Quantum Cryptography and Quantum Networks

Jarn de Jong, TU Berlin

Quantum Cryptography and Quantum Networks

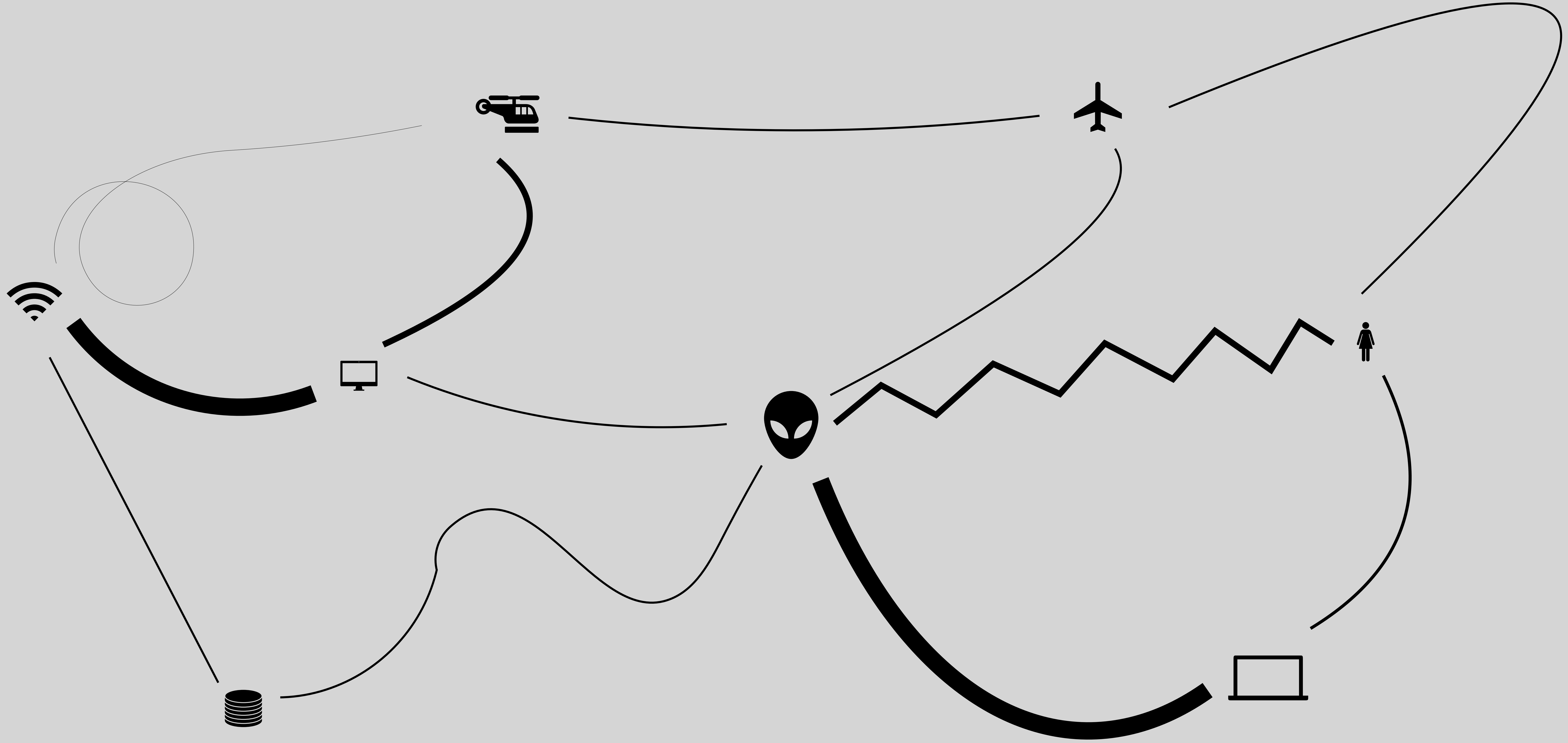
Quantum Cryptography and Quantum Networks

- QKD
- Security
- …

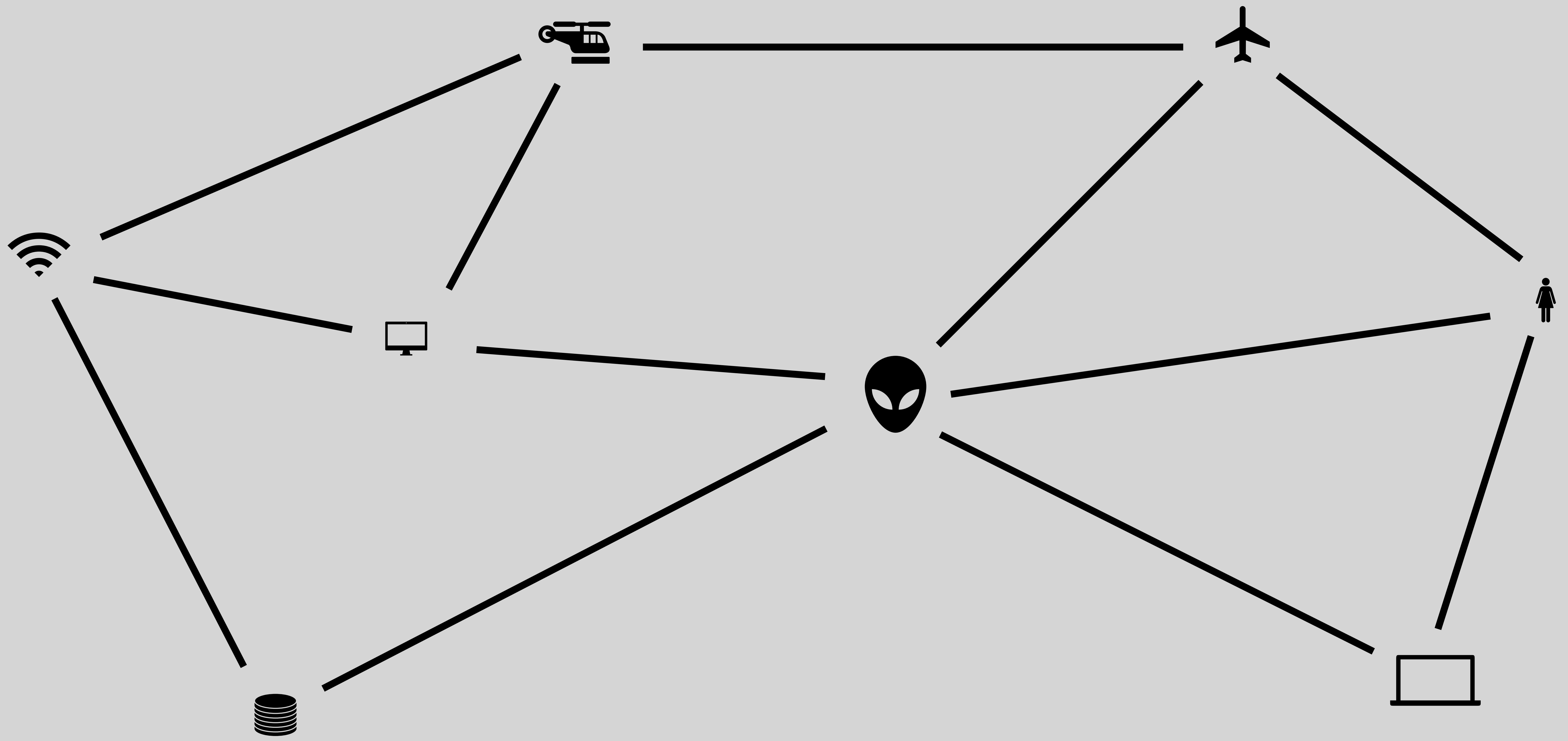
Quantum Cryptography and Quantum Networks

- QKD
- Security
- …

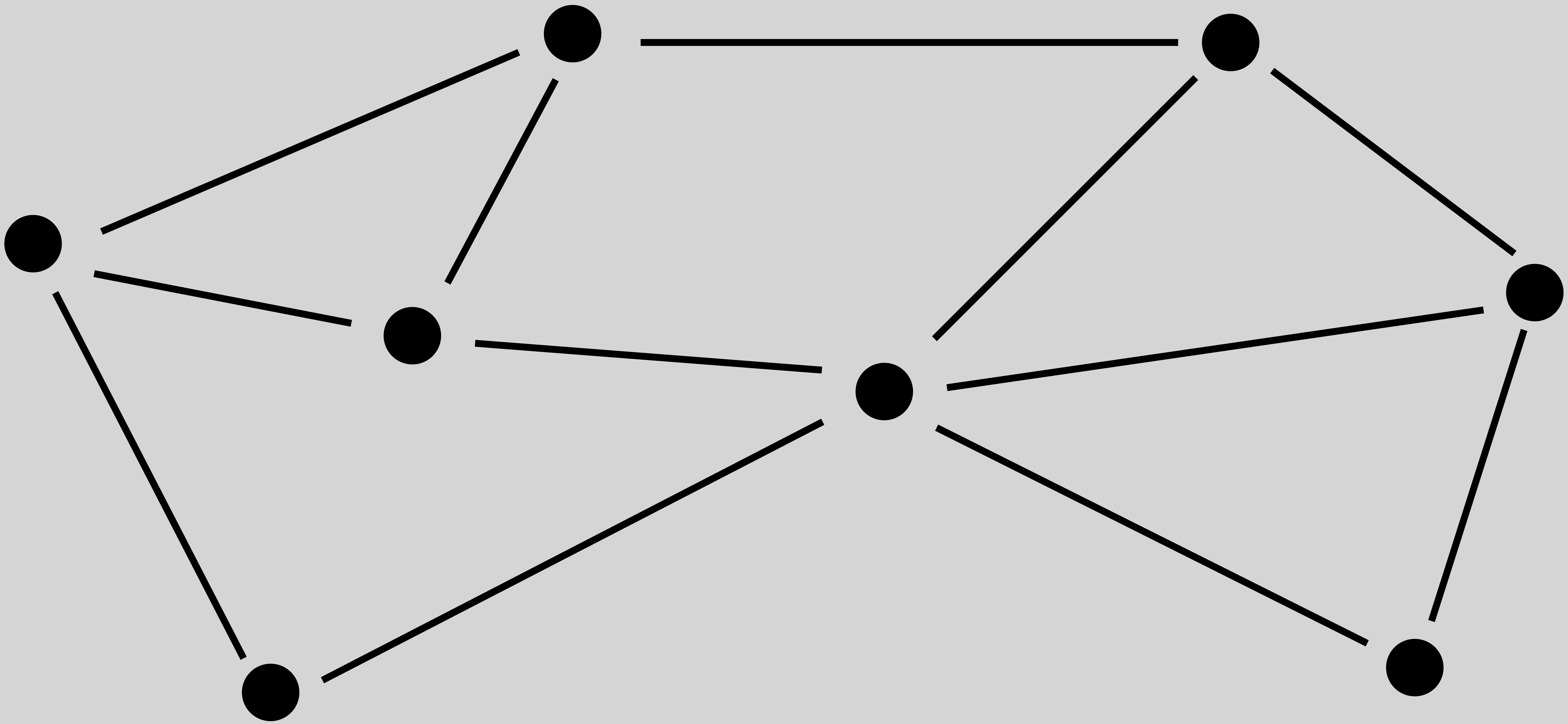
What is a network?



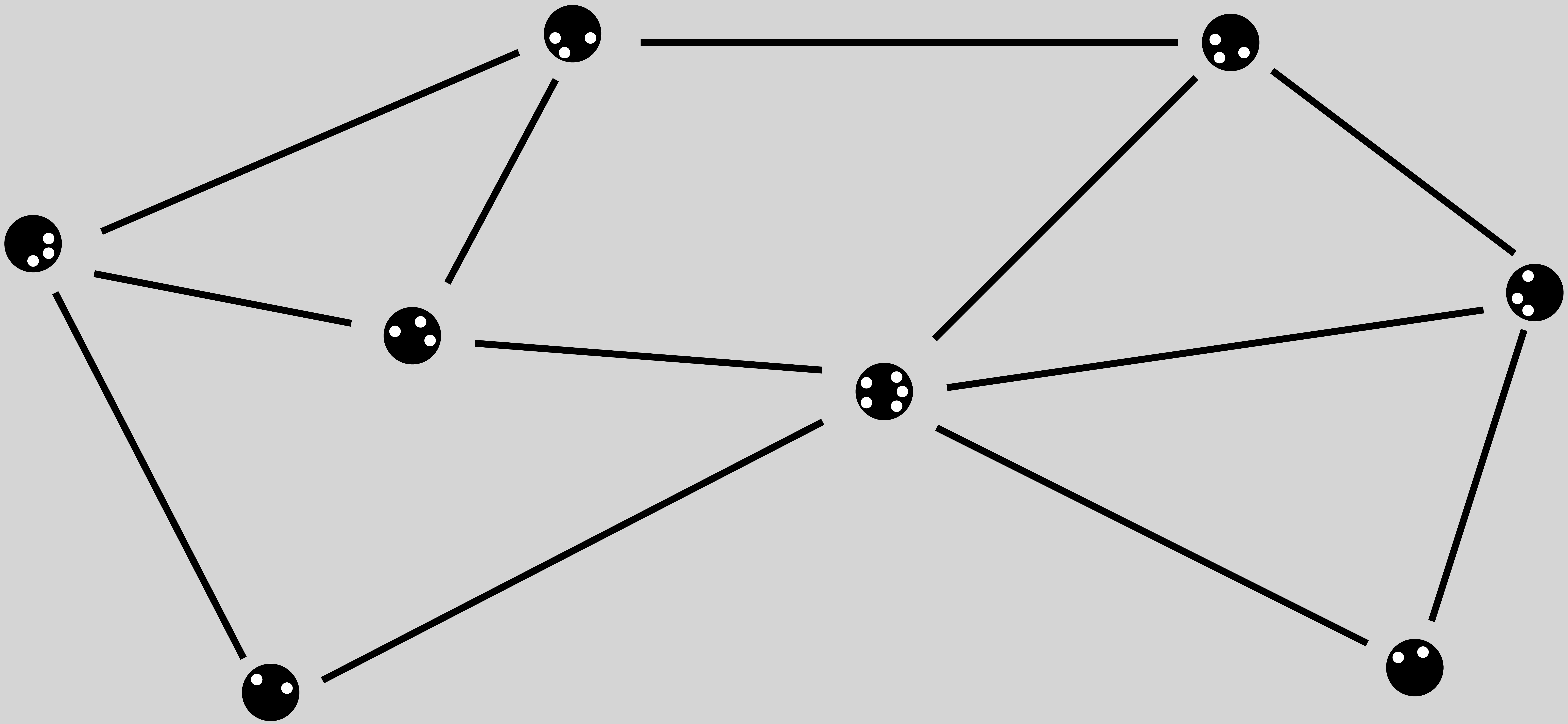
What is a network?



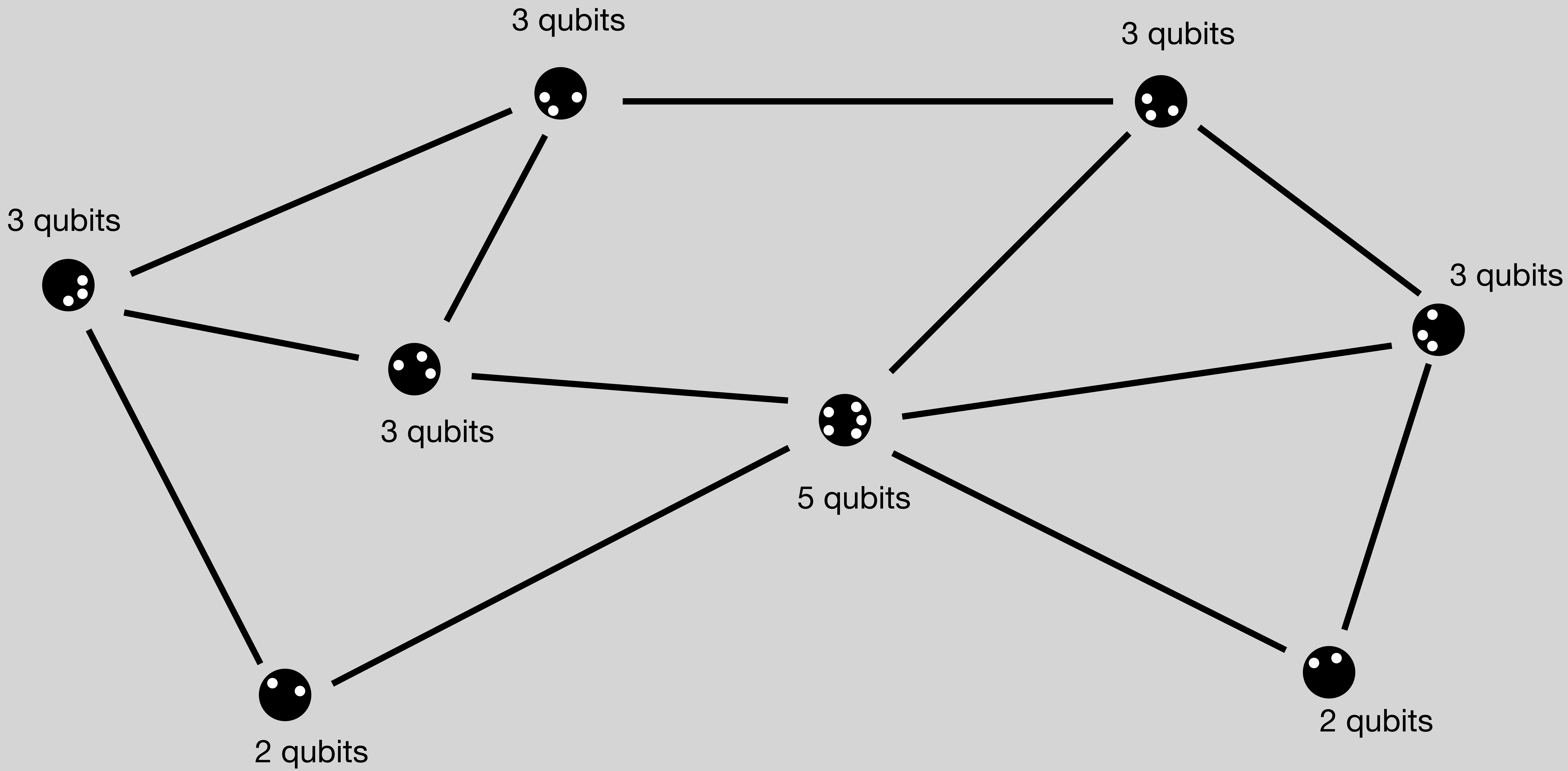
What is a network?



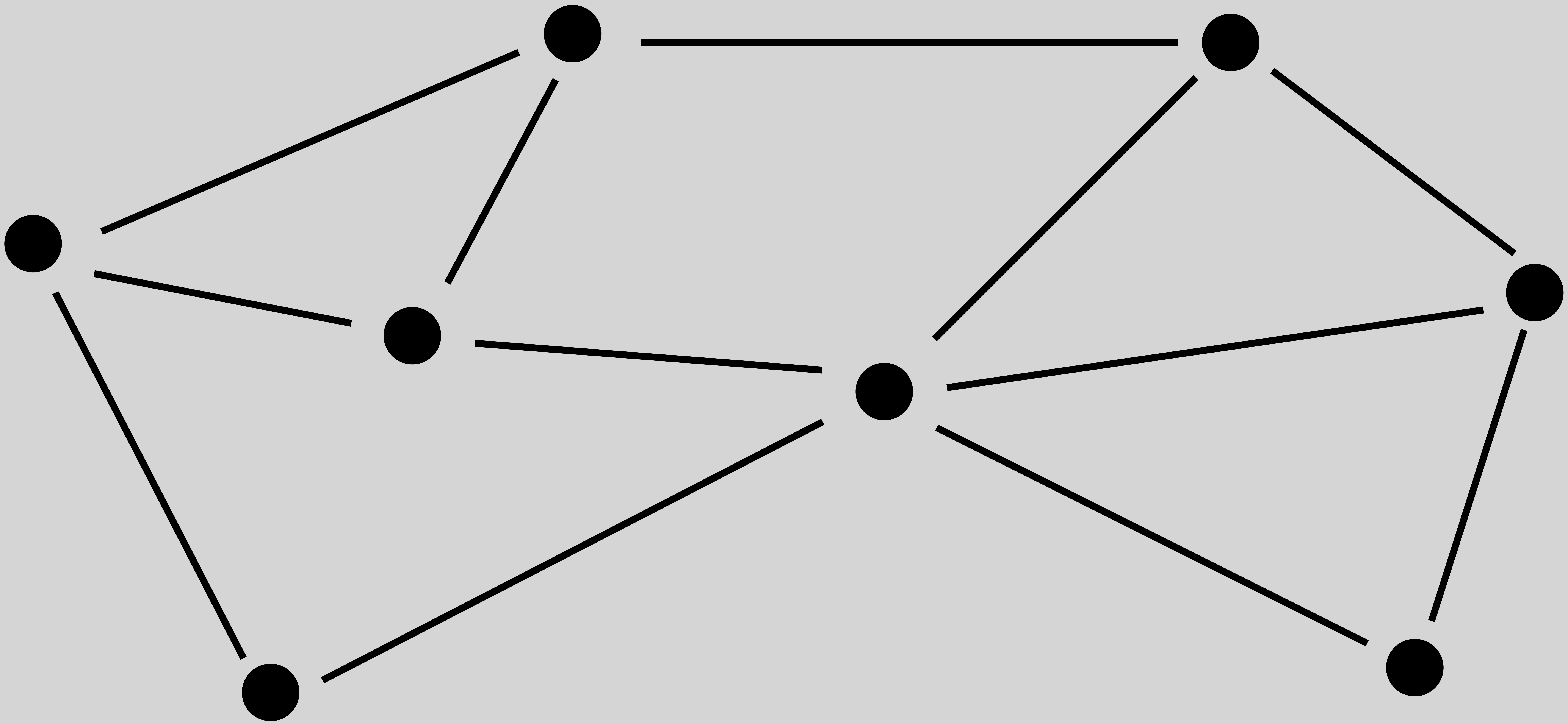
What is a network?



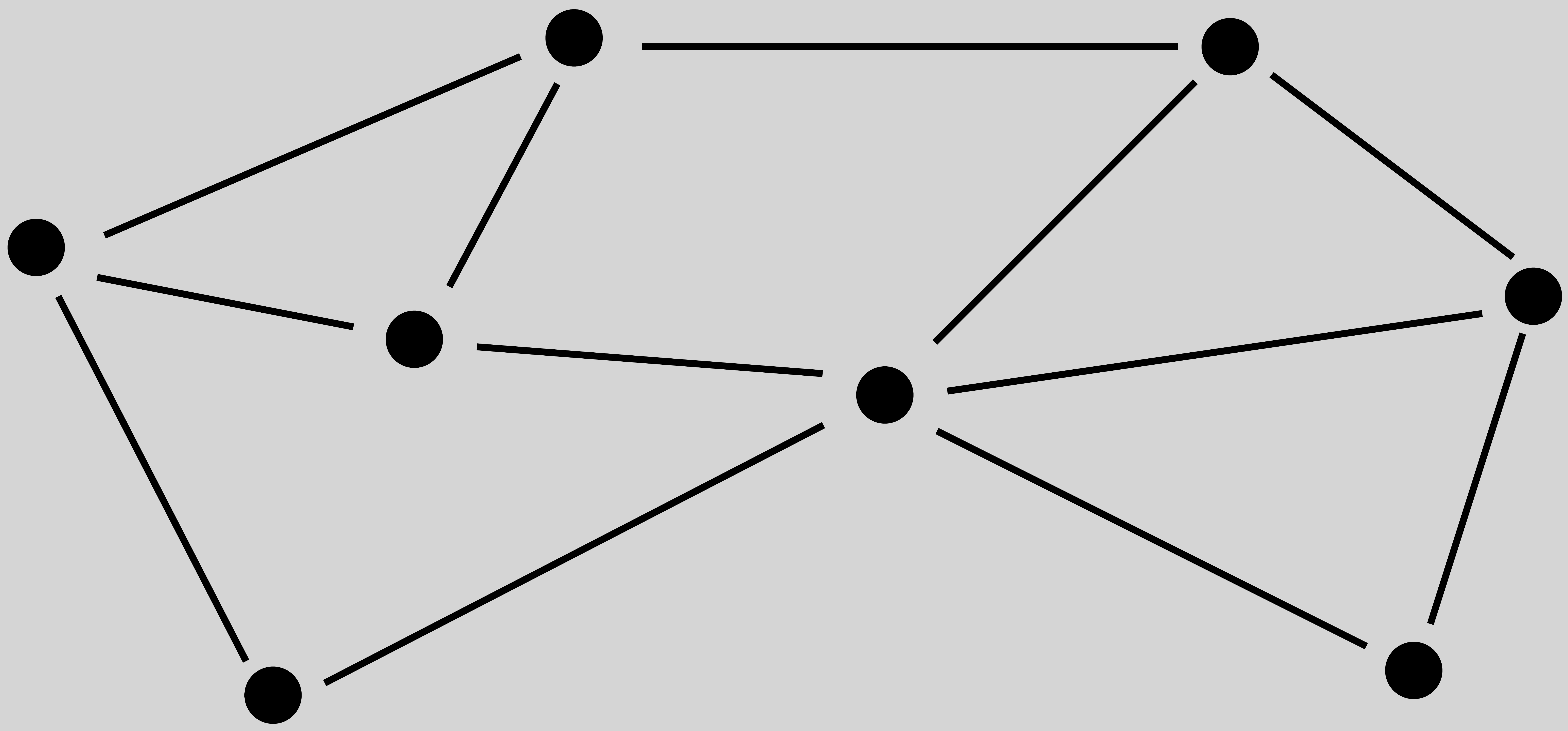
What is a network?



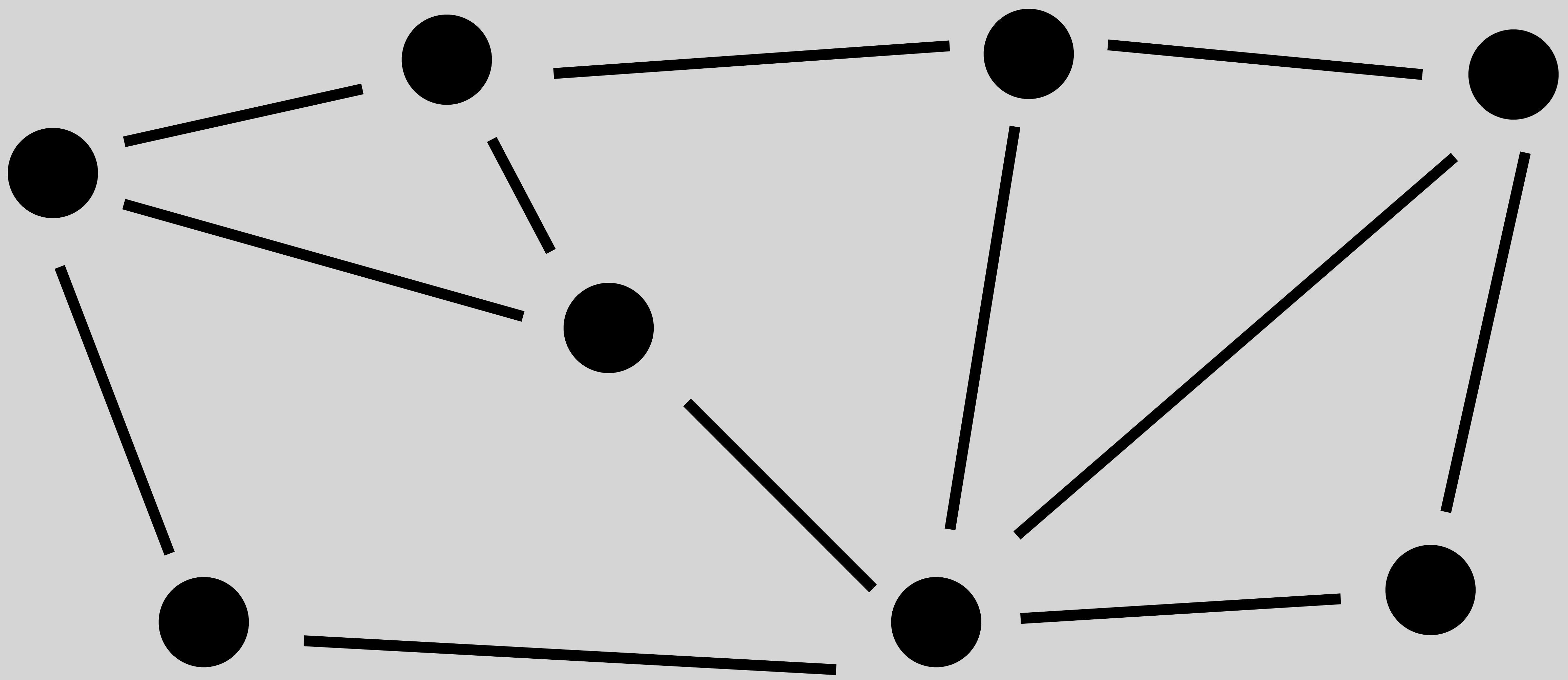
What is a network?



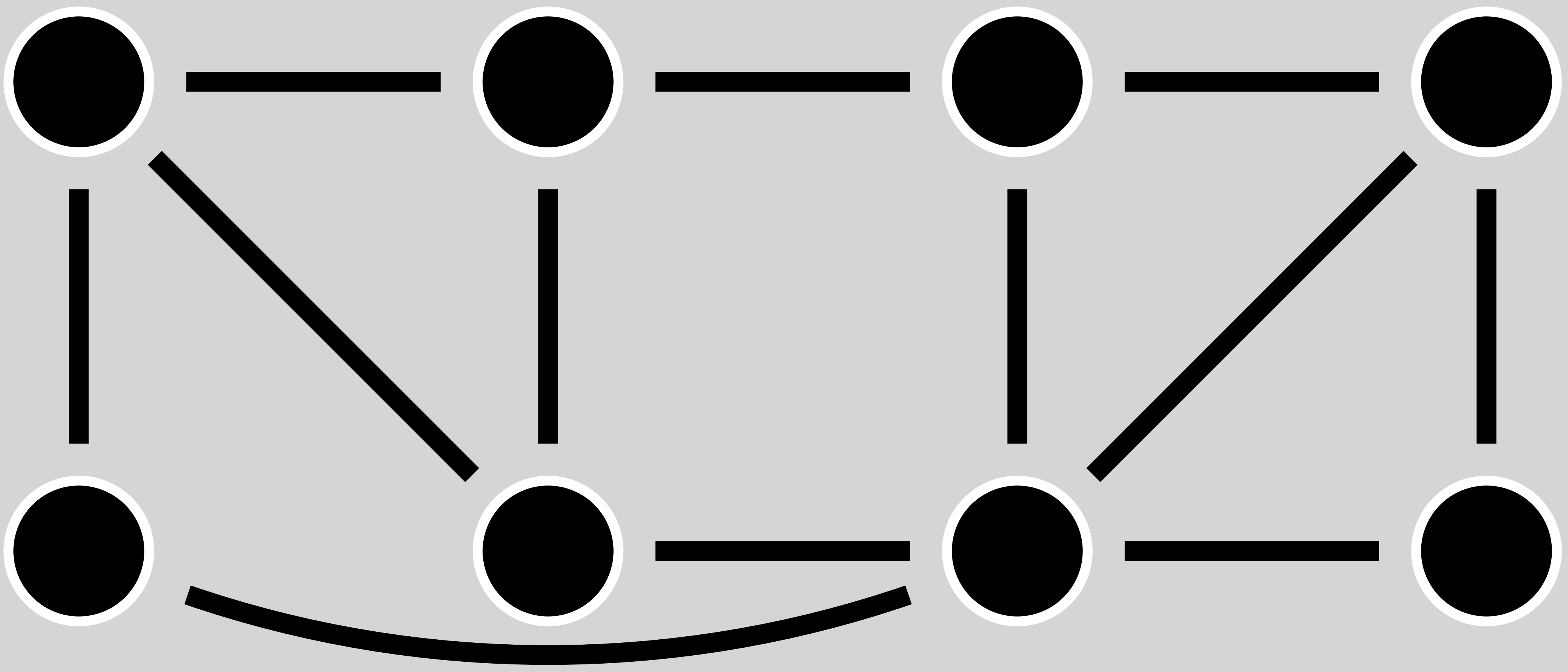
….a network is a graph



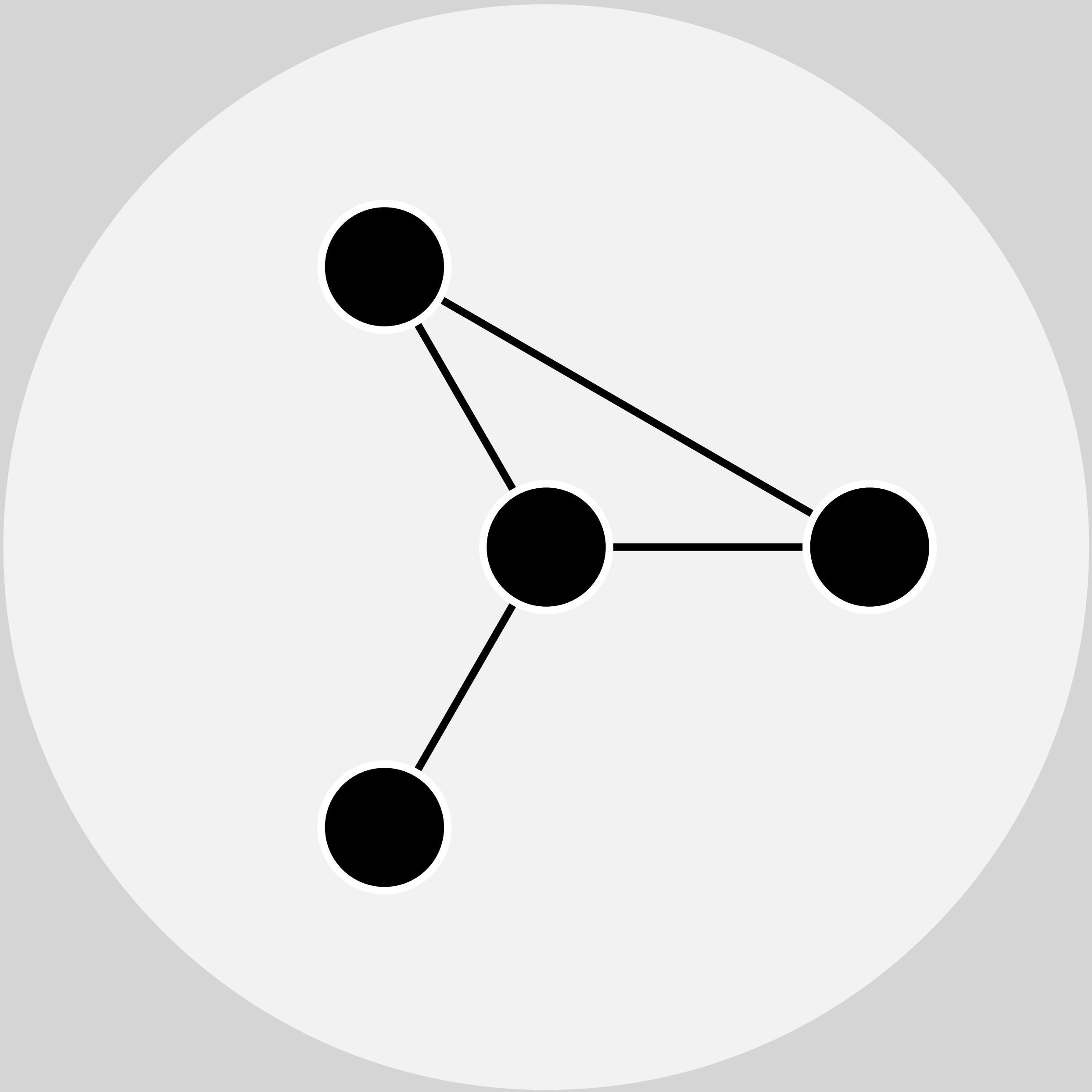
….a network is a graph

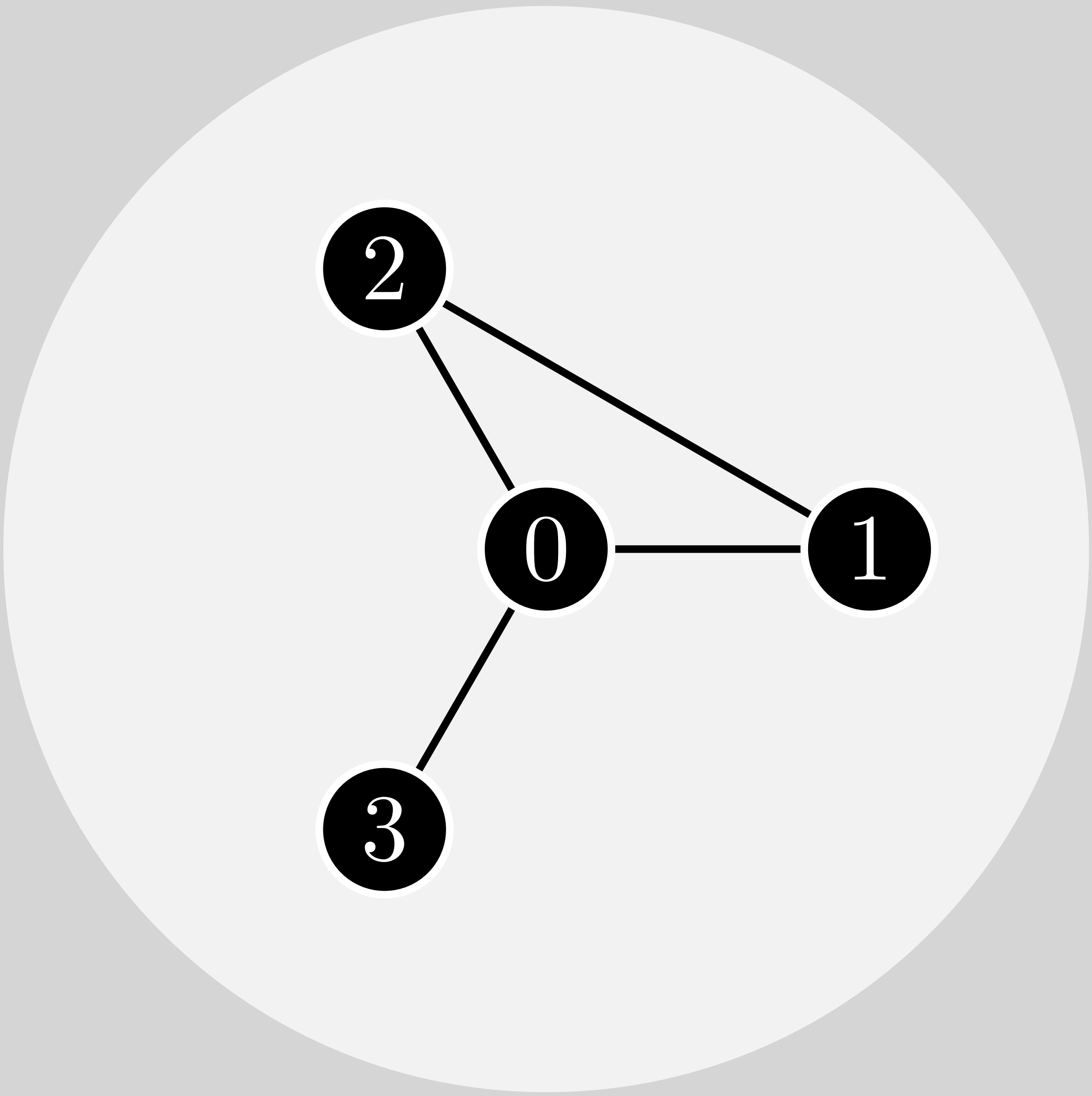


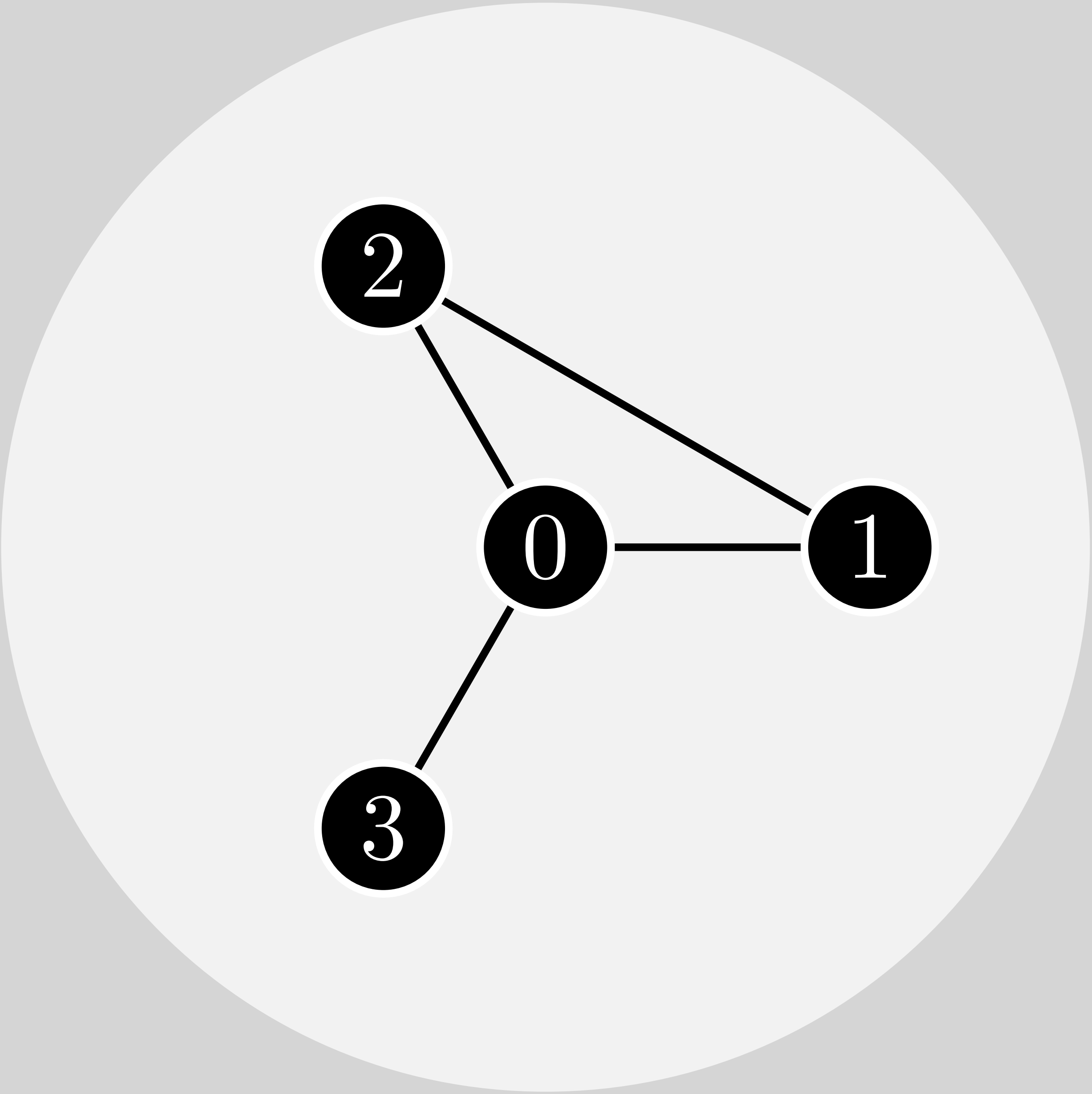
….a network is a graph

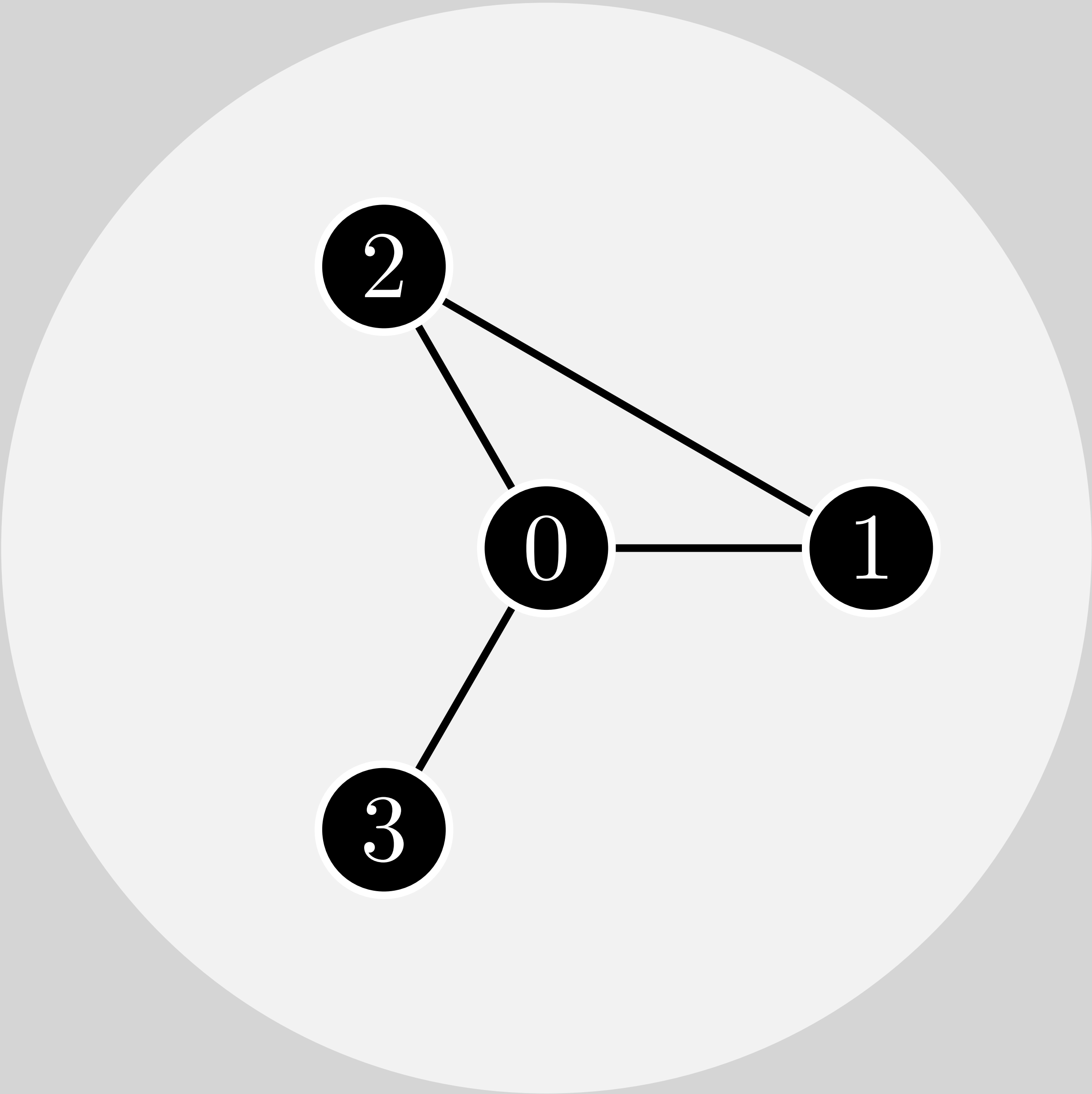


Well, what is a graph then?




2
0
1
3

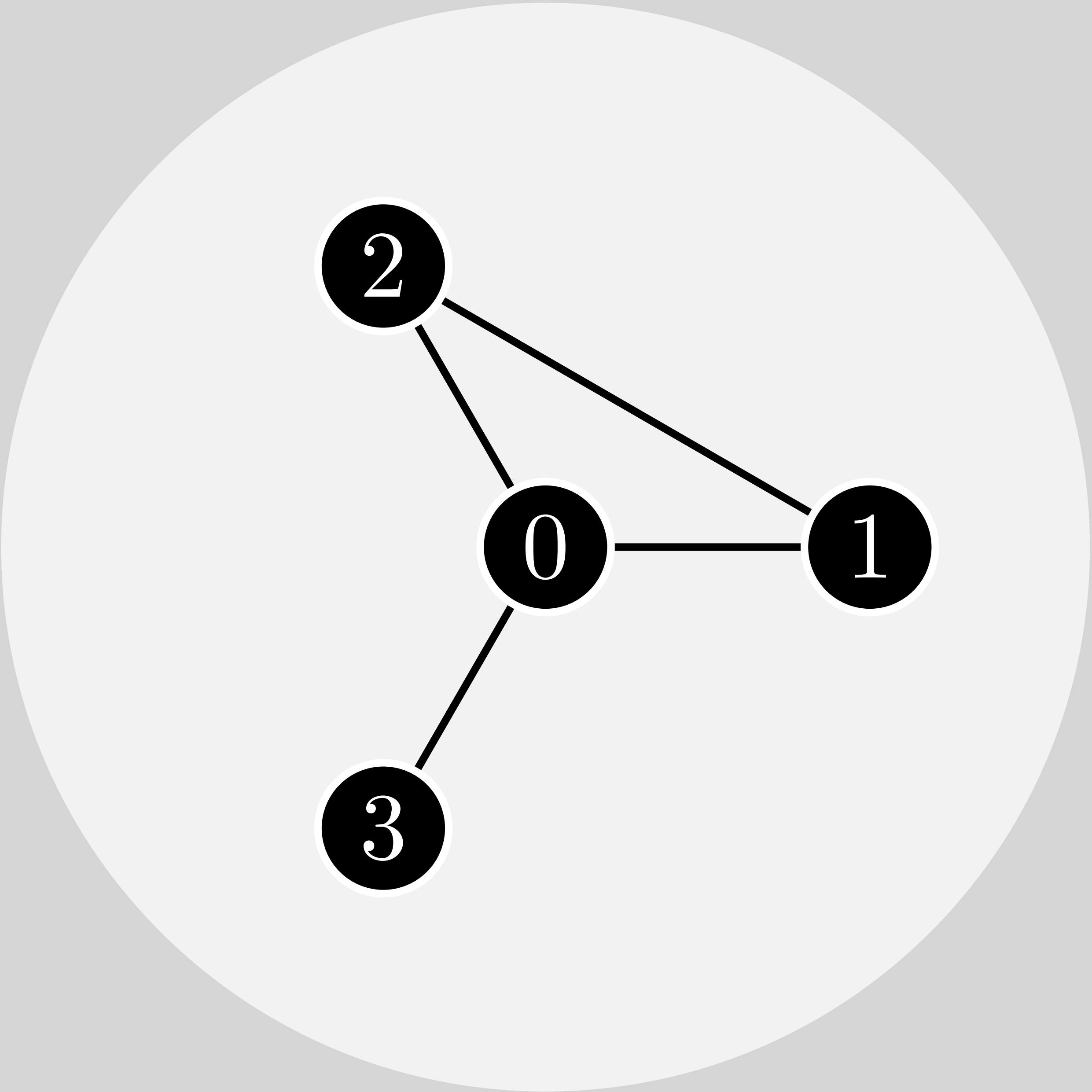

2
0
1
3



$$G = (V, E)$$

Nodes V

Edges $E \subseteq V \times V$



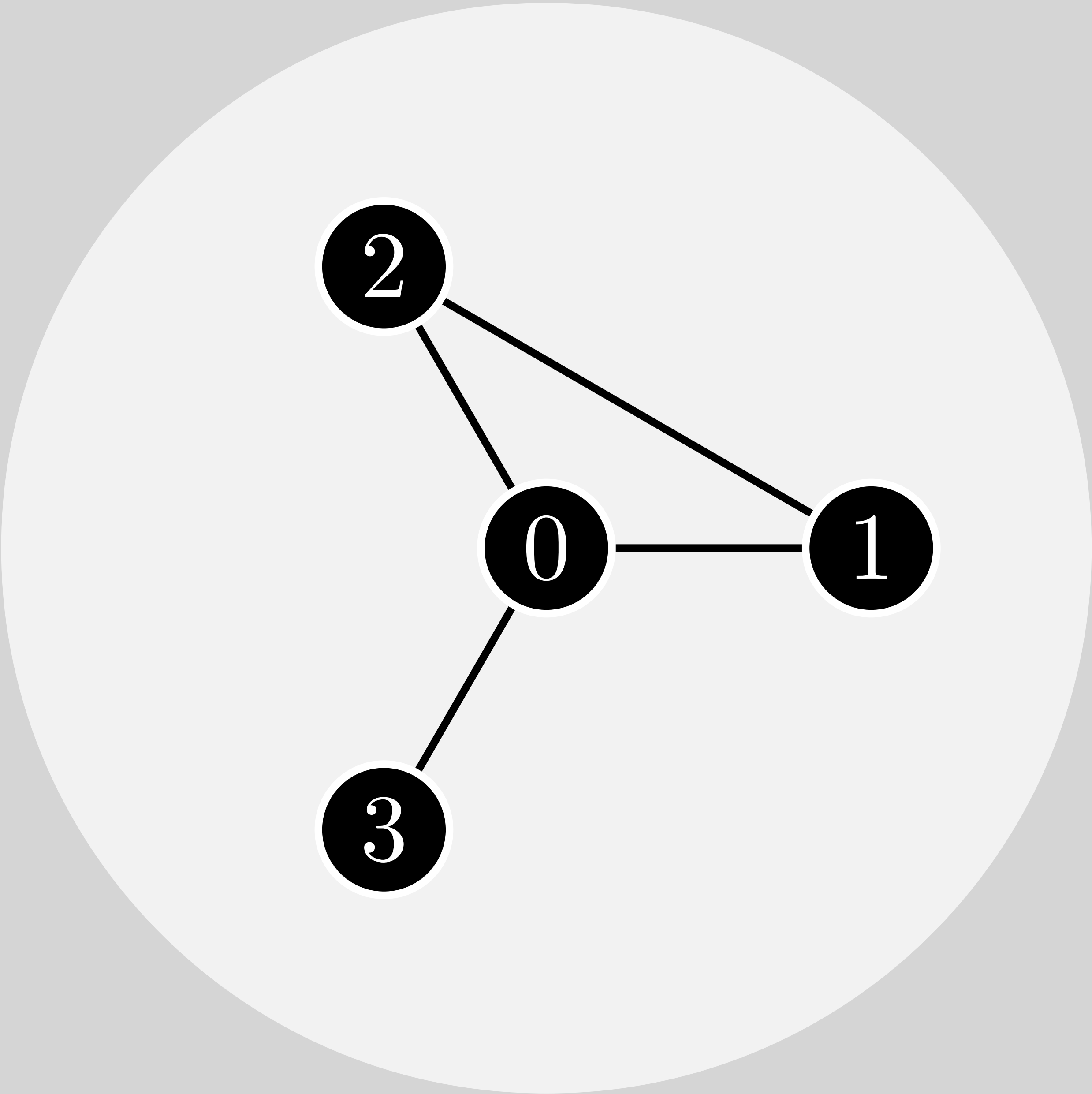
$$G = (V, E)$$

Nodes V

Edges $E \subseteq V \times V$

$$V = \{0,1,2,3\}$$

$$E = \{(0,1), (0,2), (0,3), (1,2)\}$$



$$G = (V, E)$$

Nodes V

Edges $E \subseteq V \times V$

$$V = \{0,1,2,3\}$$

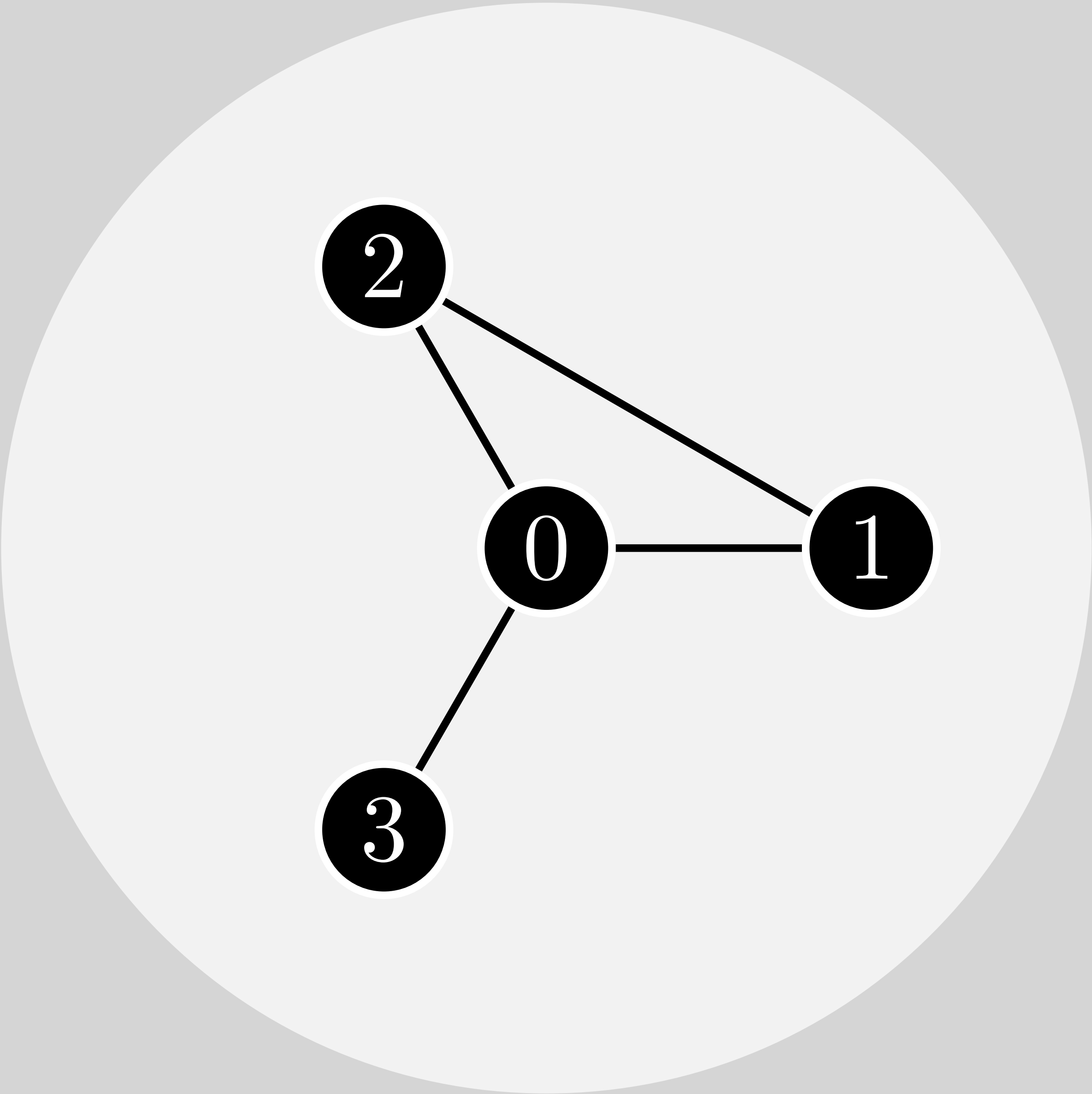
$$E = \{(0,1), (0,2), (0,3), (1,2)\}$$

Neighbourhood N_i of a node i

$$N_1 = \{0,2\} \qquad N_0 = \{1,2,3\}$$

…so what is the (quantum) state of the network?

A graph gives a *graph state*

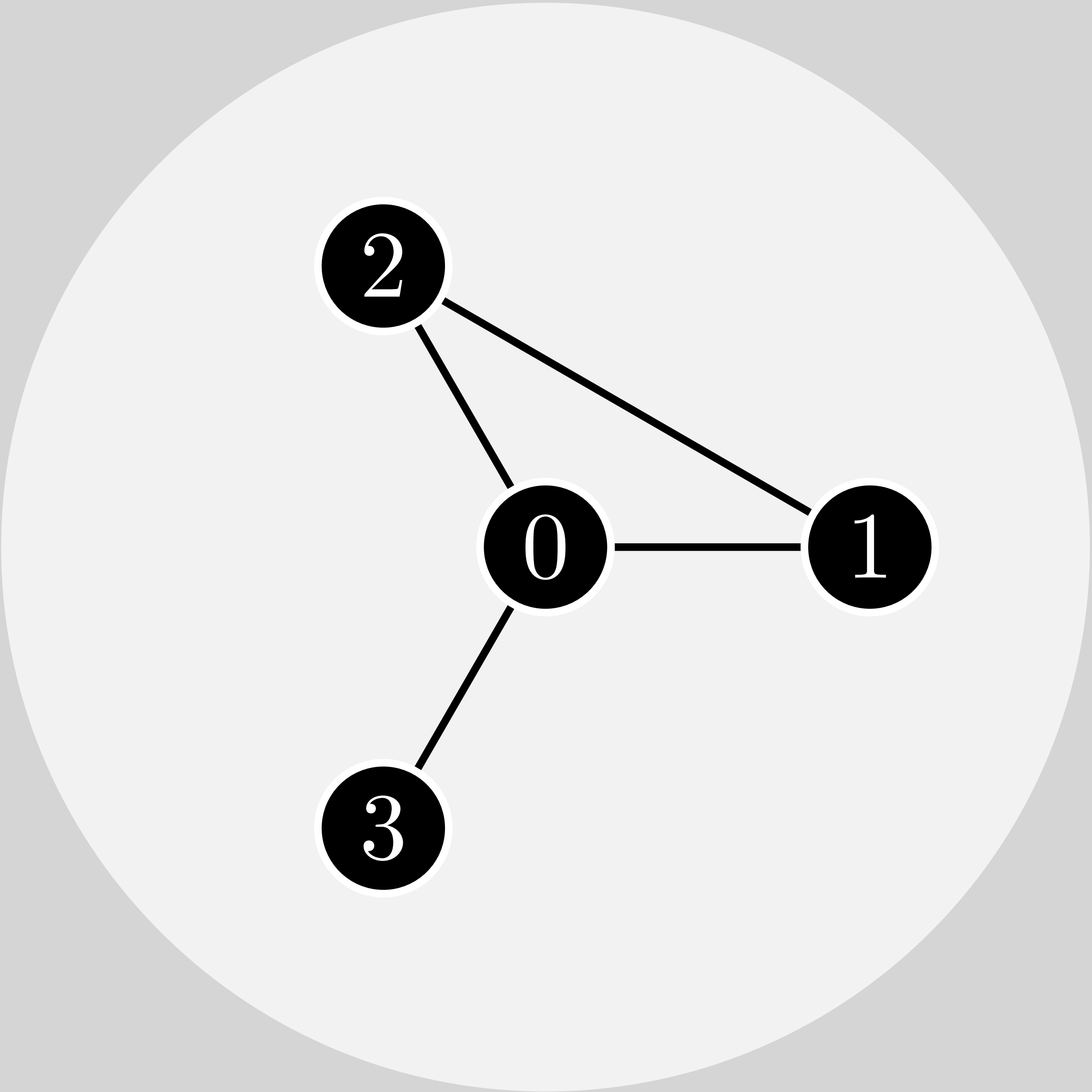


$$G = (V, E)$$

Nodes V

Edges E

A graph gives a *graph state*

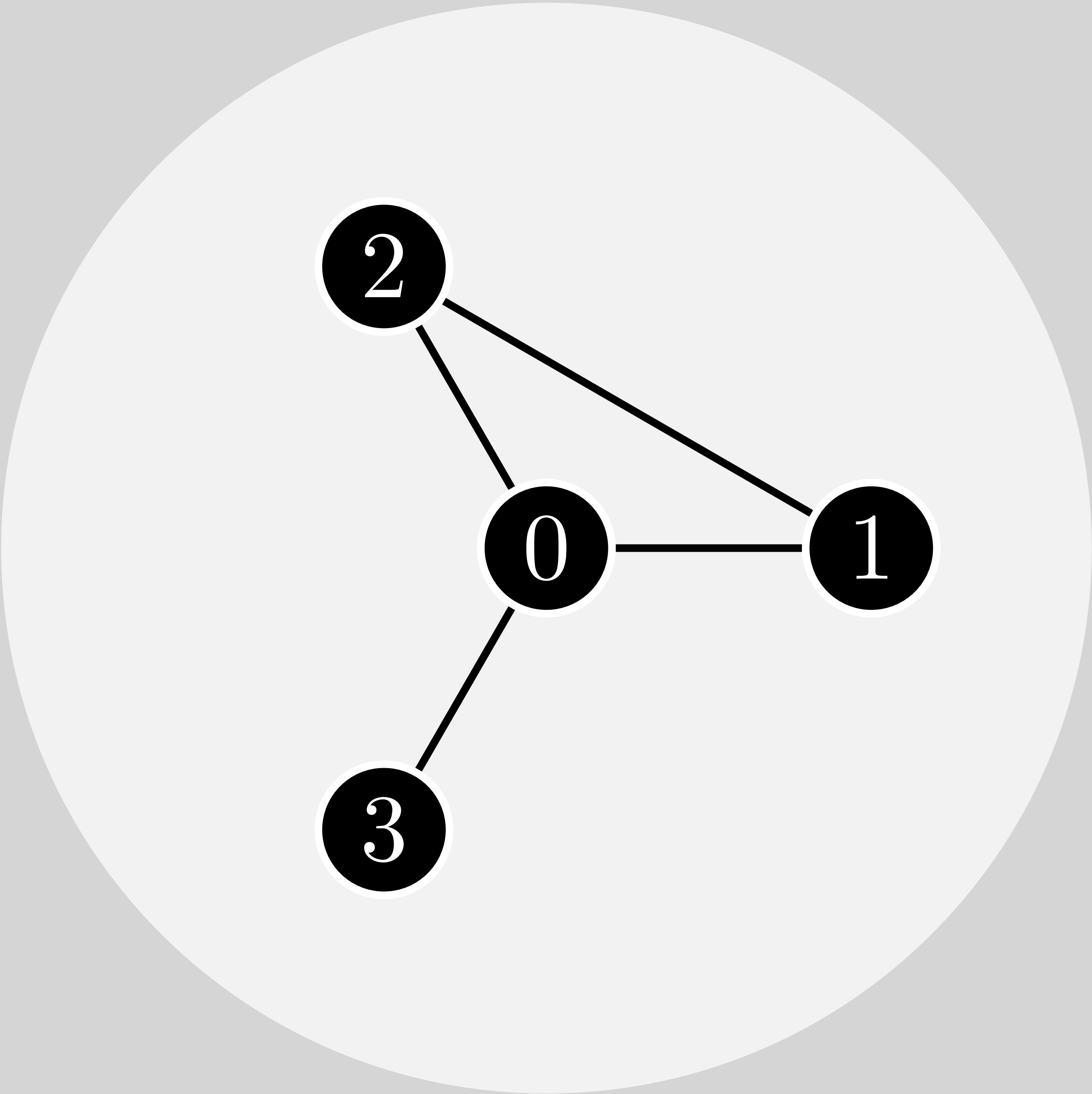


$$G = (V, E)$$

Nodes V → $|+\rangle_0 \otimes \ldots \otimes |+\rangle_V = |+\rangle^{\otimes V}$

Edges E → $(i, j) \in E \rightarrow CZ_{i,j}$

A graph gives a *graph state*



$$G = (V, E)$$

Nodes V

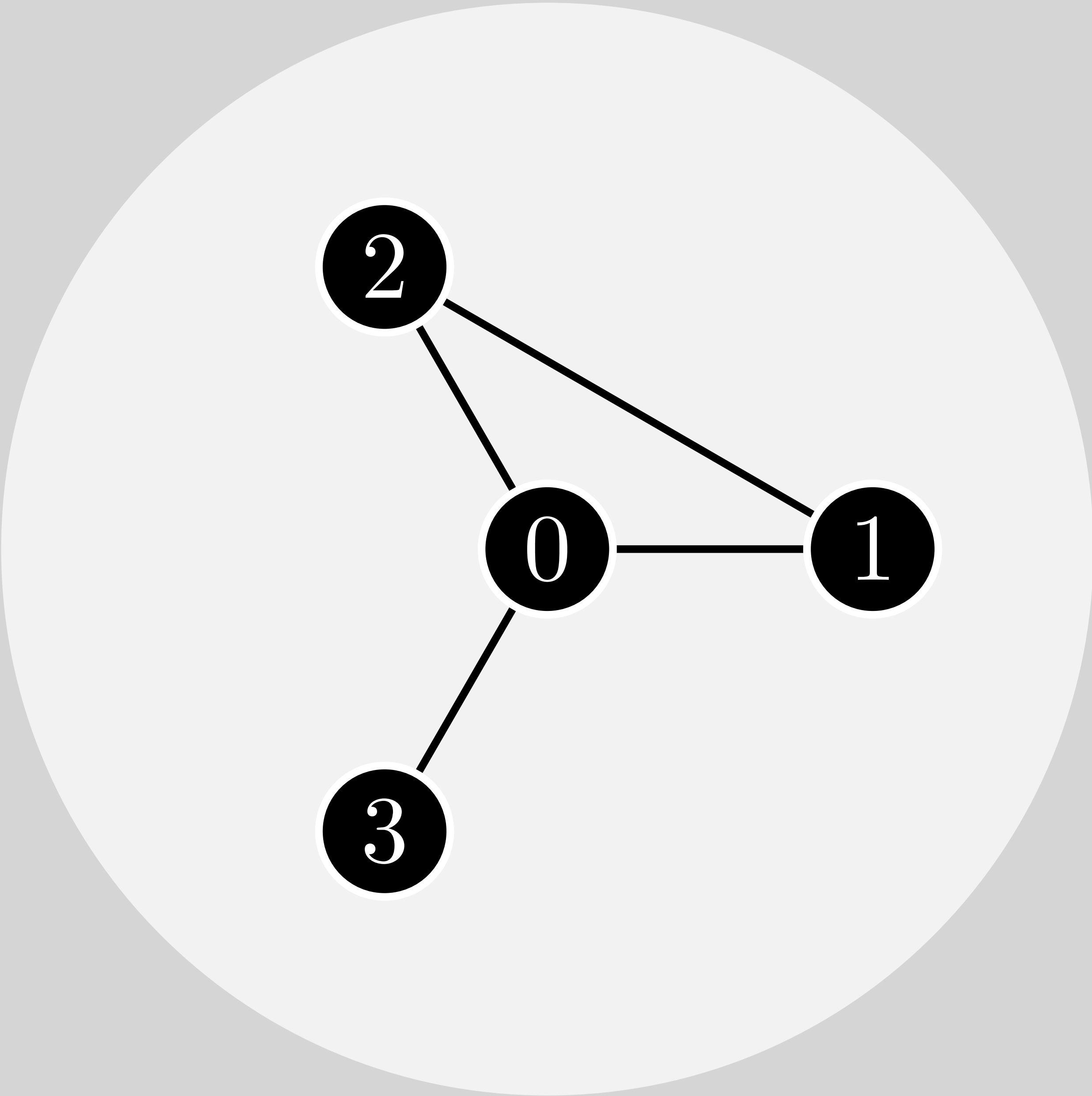
Edges E

$$|+\rangle_0 \otimes \ldots \otimes |+\rangle_V = |+\rangle^{\otimes V}$$

$$(i, j) \in E \to CZ_{i,j}$$

$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes V}$$

A graph gives a *graph state*



$$G = (V, E)$$

Nodes V

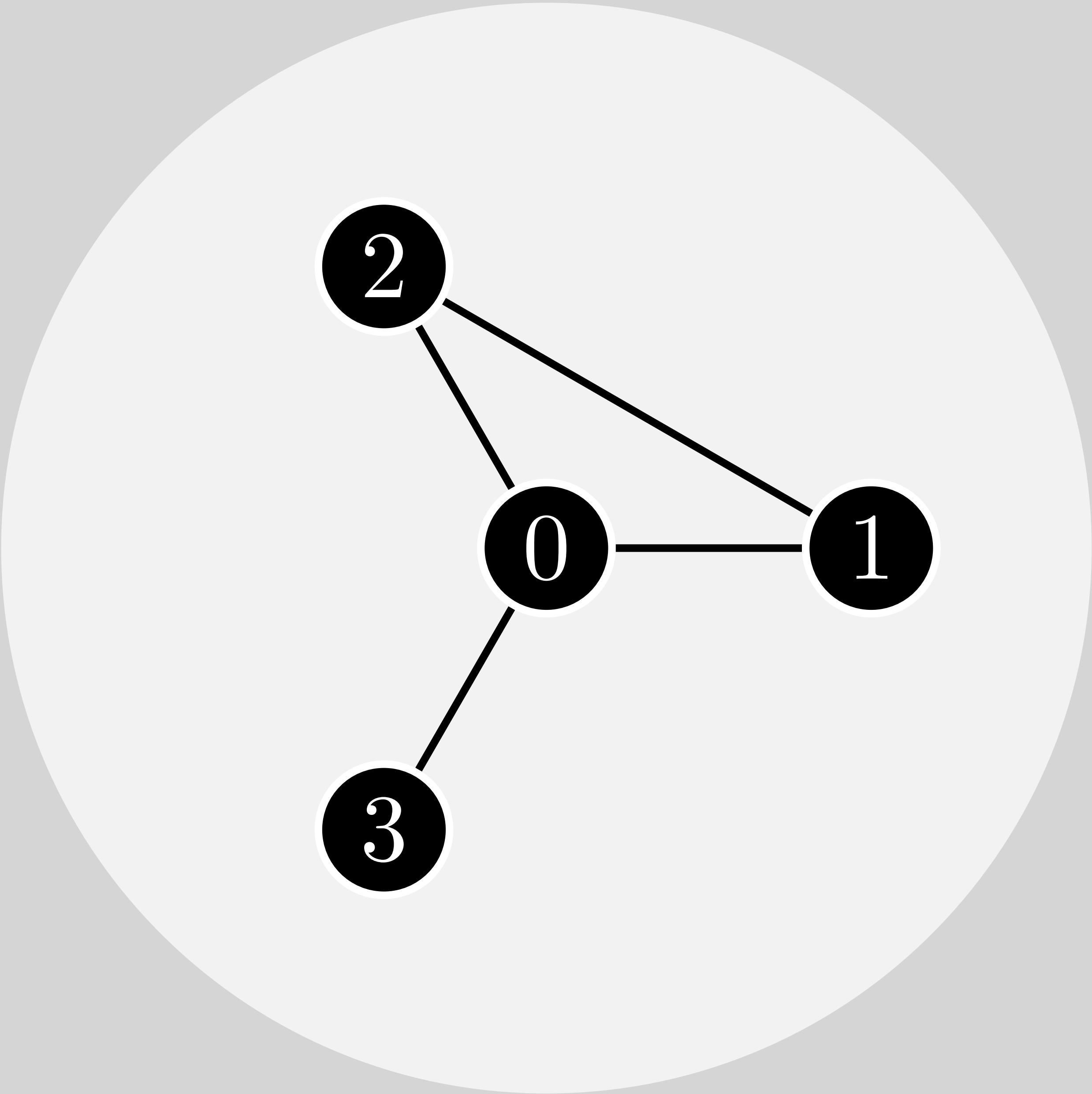
Edges E

$$|+\rangle_0 \otimes \ldots \otimes |+\rangle_V = |+\rangle^{\otimes V}$$

$$(i,j) \in E \rightarrow CZ_{i,j}$$

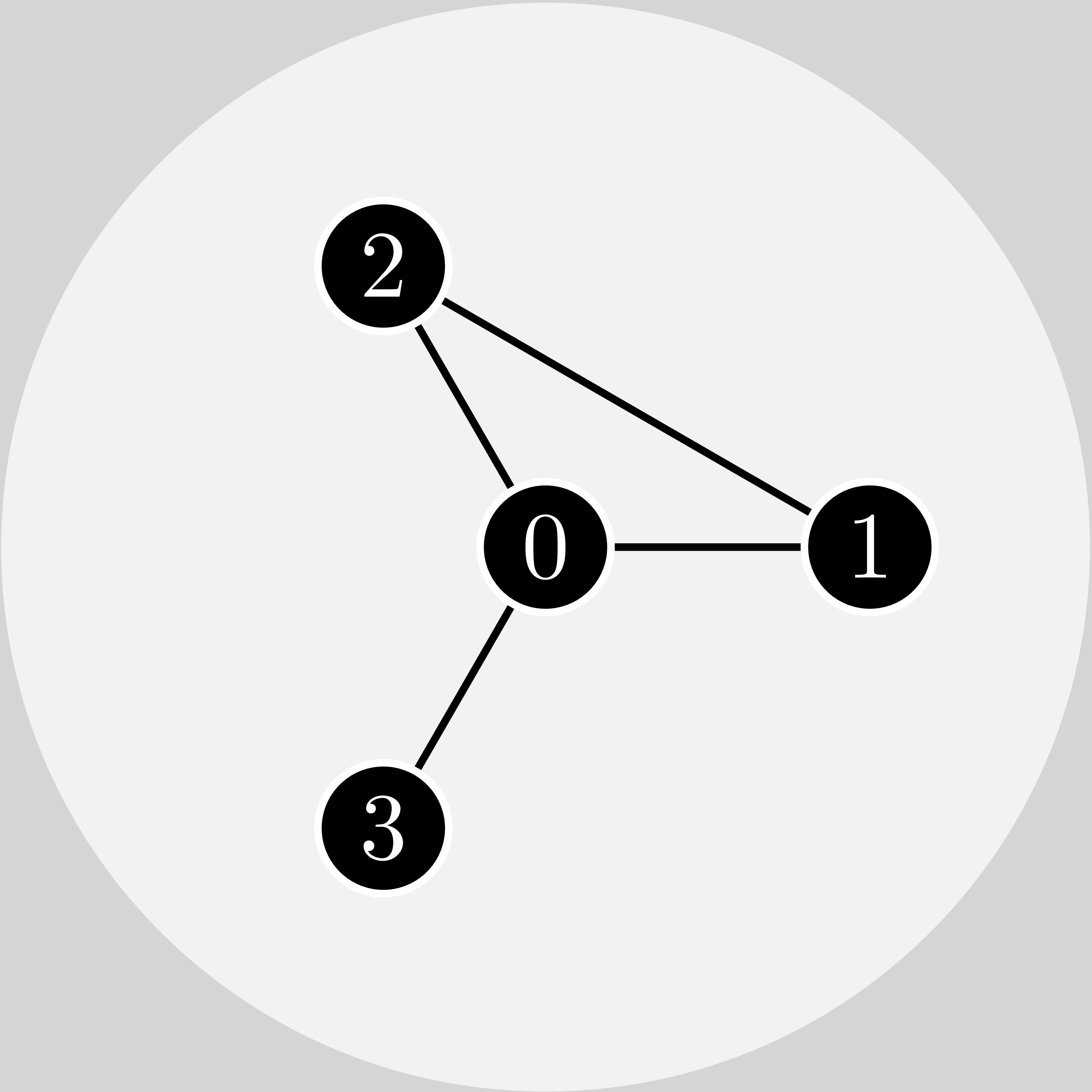
$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes V}$$

A graph gives a *graph state*



$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes V}$$

A graph gives a *graph state*

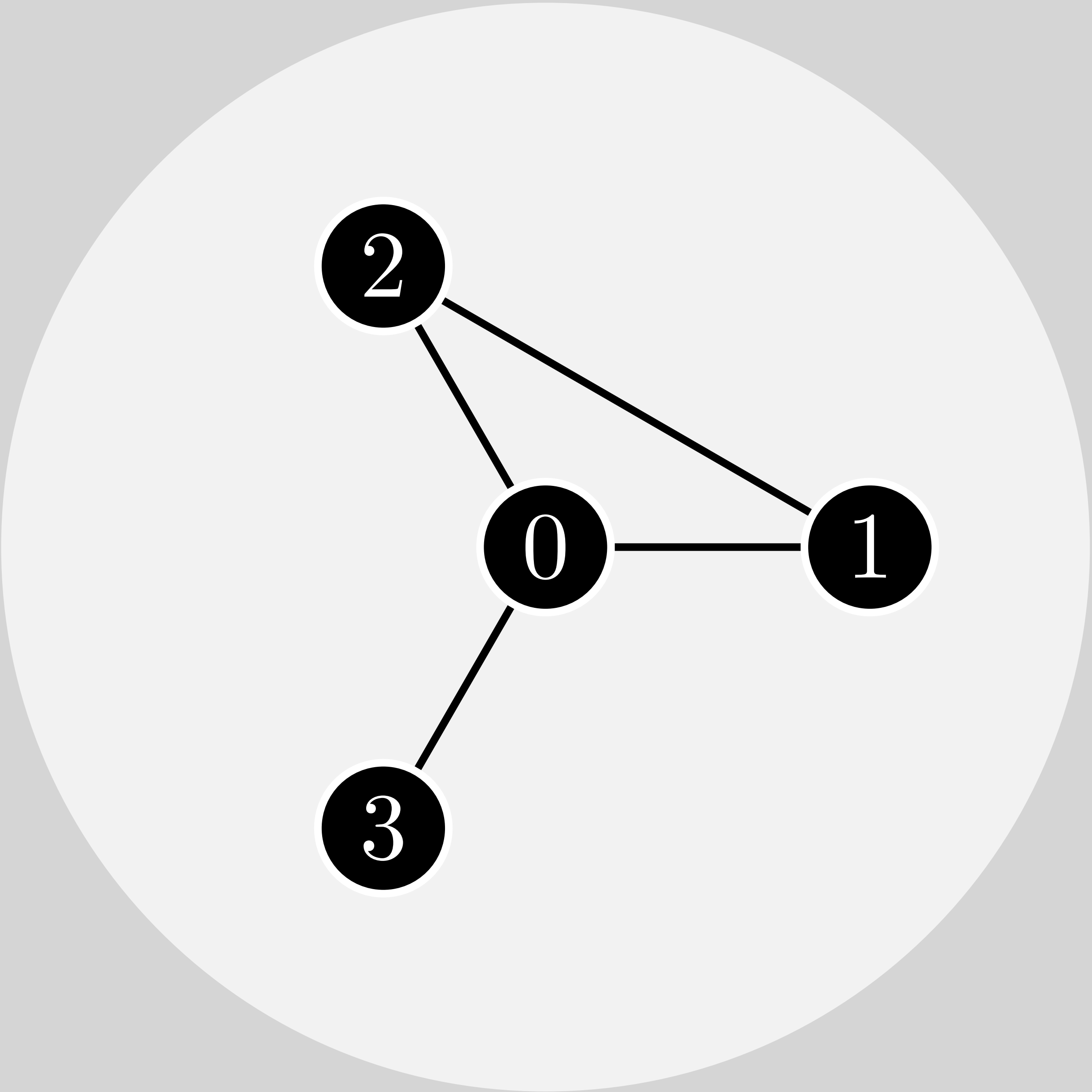


$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j} |+\rangle^{\otimes V}$$

$$\downarrow$$

$$CZ_{0,1}CZ_{0,2}CZ_{0,3}CZ_{1,2}|++++\rangle_{0,1,2,3}$$

A graph gives a *graph state*



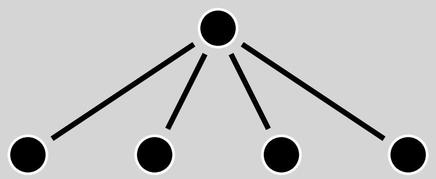
$$|G\rangle = \prod_{(i,j)\in E} CZ_{i,j}|+\rangle^{\otimes V}$$

$$CZ_{0,1}CZ_{0,2}CZ_{0,3}CZ_{1,2}|++++\rangle_{0,1,2,3}$$

$$|0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |0100\rangle + |0101\rangle - |0110\rangle - |0111\rangle + |1000\rangle - |1001\rangle - |1010\rangle + |1011\rangle - |1100\rangle + |1101\rangle - |1110\rangle + |1111\rangle$$

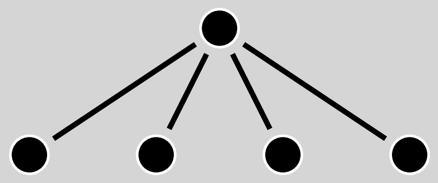
$$CZ|{+}{+}\rangle = |0{+}\rangle + |1{-}\rangle \simeq |00\rangle + |11\rangle = |\mathrm{EPR}\rangle$$

$$CZ|++\rangle = |0+\rangle + |1-\rangle \simeq |00\rangle + |11\rangle = |\mathrm{EPR}\rangle$$



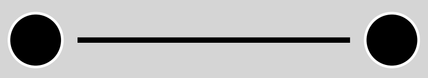
$$CZ_{0,i}\big(|0++++\rangle\big) + CZ_{0,i}\big(|1++++\rangle\big) = |0++++\rangle + |1----\rangle \simeq |\mathrm{GHZ}\rangle$$

$$CZ|++\rangle = |0+\rangle + |1-\rangle \simeq |00\rangle + |11\rangle = |\mathrm{EPR}\rangle$$

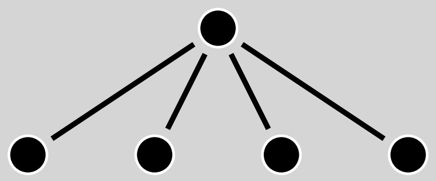


$$CZ_{0,i}\big(|0++++\rangle\big) + CZ_{0,i}\big(|1++++\rangle\big) = |0++++\rangle + |1----\rangle \simeq |\mathrm{GHZ}\rangle$$

Linear clusterstate

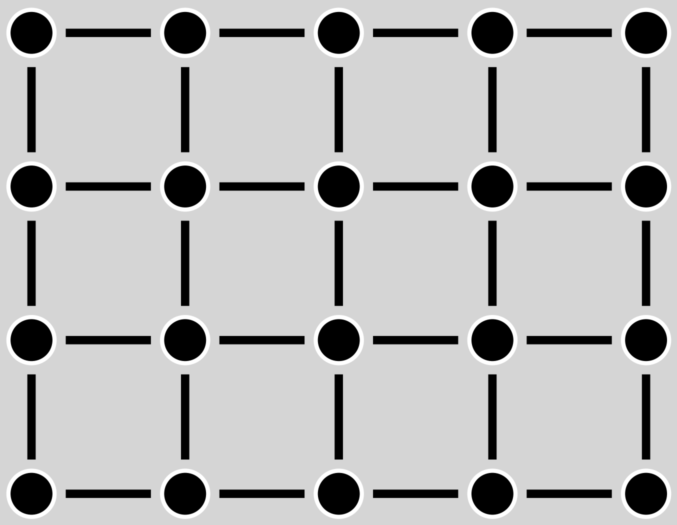


$$CZ|++\rangle = |0+\rangle + |1-\rangle \simeq |00\rangle + |11\rangle = |\mathrm{EPR}\rangle$$



$$CZ_{0,i}\big(|0++++\rangle\big) + CZ_{0,i}\big(|1++++\rangle\big) = |0++++\rangle + |1----\rangle \simeq |\mathrm{GHZ}\rangle$$

Linear clusterstate



2D clusterstate

Graphstates represent *entanglement*

Graphstates represent *entanglement*

Entanglement in the network

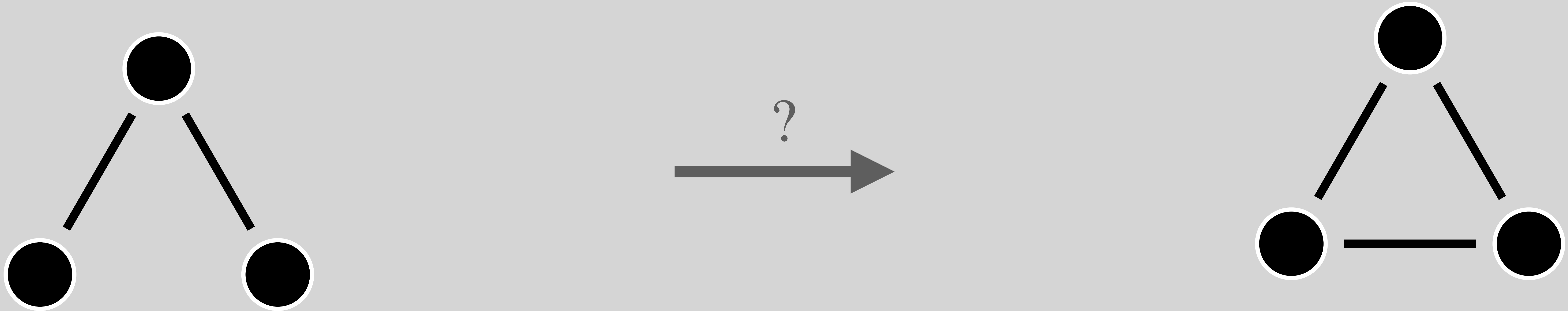
$$\sqrt{Z_0}\sqrt{X_1}\sqrt{Z_2}$$

$$|000\rangle + |010\rangle \rightarrow + |000\rangle + |010\rangle$$

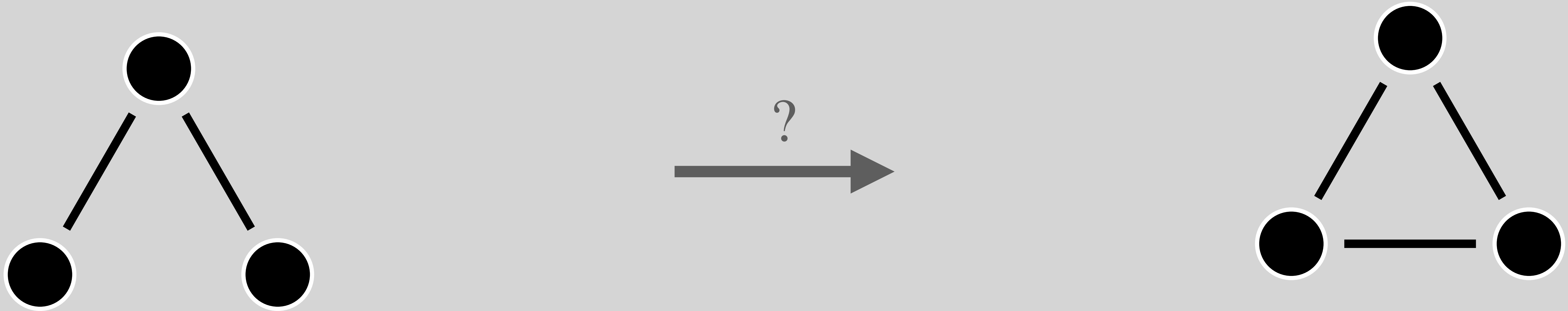
$$|001\rangle - |011\rangle \rightarrow + |001\rangle - |011\rangle$$

$$|100\rangle - |110\rangle \rightarrow + |100\rangle - |110\rangle$$

$$|101\rangle + |111\rangle \rightarrow - |101\rangle - |111\rangle$$

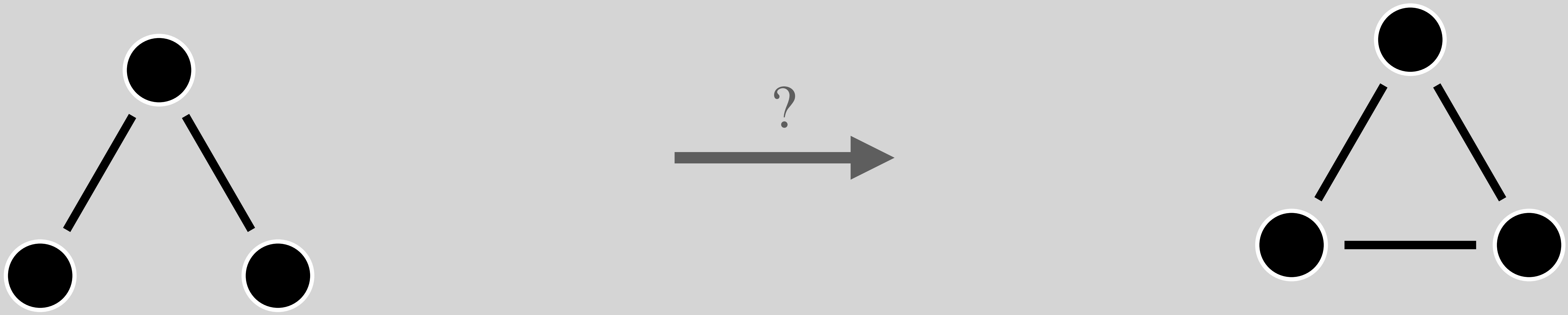


LOCC

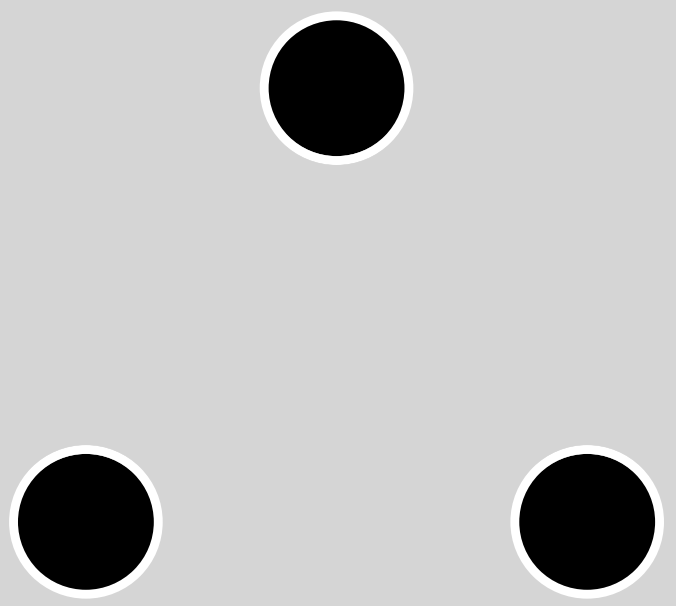


- *Local* operations
  - Single-qubit unitaries
  - **No** entangling gates

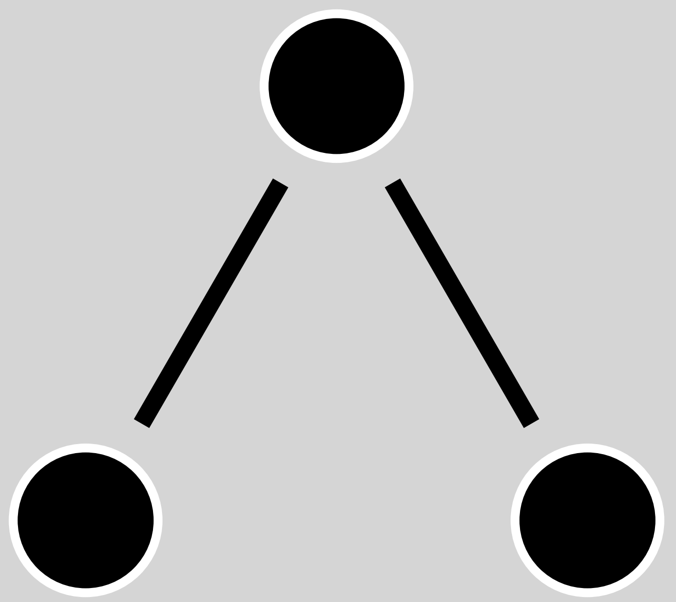
LOCC



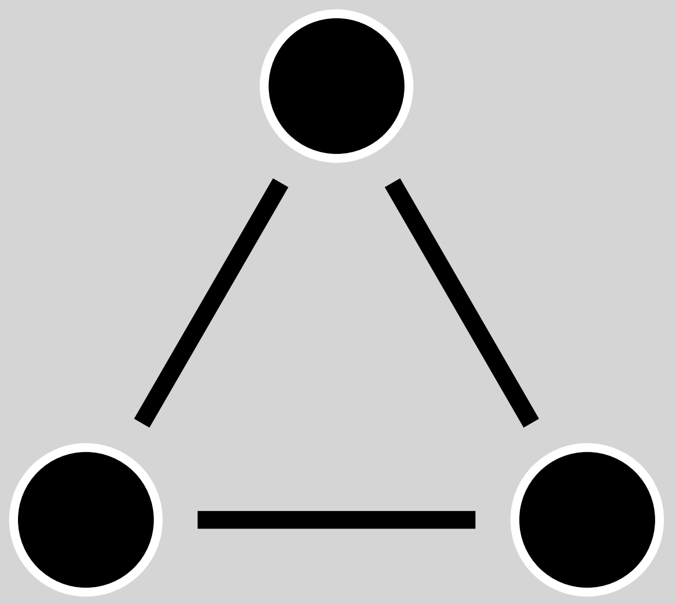
2 edges *3 edges*



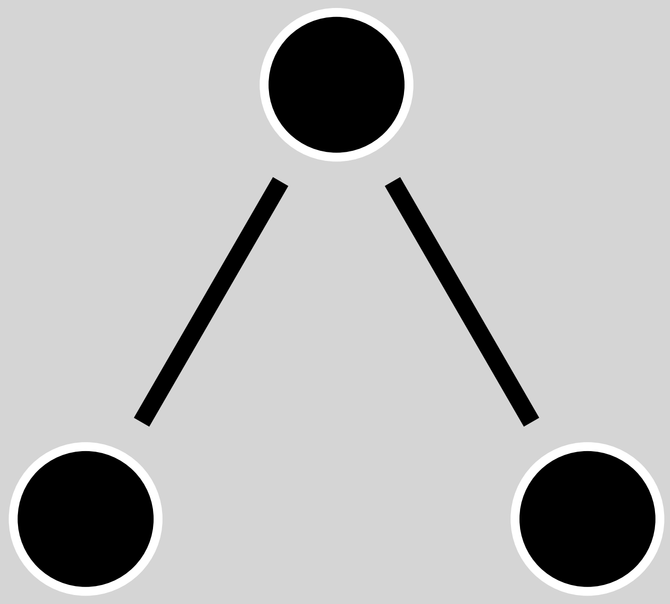
$$|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle + |011\rangle + |110\rangle + |111\rangle$$



$$|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle$$

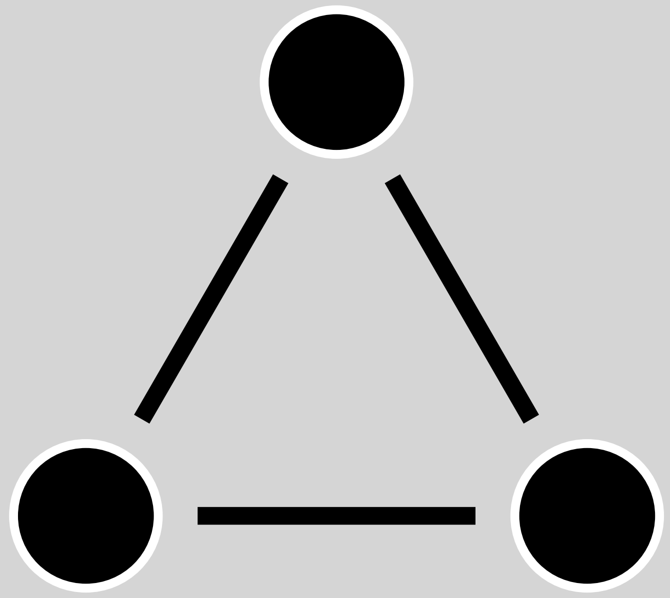


$$|000\rangle + |001\rangle + |100\rangle - |101\rangle + |010\rangle - |011\rangle - |110\rangle - |111\rangle$$



$$|000\rangle + |001\rangle + |100\rangle + |101\rangle + |010\rangle - |011\rangle - |110\rangle + |111\rangle$$

$$\Big\downarrow \sqrt{Z_0}\sqrt{X_1}\sqrt{Z_2}$$



$$|000\rangle + |001\rangle + |100\rangle - |101\rangle + |010\rangle - |011\rangle - |110\rangle - |111\rangle$$

$$|G\rangle \xrightarrow{\sqrt{X_i}\sqrt{Z_{N_i}}} |G'\rangle$$

$$G = (V, E) \xrightarrow{\tau_i} G' = (V, E')$$

$$E' = E \oplus (N_i \times N_i)$$

$$G = (V, E) \xrightarrow{\tau_i} G' = (V, E')$$

τ_i: ***local complementation***

$$G = (V, E) \xrightarrow{\tau_i} G' = (V, E')$$

τ_i: *local complementation*

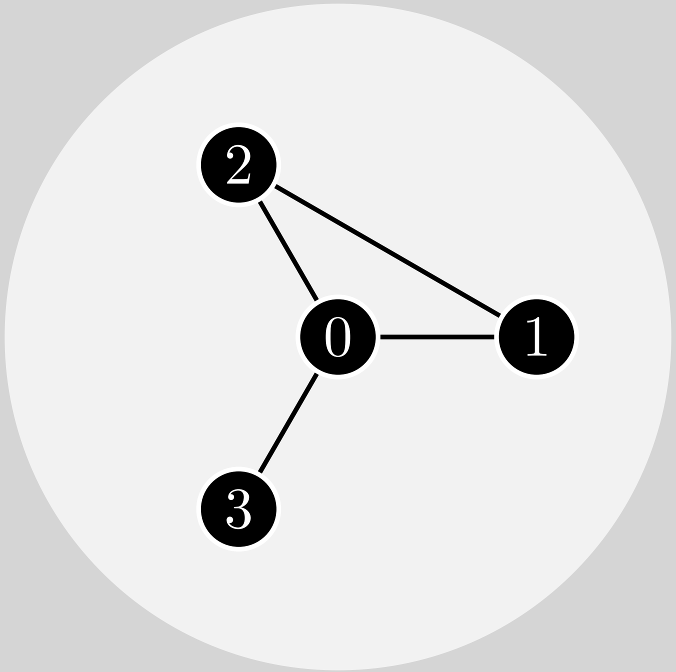
τ_i: *local complementation*

Take a & $b \in N_i$:

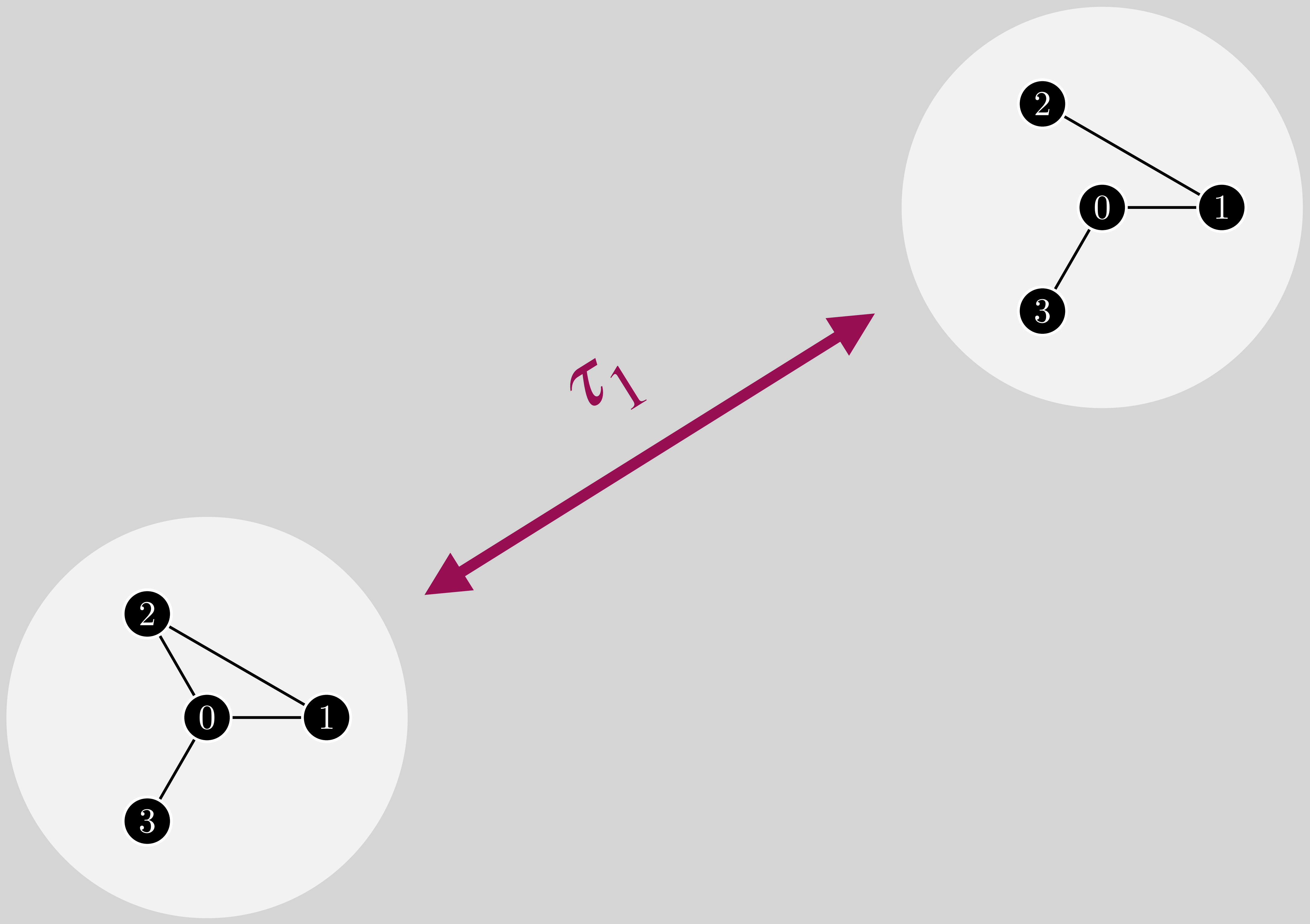
τ_i: *local complementation*

Take a & $b \in N_i$:

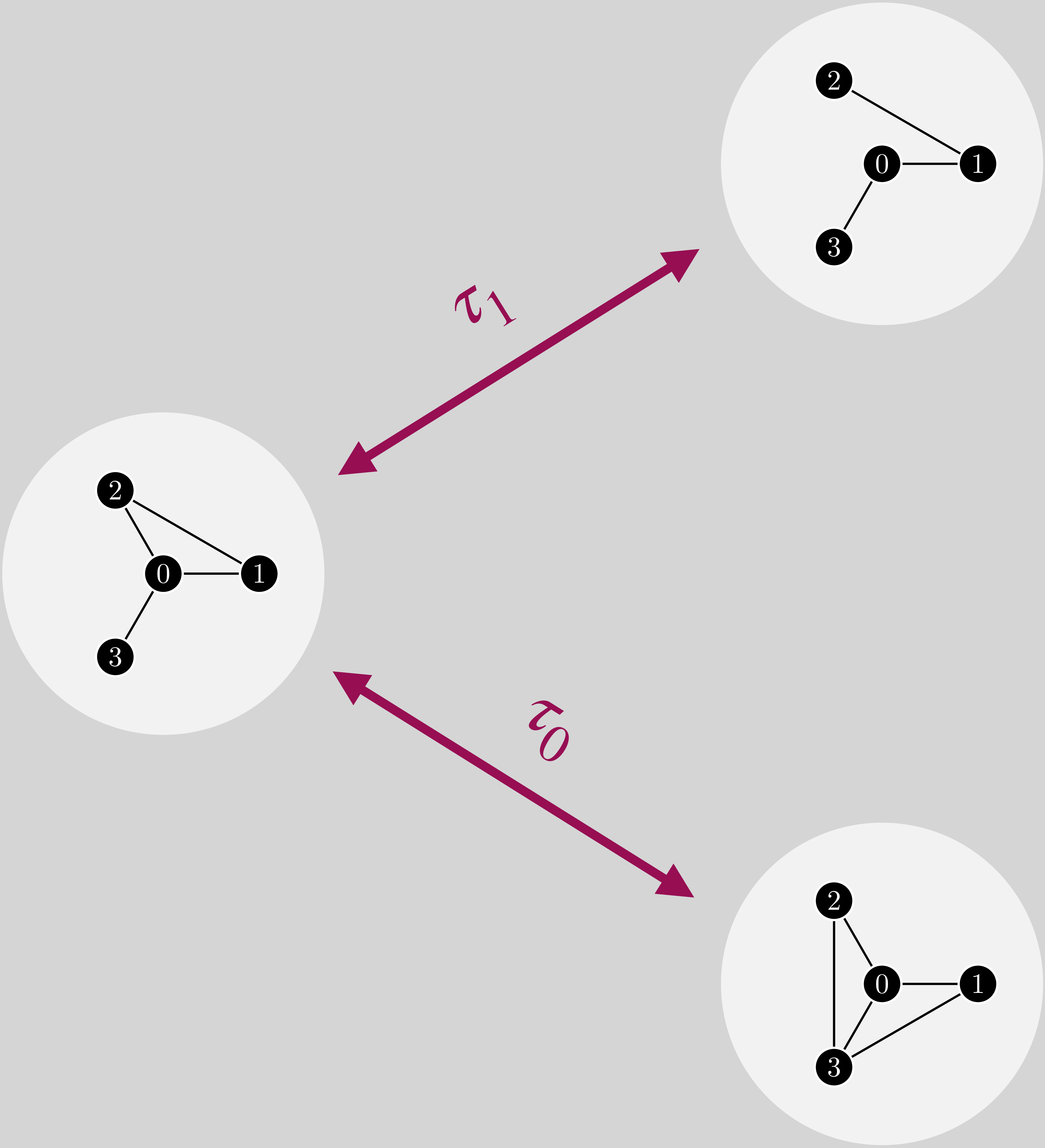
Flip edge (a, b)



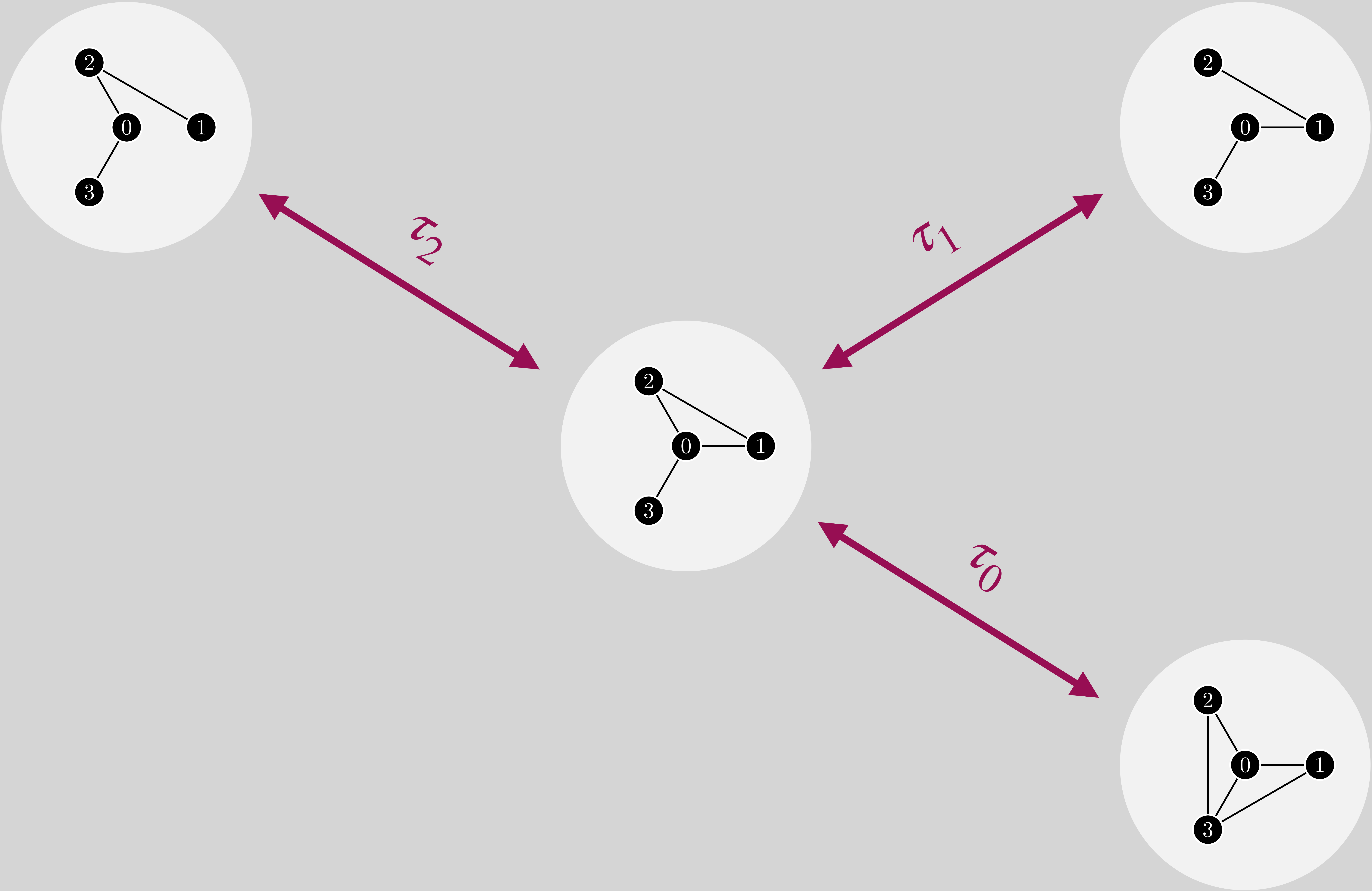
2
0
1
3



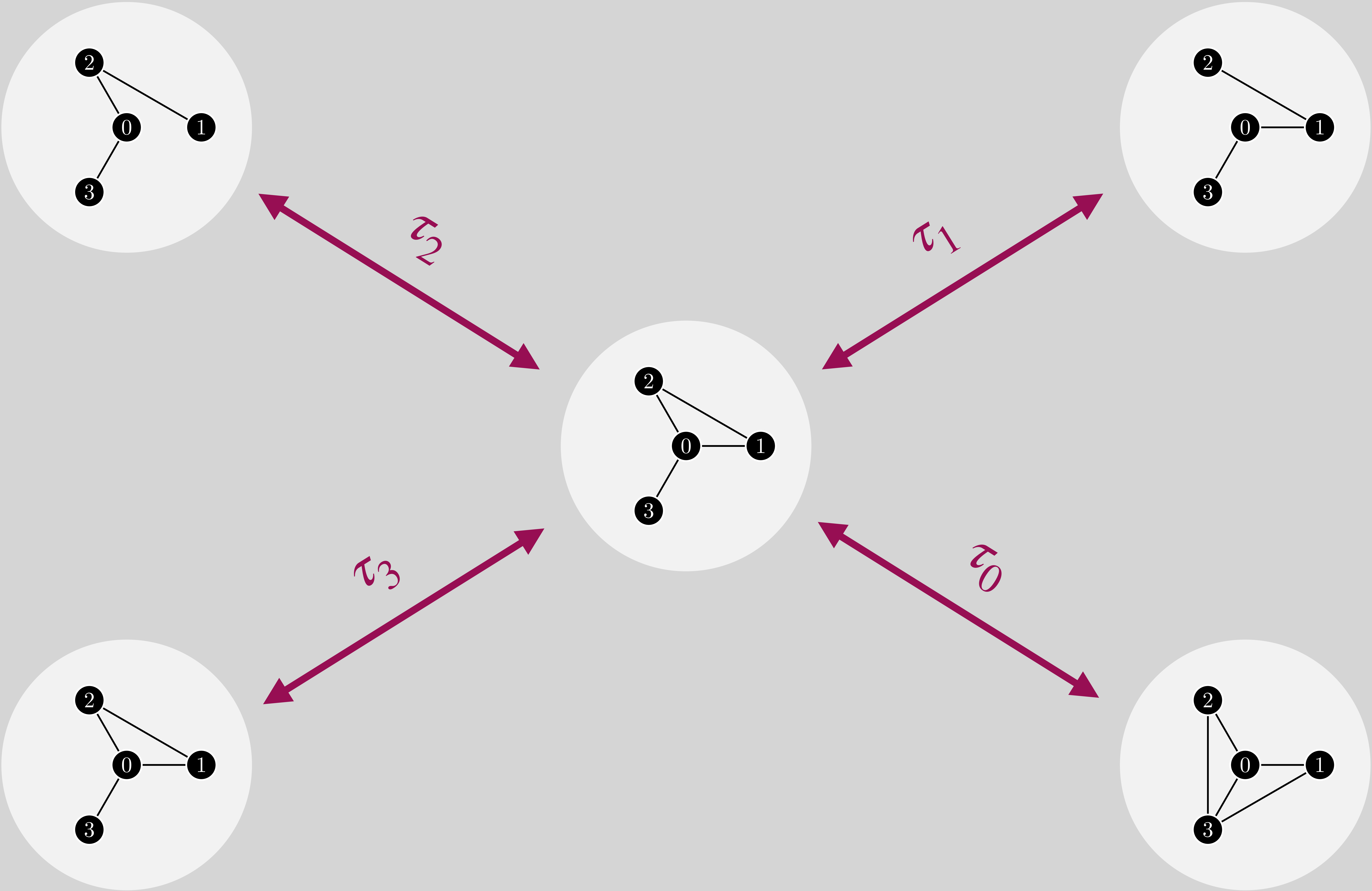
2
0
1
3
τ_1
2
0
1
3



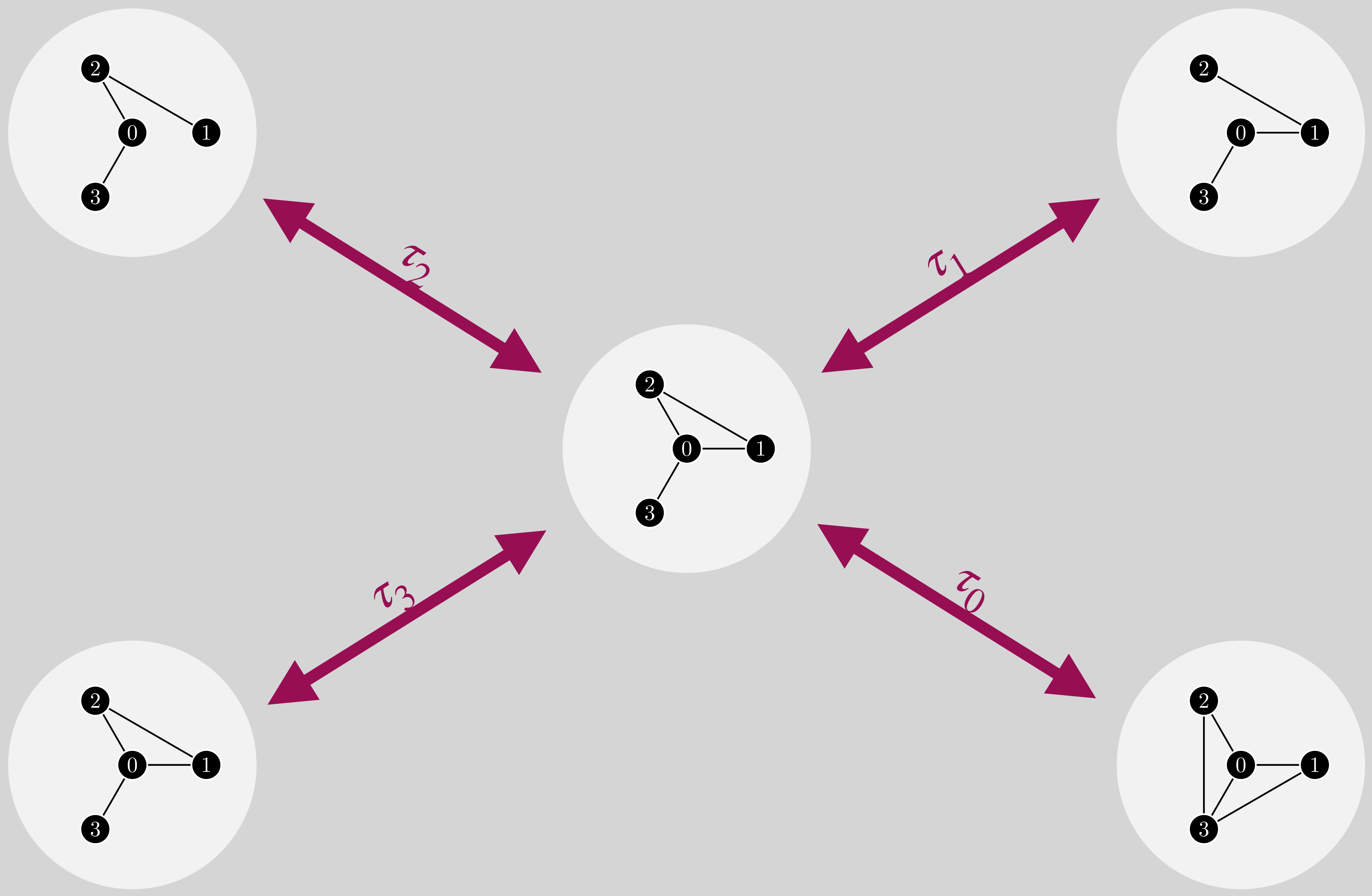
2
0
1
3
τ_1
τ_0



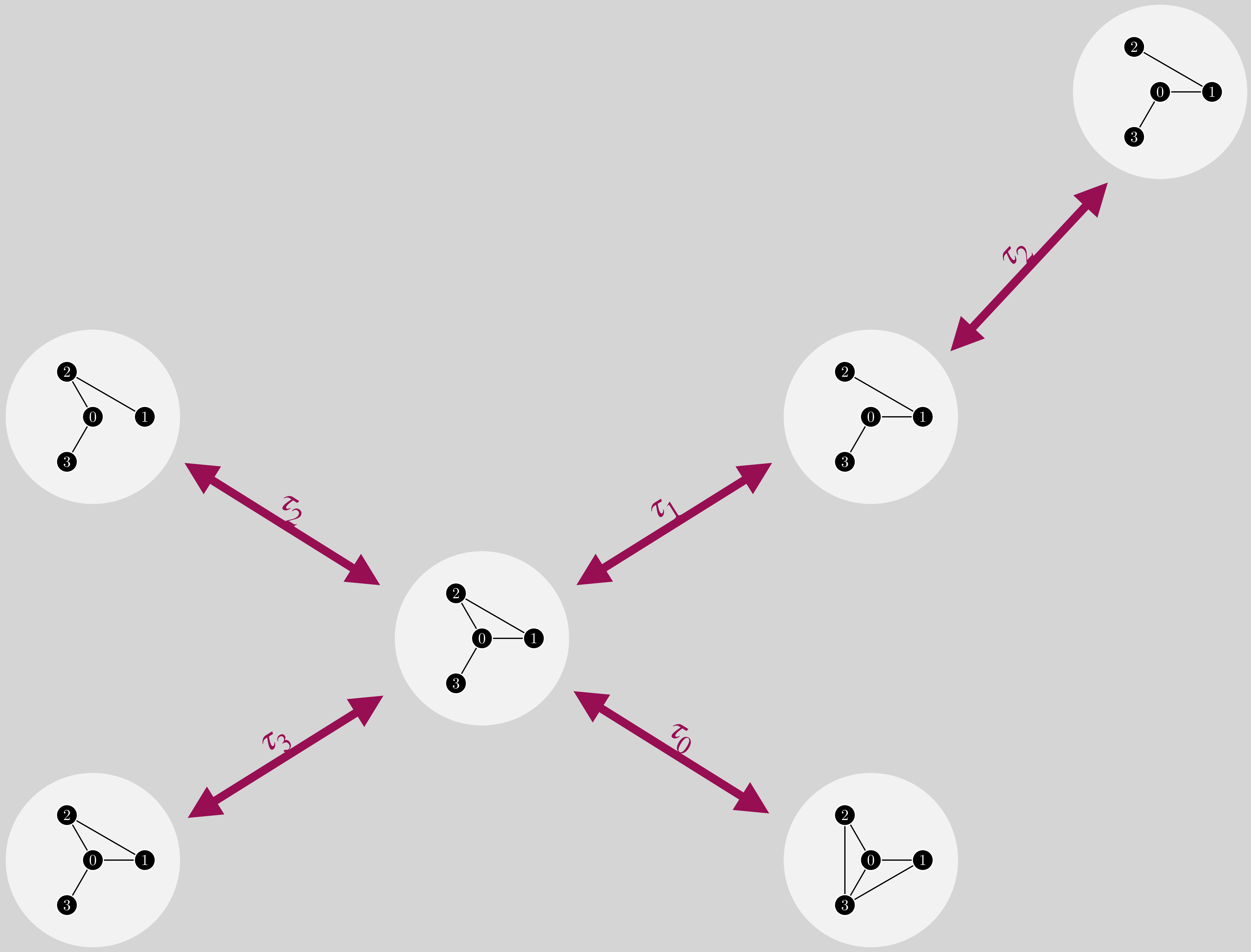
2
0
1
3
τ_2
τ_1
τ_0



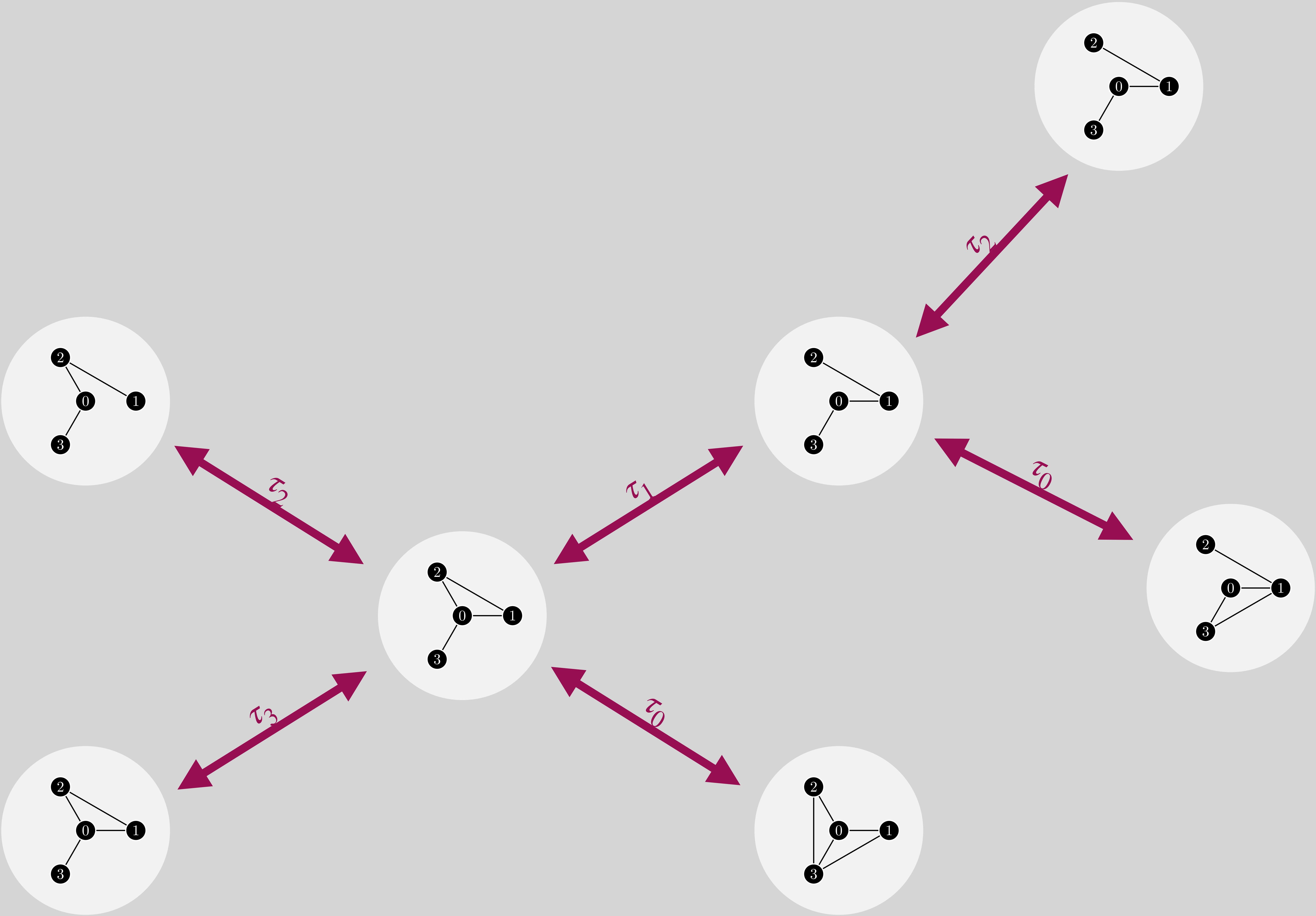
2
0
1
3
τ_2
τ_1
τ_3
τ_0



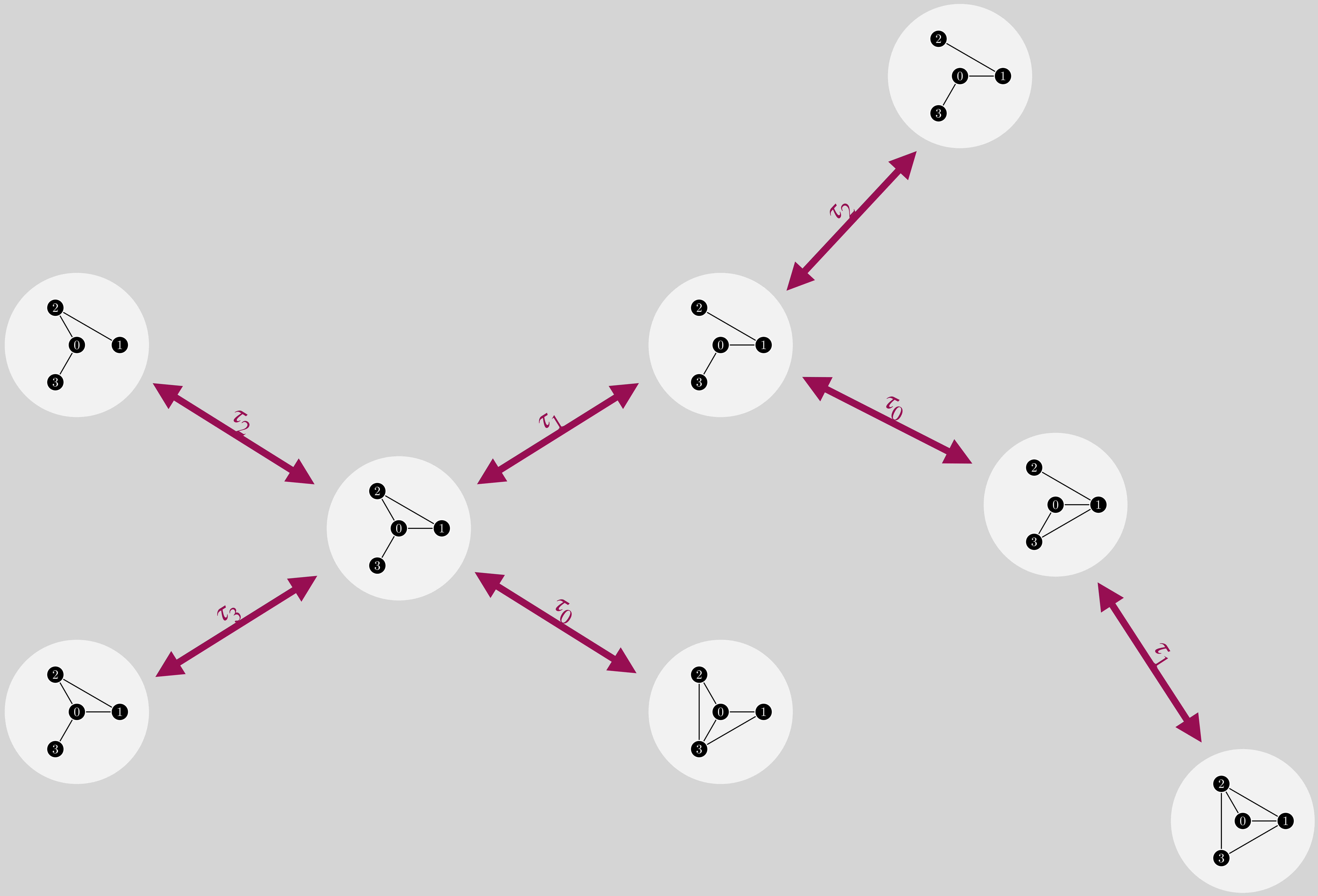
2
0
1
3
τ_2
τ_1
τ_3
τ_0



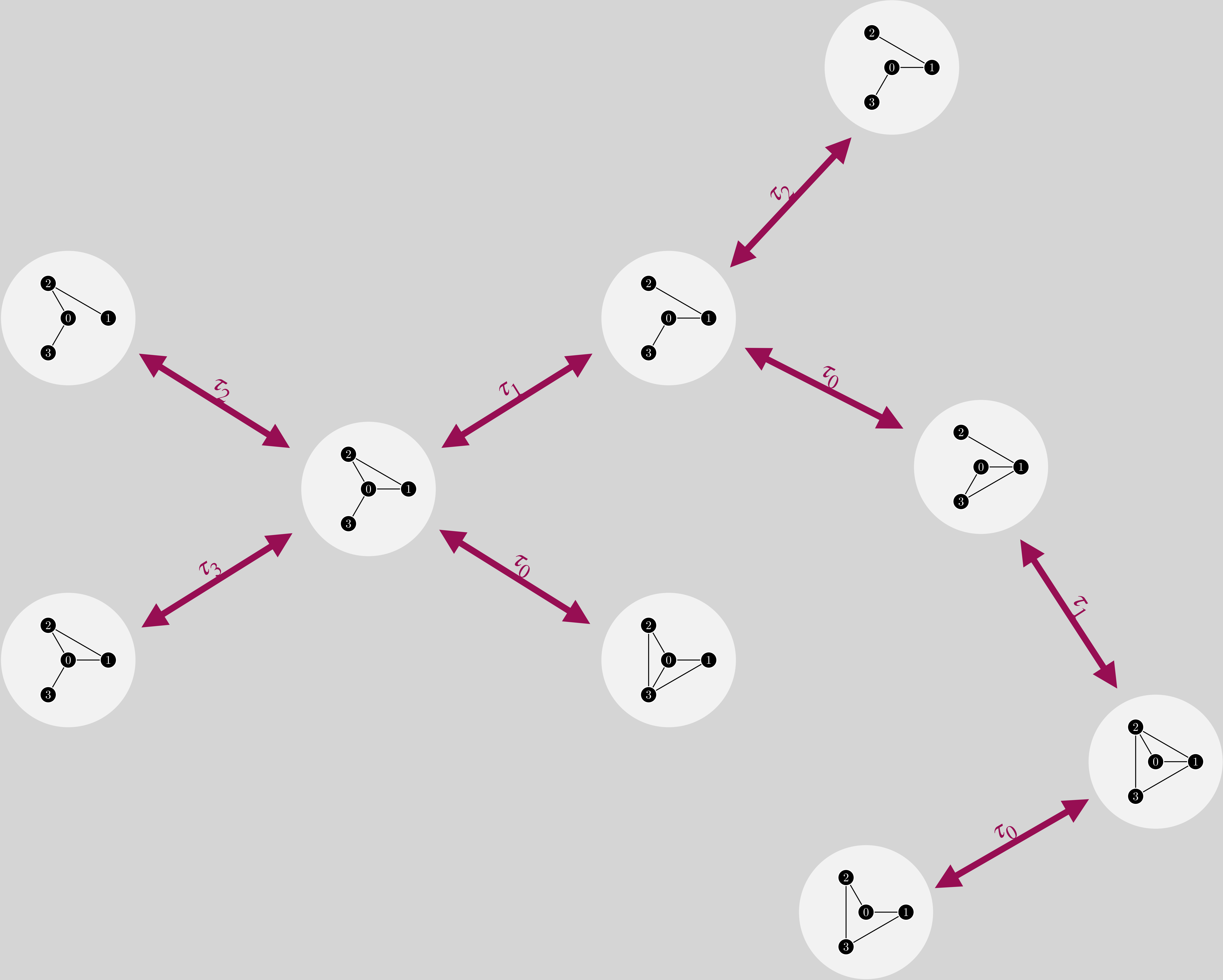
τ_2
τ_2
τ_1
τ_3
τ_0
0
1
2
3



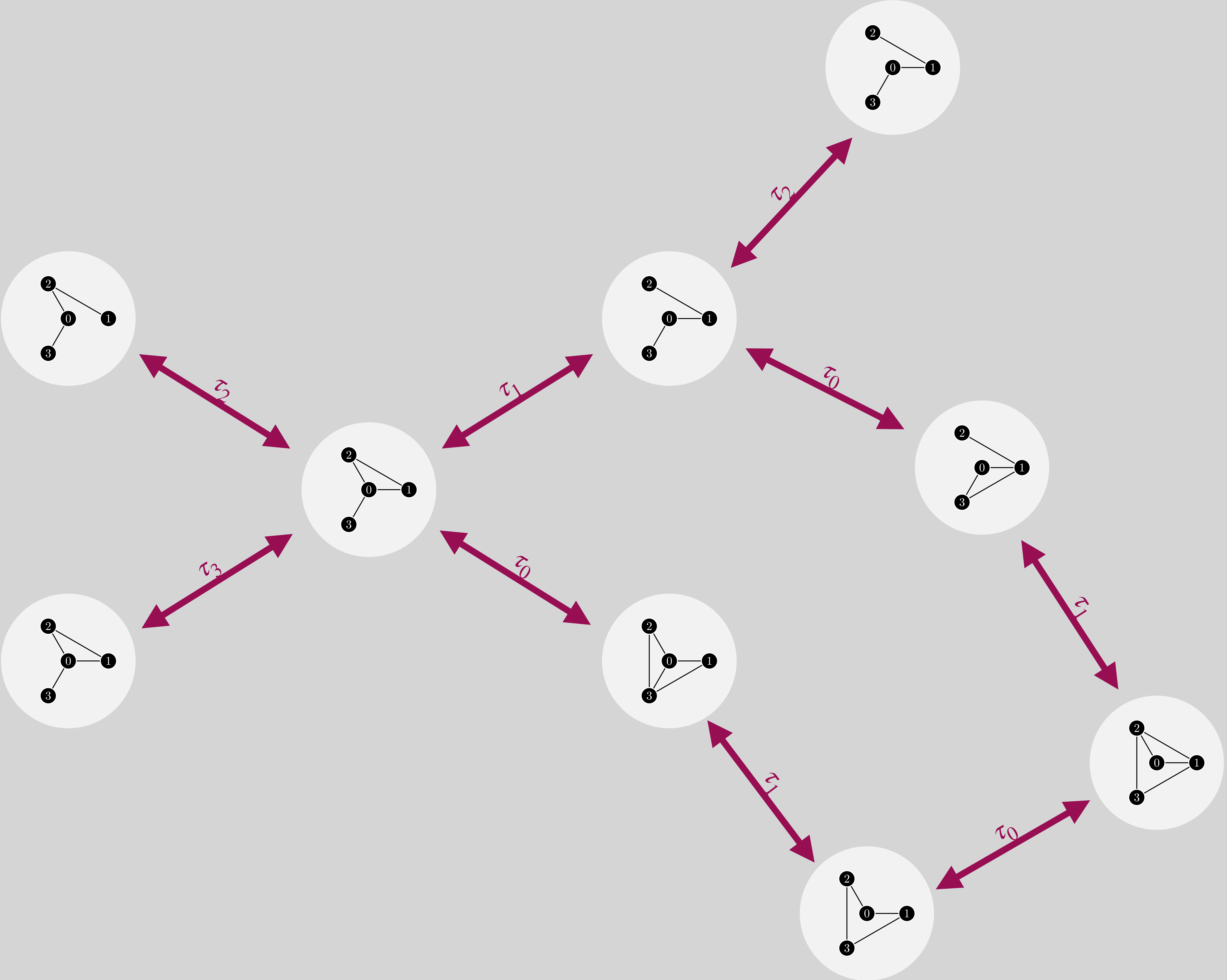
τ_2
τ_1
τ_0
τ_2
τ_3
τ_0



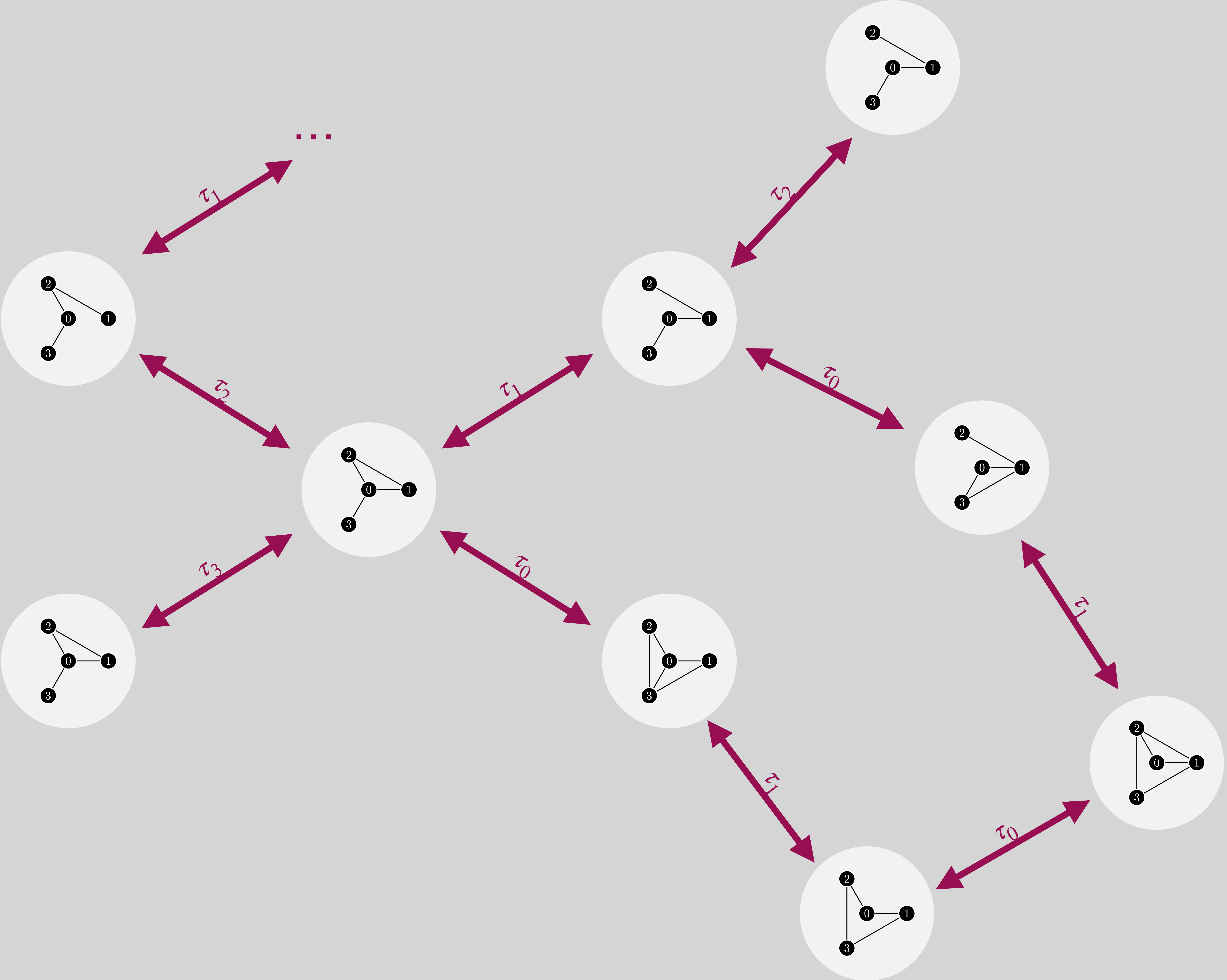
τ_2
τ_1
τ_2
τ_0
τ_3
τ_0
τ_1



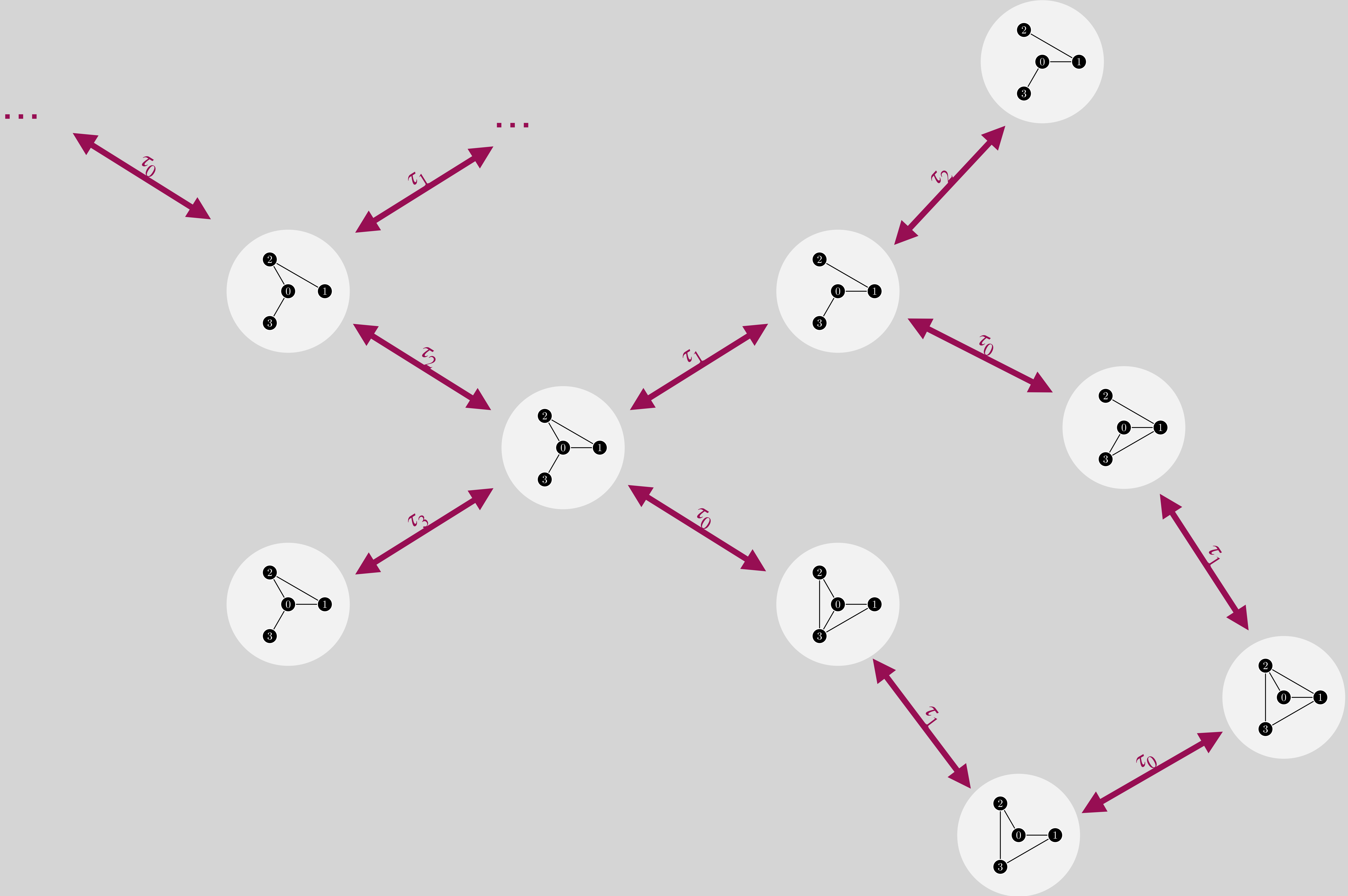
τ_2
τ_1
τ_0
τ_2
τ_3
τ_0
τ_1
τ_0
0
1
2
3



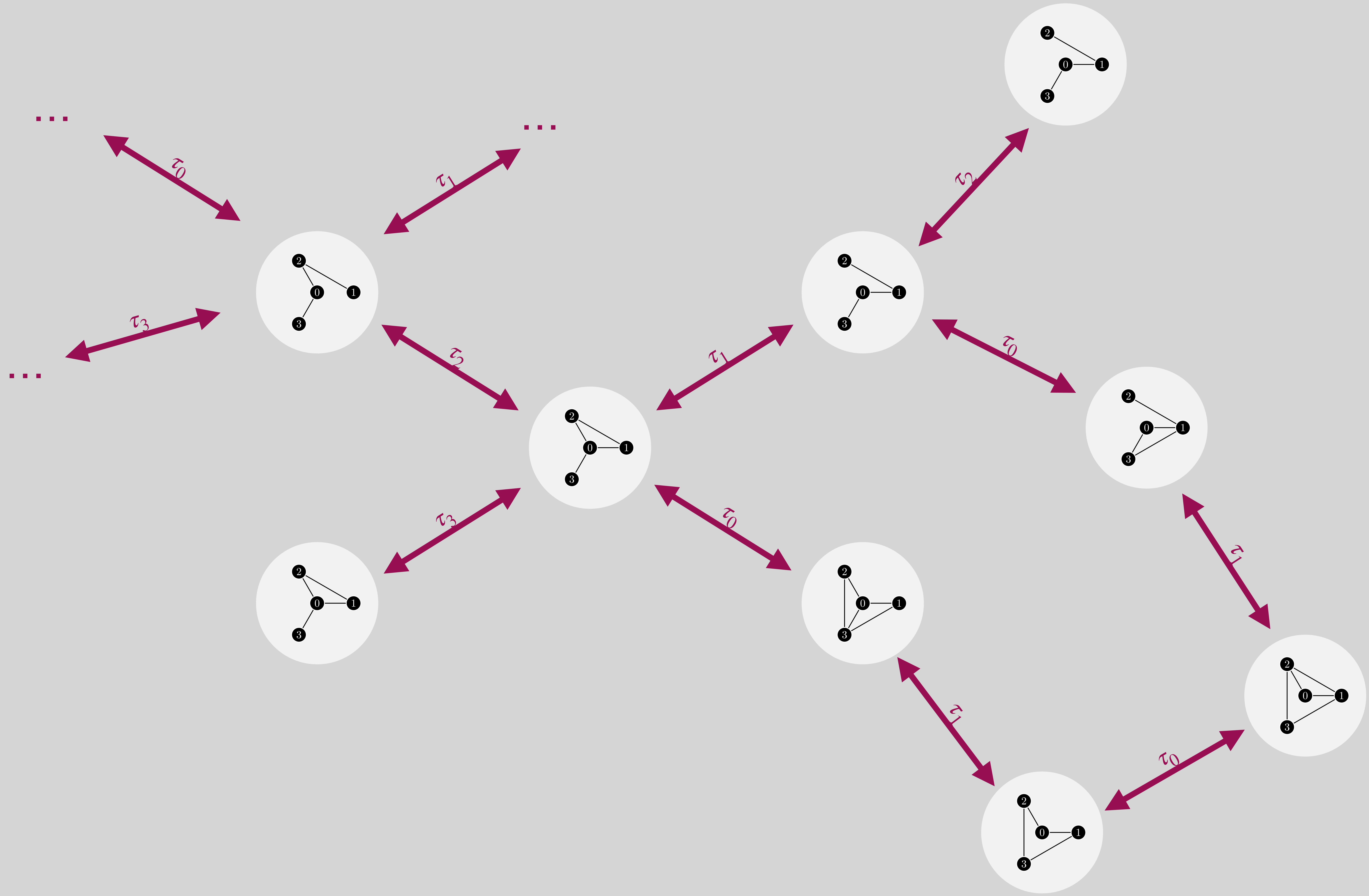
τ_2
τ_1
τ_0
τ_3
τ_0
τ_2
τ_1
τ_1
τ_0



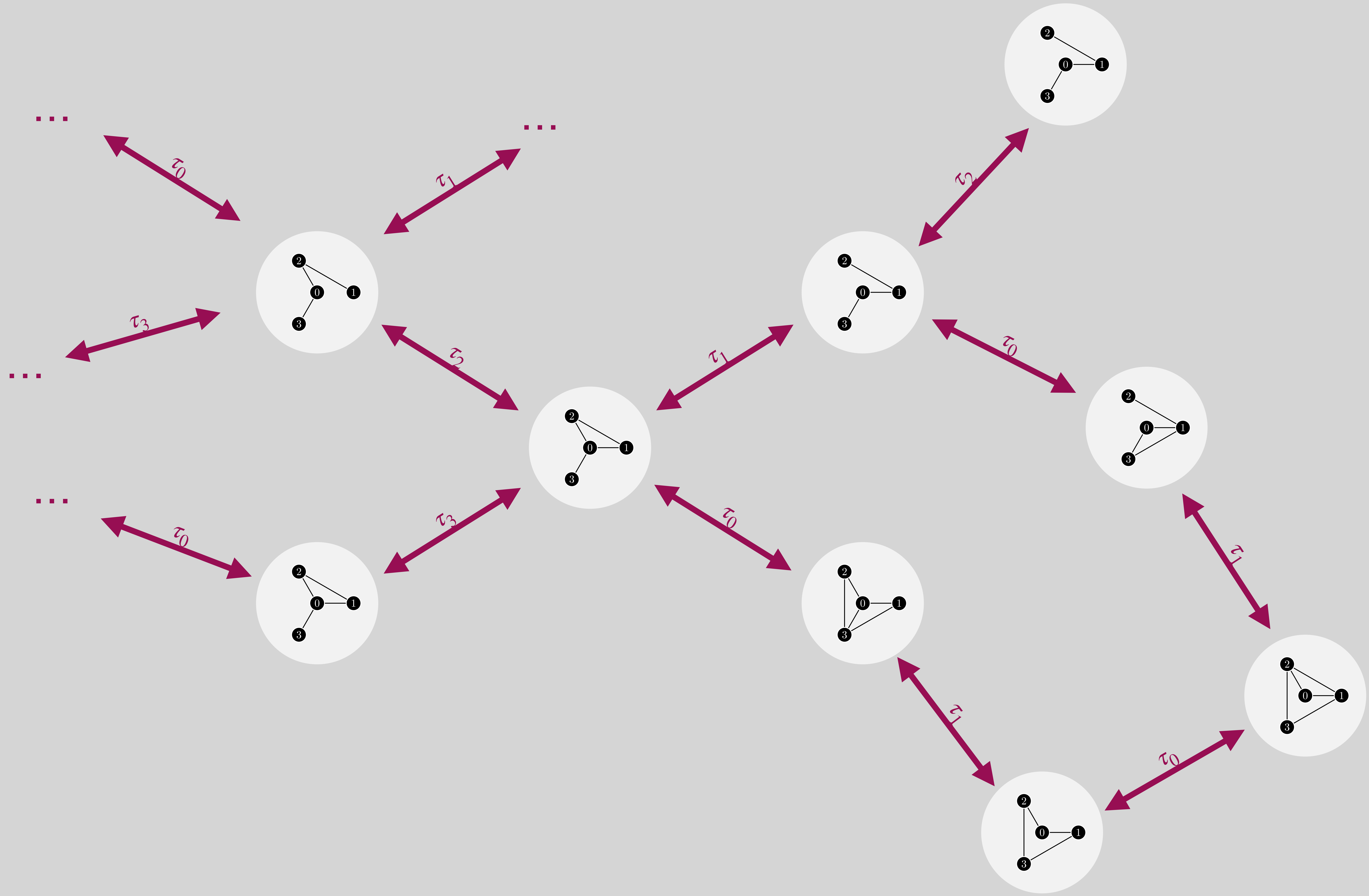
...
τ_1
τ_2
τ_3
τ_0
τ_1
τ_2
τ_0
τ_1
τ_1
τ_0



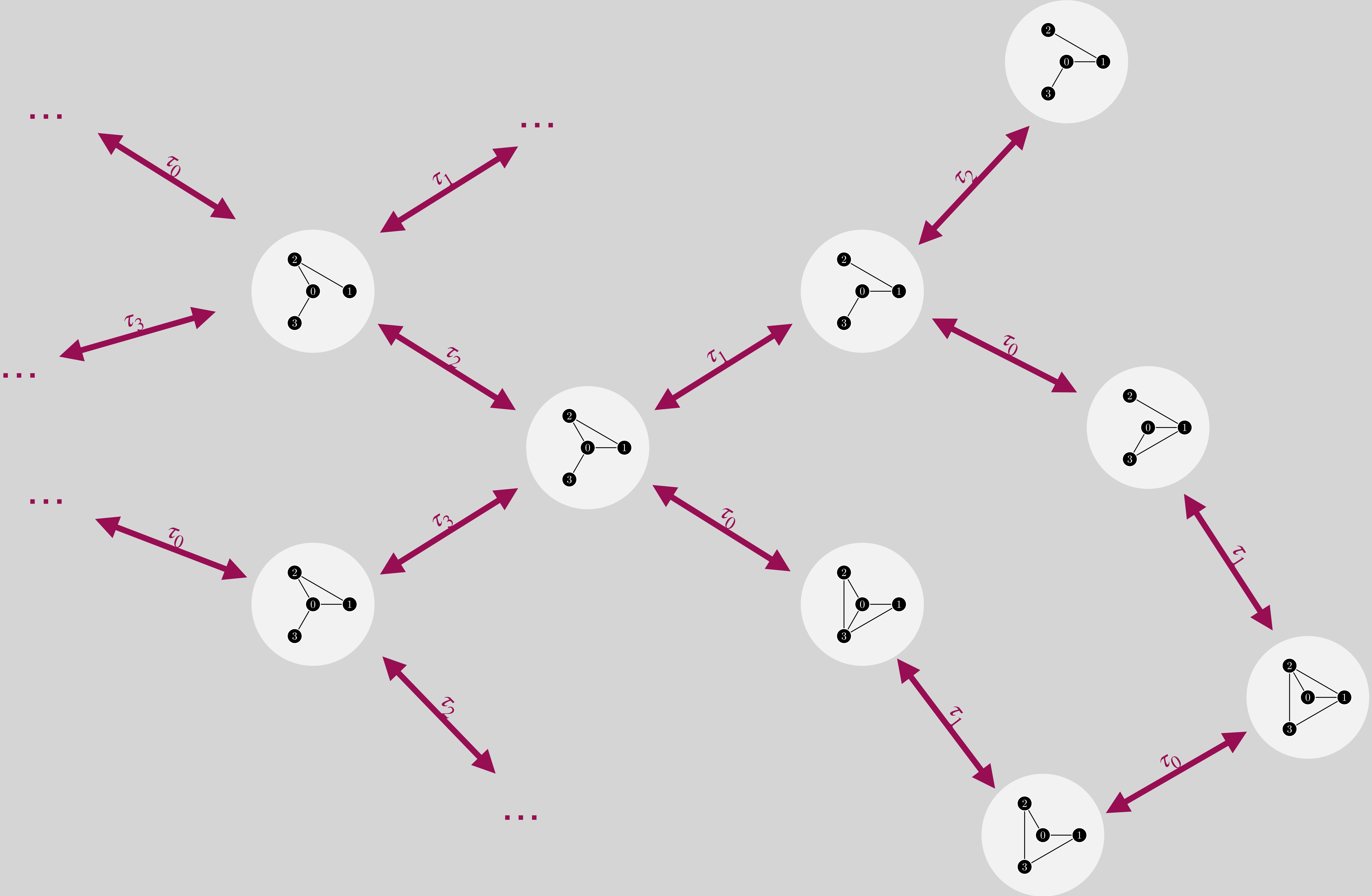
...
...
τ_0
τ_1
τ_2
τ_3
0
1
2
3



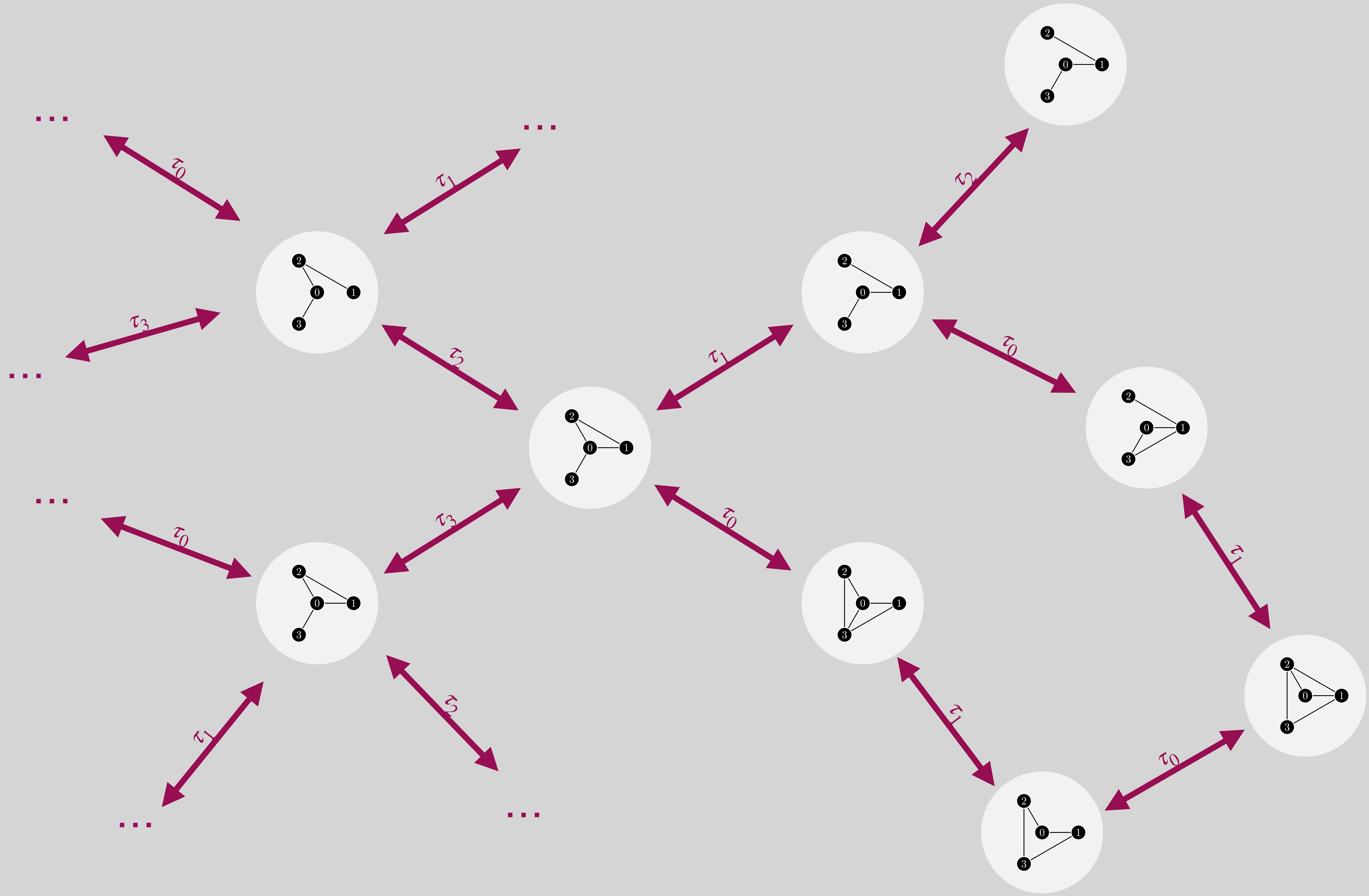
...
...
...
τ_0
τ_1
τ_2
τ_3
0
1
2
3



...
τ_0
τ_1
...
τ_3
...
τ_2
τ_3
...
τ_0
τ_1
τ_2
τ_0
τ_0
τ_1
τ_1
τ_0



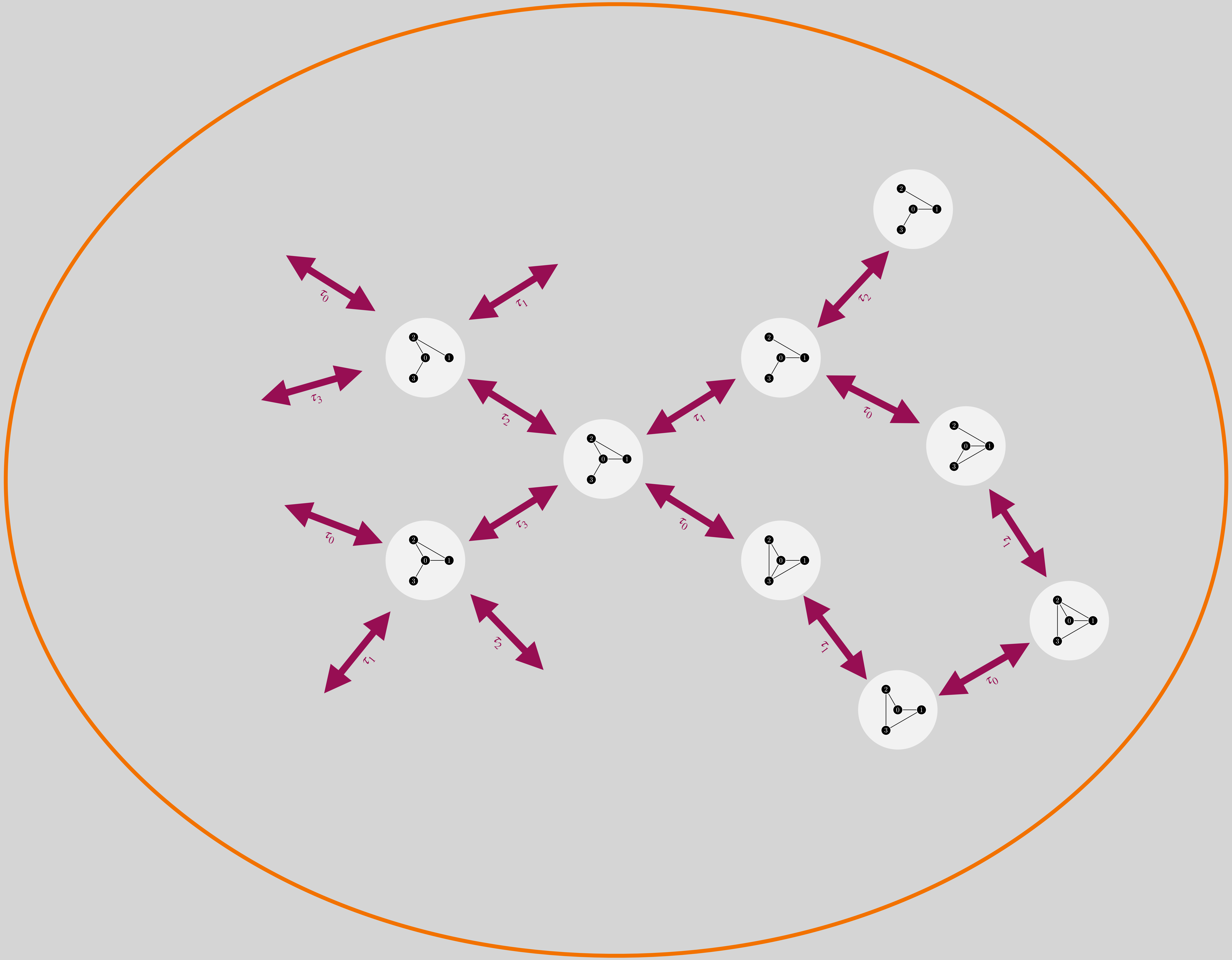
...
...
...
...
...
τ_0
τ_1
τ_2
τ_3
0
1
2
3

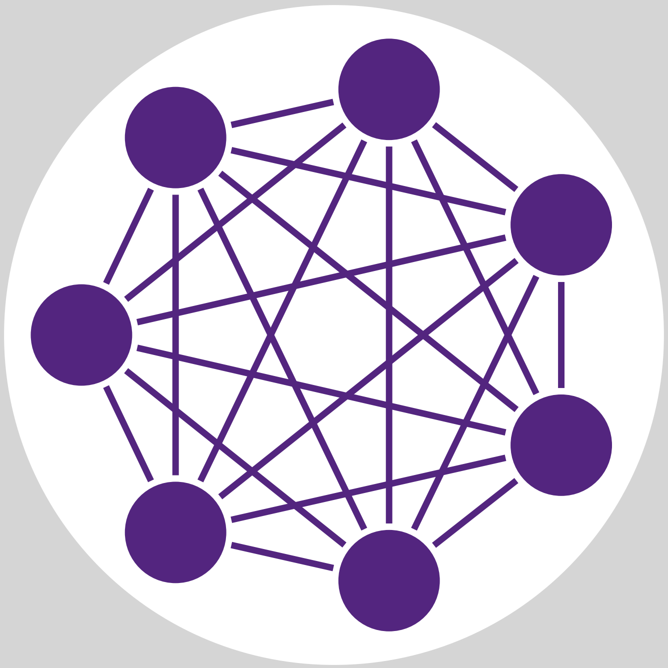


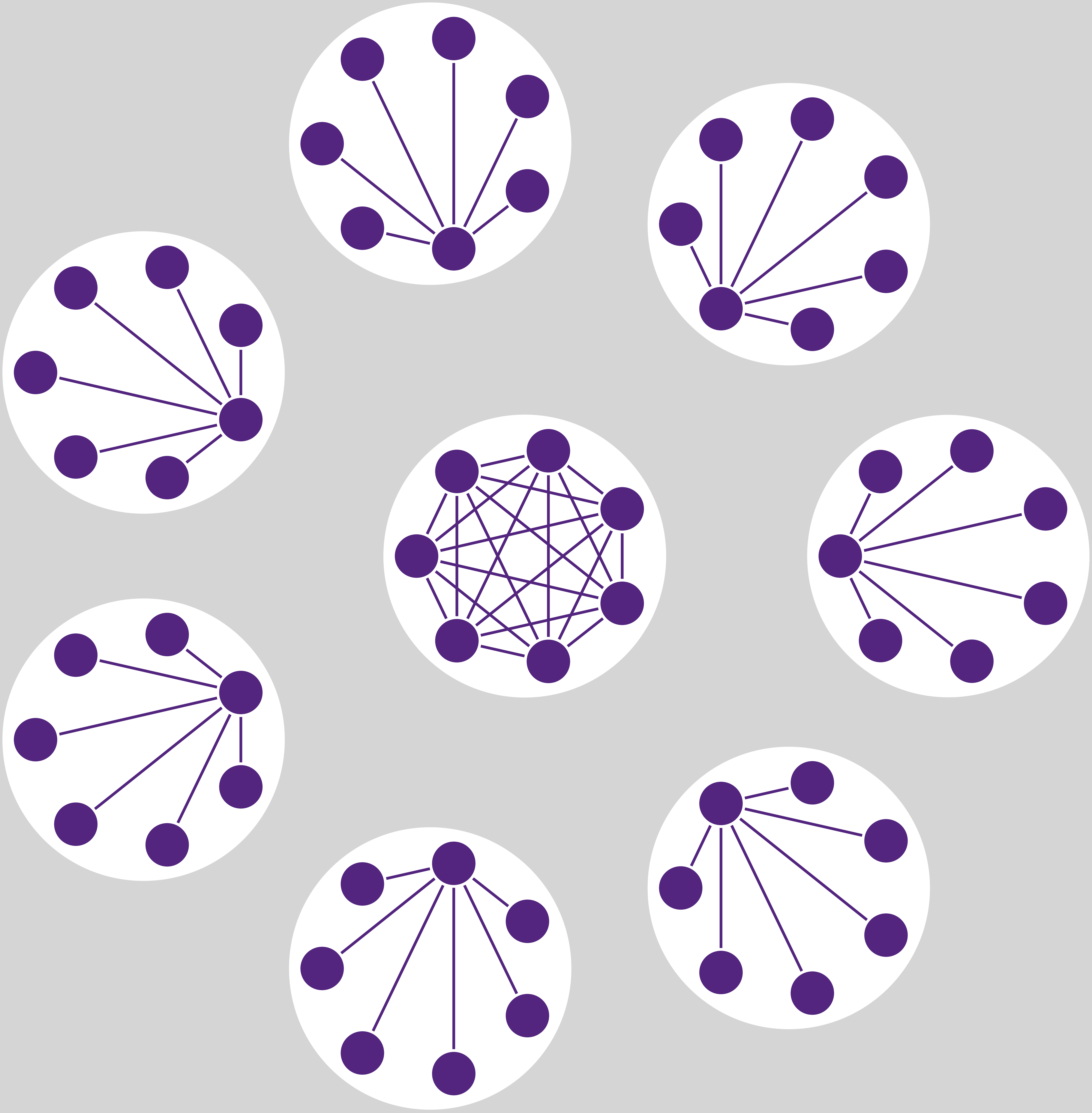
τ0
τ1
τ2
τ3

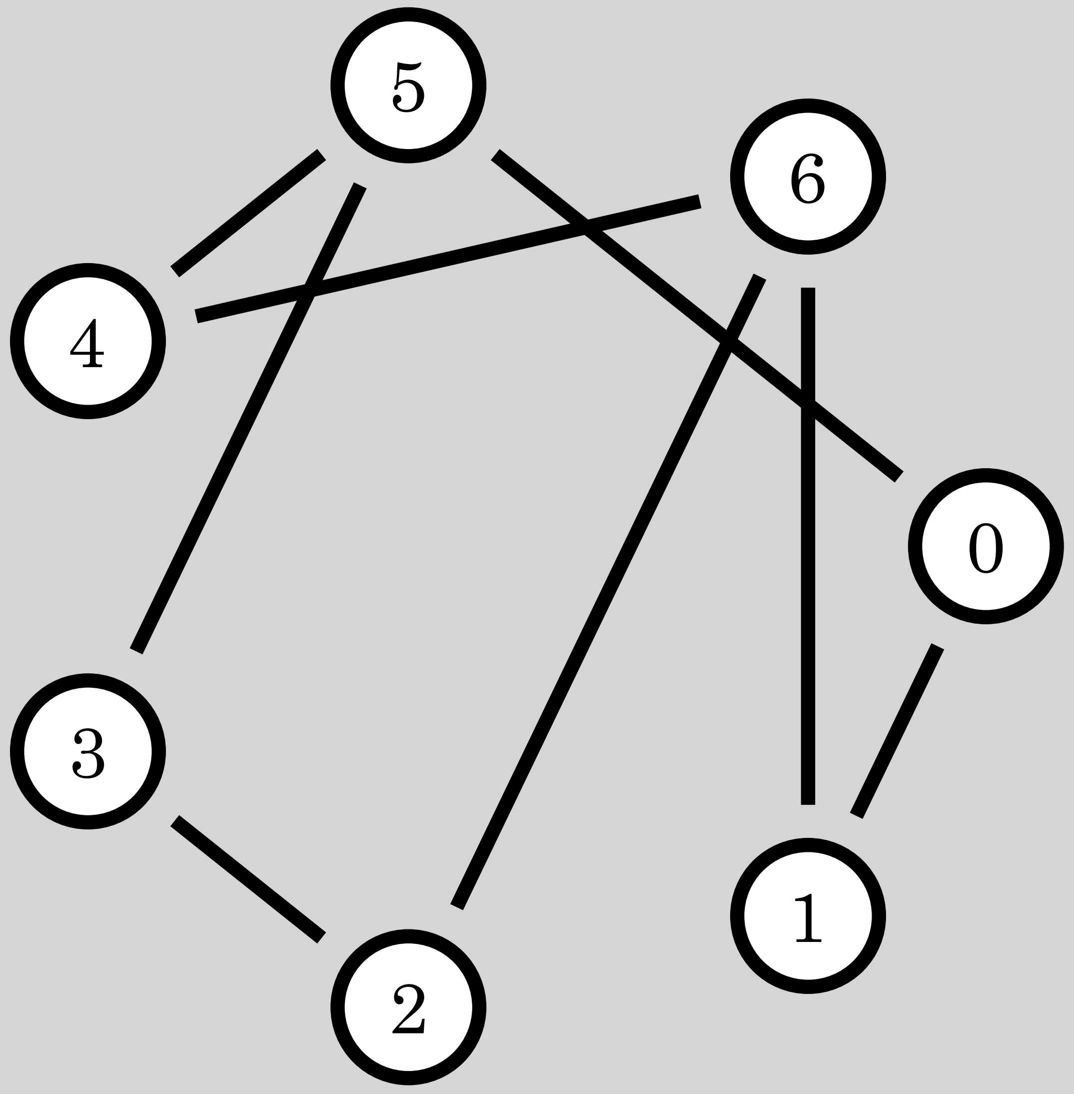
LC-orbit

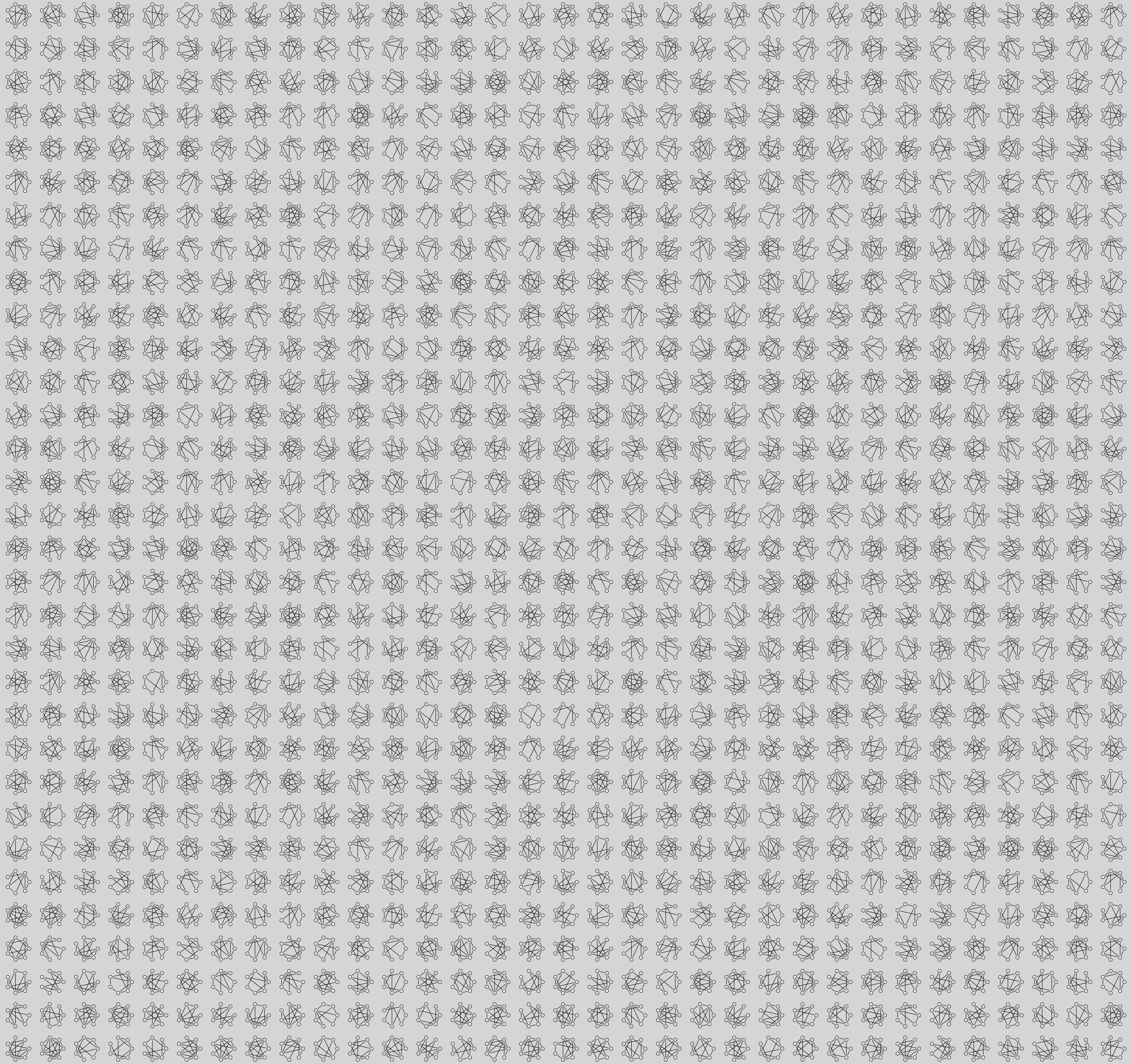
(*orbit*)








5
6
4
0
3
1
2



$$|G\rangle \xleftrightarrow{\text{Local operation*}} |G'\rangle$$

$$G \xleftrightarrow{\text{LC-orbit}} G'$$

* Only local *Clifford* operations

Orbit $\longrightarrow$ *Entanglement class*

Orbit → ***Entanglement class***

# Qubits	1	2	3	4	5	6	7	8	9	10
# Orbits	1	1	1	2	4	11	26	101	440	3132
# Orbits + permutations	1	1	1	4	27	312	6103	2E+05	1E+07	?

Measurements

Measurements

Measurements in Z basis

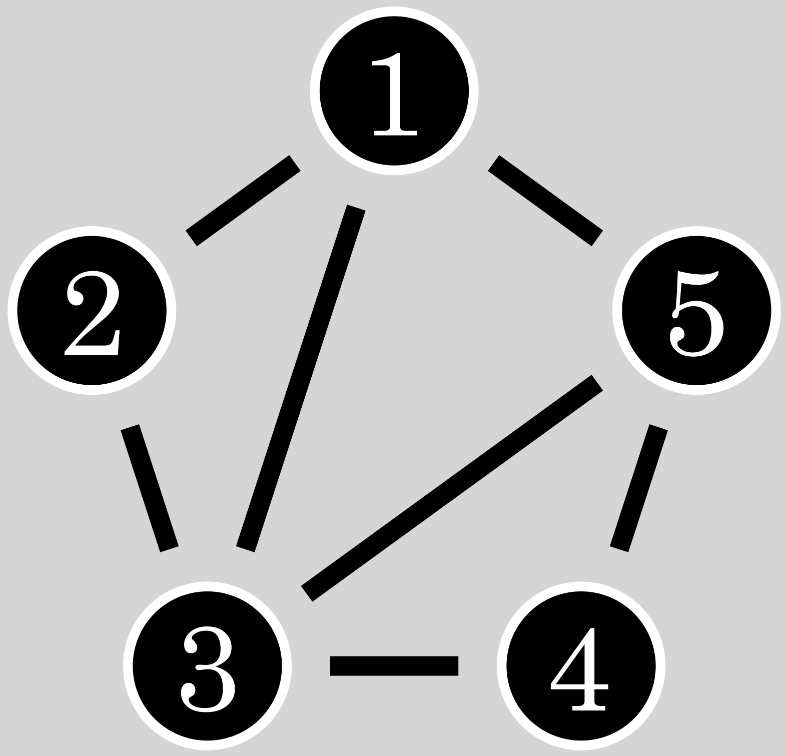
Measurements in Z basis

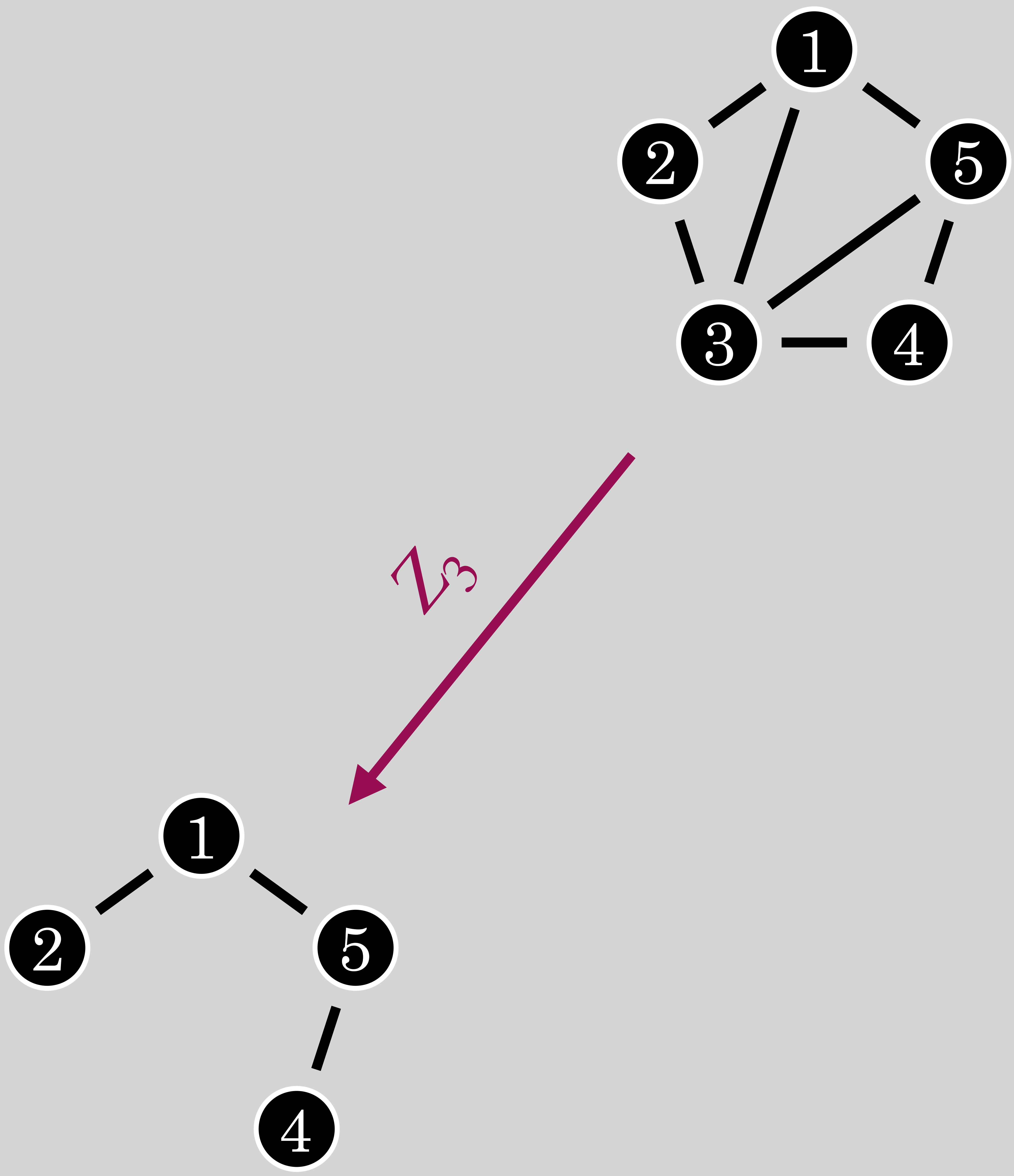
$$|G\rangle \rightarrow |G\backslash k\rangle$$

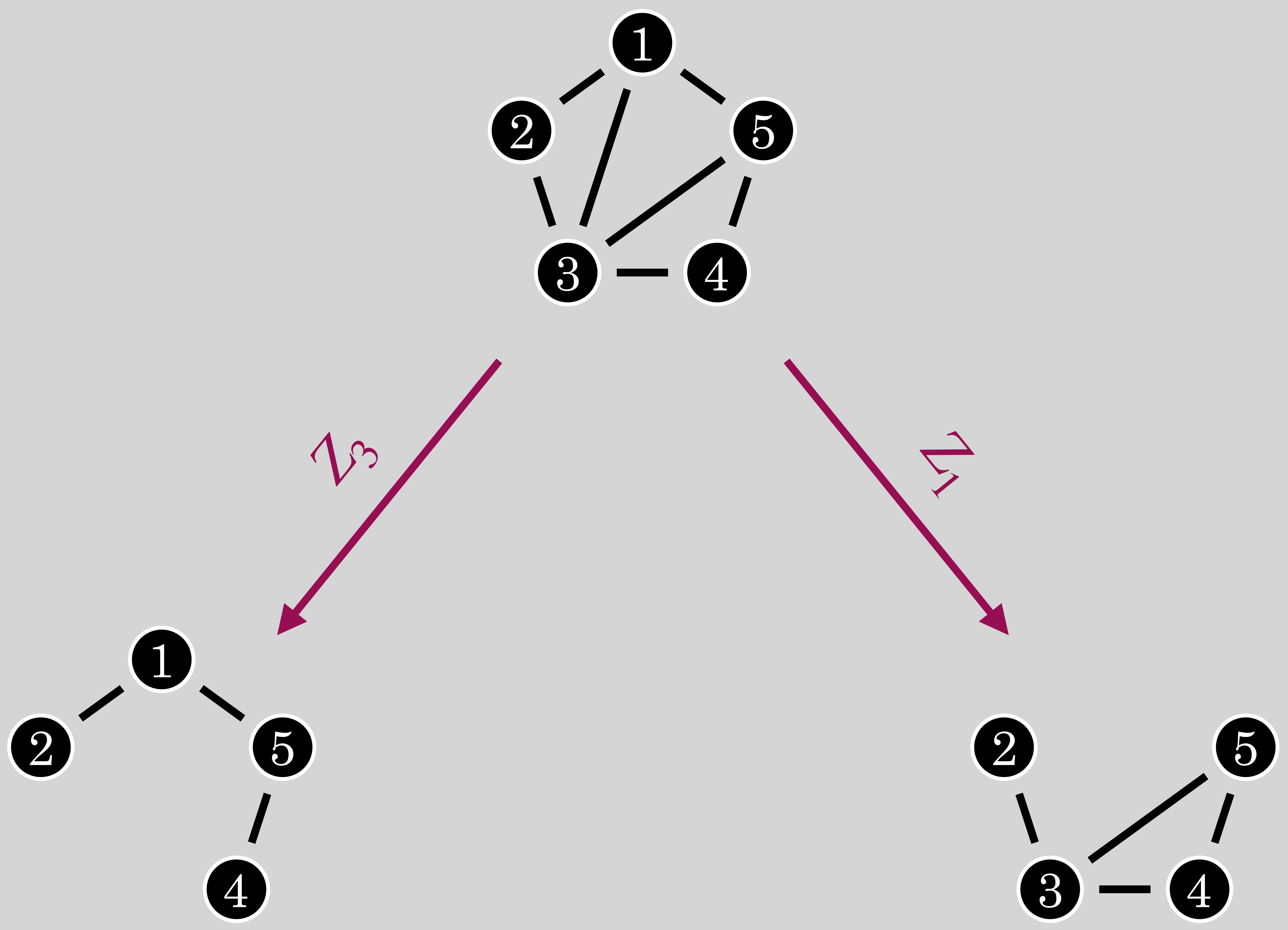
Measurements in Z basis

$$|G\rangle \to |G\backslash k\rangle$$

…. and some local Cliffords


1
2
5
3
4


1
2
5
3
4
v_3
1
2
5
4



1
2
5
3
4
Z_3
Z_1
1
2
5
4
2
5
3
4

Other bases

Other bases

$$Y = X^{-\frac{1}{2}} Z X^{\frac{1}{2}}$$

$$X = Z^{-\frac{1}{2}} X^{-\frac{1}{2}} Z X^{\frac{1}{2}} Z^{\frac{1}{2}}$$

Other bases

$$Y = X^{-\frac{1}{2}} Z X^{\frac{1}{2}}$$

$$X = Z^{-\frac{1}{2}} X^{-\frac{1}{2}} Z X^{\frac{1}{2}} Z^{\frac{1}{2}}$$

…. and some local Cliffords

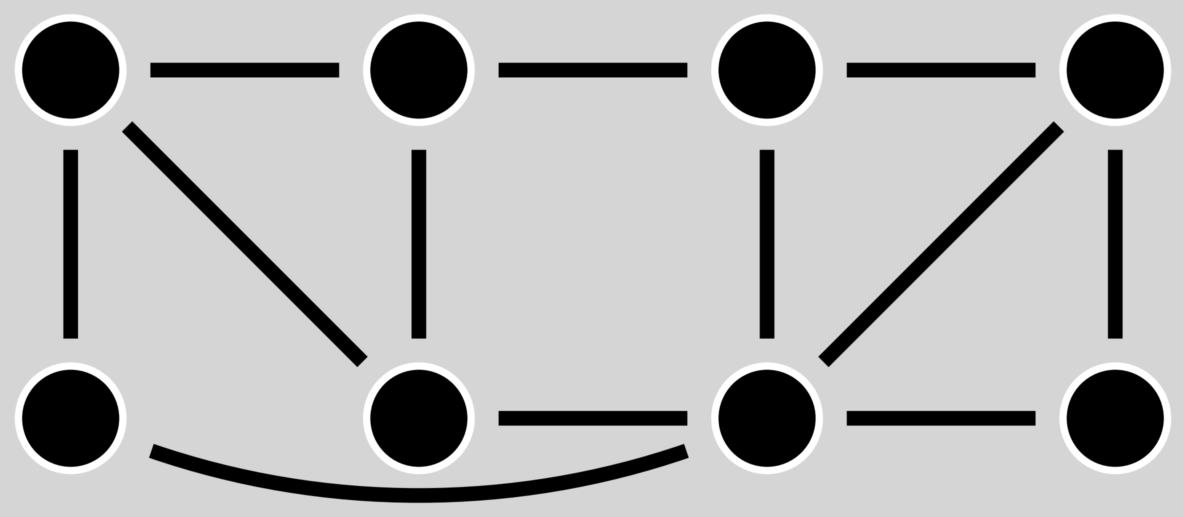
Other bases

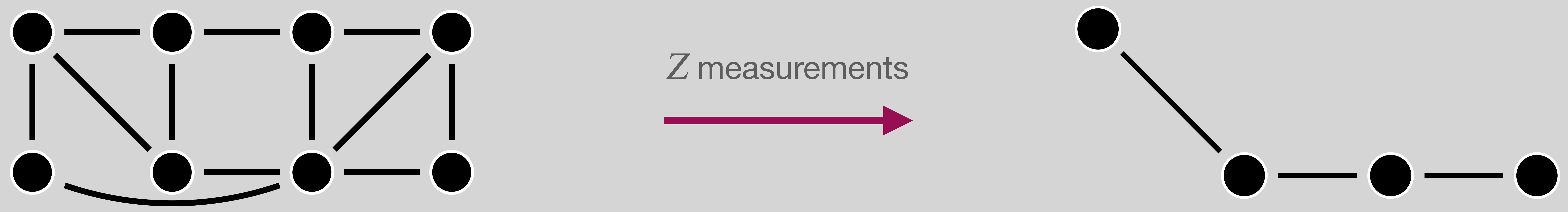
$$Y = X^{-\frac{1}{2}} Z X^{\frac{1}{2}}$$

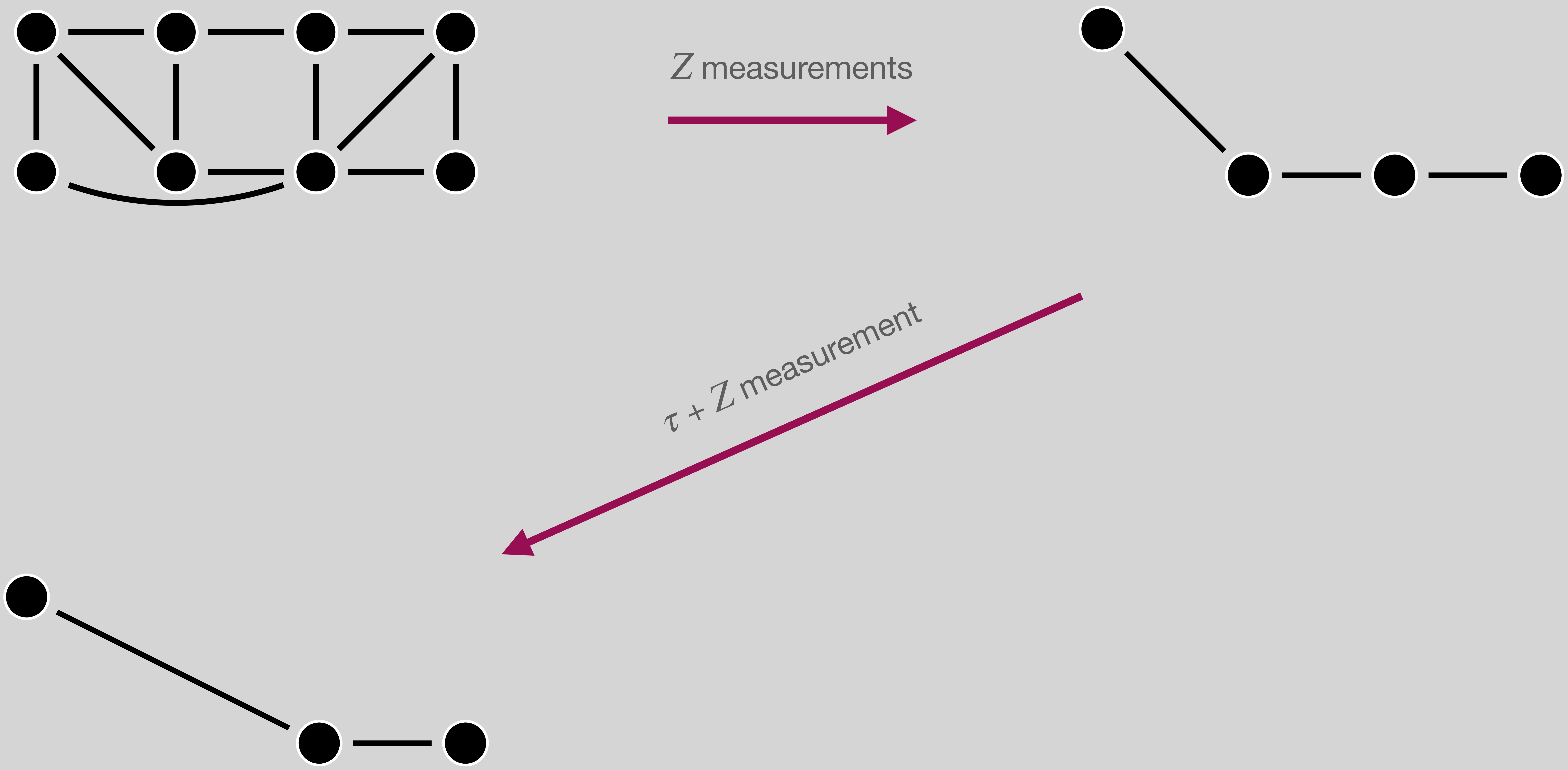
$$X = Z^{-\frac{1}{2}} X^{-\frac{1}{2}} Z X^{\frac{1}{2}} Z^{\frac{1}{2}}$$

Local Cliffords & Z measurements

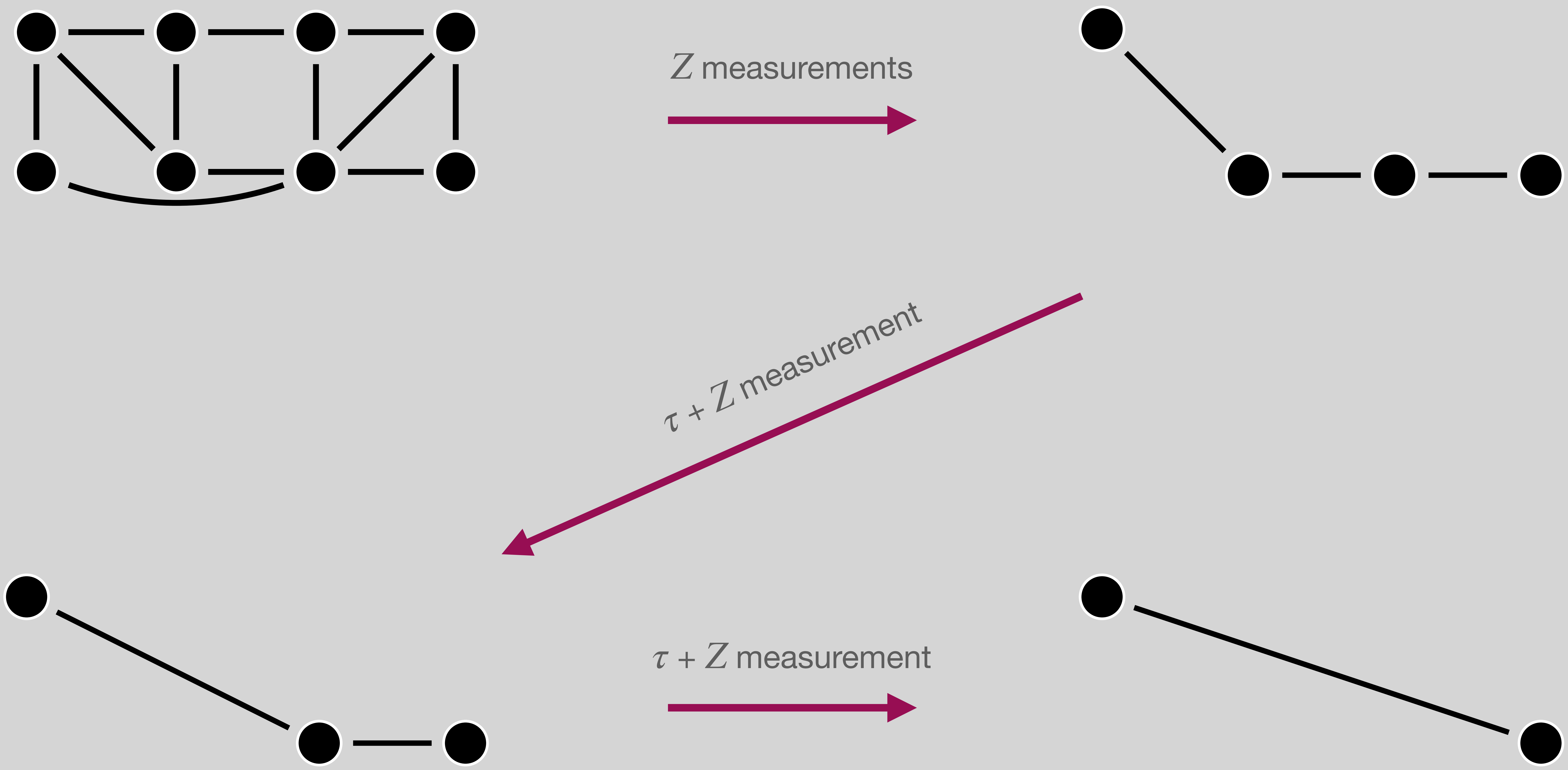
…. and some local Cliffords




Z measurements



Z measurements
τ + Z measurement



Z measurements
$\tau + Z$ measurement
$\tau + Z$ measurement

Powerful graphic tools

Powerful graphic tools

But has its limitations

Questions - or coffee