МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Пензенский государственный университет» (ПГУ)

А. И. Иванов

Малые выборки, нейроморфные вычисления: быстрые алгоритмы оценки энтропии Шеннона – Пирсона квадратичной сложности

Справочник

Пенза
Издательство ПГУ
2023

УДК 519.24; 53; 57.017
ББК 32.818
И18

Р е ц е н з е н т

доктор технических наук, профессор,
ученый секретарь Научно-производственного
предприятия «Рубин» (г. Пенза)
М. М. Бутаев

Иванов, Александр Иванович.

И18 Малые выборки, нейроморфные вычисления: быстрые алгоритмы оценки энтропии Шеннона – Пирсона квадратичной сложности : справочник / А. И. Иванов. – Пенза : Изд-во ПГУ, 2023. – 32 с.

ISBN 978-5-907752-61-0

Издание посвящено проблемам статистической обработки малых выборок реальных данных. Нейросетевой искусственный интеллект способен эффективно противостоять энтропии окружающей среды, если он заранее обучен решать некоторую конкретную задачу. Примером могут служить нейросетевые преобразователи биометрических данных человека в код его личного криптографического ключа. Ключ получается длинным – 256 бит, однако это может быть только видимостью. Разряды ключа зависимы, соответственно, нужно уметь оценивать снижение энтропии кодовой последовательности с зависимыми разрядами.

Решать эту задачу по Шеннону крайне сложно, так как она обладает экспоненциальной вычислительной сложностью. В справочнике приводятся таблицы экспериментально полученных связей энтропии Шеннона с коэффициентами корреляции разрядов кода. Вычисления выполнены по классической энтропии Шеннона для коротких кодов. Далее выполнена полиномиальная аппроксимация и экстраполяция данных. Как результат, появляется возможность заменить задачу экспоненциальной вычислительной сложности по Шеннону на более простую задачу Шеннона – Пирсона квадратичной вычислительной сложности. Рассмотренные преобразования дополняют алгоритмы быстрой оценки энтропии в пространстве расстояний Хэмминга по ГОСТ Р 52633.3–2011 с линейной вычислительной сложностью.

Представленные материалы ориентированы на студентов, инженеров и аспирантов, занимающихся разработкой и исследованием нейросетевых приложений искусственного интеллекта в защищенном исполнении.

УДК 519.24; 53; 57.017
ББК 32.818

Индексы цитирования автора:
Scopus – 57189212610;
РИНЦ 744989; SPIN-код 2277-7744

ISBN 978-5-907752-61-0

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Шеннон в середине XX в. сделал существенный шаг в информатике, перенеся понятие энтропии из физики (из теплотехники) на открытые и зашифрованные тексты. В физике и технике под энтропией окружающей среды следует рассматривать температуру. В частности, для измерения температуры в реальном мире могут использоваться термопары, собранные из двух разных металлов. Возникающая электродвижущая сила на концах любой термопары зависит только от выбранной пары самих металлов и от разницы температур между холодным и горячим спаями. В России и за рубежом для нескольких десятков наиболее часто используемых термопар созданы и используются стандарты. По сути дела каждый такой стандарт является шкалой (например, в форме таблицы), связывающей общепринятую шкалу энтропии – температуру – с некоторой частной шкалой энтропии под выходные милливольты конкретной термопары.

При такой интерпретации число частных шкал наблюдения энтропии (температуры) может быть велико и ограничивается только такими техническими ограничениями, как диапазон измеряемых температур, стоимость термометра, срок его эксплуатации. Мы можем воспользоваться для создания термопары дешевыми сплавами (например, хромель-алюмель), при этом диапазон измеряемых температур составит от –270 °C до +1370 °C. Эта термопара хорошо работает при измерении низких отрицательных температур, но служит недолго при измерении высоких положительных температур. Для измерения высоких положительных температур принято использовать термопару из чистой платины и сплава платины с родием. Таблица ее градуировки накрывает интервал от –50 °C до +1760 °C. Чтобы сталевар мог измерить температуру расплавленной стали, ему приходится использовать термопару из благородных платиновых проводков, причем сплав платины и родия дороже чистой платины.

Примерно такая же ситуация должна возникать и в информатике. Энтропия Шеннона – это общая шкала энтропии, с которой все согласны (как с температурой в обычном мире). Однако параллельно с информационной энтропией Шеннона существуют:

– энтропия Берга;
– энтропия Цаллиса;
– энтропия Колмогорова;
– энтропии Хэмминга;
– ::::::::::::::::::::::::::::::::::

Для нас важно то, что шкал энтропии может быть достаточно много, но все они как-то связаны между собой. В информатике должна быть ситуация такая же, как при изменении температуры в технике как

меры соотношения хаоса и порядка в газах. Эта проблема обостряется с быстрыми темпами развития технологий искусственного интеллекта. Естественный и искусственный интеллект – это эффективные инструменты борьбы с хаосом окружающего мира (с внешней энтропией).

То, на сколько наши естественные мозги или наши искусственные мозги точно научены предсказывать будущее, является противодействием энтропии окружающего мира. Соответственно, качество работы естественного и искусственного интеллекта должно измеряться разницей энтропии (неопределенности) до применения интеллекта и после его вмешательства.

Очевидным это стало с созданием и применением нейросетевых преобразователей биометрии в код личного криптографического ключа пользователя. Биометрия и криптография являются эффективными средствами защиты цифровых гражданских прав личности. Все операции с биометрией и все операции по реализации криптографии должны быть правильно выполнены в соответствии с требованиями национальных или международных стандартов. Криптографы точно знают, что правильно выполненные криптографические преобразования должны в итоге приводить к шифротекстам, очень похожим на идеальный «белый шум». В этом случае каждый разряд шифротекста будет нести один бит энтропии Шеннона.

Казалось бы, все очень просто, криптографический ключ длинной 256 бит должен быть носителем энтропии в 256 бит. Для этой цели генератор, от которого получают криптографические ключи, должен быть кем-то заранее проверен на близость к «белому шуму». Если такой проверки не было, то ее нужно выполнить подручными средствами. И тогда начинаются значительные технологические сложности. Вычислять энтропию по Шеннону технически крайне сложно, эта задача имеет экспоненциальную вычислительную сложность.

Просвет в этой проблеме появился в 2011 г., когда Россия ввела в действие свой национальный стандарт ГОСТ Р 52633.3 по тестированию нейросетевых преобразователей биометрии в код на малых выборках. Фактически по этому стандарту оценивается энтропия нейросетевых откликов в пространстве расстояний Хэмминга. Можно говорить о возможности вычисления энтропии Хэмминга, с одной стороны отражающей некоторые аспекты энтропии Шеннона, а с другой стороны – имеющей линейную вычислительную сложность. Формально могут быть выполнены работы по связыванию шкалы энтропии Хэмминга со шкалой энтропии Шеннона.

В данном справочнике собраны известные на текущий момент данные о связи энтропии Хэмминга – Пирсона с энтропией Шеннона – Пирсона. Из определений белого шума следует, что разряды его бинарных последовательностей должны быть независимы. В свою очередь независимость разрядов двух бинарных последовательностей

может быть оценена классической формулой парных корреляций Пирсона – Эджуорта – Эдлтона (конец XIX в.). Получается, что мы с одной стороны остаемся в пространстве бинарных кодов, как и Хэмминг, а с другой стороны при сравнивании кодов вычисляются коэффициенты корреляции. Эта комбинация позволяет оценивать энтропию при квадратичной вычислительной сложности.

Очевидно, что совместное использование энтропии Хэмминга (линейная сложность), энтропии Хэмминга – Пирсона (квадратичная сложность) и энтропии Шеннона – Пирсона должны дополнять друг друга и при этом существенно лучше отражать основную классическую энтропию Шеннона (экспоненциальная вычислительная сложность).

На сколько эффективно смогут быть использованы в будущем процедуры оценки энтропии Хемминга – Пирсона и Шеннона – Пирсона, сегодня сказать трудно. Однако для них наблюдается явная аналогия со стандартами термопар. Температурные шкалы термопар описываются либо таблицами, либо полиномами. И те, и другие математические конструкции могут быть использованы при связывании шкал энтропии Шеннона и энтропии Хэмминга – Пирсона, а также энтропии Шеннона – Пирсона. То, как формируются таблицы шкал, и полиномы шкал, является методологической основой данного справочника. Мир един: значительной разницы между измерением температуры в физическом мире и оцениванием информационной энтропии Шеннона не должно быть.

1. ФОРМИРОВАНИЕ ТАБЛИЦ КУСОЧНО-ЛИНЕЙНОГО СВЯЗЫВАНИЯ ЭНТРОПИИ ШЕННОНА НИЗКИХ РАЗМЕРНОСТЕЙ С КОЭФФИЦИЕНТОМ ПАРНОЙ КОРРЕЛЯЦИИ ПИРСОНА

1.1. Оценка двухмерной энтропии Шеннона при разном значении коэффициентов парной корреляции

Рассмотрим численную реализацию оценки двухмерной энтропии Шеннона:

$$H("x_1, x_2") = -\sum_{i=1}^{4} P_i \cdot \log_2(P_i), \quad (1)$$

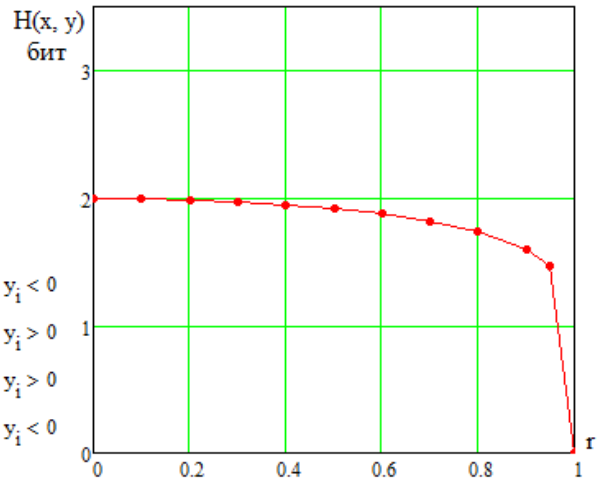
где переменные «x_1» и «x_2» могут принимать либо состояние «0», либо состояние «1».

В этом случае возможно только четыре кодовых состояния. Если какое-то кодовое состояние из четырех будет не обнаружено, то программа зависнет, так как состояние логарифма от нуля не определено. Для выполнения программы вычисления функционала (1) придется увеличивать размер выборки до момента, пока все четыре состояния в ней не появятся.

На рис. 1 представлена программная реализация оценки двухмерной энтропии Шеннона при заданном значении коэффициента парной корреляции (размер выборки – 3000 опытов).

Следует отметить, что в программе, написанной на языке MathCAD (левая часть рис. 1), используется размер выборки в 3000 опытов, а коэффициент корреляционной сцепленности данных задается параметром a. Значение регулируемого параметра a, показатель корреляционной сцепленности двух переменных и значение энтропии Шеннона приведены в таблице, расположенной в нижней части рис. 1.

$H :=$
$x \leftarrow rnorm(3000, 0, 1)$
$x1 \leftarrow rnorm(3000, 0, 1)$
$a \leftarrow 1.74$
$y \leftarrow \frac{x + a \cdot x1}{\sqrt{1 + a^2}}$
$s \leftarrow (0 \ 0 \ 0 \ 0)^T$
for $i \in 0..2999$
$s_0 \leftarrow s_0 + 1$ if $x_i < 0 \wedge y_i < 0$
$s_3 \leftarrow s_3 + 1$ if $x_i > 0 \wedge y_i > 0$
$s_1 \leftarrow s_1 + 1$ if $x_i < 0 \wedge y_i > 0$
$s_2 \leftarrow s_2 + 1$ if $x_i > 0 \wedge y_i < 0$
$H \leftarrow \sum_{i=0}^{3} \frac{-s_i \cdot \log\left(\frac{s_i}{3000}, 2\right)}{3000}$
$(corr(x,y) \ H)^T$



n	0	1	2	3	4	5	6	7	8	9	10	11
a	100	10	4.91	3.2	2.3	1.74	1.34	1.025	0.755	0.486	0.33	0
corr(x,y)	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95	1
H	2	1.996	1.988	1.972	1.949	1.917	1.875	1.815	1.731	1.592	1.471	0

Рис. 1. Связь значения двухмерной энтропии от значения парной корреляции между двумя переменными

Выборки в 3000 опытов вполне достаточно для оценки значений двухмерной энтропии. Программа не зависает.

1.2. Оценка пятимерной энтропии Шеннона при разном значении коэффициентов парной корреляции

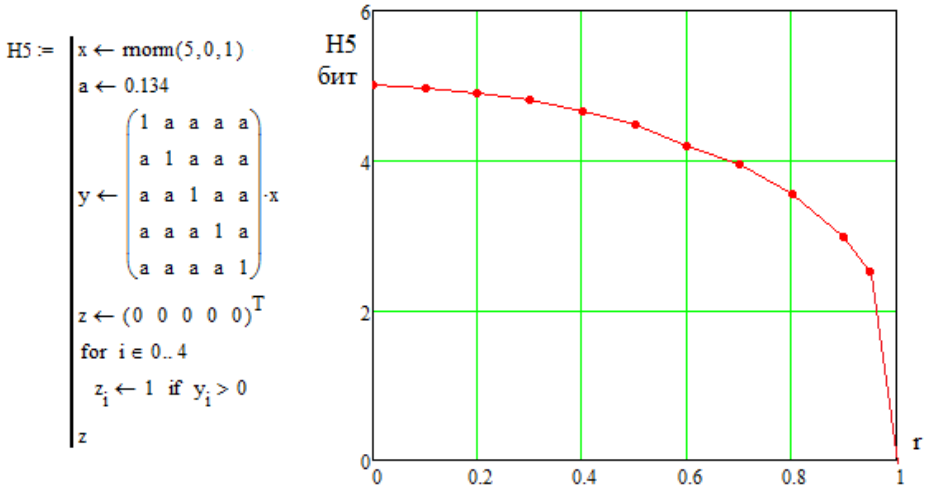
Рассмотрим численную реализацию оценки пятимерной энтропии Шеннона:

$$H("x_1, x_2, x_3, x_4, x_5") = -\sum_{i=1}^{32} P_i \cdot \log_2(P_i), \qquad (2)$$

где переменные «x_1», …, «x_5» могут принимать либо состояние «0», либо состояние «1».

В этом случае возможно 32 кодовых состояния. Если какое-то кодовое состояние из 32 будет не обнаружено, то вычисления функционала (2) может зависнуть (логарифм состояния «0» не определен).

На рис. 2 приведена программная реализация численного эксперимента по оценке значений связи пятимерной энтропии с разными значениями коэффициентов равной коррелированности между пятью переменными.



n	0	1	2	3	4	5	6	7	8	9	10	11
a		0.047	0.091	0.134	0.178	0.2245	0.277	0.3385	0.417	0.536	0.637	0
corr(x,y)	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95	1
H	5	4.967	4.897	4.801	4.646	4.477	4.186	3.95	3.559	2.974	2.52	0

Рис. 2. Связь значения пятимерной энтропии Шеннона от значений равной парной корреляции между пятью переменными

Из рис. 2 видно, что максимальное значение энтропии оказывается для независимых данных. По мере роста корреляционной сцепленности значение энтропии падает до нуля, когда все пять переменных имеют предельно высокое значение корреляции.

Следует отметить, что для получения данных программа в левой части рис. 2 была запущена 3000 раз. На столь большой выборке наблюдаются все 32 возможных состояния для всех коэффициентов корреляционной сцепленности. Проблем с объемом используемой выборки в 3000 опытов не возникает, так как она примерно в 100 раз больше, чем возможное число состояний анализируемого кода.

1.3. Номограмма связи кривых низкоразмерных энтропий с показателем равной корреляционной сцепленности анализируемых данных

Следует отметить, что выборка, на которой производятся вычисления, должна быть как минимум в 10 раз больше, чем число

возможных состояний анализируемого бинарного кода. В этом контексте выборка в 3000 опытов вполне пригодна для оценки значений восьмимерной энтропии $H(«x_1, x_2, \ldots, x_8»)$ симметризованных данных, так как все 256 возможных состояний кода на такой выборке встречаются с достаточно высокой вероятностью – 0.92.

Таким образом, на выборке в 3000 опытов мы можем экспериментально получить номограмму низкоразмерных энтропий Шеннона, приведенную на рис. 3.

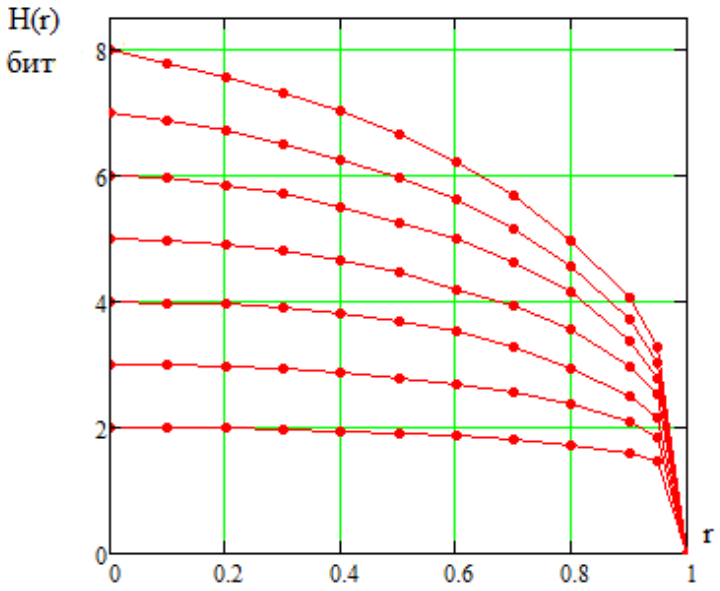


Рис. 3. Номограмма низкоразмерных энтропий Шеннона как функций данных с равной корреляционной сцепленностью – r

Из рис. 3 видно, что максимальные значения энтропии соответствуют независимым данным r = 0. В этом случае размерность задачи точно совпадает с числом бит энтропии Шеннона. Ниже приведена табл. 1, соответствующая данным номограммы рис. 3.

Таблица 1

Таблица связи значений энтропии Шеннона с коэффициентами корреляции

corr(x,y)	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	0.95	1
Энтропия Шеннона биты	2	1.996	1.988	1.972	1.949	1.917	1.875	1.815	1.731	1.592	1.471	0
	3	2.989	2.964	2.923	2.866	2.79	2.691	2.56	2.376	2.09	1.852	0
	4	3.984	3.957	3.905	3.821	3.7	3.53	3.27	2.923	2.499	2.153	0
	5	4.967	4.897	4.801	4.646	4.477	4.186	3.95	3.559	2.974	2.52	0
	6	5.959	5.853	5.713	5.282	5.262	4.99	4.614	4.145	3.38	2.767	0
	7	6.89	6.708	6.514	6.264	5.963	5.61	5.155	4.559	3.714	3.022	0
	8	7.728	7.563	7.315	7.035	6.664	6.229	5.695	4.973	4.048	3.278	0

2. ПЕРЕХОД ОТ КУСОЧНО-ЛИНЕЙНОГО ПРИБЛИЖЕНИЯ МНОГОМЕРНОЙ ЭНТРОПИИ ШЕННОНА К ЕЕ ПОЛИНОМИАЛЬНЫМ ПРИБЛИЖЕНИЯМ

2.1. Полиномиальное приближение связи восьмимерной энтропии Шеннона с коэффициентами равной коррелированности данных

Практика стандартизации градуировочных характеристик термопар свидетельствует о том, что, наряду с табличным (кусочно-линейным) приближением, активно используются приближающие полиномы. Обычно используются полиномы, учитывающие от 6 до 12 членов степенного ряда.

Следует признать подобную практику положительной. В связи с этим рассмотрим полиномиальный способ приближения многомерных энтропий Шеннона полиномами, совпадающими с экспериментальными данными в двух и более точках.

Для определенности воспользуемся квадратичным полиномом для приближения восьмимерной энтропии Шеннона:

$$H_8(\mathrm{r}) = 8 \cdot \sqrt[2]{1 - r}. \qquad (3)$$

На рис. 4 представлены графики восьмимерной энтропии и ее приближения.

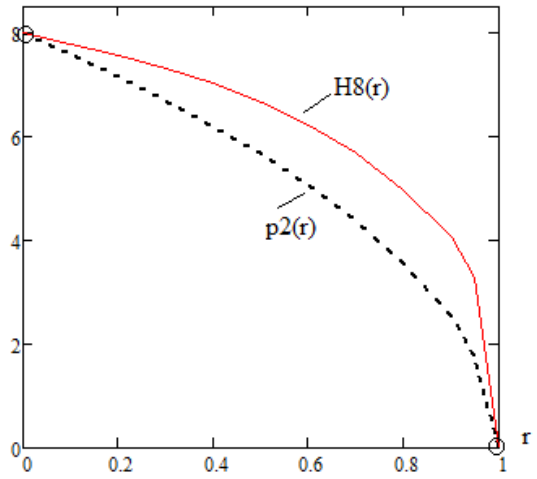


Рис. 4. Приближение экспериментальных значений энтропии H8(r) полиномом второго порядка p2(r)

Из рис. 4 видно, что аппроксимация вида (3) дает значительную погрешность. Точное совпадение приближения наблюдается только в двух точках r = 0 и r = 1.

Для того, чтобы снизить ошибку приближения, увеличим степень полинома до дробной величины n = 3.5 с двумя дополнительными точками полного совпадения:

$$H_8(\mathrm{r}) = 8 \cdot \sqrt[3.5]{1-r}. \qquad (4)$$

Повышение точности приближения и появление двух дополнительных точек пересечения иллюстрируется рис. 5.

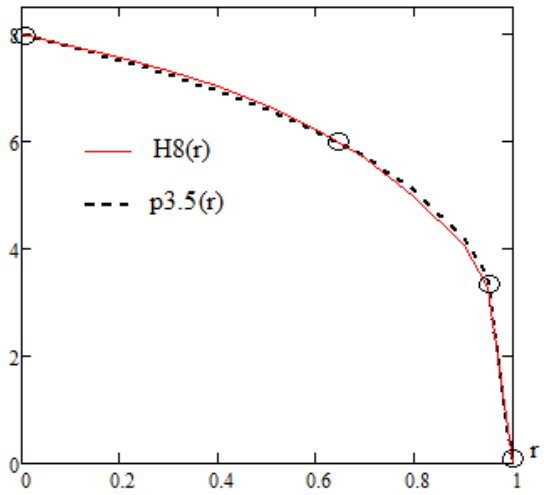


Рис. 5. Повышение точности приближения и появление двух дополнительных точек пересечения при использовании полинома с дробной степенью

Из рис. 5 следует, что полином вида (4) дает значения меньше экспериментальной функции *H*8(r) на участке от r = 0 до r = 0.62. На следующем участке от r = 0.62 до r = 0.96 полином дает завышенное значение приближаемой функции.

2.2. Полиномиальные приближения низкоразмерных энтропий Шеннона с пересечением в четырех точках экспериментальных кривых

Очевидно, что процедуру приближения экспериментально полученных данных энтропии можно применить и к другим ветвям низкоразмерных энтропий (рис. 5). Так, в случае применения полинома к данным энтропии 7-й размерности корень будет иметь показатель 4:

$$H_7(\mathrm{r}) = 7 \cdot \sqrt[4]{1-r}. \qquad (5)$$

Снижение размерности энтропии Шеннона приводит к росту степени корня аппроксимирующего экспериментальные данные полинома. Так, снижение размерности энтропии до 6 приводит к повышению показателя корня до 4.5:

$$H_6(\mathrm{r}) = 6 \cdot \sqrt[4.5]{1-r}. \tag{6}$$

Снижение размерности до 5 приводит к повышению показателя корня до 5:

$$H_5(\mathrm{r}) = 5 \cdot \sqrt[5]{1-r}. \tag{7}$$

Процесс продолжается и далее при уменьшении размерности решаемой задачи полиномиальной аппроксимацией данных:

$$H_4(\mathrm{r}) = 4 \cdot \sqrt[5.5]{1-r}, \tag{8}$$

$$H_3(\mathrm{r}) = 3 \cdot \sqrt[6]{1-r}, \tag{9}$$

$$H_2(\mathrm{r}) = 2 \cdot \sqrt[6.5]{1-r}. \tag{10}$$

Получается, что понижение размерности реальных данных энтропии Шеннона на единицу приводит к росту показателя корня аппроксимирующего полинома не 0.5.

2.3. Линейная экстраполяция степеней корня на размерности энтропии Шеннона от 9 и выше

В силу того, что приведенные выше зависимости достаточно просты, мы имеем возможность построить связи степени корня (степени полинома, представленного корнем) для того, чтобы предсказать, когда корень выродится, преобразуясь в полином первого порядка. На рис. 6 представлена прямая линия дискретного изменения степени корня (полинома) с ростом порядка приближаемой им энтропии Шеннона.

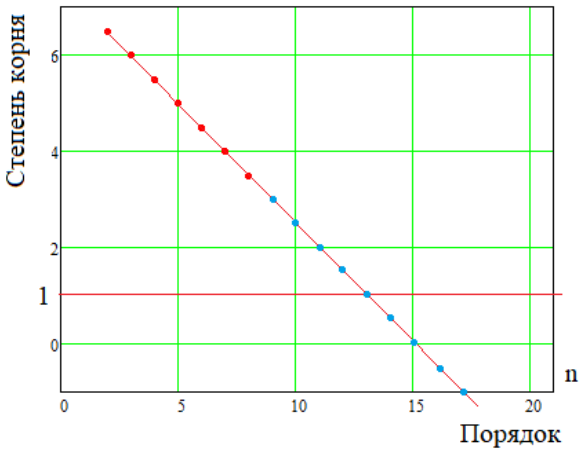


Рис. 6. Прогнозирование степени корня приближающих полиномов в зависимости от порядка энтропии Шеннона

Из рис. 6 видно, что, оставаясь на одной линии степени приближающих энтропии полиномов, должны иметь значения 3, 2.5, 2, 1.5, 1. То есть экспериментальные энтропии Шеннона размерности 9, 10, 11, 12, 13 должны приближаться следующими полиномами:

$$H_9(\mathrm{r}) = 9 \cdot \sqrt[3]{1-r}, \tag{11}$$

$$H_{10}(\mathrm{r}) = 10 \cdot \sqrt[2.5]{1-r}, \tag{12}$$

$$H_{11}(\mathrm{r}) = 11 \cdot \sqrt[2]{1-r}, \tag{13}$$

$$H_{12}(\mathrm{r}) = 12 \cdot \sqrt[1.5]{1-r}, \tag{14}$$

$$H_{13}(\mathrm{r}) = 13 \cdot \sqrt[1]{1-r} = 13 \cdot (1-r)^1. \tag{15}$$

Последний полином 13-й размерности уже не является корнем, превратившись в обычный полином первого порядка.

2.4. Шкалы нормированных значений низкоразмерной энтропии Шеннона как функций корреляционной сцепленности разрядов

Опираясь на полученные выше приближающие полиномы, мы можем перейти к нормированной энтропии и увидеть, как постепенно происходит эволюция полиномов в сторону линейной связи энтропии Шеннона 13-й размерности к шкале коэффициентов равной коррелированности разрядов. На рис. 7 представлена соответствующая номограмма кривых.

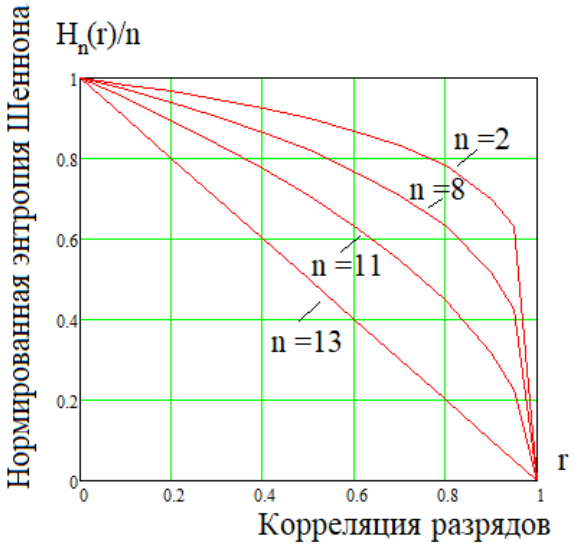


Рис. 7. Низкоразмерные шкалы энтропии Шеннона, постепенно превращающиеся с ростом размерности в линейную шкалу при n = 13

Из рис. 7 видно, что после нормировки энтропий их значение не может превышать единицы. Фактически нормированные значения отражают мультипликативный коэффициент снижения значения энтропии с ростом равной коррелированности разрядов исследуемой бинарной последовательности.

2.5. Шкалы нормированных значений высокоразмерной энтропии Шеннона как функций корреляционной сцепленности разрядов

После того как размерность энтропии оказывается выше тринадцатой, степень аппроксимирующего реальные данные полинома по-прежнему продолжает монотонно увеличиваться на 0.5 при увеличении размерности на единицу. То есть энтропии высоких размерностей будут аппроксимироваться следующими полиномами:

$$H_n(\mathrm{r}) = n \cdot (1 - r)^{(\frac{n}{2} - 5.5)}. \qquad (16)$$

Шкалы нормированных энтропий Шеннона 13-й размерности и выше иллюстрируются номограммами, приведенными на рис. 8.

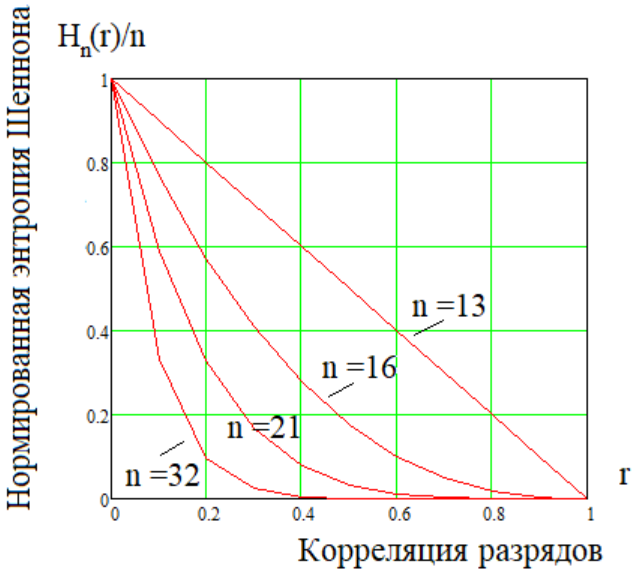


Рис. 8. Высокоразмерные шкалы энтропии Шеннона, описываемые обычными полиномами все более и более высоких порядков

Очевидно, что с ростом размерности энтропии Шеннона выше 32 приближающие полиномы должны все больше и больше прижиматься к вертикальной оси координат. То есть для высокоразмерных

оценок энтропии Шеннона правая часть шкалы корреляционной сцепленности теряет смысл. В связи с этим для высоких размерностей энтропии (64 и 128 бит) кривые приближающих их полиномов приведены на рис. 9.

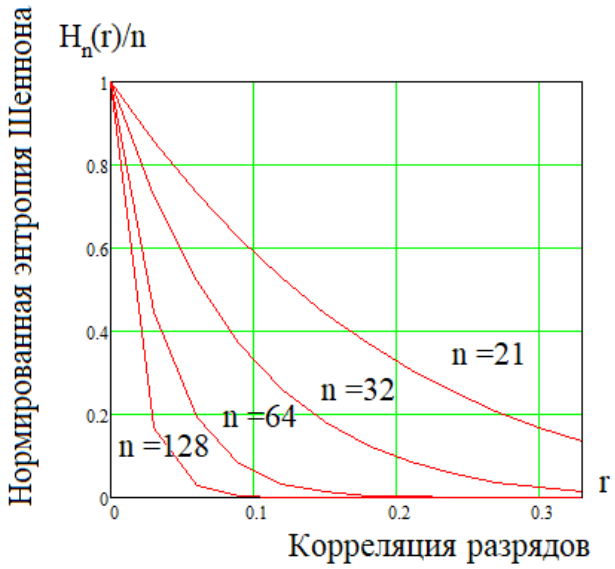


Рис. 9. Высокоразмерные шкалы энтропии Шеннона, уже пригодные для использования «ослабленной» криптографией с длиной ключа 64 и 128 бит

3. ОСНОВА ВЫСОКОРАЗМЕРНЫХ ВЫЧИСЛЕНИЙ – ЭТО ЕСТЕСТВЕННЫЙ НЕЙРОН, КАК БАЗОВЫЙ ЭЛЕМЕНТ, ВОСПРОИЗВОДЯЩИЙ КОНТИНУАЛЬНО-КВАНТОВЫЕ ПРЕОБРАЗОВАНИЯ

3.1. Некоторые исторические параллели

Казалось бы, что изложенный выше материал относится к криптографии, а именно к оценке качества криптографических ключей, полученных от некоторого источника; что это достаточно частная задача некоторого частного научно-технического направления развития общих технологий. На самом деле это все не менее значимо, чем измерение температуры. Значимость этих проблем будет только усиливаться по мере информатизации общества и параллельного развития приложений искусственного интеллекта.

Поясним ситуацию, вернувшись к классической работе Маккалока и Питтса 1943 г. [1]. На тот момент не было современных ЭВМ, кроме одной, которая была спрятана англичанами под Лондоном в Блетчли-парке. Эта машина расшифровывала перехваченные по радиоэфиру немецкие шифротексты. Возьмем точку 1943 г. как точку старта развития как обычных ЭВМ (дискретная логика), так и нейроЭВМ (аналого-дискретной логики).

Мы видим, что за прошедшие 80 лет обычные компьютеры бурно развивались, и сегодня мы имеем их огромные вычислительные ресурсы. При этом вся общедоступная математика, которая была создана человечеством за последние несколько тысяч лет, уже коммерциализована в виде приложений: MathCAD, MatLAB, …, Windows, Linux.

Уже созданной ранее математики сегодня недостаточно, сегодня принято называть искусственным интеллектом. Коммерсанты активно пытаются приватизировать и эти технологические продукты в виде читающих автоматов, переводчиков с одного языка на другой, голосовых помощников («Алиса», «Маруся», …), чата GPT. При этом у коммерсантов возникают огромные технические проблемы с размерами приложений искусственного интеллекта и их энергопотреблением. Так, «Алиса» и «Маруся» не могут разместиться в телефоне, им обязательно нужно гнездиться в интернет-«облаках», на очень больших серверах их коммерческих владельцев. Сколько «Алиса» и «Маруся» занимают памяти и сколько потребляют энергии, никто не знает – это коммерческая тайна.

3.2. Бионика связей естественных нейронов живых существ

Следует отметить, что удачная парадигма бинарных нейрологических вычислений впервые была сформулирована Питтсом и Маккалоком в 1943 г. [1] и послужила стартом для ряда последующих исследований. В 1949 г. Дональд Хэбб [2] опубликовал первый работоспособный алгоритм обучения искусственных нейронов. Еще один значимый шаг сделал нейрофизиолог Фрэнк Розенблатт в 1957 г., создавший в Корнуэльской лаборатории аэронавтики персептрон. Он же создал первый программный эмулятор нейрокомпьютера «Марк-1» на цифровой вычислительной машине IBM-704 в 1960 г. Это оказало огромное влияние на общественное внимание к тематике создания нейрокомпьютеров.

Гораздо более быстрыми темпами в 40-х и 50-х гг. прошлого века развивались обычные на сегодня компьютеры с обычной булевой логикой. К настоящему времени вычислительных ресурсов цифровой логики вполне достаточно, однако их возможности значительно уступают возможностям естественных вычислителей людей и живых существ. Так, мы, люди, способны в реальном времени решать 10 000-мерные задачи. У нас и у животных есть большие пирамидальные естественные нейроны с 10 000 входами.

Во многом теория искусственных нейронов строилась дублированием логики развития цифровых компьютеров. Это обусловлено простотой моделирования персептронов и искусственных нейронов с непрерывными выходными функциями. При моделировании на обычных компьютерах не возникает проблемы обеспечения питания вычисляющих элементов, нет проблемы поддерживания состояний «0» или состояний «1» на выходах обычной булевой логики или на выходе персептрона Розенблатта.

Совершенно иная ситуация возникает в живых организмах, естественные нейроны не имеют доступа к общему источнику электропитания. Каждый нейрон вынужден самостоятельно вырабатывать энергию на каждый выходной импульс. Передача данных между естественными нейронами живых существ выполняется пачками импульсов [3, 4], как это отражено на рис. 10.

Выходной отросток естественного нейрона (аксон) имеет длину в десятки раз больше тела нейрона. Аксоны играют роль длинных «плохих» проводов передачи информации с очень плохой изоляцией. Формально естественный нейрон одновременно выполняет вычисления и параллельно выполняет роль «модема», передающего и принимающего информацию. Так как проводящие свойства аксонов много хуже проводящих свойств хорошо изолированных медных проводов, аксоны нейронов не могут быть слишком длинными.

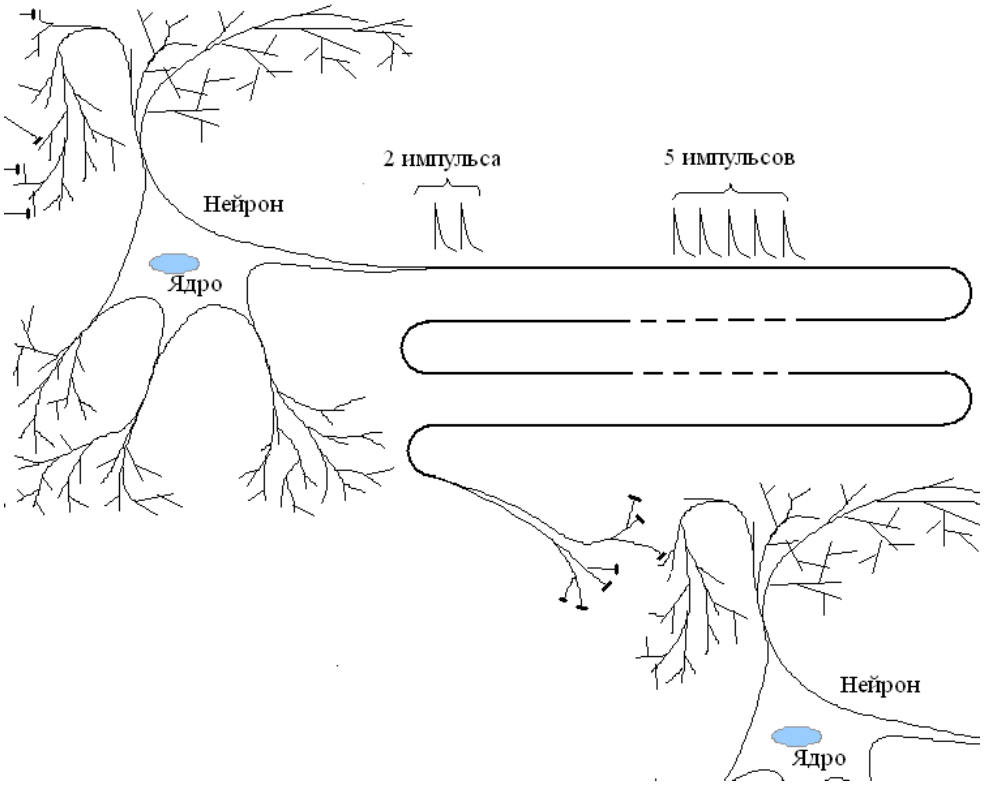


Рис. 10. Естественный нейрон одновременно является и вычислителем, и «модемом» передачи данных по длинной линии – аксону (импульсы – это вынужденный прием, являющийся следствием отсутствия «батареек» внутри «нейромодема»)

В первом приближении импульсы в аксонах можно рассматривать как реализацию некоторых протоколов передачи информации «нейромодемов/электрогенераторов». Видимо, какая-то часть нейронов может почти не заниматься вычислениями, а играет основную роль только как ретранслятор на дальние расстояния по плохим длинным линиям передачи данных в аксонах.

3.3. Концепция нейросетевой молекулы, преобразующей высокоразмерный входной континуум в дискретный спектр выходных

Заметим, что если бы была верна бинарная гипотеза Питтса – Маккалока [1], то физиологи могли бы наблюдать только отклики бинарных естественных нейронов. В этом случае нейроны должны выдавать один импульс, соответствующий состоянию «0», либо должны выдавать два импульса, соответствующие состоянию «1». Физиологи

же наблюдают пачки импульсов [3] на аксонах естественных нейронов (на рис. 11 изображена пачка из двух импульсов и пачка из 5 импульсов). То есть, оставаясь в рамках парадигмы Питтса – Маккалока [1], мы должны констатировать то, что логика естественных нейронов является Q-арной, а не бинарной.

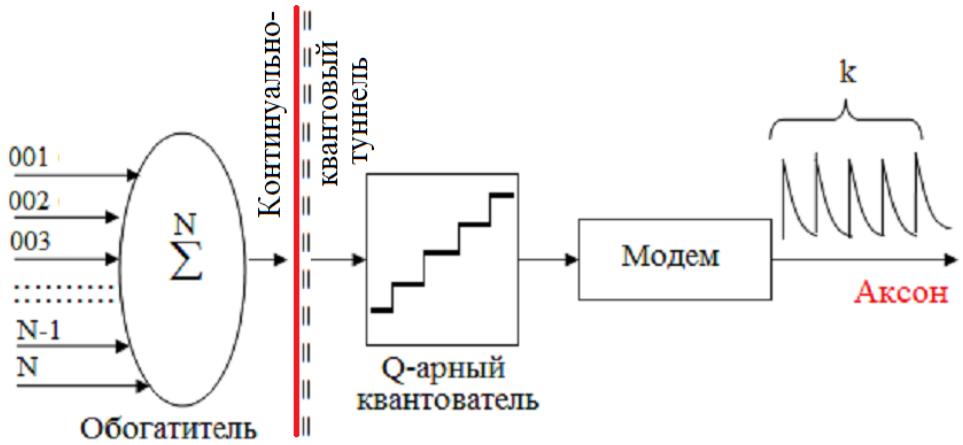


Рис. 11. Представление естественных нейронов в виде программной нейромолекулы, воспроизводящей эффект континуально-квантового перехода на микроуровне

Переходя к замене бинарной нейрологики Q-арной нейрологикой, мы вынуждены заменить в модели естественного нейрона Питтса – Маккалока бинарный персептрон на более сложный искусственный нейрон с Q-арным выходным квантователем. На рис. 12 приведена модель естественного нейрона, состоящая из Q-арного персептрона и выходного модема для передачи данных по плохой длинной линии аксона.

Заметим, что в начале XXI в. значительное внимание уделяется попыткам создания квантовых вычислителей, воспроизводящих на физическом уровне эффекты квантовой суперпозиции [4]. В этом контексте конструкцию рис. 12 мы имеем право считать некоторой программной реализацией нейромолекулы, воспроизводящей, например, свойства молекулы водорода. В этом случае Q-арный выходной квантователь должен иметь число выходных состояний (число ступенек), точно совпадающее с числом спектральных линий молекулы водорода. Спектр линий водорода приведен в нижней части рис. 12.

Показатель Q-арности (система счисления), в которой обучен естественный или искусственный нейрон, играет крайне важную роль [5]. В этом контексте физиолог, желающий оценить значение этого параметра, должен по экрану осциллографа [3] вести документирование числа импульсов в пачках конкретного аксона. Разница между максимальным числом импульсов и их минимальным числом будет являться

оценкой числа выходных состояний квантователя одного естественного нейрона.

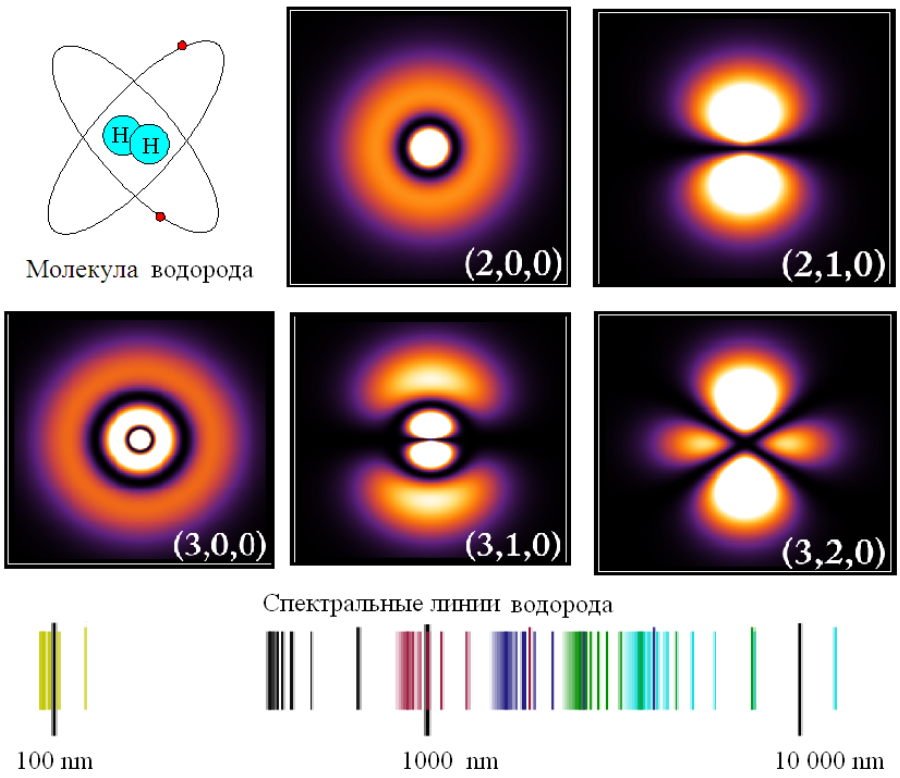


Рис. 12. Решение волнового уравнения для атома водорода, показывающее положение континуумов вероятного появления электронов (электронные облака) для разных значений волновых чисел

Следует отметить, что молекула водорода имеет порядка 32 спектральных линий, т.е. нейромодель молекулы водорода должна иметь выходной квантователь Q ≈ 32. Возможен иной вариант, когда модель собирается из нескольких искусственных нейронов [6], в этом случае сами нейроны могут быть бинарными. Если модель состоит из n искусственных бинарных нейронов, то число выходных состояний нейросетевой молекулы составляет $Q = 2^n$ возможных выходных состояний.

Последние 30 лет физико-математическая общественность значительное внимание уделяет квантовым вычислениям и квантовой информатике [7, 8]. Формально это все можно свести к попыткам перенести вычисления на микроуровень молекулы водорода и найти условия, при которых она сможет играть роль квантового триггера или иного квантово-логического элемента. Как это все должно выглядеть со стороны математики и программирования, давно изложено на бумаге [7, 8].

Однако бумага все стерпит, особенно, если ее много. Параллельно с бумагой всегда должны создаваться физические реализации новых принципов вычислений. В этом контексте особенных успехов пока нет. Вполне возможно, что их не будет в обозримом будущем.

Моя убежденность в этом опирается на бионику. Природа уже давно создала условия, как угодно длительного воспроизведения эффектов квантовой суперпозиции в форме естественных нейронов всех живых существ (см. рис. 10). Модем внутри естественного нейрона – это окончание абсолютно устойчивого фрагмента континуально-квантовых вычислений. При этом нет необходимости в жидком гелии, ионных ловушках, микрополяризаторах, синтезе нужных дефектов в кристалле алмаза. Вполне достаточно полужидкого «холодца» в наших головах при температуре от 22 до 42 °С и погруженных в этот «холодец» наших естественных нейронов.

Инженерам не следует ждать, когда в Зеленограде или на Тайване испекут для нас микросхемы или микропроцессоры с квантовой логикой на новых физических принципах. В этом контексте нужно брать то, что уже есть, и копировать природу. В результате мы получим так называемые нейроморфные конструкции [9]. Оказалось, что для кардинального снижения энергопотребления при очень сложных вычислениях достаточно в аппаратно-программной среде, эмулирующей искусственные нейроны соединять ядра, их реализующие, через USB-протоколы. Вместо модемов в начале аксона по рис. 10 модель искусственного нейрона реализует USB-протокол передачи данных. Как все оказалось просто и непритязательно. Думаю, что это видимость простоты, под ней лежит очень серьезная математика, которая пока еще на бумаге не изложена.

3.4. Некоторые полезные аналогии с уже существующей математики квантовых вычислений

Строгая математика квантовых вычислений построена на понятии «КуБита» [7, 8]. На сколько дрожание выходных бит нейросетевого преобразователя [10] близко к теоретической модели «КуБита» – вопрос открытый. Однако при тестировании нейросети по рекомендациям ГОСТ Р 52633.3–2011 [11] всегда биты выходного кода нейросети начинают «дрожать», как это показано на рис. 13.

Из рис. 13 видно, что для каждого из 30 тестовых образов «Чужой» мы наблюдаем некоторый фрагмент 256 «КуБитной» квантовой суперпозиции. Если обработка каждого образа длится 10 ms, то мы программно поддерживаем эффект квантовой суперпозиции 300 ms.

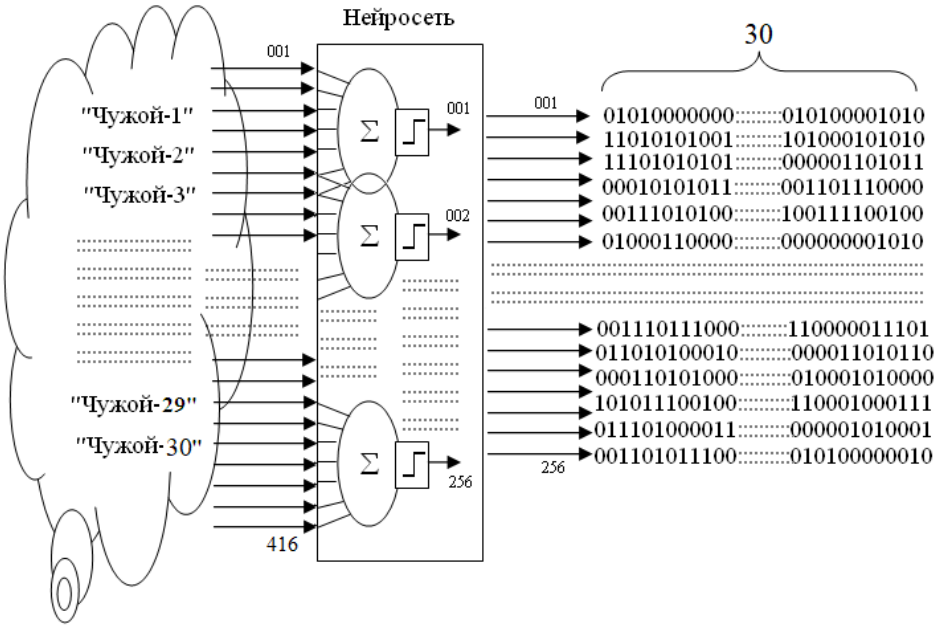


Рис. 13. Эффект «дрожания» выходных разрядов нейросети при предъявлении 30 случайных тестовых образов

Если этого времени нам недостаточно, то мы имеем возможность программно поддерживать эффект квантовой суперпозиции во много раз дольше за счет скрещивания между собой образов «Чужой» по ГОСТ Р 52633.2–2010 [12]. Из каждой пары образов-родителей «Чужой-n» удается получать 1, 2, 3, … n образов потомков и тем самым существенно увеличивать время поддержки квантовой суперпозиции. Формально следует добиваться того, чтобы времени поддержки квантовой суперпозиции было достаточно для решения поставленной задачи.

Отметим, что этот подход снимает проблему как выбора достаточно большого числа «КуБит», так и поддержки их квантовой суперпозиции достаточного для решения задачи интервала времени. Число «КуБит» задается числом нейронов в сети, а время поддержки задается числом используемых при моделировании примеров тестовых образов.

Гарантией того, что при тестировании нейросетевых преобразователей мы действительно наблюдаем что-то похожее на предсказанные на бумаге «КуБиты», является огромное ускорение тестирования и огромное сокращение потребностей в памяти [10].

3.5. Аналог понятия квантовой запутанности (квантовой сцепленности)

Кроме базового понятия «КуБита» важным является понятие квантовой сцепленности. Корректная теория квантовой сцепленности

(квантовой запутанности) для больших размерностей пока еще не создана. По этой причине укажем только метод ее оценки на данных среды моделирования «БиоНейроАвтограф» [13].

Среда моделирования [13] предназначена для проведения лабораторных работ студентами русскоязычных университетов без нарушения закона о персональных биометрических данных. Студент задает псевдослучайным программным генератором свой личный ключ длиной в 256 бит. Запомнить его студент не может, однако он может написать своим почерком манипулятором «мышь» одну или две буквы легко запоминаемого рукописного пароля. Для обучения нейросети нужно 8 и более примеров рукописного пароля «Свой». После автоматического обучения нейросети проверочный пример рукописного пароля «Свой» должен точно воспроизводить заданный ключ.

Если же манипулятором «мышь» студент пишет другой рукописный пароль, то на выходе преобразователя биометрия-код появляется случайный код. При этом для каждой реализации одного и того же рукописного пароля одним почерком будут появляться разные коды. Проще всего описать ситуацию с разными (но близкими) выходными кодами нейросети, перейдя в пространство расстояний Хэмминга:

$$"h" = \sum_{i=1}^{256} ("c_i") \oplus ("x_i"), \qquad (17)$$

где $"c_i"$ – состояние i-го разряда кода «Свой»; $"x_i"$ – состояние i-го разряда кода «Чужой»; $\oplus$ – операция сложения по модулю «два».

В пространстве расстояний Хэмминга легко оценивается энтропия Шеннона для разных биометрических образов «Чужой», эта ситуация отображена на рис. 14.

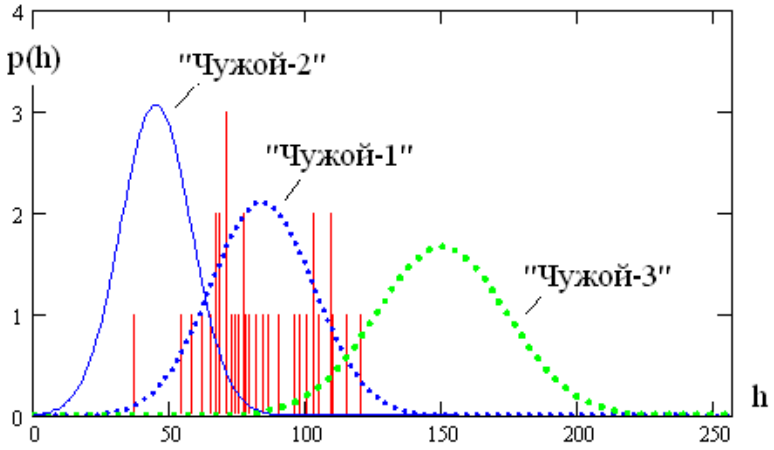


Рис. 14. Эффект нормального распределения откликов нейросети на биометрические образы «Чужой» в пространстве расстояний Хэмминга

В силу основной теоремы статистики (сложение случайных величин всегда нормализует сумму) переход от обычных длинных кодов к расстояниям Хэмминга (17) всегда приводит к нормализации данных. В связи с этим на рис. 14 распределения расстояний Хэмминга отображены нормальными распределениями.

Удобство такого представления данных позволяет «на лету» оценивать энтропию Шеннона по значениям математических ожиданий расстояний Хэмминга того или иного образа «Чужой». Из рис. 14 видно, что E(h1) ≈ 80 бит, E(h2) ≈ 45 бит, E(h3) ≈ 150 бит. Как результат, самым близким к образу «Свой» является образ «Чужой-2». Если мы построим генератор, воспроизводящий программно образы «Чужой-2», то получим отклик h = 0 с вероятностью $P_2 \approx$ pnorm(0,45,15) = 0.00135. Для расчетов использована функция MathCAD (pnorm(h,E(h),σ(h)), позволяющая найти вероятность появляния состояния h = 0 для нормально распределенных данных с математическим ожиданием 45 бит и стандартным отклонением 15 бит.

Следует отметить то, что предсказать вероятность удачной атаки $P_2 \approx 0.00135$ через моделирование данных образа «Чужой-2» удалось только потому, что мы перешли в пространство расстояний Хэмминга. В этом пространстве похожие образы оказываются рядом с друг другом.

Для нас принципиально важным является то, что похожие образы являются еще и сильно коррелированными. Они имеют как случайную компоненту, так и общую для них детерминированную компоненту. Примеры двух кодов образа «Чужой-2» приведены на рис. 15.

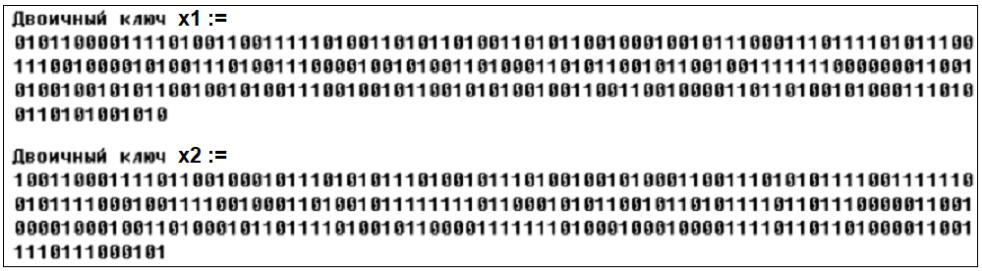


Рис. 15. Пример двух откликов нейросетевого преобразователя биометрии в код длиной 256 бит на двух разных примерах одного рукописного пароля «Чужой-2»

Беглое сравнение двух длинных ключей рис. 15 позволяет убедиться в том, что они разные (случайные). Однако они имеют между собой и существенное сходство. Их писал один и тот же человек, воспроизводя один и тот же рукописный пароль. Оценить уровень сходства удается, если вычислить коэффициент корреляции между двумя бинарными последовательностями одинаковой длины.

При оценке коэффициента корреляции используется классическая формула Пирсона – Эджуорта – Эдлтона конца XIX в.:

$$corr(x1, x2) = \sum_{i=1}^{256} \frac{("x1_i" - E(x1)) \cdot ("x2_i" - E(x2))}{256 \cdot \sigma(x1) \cdot \sigma(x2)}, \qquad (18)$$

где E(.) – операция вычисления математического ожидания; σ(.) – операция вычисления стандартного отклонения.

Если данные независимы, то функционал (18) должен давать малые по модулю значения. Если данные зависимы, то ситуация меняется. Для среды моделирования «БиоНейроАвтограф» коэффициент корреляционной сцепленности будет составлять примерно 0.33 для одинаковых рукописных паролей, написанных почерком одного и того же студента. Это и есть оценка показателя квантовой запутанности между состояниями 256 «КуБитной» квантовой суперпозиции. По сути дела, переход от расстояний Хэмминга по стандарту ГОСТ Р 52633.3 [11] к вычислению коэффициентов корреляции (18) между бинарными кодами [14, 15, 16] и приводит к простым алгоритмам быстрой оценки энтропии Шеннона квадратичной вычислительной сложности.

3.6. Причины высокой энергоэкономичности нейроморфных вычислений

Огромное потребление энергии существующими вычислителями может быть существенно снижено, если мы перейдем к использованию нейроморфных структур [9]. При этом в вычислительных структурах эмулировать модемы USB-протоколами (рис. 10 и рис. 11) нет необходимости. Покажем это на примере искусственного нейрона, генетически предобученного распознавать нормально распределенные данные состоянием «0». Этот нейрон является аналогом статистического критерия, построенного в прошлом веке проверки гипотезы нормальности распределения данных по значению стандартного отклонения выборки [17].

Программная реализация критерия приведена в левой части рис. 16 и написана на языке MathCAD. В правой части рис. 16 даны распределения вероятностей откликов критерия на нормально распределенные данные и равномерно распределенные данные.

Результаты численного эксперимента показали, что для малых выборок в 16 опытов (16 входов у искусственного нейрона) различить нормально распределенные данные удается с близкими вероятностями ошибок первого и второго рода $P_1 \approx P_2 \approx P_{EE} \approx 0.226$. Если увеличить в выборке число опытов до 32 (перейти к нейронам с 32 входами), то разделимость образов существенно увеличивается: $P_1 \approx P_2 \approx P_{EE} \approx 0.087$.

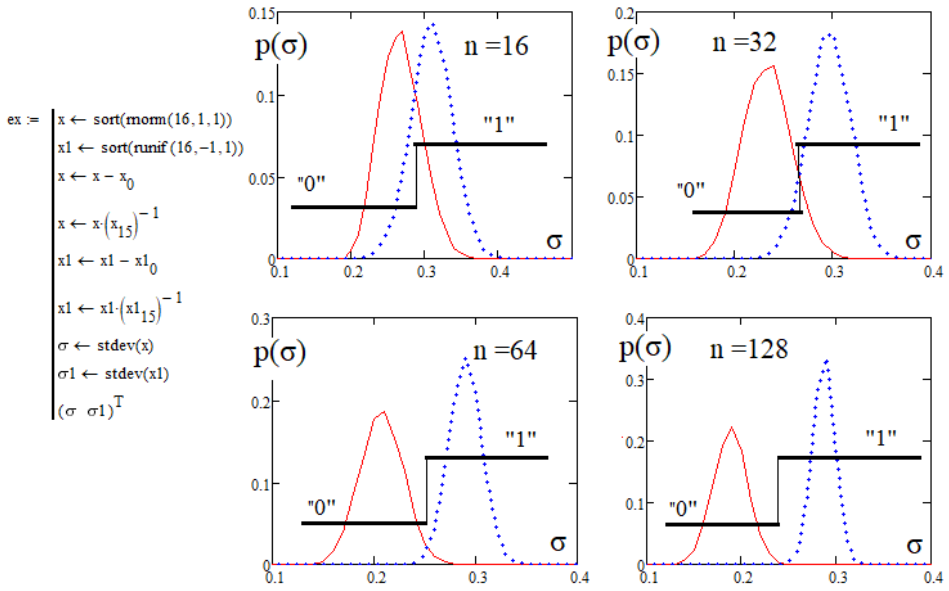


Рис. 16. Распределения откликов искусственных нейронов, построенных как аналог критерия проверки гипотезы нормального распределения при 16, 32, 64, 128 входах (состояние «0» – подтверждение гипотезы нормальности)

Следующее удвоение размеров выборки n = 64 приводит к снижению вероятностей ошибок до величины $P_1 \approx P_2 \approx P_{EE} \approx 0.014$. Мы наблюдаем экспоненциальное снижение вероятностей ошибок искусственного нейрона по мере роста объема анализируемой им выборки. При выборке n = 128 мы наблюдаем практически полную разделимость данных с нормальным и равномерным распределением: $P_1 \approx P_2 \approx \approx P_{EE} \approx 0.00005$ (распределения откликов критерия не перекрываются).

Рассмотренный нами численный эксперимент не является чем-то экзотическим. Это общее правило: рост числа входов у искусственных нейронов всегда приводит к экспоненциальному росту качества принимаемых им решений. Вопрос только в показателе роста качества экспоненты. В нашем численном эксперименте показатель экспоненциального роста качества оказался существенным (убедительным).

Важнейшим следствием экспоненциального роста является то, что, оказывается, выгодна замена двух бинарных нейронов с 16 входами на один 4-арный нейрон с 27 входами. Эта ситуация отображена на рис. 17.

По результатам численного моделирования (рис. 16) каждый из двух бинарных нейронов рис. 17 дает вероятность ошибок 0.226. Если оставаться в рамках линейной модели (двукратное увеличение входов нейрона должно приводить к двукратному увеличению его выходов), то 4-арный нейрон в правой части рис. 17 должен иметь 32 входа.

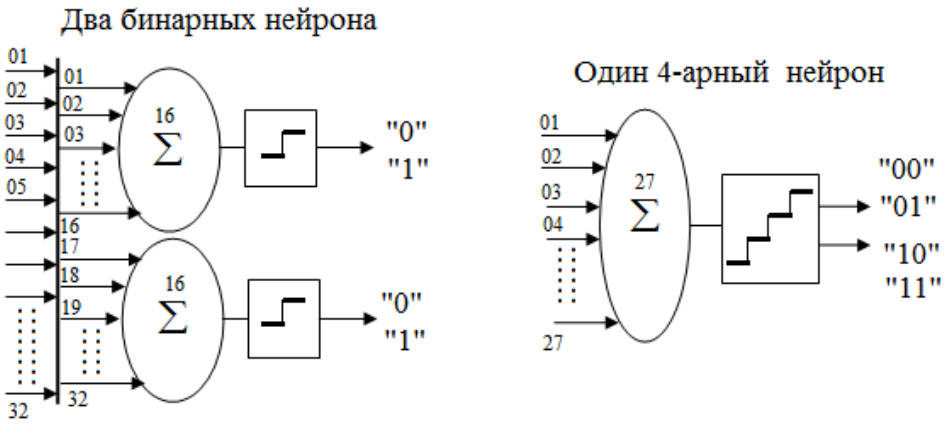


Рис. 17. Эквивалентная замена двух бинарных нейронов
с 16 входами на один 4-арный нейрон с 27 входами

Более точная экспоненциальная модель говорит о другом, у 4-арного эквивалентного нейрона достаточно иметь 27 входов. Следы графических вычислений, обосновывающих такое понижение, отображены на рис. 18.

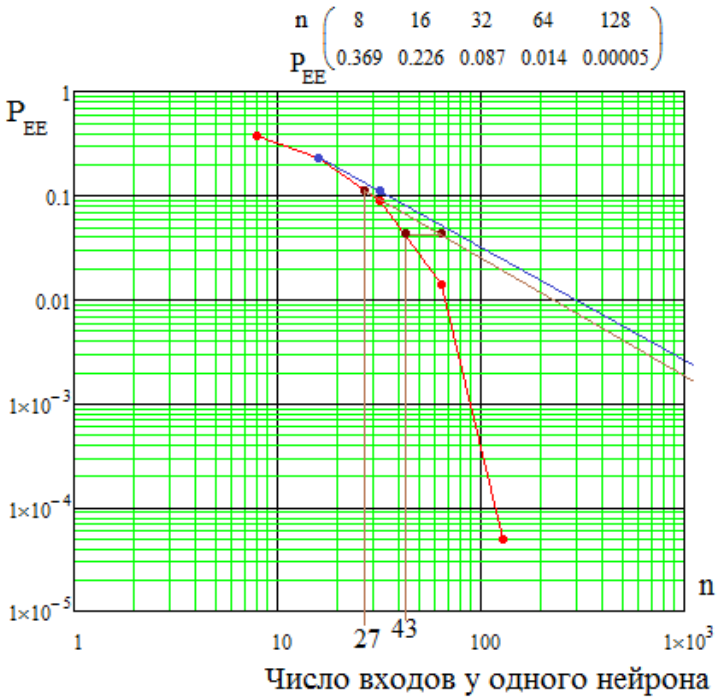


Рис. 18. Графические вычисления, позволяющие обосновать
снижение числа входов у эквивалентного 4-арного нейрона
при замене им двух бинарных нейронов

Мы наблюдаем снижение числа входов на 18,5 %. Если сеть бинарных нейронов сужается (последний слой имеет один бинарный нейрон), то замена последнего бинарного нейрона на 4-арный снижает число предыдущих бинарных нейронов на 18,5 %. Это и есть бионическая причина отсутствия в естественной природе естественных бинарных нейронов. Все естественные нейроны Q-арны, так как дают ощутимый выигрыш в числе предшествующих им естественных нейронов.

Более того, рост числа входов у нейронов усиливает выигрыш от замены последнего бинарного нейрона на Q-арный нейрон. Так, если мы в рис. 17 заменим бинарные нейроны с 16 входами на нейроны с 32 входами, то 4-арный эквивалентный нейрон будет иметь 43 входа в место 64. Это приведет уже к 48 %-й экономии потребляемой энергии искусствеными нейронами. Удвоение числа входов приводит к удвоению энергоэкономии.

Именно по этой причине естественные мозги людей имеют естественные нейроны с 10 000 входов. Именно большое число входов у естественных нейронов и обеспечивает низкое энергопотребление мозга в целом.

Следует так же отметить, что параллельно со снижением энергозатрат нейроморфные вычисления могут обеспечить значительные ускорения решения задач направленного перебора и снижение необходимого объема памяти при подобных вычислениях [18, 19].

ЗАКЛЮЧЕНИЕ

Используемые сегодня нейросети «глубокого обучения» имеют сотни слоев искусственных нейронов и требуют обучающих выборок в миллионы биометрических образов. При этом нейросети «глубокого обучения» передают информацию между одним слоем к следующему слою в псевдоцифровой форме (или псевдоаналоговой форме через кодировку 16-битными или 32-разрядными числами). Взять и заменить 16-битные данные или 32-битные данные на 4-битные выходные данные Q-арных нейронов кажется полным абсурдом. Тем не менее именно этот путь использует природа. Послойное обучение Q-арных искусственных нейронов уже является технической реальностью, получившей сегодня маркетинговое название «нейроморфные архитектуры» [9]. В рамках таких представлений каждый слой Q-арных искусственных нейронов должен снижать энтропию данных образа «Свой» и повышать энтропию образов «Все Чужие». Создавать автоматы послойного энтропийного обучения ранее было затруднительно. Классическую энтропию Шеннона нельзя было оценить на малых выборках, а энтропия Хэмминга (оцениваемая по ГОСТ Р 52633.3) непопулярна (редко применима, так как к ней нет достаточного доверия).

Целью данной работы было показать, что оценка энтропии Шеннона вполне применима к обучению нейронных сетей на малых выборках. Для этого достаточно перейти к вычислению коэффициентов корреляции бинарных или Q-арных кодов между слоями нейроморфной структуры. Тогда энтропия Шеннона – Пирсона имеет квадратичную вычислительную сложность и становится пригодной для использования при послойном автоматическом обучении нейросетей.

СПИСОК ЛИТЕРАТУРЫ

1. McCulloch, Warren S., Walter P. A logical calculus of the ideas immanent in nervous activity // Bulletin of Mathematical Biophysics. 1943. 5 (4). P. 115–133. doi: 10.1007/bf02478259

2. Hebb D. O. The Organization of Behavior: A Neuropsychological Theory. Wiley, 1949.

3. Николлс Дж., Мартин Р., Валлас Б., Фукс П. От нейрона к мозгу / пер. с англ. П. М. Балабана, А. В. Галкина, Р. А. Гиниатуллина [и др.]. М. : Едиториал УРСС, 2003. 672 с.

4. Волчихин В. И., Иванов А. И., Фунтиков В. А., Малыгина Е. А. Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометрико-нейросетевой аутентификации // Известия высших учебных заведений. Поволжский регион. Технические науки. 2013. № 4 (28). С. 88–99.

5. Малыгина Е. А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с многоуровневым квантованием биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 114 с.

6. Иванов А. И. Искусственные математические молекулы: повышение точности статистических оценок на малых выборках (программы на языке MathCAD) : препринт. Пенза : Изд-во ПГУ, 2020. 36 с.

7. Нильсон М., Чанг И. Квантовые вычисления и квантовая информация. М. : Мир, 2006. 821 с.

8. Душкин Р. В. Квантовые вычисления и функциональное программирование. М : ДМК Пресс, 2015. 234 с.

9. Сандомирская Ю. Искусственный интеллект и нейроморфные вычисления: второе дыхание // Коммерсантъ Наука. 2021. № 47. С. 26–29.

10. Иванов А. И. Искусственный интеллект высокого доверия: ускорение вычислений и экономия памяти при тестировании больших сетей искусственных нейронов на малых выборках // Системы безопасности. 2020. № 5. С. 60–62.

11. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. М., 2011.

12. ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. М., 2010.

13. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» : программный продукт / создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip.

14. Иванов А. И., Иванов А. П., Ратников К. А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров

кроссверток и автосверток Хэмминга : препринт. Пенза : Изд-во ПГУ, 2021. 56 с. doi: 10.13140/RG.2.2.16514.35524

15. Горбунов К. А., Никитин В. В. Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний Хэмминга при их применении к ключам-откликам на примеры одного образа «Чужой» // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 83–85.

16. Иванов А. И., Иванов А. П., Горбунов К. А. Нейросетевое преобразование биометрии в код аутентификации: дополнение энтропии Хэмминга энтропией корреляционных связей между разрядами // Надежность и качество сложных систем. 2023. № 1. С. 91–98. doi: 10.21685/2307-4205-2023-1-11

17. Иванов А. И. Нейросетевой многокритериальный статистический анализ малых выборок : справочник. Пенза : Изд-во ПГУ, 2022. 160 с.

18. Иванов А. И. Искусственный интеллект высокого доверия. Ускорение вычислений и экономия памяти при тестировании больших сетей искусственных нейронов на малых выборках // Системы Безопасности. 2020. № 5. С. 60–62.

19. Иванов А. И. НейроДинамика: гиперускорение направленных переборов или повышение достоверности статистических оценок на малых выборках : препринт. Пенза : Изд-во ПГУ, 2021. 106 с.

Справочное издание

Иванов Александр Иванович

Малые выборки, нейроморфные вычисления:
быстрые алгоритмы оценки энтропии
Шеннона – Пирсона квадратичной сложности

Редактор *Л. Ю. Зимина*
Технический редактор *Н. В. Иванова*
Компьютерная верстка *Н. В. Ивановой*
Дизайн обложки *И. В. Шваревой*

Подписано в печать 27.11.2023.
Формат 70×100 $^{1}/_{16}$. Усл. печ. л. 2,60.
Тираж 218. Заказ № 668.

Издательство ПГУ.
440026, г. Пенза, ул. Красная, 40.
Тел.: (8412) 66-60-49, 66-67-77; e-mail: iic@pnzgu.ru