D I P L O M A R B E I T

Quantum Random Numbers in a Steering Experiment with Entangled Photons

ausgeführt am
Atominstitut
Technische Universität Wien
Stadionallee 2, 1020 Wien

unter Anleitung von
O. Univ. Prof. Dr. Anton Zeilinger

durch

Harald Rossmann
Hameaustraße 41A, 1190 Wien

Work supported by the Austrian Science Fund
and the European Research Council via the SFB-ERC Project 8 Grant.

Ort, Datum

Unterschrift

Abstract

The experiment conducted in the scope of this thesis is a loophole-free Einstein-Podolsky-Rosen (EPR) steering experiment, which implicitly includes the test of Born's rule since for one of the distant observers the assumption of local quantum mechanics is made. The term steering goes back to Erwin Schrödinger who responded to the paradoxical situation depicted in the EPR article, which arose from the locality assumption together with the uncertainty principle. In contrast to his colleagues he believed that the quantum mechanical description by a wave function is correct but also had problems of giving up locality and therefore allowing "spooky actions at a distance". These theoretical concepts have later been formulated as a quantum information task, which made this problem accesible experimentally. If the untrusted party Alice can convince Bob that she can remotely steer his state, Bob is forced to believe Alice and give up his assumtpion on local realism. To do so the steering value has to be measured by coincidence counting of conclusive events and to be compared with the bound of a local realistic model. In the performed experiment the measured value was $S = 1.049 \pm 0.002$ which was a violation compared to the bound 1 by more than 20 standard deviations by simultaneously closing all three major loopholes through a proper space time arrangement and the implementation of three measurement settings. In addition, specific attention has to be paid to the quantum random number generators, which are also described in this thesis.

Contents

Chapter 1

Theoretical Concepts

1.1 Probabilities and quantum mechanical states

The aim of either classical or quantum physics is to describe nature as accurately as possible for any time t. Therefore predictions about the evolution of a physical system play an important role. These predictions are tainted with uncertainties, which leads to the concept of probabilities. At this point one has to differentiate between classical macroscopic systems and quantum mechanical systems. For the latter Heisenberg's uncertainty principle [1] is an intrinsic property of the theory and states that conjugate variables such as position and momentum can not be simultaneously measured with arbitrary precision. In contrast to that, a classical physical system evolves in general according to a well defined trajectory in a 6N dimensional phase space, which is a function of coordinates and momentum. In this case uncertainties can only arise by an insufficent knowledge of the system.

1.1.1 Probability amplitudes

These short introductory remarks make clear that an adequate formulation of quantum mechanics is firmly connected with the need of probabilistic methods. In quantum theory probabilities are just secondary quantities, which can be calculated by taking the squared modulus of probability amplitudes [2], which are in general complex numbers. To emphasize the concept of probability amplitudes and the resulting consequences a brief summary of the famous double slit experiment will be given. As shown in figure (1.1) a particle which leaves the source has two different ways to reach a point on the screen. The probability amplitude in this case is just the sum of the probabiliy amplitudes for taking either the upper or the lower slit:

$$P = |a_1 + a_2|^2 = |a_1|^2 + |a_2|^2 + 2\Re a_1^* a_2 \tag{1.1}$$

In classical statistical mechanics the result would just contain the first two terms. Hence the result of one slit is independent of the existence of a second open slit

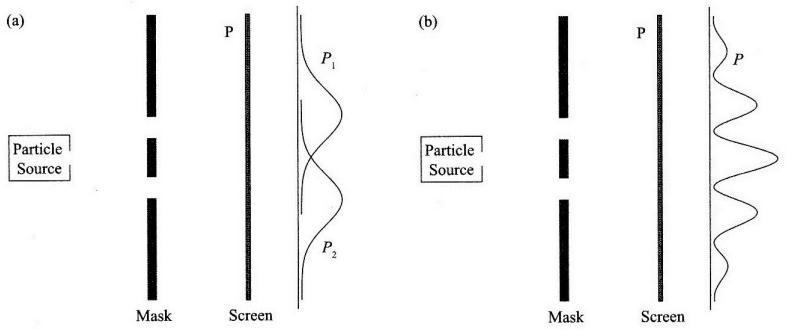

Figure 1.1: Schematic illustration of the double-slit experiment. Particles emmited from a source can act as if they are travelling through one or both slits depending on the present degree of which way information. (a) shows the probability distribution for the classical case where the individual probabilities just add up. This probability distribution can also appear in quantum mechanics, when the path the particle takes is observed. The quantum mechanical case without path information (b) shows interference fringes caused by the third term in equation 1.6 due to the addition of probability amplitudes (fig. taken from [2]).

and, therefore, the particle bevahiour of this process is revealed. The quantum mechanical probability can be greater or less than its classical counterpart, depending on the phase relation of the complex quantity $a_1^* a_2$, which is due to the superposition principle. The latter has to be considered since no path information is available. In this case the path of the particle is said to be no element of reality and a description in terms of probability waves has to be done. This wave nature leads to an interference pattern which can be registered on a photographic plate. In contrast, if the path is completely known, the collapse of the wavefunction recovers the classical result.

1.1.2 Pure states

In the next step it is important to link the concept of probabilities to a quantum state vector [3] (or a state operator) which is to some extent the quantum mechanical analogue to a trajectory in phase space. This can be done if one thinks of a (classical) statistical experiment consisting of a preparation and a measurement phase. For identical preparations of one particle the measurement results will, in general, be different. However, if a long sequence of identical preparations and measurements is regarded, the relative frequencies of the various possible outcomes approach a certain limit. This statement also holds for quantum mechanics. Concerning these two phases of a statistical experiment it is difficult to characterize the preparation by its effect, because identical preparations can lead to different measurement outcomes in subsequent measurements.

On the other hand, the same measurement outcome can result from different preparations. A specific preparation therefore determines the probabilities for various possible measurement outcomes. Since the preparation and the following measurement are independent of one other, the preparation process must specify probability distibutions for all possible measurements. More physically speaking, a state can be identified with the determination of a probability distribution for all observables. While this interpretation is based on the relative frequencies of identical preparations of one system, the quantum mechanical state can also be associated with an ensemble, which is an infinite set of similarily prepared systems. The equivalence of these two interpretations follows from the ergodic hypothesis.

The mathematical framework [4] of the quantum state vector is a complex linear vector space V on which an inner product is defined. If this vector space V is complete as well, this vector space is called a Hilbert space $\mathcal{H}$. From the last condition it follows that any pure state vector $|\Psi\rangle$ can be written as a linear combination of basis vectors

$$|\Psi\rangle = \sum_{n=1}^{N} a_n |\Psi_n\rangle \tag{1.2}$$

in a N-dimensional Hilbert space $\mathcal{H}^N$ with complex coefficients a_n. If $|\Psi\rangle$ is normalized and the states $|\Psi_n\rangle$ are orthogonal this leads to the condition

$$\langle\Psi|\Psi\rangle = 1 = \sum_{n=1}^{N} |a_n|^2 \tag{1.3}$$

which is consistent with the probability interpretation discussed in section 1.1.1 where the complex numbers a_n where associated with probability amplitudes and their squared modulus with the probability of finding the system in the state $|\Psi_n\rangle$ after a certain measurement when the originally prepared state was $|\Psi\rangle$.

1.1.3 Born's rule

Beside the quantum state vector, which determines the probability distributions for all observables, the concept of operators is needed to fully describe a quantum mechanical measurement process. These operators represent physically observable quantities (such as photon polarization or electron spin) and determine the outcome of a specific measurement. Since the measurement outcomes are real values the oberservable quantities need to be described by Hermitain operators for which $A^\dagger = A$ is valid. Every Hermitain operator can be diagonalized and therefore owns a spectral representation of the form

$$\hat{A} = \sum_i \hat{A}|a_i\rangle\langle a_i| = \sum_i a_i |a_i\rangle\langle a_i| = \sum_i a_i P_i \tag{1.4}$$

whereas the eigenvalues a_i correspond to different possible measurement outcomes.

According to the interaction of the wave function with its environement there are two possible dynamical laws that are responsible for their evolution [5]. If the system is closed and there is no interaction possible, the wave function evolves according to the time dependent Schrödinger equation:

$$i\hbar\frac{\partial\Psi}{\partial t} = H\Psi \tag{1.5}$$

In the second case, the quantum state vector gets distorted through the interaction with a classical measurement apparatus. This process can be described by the means of a projection operator P_i (see eq. 1.4) which projects the original state $|\Psi\rangle$ onto an eigenvector of a Hermitain matrix $\hat{A}$ which corresponds to the measured observable. The probability that a measurement yields a certain eigenvalue a_i of $\hat{A}$ is given by

$$\mathcal{P}(a_i) = |\langle\Psi|a_i\rangle|^2 \tag{1.6}$$

and is known as Born's rule. Actually equation 1.6 is just the special case for discrete, non degenrate eigenvalues such as it is the case for photon polarization or spin measurements. Thus, Born's rule which can be regarded as connection between the mathematical formalism and the experiment, can be tested implicitly by evaluating the expectation value of a certain operator $\hat{A}$ by the means of quantum mechanics.

$$\langle\hat{A}\rangle = \langle\Psi|\sum_i a_i|a_i\rangle\langle a_i|\Psi\rangle = \sum_i \mathcal{P}_i(a_i)a_i \tag{1.7}$$

After the measurement the preliminary undetermined value of $\hat{A}$ has been fixed to the measured eigenvalue a_i hence the state changed abruptly to the corresponding eigenfunction $|a_i\rangle$. This single process which occurs completly randomly is called collapse of the wave function or reduction of the state vector. The latter term can be understood if one thinks of the state vector as a superposition; therefore, only one of these superposition states will survive the measurement process. In general (as shown in section 1.1.1) the measurement outcomes follow a probability distribution (with the transition probabilities given by eq. 1.6) which is given by the quantum state vector.

1.1.4 Density matrix formalism

Until now, only pure states, where the observer has perfect knowledge about his state preparation device, have been taken into account. Unfortunately this is just a special case of the state operator, also known as density matrix, where one eigenvalue $a_i = 1$ and all the other eigenvalues $a_j \neq a_i$ are zero. The general case assigns a classical probability p_i to different pure states $|\Psi_i\rangle$. For the double slit experiment, for example, one can assign the probability of $\frac{1}{2}$ that either the upper or the lower slit is masked. Therefore in half of the cases the particle will travel through the upper slit and in half of the cases through the lower slit. But when the system finally has been prepared it has been transferred to a pure

state. The probability distribution for this case is the same as for the classical case for both slits open (shown in fig. 1.1a).

The state operator ρ can be defined in the following way,

$$\hat{\rho} = \sum_{i=1}^{N} p_i |\Psi_i\rangle\langle\Psi_i| = \sum_{i=1}^{N} p_i \hat{\rho}_i \tag{1.8}$$

with $\sum_{i=1}^{N} p_i = 1$. With the means of the state operator and the corresponding algebra, it can be shown that the expectation value takes the form

$$\langle \hat{A} \rangle_\rho = \sum_{i=1}^{N} p_i tr[\hat{A}\hat{\rho}_i] = tr[\hat{A}\hat{\rho}] \tag{1.9}$$

which contains classical and quantum mechanical probabilities.

1.2 Photonic qubits

The fundamental building block of classical information theory is the bit, which can either take the values *0* or *1* corresponding to a well defined *on* or *off* state of a physical system. Its analogoue in the quantum world is the quantum bit or qubit, which can represent both states simultaneously [6]. This tool of quantum mechanics is known as quantum mechanical superposition (see eq. 1.2). Concerning photonic qubits possible implementations [7] are spatial-mode qubits, time-bin qubits or even superpositions in higher dimensions, known as qunits. The state vector of such a quantum mechanical two-level system can be described in a two-dimensional Hilbert space $\mathcal{H}^2$:

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.10}$$

with $\langle Q|Q\rangle = 1 = |\alpha|^2 + |\beta|^2$.

As mentioned in section 1.1.2 obeservables correspond to Hermitain matrices. In the simple case of the two-dimensional qubit space the three Pauli matrices together with the unit matrix in two dimensions form a complete set of unitary 2x2 matrices [2]. Therefore any matrix can be written as a linear combination of these four matrices

$$\hat{A} = a\hat{\mathbb{1}} + b\hat{\sigma}_x + c\hat{\sigma}_y + d\hat{\sigma}_z \tag{1.11}$$

with

$$\hat{\mathbb{1}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \hat{\sigma}_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ \hat{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.12}$$

and real coefficients a, b, c and d. Because of these properties of any 2x2 Hermitain matrix $\hat{A}$, it is sufficient to know the algebra of the Pauli matrices:

$$(\hat{\sigma}_i)^2 = \mathbb{1}, \qquad \hat{\sigma}_i\hat{\sigma}_j = i\epsilon_{ijk}\hat{\sigma}_k \tag{1.13}$$

The information theoretical improvement of a qubit compared to a classical bit can be visualized on the so called Bloch or Poincaré sphere (see fig. 1.2) depending on what kind of two-level system is used. In this work, an experiment with polarization entangled photons is carried out, therefore, I will restrict myself to the latter.

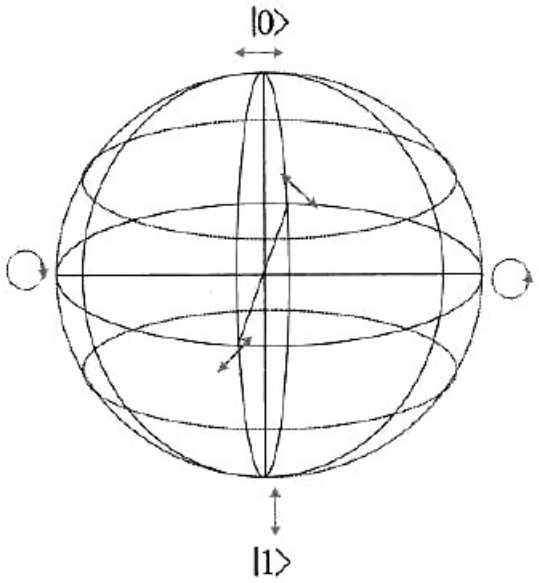

Figure 1.2: Illsutration of the Poincaré sphere for polarization qubits. Coherent superpositions of the states $|0\rangle$ and $|1\rangle$ lie on the shell of this sphere with radius $R = 1$. All states located on oppposite sides of the sphere form an orthonormal basis of the two-dimensional qubit space (fig. taken from [2]).

A classical bit can just occupy the states on the north and on the south pole of the sphere corresponding $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$. A coherent superposition of these states on the other hand can occupy any arbitrary state

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.14}$$

on the shell of this sphere. In contrast to that, decoherence effects can cause transitions to incoherent states, which are located closer to the origin of the sphere.

Beside the two elementary polarization directions $|H\rangle$ and $|V\rangle$ also the most common other directions, e.g. basis vectors for polarization qubits, are shown in figure 1.2. The relations between these three bases are shown in table (1.1). These polarization bases can be converted into each other with the help of retarding wave plates, which can represented by 2x2 matrices in the so-called Jones calculus [8].

Polarization state	Linear combination	Name	Polarization angle
$\|H\rangle$	$\|H\rangle$	horizontal	0°
$\|V\rangle$	$\|V\rangle$	vertical	90°
$\|D\rangle$	$\frac{1}{\sqrt{2}}\big(\|H\rangle + \|V\rangle\big)$	diagonal	45°
$\|A\rangle$	$\frac{1}{\sqrt{2}}\big(\|H\rangle - \|V\rangle\big)$	anti-diagonal	135°
$\|R\rangle$	$\frac{1}{\sqrt{2}}\big(\|H\rangle + i\|V\rangle\big)$	right-circular	
$\|L\rangle$	$\frac{1}{\sqrt{2}}\big(\|H\rangle - i\|V\rangle\big)$	left-circular	

Table 1.1: Common polarization measurement bases of the Poincaré sphere. The linear polarization states are assigned with linear polarization angles.

N qubits can be combined to a quantum register with the advantage of a superposition of all 2^N states compared only to a linear gain (2N) in the case of a classical computer.

1.3 Entanglement

The property of entanglement, which is a very powerful tool in quantum information processing, can be regarded as a generalization of the quantum mechanical superposition principle to composite systems, constisting of two or more subsystems (particles). For the following considerations, I will restrict myself to the bipartite case [5] because it nicely reveals the aspects of the theory without being too complex.

A bipartite system consisting of two qubits S_1 and S_2 can be described in a four-dimensional Hilbert space $\mathcal{H}^4$, which is the tensor product of the two subspaces $\mathcal{H}_1^2 \otimes \mathcal{H}_2^2$. In the case where the two systems S_1 and S_2 were independently prepared in pure states $|\lambda\rangle_1 \in \mathcal{H}_1^2$ and $|\psi\rangle_2 \in \mathcal{H}_2^2$ the composite system $S_1 + S_2$ can be written as the product state:

$$|\Psi_0\rangle = |\lambda\rangle_1 \otimes |\psi\rangle_2 \tag{1.15}$$

In the general case, especially when an interaction between the two subsystems took place for a finite time, the wave vector of the total system can not be written in this simple form anymore. However a pure state of the composite system can be written as a weighted sum with respect to two orthonormal systems of the two subspaces. This phenomenon is known as biorthogonal or Schmidt decomposition [9] and can be written in the form

$$|\Psi\rangle = \sum_{i=1}^{2} a_i |\zeta_i\rangle_1 \otimes |\eta_i\rangle_2, \qquad \{|\zeta_i\rangle\} \in \mathcal{H}_1^2,\ \{|\eta_i\rangle\} \in \mathcal{H}_2^2 \tag{1.16}$$

where the summation index i goes until two. The system $S_1 + S_2$ is said to be in an entangled state if the sum consits of more than one term.

The probability interpretation of this result states that it is impossible to make statements about the individual systems. Only the overall system is found to be in the state $|\zeta_i\rangle_1 \otimes |\eta_i\rangle_2$ with probability $|a_i|^2$.

For the two qubit systems there are four different combinations which can contribute to the sum in equation 1.16, namely $|0\rangle_1 \otimes |0\rangle_2$, $|0\rangle_1 \otimes |1\rangle_2$, $|1\rangle_1 \otimes |0\rangle_2$ and $|1\rangle_1 \otimes |1\rangle_2$. These states now can be combined to four maximally entangled qubit states or Bell-states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 \pm |1\rangle_1 \otimes |1\rangle_2) \tag{1.17}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 \pm |1\rangle_1 \otimes |0\rangle_2) \tag{1.18}$$

Which of these states finally gets prepared depends on the source and the kind of interaction. Photons of an atomic SPS collision cascade, for example, have the same polarization due to symmetry considerations [10]. Such processes are parity conserving as well, therefore the state of the system is characterized by the $|\Phi^+\rangle$ state.

1.4 The Einstein-Podolsky-Rosen paradox

1.4.1 EPR's claim

In their famous paper Einstein, Podolsky and Rosen asked the question whether a quantum mechanical description of physical reality can be considered complete [11]. To understand their way of thinking it is necessary to specifiy the definitions of completness, physical reality and also a third statement which is known as Einstein locality:

- Completeness: *"every element of the physical reality must have a counterpart in the physical theory"*
- Physical reality: *"if, without in any way disturbing a system, we can predict with certainty (i.e. with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity"*
- Einstein locality: *"since at the time of measurement of the two systems no longer interact, no real change can take place in the second system in consequence of anything that might be done to the first system"*

For further considerations they regarded a system consisting of two particles which were able to interact for a finite time (between $t = 0$ and $t = T$). After this interaction process the state vector of this entangled system can be calculated by the means of Schrödingers equations:

$$\Psi(x_1, x_2) = \int_{-\infty}^{+\infty} e^{\frac{i}{\hbar}(x_1 - x_2 + x_0)p} dp \tag{1.19}$$

In this case, x_1 and x_2 correspond to the positions of the two particles and x_0 is some constant. Since this is an entangled state only assumptions about the

total system can be made (according to section 1.3) unless the wave function is forced to collapse through additional measurements.

Let's assume that some of these, namely p_2, the momentum of the second particle, and x_1 or p_1 corresponding to the first particles position or momentum, are made. If one measures $p_1 = p$ it can easily be shown that $p_2 = -p$ with certainty, since the momentum operator $\hat{P}$ is proportional to the partial derivative of the spacial coordinate of the respective particle. Hence the momentum of the second particle is said to be an element of physical reality. This argument holds as well for x_2 if the position of the first particle is measured.

Now the question arises, what happens if conjugate variables, for example x_1 on the first system and p_2 on the second system, are measured? A measurement of x_1 has the direct consequence that due to Heisenberg's uncertainty principle no predictions about p_1 can be made with certainty. Therefore quantum mechanics is also not able to make any predictions for p_2. The same situation occurs for p_1 and x_2. The paradox about this whole situation now is the following: Since the systems are spatially separated, the choice of measurement on the first system can not affect the outcome of the second system unless superluminal signalling is permitted. Thus, a momentum measurement performed on the second particle should also yield $p_2 = -p$. Therefore both measurement outcomes (x_2 and p_2) of the second particle have to be simultaneous elements of physical reality, determined right after the separation of the two systems. This argument is obvoiusly in cotradiction with Heisenberg's uncertainty principle.

This result let Einstein, Podolsky and Rosen conclude: *"While we thus have shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."*

But they also remarked that their definition of physical reality leaves a margin for different interpretations: *"Indeed, one would not arrive at our conclusion if one insisted that two or more physical quantities can be regarded as simultaneous elements of reality only when they can be simultaneously measured or predicted."*

1.4.2 Bohr's reply

Shortly after the publication of the EPR article, it was Bohr who commented and mainly critizised some arguments of EPR's claim [12]. He agreed on the fact that each experimenter has a free will and therefore has the freedom of choice of determing whether the one or the other physical quantity is measured.

On the other hand, he offered criticism on their definition of physical reality, because after his interpretation there is no doubt that there is a disturbance of the measured system through an interaction with the measuring device. According to this influence he concluded that there have to be restrictions on what kind of predictions one can make about the system.

In order to corroborate the belief that the quantum mechanical description of physical reality through a physical wave function is complete he introduced the principle of complementarity which was based on the following two assumptions:

- Mutual exclusiveness: *"in fact, it is only the mutual exclusion of any two experimental procedures, permitting the unambiguous definition of complementary physical quantities"*

- Joint completion: *"the combination of which characterizes the method of classical physics, and which therefore in this sense may be considered as complementary to one another"*

In other words, the first argument refers to a specific experimental situation. Bohr explained that the measuring apparatus for a position measurement is totally different than the one used for a momentum measurement. Therefore only one of these quantities can be measured in a specific experimental environment.

The second argument refers to the case of classical physics, where position and momentum can indeed be measured simultaneously with arbitrary precision and therefore provide a complete description of the particles motion in the sense of a well defined trajectory in phase space [13].

1.4.3 Schrödinger's reply

Beside Bohr Schrödinger also was very interested in the EPR thought experiment, which is reflected in several publications [14, 15, 16] concerning the paradoxical situation. Probably the most famous of these is his review article [14] about the *"present situation of quantum mechanics"* where he has primarily coined the term entanglement: *"A measurement on one [system] can impossibly be an indication of what to expect from the other. If "entanglement of the predictions" exists, it can just be affiliated to the fact, that the two solids had formerly built one system, e.g. that they were affected by each other and that this interaction has left its traces."*

In another publication he also pointed out the importance of that feature: *"I would not call that **one** but rather **the** characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."* [15]

The second important remark Schrödinger made was the ability to affect the state on one side of the system by the choice of measurement on the other side. This phenomenon is kown as EPR steering: *"It is rather discomforting that the theory should allow the system to be steered or piloted into one or the other type of state at the experimenter's mercy in spite of his having no access to it."* [15]

In contrast to EPR, he believed that the description by the means of a quantum mechanical wave function is complete for a localized and isolated system. Like Einstein, Schrödinger had a problem of giving up local causality for delocalized entangled systems. But if steering is possible and the description by a quantum mechanical wave function is complete, this is the only way to explain the resulting correlations.

1.5 Bell's inequalities

1.5.1 Bohm's version of the EPR paradox

For further considerations, especially the derivation of Bell's inequalities, it is more convenient to consider Bohm's version of the EPR paradox [17, 18], which contains discrete boolean observables, such as particle spin or photon polarization, with eigenvalues $a_i = \pm 1$ rather than continuous variables like position and momentum as in the original EPR paper.

Bohm considered a molecule consisting of two atoms with total spin $S = 0$. Therefore the spin of the individual atoms has to point in opposite directions. After a seperation process, which per definition does not affect the spin of the systems, the atoms cease to interact and are still in the entangled singlet state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1 \otimes |\downarrow\rangle_2 - |\downarrow\rangle_1 \otimes |\uparrow\rangle_2) \tag{1.20}$$

According to EPR's claim the measurement of a certain spin component of the first system will predict the value of the same component of the second system with certainty. In the case of the $|\Psi^-\rangle$ state these values will be perfectly anticorrelated. According to EPR every spin component of the second system is simultaneously an element of physical reality which is in contrast to the quantum mechanical result since the Pauli spin matrices do not commute with each other (see eq. 1.13). Hence it is only possible to measure one component of the spin vector with arbitrary precision. Measurements in complementary bases compared to the measuring apartus of the first system therefore yield random results.

1.5.2 Bell's theorem

When Bell commented on the EPR paradox [19] he wanted to explain perfect correlations in a local realistic world view. He was therefore regarding a similar system to that proposed by Bohm as an experimental test of the EPR paradox. The only extension he made was the possibility of rotating the two detecting stations (Stern-Gerlach magnets) in a plane perpendicular to the travelling direction of the spin $\frac{1}{2}$ particle.

If, as suggested by Einstein, Podolsky and Rosen, variables like the three spin components correspond simultaneously to three elements of physical reality, there should be some hidden variable, which tells the particle how to react depending on the kind of measurement performed on the distant system (see sec. 1.4.1).

Assuming that the measurement $\vec{\sigma}_1 \cdot \vec{a}$ yields the value $+1$, a measurement along the same direction on the distant particle $\vec{\sigma}_2 \cdot \vec{a}$ must yield -1 due to perfect anti-correlations of the $|\Psi^-\rangle$ state. For different directions of the measurement devices one can only say that a measurement performed on system A (system B respectively) will yield one of the eigenvalues ± 1 depending on the hidden variable λ:

$$A(\vec{a}, \lambda) = \pm 1, \qquad B(\vec{b}, \lambda) = \pm 1 \tag{1.21}$$

The crucial point regarding these two equations is that the value of A does not depend on $\vec{b}$ and vice versa B is independent of $\vec{a}$. Due to this property the joint measurement on the expectation value of $(\vec{\sigma}_1 \cdot \vec{a})(\vec{\sigma}_2 \cdot \vec{b})$ factorises in the following way

$$E^{lhv}(\vec{a}, \vec{b}) = \int \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda) d\lambda \tag{1.22}$$

with the normalized probability distribution $\int \rho(\lambda) d\lambda = 1$. This expectation value should be equivalent to the one predicted by quantum mechanics:

$$E^{qm}(\vec{a}, \vec{b}) = \langle \Psi^- | (\vec{\sigma}_1 \cdot \vec{a}) \otimes (\vec{\sigma}_2 \cdot \vec{b}) | \Psi^- \rangle = -\vec{a} \cdot \vec{b} = -\cos\theta \tag{1.23}$$

The last equal sign follows from the fact that $\vec{a}$ and $\vec{b}$ are unit vectors.

As shown above $A(\vec{a}, \lambda) = -B(\vec{a}, \lambda)$, therefore the expectation value in the local hidden variable model can be rewritten as:

$$E^{lhv}(\vec{a}, \vec{b}) = -\int \rho(\lambda) A(\vec{a}, \lambda) A(\vec{b}, \lambda) d\lambda \tag{1.24}$$

Considering a third direction $\vec{c}$ yields:

$$E^{lhv}(\vec{a}, \vec{b}) - E^{lhv}(\vec{a}, \vec{c}) = -\int \rho(\lambda) A(\vec{a}, \lambda) A(\vec{b}, \lambda) d\lambda + \int \rho(\lambda) A(\vec{a}, \lambda) A(\vec{c}, \lambda) d\lambda \tag{1.25}$$

Utilization of $A^2 = 1$ leads to:

$$E^{lhv}(\vec{a}, \vec{b}) - E^{lhv}(\vec{a}, \vec{c}) = \int \rho(\lambda) A(\vec{a}, \lambda) A(\vec{b}, \lambda) [A(\vec{b}, \lambda) A(\vec{c}, \lambda) - 1] d\lambda \tag{1.26}$$

Building the modulus of this quantity together with a further estimation with respect to the triangle inequality results in

$$1 + E^{lhv}(\vec{b}, \vec{c}) \geq |E^{lhv}(\vec{a}, \vec{b}) - E^{lhv}(\vec{a}, \vec{c})| \tag{1.27}$$

which is known as Bell's inequality. Inserting the values $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{c} = \frac{1}{\sqrt{2}}$ and $\vec{a} \cdot \vec{c} = 0$ for the quantum mechanical expectation value maximally violates this inequality as can be seen in the following equation:

$$1 - \frac{1}{\sqrt{2}} \geq \frac{1}{\sqrt{2}} \tag{1.28}$$

Therefore Bell has shown that the correlations produced by quantum theory are stronger than in any local hidden variable model.

1.5.3 Clauser-Horne-Shimony-Holt inequality

The CHSH inequality [20] can be understood as a generalization of Bell's inequality. Since Bell's derivation was based on a two outcome system with perfect anti-correlations in the case of a two spin $\frac{1}{2}$ particles it is rather less applicable

to real experimental systems with imperfect measurement devices. Another experimental problem is the adjustment of a perfectly pure $|\Psi^-\rangle$ state in the case of entangled photon pairs. To overcome this difficulties only average values of the measured quantities A and B

$$|\bar{A}(\vec{a},\lambda)| \leq 1, \qquad |\bar{B}(\vec{b},\lambda)| \leq 1 \tag{1.29}$$

can be taken into account.

Inserting this ansatz into the correlation functions of the local hidden variable model yields:

$$\begin{aligned} E^{lhv}(\vec{a},\vec{b}) - E^{lhv}(\vec{a},\vec{b'}) &= \int \rho(\lambda)\bar{A}(\vec{a},\lambda)\bar{B}(\vec{b},\lambda)d\lambda - \int \rho(\lambda)\bar{A}(\vec{a},\lambda)\bar{B}(\vec{b'},\lambda)d\lambda \\ &= \int \rho(\lambda)\bar{A}(\vec{a},\lambda)\bar{B}(\vec{b},\lambda)[1 \pm \bar{A}(\vec{a'},\lambda)\bar{B}(\vec{b'},\lambda)]d\lambda \\ &\quad - \int \rho(\lambda)\bar{A}(\vec{a},\lambda)\bar{B}(\vec{b'},\lambda)[1 \pm \bar{A}(\vec{a'},\lambda)\bar{B}(\vec{b},\lambda)]d\lambda \end{aligned} \tag{1.30}$$

Utilization of equation (1.29) and of the triangle inequality results in an expression similar to Bell's original inequality:

$$\begin{aligned} |E^{lhv}(\vec{a},\vec{b}) - E^{lhv}(\vec{a},\vec{b'})| \leq &\int \rho(\lambda)[1 \pm \bar{A}(\vec{a'},\lambda)\bar{B}(\vec{b'},\lambda)]d\lambda \\ &+ \int \rho(\lambda)[1 \pm \bar{A}(\vec{a'},\lambda)\bar{B}(\vec{b},\lambda)]d\lambda \end{aligned} \tag{1.31}$$

This finally leads to the CHSH inequality:

$$|E^{lhv}(\vec{a},\vec{b}) - E^{lhv}(\vec{a},\vec{b'})| \leq 2 \pm [E^{lhv}(\vec{a'},\vec{b'}) + E^{lhv}(\vec{a'},\vec{b})] \tag{1.32}$$

For the special case of $\vec{a'} = \vec{b'}$ this just yields the original Bell inequality (1.27). Again, the quantum mechanical expectatian value can violate this inequality for certain angles. For $\alpha = 0°, \beta = 45°, \alpha' = 90°, \beta' = 135°$ this results in a maximal violation

$$\left|-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right| + \left|-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right| = 2\sqrt{2} \geq 2 \tag{1.33}$$

which is known as Tsirelson bound [21].

1.5.4 Experimental loopholes

In their thought experiment [11] the assumption of Einstein, Podolsky and Rosen, that any theory in nature has to obey locality and realism led to a paradox situation under the consideration of entangled states and therefore let them conclude that quantum mechanics was incomplete. Nevertheless they thought that a completion might be possible. Such theories are based on "local hidden

variables" or in the specific case of EPR steering on "local hidden states", which determine the particles properties at any time regardless of whether an observation occurs or not. As shown in section 1.5 the conflict between (classical) local realistic theories and quantum theory has been controversially discussed from a theoretical viewpoint. Not until three decades later the derivation of mathematical inequalities [19, 20] made this question accesible experimentally. Since then, strong experimental evidence has been collected to rule out local realistic theories [22, 23, 24, 25, 26]. Unfortunately imperfections in the experimental setup open "loopholes" for local realistic models, which could not be simultaneously closed in a single experiment until our EPR steering experiment [27].

The underlying principles of the three major loopholes, which will be discussed in the following, are influences on or of the choices of measurements, a possible hidden communication and a low detection efficiency, which are not representative for the whole ensemble.

- Freedom of choice:

  In Bell's original derivation there was no explicit assumption made concerning the dependence of the choice of measurement settings on a hidden variable λ. Only in a latter work [28] he stressed the importance of that by formulating the following hypothesis: *"The variables a and b can be considered to be free or random."* Therefore

  $$\vec{a} \neq \vec{a}(\lambda), \qquad \vec{b} \neq \vec{b}(\lambda) \tag{1.34}$$

  the measurement settings are independent of any hidden variable and vice versa.

  From an experimental point of view this loophole is closely related to the locality loophole (which will be discussed next) and can therefore be closed by a proper space time arrangement of the experimental setup. The crucial point concerning this issue is, that the measurement choices might be influenced by hidden variables which are produced at the photon pair production in the source or the other way round. Therefore the random devices which are responsible for the setting choices have to be outside the future lightcone of the source [29].

  In his work, Bell was thinking of an idealized Einstein-Podolsky-Rosen-Bohm experiment: *"Then we may imagine the experiment done on such a scale, with the two sides of the experiment seprated by a distance of order light minutes, that we can imagine these settings being freely chosen at the last second by two experimental physicists, or some other random devices."* [28]

  As mentioned above in a perfect experiment choices will be made by human beings and of course free will will not depend on any hidden variable. This seems feasible in space experiments with entangled photon pairs which are already in preparation. Unless they are not realized they

are unfortunately not more than a nice theoretical concept. Thus, a non-deterministic hardware random number generator, which exploits the objective randomness of a quantum mechanical effect, is the best source to generate reliable random numbers at a high operational speed.

- Locality:

  The locality loophole can arise if some form of hidden communication can take place between the whole measurement processes (including the random decision on the setting, the implementation of this setting and the registration at the detector) on either side of the system, since one vital assumption of Bell was local causality

  $$A(B, \vec{a}, \vec{b}, \lambda) = A(\vec{a}, \lambda), \qquad B(A, \vec{a}, \vec{b}, \lambda) = B(\vec{b}, \lambda) \tag{1.35}$$

  which bears in mind that after the interaction between the two subsystems stopped *"the real factual situation of system S2 is independent of what is done with the first system S1, which is spatially seperated from the former"* [30]. To be more precise a differenciation between setting and outcome independence is made:

  $$\begin{aligned} A \neq A(\vec{b}), \qquad & B \neq B(\vec{a}) \\ A \neq A(B), \qquad & B \neq B(A) \end{aligned} \tag{1.36}$$

  In the framework of special relativity this means, that the timescale on which the whole measurement process takes place must be much smaller than $\frac{L}{c}$, so that any form of mutual influence by subluminal signals can be excluded. In this case L corresponds to the distance between the two observers Alice and Bob and c is the speed of light.

- Detection:

  The effect of an imperfect detection efficiency, e.g. particle losses on either one or both sides of the total system or double detections (two clicks on one side), can be included in theoretical descriptions by considering a third inconclusive outcome [31], denoted as 0. Therefore the CHSH inequality gets modified by the conditional probability η, which is the probability of measuring ± 1 on the second system, when ± 1 was the outcome of the first system. If η becomes larger than 82.8% the corresponding inequallity can be violated. Later, Eberhard showed that this threshold value can be lowered further to 67% if non maximally entangled states of the form

  $$|\Psi\rangle = \frac{1}{\sqrt{1 + |\epsilon|^2}} (|H\rangle \otimes |V\rangle \pm \epsilon |V\rangle \otimes |H\rangle) \tag{1.37}$$

  are used [32].

  Otherwise the so called fair saimpling assumption, which states that the efficiency is independent of the microstate of the system, has to be made.

In this case the detected sub-ensemble can be regarded as a representative sample of the real ensemble.

For EPR steering the whole situation is different and because Bob trusts his local measurement device and therefore only reports the binary oucomes -1 and +1. Alice on the other hand is the untrusted party and has to report a guess for Bob's measurement outcome, whenever he has registered a click. Hence inconclusive events can not be discarded. This asymmetry in the steering setup results in a lowered detection efficiency for conclusive events. From an experimental point of view coincidence count detection now demands a low dark count detection rate on Bob's side, whereas Alice needs a high detection efficency so that no coincidence signal gets lost.

1.6 Steering

One of the most powerful but also most controversial tools of quantum mechanics is entanglement (cf. section 1.3). Even Einstein could not believe that a mechanism exists, that can instantaneously influence a correlated particle no matter how far away this second particle is. This was clearly in contradiction with his theory of special relativity. In the EPR paper they revealed the paradox situation that *"as a consequence of two different measurements performed upon the first system, the second system may be left in states with two different wave functions"* [11], which was in conflict with local realism and let them conclude that quantum mechanics was incomplete (cf. section 1.5.1).

This *"spooky action at a distance"* - termed steering - goes back to Schrödinger [16]: *"quantum mechanics obliges us to admit not only that by suitable measurements, taken on one of the two parts only, the state (or representative or wave function) of the other part can be determined without interfering with it, but also that, in spite of this non-interference, the state arrived at depends quite decidedly on what measurements one chooses to take - not only on the result they yield."* In his work he even took the EPR thought experiment one step further by generalizing it to more than two measurements and showed that *"it does not only know these two answers but a vast number of others"* with the only limitation on one virgin state measurement. Therefore steering might be an interesting tool in the context of quantum information theory.

1.6.1 Operational definitions

Wiseman et al. [33] primarily defined such a quantum information task, whose description contains beside the two individual parts Alice and Bob also a third party Charley (for the case of non-separability this would be an entanglement witness) to derive the smallest subset of non-seperable states, which are Bell non-local states.

- Non-separability: First, let us assume that Alice and Bob can prepare a bipartite entangled state under reproducible conditions and a trustful

communication between them is established. In this case they can freely exchange their individual measurement outcomes and do state tomography. Based on the reconstructed bipartite state they can determine if they truly shared a non separable state.

- Steerability: The steering task is more restrictive according to the preconditions made for non-separability, since Bob does not trust Alice. Therefore the initial effective one party task for non-separability became a real two party task. Now the distrustful party Alice claims that she can prepare a bipartite entangled state. Again this process can be repeated several times and both are measuring their factual parts and report their results through a classical channel. Bob, who accepts quantum mechanics, will only be convinced that they really shared an entangled state if no local hidden state description is possible. This means that Alice's cheating strategy of sending a pre-existing pure state of a local hidden state ensemble and anouncing her result according to the knowledge of Bob's state and measurement basis has to fail.

- Bell nonlocality: In this case a third sceptical party Charley, who believes in quantum mechanics but trusts neither Alice nor Bob, has to be convinced that they really share an entangled state. Therefore they have to demonstrate Bell nonlocality and violate the CHSH inequality experimentally. Since, in contrast to non-separability and steerability no further assumptions about Alice and Bob can be made, the resulting correlations might also be explained by a hidden variable model (instead of hidden states). Only if such a description fails, Charley will be convinced that they shared an entangled state.

1.6.2 Mathematical definitions

From a mathematical point of view these three different kinds of non separability (in the case of mixed states) can be described in the sense of joint probabilites.

- Non-separability: As shown above the weakest form of non-locality is the case of non-separability. Since both parties trust each other and accept quantum mechanics as complete, the joint probability can be written as

$$P(a,b|A,B) = \sum_{\lambda} P(\lambda) Tr[\Pi_a^A \rho_\alpha(\lambda)] Tr[\Pi_b^B \rho_\beta(\lambda)] \tag{1.38}$$

  whereas $\Pi_{a,b}^{A,B}$ are projection operators, projecting onto subspaces which are defined by the measurement outcomes A (B) and the measurement settings a (b). The state operators $\rho_{\alpha,\beta} \in \mathcal{H}_{\alpha,\beta}$ correspond to the mixture of local quantum states on each side of the system. If the description by the joint probability (1.38) fails, the state is said to be non separable and therefore it can not be written in the product form.

- Steerability: EPR-steering can be seen as an intermediate option between non-separability and Bell-nonlocality. In this case Bob (like Schrödinger) accepts that the quantum mechanical description of his local state is correct, whereas on the other hand for Alice no further restrictions are made. Therefore the joint probability reads

$$P(a,b|A,B) = \sum_{\lambda} P(\lambda)P(A|a,\lambda)Tr[\Pi_b^B \rho_\beta(\lambda)] \tag{1.39}$$

  which reflects the inherent asymmetry of the steering task, in contrast to Bell nonlocality and non-separability. Alice succeeds in the steering task if a local hidden state description (1.39) from Bob's point of view fails, therefore she could remotely prepare Bob's state by forcing it to collapse into a certain ensemble of states which just depends on her choice of measurement.

- Bell nonlocality: This is the strongest form of nonlocality known by quantum mechanics and occurs if the resulting correlations between a and b can not be explained by a local hidden variable model. Thus, states of this kind violate Bell's inequality, where one fundamental assumption was based on a factorizing joint probability:

$$P(a,b|A,B) = \sum_{\lambda} P(\lambda)P(A|a,\lambda)P(B|b,\lambda) \tag{1.40}$$

In summary, it can be said, that steerable states are a subset of non separable states and a superset of Bell nonlocal states.

1.6.3 The EPR steering task

As already mentioned it is convenient to formulate EPR steering as a quantum information task between two distant observers Alice and Bob. Alice claims that she is able to remotley affect and therefore steer Bob's state. To prove this, Bob, who believes in local quantum mechanics but is sceptical about any nonlocal effects, has to be convinced. Therefore Alice sends a state to him, which he regards as an unknown local quantum state, since it is not physically acessible to her anymore and he did not yet measure it. Now Alice succeeds in her task if she can convince Bob that the state he received is part of a polarization entangled photon pair and therefore the measured correlations can not be described by any local hidden state model. To do so, Bob randomly chooses a certain polarization basis out of a predefined set of mutually unbiased bases. In the next step he announces his choice of measurement basis to Alice and records his measurement outcome, which he keeps secret. Since Bob's photon of the entangled photon pair is already on the way to his laboratory Alice has no chance to influence it with the means of any local mechanism. The second photon which is stored locally in Alice's laboratory is delayed so that she can measure it in the basis predefined by Bob's random choice. According to her result, Alice is now able

to make predictions on the measurement outcomes of Bob. If the correlations violate an EPR steering inequality Bob will be convinced that she succeeded in the steering task or give up his assumption on a local quantum state.

The EPR steering inequality was derived by Wiseman and his colleagues [33] and reads

$$S = T_X + T_Y + T_Z \leq 1, \tag{1.41}$$

whereas

$$T_X = \sum_r P(r|X_A)[\langle X_B \rangle|_{X_A=r}]^2, \qquad r = -1, 0, +1 \tag{1.42}$$

and T_Y and T_Z are formulated in a similar way. $P(r|X_A)$ in this case is the probability of getting the outcome r when Alice performs a measurement in the basis X. $\langle X_B \rangle|_{X_A=r}$ on the other hand is the expectation value for Bob's measurement result, if he measures in the same basis and Alice has measured the result r.

Chapter 2

Quantum random number generation

2.1 Different types of randomness

First of all I want to start with a rather heuristical definition of randomness [34], which therefore works without any formulas: *"A random event is an event which has a chance of happening, and probability is a numerical measure of that chance"* This defintion seems to be generally valid, however to explore all underlying effects a differentiation between two different types of randomness has to be made:

- Subjective randomness: This type of randomness occurs when the underlying parameters of some kind of physical effect are not sufficiently known. Typical factors of these class are games of chance such as Roulette or Craps. The latter game can be reduced to the throw of two dice. Considering only one die, each individual throw is independent from the previous or the next one. Hence the result seems random. According to the previous definition every number has the same chance of happening, namely $p = \frac{1}{6}$. Considering two or more dice just changes the probabilities for different numbers but not the random character of the event, therefore in this case it is sufficient to remain at the example of throwing one die. The question arises what the reason for this random behaviour is. In fact the throw of a die is a deterministic process, whose number could in principle be predicted with probability $p = 1$ if all underlying parameters which influence the result of a throw, such as rotation speed, angle of incidence, roughness of the surface and many more, are well known. Since the throw of a die is a rather complex physical process, this is impossible and therefore the process is regarded as random.

- Objective randomness: In contrast to subjective randomness, which is due to insufficient knowledge of the parameters of a physical effect the

character of objective randomness is different. The nature of this kind of processes is inherently random, therefore the result can not be predicted with certainty even though we have profound knowledge about the system. Quantum mechanical processes like radioactive decays or the path of a photon passing through a 50:50 beam splitter fall into this category.

2.2 Random number generation

There are several different ways to produce a sequence of random numbers, which can be categorized into pseudo random number generators (PRNG) or true, physical random number generators (TRNG).

The first kind of them is based on certain algorithms, which strongly depend on their starting point, the so called seed, and some other parameters as will be shown in the next section. Since these generators show a certain periodicity, after a suitable number of random bits the sequence can be predicted and is therefore not trustable anymore. According to the types of randomness, as the name already indicates, generators of this kind are deterministic and therefore only produce subjective randomness. In principle algorithmic randomness would be predictable if the computing power would be high enough. Nevertheless they have several advantages such as the ease of implementation and their low costs. One also has to keep in mind that they are sufficient for a variety of applications. Since nearly everyone has a personal computer at home also the distribution is not a problem.

The second kind are true random number generators which exploit the intrinsic randomness of some physical, mostly quantum mechanical effect. These generators are more complex than pseudo random number generators but guarantee objective randomness, which is needed in the framework of quantum information processes or quantum cryptography. Underlying effects of such physical random number generators are noise, radioactive decays as well as certain optical properties.

Also a third not so common alternative should be mentioned at this point, namely a hybrid form which combines the methods of pseudo and true random number generators. In general, these hybrid generators follow the approach that a slow physical, truly random effect is utilized to determine the seed for a pseudo random number generator.

2.2.1 Pseudo random number generators

Above already some of the general advantages and disadvantages of pseudo random number generators have been mentioned. In this subsection a more detailed description of certain algorithms will be given considering the basic groups [35] consisting of linear congruental, multiple recursive congruental and inversive congruental generators. From a historical point of view these all go back to John von Neumann's pioneering work in this field, starting with the *middle square method* to produce a sequence of random numbers.

Linear congruental generators

The basic principle of linear congruental generators (LCGs) is a recurrence formula which depends on four parameters

$$X_{n+1} = (aX_n + c) \mod m, \qquad n \geq 0 \tag{2.1}$$

whereas X_0 is the starting value, the so called seed, a the multiplier, c the increment and m the modulus. The choice of these parameters is very important for the performance of the PRNG, for example the sequence length before periodicity occurs is bounded by the value of m.

Depending on the value of the increment c, generators can either be multiplicative congruental for the case of $c = 0$ or mixed congruental for $c \neq 0$. Pure multiplicative generators have the advantage that they are faster compared to mixed ones. On the other hand it is impossible to achieve the maximum period length.

Multiple recursive congruental generators

Multiple recursive congruental generators represent a generalization of linear congruental methods, which only depend on the former object of the sequence as seen in equation 2.1. In this case the next object of a sequence can depend on k others of the form:

$$X_n = (a_1 X_{n-1} + \cdots + a_k X_{n-k}) + c \mod m \tag{2.2}$$

Depending on the increment a differentiation between homogeneous and inhomogeneous multiple recursive congruental generators can be made, whereas for theoretical considerations it is sufficient to take homogenious generaters into account since every inhomogeneous generator can be transformed to a homogeneous one by subtracting two subsequent objects. A well known member of this family are the Fibonacci and the lagged Fibonacci generators, which depend only on two objects of the sequence. Lagged in this case just means that the object X_{n+1} does not necessarily depend on X_n and X_{n-1} but on any two arbitrary previous objects X_{n-i} and X_{n-j} of the sequence.

Inverse congruental generators

Several approaches were made to overcome characteristic difficulties such as the occuring lattice structure of finite sequences of overlapping d-tuples $\mathbf{x}_n = (x_n, x_{n+1}, \cdots, x_{n+d-1})$ or non-overlapping d-tuples that can be written as $\mathbf{x}_n = (x_{nd}, x_{nd+1}, \cdots, x_{nd+d-1})$ in a d-dimensional unit cube. One of these just combines the output of two individual RNGs to increase the period length to the product of the individual period lengths. Even tough this method was an improvement, the results were not satisfying at all.

Inverse congruental generators which were first described by Eichenauer and Lehn [36], were the solution to this problem. Depending on whether only the inverse of the object X_n or of the whole element before the modulo operation

is taken a differentiation between "normal" and explicit inverse congruental generators is made. The first of them is defined in the following way:

$$X_{n+1} = aX_n^{-1} + c \mod p \tag{2.3}$$

In this case the modulus is taken to be a prime number p.

The explicit generators are of the form:

$$X_{n+1} = (a(X_n + n) + c)^{-1} \mod p \tag{2.4}$$

Even though inverse congruental generators are slower than linear congruental ones, they have the advantage of larger sample sizes and fewer correlations between consecutive numbers.

2.2.2 True random number generators

Random number generation by radioactive decays

A simple, but rather "dangerous" method to generate true random numbers is the utilization of radioactive decays, since there is a trade-off between the operational speed of the random number generator and the activity of the decay products. The working principle of this kind of generators exploits the quantum nature of a radioactive decay of an atom. Therefore one can just specifiy the half life, meaning, the time when on average the half of the atoms decayed, but not the time when a particular decay will occur. Considering a one-atom picture, this means that this particular atom has a probability of $p = \frac{1}{2}$ of being decayed after this period of time or not.

One random number generator which makes use of this principle is the HotBits generator of the Fourmilab in Switzerland [37]. For the following description I will restrict myself to the first generation of the HotBits generator of 1996 since the decay process is less complicated and all effects can be revealed properly. The radioactive element used for this generator was Krypton 85, which decays with a half life of 10.73 years via β^- decay into Rubidium 85

$$^{85}Kr \longrightarrow {}^{85}Rb + \beta^- + \gamma \tag{2.5}$$

whereas the β^- "particle" consists of an electron and an electron anti-neutrino. This transition occurs due to a weak interaction process. In the third generation instead of Krypton 85 Caesium 137 with an activity of 5μCi and a half life of 30.2 years is used. In this case there is an additional intermediate state of metastable Barium 137. With an activity like this, streams of random numbers with a frequency in the order of 1 kilobit per second can be produced.

The assignment of zero and one bits is made by time bit encoding. Therefore the time intervals between two consecutive gamma ray detection events have to be measured and compared afterwards. For example if ΔT_2 is larger (smaller) than ΔT_1 the bit is attributed a zero (one). To avoid any bias this definition is switched after each registered bit.

Noise based random number generation

The second family of true random number generators are noise based generators. One approach is to use the Johnson noise [38] in an electric conductor. In contrast to shot noise this effect even arises if no voltage is applied. Since a conductive material is considered, there is always a certain amount of free electrons available. In the case of $T > 0K$ these can be treated in a model similar to the one of the electron gas. Interactions among themselves and with atoms of the material cause a random movement of these electric charge carriers. A non uniform charge distribution across the conductor then results in a randomly varying potential difference which can be amplified and measured afterwards.

Another method to generate a randomly variying noise signal is the utilization of the Zener effect in a Zener diode. An applied voltage to such a reversed biased p-n diode results in a shift of the energy bands. Hence the tunnel probability increases and for a certain voltage the avalanche effect occurs. The second effect that occurs is the shot noise, which is due to the discrete nature of electric charge and takes into account that each electron has its own random velocity and separation. Therefore a noise current gets superimposed with a steady state current. In principle a sufficiently low steady state current will register the tunneling process of individual electrons resulting in perfectly random pink noise [39].

The generation of random numbers is done afterwards by a comparison with a certain threshold value. If this threshold is exceeded (deceeded) a one (zero) is produced. This means that the threshold value has to be tuned very carefully, so that the bias of the sequence can be kept as low as possible.

Summarizing these two methods one can say that both are not well isolated effects, which makes it difficult to use them as TRNGs. The occurence of a memory effect, meaning a dependence on a voltage in the past, results in a correlation in the output bit sequence. Another disadvantage is that the low signals have to be amplified, which adds to the distortion of the signal. Also thermal stability is an issue, since a small drift in the average voltage signal will result in a large bias of the random number sequence.

Optical random number generators

A good overview concerning non-deterministic optical hardware random number generators is given by the survey articles [39, 40] written by Mario Stipcevic. In general there are two different kinds of operation, namely generators which exploit the inherent randomness of a single unpolarized photon impinging on a (polarizing) beam splitter (be it in fibre or free space), or generators that - similarly to the generators based on radioactive decays - make use of a random spontaneous emission process. In the first case, since unpolarized light can be regarded as a superposition of two orthogonal polarization directions, the photon impinging on the beamsplitter can either transmitted or reflected. Hence the path taken by the photon and the resulting click of the respective detector generate a binary sequence. This principle can be extended to the uti-

lization of diagonal polarized light, which has the advantage that the bias of the sequence can be adjusted very accurately by rotating the polarizer. Recently also experiments with entangled photon pairs have been carried out. This has the advantage that instead of attenuated laser pulses a continous wave laser can be used. The gating by the detection of the idler photon provides a well localized single photon state for the signal photon, which can either be transmitted or reflected at a semitransparent mirror [41]. Therefore a higher bit rate should be possible, as well as a better understanding for undesirable electromagnetic interference effects can be gained through coincidence detection. A second entanglement based quantum random number generator takes advantage of photon-number path entangled photons produced in a BBO crystal [42]. This non-colinear downconversion scheme results in a two photon interference on a fibre beam splitter. Thus, both photons get either transmitted or reflected. These photons are then separated again at a second beam splitter and registered via coincidence detection. Depending on the coincidence signal of detectors 1 and 2 or 3 and 4, a zero or a one bit is produced.

In the second case, the quantum nature of the spontaneous emission of a LED or a continuous wave laser and therefore the unpredictability in time of a single emission process can be exploited to generate time intervals of random length between two consecutive events [40, 43]. A comparison of the ratio of these then leads to a binary output sequence. Also attenuated pulsed sources, where each pulse can in principle contain zero or more photons can be used [44]. Another implementation which makes use of spontaneous emission are random number generators based on a measurement of the phase noise. Regarding to [45] this can be done with a stabilized in-fibre Mach-Zehnder interferometric setup. The binary random sequence is then produced by comparing single events at a certain sampling frequency with the mean value of the whole sequence as the threshold.

Both methods have their own advantages and disadvantages concerning their operation. In general, generators, that work with two detectors have a higher operating speed but are more difficult to calibrate and to keep in a stable operation mode. Therefore a fast and precise feedback control system is crucial to take small efficiency deviations of the different paths and of the photon detectors into account. On the other hand generators working with just one detector save the trouble of an extensive calibration of the system but they are limited in their operational speed, since the discretization of time intervals (due to counting of a high frequency periodic signal or a time to amplitude conversion) is more favorable to lead to time intervals of equal length, which are then discarded by the comparison algorithm.

2.2.3 Hybrid random number generators

There exist also two different types of hybrid random generators, which are a combination of true and pseudo random number generators. The first type of this kind compares the two produced bit sequences and performs an XOR operation, which yields a zero if the bits are the same and a one if they are

different. The second more common alternative is to use a physical random number generator to produce the initial values of a deterministic random number generator. In the first case a continous stream of random numbers is produced, whereas in the second random numbers are only trusted until the maximum period length of the algorithmic generator is reached. Afterwards a new seed, produced by the TRNG, has to restart the random number generation process again.

2.3 Randomness tests

Over the last decades several techniques have been developed to test if a sequence of "random" numbers is truly random or not. The particular test suites with the containing test classes will be discussed later in this section.

In general there are three criteria a random sequence has to fulfil. Since perfectly unbiased sequences will only be generated by pseudo random number generators these following criteria are valid only in a certain range of validity. Primarily all bits of a sequence should be nearly equally distributed for sufficiently long sequences. Since the bits are independent they should also be unpredictable. The third criterion is irreproducibility.

It is also important to introduce the concept of a reference level α [46], which specifies the probability that one of these tests fails even though the sequence is completely random (for example produced by a radioactive decay). Considering a binary sequence of 1000 bits, there are several different combinations of zeros and ones possible but each bit has $p = \frac{1}{2}$ of being either a zero or a one. In general zeros and ones are mixed but they should yield a uniform distribution for sufficiently long sequences. For a small sample such as 1000 bits a random sequence can also consist of 1000 identical bits. This does not seem pretty random at first sight. If one flips a coin for example one would assume some kind of trick or a certain preparation if it comes up heads 1000 times in a row. In fact, there is a very small probability that this happens, namely $p = 2^{-999}$. A statistical test would also reject the underlying hypothesis for this biased sample. The probability that such an error occurs even tough the sequence is completely random is the significance level[1] α.

For the evaluation of random numbers, there are three different approaches [47]:

- Threshold values: In this case the sequence complexity of a binary random sequence is computed and compared to a certain threshold value. According to their relation the test might be passed or failed.

- Range of validity: Again the complexity of a sequence is computed. The decision criterion now is specified by certain range depending on the significance level α. Therefore whenever one changes the significance level the range has to be recomputed.

[1] Typical values for the significance level are 0.01, 0.03 or 0.05.

- P-values: The probability for a certain test statistic is computed. These p-values hold for abitrary significance levels.

Since the latter of these guarantees the highest degree of flexibility - even though the computation might be more complex - only this approach will be considered in the next subsection.

2.3.1 General test procedures

The χ^2 test

The χ^2 test is one of the best known statistical tests to test random sequences and is therefore as well implemented in the software programme of our quantum random number generator (QRNG). More explicitly spoken the quality of the produced random numbers is displayed in "real time" at the input screen. The term real time has been put in quotation marks, because it is always a sequence of random numbers has to be considered. This argument is valid since the response time of the human eye is much greater than the sampling time of the QRNG.

In general, a sequence of n independent observations can be categorized into k different cases, which occur with a certain probability p_k. Our random number generator just generates a binary sequence of zeros and ones. Hence there are only two categories with probability $p_0 = p_1 = \frac{1}{2}$ for each independent event. The expected number of zero and one events therefore is np. Getting back to classical coin tossing with $n = 1000$ repetitions a perfectly uniform distribution yields 500 times heads and 500 times tails. The constraint that only finite sequences can be taken into account lead to a certain bias, for example 505 times zero and only 495 times one. The sum of the squares of the differences between the number of expected events and observed events is then the χ^2 value, which should be low but according to [48] not too low. This simply means that perfect randomness without any bias is "too good to be true". If the χ^2 value is still between 95 and 90 percent or 10 and 5 percent, these values are also suspicious.

Another point which is missing in this example is the possibility of different probabilities for different categories. For example considering a craps game, where the player has to throw two dice [48]. Here the probability $p_2 = \frac{1}{36}$ of throwing a two is much smaller than the probability $p_7 = \frac{1}{6}$ of throwing a seven. Therefore a bias in the latter case would contribute more to the χ^2 value. The solution of this problem is a description by a weighted sum of the form

$$\chi^2 = \sum_{i=1}^{k} \frac{(Y_i - np_i)^2}{np_i} \tag{2.6}$$

with the observed numbers Y_i. Since the equations

$$\sum_{i=1}^{k} Y_i = n, \qquad \sum_{i=1}^{k} p_i = 1 \tag{2.7}$$

hold one can easily see that the observed events are not completely independent anymore. This is important for the evaluation of the obtained χ^2 value since look up tables [49, 50] depend on the degrees of freedom of the χ^2 distribution. The first part of equation 2.7 reduces the degrees of freedom by one. In general the number of degrees of freedom is $\nu = k - 1$. For convincing results the length of the sequence should be sufficiently long that the expected number of every class is $np_i \geq 5$.

The Kolmogorov-Smirnov test

In contrast to the χ^2 test, which can be applied if the sequence can be divided into several classes k, the Kolmogorov-Smirnov or for short KS test, works for continous samples. For example if a mapping to the interval [0,1) is made, there are infinitely many values lying in between.

In this case the distribution function for different values of a random quantity X is defined in the following way

$$F(x) = p(X \leq x) \tag{2.8}$$

where x lies in the intervall [0,1).

Now the hypothesis that the random variables X really follow this distribution has to be tested. This can be done by a comparison to an empirical distribution function $F_n(x)$ of the form:

$$F_n(x) = \frac{\#\{X_j : X_j \leq x\}}{n} \tag{2.9}$$

$\#X_j$ is the number of the obtained random quantities X_j and n is the number of all independent observations. Since $F_n(x)$ can be greater or smaller than $F(x)$ the KS test consists of the two parts K_n^+ and K_n^-:

$$\begin{aligned} K_n^+ &= \sqrt{n} \max_{-\infty<x<+\infty} (F_n(x) - F(x)) \\ K_n^- &= \sqrt{n} \max_{-\infty<x<+\infty} (F(x) - F_n(x)) \end{aligned} \tag{2.10}$$

Similar to the χ^2 method these values can be looked up in mathematical formularies to get a feeling for the quality of the produced random numbers. The difference for the KS test is that these values are not approximations only valid for large n but exact values. Nevertheless the choice of n remains crucial since an overly large number of n averages out local nonrandom effects, whereas on the other hand a large number of observations is desirable for the differentiation between two similar probability distributions. To overcome these difficulties another KS test has to be made from the obtained results. This works in the following way: K_n^+ and K_n^- values are calculated for a mid-level size of obeservations such as 1000. This yields

$$K^+_{1000,1} \quad K^+_{1000,2} \quad \dots \quad K^+_{1000,r}$$

r different values for K_{1000}^{+}. Now a KS test for these values is compared to the distribution function

$$F_{\infty}(x) = 1 - e^{-2x^2} \tag{2.11}$$

with $x \leq 0$.

This approximation is valid for the case of sufficiently large n and then applies to K_{1000}^{-} as well, because the two empirical functions should behave in the same way. Hence this approach is able to rule out nonrandom behaviour on a local as well as on a global scale.

2.3.2 Empirical tests

In the following, empirical tests contained in the dieharder test suite [51] will be grouped together and discussed according to their test properties.

Bit distribution tests

One of the easiest ways to evaluate whether a series appears to be random or not is the so called monobit test. Hence this kind of test investigates the frequency of the occuring classes k. For a binary sequence zeros and ones should be equally distributed.

The series test considers non-overlapping pairs (Y_{2i+1}, Y_{2i+2}) of a sequence. In the binary case this corresponds to the four outputs produced by our two QRNGs, namely (00), (01), (10) and (11), which each appear with the probability $p = \frac{1}{4}$. The number of classes increases with $k = 2^d$ where d is the number of consecutive bits. Hence the probability of such pairs, triples and so on, of lying in a certain class is $p_k = \frac{1}{2^d}$. The subsequent analysis can be done by a χ^2 test. Since only independent non-overlapping pairs and so forth are taken into account also the sequence of random bits has to grow if one will not discard higher orders from a meaningful χ^2 test. The generalization from single bits or pairs to n-tuples is called a bit distribution test.

Matrix rank tests

This subcategory of randomness tests forms random binary NxM matrices as well as their special case of quadratic matrices with N=M. After the rank determination of the respective matrices they are organized in categories according to their rank with the exception of low rank matrices. Because of their low probabilites these are categorized together until a certain threshold value which depends on the dimension of the matrix. Finally to prove their distribution a χ^2 test is performed.

Overlapping n letter words tests

The Bitstream, the Overlapping Pairs Sparse Occupance (OPSO) test, the Overlapping Quadruple Sparse Occupance (OQSO) test and the DNA test are based on the distribution of missing n letter words using a specific alphabet. The

difference between them is the amount of letters in the corresponding alphabet and the word length. The two most extreme cases are the Bitstream test (20 letter words in a 2 letter alphabet) and the OPSO test (2 letter words in a 1024 letter alphabet). The number of missing words should in the end be normally distributed around a certain mean value with a test dependent variance.

Minimum distance tests

This test produces random points lying inside a cube. Around each of these points a sphere, that is just as large that the next point can be reached is centered. The smallest volume of such a sphere and therefore also r^3 should be exponentially distributed around a certain mean value. Subtracting this distribution from one then leads to uniform variables that can be tested with a KS test.

Also an alternative version of this test is included in the dieharder test suit. In the two-dimensional case the spheres are substituted by circles.

Permutation test

This test divides the input sequence into several subsequences $(U_0, U_1, ..., U_t)$ of length t. Afterwards the frequency of the t! permutations of this subsequence is analyzed by a χ^2 test.

2.4 Experimental realization

2.4.1 Source of random numbers

The quantum random number generator which is used in our EPR steering experiment is a modification of the one developed by Thomas Jennewein and other colleagues from our quantum information and quantum optics group [52]. According to the previous section 2.2.2 the underlying mechanism of this optical random number generator is the inherent randomness of a single photon impinging on a 50:50 or a polarizing beam splitter. In the second case the photons preliminarily have to get polarized at 45° with respect to the orientation of the optical axis of the beam splitting crystal. This can be done by putting an additional polarization foil into the photon path between the LED output and the polarizing beam splitter and has the advantage that any desired bias between the two detectors can be adjusted. According to which detector fires, a binary random sequence is produced.

The electric circuit diagram as shown in figure 2.1 shows the electric components involved in the random number generation process. In the beginning single photons of a red light emitting diode (LED) source with a very low coherence time are guided to the beam splitter where each photon randomly decides which of the two paths it will take. The low coherence time together with the photon production rate in the source guarantee no disturbing interference effects while a sufficiently high operating speed can be maintained. In the second step

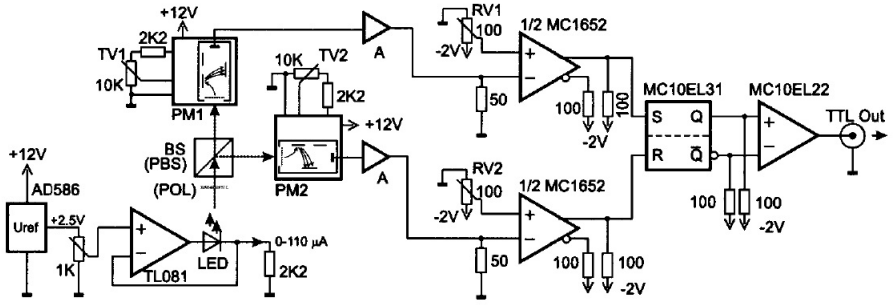

Figure 2.1: Electric circuit diagram of the optical quantum random number generator. Both configurations either with a beam splitter (BS) or a polarizing beam splitter (PBS) in combination with a polarizer (POL) are shown. After the registration ("click") at one of the two photomultiplier tubes (PM1, PM2) the signals are post processed, combined at the flip-flop (MC10EL31) and finally a binary random sequence is generated (figure taken from the original pubilcation [52]).

the photon gets detected in one of the two photomultiplier tubes (PM1, PM2), where additionally to the detection itself a first amplification occurs. Fine adjustments of the tube voltages and therefore of the pulse rates and amplitudes can be done by potentiometers (TV1, TV2). After an additional amplification stage (A) the signals have to be converted to a certain kind of logic family before they can be fed into the RS flip-flop. This conversion to a high speed emitter coupled logic (ECL) signal is done by two comparators (MC1652). The RS flip-flop is the core of our random number generator, where the binary random sequence finally gets produced. The letters RS in this context just refer to "set" and "reset" of the output signal which corresponds to a one and a zero bit at the output Q. The operating principle now is as follows: if detector one, which corresponds to the set input, fires, a high voltage signal is produced. As long as this detector clicks no change in the output signal will take place. If detector two regsiters a photon, the reset input of the flip-flop receives a signal. Hence the high signal is reset to low again. In the end it is convenient to convert the ECL signal into a transistor transistor logic (TTL) pulse, which is less power consuming and also less sensitive to discharge effects. To get a continous 32 bit stream of random numbers for the further usage on a personal computer the random sginal is stored in a shift register and read out according to the cycling time of an internal (old configuration) or external clock.

2.4.2 Operation of the QRNG

Now this is the point where our implementation differs from the original configuration since an external clock was not provided at that time. The external clock needs to be built in to tap the output signal of the QRNG before it gets

processed by the FPGA board. This has the advantage of a low internal delay time (45 ns) while the internal regulation cycle keeps running. Therefore the clock output port was converted into a clock input port which triggers the rate of random numbers loaded into the shift register. The additional clock output port at the front panel of our QRNG is responsible for the speed of the read-out mechanism. In both input ports square wave signals produced by arbitrary function generators are fed in.

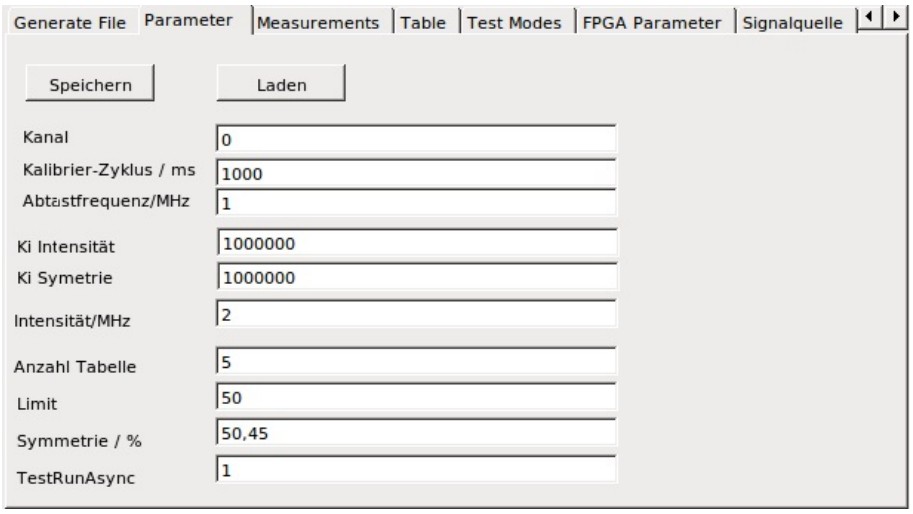

Figure 2.2: Illustration of the different parameter settings inside the TRNG software (version 1.4).

Figure 2.2 shows the input possibilities concerning the different types of operation which are determined by the TestRunAsync parameter. If it is equal to one then only the regulation cycle (intensity, symmetry and quick test of randomness) is triggered internally. The second adjustment option is zero, which states that the output can be triggered internally by the internal sampling frequency.

Another extension of the TRNG software is the symmetry parameter added to the menu. This feature is of great importance regarding the fine tuning of the occurence of the three measurement settings before each measurement run. Since any bias at least perturbs the measurement results, it has to be ruled out carefully by comparison of the number of appearances of the individual bases in the coincidence counting logic. Although it is rather difficult to control the functional interaction of two QRNGs our implementation has the advantage that these quantities can be directly read out from the coincidence counting software and therefore guarantee mutually unbiased bases.

The behaviour for a given parameter set can be viewed in the measurement control tab (fig. 2.3). Thereof there are two quantities from special interest, namely the symmetry and the χ^2 value, since it takes some time until the QRNG

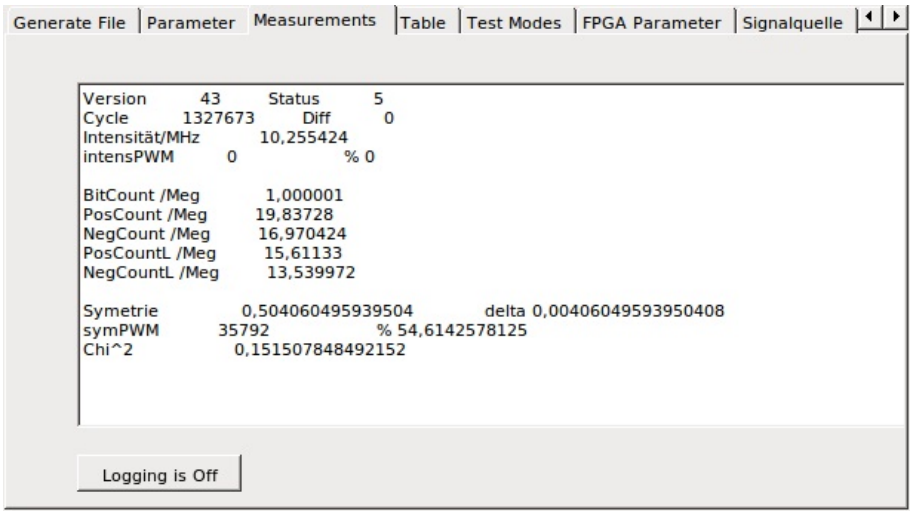

Figure 2.3: The measurement control tab of the TRNG software shows real time information of the operation of the QRNG for a given parameter set.

has reached the values which have been defined in the parameter menu. These values are updated according to the number of calibration cycles per millisecond (fig. 2.2).

The symmetry value gets computed by counting the one bits of one cycle and dividing this number through the total amount of bits from the last cycle. The rating of the quality of the generated random numbers is done by a bit occurrence test, which counts the occurrence of n-zero bit and n-one bit blocks of 32 bit random number sequences. According to the laws of probability the occurence of these n-bit blocks should approximately drop linearly. To prove this behaviour a χ^2 test, comparing the expected occurence and the actual occurence of blocks, is performed.

If finally all of these settings behave according to the set parameters either an experiment can be performed or a random file can be recorded and tested afterwards by the dieharder test suite. For the file generation there is a separate tab in the TRNG software (fig. 2.4), where the file name and the file size can be specified. Also an alternative option concerning the file type can be chosen if the output as a binary sequence is not desired. In the *text* type option, each byte gets converted into a number between 0 and 255 in decimal representation.

2.5 Test results

2.5.1 Execution of the dieharder test suite

After recording a randomxxx.dat file the dieharder test suite has to be executed to check the random properties of the generated sequence. In contrast to the

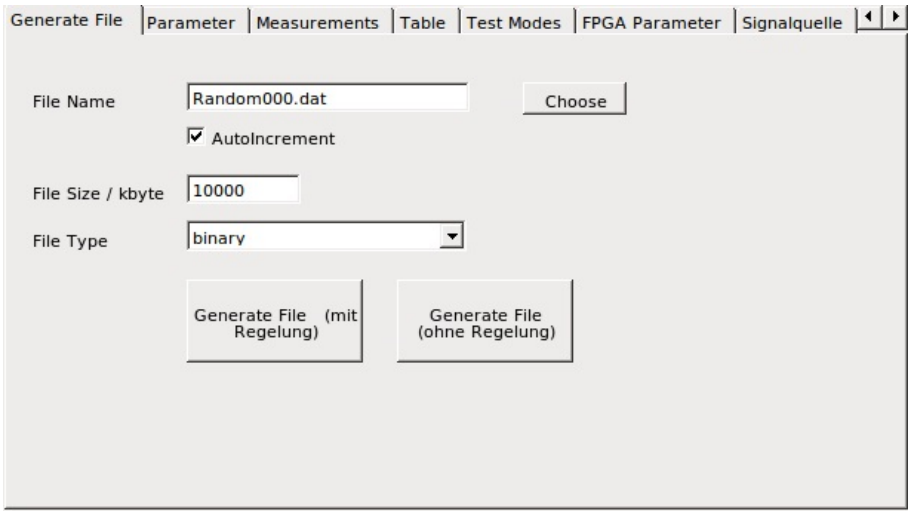

Figure 2.4: The generate file tab specifies the file name and length as well as the output format.

TRNG software dieharder (version 3.31.1) does not have such a nice graphical representation but is rather straightforward to use in the Linux terminal since there is very detailed online documentation [51] available. If one prefers to get the possible input options in the terminal directly this can be easily done as well by simply executing the command *dieharder* in the respective subfolder. The corresponding comand line regarding our tests is

dieharder -a -q -g 201 -f randomxxx.dat > outputfilexxx.txt

which has the following meaning: a tells the programm that all tests should be performed, q specifies how the output is illustrated (passed, weak, failed), g 201 is the file input raw and f is simply there to declare the filename of the inputfile.

2.5.2 Tests with fixed frequencies

Even though the main focus in testing our quantum random number generator is the operating speed, there are several other parameters which have to be determined, before it makes sense to test which frequency is ideal to trigger the read out mechanism of the produced random numbers. Therefore several parameters, such as the file size or the elapsed time between when the QRNG was switched on and the random number file generation, have been tested for fixed frequency inputs (30 MHz sampling frequency and 1 MHz read out frequency).

The test results regarding different sizes of the input file have not only an effect on the tested sequence itself but are also important for the further test

procedure, since the generation of files that are larger than 1 GB is a rather time consuming process. As shown in figure 2.6 there is a significant difference of the

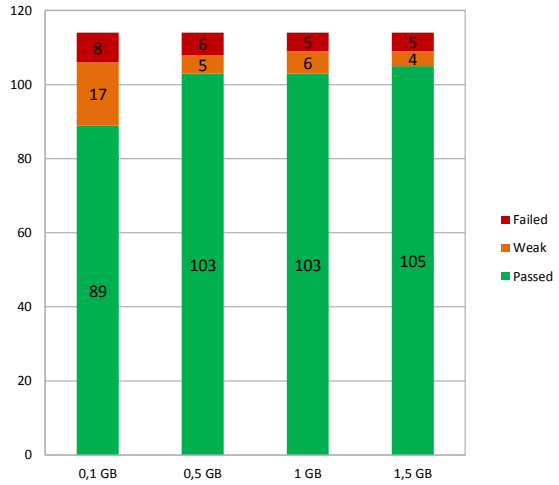

Figure 2.5: Test statistics depending on the file size of the input file.

test results concerning the 100 MB and the 500 MB file, while afterwards only small changes occur when the file size gets further increased. This result can be understood in the following way: on one hand the 100 MB file might be too small that some tests, which need a very large number of consecutive bits, can not be repeated sufficiently often and therefore suffer from worse test statistics. On the other hand an ideal infinite random sequence should not suffer from any bias. Since only the limit for large n can be treated, it is natural that the test results get better for larger file sizes even though the performance of such randomness tests itself is limited to finite samples. From a functional point of view it can be said that 500 MB files do not suffer from any test specific behaviour and can therefore be regarded as trustable samples.

The second question adressed in this section is whether the QRNG has to warm up for a certain time until a stable operation can be ensured. To answer this question five files with different time delays, starting with $\Delta t = 0$ until $\Delta t = 120$ after two hours of operation, have been recorded. According to the results of figure 2.6 there are two possible explanations. The first one is simply that no characterisic behaviour is shown since the first result and the result obtained after 90 minutes of operation are very similar. Because of the fact that the test results shown for 60 minutes of operation are better than the ones for 90 minutes one could believe that this behaviour is caused only by statistical fluctuations. On the other hand there is strong experimental evidence, especially for the adjustment of two QRNGs, that a stable operation is reached only after a certain warm up time. This suggests that the test results for $\Delta t = 90$ should be attributed to statistical fluctuations while the bad behaviour in the beginning is real and not such an artefact.

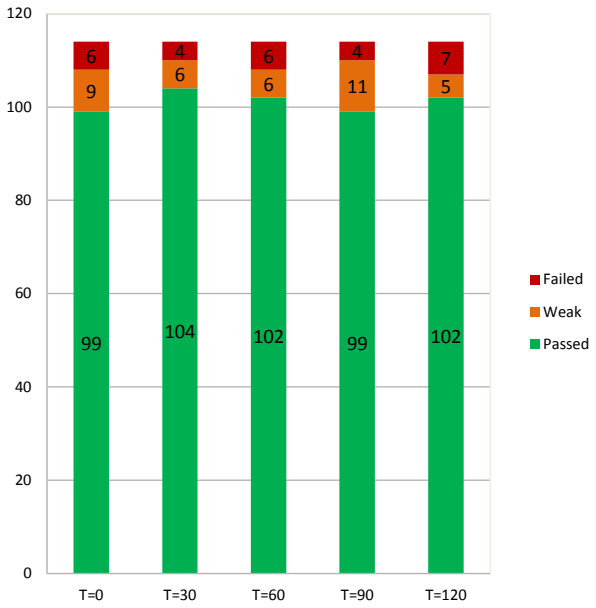

Figure 2.6: Test performance depending on the time of operation.

2.5.3 Determination of the ideal read out frequency

The read out frequency is the most crucial part about the operation of our QRNG, since it ideally has to pass all the tests contained in the dieharder test suite and simultaneously operate as fast as possible to meet experimental demands. According to the toggle rates reached in [52], the sampling frequency was again set to 30 MHz, ensuring a low autocorrelation time. To get the most precise results only 1.5 GB files have been recorded and tested. As shown in figure 2.7 it is favorable to use small read out frequencies around 1 MHz since the test results for a faster read out are not good enough. Nevertheless the lowest frequencies tested also do not pass all the tests. On one hand this is due to some tests contained in the dieharder test suite, which are known to let all random number generators fail. On the other hand this is rather a philosophical question about the definition of "perfect" randomness, if such a definition is possible. As already mentioned in the beginning of this chapter random numbers too good to be true are also suspicious. Therefore, to conclude, one should not be bothered that a small amount of tests ($< 5\%$) fails.

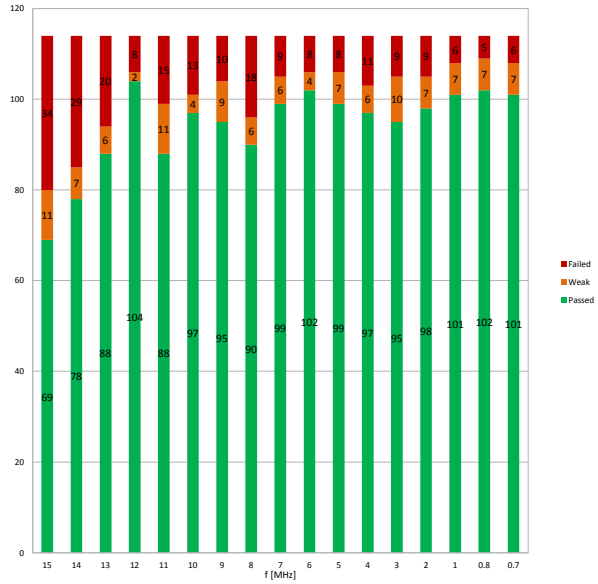

Figure 2.7: Test results for different read out frequencies.

Chapter 3

Experimental EPR-Steering Setup

3.1 Principles of the individual modules

3.1.1 Nonlinear optics, spontaneous parametric downconversion and phase matching

The origin of an induced polarization in a nonlinear crystal is the interaction of an electric field with its atoms. The resulting force on the electron cloud disturb the equilibrium position of the core-electron system and induces a spatial separation of the respective charge concentrations [53].

For small electric fields the relation between the polarization P and the electric field E is linear

$$P_i = \epsilon_0 \chi_{ij}^{(1)} E_j \tag{3.1}$$

whereas ϵ_0 is the vacuum permittivity and $\chi_{ij}^{(1)}$ is the linear term of the electric suceptibility. This approximation is valid as long as the applied electric fields are small compared to the field strengths in interatomic processes, which are approximately around $10^5 - 10^8$ V/m. If the laser power is increased the electric field strengths get close to this regime and the nonlinear expansion coefficients are not negligible anymore.

$$P_i = \epsilon_0 [\chi_{ij}^{(1)} E_j + \chi_{ijk}^{(2)} E_j E_k + \chi_{ijkl}^{(3)} E_j E_k E_l + \dots] \tag{3.2}$$

For the further description I will restrict myself to second order nonlinear processes [54], since these are relevant for our Sagnac source.

Two linearly polarized monochromatic plane waves travelling along the z-direction create the following electric field:

$$E = [E_1 \cos(k_1 z - \omega_1 t + \Phi_1) + E_2 \cos(k_2 z - \omega_2 t + \Phi_2)] \tag{3.3}$$

Inserting this superposition into the lowest order non linear term in the expansion for the polarization this yields

$$\begin{aligned} P^{(2)} = \epsilon_0 \chi^{(2)} [& \frac{1}{2} E_1^2 \cos[2(k_1 z - \omega_1 t + \Phi_1] \\ & + \frac{1}{2} E_2^2 \cos[2(k_2 z - \omega_2 t + \Phi_2] \\ & + \frac{1}{2}(E_1^2 + E_2^2) \\ & + E_1 E_2 \cos[(k_1 + k_2) z - (\omega_1 + \omega_2) t + (\Phi_1 + \Phi_2)] \\ & + E_1 E_2 \cos[(k_1 - k_2) z - (\omega_1 - \omega_2) t + (\Phi_1 - \Phi_2)]] \end{aligned} \tag{3.4}$$

which gives raise to several parametric effects. The first two terms describe the second harmonic generation (SHG) of $\omega_{1,2}$. The third term is known as optical rectification (OC). The last two terms describe the sum frequency generation (SFG, *upconversion*) and the difference frequency generation (DFG, *downconversion*).

Another - from an experimental point of view - interesting process is missing in this classical description, namely the process of spontaneous parametric downconversion (SPDC). Until now only processes with two incident photons have been taken into account. Quantum mechanically also processes with only the pump photon present can result in difference frequency generation. The origin of the signal input is in this case the zero point fluctuation of the vacuum state.

A proper description has to be done in the context of a quantized field theory, where the interaction Hamiltonian takes the form [55]:

$$H = \epsilon_0 \int_V d^3 r \chi^{(2)} E_p^{(-)} E_s^{(+)} E_i^{(+)} + h.c. \tag{3.5}$$

With

$$E_j^{(+)} = \epsilon_j \int_V d^3 r a_{j,k}^{\dagger}(\omega_j) e^{i(\mathbf{k}_j \cdot \mathbf{r} - \omega_j t)} \tag{3.6}$$

whereas $a_{j,k}^{\dagger}$ is the creation operator and the index j refers to the signal or idler field and the index k to the ordinary or extraordinary mode.

The energy and momentum conservation conditions of such three wave mixing processes are called phase matching conditions and guarantee that the waves produced at different positions in the crystal interfere constructively. The energy uncertainty is negligible hence the corresponding equation can be easily written down:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i \tag{3.7}$$

In the case of momentum conservation the finite crystal length is responsible for a phase missmatch $\Delta\vec{k}$, which reduces the maximum intensity. Therefore the condition reads

$$\hbar\Delta\vec{k} = \hbar\vec{k}_p - \hbar\vec{k}_s - \hbar\vec{k}_i \tag{3.8}$$

in the most general case. The case where all wave vectors are parallel is called collinear phase matching. Considering this situation in a birefrigent crystal it can be shown that depending on the polarization modes of the three waves phasematching can be achieved [54]. Thus, the vector of the pump photon needs to be shrunken while at least the vector of the signal or the idler photon has to get streched. These parameters mainly depend on the propagation direction in the crystal.

In positive uniaxial crystals $n_e > n_o$ is valid and therefore the k-vector of the extraordinary beam is larger. Phase matching can be reached if the pump beam is ordinarily polarized, where at least one of the two other beams has to be extraordinarily polarized. If both beams are parallel (extraordinarily polarized) the process is called type I phase matching. In the case where the signal and idler beam are orthogonally polarized the type II phase matching condition can be fullfiled. For negative uniaxial crystals these conditions get changed since $n_o > n_e$.

Recent developments in nonlinear optics came up with the idea of quasi phase matching, where phase matching can be reached even in presence of a certain phase mismatch Δk. This mismatch gets compensated by periodically changing the phase of the non-linearity during the crystal growth. One big advantage of this technique is that the crystals can be tailored in such a way that the coefficients of the non-linearity are much stronger than in birefringent crystals and therefore the down conversion efficiency gets higher. The quasi phase matching condition now depends on the poling period Λ:

$$\vec{k}_p(\lambda_p, n_p(\lambda_p, T)) = \vec{k}_s(\lambda_s, n_s(\lambda_s, T)) + \vec{k}_i(\lambda_i, n_i(\lambda_i, T)) + \frac{2\pi}{\Lambda(T)} \tag{3.9}$$

3.1.2 Electro-optics

The electro-optical effect is understood to mean that the refractive index of a transparent material gets changed if a certain voltage is applied. Hence the refractive index becomes a function of the electric field $n = n(E)$ and the index ellipsoid of the crystal gets modified. Since this quantity is slowly varying over E it can be expanded into a Taylor series around $E = 0$. For this expansion it is convenient to rewrite it in terms of the electric impermeability η which is directly proportional to the electro-optic coefficents $\mathfrak{r}$ and $\mathfrak{s}$, which are tensors of third respectively fourth order [56]:

$$\eta_{ij}(\mathbf{E}) = \eta_{ij} + \sum_k \underbrace{\frac{\partial \eta_{ij}}{\partial E_k}}_{\mathfrak{r}_{ijk}} E_k + \sum_{k,l} \underbrace{\frac{1}{2}\frac{\partial^2 \eta_{ij}}{\partial E_k \partial E_l}}_{\mathfrak{s}_{ijkl}} E_k E_l + \dots \tag{3.10}$$

The relation between the refractive index n and the electric impermeability η is given by:

$$\eta = \frac{1}{n^2} \tag{3.11}$$

In most materials the term linear proportional to the electric field is dominating and higher order terms become negligible. This second term in (3.10) is known as Pockels effect and is mainly used for phase or amplitude modulation. Depending on the direction of the electric field lines a differentiation between the longitudinal (parallel to the direction of propagation) and the transversal (perpendicular) Pockels effect is made. For centrosymmetric crystals $n(-E) = n(E)$ and therefore the linear term vanishes. These media, where the refractive index depends on E^2, are called Kerr media.

In our experiment two Pockels cells are used to manipulate the phase of horizontally or vertically polarized photons produced in our Sagnac source. They therefore act as retarding wave plates. A decomposition of the light beam into eigenfunctions of the ordinary and extraordinary crystal axis leads to the following transformation of the polarization state [8]:

$$\begin{pmatrix} V_e' \\ V_o' \end{pmatrix} = \underbrace{e^{-i\Phi} \begin{pmatrix} e^{-i\frac{\Gamma}{2}} & 0 \\ 0 & e^{i\frac{\Gamma}{2}} \end{pmatrix}}_{W_0} \begin{pmatrix} V_e \\ V_o \end{pmatrix}, \qquad R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{3.12}$$

The phase retardation of Γ is due to different phase velocities of the ordinary and extraordinary beam

$$\Gamma = (n_e - n_o)kd \tag{3.13}$$

whereas d is the thickness of the wave plate. The polarization state in the laboratory coordinate system can be obtained by a retransformation by the means of two rotation matrices $R(\theta)$.

$$\begin{pmatrix} V_x' \\ V_y' \end{pmatrix} = R(-\theta) W_0 R(\theta) \begin{pmatrix} V_x \\ V_y \end{pmatrix} \tag{3.14}$$

For a half wave plate (HWP) the phase retardation becomes $\Gamma = \pi$. In the case of a quarter wave plate (QWP) it is $\Gamma = \frac{\pi}{2}$. Hence the thickness of the crystal becomes

$$d_{HWP} = \frac{\lambda}{2} \frac{1}{(n_e - n_o)}, \qquad d_{QWP} = \frac{\lambda}{4} \frac{1}{(n_e - n_o)} \tag{3.15}$$

The question now is how this properties can be achieved by an electro-optic modulator. As already mentioned above the index elipsoid gets modified through the presence of an additional static electric field applied to the crystal. Considering the longitudinal Pockels effect with $\mathbf{E} = E_z$, the x and y axes of the ellipsoid aquire an additonal term depending on the electric field whereas $n_z = n_e$ [57]:

$$n_{x'} = n_0 - \frac{1}{2} n_o^3 \mathfrak{r}_{63} E_z, \qquad n_{y'} = n_0 + \frac{1}{2} n_o^3 \mathfrak{r}_{63} E_z \tag{3.16}$$

Thus the phase retardation

$$\Gamma = (n_{y'} - n_{x'})kd = \frac{2\pi}{\lambda} n_o^3 \mathfrak{r}_{63} V \tag{3.17}$$

depends on the applied voltage V ($E = \frac{V}{d}$). The voltage where the Pockels cell acts as a half (quarter) wave plate is therefore:

$$V_{HWP} = \frac{\lambda}{2}\frac{1}{n_o^3 \mathfrak{r}_{63}}, \qquad V_{QWP} = \frac{\lambda}{4}\frac{1}{n_o^3 \mathfrak{r}_{63}} \tag{3.18}$$

3.1.3 Avalanche photo diodes

The single photon counting modules used in our experiment are avalanche photo diodes (APDs) which are silica semiconductor devices that make use of the photoelectric effect for which Albert Einstein received the Nobel prize in 1921. Since single photon events need to be registered, an amplification is needed to work with the resulting electronic signal. This can be done by the utilization of the right working point which is biased near the breakdown voltage. An impinging photon on the detector then causes free charge carriers and in the nonlinear Geiger region, both free electrons and holes contibute to the ionization process and guarantee a sufficiently high electric signal [58]. Quenching and recharge circuitries are necessary so that on one hand the diode doesn't heat up too much and gets destroyed and on the other hand the dead time can be kept low.

Depending on the quantum information task we want to perform, there are different experimental demands on these photon detection modules.

3.2 Experimental realization

3.2.1 Entangled photon pair production

As described in section 3.1.1 spontaneous parametric downconversion is a nonlinear process of lowest order and can be used to produce pairs of entangled photons. The scheme used in our experiments is a polarization Sagnac interferometer (PSI) where in contrast to schemes using BBO crystals no additional compensation crystals are needed. The core of this configuration is a 10 mm periodically poled KTP crystal which is attached to a Peltier oven. This alows a temperature stable operation within $\Delta T = \pm 0.1°\mathrm{C}$. Quasi phase matching for type II downconversion and therefore indistinguishability between the wavelengths of signal and idler photon can be reached if the temperature gets fixed to a certain (crystal dependent) value. The functional principle of the bidirectionally pumped Sagnac loop can be easily explained by the means of figure 3.1. Fig.3.1(a) shows the vertical component of the blue 405 nm pump beam which corresponds to a clockwise run through the Sagnac loop. The vertically polarized component gets reflected at the polarizing beam splitter (PBS) and then passes through a dual wavelength half wave plate (dHWP) oriented at $\frac{\pi}{4}$. This rotates the polarization from vertical to horizontal. Next - after hitting a mirror - the downconversion process in the PPKTP crystal takes place and produces two 810 nm photons one horizontally polarized the other vertically polarized. Due to different group velocities the horizontally polarized photon

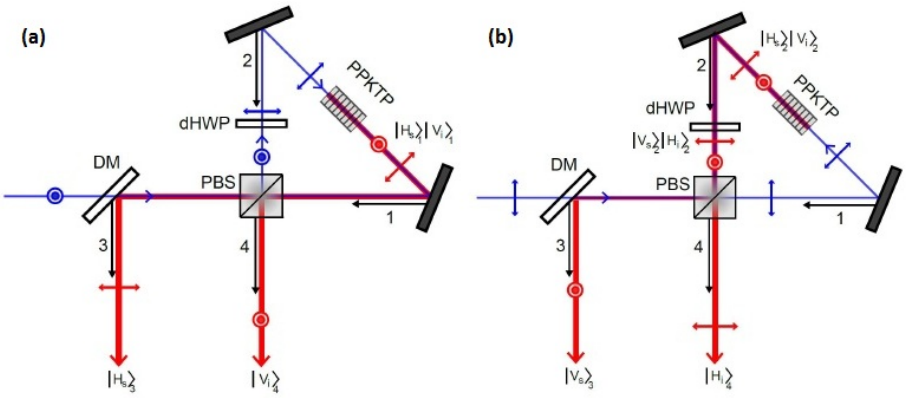

Figure 3.1: Schematic illlustration of the polarization entangled Sagnac source. (a) shows the vertical component of the pump light which propagates in clockwise direction. In (b) the horizontally polarized component, which gets transmitted at the first PBS and therefore propagates counterclockwise, is shown (figure adapted from[59]).

propagates faster through the crystal. At a mirror both polarizations get reflected and afterwards separated by the same polarizing beam splitter as in the beginning.

Fig.3.1(b) refers to the counter clockwise direction of the Sagnac loop and initially horizontally polarized pump light. This time the polarizing beam splitter is passed and after hitting the mirror the pump photons interact with the nonlinear crystal. Again the horizontally polarized photon is faster and hits the mirror first. The difference in group velocity then gets compensated by the dual wavelength half wave plate. Finally the polarizing beam splitter separates the different linear polarization directions.

If the polarization direction of the pump beam is diagonal half of the photons will get reflected and half of them will get transmitted at the polarizing beam splitter. This yields the entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|H_s\rangle_3 \otimes |V_i\rangle_4 + e^{i\Phi}|V_s\rangle_3 \otimes |H_i\rangle_4) \tag{3.19}$$

whereas the phase can be adjusted by a half wave and a quarter wave plate in the pump beam to get a proper $|\Psi^-\rangle$ state that is needed for the steering experiment.

3.2.2 Switching of the Pockels cells

The steering inequalities can be violated more easily if the number of measurement bases gets increased [60]. In our setup with avalanche photo diodes (APDs) as single-photon detectors with typical photon detection efficiencies[1] $\eta \leq 60\%$

[1] At 810 nm.

the only way of violating these inequalities loophole free, is the implementation of three different measurement bases in which the entangled photon pairs of the Sagnac source are measured. In our steering experiment these bases are H/V, D/A and R/L. The relations between them are shown in table 1.1. The simultaneous closure of the locality and freedom of choice loophole requires a fast switching process between them. This is done by two consecutive Pockels cells, one acting as half wave plate at 22.5°, the other as a quarter wave plate at 45°. The switching time of the Pockels cells is 22 ns and consits of an internal electric delay of 18 ns and of 4 ns rise time until the high voltage signal is reached [59]. According to the binary outcome of our two quantum number generators (QRNGs) there are four combinations (00), (10), (01) and (11) possible, which trigger the voltage supply for the Pockels cells:

PC1	PC2	Polarization	Transformation	Measurement
0	0	H/V	$\hat{\mathbb{1}}$	$\hat{\sigma}_z$
V_{HWP}	0	D/A	$\frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$	$\hat{\sigma}_x$
0	V_{QWP}	R/L	$\frac{1}{\sqrt{2}}(\hat{\mathbb{1}} + i\hat{\sigma}_x)$	$\hat{\sigma}_y$
V_{HWP}	V_{QWP}	L/R	$\frac{1}{2}(i\hat{\mathbb{1}} + \hat{\sigma}_x - \hat{\sigma}_y + \hat{\sigma}_z)$	$-\hat{\sigma}_y$

Table 3.1: Illustration of the four possible outcomes produced by the quantum random generators and their effect on the Pockels cells and therefore on the measured polarization.

In order to avoid double counting of $\hat{\sigma}_y$ regarding the steering inequality (1.41) the last one of these settings is discarded but has been written down here for completeness.

3.2.3 Coincidence counting logic

According to the steering task (c.f. section 1.6) and equation (1.42) the steering value can be evaluated by counting the coincidence results of the two distant observers Alice and Bob.

Thus, a coincidence counting logic is needed, whose key ingredient is a Xilinx field programmable gate array (FPGA), which performs a logical AND operation. Therefore the logic module assigns to each rising edge of a detection pulse a time bin of 1.56 ns length. The coincidence window now has to be set according to the timing jitter of the respective detectors. On Alice's side the Perkin Elmer SPCM-AQRH silicon photon detectors have a timing jitter of 1.5 ns, therefore the corresponding coincidence window has to be at least 2*1.56 ns. Since the laser components COUNT-series detectors in Bob's laboratory have a higher timing resolution of 800 ps and the fact that accidental coincidence rates resulting from dark counts on Bob's side should be kept as low as possible, the total window of four bins is divided into three on Alice's side and one on Bob's side.

3.3 Space-time arrangement

As mentioned in section 1.5.4 a proper space-time arrangement is the key to the simultaneous closure of the locality and the freedom of choice loophole.

The three main criteria for the closure of the locality loophole are a space-like separation between Alice and Bob, fast switching electro-optical modulators (EOMs) triggered by a quantum random number generator (QRNG) and an independent data aquisition of the two parties with a high timing resolution.

In the EPR-Bohm thought experiment [18] as well as in first theoretical considerations only symmetric space-time arrangements, in the sense of an EPR source in the center and two equally distant measurement apparata, were taken into account. Actually this restriction is not essential for the closure of the locality loophole but as we will see an asymmetric setup has some advantages concerning the closure of the freedom of choice loophole. The quintessence of this loophole was that the settings do not depend on hidden variables produced in the source and the other way around. Hence the asymmetric configuration, where the source is located in Alice's laboratory and the quantum random numbers are produced on Bob's side is the most suitable experimental situation. This argumentation is valid only under the assumption that the photon kept at the source has a sufficently long delay fiber and that the electronic signal produced by the QRNG is transmitted over a classical channel that is not influenceable by local hidden variables anymore.

Another limitation concerning the space-time arrangement is the operating speed of certain components. The electronic signal of the QRNG needs to be converted so that it can be further used to establish a certain measurement setting. This is done by a so called splitter box and takes 30 ns (including all cables). The Pockels cells driver afterwards takes another 22 ns to switch between our three measurement bases. The time delay caused by the measurement itself is 20 ns. This consists of the time it takes from the impinging on the detector until a classical click can be registered (10 ns) and of further 10 ns time for the setting validity window . Further 18 ns are caused by electronic delays (amplification and signal processing) in the coincidence logic. In the best case the timing considerations are equal on both sides of the experiment. Since on Bob's side the switching speed of the Pockels cells is not crucial, also a slower driver could be used, as it was done in our experiment.

The setting independence window only depends on the distance between the two measurement apparata. For a spatial separation by 48 m the resulting time window is $\frac{2L}{c} = 320$ ns. The computation of the outcome independence window is more difficult to treat since all delays on Alice's side have to be taken into account. The vital assumption to ensure outcome independence thereby is that the time when she reports her result to Bob lies outside of the future lightcone of Bob's measurement. Otherwise subluminal communication between them could not be excluded and Bell's assumptions are not valid anymore. The sooner Alice's reporting occurs, the bigger the outcome independence window gets and therefore also the overlap between setting and outcome independence windows increases.

Summarizing these considerations the following delays come into play on Alice's side. First of all Alice has to wait 90 ns until the QRNG produced a trustworthy random number. Afterwards she has to delay her photon until the setting choice has been transmitted through a BNC cable to her laboratory. This process causes a delay of 205 ns. So, in principle after 295 ns the Pockels cells switching process, which takes another 22 ns, could be initiated by a signal conversion process done by the splitter box (30 ns). For the setting validity window and the detection process another 20 ns have to be added. After the signal processing in the coincidence counting logic (18 ns) Alice's measurement can in principle be regarded as completed. However it is convenient to introduce a further 20 ns delay to increase the experimental visibility.

All in all, Alice's measurement process could be finished after 405 ns. Subtracting 160 ns ($\frac{L}{c}$) for any hypothetical influence from the Bob side and building the difference with the setting independence window results in a window of 75 ns for Bob's measurement. To make sure that outcome and setting independence are fullfilled simultaneously a buffer of 25 ns at the beginning and in the end has been introduced. This leads to a trusted measurement window of 20 ns.

3.4 Results and conclusion

Analysis of the single and coincidence counts over 360 runs (each integrated over 30 s) led to a measured steering value of $S_{exp} = 1.049 \pm 0.002$ [27], which clearly violates the steering inequality 1.41 (by more than 20 standard deviations) which is bound to $S = 1$, since a pure state vector must lie on the surface of a unit Bloch sphere. Nevertheless this value is far away from the theoretical bound of 3 which can be understood if the steering inequality is rewritten in terms of a conclusive probability and the visibility. The connection between the measured experimental and the theoretical steering values then simply is:

$$S_{exp} = S_{th}\eta V^2 \tag{3.20}$$

The main factor for the reduction of the theoretical value therefore is the probability of getting conclusive results, which was $38.3 \pm 0.1\%$. This value takes into account the total arm efficiency of the source as well as losses caused by the delay fibre and the two electro-optic modulators. The visibility V on the other hand only gets minimally reduced to $95.05 \pm 0.06\%$ in the worst case by the fact of a not perfect source visibility as well as due to imperfections in the polarization analyzer modules and fibres. Due to the asymetric steering setup and the implementation of three measurement bases the performed experiment did not suffer from any loopholes and therefore could rule out an important subclass of local realistic theories.

This result can be further regarded as a test of Born's rule since Bob locally accepts quantum mechanics and therfore his photon of the entangled pair is measured via a projective measurement as shown in equation 1.7.

Bibliography

[1] Werner Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik and Mechanik. *Zeitschrift für Physik*, 43:172–198, 1927.

[2] Stephen Barnett. *Quantum Information (Oxford Master Series in Physics: Atomic, Optical, and Laser Physics)*. Oxford University Press, USA, 2009.

[3] Leslie Ballentine. *Quantum Mechanics: A Modern Development*. World Scientific Publishing Company, 1998.

[4] Jürgen Audretsch. *Verschränkte Systeme*. Wiley, 2005.

[5] Daniel Greenberger, Klaus Hentschel, and Friedel Weinert. *Compendium of Quantum Physics: Concepts, Experiments, History and Philosophy*. Springer, 2009.

[6] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[7] Wolfgang Tittel and Gregor Weihs. Photonic entanglement for fundamental tests and quantum communication. *Quantum Information & Computation*, 1(2):3–56, 2001.

[8] Anthony Gerrard and James Burch. *Introduction to Matrix Methods in Optics*. Dover Publications, 2012.

[9] Josef Jauch. *Foundations of Quantum Mechanics*. Addison-Wesley, 1968.

[10] Asher Peres. *Quantum Theory: Concepts and Methods (Fundamental Theories of Physics)*. Springer, 1995.

[11] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.

[12] Niels Bohr. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 48(8):696–702, 1935.

[13] Andrew Whitaker. *Einstein, Bohr and the Quantum Dilemma: From Quantum Theory to Quantum Information*. Cambridge University Press, 2006.

[14] Erwin Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Die Naturwissenschaften*, 23(48,49):807–844, 1935.

[15] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4):555–563, 1935.

[16] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32(3):446–452, 1936.

[17] David Bohm. *Quantum Theory*. Prentice-Hall, 1951.

[18] David Bohm and Yakir Aharonov. Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Physical Review*, 108(4):1070–1076, 1957.

[19] John Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[20] John Clauser, Michael Horne, Abner Shimony, and Richard Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[21] Boris Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[22] Stuart Freedman and John Clauser. Experimental test of local hidden-variable theories. *Letters in Mathematical Physics*, 28(14):938–941, 1972.

[23] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters*, 81(23):5039–5043, 1998.

[24] Thomas Scheidl, Rupert Ursin, Johannes Kofler, Sven Ramelow, Xiao-Song Ma, Thomas Herbst, Lothar Ratschbacher, Alessandro Fedrizzi, Nathan Langford, Thomas Jennewein, and Anton Zeilinger. Violation of local realism with freedom of choice. *PNAS*, 107(46):19708–19713, 2010.

[25] Mary Rowe, Dave Kielpinski, Volker Meyer, Charles Sackett, Wayne Itano, Christopher Monroe, and David Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409:791–794, 2001.

[26] Alain Aspect, Jean Dalibard, and Gerard Roger. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Physical Review Letters*, 49(25):1804–1807, 1982.

[27] Bernhard Wittmann, Sven Ramelow, Fabian Steinlechner, Nathan Langford, Nicolas Brunner, Howard Wiseman, Rupert Ursin, and Anton Zeilinger. Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering. *New Journal of Physics*, 14, 2012.

[28] John Bell. *Speakable and Unspeakable in Quantum Mechanics (Collected Papers on Quantum Philosophy), 2nd Edition*. Cambridge University Press, 2004.

[29] Thomas Scheidl. *A fundamental test and an application of quantum entanglement*. PhD thesis, University of Vienna, 2009.

[30] Albert Einstein and Paul Schlipp. *Albert Einstein, philosopher-scientist*. Library of Living Philosophers, 1949.

[31] Anupam Garg and David Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Physical Review D*, 35(12):38313835, 1987.

[32] Philippe Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Physical Review A*, 47(2):R747R750, 1993.

[33] Howard Wiseman, Steve Jones, and Andrew Doherty. Steering, entanglement, nonlocality, and the EPR paradox. *Physical Review Letters*, 98(14):140402–140405, 2007.

[34] John Hammersley and David Handscomb. *Monte Carlo methods*. Chapman and Hall, 1964.

[35] Peter Hellekalek. Good random number generators are (not so) easy to find. *Mathematics and Computers in Simulation*, 46:485–505, 1998.

[36] Jürgen Eichenauer and Jürgen Lehn. A nonlinear congruential pseudorandom number generator. *Statistische Hefte*, 27(4):315–326, 1986.

[37] John Walker. HotBits: Genuine random numbers, generated by radioactive decay. http://www.fourmilab.ch/hotbits/, 1996.

[38] John Johnson. Thermal agitation of electricity in conductors. *Physical Review*, 32(1):97–109, 1928.

[39] Mario Stipcevic. Quantum random number generators and their use in cryptography. arXiv:1103.4381, 2011.

[40] Mario Stipcevic and Branka Rogina. Quantum random number generator based on photonic emission in semiconductors. *Review of Scientific Instruments*, 78, 2007.

[41] Hai-Quiang Ma, Su-Mei Wang, Da Zhang, Jun-Tao Chang, Ling-Ling Ji, Yan-Xue Hou, and Ling-An Wu. A random number generator based on quantum entangled photon pairs. *Chinese Physics Letters*, 21(10):1961–1964, 2004.

[42] Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim. Quantum random number generator using photon-number path entanglement. *Applied Optics*, 48(9):1774–1778, 2009.

[43] James Dynes, Zhi-Liang Yuan, Andrew Sharpe, and Andrew Shields. A high speed, postprocessing free, quantum random number generator. *Applied Physics Letters*, 93(3), 2008.

[44] Wei Wei, Jianwei Zhang, Tian Liu, and Hong Guo. Quantum random number generator based on the photon number decision of weak laser pulses. arXiv:0811.0082,, 2008.

[45] Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo, and Li Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, 35(3):312–314, 2010.

[46] Stephan Krenn. Pseudozufallszahlengeneratoren und ihre Anwendung in der Kryptographie. Master's thesis, Vienna University of Technology, 2007.

[47] Juan Soto. Statistical testing of random number generators. http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf, 1999.

[48] Donald Knuth. *The Art of Computer Programming: Volume 2*. Addison-Wesley, 1969.

[49] Milton Abramowitz and Irene Stegun. *Handbook of mathematical functions: With formulas, graphs, and mathematical tables*. Dover Publications, 1972.

[50] Frank Olver, Daniel Lozier, Ronald Boisvert, and Charles Clark. *NIST handbook of mathematical functions*. Cambridge University Press, 2010.

[51] Robert Brown, Dirk Eddelbuettel, and David Bauer. Dieharder: A random number test suite. http://www.phy.duke.edu/ rgb/General/dieharder.php.

[52] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1681, 2000.

[53] William Risk, Timothy Gosnell, and Arto Nurmikko. *Compact blue-green lasers*. Cambridge Studies in Modern Optics, 2003.

[54] Peter Powers. *Fundamentals of nonlinear optics*. CRC Press, 2011.

[55] Alessandro Fedrizzi. *Fundamental experiments with a high brightness source of entangled photons*. PhD thesis, University of Vienna, 2008.

[56] Bahaa Saleh and Malvin Teich. *Grundlagen der Photonik*. Wiley-VCH, 2008.

[57] Amnon Yariv and Pochi Yeh. *Optical Waves in Crystals: Propagation and Control of Laser Radiation*. Wiley, 1984.

[58] Peter Seitz and Albert Theuwissen. *Single-photon imaging*. Springer, 2011.

[59] Fabian Steinlechner. Towards a loophole-free demonstration of EPR nonlocality. Master's thesis, Vienna University of Technology, 2010.

[60] Devin Smith, Geoff Gillet, Marcelo de Almeida, Cyril Branciard, Alessandro Fedrizzi, Till Weinhold, Adriana Lita, Brice Calkins, Thomas Gerrits, Howard Wiseman, Sae Woo Nam, and Andrew White. Conclusive quantum steering with superconducting transition edge sensors. *Nature Communications*, 3(625), 2012.

Acknowledgements

There are several people which I want to thank for supporting me during my whole time at the IQOQI, from explaining fundamental quantum optical phenomena in the beginning over discussing experimental problems until the process of writing this thesis.

First of all I want to thank my supervisor Prof. Anton Zeilinger, who made it possible to get access to such an inspiring research environment with smart students from all over the world and state of the art technologies. In addition, Prof. Zeilinger and Bernhard Wittmann were proofreading my thesis and therefore have a large share of this final version.

Not only for this I am very thankful to Bernhard Wittmann but also for taking me under his wings and introducing me into the interessting field of quantum optics.

A special thanks of course goes to the coworkers of my group and closely related other sub groups: Alexandra Mech, Thomas Herbst, Marissa Giustina, Sven Ramelow, Rupert Ursin and many more for stimulating discussions even aside from physics.

I am greatly indebted to the whole Zeilinger office team, Daniela Charlesworth, Verena Bock and Manuela Csapo, as well as to Martin Aspöck for doing a great job and making it possible to finish my thesis on time.

Thanks to Morgan Russell and his cat Albert (partly named after the well-known physicist) for correcting my bad English.

Last but not least, I want to thank my family and friends for supporting me throughout my whole studies.