

М. ТЫНЫШБАЕВ атындағы
ҚАЗАҚ КӨЛІК ЖӘНЕ КОММУНИКАЦИЯЛАР АКАДЕМИЯСЫНЫҢ

ХАБАРШЫСЫ

ВЕСТНИК

Казахской академии транспорта
и коммуникаций имени
М. Тынышпаева

The BULLETIN

of Kazakh Academy of Transport
and Communications named
after M. Tynyshpayev



Редакция алқасы

Б.Е. Аркенов (т.ғ.к.) –
бас редакторы
С.Е. Бекжанова
(т.ғ.д., профессор) –
бас редактордың
орынбасары
А.К. Ибраимов
(т.ғ.к., доцент)
Г.С. Мусаева (т.ғ.д.,
проф.)
В.Г. Солоненко
(т.ғ.д., проф.)
М.С. Кульгильдинов
(т.ғ.д., проф.)
С.Е. Бекжанова
(т.ғ.д., проф.)
М.С. Изтелеуова
(т.ғ.д., проф.)
Т.К. Койшиев (т.ғ.д.,
проф.)
А.К. Калтаев (э.ғ.к.,
доцент)
О.И. Чуркина (ф.-
м.ғ.к., доцент)
А.Айтбайқызы -
техникалық редактор

Редакция мекен- жайы:

Қазақстан
Республикасы,
050012, Алматы қ.,
Шевченко көшесі, 97.

Тел./факс: +7 (727)
292-49-14, 292-44-85

E-mail:
vestnik@kazatk.kz

Сайт: www.kazatk.kz

Жекеменшік –
«М.Тынышбаев
атындағы Қазақ көлік
және
коммуникациялар
академиясы» АҚ

«Транзитивті экономика шектерінде логистикалық орталықтың қалыптасу әдістері	
А.Е. Тойлыбаев, Н.К. Булатов, У.А. Усипбаев.....	113-122
КМ ТРАНКО» ЖШС көліктік – логистикалық орталық (КЛО) ретінде жұмысын талдау және Қазақстан Республикасында КЛО даму перспективалары	
С.С. Абдуллаев, Ж.С. Сейдеметова, А.С. Абдуллаева.....	123-129
Қорғалатын көп нүктелі Wimax желісінде IPSEC бойынша VPN–нің динамикалық масштабталуын бағалау	
Ж.Ж. Ахметова, Ж.А. Сейтенова.....	130-138
“SMART HOME” -да заттар интернетінің өзара қарым-қатынасы үшін байланыс хаттамаларының стандарттарын қолдану	
А.Ш.Хасенов, Ж.Ж.Ахметова.....	138-144
Әлеуметтік желілерде қауымдастықтарды талдау	
А.Ж. Ахметова, Л.Л. Ла.....	144-149
Латане әлеуметтік ықпал теориясы және оның әлеуметтік желілердегі ақпараттарға қолданылуы	
А.Ж. Ахметова, Л.Л. Ла, Ф.А. Мурзин.....	149-156
Сөйлеулерді тануда нейрондық желіні қолдану	
О.Ж.Мамырбаев, Н.О.Мекебаев, М. Тұрдалыұлы.....	156-162
Машиналық оқыту базасына негізделіп шешім қабылдау жүйесін дамыту	
А.С. Савченко, С. Кенжеханұлы, Ж. Ж. Омирбекова, А.Е. Калабаева.....	163-169
Қазақ тіліндегі мәтіндердегі қылмыстық мәнді коллакцияларды анықтау	
О.Ж.Мамырбаев, Н.Ф. Хайрова, Қ.Ж.Мухсина.....	170-175
Кедергіге орнықты оралған кодтарды зерттеу	
Ж.К. Кенжебек, А.Д. Адамова, Ж.О. Оралбекова.....	176-182
Ашық жүйелерде тұлғаның биометриялық идентификациясының алгоритмін зерттеу және әзірлеу	
Ф.У Маликова, А.Б. Баймуханова, Г.А. Омарбекова.....	183-189
Үздіксіз өндірістегі ресурстарды тиімді үлестіру	
А.С. Бижанова, А.Д. Нұрланбек, А.Ж Молдакалыкова.....	189-194
Логистикалық жүйелердің модельдері мен әдістерін әзірлеу	
Л. С. Кунтунова, М.А. Сыдыбаева, А.И. Наурызбаева.....	194-202
Семантикалық рөлдер және семантикалық шектеулер	
А.Б. Касекеева, А.С. Еримбетова, Э.Н. Дайырбаева.....	203-207
Блокчейн технологиясы арқылы өнімдерді тексеру үшін арналған қолданбаны әзірлеу	
К.С. Дуйсебекова, Б. А. Тукибаев.....	208-214
Оқыту және аттестаттау жүйесінің сипаттамасы ретінде энтропиялық тәсілді зерттеу	
В.П. Куликов, А.С. Казанбаева, К.Е. Икласова.....	214-222
Жұмыс уақытын есепке алу Web қосымшасын құру үдерістері	
Ж.С. Исмагулова, А.Н. Нургулжанова, Т.Г. Назарбаев.....	223-228
Фонон кристалдардың сипаттамасы	
Г.М. Баенова, А.К. Жумадиллаева.....	229-235
«MODNPSS14» шифрлау алгоритміне криптографиялық талдау	
Д. Дюсенбаев, К. Алғазы, Қ. Сақан, А. Хомпыш.....	235-243
CISCO телефониясында қауіпсіздік шаралары	
А.Б. Матаева, А.А.Иванов, А.Б.Емберген.....	243-248

**Редакционная
коллегия**

Б.Е. Аркенов (к.т.н.),
главный редактор
С.Е. Бекжанова
(д.т.н., профессор),
зам. главного
редактора
А.К. Ибраимов
(к.т.н., доцент)
Г.С. Мусаева (д.т.н.,
проф.)
В.Г. Солоненко
(д.т.н., проф.)
М.С. Кульгильдинов
(д.т.н., проф.)
С.Е. Бекжанова
(д.т.н., проф.)
М.С. Изтелеуова
(д.т.н., проф.)
Т.К. Койшиев (д.т.н.,
проф.)
А.К. Калтаев (к.э.н.,
доцент)
О.И. Чуркина (к. ф.-
м.н., доцент)
А. Айтбайқызы –
технический
редактор

Адрес редакции:

Республика
Казахстан, 050012,
г. Алматы,
ул. Шевченко, 97.

Тел./факс:
+7 (727) 292-49-14,
292-44-85

E-mail:
vestnik@kazatk.kz

Сайт: www.kazatk.kz

Собственник – АО
«Казахская
академия
транспорта и
коммуникаций
имени
М. Тынышпаева»

**Методы формирования логистического центра в границах
транзитивной экономики**

А.Е. Тойлыбаев, Н.К. Булатов, У.А. Усипбаев..... 113-122

**Анализ работы ТОО «КМ ТРАНКО» как транспортно-
логистического центра (ТЛЦ) и перспективы развития
ТЛЦ в Республике Казахстан**

С.С. Абдуллаев, Ж.С. Сейдеметова, А.С. Абдуллаева..... 123-129

**Оценка масштабируемости защищенной многоточечной
динамической VPN по IPSEC в сети Wimax**

Ж.Ж. Ахметова, Ж.А. Сейтенова..... 130-138

**Применение стандартных протоколов связи для
взаимодействия Интернета вещей в “SMART HOME”**

А.Ш.Хасенов, Ж.Ж.Ахметова..... 138-144

Анализ сообществ в социальных сетях

А.Ж. Ахметова, Л.Л. Ла..... 144-149

**Теория Латане социального влияния и ее применение для
анализа данных из социальных сетей**

А.Ж. Ахметова, Л.Л. Ла, Ф.А. Мурзин..... 149-156

Использование нейронной сети в распознавании речи

О.Ж.Мамырбаев, Н.О.Мекебаев, М. Турдалыулы..... 156-162

**Разработка системы поддержки принятия решений на базе
машинного обучения**

А.С. Савченко, С. Кенжеханулы, Ж. Ж. Омирбекова,
А.Е. Калабаева..... 163-169

**Идентификация криминально значимых коллокаций в
казахскоязычных текстах**

О.Ж.Мамырбаев, Н.Ф. Хайрова, Қ.Ж.Мухсина..... 170-175

Исследование помехоустойчивых свёрточных кодов

Ж.К. Кенжебек, А.Д. Адамова, Ж.О. Оралбекова..... 176-182

**Исследование и разработка алгоритма биометрической
идентификации личности в открытых системах**

Ф.У Маликова, А.Б. Баймуханова, Г.А. Омарбекова..... 183-189

**Оптимальное распределение ресурсов в непрерывном
производстве**

А.С. Бижанова, А.Д. Нұрланбек, А.Ж Молдакалыкова..... 189-194

Разработка моделей и методов логистических систем

Л. С. Кунтунова, М.А. Сыдыбаева, А.И. Наурызбаева..... 194-202

Семантические роли и семантические ограничения

А.Б. Касекеева, А.С. Еримбетова, Э.Н. Дайырбаева..... 203-207

**Использование технологии блокчейн при разработке
приложения для верификации товаров**

К.С. Дуйсебекова, Б. А. Тукибаев..... 208-214

**Исследование энтропийного подхода как характеристики
системы обучения и аттестации**

В.П. Куликов, А.С. Казанбаева, К.Е. Икласова..... 214-222

**Процесс разработки Web-приложения по учету рабочего
времени**

Ж.С. Исмагулова, А.Н.Нургұлжанова, Т.Г. Назарбаев..... 223-228

Характеристики фононных кристаллов

Г.М. Баенова, А.К. Жумадиллаева..... 229-235

**Криптографический анализ алгоритма шифрования
«MODNPSS14»**

Д. Дюсенбаев, К. Алгазы, К. Сакан, А. Хомпыш..... 235-243

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ РАЗРАБОТКЕ ПРИЛОЖЕНИЯ ДЛЯ ВЕРИФИКАЦИИ ТОВАРОВ

Дуйсебекова Кулянда Сейтбековна, кандидат физико-математических наук, доцент кафедры «Информационные системы», Международный университет информационных технологий, dkulan1@mail.ru.

Тукибаев Бейбут Айдарович, магистрант кафедры «Информационные системы», Международный университет информационных технологий, beibit.tukibaev@gmail.com.

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ АРҚЫЛЫ ӨНІМДЕРДІ ТЕКСЕРУ ҮШІН АРНАЛҒАН ҚОЛДАНБАНЫ ӘЗІРЛЕУ

Дуйсебекова Кулянда Сейтбековна, физика-математика ғылымдарының кандидаты, Ақпараттық жүйелер кафедрасының доценті, Халықаралық ақпараттық технологиялар университеті, dkulan1@mail.ru.

Тукибаев Бейбут Айдарович, "Ақпараттық жүйелер" кафедрасының магистранты, Халықаралық ақпараттық технологиялар университеті, beibit.tukibaev@gmail.com

Аңдатпа: Бұл мақалада блокчейн технологиясы, оның жұмыс істеу принципі және қолдану салалары қарастырылған.

Блокчейн алғашқы рет биткойн ұғымымен бірге пайда болды, бірақ қазіргі таңда оның қолданылуы криптовалюта саласымен ғана шектелмейді. Блокчейннің деректерді қауіпсіз түрде сақтау ерекшелігі аутентификация мен верификацияға арналған платформаларды құруды мүмкін береді.

Осы мақалада өнімдерді верификациялауға арналған қолданба әзірлеуінің үдерісі қарастырылған. Ашық және жабық кілттер инфраструктурасы және криптографикалық алгоритмдер көмегімен өнім туралы деректерді енгізу үшін арналған қолданба құрылған. Ол қолданба ашық кілт және сандық қолданба көмегімен енгізілген деректерді тексеріп, блокчейн торына қосады. Мобильді қолданба көмегімен кез келген пайдаланушы өнім туралы деректерді оның штрих-коды арқылы тексере алады.

Түйін сөздер: блокчейн, хеш функциялар, криптография, ашық кілт, жабық кілт, сандық қолданба, майнинг.

Статья поступила в редакцию 05.06.19. Актуализирована 16.09.19. Принята к публикации 27.09.19.

The Bulletin of Kazakh Academy of Transport and Communications named after M. Tynyshpayev
ISSN 1609-1817
Vol. 110, No.3 (2019), pp.214-222

THE STUDY OF ENTROPY APPROACH THE CHARACTERISTICS OF THE TRAINING AND CERTIFICATION SYSTEM

Kulikov Vladimir Pavlovich, candidate of physical and mathematical Sciences, Professor Department of information and communication technologies, M. Kozybayev North Kazakhstan State University, Petropavlovsk, Kazakhstan, qwertyrant@mail.ru

Kazanbayeva Albina Sovetovna, doctoral student, Department of information and communication technologies, M. Kozybayev North Kazakhstan State University, Petropavlovsk, Kazakhstan, akazanbaeva83@mail.ru

Iklassova Kainizhamal Esimseitovna, doctoral student, Department of information and communication technologies, M. Kozybayev North Kazakhstan State University, Petropavlovsk, Kazakhstan, kiklasova@mail.ru

Kulikov V.P.¹, Kazanbayeva A.S.¹, Iklassova K.E.¹

¹Manash Kozybayev North Kazakhstan State University, Petropavlovsk, Kazakhstan

THE STUDY OF ENTROPY APPROACH THE CHARACTERISTICS OF THE TRAINING AND CERTIFICATION SYSTEM

Abstract. Recently, many publications have been issued on improving the quality of education and the need to introduce unbiased assessment of this quality. Often, assessments of the training/education quality are considered both in a simplified and traditional way. The discourse is mainly related to assessing only the individual achievements of students and to the procedures of licensing, certification and accreditation of educational institutions. The problem of assessing the quality of higher education is much deeper and serious. This article proposes to form characteristics of the educational achievements quality through an entropy approach. The objective of the research outlined in this article is to solve the problem using the example of the “entropy” scheme of correction of the concept of educational achievements external assessment (or other large-scale testing of knowledge) based on the results and analysis of outcomes of the regular student sessions. Also in this paper we studied the problems of development of evaluation of learning results by testing.

For any educational institution of the Republic of Kazakhstan (not statistically confirmed but derived from the personal experience of the authors), model assumptions are specified as follows:

A) As a rule, all three control subsystems: input (dropout), current (regular) and output (final) are implemented. Here we should note that “unloading” of the process recording for data processing, as a rule, represents a separate problem.

B) As a rule, “elimination of ballast” documents is either not performed or does not have any cause-effect relations with ensuring the declared quality of subsystems functioning.

C) As a rule, the pool of documents passively reaches some level of redundancy in an it-happened-accidentally way.

Key words: training system, test management, quality assessment, control, entropy, educational achievements.

Introduction

The system of testing the training results has been transformed in the direction of quality control of education. It should be emphasized that the introduction of innovative educational technologies in continuing education is becoming an increasingly effective tool for professional development.

Tests can be used at any stage of training. Some of them are designed to assess the readiness of students to learn a new training course, others are aimed to identify specific gaps in knowledge of students in order to plan the necessary targeted corrective work, and some are used to predict the further learning process. Basic testing includes input, current and progress checks, and interim certification for each discipline, including

external evaluation of educational achievements (VOUD) and state final certification.

The problems of formal description of training system processes and certification through testing approach were considered in the studies of J. Julliand, O. Kouchnarenko, P. A. Masson, G. Voironin Test Generation from Event System Abstraction to Cover Their States and Transition; H. Bride and J. Julliand, P. A. Masson in Tri-modal Under-Approximation for Test Generation; P. Godefroid in Compositional Dynamic Test Generation; P.-C. Bué, J. Julliand and P. A. Masson Association of Under-Approximation Techniques for Generating Tests from Models; P. Godefroid, N. Klarlund and K. Sen in DART: Directed Automated Random

Testing; N. Tillmann and J. DeHalleuxin Pex-White Box Test Generation for NET[1], [2], [3], [4], [5], [6], as well as at the presentation of R. Majumdar and K. Sen at the international conference with the thesis of Hybrid Concolic Testing [7].

Calculation of entropy and studies in this field have been examined in the following papers: C. E. Shannon, A Mathematical Theory of Communication; C. E. Shannon, N. Sloane, A. Wyner, Collected Papers; I. V. Toranzo, J. S. Dehesa, Exact Shannon Entropies for the Multidimensional Harmonic States; C. Tsallis, Possible Generalization of Boltzmann-Gibbs Statistics; P. A. Bromiley, Shannon Entropy, Renyi Entropy, and Information [8], [9], [10], [11], [12]. Besides A. Arnold, J. Antonio Carrillo, L. Desvillettes, J. Dolbeault, A. Jüngel, L. Claudia, P. A. Markowich, G. Toscani and C. Villani in their work called Entropies and Equilibrium of Many-Particle Systems: An Essay on Recent Research stated that in recent years entropy methods have proved to be effective as a tool for understanding the qualitative properties of physically based models, for exact numbers and for a more mathematical understanding of nonlinear partial differential equations [13].

Informational entropy

Complex socio-informational systems have, as a rule, a developed document management structure. At the same time, they support it following traditional approaches, evolving from paper-based technologies to paperless ones, preserving the corresponding rudiments (for example, paper consumption tends to increase).

It's interesting to consider a whole range of issues on analysis and construction of the document flow of an optimal structure for the subject area which uses the appropriate pool of documents as if the evolution has already occurred, or the system is initially optimal in a system-wide sense.

Let's consider the training system from a general perspective including the following subsystems:

- input control (drop-out);
- current (regular) control;
- output (final) control.

We shall introduce here assumptions/presumptions of the model.

A) At least one of the subsystems must be implemented and regularly operated. In other words it is possible to keep processes records in the form of both a documentary cross-section at a particular time and a series (versions) of documents that have evolved over time.

B) not only the subjects of training, but also the documents used in the processes are subject to dropout if those have not provided the necessary level within the relevant subsystem.

C) The pool of documents has exactly such redundancy that is actually applied one way or another (irrelevant documents are applied with zero-probability, i.e. they are actually absent).

So, out of all documents $N(t)$ only a part of documents of certain volume $n_{ij}(t)$ is used simultaneously or in a time series (session).

Symbols options:

- the first index marks the subject and the second goes to a series in which the corresponding volume of documents is applied;

- the first index marks the time sample and the second corresponds to the subject to which the corresponding volumes of documents at this stage (time sample) were applied.

A reasonable assumption on ergodicity makes it possible to identify the averaging over time and over the ensemble. Moreover, stationary ergodicity makes it possible to identify a) the average characteristics determined on the basis of observation of many similar systems at the same time, and b) the time averages determined on the basis of observation of one of these systems for a sufficiently large number of subsequent moments of time. Hence the interpretation of n_{ij} indices is of no importance for the systems that behave themselves stationary-ergodic, as the average for time or for the observations ensemble shall match.

On determining the intensities $p_{ij}(t) = \frac{n_{ij}(t)}{N(t)}$, $\sum_{ij} p_{ij} = 1$, we formulate the

ideal behavior of the system as the evolution of the entropy S of the document application $S \rightarrow \text{extr}$, subject to all the rules of the subsystem functioning.

Control systems are accompanied by the formation of indicators reflecting the content of control, expressed in quantitative form. This means that there is always a set of indicators in the volume R , given in the form of functions of some qualitative characteristics of the processes, $f_r(x_{ij}), r=\overline{1, R}$, where x_{ij} is the content-based characteristics of the interaction of subject i with the flow of documents j of the described subsystem. Characteristics of x_{ij} in integrated form are important to the system for decision-making on subsystem improvement. Usually the average characteristics E_r are available (or assigned). Then the optimization problem can take the form: $S \rightarrow \max \sum_{ij}^N p_{ij} f_r(x_{ij}) = E_r$ for any $r, r=\overline{1, R} \sum_{ij}^N p_{ij} = 1$.

The solution of the problem (in terms of assessing the entropy of document flow in the system) will determine the plan of intensity of documents application based on the achievement of the planned indicators.

A typical solution of the above problem involves the introduction of the Lagrange function with undefined multipliers (we take into account all R requirements). The Lagrange function with undetermined multipliers of Lagrange α, β_r is as follows: $L(p_{ij}, \alpha, \beta_r) = S - \alpha(\sum_{ij}^N p_{ij} - 1) - \sum_r \beta_r (\sum_{ij}^N p_{ij} f_r(x_{ij}) - E_r)$.

The distribution of p_{ij} by the criterion of the entropy extremum is the solution of a set of differential equations: $\frac{\partial L}{\partial p_{ij}} = 0$ Entropy

S can be explicitly written in the way of Shannon, Tsallis or Renyi[14].

The complexity of the study of this coupling of Lagrange multipliers is determined by the non-triviality of dependence of $f()$, which introduced a single indicator E . On receiving a couple of Lagrange multipliers that are calculated, for example, using approximate approaches, it is possible to clearly identify all milestone volumes of documents in a stable control system in each

moment of time (or the layout of volumes into the subjects of control), and also to predict how the indicator E will affect the status of any of the subject (document) in the subsystem.

As a rule, testology and paper examination are based on the equally probable distribution of exam questions/tasks. Specifically, there are test tasks/questions that are almost unclaimed, there are no statistics on them, and, accordingly, it is statistically impossible to assess their quality with all the ensuing risks of dropout and control errors.

And as long as $\sum_{ij}^N p_{ij} = 1$, then on defining $E = \sum_{ij}^N p_{ij} f(x_{ij})$ we finally get the coupling formula (q, E, α, β):

$$\frac{1}{1-q} = \alpha + \beta E \quad (1)$$

Reading:

E – indicator;

q – Renyi factor;

α – Lagrange multiplier for intensity metering;

β – Lagrange multiplier for indicator metering;

the coupling formula (q, E, α, β) literally means that the only quality indicator “averagely” can be successfully replaced by the Renyi entropy parameter.

Moreover, allowing the selection of α and β when $q=0$, the entropy can be considered as “structural” and actually expressed by the formula $S = \log N$. It would be a Hartley formula if we took equal probability distribution p_{ij} (as in the case of Shannon formula and, as mentioned above, due to the usual practice in the examination or test control). However, here it is only a coincidence due to the “appropriate” division of the subsystem documents structure and it does not imply equal intensity.

Besides:

- declaring the Renyi entropy with $q=0$;

- reducing the volumes of documents (proportionally increasing their number) of the subsystem under the scale parameter ϵ in such a manner that the entire document pool can still be associated with indices indicating

the connection of sub-documents of different volumes with the newly split evaluation procedures;

- assuming the existence of a numerical limit indicating the generalized Renyi fractal dimension we obtain the Hausdorff dimension characterizing the fractality of the structure of the evaluation documents subsystem[15]. This fractality of documents pool is uniquely useful for efficient scaling of materials for evaluation with increasing number of subjects or number of sets.

Aim of the entropy correction

Let's consider the subsystem of External Evaluation of Educational Achievements (VOUD):

- 4 sets of tasks for 25 questions;
- each question is assigned to groups of 5 to 8 potential answers;
- each group contains 1 to 3 answers marked as "correct";
- the result of the VOUD for the certified persons shall be the accrual of points for the selection of marked options in the range from 0 to 200.

- the only criterion of $E = \sum_{ij}^N p_{ij} f(x_{ij})$ is the condition: the proportion of Z subjects must score at least W points, which can be interpreted as the "average" set of points for the certified points not lower than the threshold of $E \geq W$.

We shall assume that the values of Z and W do not change with the increase in the volume of subjects (it is consistent with the VOUD practice), and the function $f(x_{ij})$ is as follows:

- argument x_{ij} plays the role of the "meeting" event of the certified lot with a sample of tests;
- substantially $f(x_{ij})$ represents the result for the i^{th} lot of the certified persons from all test pool N (the lot can consist of the only certified person) of the j^{th} sample of the test documents made by rules of an external assessment of educational achievements;
- function x_{ij} from each x_{ij} is non-negative.

Then $f(x_{ij})$ can be assumed constant, that is equal to E ($E \geq W$), which follows from

$E = \sum_{ij}^N p_{ij} f(x_{ij})$ taking into account the normalizing constraint $\sum_{ij}^N p_{ij} = 1$.

For example, such interpretations of "almost incredible" WOOD certification processes are possible:

I) *the situation is formed in an unnatural way, through the artificial creation of the certified lot.* In particular, all unable (unwilling) to be certified "receive" sick leave instead of the VOUD test. We have a situation of equal $f(x_{ij})$ (if those capable to pass VOUD test answer only to a threshold level E). This corresponds to a situation of equal p_{ij} for Shannon-Hartley entropy function $S = \log N$ (interpreted as extremely undefined), but it leads to the guaranteed $E \geq W$. In other words, "equally possible" testology approach gives, however, a guaranteed result.

P) "dummy" VOUD certification. There is only one p_{ij} value other than zero (and equal to one): the process has an absolutely regular basis, since even the entire test pool presented to a single group with x_{ij} characteristics of "test experts" (assisting the certified persons in an unauthorized way) always gives an indicator equal to the expert $E \geq W$.

However, the elimination of I) and P) situations (i.e. the ability to "clean up lists of certified persons with sick leaves" and/or actually be certified be the "experts") will lead to a change in the values of $f(x_{ij})$ and in the evaluation of entropy. Indeed, any distribution of p_{ij} , different from uniform, provokes non-constant $f(\cdot)$, since nonzero E gives correlation of p and $f(\cdot)$ in the interpretation of p and $f(\cdot)$ as random variables. The substantive requirements of VOUD include the requirement of hitting two-dimensional random variable $E(\cdot) = \sum_{ij}^N (p_{ij} f(x_{ij})) \triangleq E_{ij}$ in the ellipse of dispersion[16], parameterized by Z and W values.

The analyzed above I) and P) cases of VOUD certification processes in the proposed interpretation perform an artificial reduction

in the variance of the scatter of results with the mean shift in the direction of the maximum. Therefore, I) and P) can be recognized by comparing the entropy values calculated from both the session results and the VOUD results. The “artificiality” of the I) situation is equivalent to the “mastermindness” of the P) situation (and both are different from the session situation when, *all* are attested *independently* one way or another), while the role of entropy in the first shall belong to Renyi entropy with q -parameter calculated from the level of E index, based on W $E = \sum_{ij}^N p_{ij} f(x_{ij})$, $E \geq W$).

Let's consider a model example.

Let's say a small group of 3 people takes a session:

- every appraisee answers to 100 questions out of 300 questions in the total base volume;

- at the same time, 34, 33 and 33 questions have 5-8 answers with, respectively, one, two and three “correctly”-marked answers;

- the documents of the test record are atomic (the atom is equal to one question), and:

$\sqrt{p_{ij}} \in \{0, 1/300, 2/300, 3/300\}$, a
 $f(x_{ij}) \in \{0, 1/3, 2/3, 1, 4/3, 5/3, 2\}$ for a session;

$\sqrt{p_{ij}} \in \{0, 1/200, 2/200\}$, a
 $f(x_{ij}) \in \{0, 1/2, 1, 3/2, 2\}$ for VOUD (C-student is “hidden”);

- a “C-student”, who always puts only one check-mark, barely gains a total of 100 points and passes the session, is not involved in VOUD (has a supporting document);

- a “B-student” never selects three marks, passes the session and VOUD;

- an “A-student” is not afraid to lose points by choosing “extras” (wrong answer), hoping to score the highest possible score, successfully passes the session and VOUD.

Summarizing $\sum_{ij}^{300} p_{ij} f(x_{ij})$, we can calculate:

SE) Shannon
Entropy $S = - \sum_{ij}^{300} p_{ij} \log p_{ij}$.

The value of the Shannon entropy:

- for the session (calculations for three participants) is in the range from $\log(300) \approx 8.23$ (limit case when everyone answered different questions) to $3\log(33, (3)) \approx 15.18$ (limit case when all answered one set of questions);

- for VOUD (similar calculations for two participants) from $\log(200) \approx 7.65$ to $2\log(50) \approx 11.29$.

So, intervals [8.23; 15.18] and [7.65; 11.29] give overlapping, so we have:

- the session situation indistinguishable from that of VOUD's, if p_{ij} distributions are completely independent;

if p_{ij} s are of the same type, for example, the questions did not match with anybody, the “session” will give the value of the entropy strictly greater than the entropy of VOUD.

RE) Renyi Entropy $S_R = \frac{1}{1-q} \log \sum_{ij}^{300} p_{ij}^q$.

Similar calculations give intervals of [3.47; 8.23] and [4.64; 7.65], respectively, for the session and for VOUD, and an indistinguishable situation, except for “the same type” (as for Shannon entropy).

We shall note that the upper Renyi-evaluation of intervals *does not depend on q* and *coincides* with the lower Shannon-evaluation, which is obtained for the minimum possible set of documents (test items) – when all test takers receive the same 100 questions (such evaluation estimates give the results of a trial VOUD-testing on a single variant of tasks).

TE)

Tsallis Entropy $S_T = \frac{1}{q-1} (1 - \sum_{ij}^N p_{ij}^q)$.

Tsallis entropy, as is known [2], reaches a maximum of $S = \frac{N^{1-q}-1}{1-q}$ for $q > 1$ in the case of equally probable distributions, that is at $p_{ij} = 1/N$ for the model example. Value of the entropy:

- is $N=300$, $S \approx 8.23$ for the session at $q \approx 1$;

- is $N=200$, $S \approx 7.65$ for VOUD at $q \approx 1$.

If the questions in the test at least partially coincided, Tsallis entropy drops markedly up to $S \approx 4.61$ both for the session and for VOUD.

In this case the situation looks similar to the one described above, as variety of combinations of tasks reduces atVOUD (part of the test books will not be distributed for the reasons mentioned above). It may be worth splitting the test task into a documentary set of question-answer pairs, taking into account the fact that some pairs will require a meaningful “hint” because of the internal dependence of the answer options previously combined with the question. Tsallis entropy with $q \neq 1$ parameter is usually applied specifically for such options.

The “entropy” scheme of replacement of the VOUD concept (or other external check of residual knowledge) by results of the session results analysis is proposed here.

1. The value S_R^* of the Renyi entropy is chosen from the internal points of the overlapping intervals, for example, on the basis of correspondence to the value of E indicator. If talking about the model example, this shall be not lower than 4.64, and the possible choice of the upper level equal to 7.65 allows the variation of q parameter within a wide range without fundamental influence on the result.

2. A pool of documents is collected from the database of test tasks used at the session, the statistics on which gives exactly the selected entropy value S_R^* .

3. The results of the appraisees are surveyed on the constructed pool.

The session databases contain the entire range of the appraisees (there is no effect of replacing the test with a sick leave), and there is no specially selected group of “experts” that “enhances” the results (the testing during the session is under video surveillance; moreover, it is possible to effectively record the process by side sources of information [17]).

4. The results on the sample pool are averaged according to the VOUD requirements.

5. Repeated testing in the form of “VOUD-session” on the session basis at the graduation course and recording among others new (repeated) results according to the proposed scheme (1.-4.) shall assess the sustainability of the results following the criterion of the “residual” knowledge.

Consideration

We shall note here (not statistically proven) that since de facto the VOUD database consists of session materials of the main universities of the Republic of Kazakhstan used for their certified enrollment, the scenario (1.-4.) actually occurs (in the absence of entropy evaluations there is no guarantee that the scheme of the most unsuccessful version of the sample/test pool is not implemented).

We shall emphasize that the model calculation is given only for the ease of checking the calculations, all the conclusions and suggestions do not change for any more voluminous and realistic situation.

Conclusion

Indicators reflecting the content of the control in an average quantitative form are formed in systems of knowledge control. They are usually given as functions of the characteristics of the processes and explicitly or implicitly take into account or tend to take into account the “typical” manifestations, assuming data with stable characteristics that are statistically significant and sufficient for the analysis. The paper shows the availability and possibilities of other methods of analysis, based primarily on entropy characteristics, less demanding on the volume and quality of data and, at the same time, actively using, for example, materials already available in the system and the generally accepted document flow. New entropic approaches may be used in the control system for decision-making on its improvement.

ЛИТЕРАТУРА

1. Julliand, J., Kouchnarenko, O., Masson, P. A., Voiron, G. Test Generation from Event System Abstraction to Cover Their States and Transition// Programming and computer software. - 2018. Vol: 44. - pp. 1-14.
2. Bride, H., Julliand, J., and Masson, P.-A., Tri-modal under-approximation for test generation, Sci. Comput. Program., 2016, vol. 132, no. P2, pp. 190–208.
3. Godefroid, P. Compositional dynamic test generation (2007) ACM SIGPLAN Notices, 42 (1), pp. 47-54.

4. Bué, P.-C., Julliand, J., Masson, P.-A. Association of under-approximation techniques for generating tests from models (2011) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6706 LNCS, pp. 51-68.
5. Godefroid, P., Klarlund, N., Sen, K. DART: Directed Automated Random Testing (2005) Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), pp. 213-223.
6. Tillmann, N., De Halleux, J. Pex-white box test generation for.NET (2008) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4966 LNCS, pp. 134-153.
7. Majumdar, R., Sen, K. Hybrid Concolic Testing, ICSE 2007: 29th International conference on software engineering, proceedings (2007) pp. 416-426.
8. Shannon, C.E. A Mathematical Theory of Communication (1948) Bell System Technical Journal, 27 (3), pp. 379-423.
9. Shannon C.E., Sloane N., Wyner A. (Eds.), Collected Papers, IEEE Press, New York (1993).
10. I.V.Toranzo, J.S.Dehesa, Exact Shannon entropies for the multidimensional harmonic states Physica A: Statistical Mechanics and its Applications Vol. 516, 2019, pp. 273-279.
11. Tsallis C. Possible generalization of Boltzmann-Gibbs statistics// J. Stat. Phys. 1988. V. 52. P. 479-487.
12. Bromiley, P.A. Shannon Entropy, Renyi Entropy, and Information [Electronic resource]/P.A. Bromiley, N.A. Thacker, E. Bouhova-Thacker. – Mode of access: <http://www.tinavision.net/docs/memos/2004-004.pdf>. – Date of access: April 8, 2016.
13. A. Arnold, J. Antonio Carrillo, L. Desvillettes, J. Dolbeault, A. Jüngel, L. Claudia, P.A. Markowich, G. Toscani, C. Villani «Entropies and Equilibria of Many-Particle Systems: An Essay on Recent Research», Nonlinear Differential Equation Models pp. 35-43.
14. A.I. Wilson, 1978, Entropy in Urban and Regional Modeling, Moscow, Nauka Publishing.
15. O. V. Chumak, 2010, Entropies and Fractals in Data Analysis, Moscow, Sternberg Astronomical Institute Publishing.
16. https://matlab.ru/articles/Ver_7.pdf (Date of access: December 24, 2018).
17. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels – Santa Barbara: CRYPTO 2018 conference.

REFERENCES

18. Джулиан Д., Коучиренко О., Мэйсон П., Войрон Г. Генерация тестов из абстракции событийных систем для покрытия их состояний и переходов // Программирование и программное обеспечение. - 2018. том: 44. - стр. 1-14.
19. Брайд Х., Джулиан Д., Мэйсон П. Трехмодальное недо-приближение для генерации теста // Компьютерное программирование, 2016, том: 132, №2, стр. 190–208.
20. Годфройд П. Композиционный динамический тест поколения (2007) ACM SIGPLAN примечание, том: 42 (1), стр. 47-54.
21. Буе П., Джулиан Д., Мэйсон П. Объединение методов недостаточной аппроксимации для генерации тестов из моделей (2011) Конспекты лекций по информатике (включая подсерии конспекты лекций по искусственному интеллекту и конспекты лекций по биоинформатике), 6706 LNCS, стр. 51-68.
22. Годфройд П., Кларланд Н., Сен К. Направленное автоматизированное случайное тестирование (2005) Материалы конференции ACM SIGPLAN по разработке и внедрению языков программирования, стр. 213-223.
23. Тильман Н., Халеукс Д. Рех-белый ящик для коробки теста. Сеть. (2008) Конспекты лекций по информатике (включая подсерии конспекты лекций по искусственному интеллекту и конспекты лекций по биоинформатике), 4966 LNCS, стр. 134-153.
24. Маджумдар Р., Сен К. Гибридное соколиное тестирование, ICSE 2007: 29-я Международная конференция по программной инженерии, труды (2007) стр. 416-426.
25. Шэннон С. Математическая теория коммуникации (1948) Технический журнал Bell System, том: 27 (3), стр. 379-423.
26. Шэннон С., Слоан Н., Уайнер А. Сборник статей, IEEE Press, Нью Йорк (1993).
27. Торанзо И., Дехеса Д. Точные энтропии Шеннона для многомерных гармонических состояний физики: статистическая механика и ее приложения. 2019, стр. 273-279.
28. Тсалис С. Возможное обобщение статистики Больцмана-Гиббса // Физика. 1988. том: 52. стр. 479-487.
29. Бромелли П. Энтропия Шеннона, энтропия Рени и информация [Электронный ресурс] /П.А. Бромелли, Н.А. Тэйкер, Е. Боухова-Тэйкер. – режим доступа: <http://www.tinavision.net/docs/memos/2004-004> – Дата доступа: 08.04.2016.
30. Арнольд А., Антонио Карилло Д., Десвилатэс Л., Долбеауэльт Д., Джангл А. Клаудиа Л., Маркович П., Тоскани Г. Вилани С. «Энтропии и равновесия многочастичных систем: очерк последних исследований», Модели нелинейных дифференциальных уравнений. стр. 35-43.

31. Вилсон А.Дж., Энтропийные методы моделирования систем, Москва, изд. Наука, 1978.
32. Чумак О.В., 2010, Энтропии и фракталы в анализе данных, Москва, изд. ГАИШ МГУ.
33. https://matlab.ru/articles/Ver_7.pdf (актуальная дата 24.12.2018).
34. Генкин Д., Патани М., Счастьер Р., Тромер Е. Синестезия: Обнаружение содержимого экрана через удаленные акустические боковые каналы – Santa Barbara: Конференция CRYPTO 2018.

ОҚЫТУ ЖӘНЕ АТТЕСТАТТАУ ЖҮЙЕСІНІҢ СИПАТТАМАСЫ РЕТІНДЕ ЭНТРОПИЯЛЫҚ ТӘСІЛДІ ЗЕРТТЕУ

Куликов Владимир Павлович, ақпаратты-коммуникациялық технологиялар кафедрасының профессоры, М.Қозыбаев атындағы Солтүстік Қазақстан мемлекеттік университеті, Петропавл қ., Қазақстан, qwertyrant@mail.ru

Казанбаева Альбина Советовна, ақпаратты-коммуникациялық технологиялар кафедрасының докторанты, М.Қозыбаев атындағы Солтүстік Қазақстан мемлекеттік университеті, Петропавл қ., Қазақстан, akazanbaeva83@mail.ru

Икласова Кайнижамал Есимсеитовна, ақпаратты-коммуникациялық технологиялар кафедрасының докторанты, М.Қозыбаев атындағы Солтүстік Қазақстан мемлекеттік университеті, Петропавл қ., Қазақстан, kiklasova@mail.ru

Андатпа. Соңғы уақытта білім беру сапасын арттыру және осы сапаның объективті бағасын енгізу қажеттілігі туралы көптеген жарияланымдар пайда болды. Жиі оқыту/білім беру сапасын бағалау жеңілдетілген және дәстүрлі түрде қарастырылады. Әңгіме негізінен білім алушылардың жеке жетістіктерін бағалау және білім беру мекемелерін лицензиялау, аттестаттау және аккредиттеу рәсімдері туралы ғана жүріп жатыр. Жоғары білім беру сапасын бағалау мәселесі терең де әрі күрделі. Бұл мақалада оқу жетістіктерінің сапа сипаттамасын энтропиялық тәсіл арқылы қалыптастыру ұсынылады. Осы мақалада ұсынылған Зерттеудің мақсаты қарапайым студенттік сессиялардың нәтижелері мен қорытындыларын талдау бойынша оқу жетістіктерін сырттай бағалау (немесе білімді басқа да жаппай тексеру) тұжырымдамасын түзетудің «энтропиялық» схемасының мысалында міндеттерді шешу болып табылады.

Түйінді сөздер: оқыту жүйесі, тестілеуді басқару, сапаны бағалау, бақылау, энтропия, оқу жетістіктері.

ИССЛЕДОВАНИЕ ЭНТРОПИЙНОГО ПОДХОДА КАК ХАРАКТЕРИСТИКИ СИСТЕМЫ ОБУЧЕНИЯ И АТТЕСТАЦИИ

Куликов Владимир Павлович, к.ф.-м.н., профессор кафедры «Информационно-коммуникационные технологии», Северо-Казахстанский государственный университет имени М. Козыбаева, г.Петропавловск, Казахстан, qwertyrant@mail.ru

Казанбаева Альбина Советовна, докторант кафедры «Информационно-коммуникационные технологии», Северо-Казахстанский государственный университет имени М. Козыбаева, г.Петропавловск, Казахстан, akazanbaeva83@mail.ru

Икласова Кайнижамал Есимсеитовна, докторант кафедры «Информационно-коммуникационные технологии», Северо-Казахстанский государственный университет имени М. Козыбаева, г.Петропавловск, Казахстан, kiklasova@mail.ru

Аннотация. В последнее время появилось множество публикаций о повышении качества образования и необходимости введения объективных оценок этого качества. Зачастую оценки качества обучения/образования рассматриваются и упрощенно, и традиционно. Разговор идет, в основном, лишь об оценке индивидуальных достижений обучающихся и о процедурах лицензирования, аттестации и аккредитации образовательных учреждений. Проблема оценки качества высшего образования и глубже, и серьезнее. В данной статье характеристику качества учебных достижений предлагается формировать через энтропийный подход. Целью исследования, представленного в данной статье, является решение задачи на примере «энтропийной» схемы коррекции концепции внешней оценки учебных достижений (или иной массовой проверки знаний) по результатам анализа итогов обычных студенческих сессий.

Ключевые слова: система обучения, управление тестированием, оценка качества, контроль, энтропия, учебные достижения.

Статья поступила в редакцию 19.06.19. Актуализирована 16.09.19. Принята к публикации 27.09.19.

The Bulletin of Kazakh Academy of Transport and Communications named after M. Tynyshpaev
ISSN 1609-1817
Vol. 110, No.3 (2019), pp.223-228

WEB DEVELOPMENT PROCESS APPLICATIONS FOR WORKING TIME ACCOUNTING

Ismagulova Zhuldyz Sauekhanovna, candidate of technical Sciences, associate Professor of Kazakh academy of transport and communications named after M. Tynyshpaev, Almaty, Kazakhstan, zhulduz66@mail.ru

Nurgulzhanova Assel Nurgulzhanovna, candidate of technical Sciences, associate Professor of Kazakh academy of transport and communications named after M. Tynyshpaev, Almaty, Kazakhstan, nurgulzhanova@mail.ru

Nazarbayev Tamerlan Galievich, master student of Kazakh academy of transport and communications named after M. Tynyshpaev, Almaty, Kazakhstan, nazarbayev.nt@gmail.com

Abstract. The article describes the application development process. The current MeteorJs framework has been studied. The process of choosing a programming language is considered. The process of starting development is studied in detail, the process of working in the application is described. Were conducted basic tests for security and resistance to external threats. In the presentation of the framework, new and modern methods are described which are used in modern web programming.

The developed application allows you to record the labor of employees. To work in the application, you need to log in and go to the time accounting section, then click on the start of the day and enter your initial action. Then you need to continue to fill in all the days. After confirming the work card, the supervisor reviews and will either approve or cancel the work done. And at the end of the month, a general work card is compiled.

The head of the company can register his company in the project, for this it is necessary to register by specifying the email. Then he must add the operating units and the structure of his company, add employees to each of them and assign to each unit his manager. Next, users receive a message about the need to enter an individual password. System ready to work. Also, were conducted the necessary stress tests of the application, and security tests. No vulnerabilities were detected during these tests. The application proved to be extremely reliable and optimized. In the course of practical tests, the same problems have been identified.

Key words: Web app, design, meteorJS, JavaScript, EcmaScript, BlazeJs, MongoDB.

УДК 004.45

Исмагулова Ж.С.¹, Нургулжанова А.Н.¹, Назарбаев Т.Г.¹

¹Казахская академия транспорта и коммуникаций им. М.Тынышпаева, г. Алматы, Казахстан

ПРОЦЕСС РАЗРАБОТКИ WEB - ПРИЛОЖЕНИЯ ПО УЧЕТУ РАБОЧЕГО ВРЕМЕНИ

Аннотация. В статье рассмотрен процесс разработки приложения. Был изучен актуальный фреймворк MeteorJs. Рассмотрен процесс выбора языка программирования. Детально изучен процесс начала разработки, описан процесс работы в приложении. Были проведены основные тесты на безопасность и устойчивость к внешним угрозам.

Ключевые слова: Web - приложение, дизайн, meteorJS, JavaScript, EcmaScript, BlazeJs, MongoDB.

Введение. Учет рабочего времени является необходимым средством контроля за выполнением работниками установленной нормы продолжительности труда. Автоматизация учета рабочего времени помогает не только сократить

трудозатраты, но и исключить влияние человеческого фактора, когда табель заполняется вручную. Данная статья посвящена разработке Web - приложения по учету рабочего времени [1].

Подписано в печать 25.10.2019 г. Формат 70х100 ¹/₁₆
Объем 368 стр. Заказ № 514. Тираж 500 экз.
Бумага офсетная 80 г.
Отпечатано в ТОО «Power Print»
Адрес: г. Алматы, пр. Райымбека, 165. Тел. +7 (727) 233-08-37