Intermediate states in quantum cryptography and Bell inequalities

H. Bechmann-Pasquinucci\textsuperscript{1} and N. Gisin\textsuperscript{2}

\textsuperscript{1}UCCI.IT, via Olmo 26, I-23888 Rovagnate (LC), Italy
\textsuperscript{2}Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland

August 6, 2002

Abstract

Intermediate states are known from intercept/resend eavesdropping in the BB84 quantum cryptographic protocol. But they also play fundamental roles in the optimal eavesdropping strategy on BB84 and in the CHSH inequality. We generalize the intermediate states to arbitrary dimension and consider intercept/resend eavesdropping, optimal eavesdropping on the generalized BB84 protocol and present a generalized CHSH inequality for two entangled quNits based on these states.

1 Introduction

The quantum cryptographic protocol, known as the BB84 [1], was originally developed for qubits. In this protocol the legitimate users, Alice and Bob, both use the same two mutually unbiased bases $A$ and $A'$. Alice use them for state preparation\textsuperscript{1} and Bob chooses between the two bases for his measurement. But an eavesdropper performing the simple intercept/resend eavesdropping, may chose to measure in what is known as the intermediate basis or the Breidbart basis [2]. In the case of qubits it is possible to form four intermediate states, which falls into two mutually unbiased bases. However the eavesdropper need only use one of these bases.

It turns out that it is not only in the simple intercept/resend eavesdropping that these intermediate states appear. Also in the optimal eavesdropping strategy [3, 4], which consists of the eavesdropper using the optimal cloning machine, these states enters. In this case, they appear at the point where Bob and the eavesdropper, Eve, have the same amount of information, i.e. where their information lines cross. At this point their mixed states may be decomposed into a mixture of some of the intermediate states.

That the intermediate states also appear in the optimal eavesdropping strategy, also explains a curious observation. Namely, that the amount of

\textsuperscript{1}Notice that Alice may use a maximally entangled state of two qubits for preparing the state she sends to Bob, since a measurement on one qubit will ‘prepare’ the state of the other qubit.
information obtained by the eavesdropper at the crossing point between the information lines using optimal eavesdropping, and the amount of information she obtains performing intercept/resend eavesdropping in the intermediate basis, is the same. However, the error rates are quite different.

Further more intermediate states reappear in the Clauser-Horne-Shimony-Holt (CHSH) inequality [5] for two entangled qubits. Where the maximal violation is obtained when on the first qubit the measurement settings correspond to the two mutually unbiased bases $A$ and $A'$, and on the second qubit the two intermediate bases. Moreover when introducing the same kind of noise as the eavesdropper does in the optimal eavesdropping strategy, the Bell violation naturally decreases. But it is interesting to notice that for the critical disturbance where the classical limit is reached, Bob and Eve have the same amount of information, i.e. this happens at the crossing point of the information lines. This crossing point between the two information lines is a very important point, since upto this limit Alice and Bob can use the fact that they have more mutual information than the eavesdropper and they can create a secure key just by using classical error correction and one-way privacy amplification. Hence the CHSH inequality for qubits can be used as a security measure [6, 7].

In the three situation just described, intercept/resend eavesdropping, optimal eavesdropping and the CHSH-inequality, the intermediate states keep reappearing and seem to play a fundamental role.

A natural question to ask is 'what happens in higher dimensions?'. This is the question we try to answer, at least partially, here. It is possible to generalize the BB84 protocol to arbitrary dimension [8, 9, 10, 3, 4], simply by adding basis vectors to the two mutually unbiased bases, so that for $N$ dimension each basis contain $N$ vectors. The intermediate states may also be generalized to arbitrary dimensions. However, in higher dimensions they do in general not form bases. But it is possible to associate with each intermediate state a projector, which represents a binary measurement.

With the use of these generalized intermediate states we investigate intercept/resend eavesdropping, optimal eavesdropping and a generalized CHSH inequality in arbitrary dimension to see if they play the same role as in two dimension.

In section 2 we introduce the intermediate states for quNits. In section 3 we shortly discuss intercept/resend eavesdropping using the intermediate states. In section 4 we compare optimal eavesdropping with the intercept/resend eavesdropping strategy. Then in section 5 we present a generalized Bell inequality for two entangled quNits. In section 6 we consider the Bell violation as a function of the disturbance the optimal eavesdropping strategy would lead to. The last sections of the paper is devoted to a study of the inequality we have presented. In section 7 we discuss some features of the inequality by giving examples in three dimensions. Since recently the strength of a Bell inequality has been measured in terms of its resistance to noise we discuss this issue in section 8. Section 9 is devoted to a brief study of the required detection efficiency. Finally in section 10 we have conclusion and discussion.
2 The intermediate states

The quantum cryptographic protocol BB84 can easily be generalized to arbitrary dimension, this has already been discussed in the literature [8, 10]. The protocol works in exactly the same way as for qubits with the sole exception that for quNits each of the two mutually unbiased bases $A$ and $A'$ used by Alice and Bob contain $N$ basis states instead of two. So that Alice sends at random (and with equal probability) one of the $2N$ possible states and Bob choses to measure in one of the two bases $A$ and $A'$.

In this section we define the intermediate states between these two bases. The basis $A$ is chosen as the computational basis,

$$|a_0\rangle, \ldots, |a_{N-1}\rangle,$$

(1)

and the second basis, $A'$, is the Fourier transform of the computational basis:

$$|a'_k\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \exp\left(\frac{2\pi i k n}{N}\right) |a_n\rangle$$

(2)

These two bases are mutually unbiased, i.e.

$$\langle a_n | a'_k \rangle = \frac{\exp\left(\frac{2\pi i k n}{N}\right)}{\sqrt{N}}$$

(3)

This means that the distance between pairs of state from the two bases is $\cos(\theta) = 1/\sqrt{N}$.

Having two states, it is possible to define a state which lies exactly in between the two, which means that it has the same overlap with both states and it is the state closest to the two original states which has this property. The intermediate state are obtained by forming all possible pairs of the states from the two bases. They are shown in the table below:

<table>
<thead>
<tr>
<th></th>
<th>$a'_0$</th>
<th>$a'_1$</th>
<th>$\cdots$</th>
<th>$a'_{N-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_0$</td>
<td>$m_{00}$</td>
<td>$m_{01}$</td>
<td>$\cdots$</td>
<td>$m_{0,N-1}$</td>
</tr>
<tr>
<td>$a_1$</td>
<td>$m_{10}$</td>
<td>$m_{11}$</td>
<td>$\cdots$</td>
<td>$m_{1,N-1}$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\cdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$a_{N-1}$</td>
<td>$m_{N-1,0}$</td>
<td>$m_{N-1,1}$</td>
<td>$\cdots$</td>
<td>$m_{N-1,N-1}$</td>
</tr>
</tbody>
</table>

Explicitly the intermediate state between $|a_n\rangle$ and $|a'_k\rangle$ is defined in the following way

$$|m_{nk}\rangle = \frac{1}{C} \left[ \exp\left(\frac{2\pi i k n}{N}\right) |a_n\rangle + |a'_k\rangle \right]$$

(4)

where $C = 2(1 + 1/\sqrt{N})$ is the normalization constant and the phase comes from the overlap between $|a_n\rangle$ and $|a'_k\rangle$, see eq.(3). The index of the $m$-states are such that the first index always refers to the $A$ and the second to the $A'$-basis. Since each basis contains $N$ states it is possible to form $N^2$ intermediate states, simply by forming all pairs of states from the two bases.
In general the intermediate state \( |m_{\alpha\beta} \rangle \) between two arbitrary initial states \( |\alpha \rangle \) and \( |\beta \rangle \) is defined as
\[
|m_{\alpha\beta} \rangle = \frac{\sqrt{\langle \alpha |\beta \rangle} |\alpha \rangle + \sqrt{\langle \beta |\alpha \rangle} |\beta \rangle}{\sqrt{2}\sqrt{|\langle \alpha |\beta \rangle| + |\langle \beta |\alpha \rangle|^2}}
\] (5)

The intermediate states may be defined in complete generality for arbitrary initial states and any number of them. In this case the intermediate state is found by forming the mixture of all the initial states with equal weight, the eigenstate state with the largest eigenvalue of this mixture corresponds to the intermediate state. Naturally these definitions are equivalent and lead to the same intermediate state.

Considering the intermediate states leads to the following conditional probabilities
\[
p(m_{nk}|a_n) = p(m_{nk}|a'_k) = \frac{1 + \frac{1}{\sqrt{N}}}{2} \equiv F
\] (6)

Notice that this definition indeed recover the formula for cosine of half the angle: \( \cos(\theta/2) = \sqrt{\frac{1 + \cos(\theta)}{2}} \). This is why the states have been named intermediate states, since they indeed lie in between the the two original states.

Whereas the probability for making an error is
\[
p(m_{nk}|a_q) = p(m_{nk}|a'_p) = \frac{1 - \frac{1}{\sqrt{N}}}{2(N-1)} \equiv \frac{D}{N-1}
\] (7)

It is important to notice that the intermediates states in general not are orthogonal, indeed
\[
\langle m_{kl} | m_{nm} \rangle = \frac{1}{\sqrt{NC}} \left[ \sqrt{N} \delta_{kn} \exp \left( \frac{2\pi i}{N} (mn - lk) \right) \right. 
+ \sqrt{N} \delta_{lm} + \exp \left( \frac{2\pi i}{N} (m - l)k \right) + \exp \left( \frac{2\pi i}{N} (m - l)n \right) \bigg] \] (8)

This means that the generalized intermediate states do in general not form bases as in the two dimensional case. But they can still be used as binary measurements, this is discussed in the next section.

### 2.1 Intermediate states as binary measurements

It has just been shown that in general the intermediate states \( |m_{kl} \rangle \) are not orthogonal, and hence they do not form bases as in the two dimensional case. It is however possible to use the corresponding projectors, \( |m_{kl} \rangle \langle m_{kl}| \) as binary measurements.

Since the intermediate states are non-orthogonal, it means that the corresponding binary measurements are mutually incompatible. In other words, none of them can be measured together but they have to be measured one by one. A binary measurement, has as the name indicates two possible outcomes, 0 and 1. Where the zero outcome is interpreted as 'I guess the state was not \( |m_{kl} \rangle \)', and the '1' outcome is interpreted as 'I guess the state was \( |m_{kl} \rangle \)'. However, the answers are statistical, in the sense that there is a certain probability for making the wrong identification.
It should be mentioned that the \( N^2 \) intermediate states constitutes a generalized measurement namely a so called POVM. We have

\[
\sum_{n,k=0}^{N-1} \frac{1}{N} |m_{nk}\rangle\langle m_{nk}| = \mathbb{I} \tag{9}
\]

However, we do not make use of this in what follows.

### 3 Intercept/resend eavesdropping

Suppose that the eavesdropper, Eve, performs the simple intercept/resend eavesdropping. This means that she intercepts the particle send by Alice, performs a measurement and according to the result prepares a particle which she then sends to Bob. She may choose to measure in the same bases as Alice and Bob, but she may also choose to use the intermediate states. In higher dimensions where the intermediate states do not form bases, this strategy becomes a bit artificial. It is nevertheless interesting to consider it briefly.

In arbitrary dimension where the intermediate states corresponds to binary measurements, the intercept/resend strategy using these measurements may look like this: When ever Eve obtains a '1', which means she can make a good guess of the state, she prepares a new state and sends it to Bob. Whereas in the cases where she gets a '0', which means she is unable to make a good guess, she does not send anything to Bob. In this way we are only considering the cases where Eve does obtain a useful answer. This strategy, of course, gives rise to a huge amount of losses and errors on Bobs side, but it is however interesting to evaluate the amount of information that Eve obtains in this case, i.e. considering only the measurements where she gets a positive answer.

The probability of making the correct identification is given by eq.(6) and is equal to \( \frac{1}{2} + \frac{1}{2\sqrt{N}} \). Whereas the probability of wrong identification, i.e. of an error is given by eq.(7) and is equal to \( \frac{1}{(N-1)} \left( \frac{1}{2} - \frac{1}{2\sqrt{N}} \right) \). This means that the (Shannon) information obtained by Eve is given by \([10]\)

\[
I_{\text{int,Eve}}^N = \log_2(N) + \left( \frac{1}{2} + \frac{1}{2\sqrt{N}} \right) \log_2 \left( \frac{1}{2} + \frac{1}{2\sqrt{N}} \right) \\
+ \left( \frac{1}{2} - \frac{1}{2\sqrt{N}} \right) \log_2 \left( \frac{1}{(N-1)} \left( \frac{1}{2} - \frac{1}{2\sqrt{N}} \right) \right) \tag{10}
\]

on the '1' outcomes of her measurements.

In the next section we will compare this amount of information to the amount of information obtained performing optimal eavesdropping at the point where the information lines between Bob and Eve cross.

### 4 The optimal cloning machine

The optimal eavesdropping strategy in any dimension, is believed to be given by a asymmetric version of the quantum cloning machine \([11]\) which clones optimally the two mutually unbiased bases \([4]\). Using this cloner, Eve can obtain two copies of different fidelity of the state prepared by Alice. Usually Eve
keeps the bad copy and sends the good one on to Bob. For a full description of how this eavesdropping strategy and of the cloning machine involved, see [4]. Here we are only concerned with the final state that Bob receives, which means how the optimal eavesdropping strategy influence the state obtained by Bob. In the case of no eavesdropping Bob receives the same pure state as was send by Alice. But in the case of eavesdropping Bob receives a mixed state.

Assume that without eavesdropping Bob would have found the state \( |a_n \rangle \) if measuring in the computational basis. The question is what happens to \( |a_n \rangle \) as a result of the eavesdropping? Or in other words, how does the cloning machine influence the state \( |a_n \rangle \)? We are only interested in the final mixed state Bob receives, and that may be written as

\[
\rho_B = F_B |a_n \rangle \langle a_n | + \frac{D_B}{N-1} \sum_{j=0, j \neq n}^{N-1} |a_j \rangle \langle a_j | \tag{11}
\]

where \( F_B \) is the fidelity and \( D_B = 1 - F_B \) is the total disturbance. A similar expressing can be obtained for the \( A' \) basis states. As a result of the eavesdropping the amount of information that Bob gets is

\[
I_{opt,bob}^N = \log_2(N) + F_B \log_2(F_B) + (1 - F_B) \log_2 \left( \frac{1 - F_B}{N-1} \right) \tag{12}
\]

The optimal eavesdropping strategy is symmetric under the exchange of Bob and Eve. This means that the mixed state, \( \rho_E \), which Eve obtains can be written on the same form as Bob’s mixed state, just with different coefficients, i.e.

\[
\rho_E = F_E |a_n \rangle \langle a_n | + \frac{D_E}{N-1} \sum_{j=0, j \neq n}^{N-1} |a_j \rangle \langle a_j | \tag{13}
\]

And equivalently the amount of information obtained by Eve is given by

\[
I_{opt, eve}^N = \log_2(N) + F_E \log_2(F_E) + (1 - F_E) \log_2 \left( \frac{1 - F_E}{N-1} \right) \tag{14}
\]

It is interesting and important to consider the point where the information lines between Bob and Eve cross. Since when Alice and Bob share more information that Alice and Eve, Alice and Bob can use one-way privacy amplification to obtain a secret key. Using the explicit form and coefficients of the cloning machine it is possible to show (this was done in [4]) that the information curves cross at the point where

\[
F_B = F_E = F = \frac{1}{2} + \frac{1}{2 \sqrt{N}} \tag{15}
\]

\[
D_B = D_E = D = \frac{1}{2} - \frac{1}{2 \sqrt{N}} \tag{16}
\]

This is exactly the same fidelity (or probability of guessing correctly the state) that Eve obtained using the intercept/resend eavesdropping using the intermediate states. Which means that we have just shown that

\[
I_{int, eve}^N = I_{opt, eve}^N \text{(crossing point)} \tag{17}
\]
This is explained by the fact that, at the crossing point of the information lines, Eve’s mixed state can be decomposed into a mixture of some of the intermediate states, namely

\[
\rho_E^{\text{cross}} = \frac{1}{N} \sum_{j=0}^{N-1} |m_{nj}\rangle\langle m_{nj}| \tag{18}
\]

where again it has been assumed that |a_n\rangle was the correct state. The same result holds for Bob, since at the crossing point Bob and Eve possess the same mixed state.

The mixture of the intermediate states may be interpreted as if Eve with probability \(1/N\) has the state |m_{nj}\rangle (there are \(N\) possible values of \(j\)). Eve, naturally, waits and performs her measurement after Alice has revealed in which basis the quNit was originally prepared. Then she measures her quNit in the same basis, which means that she uses either the basis \(A\) or \(A'\).

Which means that the situation is the following: For the optimal eavesdropping strategy, Eve possesses one of the intermediate states and she measures in one of the corresponding basis \(A\) or \(A'\). Whereas in the intercept/resent eavesdropping with the intermediate states, the situation is exactly the opposite namely, Eve has one of the basis states from \(A\) or \(A'\) and she measures the intermediate states. The two situations obviously lead to the same probabilities and hence the same amount of information.

5 The Bell inequality in arbitrary dimension

Recently there has been a big interest in generalizing various type of Bell inequalities [12], [13]-[18] in higher dimension. The Bell inequality we present here [19] makes use of the intermediate states, in a way similar to the CHSH inequality. This means that first we present the measurements and the quantum limit and only afterwards the local variable bound. So at first we just write down a particular sum of joint probabilities.

5.1 The Bell inequality: The quantum mechanical limit

Suppose that Alice and Bob share many maximally entangled state of two quNits. In the computational basis this state may be written as

\[
|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |a_i, a_i\rangle \tag{19}
\]

For each of her quNits Alice has the choice of two measurements, namely to measure the basis \(A\) or the basis \(A'\). Whereas Bob for each of his quNits has the choice between \(N^2\) binary measurements, corresponding to all the intermediate states of the two bases used by Alice.

In order to write down the Bell inequality, it is convenient to assign values to the various states. In the table below is shown the values:
Notice that intermediate states have been organized into $N$ sets so that the value of the state is always given by the first index. Moreover this organization into the sets $M_0, \ldots, M_{N-1}$, simplifies the notation in what follows. However, it is important to remember that the states in each of the sets are not orthogonal, in other words they do not form $N$ orthogonal bases.

The inequality is a sum of joint probabilities. And it is obtained by summing all the probabilities for when the results of the measurements are correlated and from this sum subtract all the probabilities when the results are not correlated, i.e.

$$B_N = \sum p(\text{results correlated}) - \sum p(\text{results not correlated})$$

Suppose that Alice measures in the $A$ basis and Bob measures the projectors in the set $M_0$. For this combination of measurements, there are the following contributions to the sum $B_N$:

$$P(M_0 = A) = \sum_{i=0}^{N-1} p(m_{ii} \cap a_i) = \frac{1}{2} + \frac{1}{2\sqrt{N}}$$

$$P(M_0 \neq A) = \sum_{i,j=0, j \neq i}^{N-1} p(m_{ii} \cap a_j) = \frac{1}{2} - \frac{1}{2\sqrt{N}}$$

Where $P(M_0 = A)$ should be read as follows: Bob measures one of the projectors in $M_0$ and Alice measures $A$, and Bob obtains the value which is correlated with Alice’s result. On the other hand $P(M_0 \neq A)$ means that Bob’s result is not correlated with the result obtained by Alice. The probability $p(m_{kl} \cap a_n) = p(m_{kl} | a_n)p(a_n)$ is the joint probability for obtaining both $|a_n\rangle$ and $|m_{kl}\rangle$.

The same is the case if Bob measures the projectors in any of the other sets $M_1, \ldots, M_{N-1}$ and Alice always measures in $A$. And again if Bob uses $M_0$ and Alice $A'$. Which means we have $P(M_i = A) = P(M_0 = A') = \frac{1}{2} + \frac{1}{2\sqrt{N}}$ and $P(M_i \neq A) = P(M_0 \neq A') = \frac{1}{2} - \frac{1}{2\sqrt{N}}$.

Now consider the case where Bob uses $M_1$ and Alice $A'$, in this case Bob consistently finds a value which is $N-1$ higher than the value which correlates him with Alice. To see this, assume for example that Bob has the state $|a_0\rangle$ which is assigned the value 0. But the state in $M_1$ which gives the correct identification of this state is $|m_{N-1,0}\rangle$, but this state has been assigned the value $N-1$. Similar for all the other states, which leads to $P(M_1 = A'+(N-1)) = \frac{1}{2} + \frac{1}{2\sqrt{N}}$ and $P(M_1 \neq A'+(N-1)) = \frac{1}{2} - \frac{1}{2\sqrt{N}}$. Actually, when ever Alice measures $A'$ and Bob uses any of the $M_i$, Bob consistently finds a value which
is $N - i$ higher than the one which correlates him with Alice. This means that $P(M_i = A' + (N - i)) = \frac{1}{2} + \frac{1}{2\sqrt{N}}$ and $P(M_i \neq A' + (N - i)) = \frac{1}{2} - \frac{1}{2\sqrt{N}}$.

It is now possible to write and evaluate the sum $B_N$

\[
B_N = \sum_{i=0}^{N-1} P(M_i = A) - \sum_{i=0}^{N-1} P(M_i \neq A) + \sum_{i=0}^{N-1} P(M_i = A' + (N - i)) - \sum_{i=0}^{N-1} P(M_i \neq A' + (N - i))
\]

\[
= 2N \left( \left( \frac{1}{2} + \frac{1}{2\sqrt{N}} \right) - \left( \frac{1}{2} - \frac{1}{2\sqrt{N}} \right) \right)
\]

\[
= 2\sqrt{N}
\]

(22)

The quantity $B_N$ is a sum of $2N \times N^2$ terms if written out explicitly. In the next section we show that a local variable model which tries to attribute definite values to the observables will reach a maximum value of 2. This shows that we have obtained a Bell inequality where the quantum violation grows with the squareroot of $N$.

### 5.2 The Bell inequality: the local variable limit

On Alice’s side $a_0, \ldots, a_{N-1}$ are measured simultaneously in a single measurement as the basis $A$, which means that only one of them can come out true in a local variable model. The same is the case for $a'_0, \ldots, a'_{N-1}$ which is measured as the basis $A'$. This means that, for example, if $a_i$ is true, meaning that the measurement of $A$ will result in the outcome $a_i$, then all probabilities involving $a_j$ with $j \neq i$ must be zero. It is different on Bob’s side where each $m_{kl}$ is measured independently and hence they may all be true at the same time in a local variable model.

Assume now that according to some local variable model $a_i$ and $a'_j$ are true. At the same time, in principle, all the $m_{kl}$ could be true too. But notice now that the only $m$-state which will give a positive contribution to the quantity $B_N$ is the one which identifies both $a_i$ and $a'_j$ correctly, i.e. $m_{ij}$. This will give rise to a contribution of $+2$. Whereas $m_{ij}$ and $m_{kj}$ where only one index is correct, will only identify of the states correctly and the other one wrong. This means that these states, since this gives rise to one correct and one wrong identification, will result in a zero contribution. And finally the states $m_{kl}$ where both indices are wrong will only give rise to errors and will hence give a negative contribution of $-2$ to the sum $B_N$. Which means that

\[
B_N \leq 2
\]

(23)

However, we have already shown that quantum mechanically it is possible to violate this limit. Quantum mechanically the limit is $2\sqrt{N}$. This means that we have obtained a Bell inequality where the violation increases with the squareroot of the dimension.

For $N=3$, the inequality has been checked in various ways numerically. First of all it has been checked that $2\sqrt{3}$ is indeed the quantum mechanical limit to this sum of probabilities and that this maximum is reached for the
maximally entangled state. Moreover, it has been checked using "polytope software" [13, 20] that the inequality eq.(23) is optimal for the measurement settings which we have presented here.

6 Bell parameter as a function of \( \rho_B \)

In this section we investigate how the Bell violation decreases as a function of the disturbance introduced by the eavesdropper. It is not necessary to think of it in terms of quantum cryptography and eavesdropping, but simply that the quantum channel from Alice to Bob is noisy and that the noise which is introduced is identical to the noise an eavesdropper using the optimal cloning machine would introduce.

Assume, without loss of generality, that without disturbance, Bob would have received the state \( |a_0\rangle \), then we know that the mixed state that he obtains as a function of the disturbance can be written eq.(11)

\[
\rho_B = F_B |a_0\rangle\langle a_0| + \frac{D_B}{N-1} \sum_{i=1}^{N-1} |a_i\rangle\langle a_i|
\]

In order to compute \( S(\rho_B) \) it is enough to consider the case where Bob for example use the states in \( M_0 \) for his measurements, the rest of the terms in the inequality follows by symmetry.

All the states in the \( M_0 \) set are of the form \( |m_{jj}\rangle \). First computing the various probabilities \( \langle m_{jj} | \rho_B | m_{jj}\rangle \), we find

\[
\langle m_{jj} | \rho_B | m_{jj}\rangle = F_B \langle m_{jj} | a_0\rangle\langle a_0 | m_{jj}\rangle + \frac{D_B}{N-1} \sum_{i=1}^{N-1} \langle m_{jj} | a_i\rangle\langle a_i | m_{jj}\rangle
\]

There are two different cases which have to be checked independently, namely \( j = 0 \) and \( j \neq 0 \):

For \( j = 0 \) we have

\[
\langle m_{00} | \rho_B | m_{00}\rangle = F_B F + (N-1) \frac{D_B}{N-1} \frac{D}{N-1} \tag{25}
\]

and for \( j \neq 0 \) we have

\[
\langle m_{jj} | \rho_B | m_{jj}\rangle_{j \neq 0} = F_B \frac{D}{N-1} + F \frac{D_B}{N-1} + (N-2) \frac{D_B}{N-1} \frac{D}{N-1} \tag{26}
\]

Where we have used that \( p(m_{00}|a_0) = F \) and \( p(m_{jj}|a_0)_{j \neq 0} = \frac{D}{N-1} \), see eq.(6) and eq.(7).

In the inequality \( \langle m_{00} | \rho_B | m_{00}\rangle \) appears with a plus sign, since this is the probability of correctly identifying the state. At the same time \( \langle m_{jj} | \rho_B | m_{jj}\rangle_{j \neq 0} \) appears \( N-1 \) times with a minus sign in the inequality, since these correspond to all the possible errors. This means that we can define

\[
s(\rho) = \langle m_{00} | \rho_B | m_{00}\rangle - (N-1) \langle m_{jj} | \rho_B | m_{jj}\rangle_{j \neq 0}
\]

\[
= F_B(F - D) - FD_B - \frac{N-3}{N-1} DD_B \tag{27}
\]