

## NetXPTO - LinkPlanner

2 de Outubro de 2017

---

## Conteúdo

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Simulator Structure</b>	<b>4</b>
2.1	System . . . . .	4
<b>3</b>	<b>Development Cycle</b>	<b>5</b>
<b>4</b>	<b>Visualizer</b>	<b>6</b>
<b>5</b>	<b>Case Studies</b>	<b>7</b>
5.1	QPSK Transmitter . . . . .	7
5.2	BPSK Transmission System . . . . .	9
5.3	Quantum Noise . . . . .	13
5.4	Continuos Variable Quantum Transmission System . . . . .	24
5.5	Simplified Coherent Receiver . . . . .	37
5.5.1	Minimum Phase Signal . . . . .	37
5.5.2	KK Scheme . . . . .	38
5.5.3	Tx side . . . . .	39
5.5.4	Rx side . . . . .	45
5.6	Oblivious Transfer with Discrete Variables . . . . .	47
5.6.1	OT Protocol Detailed . . . . .	47
5.6.2	OT Protocol - Potential Problems . . . . .	51
5.6.3	Simulation . . . . .	51
5.6.4	Experimental . . . . .	53
5.7	Radio Over Fiber Transmission System . . . . .	54
5.7.1	Simulation . . . . .	54
5.7.2	Experimental . . . . .	54
<b>6</b>	<b>Library</b>	<b>55</b>
6.1	Add . . . . .	56
6.2	Bit Error Rate . . . . .	57

Conteúdo

2

6.3

Binary source . . . . .

58

6.4

Clock . . . . .

62

6.5

Coupler 2 by 2 . . . . .

64

6.6

Decoder . . . . .

65

6.7

Discrete to continuous time . . . . .

68

6.8

Homodyne receiver . . . . .

70

6.9

IQ modulator . . . . .

74

6.10

Local Oscillator . . . . .

76

6.11

MQAM mapper . . . . .

78

6.12

MQAM transmitter . . . . .

81



LinkPlanner is a signals open-source simulator.

The major entity is the system.

A system comprises a set of blocks.

The blocks interact with each other through signals.

### 2.1 System

You can run the System

The NetXPTO-LinkPlanner has been developed by several people using git as a version control system. The NetXPTO-LinkPlanner repository is located in the GitHub site <http://github.com/netxpto/linkplanner>. The more updated functional version of the software is in the branch master. Master should be considered a functional beta version of the software. Periodically new releases are delivered from the master branch under the branch name Release<Year><Month><Day>. The integration of the work of all people is performed by Armando Nolasco Pinto in the branch Develop. Each developer has his own branch with his/her name.

visualizer

## 5.1 QPSK Transmitter

2017-08-25, Review, Armando Nolasco Pinto

This system simulates a QPSK transmitter. A schematic representation of this system is shown in figure 5.1.



Figura 5.1: QPSK transmitter block diagram.

### System Input Parameters

**Parameter:** *sourceMode*

**Description:** Specifies the operation mode of the binary source.

**Accepted Values:** PseudoRandom, Random, DeterministicAppendZeros, DeterministicCyclic.

**Parameter:** *patternLength*

**Description:** Specifies the pattern length used by the source in the PseudoRandom mode.

**Accepted Values:** Integer between 1 and 32.

**Parameter:** *bitStream*

**Description:** Specifies the bit stream generated by the source in the DeterministicCyclic and DeterministicAppendZeros mode.



**Accepted Values:** "XXX..", where X is 0 or 1.

**Parameter:** *bitPeriod*

**Description:** Specifies the bit period, i.e. the inverse of the bit-rate.

**Accepted Values:** Any positive real value.

**Parameter:** *iqAmplitudes*

**Description:** Specifies the IQ amplitudes.

**Accepted Values:** Any four par of real values, for instance  $\{ \{ 1,1 \}, \{ -1,1 \}, \{ -1,-1 \}, \{ 1,-1 \} \}$ , the first value correspond to the "00", the second to the "01", the third to the "10" and the forth to the "11".

**Parameter:** *numberOfBits*

**Description:** Specifies the number of bits generated by the binary source.

**Accepted Values:** Any positive integer value.

**Parameter:** *numberOfSamplesPerSymbol*

**Description:** Specifies the number of samples per symbol.

**Accepted Values:** Any positive integer value.

**Parameter:** *rollOffFactor*

**Description:** Specifies the roll off factor in the raised-cosine filter.

**Accepted Values:** A real value between 0 and 1.

**Parameter:** *impulseResponseTimeLength*

**Description:** Specifies the impulse response window time width in symbol periods.

**Accepted Values:** Any positive integer value.

»»»»> Romil

## 5.2 BPSK Transmission System

### Introduction

This system simulates a BPSK transmitter in back-to-back configuration with additive white Gaussian noise at the receiver. The main objective of this system is to test the developed bit error rate block.

### Functional Description

A simplified diagram of the system being simulated is presented in the Figure 5.2. A random binary string is generated and encoded in an optical signal using a BPSK modulation format. The decoding of the optical signal is accomplished by an homodyne receiver, which combines the signal with a local oscillator. The received binary signal is compared with the transmitted binary signal in order to estimate the BER.

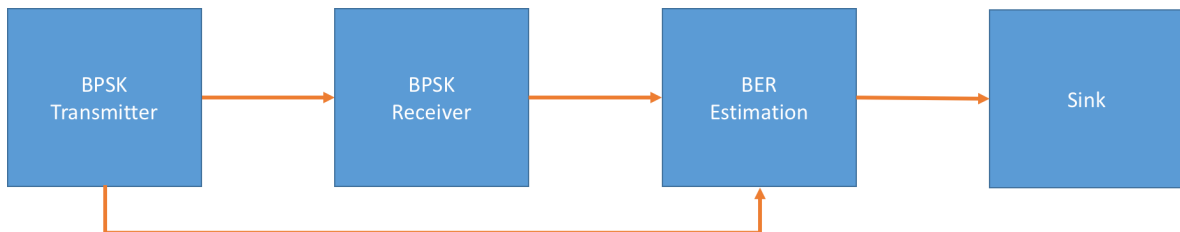


Figura 5.2: Overview of the BPSK system being simulated.

System Blocks	netxpto Blocks
BPSK Transmitter	MQamTransmitter
BPSK Receiver	HomodyneReceiver
BER Estimator	BitErrorRate

### Required files

#### Header Files

File	Description
netxpto.h	Generic purpose simulator definitions.
m_qam_transmitter.h	Generates the signal with coded constellation.
homodyne_reciever.h	Performs coherent detection on the input signal.
sampler.h	Samples the input signal at a user defined frequency.
bit_decider.h	Decodes the input signal into a binary string.
bit_error_rate.h	Calculates the bit error rate of the decoded string.
sink.h	Closes any unused signals.

#### Source Files

File	Description
netxpto.cpp	Generic purpose simulator implementations.
m_qam_transmitter.cpp	Generates the signal with coded constellation.
homodyne_reciever.cpp	Performs coherent detection on the input signal.
sampler.cpp	Samples the input signal at a user defined frequency.
bit_decider.cpp	Decodes the input signal into a binary string.
bit_error_rate.cpp	Calculates the bit error rate of the decoded string.
sink.cpp	Closes any unused signals.

### System Input Parameters

This system takes into account the following input parameters:

System Parameters	Description
numberOfBits	Gives the number of bits to be simulated
bitPeriod	Sets the time between adjacent bits
samplesPerSymbol	Establishes the number of samples each bit in the string is given
pLength	PRBS pattern length
iqAmplitudesValues	Sets the state constellation
outOpticalPower_dBm	Sets the optical power, in units of dBm, at the transmitter output
loOutOpticalPower_dBm	Sets the optical power, in units of dBm, of the local oscillator used in the homodyne detector
localOscillatorPhase	Sets the initial phase of the local oscillator used in the homodyne detector
transferMatrix	Sets the transfer matrix of the beam splitter used in the homodyne detector
responsivity	Sets the responsivity of the photodiodes used in the homodyne detector
amplification	Sets the amplification of the trans-impedance amplifier used in the homodyne detector
noiseAmplitude	Sets the amplitude of the gaussian thermal noise added in the homodyne detector
delay	Sets the delay factor of the homodyne detector
posReferenceValue	Set the positive and negative reference values for the bit decision block
negReferenceValue	
confidence	Sets the confidence interval for the calculated QBER
midReportSize	Sets the number of bits between generated QBER mid-reports

### Inputs

This system takes no inputs.

## Outputs

This system outputs the following objects:

**Parameter:** Signals:

**Description:** Initial Binary String; ( $S_0$ )

**Description:** Optical Signal with coded Binary String; ( $S_1$ )

**Description:** Local Oscillator Optical Signal; ( $S_2$ )

**Description:** Beam Splitter Outputs; ( $S_3, S_4$ )

**Description:** Homodyne Detector Electrical Output; ( $S_5$ )

**Description:** Decoded Binary String; ( $S_6$ )

**Description:** BER result String; ( $S_7$ )

**Parameter:** Other:

**Description:** Bit Error Rate report in the form of a .txt file. (BER.txt)

## Simulation Results

The following results show the dependence of the error rate with the signal power assuming a constant Local Oscillator power of  $-20$  dBm. For reference, the eye diagram at 3 different power levels are also presented. The full line represents the expected results, note that it has been computed assuming a gaussian distribution of the thermal noise, which is not exact given the effect of the matched filter applied before the decoding of the bits, this explains the deviation between the simulation results and the expected values.

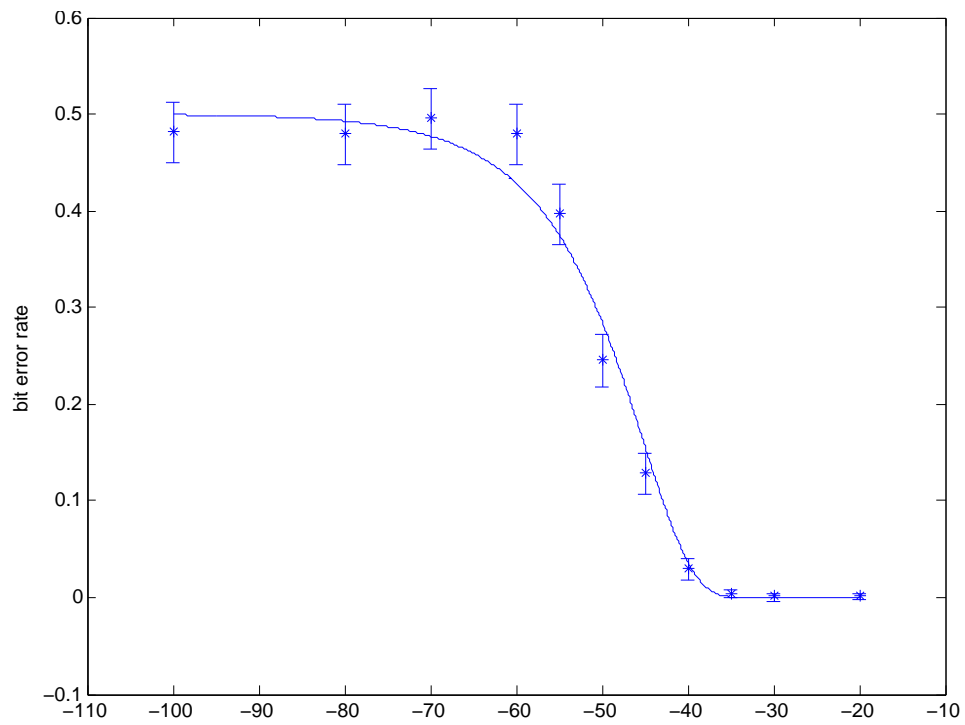
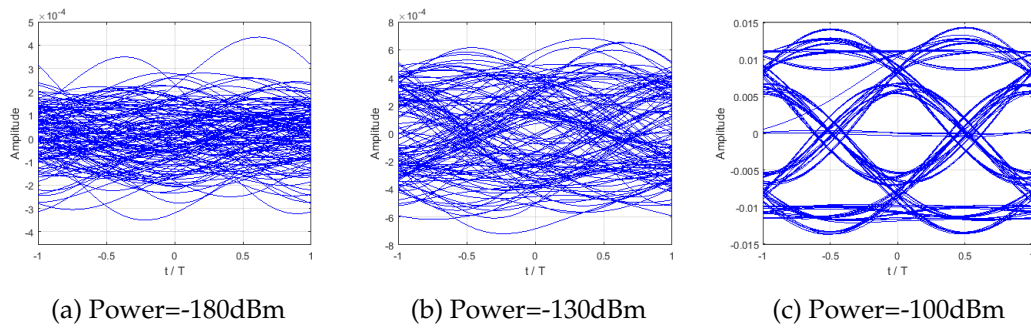


Figura 5.3: Bit Error Rate in function of the signal power in dBm.



(a) Power=-180dBm

(b) Power=-130dBm

(c) Power=-100dBm

Figura 5.4: Eye diagrams at different signal powers.

## 5.3 Quantum Noise

### Introduction

This document describes an emission and detection system which is used to simulate the effects of quantum noise. The system is based on the transmission of coherent states as the support of information. The following section introduces some aspects about coherent states, with special focus on quantum noise.

We start by defining number states  $|n\rangle$  (or Fock states), which correspond to states with perfectly fixed number of photons.<sup>1</sup> Associated to those states are two operators, the creation  $\hat{a}^\dagger$  and annihilation  $\hat{a}$  operators, which in a simple way, remove or add one photon from a given number state.<sup>2</sup> Their action is defined as:

$$\hat{a} |n\rangle = \sqrt{n} |n-1\rangle \quad \hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle \quad \hat{n} |n\rangle = n |n\rangle \quad (5.1)$$

in which  $\hat{n} = \hat{a}^\dagger \hat{a}$  is the number operator. Therefore, number states are eigenvectors of the number operator.

Coherent states have properties that closely resemble classical electromagnetic waves, and are generated by single-mode lasers well above the threshold.<sup>3</sup> We can defined them, using number states in the following manner:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (5.2)$$

in which the complex number  $\alpha$  is the sole parameter that characterizes it. In fact, if we calculate the expected number of photons with  $\langle \alpha | \hat{n} | \alpha \rangle$  we will obtain  $|\alpha|^2$ . The coherent state is an eigenstate of the annihilation operator,  $\hat{a} |\alpha\rangle = \alpha |\alpha\rangle$ .

Using the creation and annihilation operators, we can define two quadrature operators:<sup>4</sup>

$$\hat{X} = \frac{1}{2} (\hat{a}^\dagger + \hat{a}) \quad \hat{Y} = \frac{i}{2} (\hat{a}^\dagger - \hat{a}) \quad (5.3)$$

The expected value of these two operators, using a coherent state  $|\alpha\rangle$  are:

$$\langle \hat{X} \rangle = \text{Re}(\alpha) \quad \langle \hat{Y} \rangle = \text{Im}(\alpha) \quad (5.4)$$

We see that the expected value of these operators give us the real and imaginary part of  $\alpha$ . Now, we can obtain the uncertainty of these operators, using:

$$\text{Var}(\hat{X}) = \langle \hat{X}^2 \rangle - \langle \hat{X} \rangle^2 \quad (5.5)$$

---

<sup>1</sup>Loudon, p.184

<sup>2</sup>Mark Fox, p.155

<sup>3</sup>Loudon, p.190

<sup>4</sup>Loudon, p.138, (4.3.36)

For each of these quadrature operators the variance will be:

$$\text{Var}(\hat{X}) = \text{Var}(\hat{Y}) = \frac{1}{4} \quad (5.6)$$

This result show us that for both quadratures, the variance of measurement is the same and independent of the value of  $\alpha$ .

### Experimental setup

To confirm the previous theoretical results, the quadrature of the input signal  $|\alpha\rangle$  must be measured. The chosen experimental technique is the balanced homodyne detection (fig 5.5), which measures the phase of the input signal (S), relative to the phase of a local oscillator (LO). The local oscillator has the same frequency as the input signal, but a much larger amplitude. This technique consists in combining the input signal and the local oscillator, using a 50:50 beam splitter, from whom two beams emerge, which are then converted to currents using photodiodes. Finally, the two currents are subtracted, resulting in an output current.

By changing the phase of the local oscillator, in particular by  $\pi/2$ , we will obtain the quadrature of the signal. Therefore, the  $\hat{X}$  operator will correspond to the in-phase component and  $\hat{Y}$  operator correspond to quadrature component.<sup>5</sup>

In the lab and in our simulations, we will use a more complex system, the double balanced homodyne detection, which allows the simultaneous measurement of two quadratures. The signal is divided in two beam with half the power of the original. One of the beams will be used in a balanced homodyne detection with a local oscillator. The other beam will be used in another balanced homodyne detection, but using a local oscillator with a phase difference  $\pi/2$  relative to the first one.

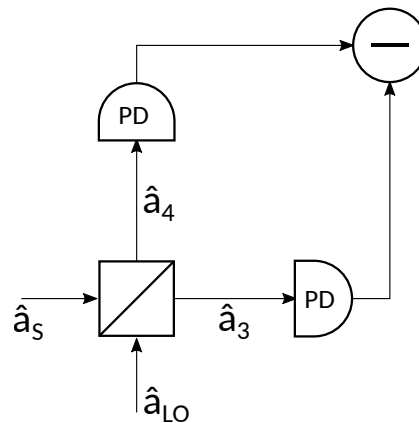


Figura 5.5: Balanced double homodyne detection.

### Noise sources

<sup>5</sup>Mark Fox, p. 140

The detection of light using photodiodes is subjected to various sources of noise. One of these sources is the electrical field itself. The interaction of the signal with the vacuum field adds quantum noise to the detection. Another source of noise comes from the detection system, such as photodiodes and other electrical circuits, originating various kinds of noise, such as thermal noise, dark noise and amplifier noise.<sup>6</sup> In the following sections, we will focus on two noise sources, quantum noise and thermal noise.

### Quantum Noise

In order to grasp this effect, the quantum mechanical description of balanced homodyne detection will be used, employing quantum operators to describe the effect of each component in the system (fig. 5.5). We start with the operators  $\hat{a}_S$  and  $\hat{a}_{LO}$  corresponding to the annihilation operator for the signal and local oscillator, which are the inputs in a beam divider. The outputs will be  $\hat{a}_3$  and  $\hat{a}_4$ . Using a balanced beam splitter, we can write the output as:

$$\hat{a}_3 = \frac{1}{\sqrt{2}} (\hat{a}_S + \hat{a}_{LO}) \quad \hat{a}_4 = \frac{1}{\sqrt{2}} (\hat{a}_S - \hat{a}_{LO}) \quad (5.7)$$

The final output of a homodyne measurement will be proportional to the difference between the photocurrents in arm 3 and 4. Then

$$I_{34} = I_3 - I_4 \sim \langle \hat{n}_3 - \hat{n}_4 \rangle \quad (5.8)$$

We can define an operator that describes the difference of number of photons in arm 3 and arm 4:

$$\hat{m} = \hat{a}_3^\dagger \hat{a}_3 - \hat{a}_4^\dagger \hat{a}_4 \quad (5.9)$$

If we assume that the local oscillator produces the coherent state  $|\beta\rangle$ , then the expected value of this measurement will be:

$$\langle m \rangle = 2|\alpha||\beta| \cos(\theta_\alpha - \theta_\beta) \quad \text{Var}(m) = |\alpha|^2 + |\beta|^2 \quad (5.10)$$

The local oscillator normally has a greater power than the signal (VER REFERENCIAS), then  $|\alpha| \ll |\beta|$ . If we use as unit,  $2|\beta|$ , then these two quantities can be simplified to:

$$\langle m \rangle = |\alpha| \cos(\theta_\alpha - \theta_\beta) \quad \text{Var}(m) \approx \frac{1}{4} \quad (5.11)$$

7

Has we have seen previously, in order to measure two quadratures simultaneously, we can use double balanced homodyne detection. For each quadrature, the input signal now has half the power, so  $|\alpha| \rightarrow |\alpha|/\sqrt{2}$ . If we use a local oscillator that produces states  $|\beta\rangle$ , then we can divide it in two beams in state  $|\beta/\sqrt{2}\rangle$  and  $|i\beta/\sqrt{2}\rangle$  which will be used in each homodyne detection. In this setting, the expected values for each quadrature,  $X$  and  $Y$ , (in normalized values of  $\sqrt{2}|\beta|$ ) are:

$$\langle m_X \rangle = \left| \frac{\alpha}{\sqrt{2}} \right| \cos(\theta_\alpha - \theta_\beta) \quad \text{Var}(m_X) \approx \frac{1}{4} \quad (5.12)$$

<sup>6</sup>Hans, p.185

<sup>7</sup>Referencia indirecta: Livro: Hans, p.207



$$\langle m_Y \rangle = \left| \frac{\alpha}{\sqrt{2}} \right| \sin(\theta_\alpha - \theta_\beta) \quad \text{Var}(m_Y) \approx \frac{1}{4} \quad (5.13)$$

Therefore the measurement of each quadrature will have half the amplitude, but the same variance.

### Thermal noise

Thermal noise is generated by electrons in response to temperature. It's contribution to the resulting current can be described by the following equation:

$$\langle (\Delta i_T)^2 \rangle = 4K_B T_0 B / R_L \quad (5.14)$$

in which  $K_B$  it's Boltzmann's constant,  $T_0$  is the absolute temperature,  $B$  is the bandwidth and  $R_L$  is the receiver load impedance. The  $B$  value is imposed by default or chosen when the measurements are made, but the  $R_L$  value is dependent in the internal setup of the various components of the detection system. Nevertheless, for simulation purposes, we can just introduce an experimental value.

### Simulation Implementation

The simulation setup is represented in figure 5.6. It starts by generating random states from a given constellation. The output from the generator is received in the Optical Hybrid where it is mixed with a local oscillator, outputting four diferent optical signals. Two of those signals are detected by a photodiode which will output a electrical signal propotional to a quadrature of the inicial signal. The other two signals are detected by the other photodiode, which outputs another quadrature of the signal dephased  $\pi/2$  relative to the first one.

System Blocks	netxpto Blocks
M - Quadrature Amplitude Modulator	MQamTransmitter
Local Oscillator	LocalOscillator
90deg Optical Hybrid	OpticalHybrid
Photodiode	Photodiode
Sampler?	Sampler

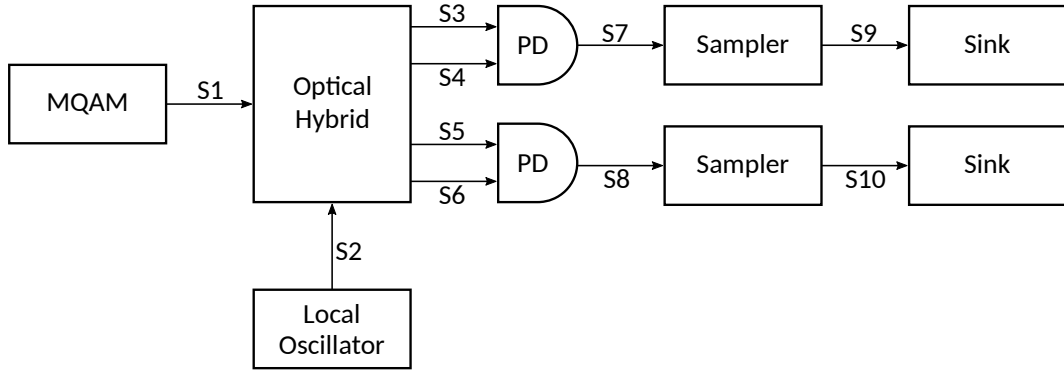


Figura 5.6: Overview of the optical system being simulated.

### Quantum Noise implementation

In the simulation, each arm's photocurrent ( $I_3$  and  $I_4$ ) is modelled as the output of the photodiode's conversion of optical power. This incident optical power follows the photon number statistics, scaled by the power of a single photon. The final current,  $I_{34}$ , will be simply the difference between the photocurrents of both arms. We start by calculating the expected value and variance of the photon number given by  $\hat{n}_3$ :

$$\langle \hat{n}_3 \rangle = \frac{1}{2} (|\alpha|^2 + |\beta|^2 + 2 \cos(\phi_\alpha - \phi_\beta)) \quad \text{Var}(\hat{n}_3) = \langle \hat{n}_3 \rangle \quad (5.15)$$

If we calculate the expected value and variance for  $\hat{n}_4$ , the resulting values will be  $\text{Var}(\hat{n}_4) = \langle \hat{n}_4 \rangle$ . Therefore both photon statistics can be modelled by Poisson distributions:

$$n_i \sim \text{Poisson}(\langle n_i \rangle) \quad (5.16)$$

In the simulation, a photodiode has 2 inputs. Each input corresponds to a mean complex amplitude  $\bar{\Psi}_i$ . This amplitude corresponds to the power  $\bar{P}_i = |\bar{\Psi}_i|^2 = \langle n_i \rangle P_\lambda$  in which  $P_\lambda$  is the power of a single photon. What we want is the power after adding noise,  $P_i = n_i P_\lambda$ . To model  $n_i$ , we will use a gaussian approximation of  $\sqrt{n_i}$ , for  $n_i \gg 0$ , which will give us a continuous distribution:

$$\sqrt{n_i} \sim \text{Gaussian}(\sqrt{\langle n_i \rangle}, 1/2) \quad (5.17)$$

Therefore:

$$n_i \approx \left( \sqrt{\langle n_i \rangle} + \frac{1}{2}G \right)^2 = \langle n_i \rangle + \sqrt{\langle n_i \rangle}G + \frac{1}{4}G^2 \quad (5.18)$$

in which  $G$  is a random variable with a gaussian distribution with mean 0 and variance 1.

Therefore, the output power of each becomes:

$$P_i = n_i P_\lambda = \bar{P}_i + \sqrt{P_\lambda \bar{P}_i}G + \frac{1}{4}P_\lambda G^2 \quad (5.19)$$

### Thermal Noise Implementation

In the experimental setting, it is assumed that this noise is created by the detection system. To simulate this noise, the photodiode will add it to the output current as a simple gaussian distribution with mean 0 and variance according to experimental settings.

### Simulation Results

To test the simulated implementation, a series of states  $\{|\phi_i\rangle\}$  were generated and detected, resulting in a series of measurements  $\{(x_i, y_i)\}$ . The simulation result is presented in figure 5.7:

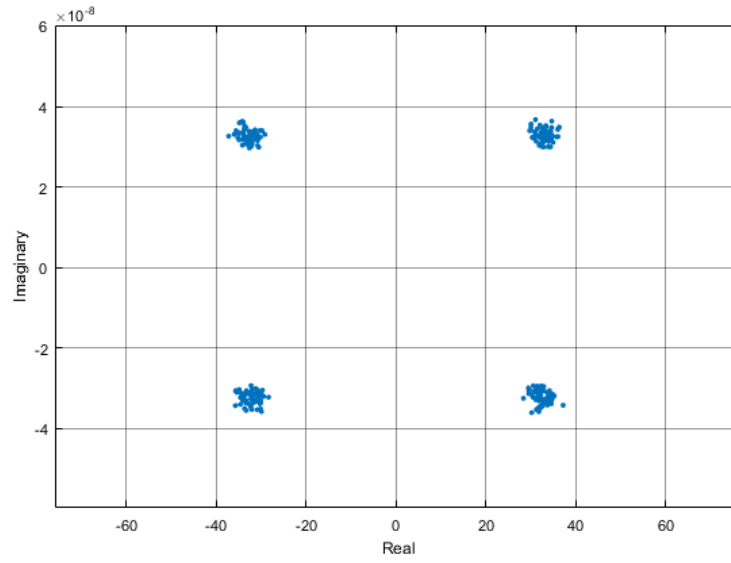


Figura 5.7: Simulation of a constellation of 4 states ( $n = 100$ )

We see that the measurements made groups in certain regions. Each of this groups is centered in the expected value  $(\langle X \rangle, \langle Y \rangle)$  of one the generated states. Also, they show some variance, which was tested for various expected number of photons,  $\langle n \rangle$ , resulting in figure 5.8:

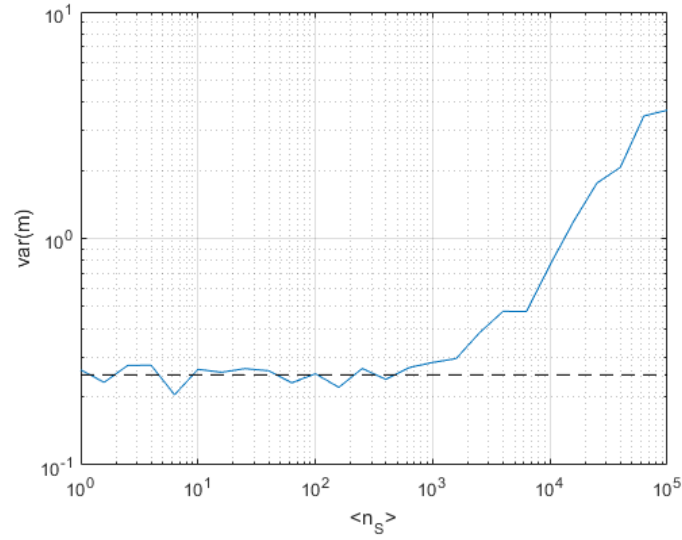


Figura 5.8: Simulation of the variance of  $m$ .  
Local oscillator expected number of photons:  $10^4$

It was expected that the variance should independent of the input's signal number of photons. Plot 5.8 shows that for low values of  $n_s$ , the simulation is in accordance with the theoretical prevision, with  $\text{Var}(X) = \text{Var}(Y) = \frac{1}{4}$ . For large values of  $n_s$ , when the number of photons is about the same has the local oscillator, the quantum noise variance starts to grow proportionally to  $n_s$ , in accordance with the non approximated calculation of quantum noise (eq. 5.10).

#### Noise Variance with LO power Simulation

The following plot shows the behavior of current noise variance  $\langle (\Delta i)^2 \rangle$  with local oscillator power,  $P_{LO}$ :

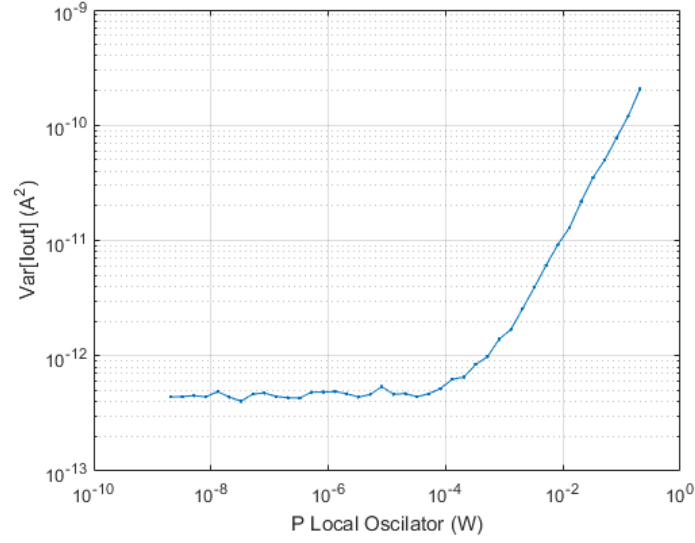


Figura 5.9: Output current variance in function of LO power.

We see that for low LO power, the dominant noise is the thermal contribution, but for higher power, quantum noise dominates, growing proportionally to  $P_{LO}$ . This in accordance with equation 5.11

### Comparison to experimental results

As we have seen earlier, the system will manifest noise even in the absence of input signal (eq 5.10). The experimental procedure for this measurement consisted in just inputting the local oscillator laser and no signal. For each value of  $P_{LO}$ , the local oscillator was pulsed, and for each pulse, the variance of the plateau of the maximum was calculated. The final variance was simply the mean of the variances of all pulses.

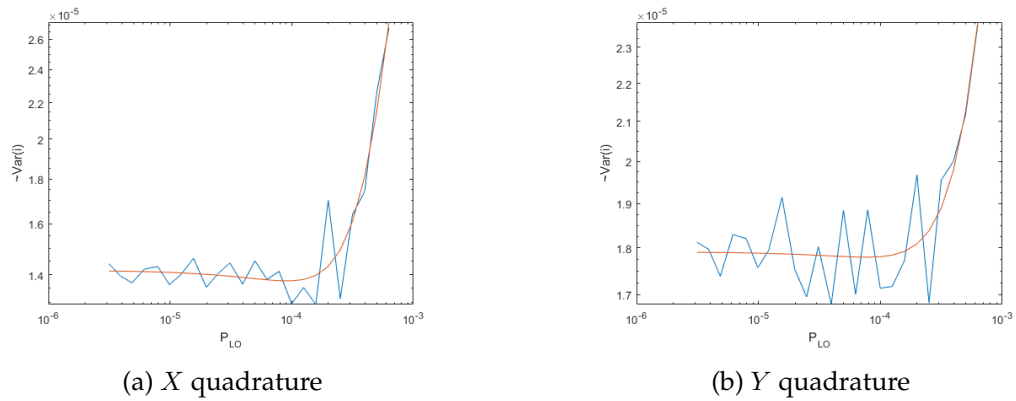


Figura 5.10: Noise variance dependency with local oscillator power for two different quadratures. Experimental vs fitted data.

Figures 5.10a and 5.10b show measures measurements of total noise for two different quadratures. For low power of LO, the noise variance fluctuates around a constant value. For high power of LO, ( $P_{LO} > 10^{-4}W$ ), the variance of noise shows an increasing trend roughly proportional to  $P_{LO}^2$ . The expected growth should be proportional to  $P_{LO}$ , but the RIN noise, originated by the electric apparatus, grows quadratically with the power, dominating the noise amplitude for large  $P_{LO}$ .

So, we see that both the simulation and experimental data display a similar behaviour, but the quadratic growth of noise for large  $P_{LO}$  was not predicted in the simulations.

## Required files

### Header Files

File	Description
netxpto.h	Generic purpose simulator definitions.
m_qam_transmitter.h	Outputs a QPSK modulated optical signal.
local_oscillator.h	Generates continuous coherent signal.
optical_hybrid.h	Mixes the two input signals into four outputs.
photodiode.h	Converts two optical signals to a difference of photocurrents.??
sampler.h	Samples the input signal.
sink.h	Closes any unused signals.

### Source Files

File	Description
netxpto.cpp	Generic purpose simulator definitions.
m_qam_transmitter.cpp	Outputs a QPSK modulated optical signal.
local_oscillator.cpp	Generates continuous coherent signal.
optical_hybrid.cpp	Mixes the two input signals into four outputs.
photodiode.cpp	Converts two optical signals to a difference of photocurrents.??
sampler.cpp	Samples the input signal.
sink.cpp	Closes any unused signals.

## System Input Parameters

This system takes into account the following input parameters:

System Parameters	Description
numberOfBitsGenerated	Gives the number of bits to be simulated
bitPeriod	Sets the time between adjacent bits
wavelength	Sets the wavelength of the local oscillator in the MQAM
samplesPerSymbol	Establishes the number of samples each bit in the string is given
localOscillatorPower1	Sets the optical power, in units of W, of the local oscillator inside the MQAM
localOscillatorPower2	Sets the optical power, in units of W, of the local oscillator used for Bob's measurements
localOscillatorPhase	Sets the initial phase of the local oscillator used in the detection
transferMatrix	Sets the transfer matrix of the beam splitter used in the homodyne detector
responsivity	Sets the responsivity of the photodiodes used in the homodyne detectors
bufferLength	Sets the length of the buffer used in the signals
iqAmplitudeValues	Sets the amplitude of the states used in the MQAM
shotNoise	Chooses if quantum shot noise is used in the simulation
samplesToSkip	Sets the number of samples to skip when writing out some of the signal files
thermalNoise	Chooses if thermal noise is used in the simulation
thermalNoiseAmplitude	Sets the amplitude of the thermal noise

### Inputs

This system takes no inputs.

**Outputs**

The system outputs the following objects:

**Parameter:** Signals:

**Description:** Binary Sequence used in the MQAM; ( $S_0$ )

**Description:** Local Oscillator used in the MQAM; ( $S_1$ )

**Description:** Local Oscillator used in the detection; ( $S_2$ )

**Description:** Optical Hybrid Outputs; ( $S_3, S_4, S_5, S_6$ )

**Description:** In phase Photodiode output; ( $S_7$ )

**Description:** Quadrature Photodiode output; ( $S_8$ )

**Description:** In phase Sampler output; ( $S_9$ )

**Description:** Quadrature Sampler output; ( $S_{10}$ )

**Known Problems**

1. —



## 5.4 Continuous Variable Quantum Transmission System

Student Name: Daniel Pereira

Starting Date: May 1, 2017

Goal: Simulation and experimental validation of a continuous variable transmission system.

Description of the Laboratorial and Simulation Setup:

Theoretical Description of the System:

Laboratorial and Simulation Results:

Discussion:

In this section a continuous variable quantum transmission system is analyzed. The results here presented follow closely the [1]. In [1], the security of a continuous variable quantum key distribution (CV-QKD) system is studied theoretically, here we complete that theoretical study with simulations results.

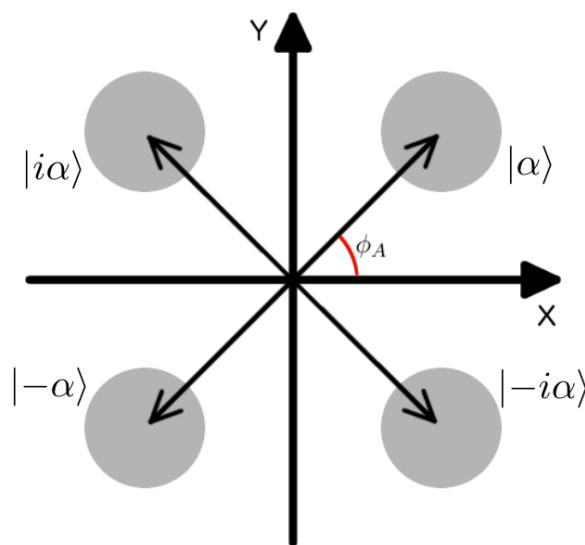


Figura 5.11: State constellation

The state constellation used in the system is presented in Figure 5.11. The emitter (usually named Alice) is going to use two basis, the  $45^\circ$  base and the  $-45^\circ$  base. In the  $45^\circ$  base, Alice sends one of two values, 1 and  $-1$ , which correspond to the states  $|\alpha\rangle$  and  $|- \alpha\rangle$ . In the  $-45^\circ$  base, Alice can also send one of two values, 1 and  $-1$ , which correspond to the states  $|-i\alpha\rangle$  and  $|i\alpha\rangle$ . At the end Alice is going to send one of the four states  $|\alpha\rangle$ ,  $|- \alpha\rangle$ ,  $|-i\alpha\rangle$ , and  $|i\alpha\rangle$ , with equal probability.

Because we don't know *a priori* which state is going to be transmitted, neither which basis is going to be used, and to incorporate our "ignorance" in the system description, we can

work with the density operator. The density operator is a proper tool to describe "statistical mixtures". A "statistical mixtures" is one state, from a possible set, but we don't know which state it is. There is no state superposition.

Since all states have the same probability of occurring, the state density operator is given by:

$$\hat{\rho} = \frac{1}{4} (|\alpha\rangle \langle\alpha| + |-\alpha\rangle \langle-\alpha| + |i\alpha\rangle \langle i\alpha| + |-i\alpha\rangle \langle -i\alpha|). \quad (5.20)$$

The probability to detect at the receiver the state  $|\alpha\rangle$  is given by

$$P(\alpha) = \langle\alpha| \hat{\rho} |\alpha\rangle = \frac{1}{4}. \quad (5.21)$$

Note that the density operator is equivalent to the wave function in terms of the system description.

From the receiver perspective, i.e. from the Bob perspective, and after knowing the base used by Alice. The density operator can be reduce to,

$$\hat{\rho}_1 = \frac{1}{2} (|\alpha\rangle \langle\alpha| + |-\alpha\rangle \langle-\alpha|), \quad (5.22)$$

$$\hat{\rho}_2 = \frac{1}{2} (|i\alpha\rangle \langle i\alpha| + |-i\alpha\rangle \langle -i\alpha|). \quad (5.23)$$

where 1 corresponds to the  $45^\circ$  base and  $-1$  corresponds to  $-45^\circ$ .

### Single Base Homodyne Detection

The probability of obtaining a quadrature  $\hat{X}_\phi = \hat{X}_1 \cos \phi + \hat{X}_2 \sin \phi$  when measuring the coherent state  $|\alpha\rangle$  is given by the following gaussian distribution:

$$|\langle X_\phi | \alpha \rangle|^2 = \sqrt{\frac{2}{\pi}} e^{-2(X_\phi - \alpha \cos \phi)^2}, \quad (5.24)$$

We can define the "correct" and "wrong" basis measurement probability density, respectively, as:

$$\langle X_i | \hat{\rho}_j | X_i \rangle = \begin{cases} \frac{1}{\sqrt{2\pi}} \left( e^{-2(X_i - \alpha)^2} + e^{-2(X_i + \alpha)^2} \right), & i = j \\ \sqrt{\frac{2}{\pi}} e^{-2X_i^2}, & i \neq j \end{cases}. \quad (5.25)$$

The post selection efficiency (PSE) can be defined as the probability of a measurement in the correct basis yields a result that satisfies the limit value  $X_0$ :

$$\begin{aligned} P(X_0, \alpha) &= \int_{-\infty}^{-X_0} \langle X_1 | \hat{\rho}_1 | X_1 \rangle dX_1 + \int_{X_0}^{\infty} \langle X_1 | \hat{\rho}_1 | X_1 \rangle dX_1 \\ &= \frac{1}{2} \left[ \text{erfc}(\sqrt{2}(X_0 + \alpha)) + \text{erfc}(\sqrt{2}(X_0 - \alpha)) \right]. \end{aligned} \quad (5.26)$$

The bit error rate (BER) is the normalized probability of, after choosing the correct basis, obtaining the wrong bit value:

$$Q(X_0, \alpha) = \frac{1}{P(X_0, \alpha)} \int_{-\infty}^{-X_0} |\langle X_i | \alpha \rangle| dX_i = \frac{\text{erfc}(\sqrt{2}(X_0 + \alpha))}{2P(X_0, n)} \quad (5.27)$$

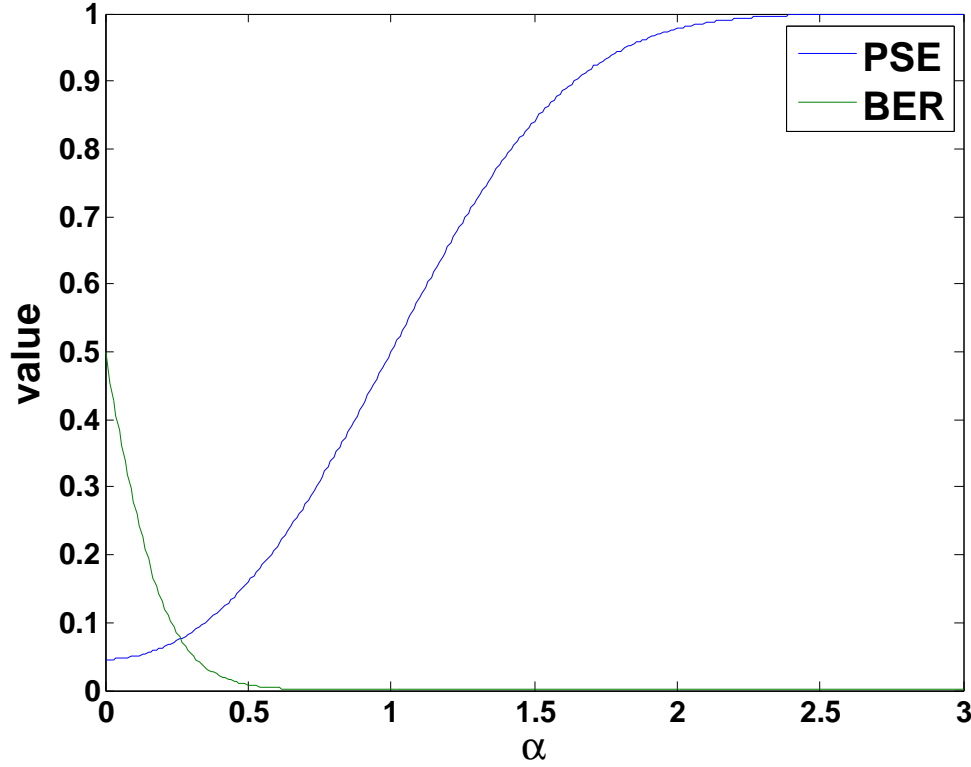


Figura 5.12: BER and PSE in function of  $\alpha$  for the single homodyne setup.  $X_0 = 1$  was used

### Double Homodyne setup

In our proposed double homodyne protocol both quadratures are measured simultaneously, as such the concept of correct and wrong basis measurements has no value. Our protocol also makes use of a locally generated Local Oscillator (LO), obtained from a different laser than the one used to generate the signal, thus we have to take into account the phase drift between both lasers. High intensity reference pulses are sent periodically to allow for an estimation of the phase drift. The double homodyne setup requires the signal to be divided into the two utilized detectors, so each measurement is made on a coherent state with half the amplitude of the incoming signal  $\alpha \rightarrow \frac{\alpha}{\sqrt{2}}$

For each incoming pulse we measure quadratures  $X_\phi$  and  $Y_\phi$ .  $\phi$  has contributions from both the encoded angle,  $\theta$ , and the phase difference between lasers,  $\epsilon$ , we assume  $\phi = \theta + \epsilon$ .

On the reference pulses no phase is encoded, that is  $\theta = 0$ , thus  $\epsilon$  can be estimated. Assuming  $\epsilon$  doesn't change between a reference pulse and the following signal pulse, the measured quadratures can be cast into the originally sent quadratures  $X_\theta$  and  $Y_\theta$  via:

$$\begin{aligned} X_\theta &= X_\phi \cos \epsilon - Y_\phi \sin \epsilon \\ Y_\theta &= X_\phi \sin \epsilon + Y_\phi \cos \epsilon \end{aligned} \quad (5.28)$$

Assuming an announcement of the coding basis, the density operators (5.22) and (5.23) still apply. We can now define the probability density of obtaining results  $X_\theta$  and  $Y_\theta$ , assuming a state in the  $X_1$  base was sent, as:

$$\langle X_\theta | \hat{\rho}_1 | X_\theta \rangle = \frac{\sqrt{\frac{2}{\pi}}}{4} \left( e^{-2\left(x_\theta - \frac{\alpha}{\sqrt{2}} \cos \theta\right)^2} + e^{-2\left(x_\theta + \frac{\alpha}{\sqrt{2}} \cos \theta\right)^2} \right), \quad (5.29)$$

$$\langle Y_\theta | \hat{\rho}_1 | Y_\theta \rangle = \frac{\sqrt{\frac{2}{\pi}}}{4} \left( e^{-2\left(y_\theta - \frac{\alpha}{\sqrt{2}} \sin \theta\right)^2} + e^{-2\left(y_\theta + \frac{\alpha}{\sqrt{2}} \sin \theta\right)^2} \right). \quad (5.30)$$

Now each state needs to satisfy two limit values,  $X_0$  and  $Y_0$ , to be accepted. Thus, the PSE is now defined as:

$$\begin{aligned} P_{DH}(X_0, Y_0, \alpha) &= \int_{-\infty}^{-X_0} \langle X_\theta | \hat{\rho}_1 | X_\theta \rangle dx_\theta \int_{-\infty}^{-Y_0} \langle Y_\theta | \hat{\rho}_1 | Y_\theta \rangle dy_\theta + \\ &\quad \int_{X_0}^{\infty} \langle X_\theta | \hat{\rho}_1 | X_\theta \rangle dx_\theta \int_{Y_0}^{\infty} \langle Y_\theta | \hat{\rho}_1 | Y_\theta \rangle dy_\theta \\ &= \frac{1}{4} \left\{ \operatorname{erfc} \left[ \sqrt{2} \left( X_0 - \frac{\alpha}{\sqrt{2}} \cos \theta \right) \right] + \operatorname{erfc} \left[ \sqrt{2} \left( X_0 + \frac{\alpha}{\sqrt{2}} \cos \theta \right) \right] \right\} \\ &\quad \left\{ \operatorname{erfc} \left[ \sqrt{2} \left( Y_0 - \frac{\alpha}{\sqrt{2}} \sin \theta \right) \right] + \operatorname{erfc} \left[ \sqrt{2} \left( Y_0 + \frac{\alpha}{\sqrt{2}} \sin \theta \right) \right] \right\}, \end{aligned} \quad (5.31)$$

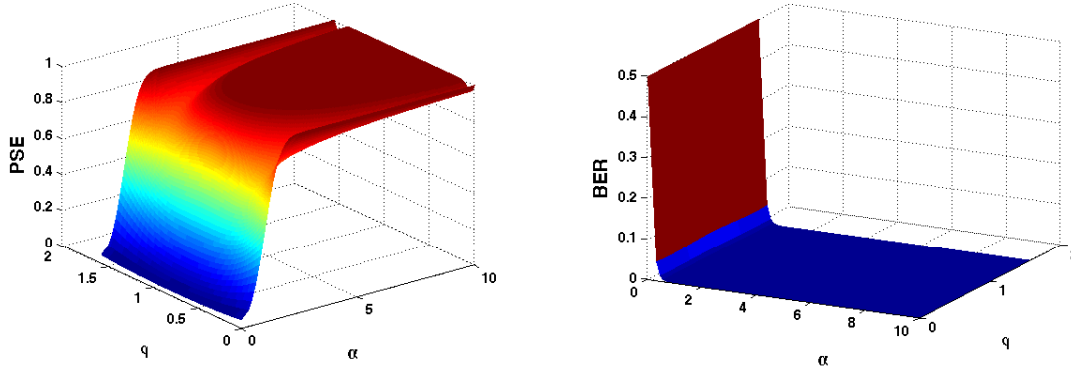
The DH subscript denotes Double Homodyne. In a somewhat similar manner, the BER is now defined as:

$$\begin{aligned} Q_{DH}(X_0, Y_0, \alpha) &= \frac{1}{P_{DH}} \left( \int_{-\infty}^{-X_0} \left| \langle X_\theta | \frac{\alpha}{\sqrt{2}} \rangle \right|^2 dx_\theta \int_{-\infty}^{-Y_0} \left| \langle Y_\theta | \frac{\alpha}{\sqrt{2}} \rangle \right|^2 dy_\theta + \right. \\ &\quad \left. \int_{X_0}^{\infty} \left| \langle X_\theta | -\frac{\alpha}{\sqrt{2}} \rangle \right|^2 dx_\theta \int_{Y_0}^{\infty} \left| \langle Y_\theta | -\frac{\alpha}{\sqrt{2}} \rangle \right|^2 dy_\theta \right) \\ &= \frac{1}{2P_{DH}} \operatorname{erfc} \left[ \sqrt{2} \left( X_0 + \frac{\alpha}{\sqrt{2}} \cos \theta \right) \right] \operatorname{erfc} \left[ \sqrt{2} \left( Y_0 + \frac{\alpha}{\sqrt{2}} \sin \theta \right) \right], \end{aligned} \quad (5.32)$$

note that, in this definition for BER, only values  $\theta \in [0, \frac{\pi}{2}]$  make sense (the sent state was  $\alpha$ ).

### Functional Description

Simplified diagrams of the systems being simulated are presented in Figures 5.14a. and 5.14b. Two optical signals are generated, one with a constant power level of 10 dBm and the other with power in multiples of the power corresponding to a single photon per



(a) PSE in function of  $\alpha$  and  $\theta$  for the double homodyne setup.  $X_0 = 1$  was used  
 (b) BER in function of  $\alpha$  and  $\theta$  for the double homodyne setup.  $X_0 = 1$  was used

Figure 5.13: Theoretical results for double homodyne setup.

sampling time ( $6.4078 \times 10^{-13}$  W for a sampling time of 200 ns). The two signals are mixed, with a Balanced Beam Splitter in the single homodyne case and with a  $90^\circ$  Optical Hybrid in the double homodyne one, and are subsequently evaluated with recourse to Homodyne Receivers.

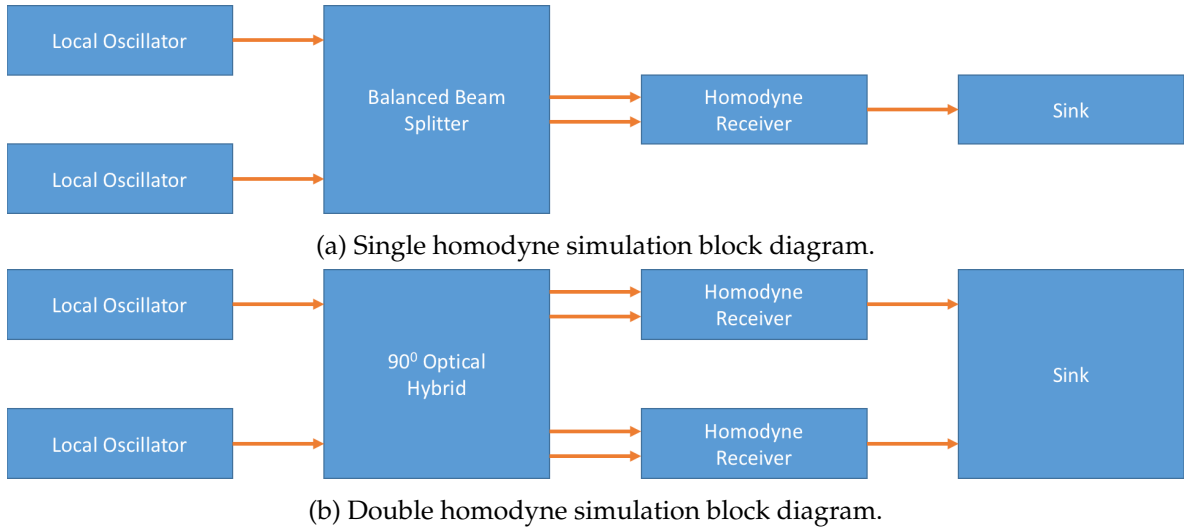


Figure 5.14: Block diagrams of both simulation results presented in this report.

System Blocks	netxpto Blocks
Local Oscillator	LocalOscillator
Homodyne Receiver	I_HomodyneReceiver
Balanced Beam Splitter	BalancedBeamSplitter
$90^\circ$ Optical Hybrid	OpticalHybrid

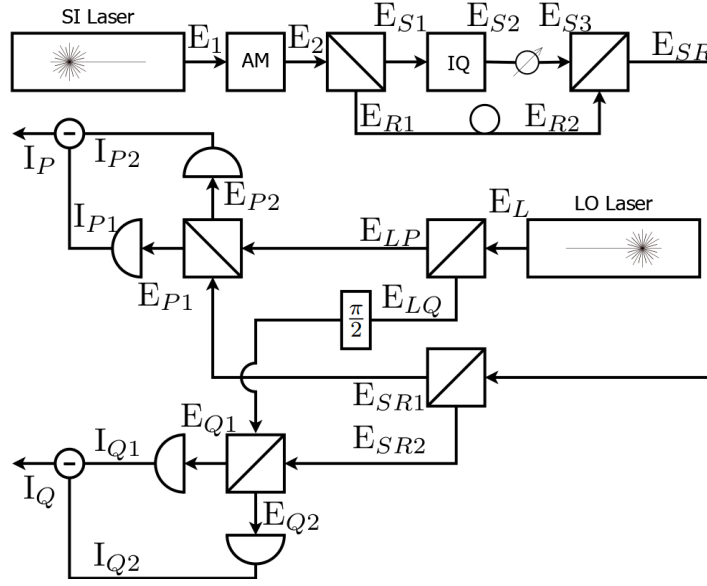


Figura 5.15: Simplified diagram of experimental setup.

### Theoretical study of the setup

A detailed diagram of the system studied is presented in Figure 5.15, with the respective mathematical treatment presented in equations (5.33) through (5.52).

$$E_1 = |E_S|e^{i(\omega_S t + \xi_S(t))} \quad (5.33)$$

$$p(t) = \begin{cases} 1, & \frac{T}{8} \leq t < \frac{T}{8} \\ 0, & \text{other} \end{cases} \quad (5.34)$$

$$E_2 = p(t)|E_S|e^{i(\omega_S t + \xi_S(t))} \quad (5.35)$$

$$E_{S1} = \frac{p(t)}{\sqrt{2}}|E_S|e^{i(\omega_S t + \xi_S(t))} \quad (5.36)$$

$$E_{S2} = \frac{p(t)}{\sqrt{2}}|E_S|e^{i(\omega_S t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t))} \quad (5.37)$$

$$E_{S3} = \frac{p(t)}{\sqrt{2}\text{Att}}|E_S|e^{i(\omega_S t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t))} \quad (5.38)$$

$$E_{R1} = \frac{p(t)}{\sqrt{2}}|E_S|e^{i(\omega_S t + \xi_S(t))} \quad (5.39)$$

$$E_{R2} = \frac{p(t - \frac{T}{2})}{\sqrt{2}}|E_S|e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \quad (5.40)$$

$$E_{SR} = \frac{|E_S|}{\sqrt{2}} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \quad (5.41)$$

$$E_{SR1} = \frac{|E_S|}{2} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \quad (5.42)$$

$$E_{SR2} = \frac{|E_S|}{2} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \quad (5.43)$$

$$E_L(t) = |E_L| e^{i(\omega_L t + \xi_L(t))} \quad (5.44)$$

$$E_{LP}(t) = \frac{1}{\sqrt{2}} |E_L| e^{i(\omega_L t + \xi_L(t))} \quad (5.45)$$

$$E_{LQ}(t) = \frac{1}{\sqrt{2}} |E_L| e^{i(\omega_L t + \xi_L(t) + \frac{\pi}{2})} \quad (5.46)$$

$$E_{P1}(t) = \frac{1}{\sqrt{2}} \left\{ \frac{|E_L|}{\sqrt{2}} e^{i(\omega_L t + \xi_L(t))} + \frac{|E_S|}{2} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ} t + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \right\} \quad (5.47)$$

$$E_{P2}(t) = \frac{1}{\sqrt{2}} \left\{ \frac{|E_L|}{\sqrt{2}} e^{i(\omega_L t + \xi_L(t))} - \frac{|E_S|}{2} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ} t + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \right\} \quad (5.48)$$

$$E_{Q1}(t) = \frac{1}{\sqrt{2}} \left\{ \frac{|E_L|}{\sqrt{2}} e^{i(\omega_L t + \xi_L(t) + \frac{\pi}{2})} + \frac{|E_S|}{2} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ} t + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \right\} \quad (5.49)$$

$$E_{Q2}(t) = \frac{1}{\sqrt{2}} \left\{ \frac{|E_L|}{\sqrt{2}} e^{i(\omega_L t + \xi_L(t) + \frac{\pi}{2})} - \frac{|E_S|}{2} \left[ \frac{p(t)}{\text{Att}} e^{i(\omega_S t + \phi_{IQ} t + \xi_S(t) + \xi_{IQ}(t))} + p\left(t - \frac{T}{2}\right) e^{i(\omega_S(t - \frac{T}{2}) + \xi_S(t - \frac{T}{2}))} \right] \right\} \quad (5.50)$$

$$I_P(t) = \frac{|E_S||E_L|}{\sqrt{2}} \left\{ \frac{p(t)}{\text{Att}} \cos((\omega_S - \omega_L)t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t) - \xi_L(t)) + p\left(t - \frac{T}{2}\right) \cos\left((\omega_S - \omega_L)t + \omega_S \frac{T}{2} + \xi_S\left(t - \frac{T}{2}\right) - \xi_L(t)\right) \right\} \quad (5.51)$$

$$I_Q(t) = \frac{|E_S||E_L|}{\sqrt{2}} \left\{ \frac{p(t)}{\text{Att}} \sin((\omega_S - \omega_L)t + \phi_{IQ}(t) + \xi_S(t) + \xi_{IQ}(t) - \xi_L(t)) + p\left(t - \frac{T}{2}\right) \sin\left((\omega_S - \omega_L)t + \omega_S \frac{T}{2} + \xi_S\left(t - \frac{T}{2}\right) - \xi_L(t)\right) \right\} \quad (5.52)$$

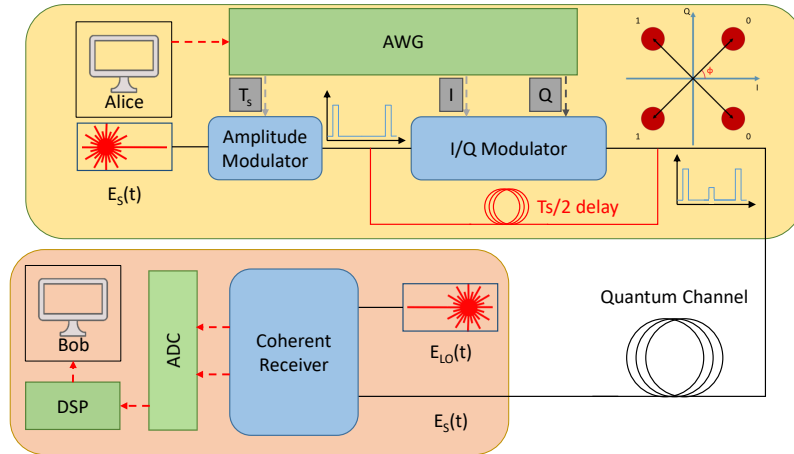


Figura 5.16: Diagram of full experimental setup.

### Experimental description

The main experimental setup utilized for the study presented in this document is presented in Figure 5.16. The setup contained two Yenista OSICS Band C/AG TLS lasers, tuned to a 1550 nm wavelength. A JDSU dual drive Mach-Zehnder Modulator with a Picosecond 5865 RF driver, employed at the output of one of the lasers, set the repetition rate at 1 GHz with a pulse time of 125 ps. The driving signal was generated by an Agilent Technologies BER Tester. A 50/50 beam-splitter was employed at the output of the Mach-Zehnder Modulator, one arm output is sent through an IQ Modulator while the other is sent through a fibre loop with length chosen such that the two arms have a relative delay of  $\sim 500$  ps. The employed IQ Modulator was a u2t photonics 32 GHz IQ Modulator with a SHF 807 RF driver, the driving signal being generated by a Tektronix AWG70002A Arbitrary Waveform Generator (AWG). A Variable Optical Attenuator (VOA) was set at the output of the IQ modulator to allow a fine tuning of the optical power to the desired level. The two arms output created by the first beam-splitter are combined by a 50/50 beam combiner. A fibre channel of  $\sim 10$  km was set between Alice's and Bob's setup. A Picometrix CR-100D 100G Integrated Balanced Receiver for Coherent Applications was employed to perform double homodyne measurements, recovering both the in-phase and in-quadrature components of the incoming light field. The response of the receiver was recorded by a Tektronix DPO77002SX-R3 oscilloscope, with an acquisition frequency of 100 GHz for a period of 400  $\mu$ s.

### Experimental results

#### Required files

Header Files



File	Description
netxpto.h	Generic purpose simulator definitions.
local_oscillator.h	Generates continuous coherent signal.
balanced_beam_splitter.h	Mixes the two input signals into two outputs.
optical_hybrid.h	Mixes the two input signals into four outputs.
homodyne_reciever.h	Performs coherent detection on the input signal.
sink.h	Closes any unused signals.

#### Source Files

File	Description
netxpto.cpp	Generic purpose simulator definitions.
local_oscillator.cpp	Generates continuous coherent signal.
balanced_beam_splitter.cpp	Mixes the two input signals into two outputs.
optical_hybrid.cpp	Mixes the two input signals into four outputs.
homodyne_reciever.cpp	Performs coherent detection on the input signal.
sink.cpp	Closes any unused signals.

### System Input Parameters

This system takes into account the following input parameters:

System Parameters	Description
numberOfBitsGenerated	Gives the number of bits to be simulated
bitPeriod	Sets the time between adjacent bits
samplesPerSymbol	Establishes the number of samples each bit in the string is given
localOscillatorPower_dBm	Sets the optical power, in units of dBm, at the reference output
localOscillatorPower2	Sets the optical power, in units of W, of the signal
localOscillatorPhase1	Sets the initial phase of the local oscillator used for reference
localOscillatorPhase2	Sets the initial phase of the local oscillator used for signal
transferMatrix	Sets the transfer matrix of the beam splitter used in the homodyne detector
responsivity	Sets the responsivity of the photodiodes used in the homodyne detector
amplification	Sets the amplification of the trans-impedance amplifier used in the homodyne detector
electricalNoiseAmplitude	Sets the amplitude of the gaussian thermal noise added in the homodyne detector
shotNoise	Chooses if quantum shot noise is used in the simulation

### Inputs

This system takes no inputs.

## Outputs

The single homodyne system outputs the following objects:

**Parameter:** Signals:

**Description:** Local Oscillator Optical Reference; ( $S_1$ )

**Description:** Local Oscillator Optical Signal; ( $S_2$ )

**Description:** Beam Splitter Outputs; ( $S_3, S_4$ )

**Description:** Homodyne Detector Electrical Output; ( $S_5$ )

The double homodyne system outputs the following objects:

**Parameter:** Signals:

**Description:** Local Oscillator Optical Reference; ( $S_1$ )

**Description:** Local Oscillator Optical Signal; ( $S_2$ )

**Description:** 90° Optical Hybrid Outputs; ( $S_3, S_4, S_5, S_6$ )

**Description:** Homodyne Detector Electrical Output; ( $S_7$ )

## Simulation Results

### Single homodyne results

The numerical results presented in Figure 5.17 were obtained with the simulation described by the block diagram in Figure 5.14a. Theoretical results are a direct trace of (5.27). One can see that the numerical results adhere quite well to the expected curve.

### Double homodyne results

The numerical results presented in Figure 5.18 were obtained with the simulation described by the block diagram in Figure 5.14b. Theoretical results are a direct trace of (5.32) with  $\theta = \frac{\pi}{4}$ . One can see that the numerical results adhere quite well to the expected curve.

## Known Problems

1. Homodyne Super-Block not functioning

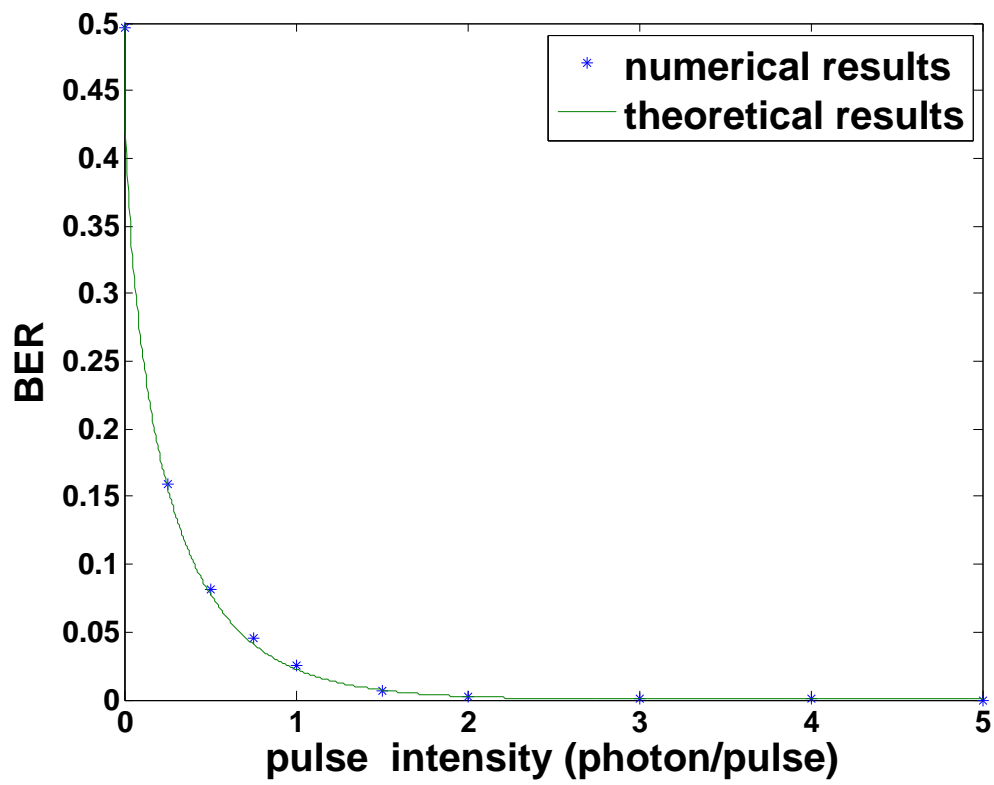


Figura 5.17: BER in function of  $\alpha$  for the single homodyne setup.  $X_0 = 0$  was used

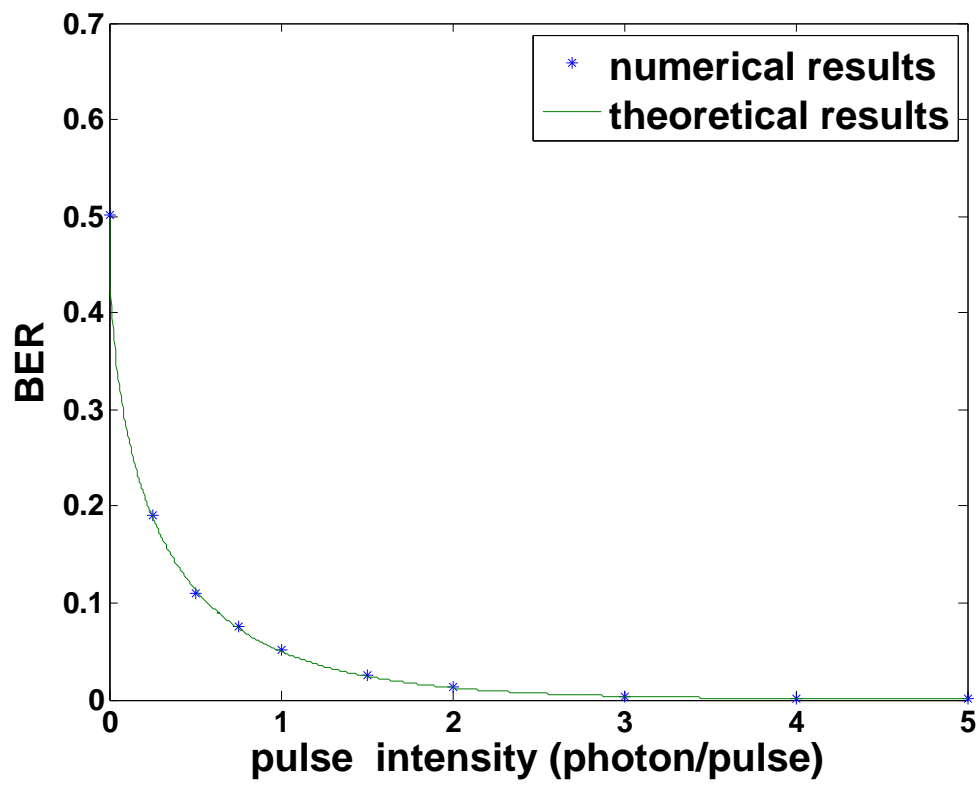


Figura 5.18: BER in function of  $\alpha$  for the double homodyne setup.  $X_0 = 0$  was used

---

## Bibliografia

- [1] Ryo Namiki and Takuya Hirano. Security of quantum cryptography using balanced homodyne detection. *Physical Review A*, 67(2):022308, 2003.

## 5.5 Simplified Coherent Receiver

<b>Student Name</b>	: Romil Patel
<b>Starting Date</b>	: August 16, 2017
<b>Goal</b>	: Develop a simplified structure (low cost) for a coherent receiver, that can be used in coherent PON, inter-data center connections, or metropolitan networks (optical path lengths <del>should be</del> < 100 km).

~~In recent days, homodyne detection has been discussed and investigated a lot due to the advancement in the DSP in the electrical domain. However,~~ a major drawback of homodyne detection is the incoming signal should be separated into inphase and quadrature (I/Q) signals in the optical domain. Therefore, it demands more hardware to accommodate the requirement of the signal separation in the optical domain. For instance, 4 balanced photodetectors with double hybrid structures and 4-channel ADCs are required. On the other hand, heterodyne receiver simplifies the detection scheme to some extent with the requirement of having only half of photodetectors and ADC.

Such coherent detection scheme constitute the solution for the medium-to-long-reach application; however, the cost of coherent receiver becomes a major obstacle in the case of short-reach links applications like PON, inter-data-center communications, metropolitan network etc. In order to get rid of higher cost and to make the transceiver more efficiently applicable in short-reach links, a new architecture of optical receiver has been proposed which combines the advantages of coherent transmission and cost effectiveness of direct detection. The working principle of the receiver is based on the famous Kramers-Kronig(KK) relationship which facilitates digital post-compensation of linear propagation impairments. The proposed Kramers-Kronig(KK) receiver structure is highly efficient in terms of spectral occupancy and energy consumptions.

### 5.5.1 Minimum Phase Signal

The communication scheme discussed here relies on the identifying a specific condition that ensures the received signal is minimum phase. This condition facilitates the unique way to extract the phase of the received signal from its intensity. If we denote  $s(t)$  as a complex data-carrying signals whose spectrum is contained between  $-B/2$  to  $B/2$ , and consider a single sideband signal of the form,

$$h(t) = A + s(t)\exp(i\pi Bt) \quad (5.53)$$

Where  $A$  is a constant. Here, Nyquist stability criterion can be used to ensure that  $s(t)$  is a minimum phase signal. The condition of minimum phase signal is satisfied when  $|A| > |s(t)|$  by guaranteeing Nyquist stability of the received signal. When  $h(t)$  is a minimum-phase

signal, its phase  $\phi(t)$  and absolute value  $|h(t)|$  are uniquely related by Hilbert transform:

$$\phi(t) = \frac{1}{\pi} \text{p.v.} \int_{-\infty}^{\infty} dt' \frac{\log[|h(t')|]}{t - t'} \quad (5.54)$$

where *p.v.* stands for *principal value*. The relationship depicted in Equation 5.54 can also be conveniently implemented in frequency domain as,

$$\tilde{\phi}(\omega) = i \text{sign}(\omega) \mathcal{F}\{\log[|h(t)|]\} \quad (5.55)$$

where  $\text{sign}(\omega)$  is the sign function which is equal to 1 when  $\omega > 0$ , to 0 when  $\omega = 0$  and to -1 when  $\omega < 0$ . Symbol  $\mathcal{F}$  denotes the Fourier transform.

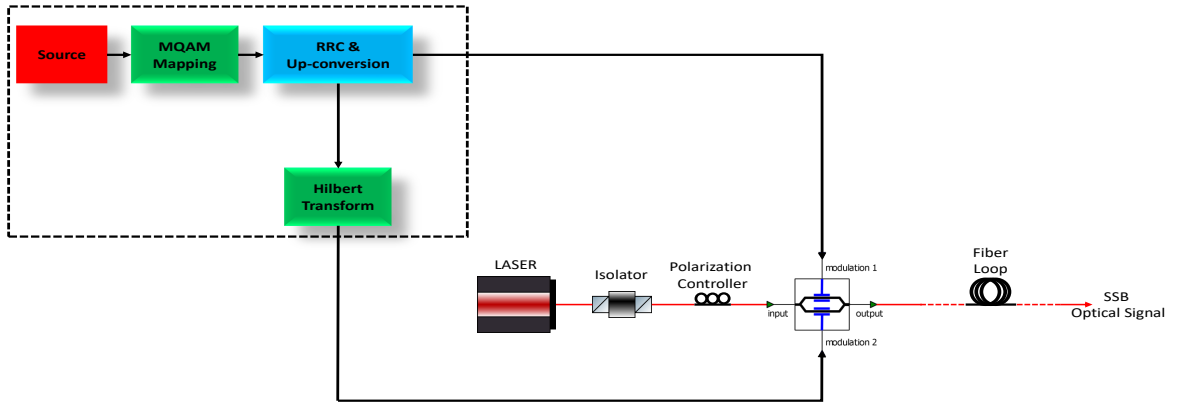


Figura 5.19: Transmitter

### 5.5.2 KK Scheme

If we consider the complex envelope of the incoming electric field by  $E_s(t)$  confined within the optical bandwidth denoted by  $B$ . The LO assumed to be a continuous wave (CW) signal whose amplitude is  $E_0$  whose frequency coincides with the left edge of the information-carrying signal spectrum. Here, we assumed that  $E_0$  is real-valued and positive, which is equivalent to referring all phase value to that of LO.

The complex envelope of the field striking upon the photo-diode can be given as,

$$E(t) = E_s(t) + E_0 \exp(i\pi Bt) \quad (5.56)$$

The photo current  $I$  produced by the photo-diode is proportional to the field intensity  $I = |E(t)|^2$ , here proportionality constant considered as 1 for the sake of simplicity. If  $E_0$  is large enough to ensure that the signal  $E(t) \exp(i\pi Bt) = E_0 + E_s(t) \exp(-i\pi Bt)$  is minimum phase. Equations 5.54 and 5.55 can be used to reconstruct the signal  $E_s(t)$  as follows:

$$E_s(t) = \{\sqrt{I(t)} \exp[i\phi_E(t)] - E_0\} \exp(i\pi Bt) \quad (5.57)$$

$$\phi_E(t) = \frac{1}{2\pi} p.v. \int_{-\infty}^{\infty} dt' \frac{\log[|I(t')|]}{t - t'} \quad (5.58)$$

Here, the average value of the phase returned by Equation 5.58 is zero, which implies the need for an additional phase-recovery procedure.

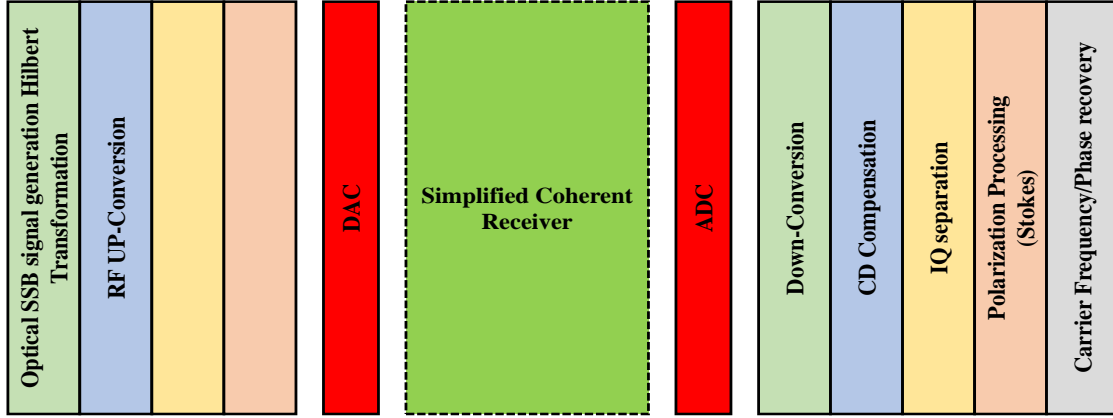


Figura 5.20: Tx/Rx DSP main subsystem

### 5.5.3 Tx side

Single polarization 16QAM signals (1.25 Gbaud) to be generated at the Tx through an IQ modulator (Figure 5.20). The IQ modulated signal is then applied to the Hilbert transformer which generates the imaginary part for our analytical signal. In analytical signal, real and imaginary parts are related to each other by Hilbert transform and it has no negative frequency contents. Such analytical signal can be used for generating bandwidth efficient single sideband (SSB) signal.

#### Analytical Signal

In mathematics and signal processing, an analytic signal is a complex-valued function that has no negative frequency components. The real and imaginary parts of an analytic signal are real-valued functions related to each other by the Hilbert transform.

$$s_a(t) = s(t) + j\hat{s}(t) \quad (5.59)$$

where,  $s_a(t)$  is an analytical signal and  $\hat{s}(t)$  is the Hilbert transform of the signal  $s(t)$ . Such analytical signal can be used to generate SSB signal. In this section, we'll discuss the brief



idea of generating SSB signal using Hilbert transform method. To understand this, we may express signal  $s(t)$  as a summation of the two complex-valued functions.

$$s(t) = \frac{1}{2}[s(t) + j\hat{s}(t)] + \frac{1}{2}[s(t) - j\hat{s}(t)] \quad (5.60)$$

where, the term  $\frac{1}{2}[s(t) + j\hat{s}(t)]$  is the analytical representation of the signal  $s(t)$  (from Equation 5.59). Another term represents the complex conjugate  $\frac{1}{2}[s(t) - j\hat{s}(t)]$  of this analytical signal. Such representation of the signal  $s_a(t)$  and  $s_a^*(t)$  divide the signal into non-negative frequency component and non-positive frequency component respectively. Alternatively, we can write it as,

$$\frac{1}{2}S_a(f) = \begin{cases} S(f) & \text{for } f > 0 \\ 0 & \text{for } f < 0 \end{cases} \quad (5.61)$$

where  $S_a(f)$  and  $S(f)$  are the Fourier transform of  $s_a(t)$  and  $s(t)$  respectively. The frequency translated version of  $S_a(f - f_0)$  contains only one side (positive) of  $S(f)$  and hence it is called single sideband signal  $s_{ssb}(t)$ ,

$$F^{-1}\{S_a(f - f_0)\} = s_a(t)e^{j2\pi f_0 t} = s_{ssb}(t) + j\hat{s}_{ssb}(t) \quad (5.62)$$

Therefore, from the Euler's formula,

$$\begin{aligned} s_{ssb}(t) &= \text{Re}\{s_a(t)e^{j2\pi f_0 t}\} \\ &= \text{Re}\{[s(t) + j\hat{s}(t)][\cos(2\pi f_0 t) + j\sin(2\pi f_0 t)]\} \\ &= s(t)\cos(2\pi f_0 t) - \hat{s}(t)\sin(2\pi f_0 t) \end{aligned} \quad (5.63)$$

This Equation 5.63 displays the mathematical modeling of the upper sideband SSB signal. Similarly, we can generate lower sideband SSB signal by,

$$s_{ssb}(t) = s(t)\cos(2\pi f_0 t) + \hat{s}(t)\sin(2\pi f_0 t) \quad (5.64)$$

### SSB Signal generation using Hilbert transformation

This section describes the SSB signal generation using Hilbert transformation method (Phase Shift Method). Consider a message signal  $m(t)$  with its frequency domain spectrum  $M(F)$  as shown in Figure 5.21. From the Figure 5.21, we can see that both the side are scaled by factor '1' which means it represents the original signal.

Now let's consider the modulated signal  $x(t)$  given as,

$$x(t) = m(t)\cos(2\pi f_c t) \quad (5.65)$$

Frequency domain representation of the equation 5.65 can be given as,

$$X(F) = \frac{1}{2}M(f - f_c) + \frac{1}{2}M(f + f_c) \quad (5.66)$$

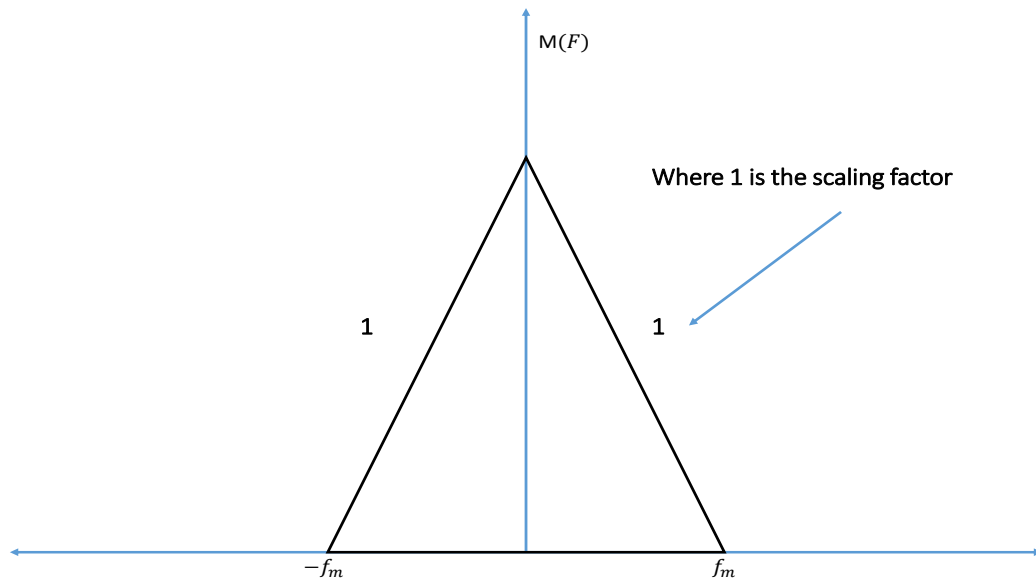


Figura 5.21: Original baseband signal

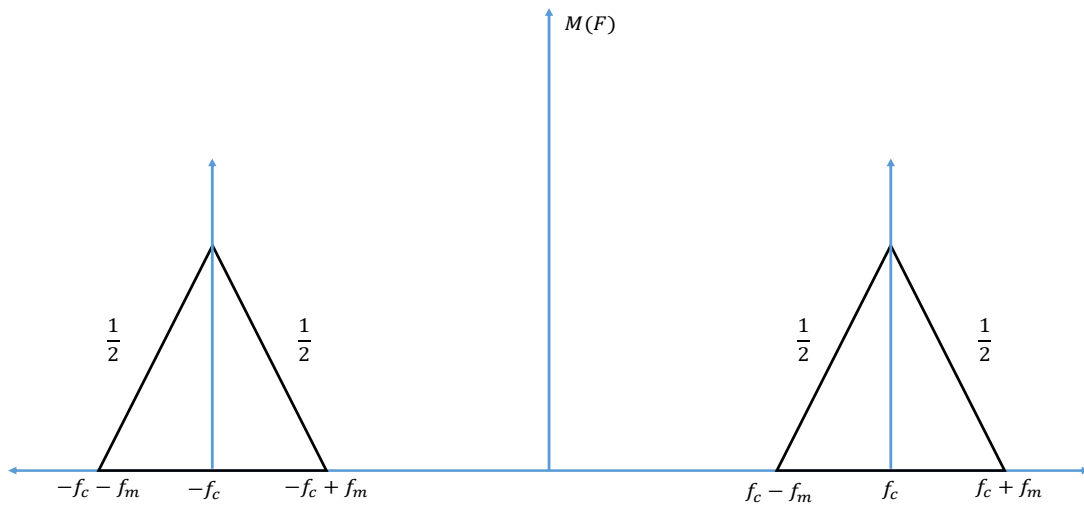


Figura 5.22: Original modulated signal

Here in equation 5.66, we can observe that each side band are scaled by  $\frac{1}{2}$  on the frequency spectrum. Figure displays the frequency domain representation of the modulated signal  $X(F)$ .

Next, we will discuss something more interesting which is called as Hilbert transform of the original message signal  $m(t)$ . As we discussed earlier, in the frequency domain, the Hilbert transformed signal  $\hat{M}(f)$  can be achieved by multiplying the Fourier transformed signal

$M(F)$  with  $[-j \operatorname{sgn}(F)]$ . Suppose we modulate the Hilbert transformed message signal  $\hat{m}(t)$

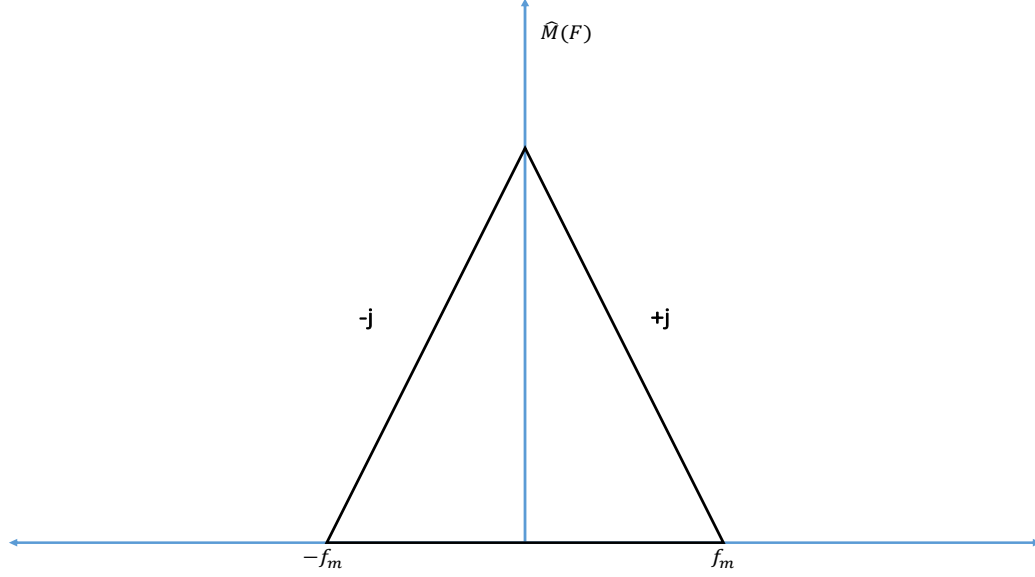


Figura 5.23: Hilbert transformed modulated signal

with the  $\sin(2\pi f_c t)$  (quadrature phase carrier), then we get the following results:

$$\begin{aligned}
 \hat{m}(t)\sin(2\pi f_c t) &= \hat{m}(t) \frac{e^{j2\pi f_c t} - e^{-j2\pi f_c t}}{2} \\
 &= \hat{m}(t) \frac{e^{j2\pi f_c t}}{2} - \hat{m}(t) \frac{e^{-j2\pi f_c t}}{2} \\
 &= \frac{\hat{M}(f - f_c)}{2j} - \frac{\hat{M}(f + f_c)}{2j} \\
 &= \frac{-j}{2} \hat{M}(f - f_c) + \frac{-j}{2} \hat{M}(f + f_c)
 \end{aligned} \tag{5.67}$$

The detailed explanation of the equation 5.70 has been described in the Figure 5.24 and 5.25. Figure 5.24 displays the spectrum of the  $\hat{M}(f + f_c)$  and  $\hat{M}(f - f_c)$  for the positive and negative frequencies respectively. The final equation resolution of equation displays that both positive and negative side of the spectrum multiplied with  $\frac{j}{2}$  and  $\frac{-j}{2}$  respectively. Finally the spectrum of the signal  $\hat{m}(t)\sin(2\pi f_c t)$  can be given as Figure 5.25.

Further, summation of the two signals  $m(t)\cos(2\pi f_c t)$  and  $\hat{m}(t)\sin(2\pi f_c t)$  will generate the upper sideband SSB signal as follows,

$$u(t) = m(t)\cos(2\pi f_c t) - \hat{m}(t)\sin(2\pi f_c t) \tag{5.68}$$

From the above discussion, the spectrum of the Equation 5.68 can be given by the Figure 5.26. Similarly, for the lower sideband SSB can be generated by Equation,

$$u(t) = m(t)\cos(2\pi f_c t) + \hat{m}(t)\sin(2\pi f_c t) \tag{5.69}$$

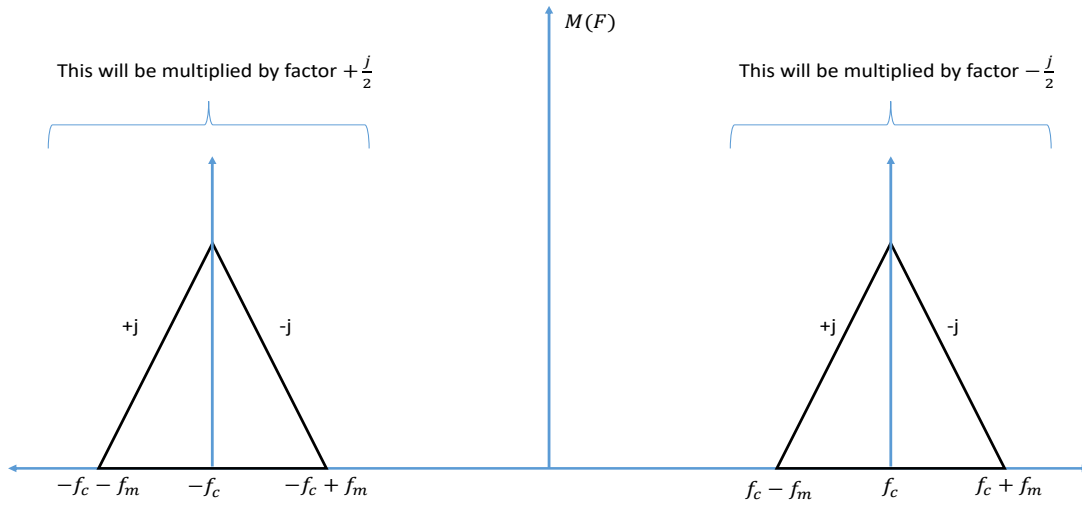


Figura 5.24: Hilbert transformed modulated signal

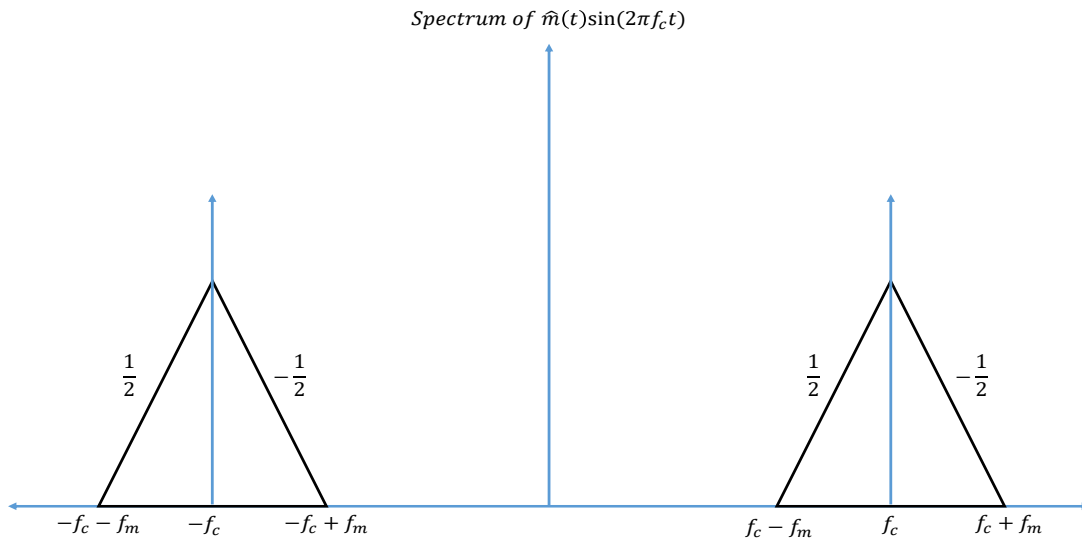


Figura 5.25: Hilbert transformed modulated signal

### Kramers Kronig Relation

Suppose we have a SSB signal  $u(t)$  described as,

$$u(t) = u_r(t) + iu_i(t) \quad (5.70)$$

In the equation 5.70, the real and imaginary parts  $U_r(t)$  and  $U_i(t)$  are related through the Kramers-Kronig relation with each other. An intuitive way to analyze the relation is based

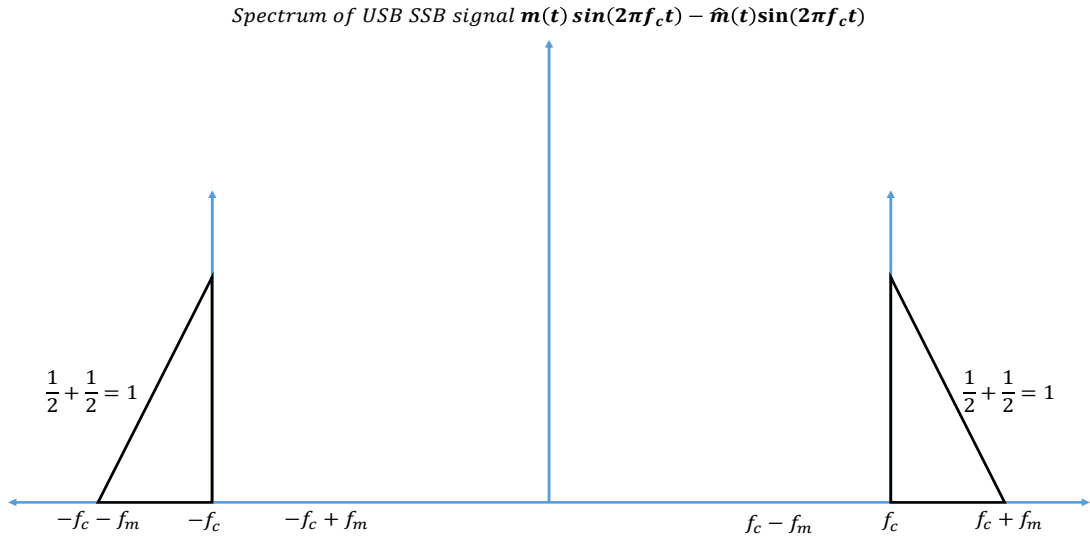


Figura 5.26: SSB signal spectrum

on expressing its Fourier transform  $\tilde{U}(\omega)$  as follows,

$$\tilde{U}(\omega) = \frac{1}{2}[1 + \text{sgn}(\omega)]\tilde{U}(\omega) \quad (5.71)$$

The equation 5.73 follows the SSB signal condition  $\tilde{U}(\omega) = 0$  for  $\omega < 0$ . Further, simplification of the signal can be summarized as follows:

$$\begin{aligned} \tilde{U}(\omega) &= \frac{1}{2}[1 + \text{sgn}(\omega)]\tilde{U}(\omega) \\ &= \frac{1}{2}\tilde{U}(\omega) + \frac{1}{2}\text{sgn}(\omega)\tilde{U}(\omega) \end{aligned} \quad (5.72)$$

Taking inverse Fourier transform of the equation 5.73,

$$\begin{aligned} u(t) &= IFT\{\tilde{U}(\omega)\} \\ &= \frac{1}{2}u(t) + \frac{1}{2}[IFT\{\text{sgn}(\omega)\} \otimes u(t)] \end{aligned} \quad (5.73)$$

The underlined term in Equation 5.73 displays that multiplication in frequency domain converted into the convolution in the time domain. Further, IFT of the function  $\text{sgn}(\omega)$  given as  $(-i/\pi t)$ . As a consequences, we can further simplify our equation as,

$$\begin{aligned} u(t) &= \frac{1}{2}U(t) + \frac{1}{2}\left[\frac{i}{\pi t} \otimes u(t)\right] \\ \frac{u(t)}{2} &= \frac{1}{2}\left[\frac{i}{\pi t} \otimes u(t)\right] \\ u(t) &= i\left[\frac{1}{\pi t} \otimes u(t)\right] \\ u(t) &= \frac{i}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u(t')}{t - t'} dt' \end{aligned} \quad (5.74)$$

Using Equation 5.73 into Equation 5.77,

$$u_r(t) + iu_i(t) = \frac{i}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u(t')}{t - t'} dt' \quad (5.75)$$

Therefore,

$$\begin{aligned} u_r(t) + iu_i(t) &= \frac{i}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u_r(t') + iu_i(t')}{t - t'} dt' \\ u_r(t) + iu_i(t) &= -\frac{1}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u_i(t')}{t - t'} dt' + \frac{i}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u_r(t')}{t - t'} dt' \end{aligned} \quad (5.76)$$

which leads to,

$$\begin{aligned} u_r(t) &= -\frac{1}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u_i(t')}{t - t'} dt' \\ u_i(t) &= \frac{1}{\pi} p.v. \int_{-\infty}^{\infty} \frac{u_r(t')}{t - t'} dt' \end{aligned} \quad (5.77)$$

#### 5.5.4 Rx side

At the receiver side, signal is coherently detected using a simplified coherent receiver and a local oscillator. The optical signal is then converted into the electrical domain using two balanced photodetector (BPD), or alternatively four photodetector, and amplified by a transimpedance amplifier (TIA). Following that, the signals are sampled by two 8-bit 2.5 GSa/s ADC and the this digitized signal sent to the FPGA (Virtex-7) where all post-detection DSP implemented in real-time.

---

## Bibliografia

- [1] Antonio Mecozzi, Cristian Antonelli, and Mark Shtaif. *Kramers-Kronig Coherent Receiver*. Optica, vol.3, no.11, 2016, p.1220., doi:10.1364/optica.3.001220.
- [2] Antonio Mecozzi. *Retrieving the full optical response from amplitude data by Hilbert transform*. Opt. Comm. 282, 4183-4187.
- [3] Antonio Mecozzi. *A necessary and sufficient condition for minimum phase and implication of phase retrieval*. arXiv:1606.04861.

## 5.6 Oblivious Transfer with Discrete Variables

<b>Student Name</b>	: Mariana Ramos
<b>Starting Date</b>	: September 18, 2017
<b>Goal</b>	: Oblivious transfer implementation with discrete variables.

Oblivious Transfer (OT) is a fundamental primitive in multi-party computation. The one-out-of-two OT consists in a communication protocol between Alice and Bob. At the beginning of the protocol Alice has two messages  $m_1$  and  $m_2$  and Bob wants to know one of them,  $m_b$ , without Alice knowing which one, i.e. without Alice knowing  $b$ , and Alice wants to keep the other message private, i.e. without Bob knowing  $m_{\bar{b}}$ . therefore two conditions must be fulfilled:

1. The protocol must be concealing, i.e at the beginning of the protocol Bob does not know nothing about the messages sent by Alice, while at the end of the protocol Bob will learn the message  $b$  chose by him.
2. The protocol is oblivious, i.e Alice cannot learn anything about bit  $b$  and Bob cannot learning nothing about the other message  $m_{\bar{b}}$ .

### 5.6.1 OT Protocol Detailed

First of all, it is important to set the initial conditions of Bob and Alice's knowledge.

In general, the first step is to establish for both Alice and Bob the message length  $s$  and the parameter  $k$ , which is multiplicative factor of message's length. In this case, lets assume message's length  $s = 4$  and a multiplicative factor  $k = 2$ .

In addition, both Alice and Bob know the following correspondence, where  $+$  corresponds to *Rectilinear Basis* and  $\times$  corresponds to *Diagonal Basis*:

<i>Basis</i>	
0	+
1	$\times$

Secondly both Alice and Bob also know the bit correspondence for each direction for each basis. For *Rectilinear basis*, "+":

	Basis "+"
0	$\rightarrow$
1	$\uparrow$

and for *Diagonal Basis*, " $\times$ ":

	Basis " $\times$ "
0	$\searrow$
1	$\nearrow$



Third, only Alice knows information about messages  $m_1$  and  $m_2$ . In this case, let's assume she sets the two messages  $m_1 = \{0011\}$  and  $m_2 = \{0001\}$ .

1. Alice randomly generate a bit sequence with length  $k.s$  being, in this case,  $k = 2$  and  $s = 4$  and both were defined at the beginning of the protocol. Therefore, she must define two sets  $S_{A1}$ , which contains the basis values, and  $S_{A2}$ , which contains the key values.

In that case, let's assume she gets the following sets  $S_{A1}$  and  $S_{A2}$ :

$$S_{A1} = \{0, 1, 1, 0, 0, 1, 0, 1\}$$

$$S_{A2} = \{1, 1, 0, 0, 0, 1, 0, 0\}$$

2. Next, Alice sends to Bob throughout a quantum channel  $ks$  photons encrypted using the basis defined in  $S_{A1}$  and according to the keys defined in  $S_{A2}$ .

In the current example, Alice sends the photons, throughout a quantum channel, according to the following basis and keys:

$$S_{AB} = \{\uparrow, \nearrow, \searrow, \rightarrow, \rightarrow, \nearrow, \rightarrow, \searrow\}$$

3. Bob also randomly generates  $ks$  bits according to the basis through which he will measure the photons sent by Alice and he fills an array  $S_{B1}$  with the basis chosen by him. In this example, let's assume:

$$S_{B1} = \{0, 1, 0, 1, 0, 1, 1, 1\}$$

4. When Bob receives photons from Alice, he measures them using the basis defined in  $S_{B1}$ . In the current example, we assumed that  $S_{B1}$  is the following set:

$$\{+, \times, +, \times, +, \times, \times, \times\}$$

In this follow-up he will get  $ks$  results. Some of them Bob is 100% sure he was succeeded and others he may be succeeded or not with a probability of  $\frac{1}{2}$ . The values which he is not sure about are underlined in the following sequence:

$$S_{B1'} = \{1, 1, 0, \underline{1}, 0, 1, \underline{1}, 0\}$$

5. Once Alice has received the confirmation of measurement from Bob, she sends throughout a classical channel the basis which she has used to codify the photons, which in this case we assumed  $S_{A1} = \{0, 1, 1, 0, 0, 1, 0, 1\}$ .
6. In order to know which photons were measured correctly, Bob does the operation  $S_{B2} = S_{B1} \oplus S_{A1}$ . In the current example the operation will be:

$S_{B1}$	0	1	0	1	0	1	1	1
$S_{A1}$	0	1	1	0	0	1	0	1
$\oplus$	1	1	0	0	1	1	0	1

In this way, Bob gets

$$S_{B2} = \{1, 1, 0, 0, 1, 1, 0, 1\}$$

. The values "1" correspond to the values he measured correctly and "0" to the values he wrongly measured.

Next, Bob sends to Alice through a classical channel information about the minimum number between "ones" and "zeros", i.e

$$n = \min(\#0, \#1) = 3$$

where  $\#0$  represents the minimum number of zeros and  $\#1$  the minimum number of ones. Function  $\min(a, b)$  counts the number of  $a$ ,  $n_a$ , and the number of  $b$ ,  $n_b$  and if  $n_a < n_b$  the function will take  $n_a$  as result and  $n = n_a$ , otherwise  $n = n_b$ .

7. If  $n < s$ , being  $s$  the message's size, Alice and Bob will repeat the steps from 1 to 7.
8. Lets assume for the values set which contains the results of Bobs measurements  $S_{B1'}$ , we have the following sequence being underlined values those which Bob is not 100% sure about, having a probability of success about  $\frac{1}{2}$  :

$$S_{B1'} = \{1, 1, 0, \underline{0}, 0, 1, \underline{0}, 0, \underline{1}, 0, \underline{0}, \underline{0}, 0, 0, \underline{1}, 1\}$$

At Alice's side the new sets  $S_{A1}$ , which contains the basis values, and  $S_{A2}$ , which contains the key values, will be the following:

$$S_{A1} = \{0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0\}$$

$$S_{A2} = \{1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1\}$$

Finally, for  $S_{B2} = S_{B1} \oplus S_{A1}$  Bob gets the following sequence:

$$S_{B2} = \{1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1\}$$

9. At this time, Bob sends again to Alice through a classical channel the minimum number between "ones" and "zeros"  $n = \min(\#0, \#1)$ . In this case,  $n$  is equal to 7 which is the number of zeros.
10. Alice checks if  $n > s$  and reveals to Bob that she already knows that  $n > s$ . In this case,  $n = 7$  and  $s = 4$  being  $n > s$  a valid condition.

11. Next, Bob defines two new sets,  $I_1$  and  $I_0$  where one contains  $s$  positions of measurements that Bob has succeeded and other contains  $s$  positions of measurements that Bob was wrong about, respectively.

In this example, Bob defines two sequences with size  $s = 4$ :

$$I_0 = \{3, 4, 7, 11\}$$

and

$$I_1 = \{2, 5, 6, 13\}$$

where  $I_0$  is the sequence of positions in which Bob was wrong and  $I_1$  is the sequence of positions in which Bob was right.

Thus, if Bob wants to know  $m_1$  he must send to Alice throughout a classical channel the set  $\{I_1, I_0\}$ , otherwise if he wants to know  $m_2$  he must send to Alice throughout a classical channel the set  $\{I_0, I_1\}$ .

12. Lets assume Bob sent  $\{I_1, I_0\}$ . Alice defines two encryption keys  $K_1$  and  $K_2$  using the values in positions defined by Bob in the set sent by him. In this example, lets assume:

$$K_1 = \{1, 0, 1, 0\}$$

$$K_2 = \{0, 0, 0, 1\}$$

Alice does the following operations:

$$m = \{m_1 \oplus K_1, m_2 \oplus K_2\}$$

$m_1$	0	0	1	1
$K_1$	1	0	1	0
$\oplus$	1	0	0	1

$m_2$	0	0	0	1
$K_2$	0	0	0	1
$\oplus$	0	0	0	0

Adding the two results,  $m$  will be:

$$m = \{1, 0, 0, 1, 0, 0, 0, 0\}$$

.

After that, Alice sends to Bob the encrypted message  $m$  through a classical channel.

13. When Bob receives the message  $m$ , in the same way as Alice, Bob uses  $S_{B1}$  values of positions given by  $I_1$  and  $I_0$  and does the decrypted operation. In this case, he does following operation:

$$\begin{array}{c|ccccccc}
 m & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 \hline
 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
 \hline
 \oplus & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0
 \end{array}$$

The first four bits corresponds to message 1 and he received  $\{0, 0, 1, 1\}$ , which is the right message  $m_1$  and  $\{0, 1, 1, 0\}$  which is a wrong message for  $m_2$ .

### 5.6.2 OT Protocol - Potential Problems

There are two potential problems with the protocol described above:

1. In step 5 Bob may says to Alice that he has already measured the photon and it could be a lie.
2. In step 10 Bob may uses some values of  $I_1$  in  $I_0$  of positions which he knows are right in order to know correct information about message  $m_2$ .

This problems can hopefully be solved using *Bit Commitment* through *Hash Functions*.

### 5.6.3 Simulation

First of all, the protocol will be simulated and then a experimental setup will be built in the laboratory.

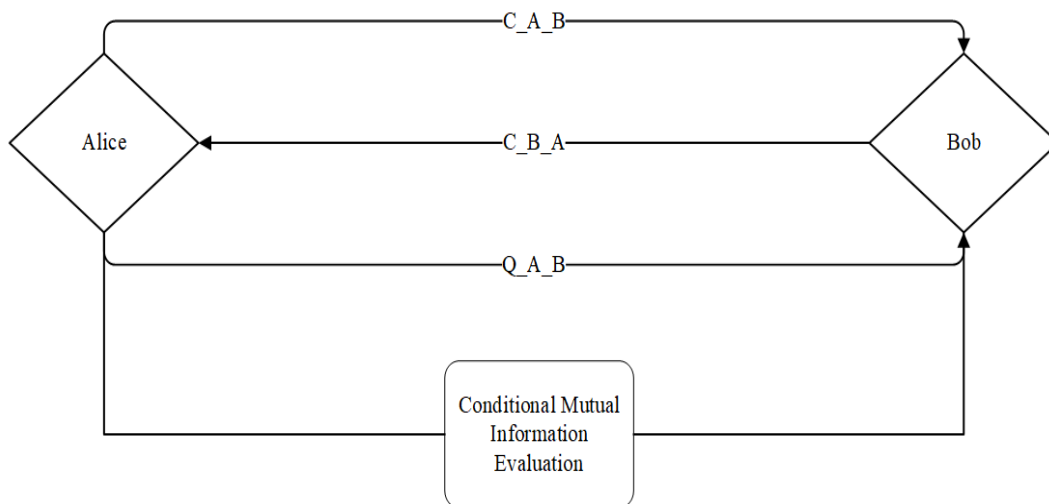


Figura 5.27: Simulation diagram at a top level

As one may see in figure 5.27 this simulation will have three top level blocks. Two of them are Alice and Bob and they are connected through two classical channels and one quantum channel. In addition, a third block will be performed for the calculation of *Mutual Information*. The mutual information (MI) between Alice and Bob is defined in terms of their join distribution.

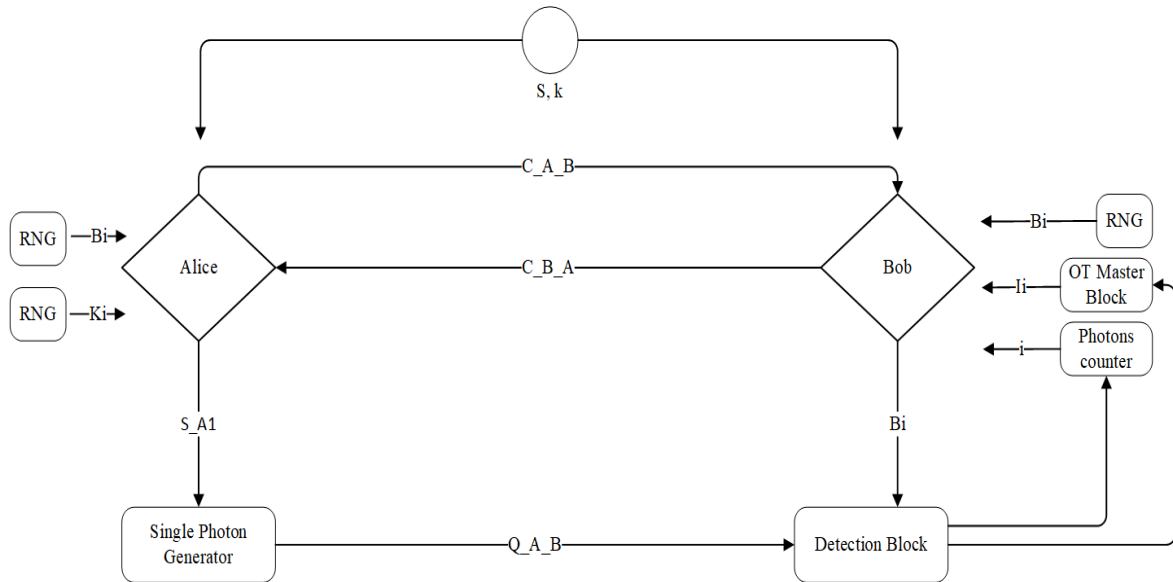


Figura 5.28: Simulation diagram - blocks

In figure 5.28 is presented the block diagram of the simulation that will be performed. There are two sides (Alice and Bob) and three channels throughout which they will communicate. At the beginning of the protocol Alice and Bob must know two values: message's size,  $s$ , and a multiplicative factor,  $k$ . Furthermore, Alice must have two blocks, *RNG - Random Number Generate*, for randomly picks the basis  $B_i$  and the keys  $K_i$ . In a similar way, Bob also has one *RNG - Random Number Generate* for randomly chooses in which basis he will measure the photons sent by Alice. In addition, Bob has one *OT Master Block* to analyse the data and picks two more sub-sets  $I_0$  and  $I_1$  and a *Photons counter* which has  $i$  as output in order to send to Alice the number of photons which Bob has received through the Quantum channel. Moreover, Alice must have a block for *Single Photon Generator* which receives information through " $S_{A1}$ " channel about the basis and keys to encrypt the photons and then send them to Bob using the Quantum channel.

In general, the simulation must have two Classical channels, one from Alice to Bob and other from Bob to Alice through which they change all the information about basis. Third channel is used only in one direction, from Alice to Bob, and Alice sends the photons to Bob through this channel.

### 5.6.4 Experimental

In figures 5.29 and 5.30 are presented the experimental setup to be performed in the lab. Starting with Alice's side and then Bob's side.

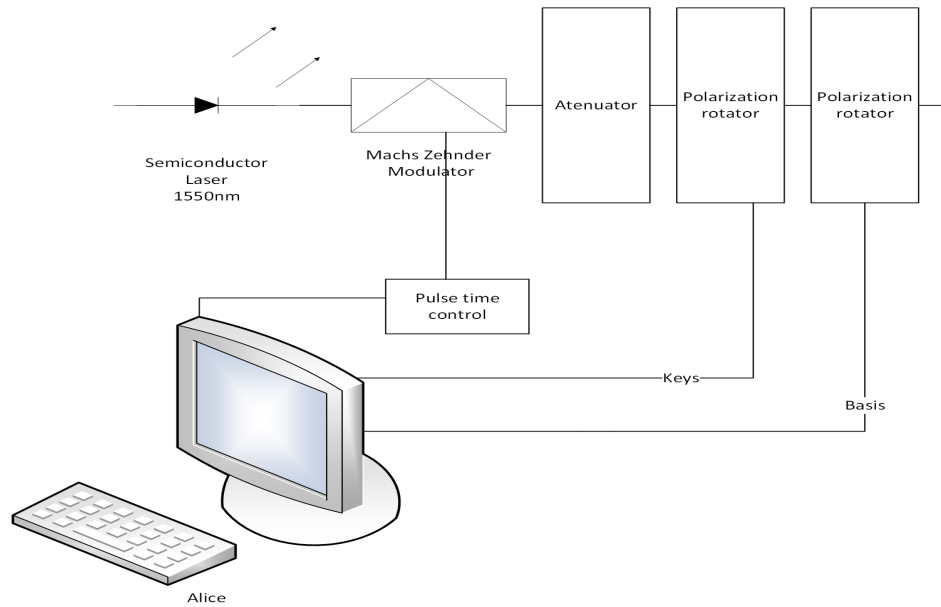


Figura 5.29: Quantum communication diagram - Alice's side

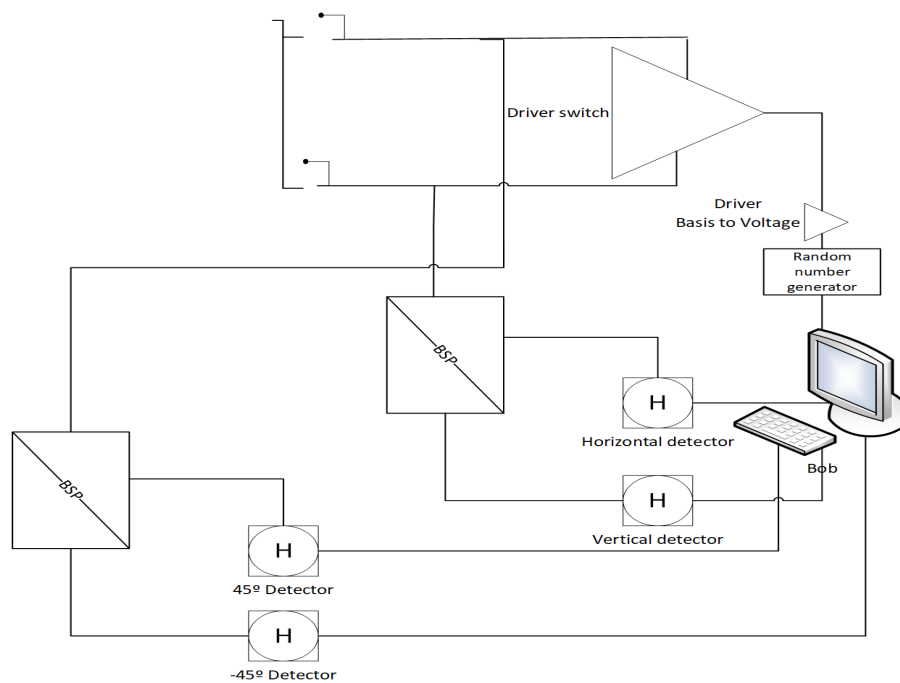


Figura 5.30: Quantum communication diagram - Bob's side

## 5.7 Radio Over Fiber Transmission System

<b>Student Name</b>	: Celestino Martins
<b>Starting Date</b>	: September 25, 2017
<b>Goal</b>	: Radio Over Fiber.

Radio over fiber (RoF) technology comprises the transmission over fiber technology, where light is modulated by a radio signal and transmitted over an optical fiber link to provide broadband wireless services. The connection is established between a base station (BS) and central processing units (CPUs) as shown in the Figure 5.31.

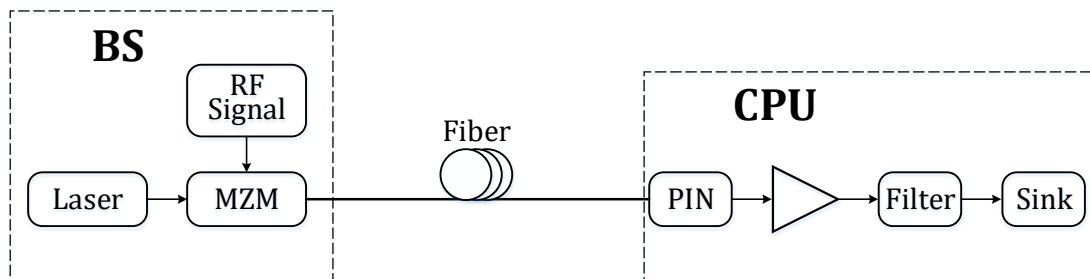


Figura 5.31: RoF transmission system block diagram.

In RoF systems, radio frequency (RF) signals are transported in optical form between a CPU and a set of BS before being radiated through the air. Each base station is adapted to communicate over a radio link with at least one user's mobile terminal located within the radio range of said BS. Considering an uplink connection in the Figure 5.31, the RF signals received from a mobile terminal are modulated using a laser and a mach-zehnder modulator (MZM) and then transmitted over optical link to CPU. In the CPU the optical signal is detected by a PIN, amplified and followed with an electrical filter. After these operations, digital signal processing techniques can be applied.

### 5.7.1 Simulation

### 5.7.2 Experimental





## 6.1 Add

### Input Parameters

This block takes no parameters.

### Functional Description

This block accepts two signals and outputs one signal built from a sum of the two inputs. The input and output signals must be of the same type.

### Input Signals

**Number:** 2

**Type:** Real, Complex or Complex\_XY signal (ContinuousTimeContinuousAmplitude)

### Output Signals

**Number:** 1

**Type:** Real, Complex or Complex\_XY signal (ContinuousTimeContinuousAmplitude)

## 6.2 Bit Error Rate

### Input Parameters

**Parameter:** setConfidence

**Parameter:** setMidReportSize

### Functional Description

This block accepts two binary strings and outputs a binary string, outputting a 1 if the two input samples are equal to each other and 0 if not. This block also outputs *.txt* files with a report of the calculated BER as well as the estimated Confidence bounds for a given probability  $P$ . The block allows for mid-reports to be generated, the number of bits between reports is customizable, if it is set to 0 then the block will only output the final report.

### Input Signals

**Number:** 2

**Type:** Binary (DiscreteTimeDiscreteAmplitude)

### Output Signals

**Number:** 1

**Type:** Binary (DiscreteTimeDiscreteAmplitude)

### 6.3 Binary source

This block generates a sequence of binary values (1 or 0) and it can work in four different modes:

- |                 |                             |
|-----------------|-----------------------------|
| 1. Random       | 3. DeterministicCyclic      |
| 2. PseudoRandom | 4. DeterministicAppendZeros |

This blocks doesn't accept any input signal. It produces any number of output signals.

#### Input Parameters

- Parameter:** mode{PseudoRandom}  
(Random, PseudoRandom, DeterministicCyclic, DeterministicAppendZeros)
- Parameter:** probabilityOfZero{0.5}  
(real  $\in [0,1]$ )
- Parameter:** patternLength{7}  
(integer  $\in [1,32]$ )
- Parameter:** bitStream{"0100011101010101"}  
(string of 0's and 1's)
- Parameter:** numberOfBits{-1}  
(long int)
- Parameter:** bitPeriod{1.0/100e9}  
(double)

#### Methods

```
BinarySource(vector<Signal *> &InputSig, vector<Signal *> &OutputSig) :Block(InputSig,
OutputSig){};
```

```
void initialize(void);
```

```
bool runBlock(void);
```

```
void setMode(BinarySourceMode m) BinarySourceMode const getMode(void)
```

```
void setProbabilityOfZero(double pZero)
```

```
double const getProbabilityOfZero(void)
```

```
void setBitStream(string bStream)
```

```

string const getBitStream(void)

void setNumberOfBits(long int nOfBits)

long int const getNumberOfBits(void)

void setPatternLength(int pLength)

int const getPatternLength(void)

void setBitPeriod(double bPeriod)

double const getBitPeriod(void)

```

### Functional description

The *mode* parameter allows the user to select between one of the four operation modes of the binary source.

**Random Mode** Generates a 0 with probability *probabilityOfZero* and a 1 with probability  $1 - \text{probabilityOfZero}$ .

**Pseudorandom Mode** Generates a pseudorandom sequence with period  $2^{\text{patternLength}} - 1$ .

**DeterministicCyclic Mode** Generates the sequence of 0's and 1's specified by *bitStream* and then repeats it.

**DeterministicAppendZeros Mode** Generates the sequence of 0's and 1's specified by *bitStream* and then it fills the rest of the buffer space with zeros.

### Input Signals

**Number:** 0

**Type:** Binary (DiscreteTimeDiscreteAmplitude)

### Output Signals

**Number:** 1 or more

**Type:** Binary (DiscreteTimeDiscreteAmplitude)

## Examples

### Random Mode

**PseudoRandom Mode** As an example consider a pseudorandom sequence with *patternLength*=3 which contains a total of 7 ( $2^3 - 1$ ) bits. In this sequence it is possible to find every combination of 0's and 1's that compose a 3 bit long subsequence with the exception of 000. For this example the possible subsequences are 010, 110, 101, 100, 111, 001 and 100 (they appear in figure 6.1 numbered in this order). Some of these require wrap.

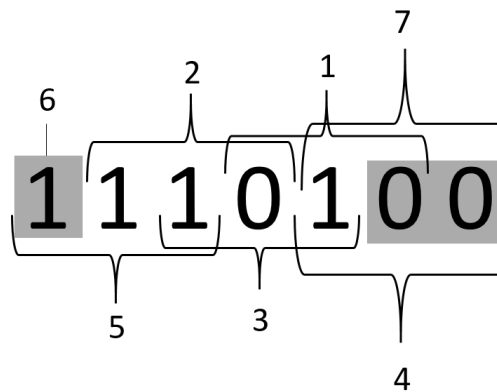


Figura 6.1: Example of a pseudorandom sequence with a pattern length equal to 3.

**DeterministicCyclic Mode** As an example take the *bit stream* '0100011101010101'. The generated binary signal is displayed in.

**DeterministicAppendZeros Mode** Take as an example the *bit stream* '0100011101010101'. The generated binary signal is displayed in 6.2.

### Sugestions for future improvement

Implement an input signal that can work as trigger.

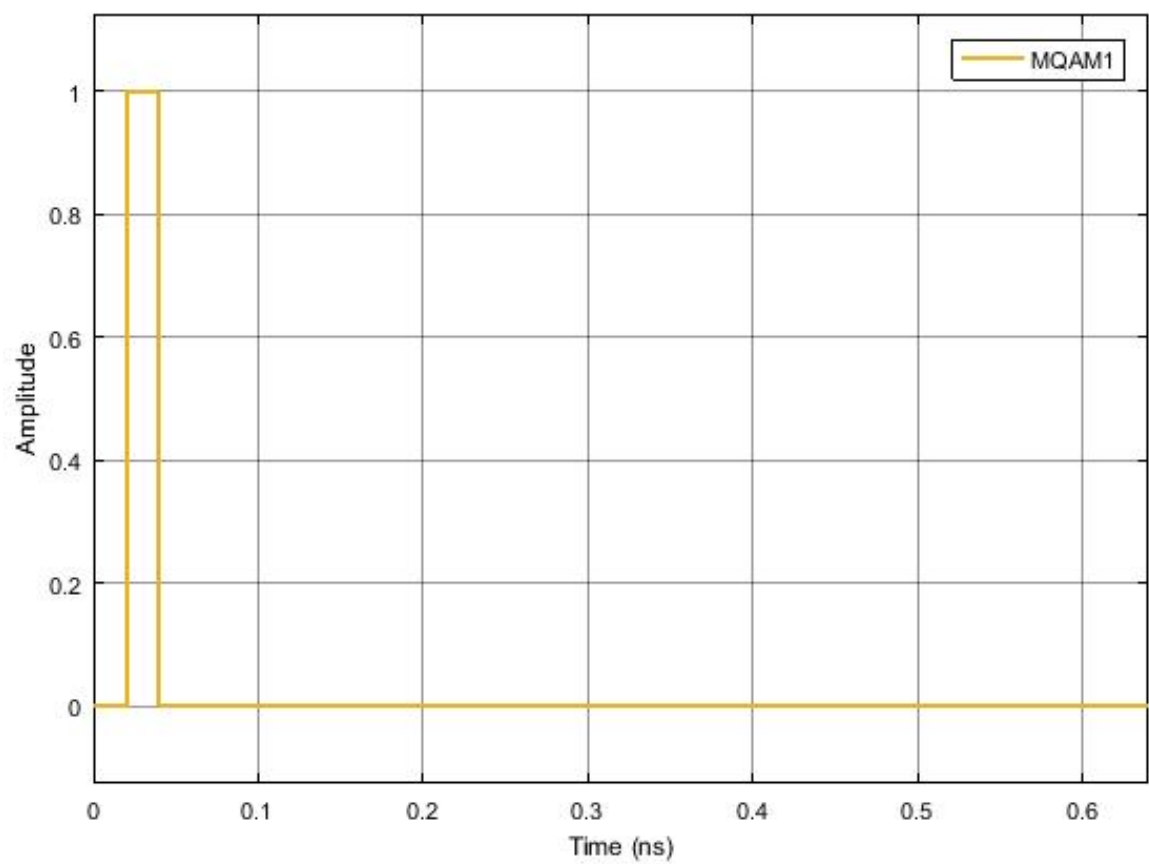


Figura 6.2: Binary signal generated by the block operating in the *Deterministic Append Zeros* mode with a binary sequence 01000...

## 6.4 Clock

This block doesn't accept any input signal. It outputs one signal that corresponds to a sequence of Dirac's delta functions with a user defined *period*.

### Input Parameters

**Parameter:** period{ 0.0 };

**Parameter:** samplingPeriod{ 0.0 };

### Methods

Clock()

Clock(vector<Signal \*> &InputSig, vector<Signal \*> &OutputSig) :Block(InputSig, OutputSig)

void initialize(void)

bool runBlock(void)

void setClockPeriod(double per)

void setSamplingPeriod(double sPeriod)

### Functional description

**Input Signals**

Number: 0

**Output Signals**

Number: 1

Type: Sequence of Dirac's delta functions.  
(TimeContinuousAmplitudeContinuousReal)

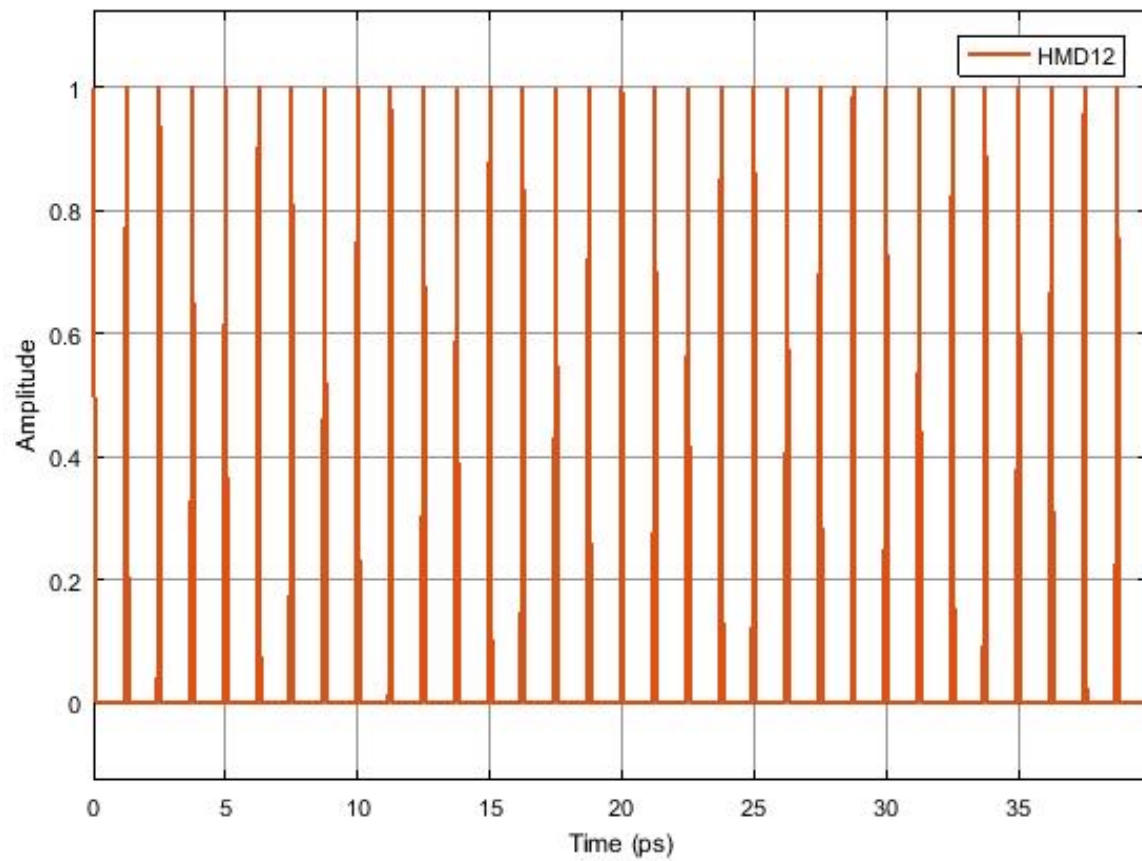
**Examples**

Figura 6.3: Example of the output signal of the clock

**Sugestions for future improvement**



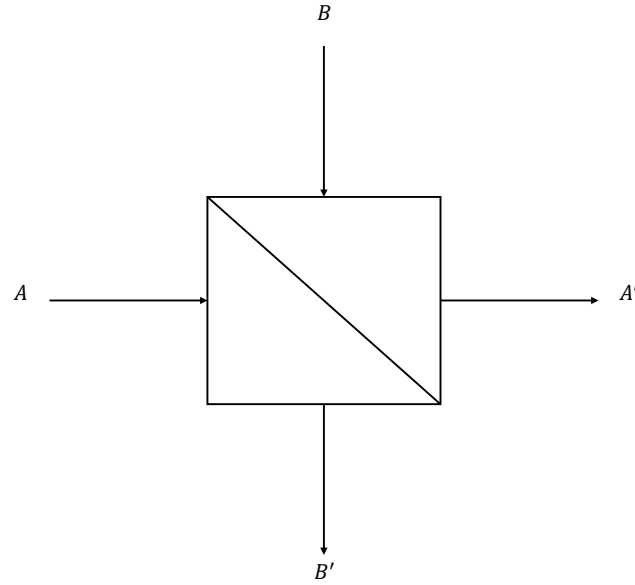


Figura 6.4: 2x2 coupler

## 6.5 Coupler 2 by 2

In general, the matrix representing 2x2 coupler can be summarized in the following way,

$$\begin{bmatrix} A' \\ B' \end{bmatrix} = \begin{bmatrix} T & iR \\ iR & T \end{bmatrix} \cdot \begin{bmatrix} A \\ B \end{bmatrix} \quad (6.1)$$

Where, A and B represent inputs to the 2x2 coupler and A' and B' represent output of the 2x2 coupler. Parameters T and R represent transmitted and reflected part respectively which can be quantified in the following form,

$$T = \sqrt{1 - \eta_R} \quad (6.2)$$

$$R = \sqrt{\eta_R} \quad (6.3)$$

Where, value of the  $\sqrt{\eta_R}$  lies in the range of  $0 \leq \sqrt{\eta_R} \leq 1$ .

It is worth to mention that if we put  $\eta_R = 1/2$  then it leads to a special case of "Balanced Beam splitter" which equally distribute the input power into both output ports.

## 6.6 Decoder

This block accepts a complex electrical signal and outputs a sequence of binary values (0's and 1's). Each point of the input signal corresponds to a pair of bits.

### Input Parameters

**Parameter:** `t_integer m{ 4 }`

**Parameter:** `vector<t_complex> iqAmplitudes{ { 1.0, 1.0 }, { -1.0, 1.0 }, { -1.0, -1.0 }, { 1.0, -1.0 } };`

### Methods

`Decoder()`

`Decoder(vector<Signal *> &InputSig, vector<Signal *> &OutputSig) :Block(InputSig, OutputSig)`

`void initialize(void)`

`bool runBlock(void)`

`void setM(int mValue)`

`void getM()`

`void setIqAmplitudes(vector<t_iqValues> iqAmplitudesValues)`

`vector<t_iqValues>getIqAmplitudes()`

### Functional description

This block makes the correspondence between a complex electrical signal and pair of binary values using a predetermined constellation.

To do so it computes the distance in the complex plane between each value of the input signal and each value of the *iqAmplitudes* vector selecting only the shortest one. It then converts the point in the IQ plane to a pair of bits making the correspondence between the input signal and a pair of bits.

### Input Signals

**Number:** 1

**Type:** Electrical complex (TimeContinuousAmplitudeContinuousReal)

### Output Signals

**Number:** 1

**Type:** Binary

### Examples

As an example take an input signal with positive real and imaginary parts. It would correspond to the first point of the *iqAmplitudes* vector and therefore it would be associated to the pair of bits 00.

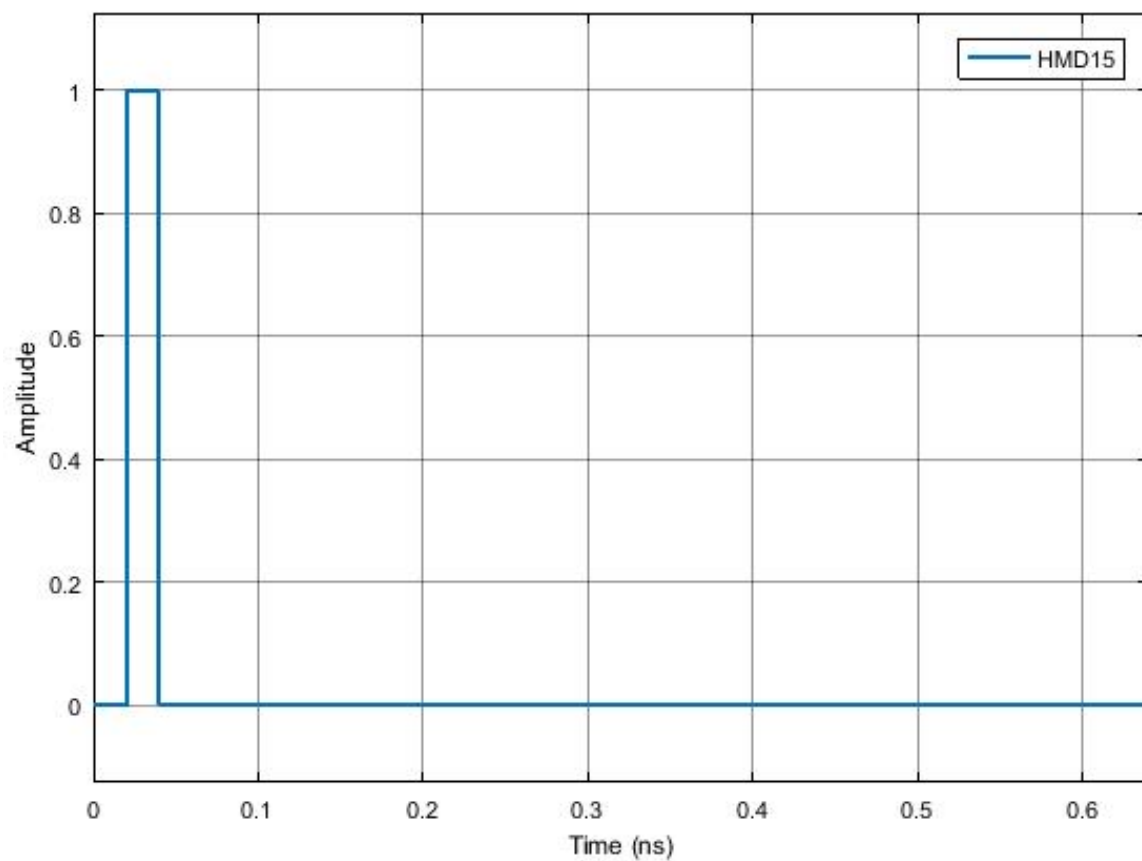


Figura 6.5: Example of the output signal of the decoder for a binary sequence 01. As expected it reproduces the initial bit stream

**Sugestions for future improvement**

## 6.7 Discrete to continuous time

This block converts a signal discrete in time to a signal continuous in time. It accepts one input signal that is a sequence of 1's and -1's and it produces one output signal that is a sequence of Dirac delta functions.

### Input Parameters

**Parameter:** `numberOfSamplesPerSymbol{8}`  
(int)

### Methods

```
DiscreteToContinuousTime(vector<Signal *> &inputSignals, vector<Signal *>
&outputSignals) :Block(inputSignals, outputSignals){};
```

```
void initialize(void);
```

```
bool runBlock(void);
```

```
void setNumberOfSamplesPerSymbol(int nSamplesPerSymbol)
```

```
int const getNumberOfSamplesPerSymbol(void)
```

### Functional Description

This block reads the input signal buffer value, puts it in the output signal buffer and it fills the rest of the space available for that symbol with zeros. The space available in the buffer for each symbol is given by the parameter *numberOfSamplesPerSymbol*.

### Input Signals

**Number** : 1

**Type** : Sequence of 1's and -1's. (DiscreteTimeDiscreteAmplitude)

### Output Signals

**Number** : 1

**Type** : Sequence of Dirac delta functions (ContinuousTimeDiscreteAmplitude)

### Example

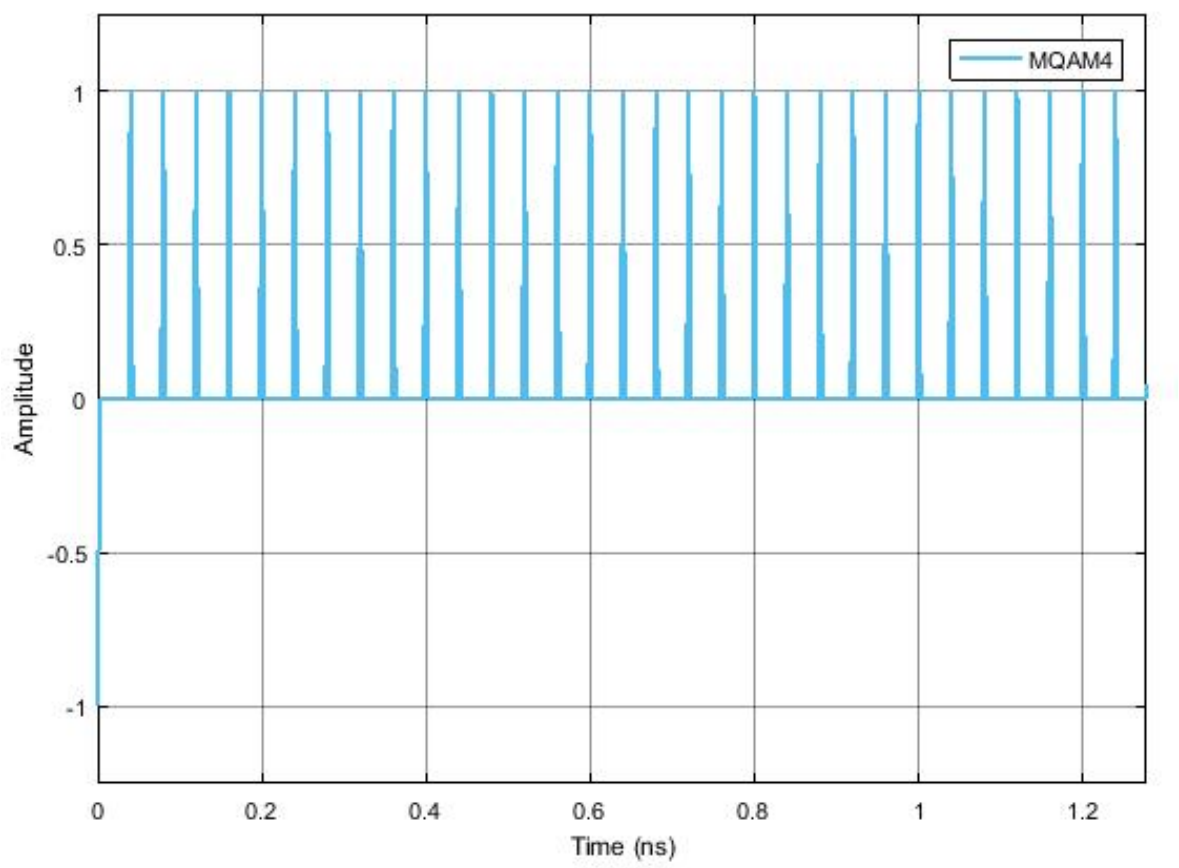


Figura 6.6: Example of the type of signal generated by this block for a binary sequence 0100...

## 6.8 Homodyne receiver

This block of code simulates the reception and demodulation of an optical signal (which is the input signal of the system) outputting a binary signal. A simplified schematic representation of this block is shown in figure 6.7.

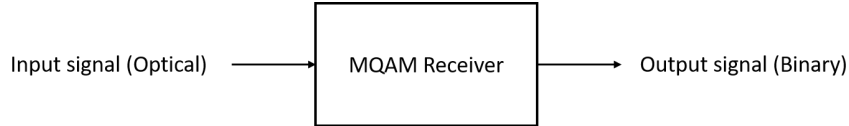


Figura 6.7: Basic configuration of the MQAM receiver

### Functional description

This block accepts one optical input signal and outputs one binary signal that corresponds to the M-QAM demodulation of the input signal. It is a complex block (as it can be seen from figure 6.8) of code made up of several simpler blocks whose description can be found in the *lib* repository.

It can also be seen from figure 6.8 that there's an extra internal (generated inside the homodyne receiver block) input signal generated by the *Clock*. This block is used to provide the sampling frequency to the *Sampler*.

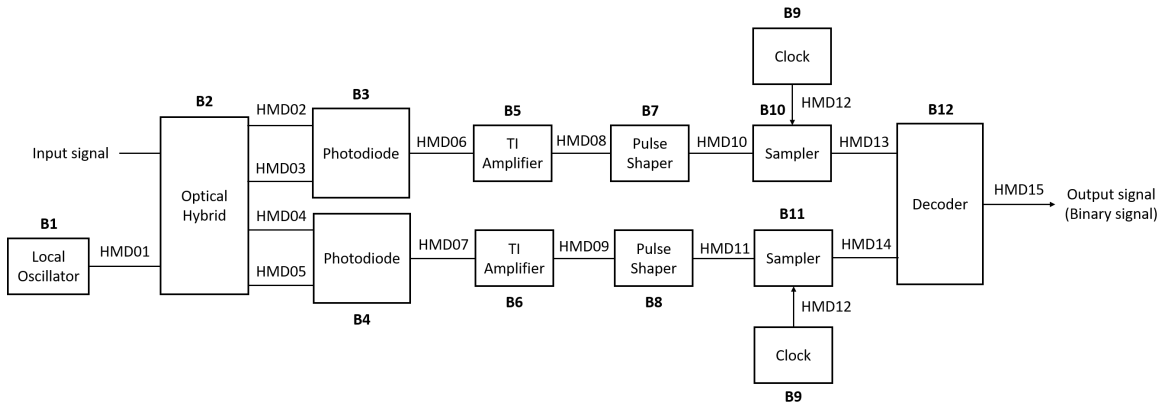


Figura 6.8: Schematic representation of the block homodyne receiver.

### Input parameters

This block has some input parameters that can be manipulated by the user in order to change the basic configuration of the receiver. Each parameter has associated a function that allows for its change. In the following table (table 6.2) the input parameters and corresponding functions are summarized.

Input parameters	Function	Type	Accepted values
IQ amplitudes	setIqAmplitudes	Vector of coordinate points in the I-Q plane	<b>Example</b> for a 4-qam mapping: { { 1.0, 1.0 }, { -1.0, 1.0 }, { -1.0, -1.0 }, { 1.0, -1.0 } }
Local oscillator power (in dBm)	setLocalOscillatorOpticalPower_dBm	double(t_real)	Any double greater than zero
Local oscillator phase	setLocalOscillatorPhase	double(t_real)	Any double greater than zero
Responsivity of the photodiodes	setResponsivity	double(t_real)	$\in [0,1]$
Amplification (of the TI amplifier)	setAmplification	double(t_real)	Positive real number
Noise amplitude (introduced by the TI amplifier)	setNoiseAmplitude	double(t_real)	Real number greater than zero
Samples to skip	setSamplesToSkip	int(t_integer)	
Save internal signals	setSaveInternalSignals	bool	True or False
Sampling period	setSamplingPeriod	double	Given by $symbolPeriod / samplesPerSymbol$

Tabela 6.1: List of input parameters of the block MQAM receiver

## Methods

HomodyneReceiver(vector<Signal \*> &inputSignal, vector<Signal \*> &outputSignal)  
(**constructor**)

void setIqAmplitudes(vector<t\_iqValues> iqAmplitudesValues)

vector<t\_iqValues> const getIqAmplitudes(void)

void setLocalOscillatorSamplingPeriod(double sPeriod)

void setLocalOscillatorOpticalPower(double opticalPower)

void setLocalOscillatorOpticalPower\_dBm(double opticalPower\_dBm)

void setLocalOscillatorPhase(double lOscillatorPhase)

void setLocalOscillatorOpticalWavelength(double lOscillatorWavelength)

void setSamplingPeriod(double sPeriod)



```
void setResponsivity(t_real Responsivity)
void setAmplification(t_real Amplification)
void setNoiseAmplitude(t_real NoiseAmplitude)
void setImpulseResponseTimeLength(int impResponseTimeLength)
void setFilterType(PulseShaperFilter fType)
void setRollOffFactor(double rOffFactor)
void setClockPeriod(double per)
void setSamplesToSkip(int sToSkip)
```

**Input Signals**

**Number:** 1

**Type:** Optical signal

**Output Signals**

**Number:** 1

**Type:** Binary signal

**Example**

**Suggestions for future improvement**

## 6.9 IQ modulator

This blocks accepts one inupt signal continuous in both time and amplitude and it can produce either one or two output signals. It generates an optical signal and it can also generate a binary signal.

### Input Parameters

**Parameter:** outputOpticalPower{1e-3}  
(double)

**Parameter:** outputOpticalWavelength{1550e-9}  
(double)

**Parameter:** outputOpticalFrequency{speed\_of\_light/outputOpticalWavelength}  
(double)

### Methods

```
IqModulator(vector<Signal *> &InputSig, vector<Signal *> &OutputSig) :Block(InputSig,
OutputSig){};
```

```
void initialize(void);
```

```
bool runBlock(void);
```

```
void setOutputOpticalPower(double outOpticalPower)
```

```
void setOutputOpticalPower_dBm(double outOpticalPower_dBm)
```

```
void setOutputOpticalWavelength(double outOpticalWavelength)
```

```
void setOutputOpticalFrequency(double outOpticalFrequency)
```

### Functional Description

This block takes the two parts of the signal: in phase and in amplitude and it combines them to produce a complex signal that contains information about the amplitude and the phase.

This complex signal is multiplied by  $\frac{1}{2}\sqrt{\text{outputOpticalPower}}$  in order to reintroduce the information about the energy (or power) of the signal. This signal corresponds to an optical signal and it can be a scalar or have two polarizations along perpendicular axis. It is the signal that is transmited to the receptor.

The binary signal is sent to the Bit Error Rate (BER) meaurement block.

### Input Signals

**Number** : 2

**Type** : Sequence of impulses modulated by the filter (ContinuousTimeContinuousAmplitude))

### Output Signals

**Number** : 1 or 2

**Type** : Complex signal (optical) (ContinuousTimeContinuousAmplitude) and binary signal (DiscreteTimeDiscreteAmplitude)

### Example

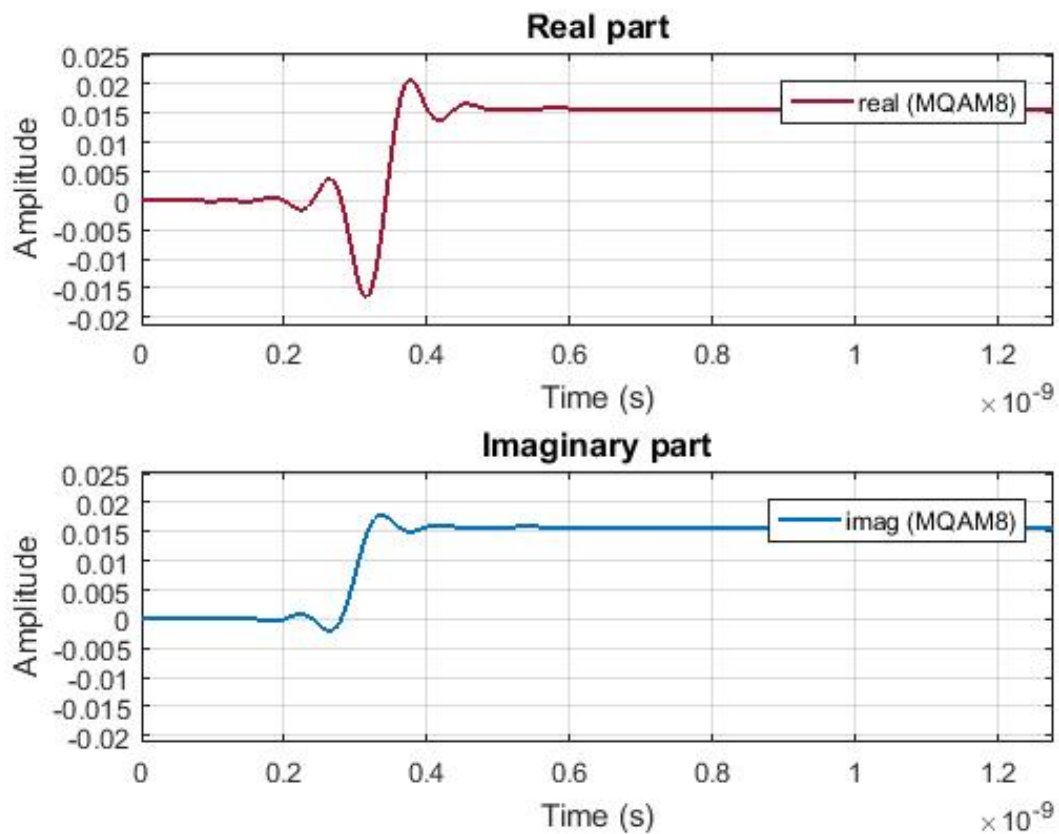


Figura 6.9: Example of a signal generated by this block for the initial binary signal 0100...

## 6.10 Local Oscillator

This block simulates a local oscillator which can have shot noise or not. It produces one output complex signal and it doesn't accept input signals.

### Input Parameters

**Parameter:** opticalPower{ 1e-3 }

**Parameter:** wavelength{ 1550e-9 }

**Parameter:** frequency{ SPEED\_OF\_LIGHT / wavelength }

**Parameter:** phase{ 0 }

**Parameter:** samplingPeriod{ 0.0 }

**Parameter:** shotNoise{ false }

### Methods

LocalOscillator()

```
LocalOscillator(vector<Signal *> &InputSig, vector<Signal *> &OutputSig)
:Block(InputSig, OutputSig){};
```

```
void initialize(void);
```

```
bool runBlock(void);
```

```
void setSamplingPeriod(double sPeriod);
```

```
void setOpticalPower(double oPower);
```

```
void setOpticalPower_dBm(double oPower_dBm);
```

```
void setWavelength(double wlength);
```

```
void setPhase(double lOscillatorPhase);
```

```
void setShotNoise(bool sNoise);
```

### Functional description

This block generates a complex signal with a specified phase given by the input parameter *phase*.

It can have shot noise or not which corresponds to setting the *shotNoise* parameter to True or False, respectively. If there isn't shot noise the the output of this block is given by  $0.5 * \sqrt{\text{OpticalPower}} * \text{ComplexSignal}$ . If there's shot noise then a random gaussian distributed noise component is added to the *OpticalPower*.

**Input Signals**

Number: 0

**Output Signals**

Number: 1

Type: Optical signal

**Examples**

**Suggestions for future improvement**

## 6.11 MQAM mapper

This block does the mapping of the binary signal using a  $m$ -QAM modulation. It accepts one input signal of the binary type and it produces two output signals which are a sequence of 1's and -1's.

### Input Parameters

**Parameter:** `m{4}`  
(`m` should be of the form  $2^n$  with `n` integer)

**Parameter:** `iqAmplitudes{{ 1.0, 1.0 }, { -1.0, 1.0 }, { -1.0, -1.0 }, { 1.0, -1.0 }}`

### Methods

```
MQamMapper(vector<Signal *> &InputSig, vector<Signal *> &OutputSig)
:Block(InputSig, OutputSig) {};
```

```
void initialize(void);
```

```
bool runBlock(void);
```

```
void setM(int mValue);
```

```
void setIqAmplitudes(vector<t_iqValues> iqAmplitudesValues);
```

### Functional Description

In the case of  $m=4$  this block attributes to each pair of bits a point in the I-Q space. The constellation used is defined by the *iqAmplitudes* vector. The constellation used in this case is illustrated in figure 6.10.

### Input Signals

**Number** : 1

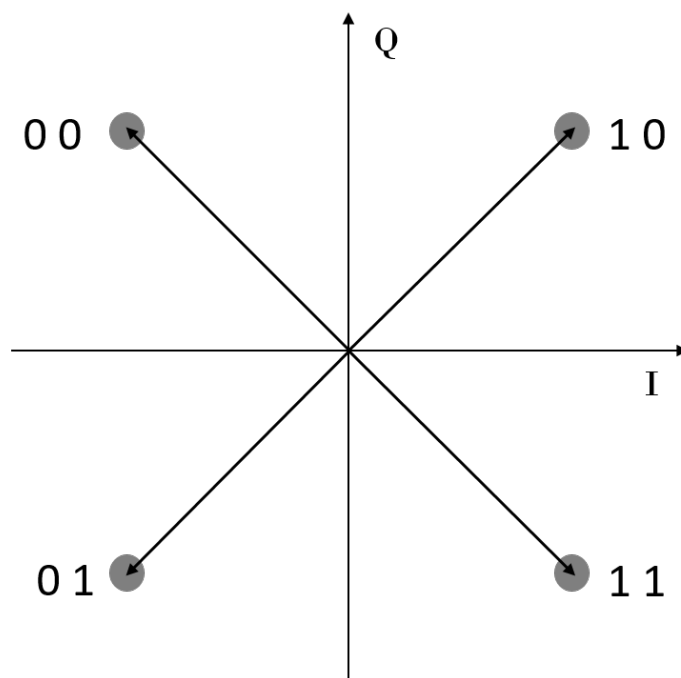
**Type** : Binary (DiscreteTimeDiscreteAmplitude)

### Output Signals

**Number** : 2

**Type** : Sequence of 1's and -1's (DiscreteTimeDiscreteAmplitude)

### Example

Figura 6.10: Constellation used to map the signal for  $m=4$



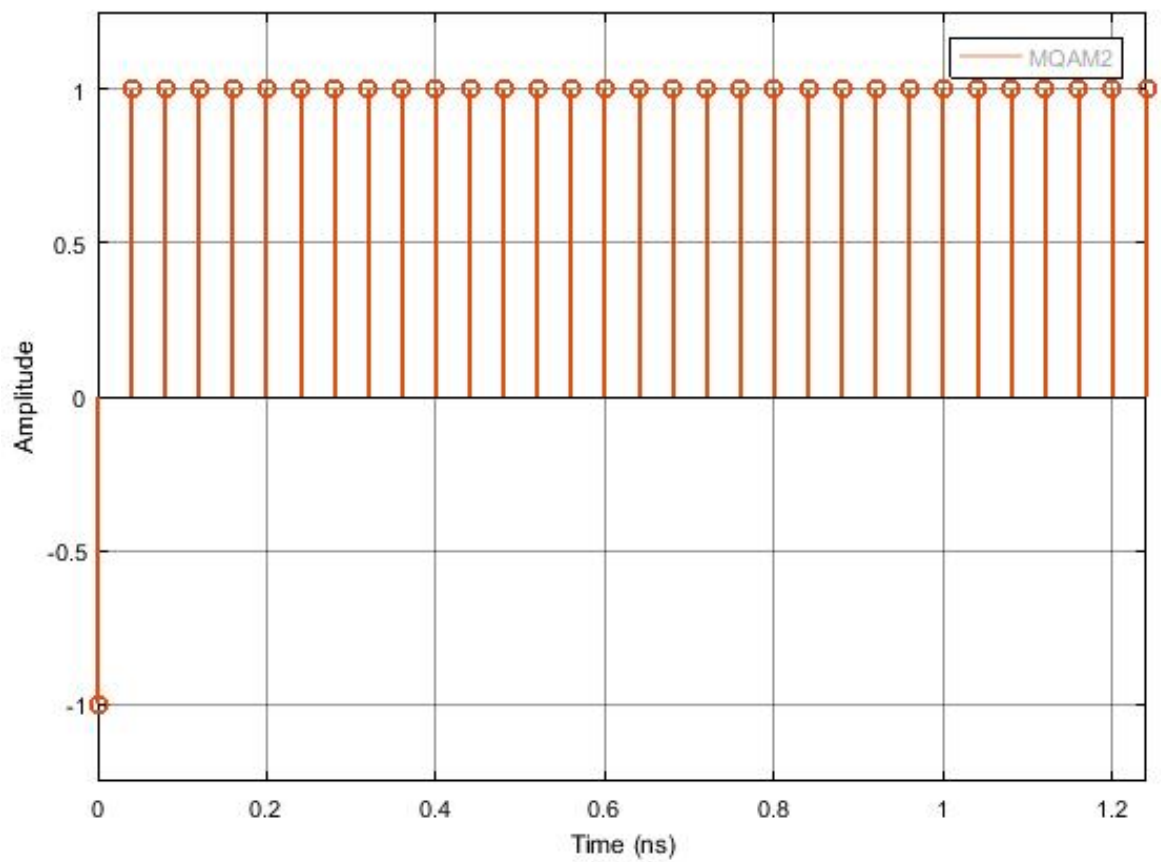


Figura 6.11: Example of the type of signal generated by this block for the initial binary signal 0100...

## 6.12 MQAM transmitter

This block generates a MQAM optical signal. It can also output the binary sequence. A schematic representation of this block is shown in figure 6.12.

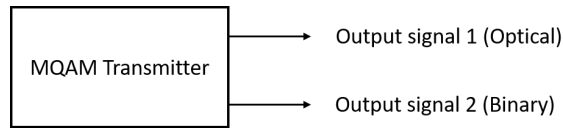


Figura 6.12: Basic configuration of the MQAM transmitter

### Functional description

This block generates an optical signal (output signal 1 in figure 6.13). The binary signal generated in the internal block Binary Source (block B1 in figure 6.13) can be used to perform a Bit Error Rate (BER) measurement and in that sense it works as an extra output signal (output signal 2 in figure 6.13).

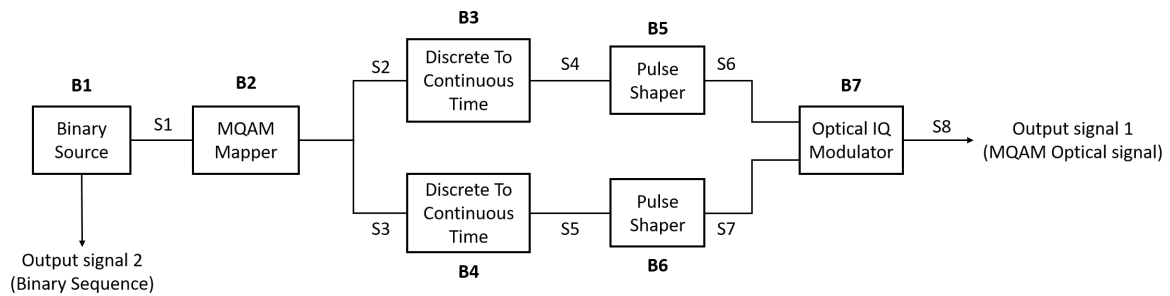


Figura 6.13: Schematic representation of the block MQAM transmitter.

### Input parameters

This block has a special set of functions that allow the user to change the basic configuration of the transmitter. The list of input parameters, functions used to change them and the values that each one can take are summarized in table 6.2.

Input parameters	Function	Type	Accepted values
Mode	setMode()	string	PseudoRandom Random DeterministicAppendZeros DeterministicCyclic
Number of bits generated	setNumberOfBits()	int	Any integer
Pattern length	setPatternLength()	int	Real number greater than zero
Number of bits	setNumberOfBits()	long	Integer number greater than zero
Number of samples per symbol	setNumberOfSamplesPerSymbol()	int	Integer number of the type $2^n$ with n also integer
Roll of factor	setRollOfFactor()	double	$\in [0,1]$
IQ amplitudes	setIqAmplitudes()	Vector of coordinate points in the I-Q plane	<b>Example</b> for a 4-qam mapping: { { 1.0, 1.0 }, { -1.0, 1.0 }, { -1.0, -1.0 }, { 1.0, -1.0 } }
Output optical power	setOutputOpticalPower()	int	Real number greater than zero
Save internal signals	setSaveInternalSignals()	bool	True or False

Tabela 6.2: List of input parameters of the block MQAM transmitter

## Methods

MQamTransmitter(vector<Signal \*> &inputSignal, vector<Signal \*> &outputSignal);  
(**constructor**)

void set(int opt);

void setMode(BinarySourceMode m)

BinarySourceMode const getMode(void)

void setProbabilityOfZero(double pZero)

double const getProbabilityOfZero(void)

void setBitStream(string bStream)

string const getBitStream(void)

```
void setNumberOfBits(long int nOfBits)

long int const getNumberOfBits(void)

void setPatternLength(int pLength)

int const getPatternLength(void)

void setBitPeriod(double bPeriod)

double const getBitPeriod(void)

void setM(int mValue) int const getM(void)

void setIqAmplitudes(vector<t_iqValues> iqAmplitudesValues)

vector<t_iqValues> const getIqAmplitudes(void)

void setNumberOfSamplesPerSymbol(int n)

int const getNumberOfSamplesPerSymbol(void)

void setRollOffFactor(double rOffFactor)

double const getRollOffFactor(void)

void setSeeBeginningOfImpulseResponse(bool sBeginningOfImpulseResponse)

double const getSeeBeginningOfImpulseResponse(void)

void setOutputOpticalPower(t_real outOpticalPower)

t_real const getOutputOpticalPower(void)

void setOutputOpticalPower_dBm(t_real outOpticalPower_dBm)

t_real const getOutputOpticalPower_dBm(void)
```

## Output Signals

**Number:** 1 optical and 1 binary (optional)

**Type:** Optical signal

## Example

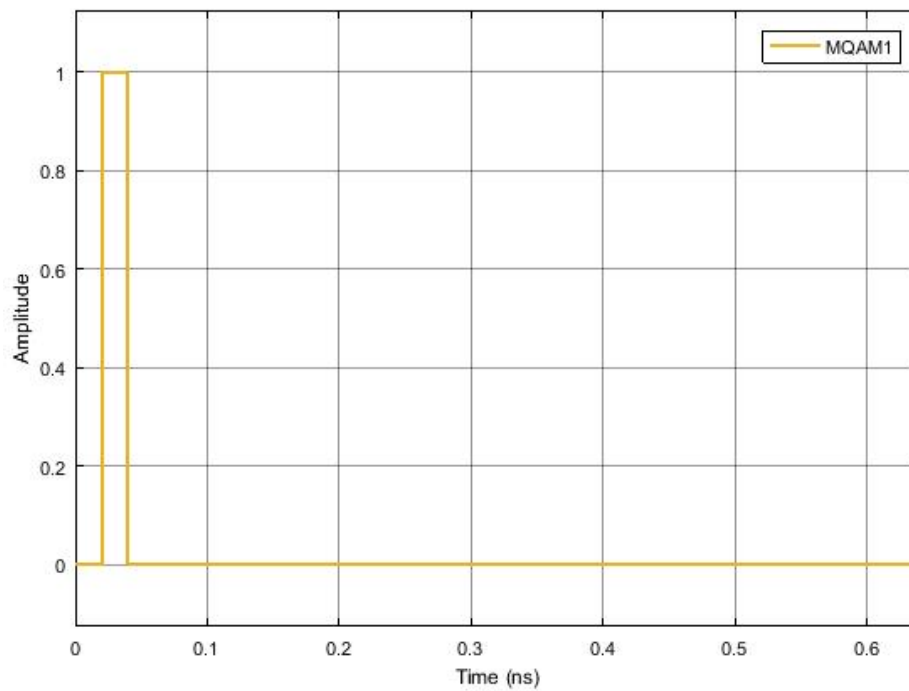


Figura 6.14: Example of the binary sequence generated by this block for a sequence 0100...

## Sugestions for future improvement

Add to the system another block similar to this one in order to generate two optical signals with perpendicular polarizations. This would allow to combine the two optical signals and generate an optical signal with any type of polarization.

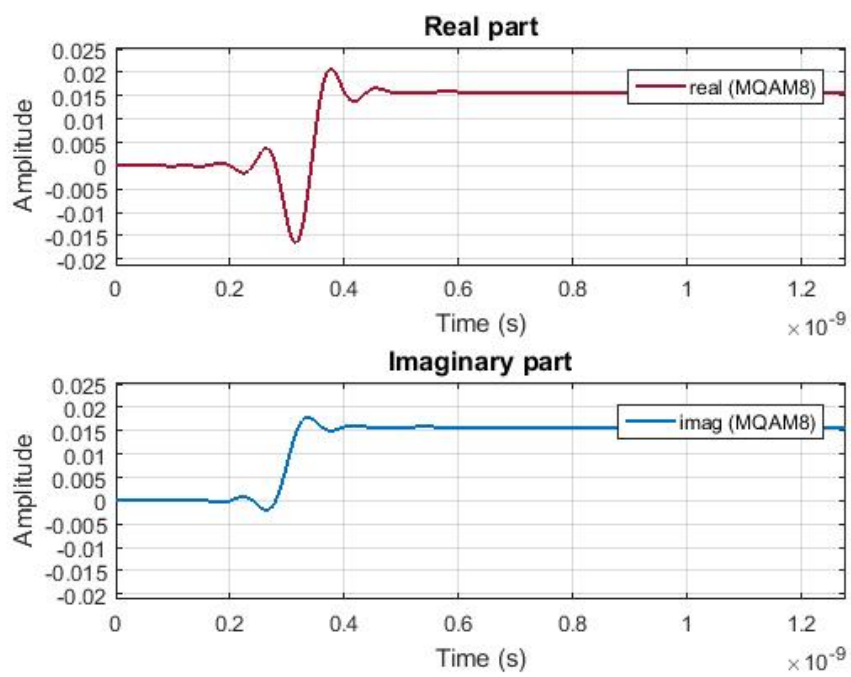


Figura 6.15: Example of the output optical signal generated by this block for a sequence 0100...

