Grokking Generalization beyond overfitting on small algorithmic datasets

Докладчик: Козлова Ольга

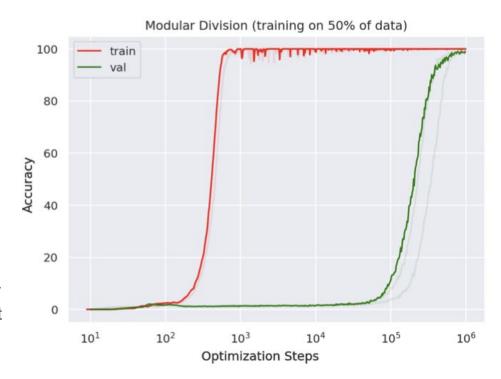
Рецензент: Княжевский Владимир

Хакер: Иванов Данила

Что такое Grokking?

Феномен, при котором обобщающая способность модели возрастает после продолжительного периода переобучения.

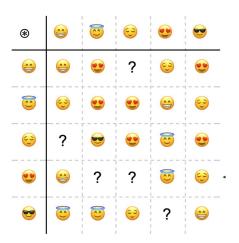
Original: We show that, long after severely overfitting, validation accuracy sometimes suddenly begins to increase from chance level toward perfect generalization. We call this phenomenon 'grokking'.



А какие условия?

- Синтетические данные (таблички, в которых часть клеток закрашена)
- Маленький размер датасета
- Маленькая модель (трансформер)

*	а	b	С	d	е
а	а	d	?	С	d
b	С	d	d	а	С
С	?	е	d	b	d
d	а	?	?	b	С
е	b	b	С	?	а



Подробнее про данные

Табличка с бинарными операциями вида:

a • b = c, где a, b, c – токены, • – различные варианты бинарных операций

Original: The datasets we consider are binary operation tables of the form $a \circ b = c$ where a, b, c are discrete symbols with no internal structure, and \circ is a binary operation.

Примеры операций:

$$x \circ y = x + y \pmod{p}$$
 for $0 \le x, y < p$
 $x \circ y = x - y \pmod{p}$ for $0 \le x, y < p$
 $x \circ y = x^3 + xy \pmod{p}$ for $0 \le x, y < p$
 $x \circ y = x^3 + xy^2 + y \pmod{p}$ for $0 \le x, y < p$
 $x \circ y = x \cdot y$ for $x, y \in S_5$
 $x \circ y = x \cdot y \cdot x^{-1}$ for $x, y \in S_5$

Что сделали авторы?

- Обнаружили сам эффект
- Провели эксперименты
 - Выяснили закономерности (какие дальше)
 - Визуализировали полученные результаты (картинки дальше)
- Пригласили всех исследовать дальше

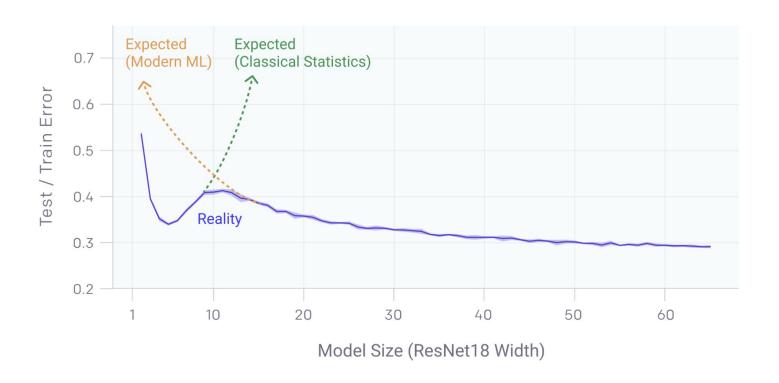
Бонус: как это обнаружили?

Ответ от авторов:

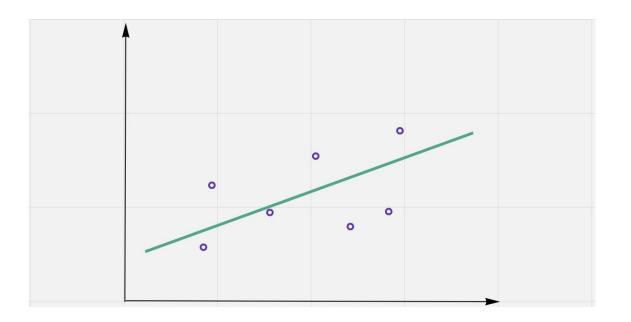
"The team at OpenAI was studying how transformers behave on algorithmic tasks, and they left a training job running over night. When they came back they were surprised to see that the transformer had somehow solved the task."

Как это работает?

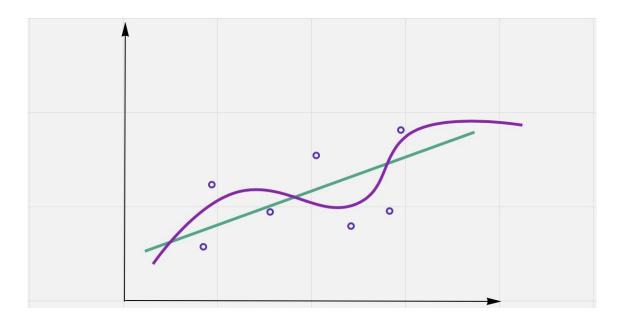
Double descent



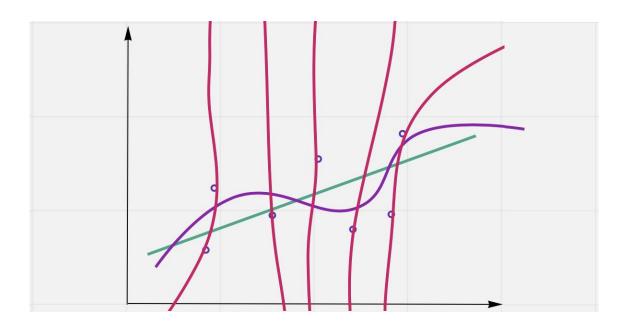
Очень простая модель



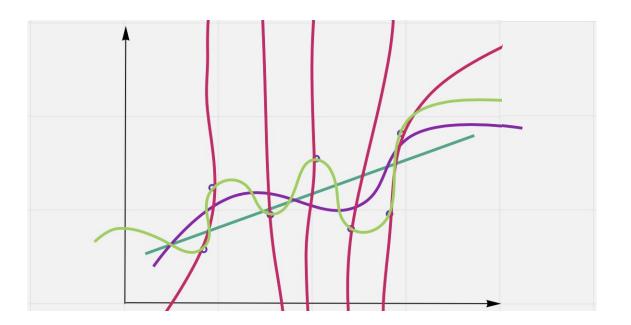
Немного усложнили – хорошо, но не идеально



Слишком много параметров – переобучение

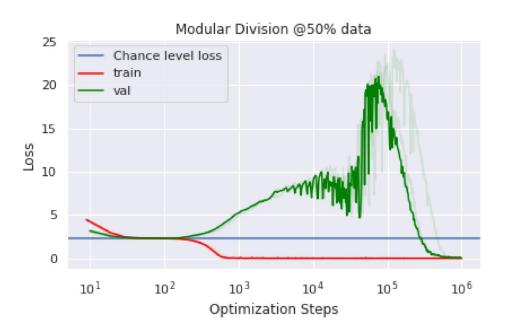


Так много параметров, что модель смогла выучить сложную закономерность

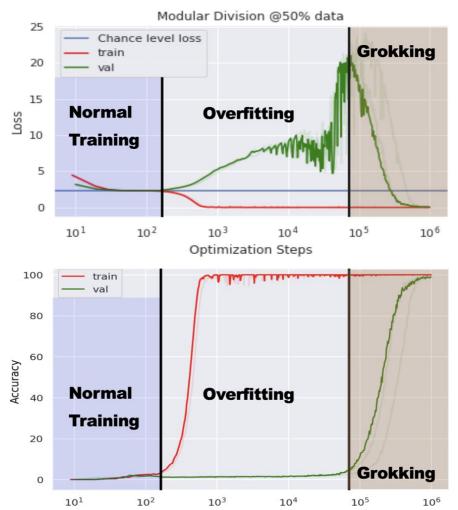


Double descent

Авторы тоже наблюдают такой эффект для функции потерь



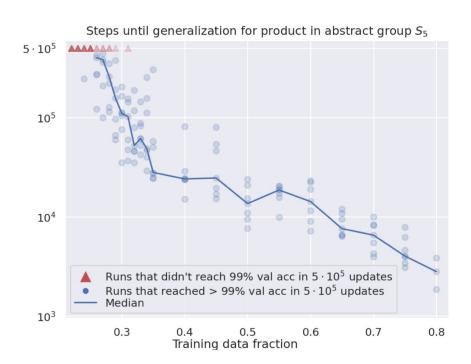
Double descent



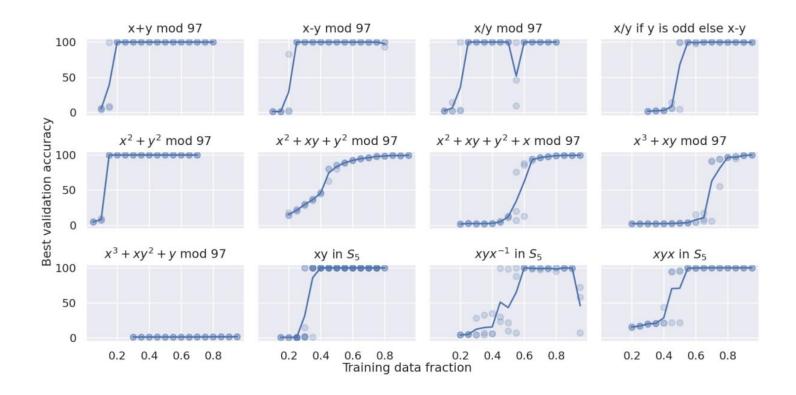
Эксперименты

Объем обучающих данных

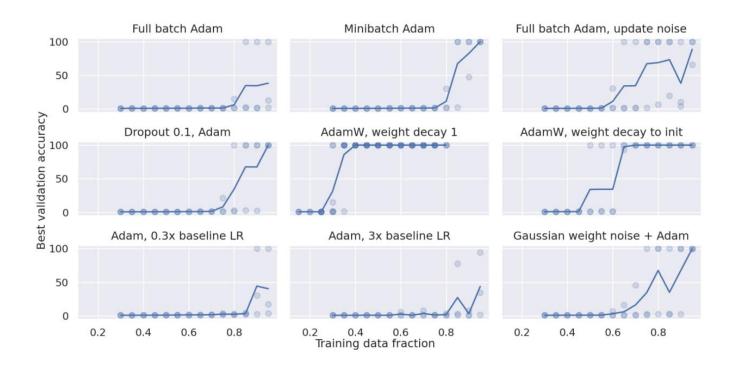
- Пробуем менять объем тренировочных данных
- Чем больше данных даем, тем быстрее обобщается



Различные бинарные операции



Эксперименты с оптимизатором



Визуализации

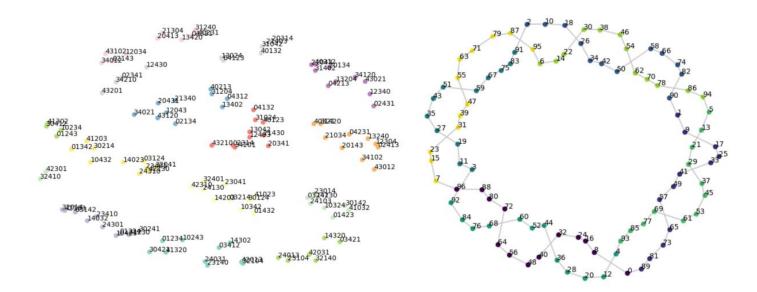
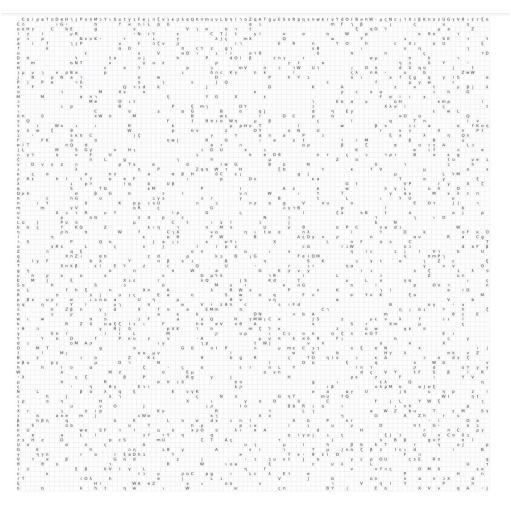


Figure 3: **Left**. t-SNE projection of the output layer weights from a network trained on S_5 . We see clusters of permutations, and each cluster is a coset of the subgroup $\langle (0,3)(1,4), (1,2)(3,4) \rangle$ or one of its conjugates. **Right**. t-SNE projection of the output layer weights from a network trained on modular addition. The lines show the result of adding 8 to each element. The colors show the residue of each element modulo 8.

Если вам скучно

One of the binary operation tables presented to the networks that the network can perfectly fill in. Each symbol is represented as a letter in English, Hebrew, or Greek alphabet for reader's convenience.

We invite the reader to guess which operation is represented here.



Источники

- Сама статья на arxiv [en]:
 - https://arxiv.org/abs/2201.02177
- Постер с воркшопа [en]:
 - https://mathai-iclr.github.io/papers/posters/MATHAI 29 poster.png
- Обзор на youtube [en]:
 - https://www.youtube.com/watch?v=dND-7llwrpw
- Обзор в telegram [ru]:
 - https://t.me/gonzo ML/831
- Картиночки про double descent (красивые):
 - https://mlu-explain.github.io/double-descent/

Некоторые заметки из рецензии

Авторы

Open Al

ICLR (International Conference on Learning Representations), 1st Mathematical Reasoning in General Artificial Intelligence Workshop

Обзор последующих работ

Чаще всего цитирование работы выглядит так:

Predictability and Surprise in Large Generative Models: "Though performance is predictable at a general level, performance on a specific task can sometimes emerge quite unpredictably and abruptly at scale".

Unsolved Problems in ML Safety: "We are better able to make models safe when we know what capabilities they possess".

Обзор последующих работ

Есть и прямые продолжения:

Understanding Grokking: An Effective Theory of Representation Learning: аналогичные результаты и попытка вывести теоремы.

A Mechanistic Interpretability Analysis of Grokking: reverse ingeneering, сложение по модулю 97 делается через дискретные преобразования Фурье.

Сильные стороны

Все понятно объяснено, эксперименты описаны подробно.

Само открытие, что grokking происходит стабильно для определенных данных и моделей.

Потенциал для исследований.

Слабые стороны

Неясно, получится ли найти у статьи какое-то применение на практике.

Одна модель.