ISSN 1061-9208, Russian Journal of Mathematical Physics, Vol. 30, No. 4, 2023, pp. 501–521. © Pleiades Publishing, Ltd., 2023.

Analytical Complexity and Signal Coding

V. K. Beloshapka[*,1]

[*] *Faculty of Mechanics and Mathematics of the M. V. Lomonosov*
Moscow State University, Leninskie Gory, 119991 Moscow, Russia
E-mail: [1]vkb@strogino.ru

Received November 13, 2023; Revised November 13, 2023; Accepted November 15, 2023

Abstract. There are two ways to describe a geometric object L: the object as an image of a mapping and the object as a preimage. Every method has its own advantages and shortcomings; together, they give a complete picture. In order to compare these descriptions by complexity, one can use Kolmogorov's approach: i.e., after the clarification of the system of basic operations, the complexity of a description is the minimum length of the defining text. Accordingly, we obtain two Kolmogorov complexities: in the first case, $K^+(L)$, and in the other, $K^-(L)$. Let Cl^n be the class of functions of two variables that can be represented by analytic functions of one variable and of the addition of the depth not exceeding n, and let $K^+(Cl^n)$ and $K^-(Cl^n)$ be their corresponding Kolmogorov complexities. There are arguments in favor of the fact that, for $n \geqslant 2$, the value of $K^-(Cl^n)$ is very large, and the task of constructing a description of Cl^n in the form of a preimage (by defining relations) even for $n = 2$ is computationally unrealizable. Based on this observation, a signal encoding-decoding scheme is proposed, and arguments are given in favor of the fact that the decoding of a signal encoded using such a scheme is inaccessible to a quantum computer.

DOI

1. Coordinate descriptions: object as an image and as a preimage

When describing geometric objects using coordinates, the descriptions widely used two types. The direct one (+) considers an object as an image of the parameter space under the action of a mapping and the inverse one (-) that considers an object as a subset of the encompassing space given by certain defining relations. Here's the simplest example.

Consider a line in the real space $\mathbf{R}^3$. In the first representation, the line l passing through a point (a, b, c) in the direction of the vector (α, β, γ) is the *image* of the mapping $\varphi = (x(t), y(t), z(t))$ of a real line with the coordinate t into the space $\mathbf{R}^3$ with the coordinates (x, y, z). And in the other representation, this is a subset of this $\mathbf{R}^3$, distinguished by two relations:

$$(+) \qquad x(t) = a + \alpha\, t, \quad y(t) = b + \beta\, t, \quad z(t) = c + \gamma\, t,$$

$$(-) \qquad t = \frac{x-a}{\alpha} = \frac{y-b}{\beta} = \frac{z-c}{\gamma} \quad \text{or}$$

$$\begin{aligned} u(x,y) &= -\beta\, a + \alpha\, b - \alpha\, y + \beta\, x = 0, \\ v(x,y) &= -a\gamma + \alpha\, c - \alpha\, z + \gamma\, x = 0. \end{aligned} \qquad .$$

That is, in the other case, the straight line is the *inverse image* of the origin for the mapping ψ from $\mathbf{R}^3$ to the plane of variables (u, v), where $\psi = (u(x, y, z), v(x, y, z))$.

These two representations, the direct one (+), in the form of an image, and the inverse one (-), in the form of preimage, complement each other and are dual with respect to each other. The first representation is focused on the explicit generation of points of the object (line). However, if there is a certain point $p = (x_0, y_0, z_0) \in \mathbf{R}^3$ and we are interested in the question of whether it belongs to a given line, then we must pass to the other representation. And this second representation solves two problems. It gives a criterion for a point p to belong to a given line, and also calculates the value of $t = t_0$ at which $\varphi(t_0) = p$. Towards the first subtask, the task of calculating t_0, the other, the membership criterion for the line, is a solvability condition.

In this simplest example, both the representations are simple and the passage from one representation to another is also simple. If, for the measure of complexity of the expression χ, we take the number $N(\chi)$ of arithmetic operations needed to calculate it, then the complexity for the direct representation is $N^+ = 6$, and for the inverse representation $N^- = 8$.

Consider another example.

Let Cl^1 be the set of analytic functions $z(x, y)$ of two variables having a representation of the form $z = c(a(x) + b(y))$, where (a, b, c) are analytical functions of one variable. This definition of Cl^1 is obviously a definition of the first type, i.e., the definition in the form of an image. If $\mathcal{A}$ is a sheaf of germs of holomorphic functions on the complex plane $\mathbf{C}$ (analytic functions of one variable), then the space of parameters is the direct sum $\mathcal{A} \oplus \mathcal{A} \oplus \mathcal{A}$. The mapping into a sheaf of analytic functions of two variables has the form

$$z(x, y) = \varphi(a, b, c)(x, y) = c(a(x) + b(y)). \tag{1}$$

This representation has all the advantages and disadvantages of a direct representation (as an image): we have an explicit expression that enables us, by varying the parameters (a, b, c), generate all functions $z(x, y) \in Cl^1$. However, if we have a specific analytic function $z(x, y)$ and we need to find out whether z belongs to the class Cl^1, then we need a representation of the other type. To pass from the representation (1) to the inverse representation, we must exclude the parameters (a, b, c) from the relation $z(x, y) - c(a(x) + b(y)) = 0$. This is not difficult to do (see [1]); as a result, we obtain a relation of the form

$$\psi(z) = z'_x\, z'_y\, (z'''_{xxy}\, z'_y - z'''_{xyy}\, z'_x) + z''_{xy}\, ((z'_x)^2\, z''_{yy} - (z'_y)^2\, z''_{xx}) = 0. \tag{2}$$

This relation is a criterion for z to belong to the family Cl^1 in the following sense. If z has a local representation of the form (1), then $\psi(z)(x, y)$ is identically zero wherever z is defined. If $\psi(z)$ is identically zero, then there are two possibilities. Either z is a function of one variable, and then it obviously has the desired representation, or in a neighborhood of any point where $z'_x\, z'_y \neq 0$, the germ of the function z has a representation of the form (1), which analytically continues along all those paths along which z continues and on which the expression $z'_x(x, y)\, z'_y(x, y)$ does not vanish. Note also that $\psi(z)$ is the numerator of the differential fraction $R(z) = (\log(z'_x/z'_y))''_{xy}$. Relation (2) is the solution to the second subtask (-), i.e., a criterion for the existence of the functions (a, b, c). When this criterion is satisfied, the components of the representation (a, b, c) are restored using the integration unambiguously, up to the choice of three constants.

In this example, to calculate the complexity of an expression, we shall count the number of entering functions of one variable, differentiations, and arithmetic operations. Then, for the direct representation, we obtain $N^+ = 4$ and, for the inverse, $N^- = 7$. Here we calculated N^- for R; for ψ we shall obtain more.

The class Cl^1 of functions of the form $c(a(x) + b(y))$ can be included in the expanding hierarchy of classes defined inductively.

$$\begin{aligned} Cl^0 &= \{a(x) \text{ or } b(y),\ a, b \in \mathcal{A}\}, \\ Cl^{n+1} &= \{z(x, y) = c(A_n(x, y) + B_n(x, y)),\ A_n, B_n \in Cl^n, c \in \mathcal{A}\}. \end{aligned}$$

All classes Cl^n in this hierarchy, by definition, obtain an explicit direct description $(+)$. For example, the functions of the 2nd class are parameterized by seven functions of one variable $(a(t), b(t), c(t), p(t), q(t), r(t), s(t))$, and an arbitrary function of the 2nd class has the form

$$z = \varphi_2(a, b, c, p, q, r, s)(x, y) = s\,(c(a(x) + b(y)) + r(p(x) + q(y)))$$

In accordance with our rule for calculating the complexity, we have $N^+(\varphi_0) = 1,\ N^+(\varphi_1) = 4,\ N^+(\varphi_2) = 10$, and then $N^+(\varphi_{n+1}) = 2\, N^+(\varphi_n) + 2$. Every class Cl^n has a finite set of defining differential polynomials $\psi_n(z) = (P^1_n(z), \ldots, P^{m_n}_n(z))$, which give the inverse (-) description of the class, i.e., $Cl^n = \{z : \psi_n(z) = 0\}$. The problem of constructing $\psi_n(z)$ is the problem of the same type as the problem of constructing $\psi_1(z)$ considered above. We have to sequentially eliminate unknown functions of one variable and obtain the solvability conditions. After eliminating the last function, we obtain the solvability conditions for the function z only. These are the equations of the class. For the purposes of elimination, one can use various techniques (resultants, methods of construction of bases of differential ideals).

The classes Cl^n considered above are classes of functions that admit a representation by functions of one variable and by the addition of depth no higher than n. One can consider classes $Cl(S)$ constructed from functions of one variable and addition according to an arbitrary composition scheme S. By a composition scheme we mean a way of arranging brackets to construct the composition. And the same argument allows us to assert that $Cl(S)$ has its own finite set of defining differential polynomials $P(Cl(S))$. In order to characterize the complexity of a finite set of differential polynomials P, we introduce into consideration the following quantities: $k(P)$ is the maximum differential order, $d(P)$ is the maximum algebraic degree, $m(P)$ is the number of polynomials, and $M(P)$ is the total number of monomials. In the paper [2], it was shown how dramatically the complexity of defining polynomials increases under a slight complication of the circuit as compared to the first class circuit. Let us present here some results of this paper.

$$\text{If } P = P(Cl^0), \text{then } k = 1,\ d = 2,\ m = M = 1.$$

$$\text{If } P = P(Cl^1), \text{then } k = 3,\ d = 4,\ m = 1,\ M = 4.$$

$$\text{If } P = P(Cl^{1+}),\ \text{where } Cl^{1+} = \{z = c(a(x) + b(y)) + p(x)\},\ \text{then}\\ k = 5,\ d = 6,\ m = 2,\ M = 68.$$

$$\text{If } P = P(Cl^{1++}),\ \text{where } Cl^{1++} = \{z = c(a(x) + b(y)) + p(x + y)\},\ \text{then}\\ k = 7,\ d = 435,\ m = 6.$$

There are no exact calculations for Cl^2. However, some estimates can be offered. The differential relations for Cl^2 begin at the 11-jet and end at the 32nd one. In this case, the defining polynomials are relations only for derivatives of z. If we restrict ourselves to the order 11, then there are 77 variables in such a jet. The estimate of the algebraic degree of the corresponding algebraic subvariety of the 11-jet, by Bezout's theorem, gives $\approx 10^{90}$. The estimate for the number of monomials is $\approx 10^{2000}$.

Thus, we can summarize:

The problem of constructing $\psi_n(z)$, i.e. constructing an inverse description of Cl^n, is very complicated for all $n \geqslant 2$

Moreover, not only the method of obtaining an answer is very complex, but also the answer itself, i.e., the defining differential polynomials $(P_n^1(z), \dots, P_n^{m_n}(z))$. And we find ourselves in a situation where, from the computational point of view, the direct problem (+) is quite simple, and the inverse (-) is absolutely inaccessible.

A good example of such a situation in number theory is the pair of reciprocal integer problems: computing the exponential functions and logarithms in the multiplicative group of a finite field. As is known, common algorithms of encryption of information [3] are based on the high difficulty of integer logarithm problems.

2. Asymmetry of the Kolmogorov complexity in problems of describing the classes Cl^n

In his 1965 paper [4], A. N. Kolmogorov discussed two well-known approaches to the definition of the "amount of information": the combinatorial and probabilistic ones, and also proposed a new approach, the algorithmic one. In the context of discrete mathematics, this algorithmic approach is commonly understood as a way to measure the "complexity" of a finite sequence of elements of some discrete set. Moreover, it is proposed to take, for a measure of the complexity of a sequence, the length of an "optimal" program (in some programming language) that writes out this sequence.

From the point of view of the two ways discussed above of describing an object, the algorithm generating the sequence Z is a direct description (+) of the object Z, i.e., as the image of some mapping of a segment of the positive integers f (a partially recursive function), i.e., $Z = \{f(1), f(2), \dots, f(m)\}$. To it, certainly, one can assign the inverse problem (-), which is the identification problem, i.e., the problem of verifying the validity of the condition $z \in Z$. Both the first and second problems have the Kolmogorov complexity: $K^+(Z)$ and $K^-(Z)$.

We can talk about computability and algorithms outside discrete mathematics (see, for example, [5]). Let us pass to an analytical context, in which we can discuss the complexity of direct and inverse problems of describing the classes Cl^n. For this, as above when discussing the complexity of Cl^1, we include into the list of elementary operations the functions of one variable, the differentiation, and the arithmetic operations. As a result, we obtain two Kolmogorov complexities of the class, $K^+(Cl^n)$ and $K^-(Cl^n)$.

The thesis formulated in the previous section can now be reformulated as follows:

For $n \geqslant 2$ the complexity of an identification algorithm of class $K^-(Cl^n)$ is significantly higher than the complexity of a generating algorithm of class $K^+(Cl^n)$.

3. Algorithm of coding a signal.

Based on the observation formulated above, we can propose a way of signal encoding-decoding. The modern cryptography is almost entirely immersed in a discrete paradigm. Therefore, we stress that we are talking about a way that does not require the discretization in itself.

Let the transmitted physical signal be a function $F(t)$ defined on a closed interval $\alpha_1 \leqslant t \leqslant \alpha_2$. There are many ways to replace the function $F(t)$ on a closed interval by its approximation on this interval by a real function $f(t)$ which is holomorphic or meromorphic on the entire complex plane. It can be a polynomial (Weierstrass theorem), a trigonometric polynomial (Fourier series expansion), an entire function of bounded growth (Kotelnikov theorem, [6]), etc. Thus, $f(t)$ is an analytic function on the whole line a direct that well approximates F on $[\alpha_1, \alpha_2]$. Moreover, taking into account the physical nature of the signal, we can assume that all such functions are uniformly bounded on $[\alpha_1, \alpha_2]$, i.e., $|f(t)| \leqslant M_f$.

Consider an expression in Cl^2 of the form

$$z(x,t) = s\left(c(a(x) + b(t)) + r(p(x) + f(t))\right).$$

Here $f(t)$ is the approximation of $F(t)$ that we constructed. The remaining six functions $K = (a, b, p, c, r, s)$ is the key for the encoding-decoding procedures. Regarding the functions r and s, we assume that their derivatives are strictly positive on the whole real line, i.e., the inverse functions r^{-1} and s^{-1} are analytic functions that are single-valued on the whole line. The remaining four functions (a, b, c, p) are arbitrary real-analytic functions on the line. Here, both as functions (a, b, c, p) and as the functions (r, s), one should choose functions *of a fairly general form*. For example, if all these functions are polynomials (this is quite admissible), then the degrees should not be chosen too small, and, in the finite-dimensional spaces of the families of coefficients of such polynomials, one should choose a point of a *sufficiently general position*.

Below, we assume that the key K is fixed and is not subjected to disclosure. The coding is carried out by applying the operator Φ to $f(t)$, and the decoding is in applying the operator Ψ to $z(x,t)$:

$$\begin{aligned} f(t) \to \Phi(K, f) &= s(c(a(x) + b(t)) + r(p(x) + f(t))) = z(x,t), \\ z(x,t) \to \Psi(K, f) &= r^{-1}(s^{-1}(z(x,t)) - w) - p(x) = f(t), \\ &\qquad \text{where } w = c(a(x) + b(t)). \end{aligned}$$

The procedure is as follows.

The sender:
(1) transforms the signal $F(t)$ into an analytical expression $f(t)$ approximating F on $[\alpha_1, \alpha_2]$,
(2) using the key K and the operator Φ, transforms $f(t)$ into $z(x,t)$ (the image),
(3) transmits $z(x,t)$ to the recipient via an open communication channel.
The recipient:
(4) using the key K and the operator Ψ, transforms $z(x,t)$ into $f(t)$, i.e., to the approximation of the original signal $F(t)$ on the closed interval $\alpha_1 \leqslant t \leqslant \alpha_2$.

This procedure is resistant to errors in the transmission of the image $z(x,y)$. Let

$$\begin{aligned} |f(t)| \leqslant M_f \text{ for } \alpha_1 \leqslant t \leqslant \alpha_2, \quad |p(x)| \leqslant M_p \ \text{ for } \beta_1 \leqslant x \leqslant \beta_2, \\ |w(x,t)| \leqslant M_w \ \text{ for } \alpha_1 \leqslant t \leqslant \alpha_2,\ \beta_1 \leqslant x \leqslant \beta_2, \\ |r(u)| \leqslant M_r \ \text{ for } |u| \leqslant M_p + M_f, \quad |s(v)| \leqslant M_s \ \text{ for } |v| \leqslant M_w + M_r. \end{aligned}$$

Then $|z| \leqslant M_s$ for $\alpha_1 \leqslant t \leqslant \alpha_2$, $\beta_1 \leqslant x \leqslant \beta_2$. Let N_s be the minimum of $|s'(v)|$ for $|v| \leqslant M_w + M_r$, and let N_r be the minimum of $|r'(u)|$ for $|u| \leqslant M_p + M_f$.

Let, as a result of errors in the formation and transmission of the message, z transformed into $\tilde{z} = z + \delta z$.

Accordingly, $\Psi(K, z+\delta z) = f + \delta f = \tilde{f}$. Then

$$\begin{aligned}|\delta f| &= |r^{-1}(s^{-1}(z(x,t)+\delta z(x,t)) - w) - r^{-1}(s^{-1}(z(x,t)) - w)|\\ &\leqslant \frac{1}{N_r}\,|s^{-1}(z(x,t)+\delta z(x,t)) - s^{-1}(z(x,t))| \leqslant \frac{1}{N_r\,N_s}\,|\delta z(x,t)|.\end{aligned}$$

Note that f does not depend on x, which is not the case for $\tilde{f}$.

The given encoding-decoding scheme uses the key K, which is applied by both participants; the sender for encoding, the recipient for decoding In the absence of a key, the decoding problem (the decomposition problem for a 2nd class function) becomes very difficult.

This is a very flexible construction, and we have many options for its complication and modification. From the scheme of composition of functions in the class Cl^2, we can pass to a scheme based on the representation of a function from Cl^n (the key is a family of $2\,(2^n - 1)$ functions of one variable). Or to $Cl(S)$ for an arbitrary composition scheme S.

In a more general situation, the construction looks as follows. We choose one of functions that are at the lowest level of composition (a function of t), and reserve it for the transmitted signal $F(t)$ (more precisely, for its analytical approximation $f(t)$). We fix all other analytical functions of one variable needed to construct a composition with a circuit S, choosing functions of a fairly general position, i.e., the key K. We obtain the coding operator $f(t) \to \Phi(S, K, f)(x,t) = z(x,t)$. The decoding operator $z(x,t) \to \Psi(S,K,z)(t) = f(t)$ is constructed similarly to what we described above for Cl^2. The decoding is carried out by step by step reducing of the complexity of the composition. In this case, the decoding operators for expressions of lesser complexity naturally arise, that use parts of our key, When constructing the operator Ψ, inversions of some functions included in the key are used. Therefore, when generating the key, we impose the condition that these functions are monotone.

Another direction of generalization of the construction is associated with the use of hierarchies of complexity for functions of larger number of variables rather than two [7]. For functions of three variables, two problems can be considered: the question on the representability by superpositions of functions of one variable and the addition (superpositions (3) → (1)) or on representability by superpositions of functions of two variables (superpositions (3) → (2)). Let us stand up at the second point of view, and now let $\mathcal{A}$ be a sheaf of germs of analytical functions of two variables. Consider the hierarchy of classes of analytical functions of three variables $w = g(x,y,z)$ determined inductively:

$$\begin{aligned}Cl^0 &= \{a(x,y) \text{ or } b(y,z) \text{ or } c(z,x), \quad a,b,c \in \mathcal{A}\},\\ Cl^{n+1} &= \{w(x,y,z) = c(A_n(x,y,z), B_n(x,y,z)),\ A_n, B_n \in Cl^n, c \in \mathcal{A}\}.\end{aligned}$$

The identification problem for Cl^2 is very difficult. This can be used for an encoding circuit for a 2-dimensional signal (image) $f(t,s)$.

The general scheme for the composition of a function $w \in Cl^2$ uses seven functions of two variables. Each of the four lower-level functions depends on some two variables from the set (x,t,s); it is necessary to clarify which ones are used. Let us fix this choice, for example, like this:

$$w(x,t,s) = \varphi(a,b,c,p,f,r,s)(x,t) = s(c(a(x,t), b(x,s)), r(p(x,s), f(t,s))),$$

We reserve one of the lower-level functions for our signal, and fix the remaining six ones and declare them as the key K. Thus we obtain the transformation

$$f(t,s) \to \Phi(K,f)(x,t,s) = s(c(a(x,t), b(x,s)), r(p(x,s), f(t,s))) = w(x,t,s).$$

To make the transformation invertible (the analog of monotonicity), we must have two keys (K, K'). Moreover, each of the three pairs of functions (s,s') and (r,r') must define a globally invertible transformation of $\mathbf{R}^2$. The coding is

$$f(t,s) \to (\Phi(K,f)(x,t,s), \Phi(K',f)(x,t,s)) = (w_1(x,t,s), w_2(x,t,s)),$$

i.e., $(w_1(x,t,s), w_2(x,t,s))$ are sent to the recipient. The decoding is carried out using the mappings of $\mathbf{R}^2$ inverse to $(s(u,v), s'(u,v))$ and $(r(u,v), r'(u,v))$. Note that this construction allows one to transmit two encoded images in one session: f using K and h using K'. But the equality $h = f$ does not interfere with the procedure. It should also be noted that a function of one variable $f(t)$ can also be transferred as f.

A further complication of the construction can be obtained by considering hierarchies related to the superposition problem of the form $(k) \to (l)$, where $k > l$ (expansion of functions of k variables in a superposition of functions of l variables).

Let us present arguments in favor of the fact that the encryption scheme using functions in Cl^2 of two variables *is not available for decoding using a quantum computer*, i.e., a computing system constructed from qubits [8]. The state of one qubit is described by a complex-valued function of time t taking values on the unit circle of the complex planes, i.e., $\exp(i\,\nu(t))$. This is a function of one variable. The quantum superposition is a transition to a linear combination. Let there be a computational device that allows, as simple basic operations, a set of four arithmetic operations, performs all (analytical) functions of one variable, as well as analytical operations on them (superposition, differentiation, and integration). Such a device appears to dominate the quantum computer. The demonstration given in [2] aims to show that the problem of constructing a decomposition for functions in Cl^2 (in the absence of a key) is apparently inaccessible even for such a powerful device.

Certainly, if we imagine that advances in the physical sciences will lead to a situation in which instead of a qubit, another unit will be proposed, the state of which is a function of not one but two variables, and a device for free manipulation with a system of such units will be suggested, then our argument for such a computer will be not applicable. Then we will need a coding scheme (considered above) based on the complexity of the Cl^2 identification problem for functions of three variables.

REFERENCES

[1] V. K. Beloshapka, “Decomposition of functions of finite analytical complexity”, J. Sib. Fed. Univ. Math. Phys., 11 (6), 680–685 (2018).

[2] V. K. Beloshapka, “On the Complextity of the Differential-Algebraic Description of Analytic Complexity Classes,” Math. Notes, 105 (3), 309–315 (2019).

[3] *Cryptography: an Introduction.* Written by V. Yaschenko, N. Varnovskii, Yu. Nesterenko, G. Kabatyansky, P. Gyrdymov, A. Zubov, A. Zyazin, and V. Ovchinnikov, American Mathematical Society, Providence, RI, 2002.

[4] A. N. Kolmogorov, “Three approaches to the definition of the concept “quantity of information” ” Probl. Peredachi Inf., 1 (1), 3-=11 (1965).

[5] L. Blum, M. Shub, S. Smale, “On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines”. Bull. Amer. Math. Soc. New Ser. 21 (1), 1–46 (1989).

[6] V. A. Kotel’nikov, “On the transmission capacity of ’ether’ and wire in electric communications”, Phys. Usp., 49 (7), 736–744 (2006).

[7] V. K. Beloshapka, “Analytic complexity of functions of several variables”, Math. Notes, 100 (6), 774–780 (2016).

[8] A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi, *Classical and Quantum Computation*, American Mathematical Society, Providence, RI, 2002.