

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Citation: A. Sheth, M. Gaur, K. Roy, R. Venkataraman and V. Khandelwal, "Process Knowledge-Infused AI: Toward User-Level Explainability, Interpretability, and Safety," in IEEE Internet Computing, vol. 26, no. 5, pp. 76-84, 1 Sept.-Oct. 2022, doi: 10.1109/MIC.2022.3182349.

DOI: <https://doi.org/10.1109/MIC.2022.3182349>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

Process Knowledge-Infused AI: Towards User-level Explainability, Interpretability, and Safety

Amit Sheth, Manas Gaur, Kaushik Roy, Revathy Venkataraman, Vedant Khandelwal
AI Institute, University of South Carolina, Columbia, SC, USA, 29201

arXiv:2206.13349v1 [cs.AI] 9 Jun 2022

AI systems have been widely adopted across various domains in the real world. However, in high-value, sensitive, or safety-critical applications such as self-management for personalized health or food recommendation with a specific purpose (e.g., allergy-aware recipe recommendations), their adoption is unlikely. Firstly, the AI system needs to follow guidelines or well-defined processes set by experts; the data alone will not be adequate. For example, to diagnose the severity of depression, mental healthcare providers use Patient Health Questionnaire (PHQ-9). So if an AI system were to be used for diagnosis, the medical guideline implied by the PHQ-9 needs to be used. Likewise, a nutritionist’s knowledge and steps would need to be used for an AI system that guides a diabetic patient in developing a food plan. Second, the BlackBox nature typical of many current AI systems will not work; the user of an AI system will need to be able to give user-understandable explanations, explanations constructed using concepts that humans can understand and are familiar with. This is the key to eliciting confidence and trust in the AI system. For such applications, in addition to data and domain knowledge, the AI systems need to have access to and use the Process Knowledge, an ordered set of steps that the AI system needs to use or adhere to. The use of process knowledge also aids in developing an AI system that has other important features for such demanding applications, such as safety, which is critical to ensure the AI system remains within the bounds and does not cause harm to a user - something that current AI systems using Large Language Models have failed to do. This article will use two demanding applications – mental health triaging and cooking recipes for diabetes to show what process knowledge they need and how process knowledge can be modeled and then infused into AI algorithms to achieve the outlined features. We also discuss user-level explainability, how to support safety and present metrics for performance evaluation.

BENEFITS AND IMPORTANCE OF PROCESS KNOWLEDGE

Benchmarking datasets that assess the natural language understanding capabilities of large language models fall short in accelerating models to achieve user-level explainability, safety, uncertainty, and risk handling (<https://tinyurl.com/KiL-MentalHealth-NLU>) [1]. These challenges are associated with the limitations of AI in restricting its learning tasks to classification and generation, which are single shots. In

comparison, real-world applications demand an orchestrated response going through a multi-step process of learning the high-level needs of the user, then drilling down to specific needs, and subsequently yielding a structured response having a conceptual flow. For example, triaging patients in mental health requires clinical process knowledge manifested in a clinical questionnaire. Figure 1 illustrates a scenario where the agent maps user input to a sequence of yes or no questions to compile suicide risk severity. The agent can keep track of user-provided cues and ask appropriate follow-up questions through these ordered sets of questions. Upon receiving the required information to derive appropriate severity labels, the agent’s outcome can be explained to mental healthcare providers for appropriate intervention. Similar but more complex applications include using ADOS (Autism Diagnostic Observation Schedule) to evaluate children with autism or using MoCA (Montreal Cognitive Assessment) score to measure the cognitive decline in post-stroke Aphasia patients [2]. To train conversational agents for such functionality requires specialized datasets grounded in the knowledge that enables AI systems to exploit the duality of data and knowledge for human-like decision-making [3] (<https://tinyurl.com/duality-data-knowledge>). Further, to develop agents that learn from such process knowledge-integrated datasets we require interpretable and explainable learning mechanisms (<https://tinyurl.com/petrinet-workflow>). These learning mechanisms have been characterized under the umbrella of Knowledge-infused Learning.

Knowledge-infused Learning (KiL) is a class of Neuro-Symbolic AI techniques that utilize a variety of knowledge (lexical, linguistic, domain-specific, common-sense, process knowledge, and constraint-based) in different forms and abstractions into deep neural networks. It improves upon data-centric statistical learning to reduce training, reduce computing needs, and broaden coverage, resulting in improved performance, safety and model interpretation, and providing user-level explanations.

SHADES OF PROCESS KNOWLEDGE INFUSED LEARNING

KiL aligns with the third phase of DARPA to promote contextual adaptation in AI systems for user-level explanations. An AI system trained with knowledge infusion techniques

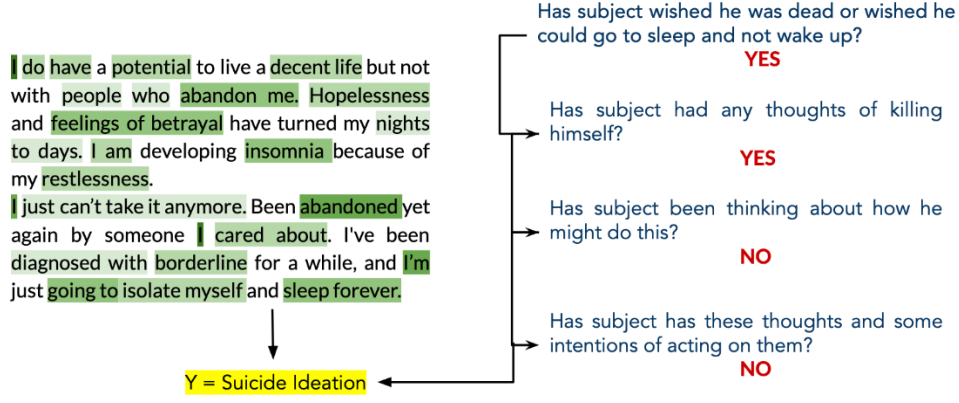


Fig. 1: An illustration of a classification task that benefits from process knowledge. Here, an AI model using a process knowledge structure would consume the user’s input, extract conceptual cues that can answer questions in process knowledge, and provide a classification label. The benefit of the process knowledge infusion in AI is the deterministic nature that it enforces in AI to achieve user-level explanations, handle uncertainty, and be safe. The figure illustrates this process in assessing suicide risk severity using a partial sequence of questions from the Columbia Suicide Severity Rating Scale (C-SSRS) (<https://tinyurl.com/Posner-CSSRS>). The highlighted text on the left is concept phrases that contribute to the yes/no in the C-SSRS questions. The graph on the right is Process knowledge in C-SSRS.

provides forms of explanations by querying, traversing, and mapping the high importance features to concepts in a knowledge graphs. Figure 2 illustrates the user-level explanations provided by an AI system infused with knowledge that highlights concept phrases in the input text. These concept phrases are used to traverse a knowledge graph, which in figure 2 is SNOMED-CT. Along with Figure 1 that explains process knowledge infusion contributing to reasonable path towards classification, Figure 2 provides additional user-level explanation. Within the three forms of knowledge-infusion under KiL (i.e., shallow, semi-deep, and deep [3]), process knowledge infusion develops a new and complementary set of methods, datasets, and evaluation methods under semi-deep and deep knowledge infusion.

Furthermore, any AI systems trained with such methods and over such datasets can also handle uncertainty and risk. They can establish the connection between the input and output, answering, “why such an outcome, given an input?”. The AI systems are context-sensitive rather than opinionated based on only the input data, i.e. a partial representation of the world. The structure and order provided by using process knowledge allows the end-users a control over the AI system. Moreover, in-process knowledge in a particular domain and for a particular task (classification or generation), an AI system with a method that makes the model adaptable to process knowledge can make the system transferable across tasks. The subsequent sections will provide a concrete definition of process knowledge and its use in understanding and controlling AI models. With a focus on natural language generation (NLG), we will conceptually describe methods for infusing process knowledge into statistical AI systems. Thereafter, we provide use-cases in the domain of mental health (continuing with Figure 1 and Figure 2) and cooking.

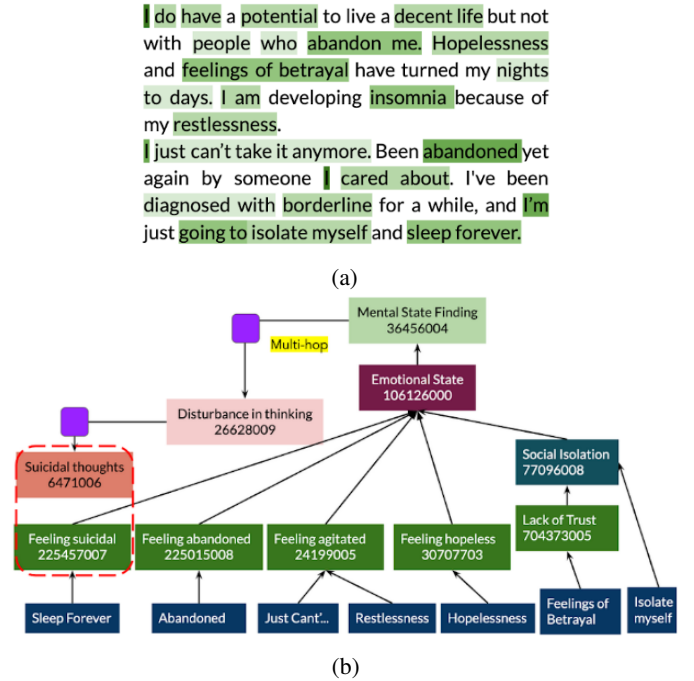


Fig. 2: An illustration of user-level explainability using the important conceptual phrases identified by a deep learning model trained using the method in (<https://tinyurl.com/contextual-classify-reddit>). Highlighted phrases in (A) are queried in SNOMED-CT, thus forming a contextual tree. The formation of this tree is stopped when a node is hit that has high similarity to either leaf nodes or one-hop parent nodes. The resulting tree is shown in (B). The numbers in the boxes are SNOMED-CT IDs.

PROCESS KNOWLEDGE AND ITS INFUSION INTO STATISTICAL AI

Process knowledge is an ordered set of information that maps to evidence-based guidelines or categories of conceptual understanding to experts in a domain. For instance, The American Academy of Family Physicians (AAFP) develops clinical practice guidelines (CPGs) that serve as a framework for clinical decisions and supporting best practices. CPG allows systematic assessment to optimize patient care. On the other hand, U.S. Departments of Agriculture (USDA) and Health and Human Services (HHS) develops Dietary Guidelines for Americans (<https://tinyurl.com/american-dietary>) that serves as an recommendation for meeting nutrient needs, promote health, and prevent disease. An AI system adapted to process knowledge can handle uncertainty in prediction, and the predicted outcomes are safe and user-level explainable. Further, an AI system can consider process knowledge as meta-information to capture the sequential context necessary for carrying out a structured conversation. Also, it allows the developer of the AI system to probe the internal decision-making of AI systems using application-specific guidelines or specifications that inform the synchrony between the end-users thought process and the model's functioning.

This unique form of knowledge differs from other forms of knowledge in the following manner: (a) knowledge graph: it is structured but not ordered. Knowledge graphs can support context capture but cannot enforce conceptual flow (<https://tinyurl.com/KI-summarization>). (b) Semantic lexicons: this is a flattened form of knowledge graph that makes deep language models context-sensitive and add constraints but cannot enforce conceptual flow [4]. (c) Ontologies are curated schematic forms of knowledge graphs with classes, instances, and constraints. Thus, ontologies can provide stricter control over context and constraints. If defined, an ontology can enforce order in question generation using deep language models [5]. Process knowledge is represented differently for different applications. For instance, to assess the severity of suicide risk, the process knowledge used is C-SSRS, which is similar to a flow chart. On the other hand, the GAD-7-based process knowledge is used to assess anxiety severity which has a flattened structure (see Figure 3). DASH Diet based process knowledge can be used to assess the dietary intake of hypertension patients and also recommend meals. These characteristic properties of process knowledge and its infusion into statistical AI would yield a new class of neuro-symbolic algorithms that would drive the question:

What if we could use the annotator's labels and the process or guidelines used to label them and explicitly control the learning of a model to recover the guideline or process (instead of implicitly).

Such an algorithm would, by design, be explainable and emulate the human model of similarity between data points. For the task of classification, a process knowledge-infused AI system would solicit the use of interpretable machine learning algorithms (e.g., Decision Trees, Random Forest)

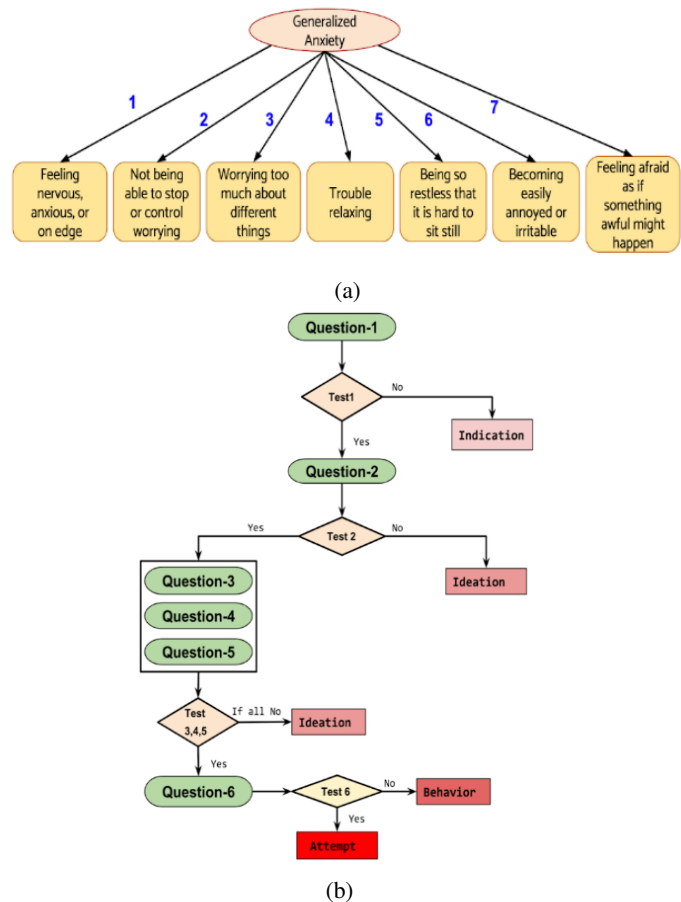


Fig. 3: Illustration of process knowledge for different purposes.

that can enforce structure in decision making over traditional deep language model-based classification (<https://tinyurl.com/PK-iL-suicide>).

In NLG, the biggest concern with deep generative language models is that they hallucinate when either asking questions or providing responses in a conversational setting. Along with the issue of hallucination, there have been extensive study about the inappropriate and unsafe risk behaviors of language models (<https://tinyurl.com/LaMDA-dialog>). Efforts to pair these language models with passage retrievers and rankers have been proposed to control incoherent, irrelevant, and factually incorrect responses and questions; however, the order, like the one defined in process knowledge, is far from being realized [6]. Such process knowledge-based NLG is even more crucial in the field of healthcare NLP, where each response from the agent can have severe consequences. These concerns are further discussed with the help of two use cases: Mental Health and Food Domain.

MENTAL HEALTH USE-CASE

AI has contributed to the domains of drug research, customized medicine, and patient care monitoring and has the potential to aid physicians in making better diagnoses. However, when AI is used in health care, various dangers and problems might arise at the individual, macro, and technological levels (e.g.,

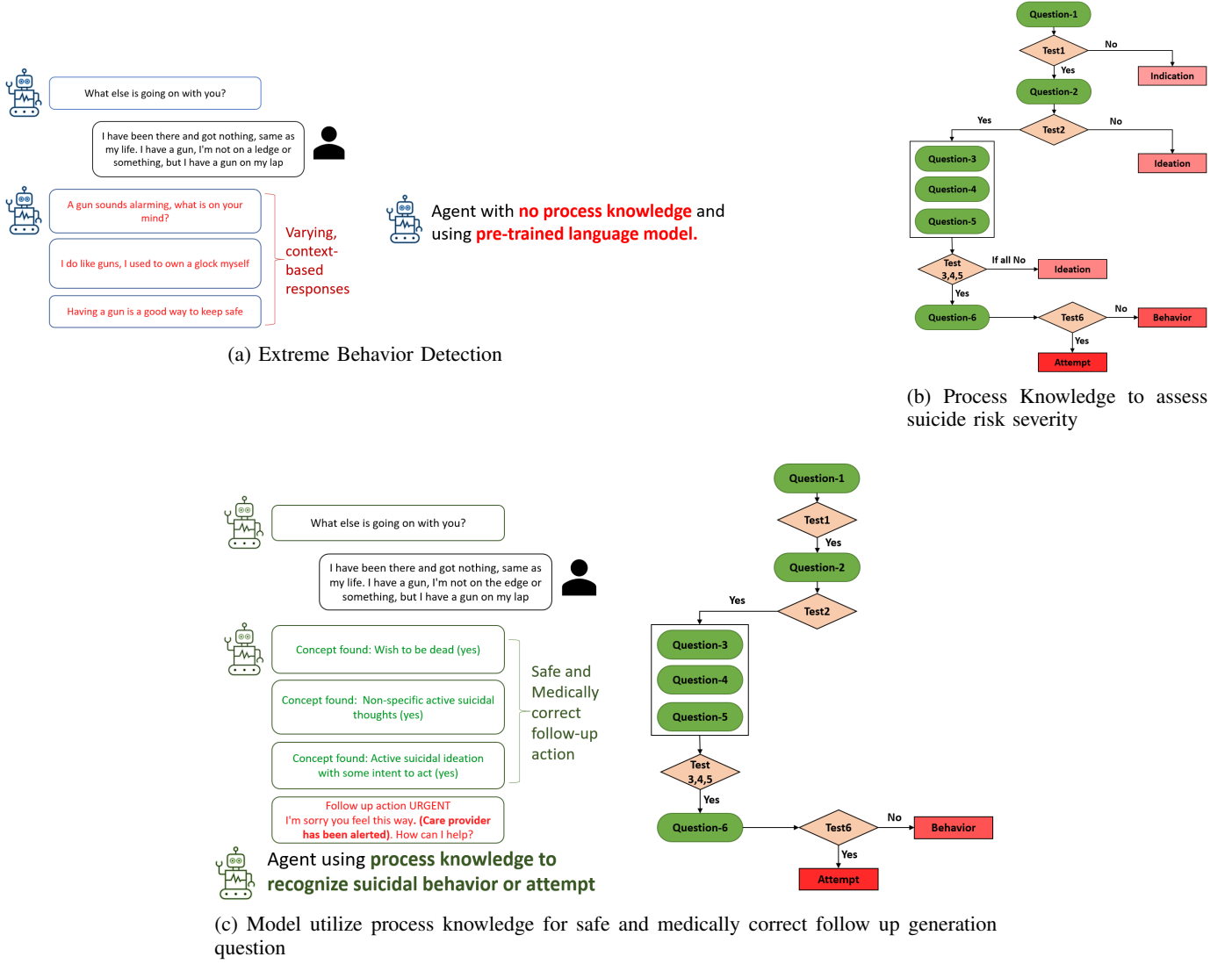


Fig. 4: An illustration of safety in conversational artificial intelligence. It explains why process knowledge is needed to avoid unsafe conversations and make models interpretable and explainable.

awareness, education, trust), as well as at the macro-level (e.g., legislation and rules, risk of accidents due to AI faults) (e.g., usability, performance, data privacy, and security). In the context of mental healthcare, conversational agents are prone to unsafe generations that can harm the user or engage in a conversation involving escalation in the severity of medical conditions.

Figure 4 illustrates a pipeline wherein (A) the deep statistical language model pre-trained on open domain corpus when tasked to converse with a user in a mental healthcare setting generates questions that it sees online. (B) Such questions are not what a mental healthcare provider would ask. If we utilize a clinical guideline, in this case, C-SSRS, the model can measure the safety of the generated question before asking. (C) Figure 4 shows a process over the detailed process knowledge that an AI agent followed to control its question generation and ask medically correct questions. A recent study from Roy et al. details this approach using C-SSRS, and Gupta et al. detail this approach using GAD-7 and PHQ-9, which are clinical

guidelines to check whether the user is a patient of an anxiety disorder (GAD-7) or clinical depression (PHQ-9) [7], [8].

PROCESS KNOWLEDGE AS CONSTRAINTS

Some more ways in which process knowledge can be infused to add constraints and improve NLG of the current AI methods are::

- Textual Entailment Constraints (TEC) is a directional relationship between sentences in a response or questions. If the two sentences share semantic relations and logically agree, they are entailed. If the two sentences are synonymous based on the entities they contain, they are neutral. If the second sentence refutes the information in the first sentence, they are contradictory. Such constraints are manifestations of process knowledge in clinical practice. In machine-understandable form, we can model them as Rules containing Tags and Rank (see Figure 5).

- Rules (Tag and Rank): These rules can help structure the question generation process, which is random and unsafe in current state-of-the-art NLG models (<https://tinyurl.com/adaptive-education>). For instance, if the conditional probability function within an AI model, defined as $P(\hat{Q}_{k+1}|\hat{Q}_k)$ is augmented with a Tag containing the following labels: {Yes/No, Degree/Frequency, Causes, Treatment/Remedies} then the model can learn to follow a definite process:

- If \hat{Q}_k is Yes then \hat{Q}_{k+1} is about Degree/Frequency
- If \hat{Q}_k is Degree/Frequency then \hat{Q}_{k+1} is about Causes
- If \hat{Q}_k is Causes then \hat{Q}_{k+1} is about Treatment/Remedies
- If \hat{Q}_k is Treatment/Remedies then \hat{Q}_{k+1} ask about Information on Other Side Effects

Here, \hat{Q}_{k+1} is the next generated question given \hat{Q}_k , a previous generated and accepted question. Further utility of constraints-based process knowledge infusion in AI is detailed in another application involving food recipe recommendation, wherein the constraints are defined based on allergens.

FOOD DOMAIN USE-CASE

A conversational system to manage diet can help patients in various applications such as hypertension and diabetes [9]. In most of the scenarios the interactions between user and system involve factual queries (e.g., Can you order a falafel for me? What are the sides offered with falafel? etc.). However, the challenge lies in how recommendations can be adapted to user preferences and context. It is still an open question [10]. Further, how can recommendations be provided when users do not ask factual questions (e.g., Can you suggest some food that helps me control my calorie intake? I want to lose weight. What should I eat for lunch?). In case of Hypertension, patients need a nudge to switch towards healthy food habits. A nutrition management system can aid and assist them in this process. In such a scenario, when a user asks the following question to an agent: “Can you recommend dishes that are calorie efficient?” if the agent is augmented with the internet, it would accurately respond to the following related questions (or people-also-ask questions) : (a) “Are restaurants required to put calories on menus,” (b) “Are calorie recommendations accurate,” (c) “Should I eat less than my recommended calories?”, and (d) “What food can you recommend?”. Moreover, top-2 searches on google for the user query are (a) Cut lots of calories and (b) How to lose weight eating more food, which are not relevant to the user query. There are two fundamental problems here: (a) The AI system behind these recommendations is confused about whether “calorie efficiency” is positive or negative. (b) The AI system fails to bridge the gap between dishes and calorie efficiency. Furthermore, a response to such a question is dependent on the time of the day: breakfast, lunch, or dinner. A process knowledge-based conversational agent would generate the following information-seeking questions: (a) Do you have any preference in cuisine? (b) Do you want to know about

low-calorie food in this cuisine for breakfast/lunch/dinner? (c) Do you want me to book reservations for restaurants that have this cuisine? (d) Do you want me to save your preferences? If the answer to (b) question is no, then an alternate path in process knowledge is triggered. Here, process knowledge is the procedure for recommending and ordering food. Moreover, the agent can benefit from the 2015-2020 Dietary Guidelines for Americans to emphasize overall healthy eating patterns supported by five food groups: fruits, vegetables, grains, protein foods, and dairy (<https://tinyurl.com/Dietary-Guidelines>).

Similarly, for type-I Diabetes, patients need to monitor carbohydrate (CHO) intake for their insulin dosage, hence the source of CHO determines whether a given food item is advisable. CHO count due to the fibers present in vegetables and fruits are considered healthy, whereas CHO from added sugars, white rice, and pasta are considered unhealthy (<https://tinyurl.com/Mayo-Diabetes-plan>). Existing models advise meals based on the daily value of the CHO limit of an individual. In this case, the CHO count of a recipe derived from added sugar will be recommended by the agent if it is within the daily CHO limit of an individual. This can have severe effects on an individual’s health. By infusing the process knowledge of diabetic dietary guidelines into the learning process, the agent can learn to advise appropriate meals and generate explanations to enhance interpretability and safety (see Figure 6).

Along with above two scenarios, the nutrients content of the food change based on the adverse effects of the cooking actions on the final cooked food item such as nutrition loss or the introduction of harmful elements. To add, the dietary restrictions for each chronic disease have respective guidelines. Hence in this scenario, two kinds of process knowledge, adverse effects of cooking actions combined with ingredients and dietary guidelines for chronic conditions, are involved in generating explanations, improving interpretability and safety of food recommendation agents.

PROCESS KNOWLEDGE AS CONSTRAINTS

In addition to specific dietary guidelines for chronic conditions, cooking actions produce adverse effects. For example, the ingredients for potato fries involve potatoes, oil, salt, pepper, and other seasonings. These are advisable ingredients as per dietary guidelines for diabetes. However, the cooking action is deep-frying which produces trans-unsaturated fatty acids. The trans-unsaturated fatty acids are not advisable for any chronic diseases and the general population as well (<https://tinyurl.com/trans-fats>, <https://tinyurl.com/trans-fat-cholesterol>).

Similarly, grilling a slice of meat can introduce carcinogenic agents [11] due to the animal fat dripping onto direct heat. However, grilling vegetables and fruits do not produce carcinogenic agents (<https://tinyurl.com/healthy-grill>). The process knowledge of cooking actions can aid the agent in learning general adverse effects due to specific combinations of cooking actions and ingredients. This process knowledge can aid the agent in learning to nudge any user towards healthy eating habits irrespective of the dietary guidelines for various chronic

metric to judge the model’s stability in light of agreement and disagreement between the annotators, a notion of uncertainty and safety. It is composed of two components: (a) Penalty: A ratio of the count of misclassified samples over the count of those samples where the annotators disagree with each other. (b) Benefit: A ratio of the count of samples where the model’s predicted label agrees with some annotators (ignoring the disagreement between them) over the total number of annotators. Such a metric is efficient for controlling unsafe predictions as opposed to using statistical loss functions that quantify uncertainty in predictions and overwhelm the experts in the loop with re-annotations [14].

- (c) *Semantic Relations and Logical Agreement Measures*: These are trained metrics constructed using the RoBERTa model, a deep language model trained independently on sentence similarity and natural language inference GLUE tasks. These metrics have been introduced in a recent study by Gaur et al. that unites meta-information-guided passage retrievers and TEC for inducing logical ordering in the generations and preventing retrieval-augmented language models from hallucinations [15]. Semantic Relation is a metric that counts the number of generations semantically similar to a user query over the total number of generations. The logical agreement score records the count when the current generated question entails a previously generated question. The score takes the sum of such counts and divides them by the number of generations.

SUMMARY AND FUTURE DIRECTIONS

Real-world interactions between the users are not a single shot activity but rather a chain of exchanges involving procedural questions and responses; at a macroscopic level and the microscopic level, it comprises entities and actions that keep changing during a task-oriented conversation. This phenomenon can be well understood and controlled through a process of knowledge that represents a human’s mental model of conversation. In this article, through example use-cases in mental healthcare and food, we explained the notion of process knowledge that naturally concerns consistency, explainability, and interpretability in AI’s decision-making process. To the best of our knowledge, this article projects its role in pushing statistical AI to be safe, less uncertain, and risky in its classification and natural language generation tasks. With process knowledge, the AI model can support reasoning, which is essential to develop trust in stakeholders using the application in various downstream tasks. We showed various existing process knowledge and the methods that data-driven AI models can use. As a future direction, we envision the utility of process knowledge in personalization which is essential in developing interventional plans for patients with other mental health disorders (e.g., autism, aphasia) and developing food plans for patients with specific dietary needs.

ACKNOWLEDGMENT

This work was supported in part by National Science Foundation (NSF) Award 2133842, “EAGER: Advancing Neuro-symbolic AI with Deep Knowledge-infused Learning.”

REFERENCES

- [1] A. Sheth, M. Gaur, K. Roy, and K. Faldu, “Knowledge-intensive language understanding for explainable ai,” *IEEE Internet Computing*, vol. 25, no. 5, pp. 19–24, 2021.
 - [2] R. D. Newman-Norlund, S. E. Newman-Norlund, S. Sayers, S. Nemati, N. Riccardi, C. Rorden, and J. Fridriksson, “The aging brain cohort (abc) repository: The university of south carolina’s multimodal lifespan database for studying the relationship between the brain, cognition, genetics and behavior in healthy aging,” *Neuroimage: Reports*, vol. 1, no. 1, p. 100008, 2021.
 - [3] A. Sheth, M. Gaur, U. Kursuncu, and R. Wickramarachchi, “Shades of knowledge-infused learning for enhancing deep learning,” *IEEE Internet Computing*, vol. 23, no. 6, pp. 54–63, 2019.
 - [4] G. Libben, “From lexicon to flexicon: The principles of morphological transcendence and lexical superstates in the characterization of words in the mind,” *Frontiers in Artificial Intelligence*, vol. 4, 2021.
 - [5] K. Stasaski and M. A. Hearst, “Multiple choice question generation utilizing an ontology,” in *Proceedings of the 12th Workshop on Innovative Use of NLP for Building Educational Applications*, 2017, pp. 303–312.
 - [6] M. Glass, G. Rossiello, M. F. M. Chowdhury, A. R. Naik, P. Cai, and A. Gliozzo, “Re2g: Retrieve, rerank, generate.”
 - [7] K. Roy, M. Gaur, Q. Zhang, and A. Sheth, “Process knowledge-infused learning for suicidality assessment on social media,” *arXiv preprint arXiv:2204.12560*, 2022.
 - [8] S. Gupta, A. Agarwal, M. Gaur, K. Roy, V. Narayanan, P. Kumaraguru, and A. Sheth, “Learning to automate follow-up question generation using process knowledge for depression triage on reddit posts,” 05 2022.
 - [9] S. Yagcioglu, A. Erdem, E. Erdem, and N. Ikizler-Cinbis, “Recipeqa: A challenge dataset for multimodal comprehension of cooking recipes,” *arXiv preprint arXiv:1809.00812*, 2018.
 - [10] F. Pecune, L. Callebort, and S. Marsella, “Designing persuasive food conversational recommender systems with nudging and socially-aware conversational strategies,” *Front. Robot. AI* 8: 733835. doi: 10.3389/frobt, 2022.
 - [11] A. J. Cross and R. Sinha, “Meat-related mutagens/carcinogens in the etiology of colorectal cancer,” *Environmental and molecular mutagenesis*, vol. 44, no. 1, pp. 44–55, 2004.
 - [12] A. Williams, N. Nangia, and S. R. Bowman, “A broad-coverage challenge corpus for sentence understanding through inference,” *arXiv preprint arXiv:1704.05426*, 2017.
 - [13] O.-M. Camburu, T. Rocktäschel, T. Lukasiewicz, and P. Blunsom, “e-snli: Natural language inference with natural language explanations,” *Advances in Neural Information Processing Systems*, vol. 31, 2018.
 - [14] R. Sawhney, A. T. Neerkaje, and M. Gaur, “A risk-averse mechanism for suicidality assessment on social media,” *Association for Computational Linguistics 2022 (ACL 2022)*, 2022.
 - [15] M. Gaur, K. Gunaratna, V. Srinivasan, and H. Jin, “Iseeq: Information seeking question generation using dynamic meta-information retrieval and knowledge graphs,” *arXiv preprint arXiv:2112.07622*, 2021.
- Amit Sheth is the founding director of the AI Institute of South Carolina (AIISC: aiisc.ai), NCR Chair and Professor of Computer Science and Engineering. Contact him at amit@sc.edu
 - Manas Gaur recently completed Ph.D and is joining UMBC as assistant professor in the department of computer science. Contact him at mgaur@email.sc.edu
 - Kaushik Roy, Revathy Venkataraman, and Vedant Khanelwal are current Ph.D. students advised by Prof. Sheth at AIISC. Contact them at {kaushikr, revathy, vedant}@email.sc.edu.