#12 (3) / 2015

Czasopismo indeksowane na liście czasopism punktowanych MNiSW 6 pkt. (Lista B, lp. 1365)

recenzowane czasopismo naukowe poświęcone zagadnieniom współczesnej humanistyki i nauk społecznych

Członkami Redakcji i Rady naukowej są uznani badacze z Polski i zagranicy

PROSOPON

Europejskie Studia Społeczno-Humanistyczne | European Humanities and Social Studies

HUMANUM Instytut Studiów Międzynarodowych i Edukacji w Warszawie

12 (3) / 2015

PROSOPON

ISSN 1730–0266

Czasopismo indeksowane na liście czasopism punktowanych MNiSW **6 pkt. (Lista B, lp. 1365)**

recenzowane czasopismo naukowe poświęcone zagadnieniom współczesnej humanistyki i nauk społecznych

Członkami Redakcji i Rady naukowej są uznani badacze z Polski i zagranicy

PROSOPON

Europejskie Studia Społeczno-Humanistyczne
European Humanities and Social Studies

Instytut Studiów Międzynarodowych i Edukacji Humanum, Ptoukha Institute for Demography and Social Studies of National Academy of Sciences of Ukraine, International School of Management in Prešov (Slovakia)

Adres redakcji i wydawcy | Publisher: **Instytut Studiów Międzynarodowych i Edukacji Humanum**, ul. Złota 61, lok. 101, 00-819 Warszawa www.humanum.org.pl / Printed in Poland
Co-editor – International School of Management in Prešov (Slovakia)

ISSN 1730-0266

Czasopismo punktowane Ministerstwa Nauki i Szkolnictwa Wyższego w Polsce. Lista B, 6 pkt, poz. 1365
The magazine scored by Ministry of Science and Higher Education in Poland. List B, 6 points, pos. 1365

12 (3) / 2015

Prosopon
Europejskie Studia Społeczno-Humanistyczne

Wydawca / Publisher:
Instytut Studiów
Międzynarodowych
i Edukacji HUMANUM
www.humanum.org.pl

12 (3) 2015
ISSN 1730–0266

Spis treści

Prosopon
Europejskie Studia Społeczno-Humanistyczne

Wydawca / Publisher:
Instytut Studiów
Międzynarodowych
i Edukacji HUMANUM
www.humanum.org.pl

12 (3) 2015
ISSN 1730–0266

Ramiro Délio Borges de Meneses
Instituto Universitário de Ciências da Saúde,
Gandra, Paredes, Portugal
E-mail: borges272@gmail.com

Normenfindung in der sexualethik / *Normenfinder in the sexualethics*

Abstract
This paper focuses the global thought for the relatinship between the ethical norm and the sense of sexual moraltity. Therefore,there is the effort to find the sociological value of this moral account in the aims of the human sciences, particularly the virtue of the moral philosophy, and ypour applications, that plays a very important role to the ethical judgment among the human conduct.

Key words: **ethics, sexuality, philosophy.**

NORMENFINDUNG DURCH ERFAHRUNG

Bei der Feststellung einer sittlichen Norm wird man sich zunächst der Wirklichkeit zuwenden müssen, von der eine Zielgerichtetheit ausgesagt werden soll. Der sittliche Handelnde ist nämlich zu allererst von einem empirischen phanomenhaften Vorgegeben betroffen. Er erlebt eine noch ungestaltete Realität, die ihn erfabt und ihm als Verlockung, Mysterium begegnet.

Diesem passiven Betroffensein entspricht nun das lehrt z.B. jede Situation der Versuchung auf der Seite des Betroffenen ein aktives Zugehen auf die gleiche Wirklichkeit. Das Subjekt öffnet sich für das Vorgegebene, es nimmt die Realität an, ergreift, formt.

Die darbietende Wirklichkeit und das nach dieser Wirklichkeit ausgreifende und sie damit gestaltende Subjekt sind aufeinander bezogen. Darbieten auf der einen Seite und ausgreifen und gestalten auf der anderen Seite bedingen einander. Das eine ist ohne das andere nicht denkbar. Das hört auf, wie eine Platitüde zu wirken, wenn man die Begriffe “Darbieten” und “Ausgreifen” bzw. “Gestalten” in anthropologische Termine übersetzt. Das erste bedeutet dann ein Sollen und das zweite

ein aktives schöpferisches Wirken. Unter einer anderen Rücksicht meint das erste eine Erfüllung, eine Bereicherung, ein Befreitwerden des Subjekts. Damit ist nichts anderes ausgesagt als die materiale Identität von Sollen und Befreitwerden, von schöpferischem Wirken und Freiheit. Aber identisch sind auch Befreitwerden und (aktive) Freiheit, Sollen und schöpferisches Wirken. Der einzige Unterschied liegt lediglich darin, dass einmal das Subjekt, d.h. der Mensch mitgedacht ist und ein anderes Mal das Objekt, d.h. die Welt.

Das, was wir Norm nennen, representiert die zweifach verschrankte Identität: Befreiung des Menschen und schöpferisches Wirken an der Welt nach dem Maβ des Menschen. Das erste ist mit dem Sollen identisch, aber es wäre ein schwerwiegendes Miβverständnis, wollten wir aus diesem Wort "Sollen" nur das Element der Eingrenzung (des Menschen) heraushören. Es bleibt in jedem Falle Befreiung. Das zweite, das schöpferische Wirken an der Welt, ist mit Formen, Gestalten, Ordnen und diesem Sinn mit Bingrenzung identisch, aber es wäre auch hier ein Miβverständnis, zu übersehen, dass es sich nichtsdestoweniger um schöpferisches Tun handelt. Es geschieht in beiden Richtungen Anreicherung von Wirklichkeit, Vermenschlichung in der einen Richtung und Weltauslegung (leider ist das Wort Verweltlichung mit anderen Sinngehalten belegt) in der anderen Richtung die Norm ist der Ort der Auslegung von Mensch und Welt, Ermöglichung von Befreiung und Schöpfung von beiden und mit der Evolution mitwandernde Garantie. Dennoch ist die Norm - das soll nicht verschwiegen werden - ambivalent: sie ist Ermöglichung von Befreiung, gewiβ, aber sie ist es gemäβ der Grenze des Menschen. Sie setzt schöpferisches Wirken frei, aber gemäβ der Grenze des Menschen. Die Norm ist Behauptung, Aussage, Darstellung und zugleich Negation, Eingren-zung, Kritik. Die Norm ist die Eröffnung von Wirklichkeit und zugleich deren Infragestellung. (Eröffnung und Infragestellung nennen wir die formale Norm, die Wirklichkeit, die eröffnet wird und in Frage gestellt wird, die materiale Norm). Nur unter beiden Aspekten zugleich erscheint der Mensch als das Maβ.

Erkannt wird die Norm aus dem Vollzug von Befreiung und schöpferischem Tun, aus der Menschen- und Weltveranderung, aus der Praxis, aus Erfahrung. Díe Norm wird bewusst in der Einheit von Erkennen und Tun in der Entwicklung und im Prozeβ. Weltauslegung geschicht im Rahmen von Weltveranderung (Erfahrung). Der Mensch erkennt nur in dem Maβ sich selbst, als er sich selbst verwirklicht (erfährt). Von der sittlichen Erkenntnis, die Erkennen und Tunzusammen ist, muss nochmal die Formulierung der Norm unterschieden werden. Diese ist nur nach langeren Abschnitten sittlichen Handelns möglich, denn ein individueller sittlicher Akt ist nicht bis ins letzte zu analysieren, sondern enthält stets einen unreflektierbaren Rest. Erst in der Wiederholung treten Strukturen, eventuelle Polaritäten und Harmonien des sittlichen Handelns zu Tage. Aus dem Gewohnten, das durch Quer - und Langsschnitte auf ihre innerere Gesetzlichkeit zurückgeführt wird, kann im Laufe der Zeit ein Sichtraster erstellt werden, der geeignet ist, die sittliche Norm auch rational begrifflich zu umschreiben. Die Formulierung, die ein Ergebnis der Theorie der sittlichen Praxis ist, ist notwendig, weil von der Mehrzahl der Menschen mit ihrer Hilfe die Wirklichkeit, auf die das handelnde Subjekt zugeht, in ihrer Sinn und Normhaftigkeit erfaβt wird.

Die Formulierung der Sinn und Normhaftigkeit wird wegen der rational begriffliche Operation nicht immer adäquat sein, sich oft mit Grobeinstellungen und allgemeinen Verhaltensmustern begnügen. Ja manchmal mag Sie auf langere Zeit sogar eine Fehlinterpretation widerspiegeln. Diese Gefahr darf sie jedoch nicht verführen, auf die Formulierung von Normen überhaupt zu verzichten. Die Porderung, dass sie auf die Praxis bezogen ist, "praktisch" ist, und zugleich auf die über und vorausschauende Theorie nicht verzichtet, muss bisweilen in Widerspruch geraten zu den anderen Forderungen der individualität und rationalen Scharfe. Die Ambiguität, die sich dabei zeigt, wird man leicht verstehen, wenn man bedenkt, dass die Formulierung der Norm wie die sittliche Erkenntnis überhaupt auf Erfahrung beruhen.

NORMEN IM SEXUALBEREICH

In einer solchen Lage müssen wir uns die einzelnen Stufen der Normenfindung bewuβt machen, die von Menschen erlebte und geformte Wirklichkeit der Sexualität auf ihren vollen Sinn hin befragen. Um zu einer gültigen Darstellung der Norm zu gelangen, werden wir daran herangehen müssen, die Realität, die sich in besonderer Weise auf den ganzen Menschen bezieht, Sie in ihrer historischen, sozialen und theologalen Verfaβtheit zu beschreiben und sie dann auf ihre inneren Möglichkeitsbedingungen zurückzuführen. Man kann damit beginnen, indem man "common sense" walten laβt, Alltagsbeobachtungen anstellt, seine Lebenserfahrungen befragt, usw. Eine wissenschaftliche Ethik kann jedoch nicht darauf verzichten, sich in ein kritisches Gesprach mit Binzelwissenschaften zu begeben, welche auf ihre Weise und nach den ihnen eigenen Methoden die Realität einmal beschreiben.

Aus der Vielzahl der möglichen Beschreibungen verweisen wir nur auf zwei, denen aber im Bewuβtsein unserer Zeitgenossen eine besondere Bedeutung zukommt, Psychologie und Soziologie.

Von der Psychologie könnte man sagen, sie bemüht sich in empirischer Beschreibung um die dominanten Handlungsmotive und Handlungsstrukturen. Die Sexualpsychologie sucht diese für das Phaenomen der Liebe zu erfassen. Ohne den Anspruch zu erheben, dabei auch nur die wichtigsten Züge heranzuheben, werden wir einige Elemente aufzahlen, die imstande sind, unsere Frage zu illustrieren: Liebe ist erlebbar und psychologisch charakterisierbar als Lust und allgemeine Steigerung des Lebensgefühls. Sie sind im ersten Augenblick nicht frei von Selbstbezogenheit, kraft deren es dem Liebenden gelingt, von der Umwelt (mit ihrer Bedrohung und ihren Schwierigkeiten) abzublenden. Eine Gefahr der Verschlieβung in sich selbst wird jedoch dadurch überwunden, dass Lust immer mit etwas biologisch Sinngegeben ist. Sie ist gekoppelt mit elementare Vorgänge und sozialen Zielen. Zwei Elemente sind stets zu unterscheiden, das Bedürfnis nach sexuellem Ausdruck ihrer Natur nach frei von jedem personalen Bezug und die Forderung, dass sexuelle Lust nur unter einer personalen Bindung sein soll. Diese Unterscheidung, die einer thematischen Trennung entspricht, hat einen inneren Sinn. Einmal gibt sie ein Mass an Freiheit. Die Möglichkeit, verschiedene

Ziele anzusteuern, gibt dem Menschen auch seelich den notwendigen Spielraum, zu reifen. Und zum anderen wird dadurch eine wichtige kybernetische Funktion frei für die Ausbilung von Verhaltensmustern. Im System der ungerichteten und undeterminierten Handlungstriébe drängt die Lust auf Institutionalisierung. Wie jedes sittliche Handeln ist auch die sexuelle Aktivität eine gesellschaftliche, soziale Wirklichkeit, die sich selbst in Sinn- und Interpretationszusammenhängen, in Symbolen und Projektionen entwirft. Lust und Liebe stehen in cinema inneren Bezug zur Sozialisation und Gemeinschaft. Es gibt ähnliches wie im Bereich des anderen gewaltigen, menschlichen Triebes, den P. Hacker folgendermaben charakterisiert: Wir definieren Aggression als dem Menschen innewohnende Disposition und Energie, die sich ursprünglich in Aktivität und spüter in verschiedenen individuellen und kollektiven, sozial gelernten und sozial vermittelten Formen von Selbstbehauptung bis zur Grausamkeiter Ausdruck. Und an ciner aderen Stelle: "Durch Aufsagen und Kanalisierung angsterzeugen der, frei Aggression verhilft Sozialisierung dem Individuum zu Angstfreiheit und zu Zweckgericht tun: weil Individuen und Gruppen nur eine gewisse Quantität freien. Aggression ohne Gefährdung ihres Lebens können, müssen sie kraft ihrer Symbolfähigkeit und ihrer Einbildungskraftinstitutionen schaffen, die einen Teil der freien Aggression abfangen, aufnehmen, regeln und in bestimmte Bahnen lenken.

Die Unabhängigkeit zwischen Trieb und sozialer Organisation ist dann auch der Grund, warum die Symbolwelt und die Projektionen, welche zunächst die Liebe (im weitesten Sinn) ermöglichen und stabilisieren auf "etwas außerhalb seiner Gegenstndlichkeit Liegendes-gerichtet sein kann. Wie das ästhetische Objekt vom Objekt verschiedene-Bewusstseinstrukturen verweisen und sie aktualisieren kann, so können die Symbolisierungen einer bestehenden Sexualmoral bestehende Herrschafts-, Konsum- und Ideologieverhältnisse anzeigen und aktualisieren. Letztlich ist die Unabhängigkeit dann auch der Grund dafür, dass man an eine wirkliche Beeinflussung, Steuerung, Soziokybernetik der sexuellen Verhaltensweisen herangehen kann. Eine ihrer Instanzen ist z.B. die Wissenschaft, nicht nur die Psychoanalyse, z.B.(Der wesentliche Einfluss und wissenschaftlicher Entwicklung liegt hier sicher in der Anregung der kulturkritischen Diskussion innerhalb einer grenzten öffentlichkeit) sondern auch der Pharmazeutik (Kontrazeptive haben sicher einen sozialen Wandel hervorgebracht). Man allerdings, dass die von ihr ausgehende Aufklärung nur bestimmte Altersgruppen reicht, in denen noch keine entgegenlaufenden Vorstellungen verankert sind. (Offenbar entspricht die Wirkung dieses Informationsstoffes auf das Publikum den Bedingungen, wie sie für die Prozesse der Massenkommuníkation allgemein geworden sind: lhre Gehalte werden vorzu, von denen aufgenommen, deren Denkrichtung sie ohnehin weitgehend entsprechen). Immer scheint die Gruppe der Altersgleichen, Kollegen und anderer Freundschaften noch eine besondere Instanz der Sexualpädagogik zu sein. Als übermíttler tabuierten Wissens werden von der Soziologie als besondere Instanz im gesellschaftlichen Erziehungsprozeβ angesehen. Sie scheinen die konkret, sozial und kulturell farbare Gemeinschaft zu sein.

Die Frage, wie die und Gestalten der Befreiung und schöpferische tun sein kann, wie sie zugleich Bingrenzung und Kritik unterworfen werden muss, um tatsäch-

lich Aussage (seiner Freiheit und seines schöpferischen Wirkens) sein ist damit noch nicht beantwortet. Zu diesem Zweck muss die sittliche Erkenntnis, die zweifellos mit der Beschreibung der ersten Intuition beginnt, weiter getrieben werden. Die Realität, die im sittlichen Akt konfrontiert wird, muss auf ihre innere Gesetzlichkeit zurückgeführt werden. Das ist gleichbedeutend - wie wir sahen - mit der anderen Wendung: Die innere Gesetzlichkeit der Wirklichkeit muss nach der Möglichkeit der Befreiung und des Tuns befragt werden, und zwar insofern beide sowohl positive Behauptung als auch Kritik sind. Das kann wegen der Bindung aller sittlichen Erkenntnis wiederum nicht apriorisch geschehen. Aber es muss geschehen unter Berücksichtigung der Totalität. Rückführung und Befragen müssen sich nach all den Kategorien, die aus ciner transzendentalen Reduktion des sittlichen Handeln des Menschen selbst gewonnen werden (Individualität, Sozialität, Geschichtlichkeit, Beziehung zu Welt und Beziehung zum Absoluten) und die zeigen, was der Mensch möglicherweise ist (Ort der Metaphysik in der Ethik). Was die innere Gesetzlichkeit der Wirklichkeit, der Mensch oder - was im gleichen Sinn gebraucht wird - seine Natur wirklich ist, worin die konkrete Gestalt der Befreiung und des schöpferischen Wirkens besteht, welche Form die Individualität und Sozialität, die Geschichtlichkeit und Evolution, der nicht austauschbare Bezug zum Absoluten hier und jetzt angenommen haben, das kann wiederum nur aus der Erfahrung heraus bestimmt und formular werden. Die Spannung, die darin besteht, dass bei der Erfassung dieser Norm die Aktualität und Praxis zusammengehen müssen mit einer möglichsten umfassenden und auf ihr aufbauenden, jedoch möglicherweise fehlgehenden Theorie, wird in der Formulierung der Norm berücksichtigt, die wir Modell nennen und die *universale concretum* und (die Individualität nicht immer voll berücksichtigendes). Die Ansätze der induktiven Normbestimmung: Intersubjektivität, Symbol und Akt der Freiheit. Die Beobachtungen der Psychologie und der Soziologie haben für die Erkenntnis der Natur, des Menschen, die nur als Kultur greifbar ist, einen Hinweis gegeben. In gewisser Hinsicht - haben wir gesehen - müssen Sexualität als Trieb und ihre Verwirklichung mit einem Partner unterschieden werden. Die letztere, die Beziehung zum Partner, übernimmt gegenüber dem Trieb eine Regelfunktion. Kraft bestimmter gesellschaftlicher Institutionen und Symbole interpretiert, kontrolliert, gestante sie die Natur des Menschen und Form der Sexualität. Das gibt uns eine erste Oriontíerung für die induktive, d.h. von der Erfahrung herkommende, Bestimmung der Norm. Geschlechtlichkeit kann verstanden werden von der sie kulturell überformenden und gestaltenden Gesellschaft. Geschlechtlichkeit ist gesellschaftliche Wirklichkeit. Die Norm Iässt sich darum in einem ersten Schritt immer bestimmen als das Maβ, das die Gemeinschaft befreit (das eingrenzt und kritisíert), das sozial und die Gemeinschaft aufbaut. Das, was eine Gemeinschaft aufbaut, ist sittlich richtig, was ihr schadet und unrichtig. Die Erkenntnis der Norm besteht zuerst und vor allem im Eingeständnis der vollen Verantwortung der eigenen Geschlechtlichkeit vor dieser Gemeinschaft. Was gemeint ist, kann am freudlichen Verständnis des Verbrechers verdeutlicht werden. Nach Freud ist z.B. beim Verbrecher das Schuldgefühl (also die Verantwortung gegenüber der Gemeinschaft) früher als das Verbrechen. Er bejaht das Verbrechen, um durch die zu erwartende Strafe die Verantwortung anzuerkennen und das Schuld-

gefühl zu mindern. Die Ortung von Verantwortung inbezug auf eine Gemeinschaft Iãsst sich auch bei sexuellen Tabus, die sich z.B. an einem Phänomen wie der Prostitution beobachten Iãsst, feststellen. Triebverdrängungen, Schuldgefühle und Konflikttatbestände innerhalb der eigenen Sexualität werden in Verkennung der Verantwortung auf eine bestimmte Gruppe innerhalb der Gemeinschaft projiziert, die eine Sündenbockfunktion annimmt. Die räumliche Isolierung, die gesellschaftliche ausgeübte Kontrolle (Gesundheitsdienst und Polizei), aber auch die bewuβten und halbbewuβten Erwartungen sind Äuβerungen einer Verantwortung. Wäre man bereit, Konflikt und Schuld auf sich zu nehmen, hãtte man den ersten Schritt zur Erkenntnis der Norm für seihe Sexualität getan. (ähnliche Tabus sind nach Adorno das unschuldige Kind, die Homosexualität, etc.) Bei der Sexualität kann man jedoch nicht eigentlich von der Gesamtgesellschaft ausgehen, da sie nur einem mittelbaren Bezug zu ihr steht, sondern man muss sich auf die Gemeinschaft mit dem anderen Partner konzentrieren. Gegenüber ihm wird man sich zuerst auf seine Verantwortung besinnen müssen. Man das wirklich, dann können z.B. ideologische Forderungen des Konsums, der Preizeit und des jeweiligen Systems der Horrschenden, in denen die Gesamtgesellschaft, von der Praxis und der Subjektivität sich entferndende Forderungen erhebt und so die "menschlichen" Möglichkeiten überfordert. Das ja oder das "mea culpa" vor dem eigenen Partner offenbart die Norm, unter der die Sexualität steht, am deutlichsten. Über die Ehe- und Familienbeziehung ist dann die Idealgrup für die Ausbildung von Normen entscheidend.

SCLUESSELSACHE

Die Sozialisation stellt sich allerdings in Symbolbildung und Institutionalisierung dar, welche den Trieb stabiliseren, ihn bei Konfliton schützen und ihn dem Individuum garantieren. Man kann sich demnach in einem zweiten Schritt der sittlichen Erkenntnis den Institutionen (z.B. Ehe) und Symbolen (z.B. Tanz) direkt zuwenden. Am Anfang mag lediglich (siehe bürgerliche Moral und Eheauffassung) ein unreflektierter Protest stehen, der aus der entgegengesetzten sittlichen Beurteilung stammt, auf ihn aufmerksam machen. Dann mögen bestimmte Bilder, Gewohnheiten, Moden, Mythen, die schon eine gewisse Zusammenfassung des Sinnes darstellen, ihre Bedeutung verlieren, auf die Stufe der Wirkungslosigkeít oder gar Lächerlichkeit herabsinken. Der sexuellen Norm kommen wir auf die Spur, wenn wir bei Protest, bei der Entwertung traditioneller Institutionen, Symbolen und Systemen unser Augenmerk darauf richten, dass sie nicht mehr oder nicht mehr im gewohnten Maβ menschliches Potential freigeben, keine echte gesellschaftliche Befreiung mehr sind, ihre Kommunikatíons~ und Verständigungsfunktion eingebukt haben, dass Antriebe, die innerhalb der Gruppe aufkommen, und im Gruppenprozess fruchtbar Gemacht werden können, die sexuelle Praktik tatsächlich problemlosen Zugang zum Glück verschafft. Sofern die Symbole oder der reflektierte Sinn von Sexualität nicht zur Ideologie herabsinkt, müssen sie der Situation, den Umständen und der Subjektivität verhaftet bleiben. Sie dürfen nicht zu einem konservativen Mittel des Gewuhnlichen und des Üblichen erstarren. Zu gleicher Zeit müssen sie überschaubare Ganzheiten bleiben, d.h. über einen gewissen Grad der Abstraktion verfügen. Es bleibt aber die Frage, wie die aktuelle Formulierung

der Norm zwar praxisbezogen sein, aber dennoch eine bestimmte geschichtliche Richtung anzeigen kann, wie sie auf den Menschen in ihrer Individualität bezogen sein kann und zugleich über eine gewisse Allgemeinheit verfügt. Wir haben früher gesagt, das sei möglich in der allgemeinen Vorstellung des Modells, das Aussage und Kritik zugleich sei, das als *universale concretum* ein in der Evolution und geschichtlichen Entwicklung stehendes Verhaltensmuster ist. Seine Plastizität, erklärt sich allem aus der Tatsache, dass die Sinn- und Normwirklichkeit nicht nur die Umschreibung der dem handelnden Subjekt gegenüberstehenden Wirklichkeit ist, sondern die Feststellung des Subjekt selbst. Die tatsächliche Annahme ciner Norm geschieht in einer Tat der Freiheit, die Wagnis ist und der letzten abstrakten Sicherheit entlehrt. Das Subjekt erfabt in einem "Sprung" der ihr gegenüberstehenden Realität der Sexualität, nachdem nach dem Maβ des Möglichen die Strukturen der Norm des Modells erfabt wurden. Unter der Dynamik der Freiheit verfeinert sich das Modell und formt sich bei jeder sittlichen Tat weiter aus. Wie diese schöpferische Umformung des Modells geschieht, lãβt sich vielleicht an folgendem Vergleich erläutern,. Manche Kinderfibeln enthalten Bilder, auf denen ein Junge zu sehen ist, der ein Buch betrachtet. Die Seite, die dieser Junge aufgeschlagen vor sich hält, zeigt wiederum das gleiche Bild: einen Jungen, der ein Buch betrachtet usw. Auf einer einzigen Seite findet sich im unterschiedlichen Maβstab, Ausführlichkeit und Färbung das gleiche Bild. Seine deutlichste, farbenprächtigste und das Auge am stärksten beeindruckende Gestalt hat in der Nähe zum Betrachter, aber diese letzte Genauigkeit ist- wenn man sowie - erst das Ergebnis vieler anderer Studien des gleichen Grundrisses und der gleichen Form. Das Modell ist ein solch plastisches Gebilde, das sich im Laufe einer Handlungsgeschichte als Folge unendlich vieler Entwürfe im Raum der Freiheit und nach den Gesetzen der menschlichen Entwicklung immer mehr ausgewestaltet hat. Das gilt für alle Bereiche der Sexualität. Freiheit, ihr Erlebnis und ihre Wirklichkeitsbejahung ist damit ein dritter Schritt und eine dritte Möglichkeit auf dem Wege, die Norm zu finden und sie zu formulieren. Alle genannten Orientierungen auf die innere Gesetzlichkeit in der Form des Modells, Befragung der eigenen Verantwortung in der Gemeinschaft des Partners, bzw. der moralischen Gruppe, wo die Mehrzahl der Normen erworben konsolidiert und verändert wird, bzw. in der Gesamtgesellschaf; Erforschungde, verbreiteteten Sexualsymbole und ihre Prüfung auf die Fähigkeit, menschliches Potential freizusetzen und die Selbsterfahrung von Freiheit sind aus dem Aspekt der Norm abgeleitet, der Behauptung besagt.

BIBLIOGRAPHIE

1. ALMADA, Fernando. *Frankensteen: retalhos da adolescência*. São Paulo: Moderna, 1996. 112 p.
2. ARATANGY, Lídia Rosenberg. *Sexualidade: a difícil arte do encontro*. São Paulo: Atica, 1995. 159 p.
3. AZEVEDO, Guila. *Adolescência.* São Paulo: Scipione, 1995. 71 p.
4. BARRETO, Ozana. *Adolescentes: aprenda a falar com eles, jogando com as palavras: dicionário do adolescente*. Salvador: Universitária Americana, 1993. 93 p.
5. BARROSO, Carmem et al. *Gravidez na adolescência*. Brasília: IPLAN/IPEA, 1986. 135 p. (Serie Instrumentos para a Ação, 6).

6. BOLOGNA, José Ernesto. *Estação desembarque: referencias existenciais para o jovem contemporâneo.* São Paulo: Aquariana, 1992. 350 p.
7. CHALITA, Gabriel (org.). *Vida para sempre jovem*. São Paulo: Siciliano, 1992. 166 p.
8. COATES, Verônica; FRANCOSO, Lucimar A.; BEZNOS, Geni Worcman. *Medicina do adolescente*. São Paulo: Sarvier, 1993. 525 p.
9. Comissao de saude do adolescente. *Adolescência e saúde. vol. 1*. São Paulo: Secretaria de Estado da Saúde, 1988. 210 p.
10. Comissao de Saude do Adolescente. *Adolescência e saúde. vol. 2*. São Paulo: Secretaria de Estado da Saúde, 1994. 93 p.
11. CONFORTO, Maria Thereza Alves. *Saúde sexual e reprodutiva na adolescência: o desafio de institucionalizar ações na saúde e na educação*. Brasília: Rumo, 1998. 73 p.
12. Consejo Nacional de Poblacion. *Sexualidad adolescente*. México: Foc, 1994. 40 p.
13. COSTA, Moacir. *Sexualidade na adolescência*. 11 ed. Porto Alegre: L&PM, 1997. 186 p.
14. CAVIEDES, Miguel. *Sexo e amor*. São Paulo: Paulinas, 1984. 166 p.
15. CHARBONNEAU, Paul-Eugene. *Adolescência e sexualidade*. São Paulo: Paulinas, 1987. 119 p.
16. CHARBONNEAU, Paul-Eugene. *Namoro e virgindade*. São Paulo: Moderna, 1985. 54 p.
17. COATES, Anne. *Gravidez*. São Paulo: Moderna, 1994. 47 p.
18. COLEMAN, John. *Emoções e sentimentos*. São Paulo: Moderna, 1994. 46 p.
19. COLEMAN, John. *Familia e amigos*. São Paulo: Moderna, 1994. 46 p.
20. COSTA, Cristina. *Caminhando contra o vento: uma adolescente dos anos 60*. São Paulo: Moderna, 1995. 126 p.
21. COSTA, Cristina. *Os grilos da galera: as questões da adolescência*. São Paulo: Moderna, 1996. 143 p.
22. DOLTO, Françoise. *A causa dos adolescentes*. 2 ed. Rio de Janeiro: Nova Fronteira, 1990. 289 p.
23. DURAN, Carlos Joaquin. *Meninas e rapazes*. São Paulo: Paulinas, 1983. 102 p.
24. ECOS, SCHERING, MARINHO, Fundação Roberto. *Sexualidade, prazer em conhecer*. São Paulo: Ecos. 2001.
25. EGYPTO, Antonio Carlos. *Sexo, Prazeres e Riscos*. São Paulo: Saraiva. 2005.
26. FERRARI, Armando B. *Adolescência, o segundo desafio: considerações psicanalíticas.* São Paulo: Casa do Psicólogo, 1996. 228 p.
27. GALLATIN, Judith E. *adolescência e individualidade: uma abordagem conceitual da psicologia da adolescência*. São Paulo: Harbra, 1978. 397 p.
28. GEILING, Katia. *Essa tal primeira vez.* São Paulo: Moderna, 1995. 118 p.
29. GEWANDSZNAJDER, Fernando. *Sexo e reprodução*. São Paulo: Atica, 1993. 56 p.
30. GIKOVATE, Flavio. *Namoro: relação de amor e sexo*. São Paulo: Moderna, 1993. 86 p.
31. GREEN, Christine. *Descoberta do sexo*.. São Paulo: Moderna, 1994. 48 p.
32. GREEN, Christine. *Mudanças no corpo*. São Paulo: Moderna, 1994. 48 p.
33. HACKER, Sylvia. *What every teenager really wants to know about sex: with the startling new information every parent should read*. New York: Carrol & Graf Publishers, (s.d.). 123 p.
34. HARRISON, Michelle. *O primeiro livro do adolescente sobre amor, sexo e Aids*. Porto Alegre: Artes Médicas, 1996. 107 p.

35. HENRIQUES, Maria Helena et al. *Adolescentes de hoje, pais do amanha: Brasil.* Bogotá: Editorial Presencia, 1989. 88 p.
36. KNOBEL, Mauricio; ABERASTURY, Arminda. *Adolescência normal: um enfoque psicanalítico*. 10 ed. Porto Alegre: Artes Médicas, 1981. 92 p.
37. LEVI, Giovanni; SCHIMITT, Jean-Claude (org.). *Historia dos jovens: da Antiguidade a Era Moderna*. vol. 1. São Paulo: Companhia das Letras, 1996. 372 p.
38. LEVI, Giovanni; SCHMITT, Jean-Claude (org.). *Historia dos jovens: a época contemporânea*. vol. 2. São Paulo: Companhia das Letras, 1996. 382 p.
39. LEVISKY, David Leo (org.). *Adolescência: pelos caminhos da violência: a psicanálise na pratica social*. São Paulo: Casa do psicólogo, 1998. 188 p.
40. LEVISKY, David Leo. *Adolescência: reflexões psicanalíticas*. 2 ed. são Paulo: Casa do psicólogo, 1998. 316 p.
41. MADDALENO, Matilde et al. *La salud del adolescente y del joven*. Washington: OPS-Organizacion Panamericana de la Salud, 1995. 572 p.
42. MADARAS, Lynda; MADARAS, Area. *Meu corpo, eu*. São Paulo: Marco Zero, 1995. 119 p.
43. MADARAS, Lynda; MADARAS, Area. *Meus sentimentos, eu*. São Paulo: Marco Zero, 1996. 159 p.
44. MAYLE, Peter; ROBINS, Arthur; WALTER, Paul. *O que está acontecendo comigo: guia para a puberdade, com respostas as perguntas mais embaraçosas*.. São Paulo: Nobel, 1984. 55 p.
45. MELLO, Anna Christina Cardoso de. *O jovem e seus direitos*. São Paulo: Moderna, 1997. 158 p.
46. MULLINAR, Gill. *Dicionário de orientação sexual para adolescentes*. São Paulo: Melhoramentos, 1993. 123 p.
47. PANTELIDES, Edith Alejandra. *Conducta reproductiva y embarazo en la adolescencia*. 2 ed. Buenos Aires: Centro de Estudios de Poblacion - CENEP, 1980. 110 p.
48. Pernambuco. Secretaria de Educacao, Cultura e Esportes. *Gravidez na adolescência: projeto de educação sexual para a comunidade escolar: I ciclo de estudos.* Recife: Sece, 1993. 80 p.
49. PEROSA, Miguel. *Descobrindo a si mesmo: a passagem para a adolescência*. São Paulo: Moderna, 1995. 136 p.
50. PICAZIO, Cláudio. *Diferentes desejos: adolescentes homo, bi e heterossexuais*. são Paulo: Summus, 1998. 165 p. (Edicoes GLS).
51. RAPPAPORT, Clara. *Encarando a adolescência*. São Paulo: Atica, 1995. 119 p.
52. Revista Capricho. *Capricho especial: 20 depoimentos*. São Paulo: Abril, (s.d.). 82 p.
53. RUBIN, Isadore; KIRKENDALL, Lester A. *Sexo e adolescência: novas orientações para o ensino da juventude*. São Paulo: Cultrix, 1970. 261 p.
54. Sayao, Rosely. *Sexo.* São Paulo: Escuta, 1998. 104 p.
55. SAYAO, Rosely. *Sexo é sexo*. São Paulo: Companhia das Letras, 1997. 188 p.
56. SAYAO, Rosely. *Sexo, prazer em conhece-lo*. Ilustrações de Angeli. Porto Alegre: Artes e Ofícios, 1995. 128 p.
57. SOUZA, Halia P. *Convivendo com seu sexo: adolescentes e jovens*. São Paulo: Paulinas, 102 p.
58. SOUZA, Halia P. *Convivendo com seu sexo: pré-adolescent***e**. São Paulo: Paulinas, 1984. 48 p.
59. SUPLICY, Marta. *Sexo para adolescentes: amor, puberdade, masturbação, homossexualidade, anticoncepção, DST/Aids, drogas*. 2.ed. são Paulo: FTD, 1998. 160 p.
60. SINGH, Susheela; WULF, Deirdre. *Adolescentes de hoy, padres del manana: um perfil de las Americas.* Bogotá: The Alan Guttmacher Institute, 1989. 96 p.

61. SUPLICY, Marta. *Sexo para adolescentes: orientação para educadores*. São Paulo: FTD, 1989. 55 p.
62. TAKIUTI, Albertina. *A adolescente esta ligeiramente grávida. E agora? Gravidez na adolescência*. São Paulo: Iglu, 1990. 118 p.
63. TAPAJOS, Lais. *Desencana que a vida engana: verdades e mentiras sobre a adolescência*. São Paulo: Globo, 1995. 104 p.
64. The Life Cycle Library. *Your first pregnancy: for the young woman who's contemplating or expecting a baby.*Life Cycle Center, 1970. 45 p.
65. TIBA, Icami. *Adolescência, o despertar do sexo: um guia para entender o desenvolvimento sexual e afetivo das novas gerações*. 4 ed. são Paulo: Gente, 1994. 130 p.
66. TIBA, Icami. *Puberdade e adolescência: desenvolvimento biopsicossocial*. 4 ed. são Paulo: Agora, 1986. 236 p.
67. TIBA, Icami. *Sexo e adolescência*. 7 ed. são Paulo: Atica, 1993. 96 p.
68. VASCONCELOS, Naumi de. *Amor e sexo na adolescência*. São Paulo: Moderna, 1985. 62 p.
69. VEIGA, Francisco Daudt da. *O aprendiz do desejo: a adolescência pela vida afora*. São Paulo: Companhia das Letras, 1997. 222 p.
70. WARREN, Andrea. *Everybody's doing it: how to survive your teenagers' sex life (and help them survive it, too)*. New York: Penguin Books, 1993. 234 p.
71. WEISS, Susan Pick de; VARGAS-TRUJILLO, Elvia. *Yo adolescente: respuestas claras a mis grandes dudas*. México: Limusa-Grupo Noriega, 1992. 216 p. (Serie Planeando tu vida).
72. WUSSTHOF, Roberto. *Descobrir o sexo*. São Paulo: Atica, 1994. 144 p.
73. ZABIN, Laurie Schwab; HIRSCH, Marilyn B. *Evaluation of pregnancy prevention: programs in the school context*. Lexington: Lexington Books, 1988. 168 p.
74. ZAGURY, Tania. *O adolescente por ele mesmo: orientação para pais e educadores*. 5 ed. Rio de Janeiro: Record, 1996. 277 p.

Prosopon
Europejskie Studia Społeczno-Humanistyczne

Wydawca / Publisher:
Instytut Studiów
Międzynarodowych
i Edukacji HUMANUM
www.humanum.org.pl

12 (3) 2015
ISSN 1730–0266

Ramirus Delius Borges Meneses
Catholica Universitate Lusitaniae – Bracarensis
Philosophiae Facultas, Portugal
E-mail: borges272@gmail.com

Physicae motus: de essentia ad esse / *Physical movement, to be of the essence*

Abstract
The science of mechanics seeks to provide a precise and consistent description of the dynamics of particles and systems of particles. That is, a set of physical laws mathematically describing the space, time, and motions of bodies. According to this philosophical idea, we need certain fundamental concepts such as distance and time, because your philosophical foundations. Meanwhile, the combination of the concepts of distance and time allows us to define the velocity and acceleration of a particle, and carries up a very new philosophical formulation by the Newtonian mechanics.

Key words: **Mechanic motion, space, time, and the mobile being, and nature and sense.**

INTRODUCTIO

Mechanicus Motus estne omnis relativus motus vel datur absolutum. Verumtamen duo sensus necessaria secundum relativum et metrice externo factus sit.

Sub duplo sensu, motus restritum et generalisatum appelatur. In primo, mechanicus motus seu localis momentum mobilis subjecti est, de initiali termino ad finali momento. Relate ad alium mobilis quicumque ens vel corpus physicum, qui in spatio et tempore distinguere positionem possumus, habetur. In secundo verbo, motus quemlibet substantialem mutationem seu accidentalem significat. Verumtamen, quivis formae motus definient, sicut mechanicus, ondulatorius, et cetera.

Quid fieri in spatio et tempore est ? Motus analysis, sicut purus phenomenus *per se*, ad physicam (relativisticam, quanticam et reliqua).

Apud axiomaticum mechanicae systema (cynematicae et dinamicae), philosophiam radicem motus instituere, sicut possibilis motus phaenomenum oportet et eius generalis lex.

Secundum motus, cuius suum conceptum a lege generali fundatur:

$$v = \frac{e}{t};\ \vec{v}(t_1) = \lim_{t_2 \to t_1} \frac{\vec{r}(t_2) - \vec{r}(t_1)}{t_2 - t_1} = \frac{d\vec{r}}{dt} = d\vec{r}\ ^{1}$$

seu:

$$E = v \cdot f(T).$$

Proprie corporis de uno loco ad alium locum seu motus localis transitus.

Sed et proprie moveri, dunc taxat quod secundum movetur locum, dicimus.

Autem localis motus duplex est, prout mutatio, tantum in loco et proprie localis est, sicut fit, aut simul in qualitate et alteratio vocatur. Tunc in quantitate, ut augmentatio et diminutio sunt; tunc in substantiale esse et generationem habet. Revera locales motus nom solum loci mutationes, sed etiam substantiarum qualitatum, producunt, uno et quantitates, ut, in vibrationibus molecullariis, quae calorem et, mediante eo, corpurum dilatationem tulerunt.

Quidem motus actum seu aliquid positivum esse, nam moveri modus realis entis est. Naturaliter quod enim movetur, in via ad actum perfectum est, qui tamem non nisi in motus termino obtinetur.

Hinc etianisi potentiae actus ut sic se evolutio potentiae nondum absoluta, sed in via et tendentia ad terminum dicitur.[2]

Quapropter quoad ad motum tria momenta, spatium, tempus et velocitas spectant.

Formaliter autem motus in ipsomet actu acquisitionis consistit.

Vero haec acquisitio medium tenet inter duo extrema, quae duo termini motus sunt, nemque principium *a quo* mobile moveri incipit, et terminus *ad quem* seu in quo sistitur. In hoc articulo explanare volumus relativi et absoluti motus naturam sensumque.

1 - Apud Selvaggi notionem motus localis formaliter in sola successiva praesentia in diversis locis consistit, ut motus ad seriem stationum referatur. Sed ipsa progressio seu transitus ab uno in alium locum facta est et aliquis fleuns et suceessivus (tempus) contactus cum extenso continuo in quo motus fiet. Naturaliter haec aliqua variatio realis est, quamvis moto corpori non intrínseca, sed scilicet ei extrinsecam esse. Igitur, motus localis reponendus in aliqua qualitate vel intrinseco facto, non videtur, quamvis verumtamen multipliciter qualitativas

1 Cf. C. GERTHSEN; KNESER; H. VOGEL – *Física*, tradução do alemão por A. A. Inocêncio e M. A. A. M. Inocêncio, Fundação Caloust Gulbenkian, Lisboa, 9-10.
2 Cf. P. HOENEN – *Cosmologia*, Apud Aedes Universitatis Gregorianae, Romae, 16-38.

notiones implicet.[3] Motus cynematicus non est localis motus. Hic est realis sed cynematicus phaenomenus sensibile quod ex positionis corporum in spatio et tempore percipimus. Nam motus universalis lex mechanici per definitionem operativam exprimitur, id est, per cynematicae fundamentalem aequationem :

$$ds = v \cdot dt; \qquad ds/dt = v\,.^{4}$$

Sic velocitas cuiuslibet corporis mobilis in instante (t_1) est functionis derivatae valor legitur $f(t)\,d \quad t = t_1$.

Haec esse constans (numerus scalaris) vel variabilis sicut vectorialis magnitudo ex motibus potest et ut sic acceleratio:

$$a = dv/dt\,.^{5}$$

Motus cynematicus seu mechanicus continua et relativa mobilis in spatio et tempore variatio.

Generalis motus lex structuram seu formam patefacit, sicut :

$$e = v \cdot f(t).$$

Apud differentialem formam habemus:

$$\vec{v} = d\vec{r}/dt$$

Quia: $d\vec{r} = dxi + dxj + dxk$.

Atqui funtionem spatium temporis variabilis esse ubi velocitatem secundum vectorialem motus essentiam habemus. Motus instantanea velocitas aequalis ad spatii derivatam a relatione temporis. Haec metrica relatio transitum fert sive movetur sive hic et nunc. Idcirco eius valor ratio inter infinitesimum spatium ($\lim de \to 0$ = punctus) e tempus infinitesimum ($\lim de \to 0$ = instans).

Apud experientiae generalizatam inductionem ex particularis motibus seu mobilium entium. De motu constante et uniformi relatione inter phaenomeni dimensiones loquimur: spatium, tempus e velocitas, quae eius intensivam variationem refert. Nam, mobile ens in reali spatio-tempore ostenditur et continua sucessio "moveturs" factura erit. Hic et nunc cinematicam lineam suponit, quae in reali spatio est et ab abstractione infertur. Haec est generalis lex, quae dynamicam relationem et constantem particularium motus ostendebit. Motus ergo relatio variabilis inter spatium et tempus est. Igitur motus perfectionis forma seu imperfectus actus complexa esset, quia a tribus componentis induitur, hoc est: spatium, tempus et velocitas.[6]

3 Cf. Ph. SELVAGGI – *Filosofia do Mundo*, Universidade Gregoriana, Roma / S. Paulo, 1988, 62-74.
4 Cf. W. G. McLEAN; E. W. NELSON – *Mecânica*, traduzido por Humberto César T. Gonçalves, Mc Graw Hill, S. Paulo, 1980, 31-311.
5 Cf. S. T. THORNTON; J. B. MARION – *Classical Dynamics of particles and systems*, fifth edition, Thomson Brooks / Cole Belmont, 2004, 49-51.
6 Cf. MARIA AMELIA CUTILEIRO INDIAS – *Curso de Física*, S. Paulo, Mc Graw Hill, 1992, 13-14.

$$M = f(e,t,v).$$

Cum spatium et tempus scalares dimensiones sint, seu motus numeri, qui quantitativas dimensiones (hic et nunc) ad motum oblaturi essent.

Verumtamen velocitas vectorialis dimensio sit, quam variationem seu qualitativam dimensionem ad motum dare. Secundum analyticam geometriam, mathematica functio a cinemática línea seu vectore repraesentanda apud planum erit:

$$O(x,y);\ \vec{e} = \vec{v} \cdot f(t).$$[7]

Et quoque Gaussii complexum planum habemus spatium sicut realem numerum et imaginariam partem sicut vectorem: $\vec{v}$. Motus mathematice punctorum et momentorum transfinitum coniugatio appelatum esset, sicut acto-potencialis. Continuitas a cortis notionibus seu limites: $\vec{v} = (P - I) \leftrightarrow C$, sed motus erit relativitas realis et métrica, probandus sit. Etenim cinematicus motus ad spatialem lineam in tempore vectorialiter fundat secundum Classicam Mechanicam.

Classica Physica mathematicum et philosophum motus legem, ut cynematicam variationem spatii et temporis scientia definit, nunc et semper docebit.

Motus causalitas a generali lege definire potest et eius mathematica formulatio est secundum classicam mechanicam:

$$e = v \cdot f(t)$$

et in differentiali locutione erit:

$$\vec{v} = d\vec{e}/dt\ .$$

Etenim spatium et tempus variabile functionem leguntur et a velocitate vectore multiplicatur, cum instantanea motus velocitas spatii derivatam temporis relate sit. Si causalitatis ratio vis sit, tunc esset motus quantitas a temporis variatione:

$$\vec{F} = m \cdot \vec{a}$$

quae est differentialis variatio:

$$\vec{F} = d\vec{p}/dt = d\left(m \cdot \vec{v}\right)/dt = m \cdot d\vec{v}/dt = m \cdot d \cdot \vec{a} = m \cdot \vec{a}$$

$$\boxed{\vec{F} = m \cdot \vec{a}}$$ [8]

Atqui, secundum Selvaggi[9], «quod in motu est, est aliquo modo perfectum et determinatum. Ergo quod in motu sit, potentia erit, nec in potentia in quantum actus est; sed erit actus, in quantum est in actu, et est in potentia, in quantum

7 Cf. LARSON, R.; HOSTETLER, B. H. EDWARDS – *Cálculo*, Volume 1, 8ª edição, tradução e revisão técnica de Helena Maria de Ávila Castro e Leila Maria Vasconcellos Figueiredo, Mc Graw Hill, S. Paulo, 2006, 111.

8 Cf. A. P. BORESI; R. J. SCHMIDT – *Dinâmica*, tradução de J. Pinheiro Nunes da Silva, Thomson, S. Paulo, 2003, 125-126.

9 Cf. Ph. SELVAGGI – *Filosofia do Mundo*, 1988, pp 75-77.

est potentia ad actuationem ulteriurem, seu actus existentis in actu est et simul erit. Motus potentiam existentis in potentia factus est . E contra, motus actus qui, in quantum tale et necessario, est, dicit ordinem ad ulteriorem actuationem et proinde, in quantum tale, est in potentia, tota sua realitate et actus naturaliter est et est in potentia, quia quod movetur, essentialiter movebatur et movebitur, ac proinde existentis in potentia actus esset, secundum quod huiusmodi.[10]

Motus existentis actus est, Selvaggi ait: "motus enim non est perfectio pura, actus subsistens, sed perfectio est et determinatio alicuius subiecti existentis, per quam subiectum est in via ad aliquod novum esse, quod prius non habebat. Ergo motus ex duplici capite dicit ordinem ad esse: in quantum est in ente, ut in subiecto, et in quantum tendit ad esse aliquod producendum. Si autem motus purum fieri esset, cessante motu, iam nihil superesset; et si non tenderet ad aliquod esse permanens in subiecto producendum, cessante motu, iam subiectum non esset mutatum, sed esset in eodem statu, in quo ante motum erat".Essentialiter actum existentis in potentia prout in potentia motus patefacit et forte iam mutatum est, seu est in termino ad quem motus, sed non movetur. Verumtamen, actus motus est, qui natura sua subiectum, in potentia ad ulteriorem actuationem in eadem linea relinquit, quia quod movetur omne, necessario movebitur.

2.1 - Etenim, linearis motus repraesentari in plano ideali duorum dimensionum seu in spatio tempore schemate potest sicut aequationem dicit: $s = f(t)$ secundum verum planum $P(s,t)$. Mobile figuratum per punctum et motus per curvam et figura pendularis motus sinusoidalem ostendetur.[11] Si planaris motus in spatio ideali trium dimensionum repraesentari potest secundum duo spatiales et unum temporale sint, tunc aequatio $y = f(x,t)$ facta est.[12] Punctum mobile $p(x,y,t)$ n-circunferentiae successivas in plano, sed cum motus etiam fiat in tempore, describit, ac si figuram helycoidalem in spatio-tempore trium dimensionum secundum geometriam et cynematicam ostendebat.

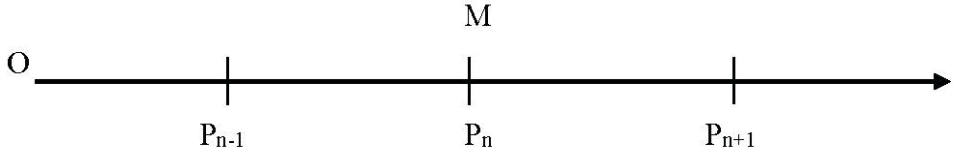
Per punctorum axium, quae momenta iuxtaposta sunt, tempus successivum est, sive spatializatur sive figuratur.[13]

Sic in spatio trium dimensionum motus repraesentari analytice in hyperspatio ideali quatuorum dimensionum (quae tres spatiales et una temporalis) secundum aequationem: $y = f(x,y,z,t)$ motus patefactus erit. Sed non intuitive figuram huius motus, sicut aeronavis vel astronautae capsae a valantis dictum est in spatio-tempore, imaginare possumus.[14] Ut synthesis progressiva actus in potentia motus, quia non est potentia pura nec actus purus, sit. Si potentia pura, tunc subiectum motus possibilis factum est in termino a quo seu indeterminatum ad motum, esset. Si tamen purus actus, tunc motus possibilis subiectum iam in termino ad quem

10 Cf. Ph. SELVAGGI – *Cosmologia*, 1962, 89.
11 Cf. A. FONSECA – *Curso de Mecânica: Dinâmica*, Volume III, Livros Técnicos e Científicos, Editora S.A., Rio de Janeiro, 1975, 171-172.
12 Cf. *Idem, Ibidem*, 190-196.
13 Cf. JAIME ARAÚJO MOREIRA – *Física Básica, para aplicações médicas e biológicas*, Fundação Calouste Gulbenkian, Lisboa, 1971, 117-119.
14 Cf. B. RICH; Ph. A. SCHMIDT – *Geometria*, tradução e revisão técnica por A. Monteiro, Mc Graw Hill, Lisboa, 2001, 1-17.

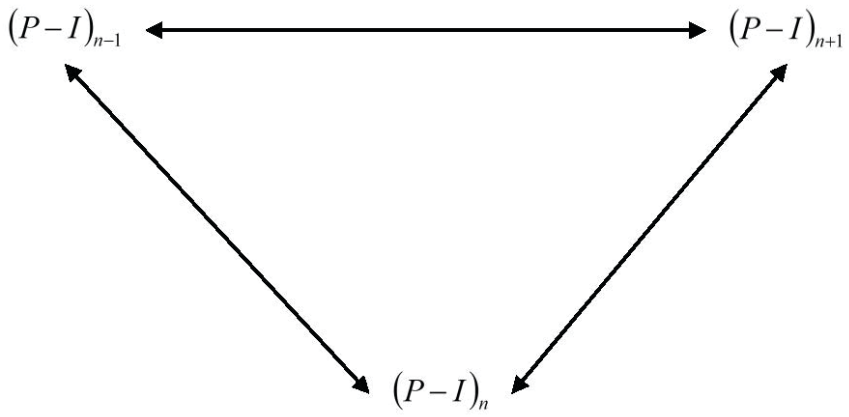
seu determinaretur non naturaliter, esset. Ergo motus aspectum etiam absolutum corpora ut mobília habet. Cum omnia corpora in motu universali, si corpus relative est imobile, habet tamen iam motus intensitatem facturus est (in potentia movebatur) et aliquis influxus cyneticae energiae sufficit ut transead ad novum motum particularem ipsum, sint.[15]

2.2 – Etiam motus relativitas metrica e ontologica esse potest e metricae relativitatis seu gnoseologicae a physicis resolvitur. In cynematica classica, relativitatis principium Galilaicae vel Newton ad rectilineum experientiae et phaenomena restringitur. Ex experimentis realizatis intus systemates seu dominii $O(x, y, z, t)$ nullum phaenomenum mechanicum internum, utrum hoc systema absolute imobile in spatio sit vel in motu rectilineo uniformi transferatur, nobis revelare potest.[16] Tantum scire potest physicus eius systema et aliud extrinsecum seu corpora esse in motu relativo seu reciproco. Etenim ad metricum calculum idem est. Si physicus clausus est intus currus ferroviarii nescit utrum ipse $O(x, y, z, t)$ moveatur vel alius currus parallelus $O'(x', y', z', t)$ sit. Etiam translationis motus relativus ad Solem spectat. Consequentur continuus motus fluens utpote seu imperfectus actus non divisibile in infinitum est. Ac tamen qui contrarium arbitrantur. Sed solus numerus motus realis seu tempus, ut per imaginem extensionis dinamicae quantificatus quae in memoria permanet, divisibilis analogicae est, id est, 90 gradum motus seu 15 minutorum angulo spatiali vel arcui correspondet, quem horologii stillus describit. Atqui numerus ordinalis 90 collectionis continuae elementum factus est numerorum realium: $(R) \leftrightarrow (P)$.[17] Motus seu in spatio varians existere necessario "esse ad" sicut cynematicam relationem esse. Ergo relatio ontologica relatio seu realis erit. Sed motus relativitas multipla est. Ut corpus M mobile in puncto P referri necessario ac simul ad punctum prius P_{n-1} et punctum posterius P_{n+1} realis extensionis sit, vel ad observatorum $O(x_3, t)$ erit:



Alia ontologica relativitas fundatur et ab activitate causali reciproca corporum oritur, sed nullum corpus concipi potest vel postulari ut imobile absolute. Et ex gravitationis universalis lege probatur. Ratio dialectica in motu arithmeticam formulationem ostendebit:

15 Cf. A. EINSTEIN – *O Significado da Relatividade*, tradução do Prof. Mário Silva, Gradiva, Lisboa, 2003, 54-55.
16 Cf. F. W. SEARS – *Física – Mecânica – Calor – Acústica*, tradução por José Cruz dos Santos, Editora Gertum Carneiro, Rio de Janeiro, 1953, 212-214.
17 Cf. J. MANUEL RESINA RODRIGUES – *Introdução à Teoria da Relatividade Restrita*, JST Press, Lisboa, 1998, 8-9.



Motus relationem cynematicam invariabilium mechanicarum inter punctum (e) et instantem (t) apud velocitatem et a vectorialem variationem datus motus est.[18]

Ergo singularis motus ut effectus alicuius extrinsicae activitatis vel intrinsicae praeferret. Curus ex energia cynetica molecularum, quae communicata a motore est: $W = 1/2\, m \cdot v^2$ .Radioactiva particula vel electromagnticus campus spontanee e se movetur.[19]

Sed solum aspectum absolutum aristotelica motus definitio, quia actus in potentia inquantum in potentia motus est. Est generica seu categorialis, quia actus imperfectus seu progressivus et continuus non declarat de qua perfectione specifica agitur, scilicet de spatiali relatione. Etiam intensiva mutatio qualitatum corporis. Sed naturaliter continua et relativa variatio corporum in spatio motus est, si verificant. Hae conditiones sunt dynamica ratio momentorum in potentia si necessario ad aliud punctum P_{n+1} refertur spatii vel observatorum $O(x,z,t)$ .Quia corpus, ut mobile, momentum "movetur" est, quod simul unus idemque momenti prioribus (movebatur) et momenti posterioris (movebitur), quae partes sunt in potentia in potentia. Etenim motus mechanici perceptio relationem ordinis spatialis inter positionum priorem mobilis et positionem posteriorem implicat.[20] Datur series sucessiva positionum varialilium. Sed hic ordo dynamicus variatio continua ex correspondentia biunivoca cum spatiali continuo lineari est.

Nam mobile corpus M non pertransire non punctum P_n tangentiae potest, nisi antea per punctum quam maxime vicinissimum P_{n-1} pertranseat. Idemque relate posterius ad punctum P_{n+1}. Sed haec puncta continua sunt in spatii linearis potentia. Ergo et ipsa momenta motus qui dimentio dynamica connexa est.Si motus obiective discontinnus seu densus inter duo momenta esset, tunc series transituum infinita seu quantorum variationis sequeretur. Atqui hoc impossibile est, quia si mobile

18 Cf. N. M. M. MAIA – *Introdução à Dinâmica Analítica*, JST Press, Lisboa, 2000, 5-10.
19 Cf. S. M. MENDIRATTA – *Introdução ao Electromagnetismo*, Fundação Calouste Gulbenkian, Lisboa, 1995, 287-289.
20 Cf. V. MENDES DE SOUSA ALVES – *Ensaio de Filosofia das Ciências*, Publicações da Faculdade de Filosofia, Braga, 1992 , pp. 234-342 .

inter duo puncta spatii salit, quantiumvis distantia infinitessimalis sit, iam motus saltus fit qui necessario continuus est. Ergo motus linea variatio continua est.

Quia si corpus spatialiter in aliquo puncto P_n alterius realis extensionis non potest mobile vel affirmari in motu existit, nisi hanc relationem positionis $\underline{OP_n}$ et occupet novum punctum P_{n+1} seu novam relationem variabilis distantiae OP_{n+1} et OP_n relinquat.Alia generalis relativitatis motuum ut iam declaratum est ex universalis gravitationis lege sequitur. Nam relativorum motuum systema qui intus riemannianae sphaerae Universi eveniunt naturaliter datur:

$$ds^2 = g_{ik} \cdot dx_i \cdot dx_k .^{21}$$

Etenim, mechanicus motus transitus progressivus et continuus corporis in spatio, tempore et velocitate est, cum operativa definitio motus quae ex scientifica analysi iam inferitur scilicet explicata sit. Nunc mobile corpus influxum cyneticae energiae et dicit relationem novam positionis spatio-tempore quae facere est proprium spatialiter patitur.

Etenim ex moleculari et atomica structura continuum formale corpus non est, sed solum virtualem esse. Ergo et motus propter biunivocam correspondentiam esse continuum formale non potest. Motus, ut abstractum conceptus, in spatio continuo formali non datur, sed singularis motus, si est totalis effectus ex molecularum motibus, virtuale continuum fundatum in continuo formali mobilis particulae erit.

Verumtamen systema unum corpus per accidens sed relate ad sensuum perceptionem movetur, ut esset unum per se sit. Motus totalis ex synthesi motum singularium collisionis molecularum, quae ligantur inter se in totius unitate, resultat.

Tantum continuum formale motus, ubi datur extensio realis continua formalis atqui hoc solum in quantis minimis verificatur extensis, praelaturum erit. Sed Universi theoria expansionis, quod extensus sphaerae totalis extra se moveatur, relate ad nihili punctum sequitur. Haec referentia pure imaginariam facta esset, quia Universi motus realis semper est.[22]

2.3 – A mobilibus entibus motus fundatur sicut motus phaenomenus possibilis est. In abracta ordine, mathematica functio dynamicae motus legis rationis entem significat sicut reale fundamentum, quia a physico-mathematica definitione relationem inter abstractas variables habemus, sicut: e, t et $\vec{v}$. In reali ordine, motus seu eius dynamica lex acto-potentialis est, id est, mobilis subiecte imperfectus. Motum in potentia existentis actum esse, nam quod totaliter in actu est, nam quod totaliter in actu sit, iam perfectum esset; forte iam mutatum est, seu in termino ad quem motus esset, sed non movetur. Aliis verbis, motus est actus

21 Cf. H. A. LORENTZ; A. EINSTEIN; H. MINKOWSKI – *O Princípio da Relatividade*, tradução do inglês de Mário José Saraiva ,Volume I, Fundação Calouste Gulbenkian, Lisboa, 2001, 243-250.

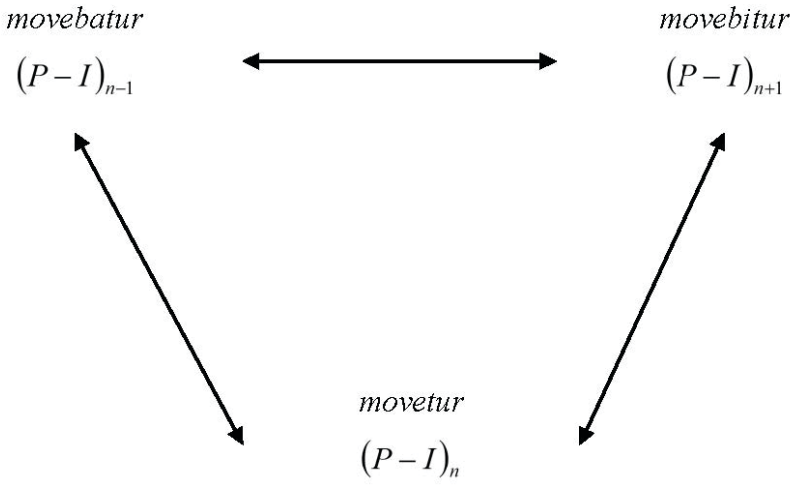
22 Cf. B. GREENE – *The Fabric of the Cosmos*, Penguin Books, London, 2004, 72-76.

imperfectus, qui medio modo se habet inter puram potentiam et actum perfectum, quod quidem partim in actu et partim in potentia erit.

Definitionis ab analysi, motus continuum et successivum transitum mobilis de $(P-I)_{n-1}$ ad $(P-I)_{n+1}$ fieri spatio-temporalis seu progressiva formulatio secundum $(P-I)_{n-1}$ et non existire in $(P-I)_{n+1}$, quia relate in $(P-I)_n$ est.

Motus synthesim inter "existere in" et non "existere in". Tunc "existere in" est esse in actu, et non existire non esse in potentia esset. Ergo, motus imperfectus seu acto-potencialis est.[23]. Igitur, Motus, cum via ad terminum ex sua essentia sit, suam unitatem et specificationem ex termino esse, sic terminus motus, qui ultimum in executione esse, etiam eius principium determinans in intentione ostendet, eius finis, qui veram causalitatem in motum exercet. Hoc etiam in motu simplicissimo et magis elementari in locali motu verificatur, in quo tamen non est in naturali loco reponendus est, ut Aristoteles putabat, sed in directione ipsa ab impressa agente quae motum specificat et in inertiali motu de se indefinite conservatur et indefinite prosequitur. Finalitatem motus localis et omnis physici motus magis expresse in ultima parte tractatus considerabimus.

Verumtamen motus phaenomenus vel perfectus actus vel pura potentia sicut potentiae et actus synthesis est. Si motus perfectus actus esset, tunc mobilis iam in finali termino (limite). Ergo non motum habeatur. Si potentia pura esset, tunc mobilis in initiali termino erit (realizabilis). Ergo motum non habemus. Idcirco motus synthesim inter actum et potentiam abfers, id est dialectice:



Et non sub eodem aspectu, quia in hoc momento "movetur" (hic-nunc) seu $(P-I)_n$, tempus semper differens. Non solum adequatus mobilis instans, sed etiam momentum obsrvationis metricae. Mobilis non est solum in spatii punctu, sed in punctu-instante, sed semper variabilis est. Atqui correlatio actus et potentia antinomica non est, quia actus et potentia contraditoria non erit, sed solum

23 Cf. Ph. SELVAGGI – *Cosmologia*, 1962, 84-86.

contraria, cum esse principia de complementaritate sint. Ergo motus inteligibilem esse. Motus cynematicus, et consequenter alii, essentialiter continui motus erant, ut in instanti seu totaliter simul fieri nequeunt, sed necessario sucessionem non solum terminorum requirunt, sed etiam ipsius motus partium. Si motus cynematicus totus esset simul in instanti, in eodem instanti corpus simul in duobus locis esset distinctis, scilicet in "termino a quo" et in "termino ad quem" referatur, quod impossibile est.[24] Si autem non est simul in duobus locis, est successivam in illis in diversis instantibus et quia extensio, secundum quam cynematicum spatium fit et in tempore continuus erit. Secundum Selvaggi et omnes scholastici localis motus infinitam successionem partium importat, seu continuo fluens ab uno extremo in aliud erit.[25]

CONCLUSIO

De motu non solum primum gressum tractatus quo a mathematica ad physicam scientiam devenitur, sed etiam pars integrans, mechanicae est, quia tantum per motum natura et a nobis cognoscitur ac proinde tantum per motum suam intrinsecam perfectionem ontologicam et gnoseologicam agit et suam manifestationem extrinsecam attingimus, verum constituit. Etiam in nostra tractatione fuerat, in primis cynematicus motus, qui in suo formali aspectu solum quantitatem et corporum praesuponit et ex ipsa immediate sequitur, ita ut passio quantitatis dici potest. Sed haec consideratio non exclusive ad solum motum localem restringeretur, sed extendetur ad omnem motum in stricto sensu. Tamen ad proprietatis et relationis categoriam motus spectat, ut perfectionis forma, quia mobilis sequitur e relatione ad corpus aliud sicut referentialem systhemam.[26] Etiam causalis actionis effectus erit, transcendens ad mobilem subiectum. Sed ergo motum spatio-temporalem fieri, quia a activo ente faciendus est. Circa motum, in naturali philosophia, ut metaphysica cynematicae scientiae applicata, inquirendum primo est na sit motus, non quidem per modum in stricto sensu problematis, cum motus realitas sit ex primis et immediatis versitatibus, sed per declarativam et vindicativam certitudinis naturalis analysim.

Et secundo quid motus sit, et hoc iterum non per strictam definitionem, cum notio simplicissima sit, quae reduci ad communiores rationes nequit, sed per ontologicam analysim, illam resolvendo in analogam notionem entis, actus et potentiae.

***Synopsis**: Post analysim spatii iam logice sequetur problema de motu quia cogitari nec definiri potest nisi per ordinis spatialis perceptionem. Ut corpora mobile sit, esse prius quantum et variari in spatio debet, quia igitur est secunda proprietas cynematica corporum. Alioquin iam motus esse conceptum universalem probavimus et necessario cum conceptibus spatii et temporis connecti. Sed omnia corpora motum generalem elypticum relate ad sidus focum systhematis planetaris participant secundum legem gravitationis universalis.*

***Clavis-verba**: Motus cynematicus, spatium, tempus, et mobile ens, natura et sensus.*

24 Cf. P. HOENEN – *Cosmologia*, 13-23.
25 Cf. Ph. SELVAGGI – *Cosmologia*, 85.
26 Cf. Ph. SELVAGGI – *Cosmologia*, 79.

Prosopon
Europejskie Studia Społeczno-Humanistyczne

Wydawca / Publisher:
Instytut Studiów
Międzynarodowych
i Edukacji HUMANUM
www.humanum.org.pl

12 (3) 2015
ISSN 1730–0266

Łukasz Gomułka
Uniwersytet Opolski, Poland

Polimorfizm języka naturalnego a twierdzenia Kurta Gödla / *Natural language polymorphism and Kurt Gödel's theorem*

Abstract
The aim of this paper is to outline Stanisław Lem's (1921-2006) original views on Kurt Gödl's theorems. The project consists of five concise paragraphs in which such issues are discussed: the introduction with an explanation of selected terms: a natural language, polymorphism.
The author of the article presents a short outline of certain mathematical problems, that is the problems of arithmetics and the history of trying to prove its absolute non-contradiction. The author also includes Gödl's theorems into the greatest achievements of the scientific thought of 20th century (limitation theorems).
After that, epistemological questions of Kurt Gödl's theorems are introduced together with their original interpretation according to Stanisław Lem. The author of the paper emphasizes that this prominent philosopher and writer introduces cultural-linguistic interpretation of Gödl's discoveries, thus suggesting that a natural language overcomes 'Gödl-made abyss' thanks to its characteristic polymorphism.

Key words: **language, polymorphism.**

WPROWADZENIE

Celem pracy jest przybliżenie poglądów Stanisława Lema (1921-2006) dotyczących filozoficznych konsekwencji jakie można „wynieść" z twierdzeń Kurta Gödla (1906-1978).

Brakuje w literaturze krytycznej recepcji poglądów Stanisława Lema dotyczących filozoficznych (epistemologicznych) konsekwencji twierdzeń limitacyjnych; w szczególności twierdzeń Kurta Gödla. Należy zauważyć, że Lem wpisuje ewentualne konsekwencje twierdzeń matematycznych nie tyle do osiągnięć danych dyscyplin naukowych ale w szerszym ujęciu zalicza je do pewnych osiągnięć kulturowych w ogóle.

Na początku przybliżę pojęcia użyte w tytule niniejszego tekstu, a mianowicie: pojęcie języka naturalnego, polimorfizmu a następnie krótko scharakteryzujemy sytuację w jakiej znaleźli się matematycy i logicy na przełomie XIX i XX wieku oraz rolę jaką odegrał Kurt Gödel w rozwoju matematyki. Następnie opiszę przykłady rozumienia wniosków płynących z twierdzenia austriackiego matematyka w różnych dyscyplinach, po czym przedstawię Lemowską interpretację twierdzenia Gödla w odniesieniu do koncepcji polimorfizmu języka naturalnego.

Język naturalny rozumiany jest w tekście jako zbiór spontanicznie powstałych zwyczajów językowych ewoluujących w czasie. Język naturalny nie jest tworem człowieka, lecz jest tworem ewolucji, co oznacza, że w odróżnieniu od języków formalnych nie posiada autorów[1].

Według Noama Chomsky`ego (*1928) język naturalny posiada ukrytą strukturę głęboką, którą jest gramatyka uniwersalna. Amerykański lingwista odróżniał e-języki, które są jedynie epifenomenami istnienia struktury głębokiej od i-języka, który jest w jego przekonaniu fizycznym mechanizmem wbudowanym w mózg człowieka umożliwiającym generowanie zdań[2]. Gramatyka uniwersalna jest wg Chomsky`ego wrodzona i podobnie jak języki logiki ma charakter swoistego mechanizmu, który determinuje strukturę gramatyczną konkretnych języków naturalnych. Język naturalny można potraktować za swoisty system obliczeniowy, za którym jest skończony zbiór reguł. Konsekwencją takiego stanowiska było wprowadzenie przez amerykańskiego lingwistę badań nad składnią aparatu matematycznego oraz powstanie gramatyki generatywnej, a następnie całej hierarchii gramatyk określanych mianem hierarchii Chomsky`ego.

Podstawą gramatyki generatywnej jest „koncepcja rachunku zdań (systemu formalnego, systemu kombinatorycznego), który według ogólnej definicji jest połączeniem zbiorów zawierających: (1) symbole, (2) reguły konstrukcji, (3) wyjściowe kombinacje symboli oraz (4) reguły transformacji, za pomocą których wytwarza się nowe kombinacje symboli”[3].

Polimorfizm (z gr. poly – wiele + morphos – postać) nie tylko ujmuje wieloznaczność słów (polisemia), lecz również ogólną nieregularność języka naturalnego. Wielopostaciowość języka przejawia się w jego użyciu, gdzie różne konstrukcje operują na szerokim wachlarzu kategorii syntaktycznych i typów semantycznych. Przykładowo G. Chierchia pokazał, jak pewien ogólny typ wyrażenia werbalnego, takiego jak np. angielskie słowo „fun”, może wchodzić w kombinacje z szerokim wachlarzem kategorii takich jak rzeczownik odsłowny (gerund), bezokolicznik (infinitives) czy rzeczownik (nouns): (a) Tennis is fun. (b) Playing tennis is fun. (c) To play tennis is fun[4]. Polimorficzność języka naturalnego łączy się z jego niezwykłą elastycznością zarówno co do formy, jak i treści. Ta cecha języka jest jednym

1 Olszewski A., *Wstęp*, Scienta Scientarum, Kraków (2004), s. 2-3.
2 Chomsky N., Knowledge of Language. Its Nature, Origin, and Use, New York 1986, 19-36.
3 Tamże, s. 35.
4 Chierchia G., Nominalisation and Montague grammar: a semantics without types for natural languages, „Linguistics and Philosophy”, 5 (1982), s. 303–354.

ze sposobów dopuszczenia „nieścisłości" logiki z zachowaniem „zewnętrznych" pozorów dedukcyjnych ścisłości.

2. PROBLEMY W MATEMATYCE – KRÓTKI ZARYS

Wśród największych osiągnięć logików XX wieku o wydźwięku filozoficznym można uznać: (H) Stworzenie metody formalno–aksjomatycznej przez Hilberta. (TS) Twierdzenie Skolema–Löwenheima. (TT) Twierdzenie Tarskiego o niedefiniowalności prawdy. (TG) Twierdzenia Gödla o niezupełności (TG1, TG2). (TC) Teza Churcha. Ścisłe twierdzenia (TS), (TT) i (TG) w sposób zaskakujący ograniczają metodę Hilberta rozwiniętą przez Tarskiego (definicja prawdy) i Gödla (twierdzenie o pełności). (TC) jest kolejnym 'zaskoczeniem' działającym na korzyść (H). O ile (TC) jest prawdziwa, to przynajmniej dla jednego pojęcia intuicyjnego — 'funkcji obliczalnej przez algorytm' — da się podać adekwatną i formalną charakterystykę[5].

Podstawą poglądu naukowego jest przekonanie o konieczności falsyfikacji hipotez. Analiza logicznej treści zasady falsyfikacji nie jest bez wad. W matematyce system falsyfikacji wydaje się jeszcze bardziej złożony niż w naukach przyrodniczych. Istotą matematyki są bowiem pewne struktury matematyczne, tzn. systemy aksjomatów, ze zbiorami swych konsekwencji. Weryfikacja sprowadza się tutaj do wewnętrznej niesprzeczności tych struktur.

W systemie powszechnie uznawanych struktur matematycznych należało zbudować pewne modele, w których wypełniane były aksjomaty nowych struktur. Jeden system konstrukcji matematycznych był interpretowany za pomocą innego systemu. Matematycy wykazali, że modelem płaszczyzny w geometrii Georga Friedricha Riemanna (1826-1866) jest powierzchnia kuli w trójwymiarowej przestrzeni Euklidesa. W ten sposób postulaty Riemanna przekształcone zostały w twierdzenia geometrii Euklidesa. Postulaty Euklidesa – jak wykazano – spełnione są w pewnym algebraicznym modelu, dlatego są niesprzeczne – o ile niesprzeczna jest algebra.

Matematykiem, za którego szczególną przyczyną zagadnienie niesprzeczności nabrało szczególnej ostrości, był Georg Ferdinand Cantor (1845-1918) ze swoją teorią mnogości, która była wykorzystywana do argumentowania analizy matematycznej.

Na początku XX wieku wybitny niemiecki matematyk David Hilbert (1862-1943) podjął próbę udowodnienia absolutnej niesprzeczności arytmetyki, uznając niewystarczalność dowodów względnych. Na przełomie lat dwudziestych i trzydziestych XX wieku Hilbert i jego szkoła publikują prace, z których wynikała (jak się wówczas wydawało) niesprzeczność arytmetyki i teorii mnogości.

W niniejszym tekście nie będę rozpatrywać twierdzenia Gödla ze względu na jego złożoność. Dowód Gödla poprzedzony jest 46 definicjami i kilkoma lematami.

5 Olszewski A., *Wstęp*, Scienta Scientarum, Kraków (2004), s. 2-3.

W 1931 roku austriacki matematyk i logik publikuje słynna pracę ***O formalnie nierozstrzygalnych zdaniach Principia Mathematica i systemów pokrewnych***, z której bezzasadność prób podejmowanych przez Hilberta. Dowód Gödla dotyczy pewnych systemów logicznych zbudowanych w określony sposób. Aksjomaty rozpatrywane są tutaj jako pewne sekwencje symboli, a reguły wnioskowania jako sposoby otrzymywania jednych sekwencji z innych.

W dowodzie tego twierdzenia istotną role odgrywa arytmetyzacja, nazwana numeracją Gödla. Z twierdzenia Gödla wynika, że niesprzeczne systemy logiczne, w języku którym wyrażona jest arytmetyka, są niepełne tzn. istnieją prawdziwe twierdzenia, które można sformułować w języku tych systemów, których w obrębie takich systemów nie da się udowodnić. Nie można również udowodnić niesprzeczności sformalizowanego logiczno- arytmetycznego systemu stosując środki, które dałoby się sformułować w ramach tego systemu a żadne skończone rozszerzenie aksjomatyki tego systemu nie można uczynić go pełnym, ponieważ zawsze znajdą się nowe prawdy, które można sformułować środkami tego systemu ale których nie można z nich wyprowadzić.

Twierdzeniom Gödla podlegają tylko takie teorie, które zawierają co najmniej elementarną arytmetykę (liczby naturalne oraz dodawanie i mnożenie). Po drugie teorie muszą być formalizowalne i aksjomatyzowalne. Po trzecie, teorie podlegają wymogowi arytmetyzacji. Po czwarte relacje, funkcje i zbiory określające i składające się na całość teorii muszą mieć charakter rekurencyjny, tzn. otrzymywanie ich wartości musi być wynikiem zastosowania operacji algorytmicznych[6].

3. ZNACZENIE EPISTEMOLOGICZNE TWIERDZENIA KURTA GÖDLA

Twierdzenie Gödla posiada ogromne znaczenie epistemologiczne, ponieważ zakończyło ono epokę wiary w determinizm, wiary, której ostatnim wyrazem było pojawienie się pozytywizmu logicznego. Gödla miał zmienić stosunek do matematyki pod wpływem Alberta Einsteina (1879-1955). Austriacki logik zwrócił z kolei uwagę Einsteina na badania matematyczno-logiczne, które zdaniem Gödla rzucają światło na ograniczenia ludzkiej wiedzy[7].

Od czasu udowodnienia tzw. twierdzeń limitacyjnych w logice toczy się spór dotyczący ich filozoficznych implikacji. Dyskusja ta (uważa Krzysztof Wójtowicz) jest wielowątkowa: (…) w przypadku drugiego twierdzenia Gödla dotyczy w szczególności programu Hilberta. Pierwsze twierdzenie Gödla stanowi inspiracje dla rozważania szeregu problemów: od zagadnień związanych z problemem psychofizycznym (czy dokładniej: od tezy, że „umysł jest maszyną"), po kwestie ograniczoności naszego poznania[8].

6 Krajewski S., Twierdzenie Gödla i jego interpretacje filozoficzne. Od mechanicyzmu do postmodernizmu. Warszawa 2003, s. 173.
7 Tamże, s. 174.
8 K. Wójtowicz., *O nadużywaniu twierdzenia Gödla w sporach filozoficznych*. http://www.opoka.org.pl/biblioteka/F/FL/ograniczenia_godla.html#

Oprócz licznych przykładów interpretacji osiągnięć Gödla w dociekaniach nad naturą matematyki, dostrzec można wiele interpretacji i odniesień do twierdzeń austriackiego matematyka, przedstawicieli innych nauk.

Znawcy teoretycznych jak i praktycznych problemów translatorskich wyrażają opinię następującą: Jeżeli arytmetyka, którą uznajemy za manifestację prawd typu dwa plus dwa równa się cztery, zdawałoby się dokładnie opisywalna i wymierna, sama zakłada sobie pętle na głowę i udowadnia własną niemoc, co począć z innymi systemami opisującymi rzeczywistość [9]?

Wybitny polski tłumacz Krzysztof Lipiński (1956-2013) uważa, że jeżeli przeniesiemy konsekwencje (rozumienia) twierdzenia Gödla na obszar języków naturalnych, które posiadają zarówno strukturę systemową (langue) jak i konkretną realizację (parole), nasunie się pytanie: czy jakikolwiek język naturalny jest w stanie opisać rzeczywistość obiektywną i subiektywną człowieka. Podobnie jak arytmetyka tak system języków naturalnych są za słabe do pełnego opisu rzeczywistości. Zjawiska opisywalne w sposób systemowy w jednym języku są w innym opisywalne przy pomocy środków leksykalnych lub określeń ***ad hoc***[10]. Przywoływane jest często w tym kontekście twierdzenie Alana Turinga (1912-1956).

Problem polega na pytaniu, czy istnieje efektywna procedura, którą można zastosować do dowolnego programu i dowolnych danych początkowych, pozwalająca stwierdzić, czy ten warunek będzie spełniony.

W 1936 roku Turing rozstrzygnął te kwestie stwierdzając, że taka procedura nie istnieje. Nie istnieje bowiem ogólny algorytm, który pozwoliłby rozstrzygnąć, czy dowolny program P, zastosowany do dowolnych początkowych I, zakończy pracę[11].

Casti i de Pauli przytaczają kwestie dotyczącą opisywalności prawdy: Zapewne nie jest szczególną niespodzianką odkrycie, że nie istnieje skończony zbiór reguł, które wystarczyłyby do wygenerowania wszystkich prawd o świecie. Reguły takie istniałyby wewnątrz świata, który miałby opisywać, a zatem próba znalezienia skończonego zbioru reguł generującego wszystkie prawdy, których jest nieskończenie wiele, wydaje się analogiczna do próby wyciągnięcia się z bagna za włosy[12]. Prawdziwym zaskoczeniem jest natomiast dowód Gödla, który wykazał, że to samo dotyczy znacznie mniejszego i bardziej uporządkowanego świata liczb naturalnych.

Zdaniem matematyków John`a Casti`ego (*1943) i Wernera de Pauli`ego (*1942), badania austriackiego matematyka mają niezwykle głębokie konsekwencje dla epistemologii oraz kwestii mechanizacji myślenia i liczenia[13]. Autorzy powyższej publikacji podają szereg przykładów odwołujących się do twierdzenia Gödla w trakcie prób stworzenia maszyny tłumaczącej w ogóle.

9 Lipiński K., *Mity przekładoznawstwa*, Kraków 2004, s. 21.
10 Tamże, s. 22.
11 Casti J. L, De Pauli W., *Gödel. Zycie i logika*. Warszawa 2003., s.112-117.
12 Tamże.
13 Tamże.

W książce E. Nagla i J. R. Newmana pt. ***Twierdzenie Gödla***, która stanowi z kolei jedno z pierwszych wnikliwych opracowań dotyczących twierdzeń limitacyjnych Gödla oraz ich ewentualnych konsekwencji dla innych dziedzin wiedzy znajdujemy stwierdzenie o niemożliwości zbudowania maszyn myślących, ponieważ programy EMC są wg autorów publikacji zawsze budowane wedle reguł ścisłej logiki**:** struktura i działalność umysłu ludzkiego jest daleko bardziej złożona i subtelna, niż budowa i sposób funkcjonowania którejkolwiek z maszyn, jakie dziś potrafimy zaprojektować[14].

Nie wiadomo na czym polegałaby to „coś", co nazwać można by „procedurą" ludzkiego myślenia. Na poziomie porozumiewania się ludzie wykorzystują zasady logiki formalnej. W języku potocznym a tym bardziej w języku nauki odnajdujemy struktury logiczne.

Warto zauważyć, że w środowisku logików istnieje „niepisane prawo" zabraniające zajmowania się filozoficznymi interpretacjami twierdzeń Gödla. Jan Woleński (*1940) uważa jednak, że wykorzystywanie twierdzeń Gödla w epistemologii jest równie zasadne, jak rozpatrywanie determinizmu w oparciu o mechanikę kwantową. I tak jak rozprawianie o determinizmie bez uwzględnienia zasady nieoznaczoności jest obecnie jałowe, tak też jałowe są analizy epistemologiczne ignorujące twierdzenia limitacyjne[15].

4. INTERPRETACJA TWIERDZEŃ GÖDLA WEDŁUG STANISŁAWA LEMA

Bazując na zaproponowanej na początku niniejszej pracy charakterystyce pojęcia polimorfizmu i twierdzenia Kurta Gödla należy zauważyć, że twierdzenie można odnieść tylko wtedy do języka naturalnego, jeżeli przyjmiemy, że dany język naturalny jest systemem zawierającym arytmetykę liczb naturalnych.

To z kolei wymusza przyjęcie pewnej przesłanki, że język musi być w jakiś sposób systemem formalnym np. w formie i-języka Chomsky`ego. To znaczyłoby, że struktura głęboka jest systemem niezupełnym, w stosunku do świata, którą język wygenerowany przez tę strukturę opisuje. Gödel prawdopodobnie nie zgodziłby się z teorią Noama Chomsky`ego ponieważ występował on przeciw poglądowi, iż myślenie ma charakter mechanistyczny. Z drugiej jednak strony koncepcja kompetencji językowej Chomsky`ego warunkująca intuicje językową dyspozytorów języka naturalnego, żywo przypomina koncepcję intuicji matematycznej Gödla.

Zanim przejdziemy do specyficznej interpretacji twierdzenia Gödla przez Stanisława Lema należy wspomnieć o tym, że w historii nauki jak i filozofii mamy do czynienia z pewnymi zadziwiającymi myślami wobec których należy przyjąć sformułowaną przez Kazimierza Ajdukiewicza (1890-1963) i Donalda Davidsona (1917-2003), dyrektywę życzliwości interpretacyjnej, polegającą na możliwie wolnym od stereotypów rozpatrywaniu cudzych myśli[16].

14 Nagel E, Newman J.R., *Twierdzenie Gödla*, tłum. S. Stanosz, Warszawa 1966, s. 71.
15 Woleński J., Metamatematyka i filozofia. *Zagadnienia Filozoficzne w Nauce*. VI (1984), s. 14.
16 Wierzbicka G., Ludwika Wittgensteina krytyka pierwszego twierdzenia Gödla, [w:] „Roczniki filozoficzne" Tom LVIII, numer 2 – 2010, s. 217.

W opinii Stanisława Lema wyróżnić można dwa sposoby rozumienia treści wynikających z twierdzeń naukowych. Lem mianowicie rozróżniał bezpośredni sposób rozumienia treści naukowych, idący w parze tylko z bezwzględnym przyrostem wiedzy, oraz pośredni sposób rozumienia (subtelny), wynikający z selektywnego przyrostu wiedzy wraz z poszerzeniem się tolerancji w kwestiach nowych np. zdanie: „wiedza nasza stała się rozmiarem olbrzymia tylko wobec człowieka, nie wobec świata" można opisać m.in. następująco: „rosnący podzbiór odkrytych prawd o świecie odsłania swoje coraz większe tło – ogółu możliwych prawd o świecie". Rozumowanie bezpośrednie byłoby typowe dla potocznie asymilowanej nauki, natomiast rozumienie pośrednie (subtelne) dla np. naukopochodnej filozofii[17].

Do rozważań dotyczących recepcji twierdzeń logiczno- matematycznych można wprowadzić pewną uwagę; wszystkie rozważania, dyskusje w trakcie których dochodzi do wymiany poglądów między znawcami problemu dokonują się na gruncie języka naturalnego lub jego materialnego relewantu jakim można uznać tekst.

Stanisław Lem w takich słowach interpretuje filozoficzno- kulturowe znaczenie twierdzenia Gödla:

Prawdopodobnie największym we współczesności nieporozumieniem, które zrodziło zarówno angielską filozofię lingwistyczną, jak odmienną od niej jawnie filozofię fenomenologiczną, wraz z późnymi naroślami tej filozofii (Heidegger, Derrida, le Man, Lyotard et alii) była ukryta przyczyna przed rozumiejącym spojrzeniem tych myślicieli: mam na uwadze mianowicie, słynny dowód Gödla (…) dla naszych potrzeb wystarczy przywołać go na poły metaforycznie (…) żaden system dostatecznie bogaty, razem ze swoim alfabetem i swoja gramatyką (czyli ze swymi zbiorami skończonymi znaków i reguł ich przetwarzania) nie jest pełny. Znaczy to, że dla każdego takiego systemu można wykryć zdania (twierdzenia) prawdziwe, których prawdziwości nie da się dowieść wewnątrz owego systemu jego sposobami[18].

Wyobraźmy sobie pewną skalę języków na której znajdują się zarówno języki „miękkie", charakteryzujące się polimorfizmem semantycznym, co oznacza w konsekwencji poliinterpretacyjność, wielowykładalność znaczeń. Języki „miękkie" cechują się wewnętrznymi sprzecznościami np. język malarstwa abstrakcyjnego czy język ZEN. Interpretacja potencjalnych treści w tego rodzaju malarstwie jak i treściach ZEN zachodzi subiektywnie a nie jest intersubiektywne jak w przypadku języka logiki, matematyki, czy języka programowania komputerowego, które będą znajdowały się na przeciwnym krańcu pewnej skali językowej. Gdzie na zaproponowanej skali usytuować można język naturalny/ etniczny? Język naturalny mógłby zająć pasmo między językami „miękkimi" a językami „twardymi". Język którym posługujemy się na co dzień jest „rozmyty" logikosemantycznie.

Dany język naturalny jest dostatecznie twardy „kodowo", aby porozumiewanie było możliwe i dostatecznie „miękki" aby można było rozumieć przekazywane

17 Okołowski P., Materia i wartości. Neolukrecjanizm Stanisława Lema. Warszawa 2010., s. 324.

18 Lem S., *Moloch*, Kraków 2003., s. 257.

za jego pomocą informacje. Za pomocą języka naturalnego (np. danego języka etnicznego) możemy „wzbić się" na kolejny poziom tego języka, mówiąc: „widzę krzesło", powiadam w odniesieniu do klasyfikacji danej rzeczy, że „widzę mebel" ale nie można powiedzieć: „widzę krzesło i widzę mebel". Nie uświadamiamy sobie na co dzień jako dyspozytorzy języka tysięcy takich „przenosin".

W języku wyzbytym bogactwa, czyli w języku „monomorficznym" panowałby nadmiar liczbowy i takim językiem nie można by się posługiwać. Każda próba definitywnego „domknięcia" systemów znakowych niepełnych prowadzi – poprzez apelacje do systemów coraz wyższych – do ***regressus ad infinitum***. Język używany na co dzień zatem ma swoje miejsce w zbiorach znaczeniowych „rozmytych". np. zdanie: „Paweł patrzy na Olę przez hormon androsteronowy", rozumiane literalnie jest nonsensem, jest zrozumiałe dzięki przeniesieniu znaczenia na inny poziom. Także w języku fizyki teoretycznej, kosmologii, biologii, czy matematyki znajdziemy metafory o rozmaitej amplitudzie znaczenia, które opisywane są za pomocą głównie matematyki[19].

5. PODSUMOWANIE

Stanisław Lem przenosi filozoficzne konsekwencje osiągnięć Kurta Gödla na pole systemów znakowych, stwierdzając przy tym, że jeżeli odniesiemy ogólnometodologiczne wnioski jakie można wynieść z twierdzenia Gödla do systemów znakowych, to również w dostatecznie bogatych systemach tego rodzaju możemy sformułować zdania, których prawdziwości nie dowiedziemy sposobami jakie oferuje dany system. Język naturalny z całym swoim bogactwem nie dba o poprawność logikosemantyczną, tworzy wyrażenia ad hoc, przenosi znaczenia na inne poziomy, nie wynika to z jego wadliwego charakteru np. z braku stosowania umownych zasad poprawności gramatyczno- semantycznej itp. Stanisław Lem stawia hipotezę, że język naturalny dzięki właściwemu sobie polimorfizmowi przezwycięża „problem gödelowski".

Nieścisłość i niewyrażalność słów, nieostrość granic między pojęciami, wieloznaczność i różnorodność stwarzają możliwości naruszenia dedukcyjnych form myślenia, które dokonuje się naturalnie bez rozdrażnienia interlokutora. Polimorfizm pozwala na wprowadzenie do rozważań tej „niezgodności", bez której system dany byłby niepełny. Granice dopuszczalnej nieścisłości ustalają się samoczynnie. Język naturalny mógłby zatem zajmować pośrednie miejsce na skali semantycznej, która na jednym krańcu umiejscawia języki twarde o ściśle określonych znaczeniach symboli, na drugim języki miękkie o arbitralnej więzi między znakiem i przedmiotem oznaczonym. Język naturalny zajmuje pasmo pomiędzy dwoma wyżej wymienionymi rodzajami języków.

LITERATURA

1. Olszewski A., *Wstęp*, „Scienta Scientarum" nr 3, Kraków (2004).
2. Pawlak Z., *Maszyna i język*, Warszawa 1964.
3. Chomsky N., Knowledge of Language. Its Nature, Origin, and Use, New York 1986.

19 Tamże, s. 258.

4. Pazukhin R., *Natywizm we współczesnej lingwistyce*, Lingwistyka a filozofia. Współczesny spór o filozoficzne założenia teorii języka, Warszawa, 1977.
5. Chierchia G., Nominalisation and Montague grammar: a semantics without types for natural languages, „Linguistics and Philosophy", 5 (1982).
6. Bodynek M., *Czy twierdzenie Gödla jest sprzeczne z mechanicyzmem*? „Czasopismo Filozoficzne" nr 6 (2010).
7. Krajewski S., Twierdzenie Gödla i jego interpretacje filozoficzne. Od mechanicyzmu do postmodernizmu. Warszawa 2003.
8. K. Wójtowicz., *O nadużywaniu twierdzenia Gödla w sporach filozoficznych*. http://www.opoka.org.pl/biblioteka/F/FL/ograniczenia_godla.html#
9. Lipiński K., *Mity przekładoznawstwa*, Kraków 2004.
10. Casti J. L, De Pauli W., *Gödel. Zycie i logika*. Tłum. Piotr Amsterdamski, Warszawa 2003.
11. Nagel E, Newman J.R., *Twierdzenie Gödla*, tłum. S. Stanosz, Warszawa 1966.
12. Woleński J., *Metamatematyka i filozofia*. „Zagadnienia Filozoficzne w Nauce". VI (1984).
13. Wierzbińska G., *Ludwiga Wittgensteina krytyka Pierwszego Twierdzenia Kurta Gödla*, „Roczniki Filozoficzne", Tom LVIII, nr 2. 2010.
14. Okołowski P., Materia i wartości. Neolukrecjanizm Stanisława Lema. Warszawa 2010.
15. Lem S., *Moloch*, Kraków 2003.

Prosopon
Europejskie Studia Społeczno-Humanistyczne

Wydawca / Publisher:
Instytut Studiów
Międzynarodowych
i Edukacji HUMANUM
www.humanum.org.pl

12 (3) 2015
ISSN 1730–0266

Michał Stachura
Rzeszów, Poland

Przedstawienie metody szyfrowania informacji ZT-UNITAKOD / *Presentation of the ZT-UNITAKOD course method*

Abstract
The Ministry of Foreign Affairs, which in 1993 had 45 diplomatic missions, stated unequivocally that modern technology is so advanced that it is best to assume the existence of eavesdropping in all settings at all times. In 1992 the Ministry of Foreign Affairs assigned 38,000 secret encrypted messages. Secret letters from the same ministry are transported on 160 different routes by couriers, ie specially trained officers for this purpose. In the sixties crashed the plane, which carried very secret messages, then killed bags with secret diplomatic mail, the rest survived.
The situation I described above clearly shows that the best and only secure means of transport can be mailed electronically in encrypted form. The cipher used to encrypt such important state information must be unbreakable. This cipher must be based on mathematical models that exclude human (human factor) from the encryption and decryption process. Only such a cipher can give us one hundred percent effective protection of information.

Key words: **safety, information, zt-unitakod.**

Ministerstwo Spraw Zagranicznych, które w roku 1993 posiadało 45 placówek dyplomatycznych stwierdza jednoznacznie, iż nowoczesna technika jest tak zaawansowana, że najlepiej jest założyć fakt istnienia podsłuchu we wszystkich placówkach przez cały czas. W roku 1992 MSZ nadało 38 tysięcy tajnych zaszyfrowanych depesz. Tajne listy z tegoż ministerstwa przewożone są na 160 różnych trasach za pomocą kurierów, czyli specjalnie przeszkolonych do tego celu oficerów. W latach sześćdziesiątych rozbił się samolot, który przewoził bardzo tajne depesze, zginęły wówczas worki z tajną pocztą dyplomatyczną, reszta ocalała.

Sytuacja, którą opisałem powyżej pokazuje wyraźnie, że najlepszym i jedynym bezpiecznym środkiem transportu może być poczta przesyłana drogą elektronicz-

ną w zaszyfrowanej postaci. Szyfr użyty do szyfrowania tak ważnych informacji państwowych musi być niemożliwy do złamania. Szyfr ten musi opierać się na modelach matematycznych, które wykluczą człowieka (czynnik ludzki) z procesu szyfrowania i deszyfracji. Tylko taki szyfr może dać nam stu procentową skuteczność ochrony informacji.

Jest to tylko jeden z przykładów, dla których szyfrowanie jest tak ważne w życiu społeczeństw. Metoda szyfrowania, która wyeliminowała człowieka z procesu szyfrowania i deszyfracji opatentowana jest pod nazwą ZT-UNITAKOD. Prace nad ta metodą rozpoczęły się w roku 1985. W roku 1988 metoda przyjęła powyższą nazwę i została bardzo pozytywnie przyjęta przez zespoły naukowe zachodu.

Do powstania metody ZT-UNITAKOD przyczynił się sam człowiek a ściśle mówiąc jego decydująca rola w szyfrowaniu informacji. Po przeanalizowaniu poszczególnych statycznych metod szyfrowania łatwo dojść do wniosku, że najsłabszym ogniwem w tej układance jest sam człowiek oraz klucz. Człowiek opracowuje dany klucz, przechowuje, przesyła, wymienia i ochrania. Nawet jeżeli sama metoda była by nie do złamania to jej wartość rzeczywista staje się zerowa. Metoda komputerowego zabezpieczenia poufności informacji musi być metodą niezależną od człowieka i posiadać klucz zmieniający się w czasie, bez ingerencji człowieka, który zależy tylko od zmieniającego się czasu przetwarzania.

1.1 PODSTAWOWE INFORMACJE

Metoda ZT-UNITAKOD posiada w swojej budowie elementy zmienne i stałe:

1. Elementy stałe – STANDARD
2. Elementy zmienne - SUPLEMENT

W skład STANDARDU wchodzą:

a) Model matematyczny szyfru.
b) Model matematyczny deszyfracji
c) Tablice kryptograficzne A1, A2, A3, A4, i A
d) Pięć rodzajów szyfrów generowanych jednocześnie
e) Wymagania metody dotyczące generatorów permutacji oraz dynamiki kryptosystemów

W skład SUPLEMENTU wchodzą:

a) Generatory permutacji
b) TIME i sposób jego generowania
c) Zasada tworzenia tablic kryptograficznych przy wykorzystaniu TIME, po jego podziale
d) Zasada szyfrowania strumienia danych i deszyfracji szyfrogramu

W metodzie ZT-UNITAKOD zastosowano sumę dwóch elementów modulowaną liczbą N = 256, a tworzenie klucza szyfrującego w postaci tablicy A uzależniono od dwóch generatorów permutacji i układu elementów dynamicznych w postaci

daty i czasu. Szyfr ten jest elementem zmiennym uzależnionym od czasu szyfrowania. Podczas szyfrowania można wygenerować pięć różnych rodzajów szyfru. Informacje sterujące są szyfrowane inaczej nić przesyłany meldunek. Metoda ta nie wymaga tak zwanego transportu tajnych kluczy, ani specjalnego utajniania informacji sterującej.

Model matematyczny szyfru metody ZT-UNITAKOD:

Szyfr = (A + B) mod N,

gdzie:

A – tablica kryptograficzna – klucz szyfrujący utworzony z 65 536 bajtów,

B – przesyłana informacja jawna

N – liczba znaków alfabetu – dla kodu ASCII wartość N = 256

Model matematyczny deszyfracji:

$$B = S - A \qquad \text{dla: } S - A > 0$$

$$B = (S - A) + N \qquad \text{dla: } S - A \leq 0$$

1.2 ZASTOSOWANE GENERATORY PERMUTACJI

1. Generator multiplikatywny G_1

$G_1 = (cx_i) \bmod n$, gdzie c – liczby nieparzyste z przedziału od 3 do 255

Są to następujące liczby: 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211, 213, 215, 217, 219, 221, 223, 225, 227, 229, 231, 233, 235, 237, 239, 241, 243, 245, 247, 249, 251, 253, 255.

Razem jest to 127 liczb. x_i – ciąg liczb całkowitych od 1 do N

1. Generator mieszany G_2

$G_2 = (ax_i + b) \bmod n$, gdzie a – liczby nieparzyste spełniające równanie: $a = 1 \pmod 4$.

Są to liczby: 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181, 185, 189, 193, 197, 201, 205, 209, 213, 217, 221, 225, 229, 233, 237, 241, 245, 249, 253.

Razem 63 liczby, b – liczby nieparzyste z przedziału od 1 do 255. Liczby te są równe iloczynom „c" z dodatkiem liczby 1(jeden), x_i – ciąg liczb całkowitych od 1 do N.

Pary a/b stosowane w G_2 tworzone są z liczb „a" oraz „b". Liczby łączymy ze sobą według następującej zasady: pierwsza liczbę „a", w naszym przypadku „5" łączymy

ze wszystkimi liczbami „b" i otrzymujemy ciąg par a/b: 5/1, 5/3, 5/5, 5/7,….,5/255. Następnie bierzemy kolejną liczbę „a", która również łączymy ze wszystkimi liczbami „b" i otrzymujemy kolejny ciąg par. Tak postępujemy ze wszystkimi liczbami „a" i „b".

Ponieważ ilość liczb a = 63 i liczb b = 128, stad liczba par wynosi: 63 * 128 = 8064.

1.3 OGÓLNY ALGORYTM METODY ZT-UNITAKOD

Algorytm ZT-UNITAKOD generuje nieokresowy podwójny szyfr strumieniowy. Strumień kluczy $k=k_1k_2k_3$ … generowany jest synchronicznie ze strumieniem tekstu jawnego. Generowanie to odbywa się deterministyczną metoda losową z użyciem szeregu jedno i dwu wymiarowych tablic kryptograficznych, funkcji i generatorów liczb pseudolosowych. Poza tym w metodzie zastosowano szyfrowanie danych inicjujących proces generowania tablic i działania generatorów liczb pseudolosowych oraz umieszczanie ich w kryptogramie w postaci zaszyfrowanej. Proces kodowania źródłowej postaci tekstu jawnego jak i danych inicjujących oparty jest o zastosowanie sumy arytmetycznej dwóch liczb całkowitych, co znacząco zwiększa odporności szyfru na złamanie. Dla przykładu kod występujący w kryptogramie może być wynikiem dodawania wielu możliwości np. kod 120 można otrzymać dodając do 119 + 1 jak i dodając do 110 + 10. Kryptoanalityk staje więc przed problemem rozwiązania pojedynczego równania z dwoma niewiadomymi, co już w pewien sposób ogranicza zakres jego możliwości. Generator strumienia klucza jest inicjowany i pracuje w oparciu o zbiór zarówno stałych jak i zmiennych elementów kryptosystemu.

Szyfrowanie za pomocą metody ZT-UNITAKOD odbywa się w 5 etapach. Na początku tworzona jest początkowa tablica kryptograficzna A0. Powstaje ona w oparciu o zestaw stałych liczb T i zawartość wektora R0. Tablica A0 ma wymiary NxN. W drugim etapie w oparciu o zawartość tej tablicy powstaje wartość zewnętrznych parametrów dynamicznych (unikalnych dla każdego kryptogramu poprzez swoją tymczasowość np. dokładny czas rozpoczęcia momentu szyfrowania, identyfikatory nadawcy i odbiorcy kryptogramu i inne) Bezpośredni proces kodowania tych wartości odbywa się w oparciu o wzór

$$D'[l] = (A0[i,j] + D[k]) \bmod N_A$$

gdzie,

D[k] - to kolejne elementy wektora zawierającego wartość parametrów dynamicznych w postaci jawnej,

A0[i,j] - elementy początkowej tablicy kryptograficznej,

D'[l] - jest elementem wektora zawierającego zaszyfrowaną postać wartości parametrów dynamicznych.

N_A jest liczbą elementów alfabetu przyjętego w kryptogramie standardu służącego do cyfrowego odwzorowania danych w kryptosystemie np. dla ASCII, $N_A = 256$.

W trzecim etapie z tablicy A0, elementów wektora D i elementów zbioru T tworzy się końcową tablicę kryptograficzną A, która służy następnie do ostatecznego i bezpośredniego kodowania źródłowego tekstu jawnego.

W czwartym etapie odbywa się bezpośrednie kodowanie źródłowego tekstu jawnego w oparciu o wzór:

$S[m] = (A[i,j] + B[m]) \bmod N_A$

gdzie,

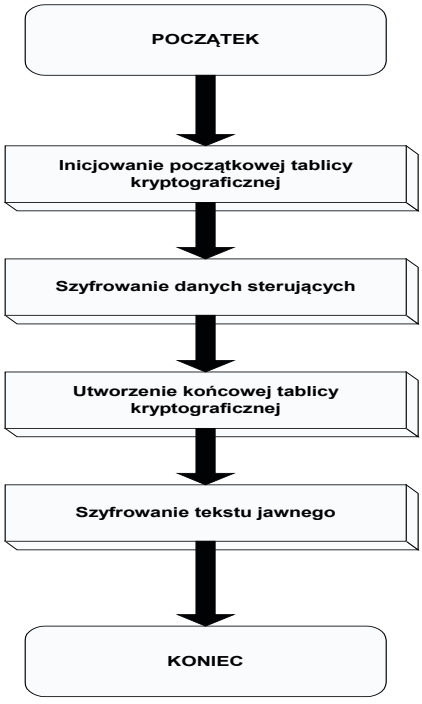
S[m] - to kolejny element zaszyfrowanej postaci tekstu jawnego,

A[i,j] - to element końcowej tablicy kryptograficznej a B[m] kodowany element tekstu jawnego.

Wyboru elementów tablicy A służących do szyfrowania kolejnych porcji (np. bajtów) tekstu jawnego dokonuje się w oparciu o funkcję będącą iloczynem kartezjańskim elementów D, T, R0 i A.

Ostatnim piątym etapem działania algorytmu jest scalenie wektora D' i zaszyfrowanych wartości tymczasowych inicjujących parametrów dynamicznych oraz wektora S zawierającego zaszyfrowaną postać źródłową tekstu jawnego. To połączenie realizowane jest w oparciu o funkcję c,, która dodatkowo może jeszcze mieszając elementy D' i S umieszczając je w sposób pseudolosowy w wektorze C zawierającym ostateczną postać kryptogramu.

Ogólny algorytm szyfrowania:

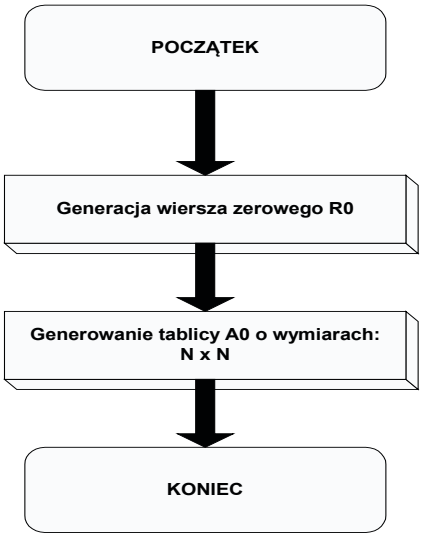


a. Inicjowanie początkowej tablicy kryptograficznej

R0 jest N - wymiarowym wektorem liczbowym. Zawiera on zestaw N dowolnych liczb. Jego postać musi być identyczna zarówno u nadawcy jak i odbiorcy zaszyfrowanej wiadomości. W kryptosystemie opartym na tym algorytmie spełnia on role dynamicznego elementu identyfikacyjnego wymienianej między nadawca i odbiorcą informacji. Może być również wbudowany na stałe w kryptosystem z możliwością lub bez możliwości modyfikacji jego postaci, w postaci jawnej lub zaszyfrowanej w oparciu o zestaw stałych liczb T, własne funkcje i generatory liczb pseudolosowych.

Wektor R0 służy do utworzenia początkowej tablicy A0. Tablica ta zawiera dokładnie N wierszy po N elementów w każdym. Wiersze zawierają wartości liczbowe, które są produktem iloczynu kartezjańskiego wektora R0 i stałych wartości liczbowych T. W najprostszym tworzenie tych wierszy może odbywać się poprzez cykliczne przesuwanie w lewo wektora R0 o ilość pozycji zgodną z kolejnymi liczbami pobranymi z T. W praktyce jednak funkcja odwzorowująca jest bardziej skomplikowana.

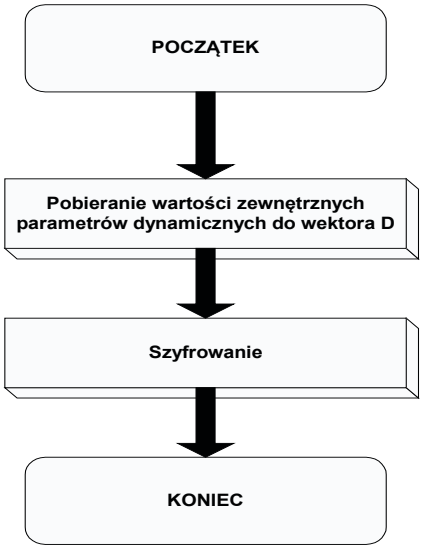
Algorytm inicjowania początkowej tablicy kryptograficznej A0;



b. Algorytm szyfrowania danych sterujących:

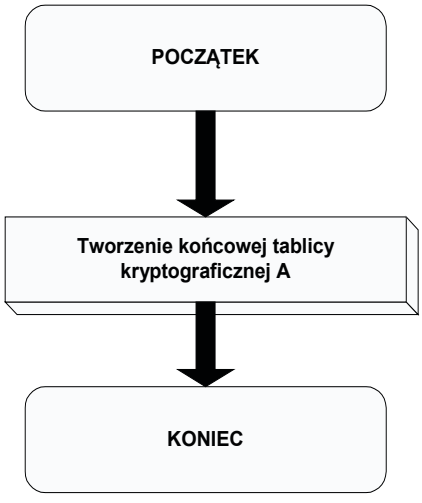
Dynamiczne wartości inicjujące pobiera się do systemu w postaci cyfrowej. Następnie kody tych wartości umieszcza się w wektorze D.

W tym etapie działania algorytmu współrzędne kolejnych elementów tablicy A0 służące do bezpośredniego kodowania elementów wektora D pobiera się w oparciu o zestaw wartości liczbowych T i przyjęte funkcje i generatory pseudolosowe.



c. Algorytm tworzenia końcowej tablicy kryptograficznej A.

Na tym etapie działania algorytmu odbywa się tworzenie końcowej tablicy kryptograficznej A, której elementy są sumowane z kolejnymi elementami tekstu jawnego. Elementy tablicy są generowane na podstawie zawartości A0, D i T. W prostej wersji może to być np. przestawianie elementów kolejnych wierszy A0 zgodnie z adresami pobranymi z T na podstawie wartości z wektora D. W praktyce funkcja f zawiera jeszcze dodatkowe elementy związane z działaniem generatorów liczb pseudolosowych.



d. Algorytm szyfrowania informacji jawnej.

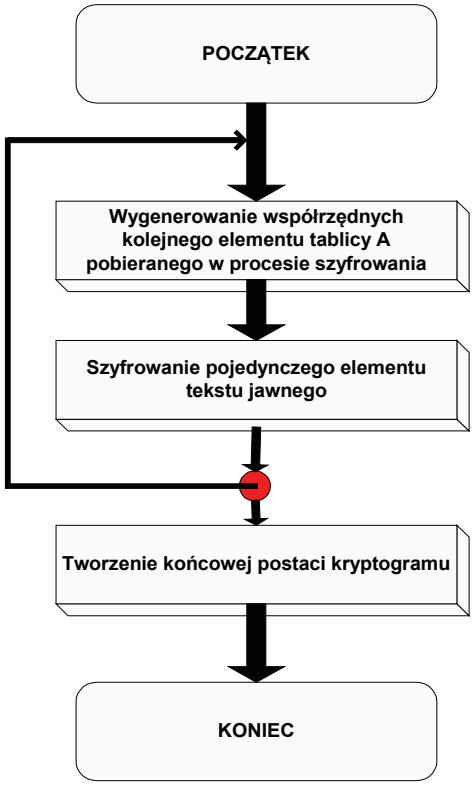
Ten etap działania algorytmu szyfrowania zawiera proces generowania współrzędnych kolejnych elementów tablicy A. Elementy te są z kolei dodawane bezpośrednio do kodów wartości elementów tekstu źródłowego. Generowanie współrzęd-

nych odbywa się w oparciu o funkcję deterministyczną w odwzorowującą iloczyn kartezjański wszystkich dotychczas wygenerowanych elementów kryptosystemu (R0, A0, T, D) w dwuwymiarowy wektor zawierający numer wiersza i kolumny w tablicy A. Wartości funkcji w są z zakresu <N ; N> dlatego elementy kolejno pobierane do szyfrowania pochodzą z dowolnego miejsca tablicy A (np. dla N = 256 jest 2^{16} elementów tablicy A).

Szyfrowanie pojedynczego elementu tekstu źródłowego odbywa się w oparciu o sumę arytmetyczną (tak jak dla dynamicznych parametrów inicjujących). Własność tej metody kodowania opisano krótko w komentarzu do ogólnego algorytmu szyfrowania.

Funkcja c powoduje przemieszanie elementów zaszyfrowanej postaci tekstu źródłowego z elementami wektora zawierającego zaszyfrowane inicjujące parametry dynamiczne. Funkcja ta musi być odwracalna.

Najprostszym rozwiązaniem implementacyjnym jest umieszczenie elementów D' na początku lub na końcu kryptogramu. Długość D' jest zmienna, więc nawet w takim przypadku wydzielenie D' i S przez kryptoanalityk jest trudne. Ostateczna postać kryptogramu może zawierać także elementy kontroli parzystości lub inne.



e. Algorytm deszyfrowania informacji.

Algorytm deszyfrujący zawiera pięć etapów działania. Na początku rozdziela się kryptogram na cześć S zawierającą zaszyfrowaną postać tekstu źródłowego i wektora D' z zaszyfrowanymi wartościami inicjujących parametrów dynamicznych. Z kolei generowanie wiersza zerowego odbywa się identycznie jak dla procesu szyfrowania. W trzecim etapie deszyfruje się wartości parametrów dynamicznych z wektora D' w oparciu o wzór:

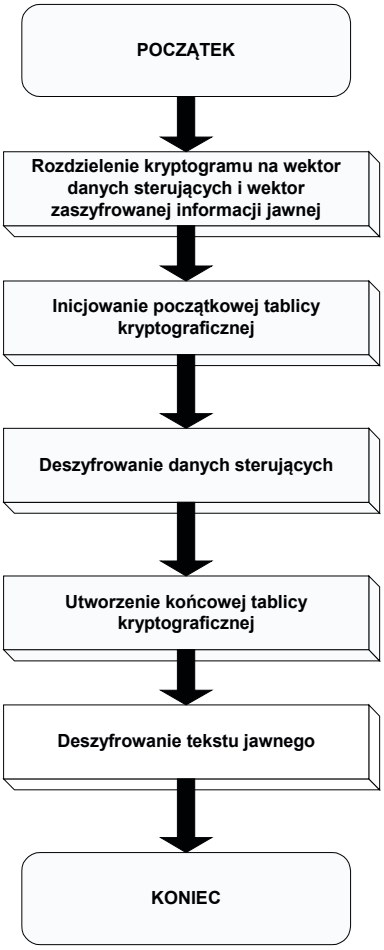
$$D[l] = (A0[i,j] - D'[k]) \bmod N_A$$

Oznaczenia i funkcja wyboru kolejnych elementów pozostaje taka sama jak dla procesu szyfrowania.

Tworzenie kryptograficznej tablicy A odbywa się identycznie jak dla szyfrowania (parametry dynamiczne są już w postaci jawnej w wektorze D). Deszyfracja elementów wektora S odbywa się w oparciu o wzór:

$$B[m] = (a[i,j] - S'[m]) \bmod N_A$$

Ostatecznie deszyfrowana postać tekstu źródłowego znajduje się w wektorze B.



Klucze dynamiczne stosowane w metodzie ZT-UNITAKOD:

1. DATA i CZAS
2. Seed lub TIME
3. liczby dla generatorów
   - pięć liczb,
   - 31 par liczb a/b
   - 256 par liczb a/b

Funkcje kluczy dynamicznych:

- wszystkie funkcje są czasowo zmienne,
- klucze dynamiczne nie biorą bezpośredniego udziału w szyfrowaniu informacji, czyli nie są częścią składową szyfru
- klucze dynamiczne inicjują tworzenie tablicy kryptograficznej, której układ zmienia się co jedną sekundę.

1.4 JAK POWSTAJE KLUCZ DYNAMICZNY

Klucz pierwszy DATA i CZAS tworzą jednorazowy układ szyfrujący.

Przykład:

DATA = 7 grudnia 2004 r. co zapisujemy: 07.12.2004.

CZAS = godzina czternasta, 32 minuty i 18 sekund, co zapisujemy 14.32.18.

Stąd DATA i CZAS utworzyły zapis: 07122004143218.

Taki sam zapis utworzony z DATY i CZASU nie powstanie już nigdy, chociaż sam zapis zmienia się co jedną sekundę. Mówiąc inaczej, szyfrogram przyjmuje ściśle określoną i jednorazową postać.

Klucz drugi to Seed, który wykorzystując wyniki DATY i CZASU tworzy tak zwany wiersz zerowy „R0" składający się z 256 znaków kodu ASCII. Liczba permutacji R0 = 256 !.

Kolejny klucz o nazwie TIME zastępuje Seed, a jego liczba permutacji wynosi:

$L_p = (256 !)^{256}$

Kolejne trzy klucze dynamiczne to układy liczb dla generatorów permutacji.

To wszystko składa się na metodę ZT-UNITAKOD. Przeprowadzenie próby łamania tej metody omówię w kolejnych rozdziałach mojej pracy.

1.5 WYMAGANIA METODY ZT-UNITAKOD

Wymagania tej metody są bardzo ściśle związane z wymaganiami generatorów permutacji. Generatory permutacji zastosowane w tej metodzie należą do SUPLEMENTU, więc mogą być inne niż te obecnie tu zastosowane. Zmiana generatorów

w żaden sposób nie wpływa ujemnie na moc kryptograficzną metody ZT-UNI-TAKOD.

Wymagania dla generatora G_1

1. $(cx_i) \bmod n \neq 0$ dla $i = 1, 2, \ldots, n - 1$
2. $(cx_i) \bmod n \neq 0$ dla $i = n$
3. $(cx_i) \bmod n \neq (cx_j) \bmod n$ dla $i \neq j$

Wymagania dla generatora G_2

1. $(ax_i + b) \bmod n \neq 0$ dla $i = 1,2, .., n.$
2. $(ax_i + b) \bmod n \neq (ax_j + b) \bmod n$ dla $i = j.$

Rodzaje tablic kryptograficzny i par a/b:

Litera „A" przedstawiona w matematycznym wzorze szyfrowania informacji zawiera trzy rodzaje tablic kryptograficznych: T1, T2, TA.

Opis poszczególnych tablic:

1. T1 – jest to tablica początkowa posiadająca przesunięty wiersz zerowy
2. T2 – jest to tablica posiadająca zmieniony układ znaków, wygenerowana za pomocą generatora G_2, po zastosowaniu jednego z 31 układów par a/b
3. TA – tablica końcowa, wygenerowana za pomocą generatora G_2 po zastosowaniu jednego z 256 układów par a/b.

Wygląd tablicy kryptograficznej:

1	2	…	255	256
2	3	…	256	1
. . .		Tablica kryptograficzna		
255	256	…	253	254
256	1	…	254	255

Pary a/b są grupowane dwojako:

1. Układ 256 par a/b
2. Układ 31 par a/b

Z par liczb „a" i „b" tworzone są tak zwane pary a/b dla generatora G_2.

Liczba wszystkich par a/b wynosi M = 8064.

Liczba permutacji dla układu 256 par a/b wynosi zatem: wpisz ze wzoru str. 38

Liczba permutacji dla układu 31 par a/b wynosi: wpisz ze str. 38

Układ liczb nieparzystych zastosowanych w tej metodzie składa się z pięciu liczb, Metoda ZT-UNITAKOD zawiera 100 takich układów. Ogólna liczbę układów po 5 liczb możemy wyrazić wzorem: wstaw ze str. 38

Całkowita liczba permutacji;

Całkowitą liczbę permutacji tablicy „A" z uwzględnieniem zmiennej pozycji początku tablicy, możemy wyrazić wzorem:

$L_p = (N!)^{2N}$,

Gdzie N = 256 – dla kodu ASCII.

5.6 GENERATORY WYKORZYSTANE W METODZIE ZT-UNITAKOD

Teorią prawdopodobieństwa w sposób ścisły są związane generatory. Rozróżnia się dwa typy generatorów:

1. generatory programowe
2. generatory fizyczne

Z generatorów fizycznych w rzeczywistości warto wyróżnić dwa szczególne typy. Pierwszy to moneta. Rzut monetą daje możliwość losowego otrzymania orła lub reszki. Prawdopodobieństwo otrzymania jednego z nich wynosi ½. Zmienna losowa ma tutaj rozkład dwupunktowy przyjmując wartości albo 0 albo 1. Drugim typem jest urna z ponumerowanymi kartkami lub kulkami. Urnę taką będziemy nazywali generatorem liczb losowych o rozkładzie równomiernym. Użycie generatorów fizycznych, całkowicie losowych było by najlepszą metodą na kryptoanalityków, ponieważ większość ataków odbywa się właśnie na generatory i to one powinny być szczególnie bezpieczne. Jednak zastosowanie generatorów fizycznych nie jest możliwe z powodu tego, że nie udałoby się odszyfrować tak zaszyfrowanej wiadomośći.

Generatory programowe odgrywają dominującą role, chociaż w świecie rzeczywistym można znaleźć bardzo wiele generatorów fizycznych, których problem łączy się z brakiem stabilności. Generatory programowe są programami wykonanymi dla maszyn cyfrowych. Ten typ generatorów jest szczególnie często wykorzystywany w kryptografii szczególnie w szyfrowaniu informacji z powodu ich stabilności. Generatory programowe przyjmują następująca postać:

$$x_{n-1} = a_0 x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} + b \pmod{M},$$

wszystkie wartości są tutaj liczbami całkowitymi z przedziału (0 – M), są to tak zwane generatory liniowe. Szczególny przykładem generatorów liniowych, są generatory multiplikatywne, które wyrażają się wzorem:

$x_{n+1} = cx_n \pmod{M}$,

a generatora mieszanego:

$x_{n+1} = ax_n + b \pmod{M}$.

Każda liczba w ciągu (x_n) powtarza się dokładnie jeden raz, a ciąg x_n jest zbudowany ze skończonej liczby różnych znaków (liczb) n = 0,1,2,…. Długość takiego ciągu jest określona za pomocą liczby - K, która nazywa się okresem tego ciągu. Jeżeli w danym ciągu spełniony jest warunek K = M, to każda liczba ciągu pojawia się w określonej kolejności i ciąg ten staje się permutacją liczb (0, 1, 2, … , M – 1). Jeżeli K < M, to pojawiają się tylko niektóre liczby ciągu. Koniecznym przypadkiem jest zjawisko, gdzie K = M spełnienie tego warunku stało się koniecznością w czasie szyfrowania informacji, bo wtedy otrzymujemy określona permutacja ciągu.

ZASTOSOWANIE GENERATORA MULTIPLIKATYWNEGO

W metodzie ZT-UNITAKOD wymagana jest możliwość generowania permutacji ciągów (x_n), dla K = M, w których każda liczba (znak) pojawi się wyłącznie tylko jeden jedyny raz. W ZT-UNITAKOD zastosowano tablice kodów kryptograficznych, która ma możliwość szyfrowania informacji w oparciu o trzy rodzaje tablic:

- zerową,
- wyjściową,
- szyfrową.

Każda z tych tablic wymaga utworzenia odpowiedniej generacji za pomocą określonego generatora. Tablica kodów kryptograficznych może mieć rozmiary:

- 256 znaków stanowiących maksymalną liczbę możliwych kombinacji kodu ASCII.
- 145 znaków stanowiących wersję międzynarodowego kodu KOI-8.
- 60 znaków stosowanych w maszynach cyfrowych.
- 34 znaki, w tym 24 litery alfabetu łacińskiego oraz 10 cyfr.

Wartość liczbowa N mieści się w przedziale (34 – 256).

Ponadto w metodzie ZT-UNITAKOD jest spełniony warunek generowania odpowiedniej liczby permutacji wyrażonej wzorem:

$(W_z!)^W$

gdzie,

W_z - jest liczbą znaków z przedziału (34 – 256) zastosowaną w tej metodzie,

W - jest liczbą wierszy w tablicy.

Dla $W_z = W = 256$,otrzymujemy maksymalna liczbę permutacji równą $P = (256!)^{256}$. Ten warunek jest podstawowym warunkiem decydującym o wyborze określonego generatora permutacji.

Generator permutacji zastosowany w metodzie ZT-UNITAKOD opiera się o zasady generatora multiplikatywnego, dla którego dokonano określonych zmian:

Stała wartość „c" jest bardzo istotnym elementem wzoru generatora multiplikatywnego, multiplikatywnego jej wartość jest praktycznie obojętna, ale musza to być liczby całkowite z przedziału od 0 do M.

Przykładem może być rozpatrzenie wyników otrzymanych dla c = 4 i ciągu liczb: 1, 2, 3, …, 10. Wartość N = 10. po podstawieniu tych danych do wzoru otrzymujemy:

$$x_1 = 4 * 1 \pmod{10} = 4$$
$$x_2 = 4 * 2 \pmod{10} = 8$$
$$x_3 = 4 * 3 \pmod{10} = 2$$
$$x_4 = 4 * 4 \pmod{10} = 6$$
$$x_5 = 4 * 5 \pmod{10} = 0$$
$$x_6 = 4 * 6 \pmod{10} = 4$$
$$x_7 = 4 * 7 \pmod{10} = 8$$
$$x_8 = 4 * 8 \pmod{10} = 2$$
$$x_9 = 4 * 9 \pmod{10} = 6$$
$$x_{10} = 4 * 10 \pmod{10} = 0.$$

wynik:

1. $x_1 = x_6 = 4$,
2. $x_2 = x_7 = 8$,
3. $x_3 = x_8 = 2$,
4. $x_4 = x_9 = 6$,
5. $x_5 = x_{10} = 0$.

Nie otrzymaliśmy natomiast liczb 1, 3, 4, 7, 9, chociaż wystepują one w ciągu x_n.

Podobnie jest dla c = 6 itd. Można więc wyciągnąć wnioski:

- Otrzymujemy liczby parzyste zakończone okresem.
- Nie otrzymujemy liczb nieparzystych
- Nie został spełniony warunek pojawienia się każdej liczby tylko jeden jedyny raz

Analiza ta jednoznacznie wskazuje nam na to, że tak zaprogramowany generator nie może być stosowany dla parzystej wartości „c".

Rozpatrując wartości nieparzyste dla liczb „c" np. 9 otrzymujemy:

9, 8, 7, 5, 4, 3, 2, 1, 0. Jest to układ malejący w kolejności od 9 do 0.

Dla wartości c = 15 otrzymujemy:

5, 0, 5, 0, 5, 0, 5, 0, 5, 0. Jeżeli teraz za M podstawimy 20 a wartości c pozostawimy bez zmian w wyniku otrzymamy: 15, 10, 5, 0, 15, 10, 5, 0, 15, 10.

We wszystkich tych układach otrzymaliśmy liczby zmieniające się w okresach. Jednak i tutaj nie otrzymaliśmy satysfakcjonującego nas wyniku, liczby dalej się powtarzają.

Rozpatrujemy, więc działanie generatora dla liczb pierwszych. Za wartość „c" podstawiamy kolejne liczby pierwsze; 3, 7, 11, 13, 17 i dokonujemy obliczeń dla M = 10, 20 oraz np. 24.

Przykład 1.

Ciąg x_n = 1, 2, 3, …, 10. M = 10, c = 3 otrzymujemy:

$$x_1 = 3 * 1 \pmod{10} = 3$$
$$x_2 = 3 * 2 \pmod{10} = 6$$
$$x_3 = 3 * 3 \pmod{10} = 9$$
$$x_4 = 3 * 4 \pmod{10} = 2$$
$$x_5 = 3 * 5 \pmod{10} = 5$$
$$x_6 = 3 * 6 \pmod{10} = 8$$
$$x_7 = 3 * 7 \pmod{10} = 1$$
$$x_8 = 3 * 8 \pmod{10} = 4$$
$$x_9 = 3 * 9 \pmod{10} = 7$$
$$x_{10} = 3 * 10 \pmod{10} = 0.$$

Ciąg x_n = 1, 2, 3, …, 10. M = 10, c = 7 otrzymujemy:

$$x_1 = 7 * 1 \pmod{10} = 7$$
$$x_2 = 7 * 2 \pmod{10} = 4$$
$$x_3 = 7 * 3 \pmod{10} = 1$$
$$x_4 = 7 * 4 \pmod{10} = 8$$
$$x_5 = 7 * 5 \pmod{10} = 5$$
$$x_6 = 7 * 6 \pmod{10} = 2$$
$$x_7 = 7 * 7 \pmod{10} = 9$$
$$x_8 = 7 * 8 \pmod{10} = 6$$
$$x_9 = 7 * 9 \pmod{10} = 3$$
$$x_{10} = 7 * 10 \pmod{10} = 0.$$

Ciąg x_n = 1, 2, 3, …, 10. M = 10, c = 11 otrzymujemy:

$$x_1 = 11 * 1 \pmod{10} = 1$$
$$x_2 = 11 * 2 \pmod{10} = 2$$
$$x_3 = 11 * 3 \pmod{10} = 3$$
$$x_4 = 11 * 4 \pmod{10} = 4$$

$$x_5 = 11 * 5 \pmod{10} = 5$$
$$x_6 = 11 * 6 \pmod{10} = 6$$
$$x_7 = 11 * 7 \pmod{10} = 7$$
$$x_8 = 11 * 8 \pmod{10} = 8$$
$$x_9 = 11 * 9 \pmod{10} = 9$$
$$x_{10} = 11 * 10 \pmod{10} = 0.$$

Ciąg $x_n = 1, 2, 3, \ldots, 10$. M = 10, c = 13 otrzymujemy:

$$x_1 = 13 * 1 \pmod{10} = 3$$
$$x_2 = 13 * 2 \pmod{10} = 6$$
$$x_3 = 13 * 3 \pmod{10} = 9$$
$$x_4 = 13 * 4 \pmod{10} = 2$$
$$x_5 = 13 * 5 \pmod{10} = 5$$
$$x_6 = 13 * 6 \pmod{10} = 8$$
$$x_7 = 13 * 7 \pmod{10} = 1$$
$$x_8 = 13 * 8 \pmod{10} = 4$$
$$x_9 = 13 * 9 \pmod{10} = 7$$
$$x_{10} = 13 * 10 \pmod{10} = 0.$$

Ciąg $x_n = 1, 2, 3, \ldots, 10$. M = 10, c = 17 otrzymujemy:

$$x_1 = 17 * 1 \pmod{10} = 7$$
$$x_2 = 17 * 2 \pmod{10} = 4$$
$$x_3 = 17 * 3 \pmod{10} = 1$$
$$x_4 = 17 * 4 \pmod{10} = 8$$
$$x_5 = 17 * 5 \pmod{10} = 5$$
$$x_6 = 17 * 6 \pmod{10} = 2$$
$$x_7 = 17 * 7 \pmod{10} = 9$$
$$x_8 = 17 * 8 \pmod{10} = 6$$
$$x_9 = 17 * 9 \pmod{10} = 3$$
$$x_{10} = 17 * 10 \pmod{10} = 0.$$

Analizując otrzymane wynik stwierdzamy, że wszystkie założenia zostały spełnione. Ciąg x_n przyjmuje zróżnicowana postać uzależnioną od wartości „c". Każda liczba ciągu jest prezentowana jeden raz a cały ciąg kończy się wartością zerowa.

Przykład 2.

Ciąg $x_n = 1, 2, 3, \ldots, 10$. M = 20, wartości c = 3, 7, 11, 13, 17. W tym przypadku otrzymujemy wartości ciągu, które zostały zaprezentowane tylko jeden raz dla wybranej wartości „c". Każdy ciąg kończy się zerem.

Przykład 3.

Ciąg x_n = 1, 2, 3, …, 10. M = 24, wartości c = 3, 7, 11, 13, 17.

Po przeanalizowaniu wyników dochodzimy do wniosku, że dla wartości c =3 generator nie spełnia początkowych warunków, obliczenia dla M = 60 potwierdzają to samo zjawisko, dlatego ten generator nie nadaje się do zastosowania w metodzie ZT-UNITAKOD. Metoda ZT-UNITAKOD postawiła nieco odmienne wymagania na generator permutacji, którego postać można wyrazić następującym zapisem matematycznym:

$P = CX_n \pmod M$

gdzie:

C – jest to określona liczba pierwsza

M – określona liczba znaków zastosowana w tablicy kodów

X_n – ciąg liczb całkowitych

Wymagania postawione generatorowi permutacji zastosowanemu w metodzie ZT-UNITAKOD można przedstawić w dwóch punktach:

1. Liczba M musi zawierać się w przedziale od 24 do 256 i musi być określoną wartością dla danego szyfru. Najczęściej są to wielkości związane z międzynarodowym kodem, mianowicie:
   - 24 – liczba znaków alfabetu
   - 34 – liczba znaków alfabetu i cyfr
   - 60 – minimalna liczba znaków zastosowanych w komputerach
   - 145 – międzynarodowa wersja kodu ośmiobitowego
   - 256 – maksymalna liczba możliwych kombinacji w kodzie międzynarodowym
2. Liczba C musi być określoną liczbą pierwszą spełniająca poniższe trzy warunki:
   - $(C * X_i) \bmod M \neq 0$ dla i = 1, 2, … , M -1
   - $(C * X_i) \bmod M = 0$ dla i = M
   - $(C * X_i) \bmod M \neq (C * X_j) \bmod M$, jeżeli $X_i \neq X_j$

Całość można opisać następującym wzorem:

$S_{wk} = (a_{xz} + b_{ij}) \bmod N$,

gdzie:

a_{xz} – tablica kodów kryptograficznych tworzona za pomocą generatora permutacji: $P = CX_n \pmod M$

N – liczba znaków zastosowanych w określonych zasadach szyfrowania.

Tylko tak opisany generator miał prawo pojawić się w metodzie ZT-UNITAKOD, ponieważ spełnia on wszystkie warunki założone w fazie projektowania metody.

Co prawda generatory programowe nie wybierają poszczególnych liczb w sposób całkowicie losowy, lecz pseudolosowy, ale tylko taki sposób wybierania liczb daje nam możliwość odszyfrowania ciągu szyfrowego.

1.7 ZASTOSOWANIE METODY JEDNORAZOWEGO KLUCZA DYNAMICZNEGO

Metody szyfrowania mogą być stosowana dla następujących przypadków;

1. Przy szyfrowaniu autonomicznym - na jednym komputerze
2. Przy szyfrowaniu na kierunku (jeden nadawca i jeden adresat)
3. Przy szyfrowaniu w sieci (jeden nadawca wielu adresatów)
4. Szyfrowanie „w locie" (możliwość szyfrowania baz danych w dowolnym czasie i wyszukiwania informacji zaszyfrowanych różnymi rodzajami szyfrów, czyli szyfrowanych w różnych czasach)
5. Sprzętowa realizacja szyfrowa

Metoda ZT-UNITAKOD może być stosowana:

1. Szyfrowaniu bezpośrednim
2. Jako szyfrująca nakładka programowa
3. Do szyfrowania „w locie"
4. Hardware

2. WYBÓR KRYTERIÓW I METOD OCENY JAKOŚCI SZYFROWANIA.

Wybór kryteriów do oceny metod szyfrowania zawsze rodzi pewne kontrowersje. Dla części użytkowników najważniejsza jest np. szybkość danej metody, dla kogoś innego może być to na przykład niezawodność, jaką ona gwarantuje a dla jeszcze kogoś innego może to być chociażby cena lub prostota w obsłudze. Wybór jest dość trudną sprawą i indywidualną danego analityka takiej metody.

Z powodu tego, że metody statyczne w szczególności metoda RSA, którą zaprezentowałem w mojej pracy jest zupełnie inna niż metoda ZT-UNITAKOD, nie sposób jest jednoznacznie podać wszystkie najlepsze kryteria, jakie powinny obie te metody spełniać. Dla mnie najważniejsze jest to by poszczególne metody cechowały się następującymi właściwościami:

1. Szybkość metody,
2. Bezpieczeństwo,
3. Prostota obsługi,
4. Niezawodność,
5. Niezależność.

Uważam, że tych sześć kryteriów, jakie wybrałem do analizy i porównania metod szyfrowania statycznego z nowatorską metodą dynamiczną w zupełności zaspokoi każdego chętnego sięgnąć i przeczytać moją pracę.

Rozumienie poszczególnych kryteriów:

a) Szybkość metody – pojęcie to jest dość względne, dla jednej osoby metoda szybka w sowim działaniu to ta, której czas pozwalający na zaszyfrowanie np. jednego megabajta informacji wynosi dwie sekundy a dla kogoś innego np. 0,003 sekundy. Dla mnie szybkość metody charakteryzuje czas rzędu setnych sekundy. Bardzo ważną rzeczą jest by prezentowane metody szyfrowania informacji były możliwe np. do szyfrowania mowy ludzkiej w telefonii cyfrowej.

b) Bezpieczeństwo – pod tym pojęciem rozumiemy wytrzymałość na złamanie przechwyconego szyfrogramu, lub samej metody. W metodach statycznych bezpieczeństwo metody ściśle było związane z mocą kryptograficzną danej metody, co w szczególności wiązało się z mocą kryptograficzną klucza zastosowanego w danej metodzie. Dynamiczna metoda ZT-UNITAKOD zmieniła sposób patrzenia na bezpieczeństwo danej metody, ponieważ nie stosuje się tu żadnych kluczy statycznych, co jednoznacznie zmienia sposób podejścia do bezpieczeństwa gwarantowanego w tej metodzie.

c) Prostota – to trzecie bardzo ważne kryterium oceny poszczególnych metod. Prostota w dzisiejszym świecie jest jedną z najważniejszych rzeczy, ponieważ gwarantuje ona w pewien sposób to, że ludzie mający możliwość korzystania z danej metody będą w rzeczywistości korzystać z niej. Na rynku istnieje wiele nakładek na systemy operacyjne poprawiających bezpieczeństwo lub „łatających" pewne niedopatrzenia wynikłe podczas używania tych metod. Mogą to być niedopatrzenia powstałe już w fazie powstawania projektów jak i te, które popełniają programiści. Jednak bardzo nieliczna grupa ludzi stosuje tego typu rozwiązania, ponieważ często wiążą się one z pewnym poświęceniem swojego czasu na instalacje, później na aktualizowanie itd. Prostota danej metody gwarantuje nam przyjęcie jej przez szerokie grono ludzi korzystających ze sprzętu informatycznego.

d) Niezawodność – niezawodność jest tym ważniejsza, że podczas szyfrowania informacji nie może być mowy o możliwości np. opuszczenia części szyfrowanego tekstu jawnego (jednego z jego bloków), lub „wykrzaczenia" się metody podczas przesyłania na przykład uwierzytelnienie do banku.

e) Niezależność metody - ten aspekt staje się podstawą w szyfrowaniu informacji. Metoda nie powinna zależeć od decydującej roli człowieka. Metoda powinna szyfrować dowolny język świata. Powinna też móc szyfrować schematy, obrazy, zdjęcia satelitarne, bazy danych itd. To wszystko wskazuje na niezależność metody. Metoda powinna być też tak skonstruowana, żeby nawet sam autor nie mając szyfrogram i część tekstu jawnego nie umiał rozszyfrować takiej metody. Spełnienie wszystkich tych zależności daje nam podstawy do sądzenia, że dana metoda jest naprawdę niezależna.

Informacja dla Autorów

Redakcja **„PROSOPON”** zaprasza do współpracy Autorów, którzy chcieliby publikować swoje teksty na łamach naszego pisma. Uprzejmie informujemy, że przyjmujemy do publikacji artykuły nie dłuższe niż 20 stron znormalizowanego maszynopisu (1800 znaków ze spacjami na stronę), a w przypadku recenzji – niż 8 stron. Do artykułów prosimy dołączyć streszczenie w języku polskim i angielskim (wraz z angielskim tytułem artykułu) o objętości do 200 słów. Prosimy o niewprowadzanie do manuskryptów zbędnego formatowania (np. nie należy wyrównywać tekstu spacjami czy stosować zróżnicowanych uwypukleń, wyliczeń itp.). Sugerowany format: czcionka Arial, 12 pkt., interlinia 1,5. Piśmiennictwo zawarte w artykule należy sformatować zgodnie z tzw. zapisem harwardzkim, zgodnie z którym lista publikacji istotnych dla artykułu ma być zamieszczona na jego końcu i ułożona w porządku alfabetyczny. Publikacje książkowe należy zapisywać:

Fijałkowska B., Madziarski E., van Tocken T.L. jr., Kamilska T. (2014). Tamizdat i jego rola w kulturze radzieckiej. Warszawa: Wydawnictwo WSM.

Rozdziały w publikacjach zwartych należy zapisywać:

Bojan A., Figurski S. (2014). Nienowoczesność – plewić czy grabić. W.S. Białokozowicz (red.), Nasze czasy – próba syntezy. Warszawa: Wydawnictwo WSM.

Artykuły w czasopismach należy zapisywać:

Bobrzyński T.A. (2009). Depression, stress and immunological activation. British Medical Journal 34 (4): 345-356.

Materiały elektroniczne należy zapisywać:

Zientkieicz K. Analiza porównawcza egocentryka i hipochondryka. Żart czy parodia wiedzy? Portal Naukowy “Endo”. www.endo.polska-nauka.pl (data dostępu: 2014.07.31).

W tekście artykułu cytowaną publikację należy zaznaczyć wprowadzając odnośnik (nazwisko data publikacji: strony) lub – gdy przywołane jest nazwisko autora/nazwiska autorów w tekście – (data publikacji: strony), np.: Radzieckie władze „[…] podjęły walkę z tamizdaten na dwóch płaszczyznach: ideologicznej i materialnej” (Fijałkowski i wsp. 2014: 23). lub: Radziecka prasa, jak stwierdzają Fijałkowski i wspólnicy, „lżyła autorów druków bezdebitowych” (2014: 45). W przypadku przywoływanych tekstów, gdy nie ma bezpośredniego cytowania, należy jedynie podać nazwisko i rok publikacji (bądź sam rok, jeśli nazwisko autora pada w tekście głównym). W odnośnikach w tekście głównym należy w przypadku więcej niż dwóch autorów wprowadzić „i wsp.”, np. (Fijałkowski i wsp. 2014). W tekście piśmiennictwa (tj. alfabetycznie ułożonej literaturze) prosimy wymienić wszystkich autorów danej publikacja. Więcej o zasadach stylu harwardzkiego m.in. na Wikipedii (http://pl.wikipedia.org/wiki/Przypisy_harwardzkie). Uwaga, przypisy krytyczne, inaczej tzw. aparat krytyczny, prosimy w miarę możliwości zredukować do minimum i wprowadzać do głównego tekstu manuskryptu.

Zaznaczamy, że Redakcja nie płaci honorariów, nie zwraca tekstów niezamówionych oraz rezerwuje sobie prawo do skracania tekstów.

Teksty prosimy przesyłać drogą elektroniczną za pomocą formularza na stronie WWW: http://humanum.org.pl/czasopisma/humanum/o-czasopismie lub na adres e-mailowy: biuro@humanum.org.pl

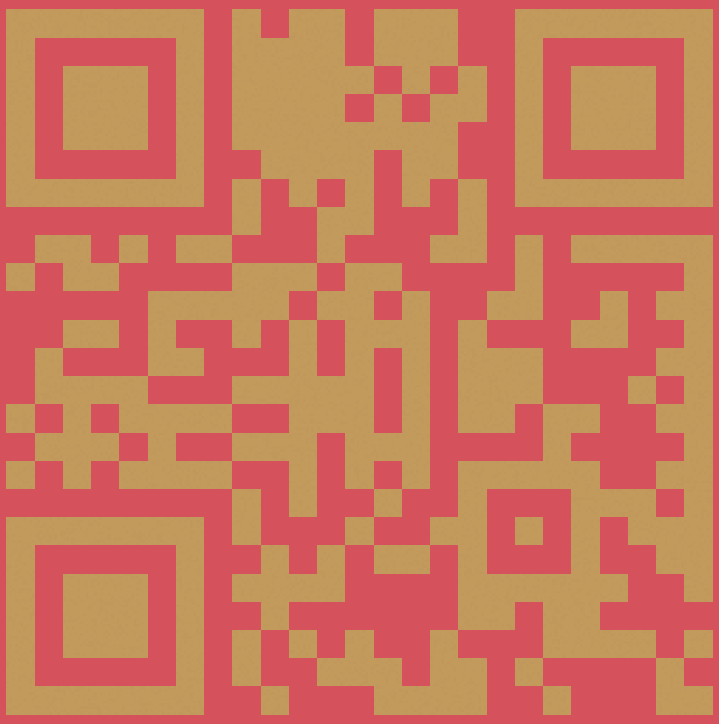
Do tekstu należy dołączyć informację o aktualnym miejscu zamieszkania, nazwie i adresie zakładu pracy, tytule naukowym, stanowisku i pełnionych funkcjach. Każdy tekst przesłany pod adres Redakcji z prośbą o druk na łamach czasopisma podlega ocenie. Proces recenzji przebiega zgodnie z założeniami „double blind” peer review (tzw. podwójnie ślepej recenzji). Do oceny tekstu powołuje się co najmniej dwóch niezależnych recenzentów (tzn. recenzent i autor tekstu nie są ze sobą spokrewni, nie występują pomiędzy nimi związki prawne, konflikty, relacje podległości służbowej, czy bezpośrednia współpraca naukowa w ciągu ostatnich 5 lat). Recenzja ma formę pisemną i kończy się stwierdzeniem o dopuszczeniu lub niedopuszczeniu tekstu do druku.

W związku z przypadkami łamania prawa autorskiego oraz dobrego obyczaju w nauce, mając na celu dobro Czytelników, uprasza się, aby Autorzy publikacji w sposób przejrzysty, rzetelny i uczciwy prezentowali rezultaty swojej pracy, niezależne od tego, czy są jej bezpośrednimi autorami, czy też korzystali z pomocy wyspecjalizowanego podmiotu (osoby fizycznej lub prawnej).

Wszystkie przejawy nierzetelności naukowej będą demaskowane, włącznie z powiadomieniem odpowiednich podmiotów (instytucje zatrudniające Autorów, towarzystwa naukowe itp.).

Do przedłożonych tekstów z prośbą o druk, Autor tekstu jest zobowiązany dołączyć:

1. Informację mówiącą o wkładzie poszczególnych Autorów w powstanie publikacji (z podaniem ich afiliacji oraz kontrybucji, tj. informacji, kto jest autorem koncepcji, założeń, metod, protokołu itp. wykorzystywanych przy przygotowaniu publikacji), przy czym główną odpowiedzialność ponosi Autor zgłaszający manuskrypt.
2. Informację o źródłach finansowania publikacji, wkładzie instytucji naukowo-badawczych, stowarzyszeń i innych podmiotów.



HUMANUM Instytut Studiów Międzynarodowych
i Edukacji w Warszawie