R.-A. Ivantsiv, Yu. Khanas
Department of Computer Aided Design Systems

DEVELOPMENT OF ALGORITHM TRANSFORMATION MATRICES BY THEIR REDUCTION

Описано суть розробленого алгоритму, котрий полягає в перетворенні матричних масивів через зміну їх розмірності за допомогою поглинання другого роду. Під час роботи алгоритму початкова матриця буде змінена так – зміниться розмір матриці та її вміст. Алгоритм оснований на порівняно простих математичних діях, що, своєю чергою, залежать від виконання низки правил та зауважень, наявність, манера застосування та послідовність котрих не завжди збігається із загально прийнятими нормами математики чи арифметики. Також тут наведено своєрідну класифікацію матриць, кожна з котрих відповідає певному правилу чи теоремі.

Ключові слова: поглинання другого роду, вхідна (початкова) матриця, ітерація скорочення матриці, ітерація зміщення матриці, ітерація доповнення матриці.

The essence of the algorithm is to convert the matrix arrays through changing their dimensions by means of absorption of the second kind. During the initial matrix of the algorithm be changed as follows – change the size of the matrix and its contents. The algorithm is based on a relatively simple mathematical operations, which in turn depend on the performance of a number of rules and observations, availability, and manner of use of the sequence which do not always coincide with the generally accepted rules of mathematics or arithmetic. It also awarded the original classification matrix, both of which fall under any rule or theorem.

Key words: absorption of the second type, the input (primary) matrix, reducing iteration matrix iteration shift matrix, matrix iteration completion.

Introduction

Algorithms, where there is a transformation matrix algebra arrays has a very wide range of applications, such as analytical geometry, graph theory, encoding and converting digital signals ...

The development of new algorithms based on the transformation matrix arrays is an urgent task, as they can provide an opportunity to develop new systems of compression or encryption.

1. Description of basic operations of the algorithm.

To get started, we need a matrix of any dimension. For example, we can take a 4x4 matrix of dimension and its content will be chaotic set of numbers (see. Fig. 1). Accordingly cited this matrix input (or start).

$$\begin{pmatrix} 2 & 6 & 0 & 9 \\ 1 & 4 & 3 & 3 \\ 2 & 4 & 9 & 5 \\ 1 & 4 & 8 & 7 \end{pmatrix}$$

Fig. 1. Example input (starting) matrix

To get started, we need an algorithm to compare the equality of all figures matrix under the same numbers that are in the same vector subjected to absorption of the second kind, that is two identical numbers are declining.

48

The comparison starts from left to right on the top row to the bottom (see. Figure 2 and 2b).
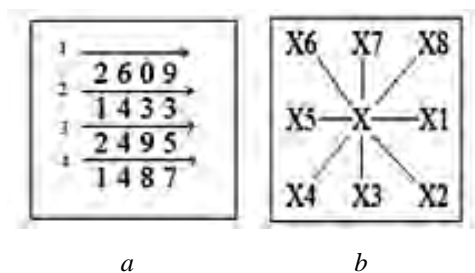

a   *b*

Fig. 2 and 2b. Direction and order numbers
for comparison matrix

As can be seen from the circuit in Fig. 2b: X is the figure which we compare and X1, ..., X8 is a vector of numbers, with which we compare X respectively comparing numbers is in order from X1 to X8, and the direction given the circuit in Fig. 2a. If the chosen matrix of dimension 4x4 the first digit, which we choose as X, will figure 2, which is in the upper left corner of the matrix, after her for X we take 6, 0 and 9, in the same way it will be with each successive line matrix .

One of the features of this algorithm is that after each iteration dimension of the matrix may vary.

The reduction, which we apply is called the absorption of the second kind.

The absorption of the second kind – between two equal components of a matrix, placed in a vector are mutually reduced, both disappear.

Accordingly, a number of inspections to be called absorption rule of the previous inspection:

- Detect – we check the contents of the matrix alternately turning over all its elements in a given order and according to a given direction, as indicated in the description of the algorithm.

- Check for vector – we check whether the numbers that we compare together to equality, are given in the same vector, or beyond its borders.

- Rule preliminary verification has three subparagraphs:

- The rule of equality matrix components.

- Rule limits the vector.

- Rule order and direction of reduction.

When carried out after checking the rules, then we can apply the absorption of the second race and it meets algorithm.

X check point – this component of the matrix, which we compare with the surrounding elements to equality.

Surroundings checking point (X1, ..., X8) – matrix components located around the point X.

Here are just observations:

- If X = X = X1 or X2 or X3 or X = X = X8 ... then these values are reduced.

- If X = X1 and / or X2 = X and / or X = X3 and / or ... X = X8, while reduction takes place according to the algorithm specified order.

Number of iterations of the algorithm N – number of points when the altered matrix after the reduction will continue to just above listed rules will be re-reduction may have altered matrix.

After iterative matrix Main (Matrix after iteration n) – matrix pislya n-th iteration reduction.Note: The dimension of the matrix after each iteration should be recorded as necessary to reverse the algorithm.

The final matrix Mf (Matrix final) – matrix derived from the original after the n-th iteration reduction and therefore this matrix has no prospects for further reductions.

2. Example of the algorithm

For your convenience, selected to show a matrix of Fig. 1. Dimensions 4x4.

$$\begin{pmatrix} 2 & 6 & 0 & 9 \\ 1 & 4 & 3 & 3 \\ 2 & 4 & 9 & 5 \\ 1 & 4 & 8 & 7 \end{pmatrix}$$

Fig. 3. The input matrix

We begin processing matrix of comparison for equality of numbers according to the above direction and order, and it will have the following form:

*Fig. 4. Ms matrix after checking
numbers on equality*

As shown in Fig. 4 in this matrix Ms we found only two cases of equality of numbers in one vector, the next step we apply here the absorption of the second kind, and these numbers are reduced, then the matrix will look like this:

*Fig. 5. Ms matrix after the absorption
and emission identical numbers in a vector*

According to our algorithm matrix can not have empty positions, so we displace the figures remaining from right to left in the direction from the bottom to the top of the matrix, so as to fill the spaces, as in this case, the uppermost row is a guideline matrix. Landmark matrix – the top row of the matrix, which determine the dimension of the matrix and its change in benchmark pidlashtovuvatymutsya all lower lines respectively if during processing matrix after the n-th iteration shrink one or more digits landmark, while the number of columns of the matrix is reduced to m – number reduced numbers landmark, and all lines of the matrix, which is below the reference point during pidlashtuyutsya landmark. So this feature is revealed algorithm as changing the dimension of the matrix during processing. According to the above rules dimension of the matrix can be changed as follows: the number of columns can only be reduced and not increased, the number of lines may increase and decrease, also have exceptions when after n iterations of the algorithm matrix disappears, that all figures matrix after comparing and acquisitions declined , this matrix is called empty and zero ("Matrix empty" Me = 0).

50

After adjusting the offset (shift operations) matrix will look like:

$$\begin{pmatrix} 2 & 6 & 0 & 9 \\ 1 & 2 & 9 & 5 \\ 1 & 4 & 8 & 7 \end{pmatrix}$$

Fig. 6. Matrix displacement after surgery

In some cases there is such a thing when, after the displacement of all digits matrix to fill gaps in the last line (the lowest) number of digits is less than the number of columns and in accordance with the matrix remaining gaps that impede the future work of the algorithm, so these spaces we fill zeros that will be taken into account in subsequent iterations of the algorithm, and this operation will be called complement matrix.

The matrix in Fig. 6 is the matrix, which passed all the necessary operations and actions during the first iteration of the algorithm (Mai1 – "Matrix after iteration 1").

Now we can move to the next iteration of the algorithm (iteration performed for as long as possible will be reducing matrix identical numbers in a vector).

Fig. 7. The second iteration of the algorithm

$$\begin{pmatrix} 6 & 0 \\ 5 & 4 \\ 8 & 7 \end{pmatrix}$$

Fig. 8. Matrix Mai2

Fig. 8 shows a matrix which during processing algorithm has the same numbers that could be cut, so called final matrix (Mf – "Matrix finish").

There are just following the comments – if all steps of the algorithm may be some likelihood that the matrix will be empty (zero). Empty matrix (zero matrix) is such input matrix, which after n – processing algorithm iterations reduction will have no content that is present all the numbers in the matrix are mutually reduced and there will be no number. According restore this matrix is not possible and therefore to prevent this kind of matrix recommended preliminary (testing) reduction for verification matrix adequacy recovery in case the test matrix shows that it is empty, then you should resize nxm, eg matrix Size in 5x10 matrix 10h5. This modified matrix will be called reverse.

When using this algorithm for compression or data encryption is possible such a case, when the number of iterations reductions given in advance and in accordance with acceptable performance of all stages of reduction is optional. It should also be noted that the results of reducing the input matrix and inverse matrix reduction results it often differ among themselves, because as stated earlier, the result of processing matrix depends not only on its content and not only its size, but on both indicators simultaneously. This dependence is caused by the relevant rules of the algorithm of direction and order numbers reducing component matrix.

51

Conclusion

The initial matrix has dimension 4x4, and after processing algorithm of the dimension of 2x3, as there may be cases when the matrix is only one line or one column only, Not possible opportunities when the final matrix has a dimension of 1x1, that consists of only one digit or character. There are exceptions when the initial matrix is not able to reduce the single digits and therefore immediately becomes final, this matrix is called identical (Mi – "Matrix identical"), ie the matrix is identical to the case when the initial matrix completely identical to the final.
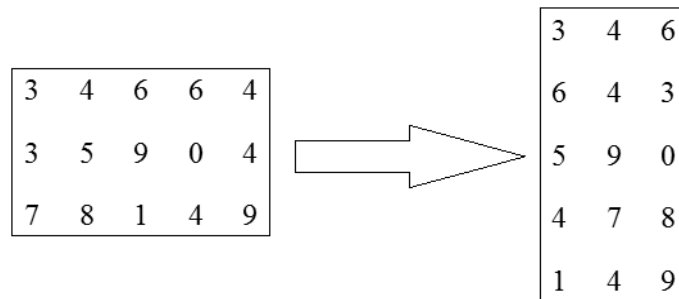

Fig. 9. Example conversion of input matrix inverse

As shown in this example procedure for reducing matrix elements changes immediately and in the same way it will affect each successive iteration reduction since changed the order, for which reduced all the same number.

References

1. Ivantsiv R.-A. Research Methods And Actions For The Transformation Matrix Arrays / Ivantsiv R.-A., Khanas Yu. // САПР у проектуванні машин. Питання впровадження та навчання: матеріали двадцять другої Міжнар. українсько-польської конф. CADMD2014 (10–11 жовтня 2014, Львів, Україна). – Л.: Вид-во Нац. ун-ту "Львівська політехніка", 2014. – С. 166– 172. – Парал. тит. арк. англ. 2. Ivantsiv R.-A. Analysis Of The Transformation Matrix Key-Based Cryptographic Algorithm DES / Ivantsiv R.-A., Khanas Yu // САПР у проектуванні машин. Питання впровадження та навчання: матеріали двадцять другої Міжнар. українсько-польської конф. CADMD2014 (10–11 жовтня 2014, Львів, Україна). – Л.: Вид-во Нац. ун-ту "Львівська політехніка", 2014. – С. 175– 185. – Парал. тит. арк. англ.