7. Патент на корисну модель № 97162 МПК G06F 7/00. Опублікований 10.03.2015 Бюл. № 5. Николайчук Я.М, Кімак В.Л., Круліковський Б.Б. / Пристрій додавання багаторозрядних двійкових чисел.

Кимак В.Л. **Архитектура спецпроцессора шифрования данных в теоретико-числовом базисе Радемахера-Крестенсона**

Результаты анализа состояния защиты информационных потоков (ИП) в компьютеризированных системах свидетельствует, что в целом состояние решения этой задачи далеко от совершенства. Тем более, что возникает потребность в построении устойчивых и продуктивных методов и алгоритмов шифрования ИП в компьютерных сетях с учетом тенденций роста требований к необходимому уровню защиты различных типов ИП. Поэтому разработка подходов, методов, алгоритмов, криптографических компьютерных средств защиты информации с использованием сетевых технологий и высокопроизводительных спецпроцессоров, особенно для проблемно-ориентированных (ПОКС) и специализированных компьютерных систем (СКС) на основе различных теоретико-числовых базисов (ТЧБ) является актуальной научной задачей. На основе алгоритмов и схемотехнических решений аппаратных компонентов процессоров шифрования данных в теоретико-числовом базисе Радемахера-Крестенсона разработана архитектура многоразрядного спецпроцессора шифрования данных, а также рассчитаны системы взаимнопростых модулей для этих процессоров.

Ключевые слова: алгоритм, спецпроцессор, шифрование данных, модульное экспоненцианирование, теоретико-числовой базис Радемахера-Крестенсона.

Kimak V.L. **The Architecture of Special Processor for Data Encryption in Rademacher-Krestenson's Theoretical-Numerical Basis**

The analysis of information flow protection (IF) in the computer systems indicates that the overall condition of solving this problem is far from perfect. Moreover, there is a need to build stable and productive methods of IF encryption algorithms in computer networks with taking into account bigger requirements for data protection of various IF types. Therefore, the development of approaches, methods, algorithms, cryptographic computer information security using networking and high-performance special processors, especially for problem-oriented (POCS) and specialized computer systems (SCS) based on various theoretical and numerical bases (TNB) is an actual scientific task. Based on algorithms and schemes and technical solutions of processor's hardware components for data encryption in Rademacher-Krestenson's theoretical-numerical basis is developed special multibit processor architecture for data encryption and is calculated system of coprime modules designed for these processors.

Keywords: algorithm, special processors, data encryption, modular exponentiation, Rademacher-Krestenson's theoretical-numerical basis.

УДК 681.5:519.7

Доц. В.М. Коцовський, канд. техн. наук – Ужгородський НУ

КІЛЬКІСНІ ОЦІНКИ РОЗПІЗНАВАЛЬНОЇ ЗДАТНОСТІ ДВОПОРОГОВИХ НЕЙРОННИХ ЕЛЕМЕНТІВ

Досліджено властивості двопорогових нейронних елементів, які є одним з найпростіших узагальнень класичних нейроелементів МакКаллока-Піттса. Використання двопорогових нейронів дає змогу подолати деякі обмеження, притаманні звичайним пороговим елементам, зокрема знайти розв'язок відомої XOR-проблеми. Вивчено питання, які стосуються оцінки кількості дихотомій скінченної множини у n-вимірному просторі, які можна отримати за допомогою двопорогових нейронів. Також досліджено асимптотичну поведінку кількості дихотомій та розглянуто питання знаходження розмірності Вапніка-Червоненкіса двопорогових нейроелементів.

Ключові слова: нейронний елемент, двопороговий нейрон, штучна нейромережа, розпізнавання.

Вступ. Конекціоністський підхід ґрунтується на використанні нейромереж до моделювання складних об'єктів та явищ. Кілька останніх десятиріч штучні нейромережі та інші нейроподібні структури широко використовують для розв'язування широкого кола актуальних господарських задач **[**1**]**. Однією з ключових проблем, які постають у практичному застосуванні штучних нейронних мереж, є проблема вибору моделі нейронів, які утворюють нейромережу. Традиційними вважають підходи з використання нейронів з лінійним вхідним оператором та функцію активації порогового типу (пороговий елемент) або сигмоїдального типу (неперервний нейрон). Кожний з цих підходів має свої переваги і недоліки **[**2**]**.

Уведення до розгляду двопорогових нейронних елементів (ДНЕ) та їх дослідження мотивується у літературі більш потужними можливостями цих елементів порівняно із звичайними пороговими елементами з розпізнавання належності точок у R^n до одного з двох заданих класів. Це саме твердження стосується і нейронів із неперервними функціями активації двопорогового типу, до яких належить широкий клас "дзвіноподібних" функцій.

У роботах **[**3, 4**]** зроблено спробу кількісно оцінити переваги використання двопорогових нейроелементів. Зокрема, встановлено оцінки кількості класифікацій точок скінченної множини у дійсному векторному просторі, які можна отримати за допомогою ДНЕ. Варто зауважити, що в асимптотичному сенсі встановлені оцінки мають різний порядок росту. У пропонованій роботі з використанням прийомів теорії лінійних нерівностей вдалося отримати та обґрунтувати уточнені оцінки кількості різних двопорогових класифікацій.

Модель двопорогового нейрона. Нехай R^n – n-вимірний дійсний евклідів простір. Якщо $\mathbf{w}=(w_1,w_2,\ldots,w_n)\in \mathrm{R}^n$, $\mathbf{x}\in(x_1,x_2,\ldots,x_n)\in \mathrm{R}^n$, то величину скалярного добутку

$$(\mathbf{w},\mathbf{x})=\sum_{i=1}^{n} w_i x_i$$

будемо називати зваженою сумою, що відповідає вектору **x**.

Штучним двопороговим дійсним нейронним елементом з ваговим вектором $\mathbf{w}\in \mathrm{R}^n$, порогами $t_1,t_2\in \mathrm{R}$ $(t_1<t_2)$ будемо називати функціональний елемент з n дійсними входами $x_1,x_2,\ldots,x_n$ та одним виходом $y\in\{-1,1\}$, поведінка якого описується співвідношеннями:

$$y=\begin{cases}-1, & t_1<(\mathbf{w},\mathbf{x})<t_2,\\ 1, & (\mathbf{w},\mathbf{x})\le t_1\vee(\mathbf{w},\mathbf{x})\ge t_2.\end{cases}$$

У термінах **[**2**]** зважена сума є вхідним оператором ДНЕ із функцією активації вигляду

$$f_{t_1,t_2}(x)=\begin{cases}-1, & t_1<x<t_2,\\ 1, & x<t_1\vee x>t_2.\end{cases}$$

ДНЕ повністю визначається впорядкованою трійкою $(\mathbf{w},t_1,t_2)$, яку будемо надалі називати вектором структури або просто структурою ДНЕ.

ДНЕ із структурою $(\mathbf{w},t_1,t_2)$ здійснює розбиття простору R^n на дві підмножини таким чином:

$$\mathrm{R}^{n+}=\{\mathbf{x}\in\mathrm{R}^n\,|\,(\mathbf{w},\mathbf{x})\le t_1\}\cup\{\mathbf{x}\in\mathrm{R}^n\,|\,(\mathbf{w},\mathbf{x})\ge t_2\},\quad \mathrm{R}^{n-}=\{\mathbf{x}\in\mathrm{R}^n\,|\,t_1<(\mathbf{w},\mathbf{x})<t_2\}.$$

Дві множини $A^+\subset\mathrm{R}^n$ і $A^-\subset\mathrm{R}^n$ назвемо двопорогово-сепарабельними (д-сепарабельними), якщо знайдеться такий ДНЕ із вектором структури $(\mathbf{w},t_1,t_2)$, що $A^+\subset\mathrm{R}^{n+}$ і $A^-\subset\mathrm{R}^{n-}$. У цьому випадку будемо казати, що ДНЕ із структурою $(\mathbf{w},t_1,t_2)$ здійснює д-розбиття (A^+,A^-) множини $A=A^+\cup A^-$ на дві множини A^+ і A^-, що не перетинаються. Якщо ДНЕ має структуру $(\mathbf{w},t_1,t_2)$, то для довільної множини $A\subset\mathrm{R}^n$ її підмножини $A^+=A\cap\mathrm{R}^{n+}$, $A^-=A\cap\mathrm{R}^{n-}$ є д-сепарабельними. Легко бачити, що д-сепарабельність множин є узагальненням лінійної сепарабельності. Вже в одновимірному просторі можна навести приклад д-сепарабельних множин, які не є лінійно сепарабельними (наприклад, $A^-=\{0\}$ $A^+=\{-1,1\}$).

Розпізнавальна здатність ДНЕ. Нехай $D_1(A)$ – кількість способів розбиття точок скінченної множини A на два класи за допомогою звичайного одношарового перцептрона (порогового елемента). Надалі будемо вважати, що $A\subset\mathrm{R}^n$ і $\mathrm{Card}\,A=m$. Нехай $D_1(m,n)=\max\{D_1(A)\,|\,A\subset\mathrm{R}^n,\mathrm{Card}\,A=m\}$. Добре відомо **[**1, 3**]**, що

$$D_1(m,n)=\begin{cases}2\sum\limits_{i=0}^{n}C_{m-1}^i, & m>n+1,\\ 2^m, & m\le n+1,\end{cases}\qquad(1)$$

де C_{m-1}^i – біномні коефіцієнти, причому $D_1(A)=D_1(m,n)$ тоді і тільки тоді, коли усі точки множини A знаходяться у *загальному положенні* (через жодні $n+1$ точки множини A не можна провести гіперплощину).

Нехай $D_2(A)$ – кількість різних д-розбиттів (A^+,A^-) скінченної m-елементної множини $A\subset\mathrm{R}^n$, $D_2(m,n)=\max\{D_2(A)\,|\,A\subset\mathrm{R}^n,\mathrm{Card}\,A=m\}$. Покажемо, що (1) можна використати для того, щоб отримати оцінки для $D_2(m,n)$, причому верхня оцінка значно покращує оцінку, отриману у роботах **[**3, 4**]**. Надалі без додаткових застережень будемо вважати, що $A\subset\mathrm{R}^n$ і $\mathrm{Card}\,A=m$.

Твердження 1. *При $m>n$ має місце нерівність*

$$D_2(m,n)<2\sum_{i=0}^{n+1}C_{2m-1}^i.\qquad(2)$$

Якщо елементи множини A знаходяться у загальному положенні і $m>n+1$, то

$$D_2(A)\ge 2\sum_{i=0}^{n+1}C_{m-1}^i-1.\qquad(3)$$

Доведення. Для кожного вектора $\mathbf{x}=(x_1,\dots,x_n)\in A$ побудуємо два $n+2$-вимірні вектори $\mathbf{x}'=(-x_1,\dots,-x_n,1,0)$ і $\mathbf{x}''=(x_1,\dots,x_n,0,-1)$. Якщо ДНЕ із структурою $(\mathbf{w},t_1,t_2)$ здійснює д-розбиття множини A, то гіперплощина $w_1x_1+\dots+w_nx_n+t_1x_{n+1}+t_2x_{n+2}=0$ здійснює лінійне розбиття (B^+,B^-) множини $B=\{\mathbf{x}'|\mathbf{x}\in A\}\cup\{\mathbf{x}''|\mathbf{x}\in A\}$ і $B_1^-=\{\mathbf{x}'|\,\varphi_{\mathbf{w},t_1,t_2}(\mathbf{x})<0\}\cup\{\mathbf{x}''|\,\varphi_{\mathbf{w},t_1,t_2}(\mathbf{x})<0\}\subset B^-$, $B_1^+=\{\mathbf{x}'|\mathbf{x}\in A,(\mathbf{w},\mathbf{x})\le t_1\}\cup\{\mathbf{x}''|\mathbf{x}\in A,(\mathbf{w},\mathbf{x})\ge t_2\}\subset B^+$. Тому кількість різних д-розбиттів множини A не перевищує кількість лінійних однорідних розбиттів множини B (насправді наявна строга нерівність, бо B_1^+ – власна підмножина множини B^+). Відомо **[1]**, що кількість лінійних однорідних розбиттів множини можна обчислити за формулою (1), зменшивши на 1 кількість доданків. Звідси випливає справедливість нерівності (2).

Оцінимо порядок росту правої частини у (2). Відомо **[**5**]**, що при $l>n+1$

$$\sum_{i=0}^{n}C_{l-1}^i\le 1{,}5\,\frac{l^n}{n!}.$$

З урахуванням останньої нерівності маємо, що

$$D_2(m,n)<3\cdot\frac{(2m)^{n+1}}{(n+1)!}=O\left(m^{n+1}\right).\qquad(4)$$

Для порівняння можна нагадати, що $D_1(m,n)=O(m^n)$ **[**1, 5**]**. Оцінка (4) є значно кращою, ніж верхня оцінка, наведена у роботі **[**3**]**, де фактично показано, що $D_2(m,n)<O\left(m^{2n+1}\right)$.

Перейдемо до встановлення нижньої оцінки. Якщо при встановленні верхньої оцінки фактично було здійснено перехід від простору R^n до простору R^{n+2}, то для з'ясування нижньої оцінки перейдемо від $\mathbf{x}=\ =(x_1,\dots,x_n)\in\mathrm{R}^n$ до $\tilde{\mathbf{x}}=(x_1,\dots,x_n,-1)\in\mathrm{R}^{n+1}$. Нехай $\tilde{\mathbf{w}}=(w_1,\dots,w_n,t_1)$. Тоді

$$\forall\mathbf{x}\in A\ \ \mathbf{x}\in A^-\Leftrightarrow 0<(\tilde{\mathbf{w}},\tilde{\mathbf{x}})<t_2-t_1.$$

Очевидно, що якщо ДНЕ із структурою $(\mathbf{w},t_1,t_2)$ здійснює д-розбиття множини A, то гіперплощина $w_1x_1+\dots+w_nx_n+t_1x_{n+1}=t_2-t_1$ розбиває множину $C=\{\tilde{\mathbf{x}}|\mathbf{x}\in A\}$ на дві множини $C^+=\{\tilde{\mathbf{x}}|(\tilde{\mathbf{w}},\tilde{\mathbf{x}})\ge t_2-t_1\}$ і $C^-=C\setminus C^+$. Тоді з урахуванням (1) отримуємо (3). Твердження доведене.

Розглянемо останній доданок у (3). Легко бачити, що при фіксованому n він є величиною порядку $\theta\left(m^{n+1}\right)$. Тому нижня оцінка має той самий асимптотичний порядок росту, що й верхня оцінка (4).

Зауваження. Нижню оцінку (3) за допомогою інших методів встановлено у роботах **[**3, 4**]** для двопорогових елементів більш загального вигляду.

Покажемо, що верхня оцінка (2) для $D_2(m,n)$ може бути використана для доведення наступного факту.

Твердження 2. *При $n>10$ для довільної множини $A\subset\mathrm{R}^n$, такої, що $\mathrm{Card}\,A\ge 5n$ знайдеться розбиття множини A, яке не є д-розбиттям.*

Для доведення використаємо (4) та формулу Стірлінга. Отримаємо

$$D_2(5n,n) < 3\cdot\frac{(10n)^{n+1}}{(n+1)!} = \frac{30\cdot 10^n n^{n+1}}{(n+1)!} = \frac{30\cdot 10^n n^{n+1} e^{n+1}}{\sqrt{2\pi(n+1)}\,(n+1)^{n+1}e^{\theta(n+1)}} < 6\cdot(10e)^n,$$

де $|\theta(n)| < (12n)^{-1}$. Якщо $n > \dfrac{\ln 6}{4\ln 2 - \ln 5e} \approx 10{,}9822$, то $D(5n,n) < 2^{5n}$. Отримали, що кількість д-розбиттів множини A менша за кількість усіх її підмножин. Звідси випливає існування розбиттів множини A, які не є д-розбиттями.

Встановимо тепер обмеження на потужність множини A, яке б забезпечувало д-сепарабельність довільного розбиття множини A, тобто виконання умови $D_2(m,n) = 2^m$.

Твердження 3. *Для всіх* $n \in \mathrm{N}$ *можна вказати таку множину* $A_n \subset \mathrm{R}^n$, *що* $\mathrm{Card}\, A_n = 2n$ *і* $D_2(A_n) = 2^{2n}$.

Для доведення використаємо індукцію з розмірності векторного простору, причому будемо доводити, що усі розбиття множин $n \in \mathrm{N}$ можна здійснити на ДНЕ, пороги яких задовольняють умову

$$t_1 = -1, \quad t_2 = 2. \tag{5}$$

Справедливість твердження при $n = 1$ для довільної множини, яка містить дві точки дійсної прямої легко отримати безпосередньою перевіркою (усі розбиття двохелементної множини є лінійно сепарабельними). Окрім того, легко переконатися, що усі д-розбиття при $n = 1$ можна отримати за допомогою з порогами, які задовольняють умову (5). Для визначеності покладемо $A_1 = \{-1, 1\}$. Нехай для всіх $r < n$ твердження вже доведене. Доведемо його при $r = n$. Задамо множину $A_n \subset \mathrm{R}^n$ таким чином:

$$A^n = \{(x_1,\ldots,x_{n-1},0) \mid (x_1,\ldots,x_{n-1}) \in A^{n-1}\} \cup \{(0,\ldots,0,-1),(0,\ldots,0,1)\}.$$

Покажемо, що усі розбиття множини A_n є д-розбиттями. Нехай (A_n^+, A_n^-) – довільне розбиття множини A_n і нехай (A_{n-1}^+, A_{n-1}^-) – відповідне розбиття множини A_{n-1} $\left(A_{n-1}^+ = \{(x_1,\ldots,x_{n-1}) \mid (x_1,\ldots,x_{n-1},0) \in A_n^+\},\ A_{n-1}^- = A_{n-1} \setminus A_{n-1}^+\right)$. За припущенням індукції його можна здійснити за допомогою ДНЕ із структурою $((w_1,\ldots,w_{n-1}),-1,2)$. Можливими є 4 випадки:

1. $\{(0,\ldots,0,-1),(0,\ldots,0,1)\} \subset A_n^+$. У цьому випадку покладемо $w_n = 3$;
2. $(0,\ldots,0,-1) \in A_n^+$, $(0,\ldots,0,1) \in A_n^-$. У цьому випадку покладемо $w_n = 1{,}5$;
3. $(0,\ldots,0,-1) \in A_n^-$, $(0,\ldots,0,1) \in A_n^+$. У цьому випадку покладемо $w_n = -1{,}5$;
4. $\{(0,\ldots,0,-1),(0,\ldots,0,1)\} \subset A_n^-$. У цьому випадку покладемо $w_n = 0$.

Легко переконатися в тому, що у кожного з чотирьох випадків ДНЕ із структурою $((w_1,\ldots,w_{n-1},w_n),-1,2)$ здійснює д-розбиття множини A_n, причому пороги t_1, t_2 задовольняють (5). Твердження доведене.

Наслідок. *Якщо* LBT_n *– множина усіх n-місних ДНЕ, то при* $n > 10$

$$2n \le \mathrm{VCDim}\left(LBT_n, \mathrm{R}^n\right) < 5n,$$

де $\mathrm{VCDim}\left(LBT_n, \mathrm{R}^n\right)$ – розмірність Вапніка-Червоненкіса.

Висновки. У роботі розглянуто питання оцінки потенційної спроможності двопорогових нейронних елементів вирішувати задачі розпізнавання підмножин n-вимірного евклідового простору. Встановлено, що за допомогою ДНЕ можна правильно розпізнати $\theta(m^{n+1})$ різних дихотомій, де m – потужність множини, елементи якої знаходяться у загальному положенні. Отриманий результат є покращенням оцінок, наведених у [3, 4], і дає змогу кількісно оцінити потенційні переваги від застосування у розпізнавальних пристроях ДНЕ замість класичних порогових елементів, для яких кількість відповідних дихотомій є величиною, порядок росту якої не перевищує $O(m^n)$.

Також знайдено оцінки розмірності Вапніка-Червоненкіса для класу ДНЕ із n входами – ключового параметра теорії навчання.

Література

1. Хайкин, С. Нейронные сети: полный курс / С. Хайкин. – Изд. 2-ое, [перераб. и доп.]. – М. : Изд-во "Вильямс-Телеком", 2006. – 1104 с.
2. Руденко, О.Г. Штучні нейронні мережі / О.Г. Руденко, Є.В. Бодянський. – Харків : Вид-во ТОВ "Компанія СМІТ", 2006. – 404 с.
3. Olafsson, S. The capacity of multilevel threshold function / S. Olafsson and Y.S. Abu-Mostafa // IEEE Trans. Pattern Anal. Machine Intell. – 1988. – Vol. 10, No. 2. – Pp. 277-281.
4. Takiyama, R. Multiple threshold perceptron / R. Takiyama // Pattern recognition. – 1978. – Vol. 10. – Pp. 27-30.
5. Вапник, В.Н. Теория распознавания образов. Статистические проблемы обучения / В.Н. Вапник, А.Я. Червоненкис. – М. : Изд-во "Наука", 1974. – 416 с.

Коцовский В.М. **Количественные оценки распознавательной мощности двупороговых нейронных элементов**

Исследованы свойства двупороговых нейронных элементов, которые являются одним из самых простых обобщений классических нейроэлементов МакКаллока-Питтса. Использование двупороговых нейронов дает возможность решить известную XOR-проблему. Изучены вопросы, касающиеся оценки числа дихотомий конечного множества в n-мерном пространстве, которые можно получить с помощью двупороговых нейронов. Исследовано асимптотическое поведение этого числа и рассмотрен связанный с этим вопрос оценки размерности Вапника-Червоненкиса двупороговых нейронов.

Ключевые слова: нейронный элемент, двупороговый нейрон, искусственная нейросеть, распознавание.

Kotsovsky V.M. **Quantitative Estimation of the Capability of Bithreshold Neural Units**

The given paper is devoted to the study of the properties of the simplest multithreshold generalization of McCulloch-Pitts neurons, namely bithreshold neurons with linear input operator. Usage of neuron supplied with two thresholds provides the possibility to find out the solution of the famous XOR-problem. The most frequent quantitative characteristic of representative power of neuron-like units with discrete activation function is the number of all possible dichotomies of the finite subset of n-dimensional space achieved by using such devices. The asymptotic behaviour of this number is given. The related question of Vapnik-Chervonenkis dimension of bithreshold neuron is also studied.

Keywords: neural unit, bithreshold neuron, artificial neural network, recognition.