rijksuniversiteit groningen

faculteit wiskunde en natuurwetenschappen

Rijksuniversiteit Groningen

Bachelor Thesis Physics

Quantum Entanglement, Bell's Inequalities and Quantum Cryptography

Author:
Bart Hake

Supervisor:
Prof. R.G.E. Timmermans

Second corrector:
Prof. R.A. Hoekstra

July 4, 2014

Abstract

This bachelor thesis contains an answer to a paradox in quantum mechanics. The quantum phenomenon of entanglement will be discussed. Based on Bell's inequalities, it is shown how was dealt with this phenomenon and what answer to the paradox imposed by it was given. Experiments substantiating this theory will be examined in Section 4. Based on the experiments of Aspect and his companions, local-hidden variables, as imposed by the paradox, are shown to be incompatible with experimental data. In Section 5 and 6, others versions and generalizations of Bell's original inequality will be given. These provide us with the same conclusion as drawn from the original one. In Section 7, a useful application of quantum entanglement will be discussed. It is shown that based on quantum mechanical laws and Bell's inequalities, cryptographic processes can be safe from potential thiefs.

Contents

1 Introduction

While learning about quantum mechanics, one is taught that nature has some strange properties. These properties can be counterintuitive. Moreover, according to Richard Feynman: "If you think you understand quantum mechanics, you don't understand quantum mechanics." I myself have always wondered if there was more to quantum mechanics than we know. Perhaps there could be a underlying theory, which is more intuitive and predictive than quantum theory. In other words, I have always wondered mysels if quantum mechanics is complete.

For my bachelor thesis, I wanted to combine quantum-mechanical theory with actual observations that would show the theory to be correct and complete. In the end, such a combination left me with the subject of Bell's inequalities. This inequalities are part of a theory that answered a paradox within quantum mechanics. This paradox was introduced in a paper of Einstein, Rosen and Podolsky and therefore called the EPR paradox. In this paper, the completeness of quantum mechanics was questioned and it was concluded that quantum theory is indeed incomplete. Should this be the case, extra variables are needed to make quantum mechanics complete. Bell introduced a theoretical basis, showing the paradox to fail. The correctness of this theory was shown on the basis of experiments. Within the whole discussion of the paradox, one quantum-mechanical phenomenon plays a central role: "*'entanglement*". The questions to be answered in this thesis are: "What is the EPR paradox?", "How was it resolved?" and "What is entanglement and what consequences does this phenomenon have?". Furthermore, generalizations of Bell's original inequality will be given and lastly a useful application of entanglement will be given.

The most important concept with which will be dealt here is that of entanglement. Therefore, it is useful to first introduce it. After that, it is described how entanglement was discovered and how it was dealt with.

2 Entanglement

The idea of entanglement will be discussed by considering two spin-1/2 particles, originated from a system with total angular momentum equal to zero. When measuring the z-component of particle 1, we can get $\pm\hbar/2$. The total wavefunction of the system wil be the singlet state

$$\Psi = \frac{1}{\sqrt{2}}(|+\rangle_1|-\rangle_2 - |-\rangle_1|+\rangle_2), \tag{2.1}$$

where $|+\rangle_1$ denotes that when measuring the z-component of particle 1, you will get $+\hbar/2$ etc. The wave function implies that when you measure the z-component of partcile 1 and you get $+\hbar/2$, the wavefunction "collapses" to $|+\rangle_1|-\rangle_2$ from which we know that partcile 2 must have a spin in the z-direction of $-\hbar/2$ due to conservation of angular momentum. So far, this is nothing mysterious. However, things begin to get interesting when you make two measurements. Say that you first measure the z-component of particle 1 and get that it is $+\hbar/2$. From this you know also the z-component of particle 2: $-\hbar/2$. Secondly, you measure the x-component of particle 1 to be $+\hbar/2$, from which you then know that the x-component of particle 2 is $-\hbar/2$. For particle 1, this does not give any problems. From quantum mechanics it is known that you cannot know both the z-component and the x-component with certainty. The second measurement of particle 1 just makes its z-component uncertain. But what about particle 2? From the first measurement you knew its z-component and from the second one its x-component. But does the same uncertainty principle holding for particle 1 also hold for particle 2? Does measuring the x-component of particle 1 make the z-component of particle 2 uncertain, even when the two particles are at such a distance from one another that no instant interactions between them can take place? According to the theory of special relativity, information cannot propagate faster than the speed of light. But the above suggests that measuring both the x- and z-component of particle 1 ensures that you will instantaneously know both components of particle 2. In other words, both particles are connected in a definite way. This phenomenon is called "*entanglement*", the results of measurements on two different particles are dependent. The principle of entanglement gave rise to a discussion that started in 1935 and has brought up discussions about quantum theory that are still contributing to the way we think about it today.

3 Questioning quantum mechanics

In this section, an overview will be given of how and when quantum entanglement was discovered and how it questioned the completeness of quantum mechanics. Furthermore, it is discussed how this "problem" was resolved and how it gave rise to experiments veryfying quantum mechanics.

3.1 The EPR paradox

In 1935, Einstein, Podolsky, and Rosen wrote an article [17], stating that quantum mechanics was not complete. They make use of a few logical conditions on which their argument is based. These will here be quoted. A theory is complete if: *"Every element of the physical reality must have a counterpart in the physical theory"*. The second condition is known as the reality condition: *"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"*. Their third condition is the locality criterion. This means that when two systems do not interact, no real change can take place on the second system when there are measurements being done on the first and vice versa. Their last condition is that of a perfect correlation. This condition is used in the kind of "Gedankenexperiment" they are considering where two particles are created from one particle. This condition means that if a quantity, for example the spin, of one particle is measured, then with certainty the outcome of measuring that same quantity on the other particle becomes the opposite. The main argument goes as follows. What they did was to begin with the fundamental concept of the quantum theory, that of a state which would completely describe the behavior of a particle by means of a wave function, and show that this would lead to a contradiction. When working in quantum theory and knowing that two operators of two physical quantities do not commute, you know that you cannot know each of these quantities with certainty when trying to determine one of them experimentally. They state that from this you can draw the conclusion that either

1. the quantum theory describing the physical reality does not obey the criterion of completeness(is not complete), or

2. two operators of two different physical quantities that do not commute cannot have the same reality.

For the condition of completeness states that if both physical quantities had a simultaneous reality, they would both be part of the complete theory. However, because of the commutation relations, there is an element of physical reality which is not accounted for by the quantum mechanical theory. Starting from the assumption that the wave function does give a complete description of physical reality, they show that two non-commuting operators belonging to two physical quantities can have the same reality. They do this by means of an example where these two quantities are position and momentum, which we know from Heisenberg's uncertainty principle, do not commute. In section 2 we have seen the example of measuring the spin of two particles in two different directions. The measurements of the spin of particle 1 in both the z- and x-direction would, according to the criterion of reality, give two precisely determined elements of reality corresponding to the simultaneous definition of both spin components. Whatever the example may be, it is clear that indeed two non-commuting operators can have simultaneous reality. Following up on their previous exclusive conslusions, this leads them to the conclusion that the quantum-mechanical description of reality given by wave functions is not complete. It is important to mention that they do not say that the quantum-mechanical theory is incorrect, they merely say that it is not complete and they do believe that a complete theory exists.

3.2 Bohm's contribution

In 1951 David Bohm made an important contribution [12] to the EPR paradox. Actually, the approach to entanglement given in Section 2, using spin-1/2 particles was introduced by Bohm. In most work discussing the EPR paradox after this, the spin-1/2 approach was mostly used. In het original paper of EPR, position and mmentum were used. Certain questions may rise when reading the article of EPR. One of those is that perhaps the paradox could be avoided by assuming that the known quantum theory breaks down when the particles that are being measured are beyond a certain distance from each other. In an article made by D. Bohm along with Y. Aharonov [13] it was shown this breakdown is not supported by their data. They tested if such a breakdown could occur by using polarization of correlated photons, which at that time was the most practical to do. These photons where created due to the annihilation of an electron and positron pair. Indeed, they showed that such a breakdown would not occur. The most important contribution they made in their article was, in light of this thesis, to show that not only the spin properties of pairs of particles, but also the polarization properties of photons may be used to test the EPR paradox. As we will see, most experiments that were done to test the validity of the EPR theorem made use of entanglement of photons.

3.3 Bell's contribution

So far, the paradox has been treated quite philosophical. The experiments treated in the concerning articles have been "Gedankenexperiments", but no one so far has been able to develop a theory that would be able to verify if quantum mechanics is indeed incomplete. But this is where John S. Bell came in. He wrote a famous article that gave the theoretical basis that would give rise to experiments verifying quantum mechanics. The basis for this article was that of so-called "local-hidden variables", predicted by EPR, that would make the quantum theory complete.

3.3.1 Bell's theorem

Bell's theorem consists of a proof that shows that the predictions of quantum mechanics differ from the predictions made by a local-hidden variable theory. A local-hidden variable theorem was based on the principle of local realism. Local realism combines the principle of locality with the "realistic" assumption that a physical quantity must have a predestined value. This predestined value would then be determined by the local-hidden variables. The contradiction shown by Bell will be named the so-called "Bell's inequality", firstly introduced in his most famous article [5]. Let us first give a proof of the original inequality as given in the article. Start with two spin-1/2 particles, in a singlet state, moving in opposite directions. Using Stern-Gerlach magnets, one can measure the spin components along a certain direction. Say that we measure the spin of the first particle along a direction $\vec{\mathbf{a}}$ and the spin of the second particle along a direction $\vec{\mathbf{b}}$. Call the outcome of the measurement of $\vec{\mathbf{s}}_1 \cdot \vec{\mathbf{a}}$ A and the outcome of the measurement of $\vec{\mathbf{s}}_2 \cdot \vec{\mathbf{a}}$ B. Then in terms of the units $\hbar/2$ both A and B can be either $+1$ or -1. The next thing to do is to split up the proof and see what we get for the expectation value of the product between the spins of the two particles from both the perspective of a local-realistic theory and quantum mechanics. Let us first consider what quantum mechanics has to say about it. The expectation value of the product of spin components according to quantum mechanics is

$$E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) = \langle(\vec{\mathbf{s}}_1 \cdot \vec{\mathbf{a}})(\vec{\mathbf{s}}_2 \cdot \vec{\mathbf{b}})\rangle_{\mathrm{QM}} = -\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}, \tag{3.1}$$

as is shown in the Appendix. Note that in the EPR paradox perfect correlations are considered. This means that the measuring directions are either parallel or anti-parallel. Quantum mechanics thus predicts for these cases

$$E(\vec{\mathbf{a}}, \vec{\mathbf{a}}) = -E(\vec{\mathbf{a}}, -\vec{\mathbf{a}}) = -1. \tag{3.2}$$

We turn to the second part and see what we will get when, as EPR sugests, local-hidden variables are added to the system. These are denoted by λ, such that the outcomes of the measurements now also depend on those

$$A = A(\lambda, \vec{\mathbf{a}}) = \pm 1, \tag{3.3}$$

and

$$B = B(\lambda, \vec{\mathbf{b}}) = \pm 1. \tag{3.4}$$

Let $\rho(\lambda)$ denote the probability distribution of λ , then we know that because of normalization $\int \rho(\lambda) \mathrm{d}\lambda{=}1$. The fact that both measurements only depend on one orientation and not on the other one, shows that we are here talking about local-hidden variables. It was these type of unknown parameters EPR suggested. The expectation value of the product of the same spin components as before is

$$E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) = \langle \vec{\mathbf{s}}_1 \cdot \vec{\mathbf{a}}\, \vec{\mathbf{s}}_2 \cdot \vec{\mathbf{b}}\rangle = \int \mathrm{d}\lambda \rho(\lambda) A(\lambda, \vec{\mathbf{a}}) B(\lambda, \vec{\mathbf{b}}). \tag{3.5}$$

We know from Eq.(3.3) and Eq.(3.4) that this equation can be at most $+1$ and at least -1. If it is -1 at $\vec{\mathbf{a}} = \vec{\mathbf{b}}$, then $A(\lambda, \vec{\mathbf{a}}) = -B(\lambda, \vec{\mathbf{a}})$ such that

$$E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) = -\int \mathrm{d}\lambda \rho(\lambda) A(\lambda, \vec{\mathbf{a}}) A(\lambda, \vec{\mathbf{b}}). \tag{3.6}$$

Now suppose that $\vec{\mathbf{c}}$ is another direction in which the spin can be measured. Then

$$\begin{aligned} E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) - E(\vec{\mathbf{a}}, \vec{\mathbf{c}}) &= -\int \mathrm{d}\lambda \rho(\lambda)[A(\lambda, \vec{\mathbf{a}}) A(\lambda, \vec{\mathbf{b}}) - A(\lambda, \vec{\mathbf{a}}) A(\lambda, \vec{\mathbf{c}})] \\ &= -\int \mathrm{d}\lambda \rho(\lambda) A(\lambda, \vec{\mathbf{a}}) A(\lambda, \vec{\mathbf{b}})[1 - A(\lambda, \vec{\mathbf{b}}) A(\lambda, \vec{\mathbf{c}})]. \end{aligned} \tag{3.7}$$

Using that the absolute value of an integral is at most the integral of the absolute value and using Eq.(3.3) and Eq.(3.4), we get

$$|E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) - E(\vec{\mathbf{a}}, \vec{\mathbf{c}})| \leq \int \mathrm{d}\lambda \rho(\lambda)[1 - A(\lambda, \vec{\mathbf{b}}) A(\lambda, \vec{\mathbf{c}})]. \tag{3.8}$$

The second part on the right of this equation can be identified as $E(\vec{\mathbf{b}}, \vec{\mathbf{c}})$, such that

$$\boxed{|1 + E(\vec{\mathbf{b}}, \vec{\mathbf{c}})| \geq |E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) - E(\vec{\mathbf{a}}, \vec{\mathbf{c}})|}. \tag{3.9}$$

Eq.(3.9) is known as the original Bell's inequality. It is a very important inequality, because in certain cases quantum mechanics predicts somethings else than a local-hidden variable theory. To see this, take the special case where

$$\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} = 0 \ , \ \vec{\mathbf{c}} = \frac{\vec{\mathbf{a}} + \vec{\mathbf{b}}}{\sqrt{2}}. \tag{3.10}$$

Then from Eq.(3.1), we see that

$$E(\vec{\mathbf{a}}, \vec{\mathbf{b}}) = 0 \ , \ E(\vec{\mathbf{a}}, \vec{\mathbf{c}}) = E(\vec{\mathbf{b}}, \vec{\mathbf{c}}) = -\frac{1}{\sqrt{2}}. \tag{3.11}$$

Plugging this in Eq.(3.9), we then get a contradiction

$$|1 - \frac{1}{\sqrt{2}}| \ngeq \frac{1}{\sqrt{2}}. \tag{3.12}$$

Note that Eq.(3.9) holds for a local-hidden variable theory in general. We have not specified λ any further. If we could use experiments that have a similar set-up as the above and compare the results with the predictions made either by quantum mechanics or a local-hidden variable theory, we could exclude either one of them. In other words, Bell's inequality left us with a basis to test wether quantum mechanic theory was complete or not in the way of EPR. Indeed, these experiments have been done. This will be part of the next section.

3.3.2 Experimental proof of Bell's theorem

The official Bell's inequality was very important for experiments proving the completeness of quantum mechanics. However, this inequality wans not used in experiments, because there were some practical problems with it. The inequality very much depends on perfect correlations between the measurements A and B. Measurement equipment in reality is not 100 percent efficient and so perfect correlations as those implicated by Eq.(3.3) and Eq.(3.4) are unlikely to be found in reality. The first correction to these problems was made by Clauser, Horne, Shimony and Holt [15]. These will from now on be referred to as CHSH.

The proposed experiment by CHSH

As I mentioned, CHSH gave an alternative form of Bell's inequality that would be applicable to realizable experiments. However, the proof that follows will be following the proof as given by Bell in 1971 [6]. The already mentioned dependence on Eq.(3.3) and Eq.(3.4) may cause another problem. That is, in the ideal situation, whenever a particle is detected at one detector, an associated particle is always detected at the other detector. But in reality, this may not always be the case. An answer to this problem was given by Bell. He assumed that A and B could now be one of the three values: 0 (if no particle is measured), -1, or $+1$. Instead of

$$A = \pm 1 \ , \ B = \pm 1, \tag{3.13}$$

we now get

$$A \leq 1 \ , \ B \leq 1. \tag{3.14}$$

If $\vec{\mathbf{a}}'$ and $\vec{\mathbf{b}}'$ are two more directions along which spin can be measured, we have in a similar way as before

$$\begin{aligned} E(\vec{\mathbf{a}},\vec{\mathbf{b}}) - E(\vec{\mathbf{a}},\vec{\mathbf{b}}') = &-\int \mathrm{d}\lambda\rho(\lambda)[A(\lambda,\vec{\mathbf{a}})A(\lambda,\vec{\mathbf{b}}) - A(\lambda,\vec{\mathbf{a}})A(\lambda,\vec{\mathbf{b}}')] \\ =&\int \mathrm{d}\lambda\rho(\lambda)A(\lambda,\vec{\mathbf{a}})A(\lambda,\vec{\mathbf{b}})[1 \pm A(\lambda,\vec{\mathbf{a}}')A(\lambda,\vec{\mathbf{b}}')] \\ &-\int \mathrm{d}\lambda\rho(\lambda)A(\lambda,\vec{\mathbf{a}})A(\lambda,\vec{\mathbf{b}}')[1 \pm A(\lambda,\vec{\mathbf{a}}')A(\lambda,\vec{\mathbf{b}})]. \end{aligned} \tag{3.15}$$

Using Eq.(3.14) we get

$$\begin{aligned} |E(\vec{\mathbf{a}},\vec{\mathbf{b}}) - E(\vec{\mathbf{a}},\vec{\mathbf{b}}')| \leq &\int \mathrm{d}\lambda\rho(\lambda)[1 \pm A(\lambda,\vec{\mathbf{a}}')A(\lambda,\vec{\mathbf{b}}')] \\ &+\int \mathrm{d}\lambda\rho(\lambda)[1 \pm A(\lambda,\vec{\mathbf{a}}')A(\lambda,\vec{\mathbf{b}})]. \end{aligned} \tag{3.16}$$

Which is equialent to

$$|E(\vec{\mathbf{a}},\vec{\mathbf{b}}) - E(\vec{\mathbf{a}},\vec{\mathbf{b}}')| \leq 2 \pm (E(\vec{\mathbf{a}}',\vec{\mathbf{b}}') + E(\vec{\mathbf{a}}',\vec{\mathbf{b}})). \tag{3.17}$$

This can be written as

$$-2 \leq S(\lambda,\vec{\mathbf{a}},\vec{\mathbf{a}}',\vec{\mathbf{b}},\vec{\mathbf{b}}') \leq 2, \tag{3.18}$$

where

$$S(\lambda,\vec{\mathbf{a}},\vec{\mathbf{a}}',\vec{\mathbf{b}},\vec{\mathbf{b}}') = E(\vec{\mathbf{a}},\vec{\mathbf{b}}) - E(\vec{\mathbf{a}},\vec{\mathbf{b}}') + E(\vec{\mathbf{a}}',\vec{\mathbf{b}}) + E(\vec{\mathbf{a}}',\vec{\mathbf{b}}'). \tag{3.19}$$

Eq.(3.18) is known as the CHSH inequality or BCHSH inequality. Based on a very similar inequality, Clauser *et* al. [15] made an experimental proposal. In this proposal, the efficiency of polarizers used in the experiment were introduced. The experiment involved polarization correlation of photons that were emitted in a cascade decay in calcium. Following on this, Aspect *et* al. [2] did measure this correlations as will be discussed next.

4 The experiments of Aspect

In this section, some of the most famous experiments that were actually done to test Bell's inequalities will be discussed. The most well-known class of experiments are those done by Alain Aspect and his collaborators. Here, three of their experiments will be discussed.

4.1 The first experiment

During the first experiment of Aspect, together with Grangier and Roger [2], measured the linear polarization correlation of the photons emitted in a radiative atomic cascade of calcium. Their results agreed with the predictions of quantum mechanics and violated the Bell's inequality. In the experiment, two photons are moving in apposite direction. A measurement of their polarization along a direction $\vec{\mathbf{a}}$ yields +1 if the polarization is found parallel to $\vec{\mathbf{a}}$ and -1 if found perpendicular to it. Here, the same notation will be used as is done in the paper

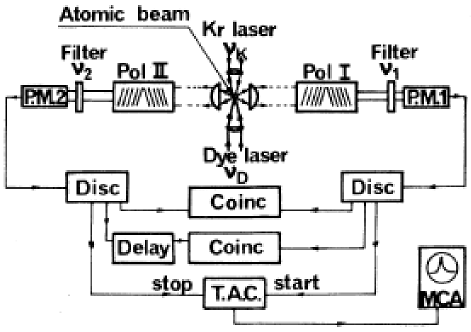

Figure 1: Schematic diagram of the first experiment [2]

.

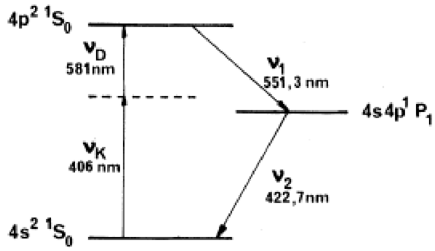

Figure 2: Relevant levels of calcium [2]

itself. By writing $P_{\pm\pm}(\vec{\mathbf{a}},\vec{\mathbf{b}})$, we denote the probabilities that you get the result ± 1 along $\vec{\mathbf{a}}$ (for particle 1) and ± 1 along $\vec{\mathbf{b}}$. The following quantity denotes the correlation coefficient of the measurement of the two particles

$$E(\vec{\mathbf{a}},\vec{\mathbf{b}}) = P_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + P_{--}(\vec{\mathbf{a}},\vec{\mathbf{b}}) - P_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}) - P_{-+}(\vec{\mathbf{a}},\vec{\mathbf{b}}). \tag{4.1}$$

In the experiment the $4p^{21}S_0$-$4s4p^1P_1$-$4s^{21}S_0$ cascade of calcium is used, as shown in Figure 2. The cascade produces two photons, ν_1 and ν_2. An atomic beam of calcium is irradiated at 90° by two laser beams which are polarized parallel to each other. The first one is a krypton ion laser with wavelength λ_K. The second one is a Rhodamine laser with wavelength λ_D. The calcium atoms

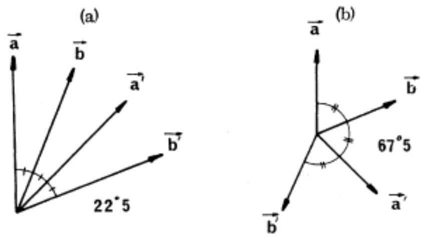

Figure 3: Orientation leading to a maximum violation of the inequalities [2]

are being pumped to their upper level by absorption of ν_K and ν_D and then, when falling back to lower levels, emit two photons: ν_1(551.3 nm) and ν_2(422.7 nm). The first one coming when the atom falls from a J=0 state and even parity to a short-lived intermediate J=1 state and odd parity. The second one coming from the intermediate state to another J=0 state with even parity.

The fluorescent light coming from this is then collected by lenses. Colored-glass filters at 551.3 nm and 422.7 nm then only let through one of the two emitted photons. Two polarizers were used, named I and II in Figure 1. These were so-called single-channel analyzers, which transmitted only one polarization and blocked the one orthogonal to it. These are set up in such a way that the angle of incidence of the fluorescent light is more or less equal to the Brewster's angle, such that there is no reflection. The transmittances of the polarizers were measured, both for light polarized parallel or perpendicular to the polarizer axis. Photomultipliers are used to feed the electronics that count the number of coincidences. These were made up of a time-to-amplitude converter and a multichannel analyzer. In this way, one gets a spectrum of the number of detected particles versus the delay between the detections of the two photons. Getting rid of background measurements due to accidental photons, one then gets a peak in the spectrum. The area enclosed by peak equals the coincidence signal. In terms of the four coincidene rates, $R_{\pm\pm}(\vec{\mathbf{a}},\vec{\mathbf{b}})$, Eq.(4.1) becomes

$$E(\vec{\mathbf{a}},\vec{\mathbf{b}}) = \frac{R_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{--}(\vec{\mathbf{a}},\vec{\mathbf{b}}) - R_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}) - R_{-+}(\vec{\mathbf{a}},\vec{\mathbf{b}})}{R_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{--}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{-+}(\vec{\mathbf{a}},\vec{\mathbf{b}})}. \tag{4.2}$$

Based on the paper of Clauser *et* al. [15] quantum mechanics predicts a relation between the rate of coincidences with polarizer I and II in certain orientations, their relative polarizer orientations and their transmittances. Several difficulties arose here [16]. When a pair was emitted and no count was obtained, one was not sure wether this was the result of the low-efficiency or that it was blocked by the polarizer. As a result of using single-channel analyzers and problems such as depicted above, only coincidence rates such as $R_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}})$ could be measured and rates like $R_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}})$ or $R_{--}(\vec{\mathbf{a}},\vec{\mathbf{b}})$ could not. Indirect measurements had to be made to actually test Bell's inequality. One can write relations between the measured coincidence rates and coincidence rates not being measured [11]

$$\begin{aligned} R_{++}(\infty,\infty) = R_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{-+}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{--}(\vec{\mathbf{a}},\vec{\mathbf{b}}) \\ R_{++}(\vec{\mathbf{a}},\infty) = R_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}) \\ R_{++}(\infty,\vec{\mathbf{b}}) = R_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) + R_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}), \end{aligned} \tag{4.3}$$

where ∞ denotes the orientation in which the polarizer is removed. By direct substitution into Eq.(3.18) and Eq.(4.2) one gets new CHSH-inequalities

$$-1 \leq S' \leq 0, \tag{4.4}$$

where

$$S' = \frac{R(\vec{\mathbf{a}},\vec{\mathbf{b}}) - R(\vec{\mathbf{a}},\vec{\mathbf{b}'}) + R(\vec{\mathbf{a}'},\vec{\mathbf{b}}) + R(\vec{\mathbf{a}'},\vec{\mathbf{b}'}) - R(\vec{\mathbf{a}'},\infty) - R(\infty,\vec{\mathbf{b}})}{R(\infty,\infty)}, \tag{4.5}$$

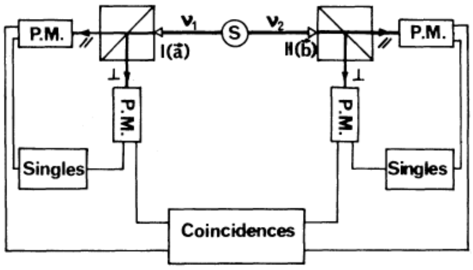

Figure 4: Schematic diagram of the second experiment [3].

where we have used an implicit ++ subscript notation, because we have exspressed S' only in terms of the measured coincidence rates R_{++}. There are, however, assumptions made before getting this new inequality. Because of the low detection efficiencies, the probabilities that arise in Eq.(4.1) must be redefined in such a way that we also take into account measurements when the polarizers are removed. This is only valid for certain assumptions, made by CHSH [15] and also by Clauser and Horne [14]. The whole of problems such as detection efficiency of measurement devices are known as the *efficiency loophole*. CHSH were the first to account for this to arrive at a quantum-mechanical value for S'. The assumption they made for example, was that whenever a pair of photons of photons would emerge from the polarizers, the probability of their joint detection would be independent of their polarizations. For the exact quantum-mechanical predictions and their derivation, one can for example look at an article by E. Fry *et* al. [19]. Making use of this along with the orientation of polarizers as shown in Figure 3, we get the following experimental and quantum-mechanical predictions

$$S'_{\mathrm{Exp}} = 0.126 \pm 0.014, \tag{4.6}$$

which violates Eq.(4.4) by 9 standarddeviations, while it is in agreement with the quantum mechanical prediction

$$S'_{\mathrm{QM}} = 0.118 \pm 0.005. \tag{4.7}$$

The error in the quantum mechanical prediction is caused by the uncertainty in the measurements of the polarizer efficiencies.

4.2 The second experiment

In the same year Aspect did his first experiment in which he measured the linear-polarization correlation described above, he did a second experiment [3]. This time, the experiment used two-channel polarizers, which are analogues of Stern-Gerlach filters. As mentioned, in the first experiment there were some difficulties that were overcome using certain assumptions. In this experiment it is now possible to avoid indirect measurements such as those that were done in the first one.

In regard to the first experiment, the polarizers are now replaced by two-channel polarizers that separate two orthogonal linear polarizers. These are then followed by two photomultipliers. It is now possible to measure all four

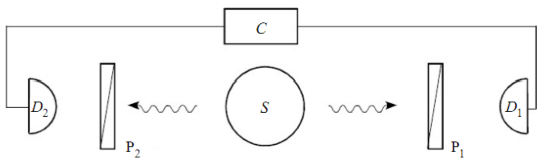

Figure 5: Schematic diagram of the experiment proposed by Bohm [27].

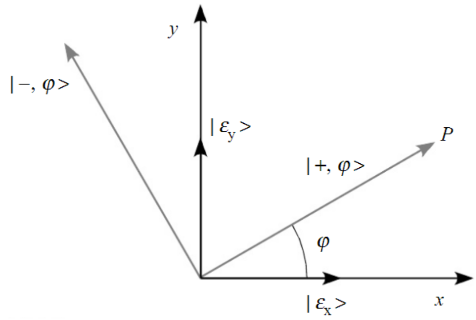

Figure 6: Rotation of the linear polarization basis [27].

coincidence rates $R_{\pm\pm}(\vec{\mathbf{a}}, \vec{\mathbf{b}})$ such that now Eq.(4.2) can be directly used along with Eq.(3.18) to test Bell's inequality. It is sufficient to measure a set of orientations. The same source was used as in the first experiment. Both polarizers transmit light polarized in the incidence plane while it reflects light polarized orthogonal to it. We can make a quantum mechanical prediction for S. This will be done following the procedure used in [27]. The same notation as in this book will be used to avoid confusion with previous notations. This confusion might arise due to the fact that previously the discussion was based on spin-1/2 particles, but now the discussion will be based on Bohm's version of photon polarization as mentioned before. The experimental setup is similar to the one used by Aspect, it is also based on photons arising from a J=0 $\longrightarrow$ J=1 $\longrightarrow$ J=0 cascade.

In this setup as shown in Figure 5, S is the source that emits the photons, P_1 and P_2 are polarizers and D_1 and D_2 are photon detectors. C is a coincident counter. Photons entangled by polarization can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\epsilon_{1x}\rangle|\epsilon_{2x}\rangle + |\epsilon_{1y}\rangle|\epsilon_{2y}\rangle), \tag{4.8}$$

where a linear polarization basis is used. The notation $|\epsilon_{ix}\rangle$ and $|\epsilon_{iy}\rangle$ means that photon i (i=1,2) is polarized along the x- or y-axis respectively. Say ϕ_1 and ϕ_2 are the angles of the polarizers P_1 and P_2 ,respectively, made with the x-axis. Then we can also write the entangled state as a combination of polarization states $|+, \phi_i\rangle$ (i=1,2) and $|-, \phi_i\rangle$. Here, + means that the direction of the polarizer is parallel to the angle made with the x-axis, and − means it is orthogonal to it.

We can use Figure 6 to get

$$|+,\phi_1\rangle = \cos\phi_1|\epsilon_{1x}\rangle + \sin\phi_1|\epsilon_{1y}\rangle \tag{4.9}$$
$$|-,\phi_1\rangle = -\sin\phi_1|\epsilon_{1x}\rangle + \cos\phi_1|\epsilon_{1y}\rangle. \tag{4.10}$$

We can invert these to get

$$|\epsilon_{1x}\rangle = \cos\phi_1|+,\phi_1\rangle - \sin\phi_1|-,\phi_1\rangle \tag{4.11}$$
$$|\epsilon_{1y}\rangle = \sin\phi_1|+,\phi_1\rangle + \cos\phi_1|-,\phi_1\rangle, \tag{4.12}$$

with similar equations for photon 2. Using this equations along with Eq.(4.8), one gets

$$\begin{aligned}|\psi\rangle = \frac{1}{\sqrt{2}}(|+,\phi_1;+,\phi_2\rangle\cos(\phi_2-\phi_1)+ \\ |-,\phi_1;-,\phi_2\rangle\cos(\phi_2-\phi_1) - |+,\phi_1;-,\phi_2\rangle\sin(\phi_2-\phi_1) \\ +|-,\phi_1;+,\phi_2\rangle\sin(\phi_2-\phi_1)).\end{aligned} \tag{4.13}$$

We can calculate the probability that both photons are polarized parallel to the directions of their polarizers

$$P_{++} = |\langle+,\phi_1;+,\phi_2|\psi\rangle|^2 = \frac{1}{2}\cos^2(\phi_2-\phi_1). \tag{4.14}$$

Similarly, one gets

$$P_{--} = \frac{1}{2}\cos^2(\phi_2-\phi_1) \tag{4.15}$$
$$P_{+-} = P_{-+} = \frac{1}{2}\sin^2(\phi_2-\phi_1). \tag{4.16}$$

Returning to the notation used in previous discussions of the experiments of Aspect, we see that

$$P_{++}(\vec{\mathbf{a}},\vec{\mathbf{b}}) = P_{--}(\vec{\mathbf{a}},\vec{\mathbf{b}}) = \frac{1}{2}\cos^2(\theta_{ab}) \tag{4.17}$$
$$P_{+-}(\vec{\mathbf{a}},\vec{\mathbf{b}}) = P_{-+}(\vec{\mathbf{a}},\vec{\mathbf{b}}) = \frac{1}{2}\sin^2(\theta_{ab}). \tag{4.18}$$

Eq.(4.1) now gives

$$E_{\mathrm{QM}}(\vec{\mathbf{a}},\vec{\mathbf{b}}) = \cos(2\theta_{ab}), \tag{4.19}$$

such that the quantum mechanical value for S becomes

$$S_{\mathrm{QM}} = \cos(2\theta_{ab}) - \cos(2\theta_{ab'}) + \cos(2\theta_{a'b}) + \cos(2\theta_{a'b'}). \tag{4.20}$$

This equation is maximal for the orientations used in the experiments: $\theta_{ab} = \theta_{a'b} = \theta_{a'b'} = 22.5°$ and $\theta_{ab'} = 67.5°$ such that

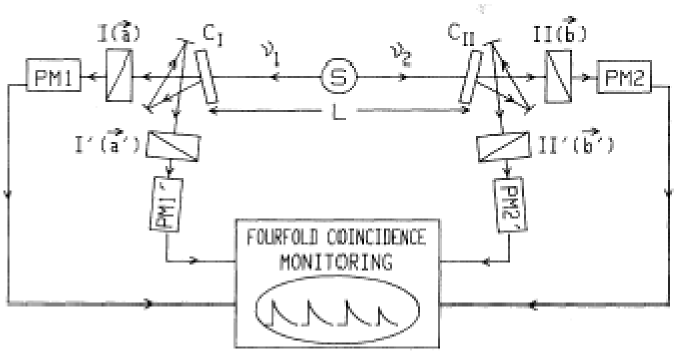

Figure 7: Schematic experimental set-up of the third experiment [4].

$$S_{\rm QM} = 2\sqrt{2}. \tag{4.21}$$

Because of the inefficiency of the used polarizers, the results that came out of the experiment were

$$S_{\rm Exp} = 2.697 \pm 0.015, \tag{4.22}$$

and

$$S_{\rm QM} = 2.70 \pm 0.05, \tag{4.23}$$

where the uncertainty in $S_{\rm QM}$ is caused by a slight lack of symmetry of the two channels of a polarizers. This again shows that experimental data is in agreement with quantum mechanics and in disagreement with Bell's inequality.

4.3 The third experiment

The third experiment of Aspect *et* al [4] is yet another variation of the previous experiments. In the same way as before two photons are created. The main difference between this experiment and the previous ones is that this one makes use of time-varying analyzers. Bell's locality condition in the case of these experiments is that the results of the measurement by the first polarize does not depend on the orientation of the other one. It is stated that such a conditon is reasonable, but it is not the consequence of any physical law. However, in the first two experiments the polarizers were held fixed. Bell pointed out that in such static experiments it is possible to reconcile local-hidden variable theories and predictions made by quantum mechanics. This would mean that the locality conditions of Bell would no longer be valid and thus would his inequality not hold. The problem with the locality condition is also known as the *locality loophole*. However, in a timing experiment, it is possible to make sure that a detection of one polarizer and a corresponding change of the orientation of the other one are spacelike separated. In this case, Bell's locality condition is a direct consequence of Einstein's causality principle. The schematic experimental set-up is shown in Figure 7.

In this case, each used before are replaced by a switching device(C_I and C_2) followed by two polarizers in two different orientations. These switches are able to fastly redirect the incident light from one polarizer to the other. Based on the fact that these systems can randomly switch without in any way being correlated, again similar CHSH-inequalities are derived

$$-1 \leq S \leq 0, \tag{4.24}$$

with

$$S = \frac{R(\vec{\mathbf{a}}, \vec{\mathbf{b}})}{R(\infty, \infty)} - \frac{R(\vec{\mathbf{a}}, \vec{\mathbf{b}'})}{R(\infty, \infty')} + \frac{R(\vec{\mathbf{a}'}, \vec{\mathbf{b}})}{R(\infty', \infty)} + \frac{R(\vec{\mathbf{a}'}, \vec{\mathbf{b}'})}{R(\infty', \infty')} \\ - \frac{R(\vec{\mathbf{a}'}, \infty)}{R(\infty', \infty)} - \frac{R(\infty, \vec{\mathbf{b}})}{R(\infty, \infty)}, \tag{4.25}$$

where the same notation is used as in Eq.(4.5). This experiment switched between the channels every 10 ns. This delay, as well as the lifetime of the intermediate J=1 level of calcium(5 ns), are both small compared to L/c(40 ns). L is the distance between the switching devices as shown in Figure 7. The result of this is that a detection on one side and a corresponding change in orientation on the other side are indeed spacelike sepated. Therefore, as mentioned before, Bell's locality condition is in this case a consequence of a physical law(causality). Again, the same orientation as in the earlier experiments is used, which results in

$$S_{\text{Exp}} = 0.101 \pm 0.020, \tag{4.26}$$

violating the CHSH inequality by 5 standard deviations, but in agreement with the quantum-mechanical prediction

$$S_{\text{QM}} = 0.112. \tag{4.27}$$

5 Another non-hidden variables theorem

In 1989, Greenberger, Zeilinger and Horne [24] showed another non-hidden variables theorem. Inspired by the work of Bell they deduced in a similar matter a theorem that quantum mechanics does not allow for any local-hidden variables. However, unlike Bell they did not make use of any inequalities to proof that. There article is called "Bell's theorem without inequalities" and their theorem will be marked as the GHZ theorem.

5.1 The GHZ theorem

The GHZ paper considers a special case in discussing Bell's theorem. They state that Bell's inequalities do not say anything about the special case of the EPR paper. This is the case where a measurement of a quantity on one paticle allows for you to know the same quantity for the other one with absolute certainty. They call this the "super-classical" case, which occurs when the measurement directions differ by 0° or 180°. They asked themselves the question wether it is

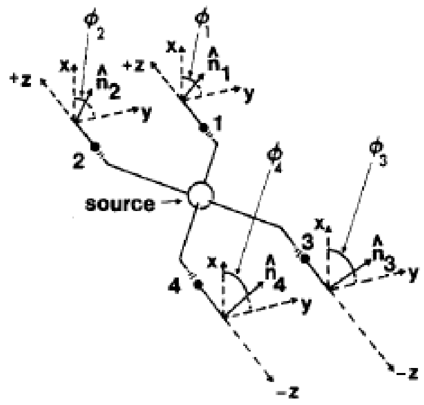

Figure 8: Gedankenexperiment with four particles [25].

possible to make a classical, local deterministic model, that is in accordance with quantum mechanics for such a case. To answer this question they considered the following case: begin with a particle of spin-1. This then decays into two particles, each of spin-1, one traveling in the $+z$-direction, the other in the $-z$-direction. Each of these then decays into two spin-1/2 particles. Based on this paper, Greenberger, Horne, Shimony and Zeilinger (GHSZ) made a second paper [25] which covers more than the GHZ paper and is in my opinion more clearifying in its manner treating this subject. Therefore, from now on, I will more closely follow their paper instead of the GHZ paper. The results are obviously the same. This Gedankenexperiment is shown in Figure 8.

There are four Stern-Gerlach analyzers, each of them measuring the spin of one of the particles along a direction $\hat{\mathbf{n}}_1, \hat{\mathbf{n}}_2, \hat{\mathbf{n}}_3$, and $\hat{\mathbf{n}}_4$ respectively. The spin state becomes

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle_1|+\rangle_2|-\rangle_3|-\rangle_4 - |-\rangle_1|-\rangle_2|+\rangle_3|+\rangle_4). \tag{5.1}$$

It can be shown that the expectation value of the product of the outcomes is

$$E^{\psi}(\hat{\mathbf{n}}_1, \hat{\mathbf{n}}_2, \hat{\mathbf{n}}_3, \hat{\mathbf{n}}_4) = -\cos(\phi_1 + \phi_2 + \phi_3 + \phi_4), \tag{5.2}$$

where ϕ_i with i=1,2,3,4 are the angles as shown in Figure 8. The proof of this equation will be given in the Appendix. This paper was interested in the "super-classical" case of perfect correlations

$$\begin{aligned} \text{If } \phi_1 + \phi_2 - \phi_3 - \phi_4 = 0 \\ \text{Then } E^{\psi}(\hat{\mathbf{n}}_1, \hat{\mathbf{n}}_2, \hat{\mathbf{n}}_3, \hat{\mathbf{n}}_4) = -1, \end{aligned} \tag{5.3}$$

and

$$\begin{aligned} \text{If } \phi_1 + \phi_2 - \phi_3 - \phi_4 = \pi \\ \text{Then } E^{\psi}(\hat{\mathbf{n}}_1, \hat{\mathbf{n}}_2, \hat{\mathbf{n}}_3, \hat{\mathbf{n}}_4) = +1. \end{aligned} \tag{5.4}$$

In analog with Bell's derivation, four outcomes are introduced beloning to measuring the spin of each particle: $A_\lambda(\phi_1), B_\lambda(\phi_2), C_\lambda(\phi_3), D_\lambda(\phi_4)$ which, like before, can take on the values ±1. Here, λ denotes again the local-hidden variables making the states complete. In terms of A,B,C and D, Eq.(5.3) and Eq.(5.4) now become

$$\begin{aligned} \text{If } \phi_1 + \phi_2 - \phi_3 - \phi_4 = 0 \\ \text{Then } A_\lambda(\phi_1)B_\lambda(\phi_2)C_\lambda(\phi_3)D_\lambda(\phi_4) = -1, \end{aligned} \tag{5.5}$$

and

$$\begin{aligned} \text{If } \phi_1 + \phi_2 - \phi_3 - \phi_4 = \pi \\ \text{Then } A_\lambda(\phi_1)B_\lambda(\phi_2)C_\lambda(\phi_3)D_\lambda(\phi_4) = +1. \end{aligned} \tag{5.6}$$

For a specific choice GHSZ then show that the four conditions imposed by EPR(See paragraph 2.1) lead to an inconsistency. Say we take

$$A_\lambda(0)B_\lambda(0)C_\lambda()D_\lambda(0) = -1 \tag{5.7a}$$
$$A_\lambda(\phi)B_\lambda(0)C_\lambda(\phi)D_\lambda(0) = -1 \tag{5.7b}$$
$$A_\lambda(\phi)B_\lambda(0)C_\lambda()D_\lambda(\phi) = -1 \tag{5.7c}$$
$$A_\lambda(2\phi)B_\lambda(0)C_\lambda()D_\lambda(\phi) = -1. \tag{5.7d}$$

From these equations, one can otain the following

$$A_\lambda(\phi)C_\lambda(\phi) = A_\lambda(0)C_\lambda(0), \tag{5.8}$$

and

$$A_\lambda(\phi)D_\lambda(\phi) = A_\lambda(0)D_\lambda(0), \tag{5.9}$$

such that

$$C_\lambda(\phi)/D_\lambda(\phi) = C_\lambda(0)/D_\lambda(0). \tag{5.10}$$

Remembering that A, B, C and D can only be ±1 we get

$$C_\lambda(\phi)D_\lambda(\phi) = C_\lambda(0)D_\lambda(0). \tag{5.11}$$

Combining this with the Eq.(A.23d) we get

$$A_\lambda(2\phi)B_\lambda(0)C_\lambda()D_\lambda(0) = -1, \tag{5.12}$$

which combines with the Eq.(A.23a) to

$$A_\lambda(2\phi) = A_\lambda(0) = \text{constant for all } \phi. \tag{5.13}$$

This is quite remarkable. According to EPR, if A denotes the result of measuring spin, then $A_\lambda(0)$ and $A_\lambda(\pi)$ would have opposite signs. When using Eq.(5.6)

instead of Eq.(5.5) like above, one gets the result

$$A_\lambda(\theta + \pi)B_\lambda(0)C_\lambda(0)D_\lambda(0) = +1, \tag{5.14}$$

which in combination with Eq.(A.23b) leads to

$$A_\lambda(\theta + \pi) = -A_\lambda(\theta). \tag{5.15}$$

This does have the correct sign based on the assumptions of the EPR paper. However, if one for example sets $\phi = \pi/2$ and $\theta = 0$, this contradicts Eq.(5.13).

This result thus shows the already mentioned inconsistency in the EPR conditions. Going back to the original paper of GHZ, this result led them to conclude that even in the super classical case it is not possible to form a classical, deterministic, local theory that is in accordance with quantum mechanical predictons. It is shown in the GHSZ paper that the above argument for four particles can be take one step back to three particles. This will also lead to a contradiction. For a pair of particles, the conditions made by EPR are consistent as shown in the EPR paper itself. Therefore it made them conclude that for systems of three or more particles, even for perfect correlations, the EPR program does not work.

Similar to the proof of Bell's theorem(by using the CHSH-inequalities), there also is an experimental proof of the GHZ theorem. This proof was done by Dik Bouwmeester and his coworkers [30]. They make use of a GHZ state of three photons, where each photon could either by polarized horizontally or vertically. It indeed confirms the conflict as predicted by GHZ shown above.

6 Generalizations of Bell's inequalities

6.1 Bell for Spin-1

In the previous sections, Bell's inequalities were derived and tested based on the model imposed by Bohm. That is, based on spin-1/2 particles. It was shown in the article he made together with Aharonov that the polarization properties of photons are similar to the spin properties of spin-1/2 particles. They concluded that experiments based on polarization of photons could be used to test Bell's theorem. However, it is well-known that photons have spin-1. Therefore, one could question wether local-hidden variable theories are also proven to be in conflict with quantum mechanics when talking about particles with spin other than 1/2. There have indeed been papers to prove this for arbitrary spin. In this section, the prove for spin-1 will be given, based on the paper by Wu *et* al. [39].

Just like with spin-1/2, they start with the singlet state of two particles, but in this case for two spin-1 particles. Making use of Clebsch-Gordan Coefficients and using an implicit s_1=s_2=1 notation we get

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|1\rangle|-1\rangle - |0\rangle|0\rangle + |-1\rangle|1\rangle), \tag{6.1}$$

here, $|m_i\rangle$ denotes the eigenvector belonging to the spin operator $\hat{S}$ along the z-direction. One can also make a rotation through an angle β along the y-axis such that the eigenvector transforms to $|m_i'\rangle$. Where we have the following relation between the two

$$|m_i'\rangle = \sum_{l=0}^{3} D_{ji}(\beta)|m_i\rangle, \tag{6.2}$$

where D is the rotation matrix for an s=1 state. It is worth noticing that in general the matrix does also depend on angles made with the z- and x-axis. In this case, the writers defined those angles to be zero such that every relevant direction is to be viewed as a rotation along the y-axis. The matrix given in the article is not completely correct, however as we will see, they will use the correct one in their further calculations. The matrix is given by

$$D(\beta) = \begin{pmatrix} \frac{1+\cos(\beta)}{2} & \frac{-\sin(\beta)}{\sqrt{2}} & \frac{1-\cos(\beta)}{2} \\ \frac{\sin(\beta)}{\sqrt{2}} & \cos(\beta) & -\frac{\sin(\beta)}{\sqrt{2}} \\ \frac{1-\cos(\beta)}{2} & \frac{\sin(\beta)}{\sqrt{2}} & \frac{1+\cos(\beta)}{2} \end{pmatrix}. \tag{6.3}$$

For a derivation of this matrix, also known as the rotation operator, see for example the book of Rose [32].

The two spin-1 particles move in opposite directions along the z-axis. Stern-Gerlach analyzers will measure the spin of partile 1 along a direction β_1 and the spin of particle 2 along β_2. Making use of Eq.(6.2) the state can be written as

$$\begin{aligned} |\psi\rangle = \frac{1}{\sqrt{3}}\{\sin^2(\frac{\beta_1-\beta_2}{2})|1\rangle|1\rangle - \frac{1}{\sqrt{2}}\sin(\beta_1-\beta_2)|1\rangle|0\rangle \\ + \cos^2(\frac{\beta_1-\beta_2}{2})|-1\rangle|1\rangle + \frac{1}{\sqrt{2}}\sin(\beta_1-\beta_2)|0\rangle|1\rangle \\ - \cos(\beta_1-\beta_2)|0\rangle|0\rangle - \frac{1}{\sqrt{2}}\sin(\beta_1-\beta_2)|0\rangle|-1\rangle \\ + \cos^2(\frac{\beta_1-\beta_2}{2})|-1\rangle|1\rangle + \frac{1}{\sqrt{2}}\sin(\beta_1-\beta_2)|-1\rangle|0\rangle \\ + \sin^2(\frac{\beta_1-\beta_2}{2})|-1\rangle|-1\rangle\}. \end{aligned} \tag{6.4}$$

The probability that a measurement finds the particles to be in the state $|m_1\rangle|m_2\rangle$ according to quantum mechanics is

$$P_{m_1m_2} = |\langle\psi|m_1\rangle|m_2\rangle|^2. \tag{6.5}$$

From this we get the following probabilities:

$$\begin{aligned} &P_{11} = \frac{1}{3}\sin^4(\frac{\beta_1-\beta_2}{2}) \\ &P_{00} + P_{0,-1} + P_{-1,0} + P_{-1,-1} = \frac{1}{3}(1+\sin^4(\frac{\beta_1-\beta_2}{2})). \end{aligned} \tag{6.6}$$

What is left is to show that a local-hidden variable theorem shows an inconsistency with Eq.(6.6). In a similar way as Bell's theorem, the singlet state now becomes complete by adding the parameter λ. Define the probability to obtain the result m for particle 1 when measuring its spin along β_1 to be $p_m(\beta_1, \lambda)$. Similarly for particle 2 to obtain n when measuring along β_2. This probability is denoted as $q_n(\beta_2, \lambda)$.

Similar to Bell's theorem, the joint probability becomes

$$P_{11}(\beta_1, \beta_2) = \int \mathrm{d}\lambda \rho(\lambda)) p_m(\beta_1, \lambda) q_n(\beta_2, \lambda). \tag{6.7}$$

Making use of a theorem of Clauser and Horne [14], one obtains (see the Appendix for the proof) the following inequality

$$\begin{aligned} S = P_{11}(\beta_1, \beta_2) - P_{11}(\beta_1, \beta_2') + P_{11}(\beta_1', \beta_2') + P_{00}(\beta_1', \beta_2) \\ +P_{0,-1}(\beta_1', \beta_2) + P_{-1,0}(\beta_1', \beta_2) + P_{-1,-1}(\beta_1', \beta_2) \leq 1. \end{aligned} \tag{6.8}$$

This is very similar to the kind of inequalities we have seen before. Moreover, it can be seen that by choosing $\beta_1 = 0°$, $\beta_1' = 2\beta_2$, $\beta_2' = 3\beta_2$ and $\beta_2 = 147.7°$, one gets the folowing contradiction

$$S = 1.12 \leq 1. \tag{6.9}$$

Therefore, once again, we get a contradiction between a local-hidden variable theorem and quantum mechanics. This time for spin-1 particles instead of spin-1/2.

6.2 Bell for two particles with arbitrary spin

Now that we have dealt with the case of two spin-1 particles, let us look at the general case: two spin-s particles. This proof is based on an article by Mermin [28]. Two spin-s particles flying apart in a singlet state $|\phi\rangle$. Mermin then gives the general state for a singlet state with the appropriate properties

$$|\phi\rangle = \frac{1}{\sqrt{2s+1}} \sum_{m=-s}^{s} (-1)^{s-m} |m\rangle | -m\rangle, \tag{6.10}$$

where agai,n as with Eq.(6.1), I made use of an implicit $s_1 = s_2 = s$ notation. To show this is indeed the case, we must see that what is done here is just a Clebsch-Gordan expansion. Using a similar notation as in the book of Sakurai [33], a general expansion of this kind will be

$$|j_1, j_2, j, m\rangle = \sum_{m_1} \sum_{m_2} \langle j_1, j_2, m_1, m_2 | j_1, j_2, j, m\rangle |j_1, j_2, m_1, m_2\rangle, \tag{6.11}$$

where $j = j_1 + j_2$, $m = m_1 + m_2$ and $\langle j_1, j_2, m_1, m_2 | j_1, j_2, j, m\rangle$ are the Clebsch-Gordan Coefficients (CGCs).

There is a general expression for the CGCs, which I took from the book of Rose [32]

$$\begin{aligned} &\langle j_1, j_2, m_1, m_2 | j_1, j_2, j, m\rangle = \\ &\quad \delta_{m,m_1+m_2} \times [(2j+1) \frac{(j_1+j_2-j)!(j+j_1-j_2)!(j+j_2-j_1)!}{(j_1+j_2+j+1)!} \\ &\quad\quad \times (j_1+m_1)!(j_1-m_1)!(j_2+m_2)!(j_2-m_2)!(j+m)!(j-m)!]^{1/2} \\ &\quad\quad \times \sum_k \frac{(-1)^k}{k!} [(j_1+j_2-j-k)!(j_1-m_1-k)!(j_2+m_2-k)! \\ &\quad\quad\quad \times (j-j_2+m_1+k)!(j-j_1-m_2+k)!]^{-1}. \end{aligned} \tag{6.12}$$

Here, the sum only runs over those values of k such that the factorial elements are positive. Plugging in the properties of the singlet state ($j = m = 0$) will indeed give Eq.(6.10). Because $|\phi\rangle$ has total spin equal to zero, it is rotationally invariant. It is the same whatever the direction may be. This property leads to the same EPR argument as we have seen before. Using Bell's inequality, this argument has been shown incorrect. However both Bell's inequality and the experiments that have been done to prove it have been experiments in which the values of the measurements were two-fold. It is therefore useful to show that a similar inequality also holds for multiple-value experiments by using two spin particles with arbitrary spin s. This proof will have the same structure as before. It will show a conflict between predictions made by a local-realistic theory and quantum mechanics. To do so, begin with the following inequality

$$s|m_1(\hat{\mathbf{a}}) + m_1(\hat{\mathbf{b}})| \geq -m_1(\hat{\mathbf{a}})m_1(\hat{\mathbf{c}}) - m_1(\hat{\mathbf{b}})m_1(\hat{\mathbf{a}}), \tag{6.13}$$

where $m_1(\hat{\mathbf{n}})$ is value obtained when measuring the spin of particle 1 in any direction $\hat{\mathbf{n}} = \hat{\mathbf{a}}, \hat{\mathbf{b}}, \hat{\mathbf{c}}$. Using the fact that for a local-realistic theory in every measuremental run $m_1(\hat{\mathbf{n}}) = -m_2(\hat{\mathbf{n}})$ and averaging over the values obtained by performing many measurement we get

$$s\langle|m_1(\hat{\mathbf{a}}) - m_2(\hat{\mathbf{b}})|\rangle_{av} \geq \langle m_1(\hat{\mathbf{a}})m_2(\hat{\mathbf{c}})\rangle_{av} + \langle m_1(\hat{\mathbf{b}})m_2(\hat{\mathbf{c}})\rangle_{av}. \tag{6.14}$$

The point being made here by Mermin is that each term given in this equation can also be determined using quantum mechanics. For the terms on the right he shows

$$\langle m_1(\hat{\mathbf{n}})m_2(\hat{\mathbf{n}}')\rangle_{av} = \langle\phi|\vec{\mathbf{S}}^{(1)} \cdot \hat{\mathbf{n}}\vec{\mathbf{S}}^{(2)} \cdot \hat{\mathbf{n}'}|\phi\rangle = -\frac{1}{3}s(s+1)\hat{\mathbf{n}} \cdot \hat{\mathbf{n}}'. \tag{6.15}$$

To show this let us first evaluate $\vec{\mathbf{S}}^{(1)} \cdot \hat{\mathbf{n}}\vec{\mathbf{S}}^{(2)} \cdot \hat{\mathbf{n}'}$ in their components. In quantum mechanics, the spins can expressed in terms of Pauli matrices σ

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \, \sigma_{\mathbf{2}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \, \sigma_{\mathbf{3}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{6.16}$$

Let

$$\hat{\mathbf{n}} = \begin{pmatrix} n_x \\ n_y \\ n_z \end{pmatrix}. \tag{6.17}$$

Then

$$\vec{\sigma} \cdot \hat{\mathbf{n}} = \sum_{l=0}^{3} n_l \sigma_l. \tag{6.18}$$

Now let us work in components to evaluate

$$(\vec{\sigma}^{(1)} \cdot \hat{\mathbf{n}})(\vec{\sigma}^{(2)} \cdot \hat{\mathbf{n}'}). \tag{6.19}$$

We have

$$\sigma_j^{(1)} n_j \sigma_k^{(2)} n'_k = (\frac{1}{2}\{\sigma_j^{(1)}, \sigma_k^{(2)}\} + \frac{1}{2}[\sigma_j^{(1)}, \sigma_k^{(2)}]) n_j n'_k, \tag{6.20}$$

where we use an implicit summation whenever we see repeated indices. In this case, the commutator vanishes such that

$$\vec{\mathbf{S}}^{(1)} \cdot \hat{\mathbf{n}} \vec{\mathbf{S}}^{(2)} \cdot \hat{\mathbf{n}'} = \frac{1}{2}\{S_\mu^{(1)}, S_\nu^{(2)}\} n_\mu n'_\nu. \tag{6.21}$$

Eq.(6.15) becomes

$$\langle \phi | \frac{1}{2}(S_\mu^{(1)} S_\nu^{(2)} + S_\nu^{(2)} S_\mu^{(1)}) n_\mu n'_\nu | \phi \rangle. \tag{6.22}$$

Mermin then uses a rather elegant argument to proceed. Remembering that we are talking about a singlet state, we know that it is rotationally invariant in spin space(in the Appendix I will show the rotationally invariance of a singlet Bell state). Based on this argument, we know that the above equation must be proportional to the unit tensor $n_\mu n'_\nu \delta_{\mu\nu}$. Taking the trace on both side then shows that the proportionality constant is

$$\frac{1}{6}\langle \phi | \vec{\mathbf{S}}^{(1)} \cdot \vec{\mathbf{S}}^{(2)} + \vec{\mathbf{S}}^{(2)} \cdot \vec{\mathbf{S}}^{(1)} | \phi \rangle = \frac{1}{6}\langle \phi | (\vec{\mathbf{S}}^{(1)} + \vec{\mathbf{S}}^{(2)})^2 - (\vec{\mathbf{S}}^{(1)})^2 - (\vec{\mathbf{S}}^{(2)})^2 | \phi \rangle. \tag{6.23}$$

Again using the fact that we are talking about a singlet state such that $\langle \phi | (\vec{\mathbf{S}}^{(1)} + \vec{\mathbf{S}}^{(2)})^2 | \phi \rangle$ vanishes and remembering that we are talking about spin-s particles we know that

$$\langle \phi | \frac{1}{2}(S_\mu^{(1)} S_\nu^{(2)} + S_\nu^{(2)} S_\mu^{(1)}) n_\mu n'_\nu | \phi \rangle = -\frac{1}{3} s(s+1) n_\mu n'_\nu \delta_{\mu\nu}, \tag{6.24}$$

which completes the proof.

For the left-hand part of Eq.(6.14) we have

$$\langle | m_1(\hat{\mathbf{n}}) - m_2(\hat{\mathbf{n}}') | \rangle_{av} = \sum_{m,m'} |m - m'| P(m, m', \alpha), \tag{6.25}$$

where $P(m, m', \alpha)$ is the probability of getting the values m for particle 1 and m' for particle 2, and α is the angle between $\hat{\mathbf{n}}'$ and $\hat{\mathbf{n}}$. This probability is given by

$$P(m, m', \alpha) = |\langle \phi | m \rangle | m' \rangle_{\hat{\mathbf{n}}, \hat{\mathbf{n}}'}|^2. \tag{6.26}$$

Plugging in Eq.(6.10) will give

$$P(m, m', \alpha) = \frac{1}{2s+1} |_{\hat{\mathbf{n}}'} \langle -m' | m \rangle_{\hat{\mathbf{n}}}|. \tag{6.27}$$

Using the notation used by Rose [32], we see that this quantity is a component of the rotation matrix $d_{m,-m'}(\alpha)$. The fact that $d_{m,-m'}(\alpha) = d_{-m',m}(-\alpha)$ will enable us to write P as

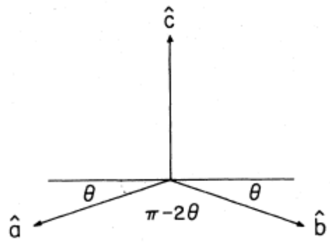

Figure 9: Orientation used by Mermin for general spin [28].

$$P(m, m', \alpha) = \frac{1}{2s+1}|\langle m|e^{i\alpha S_y}| - m'\rangle|^2 = \frac{1}{2s+1}|\langle m|e^{i(\alpha-\pi)S_y}|m'\rangle|^2. \quad (6.28)$$

Here, the y-axis is taken to be perpendicular to the $\hat{\mathbf{n}} - \hat{\mathbf{n}}'$-plane and the z-axis is taken to be parallel to $\hat{\mathbf{n}}$. In this case we use the orientation of the axes $\hat{\mathbf{a}}, \hat{\mathbf{b}}, \hat{\mathbf{c}}$ as shown in Figure 9. Using these orientations along with Eq.(6.25), Eq.(6.28), Eq.(6.14) and Eq.(6.15) we get the result

$$\frac{1}{2s+1}\sum_{m,m'}|m-m'||\langle m|e^{-2i\theta S_y}|m'\rangle|^2 \geq \frac{2}{3}(s+1)\sin\theta. \quad (6.29)$$

To show a contradiction between quantum mechanics and a local-realistic theory, Mermin finds a lower bound for θ by noting that the left-hand side of this equation can only increase if $|m - m'|$ is replaced by its square such that the inequality will certainly fail if

$$\frac{2}{3}(s+1)\sin\theta > \frac{1}{2s+1}\sum_{m,m'}(m-m')^2|\langle m|e^{-2i\theta S_y}|m'\rangle|^2. \quad (6.30)$$

The right-hand side of this equation will turn out to be

$$\frac{1}{2s+1}\sum_{m,m'}(m-m')^2|\langle m|e^{-2i\theta S_y}|m'\rangle|^2 = \frac{4\sin^2\theta}{3}s(s+1). \quad (6.31)$$

The proof will be given in the Appendix. Therefore the inequality (6.29) will fail for

$$0 < \sin\theta < 1/2s, \quad (6.32)$$

from which we can see that for this range of angles, quantum mechanics is not in agreement with local-realism. Once again, we have found a new type of Bell's inequality, this time for the most general case of the spin of two particles.

6.3 Bell for an arbitrary number of spin-1/2 particles

One can imagine two different generalizations for Bell's inequalities. The first one is a generalization of the spin of the particles as shown above. The second one is a generalization of the number of particles that are in an entangled state. This will be the subject of this section. As far as I know, the first person to do this generalization was Mermin [29]. He showed this generalization based on the same kind of state used in the GHZ experiment. The generalization of the GHZ state can be

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow .... \uparrow\rangle + i|\downarrow\downarrow ...... \downarrow\rangle), \tag{6.33}$$

where in this case $\uparrow$ in the ith position means that the ith particle has spin up and similarly $\downarrow$ for spin down. This state is in comparison with the previously used GHZ state for four particles different in the number of particles, n, and differs with a phase i which has been chosen by Mermin. One can see that the following operator is an eigenstate of this state

$$A = \frac{1}{2i}(\prod_{j=1}^{n}(\sigma_x^j + i\sigma_y^j) - \prod_{j=1}^{n}(\sigma_x^j - i\sigma_y^j)), \tag{6.34}$$

with corresponding eigenvalue 2^{n-1}.

Using the diagonal elements of this operator on the state $|\phi\rangle$ and expanding will give

$$\begin{aligned} \langle\phi|\sigma_y^1\sigma_x^2.....\sigma_x^n|\phi\rangle + ... \\ -\langle\phi|\sigma_y^1\sigma_y^2\sigma_y^3\sigma_x^4.....\sigma_x^n|\phi\rangle + ... \\ +\langle\phi|\sigma_y^1\sigma_y^2\sigma_y^3\sigma_y^4\sigma_y^5\sigma_x^6.....\sigma_x^n|\phi\rangle + ... \\ +..... = 2^{n-1} \end{aligned} \tag{6.35}$$

In this way each line in the above equation contains all distinct permutations of the subscripts, that is all permutations of x and y for which y is odd. This array then contains 2^{n-1} terms. Similar to the GHZ case for four particles, when one considers only the extreme values of each term, either being $+1$ or -1. The expansion then adds up to 2^{n-1}. However, in this case we will look at imperfect measurements, such that the functions do not attain their extreme values. In a similar way as before, one imposes a measured distribution function $P_{\mu_1...\mu_n}(m_1...m_n)$ that describes the outcomes of the functions in the above expansion. Here $\mu_i = x, y$ and $m_i =\uparrow$ or $\downarrow$. As before, defining a set of local-hidden variables λ will give a representation of the distribution function

$$P_{\mu_1...\mu_n}(m_1...m_n) = \int \mathrm{d}\lambda\rho(\lambda)p_{\mu_1^1}(m_1,\lambda)...p_{\mu_n^n}(m_n,\lambda), \tag{6.36}$$

which is the mathematical translation of local realism. Based on this representation, the mean of a product of the x- and y-component of the spin of the particles will be

$$E_{\mu_1...\mu_n} = \int \mathrm{d}\lambda\rho(\lambda)E_{\mu_1^1}(\lambda)...E_{\mu_n^n}(\lambda), \tag{6.37}$$

where

$$E_\mu^j(\lambda) = p_\mu^j(\uparrow,\lambda) - p_\mu^j(\downarrow,\lambda). \tag{6.38}$$

These correlation functions are experimentally determined and they belong to the linear combination of theoretical correlation functions, whose value is determined by Eq.(6.35). The linear combination of the experimental correlation function then is

$$F = \int \mathrm{d}\lambda\rho(\lambda)\tfrac{1}{2i}(\prod_{j=1}^{n}(E_x^j + iE_y^j) - \prod_{j=1}^{n}(E_x^j - iE_y^j)). \tag{6.39}$$

In quantum mechanics $F = \langle\phi|A|\phi\rangle$, which will just give you the eigenvalue of the operator A, which is 2^{n-1}.

The value obtained for a local-hidden variable theorem is still given by Eq.(6.39). We are left to show that it differs from the quantum mechanical value. To do this, we will find an upper bound for Eq.(6.39). As noted, consider imperfect correlations, such that each of the $2n$ terms $E_x^j E_y^j$ will lie between -1 and $+1$. We can write Eq.(6.39) as

$$F = Im(\int \mathrm{d}\lambda\rho(\lambda)\prod_{j=1}^{n}(E_x^j + iE_y^j)). \tag{6.40}$$

Again, Mermin has an elegant way of calculating this equation. His argument is based on the fact that the function F is bounded by a product of $2n$ complex numbers, each with a magnitude of $\sqrt{2}$ and phase $\pm\pi/4$ or $\pm 3\pi/4$. This results in the following upper bound for the function F

$$\begin{aligned} F &\leq 2^{n/2} \text{ if } n \text{ is even} \\ F &\leq 2^{(n-1)/2} \text{ if } n \text{ is odd.} \end{aligned} \tag{6.41}$$

We see that if $n > 2$ the quantity F as given by a local-hidden variable theorem will be less than the quantum-mechanical value. Thus, predictions by quantum mechanics exceed these predictions by a factor $2^{(n-2)/2}$ for even n and by a factor $2^{(n-1)/2}$ for odd n. This means that the amount by which quantum mechanical predictions exceed the predictions based on the EPR paper grows exponentially by the number of particles.

Ardehali [1] also discussed Bell's inequalities for n spin-1/2 particles. His results showed a similar exponentially large violation found by Mermin. Their setup was a bit different from that of Mermin. Mermin measured the spin along the x- or y-direction which were taken orthogonal to the z-direction, which was defined to lie along the line of movement of the paticles. However, Ardehali measured the spin of the nth particle differently. He measured its spin along an axis $\vec{\mathbf{a}}$ in the xy plane making an angle of 45°with the x-axis. Or he measured along $\vec{\mathbf{b}}$ making an angle of 135°with the x-axis. I am not going to show the proof of Ardehali. It is very similar to the one used by Mermin, but things are defined a bit differently as a concequence of the different way the spins are measured for the nth particle. However, it is good to mention that there have been many different ways of dealing with the EPR paper, mostly based on similar ways in which Bell did. Although one could argue that Bell's inequalities were all that was needed to show that the EPR argument was incorrect. However, I find it worthwhile to study the principle of local realism and entanglement, mostly because of its applications. These principles may be useful in theories about quantum computing, quantum cryptography (to be discussed in the next section) and quantum teleportation, which all could have an incredible impact on our current technology. To fully understand those theories, it is in my opinion useful to know as much as there is to know about their theoretical basis.

7 Entanglement, Bell's Theorem and Information

We have seen how "Bell-like" theories dealt with the strange property of quantum entanglement in combination with local theories. However, one may wonder if entanglement could be used to send messages between two observers without being limited by the speed of light. This could be a result of the "instant" correlation properties of two EPR particles. In the context of section 2, let us introduce two observers: Alice and Bob, who measure the spin of particle 1 and 2 respectively. However, when Bob makes a measurement on his particle and he gets a result, he does not know if this is the result of a measurement that Alice has made when the two are not communicating. Bob just gets a value for the spin of particle 2, without knowing if this is the value he should have gotten as a result of Alice her measurement. We thus see that when Alice and Bob are not communicating in any other way, there is no information being transfered in a "faster-than-light" way. Weinberg [36] has shown a generalization of the above argument. He shows that for systems like Bohm's version of the EPR setup, where the results of the measured quantities take on discrete values, the fact that no information is being transfered here is a result of the linearity of quantum mechanics. In fact, Polchinski [31] has shown that when one adds non-linearities in quantum mechanics, instantaneous communication would be possible. So in principle, there is no way the principle of entanglement could be used as a "fater-than-light" way of communicating. However, it might be used in an important application. A way of communicating which has been with us centuries B.C [35]: cryptography.

7.1 Quantum Cryptography

In classical cryptography, a text or some information is being transmitted from one person to another. This text is called the *plaintext*. A so-called *key* is added to this plaintext. This key, together with the plaintext is being encrypted by using an *algorithm* into a *ciphertext*. The key specifies the details of the encryptoning process. For example, if the algorithm is to substitute each letter of a plaintext with another letter. This other letter is to be chosen from an other alphabet than has been used to write the plaintext. This alphabet is called the *cipheralphabet*. The key then defines the exact cipher alphabet to be used for the particular encryptoning process. The receiver uses this key to decrypt the ciphertext into the plaintext, using the appropriate algorithm. This

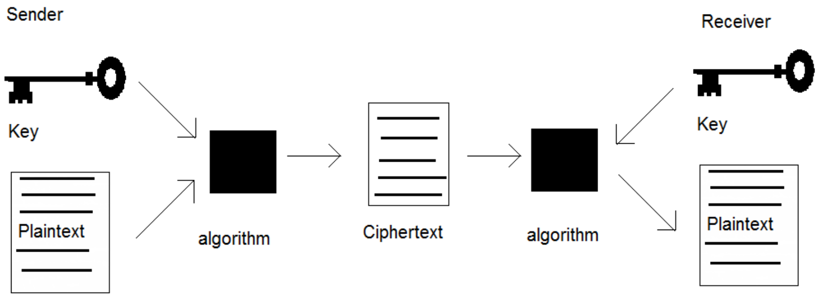

Figure 10: General illustration of encrypting a plaintext [35]

.

general process is illustrated in Figure 10. In the perfect scenario, for a message to be sent safely, it should be impossible to decypher the ciphertext without the key. The idea of using quantum mechanics [22] in cryptography is to let two observers, Alice and Bob, use a quantum channel to only transfer a key, consisting of a random sequence of bits. Quantum mechanics can be used to check wether the key has been perturbed by an eavesdropper (Eve). If Eve has not eavesdropped, the key can be safely be used to encrypt messages. If Eve has eavesdropped, Bob and Alice just discard the key. Since the key does not contain any information, no valuable information to Alice and Bob is being lost. Quantum cryptography was first introduced by Stephen Wiesner [37]. He showed two applications of quantum mechanics in information theory: the first one is transmitting two messages such that only one of the two may be received and the second one is quantum money that cannot be counterfeited. Wiesner's article made for a new articles to arise and new protocols for safe encryptoning to be developed. The first quantum cryptography protocol was introduced in 1984, by Bennett and Brassard and therefore called BB84 [10].

7.1.1 The BB84 Protocol

The BB84 protocol uses a quantum channel to safely transmit a key between two observers. Like before these observers are called Alice and Bob. In this protocol, Alice sends a sequence of polarized photons to Bob. Alice can polarize her photons in four different ways, where the polarization type defines wether the information carried by a photon is either a binary 1 or a binary 0. The polarization types are

The rectilinear bases $\bigoplus$

- horizontal basis $|\leftrightarrow\rangle$ representing a binary 0
- vertical basis $|\updownarrow\rangle$ representing a binary 1

The diagonal bases $\bigotimes$

- +45°basis $|\nearrow\rangle$ representing a binary 0
- -45°basis $|\nwarrow\rangle$ representing a binary 1

The protocol is as follows

1. Alice chooses to polarize each photon of the sequence randomly among these four states.
2. Alice sends the photon sequence to Bob.
3. Bob measures each photon randomly and independent of Alice in either the rectilinear basis $\oplus$ or in the diagonal basis $\otimes$.
4. In this way, Bob and Alice get correlated results whenever they use the same basis and anticorrelated results whenever they use a different one.
5. As a result, Bob gets a sequence of 1's and 0's that has a 25 percent error rate with respect to Alice. Because whenever Bob does use a different basis, there is still a 50 percent chance they get either both a 1 or both a 0. The sequence of bits Bob obtains is called the *raw key* [22].
6. Bob and Alice publically anounce which bases they used to either polarize or measure the photons.
7. They compare these bases and discard the results for which they did not use the same basis.
8. In this way, a sequence of bits that consists of roughly 50 percent of the bits of the original sequence sent by Alice. This sequence is called the *shifted key*.
9. Alice and Bob choose some of the remaning bits to exchange their obtained results. If everything went well and no eavesdropping has taken place, they should agree on the outcomes.
10. If they do agree on these exchaned results, they discard these bits also. In this way, there is a remaining sequence of bits. This sequence can then be used as a safe key to encrypt messages.

Let us give an example of this procedure.

Alice's bit sequence	1	1	1	0	1	0	0	1
Alice's chosen bases	$\vert\updownarrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nwarrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nearrow\rangle$	$\vert\nearrow\rangle$	$\vert\nwarrow\rangle$
Bob's measuring bases	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$
Bob's bit sequence/raw key	0	1	1	0	1	1	1	1
Same basis YES/NO?	NO	YES	NO	NO	YES	NO	YES	YES
After comparing: shifted key	-	1	-	-	1	-	1	1
Shared resulting bits	-	1	-	-	-	-	1	-
Shared bits the same?		YES					YES	
Secret key					1			1

Table 1: Example of a BB84 protocol.

Eavesdropping
Now suppose that there is an eavedropper (Eve). She wants to intercept the sequence of photons that is sent to Bob in such a way that she also knows the key. In the perfect scenario, Eve will know the key without being noticed by

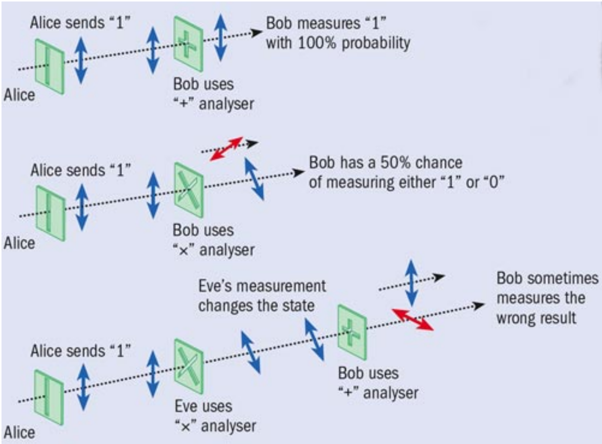

Figure 11: Schematic overview of how Bob obtains the raw key as explained in step 5 of the BB84 protocol [34]

.

Bob and Alice. In this case, it is best for Eve to intercept a photon, clone it such that Eve has a copy of the photon being intercepted with the same polarization as the original one and send the original photon to Bob. In this case, nothing in the above described procedure will have changed and Bob and Alice have not noticed Eve. However, there is a theory in quantum mechanics called the "No-cloning Theorem", which will prevent this kind of eavesdropping from happening.

7.1.2 The No-Cloning Theorem

A single quantum cannot be cloned [38] is an important aticle that states that no unknown quantum state can be copied pefectly. This theorem touches the principle of entanglement as discussed in this thesis in two ways. First, it is important with respect to eavesdropping in the BB84 protocol as stated above. Second, it again shows that no EPR pairs cannot be used to transfer information in a "faster-than-light" kind of way. Let us first consider the latter. As mentioned in the introduction of this section, it is not possible to use the particles that are in an entangled state as "instanteneous" of communicating. However, if quantum cloning would be possible, this would be possible. I will treat this subject in the context of Bohm's version of the EPR state. Using the fact that the entangled state can be written in any orthogonal basis, there are two options for the entangled state

$$\Psi = \frac{1}{\sqrt{2}}(|+\rangle_{z,1}|-\rangle_{z,2} - |-\rangle_{z,1}|+\rangle_{z,2}), \tag{7.1}$$

or

$$\Psi = \frac{1}{\sqrt{2}}(|+\rangle_{x,1}|-\rangle_{x,2} - |-\rangle_{x,1}|+\rangle_{x,2}). \tag{7.2}$$

Whenever Alice wants to send a 0, she chooses to measure the spin of the first particle in the z-direction. Whenever she wants to send a 1, she chooses the x-direction. Suppose Alice wants to send a 0. Bob's particle will then be either in the $|+\rangle_{z,2}|$ or $|-\rangle_{z,2}|$ state. As described before, solely measuring the spin of this particle in any of the two axis will not assure Bob which measuring direction Alice has chosen because any of the four states are equally likely to receive from Bob's point of view. However, if Bob could know the state of his paticle with certainty, this would allow him to instantly know wether Alice has sent him a 0 or a 1. Say now that Bob could clone his particle multiple times. In this way, from Bob's point of view, his state could be one of these four: $|+....+\rangle_{z,2}$, $|-....-\rangle_{z,2}$, $|+....+\rangle_{x,2}$ or $|-....-\rangle_{x,2}$. Here $+...+$ or $-...-$ denote the multiple copies made. Bob could measure all of these paticles in the z-direction. He will know that Alice has indeed sent him a 0 if his results will be either all $+1$ or -1 (in terms of $\hbar/2$). If Alice has sent a 1, Bob's results will be equally split between $+1$ and -1. In such a way, thanks to quantum cloning, Bob will know his state and therefore he will know Alice her message instanteneously. Obviously, this would violate causality. Let us focus on the proof that quantum-cloning is not possible to resolve both the eavesdropping poblem and the causality problem. Suppose that we have a pefect cloning system which is in an initial state $|A_0\rangle$, and we want to copy a state $|s\rangle$. In this case, copying would yield

$$|A_0\rangle|s\rangle \rightarrow |A_f\rangle|s\rangle|s\rangle. \tag{7.3}$$

where $|A_f\rangle$ is the final state of the copying system. In terms of the notation of EPR states used before, this will give

$$|A_0\rangle|+\rangle \rightarrow |A_+\rangle|+\rangle|+\rangle, \tag{7.4}$$

and

$$|A_0\rangle|-\rangle \rightarrow |A_-\rangle|-\rangle|-\rangle. \tag{7.5}$$

The problem with copying arises when we have a state that is a linear combination of these states

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle. \tag{7.6}$$

Because of the linearity of quantum mechanics, copying this combinated state will give

$$|A_0\rangle(\alpha|+\rangle + \beta|-\rangle) \rightarrow \alpha|A_+\rangle|+\rangle|+\rangle + \beta|A_-\rangle|-\rangle|-\rangle. \tag{7.7}$$

But this is not equal to a pefect copy of the state, which would be

$$|A_0\rangle(\alpha|+\rangle + \beta|-\rangle) \rightarrow |A_f\rangle(\alpha|+\rangle + \beta|-\rangle)(\alpha|+\rangle + \beta|-\rangle). \tag{7.8}$$

Thus, we have shown that indeed it is not possible to pefectly copy a quantum state. This will resolve our issue with causality. The crucial point of the cloning theorem follows from the linearity of quantum mechanics. Remember that I stated before that Polchinski and Weinberg have also dealt with the problem of causility in combination with entanglement using (non)linearity in quantum mechanics. They used a theory in which non-linearities are added to quantum mechanics. In this case, no such non-linearities were necessary, but we do see that linearity in quantum mechanics is important. Next to our issue of causality, the no-cloning theorem also provides us with a protection against an eavesdropper in the BB84 protocol. In the above prove I have used the spin-state notation to keep track of notation. However, it is obvious that this poof may be given for any chosen quantum state that is similar to that of the spin-state. Hence, this theory also holds for the polarization states as introduced in Section 7.1.1. We can conclude that in the BB84 protocol Eve cannot intercept a photon sent by Alice, keep a perfect copy and send it to Bob such that she is not being discovered.

7.1.3 Quantum Cryptography Based on Bell's Theorem

Now that we have seen how the principle of entanglement can be used in cryptographic protocols to securely transport a key. We have seen that problems with entanglement were solved using Bell's theorem. In fact, Bell's theorem can also directly be used in quantum mechanics. This was done by Artur Ekert [18]. From now on, I will refer to his protocol as the Ekert protocol. Ekert makes use of a quantum channel where two spin-1/2 paticles are in a singlet state and moving away from each other in opposite direction in the z-direction. One of these particles is sent to Alice, the other to Bob. Alice and Bob measure the spin of their particle along one of the directions $\vec{\mathbf{a}}_i$ and $\vec{\mathbf{b}}_j$ $(i, j = 1, 2, 3)$ respectively. These vectors lie in the x, y-plane, making angles $\phi_1^a = 0$, $\phi_2^a = 1/4\pi$, $\phi_3^a = 1/2\pi$, $\phi_1^b = 1/4\pi$, $\phi_2^b = 1/2\pi$ and $\phi_3^b = 3/4\pi$ with the x-axis. Superscript "a" or "b" denotes wether we are talking about the measurements of Alice or Bob respectively. Similar to the BB84 protocol, they choose their measurement axis randomly for each particle they receive. We know from Eq.(4.1) that the correlation coefficient for this process is given by

$$E(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_j) = P_{++}(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_j) + P_{--}(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_j) - P_{+-}(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_j) - P_{-+}(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_j). \tag{7.9}$$

Also, we know from Eq.(3.1) that quantum mechanics predicts

$$E(\vec{\mathbf{a}}_i, \vec{\mathbf{b}}_j) = -\vec{\mathbf{a}}_i \cdot \vec{\mathbf{b}}_j. \tag{7.10}$$

Let us consider the quantity as defined by CHSH for the specific orientations of Alice and Bob

$$S = E(\vec{\mathbf{a}}_1, \vec{\mathbf{b}}_1) - E(\vec{\mathbf{a}}_1, \vec{\mathbf{b}}_3) + E(\vec{\mathbf{a}}_3, \vec{\mathbf{b}}_1) + E(\vec{\mathbf{a}}_3, \vec{\mathbf{b}}_3). \tag{7.11}$$

Using use of the above specified angles, we see that

$$S_{\mathrm{QM}} = -2\sqrt{2}. \tag{7.12}$$

After they have made their measurements, Alice and Bob publicly announce which orientations they have chosen without saying wether they have measured spin-up or spin-down. They first discard all measurements for which one of them failed to measure a particle. They then separate the remaining measurements into two groups

1. The first group consists of all measurements for which they used different measuring orientations.

2. The second group consists of all measurements for which they used the same measuring orientations.

After that, Alice and Bob publically announce to each other which results they have obtained for their measurements belonging to group 1 only. These results allow them to find the value of S. If no evesdropping has taken place, so the system has not been disturbed, and they should get $S = -2\sqrt{2}$. When they do get this value, they that the results beloning to group 2 must be anticorrelated as a result of entanglement. They make use of this anticorrelation to obtain a secret key. For example, if Bob measured his particle to be spin-up, he knows the corresponding particle of Alice is spin-down. If they agree that whenever Alice measures spin-down, she sends a 0, and whenever she measures spin-up, she sends a 1. In this way, like before, a bit sequence is transported from Alice to Bob without an Eve founding out what this key is. To see this last argument, we look at what happens whenever Eve intervenes. The following argument is similar to Bell's argument. He first looked at the predictions of quantum mechanics and compared them with the predictions made whenever "elements of physical reality" are being added. In the case these elements were the local-hidden variables λ. To intervene in this protocol, Eve would want to intecept the particles going to both Alice and Bob. She measures them along directions of her preference, say $\vec{\mathbf{n}}_a$ for Alice her particle and $\vec{\mathbf{n}}_b$. In this way, she would be able to manipulate the quantum channel in such a way that he would know which key Bob and Alice would eventually get. However, similar to adding local-hidden variables in quantum mechanics, adding these new measurement axes as elements of reality will lead to a new Bell inequality that can be used to prevent succesful evesdropping. Following a similar procedure and notation as in Section 3.3.1 we now get a modified value for S

$$\begin{aligned} S = \int \rho(\vec{\mathbf{n}}_a, \vec{\mathbf{n}}_b) d\vec{\mathbf{n}}_a d\vec{\mathbf{n}}_b [(\vec{\mathbf{a}}_1 \cdot \vec{\mathbf{n}}_a)(\vec{\mathbf{b}}_1 \cdot \vec{\mathbf{n}}_b) - (\vec{\mathbf{a}}_1 \cdot \vec{\mathbf{n}}_a)(\vec{\mathbf{b}}_3 \cdot \vec{\mathbf{n}}_b) \\ + (\vec{\mathbf{a}}_3 \cdot \vec{\mathbf{n}}_a)(\vec{\mathbf{b}}_1 \cdot \vec{\mathbf{n}}_b) + (\vec{\mathbf{a}}_3 \cdot \vec{\mathbf{n}}_a)(\vec{\mathbf{b}}_3 \cdot \vec{\mathbf{n}}_b)], \end{aligned} \tag{7.13}$$

where $\rho(\vec{\mathbf{n}}_a, \vec{\mathbf{n}}_b)$ describes the probability that Eve interceps a particle andmeasure its spin component along a given $\vec{\mathbf{n}}_a$ or $\vec{\mathbf{n}}_b$ for particle a or b respectively. This can be written as

$$\begin{aligned} S = \int \rho(\vec{\mathbf{n}}_a, \vec{\mathbf{n}}_b) d\vec{\mathbf{n}}_a d\vec{\mathbf{n}}_b [\cos(\phi_1^a - \theta_a) \cos(\phi_1^b - \theta_b) \\ - \cos(\phi_1^a - \theta_a) \cos(\phi_3^b - \theta_b) + \cos(\phi_3^a - \theta_a) \cos(\phi_1^b - \theta_b) \\ + (\phi_3^a - \theta_a) \cos(\phi_3^b - \theta_b)], \end{aligned} \tag{7.14}$$

where θ_a, θ_b are the angles Eve her measuring directions make with the x-axis for particles a and b respectively. Using the following trigonometric identity

$$\cos(\alpha - \beta) = \cos(\alpha)\cos(\beta) + \sin(\alpha) sin(\beta), \tag{7.15}$$

and using the specific orientations used by Alice and Bob, it is straightforward to arrive at

$$S = \int \rho(\vec{\mathbf{n}}_a, \vec{\mathbf{n}}_b) d\vec{\mathbf{n}}_a d\vec{\mathbf{n}}_b \sqrt{2} \cos(\theta_a - \theta_b), \tag{7.16}$$

which implies

$$-\sqrt{2} \leq S \leq \sqrt{2}. \tag{7.17}$$

This inequality contradicts the quantum-mechanical prediction given by Eq.(7.12). In this manner, we have derived a new Bell's inequality with a practical use. Eve cannot invoke "elements of reality" to eavesdrop.

7.1.4 Discussion

We have seen that quantum mechanics, and in particular Bell's theorem can be used to safely transfer a key that can be used to encrypt messages. This process, instead of quantum cryptography, may thus well be named "quantum key distribution". The first experimental realization of quantum key distribution was published in 1992 [8]. Quantum key distribution is a relatively new subject, which has been developing since 1970. Different protocols have been developed. We have seen two of them. Several practical issues may arise, which have been discussed [7]. Bennett and Brassard, together with Mermin state that it is not necessary to invoke Bell's theorem [9]. They show however, that the protocol they use eventually boils down to the BB84 protocol. Whatever the protocol may be, they are all equivalent in a manner. Physical laws invoke restrictions on eavesdropping, such that it is possible to safely transfer a common key between two observers that do not share any information initially. In the end, a protocol's succes is based upon how securely and efficiently this key is transported. In the case of the Ekert protocol, the degree of efficiency is determined by how many photons must be sent to ascertain the security of a key that is of a specific length. The less photons needed, the more efficient the protocol.

8 Discussion and Conclusion

The famous paper of EPR has brought up discussion that still have their consequences today. This thesis began with explaining the concept of quantum entanglement. We have seen that this principle was first regarded as a philosophical difficulty, that could mean that quantum mechanics was not complete. Based on a few conditions, the EPR paper sure made people wonder that this would be indeed the case. Several contributions to the theorem have been made in the period between this paper and the discovery of a real theory that would show the EPR argument to be false. Among these contributions, Bohm's contribution might be the most important one. Not only did future theories made use of Bohm's version with spin-1/2 particles, he showed along with Aharonov that the polarization properties of photons could as well be used to test the EPR theory. The latter has had its implications especially in the experimental verification of the theory that would show EPR to be wrong.

It was not until 1964 that John Bell showed that, based on the conditions imposed by EPR, a theory that would make quantum mechanics complete would be in contradiction with quantum theory itself in certain cases. Moreover, we have seen that in order to experimentally test it, certain modifications were necessary. This resulted in the CHSH inequality. Indeed, as was shown in Section 4, there have been experiments confirming these theories. The most famous of these experiments, that is the experiments of Aspect, were discussed. We have slightly touched upon some loopholes that could occur in experimental verification of Bell's inequality. To fully close the subject of Bell's inequalities it is necessary to close all of these loopholes. It has been proposed that a loophole-free Bell experiment is possible [20]. In any further research concerning this subject, it may be worthwhile to further investigate the experimental aspects of Bell's theorem, and their associated loopholes in order to investigate if a loophole-free experiment is indeed possible. This issue of a loophole-free experiment has been discussed even more recently [23]. In this article the so-called fair-sampling loophole has been closed. In the experiments of Aspect and his collaborators, it is assumed that the detected particles are a fair sample of the total number of particles being sent. In the article, Bell's inequality is experimentally violated without this assumption. Moreover, it is mentioned that a loophole-free Bell's experiment is still an important goal for physicists and the authors mention that they think that such an experiment is not unreasonable. However, similar to what the experiments of Aspect have shown us, the experimental data so far has indeed confirmed the completeness of quantum mechanics. Local realistic theories have not only shown to be incompatible with the theoretic results of quantum mechanics, but also with experimental data. It is therefore my belief that up until there are experiments which are not in agreement with quantum mechanics, there is not need to doubt it.

Although Bell has shown that a local realistic theory is in disagreement with quantum mechanics, one could still wonder how the principle of entanglement could be consistent with quantum mechanics as we know it. We are still left with the fact that one particle could have two well-defined spin-components, whicht might be conceptually difficult to accept. In the context of section 2, the way to look at the concept of entanglement is as follows: the frst measurement puts the two-particle system in a state where only the z-components of the particles are definite, while the second measurement does the same for their x-components. Different measurements cause for entanglement of different spin-components of the system. Experimental data is very important for testing theories, and since both of these are in agreement one can draw a simple conclusion. Quantum entanglement is a conceptully strange property that is consistent with the quantum theory itself.

Although one may argue that the theoretical basis of Bell's theorem and the CHSH version of it are enough to experimentally test the completeness of quantum mechanics (apart from the loopholes maybe), we have seen that over the years there have been many different theoretical versions of Bell's theorem. We have seen not only the CHSH version, but also the GHZ theorem. In this theorem, the inequalities of Bell became equalities and it has been shown that even for perfect correlations between particles, local realistic theories as imposed by EPR are inconsistent with quantum theory. Moreover, we have looked at some generalizations. We have seen that it is possible to derive new Bell's inequalities if one considers two particles with general spin and even one when using an arbitrary number of spin-1/2 particles. In the latter case, we have seen that the violation of this new inequality grows exponentially with the number of particles. In the first case, Mermin has shown [28] that if one lets $s \to \infty$, that is in the classical limit, the contradiction between quantum mechanics and a local-realistic theory vanishes. However, if we let the number of particles grow, the similar contradiction becomes even larger. In light of these extreme generalizations, for future research in this subject it might be interesting to investigate if it would be possible to derive a Bell inequality for an arbitrary number of particles with arbitrary spin.

One could ask if all these theoretical versions and generalizations really matter? EPR has proven to be wrong, so the paradox with which we have started has been disproven. Especially when also the possible loopholes have all been closed, there is nothing more to it. But I would argue that there is. The property of quantum entanglement remains part of quantum mechanics. As we have seen in the final section of this thesis, the principle of entanglement may be used to safely transfer a key between two oberservers. Even in particular Bell's theorem itself may be used for similar purposes. With our whole society being dependent on the safety of bank accounts for example, it is important to have a good protection against potential thiefs. Now that technology and especially computers are evolving, secret information becomes less safe everyday. It is therefore very useful to protect this information using physical laws. Quantum cryptography is an example of how such information is indeed protected by laws of quantum mechanics.

During this thesis we have also slightly touched upon the combination of entanglement with causality. One could wonder if entanglement could be used for "faster-than-light" communication. By means the example of the no-cloning theorem, it has been shown that the fact that quantum mechanics is linear forbids this from happening. As I have mentioned, Weinberg and Polchinski have discussed this problem more generally. Weinberg has developed a theoretical framework in which non-linearities are added to quantum mechanics. Based on this, Polchinski has shown that this would mean that that instantenous communication would be possible. For future research, it might be interesting to study this framework along with its consequences.

We have seen how a (philosophical) problem was introduced in quantum mechanics. Nearly three decades later, the theoretical basis to resolve this problem was discoverd. Based on this theory, experimental physics became an important actor in the whole discussion. Once the experiments varified the theory, the principle of entanglement that was seen as a problem at first was discovered to have useful and practical applications in todays society. With applied physics being added to the discussion, all disciplines within physics are having their contribution to the principle of entanglement as discussed in this thesis.

Finally, I would like to thank my supervisor Prof. Rob Timmermans for his guidance throughout this project.

A Appendix

A.1 Proof of Eq.(3.1)

This proof is based on the book of Griffiths [26]. The relevant state is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle), \tag{A.1}$$

where in the book they used the following short $|sm\rangle$ notation as given on page 185, which will be used in the proof

$$\begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle) \\ |11\rangle &= |+\rangle|+\rangle \\ |1-1\rangle &= |-\rangle|-\rangle. \end{aligned} \tag{A.2}$$

Let θ be the angle between the vectors $\vec{\mathbf{a}}$ and $\vec{\mathbf{b}}$. We may very well choose $\vec{\mathbf{a}}$ to lie along the z-axis and $\vec{\mathbf{a}}$ to lie in the x,z-plane. In this case, our notation will be $\vec{\mathbf{s}}_1 \cdot \vec{\mathbf{a}} = S_z^{(1)}$ and $\vec{\mathbf{s}}_2 \cdot \vec{\mathbf{b}} = \cos\theta S_z^{(2)} + \sin\theta S_x^{(2)}$. Let us first evaluate

$$(\vec{\mathbf{s}}_1 \cdot \vec{\mathbf{a}})(\vec{\mathbf{s}}_2 \cdot \vec{\mathbf{b}})|00\rangle = \frac{1}{\sqrt{2}}[S_z^{(1)}(\cos\theta S_z^{(2)} + \sin\theta S_x^{(2)})](|+\rangle|-\rangle - |-\rangle|+\rangle). \tag{A.3}$$

This will be equal to

$$\frac{1}{\sqrt{2}}[(S_z|+\rangle)(\cos\theta S_z|-\rangle + \sin\theta S_x|-\rangle) - (S_z|+\rangle + \sin\theta S_x|+\rangle)]$$

$$= \frac{1}{\sqrt{2}}[|+\rangle(-\cos\theta|-\rangle + \sin\theta|+\rangle) + |-\rangle(\cos\theta|+\rangle + \sin\theta|-\rangle)],$$

where in this case the explicit form of the S_z matrix is used (see the Pauli matrices given in Section 6.2).

$$= [\cos\theta\frac{1}{\sqrt{2}}(-|+\rangle|-\rangle + |-\rangle|+\rangle) + \sin\theta\frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)]$$

$$= [-\cos\theta|00\rangle + \frac{1}{\sqrt{2}}\sin\theta(|11\rangle + |1-1\rangle)].$$

We will get for our expectation value

$$\begin{aligned}
\langle(\vec{\mathbf{s}}_1\cdot\vec{\mathbf{a}})(\vec{\mathbf{s}}_2\cdot\vec{\mathbf{b}})\rangle_{\mathrm{QM}} &= \langle 00|(\vec{\mathbf{s}}_1\cdot\vec{\mathbf{a}})(\vec{\mathbf{s}}_2\cdot\vec{\mathbf{b}})|00\rangle \\
&= \langle 00|[-\cos\theta|00\rangle + \frac{1}{\sqrt{2}}\sin\theta(|11\rangle + |1-1\rangle)] \\
&= -\cos\theta\langle 00|00\rangle = -\cos\theta = -\vec{\mathbf{a}}\cdot\vec{\mathbf{b}},
\end{aligned} \tag{A.4}$$

by remembering that $\vec{\mathbf{a}}$ and $\vec{\mathbf{b}}$ are unit vectors, which completes the proof.

A.2 Proof of Eq.(5.2)

In general, we now that this quantity will be given by

$$E^{\psi}(\hat{\mathbf{n}}_1,\hat{\mathbf{n}}_2,\hat{\mathbf{n}}_3,\hat{\mathbf{n}}_4) = \langle\psi|(\vec{\sigma}_1\cdot\hat{\mathbf{n}}_1)(\vec{\sigma}_2\cdot\hat{\mathbf{n}}_2)(\vec{\sigma}_3\cdot\hat{\mathbf{n}}_3)(\vec{\sigma}_4\cdot\hat{\mathbf{n}}_4)|\psi\rangle, \tag{A.5}$$

which, for the given wave function will be

$$\begin{aligned}
&E^{\psi}(\hat{\mathbf{n}}_1,\hat{\mathbf{n}}_2,\hat{\mathbf{n}}_3,\hat{\mathbf{n}}_4) = \\
&\quad\frac{1}{2}(\langle ++-- |(\vec{\sigma}_1\cdot\hat{\mathbf{n}}_1)(\vec{\sigma}_2\cdot\hat{\mathbf{n}}_2)(\vec{\sigma}_3\cdot\hat{\mathbf{n}}_3)(\vec{\sigma}_4\cdot\hat{\mathbf{n}}_4)|++--\rangle \\
&\quad -\langle ++-- |(\vec{\sigma}_1\cdot\hat{\mathbf{n}}_1)(\vec{\sigma}_2\cdot\hat{\mathbf{n}}_2)(\vec{\sigma}_3\cdot\hat{\mathbf{n}}_3)(\vec{\sigma}_4\cdot\hat{\mathbf{n}}_4)|--++\rangle \\
&\quad -\langle --++ |(\vec{\sigma}_1\cdot\hat{\mathbf{n}}_1)(\vec{\sigma}_2\cdot\hat{\mathbf{n}}_2)(\vec{\sigma}_3\cdot\hat{\mathbf{n}}_3)(\vec{\sigma}_4\cdot\hat{\mathbf{n}}_4)|++--\rangle \\
&\quad +\langle --++ |(\vec{\sigma}_1\cdot\hat{\mathbf{n}}_1)(\vec{\sigma}_2\cdot\hat{\mathbf{n}}_2)(\vec{\sigma}_3\cdot\hat{\mathbf{n}}_3)(\vec{\sigma}_4\cdot\hat{\mathbf{n}}_4)|--++\rangle).
\end{aligned} \tag{A.6}$$

In spherical coordinates, we can write $\vec{\sigma}$ as [26]

$$\vec{\sigma}\cdot\hat{\mathbf{n}} = \sigma_x\sin\theta\sin\phi + \sigma_y\sin\theta\sin\phi + \sigma_z\cos\theta, \tag{A.7}$$

or in matrix notation

$$\vec{\sigma}\cdot\hat{\mathbf{n}} = \begin{pmatrix} \cos\theta & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & -\cos\theta \end{pmatrix}, \tag{A.8}$$

where θ is the angle made with the vertical z-axis. Writing it in this way enables us to find the following quantities

$$\begin{aligned}
\langle +|\vec{\sigma}\cdot\hat{\mathbf{n}}|+\rangle &= \cos\theta \\
\langle +|\vec{\sigma}\cdot\hat{\mathbf{n}}|-\rangle &= e^{-i\phi}\sin\theta \\
\langle -|\vec{\sigma}\cdot\hat{\mathbf{n}}|+\rangle &= e^{i\phi}\sin\theta \\
\langle -|\vec{\sigma}\cdot\hat{\mathbf{n}}|-\rangle &= -\cos\theta,
\end{aligned} \tag{A.9}$$

such that Eq.(A.5) becomes

$$E^{\psi}(\hat{\mathbf{n}}_1, \hat{\mathbf{n}}_2, \hat{\mathbf{n}}_3, \hat{\mathbf{n}}_4) = \cos\theta_1 \cos\theta_2 \cos\theta_3 \cos\theta_4 \\ - \sin\theta_1 \sin\theta_2 \sin\theta_3 \sin\theta_4 \cos(\phi_1 + \phi_2 - \phi_3 - \phi_4). \tag{A.10}$$

If we restrict only to the x, y-plane ($\theta = 90°$), which is what we do in Section 5.1, Eq.(5.2) automatically follows.

A.3 Proof of Eq.(6.9)

Let us begin with giving the theorem as given by Clauser and Horne. Suppose that there are six real numbers: x_1, x_2, X, y_1, y_2, and Y in a way such that

$$\begin{aligned} 0 \leq x_1, x_2 \leq X \\ 0 \leq y_1, y_2 \leq Y, \end{aligned} \tag{A.11}$$

then

$$-XY \leq U \leq 0, \tag{A.12}$$

where

$$U \equiv x_1 y_1 - x_1 y_2 + x_2 y_2 - x_2 Y - X y_1. \tag{A.13}$$

The proof is split into two. First we will show how the upperbound is established. To do so, let us consider the following cases

First assume $x_1 \geq x_2$.
Let us rewrite U as

$$U = (x_1 - X)y_1 + (y_1 - Y)x_2 + (x_2 - x_1)y_2. \tag{A.14}$$

The first two terms are non-positive as a result of Eq.(A.11), the third term is non-positive as a result of our assumption here. So within this assumption we can see the upperbound.

Next assume $x_1 < x_2$.
Let us again rewrite U and use the inequalities(A.11) along with the assumption made here to get

$$\begin{aligned} U &= (y_1 - y_2)x_1 + (x_2 - X)y_1 + (y_2 - Y)x_2 \\ &\leq (y_1 - y_2)x_1 + (x_2 - X)y_1 + (y_2 - Y)x_1 \\ &= (x_2 - X)y_1 + (y_1 - Y)x_1 \leq 0, \end{aligned} \tag{A.15}$$

where also in this case, the upperbound is shown.
The next step is to show the lower bound. As before, we will consider multiple cases

First assume $x_2 \geq x_1$.
Rewrite Eq.(A.12) as

$$U + XY = (X - x_2)(Y - y_1) + x_1 y_1 + (x_2 - x_1)y_2 \geq 0, \quad \text{(A.16)}$$

where the inequality follows from the fact that the first two terms are non-negative as a result of inequalities(A.11) and the third term is non-negative as a result of the assumption made here.

Next assume $y_1 \geq y_2$.
Similar to the first case, we get

$$U + XY = (X - x_2)(Y - y_1) + x_2 y_2 + (y_1 - y_2)x_1 \geq 0. \quad \text{(A.17)}$$

Finally assume $x_2 < x_1$ and $y_1 < y_2$.

$$U + XY = (X - x_2)(Y - y_1) - (x_1 - x_2)(y_2 - y_1) + x_2 y_1 \geq 0. \quad \text{(A.18)}$$

The inequality follows the assumptions made here and inequalities(A.11). These namely make sure that $(X - x_2) \geq (x_1 - x_2) > 0$ and $(Y - y_1) \geq (y_2 - y_1) > 0$. Putting all these cases together completes the proof of the theorem by Clauser and Horne. To proof Eq.(6.9) let us relate this to the case considered in Section 6.1. Using the notation as used in this section, we will us the following obvious relation

$$\langle 1|1\rangle + \langle 0|0\rangle + \langle -1| - 1\rangle = I, \quad \text{(A.19)}$$

where I is the identity matrix, to invoke so-called "natural relations"

$$\begin{aligned} 0 &\leq p_1(\beta_1, \lambda) + p_0(\beta_1, \lambda) + p_{-1}(\beta_1, \lambda) \leq 1 \\ 0 &\leq q_1(\beta_2, \lambda) + q_0(\beta_1, \lambda) + q_{-1}(\beta_1, \lambda) \leq 1. \end{aligned} \quad \text{(A.20)}$$

Using the Clauser and Horne theorem, identifying the following substitutions: $x_1 = p_1(\beta_1, \lambda)$, $x_2 = p_1(\beta_1', \lambda)$, $y_1 = q_1(\beta_2, \lambda)$, $y_2 = q_1(\beta_2', \lambda)$, and $X = Y = 1$, and making use of the above "natural relations" will lead to

$$\begin{aligned} &p_1(\beta_1, \lambda)q_1(\beta_2, \lambda) - p_1(\beta_1, \lambda)q_1(\beta_2', \lambda) + p_1(\beta_1', \lambda)q_1(\beta_2', \lambda) \\ &\quad + (p_0(\beta_1', \lambda) - p_{-1}(\beta_1', \lambda)) \times (q_0(\beta_2, \lambda) - q_{-1}(\beta_2, \lambda)) \leq 1. \end{aligned} \quad \text{(A.21)}$$

Similarly to Eq.(6.7), integrating this equation over $\rho(\lambda)$ will leave us with Eq.(6.9).

A.4 Proof of rotationally invariance of a Bell singlet state

Consider the Bell singlet state

$$\Psi = \frac{1}{\sqrt{2}}(|+\rangle_1|-\rangle_2 - |-\rangle_1|+\rangle_2). \quad \text{(A.22)}$$

Here, I will proof that this state is rotationally invariant. This proof is based on a proof given here [21]. Suppose that we change the direction of measurement of both particles. Suppose that the direction of particle 1 is rotated along an angle θ and the direction of particle 2 is rotated along an angle ϕ. We will get rotated spin states

$$
\begin{aligned}
|\theta\rangle_1 &= \cos\theta|+\rangle_1 + \sin\theta|-\rangle_1 && \text{(A.23a)}\\
|\theta^{\perp}\rangle_1 &= -\sin\theta|+\rangle_1 + \cos\theta|-\rangle_1 && \text{(A.23b)}\\
|\phi\rangle_2 &= \cos\phi|+\rangle_2 + \sin\phi|-\rangle_2 && \text{(A.23c)}\\
|\phi^{\perp}\rangle_2 &= -\sin\phi|+\rangle_2 + \cos\phi|-\rangle_2. && \text{(A.23d)}
\end{aligned}
$$

In terms of this rotated spin states, the singlet state becomes

$$
\begin{aligned}
\psi = \frac{1}{\sqrt{2}}[&(\cos\theta\sin\phi - \sin\theta\cos\phi)|\theta\rangle_1|\phi\rangle_2\\
&+(\cos\theta\cos\phi + \sin\theta\sin\phi)|\theta\rangle_1|\phi^{\perp}\rangle_2\\
&-(\sin\theta\sin\phi + \cos\theta\cos\phi)|\theta^{\perp}\rangle_1|\phi\rangle_2\\
&-(\sin\theta\cos\phi - \cos\theta\sin\phi)|\theta^{\perp}\rangle_1|\phi^{\perp}\rangle_2]. \qquad \text{(A.24)}
\end{aligned}
$$

For the state to be rotationally invariant, this state should be similar to the original one if the spins of both particles are measured along the same direction. This is the case when $\theta = \phi$. Eq.(A.24) in this case becomes

$$
\Psi = \frac{1}{\sqrt{2}}(|\theta\rangle_1|\theta^{\perp}\rangle_2 - |\theta^{\perp}\rangle_1|\theta\rangle_2), \qquad \text{(A.25)}
$$

Indeed this state is similar to the original one, which proves the rotationally invariance of the Bell singlet state.

A.5 Proof of Eq.(6.31)

The proof of this equation will be a long one, therefore I will only give a summary of the real proof. This summary contains all the necessary ingredients to do the whole proof, which basically is a lot of rewriting. To start with begin with rewriting the right-hand side using the fact that $\langle m|S_z|m\rangle = m$

$$
\begin{aligned}
&\frac{-1}{2s+1}\sum_{m,m'}(m-m')^2|\langle m|e^{-2i\theta S_y}|m'\rangle|^2\\
&= \frac{1}{2s+1}\sum_{m,m'}((((\langle m|S_z|m\rangle - \langle m'|S_z|m'\rangle)|\langle m|e^{-2i\theta S_y}|m'\rangle|)^2). \qquad \text{(A.26)}
\end{aligned}
$$

Also we can use $\sum_n |n\rangle\langle n| = 1$ along with $d_{m,m'}(\alpha) = d_{m',m}(-\alpha)$ to write this in a more useful form

$$
-\frac{1}{2s+1}\sum_{m,m'}(\langle m|[S_z, e^{-2i\theta S_y}]|m'\rangle\langle m'|[S_z, e^{2i\theta S_y}]|m\rangle)^2.
$$

Working out the commutators and using the fact that S_z^2 commutes with S_y we get

$$\frac{1}{2s+1}\sum_{m,m'}(\langle m|S_z^2|m\rangle - \langle m|S_z e^{-2i\theta S_y} S_z e^{2i\theta S_y}|m\rangle$$
$$+\langle m|S_z^2|m\rangle - \langle m|e^{-2i\theta S_y} S_z e^{2i\theta S_y} S_z|m\rangle).$$

Making use of the definition of the trace, $Tr(X) = \sum_a \langle a|X|a\rangle$, we see that this becomes

$$\frac{2}{2s+1}Tr(S_z^2 - e^{-2i\theta S_y} S_z e^{2i\theta S_y} S_z).$$

What we then must do is to rewrite $e^{-2i\theta S_y} S_z e^{2i\theta S_y}$. We can do this by using the "Baker-Hausdorf Lemma", as proposed in the book of Rose [32] which is as follows: If G is an Hermitian operator and λ a real parameter and A amatrix then

$$\exp(iG\lambda)A\exp(-iG\lambda) = A + i\lambda[G,A] + \frac{i^2\lambda^2}{2!}[G,[G,A]]+$$
$$... + \frac{i^n\lambda^n}{n!}[G,...[G,A]...] + .. \tag{A.27}$$

Using this Lemma along with the known commutation relations between S_x, S_y and S_z to get

$$e^{-2i\theta S_y} S_z e^{2i\theta S_y} = S_z\cos(2\theta) + S_x\sin(2\theta).$$

Proceeding with our proof, we can write Eq.(6.31) as

$$\frac{2}{2s+1}Tr(S_z^2 - (S_z\cos(2\theta) + S_x\sin(2\theta))S_z).$$

Following the notation of the book of Griffiths [26] we have the following relation for S_x

$$\langle m'|S_x|m\rangle = (\delta_{m',m+1} + \delta_{m'+1,m})\frac{1}{2}\sqrt{s(s+1) - m'm}, \tag{A.28}$$

such that the trace of S_x will vanish. In the end we will get

$$\frac{2(1-\cos(2\theta))}{2s+1}TrS_z^2 = \frac{4sin^2(\theta)}{3}s(s+1), \tag{A.29}$$

which completes the proof.

References

[1] M. Ardehali. *Phys. Rev. A*, **46**:5375, (1992).

[2] A. Aspect, P. Grangier, and G. Roger. *Phys. Rev. Lett.*, **47**:460, (1981).

[3] A. Aspect, P. Grangier, and G. Roger. *Phys. Rev. Lett.*, **49**:91, (1982).

[4] A. Aspect, P. Grangier, and G. Roger. *Phys. Rev. Lett.*, **49**:1804, (1982).

[5] J.S. Bell. *Physics*, **1**:195, (1964).

[6] J.S. Bell. *Foundations of Quantum Mechanics, Proceedings of the International School of Physics "Enrico Fermi"*. Academic, (1971).

[7] C. Bennett, F. Bessette, G. Brassard, and K. Ekert. *Scientific American*, October:26, (1992).

[8] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. S molin. *Journal of Cryptology*, **5**:3, (1992).

[9] C. Bennett, G. Brassard, and N. Mermin. *The American Physical Society*, **68**:557, (1992).

[10] C.H. Bennett and G. Brassard. *International Conference on Computers, Systems Signal Processing, Bangalore, India, 10-12 December 1984*, page 175, (1984).

[11] R.A. Berltmann and A. Zeilinger. *Quantum [Un]speakables: From Bell to Quantum Information*. Springer, (2002).

[12] D. Bohm. *Quantum Theory*. Prentice-Hall, Inc., Englewood Cliffs, N.J., (1951).

[13] D. Bohm and Y. Aharonov. *Phys. Rev.*, **108**:1070, (1957).

[14] J.F. Clauser and M.A. Horne. *Phys. Rev. D*, **10**:526, (1974).

[15] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. *Phys. Rev. Lett.*, **23**:880, (1969).

[16] J.F. Clauser and A. Shimony. *Rep. Prog. Phys.*, **41**:1881, (1978).

[17] A. Einstein, B. Podolsky, and N. Rosen. *Phys. Rev.*, **47**:777, (1935).

[18] A. Ekert. *Phys. Rev. Lett.*, **67**:661, (1991).

[19] E. Fry, T. Walther, and S. Li. *Phys. Rev. A*, **52**:4381, (1995).

[20] R. Garcia, J. Fiuracek, N. Cerf, J. Wenger, and P. Grangier. *Phys. Rev. Lett.*, 93:130409, (2004).

[21] C. Gerry and P. Knight. *Introductory Quantum Optics*. Press syndicate of the University of Cambridge, (2005).

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. *Reviews of Modern Physics*, **74**:145, (2002).

[23] M. Giustina, S. Mech, A. an Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. Woo Nam, R. Ursin, and A. Zeilinger. *Nature*, **497**:227, (2013).

[24] D.M. Greenberger, M.A. Horne, and A. Zeilinger. *Bell's Theorem, Quantum Theory, and Conceptions of the Universe.* Kluwer Academic, (1989).

[25] D.M. Greenberger, M.A. Horne, A. Zeilinger, and A. Shimony. *Am. J. Phys*, **58**:12, (1990).

[26] D.J. Griffiths. *Introduction to Quantum Mechanics.* Pearson Education, Inc., (1995).

[27] V.S. Mathur and S. Singh. *Concepts in Quantum Mechanics.* Taylor Francis Group, (2009).

[28] N.D. Mermin. *Phys. Rev. D*, **22**:356, (1980).

[29] N.D. Mermin. *Phys. Rev. Lett.*, **15**:1838, (1990).

[30] J.W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger. *Nature*, **403**:515, (2000).

[31] J. Polchinski. *Phys. Rev. Lett.*, **66**:397, (1991).

[32] M.E. Rose. *Elementary Theory of Angular Momentum.* John Wiley Sons, Inc. and Chapman Hall, Ltd., (1957).

[33] J.J. Sakurai and J. Napolitano. *Modern Quantum Mechanics.* Pearson Education, Inc., publishing as Addison-Wesley, (1994).

[34] A. Shields and Z. Yuan. *Physics World*, March:24, (2007).

[35] S. Singh. *The Code Book.* Doubleday, (1999).

[36] S. Weinberg. *Lectures on Quantum echanics.* Cambridge University Press, (2013).

[37] S. Wiesner. *SIGACT News*, **15**:78, (1983).

[38] W. Wootters and W. Zurek. *Nature*, **299**:802, (1982).

[39] X.H. Wu, H.S. Zong, H.R. Pang, and F. Wang. *Phys. Lett. A*, **281**:203, (2001).