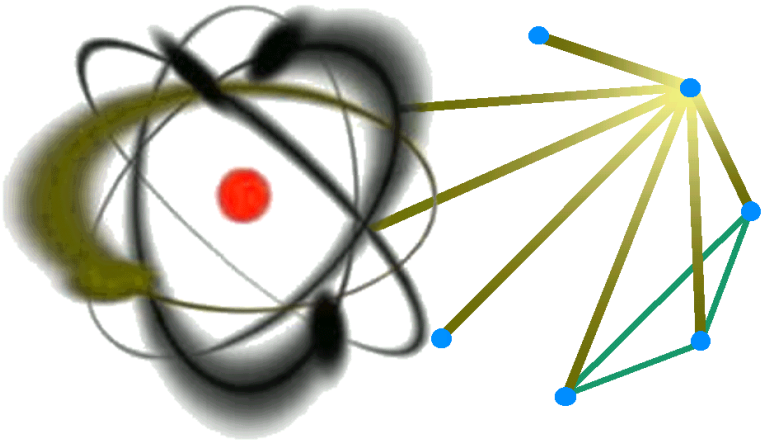
Classical Pseudo-Telepathy and Coloring Graphs

Diploma Thesis of
Viktor Galliard



ETH Zurich, Switzerland
University of Waterloo, Canada
February 9, 2001

Diploma Thesis of Viktor Galliard

Swiss Federal Institute of Technology (ETH Zurich)
Department of Computer Science
vgalliard@math.uwaterloo.ca

Supervisor
Prof. Stefan Wolf
University of Waterloo
Centre for Applied Cryptographic Research
swolf@cacr.math.uwaterloo.ca

Prof. Ueli Maurer
ETH Zurich
Institute for Theoretical Computer Science
maurer@inf.ethz.ch

Contents

Abstract

In the past few years, a challenge has manifested to quantify the amount of communication required to simulate entangled quantum systems by classical information.

On one side of the spectrum, there are quantum systems with one EPR-pair: Different approaches with different restrictions to the classical system have been investigated. Upper bounds for the amount of communication needed to simulate such a pair have been determined. For exactly simulating an EPR-pair (i. e., with a deterministic protocol), a result by Brassard, Cleve and Tapp in 1999 is known, that 8 bit suffice for general von Neumann measurements. Where people are interested in the expected amount of communication, the bounds are improving on a yearly basis. 1.19 bit expected communication could be shown in 1999 by Cerf, Gisin and Massar.

The opposite side of the spectrum reveals quantum systems with n EPR-pairs. Bounds for the expected amount are steadily improving at the moment and reached the almost optimal upper bound of $n2^n$ for POV-measurements. For the more specific von Neumann measurements an exponential amount of information is needed in order to exactly simulate the quantum system.

In this paper we show the precise amount (instead of a bound) of communication needed to simulate a bipartite quantum scenario in relation of a graph coloring problem. Instead of an asymptotical bound, we conjecture an lower bound on the amount of communication needed for exact simulation of a n-qubit bipartite quantum system by considering combinatorics of finite sets.

Keywords. Quantum entanglement, EPR-paradox, Bell-inequality, nonlocality, classical simulation, quantifying entanglement, communication complexity, coloring graphs, finite set theory.

1 Introduction

In 1935, Einstein, Podolsky, and Rosen described a Gedanken-experiment which in their opinion disclosed a paradoxical consequence of quantum mechanics. They predicted that when measurements are carried out on certain particles, (EPR pairs), their outcome is perfectly correlated even when the measurement events are space-like separated.

In 1964, John S. Bell could generally show that certain separated quantum systems cannot be classically simulated by using only hidden local variables and without any communication [Bell 64]. This motivated the following question: For a given a quantum scenario, what is the amount of information that must be exchanged for perfectly simulating it? It was shown by

Brassard, Cleve and Tapp in 1999, that surprisingly, a small number of bits is sufficient in some cases even though the number of possible measurement bases is uncountably infinite [Brassard 99].

There exist several quantum scenarios, such as the Deutsch-Jozsa algorithm [DeutschJozsa 92], for which the classical simulation is not as powerful as the algorithm in the quantum quantum domain. In this study, the analysis of a so-called pseudo-telepathy game (which is closely related to the aforementioned questions) leads to problems of graph theory and combinatorics of finite sets. Finally, we can conclude a very strong relationship between quantum entanglement and the chromatic number of certain graphs which reveals another connection between the quantum and the classical domain.

2 Entanglement and Non-Locality

We consider two quantum particles (e. g., a pair of photons or electrons). We can determine bipartite quantum systems by applying unitary transformation to either one or both quantum states in the ground configuration. Quantum mechanics claims the existence of certain scenarios that lead to correlation between the two subsystems, namely entanglement. Bell's theorem in 1964 showed that it is not always possible to simulate bipartite quantum measurement scenarios with a classical system, if the measurement events are space-like separated [Bell 64]. Such quantum states are of great interest, since the classical counterpart simply does not exist.

A quantum system of n qubits can generally be described as a superposition of basis states $|\,0\ldots00\,\rangle, |\,0\ldots01\,\rangle, \ldots, |\,1\ldots11\,\rangle$. Each state is present with a certain complex probability amplitude α_i (i. e., the probability to measure the state $|\,i\,\rangle$ is $|\alpha_i|^2$) and can be written as follows:

$$|\,\Gamma\,\rangle = \sum_{i=0}^{2^n-1} \alpha_i |\,i\,\rangle$$

The probability amplitudes of a quantum state satisfy $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. If the result of a measurement is i (with probability $|\alpha_i|^2$), the superposition $|\,\Gamma\,\rangle$ collapsed into the basis state $|\,i\,\rangle$. Therefore we lose the quantum information and 'only' get n bit of classical information from it.

As a first example we consider the quantum state (we write $|\,ij\,\rangle$ instead of $|\,i\,\rangle \otimes |\,j\,\rangle$, where $\otimes$ is the tensor product of the two subsystems)

$$|\,\Gamma_{AB}\,\rangle = \frac{1}{2}|\,00\,\rangle - \frac{1}{2}|\,01\,\rangle + \frac{1}{2}|\,10\,\rangle - \frac{1}{2}|\,11\,\rangle$$

We can easily rewrite it as follows

$$|\,\Gamma_{AB}\,\rangle = \frac{1}{\sqrt{2}}\Big(|\,0\,\rangle + |\,1\,\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|\,0\,\rangle - |\,1\,\rangle\Big)$$

Quantum states with such a product representation are called *separable* and can be treated completely independently (i. e., the probability distributions corresponding to measurements applied to each particle are statistically independent). However, we are interested in entangled states. The singlet state is one of the four Bell states:

$$|\,\Psi^-\,\rangle = \frac{1}{\sqrt{2}}|\,01\,\rangle - \frac{1}{\sqrt{2}}|\,10\,\rangle$$

There exist no quantum states $|\,\psi_A\,\rangle$ and $|\,\psi_B\,\rangle$ such that $|\,\Psi^-\,\rangle = |\,\psi_A\,\rangle \otimes |\,\psi_B\,\rangle$; such a state is called *entangled*. By measuring each subsystem in certain bases, we will have correlated results, even though the two measurement events are space-like separated. Our goal is now to quantify the amount of information we need to exactly simulate quantum entanglement in special quantum scenarios.

3 Classical Simulation

Brassard, Cleve, and Tapp showed that with von Neumann-measurements of Bell states can be perfectly simulated classically with a *local hidden variable*[1] scheme augmented with eight bits of communication [Brassard 99]. This result is somewhat surprising since the number of possible measurements is infinitely large. Cerf, Gisin, and Massar showed in 1999 that on average 1.19 bit of communication suffice to achieve an exact classical simulation of quantum teleportation [Cerf 99]. The bounded-communication model and the average-communication model are the two different models considered with investigating simulation of quantum entanglement with respect to hidden local variables.

There is another challenge in determining the amount of information needed for simulation of systems with more than one qubit with respect to coherent measurements, i. e., not only measuring a subsystem. In the bounded-communication model Brassard et al. showed that $c2^n$ bit of communication are needed, for some constant c [Brassard 99]. Their proof reduces a quantum scenario to a restricted version of the inequality problem in [Buhr 98] as a communication complexity problem. Their result

[1] Local hidden variable schemes are introduced and defined in [Brassard 99].

relies on a strong mathematical theorem from Frankl and Rödl from 1987 [FranklRödl 87]. The same expected amount of information is need in the average bounded model for n qubits.

In 2000, Massar, Bacon, Cerf and Cleve [Massar 2000] improved Steiner's [Steiner 99] 22 bit bound from 1999 and could show that simulating a Bell state without local hidden variables can be done with 20 bits on average. They showed as well that $\Omega(n2^n)$ bit of communication on average are needed to exactly simulate an n-qubit system without local hidden variables with the more general positive operator measurements (POVMs).

In this paper we will show a lower bound on the communication needed to exactly simulate n Bell states with a constant amount of local hidden variables in terms of graph coloring problem. Furthermore we conjecture how many bits of information we need in order to exactly simulate quantum entanglement for more than one qubit.

4 Quantum Pseudo-Telepathy: Previous Results

We will briefly describe the quantum scenario as examined in [Brassard 99] and determine their results. Consider the case of $\tilde{n}$ Bell states

$$|\,\Phi^+\,\rangle_{AB}^{\otimes\tilde{n}} = \frac{1}{\sqrt{2^{\tilde{n}}}} \sum_{i\in\{0,1\}^{\tilde{n}}} |\,i\,\rangle|\,i\,\rangle$$

as a resource of quantum entanglement. Furthermore, we determine a quantum measurement scenario $(|\,\Phi^+\,\rangle_{AB}^{\otimes\tilde{n}}, M_A, M_B)$ on $\tilde{n}$ qubits, with $|M_A| = M_B| = 2^{2^{\tilde{n}}}$. Due to their connection with the algorithm in [DeutschJozsa 92], M_A and M_B are called *Deutsch-Jozsa* measurements. First, we use the unitary transformation that maps $|\,i\,\rangle$ to $(-1)^{z_i}$ (z_i denotes the i-th bit of the parameter $z \in M_A$ or $z \in M_B$) acting as a phase shift. Moreover, the n-qubit Hadamard transformation which maps $|\,i\,\rangle$ to $\frac{1}{\sqrt{2^{\tilde{n}}}} \sum_{j\in\{0,1\}^{\tilde{n}}} (-1)^{i\cdot j}|\,j\,\rangle$, where $i \cdot j$ is the inner product of the two n-bit strings i and j. Finally we measure in the computational basis $\{|\,i\,\rangle : i \in \{0,1\}^{\tilde{n}}\}$, yielding an outcome in $\{0,1\}^{\tilde{n}}$.

One can verify that for the measurement $x \in M_A$, $y \in M_B$ with $x = y$ the output of the measurements a and b are equal. If the Hamming-distance[2] is $2^{\tilde{n}-1}$, the probability that a is equal to b is 0.

[2]The Hamming-distance $D_H(x, y)$ of two binary strings x, y is the number of bits in which x, y differ.

We can derive the above results by considering the resulting quantum state after applying both unitary operations and before the measurement

$$\frac{1}{\sqrt{2^{3\tilde{n}}}} \sum_{j,k,i \in \{0,1\}^{\tilde{n}}} (-1)^{x_i + y_i + i \cdot (j \oplus k)} | j \rangle | k \rangle \tag{1}$$

If $x = y$, then the state (1) becomes $\frac{1}{\sqrt{2^{\tilde{n}}}} \sum_{i \in \{0,1\}^{\tilde{n}}} | i \rangle | i \rangle$ end therefore $P[a = b | x = y] = 1$. If the Hamming-distance between x and y is $2^{\tilde{n}-1} = n/2$, then the probability amplitude of any ket of the form $| j \rangle | j \rangle$ of state (1) becomes 0, and so the $P[a = b | D_H(x, y) = n/2] = 0$.

We define now the pseudo-telepathy game as follows: Both parties Alice and Bob receive a binary string of length n, the question. The promise is, that x and y, the questions, are either equal or their Hamming-distance is $n/2$. The output strings are of length $\tilde{n} = \log_2 n$. They win the game, if their outputs are either equal if the questions are the same and different otherwise.

When the quantum system described above is considered, it can be shown that the game can be won with a resource of $\tilde{n}$ Bell states.

5 Classical Pseudo-Telepathy and Coloring Graphs

5.1 Chromatic Number and Communication Complexity

Let G be an undirected graph with vertex set V and edge set $E \subseteq V^2$. (The fact that G is undirected means that $(v, v') \in E$ implies $(v', v) \in E$ for all $v, v' \in V$.) The *pseudo-telepathy game in G with answer length $\tilde{n}$ and communication C*, denoted by $\mathrm{PT}(G, \tilde{n}, C)$, is defined as follows. Two parties A and B are given vertices v_A and v_B (the *questions*), with respect to the condition that $v_A = v_B$ or $(v_A, v_B) \in E$. The parties are allowed to exchange at most C bits of communication (each bit in either direction). Then A and B are said to win the game $\mathrm{PT}(G, \tilde{n}, C)$ if they can both generate an $\tilde{n}$-bit output r_A and r_B (the *answer*) with the property that $r_A = r_B$ holds if and only if $v_A = v_B$ does.

Theorem 1 can be proven, but the proof is not included.

Theorem 1 *Let G be a graph. Assume $PT(G, \tilde{n}, C)$ can be won. Then*

$$C \geq \log_2 \chi(G) - \tilde{n}.$$

In the following theorem we show a lower bound on the communication needed.

Theorem 2 *Let G be a graph, and let $C, \tilde{n} \in \mathbf{N}$ with*

$$C \geq \lceil \log_2 \chi(G) \rceil - \tilde{n} + 1.$$

Then PT($G, \tilde{n}, C$) can be won.

Proof. For each valid input $x \in M_A$ and $y \in M_B$, let $\kappa(x), \kappa(y) \in \{0, \ldots, \chi(G) - 1\}$ be the color to the corresponding vertices in the optimal colored graph G with chromatic number $\chi(G)$.

The two parties Alice and Bob carry out the following protocol: Alice outputs the first $\tilde{n}$ bits of the binary representation of her color $\kappa(x)$ and sends the remaining $\lceil \log_2 \chi(G) \rceil - \tilde{n}$ bits followed by the $\tilde{n}$-th bit of $\kappa(x)$ to Bob. Bob checks if the received bits match to the bits $\tilde{n}+1$ to $\lceil \log_2 \chi(G) \rceil - \tilde{n}$ of his color. If so, Bob outputs the first $\tilde{n}$ bits of $\kappa(y)$. If not, he outputs the first $\tilde{n} - 1$ bits of $\kappa(y)$ followed by the inverse of the last bit received from Alice.

Obviously, for $x = y$ this protocol succeeds. Now, let the binary representation of $\kappa(x)$ be $x'|x''$, where $|x'| = \tilde{n}$ and $|x''| = \lceil \log_2 \chi(G) \rceil - \tilde{n}$ (let $|$ be the concatenation of two strings). For $x \neq y$ we consider two cases:

where $x'' = y''$: Since $x \neq y$ and $x'' = y''$ holds, x' and y' must differ in at least one bit and so Alice's and Bob's outputs are different.

where $x'' \neq y''$: The two outputs always vary, since they differ according to the protocol at least in the last bit.

Since this protocol needs $C = \lceil \log_2 \chi(G) \rceil - \tilde{n} + 1$ bits to be exchanged from Alice to Bob, the theorem follows. □

5.2 The Graph and its Properties

To find the chromatic number of certain graphs can be very difficult. In general, the problem is *NP-hard*. The Kneser Graph is an example of a sparse graph with high chromatic number. Martin Kneser conjectured its chromatic number and it remained unproven for twenty years [Bollobás 78]. We try to find a lower bound on the chromatic number of our graph by identifying a maximum independent set.

First we define the graph corresponding to the above mentioned pseudo-telepathy game:

Definition 1 *For $n = 2^{\tilde{n}}$ and $\tilde{n} \geq 1$, let $G_n(V, E)$ be the graph with vertices $V = \{v_0, v_1, \ldots, v_{2^n-2}, v_{2^n-1}\}$ and edge-set $E = \{(v_i, v_j) \in V^2 : D_H(v_i, v_j) = \frac{n}{2}\}$.*

$D_H(v_i, v_j)$ denotes the Hamming-distance between the two codewords v_i and v_j in binary representation. We use $W_H(v_i)$ as Hamming-weight[3] of the codeword v_i. We associate each $v_i \in V$ with the codeword i in binary representation.

The definition of this graph corresponds to the quantum-telepathy game with the Deutsch-Jozsa promise defined in Section 4 and the communication complexity analysis in Section 5.1 on page 7. The questions for the game for the two parties Alice and Bob we have two vertices v_i and v_j with either $v_i = v_j$ or $D_H(v_i, v_j) = n/2$. The output corresponds to the color of the vertex v_i, v_j respectively.

Additionally, we give an equivalent, and in some cases more convenient definition in terms of subsets.

Definition 2 *For $n = 2^{\tilde{n}}$ and $\tilde{n} \geq 1$, let $G_n(\mathcal{V}, E)$ be the graph with vertices $\mathcal{V} = 2^{[n]}$ and edge-set $E = \{(A, B) \in \mathcal{V}^2 : |\triangle(A, B)| = \frac{n}{2}\}$. With the symmetric difference $\triangle(A, B) := (A \cup B) \setminus (A \cap B)$ and $[n] := \{1, 2, \ldots, n\}$.*

Lemma 1 *The graphs of Definitions 1 and 2 are isomorphic.*

Proof. The subset $A_i \in \mathcal{V}$, with $A = \{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$ is equivalent with the vertex $v_i \in V$ in Definition 1, where the bits $i_1, i_2, \ldots, i_k$ are one, and the other bits are zero. Therefore, $W_H(v_i) = |A_i|$ and the symmetric difference $\triangle(A_i, A_j)$ is equal to the Hamming-distance $D_H(v_i, v_j)$ for corresponding $v_j \in V$ and $A_j \in \mathcal{V}$. Accordingly, the edge and vertex-set of both definitions correspond and the lemma follows. □

For $\tilde{n} \geq 2$, let $V = V_{even} \cup V_{odd}$ be the two subsets of codewords with even and odd Hamming-weight in V.

Lemma 2 *For $\tilde{n} \geq 2$, the two components of $G_n(\mathcal{V}, E)$ are isomorphic.*

Proof. We define the isomorphism $\Phi_{v_e, v_o} : V_{even} \to V_{odd} : v' = v \oplus (v_e \oplus v_o)$, with $v_e \in V_{even}$ and $v_o \in V_{odd}$ that maps v to v'. Since $\forall v \in V_{even} : W_H(v) \in \{0, 2, \ldots, n-2, n\}$ and $v_e \oplus v_o$ is constant with $W_H(v_e \oplus v_o)$ odd, $\forall v \in V_{odd}$ we have $W_H(v) \in \{1, 3, \ldots, n-3, n-1\}$. Φ_{v_e, v_o} is bijective, so the Lemma follows. □

[3] The Hamming-weight of a binary string s of length l is the number of ones in s, i.e., $W_H(s) := D_H(s, 0^l)$.

Lemma 3 *For $\tilde{n} \geq 2$ in $G_n(V, E)$. For all $v_i, v_j \in V'$ and V' either V_{odd} or V_{even}, there exists a path of length 2 from v_i to v_j.*

Proof. We have $A_i, A_j \in \mathcal{V}'$ (the corresponding subset to V') in $G_n(\mathcal{V}, E)$. There exists an $A \in \mathcal{V}$ with $(A, A_i), (A, A_j) \in E$ and therefore with the property

$$\triangle(A, A_i) = \triangle(A, A_j) = n/2 \tag{2}$$

as follows ($A_\cap = A_i \cap A_j$ and $\overline{A_\cup} = [n] \setminus A_i \cup A_j$):

If $|A_i \cap A_j| \geq n/4$**, then** $A = A'_\cap \cup \overline{A_\cup}'$ for $A'_\cap \subset A_\cap$ and $\overline{A_\cup}' \subset \overline{A_\cup}$ with $|A'_\cap| = |\overline{A_\cup}'| = n/4$.

If $|A_i \cap A_j| < n/4$**, then** $A = A'_i \cup A'_j$ for $A'_i \subset A_i \setminus A_\cap$ and $A'_j \subset A_j \setminus A_\cap$ with $|A'_i| = |A'_j| = n/4$.

Those subsets A satisfy property (2), therefore $\{(A, A_i), (A, A_j)\} \subset E$ and the lemma is proved, since Lemma 1 and Lemma 2 holds. □

Lemma 4 *For $\tilde{n} \geq 2$, $G_n(\mathcal{V}, E)$ has two connected components.*

Proof. Since $\tilde{n} \geq 2$, we have for all $(v_i, v_j) \in E$ $D_H(v_i, v_j)$ even. Therefore we have no edge between a vertices with even and odd Hamming-weight. For every pair of vertices $v_i, v_j \in V_{even}$, according to Lemma 3 we find a $v \in V_{even}$, with $(v, v_i) \in E$ and $(v, v_j) \in E$. Since the two components are isomorphic by Lemma 2, both of them are connected. □

Theorem 3 *For $\tilde{n} \geq 2$, $G_n(\mathcal{V}, E)$ has two isomorphic connected components.*

Proof. Follows directly from the Lemmas 4 and 2. □

Theorem 4 *$G_n(\mathcal{V}, E)$ is vertex-transitive.*

Proof. The function $\Phi_{v_1,v_2} : V \to V : v' = v \oplus (v_1 \oplus v_2)$ that maps the vertex v_1 to v_2 is an automorphism, since two vertices are connected if their Hamming-distance is $n/2$ and the Φ_{v_1,v_2} preserves Hamming-distances between them. Therefore we can find an automorphism that for all $v_1, v_2 \in V$ maps all v_1 to v_2. □

Before proving the next lemma, we define the dual Hamming-code (see for example [vanLint 82]).

Definition 3 *Let $\{h_1, h_2, \ldots, h_{\tilde{n}}\}$ be a basis of the dual Hamming-code with $h_i = \{0,1\}^n$ and $\forall i \in \{1,\ldots,\tilde{n}\} : \forall j \in \{1,\ldots,\tilde{n}\}\backslash\{i\} : D_H(h_i, h_j) = n/2$. Moreover $W_H(h_i) = n/2$ for all i. The generator-matrix $G_M^{\tilde{n}}$ of the dual Hamming-code of length $2^{\tilde{n}}$ has size $2^{\tilde{n}} \times \tilde{n}$. The columns of $G_M^{\tilde{n}}$ are all non-zero strings of length $\tilde{n}$. And the rows finally set up a basis $\{h_1, h_2, \ldots, h_{\tilde{n}}\}$ of the dual Hamming-code.*

Furthermore define the following subset of V:

Definition 4 *For $n = 2^{\tilde{n}}$, let $CL(v^*, h_1, h_2, \ldots, h_{\tilde{n}})$ be the vertex-set $\{v \in \{0,1\}^n : v \oplus (a_1 \cdot h_1 \oplus a_2 \cdot h_2 \oplus \cdots \oplus a_{\tilde{n}} \cdot h_{\tilde{n}}) = v^*$, with $a_1, \ldots, a_{\tilde{n}} \in \{0,1\}\}$ of size n.*

Lemma 5 *The complete graph K_n is a subgraph of $G_n(V, E)$.*

Proof. We show that all $(v_i, v_j) \subset CL(v, h_1, h_2, \ldots, h_{\tilde{n}})$ are edges in $G_n(V, E)$. Suppose $v_i = a_1 \cdot h_1 \oplus a_2 \cdot h_2 \oplus \cdots \oplus a_{\tilde{n}} \cdot h_{\tilde{n}}$ and $v_j = b_1 \cdot h_1 \oplus b_2 \cdot h_2 \oplus \cdots \oplus b_{\tilde{n}} \cdot h_{\tilde{n}}$. We have $D_H(v_i, v_j) = W_H(v_i \oplus v_j) = (a_1 \oplus b_1) \cdot h_1 \oplus \cdots \oplus (a_{\tilde{n}} \oplus b_{\tilde{n}}) \cdot h_{\tilde{n}}$, due to the fact, that $a_i \cdot h_i \oplus b_i \cdot h_i = (a_i \oplus b_i) \cdot h_i$. Since this is by definition $n/2$, follows $(v_i, v_j) \in E$. Therefore we have a *clique* of size n in $G_n(V, E)$ and the statement follows. □

5.3 The Chromatic Number

Theorem 5 *The chromatic number $\chi(G_n)$ of $G_n(V, E)$ is at least n.*

Proof. We saw in Lemma 5 that K_n is a subgraph of $G_n(V, E)$. Therefore we need exactly n colors to color K_n and hence at least n colors for $G_n(V, E)$. □

We know that $\chi(G_n) \geq n$. Now, let us consider the trivial cases $\tilde{n} = 1, 2$. The pseudo-telepathy game can be won without communication by using the following strategy:

For $\tilde{n} = 1$: Alice and Bob get the questions $x = x_1x_2$ and $y = y_1y_2$. Their output will be $a_1 = x_1 \oplus x_2$, $b_1 = y_1 \oplus y_2$ respectively.

For $\tilde{n} = 2$: The two parties get the strings $x = x_1x_2x_3x_4$ and $y = y_1y_2y_3y_4$. Finally Alice output the bits $a_1 = x_1 \oplus x_2$ and $a_2 = x_2 \oplus x_3$. Bob's result is $b_1 = y_1 \oplus y_2$ and $b_2 = y_2 \oplus y_3$.

Now consider the case for $\tilde{n} = 3$.

Definition 5 *For $G(V,E)$, let $V_{IS} \subset 2^{[n]}$ be the set of all independent sets of $G(V,E)$, then for all $V_{ind} \in V_{IS}$, $\forall v_i, v_j \in V_{ind} : (v_i, v_j) \notin E$. Furthermore let*

$$\alpha(G(V,E)) := \max_{V_{ind} \in V_{IS}} \{|V_{ind}|\}$$

be the size of a maximum independent set and

$$V_{ISmax} := \{V_{ind} \in V_{IS} : |V_{ind}| = \alpha(G(V,E))\}$$

be the set of maximum independent sets in $G(V,E)$.

Lemma 6 *If $V_{ind}^{(0)}$ is an independent set in $G_n(V,E)$ and*

$$\{h_1, h_2, \ldots, h_{\tilde{n}-1}, h_{\tilde{n}}\}$$

a basis of a dual Hamming-code, then the n sets

$$V_{ind}^{(x_1+x_2 2^1+\cdots+x_{\tilde{n}}2^{\tilde{n}-1})} = \{v : v \oplus (x_1 \cdot h_1 \oplus x_2 \cdot h_2 \oplus \cdots \oplus x_{\tilde{n}} \cdot h_{\tilde{n}}) \in V_I\} \quad (3)$$

for $x_i \in \{0,1\}$ are independent sets and mutually disjoint.

Proof. First let us show that they are independent. Let $c = x_1 \cdot h_1 \oplus x_2 \cdot h_2 \oplus \ldots \oplus x_{\tilde{n}-1} \cdot h_{\tilde{n}-1} \oplus x_{\tilde{n}} \cdot h_{\tilde{n}}$, in (3), for some $x_1, \ldots, x_{\tilde{n}}$. Since $\forall v_i, v_j \in V_I^{(0)}$: $D_H(v_i, v_j) \neq n/2$, the two corresponding vertices in $V_I^{(x_1+\ldots+x_{\tilde{n}}2^{\tilde{n}-1})}$, have Hamming-distance $D_H(v_i \oplus c, v_j \oplus c) = D_H(v_i, v_j) \neq n/2$ and independence follows.

To proof disjointness, suppose they were not. Then, there must exist vertices $v, v' \in V_I^0$ and $v' \in V_I^{(l)}$, for some $l = x_1 + \ldots + x_{\tilde{n}}2^{\tilde{n}-1}$. Since the graph is vertex-transitive, we choose the first independent set $V_I^{(0)}$, instead of $V_I^{(l')}$, for $l' \neq l$. Those cases can be derived by considering a graph isomorphic to $G_n(V,E)$. We have for $l > 0$ (otherwise the sets are identical)

$$\begin{aligned} D_H(v, v') &= D_H(v, v \oplus c) && (4) \\ &= n/2. && (5) \end{aligned}$$

Equation (4) holds, since $v' \in V_I^{(l)}$, and Equation (5) follows from the fact, that $W_H(c) = n/2$ (the case $W_H(c) = 0$ drops out, since $l > 0$) as property of dual Hamming-code as stated in Definition 3. Therefore $D_H(v, v') = n/2$ and this contradicts the fact that v and v' are members of $V_I^{(0)}$. □

Theorem 6 *The chromatic number* $\chi(G_8(V,E))$ *is* 8.

Proof. Again let $V = V_{even} \cup V_{odd}$. Define

$$V_{ind} = \{0^8\} \cup \bigcup_{1 \leq i \leq 7} \{10^{i-1}10^{7-i}\}. \tag{6}$$

Obviously, V_{ind} is an independent set, since all elements have mutually Hamming-distance 2. Furthermore the set

$$\overline{V_{ind}} = \{v \in \{0,1\}^n : \overline{v} \in V_{ind}\}$$

is an independent set as well with the same property concerning the Hamming-distance as the set in Equation 6. Now the set $V_{ind} \cup \overline{V_{ind}}$ is an independent set since $\forall (v_i, v_j) \in V_{ind} \times \overline{V_{ind}} : D_H(v_i, v_j) \in \{6, 8\}$. Since $|V_i \cup \overline{V_i}| = 16$ and V_{even} and V_{odd} are isomorphic, we can find an independent set of the same size in V_{odd}. Uniting these two sets leads to the independent set $V_I^{(0)}$ of size 32. We can now determine 8 mutually disjoint maximum independent sets using a basis of a dual Hamming-code as follows:

$$V_I^{(i+2j+4k)} = \{v : v \oplus (i \cdot h_1 \oplus j \cdot h_2 \oplus k \cdot h_3) \in V_I^{(0)}\}.$$

The fact that they are mutually disjoint and independent is a consequence of Lemma 6. We know further from Theorem 5 that the chromatic number is at least 8. Since the color-classes $V_I^{(0)}, \ldots, V_I^{(7)}$ cover the vertex-set V, we found an optimal coloring for $G(V,E)$ and the theorem follows. □

Corollary 1 *The pseudo-telepathy game can be won without classical communication for* $\tilde{n} \leq 3$.

Proof. For $\tilde{n} = 1, 2$, the outputs of Alice and Bob are according to the strategy discussed at the beginning in Section 5.3 on page 11. Then, they succeed for all valid inputs and therefore win the game.

Since $G(V,E)$ can be colored with 8 colors (and $\log_2(8) = 3$ bit suffice to encode the color), Alice and Bob can output the color of the vertex of their question. □

5.4 Maximal Independent Sets

We covered the cases $\tilde{n} = 1, 2, 3$ and showed for those that the classical pseudo-telepathy game can be won without communication. Since an optimal coloring or the chromatic number itself is not easy to determine in general, we will approach the remaining cases $\tilde{n} > 3$ by identifying a maximum independent set $\alpha(G_n(V, E))$ in the graph. A subset $V_{ind} \subset V$ of a graph $G(V, E)$ is independent, if and only if $\forall (v_i, v_j) \in V_{ind}^2 : (v_i, v_j) \notin E$. We determine a maximal independent set in the following meaning.

Definition 6 *An independent set V_{ind} of a graph $G(V, E)$ is maximal if and only if*

$$\forall v' \in V \setminus V_{ind} : \exists v \in V_{ind} : (v, v') \in E.$$

For some subsets of the vertex-set $\mathcal{V}$ we make the following definitions corresponding to [AK 97].

Definition 7 *Let $\binom{[n]}{k}$ be the set of subsets of $2^{[n]}$ consisting of elements with cardinality k. For even k, with $t + 2i \geq 0$ and $0 \leq i \leq (n - t)/2$ let $\mathcal{F}_{t,i}^{n,k}$ be the following set:*

$$\mathcal{F}_{t,i}^{n,k} = \left\{ F \in \binom{[n]}{k} : |F \cap [t + 2i]| \geq t + i \right\}. \tag{7}$$

Moreover let $[t + 2i] = \{1, \ldots, t + 2i\}$ denote the intersection-spot of size $t + 2i$.

Note that in contrast to [AK 97], t will be negative for some instances for our purpose. In their paper, Ahlswede and Khachatrian proved that $\mathcal{F}_{t,i}^{n,k}$ is a maximal, t-intersecting subset of $\binom{[n]}{k}$ for a specific i, depending on n. We use the intersection-property to determine an independent set in $G_n(V, E)$. First let us consider the vertices with Hamming-weight less than $n/2$ (again in the subgraph with vertex-set V_{even}). For $\tilde{n} \geq 3$, let

$$\begin{aligned} \mathcal{V}_{ind}^{<\frac{n}{2}} &= \mathcal{F}_{-\frac{n}{4}-1,\frac{n}{4}-1}^{n,0} \cup \mathcal{F}_{-\frac{n}{4}+1,\frac{n}{4}-2}^{n,2} \cup \ldots \\ &\quad \cup \mathcal{F}_{\frac{n}{4}-3,1}^{n,\frac{n}{2}-4} \cup \mathcal{F}_{\frac{n}{4}-1,0}^{n,\frac{n}{2}-2} \\ &= \bigcup_{l=0}^{\frac{n}{4}-1} \mathcal{F}_{-c_n+2l,c_n-l}^{n,2l} \end{aligned} \tag{8}$$

be a subset in the subgraph of $G_n(V,E)$ with vertex-set $V_{even}^{<\frac{n}{2}} = \{v \in V_{even} : W_H(v) < n/2\}$, for $c_n = n/4 - 1$.

Define further the inverse set of $\mathcal{F}_{t,i}^{n,k}$ as the set $\overline{\mathcal{F}_{t,i}^{n,k}}$ with elements $\{A \in \binom{[n]}{n-k} : \overline{A} \in \mathcal{F}_{t,i}^{n,k}\}$. Now, let us determine a maximal independent set, with $\mathcal{V}_{ind}^{>\frac{n}{2}}$ analogously defined as set (8).

Theorem 7 *For $\tilde{n} \geq 3$, the set*

$$\begin{aligned} \mathcal{V}_{ind} &= \mathcal{V}_{ind}^{<\frac{n}{2}} \cup \mathcal{V}_{ind}^{>\frac{n}{2}} \\ &= \bigcup_{l=0}^{\frac{n}{4}-1} (\mathcal{F}_{-c_n+2l,c_n-l}^{n,2l} \cup \overline{\mathcal{F}_{-c_n+2l,c_n-l}^{n,2l}}) \end{aligned} \tag{9}$$

is a maximal independent set of $G_n(V_{even},E)$ for $c_n = n/4 - 1$.

To proof Theorem 7, we examine first the intersection properties of its subsets in the following lemmas.

Lemma 7 *For $0 \leq l \leq \frac{n}{4} - 1$, $\mathcal{F}_{-c_n+2l,c_n-l}^{n,2l}$ is an independent set.*

Proof. We have to consider only sets with vertices with Hamming-weight $2l \geq n/4$, since for other sets, the cardinality of the symmetric difference $(A \cup B \setminus A \cap B)$ is at most $n/2 - 2$. For the remaining cases, for all $A, B \in \mathcal{F}_{-c_n+2l,c_n-l}^{n,2l}$ and $l \geq n/8$, we have $|A \cap B| \geq -c_n + 2l = -n/4 + 1 + 2l$ because of Definition 7 and so the Hamming-distance of the corresponding codewords is at most $2(2l - (-c_n + 2l)) = n/2 - 2$ and independence follows as well. □

Lemma 8 *For all $l, l' \in \{0, \ldots, \frac{n}{4} - 1\}$, $\mathcal{F}_{-c_n+2l,c_n-l}^{n,2l} \cup \mathcal{F}_{-c_n+2l',c_n-l'}^{n,2l'}$ is an independent set.*

Proof. First note that in set (9), $t + 2i = (-c_n + 2l) + 2(c_n - l)$ is equal to $c_n = n/4 - 1$ and therefore the size of the intersection-spot is $n/4 - 1$ for all subsets. Consider $l, l' \in \{0, \ldots, n/4 - 1\}$, $A \in \mathcal{F}_{-c_n+2l,c_n-l}^{n,2l}$ and $B \in \mathcal{F}_{-c_n+2l',c_n-l'}^{n,2l'}$.

For $2l + 2l' < n/2$: Again, the cardinality of the symmetric difference is less than $n/2$ and so the union of the sets is independent.

For $2l + 2l' \geq n/2$**:** We consider the intersection between A and B in the intersection-spot. As a consequence of Definition 7 we have $|A \cap [n/4 - 1]| \geq l$ and $|B \cap [n/4 - 1]| \geq l'$, therefore A and B will be at least $(l + l' - (n/4 - 1))$-intersection (Inequality (10)). Since we consider the cases where $2l + 2l' \geq n/2$, we have $l + l' \geq n/4$ (Inequality (11)) and the symmetric difference between A and B is the following:

$$\begin{aligned} |A \cup B \setminus A \cap B| &\leq |A| + |B| - 2(l + l' - (\frac{n}{4} - 1)) && (10) \\ &\leq 2l + 2l' - 2(\frac{n}{4} - (\frac{n}{4} - 1)) && (11) \\ &= \frac{n}{2} - 2 \end{aligned}$$

Since this holds for all such A and B, the union set is independent and the lemma follows. Of course, Lemma 7 follows from Lemma 8. □

Lemma 9 *If V_{ind} is an independent set and $v \in V_{ind}$, then $V_{ind} \cup \overline{v}$ is an independent set as well.*

Proof. If V_{ind} is an independent set and $v \in V_{ind}$, then for all $v' \in V_{ind} \setminus \{v\}$, $D_H(v, v') \neq n/2$. Generally $\forall u, w \in \{0,1\}^n : D_H(u, w) = n - D_H(u, \overline{w})$ holds and so for all $v' \in V_{ind} \setminus \{v\}$ is $D_H(\overline{v}, v') = n - D_H(v, v') \neq n/2$ and the proof is complete. □

Proof of Theorem 7. Independence follows directly from Lemmas 7, 8 and 9. We proof that the set is maximal by contradiction. Suppose V_{ind} is not maximal, then by Definition 6, there must exist a vertex $v \in V_{even} \setminus V_{ind}$, such that $V_{ind} \cup \{v\}$ is still an independent set. Since $\mathcal{F}^{n,0}_{-\frac{n}{4}-1,\frac{n}{4}-1} = \{0^n\} \subset V_{ind}$, $W_H(v) \neq n/2$. Furthermore $W_H(v) \notin \{0, 2, \ldots, n/2-2, n/2+2, \ldots, n-2, n\}$, because $\mathcal{F}^{n,2l}_{-c_n+2l,c_n-l}$ are maximal by definition. The the theorem follows. □

5.5 Bounds on the Chromatic Number

Finally, we *assume* that $V^*_{ind} = V_{ind}$ as defined in Equality (9) is a maximum independent set $G_n(V_{even}, E)$.
The size of V^*_{ind} for $2^{\tilde{n}} = n \geq 8$ is

$$|V^*_{ind}| = 2 \sum_{l=0}^{\frac{n}{8}-1} \sum_{m=0}^{l} \binom{\frac{n}{4} - 1}{l + m} \binom{\frac{3n}{4} + 1}{m} +$$

$$2\sum_{l=0}^{\frac{n}{8}-1}\sum_{m=0}^{l}\binom{\frac{n}{4}-1}{\frac{n}{4}-1-l}\binom{\frac{3n}{4}-1}{\frac{n}{4}-1-l-m}. \tag{12}$$

Since the chromatic number $\chi(G_n) \geq n(G_n)/\alpha(G_n)$ and we *assume* that V^*_{ind} is a maximum independent set, we have a lower bound on the chromatic number. Using the the communication complexity bounds for the pseudo-telepathy game stated in Section 5.1 (page 7), we find a bound on the amount of communication we need to win the game. For $\tilde{n} = 4$, $\chi(G_{16}) \geq 27.3$. Therefore we would need at least $\log_2(27.3) - 4 \doteq 0.77$ bit of communication to win the game and therefore simulate the corresponding quantum system.

In the next corollary we use the notation defined in [Brassard 99]. For $\tilde{n} = 4$ have the following:

Corollary 2 *If V^*_{ind} is a maximum independent set, then there exists a pair of sets of measurements, M_A and M_B (each of size 2^{16} on 4 qubits, such that, for the quantum measurement scenario $(|\,\Phi^+\,\rangle^{\oplus 4}_{AB}, M_A, M_B)$ with $|\,\Phi^+\,\rangle^{\oplus 4}_{AB} = \frac{1}{4}\sum_{i\in\{0,1\}^4} |\,i\,\rangle|\,i\,\rangle$, any local variable hidden scheme must be augmented with at least 0.77 bit of communication in order to exactly simulate it.*

Proof. If V^*_{ind} is a maximum independent set, then we have a lower bound on the chromatic number and with Theorem 1 a lower bound on the amount of information needed to win the game. By winning the game we can exactly simulate the quantum measurement scenario depicted in [Brassard 99]. □

Theorem 8 *The chromatic number in $G_n(V, E)$ increases with*

$$c_l^n \leq \chi(G_n) \leq c_u^n$$

for two constants c_l, c_u, with $1 < c_l, c_u < 2$ and $c_l \leq c_u$.

Lemma 10 *The pseudo-telepathy game can be won with $2^{\tilde{n}-1} + 1$ bit of communication for even n.*

Proof. Alice outputs the first $\tilde{n}$ bits of her question and sends the first $n/2 + 1$ bits of her question to Bob. Bob can immediately output the first $\tilde{n} - 1$ bits of Alice's question. Since the questions are either equal or have Hamming-distance $n/2$, Bob knows now if Alice has the same question or not. Therefore, he outputs the $\tilde{n}$-th bit of Alice's question if the questions are equal and its inverse otherwise. They will always win the game with this

strategy and the lemma follows. □

Proof of Theorem 8. Using Theorem 2 and Lemma 10 we have $\log_2 \chi(G_n) - \tilde{n} + 1 \leq 2^{\tilde{n}-1} + 1$. Therefore for $\tilde{n} \geq 4$ we have

$$\log_2 \chi(G_n) \leq 2^{\tilde{n}-1} + \tilde{n} = \frac{1}{2}2^{\tilde{n}} + \tilde{n} \leq \frac{3}{4}2^{\tilde{n}} \tag{13}$$

and by exponentiating Inequality (13) with 2 we have

$$\chi(G_n) \leq 2^{\frac{3}{4}2^{\tilde{n}}} = (2^{\frac{3}{4}})^n$$

and so $2^{3/4} = c_u < 2$ follows.

Theorem 4 in [Brassard 99] states the communication needed to be exchanged is $c2^{\tilde{n}}$, for $c > 0$. Therefore by using Theorem 1 we have

$$\log_2 \chi(G_n) - \tilde{n} \leq c2^{\tilde{n}}$$

and further

$$\chi(G_n) \leq 2^{cn+\tilde{n}} \leq 2^{c'n}$$

for some $n \geq n_0$. Since $c' > c > 0$ we have $1 < 2^{c'} = c_l$ and the theorem holds. □

Now, let us find a lower bound on the maximum independent set.

Corollary 3 *The size of a maximum independent set $\alpha(G_n)$ of $G_n(V, E)$ increases exponentially with $\alpha(G_n) > b^n$, for $1 < b < 2$ and $n \geq n_0$.*

Proof. Since $\chi(G_n) \geq n(G_n)/\alpha(G_n) = 2^n/\alpha(G_n)$[4], we have

$$\alpha(G_n) \geq \frac{2^n}{c_u^n} = \left(\frac{2}{c_u}\right)^n. \tag{14}$$

Inequality (14) holds because of the lower bound on the chromatic number stated in Theorem 8 and the theorem follows with $b = 2/c_u < 2$ and $1 < b$. □

We consider the following theorem:

[4] $n(G_n)$ denotes the number of vertices in G_n.

Theorem 4 in [Brassard 99] *There exists a pair of sets of measurements, M_A and M_B (each of size $2^{2^{\tilde{n}}}$ on $\tilde{n}$ qubits, such that, for the quantum measurement scenario $(\mid \Phi^+ \rangle_{AB}^{\oplus \tilde{n}}, M_A, M_B)$ with $\mid \Phi^+ \rangle_{AB}^{\oplus \tilde{n}} = \frac{1}{\sqrt{2^{\tilde{n}}}} \sum_{i \in \{0,1\}^{\tilde{n}}} \mid i \rangle \mid i \rangle$, any local variable hidden scheme must be augmented with a constant times $2^{\tilde{n}}$ bit of communication in order to exactly simulate it.*

Theorem 4 in [Brassard 99] does not imply that the lower bound obtaining from

$$\chi(G) \geq n(G)/\alpha(G) \tag{15}$$

is asymptotically not optimal. This is because the cardinality of the independent set V^*_{ind}, defined in Equality (9), is increasing exponentially with n (Equation (12)), the maximum independent set will increase exponentially as well (probably the maximum independent set is V^*_{ind}). Moreover we saw in Theorem 8, that $\chi(G_n)$ increases exponentially with a constant $c < 2$. Therefore the bound in Equation (15) can be optimal.

6 Conclusions

We could show that determining the exact amount of communication needed to simulate a specific quantum scenario is in fact a NP-hard problem; namely determining the chromatic number of a specific graph. Now, for the first time we could conjecture an exact lower bound the amount of communication needed in order to exactly simulate the corresponding entangled quantum system, rather than an asymptotical bound. This conjecture claims that certain quantum systems with at least four EPR-pairs cannot be simulated with classical communication.

Our results might be of interest from a quantum and classical point of view. This conjecture is a generalization of the *The Complete Intersection Theorem for Systems of Finite Sets* from Ahlswede and Khachatrian [AK 97] in terms of determining maximum independent sets over several levels. We found color-classes and finally conjectured an exact bound on the chromatic number in this specific graph.

7 Open Problems

It is still to be proven that the maximal independent set V^*_{ind} defined in Equality (9) is a maximum independent set. One approach could be to prove this by considering upper and lower shadows within left-compressed

sets [Comb 86], [AK 97]. If not, then what is the structure of it and its cardinality. This does not imply (and it is not believed), that we can find a good lower bound on the chromatic number by identifying a maximum independent set. One interesting question is to determine the chromatic number of $G_n(V, E)$ or at least a good lower bound on it.

By finding the chromatic number of this graph, we would have the exact amount of information needed to exactly simulate one quantum scenario. From the graph-theoretical point of view, the connection to sparse and dense highly symmetric graphs with high chromatic number seems worth to investigate, since there already exists well-studied graphs of this form. Moreover, the isomorphic hypergraph has a highly symmetric structure as well. Much research has been done investigating hypergraphs (e.g., [Comb 86]) and such graphs are better and better understood. Another approach is to parameterize cliques with different bases of a dual Hamming-code and determining allowed colors of vertices. This could be one way to proof that $\chi(G_{16}(V, E))$ is bigger than 16. From the quantum point of view, it would be interesting to have exact or lower bounds for arbitrary quantum scenarios in order to exactly simulate them.

Even though prediction is difficult — especially of the future — we hope we are soon able to match another piece to the puzzle that surrounds the mysterious phenomenon of quantum entanglement.

Acknowledgments

I would like to thank my parents and sister from the bottom of my heart for their ongoing help and support during my studies. Their commitment to my difficult decisions has been a constant comfort to me. Without their help, I would not have been able to follow my desire and accomplish my goals.

I also would like to thank my supervisor Stefan Wolf. He has guided me through my adventurous trips in quantum worlds and several fields of modern and fundamental mathematics. His confidence me during good and especially in bad times let me feel comfortable in my role as diploma student.

If a man can be judged by the friends he keeps,
I must be the luckiest man in town.
Jon Bon Jovi

The person who accompanied me the past few years and I hope the next journey is my friend Remo. He has been there through (almost :-) all situations that life manifests and presents. I value his great and helpful character. He understood my personality and was advert at asking the right questions when I would get off track.

I deeply thank all my friends — as sister Niccolo — who gave me energy and let me feel at home in their surroundings. Although this diploma thesis has originated in Waterloo, Canada, over 7000 kilometers away from my home, I could still keep a close relationship with my friends in Switzerland and elsewhere in the world. Thank you!

I would like to thank Alain Tapp and Mike Mosca for being interested in my work. The constructive talks always solved a question or raised another very interesting problem.

I want to thank Penny Haxell for the technical and very competent talks. I also thank her for the time and her patience she had with me. I think I would got crazy, if I had to deal with students like myself.

In addition, I would like to thank Carsten Thomassen, Chris Godsil, Gordon Royle and Michael Molloy for taking time to discuss my approaches concerning graphs.

I thank Liam Bali for correcting my thesis and helping to increase the degree of readability.

Finally, I want to thank my former teacher and friend Josef Nigg for always motivating me to see things differently and fundamentally. All the personal and scientific talks with him gave me motivation to set my own trail and to not follow the conventional path.

References

[Bell 64] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics*, Vol. 1, 1964, pp. 195-200.

[Brassard 99] G. Brassard, R. Cleve and A. Tapp, The cost of exactly simulating quantum entanglement with classical communication, quant-ph/9901035, 1999

[Buhr 98] H. Buhrman, R. Cleve and A. Widgerson, Quantum vs. classical communication and computation, *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 98)*, 1998, pp. 63-68

[FranklRödl 87] P. Frankl and V. Rödl, Forbidden intersections, *Transactions of the American Mathematical Society*, Vol. 300, No. 1, 1987, pp. 259-286

[AK 97] R. Ahlswede and H. Khachatrian, The Complete Intersection Theorem for Systems of Finite Sets, *European Journal of Combinatorics*, Vol. 18, 1997, pp. 128-136

[Massar 2000] S. Massar, D. Bacon, N. Cerf and R. Cleve, Classical simulation of quantum entanglement without local hidden variables, quant-ph/0009088, 2000

[Cerf 99] N. Cerf, N. Gisin and S. Massar, Classical Teleportation of a Quantum Bit, *Phys. Rev. Lett.*, Vol. 84,No.11, 2000, pp. 2521-2524. Also available at quant-ph/9906105, 1999

[Steiner 99] M. Steiner, Towards quantifying non-local information transfer: Finite-bit non-locality, quant-ph/9902014v2, 1999

[Bollobás 78] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1978

[DeutschJozsa 92] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, *Proceedings of the Royal Society of London*, Series A, Vol. 439, 1992, pp. 553-558

[vanLint 82] J. H. van Lint, *Introduction to Coding Theory*, Springer Verlag, 1982

[Comb 86] B. Bollobás, *Combinatorics*, Cambridge University Press, 1986