В ходе работы была исследована проблема надежного хранения паролей от веб-ресурсов. Запомнить все пароли невозможно, а использовать одинаковые небезопасно, наилучшее решение этой проблемы – использование менеджеров паролей. Были проанализированы существующие менеджеры паролей, среди которых выявлены недостатки, например, хранение пользовательских данных на серверах компаний. Разработанный менеджер паролей хранит данные на устройстве пользователя, которое поддерживает технологию NFC, а по запросу, предоставляет эти данные. Аналогов среди менеджеров паролей, использующих данный принцип работы, не существует.

В ходе выполнения работы было проделано следующее:

– исследованы проблемы хранения паролей.

– ознакомление с разработкой для операционной системы Android.

– разработан менеджер паролей на базе операционной системы Android.

– разработан протокол обмена учетными данными между менеджером паролей и другими устройствами.

– разработано программное обеспечение для ПК, поддерживающее протокол обмена данных.

– ознакомление с разработкой расширений для браузера Google Chrome и разработаны расширения, для взаимодействия с приложением на базе ОС Android.

– разработано расширение для браузера Google Chrome, с поддержкой автоматического заполнения веб-форм, а также автоматического извлечения из них учетных данных для последующей передачи их в менеджер паролей.

Таким образом, разработанное ПО можно расширять для использования в других расширениях, а также в других приложениях для ПК. Также менеджер паролей можно использовать с другими устройствами, поддерживающие технологию NFC и протокол обмена данных менеджера паролей. Главным недостатком разработанных приложений является обязательная поддержка на мобильном устройстве и ПК технологии NFC.

ЛИТЕРАТУРА

1. Near Field Communication [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Near_field_communication. – Дата доступа: 30.03.2015.
2. Password manager [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Password_manager. – Дата доступа: 28.03.2015.
3. Should You Use a Password Manager? [Электронный ресурс]. – Режим доступа: http://www.tomsguide.com/us/password-manager-pros-cons,news-19018.html. – Дата доступа: 28.03.2015.
4. Three quarters of Britons risking online safety [Электронный ресурс]. – Режим доступа: https://www.cyberstreetwise.com/blog/three-quarters-britons-risking-online-safety
5. Фишинг [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/фишинг. – Дата доступа: 03.04.2015.

УДК 512.643

О ПРЕДСТАВЛЕНИИ (2 × 2)-МАТРИЦЫ С ПОЛОЖИТЕЛЬНЫМ ОПРЕДЕЛИТЕЛЕМ В ВИДЕ ПРОИЗВЕДЕНИЯ ТРЕУГОЛЬНЫХ МАТРИЦ С ПОЛОЖИТЕЛЬНЫМИ ДИАГОНАЛЬНЫМИ ЭЛЕМЕНТАМИ

В.А. ЗАЙЦЕВ, Д.А. ГОЛУБЕВ
(Представлено: канд. физ.-мат. наук, доц. А.А. КОЗЛОВ)

Одним из основных вопросов теории матриц является задача о факторизации матриц, т.е. о разложении матрицы из некоторого класса матриц в произведение матриц, принадлежащих некоторым (возможно, иным) подмножествам матриц. Рассматривается задача представления квадратной (2 × 2)-матрицы с положительным определителем в виде произведения семи треугольных матриц. Отличительной особенностью найденного разложения от иных и, прежде всего, от LU –разложения, является то, что все матрицы-сомножители в нем имеют положительную диагональ.

Имеет место
Лемма *Для матриц*

$$\alpha := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \beta := \alpha^{\mathrm{T}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma := \alpha^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \tag{1}$$

выполняются равенства

$$\alpha^{-1}=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix},\quad \beta^{-1}=\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix},$$

$$\alpha^{-1}\cdot\beta\cdot\alpha^{-1}=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}:-\mathrm{J},\quad \alpha^{-1}\cdot\beta\cdot\alpha^{-1}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}=\mathrm{J}^{-1}. \qquad (2)$$

$$\alpha\cdot\beta^{-1}\cdot\gamma\cdot\beta^{-1}\cdot\alpha=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=-\mathrm{E}.$$

Доказательство леммы приводится непосредственным перемножением матриц из (1) и обратных к матрицам α и β, которые существуют, ввиду очевидной невырожденности α и β:

$$\alpha^{-1}\cdot\beta\cdot\alpha^{-1}=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}:=\mathrm{J}$$

$$\alpha\cdot\beta^{-1}\cdot\alpha=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}=\mathrm{J}^{-1}$$

$$\alpha\cdot\beta^{-1}\cdot\gamma\cdot\beta^{-1}\cdot\alpha=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\cdot\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=$$

$$=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=-\mathrm{E}$$

Лемма доказана.

На основании этой леммы удалось получить следующую теорему:

Теорема Любую вещественную (2 × 2)-матрицу с положительным определителем можно представить в виде произведения семи вещественных треугольных (2 × 2)-матриц с положительными диагональными элементами.

Доказательство. Возьмем произвольную матрицу $H=\left\{h_{ij}\right\}_{ij}^{2}\in \mathrm{M}_2$ с положительным определителем. Тогда возможны два случая: $h_{11}\neq 0$ и $h_{11}=0$.

Пусть $h_{11}\neq 0$. Поскольку $\det H>0$, то главные угловые миноры [1, с. 30] матрицы H ненулевые, и, следовательно, для этой матрицы можно применить теоремы о LU –разложении [1, с. 194]. Тогда $H=L\cdot U$, где $L=\left\{l_{ij}\right\}_{ij=1}^{2}$ $U=\left\{U_{ij}\right\}_{ij=1}^{2}\in M_2$ – соответственно нижне- и верхнетреугольная матрицы, причем на диагонали матрицы U стоят единицы, т.е. $U_{ij=1}$, $i=1,2$. Так как $0<\det H=\det(L\cdot U)=\det L\cdot\det U=i_{11}\cdot l_{22}\cdot u_{11}\cdot u_{22}$, то диагональные элементы матрицы L одного знака. Пусть $l_{ij>0}$, $i=1,2$, тогда L – нижнетреугольная матрица с положительными диагональными элементами. Отсюда, ввиду, что единичная матрица имеет положительную диагональ и является треугольной, имеем искомое представление

$$H=\underbrace{E\cdot\ldots\cdot E}_{5\text{ сомножителей}}\cdot L\cdot U, \qquad (4)$$

Пусть теперь $l_{ii<0}$, $i=1,2$, т.е. на диагонали матрицы L стоят только отрицательные числа, тогда диагональные элементы матрицы $-L$ – положительны. Используя формулу (3) леммы, получим равенства

$$H=L\cdot U=-E\cdot(-L)\cdot U=\alpha\cdot\beta^{-1}\cdot\gamma\cdot\beta^{-1}\cdot\alpha\cdot(-L)\cdot U, \qquad (5)$$

которые, с учетом того, что матрицы $\alpha^{\pm 1}$, $\beta^{\pm 1}$, γ имеют положительные диагональные элементы и являются треугольными, дают требуемое в теореме представление.

Прежде, чем перейти ко второму случаю, введем в рассмотрение матрицу

$$J:\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

Очевидно, что эта матрица обратима, причем выполняется легко проверяемое соотношение

$$J^{-1}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

Рассмотрим теперь случай $h_{11} = 0$, т.е. когда матрица H имеет вид

$$\mathrm{H}=\begin{pmatrix}0 & h_{12}\\ h_{21} & h_{22}\end{pmatrix},$$

и, поскольку среди главных угловых миноров матрицы H есть нулевые ($h_{11} = 0$), когда для этой матрицы нельзя применить теорему о LU–разложении [1, с. 194]. Так как по условию $\det \mathrm{H} > 0$, то для рассматриваемого случая выполняется неравенство $h_{12}h_{22} < 0$, т.е. элементы побочной диагонали матрицы H имеют разные знаки.
Пусть $h_{12} < 0$, тогда у верхнетреугольной матрицы

$$G_1 \coloneqq \begin{pmatrix}h_{21} & h_{22}\\ 0 & -h_{12}\end{pmatrix}$$

на диагонали стоят положительные элементы. Так как выполняются равенства

$$J\cdot G_1=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}h_{21} & h_{22}\\ 0 & -h_{12}\end{pmatrix}=\begin{pmatrix}0 & h_{12}\\ h_{21} & h_{22}\end{pmatrix}=H,$$

то, отсюда, ввиду второй формулы из (2) и определения J, вытекает представление

$$H=\alpha^{-1}\cdot\beta\cdot\alpha^{-1}\cdot\underbrace{E\cdot\ldots\cdot E}_{\text{3 сомножителя}}\cdot G_1. \qquad (6)$$

Если же выполняется неравенство $h_{21} < 0$, тогда матрица

$$G_2 \coloneqq \begin{pmatrix}-h_{21} & -h_{22}\\ 0 & h_{12}\end{pmatrix}$$

имеет только положительные диагональные элементы. Поскольку справедливы равенства

$$J^{-1}\cdot G_2=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}-h_{21} & -h_{22}\\ 0 & h_{12}\end{pmatrix}=\begin{pmatrix}0 & h_{12}\\ h_{21} & a_{22}\end{pmatrix}=H,$$

то, отсюда, ввиду второй формулы из (2) и определения J^{1}, вытекает представление

$$H=\alpha^{-1}\cdot\beta\cdot\alpha^{-1}\cdot\underbrace{E\cdot\ldots\cdot E}_{\text{3 сомножителя}}\cdot G_2. \qquad (7)$$

В каждом из найденных представлений (4)-(7) матрицы H матрицы-сомножители, стоящие в правой части, суть треугольные и имеют положительные диагональные элементы.
Теорема доказана.

ЛИТЕРАТУРА

1. Хорн, Р. Матричный анализ / Р. Хорн, Ч. Джонсон. – М. : Мир. – 1989. – 655 с.

УДК 681.3.06

ИСПОЛЬЗОВАНИЕ ПЛИС С АРХИТЕКТУРОЙ FPGA ДЛЯ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

А.В. АНДРОЩУК
(Представлено: В.М. ЧЕРТКОВ)

Рассмотрена возможность повышения производительности цифровой обработки сигналов (ЦОС) при помощи методов параллельных вычислений. Представлены особенности использования ПЛИС. Определены преимущества использования ПЛИС с архитектурой FPGA по сравнению с DSP процессорами.