Access Structure in Graphs in High Dimension and Application to Secret Sharing

Anne Marin[1], Damian Markham[2], and Simon Perdrix[3]

1 **LTCI, INFRES, Telecom ParisTech, France**
anne.marin@telecom-paristech.fr
2 **CNRS / LTCI, INFRES, Telecom ParisTech, France**
damian.markham@telecom-paristech.fr
3 **CNRS / LIG, Grenoble University, France**
Simon.Perdrix@imag.fr

Abstract

We give graphical characterisation of the access structure to both classical and quantum information encoded onto a multigraph defined for prime dimension q, as well as explicit decoding operations for quantum secret sharing based on graph state protocols. We give a lower bound on k for the existence of a $((k,n))_q$ scheme and prove, using probabilistic methods, that there exists α such that a random multigraph has an accessing parameter $k \leq \alpha n$ with high probability.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Quantum Secret Sharing, Graph State, Multigraph, Access Structure

Digital Object Identifier 10.4230/LIPIcs.TQC.2013.308

1 Introduction

In this work we consider encoding, and accessing, both quantum and classical information onto graph states of qudits - multipartite entangled states which are one to one corresponding to multigraphs (which we will consider as simple graphs with multiple edges). We are particularly interested in using these states for secret sharing.

Secret sharing is an important cryptographic primitive, which was first put forward classically in [33], and then extended to the quantum realm in [19, 9]. The aim of the protocol is for a dealer to distribute a secret (quantum or classical) to a set of players, in such a way that only authorized sets of players can access the secret, and unauthorized sets of players cannot (there may be sets of players which are neither authorized nor unauthorized). The sets of authorized and unauthorized players is called the access structure. Any secret sharing scheme of n players can be loosely paramaterised by two numbers, k and k', such that any subset of k players is an authorized set, whereas any subset of k' players or less is unauthorized. We call such paramaterised schemes (k, k', n) ramp schemes. In the case when $k' = k - 1$, we say it is a threshold scheme, and simplify the notation to (k, n).

In this work we consider two classes of quantum schemes, one class using quantum channels to distribute classical secrets, denoted CQ schemes [19], and the other sharing quantum secrets [9, 19], denoted QQ schemes. The notation CQ and QQ used here follows the work [30, 26, 28], where both classes were phrased in the same language of graph states (first for qubits [30] then qudits [26, 28]). The equivalence of both schemes was shown in [28]. Using the graph state formalism can be useful both practically - since graph states are amongst the most well developed multipartite entangled states experimentally - and theoretically, since graph states are rich in their uses in quantum information, and allow for

graphical characterization of information flow, and access of information. The connection between error correction and secret sharing was understood early on [9], and implies that for general access structures it is necessary to use high dimensional states to encode the secret [30, 28]. In [24] an entirely graphical description of the access structure was given for the graph state protocols on qubits. This has led to many applications, for instance in proving lower and upper bounds on what k and k' are possible in ramp schemes. We are naturally interested in doing the same for higher dimensional versions.

The first result of this paper is to extend to higher dimension the characterisation of the access structure in a graph, previously done in [24] for 2-dimensional system. By gathering the graphical conditions and previous results, we show that the accessibility problem to quantum information can be reduced to study the classical information's one in both a set of player and its complementary (which was proved in [24, 21] for 2 dimensional system). Finally we use this result for the decoding phase of both QQ and CQ protocols, as we know [28] that a CQ authorised is a QQ authorised set and vice versa. In the last part, we study the existence, as a function of k, of a $((k,n))_q$ scheme (this will be defined explicitly later, but can be understood as the underlying graph encoding which gives rise to $(k, n-k, n)$ QQ secret sharing schemes). We derive a lower bound over k, that is, there exists α such that every $(k, n-k, n)$ QQ secret sharing must satisfies $k > \alpha n$, and we use probabilistic method to find $c < 1$ such that a $((cn, n))_q$ scheme exists with high probability.

2 Background

2.1 Qudit graph states, $\mathbb{F}_q^*$-graphs, and multigraphs

The *qudit graph state* formalism [32, 14, 27, 1] consists of representing a quantum state using a weighted undirected graph where every vertex represents a q-dimensional quantum system and every edge, which has assigned an element from the finite field $\mathbb{F}_q$, represents intuitively the entanglement between the elementary systems (a formal definition is given in Definition 1). Such graphs, labeled with elements of a finite field $\mathbb{F}_q$, are known as $\mathbb{F}_q^*$-*graphs* [23] and can be interpreted as edge-colored graphs. In this paper, we consider q prime, and choose to interpret $\mathbb{F}_q^*$-graphs as multigraphs i.e., graphs with possibly parallel edges between pairs of vertices. Albeit equivalent to the other interpretation of $\mathbb{F}_q^*$-graphs, we believe that the multigraph interpretation is relevant in the context of qudit graph states for secret sharing protocols, in particular for the graphical characterisation of authorised and unauthorised sets of players (see Lemmas 5 and 7).

▶ **Definition 1** (q-multigraphs)**.** Given a prime number q, a q-multigraph G is a pair (V, Γ) where V is the finite set of vertices and $\Gamma : V \times V \to \mathbb{F}_q$ is the adjacency matrix of G: for any $u, v \in V$, $\Gamma(u, v)$ is the multiplicity of the edge (u, v) in G.

The term multigraph is used for q-multigraph when q is clear from the context or irrelevant. In this paper, we consider undirected simple multigraphs $G = (V, \Gamma)$ i.e., for any vertices $u, v \in V$, $\Gamma(u, v) = \Gamma(v, u)$ and $\Gamma(u, u) = 0$. For our characterizations of encoding and accessing later on, it will be useful to introduce further concepts. We will see several examples of them along the way, but for now we state definitions. Given a set V of vertices, a vector $D : V \to \mathbb{F}^q$ represents a multiset of vertices of V: for every $v \in V$, $D(v) \in \mathbb{F}_q$ is the multiplicity of v in D. $\sup(D) = \{v \in V \mid D(v) \neq 0 \bmod q\}$ is the support of D. For any multigraph $G = (V, \Gamma)$ and any multiset of vertices $D : V \to \mathbb{F}_q$, the matrix product $\Gamma.D$ is the multiset of neighbours of D: for any $v \in V$, v is a neighbour of D with multiplicity $(\Gamma.D)(v) = \sum_{u \in V} \Gamma(u, v).D(u) \bmod q$. In particular, for any vertex u, $\Gamma.\{u\}$ is the multiset

of neighbours of u. We call $G[D] = (V', \Gamma')$ the sub-multigraph of $G = (V, \Gamma)$ induced by the multiset $D : V \to \mathbb{F}_q$, where $V' = V \cap \sup(D)$ and $\Gamma' : V' \times V' \to \mathbb{F}_q = (u, v) \mapsto D(u).\Gamma(u, v).D(v) \bmod q$. Notice that the multiplicity of an edge in $G[D]$ is the multiplicity of this edge in the original graph G times the multiplicity in D of the two vertices connected by this edge. For any $A, B \subseteq V$, $\Gamma[A, B]$ denotes the submatrix of Γ whose columns correspond to the vertices in A and rows to the vertices in B. $\Gamma[A, B]$ represents the edges which have one end in A and the other one in B.

▶ **Definition 2** (Qudit Graph State)**.** Given a q-multigraph $G = (V, \Gamma)$ with $V = \{v_1, \ldots, v_n\}$, let $|G\rangle \in \mathbb{C}^{q^n}$ be its associated qudit graph state defined as

$$|G\rangle = \frac{1}{\sqrt{q^n}} \sum_{x=(x_1,\cdots,x_n)\in\mathbb{F}_q^n} \omega^{|G[x]|}|x\rangle$$

where ω is the q^{th} root of unity and $|G[x]|$ is the number of edges of the sub-multigraph $G[x] = (V_x, \Gamma_x)$ induced by x, where $V_x = \{v_i \in V, x_i \neq 0\}$ and $\Gamma_x : V_x \times V_x \to \mathbb{F}_q = (v_i, v_j) \mapsto x_i x_j \Gamma(v_i, v_j)$.

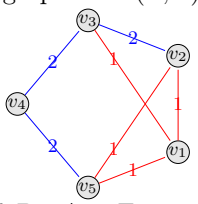
Qudit graph states satisfy the following fundamental fixpoint property. Given a q-multigraph $G = (V, \Gamma)$, $|G\rangle$ is the unique quantum state (up to a global phase) such that, for any $u \in V$,

$$X_u Z_{\Gamma.\{u\}}|G\rangle = |G\rangle \tag{1}$$

where $\Gamma.\{u\}$ is the multiset of neighbours of u, $X = |b\rangle \mapsto |b + 1 \bmod q\rangle$, $Z = |b\rangle \mapsto \omega^b|b\rangle$ are Pauli operators, and for any mulitset $D : V \to \mathbb{F}_q$, $Z_D := \bigotimes_{v\in V} Z_v^{D(v)}$.

▶ **Example 3.** We define the 3-multigraph $G = (V, \Gamma)$ by $V = \{v_1, v_2, v_3, v_4, v_5\}$,

$$\Gamma = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 1 & 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 1 & 1 & 0 & 2 & 0 \end{bmatrix}$$



Let $A = \{v_1, v_2\}$ be a subset of V, and $D : A \to \mathbb{F}_3$ a multiset such that $D(v_1) = 2$, $D(v_2) = 1$. That is $D = \{v_1, v_1, v_2\}$. Then, with previous definitions, the graph induced by D is $G[D] =$

The multiset of neighbours of A is $\{v_1, v_2, v_5, v_5\}$. The multiset of neighbours of D is $\{v_1, v_2, v_2, v_3\}$.

2.2 Local complementation and cut rank

The *local complementation* [5] is a graph transformation which is incredibly useful for the study of graph states [35]. Indeed, if two graphs G and G' are locally equivalent (i.e. one can transform G into G' by means of a series of local complementations), they represent the same entanglement (i.e. there exists a local unitary transformation U such that $|G'\rangle = U|G\rangle$) [35]. Local complementation is extended to multigraphs as follows [23]: Given a q-multigraph $G = (V, \Gamma)$, $u \in V$ and $\lambda \in \mathbb{F}_q$, the *λ-local complementation at u of G* is the q-multigraph $G \star^\lambda u = (V, \Gamma')$ such that $\forall v, w \in V$, $v \neq w$, $\Gamma'(v, w) = \Gamma(v, w) + \lambda.\Gamma(v, u).\Gamma(u, w) \bmod q$. Keet et al. [26] have proved that for any q-multigraph $G = (V, \Gamma)$, any $u \in V$ and any $\lambda \in \mathbb{F}_q$, there exists a local unitary transformation U such that $|G \star^\lambda u\rangle = U|G\rangle$.

The *cut rank* [31] is a set function which associates with every set B of vertices the rank of the matrix describing the edges of the cut $(B, V\backslash B)$: Given a multigraph $G = (V, \Gamma)$, let $\Gamma[B] := \Gamma[B, V\backslash B]$ be the cut matrix of the cut $(B, V\backslash B)$, moreover for any $A, B \subseteq V$, let $\mathrm{rk}_G(A, B) := \mathrm{rank}(\Gamma[A, B])$ and $\mathrm{cutrk}_G(B) := \mathrm{rk}_G(B, V\backslash B)$ be the cut rank of B. Notice that $\mathrm{rk}_G(A, B) = \mathrm{rk}_G(B, A)$ and $\mathrm{cutrk}_G(B) = \mathrm{cutrk}_G(V\backslash B)$.

We point out in this paper that the cut rank, which is known to be invariant by local complementation [23], is a key parameter of q-multigraphs for the study of secret sharing protocols with qudit graph states. Indeed, Theorem 9 states that the capability of a set of players to reconstruct a quantum secret is characterised by the discrete derivative of the cut rank function. Notice that the cut-rank of a bipartition is nothing but the Schmidt measure of entanglement of this bipartition in the corresponding graph state. This is shown for the qubit case in [17], and easily extends to the qudit case. As a consequence, Theorem 9 characterises the accessibility of a set of players as the derivative of the Schmidt measure of entanglement.

2.3 Description of the encoding:

We now introduce the encoding of classical and quantum information onto graph states (CQ and QQ respectively), which will be the starting point for the secret sharing protocols defined in section 4. For ease of notation we present the CQ encoding as deterministic, and in one basis. When used in the full CQ protocol this is randomised by measurement and choice of basis (described fully in section 4). The ability of players to access encoded information (both classical and quantum) is fully described in graph theoretical language in section 3.

CQ encoding:

Given a multigraph $G = (V, \Gamma)$ of order n and a distinguished non isolated vertex $d \in V$, the corresponding CQ encoding of a classical secret $s \in \mathbb{F}_q$ among $n-1$ players consists of the dealer preparing the state

$$|s_L\rangle := Z^s_{\Gamma.\{d\}}|G\backslash d\rangle$$

and sending one qudit to each player, where $G\backslash d = (V\backslash\{d\}, \Gamma[V\backslash\{d\}, V\backslash\{d\}])$ is the multigraph obtained by removing the vertex d and all its incident edges.

In the CQ protocol (described in section 4) the secret s is randomised by measurement on the dealer's vertex d of the full graph state $|G\rangle$, and further, the encoding is randomised by choice of measurement basis - the dealer chooses at random $t \in T$, $T \subseteq \mathbb{F}_q$ and $|T| \geq 2$, and measures his qudit in the associated complementary basis X^tZ. Measuring in this t basis will correspond exactly to using the above CQ encoding of the same secret value s onto the complementary multigraph $G\star^t d$.

QQ encoding:

Given a multigraph $G = (V, \Gamma)$ of order n and a distinguished non isolated vertex $d \in V$, the corresponding QQ encoding on a qudit graph state for sharing an arbitrary quantum secret $|\phi\rangle = \sum_{j=0}^{q-1} s_j|j\rangle \in \mathbb{C}^q$ among $n-1$ players consists, for the dealer, in preparing the state

$$|\phi_L\rangle = \sum_{j=0}^{q-1} s_j Z^j_{\Gamma.\{d\}}|G\backslash d\rangle = \sum_{j=0}^{q-1} s_j|j_L\rangle$$

and in sending one qudit of $|\phi_L\rangle$ to each player.

Notice that the preparation consists in applying the map $|j\rangle \mapsto Z^j_{\Gamma.\{d\}}|G\backslash d\rangle$ which is an isometry as long as d is not an isolated vertex in G. We describe encoding procedures in appendix A.

The accessing structure of the protocols (i.e. the description of the sets of players which can recover the secret, as well as those which have no information about the secret) is given in the next section which provides a graphical characterisation of the accessing structure for the secret sharing protocols using these encodings. Moreover, the operations the authorised sets of players have to perform to reconstruct the secret are also described in the next section.

3 Access Structure in a Graph in Higher Dimension:

3.1 Classical Information

In this section, we show, when the secret is classical, that the protocol is perfect (i.e. every set of players is either able to recover the secret or has no information about the secret), and that the accessing structure is graphically characterised by a simple rank-based function:

▶ **Theorem 4.** *Given a q-multigraph $G = (V, \Gamma)$ and a distinguished vertex $d \in V$, a set $B \subseteq V\backslash\{d\}$ of players can recover a classical secret for the corresponding CQ encoding if and only if $\pi_G(B, d) = 1$, where*

$$\pi_G(B, d) := \mathrm{cutrk}_G(B) - \mathrm{cutrk}_{G\backslash d}(B)$$

A graphical interpretation of Theorem 4 is that a set B is accessible if and only if the presence of the 'dealer vertex' d increases the rank of the cut between B and the rest of the vertices.

The rest of the section is dedicated to the proof of Theorem 4.

First, we prove that a set B of players can recover a classical secret if, roughly speaking, there exists a multiset D of them which is not 'seen' from outside except by the 'dealer':

▶ **Lemma 5.** *Given a q-multigraph $G = (V, \Gamma)$ and $d \in V$, a set $B \subseteq V\backslash\{d\}$ of players can recover a classical secret for the corresponding CQ encoding if there exists a multiset $D : B \to \mathbb{F}_q$ such that* $\mathrm{sup}(\Gamma[B, V\backslash B].D) = \{d\}$ *i.e.,*

- *the number of neighbours of d in D is not congruent to* $0 \bmod q$*;*
- *$\forall u \in V\backslash(B \cup \{d\})$, the number of neighbours of u in D is congruent to* $0 \bmod q$*.*

Proof. Given $B \subseteq V$ and $D : B \to \mathbb{F}_q$ such that $\mathrm{sup}(\Gamma[B, V\backslash B].D) = \{d\}$. W.l.o.g. we assume the multiplicity of d in $\Gamma.D$ is 1 (otherwise we consider the multiset $D' = u \mapsto (\Gamma.D)(d)^{-1}.D(u)$ instead of D). The players in B can recover the secret by measuring an appropriate product of stabilizers. Indeed, there exists $r \in \mathbb{F}_q$ such that $\prod_{u\in B}(X_u Z_{\Gamma.\{u\}})^{D(u)} = \omega^r X_D Z_{\Gamma.D} = Z_d \omega^r X_D Z_{\Gamma[V,V\backslash\{d\}].D}$. As $\prod_{u\in B}(X_u Z_{\Gamma.\{u\}})^{D(u)}|G\rangle = |G\rangle$, we deduce that $\omega^r X_D Z_{\Gamma[V,V\backslash\{d\}].D}|G\backslash d\rangle = |G\backslash d\rangle$. If the classical secret is $s \in \mathbb{F}_q$, $\omega^r X_D Z_{\Gamma[V,V\backslash\{d\}].D} Z^s_{\Gamma.\{d\}}|G\backslash d\rangle = \omega^{r-s} Z^s_{\Gamma.\{d\}} X_D Z_{\Gamma[V,V\backslash\{d\}].D}|G\backslash d\rangle = \omega^{-s} Z^s_{\Gamma.\{d\}}|G\backslash d\rangle$. So if the players in B measure according to $\omega^r X_D Z_{\Gamma[V,V\backslash\{d\}].D}$, they get the outcome $-s \bmod q$, so they recover the classical secret s. ◀

Lemma 5 provides a sufficient condition for a set of players to be able to reconstruct a classical secret. Notice that this reconstruction is nothing but a Pauli measurement, so it can be done by means of local Pauli measurements and classical communications.

▶ **Corollary 6.** *Given a q-multigraph $G = (V, \Gamma)$, $d \in V$, and $B \subseteq V\backslash\{d\}$, if $\pi_G(B, d) = 1$ then B can reconstruct a classical secret for the corresponding CQ encoding.*

Proof. Let $F = V\backslash(B \cup \{d\})$. According to lemma 5, B can recover a classical secret if there exists $D : B \to \mathbb{F}_q$ such that $\mathrm{sup}(\Gamma[B, V\backslash B].D) = \{d\}$. W.l.o.g. we can assume

that the multiplicity of d in $\Gamma[B, V\backslash B].D$ is one. So B can recover a classical secret if the system $\left(\frac{\Gamma[B,\{d\}]}{\Gamma[B,F]}\right).x = \left(\frac{1}{0}\right)$ has a non zero solution, which is equivalent to $\text{rank}\left(\frac{\Gamma[B,\{d\}]}{\Gamma[B,F]}\right) = \text{rank}\left(\frac{\Gamma[B,\{d\}] \mid 1}{\Gamma[B,F] \mid 0}\right)$. Using the last column of the right-side matrix to cancel terms of the row $\Gamma[B,\{d\}]$, we are finally reduced to $\text{rank}\left(\frac{\Gamma[B,\{d\}]}{\Gamma[B,F]}\right) = 1 + \text{rank}(\Gamma[B,F])$ i.e., $\text{cutrk}_G(B) - \text{rk}_G(B,F) = 1 = \pi_G(B,d)$. ◀

In the following, a sufficient condition for a set of players to have no information about the secret is introduced: roughly speaking, a multiset of players D which includes the dealer d, can 'hide' the secret to every player who is connected to D with a number of edges congruent to 0 modulo q:

▶ **Lemma 7.** *Given a q-multigraph $G = (V,\Gamma)$ and $d \in V$, a set $B \subseteq V\backslash\{d\}$ has no information about a classical secret for the corresponding CQ encoding if there exists $D : V\backslash B \to \mathbb{F}_q$, such that $D(d) \neq 0 \bmod q$ and $\Gamma[V\backslash B, B].D = 0$ i.e.,*

- *the multiplicity of d in D is not congruent to $0 \bmod q$;*
- *$\forall u \in B$, the number of neighbours of u in D is congruent to $0 \bmod q$.*

Proof. W.l.o.g. we assume $D(d) = 1 \bmod q$. Notice that $R|G\backslash d\rangle\langle G\backslash d|R^\dagger = |G\backslash d\rangle\langle G\backslash d|$ with $R = \prod_{u\in V\backslash(B\cup\{d\})} \left(X_u Z_{\Gamma[V\backslash\{d\},V\backslash\{d\}].\{u\}}\right)^{D(u)}$. Moreover $R.Z_{\Gamma.\{u\}}$ is only acting on $V\backslash(B\cup\{d\})$, so the reduced density matrix for the players in B is

$$\begin{aligned} & Tr_{V\backslash(B\cup\{d\})}(Z^s_{\Gamma.\{d\}}|G\backslash d\rangle\langle G\backslash d|{Z^\dagger}^s_{\Gamma.\{d\}}) \\ = \; & Tr_{V\backslash(B\cup\{d\})}((Z_{\Gamma.\{d\}}R)^s|G\backslash d\rangle\langle G\backslash d|(Z_{\Gamma.\{d\}}R)^{\dagger s}) \\ = \; & Tr_{V\backslash(B\cup\{d\})}(|G\backslash d\rangle\langle G\backslash d|) \end{aligned}$$

which does not depend on the secret, so the players in B have no information about the secret. ◀

▶ **Corollary 8.** *Given a q-multigraph $G = (V,\Gamma)$, $d \in V$, and $B \subseteq V\backslash\{d\}$, if $\pi_G(B,d) = 0$ then B has no information about the classical secret for the corresponding CQ encoding.*

Proof. Let $F = V\backslash(B\cup\{d\})$. According to lemma 7, B has no information about classical secret if there exists $D : V\backslash B \to \mathbb{F}_q$ such that $D(d) = 1 \bmod q$ and $\Gamma[V\backslash B, B].D = 0$, so if $\Gamma[F,B].C = -\Gamma[V,B]\{d\}$, where $C : F \to \mathbb{F}_q = u \mapsto D(u)$ is the restriction of D to F. As a consequence, B has no information about classical secret if the system $\Gamma[F,B].x = -\Gamma[V,B]\{d\}$ has a non zero solution, which is equivalent to find a non zero solution to the system $\Gamma[F,B].x = \Gamma[V,B]\{d\}$, so if $\text{rank}(\Gamma[F,B]) = \text{rank}(\Gamma[V\backslash B,B])$ i.e., $\pi_G(B,d) = 0$. ◀

Proof of Theorem 4. The proof of Theorem 4 follows from Corollaries 6 and 8 and the fact that for every B, $0 \leq \pi_G(B,d) \leq 1$. It proves that the encoding is perfect i.e., every set of players is either able to reconstruct the secret (when $\pi_G(B,d) = 1$) or has no information about the secret (when $\pi_G(B,d) = 0$). ◀

3.2 Quantum Information

In the following we prove that the accessibility of a set a players is characterised by the derivative of the cut-rank function with respect to the dealer.

▶ **Theorem 9.** *Given a q-multigraph G with a distinguished dealer $d \in V(G)$, a set $B \subseteq V(G)\backslash\{d\}$ of players can recover a quantum secret in the corresponding QQ encoding iff*

$$\partial_d \mathrm{cutrk}_G(B) = -1$$

where $\partial_d \mathrm{cutrk}_G(B) = \mathrm{cutrk}_G(B \cup \{d\}) - \mathrm{cutrk}_G(B)$ is the discrete derivative of cutrk_G in B with respect to d.

Proof. It is known that B can access a quantum secret in G iff B can access a classical secret in two mutual unbiased bases, say in G and $G *^1 d$ [28]. Moreover B can access a classical secret in G iff $\pi_G(B, d) = 1$, where $\pi_G(B, d) = \mathrm{cutrk}_G(B) - \mathrm{rk}_G(B, V\backslash(B \cup \{d\}))$.
($\Rightarrow$) If B can access a quantum secret, B can access a classical secret and $V\backslash(B \cup \{d\})$ has no information about a quantum secret [9], which implies that $V\backslash(B \cup \{d\})$ cannot access a classical secret. Thus $\pi_G(B, d) = 1$ and $\pi_G(V\backslash(B \cup \{d\}), \{d\}) = 0$. As a consequence $\pi_G(B, d) - \pi_G(V\backslash(B \cup \{d\}), \{d\}) = 1$, so $1 = \mathrm{cutrk}(B) - \mathrm{rk}_G(B, V\backslash(B \cup \{d\})) - \mathrm{cutrk}(V\backslash(B \cup \{d\})) + \mathrm{rk}_G(V\backslash(B \cup \{d\}), B) = \mathrm{cutrk}(B) - \mathrm{cutrk}(V\backslash(B \cup \{d\})) = \mathrm{cutrk}(B) - \mathrm{cutrk}(B \cup \{d\})$.
($\Leftarrow$) If $\mathrm{cutrk}_G(B) = \mathrm{cutrk}_G(B \cup \{d\}) + 1$, then $\pi_G(B, \{d\}) = 1$, so B can access a classical secret in G. Moreover, since the cut rank is invariant by local complementation [23], $\mathrm{cutrk}_{G\star^1 d}(B) = \mathrm{cutrk}_{G\star^1 d}(B \cup \{d\}) + 1$, so B can also access a classical secret in $G\star^1 d$. ◀

Notice that for any set B of players, $\partial_d \mathrm{cutrk}_G(B) \in \{-1, 0, 1\}$: if $\partial_d \mathrm{cutrk}_G(B) = -1$, B can recover the quantum secret; if $\partial_d \mathrm{cutrk}_G(B) = 1$ they have no information since $V\backslash(B \cup \{d\})$ can recover the quantum secret; and if $\partial_d \mathrm{cutrk}_G(B) = 0$ they have some partial information about the secret.

Since the cut rank function is submodular [31], its derivative is monotonic (decreasing): if $B \subseteq B'$, $\partial_d \mathrm{cutrk}_G(B) \geq \partial_d \mathrm{cutrk}(B')$. Indeed, if B can recover the secret, any superset B' of B can recover it too; and if B' has no information about the secret, any subset B of B' has no information too.

4 Application to CQ and QQ protocols

We now see how the encoding of section 2.3, and the results on access structures in section 3 can be used to provide secret sharing protocols. Following the prescription of [28] (based on [30, 26], see also [29]) we will now introduce two protocols, one for sharing classical secrets over a quantum channel (CQ) and one for sharing a quantum secret (QQ), both based on a graph state associated with a multigraph. Both protocols can be understood as using the graph state as a channel between the dealer (associated with vertex d) and the players (the remaining vertices). In the CQ case this channel is used to perform an Ekert-like key distribution protocol between the dealer and authorised players, so that when completed the dealer and authorised players will share a random 'dit' string which is unknown to anybody else. In the QQ case the channel is used to teleport the secret to the players such that only authorised sets of players can access the information (the QQ encoding in section 2.3 can be understood as this teleportation, see Appendix A). More details on the protocols and their relation to each other as well as error correction can be found in [28].

4.1 Detailed protocols

Before we write the full protocols out, we first review some background on the graph state formalism, which will be the key in seeing how the stabilisers can be used to specify how authorised sets can access the information, given the satisfaction of the conditions outlined in the previous section.

Given a multigraph $G = (V, \Gamma)$, we begin with an illustrative expansion of the graph state $|G\rangle_V$ according to the d, $V\backslash\{d\}$ partition.

$$|G\rangle = \frac{1}{\sqrt{q^n}} \sum_{x\in\mathbb{F}_q^n} \omega^{|G[x]|}|x\rangle_V = \frac{1}{\sqrt{q}} \sum_s |s\rangle_d Z^s_{\Gamma.\{d\}}|G\backslash d\rangle_{V\backslash\{d\}}$$
$$= \frac{1}{\sqrt{q}} \sum_s |s\rangle_d |s_L\rangle_{V\backslash\{d\}}$$
$$= \frac{1}{\sqrt{q}} \sum_s |s(t)\rangle_d |s_L(t)\rangle_{V\backslash\{d\}},$$

for any $t \in \mathbb{F}_q$, where the second line follows from definitions in section 2.3, corresponding to the CQ encoding achieved by the dealer measuring in the Z basis. The third line corresponds to when the dealer measures in bases X^tZ (explained in more detail later), where they are defined as $|s(0)\rangle = |s\rangle$, and $|s(t)\rangle = \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} \omega^{\frac{j(j-t)}{2t} - st^{-1}j}|j\rangle$ for $t = 1...q-1$, so that $X^tZ|s(t)\rangle = \omega^s|s(t)\rangle$, and further $|s(0)_L\rangle = |s_L\rangle = Z^s_{\Gamma.\{d\}}|G\backslash d\rangle$ and $|s_L(t)\rangle := \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} \omega^{\frac{-k(k-t)}{2t} + st^{-1}k}|k_L\rangle$ for $t = 1...q-1$. The state $|s(t)_L\rangle_{V\backslash\{d\}}$ is equivalent to the CQ encoding of i on graph $G *^t d$ [26].

We now look at how the conditions for access arrived at in section 3 can be used, along with the stabiliser (or "fixed point") condition (1), to eventually see how authorised sets can access the information in the CQ and QQ protocols. We start with the QQ case, which is enough to imply the CQ case (see [28]). Suppose a set of players $B \subset V\backslash\{d\}$ has access to quantum information in a graph $G = (V, \Gamma)$. We proved with Theorem 9 that B can access QQ encoded quantum information in G if and only if B can access the CQ encoded classical information in G and $V\backslash(B\cup\{d\})$ cannot. Thus, by rewriting lemma 5 and 7 applied to B and $V\backslash(B\cup\{d\})$, we have: there exists $D : B \to \mathbb{F}_q$ and $C : B\cup\{d\} \to \mathbb{F}_q$ such that $C(d) = 1$ and $\begin{cases} \sup(\Gamma[B, V\backslash B].D) = \{d\} & \text{(A)} \\ \Gamma[B\cup\{d\}, V\backslash(B\cup\{d\})].C = 0 & \text{(B)} \end{cases}$

Now, call $K_i = X_i Z_{\Gamma.\{i\}}$ and $k_i = X_i Z_{\Gamma[V\backslash\{d\}, V\backslash\{d\}]\{i\}}$ (these are the fixpoint operators, or stabilisers for graphs G and $G\backslash d$ respectively according to (1)).

First we have $K_C = K_d \prod_{i\in B} K_i^{C(i)} = X_d Z_d^{\beta.} Z_{\Gamma.\{d\}} \prod_{i\in B} k_i^{C(i)}$ with $\beta = \Gamma.C(d)$. Then $Z_{\Gamma.\{d\}} \prod_{i\in B} k_i^{C(i)} = \omega^\lambda \prod_{i\in B} X_i^{C(i)} Z_i^{\Gamma.C(i)}$, with $\lambda = \sum_{i,j\in B\cup\{d\}, j<i} \Gamma(j,i)C(j)C(i)$.

Next K_D satisfies $K_D = \prod_{i\in B} K_i^{D(i)} = Z_d^\alpha \prod_{i\in B} k_i^{D(i)}$, with $\alpha = \Gamma.D(d) \neq 0$ since (A), and $\prod_{i\in B} k_i^{D(i)} = \omega^{\lambda'} \prod_{i\in B} X_i^{D(i)} Z_i^{\Gamma.D(i)}$, $\lambda' = \sum_{i,j\in B, j<i} \Gamma(j,i)D(j)D(i)$.

Later we will suppose $\alpha = 1$ (change D to $\alpha^{-1}.D$ if necessary).

Hence $K_C^t {K_D}^{1-t\beta}|G\rangle = \omega^{\frac{t(t-1)}{2}\beta} X_d^t Z_d.[Z_{\Gamma.\{d\}} \prod_{i\in B} k_i^{C(i)}]^t [\prod_{i\in B} k_i^{D(i)}]^{1-t\beta}|G\rangle = |G\rangle$ which is a stabiliser / fixpoint equation involving operators only in d and B which will be used to inform which measurements should be made to recover the secret in the CQ case, and how to find the QQ decoding operation. We can rewrite this as follows

$[Z_{\Gamma.\{d\}} \prod_{i\in B} k_i^{C(i)}]^t [\prod_{i\in B} k_i^{D(i)}]^{1-t\beta} = \omega^c \prod_{i\in B} X_i^{x_i(t)} Z_i^{z_i(t)}$ with

$$x_i(t) = tC(i) + (1-t\beta)D(i) \tag{2}$$
$$z_i(t) = t\Gamma.C(i) + (1-t\beta)\Gamma.D(i), \tag{3}$$
$$c = t^2\lambda' + (1-t\beta)^2\lambda + t(1-t\beta) \sum_{i,j\in B} \Gamma(i,j)C(i)D(j) \tag{4}$$

and we further define

$$f_t(r) := -r - c - \frac{t(t-1)}{2}\beta. \tag{5}$$

We can then see that given the state $|G\rangle_V$, if the dealer measures X^tZ, getting result $\omega^{s(t)}$

and each player i in B measures its qudit in the $X^{x_i(t)}Z^{z_i(t)}$ bases, denoting their results $m_i(t)$, if we define $m(t) = f_t^{-1}(\sum_i m_i(t))$, then the fixpoint stabiliser conditions imply $m(t) = s(t)$. This will be the basis of the CQ accessing strategy.

For the QQ accessing, we define operators U_B and V_B only acting on B such that $U_B := \prod_{i\in B} k_i^{-D(i)}$, which satisfies $U_B|s_L\rangle = \omega^s|s_L\rangle$ and $V_B := Z_{\Gamma.\{d\}}\prod_{i\in B} k_i^{C(i)-\beta D(i)}$, which satisfies $V_B|s_L\rangle = |(s+1)_L\rangle$.
We also define the extended Bell basis as the following bipartite states over a system $\{a,b\}$: $\forall k,l \in F_q$, $|\beta_{k,l}\rangle_{ab} = Z_a^k X_b^l \sum_{i\in\mathbb{F}_q} \frac{|ii\rangle_{ab}}{\sqrt{q}}$. The result (k,l) of a measurement over $\{a,b\}$ in the Bell basis yield the state as $|\beta_{k,l}\rangle_{ab}$.

CQ Protocol: Let T be a subset of $\{0,\cdots,q-1\}, |T| \geq 2$

1. The dealer prepares the graph state $|G\rangle = \frac{1}{\sqrt{q}}\sum_{i=0}^{q-1} |i(t)\rangle_d |i'_L(t)\rangle_{V\setminus\{d\}}$ and sends one qudit of the state to each player.
2. The dealer randomly measures its qudit among the bases: $\{X^tZ\}_{t\in T}$ and denotes the result $\omega^{s(t)}$. That leaves the state over the players on $|i(t)_L\rangle_{V\setminus\{d\}}$.
3. A player $b \in B$ randomly chooses $t' \in T$ and send t' to the other players in B using their private channel.
4. Each player i in B measures its qudit in the $X^{x_i(t')}Z^{z_i(t')}$ bases (see (2),(3)) and sends the result $\omega^{m_i(t')} \in \{1,\omega,..,\omega^{q-1}\}$ to b.
5. b computes $m(t') = f_{t'}^{-1}(\sum_i m_i(t'))$ (see (5)).
6. Repeat step 1. 2. 3. $p \to \infty$ times. The list of measurement results $s(t)$ and $m(t')$ are the raw keys of the dealer and players B respectively.
7. SECURITY TEST: Follow standard QKD security steps. Through public discussion between d and B first sift the key followed by standard error correction and privacy amplification to generate a secure key (see [28] and [34]).

Correctness : After the QKD security steps the dealer and the authorised set B will be able to share a perfectly secure random key. Furthermore, QQ unauthorised sets for the same graph will not be able to establish such a key (see [28] for proofs).

QQ Protocol: Let $|\zeta\rangle_S = \sum_{i=0}^{q-1} s_i|i\rangle_S \in \mathbb{C}^q$ be a quantum secret.

1. A dealer prepares the state $\frac{1}{\sqrt{q}}\sum_{i=0}^{q-1} s_i Z^i_{\Gamma.\{d\}}|G\backslash d\rangle_{V\setminus\{d\}}$
2. The dealer sends one qudit of the resultant state to each player.
3. (measurement) The authorized set B uses two ancillas qudits $\{a_1,a_2\}$ prepared in the Bell pair state $|\beta_{00}\rangle_{a_1a_2}$, and performs the following two commuting projective measurement on $\{B\,a_1\}$, $V_B^{-1}X_{a_1}^{-1}$ and $U_BZ_{a_1}^{-1}$ on , with result denoted k and l respectively.
4. (correction) B applies Z^kX^{-l} over the second ancilla $\{a_2\}$.

Correctness: U_B and V_B satisfy $U_B|i_L\rangle_{V\setminus\{d\}} = \omega^i|i_L\rangle_{V\setminus\{d\}}$, and $V_B|i_L\rangle_{V\setminus\{d\}} = |(i+1)_L\rangle_{V\setminus\{d\}}$ $\forall i \in \mathbb{F}_q$. We can rewrite the state over $V\setminus\{d\}\cup\{a_1,a_2\}$ as:

$$\begin{aligned}
& \textstyle\sum_{i\in\mathbb{F}_q} s_i|i_L\rangle_{V\setminus\{d\}} \sum_{j\in\mathbb{F}_q} \frac{|jj\rangle_{a_1a_2}}{\sqrt{q}}. \\
= \; & \textstyle\frac{1}{\sqrt{q}}\sum_{l\in\mathbb{F}_q} I_{V\setminus\{d\}}X_{a_1}^lX_{a_2}^l \sum_{i\in\mathbb{F}_q} |i_Li\rangle_{V\setminus\{d\}a_1}s_i|i\rangle_{a_2} \\
= \; & \textstyle\frac{1}{\sqrt{q}}\sum_{l\in\mathbb{F}_q} I_{V\setminus\{d\}}X_{a_1}^lX_{a_2}^l \sum_{k\in\mathbb{F}_q}\sum_{i\in\mathbb{F}_q} \omega^{k.i}\frac{|i_Li\rangle_{V\setminus\{d\}a_1}}{q}\sum_j \omega^{-k.j}s_j|j\rangle_{a_2} \\
= \; & \textstyle\frac{1}{\sqrt{q}}\sum_{l\in\mathbb{F}_q} I_{V\setminus\{d\}}X_{a_1}^lX_{a_2}^l \sum_{k\in\mathbb{F}_q} U_B^kI_{a_1}Z_{a_2}^{-k}\sum_{i\in\mathbb{F}_q}\frac{|i_Li\rangle_{V\setminus\{d\}a_1}}{q}\sum_j s_j|j\rangle_{a_2} \\
= \; & \textstyle\frac{1}{q}\sum_{l,k\in\mathbb{F}_q} U_B^kX_{a_1}^l\sum_{i\in\mathbb{F}_q}\frac{|i_Li\rangle_{V\setminus\{d\}a_1}}{\sqrt{q}}X_{a_2}^lZ_{a_2}^{-k}\sum_{j\in\mathbb{F}_q}s_j|j\rangle_{a_2})
\end{aligned}$$

Table 1 List of typical subsets B of 4 players in the Reed Solomon Graph State described in Fig 1a. For each B, $B \cup \{u \in V\backslash B \mid \sum_{v\in B} D(v).\Gamma(u,v) \neq 0 \bmod q\} = B \cup \{d\} = B \cup \{d\} \cup \{u \in V\backslash(B\cup\{d\}) \mid \sum_{v\in B\cup\{d\}} C(v).\Gamma(v,u) \neq 0 \bmod q\}$, meaning that B can access quantum information, whereas $V\backslash(B\cup\{d\})$, that is all subset of 3 players, cannot. (The remaining subsets are covered by symmetry.)

B	$(D(b))_{b\in Bs}$	$(C(b))_{b\in d\cup B}$	B	$(D(b))_{b\in Bs}$	$(C(b))_{b\in d\cup B}$
$\{v_7,v_1,v_2,v_3\}$	$(1,0,0,0)$	$(1,0,4,3,6)$	$\{v_6,v_1,v_2,v_3\}$	$(1,0,0,0)$	$(1,0,2,2,1)$
$\{v_5,v_1,v_2,v_3\}$	$(1,0,0,0)$	$(1,0,3,4,1)$	$\{v_4,v_1,v_2,v_3\}$	$(1,0,0,0)$	$(1,0,4,6,2)$
$\{v_6,v_7,v_2,v_3\}$	$(3,1,0,0)$	$(1,0,0,1,3)$	$\{v_6,v_7,v_1,v_2\}$	$(1,4,0,0)$	$(1,0,0,3,6)$
$\{v_6,v_7,v_1,v_3\}$	$(4,1,0,0)$	$(1,0,0,5,5)$	$\{v_5,v_7,v_2,v_3\}$	$(3,4,0,0)$	$(1,0,0,6,1)$
$\{v_5,v_7,v_1,v_2\}$	$(1,1,0,0)$	$(1,0,0,2,1)$	$\{v_5,v_7,v_1,v_3\}$	$(4,3,0,0)$	$(1,0,0,1,4)$
$\{v_4,v_7,v_2,v_3\}$	$(4,1,0,0)$	$(1,0,0,2,2)$	$\{v_4,v_7,v_1,v_3\}$	$(3,4,0,0)$	$(1,0,0,6,1)$
$\{v_5,v_6,v_1,v_2\}$	$(3,1,0,0)$	$(1,0,0,1,3)$	$\{v_5,v_6,v_1,v_3\}$	$(1,6,0,0)$	$(1,0,0,4,3)$
$\{v_5,v_6,v_7,v_3\}$	$(2,2,1,0)$	$(1,0,0,0,2)$	$\{v_5,v_6,v_7,v_2\}$	$(4,1,1,0)$	$(1,0,0,0,5)$
$\{v_5,v_6,v_7,v_1\}$	$(5,6,1,0)$	$(1,0,0,0,6)$	$\{v_4,v_5,v_7,v_3\}$	$(1,1,1,0)$	$(1,0,0,0,6)$
$\{v_4,v_5,v_7,v_1\}$	$(4,6,1,0)$	$(1,0,0,0,3)$	$\{v_4,v_5,v_7,v_2\}$	$(6,1,4,0)$	$(1,0,0,0,3)$
$\{v_4,v_5,v_6,v_7\}$	$(5,6,1,2)$	$(1,0,0,0,0)$			

As $V_B^{-1}X_{a_1}^{-1}(U_B^k X_{a_1}^l \sum_{i\in\mathbb{F}_q} \frac{|i_L i\rangle_{V\backslash\{d\}a_1}}{\sqrt{q}}) = \omega^k U_B^k X_{a_1}^l \sum_{i\in\mathbb{F}_q} \frac{|i_L i\rangle_{V\backslash\{d\}a_1}}{\sqrt{q}}$ and $U_B Z_{a_1}^{-1}(U_B^k X_{a_1}^l \sum_{i\in\mathbb{F}_q} \frac{|i_L i\rangle_{V\backslash\{d\}a_1}}{\sqrt{q}}) = \omega^l U_B^k X_{a_1}^l \sum_{i\in\mathbb{F}_q} \frac{|i_L i\rangle_{V\backslash\{d\}a_1}}{\sqrt{q}}$, the projective measurement according to $V_B^{-1}X_{a_1}^{-1}$ and $U_B Z_{a_1}^{-1}$ reveals the syndrome (k,l), such that the correction $Z^k X^{-l}$ over the ancilla $\{a_2\}$ leaves the state as $\sum_i s_i|i\rangle_{a_2}$.

4.2 Example

We illustrate the use of characterisation of the access structure in a multigraph with a Reed Solomon Graph State that allows a quantum secret (or equivalently a random key of *dits*) to be shared between a dealer and all subset of at least $\frac{n+1}{2}$ players among a set of n players over a field of q elements, with $q \geq n$. We refer to [29], [9] for more details about Reed Solomon Graph for secret sharing.

We saw $B \subset V\backslash\{d\}$ can access quantum information with respect to d in G iff there exist $D : B \to \mathbb{F}_q$ and $C : B\cup\{d\} \to \mathbb{F}_q$ such that $C(d) = 1$ and

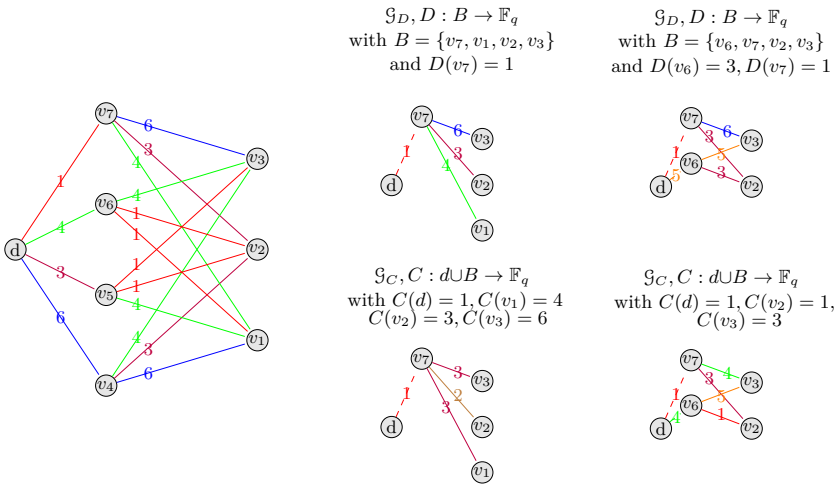
$$\sup(\Gamma[B, V\backslash B].D) = \{d\}$$
$$\Gamma[B\cup\{d\}, V\backslash(B\cup\{d\})].C = 0$$

We rewritte these conditions in the following way: $B \subset V\backslash\{d\}$ can access quantum information in G iff there exist $D : B \to \mathbb{F}_q$ and $C : B \cup \{d\} \to \mathbb{F}_q$ such that $C(d) = 1$ and

$$\begin{cases} B \cup \{u \in V\backslash B \mid \sum_{v\in B} D(v).\Gamma(u,v) \neq 0 \bmod q\} = B \cup \{d\}. & (5) \\ B \cup \{d\} \cup \{u \in V\backslash(B\cup\{d\}) \mid \sum_{v\in B\cup\{d\}} C(v).\Gamma(v,u) \neq 0 \bmod q\} = B \cup \{d\} & (6) \end{cases}$$

For $A : V \to \mathbb{F}_q$, we call $\mathcal{G}_A = (V_A, \Gamma_A)$ the subgraph induced by A and its neighbours such that: $V_A = \sup(A) \cup \{v \in V\backslash\sup(A) \mid \Gamma[\sup(A), V\backslash\sup(A)].A(v) \neq 0 \bmod q\}$ and $\forall v_i \in \sup(A)$, $\begin{cases} \Gamma_A(v_i,v_j) = A(v_i)A(v_j).\Gamma(v_i,v_j) \text{ if } v_j \in \sup(A) \\ \Gamma_A(v_i,v_j) = A(v_i)\Gamma(v_i,v_j) \text{ if } v_j \in V_A\backslash\sup(A) \end{cases}$

For example, let $G = (V,\Gamma)$, $d \in V$, $|V| = 8$, be the $(4,3,7)_7$ Reed Solomon Graph State given in Fig 1a. Such a graph can be used by dealer d to encode any quantum secret $|\xi\rangle \in \mathbb{C}^7$ and share it between 7 players such that all subset of at least 4 players can recover the secret, whereas any subset of 3 players or less cannot have any information about it. We can reprove this result using the previous graph characterisation, that is by checking if conditions (5) (6) are satisfied in a basis G for all subset $B \subset V\backslash\{d\}$ of 4 players. In fig 1b, we give the relevant induced graphs for two different subsets B. And in table 1 we give a list of relevant multiset $D : B \to \mathbb{F}_q$ and $C : B\cup\{d\} \to \mathbb{F}_q$ for typical subsets B of four players.



(a) $(4, 3, 7)_7$ Reed Solomon QQ Graph scheme.

(b) Examples of subgraphs $\mathcal{G}_D$ associated with subset B showing that B can access classical information in G and of subgraphs $\mathcal{G}_C$ associated with $d \cup B$ showing that $V \backslash B$ cannot have classical information in G.

Figure 1 Checking quantum accessibility in a $(4, 3, 7)_7$ Reed Solomon Graph.

5 Existence of $((k, n))_q$ scheme

In this section, we focus on the properties of the secret sharing scheme realised by a given $\mathbb{F}_q$-graph, as well as the existence of $\mathbb{F}_q$-graphs realising a given secret sharing protocol. A $\mathbb{F}_q$-graph G of order n with a particular dealer d is said to realise a $((k, n))_q$ scheme if $k - 1 = \max_{B \subseteq V \backslash \{d\}}(\partial_d \text{cutrk}_G(B) \geq 0)$. In other words, G realises a $((k, n))_q$ scheme if all sets of at least k players can recover a quantum secret and there exists a set of $k - 1$ players which cannot. A $\mathbb{F}_q$-graph which realises an $((k, n))_q$ scheme can be used as an $(k, k' \geq n - k, n)_q$ CQ protocol or $(k, n - k, n)_q$ QQ protocol as described in section 4 (note that they can also be used for $(k, k' \geq n - k, n)_q$ schemes to share a quantum secret using hybrid protocols (e.g. [4, 21, 11, 12])).

5.1 Finding new schemes

Theorem 9 offers a combinatorial characterisation of quantum accessibility, and raises as a consequence several questions about the complexity of deciding: (i) whether a given set of players can access a quantum secret in a given q-multigraph? (ii) whether a given q-multigraph realises a $((k, n))$ protocol? (iii) whether, given q, n and k, there exists an $\mathbb{F}_q$-graphs realising a $((k, n))$ protocol?

Problem i Given an $\mathbb{F}_q$-graph G of order n with a particular dealer d and a set B of k players, deciding whether B can access a quantum secret consists of deciding whether $\partial_d \text{cutrk}_G(B) = -1$. This can be decided efficiently since $\partial_d \text{cutrk}_G(B)$ is computed in $O(nk^{1.38})$ operations using the Gaussian elimination for computing the rank [6, 20].

Problem ii Given a $\mathbb{F}_q$-graph G of order n and $\alpha \in [0, 1]$, deciding whether G is a $((\alpha n, n))$ scheme can be done by enumerating all the $\binom{n}{\alpha n}$ sets of players of size αn and for each of them deciding whether they can access a quantum secret. It leads to $O(n^{2.38} 2^{nH_2(\alpha)})$

operations. This problem is NP-complete, as it has been shown to be NP complete when $q = 2$ [7], and also hard in terms of parameterised complexity as it is hard for $W[1]$ [7].

Problem *iii* Given n, α, and q, deciding whether there exists a $((\alpha n, n))$ $\mathbb{F}_q$-graph? A brute-force approach consists in enumerating all the $q^{\frac{n(n-1)}{2}}$ $\mathbb{F}_q$-graphs of order n and then decide whether they realise a $((\alpha n, n))$ protocol. It leads to $O(q^{\frac{n(n-1)}{2}} n^{2.38} 2^{nH_2(\alpha)})$ operations. This can be implemented for small values of n only and permits to prove that there is no $(4, 3, 7)_3$ QQ secret sharing with qutrit graph state.

Solving problem i can be done with the similar algortihm C of [13]. Note that for one thing, the later is more general and can be applied to input states (that is quantum secrets) and to multigraphs of arbitrary dimension (not necessarily prime number). For another thing, it concerns rather the access to partial information. Also it is not optimised for problem i of our particular interest.

In the following sections, we develop a different approach for deciding the existence of $((\alpha n, n))$ $\mathbb{F}_q$-graphs realising. We show an upper and a lower bound on the minimal α such that there exists an $\mathbb{F}_q$-graph realising a $((\alpha n, n))$ protocol. The upper bound (Theorem 11) is based on non constructive probabilistic methods, whereas the lower bound (Theorem 14) is based on a counting argument.

5.2 Existence of q-multigraphs realising $((\alpha n, n))_q$ schemes

In this section, we prove a Gilbert-Varshamov-like result: for any α such that $H_{q^2}(1-\alpha) < \frac{1}{2}$ there exists a q-multigraph realising a $((\alpha n, n))_q$ scheme. The proof is using probabilistic methods and is, as a consequence, non constructive. However, we prove that a random q-multigraph satisfies such $((\alpha n, n))_q$ scheme with high probability as long as $H_{q^2}(1-\alpha) < \frac{1}{2}$.

▶ **Lemma 10.** *For any q-multigraph $G = (V, \Gamma)$ of order n, and any $\alpha \in [0.5, 1]$, if for any multiset $C : V \to \mathbb{F}_q$, $|\sup(C) \cup \sup(\Gamma.C)| > (1-\alpha)n$ then for any $d \in V$ and any $B \subseteq V \backslash \{d\}$ such that $|B| \geq \alpha n$, $\partial_d \mathrm{cutrk}_G(B) = -1$.*

Proof. For any $B \subseteq V$ such that $|B| \geq \alpha n$, $\ker(\Gamma[V \backslash B]) = \{0\}$, otherwise there would be a multiset C such that $\sup(C) \subseteq V \backslash B$ and $|\sup(C) \cup \sup(\Gamma.C)| \leq (1-\alpha)n$. So for any $B \subseteq V$ such that $|B| \geq \alpha n$, $\mathrm{cutrk}_G(B) = n - |B|$. As a consequence, for any $d \in V$ and any $B \subseteq V \backslash \{d\}$ such that $|B| \geq \alpha n$, $\partial_d \mathrm{cutrk}_G(B) = n - |B \cup \{d\}| - (n - |B|) = -1$. Thus $\partial_d \mathrm{cutrk}_G(B) = -1$ ◀

A random $\mathbb{F}_q$-graph $G(n, 1/q)$ is a $\mathbb{F}_q$-graph of order n such that, for every pair of vertices u and v, the number of edges between u and v is chosen uniformly at random in $\mathbb{F}_q$.

▶ **Theorem 11.** *Given $q \geq 2$, and $\alpha \in [0.5, 1]$ such that $H_{q^2}(1-\alpha) < \frac{1}{2}$, for any $n \in \mathbb{N}$, a random q-multigraph $G(n, 1/q)$ realises a $((\alpha n, n))_q$ scheme with probability $1 - 2^{\Omega(n)}$, where d is any vertex of $G(n, 1/q)$.*

Proof. Let $\mathcal{C}_\alpha = \{C : V \to \mathbb{F}_q, |\sup(C)| \leq (1-\alpha)n\}$. For any $C \in \mathcal{C}_\alpha$, let A_C be the (bad) event $|\sup(C) \cup \sup(\Gamma.C)| \leq (1-\alpha)n$.
For any $C \in \mathcal{C}_\alpha$, $Pr(A_C) = \frac{1}{q^{(1-c)n}} \sum_{k=0}^{(1-\alpha-c)n} \binom{(1-c)n}{k} (q-1)^k$ where $c = |\sup(C)|/n$, and $\sum_{C \in \mathcal{C}_\alpha} Pr(A_C) = \sum_{j=0}^{(1-\alpha)n} f(j)$ with $f(j) = \sum_{C s.t. |\sup(C)|=j} Pr(A_C)$.
In the following, we show an upperbound on $f(k)$. For any $c \in [0, 0.5]$, $f(cn) = \binom{n}{cn}(q-1)^{cn} \frac{1}{q^{(1-c)n}} \sum_{k=0}^{(1-\alpha-c)n} \binom{(1-c)n}{k} (q-1)^k \leq \frac{(q-1)^{cn}}{q^{(1-c)n}} 2^{nH_2(c) + (1-c)nH_2(\frac{1-\alpha-c}{1-c})} (q-1)^{(1-\alpha-c)n} = 2^{ng(c)}$ where $g(c) = H_2(c) + (1-c)H_2(\frac{\alpha}{1-c}) + (1-\alpha)\log_2(q-1) - (1-c)\log_2(q)$. $g'(c) =$

$-\log_2(c)+\log_2(1-\alpha-c)+\log_2(q)$, so $g'(c)=0 \iff c=\frac{q}{q+1}(1-\alpha)$. As a consequence, $g(c) \leq g(\frac{q}{q+1}(1-\alpha)) = -\alpha\log_2(\alpha)-(1-\alpha)\log_2(\alpha)+(1-\alpha)\log_2(q^2-1)-\log_2(q) = \log_2(q)(2H_{q^2}(1-\alpha)-1)$. Thus, $\sum_{C\in\mathcal{C}_\alpha} Pr(A_C) \leq (1-\alpha)nq^{n[2H_{q^2}(1-\alpha)-1]}$, so, thanks to the union bound, $Pr(\bigcap_{C\in\mathcal{C}_\alpha}\overline{A_C}) \geq 1-(1-\alpha)nq^{n[2H_{q^2}(1-\alpha)-1]} = 1-2^{\Omega(n)}$ when $2H_{q^2}(1-\alpha)-1<0$. So according to lemma 10, $\kappa_Q(G,d)\leq \alpha n$ for any vertex d when $H_{q^2}(1-\alpha)<\frac{1}{2}$. ◀

Theorem 11 extends the upper bound of the binary case ($q=2$) [21]. Notice that even if a random $\mathbb{F}_q$-graph realises a $((\alpha n,n))_q$ scheme with probability almost 1, double checking whether a (randomly chosen) $\mathbb{F}_q$-graph actually realises a $((\alpha n,n))_q$ scheme is a hard task (see Problem (*ii*) in section 5.1).

5.3 Lower bound on quantum accessibility

The no cloning theorem implies that for any $((\alpha n,n))$ secret sharing protocol, $\alpha>0.5$. In the following we improve this lower bound for secret sharing schemes based on qudit graph states. The lower bound on α depends on the dimension q (see Theorem 14), the value of the lower bound is plotted for small values of q in figure 2.

The lower bound is based on the properties of the *kernel with respect to the dealer* defined as follows:

▶ **Definition 12.** Given a q-multigraph G, for any $d\in V(G)$ and any $B\subseteq V(G)\backslash\{d\}$, let $\mathcal{S}_d(B)=\ker(\Gamma_G[B\cup\{d\}])\backslash\ker(\Gamma_G[B])$ be the kernel of B with respect to d.

▶ **Lemma 13.** *Given a q-multigraph G, for any $d\in V(G)$ and any $B\subseteq V(G)\backslash\{d\}$, if $\partial_d \mathrm{cutrk}_G(B)=-1$, there exists $C\in\mathcal{S}_d(B)$ such that*

$$|\sup(C)|<\frac{q}{q+1}\mathrm{cutrk}_G(B)$$

Proof. Since $\mathrm{cutrk}_G(B\cup\{d\})-\mathrm{cutrk}_G(B)=-1$, $\dim(\ker(\Gamma_G[B\cup\{d\}]))-\dim(\ker(\Gamma_G[B]))=2$. Moreover, $\ker(\Gamma_G[B])\subseteq\ker(\Gamma_G[B\cup\{d\}])$, so $|\mathcal{S}_d(B)|=(q^2-1).q^t$ where $t=\dim(\ker(\Gamma_G[B]))$. Let $M=\binom{I}{M'}$ a matrix in standard form (or reduced column echelon form) generating $\Gamma_G[B\cup\{d\}]$. Since $|\mathcal{S}_d(B)|=(q^2-1).q^t$ and $|\ker(\Gamma_G[B\cup\{d\}])|=q^{t+2}$, there exist two columns C_1 and C_2 of M such that $\forall(x,y)\in[0,q-1]^2\backslash\{(0,0)\}$, $x.C_1+y.C_2\in\mathcal{S}_d(B)$. Notice that since M is in standard form, $|\sup(C_1)\cup\sup(C_2)|\leq|B|+1-t$. Moreover for any $v\in\sup(C_1)\cup\sup(C_2)$, v has a zero multiplicity in $q-1$ vectors of the q^2-1 linear combinations $x.C_1+y.C_2$ for $x,y\in[0,q-1]\backslash\{(0,0)\}$, so $\sum_{(x,y)\in[0,q-1]^2\backslash\{(0,0)\}}|\sup(x.C_1+y.C_2)| = (q^2-1-(q-1)).|\sup(C_1)\cup\sup(C_2)|$, so there exists $C\in\mathcal{S}_d(B)$ such that $|\sup(C)|\leq\frac{q^2-q}{q^2-1}(|B|+1-t)=\frac{q}{q+1}(\mathrm{cutrk}_G(B)+1)<\frac{q}{q+1}\mathrm{cutrk}_G(B)$. ◀

▶ **Theorem 14.** *If a q-multigraph G of order n realises a $((\alpha n,n))_q$ scheme, then*

$$\binom{n}{\frac{(1-\alpha)qn}{q+1}}\binom{\alpha n}{(2\alpha-1)n}\geq\frac{(2\alpha-1)(1-\alpha)}{2}\binom{n}{\alpha n}$$

Asymptotically, as n tends to infinity, α satisfies:

$$H_2(\frac{\alpha q+1}{q+1})+\alpha H_2(\frac{1-\alpha}{\alpha})\geq H_2(\alpha)$$

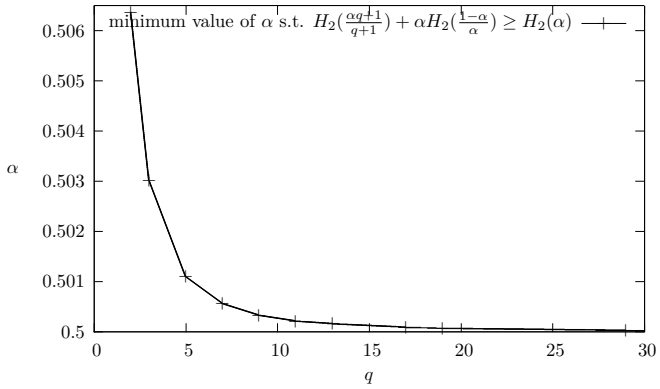


Figure 2 Lower bound on the accessibility to quantum information in a $((k,n))_q$ scheme. There is no $((k,n))_q$ scheme with $k \leq \alpha n$

Proof. Given B_0 of size αn, according to lemma 13 there exists $C_0 \in \mathcal{S}_d(B_0)$ such that $|\sup(C_0)| < \frac{q}{q+1}(1-\alpha)n$. Notice that the set $\sup(C_0) \cup \sup(\Gamma_G.C_0)$ has some partial information about the secret so $|\sup(C_0) \cup \sup(\Gamma_G.C_0)| \geq (1-\alpha)n$. Moreover for any B of size αn, if $C_0 \in \mathcal{S}_q(B)$ then $\sup(C) \cup \sup(\Gamma_G.C) \subseteq B$. So there are at most $\binom{n-1-(1-\alpha)n}{\alpha n-(1-\alpha)n} = \binom{\alpha n-1}{(2\alpha-1)n}$ sets $B \subseteq V \backslash \{d\}$ of size αn such that $C_0 \in \mathcal{S}_d(B)$. For any B of size αn there is a C which support is of size at most $\frac{q}{q+1}(1-\alpha)n - 1$, any every such C is associated with at most $\binom{\alpha n-1}{(2\alpha-1)n}$ such Bs, so a counting argument implies $\binom{n-1}{\alpha n} \leq \binom{\alpha n-1}{(2\alpha-1)n} \sum_{i=1}^{\frac{q}{q+1}(1-\alpha)n-1} \binom{n-1}{i}$. Moreover, $\sum_{i=1}^{\frac{q}{q+1}(1-\alpha)n-1} \binom{n-1}{i} \leq \frac{1+\alpha q}{q(2\alpha-1)} \binom{n-1}{\frac{(1-\alpha)qn}{q+1}-1} = \frac{(1-\alpha)(1+\alpha q)}{(2\alpha-1)(q+1)} \binom{n}{\frac{(1-\alpha)qn}{q+1}}$. So, $\frac{\binom{n}{\alpha n}}{\binom{\alpha n-1}{(2\alpha-1)n}} = \frac{\alpha}{(1-\alpha)^2} \frac{\binom{n-1}{\alpha n}}{\binom{\alpha n-1}{(2\alpha-1)n}} \leq \frac{\alpha(1+\alpha q)}{(2\alpha-1)(1-\alpha)(q+1)} \binom{n}{\frac{(1-\alpha)qn}{q+1}} \leq \frac{2}{(2\alpha-1)(1-\alpha)} \binom{n}{\frac{(1-\alpha)qn}{q+1}}$.

Since $2^{n(H_2(p)+o(1))} \leq \binom{n}{pn} \leq 2^{nH_2(p)}$, asymptotically, as n tends to infinity, α satisfies the equation $H_2(\frac{\alpha q+1}{q+1}) + \alpha H_2(\frac{1-\alpha}{\alpha}) \geq H_2(\alpha)$. ◀

6 Discussion

In this work we have studied the encoding of classical and quantum information onto graph states of qudits, and its application for secret sharing schemes. We have given complete graphical characterization of which sets of vertices (players) can access the information, and shown how this can be done both for classical and quantum information. Using this characterization we have given bounds on which protocols are possible and how difficult the access structure is to calculate given a graph.

Whilst we have focused on the application of our results for secret sharing, there may be applications to other quantum information protocols. Indeed, the QQ encoding defined in section 2.3 is exactly the same encoding procedure used in measurement based quantum computing and error correction, so we can expect that these results have implications in both these domains. Furthermore, quantum secret sharing is intimately linked to error correction [28, 9]. All secret sharing schemes are error correcting schemes, and the QQ protocols presented here are equivalent to all possible stabilizer codes [28]. Thus, the existence of $((\alpha n, n))$ protocols is an existence statement about error correcting protocols too, and the no goes on secret sharing imply no-goes for all stabilizer codes - so that there are no stabilizer codes with parameters violating our lower bounds.

Acknowledgements. The authors want to thank Mehdi Mhalla and David Cattanéo for fruitful discussions. This work has been funded by the ANR-10-JCJC-0208 CausaQ grant, the FREQUENCY (ANR-09-BLAN-0410), HIPERCOM (2011-CHRI-006) projects, and by the Ville de Paris Emergences program, project CiQWii.

References

1 M. Bahramgiri,S. Beigi, *Graph states under the action of local Clifford group in non-binary case* arXiv:quant-ph/0610267 (2006).
2 S. Beigi, I. Chuang, M. Grassl, P. Shor, B. and Zeng, *Graph concatenation for quantum codes.* J. Math. Phys. 52, 022201 (2011).
3 M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, A. Smith, *Secure Multiparty Quantum Computation with (Only) a Strict Honest.* Proc. 47th Annual IEEE Symposium on the Foundations of Computer Science (FOCS '06), pp. 249-260 (2006).
4 A. Broadbent, P. Chouha, A. Tapp, *The GHZ state in secret sharing and entanglement simulation.* Third International Conference on Quantum, Nano and Micro Technologies, ICQNM'09, 59-62 (2009).
5 A. Bouchet *Circle Graph Obstructions* Journal of Combinatorial Theory, Series B, Vol 60, 1,pp 107-144 (1994).
6 J.R. Bunch, J.E. Hopcroft. *Triangular Factorization and Inversion by Fast Matrix Multiplication.* Mathematics of Computation, 28(125):231236, (1974).
7 David Cattanéo, Simon Perdrix. *Parametrized Complexity of Weak Odd Domination Problems.* arXiv:1206.4081 (2012).
8 M. Christandl, A. Winter, *Uncertainty, Monogamy and Locking of Quantum Correlations.* IEEE Trans Inf Theory, vol 51, no 9, pp 3159-3165 (2005).
9 R. Cleve, D. Gottesman, H.K. Lo, *How to share a quantum secret.* Phys. Rev. Lett. **83**, 648 (1999).
10 A.K. Ekert, *Quantum cryptography based on Bell's theorem.* Phys. Rev. Lett., **67**, 6, pp. 661–663 (1991).
11 B. Fortescue, G. Gour, *Reducing the quantum communication cost of quantum secret sharing.* IEEE Trans. Inf. Th. 58(10), pp. 6659 - 6666 (2012)
12 V. Gheorghiu, *Generalized Semi-Quantum Secret Sharing Schemes.* Phys. Rev. A 85, 052309 (2012)
13 V. Gheorghiu, S.Y. Looi, R.B. Griffiths, *Location of quantum information in additive graph codes* Phys. Rev. A, **81**, 3, pp. 032326, (2010).
14 M. Grassl, A. Klappenecker, M. Rötteler, *Graphs, Quadratic forms and Quantum Codes*, IEEE International Symposium on Information Theory (ISIT 2002), p.45 (2002).
15 S. Gravier, J. Javelle, M. Mhalla, S. Perdrix, *On Weak Odd Domination and Graph-based Quantum Secret Sharing.* arXiv:1112.2495 (2011).
16 S. Gravier, J. Javelle, M. Mhalla, S. Perdrix, *Optimal accessing and non-accessing structures for graph protocols.* arXiv:1109.6181 (2011).
17 M. Hein, J. Eisert, H. J. Briegel. *Multiparty entanglement in graph states.* Phys. Rev. A 69, 062311 (2004).
18 M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, H. J. Briegel, *Entanglement in graph states and its applications* in Quantum Computers, Algorithms and Chaos, Proceedings of the International School of Physics Enrico Fermi, Vol. 162 (2006).
19 M. Hillery, V. Bužek, A. Berthiaume, *quantum secret sharing.* Phys. Rev. A **59**, 1829 (1999).
20 O.H. Ibarra, S. Moran, R. Hui. *A Generalization of the Fast LUP Matrix Decomposition Algorithm and Applications.* Journal of Algorithms, 3(1):4532656, (1982).
21 J. Javelle, M. Mhalla, S. Perdrix, *New Protocols and Lower Bound for Quantum Secret Sharing with Graph States.* TQC'12. LNCS Vol 7582, pp 1-12 (2013).
22 J. Javelle, M. Mhalla, S. Perdrix, *On the Minimum Degree up to Local Complementation: Bounds and Complexity.* WG'12. LNCS Vol 7551, pp 138-147 (2012).

23 M.M. Kanté, M. Rao. *The Rank-Width of Edge-Coloured Graphs.* Theory of Computing Systems, 1-46, (2012).

24 E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix. *Information flow in Secret Sharing Protocols. Electronic Proceedings in Theoretical Computer Science*, 9:87–97 (2009).

25 A. Karlsson, M. Koashi, N. Imoto, *Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A* **59**, 162–168, (1999).

26 A. Keet, B. Fortescue, D. Markham and B. C. Sanders, *Quantum secret sharing with qudit graph states.* Phys. Rev. A **82**, 062315 (2010).

27 A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, *Nonbinary Stabilizer Codes Over Finite Fields.* IEEE Trans. Inf. Th. 52, 4892 (2005).

28 A. Marin, D. Markham, *On the equivalence between sharing quantum and classical secrets, and error correction.* arxiv:1205.4182 (2012)

29 A. Marin, D. Markham, *High dimensional CSS code and application to secret sharing.* in preparation (2013).

30 D. Markham, B. C. Sanders, *Graph State for Quantum Secret Sharing.* Phys. Rev. A, **78**, (2008).

31 S. Oum, P. Seymour. *Approximating rank-width and clique-width quickly.* Journal ACM Transactions on Algorithms (TALG), vol 5, 1-20 (2008).

32 D. Schlingemann, R. F. Werner, *Quantum error-correcting codes associated with graphs.* Phys. Rev. A, vol. 65, p. 012308 (2001).

33 A. Shamir, *How to share a secret.* Communications of the ACM, **22**, 612–613 (1979).

34 L. Sheridan, V. Scarani, *Security proof for quantum key distribution using qudit systems.* Phys. Rev. A **82**, 030301(R) (2010).

35 M. Van den Nest, J. Dehaene, B. De Moor *Graphical description of the action of local Clifford transformations on graph states.* Physical Review A (69) 022316 (2004).

A Appendix-QQ Encoding-Decoding Operations

The QQ encoding-decoding can basically be done by three typical ways. The first method is based on projective Bell measurements (possibly extended to a $|B|+1$ length state) and the two last one are accessible by local measurements and/or series of two qudit control operations, which should finally result in a similar experimental complexity. We briefly describe the three encoding methods $E1, E2, E3$ and decoding $D2, D3$. ($D1$ has been done in section 4.1). For a graph $G=(V,\Gamma)$, with $d,u \in V$ such that $\Gamma(d,u)\neq 0$, $W:=V\backslash\{d\}$, a quantum secret $|\xi\rangle_S := \sum_{i=0}^{q-1} s_i|i\rangle_S$, we write $\bar{X} := Z_{\Gamma.\{d\}}$ and $\bar{Z} := (X_u Z_{\Gamma.\{u\}})^{-\Gamma(u,d)^{-1}}$, as they act like logical operators over the bases states over W, that is $\bar{Z}|i_L\rangle = \omega^i|i_L\rangle$, $\bar{X}|i_L\rangle = |(i+1)_L\rangle$ with notation of 4.1.

E1 $|\xi\rangle|G\rangle = \sum_{i\in\mathbb{F}_q} s_i|i\rangle_S \sum_{j\in\mathbb{F}_q} \frac{|j\rangle_D|j_L\rangle_W}{\sqrt{q}}$
$= \frac{1}{\sqrt{q}}\sum_{i,j\in\mathbb{F}_q}|i\rangle_S|j\rangle_D s_i|j_L\rangle_W = \frac{1}{\sqrt{q}}\sum_{l\in\mathbb{F}_q} I_S X_D^l \bar{X}_W^l(\sum_{i\in\mathbb{F}_q}|i\rangle_S|i\rangle_D s_i|i_L\rangle_W)$
$= \frac{1}{\sqrt{q}}\sum_{l\in\mathbb{F}_q} I_S X_D^l \bar{X}_W^l(\sum_{k\in\mathbb{F}_q}\sum_{i\in\mathbb{F}_q}\omega^{k.i}\frac{|i\rangle_I|i\rangle_D}{q}\sum_{j\in\mathbb{F}_q}\omega^{-k.j}s_j|j_L\rangle_W)$
$= \frac{1}{\sqrt{q}}\sum_{l\in\mathbb{F}_q} I_S X_D^l \bar{X}_W^l(\sum_{k\in\mathbb{F}_q} Z_I^k I_D \bar{Z}_W^{-k}\sum_{i\in\mathbb{F}_q}\frac{|i\rangle_I|i\rangle_D}{q}\sum_{j\in\mathbb{F}_q}s_j|j_L\rangle_W)$
$= \frac{1}{q}\sum_{l,k\in\mathbb{F}_q} Z_S^k X_D^l(\sum_{i\in\mathbb{F}_q}\frac{|i\rangle_S|i\rangle_D}{\sqrt{q}})\bar{X}_W^l\bar{Z}_W^{-k}\sum_{j\in\mathbb{F}_q}s_j|j_L\rangle_W)$

so that applying the correction: $\bar{Z}^k\bar{X}^{-l}$ over $V\backslash\{d\}$, according to the syndrom (l,k) of a Bell measurement over $\{S,D\}$, leaves the state over W as $\sum_{i\in\mathbb{F}_q} s_i|i_L\rangle$.

E2 $C\bar{X}_{dW}|\xi\rangle|0_L\rangle = \sum_{i\in\mathbb{F}_q} s_i|i\rangle\bar{X}^i|0_L\rangle = \sum_{i\in\mathbb{F}_q} s_i|ii_L\rangle = \sum_{i\in\mathbb{F}_q} s_i X^i|0\rangle|i_L\rangle$
$= \sum_{i\in\mathbb{F}_q} s_i X^i \sum_{j\in\mathbb{F}_q}\frac{|b_j\rangle}{\sqrt{q}}|i_L\rangle = \sum_{i\in\mathbb{F}_q} s_i X^i\sum_j\frac{Z^{-j}|b_0\rangle}{\sqrt{q}}|i_L\rangle$
$= \frac{1}{\sqrt{q}}\sum_{i,j} s_i\omega^{i.j}Z^{-j}|b_0\rangle|i_L\rangle = \sum_{j\in\mathbb{F}_q}\frac{|b_j\rangle}{\sqrt{q}}(\bar{Z}^j\sum_{i\in\mathbb{F}_q}s_i|i_L\rangle)$

where $|b_j\rangle = Z^{-j}|+\rangle$ constitutes the X basis, so that applying the correction $\bar{Z}^{-j}$ over W,

according to the result j of a X_d measurement, leaves the state to distribute as $\sum_i s_i|i_L\rangle$ (see also [2]).

E3 $C\bar{Z}_{dW}H_dC\bar{X}_{dW}|\xi\rangle|0_L\rangle = C\bar{Z}_{dW}H_d(\sum_i s_i|i\rangle|i_L\rangle) = C\bar{Z}_{dW}(\sum_i s_i Z_d^{-i}|+\rangle|i_L\rangle)$
$= \frac{1}{\sqrt{q}}C\bar{Z}_{dW}(\sum_{i,k} s_i|k\rangle\bar{Z}^{-k}|i_L\rangle) = |+\rangle\sum_i s_i|i_L\rangle)$.

The same process can be done for the decoding by an authorised set B, where the operators U_B and V_B defined in 4.1 will act as $\bar{Z}$ and $\bar{X}$ operators respectively. An ancilla qudit $\{a\}$ is prepared in the state $|+\rangle_a$ by B.

D2 ${CV^{-1}}_{aB}|+\rangle_a(\sum_{j\in\mathbb{F}_q} s_j|j_L\rangle_W) = \frac{1}{\sqrt{q}}\sum_{k\in\mathbb{F}_q} X_a^{-k}(\sum_{i\in\mathbb{F}_q} s_i|i\rangle_a)|k_L\rangle_W$.

D3 $CU_{aB}.H_a.\frac{1}{\sqrt{q}}\sum_{k\in\mathbb{F}_q} X^{-k}(\sum_{i\in\mathbb{F}_q} s_i|i\rangle_a)|k_L\rangle_W = \sum_{i\in\mathbb{F}_q} s_i|b_i\rangle_a\sum_{k\in\mathbb{F}_q^m}\frac{|k_L\rangle_W}{\sqrt{q}}$.