Proyecto laboratorio intermedio
Obtención de números aleatorios

Paul Díaz* and Nicolás Barbosa**
Universidad de los Andes, Departamento de Física
Laboratorio Intermedio primer semestre de 2012

(Dated: 28 de mayo de 2012)

Se obtienen 3 secuencias aleatorias de unos y ceros usando 3 fuentes de emisión de fotones: un láser de $\lambda = 650$ nm; el mismo láser pero ubicando ahora un acrílico rotante en la trayectoria de los fotones y un led de chorro rojo. Los fotones se desvían por medio de un Polarizing Beam Splitter ajustando la proporción de detecciones lo más cercano a 50/50 con una lámina de onda, lo cual hace que se tengan fotones por los dos caminos que produce el Beam Splitter. Se ubican detectores a la salida de dichos caminos y se realiza la cuenta de las detecciones de fotones en cada detector etiquetando a cada uno de estos como un 1 o un 0. Se desechan detecciones nulas [(0,0) o (1,1)] limpiando las secuencias obtenidas, obteniendo así secuencias de más de 250 mil datos.

I. OBJETIVOS GENERALES

*Obtener 3 secuencias de números aleatorios que provengan de 3 fuentes de fotones con características distintas comparando cuál de ellas tiende a tener mayor aleatoriedad. Para esto se hace uso de una serie de pruebas de aleatoriedad programadas en MATLAB.

*Comprobar que las fuentes de aleatoriedad más eficaces tienen origen cuántico.

*Programar las pruebas de aleatoriedad necesarias para evaluar los datos obtenidos de las 3 fuentes de fotones anteriormente mencionadas.

*Realizar los montajes de las 3 fuentes de aleatoriedad usando las herramientas presentes en el laboratorio de óptica cuántica y realizando pequeï£¡os montajes electrónicos por nuestra cuenta, pero siempre orientados por nuestro profesor supervisor.

*Entender por qué las fuentes de secuencias aleatorias cuánticas son más eficaces que las fuentes clásicas o computacionales.

II. MARCO TEÓRICO:

Un generador de números aleatorios es un dispositivo capaz de producir una secuencia de números de la que no se puede extraer fácilmente propiedades del tipo determinista. En la actualidad se usan métodos físicos para producir una secuencia aleatoria aprovechando el carácter aleatorio de los fenómenos cuánticos.

La utilidad de los números aleatorios está presente en diversos campos de estudio, como por ejemplo la teoría de juegos, simulaciones y análisis de datos, muestreo, seguridad informática (criptografía), simulaciones de sistemas físicos complejos, biológicos y químicos, información cuántica entre otras. La aleatoriedad es un concepto muy difícil de definir matemáticamente por lo cual, para realizar un estudio adecuado de esta propiedad, es necesario aprovechar el uso de algunos fenómenos que son intrínsecamente aleatorios. Como problema se tiene que dichos fenómenos poseen un comportamiento aleatorio bajo unas circustancias muy específicas, las cuales son un poco difíciles de lograr.

La aleatoriedad es el fenómeno opuesto al orden donde no hay un patrón a seguir. De ahí que las secuencias producidas por fenómenos físicos o computacionales clásicos no sean 100 % aleatorios (son llamados pseualeatorios). La teoría de la información en física permite llegar a pensar que todo sistema físico puede ser descrito por la cantidad de información que éste almacena o intercambia con otros donde la información clásica se ve como una secuencia ordenada y estructurada de símbolos o etiquetas; en consecuencia, la aleatoriedad verdadera estaría en contra de esta definición clásica de información y entonces hace que definir el concepto de aleatoriedad matemáticamente sea muy difícil de lograr.

Lo que sí se ha definido es el concepto de aleatoriedad verdadera y pseudoaleatriedad lo cual se ha venido estudiando en estas dos primeras décadas del siglo XXI, obteniendo como resultado que las secuencias provenientes de fenómenos cuánticos tienden a ser verdaderamente aleatorias debido al carácter no determinista y no local de la mecánica cuántica, y por esto se tiene un azar verdadero en los fenómenos del mundo microscópico, debido al cual es imposible enviar información de manera instantánea. Si fuese posible sería una contradicción del principio de causalidad relativista, uno de los pilares de

*Código: 200823716,Departamento de Física, Universidad de los Andes.
**Código: 200911134,Departamento de Física, Universidad de los Andes.

la física moderna.

Aquellas secuencias aleatorias que provienen de fenómenos clásicos tanto físicos como computacionales presentan una aleatoriedad ficticia o pseudoaleatoriedad. Realmente los procesos de la física clásica no son aleatorios; la aparente aleatoriedad es producto de la imprecisión tanto computacional como experiemntal, de ahí que fenómenos estadísticos macroscópicos como lanzar un dado N-veces, una moneda o secuencias generadas por los computadores actuales no sean totalmente aleatorias.

Debido a la importancia práctica de las secuencias aleatorias, actualmente se dedica un enorme esfuerzo a desarrollar buenos generadores de números aleatorios, detectores, electrónica y programación. Es importante considerar los problemas fundamentales que tienen las secuencias aleatorias y sus posibles soluciones.

El primer problema es certificar la aleatoriedad de la secuencia: para resolver lo mejor posible este problema se implementan una serie de controles estadísticos diseï£¡ados para encontrar algún tipo de patrón en dicha frecuencia, aunque hoy en día se plantea adicionalmente un problema de criterio debido a que se está juzgando la aleatoriedad de una secuencia que proviende de fenómenos cuánticos con pruebas estadísticas realizadas de manera clásica.

Como segundo problema se tiene la independencia respecto al dispositivo de generación usado: este problema actualmente no se ha podido corregir ya que las propiedades de las secuencias aleatorias dependen del montaje experimental, cosa que se debería evitar con el fin de lograr una secueencia perfectamente aleatoria.

A. Aleatoriedad cuántica

La aleatoriedad cuántica se presenta en la medida de un sistema en la superposición cuántica de estados base:

$$|\psi\rangle = \sum a_i |x_i\rangle \tag{1}$$

Los coeficientes a_i con $i \epsilon$ N nos da la amplitud de probabilidad con $\sum |a_i|^2 = 1$. Para el caso especial cuando la base del espacio de Hilbert del sistema en estudio está formada por dos kets tenemos:

$$|\psi\rangle = a_1 |x_1\rangle + a_2 |x_2\rangle \tag{2}$$

Con lo que se tiene un vector de estado que es la superposición de los elementos de una base de un sistema de dos niveles también llamado Qubit. Por los postulados de la mecánica cuántica se tiene que la medida sobre un Qubit nos da la proyección sobre uno de los estados bases donde la probabilidad que el sistema colapse a uno de dichos estados base está dada por la norma cuadrada de los coeficientes a_i.

Para este proyecto se usa un fotón simple que, junto al Beam Splitter 50/50, generan un sistema Qubit donde el vector de estado es:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|T\rangle + |R\rangle) \tag{3}$$

Donde T representa uno de los vectores base del sistema que nos dice si el fotón fue transmitido por el Beam Splitter y R el otro vector de la base del sistema que nos dice si el fotón incidente fue reflejado; para este caso, como los coeficientes a_i del sistema son iguales a $1/\sqrt{2}$, se tiene que el fotón tiene igual probabilidad de colapsar en el estado T como en el estado R. En consecuencia se tiene un fenómeno claramente no determinista a estudiar como se desea para obtener la secuencia aleatoria.

B. Tipos de generadores de números aleatorios

Generadores fundamentados en fenómenos imprevisibles, aunque en algunas ocasiones se presentan secuencias seguidas de números, son a menudo medios prácticos para producir aletoriedad de manera poco sofisticada, entre ellos están los dados, la ruleta, loterías, sorteos, entre otras.

C. Generadores basados en algoritmos

Un algoritmo tiende a ser determinista debido a que si éste se aplica a los mismos parámetros el resultado es idéntico, pero existen algunas operaciones que son lo suficientemente imprevisibles para dar como resultado datos que parecen ser aleatorios. Los números obtenidos de esta forma son llamados *pseudoaleatorios*. Estos números son usados debido a que es mucho más fácil de producir que una secuencia totalmente aleatoria donde los métodos de producción son mucho más sencillos de implementar. Algunas veces, a partir de estos números pseudoaleatorios se pueden obtener secuencias de números verdaderamente aleatorias implementando otro algoritmo que sea mucho más sencillo que aquel que se quisiera implementar al principio, sin pasar por la obtención de la secuencia pseudoaleatoria.

D. Generadores basados en fenómenos físicos

Los mejores generadores se basan comúnmente en fenómenos como la radiactividad, ruidos térmicos, ruidos electromagnéticos, mecánica y óptica cuántica. En el caso de estos dos últimos, que es el caso que interesa en

este proyecto, se tiene que es la mejor fuente de estos tipos de secuencias ya que la aleatoriedad de la mecánica cuántica está implícita en el carácter probabilístico y no determinista de esta teoría.

E. Generadores mixtos

Usan de manera simultánea fenómenos físicos de aleatoriedad y algoritmos pseudoaleatorios para producir una secuencia cercana a la perfección.
Para el proyecto se hace uso de la aletoriedad intrínseca en la mecánica cuántica donde los fotones emitidos por un rayo láser inciden en un Beam Splitter con el cual el fotón tiene igual probabilidad de ser reflejado o transmitido. Establecer con anticipación una secuencia de números definida por la llegada de fotones a cada uno de los dos detectores es imposible debido al carácter no determinista de la mecánica cuántica. El láser, al tener un comportamiento dual, es regido por las leyes cuánticas por lo que no es posible establecer de antemano a qué detector llega el fotón emitido, de ahí que sea una buena fuente de obtención de números aleatorios.

F. Pruebas estadísticas de aleatoriedad

Para establecer si una secuencia de números es aleatoria o no, es necesario realizar una serie de pruebas que analicen si se cumplen determinadas características propias de la aleatoriedad. Si la secuencia no pasa alguna de las pruebas, se puede establecer que el generador o fuente de dicha secuencia es poco eficiente. Pasar una prueba de aleatoriedad es una condición necesaria mas no suficiente, ya que puede que exista una prueba mucho más rigurosa que la secuencia en estudio no pueda pasar.

A continuación se muestran las características generales de las pruebas de aleatoriedad, las pruebas específicas usadas en este proyecto se muestran en el análisis de resultados:

- **Prueba de Chi-cuadrado:** Se comparan las frecuencias observadas con las frecuencias obtenidas.
- **Prueba de Kolmogorov-Smirnov:** Permite establecer si una muestra de datos u observaciones tiene el comportamiento de una distribución continua particular comparando la desviación máxima esperada con la observada.
- **Prueba de correlación serial:** Probar la posible dependendencia de las dos variables calculando covarianza.
- **Prueba de dos niveles:** Realizar las pruebas estadísticas descritas anteriormente a un grupo de datos para tener un análisis local y a toda la secuencia para tener un análisis global.
- **Prueba serial:** Probar la uniformidad de los datos en 1 o más dimensiones.
- **Prueba de rachas:**Probar si la secuencia obtenida tiene una racha de aparición de eventos consecutivos de un mismo tipo. Tipos de rachas: rachas crecientes y decrecientes, rachas bajo y sobre la media. La longitud de las rachas es de vital importancia para determinar si la aparición de determinado número de manera consecutiva es poco despreciable.

III. PASOS GENERALES A SEGUIR PARA LA OBTENCIÓN DE LAS 3 SECUENCIAS.

A. Realizar el montaje de las fuentes de fotones

Fue necesario relaizar 3 distintos montajes para obtener las 3 fuentes de emisión de fotones de las que se obtiene las frecuencias a analizar, claro que reutilizando algunos elementos del primer montaje como los espejos guía, la lámina de onda y filtros polarizadores. Los montajes se realizaron usando los elementos dispuestos en el laboratorio de óptica cuántica y algunos circuitos electrónicos básicos que facilitaban la distribución de voltaje para el funcionamiento de todos los aparatos electrónicos del montaje y para el funcionamiento de una de las fuentes como es el caso del montaje donde se usa un LED rojo.

B. Establecer la intensidad de recepción de fotones adecuada

Para obtener las secuencias aleatorias de 1 y 0 fue necesario calibrar la intensidad de fotones que son transmitidos o reflejados debido a que los detectores de alta presición que son ubicados a la salida del Beam splitter pueden sufrir avería al incidir un gran número de fotones. Así se hizo la calibración para los tres montajes ya que la intensidad varía en cada uno de ellos, todo con el fin de tener un buen número de fotones que llegan a cada detector, pero teniendo especial cuidado en la intensidad límite que soportan los detectores. También fue indispensable hacer uso de una lámina de onda para calibrar la proporción de unos y ceros donde dicha calibración es propia de cada montaje.

C. Establecer una ventana de tiempo adecuada para la recepción de fotones

Además de calibrar la intensidad de recepción de fotones para cada detector, fue necesario calibrar la

ventana de tiempo con la cual el detector realiza un conteo, es decir el tiempo en el cual se puede establecer si al detector llega o no llega un fotón. Si la ventana es muy grande llegarán muchos fotones y no es posible obtener la secuencia aleatoria. Si la ventana es muy pequeï£¡a se puede presentar que el detector informe que nunca recibió un fotón.

Para los montajes se manejaron ventanas de $1\mu s$ y $2\mu s$ donde se tenían a lo sumo 2 ó 3 detecciones, pero en general se observaba una detección en el intervalo de tiempo dado por la ventana. Los casos donde se tienen más de una detección fueron eliminados cuando se obtiene el archivo con la secuencia.

D. Obtener el mismo número de ceros y unos

Al obtener la secuencia aleatoria se establece qué detector es titulado como el detector de un cero o de un uno. Para que se pueda hablar de una secuencia aleatoria es necesario que se obtengan el mismo número de unos y ceros, lo cual se logra con el uso del Beam Splitter 50/50 casi perfecto.

Como encontrar un instrumento perfecto es imposible, se hace uso de un Beam-splitter de polarización y una lamina de onda para generar asi un Beam splitter 50/50. Se tiene que los fotones salen de la fuente prepolarizados, llegan a la lamina de onda la cual cuadra el angulo de polarización a un valor cercano a 45 grados, los fotones con dicha polarización llegan al Beam splitter de polarización, teniendo la misma probabilidad de ser reflejados o transmitidos.

E. Programar los algoritmos de prueba de secuencia aleatoria

Después de obtener la secuencia de unos y ceros se programan las pruebas de aleatoriedad usando MATLAB. Estas pruebas tienen como fin establecer si la secuencia obtenida cumple con las propiedades de una secuencia aleatoria para establecer qué fuente de fotones permite obtener dicha secuencia con mayor facilidad y efectividad, como se dijo anteriormente, estas pruebas se explican en el análisis de resultados.

IV. MONTAJE Y PROCEDIMIENTO EXPERIMENTAL

A. Montaje 1:Fuente de fotones Láser $\lambda = 650nm$

Se hizo uso de un láser cuya longitud de onda de la luz emitida tiene un valor de $650nm$, ubicando dicho laser lejos de el Beam Splitter y de la lamina de onda.

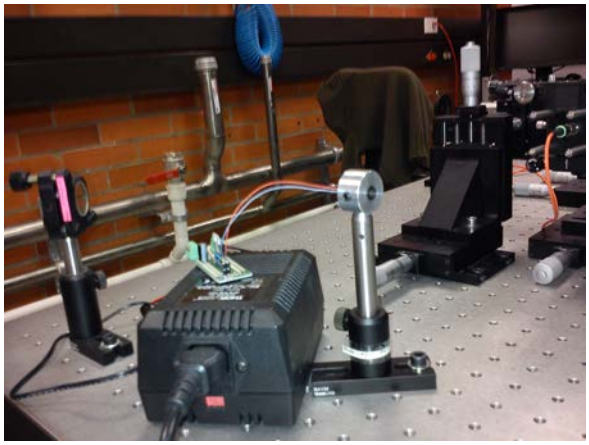

Figura 1: Imagen del láser utilizado en el experimento, la ámina de onda y el beam splitter no están frente al láser.

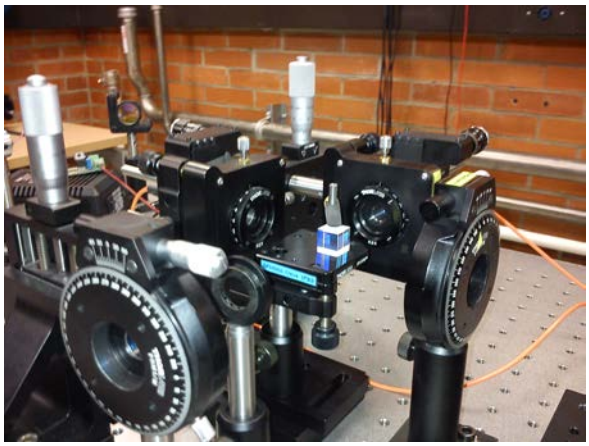

Figura 2: Imagen del montaje donde está ubicado el beam splitter y la lámina de onda se alcanza a observar que la fuente del láser está ubicado al lado de este montaje para que los fotones no incidan de frente.

Los fotones que salen del láser son guiados al lugar de la detección por medio de dos espejos los cuales reflejan el paquete de fotones incidente hasta que llegan al montaje donde se ubica el Beam Splitter. En las dos salidas de este dispositivo donde se obtiene los fotones que son reflejados o transmitidos se ubican dos dispositivos de recepción los cuales se conectan a los detectores por fibras y a una placa electrónica que realiza el conteo de las detecciones para luego ser enviadas al computador, y se registran usando el programa Lab-View.

La luz que proviene del láser tiene una potencia de mas de $6,91\mu W$ lo que implica una incidencia sobre los receptores del orden de 10^{14} fotones por segundo. Teniendo en cuenta que los detectores dejan de tener un comportamiento lineal al incidir sobre ellos más de 1 millon de fotones por segundo, y presentan daño cuando estas detecciones supera las 10 millones por segundo. Fue necesario utilizar filtros y polarizadores para atenuar

Figura 3: Imagen que muestra los dos espejos usados para alinear y cambiar la trayectoria del rayo de luz que sale del láser y llega al beam splitter.

en 5 órdenes de magnitud los fotones que inciden por segundo sobre los detectores.

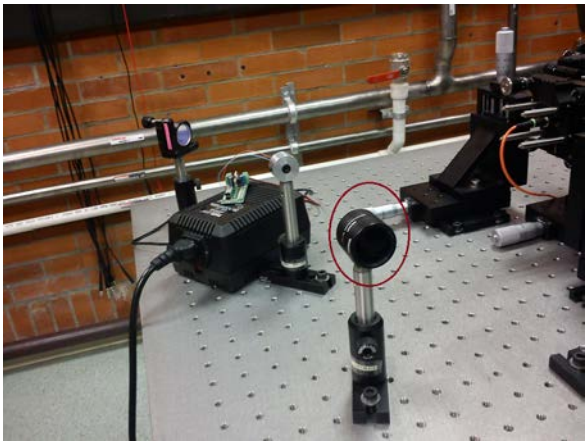

Figura 4: Imagen que muestra los filtros neutros usados para reducucir la intensidad de los fotones incidentes en 5 órdenes de magnitud.

Después de obtener una intensidad del orden de 10^6 fotones por segundo, fue necesario alinear el haz de luz para que incida paralelo a la superficie donde se dispuso el montaje, para lo cual se utilizó las perillas con las que vienen equipados las monturas donde se ubican los espejos, con lo cual es posible alinear el haz de luz variando la inclinación de estos, tanto horizontal como vertical, con el fin de que el haz incida sobre el Beam Splitter. Para que éste se encuentre lo más horizontal posible se hizo uso de dos Iris a una altura de 12,2 cm para que la luz pase por los dos pequeños agujeros que quedan al cerrar dichos dispositivos.

Posteriormente fue necesario ubicar el Beam Splitter en una posición adecuada para que lleguen fotones a los

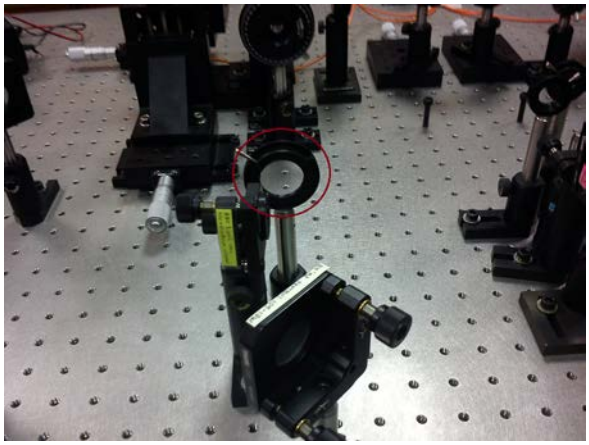

Figura 5: Imagen que muestra uno de los iris usados para cuadrar que el rayo incida paralelo a la mesa donde se realiza el montaje.

dos detectores dejándolo a 2,1mm respecto a la base. Para finalizar el ajuste de la proporción de unos y ceros del experimento, se prenden los detectores y se mueve el ángulo respecto a la vertical de la lámina de onda hasta que la proporción sea casi 50/50 en los dos detectores salvo algunas milésimas; se usó ventana de tiempo de $1\mu s$ y se tomaron los datos.

B. Montaje 2: Fuente de fotones Láser con acrílico rotante

El método de calibración para este montaje fue similar al del montaje anterior, las modificaciones se deben a la parte estructural del experimento. Se colocó, entre la lámina de onda y el último espejo que enfoca, un montaje electrónico compuesto por el motor que hace girar el acrílico, y la base donde se soporta, como el efecto del acrílico genera dispersión de la trayectoria original de los fotones.

Fue necesario hacer uso de un lente que enfocara la luz dispersada ubicado entre el acrílico y la lámina de onda de tal manera que el foco del lente quede lo más cercano posible a la región de incidencia normal de los fotones en el Beam Splitter. Para enfocar aún más el haz de luz, se usa un Pin Hole que permite el paso de un haz de poca sección transversal.

Como se observó una disminución de la intensidad del haz de luz, se retiran los filtros pero se dejan los polarizadores y con ellos, junto con la lámina de onda, se cuadra el número de recepciones por segundo a detecciones del orden de 10^6 fotones por segundo como en el caso de la fuente Laser y se realiza la toma de datos correspondiente.

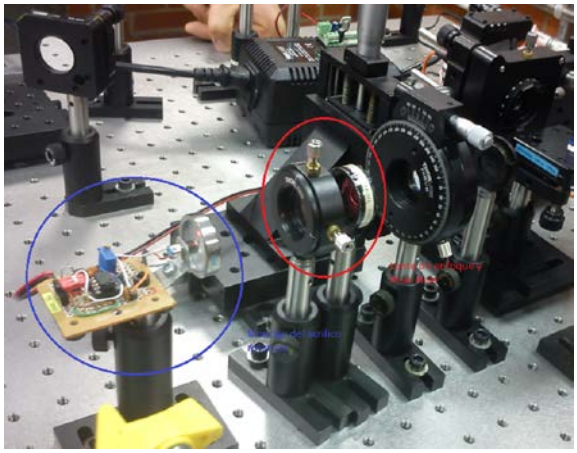

Figura 6: Imagen que muestra las modificaciones realizadas al montaje ubicando el acrílico rotante, el lente de enfoque y el Pin Hole.

C. Montaje 3: Fuente de fotones LED de chorro rojo

Para este montaje se dejó de usar los espejos de enfoque, los filtros de polarización, el lente de enfoque y la fuente de emisión. Se retira el láser y se ubica cerca del Beam Splitter un LED de luz roja de chorro el cual presenta una clara dispersión que debe ser recogida por medio del Pin Hole usado en el montaje anterior. El LED se dispone en un placa acompañada de un montaje electrónico básico para cuidar el dispositivo de un alto voltaje. La manera de calibrar la proporción de unos y ceros es igual que en los montajes anteriores, así que después de lograr esto se procede a tomar los datos.

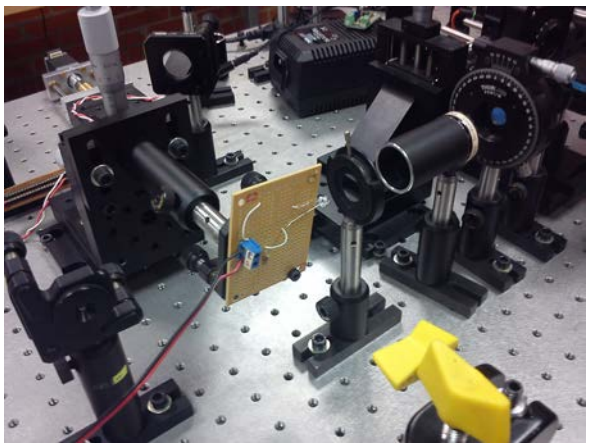

Figura 7: Imagen que muestra las modificaciones para el montaje 3 donde se reemplaza el láser por un Led rojo de chorro como fuente de fotones.

V. RESULTADOS Y ANÁLISIS DE RESULTADOS

A. Pruebas estadísticas

Como se mencionó en el marco teórico, en esta sección se explica las pruebas estadísticas de aleatoriedad que se usaron para analizar los datos obtenidos.

1. Longest Run Ones Test

Con esta prueba se quiere examinar si la secuencia mas larga de unos hallada en bloques de tamaño M de la secuencia total, es consistente con la longitud de la secuencia mas larga de unos que se puede obtener en una secuencia aleatoria. Se realiza la prueba para unos ya que la no aleatoriedad de una secuencia de unos implica no aleatoriedad de una secuencia de ceros.

2. Frequency Block Test

Con esta prueba se determina la frecuencia de unos en un bloque de tamaño M de la secuencia total, se desea que sea aproximadamente M/2 como es de esperarse en una secuencia aleatoria.

3. Runs Test

Con esta prueba se probar el numero total de cadenas en la secuencia, donde una cadena es una ininterrumpida secuencia de idénticos bits. Se quiere determinar cuando el numero de cadenas de unos y zeros de varias longitudes es cercano al que experimenta una secuencia aleatoria.

4. Frequency Test

Con esta prueba se calcula el numero de unos y ceros de la secuencia total. Se desea determinar si el numero de unos y ceros de la secuencia es el mismo como es de esperarse para secuencias aleatorias.

5. Binary Matrix Rank Test

Con esta prueba se revisa la dependencia lineal de cadenas de bits fijas de la secuencia original, el parámetro M que le entra a la prueba nos dice el numero de filas y de columnas de las matrices a las cuales se les va a calcular el rango y luego determinar la independencia de los vectores de este.

6. *Maurer's Universal Statistical Test*

Con esta prueba se desea detectar si es posible realizar una significativa compresión de la frecuencia sin tener perdida de información. Se tiene que una secuencia que se deje comprimir y no se pierda información es considerada no aleatoria.

B. Distribución de probabilidad de las detecciones

Usando Matlab se cargaron los datos de detecciones para la ventana de tiempo de $1\mu s$ comparando la distribución de probabilidad de los datos con las distribuciones discretas de Poisson y Bose-Einstein. Para el laser se muestran los resultados en la figura 8 donde se presentan el numero de detecciones en función de la probabilidad de ocurrencia. Se observa que la distribución de los datos se ajusta igualmente a las distribuciones de Bose-Einstein y Poisson con $\lambda = 0{,}314201$ donde el mean value para B-E es de $0,314201$ y se tiene una varianza de $0,32004$.

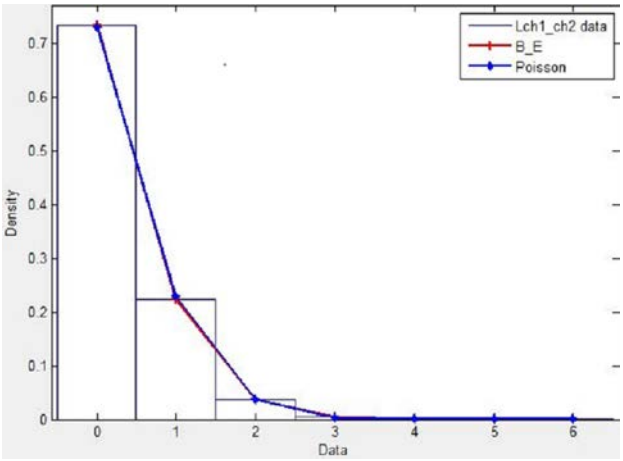

Figura 8: Imagen que muestra la distribución de probabilidad del numero de detecciones para la fuente Laser comparada con una distribución Bose-Einstein y Poisson.

Para el laser con acrílico rotante se tiene que la distribución de probabilidad que mejor se ajusta a los datos es la Bose-Eintein, hay que tener en cuenta que el acrílico genera dispersion de los fotones aumentando el area transversal de estos. En este caso B-E si difiere un poco de la distribución de Poisson para la cual se obtiene un valor de $\lambda = 0,256068$ y para B-E un valor medio de 0,250668 y una varianza de 0,289741. Los resultados se presentan en la figura 9 donde se muestra el numero de detecciones en función de la probabilidad de ocurrencia.

Para la Fuente Led también coinciden las estadísticas de B-E y Poisson aunque la varianzas calculadas para cada distribución difieren mas en este caso que en el caso del Laser, Para la distribución de Poisson se obtuvo un $\lambda = 0,11977$ para Bose-Eintein se tiene un valor medio de

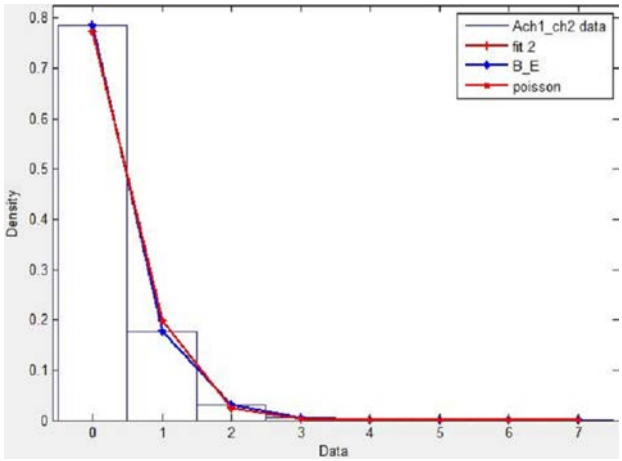

Figura 9: Imagen que muestra la distribución de probabilidad del numero de detecciones para la fuente Laser con acrilico rotante comparada con una distribución Bose-Einstein y Poisson.

0,11977 y una varianza de 0,13645. Los datos se presentan en la figura 10.

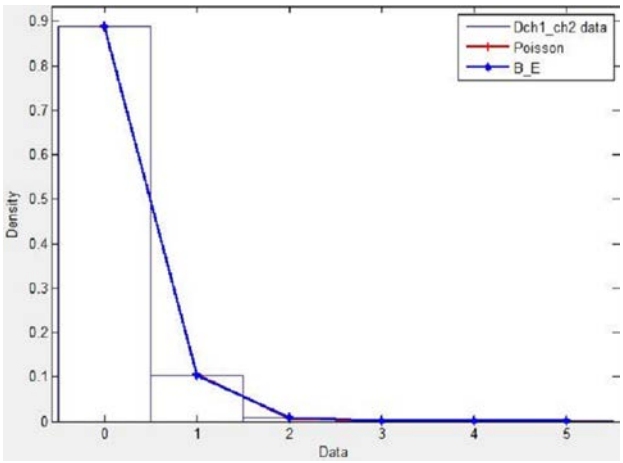

Figura 10: Imagen que muestra la distribución de probabilidad del numero de detecciones para la fuente Led de chorro comparada con una distribución Bose-Einstein y Poisson.

Se puede observar que a mayor dispersión del rayo de fotones la distribución de probabilidad del numero de detecciones tiende a comportarse como una distribución de Bose-Einstein o también conocida como distribución de fotones, la cual describe fuentes de alta dispersión como un bombillo de filamento.

C. Análisis Estadístico de las secuencias.

Los datos que se obtiene de los detectores tiene que ser reducidos a una única secuencia de unos y ceros para ser analizar con las pruebas estadísticas de aleatoriedad, para lo cual fue necesario implementar la función

"$vector - valido$" la cual nos permite armar la secuencia de unos y ceros pedida desechando datos donde se tiene mas de 2 detecciones en la ventana de tiempo de $1\mu s$.

Después de tener las 3 secuencias limpias para las tres fuentes de fotones se les aplicó las pruebas de aleatoriedad descritas al inicio de esta sección. A continuación se muestra la tabla con los datos obtenidos para la fuente laser donde se corren las pruebas de dos formas distintas: primero se le aplica las pruebas a la secuencia total y se obtienen los valores correspondientes de p-value, luego se divide cada secuencia en bloques de 30000 datos y a cada bloque se le aplicaron todas las pruebas, luego se calcula el promedio, los datos se muestran en la tabla de la figura 11.

El criterio para juzgar si una secuencia es aleatoria o no es el p-value de lo que se tiene que si el pi-value es mayor a $0,01$ la secuencia es aleatoria, de manera opuesta si el p-value es menor a $0,01$ la secuencia es no aleatoria.

Se observa que la secuencia pasa todas las pruebas implementadas con un p-value muy alto, la única prueba donde p-value es bajo esta relacionada con la proporción de unos y ceros. Se tiene que el p value da mucho mas alto cuando se le aplica a toda la secuencia que cuando se le aplica a los segmentos y se calcula el promedio.

Intervalos	Universal Statistical	runs_test	long_run_ones	Freq_Blo_tst	Freq_test
	p-value	p-value	p-value	p-value	prop_ceros
1:30000	0,1763	0,1764	5,40E-13	0,8208	49,89%
30000:60000	0,3732	0	5,58E-13	0,6149	48,55%
60000:90000	0,4455	0,1175	5,61E-13	0,0431	49,18%
90000:120000	0,1881	0,2544	5,73E-13	0,7711	49,07%
120000:150000	0,3647	0,6866	5,33E-13	0,1303	50,31%
150000:180000	0,2344	0,6507	5,40E-13	0,5449	50,98%
180000:210000	0,6481	0	5,38E-13	0,1992	51,16%
210000:240000	0,4053	0	5,52E-13	0,1511	51,60%
240000:270000	0,3809	0	5,34E-13	0,0011	51,72%
270000:300000	0,6697	0	4,40E-13	0,85	51,48%
300000:330000	0,9603	0,5232	5,53E-13	0,1435	51,10%
330000:360000	0,1973	0,6981	5,73E-13	0,4096	50,83%
360000:390000	0,0522	0,2484	5,56E-13	0,9616	50,87%
390000:420000	0,5554	0,5322	5,54E-13	0,5942	49,96%
420000:450000	0,3239	0,8294	5,65E-13	0,0711	49,61%
450000:480000	0,9533	0,0472	5,50E-13	0,7344	48,94%
480000:510000	0,164	0,8193	5,54E-13	0,3702	48,91%
510000:537312	0,7577	0,4597	2,39E-13	0,018	48,83%
Promedio	0,436127778	0,33572778	5,28557E-13	0,4127	50,16%
Completo	0,9125	0,9172	0,0313	0,0519	50,17%
Desv. Estándar	0,269346346	0,31195457	7,77169E-14	0,3279575	0,01076064

Figura 11: Tabla que muestra los valores de p-value para la secuencia total que se obtuvo de la fuente Laser como para las particiones de 30000 datos.[1]

La prueba de Binary Test se analiza aparte debido al comportamiento particular de esta prueba. Para el Laser se muestra la gráfica de p-value en función del parámetro M que se le mete a la prueba. Se tiene que la secuencia es aleatoria para valores de M muy grandes, la linea muestra el valor para el cual la secuencia pasa la prueba, esto se observa en la gráfica 12.

Para el acrilico rotante los valores de p-value se muestran en la tabla de la figura 13 se realizó el mismo análisis que para el laser, se divide la secuencia en bloques de 30000 detecciones y se le aplican las pruebas de aleatoriedad, tanto a los bloques como a la secuencia general, se observa que la única prueba que no pasa la secuencia es la Longest Run Ones test a diferencia de la del Laser.

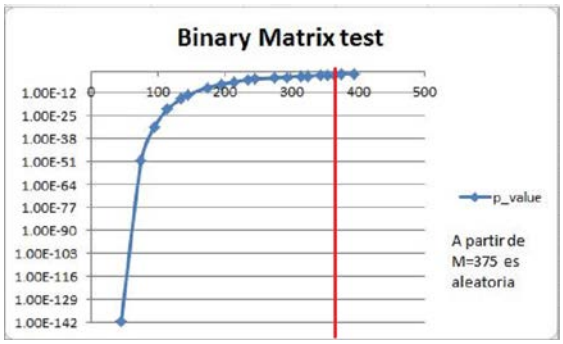

Figura 12: Imagen que muestra la dependencia del M con el p-value para la prueba Binary Matrix test para la secuencia obtenida con la fuente Laser, la linea roja indica el valor del M para el cual la secuencia ya es aleatoria.[1]

Intervalos	Universal Statistical	runs_test	long_run_ones	Freq_Blo_tst	Freq_test
	p-value	p-value	p-value	p-value	prop_ceros
1:30000	0,1768	0,498	0	0,359	48,87%
30000:60000	0,3732	0,2039	0	0,9841	49,50%
60000:90000	0,4455	0,573	5,6266E-13	0,4575	50,10%
90000:120000	0,1881	0,5032	5,6266E-13	0,622	50,96%
120000:150000	0,3647	0,1867	5,6266E-13	0,2375	49,84%
150000:180000	0,2344	0,7235	5,537E-13	0,2219	50,38%
180000:210000	0,6481	0,5943	6,0041E-13	0,2179	50,25%
210000:240000	0,4053	0,5064	5,6499E-13	0,543	49,92%
240000:270000	0,3809	0,7373	6,0041E-13	0,2199	50,30%
270000:300000	0,6697	0,2602	5,6266E-13	0,4487	50,01%
300000:330000	0,9603	0,2664	5,5156E-13	0,2271	50,54%
330000:360000	0,1973	0,7655	2,2637E-13	0,4252	50,06%
Promedio	0,420316667	0,48445	4,45673E-13	0,41365	50,06%
Completo	0,9125	0,8325	0,0013	0,2906	50,06%
Desv. Estándar	0,23571092	0,21021179	2,3063E-13	0,2276921	0,00525837

Figura 13: Tabla que muestra los valores de p-value para la secuencia total que se obtuvo de la fuente Laser con Acrilico rotante como para las particiones de 30000 datos .[1]

En la figura 14 se muestra la dependencia del valor de p-value con el valor del M que entra como parámetro a la prueba de Binary Matrix test también es necesario un valor de M muy grande para que la prueba sea aleatoria.

Para el led de Chorro los datos se muestran en la tabla de la figura 15, esta secuencia tampoco paso la prueba de Longest runs test a diferencia del la fuente Laser, la proporción de ceros y unos estuvo fue mucho mejor que lo que se presento para las otras dos secuencias.

Al igual que para las otras secuencias se presenta en la figura 16 la gráfica de la dependencia del p-value del valor de M que entra como parámetro.

Se obtiene que la única frecuencia que pasa todas las pruebas es la secuencia de unos y ceros del Laser, para las otras dos fuentes se presentó que la prueba

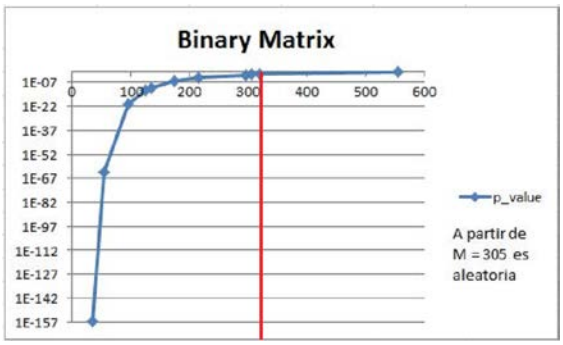

Figura 14: Imagen que muestra la dependencia del M con el p-value para la prueba Binary Matrix test para la secuencia obtenida de la fuente Laser con Acrilico rotante, la linea roja indica el valor del M para el cual la secuencia ya es aleatoria.[1]

Intervalos	Universal Statistical	runs_test	long_run_ones	Freq_Blo_tst	Freq_test
	p-value	p-value	p-value	p-value	prop_ceros
1:30000	0,5996	0,6442	5,67E-13	0,0744	50,00%
30000:60000	0,4831	0,3691	5,40E-13	0,5274	49,78%
60000:90000	0,1794	0,8594	5,67E-13	0,9483	50,17%
90000:120000	0,5047	0,9635	5,6666E-13	0,8009	52,98%
120000:150000	0,9974	0,5365	5,24E-13	0,8652	50,07%
150000:180000	0,7663	0,7663	5,24E-13	0,8234	49,93%
180000:210000	0,1061	0,9414	3,84E-14	0,2929	49,31%
210000:231393	0,4527	0,1269	3,84E-10	0,7777	49,70%
Promedio	0,5111625	0,6509125	4,84333E-11	0,638775	50,24%
Completo	0,9325	0,8391	1,83E-06	0,7962	49,91%
Desv. Estándar	0,289761567	0,29423458	1,35646E-10	0,31105767	0,01138084

Figura 15: Tabla que muestra los valores de p-value para la secuencia total que se obtuvo de la fuente Led de chorro como para las particiones de 30000 datos .[1]

Longest runs ones no obtuvo un p-value mayor a 0,01 como se deseaba, posibles causas de esto radica en la longitud de las secuencias donde se tiene que la secuencia con un mayor numero de datos es la de la fuente Laser y la de menor numero de datos la fuente led de chorro. Se tiene entonces que al tener menos datos también tiene menor p-value en esta prueba, de las figuras 11, 13 y 15 se tiene que a mayor numero de datos validos mayor p-value para la prueba de Longest Run.

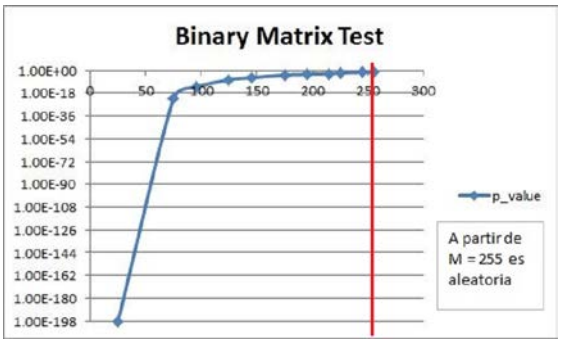

Figura 16: Imagen que muestra la dependencia del M con el p-value para la prueba Binary Matrix test para la secuencia obtenida de la fuente Led de chorro, la linea roja indica el valor del M para el cual la secuencia ya es aleatoria.[1] .[1]

Para las pruebas del tipo Frequency y Binary Matrix la secuencia que se obtuvo de la fuente laser obtuvo un p-value cercano a el valor limite para las Frequency y fue necesario suministrarle a la prueba Binary Matrix un M mayor al usado en las demas secuencias, al observar las 3 tablas donde se presentan los resultados se tiene que al haber mayor diferencia entre la proporción de unos y ceros menor p value se obtendrá en las pruebas del tipo Frequency y se necesitara un mayor M para que la secuencia pase la prueba de Binary Matrix.

En general con las tres fuentes se pueden obtener secuencias aleatorias, en lo que difieren es en la eficiencia con la que se obtiene los datos ya que para el laser se obtiene 532312 datos validos en una toma de detecciones de 4.5 horas, para el laser con acrílico 360000 en el mismo intervalo de tiempo en cambio para la fuente led fue necesario realizar una toma de datos por 5 horas para obtener tan solo 231393 datos validos.

En consecuencia la fuente mas eficiente para obtener uns secuencia aleatoria cuantica es el laser, pero en general se puede usar cualquier fuente que emita fotones para realizar el proyecto el problema radica en el tiempo de toma de datos que implica usar un tipo de fuente que genere gran dispersion como para este caso el Led o un bombillo corriente.

La fuente no es la que garantiza si la secuencia obtenida es aleatorio o pseudoaleatoria, solo permite que la toma de datos sea mas o menos eficiente; el fenómeno cuántico que se presenta en el montaje el cual ocurre cuando el fotón llega al beam splitter y su función de estado colapsa a el estado transmitido o reflejado del que se hablo en el marco teórico, es el que presenta el comportamiento no determinista del montaje, es en ese instante donde radica la aleatoriedad de la secuencia obtenida, donde si se logra de manera muy precisa que la probabilidad de que el fotón incidente se refleje o se transmita sea la misma es decir 1/2, se obtiene detecciones en los dos dispositivos de manera aleatoria.

VI. CONCLUSIONES

- A mayor longitud de la secuencia aleatoria se puede obtener un mayor p-value.
- De las pruebas usadas, Binary Matrix y Longest Runs ones son las que tiene el criterio de aleatoriedad mas fuerte.
- Las 3 secuencias pasaron casi todas las pruebas de aleatoriedad, así que con diferentes fuentes que emitan fotones se puede obtener una secuencia aleatoria.

- La fuente usada en la obtención de la secuencia, no influye en el fenómeno cuántico del montaje, la fuente solo permite hacer mas o menos eficiente la toma de datos
- El comportamiento cuántico que experimenta el fotón cuando incide en el Beam Splitter de polarización es el que genera la aleatoriedad de los datos que se obtiene de las detecciones.
- Si se cuadra de manera precisa que el fotón tenga la misma probabilidad de ser transmitido o Reflejado en el Beam Splitter de polarización, se puede obtener la secuencia aleatoria requerida sin importar el tipo de fuente de emisión usada.

VII. REFERENCIAS

1 Bronner, P., Strunz, A., Silberhorn, C. & Meyn, J.P.(2009). Demonstrating quantum random with single photons. European Journal of Physics, 30, (5), 1-13. Recuperado el 27 de enero de 2012 de iopscience.org

2 Rukhin, A., Soto, J., Nechvatal, J. & others. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Recuperado el 27 de enero de 2012 de csrc.nist.gov

3 Uchida, A., Amano, K., Inoue, M. & others. Fast physical random bit generation with chaotic semiconductor lasers. Recuperado el 27 de enero de 2012 de nature.com.

4 Probando generadores de números aleatorios. Recuperado el 6 de febrero de 2012 de ing.ula.ve

5 Generador de números aleatorios. Recuperado el 6 de febrero de 2012 de multilingualarchive.com

6 Óptica cuántica. Recuperado el 6 de febrero de 2012 de citedef.gob.ar