

# Exploring Quantum Secret Sharing with the ZX Calculus

Vladimir Nikolaev Zamdzhiev

Oriel College,  
University of Oxford

29 October 2013

# Secret Sharing Motivation

- Independently introduced in 1979 by Blakley [3] and Shamir [1]
- Main idea – a dealer wishes to share a secret between several players
- Secret is only accessible to players if they work together and denied otherwise
- Cryptographic problem which has been studied extensively

# Secret Sharing Motivation

- Independently introduced in 1979 by Blakley [3] and Shamir [1]
- Main idea – a dealer wishes to share a secret between several players
- Secret is only accessible to players if they work together and denied otherwise
- Cryptographic problem which has been studied extensively
- Applications :
  - secure nuking of countries (or activation of weapons / bombs)

# Secret Sharing Motivation

- Independently introduced in 1979 by Blakley [3] and Shamir [1]
- Main idea – a dealer wishes to share a secret between several players
- Secret is only accessible to players if they work together and denied otherwise
- Cryptographic problem which has been studied extensively
- Applications :
  - secure nuking of countries (or activation of weapons / bombs)
  - joint access to a shared bank account

# Secret Sharing Motivation

- Independently introduced in 1979 by Blakley [3] and Shamir [1]
- Main idea – a dealer wishes to share a secret between several players
- Secret is only accessible to players if they work together and denied otherwise
- Cryptographic problem which has been studied extensively
- Applications :
  - secure nuking of countries (or activation of weapons / bombs)
  - joint access to a shared bank account
  - guard commercial secrets

# Secret Sharing Example

- Consider 3 people – Alice, Bob and Charlie.
- Alice wants to share a secret bit string  $s$  (e.g. 100101) between Bob and Charlie.
- Alice can do so by following these steps :
  - 1 Alice generates a random bit string  $k$  (key) of the same length (e.g. 111001)
  - 2 Alice computes  $b := s \oplus k$  (result 011100)
  - 3 Alice sends  $b$  to Bob and  $k$  to Charlie
  - 4 Neither Bob, nor Charlie has any information about the secret
  - 5 If Bob and Charlie work together, they can compute the secret by summing their bit strings

# Threshold Secret Sharing

A  $(k, n)$  Threshold Secret Sharing Scheme is described by :

- $n$  players and a dealer
- Every set of  $k$  (or more) players working together must be able to reconstruct the secret
- Fewer than  $k$  players are denied some information about the secret
- If any set of fewer than  $k$  players gain no information about the secret, then the sharing scheme is called *perfect*

# Quantum Secret Sharing

- Type of secret sharing, where quantum mechanical phenomena are used to achieve the goal
- Information to be shared can be either classical bit ( $s$ ) or qubit ( $|s\rangle$ )
- We formally prove the correctness of two aspects of QSS protocols :
  - reconstruction of secret by authorized sets of players
  - denial of secret to unauthorized sets of players
- We do not consider security aspects like eavesdropping, cheating and other attacks (arguments don't easily translate to ZX calculus)



# Threshold Quantum Secret Sharing

Three main types :

- $CC(k, n)$  – share a classical secret over private channels
- $CQ(k, n)$  – share a classical secret over public channels between dealer and players
- $QQ(k, n)$  – share a quantum secret, private channel between players
- Since we ignore security, we also ignore difference between public and private channels

# Computational observations for $T(Q)SS$

For a  $(k, n)$   $T(Q)SS$  we have :

- If  $k - 1$  players cannot distinguish between two fixed secrets, independently from the actions of the rest of the players, then we establish the deniability property
- If  $k - 1$  players cannot distinguish between any two secrets, independently from the actions of the rest of the players, then we establish perfect deniability
- That's how we model the deniability phase using the ZX calculus

# ZX Calculus Motivation

- formally reason about Quantum Computation and Information
- use a graphical notation
- avoid Hilbert Space formalism

# ZX Calculus syntax and semantics

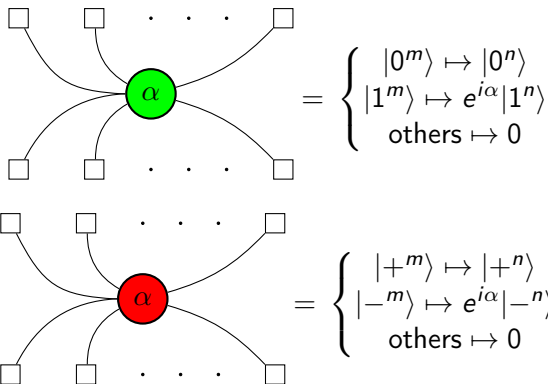
$$\begin{array}{c}
 \square \\
 \downarrow \\
 \square
 \end{array}
 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_Q$$
  

$$\begin{array}{cc}
 \square & \square \\
 \diagdown & \diagup \\
 & \\
 \diagup & \diagdown \\
 \square & \square
 \end{array}
 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \sigma_{Q^2}$$
  

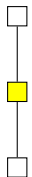
$$\begin{array}{cc}
 & \text{---} \\
 \square & \square \\
 & \text{---} \\
 \square & \square
 \end{array}
 = \langle 00 | + \langle 11 |$$
  

$$\begin{array}{cc}
 & \text{---} \\
 \square & \square \\
 & \text{---} \\
 \square & \square
 \end{array}
 = |00\rangle + |11\rangle$$

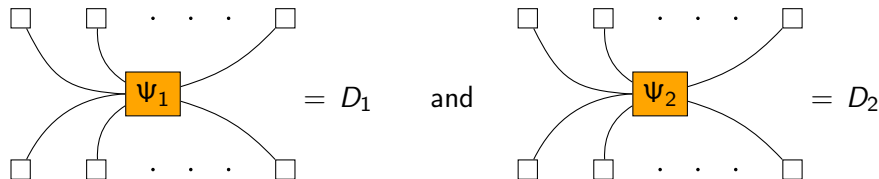
# ZX Calculus syntax and semantics



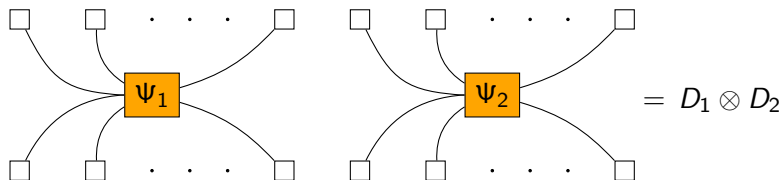
# ZX Calculus syntax and semantics


$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

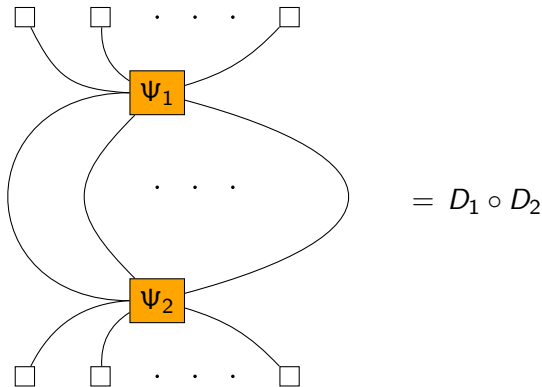
# ZX Calculus syntax and semantics



then



# ZX Calculus syntax and semantics



By following the above rules we can represent any pure state map  $f : Q^m \mapsto Q^n$  as a diagram in the ZX calculus [2].



# CP construction

The ZX calculus as introduced so far has some limitations

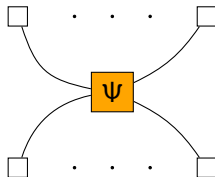
- post-selecting measurement results leading to case distinction
- can't model flow of classical information
- can't do conditional unitary operations without case distinction

We can avoid that by using the CP construction and working in  $\text{CP}(\text{FHilb})$  instead of  $\text{FHilb}$ .

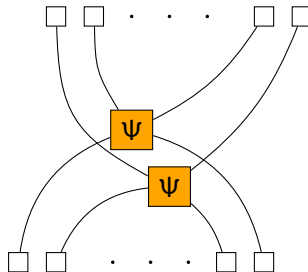
- doubles the size of diagrams with the same Hilbert space interpretation
- syntax and rewriting rules remain the same
- semantics extend straightforwardly

# From FHilb to CP(FHilb)

FHilb :




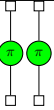

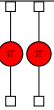




CP(FHilb) :



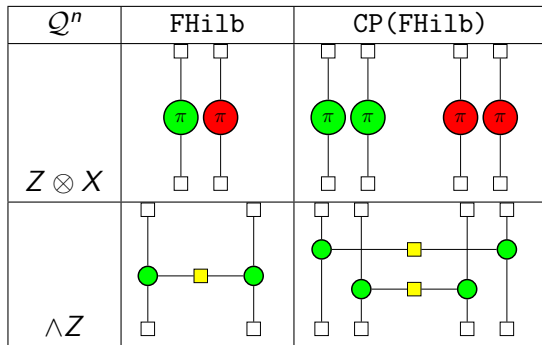
# Common Quantum States

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



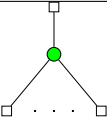
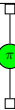
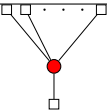
# Common unconditional unitary operations

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

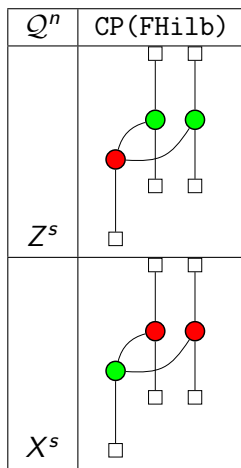
# Common 2-qubit gates





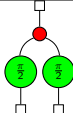
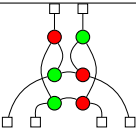
# Classical data and operations

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

# Conditional Unitary Operations



# Measurements

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

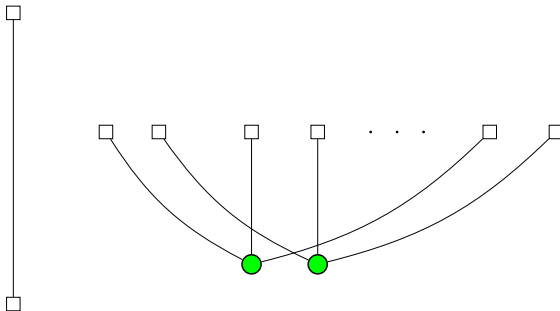


# HBB protocols overview

- In 1999, Hillery, Buzek and Berthiaume proposed the first quantum secret sharing protocols [4]
- Based on the GHZ state :  $(|000\rangle + |111\rangle)$
- Two protocols – CQ(2,2) and QQ(2,2)
- Straightforward generalisation to CQ(n,n) based on generalised GHZ state  $(|0^n\rangle + |1^n\rangle)$  [7]

# 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.

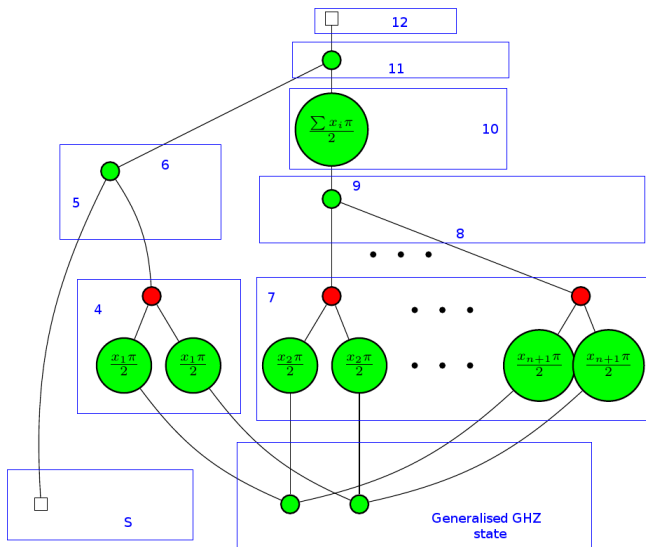
# Protocol Description

- 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)

# Protocol Description

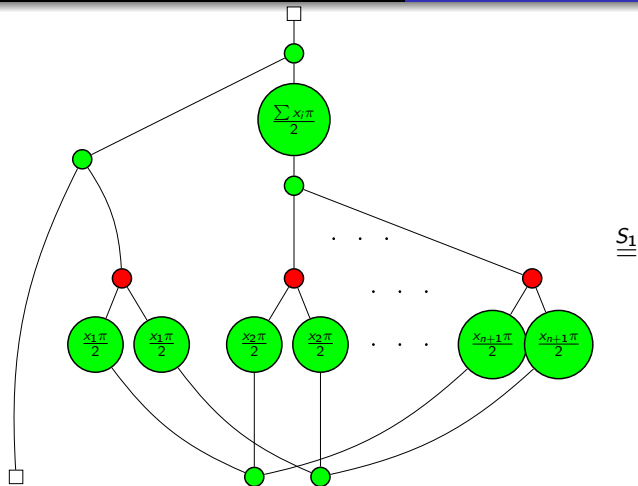
- 7 Every player measures his qubit in the selected direction
- 8 All players send their measurement outcomes to player 1.
- 9 Player 1 sums all measurement outcomes (including his) modulo 2.
- 10 Depending on the announced measurement directions, player 1 performs a negation on the result of the previous 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  $S$

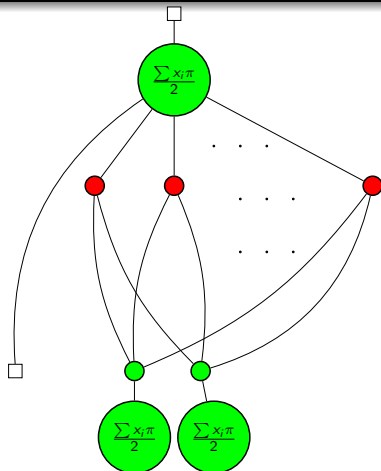
# Protocol Description in ZX Calculus



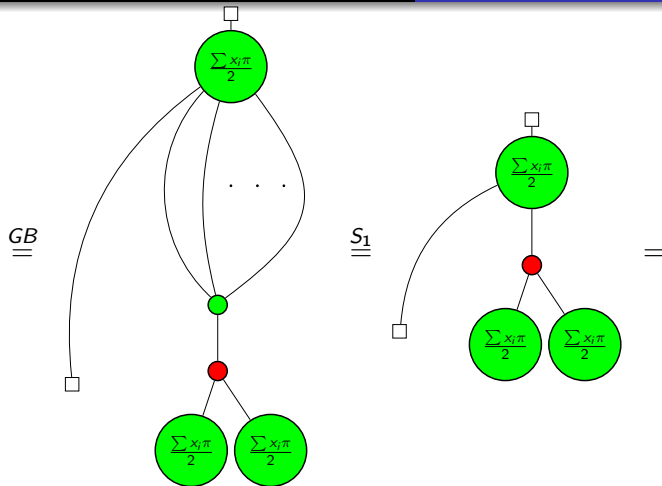
# Secret Reconstruction

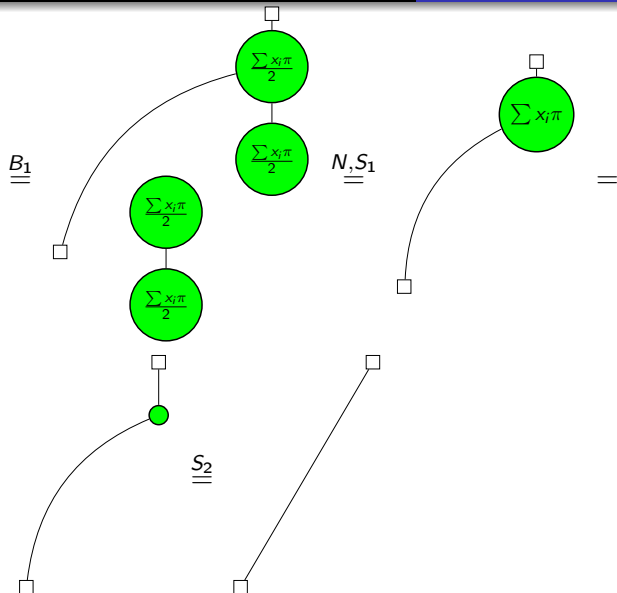
- Now we have to show that the secret can be reconstructed by the players
- Proof is on the next few slides









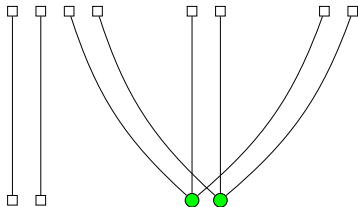


# Secret inaccessibility

Nothing to depict, because if one player is not collaborating, then he won't announce a measurement direction and protocol stops.

# State and Secret Distribution

Quantum secret and a GHZ state

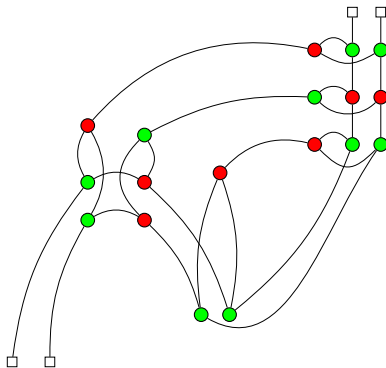


# Protocol Description

WLOG, we assume that the second player will receive the quantum secret.

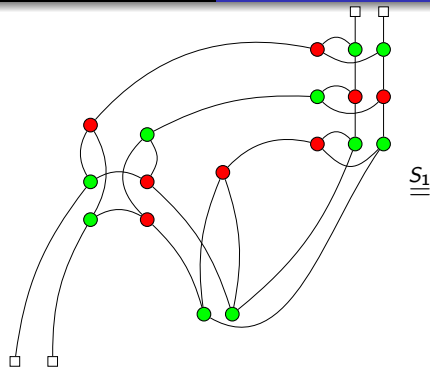
- 1 The dealer measures his qubits in the Bell basis and sends two classical bits  $(d_1, d_2)$  to player 2 to inform him of the measurement outcome
- 2 Player 1 measures his qubit in the  $X$  basis and sends a classical bit  $(p_1)$  to player 2 to inform him of the outcome
- 3 Player 2 performs the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

# Protocol Description in the ZX Calculus

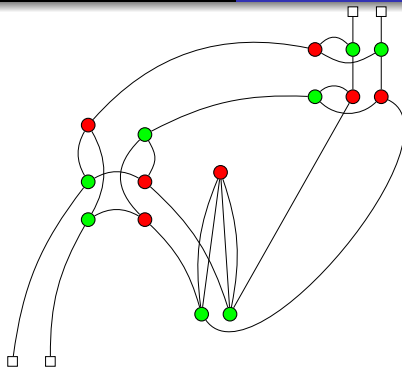


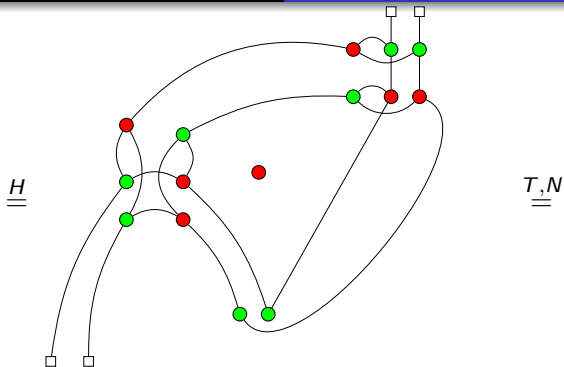
# Secret Reconstruction

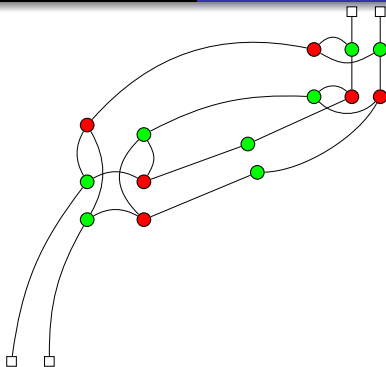
Next, we have to show that the players can reconstruct the quantum secret, that is, the diagram is equal to the identity map.

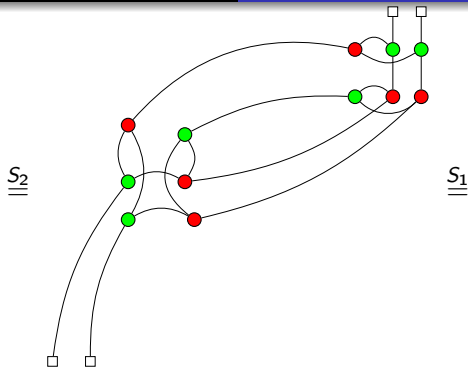


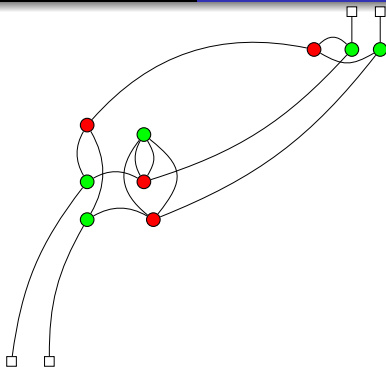


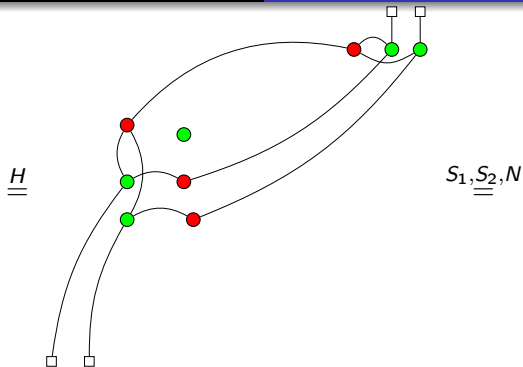


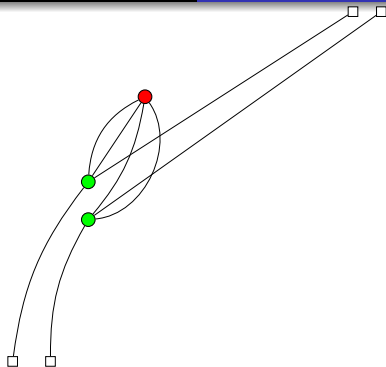


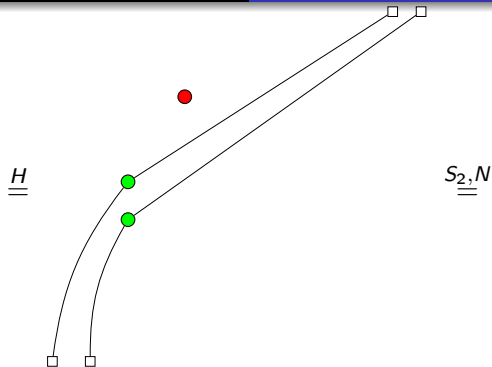




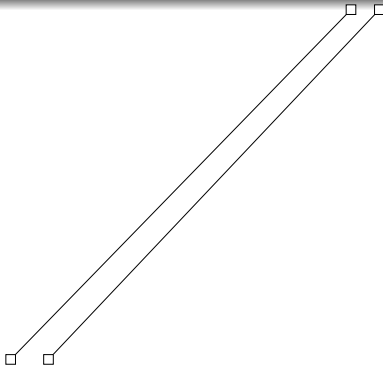






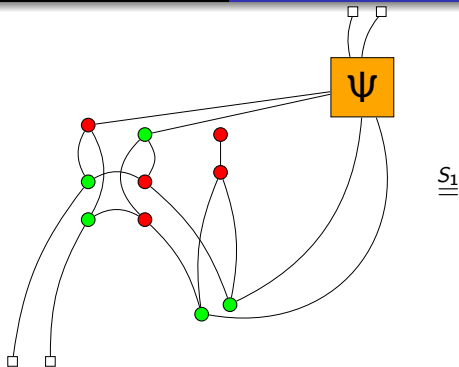


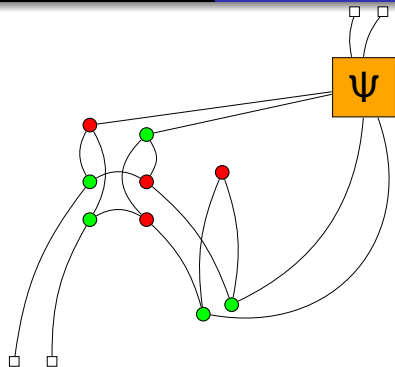


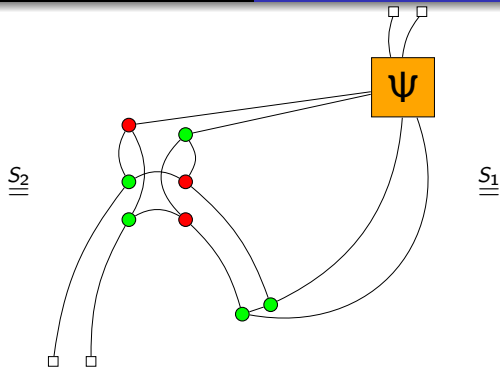


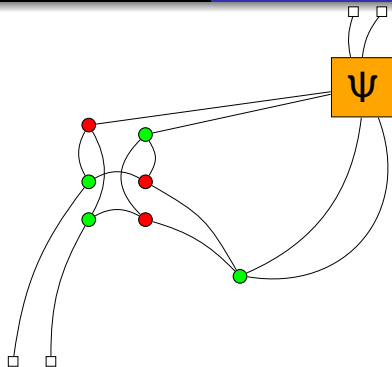
# Secret inaccessibility

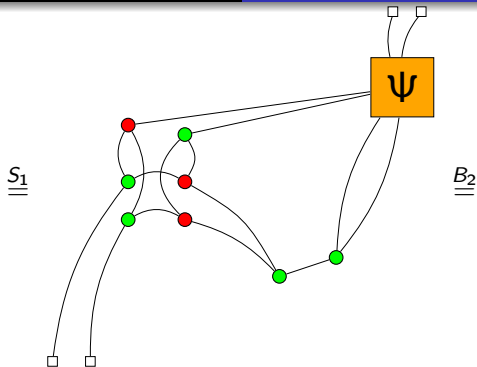
We will show that player 2 is unable to reconstruct the state  $|S\rangle$ , when player 1 performs an  $X$  measurement on his qubit and does not inform player 2 of the outcome. This means, that one player cannot independently obtain the secret and thus this is an example of a (2,2) QQ sharing scheme.

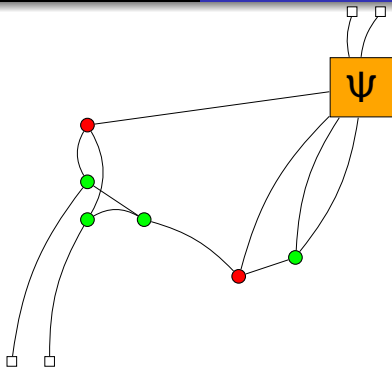




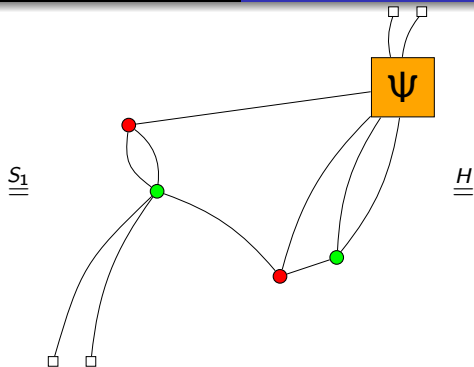


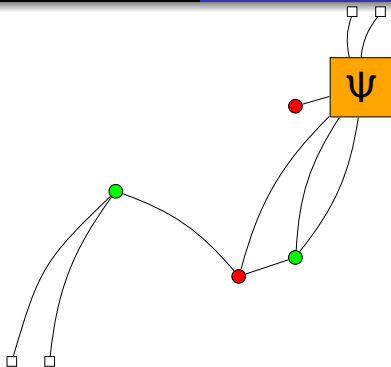












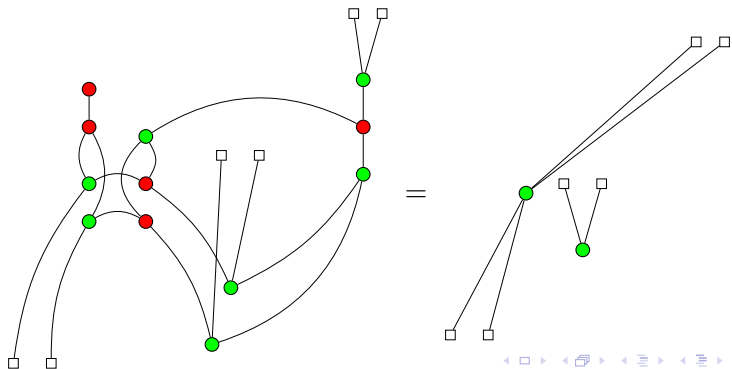
# Secret inaccessibility

The last diagram reveals that, for any  $\Psi$ , 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.

# Secret inaccessibility (not perfect)

The sharing scheme is not perfect however.

We can take  $\Psi$  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 perfectly distinguish between  $|0\rangle$  or  $|1\rangle$ .



# Graph State protocols overview

- Introduced in 2008 by Markham and Sanders [6]
- Important class of QSS protocols
- Based on (extended) graph states
- Authors develop their own graphical formalism to reason about accessibility of information
- ZX Calculus is complete for stabilizer quantum mechanics and therefore graph states

# Graph States

## Definition

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  $(v_i, v_j) \in E$

# Graph States in the ZX Calculus

Graph states are represented in the ZX calculus by

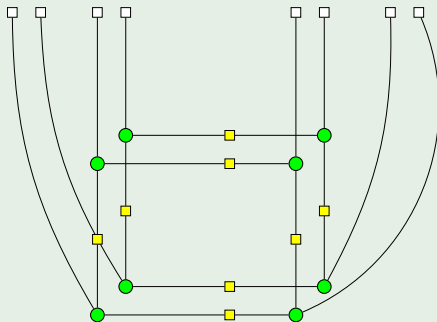
- 1 Drawing two green dots for each vertex and connecting each green dot to an output box
- 2 For every edge  $(v_i, v_j) \in E$  connecting one of the green dots representing vertex  $v_i$  to one of the green dots representing vertex  $v_j$  by a wire and putting a Hadamard gate on the wire. Then do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



# Example : $C_4$ graph state in ZX

## Example

The graph state induced by the cycle graph  $C_4$  is represented in the ZX calculus as :



# CC(3,4) protocol

Based on the cycle graph  $C_4$

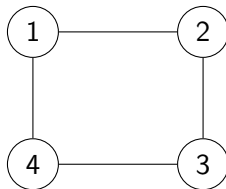
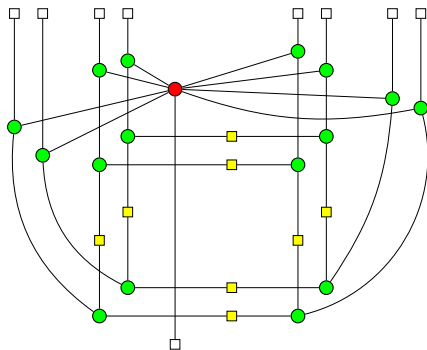


Figure: CC (3,4) graph

# State and secret distribution

The dealer prepares the graph state induced by the graph. The secret is distributed, by performing controlled unitary Z operations on each qubit of the graph state.



Dealer doesn't do anything else for the remainder of the protocol.

# Protocol Description

WLOG, we assume that the players who want to obtain the secret are players 1,2 and 3.

- 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

# Protocol Description in the ZX Calculus

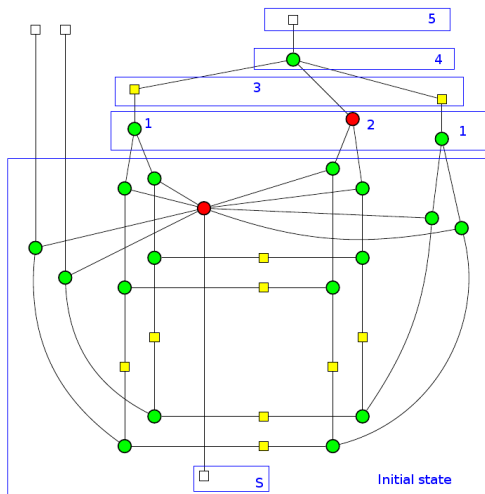
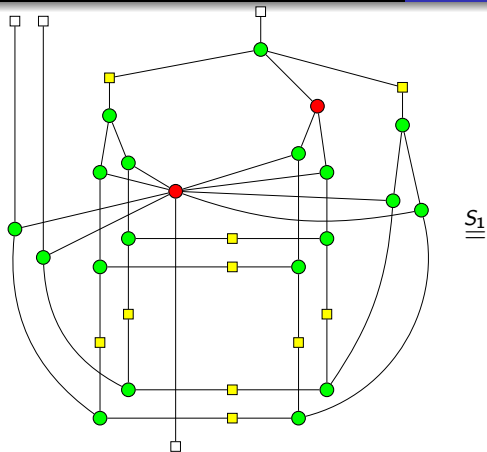
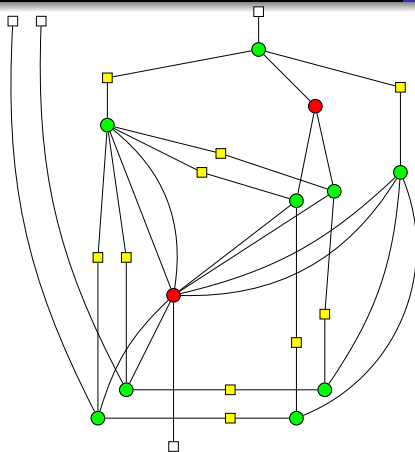


Figure: CC (3,4) protocol

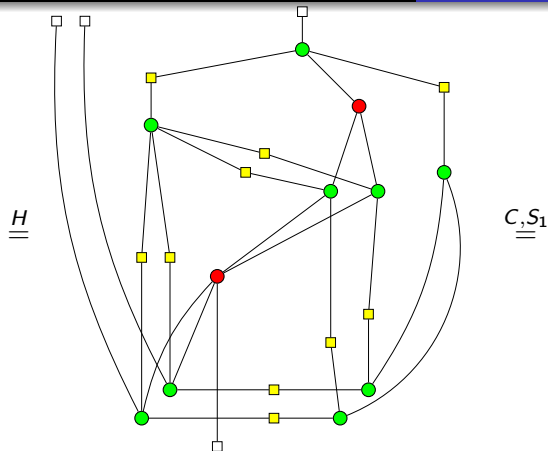
# Secret Reconstruction

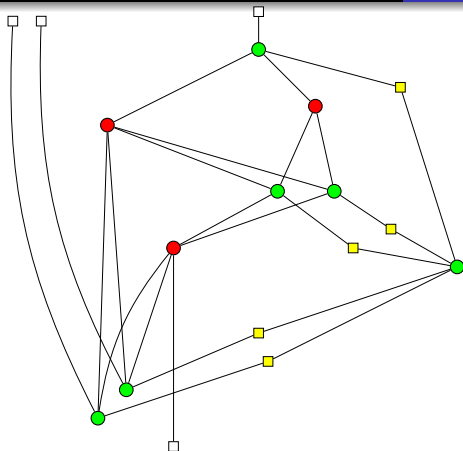
We need to show that the previous diagram contains the identity function on the bit input

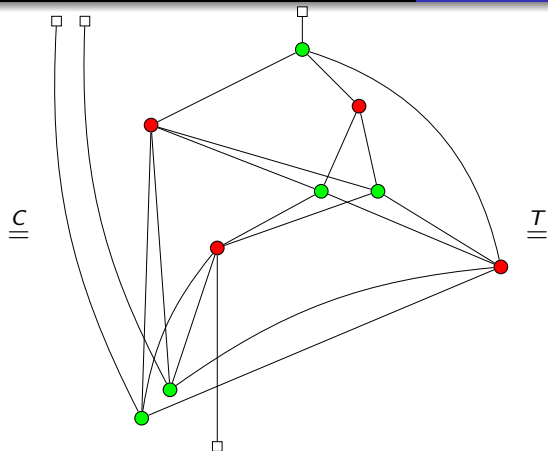


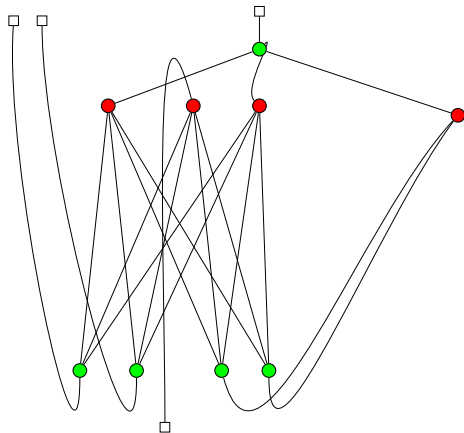


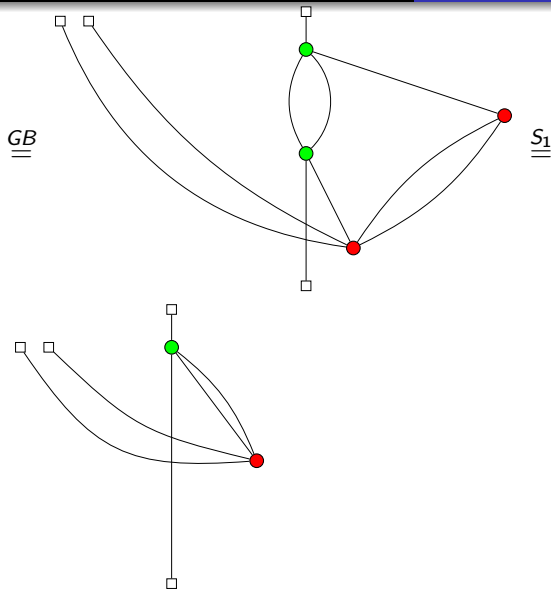


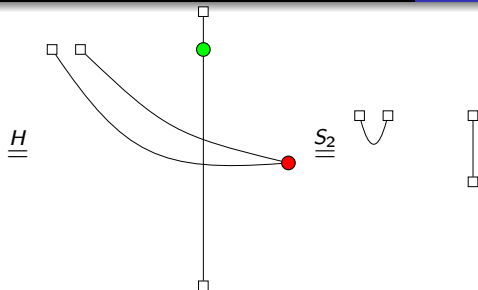








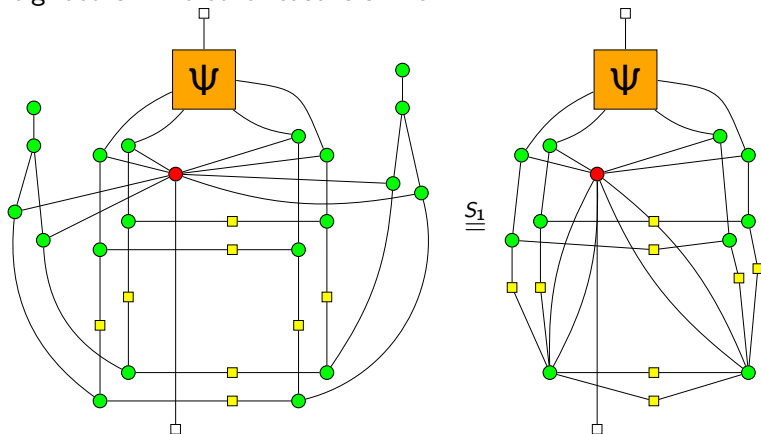




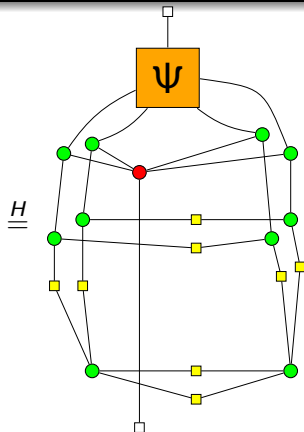
# Secret inaccessibility

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.

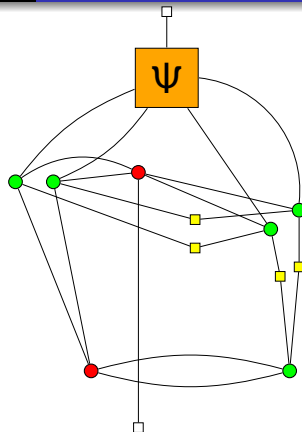
We consider only one case - the two collaborating players are neighbours. The other case is similar.

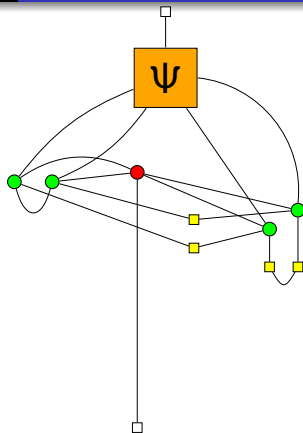
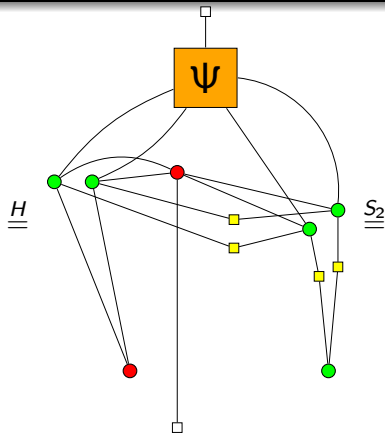


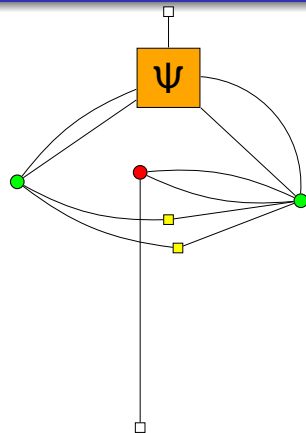
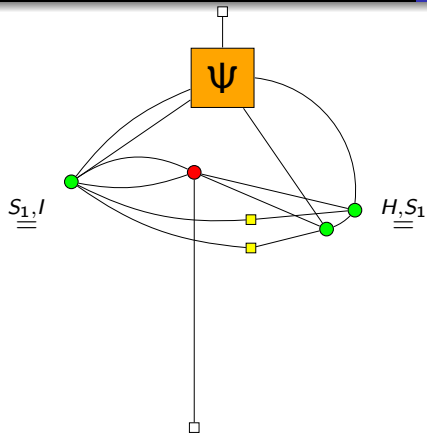


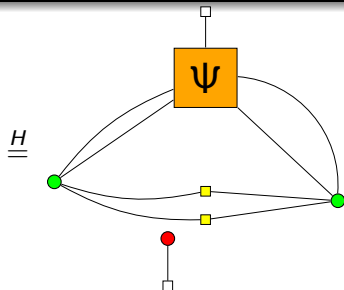


$C, S_1$









# QQ(n,n) protocol

Based on the following graph

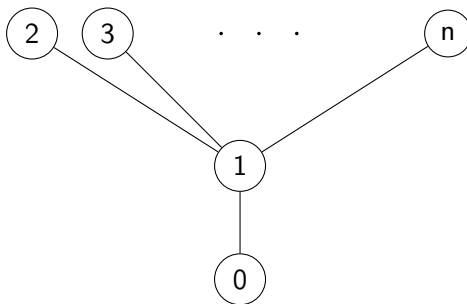
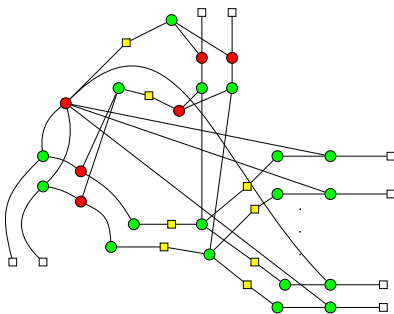


Figure: QQ (n,n) graph

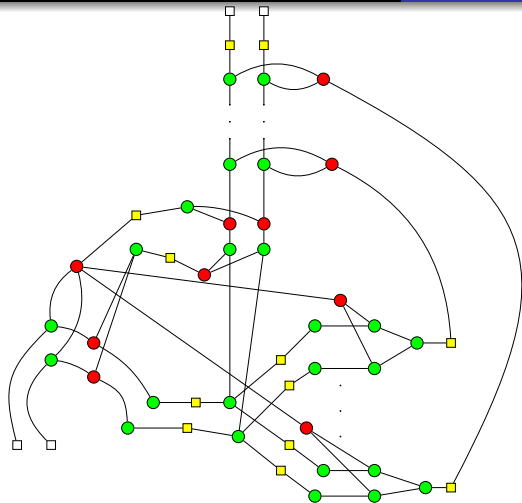
# State and Secret Distribution

The dealer prepares the mentioned graph state. 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. Sends each player one particle and doesn't participate further.



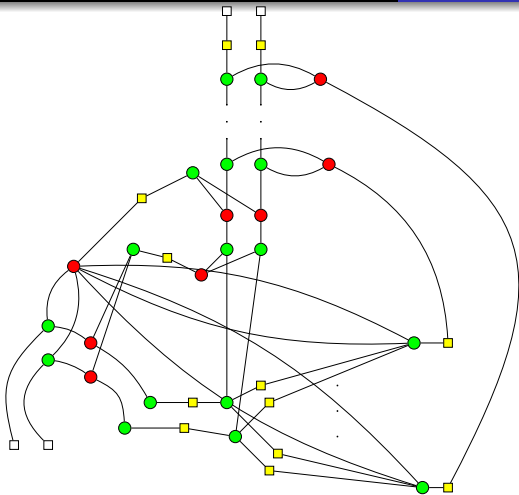
# Protocol Description

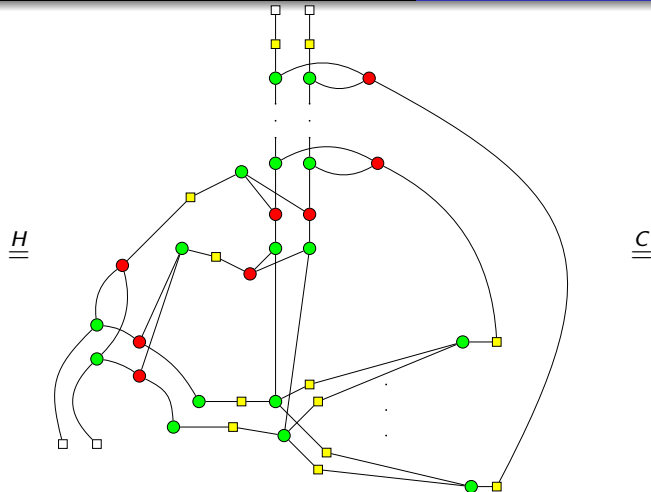
- ① Players 2, 3, ...,  $n$  measure in the computational basis
- ② Players 2, 3, ...,  $n$  send their measurement results  $x_i$  to player 1
- ③ Player 1 performs the unitary correction  $Z^{\bigoplus x_i} \circ H$
- ④ Player 1 now has the quantum secret  $|S\rangle$

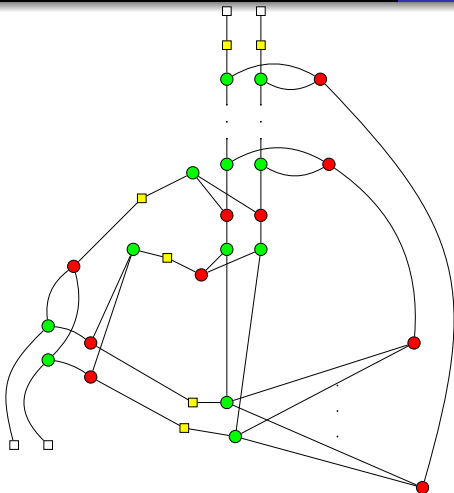


$$\underline{\underline{S_1, S_2}}$$



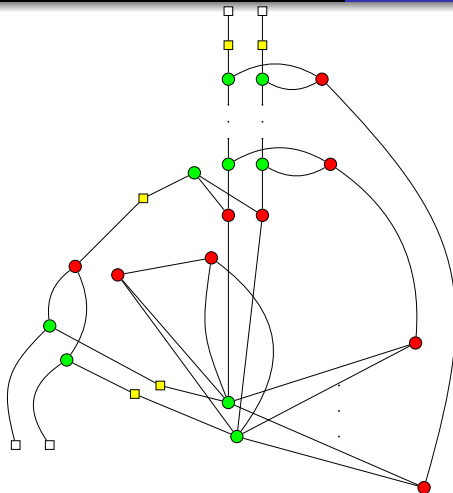


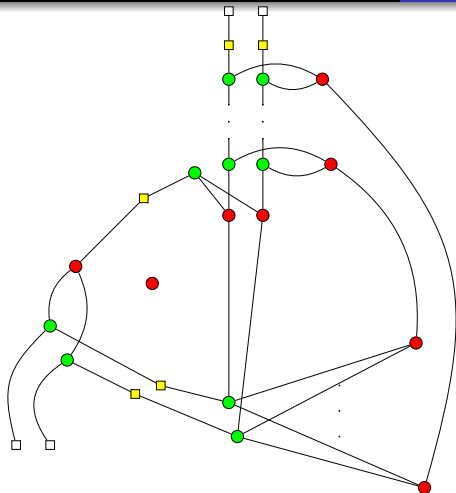


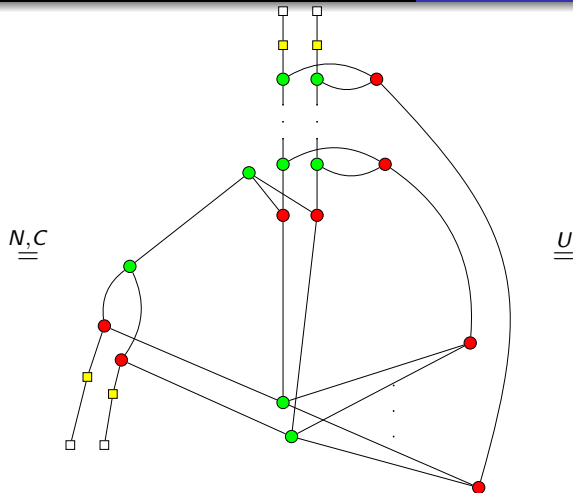


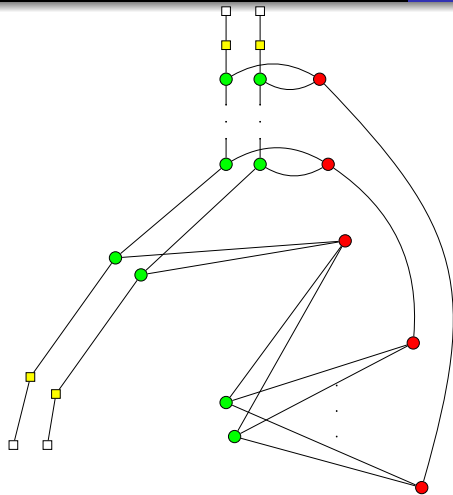
$C, S_1$

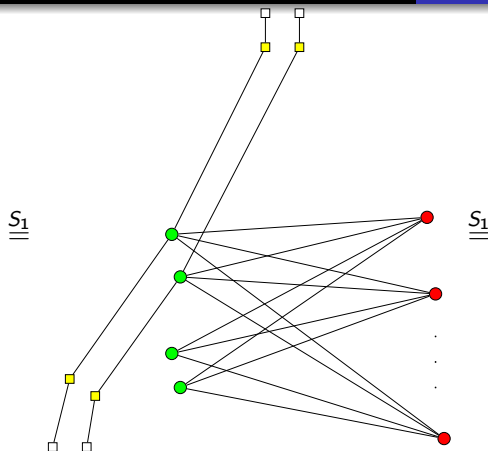
$H, S_1$



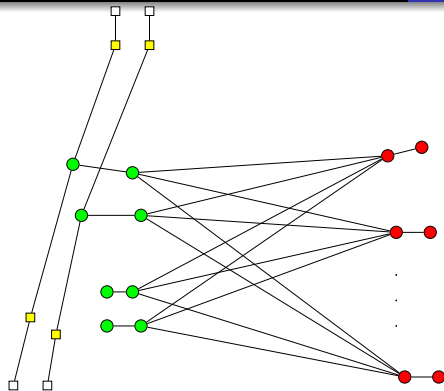


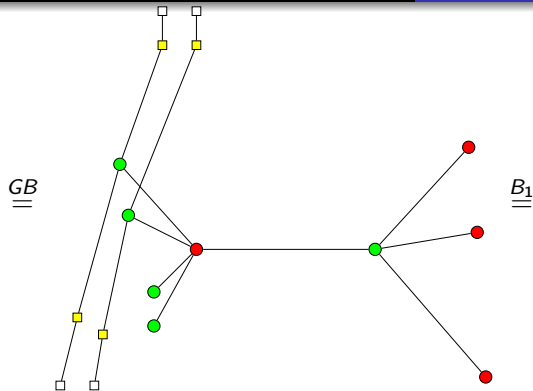


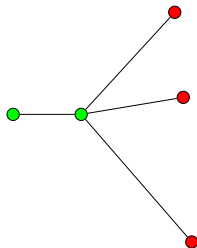
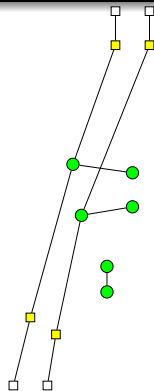


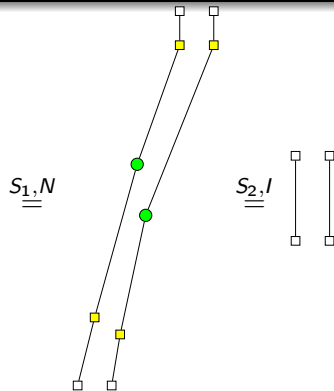








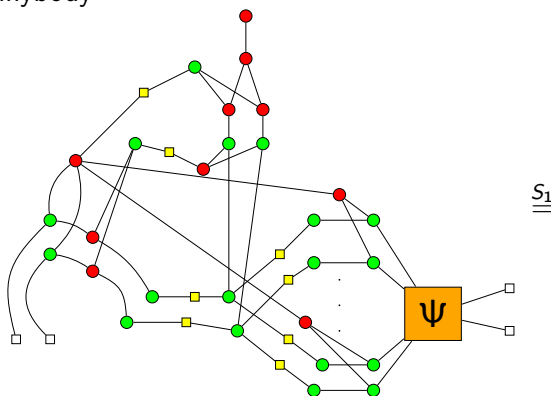


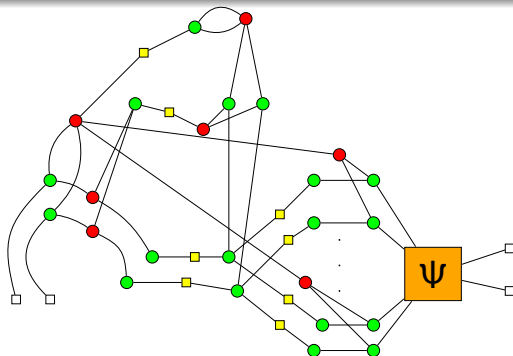


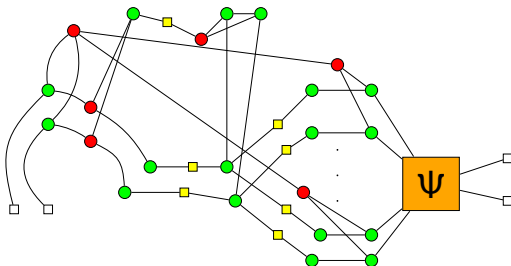
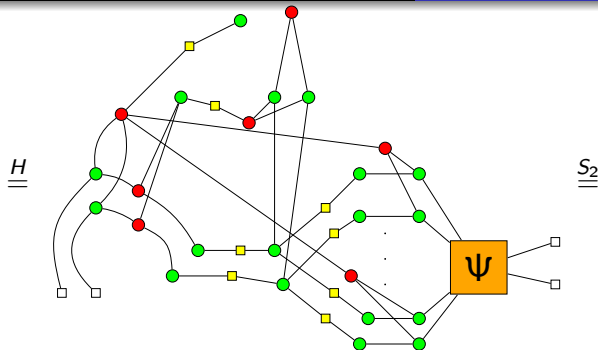
# Secret inaccessibility

There are two cases to consider for proving secret inaccessibility – when player 1 is not collaborating or when some other player is not collaborating. We will only consider the first case.

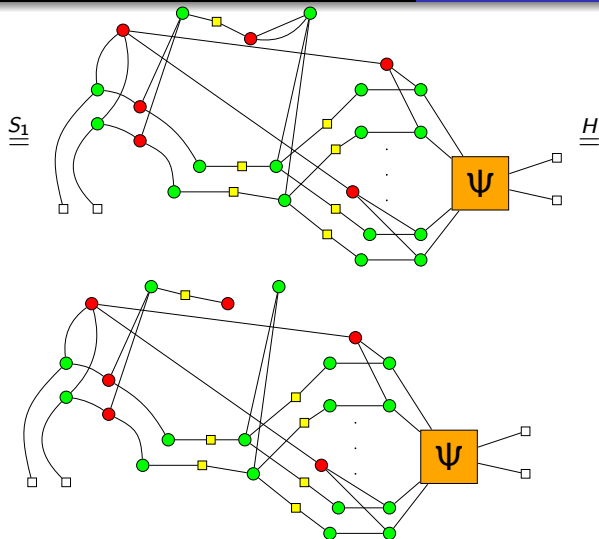
First case - player 1 is not collaborating. Let's see what happens when he measures his qubit, but does not share the result with anybody

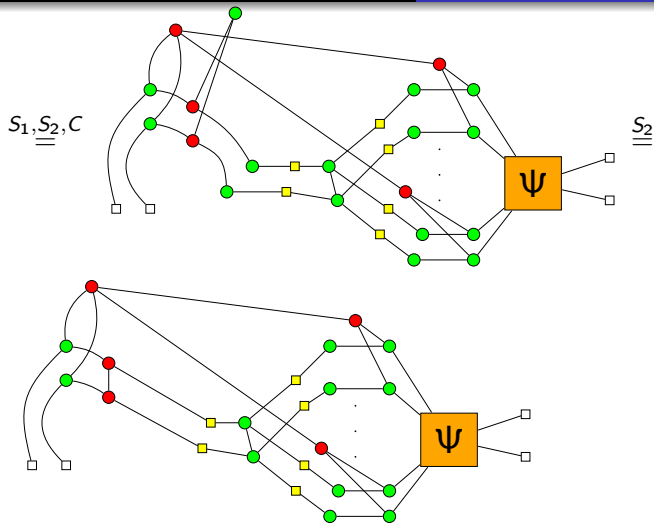


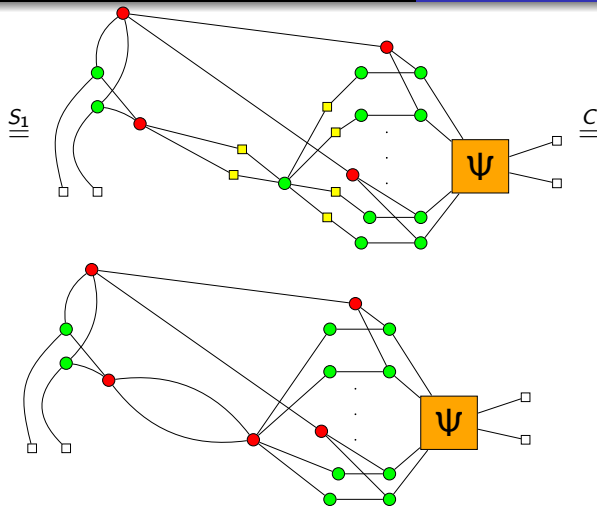


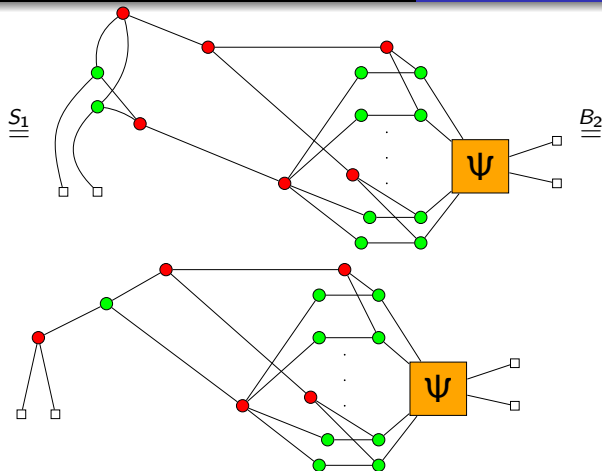










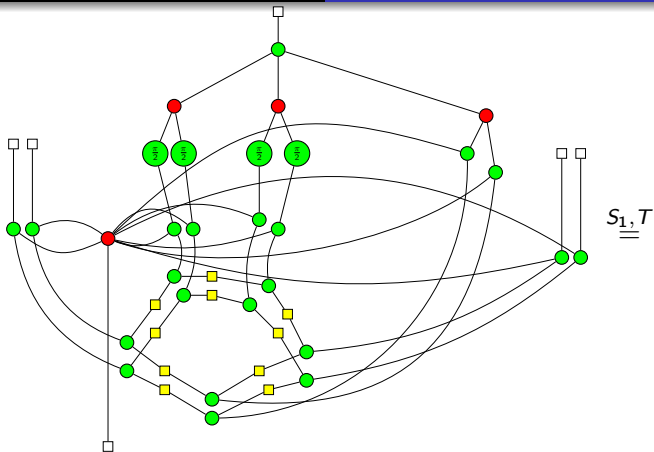


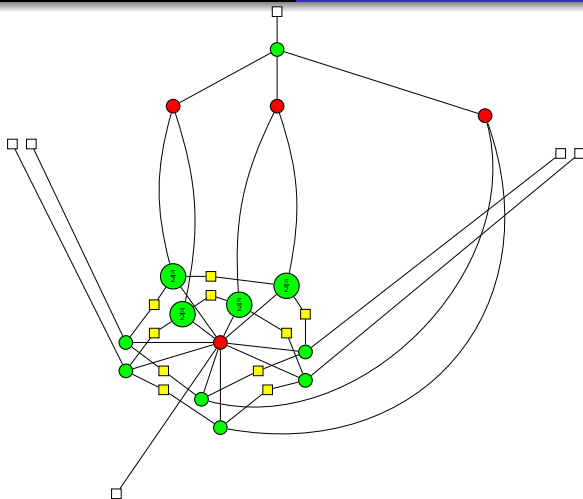
# Secret inaccessibility

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 [5]. By using similar arguments to the HBB QQ protocol, for a good choice of  $\Psi$ , we can show how these two states are teleported.

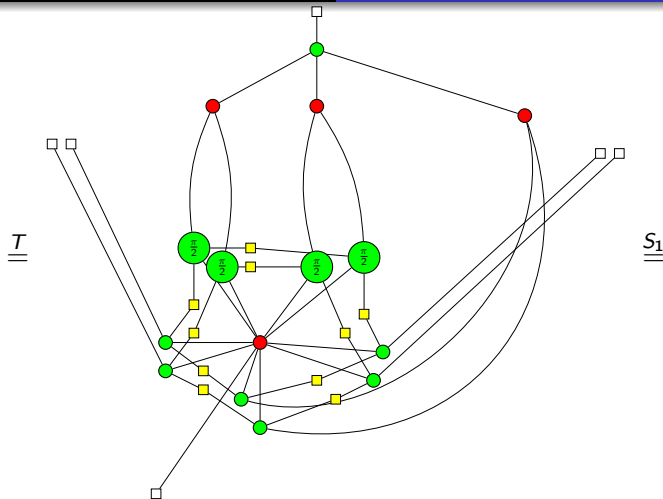
# Long derivations

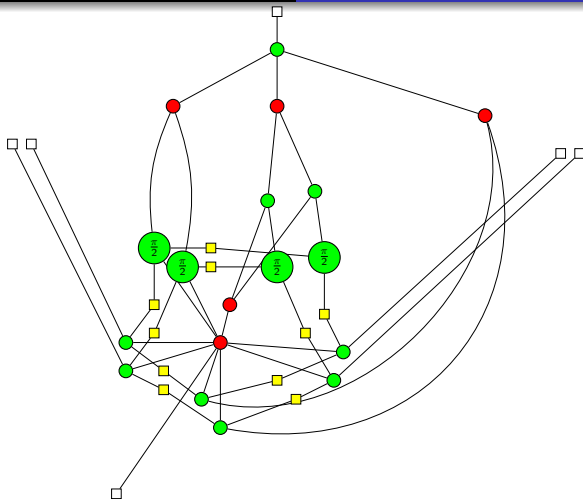
There are even longer derivations. Consider *one* case of the CC(3,5) protocol

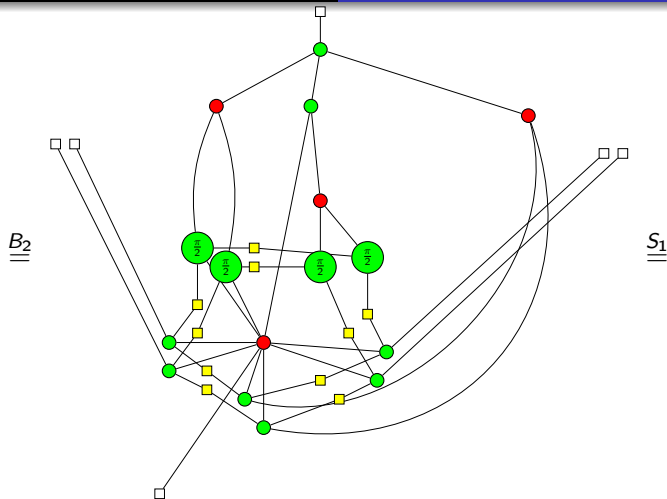


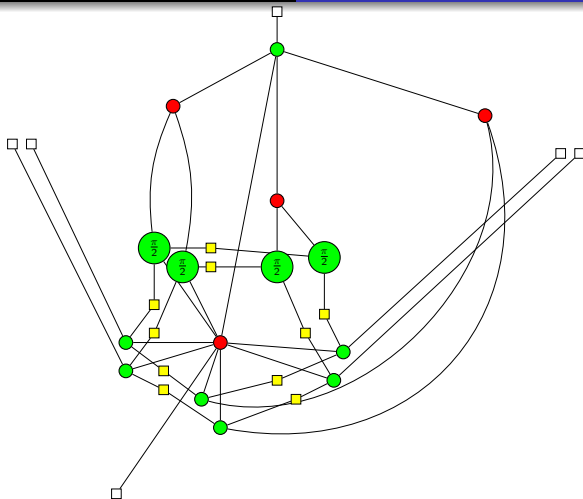


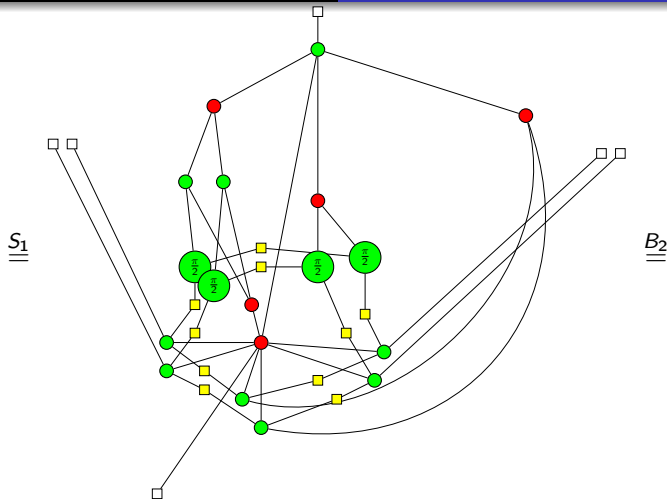


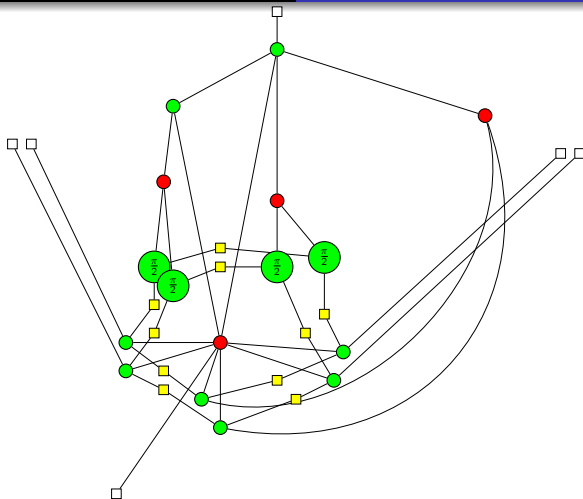


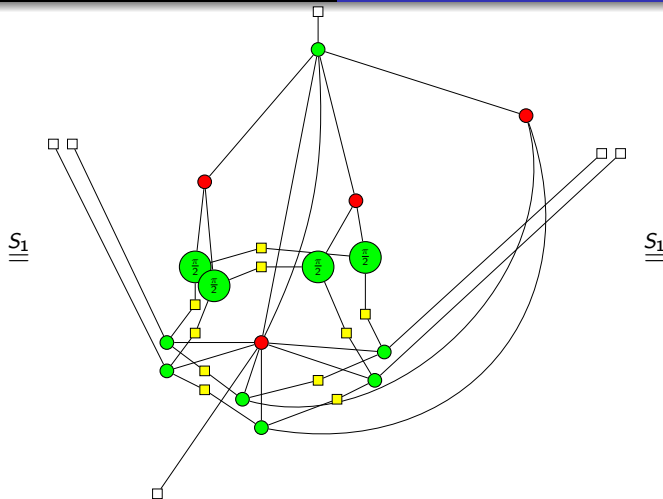


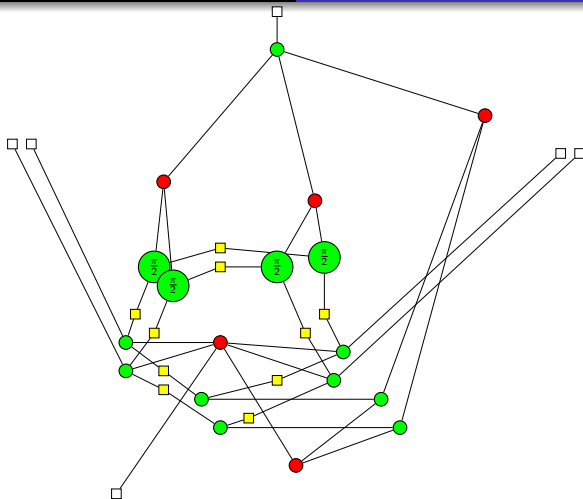




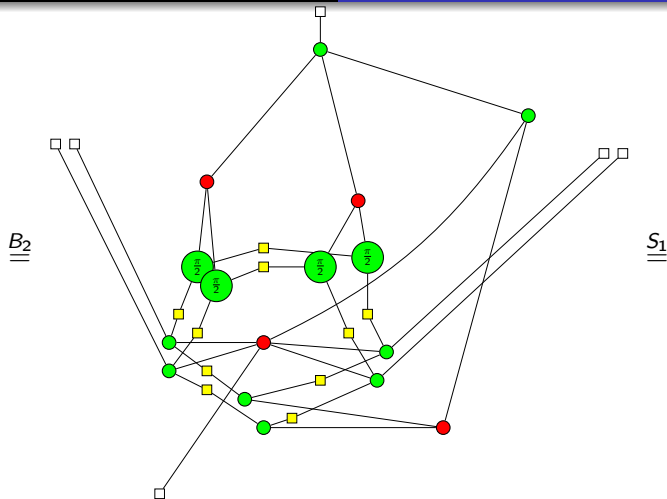


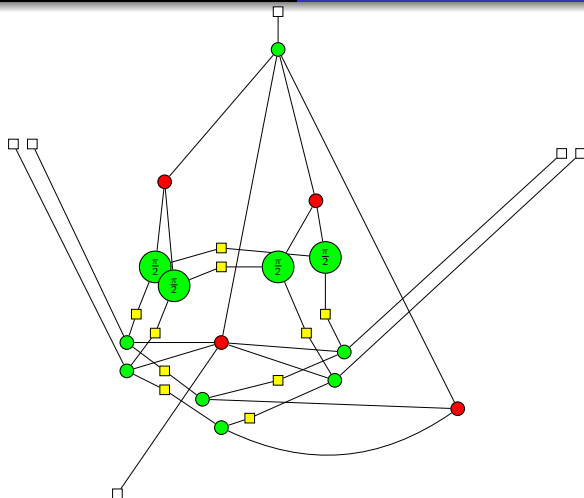


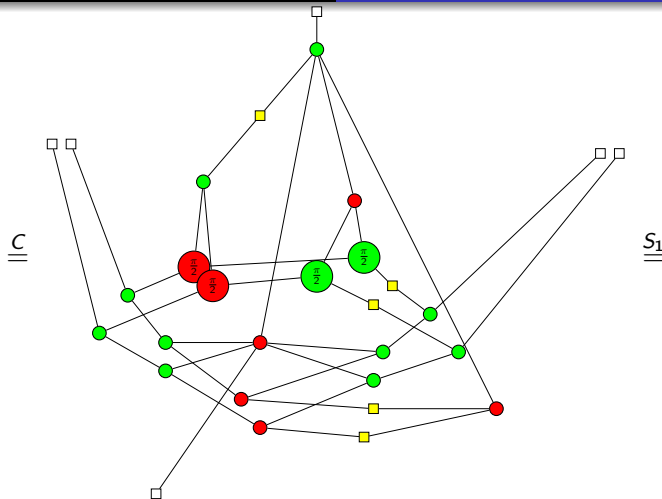


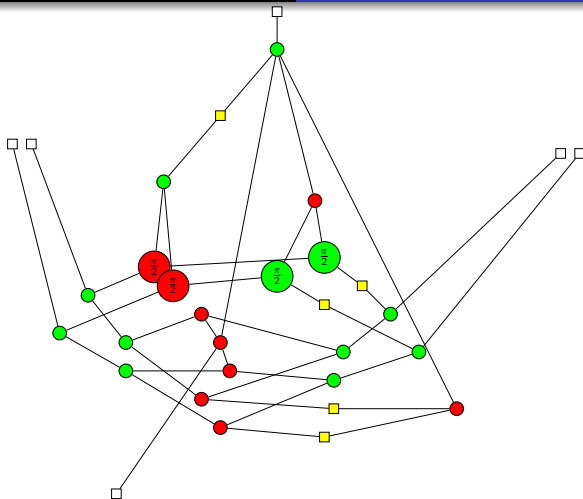


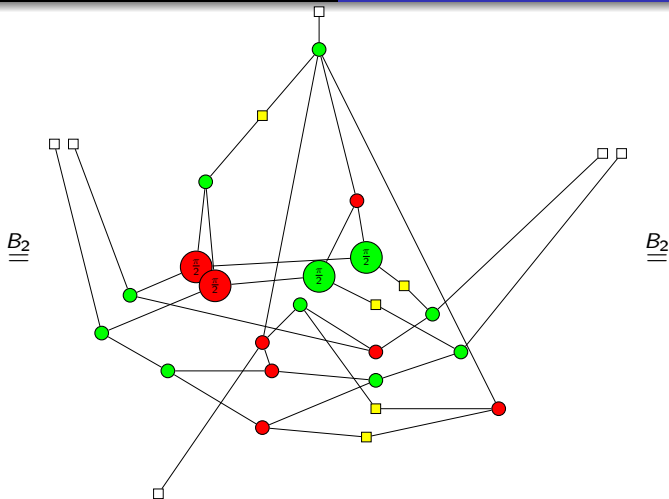


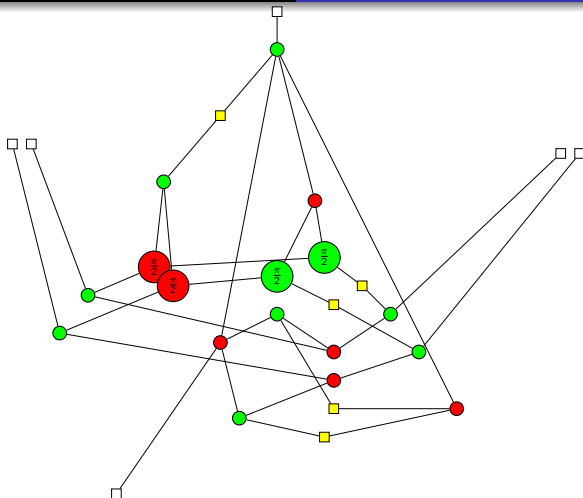


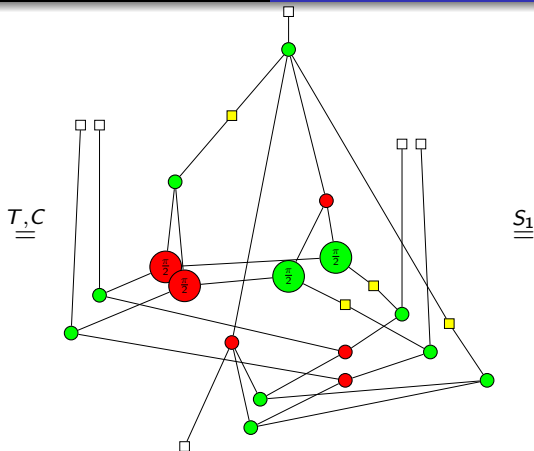


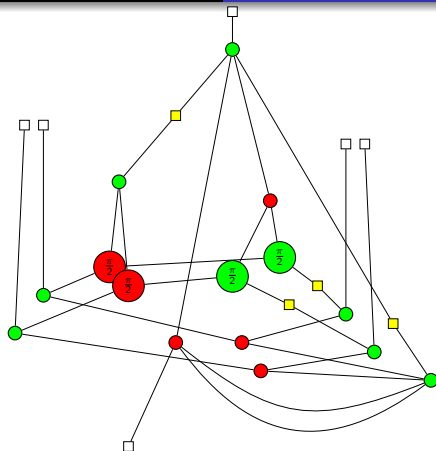




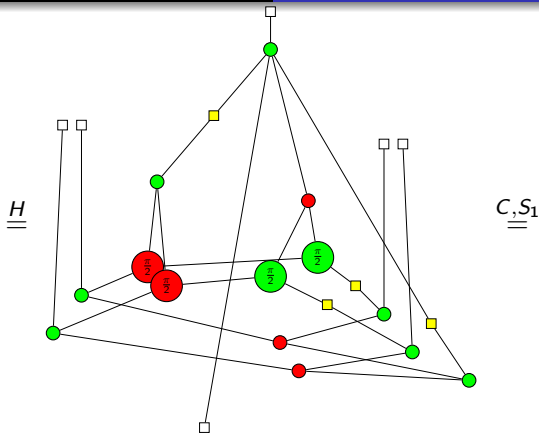


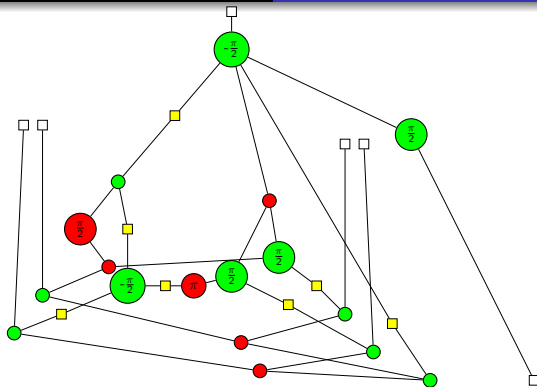


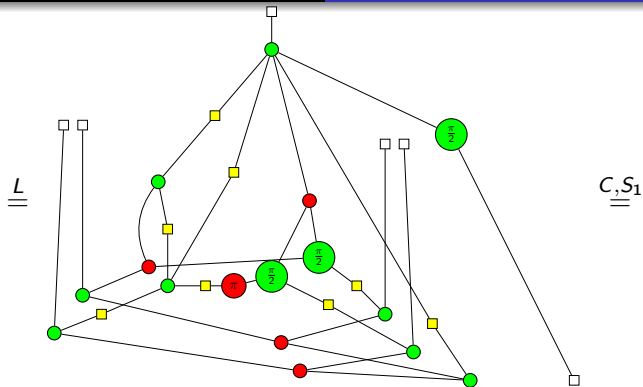


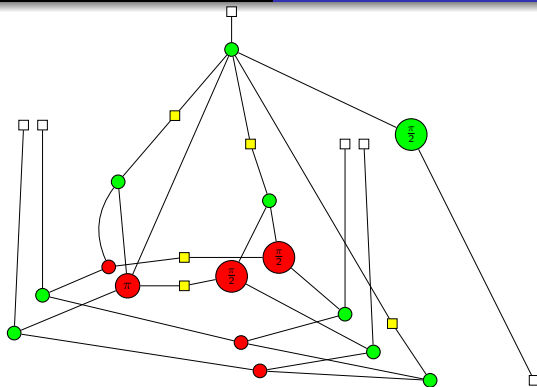


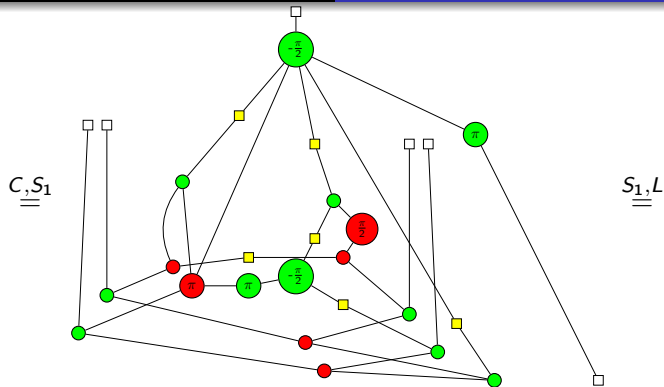


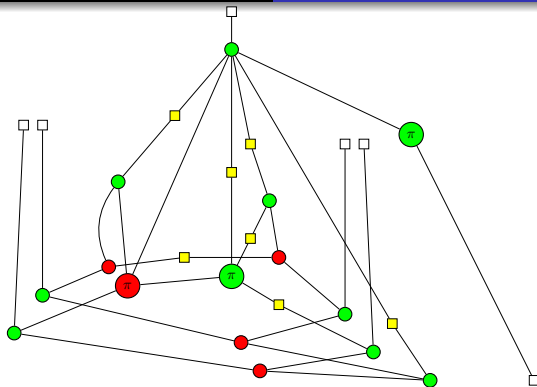


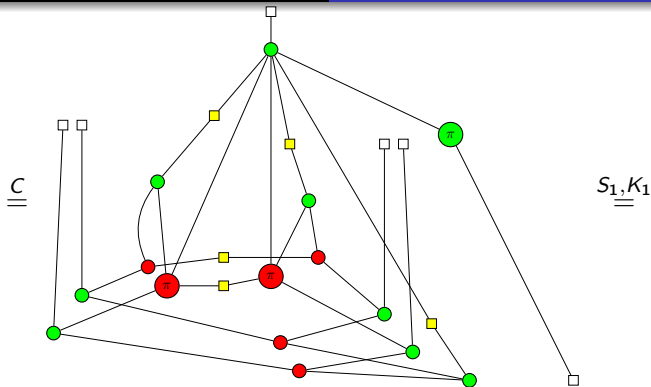


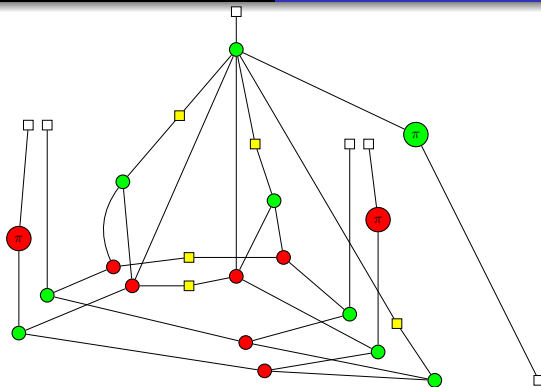




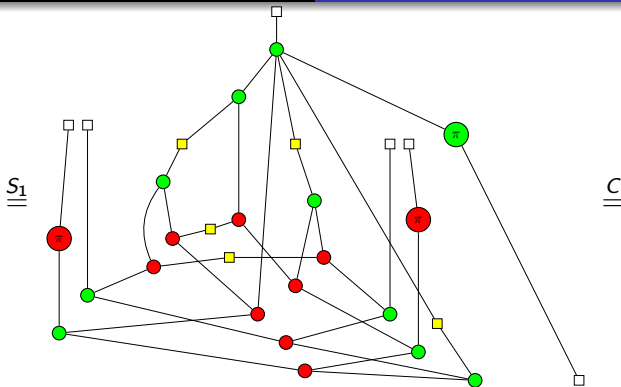


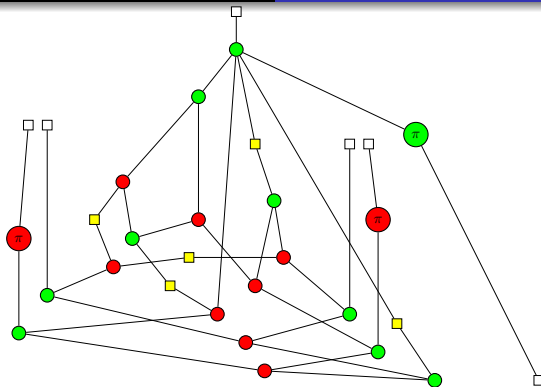


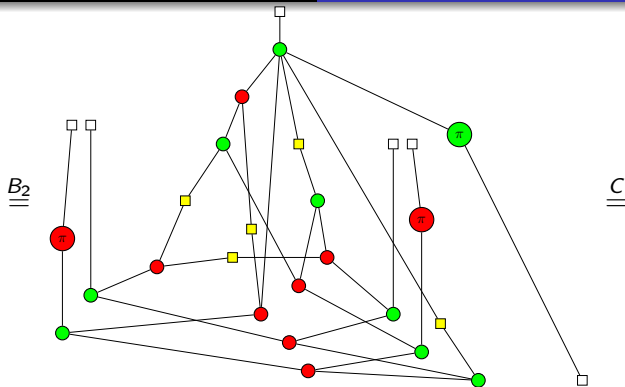


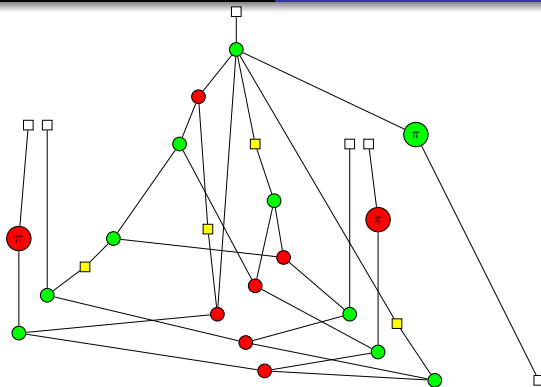


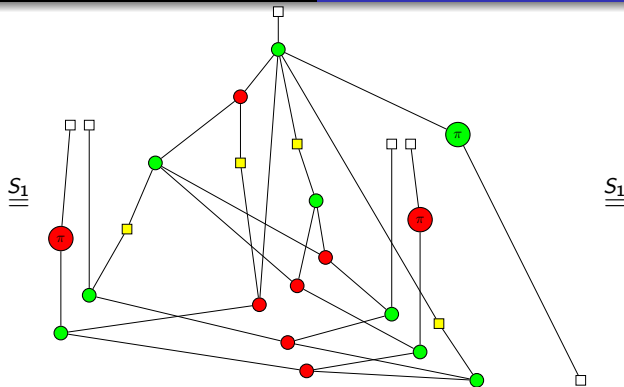


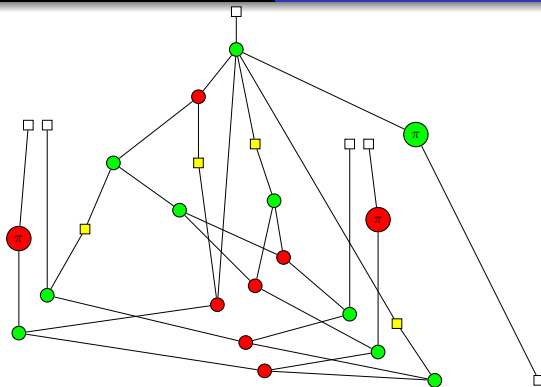


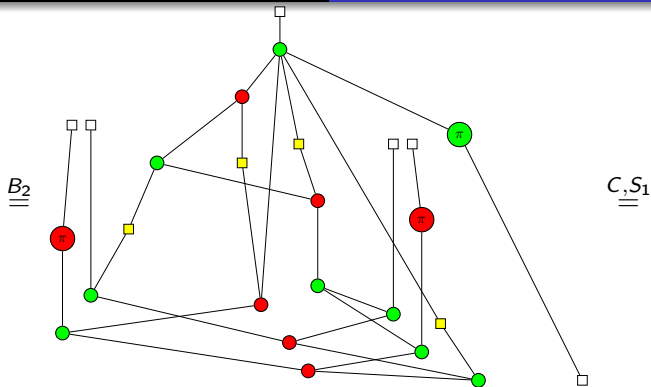


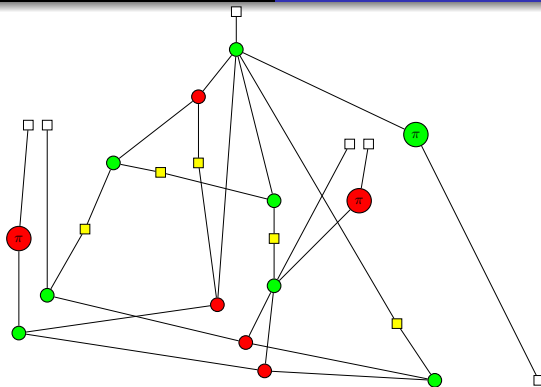




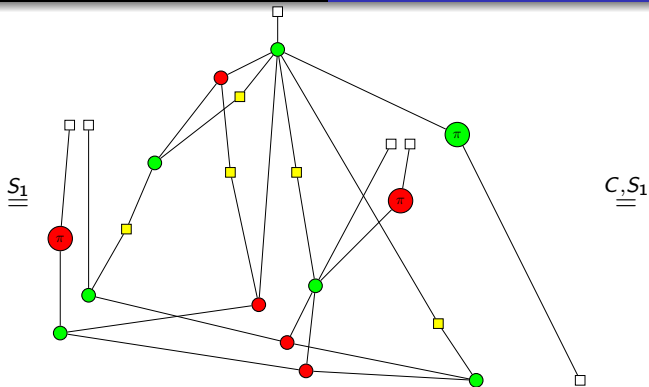


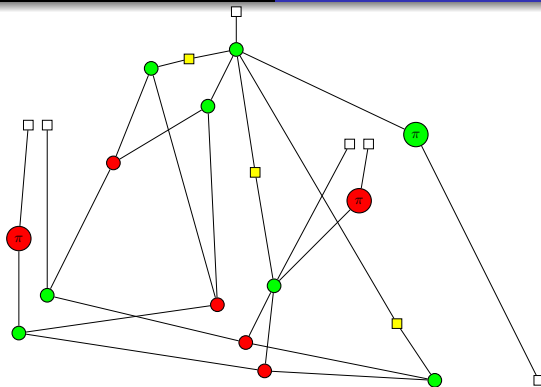


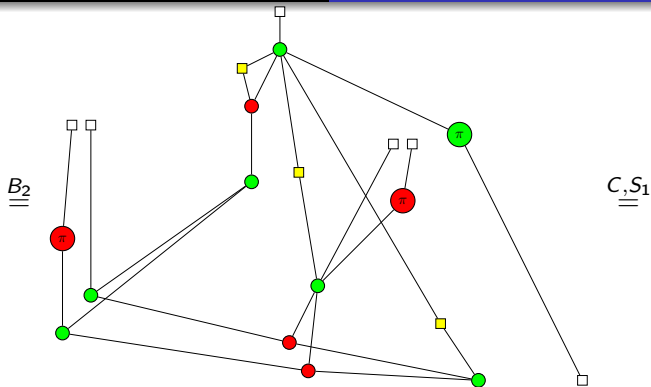


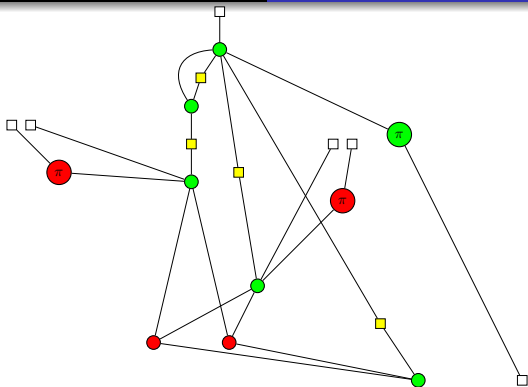


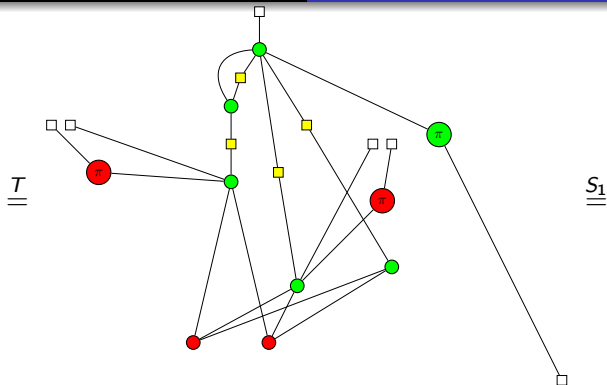


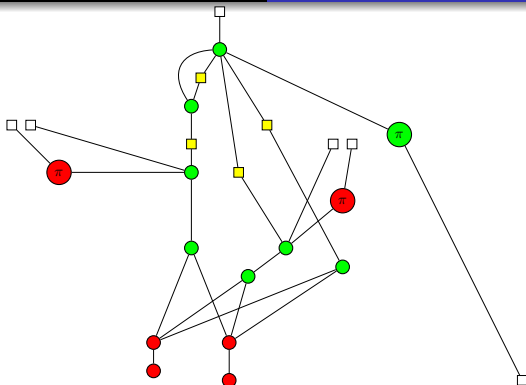


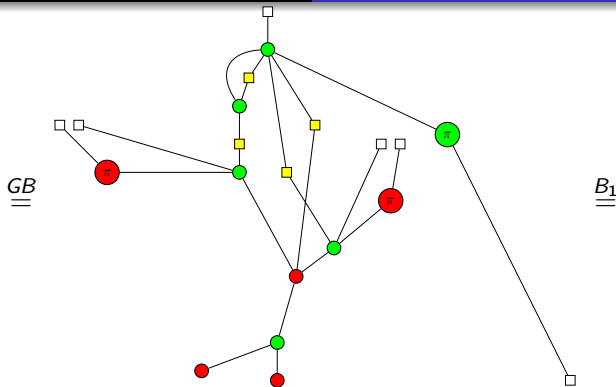


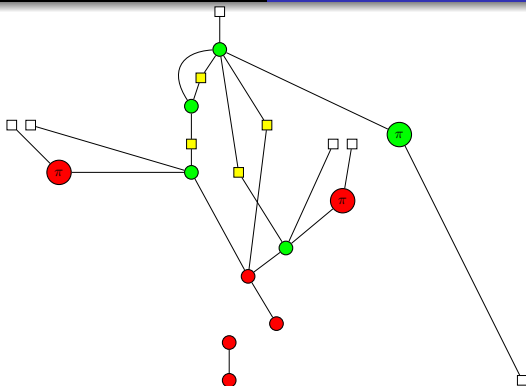




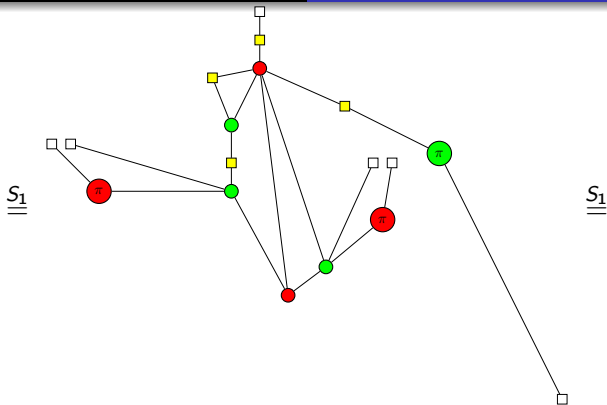


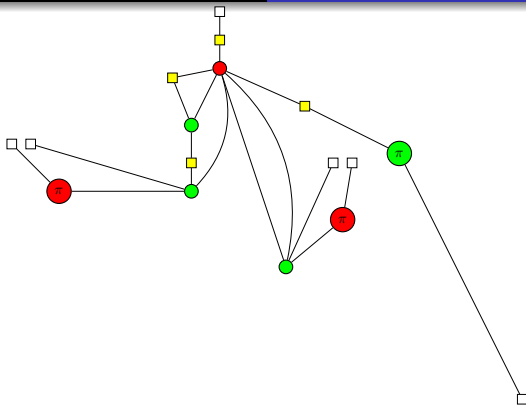


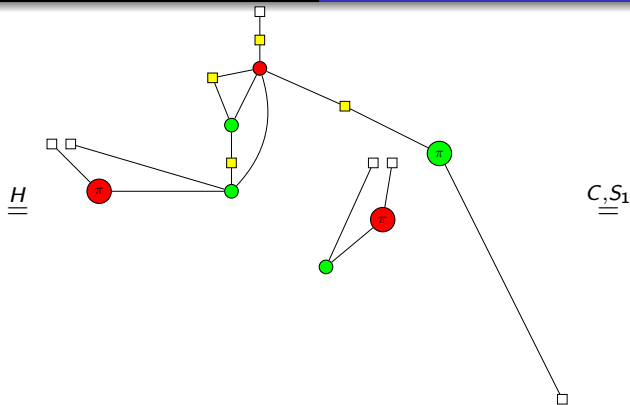


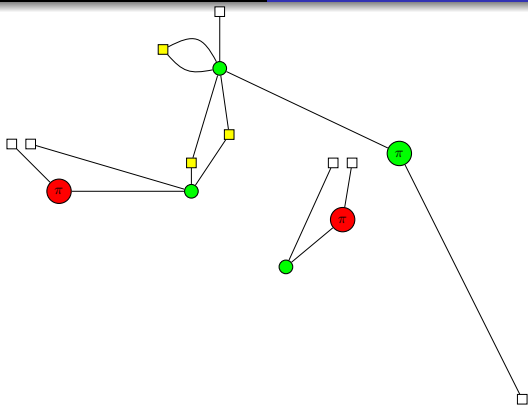


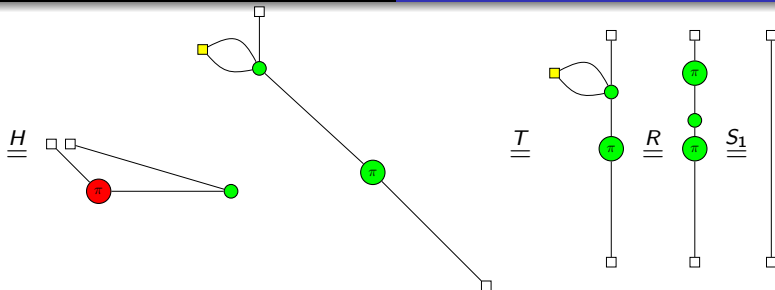






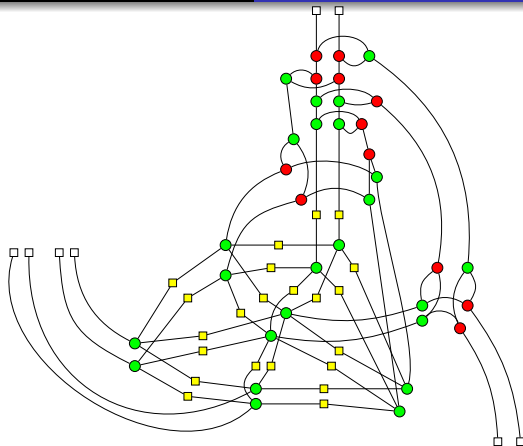






# I couldn't do one protocol

I couldn't do the QQ(3,5) protocol, because the diagram is too large and complicated. However, we do know that it is possible to rewrite it to the identity. Here's how it looks (first case) :



# Conclusions

- need software support (Quantomatic) for larger diagrams
  - !-boxes necessary to express some of the protocols in Quantomatic
  - possible extension necessary if work to be done using  $C_n$  and other recursive graph states within Quantomatic
- protocols need to be expressed very formally and precisely (even tiny details must be considered)
- proving security does not seem to be straightforward
- rigorous approach identified errors in QQ(n,n) approach easily





A. Shamir.

How to share a secret.

*Communications of the ACM*, 26:313–317, 1979.



B. Coecke and R. Duncan.

Interacting quantum observables: categorical algebra and diagrammatics.

*New Journal of Physics*, 13(043016), 2011.



G. R. Blakley.

Safeguarding cryptographic keys.

In *AFIPS National Computer Conference*, pages 313–317, 1979.



M. Hillery, V. Buzek, and A. Berthiaume.

Quantum Secret Sharing.

*Physical Review A*, 59:1829–1834, 1999.



B. C. Sanders and D. Markham.

Erratum: Graph states for quantum secret sharing.

*Physical Review A*, 78(042309), 2008.



B. C. Sanders and D. Markham.

Graph States for Quantum Secret Sharing.

*Physical Review A*, 78(042309), 2008.



L. Xiao, G.L. Long, F-G. Deng, and J-W Pan.

*Physical Review A*, 69(052307), 2004.