UNIVERSITÄT KOBLENZ · LANDAU

Statistische Parametersynthese für hybride Systeme

Christian Schwarz
chrschwarz@uni-koblenz.de

Workshop
Echtzeit 2013

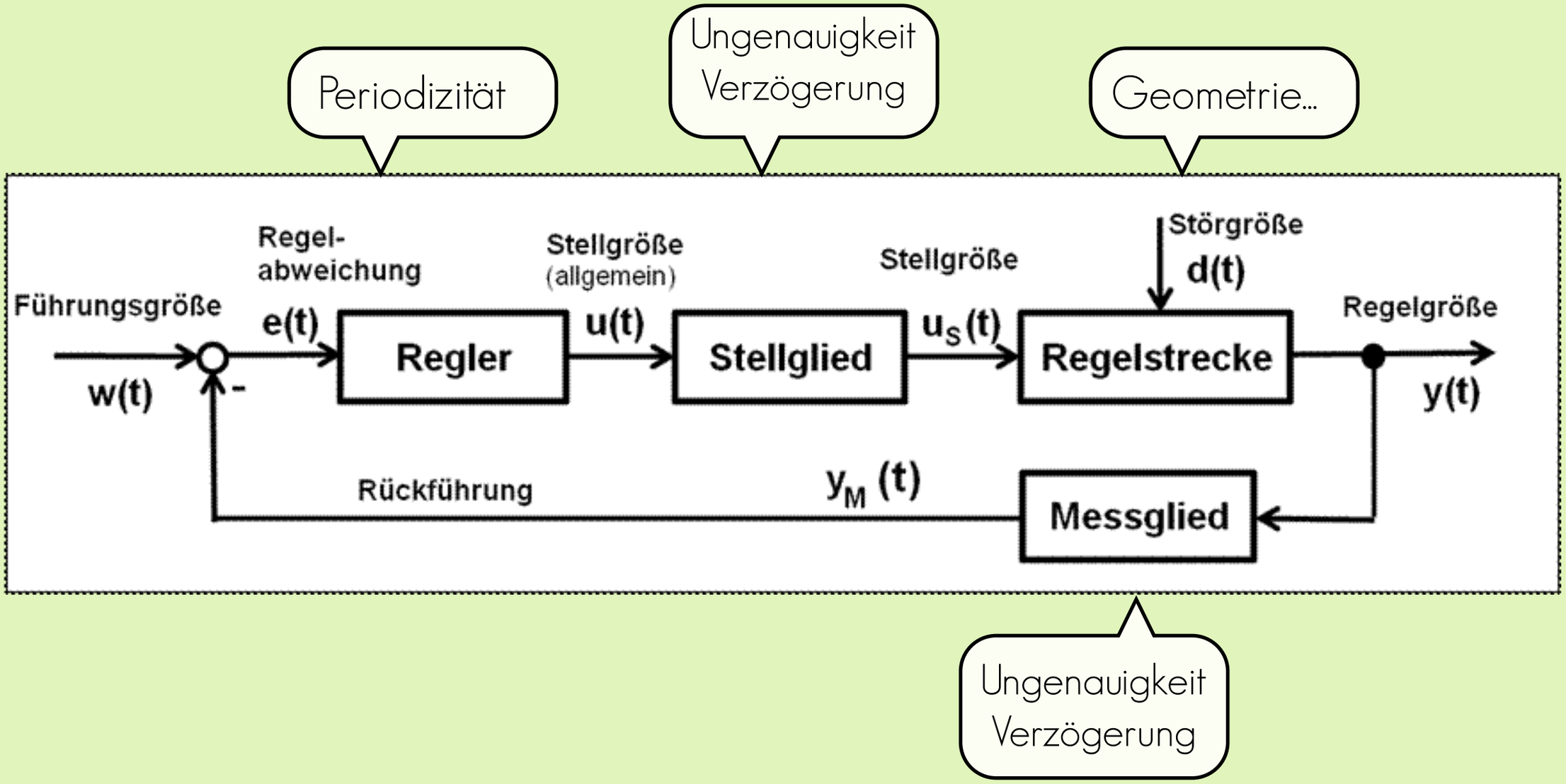
2013-11-22

Motivation

- Szenario: Sicherheitskritische Cyber-Physikalische Systeme
- Aufgabe: Finden von sicheren Parametern für das System
- Klassische Ansätze habe Probleme mit komplexen und nicht-linearen Systemen

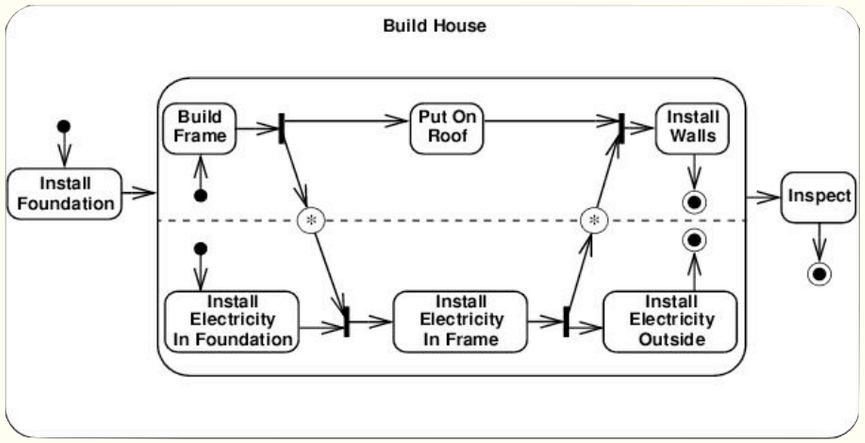
Warum Parametersynthese?

- Unterstützung des Entwicklers zur Designzeit
- Validierung einer ganzen Klasse von Systemen



Rechensysteme

Diskrete Zustandsübergänge



Physikalische Systeme

Kontinuierliche Zustandsübergänge

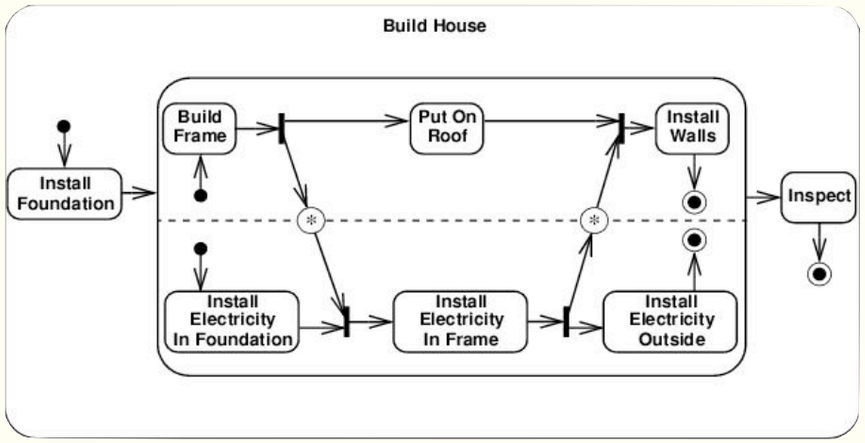
$$\dot{v} = g - \frac{kv^2}{m}$$

Hybride Systeme

Kontinuierliche und diskrete Zustandsübergänge

Rechensysteme

Diskrete Zustandsübergänge



Physikalische Systeme

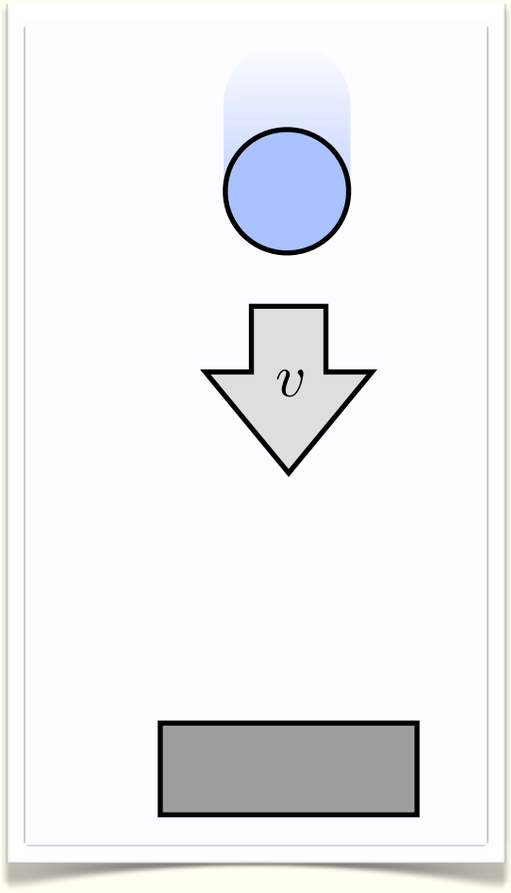
Kontinuierliche Zustandsübergänge

$$\dot{v} = g - \frac{kv^2}{m}$$

Modellierungssprache

Hybride Automaten (HA)

am Beispiel



steigend

...

$$x = 0$$
$$x' = x$$
$$v' = -\alpha \cdot v$$

Sprung

$$x_0 = 3$$
$$v_0 = 0$$

fallend

$$I: \quad x \geq 0$$

Invariante

$$F: \quad \dot{v} = g - \frac{kv^2}{m}$$
$$\dot{x} = v$$

Fluss

Modellierungssprache

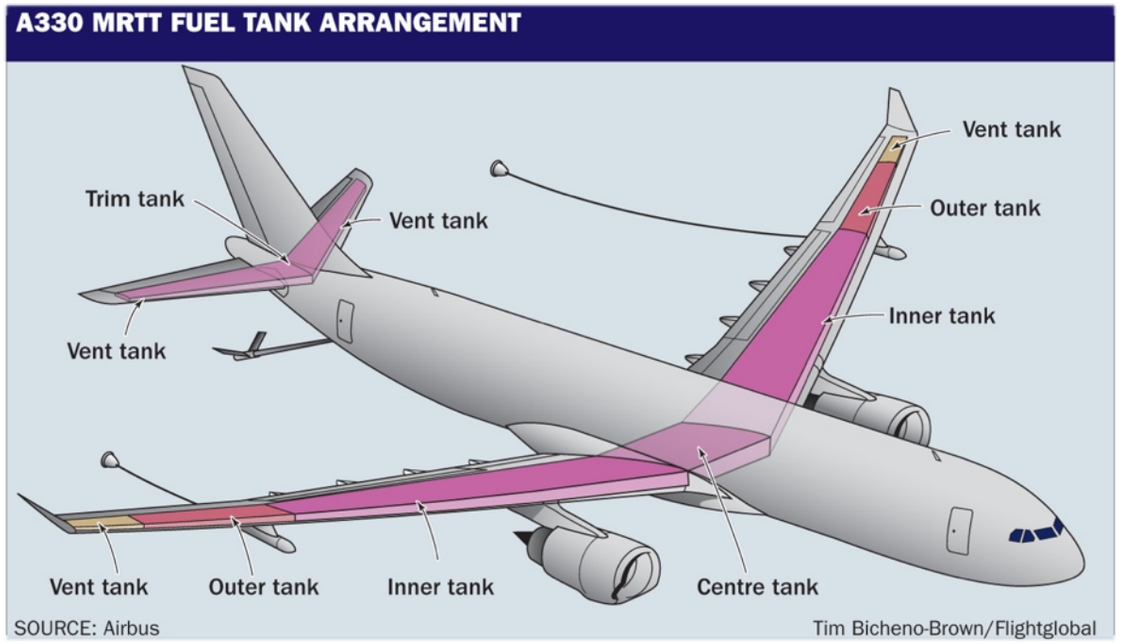
Determinismus	Determiniert	Stochastisch		Nicht-determiniert
Verifizierung	Simulation	SMC	Symbolisch	
			PMC	MC
Dynamik	beliebig		stark eingeschränkt	

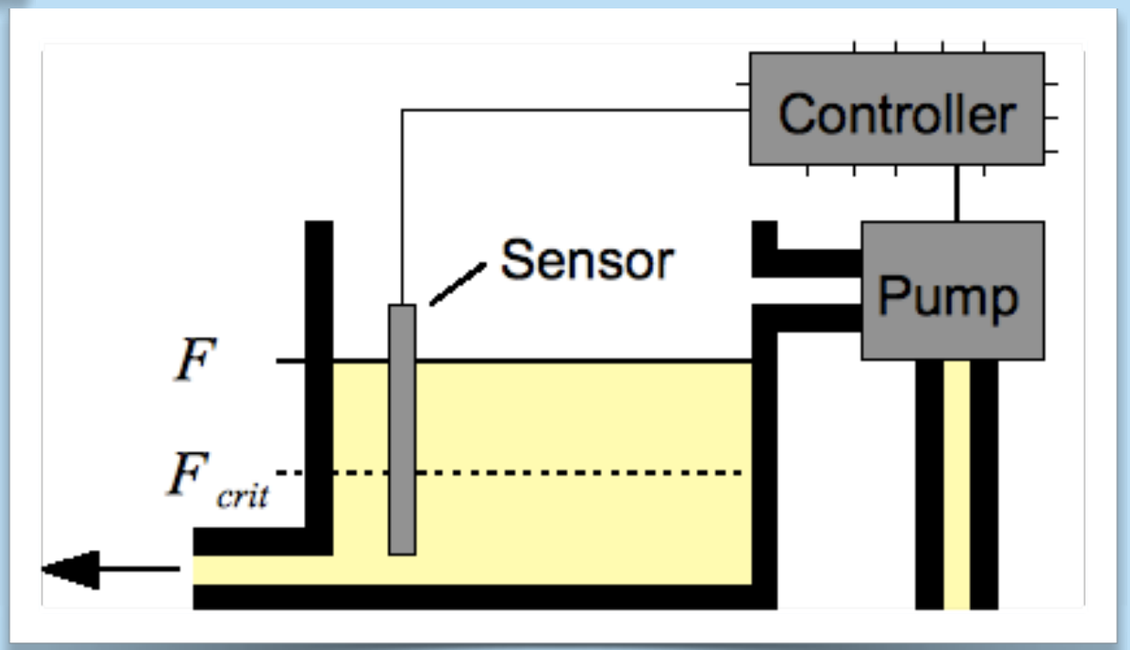
Modellierungssprache

Parametrisierbare Stochastische Hybride Automaten (PSHA)

- Parameter sind überall erlaubt, wo auch numerische Konstanten auftreten können
- kein nicht-stochastischer Nicht-Determinismus
- Stochastische Auswahl nur beim Sprung
- grundsätzlich beliebige Dynamik erlaubt, solange sie numerisch berechnet werden kann

Fallbeispiel





Fallbeispiel

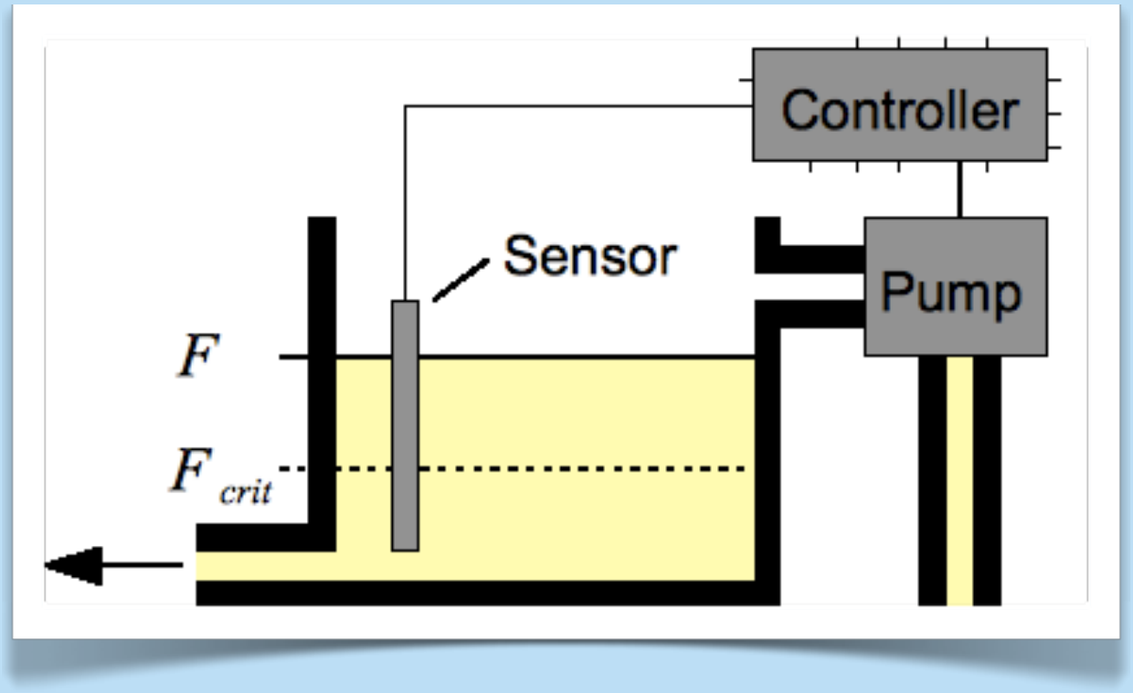
Tank
- Sicherheitsbedingung

Sensor
- Messfehler
- Alter des Messdatums

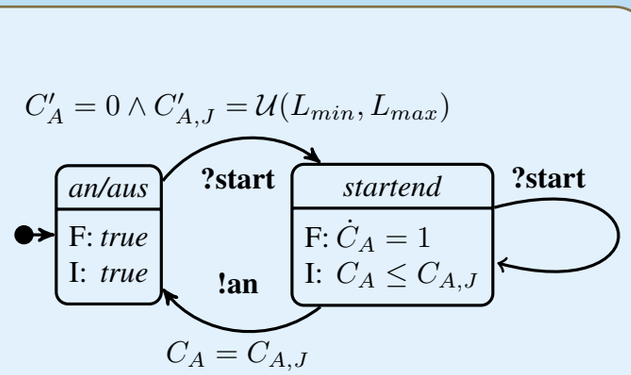
Pumpe
- Verzögerung

Kontrollprozess
- Unterbrechbar
- Periodisch

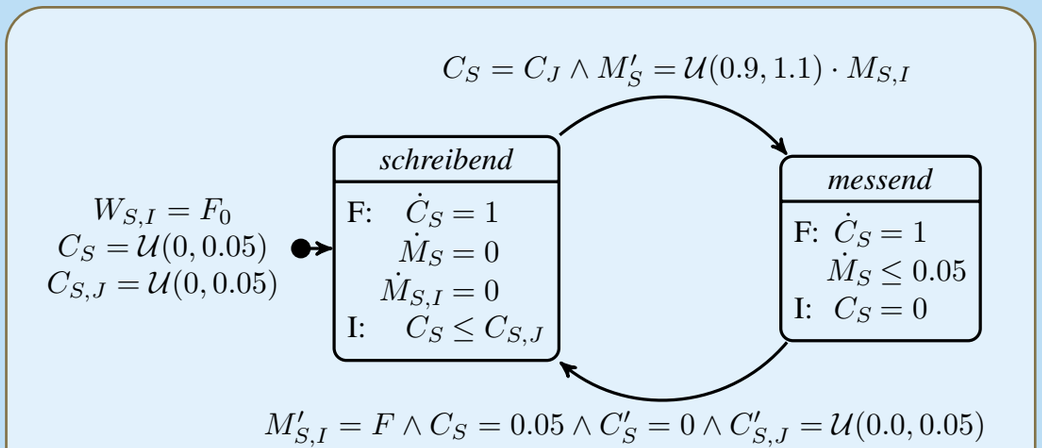
```
while true
  x = hole Sensordatum()
  if (x <= I)
    startePumpe()
  endif
endwhile
```



Fallbeispiel

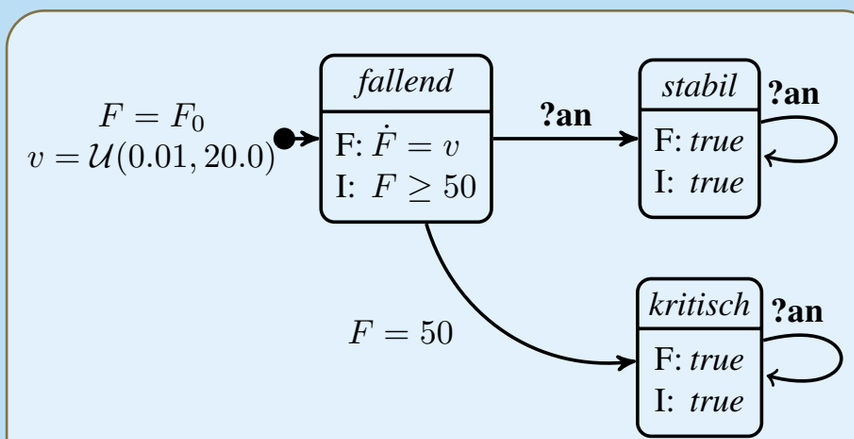


(a) Pumpensystem

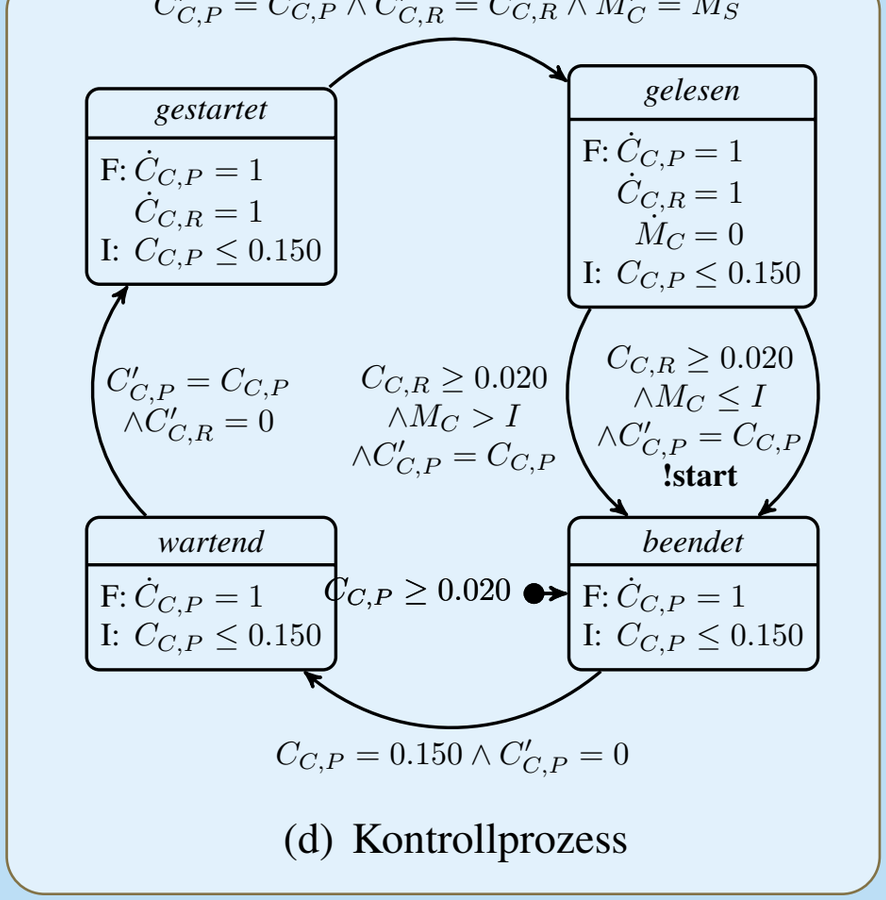


(b) Füllstandssensor

$$\phi = \neg\exists\Diamond \text{tank:kritisch}$$

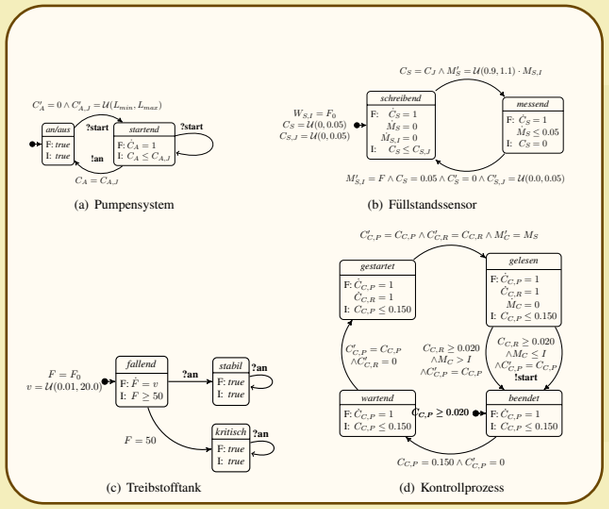


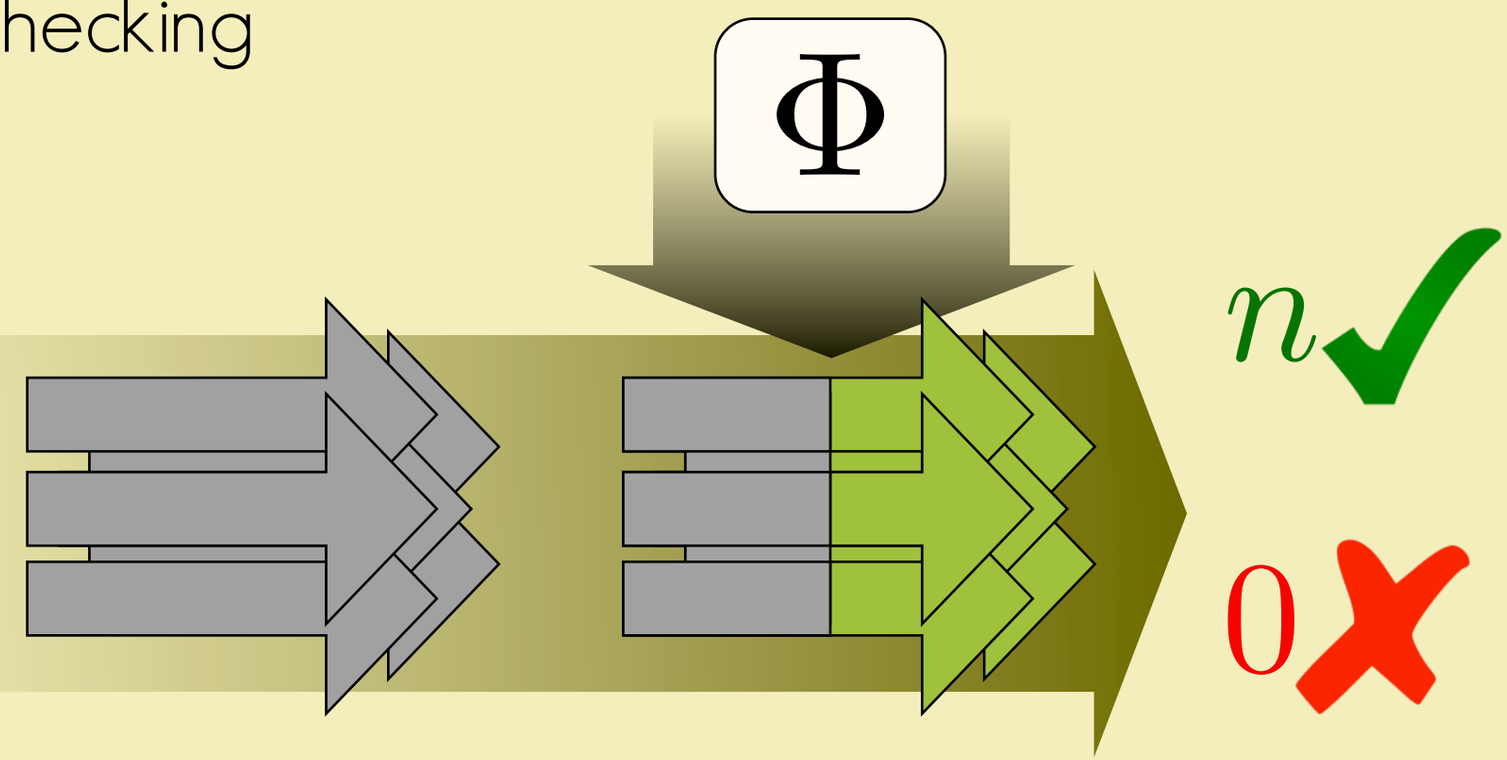
(c) Treibstofftank



(d) Kontrollprozess

Statistisches Model-Checking





n *Ausführungen*

Prüfung der Eigenschaft für konkrete Ausführungen

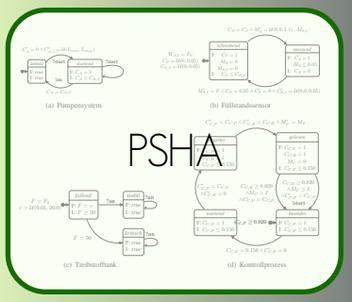
Was ist die Wahrscheinlichkeit nur ✓ zu sehen, obwohl $\mathrm{P}(\overline{\Phi})$ größer ist als p_{max}?

$$\mathrm{P}(0\text{✗}) \leq (1 - p_{max})^n =: \alpha$$

Mit einer Wahrscheinlichkeit von $1 - \alpha$ ist $\mathrm{P}(\overline{\Phi}) < p_{max}$

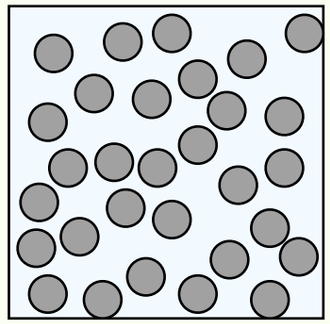
Statistische Parametersynthese

Kandidaten-Parameter-Raum

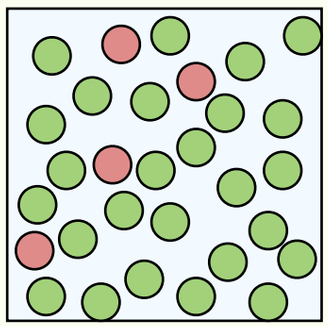


Φ

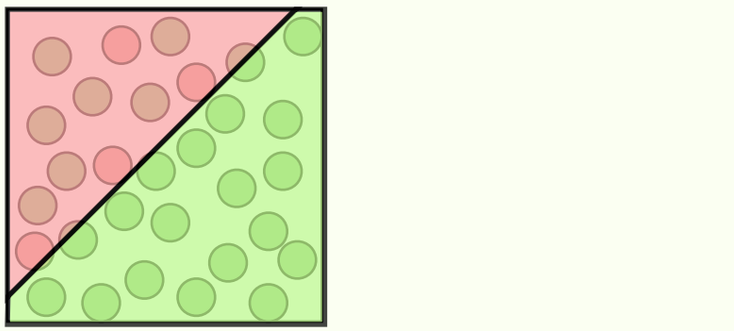
α
p_{max}



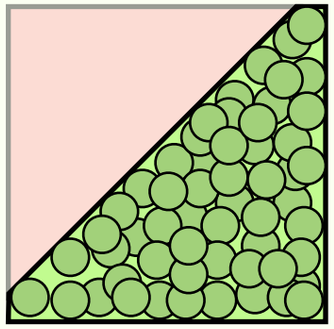
(1) Sampling



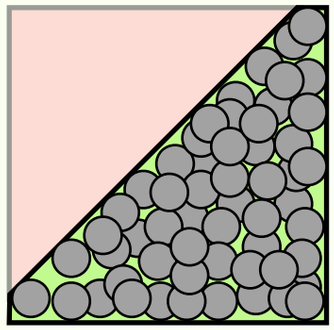
(2) Simulation



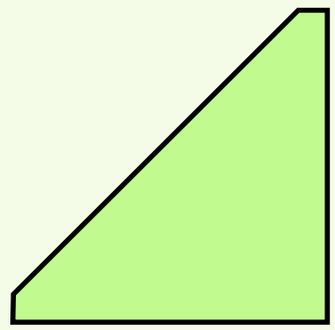
(3) Klassifizierung



(5) SMC

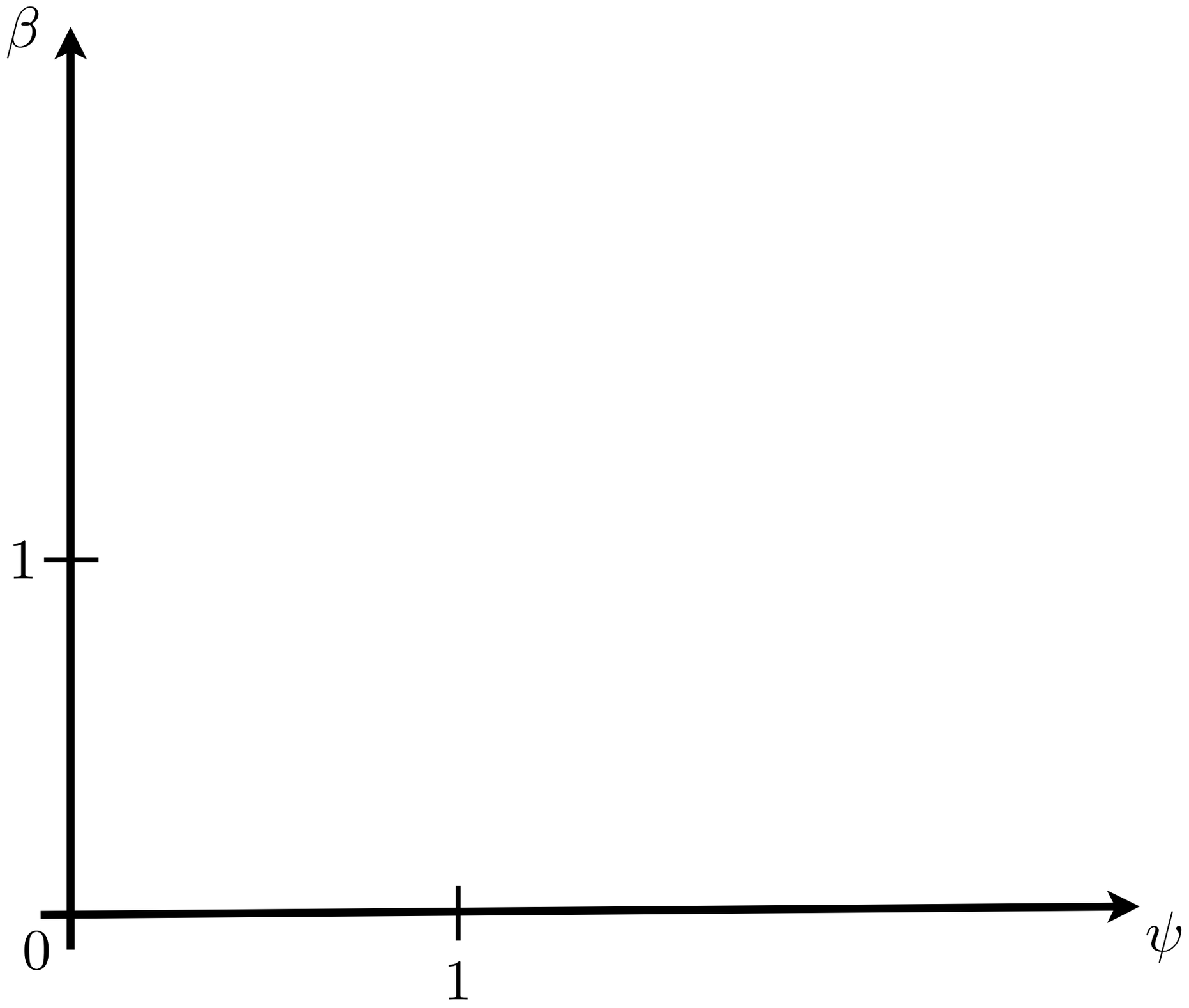


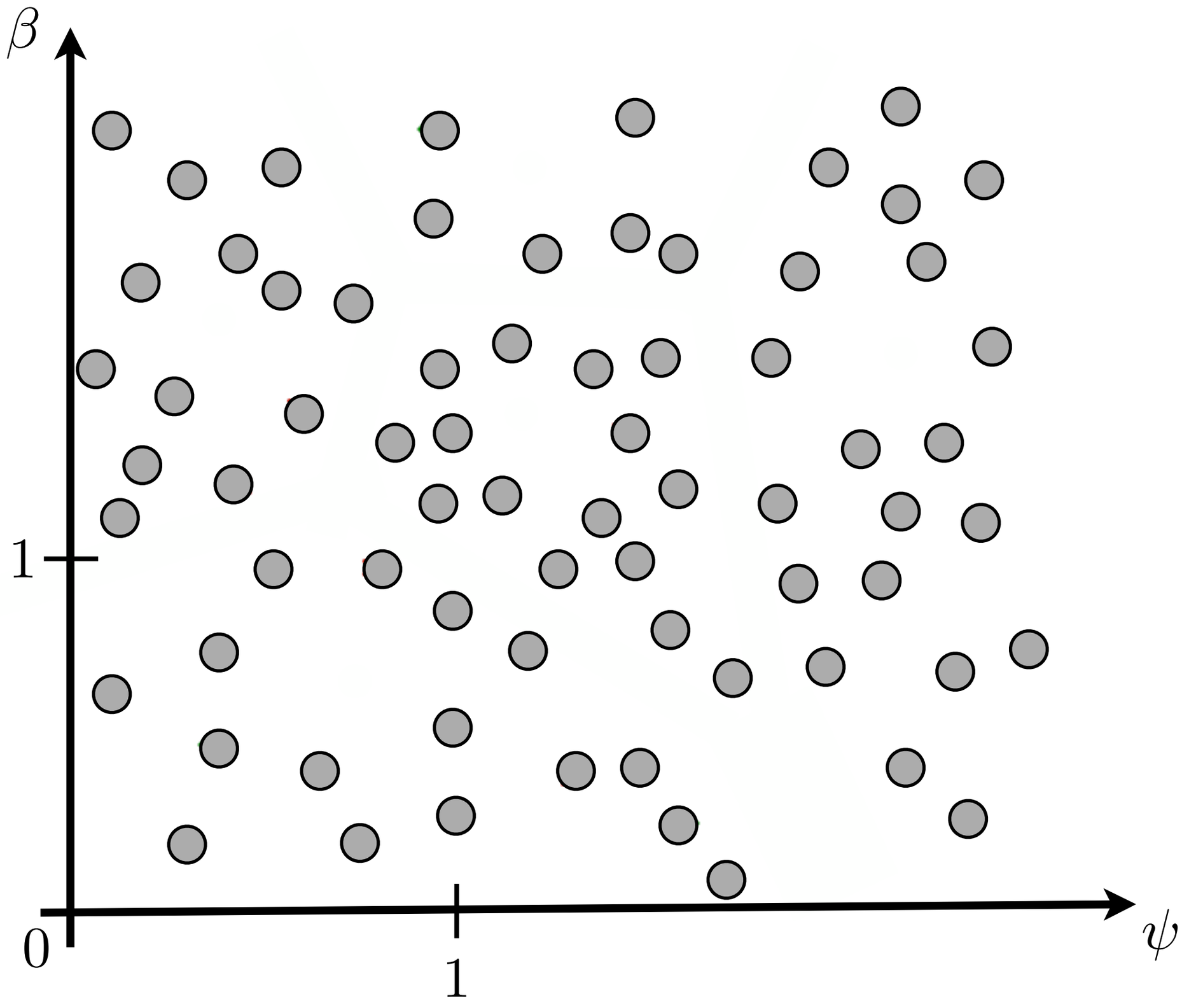
(4) Sampling

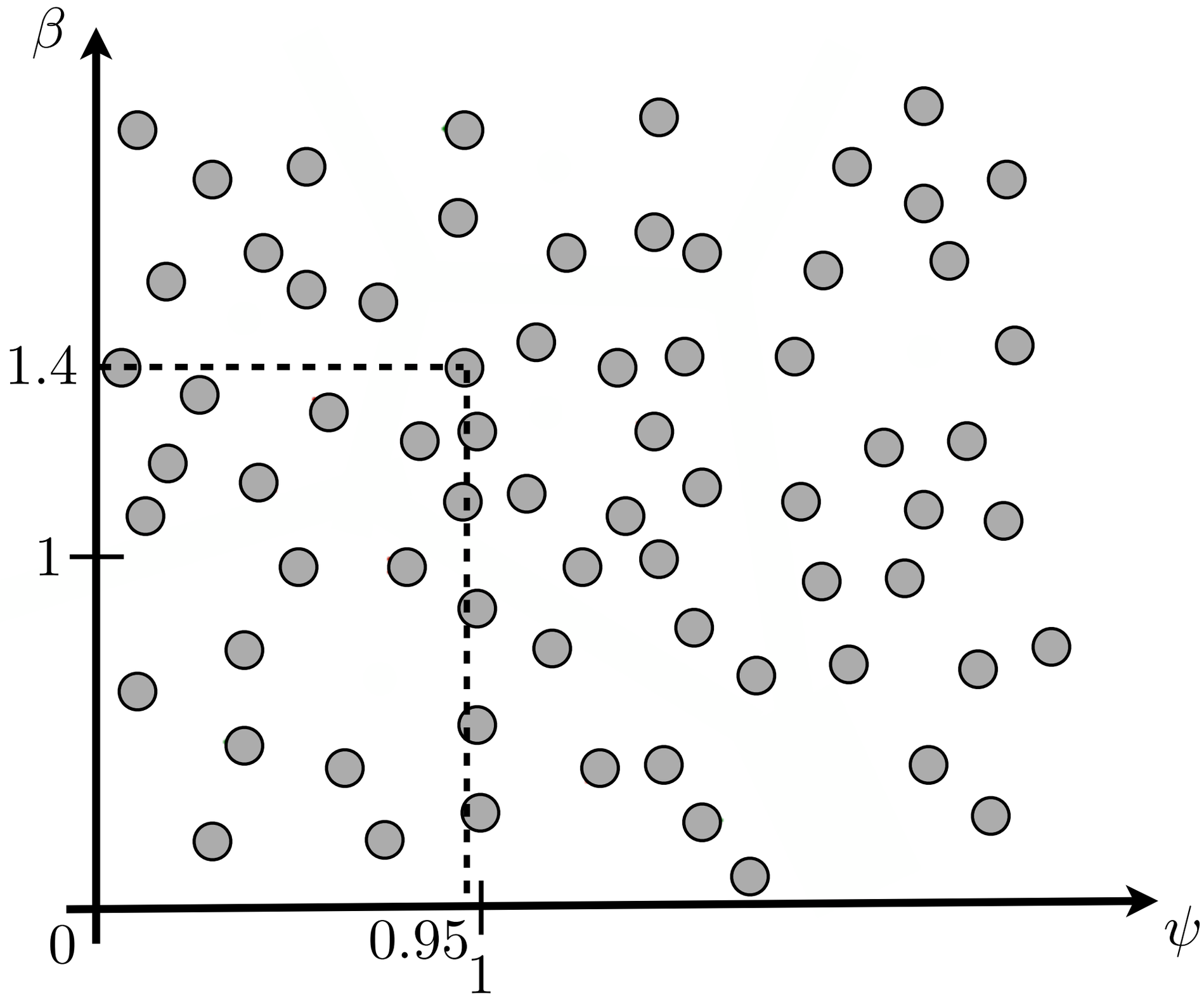


sicherer Parameterraum bezgl. α und p_{max}

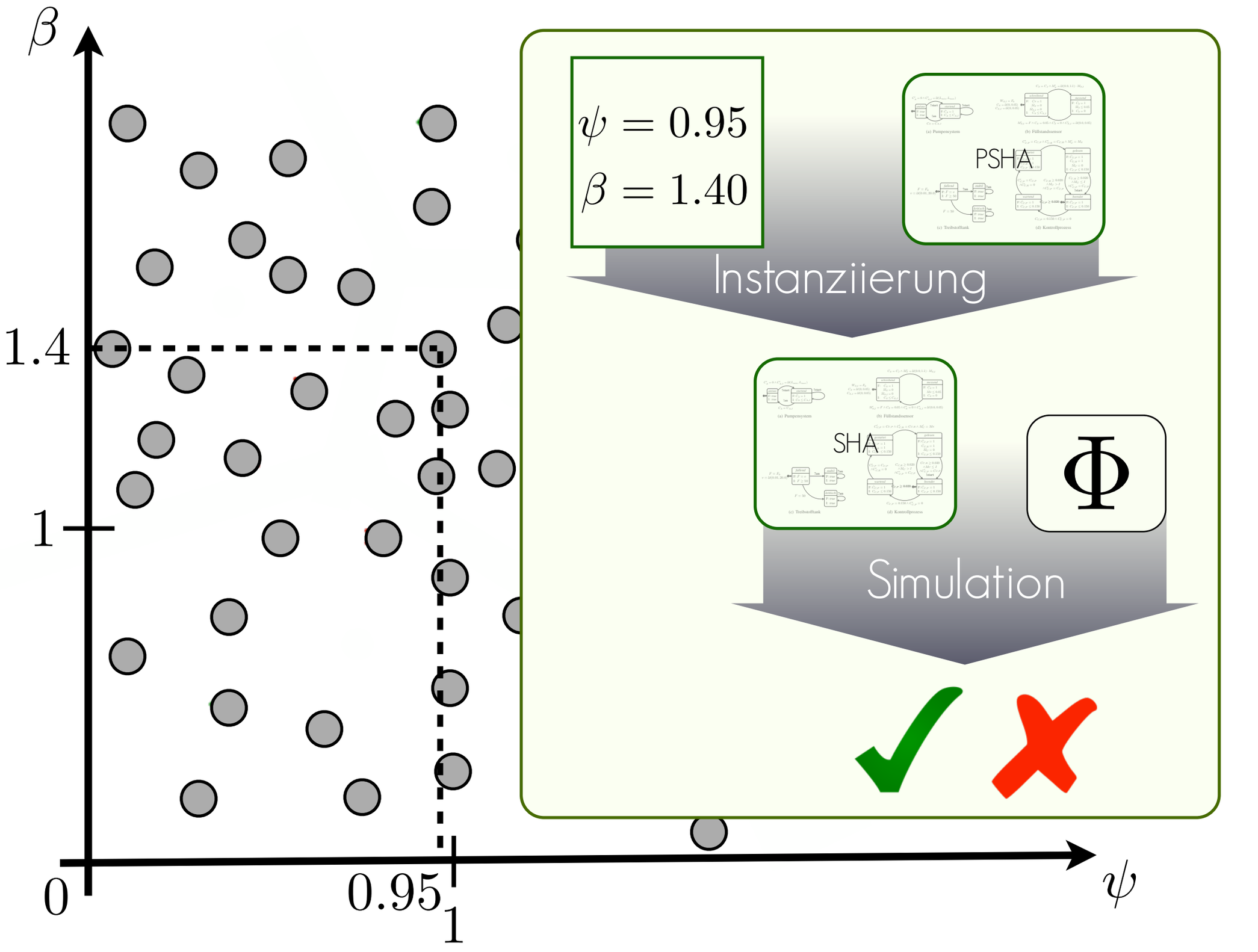
Kandidaten-
Parameter-
Raum

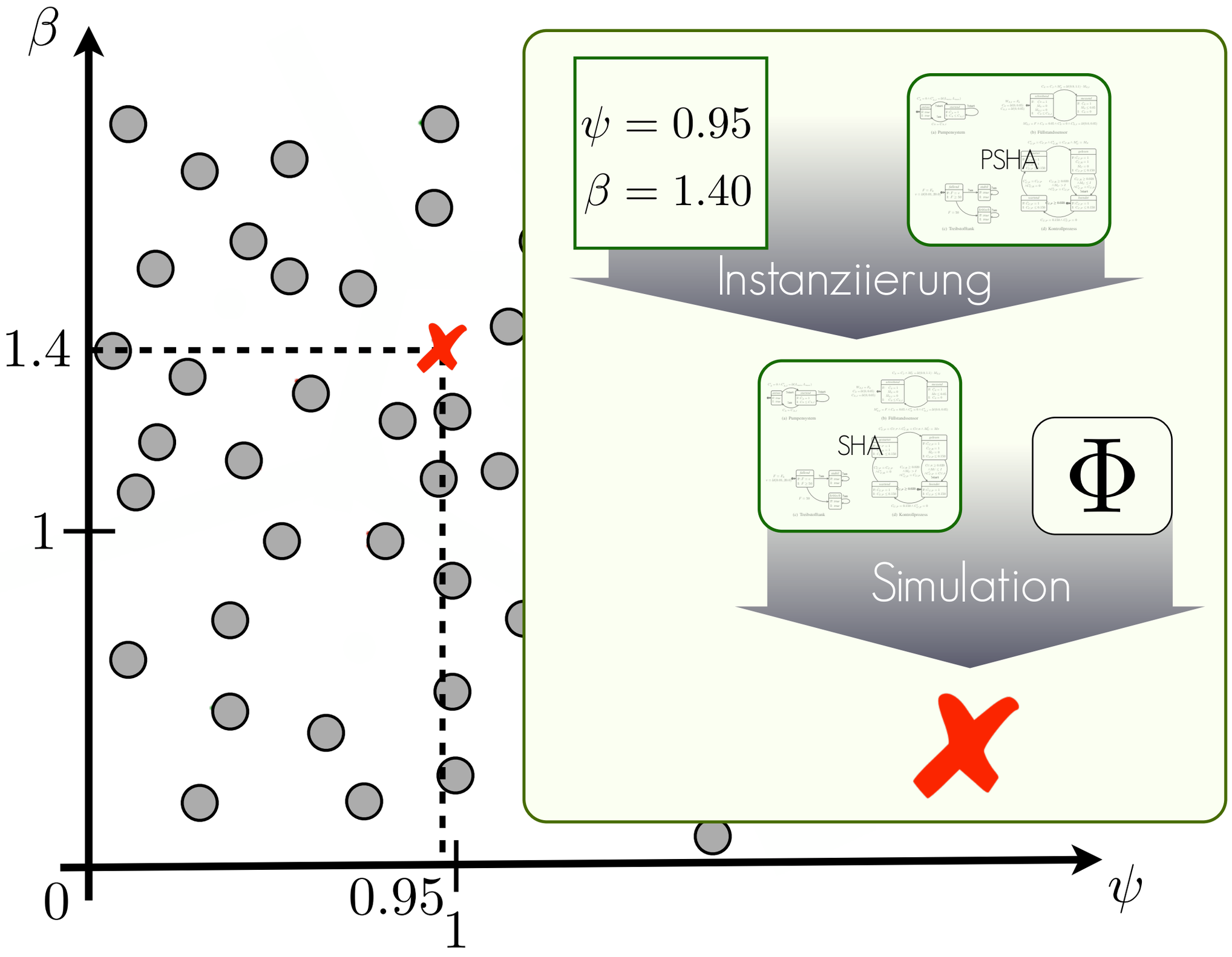

β
1
0
1
ψ

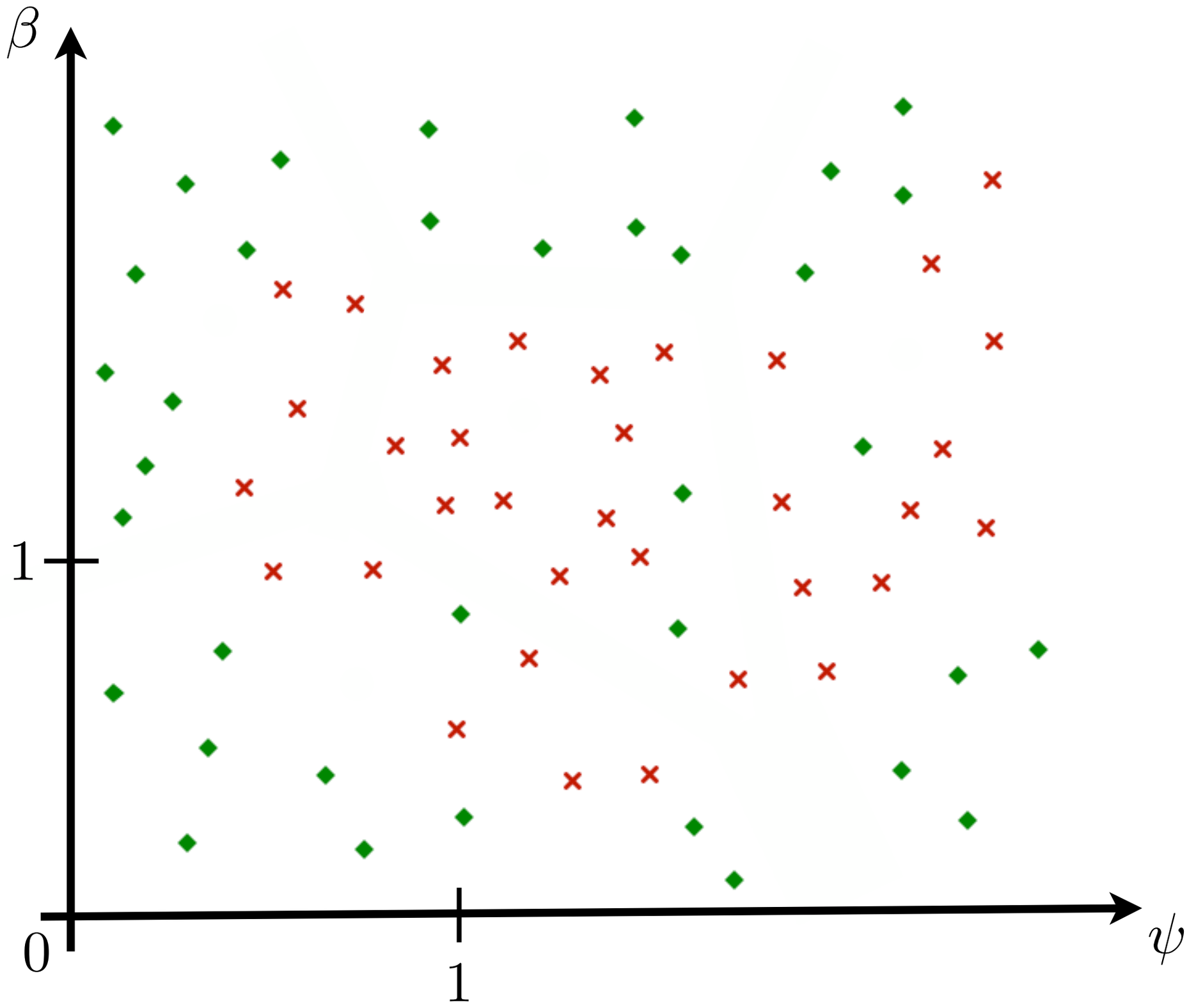

β
1
0
1
ψ


β
1.4
1
0
0.95
1
ψ

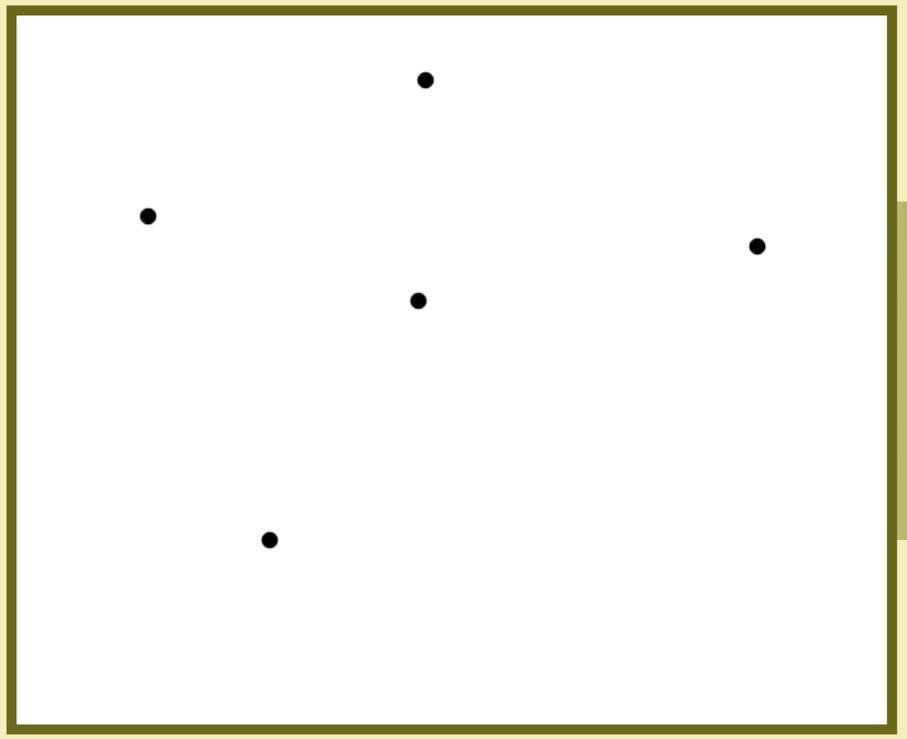
Sampling


β
1.4
1
0
0.95
1
ψ
ψ = 0.95
β = 1.40
PSHA
Instanziierung
SHA
Φ
Simulation

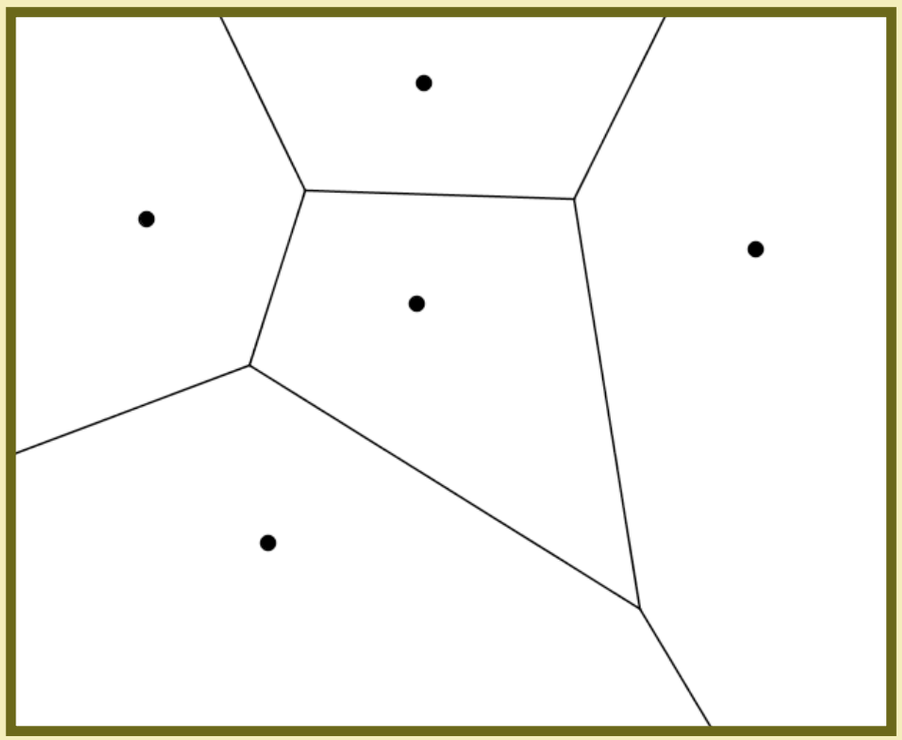

β
1.4
1
0
0.95
1
ψ
ψ = 0.95
β = 1.40
PSHA
Instanziierung
SHA
Φ
Simulation


β
1
0
1
ψ

Voronoi-Zellen



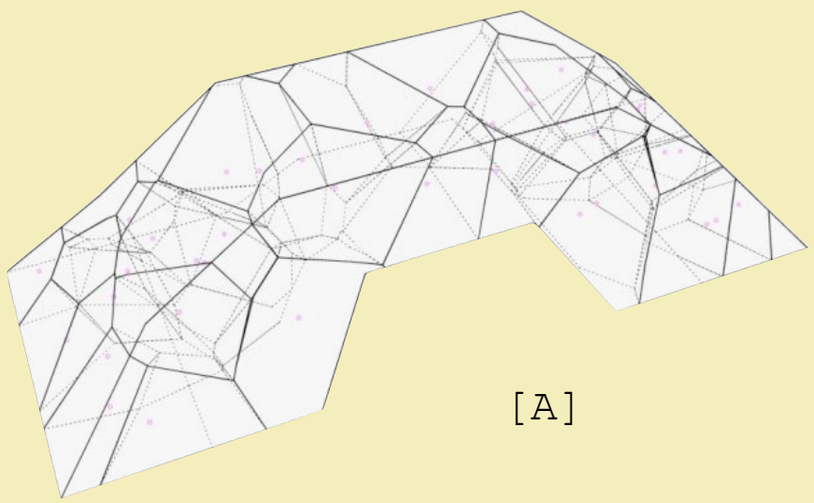
Eingabe: Menge von Zentren



Ausgabe: Voronoi-Regionen

Vorteile

- Einfache Repräsentation (Vektor von Zentren)
- Flexibel
- Einfache Umwandlung in Ungleichheitssystem (konvexe Polytope)
- Anwendbar für beliebige Dimensionen

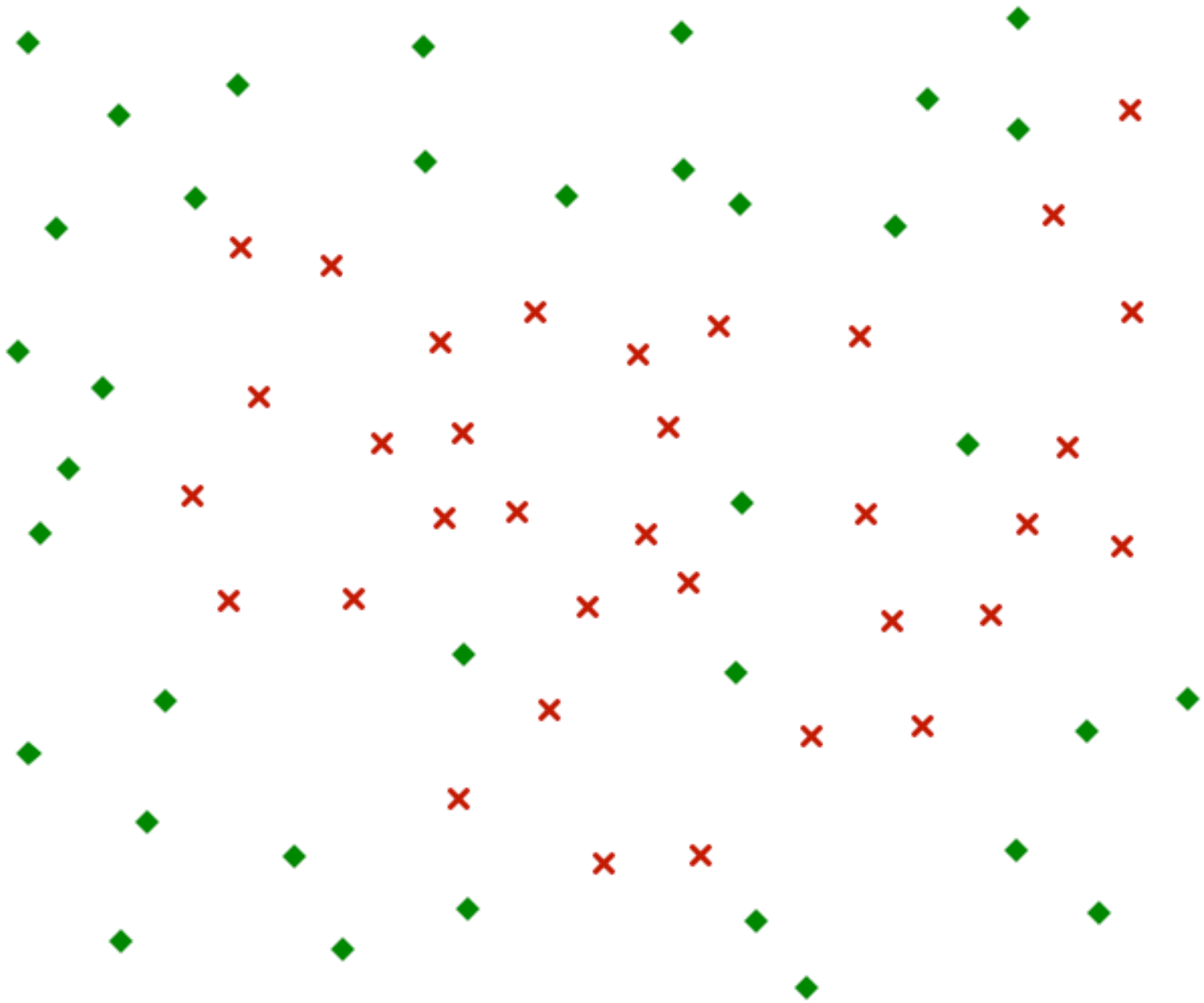


[A]

Klassifizierung

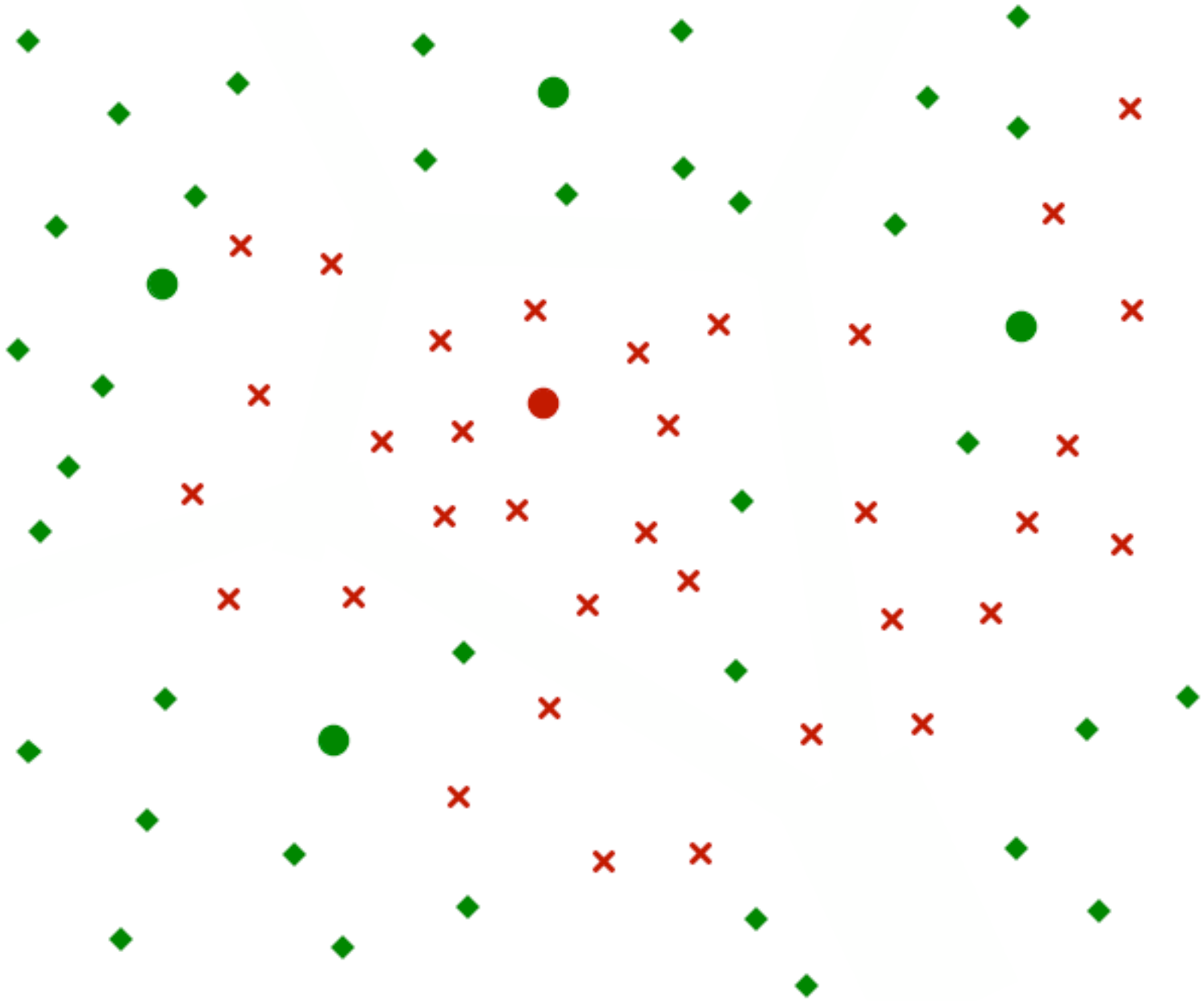
UNIVERSITÄT KOBLENZ · LANDAU

Beispiel:

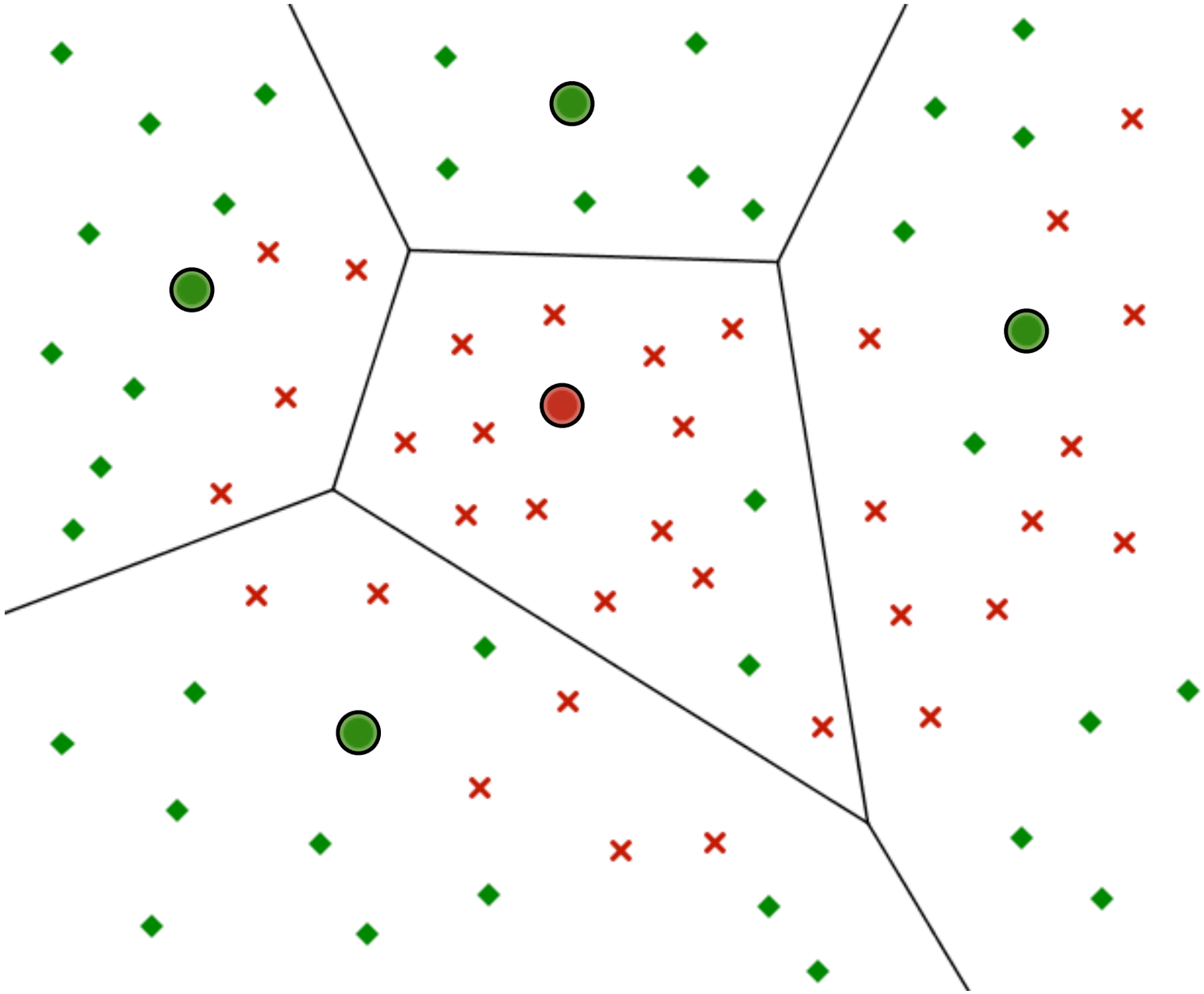


UNIVERSITÄT KOBLENZ · LANDAU

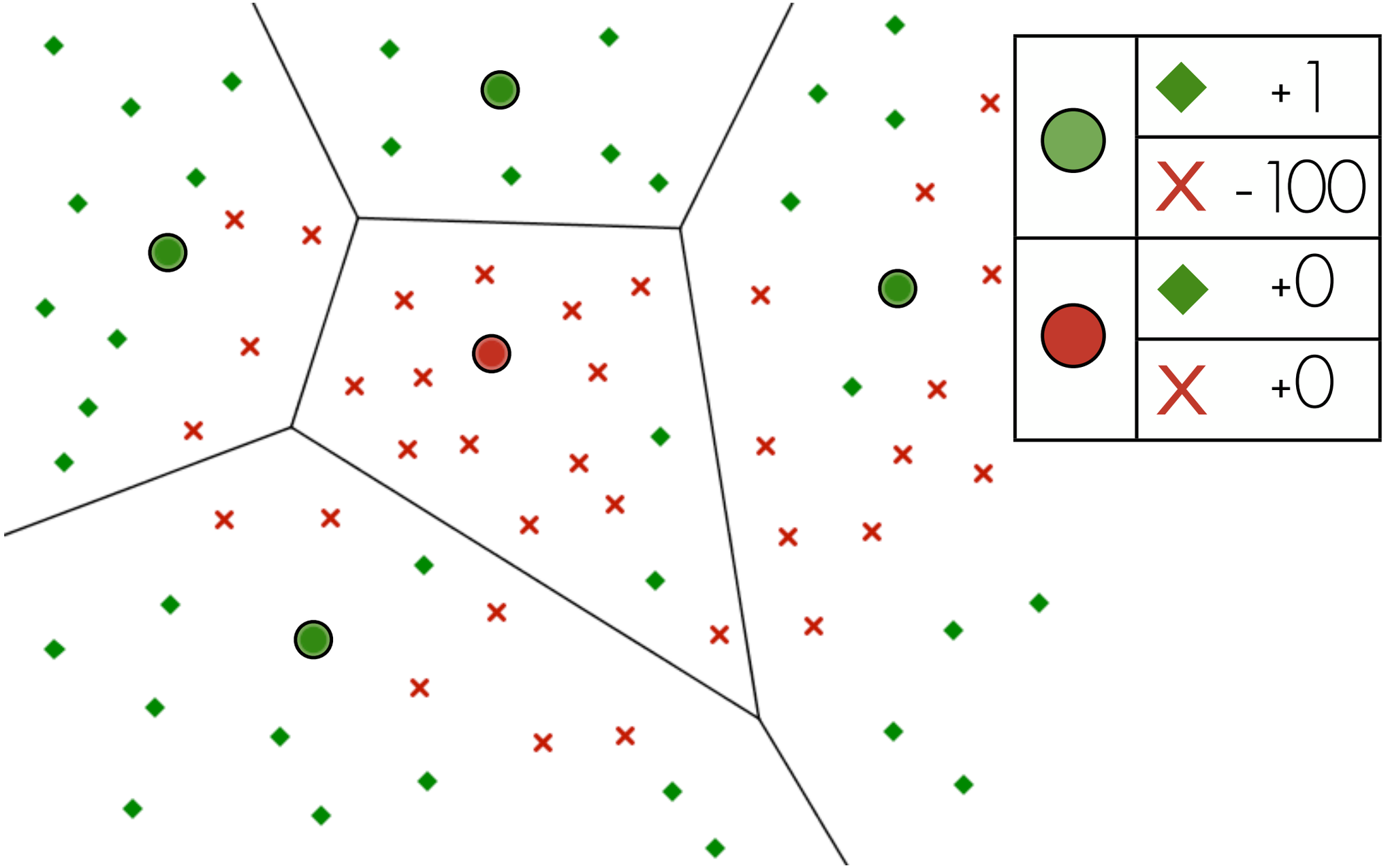
Beispiel:



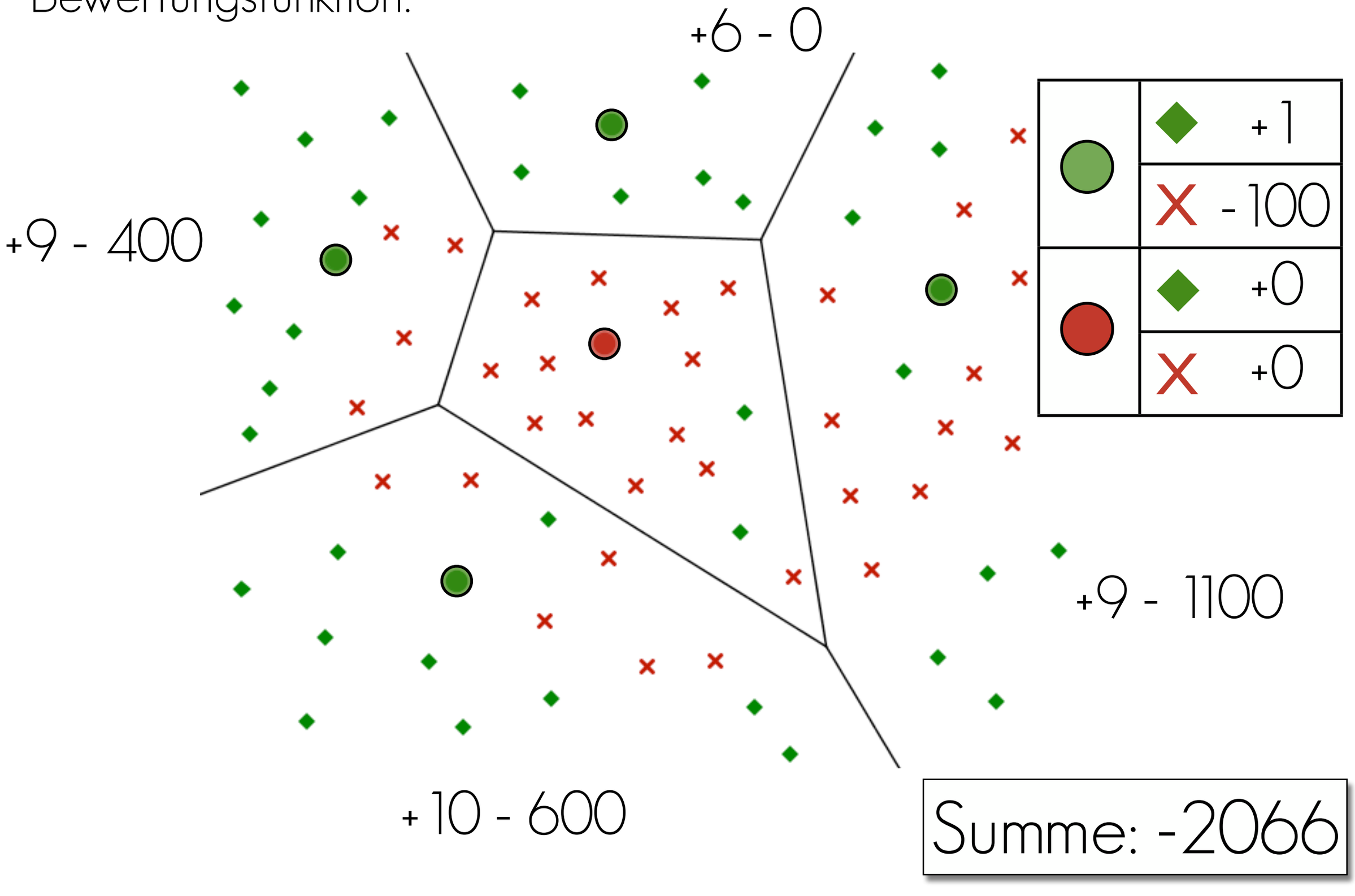
Initialisierung:



Bewertungsfunktion:

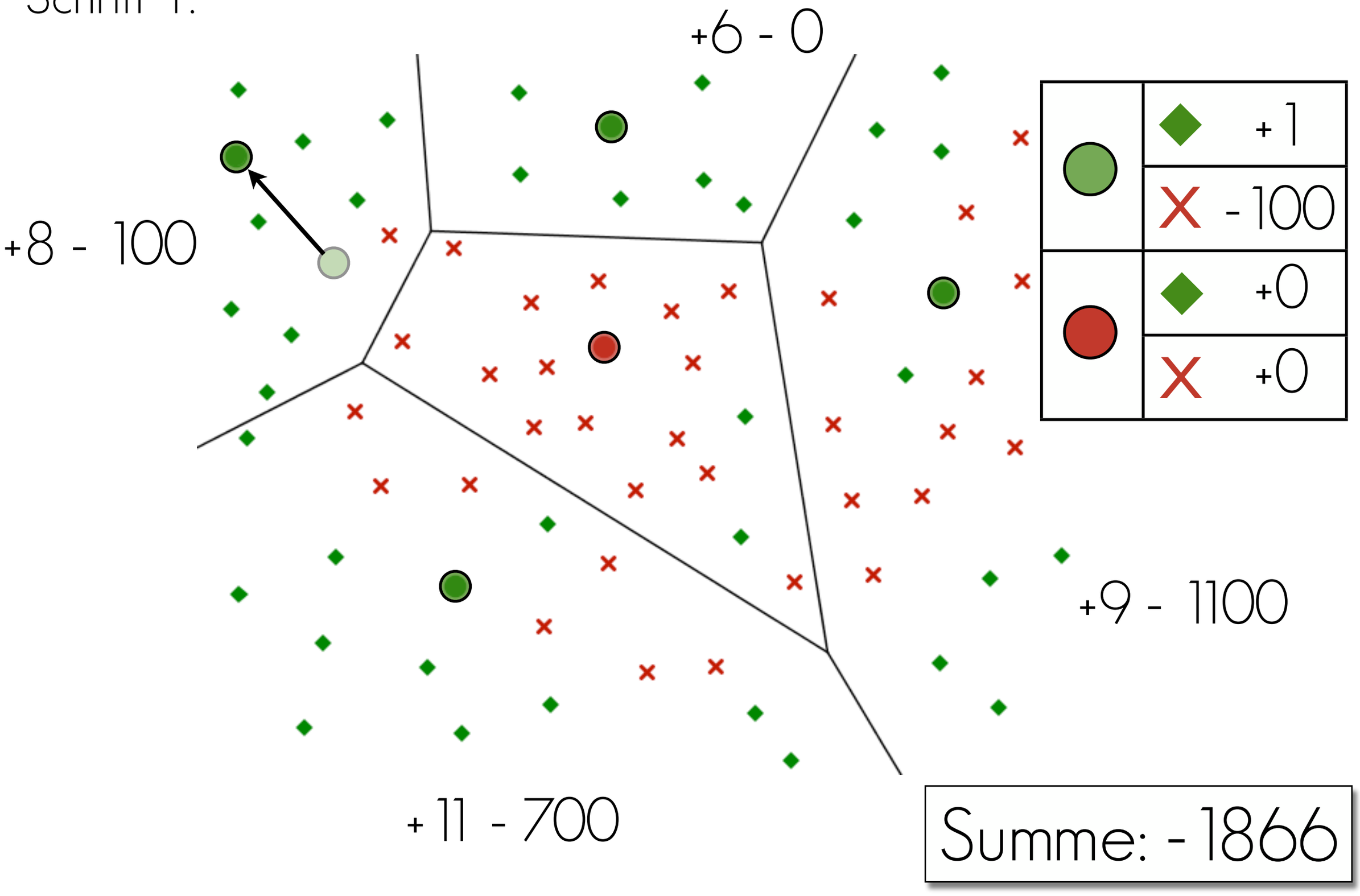


Bewertungsfunktion:



Summe: -2066

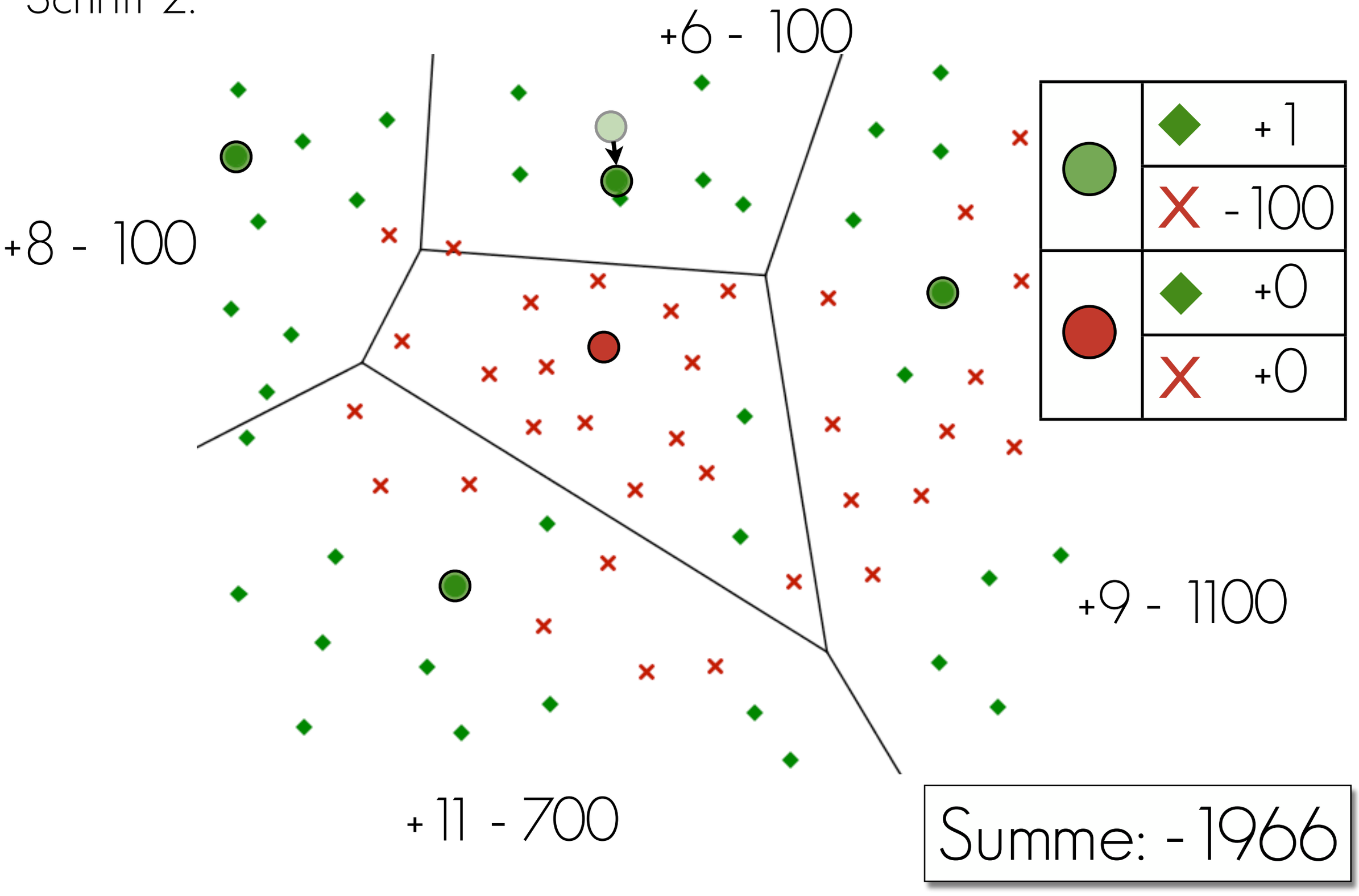
Schritt 1:



Summe: - 1866

UNIVERSITÄT KOBLENZ · LANDAU

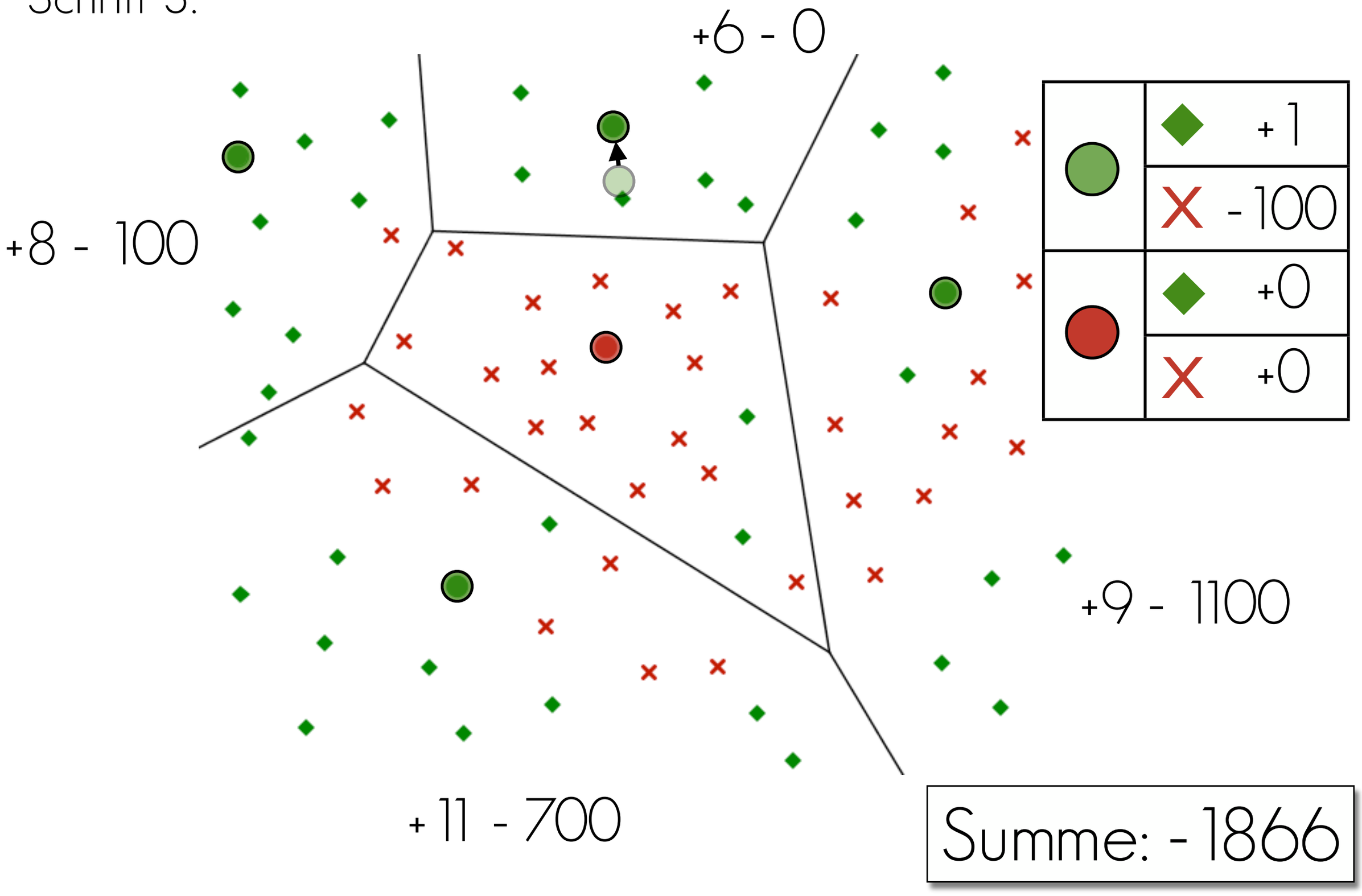
Schritt 2:



Summe: - 1966

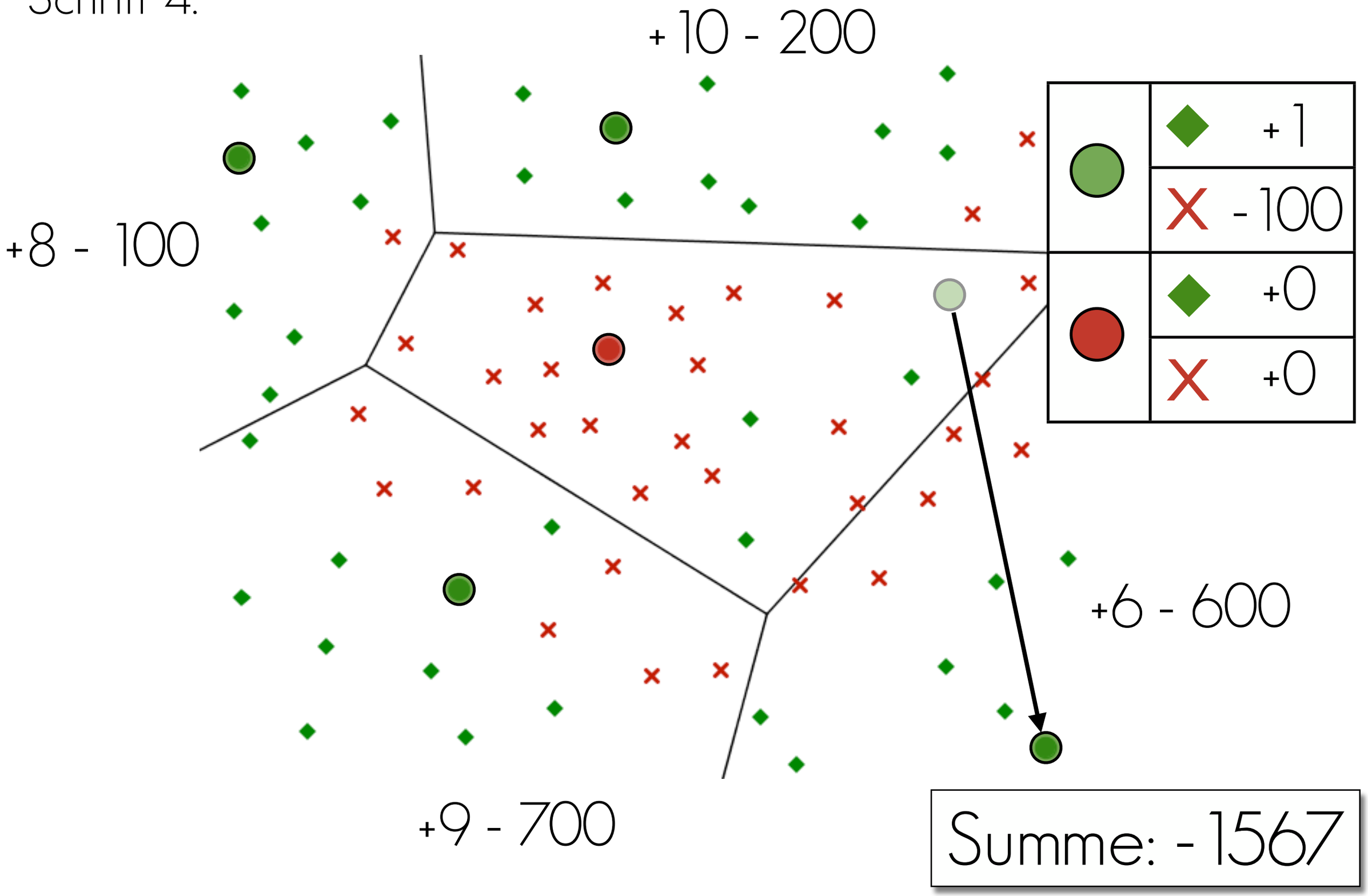
UNIVERSITÄT KOBLENZ · LANDAU

Schritt 3:



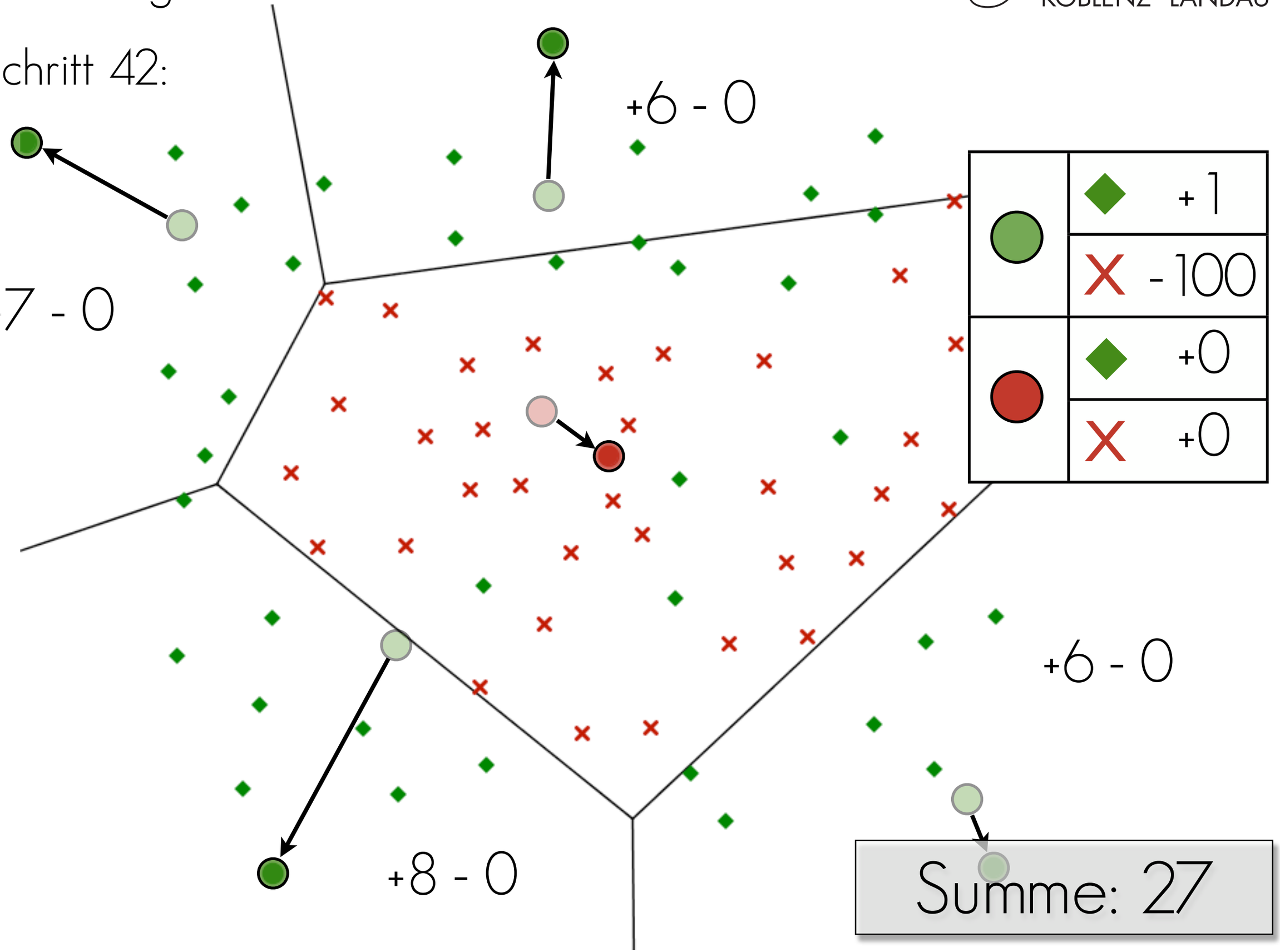
UNIVERSITÄT KOBLENZ · LANDAU

Schritt 4:



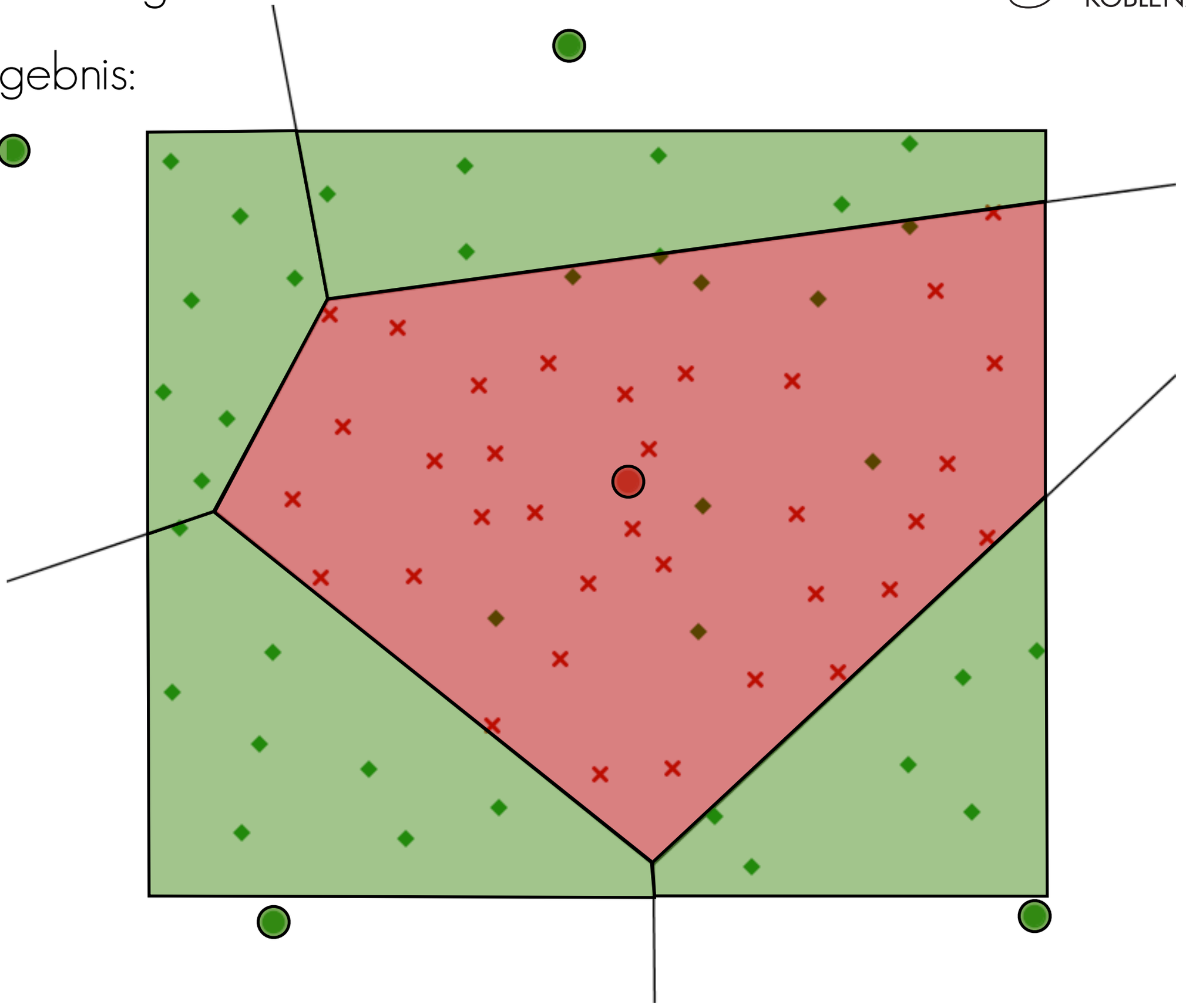
Klassifizierung

Schritt 42:

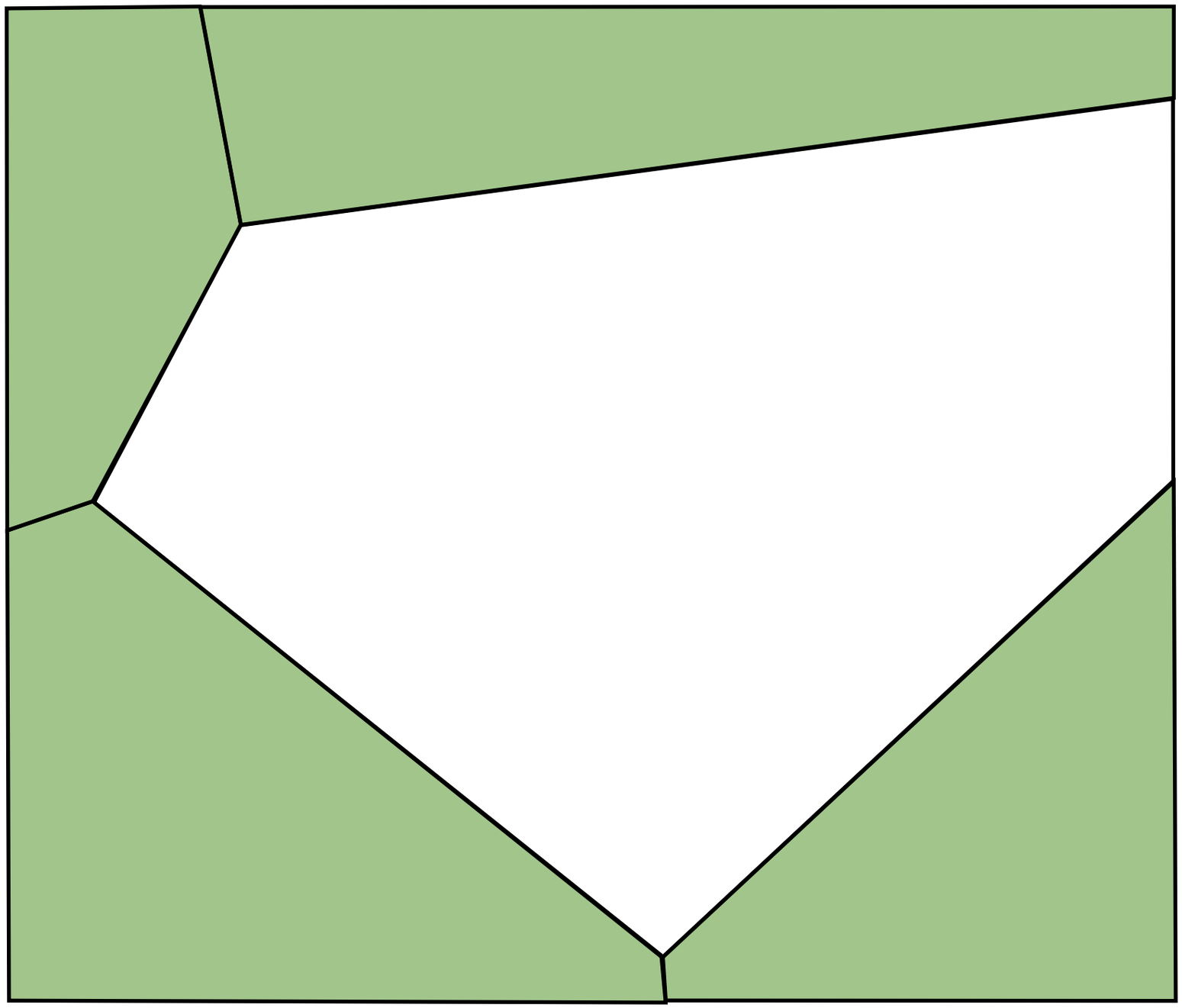


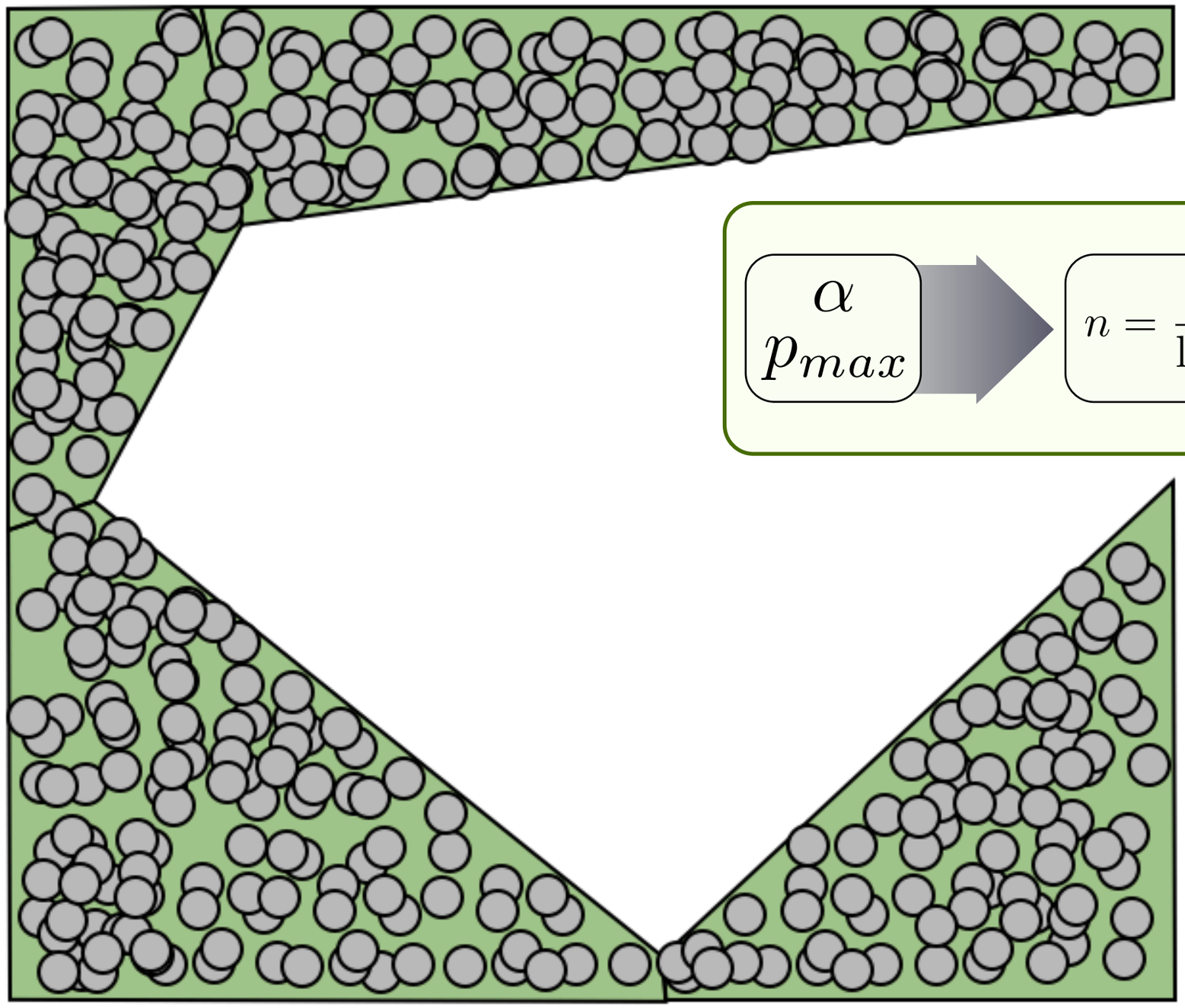
Klassifizierung

Ergebnis:

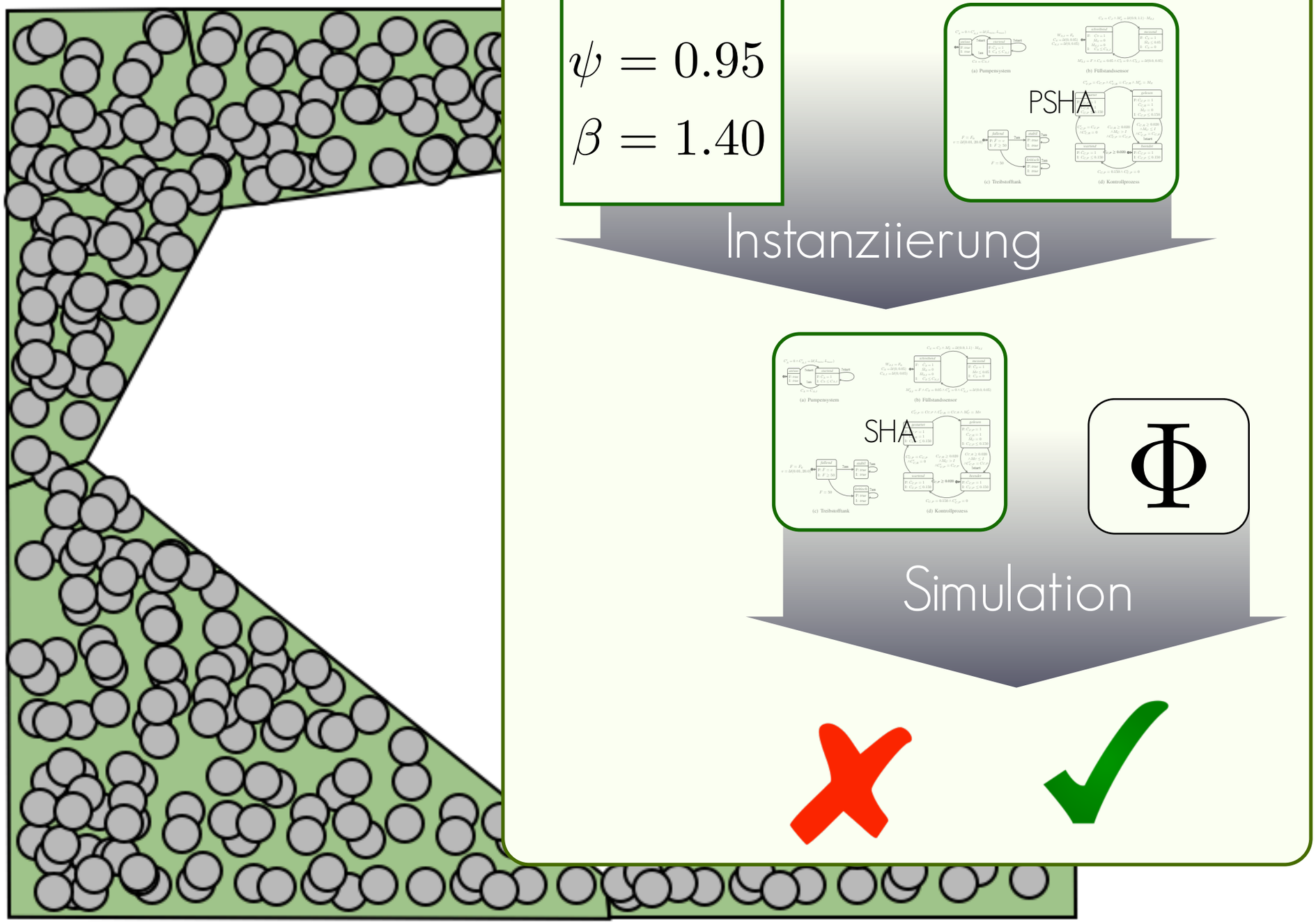


Ergebnis:

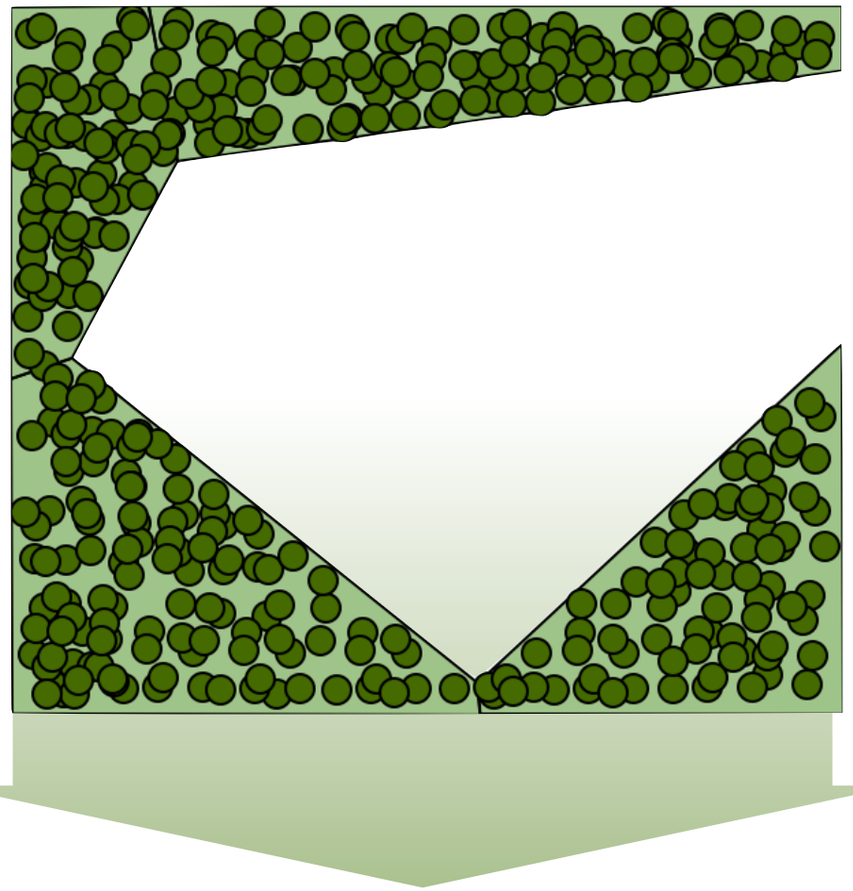


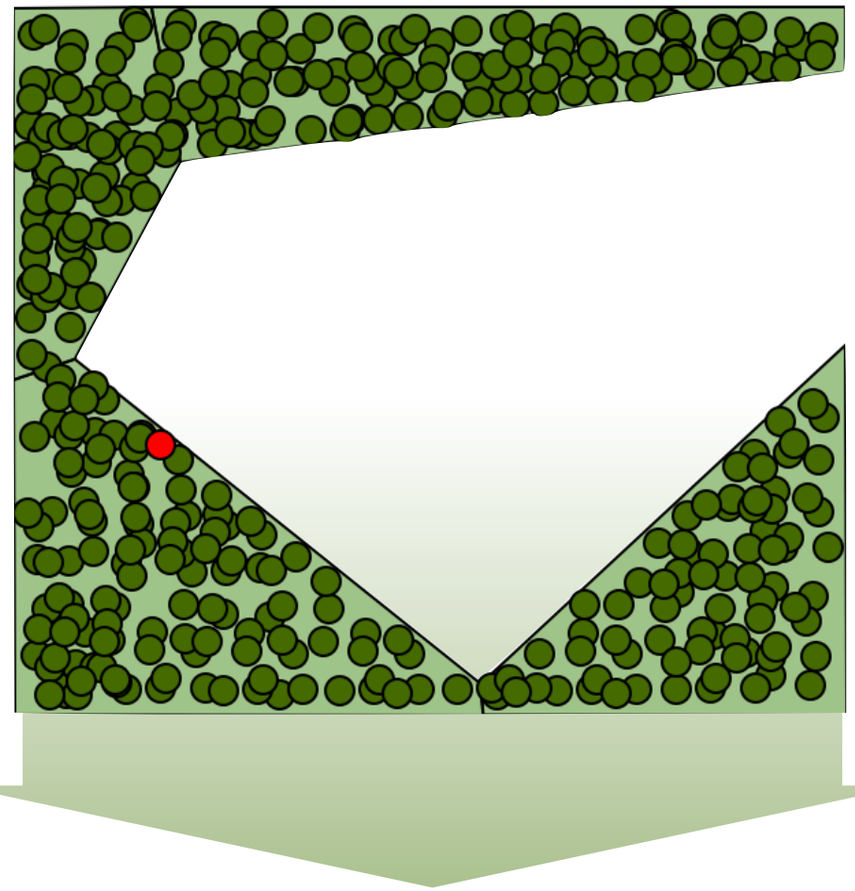


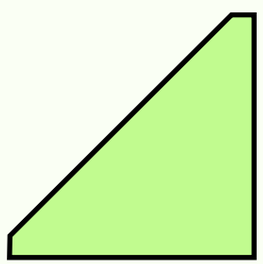
$$\begin{matrix}\alpha \\ p_{max}\end{matrix} \Rightarrow n = \frac{\ln \alpha}{\ln(1 - p_{max})}$$


$\psi = 0.95$
$\beta = 1.40$
PSHA
Instanziierung
SHA
Φ
Simulation

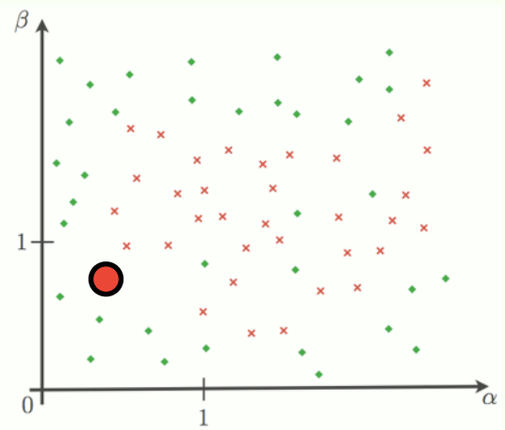
Ergebnis:





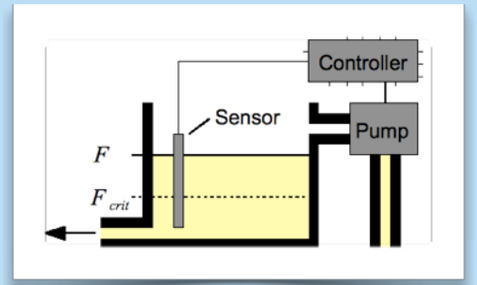


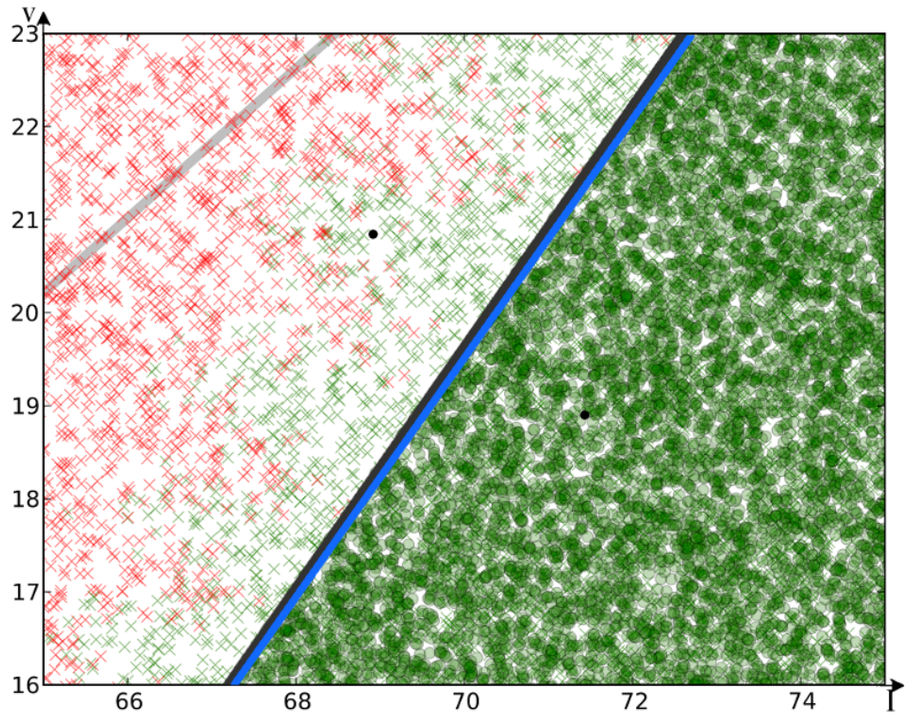
sicherer Parameterraum bezgl. α und p_{max}



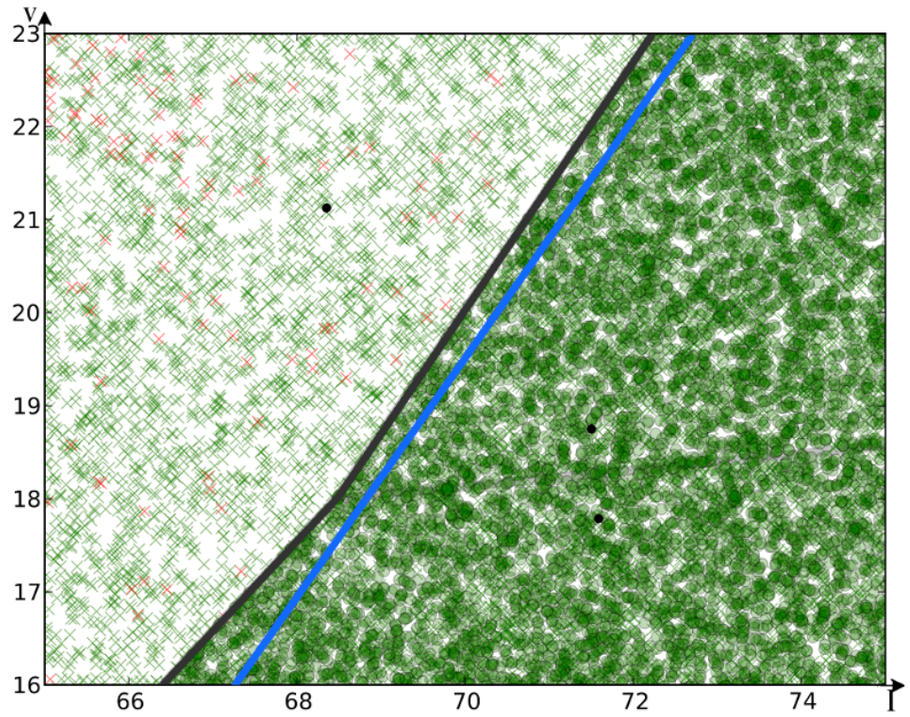
- füge Gegenbeispiel hinzu
- wiederhole:
  - Klassifikation,
  - Sampling,
  - Simulation

Evaluierung:
Sicherer Parameterraum:





(a) Parameterraum für eingeschränkt stochastisches Modell (Konfidenzniveau 99.9%, $p_{max} = 0.06$)



(b) Parameterraum für gleichverteilten Sensorfehler (Konfidenzniveau 99.99%, $p_{max} = 0.0001$)

schwarz: Statistische Parametersynthese
blau: Symbolische Worst-Case Analyse

Fazit

- natürliche Erweiterung des statistischen Modell-Checking-Verfahrens um Parametersynthese

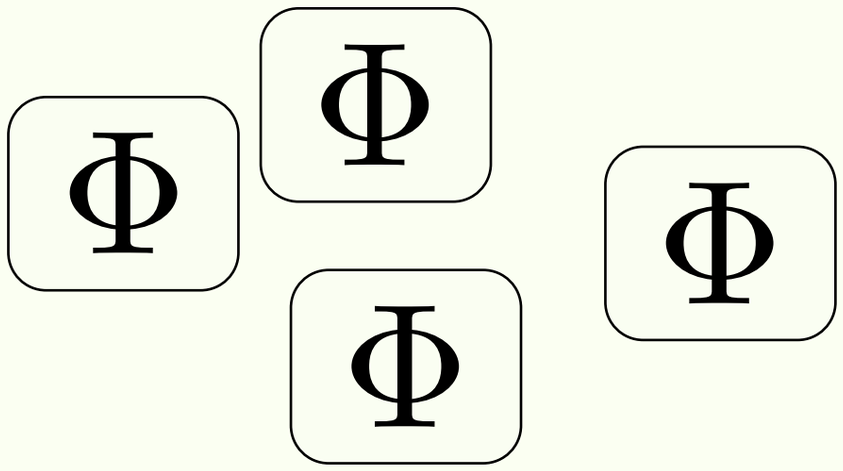
Nachteile:

- Zusätzlicher Modellierungsaufwand für PSHA
- liefert nur probabilistische Garantien
- bei hoher Genauigkeit viele Stichproben benötigt

Vorteile:

- Reiche Modellierungssprache
- Modelle müssen nur ausführbar sein
- leicht parallelisierbar

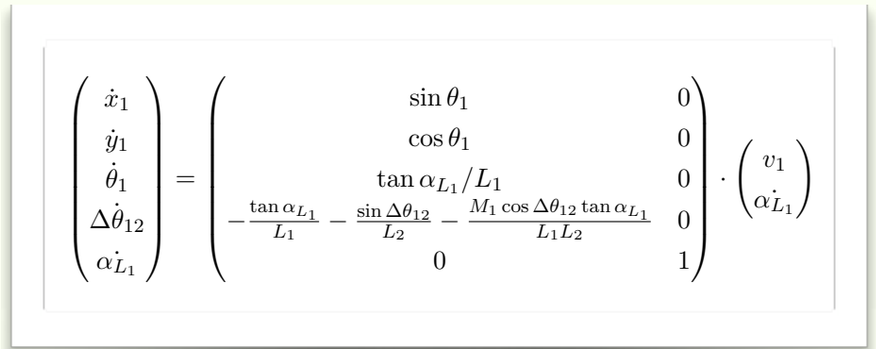
Ausblick



Komplexere Eigenschaften

Optimierungen:

- Parallelisierung
- Importance Based Sampling



$$\begin{pmatrix} \dot{x}_1 \\ \dot{y}_1 \\ \dot{\theta}_1 \\ \Delta\dot{\theta}_{12} \\ \dot{\alpha_{L_1}} \end{pmatrix} = \begin{pmatrix} \sin\theta_1 & 0 \\ \cos\theta_1 & 0 \\ \tan\alpha_{L_1}/L_1 & 0 \\ -\frac{\tan\alpha_{L_1}}{L_1} - \frac{\sin\Delta\theta_{12}}{L_2} - \frac{M_1\cos\Delta\theta_{12}\tan\alpha_{L_1}}{L_1 L_2} & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \dot{\alpha_{L_1}} \end{pmatrix}$$

Komplexere Systeme

Vielen Dank für Ihre Aufmerksamkeit!

Bildnachweis

[A] http://object-e.net/tools/voronoi-3d-v0-1-ms