# On the Quantum Formalization of Coherent Light in HOL

Mohamed Yousri Mahmoud and Sofiène Tahar

Electrical and Computer Engineering Dept., Concordia University
1455 De Maisonneuve Blvd. W., Montreal, Canada
{mo_solim,tahar}@ece.concordia.ca
http://hvg.ece.concordia.ca

**Abstract.** During the last decade, formal methods, in particular theorem proving, have proven to be effective as analysis tools in different fields. Among them, quantum optics is a potential area of the application of theorem proving that can enhance the analysis results of traditional techniques, e.g., paper-and-pencil and lab simulation. In this paper, we present the formal definition of coherent light, which is typically a light produced by laser sources, using higher-order logic and show the effect of quantum operations on it. To this aim, we first present the formalization of underlying mathematics, in particular, finite/infinite summation over quantum states, then prove important theorems, such as uniqueness and the effect of linear operators. Thereafter, basic quantum states of light, called fock states, are formalized and many theorems are proved over such states, e.g., the effect of the quantum creation operation over fock states. Finally, the fundamental notions of coherent light are formalized and their properties also verified.

**Keywords:** Quantum optics, Fock states, Coherent states, Infinite summation, Theorem proving, HOL-Light.

## 1 Introduction

Classical physics has studied light from different points of view, i.e., ray and wave. Each corresponding theory exposed new optical properties, which later were used in developing several optical systems, such as cameras and high speed communications systems. In contrast, quantum optics treats light as a stream of particles, called *photons* [19]. It was started by Planck in 1900 when he explained the discrete nature of light energy based on the photon definition [2]. Light streams of a low number of photons are the best examples for applying quantum optics rules where non-classical optical properties appear, e.g., fluctuating absolute phase of a wave [12]. An important example is single-photon light streams which have wide applications in the area of quantum cryptography and quantum networks [17]. Quantum optics also introduces the most practical implementations of quantum computers, e.g., [9] and [8]. This application is quite important since it promises to solve "hard" computational problems [14].

J.M. Badger and K.Y. Rozier (Eds.): NFM 2014, LNCS 8430, pp. 128–142, 2014.

Despite the advantages of quantum optics, the analysis of quantum systems is not easy, and it poses many difficulties. Unlike regular systems, quantum ones cannot be simulated on ordinary computers, i.e., computers based on Turing machine [4]. Alternatively, a physical-lab simulation is being utilized for systems analysis. However, it is costly and not safe: every little optical element varies in cost from a few hundred to a few thousand of dollars [5]. In addition, scientists and engineers who carry out the simulation process should be well protected against the beams due to their harmful nature [15]. Another analysis method is using numerical tools (typically Matlab [18]) and CAS (typically Mathematica [3]) besides traditional paper-and-pencil based analytical approaches. However, such tools cannot completely replace paper-and-pencil analysis due to accuracy and expressiveness problems. In this paper, we propose to formalize a milestone in the vast theory of quantum optics using the HOL-Light theorem prover [6] in order to mechanize the paper-and-pencil reasoning process. Thus we can provide better and accurate results about the system subject to analyse.

An important notion of quantum mechanics is the *uncertainty principle*. It admits that performing a measurement on a quantum system affects the accuracy of the subsequent measurements. In 1926, Schrödinger discovered the notion of coherent states that achieve minimal measurement error [13]. Coherent states are of high interest in quantum optics analysis, as they are able to express the quantum systems in different states [12]. Therefore, their development allows the analysis of optical systems in several situations. Our formal development of coherent states is based on the formalization of quantum mechanics presented in [10]. Nevertheless, the formalization requires additional mathematical concepts, e.g., summation over infinite dimension vector spaces, which are presented here. The entire formalization presented in this paper is available at [11].

The rest of the paper is organized as follows: Section 2 briefly summarizes some basics of quantum optics and quantum-related mathematical definitions which are developed in [10]. Section 3 deals with the formalization of infinite summation over quantum states. Section 4 presents the development of fock and coherent states. Finally, we conclude the paper in Section 5 and give an overview of a potential application of coherent light.

## 2 Preliminaries

In this section we briefly present the basic knowledge of quantum optics, in particular coherent light. We then summarize the required mathematical notions for the coherent light formalization.

### 2.1 Quantum Physics

A quantum system is fully described with what is so-called *quantum states*, to which we refer as $|\psi\rangle$. Mathematically, it is a square integrable complex-valued function, and the set of all states forms an inner product space. The product

function of such a space is the integration function. In addition, the square integration of each state is equal to one.

Usually, a system has a set of *pure quantum states* (or we can call them basis states, similar to the basis of a vector space). At any time, the system is described with a pure state or a mix of them:

$$|\psi\rangle = \sum |c_i| * |\psi\rangle_i \; i = 0, 1, 2, ... \tag{1}$$

where $c_i$ is a complex number, $\sum |c_i| = 1$ and $|\psi\rangle_i$ is a pure state. A system is at a pure state $i$, if $c_i = 1$ and for any $j \neq i, c_j = 0$.

In quantum optics, light is considered as a stream of particles called photons, in contrast to the classical theory that considers light as an electromagnetic wave. As a quantum system, light has a set of pure states, called *fock states*. Light in a fock state $|n\rangle$, where $n = 0, 1, 2...$, means that the light stream exactly contains $n$ photons. Light is said to be coherent if the number of photons in the light stream (at any time instance) is probabilistically Poisson distributed. In other words, the probability of having (or observing) $n$ photons is:

$$P(N = n) = \frac{|\alpha|^n \; e^{|\alpha|}}{n!} \tag{2}$$

where $|\alpha|$ is the expected number of observed photons ($\alpha$ is a complex number). A coherent light with expected photons $|\alpha|$ is in the quantum state $|\alpha\rangle$. It is represented in terms of fock states as follows (see Equation (1)):

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{3}$$

Similar to classical physics, quantum mechanics physicists are interested in some information about the system, e.g., temperature, velocity, pressure,.etc. Classically, those quantities are expressed by *real* variables. However, they are complete functions (or operators) in quantum mechanics. Those functions operate on quantum states, i.e., they map complex-valued functions (i.e., quantum state space) onto complex-valued-functions. The important information we have to keep in mind is that a quantum operator (denoted as $\hat{O}$) is a linear transformation over the quantum states space.

In the case of optics, there are two basic quantum operators: *creator* and *annihilator* operators. Their names suggest how these operators affect a stream of photons. An annihilator $\hat{a}$ decreases the number of photons by one (i.e., destroys a photon):

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \tag{4}$$

Note that the resulting state is not exactly the quantum state $|n-1\rangle$ , it is scalar-multiplied by $\sqrt{n}$. Similarly, the creation $\hat{a}^\dagger$ increases the number of photons by one (i.e., creates a photon):

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{5}$$

It is important to mention here that the scalar-multiplication does not change the behavior of a quantum state. Thereby, the resulting states in (4) and (5) still have $n-1$ and $n+1$ photons, respectively.

By solving Equation (5) as a recurrence relation, we obtain a general representation of any fock state $|n\rangle$:

$$|n\rangle = \frac{(\hat{a}^\dagger)^n \ |0\rangle}{\sqrt{n!}} \tag{6}$$

where $|0\rangle$ is called vacuum state since it does not contain any photon. Note here that the power notation used in $(\hat{a}^\dagger)^n$ means the application of the creation operator $n$ times (recall that quantum operators are functions).

According to Equations (3) and (6), we can re-express coherent state in terms of the vacuum state and creation operator:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \left( \sum_{n=0} \frac{(\alpha\hat{a}^\dagger)^n}{n!} \right) |0\rangle \tag{7}$$

Note that for a linear operator $a^\dagger$, $(\alpha\hat{a}^\dagger)^n = \alpha^n(\hat{a}^\dagger)^n$.

In a nutshell, formalizing quantum optics, in particular coherent states, requires different mathematical aspects: 1) Linear spaces of complex functions (i.e., quantum states), 2) Inner product space, 3) Linear transformation (i.e., quantum operators) over those spaces, and 4) infinite/finite summation of quantum states. The following section addresses the formalization of aspects (1-3) which were initially introduced in [10]. Infinite/finite summation and related aspects (e.g., notion of limit) will be covered in Section 3.

### 2.2 Quantum State Space Formalization

In order to reason about any quantum system, we first need to formalize the quantum space, which is mathematically an inner product space of square integrable complex-valued functions. In the following, we provide the most important definitions, for details see [10].

We start by defining a new HOL type for a quantum state, $\texttt{cfun} : \texttt{A} \to \texttt{complex}$ which stands for *c*omplex *fun*ction. The type is a complex-valued function with an abstract domain. This type definition basically fits different systems. Before we go through the states space definition, we have to list the arithmetic operations allowed among quantum states. The following are the addition, scalar-multiplication, negation and subtraction:

**Definition 1.**

$\texttt{cfun\_add}\ (\texttt{v}_1 : \texttt{cfun})\ (\texttt{v}_2 : \texttt{cfun})\ : \texttt{cfun} = \lambda \texttt{x} : \texttt{A}.\ \texttt{v}_1\ \texttt{x} + \texttt{v}_2\ \texttt{x}$
$\texttt{cfun\_smul}\ (\texttt{a} : \texttt{complex})\ \texttt{v} = \lambda \texttt{x} : \texttt{A}.\ \texttt{a} * \texttt{v}\ \texttt{x}$
$\texttt{cfun\_neg}\ (\texttt{v} : \texttt{cfun})\ : \texttt{cfun} = \texttt{cfun\_smul}\ (-\texttt{Cx}(1))\ \texttt{v}$
$\texttt{cfun\_sub}\ (\texttt{v}_1 : \texttt{cfun})\ (\texttt{v}_2 : \texttt{cfun})\ : \texttt{cfun} = \texttt{cfun\_add}\ \texttt{v}_1\ (\texttt{cfun\_neg}\ \texttt{v}_2)$

where Cx is a function to cast real numbers to complex ones. Note that multiplication is not allowed (or meaningless) between two quantum states. A vector space of states is then defined as follows:

**Definition 2.**

$$\begin{aligned}&\texttt{is\_cfun\_subspace}\ (\texttt{spc} : \texttt{cfun} \to \texttt{bool}) \Leftrightarrow \\ &\quad \forall \texttt{x}\ \texttt{y}.\ \texttt{x}\ \texttt{IN}\ \texttt{spc} \wedge \texttt{y}\ \texttt{IN}\ \texttt{spc} \Rightarrow \\ &\quad \texttt{x} + \texttt{y}\ \texttt{IN}\ \texttt{spc} \wedge (\forall \texttt{a}.\ \texttt{a}\%\texttt{x}\ \texttt{IN}\ \texttt{spc}) \wedge \texttt{cfun\_zero}\ \texttt{IN}\ \texttt{spc}\end{aligned}$$

where $\texttt{cfun\_zero} = \lambda \texttt{x} : \texttt{A}.\ \texttt{Cx}(0)$ and it is the identity element of the space. To complete the states space definition, we have to define the inner product over the space. As previously mentioned, the inner product function of a quantum space is the integral function. However, in quantum mechanics, we are not interested in the operation itself but in the properties of the product function. Thus, we define the inner product function axiomatically as follows:

**Definition 3.**

$$\begin{aligned}&\texttt{is\_inner\_space}\ ((\texttt{s}, \texttt{inprod}) : \texttt{qs} \to \texttt{bool} \times \texttt{cfun} \to \texttt{cfun} \to \texttt{complex}) \Leftrightarrow \\ &\quad \texttt{is\_cfun\_subspace}\ \texttt{s} \wedge \\ &\quad \forall \texttt{x}.\ \texttt{x} \in \texttt{s} \Rightarrow \\ &\qquad \texttt{real}\ (\texttt{inprod}\ \texttt{x}\ \texttt{x}) \wedge 0 \leq \texttt{real\_of\_complex}\ (\texttt{inprod}\ \texttt{x}\ \texttt{x}) \wedge \\ &\qquad (\texttt{inprod}\ \texttt{x}\ \texttt{x} = \texttt{Cx}(0) \Leftrightarrow \texttt{x} = \texttt{qs\_zero}) \wedge \\ &\qquad \forall \texttt{y}.\ \texttt{y} \in \texttt{s} \Rightarrow \\ &\qquad \texttt{cnj}\ (\texttt{inprod}\ \texttt{y}\ \texttt{x}) = \texttt{inprod}\ \texttt{x}\ \texttt{y} \wedge \\ &\qquad (\forall \texttt{a}.\ \texttt{inprod}\ \texttt{x}\ (\texttt{a}\%\texttt{y}) = \texttt{a} * (\texttt{inprod}\ \texttt{x}\ \texttt{y})) \wedge \\ &\qquad \forall \texttt{z}.\ \texttt{z} \in \texttt{s}\ \Rightarrow \\ &\qquad \texttt{inprod}\ (\texttt{x} + \texttt{y})\ \texttt{z} = \texttt{inprod}\ \texttt{x}\ \texttt{z} + \texttt{inprod}\ \texttt{y}\ \texttt{z}\end{aligned}$$

where real x admits that the complex value x has no imaginary part, and real_of_complex is a function converting a complex number into a real one (if it is real).

Now we turn to quantum operators. Similar to the quantum state, we define a new type for an operator, $\texttt{cop} : \texttt{cfun} \to \texttt{cfun}$. A quantum operator attains two main properties, first its linearity:

**Definition 4.**

$$\begin{aligned}&\texttt{is\_linear\_qop}\ (\texttt{op} : \texttt{cop}) \Leftrightarrow \\ &\quad \forall \texttt{x}\ \texttt{y}.\ \texttt{op}\ (\texttt{x} + \texttt{y}) = \texttt{op}\ \texttt{x} + \texttt{op}\ \texttt{y}\ \wedge \forall \texttt{a}.\ \texttt{op}\ (\texttt{a}\ \%\ \texttt{x}) = \texttt{a}\ \%\ (\texttt{op}\ \texttt{x})\end{aligned}$$

and second its self-adjointness:

**Definition 5.**

$$\begin{aligned}&\texttt{is\_self\_adjoint}\ (\texttt{s}, \texttt{inprod})\ \texttt{op}_1\ \texttt{op}_2 \Leftrightarrow \\ &\quad \texttt{is\_inner\_space}\ (\texttt{s}, \texttt{inprod}) \Rightarrow \\ &\qquad \texttt{is\_closed\_by}\ \texttt{s}\ \texttt{op} \wedge \\ &\qquad \texttt{is\_linear\_cop}\ \texttt{op} \wedge \\ &\qquad \forall \texttt{x}\ \texttt{y}.\ \texttt{inprod}\ \texttt{x}\ (\texttt{op}\ \texttt{y}) = \texttt{inprod}\ (\texttt{op}\ \texttt{x})\ \texttt{y}\end{aligned}$$

where $\texttt{is\_closed\_by}\ \texttt{s}\ \texttt{op} \Leftrightarrow \forall \texttt{x}.\ \texttt{x} \in \texttt{s} \Rightarrow \texttt{op}\ \texttt{x} \in \texttt{s}$.

This concludes the preliminaries section where we acquired a basic knowledge of quantum optics, and how we can formalize some of its essential notions such as quantum states and quantum operators. In the next section, we will complete the formalization of the mathematical notions needed for the coherent states formalization.

## 3 Formalization of Quantum States Summation

In this section, we formalize the notion of infinite/finite summation over `cfun`. Being inspired by Harrison's formalization of summation over finite vector spaces [7], we develop ours for infinite complex space. The summation formalization goes through three major steps: 1) define the finite summation, 2) define the limit notion, then 3) extend the finite one to the infinite summation by applying the notion of limit.

### 3.1 Finite Quantum State Summation

HOL-Light supports the `iterate` function that accepts an operation and finite set of elements, then repeatedly applies the operation on the elements belonging to the set. Hence, `iterate` is the best way to define finite summation:

**Definition 6.**
`cfun_sum` = `iterate cfun_add`

where `cfun_add` is the addition operation between two quantum states. Now, `cfun_sum` is a new operation that accepts two parameters: a finite indexing set `s` (typically, but not limited to, a subset of natural numbers $\mathbb{N}$) and a function `f` : `s` $\rightarrow$ `cfun`. About 19 theorems have been proved for the finite summation over quantum states, we present here the most important ones.

In order to prove useful properties about `cfun_sum`, we first need to provide the following essential theorem, *sum clauses*:

**Theorem 1.**
$(\forall$`f. cfun_sum {} f = cfun_zero`$)\wedge$
  $(\forall$`f n m. FINITE s` $\Rightarrow$
    `cfun_sum (n..m) f = f(m) + cfun_sum(n + 1..m) f`$)$

Here, the theorem states that if the indexing set is empty then the summation is trivial and the result is `cfun_zero`. Or, given a set of natural numbers $\{x : x \geq n \wedge x \leq m\}$ then the summation can be divided into two terms as shown in the third line of Theorem 1. We can then prove many interesting results, such as *sum of constant*:

**Theorem 2.**
$\forall$`c s. FINITE s` $\Rightarrow$ `cfun_sum s` $(\lambda$`n. c`$) = ($`CARD s`$)\%$`c`

where `CARD s` returns the number of elements in `s`. Theorem 2 simply shows that a finite summation turns into a scalar multiplication whenever `f` is a constant function. The next theorem is about closure under `cfun_sum`:

**Theorem 3.**
$\forall$g spc. is_cfun_subspace spc$\wedge$ ($\forall$n. g n IN spc) $\Rightarrow$
  $\forall$s. FINITE s $\Rightarrow$ cfun_sum s g IN spc

The theorem describes that given a set of vectors which belong to a subspace spc, the resulting sum over those vectors belongs to the subspace spc, and hence it is a vector too. Another important theorem is linearity over summation:

**Theorem 4.**
$\forall$f g s.is_linear_cop f $\wedge$ FINITE s $\Rightarrow$ (f(cfun_sum s g) = cfun_sum s (f o g))

The theorem states that linear functions are interchangeable with the summation operation, i.e., applying a linear function on a set of elements then doing the summation is equivalent to applying the summation of elements then doing the linear function. A known application of this theorem is exchanging the integration function with the summation operation.

### 3.2 Infinite Quantum State Summation

The infinite summation can be easily extended from the finite one as long as the notion of limit is provided. The latter is tightly coupled with the existence of a normed-space (i.e., a linear space augmented with a norm function which is defined over its elements). The quantum state space is a normed-space by definition: the square root of an inner product of a vector and itself yields the norm operation. Thus, the notion of limit can be implemented for quantum spaces:

**Theorem 5.**
cfun_lim (s, inprod) f l net $\Leftrightarrow$
  is_inner_space (s, inprod) $\wedge$ l IN s/ ($\forall$x. (f x) IN s)$\wedge$
    ($\forall$e. 0 $\leq$ e $\Rightarrow$ eventually($\lambda$ x. cfun_dist inprod (f x) l $<$ e) net)

where cfun_dist inprod x y = cfun_norm inprod (x $-$ y) and cfun_norm inprod x = $\sqrt{\text{inprod x x}}$. The definition starts by the guarding antecedents which assure that we have an inner space and all elements, we are dealing with, are inside this space. The limit comes as a predicate which ensures that the difference (or cfun_dist) between a vector f x and vector l is getting smaller, while x changes according to the net. An example of nets is sequential net for which the parameter x starts from 0 and increases gradually until infinity.

About 15 theorems have been proved for the notion of limit. Since limit is not the main interest of this section, we are presenting only one theorem as an example, which is believed to be the most important one, *uniqueness*:

**Theorem 6.**
$\forall$ net f l l$'$ innerspc.
  cfun_lim innerspc f l net $\wedge$cfun_lim innerspc f l$'$ net $\Rightarrow$ (l = l$'$)

We mean by uniqueness here that if it happens that a function `f : A → cfun` limits to a vector `l:cfun`, and at the same time to vector a `l':cfun`, then `l` should be equal to `l'`.

Now, we can define infinite summation of `cfun` as follows:

**Definition 7.**

```
cfun_sums innerspc f l s ⇔
  cfun_lim innerspc (λn. cfun_sum (s INTER (0..n)) f) l sequentially
```

where `INTER` is the sets intersection operator. In order to easily understand the definition, let us assume `s` is equal to the set of natural numbers. Consequently, `(s INTER (0..n))= 0..n`. Then, the definition states that while $n$ increases, the finite summation `cfun_sum` coincides with (or limit to) `l`. However, this predicate definition does not help much in usual mathematical manipulation. Therefore, we develop another functional definition:

**Definition 8.**

```
cfun_infsum innerspc s f = @l. cfun_sums innerspc f l s
```

Here, the definition uses the Hilbert choice operator `@` to get a vector that satisfies the `cfun_sums` predicate.

In order to proceed with proving theorems related to infinite summation, we have first to make sure that the series of vectors subject to summation is convergent, i.e., the limit exits. For this purpose, we define the `summable` predicate:

**Definition 9.**

```
cfun_summable innerspc s f = ∃l. cfun_sums innerspc f l s
```

It is important to know how `cfun_infsum` deals with arithmetic operations, i.e., addition and scalar multiplication. Thereby, we provide the following two essential theorems:

**Theorem 7.**

```
∀ f g innerspc.
cfun_summable innerspc s f ∧ cfun_summable innerspc s g ⇒
  cfun_infsum innerspc s(λn.fn + gn) =
    cfun_infsum innerspc s f + cfun_infsum innerspc s g
```

**Theorem 8.**

```
∀ f innerspc a. cfun_summable innerspc s f ⇒
  cfun_infsum innerspc s(λn.a % f n) = a% cfun_infsum innerspc s f
```

Similar to the notion of limit, uniqueness of infinite summation is proved. Since we have already presented it, there is no need to re-express it here for infinite summation. Likewise, we prove the linearity theorem for `cfun_infsum` as it is developed for the finite summation. However, the linearity of a function is not enough to exchange it with infinite summation. It should be a bounded function too. Before we present the theorem of linearity, let us express the definition of boundness:

**Definition 10.**
is_bounded (s, inprod) h ⇔ is_inner_space (s, inprod)
⇒ is_closed_by s h ∧ ∃B. 0 < B∧
(∀x. x IN s ⇒ cfun_norm inprod (h x))) ≤ B ∗ cfun_norm inprod x)))

Here, a linear operator h is bounded if for all x the norm of h x is less than or equal to the norm of x multiplied by a scalar B, given that B does not depend on x. Now we can present the effect of a linear operator on the cfun_infsum operation:

**Theorem 9.**
∀f h s innerspc.
cfun_summableinnerspcsf ∧ is_linear_cop h ∧ is_bounded innerspc h
⇒ cfun_infsum innerspc s(λn. h(f n)) = h(cfun_infsum innerspc s f)

The theorem shows that a linear bounded operator (or function) is exchangeable with the cfun_infsum operation.

We conclude this section by mentioning that about 50 theorems have been proved for the finite/infinite summation of over cfun. In the next section, we will describe the coherent states formalization where the notions presented in this section are being utilized.

## 4 Coherent Light Formalization

In this section, the formal definition of coherent states is presented, then we prove that coherent states are eigenvectors of the annihilation operator. The coherent light formal development is carried out in three steps: 1) quantum light formalization, 2) fock states formalization which are the basis of quantum optics states space, then finally 3) coherent states formalization.

### 4.1 Single Mode

Classically, light is consider as an electromagnetic field. Quantum physics restudies such a field according to quantum rules. Thereby, the first step towards quantum optics formalization is implementing the electromagnetic field quantization. Electromagnetic fields can be classified according to the number of resonance frequencies per field. Accordingly, there are single-mode fields, i.e., single resonance frequency and multi-mode fields for a higher number of frequencies. For simplicity, we are concerned with properties of single-mode field which can be extended for multi-mode fields. The first formal definition of quantum single-mode field is presented in [10]. We use it here with some changes: we fix the vacuum state of the field and add its properties to the definition itself (see the last two lines of the definition):

**Definition 11.**

$$\begin{aligned}&\texttt{is\_sm}\ ((\texttt{sp},\texttt{cs},\texttt{H}),\texttt{w},\texttt{vac}) \Leftrightarrow\\ &\quad \texttt{is\_qsys}\ (\texttt{sp},\texttt{cs},\texttt{H}) \wedge 0 < \texttt{w} \wedge \exists \texttt{q}\ \texttt{p}.\ \texttt{cs} = [\texttt{q};\texttt{p}]\\ &\quad \wedge\ \forall \texttt{t}.\texttt{is\_observable sp}\ (\texttt{p t}) \wedge \texttt{is\_observable sp}(\texttt{q t})\\ &\quad \wedge\ \texttt{H t} = \tfrac{\texttt{w}^2}{2}\%((\texttt{q t})\ \texttt{pow}\ 2) + \quad \tfrac{1}{2}\%((\texttt{p t})\ \texttt{pow}\ 2)\\ &\quad \wedge \texttt{is\_qst sp vac} \wedge \texttt{is\_eigen\_pair}\ (\texttt{H t})\ (\texttt{vac}, \tfrac{\texttt{planck}*\texttt{w}}{2})\end{aligned}$$

The reason behind these changes is that quantum states spaces consist of equivalent classes of quantum states. In this way, we specify the representative of the vacuum state class, and hence of all other classes. The `is_qst` predicate ensures that the norm of the state is equal to unity and belongs to the space `sp`. According to the definition, we assume that `vac` is an eigenvector of the quantum operator `H` which is responsible for calculating the total energy inside the field. The corresponding eigenvalue is equal to $\frac{\texttt{planck}*\texttt{w}}{2}$. We can then prove that `vac` is an eigenvector of the photon number operator `N` which is responsible for calculating the number of photons inside the field. The corresponding eigenvalue is equal to zero:

**Theorem 10.**

$$\begin{aligned}&\forall \texttt{sp cs H omega vac}.\\ &\quad \texttt{let sm} = (\texttt{sp},\texttt{cs},\texttt{H}),\texttt{omega},\texttt{vac in}\\ &\qquad \texttt{is\_sm sm} \Rightarrow \texttt{is\_eigen\_pair}\ (\texttt{n\_of\_sm sm})(\texttt{vac}, 0)\end{aligned}$$

Before we tackle the notion of fock states, we have to consider two important theorems, which show the effects of creation and annihilation operators on eigenvectors of the photon number operator. Here is the creation operator effect:

**Theorem 11.**

$$\begin{aligned}&\forall \texttt{sp cs H omega vac}.\\ &\quad \texttt{let sm} = (\texttt{sp},\texttt{cs},\texttt{H}),\texttt{omega},\texttt{vac in}\\ &\quad \texttt{is\_sm sm} \Rightarrow\\ &\qquad \forall \texttt{v}.\ (\texttt{create\_of\_sm sm v} = \texttt{cfun\_zero}) \Rightarrow\\ &\qquad \forall \texttt{n}.\ \texttt{is\_eigen\_pair}\ (\texttt{n\_of\_sm sm})\ (\texttt{v},\texttt{n}) \Rightarrow\\ &\qquad \texttt{is\_eigen\_pair}\ (\texttt{n\_of\_sm sm})(\texttt{herma\_of\_sm sm f}, \texttt{n} + 1))\end{aligned}$$

where the last line shows that the number of photons is increased by one. Similarly, the annihilation operator affects the number of photons as follows:

**Theorem 12.**

$$\begin{aligned}&\forall \texttt{sp cs H omega vac}.\\ &\quad \texttt{let sm} = (\texttt{sp},\texttt{cs},\texttt{H}),\texttt{omega},\texttt{vac in}\\ &\quad \texttt{is\_sm sm} \Rightarrow\\ &\qquad \forall \texttt{v}.\ (\texttt{create\_of\_sm sm v} = \texttt{cfun\_zero}) \Rightarrow\\ &\qquad \forall \texttt{n}.\ \texttt{is\_eigen\_pair}\ (\texttt{n\_of\_sm sm})\ (\texttt{v},\texttt{n}) \Rightarrow\\ &\qquad \texttt{is\_eigen\_pair}\ (\texttt{n\_of\_sm sm})(\texttt{ann\_of\_sm sm v}, \texttt{n} - 1))\end{aligned}$$

Here, the number of photons is decreased by one. In the same context, it is important to know how annihilation operator affects the vacuum state, where there are no photons:

**Theorem 13.**
```
∀sp cs H omega vac.
  let sm = (sp, cs, H), omega, vac in
    is_sm sm ⇒ (a_of_sm sm) vac = cfun_zero
```

Note that the resulting state is a non-quantum state since the norm of `cfun_zero` is equal to zero.

### 4.2 Fock States

Recall that a single-mode field at a fock state $|n\rangle$ means that the light stream contains exactly $n$ photons. Such states are quite important since they form the basis of the single-mode quantum states space. Moreover, it is widely used in the development of single-photon devices which have direct applications in quantum cryptography. We start by giving the formal definition of a `fock` state:

**Definition 12.**
```
let (((s, inprod), cs, H), omega, vac) = sm in
  fock sm 0 = vac ∧ fock sm (SUC n) =
    get_qst inprod (creat_of_sm sm (fock sm n)))
```

As shown, it is recursively defined with `vac` state as the base case. Recall that we have proved before that `vac` is the eigenvector of the photon number operator with zero photons. Then, we can get any higher fock state by applying the creation operator. The function `get_qst` returns the normalized version of a vector, i.e., by dividing by the norm of the vector itself. This is to ensure that the norm of the resulting quantum state is equal to one. Here is the theorem that shows that a fock state is normalized:

**Theorem 14.**
```
∀s inprod cs H omega vac.
  let sm = ((s, inprod), cs, H), omega, vac in
    is_sm sm ⇒ ∀n. fock sm n ∈ s ∧ inprod (fock sm n) (fock sm n) = 1
```

Now, we provide the semantic of the `fock` definition by proving that it is an eigenvector of the photon number with `n` photons as an eigenvalue:

**Theorem 15.**
```
∀n sm.
  is_sm sm ∧ ((creat_of_sm sm (fock sm n)) = cfun_zero)
    ⇒ is_eigen_pair(n_of_sm sm) (fock sm n, n)
```

We also provide the effect of creation and annihilation operators on fock states. The following two theorems correspond to Equations (4) and (5) (See Section 2):

**Theorem 16.**

$\forall$n sm.
  is_sm sm $\wedge$ ((creat_of_sm sm (fock sm n)) = cfun_zero)
    $\Rightarrow$ (anhh_of_sm sm) (fock sm (SUC n)) = $\sqrt{\text{SUC n}}$ % fock sm n

Since that the state number in the left hand side is SUC n, then the theorem is valid for all fock states except at zero, i.e., the vac state. Recall that we have proved that the left hand side is equal to zero_cfun for the vac state. However, the following theorem is valid for any state including the vac state:

**Theorem 17.**

$\forall$n sm.
  is_sm sm $\wedge$ ((creata_of_sm sm (fock sm n)) = cfun_zero)
    $\Rightarrow$ (creat_of_sm sm) (fock sm n) = $\sqrt{\text{SUC n}}$ % fock sm (SUC n)

The above theorems are recurrence relations, if we are able to solve any of them, we can then get a non-recursive definition. The following provides the solution of the recurrence relation of Theorem 17:

**Theorem 18.**

$\forall$s inprod cs H omega vac.
  let sm = ((s, inprod), cs, H), omega, vac in
  is_sm sm $\wedge$ ($\forall$n. (creat_of_sm sm) (fock sm n) = cfun_zero)
    $\Rightarrow$ $\forall$m. fock sm m = $\frac{1}{\sqrt{\text{m!}}}$ % (creat_of_sm sm pow m) vac

This concludes the fock states formalization. In the next section, we will see how to formalize coherent states using the previously presented theorems and definitions.

### 4.3 Coherent States

Based on the fock states definition and infinite summation, a coherent state is defined as follows:

**Definition 13.**

coherent sm $\alpha$ =
  let sm = ((s, inprod), cs, H), omega, vac in
    $\exp(-\frac{|\alpha|^2)}{2}))\%$ cfun_infsum (s, inprod) (from 0) ($\lambda$n. $\frac{\alpha^{\text{n}}}{\sqrt{\text{n!}}}\%$(focksmn))

where $\alpha$ is the state parameter. Recall that, the number of photons in a coherent stream is Poisson distributed with expectation $|\alpha|^2$. Note that Definition 13 corresponds to Equation (3).

Next, we need to make sure that the above definition is convergent. As illustrated in Section 3, we have handled a similar situation by defining the summable predicate:

**Definition 14.**

coherent_summable sm $\alpha \Leftrightarrow$
  let (((s, inprod), cs, H), omega, vac) = sm in
    cfun_summable (s, inprod) (from 0) ($\lambda$n. $\frac{\alpha^{\text{n}}}{\sqrt{\text{n!}}}\%$(fock sm n))

Theorem 16 plays a crucial role in proving the relation between coherent states and the annihilation operator. However, it has a problem since it is only valid for fock states greater than zero (i.e., vac state). Consequently, we have to rewrite the coherent definition in a way that allows the application of Theorem 16:

**Theorem 19.**

$$\begin{array}{l}\forall \texttt{s inprod cs H omega vac } \alpha.\\ \quad \texttt{let sm} = ((\texttt{s}, \texttt{inprod}), \texttt{cs}, \texttt{H}), \texttt{omega}, \texttt{vac in}\\ \quad \texttt{coherent\_summable sm } \alpha \Rightarrow\\ \qquad \texttt{coherent sm a} = \exp(-\frac{|\alpha|^2)}{2})) \ \%(\texttt{vac}+\\ \texttt{cfun\_infsum } (\texttt{s}, \texttt{inprod}) \ (\texttt{from 0}) \ (\lambda \texttt{n}. \frac{\alpha^{(\texttt{SUC n})}}{\sqrt{(\texttt{SUC n})!}} \%(\texttt{fock sm } (\texttt{SUC n}))))\end{array}$$

It is important to mention here that vac is a coherent state with $\alpha = 0$. Although it is not covered by Definition 13, we can still prove this based on Theorem 13, by showing that the vac state is an eigenvector of the annihilator. We can appreciate the importance of the vac state since it acts as a coherent and a fock state at the same time. Fortunately, this allows us to use the properties of both notions which is very helpful.

Now, we can prove that coherent states are eigenvectors of the annihilation operator, with eigenvalue $\alpha$ based on Theorems 13, 16 and 19:

**Theorem 20.**

$$\begin{array}{l}\forall \texttt{sm } \alpha.\\ \quad \texttt{is\_sm sm} \wedge \ ((\texttt{creat\_of\_sm sm } (\texttt{fock sm n})) = \texttt{cfun\_zero})\\ \quad \wedge \ \texttt{coherent\_summable sm } \alpha \wedge \texttt{is\_bounded } (\texttt{s}, \texttt{inprod}) \ (\texttt{anhh\_of\_sm sm})\\ \quad \wedge \ (\texttt{coherent sm a} = \texttt{cfun\_zero}) \Rightarrow\\ \qquad \texttt{is\_eigen\_pair}(\texttt{a\_of\_sm sm}) \ (\texttt{coherent sm } \alpha, \alpha)\end{array}$$

This concludes our HOL formalization of coherent light and the underlying mathematical and physical aspects which costs 1500 lines of HOL code. In the following section, we briefly present a potential application of our formalization in quantum computers as a future work.

## 5 Conclusion and Future Work

Quantum optics explores new and extremely useful phenomena and properties of light as a stream of photons. However, the analysis of quantum optical systems is complex. In particular, the traditional analysis techniques – simulation in optical laboratories, paper-and-pencil, numerical methods, and computer algebra systems – suffer from a number of problems: 1) Safety, 2) Cost, 3) Expressiveness and 4) Human Error. We believe that the proposed formalization of quantum optics can alleviate the limitations listed above.

Coherent light (or states) is an essential notion in quantum optics since it eases the analysis of many quantum systems. We have addressed the formal definition of coherent states, then we provided a theorem which proves that

coherent states are eigenvectors of the creator operator. This development is handled in three major steps: 1) we started by formally defining fock states which represent the basis of quantum optics states space, then proved how the creation and annihilation operators affect the fock states, and finally derived a non-recursive definition for them. We also have proved that fock states are eigenvectors of the photon number operator; 2) since coherent states are formed by infinite summation of fock states, we have developed infinte/finite summation over quantum states in addition to the notion of limit; and 3) we were able to provide a formal definition of coherent light and show its relation with the annihilation operator.

One of the most interesting applications of coherent light is quantum computers, where coherent states are proposed to model quantum bits. Quantum computers firstly proposed in 1985 by Deutsch [1], after Feyman [4] had proved that quantum physics phenomena cannot be simulated over ordinary machines. They have the potential of solving certain problems exponentially faster than ordinary machines. Quantum bits and quantum gates are pillars of a quantum machine, as digital bits and gates for computers. $|0\rangle$ and $|1\rangle$ are the pure states of quantum computers. And hence, a quantum bit is equal to : $|Qbit\rangle = \delta|0\rangle + \beta|1\rangle$.

Coherent states are proposed to model quantum bits [16], where $|\alpha\rangle$ and $|-\alpha\rangle$ correspond to $|0\rangle$ and $|1\rangle$, respectively. Many quantum gates where implemented based on this model. For example, the quantum flip gate, which converts $\delta|0\rangle + \beta|1\rangle$ into $\beta|0\rangle + \delta|1\rangle$. Implementing such a gate requires to correlate coherent states with the so-called *displacement operator*, which can be physically implemented as a beam splitter and then cascade a phase conjugating mirror along with a beam splitter to form a quantum flip gate. In order to tackle such a gate in the future, it requires us to define a mirror and a displacement operator (or a beam splitter). The formalization of these devices can be handled using the foundations presented in this paper along with some additional mathematical concepts, such as summation over quantum operators and exponentiation of quantum operators. Thereby, the formalization and analysis of quantum flip gates is one of our essential future work.

## References

1. Deutsch, D.: Quantum theory, the church-turing principle and the universal quantum computer. Proceedings of the Royal Society 400(1818), 97–117 (1985)
2. Duck, I., Sudarshan, E.C.G.: 100 Years of Planck's Quantum. World Scientific (2000)
3. Feagin, J.M.: Quantum Methods with Mathematica. Springer (2002)
4. Feynman, R.: Simulating physics with computers. International Journal of Theoretical Physics 21, 467–488 (1982), doi:10.1007/BF02650179
5. Institute for Quantum Science and Technology at the University of Calgary. Introduction to an Optical lab (2014), `http://old.rqc.ru/quantech/memo.php`
6. Harrison, J.: HOL Light: A Tutorial Introduction. In: Srivas, M., Camilleri, A. (eds.) FMCAD 1996. LNCS, vol. 1166, pp. 265–269. Springer, Heidelberg (1996)
7. Harrison, J.: The HOL Light Theory of Euclidean Space. Journal of Automated Reasoning 50(2), 173–190 (2013)

8. Jennewein, T., Barbieri, M., White, A.G.: Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. Journal of Modern Optics 58(3-4), 276–287 (2011)
9. Li, Y., Browne, D.E., Ch, L.: Kwek, R. Raussendorf, and T. Wei. Thermal states as universal resources for quantum computation with always-on interactions. Physical Review Letter 107, 060501 (2011)
10. Mahmoud, M.Y., Aravantinos, V., Tahar, S.: Formalization of infinite dimension linear spaces with application to quantum theory. In: Brat, G., Rungta, N., Venet, A. (eds.) NFM 2013. LNCS, vol. 7871, pp. 413–427. Springer, Heidelberg (2013)
11. Mahmoud, M.Y.: On the Quantum Formalization of Coherent Light in HOL - HOL Light script, `http://hvg.ece.concordia.ca/projects/qoptics/coh-light.php`
12. Mandel, L., Wolf, E.: Optical Coherence and Quantum Optics. Cambridge University Press (1995)
13. Milonni, P., Nieto, M.M.: Coherent states. In: Compendium of Quantum Physics, pp. 106–108. Springer (2009)
14. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2010)
15. Institute of Quantum Optics at Leibniz University of Hannover. General directives for safety in the institute of quantum optics (2014), `http://www.iqo.uni-hannover.de/fileadmin/institut/pdf/job%20security/3._Sicherheitmerkblatt06012014_engl.pdf`
16. Ralph, T.C., Gilchrist, A., Milburn, G.J., Munro, W.J., Glancy, S.: Quantum computation with optical coherent states. Physical Review A 68, 042319 (2003)
17. Santori, C., Fattal, D., Yamamoto, Y.: Single-photon Devices and Applications. Physics textbook. John Wiley & Sons (2010)
18. Tan, S.M.: A computational toolbox for quantum and atomic optics. Journal of Optics B: Quantum and Semiclassical Optics 1(4), 424 (1999)
19. Walls, D.F., Milburn, G.J.: Quantum Optics. Springer (2008)