# Elmo: Recursive Virtual Channels for Bitcoin

Orfeas Stefanos Thyfronitis Litos
University of Edinburgh
10/5/2021


20,000 tx/s


7 tx/s

Problem

All txs validated by all wallets

Solution

- Move most txs off-chain
- Resolve disputes on-chain

# Features

- Enables long-lived “virtual” channels w/o an on-chain funding TX
- Virtual channels built on top of a path of preexisting “base” channels – left endpoint funds the channel
- Base channels may themselves be virtual!
- Virtual channels can leverage a path of many base channels

# Construction

Intermediary *i* has 3 classes of TXs:

- “Initiator” TX
  - Spends left & right funding outputs
  - Has virtual output with interval [*i*]

# Construction

Intermediary *i* has 3 classes of TXs:

- “Initiator” TX
  - Spends left & right funding outputs
  - Has virtual output with interval [*i*]
- “Extend-interval” TXs
  - Spends 1 funding output and 1 virtual output with interval [*j*, …, *i*-1] or [*i*+1, …, *j*]
  - Has virtual output w/ interval [*j*, …, *i*] or [*i*, …, *j*]

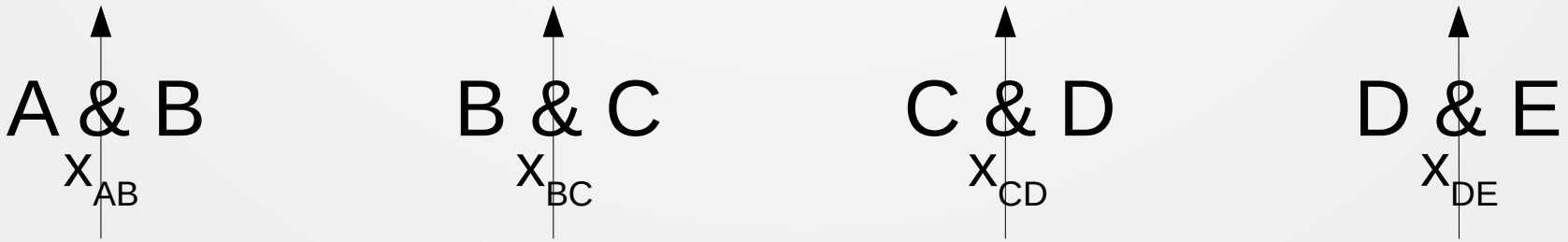
# Construction

Intermediary *i* has 3 classes of TXs:

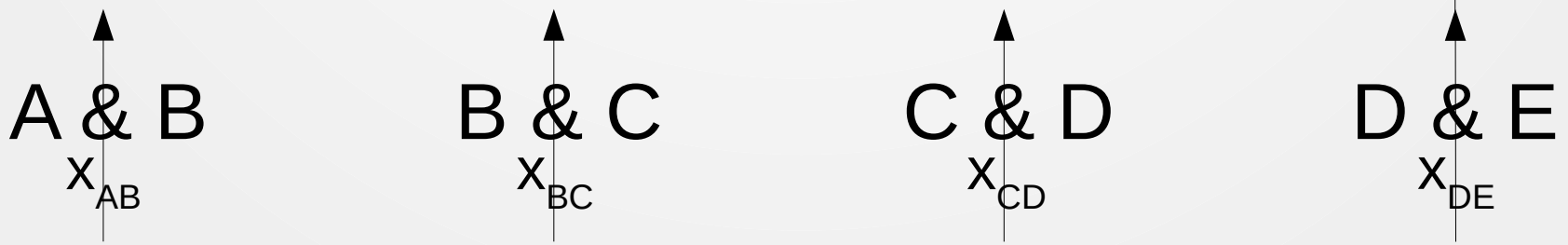
- "Initiator" TX
  - Spends left & right funding outputs
  - Has virtual output with interval [*i*]
- "Extend-interval" TXs
  - Spends 1 funding output and 1 virtual output with interval [*j*, ..., *i*-1] or [*i*+1, ..., *j*]
  - Has virtual output w/ interval [*j*, ..., *i*] or [*i*, ..., *j*]
- "Merge-intervals" TXs
  - Spends 2 virtual outputs with intervals [*j*, ..., *i*-1] and [*i*+1, ..., k]
  - Has virtual output with interval [*j*, ..., *k*]

# Example 1
# Fundee wants to close

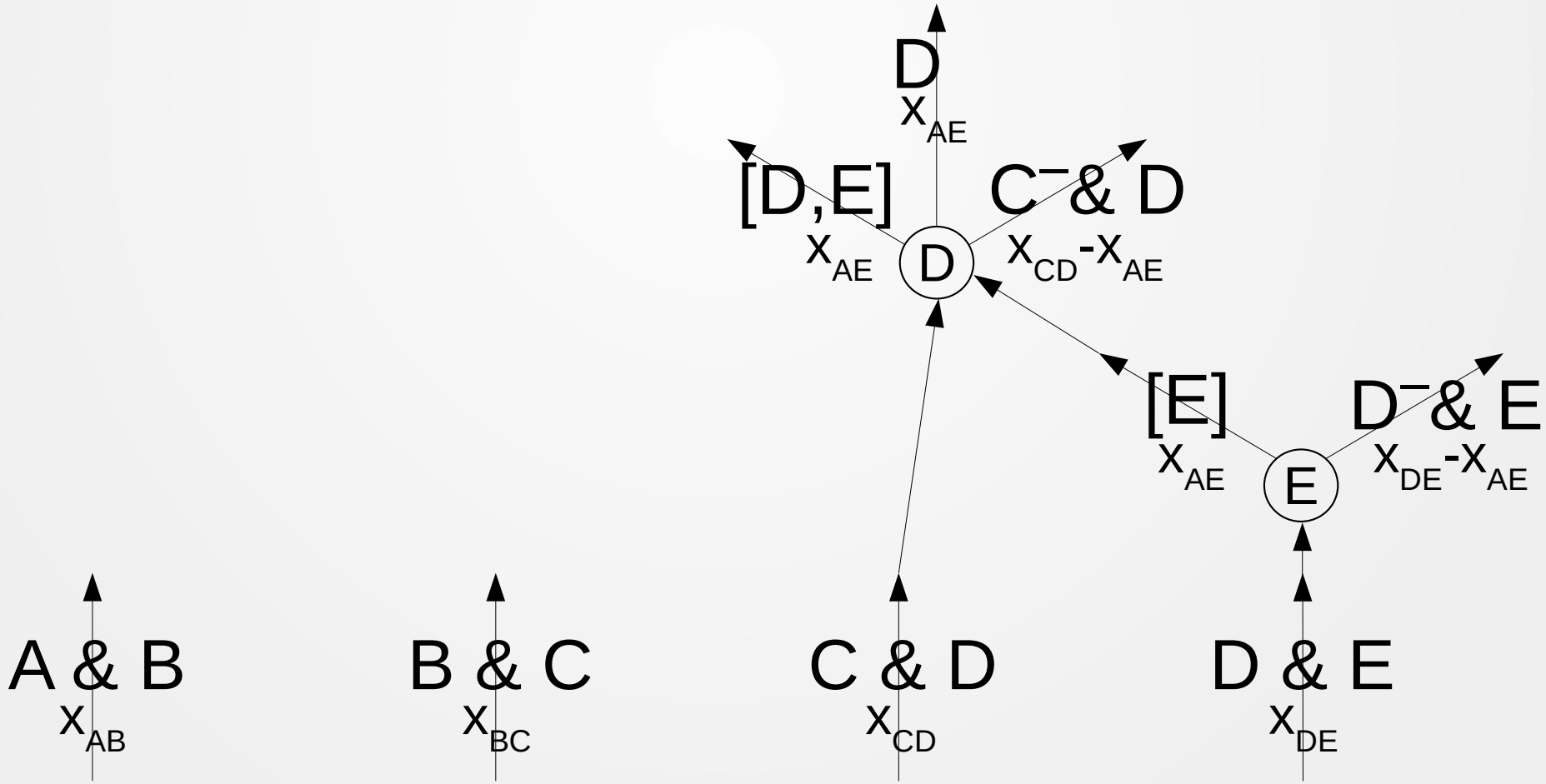
t=0

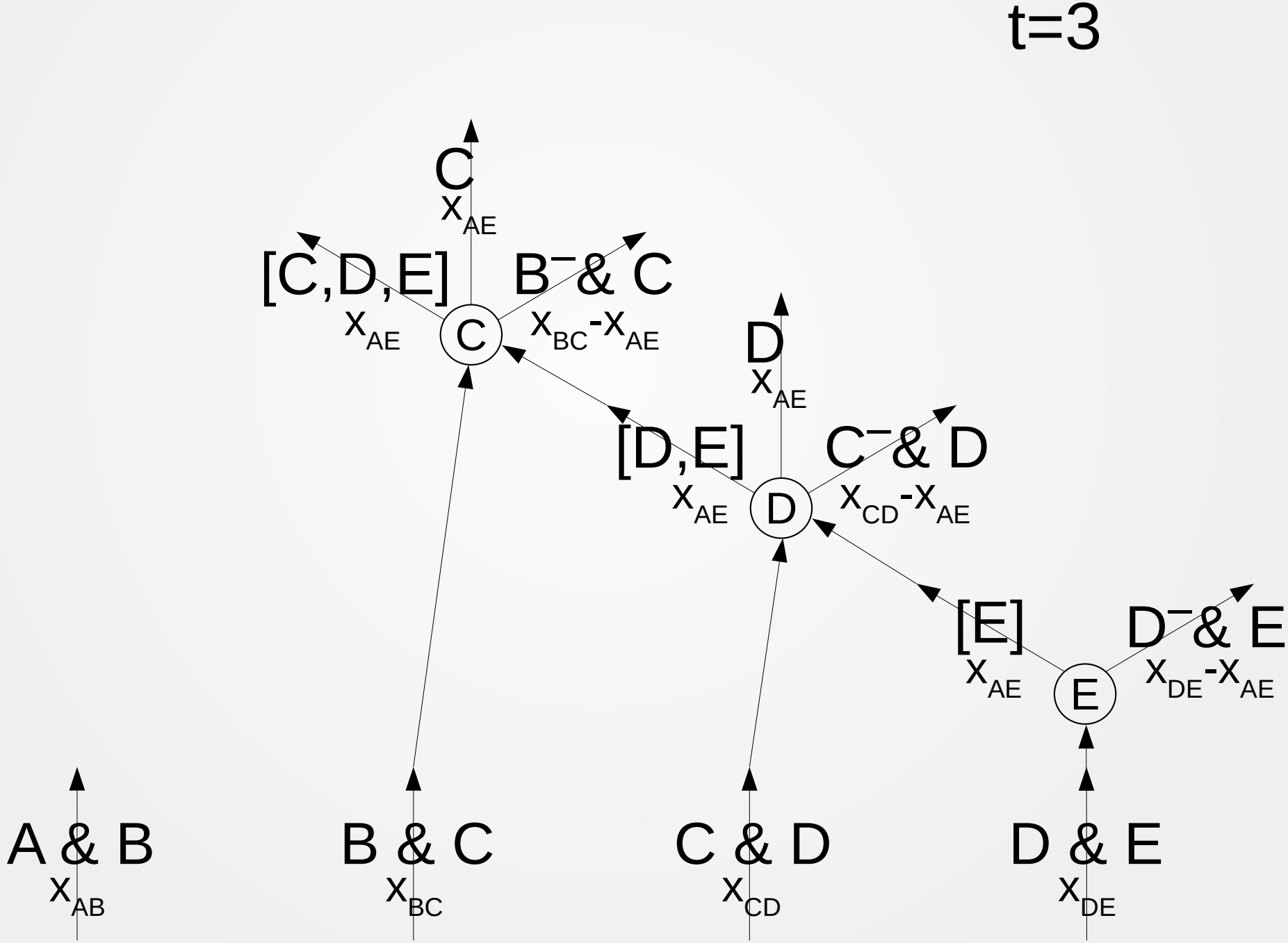


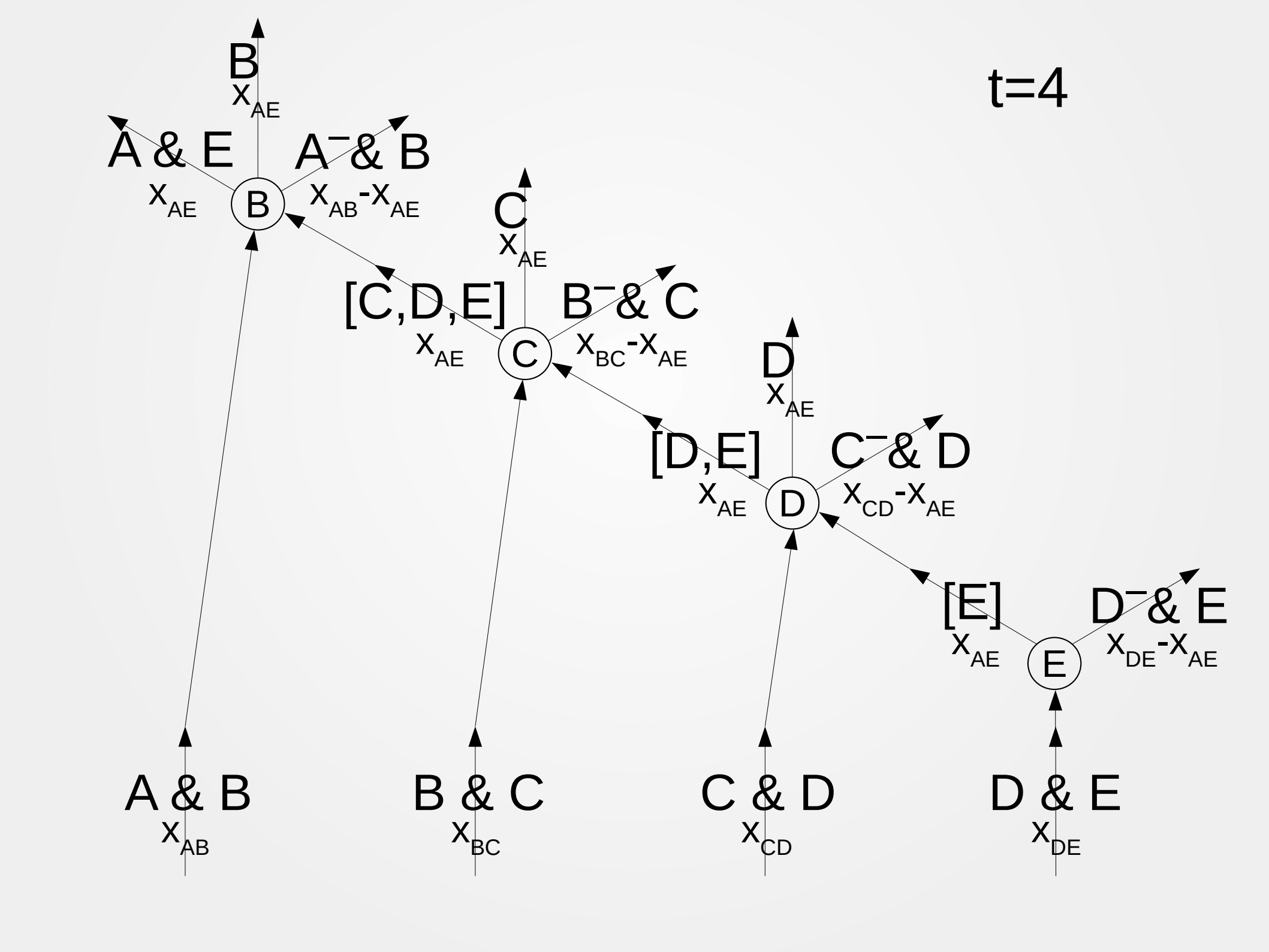
t=1



t=2

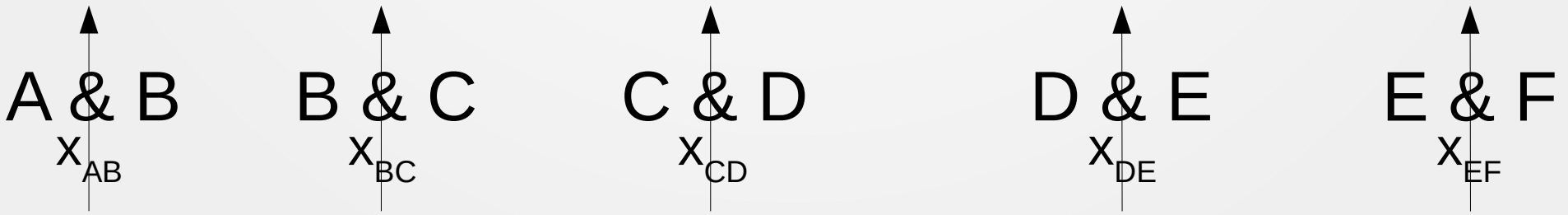

D
$x_{AE}$
[D,E]
$x_{AE}$
D
$C^- \& D$
$x_{CD}$-$x_{AE}$
[E]
$x_{AE}$
E
$D^- \& E$
$x_{DE}$-$x_{AE}$
A & B
$x_{AB}$
B & C
$x_{BC}$
C & D
$x_{CD}$
D & E
$x_{DE}$


t=3
C
x_AE
[C,D,E]
x_AE
C
B⁻ & C
x_BC-x_AE
D
x_AE
[D,E]
x_AE
D
C⁻ & D
x_CD-x_AE
[E]
x_AE
E
D⁻ & E
x_DE-x_AE
A & B
x_AB
B & C
x_BC
C & D
x_CD
D & E
x_DE

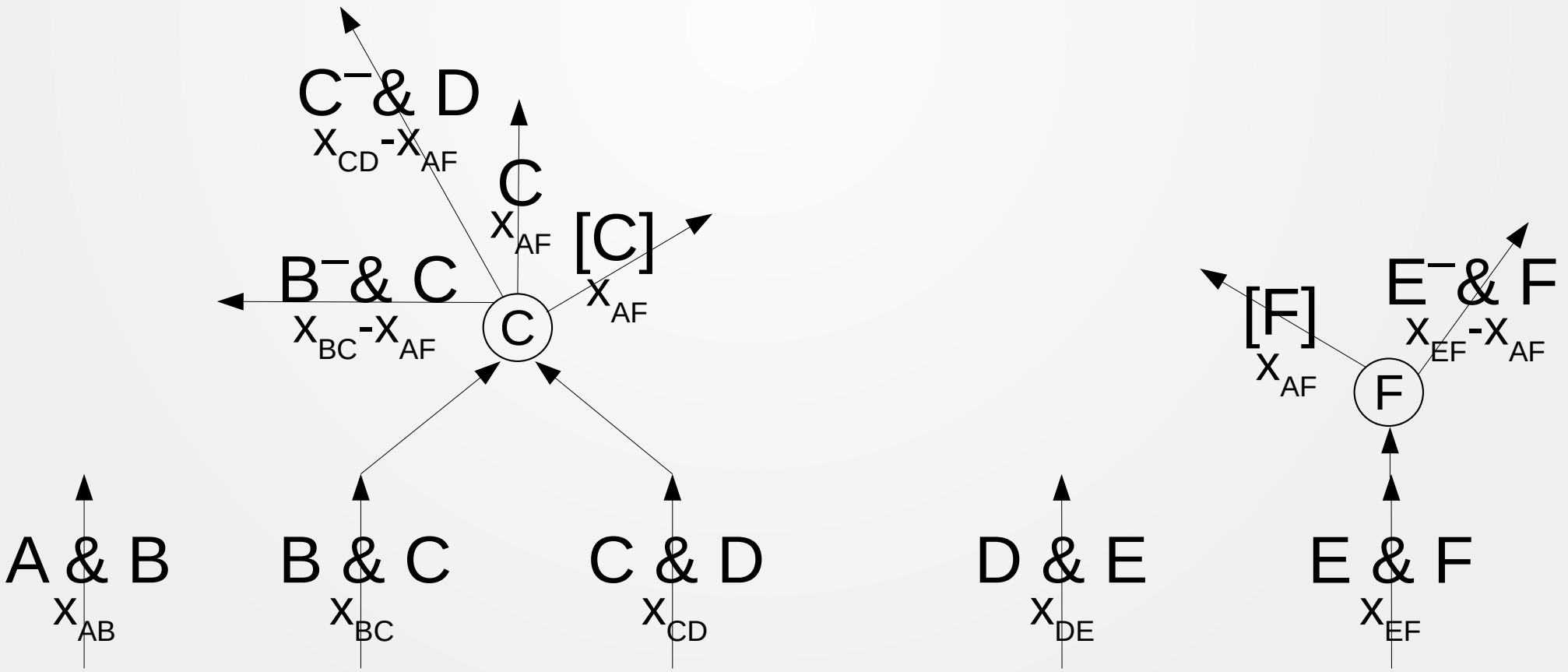

t=4
B
$x_{AE}$
A & E
$x_{AE}$
B
$A^- \& B$
$x_{AB}-x_{AE}$
C
$x_{AE}$
[C,D,E]
$x_{AE}$
C
$B^- \& C$
$x_{BC}-x_{AE}$
D
$x_{AE}$
[D,E]
$x_{AE}$
D
$C^- \& D$
$x_{CD}-x_{AE}$
[E]
$x_{AE}$
E
$D^- \& E$
$x_{DE}-x_{AE}$
A & B
$x_{AB}$
B & C
$x_{BC}$
C & D
$x_{CD}$
D & E
$x_{DE}$

# Example 2
# Simultaneous initiators

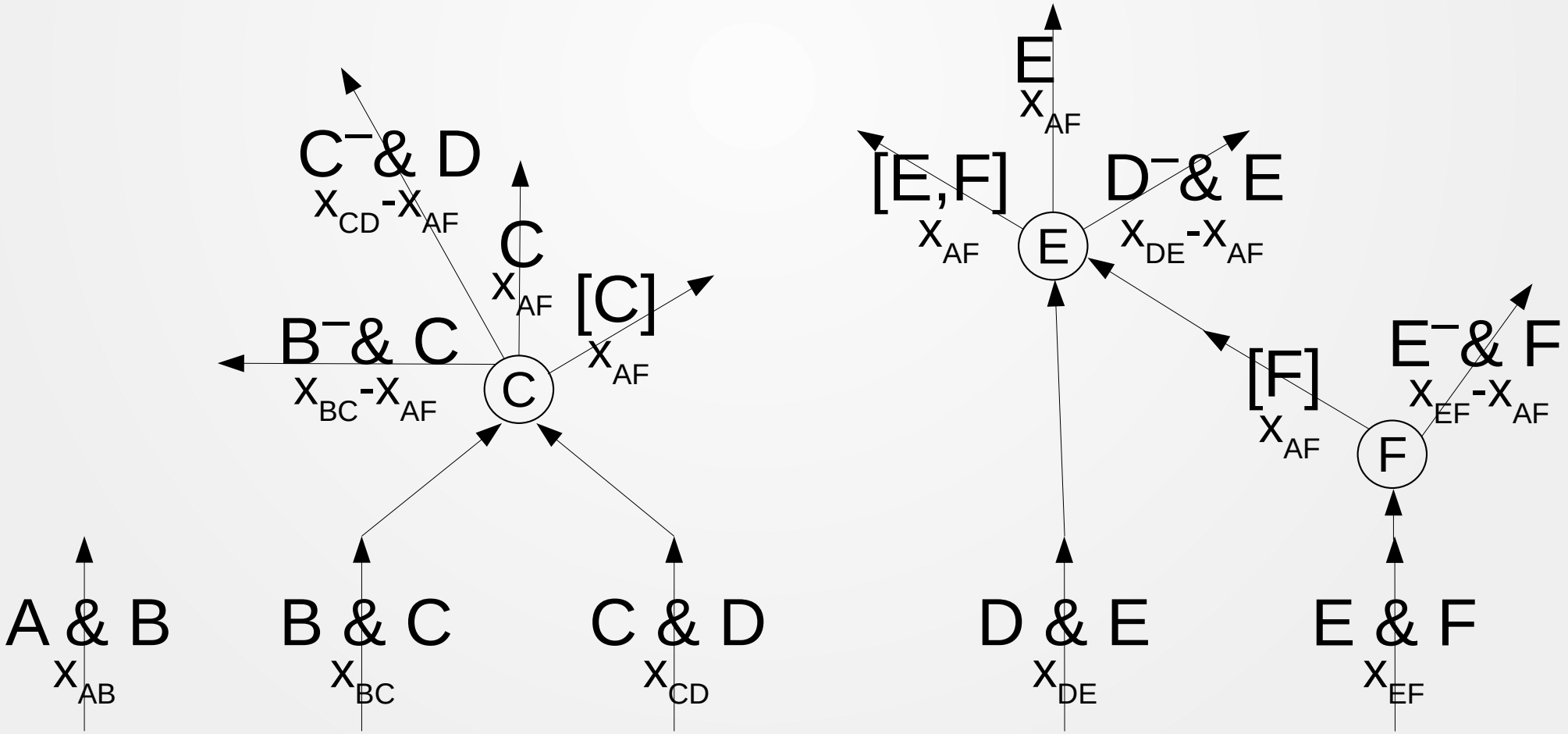
t=0



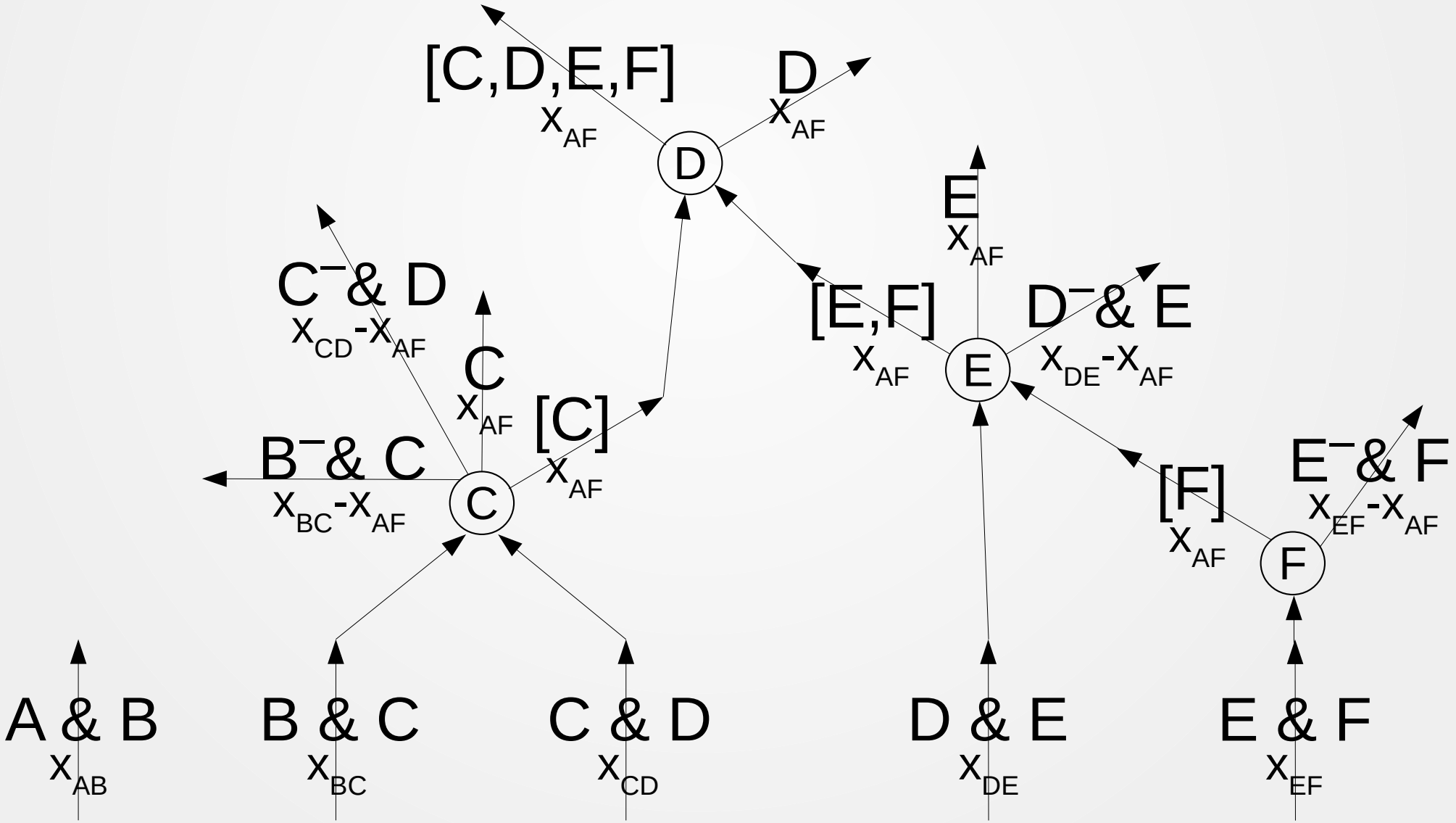
t=1


C⁻ & D
x_CD-x_AF
C
x_AF
[C]
x_AF
B⁻ & C
x_BC-x_AF
C
A & B
x_AB
B & C
x_BC
C & D
x_CD
D & E
x_DE
[F]
x_AF
E⁻ & F
x_EF-x_AF
F
E & F
x_EF

t=2

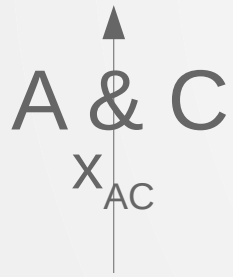

A & B
$x_{AB}$
B & C
$x_{BC}$
C & D
$x_{CD}$
C
$x_{AF}$
$C^{-}$& D
$x_{CD}$-$x_{AF}$
$B^{-}$& C
$x_{BC}$-$x_{AF}$
[C]
$x_{AF}$
C
D & E
$x_{DE}$
E & F
$x_{EF}$
E
$x_{AF}$
[E,F]
$x_{AF}$
$D^{-}$& E
$x_{DE}$-$x_{AF}$
E
[F]
$x_{AF}$
$E^{-}$& F
$x_{EF}$-$x_{AF}$
F

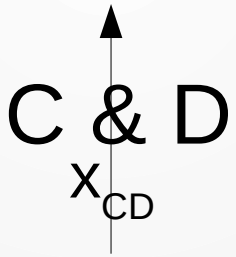
t=3

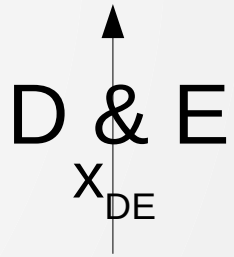

[C,D,E,F]
$x_{AF}$
D
$x_{AF}$
D
E
$x_{AF}$
$C^{-}$& D
$x_{CD}$-$x_{AF}$
C
$x_{AF}$
[C]
$x_{AF}$
[E,F]
$x_{AF}$
E
$D^{-}$& E
$x_{DE}$-$x_{AF}$
$B^{-}$& C
$x_{BC}$-$x_{AF}$
C
[F]
$x_{AF}$
$E^{-}$& F
$x_{EF}$-$x_{AF}$
F
A & B
$x_{AB}$
B & C
$x_{BC}$
C & D
$x_{CD}$
D & E
$x_{DE}$
E & F
$x_{EF}$

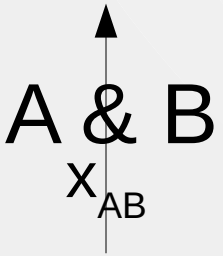
# Example 3
# Virtual base channel

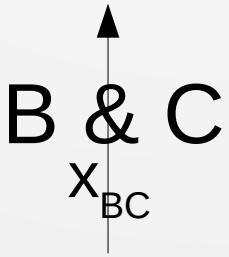
t=0



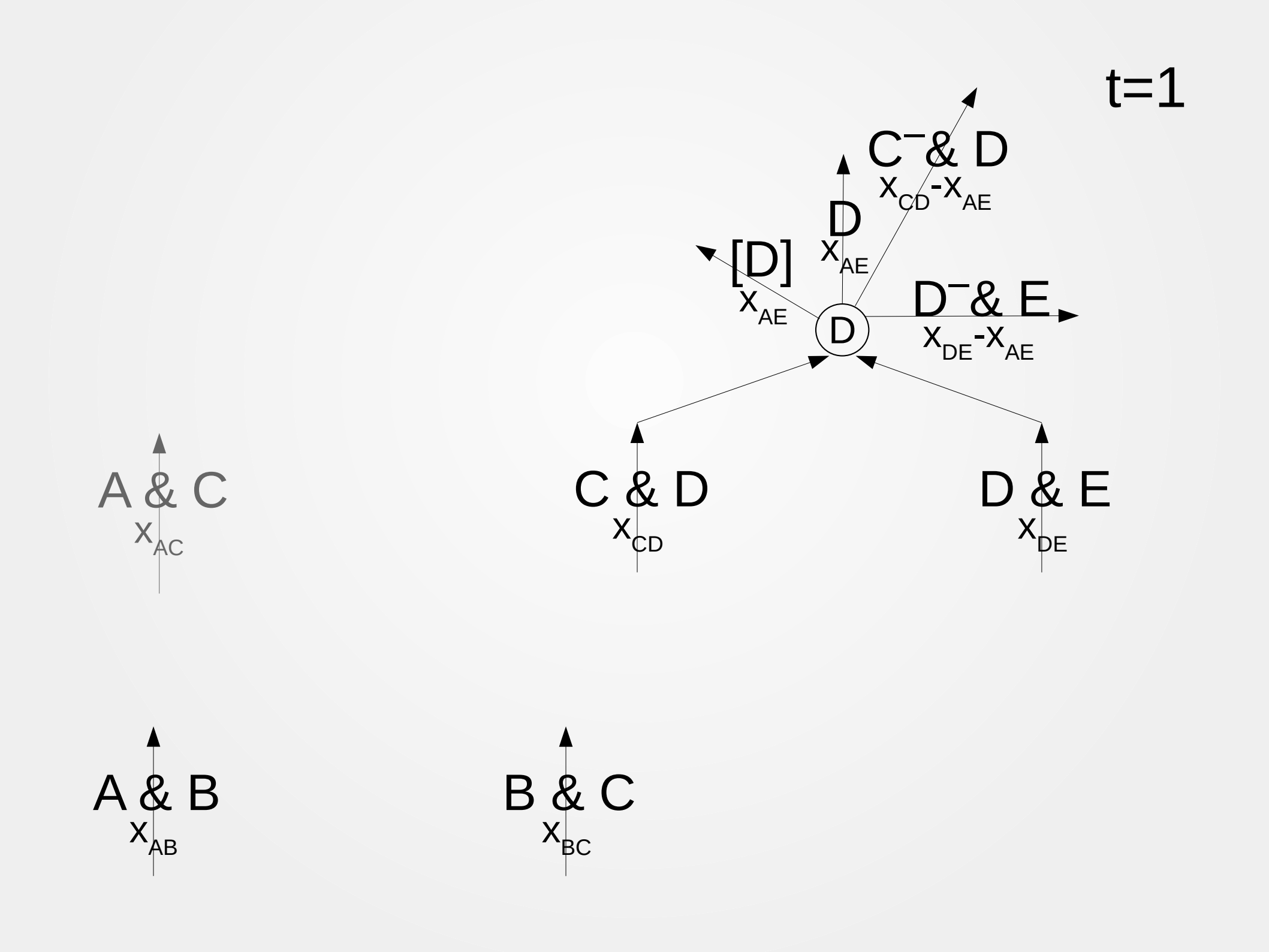



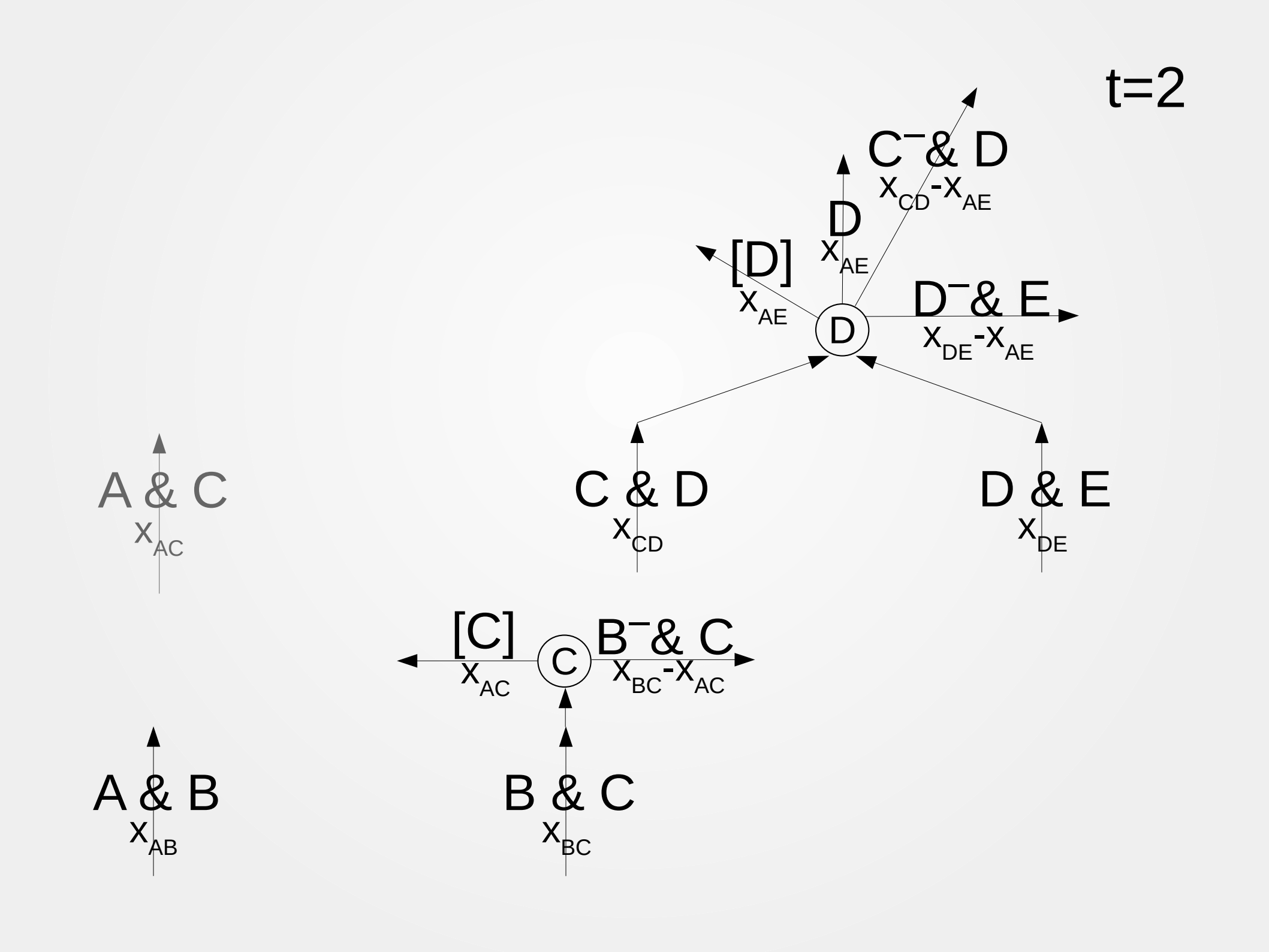



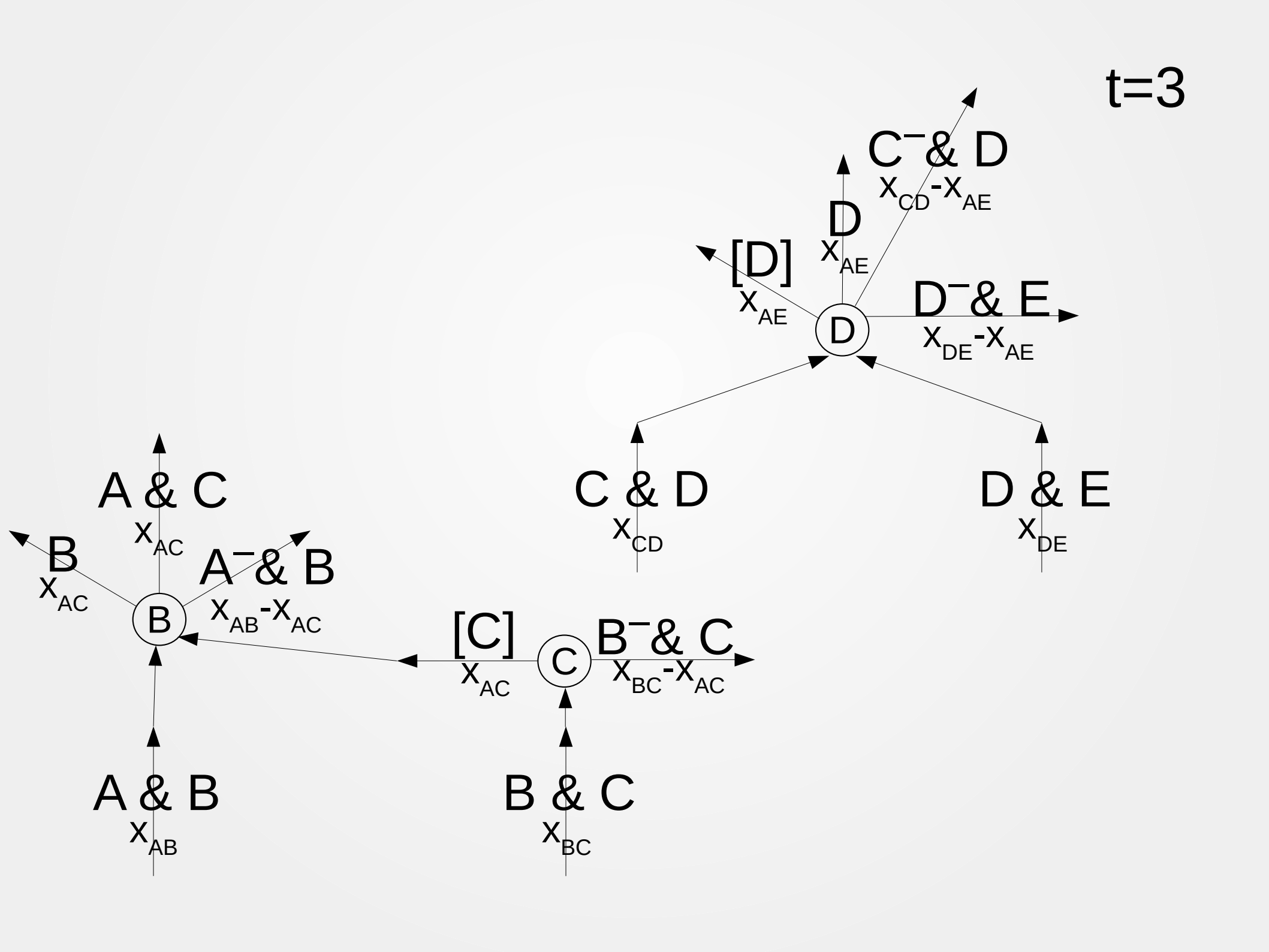



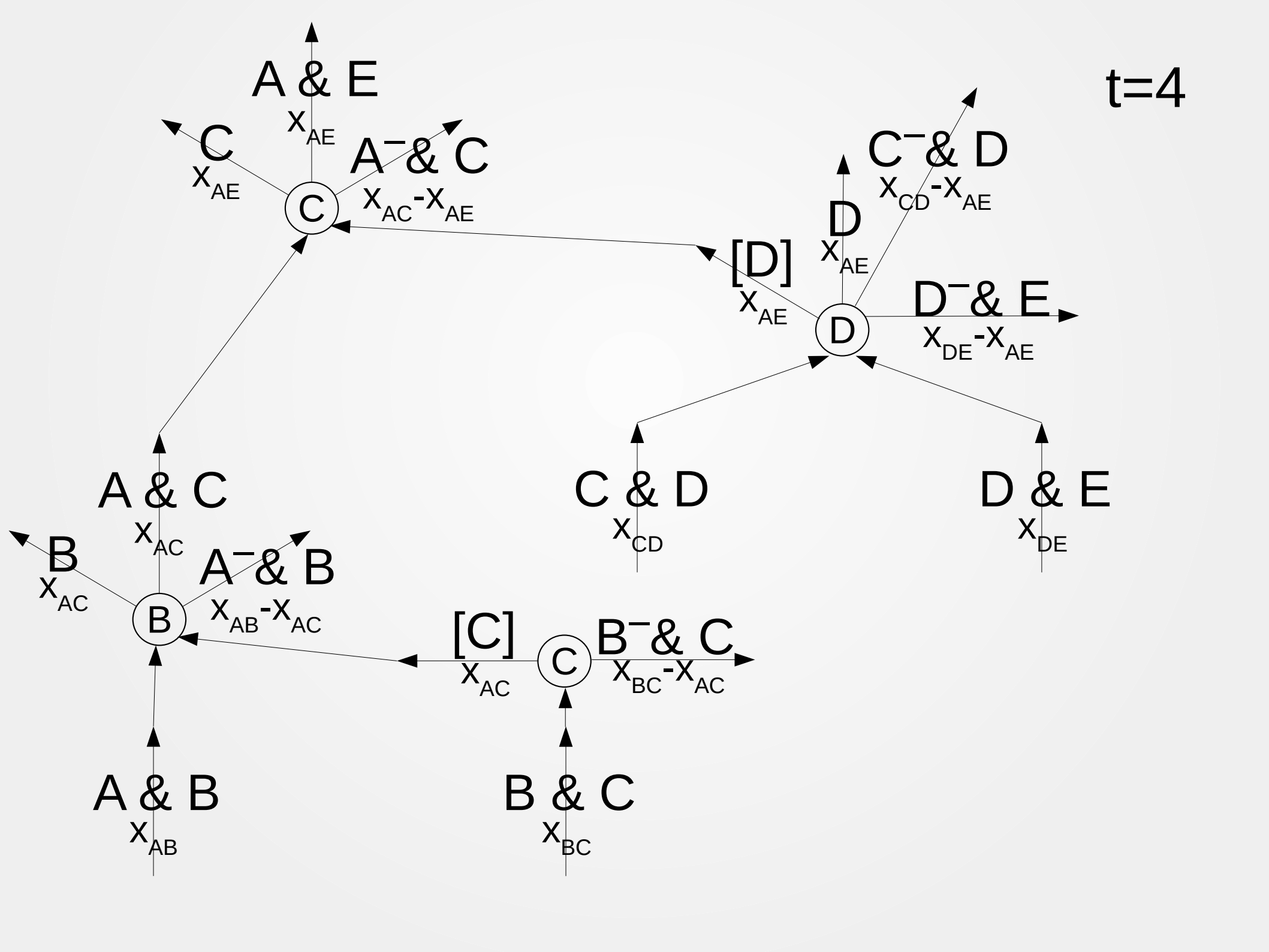
t=1


C⁻ & D
x_CD -x_AE
D
x_AE
[D]
x_AE
D⁻ & E
x_DE -x_AE
D
A & C
x_AC
C & D
x_CD
D & E
x_DE
A & B
x_AB
B & C
x_BC

t=2


C⁻ & D
x_CD - x_AE
D
x_AE
[D]
x_AE
D
D⁻ & E
x_DE - x_AE
A & C
x_AC
C & D
x_CD
D & E
x_DE
[C]
x_AC
C
B⁻ & C
x_BC - x_AC
A & B
x_AB
B & C
x_BC


t=3
C⁻ & D
x_CD - x_AE
D
x_AE
[D]
x_AE
D⁻ & E
x_DE - x_AE
D
C & D
x_CD
D & E
x_DE
A & C
x_AC
B
x_AC
A⁻ & B
x_AB - x_AC
B
[C]
x_AC
C
B⁻ & C
x_BC - x_AC
A & B
x_AB
B & C
x_BC


t=4
A & E
x_AE
C
x_AE
A⁻ & C
x_AC-x_AE
C
[D]
x_AE
C⁻ & D
x_CD-x_AE
D
x_AE
D⁻ & E
x_DE-x_AE
D
A & C
x_AC
C & D
x_CD
D & E
x_DE
B
x_AC
A⁻ & B
x_AB-x_AC
B
[C]
x_AC
B⁻ & C
x_BC-x_AC
C
A & B
x_AB
B & C
x_BC

# Design decisions

- UC secure
- Intuitive functionality
- State machine
- Uses $\mathcal{G}_{\mathrm{ledger}}$

# Summary

Construction and composable analysis of Variadic Recursive Virtual Channels for Bitcoin

*Thank you!*