

Резюмета на представените трудове

на Силвия Първанова Бумова

за конкурса за доцент (ДВ бр.40 / 27.05.2016)

I. Статии

1. On the Advanced Encryption Standard (Rijndael), *Proc. of Annual Workshop on Coding Theory, Bankja, BULGARIA, 11-15 December 2002* (papers/P_1.pdf)

The idea of Advanced Encryption Standard (AES) is introduced. The Advanced Encryption Standard (AES) specifies a FIPS (Federal Information Processing Standards)-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt(encipher) and decrypt(decipher) information. The standard becomes effective on May 26, 2002.

Идеята за AES е разгледана. AES е FIPS (Federal Information Processing Standards) - одобрен криптографски алгоритъм, който може да се използва за защита на електронни данни. Алгоритъмът AES е симетричен блок шифър, който може да криптира (шифроване) и декриптира (дешифрира) информация. Стандартът влиза в сила на 26 май 2002 година.

2. On millionaires' problem or comparing information without learning it, *Proc. of Annual National Seminar on Coding Theory, Blagoevgrad, Nov. 30 – Dec. 3, 2006.* (papers/P_2.pdf)

We present the Tierce problem and related to it millionaires' problem. The version of Millionaires' problem is introduced by Yao: two millionaires want to compare their riches and wish to know who is richer, without revealing the precise amount of their wealth. There is a relation between Millionaires' problem and cryptography. Our aim is to present different solutions of this problem.

Представяме на задачата на Tierce. Версията на задачата за милионерите е въведен от Yao: два милионери искат да сравнят своите богатства и искат да знаят кой е по-богат, без да разкриват точното количество на богатството си. Този проблем има връзка с криптографията. Целта ни е да се представят различни решения на този проблем.

3. (with **P. Boyvalenkov, H. Kulina, M. Stoyanova**) New nonexistence results for spherical 5-designs, *Proc. of Fifth International Workshop on Optimal Codes and Related Topics, White Lagoon, Bulgaria, 16-22 June, 2007*. (papers/P_3.pdf)

We investigate the structure of spherical designs of relatively small odd cardinalities and of odd strength. We obtain some bounds on the inner products of 5-designs. In many cases we are able to prove nonexistence of designs of corresponding parameters.

Разглеждаме структурата на сферични дизайни от сравнително малка нечетна мощност и от нечетна сила. Получаваме граници за някои скаларни произведения на 5-дизайните. В много случаи доказваме несъществуване на дизайни от съответните параметри.

4. (with **P. Boyvalenkov, H. Kulina, M. Stoyanova**) New nonexistence results for spherical 5-designs, Scientific Research, *Scientific Research, e-journal of South-western University, (14 pp.)*, 2007.
(<http://press.swu.bg/medial19338/139pdf.pdf>) (papers/P_4.pdf)

We investigate the structure of spherical 5-designs of relatively small cardinalities. We obtain some bounds on the extreme inner products of such designs. As a result, in 42 cases we prove nonexistence of designs of corresponding parameters. Our approach can be applied for other strengths and cardinalities.

Изучаваме структурата на сферичните 5 дизайни със сравнително малка мощност. Получаваме граници за най-голямото и най-малки скаларни произведения на такива дизайни. Като резултат в 42 случая доказваме несъществуване на дизайни от съответните параметри. Нашият подход може да бъде приложен и за друга сила и мощност.

5. (with **P. Boyvalenkov, M. Stoyanova**) Nonexistence results for spherical 7-designs, *Proc. of Eleventh International Workshop on Algebraic and Combinatorial Coding Theory June 16-22, 2008, Pamporovo, Bulgaria*. (papers/P_5.pdf)

We obtain new nonexistence results for spherical 7-designs of odd cardinality. We combine polynomial techniques with some geometric argument to obtain restrictions of the structure of 7-designs with fixed cardinality.

Получаваме резултати за несъществуване на сферични 7-дизайни от нечетна мощност. Комбиниране полиномиални техники с някои геометрични съображения да получим ограничения върху структурата на 7-дизайни с фиксирана мощност.

6. (with **P. Boyvalenkov, M. Stoyanova**) A method for proving nonexistence of spherical designs of odd strength and odd cardinality, *Problems of Information Transmission*, vol. 45, No. 2, 2009, 41-55; *English translation: Problems of Information Transmission* 45, No. 2, 2009, pp. 110-123. (**Impact factor 0.393**) (papers/P_6_en.pdf, papers/P_6_ru.pdf)

We combine polynomial techniques with some geometric arguments to obtain restrictions of the structure of spherical designs with fixed odd strength and odd cardinality. Our bounds for the extreme inner products of such designs allow proving nonexistence results in many cases. Applications are shown for 7-designs.

Комбиниране полиномиални техники с някои геометрични аргументи за да намерим ограничения на структурата на сферични дизайни със фиксирани сила и мощност. Нашите граници за най-малките и най-големите скаларни произведения на такива дизайни позволяват доказателството на несъществуването на много от тях. Показани са приложения за 7-дизайни.

7. (with **P. Boyvalenkov, H. Kulina, M. Stoyanova**) Polynomial techniques for investigation of spherical designs, *Designs, Codes and Cryptography*, 2009, 51, No. 3, 2009, pp. 275-288. (**Impact factor 0.825**) (papers/P_7.pdf)

We investigate the structure of spherical τ -designs by applying polynomial techniques for investigation of some inner products of such designs. Our approach can be used for large variety of parameters (dimension, cardinality, strength). We obtain new upper bounds for the largest inner product, lower bounds for the smallest inner product and some other bounds. Applications are shown for proving nonexistence results either in small dimensions and in certain asymptotic process. In particular, we complete the classification of the cardinalities for which 3-designs on $\mathbb{S}_{n-1}$ exist for $n = 8, 13, 14$ and 18. We also obtain new asymptotic lower bound on the minimum possible odd cardinality of 3-designs.

Изследваме структурата на сферични τ -дизайни чрез прилагане на полиномиални техники, за да намерим някои скаларни произведения на такива дизайни. Методът може да бъде прилаган за голямо разнообразие от параметри (размерност, мощност и сила). Получаваме горни граници за най-голямото скаларно произведение, долна граница за най-малкото скаларно произведение и някои други граници. Показани са резултати за несъществуване в малки размерности в асимптотичен процес. В частност, завършихме класификацията на мощности, за които 3-дизайни върху $\mathbb{S}_{n-1}$ съществуват за $n = 8, 13, 14$ и 18 . Получихме и нова асимптотична долна граница за минималната възможна нечетна мощност за 3-дизайни.

8. (with **H. Kostadinov**, **N. L. Manev**) Watermarking, Steganography, and Error-Control Codes, *American Institute Physics Conference Proceedings*, vol. 1404, (2011) pp. 193-199, ISBN: 978-0-7354-0976-7. (**SJR 0.139**) (papers/P_8.pdf)

An algorithm for embedding binary messages in spatial domain of images is proposed. The algorithm exploits erasure capability of error-control codes that results in improving the robustness and increasing the size of the embedded message. This enables the described algorithm to be used for steganographic purposes, too.

Предлага се алгоритъм за влагане (в пространствената област) на скрита информация в изображения, който използва възможностите на коригиращите кодове да изправят изтривания (два пъти повече от грешките, които изправят). При този алгоритъм се постига по-голям капацитет и увеличаване на размера на вложеното съобщение. Това позволява описаният алгоритъм да бъде използван и в стеганографията.

9. (with **V. Drensky**) Cocharacters of polynomial identities of upper triangular matrices, *J. Algebra and its Applications* 11 (2012), No. 1, 1250018 (24 pages), DOI: 10.1142/S0219498811005440. (**Impact factor 0.968**) (papers/P_9.pdf)

Let $T(U_k)$ be the T-ideal of the polynomial identities of the algebra of $k \times k$ upper triangular matrices over a field of characteristic zero. We give an easy algorithm which calculates the generating function of the cocharacter sequence $\chi_n(U_k) = \sum_{\lambda \vdash n} m_\lambda(U_k) \chi_\lambda$ of the T-ideal $T(U_k)$. Applying this

algorithm we have found the explicit form of the multiplicities $m_\lambda(U_k)$ in two cases: (i) for the “largest” partitions $\lambda = (\lambda_1, \dots, \lambda_n)$ which satisfy $\lambda_{k+1} + \dots + \lambda_n = k - 1$; (ii) for the first several k and any λ .

Нека $T(U_k)$ е Т-идеала на полиномните твърдения на алгебрата на $k \times k$ горно-триъгълни матрици върху поле с характеристика нула. Даваме лесен алгоритъм, който пресмята производящата функция на редицата от кохарактери $\chi_n(U_k) = \sum_{\lambda \vdash n} m_\lambda(U_k) \chi_\lambda$ на Т-идеала $T(U_k)$. Прилагайки този алгоритъм ние намираме точната форма на кратностите $m_\lambda(U_k)$ в два случая: (i) за “най-големите” разбивания $\lambda = (\lambda_1, \dots, \lambda_n)$, за които $\lambda_{k+1} + \dots + \lambda_n = k - 1$; (ii) за първите няколко k и за всяко λ .

10. (with **V. Drensky**) Algebraic properties of codimension series of PI-algebras, *Israel Journal of Mathematics* (2013) 195, pp: 593-611. (**Impact factor 0.659**) (papers/P_10.pdf)

Let $c_n(R)$, $n = 0, 1, 2, \dots$, be the codimension sequence of the PI-algebra R over a field of characteristic 0 with T-ideal $T(R)$ and let $c(R, t) = c_0(R) + c_1(R)t + c_2(R)t^2 + \dots$ be the codimension series of R (i.e., the generating function of the codimension sequence of R). Let R_1, R_2 and R be PI-algebras such that $T(R) = T(R_1)T(R_2)$. We show that if $c(R_1, t)$ and $c(R_2, t)$ are rational functions, then $c(R, t)$ is also rational. If $c(R_1, t)$ is rational and $c(R_2, t)$ is algebraic, then $c(R, t)$ is also algebraic. The proof is based on the fact that the product of two exponential generating functions behaves as the exponential generating function of the sequence of the degrees of the outer tensor products of two sequences of representations of the symmetric groups S_n .

Нека $c_n(R)$, $n = 0, 1, 2, \dots$, е редицата на коразмерностите на PI-алгебрата R върху поле с характеристика нула с Т-идеал $T(R)$ и нека $c(R, t) = c_0(R) + c_1(R)t + c_2(R)t^2 + \dots$ е редът от коразмерностите на R (т.е. производящата функция на редицата от коразмерности на R). Нека R_1, R_2 и R са PI-алгебри, такива че $T(R) = T(R_1)T(R_2)$. Ние показваме, че ако $c(R_1, t)$ и $c(R_2, t)$ са рационални функции, тогава $c(R, t)$ е също рационална. Ако $c(R_1, t)$ е рационална и $c(R_2, t)$ е алгебрична, тогава $c(R, t)$ алгебрична. Доказателството се базира на факта, че произведението на две експоненциални производящи функции е като експоненциална производяща функция на редицата от степените на външно тензорно произведение на две редици на представянията на симетричната група S_n .

11. (with **F. Benanti, V. Drensky, G. Genov, and P. Koev**) Computing with rational symmetric functions and applications to invariant theory and PI-algebras, *arXiv:1201.4448v1 [math.RA] and Serdica Mathematical Journal, 38 (2012), pp. 137–188.* (papers/P_11.pdf)

Let K be a field of any characteristic. Let the formal power series

$$f(x_1, \dots, x_d) = \sum \alpha_n x_1^{n_1} \cdots x_d^{n_d} = \sum m(\lambda) S_\lambda(x_1, \dots, x_d),$$

$$\alpha_n, m(\lambda) \in K,$$

be a symmetric function decomposed as a series of Schur functions. When f is a rational function whose denominator is a product of binomials of the form $1 - x_1^{a_1} \cdots x_d^{a_d}$, we use a classical combinatorial method of Elliott of 1903 further developed in the Ω -calculus (or Partition Analysis) of MacMahon in 1916 to compute the generating function

$$M(f; x_1, \dots, x_d) = \sum m(\lambda) x_1^{\lambda_1} \cdots x_d^{\lambda_d}, \quad \lambda = (\lambda_1, \dots, \lambda_d).$$

M is a rational function with denominator of a similar form as f . We apply the method to several problems on symmetric algebras, as well as problems in classical invariant theory, algebras with polynomial identities, and noncommutative invariant theory.

Нека K е поле с произволна характеристика. Нека формалния степенен ред

$$f(x_1, \dots, x_d) = \sum \alpha_n x_1^{n_1} \cdots x_d^{n_d} = \sum m(\lambda) S_\lambda(x_1, \dots, x_d),$$

$$\alpha_n, m(\lambda) \in K,$$

е симетрична функция, представена по като ред от функциите на Шур. Ако f е рационална функция, чийто знаменател е произведение от биноми от вида $1 - x_1^{a_1} \cdots x_d^{a_d}$, използваме класически комбинаторен метод на Елиот от 1903 и по-нататък доразвит в Ω -calculus (or Partition Analysis) от MacMahon през 1916 за да изчисли производящата функция

$$M(f; x_1, \dots, x_d) = \sum m(\lambda) x_1^{\lambda_1} \cdots x_d^{\lambda_d}, \quad \lambda = (\lambda_1, \dots, \lambda_d).$$

M е рационална функция с знаменател от подобна форма като f . Прилагаме метода за различни задачи за симетрични алгебри, както и за задачи в класическата теория на инвариантите, алгебрите с полиномни твърдения и некомутативната теория на инвариантите.

12. Colength of $*$ -Polynomial Identities of Simple $*$ -Algebras, *Proc. of Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, June 18-24, 2016, Albena, Bulgaria, pp. 66-71.* (papers/P_12.pdf)

We compute the sequence of colengths in the cocharacters of the $*$ - polynomial identities of the $*$ - simple algebra $M_2(F) \oplus M_2(F)^{\text{op}}$, $\text{char}(F) = 0$.

Разглеждаме простата алгебра $M_2 \oplus M_2^{\text{op}}$ с полиномни тъждества с инволюция $(*)$. Използваме резултат на В. Дренски и А. Джамбруно за реда на Хилберт на собствените елементи на тази алгебра, за да намерим редицата от коширина на кохарактерите на $*$ -полиномните тъждества на разглежданата алгебра над поле с характеристика нула.

II. Учебни пособия.

- (a) (с **Н. Л. Манев**) Пермутационни групи,

- * <http://www.moi.math.bas.bg/silvi/>
- * lecture notes/PG1.pdf, lecture notes/PG2.pdf
- lecture notes/PG3.pdf, lecture notes/PG4.pdf

Лекциите са написани да покрият материала на курса по “Пермутационни групи” във ФМИ на СУ “Св. Климент Охридски” за магистри. Лекциите са в електронен вариант и са достъпни в интернет. Състои се от 4 глави - Въведение, Симетрична група и крайни матрични групи, Групи, геометрични фигури и графи и Действие на група върху множество.

- (b) (с **Н. Л. Манев, В. Милошева**) Линейна алгебра и Аналитична геометрия,

- * <http://www.moi.math.bas.bg/silvi/>
- * lecture notes/LAAG1.pdf, lecture notes/LAAG2.pdf
- lecture notes/LAAG3.pdf, lecture notes/LAAG4.pdf
- lecture notes/LAAG5.pdf

Целта на този курс е да покрие програмата по Линейна алгебра и аналитична геометрия във ВСУ “Любен Каравелов”.

- (c) (с **Н. Л. Манев**) Математически Анализ 2,

- * <http://www.moi.math.bas.bg/silvi/>
- * <https://my.vsu.bg/moodle/course/index.php?categoryid=16>

* lecture notes/MA2.pdf

Курсът по Математически Анализ 2 съдържа теория и задачи и е съобразен с програмата за студентите от ВСУ “Любен Каравелов”. Лекциите са в електронен вариант и са достъпни в интернет (и moodle).