РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

3. Краткий справочник для инженеров и студентов: Высшая математика. Физика. Теоретическая механика. Сопротивление материалов / А. Д. Полянин и др. - М. : Международная программа образования, 2008. - 432 с.

УДК 519.6

КЕЗДЕЙСОҚ САНДАРДЫ ТЕСТІЛЕУДІҢ ӘДІСІ ТУРАЛЫ

Өмірбек Мерей Нұржанұлы
omirbek.m@mail.ru
Л. Н. Гумилев атындағы ЕҰУ Механика- математика факультеті Математикалық және компьютерлік моделдеу кафедрасының 4- курс студенті, Астана, Қазақстан
Ғылыми жетекші – К. Сулейменов

1. Тестілеудің характеристикалары

Кездейсоқ және псевдокездейсоқ сандар есептеу тәсілдерінде және имитациалық моделдеуде, соңғы жылдары криптографиялық алгоритм қолданатын, ақпаратты қорғау жүйесінде кеңінен қолданылады. Бұл, өз кезегінде, [1, 2] кездейсоқтықтан мүмкін ауытқуды анықтауға арналған, тиімді статистикалық тестілеуді құру мәселесін өзекті етеді.

Көптеген белгілі статистикалық тестілеу ақпаратық теорияның тәсілі мен идеясына негізделген. Солардың арасында танымал Маурер тестілеу сонымен қатар, Лемпел- Зива кодына және энтропияны бағалауға негізделген, тәсілдерді атап кеткен жөн. Берілген мақалада, «кітаптар жиыны» бейімдеу кодының конструкциясына негізделген, [2] –де көрсетілген, статистикалық тестілеуді ұсынамыз.

Берілген тестілеуді сипаттау үшін бірқатар анықтамалар қажет болады. Бірқатар көз алфавиттің әріптерін шығарсын $A = \{a_1, a_2, \dots, a_s\}, S > 1$, және $x_1, x_2, \dots, x_n$ таңдама бойынша H_1 балама гипотезаға қарсы (мұндағы H_1 H_0 гипотезасын жоққа шығаратын гипотеза) $H_0: p(a_1) = p(a_2) = \cdots p(a_s) = 1/S$ гипотезасын тексеру қажет.

Қарастырылып отырған тәсіл бойынша тестілеу кезінде A алфавитінің әріптері реттелген (және сол ретке байланысты 1-ден S -ке дейін нөмірленген), бірақ бұл рет таңдалған әрбір x_i - дің мәніне жасалған талдаудан кейін келесідей өзгеріп отырады: a арқылы белгіленген, x_i әріпі 1-ші нөмірді алады, ал нөмірі a -ның нөмірінен кіші болған әріптердің нөмірі 1-ге артады, ал қалғандарының нөмірі өзгеріссіз қалады. Бұл түрлендіруді толығырақ сипаттау үшін $x_1, x_2, \dots, x_{t-1}$ талдауда кейін $a \epsilon A$ әрпінің нөмірін $v_t(a)$ деп белгілейік және A-дағы әріптердің бастапқы $v^1(\bullet)$ реті еркін түрде орнатылады. Онда x_t талдаудан дан кейінгі нөмірлеу келесідей анықталады:

$$v^{t+1}(a) = \begin{cases} 1, & \text{егер } x^t = a \\ v^t(a) + 1, & \text{егер } v^t(a) < v^t(x_t) \\ v^t(a), & \text{егер } v^t(a) > v^t(x_t) \end{cases} \qquad (1)$$

(Кітап жинағы секілді, егер кітап нөмірі кітап жинағындағы орнымен сәйкес келеді деп есептесек, кітап сол орыннан алынып ең үстіне қойылады. Оның нөмірі 1-ші болады, ал басында сол кітаптің үстінде тұрған кітаптар төменге жылжиды, ал қалғандары өз орнында қалады.) Тәсілдің басты идеясы $-x_1, x_2, \dots, x_n$ таңдамасында әріптің кездесу жиілігі емес, әріптің нөмірінің кездесу жиілігі есептеледі. H_1 гипотезасы орындалғанда, бірқатар әріптердің ықтималдығы (және таңдамада кездесу жиілігі) $1/S$ –тен артық, және олардың нөмірі орта есеппен ықтималдығы кіші әріптердің нөмірінен кем болады. (Басқаша айтқанда, көп қолданылатын кітаптар, кітаптар жинағының ең үстінде қалғандарына қарағанда ұзағырақ болады. Сондықтан, керек кітапты кітаптар жинағының үстіңгі жағынан табу ықтималдығы, астыңғы жағынан табу ықтималдығына қарағанда көбірек.) Егер де H_0

гипотезасы орындалса, онда әріптер таңдамадасында кез келген нөмірмен пайда болуы ықтималдығы $1/S$- ке тең.

Сипатталып отырған тестілеуді қолданғанда $\{1, \dots, S\}$ сандарының жиыны алдын ала, таңдаманы талдауға дейін, қиылыспайтын $r > 1$ $A_1 = \{1,2, \dots, k_1\}, A_2 = \{k_1 + 1, \dots, k_2\}, \dots, A_r = \{k_{r-1} + 1, \dots, k_r\}$ бөліктерге жіктеледі. Одан кейін $x_1, x_2, \dots, x_n$ таңдамасы бойынша $A_j, n_j, j = 1, \dots, r$ деп белгілеп аламыз, жиыншасына тиісті $v^t(x_t)$нөмірінің саны есептеледі. H_0 гипотезасы орындалғанда $v^t(x_t)$ A_j жиыншасына тиісті болу ықтималдығы, оның элементтерінің сандарына пропорционал, яғни $|A_j|/S$ -ке тең. Одан кейін $n_1, \dots, n_r$ бойынша χ^2 критерийі бойынша H_0 * гипотезасы тексеріледі:

$$P\{v^t(x_t) \epsilon A_j = |A|/S\} \qquad (2)$$

Балама $H_1{}^* = \urcorner H_0{}^*$ гипотезасына қарсы. Демек, алғашқы H_0 гипотезасы орындалса $H_0{}^*$ гипотезасы орындалады, және керісінше, $H_1{}^*$ гипотезасы орындалса H_1 гипотезасы орындалады. Сондықтан сипатталған критерийді қолдану корректілі.

χ^2 критерийі қолданғанда келесі шама анықталады:

$$x^2 = \sum_{i=1}^{r} \frac{(n_i - nP_i^0)^2}{nP_i^0}, \qquad (3)$$

мұндағы $P_i{}^2 = |A_i|/S$ (см. (2)). H_0 орындалғанда кездейсоқ x^2 шамасының таралуы χ^2 таралуына $r - 1$ еркіндік дәрежесімен ассимптотикалық жақындайды.

A_j жиыншасының санын және өлшемін таңдау алгоритмін сипаттаймыз, бұл характеристикаларды эксперимент жүзінде анықтауды ұсынамыз. Кездейсоқ және псевдокездейсоқ сандардың генераторын тестілеу кезінде, басқа есептердегі сияқты, осы шамалардың мәнін табу үшін арнайы эксперименттер жүргізілуі, одан кейін тәуелсіз деректер бойынша гипотезаны тексеру мүмкін (немесе көрсетілген мәнді таңдау кезінде қолданылмаған, псевдокездейсоқ сандардың тізбегінің бөлігі бойынша). Мұндай эксперименттер таңдаудың қолайлы көлемі болғанда (немесе есептеудің қолайлы уақытында) кездейсоқтықтан ауытқуын анықтауға мүмкіндік беретін, параметрлердің мәнін табуға бағытталған.

Критерийдің қолданылу мүмкіндігі ақпараттық теорияның келесі екі нәтижесіне негізделген: біріншіден, H_0 гипотезасы орындалғанда Шеннон энтропиясы әріпке $\log_2 S$ битке тең, ал кез келген басқа ықтималдық таралуында энтропия $\log_2 S$ –тен кіші. Екіншіден, «кітап жинағы» коды кілтті сөздің орташа ұзындығы энтропияға жақын болатын, универсал (әмбебап немесе бейімделгіш) кодқа жатады. Сондықтан кодтың орташа ұзындығын энтропияны бағалау үшін қолдануға болады, енді осы бағалауға сүйене отырып, статистикалық критерий құруға болады.

2. Статистикалық тестілеу

Сипатталған тәсіл [1]-де ұсынылған генераторды тестілеу үшін қолданылады. [1]-дің авторы $\text{B}, \dots, F$ арқылы белгіленген, бірнеше псевдокездейсоқ сандардың генераторына әртүрлі статистикалық тестілер қолданған. $\text{B} -$ E генераторлары, сызықты конгруэнтті тізбек деп аталатын формула арқылы табылады

$$X_{n+1} = (aX_n + c) mod m, \qquad (4)$$

мұндағы a, c, m, X_0 – тәсіл параметрлері, ал F параметрі Фибоначчи тәсілінде құрылған. [1]-ден алынған генераторлар (4) теңдігі арқылы беріледі, және де $c = 0$. [1]-ден алынған генераторлардың бөлігі жаман статистикалық қасиеттерге ие, қалған бөлігі жақсы, ал [1]- дан алынған барлық тәсілдер ең жақсы (берілген класста) болып табылады және практикалық қолдануға ұсынылған болып есептеледі.

Қарастырылып отырған барлық тәсілдер $\{0, \ldots, m-1\}$ жиынынан алынған бірқалыпты үлестірілген бүтін сандарды генерациялауға арналған, мұндағы m – тәсілдің параметрі. (4) бойынша туындайтын сандардың кіші белгісі кездейсоқ үлестірілгеннен көп жағдайда алыс екені белгілі, сондықтан негізінен кездейсоқ сан ретінде тек үлкен таңбаларды қолдану ұсынылады. Осы ұсынысқа сүйенсек, генератордан туындайтын шамалардан «үлкен бит» немесе «үлкен байт» ерекшеленді (келесіде сәйкесінше R_1 және R_8 болып белгіленетін нұсқа). Дәлірек айтқанда, R_1 режимінде жұп m y_n үлкен бит

$$y_n = \begin{cases} 0, & \text{егер } x_n < \dfrac{m}{2} \\ 1, & \text{егер } x_n \geq \dfrac{m}{2} \end{cases}$$

ал тақ үшін келесі формула

$$\mathrm{y_n} = \begin{cases} 0, & \text{егер } x_\mathrm{n} < \dfrac{\mathrm{m}-1}{2} \\ 1, & \text{егер } \mathrm{x_n} > \dfrac{\mathrm{m}-1}{2} \\ \wedge, & \text{егер } \mathrm{x_n} = \dfrac{\mathrm{m}-1}{2} \end{cases}$$

мұндағы ∧- бос сөз.

R_8 режимінде 8- биттік сөз $\hat{y}_n$ X_n формуласынан «шығады»

$$\hat{y}_n = \begin{cases} \lfloor 256X_n/m^* \rfloor, & \text{егер } X_n < m^* \\ \wedge, & \text{егер } X_n \geq m^* \end{cases}$$

мұндағы $m^* = 256\,\lfloor m/256 \rfloor$, ал $\lfloor 256X_n/m^* \rfloor$ бүтін саны 8-биттік сөз ретінде жазылған. y_n є $\{0,1\}$ тізбегі ұзындығы s болатын блоктарға бөлінген және тестілеу кезінде, ұзындығы s болатын барлық екілік сөздерден құралған, өлшемі $S = 2^s$ болатын алфавиттен алынған таңдама ретінде қарастырылған.

«Кітаптар жиынында» жиынында барлық орындардың жиындары екі жиыншаға:

$$A_1 = \{a_1, \ldots, a_k\}, \qquad A_2 = \{a_{k+1}, \ldots, a_s\}$$

немесе үш:

$$A_1 = \{a_1, \ldots, a_k\},\ A_2 = \{a_{k+1}, \ldots, a_l\},\ A_3 = \{a_{l+1}, \ldots, a_s\}$$

бөлінген. 1- кестеде, [1]-де сипатталған, датчикті тестілеу бойынша деректер келтірілген. 1 және 2-кестеде сипатталған, тәжірибелерді жүргізгенде, әрбір генератор, әртүрлі өлшемі бар таңдамалар үшін R_1 режимінде тестіленеді. Кездейсоқтықтан ерекшеленетін генерацияланатын тізбек үшін таңдаманың ұзындығын анықтауға болса, онда есептеулер таңдаманың осы ұзындығына сәйкес, алдын тестілеуде қолданылмаған, басқа да жүз тізбек бойынша қайталанады. Таңдама бойынша есептелген x^2 шамасы α-ның: 0,5 және 0,95 екі

мәніне сәйкес келетін еркіндік дәрежесінің саны бар χ^2 үлестірімінің α деңгейінің квантилінің мәнінен артық болатын жағдайлар санына тең болатын, Q_α шамасының мәні есептелінеді. Ал егер де зерттеліп отырған таңдамалардың ұзындығында ауытқу табу мүмкін болмаса, онда барлық есептеулер R_8 режимінде жүргізіледі.

[1]- дің авторы көрсетілген датчиктерді басқа тәсілдермен тексерген және келесі тұжырымға келді: D генераторы, әсіресе E және F генераторларлары жарамсыз болып есептелуі керек, B тестілеуді қанағаттанарлық деген бағамен өтті, ал C «шекарада тұр» деп айтуға болады. Біз алған деректер бұл нәтижелермен жақсы сәйкес келді. Шынымен, жаңа тестілеуді қолдану F генераторы таңдаманың ұзындығы 240 бит болған кезде жарамасыз болып есептеледі: (3) бойынша есептелген 100 тестілеуден кейін x^2 шамасы реті 0,95 және 0,5 болатын квантильден, сәйкесінше 80 және 83 есе (100- ден) артық (ал «идеал» кездейсоқ үшін бит орта есеппен жүзден 5 және 50 болуы керек). C және D генераторлары ұсынылып отырған тестілеу бойынша жарамсыз болып есептелінеді, бірақ таңдаманың ұзындығы үлкен болған кезде. Мұны χ^2 критерийін қолдану арқылы көрсетуге болады. Атап кеткендей, идеалды кездейсоқ сандар кезінде $Q_{0,95}$ бағанына «түсу» ықтималдығы 0,05-ке тең болуы керек. Тура есептеу, «тию» ықтималдығы 0,05- ке тең деген гипотезаны маңыздылық деңгейі 0,01 болатын χ^2 критерийі бойынша қабылмадау керек екенін көрсетеді, егер тию саны 100-дің ішінде 11-ден артық болса. 1- кестеден барлық жағдайлар үшін $C - F$ генераторларынан туындайтын, «идеал» кездейсоқ сан туралы гипотезаны маңыздылық деңгейі 0,01 болған жағдайда теріске шығару керек, себебі $Q_{0,95}$ барлық жағдайда 11- ден артық. C датчигі [1]-ден алынған ешбір статистикалық критерий бойынша жарамсыз деп танымағанын атап кеткен жөн. Ал ұсынылып отырған тестілеу бұл датчикті, тіпті R_1 режимінде жарамсыз деп танып отыр. Сол себептен, ұсынылып отырған тестілеу, кездейсоқ санды генерациялауға арналған тестілеу үшін қолданылатын дәстүрлі тәсілдерге қарағанда мықтырақ болып шықты. [1]-ден алынған генераторлардан басқа, [1]- де зерттелген, $c = 0$ және (4) түріндегі датчиктерді тексеруге «кітаптар жиыны» тәсілі қолданылған. Бұл мақалада, генерацияланатын тізбектер неғұрлым жақсы статистикалық қасиеттерге ие («идеалды» кездейсоқтыққа жақын) болатын a және m параметрлерінің мәндері келтірілген. Бұл тұжырым [1]-де келтірілген танымал критерийлердің арасында ең қуатты болып есептелетін спектральді тестілеуге төзіп беру негізінде жасалады.

Қолданылған әдебиеттер тізімі

1. Кнут Д. Искусство программирования на ЭВМ. Т. 2. Получисленные алгоритмы. М.: Мир, 1977.
2. Рябко В.Я. Сжатие данных с помощью стопки книг / / Пробл. передачи информ. 1980. Т. 16. № 4. С. 16-21.

УДК 519.872

МАРШРУТТАУ АЛГОРИТМДЕРІН ЗЕРТТЕУДІҢ МАТЕМАТИКАЛЫҚ МОДЕЛДЕРІ

Тогисова Акерке Бакитбековна

a.erkesha.kz@mail.ru

Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің математикалық және компьютерлік моделдеу кафедрасының магистранты

Ғылыми жетекшісі – Р. Сергибаев

Операцияларды зерттеу барысында бір типті есептерді шешуде көп мәрте қолдануға арналған жүйелермен кездесуге болады. Мұнда пайда болатын үрдістер қызмет көрсету үрдістері, ал жүйелер – жалпыға қызмет көрсету жүйелері деп аталады. Осыған қарағанда,