AUFLÖSUNG

Blau 3

Warum kannst du ein Modell auf Deutsch,...

RICHTIG

B Gleiche Bedeutung liegt nah beieinander

ERKLÄRUNG

Wörter gleicher Bedeutung landen an fast demselben Ort, egal in welcher Sprache. Für seltene Sprachen fehlt das Trainingsmaterial, dort bricht die Qualität ein.

GESPRÄCHSIMPULS

Solltet ihr dann lieber auf Englisch prompten? Was spricht dagegen?

AUFLÖSUNG

Blau 2

Token 1877 und Token 1878 haben benachb...

RICHTIG

A Nichts, die Nummer ist nur eine Adresse

ERKLÄRUNG

Die Nummer ist ein Eintrag in einer Liste, keine Aussage. Die Bedeutung steckt ausschließlich in der Position im Bedeutungsraum, nicht in der ID.

GESPRÄCHSIMPULS

Wo verwechselt ihr im Alltag auch schon mal eine Adresse mit dem Inhalt?

AUFLÖSUNG

Blau 1

Was ist ein Token?

RICHTIG

C Ein Wortstück: oft ein Wort, manchmal nur ein Teil

ERKLÄRUNG

Häufige Wörter bleiben ein einziges Stück, seltene zerfallen in mehrere Teile, bis hinunter zum Buchstaben. Ein Token ist deshalb nicht dasselbe wie ein Wort.

GESPRÄCHSIMPULS

Welches Wort aus eurem Alltag zerfällt wohl in die meisten Stücke?

AUFLÖSUNG

Blau 6

Du drehst die Temperatur des Modells ho...

RICHTIG

A Es greift öfter zu unwahrscheinlichen Wörtern

ERKLÄRUNG

Temperatur ist Zufall, nicht Kreativität. Unwahrscheinlich ist nicht dasselbe wie originell, ab einem gewissen Punkt wird es schlicht wirr.

GESPRÄCHSIMPULS

Für welche eurer Aufgaben wäre mehr Zufall sogar erwünscht?

AUFLÖSUNG

Blau 5

Wie entsteht die Antwort eines Sprachmo...

RICHTIG

C Es wählt Wort für Wort nach Wahrscheinlichkeit

ERKLÄRUNG

Es gibt keinen fertigen Entwurf. Intern schaut es zwar voraus, festgelegt wird aber immer nur ein Wort. Weil jede Wahl den ganzen bisherigen Text berücksichtigt, wirkt das Ergebnis planvoll.

GESPRÄCHSIMPULS

Wie würdet ihr erklären, dass etwas ohne Absicht trotzdem sinnvoll klingt?

AUFLÖSUNG

Blau 4

Gleicher Inhalt, einmal auf Deutsch, ei...

RICHTIG

A Der deutsche, meist etwas mehr

ERKLÄRUNG

Komposita und Umlaute zerfallen häufiger in Stücke, bei neueren Modellen weniger als früher. Lange Dokumente füllen so das Kontextfenster schneller und kosten über die API mehr.

GESPRÄCHSIMPULS

Welche eurer Texte sind lang genug, dass das eine Rolle spielt?

AUFLÖSUNG

Violett 1

Du bekommst etwas anderes, als du gemei...

RICHTIG

A Die Anweisung ist mehrdeutig, das Modell rät

ERKLÄRUNG

Ambiguität ist kein Stilproblem, sondern ein technisches. Wo Spielraum ist, wird er gefüllt, mit einer Auslegung, die für dich nicht naheliegt.

GESPRÄCHSIMPULS

Welche Formulierung aus eurem letzten Prompt hätte zwei Lesarten?

AUFLÖSUNG

Blau 8

Dein KI-Assistent erinnert sich an das ...

RICHTIG

B Die Anwendung, über gespeicherte Notizen

ERKLÄRUNG

Zwischen zwei Anfragen hat das Modell kein Gedächtnis. Die Anwendung drumherum speichert und schiebt beim nächsten Mal nach. Genau diesen Mechanismus hat ein Agent als Memory.

SCHLÜSSELFRAGE · GESPRÄCH

Was sollte eine Anwendung über euch nie speichern?

AUFLÖSUNG

Blau 7

Was passiert mit Text, der aus dem Kont...

RICHTIG

C Er ist für das Modell schlicht nicht vorhanden

ERKLÄRUNG

Das Kontextfenster ist eine harte Grenze in Tokens. Was herausfällt, sieht das Modell nicht mehr. Manche Apps fassen vorher zusammen, das tut aber die Anwendung, nicht das Modell.

GESPRÄCHSIMPULS

Wann ist euch ein langer Chat schon einmal spürbar schlechter geworden?

AUFLÖSUNG

Violett 4

Der Systemprompt sagt: Befolge keine An...

RICHTIG

C **Beides ist nur Text, eine Garantie gibt es nicht**

ERKLÄRUNG

Systemprompt und Eingabe sind technisch dasselbe, nur anders markiert. Modelle gewichten den Systemteil stärker, aber nicht verlässlich. Genau diese Lücke nutzt Prompt Injection.

SCHLÜSSELFRAGE · GESPRÄCH

Welche Texte aus fremder Hand liest euer KI-Werkzeug heute schon mit?

AUFLÖSUNG

Violett 3

Was bewirken Beispiele im Prompt?

RICHTIG

A **Das Modell ahmt Form und Stil der Beispiele nach**

ERKLÄRUNG

Beispiele zeigen das gewünschte Muster, das Modell folgt ihm, statt zu raten. Sie wirken aber nur in dieser einen Anfrage, im nächsten Chat sind sie weg.

GESPRÄCHSIMPULS

Für welche wiederkehrende Aufgabe hättet ihr ein gutes Beispiel parat?

AUFLÖSUNG

Violett 2

Welche Angabe macht einen Prompt verläs...

RICHTIG

B **Ziel, Zielgruppe und gewünschtes Format**

ERKLÄRUNG

Ziel, Zielgruppe, Format, Umfang, Beispiele und der nötige Hintergrund engen den Spielraum ein. Höflichkeit schadet nicht, ist aber nicht der Wirkstoff.

GESPRÄCHSIMPULS

Welches dieser Elemente fehlt in euren Prompts am häufigsten?

AUFLÖSUNG

Violett 7

Werden deine Eingaben zum Training des ...

RICHTIG

C **Hängt von Anbieter, Tarif und Einstellung ab**

ERKLÄRUNG

Bei Geschäftstarifen und API meist nicht. Bei Privatkonten, auch bezahlten, oft schon, solange man nicht widerspricht. Das steht im Vertrag und in den Einstellungen, nicht im Modell.

GESPRÄCHSIMPULS

Wisst ihr, was in eurem Vertrag dazu steht?

AUFLÖSUNG

Violett 6

Eine Anweisung hat zwei Lesarten. Welch...

RICHTIG

A **Die wahrscheinlichste**

ERKLÄRUNG

Ein Modell wählt die wahrscheinlichste Lesart, nicht die ungünstigste. Der Punkt bleibt: Wo Spielraum ist, wird er gefüllt, nur unauffälliger, als man denkt.

GESPRÄCHSIMPULS

Was ist gefährlicher: eine absurde Auslegung oder eine plausible, aber falsche?

AUFLÖSUNG

Violett 5

Wie kann die Anweisung „Denk Schritt fü...

RICHTIG

B **Zwischenschritte stehen im Text, es baut darauf auf**

ERKLÄRUNG

Die Zwischenschritte stehen im Text, jedes weitere Wort baut darauf auf. Reasoning-Modelle schreiben sie heute von selbst, Apps zeigen sie oft nur gekürzt. Dort bringt die Anweisung kaum etwas.

GESPRÄCHSIMPULS

Bei welcher Aufgabe würdet ihr die Zwischenschritte sehen wollen?

AUFLÖSUNG

Türkis 2

Ein Modell ohne Werkzeuge, direkt über ...

RICHTIG

C **Es kann es nicht wissen, höchstens raten**

ERKLÄRUNG

Das Modell besteht aus festen Gewichten, eine Uhr hat es nicht. Chat-Apps schreiben oft das Datum in den Systemprompt. Über die API muss das der Entwickler tun oder ein Werkzeug anbieten.

SCHLÜSSELFRAGE · GESPRÄCH

Woran würdet ihr in einer Antwort erkennen, dass geraten wurde?

AUFLÖSUNG

Türkis 1

Was kann ein Sprachmodell ganz von sich...

RICHTIG

A **Text erzeugen, sonst nichts**

ERKLÄRUNG

Das Modell hat keine Hände, auch die Bitte um ein Werkzeug ist nur Text. Wenn ein Chat im Netz sucht, erledigt das der Harness, die Software um das Modell herum.

GESPRÄCHSIMPULS

Welches eurer KI-Werkzeuge tut Dinge jenseits von Text, und wer führt die aus?

AUFLÖSUNG

Violett 8

Gibt es für eine Aufgabe den einen rich...

RICHTIG

B **Nein, nur verlässlichere und unzuverlässigere**

ERKLÄRUNG

Wer eine Formulierung im Betrieb einsetzt, sollte sie an mehreren echten Fällen ausprobieren, statt sie einmal zu bewundern.

GESPRÄCHSIMPULS

Welcher Prompt hat sich bewährt, und an wie vielen Fällen geprüft?

AUFLÖSUNG

Türkis 5

Der Harness bekommt ein perfekt formati...

RICHTIG

B **Nichts, er prüft die Form, nicht den Sinn**

ERKLÄRUNG

Ein formal korrekter Unsinn läuft durch. Diese Lücke schließt in einem Agenten der Kritiker, und auch der nur teilweise.

GESPRÄCHSIMPULS

Wer prüft bei euch heute Ergebnisse auf Sinn, nicht nur auf Form?

AUFLÖSUNG

Türkis 4

Der Werkzeugaufruf des Modells hat eine...

RICHTIG

A **Der Aufruf greift nicht, nichts wird ausgeführt**

ERKLÄRUNG

Das Format ist technische Voraussetzung, keine Konvention. Gute Harnesses melden den Fehler zurück. Sonst bleibt der Wunsch reiner Text, schlimmstenfalls erfindet das Modell ein Ergebnis.

GESPRÄCHSIMPULS

Was ginge verloren, wenn der Harness großzügig wäre und Formate verhandelbar würden?

AUFLÖSUNG

Türkis 3

Wer führt ein Werkzeug aus, wenn das Mo...

RICHTIG

C **Der Harness, die Software um das Modell herum**

ERKLÄRUNG

Das Modell bittet, der Harness entscheidet und führt aus. Er darf auch ablehnen. Genau dort sitzen später Rechte, Limits und Freigaben.

GESPRÄCHSIMPULS

Wo in eurem Unternehmen sitzt heute die Stelle, die ablehnen darf?

AUFLÖSUNG

Türkis 8

Was ist „Tool Calling“ (früher „Functio...

RICHTIG

B **Modell bittet, Software führt es aus**

ERKLÄRUNG

Die API liefert Werkzeugaufrufe heute als strukturierte Daten, die Anwendung bindet Werkzeuge oft über den Standard MCP an. Die Formatstrenge ist geblieben, sie ist nur nicht mehr sichtbar.

GESPRÄCHSIMPULS

Seht ihr in euren Werkzeugen, wann ein Werkzeug aufgerufen wurde?

AUFLÖSUNG

Türkis 7

Kann ein Sprachmodell rechnen?

RICHTIG

B **Meist richtig, aber ohne Garantie**

ERKLÄRUNG

Heutige Modelle rechnen oft gut, vor allem mit Zwischenschritten. Garantiert ist es nie, und man sieht es dem Ergebnis nicht an. Viele Apps rechnen deshalb unsichtbar mit einem Werkzeug.

GESPRÄCHSIMPULS

Welche Zahlen aus KI-Antworten habt ihr schon ungeprüft übernommen?

AUFLÖSUNG

Türkis 6

Woher weiß das Modell, welche Werkzeuge...

RICHTIG

C **Sie werden ihm bei jeder Anfrage mitgeschickt**

ERKLÄRUNG

Name, Zweck und erwartete Eingaben kommen mit jeder Anfrage mit. Deshalb kosten Werkzeuge Kontext und Geld, und deshalb kann man nicht beliebig viele anbieten.

GESPRÄCHSIMPULS

Welche drei Werkzeuge bräuchte ein Assistent an eurem Arbeitsplatz mindestens?

AUFLÖSUNG

Orange 3

Wozu braucht ein Agent ein Gedächtnis (...

RICHTIG

B **Damit Schritt drei weiß, was Schritt eins ergab**

ERKLÄRUNG

Memory ist ein Ablageort außerhalb des Kontextfensters, aus dem gezielt etwas zurückgeholt wird. In echten Systemen ist das eine Datei, eine Datenbank oder eine Suche.

GESPRÄCHSIMPULS

Was passiert, wenn Veraltetes nie aus dem Gedächtnis gelöscht wird?

AUFLÖSUNG

Orange 2

Ein Agent hat sechs Rollen: Planer, Ged...

RICHTIG

A **Meist ein einziges, mehrfach anders angewiesen**

ERKLÄRUNG

Meist ist es dasselbe Modell mit unterschiedlichen Anweisungen, manchmal ein günstiges für Routine und ein starkes fürs Planen. Die Trennung ist Organisation, nicht Hardware.

GESPRÄCHSIMPULS

Welche Rolle würdet ihr dem stärksten, welche dem günstigsten Modell geben?

AUFLÖSUNG

Orange 1

Was unterscheidet einen KI-Agenten von ...

RICHTIG

C **Er plant, nutzt Werkzeuge, prüft, wiederholt**

ERKLÄRUNG

Der Agent plant mehrere Schritte, nutzt Werkzeuge, prüft Zwischenergebnisse und läuft in Schleifen, bis das Ziel erreicht ist. Viele Chat-Apps haben dafür inzwischen einen eigenen Modus.

GESPRÄCHSIMPULS

Welche Aufgabe bei euch besteht aus genau solchen Schritten?

AUFLÖSUNG

Orange 6

Warum sind die Kosten eines Agenten sch...

RICHTIG

B **Weil die Zahl der Schritte von der Aufgabe abhängt**

ERKLÄRUNG

Die Schrittzahl steht vorher nicht fest. Jede Runde kostet einen Modellaufruf, und wie viele es werden, zeigt sich erst beim Laufen.

GESPRÄCHSIMPULS

Wie würdet ihr ein Budget für so etwas festlegen?

AUFLÖSUNG

Orange 5

Was passiert ohne Abbruchbedingung in e...

RICHTIG

C **Er dreht sich im Kreis, teuer und ohne Ergebnis**

ERKLÄRUNG

Technisch kann ein Agent endlos laufen. Praktisch werden Schrittzahl, Zeit und Kosten begrenzt, sonst merkt niemand sofort, dass er sich im Kreis dreht.

GESPRÄCHSIMPULS

Welche Grenze würdet ihr zuerst setzen: Schritte, Zeit oder Geld?

AUFLÖSUNG

Orange 4

Wonach prüft der Kritiker (Critic) im A...

RICHTIG

A **Nach dem Erfolgskriterium der Aufgabe**

ERKLÄRUNG

Der Kritiker ist selbst ein Modell mit denselben Schwächen. Er hilft, wo ein klares Kriterium steht. Bei der Frage, ob etwas gut ist, hilft er kaum.

SCHLÜSSELFRAGE · GESPRÄCH

Welche eurer Aufgaben hat ein klares Erfolgskriterium, welche nicht?

AUFLÖSUNG

Grün 1

Wie viele Risikoklassen kennt die KI-Ve...

RICHTIG

B **Vier: verboten, hoch, Transparenzpflicht, minimal**

ERKLÄRUNG

Verboten, Hochrisiko, Transparenzpflicht, minimales Risiko. Die Klasse hängt am Zweck, nicht an der Technik. Transparenzpflichten können zusätzlich greifen, große KI-Modelle haben eigene Regeln.

GESPRÄCHSIMPULS

In welcher Klasse bewegt ihr euch mit euren heutigen Werkzeugen vermutlich?

AUFLÖSUNG

Orange 8

Warum eine Aufgabe in Rollen und Schrit...

RICHTIG

B **Weil man nachvollziehen kann, wo es schiefging**

ERKLÄRUNG

Für kleine Aufgaben ist ein einziger Prompt sogar richtig. Ab einer gewissen Länge steigt die Fehlerquote, und vor allem wird prüfbar, an welcher Stelle etwas schiefging.

GESPRÄCHSIMPULS

Welche eurer Aufgaben ist klein genug für einen einzigen Prompt?

AUFLÖSUNG

Orange 7

Zwei Agenten „unterhalten sich". Was pa...

RICHTIG

A **Text geht hin und her, jede Runde kostet**

ERKLÄRUNG

Der Nutzen liegt in den unterschiedlichen Blickwinkeln. Der Preis sind Zyklen, jeder davon ein Modellaufruf.

GESPRÄCHSIMPULS

Wann lohnt ein zweiter Blickwinkel die doppelten Kosten?

AUFLÖSUNG

Grün 4

Emotionserkennung per Webcam im Meeting...

RICHTIG

C **Nein, am Arbeitsplatz verboten, auch freiwillig**

ERKLÄRUNG

Ein Verbot lässt sich nicht per Einwilligung oder Betriebsvereinbarung aufheben. Ausnahmen gibt es nur aus medizinischen oder Sicherheitsgründen.

GESPRÄCHSIMPULS

Dieselbe Software im Computerspiel wäre harmlos. Was sagt das über die Klassen?

AUFLÖSUNG

Grün 3

Ihr nutzt nur ein fertiges KI-Werkzeug ...

RICHTIG

A **Ja, als Betreiber habt ihr eigene Pflichten**

ERKLÄRUNG

Die Verordnung unterscheidet Anbieter und Betreiber. Wer ein KI-System beruflich einsetzt, ist Betreiber. Art. 4 verpflichtet beide, die KI-Kompetenz ihrer Leute aktiv zu fördern.

SCHLÜSSELFRAGE · GESPRÄCH

Wer in eurem Unternehmen müsste das eigentlich auch wissen?

AUFLÖSUNG

Grün 2

Ein Tool bewertet Bewerbungen und sorti...

RICHTIG

C **Hochrisiko**

ERKLÄRUNG

Systeme zur Auswahl von Bewerbungen zählen ausdrücklich zu den Hochrisiko-Anwendungen. Ab Dezember 2027 sind menschliche Aufsicht, Protokollierung und Information der Betroffenen Pflicht.

GESPRÄCHSIMPULS

Wer würde bei euch eine automatische Absage am Ende verantworten?

AUFLÖSUNG

Grün 7

Ein Bestätigungsklick vor jeder Aktion …

RICHTIG

B **Nur mit Information, Zeit zum Prüfen und echtem Nein**

ERKLÄRUNG

Ein Dialog, den man fünfzig Mal am Tag wegklickt, ist Dokumentation, nicht Kontrolle. Für Hochrisiko-Systeme verlangt die Verordnung wirksame Aufsicht und warnt ausdrücklich vor Automatisierungsbias.

GESPRÄCHSIMPULS

Welche Bestätigung klickt ihr heute schon weg, ohne zu lesen?

AUFLÖSUNG

Grün 6

Wann muss ein Mensch in den Loop?

RICHTIG

B **Bei hohem Einsatz oder schwer umkehrbaren Folgen**

ERKLÄRUNG

Kriterien sind Schadenshöhe, Umkehrbarkeit und ob der Agent eigene Fehler erkennt. Die Stufe hängt an der einzelnen Handlung, nicht am Produkt: unter 50 Euro allein, darüber Freigabe.

GESPRÄCHSIMPULS

Welche Handlung in eurem Alltag wäre die erste, die ihr freigeben lassen würdet?

AUFLÖSUNG

Grün 5

Im Prompt steht: „Versende keine E-Mail…

RICHTIG

A **Nein, das ist eine Bitte, keine Grenze**

ERKLÄRUNG

Ein Guardrail begrenzt Handlungen technisch oder organisatorisch: Rechte, Betragsgrenzen, Freigaben. Ein Prompt ist nur eine Bitte an ein System, das Wahrscheinlichkeiten berechnet.

SCHLÜSSELFRAGE · GESPRÄCH

Welche echte Grenze hat euer KI-Werkzeug heute?

LIZENZ

CC BY-SA 4.0

creativecommons.org/licenses/by-sa/4.0

Du darfst das Material teilen und bearbeiten, auch kommerziell. Bedingung: Namensnennung mit Quelle und Lizenz, Änderungen kennzeichnen, Bearbeitungen unter derselben Lizenz weitergeben.

SO NENNST DU DIE QUELLE

„Fragen-Bingo – Vom Token zum Agenten“ von Peter Schmidt (versabilit.com), CC BY-SA 4.0

KI-HINWEIS

Erstellt mit KI-Unterstützung (Claude, Anthropic) für Icons, Recherche und Formulierungen, geprüft und verantwortet vom Urheber.

Keine Rechtsberatung. Rechtsangaben Stand Oktober 2026, nicht fachlich geprüft.

AUFLÖSUNG

Grün 8

Ein voll autonomer Agent trifft eine Fe…

RICHTIG

C **Das Unternehmen, das ihn einsetzt**

ERKLÄRUNG

Autonomie verschiebt die Arbeit, nicht die Verantwortung. Am Ende steht ein Mensch oder eine Organisation gerade, in aller Regel nicht die Person, die den Knopf gedrückt hat.

GESPRÄCHSIMPULS

Wer unterschreibt bei euch, wenn der Agent entscheidet?