РЕЗЮМЕТА

на трудовете на Н. Манев представени за участие в конкурса за професор (ДВ бр.54/1.07.2014)

1 Статии в списания

1. B. Kostova, N. L. Manev, A $[25, 8, 10]$ **does not exist, Comptes rendus de l'Academie bulgare des Sciences, 43 (1990), no.3, pp. 41-44**:

A characterization up to isomorphism of $[16, 7, 6]$ and $15, 7, 5]$ codes is given. As a consequence is proven that $[25, 8, 10]$ does not exist.

Описани са всички неизоморфни $[16, 7, 6]$ и $15, 7, 5]$ кодове. Като следствие е получено, че $[25, 8, 10]$ не съществува.

2. Е. Колев, Н. Манев, Двоичный весовой спектр разширинoго $[2^m, 5]$ **кода Рида-Соломона и дуалного кода, Проблемы передачи информации, 30 (1994), no. 3, 38-46**:

Рассматривается расширенный $[2^m, 5]$ код Рида-Соломона над $GF(2^m)$ и его двоичный образ, задаваемый выбором базиса $\beta_1, \beta_2, \ldots, \beta_m$ над GF(2). Для некоторого класса базисов вычислен весовой спектр двоичного образа.

Разглежда се расширен $[2^m, 5]$ код на Рид-Соломон над $GF(2^m)$ и неговият двоичен образ, зададен чрез избор на базис $\beta_1, \beta_2, \ldots, \beta_m$ над GF(2). За определен клас от базиси е намерен тегловния спектър на двоичния образ.

3. Ю. Борисов, Н. Манев, Минимальные кодовые слова примитивного кода БЧХ, Проблемы передачи информации, 34 (1998), no. 3, 37-46:

Определено число минимальных (неминимальных) кодовых слов веса 10, 11 двоичного примитивного $[n = 2^m - 1, n - 2m, 5]$-кода БЧХ, исправляющего две ошибки, и слов веса 12 его расширенного кода.

Намерен е броят на минималните (неминималните) кодови думи с тегла 10, 11 в примитивния двоичен БЧХ $[n = 2^m - 1, n - 2m, 5]$-код, изправящ две грешки, и на минималните думи с тегло 12 в разширения му код.

4. Y. Borissov, N. L. Manev, S. Nikova, On the non-minimal codewords in binary Reed - Muller codes, Discrete Applied Mathematics, vol 128 (2003), no.1 pp. 65-74:

First, we compute the number of non-minimal codewords of weight $2d_{\min}$ in the binary Reed-Muller code $RM(r,m)$. Second, we prove that all codewords of weight greater than $2^m - 2^{m-r+1}$ in binary $RM(r,m)$, are non-minimal.

Намерен е броят на неминималните кодови думи с тегло $2d_{\min}$ в двоичния код на Рид-Малер $RM(r,m)$ и е доказано, че всички кодови думи с тегло по-голямо от $2^m - 2^{m-r+1}$ в двоичния $RM(r,m)$ са неминимални.

5. H. Kostadinov, H. Morita, N. L. Manev, Integer codes correcting single errors of specific types $(\pm\mathbf{e_1}, \pm\mathbf{e_2}, \ldots, \pm\mathbf{e_s})$, IEICE Trans. Fundamentals, vol. E86-A, no. 7, July 2003, pp. 1843-1849:

In this paper, we investigate the problem how to construct integer codes capable of correcting any single error in the set $\{\pm 1, \pm t, \ldots, \pm t^{k-1}\}$ and generalize our results to obtain $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ single error correctable codes where e_i's are different elements in $\mathbb{Z}_A$. Moreover, we shall give the exact form of the check matrix in most of the classes considered in this paper.

Изучават се кодове над крайни пръстени $\mathbb{Z}_A$ от остатъци по модул някакво естествено число A (мощност на алфавита). Дискутиран е проблемът как да се конструират кодове способни да изправят единични грешки от вида $\{\pm 1, \pm t, \ldots, \pm t^{k-1}\}$. Полученият резултат се обобщава до метод за намиране на кодове изправящи $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ единични грешки, където e_iтата са различни елементи на $\mathbb{Z}_A$. Нещо повече, дава се точната на проверочната матрица в повечето от разгледаните класове кодове.

6. Y. Borissov, N. L. Manev, Minimal codewords in linear codes, Serdica, vol. 30 (2004), no. 2-3, pp. 303 - 324:

Cyclic binary codes $\mathcal{C}$ of block length $n = 2^m - 1$ and generator polynomial $g(x) = m_1(x)m_{2^s+1}(x),\ (s,m) = 1$, are considered. The cardinalities of the sets of minimal codewords of weights 10 and 11 in codes $\mathcal{C}$ and of weight 12 in their extended codes $\widehat{C}$ are determined. The weight distributions of minimal codewords in the binary Reed-Muller codes $RM(3,6)$ and $RM(3,7)$ are determined. The applied method enables codes with larger parameters to be attacked.

Изследват се циклични кодове $\mathcal{C}$ с дължина $n = 2^m - 1$ и пораждащ полином $g(x) = m_1(x)m_{2^s+1}(x),\ (s,m) = 1$,. Определени са мощностите на множествата от минимални кодови думи с тегла 10 и 11 в $\mathcal{C}$ и с тегло 12 в $\widehat{\mathcal{C}}$. Намерено е тегловното разпределение на на минималните думи в $RM(3,6)$ and $RM(3,7)$. Приложените методи дават надежда, че ще могат да се атакуват и кодове с по-големи параметри.

7. H. Kostadinov, H. Morita, N. L. Manev, Derivation on bit error probability of coded QAM using integer codes, IEICE Trans. Fundamentals, vol. E87-A, no. 12 (Dec.2004), 3397-3403:

In this paper we present the exact expressions for the bit error probability over a Gaussian noise channel of coded QAM using single error correcting integer codes. It

is shown that the proposed integer codes have a better performance with respect to the lower on the bit error probability for trellis coded modulation The comparison of bit error probability versus signal-to-noise ratio between integer coded modulation and trellis coded modulation shows that the former has a better performance and less complexity

Намерена е формула за вероятността за грешка на бит (BER) при канал с Гаусов шум, когато при комуникацията е използвана модулация QAM (зададава се със съзвездие представляващо равнина решеткя) и код над $\mathbb{Z}_A$ изправящ единични грешки. Показано е, че тези кодове имат по-малка сложност и дават по-добро отношение на BER към сигнал/шум частното в срявнение с класическата trellis coded modulation.

8. M. H. Lee, N. L. Manev, Xiao-Dong Zhang, Jacket transform eigenvalue decomposition, Applied Mathematics and Computation, Elsevier, 198/2 (May 2008), pp. 858-864:

In this paper we give necessary and sufficient conditions for a Jacket decomposability. Some properties of Jacket matrices are also proved. Jacket matrices are interesting for an eigenvalue decomposition and signal processing because they are easily invertible.

Дадени са необходимите и достатъчни условия за диагонализируемост на матрици с Jacket матрици. Доказани са и някои свойства на Jacket матриците. Последните са интерестни защото лесно се намират обратните им матрици.

9. N. L. Manev, Sequences generating permutations, Applied Mathematics and Computation, Elsevier, Vol. 216 (2010), no. 3, pp. 708-718:

Linear recurring sequences generating permutations of the elements of a finite ring are introduced and examined. A complete answer to the discussed problems is given for the second-order sequences over $\mathbb{Z}_M$. The possibilities for applications are also discussed.

Изучавани са линейни рекурентни редици пораждащи пермутации на елементите на крайни пръстени. За редиците от втори ред над $\mathbb{Z}_M$ са дадени неоходими и достатъчни условия да са от разглеждания тип. Дискутирани са и възможни приложения.

10. N. L. Manev, Grid and simulation of digital communication systems, Serdica Journal of Computing, vol. 4 (2010), pp. 101-112:

The purpose of this paper is to turn researchers' attention to the usage of grid computing for simulating digital communications and its large potential for decreasing significantly the duration of the experiments and for improving statistical representativeness and reliability of the obtained results.

Целта на статията е да привлече вниманието на специалистите по комуникации към възможностите, които предлагат изчислителните грид технологи за сумулации на дигитални комуникационни системи. Използването им може

да намали драстично времето за експерименти и да повиши статистическата представителност и надежност на получените изводи.

11. H. Kostadinov, H. Morita, Noboru Iijima, A. J. Han Vinck, N. L. Manev, Soft decoding of integer codes and their application to coded modulation, IEICE Trans. Fundamentals, vol. E93-A (2010), no. 7, 1363-1370:

Integer codes are very flexible and can be applied in different modulation schemes. A soft decoding algorithm for integer codes will be introduced. Comparison of symbol error probability (SEP) versus signal-to-noise ratio (SNR) between soft and hard decoding using integer coded modulation shows us that we can obtain at least 2 dB coding gain. Also, we shall compare our results with trellis coded modulation (TCM) because of their similar decoding schemes and complexity.

Кодовете над $\mathbb{Z}_M$ са много гъвкави по отношение на възможтта за прилагане в разлчни системи за модулация. В статията се дава алгоритъм за меко декодиране на такива кодове. Сравнението на отношенията вероятност за грешка на символ (SEP) към частното сигнал/шум (SNR) между мекото и твърдото декодиране при използване на кодове над $\mathbb{Z}_M$ показва подобрение от 2 db в полза на мекото. Положителни са и сравненията с класическата trellis coded modulation (TCM).

12. H. Kostadinov, H. Morita, N. L. Manev, On (± 1) **Error Correctable Integer Codes, IEICE Trans. Fundamentals, vol. E93-A (2010), no. 12, pp. 2758-2761**:

Integer codes correct errors of a given type, which means that for a given communication channel and modulator we can choose the type of the errors (which are the most common) then construct integer code capable of correcting those errors. A new general construction of single (± 1) error correctable integer codes will be presented. Comparison between single and multiple (± 1) error correctable integer codes over AWGN channel using QAM scheme will be presented

Кодовете над $\mathbb{Z}_M$ изправят грешки от даден тип, което дава възможност за дадени комуникационнен канал и модулатор да определим най-често срещания тип грешки и да конструираме код изправящ този тип грешки. В статията се предлага нова обща конструкция на кодове коригиращи единични (± 1) грешки. Дадено е и сравнение между кодове кригиращи единични и многократни (± 1) грешки по канал с бял адитивен Гаусов шум и QAM модулация

2 Статии в поредици и глави от книги

1. Y.Borissov, N.Manev, Some Comments on Bossert-Mahr-Heilig Scheme, Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 23, IOS Press, 2009, pp. 244-249:

In 1993, Bossert, Mahr and Heilig proposed a cryptographic scheme based on error-correcting codes that provides simultaneously error correction and message authentication. They also sketched out an idea how their scheme to be analyzed. Developing their idea after detailed analysis we reveal an weakness in a concrete implementation which can be exploited by active intruder to maintain an attack with considerable probability of success. Countermeasures against this probabilistic attack are given

В 1993 Bossert, Mahr и Heilig предложиха криптографска схема базирана на кодове изправящи грешки, която реализира едновременно аутетификация на съобщението и поправя грешки в него причинени в процеса на комуникация. В работата си те дават идея и как схемата им да бъде анализирана. Развивайки тази идея след детаилен анализ ние посочваме слабост на схемата, която би позволила при определена реализация да се осъществи атака със значителна вероятност за успех. Предлагаме контрамерки за да се избегне тази възможност.

2. S. Boumova, H.Kostadinov, N.L.Manev, Watermarking, steganography, and error-control codes, American Institute of Physics Conference proceedings, vol. 1404, 193-199:

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 устойчивост на влаганата информация.

3. S. Ivanovska, A. Karaivanova, N. L. Manev, Numerical integration using sequences generating permutations, LSSC 2011, Lecture Notes in Computer Sciences, Springer, 2012, vol. 7116 (2012), pp. 455-463:

In this paper we propose a new class of pseudo random number generators based on a special linear recursions modulo m. These generators produce sequences which are permutations of the elements of a $\mathbb{Z}_m$. These sequences have been developed for

other applications but the analysis of their statistical properties and the experiments described in this paper show that they are appropriate for multiple integration. Here we present some results from numerical tests comparing the performance of the two proposed generators with Mersenne Twister.

В статията се описва нов клас генератор на псевдослучайни числа, който се използва за интегриране на многомерни интеграли. Генераторът се базира на рекурентна редица, която дава пермутация на елументите на $\mathbb{Z}_m$. Числените експерименти за сравняване на разглеждания генератор с генератора Mersenne Twister. показва, че новият генератор дава най-малко същите (често и по-добри) резултити в тези приложения.

4. T. Gurov, S. Ivanovska, A. Karaivanova, N.L.Manev, Monte Carlo methods using a new class of congruential generators, L. Kocarev (Ed.): ICT Innovations 2011, AISC Volume 150, pp. 257-267, Springer-Verlag Berlin Heidelberg, 2012:

In this paper we propose a new class of congruential pseudo random number generator based on sequences generating permutations. These sequences have been developed for other applications but our analysis and experiments show that they are appropriate for approximation of multiple integrals and integral equations.

Нов клас генератор на псевдослучайни числа базиран на рекурентни редици се тества за симулации и числено решаване на интегрални уравнения описващи процеса на движение на електроните в полупроводници.

5. E. Atanassov, D. Georgiev, N. L. Manev, Number Theory Algorithms on GPU Clusters, M. Dulea et al. (eds.), High-Perf. Comp. Infrastr. for South East Europe's Research Communities, Modeling and Optimization in Science and Technologies 2, Springer International Publishing Switzerland 2014, Volume 2, pp. 131-138:

Many algorithms from Number Theory and their implementation in software are of high practical importance, since they are the building primitives of many protocols for data encryption and authentication of Internet connections. Number theory algorithms are also the basic part of cryptanalytic procedures. Many of these algorithms can be parallelized in a natural way. In this paper we describe our efforts to develop a software package that implements various Number Theory algorithms on GPU clusters and in partial our implementations of integer factorization using NVIDIA CUDA on clusters equipped with NVIDIA GPUs. Also we report results of our experiments regarding the performance of our implementation.

Много алгоритми от теория на числата са в основата на криптографски примитиви и протоколи. В статията се описват усилията ни да се разработи софтуерен пакет реализиращ на GPU клъстер различни алгоритми от теория на числата и в частност алгоритъм за разлагане на множители на големи цели числа чрез алгебрични криви. Езикът с който се програмира е NVIDIA CUDA.

3 Статии в сборници от трудове на конференции

1. N.Manev, S. Topalova, Software system for testing Reed-Solomon codes in different channel, Proceedings of XXI Spring Conference of Union of Bulgarian Mathematicians, April 3-6, 1992:

Описана е софтуерна система реализираща декодиране с алгоритъм на Евклид на код на Рид-Соломон изправящ l грешки над $GF(2^7)$ и интерливинг. Системата е разработена за да се тестват различни параметри върху данни от реални полеви условия събрани от военното училище във В. Търново (данните са от грешките при радиокомуникации между свързочни поделения на територията на България).

2. S. Ilieva, N.L.Manev, Error-correcting pairs for binary cyclic codes of length 63 and 65, Proceeding of IV Int. Workshop on Algebraic and Combinatorial Theory, September 11-17, 1994, Novgorod, pp.102-106

The error-correcting pairs for binary cyclic codes of length 63 and 65 with $d > d_{BCH}$ have been found by computer search.

С компютърно търсене са намерени така наречените двойки кодове за изправяне на грешки за двоични циклични кодове с $d > d_{BCH}$ и дължини 63 и 65.

3. E.Kolev, N.L.Manev, The binary weight distribution of concatenated codes based on Reed-Solomon codes, Proceeding of IV Int. Workshop on Algebraic and Combinatorial Theory, September 11-17, 1994, Novgorod, pp.116-121.

Consider $[2^m, k, 2^m - k + 1]$ extended Reed-Solomon code. If every coordinate symbol is represented by the corresponding m-tuple over $GF(2)$ using a basis of $GF(2^m)$ and a parity check symbol is added to each m-tuple we obtain a $[(m+1)2^m,\ mk]$ binary code. Herein we determine the binary weight distribution of the obtained concatenated binary code for $k \leq 3$. The distribution does not depend on the basis. For $k = 4$ and m odd the binary distribution is calculated and the dependence with the basis is revealed.

Ако всяка координата в $[2^m, k, 2^m - k + 1]$ разширен код на Рид-Соломон се замени с m-орката над $GF(2)$ използвайки някакъв базис на $GF(2^m)$ и се добави проверка по четност към всяка такава m-орка се получава двоичен $[(m + 1)2^m,\ mk]$ код. В тази статия определяме тегловното разпределение на

получения двоичен код за $k \leq 3$ и показваме, че не зависи от избора на базиса. При $k = 4$ и m нечетно разпределението също е намерено и е определена зависимоста му от базиса.

4. Y. Borissov, N.L.Manev, A note on the Stern's syndrome identification scheme, Proceedings of XXVI Spring Conference of Union of Bulgarian Mathematicians, April, 1997:

The security of a variant of the Stern's syndrome identification scheme is analyzed as well as some measures for improving the scheme are proposed. In particular, an answer to the question formulated by Stern is given.

Изследвана е сигурността на вариант на схемата за идентификация на Щерн. Предложени са мерки за подобряване на сигурността. В частност е даден отговор на въпроса поставен от Щерн.

5. Y. Borissov, N.L.Manev, Minimal codewords of weight 10 in the cyclic code with generating polynomial $m_1(x)m_5(x)$, Proceedings of XXVII Spring Conference of Union of Bulgarian Mathematicians, April, 1998, pp. 183-189:

The number of nonminimal codewords of weight 10 is determined for the class of cyclic codes with zeros α and α^5, where α is a primitive element of the field $GF(2^m)$

Определя се броят на неминималните кодови вектори с тегло 10 за клас от циклични кодови с нули α и α^5, където α е примитивен елемент на полето $GF(2^m)$

6. N.L.Manev, Error-correcting codes in cryptography (Invited lecture), Proceedings of XXVII Spring Conference of Union of Bulgarian Mathematicians, April, 1998, pp. 48-62:

The purpose of this paper is to make the reader acquainted with the applications of error-correcting codes in designing cryptographic systems as well as to serve as a brief introduction into the cryptography as whole. Throughout the text the emphasis is on explaining the main ideas rather than providing results in complete generality.

Целта на статията е да запознае читателите с приложенията на кодовете изправящи грешки за проектиране на криптографски системи. Наблегнато е поскоро на излагането на идеите и принципите, отколкото на конкретни резултати.

7. Y. Borissov, N.L.Manev, Minimal codewords in binary cyclic codes of length 31, Proceed. of the II Intern. Workshop on Optimal Codes and Related Topics , 1998, pp. 19-27:

It is shown that two classes of codes are intersecting. Set of minimal codewords for any cyclic code of length 31 is described.

За два класа кодове е доказано, че са "intersecting". За всички циклични кодове с дължина 31 са определени множествата от минималните им думи.

8. T. Nikolov, N. L. Manev, On the binary complementary sequences, Proceeding of the VII International Workshop on Algebraic and Combinatorial Coding Theory, 2000, pp. 245-250.:

We describe a new algorithm for searching pears of complementary sequences and apply it to check all possible lengths $n \leq 100$.

Представяме нов алгоритъм за търсене на двойки допълващи се редици и прилагаме този алгоритъм за да търсим такива редици за дължини $n \leq 100$..

9. N. L. Manev, F. A. Sallam, Primes of shape 2pq+1, p,q primes, Proceeding of the conference "20 years mathematics and informatics in VTU "St. St. Kiril and Metodi", May 12-13, 2006, V.Turnovo, pp. 75-80 (докладвано на MASSEE Int. Congress on Mathematics, May 31 Ц June 4, 2006, Cyprus):

The primes of the form $2pq + 1$, where p and q are also primes are considered. Some properties of these numbers are given and their distribution is studied. A special attention is paid to the cases $q = p + 2$ (twin primes) and $q = p + 4$ (cousin primes). How to calculate (with a prescribed accuracy) the constants defined in this paper is described, too.

Разглеждат се прости числа от вида $2pq+1$, където p и q са също прости и се доказват някои техни свойства. Изследва се и разпределението им. Специално внимание се обръща на числата ''близнаци" ($q = p+2$) и ''братовчеди" ($q = p+4$). Пресмятането на константите на разпределението се свежда до пресмятане с много голяма точност (до 500-я знак) на дзета функцията и L-функцията на Дирихле.

10. H. Kostadinov, H. Morita, N. L, Manev, A. J. Han Vinck, Coded modulation with single error correctable integer codes, 10th Int. Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, Russia, Sept. 3-9, 2006:

In this paper we proposed two constructions of single error correctable integer codes and showed how to apply them to QAM and PSK schemes. The comparison on bit error probability versus signal-to-noise ratio between ICM and TCM shows that ICM and TCM have almost the same performance. As advantage of ICM we can point out the low decoding complexity. We proposed soft decoding algorithm for single error correctable integer codes. From the experimental results we can conclude that the soft decoding algorithm using single error correctable integer codes has better performance than the hard decoding algorithm for small value of code length n. For larger value of n the soft decision decoder is substantially more complex than the hard decision decoder. The using of integer codes capable of correcting more than one error makes it possible to improve the performance, but increases the complexity.

Предлага т се две конструкции на кодове над $\mathbb{Z}_A$ изправящи единични греш-

ки и приложението им при QAM и PSK модулации. Сравнява се BER по отношение на SNR при приложението на тези кодове (ICM) и трелис кодирането (TCM). Нашият метод дава същите резултати при значително по-малка сложност на реализация. Ако се приложи и предлаганото меко декодиране се получават по-добри резултати.

11. H. Kostadinov, N. L. Manev, H. Morita, Double ± 1-error correctable codes and their applications to modulation schemes, Eleventh Int. Workshop on Algebraic and Combinatorial Coding Theory, June 16-22, 2008, Pamporovo, pp. 155-160:

Codes capable to correct two errors of value ± 1 in a codeword are constructed and studied. Large number of experiments simulating the implementation of several double ± 1-error correctable codes in QAM-modulation schemes have been carried out. The obtained results present in graphical form the performance of the coded modulation schemes based on the considered codes versus signal-to-noise ratio (SNR). The results confirm the good performance of integer coded modulation in comparison to the other schemes for coded modulation.

Конструират се и изследват кодове изправящи две грешки от вида ± 1. Голям брой експерименти с такива кодове при QAM модулационни схеми са реализирани. Получените резултати са представени в графична форма по отношение на частното сигнал/шум. Резултатите подтвърждават добрите качества на разглежданите кодове.

12. H. Kostadinov, N. L. Manev, N. Iijima, H. Morita, Double error correctable integer code and its application to QAM, Proceedings of the IEEE International Symposium on Information Theory and Its Applications (ISITA2008), Auckland, New Zenland, December 7-10, 2008, pp. 566-571:

A new construction of double error correctable integer codes and their application to QAM scheme are presented. Soft decoding algorithm for multiple error correctable integer code which are suited to any modulation scheme (QAM, PSK, ASK) will be introduced. Comparison of bit error rate (BER) versus signal-to-noise ratio (SNR) between soft and hard decoding using integer coded modulation (ICM) shows us that we can obtain approximately 2 dB coding gain.

Конструира се нов изправящ две грешки код над $\mathbb{Z}_m$ и се прилага за QAM схеми. Дава се и алгоритъм за меко декодиране подходящо за различни модулационни схеми (QAM, PSK, ASK). Сравняването на вероятността за грешка на бит (BER) по отношение на сигнал/шум (SNR) между мекото и твърдо декодиране при описаната ICM показва подобрение от 2 dB.

13. E. Atanassov, D. Georgiev, N. L. Manev, ECM Integer factorization on GPU Cluster, Proceeding of MIPRO 2012 - Jubilee 35th International Convention on information and communication technology, DC-VIS -

Distributed Computing and Visualization Systems, May 21-25, 2012, Opatija, Croatia, pp. 343 - 347:

The problem of integer factorization is of high practical importance because of the widespread use of public key cryptosystems for encryption and authentication of Internet connections. In this paper we describe our implementation of the elliptic curve method of integer factorization on an NVIDIA GPU-based cluster using the CUDA technology and report the results of our experiments. The performance of our implementation is compared with other known experiments and software.

В статията описваме наша имплементация върху NVIDIA GPU клъстер с използване на CUDA езика на метод за разлагане на големи цели числа базиран на елиптични криви.

14. H. Kostadinov, N. L. Manev, On codes for flash memory, proceeding of the Thirteenth Inernational Workshop on Algebraic and Combinatorial Coding Theory, June 15-21, 2012, Pomorie, pp. 197-202:

In this paper, we give a construction of a single asymmetric 2-limited magnitude error correctable code and apply it to solve the problem of writing data in flash memories. For some parameters, the codes we obtained by this construction are optimal.

Описва се конструкция на кодове изправящи единични до 2 нива грешки и прилагането им при запис на данни на флаш памет.

15. H. Kostadinov, N. L. Manev, On integer code correcting single error of type $(\pm 1; 2)$, Proc. of Seventh International Workshop on Optimal Codes and Related Topics OC 2013 September 6 - 12, 2013, Albena, Bulgaria, pp. 134-139:

In this work we have presented a new class of single error correctable integer codes designed for an application in a flash memory. Moreover, we gave the exact form of the check matrix for those codes. The decoding complexity of the codes is linear, regarding to the code length, and can be used a look-up table to decode them. All these advantages of integer codes makes them very suitable for their usage in the practice.

Даваме нов клас от кодове над $\mathbb{Z}_m$ поправящи една грешка специално създаден за приложение във флаш паметите. Определяме и точния вид на проверочната матрица на тези кодове. Сложността при декодиране за тези кодове е линейна по дължината им и за практически цели може да се реализира таблично.

4 Учебни материали

Лекции по теория на числата

Лекциите бяха написани за да покрият материала, който четях в курса по теория на числата за бакалаври във ФМИ на СУ "Св. Кл.Охридски". Базисният материал се състои от 7 глави:

Гл.1. **Аритметика**. След аксиоматичното (Пеано) построяване на естествените числа и разширяването им до пръстена на целите числа се формулират и доказват основните аритметични свойства на целите числа. Разглеждат се сложност на аритметичните операции и верижни дроби.

Гл.2. **Разпределение на простите числа**. Разглеждат се основните аритметични функции и с елементарни методи се получават някои оценки за разпределението на простите числа. След това се формулира известната теорема за асимптотичното разпределение на простите числа.

Гл.3. **Сравнения**. Установяват се основните свойства на сравненията и се доказва китайската теорема. Описва се общ метод за решаване на нелинейни полиномиални сравнения. Дефинират се примитивни корени и индекси и се намират всички естествени числа n, за които обратимите остатъци по модул n образуват циклична група.

Гл.4. **Квадратични остатъци.**. Разглеждат се квадратични и k-степенни остатъци, доказва се законът за реципрочност и необходимите и достатъчни условия за преставяне като сума от квадрати.

Гл.5. **Нелинейни диофантови уравнения**. Изследват се изчерпателно диофантовите уравнения от втора степен на две променливи и в частност уравнението на Пел.

Гл.6. **Криптография**. Увод в криптографията като се обръща внимание на приложението на теорията на числата.

Гл.7. **Теоретико-числови преобразования**. Описва се дискретното преобразуване на Фурие.

Последната година реших да добавя и материала от курса за магистри, който има алгоритмична насоченост и включва и допълнителни материали. За съжаление напълно завършена и качена on-line е само Гл. 10: Елиптични криви. В нея се дава кратко въведение към кривите използвани в криптографските стандарти и описание на криптографските протоколи основани на елиптични криви. Подготвям материалите за различните алгоритми за разлагане на цели числа (Глава 9), допълнителни параграфи към Гл.5 Нелинейни диофантови уравнения и Глава 8 с различни алгоритми за модулярна аритметика.

Лекциите са налични само on-line : на сайта на ФМИ (учебници) и на http://sharoacademy.math.bas.bg/NumbTh.html

Кодиране и криптография

Лекциите са налични в книжен и електронен формат. Книжният вече е изчерпан, електронният е по-пълен, съдържа повече информация. Има и слайдове на английски - съдържанието на курса, който четох в Chonbuk University в Южна Корея. Учебникът съдържа увод в теория на информацията, материали по теория кодирането, в това число и описание на алгоритми за декодиране на циклични кодове, и увод в криптографията. В електронния вариант (http://sharoacademy.math.bas.bg/CodingTh.html) към главата по криптография е добавен и увод в стеганографията с примери за използване на кодове изправящи грешки. В on-line лекциите са разтледани и LDPC кодовете.

MATLAB в механиката и съпротивление на материалите

Този учебен материал е написан във връзка с курса по Matlab, който водих летния семестър на 2013 г. Следва общо взето материала по съпромат и примерите са по варианти на курсови задачи. В процес на разширение е.