http://www.fortiss.org/en
Munich, Germany

Formal Verification of Optical Quantum Flip Gate

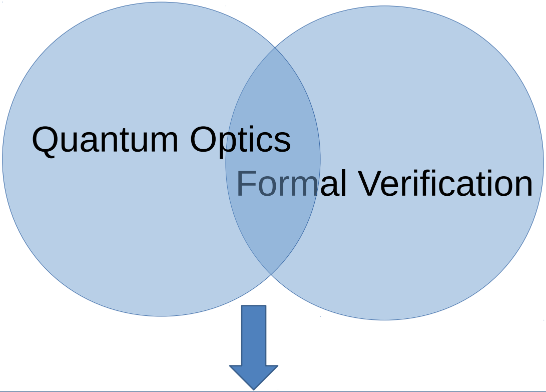
Mohamed Yousri Mahmoud (slides author) Vincent Aravantinos Sofiène Tahar

Hardware Verification Group
Electrical and Computer Engineering Dept.
Concordia University
Montreal, Quebec, Canada
http://hvg.ece.concordia.ca

July 16, 2014

Outline

Motivation



Optical Quantum Computers Verification

Context

Global context:

- Research program carried out at Concordia University
- Objective: formal verification of *optical systems* (e.g., fiber optic, optic circuits, quantum computers, etc.)

To do so, formalization of various theories of optics:

- Ray optics
- Electromagnetic optics
- Quantum optics

Outline

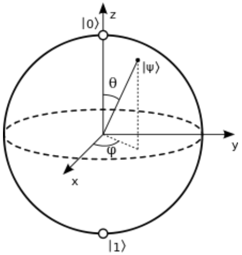
Quantum Computers

Classical Bit

Classical bit = 0 or 1

Qubit

Quantum bit = "mix" of $|0\rangle$ and $|1\rangle \rightarrow \delta|0\rangle + \beta|1\rangle$



Implementation:

- Physical implementations of Qubits: photons, electrons or ions
- *Photon*-based implementations are the most promising

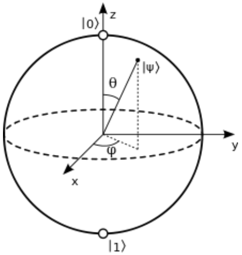
Quantum Computers

Classical Bit

Classical bit = 0 or 1

Qubit

Quantum bit = "mix" of $|0\rangle$ and $|1\rangle \rightarrow \delta|0\rangle + \beta|1\rangle$



Implementation:

- Physical implementations of Qubits: photons, electrons or ions
- *Photon*-based implementations are the most promising

Photon-based implementation of Qubits

Coherent light is used to represent quantum bits:

Coherent Light Qubit

- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Photon-based implementation of Qubits

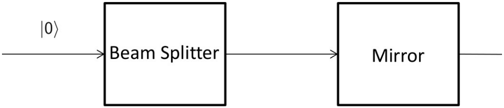
Coherent light is used to represent quantum bits:

Coherent Light Qubit

- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate, converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a *beam splitter* and a *phase conjugating mirror*.



Photon-based implementation of Qubits

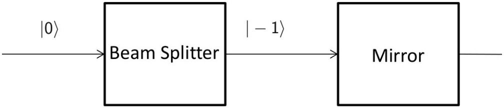
Coherent light is used to represent quantum bits:

Coherent Light Qubit

- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate, converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a *beam splitter* and a *phase conjugating mirror*.



Photon-based implementation of Qubits

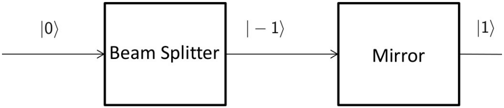
Coherent light is used to represent quantum bits:

Coherent Light Qubit

- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate, converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a *beam splitter* and a *phase conjugating mirror*.



Photon-based implementation of Qubits

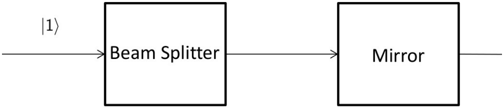
Coherent light is used to represent quantum bits:

Coherent Light Qubit

- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate, converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a *beam splitter* and a *phase conjugating mirror*.



Photon-based implementation of Qubits

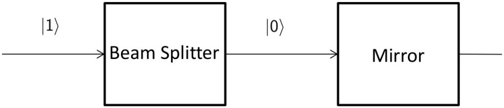
Coherent light is used to represent quantum bits:

Coherent Light Qubit

- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate, converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a *beam splitter* and a *phase conjugating mirror*.



Photon-based implementation of Qubits

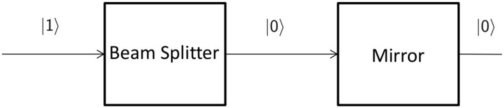
Coherent light is used to represent quantum bits:

Coherent Light Qubit

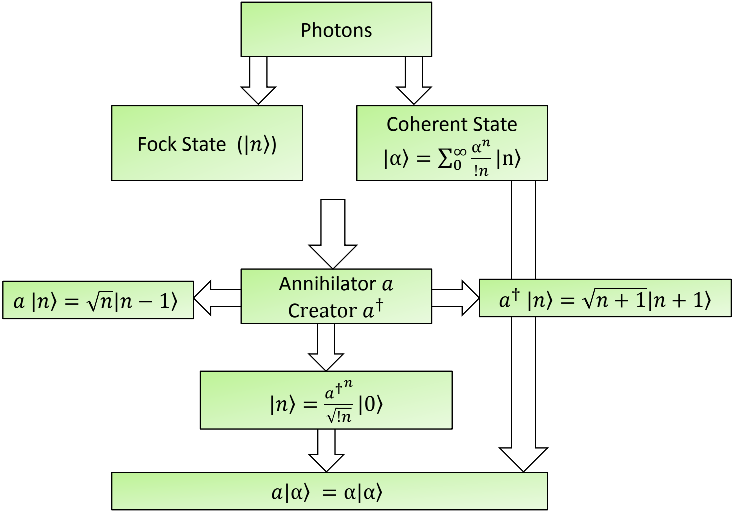
- Qubit = coherent light with states $|0\rangle$ and $|\alpha\rangle$
- $|0\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate, converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a *beam splitter* and a *phase conjugating mirror*.



Quantum Optics: Overview



Outline

Outline

Mathematics Prerequisites

- Complex functions spaces (`cfun`). NFM13
- Infinite summation over `cfun`. NFM14
- Infinite summation over quantum operators.
- Exponentiation of quantum operators.

Infinite Summation over Operators: Definition

$\sum_{n=0}^{\infty} f_n = g_n \Leftrightarrow \forall x \sum_{n=0}^{\infty} f_n(x) = g_n(x)$

Definition

- *Specification:*
  cop_sums (s, inprod) f l (from 0) $\Leftrightarrow$ $\forall$x. x IN s $\Rightarrow$
  cfun_sums (s, inprod) (λn.(f n) x) (l x) (from 0)
- *Hilbert operator to make a function out of it:*
  cop_infsum innerspc s f = @l. cop_sums innerspc f l s
- *Existence predicate:*
  cop_summable innerspc s f = $\exists$l. cop_sums innerspc f l s

Infinite Summation: Properties

" $\sum_{n=0}^{\infty}(f_n + g_n) = \sum_{n=0}^{\infty} f_n + \sum_{n=0}^{\infty} g_n$"

Theorem (Linearity of infinite summation - 1)

$\forall$ f g innerspc.
cop_summable innerspc s f $\wedge$ cop_summable innerspc s g $\Rightarrow$
cop_infsum innerspc s (λn. fn + gn) =
cop_infsum innerspc s f + cop_infsum innerspc s g

" $\sum_{n=0}^{\infty}(a.f_n) = a.\sum_{n=0}^{\infty} f_n$"

Theorem (Linearity of infinite summation - 2)

$\forall$ f innerspc a. cop_summable innerspc s f $\Rightarrow$
cop_infsum innerspc s (λn. a % f n)
= a % cop_infsum innerspc s f

% = multiplication by a scalar

Commutativity of Fun. Inf. Summation with Linear Operators

Definition (Linearity)

is_linear_cop s (op : cop) $\Leftrightarrow$
$\forall$x y.x IN s $\wedge$ y IN s $\Rightarrow$ op (x + y) = op x + op y
$\wedge$ $\forall$a. op (a % x) = a % (op x)

"if *op* linear & bounded: $\sum_{n=0}^{\infty}(op\ (f_n)) = op\ (\sum_{n=0}^{\infty} f_n)$"

Theorem (Commutativity of Inf. Summation with Linear Op.)

$\forall$f h s innerspc.
is_linear_cop s h $\wedge$ is_bounded innerspc h
$\Rightarrow$ cfun_infsum innerspc s (λn. h(f n))
= h (cfun_infsum innerspc s f)

Exponentiation of Quantum Operators

"$e^{op} = \sum_{i=0}^{\infty} \frac{op^n}{!n}$"

Definition

$\texttt{cop\_exp innerspc (op : cfun} \rightarrow \texttt{cfun)} \Leftrightarrow$
$\quad \texttt{cop\_infsum innerspc (from 0) (}\lambda\texttt{n. } \frac{1}{\texttt{!n}} \texttt{ \% (op pow n)}$

" $e^{constantly\ \ null\ \ operator} = identity$"

Theorem

$\forall \texttt{s inprod x. x IN s} \wedge \texttt{is\_inner\_space (s, inprod)} \Rightarrow$
$\quad \texttt{cop\_exp (s, inprod) cop\_zero x = x}$

" $e_{op}^{a.op}(x) = e_{\mathbb{C}}^{a}.op(x)$"

Theorem

$\forall \texttt{ s inprod a x. x IN s} \wedge \texttt{is\_inner\_space (s, inprod)} \Rightarrow$
$\quad \texttt{(cop\_exp (s, inprod) (}\lambda\texttt{y. a\%y)) x = cpow a \% x}$

Outline

Coherent Light: Definition

Coherent light $\Rightarrow$ number of photons follows Poisson distribution at any time

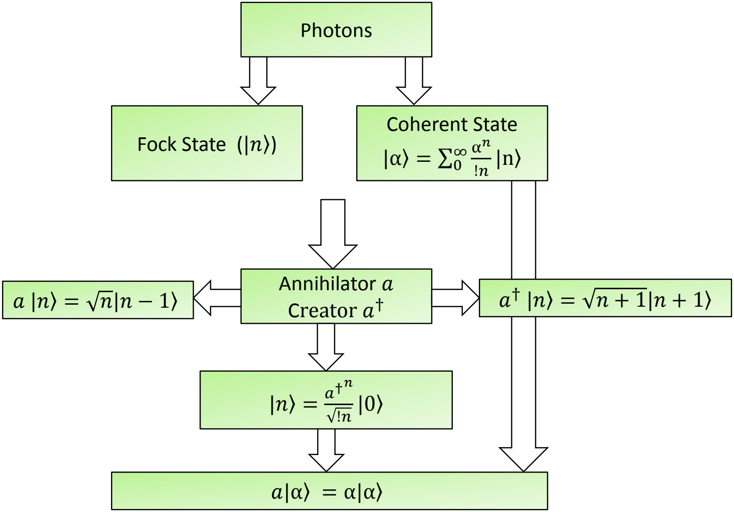
More precisely: state of a coherent light $= |\alpha\rangle$ where $|\alpha|^2$ is the distribution parameter, i.e., the number of expected photons.

Definition

$$\texttt{coherent sm } \alpha = \exp(-\frac{|\alpha|^2)}{2}))\% \; \textcolor{red}{\texttt{cfun\_infsum}} \; (\texttt{s}, \texttt{inprod}) \; (\texttt{from } 0) \; (\lambda \texttt{n}. \frac{\alpha^{\texttt{n}}}{\sqrt{\texttt{n!}}} \% (\textcolor{red}{\texttt{fock}} \; \texttt{sm n}))$$

fock sm n = state where we have *n* photons
$\rightarrow$ defined using the creation operator and the vaccum state (...)
$\rightarrow$ themselves defined using the definition of sm (...)

Quantum Optics: Overview (Recall)



Coherent Light: Property

Theorem (Expression using the displacement operator)

$$(\forall \mathtt{n}.\mathtt{creat\_of\_sm\ sm\ (fock\ sm\ n)} \neq \mathtt{cfun\_zero}))$$
$$\wedge\ \mathtt{cfun\_summable\ (s, inprod)\ (from\ 0)}(\lambda \mathtt{n}.\frac{\alpha\ \mathtt{pow\ n}}{\sqrt{\mathtt{!n}}}\ \mathtt{\%\ fock\ sm\ n})$$
$$\mathtt{is\_sm\ sm} \wedge\ \mathtt{exp\_summable\ (qspc\_of\_sm\ sm)}\ (\alpha\ \mathtt{creat\_of\_sm\ sm})$$
$$\Rightarrow \mathtt{coherent\ sm}\ \alpha = (\mathtt{disp\ sm}\ \alpha)\ \mathtt{vac}$$

vac = lowest energy coherent state ("vaccum")

Displacement Operator

$$D(\alpha) = e^{\alpha \hat{a}^\dagger} \; e^{-\alpha^* \hat{a}} \; e^{[\alpha \hat{a}^\dagger, \alpha^* \hat{a}]}$$

$\hat{a}$ = creation operator (adds a level of energy/photon to a quantum system)
$[a, b]$ = commutator between a and b, i.e., $a \circ b - b \circ a$

Definition (Displacement Operator)

disp sm α =
  (cop_exp sm (α % creat_of_sm sm) $**$
    cop_exp sm ($-$(cnj α) % a_of_sm sm) $**$
     cop_exp sm ((α % creat_of_sm sm) com ((cnj α) % a_of_sm sm)

Main interest of the displacement operator:
easily implemented (physically) using a beam splitter

Outline

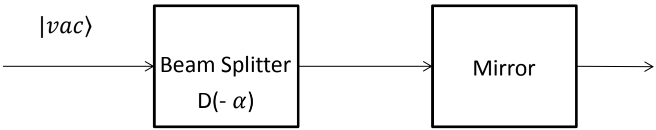
Optical Flip Gate (Recall)

Coherent Light Qubit

- Qubit = coherent light with states $|vac\rangle$ and $|\alpha\rangle$
- $|vac\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a beam splitter and a phase conjugating mirror.



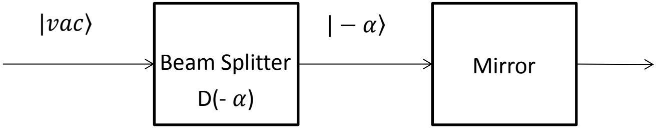
Optical Flip Gate (Recall)

Coherent Light Qubit

- Qubit = coherent light with states $|vac\rangle$ and $|\alpha\rangle$
- $|vac\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a beam splitter and a phase conjugating mirror.



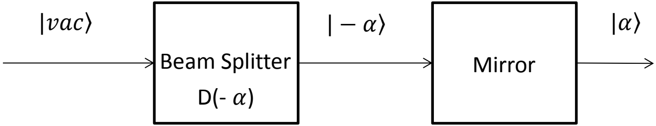
Optical Flip Gate (Recall)

Coherent Light Qubit

- Qubit = coherent light with states $|vac\rangle$ and $|\alpha\rangle$
- $|vac\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a beam splitter and a phase conjugating mirror.



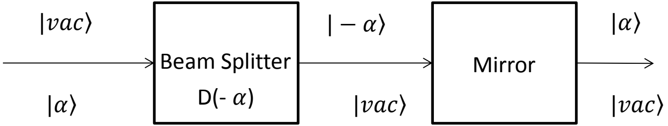
Optical Flip Gate (Recall)

Coherent Light Qubit

- Qubit = coherent light with states $|vac\rangle$ and $|\alpha\rangle$
- $|vac\rangle$ and $|\alpha\rangle$ represent $|0\rangle$ and $|1\rangle$, respectively

Coherent Light Quantum Flip Gate

- Quantum flip gate converts $|0\rangle$ into $|1\rangle$ and vice versa
- Implemented as a beam splitter and a phase conjugating mirror.



Beam Splitter over Coherent states

Theorem (Beam splitter over $|1\rangle$)

$$\wedge\ (\forall \mathtt{x}\ \mathtt{op}.\ \mathtt{is\_linear\_cop}\ \mathtt{op} \wedge \mathtt{x}\ \mathtt{IN}\ \mathtt{s} \Rightarrow$$
$$(\mathtt{cop\_exp}\ (\mathtt{s}, \mathtt{inprod})\ (-\mathtt{op}) **\ \mathtt{cop\_exp}\ (\mathtt{s}, \mathtt{inprod})\ (\mathtt{op}))\ \mathtt{x} = \mathtt{x}$$
$$\Rightarrow \mathtt{disp}\ \mathtt{sm}\ (-\alpha)\ (\mathtt{coherent}\ \mathtt{sm}\ \alpha) = \mathtt{vac}$$

Theorem (Beam splitter over $|0\rangle$)

$$\wedge\ (\forall \mathtt{x}\ \mathtt{op}.\ \mathtt{is\_linear\_cop}\ \mathtt{op} \wedge \mathtt{x}\ \mathtt{IN}\ \mathtt{s} \Rightarrow$$
$$(\mathtt{cop\_exp}\ (\mathtt{s}, \mathtt{inprod})\ (-\mathtt{op}) **\ \mathtt{cop\_exp}\ (\mathtt{s}, \mathtt{inprod})\ (\mathtt{op}))\ \mathtt{x} = \mathtt{x}$$
$$\Rightarrow \mathtt{disp}\ \mathtt{sm}\ (-\alpha)\ (\mathtt{coherent}\ \mathtt{sm}\ \mathtt{vac}) = -\alpha$$

Note: These proofs requires Baker-Campbell-Hausdorf theorem
→ assumed in this work

Mirror over Coherent states

Definition (Mirror)

$$\texttt{mirror sm} = \texttt{cop\_exp (s, inprod) (i}\pi\texttt{ \% n\_of\_sm sm)}$$

Theorem (Main mirror property)

$$\texttt{mirror\_summable sm} \wedge \texttt{is\_bounded (qspc\_of\_sm sm) (mirror sm)} \wedge (\forall \texttt{n.creat\_of\_sm sm (fock sm n)} \neq \texttt{cfun\_zero)}) \Rightarrow \texttt{mirror sm (coherent sm } \alpha\texttt{)} = \texttt{coherent sm } (-\alpha)$$

Theorem (Main mirror property)

$$\texttt{mirror\_summable sm} \wedge \texttt{is\_bounded (qspc\_of\_sm sm) (mirror sm)} \wedge (\forall \texttt{n.creat\_of\_sm sm (fock sm n)} \neq \texttt{cfun\_zero)}) \Rightarrow \texttt{mirror sm (coherent sm vac)} = \texttt{coherent sm vac}$$

Formal Flip Gate Verification

Definition (Flip Gate)

$$\texttt{flip\_gate}\ \alpha\ \texttt{sm} = (\texttt{mirror sm})\ **\ (\texttt{disp sm}\ (-\alpha))$$

Main result of this work:
"flip gate applied to $|1\rangle$ returns $|0\rangle$"
and
"flip gate applied to $|0\rangle$ returns $|1\rangle$"

Theorem

$$\begin{aligned}
&(\texttt{coherent sm}\ \alpha \neq \texttt{cfun_zero})\wedge\\
&\wedge\ (\texttt{cop_exp}\ (\texttt{s}, \texttt{inprod})\ (-\texttt{op})\ **\ \texttt{cop_exp}\ (\texttt{s}, \texttt{inprod})\ (\texttt{op}))\ \texttt{x} = \texttt{x})\\
&\wedge\ \texttt{mirror_summable sm} \wedge \texttt{is_bounded}\ (\texttt{qspc_of_sm sm})\ (\texttt{mirror sm})\\
&\quad \Rightarrow\ (\texttt{flip_gate}\ \alpha\ \texttt{sm})\ (\texttt{coherent sm}\ \alpha) = \texttt{vac}\\
&\quad\ \wedge\ (\texttt{flip_gate}\ \alpha\ \texttt{sm})\ \texttt{vac} = \texttt{coherent sm}\ \alpha
\end{aligned}$$

Outline

Conclusion

- Used HOL Light to formally verify that a quantum-optic-based physical system implements a flip gate *(under reasonable assumptions)*
- Required the formal development of several theories
- Most important fact: we went from the maths foundations to a close-to-practice implementation

Concordia University
Hardware Verification Group
Faculty of Engineering and Computer Science

Thanks!
Questions?

http://hvg.ece.concordia.ca