ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 141–144
ISSN 1930-1235: (2008)

ALGEBRAIC ASPECTS OF DIGITAL COMMUNICATIONS

T. Shaska

Department of Mathematics and Statistics
Oakland University,
Rochester, MI, USA
shaska@oakland.edu

M. Qarri

Department of Computer Science and Electrical Engineering
University of Vlora,
Vlora, Albania
mbifsha@univlora.edu.al

Developments of the last few decades in digital communications have created a close link between mathematics and areas of computer science and electrical engineering. A collaboration between such areas now seems very natural due to problems which require deep knowledge and expertise in each area. A special role in such collaboration has played algebra and some of its branches such as algebraic geometry, computational algebra, group theory, etc. As a result of such cooperation now we have disciplines such as coding theory and cryptography which are considered a mix of mathematics, computer science, and electrical engineering.

Coding theory is one of the most important and direct applications of information theory. It is a branch of electrical engineering, digital communication, mathematics, and computer science designing efficient and reliable data transmission methods, so that redundancy in the data can be removed and errors induced by a noisy channel can be corrected. It started with Shannon, Hamming, and many others in the mid 20-th century and became one of the most active areas of research for most of the second half of the 20-th century. Algebraic coding theory was the main direction of coding theory, even though recently other ways of coding have been developed. For more details in coding theory a wonderful source is [2] among many other publications.

Cryptology, is the science of hiding information, and historically has received much attention from the public. As a science was also put in solid background in the second half of the 20-th century. It is a mixture of theoretical mathematics and computer science which focuses more in areas such as number theory, algebraic geometry, graph theory, algorithm analysis, etc. There have been many conferences and publications which have explored the common ground among such areas; some of the more recent ones are [6, 7].

This special issue came out of the conference "New Challenges in Digital Communications" which was organized at the University of Vlora, during April 27 - May 9, 2008. This was funded by a NATO grant as a "Advanced Study Institute"; see [4], [5] for details. The conference focused precisely on connections between algebra, algebraic geometry, number theory, graph theory, and related areas of mathematics with coding theory and cryptography.

There were over 130 participants in the conference from all over the world. We want to thank NATO, the University of Vlora, and the Albanian Ministry of Science and Education for providing the funding of such conference. Special thanks to all the staff of the University of Vlora who were involved in all organizational tasks of the conference, especially the Department of Mathematics and the Department of Computer Science and Electrical Engineering, and the Vlora Conference Center at the University of Vlora.

Most of the papers focus on coding theory and some others in cryptography. While such topics were the main focus of the conference, we did accept papers which explore more theoretical aspects such as computational group theory, computational algebraic geometry, etc. There are overall 13 papers in this volume which cover a wide range of topics. There is also a proceedings volume of the conference which will be published by NATO. This volume will contain all the lectures which were held during the Advanced Study Institute; see [3].

We hope that such collection of papers will serve the scientific community in mathematics, computer science, and electrical engineering and foster closer relations among such communities. It is our intention to organize yearly conferences in Vlora in similar topics and with similar goals.

Acknowledgements: We sincerely thank all the authors for their contributions of this special issue. We also thank the anonymous referees for all their work going through all the papers. Our final thanks to NATO for sponsoring such conference.

1. Aspektet algjebrike te komunikacioneve dixhitale

Zhvillimet e dekadave të fundit në fushën e komunikimit dixhital kanë krijuar një lidhje të ngushtë midis matematikës dhe fushave të inxhinierisë kompjuterike dhe elektrike. Një bashkëpunim ndërmjet këtyre fushave tashmë duket tepër natyral në sajë të problemeve që kërkojnë njohuri të thella dhe ekspertizë në secilën fushë. Një rol të vecantë në një bashkëpunim të tillë ka luajtur algjebra dhe disa nga degët e saj të tilla si gjeometria algjebrike, algjebra kompjuterike, teoria e grupeve, etj. Si rezultat i një bashkëpunimi të tillë tani disponojmë disiplina të tilla si teoria e kodeve dhe kriptografia, të cilat janë konsideruar si përzierje e matematikës, inxhinierisë se shkencave kompjuterike dhe elektrike.

Teoria e kodeve është një nga aplikimet më të rëndësishme dhe të drejtpërdrejta të teorisë së infomacionit. Ajo është një degë e inxhinierisë elektrike, komunikimit dixhital, matematikës dhe shkencave kompjuterike, që përdor metoda eficente dhe të besueshme të transmetimit të të dhënave, në mënyrë që të eleminohen humbjet në informacionet dhe të korrigjohen gabimet e induktuara nga një kanal zhurme. Kjo degë ka filluar me Shannon, Hamming dhe shumë të tjerë në mes të shekullit XX dhe u bë një nga fushat më aktive të kërkimit për pjesën më të madhe të gjysmës së shekullit XX. Teoria e kodeve algjebrike ishte një nga drejtimet kryesore të teorisë së kodeve, edhe pse së fundmi mënyra të tjera kodimi janë zhvilluar. Për

më shumë detaje në teorinë e kodeve një burim i mrekullueshëm është : [2] midis publikimeve të tjera.

Kriptologjia është shkenca e fshehjes së informacionit, dhe historikisht ka qenë në vëmendjen e publikut. Si shkencë gjithashtu ka marrë formën e plotë në gjysmën e dytë të shekullit XX. Ajo është një kombinim i matematikës teorike dhe shkencës kompjuterike, e cila fokusohet me shumë në fusha të tilla si teoria e numrave, gjeometria algjebrike, teoria e grafeve, analiza algoritmike, etj. Janë zhvilluar shumë konferenca dhe ka patur mjaft publikime të cilat kanë eksploruar bazën e përbashkët midis këtyre fushave; ndër më të fundit janë [6, 7].

Ky numër i vecantë i revistës *Albanian J. Math.* rezultoi nga konferenca "Sfida të reja në Komunikimin Dixhital", e cila u organizua pranë Universitetit të Vlorës, gjatë periudhës 27 Prill- 9 Maj, 2008. Ajo u financua nga një grant i NATO-s si "Instituti i Studimeve të Avancuara"; për detaje shih [4], [5]. Konferenca u përqëndrua saktësisht në lidhjet midis algjebrës, gjeometrisë algjebrike, teorisë së numrave, teorisë së grafeve, dhe fushave të tjera të matematikës të lidhura me teorinë e kodeve dhe kriptografinë.

Në konferencë kishte më shumë se 130 pjesëmarrës nga e gjithë bota. Ne duam të falënderojmë NATO-n, Universitetin e Vlorës dhe Ministrinë e Arsimit dhe Shkencës shqiptare që na siguruan fondet për një konferencë të tillë. Një falënderim i vecantë shkon për gjithë stafin e universitetit të Vlorës që mori pjesë në detyrat organizative, vecanërisht Departamentin e Matematikës dhe të Shkencave Kompjuterike dhe Elektrike, dhe Qendrën e Konferencave Vlorë pranë Universitetit të Vlorës.

Pjesa më e madhe e artikujve përqëndrohen tek teoria e kodeve dhe disa prej tyre në kriptografi. Ndërsa këto tema ishin fokusi kryesor i konferencës, ne pranuam edhe artikuj që eksploronin më shumë aspekte teorike të tilla si toeria e grupeve llogaritëse, gjeometria algjebrike llogaritëse, etj. Janë gjithsej 13 artikuj në këtë volum që mbulojnë një gamë të gjerë cështjesh. Gjithashtu, ekziston një volum i punimeve të konferencës që do të publikohet nga NATO. Ky volum do të përmbajë gjithë leksionet që u mbajtën gjatë Institutit të Studimeve të Avancuara; shih [3].

Ne shpresojmë që ky koleksion artikujsh do t'i shërbejë komunitetit shkencor të matematikës. Shkencave kompjuterike dhe inxhinerisë elektrike dhe do t'i japë zhvillim marrëdhënieve të ngushta midis këtyre komuniteteve. Qëllimi ynë është që të organizojmë në Vlorë cdo vit konferenca të tilla me tema të ngjashme dhe me objektiva të ngjashëm.

Ne falënderojmë sinqerisht të gjithë autorët për kontributin e tyre në këtë cështje të vecantë. Ne falënderojmë gjithashtu shkruarësit anonimë të referencave për punën e tyre mbi gjithë këto artikuj. Dhe falënderimi ynë final shkon tek NATO për sponsorizimin e kësaj konference.

References

[1] W. Cary Huffman, *Codes and groups*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1345–1440. MR1667953

[2] V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds.), *Handbook of coding theory. Vol. I, II*, North-Holland, Amsterdam, 1998. MR1667936 (2000h:94001)

[3] T. Shaska, *New Challenges in Digital Communications*, IOS Press, Brussels, 2008.

[4] *NATO Science for Peace and Security Programme.* Website: http://www.nato.int/science/index.html.

[5] *NATO Advanced Study Institute New Challenges in Digital Communications.* Directors:T. Shaska, E. Hasimaj; April 27 - May 9, 2008, Vlora, Albania.

[6] Tanush Shaska (ed.), *Computational aspects of algebraic curves*, Lecture Notes Series on Computing, vol. 13, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005. Papers from the conference held at the University of Idaho, Moscow, ID, May 26–28, 2005. MR2182657 (2006e:14003)

[7] T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko (eds.), *Advances in Coding Theory and Cryptography*, Developments in Mathematics, vol. 12, World Scientific, Hackensack, NJ:, 2007.

[8] Helmut Voelklein and Tanush Shaska (eds.), *Progress in Galois theory*, Developments in Mathematics, vol. 12, Springer, New York, 2005. MR2150438 (2006a:00014)

[9] W. Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. MR1996953 (2004k:94077)

[10] V. A. Ustimenko, *On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography*, Albanian J. Math. **1** (2007), no. 4, 283–295. MR2367220 (2008k:05111)

[11] Arnaldo Garcia and Henning Stichtenoth (eds.), *Topics in geometry, coding theory and cryptography*, Algebras and Applications, vol. 6, Springer, Dordrecht, 2007. MR2265387 (2007h:11003)

[12] Gary L. Mullen, Henning Stichtenoth, and Horacio Tapia-Recillas (eds.), *Finite fields with applications to coding theory, cryptography and related areas*, Springer-Verlag, Berlin, 2002. MR1995324 (2004c:11003)

[13] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Wall, *Coding theory and cryptography: the essentials*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 234, Marcel Dekker Inc., New York, 2000. Second edition, revised and expanded. MR1792696 (2002h:94091)

[14] David Joyner (ed.), *Coding theory and cryptography*, Springer-Verlag, Berlin, 2000. From Enigma and Geheimschreiber to quantum theory; Papers from the Conference on Coding Theory, Cryptography, and Number Theory (Cryptoday) held in Annapolis, MD, October 25–27, 1998. MR1747832 (2000k:94042)

[15] T. Shaska and G. S. Wijesiri, *Codes over rings of size four, Hermitian lattices, and corresponding theta functions*, Proc. Amer. Math. Soc. **136** (2008), no. 3, 849–857 (electronic). MR2361856 (2008m:11132)

[16] A. Elezi and T. Shaska, *Special issue on algebra and computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 175–177. MR2367211

[17] Tanush Shaska and Quanlong Wang, *On the automorphism groups of some AG-codes based on $C_{a,b}$ curves*, Serdica J. Comput. **1** (2007), no. 2, 193–206. MR2363086 (2008m:94029)