Mathematics of Communications: Sequences, Codes and Designs (15w5139)

Shamgar Gurevich (University of Wisconsin-Madison),
Jonathan Jedwab (Simon Fraser University),
Dieter Jungnickel (Universität Augsburg),
Vladimir Tonchev (Michigan Technological University)

25–30 January 2015

1 Overview

Modern society depends crucially on the ability to store and transmit large amounts of digital information at high speed. Satellite communication, movies on demand, portable music players, flash drives, and cellphones all rely on the mathematical theory of coding to ensure that the original images, speech, music, or data can be recovered perfectly even if mistakes are introduced during storage or transmission [2], [27]. As coding theory has developed over the last 65 years, deep connections with the theory of combinatorial designs [1], [3], [7] and with sequences [18] [20], have been discovered. Emerging applications continually lead to new problems of codes, designs and sequences; conversely, new theoretical developments in these areas enable novel applications [8].

The workshop brought together representatives of the applied and theoretical communities that study the mathematics of communications, working in Mathematics, Computer Science, and Engineering departments, in order to promote new linkages and collaborations. Among the participants were four graduate students and two postdoctoral fellows. Five speakers gave extended expository lectures, accessible to all participants, with an emphasis on methods, approaches, and open questions. Nineteen speakers gave contributed talks on a range of theoretical and practical topics. A panel discussion gave participants an opportunity to reflect on the entire workshop and to assess future research directions. Throughout these events, as well as in numerous individual interactions, participants exchanged information and ideas about both theoretical and practical aspects, and identified new connections between the principal objects of study.

2 Presentations

Codes and Designs

Tuvi Etzion opened the workshop with a wide-ranging expository talk illustrating many of the deep connections between coding theory and design theory. His examples included classical connections between perfect codes, Steiner systems, maximum distance separable (MDS) codes, and projective geometries, as well as modern applications of codes and designs in write-once memory [32], network coding [31], and distributed storage. Etzion emphasized throughout that, despite considerable recent progress, major open problems remain.

Coding Theory and Patent Law

Jim Davis gave a fascinating account of his role as a testifying expert in 2012, in one of the more than fifty patent lawsuits fought in multiple jurisdictions between Apple and Samsung over third generation wireless technology. The disputed patent [23] describes a method for transmitting multiple services simultaneously and correctly, and is essential to an international standard that ensures wireless devices can interoperate. The technical heart of the patent centres on a specific subcode of the second order Reed-Muller code of length 32. Davis described how academic questions of coding theory intersected with patent law, against a backdrop of intense global competition in the mobile communications market. The dispute culminated in 2013 in President Obama's overturning of an International Trade Commission ban on the import of certain models of Apple products into the U.S., which was the first time a U.S. President had vetoed such a ban in more than 25 years [29].

Sequences

Maximal linear recursive sequences (m-sequences) are used extensively in digital communications and remote sensing because of their favorable correlation properties [17]. Excluding trivial cases, the cross-correlations of a pair of m-sequences must take at least three distinct values. An equivalent formulation is that the dual of a cyclic error-correcting code with two primitive zeroes must have at least three nonzero weights. Until recently, only ten infinite families of m-sequence pairs attaining the minimum number (three) of distinct values were known. Daniel Katz (with P. Langevin) established the existence of an eleventh such family [21], and so proved a 2001 conjecture due to Dobbertin, Helleseth, Kumar, and Martinsen [11]. Katz's talk was the first public lecture describing this result, and Tor Helleseth was present as one of the workshop participants. In his talk, delivered very effectively on a chalkboard, Katz gave a careful overview of the study of m-sequences before outlining the proof of the conjecture involving trilinear forms, enumeration of points on curves via multiplicative character sums, and divisibility properties of Gauss sums.

A linear feedback shift register (LFSR) is a physical device for generating sequences over a finite field, including m-sequences. A transformation shift register is a generalization of an LFSR that confers practical advantages when used in a stream cipher. Whereas the number of irreducible LFSRs over a finite field is well known, the number of irreducible transformation shift registers in general is not. Daniel Panario's talk examined this counting question for irreducible transformation shift registers, giving an asymptotic formula for some special cases using classical results due to Cohen [6], and a new proof of Ram's exact formula for order two using Ahmadi's recent generalization of a theorem due to Carlitz.

Difference sets correspond to sequences or arrays with constant out-of-phase periodic autocorrelation. They are often studied by applying characters to a group ring equation, resulting in a set of Weil numbers that must satisfy certain mutual properties [25] [35]. Bernhard Schmidt considered the contrary question: when does a single Weil number yield a solution of a group ring equation? This not only gives immediate nonexistence results for relative difference sets, but allows progress to be made in problems involving unique differences in cyclic groups.

Network Coding

In multicast network communications, data is sent to several receivers at the same time. Network coding permits multiple sources to transmit simultaneously to multiple receivers, by allowing each intermediate network node to re-encode information via linear combination of its inputs. This process is highly sensitive to errors, because a single corrupted message can affect the entire network via successive linear combinations with other messages. For this reason, effective error control is a crucial requirement in network coding [34]. In her expository lecture, Emina Soljanin of Bell Labs gave a broad survey of the main ideas from information theory, algebra, and combinatorics. She then focussed on the combinatorial framework, showing how practical questions of network coding lead to fundamental open problems involving arcs in projective spaces.

Two very important classes of codes now used in network coding are the rank metric codes introduced by Gabidulin in 1985 [12] and the closely related subspace codes. A rank metric code consists of $n \times n$ matrices over $\mathbb{F}_q$ with the distance function $d(X, Y) = \operatorname{rank}(X - Y)$; these codes are also useful in space-time coding [26] and distributed storage.

Relinde Jurrius investigated the rank weight enumerator of a rank metric code and some of its generalizations, namely the r-th generalized rank weight enumerator and the extended rank weight enumerators. Analogously to results for ordinary linear codes, these objects determine each other. Moreover, Jurrius used counting polynomials to extend her results from the case of codes over $\mathbb{F}_q$ to codes over a finite field extension.

Arguably the most important subclass of rank metric codes is given by the linear maximum rank distance codes (MRD codes) which were constructed by Gabidulin; these are analogues of the classical Reed-Solomon codes. Anna-Lena Trautmann addressed the practical problem of list decoding the Gabidulin codes, using minimal bases of linearized polynomial modules. Her decoding algorithm computes a list of all closest codewords to a given received word. Although the complexity of the algorithm becomes exponential as soon as the closest codewords are beyond the unique decoding radius, it still beats the complexity of exhaustive search.

John Sheekey considered MRD codes that are not necessarily linear; the first non-trivial example of a non-linear MRD code was recently given by Cossidente, Marino and Pavese for the case where $n = 3$ and the minimum distance d is 2. Sheekey studied the case $d = n$, which corresponds to a finite semifield (namely a non-associative division algebra). He gave an overview on semifields (which have been studied intensively in recent years for other reasons) and introduced a new family of linear MRD-codes for each parameter; using some of the theory of semifields, he proved that these are inequivalent to the Gabidulin codes.

Kai-Uwe Schmidt's talk focussed on subgroups of the set of $n \times n$ symmetric matrices over $\mathbb{F}_q$ for odd q, for which the rank of the difference of any pair of distinct matrices in the subgroup is at least d. (Such sets can be considered as rank metric codes that are subject to the additional constraints that the matrices of the code must be symmetric and the set must form a subgroup.) Schmidt derived an upper bound on the size of such a subgroup in terms of n, q and d, and showed how to construct subgroups for which the upper bound is attained. A key insight is a new understanding of the association scheme of symmetric bilinear forms. His results can be equivalently formulated in terms of the weight enumerators of certain cyclic codes.

Planar Functions and their Generalizations

A perfect non-linear (PN) function is a map $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with the property that $x \mapsto F(x+a) - F(x)$ is a permutation for all $a \neq 0$. Such functions are also called planar functions, because they define projective planes. Most known PN functions are associated with semifields [30]. In the binary case $p = 2$, PN functions unfortunately cannot exist; this motivates the study of almost perfect nonlinear (APN) functions, where now $x \mapsto F(x+a) + F(x)$ is required to have 0 or 2 solutions for all $a \neq 0$. APN functions are of great interest in cryptography, as they provide optimal resistance of a block cipher to differential attacks. In his expository lecture, Alexander Pott introduced these notions and gave a comprehensive overview of the known constructions of PN and APN functions. He also discussed both the similarities and the differences between the PN and the APN case, and highlighted several important open problems.

Petr Lisoněk considered the existence of APN functions which are also permutations of $\mathbb{F}_{2^n}$; this additional property is desirable in the design of block ciphers. While many APN permutations are known when n is odd, their existence in even dimensions $n > 6$ is an open problem. An example for $n = 6$ was given by Browning, Dillon, McQuistan and Wolfe in 2009 [4]. Lisoněk related some parts of their construction to consideration of the number of rational points on a certain family of hyperelliptic curves of genus 2 over $\mathbb{F}_{2^6}$, and discussed the possibility of obtaining similar constructions in higher even dimensions.

Yin Tan studied the related notion of zero-difference δ-balanced functions, where one requires that the equation $F(x+a) - F(x) = 0$ has exactly δ solutions for all $a \neq 0$. All known quadratic planar functions are zero-difference 1-balanced, and some quadratic APN functions are zero-difference 2-balanced. After considering the relationship between this notion and differential uniformity, Tan gave new families of zero-difference p^t-balanced functions and used these to construct new partial difference sets and hence new strongly regular graphs.

Yue Zhou considered monomial negabent functions. Like the related but better-known bent functions (which arise as component functions of PN functions), negabent functions play an important role in both cryptography and coding theory. Here the defining property is that the map $x \mapsto F(x+a) + F(x) + \mathrm{Tr}(ax)$ (where Tr denotes the trace function) should be balanced for every $a \neq 0$. Zhou presented families and examples of quadratic and cubic negabent polynomials in the special case $F(x) = \mathrm{Tr}(\gamma x^d)$.

Sequences and Quantum Information Theory

In his expository lecture, Bill Martin described two notoriously challenging problems of quantum information theory that he considered the workshop participants were "born to solve". The first problem is the construction of large sets of equiangular lines in $\mathbb{C}^d$ or in $\mathbb{R}^d$, namely sets of unit vectors for which distinct vectors have inner product of constant magnitude. The second problem is the construction of large sets of mutually unbiased bases in $\mathbb{C}^d$ or in $\mathbb{R}^d$, namely orthonormal bases for which unit vectors from distinct bases have inner product of constant magnitude. Much of what is currently known about these two problems is related to bent functions, PN functions and codes that are linear over the ring $\mathbb{Z}_4$ [5], [14]. Martin carefully and entertainingly explained how these problems arise in quantum information theory, and why he believes they should be regarded as fundamentally combinatorial problems.

Golay complementary sequences and arrays have the property that the sum of their aperiodic autocorrelations is zero at all non-zero shifts [16]. They have been applied to a wide range of digital communications technologies, including infrared spectrometry [15], optical time domain reflectometry [28], and especially multicarrier wireless communications [9]. Matthew Parker introduced the novel idea of constructing Golay sequences and arrays using mutually unbiased bases. This allows the construction of larger sets of Golay sequences/arrays than those described by Davis and Jedwab [9], and therefore a higher code rate when used for transmission; this advantage occurs at the cost of an increase in the size of the sequence/array alphabet. The new constructions lead to interesting enumeration problems.

Codes and Groups

It has long been recognized that codes with strong error-correction capabilities are often related to finite simple groups, extremal graphs, and extremal finite geometries. These connections are still being fruitfully exploited.

Dimitri Leemans described a new method of studying primitive coset geometries, using the permutation representations of groups. This method enables the construction of new binary codes, from the row span over $\mathbb{F}_2$ of the incidence matrices of some strongly regular graphs associated with large groups. Leemans presented an algorithm for handling the calculations for these groups, that is at least 1000 times faster than the best previously known. It permits the classification of rank two primitive coset geometries for the five Mathieu groups, the first three Janko groups, the Higman-Sims group, and the McLaughlin group.

The Hoffman-Singleton graph and the Higman-Sims graph are associated with the finite simple group $PSU_3(5)$ and the Higman-Sims group, respectively. Bernardo Rodrigues examined the codes of these graphs, producing examples of codes having optimal or best-known minimum distance for their length and dimension, and examples meeting the classical Gilbert-Varshamov bound [13], [36]. He also constructed new 2-designs that are invariant under the Higman-Sims group.

Dean Crnković described a method for constructing self-orthogonal and self-dual codes using orbit matrices of symmetric 2-designs with prescribed automorphism group. The method employs Lander's results on linear codes spanned by incidence matrices of symmetric designs [24], and extends previous constructions due to Harada and Tonchev [19].

Emerging Applications in the Mathematics of Communications

Researchers are able to draw on an enormous body of coding theory knowledge, accumulated over many decades, in order to solve entirely new practical problems soon after they present themselves. This was powerfully illustrated by five of the workshop talks, whose topics were channel estimation, efficient spectrum allocation, chip design, tamper-resistant cryptography, and random number generator hardware.

Digital information can be transmitted over a noisy channel by modulating a carrier signal with a sequence of values drawn from a finite alphabet. The channel estimation problem is to find the parameters that determine how the channel transforms the transmitted sequence into the received sequence. In his expository lecture, Alexander Fish described the classical pseudo-random method for solving the channel estimation problem for a delay-Doppler channel. This method has complexity $O(N^2 \log N)$, where N is the length of the transmission sequence. Fish then introduced alternative solutions to this problem, developed with Gurevich and others, whose complexity is only $O(N \log N + r^2)$ for a channel of sparsity r.

Conventional coding theory is used to recover information in the presence of errors introduced by transmission over a noisy channel. Anant Sahai introduced the novel concept of an identity code, for determining the identity of the transmitter without necessarily being able to decode the actual message that was transmitted. This has potential application to the problem of allocating available electromagnetic spectrum more efficiently than under the current regulatory constraints.

On-chip data buses frequently experience problems of crosstalk, in which a signal travelling along one path experiences interference from signals on adjacent parallel paths. These problems are growing in severity as circuits are becoming progressively more miniaturized. Charlie Colbourn showed how balanced sampling plans from statistical experimental design theory can be modified to produce packing sampling plans, leading to coding schemes that eliminate various types of crosstalk while simultaneously achieving low power and error correction.

Designers of cryptographic systems always attempt to protect against attacks based on the theoretical properties of their cryptosystems. In addition, they must also guard against side-channel attacks exploiting information, such as timing or power consumption, that is leaked when the cryptosystem is physically implemented. Jon-Lark Kim discussed complementary information codes that reduce the cost of countermeasures against side-channel attacks. He showed how to construct such codes from strongly regular graphs and doubly regular tournaments.

The generation of truly random numbers by physical means is important for producing cryptographic keys and for resisting cryptographic attacks such as side-channel attacks and fault injection. In his talk, Florian Caullery assumed that a true random number generator is embedded in an electronic device. He then examined how one can test at run time whether the generator is operating correctly, using limited memory and processing. His tests are based on the computation of the nonlinearity and absolute indicator of Boolean functions.

3 Panel Discussion

The final formal event of the workshop was a panel discussion on future research directions in the mathematics of communications, moderated by Jonathan Jedwab. The panellists were Claude Carlet, Charlie Colbourn, Bill Martin, and Anant Sahai. The discussion began with each of the four panellists explaining their view of the important trends, emerging areas, major open problems, and new connections. This was followed by a lively and wide-ranging discussion among the workshop participants, which extended well beyond the allotted 90 minutes.

Many specific future research directions were identified during the discussion, including:

- decoding random linear codes
- using coding theory to manage distributed data storage
- developing new types of stream cipher
- applying the considerable body of existing knowledge about APN functions to the design of better cryptographic S-boxes
- attacking longstanding open conjectures in coding theory, such as the MDS conjecture [33] or Delsarte's constant-weight conjecture [10].
- developing codes suited for low power consumption, particularly as the "Internet of Things" (interconnecting computing devices embedded within existing infrastructure) emerges
- using coding theory to enable efficient version control for distributed file storage
- solving problems arising in the construction of practical quantum computers.

Special mention was made of Peter Keevash's spectacular and unexpected 2014 solution [22] of one of the most important open problems in design theory: the existence conjecture for Steiner t-designs. One of the panellists declared that this put design theory "at a crossroads", and challenged participants to try to find applications of this new theory to practical problems, rather than solely seeking to develop the theory further.

There was general agreement among panellists and participants that theory and application are both important, that neither one should be neglected in favour of the other, and that the study of the mathematics of communications is renewed each time a new connection is made in either direction. There was considerable discussion of specific strategies by which theoreticians can identify and explore possible applications, for example:

- teaching a course geared to students in application-oriented disciplines such as biology, engineering, or anthropology
- participating in an industrial problem-solving event such as the Graduate Industrial Mathematical Modelling Camp (Canada) or Mathematical Problems in Industry (USA)
- organizing cross-disciplinary seminars for graduate students
- maintaining contact with former graduate students who are now employed in industry
- browsing various IEEE journals in search of familiar combinatorial structures, and then trying to understand the underlying reason for their appearance.

One of the workshop participants remarked after the panel discussion that he had never seen such frank self-examination take place in public at a conference, and that he found it extremely interesting and helpful.

4 Interactions

The workshop schedule was designed with copious time for unstructured private discussions, and the participants eagerly took advantage of the opportunities. The following (decidedly not exhaustive) examples of participant interaction are intended to give a sense of the activity and excitement that occurred outside the formal sessions of the workshop, and to indicate that many discussions took place between researchers who had not previously collaborated.

Bill Martin hosted an open session, attended by over a dozen researchers, attempting to catalogue as many documented examples as possible of specific error-correcting codes used in practical applications.

The seven participants based at Canadian institutions had a group discussion about long-term plans for collaborating more closely with each other.

Several participants spoke to Emina Soljanin about her experience of working in an industrial research lab.

Brett Stevens and Daniel Katz began a collaboration, investigating a construction of covering arrays using multiplicative characters over finite fields.

Jim Davis and Anant Sahai had several conversations about legal and engineering questions arising from their respective presentations, as well as academic and public policy issues.

Bill Kantor had discussions with Claude Carlet about constructing new Kerdock codes, with Jim Davis about mutually unbiased bases and bent function and difference sets, and with Brett Stevens about PN and APN functions.

5 Participant Feedback

This report concludes with some samples of participant feedback.

“This was one of the best workshops I have attended in years. The talks were all very interesting and the idea of including Jim Davis’ talk was just perfect. Jim had a unique experience and sharing it with us was so enlightening. I had no idea how the judicial system works in a scientific dispute, before his talk. Having someone from the industry was an excellent idea. Not jamming too many talks each day was very helpful in staying alert. Bill Martin’s session and talk were both very interesting.
The fact that we met and planned for a joint venture, if fruitful, would be a great highlight of the workshop.
Thank you very much for a great workshop.”

“Thank you for organizing such an amazing meeting. I really had a good time. And this may really cement [named graduate student] into this research area. He’s totally pumped to do research now.”

“Thanks for the excellent meeting.”

“Thank you, thank you, thank you for not scheduling too many talks!”

“Once again thank you for the opportunity I was given to attend a well run workshop. I think that the workshop was extremely useful to me in particular, since I had three collaborators attending the meeting and this was a good opportunity for us to have a look at outstanding projects and discuss ideas of how best to address them. Two papers which were in advanced stage of preparation are about to be submitted thanks to the fact that we met. We spoke and got new ideas about finishing some outstanding papers. In addition we were able to start new projects and discussed ideas regarding directions for joint work. I was approached by two colleagues on the possibility of joint work in the near future, and possible collaborative visit to our universities. The panel discussion was an essential component of the discussion to me and it enlightened me on the various problems that one can address. The idea of a common and yet beautiful remote research place is a plus for the meeting.”

“Thank you for a great workshop!”

“It was indeed an enjoyable, informative, and productive week!”

“I thought the quality of all the talks, both expository and contributed, was higher than the average conference in regards to both delivery and content. Quite a few of even the contributed talks included “big problems” that should be or were in the process of being tackled. There was a variety of topics discussed, yet the conference was very cohesive overall. The schedule made it possible to attend all the talks without feeling burnt out and while still having time for small collaboration sessions. I did not leave at the end being glad it was over, but rather looking forward to the next one!”

“I would add my voice to say that this workshop was one of the more useful gatherings I have had in the past decade. The talks were interesting, and those talks sparked conversations. There was plenty of free time that enabled participants to do the work we love to do. Well done!”

References

[1] E.F. Assmus and J.D. Key, *Designs and their Codes*, Cambridge University Press, Cambridge, 1992.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, revised 1984 edition, Aegean Park Press, 1984.

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd edition, Volumes 1 and 2, Cambridge University Press, Cambridge, 1999.

[4] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe, An APN permutation in dimension six. In *Finite Fields — Theory and Applications (G. McGuire, G.L. Mulen, D. Panario, I.E. Shparlinki, eds.)*, *Contemp. Math.* **518**, 33–42, Amer. Math. Soc., Providence, RI, 2010.

[5] A.R. Calderbank, P.J. Cameron, W.M. Kantor, and J.J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, *Proc. London Math. Soc. (3)* **75** (1997), 436–480.

[6] S.D. Cohen, Uniform distribution of polynomials over finite fields, *J. London Math. Soc.* **6** (1972), 93–102.

[7] C. Colbourn and J.H. Dinitz (eds.), *Handbook of Combinatorial Designs*, 2nd edition, Chapman & Hall/CRC, Boca Raton, 2007.

[8] D.J. Costello, Jr., J. Hagenauer, H. Imai, and S.B. Wicker, Applications of error-control coding, *IEEE T. Inform. Theory* **44** (1998), 2531–2560.

[9] J.A. Davis and J. Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, *IEEE T. Inform. Theory* **45** (1999), 2397–2417.

[10] P. Delsarte, An algebraic approach to association schemes of coding theory, *Philips J. Res.* **10** (1973), 1–97.

[11] H. Dobbertin, T. Helleseth, P.V. Kumar, and H. Martinsen, Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type, *IEEE T. Inform. Theory* **47** (2001), 1473–1481.

[12] E.M. Gabidulin, Theory of codes with maximum rank distance, *Problems Inf. Transmiss.* **21** (1985), 1–12.

[13] E.N. Gilbert, A comparison of signalling alphabets, *Bell System Technical Journal* **31** (1952), 504–522.

[14] C. Godsil and A. Roy, Equiangular lines, mutually unbiased bases, and spin models, *European J. Combin.* **30** (2009), 246–262.

[15] M.J.E. Golay, Static multislit spectrometry and its application to the panoramic display of infrared spectra, *J. Opt. Soc. Amer.* **41** (1951), 468–472.

[16] M.J.E. Golay, Complementary series, *IEEE T. Inform. Theory* **IT-7** (1961), 82–87.

[17] S.W. Golomb, *Shift Register Sequences*, revised edition, Aegean Park Press, Laguna Hills, CA, 1982.

[18] S.W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar*, Cambridge University Press, Cambridge, 2005.

[19] M. Harada and V.D. Tonchev, Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms, *Discrete Math.* **264** (2003), 81–90.

[20] T. Helleseth and P.V. Kumar, Sequences with low correlelation. In *Handbook of Coding Theory Volume II (V.S. Pless and W.C. Huffman, eds.)*, 1765–1853, Elsevier, Amsterdam, 1998.

[21] D.J. Katz and P. Langevin, Proof of a conjectured three-valued family of Weil sums of binomials, arXiv:1409.2459 [math.NT].

[22] P. Keevash, The existence of designs, arXiv:1401.3665 [math.CO].

[23] J.-Y. Kim and H.-W. Kang, Apparatus and method for encoding/decoding transport format combination indicator in CDMA mobile communication system, U.S. Patent 7,706,348, April 27, 2010.

[24] E.S. Lander, *Symmetric Designs: an Algebraic Approach*, LMS Lecture Notes **74**, Cambridge University Press, Cambridge, 1983.

[25] K.H. Leung and B. Schmidt, The field descent method, *Des. Codes Cryptogr.* **36** (2005), 171–188.

[26] P. Lusian, E. Gabidulin, and M. Bossert, Maximum rank distance codes as space-time codes, *IEEE T. Inform. Theory* **49** (2003), 2757–2760.

[27] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1986.

[28] M. Nazarathy, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka, W.R. Trutna, Jr., and S. Foster, Real-time long range complementary correlation optical time domain reflectometer, *IEEE J. Lightwave Technology* **7** (1989), 24–38.

[29] M. Phillips, Obama's Apple rescue, *The New Yorker*, August 6, 2013. Available online: http://www.newyorker.com/tech/elements/obamas-apple-rescue.

[30] A. Pott, K.-U. Schmidt, and Y. Zhou, Semifields, relative difference sets, and bent functions. In *Algebraic Curves and Finite Fields (H. Niederreiter, A. Ostafe, D. Panario, and A. Winterhof, eds.)*, *Radon Ser. Comput. Appl. Math.* **16** (2014), 161–178, de Gruyter.

[31] S. Riis and R. Ahlswede, Problems in network coding and error correcting codes appended by a draft version of S. Riis "Utilising public information in network coding". In *Information Transfer and Combinatorics (R. Ahlswede et al., eds.)*, *Lecture Notes. Comput. Science* **4123** (2006), 861–897, Springer-Verlag, Berlin.

[32] R.L. Rivest and A. Shamir, How to reuse a "write-once" memory, *Inform. Control* **55** (1982), 1–19.

[33] B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* **39** (1955), 357–379.

[34] D. Silva, F.R. Kschischang, and R. Kötter, A rank-metric approach to error control in random network coding, *IEEE T. Inform. Theory* **54** (2008), 3951–3967.

[35] R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.

[36] R.R. Varshamov, Estimate of the number of signals in error correcting codes, *Dokl. Acad. Nauk SSSR* **117** (1957), 739–741.