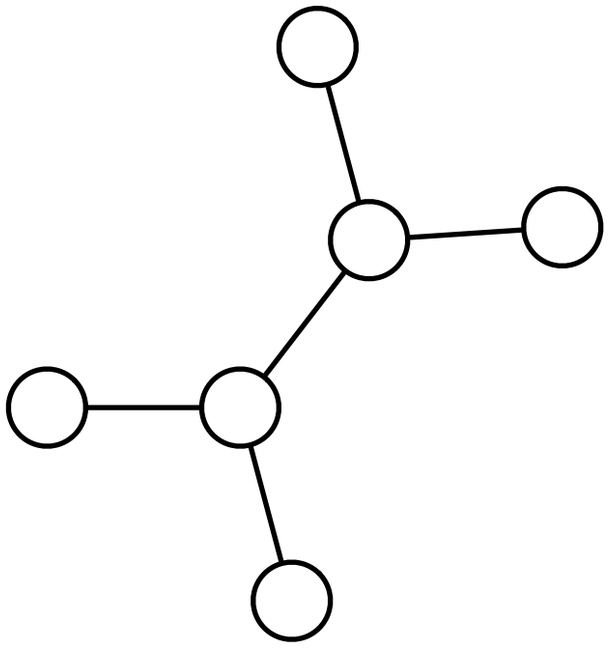
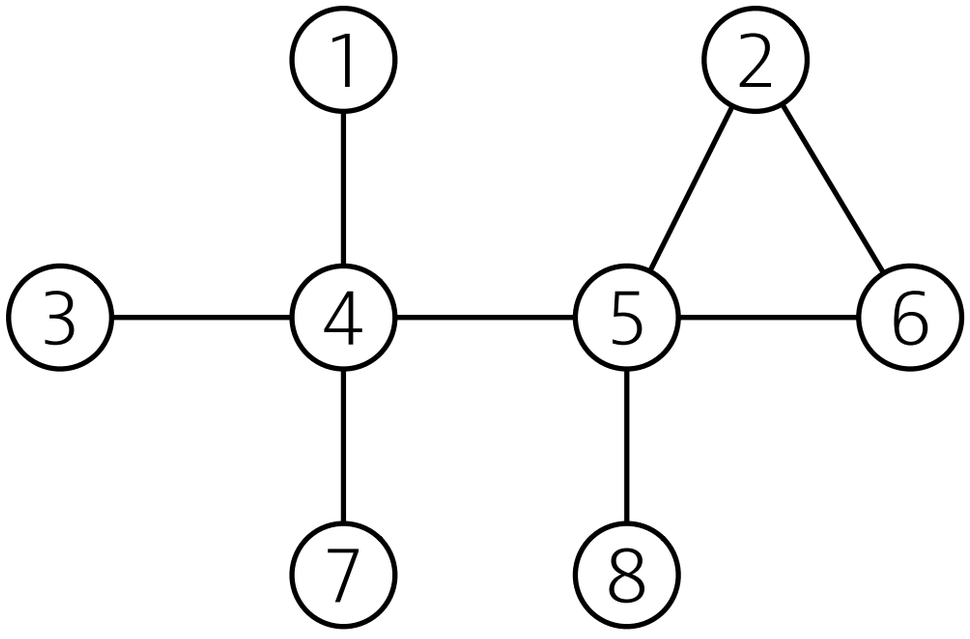
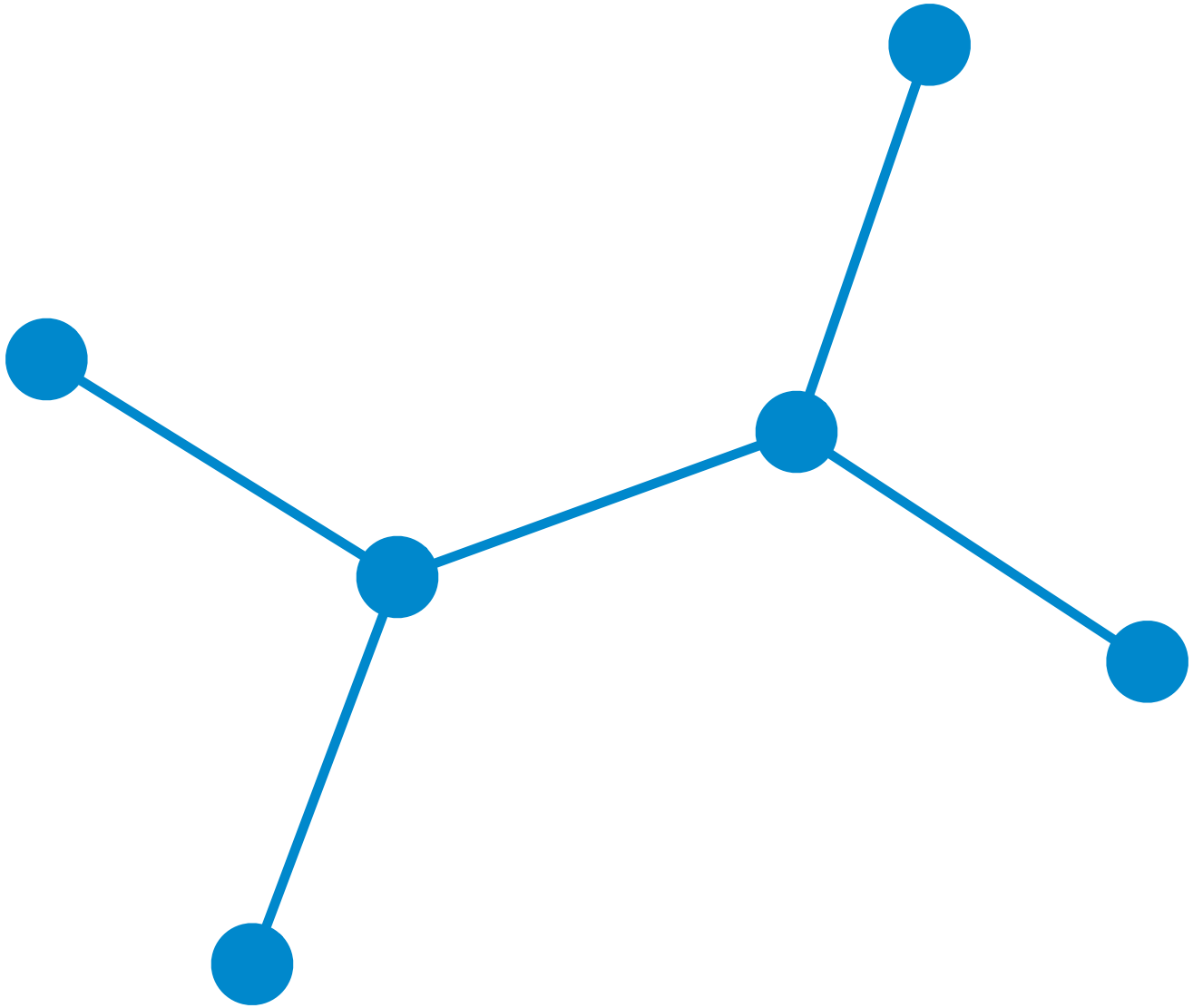
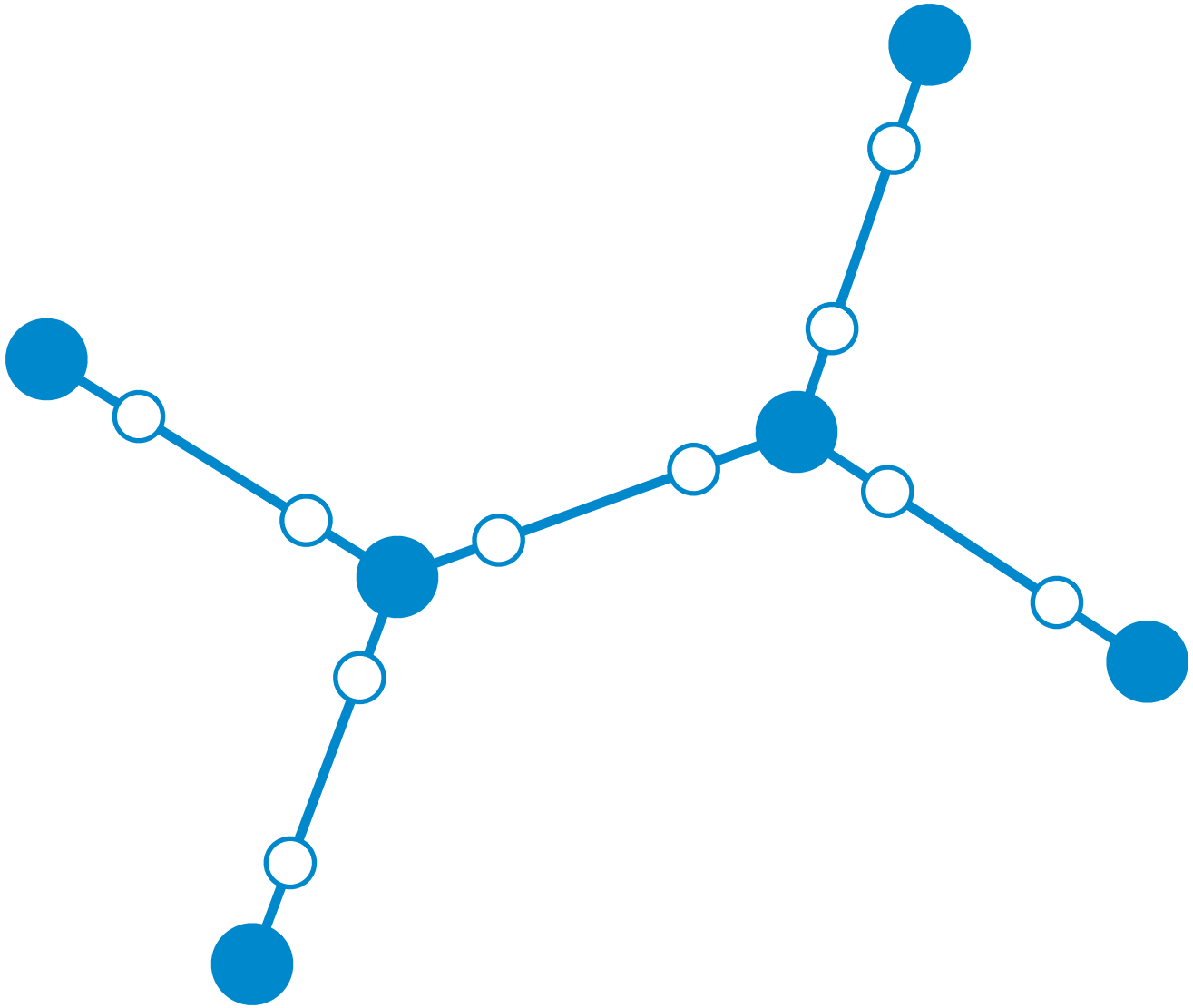
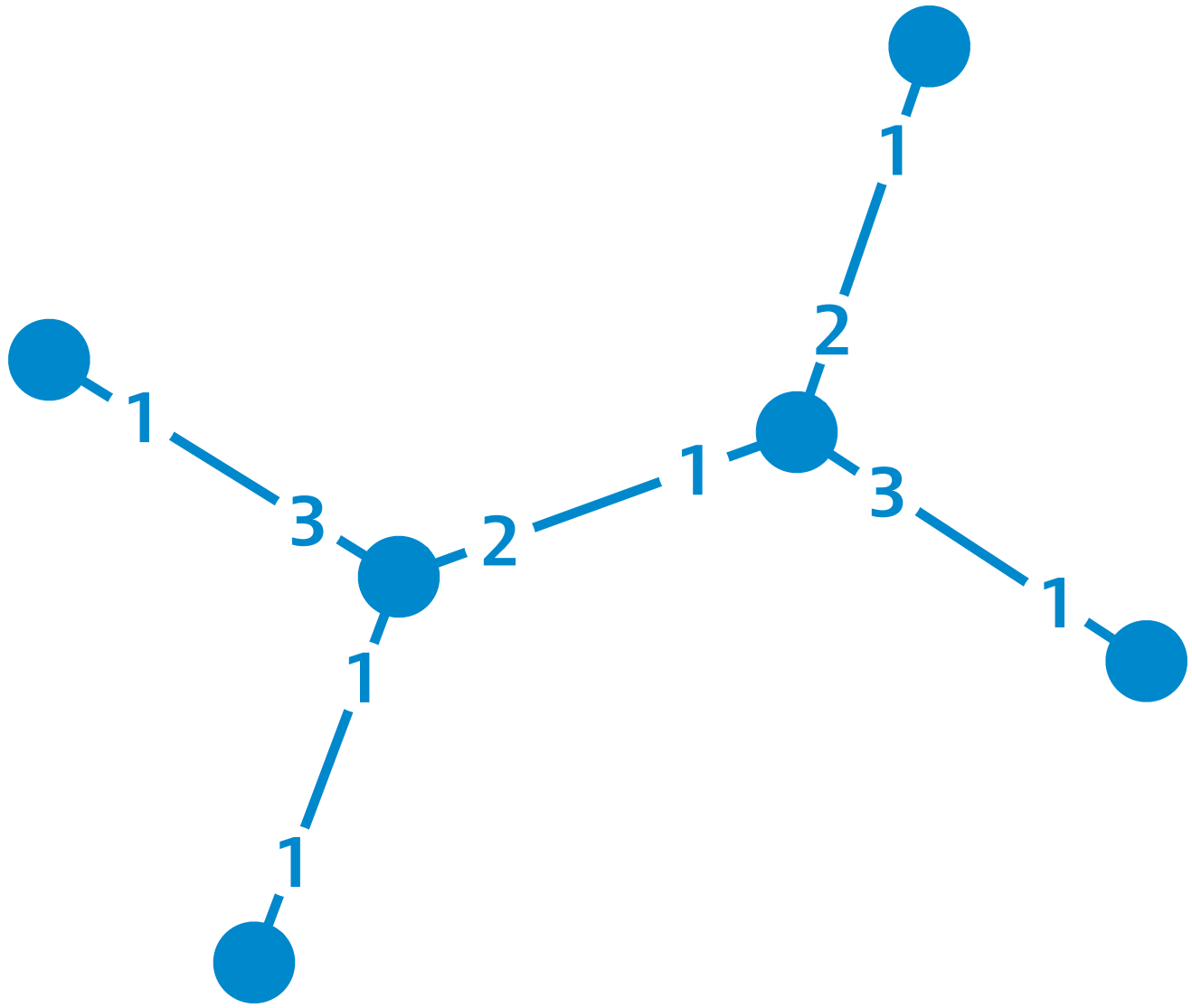
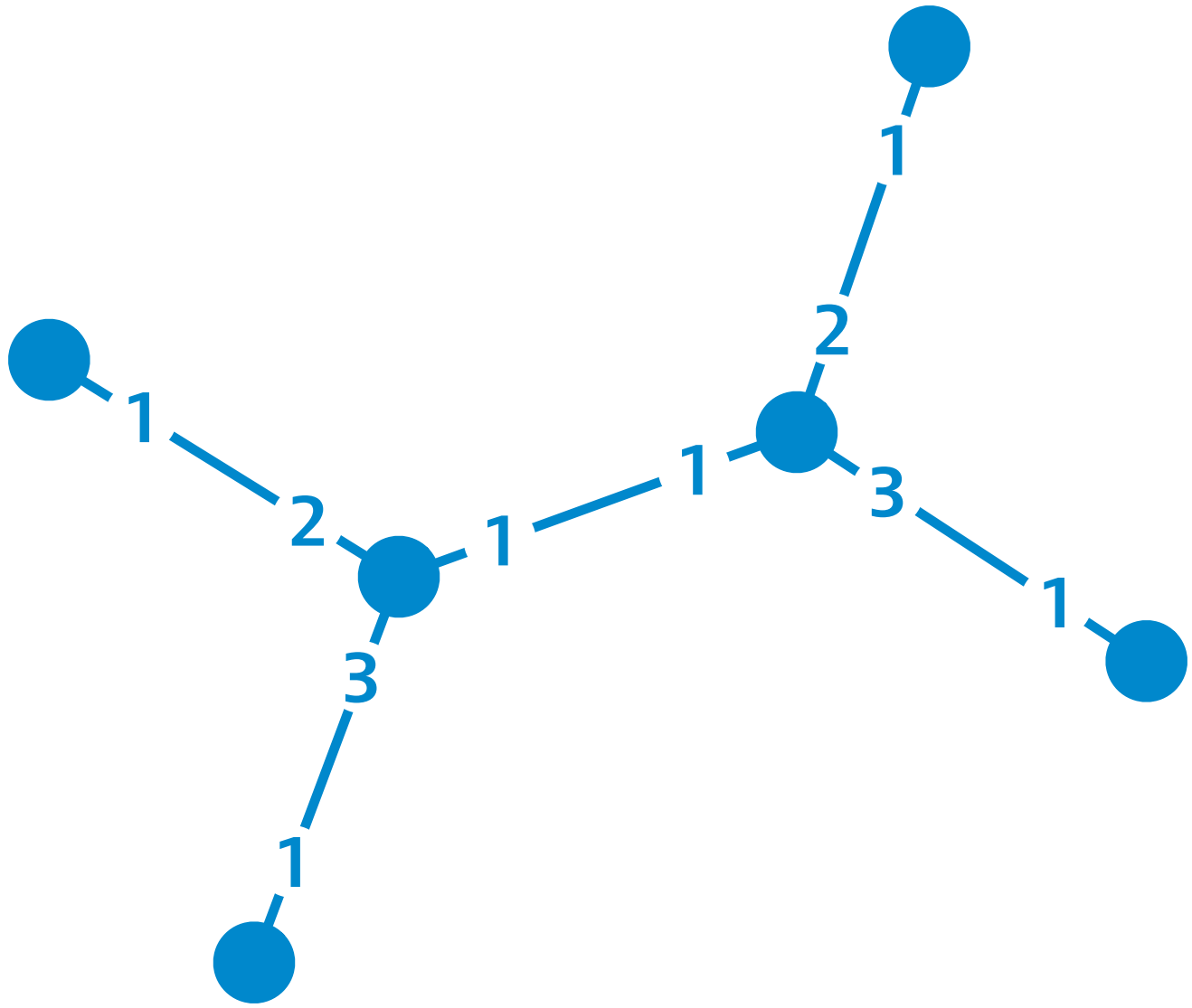


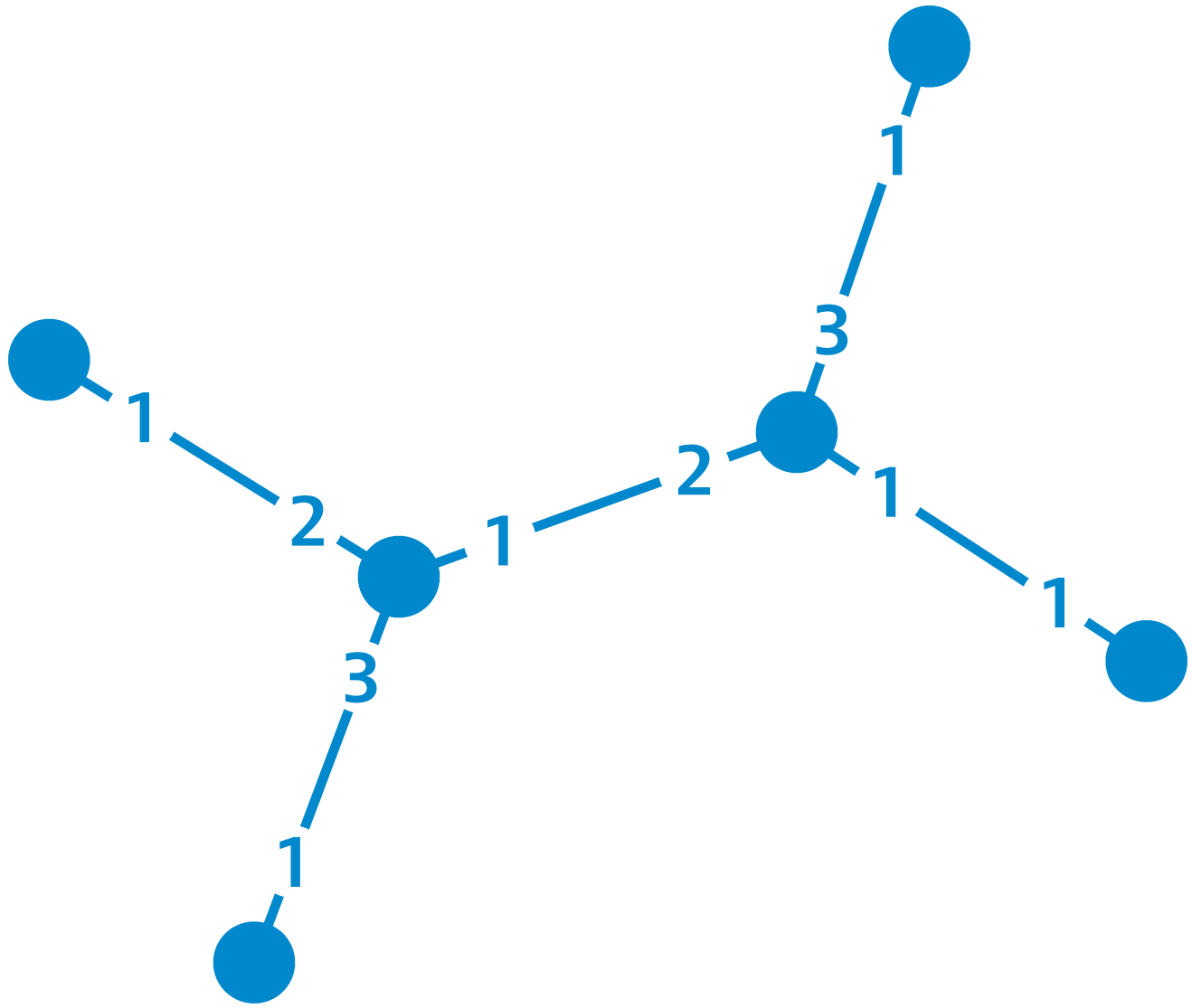

1
2
3
4
5
6
7
8

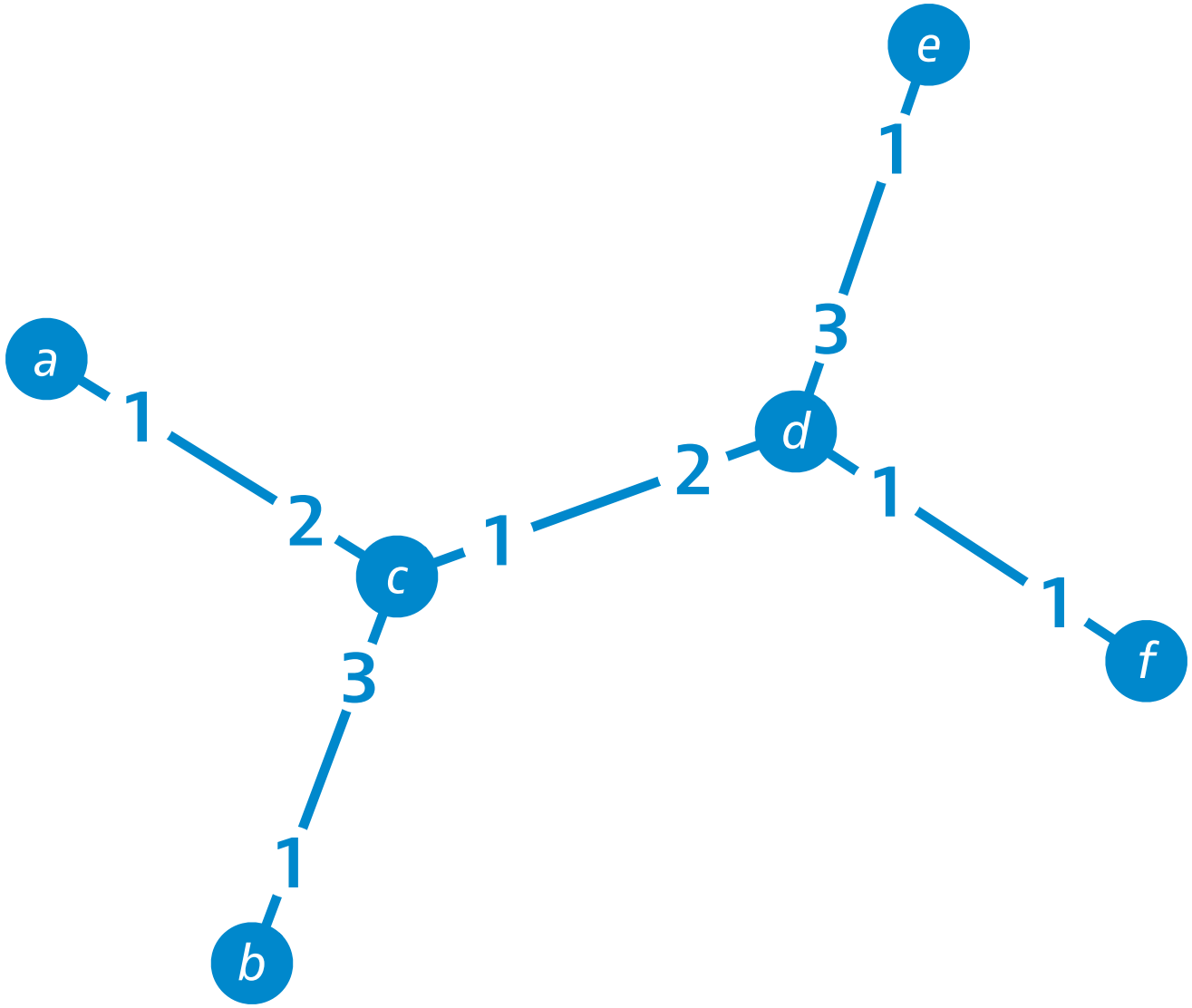


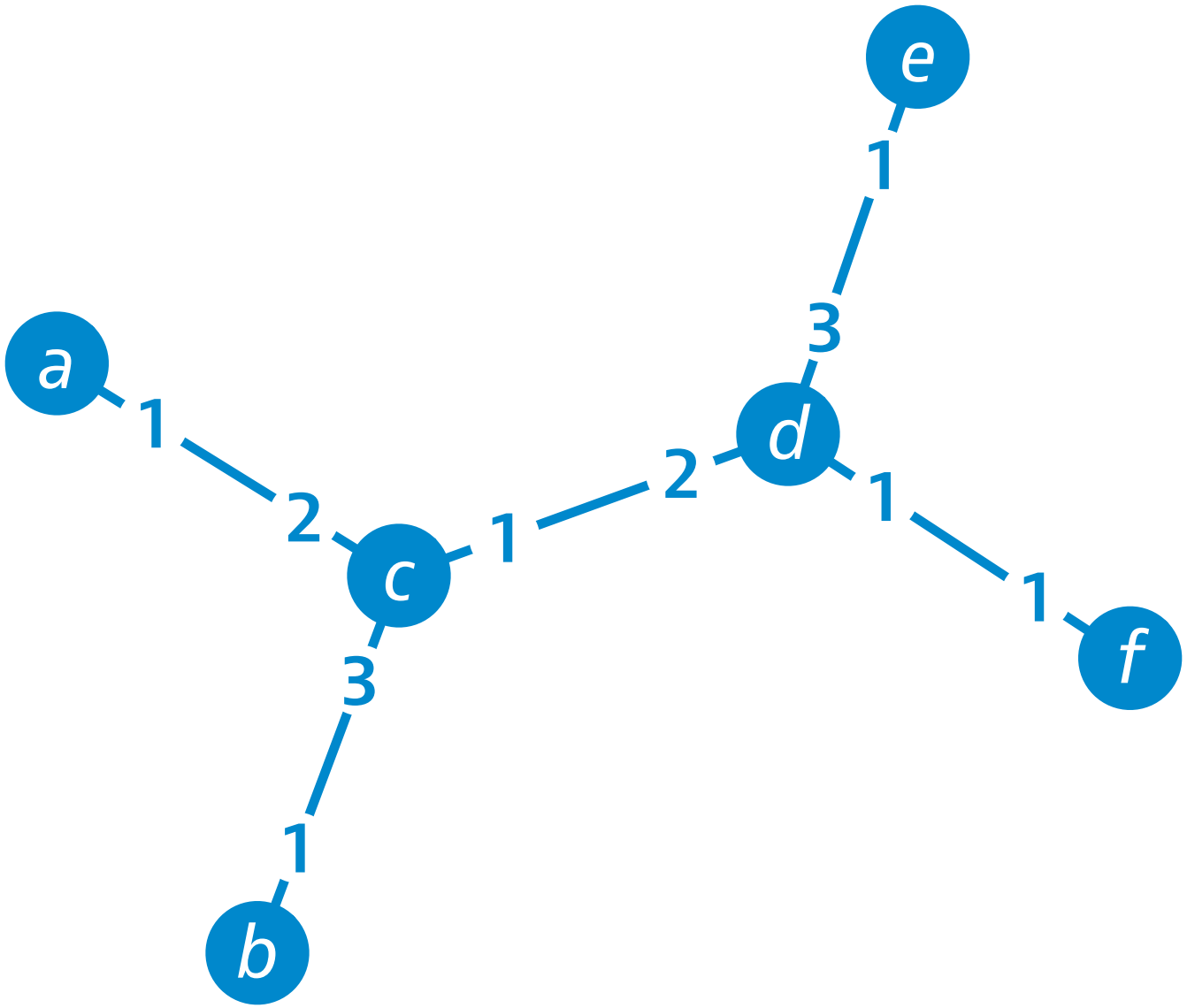


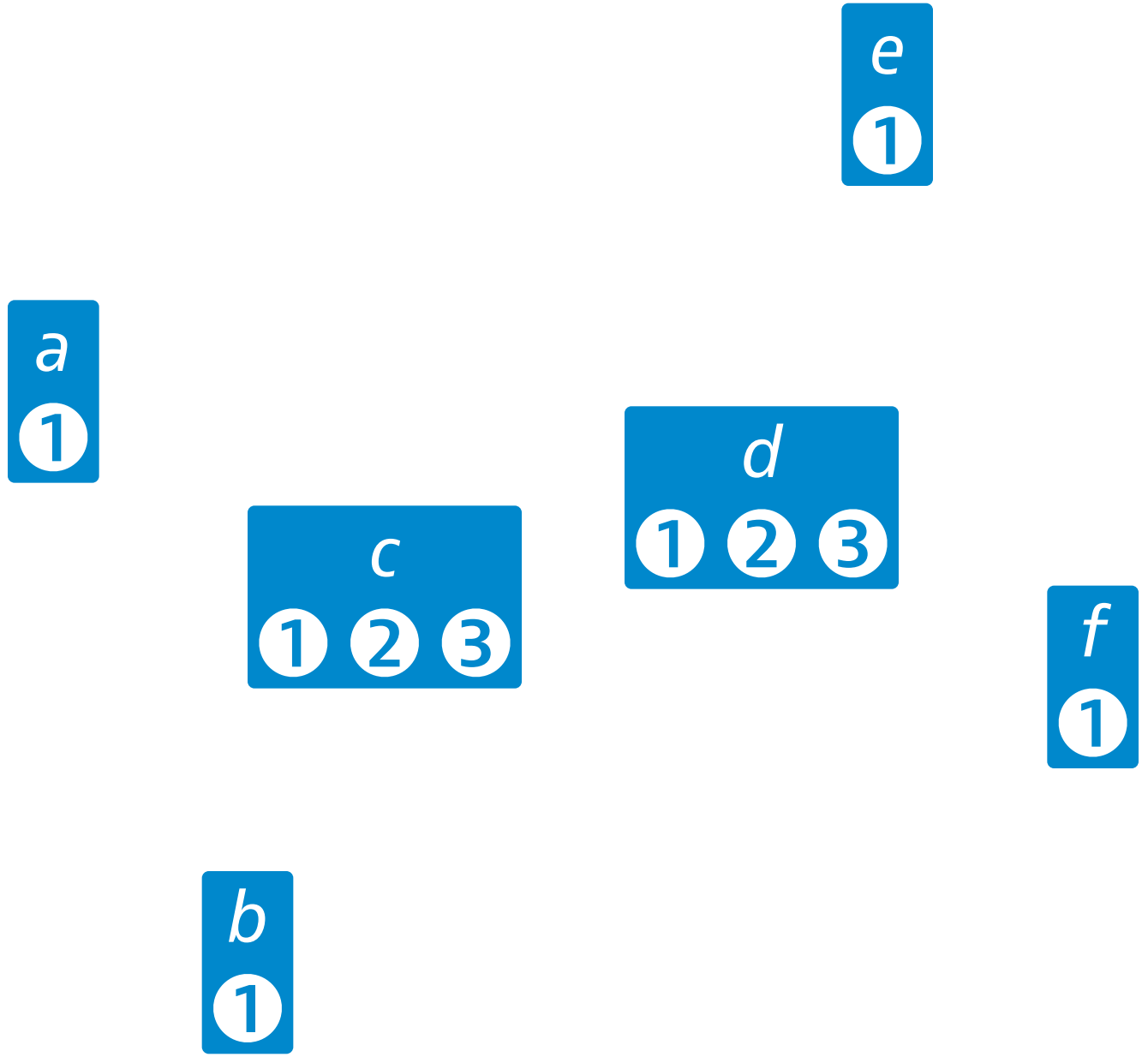

1
2
1
3
1
2
3
1
1
1

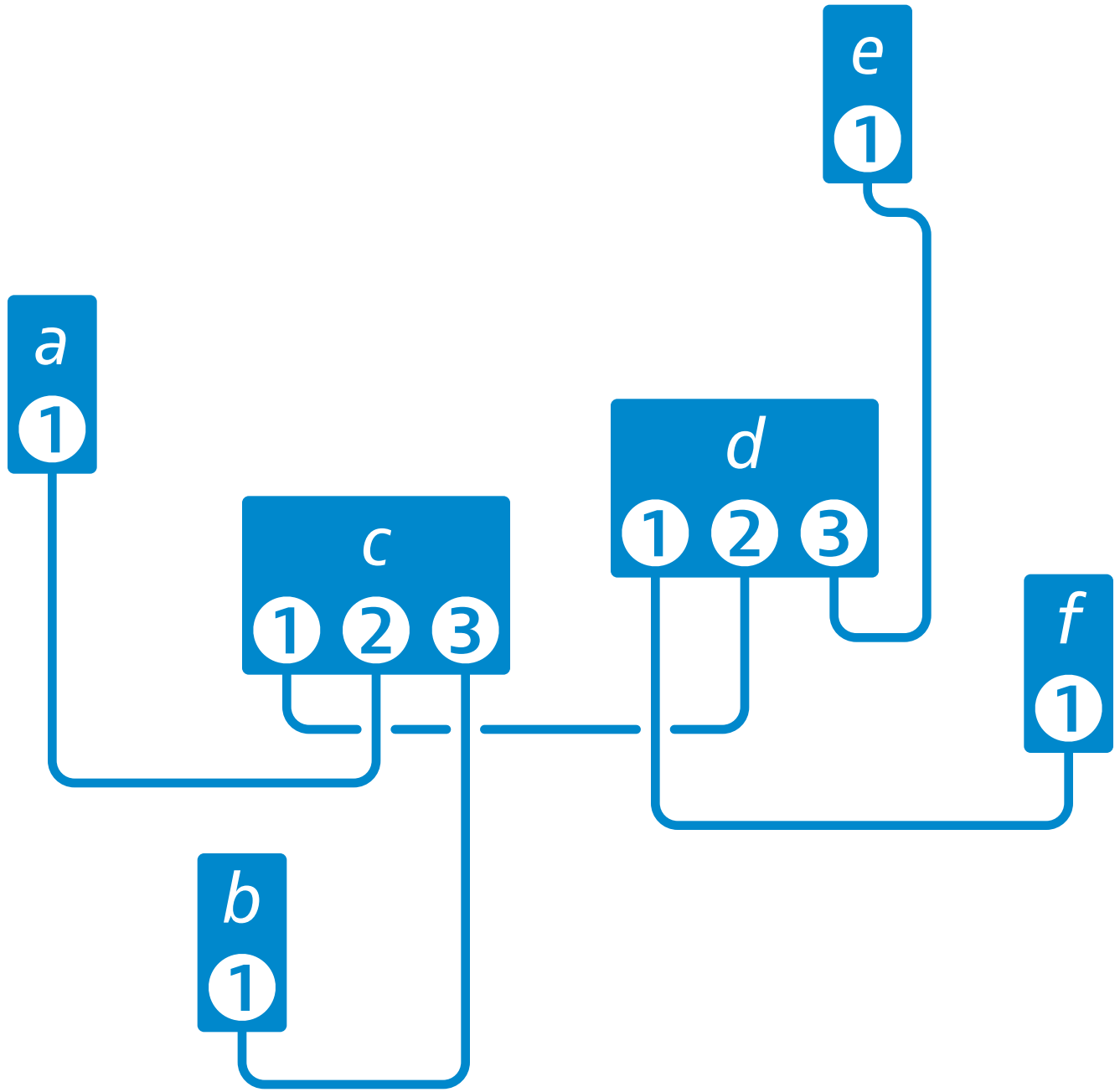

1
2
1
1
3
1
2
1
3
1

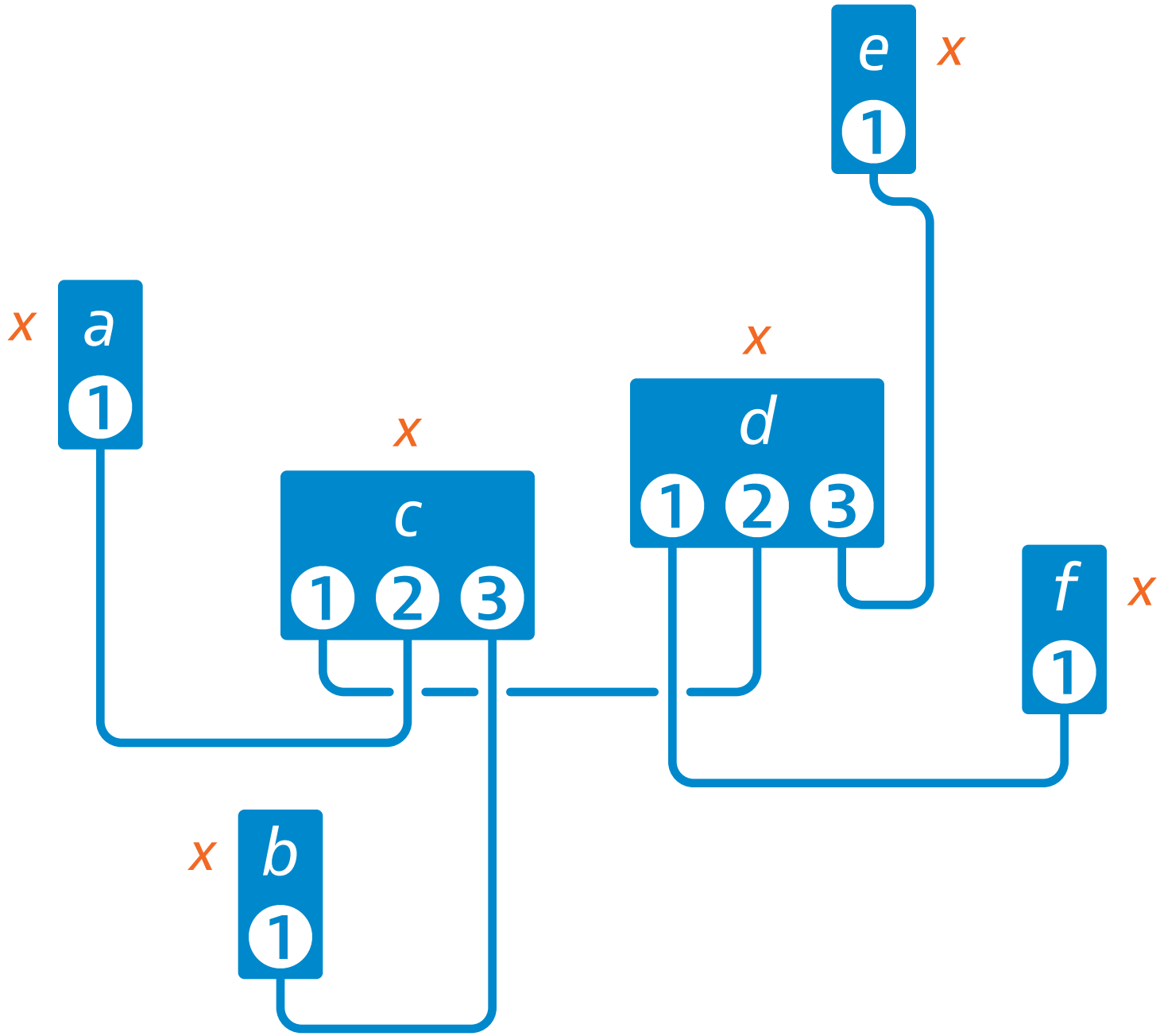

1
3
1
2
1
2
1
1
3
1

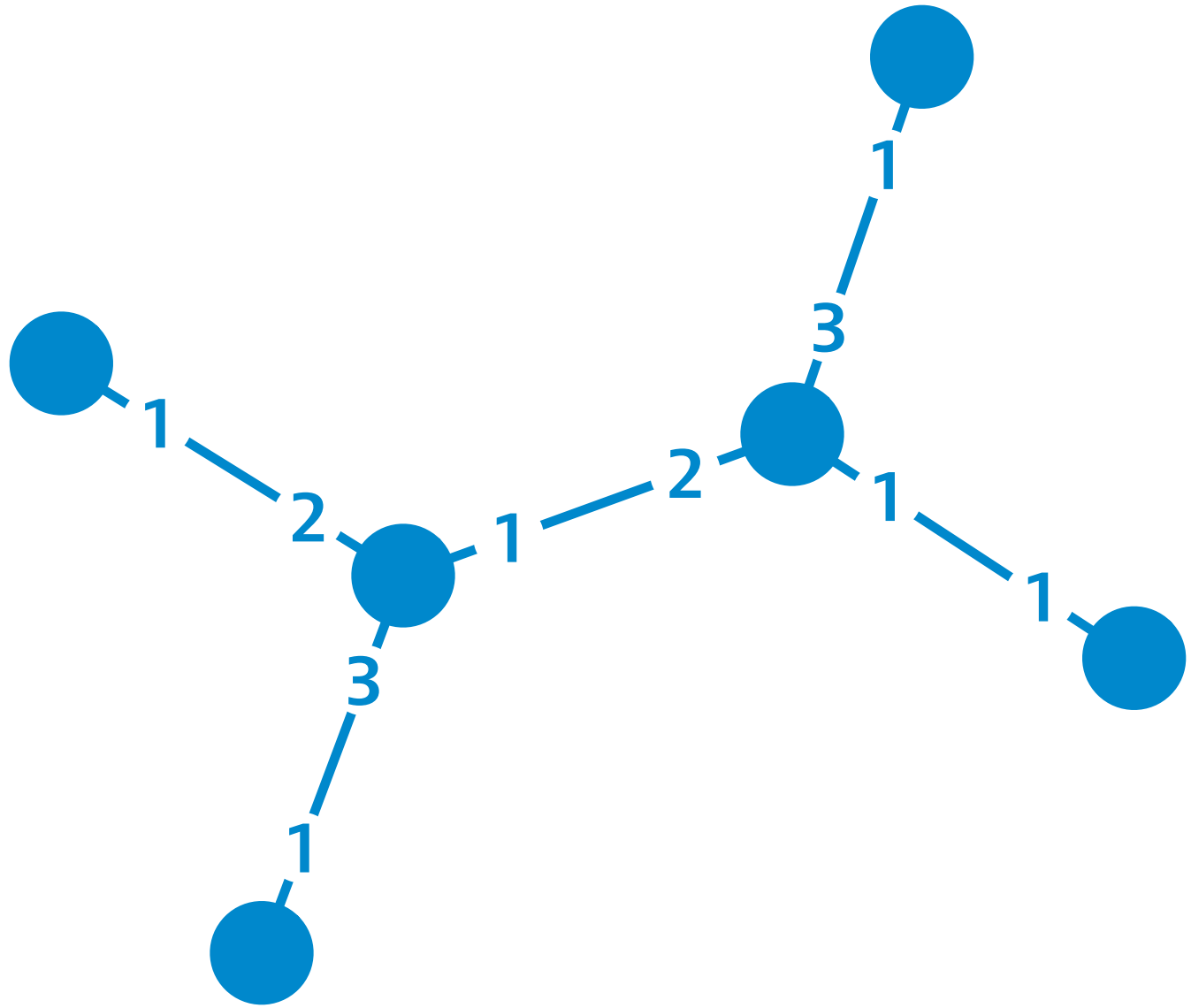

e
1
3
a
1
d
2
1
2
1
1
c
3
f
1
b

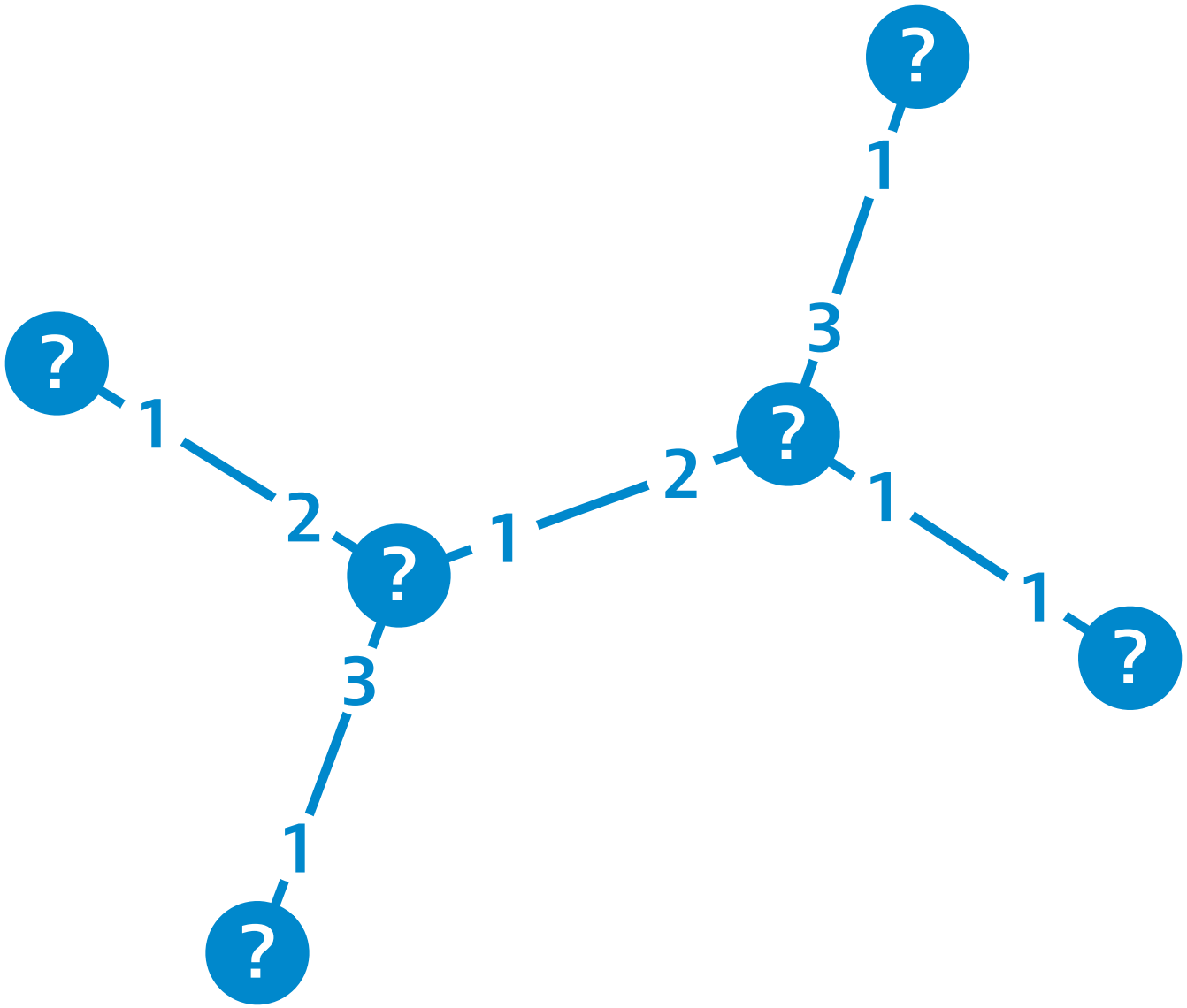

e
1
3
a
1
d
2
2
1
1
c
1
f
3
1
b

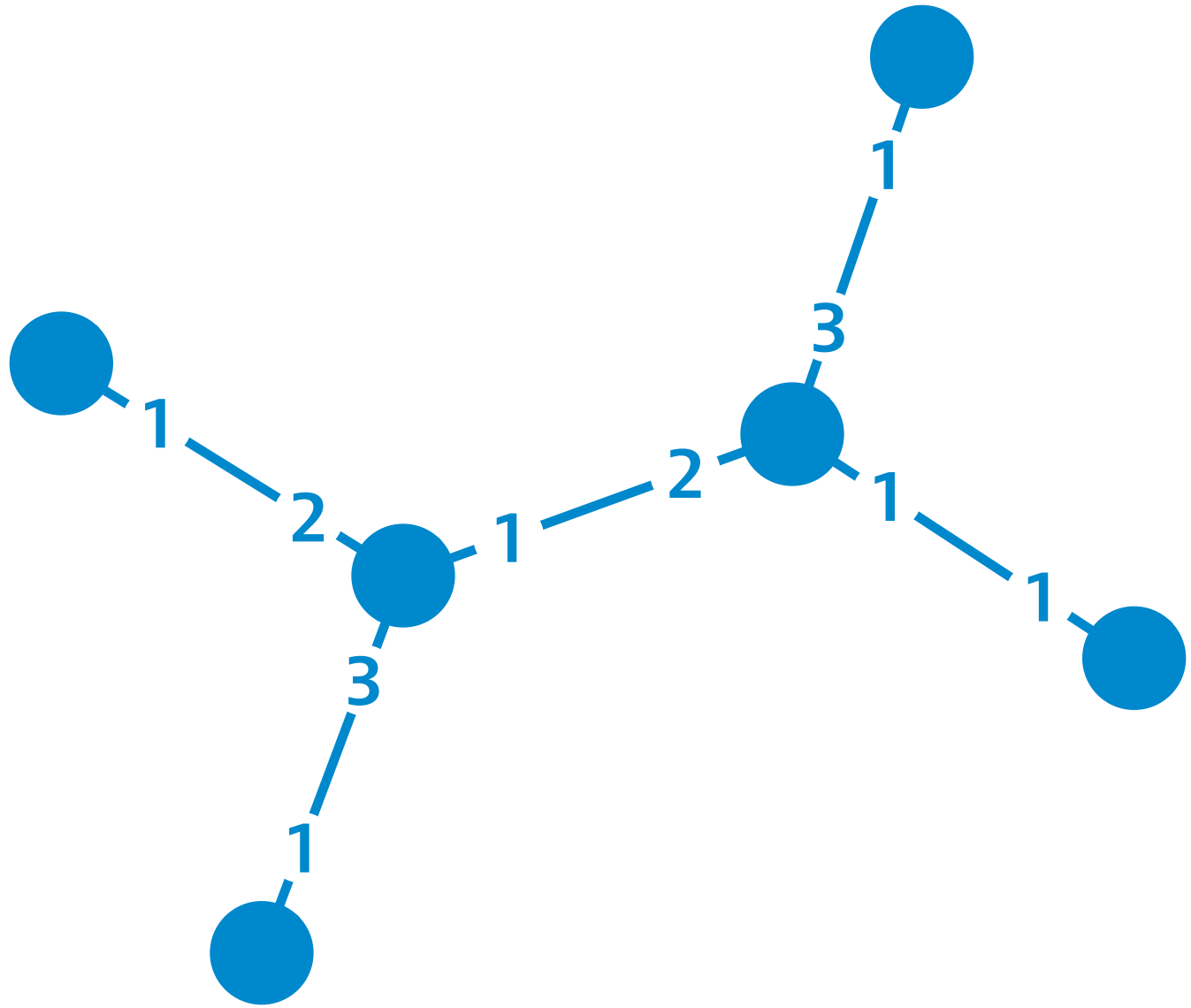

e
1
a
1
d
1 2 3
c
1 2 3
f
1
b
1

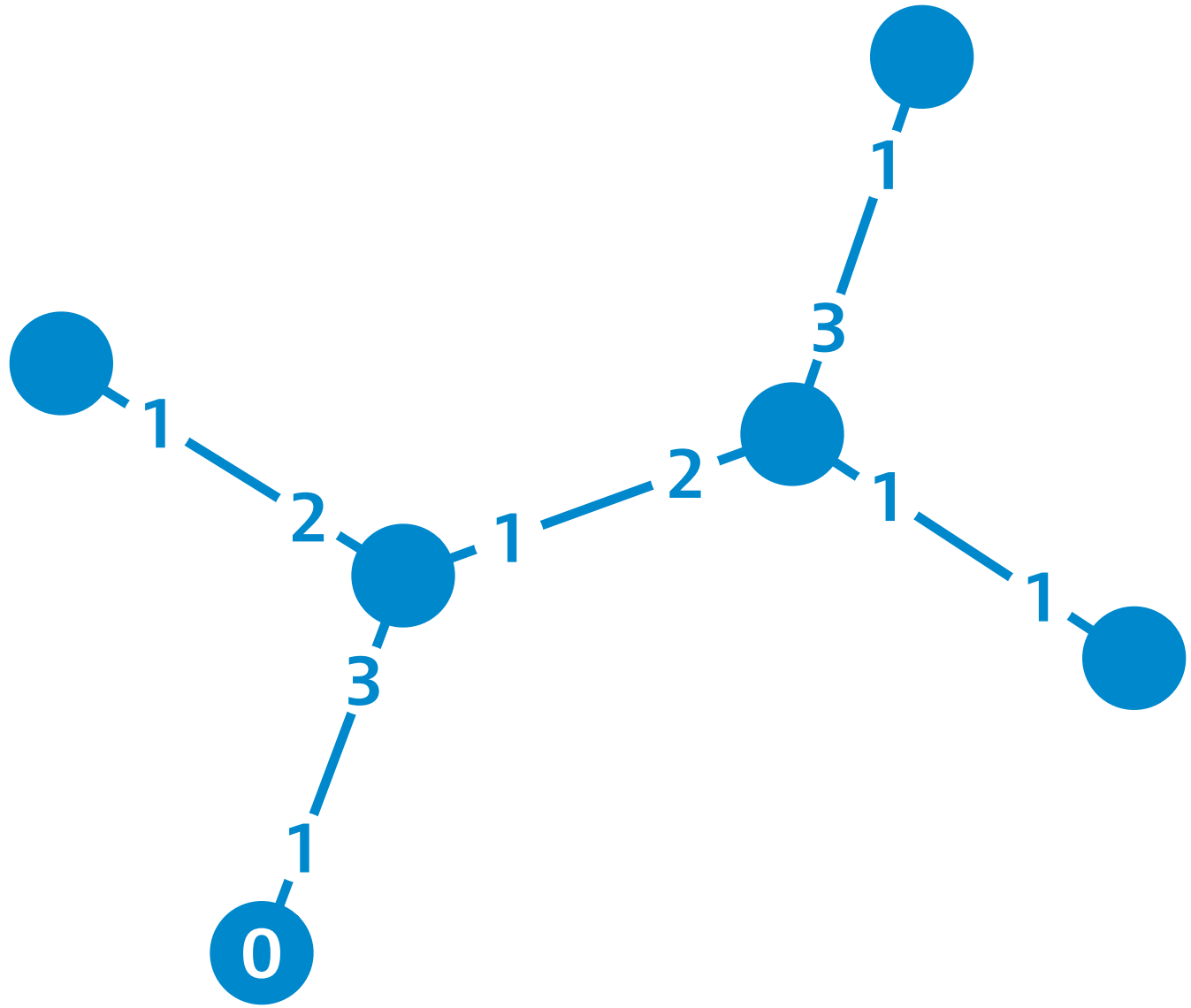

e
1
a
1
d
1
2
3
c
1
2
3
f
1
b
1

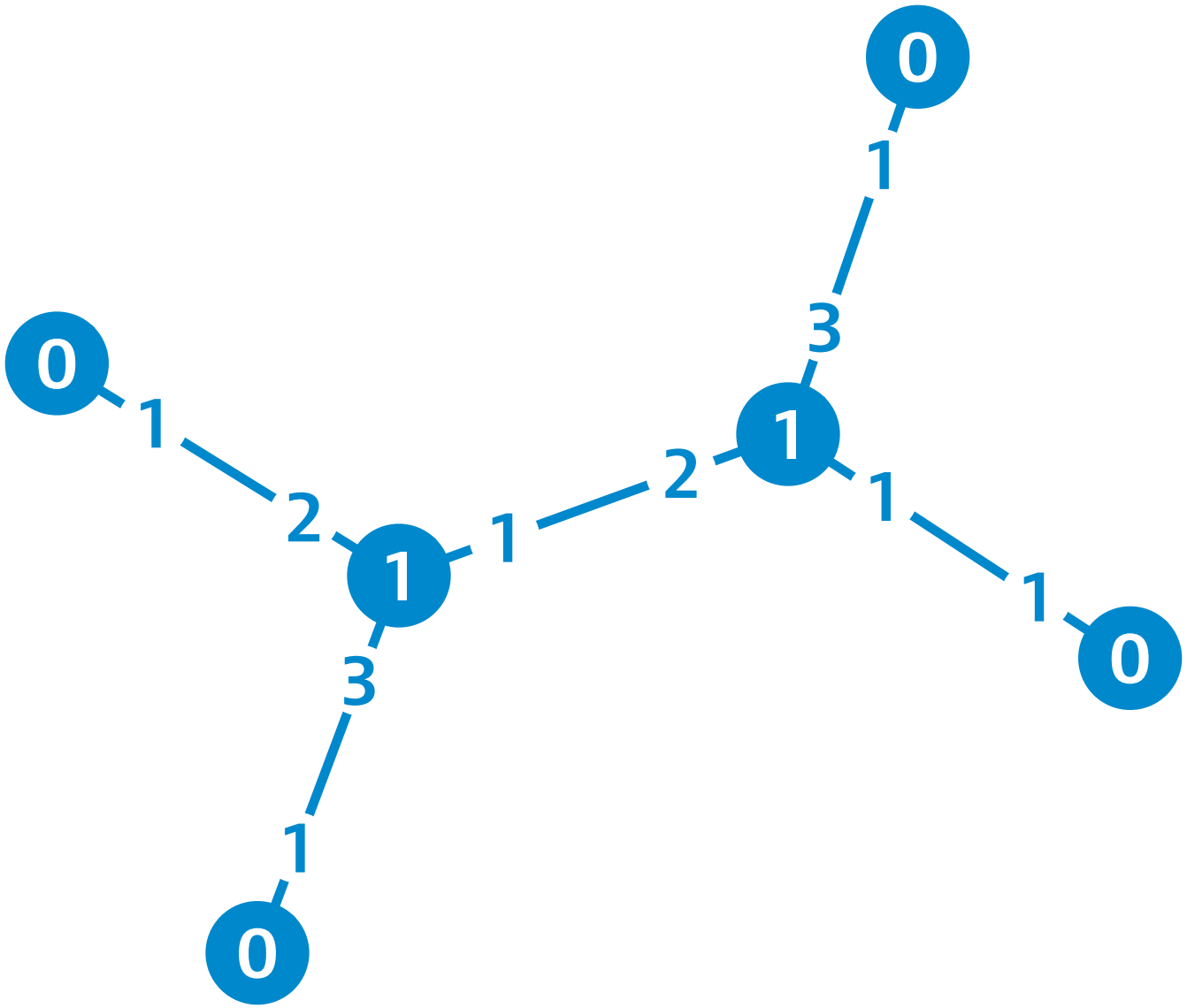

e
x
1
x
a
1
x
d
1
2
3
x
c
1
2
3
f
x
1
x
b
1

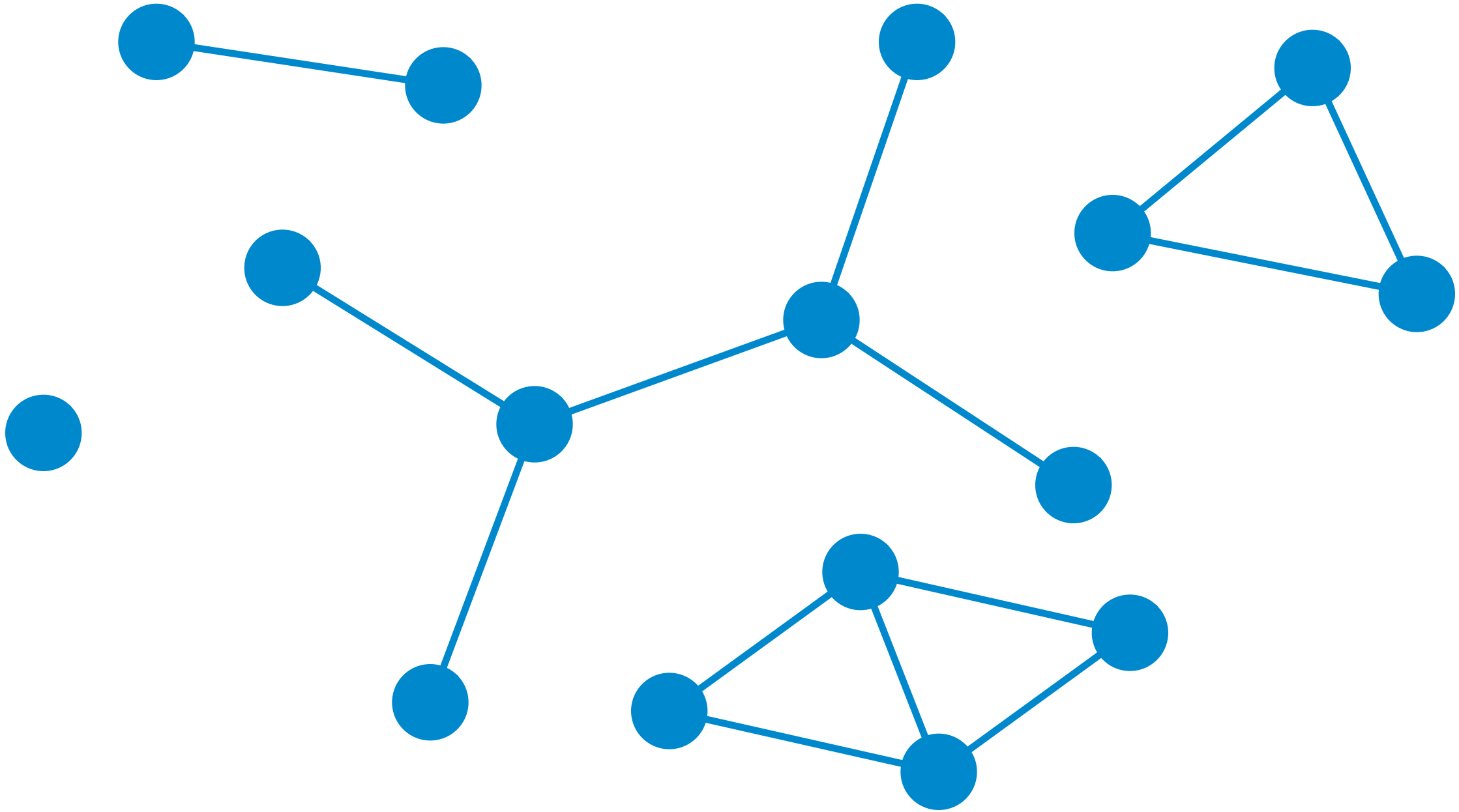

1
3
1
2
1
2
1
1
3
1

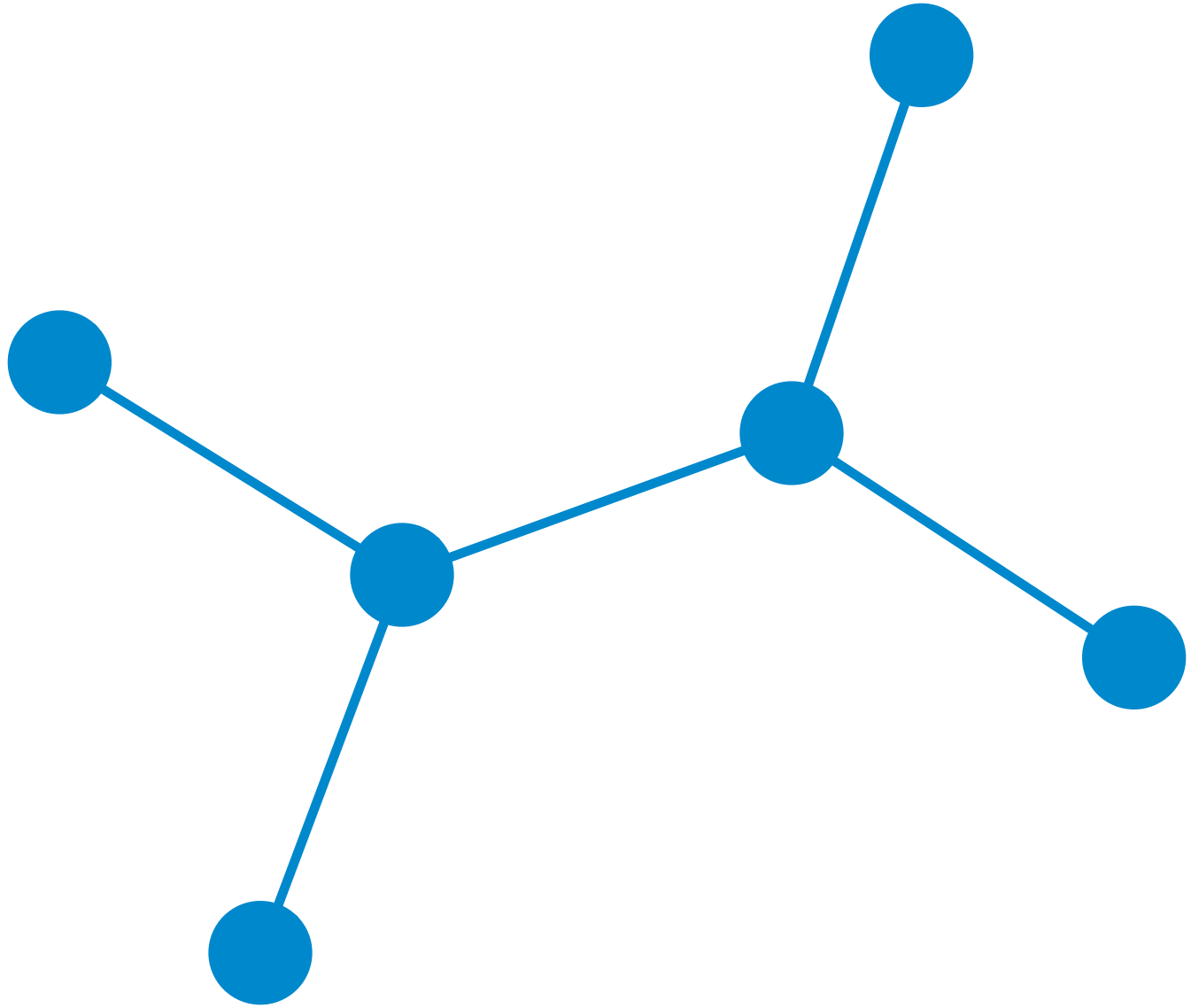

?
?
?
?
?
?
1
2
1
2
1
3
1
1
3
1

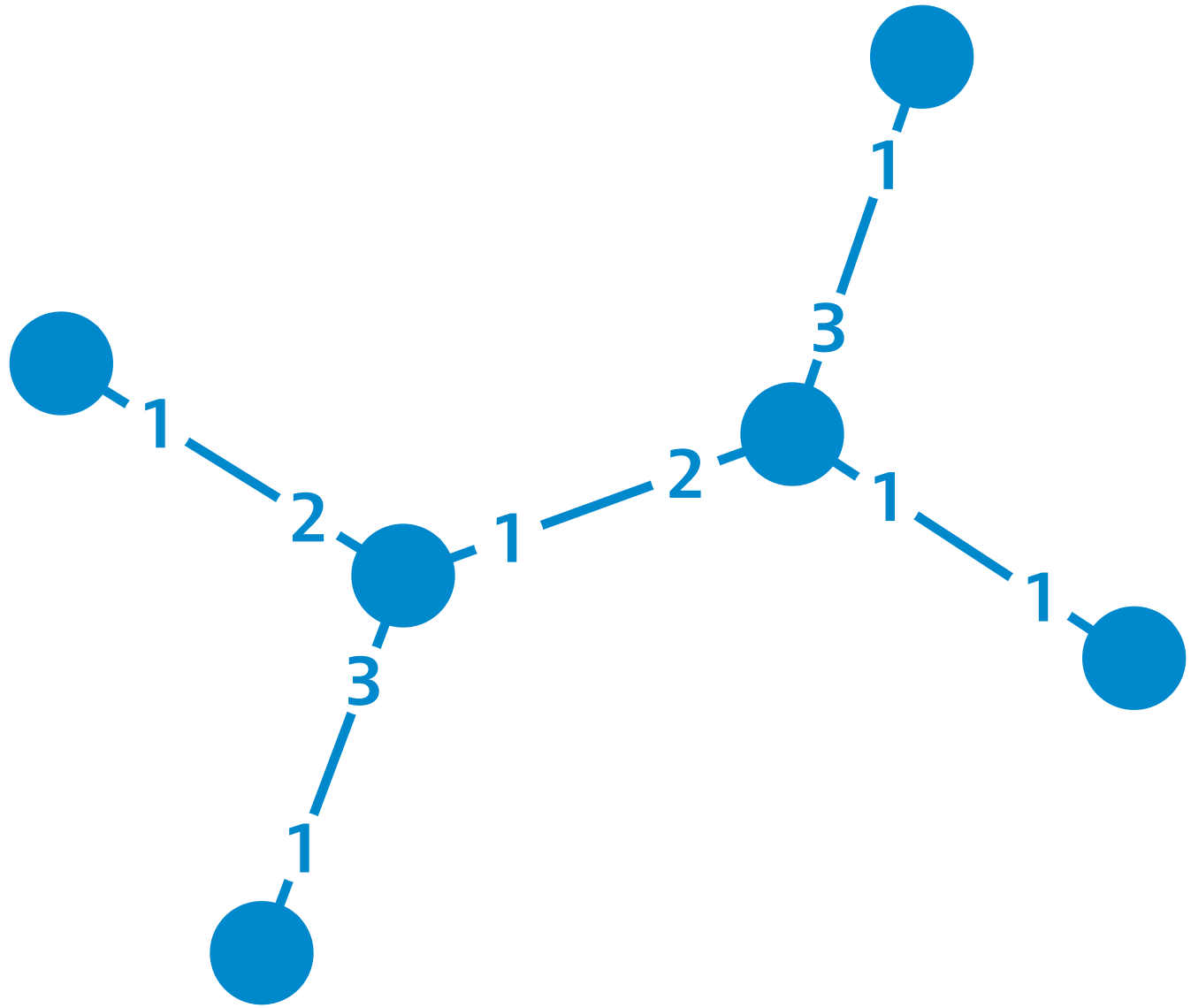

1
3
1
2
1
2
1
1
3
1

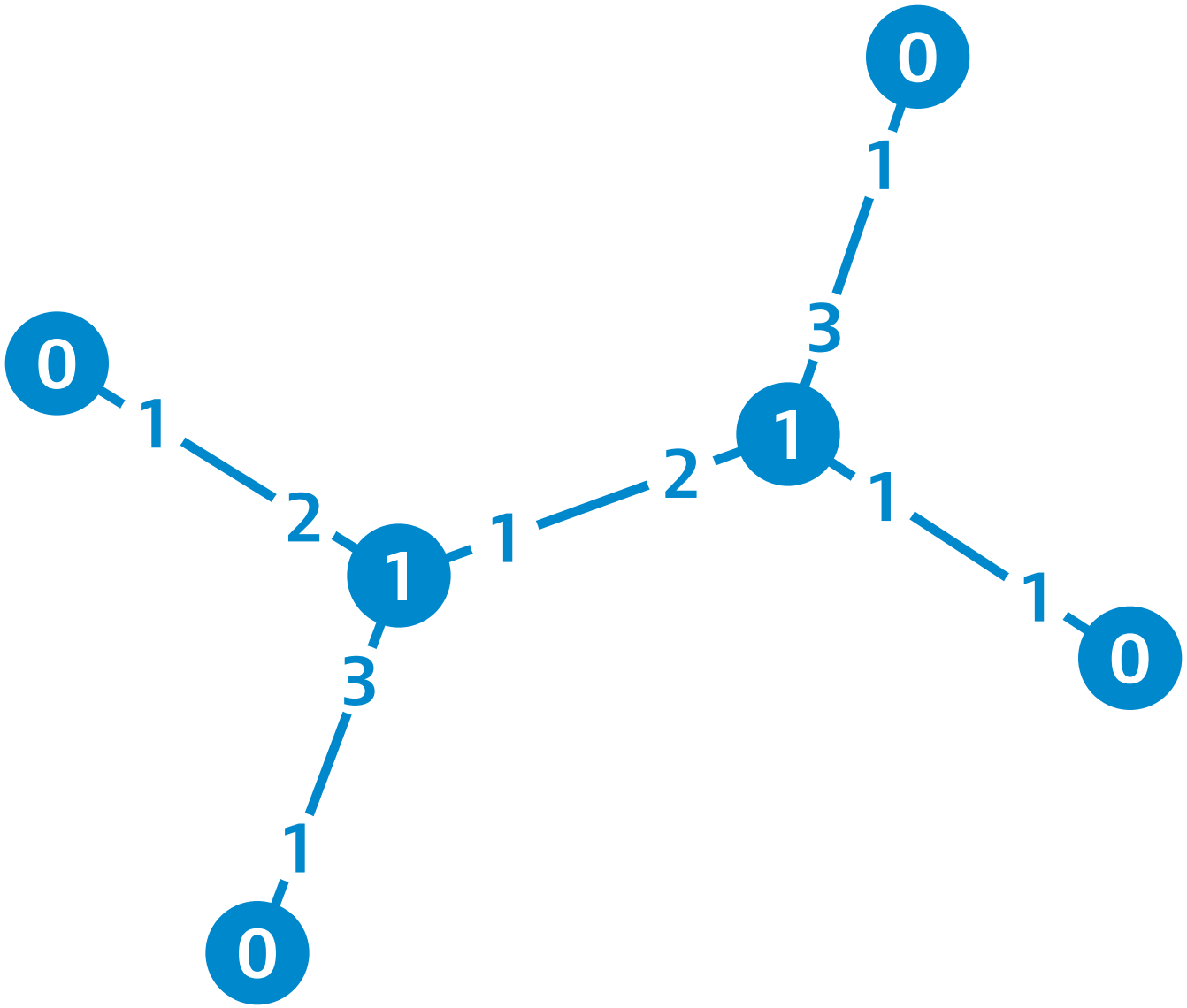

1
3
1
2
1
2
1
1
3
1
0

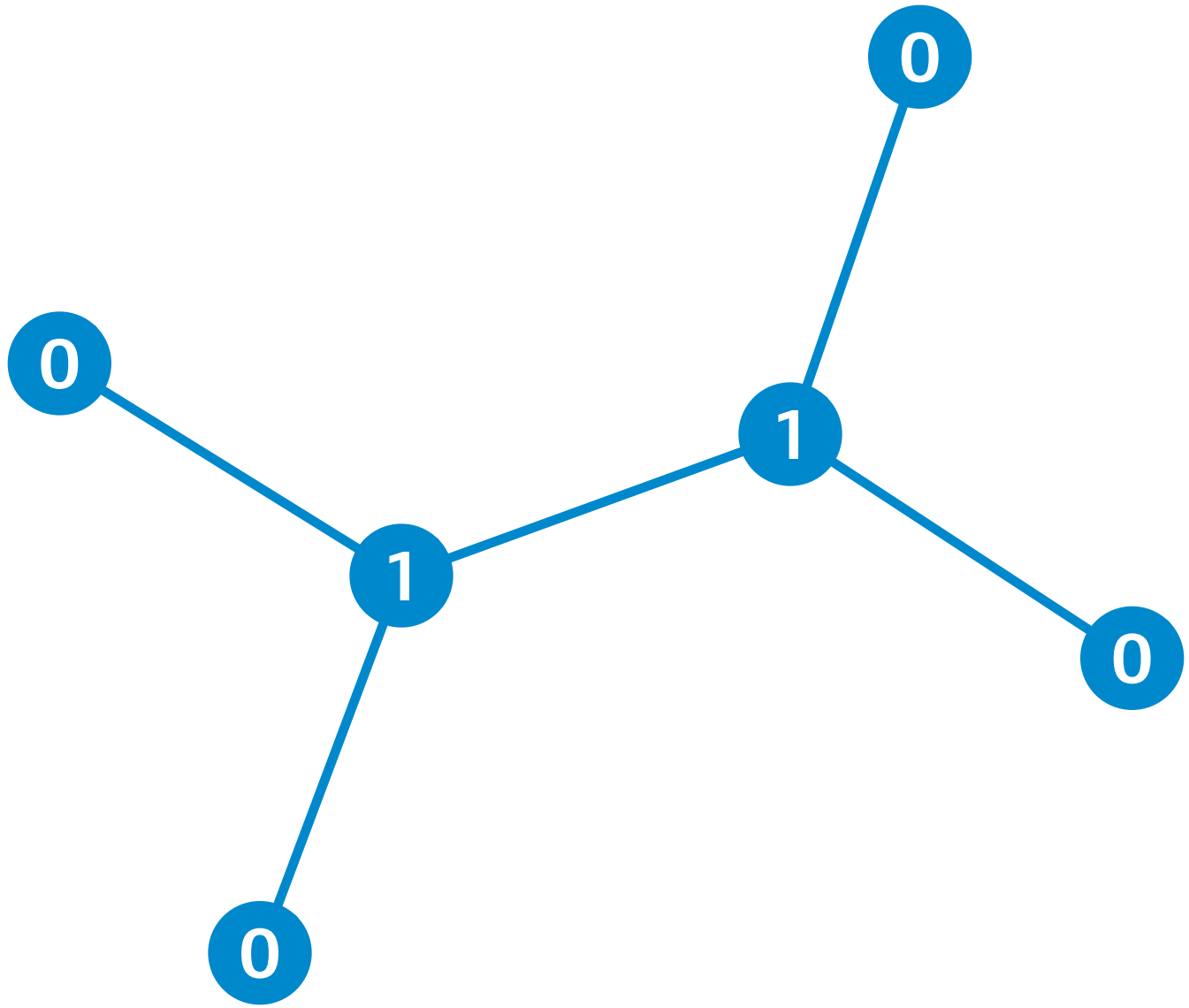

0
1
3
1
2
1
1
2
1
1
0
3
1
0

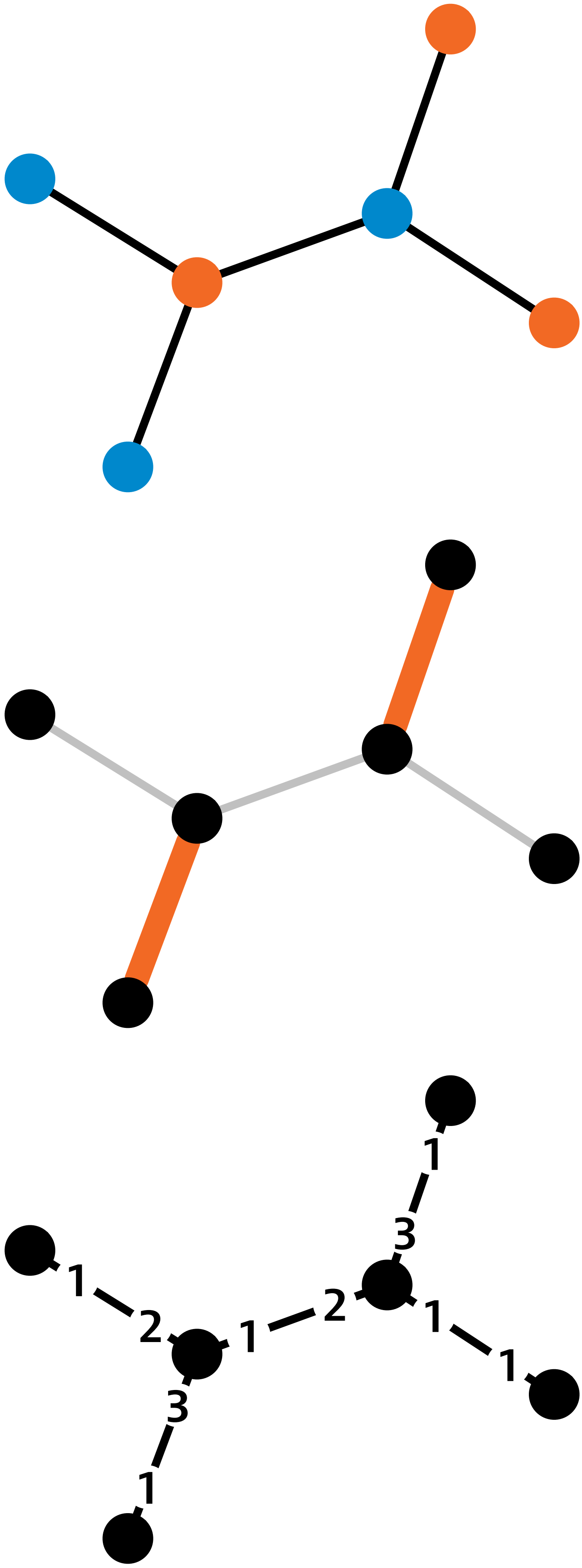


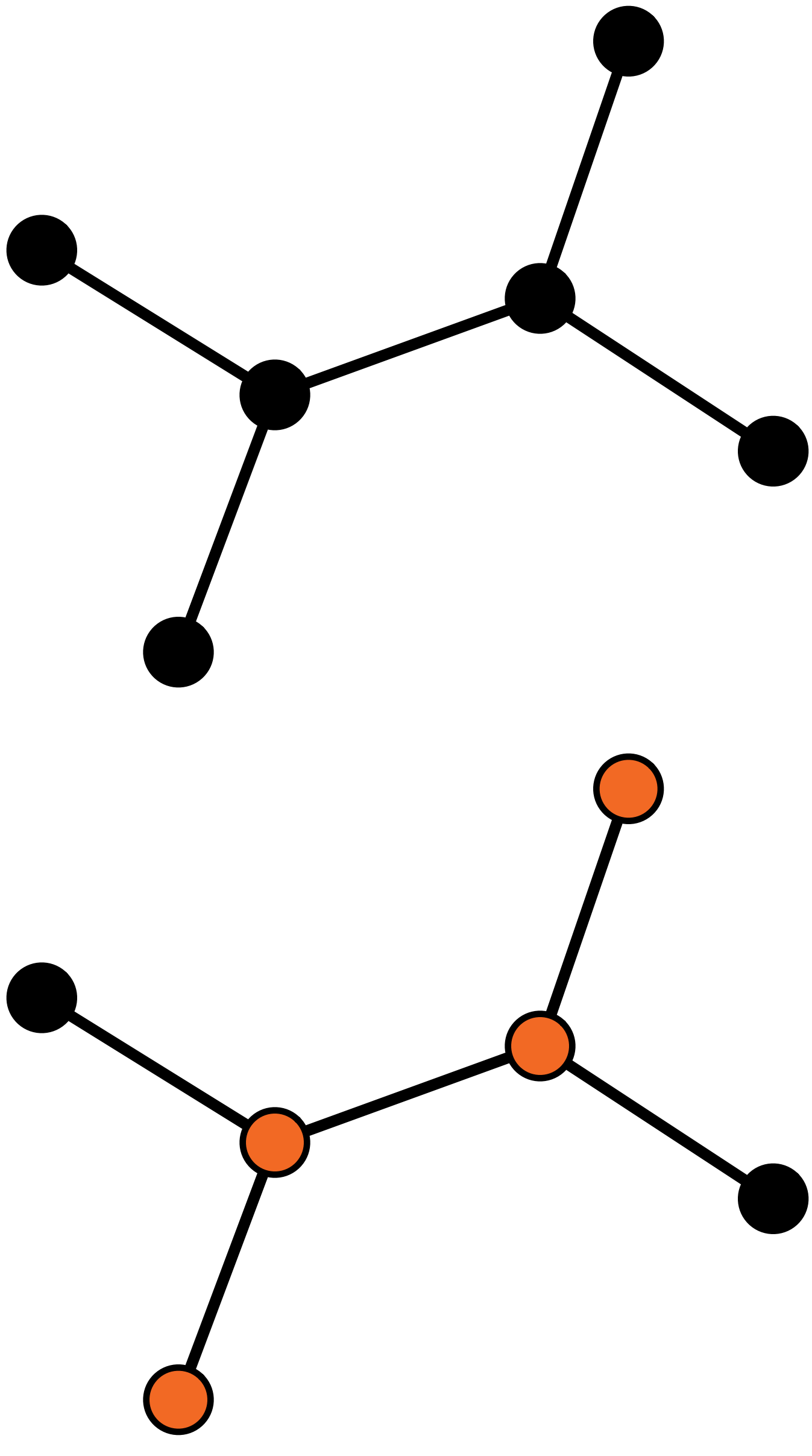


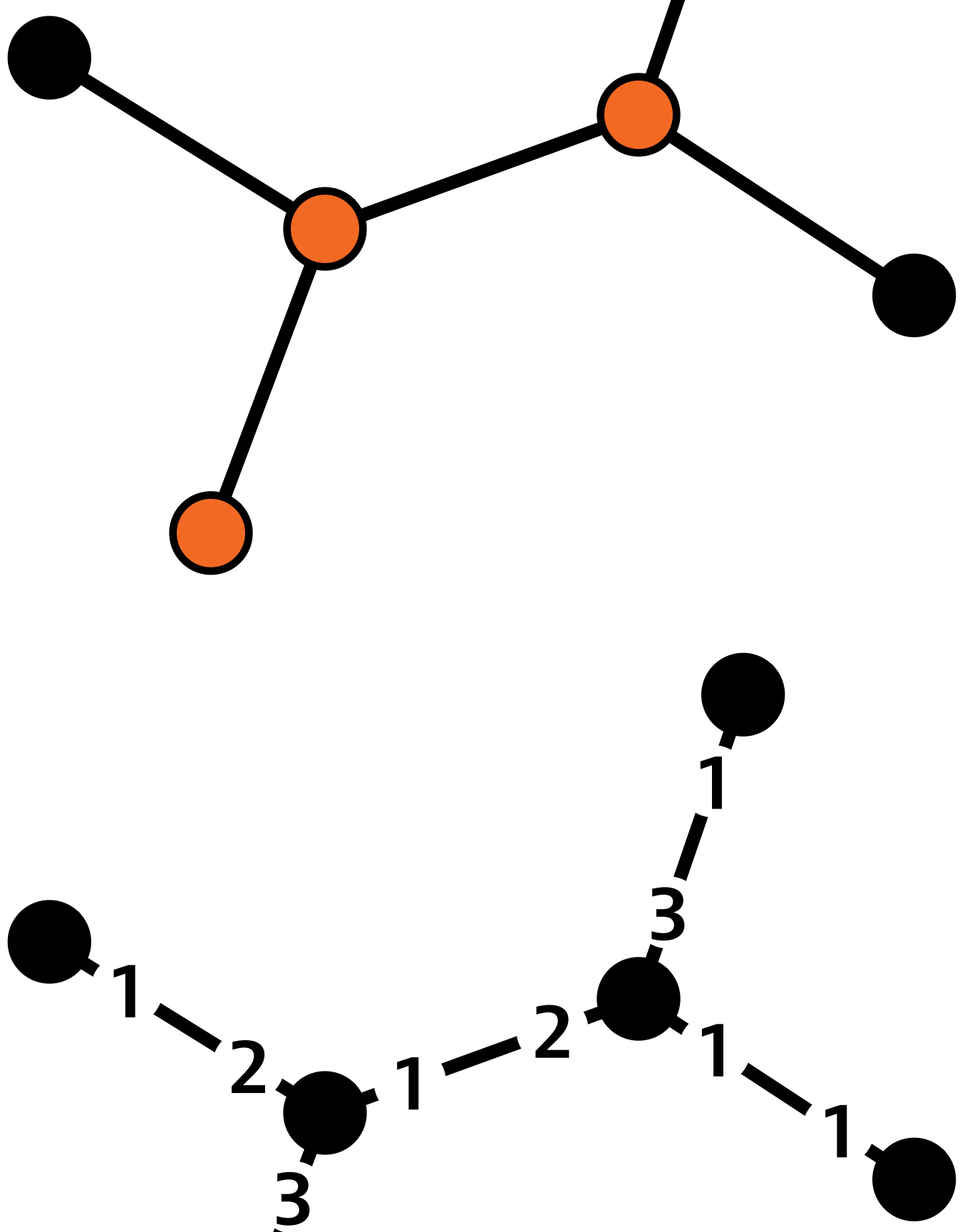

1
3
1
2
1
2
1
1
3
1

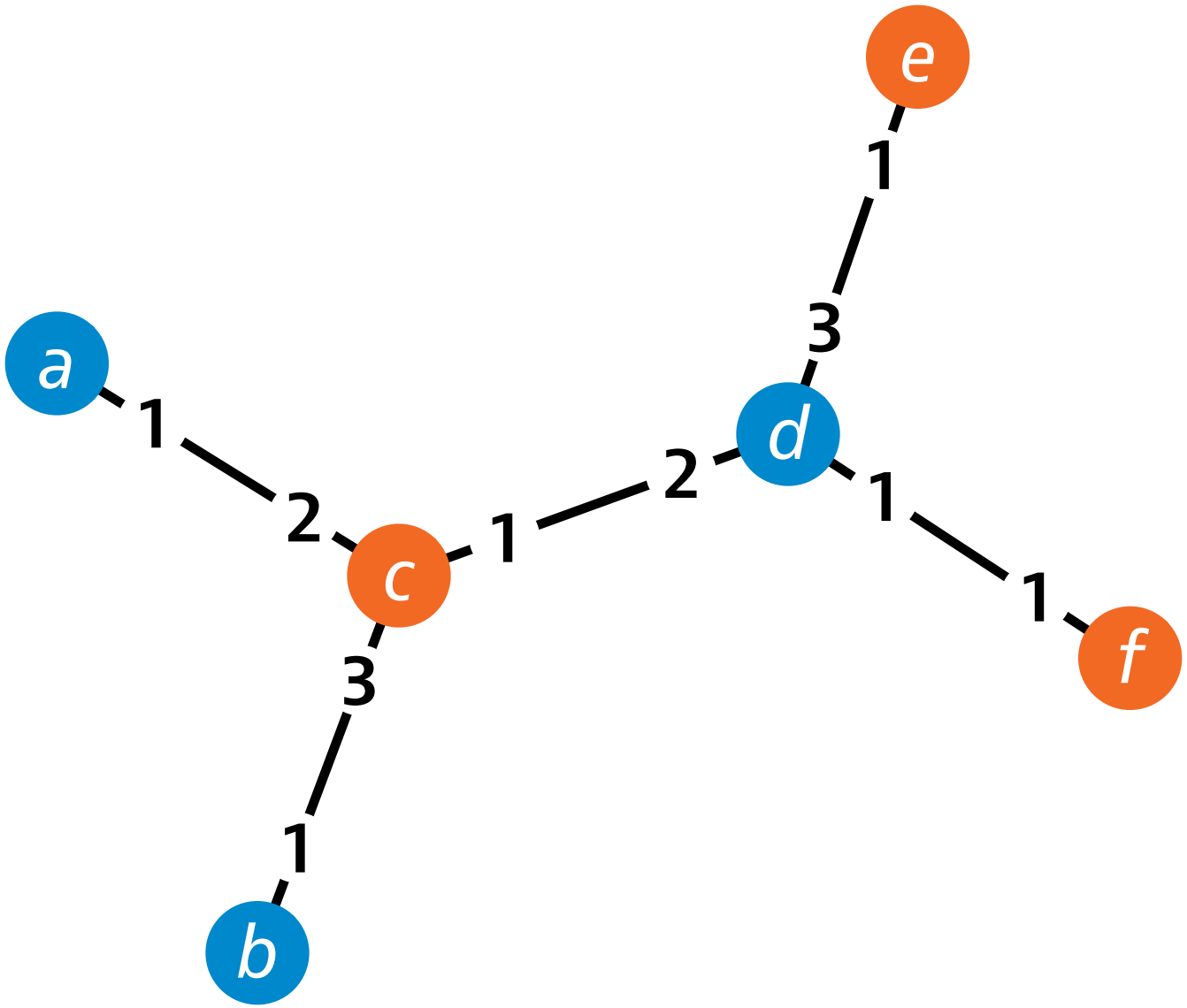

0
1
3
1
2
1
1
2
1
1
0
3
1
0

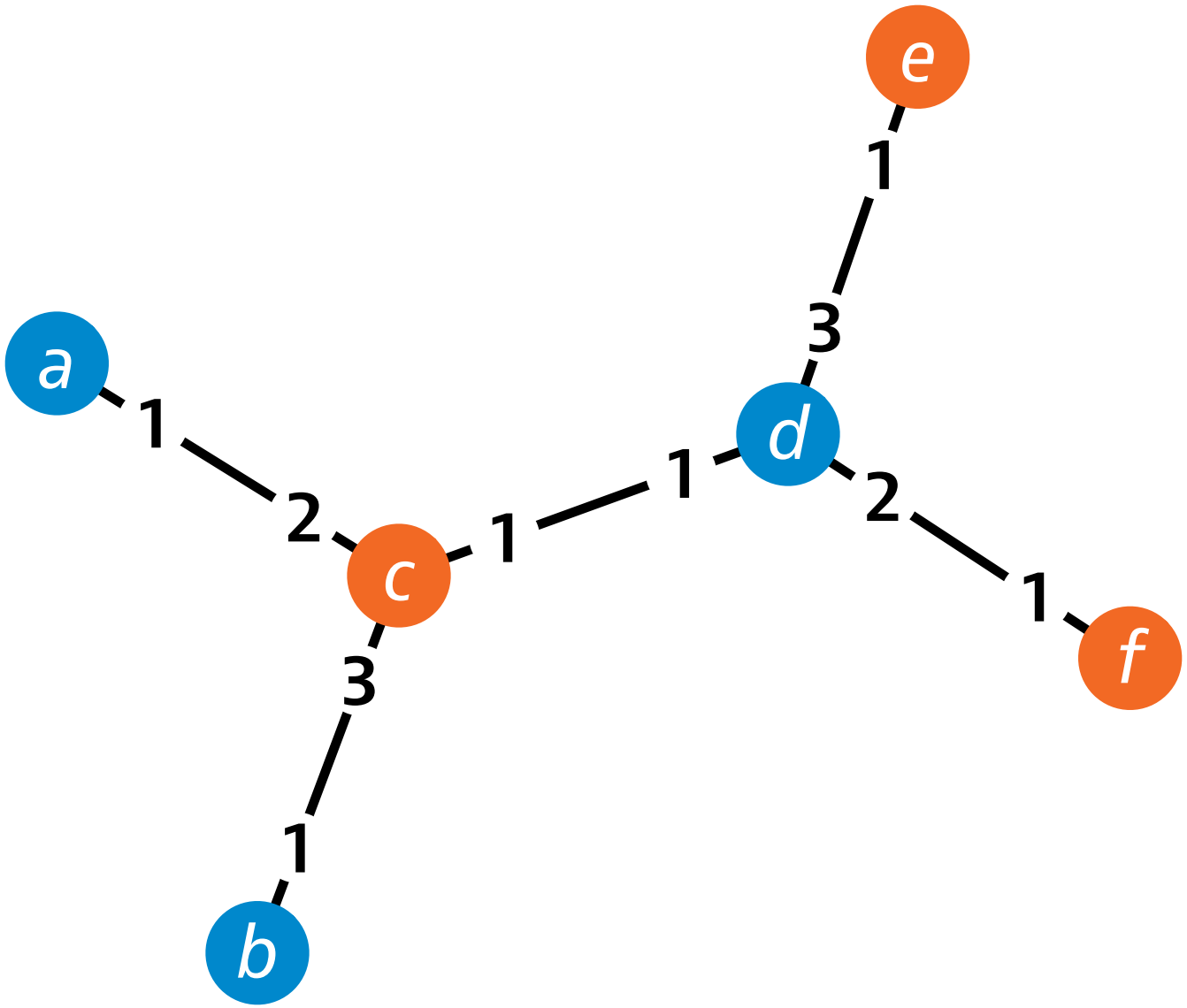

0
0
1
1
0
0

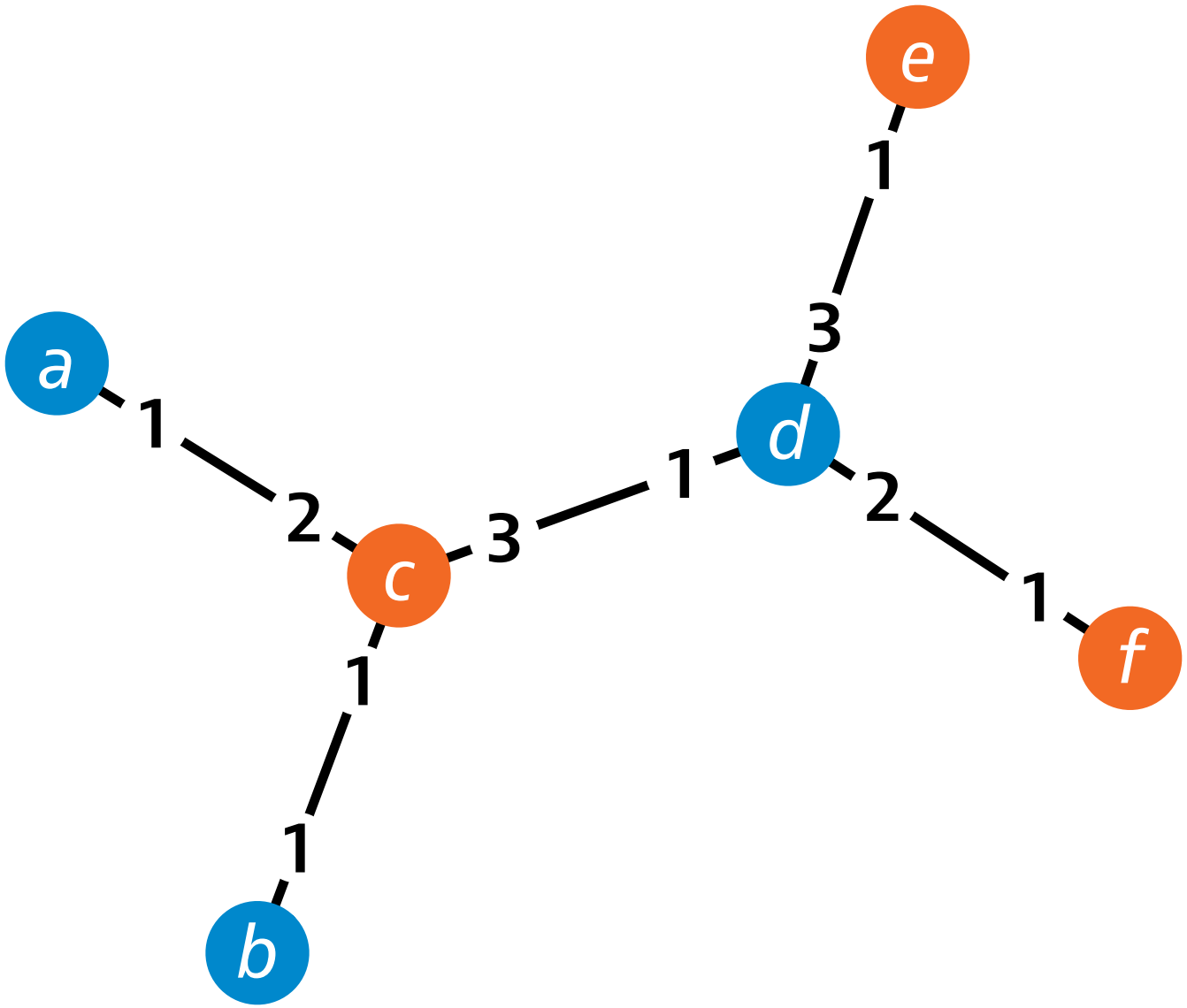


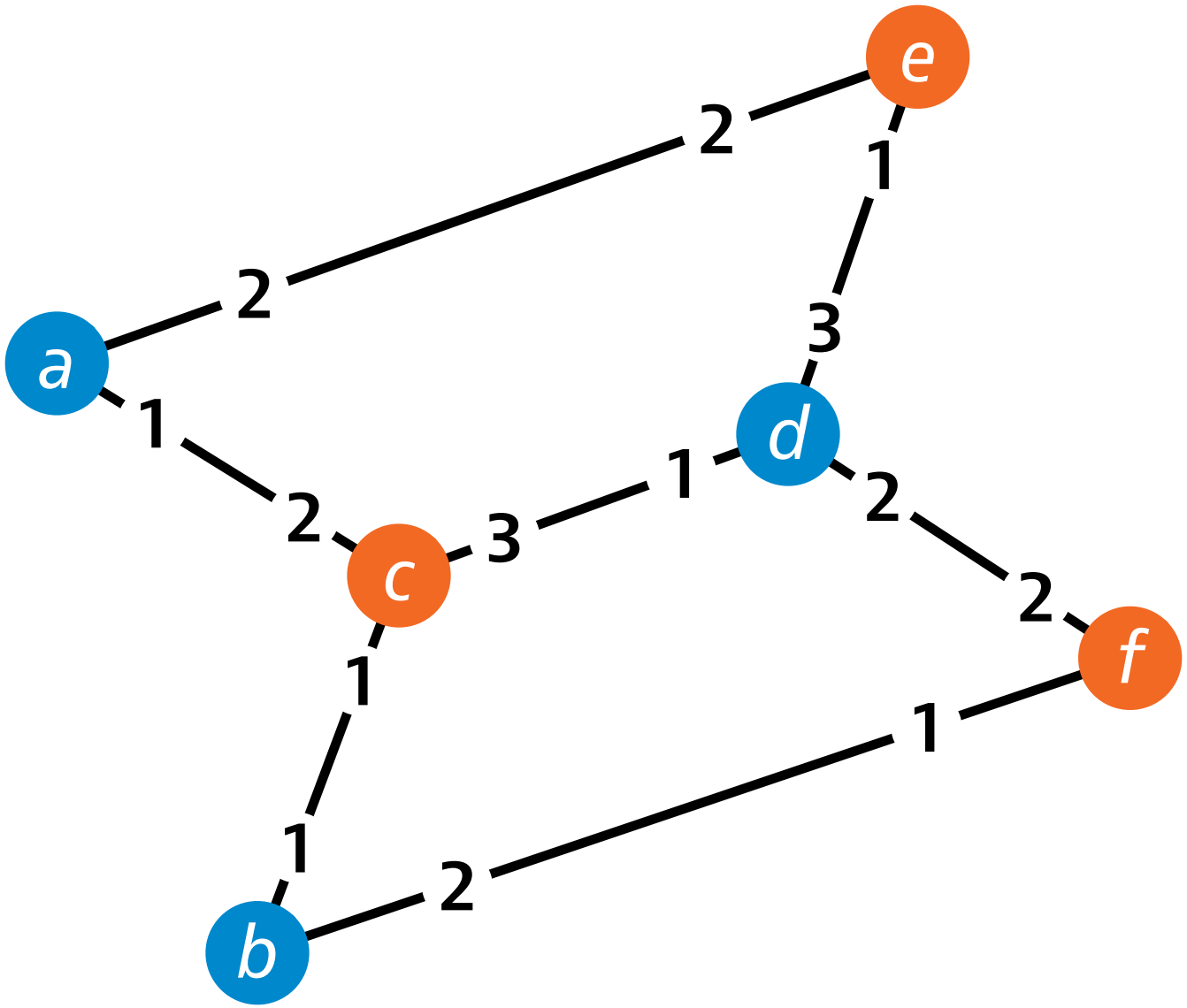


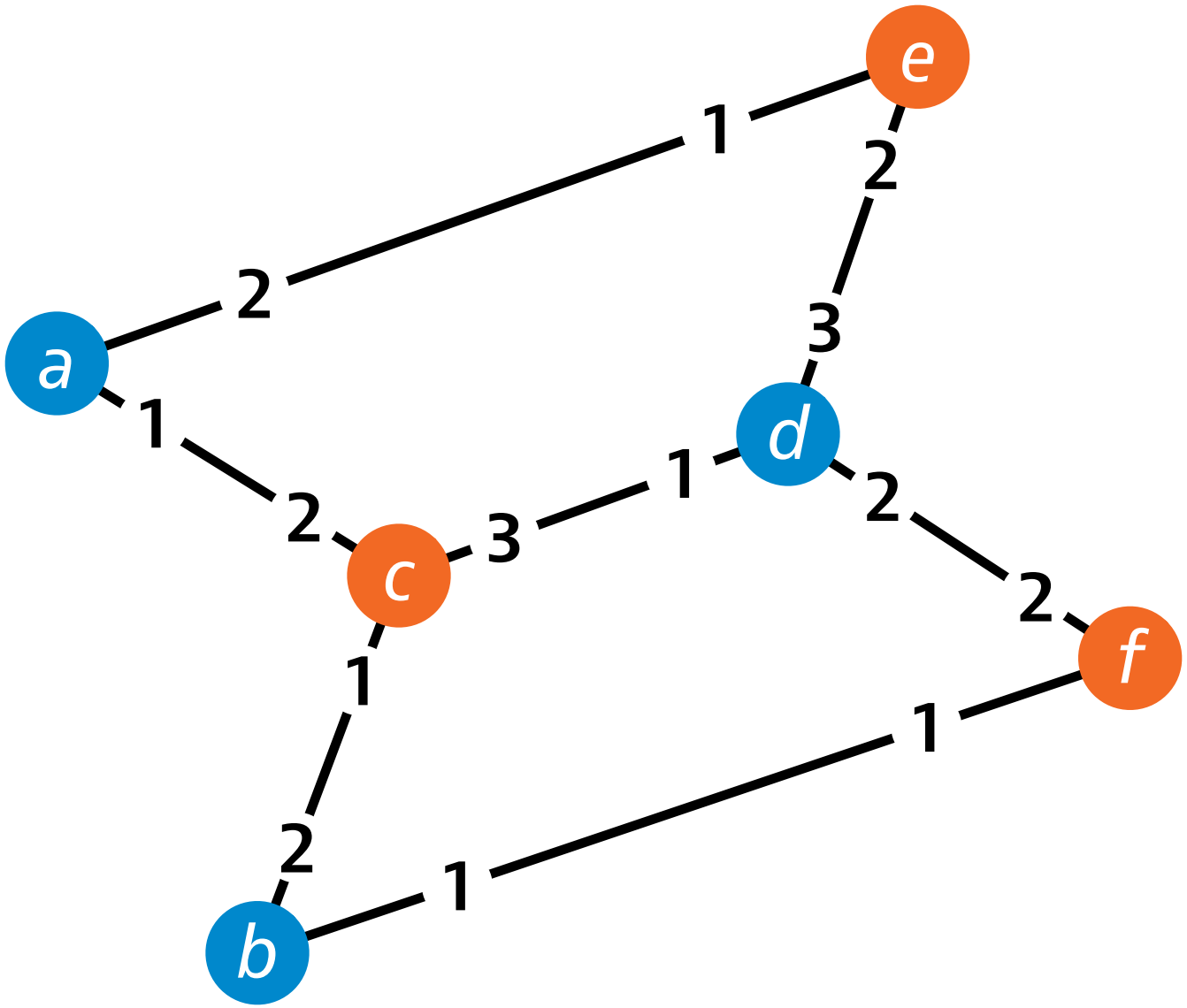

1
3
1
2
1
2
1
1
1

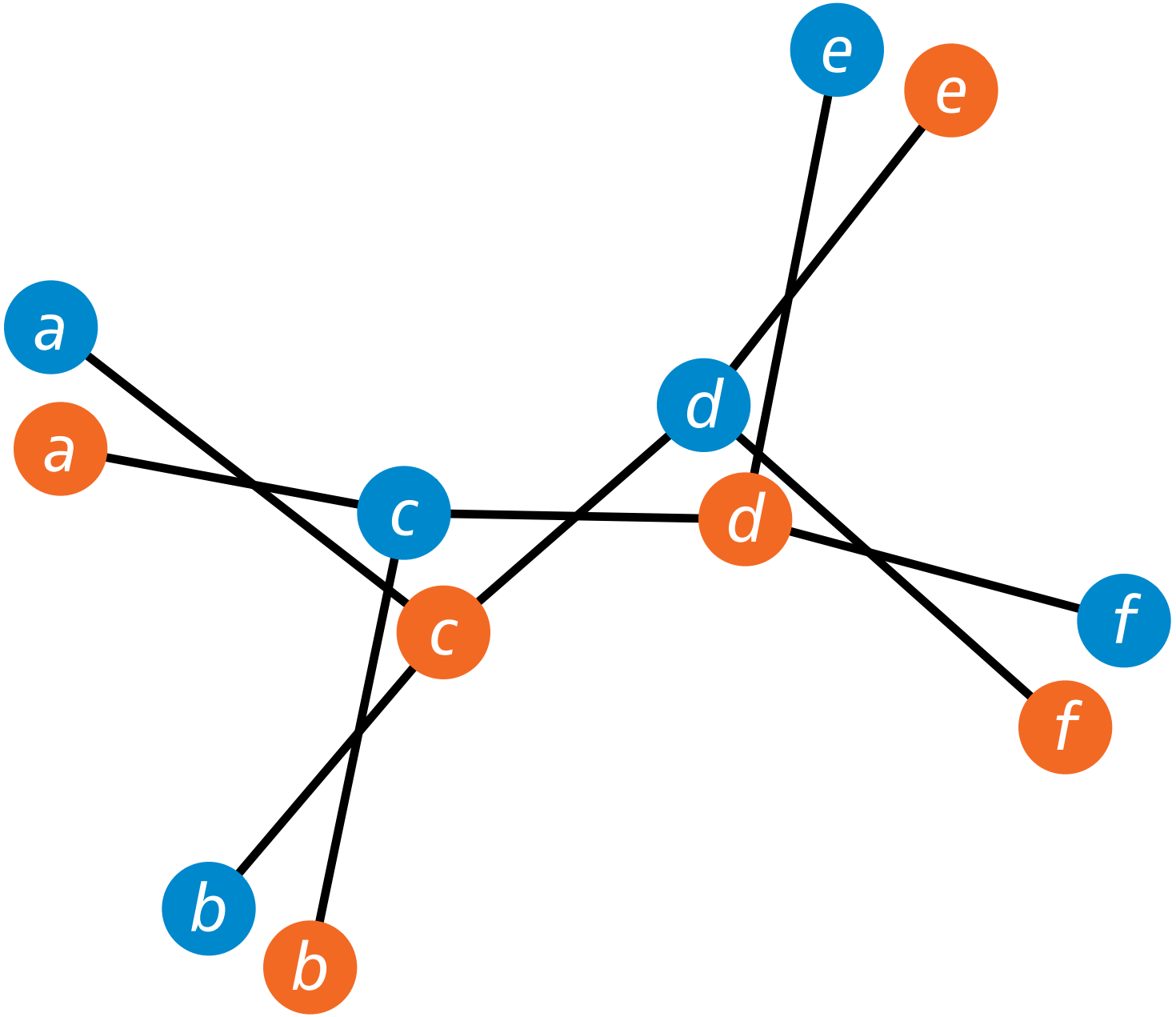

e
1
3
a
1
d
2
2
1
1
c
1
f
3
1
b

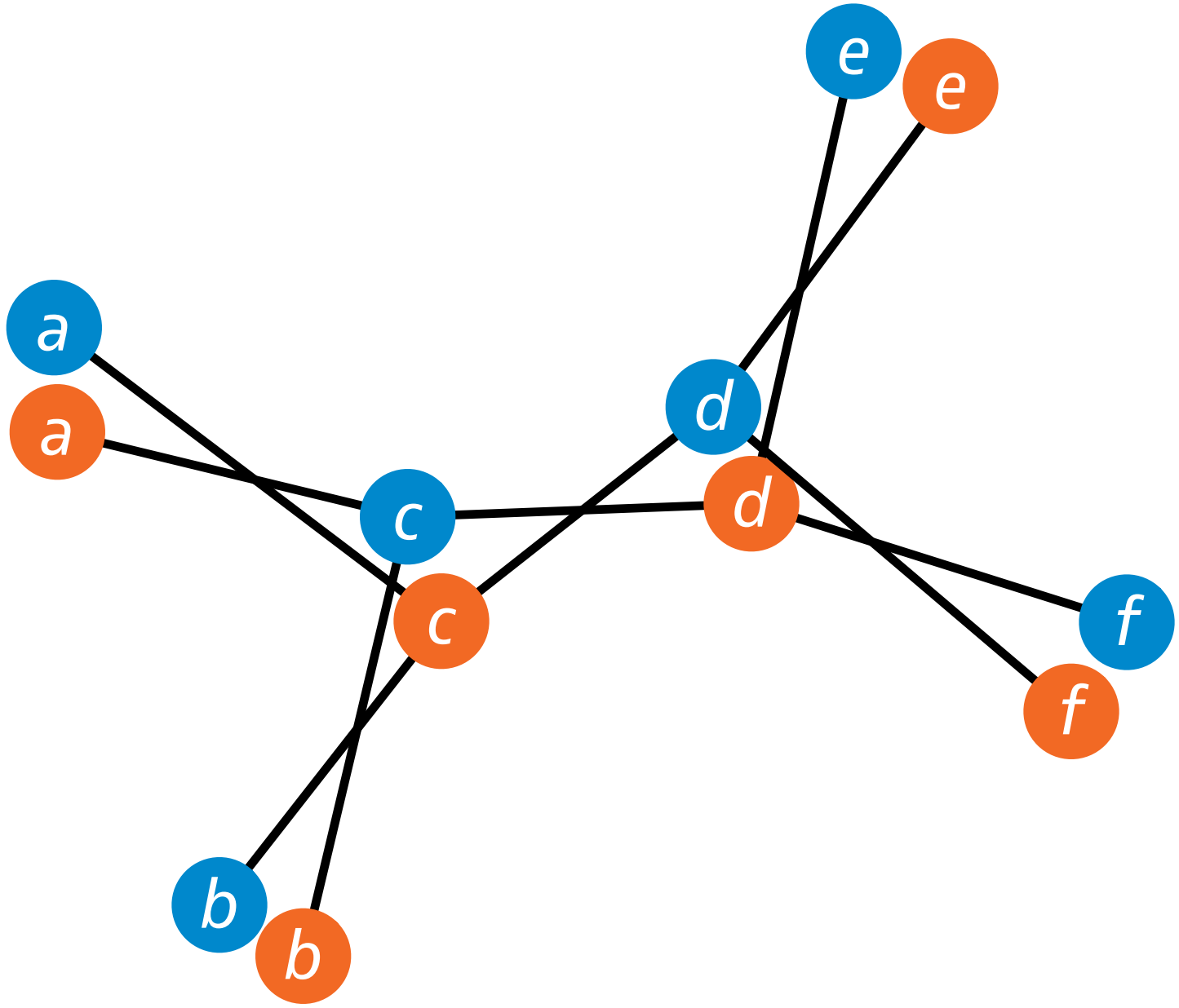

e
1
a
3
1
d
1
2
2
c
1
1
f
3
1
b

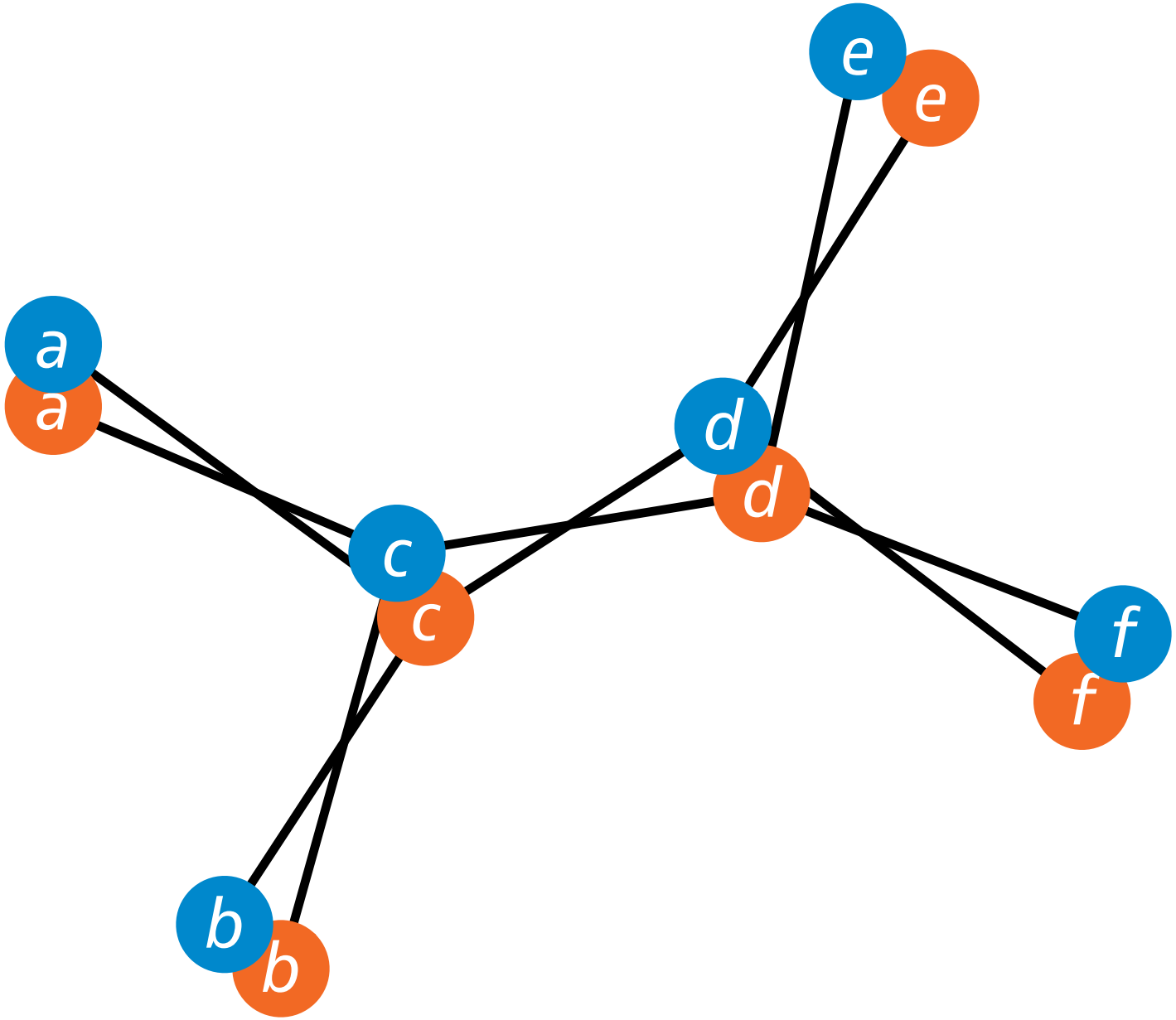

e
1
3
a
1
d
1
2
2
3
c
1
f
1
1
b

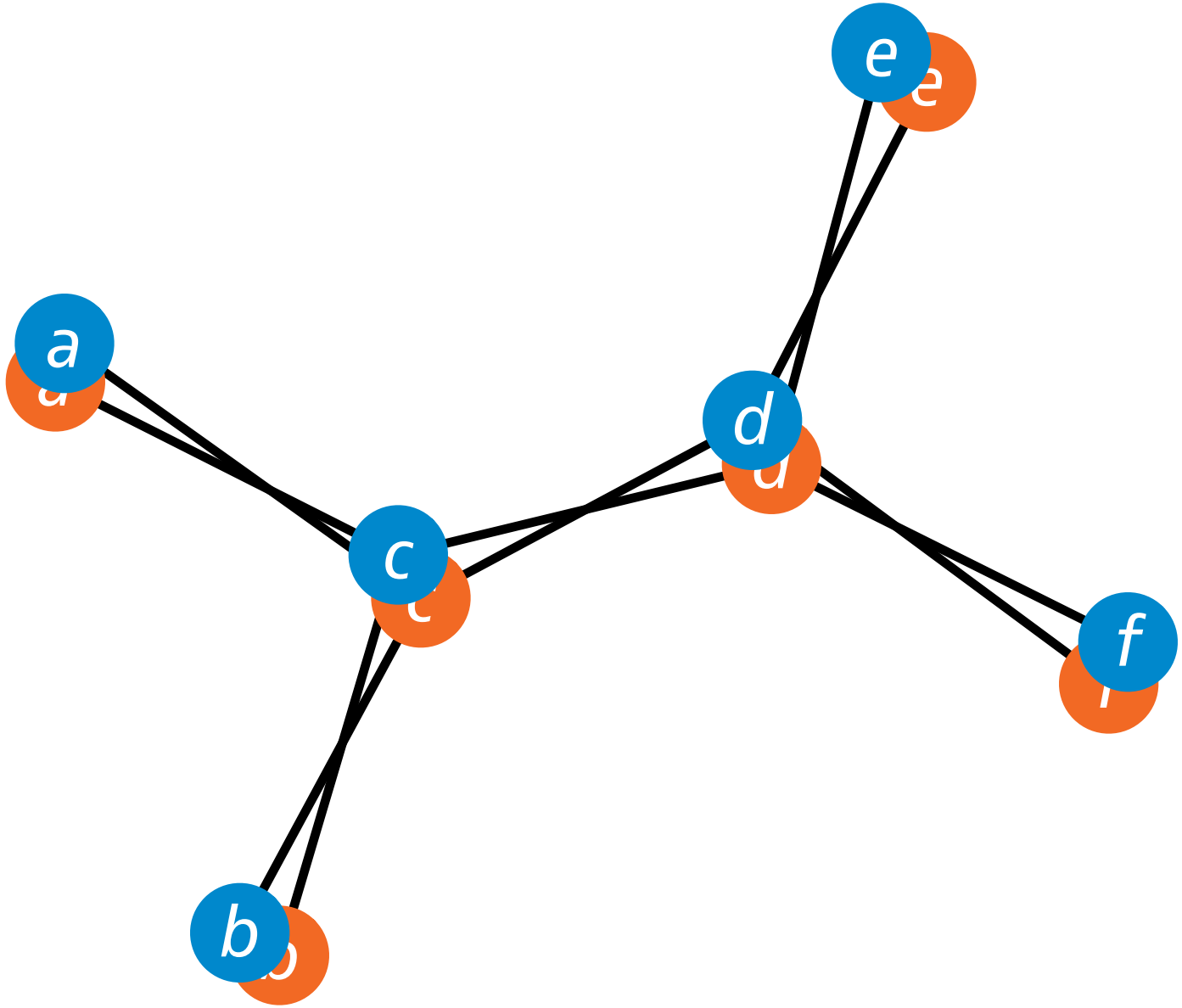

e
2
1
2
3
a
1
d
2
1
3
2
c
2
f
1
1
1
2
b

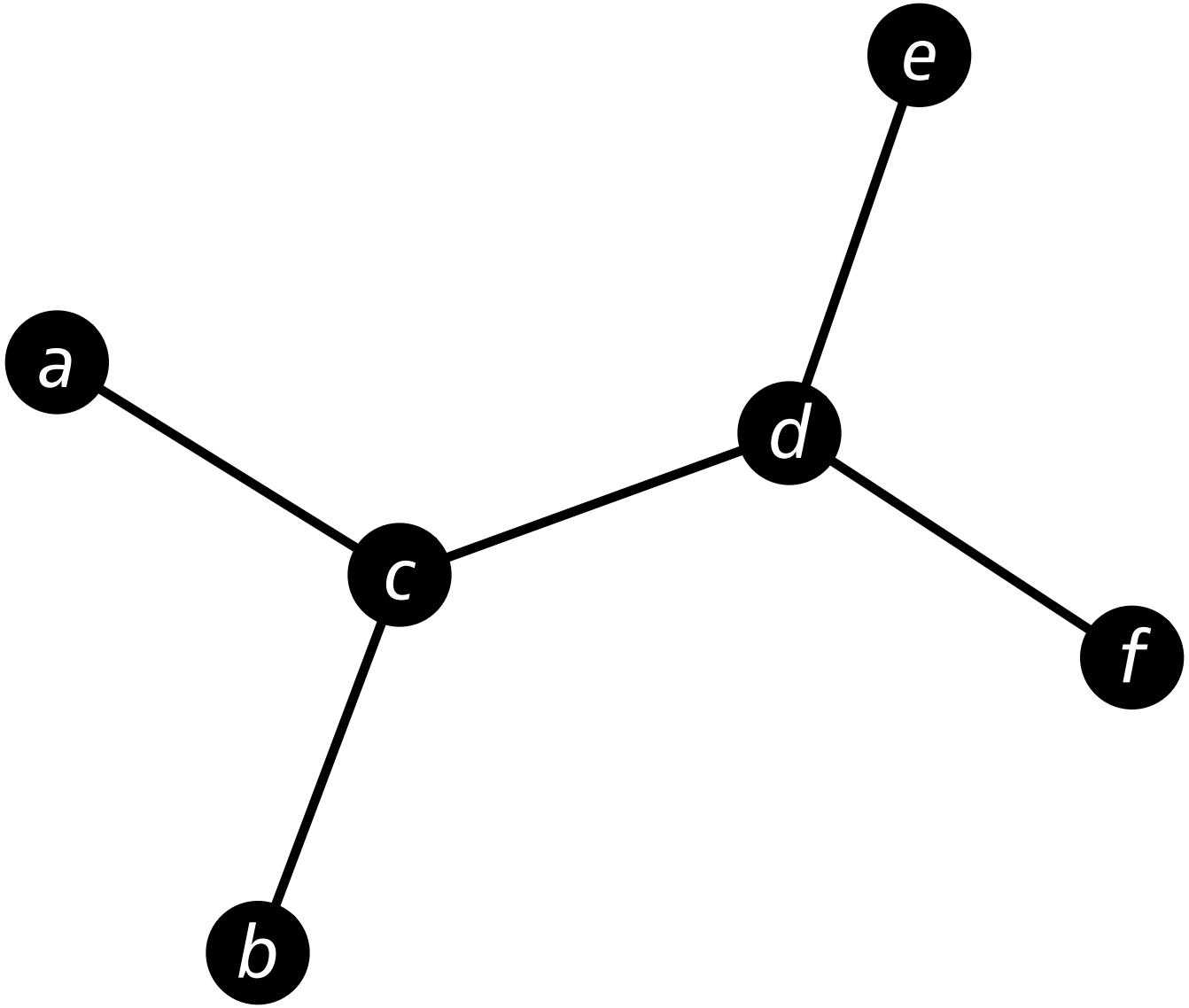

e
1
2
a
2
3
1
d
1
2
c
3
2
f
1
1
2
1
b

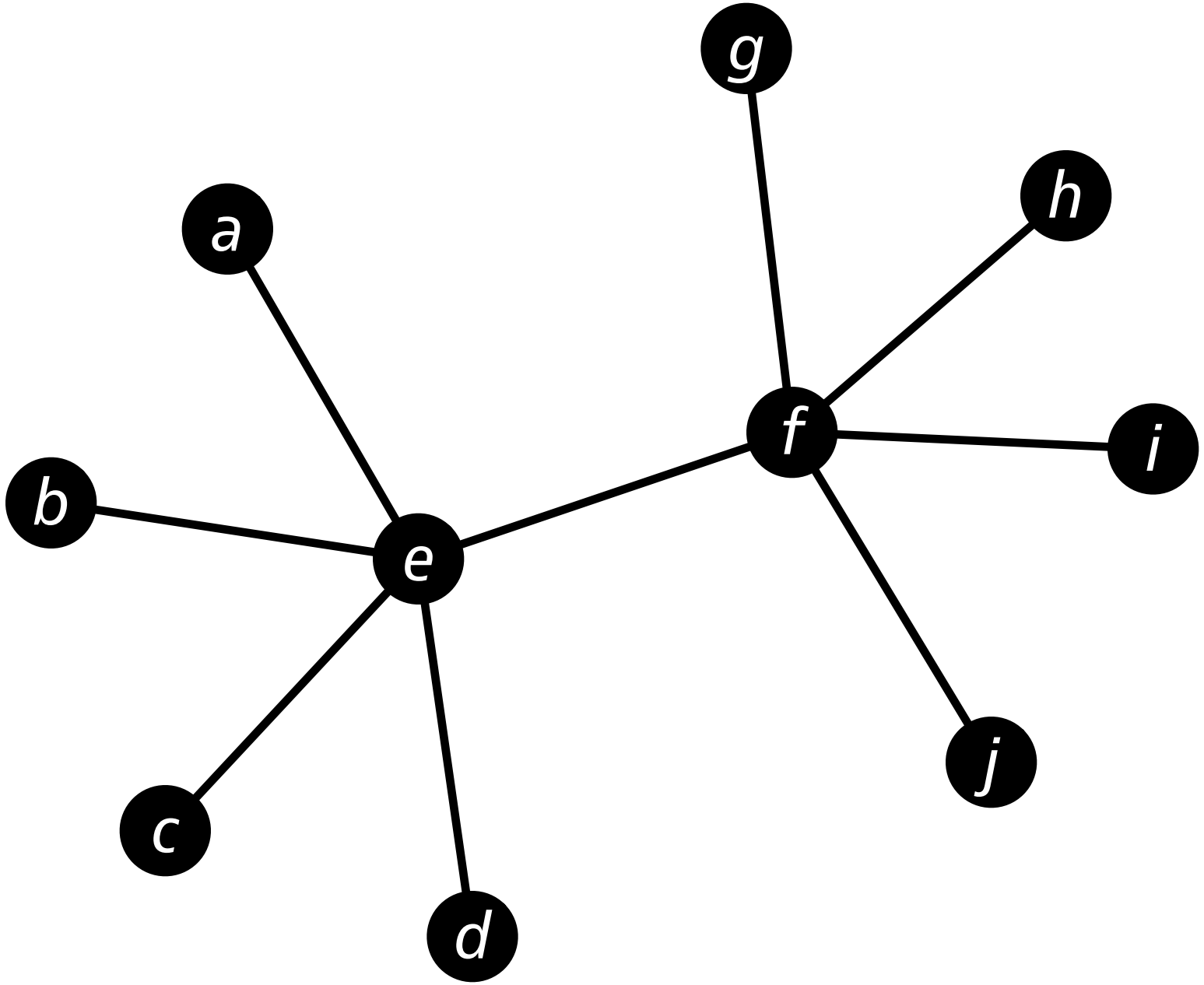

e
e
a
d
a
c
d
f
c
f
b
b

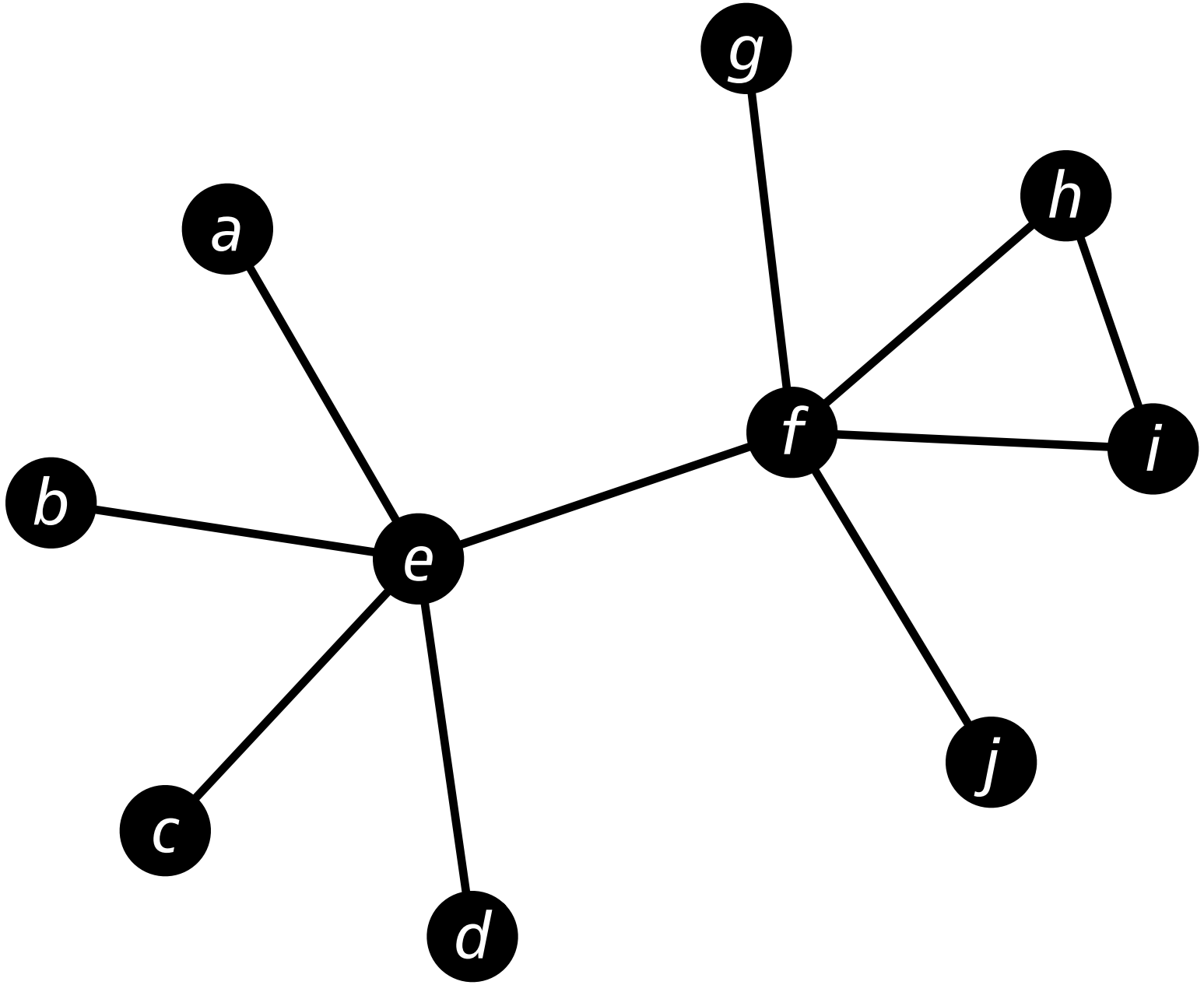

e
e
a
a
d
c
d
f
c
f
b
b

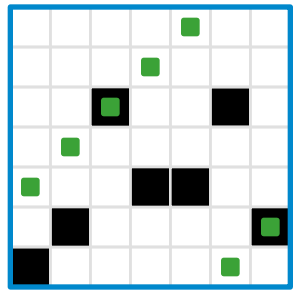

e
e
a
a
d
d
c
c
f
f
b
b


a
d
e
e
d
d
c
c
f
f
b
b

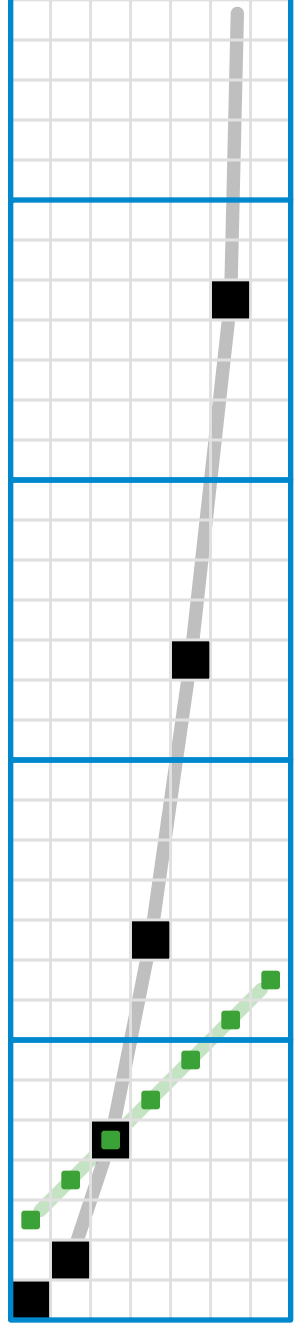

e
a
d
c
f
b


g
h
a
f
i
b
e
j
c
d

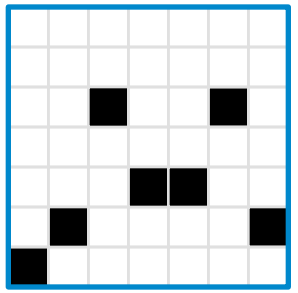

g
h
a
f
i
b
e
j
c
d



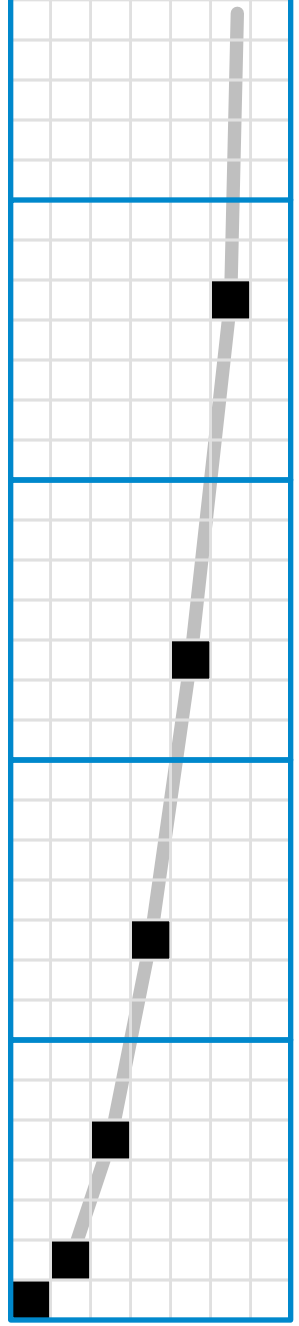
$f(x)$, $g(x)$ mod q



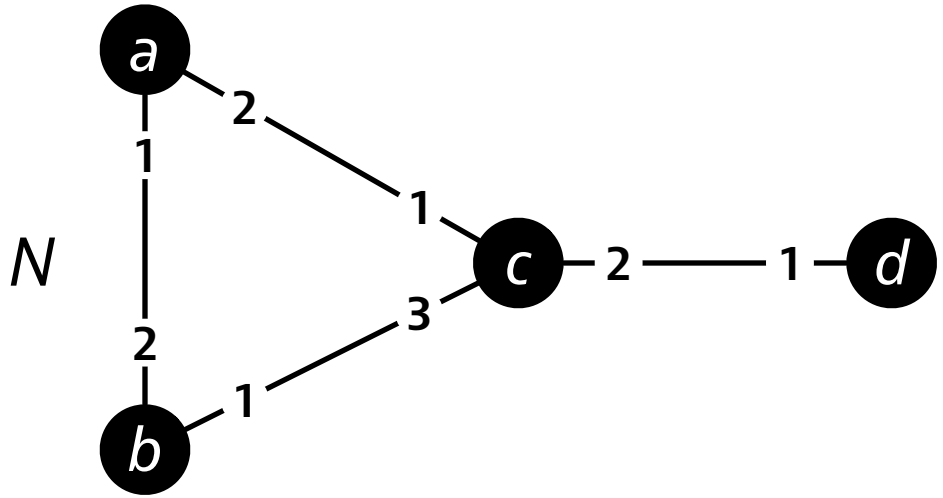
$f(x)$, $g(x)$

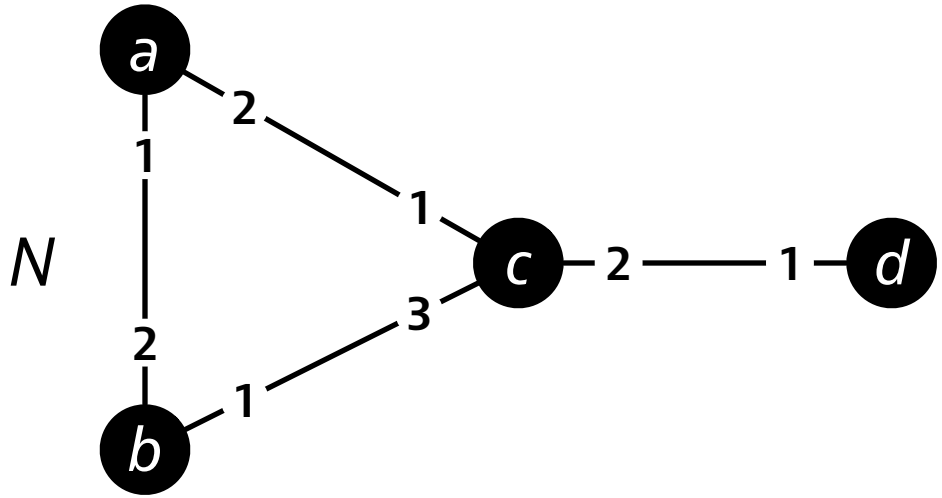


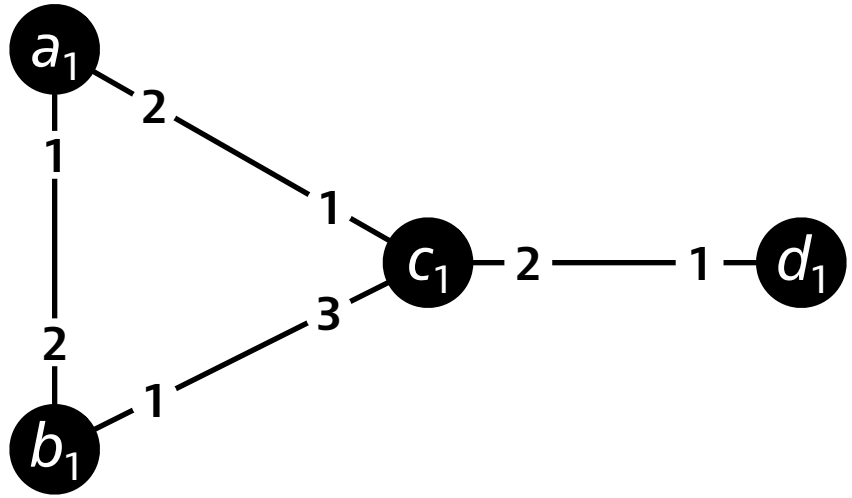
$f(x) \bmod q$

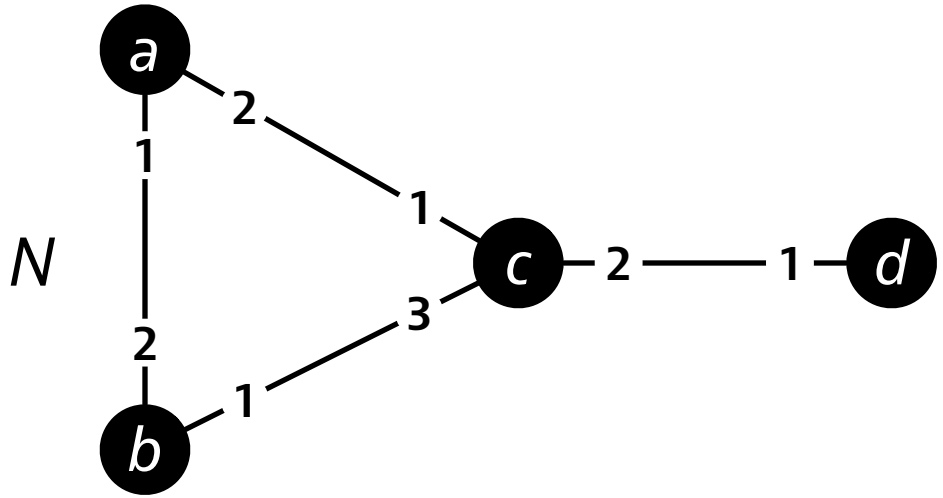


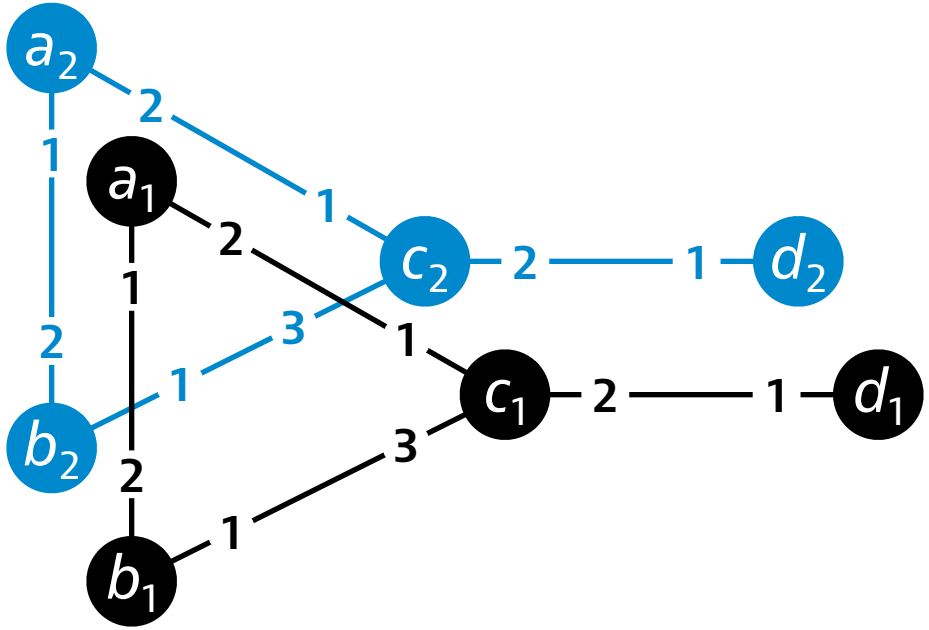
$f(x)$

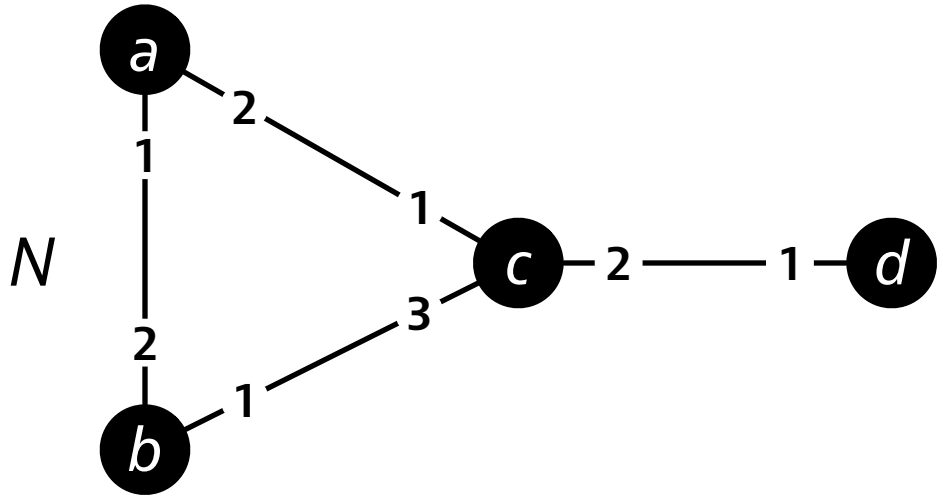

N
a
b
c
d
2
1
1
2
1
3
2
1

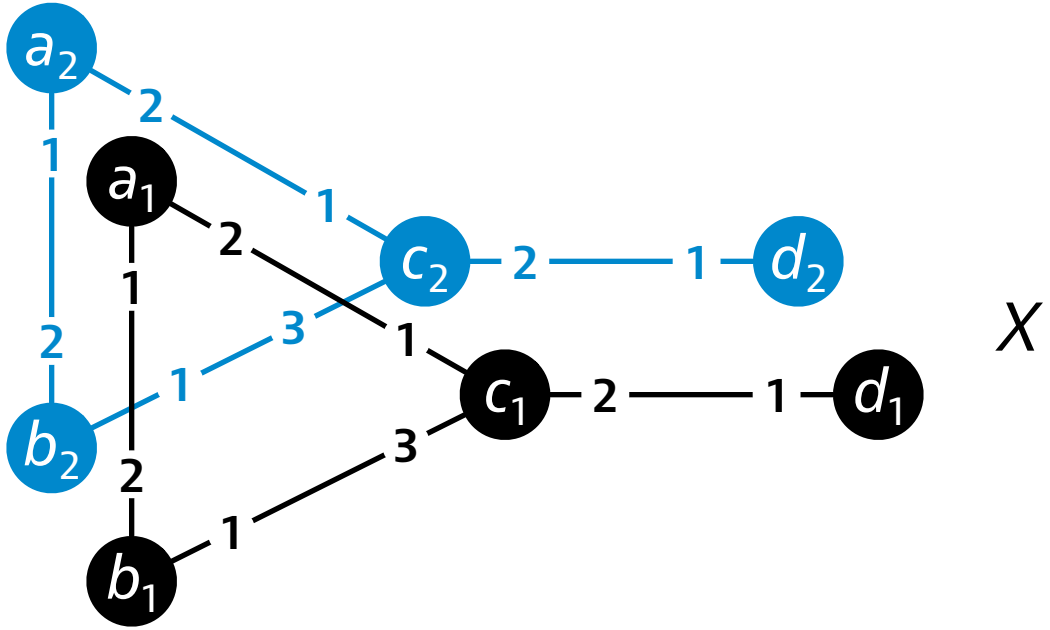

N
a
b
c
d
1
2
3
1
2
1
2
1
2
1

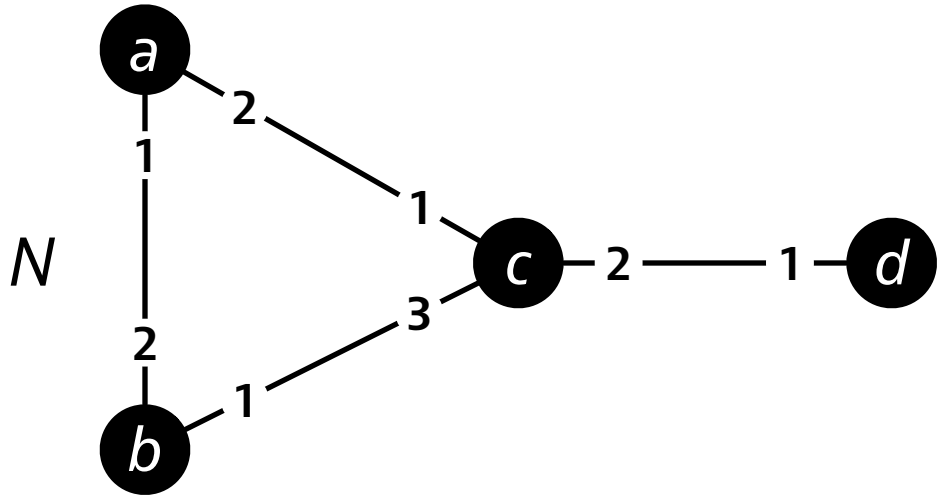

a_1
b_1
c_1
d_1
1
2
3
1
2
1
2
1
2
1

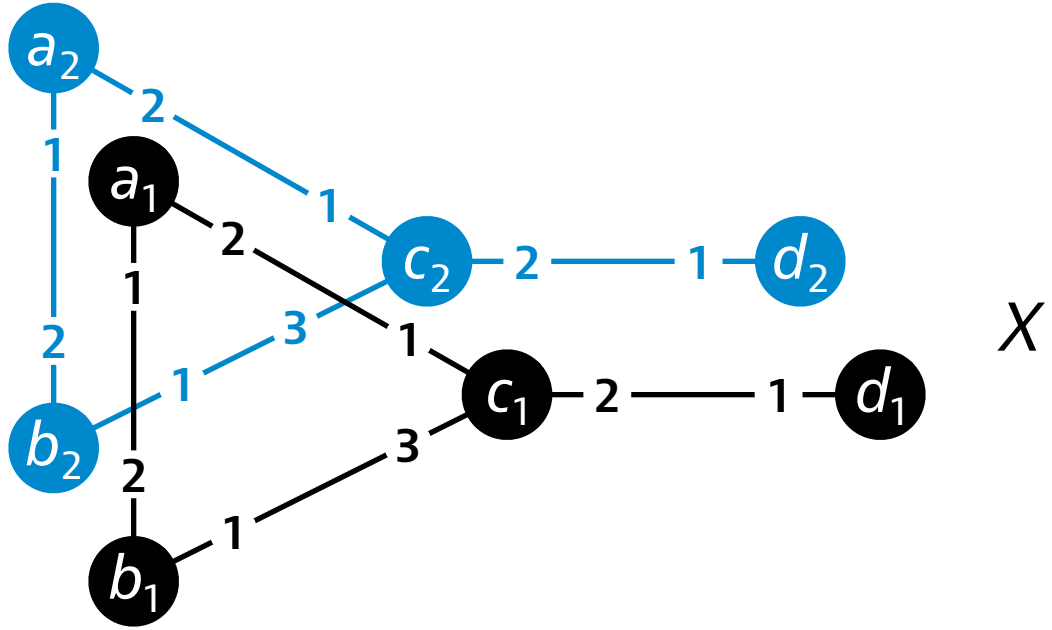

N
a
b
c
d
2
1
1
2
3
1
2
1

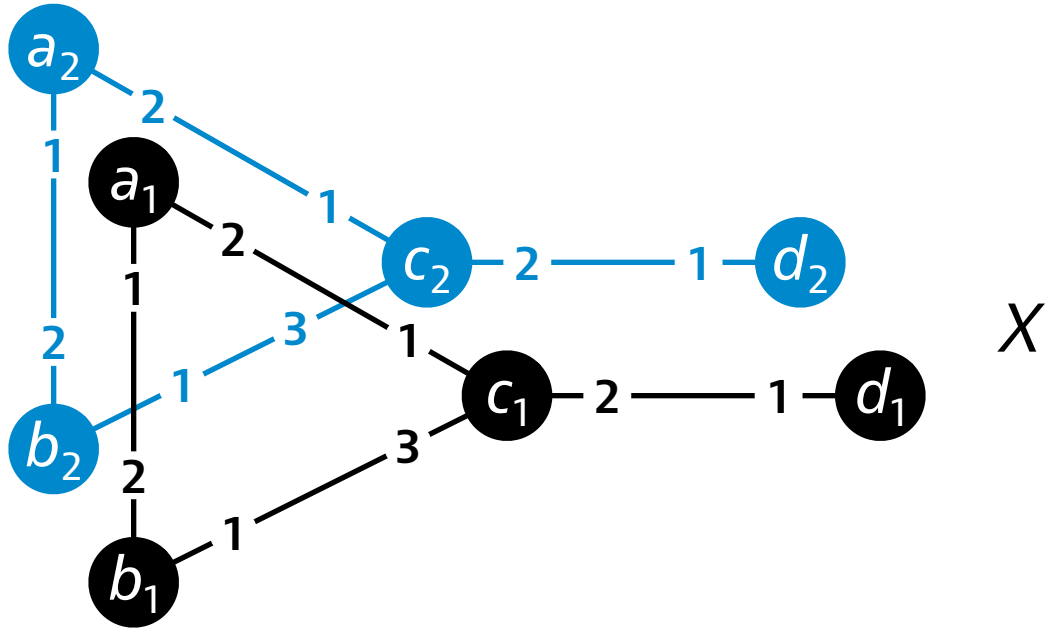

a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1
2
1
1
2
1
2
1
3
1
2
3
1
2
1

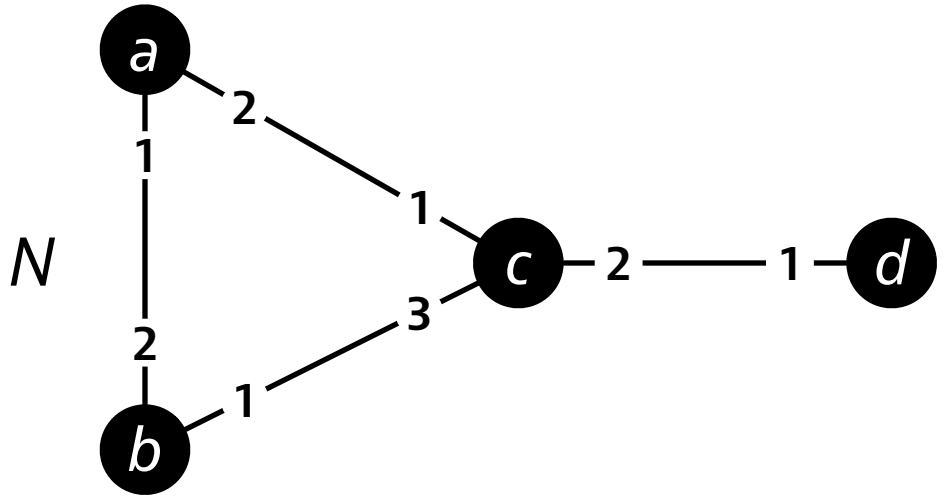

N
a
b
c
d
2
1
1
2
3
1
2
1

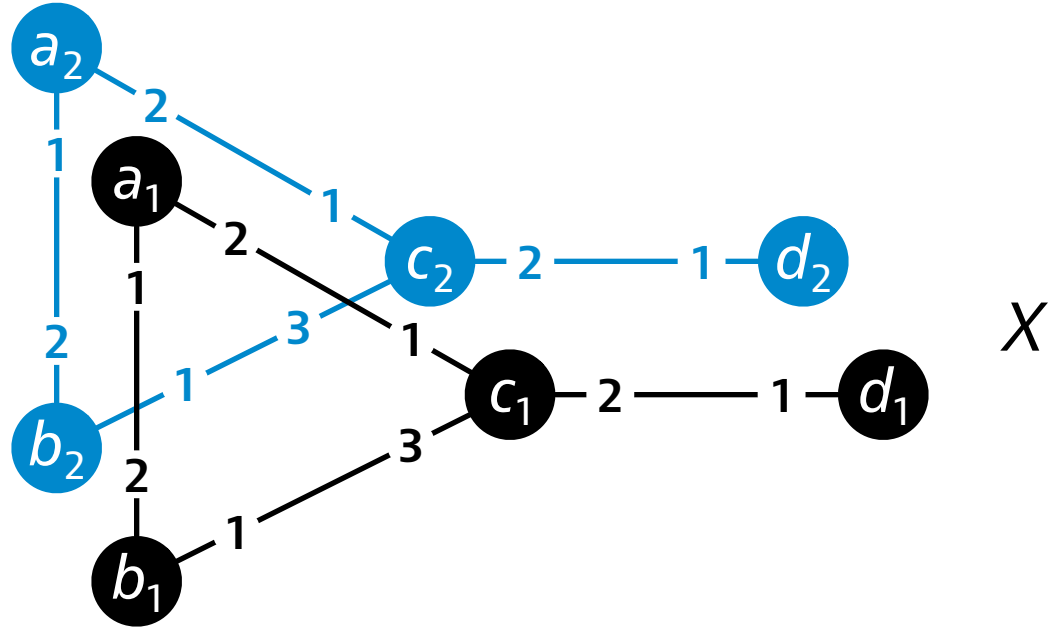

X
a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1
2
1
1
2
1
2
3
1
2
1
3
1
2
1

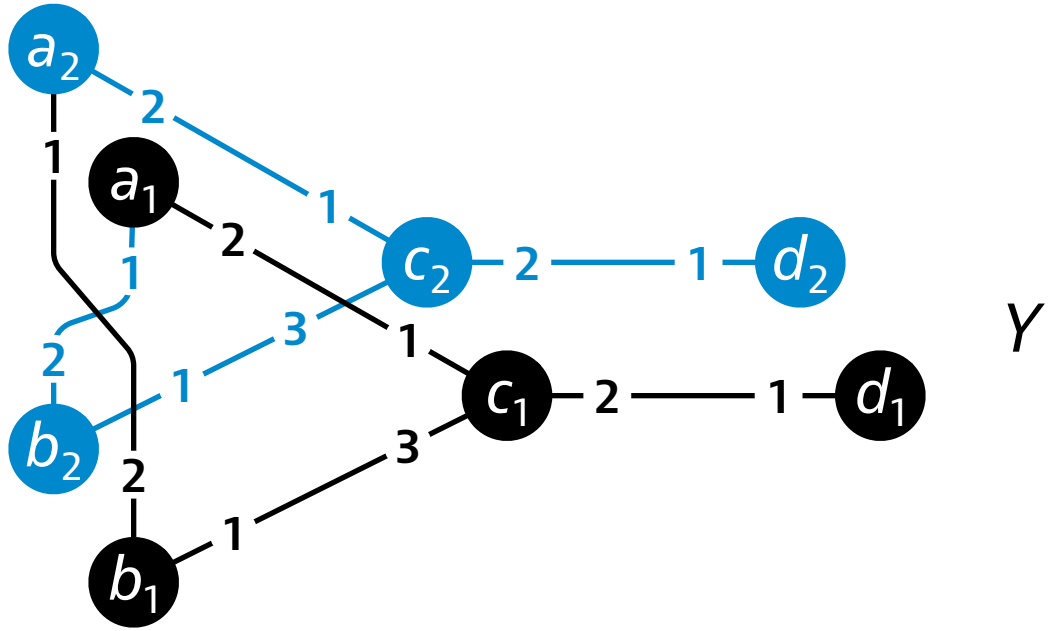

N
a
b
c
d
1
2
3

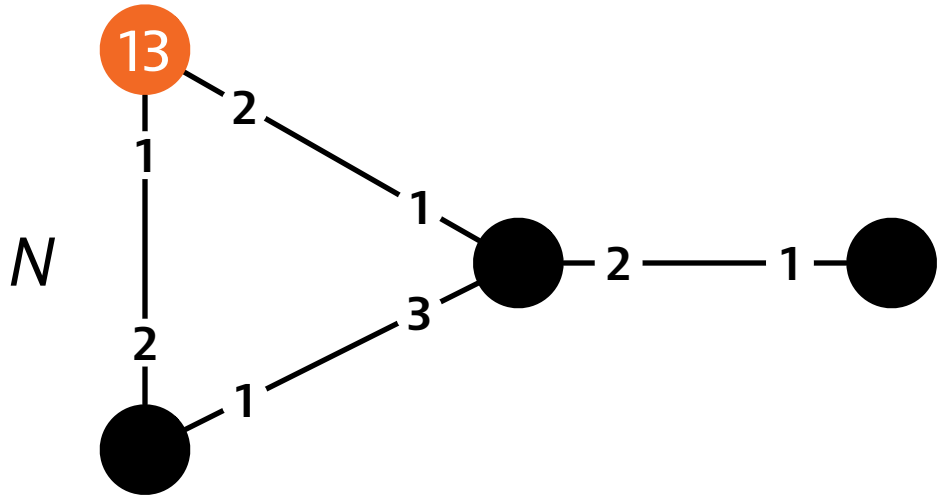

X
a2
a1
b2
b1
c2
c1
d2
d1

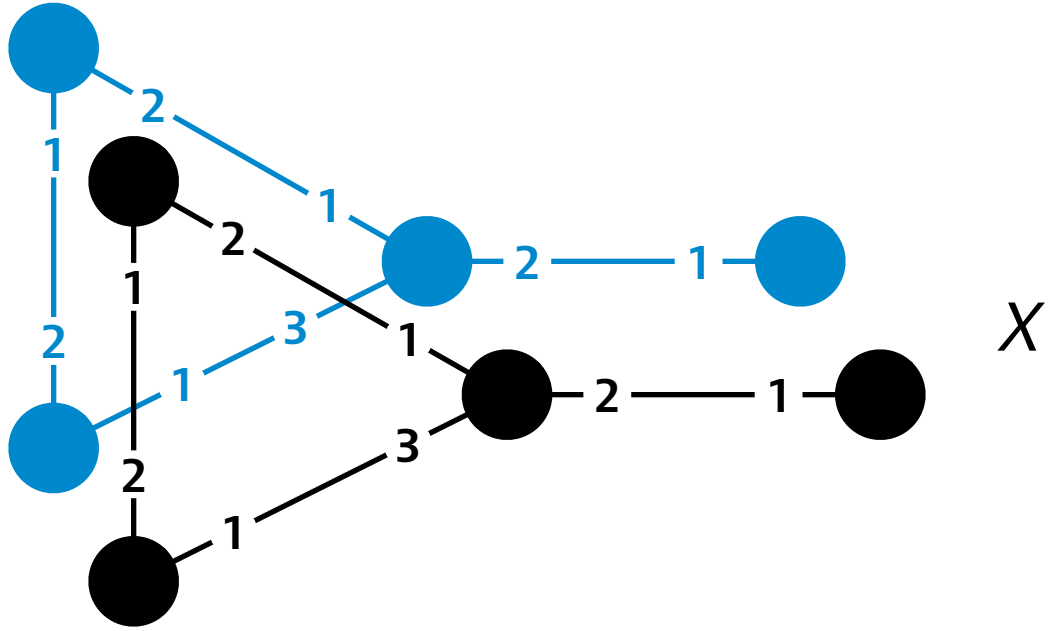

X
a2
a1
b2
b1
c2
c1
d2
d1

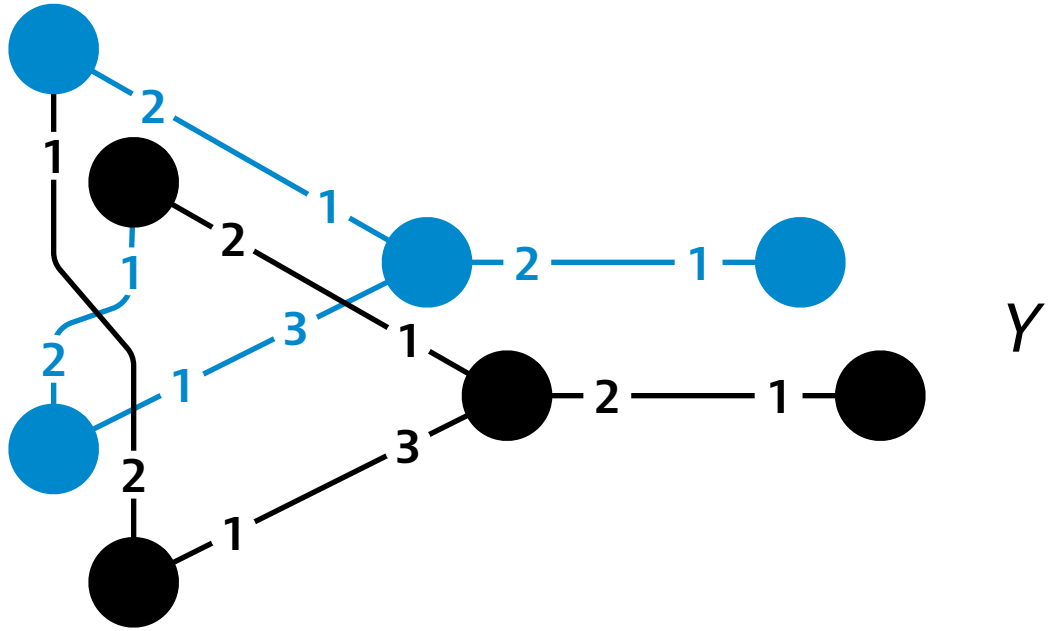

N
a
b
c
d
2
1
1
2
3
1
2
1

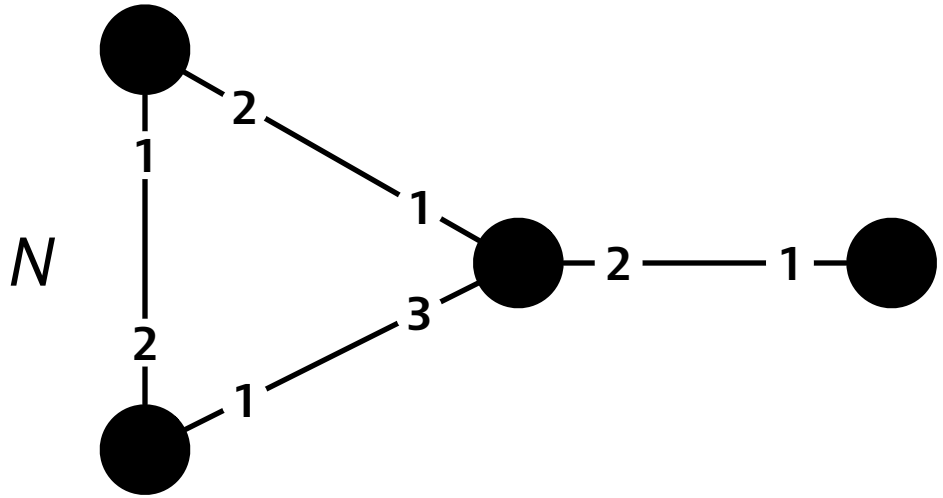

X
a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1
2
1
2
1
1
2
3
1
2
1
2
1
3
1
2
1

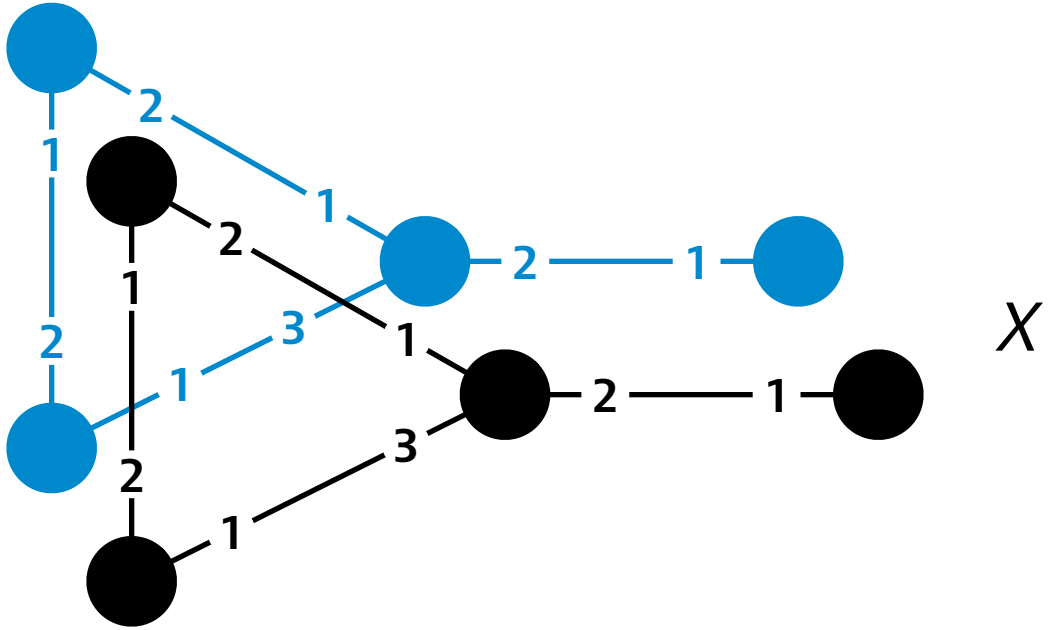

Y
a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1
2
1
2
1
1
2
3
1
2
1
2
1
3
1
2
1

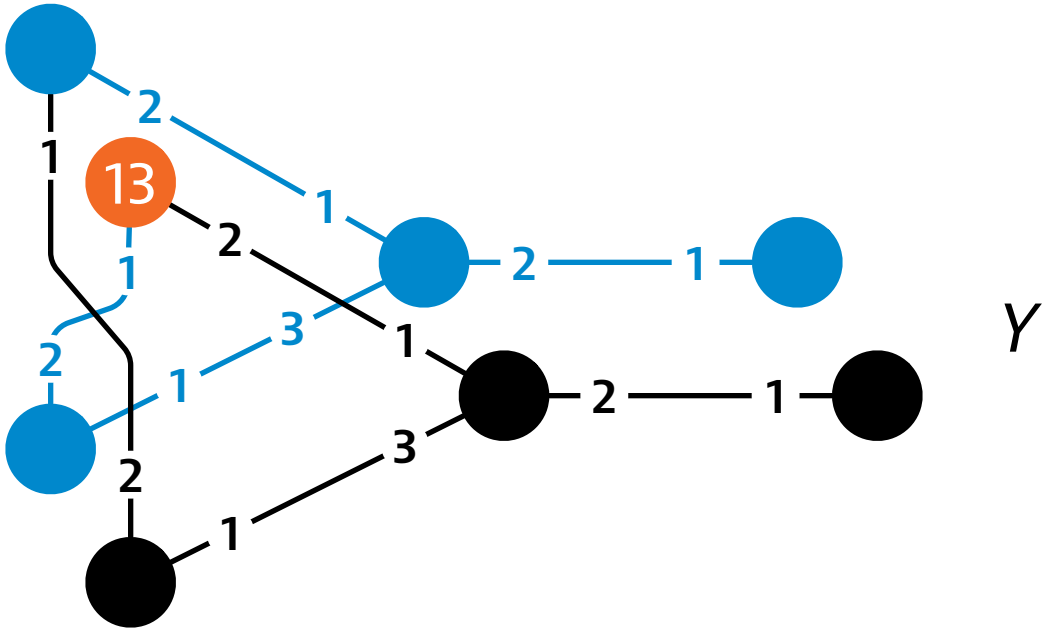

13
N

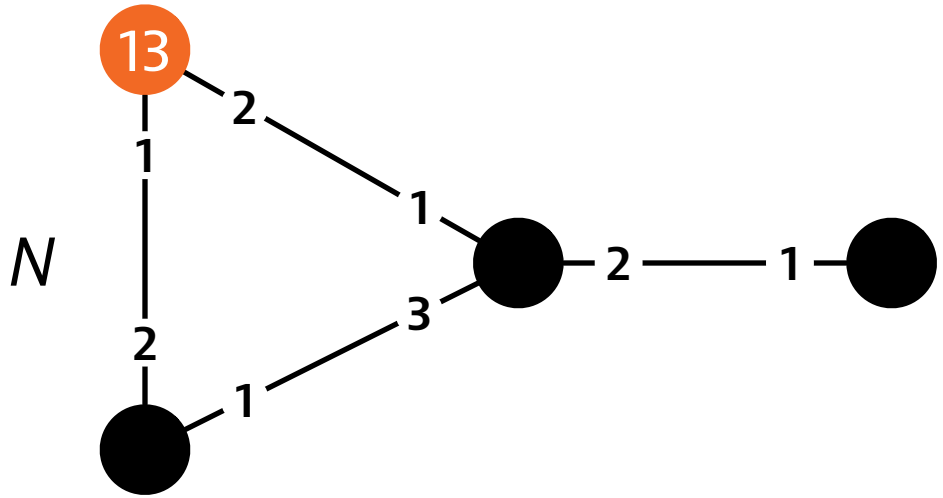

X

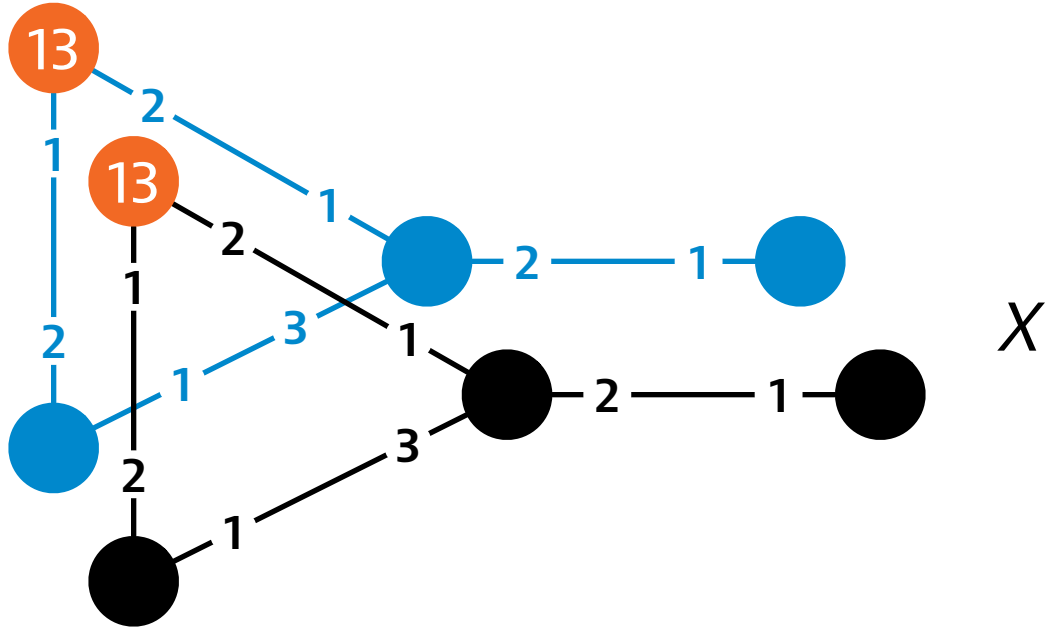

Y

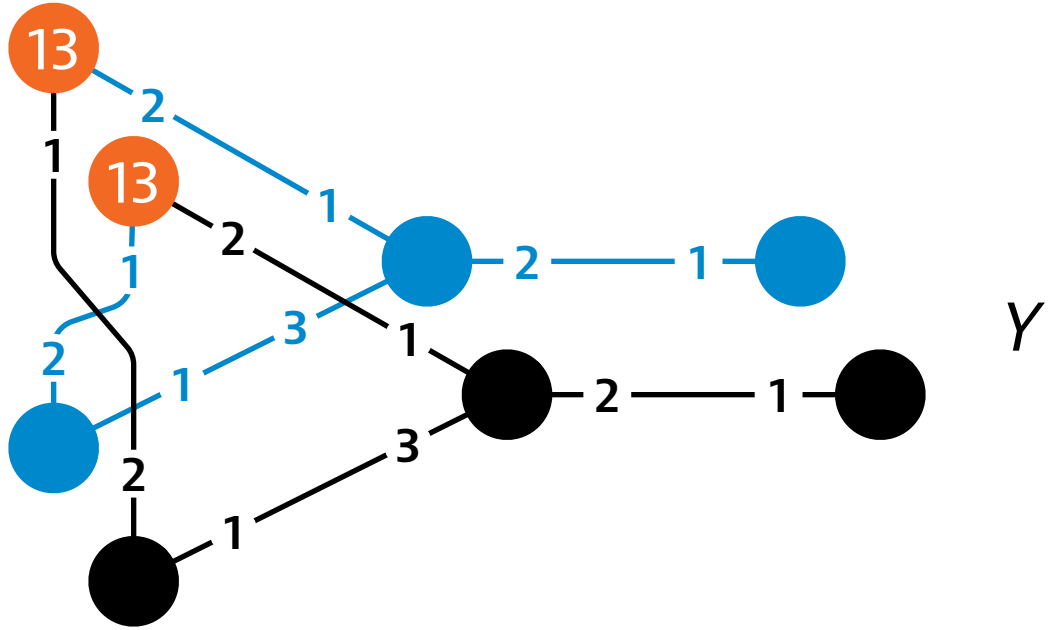

N
2
1
1
2
1
2
3
1
2
1

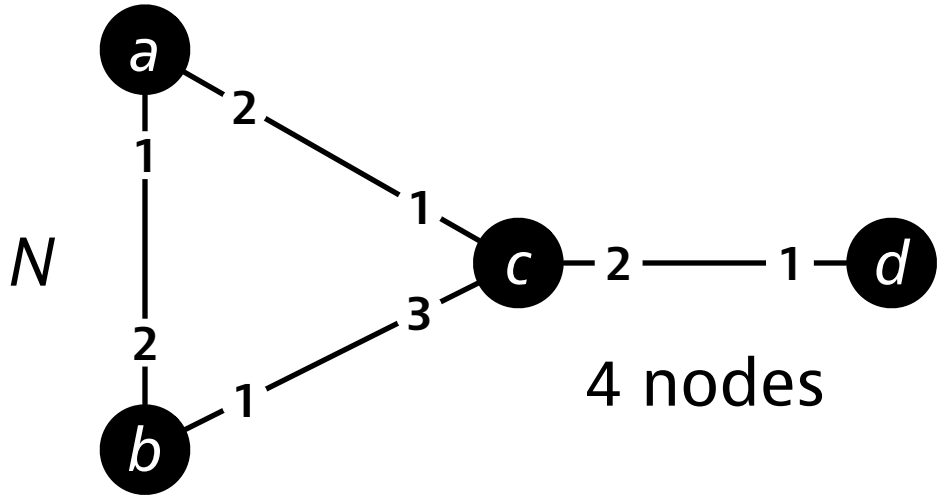

X
2
1
1
2
1
2
1
2
3
1
2
1
2
3
1
2
1

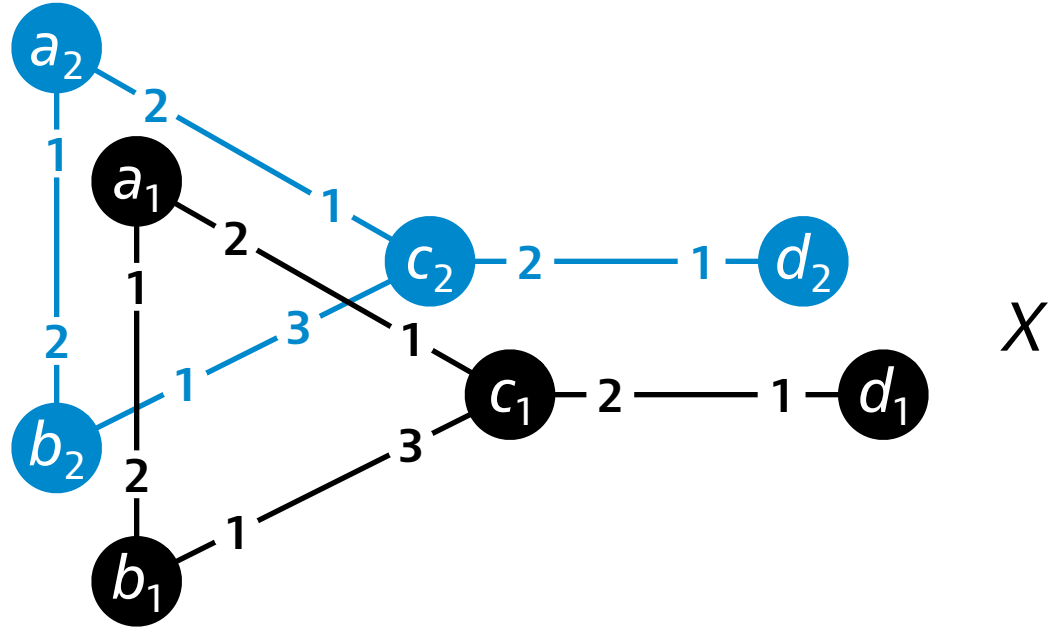

Y
13
2
1
1
2
1
2
1
2
3
1
2
1
2
3
1
2
1

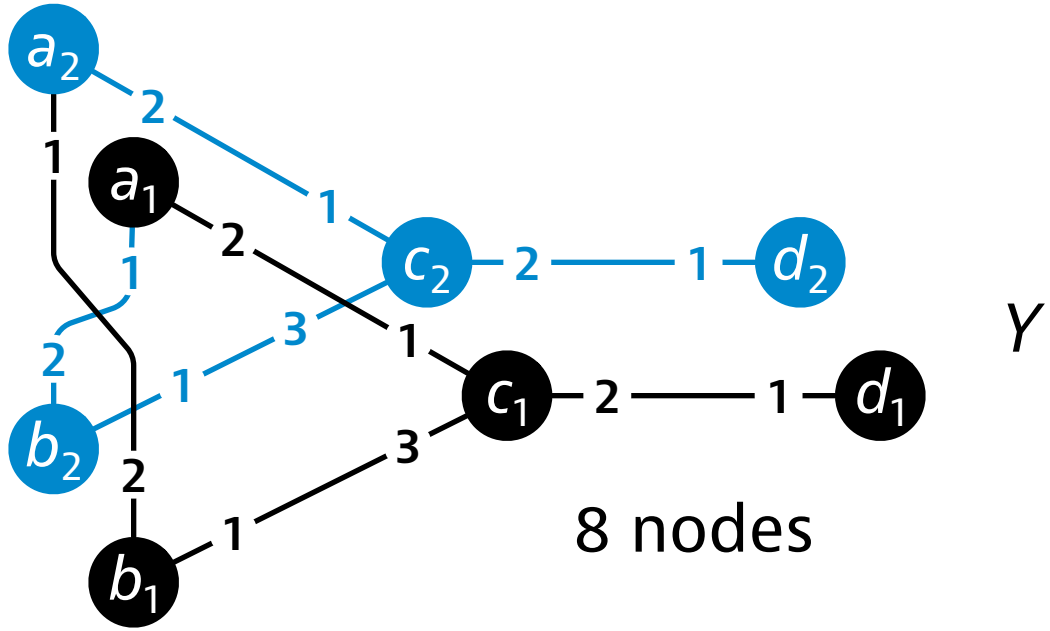

13
N

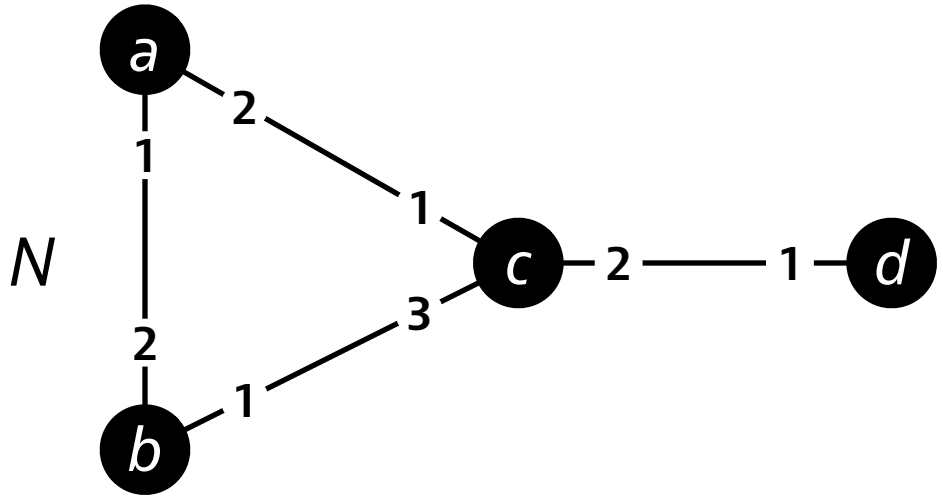

13
13
X

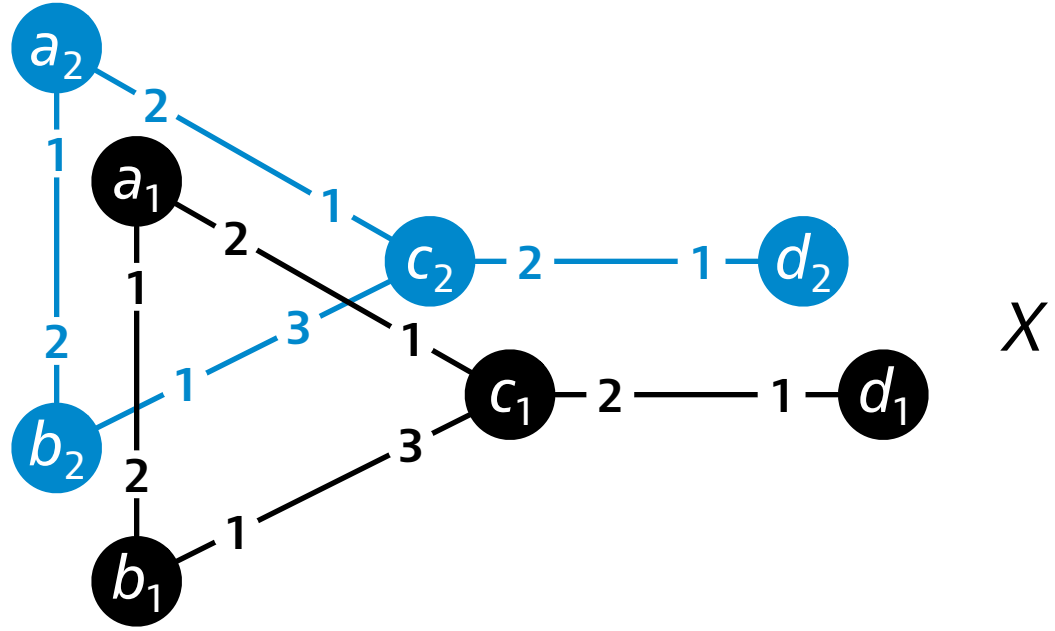

13
13
Y

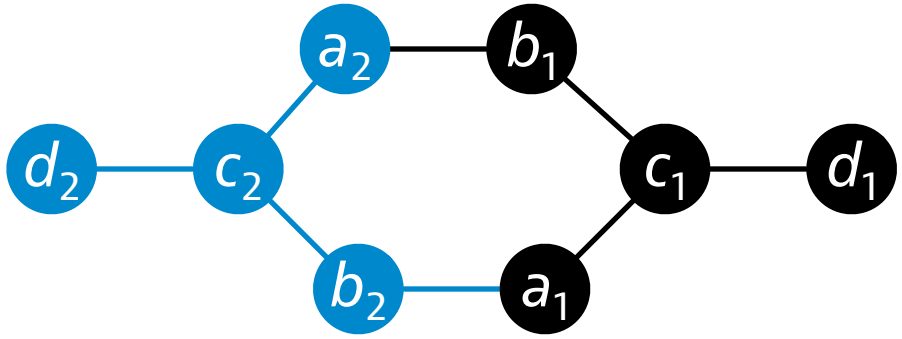

N
a
b
c
d
4 nodes


X

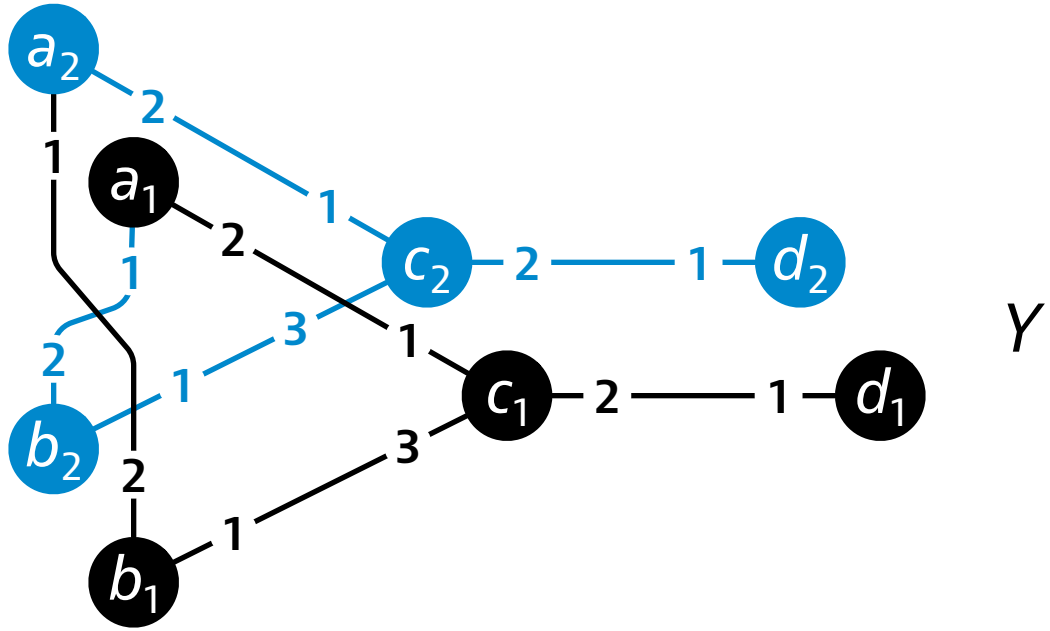

Y
8 nodes

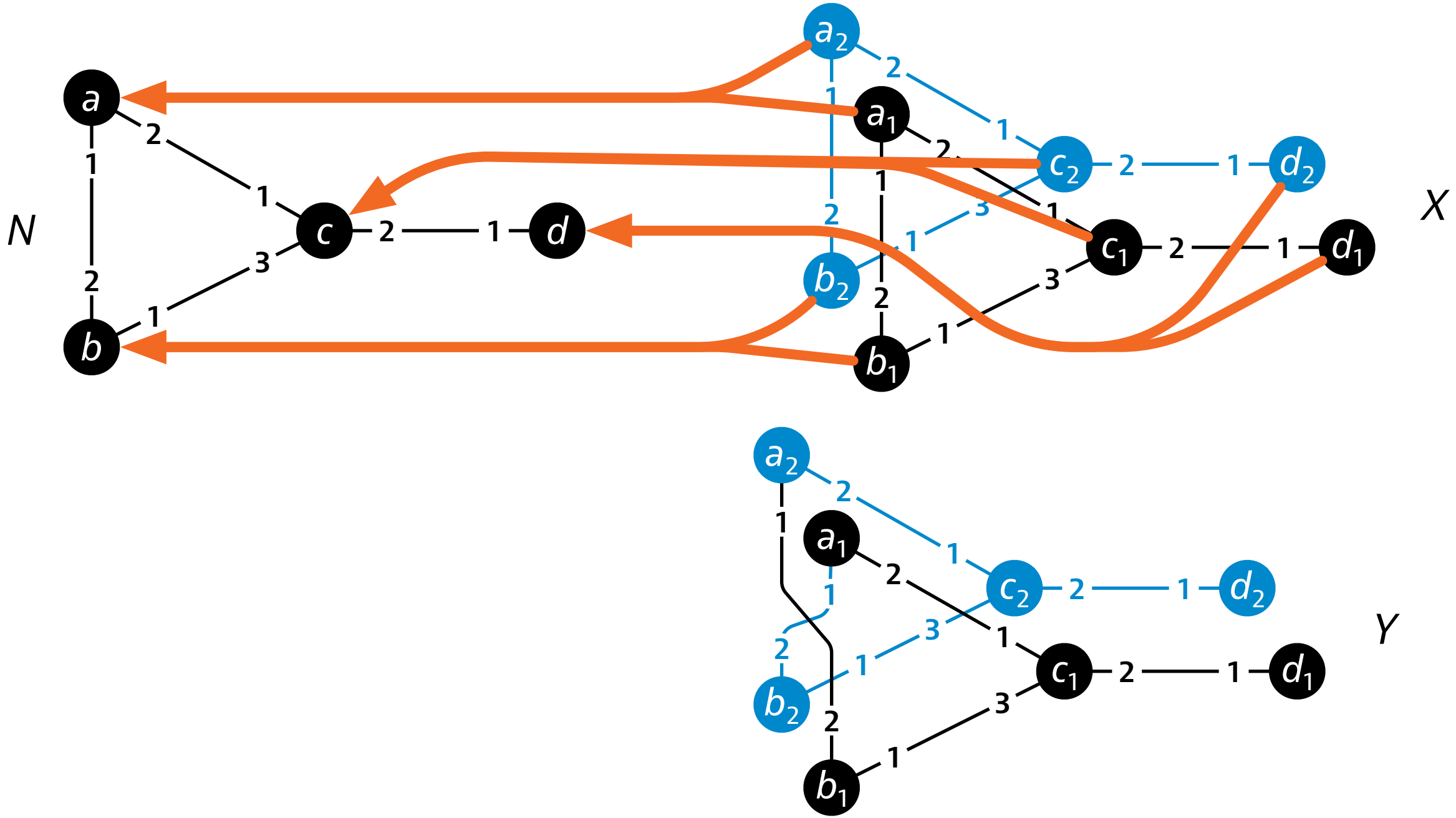

N
a
b
c
d
1
2
3

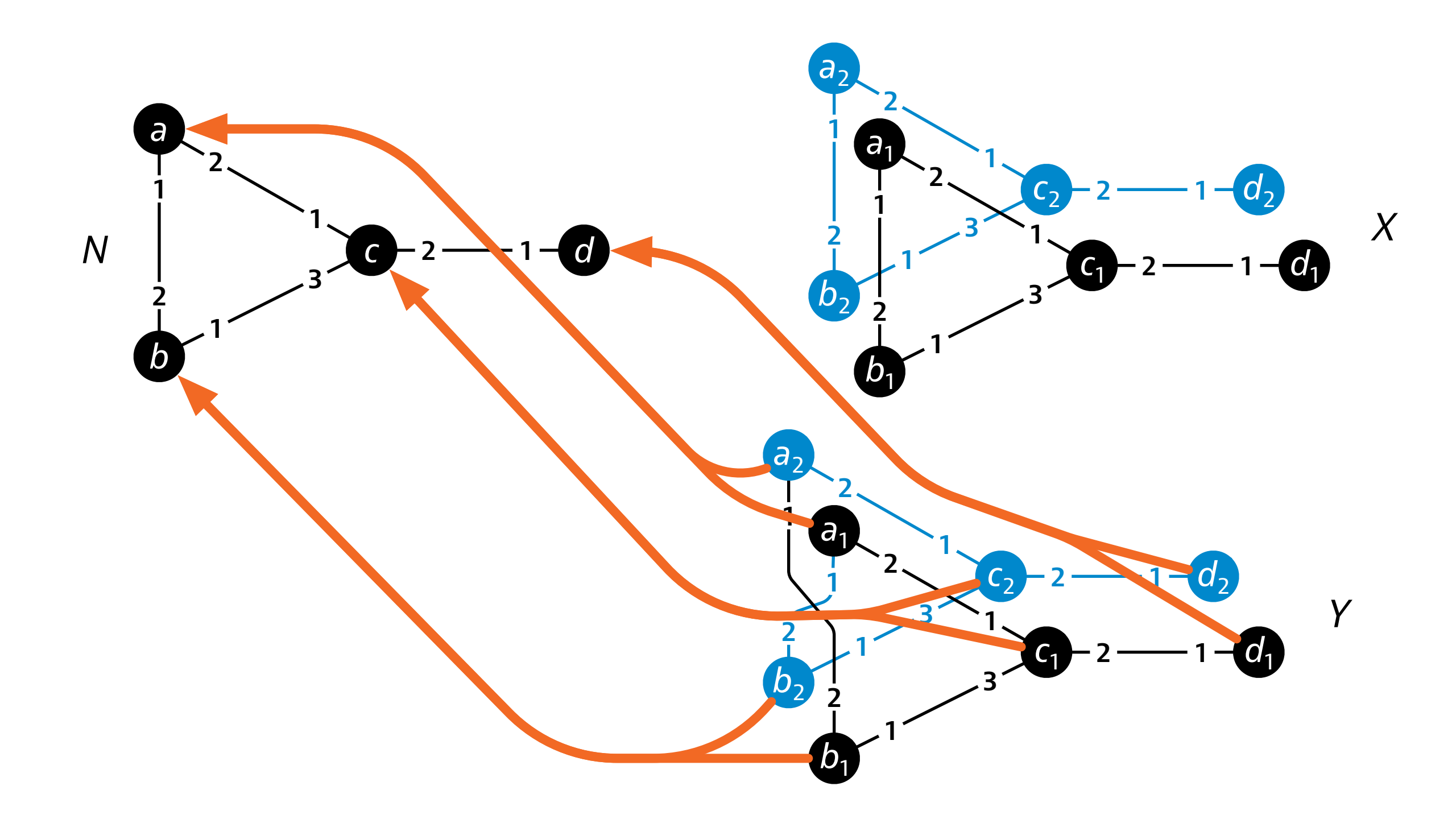

X
a2
a1
b2
b1
c2
c1
d2
d1

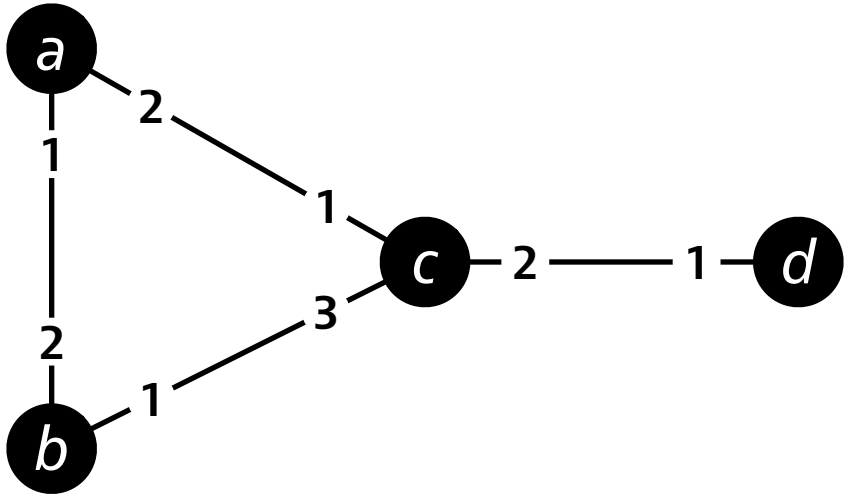

a2
b1
d2
c2
c1
d1
b2
a1

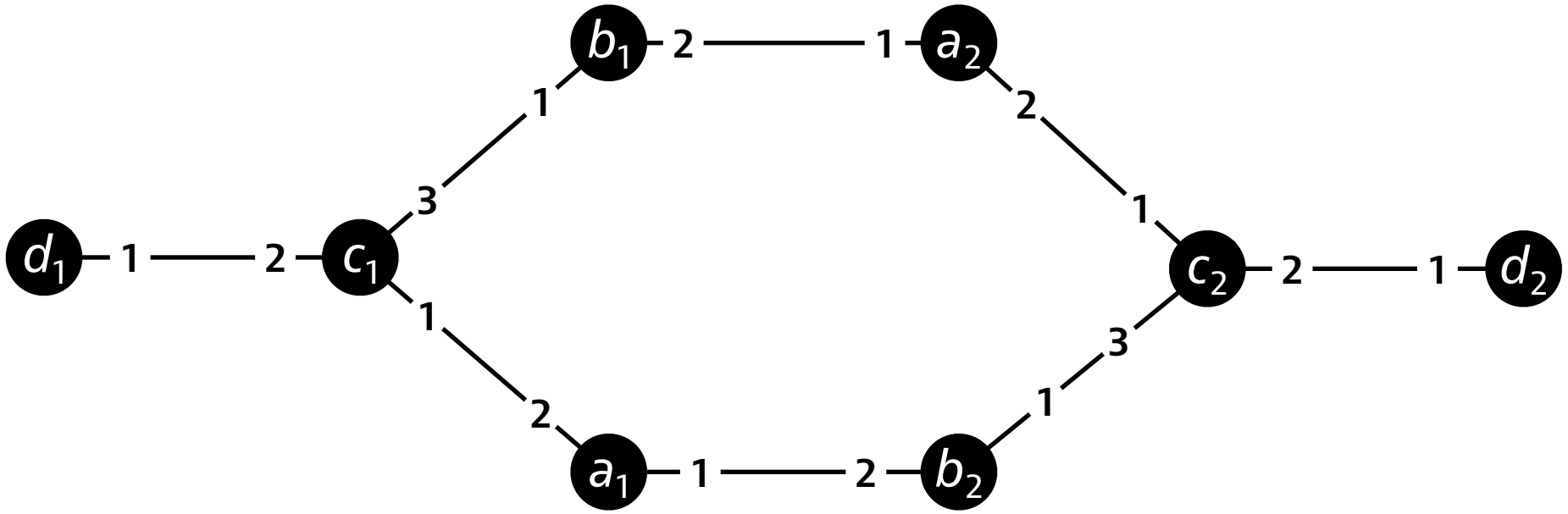
=

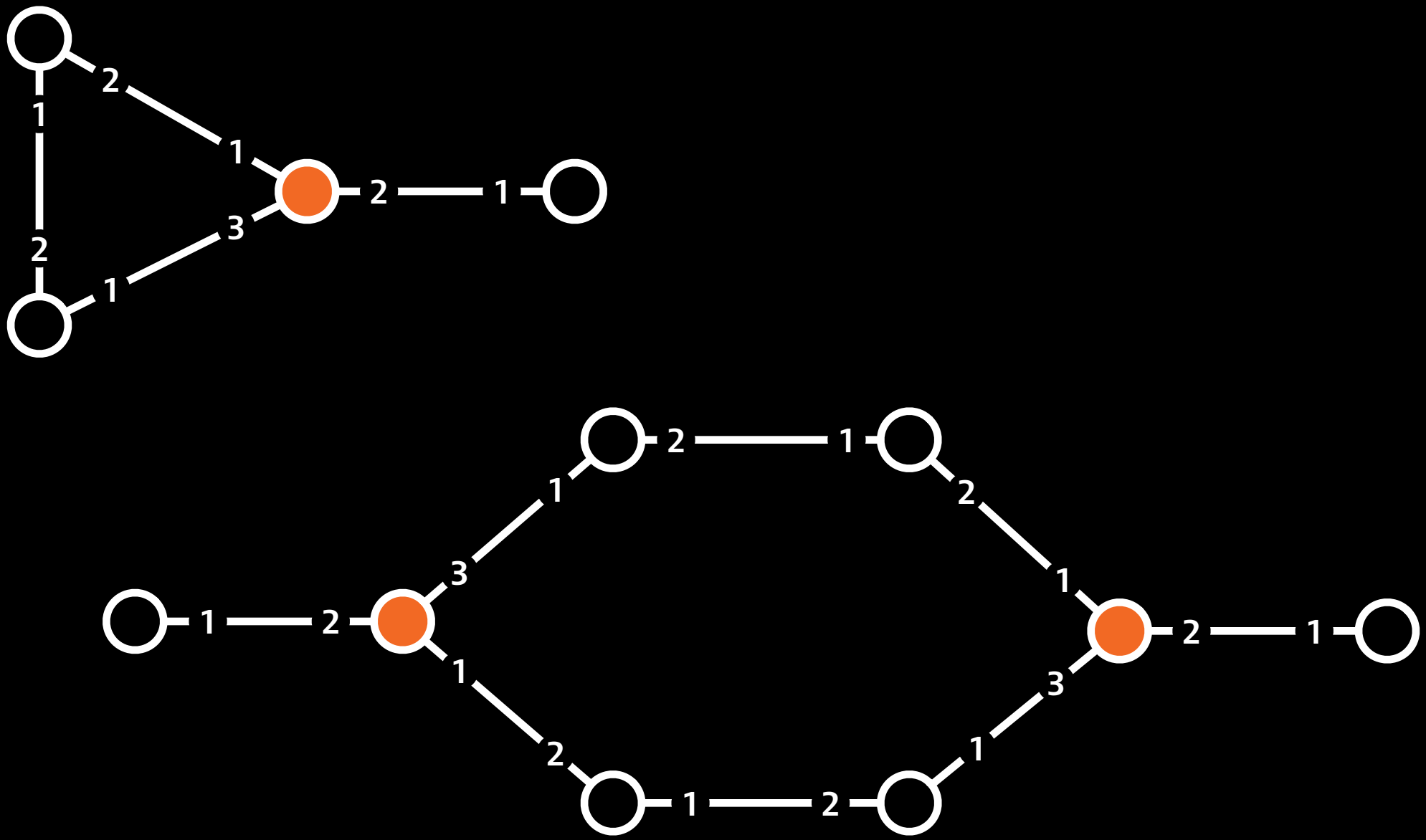

Y
a2
a1
b2
b1
c2
c1
d2
d1

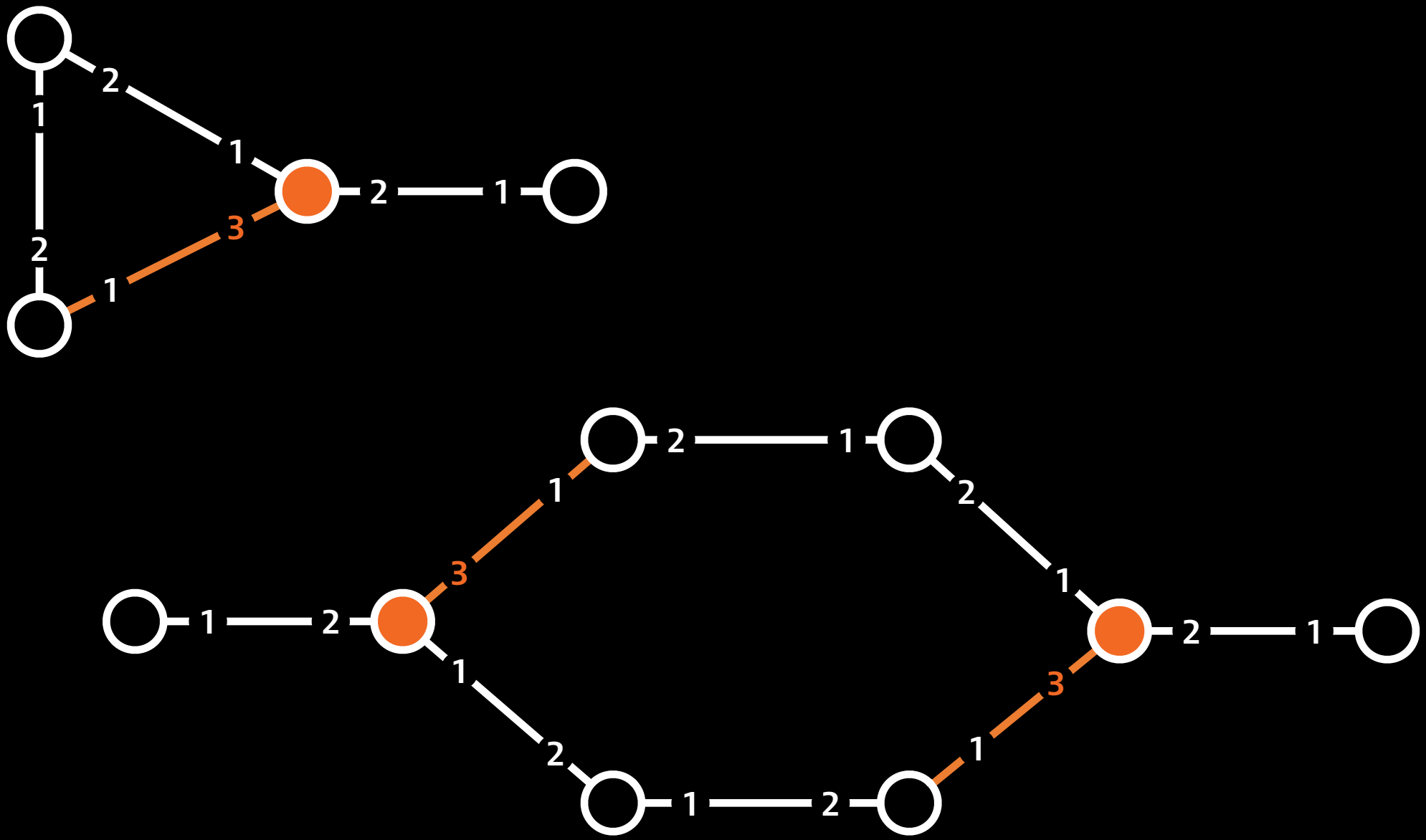

N
a
b
c
d
X
a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1
Y

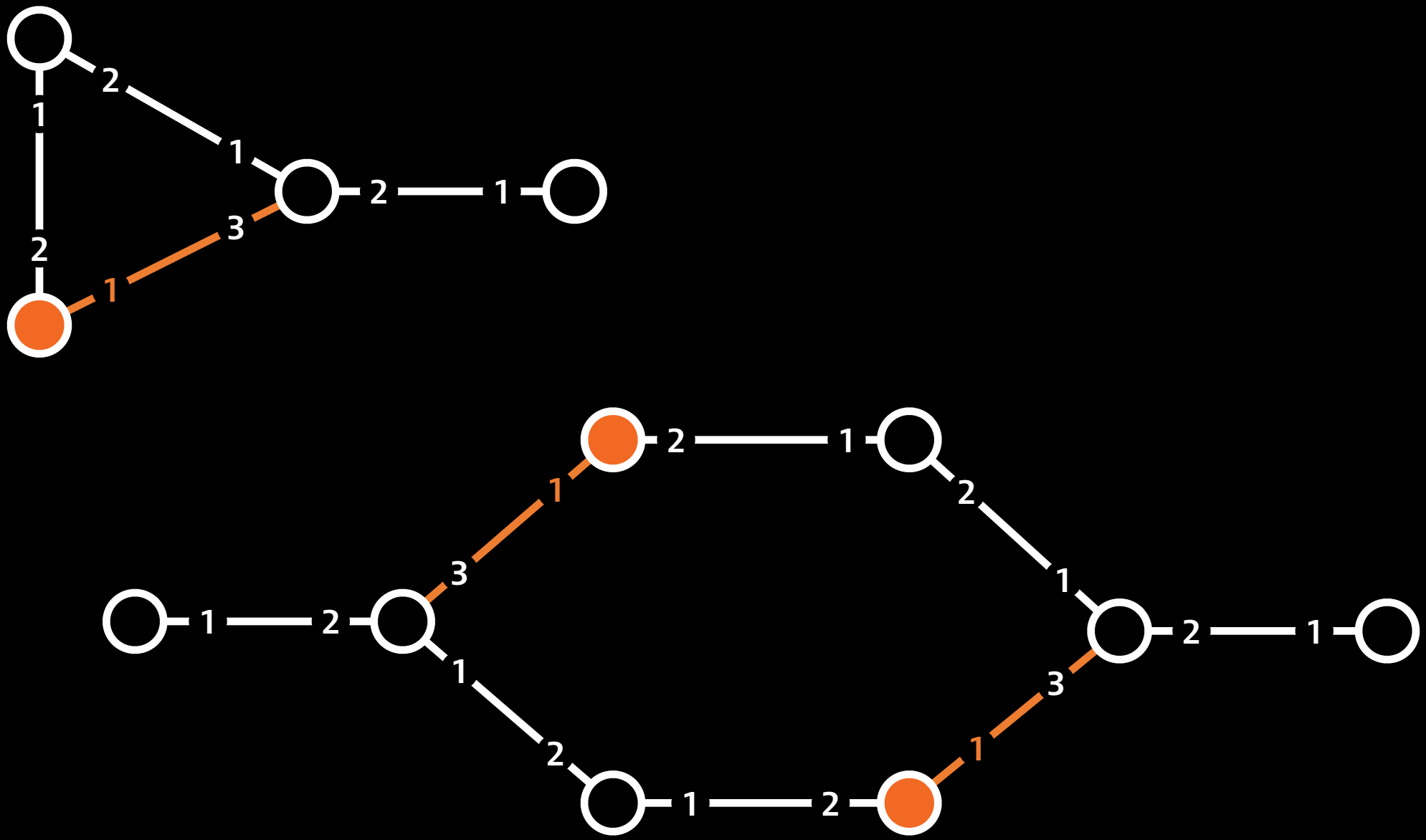

N
a
b
c
d
X
a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1
Y
a_2
a_1
b_2
b_1
c_2
c_1
d_2
d_1

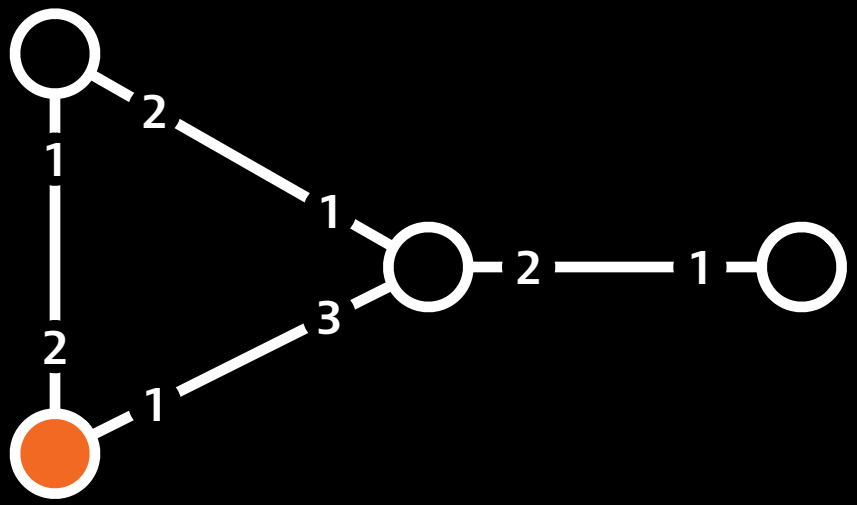

a
b
c
d
2
1
1
2
3
2
1
1

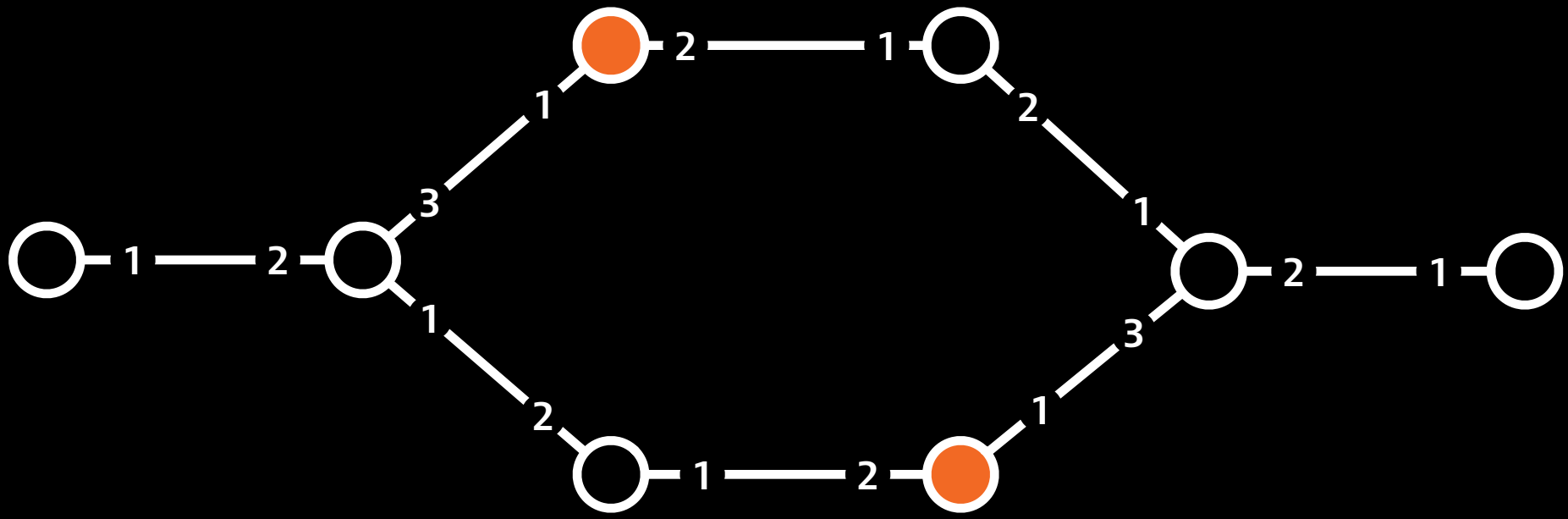

b_1
a_2
d_1
c_1
c_2
d_2
a_1
b_2
2
1
1
2
3
1
2
1
1
2
3
1
2
1
1
2

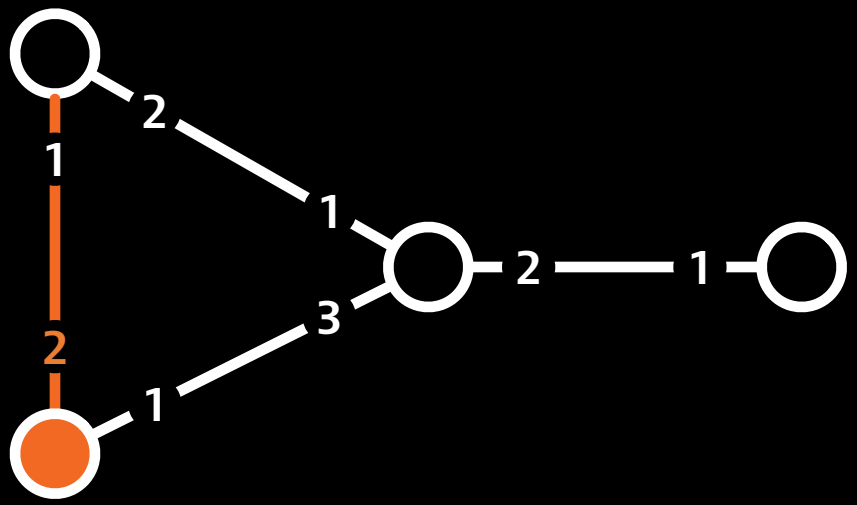

2
1
1
2
1
3
2
1
2
1
1
2
3
1
2
1
1
2
1
2
1
2
1
3
1
2
1
2

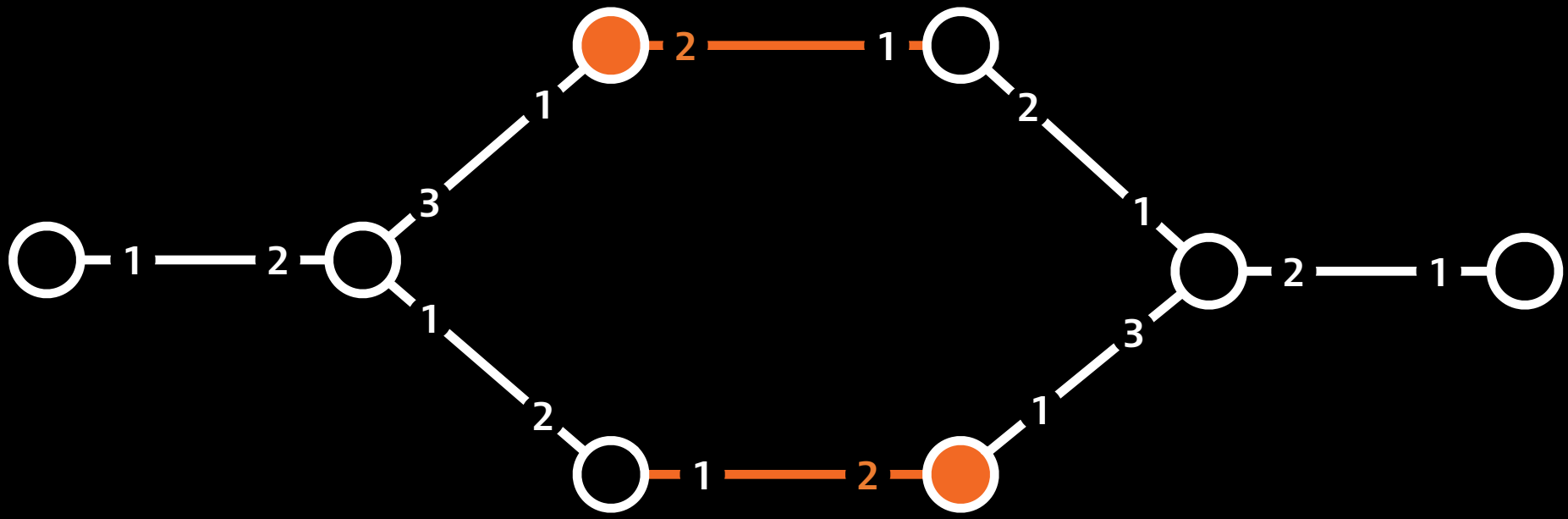

2
1
1
2
1
3
2
1
2
1
1
2
1
3
1
2
1
2
1
2
1
3
1
2
1
2

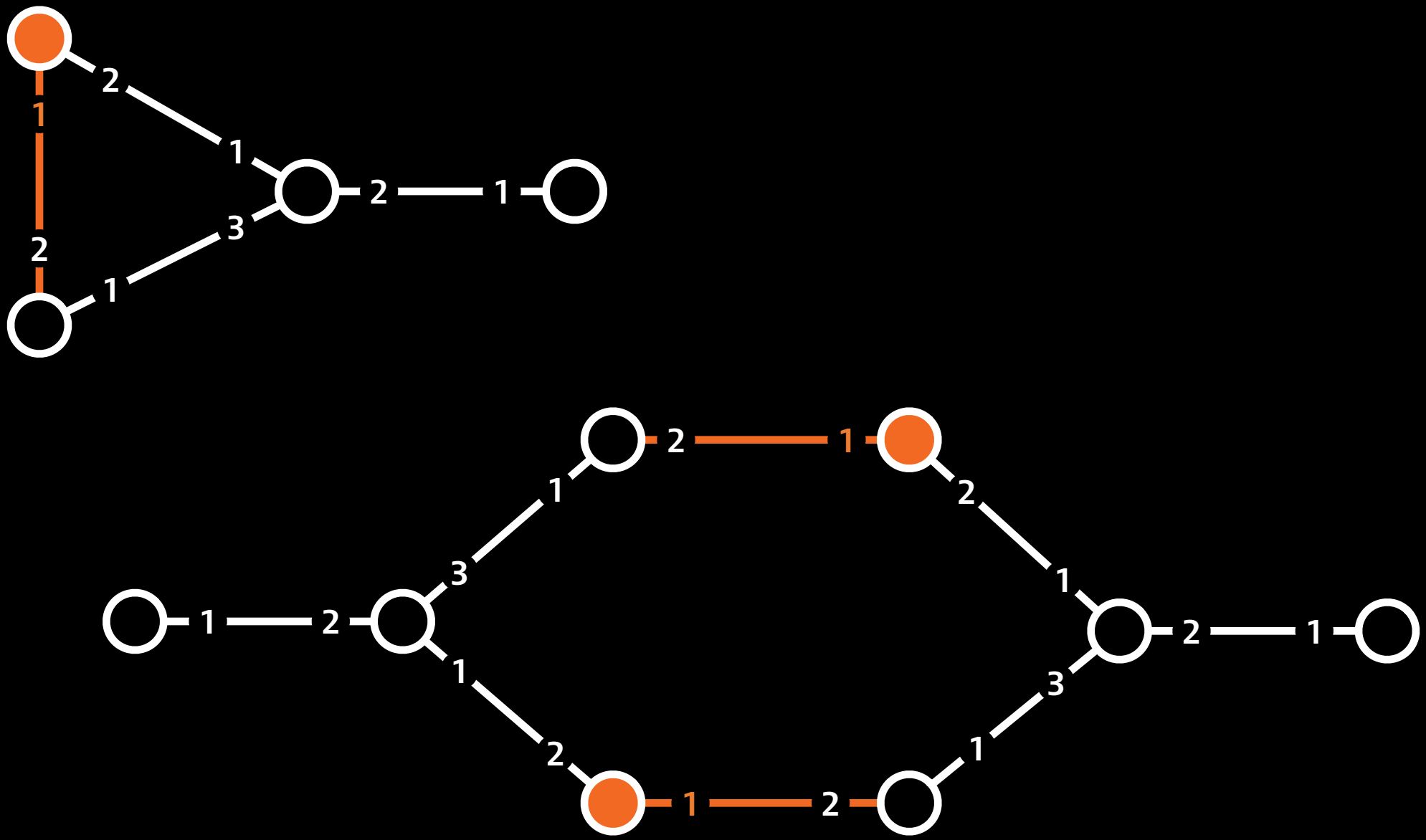

2
1
1
2
1
3
2
1
2
1
1
2
3
1
2
1
2
1
1
2
3
1
2
1
2
1

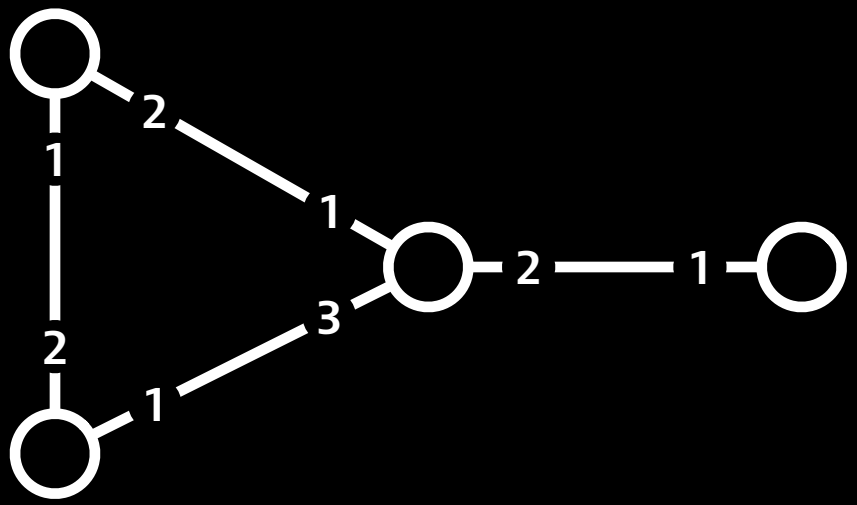

2
1
1
2
1
3
2
1

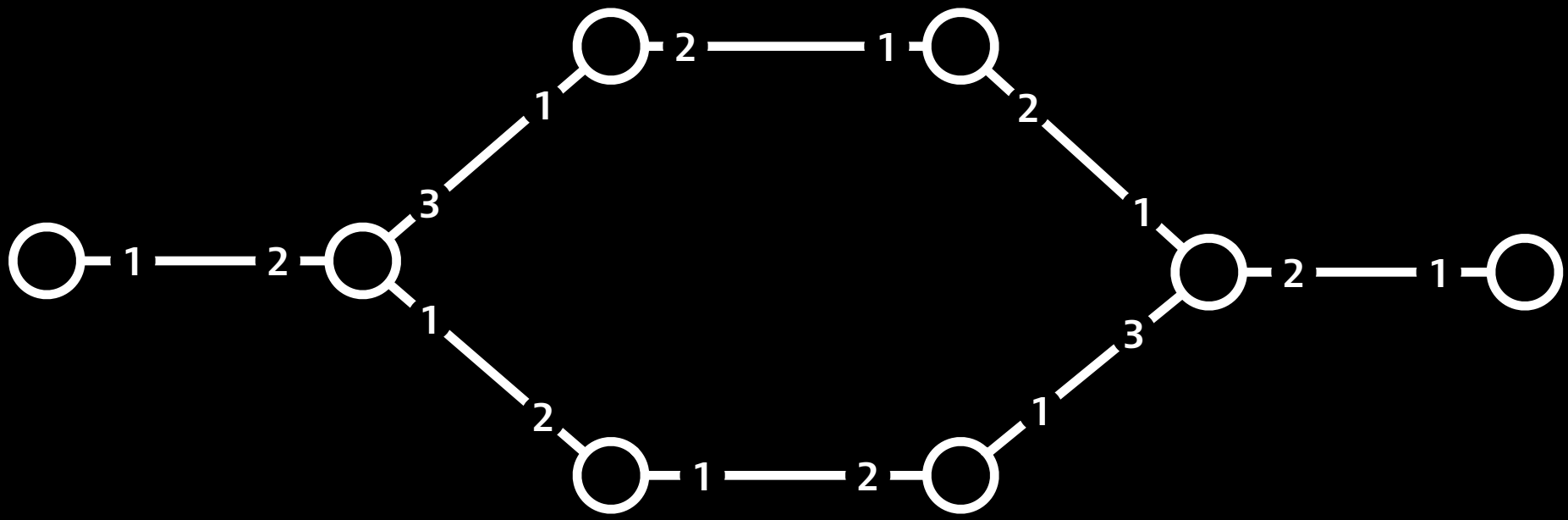

2
1
1
2
3
1
2
1
2
1
3
1
2
1
2

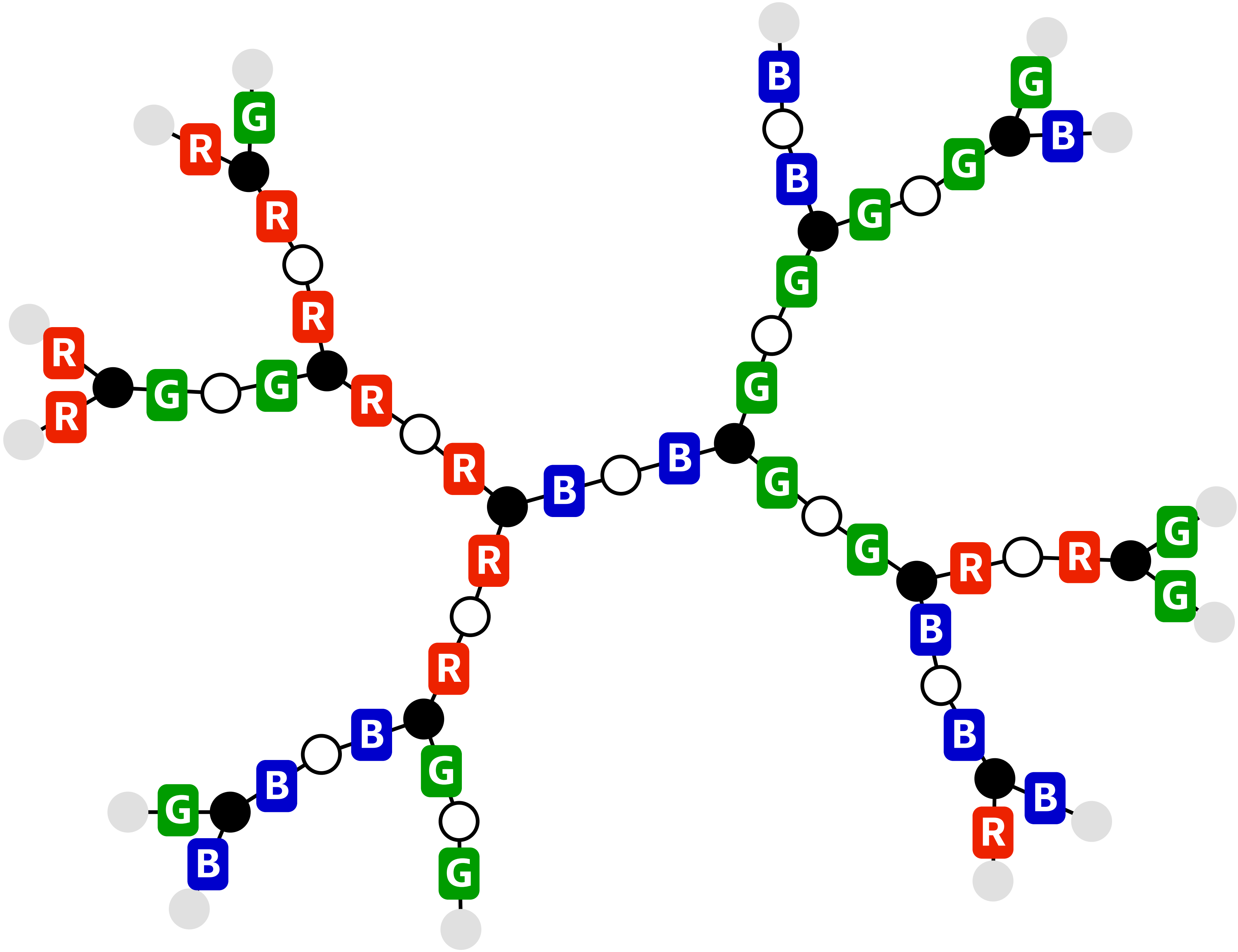

2
1
1
2
1
3
2
1

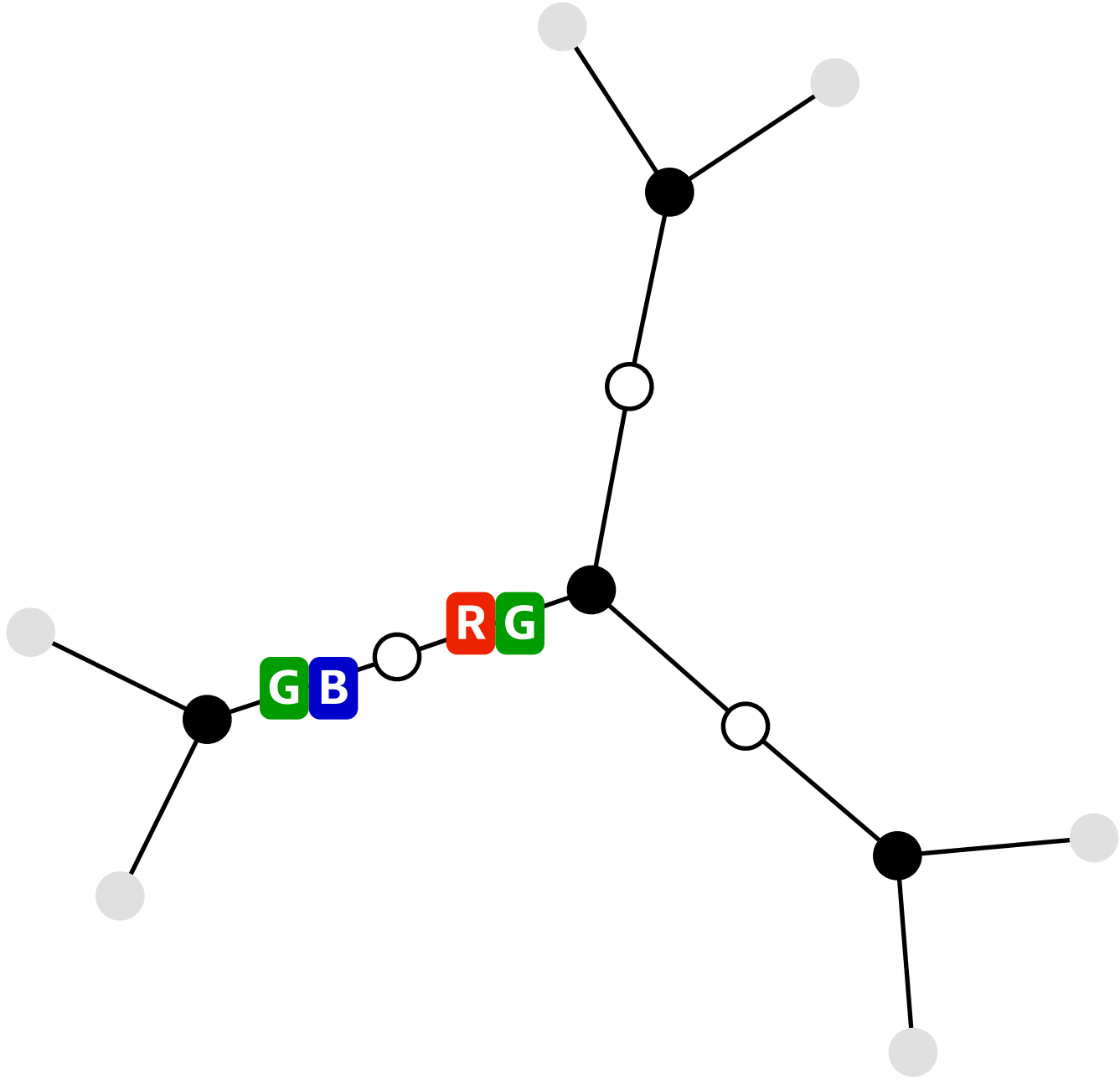

2
1
1
2
1
3
2
1
2
1
3
1
2
1
2
1


2
1
1
2
1
3
2
1
2
1
1
2
3
1
2
1
2
1
1
2
3
1
2
1
2
1


2
1
1
2
1
3
2
1


2
1
1
2
3
1
2
1
2
1
3
1
2
1
2




R
G
G
B