Quantum Secret Sharing with Graph States

Sylvain Gravier[1,2], Jérôme Javelle[3], Mehdi Mhalla[1,3], and Simon Perdrix[1,3]

[1] CNRS
[2] Institut Fourier, University of Grenoble, France
[3] LIG, University of Grenoble, France

Keywords: Quantum Information, Graph Theory, Quantum Cryptography, NP-Completeness

Abstract. We study the graph-state-based quantum secret sharing protocols [24, 17] which are not only very promising in terms of physical implementation, but also resource efficient since every player's share is composed of a single qubit. The threshold of a graph-state-based protocol admits a lower bound: for any graph of order n, the threshold of the corresponding n-player protocol is at least $0.506n$. Regarding the upper bound, lexicographic product of the C_5 graph (cycle of size 5) are known to provide n-player protocols which threshold is $n - n^{0.68}$. Using Paley graphs we improve this bound to $n - n^{0.71}$. Moreover, using probabilistic methods, we prove the existence of graphs which associated threshold is at most $0.811n$. Albeit non-constructive, probabilistic methods permit to prove that a random graph G of order n has a threshold at most $0.811n$ with high probability. However, verifying that the threshold of a given graph is acually smaller than $0.811n$ is hard since we prove that the corresponding decision problem is NP-Complete. These results are mainly based on the graphical characterization of the graph-state-based secret sharing properties, in particular we point out strong connections with domination with parity constraints.

1 Introduction

1.1 Quantum secret sharing

Secret sharing schemes were independently introduced by Shamir [33] and Blakley [3] and extended to the quantum case by Hillery [14] and Gottesman [8, 10]. A quantum secret sharing protocol consists in encoding a secret into a multipartite quantum state. Each of the players of the protocol has a *share* which consists of a subpart of the quantum system and/or classical bits. *Authorized* sets of players are those that can recover the secret collectively using classical and quantum communications. A set of players is *forbidden* if they have no information about the secret. The encrypted secret can be a classical bit-string or a quantum state.

A *threshold* ((k, n)) quantum secret sharing protocol [14, 8, 10] is a protocol by which a dealer distributes shares of a quantum secret to n players such that any subset of at least k players is authorized, while any set of less than k players is forbidden. It is assumed that the dealer has only one copy of the quantum

secret he wants to share. A direct consequence of the no-cloning theorem [36] is that no $((k, n))$ quantum secret sharing protocol can exists when $k \leq \frac{n}{2}$ – otherwise two distinct sets of players can reconstruct the secret implying a cloning of the quantum secret. On the other hand, for any $k > \frac{n}{2}$ a $((k, n))$ protocol has been introduced in [8] in such a way that the dimension of each share is proportional to the number of players. The unbounded size of the share is a serious drawback of the protocol, as a consequence several schemes of quantum secret sharing using a bounded amount of resources for each player have been introduced [24, 4, 20].

1.2 Graph-state-based quantum secret sharing

In [24] a quantum secret sharing scheme using particular quantum states, called *graph states* [12], and such that every player receives a single qubit, has been introduced. The graph-state-based protocols are also of interest because graph states are at the forefront in terms of implementation and have emerged as a powerful and elegant family of entangled states [13, 30].

As introduced in [24], only one non-trivial graph (the cycle of size 5) corresponds to a threshold protocol. In [17], the graph-state-based protocol has been extended to ensure that any graph correspond to a threshold protocol. Given a graph G, the threshold of the corresponding protocol is $\kappa_Q(G)$. This threshold is characterized graphically by the notion of weak odd domination. In [17], it has been proved that for any graph G of order n, $\kappa_Q(G) > 0.506n$, refining the no-cloning theorem. This bound is not known to be tight. All known constructions of graph-state-based quantum secret sharing protocols lead to quasi-uninimity protocols (i.e. the threshold is $n - o(n)$, where n is the number of players). The best known construction is based on the lexicographic product of graphs, and leads to protocols with a threshold $n - n^{0.68}$ [17].

We improve this threshold to $n - n^{0.71}$ using Paley graphs. Moreover, we show, using probabilistic methods, that for any (large enough) n there exists a graph G of order n such that $\kappa_Q(G) \leq 0.811n$. The proof is not constructive, but it crucially shows that graph-state based quantum secret sharing protocols are not restricted to quasi-unanimity thresholds. We actually prove that almost all the graphs have such a 'small' κ_Q: if one picks a random graph G of order n (every edge occurs with probability 1/2), then $\kappa_Q(G) \leq 0.811n$ with probability greater than $1 - \frac{1}{n}$. We also prove that, given a graph G and a parameter k, deciding whether $\kappa_Q(G) \geq k$ is NP-complete. As a consequence, one cannot efficiently verify that a particular randomly generated graph has actually a 'small' κ_Q.

1.3 Combinatorial properties of graph states.

The development and the study of graph-based protocols [24, 20, 17, 31, 16] have already pointed out deep connections between graph theory and quantum

information theory. For instance, it has been shown [19] that a particular notion of flow [9, 5, 26, 25] in the underlying graph captures the flow, during the protocol, of the information contained in the secret from the dealer – who encodes the secret and sends the shares – to the authorized sets of players. The results presented in this paper contribute to these deep connections: we show that weak odd domination is a key concept for studying the properties of graph-based quantum secret sharing protocols.

The study of graph-state-based protocols also contributes, as a by-product, to a better understanding of the combinatorial properties of the graph states. The graph state formalism is a very powerful tool which is used in several areas of quantum information processing. Graph states provide a universal resource for quantum computing [30, 34, 27] and are also used in quantum correction codes [32, 6] for instance. They are also used to define pseudo-telepathy games [1]. Moreover, they are very promissing in terms of physical implementation [29, 35]. As a consequence, progresses in the knowledge of the fundamental properties of graph states can potentially impact not only quantum secret sharing but a wide area of quantum information processing.

2 Graph state secret sharing

2.1 Graph states

For a given graph $G = (V, E)$ with vertices $v_1, \ldots, v_n$, the corresponding graph state $|G\rangle$ is a n-qubit quantum state defined as

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q(x)} |x\rangle$$

where $q(x)$ is the number of edges in the induced subgraph $G[x] = (\{v_i \in V \mid x_i = 1\}, \{(v_i, v_j) \in E \mid x_i = x_j = 1\})$.

Graph states have the following fundamental fixpoint property: given a graph G, for any vertex $u \in V$,

$$X_u Z_{N(u)} |G\rangle = |G\rangle$$

where $N(u)$ is the neighborhood of u in G, $X = |x\rangle \mapsto |\bar{x}\rangle$, $Z = |x\rangle \mapsto (-1)^x |x\rangle$ are one-qubit Pauli operators and $Z_A = \bigotimes_{u \in A} Z_u$ is a Pauli operator acting on the qubits in A.

2.2 Sharing a classical secret using a graph state

Graph-state-based classical sharing protocols have been introduced in [24]. In these protocols a classical secret is shared by means of a quantum state. The authorized sets of players are those which are satisfying the following graphical property, called *c-accessibility*:

Definition 1. *Given a graph $G = (V, E)$, a set $B \subseteq V$ of vertices is* c-accessible *if $\exists D \subseteq B$ such that $|D| = 1 \bmod 2$ and $Odd(D) \subseteq B$, where $Odd(D) := \{v \in V \mid |N(v) \cap D| = 1 \bmod 2\}$.*

Given a graph $G = (V, E)$ of order n, the **graph state-based protocol for sharing a classical secret** $s \in \{0, 1\}$ among n players is defined as:

1. **Encryption.** The dealer prepares the graph state $|G\rangle$. If $s = 1$ the dealer applies Z_V on the qubits of the graph state. The resulting state is
$$|G_s\rangle := Z_V^s |G\rangle$$
2. **Distribution.** Player j's share is qubit j of $|G_s\rangle$.
3. **Reconstruction.** Let B be a c-accessible set of player, with $D \subseteq B$ such that $|D| = 1 \bmod 2$ and $Odd(D) \subseteq B$.
   - The players in $Odd(D)$ apply $S = |x\rangle \mapsto i^x |x\rangle$ on their qubit.
   - The players in D apply $H = |x\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$ on their qubit.
   - Each player $j \in D \cup Odd(D)$ measures his qubit in the $\{|0\rangle, |1\rangle\}$-basis and broadcasts his result $s_i \in \{0, 1\}$ to the players in B.
   - The reconstructed secret is
$$|G_D| + \sum_{j \in D \cup Odd(D)} s_j \bmod 2$$
   where $|G_D|$ is the size (i.e. the number of edges) of the subgraph induced by D.

Proof of the protocol [Sketch]. The proof that the reconstructed secret is the actual secret relies on the fact that for any $D \subseteq V$, $(-1)^{|G_D|} X_D Z_{Odd(D)} |G\rangle = |G\rangle$, as a consequence $(-1)^{|G_D|} X_D Z_{Odd(D)} |G_s\rangle = (-1)^s |G_s\rangle$, so a measurement according to $X_D Z_{Odd(D)}$ produces the classical outcome $s + |G_D| \bmod 2$. Finally, the non local measurement according to $X_D Z_{Odd(D)}$ can be decomposed into local measurements such that the parity of the local measurements is the same as the outcome of the non-local measurement. □

Sharing a classical bit can be done using a classical scheme, like [33], instead of using a quantum state. Moreover the above protocol can be simulated by purely classical graph-based schemes [16]. However, the study of the graph-state-based classical secret sharing, and in particular the characterization of their authorized structure are essential for the next sections where the sharing of a quantum secret is considered.

The graph-state-based classical secret sharing protocol is *perfect*, i.e. any set of players is either c-accessible, or has no information about the secret [17].

The proof of perfectness has two steps: using graph theory arguments, one can prove that if a set B of players is not c-accessible in a graph, then B is a WOD set (WOD stands for *weak odd domination*), i.e. there exists $C \subseteq V \setminus B$ such that $B \subseteq Odd(C)$. The second part of the proof consists in proving that the reduced density matrix of a WOD set of players does not depend on the secret, thus the players in this set have no information about the secret [19].

Since any subset of a WOD set is a WOD set and that any superset of a c-accessible is a c-accessible set, the important quanties for a graph state-based classical secret sharing protocol are the largest WOD set and the smallest c-accessible set by considering the following quantities:

Definition 2. *For a given graph G, let*

$$\kappa(G) = \max_{B \ WOD} |B| \qquad \kappa'(G) = \min_{B \ c\text{-}accessible} |B|$$

For instance, for a C_5 graph, i.e. a cycle of size 5, $\kappa(C_5) = 2$ and $\kappa'(C_5) = 3$. So it means that any set of at least 3 players can recover the secret whereas any set of at most 2 players have no information about the secret. In other words, the C_5 graph induces a threshold protocol. Another example is the complete graph K_n. Since $\kappa(K_n) = n - 1$ and $\kappa'(K_n) = n$, complete graphs induce unanimity protocol.

We consider a third example: for any $p, q \in \mathbb{N}$, let $G_{p,q}$ be the complete q-partite graph where each independent set is of size p: the vertices of $G_{p,q}$ are pairs (i, j), with $0 \leq i < p$, $0 \leq j < q$, two vertices (i, j), (i', j') are connected if and only if $j \neq j'$. $G_{p,q}$ is of order $n = pq$.

Lemma 1. *For any $p, q \in \mathbb{N}$,*

$$\begin{array}{rl} \kappa(G_{p,q}) = n - p \text{ and } \kappa'(G_{p,q}) = q & \text{if } q = 1 \bmod 2 \\ \kappa(G_{p,q}) = \max(n-p, n-q) \text{ and } \kappa'(G_{p,q}) = p + q + 1 & \text{if } q = 0 \bmod 2 \end{array}$$

Proof. If $q = 1 \bmod 2$

- $[\kappa(G_{p,q}) \geq n - p]$: The subset B composed of all the vertices but a maximal independent set (MIS) – i.e. an independent set of size p – is in the odd neighborhood of each vertex in $V \setminus B$. Therefore B is WOD and $|B| = n - p$. Consequently $\kappa(G_{p,q}) \geq n - p$.

- $[\kappa(G_{p,q}) \leq n - p]$: Any set B such that $|B| > n - p$ contains at least one vertex from each of the q MIS, i.e. a clique of size q. Let $D \subseteq B$ be such a clique of size $|D| = q = 1 \bmod 2$. Every vertex v outside D is connected to all the elements of D but the one in the same MIS as v. Thus $Odd(D) = \emptyset$. As a consequence, B is non-WOD.

– $[\kappa'(G_{p,q}) \leq q]$: B composed of one vertex from each MIS is a non-WOD set (see previous item).

– $[\kappa'(G_{p,q}) \geq q]$: If $|B| < q$ then B does not intersect all the MIS of size p, so B is in the odd neighborhood of each vertex of such a MIS. So B is WOD.

If $q = 0 \bmod 2$

– $[\kappa(G) \geq max(n-p, n-q)]$: For $\kappa(G) \geq n-p$, see previous lemma. The subset B composed of all the vertices but a clique of size q (one vertex from each MIS) is in the odd neighborhood of $V \setminus B$. Indeed each vertex of B is connected to $q-1 = 1 \bmod 2$ vertices of $V \setminus B$. So B of size $n-q$ is WOD, as a consequence $\kappa(G) \geq n-q$.

– $[\kappa(G) \leq max(n-p, n-q)]$: Any set B such that $|B| > max(n-p, n-q)$ contains at least one vertex from each MIS and moreover it contains a MIS S of size q. Let $D \subseteq B \setminus S$ be a clique of size $q-1 = 1 \bmod 2$. Every vertex u in $V \setminus B$ is connected to all the vertices in D but one, so $Odd(D) \subseteq B$.

– $[\kappa'(G) \leq p+q-1]$: Let S be an MIS. Let B be the union of S and of a clique of size q. Let $D = B \setminus S$. $|D| = q-1 = 1 \bmod 2$. Every vertex u in $V \setminus B$ is connected to all the vertices of D but one, so $Odd(D) \subseteq B$.

– $[\kappa'(G) \geq p+q-1]$: Let $|B| < p+q-1$. If B does not intersect all the MIS of size p, then B is in the odd neighborhood of each vertex of such a non intersecting MIS. If B intersects all the MIS then it does not contain any MIS, thus there exists a clique $C \subseteq V \setminus B$ of size q. Every vertex in B is in the odd neighborhood of C.

□

2.3 Sharing a quantum secret

Graph state based classical secret sharing can be extended to the quantum case as follows (the encryption method has been introduced in [24], and for the reconstruction method in [17]):

Given a graph G of order n, the **graph state-based protocol for sharing a quantum secret** $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ among n players is:

1. **Encryption.** The dealer prepares the quantum state $\alpha|G_0\rangle + \beta|G_1\rangle$ where $|G_0\rangle := |G\rangle$ and $|G_1\rangle := Z_V|G\rangle$.
2. **Distribution.** Player i's share is qubit i of $\alpha|G_0\rangle + \beta|G_1\rangle$.
3. **Reconstruction.** Let B be a c-accessible set of players such that $V \setminus B$ is WOD. So $\exists C, D \subseteq B$ such that $V \setminus B \subseteq Odd(C)$, $|D| = 1 \bmod 2$, and $Odd(D) \subseteq B$.
   - Players in B choose $u \in B$ who will reconstruct the secret. Every player in $B \setminus \{u\}$ sends his qubit to u.
   - u applies the unitary $\frac{1}{\sqrt{2}}\left(\begin{array}{c|c} I & U \\ \hline -U & I \end{array}\right)$ where $U = (-1)^{|G_D|}X_D Z_{Odd(D)}$ on the $(|B|+1)$-qubit system composed of an ancillary qubit $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and the received qubits. The resulting state of the $(n+1)$-qubit system is
   $$\alpha|0\rangle \otimes |G_0\rangle + \beta|1\rangle \otimes |G_1\rangle$$
   - u applies the unitary $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & U' \end{array}\right)$ where $U' = (-1)^{|G_C|}X_C Z_{V\setminus Odd(C)}$. The resulting state of the $(n+1)$-qubit system is
   $$(\alpha|0\rangle + \beta|1\rangle) \otimes |G\rangle$$
   Thus the secret is reconstructed on the first qubit.

In this protocol of graph-state based quantum secret sharing, the authorized sets of players are c-accessible such that their complementary sets are WOD. Intuitively the c-accessibility allows the players to extend the superposition to an ancillary qubit (i.e. to transform the state $\alpha|G_0\rangle + \beta|G_1\rangle$ to $\alpha|0\rangle \otimes |G_0\rangle + \beta|1\rangle \otimes |G_1\rangle$). Notice that if the secret is classical (either α or β is equal to 0), then the state of the ancillary qubit is nothing but the secret. In the general case, when the secret is a superposition, the ancillary qubit is entangled with the rest of the system. The second requirement, namely that the complementary set $V \setminus B$ is WOD allows the players in B to make the ancillary qubit separable from the rest of system, producing the state $(\alpha|0\rangle + \beta|1\rangle) \otimes |G\rangle$.

Since authorized players are c-accessing such that their complementary are WOD, the important quantity for graph-state based quantum secret sharing protocols is

$$\kappa_Q(G) = \max(\kappa(G), n - \kappa'(G))$$

Indeed any set B of players such that $|B| > \kappa_Q(G)$ is c-accessing since $|B| > \kappa(G)$ and its complementary set is WOD since $|V \setminus B| < \kappa'(G)$.

2.4 Threshold schemes

Notice that the graph-state based quantum secret sharing are not perfect in general. One can prove that the authorized sets are those which are c-accessible such that their complementary set is WOD [17]. On the otherhand, if a set is WOD and its complementary is c-accessible, then such a set has no information about the secret. But all sets which are not of that kind, for instance those such that both B and $V \setminus B$ are c-accessible, have some partial information about the secret.

To make the protocol perfect, and even to obtain a threshold protocol, a variant of the previous protocol has heen introduced in [17]. The idea is to add a one-time padding of the secret to ensure that the sets of players which size is below the threshold have no information about the secret. To implement this one-time padding the previous protocol is coupled with a classical protocol for sharing the classical key of the one-time padding.

Given a graph G and an integer $k > \kappa_Q(G)$ the **threshold graph state-based protocol for sharing a quantum secret** $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ among n players is:

1. **Encryption.** The dealer chooses uniformly at random two bits $p, q \in \{0,1\}$ and applies X^pZ^q to the secret. The resulting state is $\alpha|p\rangle + \beta(-1)^q|1-p\rangle$. Then, the dealer prepares the quantum state $\alpha|G_p\rangle + (-1)^q\beta|G_{1-p}\rangle$.
2. **Distribution.** Player i's share is qubit i of $\alpha|G_p\rangle + (-1)^q\beta|G_{1-p}\rangle$. Moreover p and q are shared among the n players using a classical secret sharing protocol (not described here) with threshold k.
3. **Reconstruction.** For any B such that $|B| \geq k$, since $|B| > \kappa_Q(G)$, $\exists C, D \subseteq B$ such that $V \setminus B \subseteq Odd(C)$, $|D| = 1 \bmod 2$, and $Odd(D) \subseteq B$.
   - Players in B choose $u \in B$ who will receive the secret. Every player in $B \setminus \{u\}$ sends his qubit to u.
   - u applies $\frac{1}{\sqrt{2}}\left(\begin{array}{c|c} I & U \\ \hline -U & I \end{array}\right)$ where $U = (-1)^{|G_D|}X_DZ_{Odd(D)}$ and then $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & U' \end{array}\right)$ where $U' = (-1)^{|G_C|}X_CZ_{V\setminus Odd(C)}$. The resulting state is
   $$(\alpha|p\rangle + \beta(-1)^q|1-p\rangle) \otimes |G\rangle$$
   - Using the classical secret sharing protocol, the players in B reconstructs the classical bits p and q.
   - u applies Z^qX^p to the ancillary qubit. The resulting state is $\alpha|0\rangle + \beta|1\rangle$.

This protocol is a $((k, n))$ threshold quantum secret sharing protocol. Indeed for any set of at most $k-1$ players, they have no information about the classical keys p and q which garantees that they have no information about the quantum secret. For the sets of at least k players, since $k > \kappa_Q(G)$, they can reconstruct the state $\alpha |p\rangle + \beta(-1)^q |1-p\rangle$, like in the previous protocol, moreover they have access to the keys p and q, so they can reconstruct the quantum secret.

2.5 Lower bound and quasi-unanimity protocols

Graph-state-based secret sharing protocols are very promising in terms of physical implementations [29, 35], moreover, contrary to the family of quantum secret sharing introduced by Gottesman [10], the size of each quantum share does not depend on the number of players. The drawback is that some threshold protocols cannot be implemented using a graph-state-based protocol:

Lemma 2 (Lower bound [17]). *For any graph G of order $n > 5$,*

$$\kappa_Q(G) > 0.506n$$

Notice that for any quantum secret sharing scheme, if there is a threshold, this threshold must be larger than $n/2$. This bound [10] is a direct application of the no-cloning theorem: if $k < n/2$ then two distinct sets of k players can recover the quantum secret, leading to a cloning of the quantum secret. The lower bound for graph-state-based protocols is not known to be tight.

Regarding the upper bound, all known constructions of graph-state-based quantum secret sharing protocols are quasi-unanimity protocols. In the next section, we will prove using non constructive methods that for any n there exists a graph G of order n such that $\kappa_Q(G) < 0.811n$.

Thanks to lemma 1, for any $p, q \in \mathbb{N}$, the complete q-partite graph $G_{p,q}$ of order $n = pq$ (see section 2.2), $\kappa_Q(G_{p,q}) = \max(n-p, n-q)$. Thus, for any square number n, $\kappa_Q(G_{\sqrt{n},\sqrt{n}}) = n - \sqrt{n}$. The corresponding secret sharing protocol is a quasi-unanimity protocol since the ratio k/n tends to 1 as n tends to infinity.

The best known construction is based on the lexicographic product of graphs: Given $G = (V, E)$ $G \bullet G = (V', E')$ is defined as $V' := V \times V$ and $E' := \{((u_1, u_2), (v_1, v_2)) \mid (u_1, v_1) \in E \text{ or } (u_1 = v_1 \wedge (u_2, v_2) \in E)\}$.

Lemma 3 ([17]). *For any graph G, of order n*

$$\kappa_Q(G \bullet G) \leq 2n.\kappa_Q(G) - \kappa_Q(G)^2$$

Graphs-state-based quantum secret sharing protocols with threshold $n - n^{0.68}$, where n is the number of players, can be obtained using inductively the lexicographic product of C_5 graph (cycle on five vertices) [17].

In fact, the C_5 graph is a particular case of a family of graphs called Paley graphs, that have been used recently in [18] to provide the best known upper bound for the minimum degree up to local complementation which can be defined as $\min_{D \subseteq V, D \neq \emptyset} |D \cup Odd(D)| - 1$.

For any prime p such that $p = 1 \bmod 4$, the Paley graph Pal_p is a graph on p vertices where each vertex is an element of $\mathbb{F}_p$. There is an edge between two vertices i and j if and only if $i - j$ is a square in $\mathbb{F}_p$.

Graphs-state-based quantum secret sharing protocols with n players and threshold $n - n^{0.71}$ is obtained using the lexicographic product of Pal_{29} graphs. This is, up to our knowledge, the best known constructive threshold.

Theorem 1. *For any $i > 0$,*

$$\kappa_Q({Pal_{29}}^{\bullet^i}) \leq n - n^{\frac{\log(11)}{\log(29)}} \approx n - n^{0.71}$$

where ${Pal_{29}}^{\bullet^1} = Pal_{29}$, ${Pal_{29}}^{\bullet^i} = {Pal_{29}}^{\bullet^{i-1}} \bullet {Pal_{29}}^{\bullet^{i-1}}$ and $n = 29^{2^i}$ is the order of the graph.

Proof. $\kappa_Q(Pal_{29})$ is computed taking benefits of the symmetries of the Paley graphs (strong regularity, vertex transitivity, edge transitivity, self complementarity). The evolution with the lexicographic product is given by lemma 3. □

It is significant and interesting to notice that the conjecture of the existence of an infinite family of Paley graphs leading to non quasi-unanimity protocols is related to the Bazzi-Mitter conjecture [2].

3 Graphs with small κ_Q

In this section, we prove the existence of graph-state-based secret sharing protocols which are not quasi-unanimity. More precisely, using the asymmetric Lovász Local Lemma [23] we show that there exists an infinite family of graphs $\{G_i\}$ such that $\kappa_Q(G_i) \leq 0.811 n_i$ where n_i is the order of G_i. Moreover, we prove that a random graph $G(n, 1/2)$ (graph on n vertices where each pair of vertices have probability $1/2$ to have an edge connecting them) satisfies $\kappa_Q(G(n, 1/2)) \leq 0.811n$ with high probability.

First we prove the following lemma:

Lemma 4. *Given k and $G = (V, E)$, if for any non empty set $D \subseteq V$, $|D \cup Odd(D)| > n - k$ and $|D \cup (V \setminus Odd(D))| > n - k$ then $\kappa_Q(G) < k$.*

Proof. Since $\forall D \subseteq V \ |D \cup Odd(D)| > n-k$, $\kappa'(G) > n-k$. Let $B \subseteq V$, $|B| \geq k$, if B is not WOD then $\exists C \subseteq V \setminus B$ such that $B \subseteq Odd(C)$, so $(V \setminus Odd(C)) \subseteq V \setminus B$ which implies $|C \cup (V \setminus Odd(C))| \leq n-k$. □

We use the asymmetric form of the Lovász Local Lemma that can be stated as follows:

Theorem 2 (Asymmetric Lovász Local Lemma, no independency case). *Let $\mathcal{A} = \{A_1, \cdots, A_n\}$ be a set of bad events in an arbitrary probability space. If for every A_i there exists $w(A_i) \in [0,1)$ such that $Pr(A_i) \leq w(A_i).p$, where $p = \prod_{A_j \in \mathcal{A}}(1-w(A_j))$ then $Pr(\overline{A_1}, \cdots, \overline{A_n}) \geq p$*

Theorem 3. *There exists an infinite family of graphs $\{G_i\}$ such that $\kappa_Q(G_i) \leq 0.811 n_i$ where n_i is the order of G_i.*

Proof. Let $G(n, 1/2) = (V, E)$ be a random graph. We use the asymmetric Lovász local lemma to show that the probability that for all non empty set $D \subseteq V \ |D \cup Odd(D)| > (1-c)n$ and $|D \cup (V \setminus Odd(D))| > (1-c)n$ is positive for some constant c. This ensures by Lemma 4 that $\kappa_Q(G) < cn$.

We consider the "bad" events A_D : $|Odd(D) \cup D| \leq (1-c)n$ and A'_D : $|Odd(D) \cup (V \setminus Odd(D))| \leq (1-c)n$. When $|D| > (1-c)n$, $Pr(A_D) = Pr(A'_D) = 0$, therefore the previous events are defined for all D such that $|D| \leq (1-c)n$.

For all D such that $|D| \leq (1-c)n$, we want to get an upper bound on $Pr(A_D)$. Let $|D| = dn$ for some $d \in (0, 1-c]$. For all $u \in V \setminus D$, $Pr(\text{“}u \in Odd(D)\text{”}) = \frac{1}{2}$. If D is fixed, the events “$u \in Odd(D)$” when u is outside D are independent. Therefore, if the event A_D is true, any but at most $(1-c-d)n$ vertices outside D are contained in $Odd(D)$. There are $(1-d)n$ vertices outside D, then $Pr(A_D) = \left(\frac{1}{2}\right)^{(1-d)n} \sum_{k=0}^{(1-c-d)n} \binom{(1-d)n}{k} \leq \left(\frac{1}{2}\right)^{(1-d)n} 2^{(1-d)nH\left(\frac{1-c-d}{1-d}\right)} = 2^{(1-d)n\left[H\left(\frac{c}{1-d}\right)-1\right]}$ where $H : t \mapsto -t\log_2(t) - (1-t)\log_2(1-t)$ is the binary entropy function. Similarily, $Pr(A'_D) \leq 2^{(1-d)n\left[H\left(\frac{c}{1-d}\right)-1\right]}$.

We consider that all the events can be dependent. For any $D \subseteq V$ such that $0 < |D| \leq (1-c)n$, we define $w(A_D) = w(A'_D) = \frac{1}{r\binom{n}{|D|}}$. First, we verify that $Pr(A_D) \leq w(A_D) \prod_{D' \subseteq V, |D| \leq (1-c)n}(1-w(A_{D'}))(1-w(A'_{D'}))$. The product of the right-hand side of the previous equation can be written $p = \prod_{|D'|=1}^{(1-c)n}\left(1 - \frac{1}{r\binom{n}{|D'|}}\right)^{2\binom{n}{|D'|}} = \left[\prod_{|D'|=1}^{(1-c)n}\left(1 - \frac{1}{r\binom{n}{|D'|}}\right)^{r\binom{n}{|D'|}}\right]^{\frac{2}{r}}$. The function $f : x \mapsto \left(1-\frac{1}{x}\right)^x$ verifies $f(x) \geq \frac{1}{4}$ when $x \geq 2$, therefore $p \geq \left(\frac{1}{4}\right)^{\frac{2}{r}(1-c)n} = 2^{-\frac{4(1-c)n}{r}}$ for any $r \geq 2$. Thus, it is sufficient to have $2^{(1-d)n\left[H\left(\frac{c}{1-d}\right)-1\right]} \leq \frac{1}{r\binom{n}{dn}} 2^{-\frac{4(1-c)n}{r}}$. Rewriting this inequality gives $r\binom{n}{dn} 2^{(1-d)n\left[H\left(\frac{c}{1-d}\right)-1\right]+\frac{4(1-c)n}{r}} \leq 1$. Thanks to the bound $\binom{n}{dn} \leq 2^{nH\left(\frac{dn}{n}\right)}$ and after applying the logarithm function and dividing by n, it is sufficient that $(1-d)\left[H\left(\frac{c}{1-d}\right) - 1\right] + H(d) +$

$\frac{4(1-c)}{r} + \frac{\log_2 r}{n} \leq 0$. If we take $r = n$, the condition becomes asymptotically $(1-d)\left[H\left(\frac{c}{1-d}\right) - 1\right] + H(d) \leq 0$.

Numerical analysis shows that this condition is true for any $c > 0.811$ and for all $d \in (0, 1-c]$. Thus, thanks to the Lovász Local Lemma, for any $c > 0.811$, $Pr(\kappa_Q(G) < cn) \geq p \geq \left(\frac{1}{4}\right)^{\frac{2}{r}(1-c)n} > 0$, therefore there exists an infinite family of graphs $\{G_i\}$ such that $\kappa_Q(G_i) \leq 0.811 n_i$ where n_i is the order of G_i for $n_i \geq N_0$ for some $N_0 \in \mathbb{N}$. □

Recently [31], Sarvepalli proved that quantum secret sharing protocols based on graph states are equivalent to quantum codes. Combining this result with the Gilbert Varshamov bounds on quantum stabilizer codes [11], we can provide an alternative proof of theorem 3. However, we believe the use of the Lovász Local Lemma offers several advantages: the proof is a purely graphical proof with a potential extension to the construction of good quantum secret sharing schemes using the recent development in the algorithmic version [28] of the Lovász Local Lemma. Moreover, the use of the probabilistic methods already offers a way of generating good quantum secret sharing protocols with high probability by adjusting the parameters of the Lovász Local Lemma:

Theorem 4. *There exists n_0 such that for any $n > n_0$, a random graph $G(n, \frac{1}{2})$ has a κ_Q smaller than $0.811n$ with high probability:*

$$Pr\left(\kappa_Q(G(n, \frac{1}{2})) < 0.811n\right) \geq 1 - \frac{1}{n}$$

Proof. The proof of the theorem is done as in the proof of theorem 3, by taking $c = 0.811$ and $r = 4\ln(2)(1-c)n^2$. It guarantees that for $n \geq 26681$, $(1-d)\left[H\left(\frac{c}{1-d}\right) - 1\right] + H(d) + \frac{4(1-c)}{r} + \frac{\log_2 r}{n} \leq 0$. Thus, for any $D \subseteq V$ such that $0 < |D| \leq (1-c)n$, $Pr(A_D) \leq w(A_D) \prod_{D' \subseteq V, |D| \leq (1-c)n} (1 - w(A_{D'}))(1 - w(A'_{D'}))$. Moreover the probability that none of the bad events occur is $Pr\left(\kappa_Q(G(n, \frac{1}{2})) < 0.811n\right) \geq \left(\frac{1}{4}\right)^{\frac{2}{r}(1-c)n} = \left(\frac{1}{4}\right)^{\frac{1}{2n\ln(2)}} = e^{-\frac{1}{n}} \geq 1 - \frac{1}{n}$. □

4 Complexity of computing the threshold of graph-state-based protocols

According to Theorem 4, a random graph $G(n, 1/2)$ induces a secret sharing protocol with a threshold smaller than $0.811n$ with high probability: $Pr\left(\kappa_Q(G(n, \frac{1}{2})) < 0.811n\right) \geq 1 - \frac{1}{n}$. So even if the Lovász local Lemma is not constructive, one can pick uniformly at random a graph G of order n, if $\kappa_Q(G) \geq 0.811n$, he picks another one and so on. Since the probability that $\kappa_Q(G) \geq 0.811n$ this procedure seems to be efficient, however the crucial point

here is the complexity of deciding whether $\kappa_Q(G) \geq 0.811n$ or not. In this section we consider the complexity of this problem and show that the problem is NP-complete (Theorem 10). To prove this result we introduce several bounds and complexity results on weak odd domination, and in particular on the quantities $\kappa(G)$, $\kappa'(G)$ and $\kappa_Q(G)$ of a graph G.

First, we show that the sum of $\kappa(G)$ and $\kappa'(\overline{G})$ is always greater than the order of the graph G. The proof is based on the duality property that the complement of a non-WOD set in G is a WOD set in $\overline{G}$, the complement graph of G.

Lemma 5. *Given a graph $G = (V, E)$, if $B \subseteq V$ is not a WOD set in G then $V \setminus B$ is a WOD set in $\overline{G}$.*

Proof. Let B be a non-WOD set in G. $\exists D \subseteq B$ such that $|D| = 1 \bmod 2$ and $Odd_G(D) \subseteq B$. As a consequence, $\forall v \in V \setminus B$, $|N_G(v) \cap D| = 0 \bmod 2$. Since $|D| = 1 \bmod 2$, $\forall v \in V \setminus B$, $|N_{\overline{G}}(v) \cap D| = 1 \bmod 2$. Thus, $V \setminus B$ is a WOD set in $\overline{G}$. □

Theorem 5. *For any graph G of order n, $\kappa'(G) + \kappa(\overline{G}) \geq n$.*

Proof. There exists a non-WOD set $B \subseteq V$ such that $|B| = \kappa'(G)$. According to Lemma 5, $V \setminus B$ is WOD in $\overline{G}$, so $n - |B| \leq \kappa(\overline{G})$, so $n - \kappa'(G) \leq \kappa(\overline{G})$. □

For any vertex v of a graph G, its (open) neighborhood $N(v)$ is a WOD set, whereas its closed neighborhood (i.e. $N[v] = \{v\} \cup N(v)$) is a non-WOD set, as a consequence:

$$\kappa(G) \geq \Delta \qquad\qquad \kappa'(G) \leq \delta + 1$$

where Δ (resp. δ) denotes the maximal (resp. minimal) degree of the graph G.

In the following, we prove an upper bound on $\kappa(G)$ and a lower bound on $\kappa'(G)$.

Lemma 6. *For any graph G of order n and degree Δ, $\kappa(G) \leq \frac{n.\Delta}{\Delta+1}$.*

Proof. Let $B \subseteq V$ be a WOD set. $\exists C \subseteq V \setminus B$ such that $B \subseteq Odd(C)$. $|C| \leq n - |B|$ and $|B| \leq |Odd(C)| \leq \Delta.|C|$, so $|B| \leq \Delta.(n - |B|)$. It comes that $|B| \leq \frac{n.\Delta}{\Delta+1}$, so $\kappa(G) \leq \frac{n.\Delta}{\Delta+1}$. □

In the following we prove that this bound is reached only for graphs having a perfect code. A graph $G = (V, E)$ has a perfect code if there exists $C \subseteq V$ such that C is an independent set and every vertex in $V \setminus C$ has exactly one neighbor in C.

Theorem 6. *For any graph G of order n and degree Δ, $\kappa(G) = \frac{n.\Delta}{\Delta+1}$ if and only if G has a perfect code C such that $\forall v \in C$, $d(v) = \Delta$.*

Proof. ($\Leftarrow$) Let C be a perfect code of G such that $\forall v \in C$, $\delta(v) = \Delta$. $V \setminus C$ is a WOD set since $Odd(C) = V \setminus C$. Moreover $|V \setminus C| = \frac{n\Delta}{\Delta+1}$, so $\kappa(G) \geq \frac{n.\Delta}{\Delta+1}$. According to Lemma 6, $\kappa(G) \leq \frac{n\Delta}{\Delta+1}$, so $\kappa(G) = \frac{n\Delta}{\Delta+1}$.
($\Rightarrow$) Let B be a WOD set of size $\frac{n.\Delta}{\Delta+1}$. There exists $C \subseteq V \setminus B$ such that $B \subseteq Odd(C)$. Notice that $|C| \leq n - \frac{n.\Delta}{\Delta+1} = \frac{n}{\Delta+1}$. Moreover $|C|.\Delta \geq |Odd(C)| \geq |B|$, so $|C| = \frac{n}{\Delta+1}$. It comes that $|B| = |B \cap Odd(C)| \leq \sum_{v \in C} d(v) \leq \Delta.\frac{n}{\Delta+1} = |B|$. Notice that if C is not a perfect code the first inequality is strict, and if $\exists v \in C$, $d(v) < \Delta$, the second inequality is strict. Consequently, C is a perfect code and $\forall v \in C$, $d(v) = \Delta$. □

Corollary 1. *Given a Δ-regular graph G, $\kappa(G) = \frac{n\Delta}{\Delta+1}$ if and only if G has a perfect code.*

We consider the problem MaxWOD which consists in deciding, given a graph G and an integer $k \geq 0$, whether $\kappa(G) \geq k$.

Theorem 7. MaxWOD *is NP-Complete.*

Proof. MaxWOD is in the class NP since a WOD set B of size k is a YES certificate. Indeed, deciding whether the certificate B is WOD or not can be done in polynomial time by solving for X the linear equation $\Gamma_{V \setminus B}.X = 1_B$ in $\mathbb{F}_2$, where 1_B is a column vector of dimension $|B|$ where all entries are 1, and $\Gamma_{V \setminus B}$ is the cut matrix, i.e. a submatrix of the adjacency matrix of the graph which columns correspond to the vertices in $V \setminus B$ and rows to those in B. In fact, $X \subseteq V \setminus B$ satisfies $\Gamma_{V \setminus B}.X = 1_B$ if and only if ($X \subseteq V \setminus B$ and $B \subseteq Odd(X)$) if and only if B is WOD. For the completeness, given a 3-regular graph, if $\kappa(G) \geq \frac{3}{4}n$ then $\kappa(G) = \frac{3}{4}n$ (since $\kappa(G) \leq \frac{n\Delta}{\Delta+1}$ for any graph). Moreover, according to Corollary 1, $\kappa(G) = \frac{3}{4}n$ if and only if G has a perfect code. Since the problem of deciding whether a 3-regular graph has a perfect code is known to be NP complete (see [22] and [21]), so is MaxWOD. □

Now we introduce a lower bound on κ'.

Lemma 7. *For any graph G, $\kappa'(G) \geq \frac{n}{n-\delta}$ where δ is the minimal degree of G.*

Proof. According to Theorem 5, $\kappa'(G) \geq n - \kappa(\overline{G})$. Moreover, thanks to Lemma 6, $n - \kappa(\overline{G}) \geq n - \frac{n\Delta(\overline{G})}{\Delta(\overline{G})+1} = n - \frac{n(n-1-\delta(G))}{n-\delta(G)} = \frac{n}{n-\delta}$. □

This bound is reached for the regular graphs for which their complement graph has a perfect code, more precisely:

Theorem 8. *Given G a δ-regular graph such that $\frac{n}{n-\delta}$ is odd, $\kappa'(G) = \frac{n}{n-\delta}$ if and only if $\overline{G}$ has a perfect code.*

Proof. ($\Leftarrow$) Let C be a perfect code of $\overline{G}$. Since $|C| = \frac{n}{\Delta(\overline{G})+1} = \frac{n}{n-\delta} = 1 \mod 2$, $Odd_G(C) \subseteq C$, thus C is a non-WOD set in G, so $\kappa'(G) \leq \frac{n}{n-\delta}$. Since $\kappa'(G) \geq \frac{n}{n-\delta}$ for any graph, $\kappa'(G) = \frac{n}{n-\delta}$
($\Rightarrow$) Let B be a non-WOD set of size $\frac{n}{n-\delta}$ in G. $\exists D \subseteq B$ such that $|D| = 1 \bmod 2$ and $Odd_G(D) \subseteq B$. According to Lemma 5, $V \setminus B \subseteq Odd_{\overline{G}}(D)$, so $|Odd_{\overline{G}}(D)| \geq \Delta(\overline{G})\frac{n}{n-\delta}$, which implies that $|D|.\Delta(\overline{G}) \geq \Delta(\overline{G})\frac{n}{n-\delta}$. As a consequence, $|D| = \frac{n}{n-\delta}$ and since every vertex of $V \setminus B$ (of size $\Delta(\overline{G})\frac{n}{n-\delta}$) in $\overline{G}$ is connected to D, D must be a perfect code. □

We consider the problem Min¬WOD which consists in deciding, given a graph G and an integer $k \geq 0$, whether $\kappa'(G) \leq k$?

Theorem 9. Min¬WOD *is NP-Complete.*

Proof. Min¬WOD is in the class NP since a non-WOD set of size k is a YES certificate. For the completeness, given a 3-regular graph G, if $\frac{n}{4}$ is odd then according to Theorem 8, G has a perfect code if and only if $\kappa'(\overline{G}) = \frac{n}{4}$. If $\frac{n}{4}$ is even, we add a K_4 gadget to the graph G. Indeed, $G \cup K_4$ is a 3-regular graph and $\frac{n+4}{4} = \frac{n}{4} + 1$ is odd. Moreover, G has a perfect code if and only if $G \cup K_4$ has a perfect code if and only if $\kappa'(\overline{G \cup K_4}) = \frac{n}{4} + 1$. Since deciding whether a 3-regular graph has a perfect code is known to be NP complete, so is Min¬WOD □

In the following, we prove that deciding, given a graph G and $k \geq 0$, whether $\kappa_Q(G) \geq k$ is NP complete (Theorem 10). The proof consists in a reduction from the problem Min¬WOD, which is based on the evaluation of κ and κ' for particular graphs consisting of multiple copies of a same graph:

Lemma 8. *For any graph G and any $r > 0$, $\kappa(G^r) = r.\kappa(G)$ and $\kappa'(G^r) = \kappa'(G)$ where $G^1 = G$ and $G^{r+1} = G \cup G^r$.*

Proof.
– $[\kappa(G^r) = r.\kappa(G)]$: Let B be a WOD set in G of size $\kappa(G)$. B is in the odd neighborhood of some $C \subseteq V$. Then the set $B_r \subseteq V(G^r)$ which is the union of sets B in each copy of the graph G is in the odd neighborhood of $C_r \subseteq V(G^r)$, the union of sets C of each copy of G. Therefore B_r is WOD and $\kappa(G^r) \geq r.\kappa(G)$. Now if we pick any set $B_0 \subseteq V(G^r)$ verifying $|B_0| > r.\kappa(G)$, there exists a copy of G such that $|B_0 \cap G| > \kappa(G)$. Therefore B_0 is a non-WOD set and $\kappa(G^r) \leq r.\kappa(G)$.
– $[\kappa'(G^r) = \kappa'(G)]$: Let B be a non-WOD set in G of size $\kappa'(G)$. If we consider B as a subset of $V(G^r)$ contained in one copy of the graph G, B is a non-WOD set in G^r. Therefore $\kappa'(G^r) \leq \kappa'(G)$. If we pick any set $B \subseteq V(G^r)$ verifying $|B| < \kappa'(G)$, its intersection with each copy of G verifies $|B \cap G| < \kappa'(G)$. Thus, each such intersection is in the odd neighborhood of some C_i. So B is

in the odd neighborhood of $\bigcup_{i=1..r} C_i$. Consequently, B_0 is a WOD set in G^r and $\kappa'(G^r) \geq \kappa'(G)$. □

We consider the problem QuantumThreshold which consists in deciding, for a given graph G and $k \geq 0$, whether $\kappa_Q(G) \geq k$, i.e. $\kappa(G) \geq k$ or $\kappa'(G) \leq n - k$?

Theorem 10. QuantumThreshold *is NP-Complete.*

Proof. QuantumThreshold is in NP since a WOD set of size k or a non-WOD set of size $n - k$ is a YES certificate. For the completeness, we use a reduction to the problem Min¬WOD. Given a graph G and any $k \geq 0$, $\kappa_Q(G^{k+1}) \geq (k+1)n - k \Leftrightarrow \Big(\kappa(G^{k+1}) \geq (k+1)n - k \text{ or } \kappa'(G^{k+1}) \leq k\Big) \Leftrightarrow \Big(\kappa(G) \geq n-1+\frac{1}{k+1} \text{ or } \kappa'(G) \geq k\Big) \Leftrightarrow \Big(\kappa(G) > n-1 \text{ or } \kappa'(G) \geq k\Big)$. In the last disjunction, the first inequality $\kappa(G) > n-1$ is always false since for any graph G of order n we have $\kappa(G) \leq n - 1$. Thus, the answer of the oracle call gives the truth of the second inequality $\kappa'(G) \geq k$ which corresponds to the problem Min¬WOD. As a consequence, QuantumThreshold is NP-complete. □

5 Conclusion

In this paper, we have studied secret sharing with graph states which lead to the analysis of the combinatorial quantity κ_Q that can be computed on graphs. We have studied and computed these quantities on some specific families of graphs, providing the best known constructive threshold protocols for graph-state based secret sharing. Then, we have proven using probabilistic methods that there exist graphs that allow non-quasi-unanimity protocols and that a random graph G of order n satisfies $\kappa_Q(G) \leq 0.811n$ with high probability. Finally, we have shown that given a graph G and an integer k, deciding whether $\kappa_Q(G) \geq k$ is NP-Complete. Recently, in [7], the analysis of this problem has been refined by considering its parameterized complexity: the problem belongs to W[2] and is hard for W[1].

It is very interesting to see that the best known protocols use Paley graph states and that they seem promising candidates to have even better bounds. Paley graph states have also been used in [18] to provide the best known family in terms of minimum degree up to local complementation, which is related to the complexity of graph state preparation [15]. Paley graph states also form an optimal family in terms of multipartie nonlocality [1]. Thus, these states seem very interesting in terms of entanglement and might be useful for other applications in quantum information theory.

Acknowledgements

This work has been funded by the ANR-10-JCJC-0208 CausaQ grant.

References

1. A. Anshu and M.Mhalla *Pseudo-telepathy games and genuine NS n-way nonlocality using graph states* arxiv:1207.2276
2. L.M.J. Bazzi and S.K. Mitter. Some randomized code constructions from group actions. *IEEE Transactions on Information Theory*, 52(7):3210–3219, 2006.
3. G.R. Blakley, *Safeguarding cryptographic keys. AFIPS Conference Proceedings.* 48 313317, 1979.
4. A. Broadbent, P. R. Chouha, and A. Tapp *The GHZ state in secret sharing and entanglement simulation. arXiv:0810.0259*, 2008.
5. D. E. Browne, E. Kashe, M. Mhalla, and S. Perdrix. Generalized ow and determinism in measurement-based quantum computation. *New Journal of Physics (NJP)*, 9(8), 2007.
6. S. Beigi, Isaac Chuang, M. Grassl, P. Shor, and B. Zeng. Graph concatenation for quantum codes. *Journal of Mathematical Physics*, 52(2)(022201), 2011.
7. D. Cattanéo and S. Perdrix. Parametrized Complexity of Weak Odd Domination Problems. arXiv:1206.4081, 2012.
8. R. Cleve, D. Gottesman, and H.-K. Lo, *How to Share a Quantum Secret Phys. Rev. Lett. 83, 648-651,* 1999.
9. V. Danos and E. Kashe. Determinism in the one-way model. *Physical Review A*, 74(052310), 2006.
10. D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, 2000.
11. K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Transactions on Information Theory*, 50, pp 3323 - 3325, 2004.
12. M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in graph states and its applications. In *Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos"*, 2005
13. M. Hein, J. Eisert, and H. J. Briegel. *Multi-party entanglement in graph states. Physical Review A*, 69, 062311 quant-ph/0307130, 2004.
14. M. Hillery, V. Buzek and A. Berthiaume. *Quantum Secret Sharing Phys. Rev. A 59, p.1829; arXiv/9806063*, 1999.
15. P. Høyer M. Mhalla and S. Perdrix, *Resources required for preparing graph states*,17th International Symposium on Algorithms and Computation, 2006.
16. J. Javelle, M. Mhalla, and S. Perdrix. Classical versus Quantum Graph-based Secret Sharing. *eprint:arXiv:1109.4731*, 2011.
17. J. Javelle, M. Mhalla, and S. Perdrix. New protocols and lower bound for quantum secret sharing with graph states. In *Theory of Quantum Computation, Communication and Cryptography. (TQC12)*, To appear in Lecture Notes in Computer Science, 2012. *eprint:arXiv:1109.1487*, 2012.
18. J. Javelle, M.Mhalla and S. Perdrix, *On the Minimum Degree up to Local Complementation: Bounds and Complexity*, 38th International Workshop on Graph Theoretic Concepts in Computer Science, 2012.
19. E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix. Information flow in secret sharing protocols. *EPTCS 9, 2009, pp. 87-97*, 09 2009.
20. A. Keet, B. Fortescue, D. Markham, and B. C. Sanders. Quantum secret sharing with qudit graph states. *Phys. Rev. A, 82:062315*, 2010.
21. S. Klavzar, U. Milutinovic, and C. Petr. 1-perfect codes in sierpinski graphs. *Bulletin of the Australian Mathematical Society*, 66:369–384, 2002.
22. J. Kratochvil. Perfect codes in general graphs. *7th Hungarian colloqium on combinatorics, Eger*, 1987.
23. L. Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. In *Colloquia Mathematica Societatis Janos Bolyai*, pages 609–627, 1975.
24. D. Markham and B. C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78:042309, 2008.

25. M. Mhalla, M. Murao, S. Perdrix, M. Someya, and P. Turner. Which graph states are useful for quantum information processing? In *Theory of Quantum Computation, Communication and Cryptography. (TQC11)*, To appear in Lecture Notes in Computer Science, 2011.
26. M. Mhalla and S. Perdrix. Finding optimal flows effciently. *In the 35th International Colloquium on Automata, Languages and Programming (ICALP)*, LNCS, volume 5125, pages 857868, 2008.
27. M. Mhalla, S. Perdrix. Graph States, Pivot Minor, and Universality of (X,Z)-measurements. *International Journal of Unconventional Computing*. (to be published), 2012.
28. R. A. Moser, G. Tardos. *A constructive proof of the general Lovász Local Lemma*. Journal of the ACM (JACM), v.57 n.2, p.1-15, 2010.
29. R. Prevedel, P. Walther, F. Tiefenbacher, P. Bohi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445(7123):65–69, 2007
30. R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188–5191, 2001.
31. P. Sarvepalli. Non-Threshold Quantum Secret Sharing Schemes in the Graph State Formalism *eprint:arXiv:1202.3433*, 2012.
32. D. Schlingemann and R. F. Werner Quantum error-correcting codes associated with graphs. *Phys. Rev. A 65, 012308*, 2001.
33. A. Shamir *How to share a secret Communications of the ACM 22* (11): 612613, 1979.
34. M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel. Universal resources for measurement-based quantum computation. *Phys. Rev. Lett.*, 97:150504, 2006.
35. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, 2005
36. W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* 299, 802-803, 1982.