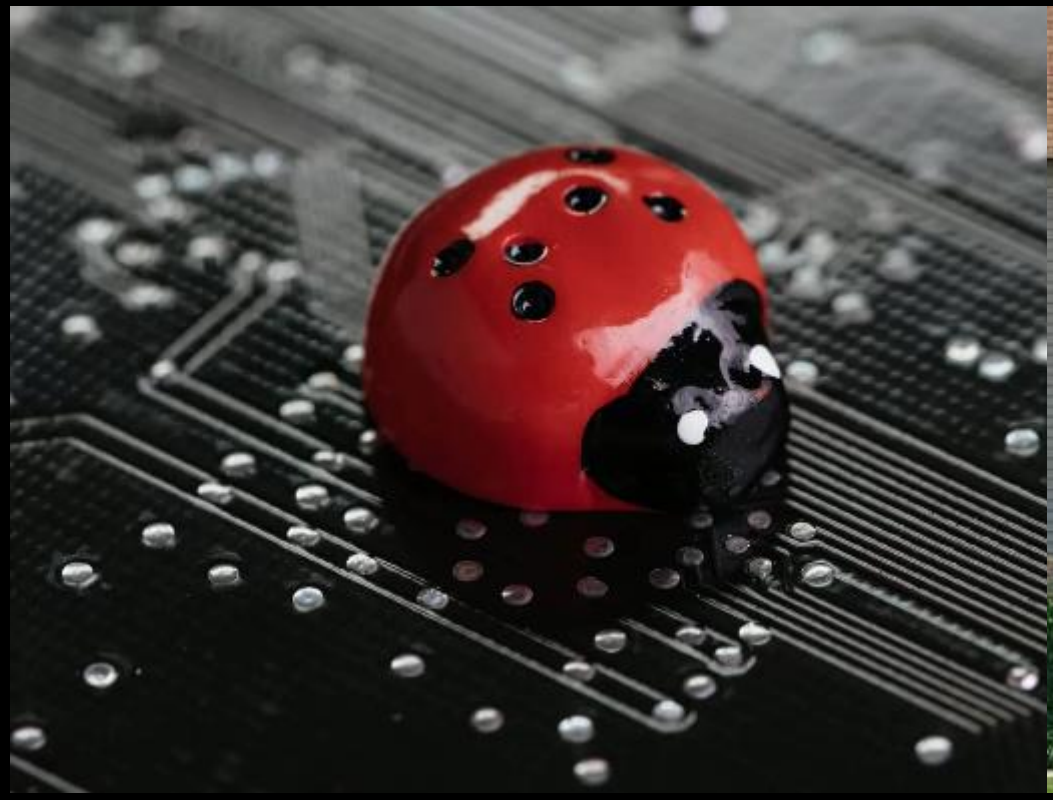
Lecture 2: Fault Tree Analysis



Milan Lopuhaä-Zwakenberg

Formal Methods & Tools

Today's Agenda

Videos

1. Why models
2. What are fault trees?
3. Qualitative analysis via cut sets
4. Visualization

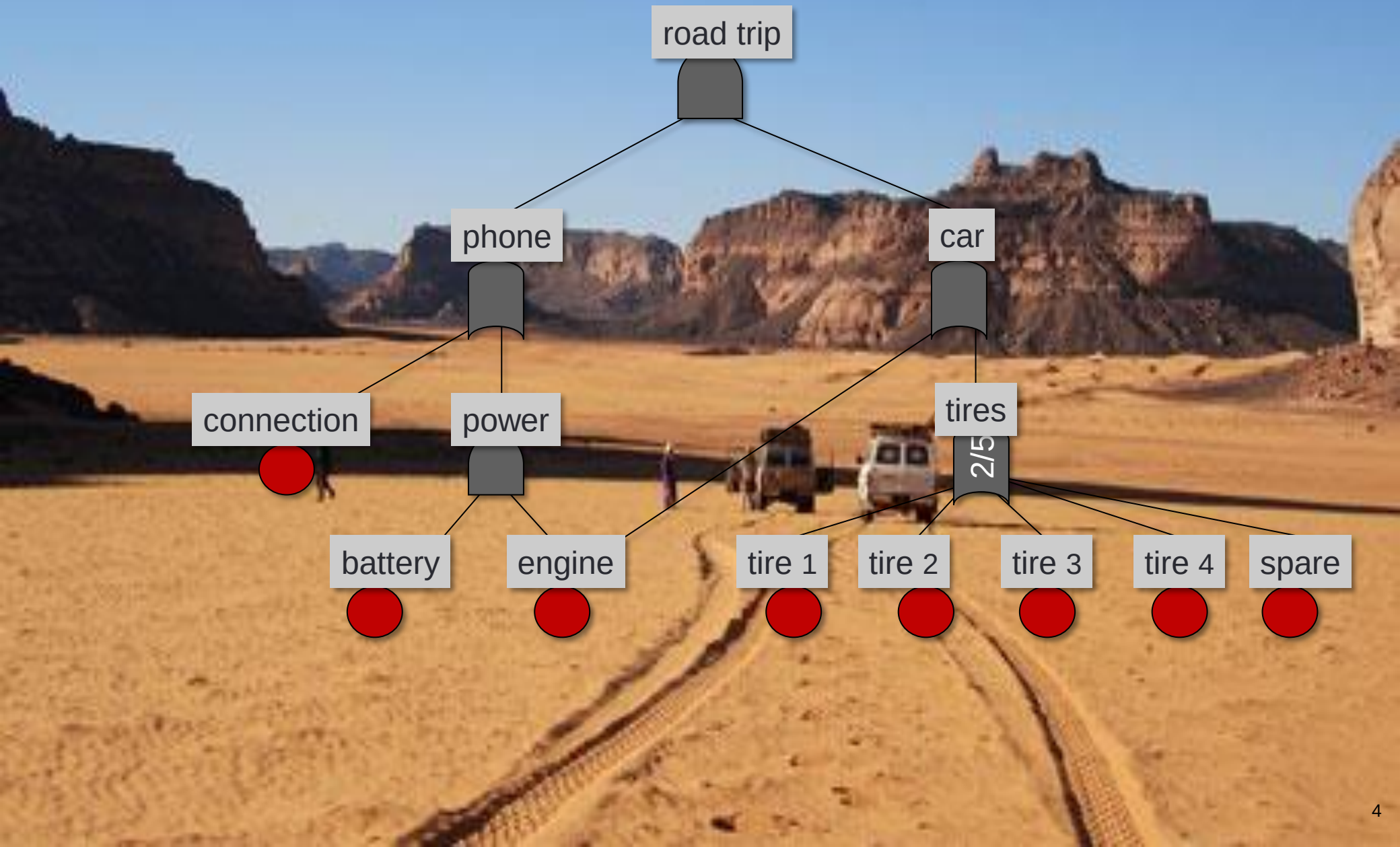
Now

1. Quantitative analysis
   a. Discrete probability
   b. Continuous probability
2. Remarks
3. Conclusions

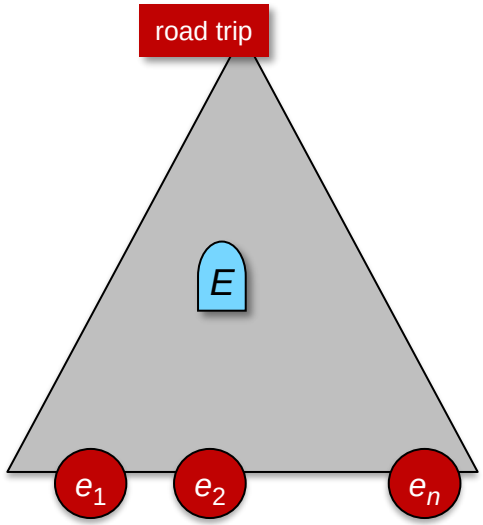
Planning

Week	date	Tuesday	Lecturer	Thursday	TA
1	Feb 7			Lecture: intro	MLZ
2	Feb 14	Fault trees	MLZ	Exercises	Matthias Volk
3	Feb 21	Dynamic FTs, FMEA	MLZ	Exercises	LJR
	Feb 28	**BREAK**			
4	Mar 7	Classical testing	MLZ	Exercises	LJR,TZ
5	Mar 14	State machines	MLZ	Exercises	TZ
6	Mar 21	Model-based testing	Petra van den Bos	Exercises	TZ
7	Mar 28	Student presentations	You guys	Exercises	TZ
8	Apr 4	Guest lecture: mutation testing	Infosupport	Exam practice	LJR, TZ

Example: Safe road trip



The fault trees: structure function



Structure function Φ_F: $\{0,1\}^{\#BEs} \rightarrow \{0,1\}$

- **1** = fail; **0** = operational
- Given values $e_1,\ldots,e_n$, $\Phi_F(e_1,\ldots,e_n)$ tells whether F fails

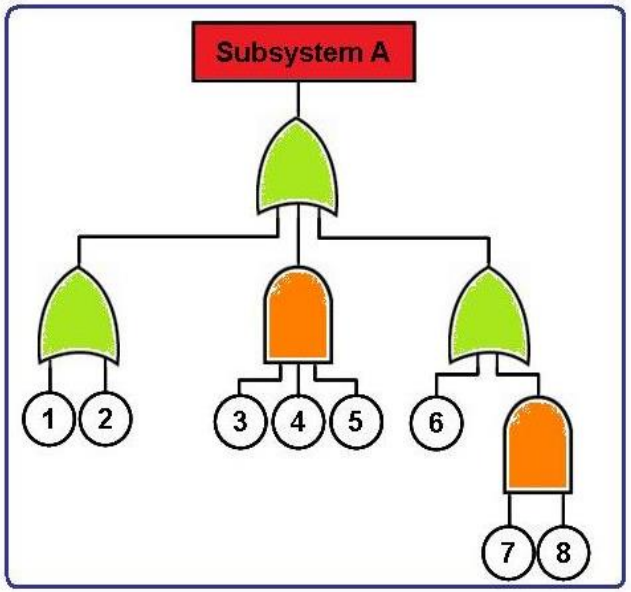
Extension: Φ_F: $\{0,1\}^{\#BEs}$ x Elt $\rightarrow \{0,1\}$

- Given values $e_1,,\ldots,e_n$, $\Phi_F(e_1,\ldots,e_n,E)$ tells whether element E fails

Recursive definition

- If E is an AND-gate: $\Phi_F(e,E) = 1$ iff $\Phi_F(e,E') = 1$ for all children E' of E
- If E is an OR-gate: $\Phi_F(e,E) = 1$ iff $\Phi_F(e,E') = 1$ for some child E' of E
- …etc...

Fault trees: what are they?



Graphical Model

- Tell how systems fail
- How do component failures lead to system failures?

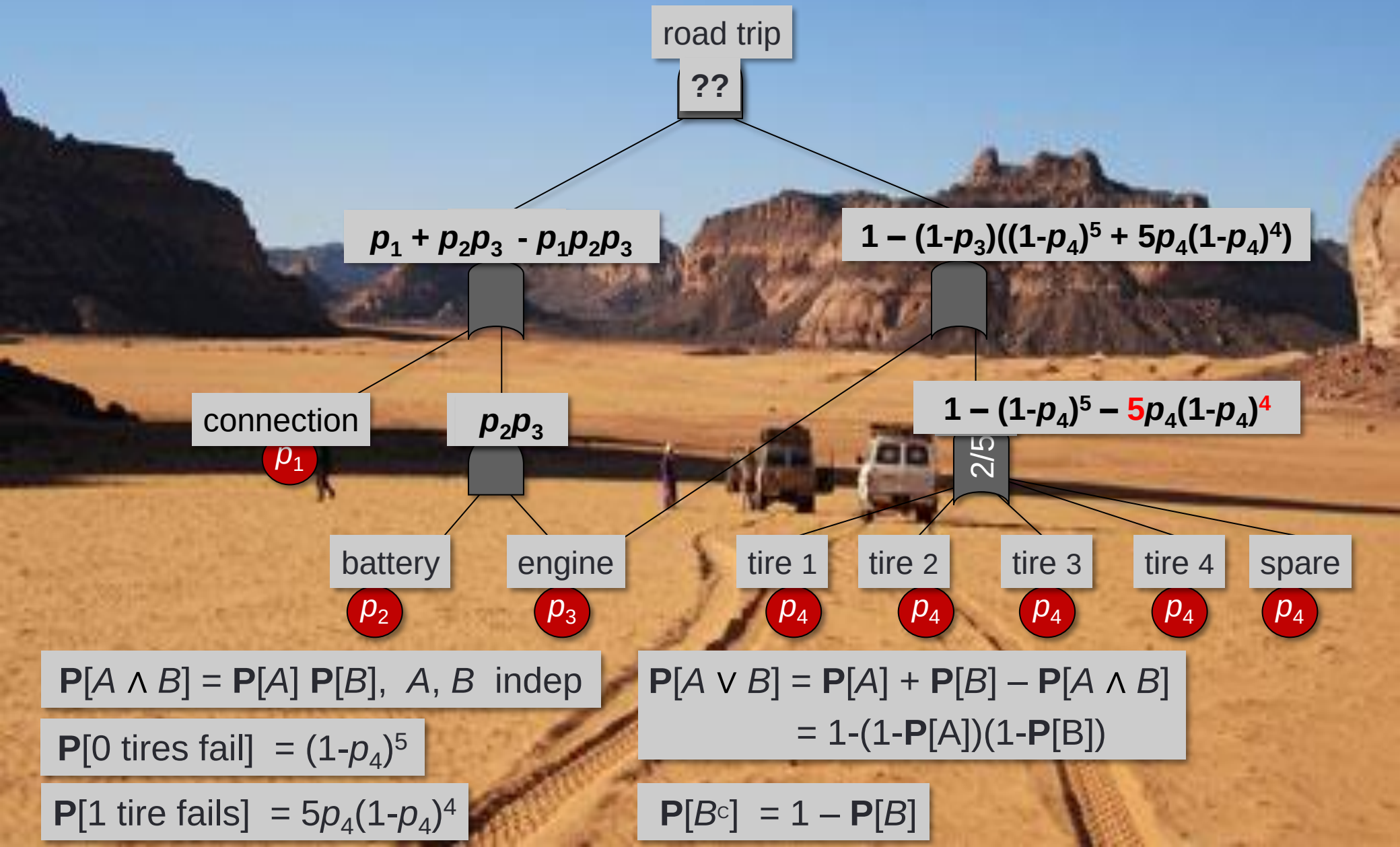
Qualitative Analysis

- Pinpoint to root causes & critical parts

Quantitative Analysis: metrics / KPIs

- Reliability: **P**[no failure during mission time]
- Availability: **E**[up-time]
- MTTF: mean time to failure
- MTBF: mean time between failures

Question: determine unreliability / failure probability



$\mathbf{P}[A \wedge B] = \mathbf{P}[A]\,\mathbf{P}[B]$, A, B indep

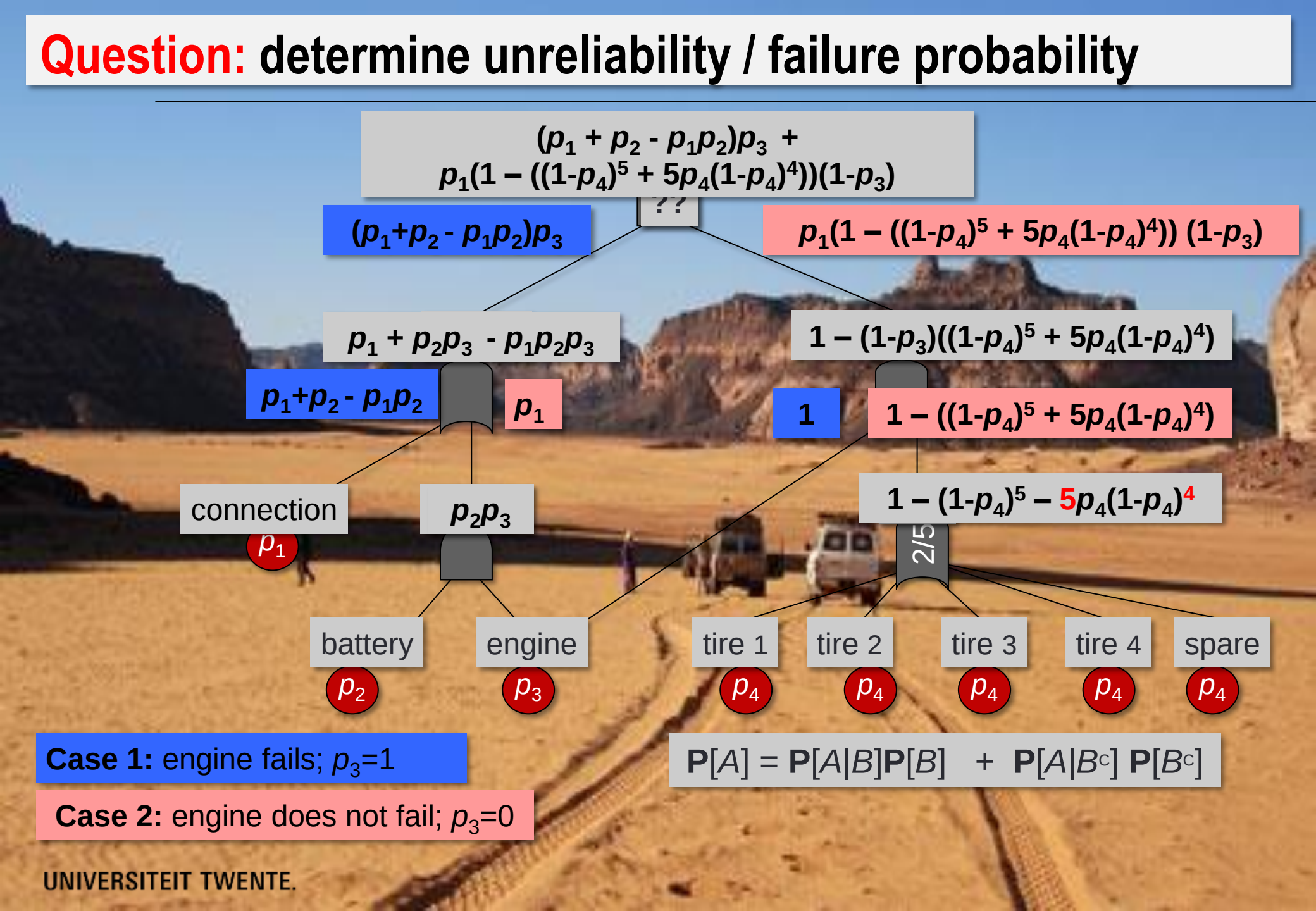
$\mathbf{P}[A \vee B] = \mathbf{P}[A] + \mathbf{P}[B] - \mathbf{P}[A \wedge B]$
$= 1-(1-\mathbf{P}[A])(1-\mathbf{P}[B])$

$\mathbf{P}[\text{0 tires fail}] = (1-p_4)^5$

$\mathbf{P}[\text{1 tire fails}] = 5p_4(1-p_4)^4$

$\mathbf{P}[B^c] = 1 - \mathbf{P}[B]$

Question: determine unreliability / failure probability



Case 1: engine fails; p_3=1

Case 2: engine does not fail; p_3=0

$$\mathbf{P}[A] = \mathbf{P}[A|B]\mathbf{P}[B] + \mathbf{P}[A|B^c]\,\mathbf{P}[B^c]$$

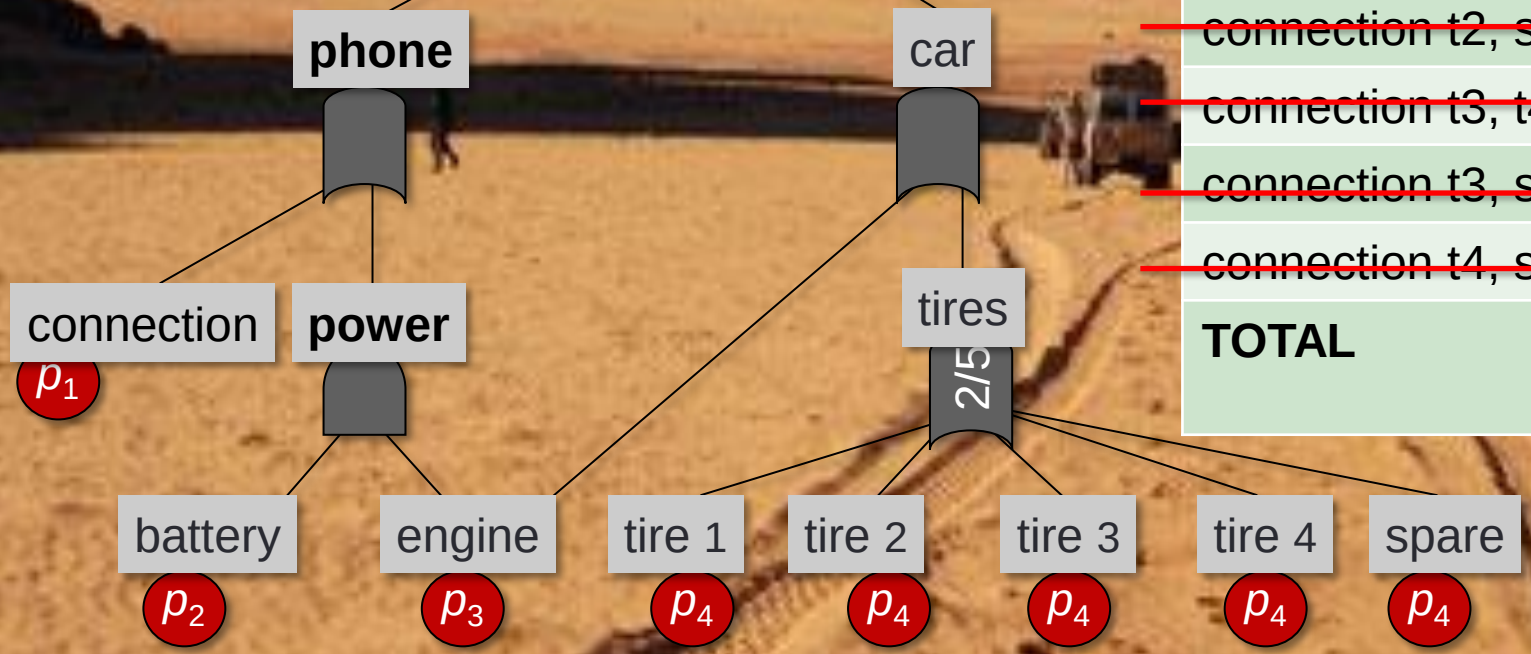
Simplify the computation

Find 3 ways to speed up this computation

1. Use minimal cut sets
2. Disregard extremely small probabilities
3. Use BDDs

Speed up: Using cut sets

$$(p_1 + p_2 - p_1p_2)p_3 + p_1(1 - ((1-p_4)^5 + 5p_4(1-p_4)^4)(1-p_3)$$



Min cut set	prob
connection, engine	$p_1 * p_3$
battery, engine	$p_2 * p_3$
~~connection, t1, t2~~	~~$p_1 * p_4^2$~~
~~connection, t1, t3~~	~~$p_1 * p_4^2$~~
~~connection t1, t4~~	~~$p_1 * p_4^2$~~
~~connection t1, spare~~	~~$p_1 * p_4^2$~~
~~connection t2, t3~~	~~$p_1 * p_4^2$~~
~~connection t2, t4~~	~~$p_1 * p_4^2$~~
~~connection t2, spare~~	~~$p_1 * p_4^2$~~
~~connection t3, t4~~	~~$p_1 * p_4^2$~~
~~connection t3, spare~~	~~$p_1 * p_4^2$~~
~~connection t4, spare~~	~~$p_1 * p_4^2$~~
TOTAL	$p_1*p_3 + p_2*p_3$ ~~$+ 10* p_1 * p_4^2$~~

Note: p_1 , p_4 should be low

Speed up 4: Using BDDs

Binary Decision Diagrams (BDDs)

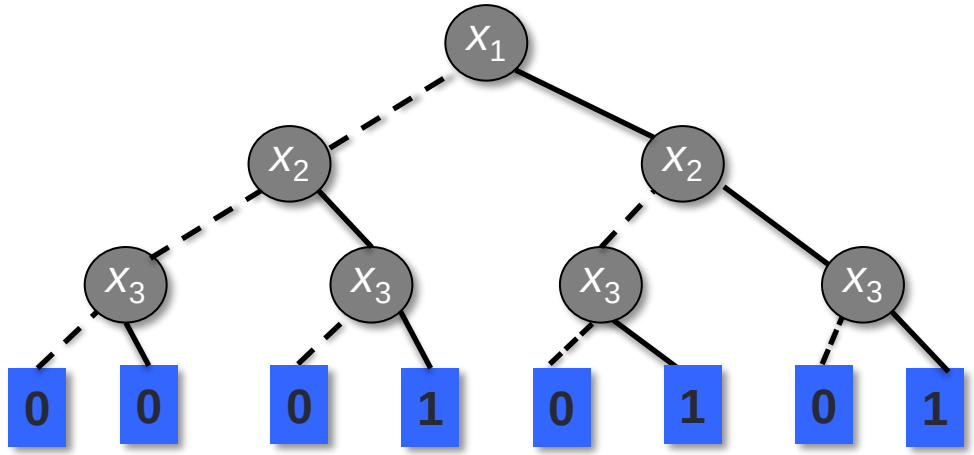
- Compact representation for Boolean functions $f(x_1,x_2,\ldots,x_n)$
  - e.g. the structure function of a FT
- Heavily used in model checking
  - state space
- Based on Shannon expansion / pivotal decomposition
  - $f(x_1,x_2,\ldots,x_n) = \underline{x_1} f(0,x_2,\ldots,x_n) + x_1 f(1,x_2,\ldots,x_n)$

Example: $(x_1 \vee x_2) \wedge x_3$

Truth Table

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

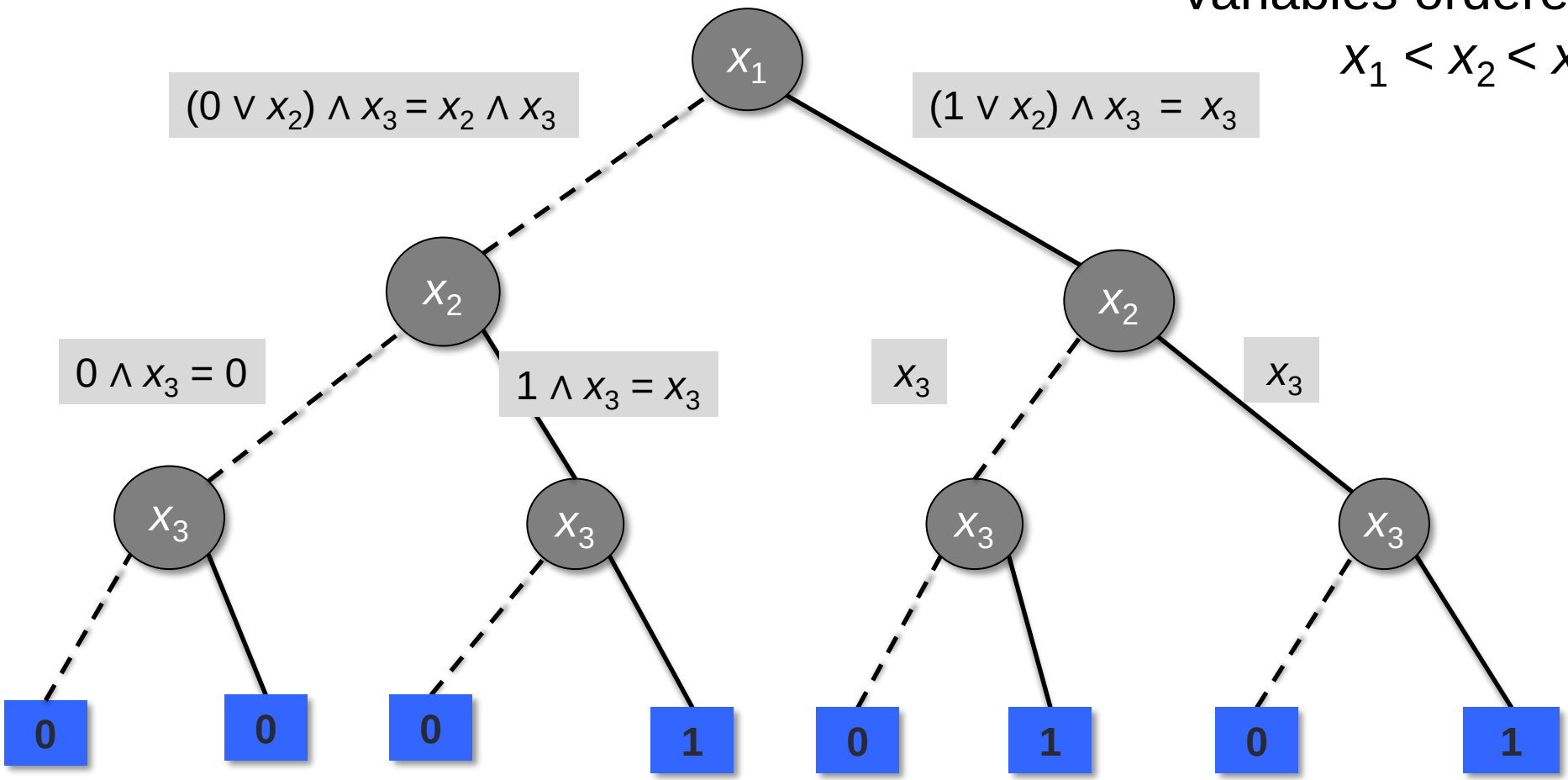
Decision Tree



- Vertex represents decision
- Follow dashed line for value 0
- Follow solid line for value 1
- Function value in leaf

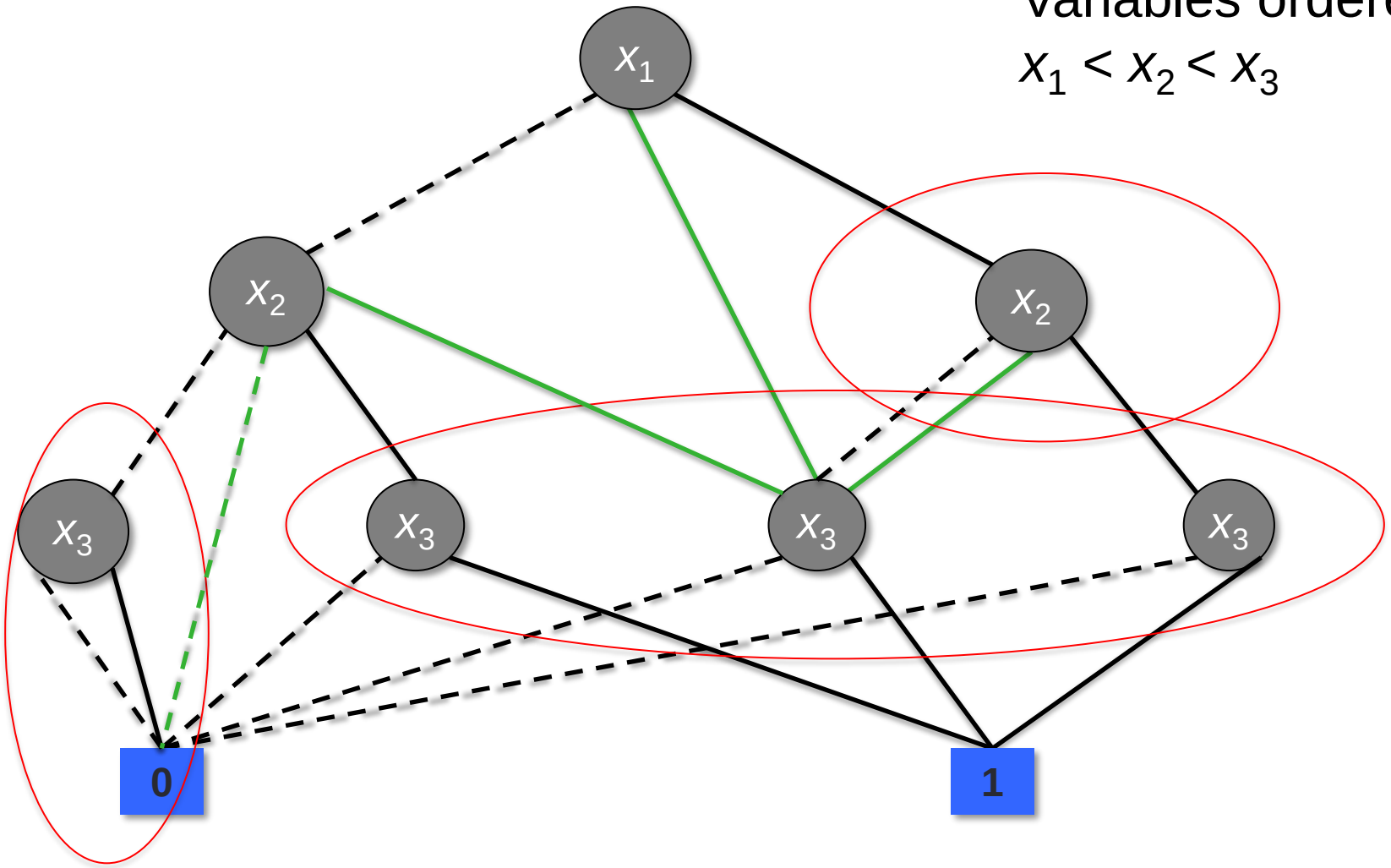
Deriving the BDD: $(x_1 \vee x_2) \wedge x_3$

Variables ordered
$x_1 < x_2 < x_3$

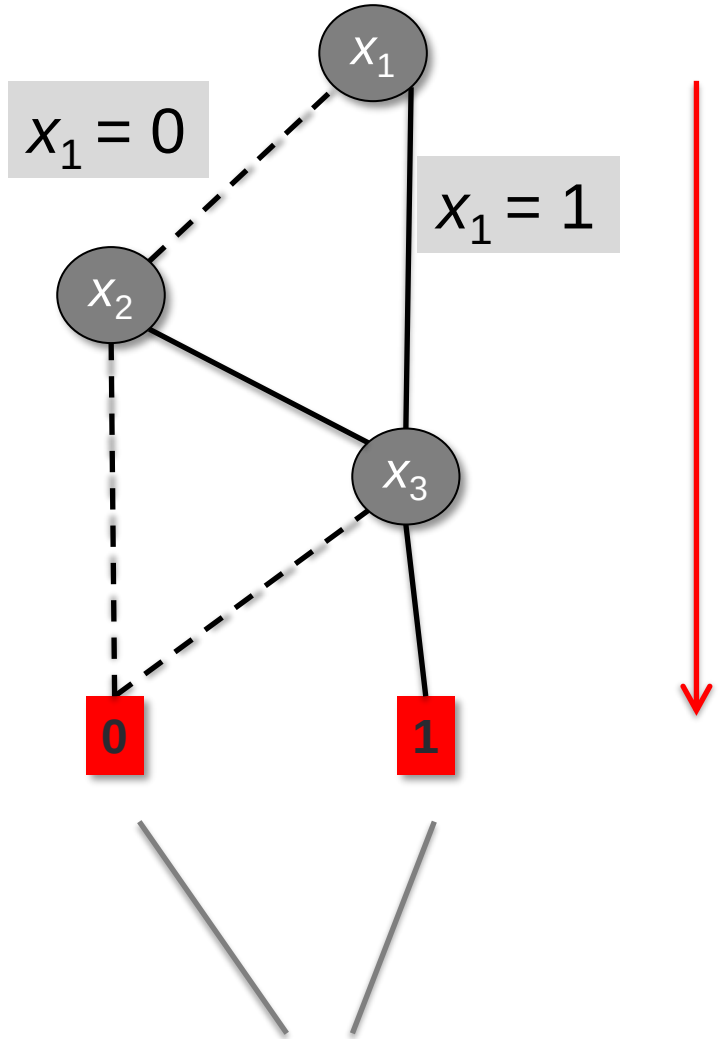


Reducing the BDD: $(x_1 \vee x_2) \wedge x_3$

Variables ordered
$x_1 < x_2 < x_3$



Example: $(x_1 \vee x_2) \wedge x_3$

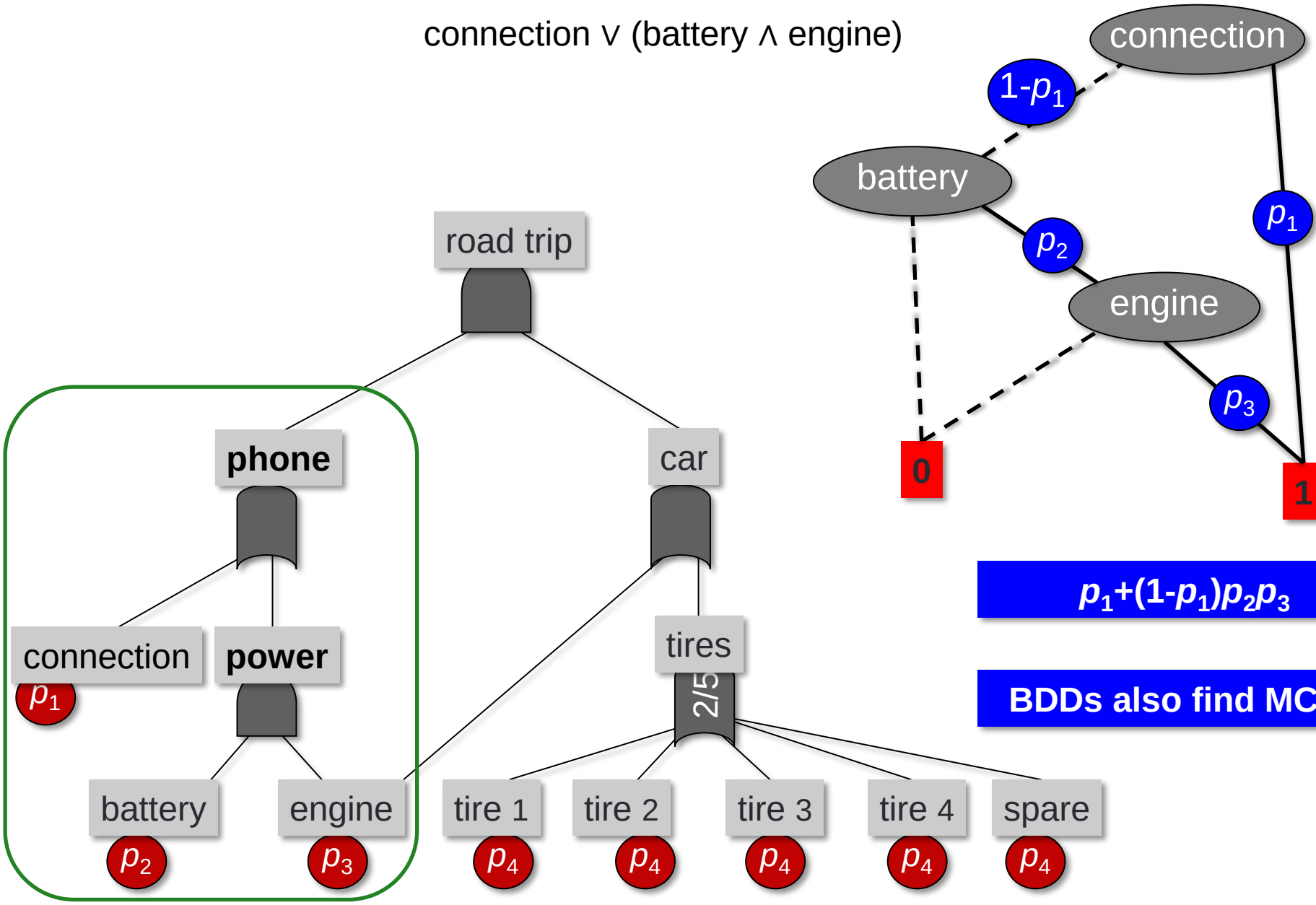


Variables ordered
$x_1 < x_2 < \ldots < x_n$

- Size of BDDs heavily depends on variable order $x_1 < x_2 < \ldots < x_n$
- Finding best order is NP-hard
- Good algos in practice

Using BDDs

connection ∨ (battery ∧ engine)



$p_1+(1-p_1)p_2p_3$

BDDs also find MCSs

Today's Agenda

Videos

1. Why models
2. What are fault trees?
3. Qualitative analysis via cut sets
4. Visualization

Now

1. Quantitative analysis
   a. Discrete probability
   b. Continuous probability
2. Remarks
3. Conclusions

System (un)reliability

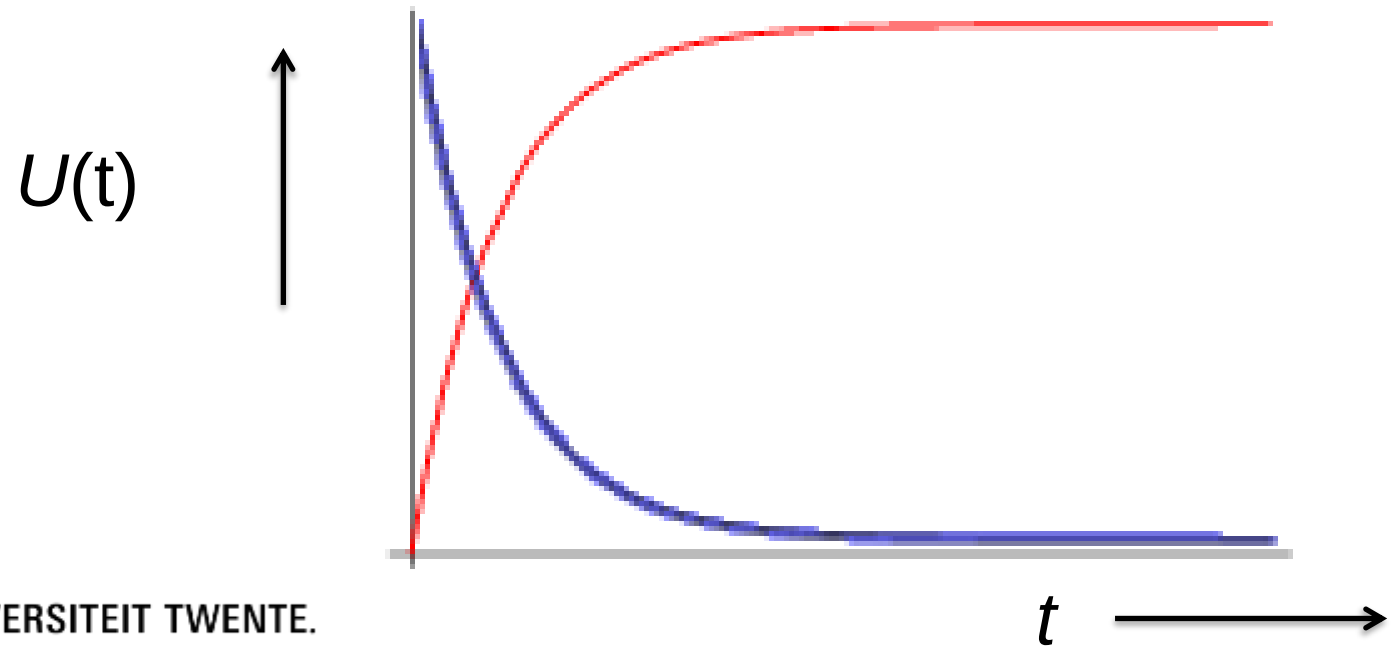
- Unreliability

  $U(t)$ = **P**[failure before time t]

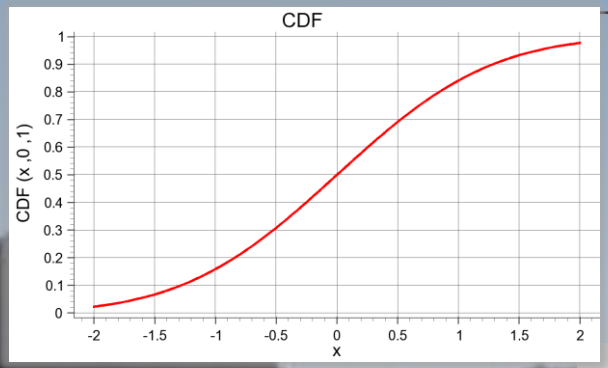
- Reliability / Survivor function

  $R(t)$ = **P**[no failure until time t]

  = 1- $U(t)$

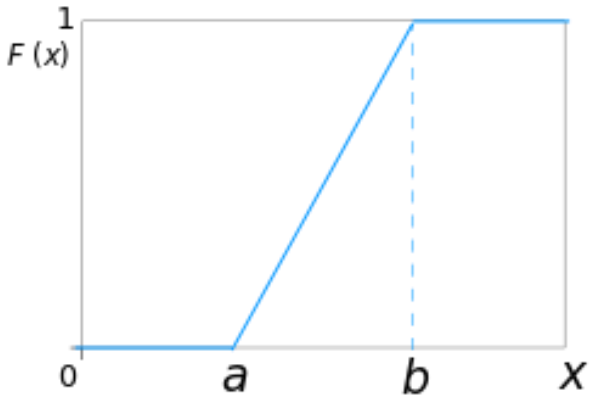


Continuous probability: failure behaviour over time

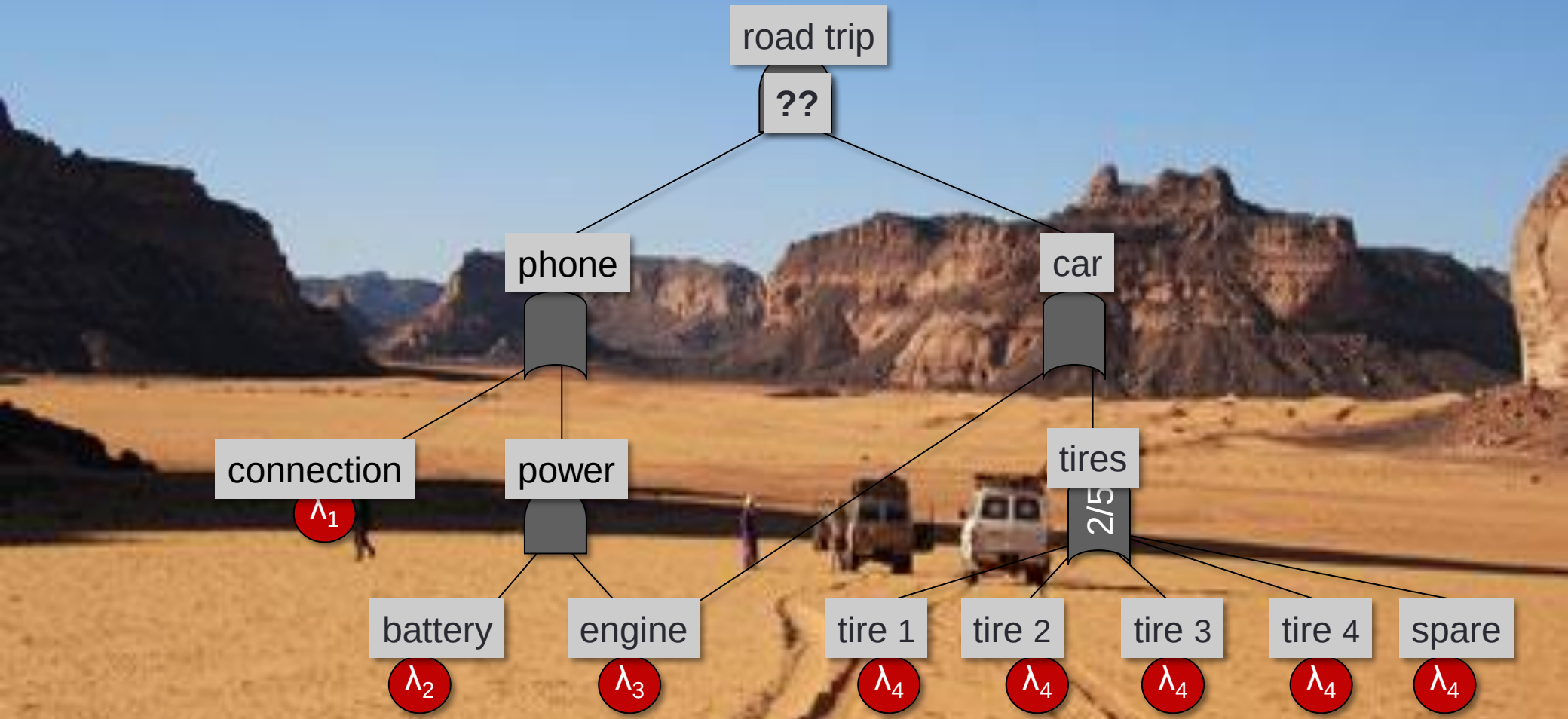


Continuous probability distributions: which one?

- **Uniform distribution**
- **Gaussian**
- **Exponential**
  - realistic model for degradation
  - mathematically tractable
  - approximation via composed exponentials
- **Weibull**
  - generalized exponential
  - often used
  - not discussed
- Use the cumulative density function:
  - $F(x) = \mathbf{P}[X \leq x]$

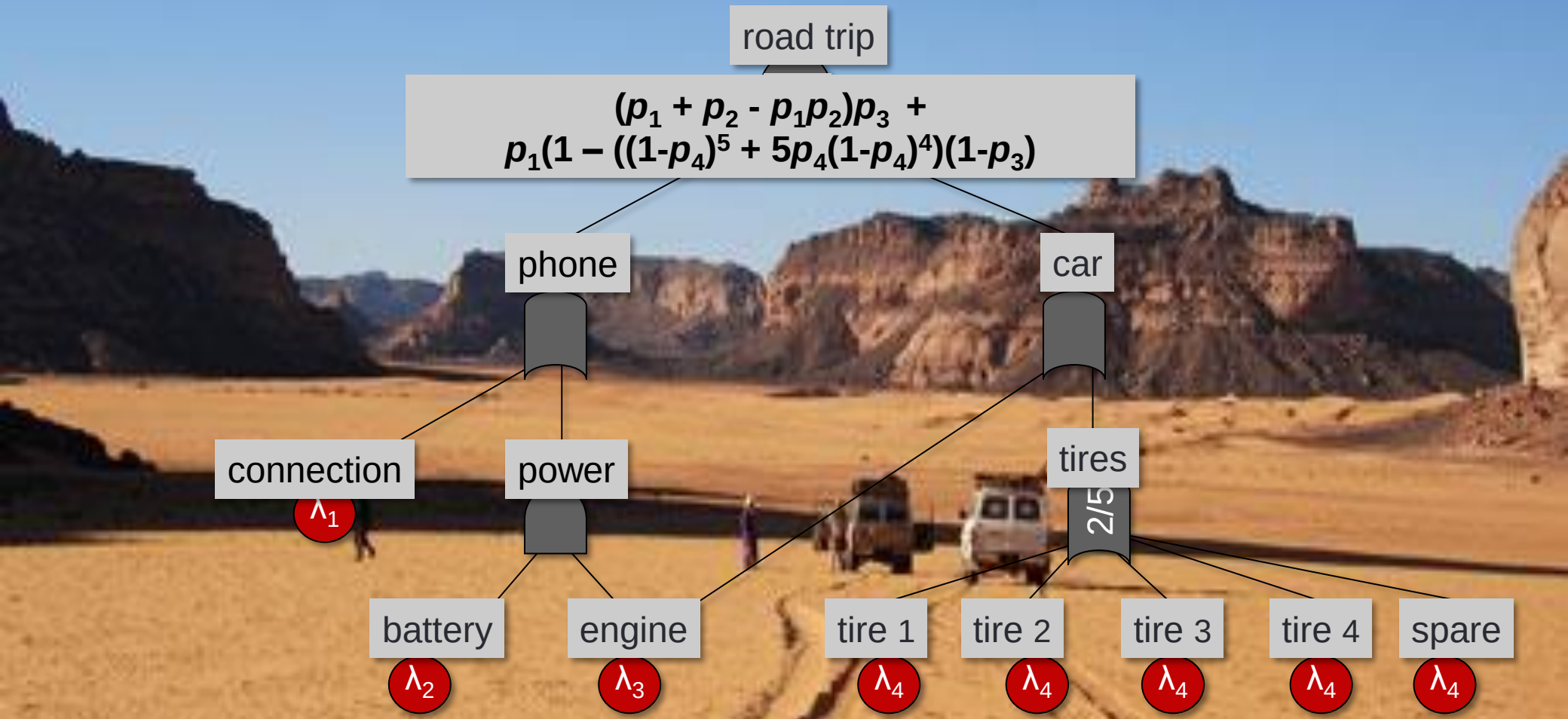


Example: probabilistic analysis



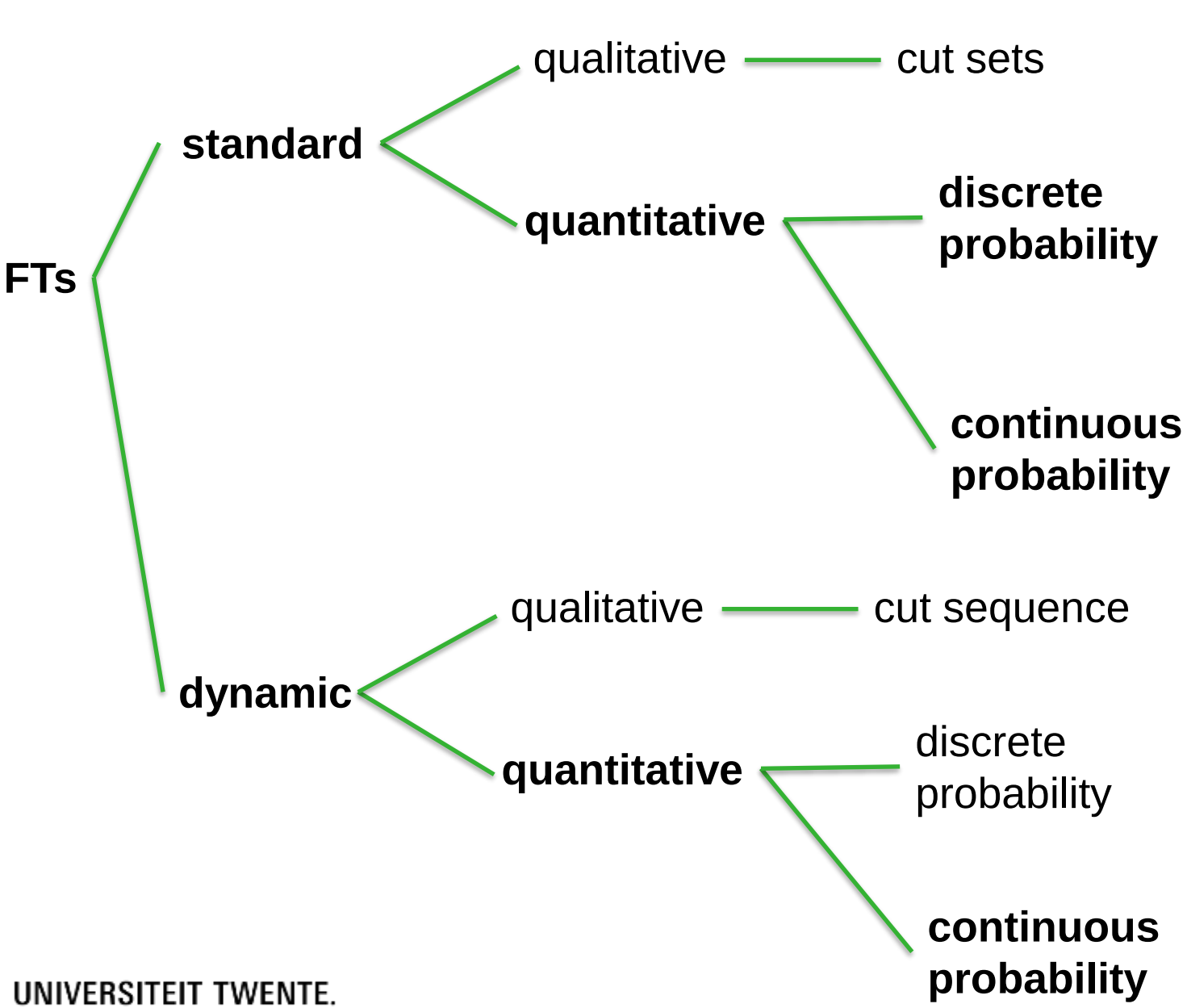
$p_i(t)$ = **P**[BE *i* fails before time *t*] = 1- $e^{-\lambda i * t}$

Example: probabilistic analysis



- $p_1(t)$ varies over time
- $p_1(t)$ probability of having failed at time t
- Substitute $p_1(t) = 1 - e^{-\lambda 1 t}$
- … works the same for other probability distributions

Overview



Technique
- Recursive
- BDDs

Technique
- Bottom up
- Cut sets
- BDDs

Technique
- The same!

Technique
- Model checking
- Next time

This week's assignment

- Multiple choice questions
  - See quizzes on Canvas
  - optional
- Homework
  - See Canvas
  - Due next Tuesday 13:00, in pairs
- Project homework
  - See Canvas
  - Due next Tuesday 13:00, in project groups
- On Canvas: background literature
  - Optional

Planning

Week	date	Tuesday	Lecturer	Thursday	TA
1	Feb 7			Lecture: intro	MLZ
2	Feb 14	Fault trees	MLZ	Exercises	Matthias Volk
3	Feb 21	Dynamic FTs, FMEA	MLZ	Exercises	LJR
	Feb 28	**BREAK**			
4	Mar 7	Classical testing	MLZ	Exercises	LJR,TZ
5	Mar 14	State machines	MLZ	Exercises	TZ
6	Mar 21	Model-based testing	Petra van den Bos	Exercises	TZ
7	Mar 28	Student presentations	You guys	Exercises	TZ
8	Apr 4	Guest lecture: mutation testing	Infosupport	Exam practice	LJR, TZ