JOHANNES GUTENBERG UNIVERSITÄT MAINZ

JG|U

TOP ML
Trading Off Non-Functional Properties of Machine Learning

JG|U UNIVERSITÄTSmedizin.
Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) MAINZ

Datenschutzaspekte bei gelernten Wissensbasen im Kontext von synthetischen und medizinischen Daten

Xenia Heilmann[1], Valentin Henkys[1], Daan Apeldoorn[2], Konstantin Strauch[2], Bertil Schmidt[1], Timm Lilienthal[2], Torsten Panholzer[2]

[1]Johannes Gutenberg-Universität Mainz, Institut für Informatik

[2]Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI)
Universitätsmedizin der Johannes Gutenberg-Universität Mainz

29.10.2024

Datenschutzaspekte bei gelernten Wissensbasen im Kontext von synthetischen und medizinischen Daten

- **Einführung: Ausnahmetolerante hierarchische Wissensbasen (HKBs)**
- Datenschutzaspekte
- Evaluation und Ergebnisse
- Zusammenfassung und Ausblick

Ausnahmetolerante hierarchische Wissensbasen

- Ursprünge in den Bereichen „lernende Agenten“/„KI in Spielen“
  z. B. [Apeldoorn, Kern-Isberner; Commonsense 2017], [Apeldoorn, Dockhorn; IEEE Transactions on Games 2021]
- Hierarchisches Wissen basierend auf *Regeln mit Ausnahmen*; kann aus Daten gelernt werden
- Leicht verständlich, auch ohne Wissensrepräsentationsexpertise
  [Krüger, Apeldoorn, Kern-Isberner; QR 2017]
- Implementierung: InteKRator-Toolbox
  [Apeldoorn, Panholzer; GMDS 2021]

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Wissensbasen Lernen

- Datensatz:

female	overweight	smoker	therapyA	no_recovery
female	no_overweight	smoker	therapyA	no_recovery
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]

no_overweight -> recovery [0.8]

therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]

male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A …"

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) MAINZ

Inferenz [Apeldoorn, Kern-Isberner; GCAI 2016]

SUCHE

no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75] female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0] male ^ no_overweight ^ smoker -> recovery [1.0]

INFERENZ

Gegeben diese Informationen und gemäß dem Datensatz liegt die Heilungschance bei 0.25!

Warum?

*Das Ergebnis konnte von der Information **Therapie A und Raucher** inferiert werden, welche in **75%** der Fälle zu keiner Heilung führt.*

Datenschutzaspekte bei gelernten Wissensbasen im Kontext von synthetischen und medizinischen Daten

- Einführung: Ausnahmetolerante hierarchische Wissensbasen (HKBs)
- **Datenschutzaspekte**
- Evaluation und Ergebnisse
- Zusammenfassung und Ausblick

Datenschutzaspekte

- Wichtig im medizinischen Bereich, besonders für *Patientendaten*
- Wenn eine Wissensbasis aus Daten gelernt wurde:
  Inwiefern lassen sich die Originaldaten (z. B. einzelne Patienten) wiederherstellen?
- Intuition:
  Größere und *schlechter generalisierende* Wissensbasen mit *vielen Ausnahmen* anfälliger für *Datenschutzverletzungen*

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Wiederherstellen der Originaldaten

- Datensatz:

female	overweight	smoker	therapyA	no_recovery
female	no_overweight	smoker	therapyA	no_recovery
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]

no_overweight -> recovery [0.8]

therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]

male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A …“

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) MAINZ

Wiederherstellen der Originaldaten

- Datensatz:

female	overweight	smoker	therapyA	no_recovery
female	no_overweight	smoker	therapyA	no_recovery
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery

!

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A …“

Exception tracing

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Exkurs: *k*-Anonymität [Sweeney; Int. J. Uncertain. Fuzziness Knowl. Based Syst. 2002]

- Datensatz:

female	overweight	smoker	therapyA	no_recovery
female	no_overweight	smoker	therapyA	no_recovery
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery

!

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A …“

Exception tracing

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Exkurs: *k*-Anonymität [Sweeney; Int. J. Uncertain. Fuzziness Knowl. Based Syst. 2002]

- Datensatz:

...				
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery
male	no_overweight	smoker	therapyA	recovery

2-anonym

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]

no_overweight -> recovery [0.8]

therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]

male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A ...“

Exception tracing

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) MAINZ

Exkurs: *k*-Anonymität [Sweeney; Int. J. Uncertain. Fuzziness Knowl. Based Syst. 2002]

- Datensatz:

...				
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery
male	no_overweight	smoker	therapyA	recovery
male	no_overweight	smoker	therapyA	recovery

3-anonym

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A ...“

Exception tracing

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Exkurs: *k*-Anonymität [Sweeney; Int. J. Uncertain. Fuzziness Knowl. Based Syst. 2002]

- Datensatz:

...				
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery
male	no_overweight	smoker	therapyA	recovery
male	no_overweight	smoker	therapyA	recovery
male	no_overweight	smoker	therapyA	recovery

4-anonym

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A ...“

Exception tracing

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) MAINZ

Bereinigungsalgorithmus (für $k := K$)

- Datensatz:

female	overweight	smoker	therapyA	no_recovery
female	no_overweight	smoker	therapyA	no_recovery
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery

!

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0]
male ^ no_overweight ^ smoker -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut,
außer wenn nicht übergewichtig,
außer Raucher mit Therapie A
...“

Spezifischste Regel(n) entfernen!

TOP ML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Bereinigungsalgorithmus (für $k := K$)

- Datensatz:

female	overweight	smoker	therapyA	no_recovery
female	no_overweight	smoker	therapyA	no_recovery
female	overweight	smoker	therapyB	no_recovery
female	no_overweight	non-smoker	therapyB	recovery
male	overweight	smoker	therapyA	no_recovery
male	no_overweight	non-smoker	therapyA	recovery
male	overweight	non-smoker	therapyB	no_recovery
male	no_overweight	smoker	therapyB	recovery
male	no_overweight	smoker	therapyA	recovery

- Kompakte Wissensbasis als *Regeln mit Ausnahmen*:

```
no_recovery [0.556]
no_overweight -> recovery [0.8]
therapyA ^ smoker -> no_recovery [0.75]
female ^ smoker -> no_recovery [1.0]
male ^ therapyA ^ no_overweight -> recovery [1.0]
```

„Allgemein genesen Patienten nicht gut, außer wenn nicht übergewichtig, außer Raucher mit Therapie A …“

Bei Bedarf für weitere Regeln wiederholen...

Datenschutzaspekte bei gelernten Wissensbasen im Kontext von synthetischen und medizinischen Daten

- Einführung: Ausnahmetolerante hierarchische Wissensbasen (HKBs)
- Datenschutzaspekte
- **Evaluation und Ergebnisse**
- Zusammenfassung und Ausblick

Evaluationsdaten

- Synthetische Daten
- Zwei öffentlich verfügbare Realdatensätze:
  - *Breast Cancer* (9 Features, zweiwertiger Outcome)
    [Zwitter, Soklic 1988; UCI Machine Learning Repository]
  - *National Poll on Healthy Aging (NPHA) Doctor Visits* (14 Features, dreiwertiger Outcome)
    [National Poll on Healthy Aging (NPHA) 2023; UCI Machine Learning Repository]

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Experimente mit synthetischen Daten

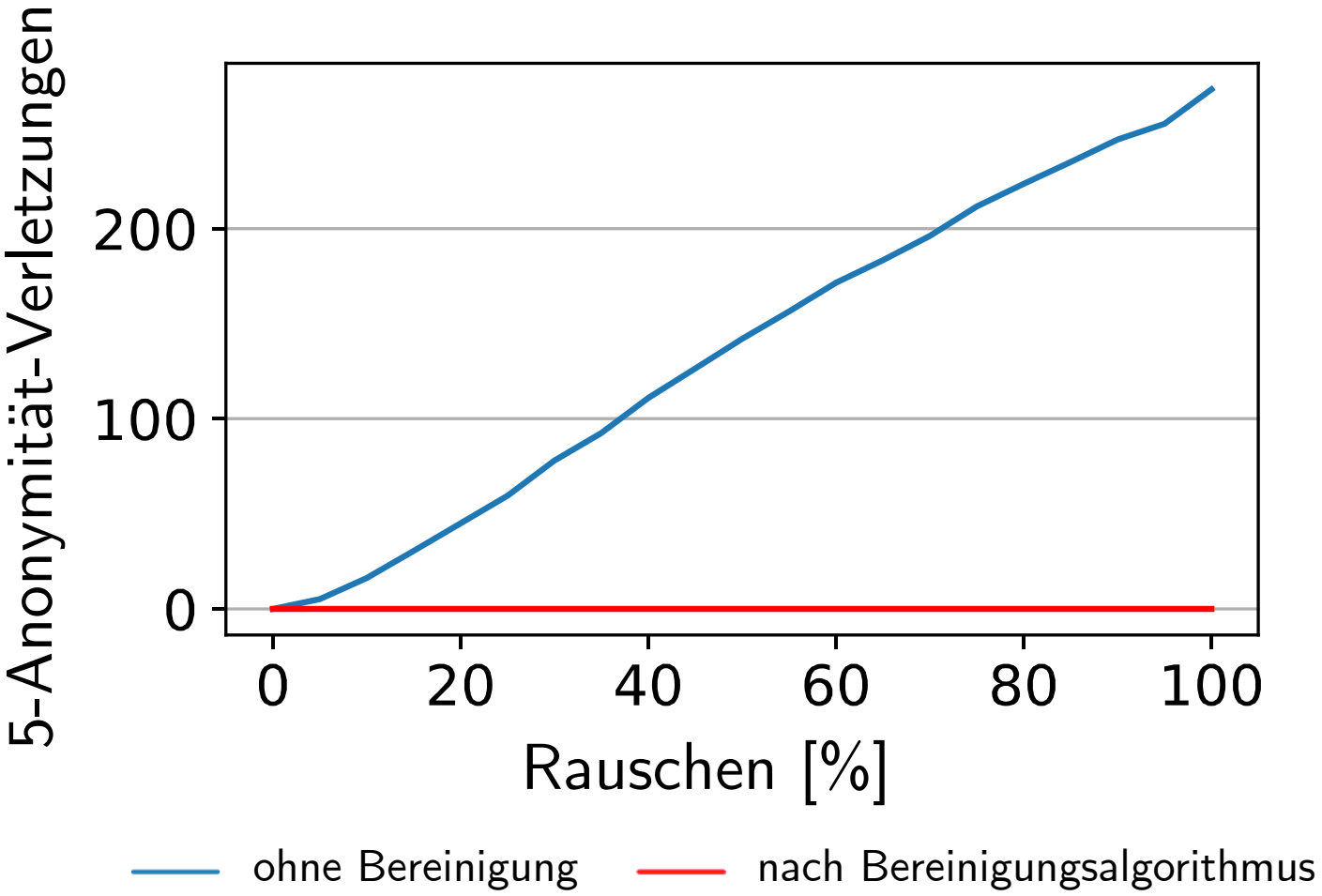
- 100 Datensätze moderater Größe, 2-wertige Features, 10^3 Zeilen
- Erhöhung Rauschanteil in 5% Schritten ($\hat{=} 2000$ Datensätzen)

(1) Messen der *Anzahl Verletzungen von k-Anonymität*

(2) Messen der *Inferenzqualität* (im Vergleich zur *k-Anonymisierung als Vorverarbeitung* der Daten vgl. [LeFevre et al.; ICDE 2006])

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI) MAINZ

Verletzungen bei synthetischen Daten ($k := 5$)

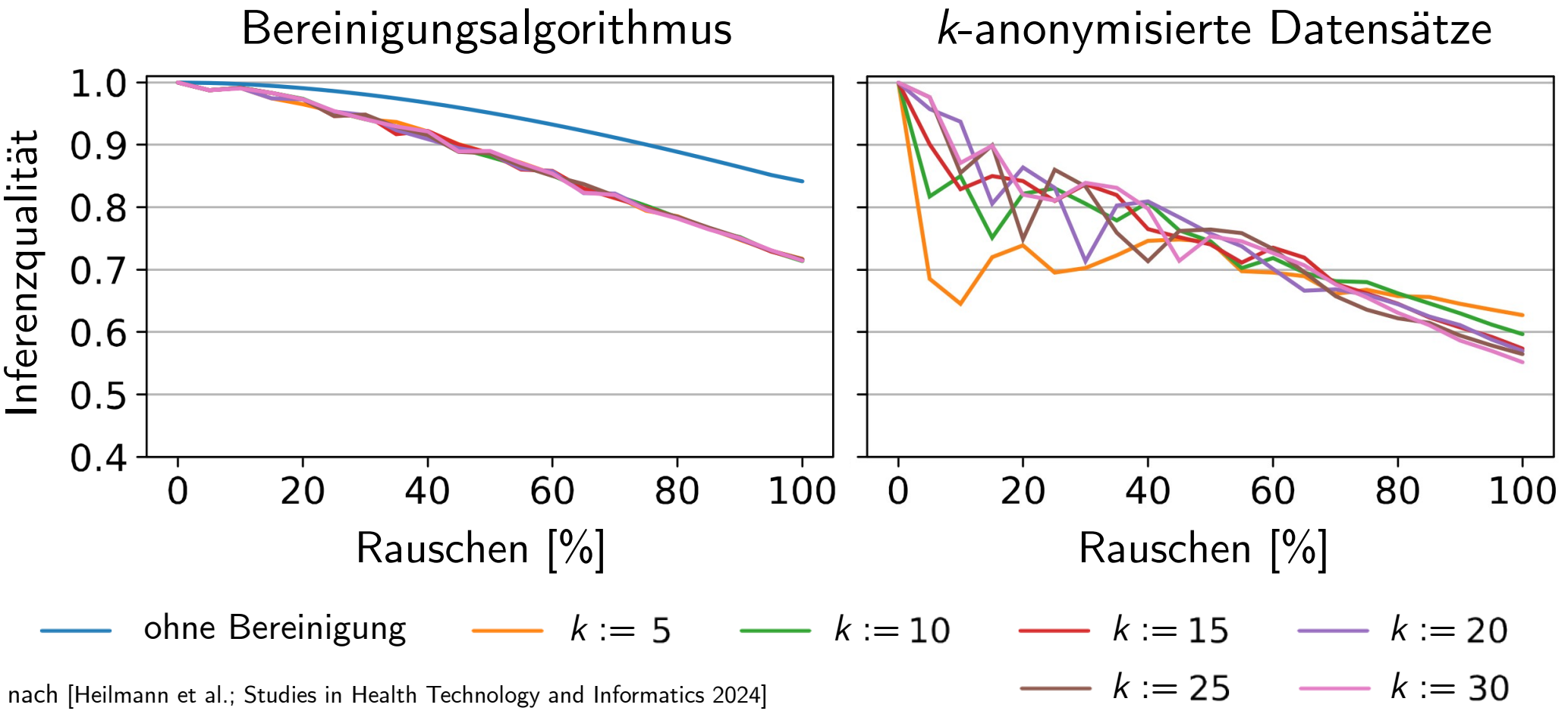


vereinfachte Darstellung nach [Heilmann et al.; Studies in Health Technolgy and Informatics 2024]

→ Bereinigungsalgorithmus kann Anonymität erzeugen

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Inferenzqualität bei synthetischen Daten

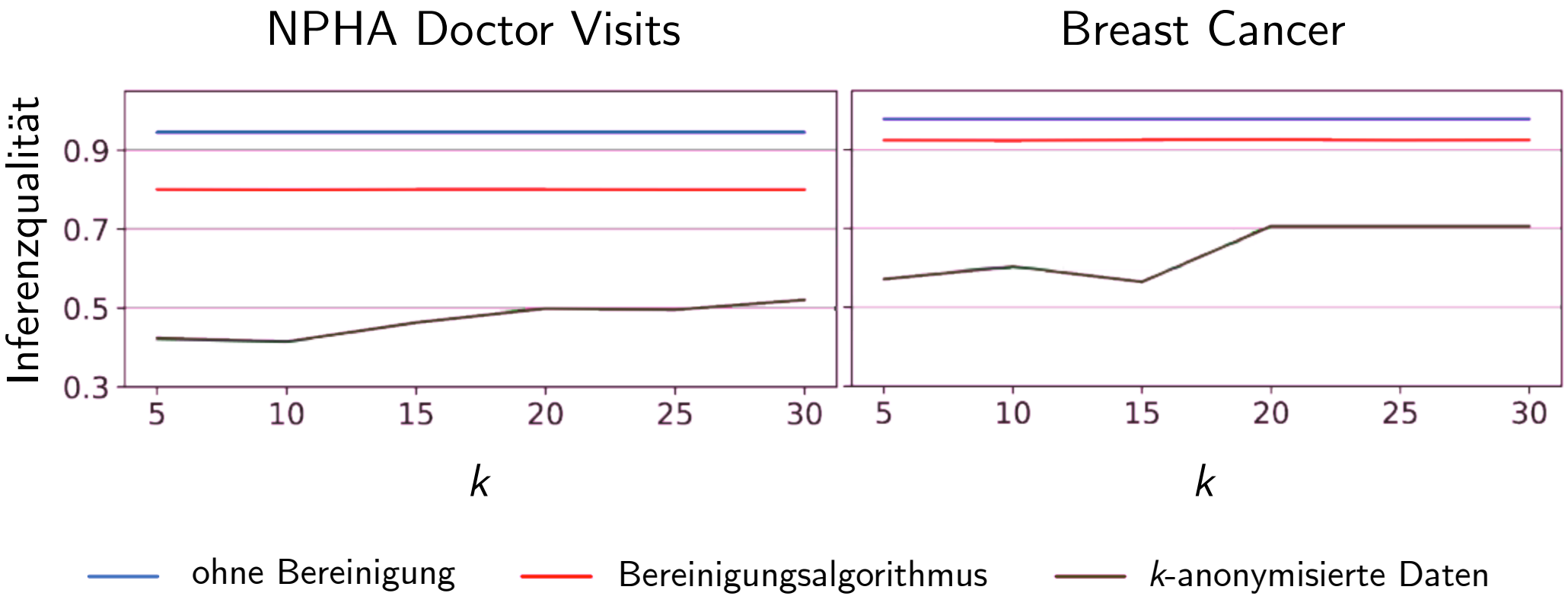


nach [Heilmann et al.; Studies in Health Technology and Informatics 2024]

→ Geringerer Verlust der Inferenzqualität, stabiler gegenüber k

TOPML Trading Off Non-Functional Properties of Machine Learning
JG|U UNIVERSITÄTSmedizin. Institut für Medizinische Biometrie, MAINZ Epidemiologie und Informatik (IMBEI)

Inferenzqualität bei realen Daten



vereinfachte Darstellung nach [Heilmann et al.; Studies in Health Technology and Informatics 2024]

→ Geringerer Qualitätsverlust als k-Anonymisierung der Daten

Datenschutzaspekte bei gelernten Wissensbasen im Kontext von synthetischen und medizinischen Daten

- Einführung: Ausnahmetolerante hierarchische Wissensbasen (HKBs)
- Datenschutzaspekte
- Evaluation und Ergebnisse
- **Zusammenfassung und Ausblick**

Zusammenfassung und Ausblick

- Datenschutz spielt auch beim Lernen von Wissensbasen aus Daten eine wichtige Rolle – insbesondere in sensiblen Bereichen
- Entfernen von Regeln ermöglicht Datenschutz
- Bereinigungsalgorithmus erhält Inferenzqualität besser als andere Verfahren (z. B. *k*-Anonymisierung der Daten)
- Ausblick: Implementierung in der InteKRator-Toolbox
- Alternativer Ansatz: Erweiterung des Lernalgorithmus

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

Trading Off Non-Functional Properties of Machine Learning

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI)

Vielen Dank!

Beteiligte:

Xenia Heilmann[1], Valentin Henkys[1], Daan Apeldoorn[2], Konstantin Strauch[2], Bertil Schmidt[1], Timm Lilienthal[2], Torsten Panholzer[2]

[1]Johannes Gutenberg-Universität Mainz, Institut für Informatik

[2]Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI)
Universitätsmedizin der Johannes Gutenberg-Universität Mainz

Vortrag:

Daan Apeldoorn
daan.apeldoorn@uni-mainz.de

Medizinische Informatik
Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI)
Universitätsmedizin der Johannes Gutenberg-Universität Mainz

Paper:

erstellt mit: https://goqr.me

DOI: 10.3233/SHTI240866

Literatur und Verweise (Auswahl)

Apeldoorn, D., Dockhorn, A.: Exception-Tolerant Hierarchical Knowledge Bases for Forward Model Learning. IEEE Transactions on Games, 13(3):249–262, 2021.

Apeldoorn, D., Kern-Isberner, G.: An Agent-Based Learning Approach for Finding and Exploiting Heuristics in Unknown Environments. In: Gordon, A. S., Miller, R., Turán, G. (eds.) Proceedings of the Thirteenth International Symposium on Commonsense Reasoning, London, UK, November 6-8, 2017. CEUR Workshop Proceedings (Vol-2052), Aachen, 2018.

Apeldoorn, D., Panholzer, T.: Automated Creation of Expert Systems with the InteKRator Toolbox. Studies in Health Technology and Informatics, 283:46–55, 2021.

Heilmann, X., Henkys, V., Apeldoorn, D., Strauch, K., Schmidt, B., Lilienthal, T., Panholzer, T.: Studying Privacy Aspects of Learned Knowledge Bases in the Context of Synthetic and Medical Data. Studies in Health Technology and Informatics, 317:261–269, 2024.

Krüger, C., Apeldoorn, D., Kern-Isberner, G.: Comparing Answer Set Programming and Hierarchical Knowledge Bases Regarding Comprehensibility and Reasoning Efficiency in the Context of Agents. In: Proceedings of the 30th International Workshop on Qualitative Reasoning (QR 2017) at International Joint Conference on Artificial Intelligence (IJCAI 2017) in Melbourne, Australia. Northwestern University, Evanston, Illinois, 2017.

LeFevre K., DeWitt D. J., Ramakrishnan R.: Mondrian Multidimensional K-Anonymity. In: 22nd International Conference on Data Engineering (ICDE'06), p. 25–25. IEEE, Piscataway, 2006.

National Poll on Healthy Aging (NPHA) 2023. UCI Machine Learning Repository. https://doi.org/10.3886/ICPSR37305.v1, accessed on Oct 1st, 2024.

Sweeney L.: k-Anonymity: A Model for Protecting Privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems. 2002;10(5):557–570.

Zwitter M., Soklic M.: Breast Cancer 1988. UCI Machine Learning Repository. https://doi.org/10.24432/C51P4M, accessed on Oct 1st, 2024.