A Notion of Complexity for Theory of Mind via Discrete World Models

Anonymous ACL submission

Abstract

 Theory of Mind (ToM) can be used to assess the capabilities of Large Language Models (LLMs) in complex scenarios where social reasoning is required. While the research community has proposed many ToM benchmarks, their hard- ness varies greatly, and their complexity is not well defined. This work proposes a framework to measure the complexity of ToM tasks. We quantify a problem's complexity as the number of states necessary to solve it correctly. Our complexity measure also accounts for spurious states of a ToM problem designed to make it apparently harder. We use our method to as- sess the complexity of five widely adopted ToM benchmarks. On top of this framework, we de- sign a prompting technique that augments the information available to a model with a descrip- tion of how the environment changes with the agents' interactions. We name this technique Discrete World Models (DWM) and show how it elicits superior performance on ToM tasks.^{[1](#page-0-0)} **021**

⁰²² 1 Introduction

 Theory of Mind (ToM) studies how agents form and use beliefs to reason in dynamic environ- ments [\(Premack and Woodruff,](#page-9-0) [1978\)](#page-9-0). Originally [d](#page-9-1)eveloped to describe human interactions [\(Preston](#page-9-1) [and De Waal,](#page-9-1) [2002;](#page-9-1) [Tomasello,](#page-9-2) [2009\)](#page-9-2) as well as [t](#page-9-3)oddlers' psychological development [\(Wimmer and](#page-9-3) [Perner,](#page-9-3) [1983;](#page-9-3) [Baron-Cohen et al.,](#page-8-0) [1985\)](#page-8-0), ToM has been quickly adopted by other fields, including [a](#page-9-5)rtificial intelligence [\(McCarthy,](#page-9-4) [1979;](#page-9-4) [Scassel-](#page-9-5) [lati,](#page-9-5) [2002\)](#page-9-5) and machine learning [\(Rabinowitz et al.,](#page-9-6) [2018\)](#page-9-6). In machine learning, ToM has both descrip- tive and prescriptive usage: on the one hand, ToM benchmarks assess the capabilities of a model in **complex environments; on the other, ToM's frame-** works such as *theory-theory* [\(Gopnik and Wellman,](#page-8-1) [1994\)](#page-8-1) and *simulation theory* [\(Churchland,](#page-8-2) [2013\)](#page-8-2)

Question: Where does Bob think the apple is?

CoT Answer: Bob thinks the apple is on the floor. $\boldsymbol{\times}$ DWM Answer: Bob thinks the apple is on the table. \checkmark

Figure 1: Example of the DWM prompting technique on a classical *Sally-Anne* QA task [\(Baron-Cohen et al.,](#page-8-0) [1985\)](#page-8-0). Inspired by our complexity framework (Section [3.1\)](#page-1-0), DWM takes the original task and splits it into sequences, the *state events* (see Def. [3.1\)](#page-2-0), and prompts the LLMs to describe the states. We show that, in most cases, this aids the LLM in providing correct answers.

have been widely adopted to test the proficiency **039** of Large Language Models (LLMs) in social tasks **040** where humans excel [\(Strachan et al.,](#page-9-7) [2024\)](#page-9-7).

In this work, we propose a framework to charac- **042** terise a ToM benchmark's difficulty, i.e., its com- **043** plexity, as the number of *state events* that are suf- **044** ficient to track the state of an object, including **045** kth -order beliefs. 046

We characterise the complexity of five standard 047 ToM benchmarks, from false belief to common- **048** sense and social reasoning, and compute their com- **049** plexity as a proxy of their inherent difficulty. In- **050** spired by prompting techniques that split a task **051** into elementary sub-problems that are solved se- **052** quentially, like Tree of Thoughts [\(Yao et al.,](#page-10-0) [2023\)](#page-10-0) **053** and least-to-most prompting [\(Zhou et al.,](#page-10-1) [2023a\)](#page-10-1), **054** we introduce a technique that stimulates a model's **055** reasoning capabilities via Discrete World Mod- **056** els (DWM). DWM leverages the notion of state- **057**

 1 Code and data for full reproducibility are available in the Code Material.

 fulness via a succinct and coherent representa- tion of each *state events*, as illustrated in Fig- ure [1.](#page-0-1) We test DWM on ToMi [\(Le et al.,](#page-9-8) [2019\)](#page-9-8), MindGames [\(Sileo and Lernould,](#page-9-9) [2023\)](#page-9-9), Adv- CSFB [\(Shapira et al.,](#page-9-10) [2023\)](#page-9-10), SocialIQA [\(Sap et al.,](#page-9-11) [2019\)](#page-9-11), and FANToM [\(Kim et al.,](#page-8-3) [2023\)](#page-8-3), elicit- ing superior performance than Chain of Thoughts (CoT) [\(Wei et al.,](#page-9-12) [2022\)](#page-9-12) and Tree of Thoughts (ToT) [\(Yao et al.,](#page-10-0) [2023\)](#page-10-0) on those problems whose *state spaces* are informative. We further as- sess whether memorisation affects a model's per- formance, and we discover that while this phe- nomenon happens for standard benchmarks such as ToMi [\(Le et al.,](#page-9-8) [2019\)](#page-9-8), with input-output pairs that can be retrieved *word for word* via prompt- ing, it does not correlate with a drop of perfor- mance. We conduct our experiments on a vari- ety of open- and closed-source LLMs, including **GPT-3.5-Turbo, GPT-4 [\(OpenAI,](#page-9-13) [2023\)](#page-9-13), LLaMA3-** [7](#page-8-5)0B [\(AI@Meta,](#page-8-4) [2024\)](#page-8-4) and Mixtral 8x7B [\(Jiang](#page-8-5) [et al.,](#page-8-5) [2024\)](#page-8-5). In summary, in this paper:

- **We introduce the concept of complexity** of a **080** ToM task to quantify the hardness of keeping **081** track of the elements (e.g., agents' beliefs or **082** objects' states) that are sufficient to produce **083** the correct answer to different problems.
- **084** We propose DWM, a simple yet effective **085** prompting technique that improves a model's 086 **capability by making implicit** information ex-**087** plicit while not necessitating *exogenous in-***088** *formation* (i.e., it does not require RAG or **089** fine-tuning).

 We consider our work a step towards a framework that formalizes the hardness of a ToM problem univocally inspired by the theory of World Mod-els [\(Wong et al.,](#page-10-2) [2023\)](#page-10-2).

⁰⁹⁴ 2 Related Work

 Over 40 years of research on ToM in psychol- [o](#page-8-0)gy [\(Premack and Woodruff,](#page-9-0) [1978;](#page-9-0) [Baron-Cohen](#page-8-0) [et al.,](#page-8-0) [1985;](#page-8-0) [Dennett,](#page-8-6) [1988;](#page-8-6) [Wellman,](#page-9-14) [2017\)](#page-9-14) on hu- man development has created a fertile ground for the development of these ideas in adjacent fields. In the last decade, many works studied ToM in artifi- cial intelligence and machine learning [\(Baker et al.,](#page-8-7) [2011;](#page-8-7) [Rabinowitz et al.,](#page-9-6) [2018\)](#page-9-6), with applications to multi-agent systems and reinforcement learn- ing [\(Gronauer and Diepold,](#page-8-8) [2022\)](#page-8-8). More recently, the rise in popularity of LLMs shifted the inter-est towards understanding and benchmarking large

models' capacity to solve increasingly complex **107** ToM tasks [\(Aru et al.,](#page-8-9) [2023;](#page-8-9) [Zhou et al.,](#page-10-3) [2023b;](#page-10-3) **108** [Mahowald et al.,](#page-9-15) [2024\)](#page-9-15). While some researchers **109** believe LLMs have already become proficient in **110** solving ToM tasks [\(Bubeck et al.,](#page-8-10) [2023;](#page-8-10) [Kosinski,](#page-9-16) **111** [2023;](#page-9-16) [Strachan et al.,](#page-9-7) [2024\)](#page-9-7), others show scepti- **112** cism and illustrate cases where they fail on trivial **113** variations of well-known problems [\(Ullman,](#page-9-17) [2023;](#page-9-17) 114 [Shapira et al.,](#page-9-10) [2023;](#page-9-10) [Sap et al.,](#page-9-18) [2023\)](#page-9-18). In a joint **115** effort between computer scientists and psycholo- **116** gists, many ToM benchmarks have been developed **117** and used to test neural-network models, includ- **118** ing LLMs [\(Gandhi et al.,](#page-8-11) [2022;](#page-8-11) [Chen et al.,](#page-8-12) [2024;](#page-8-12) **119** [Strachan et al.,](#page-9-7) [2024\)](#page-9-7). Recently, concepts such as **120** World Models [\(Ha and Schmidhuber,](#page-8-13) [2018\)](#page-8-13) have **121** found applicability and mostly as discrete prompt- **122** ing techniques in conjunction with optimisation **123** [p](#page-9-19)rocedures [\(Hao et al.,](#page-8-14) [2023;](#page-8-14) [Moghaddam and](#page-9-19) **124** [Honey,](#page-9-19) [2023\)](#page-9-19). Researchers have found evidence **125** of an emergent internal representation (e.g., World **126** Model's surrogates) of the state games [\(Li et al.,](#page-9-20) **127** [2022;](#page-9-20) [Toshniwal et al.,](#page-9-21) [2021\)](#page-9-21) and state-tracking **128** abilities [\(Li et al.,](#page-9-22) [2021;](#page-9-22) [Kim and Schuster,](#page-8-15) [2023;](#page-8-15) **129** [Kim et al.,](#page-8-16) [2024\)](#page-8-16), necessary for correct belief track- 130 ing in ToM problems. The works more similar to **131** our complexity framework are only tangentially re- **132** lated to ToM. Inspired by the work in [\(Zhou et al.,](#page-10-1) **133** [2023a\)](#page-10-1) and the results in [\(Zhou et al.,](#page-10-3) [2023b\)](#page-10-3). Our **134** prompting technique is inspired by [\(Park et al.,](#page-9-23) **135** [2023\)](#page-9-23) and [\(Nye et al.,](#page-9-24) [2021\)](#page-9-24): the former devel- **136** ops an architecture to record the agent's experi- **137** ences. The latter proposes a prompting technique **138** that forces a model to express the intermediate com- **139** putational steps to solve a problem. **140**

3 Methodology **¹⁴¹**

In this section, we introduce a notion of complexity **142** for ToM problems: such notion quantifies the hard- **143** ness of a problem as the number of *computational* **144** *steps* humans take to solve them. We then present **145** the DWM prompting technique within the com- **146** plexity framework and show how it differs from **147** standard methods like CoT and ToT. We further **148** characterise its efficiency with the number of in- **149** put/output tokens and queries to a model as the **150** control variables. **151**

3.1 On the Complexity of ToM **152**

Providing a consistent representation of the envi- **153** ronment, including each agent's beliefs, inspired us **154** to characterise the complexity of a ToM problem **155**

Complexity
$$
(obj_2)
$$
 = T_{obj2} + τ (T_{obj1} + T_{obj3})

Figure 2: How statefulness and statelessness (Def. [3.2\)](#page-3-0) are computed for the motivating example in Fig. [1.](#page-0-1) For obj_1 , an optimal split to track the apple merges the first two states and chunks of the input prompt. For obj_2 , which involves the 1st-order belief of **Bob**, the statefulness is higher, with e_2 that cannot be merged with e_3 as it introduces partial observability. The complexity of the task (bottom) is computed as per Eq. [2,](#page-3-1) with the complexity of stateless objects that is discounted as not directly relevant to the question/answer.

 in terms of sufficient elements to track to output 157 the correct result. Consider a problem prompt p, expressed in natural language, that describes how multiple agents interact with an environment ob- ject obj, as illustrated in Figure [2](#page-2-1) (top). In our framework, an object can be the state of the apple 162 as well as the kth -order belief of an agent about the apple position. Our framework naturally extends to multiple objects by considering their union.

165 Suppose that in p, the state of \textbf{obj} is modified 166 $T > 0$ times, thus identifying T unique configu-167 rations, namely $E_{\text{obj}} = \{e_1, ..., e_T\}$. To correctly 168 solve a ToM task where p is complemented by a **169** query about obj, a model should distinguish be-**170** tween the interactions that modify the configura-**171** tion of obj, i.e., the stateful states, from those that 172 modify any other **stateless** object $Obj \setminus obj$, i.e., **173** those one does not need to track.

 We first show how to define the cost of tracking a task's stateful states, which we complement with that of the stateless. Both definitions concur in defining the complexity of a ToM task.

178 3.1.1 Stateful and Stateless Complexity

 For a ToM task, expressed as p, that describes the evolution of an environment where an unknown **number of atomic iterations T modifies obj or its perception, each environment state** $e_t \in E_{\text{obj}}$ can 183 be coupled with the prompt prefix $p \leq t$ s.t. $p \leq t \oplus$

 $p_{>t} = p$, that describes such configuration. We 184 denote $(e_t, p_{\leq t})$ as a generic *state description*, as **185** illustrated in Figure [2](#page-2-1) (top). **186**

Definition 3.1 (State event). A *state event* for an **187** object obj is an event that links adjacent *state de-* **188** *scriptions* that involve, for both the environment **189** state e_t and the sub-prompt $p_{\leq t}$, a state change 190 of obj. Formally, we define a relation, F_{obj} , to **191** specify which pairs of state descriptions form a **192 state event:** $F_{obj}((e_t, p_{\leq t}), (e_{t+1}, p_{\leq t+1})) \equiv e_t \neq 193$ $e_{t+1} \wedge p_{\leq t+1} = p_{\leq t} \oplus p_{t+1}$ where $1 \leq t \leq |p|$. 194 $(|p|)$ denotes the number of atomic prompts.) 195

Thus a *state event* F_{obj} identifies those *state* 196 *descriptions* $(e_t, p_{\leq t})$ which have a successor 197 $(e_{t+1}, p_{\leq t+1})$ where obj has changed its config- 198 uration. **199**

In the context of ToM tasks, a *state event* could **200** be a person who moves an object, exits (thus intro- **201** ducing partial observability) or witnesses a change **202** in the environment (as now the description of the **203** environment will take that change into account), 204 as illustrated Figure [2](#page-2-1) (middle). Our prompting **205** technique, namely DWM (Section [3.2.1\)](#page-3-2), aims at **206** making implicit observations about objects explicit. **207**

We finally introduce the notion of *partition func-* **208** *tion* to connect the **maximum number** of nonempty *state events* relative to a prompt. Such a **210** notion will serve as the building block to compute **211** the complexity of a ToM problem. **212** Definition 3.2 (Partitions). A *partition* partobj w.r.t. obj identifies those *state events* which par- tition a ToM prompt p into sequential segments where obj changes its value. Formally:

$$
\begin{aligned}\n\text{Let } part_{\mathbf{obj}} &= \{ (e_t, p_{\leq t}) : \\
F_{\mathbf{obj}}((e_t, p_{\leq t}), (e_{t+1}, p_{\leq t+1})) \\
&\wedge e_t \in E_{\mathbf{obj}} \}\n\end{aligned}
$$
\n
$$
(1)
$$

Def. [3.2](#page-3-0) describes an optimal partition, $part_{\textbf{obj}}$ of *state descriptions* that covers all the relevant changes to obj. The partition is represented by the set of event descriptions where obj changes its description immediately after. Note that this set of event descriptions is unique for any obj.

224 3.1.2 The Complexity of a ToM Task

 We can now define the notion of statefulness of a ToM task specified as a prompt p as the size of **Eq. [3.2,](#page-3-0) namely** $T_{\text{obj}} = |E_{\text{obj}}|$ **. The process of** computing the statefulness of an object or its belief is illustrated in Fig. [2.](#page-2-1)

 For a ToM task where the question to solve re- lates to an object obj, one must ensure that changes 232 to any other object, namely $Obj \setminus obj$, do not af- fect obj. While tracking the evolution of what is irrelevant to answer the question is unnecessary, a computation model must assess whether a partic- ular environmental change affected obj. We thus introduce the notion of statelessness, i.e., the cost of discerning whether a change in the environment affects obj. The computation is similar to that of Def. [3.2,](#page-3-0) with obj that is replaced by any object in $Obj \, \bold{obj}$; yet, for stateless objects, we introduce a discount factor τ to penalise the complexity of *state events* that do not affect obj. Mathematically, we formalise the statelessness of a ToM task involving **an object obj as** $\tau \sum_{obj \in Obj} \text{obj} \cdot \text{obj}$.

 Finally, we formalise the complexity of a ToM task w.r.t. an object obj as the complexity of the stateful states plus the (discounted) sum of the oth-ers (i.e., stateless). Namely:

$$
T_{\mathbf{obj}} + \tau \sum_{obj \in Obj} T_{obj} \tag{2}
$$

251 The process of computing the complexity of a **252** ToM task is illustrated in Figure [2.](#page-2-1)

253 3.2 Discrete World Models

254 We first introduce the background notation for **255** prompting LLMs and assessing their accuracy on **256** a standard classification task. We then propose our technique, namely DWM, which we eventually **257** connect with the notion of statefulness of a ToM **258** task. **259**

Background notation. A (Large) Language **260** Model is a function that predicts the next token 261 (out of a finite vocabulary) conditioned on the se- **262** quence of previously fed/generated tokens, namely **263** $\psi : \mathbf{v} \in V^* \to v \in V$. Such a mechanism can 264 be used to sample multiple token outputs until an **265** `end-of-text' token is predicted by invoking ψ 266 in an auto-regressive fashion, i.e., $\psi(v|\mathbf{v})$. In our **267** setting, a problem is specified as a tuple (p, Q) , 268 where p is a ToM problem and Q is a *query* function 269 that modifies p according to a prompting technique, **270** namely $Q: p \to p'$. The LLMs output y for an input $Q(p)$ is then compared for correctness against **272** an oracle Ω , i.e., Ω : $\psi(Q(p)) \to \{0, 1\}$, where 1 273 means correct classification (0, otherwise). On a **274** sample of $N > 0$ ToM problems, the accuracy of a 275 model ψ is then measured as $\frac{1}{N} \sum_{i=1}^{N} \Omega(\psi(Q(p_i)))$, 276 i.e., the average number of times a model is correct **277** in its prediction. **278**

3.2.1 Discrete World Models via Prompting **279**

Given a ToM problem p and a constant $T \n\leq |p|$, 280 we can rewrite p as $p_1 \oplus p_2 \oplus \cdots \oplus p_T$. Our *query* 281 function adds a standard preamble x similar to 282 that of CoT. DWM inserts, after each "split" p_t , an additional prompt w like 'Now, provide a **284** succinct description of the state of the **285** environment and each agent's belief.' and **286** query an LLM to provide a representation of the **287** current *state description* of the environment. An **288** LLM is initially queried with $x \oplus p_1 \oplus w$, and the 289 answer a_1 is concatenated to the next query, i.e., 290 $\psi(x \oplus p_1 \oplus w \oplus a_1 \oplus p_2 \oplus w)$ to retrieve a_2 . The 291 process is carried on for each of the T chunks, and, **292** at the end, y is concatenated to eventually prompt **293** the model for the correct answer to p. 294

Let $z_1 = \psi(x \oplus p_1), z_t = \psi(x \oplus p_1 \oplus z_1 \oplus p_2 \oplus z_2)$ 295 $\cdots \oplus z_{t-1} \oplus p_t) = \psi(x \oplus \left(\bigoplus_{i=1}^{t-1} p_i \oplus z_i\right) \oplus p_t),$ 296 then, the final query is ²⁹⁷

$$
\psi(x \oplus \left(\bigoplus_{t=1}^{T} p_t \oplus z_t\right) \oplus y) \qquad (3) \qquad \qquad 298
$$

In this sense, our partition function (Def. [3.2\)](#page-3-0) **299** consists of splitting a prompt into sequential chunks **300** of the prompt, while the LLM is prompted to **301** provide each *state event* at time $1 \le t < T$ as 302 $e_t = \psi(x \oplus (\bigoplus_{t'=1}^t p_{t'} \oplus z_{t'}) \oplus \omega)$. The process 303

Figure 3: Left: illustration of DWM prompting as per the example in Figure [1.](#page-0-1) We interactively prompt an LLM with a ToM problem, asking to provide a succinct representation of each agent's beliefs. Right: schematic presentation of the DWM method. We first break the input string into T *state descriptions*. Then, for each part, we ask the LLM to provide the state event of the environment and how it changes. In the last step, every part of the input and description is fed to the LLM with another prompt to get the answer for the task.

304 of prompting a model with DWM is illustrated in **305** Figure [3.](#page-4-0)

306 3.2.2 On the Complexity of DWM

 DWM progressively calls an LLM T > 0 times to generate informative states. For a ToM problem of length n (i.e., the number of input tokens), which we assume, w.l.o.g., that can be split into k chunks of approximately the same length $|x \oplus p_i \oplus w| = \frac{n}{l}$ 311 of approximately the same length $|x \oplus p_i \oplus w| = \frac{n}{T}$, the number of tokens generated by an LLM is in the 313 order of $\mathcal{O}(\sum_{t=1}^T |x \oplus p_t \oplus w \oplus a_t|^2)$, where $p_t(a_t)$ is the portion of the problem (answer) prompted (retrieved) at iteration t. With the further assump-316 tion that each answer retrieved at split $t < T$ has the same length o, the complexity is further simpli-**fied to be asymptotic to** $\mathcal{O}((\frac{n}{T} + o)^2)$ **. Compared to** 319 CoT, whose complexity is $\mathcal{O}(n+o)$, DWM requires an additional linear number of calls to the model. On the other hand, ToT with the same number of splits $\frac{n}{T}$ and $m > 1$ experts results in even higher **complexity, i.e., asymptotic to** $\mathcal{O}(m(\frac{n}{T} + o)^2)$ **.**

³²⁴ 4 Experimental Evaluation

 The experiments are organised as follows. We first test the performance of DWM on ToMi [\(Le et al.,](#page-9-8) [2019\)](#page-9-8), MindGames [\(Sileo and Lernould,](#page-9-9) [2023\)](#page-9-9), [A](#page-9-11)dv-CSFB [\(Shapira et al.,](#page-9-10) [2023\)](#page-9-10), SocialIQA [\(Sap](#page-9-11) [et al.,](#page-9-11) [2019\)](#page-9-11), and FANToM [\(Kim et al.,](#page-8-3) [2023\)](#page-8-3), com- [p](#page-10-0)aring it with CoT [\(Wei et al.,](#page-9-12) [2022\)](#page-9-12), ToT [\(Yao](#page-10-0) [et al.,](#page-10-0) [2023\)](#page-10-0) and prompting with structured data (struct), i.e., the model is queried to first represent the problem in a structured format such as JSON or Yaml. We further show that ToMi has been memorised *word for word* by GPT models, with CoT (and any technique that leaves the input un-changed) being the best-performing method. We then quantify the complexity of the benchmarks **338** introduced above and highlight the correlation with **339** the models' performances. Our framework shows **340** complexity ranges between easy and hard prob- **341** lems, even within a benchmark. We conduct our **342** experiments on GPT-3.5-Turbo, GPT-4 [\(OpenAI,](#page-9-13) **343** [2023\)](#page-9-13), LLaMA3-70B [\(AI@Meta,](#page-8-4) [2024\)](#page-8-4) and Mix- **344** tral 8x7B [\(Jiang et al.,](#page-8-5) [2024\)](#page-8-5). **345**

4.1 DWM on ToM Benchmarks **346**

We report results for GPT-3.5-Turbo and Mix-
347 tral 8x7B on the five ToM benchmarks: for rea- **348** sons of space, results for LLaMA3-8B, LLaMA3- **349** 70B and GPT-4 are reported in the Appendix, Sec- **350** tion [B.1.](#page-13-0) As illustrated in Figure [4](#page-5-0) (top), DWM **351** improves the performance of GPT-3.5-Turbo on **352** Mindgames, FANToM and Adv-CSFB by a solid **353** margin. On SocialIQa, which has very short in- **354** puts, DWM performs slightly worse than CoT but **355** better than ToT. On the other hand, on ToMi, the **356** best prompting techniques are CoT and ToT. As **357** analysed in the next section, we believe this not **358** be caused by memorisation, which we prove hap- **359** pening, but by the inherent complexity of the task. **360** With Mixtral 8x7B (Fig. [4](#page-5-0) (bottom)), DWM improves the performance on ADVcsfb, FANToM, **362** ToMi and Mindgames, and pairs that of CoT on **363** SocialIOa. 364

DWM elicits more informed *state spaces*. We **365** qualitatively analysed the information elicited by **366** an LLM when prompted with DWM and discov- **367** ered that it forces a model to output information **368** not explicitly available in the prompt. Consider **369** the ToMi example in Figure [5](#page-6-0) where GPT-4 is **370** prompted with a situation where agents interact **371**

Figure 4: Benchmarks of GPT-3.5-Turbo (top) and Mixtral 8x7B (bottom) models on different ToM tasks for DWM (one to five splits), CoT, ToT and structured prompts (JSON and Yaml).

Table 1: Summary of the memorisation test on five ToM benchmarks. We prompted GPT-3.5-Instruct to predict the continuation of 100 randomly sampled test points. We computed the exact and fuzzy memorisation rate (second row, similarity score computed via the Levenshtein distance, see the [thefuzz](https://github.com/seatgeek/thefuzz) package), which we complement with the best performance across models of CoT and DWM.

Table 2: Summary of the statefulness and statelessness of different ToM benchmarks. At the bottom, the value of the split that guarantees max performance of GPT-3.5-Turbo with DWM, which we notice is strongly correlated with the statefulness of each benchmark.

Figure 5: Example of a real ToMi example where GPT-4 fails when prompted with CoT, yet succeeds with DWM. CoT elicits an untruthful reasoning process (in red), while DWM correctly informs the model with the implicit information about Benjamin's first-order belief (in green). More examples are reported in the Appendix, Section [B.2.](#page-13-1)

Figure 6: Each boxplot summarizes the complexity analysis of the five ToM benchmarks in ascending order. We report the average error rate (i.e., 1-accuracy) of GPT-3.5-Turbo, GPT-4, Mixtral 8x7B and LLaMA3-70B on the task when prompted with CoT.

 and are then queried with the first-order belief of Benjamin. With CoT, the model makes an erro- neous assumption about the presence of Benjamin and Isabella in the room. On the other hand, when prompted with DWM, GPT-4 provides an informa- tive description of each *state space*, particularly the knowledge and the uncertainty of each agent's beliefs, and eventually answers correctly. One ex- ample per benchmark is available in the Appendix, Section [B.2,](#page-13-1) while many more are available for in- spection in the Code Supplementary Material. Such phenomenon is ubiquitous to all the ToM tasks we tested, a hint that DWM elicits the ToM capabilities of LLMs without requiring external information or **386** solvers.

387 Memorisation in Theory of Mind. Recent **388** works expressed concern about ToM benchmarks' efficacy in memorisation [\(Jacovi et al.,](#page-8-17) [2023;](#page-8-17) **389** [La Malfa et al.,](#page-9-25) [2024\)](#page-9-25). This motivated us to quan- **390** tify and then analyse the impact of memorisation **391** of ToM benchmarks on performance. We com- **392** puted the percentage of memorised prompts to un- **393** derstand whether that affects the performance of **394** techniques, such as DWM, that split the prompt **395** into chunks and introduce additional information **396** instead of CoT, which leaves the input prompt un- **397** changed. As illustrated in Table [1,](#page-5-1) ToMi and FAN- **398** ToM have been heavily memorised, with entire **399** portions of the benchmarks that can be retrieved **400** *word for word* from GPT-3.5-Instruct (the auto- 401 complete model by OpenAI). Despite that, no clear **402** evidence of a performance drop in DWM induced **403** by memorisation exists. For GPT-3.5, despite CoT **404** having higher performance on ToMi, DWM is bet- **405** ter on FANToM (Figure [4\)](#page-5-0). We hypothesise that as **406** long as a memorised problem is prompted, either **407** in its exact form (as for CoT) or split as in DWM, **408** the most potent models can recover it alongside **409** the ground truth label, thus invalidating the test for **410** both. We conclude with a note of caution. While **411** we discovered that ToMi and FANToM are memo- **412** rised by GPT-3.5-Instruct, that doesn't imply any **413** LLM, including GPT-3.5-Turbo and GPT-4, whose **414** training details are not released publicly, has been **415** trained on that data. **416**

4.2 Statefulness of ToM Benchmarks **417**

We used the complexity framework introduced in **418** Section [3.1](#page-1-0) to characterise the statefulness and 419 statelessness of the five ToM benchmarks used for **420** the experimental evaluation. We randomly sampled **421** 50 problems from each dataset, identified the ob- **422** jects, and manually labelled stateful and stateless **423**

Figure 7: Each boxplot summarizes the statefulness (left), statelessness (middle, y-axis in log-scale) and complexity analysis (right) of the five ToM benchmarks. We report mean, standard deviation and outliers alongside the best DWM method (by the number of prompt splits) and observe a strong correlation between the number of splits and the statefulness.

 state events. We release the split samples alongside a web application that facilitates manual labelling. As illustrated in Figure [7](#page-7-0) (left), the statefulness of each problem, i.e., that of the object a model must track to answer correctly, strongly correlates with the best-performing DWM split. The stateless- ness complexity, reported in Figure [7](#page-7-0) (middle), i.e., that of objects that a model does not need to track, grows larger for problems such as FANToM, only partially influencing the models' performance. We hypothesise that the most potent models developed some competency in discerning the relevant part of a prompt (the stateful events) from the confound- ing ones. We finally report, in Figure [7](#page-7-0) (right), the complexity of each problem computed as per Eq. [2,](#page-3-1) 439 with τ set in a range between 0.05 and 0.2 (i.e., the relative weight of stateless compared to stateful events). Results suggest that FANToM is the most difficult ToM task for humans and LLMs (see Fig- ure [4\)](#page-5-0), followed by ToMi (the second most difficult for LLMs as well) and Adv-CSFB (which seems easier than the others); in contrast, Mindgames and SocialIQa tend to be easier. Finally, in Figure [6,](#page-6-1) we compare the accuracy of GPT-3.5-Turbo, GPT-4, Mixtral 8x7B and LLaMA3-70B when prompted with CoT (i.e., without split) on the five ToM bench- marks with the complexity of the task as per Def. [2.](#page-3-1) We observe a strong correlation between the error- rate and the complexity of a task, i.e., our frame- work correctly identifies the tasks that are harder both for humans and current state-of-the-art LLMs.

⁴⁵⁵ 5 Conclusions

456 This paper introduces a complexity framework to **457** measure the difficulty of Theory of Mind (ToM) **458** problems. It quantifies the difficulty by tracking

necessary states (stateful) and unnecessary states **459** (stateless), with the latter discounted in the com- **460** plexity computation. The framework evidences a **461** strong correlation between complexity and model **462** performance. Inspired by this framework, we pro- **463** pose DWM, a prompting technique that splits a **464** prompt into parts to query a model for a consis- **465** tent representation of the environment and agents' **466** beliefs. DWM outperforms CoT and ToT by ex- **467** tracting implicit but relevant information. **468**

Limitations **⁴⁶⁹**

Higher order belief tracking. Our theoretical **470** framework reduces the problem of solving a belief **471** ToM problem to finding the correct descriptions **472** that need to be tracked. It extends seamlessly to **473** tasks with much higher complexity, however, we **474** have not had the opportunity to test this theory in **475** those settings. We noticed that most theory of mind **476** tasks available in the community only require one **477** to five states to be correctly answered. A possible **478** extension would be testing the theory upon tasks 479 with higher state complexity, e.g. kth -order belief 480 tracking tasks. However, it is unclear whether this **481** could be useful in real applications as most human **482** belief tracking is limited to 5 or 6 orders [\(Cargile,](#page-8-18) **483** [1970;](#page-8-18) [Dennett,](#page-8-6) [1988\)](#page-8-6). **484**

On task splitting methods. It is not straightfor- **485** ward to automatically find the correct task splits **486** in a manner that correctly describes the state. An **487** LLM could find a way to split it by itself correctly **488** and use those splits to answer the question. We at- **489** tempted this approach, yet with a simple prompting **490** method, the model splits every sentence, making **491** the descriptions much noisier and less accurate. **492** Future work could try to find the best splits auto- **493**

494 matically.

 Memorization analysis. Training and evaluating on the same dataset produce positively biased data on the model's performance. While running our benchmarks on ToMi, we discovered that the GPT- 3.5 model had completely memorized parts of the dataset. This motivated us to extend the memoriza- tion test to the other tasks. We urge the research community to include a memorization section on every benchmark study with public datasets used in their works. This data is crucial to conduct fair and unbiased research on evaluating LLMs' abili- ties [\(Jacovi et al.,](#page-8-17) [2023\)](#page-8-17). Future works will include an analysis of the memorisation rate of other ToM tasks alongside tests to quantify their impact on different models.

⁵¹⁰ Ethical Statement

 The datasets and pre-trained LLMs that we use are all publicly available. This paper focuses on ToM problems' hardness and prompting methods. We highlight that LLMs do not guarantee the pro- duction of factual data or correct reasoning steps, and the prompting methods developed here should not be regarded as the source of truth in making decisions.

⁵¹⁹ References

- **520** AI@Meta. 2024. [Llama 3 model card.](https://github.com/meta-llama/llama3/blob/main/MODEL_CARD.md)
- **521** Jaan Aru, Aqeel Labash, Oriol Corcoll, and Raul Vi-**522** cente. 2023. Mind the gap: Challenges of deep learn-**523** ing approaches to theory of mind. *Artificial Intelli-***524** *gence Review*, 56(9):9141–9156.
- **525** Chris Baker, Rebecca Saxe, and Joshua Tenenbaum. **526** 2011. [Bayesian Theory of Mind: Modeling Joint](https://escholarship.org/uc/item/5rk7z59q) **527** [Belief-Desire Attribution.](https://escholarship.org/uc/item/5rk7z59q)
- **528** Simon Baron-Cohen, Alan M. Leslie, and Uta Frith. **529** 1985. [Does the autistic child have a "theory of mind"](https://doi.org/10.1016/0010-0277(85)90022-8) **530** [?](https://doi.org/10.1016/0010-0277(85)90022-8) 21(1):37–46.
- **531** Sébastien Bubeck, Varun Chandrasekaran, Ronen El-**532** dan, Johannes Gehrke, Eric Horvitz, Ece Kamar, Pe-**533** ter Lee, Yin Tat Lee, Yuanzhi Li, Scott Lundberg, **534** Harsha Nori, Hamid Palangi, Marco Tulio Ribeiro, **535** and Yi Zhang. 2023. [Sparks of Artificial General](https://arxiv.org/abs/2303.12712) **536** [Intelligence: Early experiments with GPT-4.](https://arxiv.org/abs/2303.12712)
- **537** James Cargile. 1970. [A note on" iterated knowings".](https://www.jstor.org/stable/3328051) **538** *Analysis*, 30(5):151–155.
- **539** Zhuang Chen, Jincenzi Wu, Jinfeng Zhou, Bosi Wen, **540** Guanqun Bi, Gongyao Jiang, Yaru Cao, Mengt-**541** ing Hu, Yunghwei Lai, Zexuan Xiong, et al. 2024.

Tombench: Benchmarking theory of mind in large **542** language models. *arXiv preprint arXiv:2402.15052*. **543**

- Paul M Churchland. 2013. Folk psychology and the **544** explanation of human behavior 1. In *Folk psychology* **545** *and the philosophy of mind*, pages 247–262. Psychol- **546** ogy Press. **547**
- Daniel C. Dennett. 1988. The intentional stance in **548** theory and practice. In *Machiavellian Intelligence:* **549** *Social Expertise and the Evolution of Intellect in* **550** *Monkeys, Apes, and Humans*, pages 180–202. Claren- **551** don Press/Oxford University Press. **552**
- Kanishk Gandhi, Gala Stojnic, Brenden M. Lake, and **553** Moira R. Dillon. 2022. [Baby Intuitions Benchmark](https://arxiv.org/abs/2102.11938) **554** [\(BIB\): Discerning the goals, preferences, and actions](https://arxiv.org/abs/2102.11938) **555** [of others.](https://arxiv.org/abs/2102.11938) **556**
- [A](https://doi.org/10.1017/CBO9780511752902.011)lison Gopnik and Henry M. Wellman. 1994. [The](https://doi.org/10.1017/CBO9780511752902.011) 557 [theory theory.](https://doi.org/10.1017/CBO9780511752902.011) In Lawrence A. Hirschfeld and Su- **558** san A. Gelman, editors, *Mapping the Mind: Domain* **559** *Specificity in Cognition and Culture*, pages 257–293. **560** Cambridge University Press. **561**
- Sven Gronauer and Klaus Diepold. 2022. Multi-agent **562** deep reinforcement learning: a survey. *Artificial* **563** *Intelligence Review*, 55(2):895–943. **564**
- [D](https://doi.org/10.5281/zenodo.1207631)avid Ha and Jürgen Schmidhuber. 2018. [World Mod-](https://doi.org/10.5281/zenodo.1207631) **565** [els.](https://doi.org/10.5281/zenodo.1207631) **566**
- Shibo Hao, Yi Gu, Haodi Ma, Joshua Hong, Zhen **567** Wang, Daisy Wang, and Zhiting Hu. 2023. [Rea-](https://doi.org/10.18653/v1/2023.emnlp-main.507) **568** [soning with language model is planning with world](https://doi.org/10.18653/v1/2023.emnlp-main.507) **569** [model.](https://doi.org/10.18653/v1/2023.emnlp-main.507) In *Proceedings of the 2023 Conference on* **570** *Empirical Methods in Natural Language Processing*, **571** pages 8154–8173, Singapore. Association for Com- **572** putational Linguistics. **573**
- Alon Jacovi, Avi Caciularu, Omer Goldman, and Yoav **574** Goldberg. 2023. [Stop uploading test data in plain](https://arxiv.org/abs/2305.10160) **575** [text: Practical strategies for mitigating data contam-](https://arxiv.org/abs/2305.10160) **576** [ination by evaluation benchmarks.](https://arxiv.org/abs/2305.10160) *ArXiv preprint*, **577** abs/2305.10160. **578**
- Albert Q Jiang, Alexandre Sablayrolles, Antoine **579** Roux, Arthur Mensch, Blanche Savary, Chris Bam- **580** ford, Devendra Singh Chaplot, Diego de las Casas, **581** Emma Bou Hanna, Florian Bressand, et al. 2024. **582** Mixtral of experts. *arXiv preprint arXiv:2401.04088*. **583**
- Hyunwoo Kim, Melanie Sclar, Xuhui Zhou, Ronan Le **584** Bras, Gunhee Kim, Yejin Choi, and Maarten Sap. **585** 2023. [FANToM: A Benchmark for Stress-testing](https://arxiv.org/abs/2310.15421) **586** [Machine Theory of Mind in Interactions.](https://arxiv.org/abs/2310.15421) **587**
- [N](https://arxiv.org/abs/2305.02363)ajoung Kim and Sebastian Schuster. 2023. [En-](https://arxiv.org/abs/2305.02363)
tity tracking in language models. Preprint. 589 [tity tracking in language models.](https://arxiv.org/abs/2305.02363) Preprint, arXiv:2305.02363. **590**
- Najoung Kim, Sebastian Schuster, and Shubham Tosh- **591** niwal. 2024. [Code pretraining improves entity](https://arxiv.org/abs/2405.21068) **592** [tracking abilities of language models.](https://arxiv.org/abs/2405.21068) *Preprint*, **593** arXiv:2405.21068. **594**

-
-
-
-
-
-
-
-

-
-
-
- **595** Michal Kosinski. 2023. Theory of mind may have spon-**596** taneously emerged in large language models. *arXiv* **597** *preprint arXiv:2302.02083*, 4:169.
- **598** Emanuele La Malfa, Aleksandar Petrov, Simon Frieder, **599** Christoph Weinhuber, Ryan Burnell, Raza Nazar, **600** Anthony G. Cohn, Nigel Shadbolt, and Michael **601** Wooldridge. 2023. [Language Models as a Service:](https://doi.org/10.48550/arXiv.2309.16573) **602** [Overview of a New Paradigm and its Challenges.](https://doi.org/10.48550/arXiv.2309.16573)
- **603** Emanuele La Malfa, Christoph Weinhuber, Orazio **604** Torre, Fangru Lin, Anthony Cohn, Nigel Shadbolt, **605** and Michael Wooldridge. 2024. [Code Simulation](https://arxiv.org/abs/2401.09074) **606** [Challenges for Large Language Models.](https://arxiv.org/abs/2401.09074)
- **607** Matthew Le, Y-Lan Boureau, and Maximilian Nickel. **608** 2019. [Revisiting the Evaluation of Theory of Mind](https://doi.org/10.18653/v1/D19-1598) **609** [through Question Answering.](https://doi.org/10.18653/v1/D19-1598) In *Proceedings of* **610** *the 2019 Conference on Empirical Methods in Natu-***611** *ral Language Processing and the 9th International* **612** *Joint Conference on Natural Language Processing* **613** *(EMNLP-IJCNLP)*, pages 5871–5876. Association **614** for Computational Linguistics.
- **615** Belinda Z. Li, Maxwell Nye, and Jacob Andreas. 2021. **616** [Implicit representations of meaning in neural lan-](https://arxiv.org/abs/2106.00737)**617** [guage models.](https://arxiv.org/abs/2106.00737) *Preprint*, arXiv:2106.00737.
- **618** Kenneth Li, Aspen K Hopkins, David Bau, Fernanda **619** Viégas, Hanspeter Pfister, and Martin Wattenberg. **620** 2022. Emergent world representations: Exploring a **621** sequence model trained on a synthetic task. *arXiv* **622** *preprint arXiv:2210.13382*.
- **623** Kyle Mahowald, Anna A Ivanova, Idan A Blank, Nancy **624** Kanwisher, Joshua B Tenenbaum, and Evelina Fe-**625** dorenko. 2024. Dissociating language and thought in **626** large language models. *Trends in Cognitive Sciences*.
- **627** John McCarthy. 1979. Ascribing Mental Qualities To **628** Machines.
- **629** Shima Rahimi Moghaddam and Christopher J. Honey. **630** 2023. [Boosting theory-of-mind performance in](https://arxiv.org/abs/2304.11490) **631** [large language models via prompting.](https://arxiv.org/abs/2304.11490) *Preprint*, **632** arXiv:2304.11490.
- **633** Maxwell Nye, Anders Johan Andreassen, Guy Gur-Ari, **634** Henryk Michalewski, Jacob Austin, David Bieber, **635** David Dohan, Aitor Lewkowycz, Maarten Bosma, **636** David Luan, et al. 2021. Show your work: Scratch-**637** pads for intermediate computation with language **638** models. *arXiv preprint arXiv:2112.00114*.
- **639** OpenAI. 2023. [GPT-4 technical report.](https://arxiv.org/abs/2303.08774) *ArXiv preprint*, **640** abs/2303.08774.
- **641** Joon Sung Park, Joseph C. O'Brien, Carrie J. Cai, **642** Meredith Ringel Morris, Percy Liang, and Michael S. **643** Bernstein. 2023. [Generative agents: Interac-](https://arxiv.org/abs/2304.03442)**644** [tive simulacra of human behavior.](https://arxiv.org/abs/2304.03442) *Preprint*, **645** arXiv:2304.03442.
- **646** [D](https://doi.org/10.1017/S0140525X00076512)avid Premack and Guy Woodruff. 1978. [Does the](https://doi.org/10.1017/S0140525X00076512) **647** [chimpanzee have a theory of mind?](https://doi.org/10.1017/S0140525X00076512) 1(4):515–526.
- Stephanie D Preston and Frans BM De Waal. 2002. Em- **648** pathy: Its ultimate and proximate bases. *Behavioral* **649** *and brain sciences*, 25(1):1–20. **650**
- Neil C. Rabinowitz, Frank Perbet, H. Francis Song, **651** Chiyuan Zhang, S. M. Ali Eslami, and Matthew **652** Botvinick. 2018. [Machine Theory of Mind.](https://doi.org/10.48550/arXiv.1802.07740) **653**
- Maarten Sap, Ronan LeBras, Daniel Fried, and Yejin **654** Choi. 2023. [Neural Theory-of-Mind? On the Limits](https://arxiv.org/abs/2210.13312) **655** [of Social Intelligence in Large LMs.](https://arxiv.org/abs/2210.13312) **656**
- Maarten Sap, Hannah Rashkin, Derek Chen, Ronan **657** Le Bras, and Yejin Choi. 2019. [Social IQa: Com-](https://doi.org/10.18653/v1/D19-1454) **658** [monsense Reasoning about Social Interactions.](https://doi.org/10.18653/v1/D19-1454) In **659** *Proceedings of the 2019 Conference on Empirical* **660** *Methods in Natural Language Processing and the* **661** *9th International Joint Conference on Natural Lan-* **662** *guage Processing (EMNLP-IJCNLP)*, pages 4463– **663** 4473. Association for Computational Linguistics. **664**
- [B](https://doi.org/10.1023/A:1013298507114)rian Scassellati. 2002. [Theory of Mind for a Hu-](https://doi.org/10.1023/A:1013298507114) **665** [manoid Robot.](https://doi.org/10.1023/A:1013298507114) 12(1):13–24. **666**
- Natalie Shapira, Mosh Levy, Seyed Hossein Alavi, **667** Xuhui Zhou, Yejin Choi, Yoav Goldberg, Maarten **668** Sap, and Vered Shwartz. 2023. [Clever Hans or Neu-](https://doi.org/10.48550/arXiv.2305.14763) **669** [ral Theory of Mind? Stress Testing Social Reasoning](https://doi.org/10.48550/arXiv.2305.14763) **670** [in Large Language Models.](https://doi.org/10.48550/arXiv.2305.14763) **671**
- Damien Sileo and Antoine Lernould. 2023. **672** [MindGames: Targeting Theory of Mind in](https://doi.org/10.48550/ARXIV.2305.03353) **673** [Large Language Models with Dynamic Epistemic](https://doi.org/10.48550/ARXIV.2305.03353) **674** [Modal Logic.](https://doi.org/10.48550/ARXIV.2305.03353) 675
- James WA Strachan, Dalila Albergo, Giulia Borghini, **676** Oriana Pansardi, Eugenio Scaliti, Saurabh Gupta, **677** Krati Saxena, Alessandro Rufo, Stefano Panzeri, **678** Guido Manzi, et al. 2024. Testing theory of mind in **679** large language models and humans. *Nature Human* **680** *Behaviour*, pages 1–11. **681**
- Michael Tomasello. 2009. *The cultural origins of hu-* **682** *man cognition*. Harvard university press. **683**
- Shubham Toshniwal, Sam Wiseman, Karen Livescu, **684** and Kevin Gimpel. 2021. [Learning chess blindfolded:](https://arxiv.org/abs/2102.13249) **685** [Evaluating language models on state tracking.](https://arxiv.org/abs/2102.13249) *CoRR*, **686** abs/2102.13249. **687**
- [T](https://doi.org/10.48550/arXiv.2302.08399)omer Ullman. 2023. [Large Language Models Fail on](https://doi.org/10.48550/arXiv.2302.08399) **688** [Trivial Alterations to Theory-of-Mind Tasks.](https://doi.org/10.48550/arXiv.2302.08399) **689**
- Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten **690** Bosma, Brian Ichter, Fei Xia, Ed Chi, Quoc Le, and **691** Denny Zhou. 2022. [Chain-of-Thought Prompting](https://doi.org/10.48550/arXiv.2201.11903) **692** [Elicits Reasoning in Large Language Models.](https://doi.org/10.48550/arXiv.2201.11903) **693**
- [H](https://doi.org/10.1111/cdep.12236)enry M. Wellman. 2017. [The Development of Theory](https://doi.org/10.1111/cdep.12236) **694** [of Mind: Historical Reflections.](https://doi.org/10.1111/cdep.12236) 11(3):207–214. **695**
- [H](https://doi.org/10.1016/0010-0277(83)90004-5)einz Wimmer and Josef Perner. 1983. [Beliefs about](https://doi.org/10.1016/0010-0277(83)90004-5) **696** [beliefs: Representation and constraining function of](https://doi.org/10.1016/0010-0277(83)90004-5) **697** [wrong beliefs in young children's understanding of](https://doi.org/10.1016/0010-0277(83)90004-5) **698** [deception.](https://doi.org/10.1016/0010-0277(83)90004-5) 13(1):103–128. **699**
- Lionel Wong, Gabriel Grand, Alexander K. Lew, Noah D. Goodman, Vikash K. Mansinghka, Jacob Andreas, and Joshua B. Tenenbaum. 2023. [From](https://arxiv.org/abs/2306.12672) [Word Models to World Models: Translating from](https://arxiv.org/abs/2306.12672) [Natural Language to the Probabilistic Language of](https://arxiv.org/abs/2306.12672) [Thought.](https://arxiv.org/abs/2306.12672)
- Shunyu Yao, Dian Yu, Jeffrey Zhao, Izhak Shafran, Thomas L. Griffiths, Yuan Cao, and Karthik Narasimhan. 2023. [Tree of Thoughts: Deliberate](https://arxiv.org/abs/2305.10601) [Problem Solving with Large Language Models.](https://arxiv.org/abs/2305.10601)
- Denny Zhou, Nathanael Schärli, Le Hou, Jason Wei, Nathan Scales, Xuezhi Wang, Dale Schuurmans, Claire Cui, Olivier Bousquet, Quoc V Le, and Ed H. Chi. 2023a. [Least-to-most prompting enables com-](https://openreview.net/forum?id=WZH7099tgfM) [plex reasoning in large language models.](https://openreview.net/forum?id=WZH7099tgfM) In *The Eleventh International Conference on Learning Rep-resentations*.
- Pei Zhou, Aman Madaan, Srividya Pranavi Potharaju, Aditya Gupta, Kevin R. McKee, Ari Holtzman, Jay Pujara, Xiang Ren, Swaroop Mishra, Aida Ne- matzadeh, Shyam Upadhyay, and Manaal Faruqui. 2023b. [How far are large language models from](https://arxiv.org/abs/2310.03051) [agents with theory-of-mind?](https://arxiv.org/abs/2310.03051)

754

767

⁷²³ A Experimental Setup

724 A.1 Experimental Details

 Most of the language models used in this work fol- low the Language Models as a Service (LMaaS) paradigm [\(La Malfa et al.,](#page-9-26) [2023\)](#page-9-26). This model of ser- vice does not allow transparency and hinders repro- ducibility. Reproducibility is difficult to achieve as common software development frameworks, such as CI/CD pipeline, ease the update of the public service, but change the underlying entity. From this follows that the model tested by the researcher could change at any time. This is not solvable from the outside. Researchers have no control over the software engineering practices inside a LMaaS, but could set some parameters to offer the highest pos- sible grade of reproducibility. We set the tempera- ture to zero or enable greedy decoding by default (this does not imply determinism even if model 741 weights are not changed). ^{[2](#page-11-0)} In prompting methods where the creativity of the response is exploited [f](#page-10-0)or better performance, e.g., Tree of Thoughts [\(Yao](#page-10-0) [et al.,](#page-10-0) [2023\)](#page-10-0), we set the temperature to 0.7, the value proposed in the reference papers.

 LMaaS providers. We use [Huggingface](https://huggingface.co/) for Mixtral 8x7B. Groq Cloud for LLama-3-7B and LLama-3-70B. Microsoft sponsorship for GPT-3.5 and GPT-4 access.

750 A.2 Prompting Templates

751 We present the different prompting techniques, tak-**752** ing as an example the following prompt from ToMi **753** and GPT-3.5-Turbo as the reference model:

1. Benjamin entered the workshop. 2. Isabella entered the workshop. 3. Hannah entered the workshop. 4. Isabella hates the onion 5. Hannah hates the t-shirt 6. The pajamas is in the bottle. 7. Isabella moved the pajamas to the drawer. 8. Benjamin exited the workshop. 9. Isabella exited the workshop. 10. Benjamin entered the workshop. **⁷⁶⁵** And the following question:

768 Where does Benjamin think that Isabella **⁷⁶⁹** searches for the pajamas? **⁷⁷⁰**

771 Chain of Thought

803

808

819

822

tion paths to solve a task. **802**

We then pick the best idea via a majority vote over 827 three agents simulated by the LLM itself: **828**

4. Isabella hates the onion **839**

²The main explanation are the [https://github.com/](https://github.com/pytorch/pytorch/issues/75240) [pytorch/pytorch/issues/75240](https://github.com/pytorch/pytorch/issues/75240)"non deterministic cuda cores" another could "be batched inference in sparse MoE models", see [https://152334h.github.io/blog/](https://152334h.github.io/blog/non-determinism-in-gpt-4/) [non-determinism-in-gpt-4/](https://152334h.github.io/blog/non-determinism-in-gpt-4/)here

842 7. Isabella moved the pajamas to the drawer.

840 5. Hannah hates the t-shirt **841** 6. The pajamas is in the bottle.

846

850 849 prompt.

852

867

870

873

877

891

902

905

908

843 8. Benjamin exited the workshop.

845 10. Benjamin entered the workshop.

844 9. Isabella exited the workshop.

- **883** # 1. Write down a succinct description of what **884** each agent knows about the environment and **885** about the other agents. Keep the **886** description short and do not produce 887 **redundant information.**
888 **#2. Each considerations vo**
- **888** # 2. Each considerations you make must be **889** preceded by the symbol #GPT#.

890 Here's the dialogue:

- **892** 1. Benjamin entered the workshop.
- **893** 2. Isabella entered the workshop.
- 894 3. Hannah entered the workshop.
895 4. Isabella hates the onion
	- **895** 4. Isabella hates the onion
- **896** 5. Hannah hates the t-shirt
- **897** 6. The pajamas is in the bottle.
- **898** 7. Isabella moved the pajamas to the drawer.
- **899** 8. Benjamin exited the workshop.
- **900** 9. Isabella exited the workshop.
- **901** 10. Benjamin entered the workshop.
- **903** This is the end of the dialogue. Now, this is a **904** question for you to answer.
- **906** Question: Where does Benjamin think that **907** Isabella searches for the pajamas?

Discrete World Model - 3 Split 914

prompt).

- 1004 **Now give a structured representation of the**
1005 **dialogue in YAML format. Keep track of** dialogue in YAML format. Keep track of the 1006 **information that each agent has access to**
1007 **at each point in the dialogue.** at each point in the dialogue.
- It is important to have a relative representation of the information that each agent has access to at each point in the dialogue. **¹⁰¹²**

B Additional Results

B.1 DWM Prompting

 In this section, and, in particular in Figure [8,](#page-14-0) we report results for LLaMA3-7B, LLaMA3-70B and GPT-4 on the five ToM benchmarks and for differ- ent prompting techniques, namely DWM (one to five splits), JSON, Yaml, CoT and ToT.

 B.2 DWM Elicits More Informed Mental States in LLMs

 In this section, we report and discuss an example of a real prompt and the answers provided by GPT-4 for each ToM task we evaluated in this paper. For FANToM (Figure [10\)](#page-15-0), we just reported the portion of the prompt that induces an unfaithful reasoning process in GPT-4, due to the prohibitive length of the input prompts. Results for ToMi, FANToM, ADV-csfb, Mindgames and SocialIQa are reported respectively in Figures [9,](#page-15-1) [10,](#page-15-0) [11,](#page-16-0) [12](#page-17-0) and [13.](#page-18-0)

Figure 8: Benchmarks of LLaMA3-7B (top), LLaMA3-70B (middle) and GPT-4 (bottom) models on different ToM tasks for DWM (one to five splits), CoT, ToT and structured prompts (JSON and Yaml). For GPT-4 and ToT, we tested 50 samples (instead of 1000).

Figure 9: Example of a real ToMi example where GPT-4 fails when prompted with CoT, yet succeeds with DWM. CoT elicits an untruthful reasoning process (in red), while DWM correctly informs the model with the correct information about Benjamin's first-order belief (in green).

Input Prompt

 $[...]$

Conor: Raegan, you were saying about being a vegetarian. Has it had a big impact on your personal life?

Raegan: Absolutely, Conor. It's definitely been a transformation. Initially, it was challenging to find vegetarian alternatives to my favorite meals, but over time, it's made me be more aware of what I'm eating. It's also made me try out a lot of new and interesting foods, vegan ones included! **Conor:** That's really insightful. I've been considering it, mainly for health reasons, but haven't taken

the leap yet. Maybe trying out that vegan restaurant is a good place to start.

Raegan: Definitely! Exploring yegan or yegetarian food can be a great first step. The variety and flavors might surprise you! Conor: I'll keep that in mind. It's always exciting to discover something new!

Brittney: Hey guys, I'm back! I find our talks about food trends so interesting. Γ . 1

Ouestion

What does Brittney believe were Conor's primary motivations for considering a shift to vegetarianism?

Chain of Thoughts

"Based on the dialogue, Brittney did not explicitly state what she believes Conor's primary motivations are for considering a shift to vegetarianism. However, Conor himself mentions that he has been considering vegetarianism mainly for health reasons. Thus, if Brittney is aware of this part of the conversation, she would likely think that health reasons are Conor's primary motivation for considering the change to a vegetarian diet. <answer>**Health reasons**</answer>" $\mathbf{\times}$ "

Discrete World Models

"Brittney knows that she was part of a conversation with Conor and Raegan. She had to leave **temporarily due to her parking meter expiring.** She also knows that the conversation was about food trends, specifically vegetarianism and veganism, and finds it interesting [...] She also knows that **Conor is considering becoming a vegetarian** and has suggested trying out vegan or vegetarian food as a first step. [...] <answer>brittney doesn't have information about conor's primary motivations for considering a shift to vegetarianism as she was not present during that part of the conversation. </answer>" \bigvee

Figure 10: Example of a real FANToM example where GPT-4 fails when prompted with CoT, yet succeeds with DWM. CoT elicits an untruthful reasoning process (in red), while DWM correctly informs the model with the correct information about the partial observability Brittney has about Conor (in green).

Input Prompt

There is a closed glass box on the table of an empty meeting room, in which a seminar is about to take place.

Ouestion

Fill in the blank with the best option. She loves writing with

- pens

pencils

Chain of Thoughts

"Based on the information provided, the attendee reads the label on the box marked "pencils" and feels delighted upon finding it. This suggests that she has a preference for what she believes the box contains, which according to the label are pencils, even though the box actually contains **pens.** Therefore, the best answer, given her reaction to the label, would be:

<answer>**pencils**</answer>

Discrete World Models

"Agent: James

James knows that the box on the table is filled with pens, not pencils, despite the label saving "pencils". He knows that he labeled the box himself. He is aware of his own actions and the contents of the box. He also knows that he is alone in the room and that a seminar is about to take place. <answer>pens</answer>" √

Figure 11: Example of a real ADV-csfb example where GPT-4 fails when prompted with CoT, yet succeeds with DWM. CoT elicits an untruthful reasoning process (in red), while DWM correctly informs the model with the correct information about the content of the glass box (in green).

Input Prompt

There are three persons. Everyone is visible to others. Each person draws a card, face unrevealed (red or black). Leah's card is shown to Leah. Raymond's card is shown to Leah. Brittney's card is shown to Leah. Raymond's card is shown to Raymond. It is publicly announced that someone picked a red card.

Question

Leah can now know that Raymond can know whether or not nobody picked a red card. Is the above statement in entailment or contradiction with the previous situation?

Chain of Thoughts

"In the given situation, Leah sees Raymond's card and Brittney's card, but she does not see her own card. It is publicly announced that someone picked a red card, but **Leah cannot determine whether it** was Raymond or Brittney who picked the red card based on the information she has. \langle <answer>contradiction \langle /answer>

Discrete World Models

"Leah: Knows the color of her own card. Does not know the color of the other two persons' cards. Knows that the other two persons can see her.

Other two persons: Do not know the color of their own cards or each other's cards. Knows that Leah knows the color of her card. Knows that Leah can see them.

Leah: Knows the color of her own card, Raymond's card, and Brittney's card. Knows that Raymond knows the color of his card. Knows that someone picked a red card. Raymond: Knows the color of his own card. Does not know the color of Leah's or Brittney's cards. Knows that Leah knows the color of his card and Brittney's card. Knows that someone picked a red card.

Brittney: Does not know the color of her own card or Raymond's card. Knows that Leah knows the color of her card and Raymond's card. Knows that Raymond knows the color of his card. Knows that someone picked a red card. <answer>entailment</answer>" v

Figure 12: Example of a real Mindgames example where GPT-4 fails when prompted with CoT, vet succeeds with DWM. CoT elicits an untruthful reasoning process (in red), while DWM correctly informs the model with the correct information about the knowledge Leah has about Raymond (in green).

Input Prompt

Skylar was pushed by the bully in the lunch line, so Skylar poured milk over their head.

Ouestion

Consider the following statement, you will need to infer the correct response. At the end, I will ask you a question to answer.

Here's the statement:

Skylar was pushed by the bully in the lunch line, so Skylar poured milk over their head.

This is the end of the dialogue. Now, this is a question for you to answer.

Question: What will Skylar want to do next?

- 1: Run away
- 2: Wait for a reaction
- 3: wanted to fight with the bully

Chain of Thoughts

"Based on the statement, Skylar's response to being pushed by the bully was to pour milk over their head. This suggests that Skylar wanted to retaliate or stand up to the bully, indicating a desire to fight back.

 \langle <answer>3: wanted to fight with the bully \langle /answer> $\mathbf{\times}$

Discrete World Models

"Agent: Skylar Knowledge about the environment: Skylar knows they are in a lunch line and that there is a bully present. Skylar also knows they have access to milk. Knowledge about other agents: Skylar knows the bully is aggressive and has pushed them.

Agent: The Bully Knowledge about the environment: The bully knows they are in a lunch line and that Skylar is present. Knowledge about other agents: The bully knows Skylar is someone they can push around, but may not anticipate Skylar's retaliatory action.

<answer>1: Run away</answer>"

Figure 13: Example of a real SocialIOa example where GPT-4 fails when prompted with CoT, yet succeeds with DWM. CoT elicits an untruthful reasoning process (in red), while DWM correctly informs the model with the correct next actionSkylar will take (in green).