

An Abstract Approach towards Quantum Secret Sharing



Vladimir Nikolaev Zamdzhiev

Oriel College
University of Oxford

A thesis submitted for the degree of
MSc Computer Science

August 31, 2012

Contents

1	Introduction	1
1.1	Related Work	2
1.2	Outline	2
2	Background	3
2.1	ZX Calculus	3
2.1.1	Syntax and Semantics	3
2.1.2	Rewriting Rules	5
2.1.3	Classical vs Quantum Information in the ZX Calculus	9
2.1.4	Examples	10
2.2	Quantum Secret Sharing	13
3	HBB Protocols	15
3.1	HBB CQ (n,n) protocol	15
3.1.1	State and secret distribution	15
3.1.2	Secret Reconstruction	16
3.1.3	Secret inaccessibility	18
3.2	HBB QQ (2,2) protocol	18
3.2.1	State and secret distribution	19
3.2.2	Secret Reconstruction	19
3.2.3	Secret inaccessibility	21
4	Graph State Protocols	24
4.1	Graph States in the ZX Calculus	24

4.2	CC (n,n)	26
4.2.1	State and secret distribution	26
4.2.2	Secret Reconstruction	27
4.2.3	Secret inaccessibility	28
4.3	CC (3,4)	30
4.3.1	State and secret distribution	30
4.3.2	Secret Reconstruction	30
4.3.3	Secret inaccessibility	33
4.4	CC (3,5)	35
4.4.1	State and secret distribution	36
4.4.2	Secret Reconstruction	36
4.4.3	Secret inaccessibility	46
4.5	CQ (n,n)	49
4.5.1	State and secret distribution	49
4.5.2	Secret Reconstruction	49
4.5.3	Secret inaccessibility	59
4.6	CQ (3,5)	59
4.6.1	State and secret distribution	60
4.6.2	Secret Reconstruction	60
4.6.3	Secret inaccessibility	70
4.7	QQ (n,n)	70
4.7.1	State and secret distribution	70
4.7.2	Secret Reconstruction	71
4.7.3	Secret inaccessibility	76

5 Conclusion

Chapter 1

Introduction

In this thesis we prove in a formal and rigorous way the correctness of some aspects of quantum secret sharing protocols. We do not use the traditional Hilbert space formalism to reason about quantum computation, but we instead approach the problem from another, more abstract perspective. All of our proofs are written in the ZX calculus [10] - a diagrammatic language developed from the study of categorical quantum mechanics [4].

Secret sharing was independently introduced by George Blakley[14] and Adi Shamir[3] in 1979. The problem consists of a dealer who needs to encode and send a secret, in such a way, that some sets of players can recover the secret information by working together and all other sets of players do not obtain any information about it. Secret sharing is an important problem in cryptography and as such has been studied extensively[1]. Quantum secret sharing is a type of secret sharing problem, where quantum mechanical phenomena are used to achieve the goal. The information to be shared can be either classical or quantum. In our investigation of these protocols, we will formally prove the correctness of two aspects of quantum secret sharing schemes - the ability of authorized sets of players to reconstruct the secret and the inability of unauthorized sets of players to gain information about the secret. However, in our approach to the problem we do not consider security aspects of the different protocols, like eavesdropping, cheating by players and other types of attacks.

In 1982, Richard Feynman was the first person to propose the idea of a quantum computer[12] - a device which uses the power of quantum mechanics to perform computations. An important discovery made by the mathematician Peter Shor in 1997 has since sparked considerable interest in the field of quantum computation[21]. He proposed a quantum algorithm which solves the integer factorization problem, with high probability, in polynomial time. This algorithm is exponentially faster than any other known classical algorithm which solves the same problem. However, despite this impressive result and active research in quantum computation, there is still little understanding of how quantum algorithms are designed. Perhaps one of the reasons behind this is the Hilbert space formalism, which is the language used to reason about quantum computation and information. This formalism has been immensely successful in describing quantum mechanics, but the description of even the simplest quantum protocols is much more complicated and convoluted than their classical counterparts. Criticism has been raised[7] against it for the relatively late discovery of fundamental protocols, like quantum teleportation[8], considering the timeline of quantum mechanics and quantum computation.

This has lead researchers to consider alternative, more high-level approaches to quantum computation. One such area of study is Categorical Quantum Mechanics, introduced by Abramsky and Coecke in 2004[4]. A central notion in this investigation is that of a dagger compact category. These types of categories have nice graphical representations in the form of diagrammatic calculi. In this thesis, we will be working with one such graphical language - the ZX calculus[10]. It can be used to graphically represent

quantum states and operations. Reasoning in the calculus is performed by rewriting of diagrams via a set of rules which is formally justified. As we will see, the ZX calculus provides a good framework for the study of quantum secret sharing protocols.

1.1 Related Work

In her master thesis[5], Anne Hillebrand studies many different quantum protocols using the ZX calculus. Some of these protocols include the ones presented in chapter 3 in this work. Compared to her work, this thesis is more comprehensive because it considers additional quantum secret sharing protocols. The two works are also different in the approaches used by the authors. Hillebrand's approach uses a simpler version of the ZX calculus based on the categorical properties of the \mathbf{FHilb} category, whereas in this work we are using a rather more complex extension to the calculus which is based on the $\mathbf{CP}(\mathbf{FHilb})$ category. For more information refer to section 2.1.

The differences are crucial and this work models several key characteristics which cannot be represented using Hillebrand's approach. Most notably, the flow of classical information, a key aspect of quantum secret sharing protocols, cannot be represented using Hillebrand's approach. Also, in her investigation, she reasons about measurement by performing case distinction on the measurement outcomes, which are post-selected. We can avoid this by expressing the measurement operation together with the outcome, which leads to a significant decrease in the cases that need to be considered. However, our approach has increased complexity in both the size of diagrams and the number of rewriting steps needed to bring the diagrams to the desired form.

1.2 Outline

Chapter 2 contains an introduction to the ZX calculus and the quantum secret sharing problem. The understanding of the content presented in this chapter is crucial for the rest of the thesis. The chapter does not contain any original work except for a simple derivation of the (U) rewriting rule.

Chapters 3 and 4 contain the original part of the work in this thesis. The chapters consider different classes of quantum secret sharing protocols. In each chapter, different protocols are summarised and their correctness is shown using the ZX calculus. As already mentioned, security aspects of the protocols are not considered in this thesis.

Chapter 2

Background

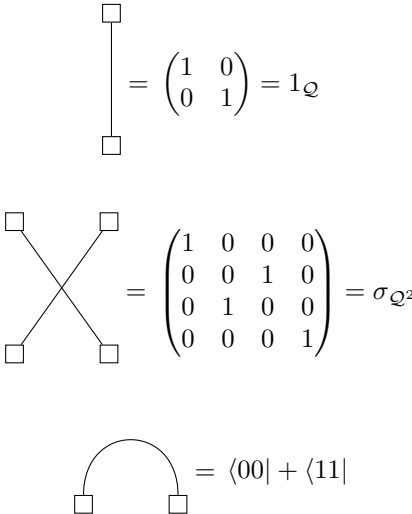
2.1 ZX Calculus

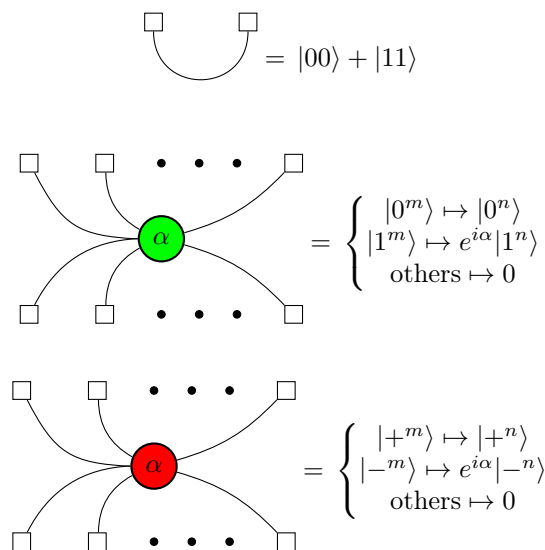
The ZX calculus is a graphical language which can be used to reason about quantum computation. Using this language, we study and prove the correctness of different quantum secret sharing protocols in the chapters that follow.

In this section, we will introduce the reader to the ZX calculus in a way that would allow him to follow the rest of the presentation in this work and we provide references for further reading, which, in addition, also explain the theoretical underpinnings behind it. Original work is a simple derivation of the U rule. The content in the next subsections is a summary of the ZX calculus as presented in [10], [6], [9], [11].

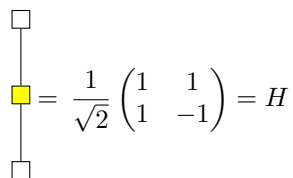
2.1.1 Syntax and Semantics

In this section, we will present the syntax and semantics of the ZX calculus. The semantics are presented in Hilbert space. We begin with atomic diagrams. The square white boxes represent either inputs or outputs. The inputs to the diagrams are located at the bottom and the outputs are located at the top.

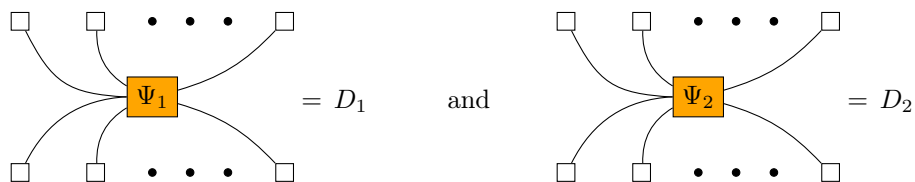




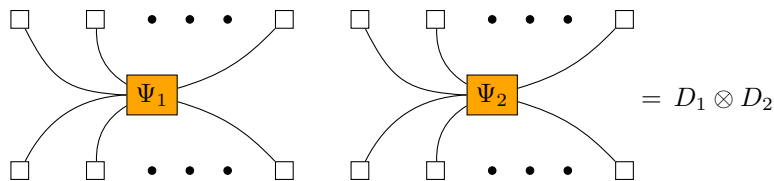
where in the last two diagrams m is the number of inputs and n is the number of outputs. The labels of the red and green dots form the circle group under addition. So, admissible values are $\alpha \in [0, 2\pi)$. We also make the convention that we will not write a label for the points when $\alpha = 0$.

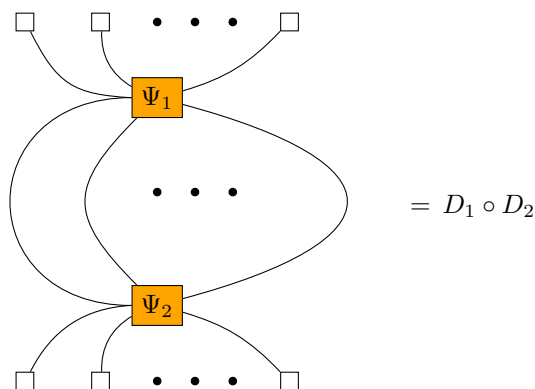


We can create compound diagrams from smaller diagrams in two ways - either placing two diagrams next to each horizontally, or plugging the outputs of one diagram to the inputs of another. Let



then





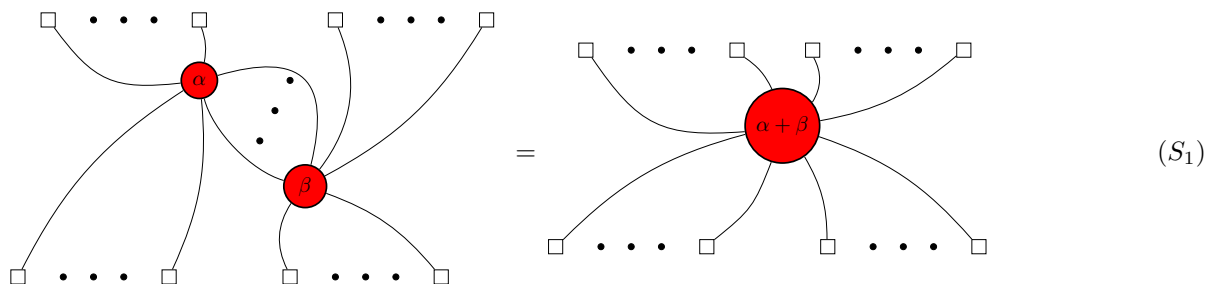
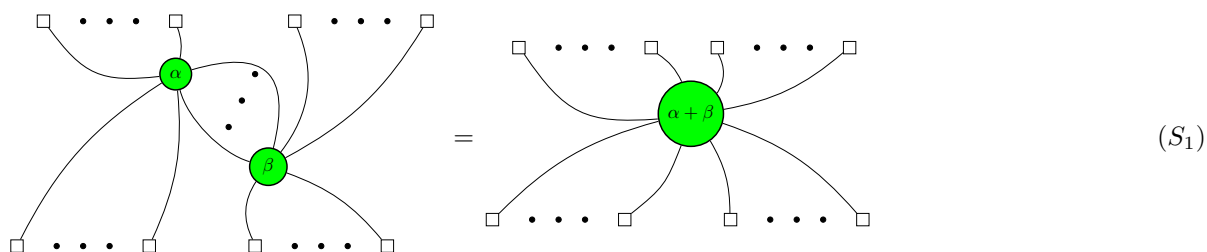
In the latter diagram, the number of outputs of Ψ_2 has to be the same as the number of inputs of Ψ_1 .

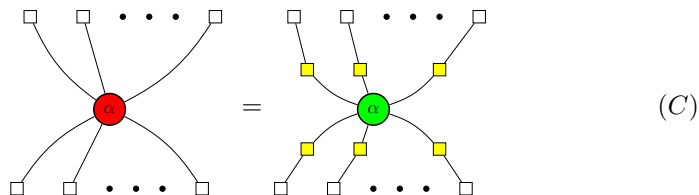
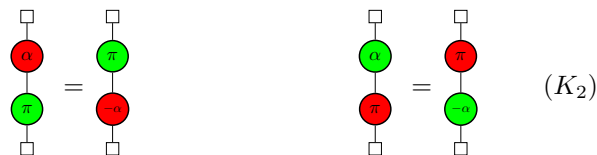
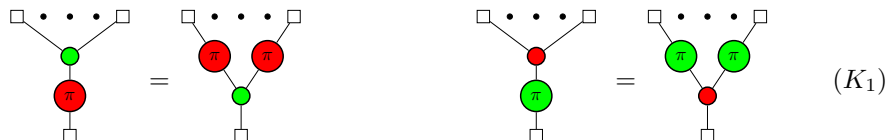
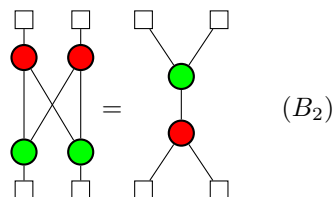
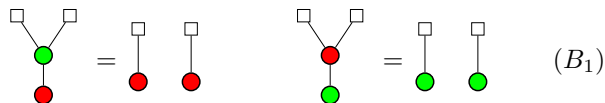
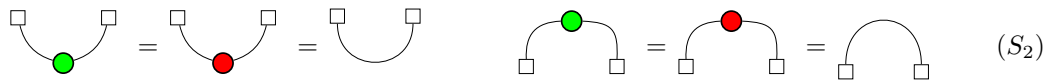
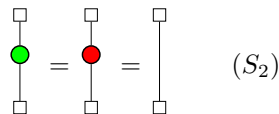
By following the above rules we can represent any pure state map $f : \mathcal{Q}^m \mapsto \mathcal{Q}^n$ as a diagram in the ZX calculus [10].

2.1.2 Rewriting Rules

In this section, we will list the rewriting rules of the calculus. We will first present the basic rules and then some derived ones. The rewriting rules ensure that if one diagram is obtained from another by applying a rule, then the two diagrams have the same Hilbert space interpretation. Note, that the rewriting rules are not normalized. Therefore, all results that we obtain will be true up to a scalar multiple. Note that the set of basic rules is not minimal. Even some of the basic rules can be derived, but we present them in one section in order to maintain consistency with the published works we are summarising.

Basic Rules

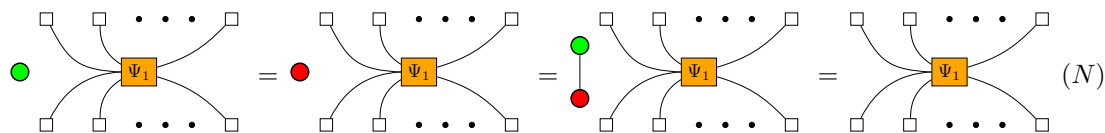




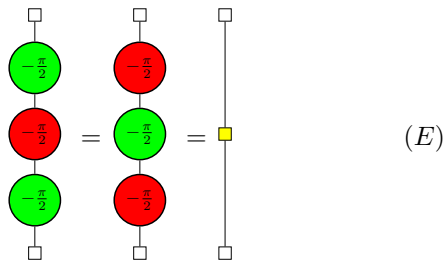
“Only the topology matters” (*T*)

The (*T*) rule means that we are allowed to twist in any way the wires as long as their endpoints remain the same.

When writing down proofs we will explicitly show when we remove scalars from the diagrams using the (*N*) rule.

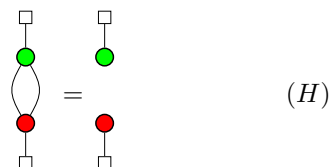


The last basic rule is the Euler decomposition of the Hadamard gate. The rule was not initially included in the ZX calculus, but its inclusion has been later justified [17], [13].



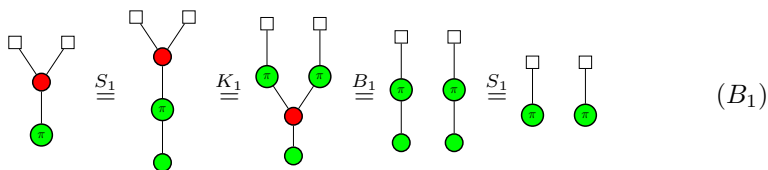
Derived Rules

Here we list some rules which are derivable from the basic rules and which will be used in some of the proofs.

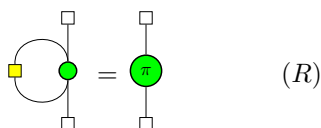
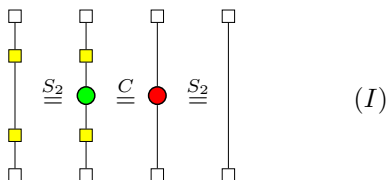


For a proof see [10]. This is also known as the Hopf rule.

The following diagrams : \bullet , \bullet , \bullet , \bullet , are known as classical points. We can show that the points with phase π can also be copied, just like their unphased counterparts and therefore we give this rule the same name (B_1).

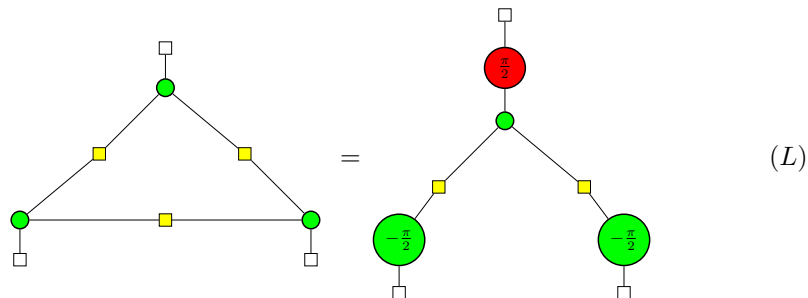


Another derived rule is the (I) rule which says that two Hadamard gates cancel each out.

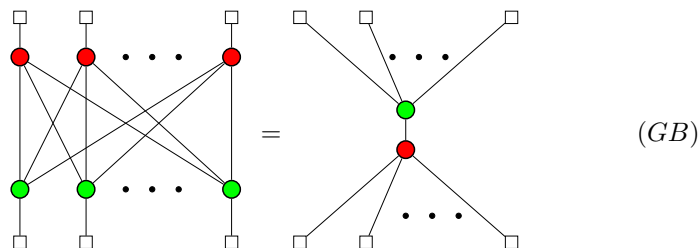


For a proof of the (R) rule, see [17].

In [13], the authors show that the (E) rule is equivalent to local complementation of graph states. For our purposes, it is sufficient to present only the simplest case of local complementation.

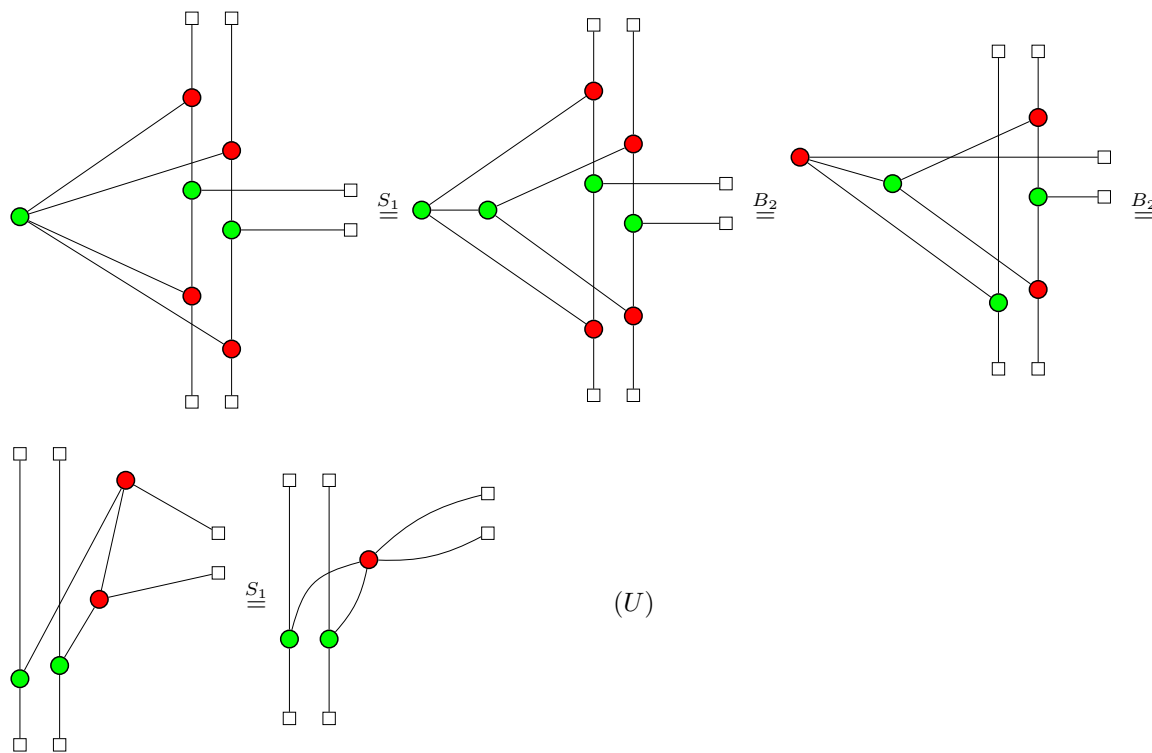


In the same paper [13], the authors introduce the generalised bialgebra rule, which we will refer to as (GB) . It follows from the bialgebra rule (B_2) using an induction argument.



The numbers of inputs and outputs can be different in the above rule.

Finally, we introduce a rule which is useful when working with QQ quantum secret sharing scheme.



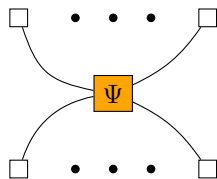
2.1.3 Classical vs Quantum Information in the ZX Calculus

The ZX calculus as presented so far has several key limitations that we would like to address. First, we can only depict measurement operations by post-selecting the measurement results. This is undesirable as it leads to many cases which have to be considered for each protocol. More importantly, we also cannot model the flow of classical information, which is a key aspect of all of the quantum secret sharing schemes that we consider. Finally, it is not possible to perform conditional unitary operations, which is needed by some of the protocols we consider.

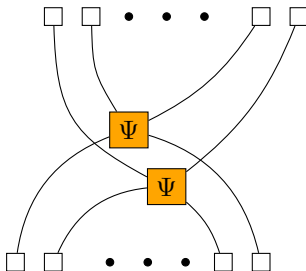
We are able to address all of these issues by using Selinger's CP construction [20]. The approach and how it relates to the ZX calculus is detailed in [6], [11], [9].

The ZX calculus is based on the diagrammatic properties of the category \mathbf{FHilb} - the category of finite dimensional Hilbert spaces. By applying the CP construction to this category, we obtain a new category $\mathbf{CP}(\mathbf{FHilb})$. Its diagrammatic properties are similar to the ones of \mathbf{FHilb} and it allows us to address the limitations identified above. However, this comes at the expense of doubling the size of diagrams who have the same Hilbert space interpretation. The syntax and rewriting rules remain the same. Composition of diagrams and tensor product of diagrams also remains the same as in \mathbf{FHilb} . We will now illustrate how diagrams from \mathbf{FHilb} translate to the new category such that their Hilbert space interpretation remains the same.

Let Ψ be a diagram in \mathbf{FHilb} with Hilbert space interpretation D . Graphically

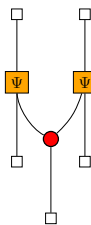


Then the diagram $CP(\Psi)$ in $\mathbf{CP}(\mathbf{FHilb})$ given by :

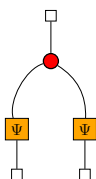


where all the inputs/outputs are paired has the same Hilbert space interpretation D . As a general rule of thumb, quantum information is represented by double wires and classical information is represented by single wires. It should be clear from the context when we are working with classical or quantum information.

The CP construction allows us to represent conditional unitary operations. They will be of the following general form



Destructive effects, which include measurements, have the form



The next section provides examples which are relevant to our study of quantum secret sharing protocols.

2.1.4 Examples

In this section we provide examples for quantum states and operations which will be used extensively when investigating the different protocols. The reader should keep in mind that in our study of quantum secret sharing protocols, we will be working with the diagrams representing morphisms from $\text{CP}(\text{FHilb})$ and should make sure to understand how these diagrams relate to their Hilbert space interpretations. We also provide the FHilb diagrams, where possible, so that the reader can get a sense of how the CP construction works.

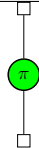
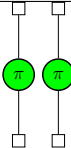
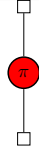
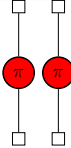


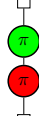
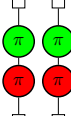
Quantum States

The examples provided are the Z basis states ($|0\rangle, |1\rangle$) which are also known as “the computational basis” states, the X basis states ($|+\rangle, |-\rangle$) and the Bell state ($|00\rangle + |11\rangle$).

\mathcal{Q}^n	FHilb	$\text{CP}(\text{FHilb})$
$ 0\rangle$		
$ 1\rangle$		
$ +\rangle$		
$ -\rangle$		
$ 00\rangle + 11\rangle$		

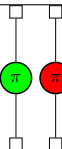
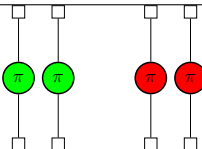
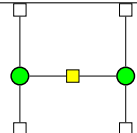
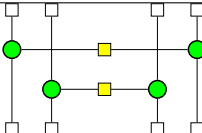
Unconditional unitary operations

All of the presented gates are used extensively. The last example demonstrates composition of unitary operations.

Q^n	FHilb	CP(FHilb)
Z		
X		
H		
$Z \circ X$		

2-qubit gates

The first example illustrates how two unitary gates compose to form a 2-qubit gate and the second one shows the controlled-Z gate, whose use in creating entangled states is fundamental in the graph state class of protocols.

Q^n	FHilb	CP(FHilb)
$Z \otimes X$		
$\wedge Z$		

In the remaining examples we illustrate concepts which cannot be represented in the category FHilb.

Classical data and operations

In this work we will identify classical data as bits. We therefore use the group $\mathbb{Z}_2 = (\{0, 1\}, \oplus, 0)$ to represent the state space of bits. The group operation can be interpreted as a logical XOR. Then, $1 \oplus s$ would represent a logical NOT operation on bit s .

Classical data can be represented in two equivalent ways. They are distinguished only by the color of the elements which we choose. The presentation below uses green points for bits 0 and 1 and the listed operations use this assumption. If we choose to represent the bits as red points instead, we can get the same operations simply by changing their color. The C rewriting rule allows us to change the color of the data, so we can use a mixture of both approaches by carefully placing \blacksquare elements, where appropriate.

\mathbb{Z}_2^n	CP(FHilb)
0	
1	
$\bigoplus_i^n s_i$	
$s \oplus 1$	
$s \mapsto (s, s, \dots, s)$	



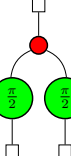
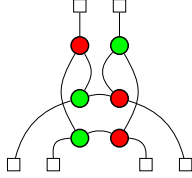
Conditional unitary operations

The two conditional operations shown below depend on a classical bit s . In the case of Z^s , the controlling bit should be green. We will sometimes refer to these operations as “controlled unitary” operations because of this fact. We can see via an application of the copy rule (B_1), that the bit gets copied and depending on its value, the resulting quantum operation will be either the identity or the Z gate.

\mathcal{Q}^n	CP(FHilb)
Z^s	
X^s	

Measurements

A measurement on a qubit is a destructive effect which produces one bit of classical data. Depending on the value of the bit and on the observable used, the observer is able to determine with certainty the new state of the qubit. The table below illustrates how the measurements we will be using look in the ZX calculus.

Q^n	CP(FHilb)
Z-measure	
X-measure	
Y-measure	
Bell basis measurement	

It is important to remember that a Z basis measurement produces red classical data, whereas X and Y basis measurements produce green classical data. A Bell basis measurement produces two bits of data - one bit of each color. If we would like to perform a classical operation on these two bits, then we should convert one of them to the other color via a \square box. Notice that the outcome of measurements can be used as the input bit controlling subsequent unitary operations. This is what we refer to as unitary corrections in latter chapters.

2.2 Quantum Secret Sharing

In this section we provide more details on the quantum secret sharing problem. The section does not contain any original work. The content presented is a summary of the descriptions of the problem in [16] and [19].

All of the protocols we consider in this thesis are (k, n) threshold secret sharing problems. In addition, we are only considering protocols where the dealer has to share one bit or one qubit. In such a problem, a dealer needs to encode and split the secret bit S (or qubit $|S\rangle$) in several parts and send a share to each of the n players in such a way that any k players who work together are able to reconstruct the secret independently from the actions of others and any set of less than k players cannot do so. If the latter set of players obtain no information about the secret, then we say that the sharing scheme is perfect.

In [19] the authors introduced a classification of quantum secret sharing problems and we will use it in this work. However, we first need to explain the distinction between private and public communication channels. A private channel is a channel which can be assumed to be secure from eavesdropping. Transmitting information on a public channel, however, cannot be assumed to be secure. A classical

(quantum) channel can be used to transmit classical (quantum) data. The authors classify QSS problems into three broad classes. In all three of them, there have to be quantum channels between the dealer and the players, as the dealer needs to send one qubit to each player after preparing the initial state.

CC - sharing a classical secret where all used channels are private. The channels between the players are classical.

CQ - sharing a classical secret where the channels between the dealer and the players are public. The channels between the players can be either classical or quantum and can be either private or public.

QQ - sharing a quantum secret where all the channels between the dealer and the players can be either public or private. The channels between the players are private and can be either classical or quantum.

In this work, we do not consider security aspects of the problems and we assume that all channels are private.

When investigating a (k, n) protocol, we will formally prove the correctness of two aspects - the ability of k players to reconstruct the secret independently and the inaccessibility of the secret to any set of $k - 1$ players. For the latter aspect, we demonstrate that the secret is denied to any set of $k - 1$ players when the remaining players are performing certain actions. This indicates that they cannot independently reconstruct the secret and proves the correctness of the protocol, excluding some security considerations, which we ignore in this work.

Chapter 3

HBB Protocols

In 1999, Hillery, Buzek and Berthiaume proposed the first quantum secret sharing protocols[16]. We will refer to their protocols as HBB. In that work, they first describe a (2,2) CQ scheme using the Greenberger-Horne-Zeilinger (GHZ) state[15]. Next, they modify this protocol so that it can serve as a (2,2) QQ scheme. They also demonstrate how the protocol can be extended to a (3,3) CQ scheme and suggest it can be further generalised to (n, n) schemes. Their protocol has been further extended to arbitrary (n, n) CQ by others [22].

In this work, we will formalise the extended (n, n) protocol and the (2,2) QQ protocol. The extended protocol coincides perfectly with the HBB CQ (2,2) protocol when $n = 2$ in our graphical representation.

3.1 HBB CQ (n, n) protocol

An (n, n) CQ sharing scheme can be implemented by using the generalised n GHZ state.

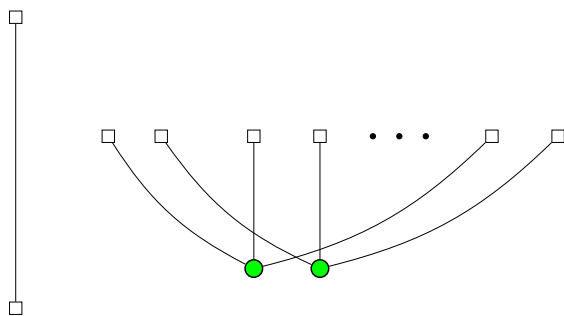
Definition 3.1.1. *The GHZ state is given by $|000\rangle + |111\rangle$*

Definition 3.1.2. *The generalised n GHZ state is given by $|0^n\rangle + |1^n\rangle$*

The protocol makes use of the entanglement properties of the n GHZ state in order to establish a shared key, which is used to encrypt the classical message.

3.1.1 State and secret distribution

In the distribution phase, the dealer prepares the $(n+1)$ GHZ state and sends each player one qubit. The dealer also keeps one qubit for himself. Graphically, the quantum state and classical secret are given by :



The classical secret is encrypted and shared in later steps, after a shared key has been established.

3.1.2 Secret Reconstruction

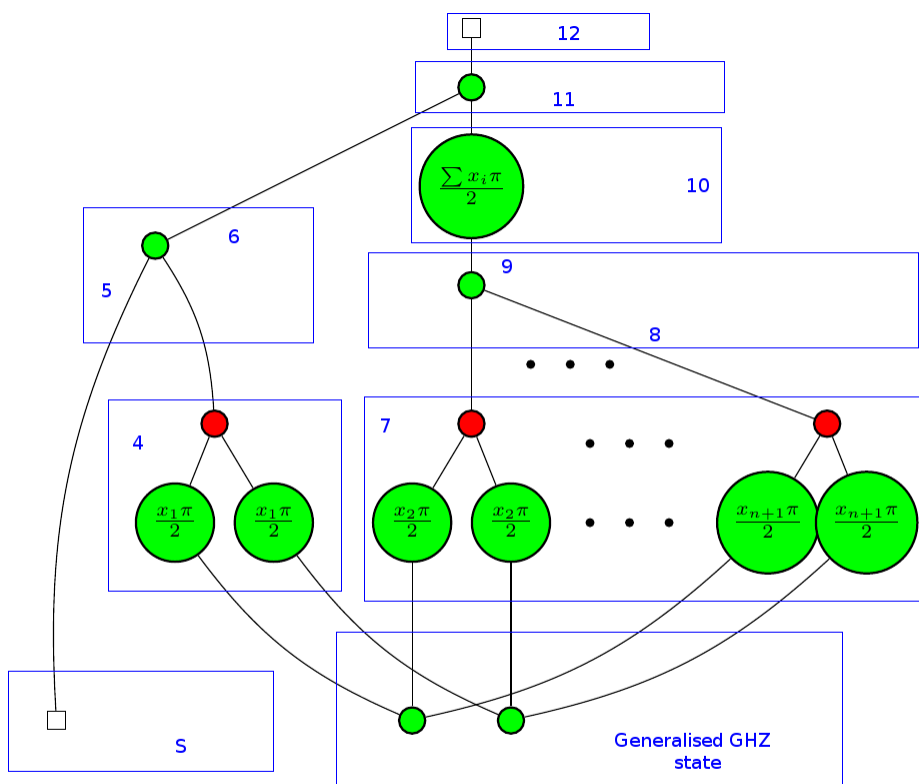


Figure 3.1: HBB CQ measurement protocol

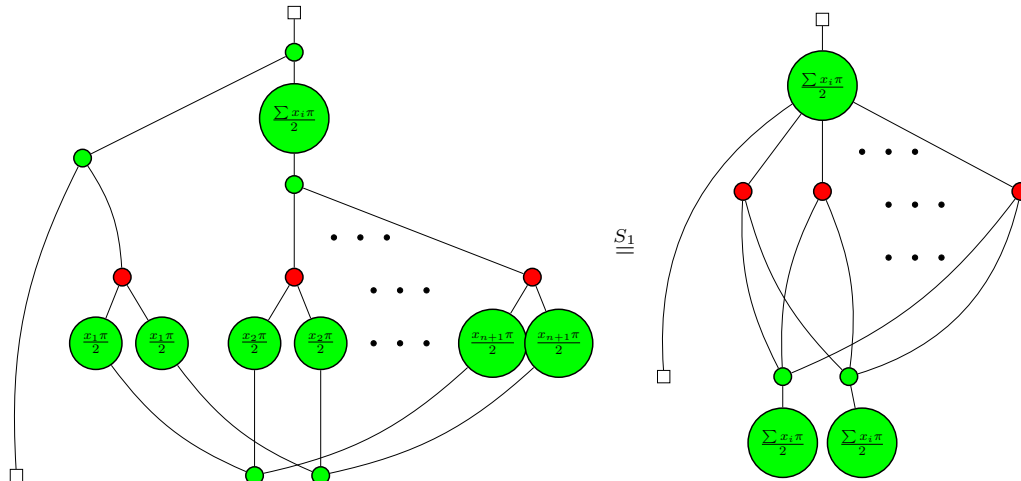
The protocol works by establishing a shared key between the dealer and all of the players, in such a way that all the players need to collaborate together in order to obtain the key. The key is used by the dealer to encrypt the classical input bit S and it is used by the players to decrypt it afterwards. In order to ensure security, the authors introduce randomness when performing the measurements. The dealer and the players have to choose one of two measurement directions at random and then announce

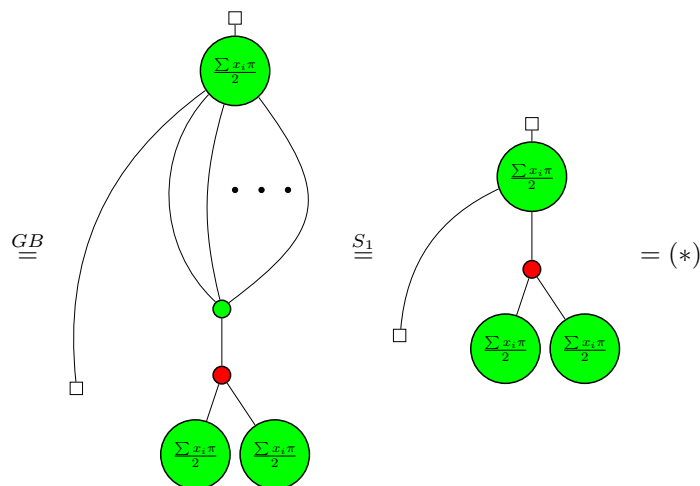
it publicly to the rest. After learning the measurement directions of everyone, the players decide whether to continue with the protocol or restart it, until favorable measurement directions have been selected. The exact steps which have to be performed by the dealer and the players are summarised below :

Without loss of generality, we assume that player 1 will be the one to receive the classical secret and that after doing so, he will send a copy to the other players. Figure 3.1 illustrates how the steps of the algorithm are formalised in the graphical language.

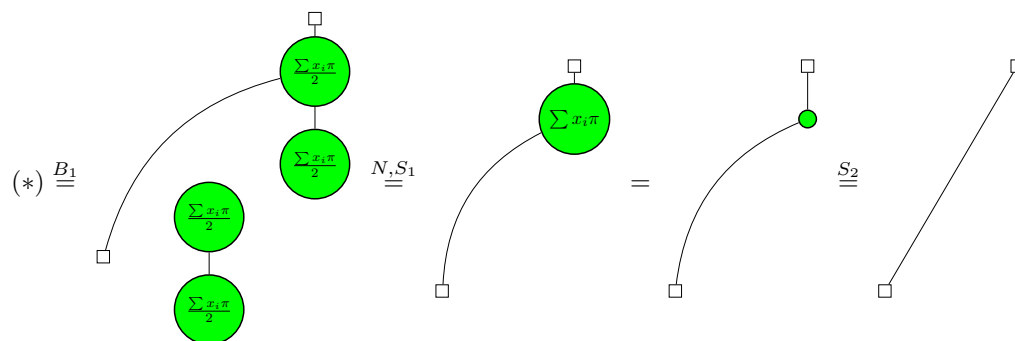
1. The dealer and all players randomly choose a measurement direction - either X or Y . We can depict this by assigning a boolean variable x_i to each player and the dealer. $x_i = 1$ iff player $i - 1$ has chosen Y for his measurement direction (x_1 is the direction of the dealer)
2. Each player and the dealer publicly announce their measurement directions
3. The players and the dealer restart the protocol if $\sum x_i$ is odd, i.e. there is an odd number of Y measurements. Otherwise, the protocol proceeds to the next step
4. The dealer measures his qubit in the selected direction
5. The dealer encrypts the classical bit S with the measurement outcome. This is achieved by adding modulo 2 the two bits.
6. The dealer sends the encrypted message to all players (player 1 will decrypt it, so we depict only this scenario)
7. Every player measures his qubit in the selected direction
8. All players send their measurement outcomes to player 1.
9. Player 1 sums all measurement outcomes (including his) modulo 2.
10. Depending on the announced measurement directions, player 1 performs a negation on the result of the previous step. He performs a negation iff $\sum x_i$ is divisible by 2, but not by 4.
11. Now player 1 has obtained the shared key and he uses it to decrypt the bit he received from the dealer. This is done by adding modulo 2 the two bits.
12. Player 1 has the secret bit S

We formalize steps 4-12 in the ZX calculus and we can show the correctness of the protocol.





We can further simplify this diagram, because all players and the dealer announce their measurement directions (x_i). If the sum x_i is odd, then the protocol is reset and players have to announce new measurement directions. Therefore, for the rest of the proof, we can assume that the sum is even, which means that it corresponds to a classical point for the red observable and will therefore be copied.



3.1.3 Secret inaccessibility

There is nothing to depict graphically for this aspect of the protocol. If there is one player who is not collaborating, then he will not announce a measurement direction, the dealer will not continue with the protocol any further and will not send a message to the players.

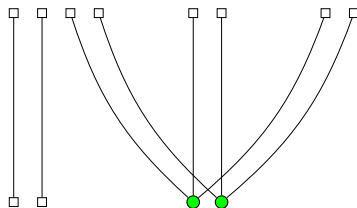
This proves that the algorithm realises an (n, n) classical secret sharing scheme.

3.2 HBB QQ (2,2) protocol

In the same paper, the authors modify the first proposed protocol to realise a (2,2) QQ scheme. In the next subsections we summarise and explain how the protocol works and we also express and prove the correctness of the protocol in the graphical language.

3.2.1 State and secret distribution

The dealer prepares and distributes the GHZ state which is entangled with an extra qubit $|S\rangle$, which is the quantum state to be shared. The two players are each in possession of one qubit of the GHZ state. The dealer has the remaining qubit of the GHZ state and also the qubit $|S\rangle$. Graphically :

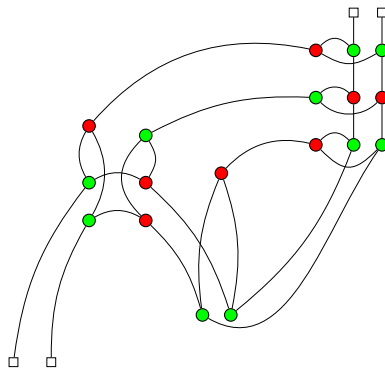


3.2.2 Secret Reconstruction

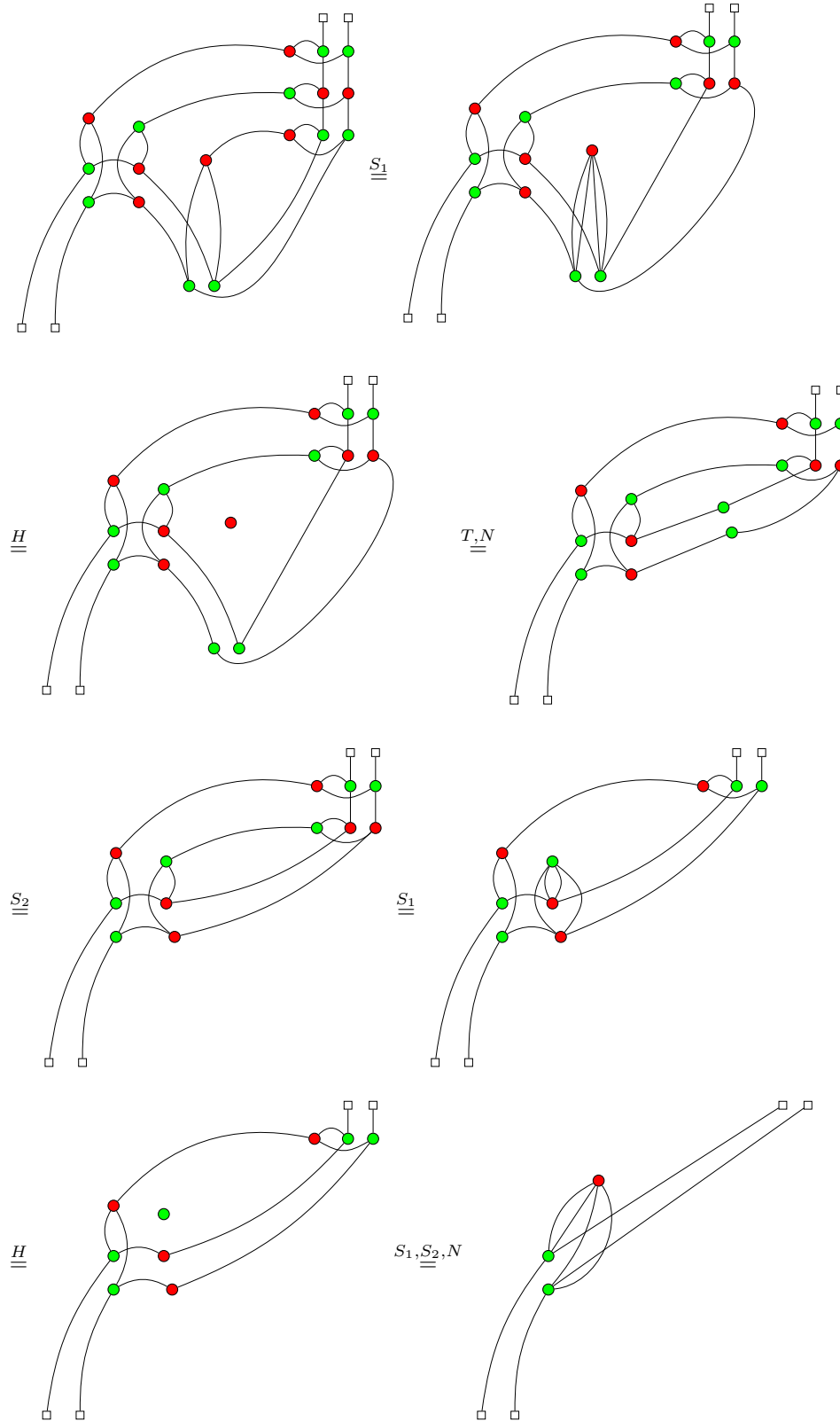
Without loss of generality, we assume that the second player will receive the quantum secret. The reconstruction of the secret is then performed by the following steps :

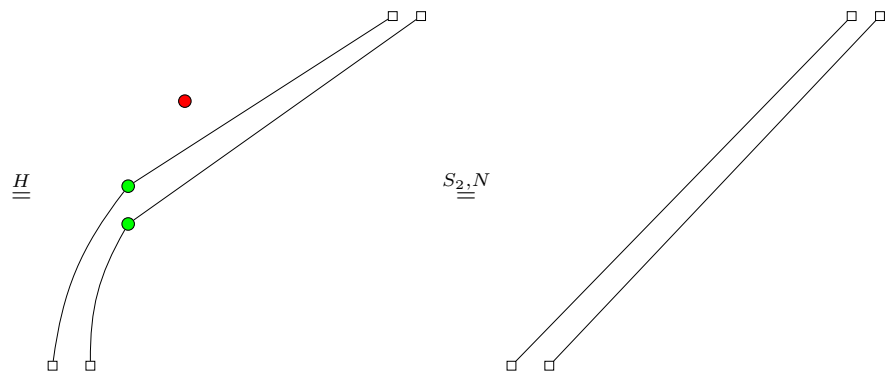
1. The dealer measures his qubits in the Bell basis and sends two classical bits (d_1, d_2) to player 2 to inform him of the measurement outcome
2. Player 1 measures his qubit in the X basis and sends a classical bit (p_1) to player 2 to inform him of the outcome
3. Player 2 performs the unitary correction $Z^{p_1 \oplus d_1} \otimes X^{d_2}$
4. Player 2's qubit is now in the state $|S\rangle$

Graphically, this is represented by



We can now prove, using the ZX calculus, that the above steps indeed result in state $|S\rangle$ being teleported to player 2.

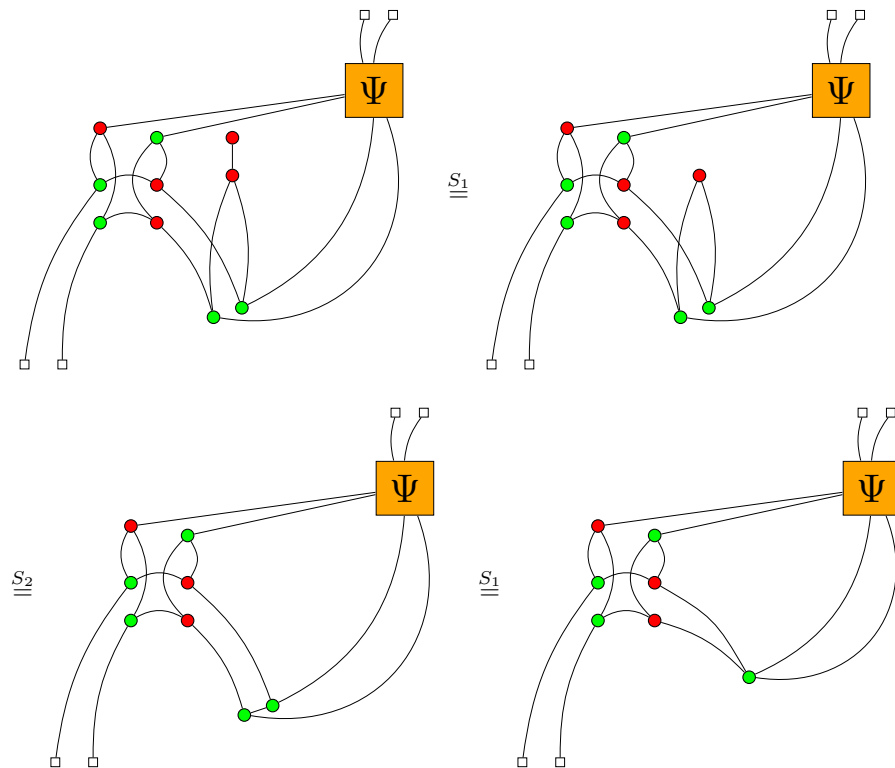


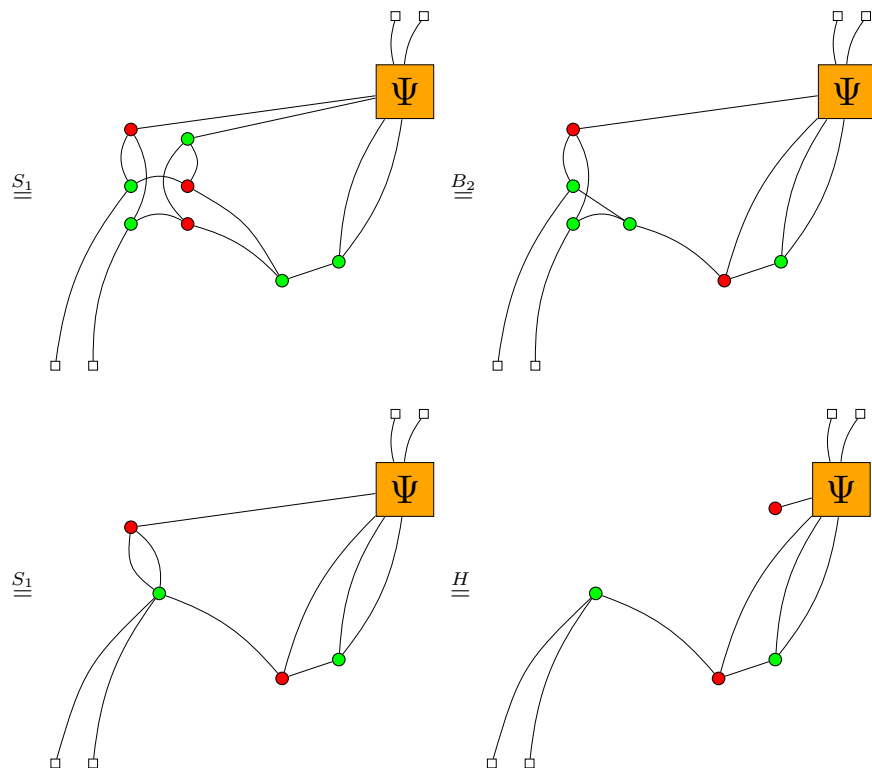


3.2.3 Secret inaccessibility

We will now show that the secret is inaccessible to only one player. Without loss of generality, let's assume that player 2 wants to receive and reconstruct the secret qubit. We will show that player 2 is unable to reconstruct the state $|S\rangle$, when player 1 performs an X measurement on his qubit and does not inform player 2 of the outcome. This means, that one player cannot independently obtain the secret and thus this is an example of a (2,2) QQ sharing scheme.

In the diagrams below, Ψ is an arbitrary diagram with one quantum input and two classical inputs. It is used to represent arbitrary actions on behalf of player 2, given all the information available to him.

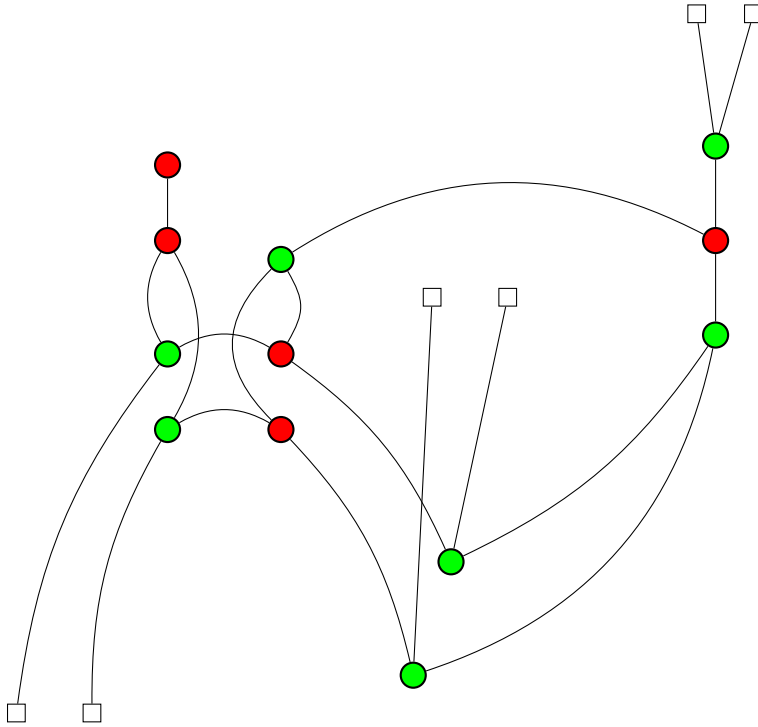




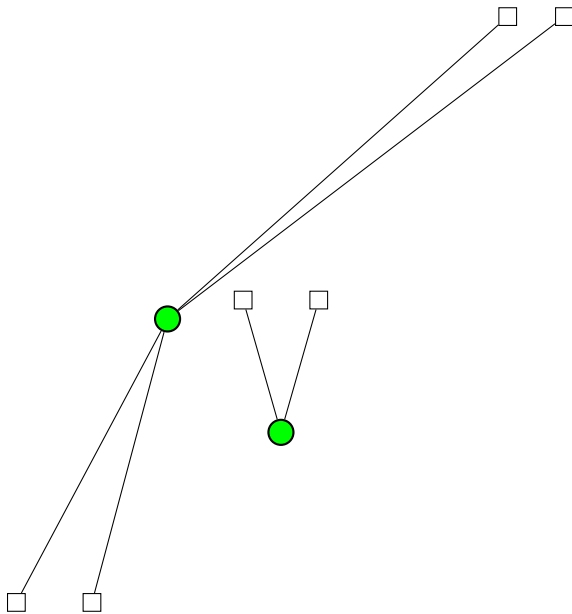
The last diagram reveals that, for any Ψ , the diagram cannot compute the identity function. This can be seen by plugging in states $|+\rangle$ and $|-\rangle$, which result in the same behaviour. Therefore, the secret is denied to the player.

Computationally, this is equivalent to the dealer performing a measurement in the computational basis on the secret and then sending the measurement outcome to player 2. Clearly, the measurement will destroy the initial state $|S\rangle$ unless it is $|0\rangle$ or $|1\rangle$ and player 2 will be able to obtain only those states with certainty, for a proper choice of Ψ , in this case. Therefore, the sharing scheme is not perfect.

In order to illustrate the error in the authors' claims, we can take Ψ to be the diagram representing the actions of player 2 where he measures in the computational basis and then compares his result with one of the bits which the dealer has send him. Then, he can prepare the correct quantum state to correctly obtain either $|0\rangle$ or $|1\rangle$. Graphically, this is represented by :



Using similar rewriting strategies, we show that the diagram is equivalent to :



And now we can see, that if the secret is either $|0\rangle$ or $|1\rangle$, then player 2 obtains it with certainty, without the help of player 1. So, the sharing scheme is not perfect, contrary to the authors claims.

Chapter 4

Graph State Protocols

In 2008, Markham and Sanders introduced an entire class of quantum secret sharing protocols based on the graph state formalism [19]. The classification of QSS schemes which we presented earlier was first formulated in this work. They describe three CC, two CQ and two QQ protocols in their work. Before deriving these protocols, they propose an extension to existing graph states in order to better encode information which is needed for the protocols to work. They develop their own formalism for working with these graph states and prove some properties which allow one to reason graphically about the accessibility of information in their formalism.

In this chapter, we will formalize all of the described protocols, except for the QQ (3,5) one, in the ZX calculus. The reason for this omission is due to the large number of rewriting steps needed, but the protocol should be provable in the graphical language [17].

4.1 Graph States in the ZX Calculus

In this section, we will provide some key definitions, as presented by the authors in their work, which will allow the reader to follow the rest of the chapter. We also show how these key concepts are represented in the graphical calculus.

Definition 4.1.1. *Given an undirected graph $G = (V, E)$, with $|V| = n$, the graph state induced by G is the n -qubit state*

$$|G\rangle := \prod_{e \in E} \wedge Z_e |+\rangle^n$$

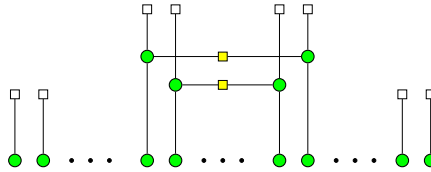
Therefore, any graph $G = (V, E)$ gives rise to a graph state by :

1. Preparing the state $|+\rangle^n$, where n is the number of vertices
2. Applying a $\wedge Z$ gate on qubits (i, j) iff $(v_i, v_j) \in E$

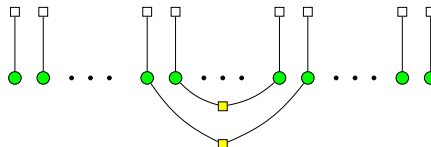
We will now show how graph states can be represented in the ZX calculus. The initial state $|+\rangle^n$ is given by :



Applying a $\wedge Z$ gate on qubits (i, j) has the following effect :



which is equivalent to (via S_1 rule) to :



Therefore, graph states are represented in the ZX calculus by

1. Drawing two green dots for each vertex and connecting each green dot to an output box
2. For every edge $(v_i, v_j) \in E$ connecting one of the green dots representing vertex v_i to one of the green dots representing vertex v_j by a wire and putting a Hadamard gate on the wire. Then do the same for the remaining pair of dots.

The above fact has been recognized in [13] for the unmixd category \mathbf{FHilb} .

Example 4.1.1. *The graph state induced by the cycle graph C_4 , shown in 4.1 is represented in the ZX calculus as :*

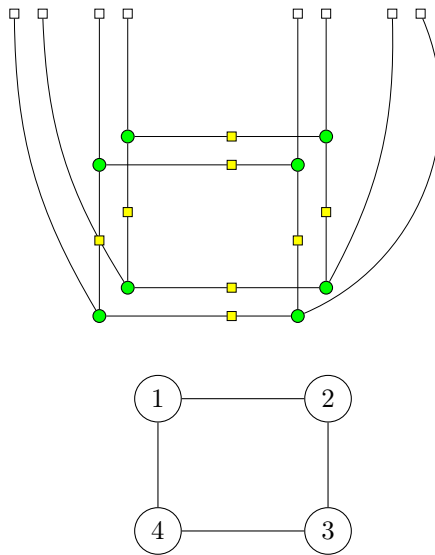


Figure 4.1: Cycle graph C_4

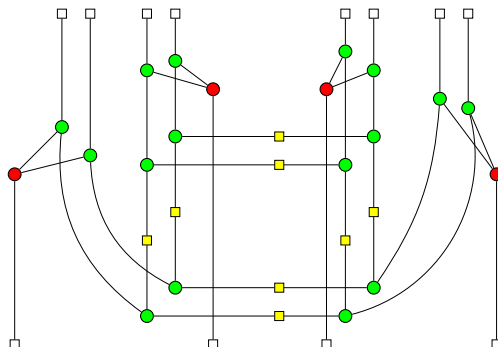
The authors then proceed to extend graph states by adding three bit labels (l_{i1}, l_{i2}, l_{i3}) to each vertex v_i in a graph G , which they use to encode additional information in the extended graph state and also to prove some important properties in their formalization of graph states. For our purposes, however, we are only interested in bit labels l_{i2} and we will present this type of extended graph states, which the authors refer to as “encoded graph states”. We will keep the same notation as the authors to avoid confusion.

Definition 4.1.2. Given a graph $G = (V, E)$ with bit label vector $(l_{12}, l_{22}, \dots, l_{n2})$, the encoded graph state $|G\rangle$ is given by

$$|G\rangle := \bigotimes_i Z_i^{l_{i2}} |G\rangle$$

Therefore, we can obtain an encoded graph state $|G\rangle$ from a normal graph state $|G\rangle$ by performing unitary Z operations on the qubits, whose bit value $l_{i2} = 1$. This is equivalent to doing controlled unitary Z operations, which we already know how to represent.

Example 4.1.2. The encoded graph state induced by the cycle graph C_4 , shown in 4.1, with bit label vector $\mathbf{l} = (l_{12}, l_{22}, l_{32}, l_{42})$ is represented in the ZX calculus as



where the input vector to the diagram is the bit label vector \mathbf{l} represented as green classical data.

Finally, in the sections that follow, we will say that two players are neighbours iff the qubits they own from a given graph state $|G\rangle$ correspond to vertices in G which are connected by an edge.

4.2 CC (n,n)

The first protocol proposed by the authors realises an (n, n) sharing scheme. The initial graph state is induced by the graph in 4.2. All labels are set to zero, except for label l_{12} , which is set to S - the secret bit.

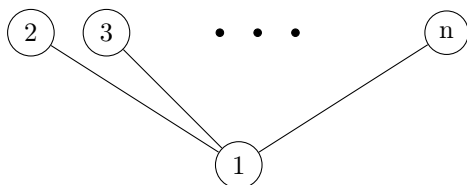
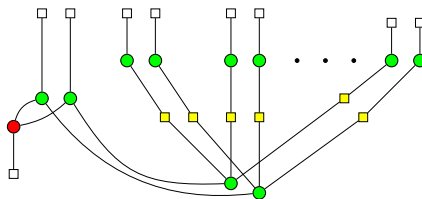


Figure 4.2: CC (n,n) graph

4.2.1 State and secret distribution

The dealer prepares the graph state created from 4.2. Because $l_{12} = S$, the dealer performs a controlled unitary Z operation on qubit 1. Graphically, this is represented by :



The secret S is encoded in the initial state and the dealer does not participate in the rest of the protocol.

4.2.2 Secret Reconstruction

The protocol is executed by all players following this sequence of steps :

1. Player 1 measures in the X basis
2. All other players measure in the Z basis
3. All players send their measurement results to player 3
4. Player 3 adds modulo 2 all measurement outcomes (including his own)
5. Player 3 now has the secret bit S

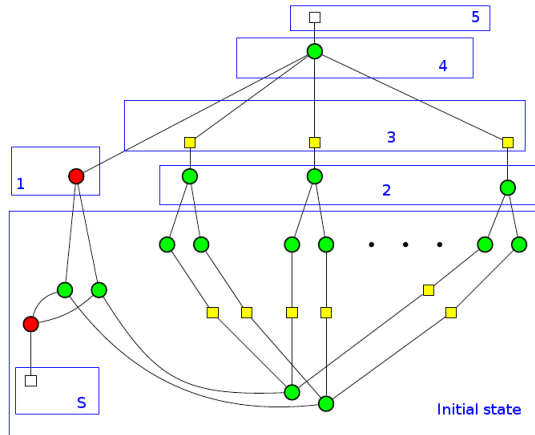
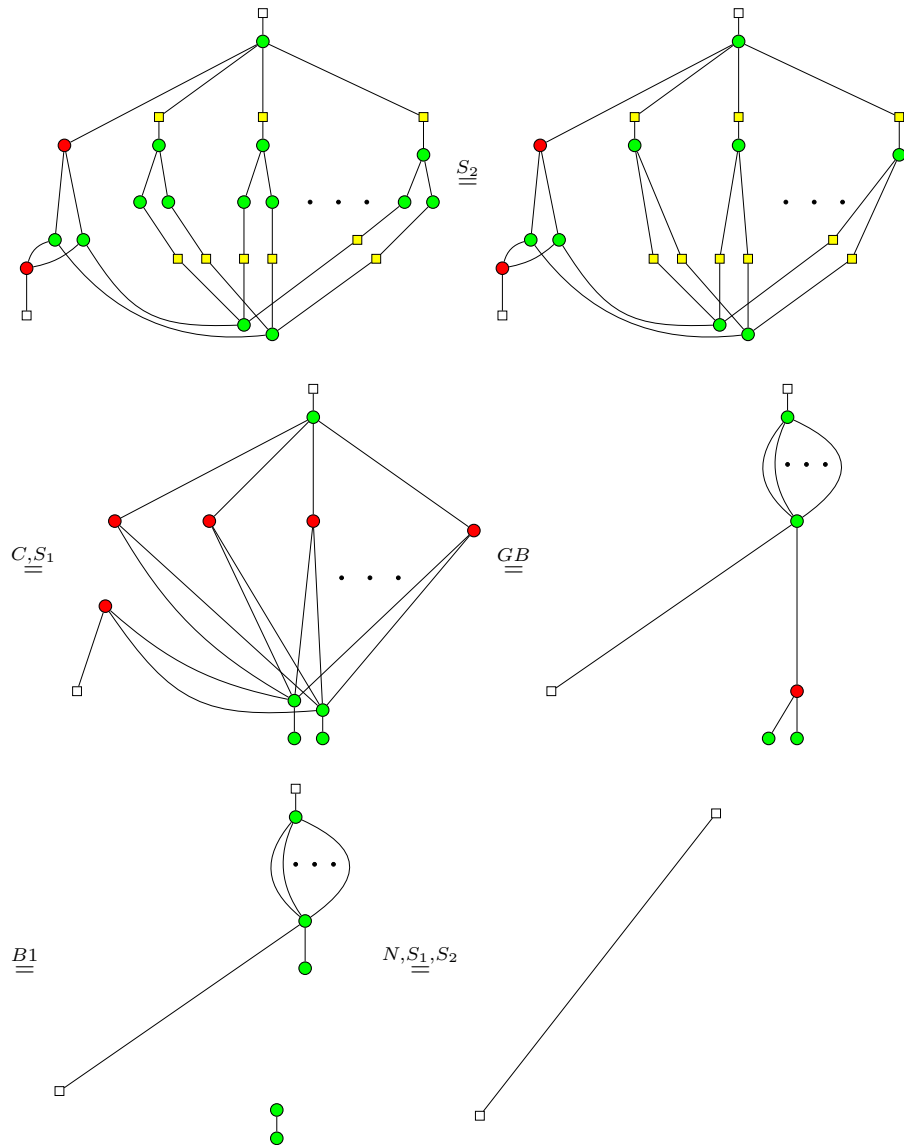


Figure 4.3: CC (n,n) measurement protocol

Above, we simply chose player 3 to reconstruct the classical secret. Any other player can obtain the secret using the same procedure. Moreover, if all players inform all other players of their measurement outcomes, then everybody is able to recover the secret. We just choose only one player in order to simplify the presentation. For an explanation of how each step is formalized, see figure 4.3

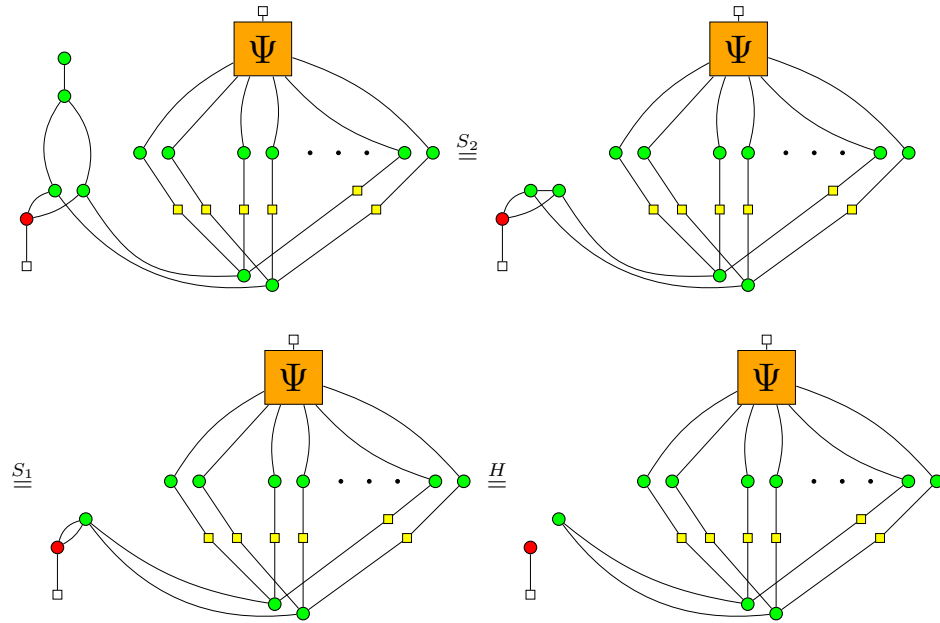
Now we can show the correctness of the protocol. First, we demonstrate that the players are able to reconstruct the secret.



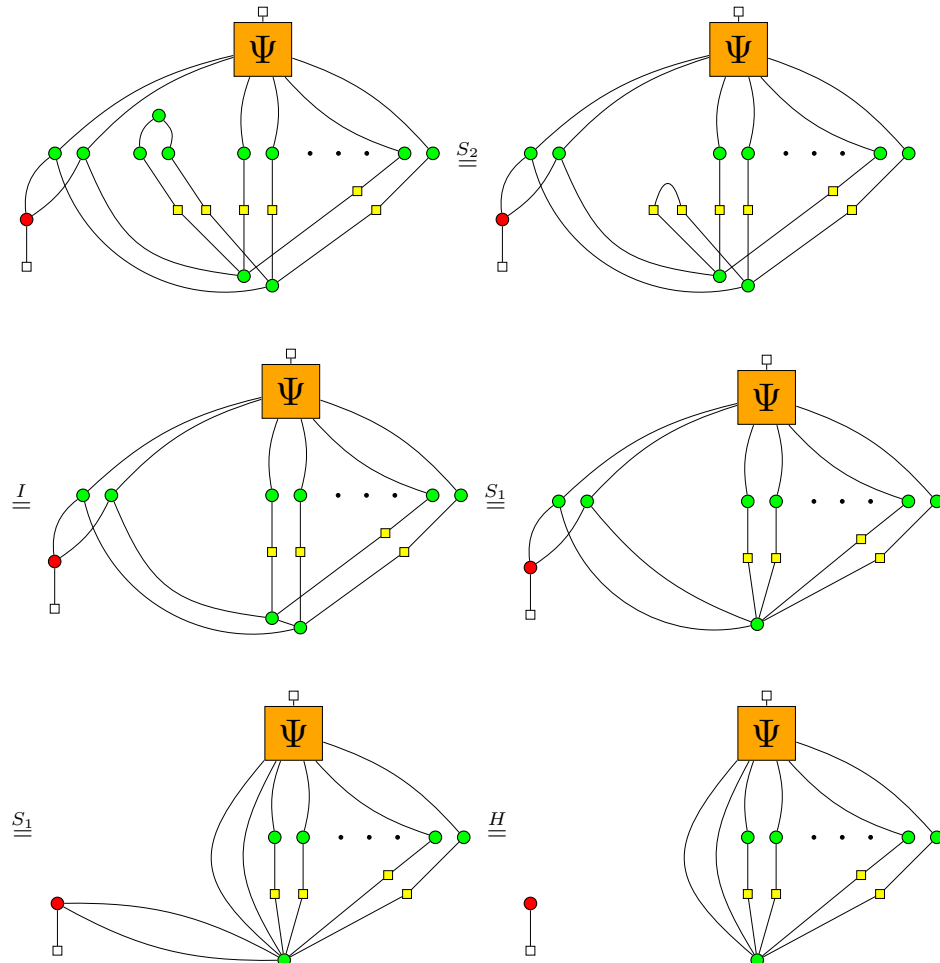
4.2.3 Secret inaccessibility

In this section, we will show that the secret is denied to any set of $n - 1$ players. Due to the structure of the graph, it is enough to consider two cases - player 1 is not collaborating or some other player is not helping (without loss of generality we assume it is player 2). In both cases we examine the information flow when the non-helping player measures his qubit and does not share the result with the other players. In the diagrams that follow, Ψ is used to represent arbitrary actions on behalf of the players with the goal of obtaining the input bit S .

First case - player 1 is not collaborating.



Second case - some player other than player 1 is not collaborating. Without loss of generality, let's assume that is player 2.



We see that the flow of information is disconnected and so the secret is denied to the players, because they are unable to reconstruct it independently from the actions of the non-helping player.

This completes the proof of correctness of the protocol.

4.3 CC (3,4)

The authors discover another CC protocol using the cycle graph C_4 , shown in 4.4. The secret is encoded by setting $l_{12} = l_{22} = l_{32} = l_{42} = S$.

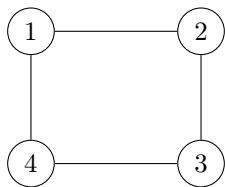
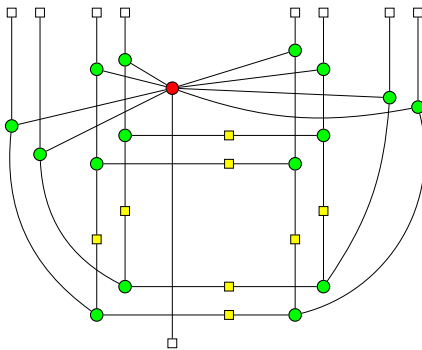


Figure 4.4: CC (3,4) graph

4.3.1 State and secret distribution

The dealer prepares the graph state induced by the graph in 4.4. The secret is distributed, by performing controlled unitary Z operations on each qubit of the graph state. The representation in the ZX calculus is :



The dealer does not do anything else for the remainder of the protocol.

4.3.2 Secret Reconstruction

Any set of three players in the graph are neighbours, so we only have to consider one case. Without loss of generality, we assume that the players who want to obtain the secret are players 1,2 and 3.

The players can carry out the protocol by doing :

1. Players 1 and 3 measure in the computational basis
2. Player 2 measures his qubit in the X basis
3. Players 1 and 3 send their results to player 2
4. Player 2 sums all measurement results modulo 2 (including his own)
5. Player 2 now has the secret S

Again, we choose player 2 to recover the secret, for simplicity of the presentation. Any of the three players can obtain the secret in the same way. Each step is formalized in figure 4.5

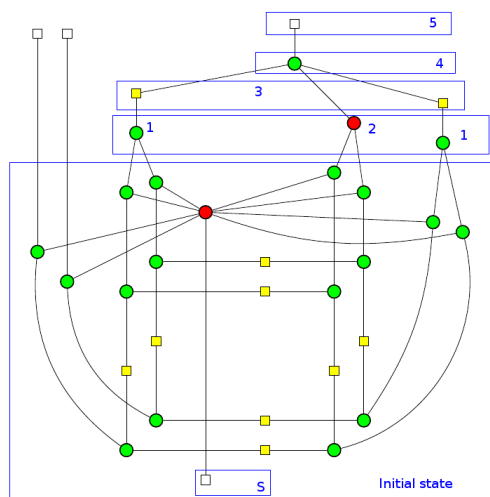
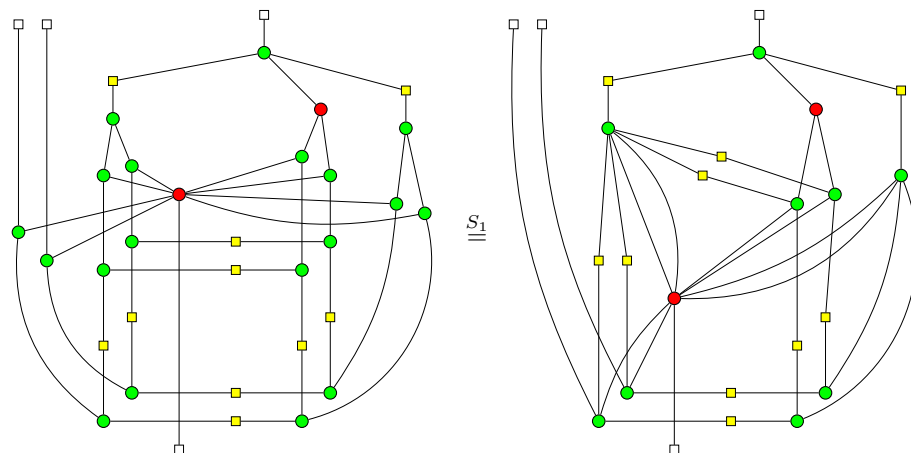
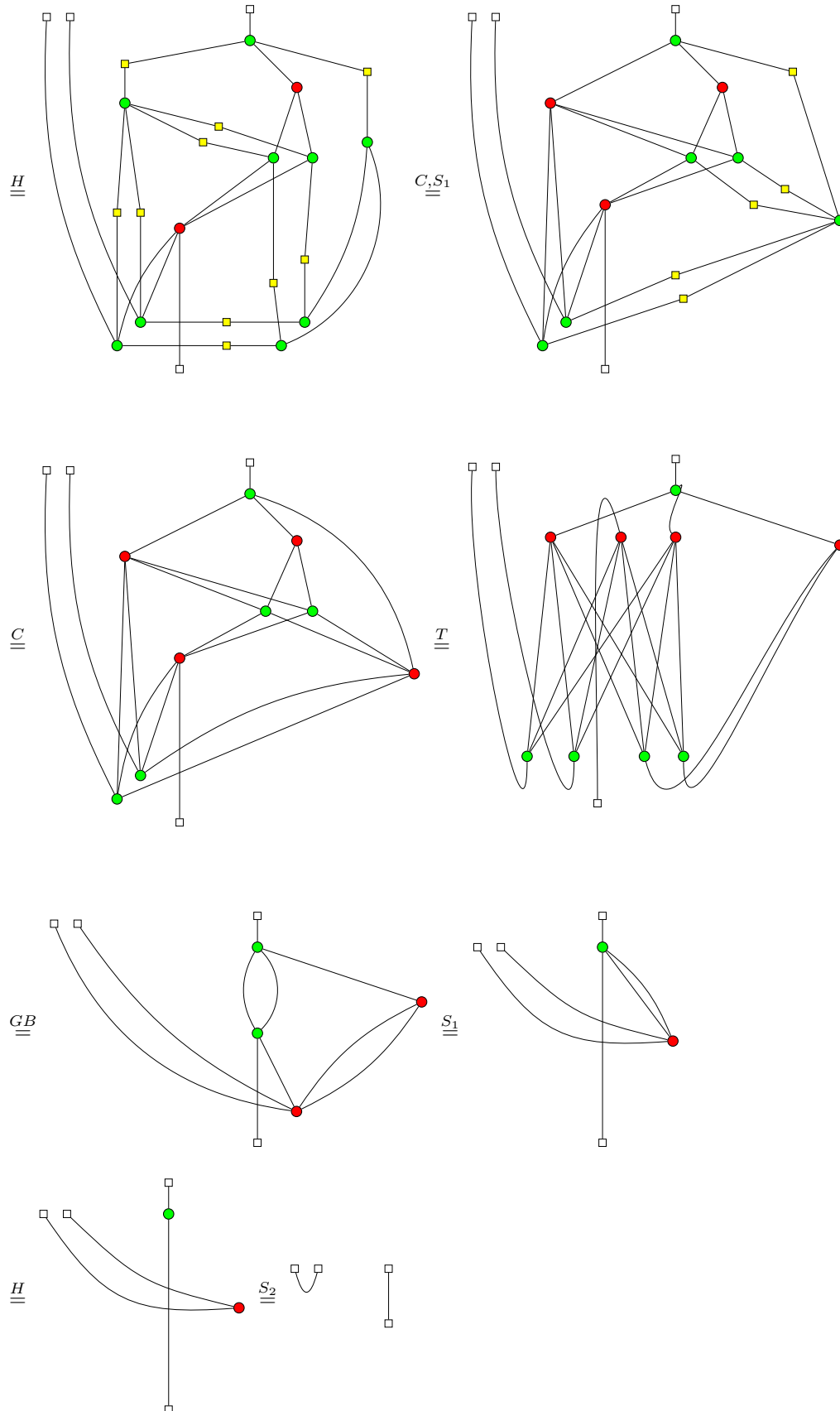


Figure 4.5: CC (3,4) protocol

We can now show that the above steps result in the players recovering the secret.

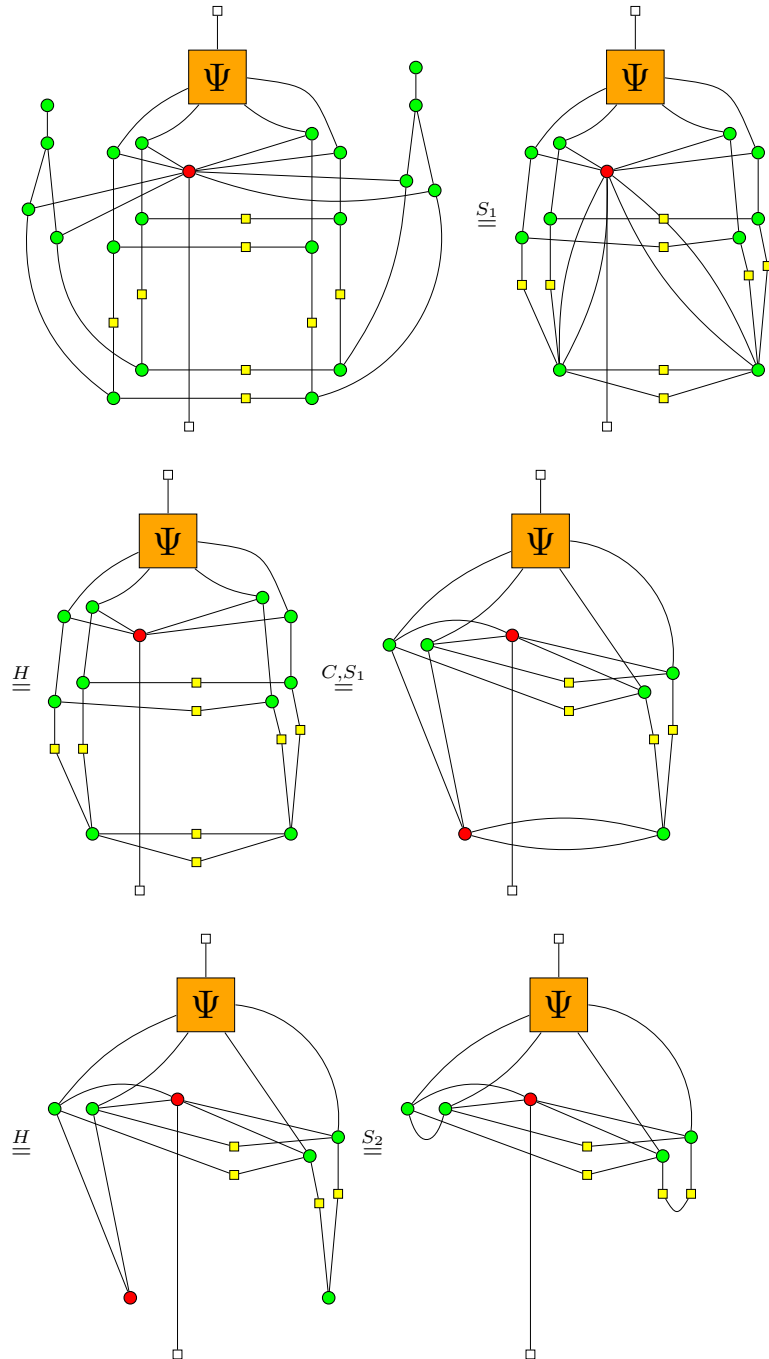


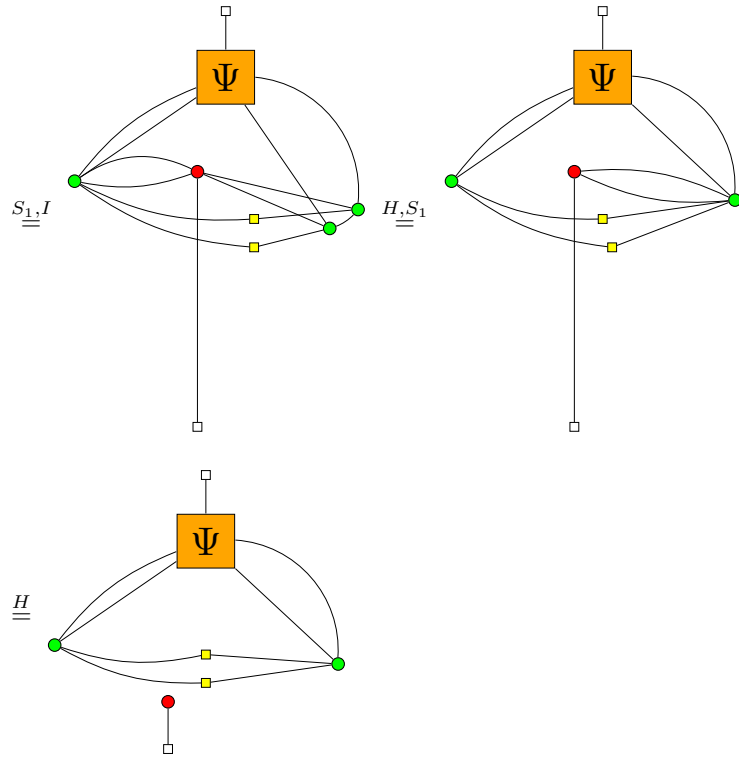


4.3.3 Secret inaccessibility

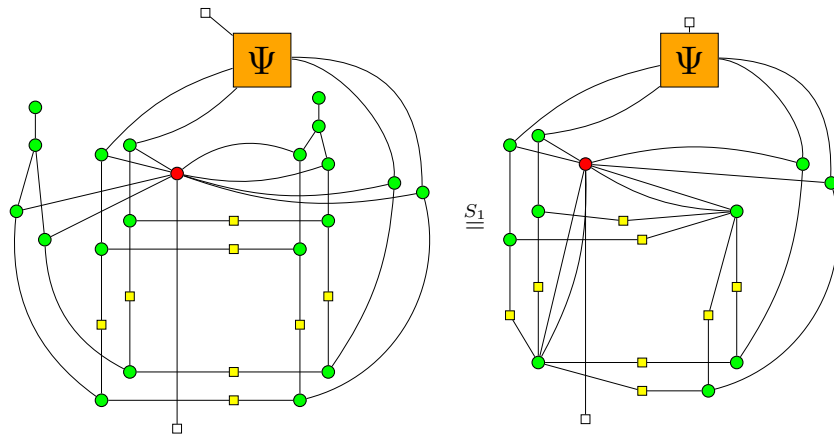
Finally, the secret is denied to any set of two players. We use similar arguments as in the previous protocols - two players will measure their qubits without sharing the results with the others. We will see that no information is recovered by the players, which completes the proof of correctness.

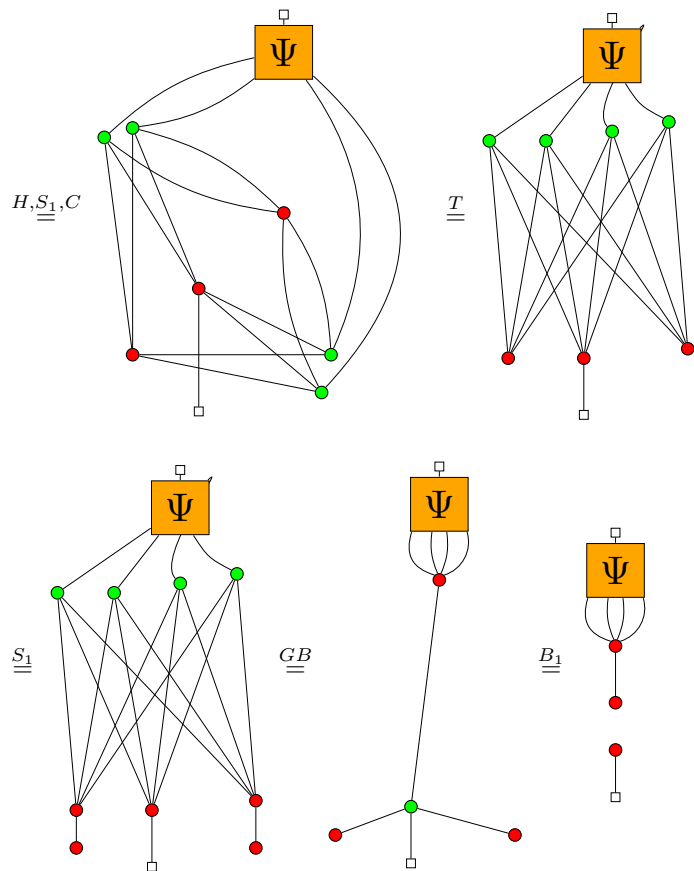
First case - the two collaborating players are neighbours





Second case - the two collaborating players are not neighbours





4.4 CC (3,5)

The final CC scheme described by the authors is a (3,5) threshold scheme. It uses the cycle graph C_5 shown in 4.6. The secret is encoded by setting $l_{12} = l_{22} = l_{32} = l_{42} = l_{52} = S$.

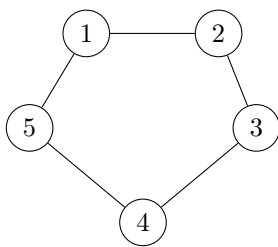
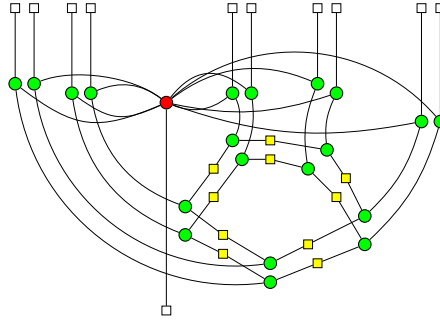


Figure 4.6: CC (3,5) graph

4.4.1 State and secret distribution

The dealer prepares the graph state induced by the cycle graph C_5 . All bit labels l_{i2} are set to S and therefore, the dealer has to perform controlled unitary Z operations on all qubits. Graphically, this is represented as :



The classical secret is encoded and distributed to the players and the dealer's part in the protocol is done.

4.4.2 Secret Reconstruction

We have to consider two cases in order to fully describe the protocol. In the first one, the players who are working together are players 1,2 and 3. The second case is players 1,2 and 4. All other sets of three players fall into one of these cases after rotation of the graph.

Let's consider the protocol for players 1,2 and 3. They can recover the secret by doing :

1. Players 1 and 3 measure in the computational basis
2. Player 2 measures in the X basis
3. Players 1 and 3 send their measurement outcomes to player 2
4. Player 2 sums all measurement results modulo 2 (including his own)
5. Player 2 now has the secret S

The formalization of each step in the ZX calculus is shown in 4.7

We now show that the players can recover the secret by following the above procedure.

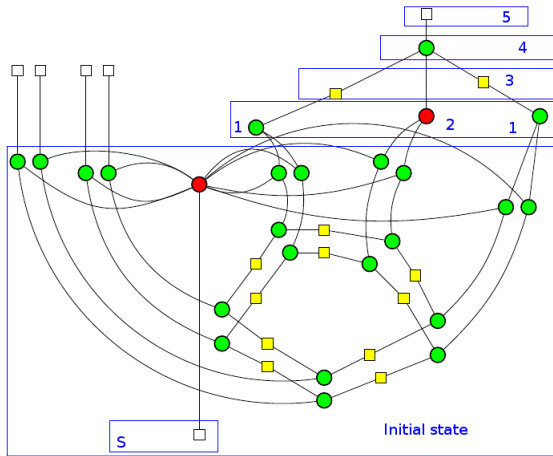
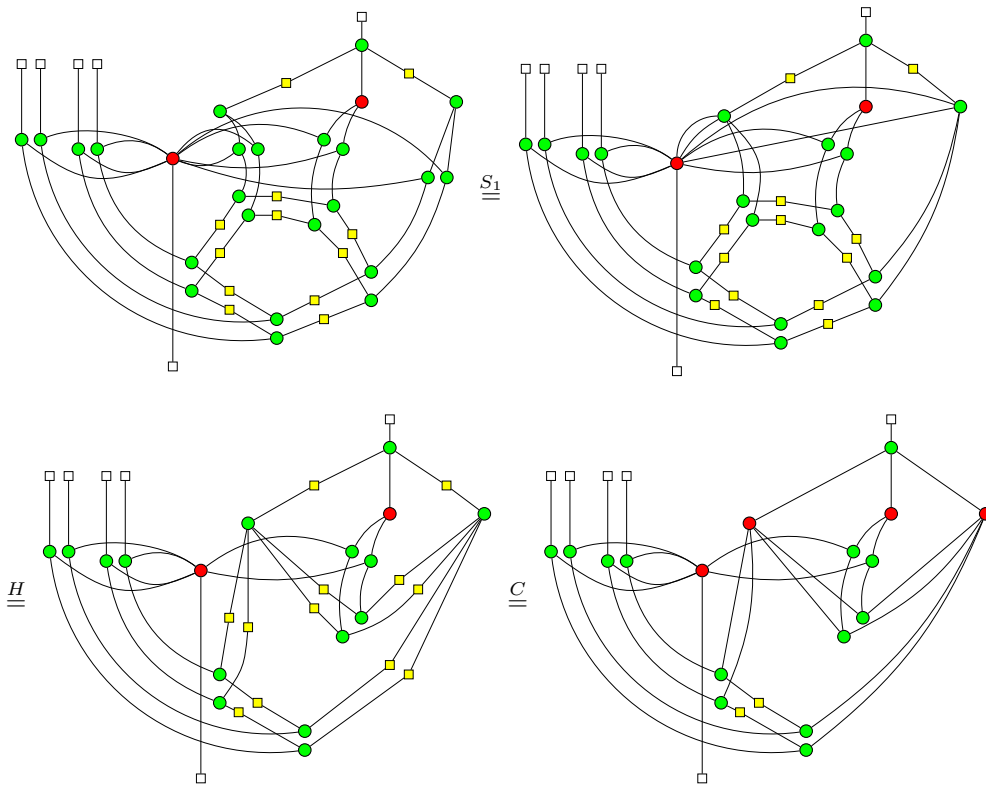
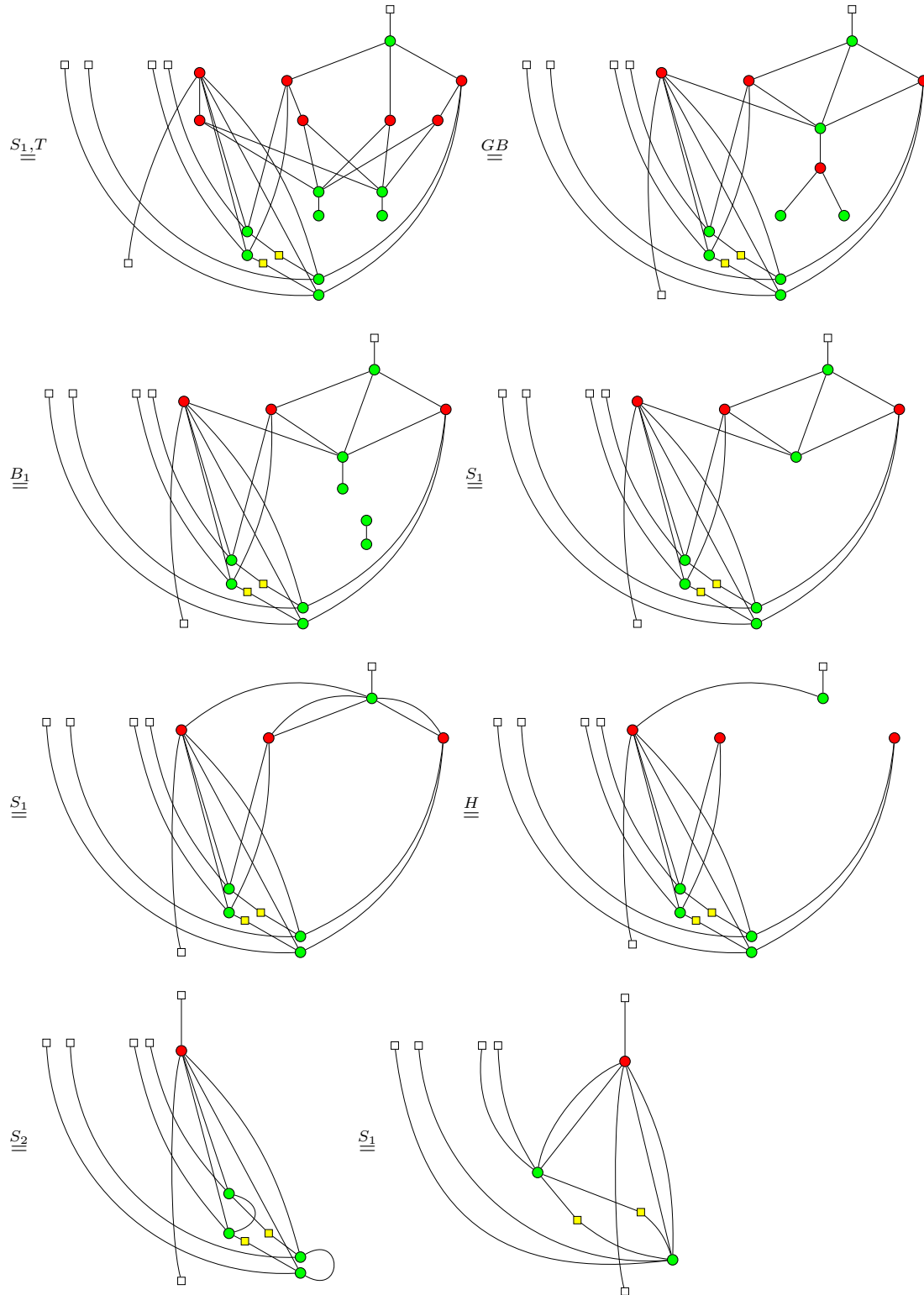
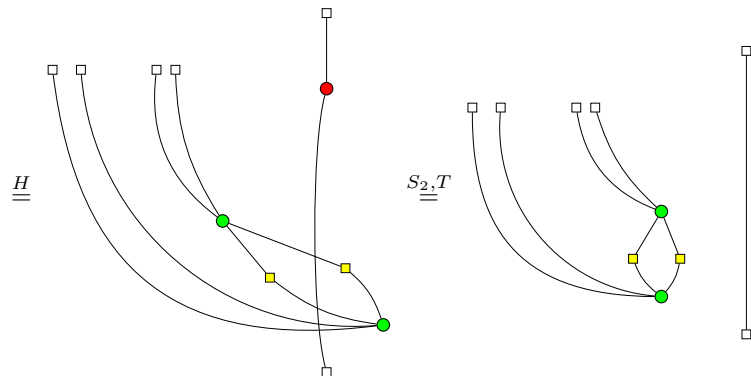


Figure 4.7: CC (3,5) measurement protocol for players 1,2,3







In the second case, players 1,2 and 4 should do :

1. Players 1 and 2 measure in the Y basis
2. Player 4 measures in the X basis
3. Players 1 and 4 send their measurement outcomes to player 2
4. Player 2 sums all measurement outcomes modulo 2 (including his own)
5. Player 2 now has the secret bit S

Figure 4.8 shows each step in the graphical language.

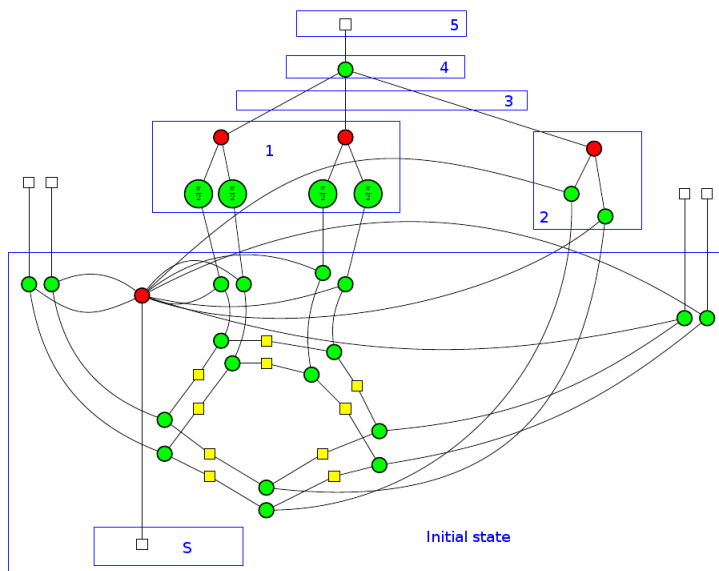
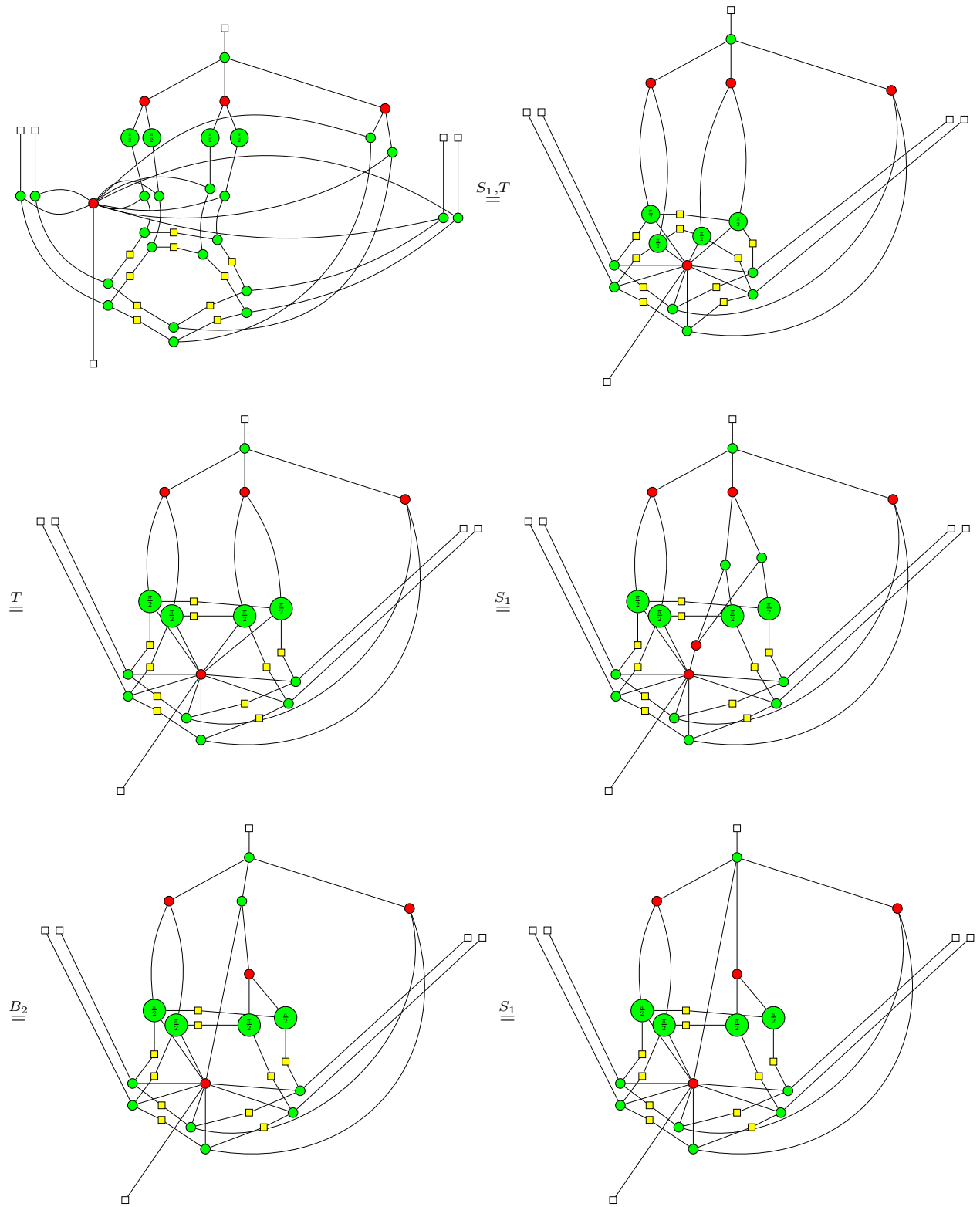
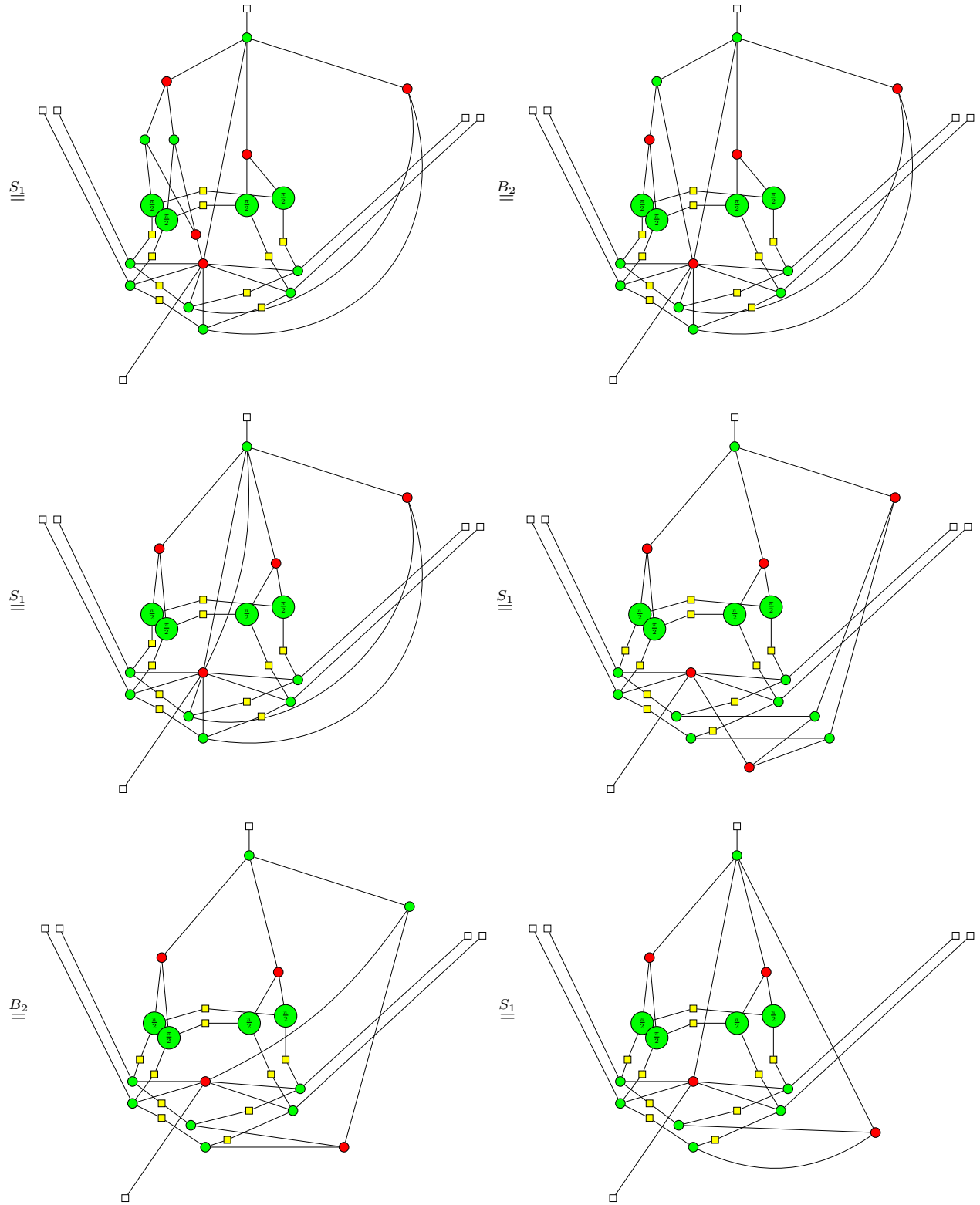
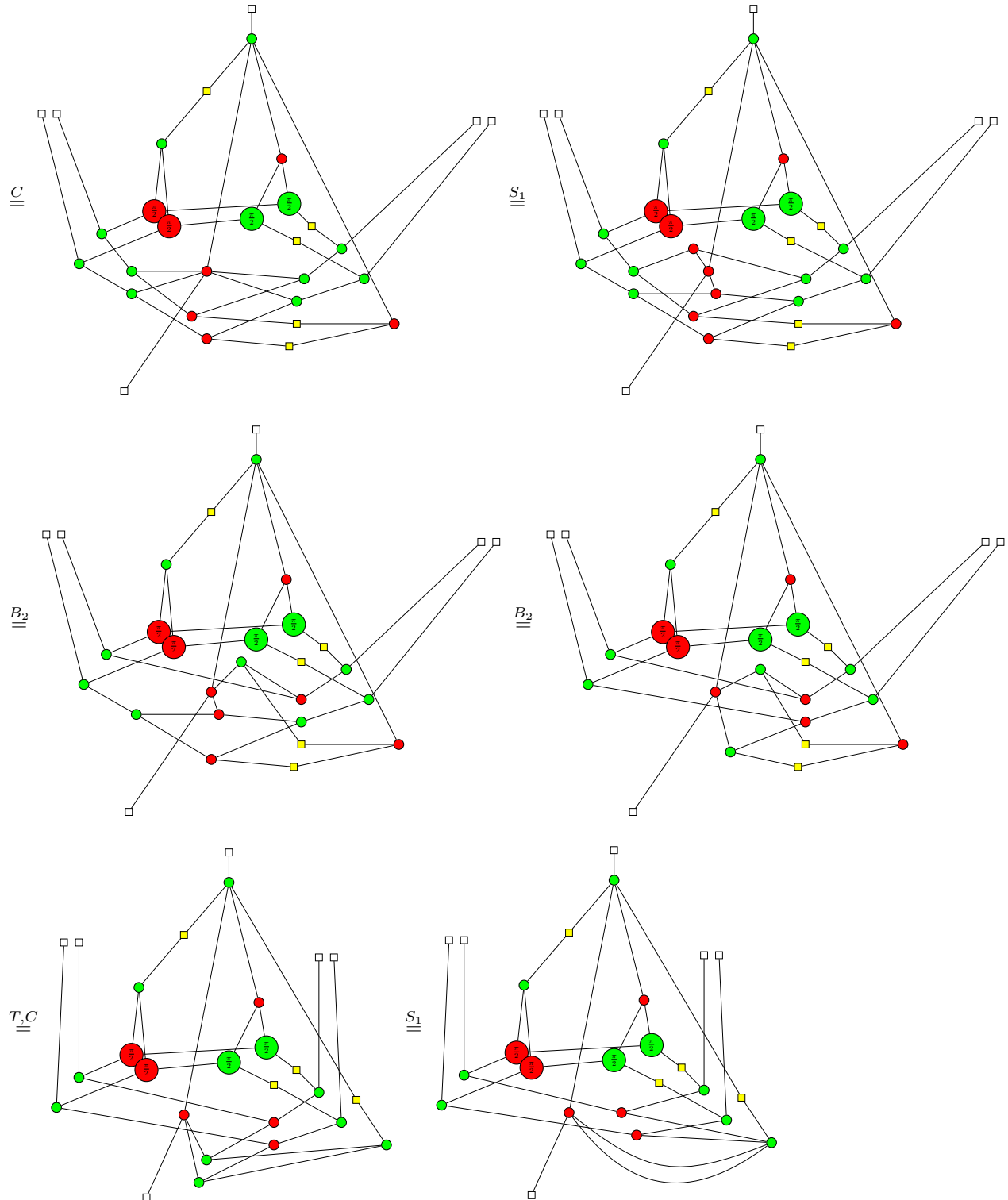


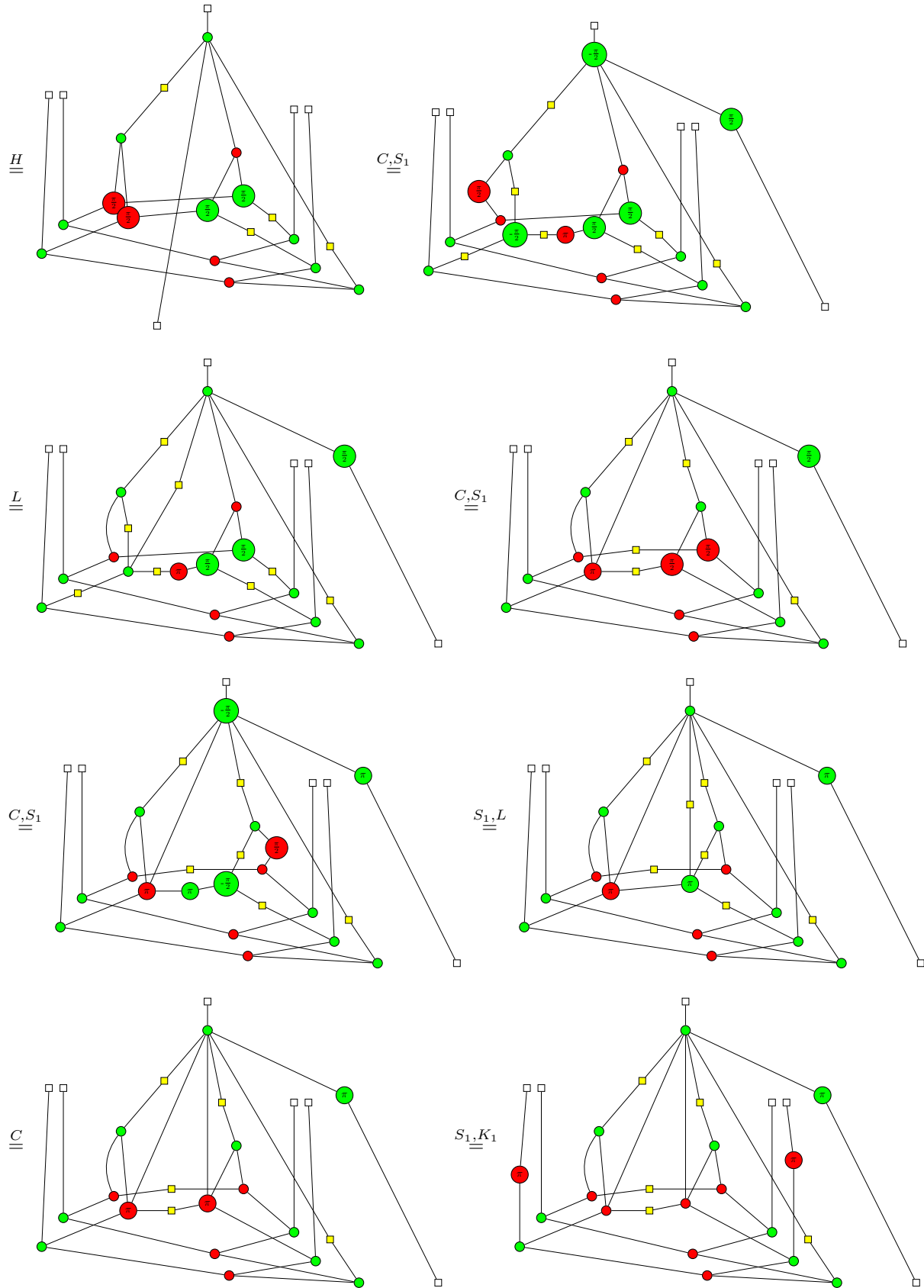
Figure 4.8: CC (3,5) measurement protocol for players 1,2, 4

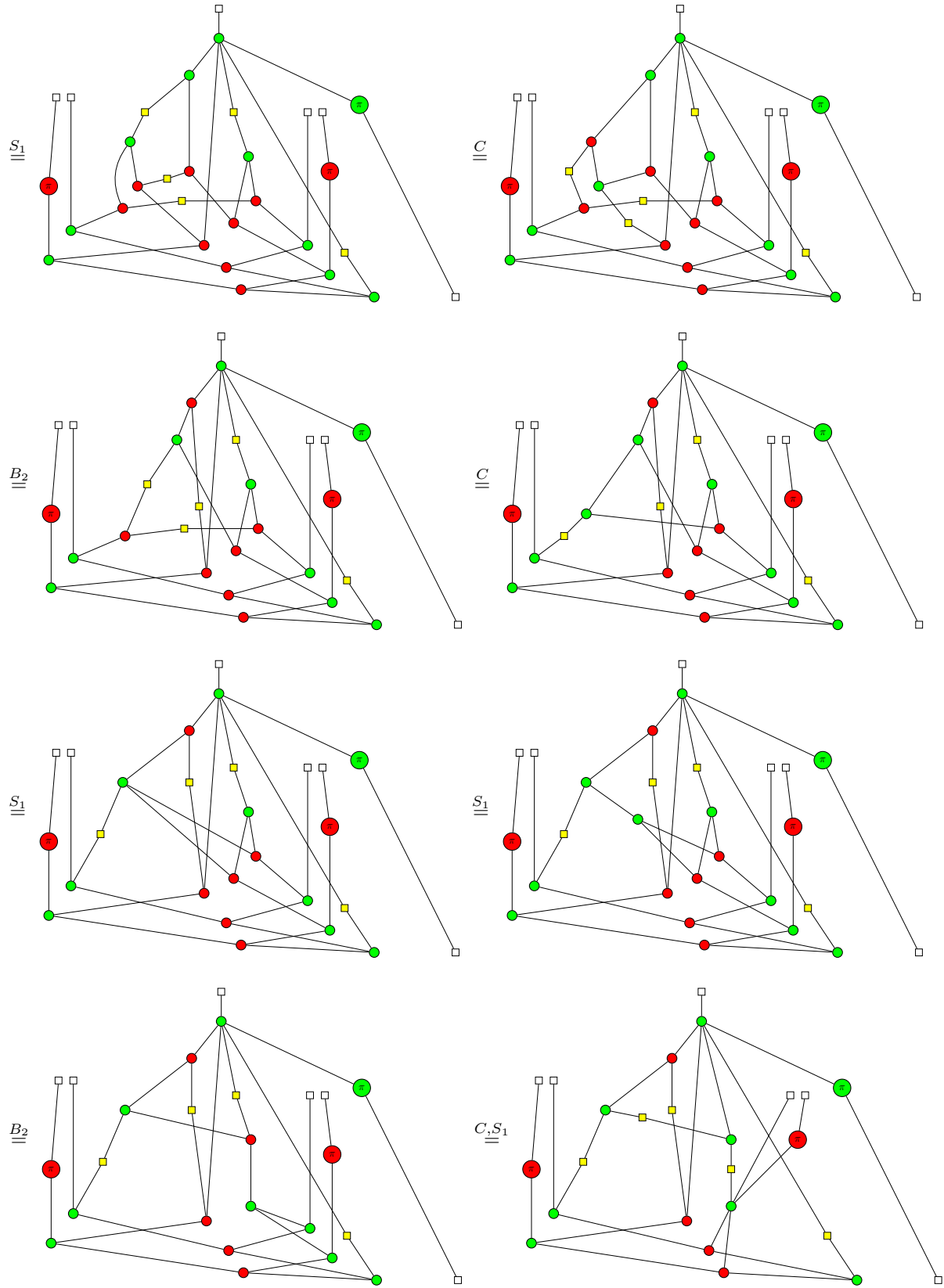
We will now prove that the above actions would lead to the recovery of the secret S .

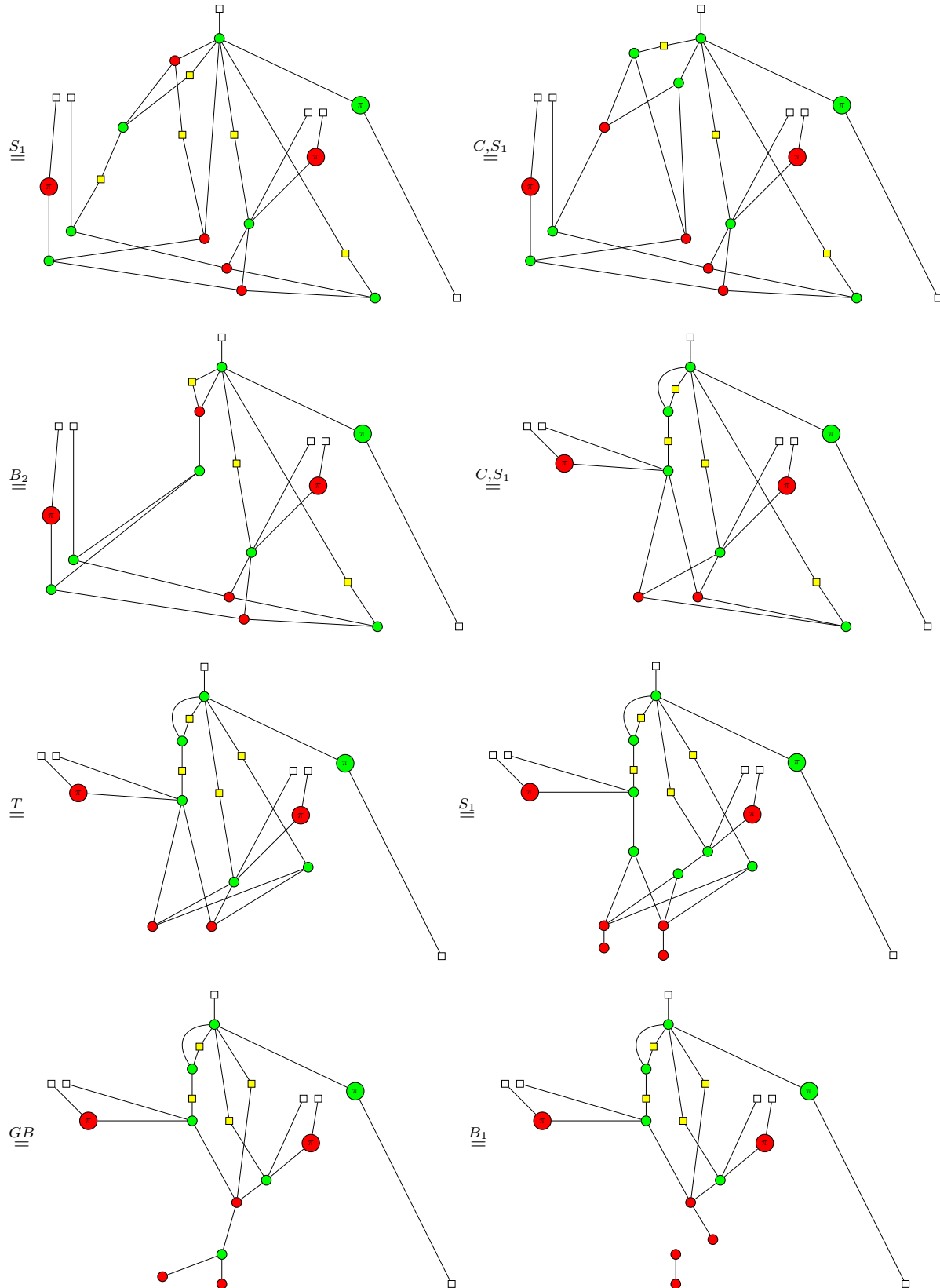


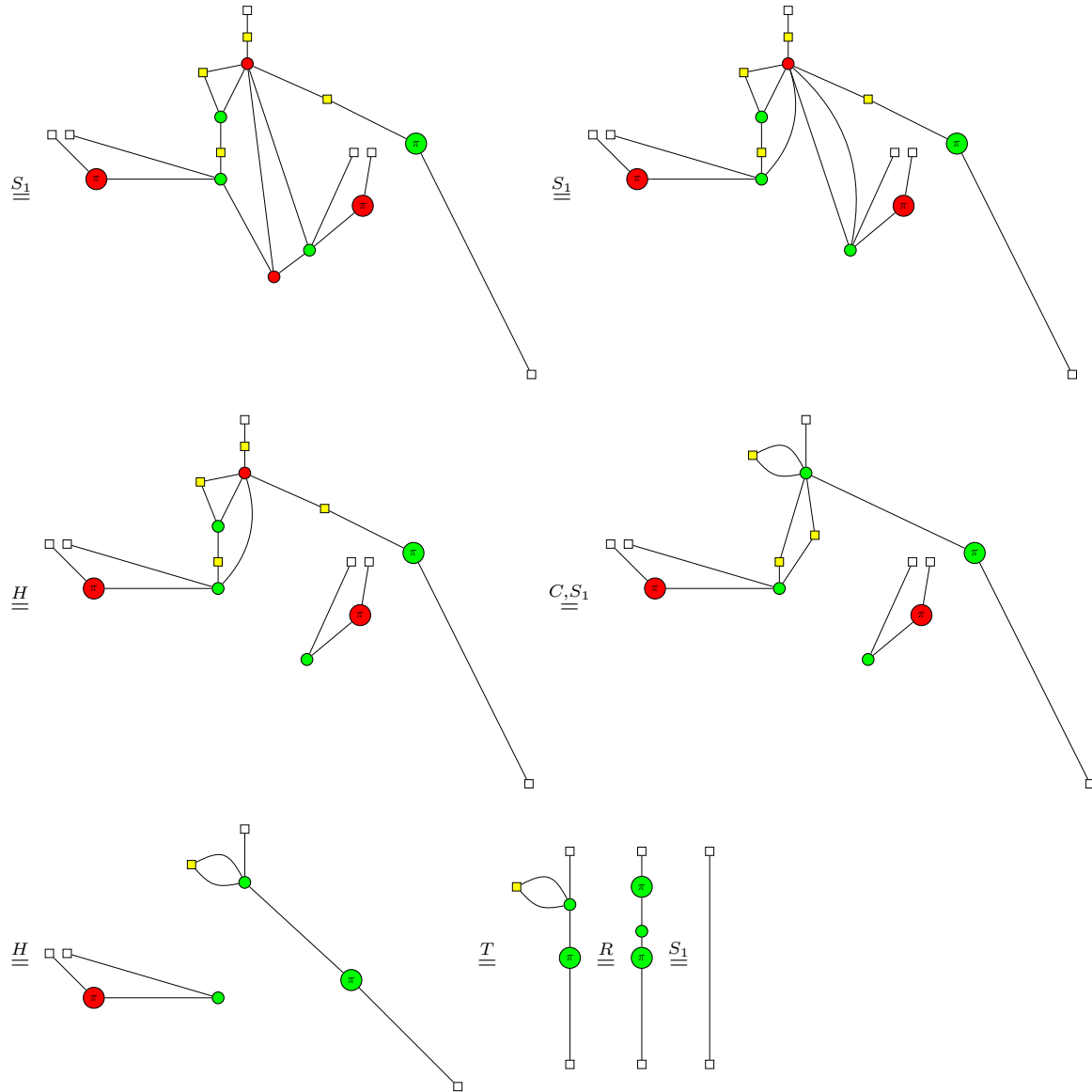










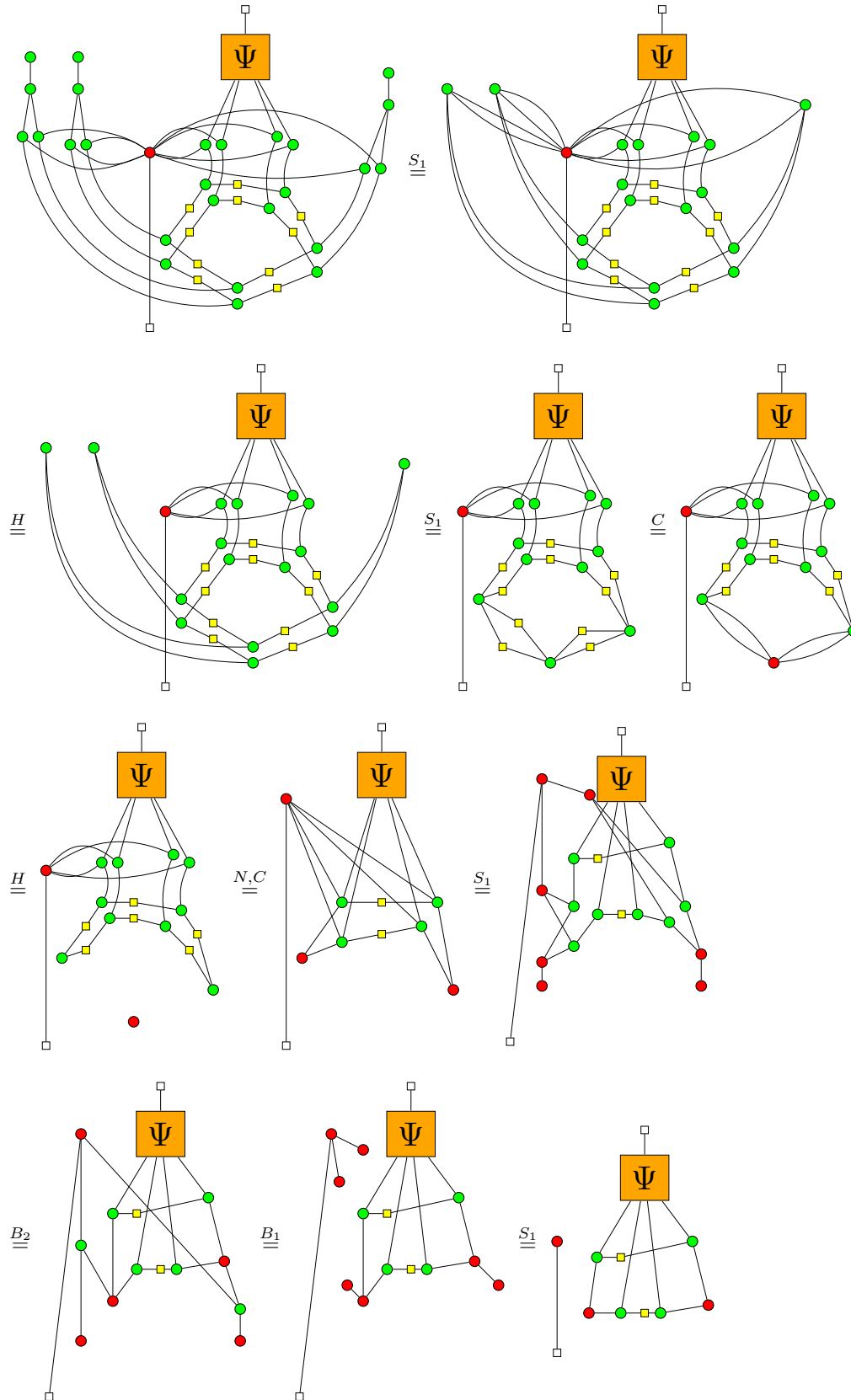


In the last few diagrams we did not depict the subdiagrams associated with the qubit outputs of the non-participating players after they became disconnected from the classical information flow, because they can have no effect on it and are thus irrelevant.

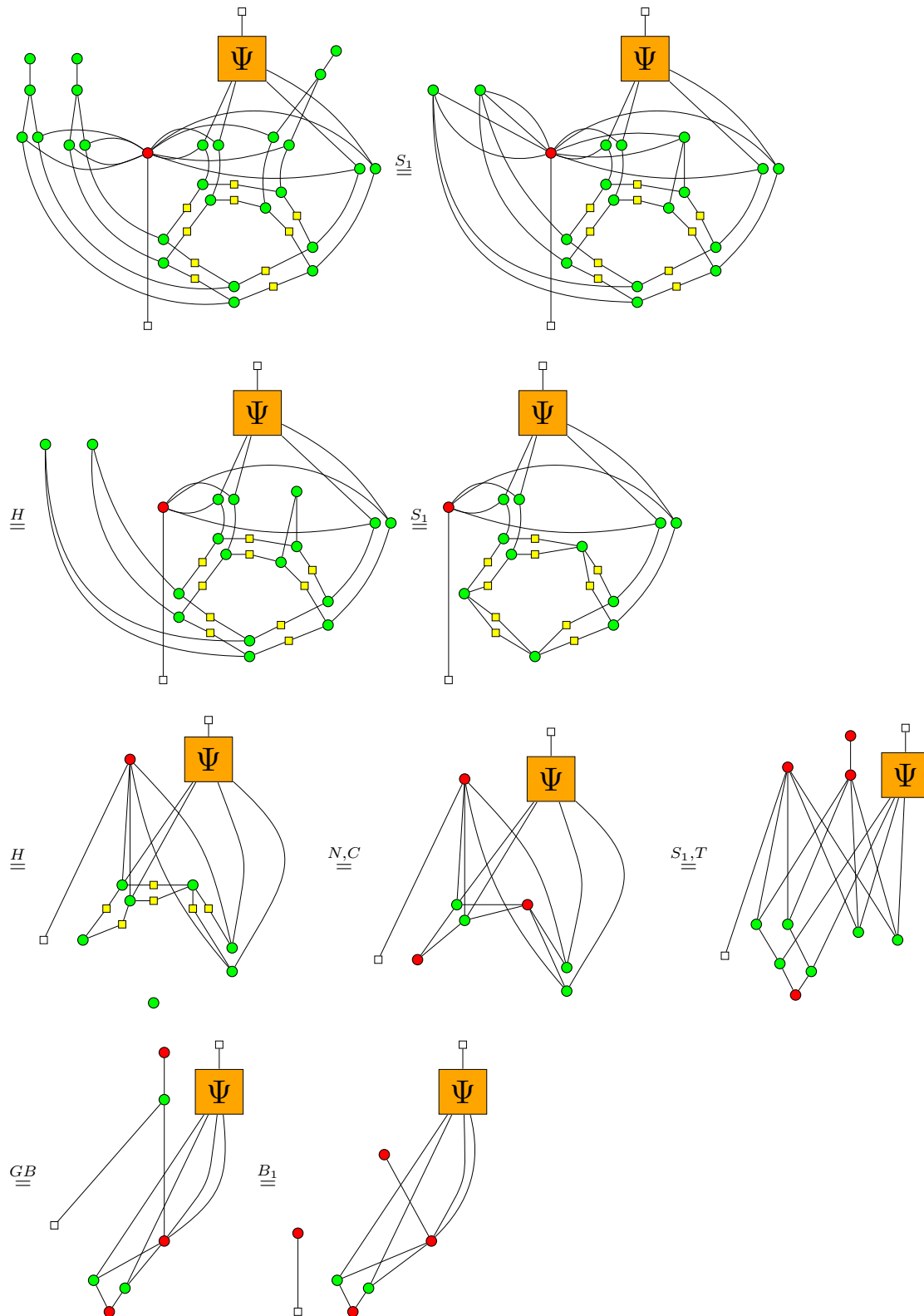
4.4.3 Secret inaccessibility

What remains to be shown is that the secret is denied to any set of two players. We use the same arguments as in the previous two CC protocols. We will show that, if the non-helping players measure their qubits and do not share their results, then the secret is denied to the players. Again, we have to consider two cases.

First case - the two collaborating players are neighbours



Second case - the two collaborating players are not neighbours. Due to the structure of the graph, they will share exactly one neighbour, so there is no need to consider additional cases.



This completes the proof of correctness for this protocol.

4.5 CQ (n,n)

The authors propose a CQ (n,n) sharing scheme using the graph state induced by the graph in 4.9, where all bit labels are set to zero. The protocol is similar to the HBB CQ protocol in that security is ensured by requiring players to perform random measurements in different directions and publicly announce their direction to the rest. Another similarity is that both protocols establish a shared key between the dealer and the players which is used to encrypt the message.

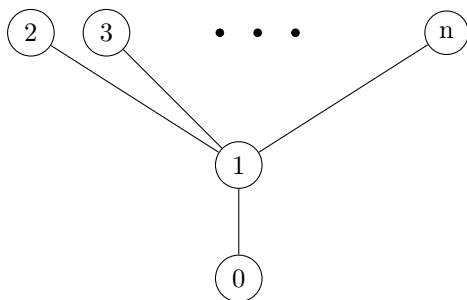
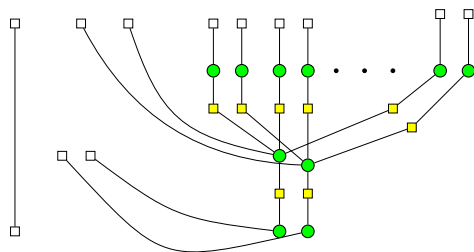


Figure 4.9: CQ (n,n) graph

4.5.1 State and secret distribution

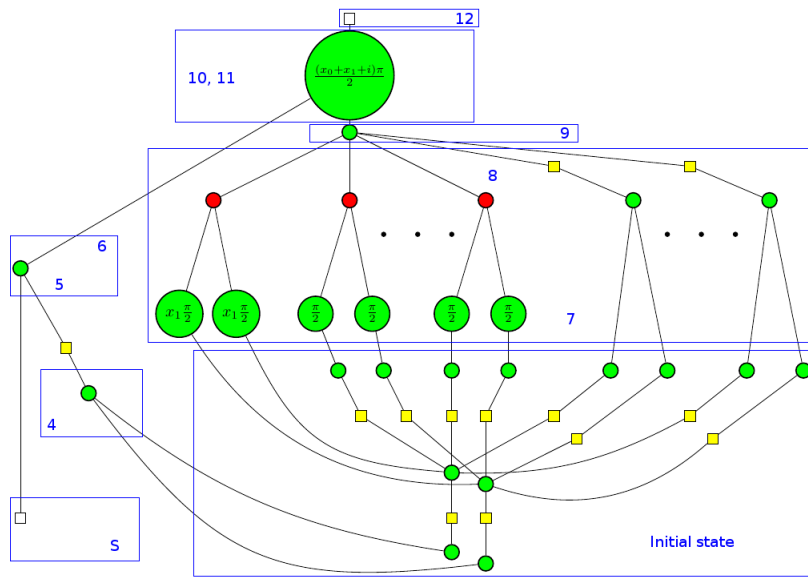
The dealer prepares the graph state in 4.9 and sends each player one qubit. Qubit 0 is retained by the dealer. Graphically, the initial quantum state and classical secret are depicted as :



The secret is encoded at later stages in the protocol, once a common key has been established by the players and the dealer.

4.5.2 Secret Reconstruction

The protocol is executed by the following steps. Figures 4.10 and 4.11 demonstrate how the different steps are formalized in the ZX calculus, in the two different cases, where the dealer performs either a Z

Figure 4.10: CQ (n,n) measurement protocol (dealer Z)

or a Y measurement. The steps are exactly the same as those in the HBB CQ protocol, except for the choice of measurement directions. We present them for completeness.

1. Each player and the dealer randomly choose a measurement direction. Player 1 chooses between X and Y. The rest of the players and the dealer choose between Z and Y. We assign a variable x_i to each player and the dealer, where $x_i = 1$ iff the player (or dealer) performs a Y measurement.
2. Each player and the dealer publicly announce their measurement directions
3. The players and the dealer restart the protocol if $\sum x_i$ is odd, i.e. there is an odd number of Y measurements. Otherwise, the protocol proceeds to the next step
4. The dealer measures his qubit in the selected direction
5. The dealer encrypts the classical bit S with the measurement outcome. This is achieved by adding modulo 2 the two bits.
6. The dealer sends the encrypted message to all players (player 2 will decrypt it, so we depict only this scenario)
7. Every player measures his qubit in the selected direction
8. All players send their measurement outcomes to player 2.
9. Player 2 sums all measurement outcomes (including his) modulo 2.
10. Depending on the announced measurement directions, player 2 performs a negation on the result of the previous step. He performs a negation iff $\sum x_i$ is divisible by 2, but not by 4.
11. Now player 2 has obtained the shared key and he uses it to decrypt the bit he received from the dealer. This is done by adding modulo 2 the two bits.
12. Player 2 has the secret bit S

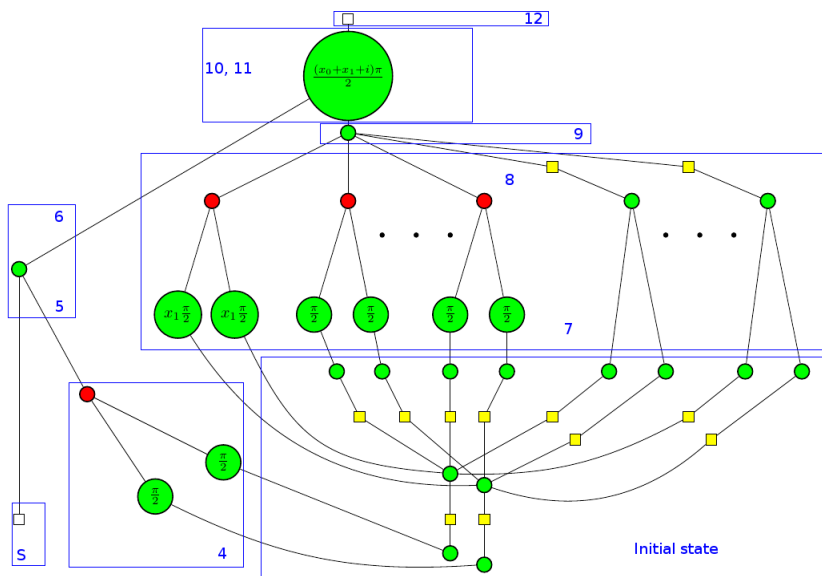
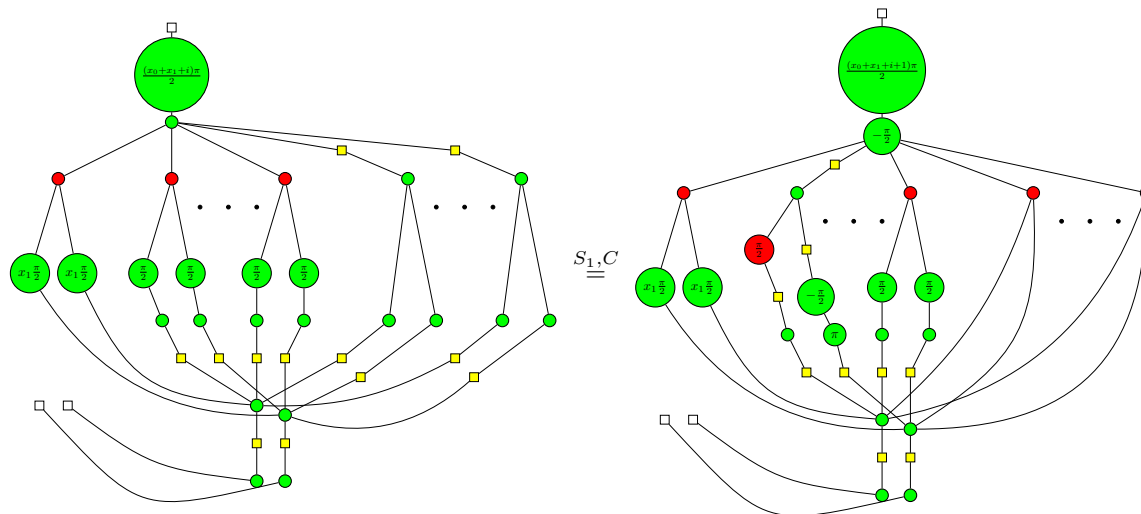
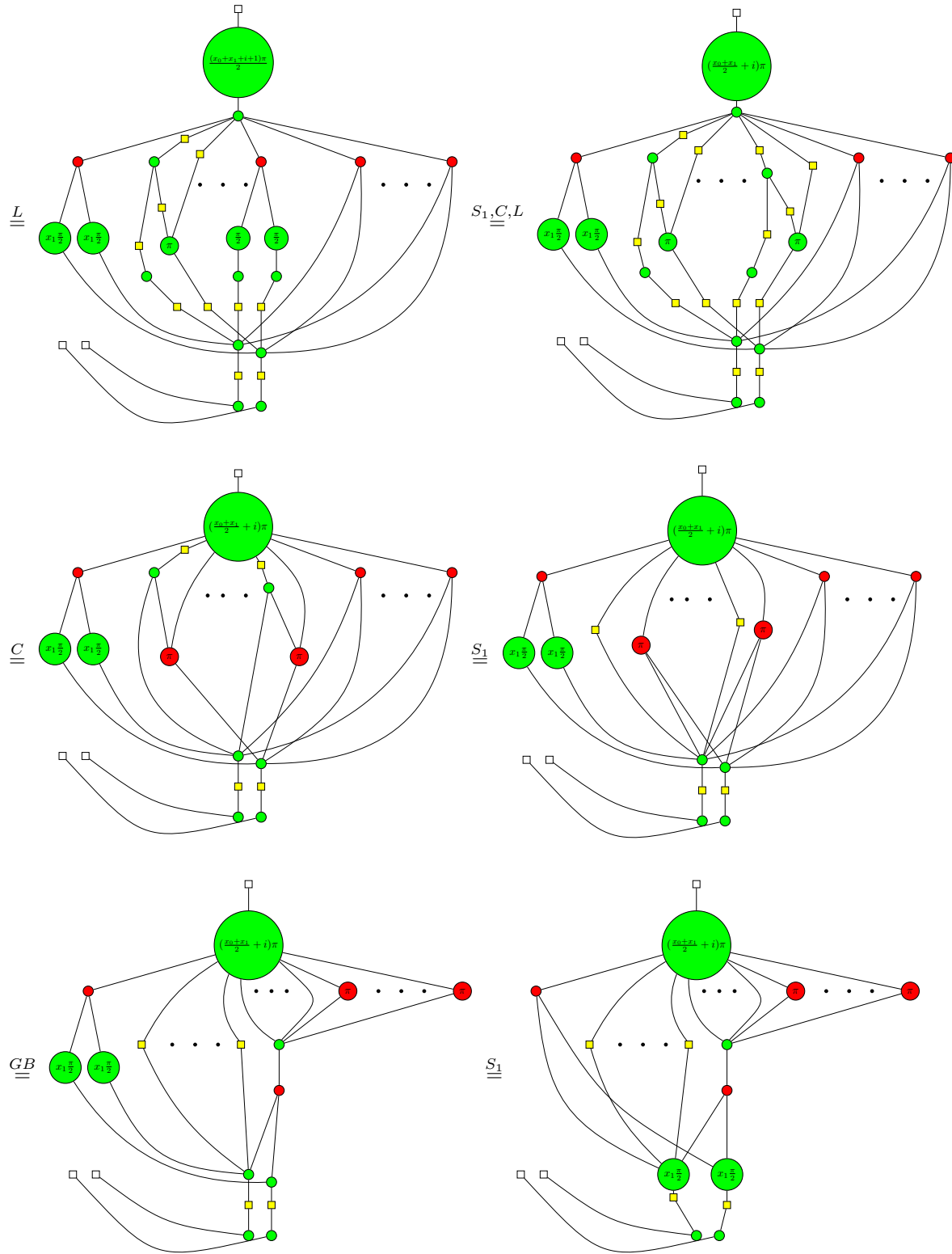
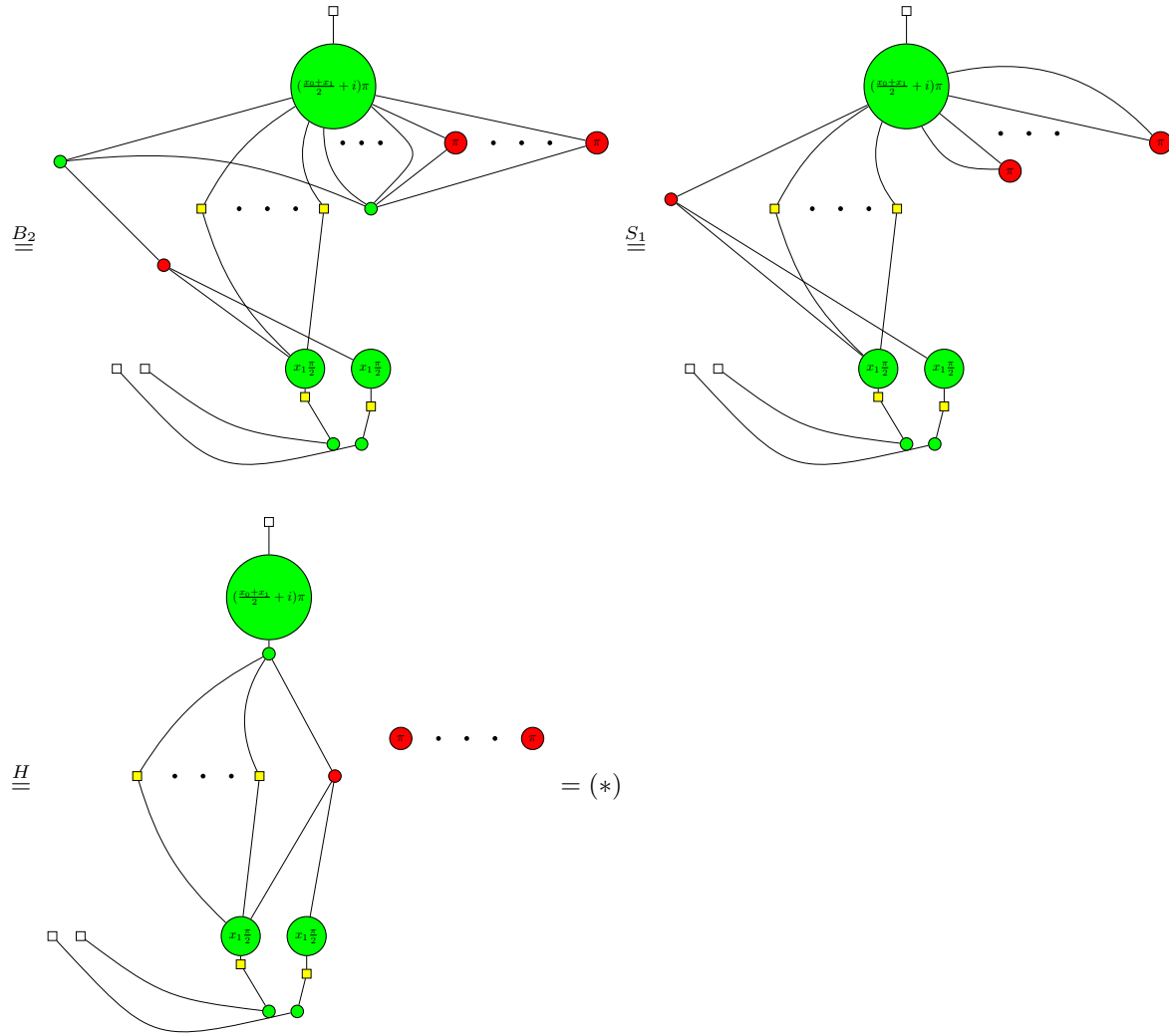


Figure 4.11: CQ (n,n) measurement protocol (dealer Y)

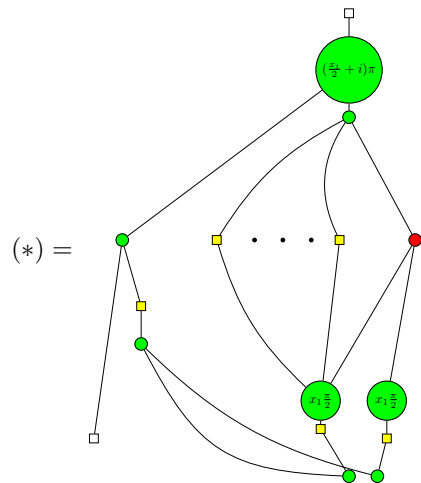
We now proceed to formally proving the correctness of the protocol. We assume that players $2, 3, \dots, i + 1$ choose the Y measurement direction, players $i + 2, i + 3, \dots, n$ choose the X measurement direction. In order to simplify the presentation, we leave the directions of the dealer and player 1 in full generality for now and simplify the initial state after measurements from players $2, 3, \dots, n$. Once in simpler form, we add the remaining parts of the protocol to the diagram and complete the proof.

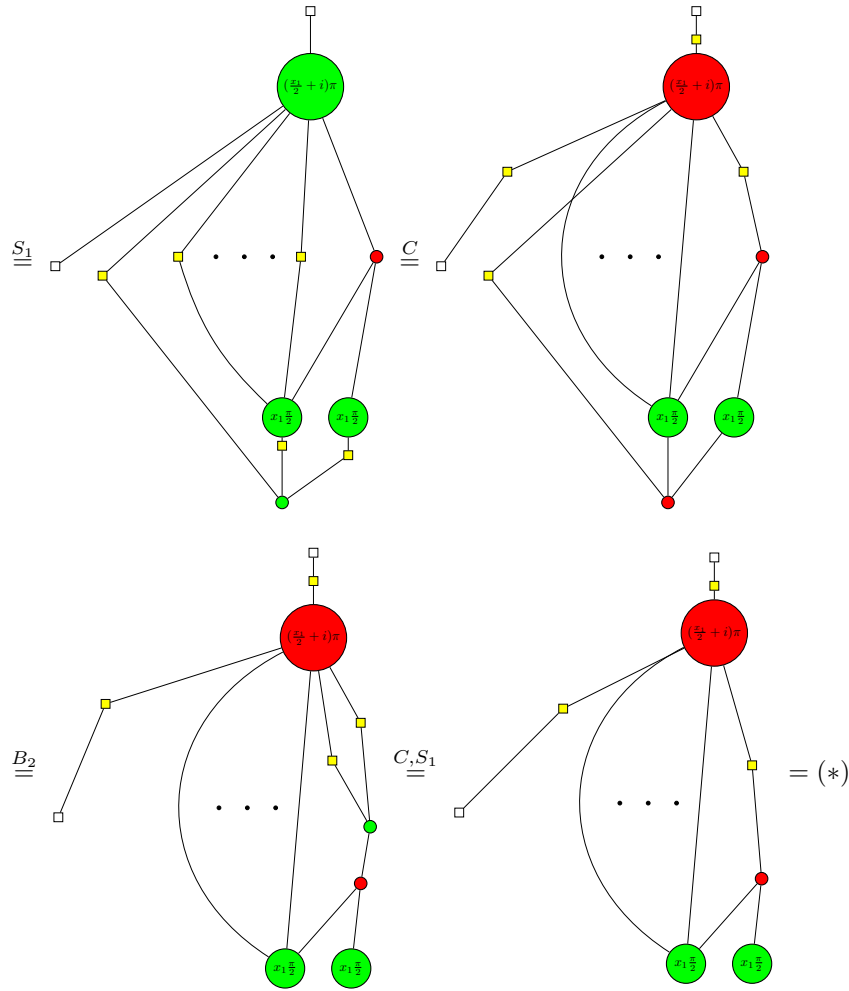




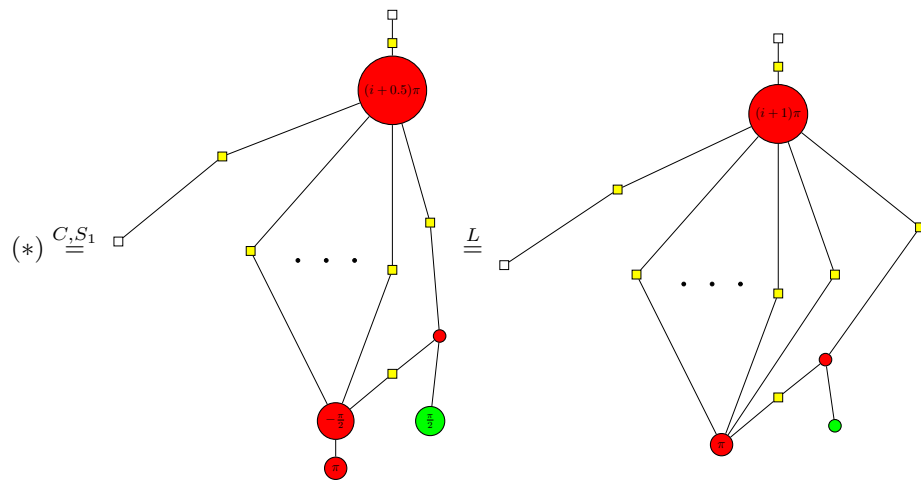


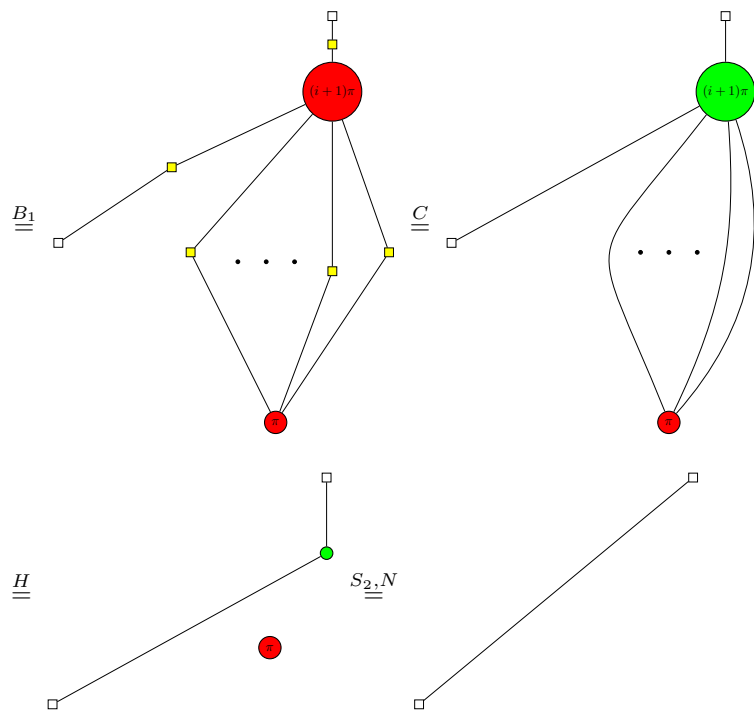
Let's consider the first case, where the dealer measures in the Z direction.





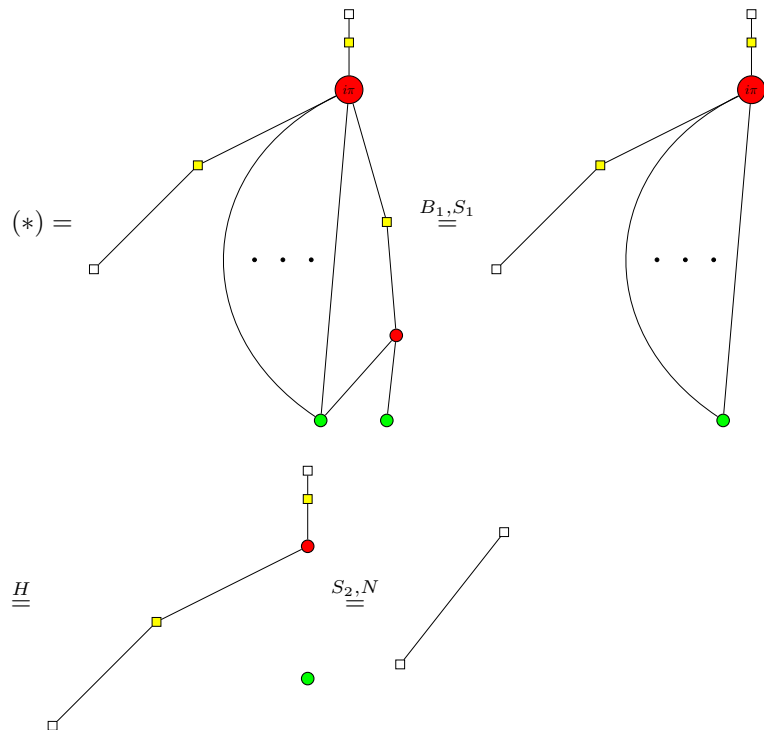
We can further simplify the diagrams, by performing case distinction on x_1 . When $x_1 = 1$, we get :





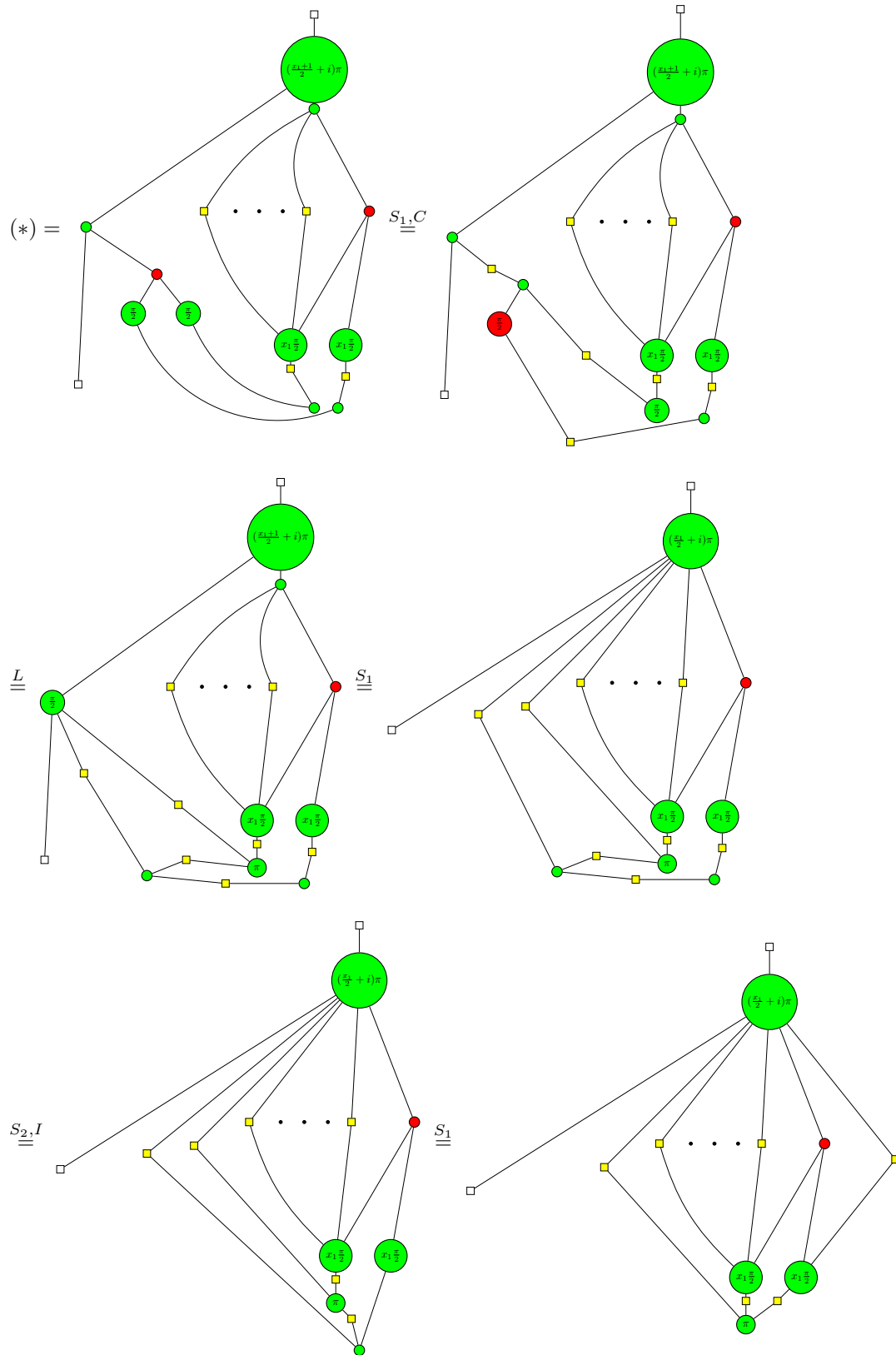
The H rule can be applied like that, because in this case, $(i+1)$ is even (if it isn't the algorithm would have been terminated earlier).

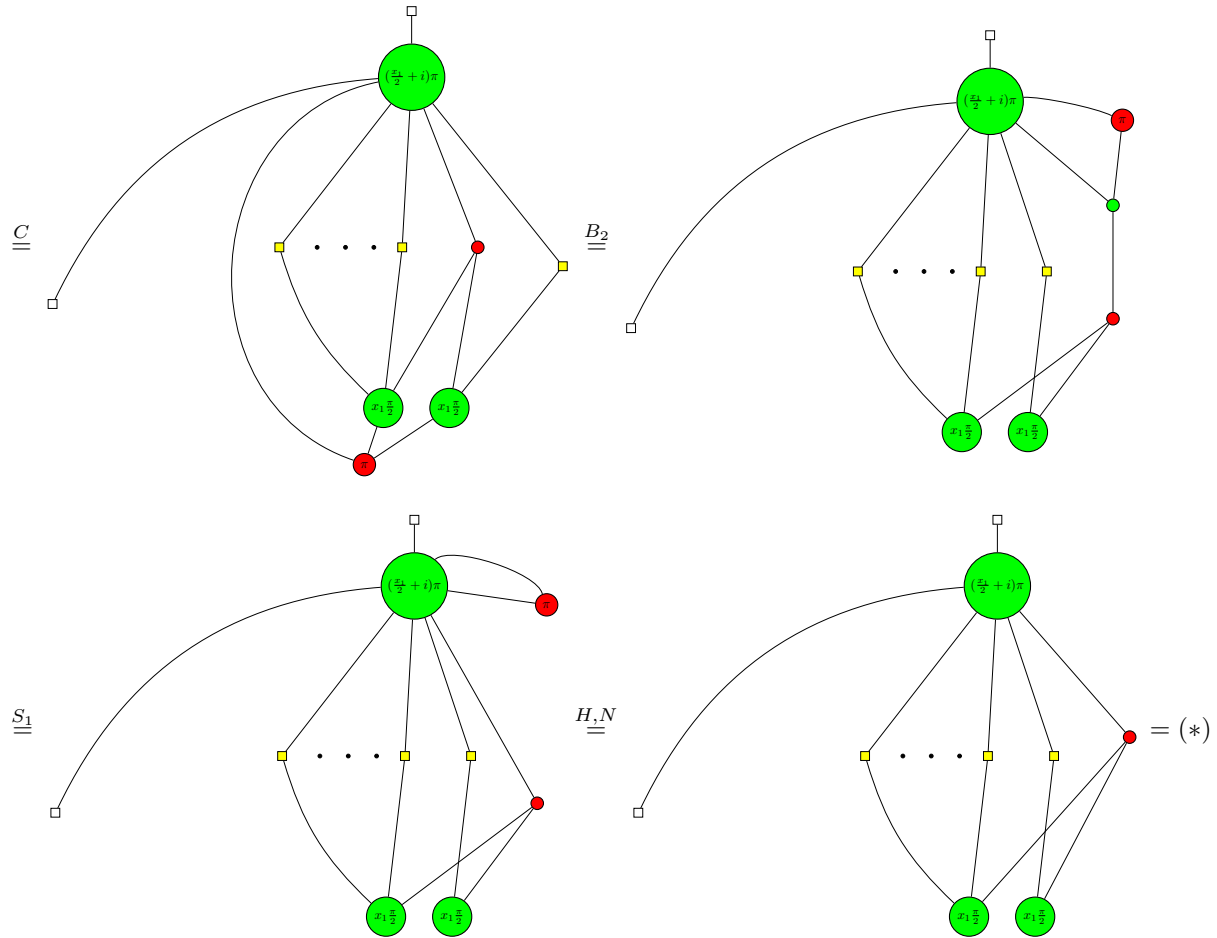
When $x_i = 0$ we get:



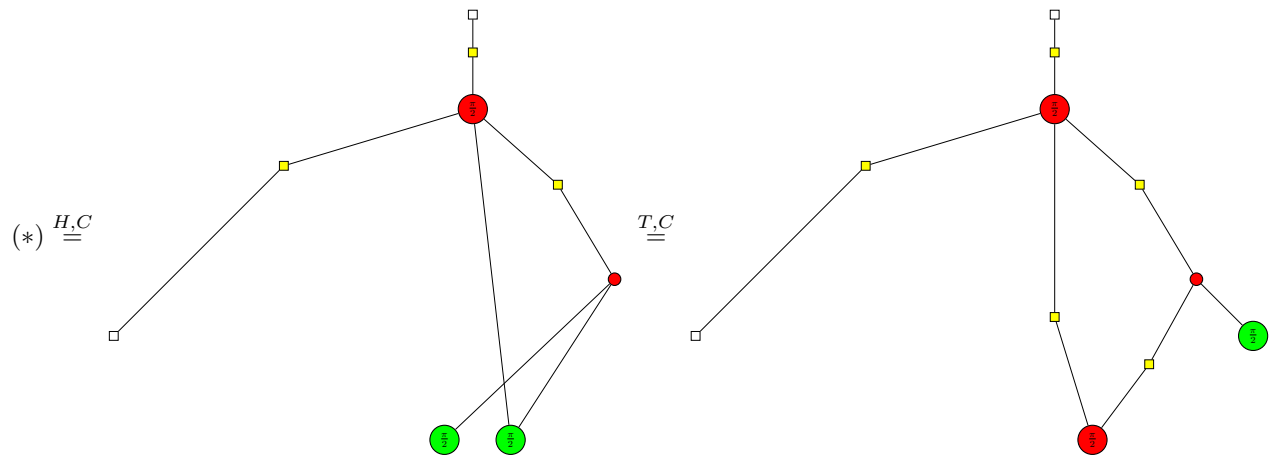
Again, the H rule can be applied in the end to an even number of wires (i), because otherwise, there would be an odd number of Y measurements and the protocol wouldn't reach this step.

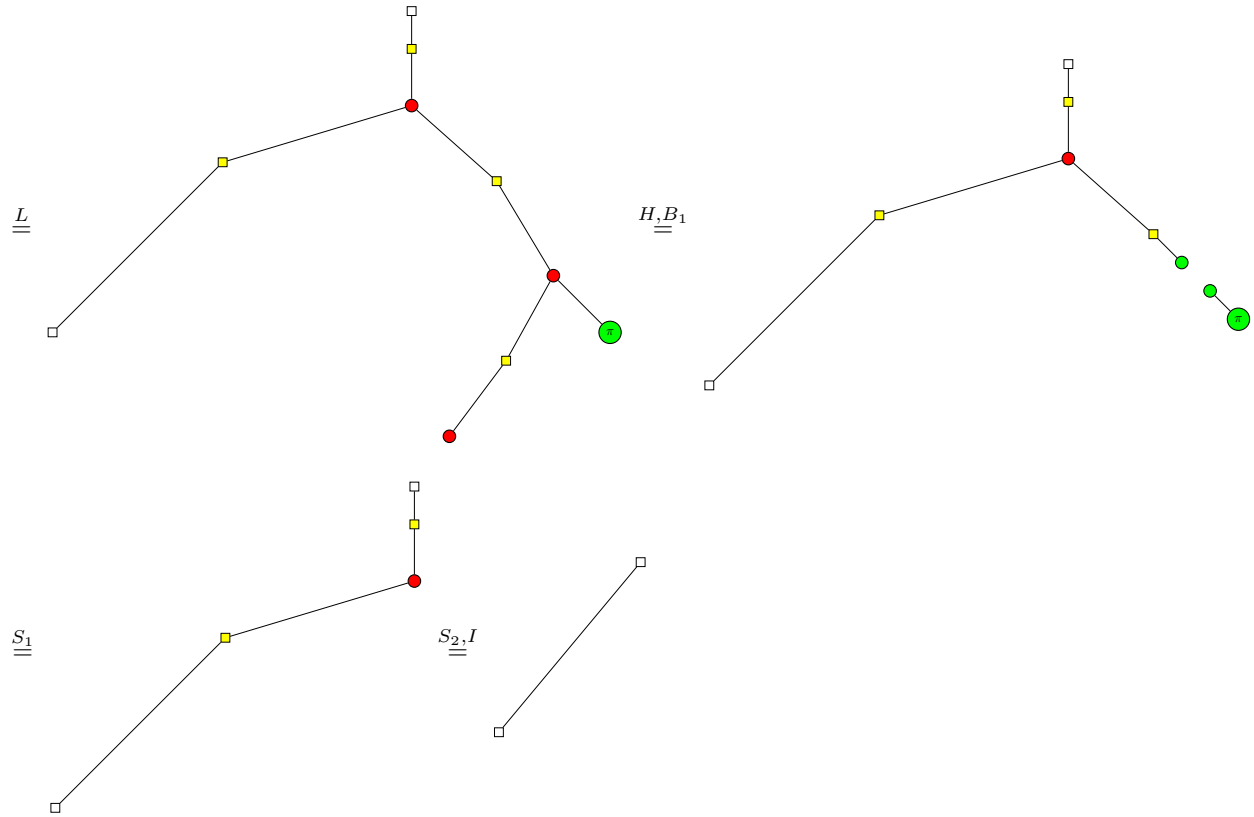
In the second case, the dealer performs a Y measurement.



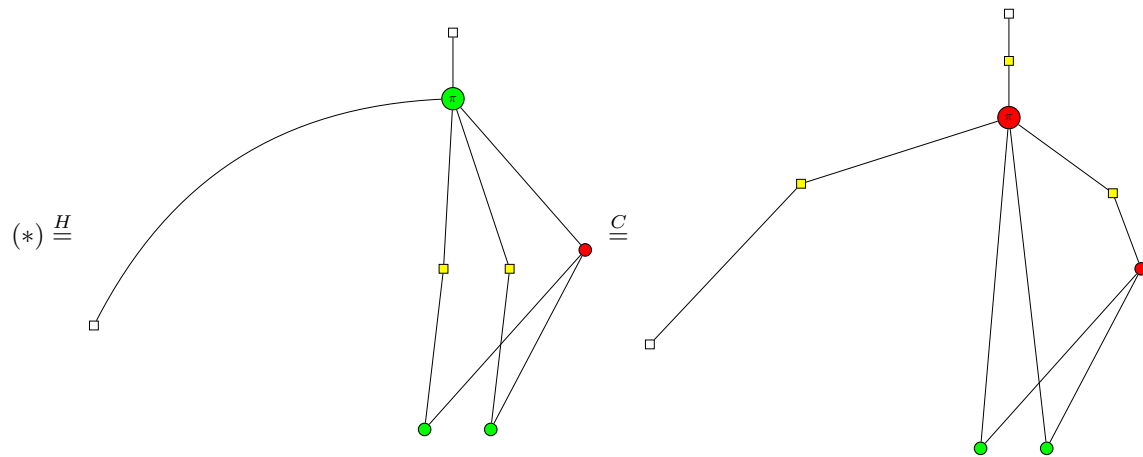


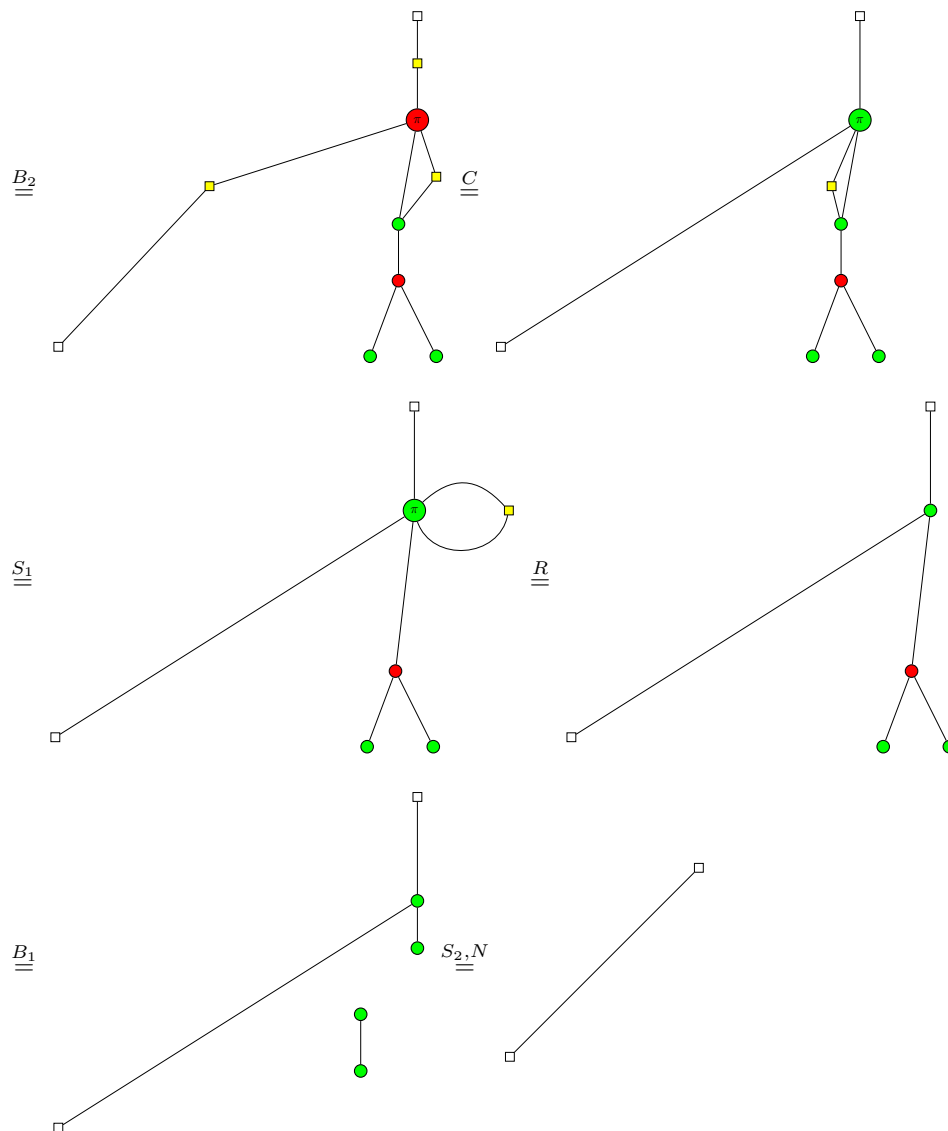
We now consider two cases in order to further simplify the diagrams. First, we consider the case when i is even. This means that x_1 must be 1 in order to have an even number of Y measurements.





The remaining case is i is odd, which implies $x_1 = 0$.





4.5.3 Secret inaccessibility

Similarly to the HBB protocol, there is nothing to show for this part of the protocol. The non-collaborating player will not announce a direction and the protocol terminates before the dealer sends any information to the players.

This completes the proof of correctness.

4.6 CQ (3,5)

The CQ (3,5) sharing protocol uses the graph state given by the graph in 4.12 . All bit labels are again set to zero. The protocol is very similar to the CQ(n,n) protocol and the only differences are the initial state prepared and distributed by the dealer, the individual measurement directions of the players and the corrections performed on the classical data. We will only present the case where the players

working together are all neighbours (players 1,2,3). The remaining case differs only by the measurement directions of the players and the dealer, but the proof of correctness consists of similar diagram rewriting strategies.

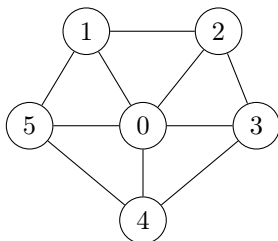
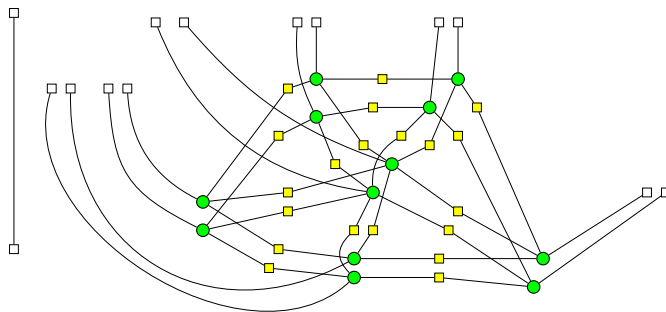


Figure 4.12: CQ (3,5) graph

4.6.1 State and secret distribution

The dealer prepares the graph state in 4.12 and sends each player one qubit. Qubit 0 is retained by the dealer. Graphically, the initial quantum state and classical secret are depicted as :



The secret is encoded and transmitted after a key has been established.

4.6.2 Secret Reconstruction

The protocol is executed by the following steps. Figures 4.13 and 4.14 demonstrate how the different steps are formalized in the ZX calculus, in the two different cases, where the dealer performs either a Z or a Y measurement. The steps are almost the same as the ones presented in the CQ (n, n) protocol.

1. Players 1,2 and 3 and the dealer randomly choose a measurement direction. Players 1 and 3 choose between X and Z. Player 2 chooses between X and Y. The dealer chooses between Z and Y.
2. The three players and the dealer publicly announce their measurement directions
3. There are exactly two desired direction vectors, which are $(D, P_1, P_2, P_3) = (Z, Z, X, Z)$ or $(D, P_1, P_2, P_3) = (Y, X, Y, X)$. If the players have chosen another configuration, then the protocol is restarted

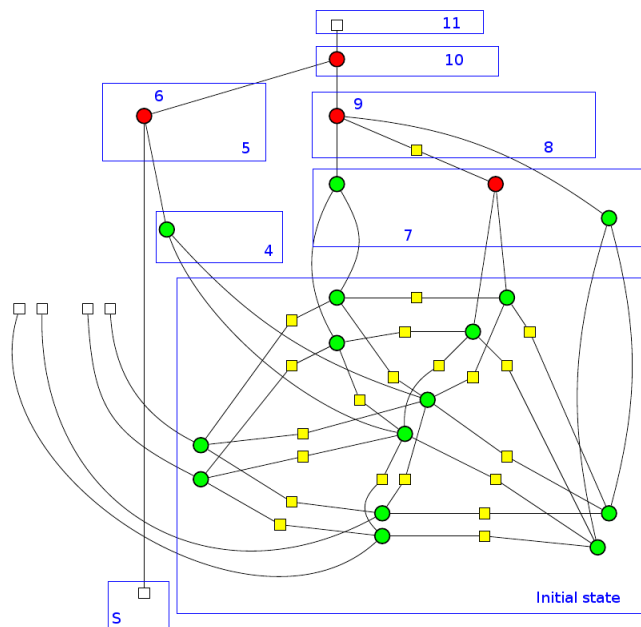


Figure 4.13: CQ (3,5) measurement protocol (dealer Z)

4. The dealer measures his qubit in the selected direction
5. The dealer encrypts the classical bit S with the measurement outcome. This is achieved by adding modulo 2 the two bits.
6. The dealer sends the encrypted message to the collaborating players (player 1 will decrypt it, so we depict only this scenario)
7. The three players measure their qubits in the selected directions
8. The three players send their measurement outcomes to player 1.
9. Player 1 sums all measurement outcomes (including his) modulo 2.
10. Now player 1 has obtained the shared key and he uses it to decrypt the bit he received from the dealer. This is done by adding modulo 2 the two bits.
11. Player 1 has the secret bit S

We can now prove the correctness of the protocol in the graphical language. Let's consider the first case, where the dealer measures in the Z basis. We get :

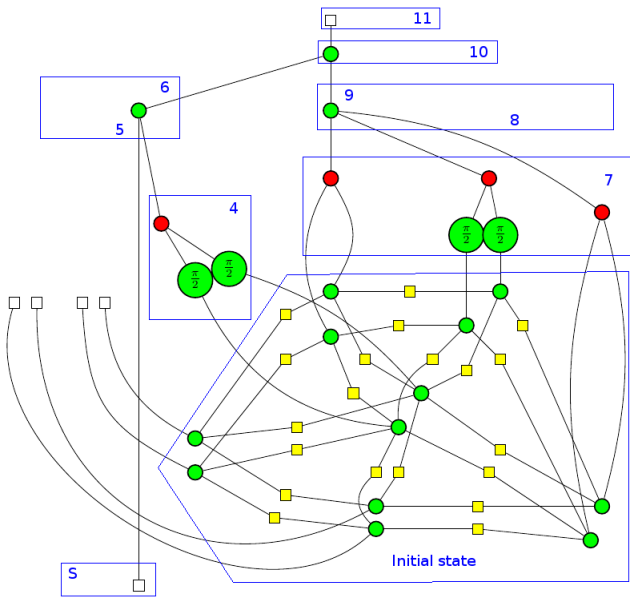
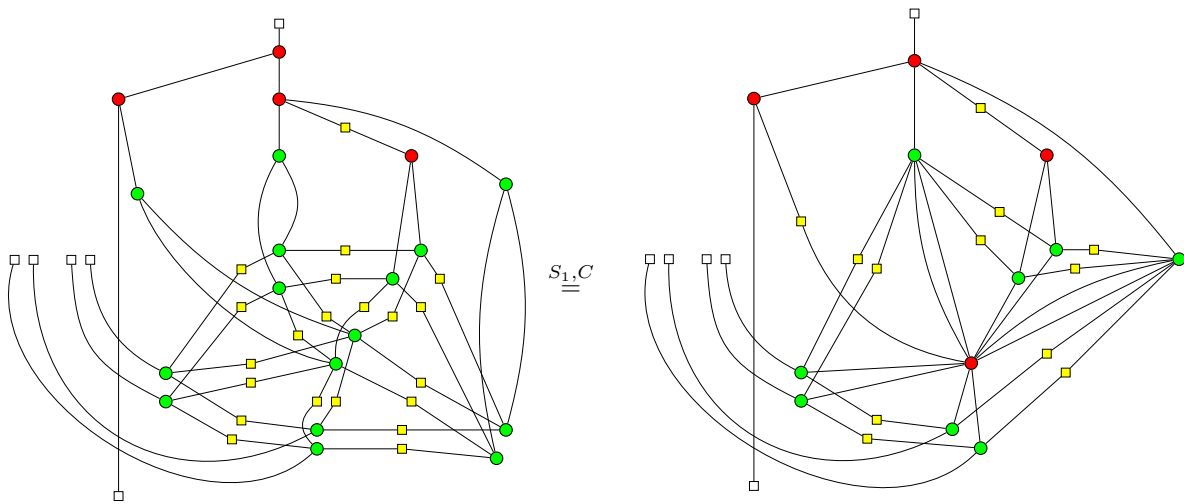
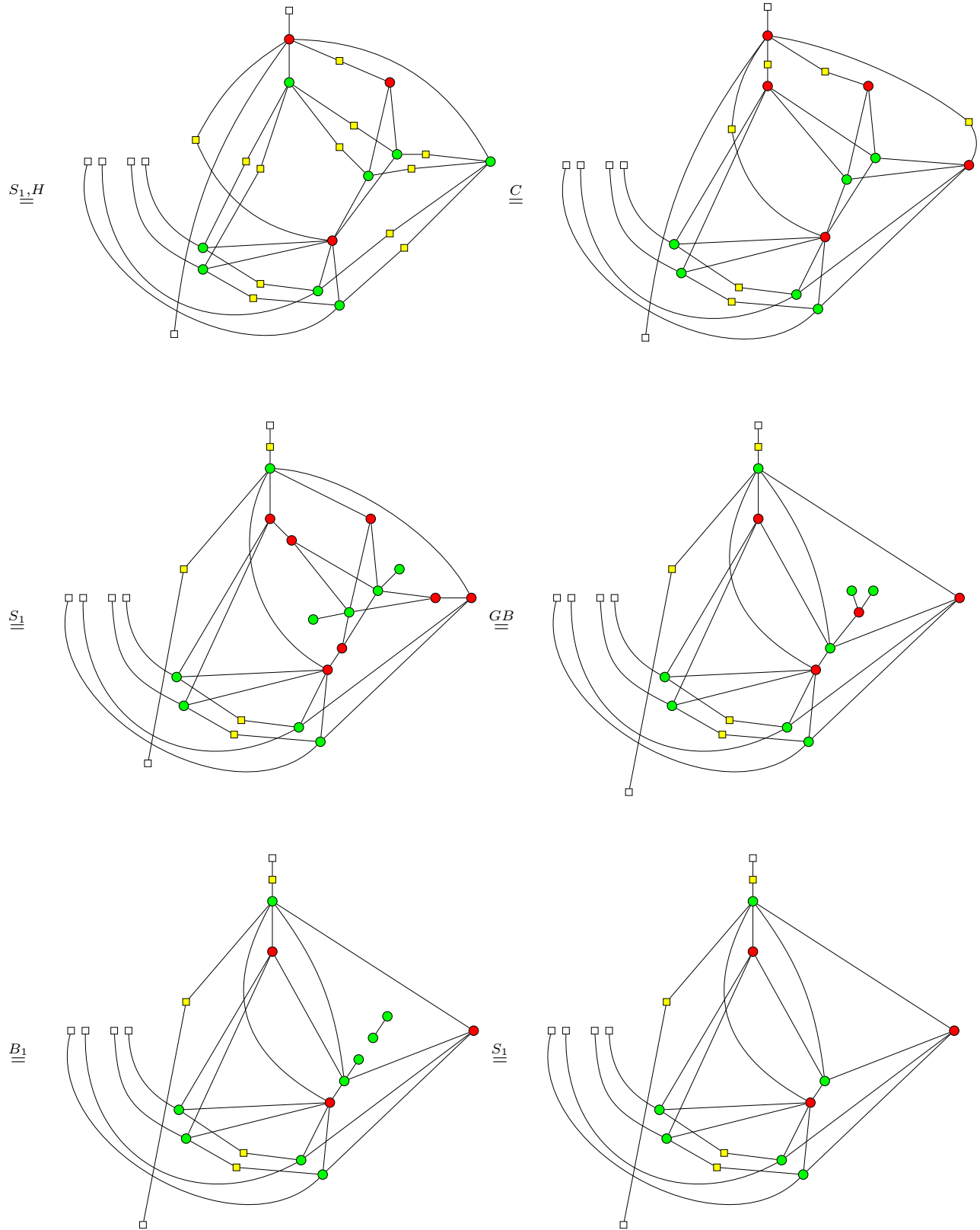
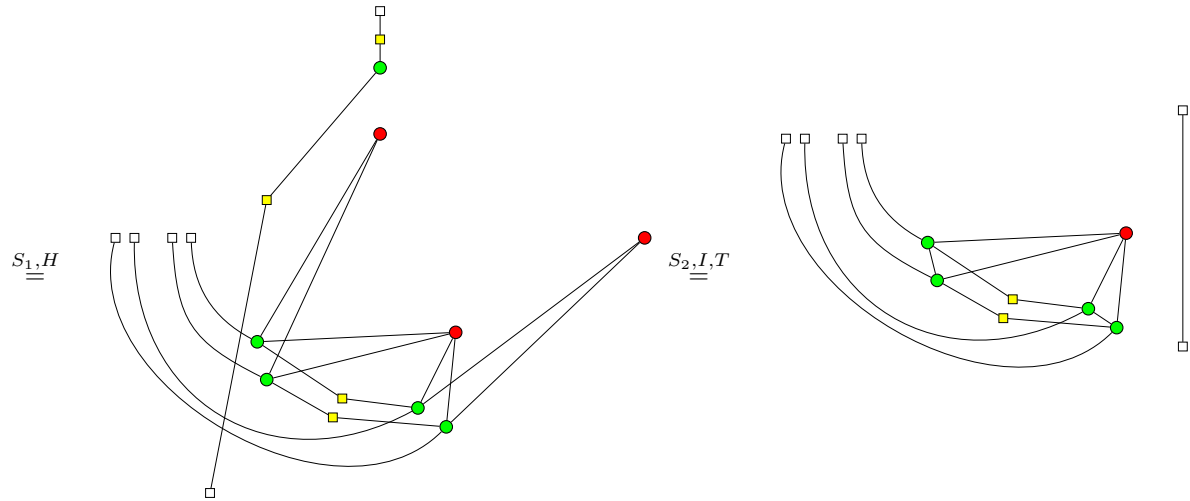


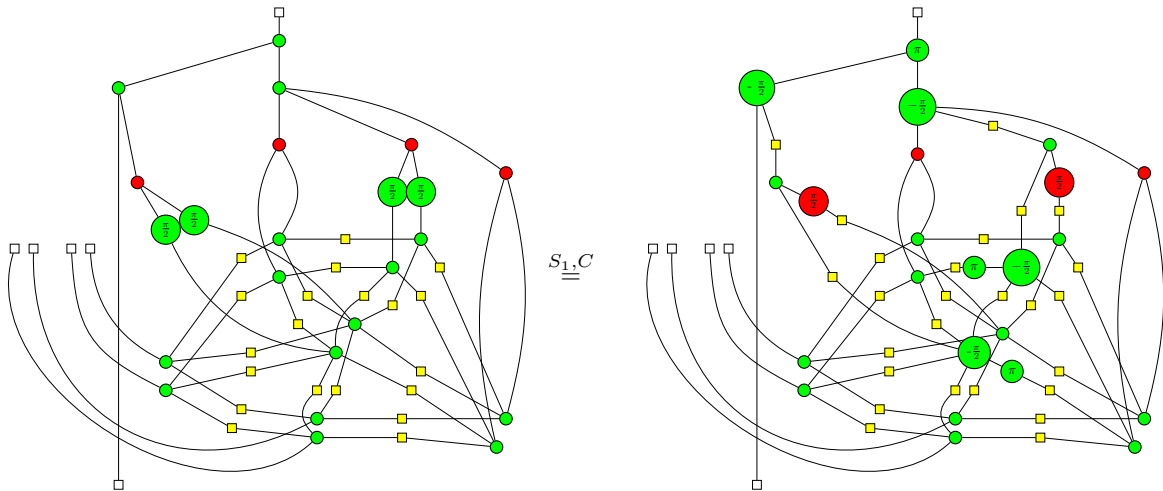
Figure 4.14: CQ (3,5) measurement protocol (dealer Y)

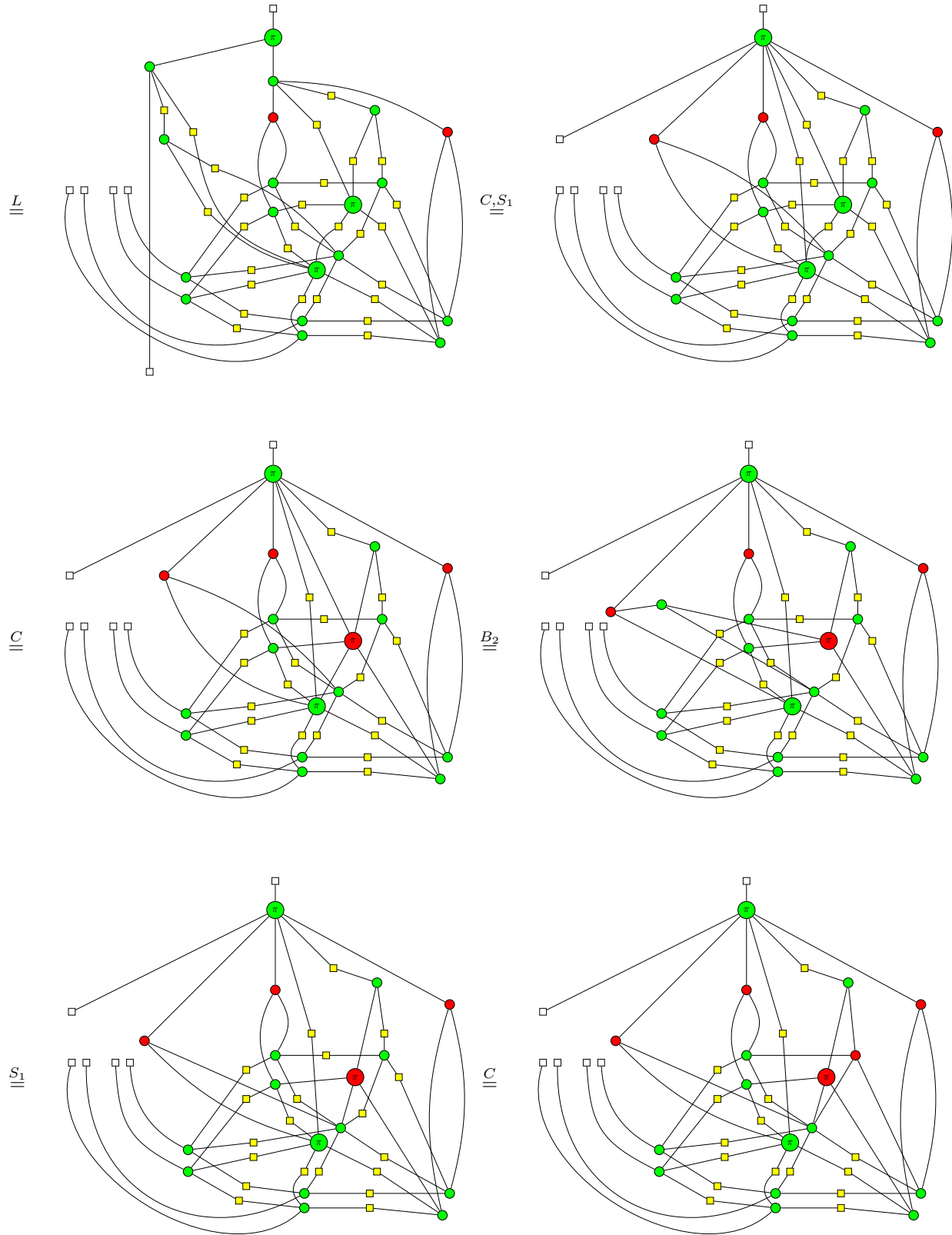


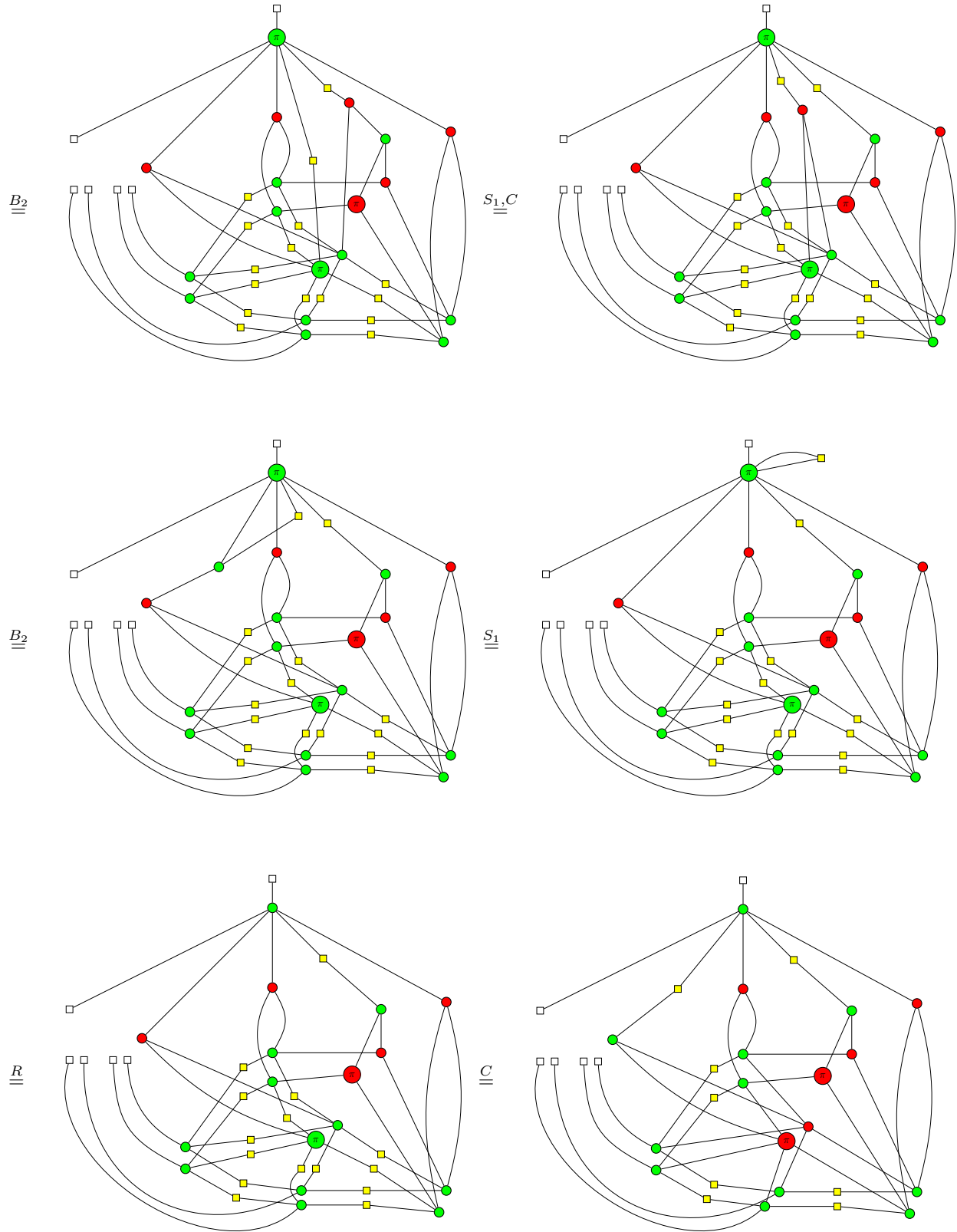


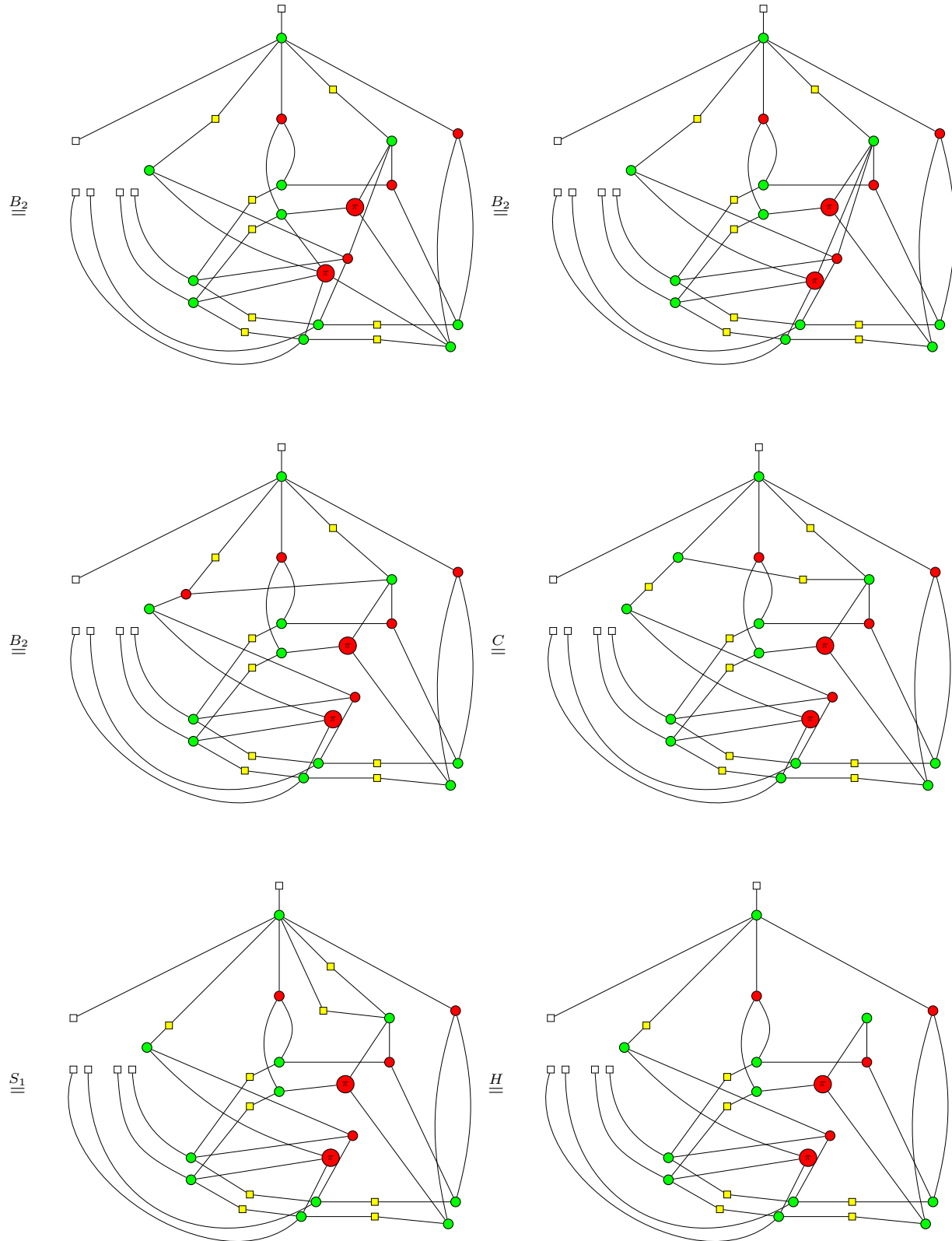


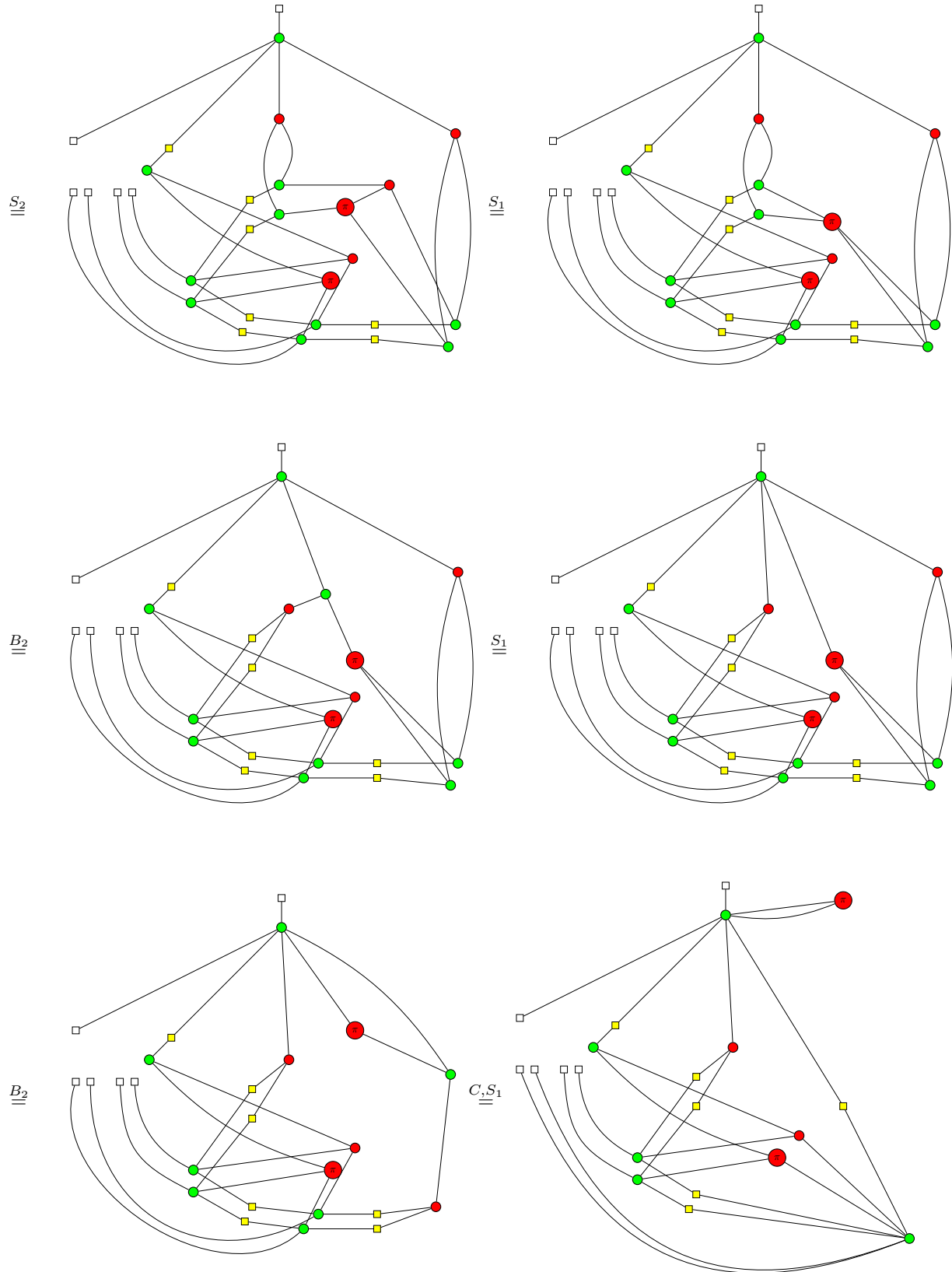
In the other case, the dealer measures in the Y basis. We get :

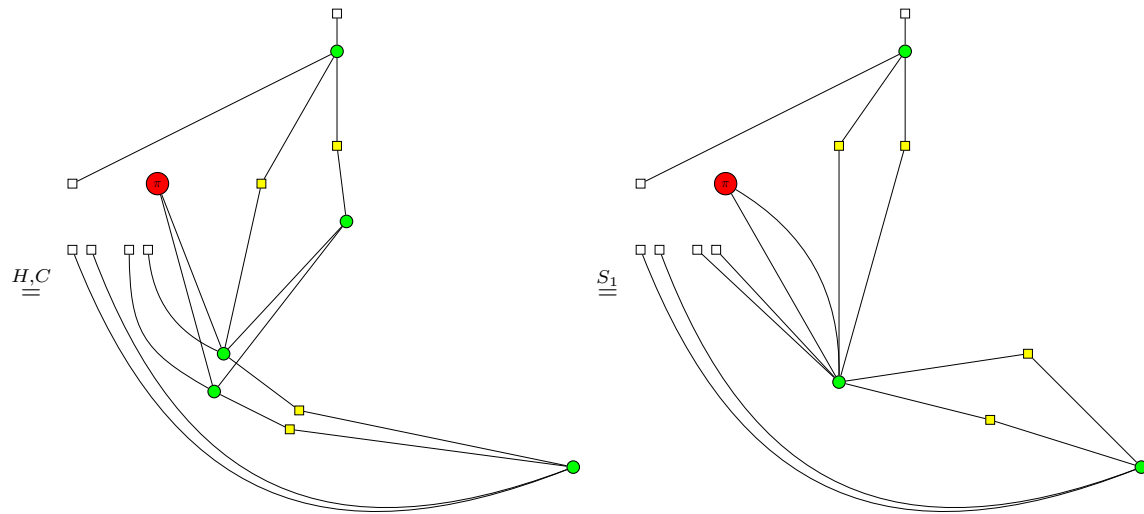
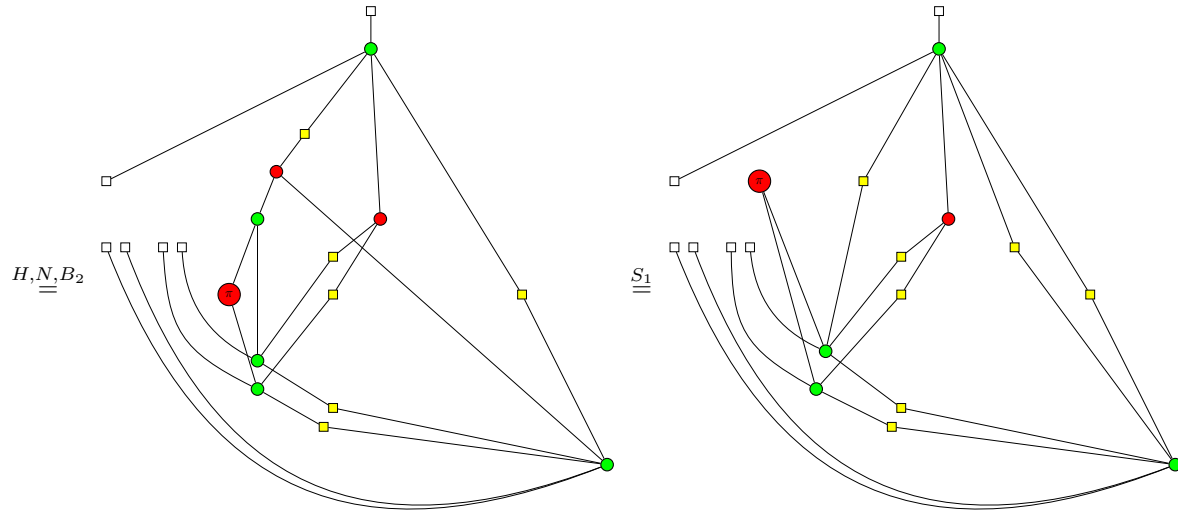


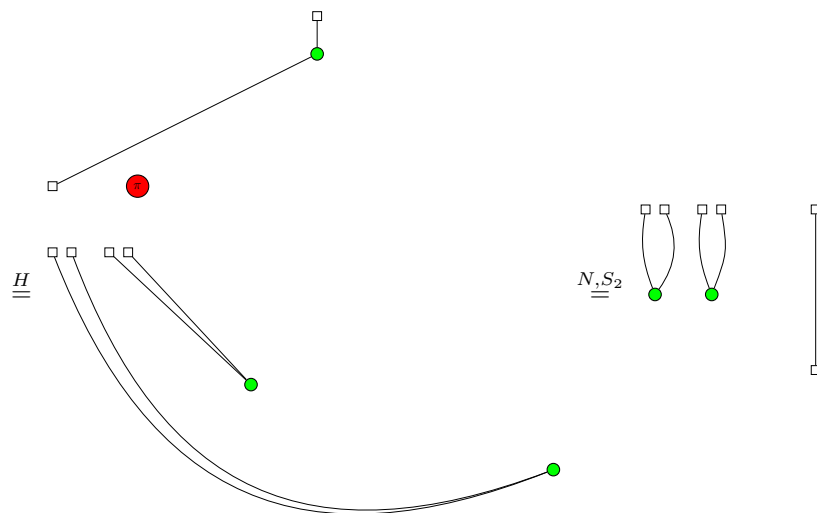












4.6.3 Secret inaccessibility

Similarly to the CQ (n, n) protocol, there is nothing to show for this part of the protocol. When there are only two collaborating players, the protocol terminates before the dealer sends any information to the players.

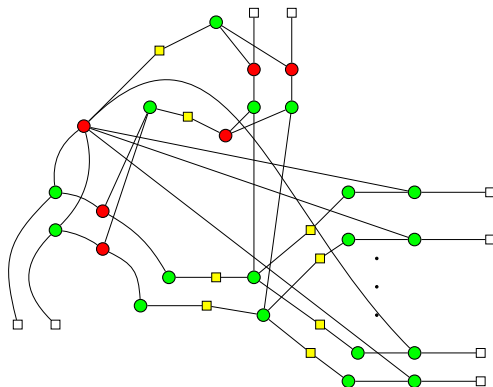
This completes the proof of correctness.

4.7 QQ (n,n)

The QQ (n, n) scheme is obtained by extending the CQ (n, n) protocol. The same graph is used as presented in 4.9, where all the bit labels are again set to zero. However, after preparing the same graph state, the dealer performs some extra actions before distributing the qubits to the players.

4.7.1 State and secret distribution

First, the dealer prepares the graph state induced by 4.9. Then, the dealer does a Bell basis measurement on the input qubit $|S\rangle$ and the qubit 0. Depending on the measurement outcome, the dealer then applies unitary corrections to the remaining qubits. These involve Z corrections on the qubits of players 2,3,..., n and potential Z and X corrections on the qubit of player 1. In particular, if (b_1, b_2) encode the result of the Bell basis measurement, then player 1 performs the correction $X^{b_1} \circ Z^{b_2}$ and the remaining players perform Z^{b_1} on their qubits. Graphically, the initial state is given by :



After preparing this state, the dealer sends each player one qubit. The secret is already encoded in the initial state and the dealer takes no further part in the protocol.

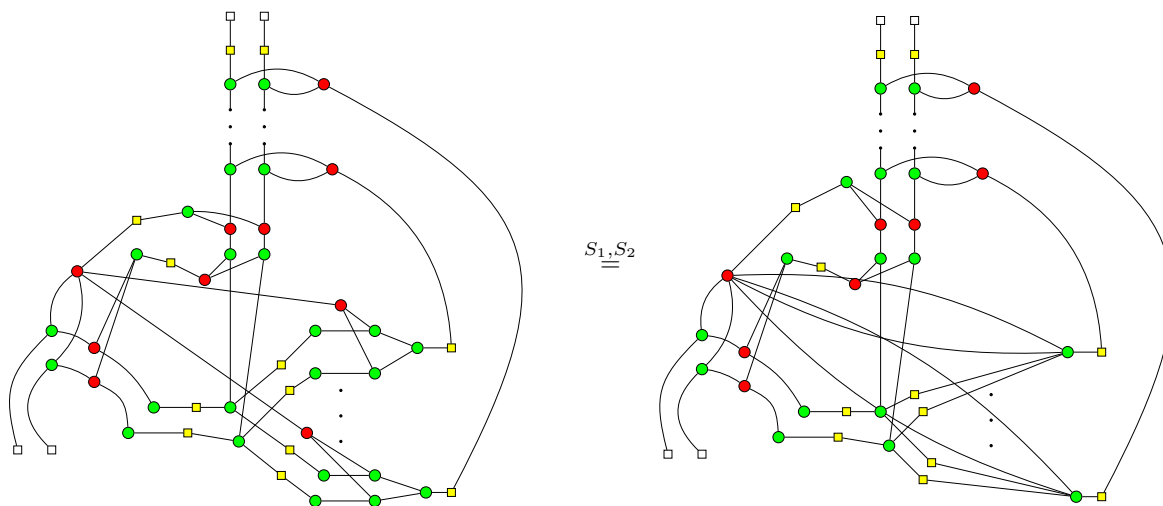
4.7.2 Secret Reconstruction

There are two cases to consider for this part of the protocol. If player 1 is to receive the quantum secret $|S\rangle$, then the protocol is executed by the following steps :

1. Players 2, 3, ..., n measure in the computational basis
2. Players 2, 3, ..., n send their measurement results x_i to player 1.
3. Player 1 performs the unitary correction $Z^{\oplus x_i} \circ H$
4. Player 1 now has the quantum secret $|S\rangle$

Figure 4.15 shows how each step is formalized.

We can show that these steps indeed result in the secret being teleported to player 1.



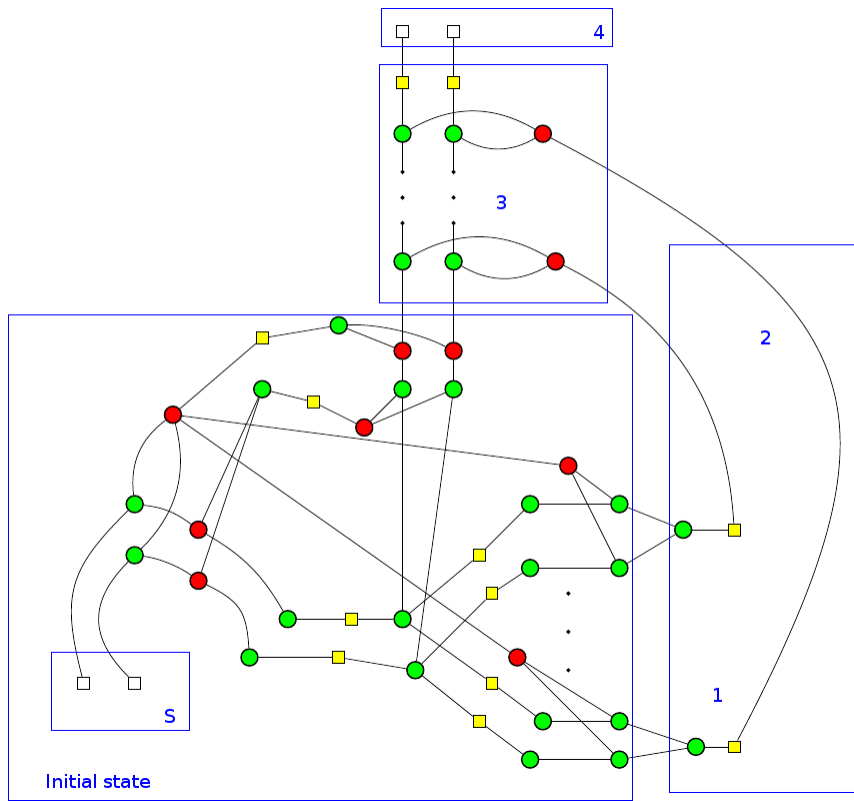
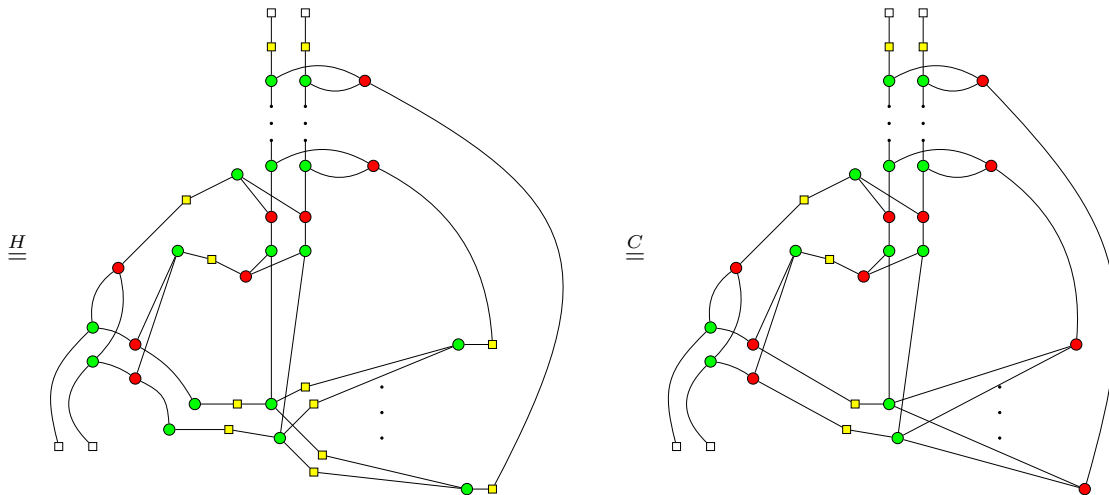
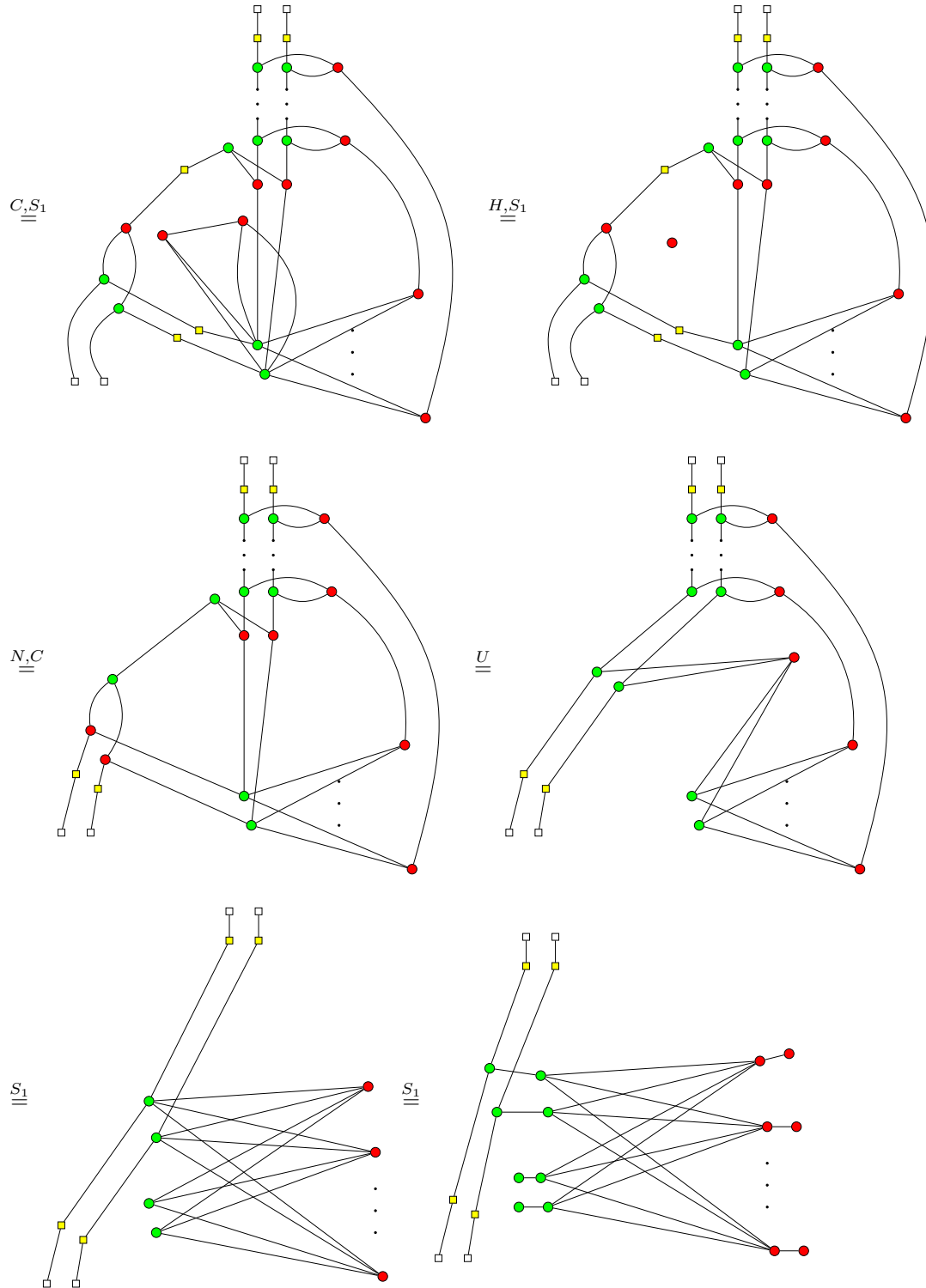
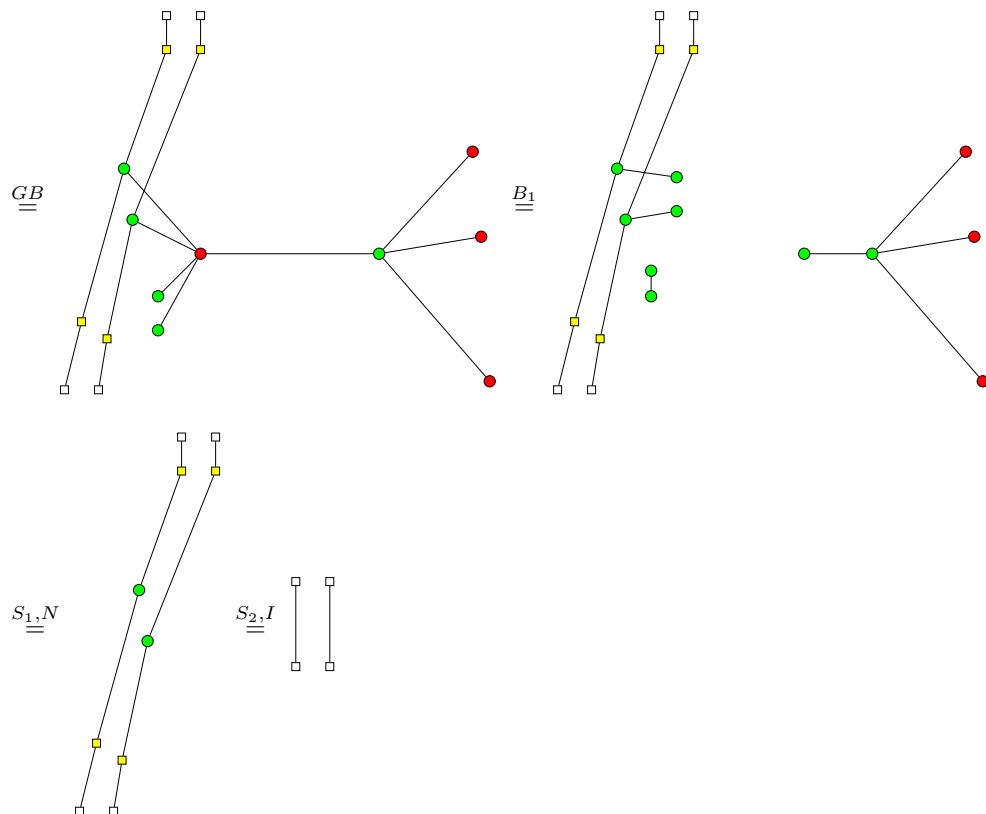


Figure 4.15: QQ (n,n) measurement protocol





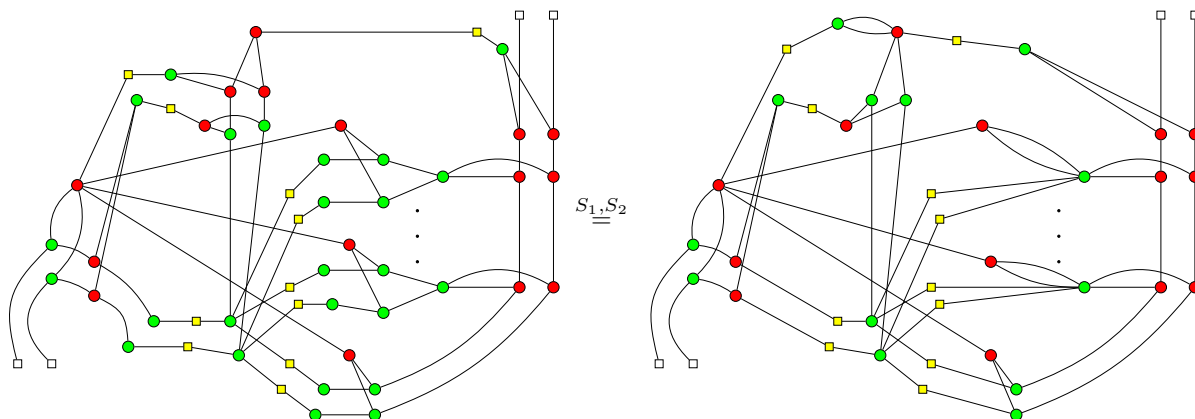


In the remaining case, one of players 2, 3, ..., n should receive the secret. Let's assume player n will reconstruct it. This is done by the following steps :

1. Player 1 measures in the X direction and sends his result x_1 to player n
2. Players 2,3,..., n - 1 measure in the Z basis and send their results x_i to player n
3. Player n performs the unitary correction $X^{\oplus x_i}$
4. Player n now has the quantum secret $|S\rangle$

Figure 4.16 shows the graphical representation of each step.

Proof of correctness is given below.



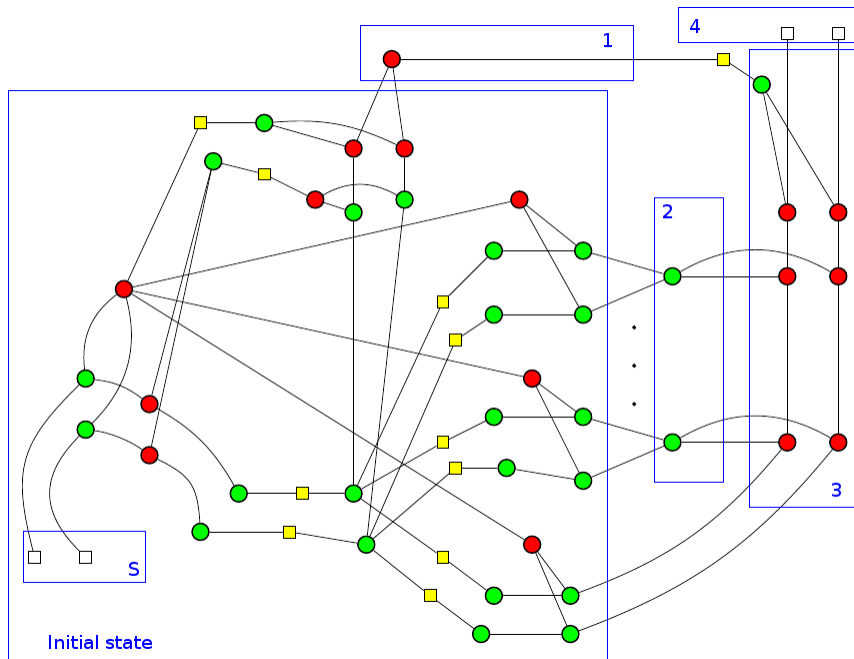
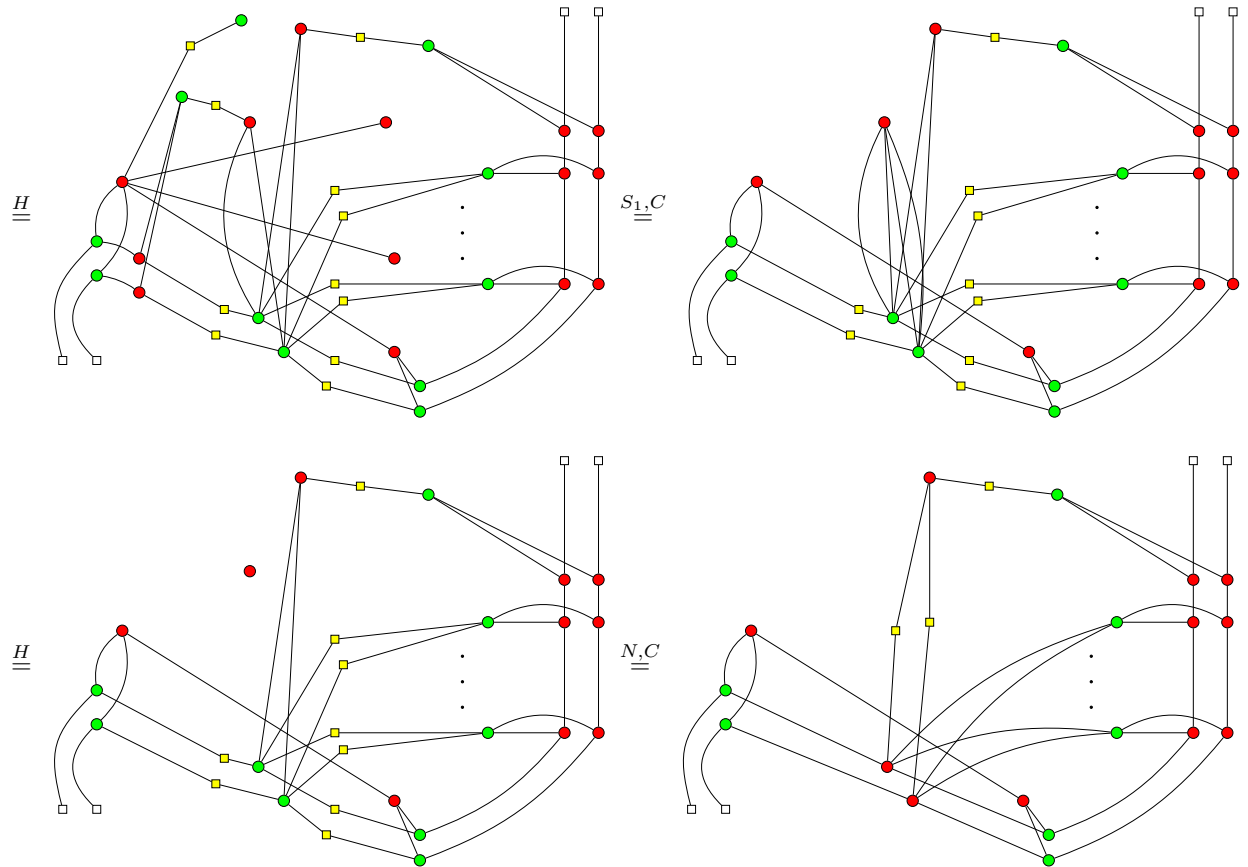
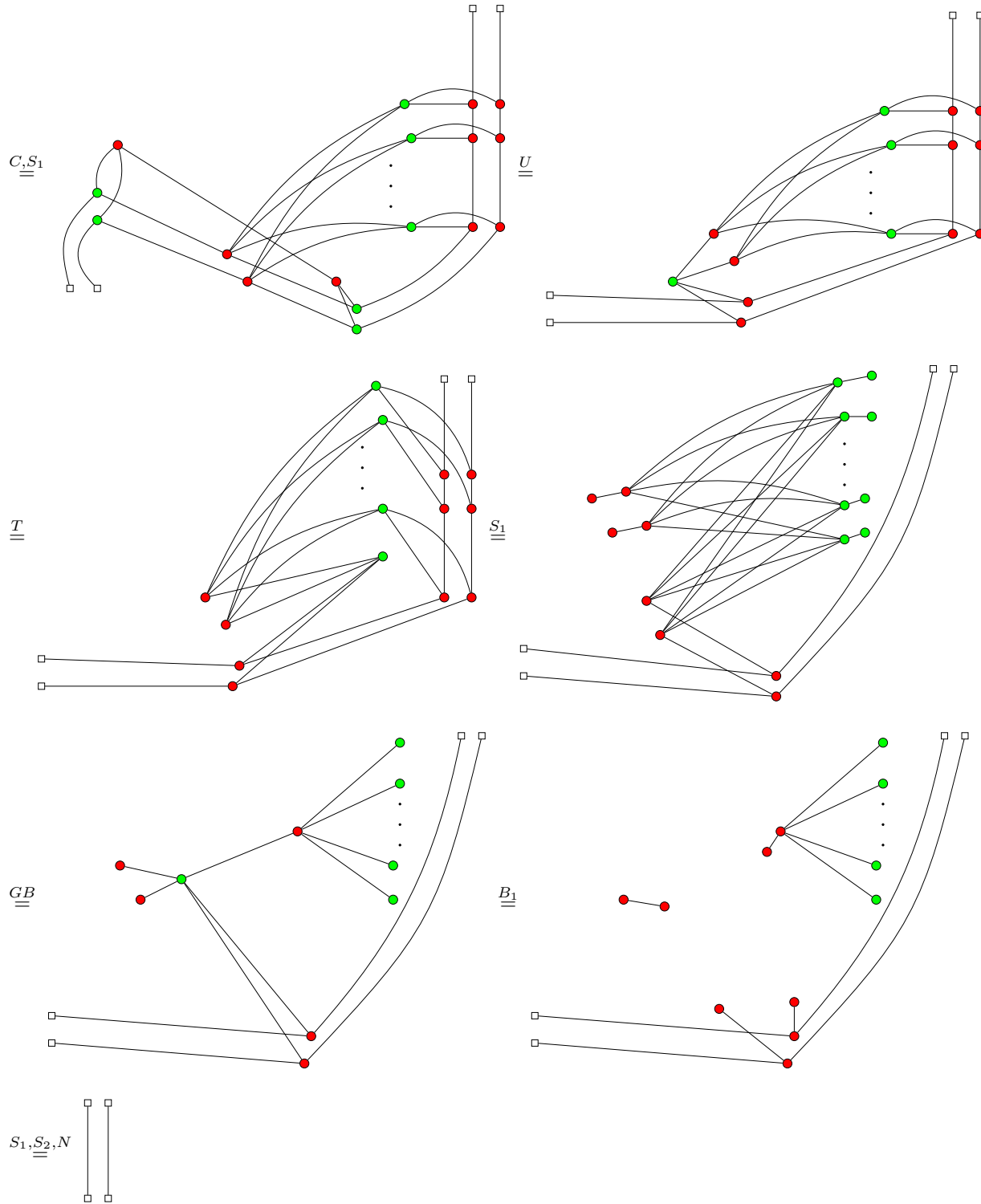


Figure 4.16: QQ (n,n) measurement protocol



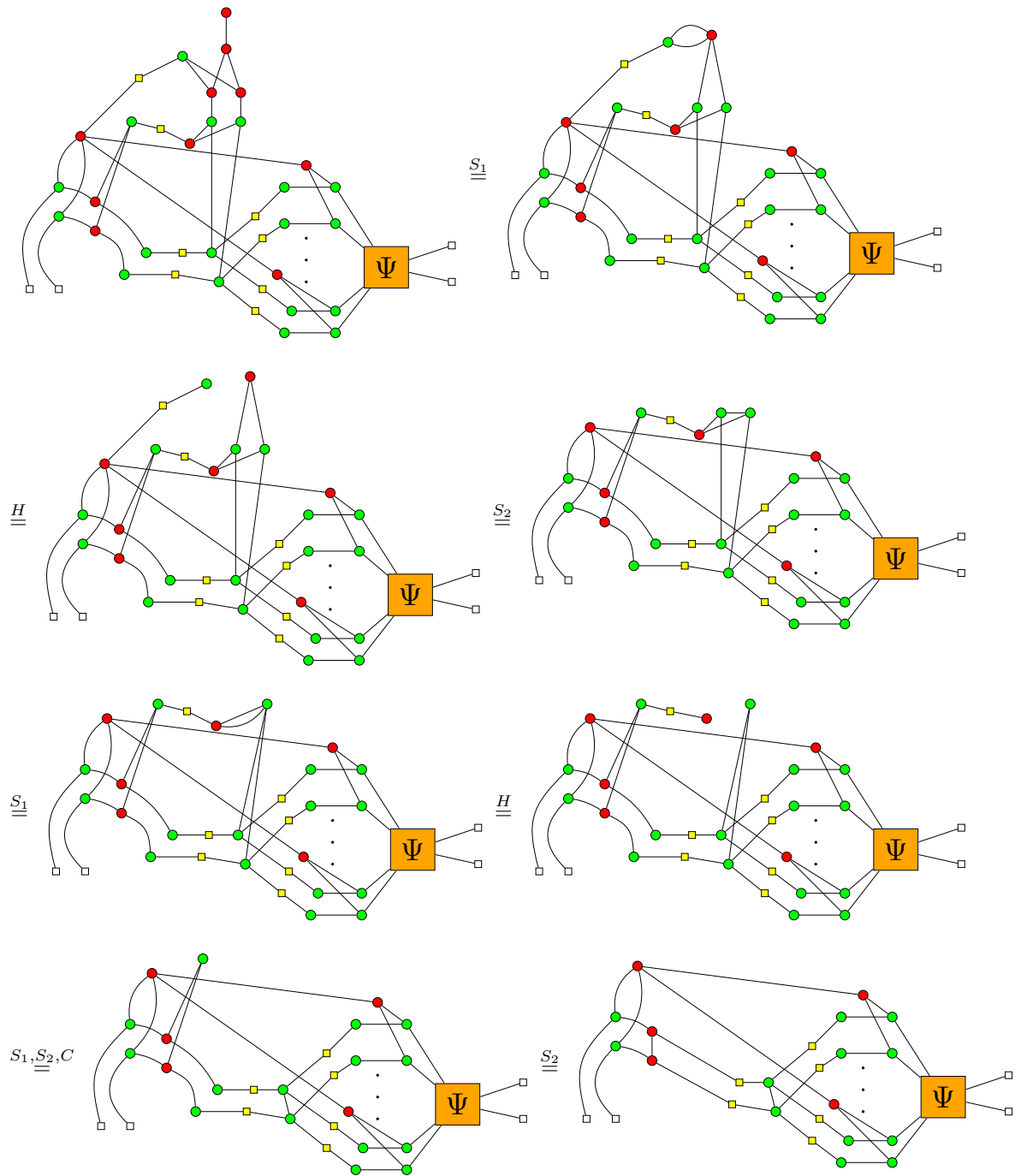


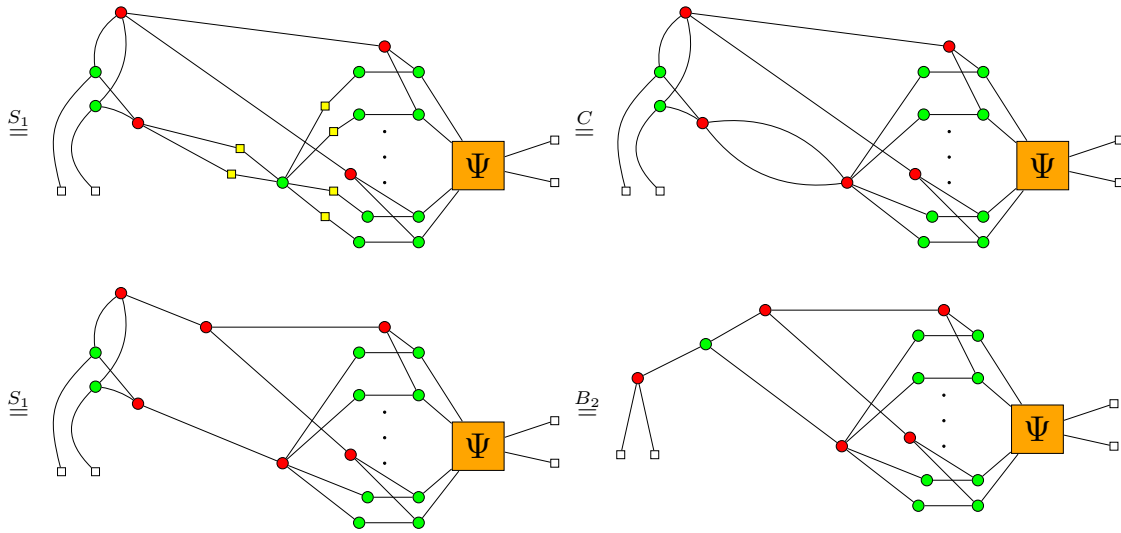
4.7.3 Secret inaccessibility

In order to prove the secret inaccessibility of the protocol, we use similar arguments to the HBB QQ protocol - we consider the information flow when one player is not helping the others. Due to the

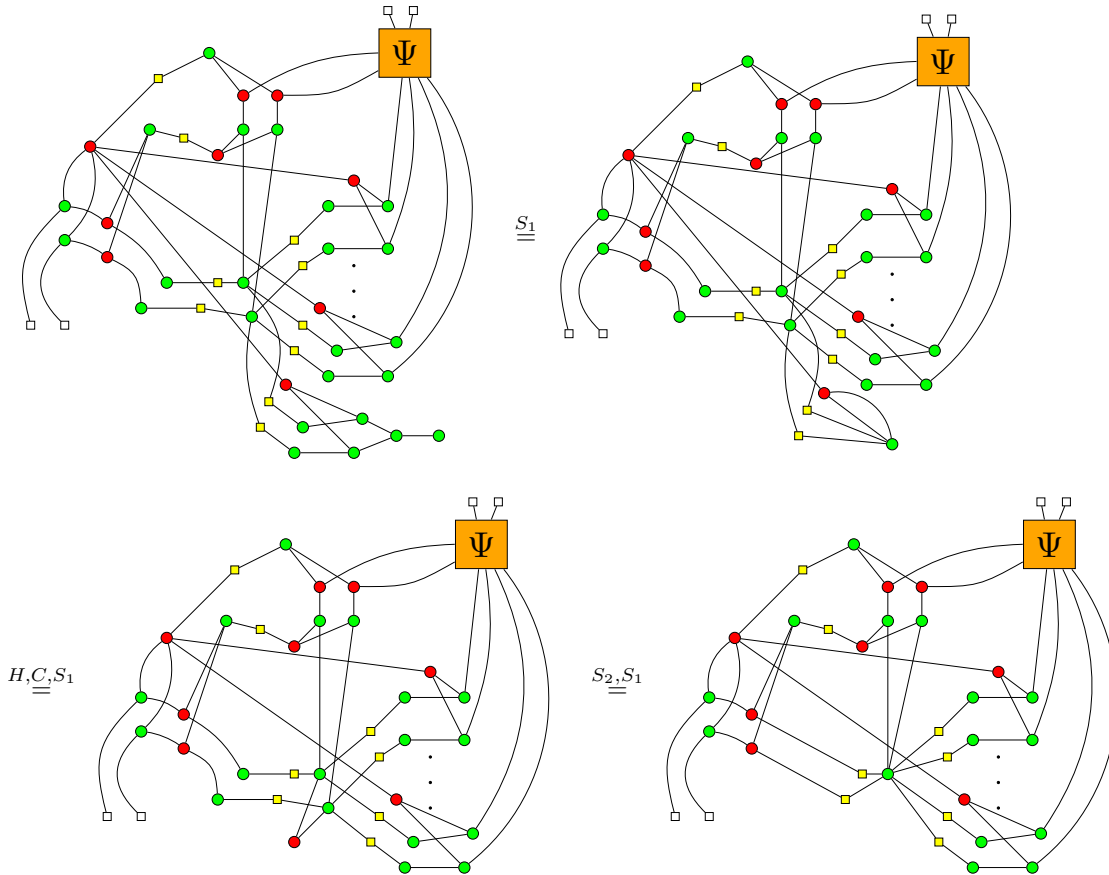
topology of the graph, we need to consider two cases - when player 1 is not helping and when some other player is not collaborating (without loss of generality we assume it is player n).

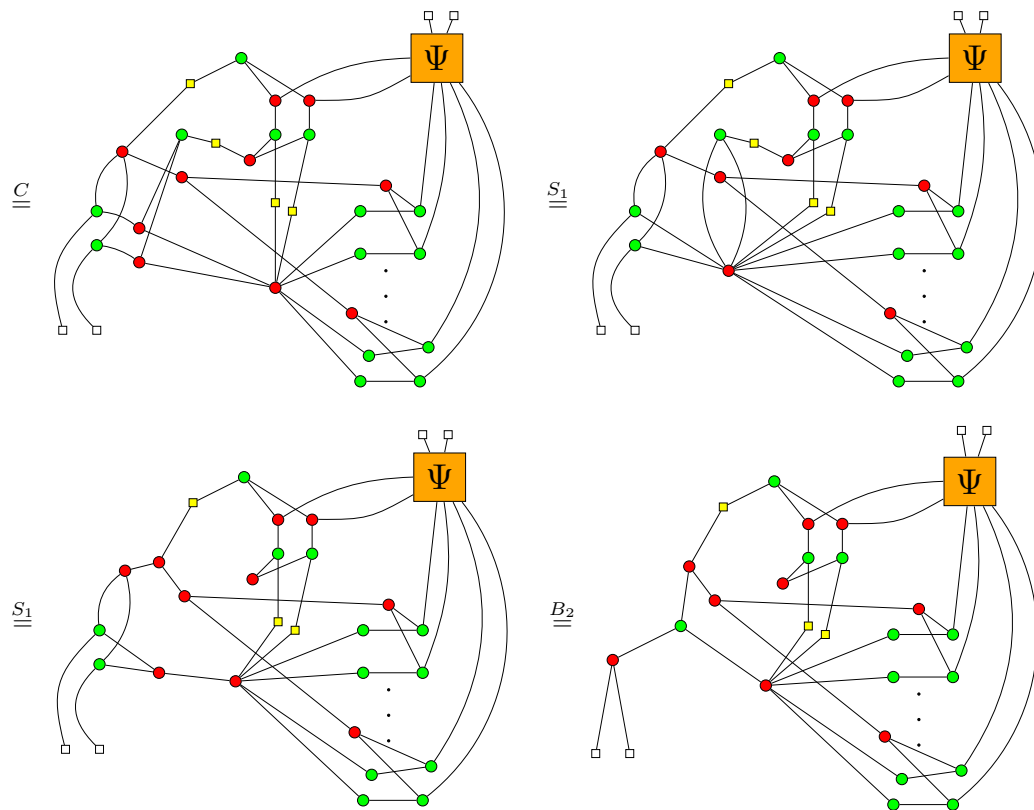
First case - player 1 is not collaborating. Let's see what happens when he measures his qubit, but does not share the result with anybody





Second case - player n is not helping the others.





We can see that, in both cases, the output would be the same for states $|0\rangle$ and $|1\rangle$. Therefore, this is an example of a quantum secret sharing scheme. However, the QSS scheme is not perfect, because the players are able to perfectly discriminate between states $|+\rangle$ and $|-\rangle$ as noted in the erratum which the authors published afterwards [18]. By using similar arguments to the HBB QQ protocol, for a good choice of Ψ , we can show how these two states are teleported.

Chapter 5

Conclusion

We studied different quantum secret sharing protocols in an abstract way. Instead of using the traditional Hilbert space formalism, we used the ZX calculus. We were able to formally prove the correctness of two important aspects of quantum secret sharing protocols. By doing so, our intuitive and rigorous graphical approach enabled us to identify errors in some of the proposed protocols. This shows that the ZX calculus is an adequate framework for the study of quantum secret sharing protocols and of quantum computation in general.

However, our approach is certainly not perfect. We did not consider one important aspect of quantum secret sharing protocols - security. Finding a good way to model the security of protocols does not seem to be easy and this could perhaps be addressed in future work.

Another question which naturally arises is the scalability of the approach. Although the exact complexity for this types of problems is currently unknown, the author's personal experience has been that increasing the size of diagrams significantly increases the number of rewriting rules which are needed. In particular, the author was unable to find a short rewriting strategy for proving the correctness of the $QQ(3,5)$ GSS protocol, whose diagram representation is certainly the largest of all presented here. We have also seen that Y measurements greatly increase the complexity for some of the diagrams. The proof of correctness of the $(3,5)$ sharing schemes (some of the largest diagrams) has taken a considerable amount of time for the author. The scalability of the approach can perhaps be improved by discovering common patterns in these diagrams and introducing appropriate notations and rewriting rules.

Finally, future work in using computer assistance for proving the correctness of quantum secret sharing protocols seems to be promising. `Quantomatic`[2] is a software tool which can be used to work with the diagrams from the ZX calculus. Implementing features in `Quantomatic` which would help a person to work with these diagrams can further improve the scalability of the approach.

Bibliography

- [1] Bibliography on Secret Sharing Schemes as of 1998. <http://cacr.uwaterloo.ca/~dstinson/ssbib.html>.
- [2] Quantomatic. <https://sites.google.com/site/quantomatic/>.
- [3] A. Shamir. How to share a secret. *Communications of the ACM*, 26:313–317, 1979.
- [4] S. Abramsky and B. Coecke. A Categorical Semantics of Quantum Protocols. In *19th IEEE conference on Logic in Computer Science (LiCS'04)*. IEEE Computer Science Press, 2004.
- [5] Anne Hillebrand. Quantum Protocols involving Multipartite Entanglement and their Representations in the zx-calculus. Master Thesis, 2011. <http://www.cs.ox.ac.uk/people/bob.coecke/Anne.pdf>.
- [6] B. Coecke, R. Duncan, A. Kissinger and Q. Wang. Strong Complementarity and Non-locality in Categorical Quantum Mechanics. *Symposium on Logic in Computer Science (LICS), 2012 27th Annual IEEE*, pages 245–254, 2012.
- [7] Bob Coecke. Kindergarten Quantum Mechanics, arXiv:quant-ph/0510032v1, 2005. <http://arxiv.org/abs/quant-ph/0510032>.
- [8] C. H. Bennett and G. Brassard and C. Crepeau and R. Jozsa and A. Peres and W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Physical Review Letters*, 1993.
- [9] Chris Heunen and Jamie Vicary. Lectures on Categorical Quantum Mechanics, 2012. <https://www.cs.ox.ac.uk/files/4551/cqm-notes.pdf>.
- [10] B. Coecke and R. Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(043016), 2011.
- [11] B. Coecke, E. Paquette, and D. Pavlovic. *Classical and quantum structuralism*, pages 29–69. Cambridge University Press, 2009.
- [12] David Deutsch. Quantum computation. *Physics World*, 1992.
- [13] R. Duncan and S. Perdrix. Graph States and the Necessity of Euler Decomposition. In *CiE '09 Proceedings of the 5th Conference on Computability in Europe: Mathematical Theory and Computational Practice*, pages 167–177. Springer, 2009.
- [14] G. R. Blakley. Safeguarding cryptographic keys. In *AFIPS National Computer Conference*, pages 313–317, 1979.
- [15] D. Greenberger, M. Horne, and A. Zeilinger. Going beyond Bell’s theorem. *Quantum Theory and Conceptions of the Universe*, page 69, 1999.

-
- [16] M. Hillery, V. Buzek, and A. Berthiaume. Quantum Secret Sharing. *Physical Review A*, 59:1829–1834, 1999.
- [17] Miriam Backens. The ZX-calculus is complete for stabilizer quantum mechanics, 2012. Draft paper.
- [18] B. C. Sanders and D. Markham. Erratum: Graph states for quantum secret sharing.
- [19] B. C. Sanders and D. Markham. Graph States for Quantum Secret Sharing.
- [20] P. Selinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical computer science*, 170:139–167, 2007.
- [21] P. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Scientific Computing*, 26:1484–1509.
- [22] L. Xiao, G.L. Long, F-G. Deng, and J-W Pan. *Physical Review A*, 69(052307), 2004.