Todo list

Contents

1 Einleitung

Struktur vom Dokument erläutern

1.1 Begriffe

Definition: Eigenes,Gesamtes
M sei eine Menge von Elementen, die in zwei Teilmengen M_A und M_B zerfällt, sodass $M = M_A \cup M_B$ ist. Wir nehmen desweiteren an, dass Alice M_A kennt, aber weder M noch M_B und dass Bob M_B kennt, aber weder M noch M_A. Dann bezeichnen wir:

- M als **gesamtes** Wissen
- M_A als das **eigene** Wissen von Alice
- M_B als das **eigene** Wissen von Bob
- M_B als das **andere** Wissen von Alice
- M_A als das **andere** Wissen von Bob

Definition: 'Gemeinsam' := "etwas, was beide anwender haben und gleich ist"

Definition: Vorwissen := "Wissen aus vorherigen Phasen"

Definition: Entscheidungsbaum

Definition: Attribut

Definition: Schaltkreis

Definition: Entstellter Schaltkreis

1.2 Annahmen

Annahme: ehrliche anwender := "handeln nach protokoll"

2 Grundlagen der Anwendung

Vision der Anwendung

2.1 Form der Benutzereingabe

Festlegen, wie die E-Mails ins Programm kommen

2.2 Interaktion der verteilten Programme

Festlegen, wie das Programm verteilt wird und die Teile kommunizieren

2.3 Phasen der Anwendung

Kurz die Einzelnen phasen der Anwendung beschreiben

3 Finden der gemeinsamen Wortliste

Einleitung, Verweisen auf Figure für gemeinsame Wortliste

Für section-Titel besseren Begriff für "Vorkomnisse der Worte in eigenen Spam/Nicht Spam E-Mails" finden

3.1 Berechnung der Vorkomnisse

Content

3.2 Sortierung der Worte nach Informationsheuristik

Content

3.3 Syncronisierung der Wortlisten

Content

4 Finden der gemeinsamen Schwellwerte

Einleitung, auf Figure für Schwellwerte verweisen

Für section-Titel besseren Begriff für "Vorkomnisse der Worte in eigenen Spam/Nicht Spam E-Mails" finden

4.1 Berechnung der Vorkomnisse

Content

4.2 Bestimmung der eigenen Schwellwerte

Content

4.3 Syncronisierung der Schwellwerte

Content

5 Diskretisieren der eigenen E-Mails

Einleitung, Figure referenzieren

Content

6 Lernen der gesamten E-Mails

verteiltes ID3 beschreiben

6.1 Yaos Protokoll

Yaos algorithmus grundlegend zusammenfassen (garbled decision table, garbled gate, garbled circuit)

Verschlüsselung für die garbled Circuits festlegen (RSA?)

1-2 Oblivious Transfer festlegen (mit RSA?)

Feststellung der benoetigten Bytezahl beschreiben

6.2 Feststellen der dominierenden Ausgabe

Schaltkreis designen: Maximum von Summen von positiven Zahlensequenzen

6.3 Feststellen ob Ausgabe eindeutig

Schaltkreis designen: Gleichheit.

6.4 Das Entropien-Protokoll

Schaltkreis für x * log x -Protokoll aus dem Paper zusammenfassen

6.5 Attribut mit maximalem Informationsgewinn finden

Vorgheen zusammenfassen, Schaltkreis aus dominierender Ausgabe wiederverwenden

7 Verwenden des Klassifikators

Einleitung: Wir brauchen ein Programm, was den Klassifkator auf eine MAil oder Mails anwendet

7.1 Eingabe des Klassifikators

Anhand der Definition von Attributen und Entscheidungsbäumen beschreibungssprache fuer Entscheidungsbaum herleiten

7.2 Arbeitsweise des Klassifikators

Arbeitsweise des Klassifikators erklären

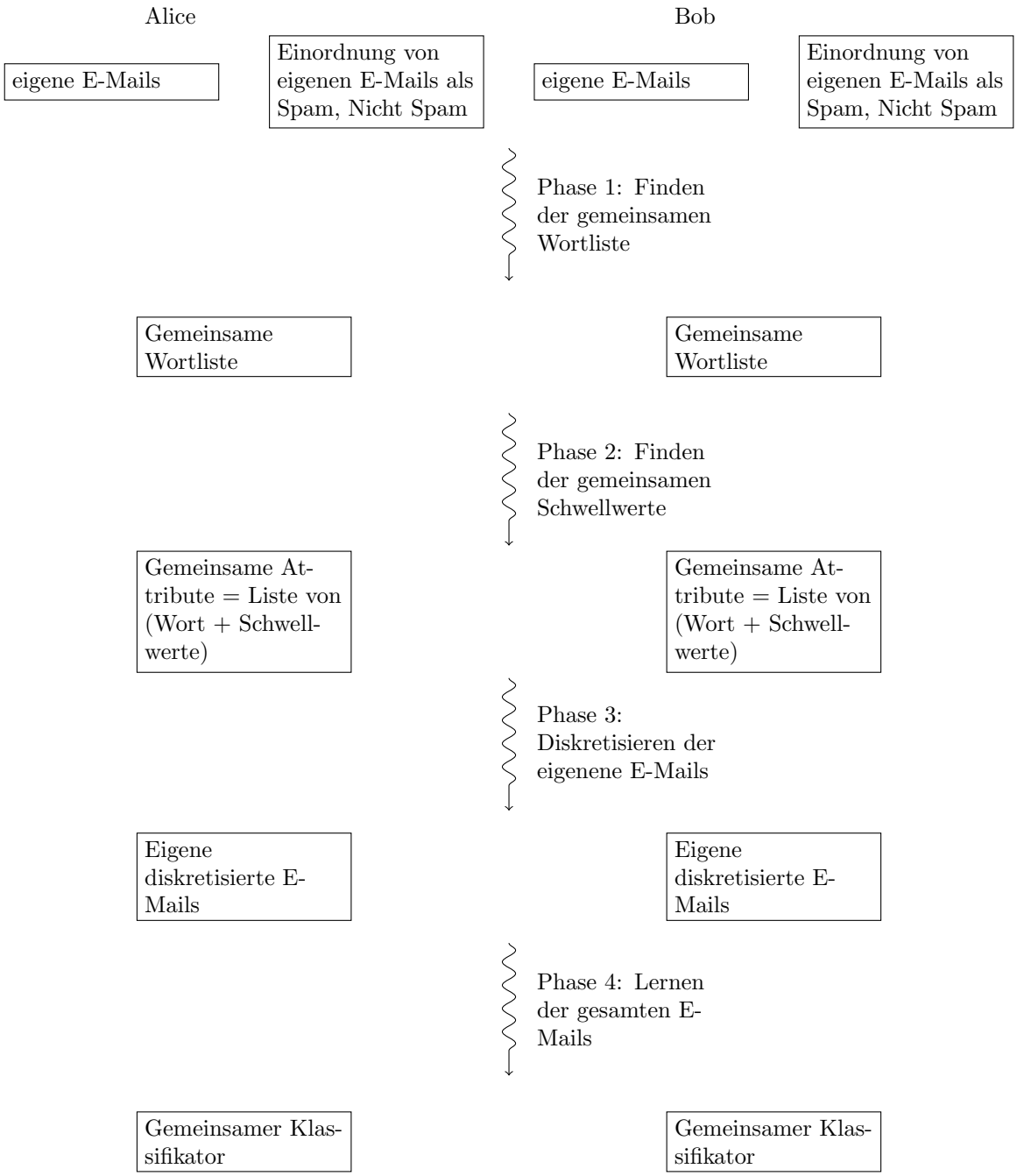


Figure 1: Phasen der Anwendung

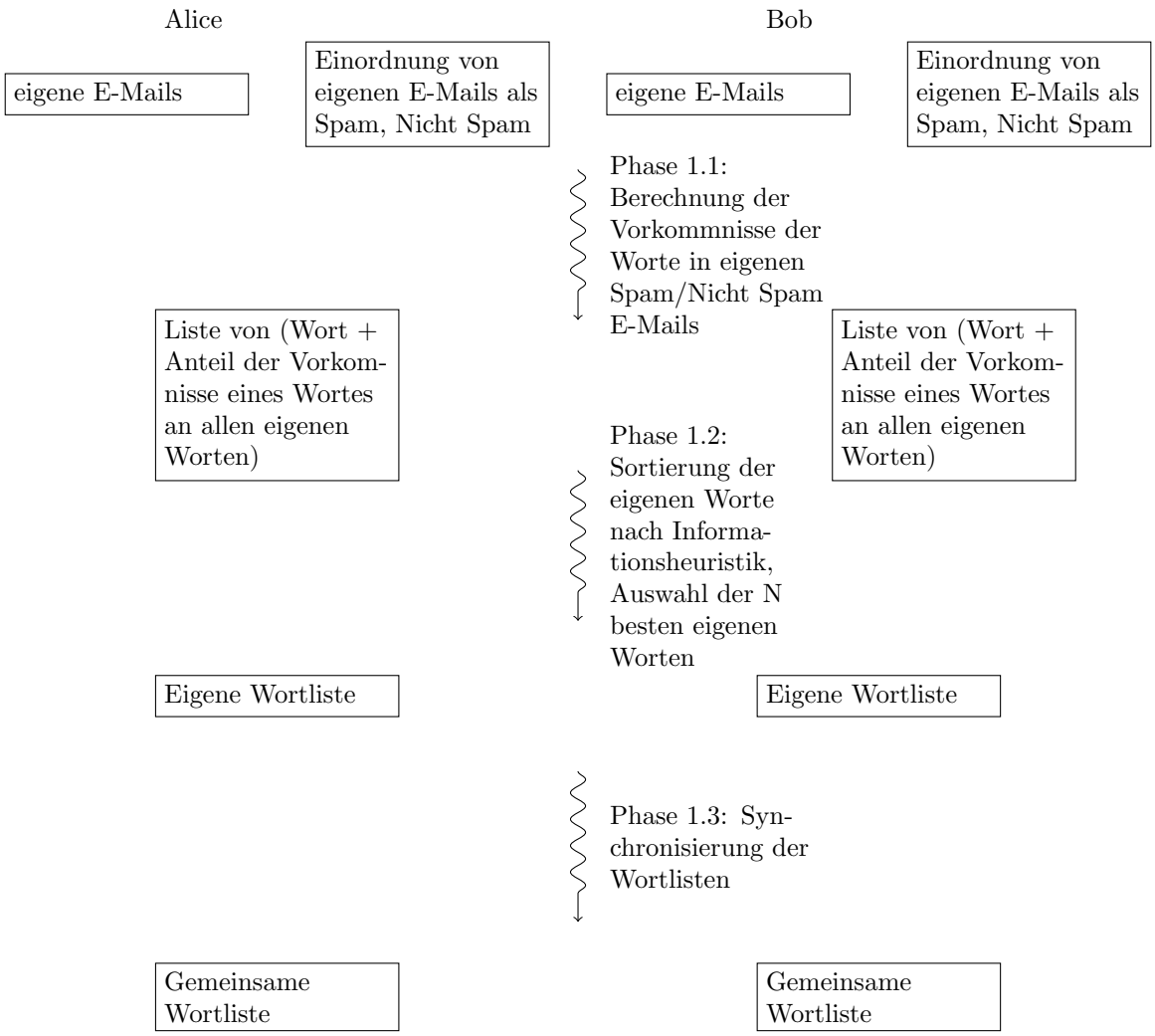
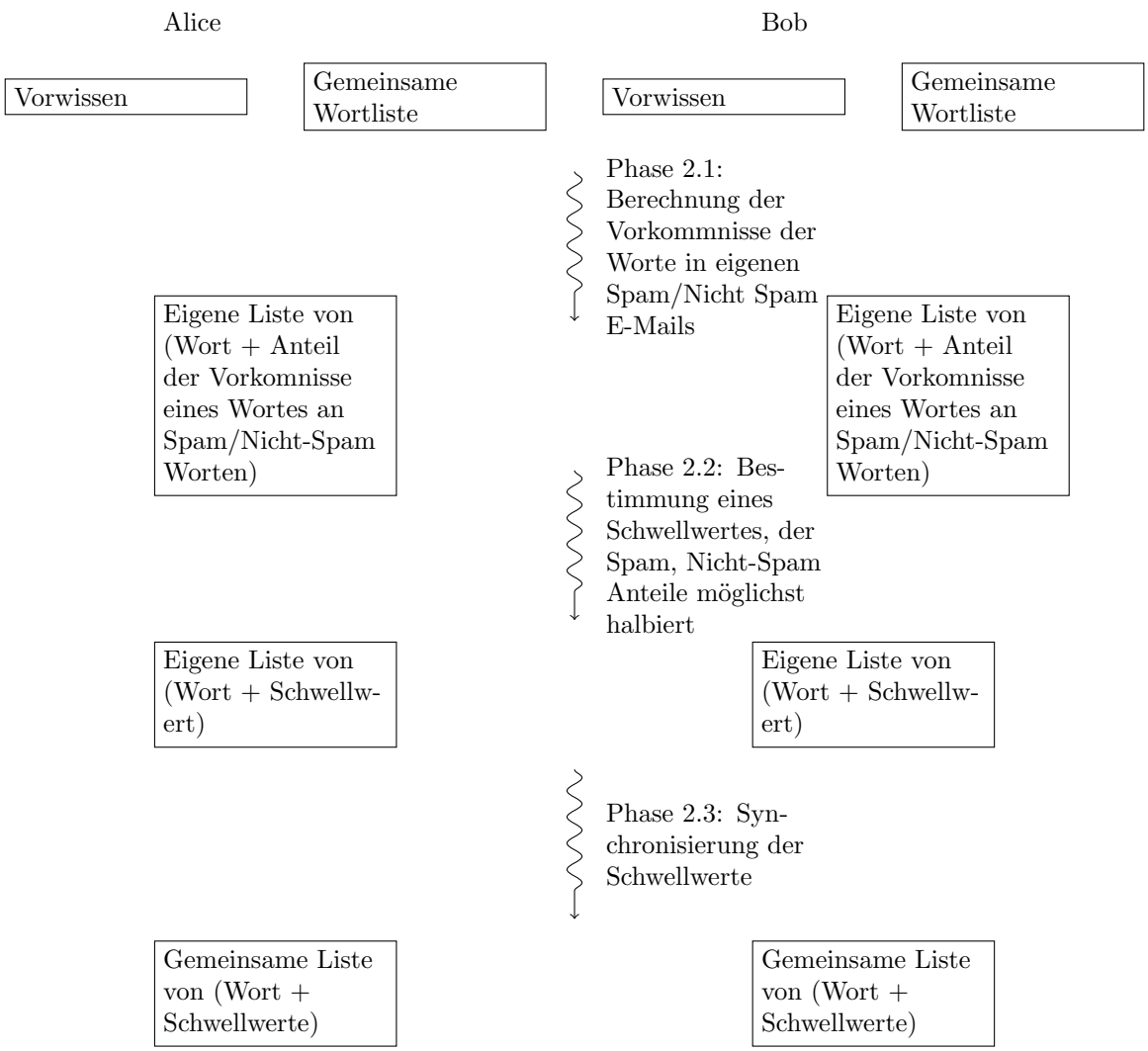
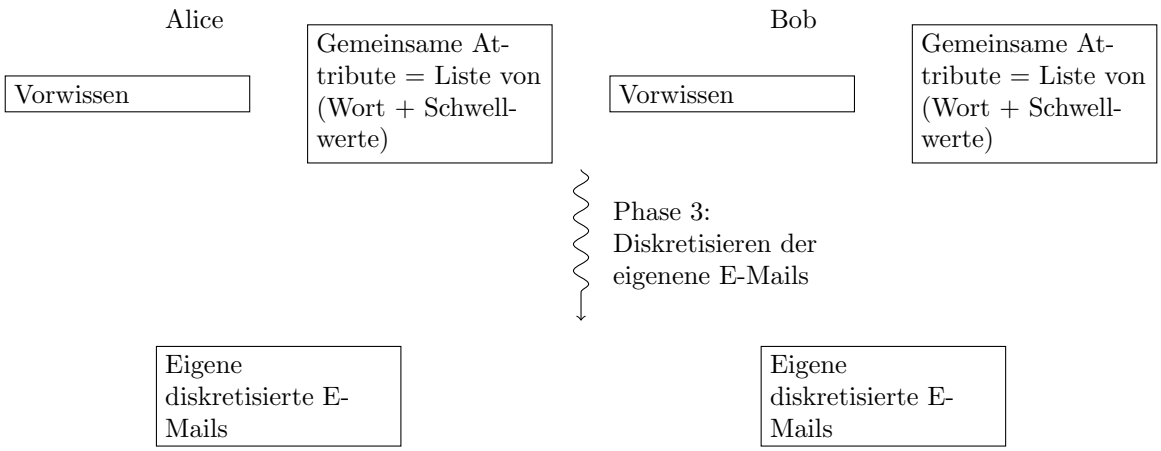


Figure 2: Schritte zum Berechnen der gemeinsamen Wortliste


Alice
Bob
Vorwissen
Gemeinsame Wortliste
Vorwissen
Gemeinsame Wortliste
Phase 2.1: Berechnung der Vorkommnisse der Worte in eigenen Spam/Nicht Spam E-Mails
Eigene Liste von (Wort + Anteil der Vorkomnisse eines Wortes an Spam/Nicht-Spam Worten)
Eigene Liste von (Wort + Anteil der Vorkomnisse eines Wortes an Spam/Nicht-Spam Worten)
Phase 2.2: Bestimmung eines Schwellwertes, der Spam, Nicht-Spam Anteile möglichst halbiert
Eigene Liste von (Wort + Schwellwert)
Eigene Liste von (Wort + Schwellwert)
Phase 2.3: Synchronisierung der Schwellwerte
Gemeinsame Liste von (Wort + Schwellwerte)
Gemeinsame Liste von (Wort + Schwellwerte)


Alice
Vorwissen
Gemeinsame Attribute = Liste von (Wort + Schwellwerte)
Bob
Vorwissen
Gemeinsame Attribute = Liste von (Wort + Schwellwerte)
Phase 3: Diskretisieren der eigenene E-Mails
Eigene diskretisierte E-Mails
Eigene diskretisierte E-Mails

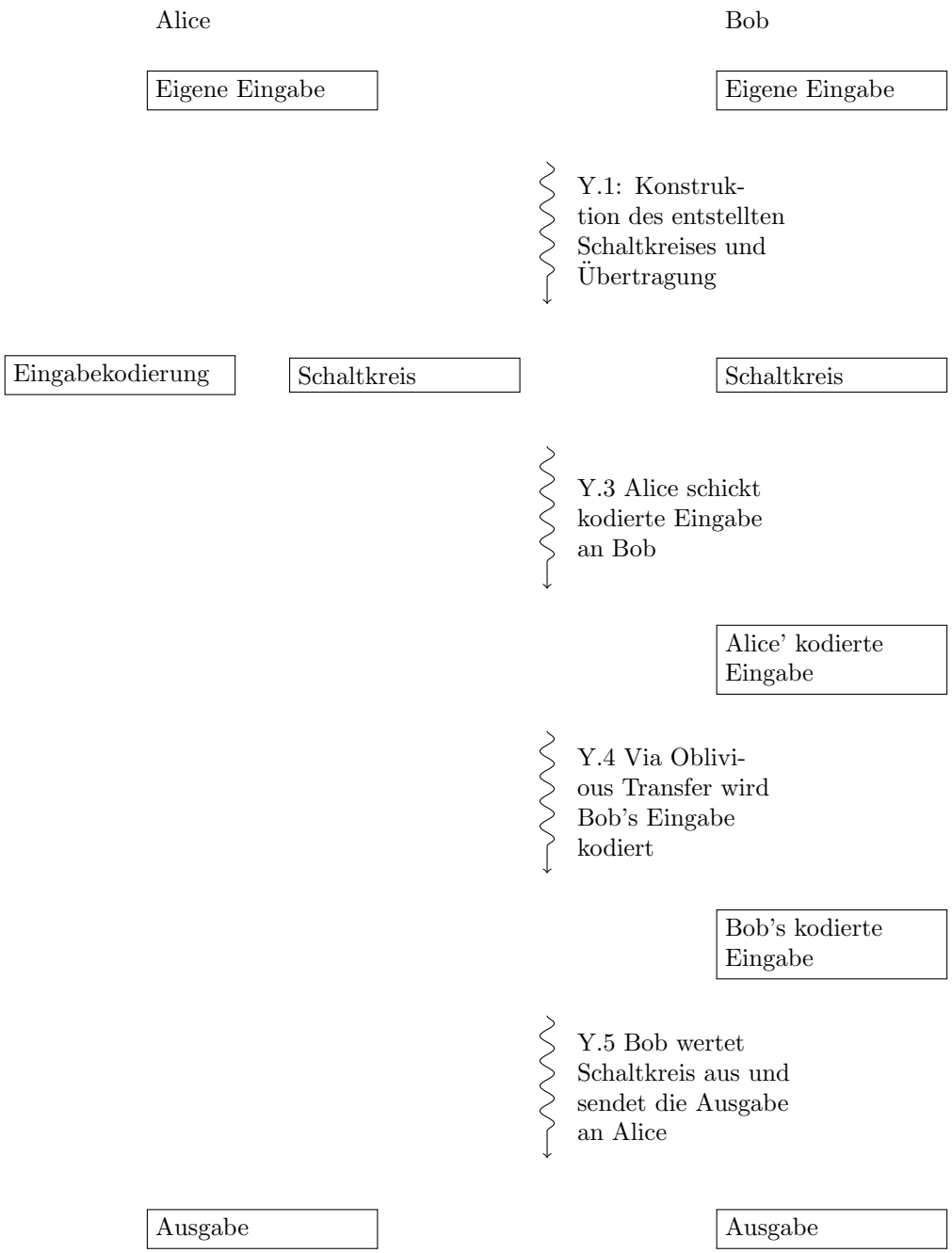


Figure 3: Yaos Algorithmus

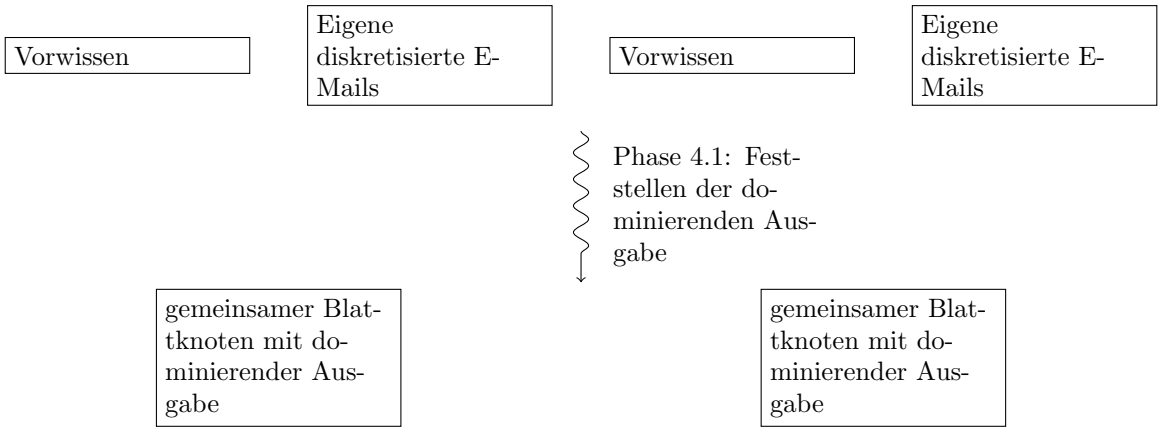


Figure 4: ID3-Algorithmus, Fall 1: Keine Attribute mehr vorhanden

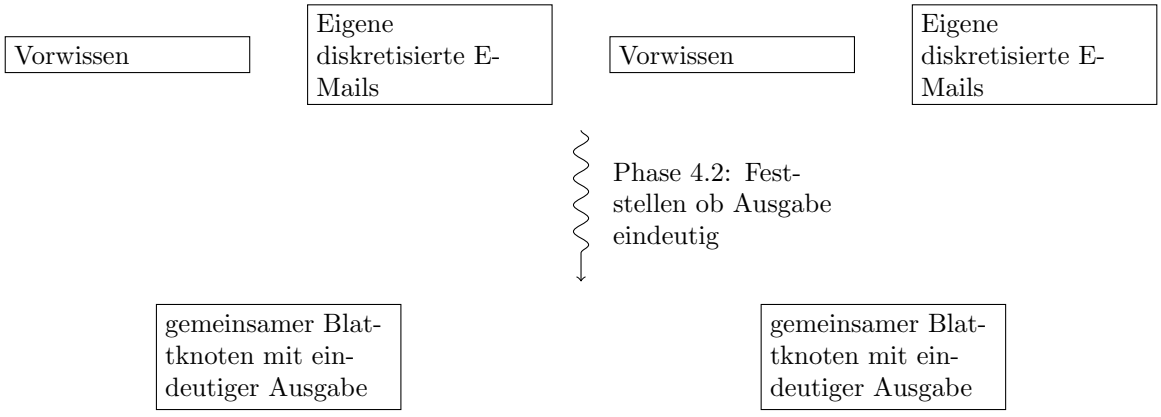


Figure 5: ID3-Algorithmus, Fall 2: Ausgabe eindeutig

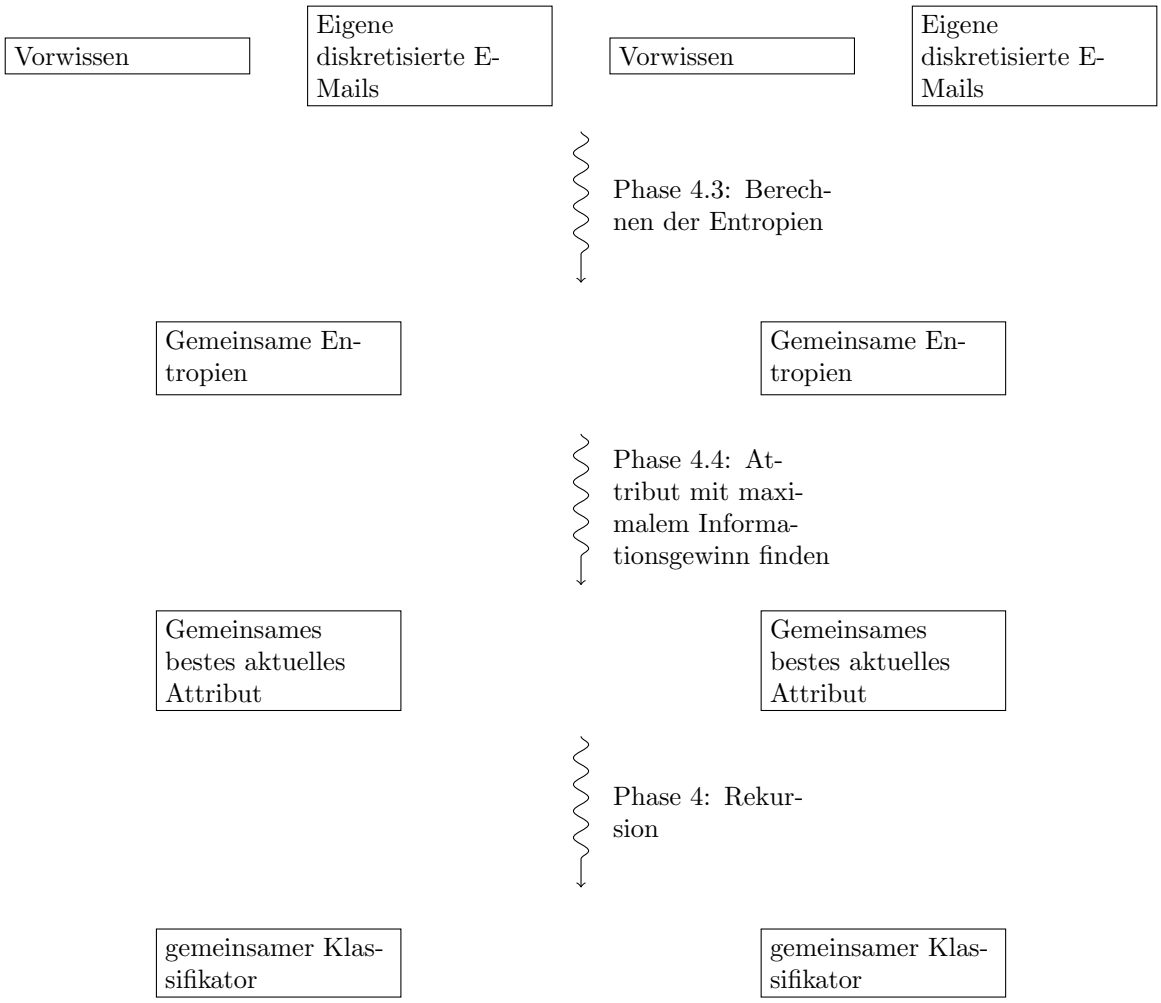


Figure 6: ID3-Algorithmus, Fall 3: Erzeugung eines Astes