UvA-DARE (Digital Academic Repository)

Cryptography in a quantum world
Wehner, S.D.C.

Link to publication

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Locking classical correlations in quantum states [DHL+04] is an exciting feature of quantum information, intricately related to entropic uncertainty relations. In this chapter, we will investigate whether good locking effects can be obtained using mutually unbiased bases.

5.1 Introduction

Consider a two-party protocol with one or more rounds of communication. Intuitively, one would expect that in each round the amount of correlation between the two parties cannot increase by much more than the amount of data transmitted. For example, transmitting $2\ell$ classical bits or $\ell$ qubits (and using superdense coding) should not increase the amount of correlation by more than $2\ell$ bits, no matter what the initial state of the two-party system was. This intuition is accurate when we take the classical mutual information $I_C$ as our correlation measure, and require all communication to be classical. However, when quantum communication was possible at some point during the protocol, everything changes: there exist two-party mixed quantum states, such that transmitting just a single extra bit of classical communication can result in an arbitrarily large increase in $I_C$ [DHL+04]. The magnitude of this increase thereby only depends on the dimension of the initial mixed state. Since then similar locking effects have been observed, also for other correlation measures [CW05b, HHHO05]. Such effects play a role in very different scenarios: they have been used to explain physical phenomena related to black holes [SO06], but they are also important in cryptographic applications such as quantum key distribution [KRBM07] and quantum bit string commitment that we will encounter in Chapter 10. We are thus interested in determining how exactly we can obtain locking effects, and how dramatic they can be.
5.1.1 A locking protocol

The correlation measure considered here, is the classical mutual information of a bipartite quantum state $\rho_{AB}$, which is the maximum classical mutual information that can be obtained by local measurements $M_A \otimes M_B$ on the state $\rho_{AB}$ (see Chapter 2):

$$I_c(\rho_{AB}) = \max_{M_A \otimes M_B} I(A,B). \tag{5.1}$$

Recall from Chapter 2 that the mutual information is defined as $I(A,B) = H(P_A) + H(P_B) - H(P_{AB})$ where $H$ is the Shannon entropy. $P_A$, $P_B$, and $P_{AB}$ are the probability distributions corresponding to the individual and joint outcomes of measuring the state $\rho_{AB}$ with $M_A \otimes M_B$. The mutual information between $A$ and $B$ is a measure of the information that $B$ contains about $A$. This measure of correlation is of particular relevance for quantum bit string commitments in Chapter 10. Furthermore, the first locking effect was observed for this quantity in the following protocol between two parties: Alice (A) and Bob (B). Let $B = \{B_1, \ldots, B_m\}$ with $B_t = \{|b_1^t\}, \ldots, |b_d^t\}$ be a set of $m$ MUBs in $\mathbb{C}^d$. Alice picks an element $k \in \{1, \ldots, d\}$ and a basis $B_t \in B$ uniformly at random. She then sends $|b_k^t\rangle$ to Bob, while keeping $t$ secret. Such a protocol gives rise to the joint state

$$\rho_{AB} = \frac{1}{md} \sum_{k=1}^d \sum_{t=1}^m (|k\rangle\langle k| \otimes |t\rangle\langle t|)_A \otimes (|b_k^t\rangle\langle b_k^t|)_{B}. $$

Clearly, if Alice told her basis choice $t$ to Bob, he could measure in the right basis and obtain the correct $k$. Alice and Bob would then share log $d + \log m$ bits of correlation, which is also their mutual information $I_c(\sigma_{AB})$, where $\sigma_{AB}$ is the state obtained from $\rho_{AB}$ after the announcement of $t$. But, how large is $I_c(\rho_{AB})$, when Alice does not announce $t$ to Bob? It was shown [DHL+04] that in dimension $d = 2^n$, using the two MUBs given by the unitaries $U_+ = \mathbb{I}^\otimes n$ and $U_x = H^\otimes n$ applied to the computational basis we have $I_c(\rho_{AB}) = (1/2) \log d$ (see Figure 5.1, where $|x_k\rangle = U_k|x\rangle$). This means that the single bit of basis information Alice transmits to Bob “unlocks” $(1/2) \log d$ bits: without this bit, the mutual information is $(1/2) \log d$, but with this bit it is log $d + 1$. To get a good locking protocol, we want to use only a small number of bases, i.e., $m$ should be as small as possible, while at the same time forcing $I_c(\rho_{AB})$ to be as high as possible. That is, we want $\log m/(\log d - I_c(\rho_{AB}))$ to be small.

It is also known that if Alice and Bob randomly choose a large set of unitaries from the Haar measure to construct $B$, then $I_c(\rho_{AB})$ can be brought down to a small constant [HLSW04]. However, no explicit constructions with more than two bases are known that give good locking effects. Based on numerical studies for spaces of prime dimension $3 \leq d \leq 30$, one might hope that adding a third MUB would strengthen the locking effect and give $I_c(\rho_{AB}) \approx (1/3) \log d$ [DHL+04].

Here, however, we show that this intuition fails us. We prove that for three MUBs given by $\mathbb{I}^\otimes n$, $H^\otimes n$, and $K^\otimes n$ where $K = (\mathbb{I} + i\sigma_z)/\sqrt{2}$ and dimension
5.1 Introduction

1: choose \( x \in \{0,1\}^n, b \in \{+,x\} \)

2: \( |xb\rangle \)

3: \( b \)

\[ I_c(\rho_{AB}) = \frac{n}{2} \]

\[ I_c(\sigma_{AB}) = n + 1 \]

Figure 5.1: A locking protocol for 2 bases.

d = 2^n for some even integer \( n \), we have

\[ I_c(\rho_{AB}) = \frac{1}{2} \log d, \]  

(5.2)

the same locking effect as with two MUBs. We also show that for any subset of the MUBs based on Latin squares and the MUBs in square dimensions based on generalized Pauli matrices [BBRV02], we again obtain Eq. (5.2), i.e., using two or all \( \sqrt{d} \) of them makes no difference at all! Finally, we show that for any set of MUBs \( \mathbb{B} \) based on generalized Pauli matrices in any dimension, \( I_c(\rho_{AB}) = \log d - \min_\phi (1/|\mathbb{B}|) \sum_{B \in \mathbb{B}} H(\mathbb{B}||\phi), \) i.e., it is enough to determine a bound on the entropic uncertainty relation to determine the strength of the locking effect. Although bounds for general MUBs still elude us, our results show that merely choosing the bases to be mutually unbiased is not sufficient and we must look elsewhere to find bases which provide good locking.

5.1.2 Locking and uncertainty relations

We first explain the connection between locking and entropic uncertainty relations. In particular, we will see that for MUBs based on generalized Pauli matrices, we only need to look at such uncertainty relations to determine the exact strength of the locking effect.

In order to determine how large the locking effect is for some set of mutually unbiased bases \( \mathbb{B} \), and the shared state

\[ \rho_{AB} = \sum_{k=1}^{d} p_{t,k} (|k\rangle \otimes |t\rangle) A \otimes (|b_k^t\rangle \langle b_k^t|) B, \]  

(5.3)

we must find the value of \( I_c(\rho_{AB}) \) or at least a good upper bound. That is, we must find a POVM \( M_A \otimes M_B \) that maximizes Eq. (5.1). Here, \( \{p_{t,k}\} \) is a probability distribution over \( \mathbb{B} \times [d] \). It has been shown in [DHL+04] that we can
restrict ourselves to taking $M_A$ to be the local measurement determined by the projectors $\{ |k\rangle\langle k| \otimes |t\rangle\langle t| \}$. It is also known that we can limit ourselves to take the measurement $M_B$ consisting of rank one elements $\{ \alpha_i |\Phi_i\rangle \langle \Phi_i| \}$ only [Dav78], where $\alpha_i \geq 0$ and $|\Phi_i\rangle$ is normalized. Maximizing over $M_B$ then corresponds to maximizing Bob’s accessible information as defined in Chapter 2 for the ensemble $E = \{ p_{k,t}, |b^t_k\rangle\langle b^t_k| \}$

$$I_{\text{acc}}(E) = \max_{M_B} \left( -\sum_{k,t} p_{k,t} \log p_{k,t} + \sum_i \sum_{k,t} p_{k,t} \alpha_i \langle \Phi_i | \rho_{k,t} | \Phi_i \rangle \log \frac{p_{k,t} \langle \Phi_i | \rho_{k,t} | \Phi_i \rangle}{\langle \Phi_i | \mu | \Phi_i \rangle} \right), \quad (5.4)$$

where $\mu = \sum_{k,t} p_{k,t} \rho_{k,t}$ and $\rho_{k,t} = |b^t_k\rangle\langle b^t_k|$. Therefore, we have $I_c(\rho_{AB}) = I_{\text{acc}}(E)$. As we saw in Chapter 2, maximizing the accessible information is often a very hard task. Nevertheless, for our choice of MUBs, the problem will turn out to be quite easy in the end.

### 5.2 Locking using mutually unbiased bases

#### 5.2.1 An example

We now determine how well we can lock information using specific sets of mutually unbiased bases. We first consider a very simple example with only three MUBs that provides the intuition behind the remainder of our proof. The three MUBs we consider now are generated by the unitaries $I$, $H$ and $K = (I + i\sigma_x)/\sqrt{2}$ when applied to the computational basis. For this small example, we also investigate the role of the prior over the bases and the encoded basis elements. It turns out that this does not affect the strength of the locking effect positively, i.e., we do not obtain a stronger locking affect using a non-uniform prior. Actually, it is possible to show the same for encodings in many other bases. However, we do not consider this case in full generality as to not obscure our main line of argument.

#### 5.2.1. Lemma

Let $U_1 = I^n$, $U_2 = H^n$, and $U_3 = K^n$, and take $k \in \{0, 1\}^n$ where $n$ is an even integer. Let $\{ p_t \}$ with $t \in [3]$ be a probability distribution over the set $S = \{ U_1, U_2, U_3 \}$. Suppose that $p_1, p_2, p_3 \leq 1/2$ and let $\{ p_{t,k} \}$ with $p_{t,k} = p_t/d$ be the joint distribution over $S \times \{0, 1\}^n$. Consider the ensemble $E = \{ p_{1/3}^{1}, U_1 |k\rangle\langle k| U_1^\dagger \}$, then

$$I_{\text{acc}}(E) = \frac{n}{2}. \quad (5.5)$$

If, on the other hand, there exists a $t \in [3]$ such that $p_t > 1/2$, then $I_{\text{acc}}(E) > n/2$.

**Proof.** We first give an explicit measurement strategy and then prove a matching upper bound on $I_{\text{acc}}$. Consider the Bell basis vectors $|\Gamma_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$,
5.2. Locking using mutually unbiased bases

\[ |\Gamma_{01}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}, \quad |\Gamma_{10}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}, \quad \text{and} \quad |\Gamma_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}. \]

Note that we can write for the computational basis

\[ |00\rangle = \frac{1}{\sqrt{2}}(|\Gamma_{00}\rangle + |\Gamma_{01}\rangle), \]

\[ |01\rangle = \frac{1}{\sqrt{2}}(|\Gamma_{10}\rangle + |\Gamma_{11}\rangle), \]

\[ |10\rangle = \frac{1}{\sqrt{2}}(|\Gamma_{10}\rangle - |\Gamma_{11}\rangle), \]

\[ |11\rangle = \frac{1}{\sqrt{2}}(|\Gamma_{00}\rangle - |\Gamma_{01}\rangle). \]

The crucial fact to note is that if we fix some \( k_1, k_2 \), then there exist exactly two Bell basis vectors \(|\Gamma_{i_1i_2}\rangle\) such that \( |\langle \Gamma_{i_1i_2}|k_1, k_2\rangle|^2 = 1/2 \). For the remaining two basis vectors the inner product with \(|k_1, k_2\rangle\) will be zero. A simple calculation shows that we can express the two-qubit basis states of the other two mutually unbiased bases analogously: for each two qubit basis state there are exactly two Bell basis vectors such that the inner product is zero and for the other two the inner product squared is 1/2.

We now take the measurement given by \( \{ |\Gamma_i\rangle\langle \Gamma_i| \} \) with \( |\Gamma_i\rangle = |\Gamma_{i_1i_2}\rangle \otimes \ldots \otimes |\Gamma_{i_{n-1}i_n}\rangle \) for the binary expansion of \( i = i_1i_2\ldots i_n \). Fix a \( k = k_1k_2\ldots k_n \). By the above argument, there exist exactly \( 2^{n/2} \) strings \( i \in \{0,1\}^n \) such that \( |\langle \Gamma_i|k\rangle|^2 = 1/2^{n/2} \). Putting everything together, Eq. (5.4) now gives us for any prior distribution \( \{p_t,k\} \) that

\[ - \sum_i \langle \Gamma_i|\mu\rangle \log \langle \Gamma_i|\mu\rangle - \frac{n}{2} \leq \mathcal{I}_{\text{acc}}(\mathcal{E}). \tag{5.5} \]

For our particular distribution we have \( \mu = I/d \) and thus

\[ \frac{n}{2} \leq \mathcal{I}_{\text{acc}}(\mathcal{E}). \]

We now prove a matching upper bound that shows that our measurement is optimal. For our distribution, we can rewrite Eq. (5.4) for the POVM given by \( \{\alpha_i|\Phi_i\rangle\langle \Phi_i|\} \) to

\[ \mathcal{I}_{\text{acc}}(\mathcal{E}) = \max_M \left( \log d + \sum_i \frac{\alpha_i}{d} \sum_{k,t} p_t |\langle \Phi_i|U_t|k\rangle|^2 \log |\langle \Phi_i|U_t|k\rangle|^2 \right) \]

\[ = \max_M \left( \log d - \sum_i \frac{\alpha_i}{d} \sum_{t} p_t H(B_t||\Phi_i)) \right), \]

for the bases \( B_t = \{U_t|k\rangle \mid k \in \{0,1\}^n \}. \)
It follows from Corollary 4.2.2 that $\forall i \in \{0, 1\}^n$ and $p_1, p_2, p_3 \leq 1/2$
\[
(1/2 - p_1)[H(\mathcal{B}_2||\Phi_i)] + H(\mathcal{B}_3||\Phi_i)] + \n(1/2 - p_2)[H(\mathcal{B}_1||\Phi_i)] + H(\mathcal{B}_3||\Phi_i)] + \n(1/2 - p_3)[H(\mathcal{B}_1||\Phi_i)] + H(\mathcal{B}_2||\Phi_i)] \geq n/2,
\]
where we used the fact that $p_1 + p_2 + p_3 = 1$. Reordering the terms we now get $\sum_{t=1}^{3} p_t H(\mathcal{B}_t||\Phi_i)) \geq n/2$. Putting things together and using the fact that $\sum_i \alpha_i = d$, we obtain
\[
\mathcal{I}_{acc}(\mathcal{E}) \leq \frac{n}{2},
\]
from which the result follows.

If, on the other hand, there exists a $t \in [3]$ such that $p_t > 1/2$, then by measuring in the basis $\mathcal{B}_t$ we obtain $\mathcal{I}_{acc}(\mathcal{E}) \geq p_t n > n/2$, since the entropy will be 0 for basis $\mathcal{B}_t$ and we have $\sum_t p_t = 1$. \qed

Above, we have only considered a non-uniform prior over the set of bases. In Chapter 3, we observed that when we want to guess the XOR of a string of length 2 encoded in one (unknown to us) of these three bases, the uniform prior on the strings is not the one that gives the smallest probability of success. This might lead one to think that a similar phenomenon could be observed in the present setting, i.e., that one might obtain better locking with three basis for a non-uniform prior on the strings. In what follows, however, we show that this is not the case.

Let $p_t = \sum_k p_{k,t}$ be the marginal distribution on the basis, then the difference in Bob’s knowledge between receiving only the quantum state and receiving the quantum state and the basis information, where we will ignore the basis information itself, is given by
\[
\Delta(p_{k,t}) = H(p_{k,t}) - \mathcal{I}_{acc}(\mathcal{E}) - H(p_t),
\]
Consider the post-measurement state $\nu = \sum_i \langle \Gamma_i | \mu |\Gamma_i\rangle \langle \Gamma_i |$. Using Eq. (5.5) we obtain
\[
\Delta(p_{k,t}) \leq H(p_{k,t}) - S(\nu) + n/2 - H(p_t), \tag{5.6}
\]
where $S$ is the von Neumann entropy. Consider the state
\[
\rho_{12} = \sum_{k=1}^{d} \sum_{t=1}^{3} p_{k,t} |t\rangle\langle t|_1 \otimes (U_t |k\rangle \langle k|U_t^\dagger)_2,
\]
for which we have that
\[
S(\rho_{12}) = H(p_{k,t}) \leq S(p_1) + S(p_2) \\
= H(p_t) + S(\mu) \\
\leq H(p_t) + S(\nu).
\]
Using Eq. (5.6) and the previous equation we get
\[ \Delta(p_{k,t}) \leq \frac{n}{2}, \]
for any prior distribution. This bound is saturated by the uniform prior and therefore we conclude that the uniform prior results in the largest gap possible.

### 5.2.2 MUBs from generalized Pauli matrices

We now consider MUBs based on the generalized Pauli matrices \( X_d \) and \( Z_d \) as described in Chapter 2.4.2. We consider a uniform prior over the elements of each basis and the set of bases. Choosing a non-uniform prior does not lead to a better locking effect.

**5.2.2. Lemma.** Let \( \mathcal{B} = \{ \mathcal{B}_1, \ldots, \mathcal{B}_m \} \) be any set of MUBs constructed on the basis of generalized Pauli matrices in a Hilbert space of prime power dimension \( d = p^N \). Consider the ensemble \( \mathcal{E} = \{ \frac{1}{dm}, |b_k^t \rangle \langle b_k^t | \} \). Then
\[ I_{\text{acc}}(\mathcal{E}) = \log d - \frac{1}{m} \min_{B_t \in \mathcal{B}} \sum_{|\psi\rangle} H(B_t|\psi\rangle). \]

**Proof.** We can rewrite Eq. (5.4) for a POVM \( M_B \) of the form \( \{ \alpha_i |\Phi_i\rangle \langle \Phi_i | \} \) as
\[ I_{\text{acc}}(\mathcal{E}) = \max_{M_B} \left( \log d + \sum_{i} \frac{\alpha_i}{dm} \sum_{k,t} |\langle \Phi_i | b_k^t \rangle|^2 \log |\langle \Phi_i | b_k^t \rangle|^2 \right) \]
\[ = \max_{M_B} \left( \log d - \sum_{i} \frac{\alpha_i}{d} \sum_{t} p_t H(B_t|\Phi_i\rangle) \right). \]

For convenience, we split up the index \( i \) into \( i = a, b \) with \( a = a_1, \ldots, a_N \) and \( b = b_1, \ldots, b_N \), where \( a_\ell, b_\ell \in \{0, \ldots, p-1\} \) in the following.

We first show that applying generalized Pauli matrices to the basis vectors of a MUB merely permutes those vectors.

**1. Claim.** Let \( \mathcal{B}_t = \{ |b_1^t \rangle, \ldots, |b_d^t \rangle \} \) be a basis based on generalized Pauli matrices (Chapter 2.4.2) with \( d = p^N \). Then \( \forall a, b \in \{0, \ldots, p-1\}^N \), \( \forall k \in [d] \), we have that \( \exists k' \in [d], \) such that \( |b_{k'}^a \rangle = X_a^N Z_{k'}^N \cdots X_1^N Z_{k'}^N |b_k^b \rangle \).

**Proof.** Let \( T_p^i \) for \( i \in \{0, 1, 2, 3\} \) denote the generalized Pauli’s \( T_p^0 = I_p, \ T_p^1 = X_p, \ T_p^2 = Z_p \), and \( T_p^3 = X_pZ_p \). Note that \( X_pZ_p = \omega^{uv} Z_pX_p \), where \( \omega = e^{2\pi i/p} \). Furthermore, define \( T_p^{i(z_1)} = I_p^{\otimes (z_1-1)} \otimes T_p^i \otimes I_p^{N-z} \) to be the Pauli operator \( T_p^i \) applied to the \( x \)-th qupit. Recall from Section 2.4.2 that there exist sets of Pauli operators \( C_t \) such that the basis \( \mathcal{B}_t \) is the unique simultaneous eigenbasis of the set of operators in \( C_t \), i.e., for all \( k \in [d] \) and \( f, g \in [N] \),
\(|b'_k\rangle \in \mathcal{B}_t\) and \(c'_{f,g} \in C_t\), we have \(c'_{f,g}|b'_k\rangle = \lambda'_{k,f,g}|b'_k\rangle\) for some value \(\lambda'_{k,f,g}\). Note that any vector \(|v\rangle\) that satisfies this equation is proportional to a vector in \(\mathcal{B}_t\).

To prove that any application of one of the generalized Paulis merely permutes the vectors in \(\mathcal{B}_t\), it is therefore equivalent to proving that \(\mathcal{T}_p^{i(x)}|b'_k\rangle\) are eigenvectors of \(c'_{f,g}\) for any \(f, g \in [k]\) and \(i \in \{1, 3\}\). This can be seen as follows: Note that \(c'_{f,g} = \bigotimes_{n=1}^N \left( \mathcal{T}_p^{1(n)} \right)^{f_n} \left( \mathcal{T}_p^{3(n)} \right)^{g_n}\) for \(f = (f_1, \ldots, f_N)\) and \(g = (g_1, \ldots, g_N)\) with \(f_N, g_N \in \{0, \ldots, p-1\}\) [BBRV02]. A calculation then shows that \(c'_{f,g} \mathcal{T}_p^{i(x)}|b'_k\rangle = \tau_{f,g,i}^t \lambda'_{k,f,g} \mathcal{T}_p^{i(x)}|b'_k\rangle\), where \(\tau_{f,g,i}^t = \omega^{q_{x_s}}\) for \(i = 1\) and \(\tau_{f,g,i}^t = \omega^{-f_s}\) for \(i = 3\). Thus \(\mathcal{T}_p^{i(x)}|b'_k\rangle\) is an eigenvector of \(c'_{f,g}\) for all \(t, f, g\) and \(i\), which proves our claim.

Suppose we are given \(|\psi\rangle\) that minimizes \(\sum_{\mathcal{B}_t \in \mathcal{E}} H(\mathcal{B}_t||\psi\rangle\). We can then construct a full POVM with \(d^2\) elements by taking \(\{1_\mathcal{D}|\Phi_{ab}\rangle\langle\Phi_{ab}|1_\mathcal{D}\}\) with \(|\Phi_{ab}\rangle = (X_{d}^{a_1} Z_{d}^{b_1} \otimes \ldots \otimes X_{d}^{a_N} Z_{d}^{b_N})|\psi\rangle\). However, it follows from our claim above that for any \(a, b, k, k'\) such that \(|\langle\Phi_{ab}|b'_k\rangle|^2 = |\langle\psi|b'_k\rangle|^2\), and thus \(H(\mathcal{B}_t||\psi\rangle) = H(\mathcal{B}_t||\Phi_{ab}\rangle)\) from which the result follows.

Determining the strength of the locking effects for such MUBs is thus equivalent to proving bounds on entropic uncertainty relations. We thus obtain as a corollary of Theorem 4.2.3 and Lemma 5.2.2, that, for dimensions which are the square of a prime power (i.e. \(d = p^{2N}\)), using any product MUBs based on generalized Paulis does not give us any better locking than just using 2 MUBs.

**5.2.3. Corollary.** Let \(\mathcal{S} = \{S_1, \ldots, S_m\}\) with \(m \geq 2\) be any set of MUBs constructed on the basis of generalized Pauli matrices in a Hilbert space of prime (power) dimension \(s = p^N\). Define \(U_t\) as the unitary that transforms the computational basis into the \(t\)th MUB, i.e., \(S_t = \{U_t |1\rangle, \ldots, U_t |s\rangle\}\). Let \(\mathcal{B} = \{B_1, \ldots, B_m\}\) be the set of product MUBs with \(B_t = \{U_t \otimes U'_t |1\rangle, \ldots, U_t \otimes U'_t |d\}\) in dimension \(d = s^2\). Consider the ensemble \(\mathcal{E} = \{1_\mathcal{D}, |b'_k\rangle\langle b'_k|\}\). Then

\[
\mathcal{I}_{acc}(\mathcal{E}) = \frac{\log d}{2}.
\]

**Proof.** The claim follows from Theorem 4.2.3 and the proof of Lemma 5.2.2, by constructing a similar measurement formed from vectors \(|\tilde{\Phi}_{ab}\rangle = K_{\tilde{a}_1\tilde{b}} \otimes K_{a_2b_2}^*|\psi\rangle\) with \(\tilde{a} = a_1 a_2^*\) and \(\tilde{b} = b_1 b_2^*\), where \(a_1, a_2^*\) and \(b_1^*, b_2^*\) are defined like \(a\) and \(b\) in the proof of Lemma 5.2.2, and \(K_{ab} = (X_{d}^{a_1} Z_{d}^{b_1} \otimes \ldots \otimes X_{d}^{a_N} Z_{d}^{b_N})^\dagger\) from above.

The simple example we considered above is in fact a special case of Corollary 5.2.3. It shows that if the vector that minimizes the sum of entropies has certain symmetries, the resulting POVM can even be much simpler. For example, the Bell states are vectors which such symmetries.
5.3 Conclusion

5.2.3 MUBs from Latin squares

At first glance, one might think that maybe the product MUBs based on generalized Paulis are not well suited for locking just because of their product form. Perhaps MUBs with entangled basis vectors do not exhibit this problem? Let’s examine how well MUBs based on Latin squares can lock classical information in a quantum state. All such MUBs are highly entangled, with the exception of the two extra MUBs based on non-Latin squares. Surprisingly, it turns out, however, that any set of at least two MUBs based on Latin squares, does equally well at locking as using just 2 such MUBs. Thus such MUBs perform equally “badly”, i.e., we cannot improve the strength of the locking effect by using more MUBs of this type.

5.2.4 Lemma. Let $\mathcal{B} = \{B_1, \ldots, B_m\}$ with $m \geq 2$ be any set of MUBs in a Hilbert space of dimension $d = s^2$ constructed on the basis of Latin squares. Consider the ensemble $\mathcal{E} = \{\frac{1}{\sqrt{m}}, |b_k\rangle\langle b_k|\}$. Then

$$I_{\text{acc}}(\mathcal{E}) = \log \frac{d}{2}.$$  

Proof. Note that we can again rewrite $I_{\text{acc}}(\mathcal{E})$ as in the proof of Lemma 5.2.2. Consider the simple measurement in the computational basis $\{|i, j\rangle\langle i, j|\mid i, j \in [s]\}$. The result then follows by the same argument as in Lemma 4.2.4.

Intuitively, our measurement outputs one sub-square of the Latin square used to construct the MUBs as depicted in Figure 5.2.3. As we saw in the construction of MUBs based on Latin squares in Chapter 2.4.1, each entry “occurs” in exactly $\sqrt{d} = s$ MUBs.

![Figure 5.2: Measurement for $|1, 1\rangle$.](image)

5.3 Conclusion

We have shown tight bounds on locking for specific sets of mutually unbiased bases. Surprisingly, it turns out that using more mutually unbiased basis does not
always lead to a better locking effect. It is interesting to consider what may make these bases so special. The example of three MUBs considered in Lemma 5.2.1 may provide a clue. These three bases are given by the common eigenbases of \( \{ \sigma_x \otimes \sigma_x, \sigma_x \otimes I, I \otimes \sigma_x \} \), \( \{ \sigma_z \otimes \sigma_z, \sigma_z \otimes I, I \otimes \sigma_z \} \) and \( \{ \sigma_y \otimes \sigma_y, \sigma_y \otimes I, I \otimes \sigma_y \} \) respectively [BBRV02]. However, \( \sigma_x \otimes \sigma_x, \sigma_z \otimes \sigma_z \) and \( \sigma_y \otimes \sigma_y \) commute and thus also share a common eigenbasis, namely the Bell basis. This is exactly the basis we will use as our measurement. For all MUBs based on generalized Pauli matrices, the MUBs in prime power dimensions are given as the common eigenbasis of similar sets consisting of strings of Paulis. It would be interesting to determine the strength of the locking effect on the basis of the commutation relations of elements of different sets. Furthermore, perhaps it is possible to obtain good locking from a subset of such MUBs where none of the elements from different sets commute.

It is also worth noting that the numerical results of [DHL+04] indicate that at least in dimension \( p \) using more than three bases does indeed lead to a stronger locking effect. It would be interesting to know, whether the strength of the locking effect depends not only on the number of bases, but also on the dimension of the system in question.

Whereas general bounds still elude us, we have shown that merely choosing mutually unbiased bases is not sufficient to obtain good locking effects. We thus have to look for different properties. Sadly, whereas we were able to obtain good uncertainty relations in Chapter 4.3, the same approach does not work here: To obtain good locking we must not only find good uncertainty relations, but also find a way to encode many bits using only a small number of encodings.