UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Un generador cuántico de números al azar: de un PBS a etiquetas temporales.

Tesis

Que para obtener el título de:
Físico

Presenta:
Aldo Camilo Martínez Becerril.

Director de tesis:
Dr. Jorge Gustavo Hirsch Ganievich.

Ciudad Universitaria, CDMX, agosto de 2017

Datos del jurado.

1-Datos del alumno.
Martínez
Becerril
Aldo Camilo
Número de cuenta 310139232
mbac@ciencias.unam.mx

2- Datos del tutor.
Dr.
Jorge Gustavo
Hirsch
Ganievich

3-Datos del sinodal 1.
Dr.
Oleg
Kolokoltsev

4-Datos del sinodal 2.
Dr.
Ricardo
Méndez
Fragoso

5-Datos del sinodal 3.
Dr.
Pedro Antonio
Quinto
Su

6-Datos del sinodal 4.
Dra.
Andrea
Valdés
Hernández

7-Datos del trabajo escrito.
Un generador cuántico de números al azar: de un PBS a etiquetas temporales.
60 páginas
2017.

Resumen.

Uno de los grandes avances en la física del siglo pasado lo constituye el reconocimiento de que, salvo algunas excepciones, el resultado de una medición en sistemas cuánticos individuales es un evento aleatorio [1]. En [2] se analizan cadenas binarias aleatorias obtenidas de dos grupos de fuentes distintas (un proceso óptico-cuántico y fuentes pseudo-aleatorias). Es notorio el resultado de que las cadenas obtenidas por el grupo de Óptica Cuántica (IQOQI) de Viena no pasan la prueba de Normalidad de Borel, indicando la presencia de patrones, lo que es contrario a lo esperado de una fuente cuántica.

En este trabajo de tesis de licenciatura realicé un experimento de generación de números al azar usando un divisor de haz polarizante, al estilo de los reportados en [2, 3]. La pregunta planteada es ¿por qué un generador cuántico de números al azar presenta patrones indicando carencia de azar? Lo que aprendimos de mi trabajo es que los detectores de fotones individuales introducen sesgos alterando la calidad de las cadenas. Fue necesario implementar otros esquemas de generación, basados en tiempos de llegada y etiquetas temporales, que sean más robustos.

Realicé un montaje experimental para generar cadenas binarias al azar en el laboratorio de Óptica Cuántica del Instituto de Ciencias Nucleares de la UNAM. El experimento consistió de un láser atenuado, la preparación de los fotones en el estado diagonal de polarización, un divisor de haz polarizante y la detección de los fotones en dos fotodiodos de avalancha. Fue necesario caracterizar la respuesta del sistema para implementar un sistema de retroalimentación, programado en LabView, de forma que los dos posibles resultados de la medición sean equiprobables a lo largo de toda la medición.

El análisis de datos consistió en generar cadenas binarias mediante 3 métodos diferentes. El primero de ellos es la asignación binaria a las salidas del divisor de haz al estilo de los generadores reportados en [2, 3], el segundo se basa en la distribución de tiempos de llegada y se detalla en [4] y por último uno basado en la etiqueta temporal de los eventos [5].

Para certificar la aleatoriedad de las cadenas binarias utilicé las pruebas de Normalidad de Borel [2, 4] y la batería del NIST [6] cuando fuese necesaria. Los resultados del experimento contribuyen a entender los retos tecnológicos de estos esquemas de generación para su implementación en un dispositivo de uso práctico.

Índice general

Capítulo 1

Introducción.

Ningún algoritmo puede generar verdadero azar. Si queremos un número que realmente lo sea, necesitamos extraerlo de un proceso físico cuya naturaleza sea aleatoria como lo son mediciones en sistemas cuánticos individuales. Contradictoriamente, se ha reportado en [2] que un generador cuántico de números al azar no pasa la prueba de Normalidad de Borel, lo cual quiere decir que no produce números aleatorios. ¿Cuál es la explicación de este resultado negativo? Esa es la pregunta que dio inicio a esta tesis. Los siguientes párrafos comentan en torno a las proposiciones que acabo de mencionar.

Motivación.

La Mecánica Cuántica es un marco formal dentro del cual podemos hacer predicciones para ciertos sistemas físicos. Uno de los hallazgos más importantes dentro de esta teoría física, que le imprime un sello distintivo respecto a la mecánica clásica, es que el resultado de una medición de un sistema cuántico individual es un proceso auténticamente aleatorio, nadie puede predecir con certeza cuál será el resultado [1].

Diversos grupos de investigación han dedicado esfuerzos a desarrollar generadores de números aleatorios utilizando diferentes tipos de sistemas cuánticos (por ejemplo decaimiento nuclear, iones atrapados). Gran parte de esos esquemas caen en el dominio de la Óptica Cuántica, en el apéndice D hago un resumen de varios de estos trabajos.

En [2] se hace un estudio para distinguir el sello de azar de los fenómenos cuánticos. Los autores utilizan diversas fuentes de números aleatorios, dos de las cuales son un proceso cuántico, y someten sus cadenas obtenidas a varias pruebas para determinar si son compatibles con la hipótesis de aleatoriedad. Sus resultados son positivos excepto por la prueba de Normalidad de Borel, donde hay fallas del generador basado en fotones incidentes en un divisor de haz polarizante, experimento realizado por el grupo de Óptica Cuántica de Viena. ¿Por qué se obtuvo ese resultado si esas cadenas provienen de un proceso realmente aleatorio?

Con el objetivo de determinar la razón del resultado negativo de [2], realicé un experimento para generar cadenas binarias de números al azar utilizando un divisor de haz polarizante (PBS por sus siglas en inglés). Los resultados obtenidos muestran los desafíos presentes en cualquier generador de números al azar basado en el esquema de un PBS, mismo que se describe en el capítulo 4. En el camino he extendido mi estudio para superar las dificultades encontradas. La descripción del experimento, los métodos de generación de las cadenas y su análisis son el contenido de este trabajo de tesis.

Antes de describir lo que he hecho, conviene poner un contexto del campo de generación cuántica de números al azar. Uno de los debates más famosos de la Mecánica Cuántica es el que protagonizaron Einstein y Bohr en torno al enredamiento cuántico. El tema es sutil y susceptible de desacuerdos. En este espacio, baste decir que el debate ha extendido su ring a los laboratorios a través de la confirmación experimental de las desigualdades de Bell, que establecen un criterio para descartar la posibilidad de describir ciertas observaciones con teoría de variables ocultas locales.

Uno de los requerimientos de este tipo de experimentos es un generador de números al azar de muy buena calidad, que tenga una tasa de producción alta de bits, y que sea robusto. Muy bien, se podría utilizar cualquier software de cálculo numérico como Python, Mathematica, Maple, Matlab, etc. ¿Por qué no? El asunto con esta propuesta es que los números generados por cualquier software no son realmente aleatorios, de hecho se les cataloga como números pseudo-aleatorios. Los experimentos de desigualdades de Bell han sido reportados en [7–10]. Por ahora comentemos sobre números al azar.

Números pseudo-aleatorios.

El software para generar números aleatorios de las computadoras actuales se basa en el siguiente esquema [5]: un valor inicial, conocido como semilla (que puede provenir del movimiento del mouse por parte del usuario por ejemplo), se da como entrada a un algoritmo que lo transforma en un número al azar. Este algoritmo es una serie de pasos reproducible y determinista, así que cualquier otra persona con conocimiento del algoritmo y de la semilla puede deducir el resultado.

Otros generadores clásicos de números aleatorios.

Existen otras fuentes de números al azar basadas en un fenómeno tremendamente díficil de predecir, pero que es clásico (en el sentido de que su estudio cae dentro de la física clásica). Un ejemplo de esos procesos es el ruido atmosférico [11]. Estas fuentes se fundamentan en la dificultad de determinar con precisión las variables que afectan al sistema en cuestión, en caso de que las conociéramos, podríamos predecir la evolución del sistema. En la práctica, no es factible predecir el resultado.

Entonces ¿qué fenómeno es auténticamente aleatorio? La respuesta la encontramos en la Mecánica Cuántica. Dentro de este marco formal, los físicos podemos calcular probabilidades de obtener, a través de un proceso de medición, el resultado de alguna observable de interés. Si repetimos muchas veces un mismo experimento, obtendremos esa distribución de resultados. ¿Podemos predecir el resultado de una medición en un sistema cuántico individual?

Uno de los hallazgos más importantes de la teoría cuántica es que la respuesta a la última pregunta, en general, es "no" [1]. El resultado de una medición de un solo sistema cuántico es un evento realmente aleatorio. La siguiente sección puntualiza a lo que me refiero.

Medición individual en una superposición de estados propios.

Sea $\hat{A}$ un operador asociado a una observable y $\{|\phi_i\rangle\}$ una base ortonormal de estados propios de $\hat{A}$. Un sistema cuántico puede estar en una superposición coherente de esta base: $|\psi\rangle = \sum_i c_i |\phi_i\rangle$. El coeficiente c_k corresponde a la amplitud de probabilidad de encontrar al sistema en el estado $|\phi_k\rangle$. Podemos calcular la distribución de resultados y obtenerla experimentalmente, repitiendo el mismo experimento muchas veces, pero es imposible predecir el resultado de una medición individual (ignorando el caso en que el sistema se prepara en un determinado estado propio de $\hat{A}$).

Hay otros casos, que a continuación menciono, donde nuestro conocimiento de un sistema cuántico está limitado, aunque no necesariamente haya una componente de aleatoriedad.

Mezclas.

Puede ser que un sistema cuántico se encuentre en un estado específico, pero no tengamos información de cuál es. En ese caso, describimos al sistema como una mezcla de estados. Al hacer una medición podemos determinar el estado en el que se encontraba el sistema y el resultado lo veremos como al azar aunque se debe a ignorancia.

Desigualdades de Heisenberg.

Las desigualdades de Heisenberg establecen una cota mínima en la dispersión del valor de expectación de dos observables cuyo conmutador sea distinto de cero. Este resultado tiene sentido si hay muchas mediciones en un ensamble de partículas.

Desigualdades de Bell.

La violación de las desigualdades de Bell garantiza que no existe un pre-acuerdo, entre partículas correlacionadas, de los resultados de ciertas mediciones. Este resultado puede ser utilizado para generar una lista de números al azar certificada [12].

Además de las cuestiones en torno a los fundamentos de la Mecánica Cuántica, ¿son de interés los números aleatorios? La respuesta la debemos buscar en el abanico de aplicaciones en donde se necesitan. Podemos nombrar las simulaciones computacionales, particularmente el método Monte-Carlo donde se requiere un muestreo sin sesgos, en la realización de encuestas (donde igualmente se requiere un buen muestreo), en

juegos de suerte en línea. Sin duda, la aplicación que sobresale en la generación cuántica de números al azar es la distribución cuántica de claves (QKD por sus siglas en inglés).

Distribución cuántica de claves.

Para poder enviar un mensaje entre dos interlocutores de manera privada y segura es suficiente que ambos posean una misma clave secreta y que se manden mensajes encriptados bajo esta llave común. De esa manera, sólo ellos podrán decriptar los mensajes logrando una comunicación privada y segura. Sin embargo, existe el riesgo de que alguien más logre obtener la clave y tenga acceso al canal de comunicación.

Entonces el punto clave para tener una comunicación privada es distribuir una clave entre dos interlocutores de manera segura. La idea de QKD es aprovechar los fenómenos cuánticos para lograr este propósito. QKD no está exenta de que alguien espíe la llave, en cuyo caso el esquema mostrará los intentos de hackeo y la llave se desechará [13].

Una comunicación segura tiene relevancia en asuntos de política y en eventos que contengan información confidencial. Se han utilizado esquemas de QKD en las elecciones de Suiza y en la copa del mundo de la FIFA [13]. En un terreno cada vez más presente, como lo es el de las transacciones electrónicas a través de internet, también es importante una comunicación segura.

Dadas estas aplicaciones, es entendible que los esquemas de QKD quieran ser llevados a la práctica con dispositivos comerciales. Como ocurre con la tecnología, generalmente existe un periodo largo de mejora y desarrollo antes de que los nuevos dispositivos sean ampliamente utilizados. QKD no está exenta de este proceso, algunos requerimientos que se tienen son: detectores de fotones, canales ópticos de largo alcance (fibras ópticas, satélites y propagación en el aire) que no degraden el contenido de información y generadores de números al azar auténticos [13].

La generación de números al azar también es un tema que está en desarrollo y que tiene sus propios retos [5]: lograr tasas de generación de números al azar de Gbps, tener métodos robustos que sean sencillos de implementar y que puedan ser integrados en otros dispositivos como computadoras o teléfonos celulares.

Como cierre de esta introducción, puedo decir que la generación cuántica de números aleatorios es un tema presente desde cuestiones fundamentales de la teoría Cuántica, hasta asuntos, cada vez más frecuentes en la vida cotidiana, como el comercio electrónico y la seguridad criptográfica.

Inicialmente, mi trabajo de tesis estuvo encaminado hacia la parte fundamental de entender por qué una fuente cuántica produce cadenas que no son aleatorias ya que presentan patrones como se reporta en [2]. Con el andar del proyecto, he explorado esquemas más robustos de generación y logré obtener resultados que pueden merecer ser considerados para un prototipo de uso práctico.

Capítulo 2

Pruebas: Normalidad de Borel y NIST.

Las pruebas de azar son pruebas estadísticas y requieren evaluar muchas cadenas largas, de longitud del orden de millones de bits, de un generador de números para determinar si es aleatorio o no lo es. En esta tesis, la principal prueba de aleatoriedad es la de normalidad de Borel que tiene la virtud de estar enmarcada dentro de un formalismo matemático presentado en [14]. Las pruebas de NIST, quizá la batería más socorrida a la hora de certificar aleatoriedad, ofrece 15 pruebas que detectan un espectro amplio de comportamientos incompatibles con la hipótesis de que una cadena es aleatoria.

2.1. Normalidad de Borel.

El criterio de normalidad de Borel fue creado por el matemático francés Émile Borel para sucesiones infinitas. Esta prueba ha demostrado ser útil y toda sucesión realmente aleatoria la debe pasar. En [14] se extiende formalmente una condición tipo Borel a casi todas las cadenas finitas, que son a las que tenemos acceso en la práctica. Se dice que una cadena es Borel normal si pasa la prueba de Normalidad de Borel.

Para que una cadena binaria sea Borel normal la frecuencia de aparición de cada bloque de m bits debe ser uniforme, por tanto tiene que ser cercana a $\frac{1}{2^m}$ [2, 4]. Formalmente el criterio se establece de la siguiente forma.

Sea $B_m = \{0,1\}^m$ todas las cadenas de longitud m ($m > 1$) y x una cadena de longitud $|x|$. Sea $N_i^m(x)$ el número de apariciones de la subcadena binaria i-ésima, de longitud m, en x. Denotemos por $|x|_m$ la longitud de la cadena x bajo el alfabeto B_m (e.g. $|x|_1 = |x|$). La cadena x es Borel normal si, para todo natural $1 \leq m \leq \mathsf{log_2}(\mathsf{log_2}\,|\mathsf{x}|)$, se cumple que

$$\left| \frac{N_i^m(x)}{|x|_m} - 2^{-m} \right| \leq \sqrt{\frac{\mathsf{log_2}\,|\mathsf{x}|}{|x|}}, \tag{2.1}$$

para cada $1 \leq i \leq 2^m$. Como ejemplo de la forma en que se hace el conteo de bloques de m bits consideremos la cadena $x = 0010101110 = y_1y_3y_3y_4y_3$ con $\{y_1, y_2, y_3, y_4\} = \{00, 01, 10, 11\}$. Para $m = 1$ se tiene $|x| = 10$, $N_1^1 = N_2^1 = 5$. Para $m = 2$, $|x|_2 = 5$, $N_1^2 = 1$, $N_2^2 = 0$, $N_3^2 = 3$, $N_4^2 = 1$.

La longitud de las cadenas que vamos a generar es de 4.3×10^9 bits por lo que $\mathsf{log_2}(\mathsf{log_2}(\mathsf{4.3\times10^9})) = \mathsf{5.00}$. Para $m = 1$ se van a buscar los bits del conjunto $\{0, 1\}$. Para $m = 2$ se contarán los bloques del conjunto $\{00, 01, 10, 11\}$. A $m = 3$ le corresponde el conjunto $\{000, 001, 010, 100, 110, 011, 111\}$ y lo análogo para $m = 4$ y 5.

La cota de Normalidad de Borel es $\sqrt{\frac{\mathsf{log_2(4.3\times10^9))}}{\mathsf{4.3\times10^9}}} = 8.62685 \times 10^{-5}$. Cada una de nuestras cadenas será Borel normal si, para todo natural $1 \leq m \leq 5$, se cumple

$$\left| \frac{N_i^m(x)}{|x|_m} - \frac{1}{2^m} \right| \leq 8.62685 \times 10^{-5}. \tag{2.2}$$

2.2. Análisis de las cadenas con las pruebas de NIST.

El NIST (por sus siglas de National Institute of Standards and Technology) es un laboratorio de cantidades físicas que se encuentra en Estados Unidos. Realiza investigación en diversos temas permeando el

ámbito tecnológico, el establecimiento de patrones y el desarrollo de ciencia básica. NIST desarrolló una batería de 15 pruebas, que detectan propiedades incompatibles con la hipótesis de que una cadena binaria sea aleatoria. Si una cadena falla las pruebas de NIST, entonces no es aleatoria [6].

En el manual de NIST se dan 3 característcas esenciales que un generador de números al azar y sus cadenas producidas deben tener:

- Uniformidad. El bit 0 y 1 deben tener la misma frecuencias de aparición.

- Escalamiento. Si una cadena pasa una prueba de aleatoriedad, entonces cualquier subcadena también la debe pasar (respetando los tamaños mínimos impuestos por las pruebas por supuesto).

- Consistencia. Los resultados de un generador de números al azar (ya sea una fuente física o de software) deben mantenerse, independientemente de los parámetros de entrada. Para una fuente de números pseudo-aleatorios se deben utilizar diversas semillas y en el de una fuente física se deben probar distintas cadenas.

Las pruebas implementadas por NIST necesitan estadística para dar un resultado. Dada una prueba de aleatoriedad, existe la probabilidad α de que la cadena producida por una fuente aleatoria falle la prueba. También existe la probabilidad β de que una fuente no-aleatoria produzca una cadena que pase la prueba.

Idealmente estos casos deben ser muy raros. Típicamente, se escoge $\alpha \in [0.001, 0.01]$. El valor de β no tiene un valor fijo y su tratamiento es más complicado. Las pruebas de NIST usan α como un parámetro de entrada. En todos los análisis que hice, utilicé $\alpha = 0.01$ indicando que se espera que una cadena en cien falle las pruebas.

En lo que sigue doy una descripción de lo que cada prueba hace en general y denotaré con $|x|$ la longitud de la cadena x. Los detalles técnicos se pueden encontrar en [6].

1. Prueba de frecuencia.

Mide que la cantidad de los bits 0 y 1 de la cadena sea aproximadamente la misma.

2. Prueba de frecuencia en un bloque.

Considera bloques de M bits dentro de la cadena . Mide la cantidad de 0 y 1 en el bloque y determina si es lo suficientemente cercana a $\frac{M}{2}$. Yo utilicé $M = 128$.

3. Prueba de secuencias de un mismo bit.

Determina la longitud de las secuencias de un mismo bit. Nos da información de la rapidez de la oscilación de 0 a 1 y viceversa. Además detecta el comportamiento no deseado de tener secuencias muy largas.

4. Secuencia más larga de "1" en bloques de M bits.

Consiste en encontrar la secuencia más larga de "1"(que da información sobre el bloque más largo de "0") dentro de un bloque de M bits. Compara si la longitud de la secuencia es la esperada respecto a la longitud de M.

5. Prueba del rango de la matriz binaria.

Consiste en generar matrices utilizando los bits de la cadena binaria. Si la cadena es aleatoria, las filas y columnas deben ser linealmente independientes. La prueba determina la independencia lineal mediante el rango de la matriz, que debe ser igual a la dimensión de la matriz en caso de independencia lineal.

6. Prueba espectral (transformada de Fourier discreta).

Calcula la transformada de Fourier discreta de la cadena para detectar algún patrón periódico y determina si hay muchas componentes de Fourier grandes.

Sea x_k el k-ésimo bit de la cadena ($1 \leq k \leq |x|$) con valores de ± 1 (que se hace restando un 1 al bit 0), se calcula la transformada de Fourier discreta de estos datos:

$$f_j = \sum_{k=1}^{|x|} x_k e^{2\pi(k-1)j/|x|}. \tag{2.3}$$

Bajo la hipótesis de aleatoriedad, el 95 % del módulo de estos f_j deben ser menores a $\sqrt{ln\left(\frac{1}{0.005}\right)|x|}$.

7. La prueba de similitud con una plantilla sin hacer traslapes.

La idea es dar una plantilla de m bits, utilicé $m = 9$, y contar su número de apariciones en la cadena. En cada iteración, el programa realiza la búsqueda del patrón en los m bits consecutivos, respecto al bit actual. Si el patrón no se encuentra, se repite el proceso con el siguiente bit. Si se encuentra, la búsqueda continúa después de la plantilla encontrada.

Una cadena aleatoria no debería tener muchas ocurrencias. La prueba sirve para identificar patrones recurrentes, no necesariamente periódicos, en la cadena.

8. La prueba de similitud con una plantilla permitiendo traslapes.

La única diferencia con el anterior es que si el patrón se encuentra, entonces la búsqueda continúa en el bit siguiente.

9. La prueba de estadística universal de Maurer.

La idea es ver qué tanto se puede comprimir la cadena sin perder información. La compresión de la cadena busca patrones y cuenta el número de bits entre ellos, si son pocos se puede comprimir conservando información. En caso contrario, la compresión no se puede realizar. Una cadena aleatoria no se puede comprimir porque no presenta patrones.

10. La prueba de complejidad lineal.

Esta prueba está relacionada con la dificultad y tiempo requerido para reproducir, mediante un algoritmo, la cadena que se está probando.

Se utiliza un LFSR (Linear Feedback Shift Register) que es una estructura con L elementos (utilicé $L = 500$), cada uno con una entrada y una salida.

Inicialmente el estado del LFSR es $(\epsilon_{L-1}, ..., \epsilon_1, \epsilon_0)$ que evoluciona en un estado final $(\epsilon_L, \epsilon_{L+1}, ...)$ de acuerdo a la ecuación siguiente:

$$\epsilon_j = \left(\sum_{i=1}^{L} c_i \epsilon_{j-i} \right) mod\ 2. \tag{2.4}$$

Donde c_i, $i \in 1 \leq i \leq L$, son coeficientes. Se dice que un LFSR genera una cadena binaria si la cadena es la salida del LFSR para algún estado inicial.

En esta prueba se encuentra la longitud del LFSR que genere a la cadena que se está analizando. A una cadena no aleatoria le corresponde un LFSR corto.

11. Serial.

Cuenta el número de apariciones, permitiendo traslape, de un patrón de m bits (utilicé $m = 16$). Una cadena aleatoria debe tener la misma frecuencia de cualquiera de los 2^m bloques de m bits. Para $m = 1$ se reduce a la prueba de frecuencia de monobits.

Esta prueba es similar a Normalidad de Borel, una distinción entre ambas, es que la de Serial permite traslapes mientras que Normalidad de Borel no.

12. Entropía aproximada.

Determina la frecuencia, permitiendo traslape, de subcadenas de m y de $m + 1$ bits. Después compara esas frecuencias y las compara con lo que se espera para una cadena aleatoria.

13. Sumas cumulantes (Cusum).

En esta prueba se considera el caminante aleatorio asociado a las sumas cumulantes de la cadena binaria. El indicador de la prueba es la longitud del desplazamiento máximo del caminante aleatorio respecto a 0.

El bit i-ésimo de la cadena binaria x se puede codificar en los valores $X_i = \pm 1$, mediante $X_i = 2\epsilon - 1$. Las sumas cumulantes se calculan con la siguiente ecuación si se empieza con -1:

$$S_k = S_{k-1} + X_k; \tag{2.5}$$

Si el primer dígito es 1, la ecuación es:

$$S_k = S_{k-1} + X_{|x|-k+1}; \tag{2.6}$$

El indicador utilizado para evaluar la prueba es $max\{|S_k|$ con $1 \leq k \leq$ longitud de la cadena $\}$. Para una cadena aleatoria, este valor debe ser chico.

14. Excursiones aleatorias.

Considera la caminata aleatoria asociada a las sumas cumulantes de la cadena. Se fija en los ciclos (conjunto de pasos unitarios que inician y terminan en cero) y ve si hay posiciones sobre o sub-visitadas por el caminante.

15. Variante de Excursiones aleatorias.

Considera la caminata aleatoria asociada a las sumas cumulantes cadena. Mide la cantidad de veces que un sitio es visitado en toda la cadena, no sólo en ciclos.

Interpretación de los resultados de la prueba de NIST.

Los resultados de la batería del NIST se pueden presentar en dos estadísticas independientes. Una de ellas es obtener la distribución de valores P en el intervalo $[0, 1]$ y la otra es la proporción de cadenas que pasan cada prueba. Yo usé el último método.

Proporción de cadenas que pasan el test.

Sea m el número de cadenas analizadas y n el número de cadenas que pasan la prueba. La proporción de cadenas que pasan el test es $\frac{n}{m}$. El rango de aceptación, que indica el intervalo aprobatorio de cada prueba, es $\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}$ con $\hat{p} = 1 - \alpha$ [6].

En mis análisis con la batería de NIST me basé en la proporción de cadenas aprobatorias para analizar los resultados. Utilicé $\alpha = 0.01$ esperando que una cadena en cien falle las pruebas.

Capítulo 3

Experimento: un mecanismo de retroalimentación.

El trabajo experimental lo realicé en el laboratrio de Óptica Cuántica del Instituto de Ciencias Nucleares (ICN) de la UNAM. Mi experimento se basa en el control de la polarización lineal de fotones incidentes en un divisor de haz polarizante (PBS por sus siglas en inglés). Necesito preparar fotones en el estado $|\psi\rangle = \frac{|H\rangle+e^{i\phi}|V\rangle}{\sqrt{2}}$, para que cada polarización ($|H\rangle$ o $|V\rangle$) tenga la misma probabilidad de ser detectada. La detección emplea un PBS, que refleja a los fotones con polarización $|V\rangle$ y transmite a la componente $|H\rangle$.

La idea es mantener al sistema cuidadosamente balanceado a lo largo de toda la medición y tomar datos suficientes para generar cadenas de 4.3×10^9 bits. Para esa longitud, la cota de Normalidad de Borel es de 8.6×10^{-5}, este valor es la precisión que debo lograr en el experimento, es decir, si $C_{1(2)}$ son las cuentas en el canal 1(2), requiero que $|C_1 - C_2| \leq 8.6 \times 10^{-5}$.

El experimento tiene dos fases. En la primera implementé el sistema con un láser sin atenuar y utilicé potenciómetros ópticos. En la segunda atenué el láser y realicé los cambios requeridos.

3.1. Fase 1: potenciómetros.

Arreglo experimental.

El esquema experimental se muestra en la Figura 3.1. Un diodo láser, linealmente polarizado, emite a una longitud de onda $\lambda = 405$ nm. Dos espejos reflejan el haz a la altura de 2 microbloques y lo orientan hacia una placa de media onda motorizada, donde se prepara a los fotones en el estado $\frac{|H\rangle+e^{i\phi}|V\rangle}{\sqrt{2}}$. Los fotones inciden en un PBS con dos posibles resultados, cada uno de ellos con probabilidad 0.5 de ocurrir. En cada salida del PBS coloqué un polarizador, orientado de forma que maximice la potencia a su salida, y un potenciómetro cuya medición se manda a una computadora a través de LabView. En la Figura 3.2 se aprecia el montaje experimental.

Nuestro experimento se basa en el control de la polarización de fotones. Si las fluctuaciones en la polarización del láser son lo suficientemente grandes, pueden impedir que logremos balancear al sistema con la precisión requerida. Lo primero que hice fue determinar si la polarización del láser es lineal y si era necesario un polarizador para mejorarla.

La polarización del láser es lineal.

Luz linealmente polarizada sigue la ley de Malus. Esta ley establece la variación en la intensidad de la luz (I), después de un polarizador, como función del ángulo ω entre el eje del polarizador y la polarización de la luz [15]:

$$I(\omega) = I_{max} cos^2(\omega). \tag{3.1}$$

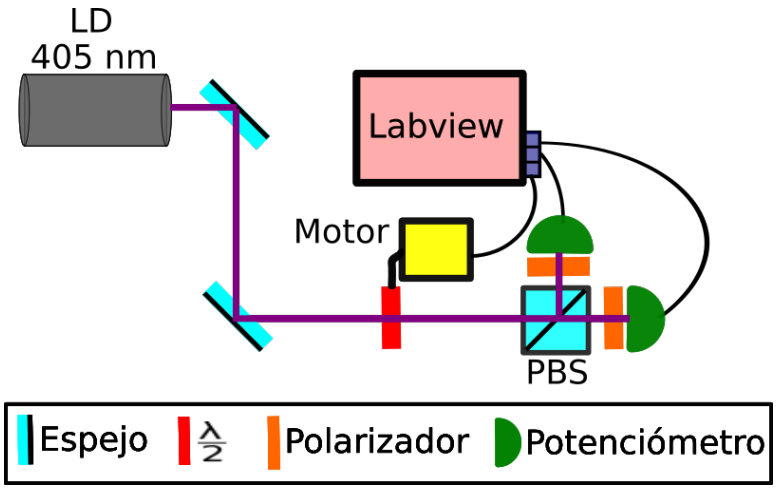


Figura 3.1: Esquema del experimento. Nuestra fuente es un láser diodo (LD) de 405 nm con polarización vertical que es rotada por una lámina de media onda motorizada que prepara a los fotones en el estado de polarización $\frac{H+e^{i\phi}V}{\sqrt{2}}$. La probabilidad de que un fotón de este ensamble se transmita o se refleje al incidir en un PBS es 0.5 en cada caso. En cada brazo del PBS coloqué un sensor óptico para medir la potencia de salida.

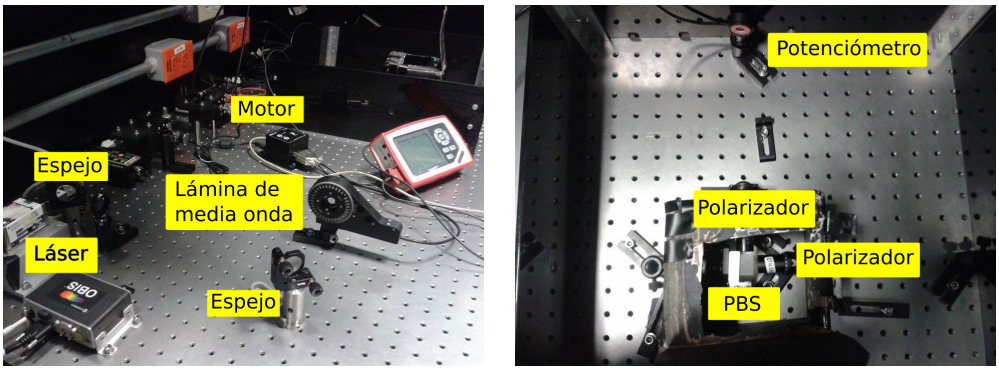


Figura 3.2: Fotografías del arreglo experimental en el laboratorio de Óptica Cuántica del Instituto de Ciencias Nucleares (ICN) de la UNAM. A la izquierda se muestra el láser diodo, los dos espejos que orientan al haz, la lámina de media onda, el motor y la consola del sensor óptico. A la derecha se ve el PBS seguido de polarizadores y un sensor óptico.

Para verificar la polarización lineal, utilicé la lámina de media onda (que rotaba en cada iteración) y un polarizador posterior fijo. Realicé un muestreo del intervalo $[0, 360°]$ en pasos de 6°, tomando 20 muestras en cada ángulo.

Dado que una rotación de un ángulo θ de la placa de media onda corresponde a un giro de 2θ en polarización [15], se espera un comportamiento de la forma $I(\theta) = I_0 cos^2(2\theta + \gamma)$. Analicé la ley de Malus directamente del láser y después de colocar un polarizador, entre el láser y la placa de media onda, para ver si hay una mejora considerable. En ambos casos, los datos varían armónicamente con un buen ajuste numérico que se muestra en linea continua en la gráfica 3.3.

La visibilidad para el láser es

$$\begin{aligned} V &= \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \\ &= 0.996 \pm 0.03\,\%. \end{aligned} \tag{3.2}$$

Después de poner un polarizador es

$$\begin{aligned} V &= \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \\ &= 0.999 \pm 0.007\,\%. \end{aligned} \tag{3.3}$$

La polarización del láser es suficientemente buena y no se requiere colocar un polarizador.

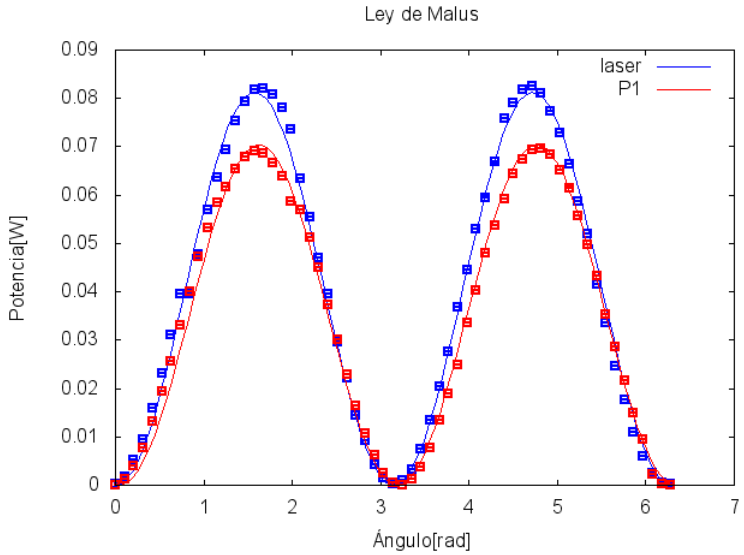


Figura 3.3: Gráfica de potencia como función del ángulo absoluto de la lámina de media onda. Este experimento corresponde a la ley de Malus. La curva obtenida tiene el comportamiento oscilatorio esperado corroborando la polarización lineal del láser. Repetí el experimento, después de colocar un polarizador a la salida del láser, con la idea de obtener una mayor visibilidad. En ambos casos, la visibilidad es mayor al 90 % y no es necesario colocar un polarizador frente al láser. La diferencia en la amplitud de las curvas se debe a pérdidas por absorción, esparcimiento y retroreflección.

Mediciones.

El control de los aparatos y la adquisición de datos se realizó en un programa de LabView que se muestra en el apéndice C.

El sistema se encuentra balanceado si la potencia en el canal 1 es lo más cercana posible experimentalmente a la del canal 2. Para evaluar si el sistema se encuentra balanceado o no, independiente de la potencia que estemos utilizando, definimos una función de respuesta R como

$$R(\theta, t) = \frac{P_1 - P_2}{P_1 + P_2}. \tag{3.4}$$

Con $P_{1(2)}$ la potencia en el canal 1(2). Tenemos que $-1 \leq R \leq 1$, toma los valores de "-1" y "1" cuando bloqueamos uno de los canales y queremos que $\left|\bar{R}\right| \leq 8.6 \times 10^{-5}$ donde $\bar{R}$ es el promedio de R sobre el tiempo requerido para tomar datos suficientes para generar una cadena de 4.3 Gbits. R es una función del ángulo de la placa de media onda θ y del tiempo t como se muestra a continuación.

Evaluación del sistema.

La primera serie de datos fue de 230 000 cuentas tomadas cada 200 ms (el tiempo de medición fue de 12.7 horas). Inicialmente dejé al sistema balanceado, esta conFiguración dura alrededor de 1 hora. Después aparece una tendencia hacia el canal 1. La Figura 3.4 muestra la evolución de R en el tiempo. La línea negra son eventos cada 200 ms, la azul es el promedio cada minuto y la roja cada 10 minutos. Al promediar, las oscilaciones desaparecen y queda la tendencia hacia el canal 1.

Tal vez el corrimiento observado es una etapa hacia un estado de equilibrio, en [2] dejan su experimento correr un día entero para estabilizarlo. Para ver si estamos ante el mismo caso, no apagué el láser durante un día completo. Después de lo cual, tomé datos durante 3 horas, el resultado se muestra en la Figura 3.5.

La tendencia no desapareció. El sistema no está más estable si se mantiene encendido un día. ¿Por qué observamos este comportamiento? ¿Cuál es el plan para lograr el objetivo de un sistema estable y balanceado? Un camino a seguir es determinar con exactitud el origen del comportamiento y corregirlo experimentalmente. Las posibles causas son fluctuaciones en la polarización del láser, efectos de temperatura en el láser y en la óptica, principalmente la película entre los dos prismas del PBS. En la Figura 3.6 grafico la temperatura en la superficie del láser. Se aprecian oscilaciones entre 23.7° y 24.4° con un periodo de 24 minutos. Estas oscilaciones pueden estar relacionadas con el funcionamiento del aire acondicionado del laboratorio. Otra idea es utilizar un algoritmo de retroalimentación como el PID. El primer método requiere

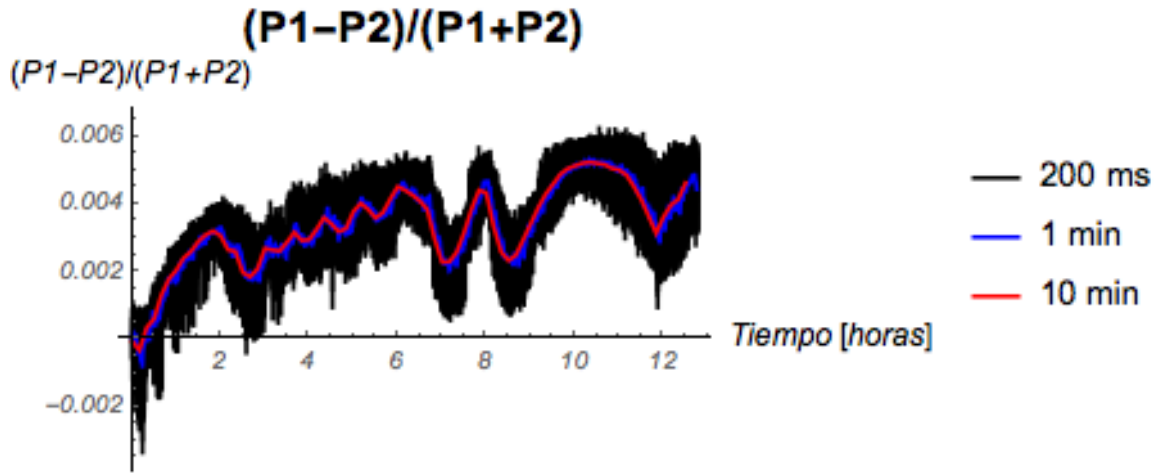


Figura 3.4: Gráfica de $R(\theta, t)$ como función del tiempo. Al inicio, el sistema permanece centrado por 1 hora. Aparece un corrimiento hacia uno de los canales.

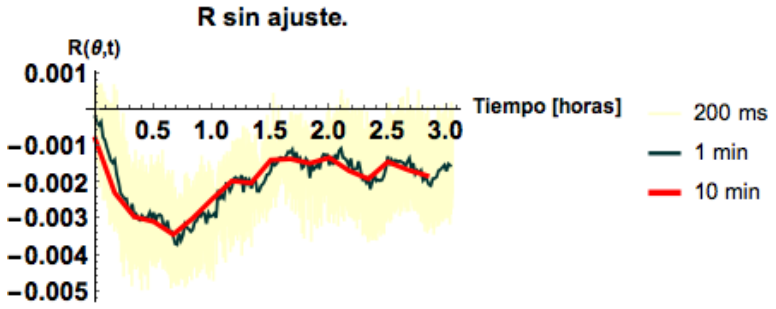


Figura 3.5: Valor de $R(\theta, t)$ en el tiempo para un valor de θ fijo, los datos se tomaron después de que el sistema estuviera encendido un día completo. Aún se observan fluctuaciones del balanceo hacia uno de los canales. Mantener encendido al sistema no ayudó.

pruebas que pueden desviar mucho el curso del proyecto. La idea del algoritmo PID, la implementé en LabView pero resultó lento e introducía un patrón periódico.

Dado que el desbalanceo ocurre a tiempos de decenas de minutos, puedo considerar que $R(\theta, t) \approx R(\theta)$ para tiempos cortos. Opté por caracterizar experimentalmente la respuesta del sistema ante cambios en el ángulo de la lámina de media onda.

Obtención de $R(\theta)$.

El método consitió en buscar el ángulo θ_0 en el que el sistema está balanceado. Luego tomé N de datos en el intervalo $[\theta_0 - 1°, \theta_0 + 3°]$ en pasos unidireccionales de $0.1°$. El comportamiento es lineal, se muestra en la Figura 3.7, y su ajuste es el siguiente:

$$B(\theta - \theta_0) = 6.87(\pm 0.67) \times 10^{-4} - 6.84(\pm 0.003) \times 10^{-2} \Delta\theta. \tag{3.5}$$

Que al invertir nos da el ángulo que tenemos que mover dado un desbalanceo. De acuerdo a lo anterior, para $\Delta\theta = 10^{-3}$, $B = 6.19 \times 10^{-4}$.

La caracterización se puede mejorar con rotaciones más pequeñas como muestro a continuación.

Respuesta más fina del sistema.

Repetí el procedimiento anterior en el intervalo $[\theta_0 - 0.01°, \theta_0 + 0.01°]$ en pasos de $0.001°$ (que es la rotación mínima del motor). También consideré la dirección de las rotaciones. En cada ángulo, tomé datos durante 30 s (300 datos espaciados 1 ms). Este ejercicio lo repetí con rotaciones en ambos sentidos por lo que al final tuve un ajuste para el movimiento hacia adelante (véase la Figura 3.8) y otro hacia atrás (Figura 3.9).

Ajuste hacia adelante:

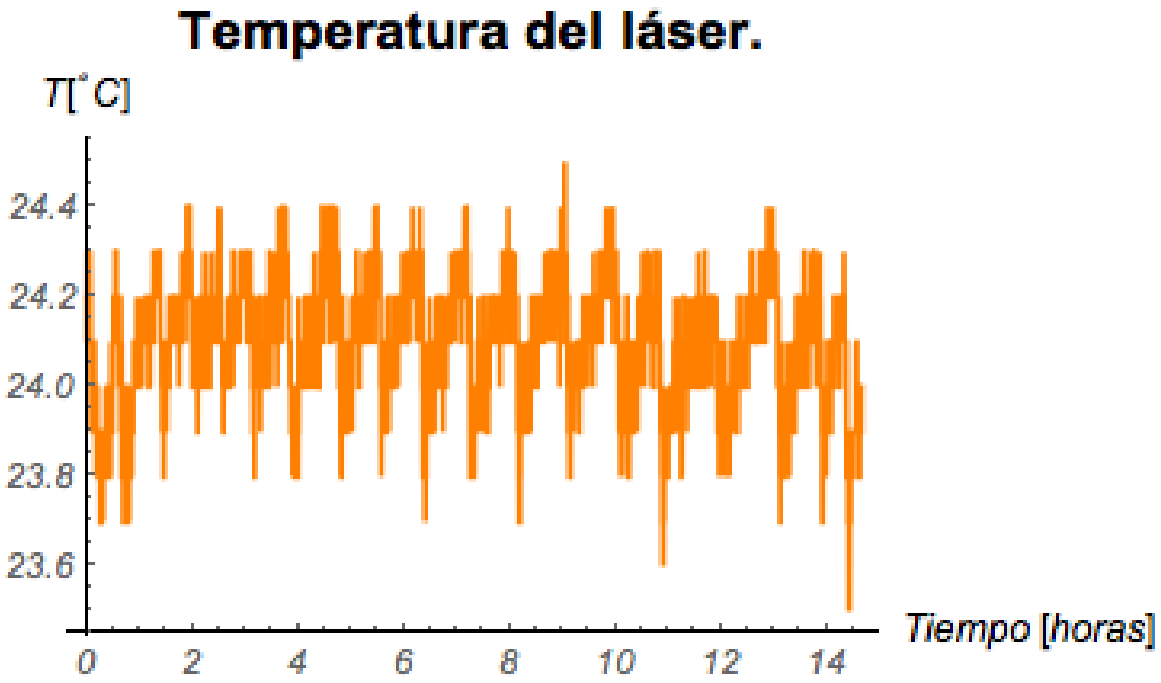


Figura 3.6: Temperatura en la superficie del láser. Se ve una oscilación con un periodo de 24 minutos.

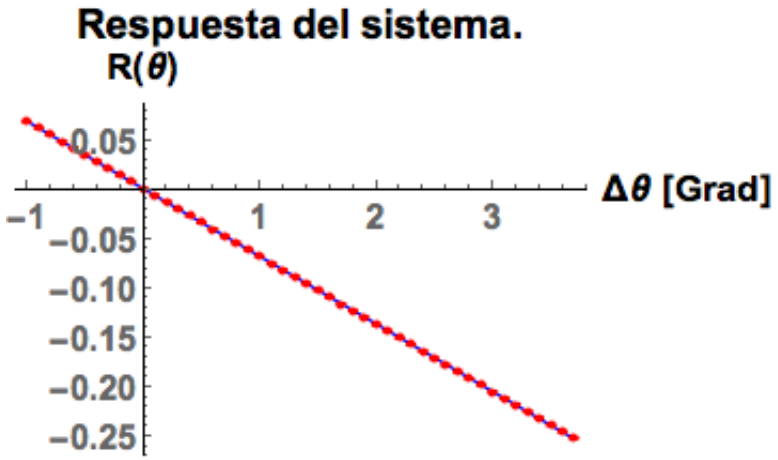


Figura 3.7: Respuesta del sistema como función de cambios en el ángulo de la lámina de media onda ($\Delta\theta$). El intervalo estudiado es $[\theta_0 - 1°, \theta_0 + 3°]$. La respuesta es lineal.

$$B(\theta - \theta_0) = -1.15(\pm 0.03) \times 10^{-1}\Delta\theta. \tag{3.6}$$

Ajuste hacia atrás:

$$B(\theta - \theta_0) = 1.2(\pm 0.1) \times 10^{-4} - 9.23(\pm 0.11) \times 10^{-2}\Delta\theta. \tag{3.7}$$

Prueba del método.

¿Funciona el método de caracterizar al sistema e implementar las funciones obtenidas? Invertí las funciones 3.6 y 3.7 y las programé en el programa de LabView.

Para probar el método, tomé valores de flujos por un periodo de tiempo T y calculé el promedio de $R(\theta)$. Con este valor, el programa calcula y efectúa la rotación requerida para balancear al sistema. Tomé datos durante 8 horas, la retroalimentación se efectuó cada 2.5 minutos.

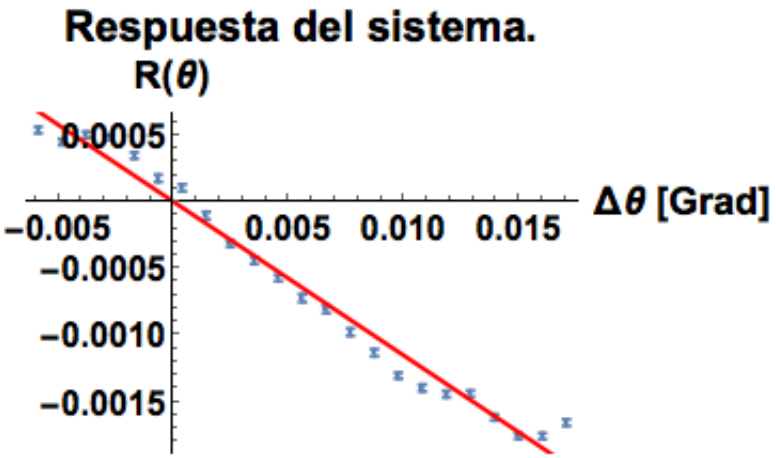


Figura 3.8: Respuesta del sistema, ante cambios de ángulo, con rotaciones de 1×10^{-3} ° hacia adelante en el intervalo $[\theta_0 - 0.01°, \theta_0 + 0.01°]$.

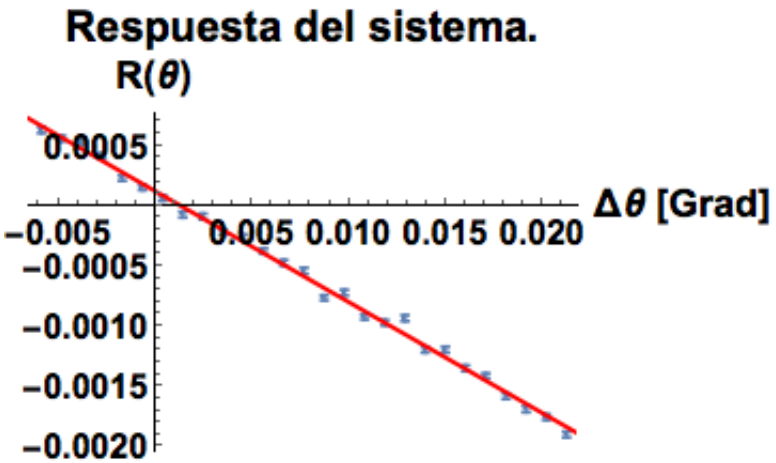


Figura 3.9: Respuesta del sistema, ante cambios de ángulo, con rotaciones de 1×10^{-3} ° hacia atrás en el intervalo $[\theta_0 - 0.01°, \theta_0 + 0.01°]$.

Retroalimentación cada 2.5 minutos.

El resultado es que $R(\theta, t)$ se mantuvo centrado en cero durante toda la medición (Figura 3.10). La tabla 3.1 resume el tiempo de muestreo, el promedio y desviación estándar de $R(\theta, t)$. El sistema se mantuvo balanceado con una parte en diez a la cuatro. Observé en estos datos que la desviación estándar no disminuyó al tomar promedios con tiempos 100 veces más largos. En la Figura 3.10 se ven picos, con una amplitud grande, que tienen estructura. Estos picos son indeseables y busqué eliminarlos cambiando el tiempo de retroalimentación.

Tiempo de muestreo.	Promedio	Desviación estándar (σ)
200 ms	1.2×10^{-4}	6.6×10^{-4}
1 min	1.2×10^{-4}	3.8×10^{-4}
2.5 min	1.2×10^{-4}	3.6×10^{-4}
10 min.	1.2×10^{-4}	2.8×10^{-4}

Tabla 3.1: Promedio, desviación estándar y su tiempo de muestreo para los datos tomados con retroalimentación cada 2.5 minutos.

El tabla 3.2 es análogo al tabla 3.1 sólo considerando los primeros 20 minutos del muestreo. La cuestión que surgió fue elegir el tiempo de retroalimentación que mantuviera al sistema balanceado y suprimiera las oscilaciones con estructura (las que tengan un ruido blanco son incorregibles por nuestro método). Probé otros dos tiempos de retroalimentación: 1 y 0.5 minutos.

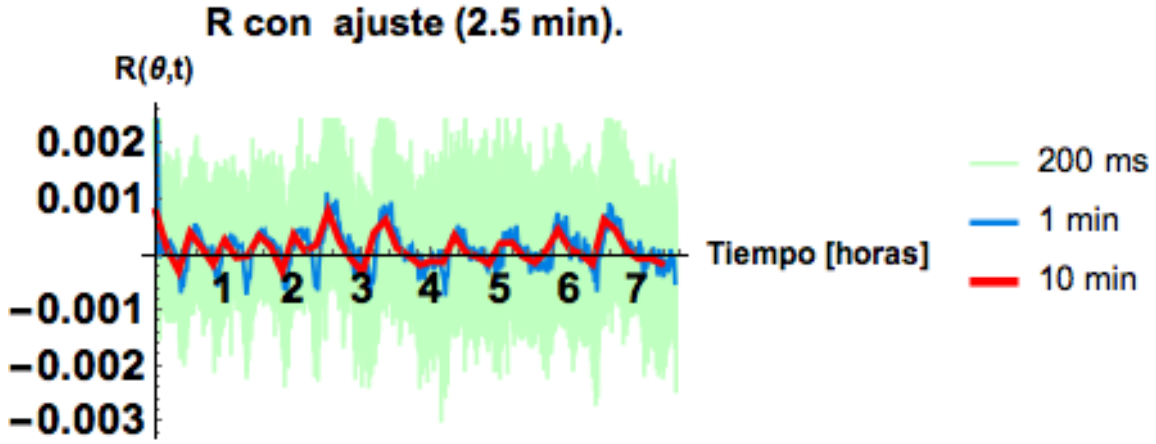


Figura 3.10: Valor de $R(\theta, t)$ en el tiempo. La retroalimentación, cada 2.5 minutos, estuvo funcionando durante toda la medición. Los datos (en verde) fueron tomados cada 200 ms, se muestra su promedio en azul (cada minuto) y en rojo (cada 10 minutos). Hay picos que no desaparecen al promediar y que impiden que la dispersión disminuya.

Tiempo de muestreo.	Promedio	Desviación estándar (σ)
200 ms	4.6×10^{-4}	9.6×10^{-4}
1 min	4.6×10^{-4}	8.6×10^{-4}

Tabla 3.2: Promedio, desviación estándar y su tiempo de muestreo para los datos tomados con retroalimentación cada 2.5 minutos y considerando únicamente los primeros 20 minutos.

Balanceo cada minuto.

Disminuí el tiempo de retroalimentación a 1 minuto. En la Figura 3.11 izquierda podemos ver el comportamiento de $R(\theta, t)$ durante 20 minutos. La gráfica de la derecha tiene los valores del ángulo de la lámina de medida onda. Vemos que hay momentos en los que no hay rotación indicando que no es necesario disminuir más el tiempo de retroalimentación. La tabla 3.3 tiene el promedio y desviación estándar de $R(\theta, t)$ para distintos intervalos de tiempo.

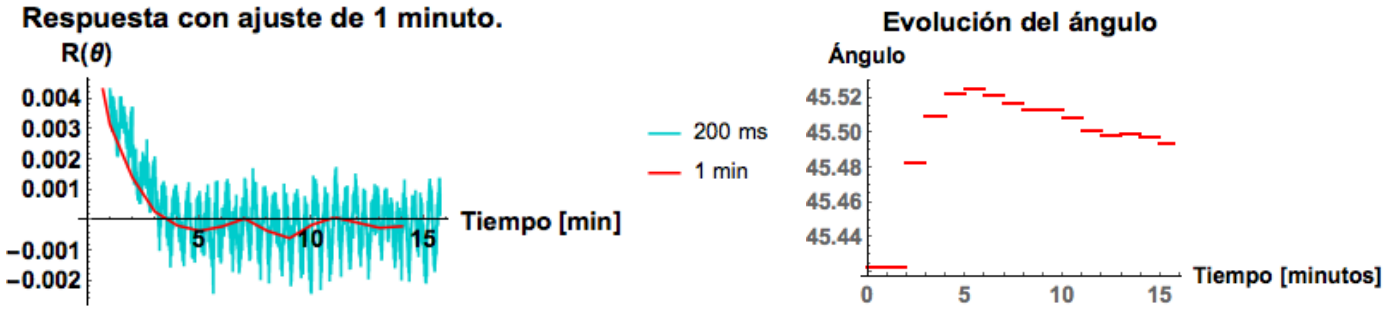


Figura 3.11: Respuesta del sistema con una retroalimentación cada minuto (izq.). También se muestra la evolución del ángulo de la lámina de media onda (der.).

Balanceo cada medio minuto.

También cambié el tiempo de retroalimentación a medio minuto. La Figura 3.12 muestra el valor de $R(\theta, t)$ y de $\theta(t)$ para este caso. La evolución de la lámina de media onda presenta muchos saltos como es de esperarse ya que el sistema está siguiendo a las oscilaciones rápidas que son incorregibles. Una rotación tan chica afectaría al sistema en lugar de mantenerlo estable. Decidí tomar un muestreo largo con retroalimentación de 1 minuto y ver si las estructuras observadas en la Figura 3.10 desaparecen.

Tiempo de muestreo.	Promedio	Desviación estándar (σ)
200 ms	6.0×10^{-4}	2×10^{-3}
1 min	6.4×10^{-4}	1.9×10^{-3}

Tabla 3.3: Promedio, desviación estándar y tiempo para promediar para los datos con rotación cada minuto.

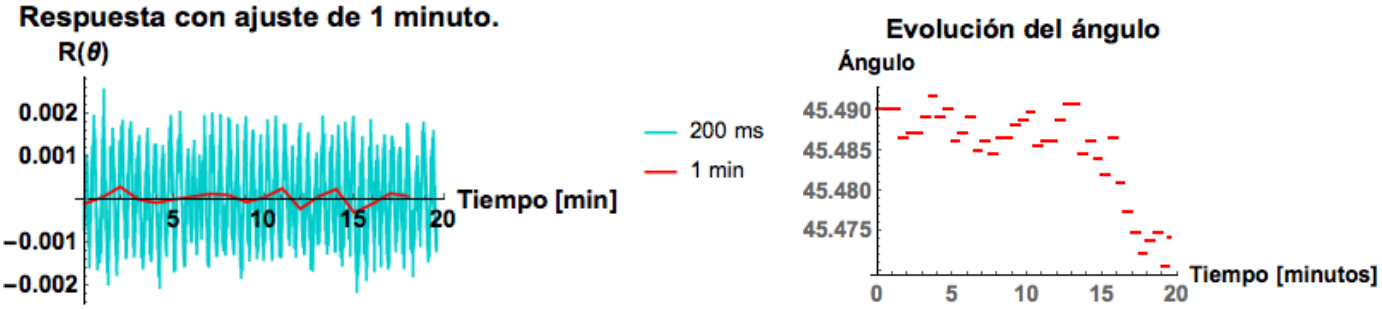


Figura 3.12: Gráfica del balanceo como función del tiempo con una retroalimentación de 30 s y su promedio cada minuto en rojo (izq.). A la derecha se muestra la evolución del ángulo de la lámina de media onda.

Muestreo largo con tiempo de retroalimentación de 1 minuto.

Tomé un muestreo de 12 horas con un tiempo de retroalimentación de 1 minuto. El valor de $R(\theta, t)$ y su promedio cada minuto y cada 10 minutos se grafican en la Figura 3.13. El sistema se mantiene centrado y la lámina de media onda absorbe el corrimiento y oscilaciones. Esta serie de datos es la primera con un promedio del orden de 10^{-5} (tabla 3.5). La desviación estándar escala con la raíz del número de datos.

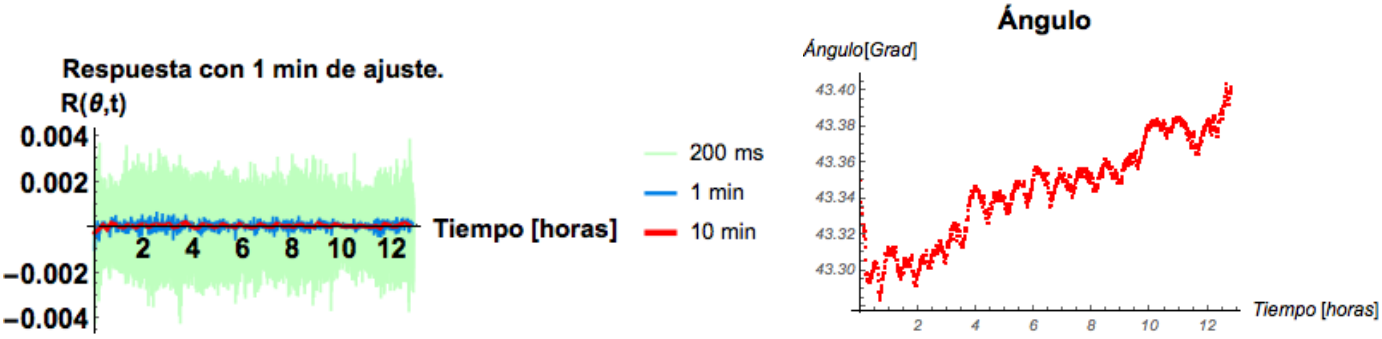


Figura 3.13: Gráfica de $R(\theta, t)$ como función del tiempo con una retroalimentación. En rojo y azul se muestra el promedio cada 1 minuto y 10 minutos respectivamente. A la derecha se muestra la evolución del ángulo de la lámina de media onda. Las oscilaciones y el corrimiento se transfieren de las cuentas por canal al ángulo de la lámina de media onda.

Elección del tiempo de retroalimentación en 1 minuto.

Los promedios y desviación estándar con tiempo de retroalimentación de 2.5 minutos son un poco más chicos (tabla 3.2) que los de 1 minuto y medio minuto (tablas 3.3 y 3.4). Sin embargo, con 2.5 minutos se observan oscilaciones con estructura indeseables. Al cambiar el tiempo a 1 minuto, desaparece esa estructura. Además el promedio y desviación estándar de $R(\theta, t)$ mejoró (tablas 3.1 y 3.5). Por tanto fijé el tiempo de retroalimentación en 1 minuto.

Con el valor del promedio de $R(\theta, t)$ de 6.8×10^{-5}, decidí pasar a la siguiente fase del experimento: Atenuar el láser y repetir lo hecho empleando detectores de fotones individuales.

polarizador (durante 30 minutos). No aprecio una diferencecia clara entre las dos pruebas.

Tiempo de muestreo.	Promedio	Desviación estándar (σ)
200 ms	6.0×10^{-4}	1.9×10^{-3}
1 min	6.4×10^{-4}	1.9×10^{-3}

Tabla 3.4: Promedio, desviación estándar y tiempo de muestreo para los datos de rotación cada medio minuto.

Tiempo de muestreo.	Promedio	Desviación estándar (σ)
200 ms	6.8×10^{-5}	8×10^{-4}
1 min	6.8×10^{-5}	2×10^{-4}
10 min.	6.8×10^{-5}	7×10^{-5}

Tabla 3.5: Valores del promedio, desviación estándar y el tiempo de muestreo correspondiente. Estos valores corresponden a los datos tomados durante 12 horas con un tiempo de retroalimentación de 1 minuto. La tabla 3.2 es diferente porque corresponde a un muestreo de 15 minutos.

La siguiente etapa consistió en atenuar el láser y hacer los cambios necesarios en el experimento y programa de LabView. Fue necesario cambiar el sistema de medición a detectores de fotones individuales, utilicé un par de fotodiodos de avalancha (APD por sus siglas en inglés), y un etiquetador temporal iD800. Las características del iD800 y de los APDs se describen en el apéndice C.

3.2. Fase 2: láser atenuado.

El esquema experimental se muestra en la figura 3.14. Los cambios al experimento son la atenuación del láser con filtros absorbentes de densidad neutra (en total utilicé una densidad óptica de 7.3). En cada salida del PBS, coloqué un microbloque con una lente asférica que enfoca los fotones a fibras multimodo, donde se propagan hasta un APD. La salida de cada APD está conectada a un etiquetador temporal iD800.

En la figura 3.15 se muestran dos fotografías de la parte central del experimento.

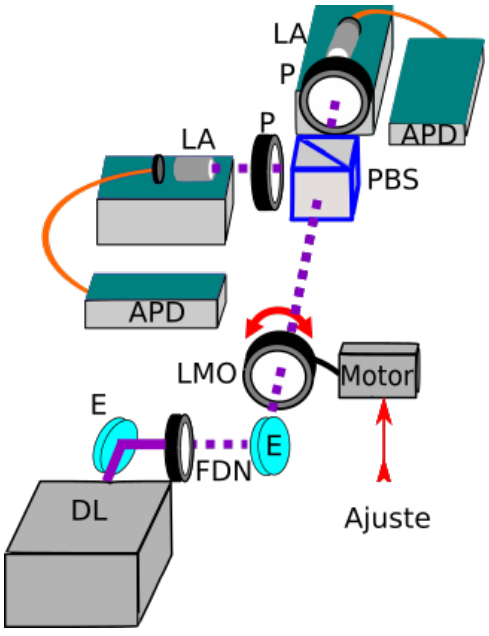


Figura 3.14: Esquema del experimento. Nuestra fuente es un diodo láser (DL) de 405 nm, atenuado con filtros absorbentes de densidad neutra (FDN), con polarización vertical. La alineación del láser la hice con dos espejos (E). La polarización es rotada por una lámina de media onda (LMO) motorizada que prepara a los fotones en polarización $\frac{H+e^{i\phi}V}{\sqrt{2}}$. La probabilidad de que un fotón de este ensamble se transmita o se refleje al incidir en un PBS es 0.5 en cada caso. En cada salida del PBS hay un polarizador (P) seguido de un microbloque con una lente aesférica (LA) para enfocar a los fotones a fibras multimodo conectadas a un APD. La salida de ambos APDs se registra en un etiquetador iD800.

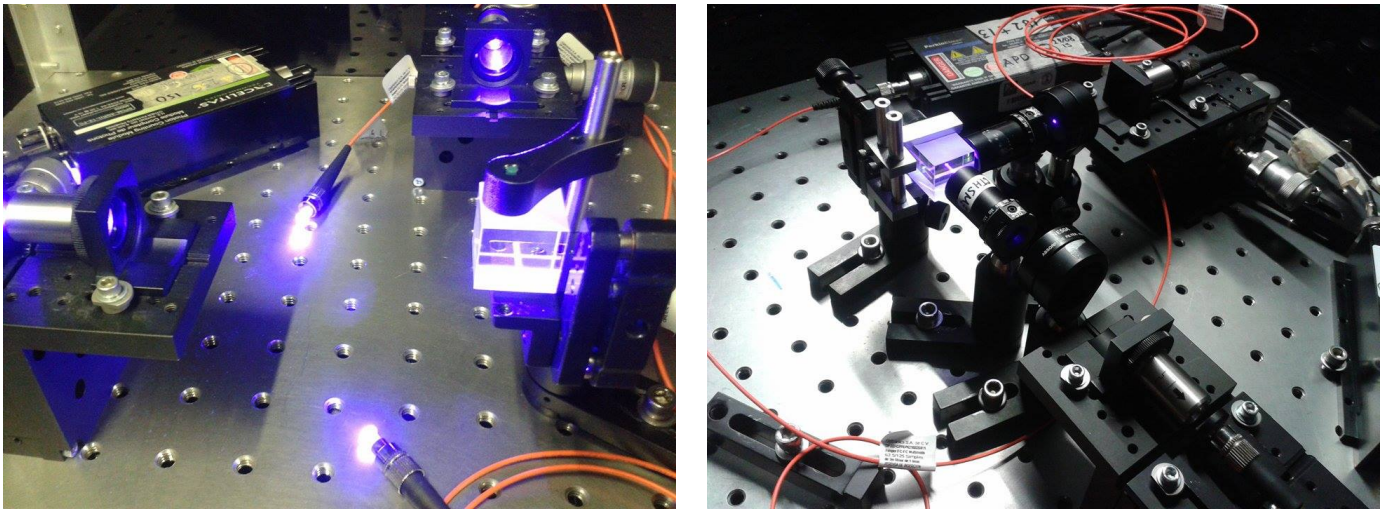


Figura 3.15: Fotografías de la parte central del arreglo experimental. Se muestra el PBS donde los fotones se separan según su polarización. Posteriormente, los fotones se enfocan en fibras monomodo donde viajan hasta un APD donde se genera un pulso por cada detección. El conteo de eventos y su etiquetamiento se realiza en un etiquetador de tiempos iD800.

Escaneo del ángulo de la lámina de media onda.

Adapté el programa de LabView para que fuera compatible con el software del iD800 para obtener el flujo de fotones. Las rotaciones de la lámina de media onda siguen siendo controladas desde el mismo programa.

Durante el montaje del experimento me percaté de que una de las lentes acopladoras, que son del mismo fabricante y mismo modelo, era más eficiente que la otra. Utilizando los tornillos micrométricos de los microbloques, ajusté el acoplamiento de las fibras para tener simetría en las eficiencias de ambos canales.

Hecho lo anterior, realicé un escaneo para ubicar la región de balanceo. Con un flujo de 1.7 Mcs tomé 200 datos (cada 100 ms esperando 50 ms para asegurarnos de no repetir valores), roté el motor en ángulos de 5° en el intervalo $[0°, 90°]$ (que corresponden a un intervalo de 180° en polarización). La figura 3.16 presenta las cuentas en cada canal como función del ángulo absoluto de la lámina de media onda.

En 22° los fotones están en el estado $|H\rangle$ y en 65° en $|V\rangle$. Alrededor de 0°, 45° y 90° hay zonas con el mismo número de cuentas en cada canal, que corresponden a las regiones donde se prepara el estado $\frac{|H\rangle+e^{i\phi}|V\rangle}{\sqrt{2}}$ (con una fase distinta en cada caso). La zona de 0° no debe ser usada porque hace la retroalimentación lenta, debido a rotaciones de casi 360° para balancear el sistema. Elegí la zona de 45° para tomar datos.

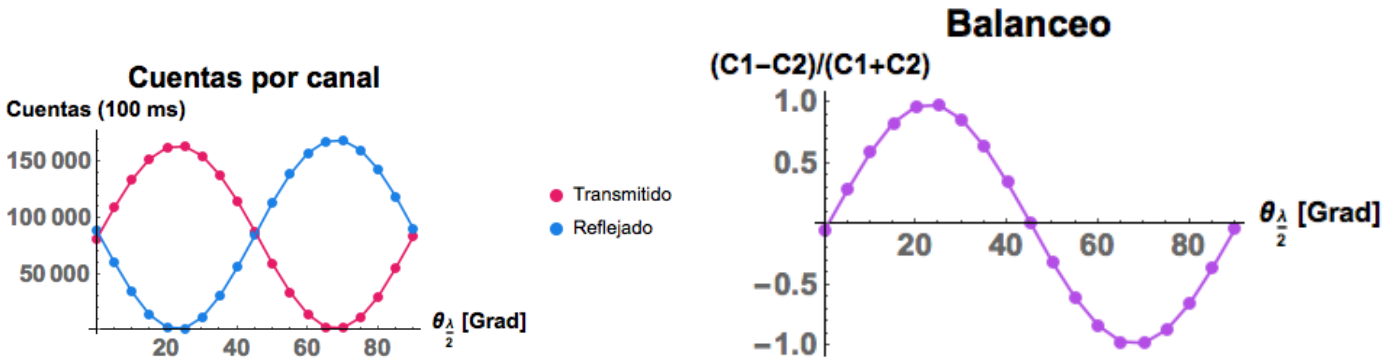


Figura 3.16: A la izquierda se muestra un escaneo del intervalo $[0°, 90°]$ del ángulo absoluto de la placa retardadora. En cada iteración se hacía una rotación de 5° y se tomaban el flujo de fotones con un tiempo de exposición de 100 ms. Ambos canales fueron ajustados para lograr simetría en las eficiencias. A la derecha se grafica la respuesta del sistema (véase definición 3.8). Hay 3 zonas de balanceo separadas 45° entre sí.

Siguiendo lo hecho con potenciómetros, para tener una forma sencilla de evaluar el balanceo del sistema, definimos

$$R = \frac{C_1 - C_2}{C_1 + C_2}. \tag{3.8}$$

Con C_1 y C_2 las cuentas por unidad de tiempo en el canal 1 y en el 2. Lo que siguió fue ver si el sistema se mantiene estable por sí solo o si se desbalancea.

Evaluación inicial del sistema.

Coloqué al sistema balanceado, tomé une medición de 120 000 datos con un tiempo de exposición de 100 ms, con un retraso de 50 ms para evitar cuentas desactualizadas.

La figura 3.17 muestra el valor de R para esta serie de datos y su promedio cada minuto y cada 10 minutos. Se observan oscilaciones que dan un ancho a la curva. En estas oscilaciones están el ruido blanco del fenómeno, el ruido óptico, electrónico y térmico de los aparatos. Hay una tendencia hacia uno de los canales (cuya explicación suponemos está en cambios en temperatura que afectan el PBS y a fluctuaciones en la óptica particularmente de la lámina de media onda) que es necesario suprimir. Al promediar en el tiempo, las oscilaciones desaparecen dejando únicamente la tendencia del sistema.

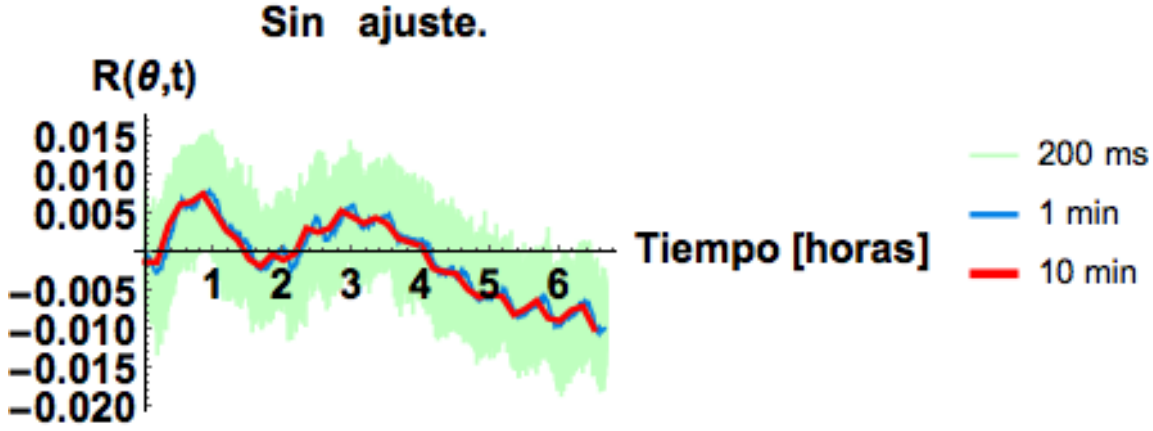


Figura 3.17: Gráfica de la diferencia normalizada de cuentas en cada canal. Estos datos se tomaron sin retroalimentación. En negro se grafican cada uno de los datos, en azul el promedio cada minuto y en rojo el promedio cada 10 minutos. Al promediar, las oscilaciones desaparecen y queda la tendencia únicamente.

Siguiendo lo que hicimos con los potenciómetros, obtuve la respuesta del sistema como función del ángulo de la lámina de media onda. El ajuste lo hice para rotaciones hacia adelante y hacia atrás.

Obtención de la respuesta del sistema.

Busqué el ángulo θ_0 en el que el sistema está balanceado. Luego tomé N datos en el intervalo $[\theta_0 - 1°, \theta_0 + 3°]$, las rotaciones fueron de 0.001° hacia un solo sentido. El comportamiento se muestra en la figura 3.18. Los ajustes lineales son los siguientes:

Rotaciones en sentido positivo:

$$B(\theta - \theta_0) = 2.4(\pm 0.1) \times 10^{-2} + 1.8(\pm 0.1) \times 10^{-1} \Delta\theta. \tag{3.9}$$

En sentido contrario, el ajuste es

$$B(\theta - \theta_0) = 5.3(\pm 0.3) \times 10^{-2} + 3.9(\pm 0.2) \times 10^{-1} \Delta\theta. \tag{3.10}$$

El valor de R no pasa por cero, lo que indica que no estamos centrados en el punto de balanceo. La razón es que la toma de datos fue muy larga (20 minutos hacia cada dirección) y el sistema se desajustó. Para evitar este problema, utilicé rotaciones de 0.007°.

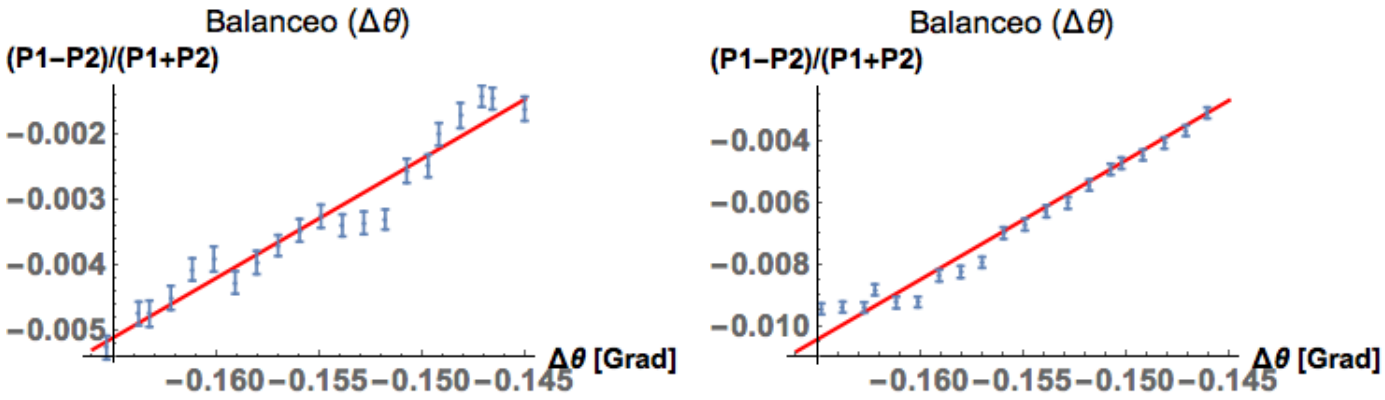


Figura 3.18: Balanceo como función del ángulo de rotación hacia adelante (izquierda) y hacia atrás (derecha). En ambos casos hice un ajuste lineal aunque los datos no cruzan por cero.

Ajuste con rotaciones de $0.007°$.

Tomé 400 datos, espaciados 150 ms. Los datos los tomé en el intervalo $[\theta_0 - 0.07°, \theta_0 + 0.07°]$ rotando $0.007°$ en cada iteración. Una gráfica de los ajustes y sus datos se muestran en la Figura 3.19.

Ajuste hacia adelante:

$$B(\theta - \theta_0) = -2.8(\pm 14.5) \times 10^{-5} + 4(\pm 0.3) \times 10^{-2}\Delta\theta. \tag{3.11}$$

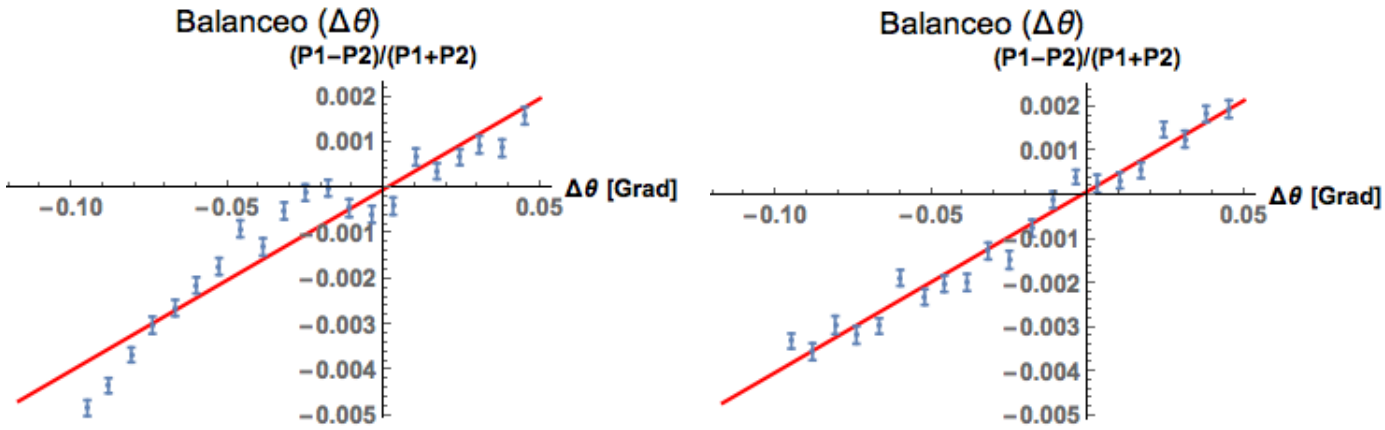


Figura 3.19: Balanceo como función de la diferencia de ángulo de rotación ($\Delta\theta = \theta_0 - \theta$ con θ_0 el ángulo donde el sistema está balanceado) hacia adelante (izquierda) y hacia atrás (derecha). En ambos casos hice un ajuste lineal.

Ajuste hacia atrás:

$$B(\theta - \theta_0) = 9.1(\pm 8.1) \times 10^{-5} + 4.1(\pm 0.2) \times 10^{-2}\Delta\theta. \tag{3.12}$$

La pendiente es 3 veces más pequeña que la obtenida con potenciómetros.

Prueba del método.

Invertí las funciones 3.11 y 3.12 y las implementé en el programa de LabView. Procedí a probar el funcionamiento del sistema de retroalimentación. En la figura 3.20 se muestra $R(\theta, t)$ como función del tiempo. El sistema inicia sesgado hacia un canal, se enciende la retroalimentación (con un periodo de 1 minuto) y en 10 minutos el sistema se balancea. El método funciona en tiempos cortos.

La figura 3.21 muestra la continuación de la figura 3.20. Dejé la retroalimentación encendida durante 7 horas y el sistema se mantiene estable. El método es exitoso a tiempos largos.

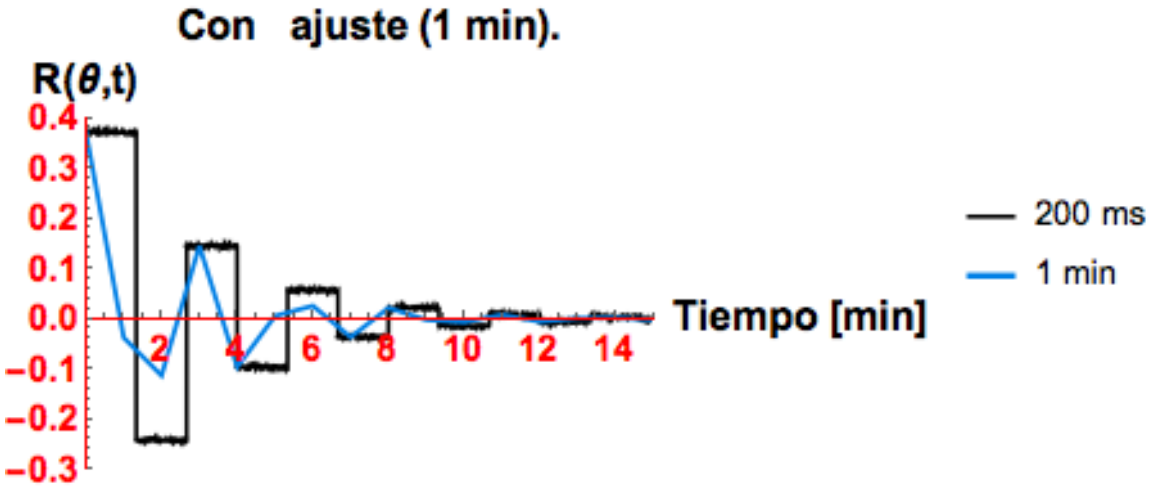


Figura 3.20: Demostración de que el mecanismo de retroalimentación basado en la función de respuesta del sistema funciona. El sistema comienza desbalanceado y se centra en 10 minutos.

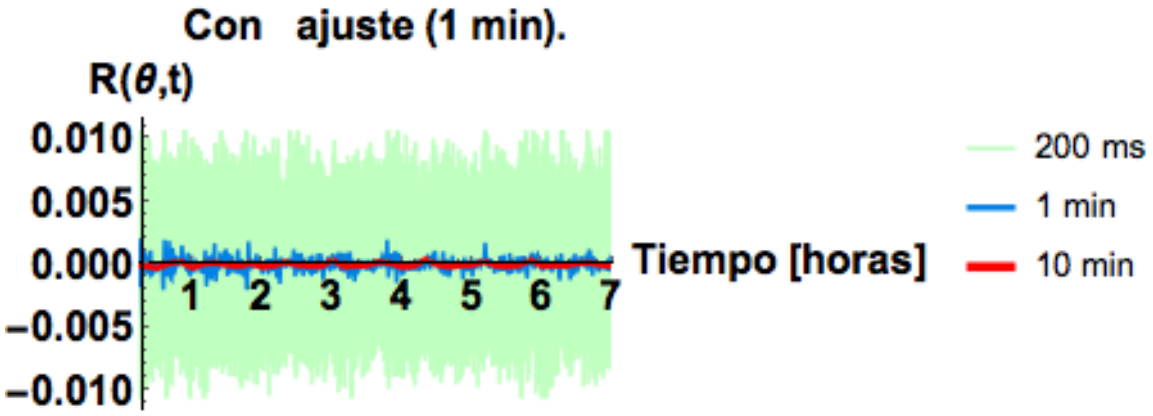


Figura 3.21: Datos de $R(\theta, t)$. Esta gráfica es la continuación de la anterior y demuestra que el mecanismo de retroalimentación funciona a tiempos largos.

El ángulo de la lámina de media onda como función del tiempo se muestra en la gráfica 3.22. Hay una tendencia muy ligera hacia uno de los canales con oscilaciones de 35 minutos y una amplitud de 0.8°.

La tabla 3.5 contiene el promedio y desviación estándar de $R(\theta, t)$ con sus respectivos tiempos de muestreo. El sistema se mantuvo balanceado con un promedio de 2 partes en diez a la cinco. Al promediar, la desviación estándar disminuye y no se ve algún tipo de estructura remanente.

Tiempo de muestreo.	Promedio	Desviación estándar (σ)
150 ms	-2.4×10^{-5}	2.7×10^{-3}
1 min	-2.4×10^{-5}	6.7×10^{-4}
10 min.	-2.3×10^{-5}	1.3×10^{-4}

Tabla 3.6: Promedio, desviación estándar y su tiempo de muestreo para los datos tomados con retroalimentación cada minuto.

Los valores tan buenos del promedio nos permiten movernos hacia la siguiente fase del proyecto que es tomar datos en binario como eventos completos (cada evento aparece con su canal y una etiqueta de tiempo), generar cadenas y poner a prueba su aleatoriedad.

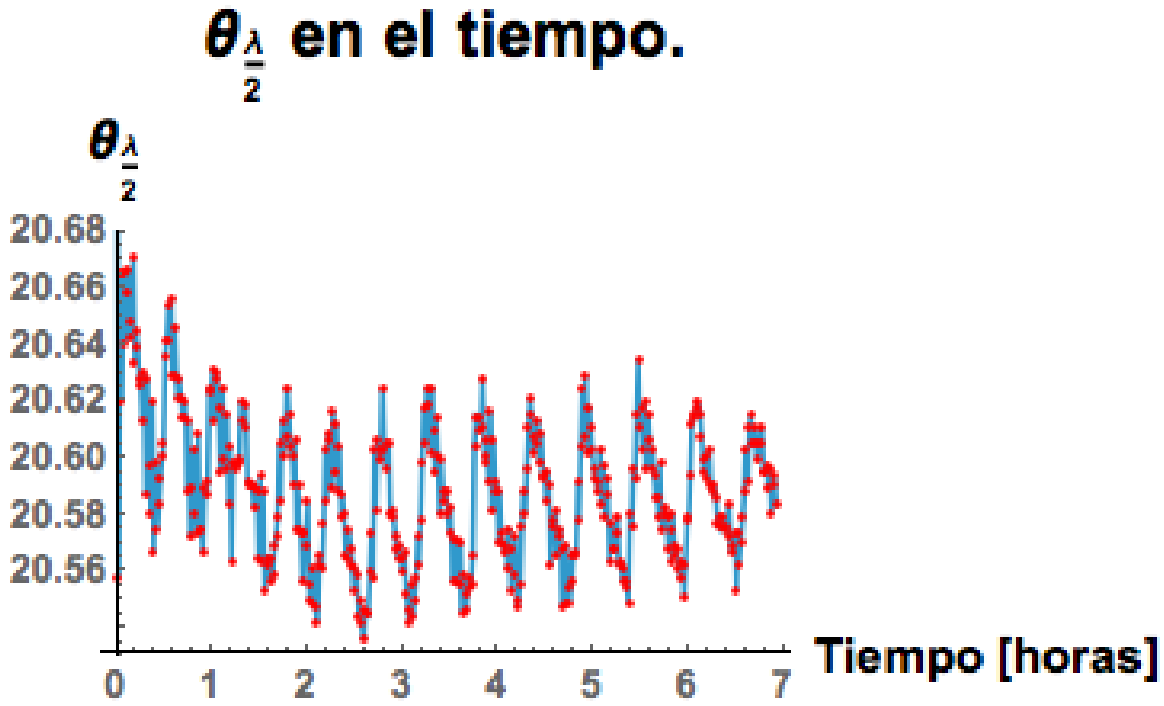


Figura 3.22: Serie de tiempo de los ángulos de la lámina de media onda. Hay una oscilación alrededor de 20.5889°. Después de la primera parte se ven unas oscilaciones de 35 minutos con una amplitud de 0.8°.

Capítulo 4

Sobre cómo generamos las cadenas binarias y su evaluación.

El sistema de retroalimentación fue exitoso, alcanzando promedios de $R(\theta, t)$ del orden de 10^{-5}. Esa precisión es suficiente para generar cadenas binarias y someterlas a la prueba de Normalidad de Borel.

Tomé dos series de datos, con flujos de fotones distintos, con la idea de detectar posibles diferencias ocasionadas por el efecto de afterpulsing. El flujo de fotones chico fue de 130 kcs (kilocuentas por segundo) con el que tomé datos para 7 cadenas, requirió un tiempo de adquisición por cadena de 9.5 horas. El flujo de fotones grande fue de 1.7 Mcs (Megacuentas por segundo) y tomé datos para 10 cadenas (cada cadena requirió un tiempo de 50 minutos). En ambos casos la longitud de las cadenas esperada fue de 4.3×10^9. Los resultados obtenidos, para un mismo flujo de fotones, son similares para todas las cadenas por lo que sólo mencionaré una cadena representativa.

Para estas mediciones utilicé los mismos detectores etiquetados por los números 6 (canal 2) y 12 (canal 1).

La salida de cada evento del iD800 tiene diez bytes, ocho de los cuales representan la etiqueta temporal y dos el canal de detección. Cada archivo, escrito en binario, pesa 43 GBytes por lo que es necesario utilizar un disco duro extra en la computadora. Posteriormente, los archivos se guardan en el cluster del ICN donde se pueden analizar. El siguiente paso es desarrollar programas que implementen el método de generación de cadenas binarias descrito a continuación.

4.1. Asignación binaria de las salidas de un PBS.

El método de generación basado en un PBS es bonito por su sencillez conceptual. Consiste en preparar a los fotones en el estado de polarización $\frac{|H\rangle+e^{i\phi}|V\rangle}{\sqrt{2}}$. Al incidir en un PBS, la probabilidad que el fotón se refleje con polarización $|V\rangle$, o se transmita con polarización $|H\rangle$, es 0.5. Al resultado de detectar $|V\rangle$ lo etiquetamos con un "0" y $|H\rangle$ con un "1". La tasa de producción de bits es igual al flujo de fotones.

El programa que implemente este esquema debe fijarse en el canal de detección y asignarle un "0" ("1") al canal 2 (1). Pese a la sencillez de la idea, la implementación puede ser ineficiente debido a la cantidad de datos y al manejo directo de bytes que se requiere. Mis primeros intentos fueron un programa en Python y otro en bash que tardaban varias horas en generar una sola cadena.

Finalmente, implementé el algoritmo en C. La diferencia es enorme, el programa tarda un par de minutos en generar una cadena.

Resultados.

Flujo de 130 kcs.

La figura 4.1 izquierda muestra los resultados de la prueba de Normalidad de Borel detallada en el capítulo 2, específicamente muestra los valores de $\left|\frac{N_m^i(x)}{|x|_m} - P_{ideal} = \frac{1}{2^m}\right|$ para $1 \leq m \leq 5$ e $1 \leq i \leq 2^m$, para la cadena 7. La cota para que una cadena sea Borel normal es de 8.63×10^{-5} y se muestra en rojo.

Los resultados para $m = 1$ son buenos y es una confirmación más de que el sistema de retroalimentación es efectivo. El exceso de un canal es simétrico con la carencia del otro. En nuestras cadenas, dentro del margen aceptable, hay un poco más de '0' que de '1', lo que corresponde a más eventos en el canal reflejado (2).

Sin embargo, para $m = 2$ las cadenas presentan exceso de los bloques "00" y "11". Estos bloques están favorecidos por el efecto de afterpulsing. El bloque de '11' está ligeramente más presente que el otro indicando una asimetría entre los 2 APDs. Para $m = 3$ también hay exceso de "000" y "111".

Quitar afterpulsing.

El afterpulsing, un fenómeno que se presenta en detectores de fotones individuales (véase apéndice B), introduce correlaciones de bits consecutivos, favoreciendo los bloques "00" y "11". Los resultados anteriores detectaron este patrón, así que es deseable suprimirlo.

Para quitar el afterpulsing, tomé la diferencia de tiempo entre dos eventos sucesivos en un mismo canal, e ignoré aquellos eventos separados por un tiempo menor a una ventana arbitraria ($V_{aftp} \approx 100$ ns). Generé nuevas cadenas y las analicé.

La figura 4.1 (derecha) muestra los resultados de la cadena 7 con $V_{aftp} = 100$ ns. Las cadenas sin afterpulsing están desbalanceadas y no pasan Borel para $m = 1$(las desviaciones son del orden de 5×10^{-3} para 100 ns). El desbalanceo se agudiza al incrementar el valor de V_{aftp}.

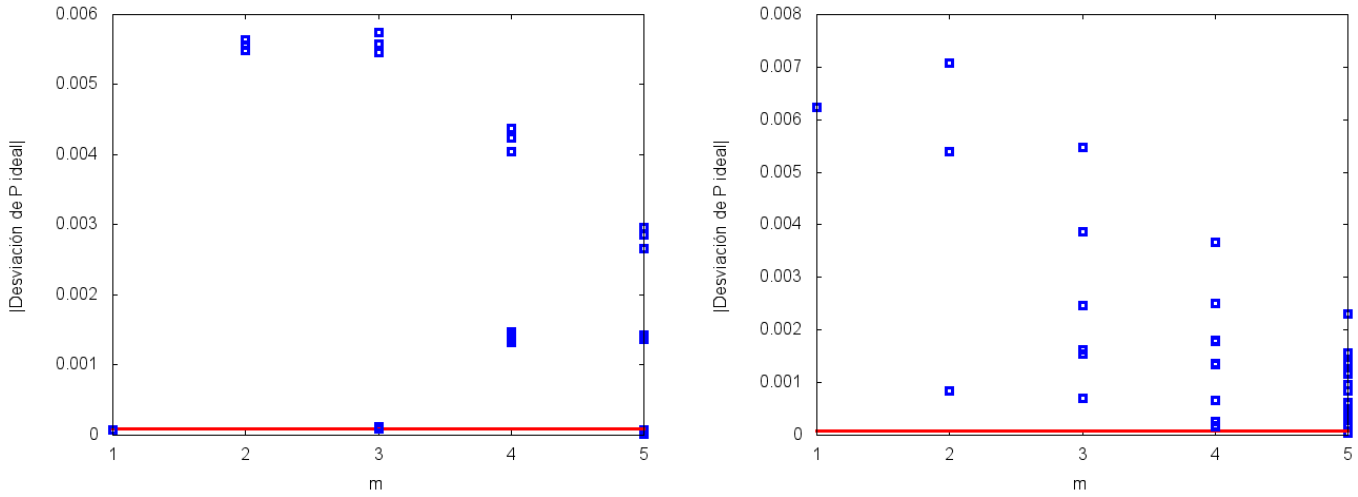


Figura 4.1: Resultados de Normalidad de Borel para la cadena 7 generada con asignación de PBS (izquierda) y quitando eventos separados por 100 ns o menos (derecha). En rojo se muestra la cota impuesta por normalidad de Borel y los puntos indican los resultados para bloques de m ($m = 1..., 5$)

Como un intento de eliminar las correlaciones detectadas de bits consecutivos repetidos, surgió la idea de cambiar la etiqueta asociada a las salidas del PBS después de cada evento. La implementación la hice con una operación binaria XOR en el byte del canal de detección.

El resultado es que se mantiene el balanceo mejorando la proporción de "0" y "1". Para Borel 2, se transfiere el exceso de "00" y "11" a los bloques "10" y "10".

Flujo de 1.7 Mcs.

Los resultados son similares al de flujo chico.

4.2. Histogramas.

Para poder entender por qué las cadenas obtenidas con el PBS no pasan las pruebas de normalidad de Borel, realizamos los histogramas de tiempos de llegada de fotones a cada uno de los dos APDs.

La resolución utilizada es de 162 ps (resolución mínima estable del iD800) y el intervalo en que lo hice fue en los primeros 50 us.

Los parámetros determinantes en el histograma son características del detector: tiempo muerto, afterpulsing y eficiencia.

El tiempo muerto de 20 ns favorece la presencia de bloques "01" y "10". El afterpulsing ocurre en la región de $[20, 100]$ ns provocando un porcentaje alto de los eventos en esta zona y favoreciendo la aparición de "00" y "11". La eficiencia del detector cobra relevancia en el resto de la distribución, donde la curva es una exponencial que decae [4].

Idealmente desearíamos tener dos curvas idénticas. Sin embargo, el proceso de fabricación y las componentes (electrónica y material semiconductor) de cada APD introducen diferencias. Las oscilaciones de los histogramas se ven en fase con amplitudes distintas. Quizá esta sea un sello característico de cada modelo de los detectores.

Flujo de 130 kcs.

La figura 4.2 (izq) muestra el histograma de ambos canales para la cadena 7. El tiempo muerto de cada detector es de 20 ns y se omite en la gráfica. La primera zona (gráfica principal) muestra que el canal 2 tiene un mayor efecto de afterpulsing que el canal 1. La gráfica más pequeña es el histograma en la región $[1, 50]$ μs. En esta última zona, el canal 1 tiene más cuentas que el canal 2 indicando una eficiencia mayor en el canal 1. El área bajo cada curva es la misma, varía la forma en que se distribuyen los eventos.

La figura 4.2 (der.) es una gráfica log-log del histograma de la cadena 7. La diferencia en afterpulsing es notoria al inicio de la gráfica.

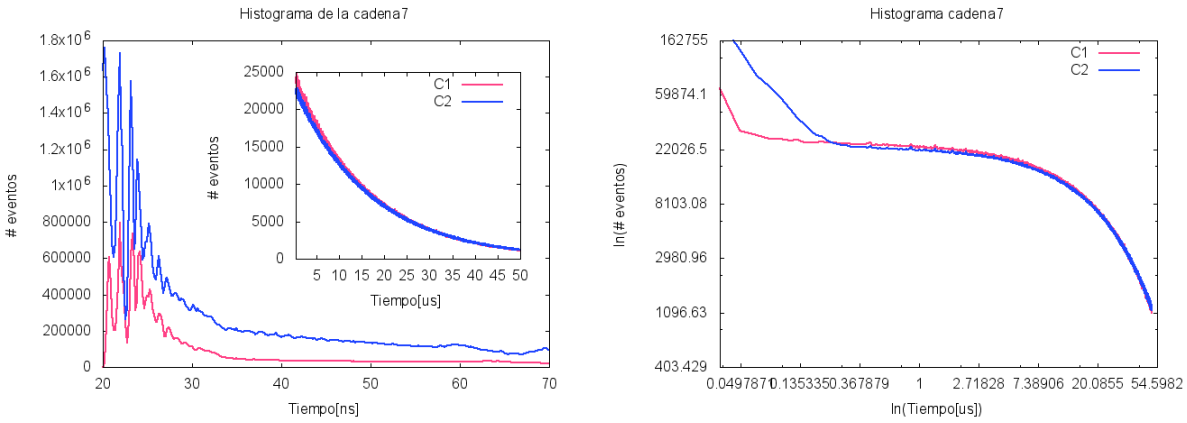


Figura 4.2: Histograma de los tiempos de llegada al canal 1 y 2. Los datos son de la cadena 7 y fueron tomados con un flujo de 130 kcs.

Flujo de 1.7 Mcs.

Las figuras 4.3 y 4.4 muestra el histograma de la cadena 7 con un flujo de 1.7 Mcs. El canal 2 tiene más afterpulsing que el canal 1.

Estos datos presentan más ruido numérico que las de flujo chico. Por eso presento el intervalo $[1, 10]$ μs del histograma en escala log-log. De la gráfica log-log, vemos que la diferencia de afterpulsing es mayor para el flujo de 130 kcs.

Los histogramas muestran diferencias en las características de los detectores, pese a que sean del mismo fabricante y mismo modelo. La razón de que nuestras cadenas fallen está contenida en estos histogramas:

Los APDs utilizados (6 y 12) tienen características muy diferentes. El APD 6 tiene más afterpulsing que el 12, explicando que haya más bloques de "00" que de "11" . El 12 tiene una eficiencia ligeramente mayor y permite el balanceo al considerar tiempos largos. Alrededor de 200 ns hay un cruce entre las gráficas, después del cual el canal 1 queda por arriba ligeramente. La diferencia se minimiza en el resto del histograma.

Al suprimir los eventos en la región $[20, 100]$ ns queda una cadena desbalanceada con exceso de eventos en el canal con mayor eficiencia (que es el canal 1 en nuestro caso). Las cadenas con ventana tienen exceso de "1".

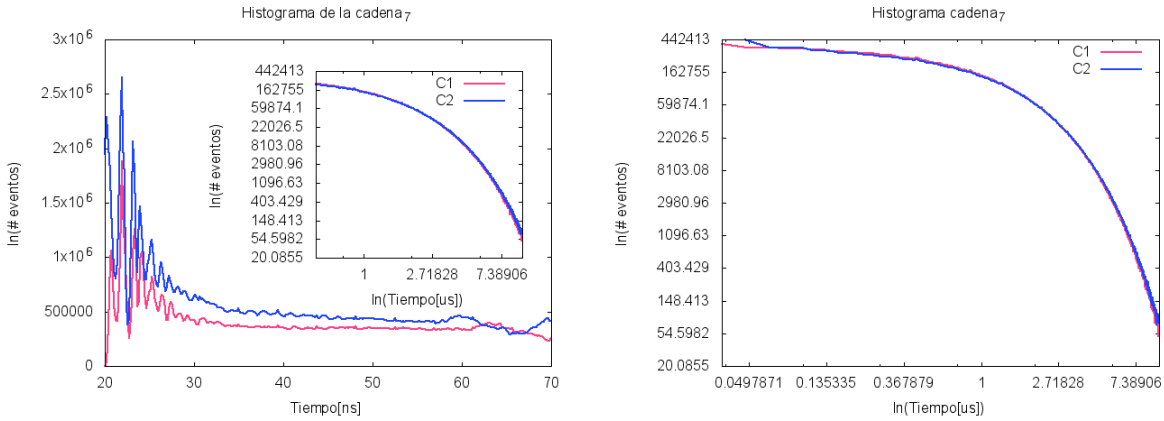


Figura 4.3: Histogramas de la cadena 7 con flujo grande de 1.7 Mcs. A la derecha presento el histograma en escala log-log.

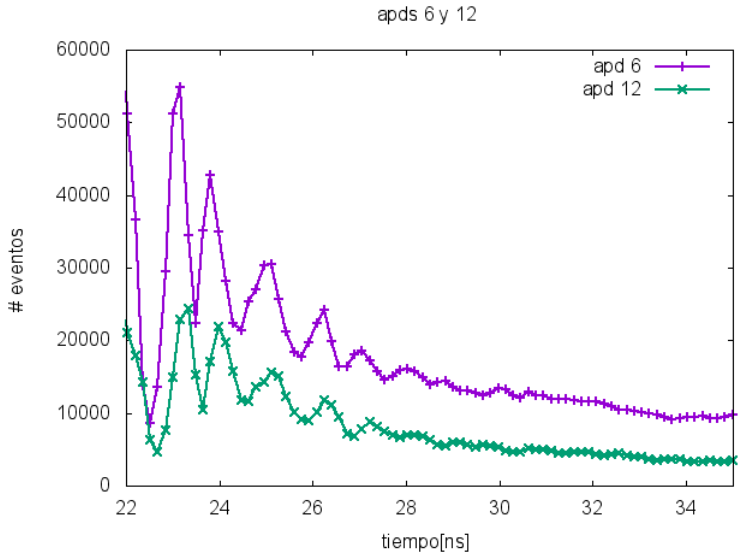


Figura 4.4: Histograma de los APDs 6 y 12, con los que se tomaron las primeras series de datos.

La relación con el resultado negativo de [2].

Algunas de las cadenas, generadas por el grupo de Viena, utilizadas en [2] fallan Normalidad de Borel para $m = 2$, 3 y 4. Su escenario es muy parecido al nuestro: Utilizan un LED, un divisor de haz sin sensibilidad a la polarización y tubos fotomultiplicadores (que también presentan afterpulsing). Incluso realizan ajustes en el voltaje de cada detector para tener simetría en ambos canales de detección, y sus cadenas pasan Borel 1. Muy probablemente, la razón de su resultado sea la misma que hemos encontrado en nuestro experimento.

¿ Qué tan similares tienen que ser los detectores para que el generador cuántico de números al azar funcione?

Para suprimir las correlaciones inducidas por la asimetría de los APDs, tomé datos de los 6 detectores SPCM-AQRH-13-FC marca Excellitas del laboratorio a un flujo de 250 kcs para elegir los dos con curvas más parecidas.

Los APDs 9, 10 y 11 son los más parecidos y sus histogramas se presentan en la figura 4.6. Los 3 detectores tienen oscilaciones que parecen estar en fase aunque con amplitudes diferentes siendo el APD 11 el que tiene mayor amplitud y el 9 la menor. En esta zona el 9 y el 10 son los más parecidos. El APD 9 muestra una eficiencia ligeramente menor a los otros dos y hace que, a tiempos largos, el histograma del APD 9 quedé debajo de los otros. Preferimos tomar los detectores 10 y 11 que tienen un afterpulsing algo diferente pero eficiencias más parecidas.

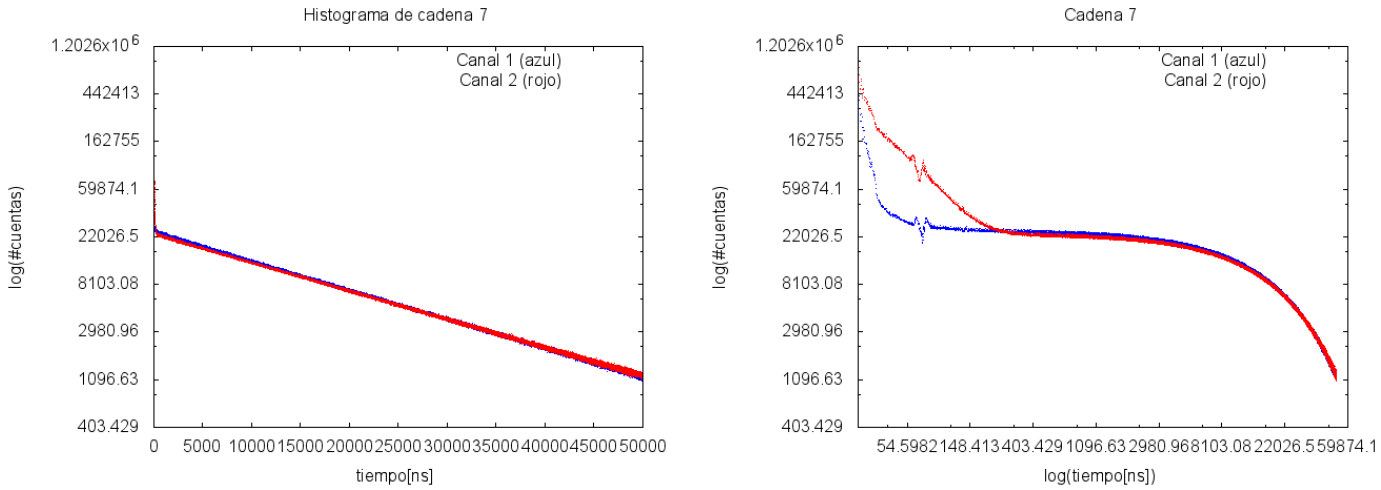


Figura 4.5: Histograma en escala semilog (izquierda) y logarítmica (derecha) de la cadena 7 tomadas con los APDs 6 y 12. El inicio de la gráfica muestra dos curvas muy separadas, la diferencia se minimiza gradualmente.

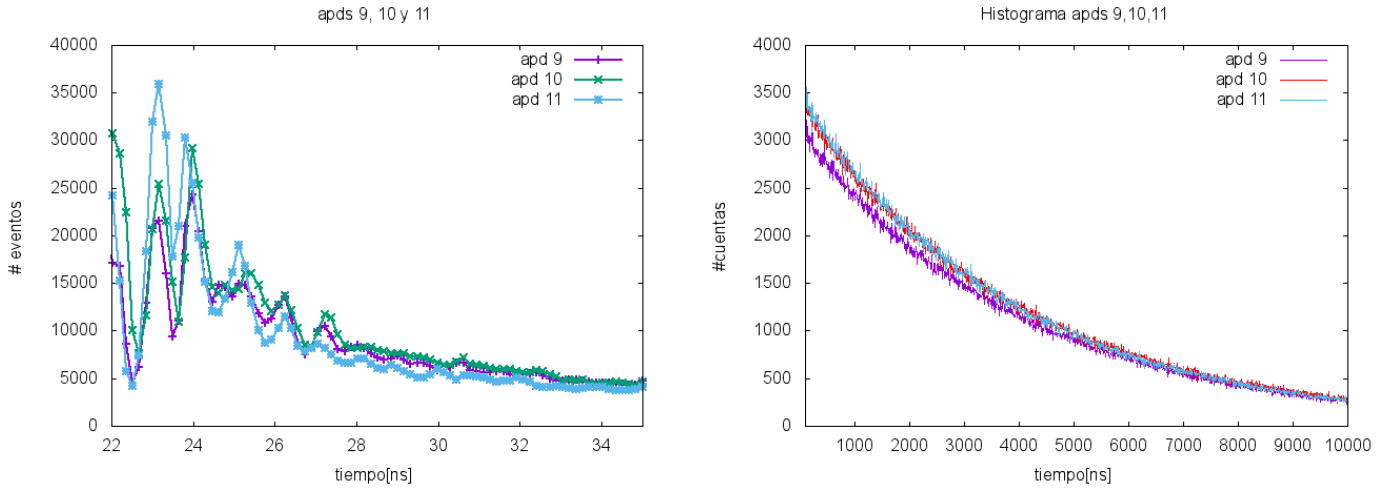


Figura 4.6: Histograma de los APDs 9, 10 y 11, que son los que tienen curvas más parecidas. A la izquierda se muestra el intervalo $[0, 35]$ ns y a la derecha el de $[100, 10000]$ ns.

APD10-11.

Tomé datos para generar una cadena con los detectores 10 y 11 a dos flujos distintos (70 kcs y 700 kcs). Borel para $m = 1$se pasa, pero Borel 2 sigue presentando (aunque en menor medida) exceso de "00" y "11".

Quité eventos por afterpulsing con una ventana de $V_{aft} = 81$ ns y 105.3 ns para el canal 1 y el 2 respectivamente. El balanceo se mantiene aunque siguen existiendo correlaciones. Al eliminar las correlaciones introducidas por el APD, se hacen presentes las correlaciones introducidas por el tiempo muerto de los detectores, el exceso ahora es de bloques "01" y "10".

Puede ser interesante balancear al sistema quitando el afterpulsing desde la adquisición de datos. Esto se puede hacer con el HydraHarp ya que tiene un tiempo muerto para un mismo canal de ≈ 80 ns (aunque la resolución entre canales distintos es de 1 ps).

Comentarios finales de este método.

Hemos encontrado que mantener a nuestro sistema balanceado requiere un trabajo cuidadoso de monitoreo y caracterización del sistema. Eso es suficiente para pasar Normalidad de Borel para $m = 1$. Sin embargo, existen los efectos de afterpulsing y tiempo muerto, inherentes a todo detector de fotones individuales, que compiten entre sí introduciendo correlaciones.

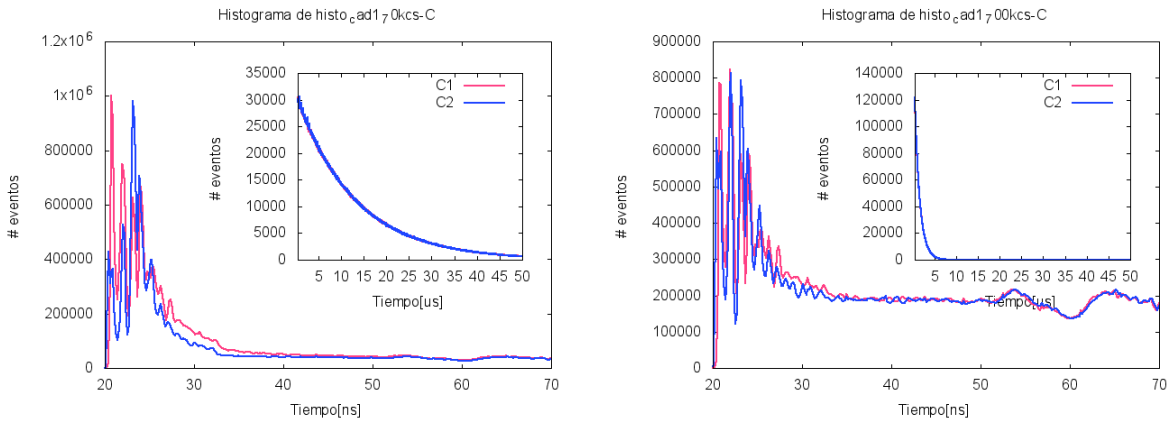


Figura 4.7: Histogramas de con APDs 10 y 11 con flujo de 70 kcs (izq) y 700 kcs (der).

Las correlaciones de afterpulsing son dominantes. Al suprimir los eventos de afterpulsing, el peor escenario es que los detectores sean muy distintos y el sistema se desbalancee completamente. Si los detectores son similares, el tiempo muerto se encarga de que las cadenas fallen Normalidad de Borel. Esto sugiere la idea de que exista un valor de tiempo muerto y de afterpulsing donde haya un equilibrio y las cadenas no estén sesgadas.

Mis resultados ofrecen una explicación de la falla de las cadenas generadas por el grupo de Óptica Cuántica de Viena reportado en [2].

El trabajo presentado es de interés ya que las dificultades en la generación de números al azar, que he encontrado experimentalmente, están presentes en cualquier generador que utilice un PBS y detectores de fotones individuales. Es sorprendente el grado de simetría que se requiere para lograr un buen generador cuántico de números al azar basado en un PBS.

Pese a la sencillez conceptual y directa implementacón de este esquema, estoy convencido de que un generador cuántico de números al azar de uso práctico requiere otro método de generación más robusto ante imperfecciones de detectores y de equipo óptico.

En este esquema del PBS un fotón produce un solo bit. La limitación en el flujo máximo de fotones es el tiempo muerto del detector de fotones individuales, de los cuales los fotodiodos de avalancha son los más utilizados. El tiempo muerto de estos detectores es de decenas de ns, lo que limita la tasa de generación a decenas de Mbits por segundo que es baja para esquemas de QKD [16].

Con la idea de encontrar un método que supere las imperfecciones en la tecnología que hemos utilizado y que tenga una tasa de generación más grande, decidimos probar un método de generación de números al azar basado en diferencias de tiempos de llegada. Este método fue implementado con éxito en [4] con parejas de fotones generados por el proceso de conversión paramétrica descendente (SPDC por sus siglas en inglés).

4.3. Tiempos de llegada.

La idea del método es utilizar la distribución de diferencias de tiempo de llegada de fotones. Esta distribución se divide en dos partes, a través de la mediana de la distribución, con la misma frecuencia de aparición y se asocia un bit a cada bloque.

Los eventos en los detectores se distribuyen en el tiempo t de acuerdo a una distribución exponencial [4], formalmente idéntica al decaimiento radioactivo.

$$\zeta e^{-\zeta t}. \tag{4.1}$$

El parámetro que caracteriza a la distribución es el flujo promedio de fotones (ζ) . La mediana de la distribución es el tiempo τ_0 tal que

$$\int_0^{\tau_0} \zeta e^{-\zeta t} dt = \int_{\tau_0}^{\infty} \zeta e^{-\zeta t} dt = \frac{1}{2}. \tag{4.2}$$

$$\begin{aligned}\int_0^{\tau_0} \zeta e^{-\zeta t} dt &= -\frac{1}{\zeta}\left(e^{-\zeta t}\big|_0^{\tau_0}\right) \\ &= \left(1 - e^{-\zeta \tau_0}\right) \\ &= \frac{1}{2}.\end{aligned} \tag{4.3}$$

Resulta que $\tau_0 = \frac{1}{\zeta} ln(2)$.

El afterpulsing hace que la primera parte de la distribución sea más complicada que una exponencial, así que es necesario suprimirla para lograr una buena estimación de τ_0. La corrección contempla un corrimiento temporal t_a, de modo que la distribución sea $\zeta e^{-\zeta(t-t_a)}$. El valor de τ_0 también sufre el mismo corrimiento $\tau_0 = \frac{1}{\zeta} ln(2) + t_a$.

Generé cadenas con esta corrección y también distinguí entre canales para evitar las diferencias entre los dos detectores.

La primera parte de los programas computacionales, donde implementé este método, es calcular ζ. Después obtiene τ_0. Finalmente tomamos diferencias de tiempo de llegada $(t_1 - t_2)$ de cada evento y las comparamos con τ_0. Hacemos la siguiente asignación

$$\begin{cases} \text{"0"} & \text{si } t_1 - t_2 < \tau_0. \\ \text{"1"} & \text{si } t_1 - t_2 > \tau_0. \\ \emptyset & \text{si } t_1 - t_2 = \tau_0. \end{cases} \tag{4.4}$$

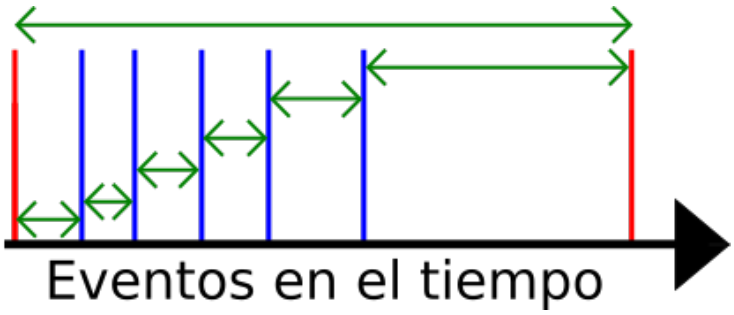


Figura 4.8: Esquema del proceso de generación de las cadenas usando tiempos de llegada. Tomamos diferencias de tiempo entre eventos sucesivos en un mismo canal y las sumamos para obtener el tiempo total. También hay un contador del número de eventos. Los eventos con una separación muy grande (que corresponden a eventos donde el contador del iD800 hace cambios abruptos) se ignoran.

Los datos que utilicé fueron los que ya teníamos de la etapa anterior. Los flujos que utilicé fueron 1.7 Mcs y 130 kcs lo que nos da diferencias de tiempos de llegada promedio de $\frac{1}{1.7\times10^6} = 5.8823 \times 10^{-7} = 0{,}58823$ [μs] y de $\frac{1}{130\times10^3} = 7.69 \times 10^{-6} = 7.69$ [μs].

El flujo promedio obtenido de los programas es de 124 kcs para el flujo de 130 kcs y corresponde a una mediana de 5.6 [μ s].

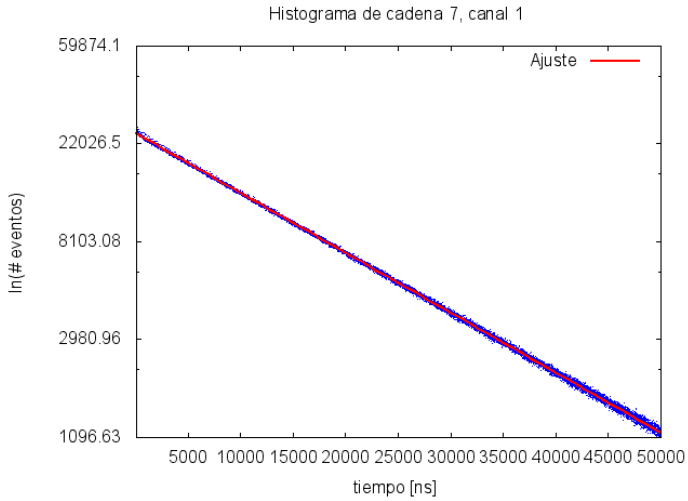
Para el flujo de 1.7 Mcs, el programa nos da un flujo de 1.72 Mcs y una mediana de 0.4 [μ s].

Borel.

Las cadenas fueron generadas con tiempos de llegada excluyendo los eventos separados temporalmente menos de 100 ns y diferenciando entre canales (generando 2 cadenas por cada archivo). El resultado es que no pasan Borel 1.

La figura 4.9 muestra una gráfica semi-log del histograma del canal 1 de la cadena 7. Hice un ajuste de la forma Ne^{-at+b}. En esa misma figura se muestra la matriz de correlación del ajuste.

La razón del fallo de estas cadenas es que el cálculo de la mediana de la distribución estaba sobrevalorada (había más 0 que 1) ya que no contaba algunos tiempos entre eventos. Corregí la anterior y optimicé el valor de t_a para que la cadena 7 fuera Borel normal. Para las otras cadenas el mismo valor de t_a no funciona, en la figura 4.10 se muestran los resultados para la cadena 7 y 4.




```
degrees of freedom    (FIT_NDF)                        : 15399
rms of residuals      (FIT_STDFIT) = sqrt(WSSR/ndf)    : 121.955
variance of residuals (reduced chisquare) = WSSR/ndf   : 14872.9

Final set of parameters            Asymptotic Standard Error
=======================            ==========================
N               = 13577.3          +/- 8.69e+12     (6.4e+10%)
a               = 6.12612e-05      +/- 1.279e-08    (0.02087%)
b               = 0.594622         +/- 6.398e+08    (1.076e+11%)

correlation matrix of the fit parameters:
                N      a      b
N               1.000
a               0.088  1.000
b              -1.000 -0.088  1.000
```

Figura 4.9: En la izquierda se muestra el histograma en escala semi-log de los eventos de la cadena 7 en el canal 1. En rojo se muestra el ajuste a los datos. A la derecha se muestran los parámetros del ajuste.

La razón de esta diferencia de resultados es que la mediana de cada cadena es muy sensible a pequeñas diferencias. El grado de balanceo es tan alto que sólo se logra en intervalos extremadamente restrictivos, de un par de centenas de ps.

En este punto del proyecto pude haber dedicado más tiempo a mejorar los resultados con el método de tiempos de llegada. Sin embargo, decidí probar otra forma de generación.

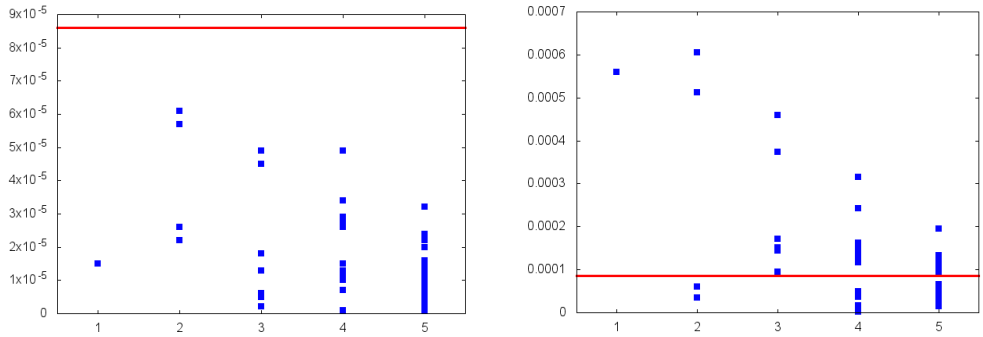


Figura 4.10: Resultados de la prueba de normalidad de Borel para las cadenas generadas con tiempos de llegada en el canal 1 para la cadena 7 (izq.) y 4 (der.). Ajusté el valor de t_a para que la cadena 7 pasara Borel 1. Con ese mismo valor de t_a, generé las demás cadenas.

Comentarios sobre este método.

Este método, por su construcción, siempre permite que se pase Borel 1. Sin embargo, se requiere un cálculo cuidadoso del tiempo medio de la distribución. La simetría en las cadenas generadas es extremadamente sensible a cambios en el valor de τ_0.

En [4] utilizan parejas de fotones, con un flujo más chico que el mio, y obtienen resultados positivos. En este trabajo, el intervalo del tiempo medio es más restrictivo.

4.4. Método basado en la etiqueta de tiempo.

Para mis propósitos, me tomo la libertad de definir una etiqueta de un evento como un conjunto de dos coordenadas: una temporal y otra espacial. Una persona parada en el anden del metro anotando la hora en la que pasa cada metro es un ejemplo de un etiquetador. En este último método que exploré, me interesa sólo la parte temporal de una etiqueta de un evento y es a lo que me refiero con etiqueta de tiempo.

Uno de los primeros métodos de generación cuántica de números al azar utiliza la etiqueta de tiempo de eventos de decaimiento radiactivo [5]. ¿Qué desempeño tiene este esquema con la tecnología actual? ¿Qué tan buena es la calidad de las cadenas producidas? Nuestros datos fueron tomados con un etiquetador de tiempo así que tenemos todos los ingredientes para averiguarlo.

Este esquema requiere dos cosas: un evento cuántico susceptible de ser detectado individualmente y un reloj. Los eventos del proceso cuántico tienen un flujo promedio Φ. El reloj se caracteriza por una frecuencia de operación ν [5].

En caso de tener un reloj lento ($\nu < \Phi$), el esquema consiste en hacer mediciones en intervalos de tiempo constante. Hay un contador que registra el número de eventos, se lee en cada medición y se reinicia. El contador se restringe a valores que van de 0 a $M - 1$ (si $M = 2$ se tiene una cadena binaria). En cada medición se toma el valor del contador para producir un número al azar [5].

Si se cuenta con un reloj rápido ($\nu > \Phi$), el esquema se basa en leer el contador y asignar un "0" ("1") si el número de detecciones es par (impar) [5]. El contador se reinicia en cada iteración.

El método que implementé es ligeramente distinto, ignoro el contador y utilizo sólo la etiqueta temporal. Simplemente asocio un "0" ("1") a los eventos con una etiqueta de tiempo par (impar). O bien, tomando a las etiquetas en binario, tomo el bit menos significativo.

El iD800 tiene una resolución de 81 ps, pero no es estable. Nosotros utilizamos el segundo bit, que hace referencia a 162 ps, y es estable. El valor de Φ para fotones de nuestro láser atenuado es del orden de μs así que se cumple la condición $\nu > \Phi$.

En la figura 4.11 se muestra el formato de salida de cada evento del iD800, el cual consiste de 10 bytes. Los primeros 8 bytes corresponden a la etiqueta de tiempo y los últimos 2 al canal del evento. El formato es "Little Endian" (byte más chico al principio). Se puede apreciar que los bytes del 3 al 8 son constantes, mientras que el byte 1 y 2 (que son los que uso) varian rápidamente.

```
11110110 01010001 11000111 11011101 01010001 00000000 00000000 00000000 00000001 00000000
11001000 00100011 11001000 11011101 01010001 00000000 00000000 00000000 00000010 00000000
10101010 10110011 11001000 11011101 01010001 00000000 00000000 00000000 00000001 00000000
10011010 00011101 11001110 11011101 01010001 00000000 00000000 00000000 00000001 00000000
01111101 01110010 11010000 11011101 01010001 00000000 00000000 00000000 00000010 00000000
10011110 01111001 11010001 11011101 01010001 00000000 00000000 00000000 00000010 00000000
00010011 11001011 11010001 11011101 01010001 00000000 00000000 00000000 00000001 00000000
01110011 01011000 11010011 11011101 01010001 00000000 00000000 00000000 00000001 00000000
00011110 11001000 11010100 11011101 01010001 00000000 00000000 00000000 00000001 00000000
11001110 00000110 11010101 11011101 01010001 00000000 00000000 00000000 00000010 00000000
10001010 01011001 11010111 11011101 01010001 00000000 00000000 00000000 00000010 00000000
10111011 11010100 11010111 11011101 01010001 00000000 00000000 00000000 00000010 00000000
00001111 00011101 11011000 11011101 01010001 00000000 00000000 00000000 00000010 00000000
00010011 10111111 11011100 11011101 01010001 00000000 00000000 00000000 00000010 00000000
11101010 01111011 11011101 11011101 01010001 00000000 00000000 00000000 00000010 00000000
11111110 01001000 11011110 11011101 01010001 00000000 00000000 00000000 00000010 00000000
11011100 01010111 11011110 11011101 01010001 00000000 00000000 00000000 00000010 00000000
```

Figura 4.11: Imagen de la salida del iD800 funcionando con etiquetas de tiempo. Cada evento consiste de 10 bytes escritos en formato "Little Endian". Los primeros 8 bytes refieren a la etiqueta temporal y los 2 restantes al canal.

Las cadenas generadas pasan Normalidad de Borel sin problemas. La figura 4.12 derecha muestra los resultados para la cadena 7.

Bits individuales.

Es factible que el método funcione para los bits siguientes de la etiqueta de tiempo ya que la condición necesaria de este método es válida para ellos. Es claro de la figura 4.11 que a partir del bit 16 (que corresponde a $0.081 \times (2^{15}) = 2.65\ \mu s$) hay una constancia evidente. ¿ Hasta qué bit funciona el método? Realicé la prueba con el bit n-ésimo y estos son los resultados.

Resultados.

Los resultados de Borel se muestran en las figuras 4.12 - 4.14. El bit 1 no pasa la prueba, indicando que este bin (81 ps) no es estable y presenta una asimetría en el número de etiquetas pares e impares. El bit 2 y 3 pasan la prueba cómodamente. El bit 4 también tiene buenos resultados excepto por la cadena 7 que falla en $m = 2$ y $m = 3$. Del bit 5 hacia adelante, las cadenas no son Borel normales.

Para un bit > 5, las cadenas están balanceadas, pero existen correlaciones, que seguramente vienen dadas por la constancia de ese bit. Hay exceso de dobletes y tripletes de bits repetidos, es decir de "00", "11", "000" y "111". Que indica que el bit se mantiene constante unos 3-4 eventos. Este comportamiento se amplifica en los siguientes bits. El bit 5 corresponde a $(2^4) \times 0.081 = 1.296$ [ns] que es 1000 veces más chico que el tiempo medio entre eventos.

Entonces el método funciona para los primeros 4 bits excluyendo el primero que tiene un sesgo en el iD800.

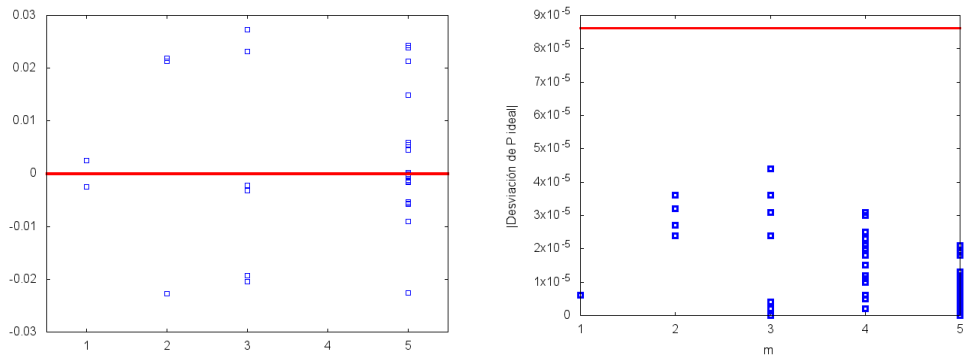


Figura 4.12: Resultados de la prueba de normalidad de Borel para la cadena 7 generada con el bit 1 y 2. En rojo se muestran las cotas superior e inferior para determinar si una cadena es Borel normal. El bit 1 presenta un sesgo en la cantidad de etiquetas pares e impares que hacen que falle las pruebas, a este nivel de resollución el iD800 es inestable. Para el bit 2 los resultados son positivos.

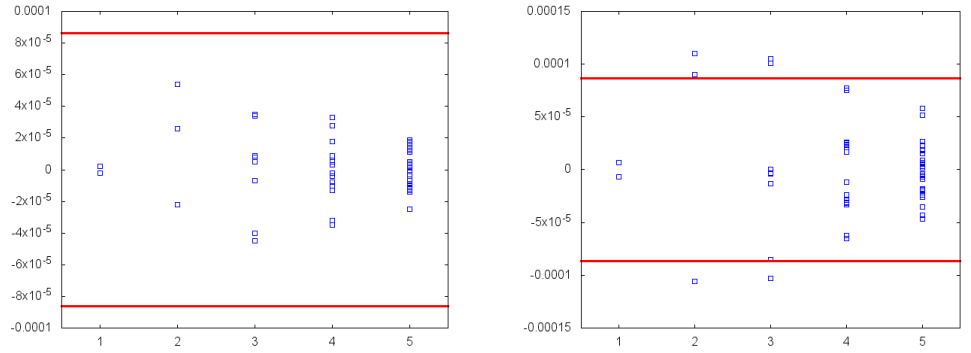


Figura 4.13: Resultados de la prueba de normalidad de Borel para la cadena 7 generada con el bit 3 y 4. En rojo se muestran las cotas superior e inferior para determinar si una cadena es Borel normal. La cadena 3 pasa las pruebas. La cadena 4 no pasa los niveles 2 y 3. El bit 4 es el bit límite al que el método funciona para bits individuales.

Las cadenas generadas con un solo bit tienen una tasa de producción de 1 bit por evento. Dado que

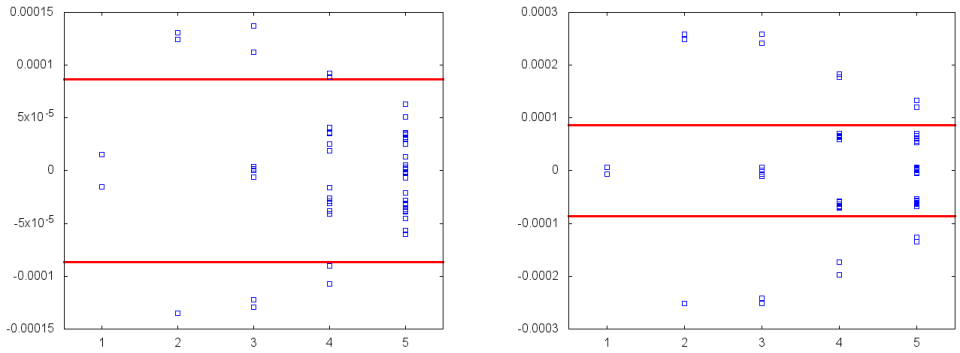


Figura 4.14: Resultados de la prueba de normalidad de Borel para la cadena 7 generada con el bit 5 y 6. En rojo se muestran las cotas superior e inferior para determinar si una cadena es Borel normal. La cadena 3 pasa las pruebas, mientras que la 4 no pasa los niveles 2 y 3.

3 bits generan cadenas que pasan Normalidad de Borel, ¿qué tan aleatorias son las cadenas generadas al concatenar varios bits de una misma etiqueta de tiempo?

Concatenar varios bits de un mismo evento.

De una misma etiqueta de tiempo, tomé los primeros N bits y los fui concatenando con los demás eventos para generar cadenas binarias. De esta forma se amplifica un factor N la tasa de producción de bits de la cadena. Para evitar cadenas excesivamente largas, limité la longitud de todas las cadenas a 5×10^9 bits.

Borel.

He generado cadenas usando los bits de las posiciones 2 (la 1 tiene un sesgo que no queremos heredar) hasta la 24. Todas las cadenas pasan bastante bien las pruebas de Normalidad de Borel. En las figuras 4.15 y 4.17 se muestran los resultados para 4, 5, 6 y 7 bits.

La prueba de Normalidad de Borel no ve la constancia del bit 15 y posteriores. La razón es que Normalidad de Borel mide la aparición de un bloque de bits de manera global (en toda la cadena y no en subcadenas de longitud menor). Los bloques constantes se compensan en cadenas suficientemente largas.

Las pruebas de NIST son un buen candidato para detectar estos sesgos.

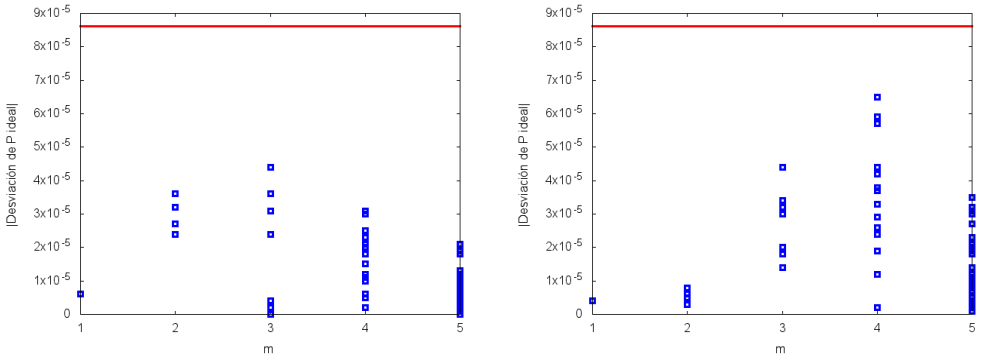


Figura 4.15: Resultados de la prueba de normalidad de Borel para la cadena 7 generada concatenando 1 y 2 bits (empezando con el bit 2). En rojo se muestra la cota superior para determinar si una cadena es Borel normal.

NIST.

Subdividí cada cadena en otras de 10^9 caracteres y les apliqué la batería de NIST, cada análisis tuvo 1000 subcadenas con los cuales obtener un resultado estadístico. Los resultados son buenos hasta concatenar 8 bits.

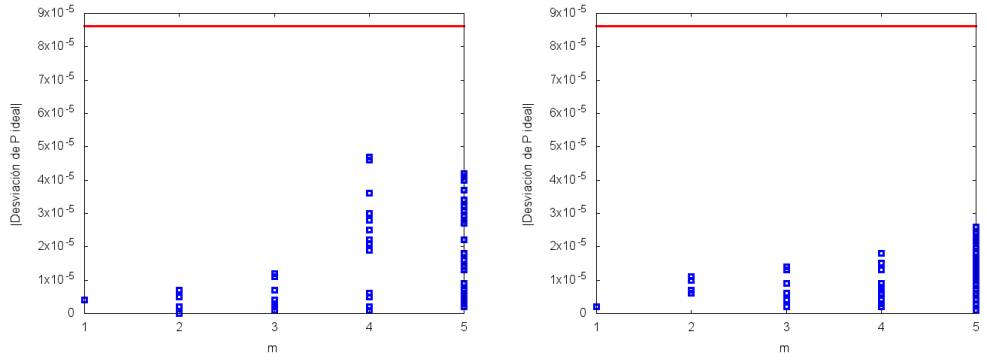


Figura 4.16: Resultados de la prueba de normalidad de Borel para la cadena 7 generada concatenando 3 y 4 bits. En rojo se muestra la cota superior para determinar si una cadena es Borel normal.

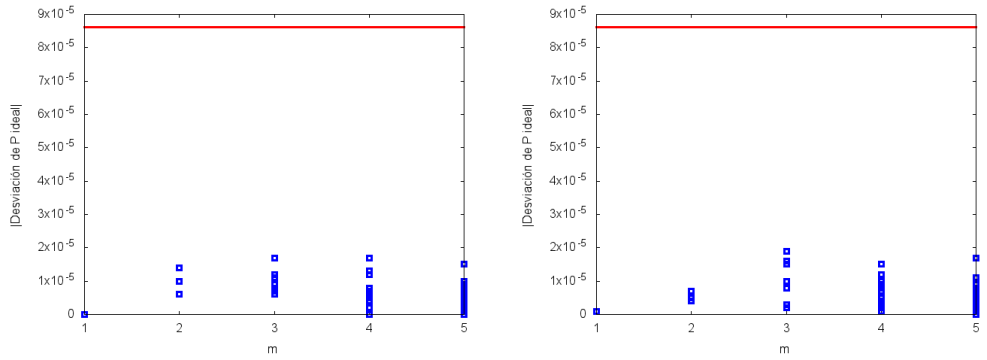


Figura 4.17: Resultados de la prueba de normalidad de Borel para la cadena 7 concatenando 5 y 6 bits. En rojo se muestra la cota superior para determinar si una cadena es Borel normal.

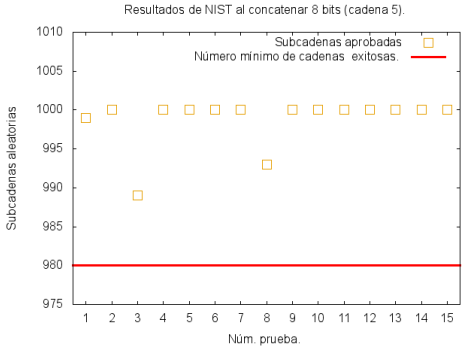


Figura 4.18: Resultados de la batería de NIST al concatenar 8 bits. Los resultados corresponden a mil subcadenas de 10^6 de la cadena 5. Para esta cantidad de subcadenas, el número mínimo de subcadenas aleatorias debe ser de 9800 para tener resultados positivos.

Capítulo 5

Conclusiones.

Si se quiere generar un número cuya naturaleza sea aleatoria se debe recurrir a mediciones en sistemas cuánticos individuales. En este trabajo, implementé un esquema de generación de números al azar conceptualmente muy claro y directo basado en fotones incidentes en un PBS. Experimentalmente, con un mecanismo de retroalimentación, demostré que es posible mantener al sistema balanceado para generar cadenas binarias, de 4.3 Gbits, con una diferencia en la proporción del bit "1" y el "0" menor a 8.6×10^{-5}, precisión necesaria para lograr obtener un generador cuántico de números al azar de alta calidad.

El resultado negativo reportado en [2], donde un generador cuántico de números al azar produce cadenas con patrones, no contradice el que la mecánica cuántica sea aleatoria. La explicación de tal resultado la he encontrado en diferencias en afterpulsing, tiempo muerto y eficiencia de los dos detectores. En general, cualquier generador cuántico de números al azar que se base en el método del PBS, no haga post-procesamiento y utilice detectores de fotones individuales comerciales, no mejores que los existen actualmente, sufrirá los mismos sesgos. Futuros generadores de números al azar deberán superar las imperfecciones de la tecnología actual, ya hay investigación y propuestas de generadores más robustos basados en tiempos de llegada o fluctuaciones en la fase de un láser, el lector interesado puede consultar estos esquemas en [5] y las referencias que allí se encuentran.

En esta búsqueda de un método de generación de números al azar robusto, retomé, a la luz de la tecnología actual, una forma de generación basada en la etiqueta temporal de cada evento que fue exitoso. He extendido el método logrando una tasa de producción a 8 bits por fotón. Todas las cadenas obtenidas son Borel Normales, aunque hay un sesgo no detectado por la prueba debido a su carácter global. La batería de NIST detectó esos patrones imponiendo un límite a la tasa de generación de mi experimento a 13.5 Mbps. El esquema de las etiquetas temporales es sencillo, no requiere post-procesamiento, tiene un mínimo costo computacional y permite generar varios bits por evento. Sería interesante considerarlo para un dispositivo de uso práctico, sus posibles aplicaciones son juegos de suerte en línea, simulaciones numéricas y seguridad criptográfica.

Como trabajo a futuro se podría diseñar y realizar el experimento con óptica integrada con la idea de obtener un dispositivo de uso práctico. La limitación inmediata es escalar el costo del experimento: los aparatos que utilicé son dispositivos de punta que son muy caros principalmente los fotodetectores y el etiquetador temporal. Otra posible línea de trabajo es generar números al azar certificados mediante desigualdades de Bell, se requeriría implementar una buena fuente de fotones enredados lo que aumenta de inmediato el tamaño del experimento.

Apéndice A

Un contexto cuántico.

La Mecánica Cuántica es un marco formal dentro del cual podemos hacer predicciones para ciertos sistemas físicos. Los libros de texto establecen una serie de postulados en los que se basa la teoría. A manera de contextualizar nuestro experimento repito estos postulados de la MC no relativista para una partícula [17, 18].

El estado de una partícula se describe con un vector de un espacio de Hilbert H.

La evolución de una partícula aislada se hace mediante una transformación unitaria $\hat{U}$. Si $|\psi\rangle$ es el estado a un tiempo t_1 y $|\psi^{'}\rangle$ el estado a un tiempo t_2, entonces $|\psi^{'}\rangle = \hat{U}\,|\psi\rangle$.

La evolución temporal del estado se describe mediante la ecuación de Schrödinger: $i\hbar\frac{d|\psi\rangle}{dt} = \hat{H}\,|\psi\rangle$, donde el operador $\hat{H}$ es el hamiltoniano del sistema.

Mediciones [17].

Se describen mediante un operador $\hat{M}$ hermitiano que actúa en el espacio de Hilbert de la partícula. $\hat{M}$ tiene estados propios $\{|\phi_m\rangle\}$, que forman una base ortonormal, con valores propios λ_m. Un estado $|\psi\rangle$ se puede expresar como una superposición coherente de $\{|\phi_m\rangle\}$: $|\psi\rangle = \sum_m c_m\,|\phi_m\rangle$. Los coeficientes c_k representan amplitudes de probabilidad de encontrar al sistema en el estado $|\phi_k\rangle$.

El valor de expectación de $\hat{M}$ se denota por $\langle\hat{M}\rangle$ y se define como $\langle\hat{M}\rangle = \langle\psi|\hat{M}|\psi\rangle$.

La desviación estándar es una medida de la dispersión de los resultados al hacer mediciones de $\hat{M}$ sobre un ensamble de estados $|\psi\rangle$:

$$\Delta(\hat{M}) = \sqrt{\langle\hat{M}^2\rangle - \langle\hat{M}\rangle^2}. \tag{A.1}$$

Desigualdades de Heisenberg.

Consideremos dos operadores $\hat{A}$ y $\hat{B}$. Si se cumple que

$$\Big[\hat{A},\hat{B}\Big] = \hat{A}\hat{B} - \hat{B}\hat{A} = 0, \tag{A.2}$$

entonces existe una base común de estados propios de $\hat{A}$ y de $\hat{B}$ donde se describe al sistema. En este caso, decimos que $\hat{A}$ y $\hat{B}$ son compatibles. La información que podemos obtener de las mediciones de $\hat{A}$ y $\hat{B}$ no se afectan entre sí por lo que podemos efectuarlas en un orden arbitrario.

La negación de lo anterior define a los observables incompatibles. Para ellos el conmutador es no nulo y la medición es sensible al orden de la medición.

Dos operadores son conjugados si

$$\Big[A,B\Big] = ih. \tag{A.3}$$

En este caso se puede demostrar formalmente la siguiente desigualdad [17, 18]

$$\Delta A\Delta B \geq \frac{1}{2}\Big|[A,B]\Big|. \tag{A.4}$$

Que nos dice que las dispersiones en los observables está acotada inferiormente de manera natural.

Nuestro experimento en este contexto.

En mi experimento, el espacio de Hilbert que nos interesa es el de la polarización de los fotones y es bidimensional.

Partimos de $|0\rangle$, aplicamos al sistema una transformación unitaria conocida como Hadamard H [17]: $|\psi\rangle = \hat{H}\,|0\rangle = \frac{1}{\sqrt{2}}[\,|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\,]\,|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Finalmente hacemos una medición en la base canónica y obtenemos las probabilidades de medir $|0\rangle$ y $|1\rangle$: $P_{|0\rangle} = |\langle 0|\psi\rangle|^2 = \left|\langle 0|\frac{|0\rangle+|1\rangle}{\sqrt{2}}\rangle\right|^2 = \frac{1}{2}$.

$P_{|1\rangle} = |\langle 1|\psi\rangle|^2 = \left|\langle 1|\frac{|0\rangle+|1\rangle}{\sqrt{2}}\rangle\right|^2 = \frac{1}{2}$.

Apéndice B

Programa de LabView y de generación de cadenas.

Programa de Labview con potenciómetros.

El esquema del programa consiste en inicializar los aparatos, hacer la retroalimentación del sistema y tomar datos.

En este apéndice se muestra el programa desarrollado.

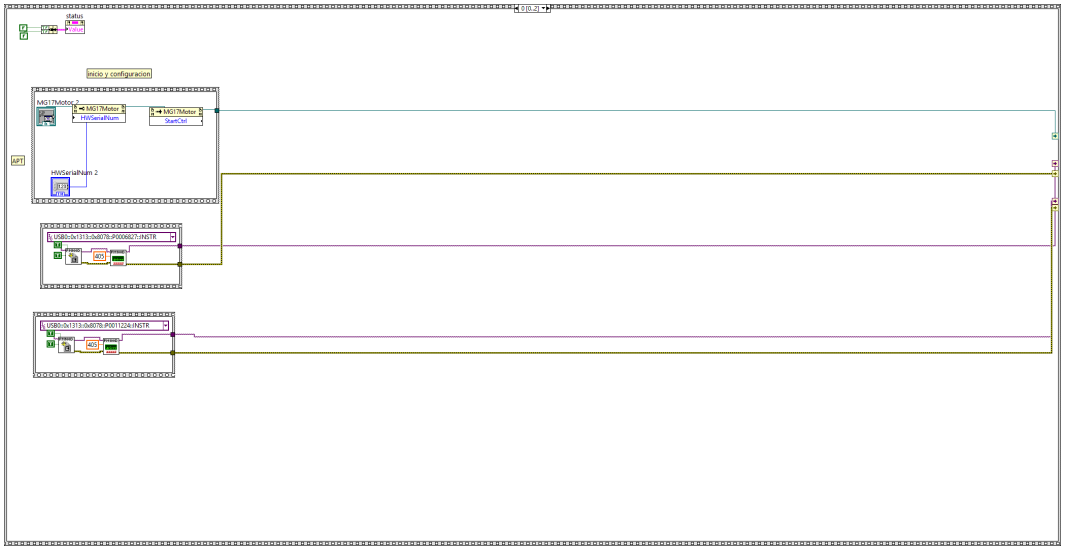


Figura B.1: Ventana de inicialización del motor y los dos potenciómetros, es necesario especificar la longitud de onda en la que se va a medir la potencia (405 nm).

Programa de Labview con APDs.

El programa que utiliza APDs es análogo al de potenciómetros. La parte que fue necesario cambiar es la adquisición de datos, para la cual nos basamos en el programa del iD800.

Programa muestra para analizar las cadenas.

Las siguientes imágenes muestran el programa para generar cadenas usando las salidas de un PBS sin supresión de afterpulsing. El programa carga los datos a memoria y los procesa. De esta forma el programa termina de correr ≈ 5 Giga eventos en un par de minutos.

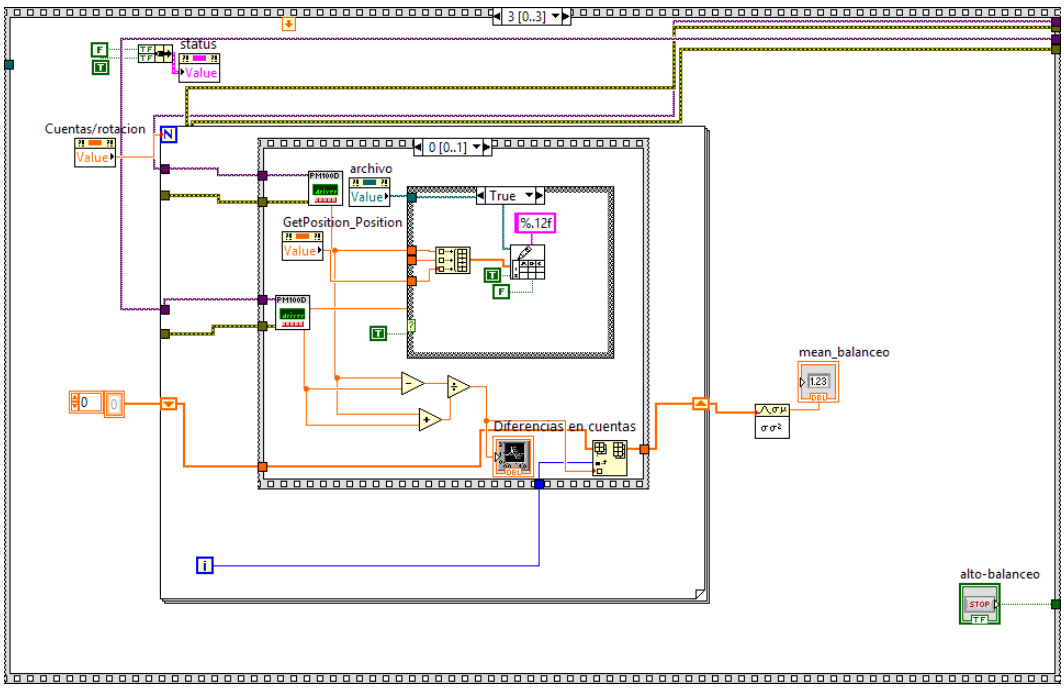


Figura B.2: Se muestra el ciclo donde se hace la toma de datos, se calcula el valor de R y se almacenan los datos. El programa adquiere un número N de mediciones de potencia. En cada iteración se guardan los datos y se calcula el factor de balanceo. Al final de las N mediciones se toma el promedio del factor de balanceo con el que se realiza la retroalimentación.

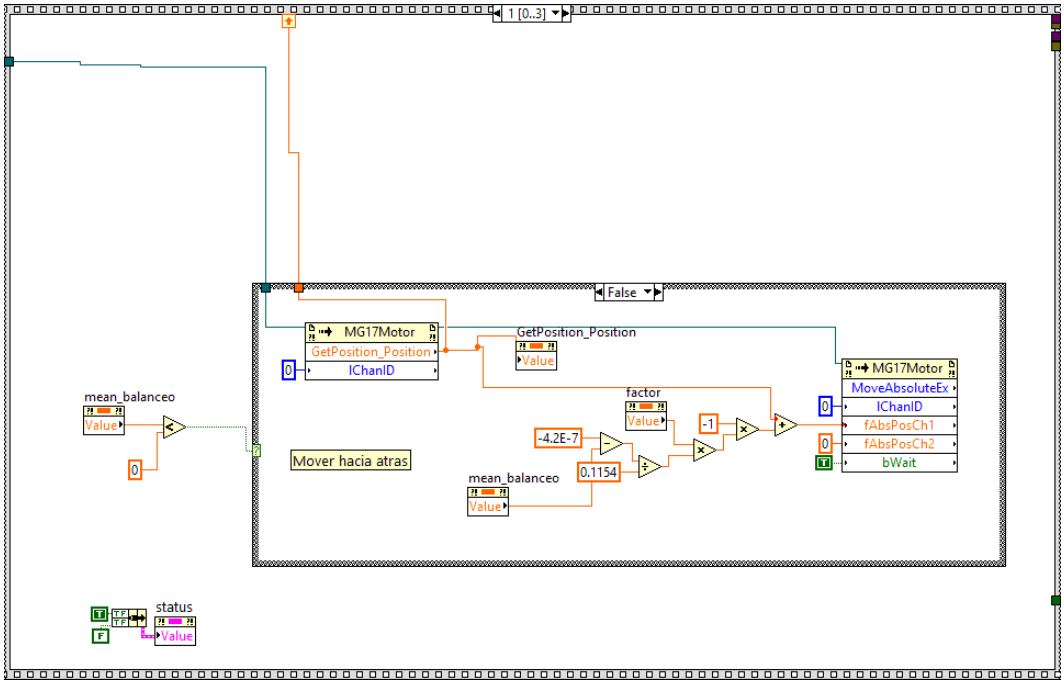


Figura B.3: Ventana donde se lleva a cabo la retroalimentación. Se distingue si el balanceo es positivo o negativo y se implementa una rotación, basada en la caracterización previa, apropiada para centrar al sistema.

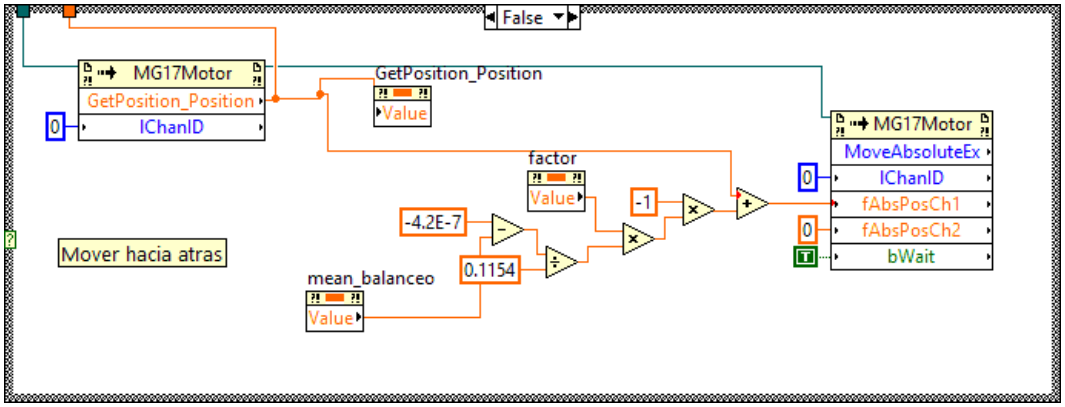


Figura B.4: Implememtación de la rotación hacia adelante con la fucnión de balanceo.

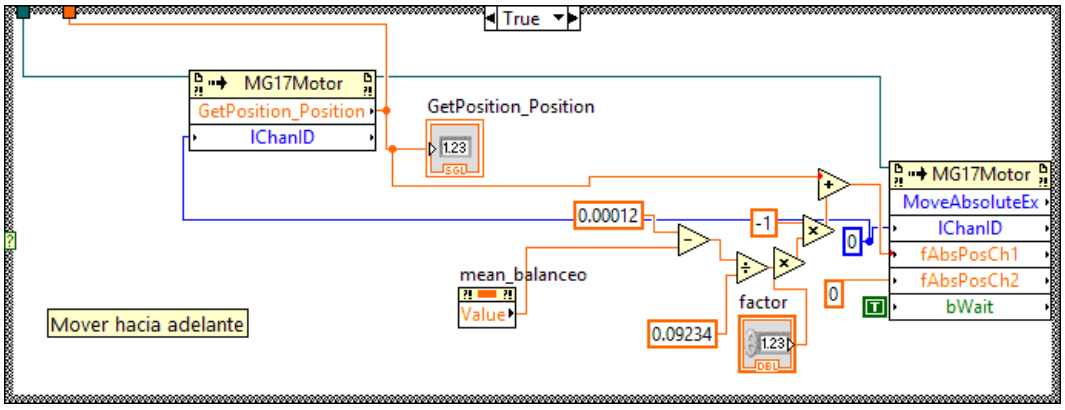


Figura B.5: Implememtación de la rotación hacia atrás con la función de balanceo.

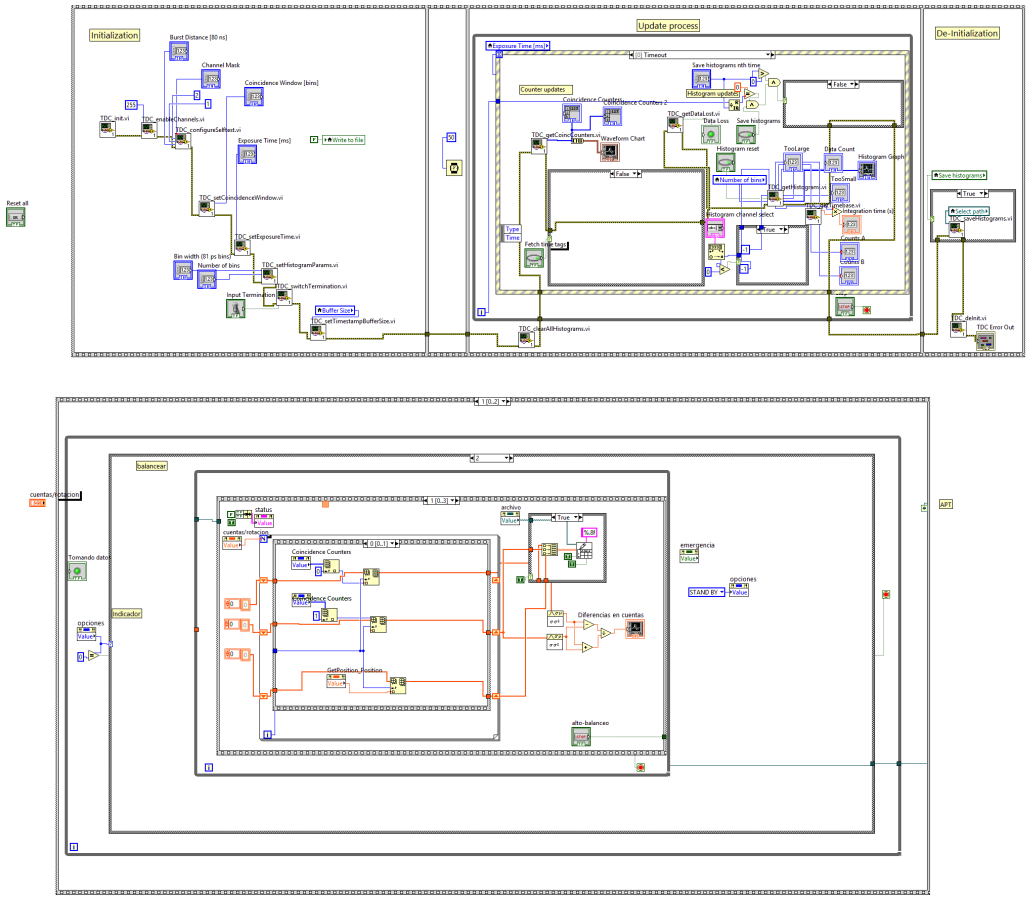


Figura B.6: Diagrama de bloques del programa implementado en LabView. Arriba se muestra el programa del fabricante del iD800 y abajo el nuestro.

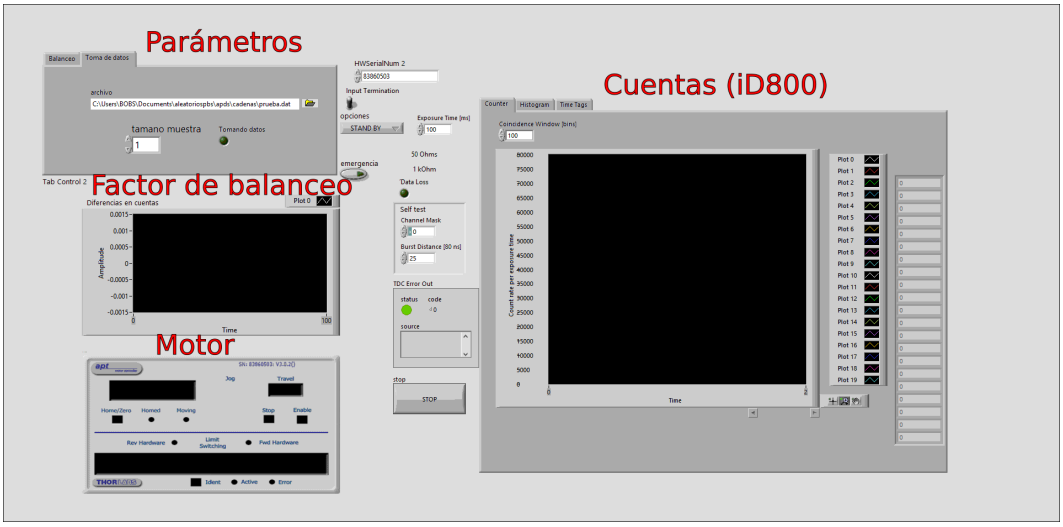


Figura B.7: Imagen de la interfaz del programa implementado en LabView. Desde aquí se puede modificar los parámetros, ver la evolución del factor de balanceo, el ángulo actual del motor y las cuentas en cada canal. Los datos se actualizan en tiempo real.

```c
#include<stdio.h>
#include<stdlib.h>
#include<unistd.h>
#include<sys/types.h>
#include<sys/stat.h>
#include<fcntl.h>
#include<errno.h>
#include<string.h>
#include<math.h>

#define LONG1 1000000
#define LIMITE 5000000000

int main (int argc,char **argv){

        long int leidos;
        long int bescribir;
        long int acumulados;
        char *ptr;
        int fp,pf;
        char *pointers, *ptrs;
        char *pointercanal;

        if(argc<3){
                fprintf(stderr,"USO:%s [ARCHIVO ENTRADA] [ARCHIVO SALIDA ]\n",argv[0]);
                exit(0);
        }
        fp=open(argv[1],O_RDONLY);
        pf=open(argv[2],O_WRONLY | O_TRUNC | O_CREAT,0644);

        if(fp<0 || pf<0 ){
                fprintf(stderr,"problema al abrir archivo(error: %s)\n",strerror(errno));
                exit(0);
      }
```

Figura B.8: Imágen del código para generar cadenas binarias mediante el método del PBS sin quitar eventos de afterpulsing. En esta primera parte se definen variables y se abren los archivos de lectura y escritura.

```
                exit(0);
        }

        ptr=(char*)((void*)malloc(10*LONG1));
        ptrs=(void *)malloc(LONG1);

        acumulados=0;
        bescribir=0;
        while(  ( leidos=read(fp,ptr,10*LONG1)/10 )>0 && acumulados<LIMITE){
                acumulados+=leidos;
                pointercanal=ptr + 8;
                leidos--;
                pointers = ptrs;
                while(leidos>0){
                        if(*pointercanal==0x01){
                                *pointers='1';
                        }else{
                                *pointers='0';
                        }
                        pointers++;
                        bescribir++;
                        pointercanal=pointercanal + 10;
                        leidos--;
                }
                write(pf,ptrs,bescribir);
                bescribir=0;
        }

        free(ptr);
        free(ptrs);
        close(fp);
        close(pf);
        return 0;
}
```

Figura B.9: Imágen del código para generar cadenas binarias mediante el método del PBS sin quitar eventos de afterpulsing. Muestro el ciclo del programa: se lee el canal de cada evento asignando su bit correspondiente.

Apéndice C

Equipo utilizado.

En esta apéndice se menciona el equipo utilizado y se da una descripción breve del funcionamiento de algunos de sus elementos.

APD.

El funcionamiento de un APD (por las siglas en inglés fotodiodo de avalancha) consiste en la conversión de fotones en cascadas de electrones, y la detección de la corriente producida. Un APD es una unión pn que opera en la zona de corriente negativa de su curva de corriente contra voltaje. En esta configuración, se crea un campo eléctrico muy intenso que acelera a los fotoelectrones, liberando más electrones mediante colisiones. En cada evento, las cargas residuales deben ser eliminadas por un circuito [19].

Los APDs que utilicé son del modelo SPCM-AQRH-13-FC marca Excellitas y están hechos de silicio. Generan un pulso TTL por cada evento y lo mandan a una salida BNC. El rango de temperatura en el que funciona es de $5°C$ y $70°C$. El tiempo muerto es de 20 ns. Tiene 250 cuentas oscuras por segundo. El flujo antes de saturación es de 20 Mcs [20].

En las últimas décadas, han habido mejoras en los detectores de fotones individuales. Las características de los fotodetectores más importantes se resumen a continuación [21].

Rango espectral.

Los fotodetectores funcionan en un rango de frecuencias determinado por el material del que está hecho. Generalmente se usan en el rango de luz visible e IR.

Tiempo muerto.

Después de cada evento registrado en el APD, el detector debe 'recuperarse' para su siguiente registro dejando una ventana en la que no puede contar eventos. Este tiempo puede depender de diversos factores uno de ellos es la electrónica asociada. El tiempo muerto puede alagarse intencionalmente para disminuir el ruido por afterpulsing.

Cuentas oscuras.

Son las cuentas correspondientes a detecciones 'falsas' o no deseadas. Puede deberse a ruido externo (que los detectores no estén bien aislados del exterior y que haya iluminación) o a las características del detector. Se puede disminuir con coincidencias

Eficiencia.

Se define la eficiencia η de un detector como la probabilidad de que un fotón que llegue al detector sea registrado.

$$\eta = \frac{R_{registrado}}{R_{incidente}} \tag{C.1}$$

R significa número de fotones.

Aparato	Modelo (Thorlabs)	Especificaciones
Lámina de media onda	WPH05M-532	Funcionamiento óptimo en 532 nm
Polarizador	GTH10M-B	Razón de extinción = 100 000 : 1
Motor	PRM1Z8	Rotación mínima 25 arcsec $\approx 6.9 \times 10^{-3}$ grados
PBS	PBS101	Funcionamiento óptimo en 420-680 nm
Sensor de potencia	S121-C	Rango de potencia 500 nW - 500 mW en 400 - 1100 nm

Tabla C.1: Aparatos utilizados y algunas especificaciones.

Tiempo de jitter.

El tiempo que transcurre entre la absorción de un fotón por el detector y la generación de una señal tiene una distribución (muchas veces gaussiana) con una dispersión. Estas variaciones de tiempo se conocen como el jitter del detector (que puede variar de decenas a centenas de ps). Se mide con láseres pulsados y electrónica rápida.

Afterpulsing.

El afterpulsing es un efecto que consiste en eventos posteriores a la detección de un solo fotón. El mecanismo para eliminar las cargas residuales de un APD no es completamente eficiente, las cargas no neutralizadas pueden comenzar una avalancha de electrones que será detectada como si se tratara de un fotón [22].

Etiquetador de eventos.

iD800.

El iD800 consiste de un circuito ASIC (application-specific integrated circuit) y una tarjeta FPGA (field programmable array). El ASIC recoge, guarda y envía la información de los 8 canales hacia la FPGA. En esta unidad, se colocan etiquetas de tiempo y se realiza el conteo de coincidencias.

La interface del iD800 se puede hacer desde un programa del desarrollador, LabView o la terminal. La salida puede hacerse en varios formatos, yo la utilicé en binario. Los eventos se imprimen de manera secuencial, cada evento consiste de 8 bytes con la etiqueta de tiempo y 2 correspondientes al canal del evento. La resolución mínima es de 81 ps. Funciona como etiquetador de eventos hasta 3 Mcs

Láser.

Consideremos un material dopado con exceso de electrones (tipo n) y otro con exceso de agujeros (tipo p), si unimos los materiales obtenemos una región caracterizada por un voltaje que previene a las cargas difundirse y recombinarse. Al aplicar un voltaje en esta zona, podemos hacer que las cargas se recombinen generando fotones en el proceso. Si no hay una cavidad, la fuente de luz obtenida es un LED. Si hay una cavidad óptica, diseñada apropiadamente, se puede amplificar la luz mediante el proceso de emisión estimulada y se tiene un diodo láser [23].

Utilicé un láser diodo de 405 nm, modelo OBIS405LX, de 100 mW, con un modo gaussiano (TEM_{00}).

La siguiente tabla resume algunas características del equipo utilizado.

Apéndice D

Revisión de artículos relacionados con el trabajo presentado.

Experimental evidence of quantum randomness incomputability [2].

Los autores analizan cadenas de $2^{32} \approx 4.3 \times 10^9$ binarias, generadas por un fenómeno cuántico y por software. El objetivo es distinguir los generadores de números pseudo-aleatorios de las fuentes cuánticas.

Las fuentes que usan son las de Quantis [24] y las obtenidas de fotones incidentes en un BS (el experimento lo realizó el grupo de Óptica Cuántica IQOQI de Viena).

Sobre el dispositivo del grupo de Viena, su fuente es un LED azul que incide en un BS (sin sensitividad a polarización). No realizan post-procesamiento, aunque el sistema se mantiene bajo monitoreo constante que garantiza que la cantidad de "0" y "1" sea simétrica. Sorpresivamente, estas cadenas no pasan la prueba de Normalidad de Borel para $m = 2$, 3 y 4. Las demás cadenas pasan las pruebas utilizadas.

El artículo cierra con una nota de precaución sobre la imposibilidad de decir que una cadena es absolutamente aleatoria. Lo es respecto a una clase grande de comportamientos o leyes conocidas.

A fast and compact quantum random number generator [3].

El GNA presentado se desarrolló para comprobar una violación de las desigualdades de Bell.

Los autores presentan el esquema de 2 GNA. El primero consiste en una fuente de luz y un BS 50:50, el estado del fotón es $\frac{|R\rangle+|T\rangle}{\sqrt{2}}$. Si en lugar de un BS, se usa un PBS, es necesario un polarizador orientado a 45° de manera que el estado sea $\frac{|H\rangle+|V\rangle}{\sqrt{2}}$. En ambos casos, los dos posibles resultados (reflección o transmisión) son equiprobables. Su fuente es un LED rojo (tiempo de coherencia < 1 ps) de manera que no hay interferencia entre fotones y se eliminan efectos de estadística.

La cadena binaria se genera con un switch que cambia su valor de 0 a 1 (1 a 0) con la detección de un evento en el Detector 1 (2). Los tiempos de duración de cada valor son aleatorios.

En este artículo se menciona que a la fecha no existe definición rigurosa de azar. Las pruebas que existen buscan encontrar regularidades ocultas o pequeñas (entre más ocultas la prueba es mejor) y entre más pruebas pase una cadena, tendremos mayor certeza de su carácter aleatorio.

Las pruebas que usaron son: equiprobabilidad de 0 y 1, autocorrelación de la señal temporal y distribución de intervalos de tiempo (que debe ser poissoniana). Sus resultados son positivos.

Optical Quantum Random Generator [25].

La aleatoriedad de una cadena puede ser puesta a prueba mas no demostrada. De ahí la importancia de asegurarse de usar un proceso cuántico que sabemos es aleatorio por naturaleza.

Su implementación consiste en un LED de 880 nm pulsado. La salida del láser se acopla a una fibra monomodo, que a su salida tiene otras dos fibras multimodo juntas conectadas a un mismo APD. Una fibra es más larga e introduce un retraso de 60 ns. La señal del detector se analiza con la señal del pulsador y se asocia un "0" con la trayectoria corta y un "1" con la larga.

Se espera que la distribución de fotones se aproxime a una poissoniana. Los autores dicen que hay eventos espurios, que se pueden disminuir usando coincidencias con una ventana de 10 ns.

Usar un solo detector evita la asimetría que podría existir entre dos detectores distintos. El autor menciona un sesgo debido a las eficiencias diferentes entre dos detectores. Esto ocurre en el régimen de un flujo alto.

Las pruebas que aplican son de autocorrelación entre bits separados una distancia de n bits, entropía y la prueba de Maurer. Sus resultados son positivos.

Scheme for a quantum random number generator [26].

Presentan un esquema de generación de números al azar basado en un prisma de Fresnel. Un láser diodo pulsado y atenuado al nivel de fotones individuales, inciden en un prisma. El prisma cambia la polarización lineal a circular (R o L) con la misma probabilidad.

Cada componente de polarización (R o L) se detecta con un APD. Proponen evitar las cuentas oscuras sincronizando los APDs con el pulso del láser. Otro problema es que los detectores no son idénticos y el post procesar, introduce problemas de números pseudo-aleatorios, tampoco es viable. La solución que ofrecen es cambiar el bit asociado a cada salida del detector por un periodo de tiempo. Esta técnica puede tener complicaciones relacionadas con el periodo de cambio de asignación. Se requiere cambiar aleatoriamente, ingeniosamente, proponen usar la misma cadena, producida en tiempo real, para decidir si hacer el cambio o no.

An On demand optical RNG with In-Future action and ultra fast response [27].

Los autores destacan 3 cosas de su GNA: tiempo de espera corto (9.8 ± 0.2 ns) (tiempo entre el requerimiento de un bit al azar y su generación), el proceso físico ocurre después de la petición y se tiene una eficiencia de producción del 100 %.

Su dispositivo inicia con un pulso como trigger, que va a un circuito controlador de un diodo láser (LD), montado en una pieza con grados de libertad en xy. Detrás del LD hay un pinhole y un detector. El proceso cuántico es la emisión de cuantos de luz detectables. Hay un sistema electrónico en paralelo que abre una ventana para coincidencias. Si hay (o no) detección se asigna un 1 (0). Como siempre hay respuesta del sistema, el GNA es totalmente eficiente.

Testing Quantum Randomness in Single-photon Polarization Measurements With the NIST Test Suite [28].

Usan una fuente de SPDC, un fotón actúa como anunciante y el otro se prepara en un estado de polarización diagonal y es mandado a un PBS. Obtienen coincidencias mediante un sistema electrónico. Asignan "0" y "1" a las detecciones con fotón con polarización vertical u horizontal.

La tasa de prodcción es de 10 kHz. Realizan un histograma de coincidencias por fracción de bin y la ajustan a una poissoniana (ya que la fuente es coherente) para determinar el número de eventos. Utilizan la batería de NIST para analizar sus cadenas. Los resultados son positivos.

On-chip generation of high-order single-photon W-states [29].

Los autores generan estados W en modos espaciales en un circuito integrado. Un estado W es una superposición, con mismo peso para cada estado, de w estados propios de un operador. Como una aplicación, generan números al azar.

A cada modo espacial se le etiqueta con un número entero, que inicia en 1 y aumenta una unidad por cada modo. En cada detección, la cadena binaria se va formando con la etiqueta del modo detectado. Usan la test de NIST para verificar sus números y reportan el valor P de las pruebas. El resultado es positivo.

Single-photon decision maker [30].

En este trabajo tienen un montaje experimental muy similar al que realicé. La idea de su experimento no es generar números al azar sino implementar un tomador de decisiones.

Envían fotones a un PBS e interpretan la medición como una decisión tomada. Después hay un mecanismo de retribución por haber tomado cierta decisión. El sistema ajusta su elección hacia la opción más conveniente.

Este trabajo tiene miras hacia la inteligencia artificial.

Apéndice E

Agradecimientos.

Aprovecho este espacio para agradecer a las personas que me han dado los pinturas para hacer este cuadro que es una parte de mi vida. A mis padres Soledad y Amado, a mis hermanos Fabián, Fabiola y Sebastián. A mis amigas y amigos Laura, Brenda, Daniel, Gaby, Luis, Omar, Rodrigo, Abel, Abril.

Especialmente quiero agradecer a la UNAM, a la que ingresé desde la prepa, en la que he tenido excelentes profesores y he pasado gran parte de mi vida desde entonces.

Al grupo de Óptica Cuántica del ICN por sus discusiones que permitieron el desarrollo y avance de este proyecto. Particularmente a mi tutor el Dr. Jorge Hirsch Ganievich quien me ha guiado desde el verano de 2015, cuando realicé una estancia de verano dentro del programa "Verano de la Investigación Científica" de la Academia Mexicana de Ciencias. Desde entonces he contado con su apoyo en la realización de mi servicio social y ahora con este trabajo de tesis.

Al Dr. Alfred U'Ren Cortés, quien lidera el laboratorio de Óptica Cuántica del Instituto de Ciencias Nucleares de la UNAM, por brindar las facilidades para realizar este trabajo y su interés en el proyecto.

Al Dr. Héctor Cruz Ramírez por su apoyo técnico en el laboratorio y su enseñanza en la programación de LabView.

Al Fís. Aldo Solís por sus discusiones, enseñanzas e interés en este proyecto.

Al M. en C. Alí M. Angulo por su apoyo técnico en el laboratorio.

Al proyecto PAPIIT IN109417 " Caos y azar en sistemas cuánticos" con el que se adquirió parte del equipo de laboratorio utilizado.

También quiero agradecer a los programas de Taller de Ciencia para Jóvenes, del Centro de Geociencias de la UNAM, proyecto PAPIME-PE103409, y al "Verano de la Investigación Científica" de la Academia Mexicana de Ciencias por haber motivado mi interés en la ciencia y darme una experiencia en la investigación científica.

Finalmente le doy las gracias a mis sinodales Dr. Oleg Kolokoltsev, Dr. Ricardo Méndez Fragoso, Dr. Pedro Antonio Quinto Su y Dra. Andrea Valdés Hernández por tomarse el tiempo de leer mi tesis y darme sus comentarios.

Bibliografía

[1] Zeilinger A. et al. Happy centenary, photon. *Nature*, 433:230–238, 03 2005.

[2] Cristian S. Calude et al. Experimental evidence of quantum randomness incomputability. *Phys. Rev. A*, 82:022102, 08 2010.

[3] Jennewein T. et al. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000.

[4] Solis A. et al. How random are random numbers generated using photons? *Physica Scripta*, 90(7):074034, 2015.

[5] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Rev. Mod. Phys.*, 89:015004, 02 2017.

[6] Publicación especial 800-22 de nist versión consultada en julio de 2017. `http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf`.

[7] Aspect A. et al. Experimental test of Bell's inequalities using time- varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 12 1982.

[8] Lynden K. Shalm et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, 12 2015.

[9] D. L. Moehring et al. Experimental Bell inequality violation with an atom and a photon. *Phys. Rev. Lett.*, 93:090410, 08 2004.

[10] John C. Howell et al. Experimental violation of a spin-1 Bell inequality using maximally entangled four-photon states. *Phys. Rev. Lett.*, 88:030401, 01 2002.

[11] Generador de números al azar usando ruido atmosférico. `https://www.random.org/randomness/`.

[12] S. Pironio et al. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 04 2010.

[13] Lo Hoi-Kwong et al. Secure quantum key distribution. *Nat. Photon*, 8:595–604, 08 2014.

[14] Calude C. *Borel Normality and Algorithmic Randomness en Developments in Language Theory.* World Scientific, Singapore, 1994.

[15] Hecht Eugene. *Optics. 4 edición.* Addison Wesley., E.U.A., 2002.

[16] Ma Xiongfeng et al. Quantum random number generation. *npj Quantum Information*, 2:16021, 06 2016.

[17] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, E.U.A. New York, 2010.

[18] Shankar R. *Principles of Quantum Mechanics.* Plenum Press, E.U.A. New York, 1994.

[19] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics.* John Wiley & Sons, Inc., New York, 1991.

[20] Hoja de datos de detectores de fotones individuales marca excellitas. `http://www.excelitas.com/Downloads/DTS_SPCM-AQRH.pdf`.

[21] Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nat. Photonics*, 3:696–705, 12 2009.

[22] M. D. Eisaman et al. Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, 2011.

[23] Csele Mark. *Fundamentals of light sources and lasers.* Wiley-InterScience, New Jersey E.U.A., 2004.

[24] Generador cuántico de números al azar de idquantique. `http://marketing.idquantique.com/acton/attachment/11868/f-004c/1/-/-/-/-/Randomness%20Test%20Report.pdf`.

[25] Stefanov A. et al. Optical quantum random number generator. *Journal of Modern Optics*, 47(4):595–598, 2000.

[26] Wang P. X. et al. Scheme for a quantum random number generator. *Journal of Applied Physics*, 100(5):056107, 2006.

[27] Stipčević Mario and Ursin Rupert. An on-demand optical quantum random number generator with in-future action and ultra-fast response. *Sci. Rep.*, 5:10214, 2015.

[28] Branning D. and Bermudez M. Testing quantum randomness in single-photon polarization measurements with the NIST test suite. *J. Opt. Soc. Am. B*, 27(8):1594–1602, 08 2010.

[29] Gräfe M. et al. On-chip generation of high-order single-photon W-states. *Nat Photon*, 8:791–795, 10 2014.

[30] Naruse M. et al. Single-photon decision maker. *Scientific Reports*, 5:13253, 08 2015.