

Duże modele językowe (LLMs) w systemie wspomagania decyzji - dokumentacja wstępna

Maksim Makaranka

1 Temat

Temat dotyczy opracowania koncepcji systemu wspomagania decyzji z językiem naturalnym jako interfejsem człowiek-maszyna. Decydent definiuje problem w języku naturalnym, a agent lub zbiór agentów językowych tworzy model decyzyjny i potencjalnie kod, który może być uruchomiony i oceniony przez decydenta lub kolejnego agenta językowego. Sugerowane rozwiązanie mogłoby być budowane w oparciu o framework AutoGen. W ramach pracy należy wymyślić architekturę systemu, dokonać prototypowej implementacji najistotniejszych fragmentów, która służyłaby walidacji całej koncepcji.

2 Opis problemu

Współczesne systemy wspomagania decyzji muszą sprostać wyzwaniom rosnącej złożoności i zmienności świata, w którym decyzje są podejmowane w warunkach niepewności. Tradycyjna teoria decyzji dostarcza nam narzędzi do analizy i podejmowania decyzji, zwłaszcza gdy kompletne informacje dotyczące wszystkich możliwych opcji są niedostępne lub niepewne. W warunkach niepewności decydenci muszą zarządzać ryzykiem i zmiennością wynikającą z różnorodnych czynników zewnętrznych i wewnętrznych, które mogą wpływać na rezultat decyzji.

Niniejsza praca dąży do implementacji tej koncepcji poprzez wykorzystanie dużych modeli językowych w systemie wieloagentowym. System taki działa jako sieć agentów, gdzie każdy agent oparty na LLM pełni określoną rolę w analizie, przetwarzaniu informacji i generowaniu rekomendacji decyzyjnych. Dzięki wykorzystaniu dużych modeli językowych, każdy agent jest w stanie zrozumieć i przetwarzać dane wyrażone w języku naturalnym, co umożliwia bardziej naturalną interakcję z użytkownikami oraz lepsze uwzględnienie złożonych, kontekstowych informacji.

Kluczowym celem jest zastosowanie metod teorii decyzji do modelowania sytuacji decyzyjnych pełnych niepewności i dynamicznych zmian. Agenci współpracują, aby zinterpretować dane, prognozować potencjalne scenariusze i sugerować najbardziej korzystne decyzje, uwzględniając prawdopodobieństwa różnych wyników.

Warto zauważyć, że różni badacze już wcześniej adresowali problem podejmowania decyzji z wykorzystaniem dużych modeli językowych, co stanowi doskonały punkt wyjścia do dalszego opracowania tego zagadnienia. W następnej sekcji omówiony zostanie artykuł naukowy, który posłuży jako podstawowa inspiracja i podstawa metodyczna dla dalszych prac nad tym projektem.

3 DeLLMa: Ogólny Zarys

Artykuł przedstawiający koncepcję DeLLMa (Decision-making Large Language Model assistant)[1] został opracowany przez zespół badaczy z Uniwersytetu Południowej Kalifornii w lutym 2024 roku (ostatnia rewizja w październiku). Framework DeLLMa ma na celu wspieranie procesu podejmowania decyzji w warunkach niepewności, wykorzystując duże modele językowe i techniki rozumowania oparte na klasycznej teorii decyzji. Kluczowym celem pracy było nie tylko zwiększenie dokładności decyzji podejmowanych przez LLM, ale także zapewnienie możliwości zrozumienia każdego etapu procesu decyzyjnego przez użytkownika.

W ramach tego podejścia autorzy zaprojektowali czterostopniową procedurę, która obejmuje identyfikację i prognozowanie nieznanych stanów wpływających na decyzję, dostosowanie funkcji użyteczności do określonych preferencji oraz maksymalizację oczekiwanej użyteczności. DeLLMa opiera się na prognozowaniu możliwych stanów na podstawie dostępnych informacji, a następnie dobiera decyzję w taki sposób, aby osiągnąć najwyższą przewidywaną użyteczność zgodnie z kontekstem decyzyjnym.

Przeprowadzone eksperymenty wykazały, że DeLLMa osiąga nawet 40% wyższą skuteczność niż inne dostępne metody, zwłaszcza w przypadku bardziej złożonych scenariuszy decyzyjnych. Metodologia DeLLMa jest elastyczna i umożliwia dalsze doskonalenie jej komponentów. W kolejnej sekcji przedstawiono szczegółowy opis matematyczny i metodologiczny rozwiązania, zawierający teoretyczne założenia i formalizmy leżące u jego podstaw.

4 Podstawy matematyczne i metodologiczne

Poniżej przedstawiono opis metody modelowania decyzyjnego zastosowanej w DeLLMa, wzbogaconej o pewne modyfikacje zaproponowane przez autora. Metoda ta stanowi punkt wyjścia do realizacji całego zagadnienia i jest oparta na klasycznych założeniach teorii decyzji, z uwzględnieniem niepewności oraz preferencji decydenta. Przewiduje się, że koncepcja ta może być dalej rozwijana i rozszerzana podczas realizacji pracy, co pozwoli na lepsze dostosowanie modelu do specyficznych wymagań i bardziej złożonych scenariuszy decyzyjnych.

Formalizacja problemu decyzyjnego. W kontekście podejmowania decyzji przez decydenta, kluczowe jest zrozumienie trzech podstawowych komponentów: akcji, stanów natury oraz użyteczności. Stany natury, oznaczone jako Θ , reprezentują zestaw nieznanych czynników, które mają realny, ale niepewny wpływ na wyniki istotne dla celów decydenta. Ich rzeczywiste wartości pozostają nieznane, co wprowadza element niepewności w procesie decyzyjnym. Decydent formułuje problem decyzyjny za pomocą tzw. user prompt'a, oznaczonego jako $\mathcal{P} = (\mathcal{G}, \mathcal{A}_0, \mathcal{C}_0)$. User prompt składa się z opisu celu użytkownika \mathcal{G} , listy akcji wejściowych $\mathcal{A}_0 = (a_1, \dots, a_n)$ oraz kontekstu wejściowego \mathcal{C}_0 , który może zawierać požądane przez użytkownika fragmenty raportów lub historyczne dane. Twórcy oryginalnego artykułu zakładają, że skończona docelowa przestrzeń możliwych akcji jest podana na wejściu przez decydenta, jednak w opracowywanym rozwiązaniu planowane są specjalne kroki, które pozwolą na uzupełnienie tej przestrzeni o inne, potencjalnie dobre dla tego problemu akcje. Podobnie, autorzy artykułu zakładają, że cały kontekst decyzyjny jest podany na wejściu, podczas gdy w tej pracy zostaną opracowane metody na dyskretyzację tego kontekstu względem każdego stanu natury z uzupełnieniem poszczególnych kontekstów o specyficzne dane przydatne do prognozowania prawdopodobieństw wartości tych stanów. Funkcja użyteczności, oznaczona jako $U : \Theta \times \mathcal{A} \rightarrow \mathbb{R}$, przypisuje wartość liczbową dowolnej parze stan-akcja (θ, a) , oceniając, na ile preferowany jest wynik wynikający z tej pary. Celem jest wybór akcji $a^* \in \mathcal{A}$, która maksymalizuje użyteczność, uwzględniając niepewność związaną z nieznanymi stanami $\theta \in \Theta$.

Krok 1: Uzupełnienie przestrzeni akcji. W tym kroku przestrzeń akcji początkowych \mathcal{A}_0 , dostarczonych przez decydenta, jest dostrajana do szerszej przestrzeni akcji \mathcal{A} . Proces ten polega na wyszukiwaniu i analizie zewnętrznych źródeł informacji, takich jak internet, w celu zidentyfikowania podobnych problemów decyzyjnych oraz działań, które zostały podjęte w przeszłości w celu ich rozwiązania. Dzięki temu możliwe staje się uzupełnienie listy dostępnych akcji o potencjalnie wartościowe wybory, które mogą nie być pierwotnie uwzględnione. Warto jednak zauważyć, że ten krok jest mocno zależny od kontekstu konkretnego problemu decyzyjnego. W niektórych przypadkach przestrzeń akcji wejściowych \mathcal{A}_0 może być już kompletna i adekwatna w odniesieniu do specyfiki tego problemu, co oznacza, że rozszerzenie przestrzeni akcji może być zbędne.

Krok 2: Enumeracja stanów. Celem tego kroku jest stworzenie pełnej listy możliwych stanów natury $\Theta = (\theta_1, \dots, \theta_m)$, które są nieznanymi wielkościami przewidywanymi jako mające wpływ na realizację celu użytkownika \mathcal{G} . Proces ten polega na identyfikacji i dyskretyzacji ukrytych czynników, które opisują przestrzeń stanów, umożliwiając prognozowanie różnych scenariuszy decyzyjnych w ramach zadania decyzyjnego. W pierwszym etapie, duży model językowy (LLM) analizuje kontekst \mathcal{P} , aby zidentyfikować zestaw kluczowych czynników ukrytych, które mogą wpływać na cel użytkownika. Następnie dla każdego zidentyfikowanego czynnika model generuje zestaw możliwych wartości, które mogą symbolizować różnorodność rzeczywistości w tym kontekście. Te wartości są używane do dyskretyzacji przestrzeni stanów, tworząc różne kombinacje reprezentujące szeroki wachlarz możliwych rezultatów.

Matematyczny opis procedury polega na tym, że z kontekstu \mathcal{P} LLM identyfikuje k ukrytych czynników, które mogą wpływać na cel użytkownika \mathcal{G} , oznaczanych jako (f_1, \dots, f_k) . Dla każdego ukrytego czynnika f_j , model generuje $\leq \ell$ możliwych wartości, oznaczanych jako $\tilde{f}_j^{1:\ell_j}$. Te wartości, przedstawione jako ciągi znaków (słowa bądź frazy), dyskretyzują przestrzeń stanów, a każdy stan θ_j w przestrzeni Θ stanowi kombinację jednej wartości z każdego z k czynników, co można wyrazić jako $\theta_j = \theta_j^{1:k} \in \Theta$. Łączna liczba możliwych stanów wynosi $|\Theta| = m = \ell^k$, co skutkuje bardzo rozbudowaną przestrzenią, którą należy rozpatrzyć. Pomimo dużej liczby stanów, w kolejnych krokach przedstawiona zostanie procedura prognozowania prawdopodobieństw tych stanów w sposób skalowalny, co umożliwia praktyczne zastosowanie w rzeczywistych scenariuszach decyzyjnych.

Krok 3: Dyskretyzacja i uzupełnienie kontekstu stanów. W tym kroku, dla każdego z ukrytych czynników, w kontekście problemu \mathcal{P} , korzystamy z możliwości dużego modelu językowego (LLM), aby uzyskać informacje o potencjalnie potrzebnych dodatkowych danych, które uzupełnią kontekst. Celem tego działania jest zgromadzenie bardziej szczegółowych informacji, które pozwolą na dokładniejsze późniejsze oszacowanie prawdopodobieństw wartości stanu. Na podstawie sugestii otrzymanych od LLM, przeszukujemy zewnętrzne źródła danych, takie jak skonfigurowane bazy danych czy internet, aby zdobyć odpowiednie dane. Wynikiem tego procesu są zdyskretyzowane konteksty dla każdego ze stanów natury, oznaczone jako $C = (c_1, \dots, c_k)$.

Krok 4: Prognozowanie stanów. Następnym etapem jest prognozowanie prawdopodobieństw stanów θ_j , biorąc pod uwagę zdyskretyzowane i uzupełnione konteksty uzyskane w poprzednim kroku. Autorzy artykułu wspominają o badaniach, które pokazują, że duże modele językowe są zdolne do generowania dobrze skalibrowanych prognoz

na podstawie dostarczonych informacji [2, 3]. Używają oni prostej metody prognozowania, która jest przedstawiona tutaj i potencjalnie może być celem do ulepszenia w ramach dalszej pracy. Dla każdego z k ukrytych czynników oraz każdej z $\leq \ell$ ich możliwych wartości $\tilde{f}_j^{1:\ell_j}$, LLM przypisuje werbalne oceny prawdopodobieństwa, takie jak *bardzo prawdopodobne*, *prawdopodobne*, *raczej prawdopodobne*, *raczej mało prawdopodobne*, *mało prawdopodobne*, *bardzo mało prawdopodobne*. Każda z tych ocen jest następnie zamieniana na wartość liczbową przy użyciu słownika \mathcal{V} . Określone w ten sposób prawdopodobieństwo dla poszczególnej wartości czynnika ukrytego \tilde{f}_i , uwzględniając jego specyficzny kontekst c_i , definiujemy jako $\pi_i(\tilde{f}_i | c_i)$.

Po normalizacji, otrzymany rozkład prawdopodobieństwa dla stanu θ_j można wyrazić jako:

$$\pi^{LLM}(\theta_j | \mathcal{C}) = \prod_{i=1}^k \pi_i(\tilde{f}_i | c_i),$$

gdzie π_i jest rozkładem prawdopodobieństwa dla poszczególnego czynnika określonym na podstawie kontekstu zdyskretyzowanego i uzupełnionego w poprzednim kroku. Prawdopodobieństwa wartości poszczególnych stanów są określane przez LLM na podstawie tego kontekstu. Pomimo upraszczającego założenia o niezależności ukrytych czynników, ta procedura prognozowania wspiera prognozy stanów, które mogą być wykorzystywane w różnych scenariuszach decyzyjnych, co zapewnia solidne podstawy do dalszej analizy.

Krok 5: Elicytacja funkcji użyteczności. Na tym etapie niezbędna jest elicytacja (czyli skonstruowanie) funkcji użyteczności $U : \Theta \times \mathcal{A} \rightarrow \mathbb{R}$, która przypisuje wartość każdej parze stan-akcja (θ_j, a_i) . Funkcja ta ma na celu odzwierciedlenie preferencji użytkownika w kontekście zdefiniowanego celu \mathcal{G} . W tym kroku połączono standardowe metody z mocą dużych modeli językowych, aby automatycznie skonstruować funkcję użyteczności.

Proces rozpoczyna się od próbkowania stanów z prognostycznego rozkładu $\pi^{LLM}(\theta | \mathcal{C})$ i tworzenia zestawu par stan-akcja. Parowanie tych par w minibatche umożliwia modelowi LLM nadanie im rang według celu użytkownika \mathcal{G} . Autorzy artykułu wspominają, że ranking przedmiotów na podstawie LLM, gdzie każdy przedmiot składa się z akcji i konkretnej instancji stanów, to procedura, która ma szerokie zastosowanie, a LLM-y były wcześniej skutecznie wykorzystywane do podobnych porównań [4, 5]. Na podstawie tych klasyfikacji wyciągane są preferencje parowe, które znajdują zastosowanie w algorytmach klasycznej elicytacji użyteczności, takich jak model Bradley-Terry.

W algorytmie przedstawionym w artykule pokazano procedurę oraz dwie strategie formatowania rankingów: Rank2Pairs i One-vs-All. Rank2Pairs konwertuje ranking o malejącej preferencji $\mathcal{R} = ((\theta, a)_{(1)}, \dots, (\theta, a)_{(b)})$ na listę porównań, dodając $(\theta, a)_{(i)} \succ (\theta, a)_{(j)}$, gdy $i < j$. Natomiast One-vs-All zakłada, że LLM jest obojętny w stosunku do wszystkich par stan-akcja oprócz najwyższej ocenionej, czyli $\{(\theta, a)_{(1)} \succ (\theta, a)_{(i)} \mid \forall 2 \leq i \leq b\}$. To rozwiązanie można preferować, gdy dokładne porównania mniej optymalnych par stan-akcja są trudne.

Wreszcie, aby skalować wnioskowanie w czasie rzeczywistym, efektywność obliczeń i dokładność elicytacji użyteczności mogą być zrewolucjonizowane przez wykorzystanie procedur *batchingu* oraz *redukcji wariancji*. W *batchingu* próbki par stan-akcja $S_A = \{(\theta, a)\}$ są dzielone na nakładające się na siebie minibatche do rankingów, z częścią próbek $q\%$ wspólną dla kolejnych minibatchów, co pozwala na bardziej precyzyjną elicytację. Redukcja wariancji polega na próbkowaniu niezależnych wartości stanu oraz tworzeniu ich duplikatów dla każdej możliwej akcji, co pozwala na uzyskanie bardziej stabilnych oszacowań użyteczności.

Krok 6: Maksymalizacja oczekiwanej użyteczności. W tej końcowej fazie procesu obliczana jest oczekiwana użyteczność dla każdej możliwej akcji, a następnie wybierana jest ta, która maksymalizuje oczekiwane korzyści. Dla każdej akcji stosuje się oszacowanie oczekiwanej użyteczności metodą Monte Carlo, bazując na próbkach par stan-akcja pobranych z prognostycznego rozkładu stanów $\pi^{LLM}(\theta | \mathcal{C})$ oraz uzyskanej funkcji użyteczności. Obliczenia te przeprowadza się analitycznie, bez bezpośredniego wykorzystania LLM. Oczekiwaną użyteczność $U_{\mathcal{C}}(a)$ można przybliżyć jako:

$$U_{\mathcal{C}}(a) \approx \frac{1}{|S|} \sum_{\theta \in S} U(\theta, a),$$

gdzie $S \subseteq \Theta$ to zbiór próbek stanów wylosowanych z rozkładu prognozowanego przez LLM, który jest przybliżeniem rozkładu post-priori o stanach, uwzględniając kontekst \mathcal{C} , czyli $S \stackrel{i.i.d.}{\sim} \pi^{LLM}(\theta | \mathcal{C}) \approx \pi(\theta | \mathcal{C})$. Po obliczeniu oczekiwanej użyteczności $U_{\mathcal{C}}(a)$ dla każdej akcji wybiera się ostateczną decyzję poprzez maksymalizację:

$$a^* = \operatorname{argmax}_{a \in \mathcal{A}} U_{\mathcal{C}}(a).$$

Ten wybór zapewnia, że podejmowana decyzja maksymalizuje potencjalne korzyści, biorąc pod uwagę prognozowane prawdopodobieństwa stanów w kontekstach, które są analizowane.

Dalsze kierunki rozwoju. Metodologia DeLLMa stanowi podstawowy schemat decyzyjny oparty na teorii decyzji, który może być rozbudowywany o dodatkowe funkcje prognozowania i bardziej zaawansowane modelowanie niepewności. Możliwości modyfikacji obejmują np. uwzględnienie bardziej złożonych funkcji użyteczności oraz metod prognozowania stanów.

5 Propozycja rozwiązania

Wstępny prototyp systemu wspomagania decyzji, wykorzystujący interfejs w języku naturalnym, opiera się na zharmonizowanej współpracy kilku agentów, z których każdy ma przypisane konkretne zadania związane z różnymi etapami procesu decyzyjnego. Modułarna struktura systemu pozwala na elastyczne zarządzanie agentami oraz ich integrację, co czyni projekt bardziej adaptowalnym do zmieniających się warunków i specyfikacji użytkownika. Należy jednak podkreślić, że jest to wstępna wersja koncepcji, będąca „prototypem prototypu”, która wymaga dalszej walidacji i rozwoju w kontekście rzeczywistych zastosowań.

1. Agent Analizy Wstępnej

- **Zadanie:** Analizuje user prompt dostarczony przez decydenta, przeprowadza wstępną dekonstrukcję problemu decyzyjnego na potrzeby kolejnych agentów. Generuje definicję celu \mathcal{G} , wstępne przestrzeń akcji \mathcal{A}_0 oraz kontekst \mathcal{C}_0 .
- **Komunikacja:** Współpracuje z resztą agentów, przekazując im wstępne dane do dalszej analizy i przetwarzania.

2. Agent Rozszerzania Przestrzeni Akcji

- **Zadanie:** Eksploruje zewnętrzne źródła informacji w celu rozszerzenia przestrzeni możliwych akcji \mathcal{A} .
- **Komunikacja:** Pobiera dane od Agentu Analizy Wstępnej i przekazuje rozszerzoną przestrzeń akcji do kolejnych agentów. Współpracuje także z Agentem Pozyskiwania Danych.

3. Agent Analizy Stanów Natury

- **Zadanie:** Identyfikuje i dyskretyzuje ukryte czynniki wpływające na wyniki decyzyjne, tworząc pełną listę możliwych stanów Θ .
- **Komunikacja:** Współpracuje z Agentem Dyskretyzacji i Uzupełniania Kontekstów w celu uzupełnienia kontekstów o dodatkowe dane dla każdego stanu. Komunikuje się również z Agentem Pozyskiwania Danych.

4. Agent Dyskretyzacji i Uzupełniania Kontekstów

- **Zadanie:** Uzupełnia konteksty stanów, przeszukując brakujące dane w zewnętrznych bazach danych czy internecie przy wsparciu Agentu Pozyskiwania Danych. Efektem jego pracy jest stworzenie kompletnej listy kontekstów \mathcal{C} .
- **Komunikacja:** Współpracuje z Agentem Analizy Stanów Natury, by zapewnić kompletność kontekstów i ich przygotowanie dla Agentu Prognozowania Stanów.

5. Agent Prognozowania Stanów

- **Zadanie:** Prognozuje prawdopodobieństwa stanów na podstawie zdyskretyzowanych i uzupełnionych kontekstów.
- **Komunikacja:** Przekazuje rozkład prawdopodobieństw stanów Agentowi Elicytacji Funkcji Użyteczności w celu dalszej analizy i zastosowania w elicytacji.

6. Agent Elicytacji Funkcji Użyteczności

- **Zadanie:** Elicytuje funkcję użyteczności, generując klasyfikacje rang par stanów i akcji na podstawie celu zdefiniowanego przez decydenta.
- **Komunikacja:** Współpracuje z Agentem Maksymalizacji Oczekiwanej Użyteczności, przekazując wyniki elicytacji do ostatecznej oceny akcji.

7. Agent Maksymalizacji Oczekiwanej Użyteczności

- **Zadanie:** Oblicza oczekiwaną użyteczność dla każdej akcji i wybiera tę, która maksymalizuje korzyści. Jest to agent analityczny, który działa niezależnie od dużych modeli językowych, stosując techniki statystyczne i analityczne.
- **Komunikacja:** Działa jako końcowy decydent, wykorzystując dane od Agentu Elicytacji Funkcji Użyteczności do podjęcia ostatecznej decyzji i wyboru najlepszej akcji.

8. Agent Pozyskiwania Danych

- **Zadanie:** Specjalny agent, lub potencjalnie zbiór agentów, przeszukujący internet i możliwie inne skonfigurowane źródła danych w celu uzyskiwania dodatkowych informacji, które mogą być użyte przy rozszerzaniu przestrzeni akcji i uzupełnianiu kontekstów.
- **Komunikacja:** Współpracuje z Agentem Rozszerzania Przestrzeni Akcji, Agentem Analizy Stanów Natury oraz Agentem Dyskretyzacji i Uzupełniania Kontekstów.

9. Agent Komunikacji Wyników

- **Zadanie:** Kompiluje zebrane wyniki analizy i przetwarzania danych przez poszczególne agenty oraz tworzy raport, który wyjaśnia podjętą decyzję. Raport jest generowany w formacie pożądanym przez użytkownika, jeśli taki został określony, zapewniając przejrzystość i zrozumiałość wyników.
- **Komunikacja:** Współpracuje z innymi agentami, aby uzyskać pełny obraz procesu decyzyjnego. Odpowiada za przedstawienie nie tylko ostatecznej decyzji, ale także wyjaśnienie każdego etapu procesu decyzyjnego, co wspiera użytkownika w zrozumieniu logiki stojącej za podejmowanymi działaniami.

Integracja agentów Aby zapewnić sprawne działanie całego systemu, wszystkie agenty powinny być zintegrowane za pomocą centralnego systemu zarządzania komunikacją. System ten będzie odpowiedzialny za nadzorowanie przepływu informacji między agentami, koordynację zadań oraz zarządzanie potencjalnymi błędami w procesie decyzyjnym. W celu realizacji tych funkcji, można utworzyć oddzielnego, wyspecjalizowanego **Agenta Zarządzania Komunikacją**, który będzie pełnił rolę centralnego koordynatora.

Prototypowa Implementacja Aby zweryfikować koncepcję systemu, początkowa implementacja będzie obejmować kluczowych agentów, takich jak Agent Analizy Wstępnej, Agent Analizy Stanów Natury, Agent Prognozowania Stanów, Agent Elicytacji Funkcji Użyteczności oraz Agent Maksymalizacji Oczekiwanej Użyteczności. Taki prototyp pozwoli na walidację funkcjonalną całej koncepcji, weryfikując poprawność działania systemu oraz sposób komunikacji między agentami.

6 Sposób rozwiązania

Planowana jest implementacja systemu przy użyciu sugerowanego frameworku AutoGen. W ramach pracowni problemowej magisterskiej przebadane zostaną jednak także inne frameworki do tworzenia wieloagentowych systemów LLM, takie jak LangGraph, CrewAI oraz niedawno wprowadzony przez OpenAI Swarm. Po analizie porównawczej różnych podejść zostanie podjęta ostateczna decyzja dotycząca wyboru najodpowiedniejszego frameworku. Wybór ten będzie oparty na kryteriach takich jak wydajność, skalowalność, łatwość integracji, wsparcie społeczności oraz dostępność dokumentacji.

7 Planowane badania

W celu oceny skuteczności i przydatności modelu, planowane są testy symulacyjne oraz analiza wyników w kontekście wspierania procesów decyzyjnych pod wpływem niepewności. Badania będą prowadzone zgodnie z poniższymi krokami:

1. **Symulacja złożonych scenariuszy decyzyjnych:** W pierwszej kolejności przeprowadzone zostaną symulacje, obejmujące różnorodne scenariusze decyzyjne, w których model będzie oceniany pod kątem trafności przewidywań oraz zdolności do maksymalizacji użyteczności. Nacisk zostanie położony na generowaniu syntetycznych scenariuszy, które pozwolą na testowanie reakcji modelu na różne stany wejściowe i ich kombinacje.

2. **Testy na zestawach decyzyjnych z próbą wdrożenia w organizacji, w której pracuje autor:** W przypadku możliwości przeprowadzenia testów na danych rzeczywistych, planowane jest wdrożenie modelu w firmie Eracent, która ma ugruntowaną pozycję na rynku, oferując różnorodne rozwiązania w obszarze ITAM (Information Technology Asset Management) oraz SAM (Software Asset Management). ITAM i SAM to obszary związane z zarządzaniem zasobami i oprogramowaniem IT w organizacjach. W tym kontekście przeanalizowana zostanie efektywność podejmowanych decyzji oraz zdolność modelu do wspierania decyzji w praktycznym środowisku biznesowym.

3. **Elicytacja i prognoza zmiennych stanu oraz użyteczności:** Model zostanie przetestowany pod kątem skuteczności prognozowania kluczowych zmiennych stanu oraz precyzji w ustalaniu funkcji użyteczności, mającej na celu maksymalizację oczekiwanej korzyści decyzji. Ocena obejmie zgodność wyników z metodologią DeLLMa, w tym stabilność prognoz w obliczu zmieniających się danych wejściowych.

Realizacja powyższych badań umożliwi kompleksową ocenę modelu, szczególnie pod kątem jego trafności i użyteczności w różnych kontekstach decyzyjnych.

Literatura

- [1] Ollie Liu, Deqing Fu, Dani Yogatama, and Willie Neiswanger. DeLLMa: Decision Making Under Uncertainty with Large Language Models. arXiv preprint arXiv:2402.02392, 2024. <https://arxiv.org/abs/2402.02392>.
- [2] Katherine Tian, Eric Mitchell, Allan Zhou, Archit Sharma, Rafael Rafailov, Huaxiu Yao, Chelsea Finn, and Christopher D Manning. Just ask for calibration: Strategies for eliciting calibrated confidence scores from language models fine-tuned with human feedback. arXiv preprint arXiv:2305.14975, 2023
- [3] Miao Xiong, Zhiyuan Hu, Xinyang Lu, Yifei Li, Jie Fu, Junxian He, and Bryan Hooi. Can llms express their uncertainty? an empirical evaluation of confidence elicitation in llms. arXiv preprint arXiv:2306.13063, 2023.
- [4] Harrison Lee, Samrat Phatale, Hassan Mansoor, Thomas Mesnard, Johan Ferret, Kellie Lu, Colton Bishop, Ethan Hall, Victor Carbune, Abhinav Rastogi, and Sushant Prakash. RLAIIF: Scaling reinforcement learning from human feedback with ai feedback, 2024. URL: <https://openreview.net/forum?id=AAxIs3D2ZZ>
- [5] Zhen Qin, Rolf Jagerman, Kai Hui, Honglei Zhuang, Junru Wu, Jiaming Shen, Tianqi Liu, Jialu Liu, Donald Metzler, Xuanhui Wang, and Michael Bendersky. Large language models are effective text rankers with pairwise ranking prompting, 2023.