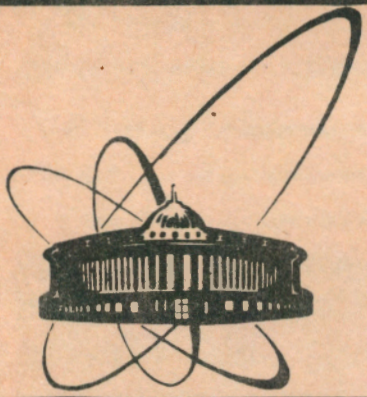

сообщения
объединенного
института
ядерных
исследований
дубна

E10-92-343

V.I.Ilyushchenko

REVERSIABLE MATHEMATICS — AN ARTIFICIAL SCIENCE OR A SCIENTIFIC ART?

1992

1.Introduction

The Fortran arithmetic replacement statement is one of the most frequently used programming tools having the form

$$A = E \tag{1}$$

where A is any variable name, the symbol = stands for the equality sign (ES) and E is an arithmetic expression.

However the true meaning of the ES in (1) is to place the corresponding right-hand-side (r.h.s.) arithmetic expression, E, into the left-hand-side (l.h.s.) storage cell, A, i.e. here we have not an equation with a true ES but a reduced equation (requation) like

$$A \leftarrow E \tag{2}$$

For our subsequent purposes it is very important that here the opposite reduction like

$$A \rightarrow E \tag{3}$$

is totally false.

The detailed analysis shows such semantic and logical controversies (semiconductivity) to be a specific property of the vast majority of mathematical formulas. In terms of information theory here we deal with a unidirected flow of mathematical information accompanied by irreversible information losses.

Let us introduce two nonspecified measures of information,an l.h.s.one, I_L, and an r.h.s. one, I_R, related by a requation like

$$I_L \rightarrow I_R \tag{4}$$

Then the information reversibility ratio, RR, can be expressed as

$$RR = \frac{I_R}{I_L} \tag{5}$$

here the initial information, I_L, is supposed to be given within a range from 0.0 to 1.0 and the only singular point, $I_L = 0.0$, corresponds to $I_R = 0.0$.

2.Fundamentals of reversible mathematics

The notion of reversirility is fundamental for mathematics since the classical interpretation of mathematics as an exact natural science is far from being true – to arrive at a condradiction it is sufficient to solve a more or less involved mathematical problem. The widespread use of computers provides numberless examples of the quite approximate nature of applied mathematics in general.

We will not discuss here the logical axiomatic basis of fundamental mathematics, where relevant information can be obtained from the well-known Godel theorems [1].

Our goal is more pragmatic – to formulate direct and inverse reversibility problems. Here the direct problem must be solved for (4) to obtain an r.h.s., I_R, from an l.h.s., I_L, while its inverse counterpart tends to gain I_L from I_R. It is very important that the singular case with $I_L = 0$ corresponds in (5) to $RR = 0$.

First, instead of the unique old ES we introduce a reversible equality sign (RES, $\leftrightarrow$) and a reduction sign (RS, $\rightarrow$ or $\leftarrow$) so that

$$A \leftrightarrow E \tag{6}$$

$$E \rightarrow A \tag{7}$$

$$A \leftarrow E \tag{8}$$

respectively.

It must be noted that the new RES used in (6) is not equivalent to the old identity sign ($\equiv$) because the latter also conserves the ES reducibility mentioned above.

Second, by starting from an old "equation" and analyzing the real meaning of its ES we will try to find out a true equation by transforming the corresponding requations. For example, in (7) and (8) one needs to transform A – terms to arrive at (6).

These reversifying transforms are equivalent to the use of some additional a priori hypotheses intended for compensating irreversible information losses.

On the other hand, it is principally impossible to formulate here exact algorithmic rules for arbitrary transition from an old requation (1) to a true equation (6). Each specific case requires a specific transformation recipe and it is in this very sense that we use the synonimous name "a scientific art".

Now, to illustrate the potential power of the reversible mathematics approach, let us consider two main problems of linear algebra and the so-called cryptoproblem.

3.Two main linear algebra problems (SLAE-problem and eigen-problem)

3.1.Systems of linear algebraic equations (SLAE)

The first main problem of linear algebra concerns the solution of the SLAE like

$$At = f + n \tag{9}$$

where A is the coefficient (apparatus) matrix, t – a true solution column vector, f – an input r.h.s. column vector and n – a noise (error) column

vector. This "equation" corresponds to a trivial additive noise model.

The widely accepted folklore tradition of using the matrix-vector SLAE (9) can be traced back to the second century B.C., when the ancient Chinese statesman and mathematician Zhang Cang compiled and published the book "Mathematics in nine chapters" [2]. The eigth chapter of this script contains the algorithmized description of the elimination method rediscovered by C.F.Gauss only in 1849 [3].

If the A-matrix in (9) is square and nonsingular, an inverse t-solution can be found from

$$t = A^{-}(f + n) \tag{10}$$

where A^{-} is an inverse matrix satisfying the condition

$$AA^{-} = I \tag{11}$$

with I being the diagonal identity matrix.

For a rectangular and/or singular A-matrix the condition (11) is invalid and one has to use the pseudoinverse (Moore-Penrose) matrix, A^{+}, valid in the least-square sense:

$$t = A^{+}(f + n) \tag{12}$$

In practice the A^{+}-matrix can be computed by means of a Singular Value Decomposition (SVD) [4] or from the generalized approximation like

$$A^{+} = \frac{A^{*}}{A^{*}A + \alpha C} \tag{13}$$

where A^{*} is a complex conjugate matrix, C - a correction matrix (with $C = I$ as a trivial case) and $\alpha < 1.0$ being a correction factor [5].

For a square nonsingular A-matrix one obtains

$$A^{-} = A^{+} \tag{14}$$

Now let us try to solve (9) for A:

$$A = (f + n)t^{-} \tag{15}$$

where t^{-} is a nonexistent inverse vector. This simple bit-like situation clearly demonstrates the strong reducing action of the A-matrix and an evident inadequacy of using t, f, and n in a vector form. In other words, the "equation" (9) must be rewritten as

$$At \rightarrow f + n \tag{16}$$

Let us transform this requation into an all-matrix form [6]:

$$AT \rightarrow F + N \tag{17}$$

we use here the left-to-right RES because it is impossible to reconstruct AT from $F + N$ and the operation of matrix multiplication, AT, results in specific information losses due to orthogonal and homogeneous components of the T-solution. Now, the above transition from the standard matrix-vector form (9) to the nonstandard all-matrix one (17) enables us to realize the A-solution like

$$A = (F + N)T^{-} \tag{18}$$

This novel possibility greatly extends the validity domain of the first main linear algebra problem.

A still further extension of the degree of reversibility of req.(17) will be discussed in subsequent papers.

3.2.Eigenproblem

The second main problem of linear algebra can be expressed in a standard matrix-vector form as follows:

$$Av = \lambda v \tag{19}$$

where v is an eigenvector and λ – a scalar eigenvalue.

By introducing relevant matrices one gets

$$AV = \Lambda V \tag{20}$$

where V – an eigenmatrix composed of column eigenvectors and Λ – the diagonal eigenvalue matrix.

However, the resulting all-matrix r.h.s. of req.(20) contradicts the well-known spectral decomposition theorem that claims [7] that

$$AV = V\Lambda \tag{21}$$

As opposed to the previous SLAE problem, the present all-matrix form (21) indicates the classical matrix-vector form (19) to have the permutationally improper r.h.s., λv. The latter must be replaced by

$$Av = v\lambda \tag{22}$$

for the basic spectral decomposition theorem (21) to be correct as a potential extension of (22).

3.3.An analysis of all-matrix forms

Now let us analyze both main problems formulated in the all-matrix forms (17) and (21).

First, the matrix solution of the SLAE (9) will look as

$$T = A^{-}(F + N) \tag{23}$$

By computing the A^{-}-matrix from (21) one gets

$$A^{-} = V^{-}\Lambda^{-}V \tag{24}$$

That is valid for nonsingular square V-matrices. The diagonal inverse, L^{-}, can be easily computed to yield

$$T \sim \frac{1}{\lambda_{min}} \tag{25}$$

where l_{min} is the minimum eigenvalue.

On the other hand. The analysis of mechanic and electrical systems shows that

$$\lambda = \frac{1}{w_I^2} \tag{26}$$

where w_I are eigenfrequencies, so that

$$T \sim w_{max}^2 \tag{27}$$

The main difficulty in interpreting (26) arises for

$$\lambda_I < 0.0 \tag{28}$$

However, here the negative eigenvalues may witness not eigenfrequencies but instability induced frequencies due to noise.

4.Cryptoproblem

In solving a cryptoproblem, a sender of secret information tries to gain a maximum possible irreversibility with $RR \rightarrow 0$ [8]. To do this, a message plaintext, P,is encrypted into a ciphertext, C, by means of some encrypting transform,T , so that

$$TP \rightarrow C \tag{29}$$

To decrypt this ciphertext, a cryptanalyst tries to find out an efficient inverse transform, T^{-} [9]:

$$P \rightarrow T^{-}C \tag{30}$$

The first encrypted messages were used by ancient Greeks as early as $\underline{V}$ C.B.C. [10].

However, the only really unbreakable (absolutely protected or "semiconductor") ciphers are those based on one-time (expandable) pads invented in the early 1920's [11].

The widely acclaimed novel unbreakable public-key ciphers based on trapdoor one-way functions and realized within GF(p) from 1975 [12] are too slow to be mass-production compatible and in some cases appear to be quite breakable [13-14]. Moreover, the latest hybrid version accepted in the USA, consists of the fast (10^6 bit/s) standard DES and a slow (10^3 bit/s) public-key distributor [15]. However, since DES keys are provided by the National Security Agency, this version is acceptable – by definition – only within internal USA borders.

In this sense much more promising seems to be the socalled real modular arithmetic, topological and fragmentation ciphers developed by the present

author [15]. These ciphers are easy to use, devoid of any long keys as in the case of the classical expandable ciphers and adapted to any coniputerless or computerized environment. The tests are now in progress.

5.Conclusions

Until recently the problem of reversibility in applied mathematics has been solved only in an inverse way, i.e. by increasing the irreversibility up to $RR \rightarrow 0$ as, e.g. in cryptology. The direct problem of mathematical reversibility has not been formulated at all.

However, the above illustrative examples taken from the repertoire of linear algebra show the direct reversibility problem to be solvable in a quite satisfactory manner. Unfortunately, now it is not possible to formulate any general exact algorithm for solving this problem.

6.Acknowledgements

The author would like to acknowledge the late Prof.V.I.Ogurenkov for his highly productive and caustic comments concerning the problems of diaphragm and the science of errors, lathology.

References

[1] K.Godel, Monatshefte für Math. und Phys., 38, 173 (1931).

[2] V.I.Ilyushchenko, JINR Preprint E10-92-295, JINR, Dubna (1992).

[3] C.F.Gauss, Beitrage zur Theorie der Algebraischen Gleichungen, Gottingen (1849).

[4] C.Lanczos, Linear Differential Operators, Van Nostrand, New York (1961).

[5] C.R.Rao and S.K.Mitra, General Inverse of Matrices and its Application, Wiley, New York (1971).

[6] V.I.Ilyushchenko, JINR Preprint, JINR, Dubna (to be published) (1992).

[7] R.A.Horn and C.R.Johnson, Matrix Analysis, Cambridge University Press, Cambridge (1986).

[8] W.Diffie and M.F.Hellman, Proc. IEEE, 67, 397 (1979).

[9] L.S.Hill, Amer.Math.Monthly, 36, 306 (1929); 38, 135 (1931).

[10] D.Kahn, The Codebreakers – The Story of Secret Writing, 3rd ed., Macmillan, New York (1968).

[11] M.Givierge, Cours de Cryptographie, Berger- Levrault, Paris (1925).

[12] W.Diffie and M.E.Hellman, IEEE Trans., IT-22, 644 (1976).

[13] G.I.Simmons, The Math. Intelligencer, 1, 233 (1979).

[14] A.Shamir and R.E.Zippel, IEEE Trans., IT-26, 339 (1980).

[15] V.I.Ilyushchenko, Rational, Fragmentational and Topological Ciphers, JINR, Dubna (to be published) (1992).

Received by Publishing Department
on August 12, 1992.

Илющенко В.И. E10-92-343

Реверсивная математика – искусственная наука
или научное искусство?

Анализ информационной эквивалентности левой и правой частей любого математического уравнения свидетельствует о семантической и логической противоречивости математического знака равенства. В действительности вместо двустороннего знака равенства обычно реализуется знак (и операция) односторонней редукции, который указывает направление потерь информации для иллюстрации общих положений нового подхода. В рамках реверсивного подхода выполнен концептуальный качественный анализ двух основных проблем линейной алгебры и криптопроблемы.

Работа выполнена в Лаборатории высоких энергий ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна 1992

V.I.Ilyushchenko E10-92-343

Reversible Mathematics – an Artifical Science or
a Scientific Art?

The analysis of informative equivalence of left-hand-side and right-hand-side parts of any mathematical equation uncovers both semantic and logical contradictions inherent in the mathematical equality sign. In fact, instead of a bidirectional equality sign one usually deals with a monodirectional reduction sign (and an operation) indicating the direction of information losses. General ideas of the novel approach are illustrated by means of a conceptual qualitative analysis of two main problems of linear algebra and main cryptoproblem.

The investigation has been performed at the Laboratory of High Energies, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna 1992