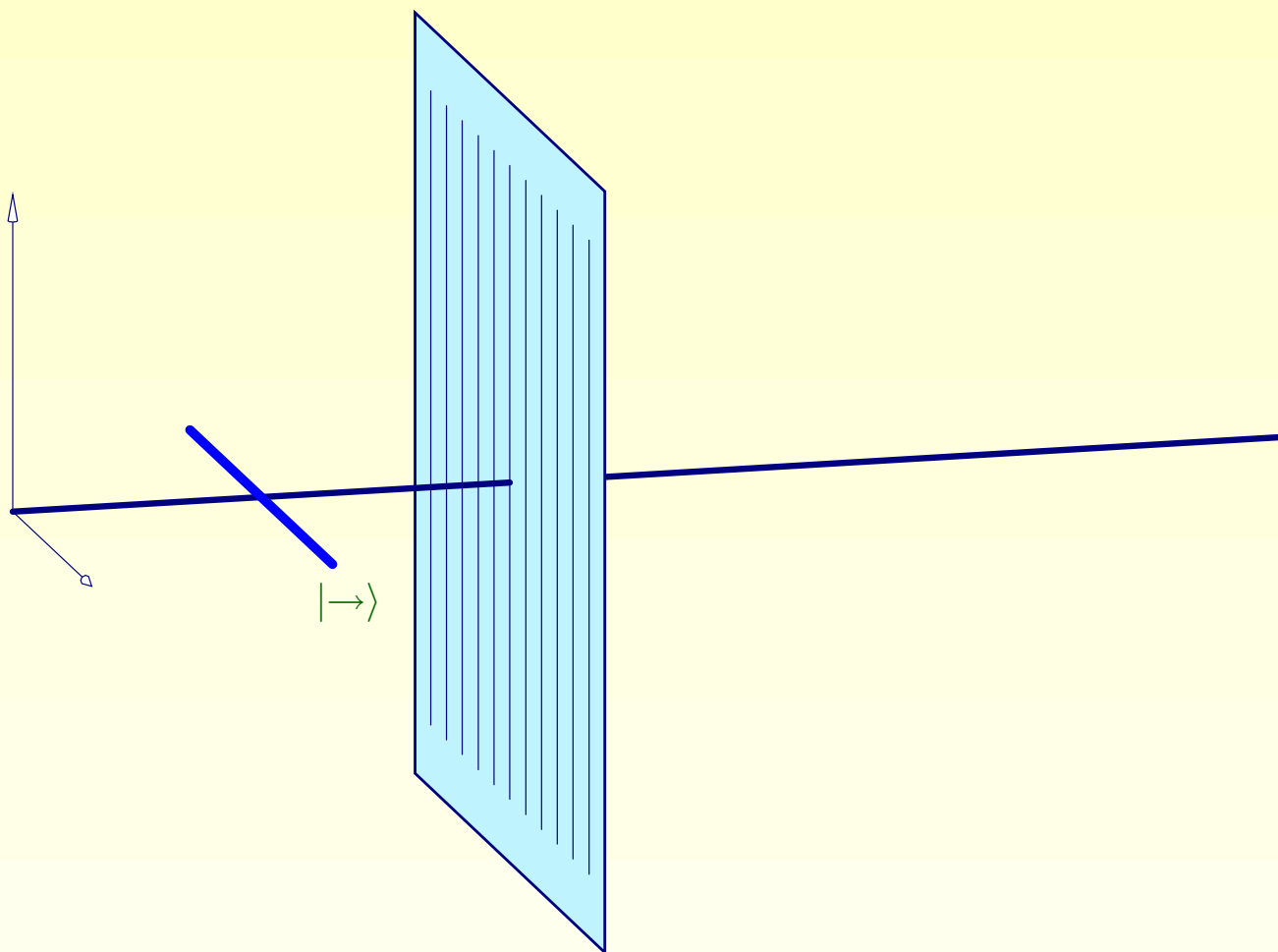
Pomiar $M_1 = |1\rangle\langle 1|$: $|\Psi(t_m)\rangle \mapsto |1\rangle$, $P_1 = |A_1(t_m)|^2$



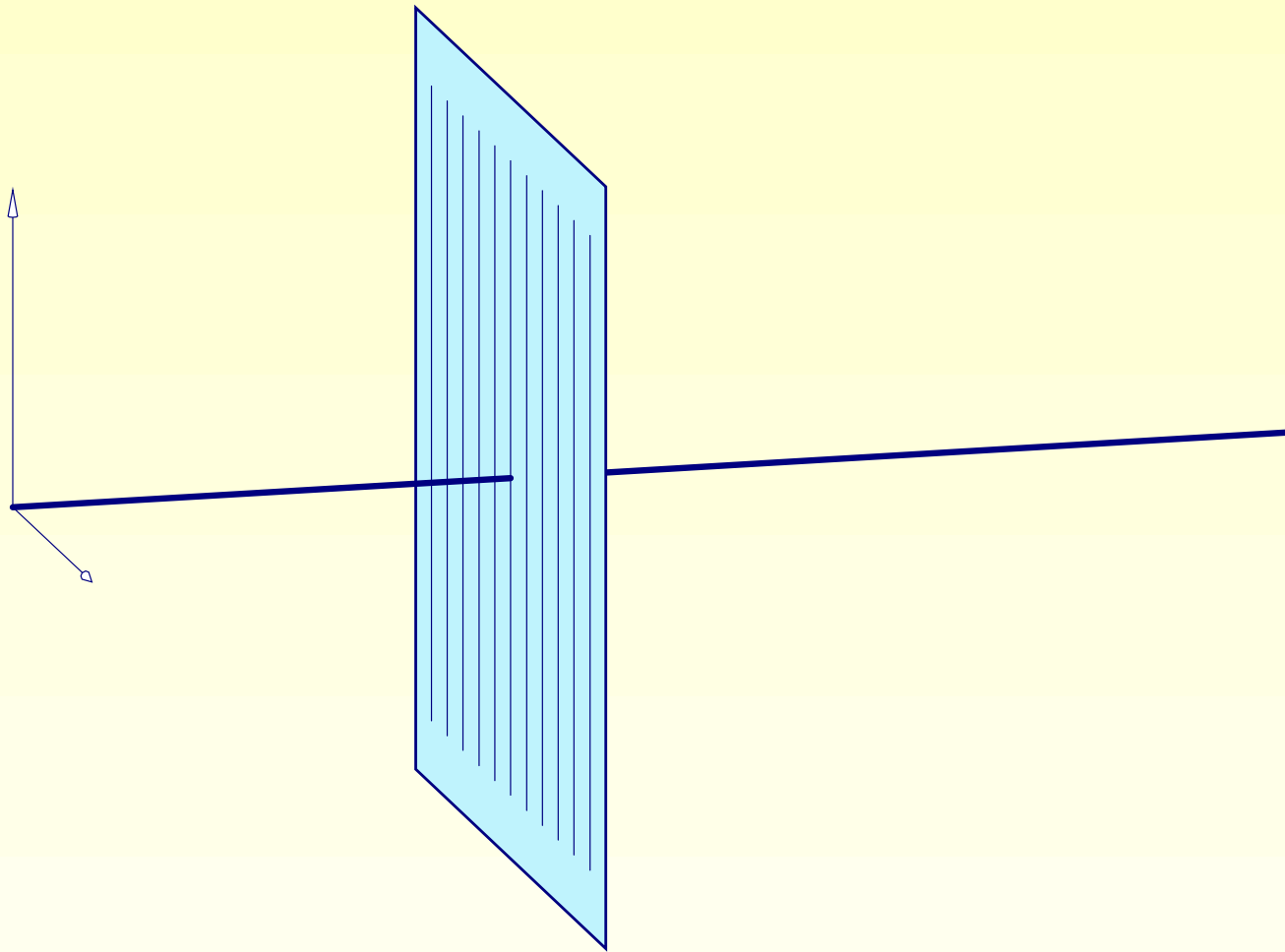
Foton w stanie $|\uparrow\rangle$...



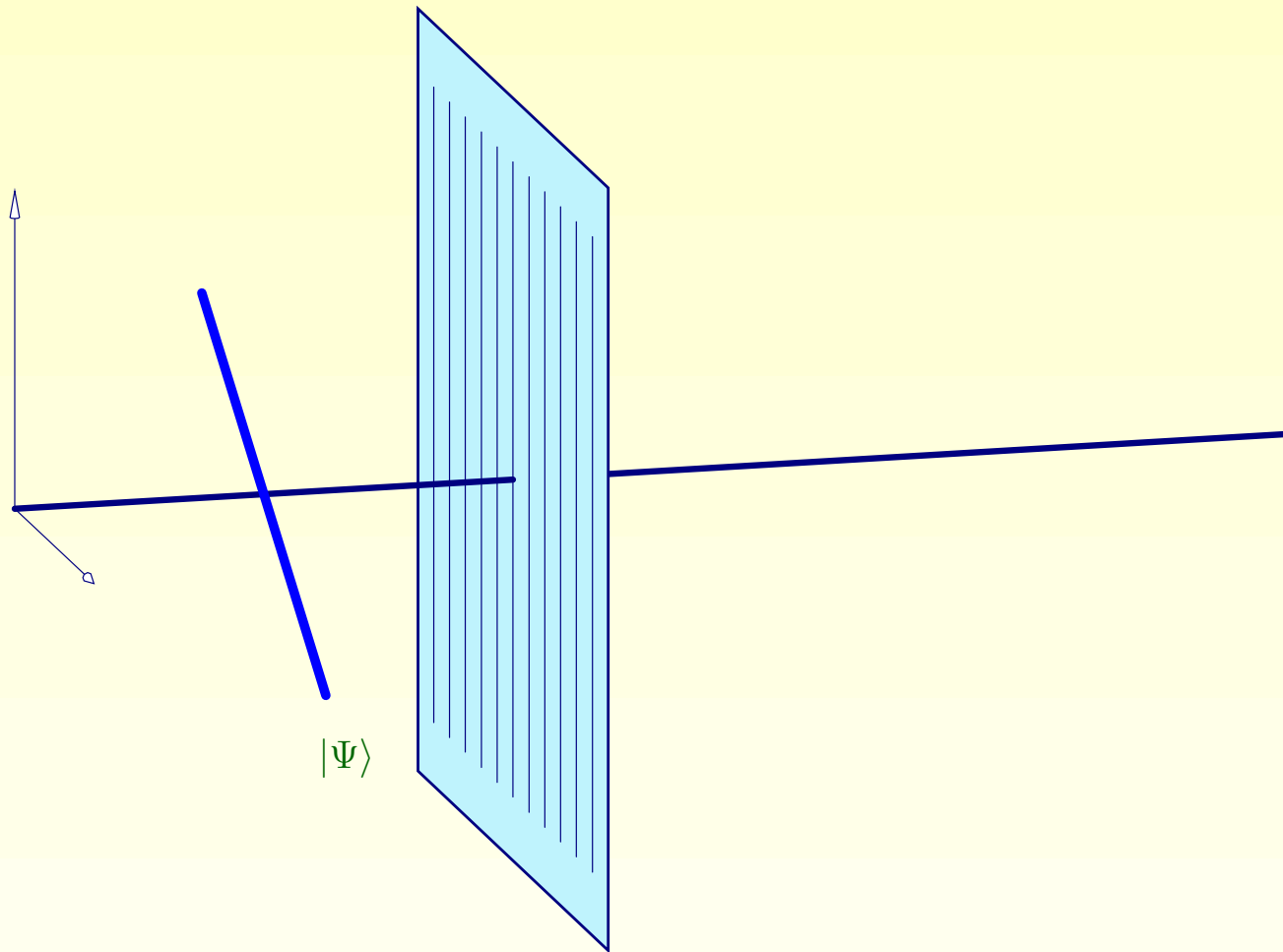
przechodzi przez polaryzator ustawiony pionowo i pozostaje w stanie $|\uparrow\rangle$. Prawdopodobieństwo przejścia równe **1**.



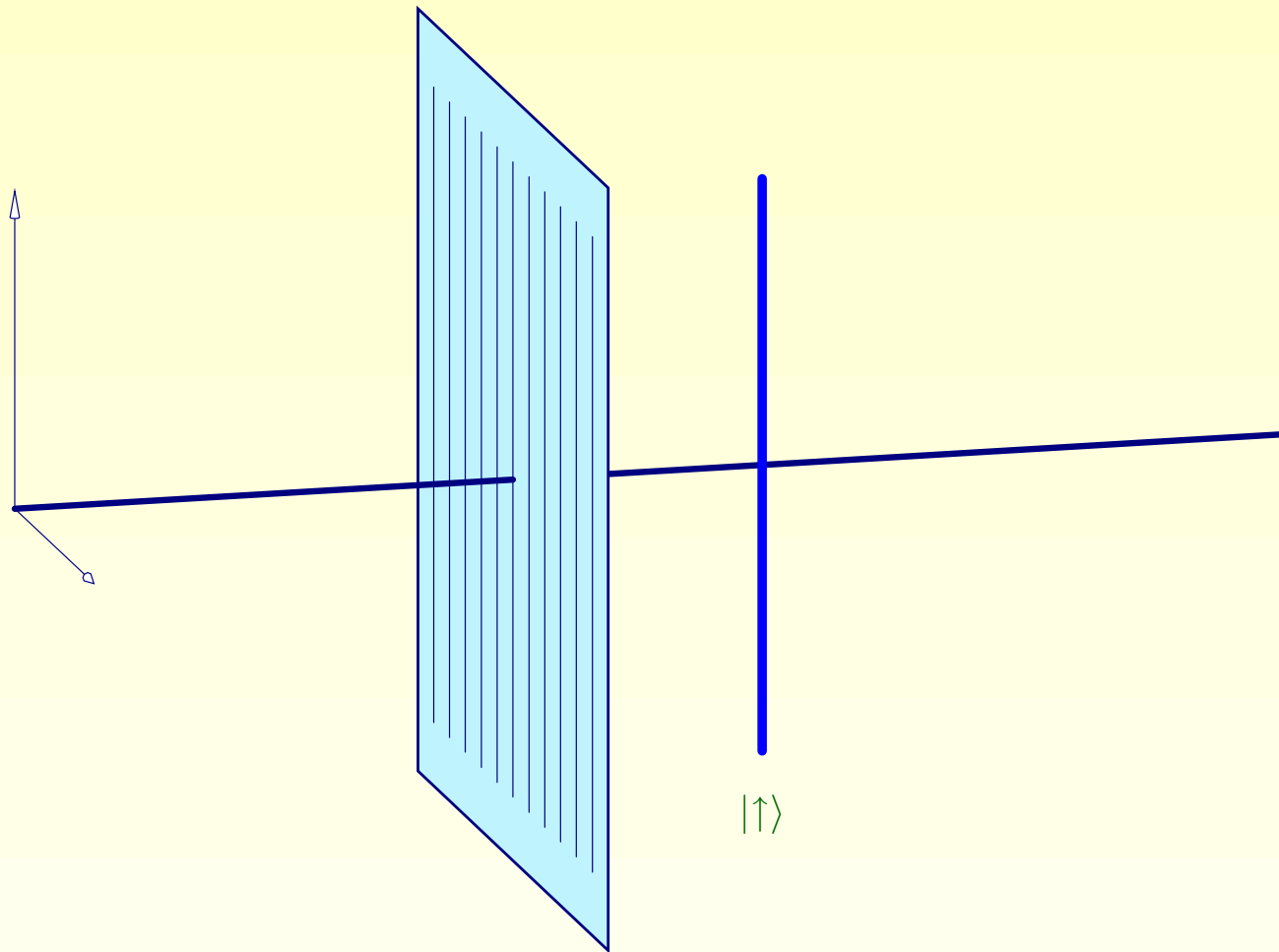
Foton w stanie $|\rightarrow\rangle$...



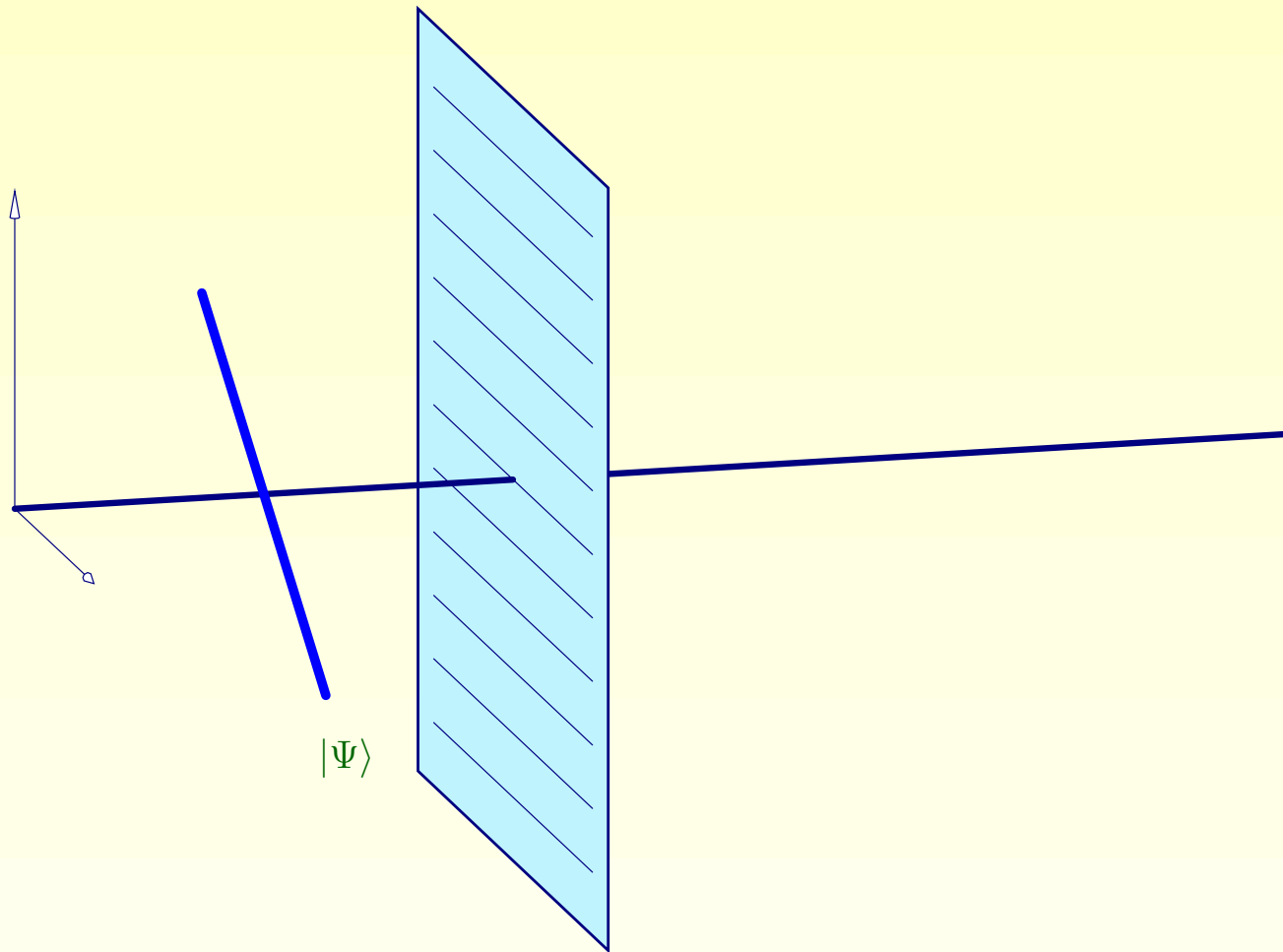
nie przechodzi przez polaryzator ustawiony pionowo.
Prawdopodobieństwo przejścia równe 0.



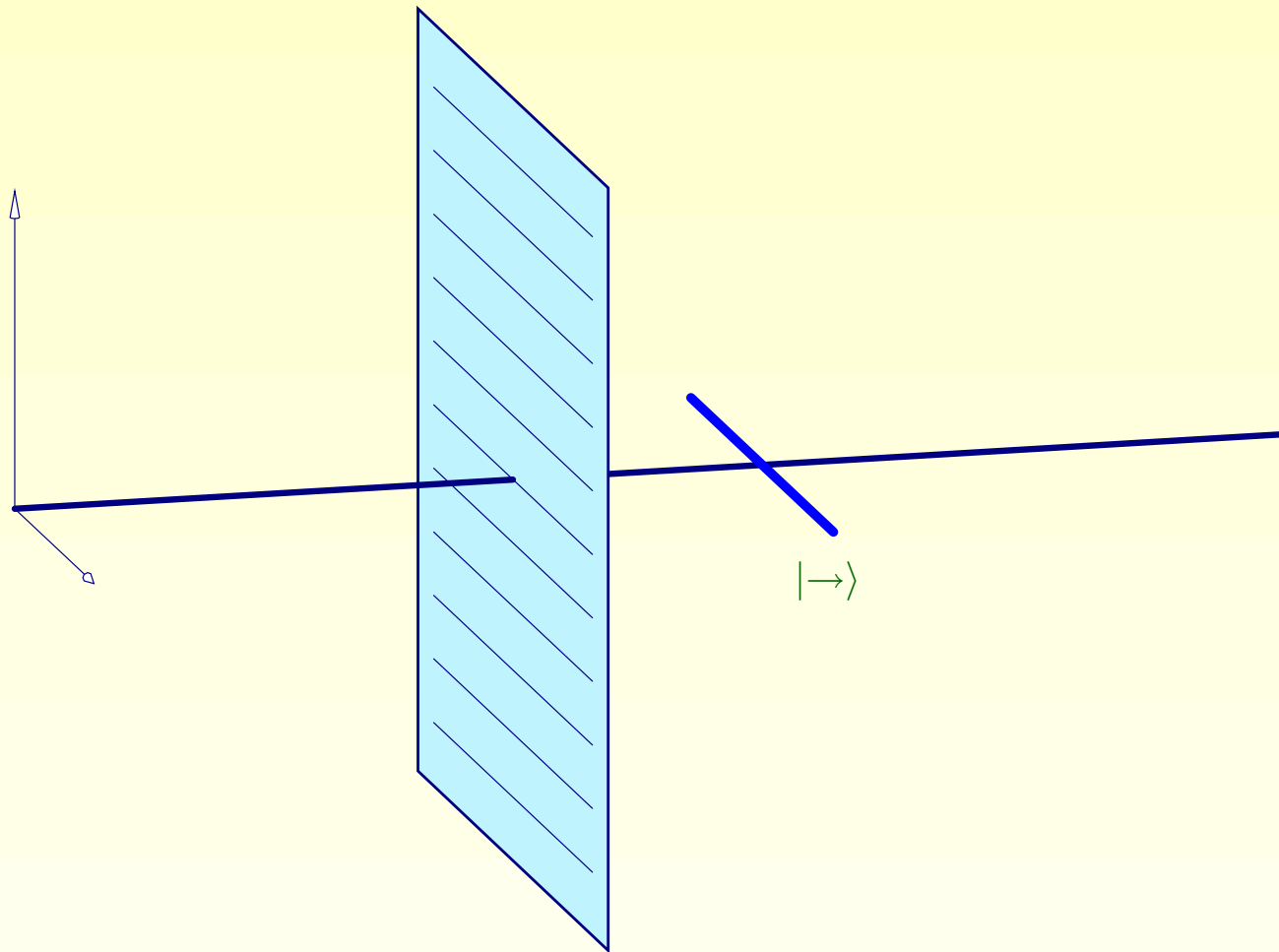
Foton w stanie $|\Psi\rangle = A_{(\uparrow)} |\uparrow\rangle + A_{(\rightarrow)} |\rightarrow\rangle \dots$



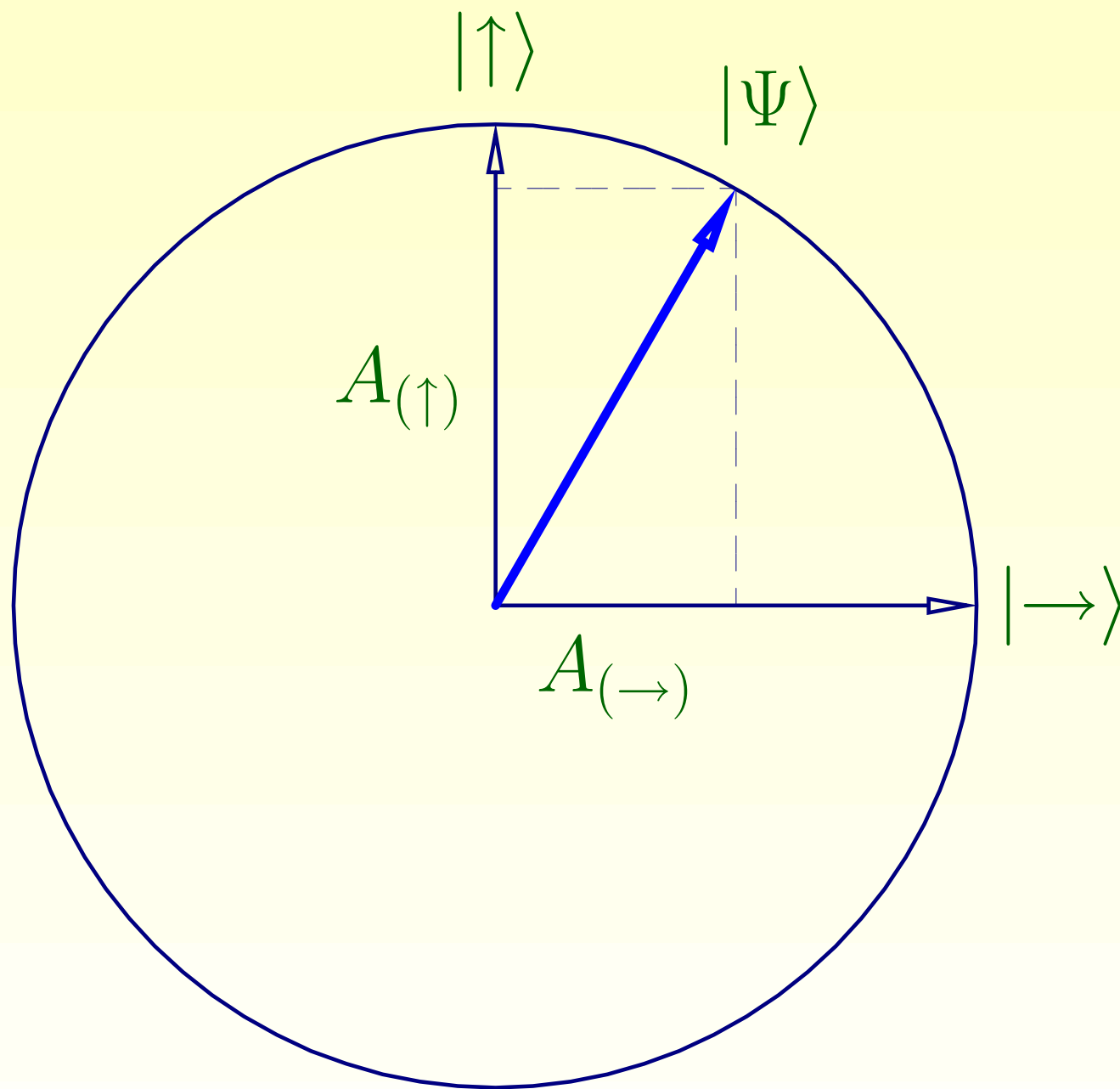
przechodzi przez polaryzator ustawiony pionowo i staje się fotonem w stanie $|\uparrow\rangle$ z prawdopodobieństwem równym $|A_{(\uparrow)}|^2$.



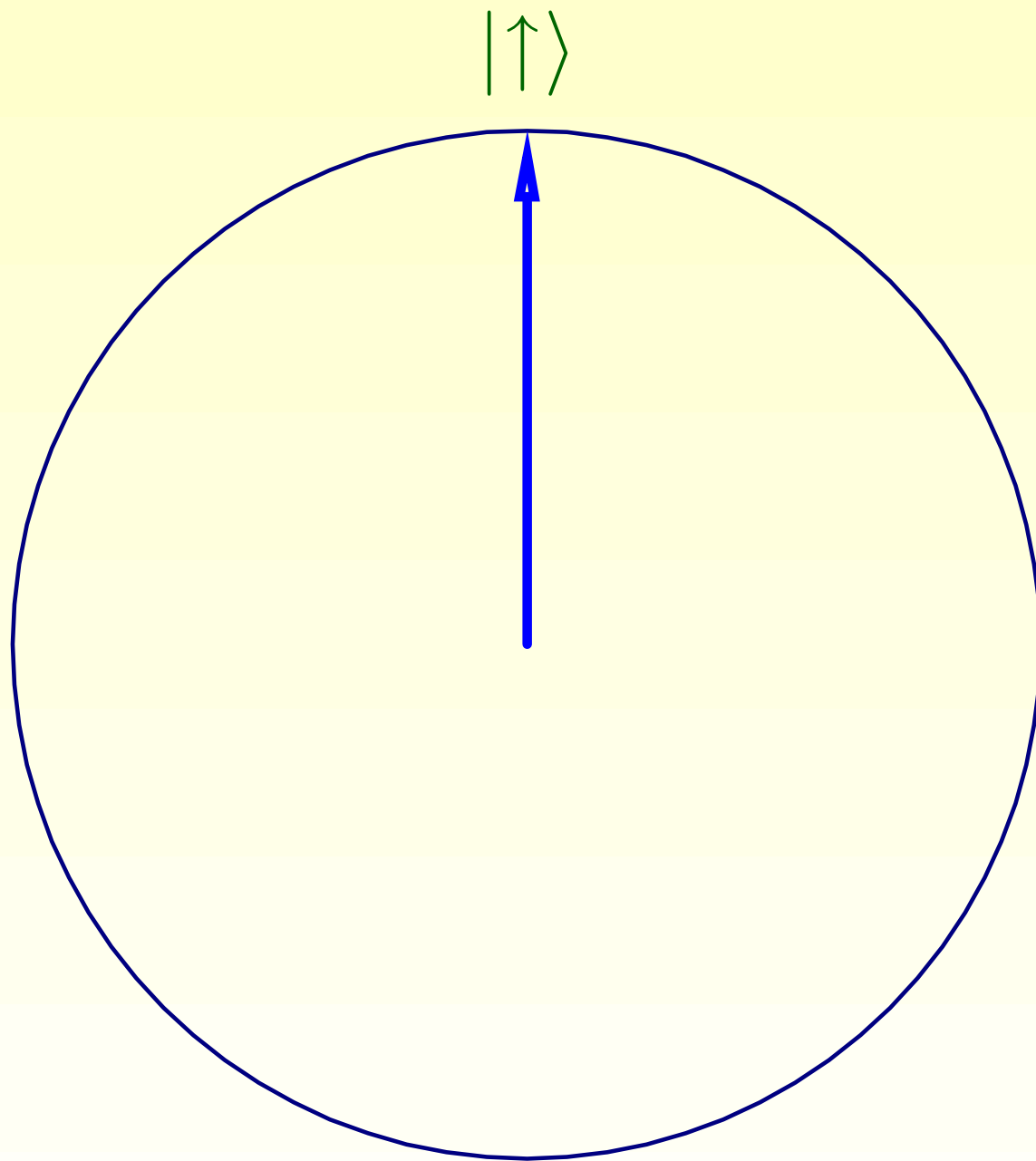
Foton w stanie $|\Psi\rangle = A_{(\uparrow)} |\uparrow\rangle + A_{(\rightarrow)} |\rightarrow\rangle \dots$



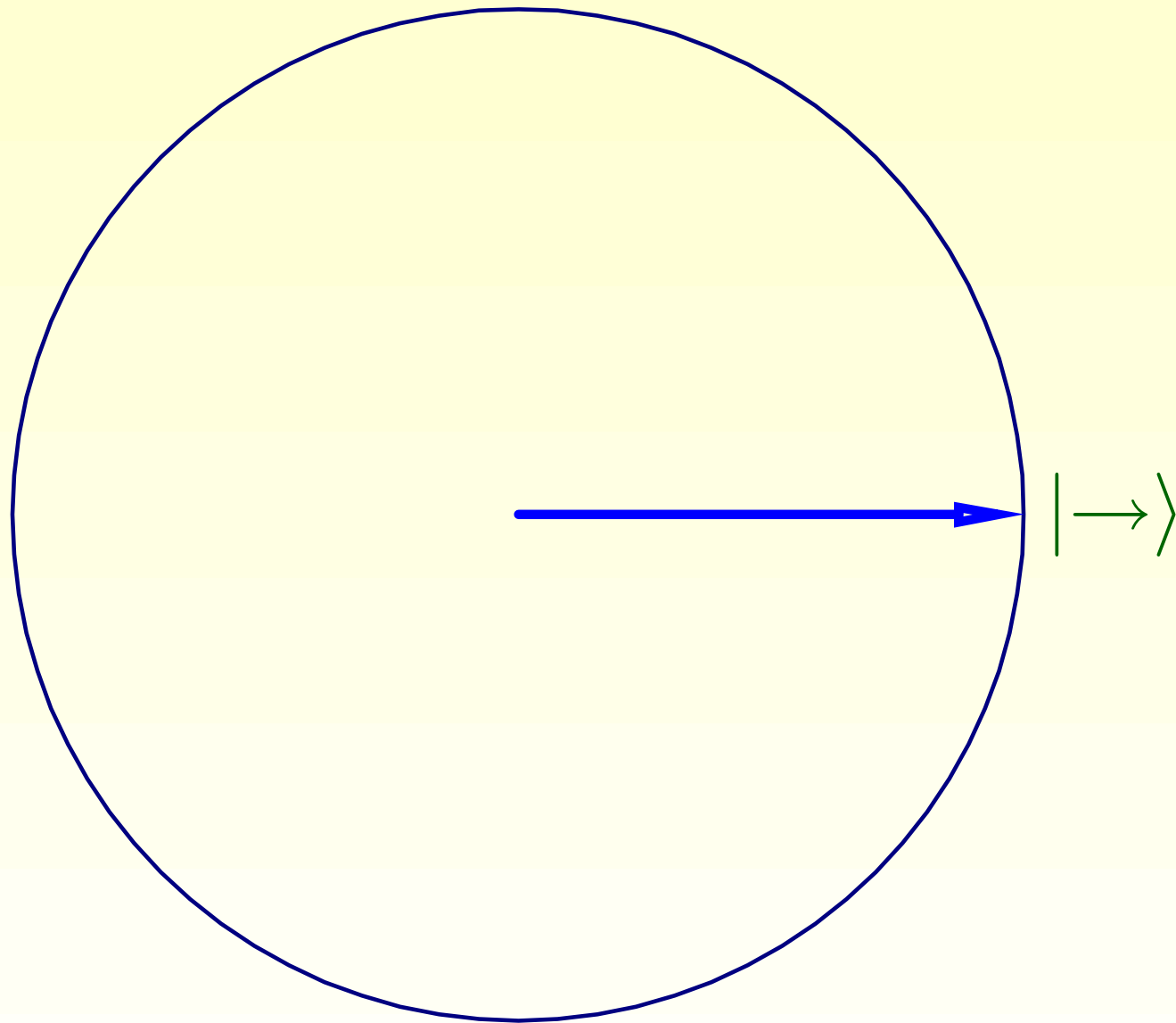
przechodzi przez polaryzator ustawiony poziomo i staje się fotonem w stanie $|\rightarrow\rangle$ z prawdopodobieństwem równym $|A_{(\rightarrow)}|^2$.



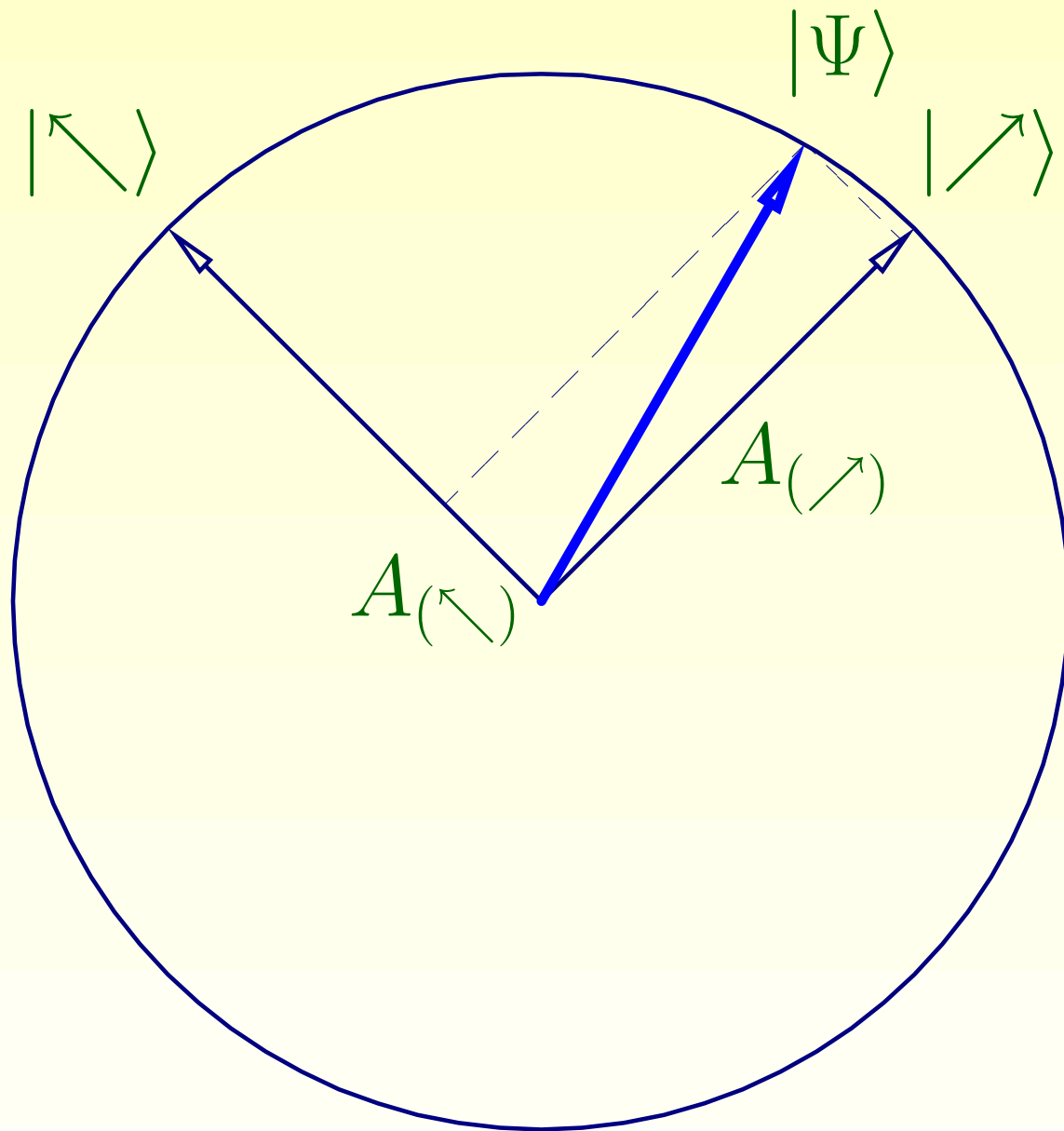
Baza prosta: $|\Psi\rangle = A_{(\rightarrow)} |\rightarrow\rangle + A_{(\uparrow)} |\uparrow\rangle$



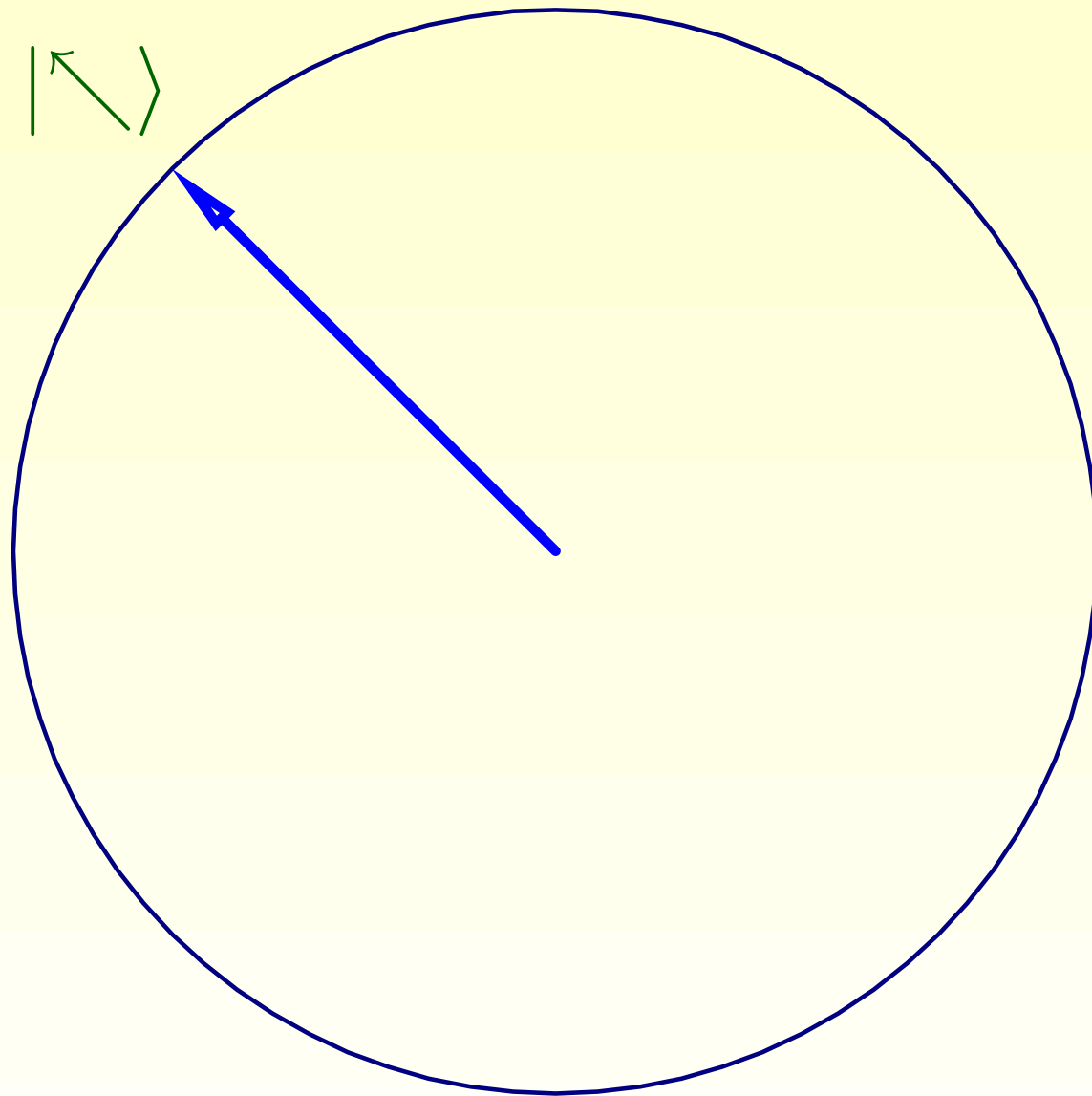
Pomiar $|\uparrow\rangle\langle\uparrow|$: $|\Psi\rangle \mapsto |\uparrow\rangle$, $P_{(\uparrow)} = |A_{(\uparrow)}|^2$



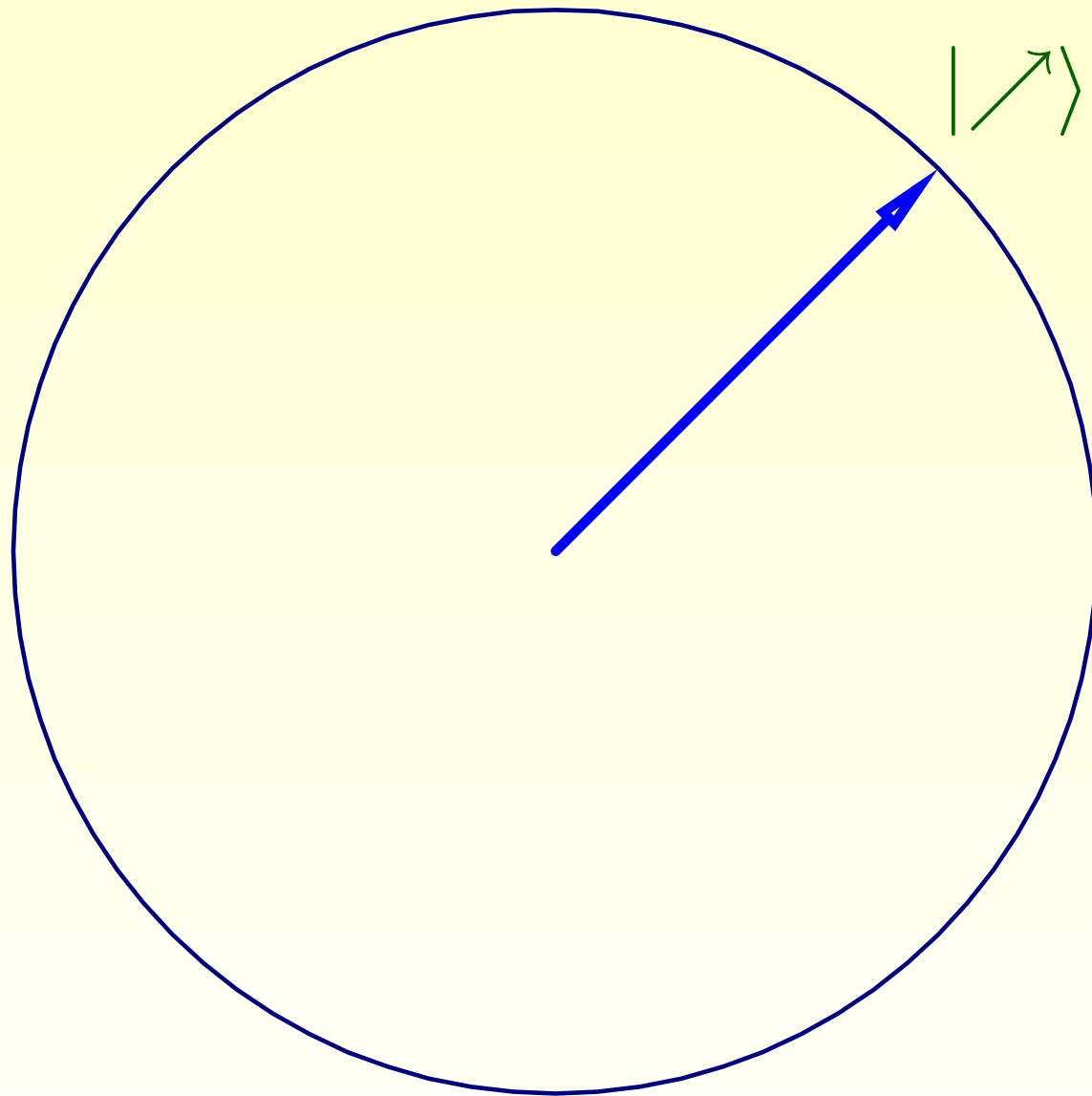
Pomiar $|\rightarrow\rangle\langle\rightarrow|$: $|\Psi\rangle \mapsto |\rightarrow\rangle$, $P_{(\rightarrow)} = |A_{(\rightarrow)}|^2$



Baza ukošna: $|\Psi\rangle = A_{(\nearrow)} |\nearrow\rangle + A_{(\nwarrow)} |\nwarrow\rangle$



Pomiar $|\nearrow\rangle\langle\nearrow|$: $|\Psi\rangle \mapsto |\nearrow\rangle$, $P_{(\nearrow)} = |A_{(\nearrow)}|^2$



Pomiar $|\nearrow\rangle\langle\nearrow|$: $|\Psi\rangle \mapsto |\nearrow\rangle$, $P_{(\nearrow)} = |A_{(\nearrow)}|^2$

Pomiar kwantowy zmienia stan kubitów!

Pomiar kwantowy zmienia stan kubit!

Taka zmiana jest **nieodwracalna!**

Pomiar kwantowy zmienia stan kubitu!

Taka zmiana jest **nieodwracalna!**

Pomiędzy pomiarami kubity mogą ewoluować w sposób **odwracalny!**

Pomiar kwantowy zmienia stan kubitu!

Taka zmiana jest **nieodwracalna!**

Pomiędzy pomiarami kubity mogą ewoluować w sposób **odwracalny!**

Trochę o ewolucji odwracalnej ...

3.2 Reguła Feynmana

W mechanice kwantowej dodają się amplitudy a nie prawdopodobieństwa.

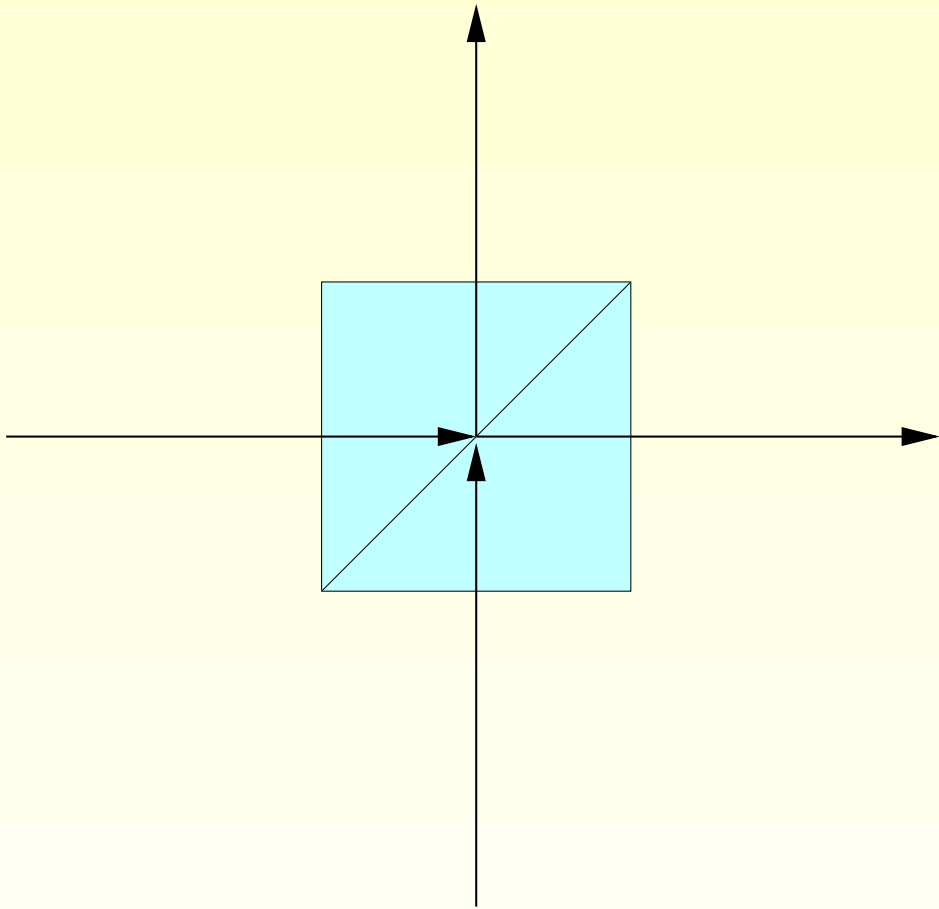


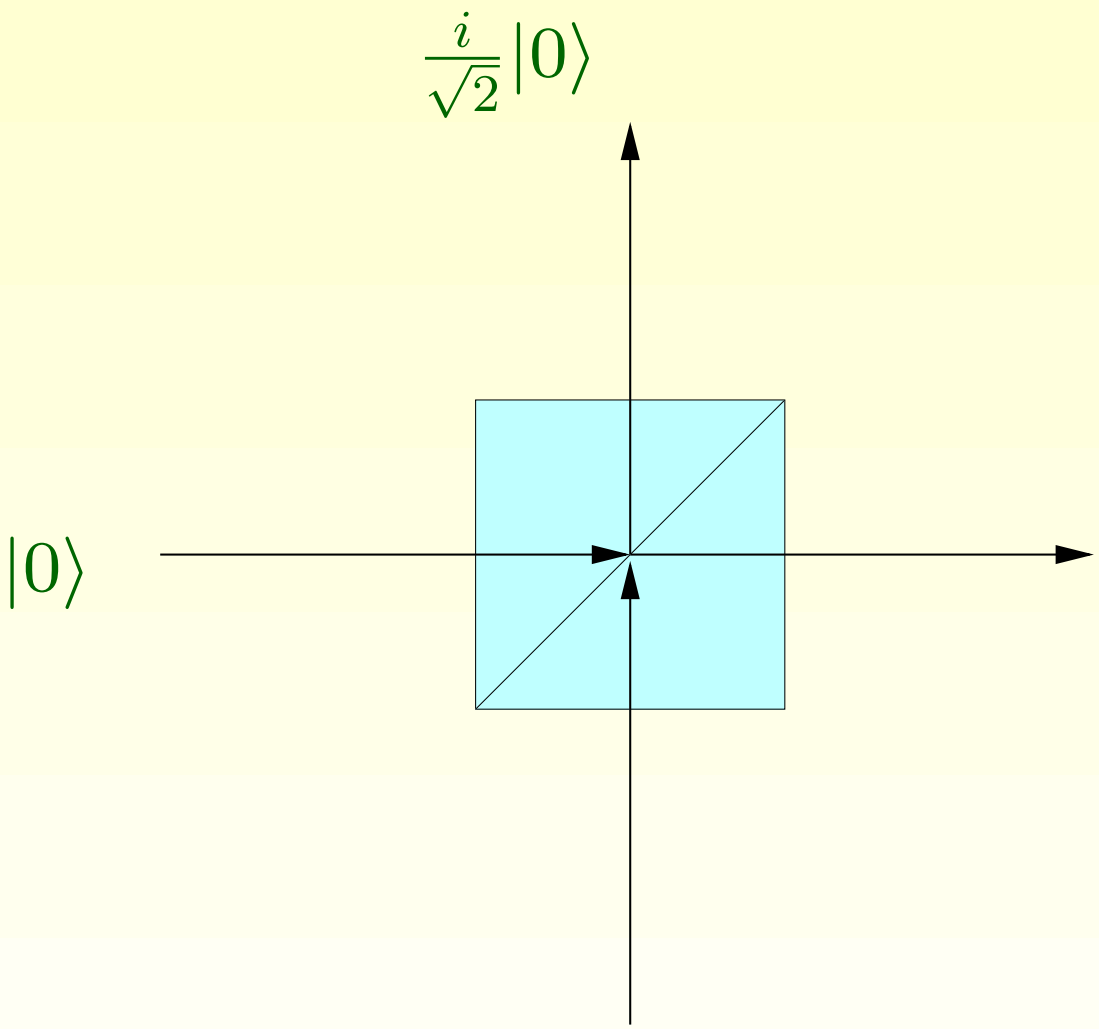
Richard P. Feynman (1918-1988)

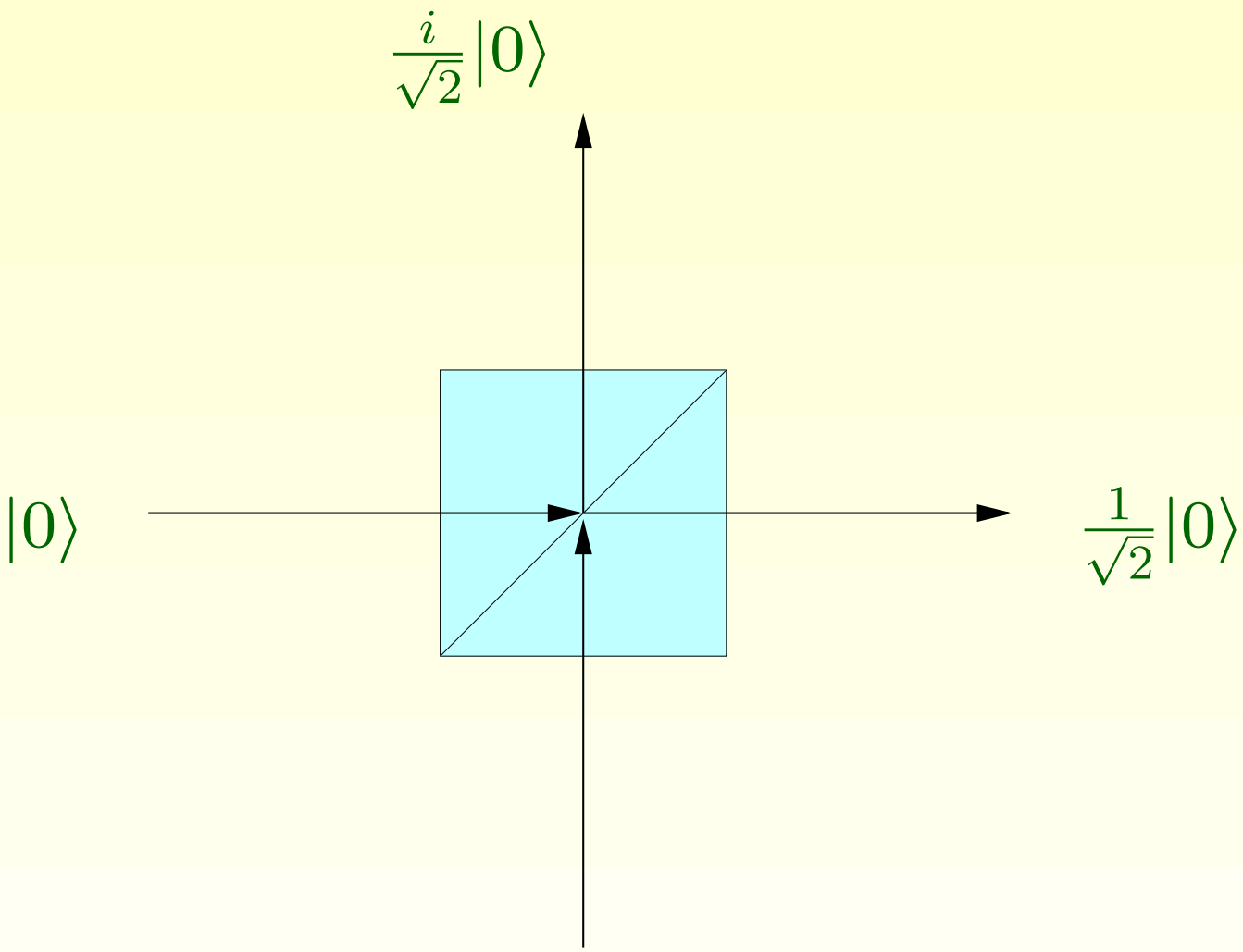
Tam na dole jest jeszcze dużo
miejsca!

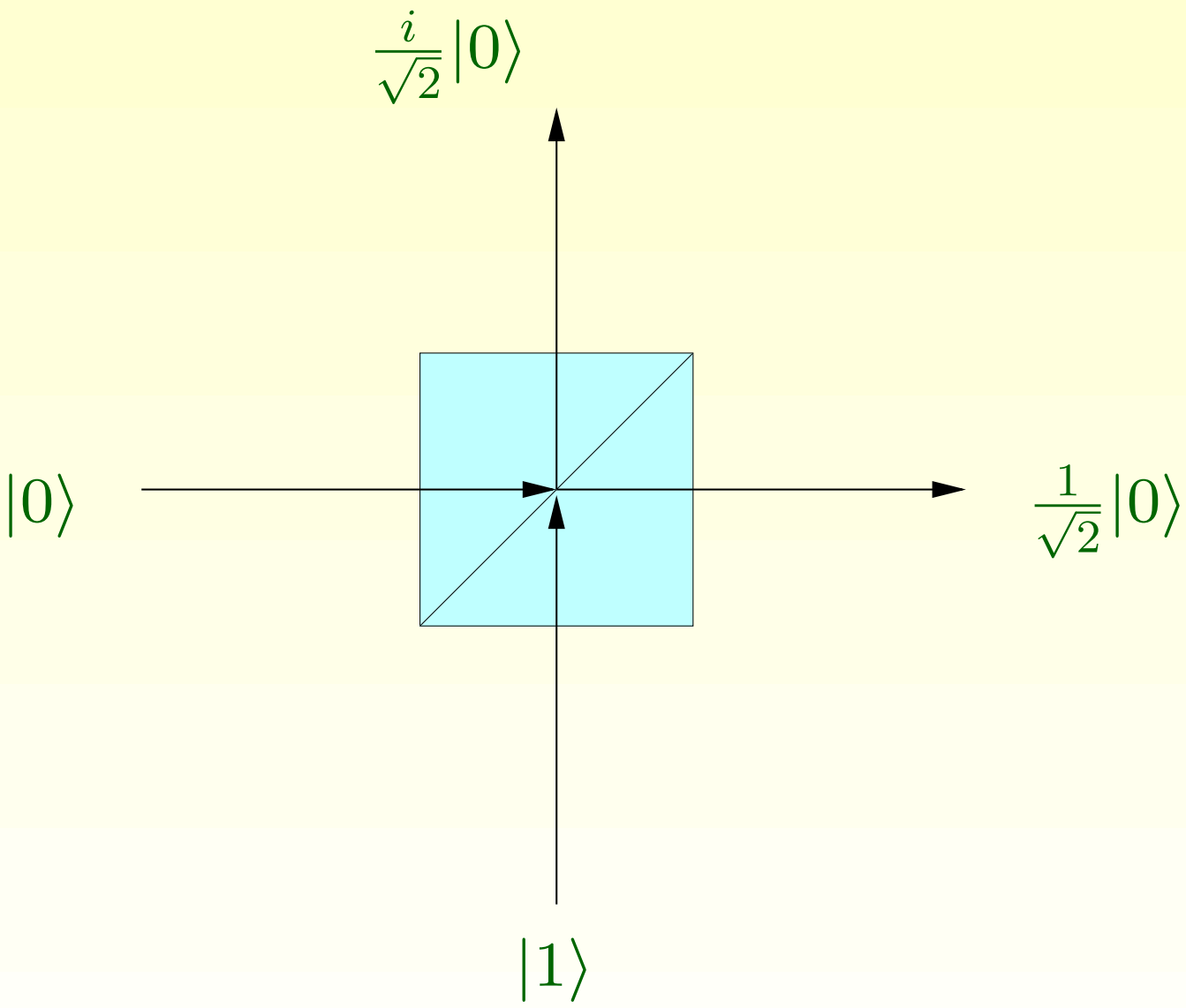
W 1982 r. Feynman pokazał, że nie da się symulować efektywnie procesów kwantowych na komputerach klasycznych.

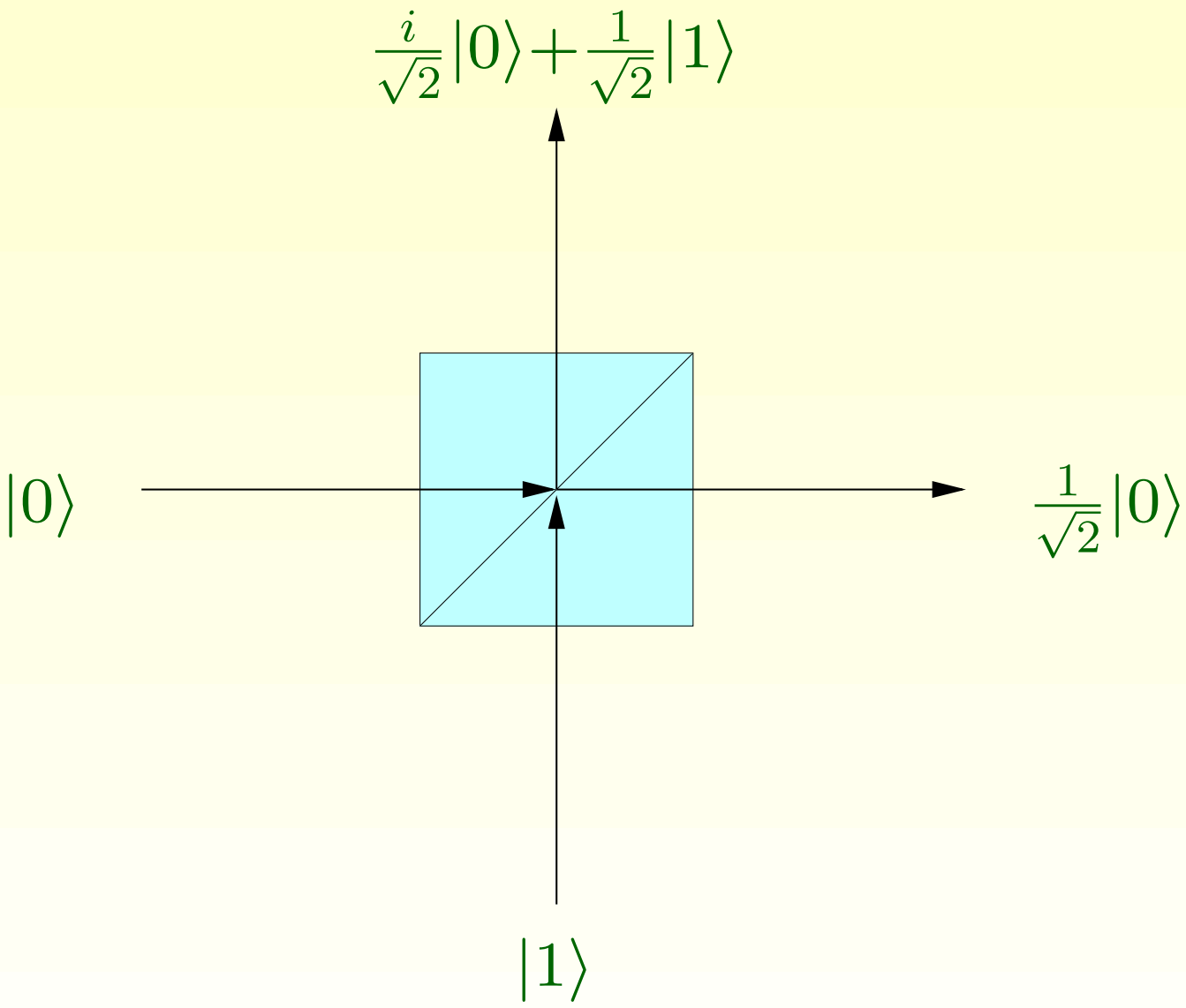
$|0\rangle$

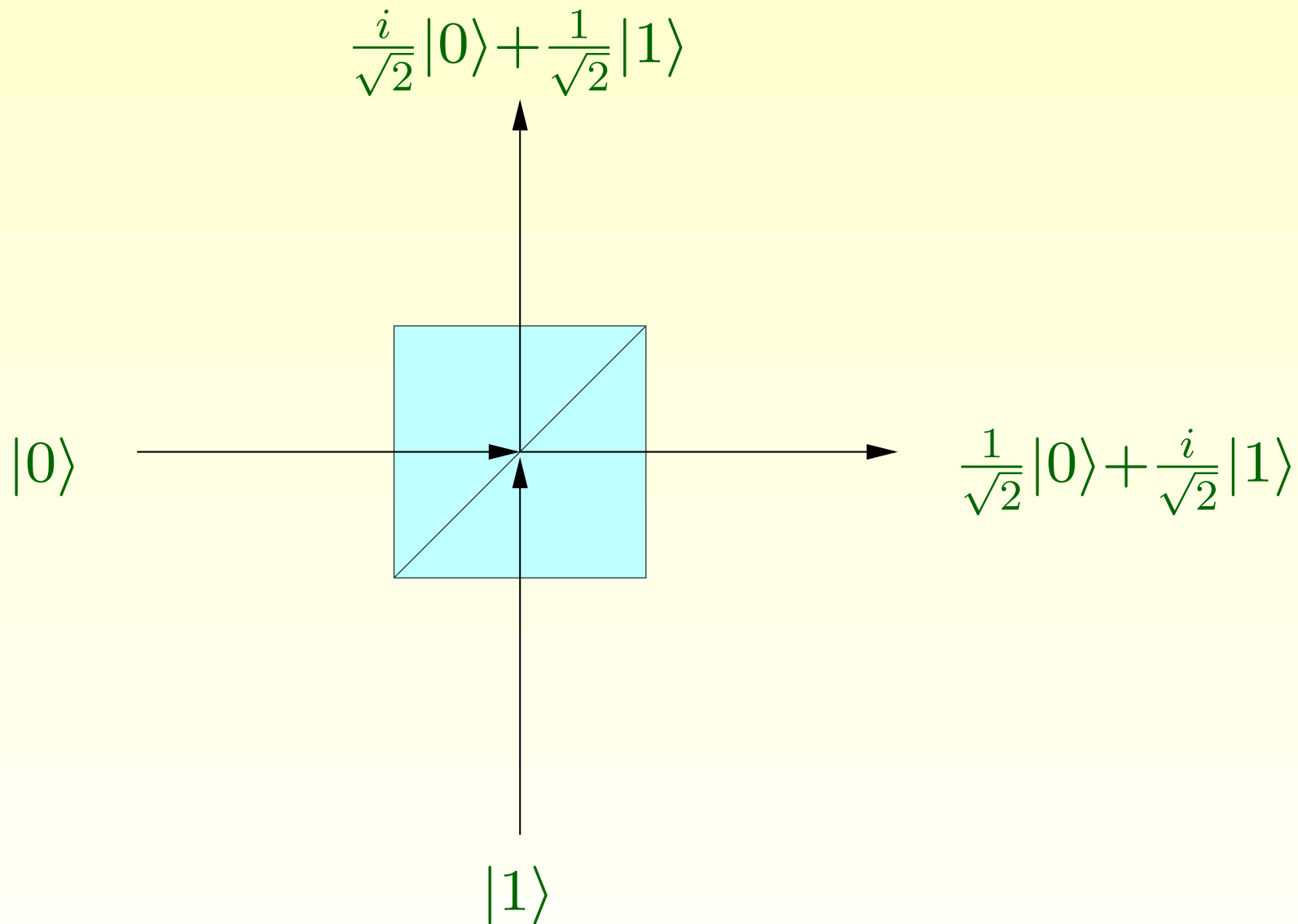




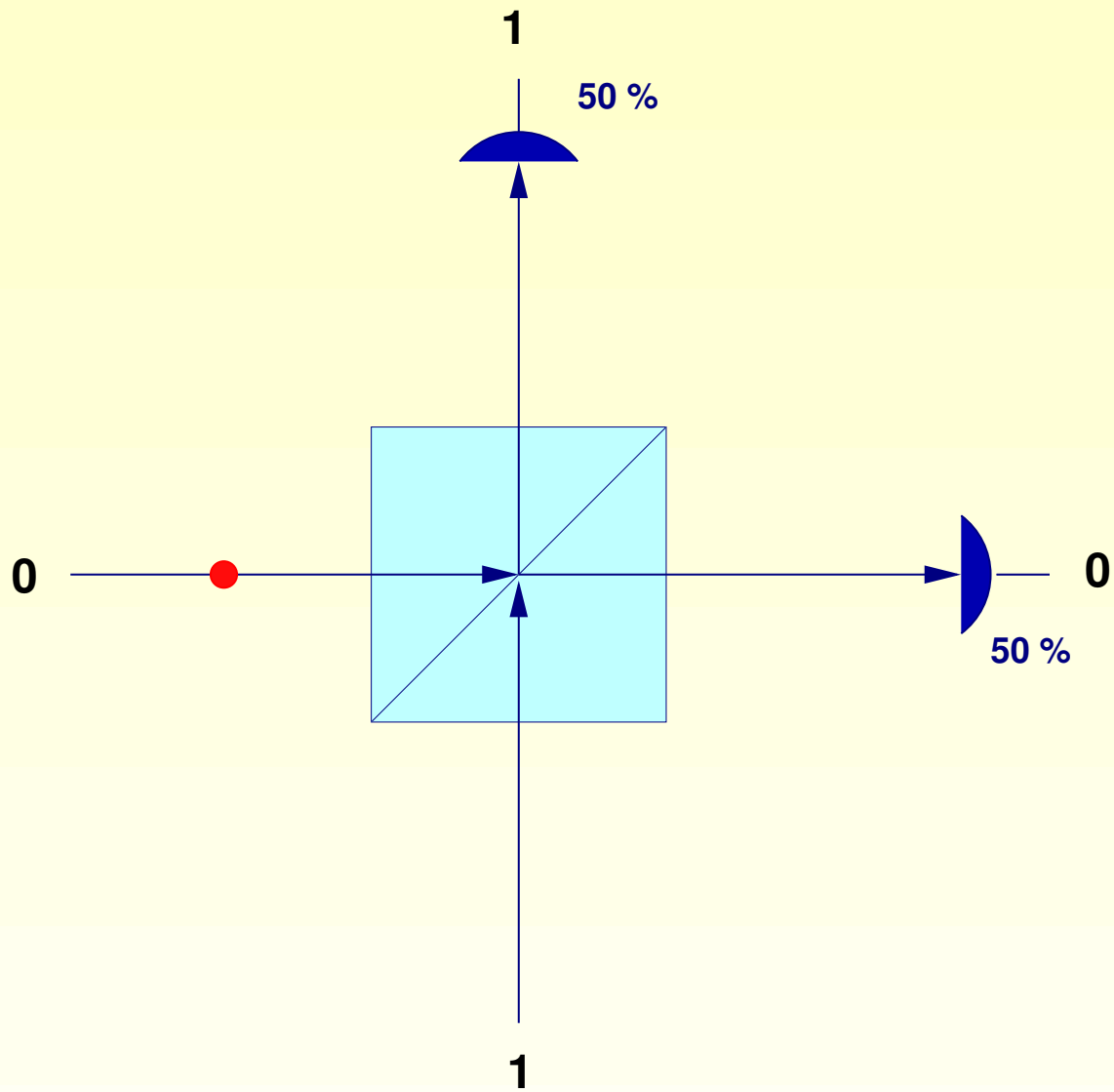




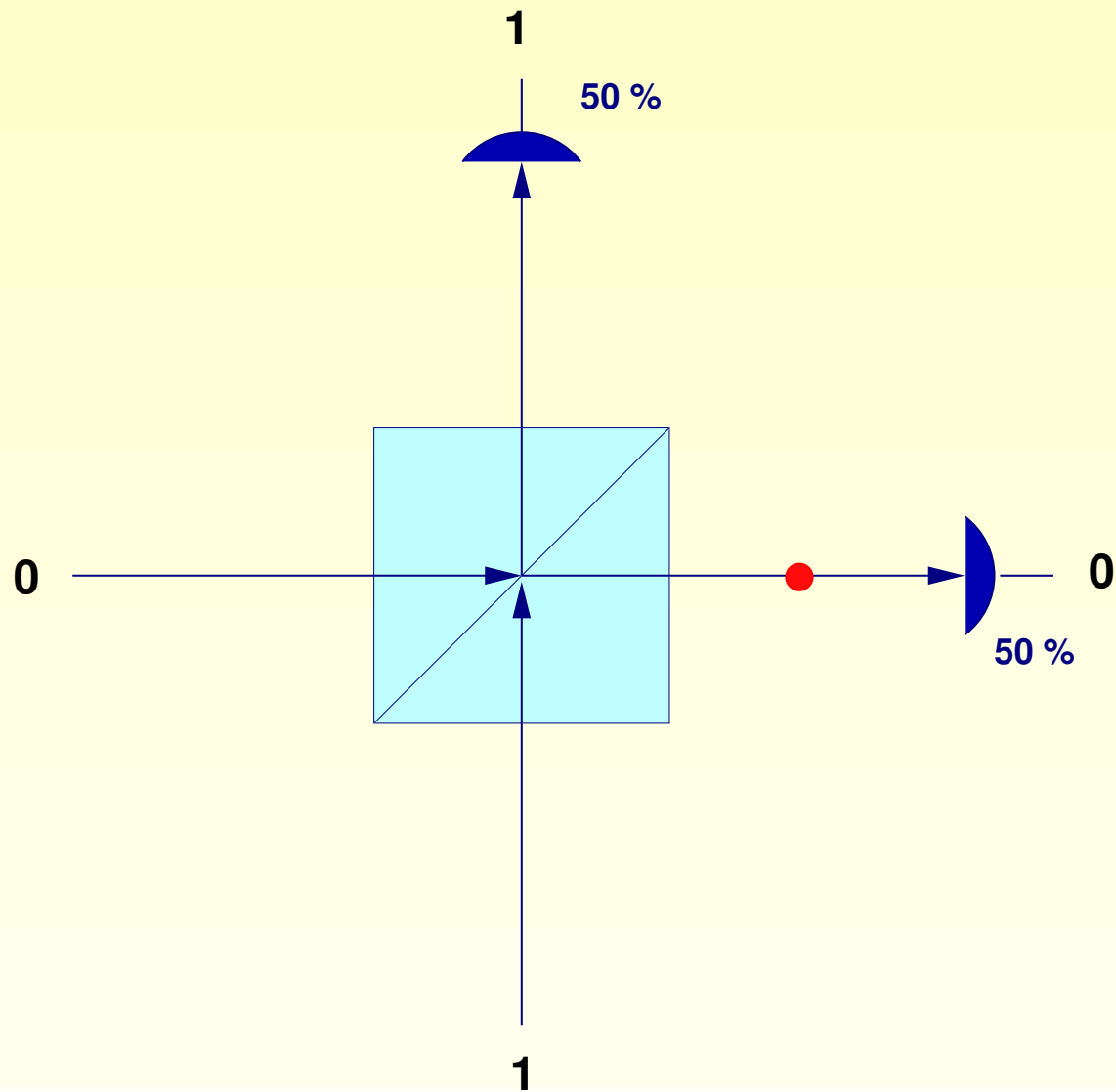




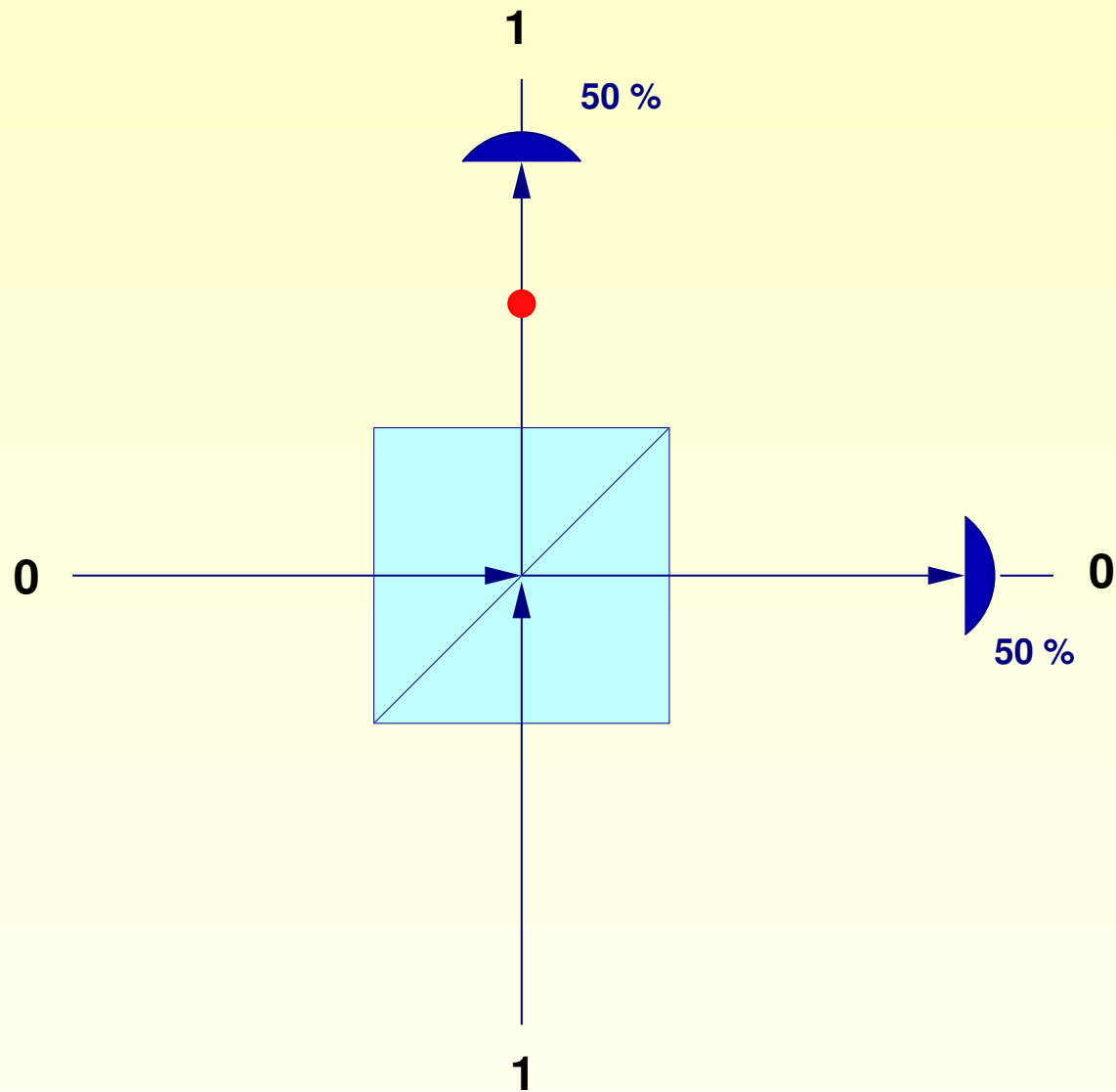
Płytką światłodzielną tworzy superpozycje stanów!



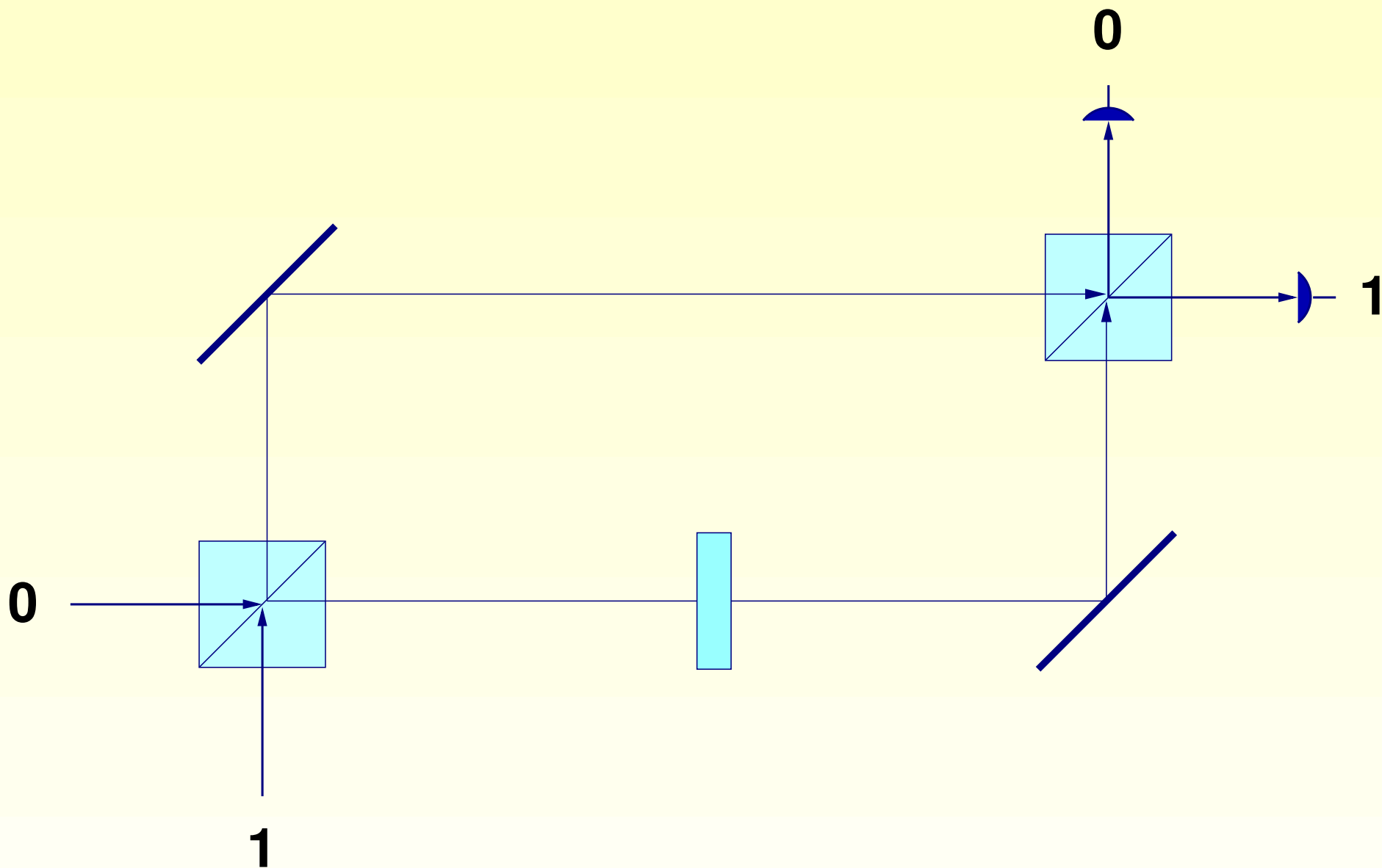
Foton padający drogą 0 ...



z prawdopodobieństwem 50% zostanie zarejestrowany przez detektor 0...

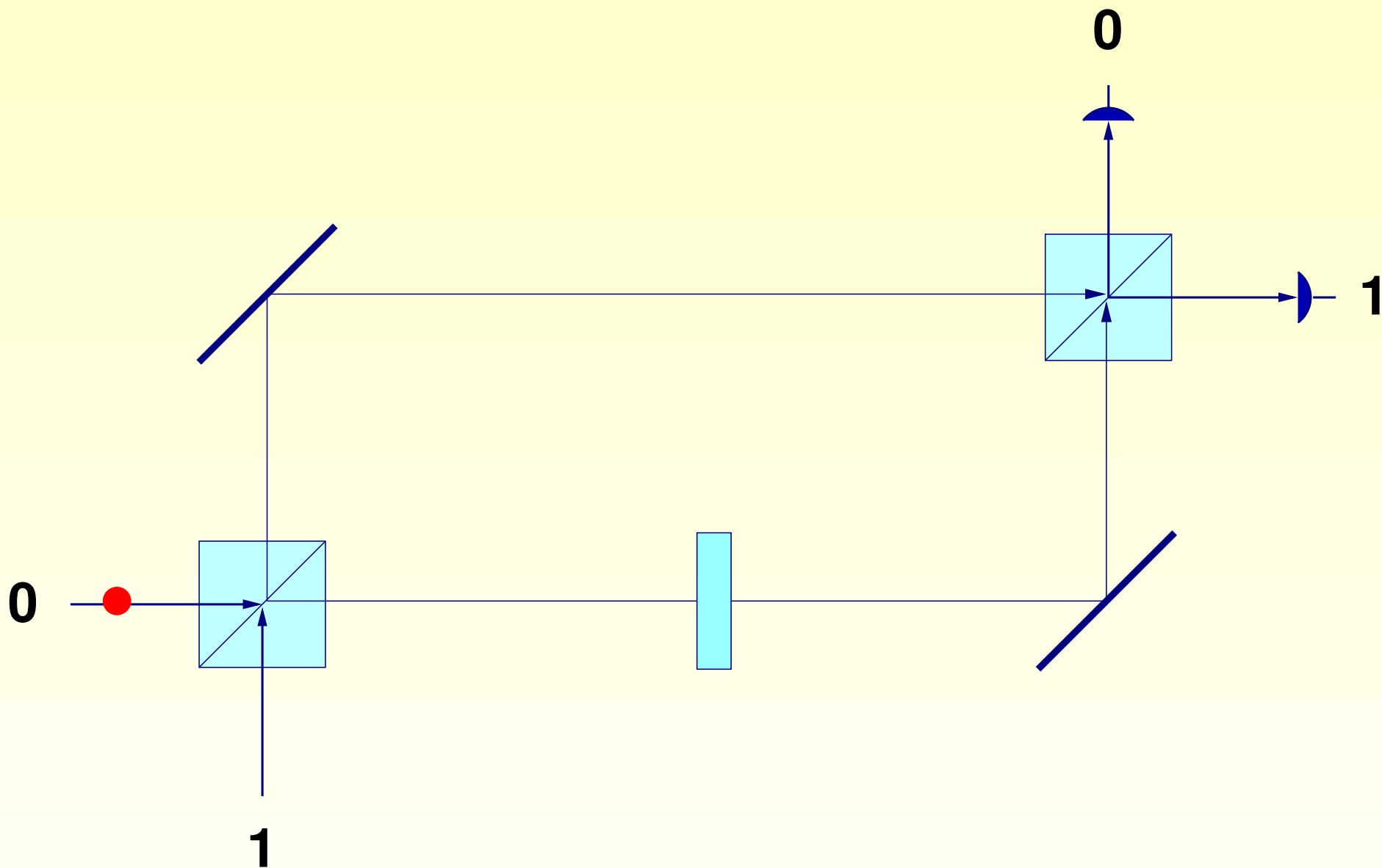


lub przez detektor 1
Pomiar niszczy superpozycję!



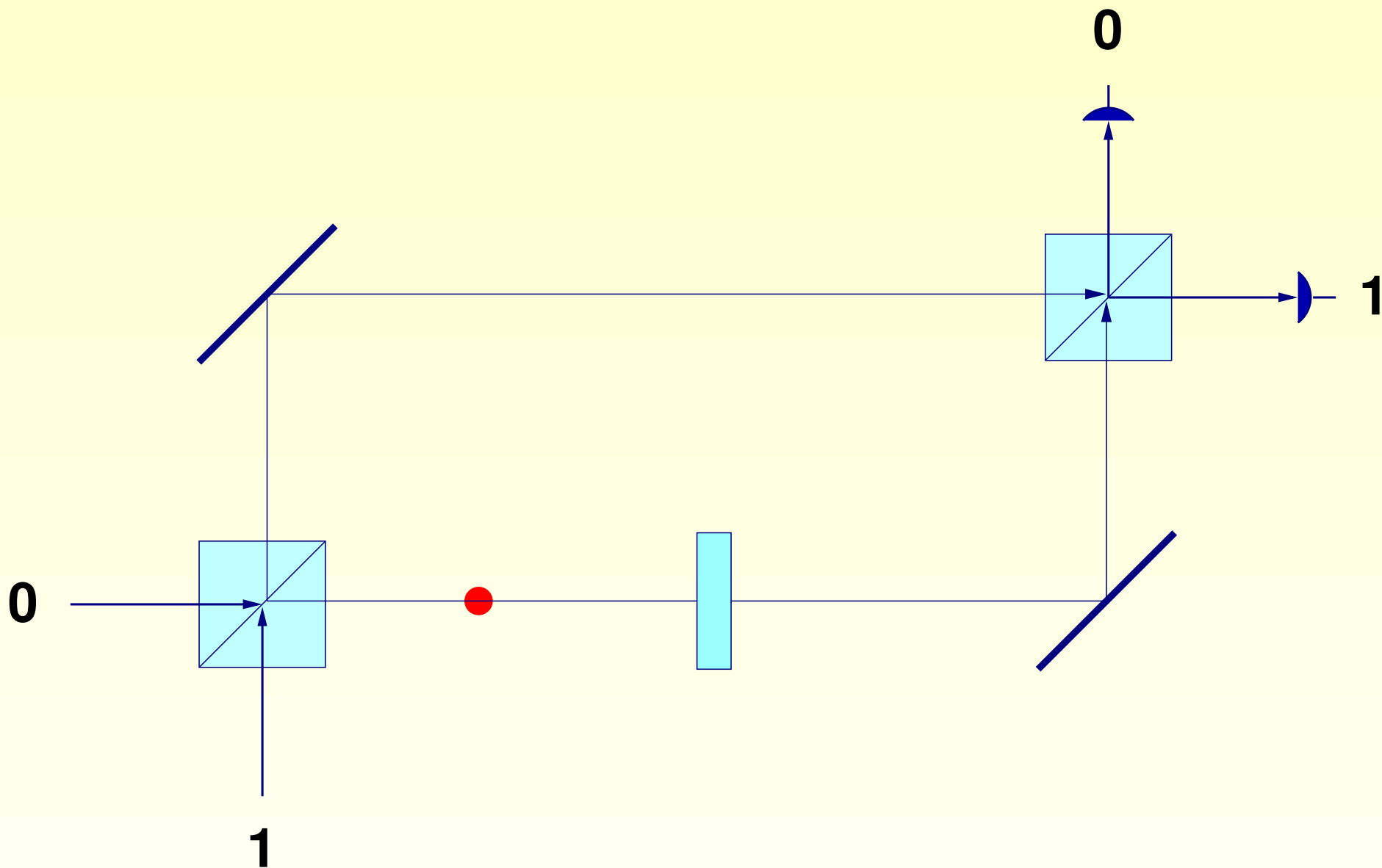
Interferometr Macha-Zehndera

Dwie płytki, pomiaru dokonujemy po drugiej płytce.



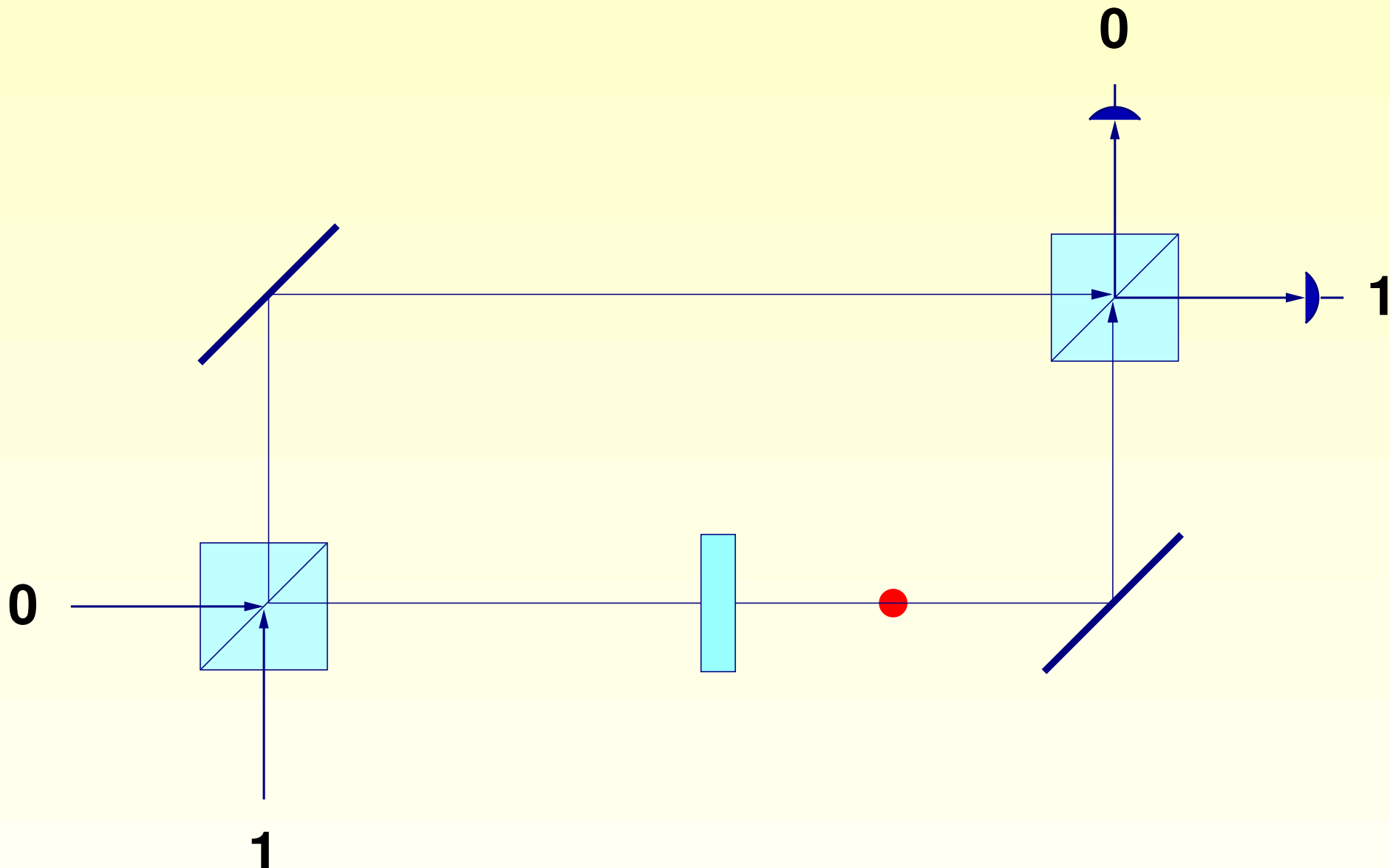
Dodajemy amplitudy!

Foton padający drogą 0 jest kubitem w stanie $|0\rangle$



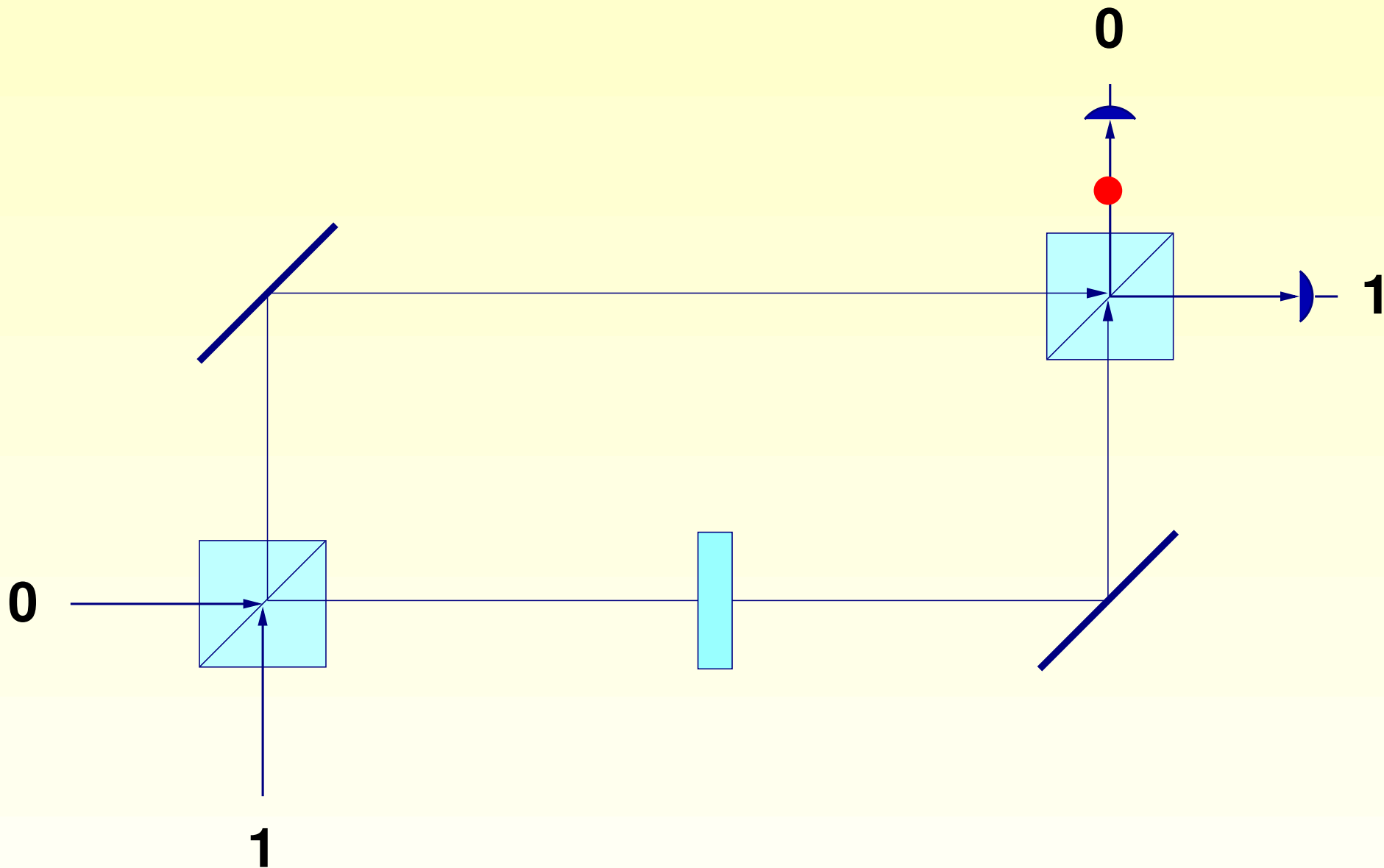
Przejdźcie przez pierwszą płytkę:

$$\frac{1}{\sqrt{2}} \dots$$



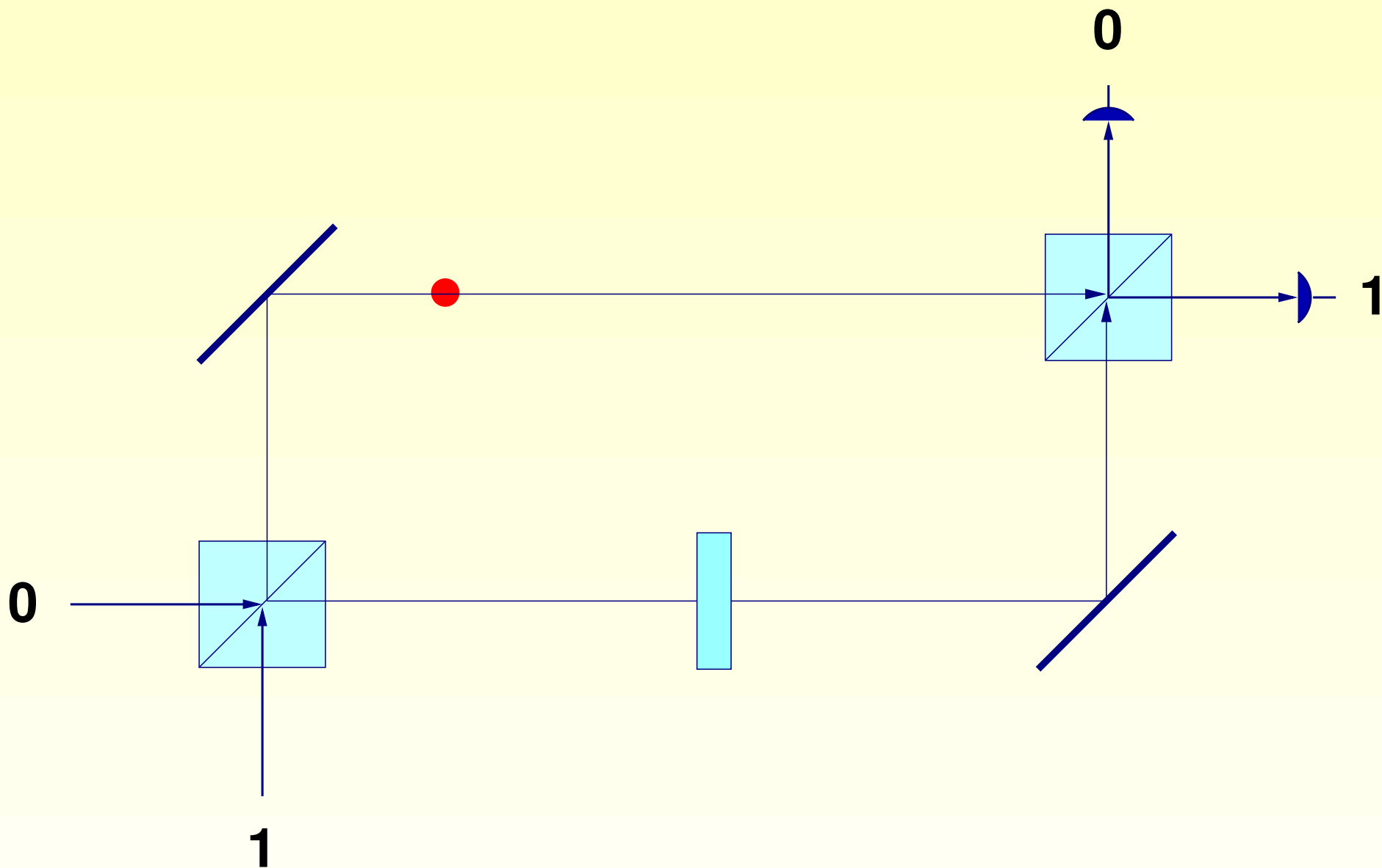
Zmiana fazy:

$$\frac{e^{i\theta}}{\sqrt{2}} \dots$$



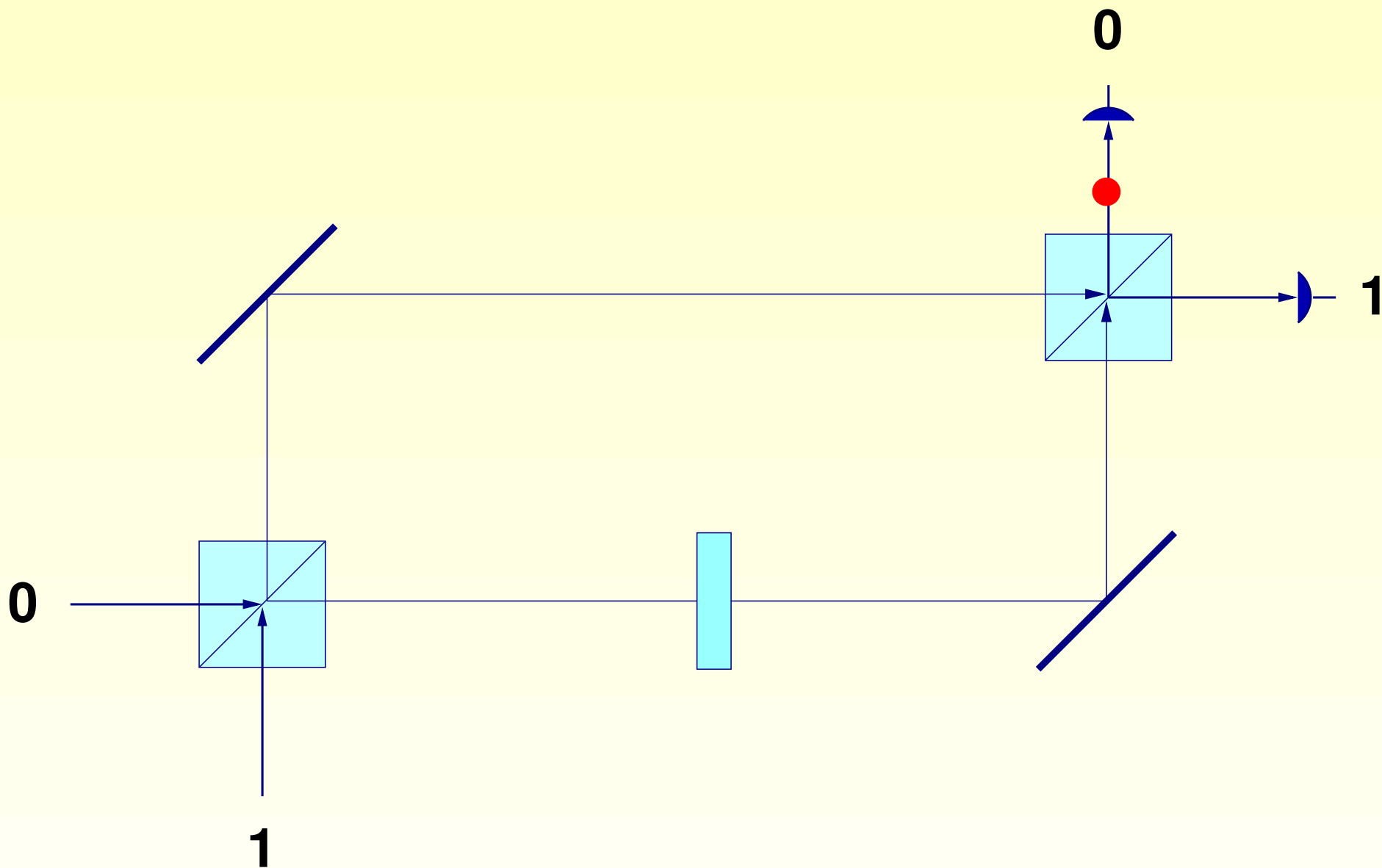
Przejsie przez drugą płytke:

$$\frac{e^{i\theta}}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \dots$$



Dodajemy druga drogę. Odbicie na pierwszej płytce:

$$\frac{1}{\sqrt{2}} \cdot \frac{e^{i\theta}}{\sqrt{2}} + \frac{i}{\sqrt{2}} \dots$$



I znowu odbicie:

$$\frac{1}{\sqrt{2}} \cdot \frac{e^{i\theta}}{\sqrt{2}} + \frac{i}{\sqrt{2}} \cdot \frac{i}{\sqrt{2}} = \frac{1}{2}(e^{i\theta} - 1)$$

Amplituda stanu $|0\rangle$ w detektorze 0 jest równa

$$A_0 = \frac{1}{2}(e^{i\theta} - 1)$$

Amplituda stanu $|0\rangle$ w detektorze 0 jest równa

$$A_0 = \frac{1}{2}(e^{i\theta} - 1)$$

Prawdopodobieństwo zarejestrowania w detektorze 0 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_0 = \left| \frac{1}{2}(e^{i\theta} - 1) \right|^2 = \frac{1}{2}(1 - \cos \theta)$$

Amplituda stanu $|0\rangle$ w detektorze 0 jest równa

$$A_0 = \frac{1}{2}(e^{i\theta} - 1)$$

Prawdopodobieństwo zarejestrowania w detektorze 0 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_0 = \left| \frac{1}{2}(e^{i\theta} - 1) \right|^2 = \frac{1}{2}(1 - \cos \theta)$$

Dla $\theta = 0$ prawdopodobieństwo to jest równe zero.

Amplituda stanu $|0\rangle$ w detektorze 0 jest równa

$$A_0 = \frac{1}{2}(e^{i\theta} - 1)$$

Prawdopodobieństwo zarejestrowania w detektorze 0 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_0 = \left| \frac{1}{2}(e^{i\theta} - 1) \right|^2 = \frac{1}{2}(1 - \cos \theta)$$

Dla $\theta = 0$ prawdopodobieństwo to jest równe zero.

Foton nigdy nie trafi do detektora 0!

Amplituda stanu $|0\rangle$ w detektorze 0 jest równa

$$A_0 = \frac{1}{2}(e^{i\theta} - 1)$$

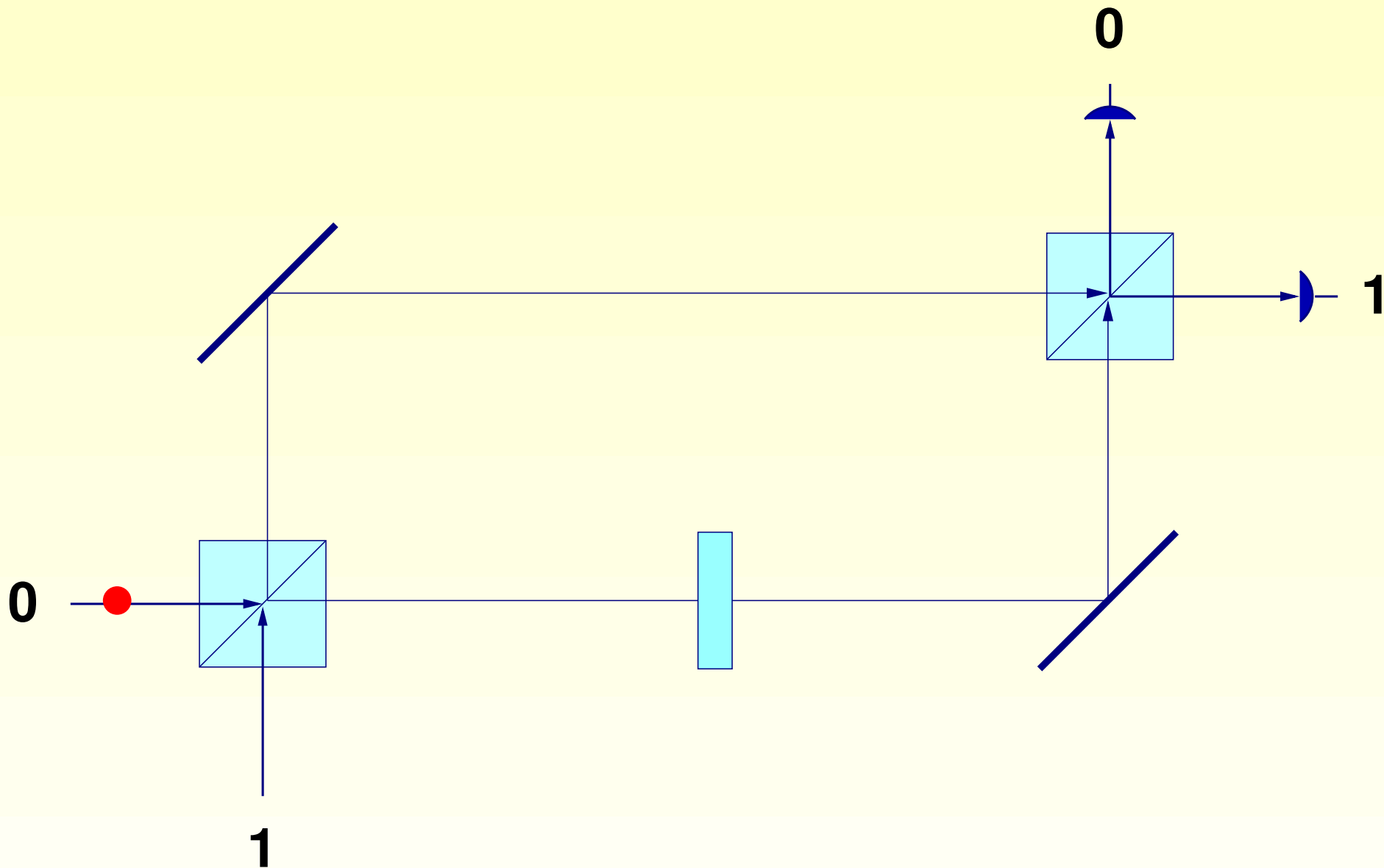
Prawdopodobieństwo zarejestrowania w detektorze 0 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_0 = \left| \frac{1}{2}(e^{i\theta} - 1) \right|^2 = \frac{1}{2}(1 - \cos \theta)$$

Dla $\theta = 0$ prawdopodobieństwo to jest równe zero.

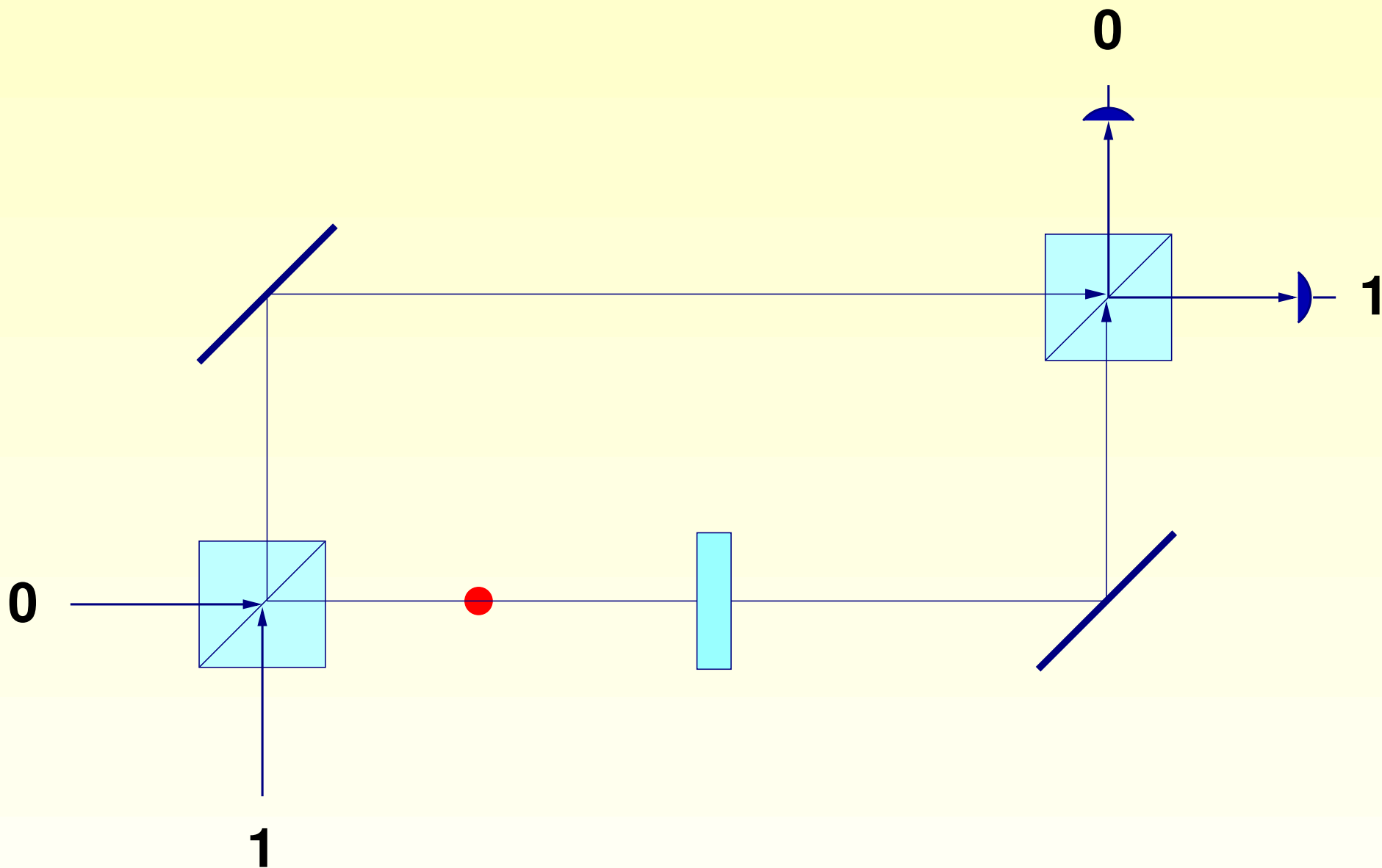
Foton nigdy nie trafi do detektora 0!

Zmieniając fazę θ możemy dowolnie zmieniać prawdopodobieństwo.



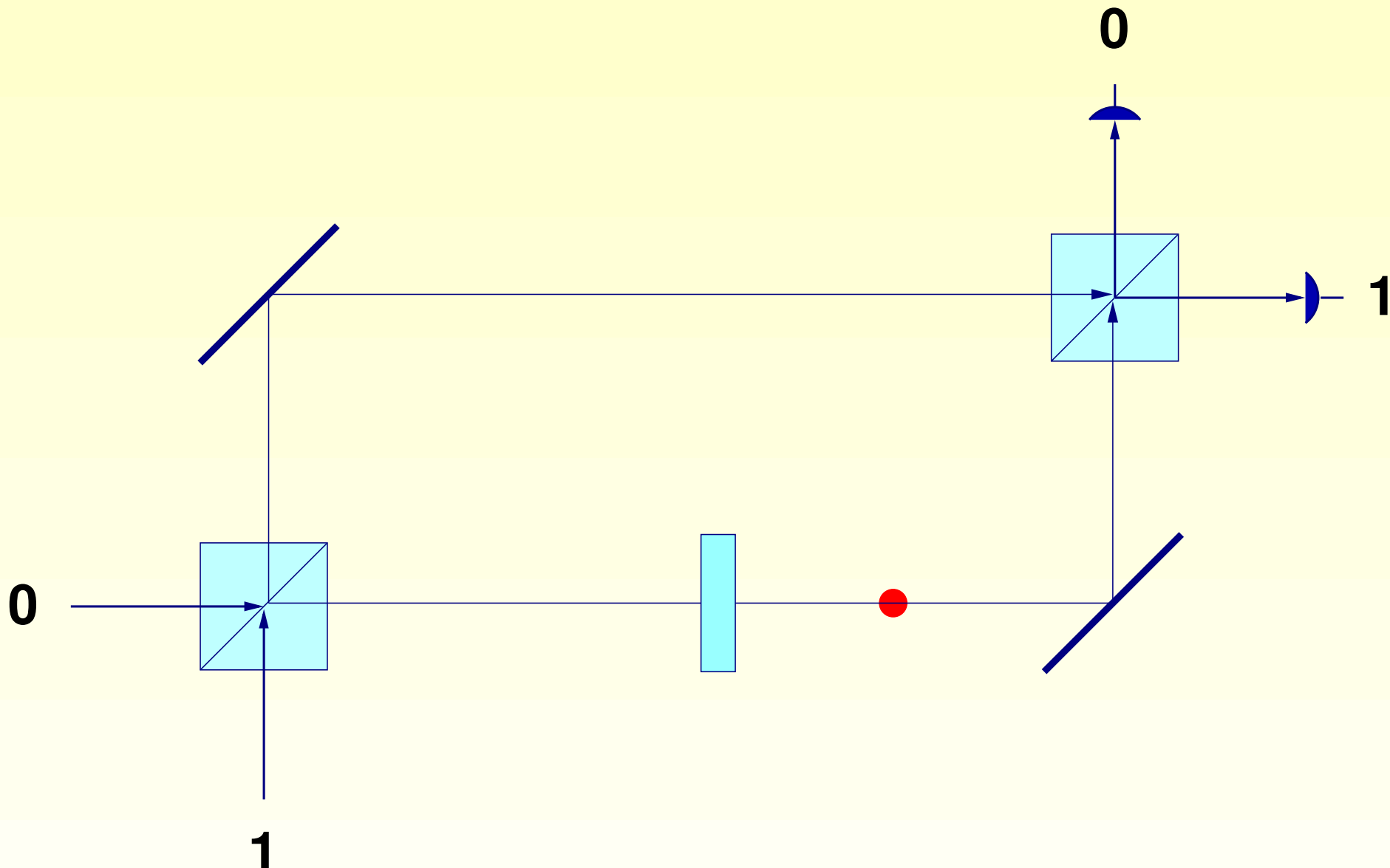
Teraz detektor 1.

Znowu, foton padający drogą 0



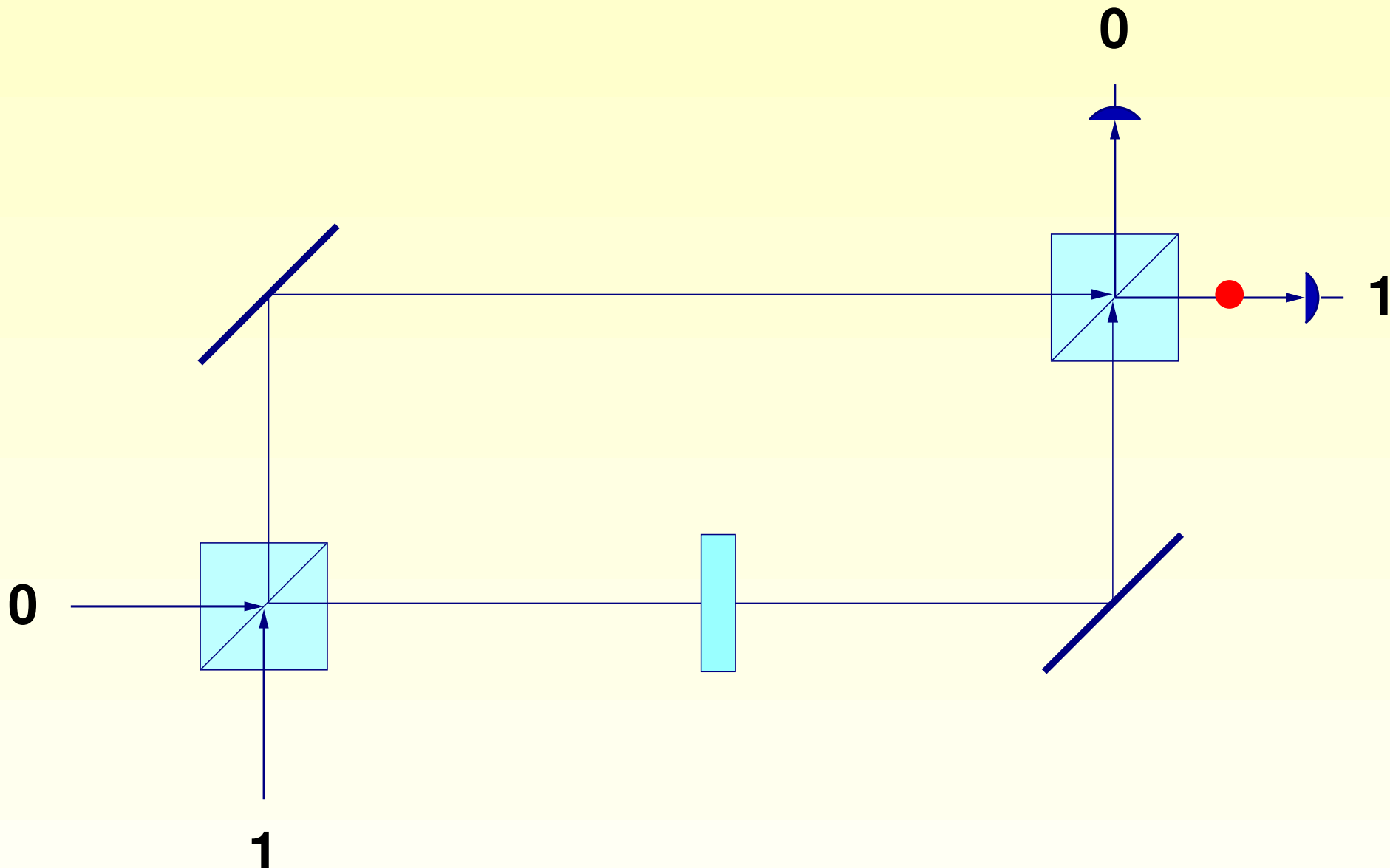
Przejdźcie przez pierwszą płytkę:

$$\frac{1}{\sqrt{2}} \dots$$



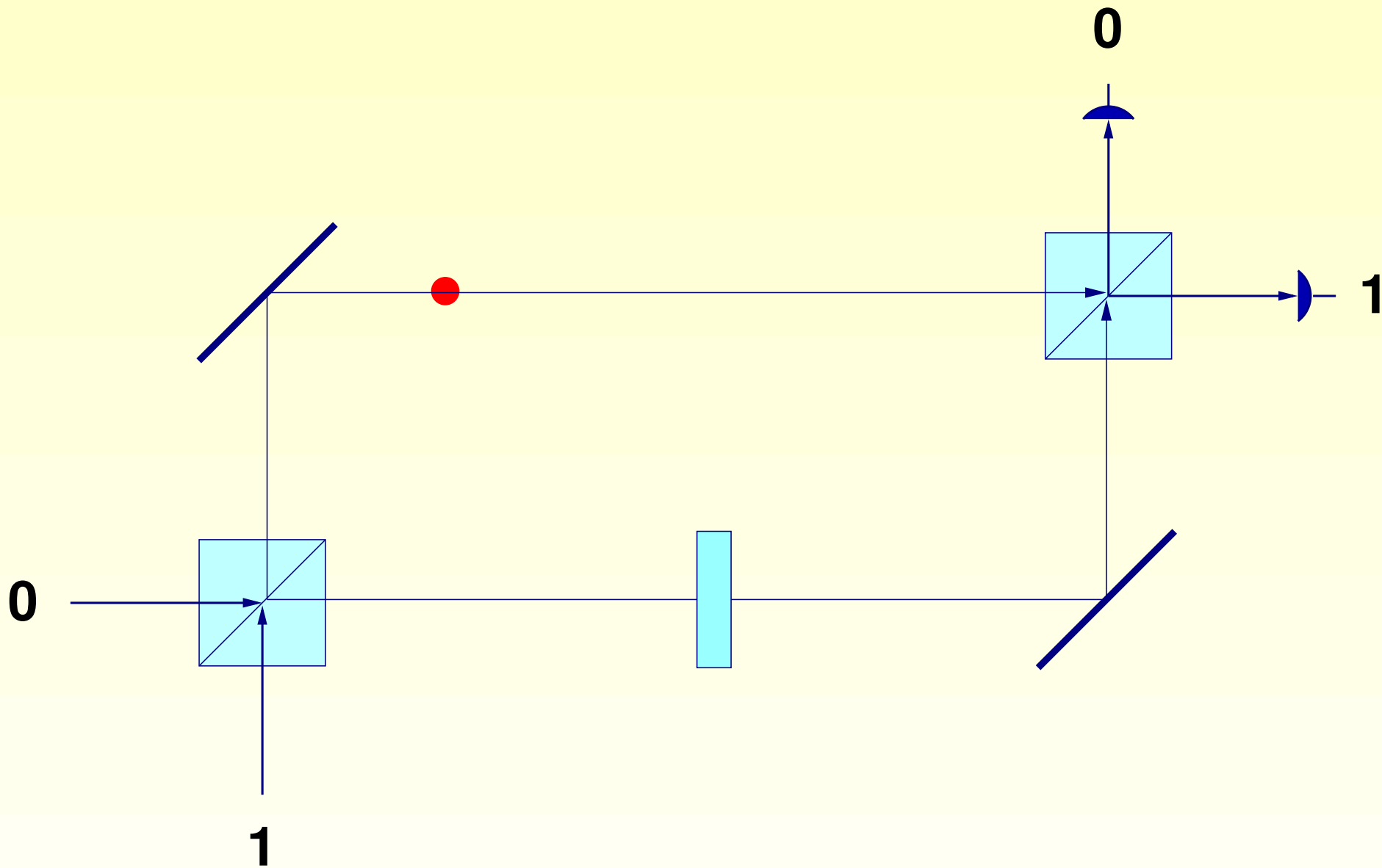
Zmiana fazy:

$$\frac{e^{i\theta}}{\sqrt{2}} \dots$$



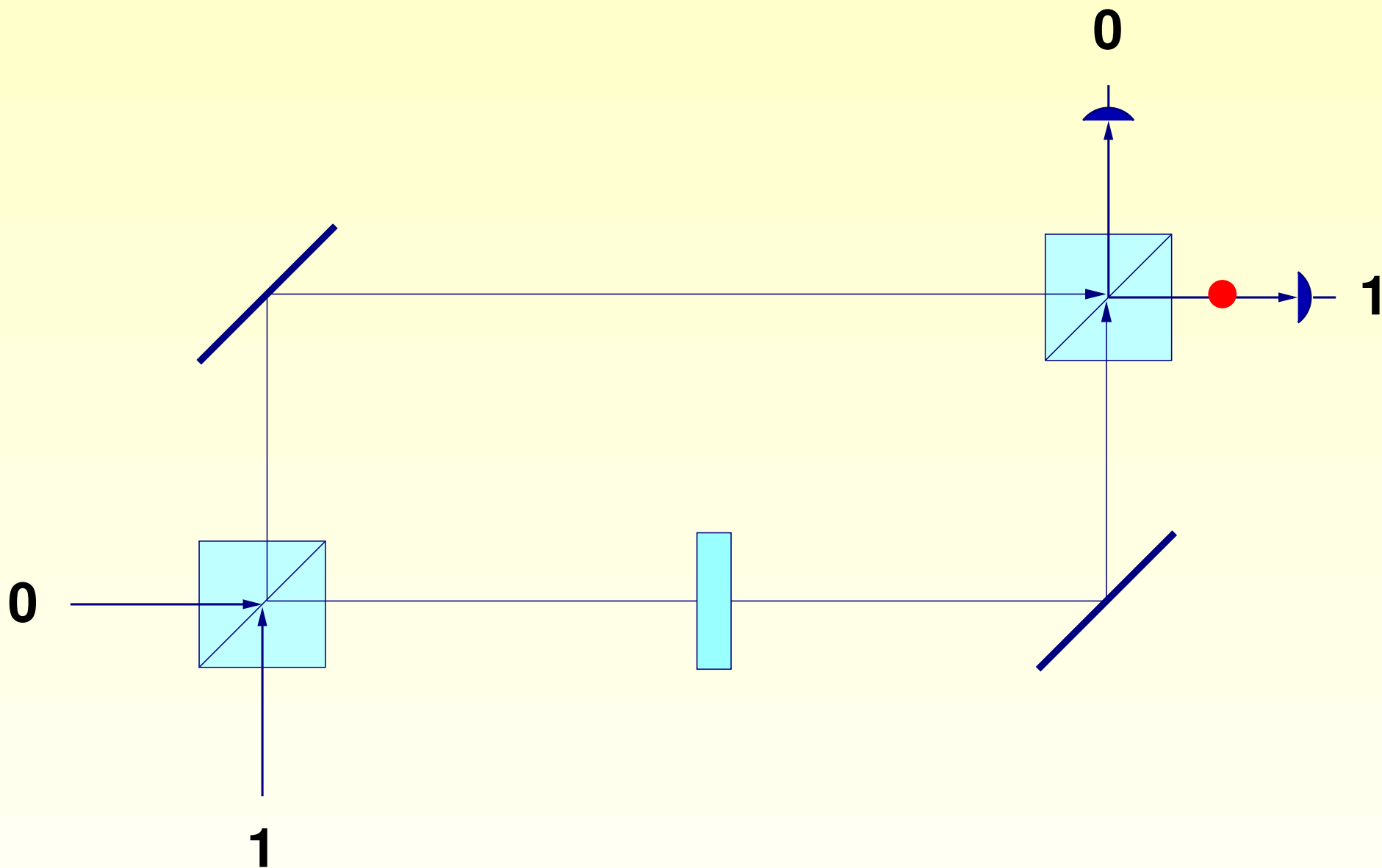
Odbicie:

$$\frac{e^{i\theta}}{\sqrt{2}} \cdot \frac{i}{\sqrt{2}} \dots$$



I druga droga. Odbicie:

$$\frac{e^{i\theta}}{\sqrt{2}} \cdot \frac{i}{\sqrt{2}} + \frac{i}{\sqrt{2}} \dots$$



Przejście:

$$\frac{e^{i\theta}}{\sqrt{2}} \cdot \frac{i}{\sqrt{2}} + \frac{i}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} = \frac{i}{2} (e^{i\theta} + 1)$$

Amplituda stanu $|0\rangle$ w detektorze 1 jest równa

$$A_1 = \frac{i}{2}(e^{i\theta} + 1)$$

Amplituda stanu $|0\rangle$ w detektorze 1 jest równa

$$A_1 = \frac{i}{2}(e^{i\theta} + 1)$$

Prawdopodobieństwo zarejestrowania w detektorze 1 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_1 = \left| \frac{i}{2}(e^{i\theta} + 1) \right|^2 = \frac{1}{2}(1 + \cos \theta)$$

Amplituda stanu $|0\rangle$ w detektorze 1 jest równa

$$A_1 = \frac{i}{2}(e^{i\theta} + 1)$$

Prawdopodobieństwo zarejestrowania w detektorze 1 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_1 = \left| \frac{i}{2}(e^{i\theta} + 1) \right|^2 = \frac{1}{2}(1 + \cos \theta)$$

Dla $\theta = 0$ prawdopodobieństwo to jest równe jeden.
Foton zawsze trafi do detektora 1!

Amplituda stanu $|0\rangle$ w detektorze 1 jest równa

$$A_1 = \frac{i}{2}(e^{i\theta} + 1)$$

Prawdopodobieństwo zarejestrowania w detektorze 1 fotonu, który wpadł drogą 0 do interferometru wynosi więc:

$$P_1 = \left| \frac{i}{2}(e^{i\theta} + 1) \right|^2 = \frac{1}{2}(1 + \cos \theta)$$

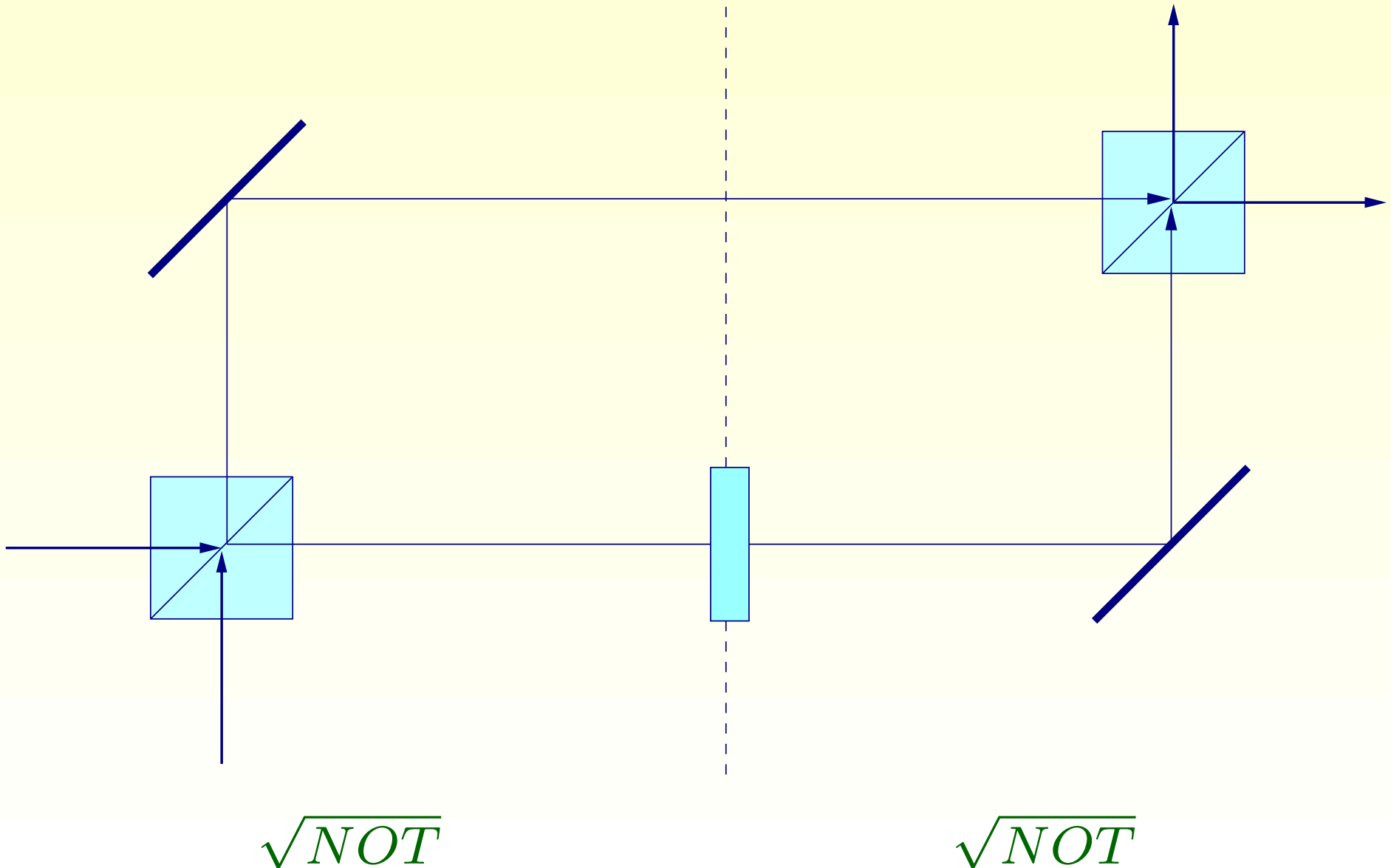
Dla $\theta = 0$ prawdopodobieństwo to jest równe jeden.

Foton zawsze trafi do detektora 1!

Interferometr Macha-Zehndera działa jak bramka logiczna *NOT*.

Skoro cały interferometr to bramka logiczna *NOT*, to jedna płytką światłodzielącą to \sqrt{NOT} !

$$\sqrt{NOT} \cdot \sqrt{NOT} = NOT$$



Interferencja kwantowa pozwala uzyskać operacje „logiczne” niedostępne w informatyce klasycznej

Interferencja kwantowa pozwala uzyskać operacje „logiczne” niedostępne w informatyce klasycznej

Czy takie nielogiczne bramki logiczne mogą się do czegoś przydać?

Interferencja kwantowa pozwala uzyskać operacje „logiczne” niedostępne w informatyce klasycznej

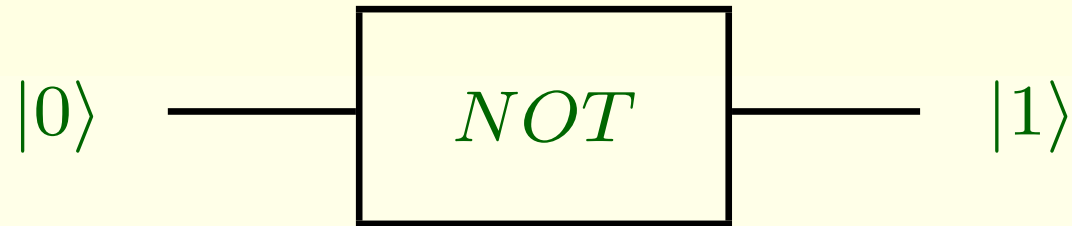
Czy takie nielogiczne bramki logiczne mogą się do czegoś przydać?

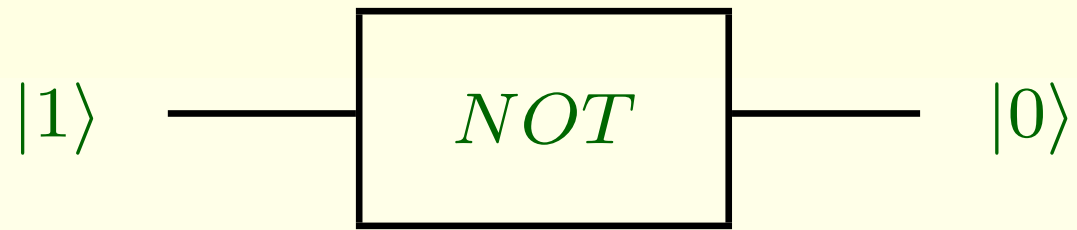
Okazuje się, że tak!

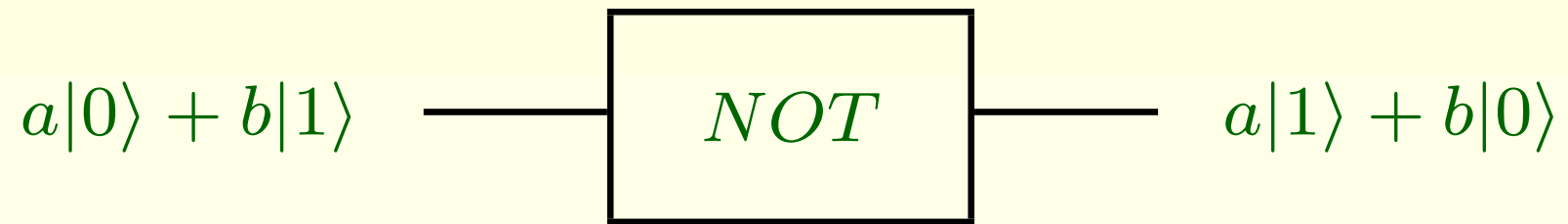


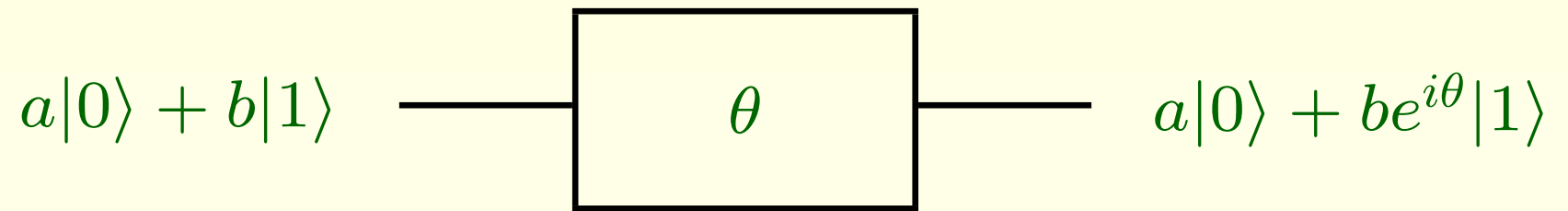
Kwantowa interferencja?!

3.3 Kwantowe, czyli nielogiczne bramki logiczne

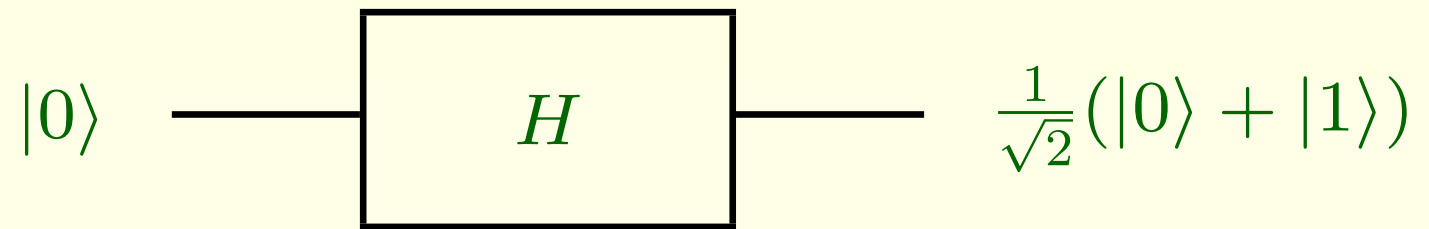




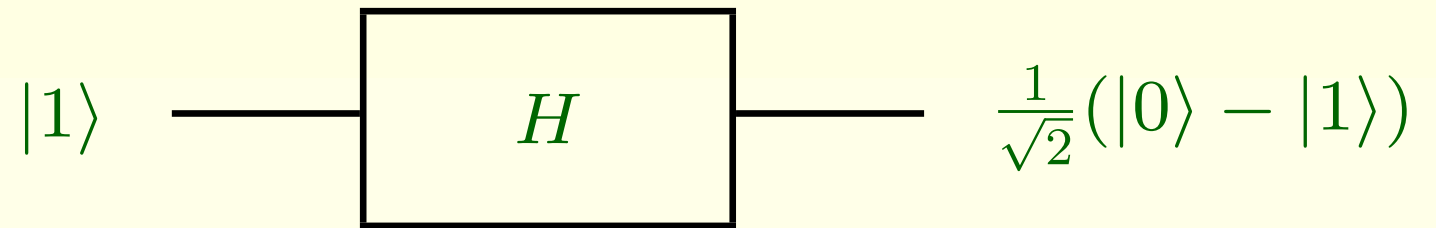


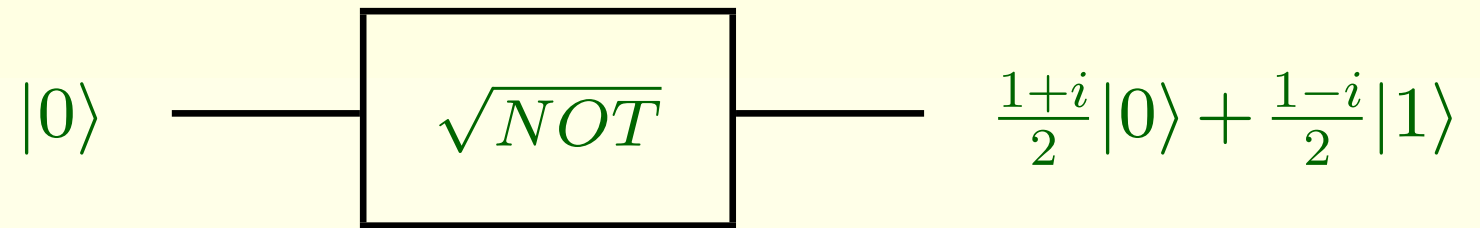


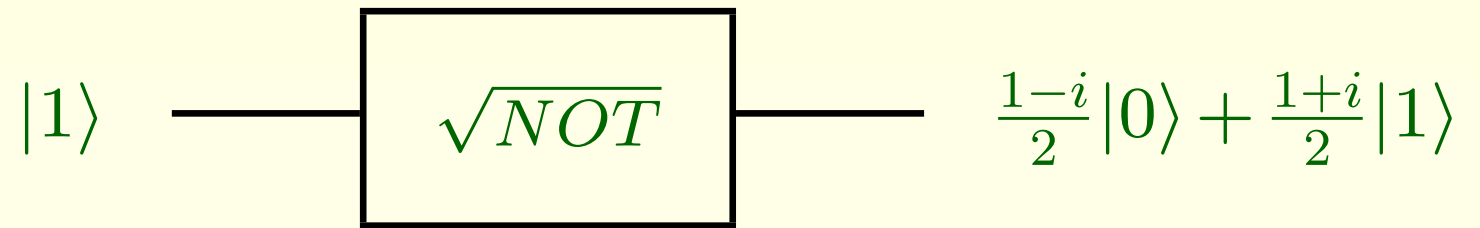
Bramka fazowa

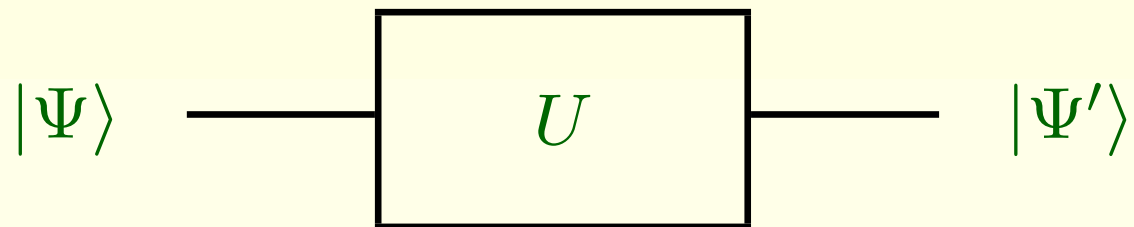


Bramka Hadamarda

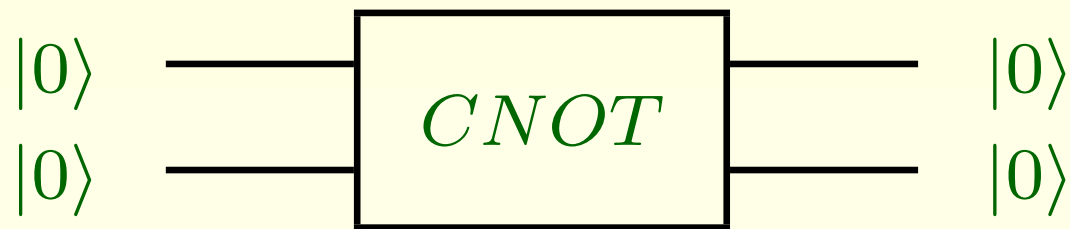








Ogólnie

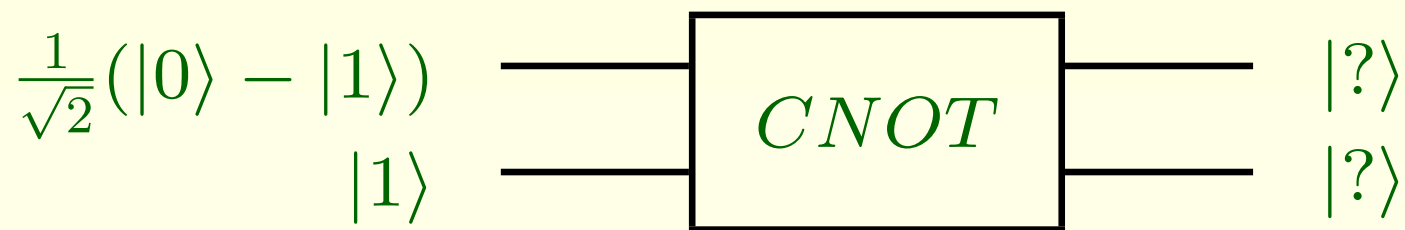


Sterowane zaprzeczenie









O tym za chwilę!

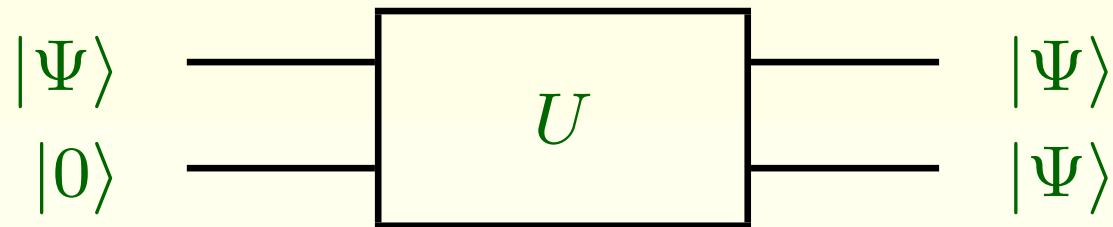
3.4 Zakaz klonowania



3.4 Zakaz klonowania



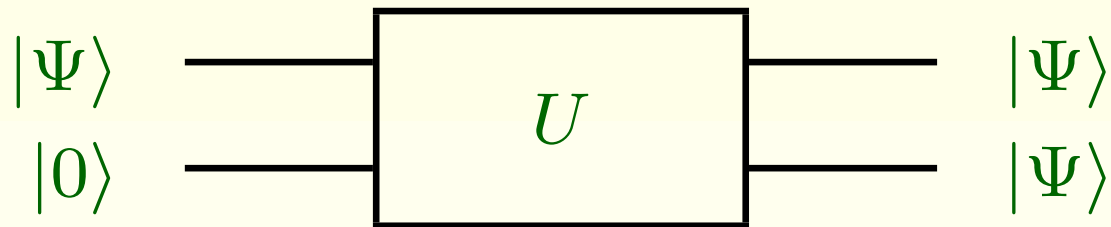
Założmy, że istnieje maszyna klonująca kubity



3.4 Zakaz klonowania



Założmy, że istnieje maszyna klonująca kuby



wtedy

$$U|0\rangle|0\rangle = |0\rangle|0\rangle$$

$$U|1\rangle|0\rangle = |1\rangle|1\rangle$$

Ale

$$U|\Psi\rangle|0\rangle = U(A_0|0\rangle + A_1|1\rangle)|0\rangle$$

Ale

$$\begin{aligned} U|\Psi\rangle|0\rangle &= U(A_0|0\rangle + A_1|1\rangle)|0\rangle \\ &= A_0 U|0\rangle|0\rangle + A_1 U|1\rangle|0\rangle \end{aligned}$$

Ale

$$\begin{aligned} U|\Psi\rangle|0\rangle &= U(A_0|0\rangle + A_1|1\rangle)|0\rangle \\ &= A_0 U|0\rangle|0\rangle + A_1 U|1\rangle|0\rangle \\ &= A_0 |0\rangle|0\rangle + A_1 |1\rangle|1\rangle \end{aligned}$$

Ale

$$\begin{aligned}U|\Psi\rangle|0\rangle &= U(A_0|0\rangle + A_1|1\rangle)|0\rangle \\ &= A_0 U|0\rangle|0\rangle + A_1 U|1\rangle|0\rangle \\ &= A_0 |0\rangle|0\rangle + A_1 |1\rangle|1\rangle \\ &\neq |\Psi\rangle|\Psi\rangle\end{aligned}$$

Ale

$$\begin{aligned}U|\Psi\rangle|0\rangle &= U(A_0|0\rangle + A_1|1\rangle)|0\rangle \\&= A_0 U|0\rangle|0\rangle + A_1 U|1\rangle|0\rangle \\&= A_0 |0\rangle|0\rangle + A_1 |1\rangle|1\rangle \\&\neq |\Psi\rangle|\Psi\rangle \\&= A_0^2 |0\rangle|0\rangle + A_0 A_1 |0\rangle|1\rangle + A_1 A_0 |1\rangle|0\rangle + A_1^2 |1\rangle|1\rangle\end{aligned}$$

Ale

$$\begin{aligned}U|\Psi\rangle|0\rangle &= U(A_0|0\rangle + A_1|1\rangle)|0\rangle \\&= A_0 U|0\rangle|0\rangle + A_1 U|1\rangle|0\rangle \\&= A_0 |0\rangle|0\rangle + A_1 |1\rangle|1\rangle \\&\neq |\Psi\rangle|\Psi\rangle \\&= A_0^2 |0\rangle|0\rangle + A_0 A_1 |0\rangle|1\rangle + A_1 A_0 |1\rangle|0\rangle + A_1^2 |1\rangle|1\rangle\end{aligned}$$

Nieznany stan kwantowy nie może być sklonowany!

4 Rejestry kwantowe

4.1 Dwa kubity

Cztery możliwe stany bazowe:

$$\begin{aligned} \left| \begin{array}{cc} \text{red} \uparrow & \text{red} \uparrow \end{array} \right\rangle &= |00\rangle = |0\rangle \\ \left| \begin{array}{cc} \text{red} \uparrow & \text{cyan} \downarrow \end{array} \right\rangle &= |01\rangle = |1\rangle \\ \left| \begin{array}{cc} \text{cyan} \downarrow & \text{red} \uparrow \end{array} \right\rangle &= |10\rangle = |2\rangle \\ \left| \begin{array}{cc} \text{cyan} \downarrow & \text{cyan} \downarrow \end{array} \right\rangle &= |11\rangle = |3\rangle \end{aligned}$$

Cztery liczby $\{0, 1, 2, 3\}$, każda w innym rejestrze.

Ale kubity mogą być w stanie superpozycji, i nasz dwukubitowy rejestr może wyglądać tak

$$\left| \begin{array}{c} \text{green oval with red dot} \\ \text{green oval with red dot} \end{array} \right\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

Ale kubity mogą być w stanie superpozycji, i nasz dwukubitowy rejestr może wyglądać tak

$$\left| \begin{array}{c} \text{green oval with red dot} \\ \text{green oval with red dot} \end{array} \right\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Ale kubity mogą być w stanie superpozycji, i nasz dwukubitowy rejestr może wyglądać tak

$$\begin{aligned} \left| \begin{array}{c} \text{green oval} \\ \text{green oval} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2} (|0\rangle + |1\rangle + |2\rangle + |3\rangle) \end{aligned}$$

Ale kubity mogą być w stanie superpozycji, i nasz dwukubitowy rejestr może wyglądać tak

$$\begin{aligned} \left| \begin{array}{c} \text{red} \\ \text{red} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2} (|0\rangle + |1\rangle + |2\rangle + |3\rangle) \end{aligned}$$

Cztery liczby $\{0, 1, 2, 3\}$ w **jednym rejestrze!**

Wszystkie z **jednakowymi amplitudami.**

A může být tak

$$\left| \begin{array}{c} \text{purple ellipse with arrow} \\ \text{green ellipse with arrow} \end{array} \right\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

A může být tak

$$\left| \begin{array}{c} \text{purple ellipse with arrow} \\ \text{green ellipse with arrow} \end{array} \right\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$= \frac{1}{2} (|00\rangle + |01\rangle - |10\rangle - |11\rangle)$$

A může být tak

$$\begin{aligned} \left| \begin{array}{c} \text{purple} \\ \text{green} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= \frac{1}{2} (|00\rangle + |01\rangle - |10\rangle - |11\rangle) \\ &= \frac{1}{2} (|0\rangle + |1\rangle - |2\rangle - |3\rangle) \end{aligned}$$

A może być tak

$$\begin{aligned} \left| \begin{array}{c} \text{blue} \\ \text{red} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= \frac{1}{2} (|00\rangle + |01\rangle - |10\rangle - |11\rangle) \\ &= \frac{1}{2} (|0\rangle + |1\rangle - |2\rangle - |3\rangle) \end{aligned}$$

Cztery liczby $\{0, 1, 2, 3\}$ w jednym rejestrze!

Dwie amplitudy mają znaki ujemne!

4.2 Kwantowy paralelizm

Klasycznie na przechowanie czterech liczb potrzebujemy **czterech** rejestrów dwubitowych — każda liczba w innym rejestrze.

4.2 Kwantowy paralelizm

Klasycznie na przechowanie czterech liczb potrzebujemy **czterech** rejestrów dwubitowych — każda liczba w innym rejestrze.

Gdybyśmy dysponowali **rejestrem kwantowym** złożonym z **N** kubitów, to moglibyśmy przechować w takim rejestrze **2^N** liczb!

4.2 Kwantowy paralelizm

Klasycznie na przechowanie czterech liczb potrzebujemy **czterech** rejestrów dwubitowych — każda liczba w innym rejestrze.

Gdybyśmy dysponowali **rejestrem kwantowym** złożonym z N kubitów, to moglibyśmy przechować w takim rejestrze 2^N liczb!

Przy $N = 300$ liczba ta przekraczałaby liczbę atomów we wszechświecie!

4.2 Kwantowy paralelizm

Klasycznie na przechowanie czterech liczb potrzebujemy **czterech** rejestrów dwubitowych — każda liczba w innym rejestrze.

Gdybyśmy dysponowali **rejestrem kwantowym** złożonym z N kubitów, to moglibyśmy przechować w takim rejestrze 2^N liczb!

Przy $N = 300$ liczba ta przekraczałaby liczbę atomów we wszechświecie!

Komputer kwantowy wykonuje operacje na **całym rejestrze**, czyli na wszystkich 2^N liczbach jednocześnie. Nazywa się to **kwantowym paralelizmem**.

4.3 Splątane kubity

Przypuśćmy, że udało nam się przygotować rejestr dwukubitowy w stanie

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$$

4.3 Splątane kubity

Przypuśćmy, że udało nam się przygotować rejestr dwukubitowy w stanie

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$$

Taki stan nie daje się zapisać w postaci iloczynu dwóch kubitów!

$$|\Psi^-\rangle \neq (\alpha_0|0\rangle - \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$

4.3 Splątane kubity

Przypuśćmy, że udało nam się przygotować rejestr dwukubitowy w stanie

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$$

Taki stan nie daje się zapisać w postaci iloczynu dwóch kubitów!

$$\begin{aligned} |\Psi^-\rangle &\neq (\alpha_0|0\rangle - \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle - \alpha_1\beta_0|10\rangle - \alpha_1\beta_1|11\rangle \end{aligned}$$

4.3 Splątane kubity

Przypuśćmy, że udało nam się przygotować rejestr dwukubitowy w stanie

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$$

Taki stan nie daje się zapisać w postaci iloczynu dwóch kubitów!

$$\begin{aligned} |\Psi^-\rangle &\neq (\alpha_0|0\rangle - \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle - \alpha_1\beta_0|10\rangle - \alpha_1\beta_1|11\rangle \end{aligned}$$

$$\alpha_0\beta_0 = 0 \Rightarrow \alpha_0 = 0 \vee \beta_0 = 0$$

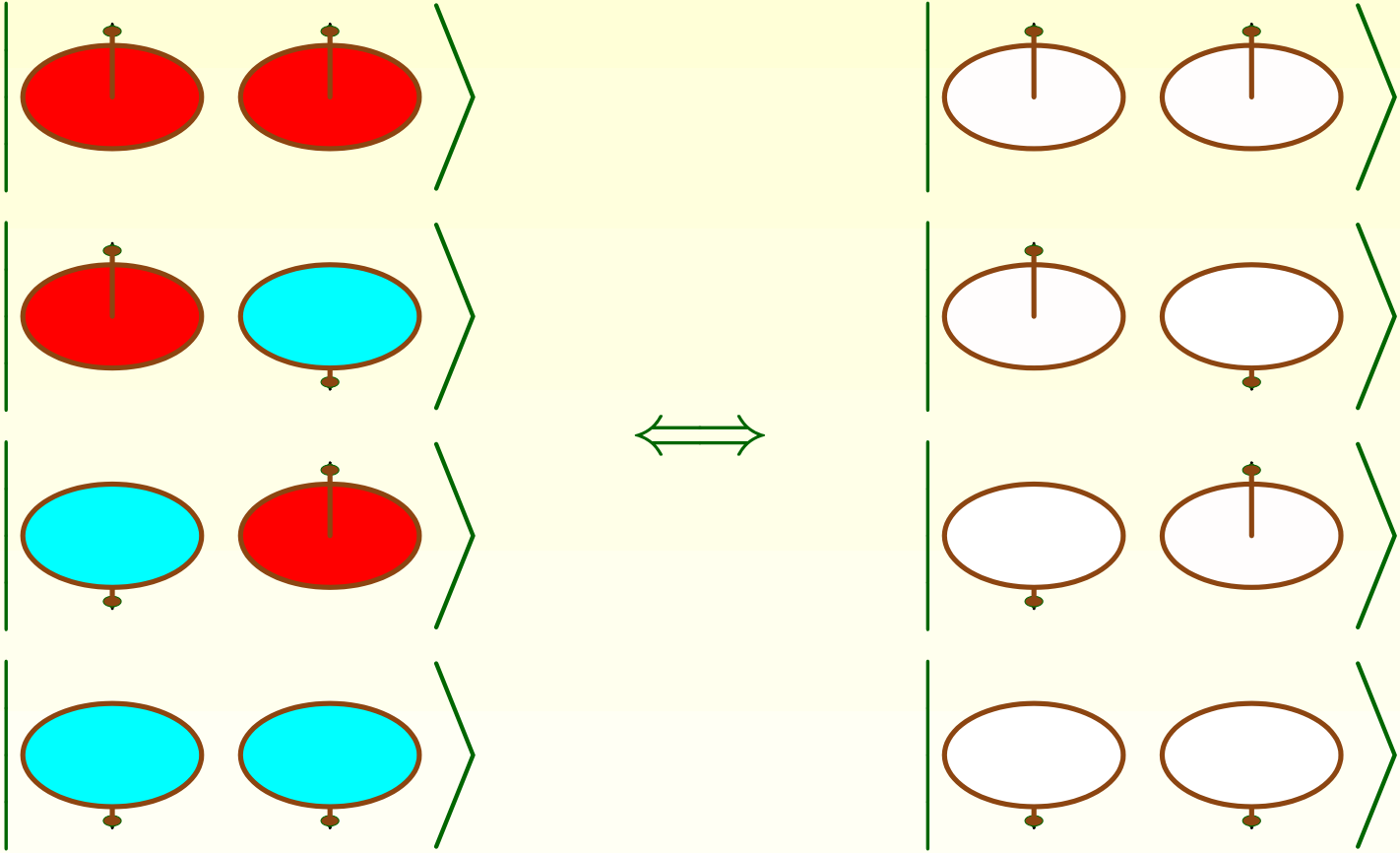
4.4 Stany Bella

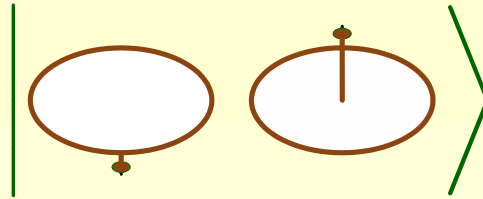
$$\begin{aligned} \left| \begin{array}{cc} \uparrow & \uparrow \\ \text{---} & \text{---} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |\Phi^+\rangle \\ \left| \begin{array}{cc} \uparrow & \downarrow \\ \text{---} & \text{---} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = |\Psi^+\rangle \\ \left| \begin{array}{cc} \downarrow & \uparrow \\ \text{---} & \text{---} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) = |\Psi^-\rangle \\ \left| \begin{array}{cc} \downarrow & \downarrow \\ \text{---} & \text{---} \end{array} \right\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = |\Phi^-\rangle \end{aligned}$$

Splątane kubity tworzące stany Bella nie mają indywidualnych kolorów — są białe w naszej konwencji (kolor biały można otrzymać na wiele sposobów)

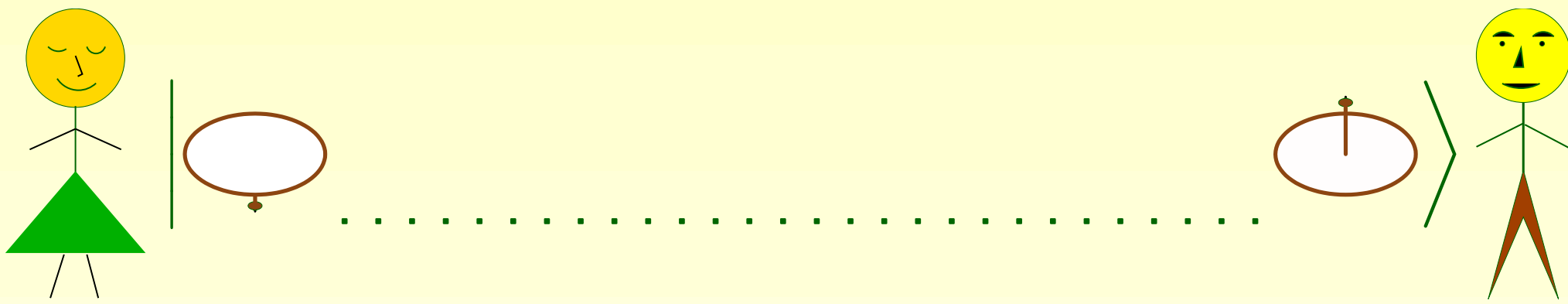
mieszając ze sobą kolory dopełniające).

Stany Bella stanowią bazę dla dwóch kubitów.

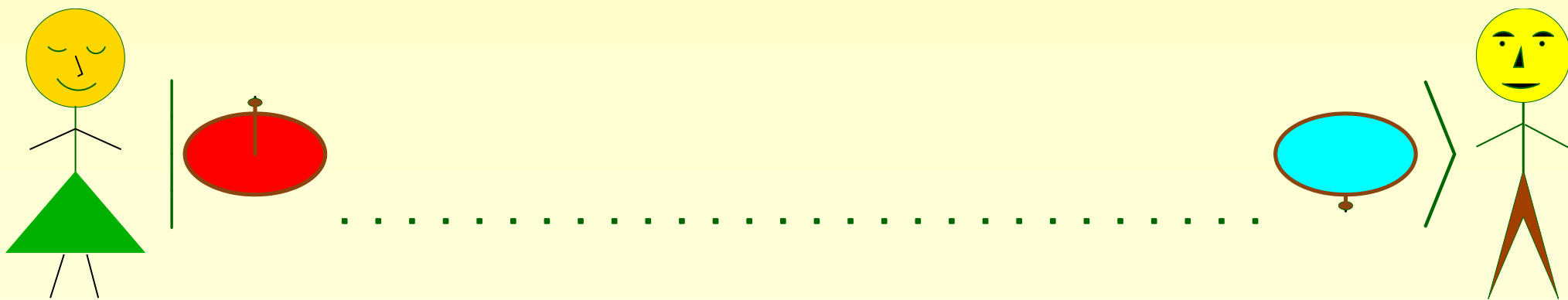




Wyobraźmy sobie, że mamy dwa splątane kubity w stanie Bella $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ (para EPR)

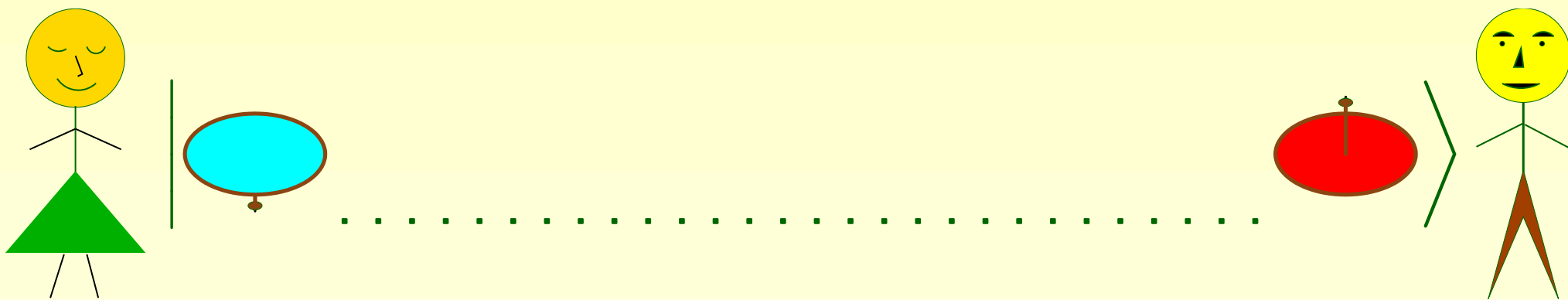


Przesyłamy jeden kubit do Alicji a drugi do Bolka



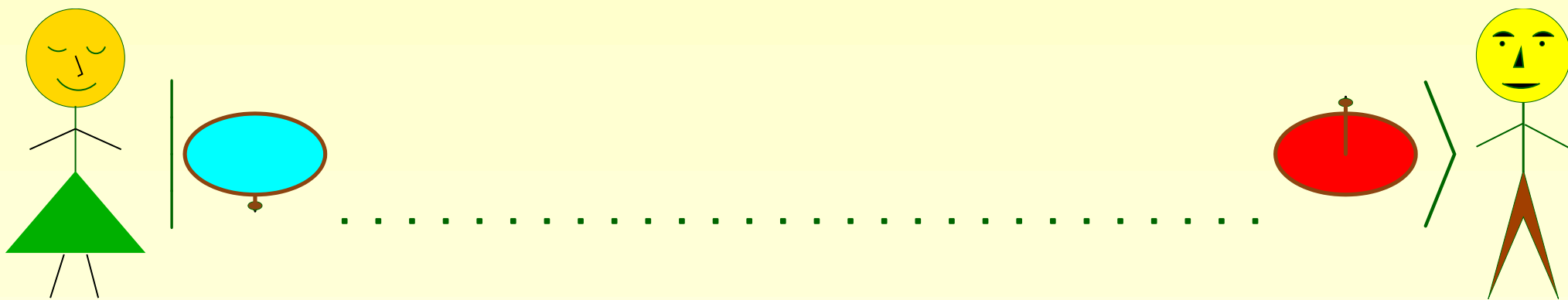
Alicja dokonuje pomiaru na swoim kubicie

$$|0\rangle\langle 0|: |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \mapsto |01\rangle$$



Alicja dokonuje pomiaru na swoim kubicie

$$|1\rangle\langle 1|: |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \mapsto |10\rangle$$



Alicja dokonuje pomiaru na swoim kubicie

$$|1\rangle\langle 1|: |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \mapsto |10\rangle$$

Pomiar wykonany na kubicie Alicji zmienia stan kubitów Bolka!

Bolek wykonując pomiar na swoim kubicy otrzyma wynik **przeciwny** niż otrzymała Alicja, jakkolwiek daleko nie byłby oddalony od Alicji.

Bolek wykonując pomiar na swoim kubicie otrzyma wynik **przeciwny** niż otrzymała Alicja, jakkolwiek daleko nie byłby oddalony od Alicji.

Po wykonaniu **pomiaru lokalnego** przez Alicję obydwa kubity przestały być splątane.

Bolek wykonując pomiar na swoim kubicie otrzyma wynik **przeciwny** niż otrzymała Alicja, jakkolwiek daleko nie byłby oddalony od Alicji.

Po wykonaniu **pomiaru lokalnego** przez Alicję obydwa kubity przestały być splątane.

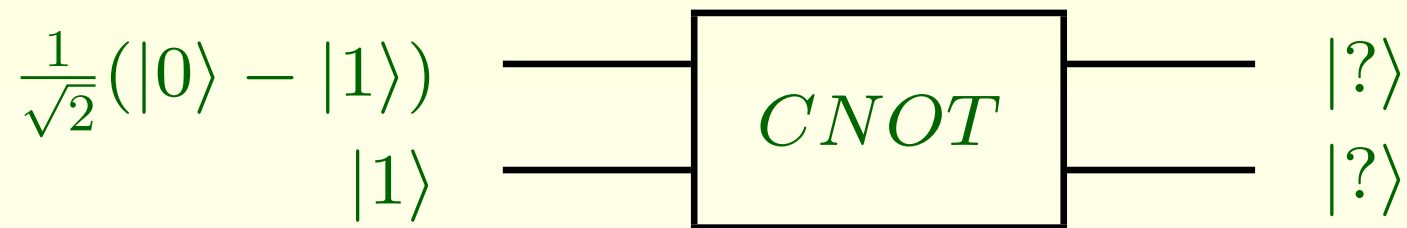
Mechanika kwantowa jest nielokalna!

Bolek wykonując pomiar na swoim kubicie otrzyma wynik **przeciwny** niż otrzymała Alicja, jakkolwiek daleko nie byłby oddalony od Alicji.

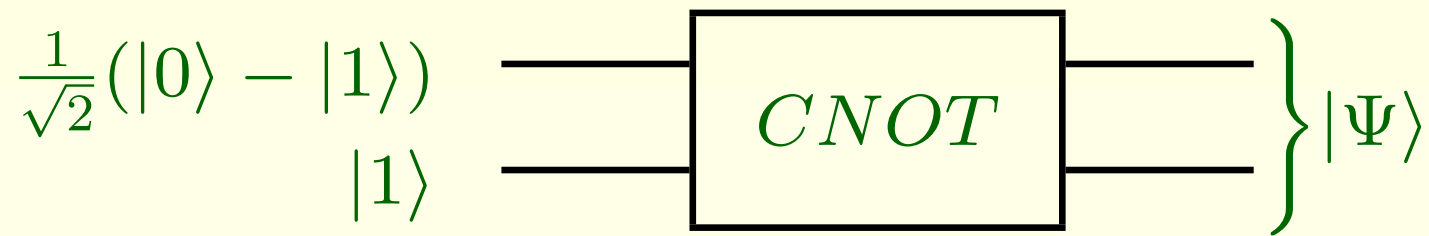
Po wykonaniu **pomiaru lokalnego** przez Alicję obydwa kubity przestały być splątane.

Mechanika kwantowa jest nielokalna!

Jak uzyskać stan splątany?



Bramka $CNOT$



Bramka *CNOT*

Otrzymujemy stan splątany

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Otrzymujemy stan splątany

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Bramka Hadamarda H oraz bramka $CNOT$ pozwalają przejść z bazy standardowej do bazy Bella.

Otrzymujemy stan splątany

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Bramka Hadamarda H oraz bramka $CNOT$ pozwalają przejść z bazy standardowej do bazy Bella.

Potrafimy wytwarzać stany splątane!

Otrzymujemy stan splątany

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Bramka Hadamarda H oraz bramka $CNOT$ pozwalają przejść z bazy standardowej do bazy Bella.

Potrafimy wytwarzać stany splątane!

Po co nam stany splątane?

5 Kwantowe przesyłanie informacji

5.1 Gęste kodowanie

Przypuśćmy, że Alicja chce przesłać Bobowi dwa klasyczne bity informacji.

5 Kwantowe przesyłanie informacji

5.1 Gęste kodowanie

Przypuśćmy, że Alicja chce przesłać Bobowi **dwa klasyczne bity** informacji.

Przesłanie dwóch bitów informacji to przesłanie jednej z czterech liczb $\{0, 1, 2, 3\}$.

5 Kwantowe przesyłanie informacji

5.1 Gęste kodowanie

Przypuśćmy, że Alicja chce przesłać Bobowi **dwa klasyczne bity** informacji.

Przesłanie dwóch bitów informacji to przesłanie jednej z czterech liczb $\{0, 1, 2, 3\}$.

Mając do dyspozycji **kanał kwantowy** może to zrobić przesyłając tylko **jeden kubit**.

5 Kwantowe przesyłanie informacji

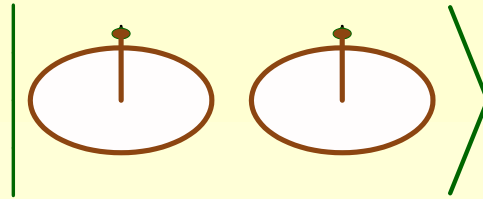
5.1 Gęste kodowanie

Przypuśćmy, że Alicja chce przesłać Bobowi **dwa klasyczne bity** informacji.

Przesłanie dwóch bitów informacji to przesłanie jednej z czterech liczb $\{0, 1, 2, 3\}$.

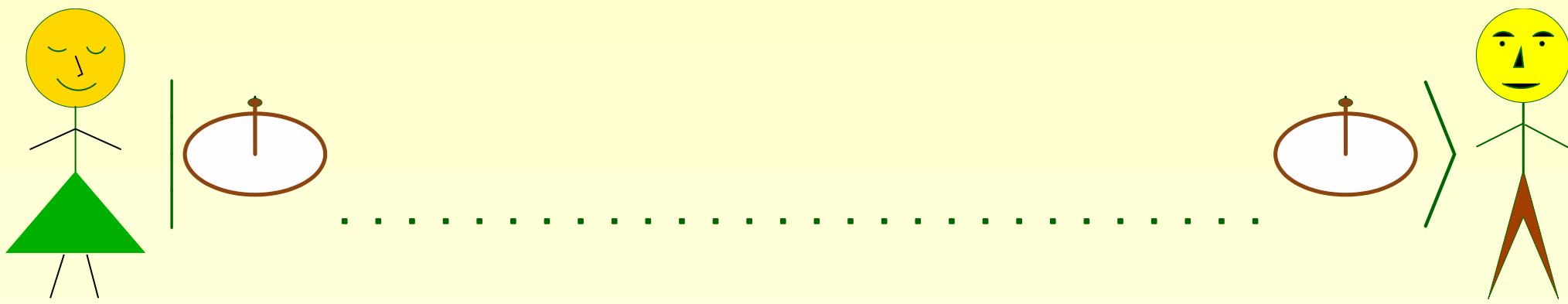
Mając do dyspozycji **kanał kwantowy** może to zrobić przesyłając tylko **jeden kubit**.

W jaki sposób?

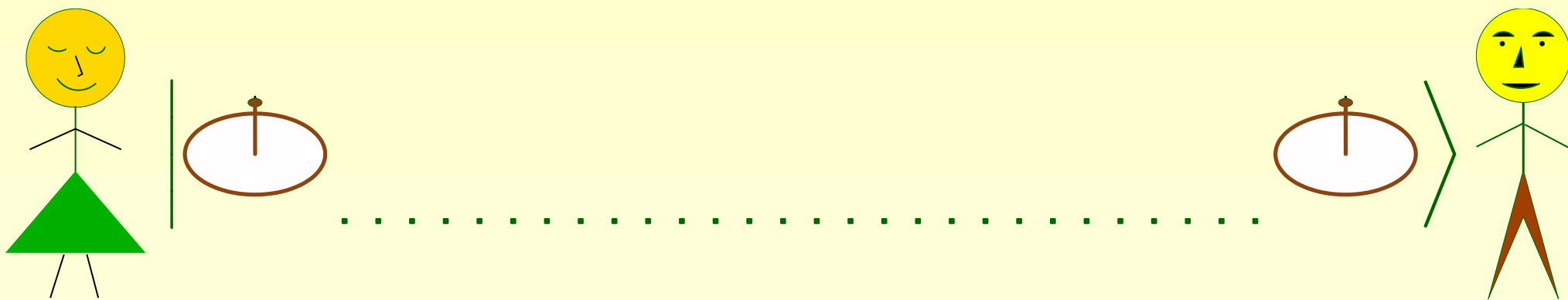


Przygotowujemy dwa splątane kubity w jednym ze stanów Bella, np.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

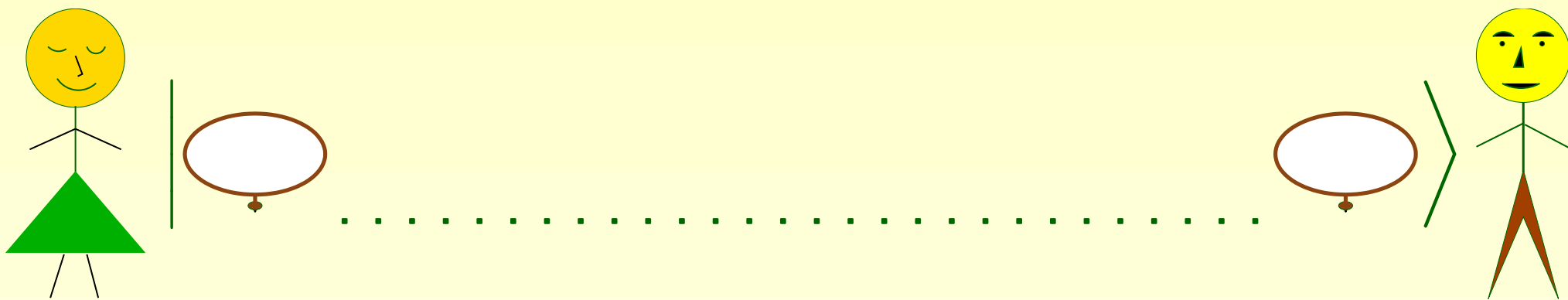


Przesyłamy jeden kubit do Alicji a drugi do Bolka



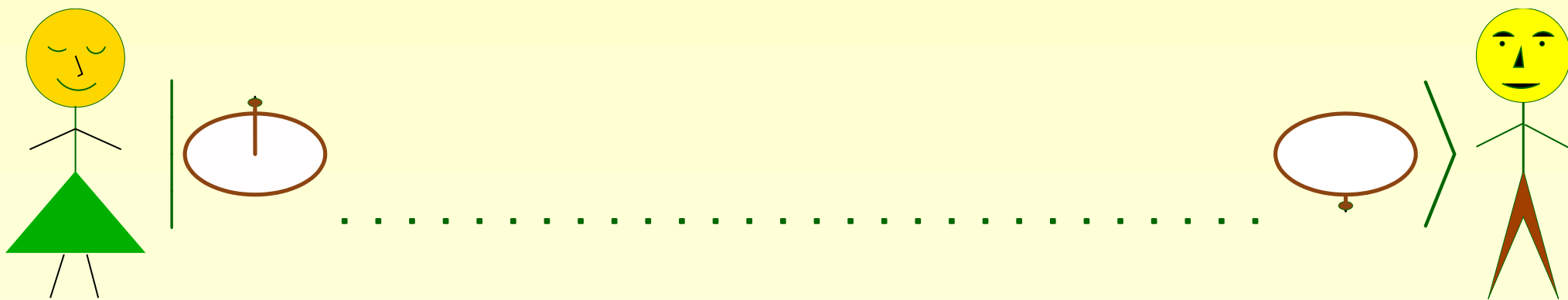
Alicja koduje liczbę, którą chce przesłać dokonując operacji na **swoim kubicie**

$$0 \rightarrow \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \left\{ \begin{array}{c} \text{---} \boxed{I} \text{---} \\ \text{---} \end{array} \right\} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$



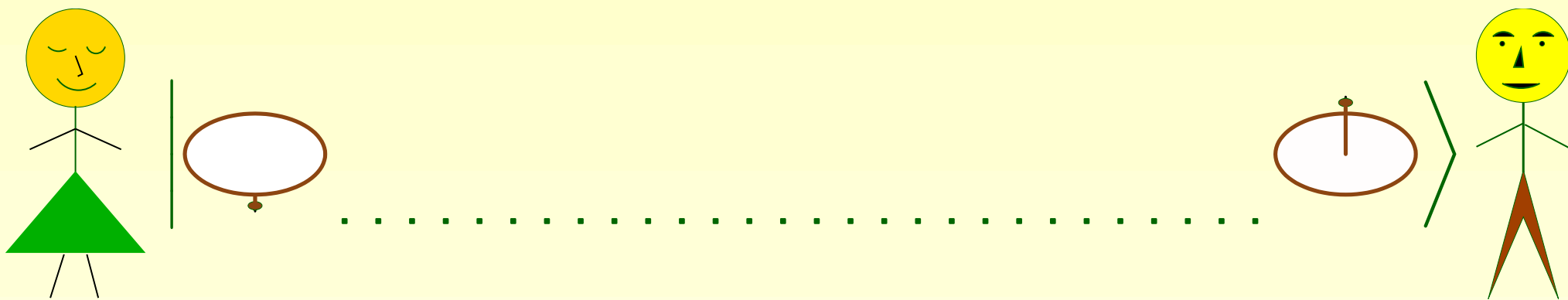
Alicja koduje liczbę, którą chce przesałać dokonując operacji na **swoim kubicie**

$$\mathbf{1} \rightarrow \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \left\{ \begin{array}{c} \text{---} \boxed{\theta} \text{---} \\ \text{---} \end{array} \right\} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$



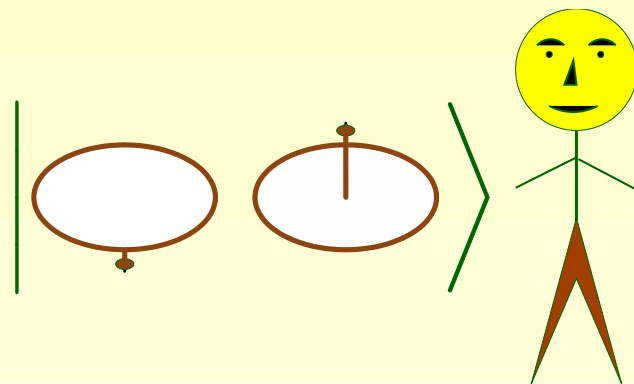
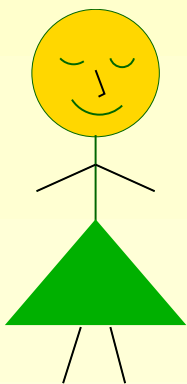
Alicja koduje liczbę, którą chce przesałać dokonując operacji na swoim kubicie

$$2 \rightarrow \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \left\{ \begin{array}{c} \text{---} \boxed{NOT} \text{---} \\ \text{---} \end{array} \right\} \frac{1}{\sqrt{2}} (|10\rangle + |01\rangle)$$



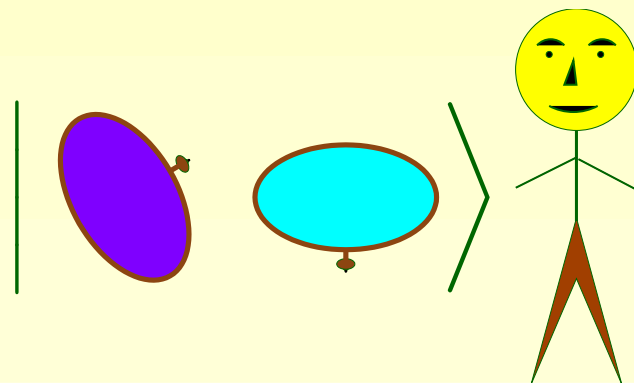
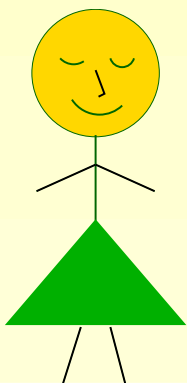
Alicja koduje liczbę, którą chce przesałać dokonując operacji na **swoim kubicie**

$$\mathbf{3} \rightarrow \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \left\{ \begin{array}{c} \text{---} \boxed{NOT} \text{---} \boxed{\theta} \text{---} \\ \text{---} \end{array} \right\} \frac{1}{\sqrt{2}} (-|10\rangle + |01\rangle)$$



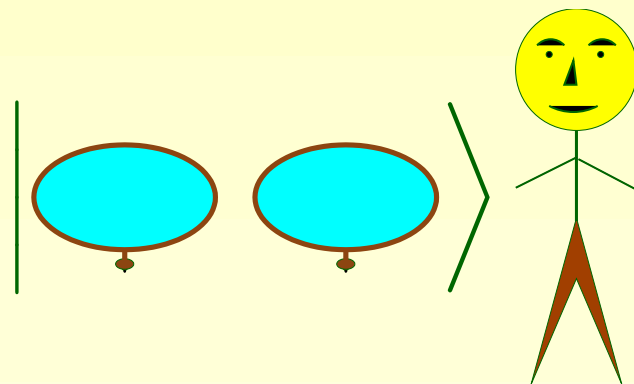
Alicja przesyła swój kubit do Bolka

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



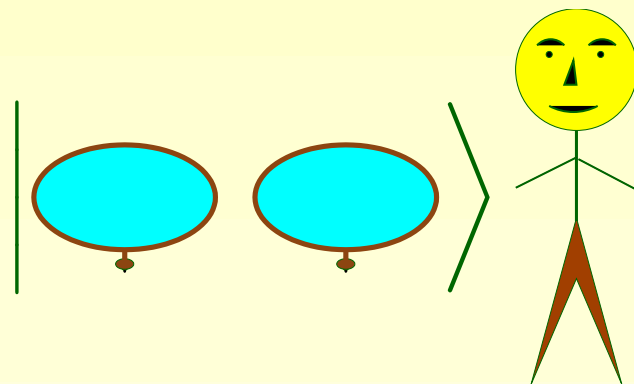
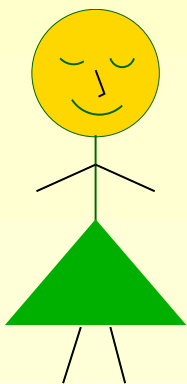
Bolek wykonuje operację $CNOT$ na obydwu kubitach

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$
$$\Rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle$$

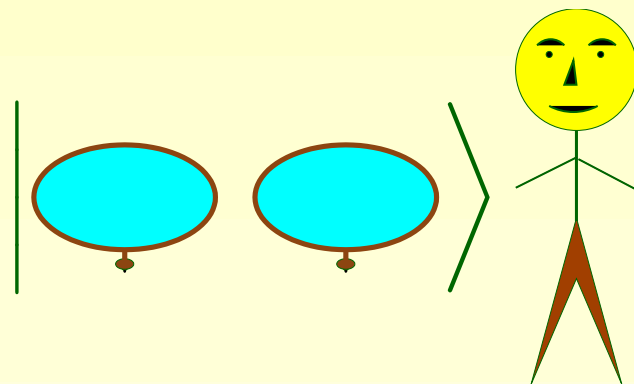
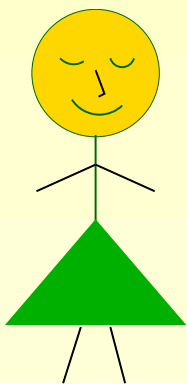


Bolek wykonuje operację Hadamarda H na pierwszym kubicie.

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle \Rightarrow \frac{1}{\sqrt{2}} \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\} |1\rangle$$
$$= |11\rangle$$

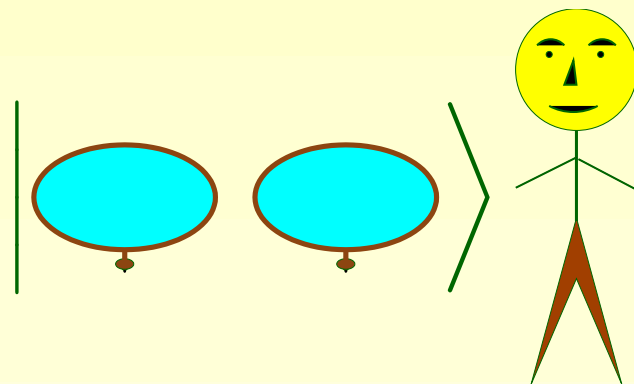
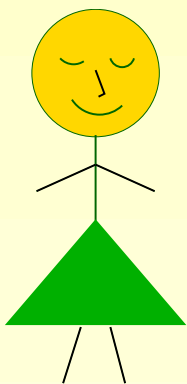


Pomiar obydwu kubitów daje wynik $(11)_2 = 3$, zgodnie z tym co zakodowała Alicja!



Pomiar obydwu kubitów daje wynik $(11)_2 = 3$, zgodnie z tym co zakodowała Alicja!

Przesyłając jeden kubit można przesłać dwa bity klasycznej informacji!



Pomiar obydwu kubitów daje wynik $(11)_2 = 3$, zgodnie z tym co zakodowała Alicja!

Przesyłając jeden kubit można przesłać dwa bity klasycznej informacji!

Gęste kodowanie!

5.2 Teleportacja kwantowa

Wiemy już, że mechanika kwantowa **zabrania klonowania** nieznananych stanów kwantowych.

5.2 Teleportacja kwantowa

Wiemy już, że mechanika kwantowa **zabrania klonowania** nieznananych stanów kwantowych.

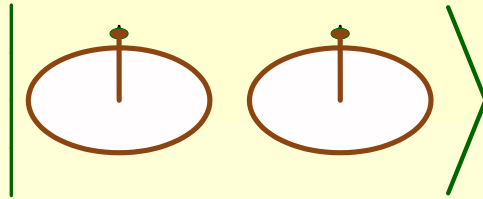
Alicja ma **nieznany kubit**, którego nie może bezpośrednio przesłać do Bolka, ale może się z Bolkiem komunikować klasycznie, np. przez telefon.

5.2 Teleportacja kwantowa

Wiemy już, że mechanika kwantowa **zabrania klonowania** nieznananych stanów kwantowych.

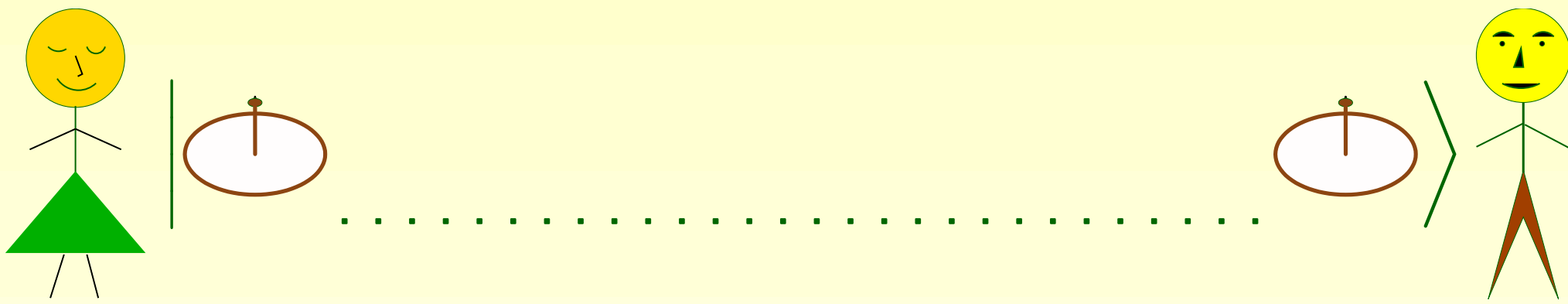
Alicja ma **nieznany kubit**, którego nie może bezpośrednio przesłać do Bolka, ale może się z Bolkiem komunikować klasycznie, np. przez telefon.

Czy można klasycznie przesłać informację pozwalającą Bolkowi odtworzyć kubit Alicji?

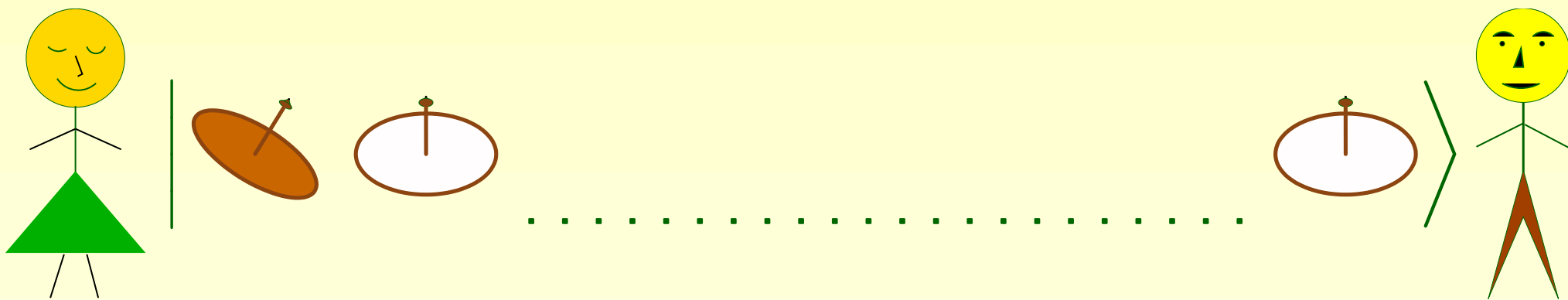


Przygotujemy dwa splątane kubity w jednym ze stanów Bella, np.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

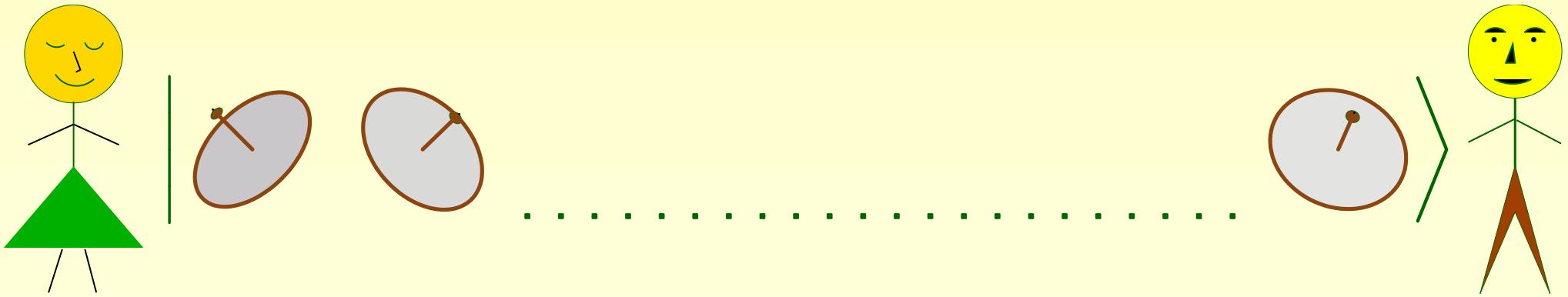


Przesyłamy jeden kubit do Alicji a drugi do Bolka



Nieznany kubit $|\phi\rangle$ zostaje dołączony do należącego do Alicji kubit z splątanej pary.

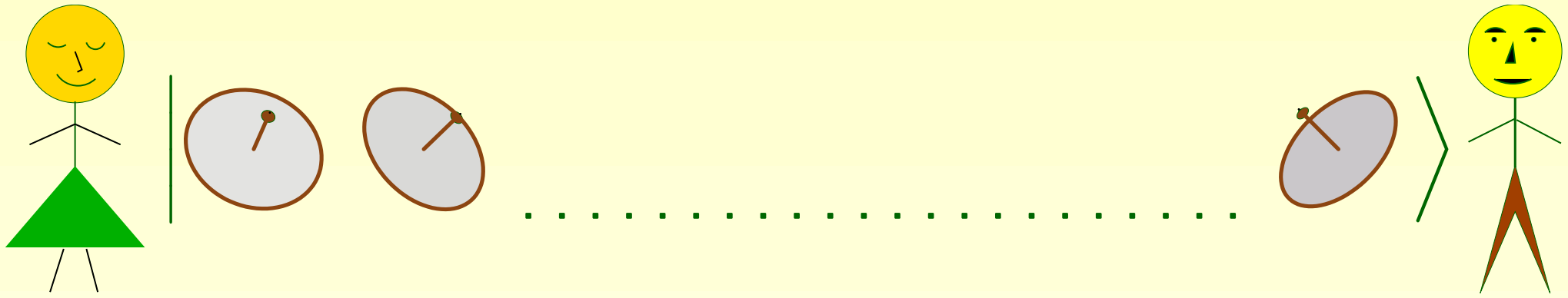
$$\begin{aligned}
 |\phi\rangle \otimes |\Phi^+\rangle &= (A_0|0\rangle + A_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 &= \frac{1}{\sqrt{2}} \{A_0(|000\rangle + |011\rangle) + A_1(|100\rangle + |111\rangle)\}
 \end{aligned}$$



Alicja wykonuje operację $CNOT$ na obydwu kubitach będących w jej posiadaniu

$$\frac{1}{\sqrt{2}} \{ A_0(|000\rangle + |011\rangle) + A_1(|100\rangle + |111\rangle) \}$$

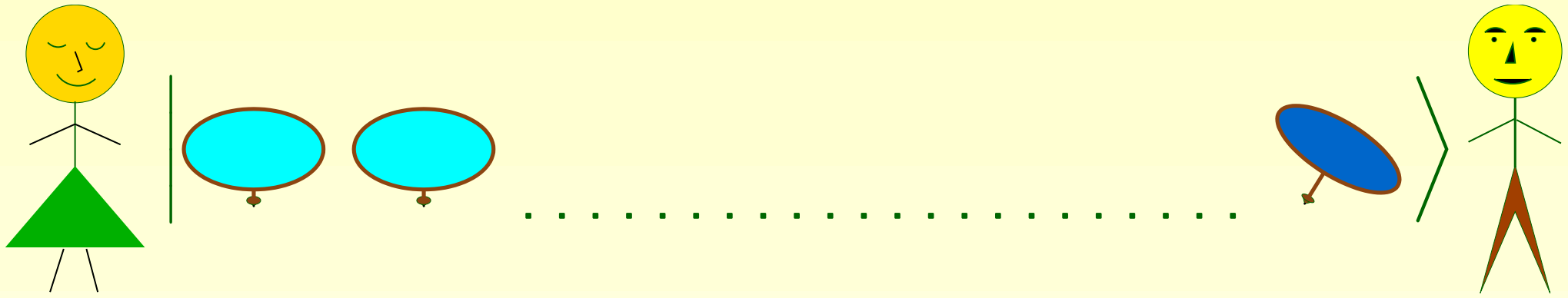
$$\Rightarrow \frac{1}{\sqrt{2}} \{ A_0(|000\rangle + |011\rangle) + A_1(|110\rangle + |101\rangle) \}$$



Alicja wykonuje operację H na pierwszym kubicie.

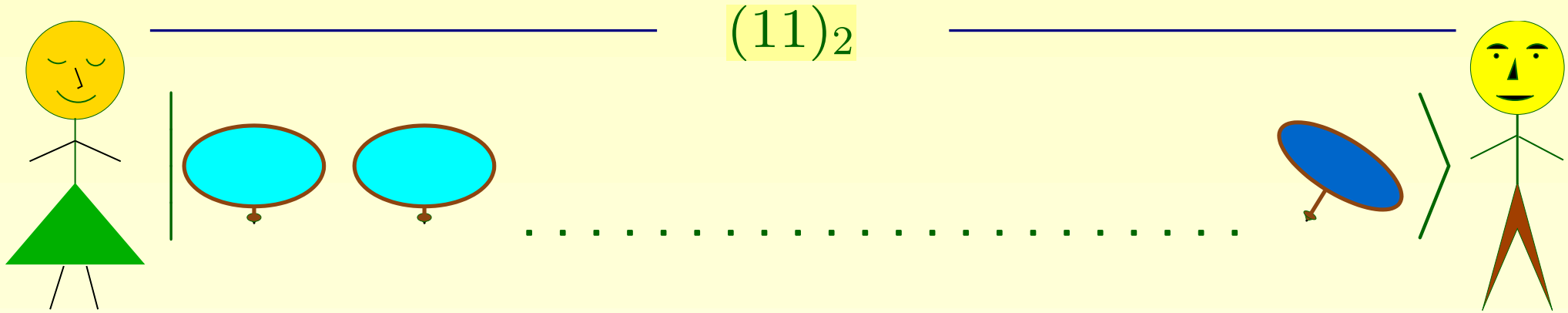
$$\frac{1}{\sqrt{2}} \{ A_0(|000\rangle + |011\rangle) + A_1(|110\rangle + |101\rangle) \}$$

$$\Rightarrow \frac{1}{2} \{ |00\rangle(A_0|0\rangle + A_1|1\rangle) + |01\rangle(A_0|1\rangle + A_1|0\rangle) \\ + |10\rangle(A_0|0\rangle - A_1|1\rangle) + |11\rangle(A_0|1\rangle - A_1|0\rangle) \}$$



Alicja wykonuje pomiar na obydwu kubitach
otrzymując, np. $(11)_2 = 3$

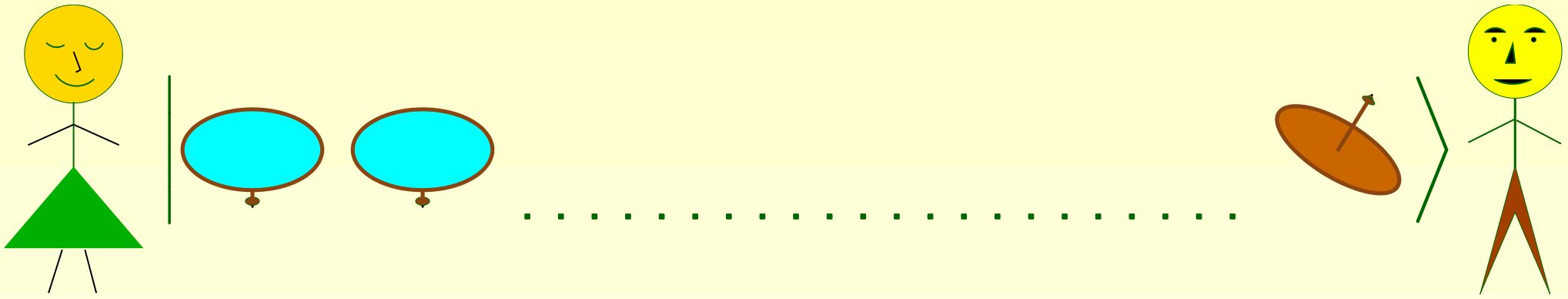
$$\frac{1}{2} \{ |00\rangle(A_0|0\rangle + A_1|1\rangle) + |01\rangle(A_0|1\rangle + A_1|0\rangle) \\ + |10\rangle(A_0|0\rangle - A_1|1\rangle) + |11\rangle(A_0|1\rangle - A_1|0\rangle) \} \\ \Rightarrow |11\rangle(A_0|1\rangle - A_1|0\rangle)$$



Alicja przekazuje Bolkowi otrzymany wynik, np.

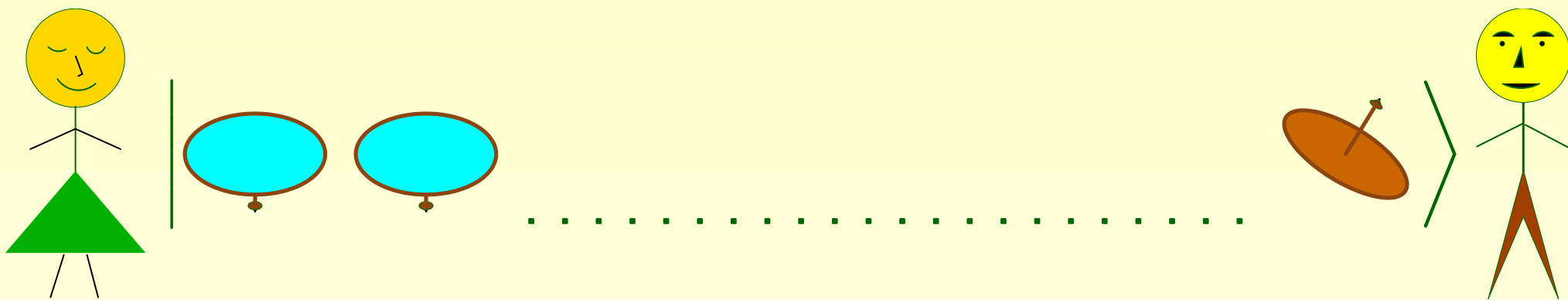
$(11)_2 = 3$, kanałem klasycznym

$$|11\rangle(A_0|1\rangle - A_1|0\rangle)$$



Bolek, znając wynik Alicji, dokonuje odpowiedniej operacji (\boxed{NOT} $\boxed{\theta}$) na własnym kubicie odtwarzając kubit Alicji

$$\begin{aligned}
 & |11\rangle(A_0|1\rangle - A_1|0\rangle) \\
 \Rightarrow & |11\rangle(A_0|0\rangle + A_1|1\rangle) = |11\rangle \otimes |\phi\rangle
 \end{aligned}$$



Bolek, znając wynik Alicji, dokonuje odpowiedniej operacji (\boxed{NOT} $\boxed{\theta}$) na własnym kubicie odtwarzając kubit Alicji

$$|11\rangle(A_0|1\rangle - A_1|0\rangle)$$

$$\Rightarrow |11\rangle(A_0|0\rangle + A_1|1\rangle) = |11\rangle \otimes |\phi\rangle$$

Teleportacja kwantowa!

Anton Zeilinger

W 1997 roku, wspólnie ze swoimi współpracownikami, pokazał eksperymentalnie, że teleportacja kubitów jest możliwa.



6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

6 Czego się dowiedzieliśmy?

- Informacja kwantowa jest reprezentowana przez kubity
- Kubity mogą być w stanie superpozycji
- Kubity mogą być splątane
- Kubitów nie można klonować
- Kubity można teleportować
- Pomiar kwantowy to ewolucja nieodwracalna
- Bramki kwantowe to ewolucja odwracalna
- Na naszych oczach powstaje informatyka kwantowa!

Więcej informacji:

<http://zon8.physd.amu.edu.pl/~tanass>

Więcej informacji:

<http://zon8.physd.amu.edu.pl/~tanas>

Powodzenia!