



Санкт-Петербургский
Государственный
Политехнический
Университет

Институт прикладной
математики и механики

КАФЕДРА

ТЕЛЕМАТИКА

Высшая школа ИИ

курс: Решение прикладных задач методами машинного обучения

Лекция 2

Характеристика фундаментальной проблемы
«машинного обучения»

14 сентября 2022 г.

Что было на прошлой лекции:

Представлена структура курса

- Характеристика фундаментальной проблемы «машинного обучения»
- *Проблемы «решения» прикладных задач методами МО*
- *Технологии решению прикладных задач*
- *Перспективы: технологические, футурологические...*

Сформулированы

Ключевые слова: фундаментальная проблема, прикладные задачи, искусственный интеллект, машинное обучение, технология

Определены области прикладной деятельности:

- Профессиональная медицина
- Персональное использование
- Образование.
- Промышленность.
- Сельское хозяйство.
- Дорожное движение.
- Бытовое применение

Характеристика фундаментальной проблемы «машинного обучения»

Проблема: **Чему** и **как** можно научить «машину» ?

К. Гедель: Истинно то, что логически **доказуемо**
Доказуемо не все, что **истинно**

Мы можем вычислить даже то, что невозможно себе представить
Л. Ландау

Машина Тьюринга: решение **прямых задач** с помощью алгоритмов.
Загрузка алгоритма-программы в автомат не есть обучение

построение **алгоритмов на основе решения «обратных» задач**



*Уточните значение слов, и вы избавите
человечество от половины заблуждений. ©
Рене Декарт*

Начнем с уточнения:

- **обучение** - сознательный процесс выработки универсальных **реакций**
- **научение** – сознательный или бессознательный процесс формирования **поведения**.

Частный случай:

- Машинное обучение— использование математических моделей данных, для управления работой компьютера без использования программ в форме набора машинных команд (специально подобранные входные данные и есть «команды») .
- Научение – формирование индивидуального опыта, состоящего из набора действий, изменяющих поведение субъекта в зависимости от конкретных условий и внешней среды (данные определяют изменение «поведения»)



ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ ФУНДАМЕНТАЛЬНАЯ ПРОБЛЕМА «ОБУЧАТЬСЯ» ?

Проблема обучения связана с целенаправленным изменением восприятия данных неким субъектом. Обучение можно рассматривать как саморегулируемый процесс фильтрации сигналов окружающего мира с целью вычленения значимой информации, не требующий внешнего вмешательства.

Обучение субъекта не отделимо от феномена «**интеллектуальности**».

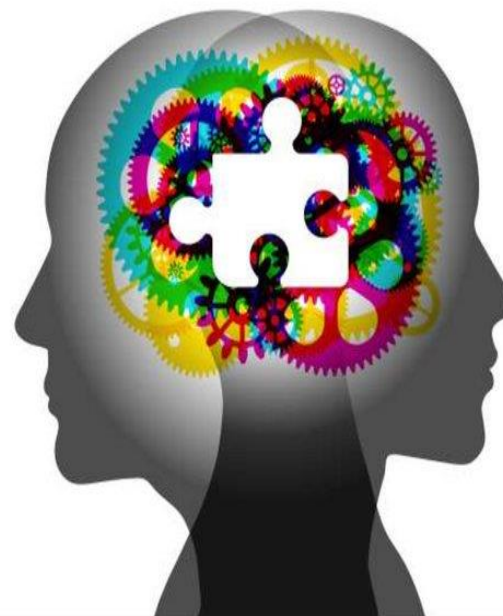
Например, в узком смысле «интеллектуальность компьютеров» – это их способность реализовывать различные классы алгоритмов решения прикладных задач, достигая при этом заданных критериев оптимальности. Заметим, что:.

- Функция «обучения» применительно к современным компьютерным технологиям (КТ) – «конечным автоматам или машинам Тьюринга носит «экзо» характер и сводится к целевой **реконфигурации** доступного для этого множества программных и аппаратных компонент для повышения эффективности вычислений (производительности, точности, надежности, потребления энергии...).
- Способность обучаться применительно к **экзо-интеллектуальным компьютерным системам** требует от совокупности аппаратно-программных средств, способности **реконфигурации с помощью** технологии «машинного обучения» на выборке данных, пополняемой в ходе функционирования вычислительной системы



Перцептивное научение

- Готовность организма к научению имеет первостепенное значение для его выживания, и эта готовность в значительной степени зависит от его перцептивных навыков. Научение позволяет человеку замечать стимулы, на которые он до того не обращал внимания, например, как происходит восприятие обычных пространственных отношений.
- Перцептивные способности не являются неизменными и меняются при обучении.

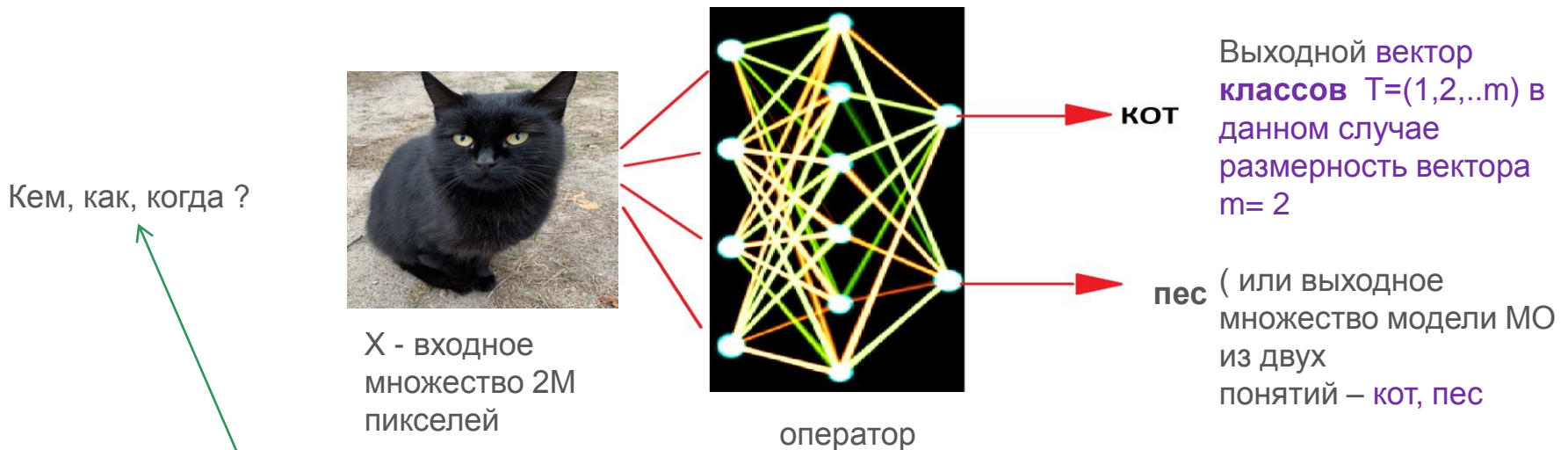




ПОЛИТЕХ

СТАНДАРТНАЯ МОДЕЛЬ МО С ТОЧКИ ЗРЕНИЯ РАЗРАБОТЧИКА

задаче классификации обучающая выборка представляет собой набор отдельных объектов $X = \{x_i\} \text{ n } i=1$, характеризующихся вектором вещественнозначных признаков $x_i = (x_{i,1/2}, \dots, x_{i,d})$



"заранее **обученная** нейроморфная модель-оператор **предсказывает**, что **2 M пикселей** входного изображения **кодируют** с помощью hidden (скрытой) **сигнатуры** в выходном embedding векторе позицию «кот» с вероятностью **0.98**", а слово «пес» с вероятностью **2%**.

Требуется настроить оператор (классификатор), который, обработав входной вектор X, сформировал бы вектор оценок принадлежности (апостериорных вероятностей) X к каждому из классов $\{p(s|x)\}$. В данном случае $s=1$, с вероятностью 0.98

- получение верного ответа с помощью **неверных в общем случае рассуждений** ("right for the wrong reasons"), которые хорошо работают только для обучающего распределения данных и на этапе тестирования (Shortcut learning или ускоренное обучение)

(См. <https://arxiv.org/abs/2004.07780>)

- учета «контекста» для получения правильного решения
 - современные сверточные нейронные сети «предпочитают» ориентироваться на локальные участки текстур (классификация черных котов как породу собак схипперк)



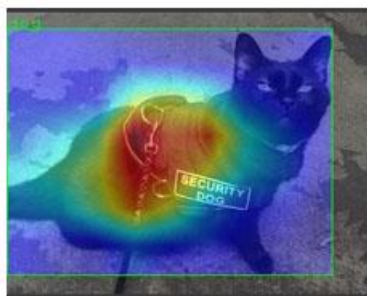
YOLOv5m, 320x320



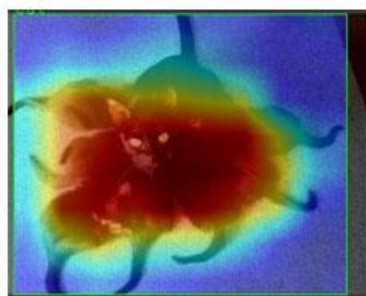
YOLOv5m, 320x320



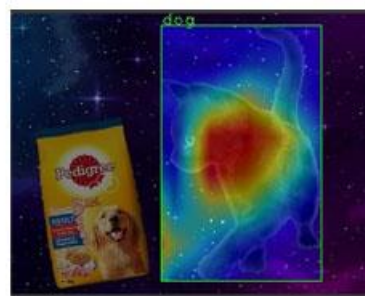
YOLOv5m, 320x320



Grad-CAM explanation



Grad-CAM explanation



Grad-CAM explanation

Что такое в данном случае «контекст»:

- добавление на фото коробки собачьего корма в существенно повышает уверенность в распознавании объекта, хотя сам корм нейронная сеть распознает как "книгу"



КАК ЭТО ПРОИСХОДИТ В МОЗГУ ЧЕЛОВЕКА

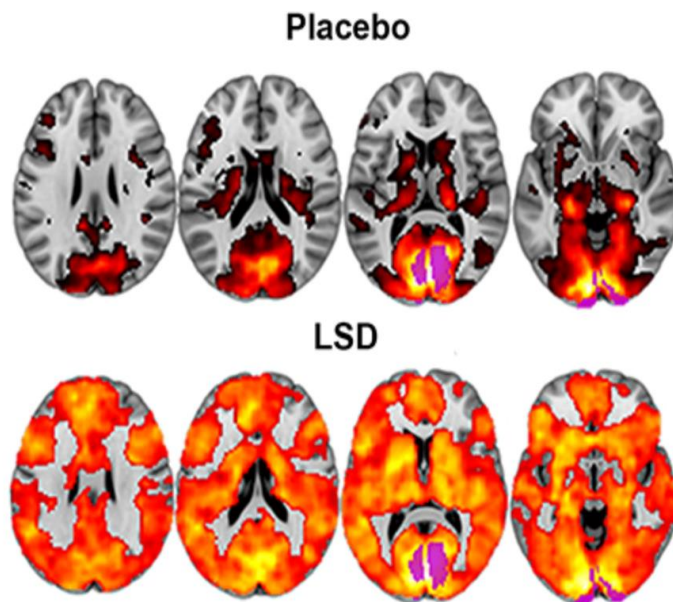
- Каждую секунду тело (совокупность всех органов) отправляет в мозг 11 миллионов бит информации.
- Сколько из этих битов мозг обрабатываете сознательно? Оказывается максимум 50, что лишь 0,00001% от данных, которые генерируют все части нашего организма. Остальная часть данных обрабатывается «подсознательно»....
- Понимая это многие с энтузиазмом утверждают «*Мы используем только малую часть около 10% нашего мозга!*». Поэтому надо разблокировать «подсознание» и таким образом усилить интеллектуальные возможности человека.
- Итак, сознание не использует 100%, ресурсов мозга, но мозг, имея вес около 1.5 кг или 2% веса всего организма, потребляет 20 % всей энергии организма. Поддерживать жизнь, управляя работой всех органов - это большая работа.

Вопрос: почему эволюция не использовала все ресурсы мозга ?

- Почти любая «обучающая выборка» имеет ограниченное разнообразие и не покрывает всех ситуаций, в которых желательна корректная работа модели МО. Это важно в случае сложных структур данных, совмещающих изображения, тексты и звукозаписи.
- Какие при этом возникают «ошибки»
 - используются признаки, которые не позволяют вычислить правильный ответ даже на обучающей выборке
 - используются признаки, которые позволяют эффективно предсказывать ответ на обучающей выборке, но не на всем распределении, из которого получена эта выборка.
 - используются данные, которые отличается от данных обучающей выборки путем сдвига распределения данных (distributional shift).

Кора головного мозга обрабатывает лишь ~ 50 бит информации в секунду. Куда деваются остальные 10 999 950? Вся информация проходит через специальный фильтр, который работает как гигантское «умное» гибкое сито – **таламусом** или шлюз между сенсорной информацией, передаваемой в ваш мозг — от различных органов и частей тела (рук, глаз, волос, пальцев ног, носа, языка и т. д.) и корой головного

Вещество, которое запускает безумное количество нейронов мозга без всякой причины, называется диэтиламид лизергиновой кислоты, или ЛСД. Его прием приводит к резкому повышению нейронной



Нормальная работа мозга

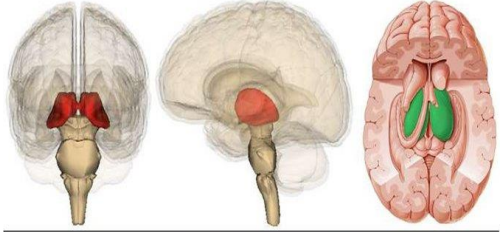
Какофония галлюцинаций.

Сенсорная информация блокируется ретикулярным ядром **таламуса** (TRN).

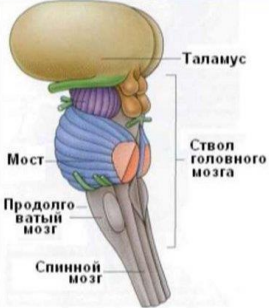
- Сенсорное «обеспечение» человеческого организма генерирует данные со скоростью 11 миллионов бит в секунду, но в кору головного мозга, где «обитает» сознание, передается — не более пяти десятков бит в секунду. Все другие данные фильтруются в таламусе — органе, который отвечает за перераспределение информации
- Выводы:
 - из всей информации, которая каждую секунду поступает в мозг от органов чувств, только малая часть достигает сознания и обрабатывается в больших полушариях головного мозга:
 - отношение производительности **перцепции** к производительности **апперцепции** составляет миллион к одному

Таламус

Таламус представляет своего рода ворота, через которые в кору поступает и достигает сознания основная информация об окружающем мире и о состоянии тела.



Таламус состоит примерно из 40 пар ядер, которые функционально делятся на **специфические, неспецифические и ассоциативные**.






ПОЛИТЕХ

ИНТЕЛЛЕКТУАЛЬНЫЙ ФИЛЬТР ПОТОКА СЕНСОРНЫХ ДАННЫХ

Ретикулярное ядро таламуса (TRN) таламуса работает как «светофор» или шлюз на информационной сети потока сенсорных данных. Таламус «пропускает» лишь ту информацию, которая наиболее актуальна в контексте текущей задачи. Остальные данные он как бы убирает в «дальний ящик».

Вопросы:

- как TRN расставляет приоритеты?
- какие именно данные из всего потока битов необходимо оставить, а какие «выкинуть»?

Ответ: никто точно этого не знает. На эту тему есть несколько исследований, но они весьма неполные и запутанные.

Вывод: мозг получает большой объем информации, но 99,99999% этой информации не доходит до сознательной части сознания человека.

Вопрос: Можно ли и подобный интеллектуальный фильтр реализовать средствами современных компьютерных технологий ?

Это и есть фундаментальный вопрос использования технологий ИИ

1. восстановление регрессии при решении задач:

- Оценки стоимости объекта по его характеристикам
- Прогноз свойств соединений по параметрам химических элементов
- Оценка времени заживления травмы
- Оценка заемщика при выдаче ему кредитного лимита
- Оценка расхода топлива по техническим характеристикам автомобиля и режиму езды спрогнозировать

В классической задаче восстановления регрессии обучающая выборка представляет собой

- набор отдельных объектов $X = \{x_i\}_{i=1}^n$, характеризующихся вектором вещественнозначных признаков $x_i = (x_{i,1}, \dots, x_{i,d})$

результат построения регрессии

- непрерывная вещественнозначная переменная t (регрессор), входящая в апостериорное распределение на множестве значений регрессионной переменной $p(t|x)$



2. Извлечение знаний. Области применения:

- Медицина: поиск синдромов болезни
- Социология: определение факторов, влияющих на выборы
- Генная инженерия: выявление связанных участков генома
- Научные исследования: получение новых знаний об исследуемом процессе

.....

Суть механизма : построение зависимостей между **КОСВЕННЫМИ** классификационными признаками одного и того же объекта или явления

Обучающая выборка - набор отдельных объектов $X = \{x_i\}_{i=1}^n$, характеризующихся вектором вещественнозначных признаков $x_i = (x_{i,1}, \dots, x_{i,d})$

Задача: построить алгоритм, генерирующий набор объективных связей между признаками, имеющих место в генеральной совокупности. Результат может иметь форму

- предикатов «ЕСЛИ ... ТО ...»
- цифровых диапазонов $((0.3 \leq x_4 \leq 2.1) \& (-6.98 \leq x_7 \leq -7.59)) \Rightarrow (3.2 \leq x_2 \leq 8.345)$,
- текстовых сообщений («ЕСЛИ высота – низкая И (облачность – слабая ИЛИ – отсутствует) ТО полет – безопасный»)



(поведение моделей МО за пределами обучающего распределения данных)

Для каждой задачи может существовать бесконечное количество разных обученных моделей с разными весами и вычислительными архитектурами, дающих примерно одинаковую точность на обучающей выборке. (см.

http://www.cs.cmu.edu/~tom/pubs/NeedForBias_1980.pdf)

«плохое» поведение систем ИИ в реальных условиях применения «обученных моделей»

<https://arxiv.org/abs/2011.03395>

Н. Винер (книга Творец и робот):

- исполнение заданного осуществляется в высшей степени буквально
- Если магия вообще способна даровать что-либо, то она дарует именно то, что вы попросили, а не то..., что подразумевали, но не сумели точно сформулировать



Решение задач анализа данных путем обработки прошлого опыта (case-based reasoning) и построение оператора отображения вектора из признаков класса объектов на множество данных измерения.

- Что это дает: Альтернатива построению формальных математических моделей (model-based reasoning)
- Основное требование – наличие «обучающей» информации, которая инвариантна к шумам «экспериментальных» данных, которые подаются на вход системы ИИ. Это могут быть:
 - выборка прецедентов – ситуационных примеров из прошлого опыта с известными исходами
 - обобщенный опыт прошлых наблюдений/ситуаций, исход которых известен
- Основные проблемы:
 - Малый объем и разнообразие опытных данных
 - Некорректность входных данных
 - «Переобучение»

Объект разработки – обучающая выборка. Цель - нахождение эффективного размера выборки, которая сохраняет репрезентативность

При малых выборках

Можно использовать только простые модели

Скорость обучения **максимальна**

Можно использовать методы, требующие **много времени на обучение**

Хотя большой объем выборки позволяет

- Получить более надежные результаты
- Использовать более **сложные** модели алгоритмов
- Повысить точность обучения

НО: при этом время обучения быстро растет, а также высока вероятность переобучения выборе излишне сложной модели

Противоречивость. Объекты с одним и тем же признаковым описанием могут иметь разные исходы (принадлежать к разным классам, иметь отличные значения регрессионной переменной и т.п.)

Что надо делать:

- Необходимо заранее исключать или корректировать противоречащие объекты
- Использование вероятностных методов обучения позволяет корректно обрабатывать противоречивые данные, имеющие условное распределение $p(t|x)$

Разнородность. Признаки могут быть вещественнозначными, дискретными, номинальными и текстовыми:

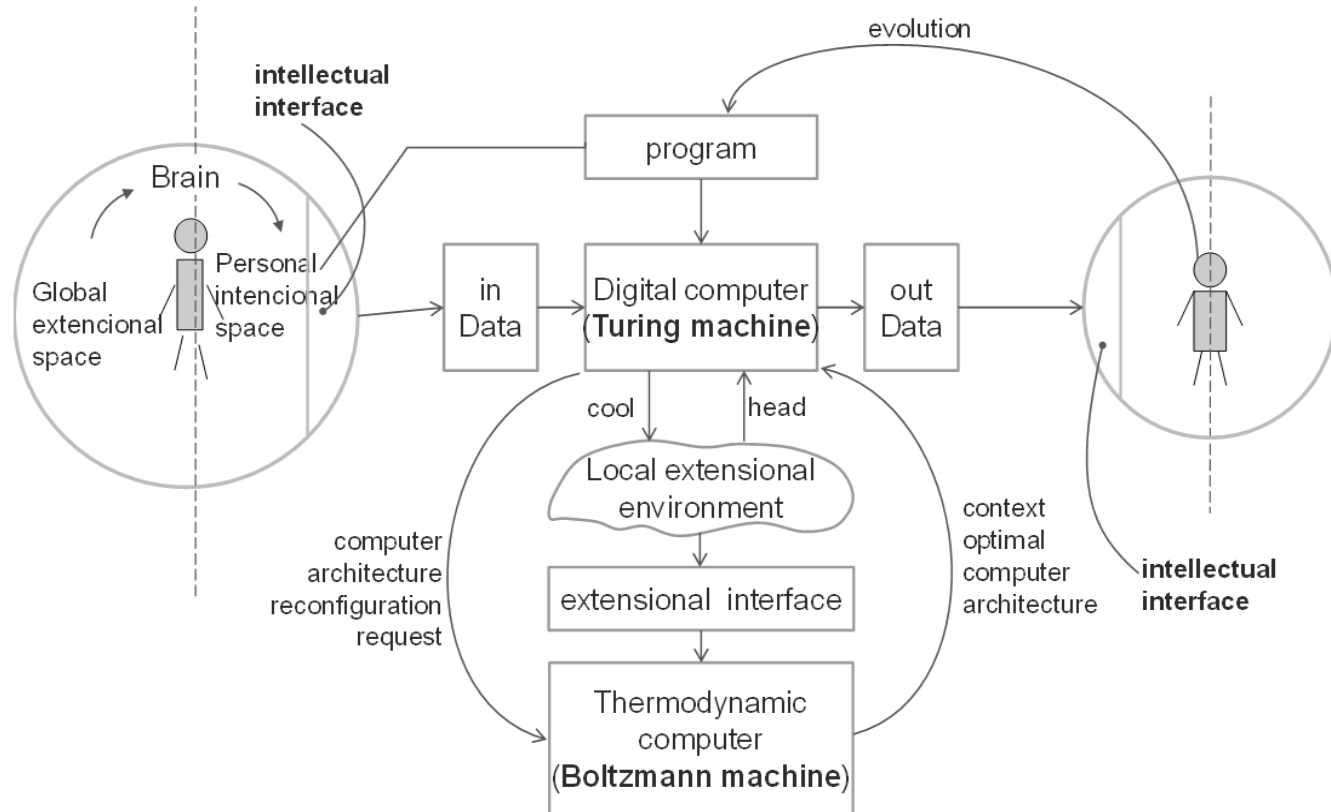
- Номинальные признаки отличаются особенностями метрики между значениями и могут быть заменены на набор бинарных переменных по числу значений номинального признака
- Текстовые признаки, признаки-изображения, даты и пр. необходимо заменить на соответствующие номинальные либо числовые значения



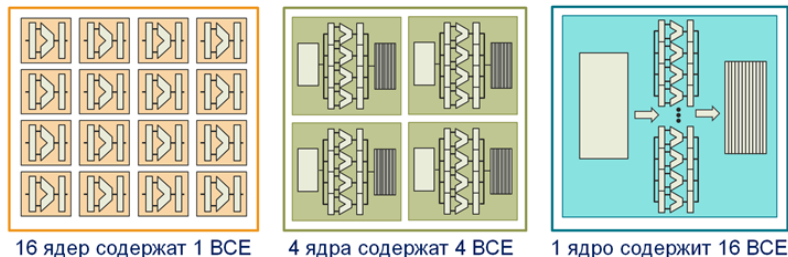
ПОЛИТЕХ

Выводы: НЕОБХОДИМА ПЛАСТИЧНОСТЬ МОДЕЛЕЙ МО

«пластичность»
архитектуры вычислителя,
как платформы системы МО
основанная на
использовании
интеллектуальных
интерфейсов, **накоплении**
информации о
функционировании,
фильтрации данных с целью
«выявления» значимых
признаков, которые
повышают точность
решения прикладных задач
классификации,
кластеризации и регрессии

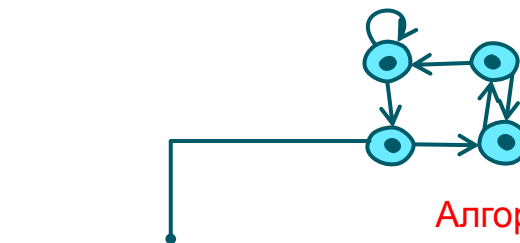
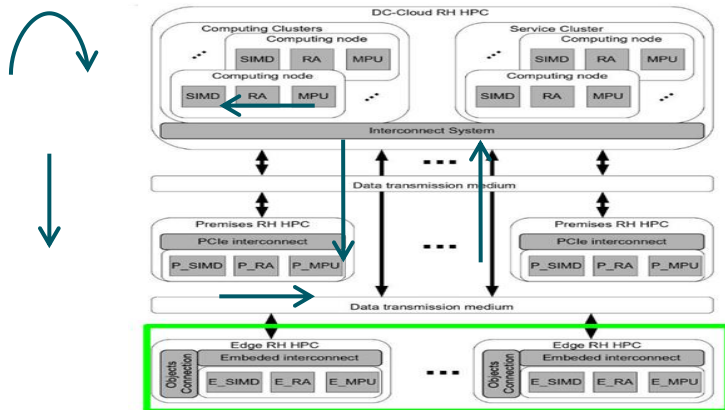


- 1) В пространстве двух измерений
 - (BCE – basic calculation element)



согласно закону Амдаля переход на многоядерные структуры, может **ускорить** выполнение как последовательных (1-F), так и параллельных (F) частей алгоритма

- 2) Гетерогенность + реконфигурируемость вычислительных структур расширяет пространство возможностей до уровня «**самоорганизации**» путем **пополнения сигнатуры базовых вычислительных операций (БВО)**

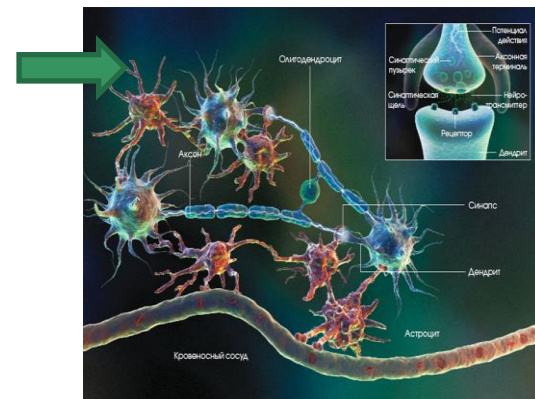


Представление алгоритма с помощью БВО

Алгоритм как функция, вычисляющая решение в потоке обрабатываемых данных

Аспекты проблемы:

- **Какие** интерфейсы и протоколы нужны для **взаимодействия** вычислителя и естественного интеллекта ?
- **Как ускорить процесс обучения,** используя фактор внимания и интеллектуальной фильтрации входного потока данных ?
- **Можно ли решить проблемы синтеза систем ИИ** путем динамической реконфигурации используемой вычислительной платформы ?



Поиск решений задач ИИ возможен на пути следования природоподобным аналогам, реализуемым в биологическом мозгу животных и мозге человека.

Теоретические основы обсуждаемой проблемы:

- Анализ топологии многообразия «больших» данных
- Вычислительные методы решения «обратных» задач
- Цифровая обработка сигналов

Мозг человека «пластичен» и поэтому способен к обучению путем реконфигурации своей структуры, Мозг содержит содержит 100 млрд. нейронов, потребляет на «работу» не более 20 Вт. При этом их всего потока сенсорных данных, объем которых достигает 10 Мбит/с в кару головного мозга поступают данные со скоростью не более 50 бит/с.

Фундаментальные проблемы «машинного обучения» (МО) связаны с тем, что:

- Объекты с одним и тем же признаковым описанием могут:
 - принадлежать к разным классам, и поэтому
 - использовать отличные аргументы для построения регрессионных зависимостей
 - иметь различные структуры «операторов» отображения пространства классификационных признаков на пространство измеряемых данных.
- Классификационные признаки могут быть числами (вещественными, рациональными, дискретными), номинальными или текстовыми структурами, при этом:
 - Номинальные признаки отличаются особенностями метрики между значениями и могут быть заменены на набор бинарных переменных по числу значений номинального признака
 - Текстовые признаки, признаки-изображения, даты и пр. необходимо заменить на соответствующие номинальные либо числовые значения
- В общем случае проблемы МО сводятся к решению обратных задач, имеющих множество решений, из которых выбор «верного решения» возможен при учете контекстных ограничений и регуляризации решаемой оптимизационной задачи.

- Вьюгин В. Математические основы машинного обучения и прогнозирования
- Осипов, Г.С. Методы искусственного интеллекта , Москва 2011
- Петер Флах. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных