

LATVIJAS UNIVERSITĀTE
FIZIKAS UN MATEMĀTIKAS FAKULTĀTE
MATEMĀTIKAS NODAĻA

BIIDEĀLU STATISTISKĀS ĪPAŠĪBAS BIEŽUMA
TESTĀ

MAĢISTRA DARBS

Autors: **Edmunds Cers**

Stud. apl. Mate777

Darba vadītājs: asoc.prof. Dr.math. Jānis Buls

RĪGA 2007

Anotācija

Darbs aplūko iespēju izmantot biideālus kā gadījuma skaitļu ģenerātoru. Šādu ģenerātoru būtu iespējams izmantot datu šifrēšanai. Tā kā tēma ir ļoti plaša, un ir grūti prognozēt pie kādiem rezultātiem iespējams nonākt, izdarītais uzskatāms par pirmajiem soļiem dotajā virzienā. Darbs veikts izmantojot pragmatisku pieeju, un iespēja izmantot biideālus gadījumu skaitļu ģenerēšanai aplūkota sākot ar vienu statistisko testu, un novedot biideālu līdz stāvoklim, kad tas šo testu iztur.

Izveidota programma biideālu ģenerēšanai, kā arī to statistisko īpašību pārbaudei. Uzsvars likts uz vārdu biežuma testu, kas ir viens no gadījumu skaitļu pārbaudes pamattestiem. Pierādītas biideālu īpašības saistībā ar šo testu. Parādīts, ka biideāli ir stabili šī testa nozīmē - ja biideāls neiztur testu ideāli, tad ar laiku tas to neizturēs vispār.

Izveidota un pierādīta metode, kā veidot biideālus, kas iztur biežumu testu pie patvaļīga testējamo vārdu garuma.

Atslēgas vārdi: biideāls, biežuma tests

Abstract

In this thesis we consider the use of biideals as random bit-sequence generators, which could eventually be used as a stream cypher. As this field is completely unexplored, the thesis can be considered as the first steps in this direction. We take a pragmatic approach and start with a single test statistic, exploring the properties of biideals, and offering a method for the improvement of biideals in regard to this test.

A program for generating biideals and testing their statistical properties was created. Mostly the frequency test is considered. We prove the properties of biideals regarding this test. We show, that biideals are stable in regard to the frequency test - either the biideal passes the test perfectly, or it will fail sooner or later.

We have created and proven a method, which allows to generate biideals, that will pass the frequency test at any given length of the test words.

Keywords: biideal, frequency test

Saturs

Apzīmejumi	2
Ievads	3
1. Teorijas apskats	4
1.1. Vairākšķiru algebras	4
1.2. Normālais sadalījums	4
Rezultāti	6
Secinājumi	7
Pateicības	8
Izmantotā literatūra un avoti	9
A Izveidoto programmu kods	10

Apzīmejumi

\mathbb{N} naturālo skaitļu kopa,

\mathbb{Z} veselo skaitļu kopa,

\aleph_0 kopas \mathbb{N} apjoms,

...

Ievads

Darbā aplūkota iespēja izmantot biideālus kā gadījuma skaitļu ģeneratorus[1]. Šādu ģeneratoru būtu iespējams izmantot datu šifrēšanai[2].

Ņemot vērā kriptogrāfijas pieaugošo nozīmi attīstoties internetam, kā arī e-parakstu ieviešanas gaismā, jautājums ir uzskatāms par ļoti aktuālu. Kā papildus apliecinājumu tā aktualitātei var minēt daudzgadīgo ECRYPT projektu, kuru atbalsta Eiropas Komisija, un kura viens no galvenajiem profiljiem ir plūsmas šifrēšanas algoritmi (algoritmi, kas balstīti uz gadījuma skaitļu ģenerātoriem).[3]

...

1. Teorijas apskats

1.1. Vairākšķiru algebras

Definīcija 1. Kopu $\{\{x\}, \{x, y\}\}$ sauc par elementu $x \in X$ un $y \in Y$ sakārtotu pāri un lieto apzīmējumu (x, y) vai $\langle x, y \rangle$.

Definīcija 2. Pāri $((x_1, x_2, \dots, x_{n-1}), x_n)$, kur $\forall i \in \overline{1, n} (x_i \in A_i)$ sauc par n -dimensionālu kartežu pār kopām A_1, A_2, \dots, A_n .

Turpmāk n -dimensionāla karteža apzīmēšanai lietosim vai nu pierakstu

$$(x_1, x_2, \dots, x_n) \quad \text{vai arī} \quad \langle x_1, x_2, \dots, x_n \rangle.$$

Definīcija 3. Par kopu A_1, A_2, \dots, A_n Dekarta reizinājumu sauc visu n -dimensionālo kartežu kopu pār kopām A_1, A_2, \dots, A_n , t.i.,

$$A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) \mid \forall i \in \overline{1, n} (x_i \in A_i)\}. \quad (1.1.1)$$

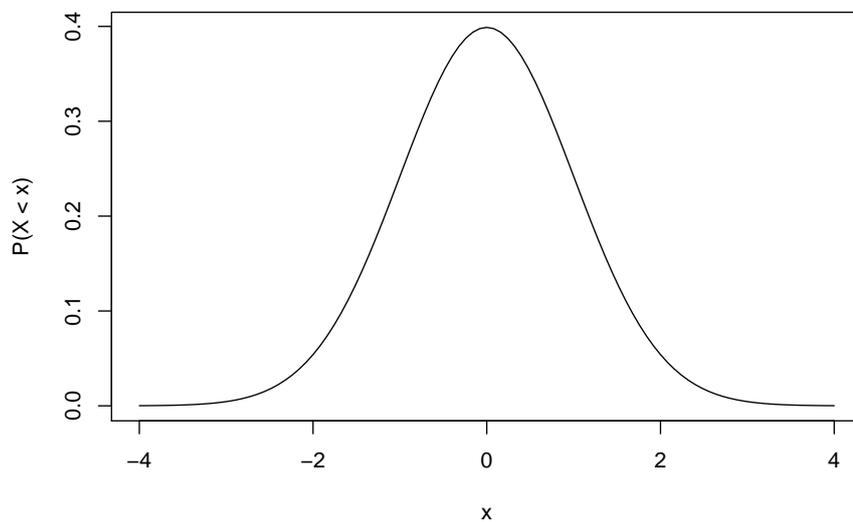
Piezīme 1. Ja $A = A_1 = A_2 = \dots = A_n$, tad lieto arī pierakstu $A^n = A_1 \times A_2 \times \dots \times A_n$. Kopas $A_1 \times A_2 \times \dots \times A_n$ (skat. 1.1.1 pie 3. definīcijas) apakškopu ϱ mēdz saukt arī par n -vietīgu attieksmi, kas definēta kopā $A_1 \times A_2 \times \dots \times A_n$. Šai situācijā kopu A_i , $i \in \overline{1, n}$, sauc par attieksmes ϱ i -to projekciju un lieto apzīmējumu $A_i = \text{pr}_i \varrho$ [4, 42.-45. lpp.].

...

1.2. Normālais sadalījums

Normālā sadalījuma $N(0, 1)$ blīvuma funkcija parādīta 1.1. attēlā. Dažas pārklājuma precizitātes $P - P$ grafikiem, salīdzinot normāli sadalītas gadījuma izlases parādītas 1.1. tabulā.

...



1.1. att. Normālā sadalījuma blīvuma funkcija

1.1. tabula Pārklājuma precizitāte $P - P$ grafikiem.

		$t = 0.1$	$t = 0.3$	$t = 0.5$	$t = 0.7$	$t = 0.9$
$h = n^{-1/6}$	$n_1 = n_2 = 50$	0.960	0.966	0.952	0.940	0.950
	$n_1 = n_2 = 100$	0.934	0.962	0.944	0.922	0.960
	$n_1 = 50 \quad n_2 = 100$	0.922	0.948	0.950	0.952	0.948
$h = n^{-1/5}$	$n_1 = n_2 = 50$	0.944	0.946	0.950	0.942	0.956
	$n_1 = n_2 = 100$	0.946	0.952	0.934	0.948	0.942
	$n_1 = 50 \quad n_2 = 100$	0.936	0.950	0.938	0.938	0.922
$h = n^{-1/4}$	$n_1 = n_2 = 50$	0.956	0.946	0.956	0.942	0.950
	$n_1 = n_2 = 100$	0.950	0.946	0.924	0.970	0.954
	$n_1 = 50 \quad n_2 = 100$	0.954	0.934	0.952	0.930	0.934
$h = n^{-1/3}$	$n_1 = n_2 = 50$	0.946	0.954	0.946	0.960	0.968
	$n_1 = n_2 = 100$	0.956	0.954	0.970	0.950	0.954
	$n_1 = 50 \quad n_2 = 100$	0.938	0.952	0.948	0.948	0.914

Rezultāti

Darbā pierādītas divas teorēmas par apakšvārdu biežumu biideālos. Pirmkārt piedāvāta metode ...

...

Secinājumi

Darba ietvaros izdevies pierādīt, ka “pareizi” izvēloties biideāla bāzi, iespējams panākt, lai tas izturētu vārdu biežumu testu. Šis rezultāts ļauj cerēt, ka varētu izdoties uzlabot arī rādītājus citos statistiskajos testos, izmantojot biideālus kā gadījuma skaitļu ģenerātorus.

Iespējams, ka šo rezultātu pat iespējams vispārināt - tas ir jautājums, pie kura ir vērts turpināt strādāt nākotnē. Vēl mūsu parādītās biideālu īpašības paver iespējas īpašību uzlabošanai citos testos, jo tā nozīmē, ka, iespējams, ģenerējot biideālus var iestarpināt arī bāzes vārdus, kas nav “uzlaboti”.

...

Pateicības

Šis darbs veltīts manam kaķim Saulītim, bez kura to veikt man droši vien nebūtu bijis pa spēkam.

Izmantotā literatūra un avoti

- [1] S. Nicolay and M. Rigo. About frequencies of letters in generalized automatic sequences. *Theoretical Computer Science*, 374:75–121, 2007.
- [2] I. Simon. Infinite words and a theorem of hindman. *Revista de Matematicas Aplicadas*, 9:152–178, 1988.
- [3] H. Hese. *Stikla pērlīšu spēle*. Liesma, Rīga, 1976. Tulkojis Ģirts Bļodnieks.
- [4] Б.П. Демидович и В.А. Кудрявцев. *Краткий курс высшей математики*. Наука, Москва, 1999.

Maģistra “Biideālu statistiskās īpašības biežuma testā” izstrādāts LU Fizikas un Matemātikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Edmunds Cers

(paraksts)

(datums)

Rekomendēju darbu aizstāvēšanai.
Vadītājs: asoc.prof. Dr.math. Jānis Buls

(paraksts)

(datums)

Recenzents: doc. Dr.math. Jānis Valeinis

(paraksts)

(datums)

Darbs iesniegts Matemātikas nodaļā _____

(datums)

(darbu pieņēma)

Darbs aizstāvēts maģistra gala pārbaudījuma komisijas sēdē

_____ prot. Nr. _____, vērtējums _____

(datums)

Komisijas sekretārs/-e: _____

(Vārds, Uzvārds)

(paraksts)