

## LETTERS TO THE EDITOR

### To the editor:

Dear Sirs,

As I understood from your Newsletter [7, page 6] "The 1995 Information Theory Society Paper Award has been awarded to A.Roger Hammons, Jr., P.Vijay Kumar, A.R. Calderbank, N.J.A. Sloane, and Patrick Sole for their paper [4]". To my opinion, awarding of such a prestigious award to the authors of this paper without mentioning the results of [1, 2] creates a distorted picture of the priorities in the new branch of the Coding Theory which we will refer to as Z4-linearity. Besides, it pinches my personal scientific reputation.

The main result of [4] which may be treated as a discovery, for it opens up a new direction in the Coding Theory, states that some "good" non-linear binary codes could be derived from linear codes over the ring Z4. The first example of such a code is the Kerdock code; in [4] it is considered to be a fundamental one.

I am greatly satisfied with such a high estimate of this result by the Information Theory Society, and congratulate the nominees who earned the award with all their works. However, I believe that it should be noted that this result was first published much earlier than [4]. I received the first result on Z4-linearity (consisting in the proof of Z4-linearity of the Kerdock code) in 1982, and presented it at the 5th All-Union Conference on the Theory of Rings, Algebras and Modules. The English language translation of the report [1, page 97] is enclosed.

It was shown there that the Kerdock code punctured in two coordinates may be constructed as a family of segments of highest binary coordinates of some linear recursive sequences family over Z4. Moreover, this code has the cyclic form, – the result which is missing from [4].

The full proofs were published in Russian [2, (1989)], the English translation  $\zeta$  in [2, (1991)]. Furthermore, in January 1991 (one year prior to the submission of [3, 4] for publication) an abstract of [2] was published in the Mathematical Reviews (M.R.91 a:94038) where the reviewer stresses that this implementation of the Kerdock code "appears to have simple description in terms of linear recursive sequences on Z4." In addition, all properties of Galois rings related to the trace functions which were used in [4] are fully described in [2].

I'm grateful to Professor V.I.Levenstein who drew attention of the authors of [4] to the results of [2]. I'd like to express my confusion both with the interpretation of "Z4-linearity" discovery, and biased estimation of my results, given in [4]. First of all, the results in [4] are treated as received independently of [1, 2], although the authors themselves admit that they "discovered Z4-linearity" notably on the Kerdock code example only in 1992, when [1, 2] and M.R.91a:94038 had been already published. Moreover, the results of my research have been known to a wide circle of Coding Theory professionals as early as 1987, when I first presented them at Professor's L.A.Bassalygo seminar at the Institute of Information Processing of the Russian Academy of Sciences.

In this connection, I believe that the authors of [4] should have stressed my priority in Z4-linearity. Instead, in [4] it's not even mentioned that Z4-linearity of Kerdock code has already been proven in [2].

As far as I see it, the new branch of the Coding Theory, engulfing linear representations over rings (and modules!) of non-linear codes over fields, evolved as follows. The basic results on Z4-linearity of Kerdock code were received by A.A.Nechaev and first published in [1, 2]. The follow-up results on Z4-linearity of Preparata's (dual to Kerdock's), Goethals' and related codes are due to A.R.Hummons, P.V.Kumar Jr., A.R.Calderbank, N.J.A.Sloane, and P.Sole [3, 4]. Independently at the same time, a generalized Kerdock code over arbitrary field of characteristics 2, and having a linear representation on a Galois ring, was obtained by A.A.Nechaev and A.S.Kuzmin [5, 6].

Sincerely yours, A.Nechaev

## References

- [1] A.A.Nechaev, "Trace-function in Galois Rings and Noise-stable Codes.", 5th All-Union Symposium on the Theory of Rings, Algebras and modules (USSR). Thes. of Rep. (in Russian)
- [2] A.A. Nechaev, "Kerdock Code in a Cyclic Form." *Discr. Mat. (USSR)* 1 (1989), N4, pp.123 - 139 (in Russian). English translation: *Discrete Math. and Appl.*, V.1(1991), N4, 365-384 (VSP)
- [3] Hummons A.R., Kumar P.V. Jr., Calderbrank., A.R., Sloane N.J.A, Sole P., "The  $\mathbb{Z}_4$ -Linearity of Kerdock, Preparata, Goethals and Related Codes", *Bull. Amer. Math. Soc.* 29 (1993), N2, pp.218-222.
- [4] Hummons A.R., Kumar P.V. Jr., Calderbrank A.R., Sloane N.J.A, Sole P., "The  $\mathbb{Z}_4$  - Linearity of Kerdock, Preparata, Goethals and Related Codes", *IEEE Trans. Inf. Theory* V.40, N2, March 1994, pp. 301-319.
- [5] Kuzmin A.S., Nechaev A.A., "Construction of Noise Stable Codes Using Linear Recurring Sequences over Galois Rings", *Uspekhi Math. Nauk*, 48 (1993), V3, pp.197-198 (in Russian). English translation: *Russian Math. Surv.*
- [6] Kuzmin A.S., Nechaev A.A., "Linearly Presented Codes and Kerdock Code over Arbitrary Galois Field of the Characteristic 2", *Uspekhi Math. Nauk*, 49 (1994), pp.165-166.
- [7] *IEEE Information Theory Newsletter*, Vol. 45, N3, Sept.1995.

## Authors' response:

We all have the highest appreciation for the scientific achievements of Professor Nechaev. In the Introduction to our paper we acknowledge that prior to our work Professor Nechaev did employ Galois rings to make a connection between cyclic codes over  $\mathbb{Z}_4$  and the nonlinear binary Kerdock code. Specifically Prof. Nechaev constructed a  $\mathbb{Z}_4$ -linear code that yields upon the "highest coordinate" map a cyclic code equivalent to the Kerdock code whose codewords can be generated using linear feedback shift registers. We had hoped this would be clear from the postscript that concludes the introductory section of our paper, and which is reproduced at the end of this letter.

Our perspective on this subject is slightly different; aside from their excellent error-correcting properties, the Kerdock and Preparata codes are remarkable because they are "formal duals" in the sense that although these codes are nonlinear, the distance distribution of one is the MacWilliams transform of the other. The main unsolved problem concerning these codes had always been whether they were dual in some more algebraic sense. The paper we wrote explains this conundrum by showing that the Kerdock code and (a variant of) the Preparata code can be obtained as the images of a dual pair of linear codes over  $\mathbb{Z}_4$  under a fundamental isometry that connects two metric spaces;  $(\mathbb{Z}_4^N, \text{Lee metric})$  and  $(\mathbb{Z}_2^{2N}, \text{Hamming metric})$ . This fundamental isometry is the Gray map and it is different from the highest coordinate map employed by Nechaev. The Gray map served as our key to the Kerdock/Preparata mystery and led to many other results presented in our paper and elsewhere.

We came to our discoveries by following a different path from Prof. Nechaev. Our path begins with the book by MacDonald [Mc74] which explains the arithmetic structure of Galois rings and the paper of Shankar [Sh79] who uses Galois rings to construct cyclic codes over integer rings. We also made use of papers by Liebler and Mena [LM88] who constructed distance regular graphs using Galois rings, by Solé [S89] and Boztas, Hammons and Kumar [BHK92] who used Galois rings to define and analyze families of quaternary sequences with good correlation properties, and by Yamada [Y90] who also used Galois rings in graph theory.

Only after our paper was completed did we become aware of Prof. Nechaev's work. We added the reference ([N89/91]) and the following postscript that appears at the end of the introductory section to our paper.

**Postscript:** After this paper was completed, V. I. Levenshtein drew our attention to an article by Nechaev [N89/91]. In this article Nechaev considers the quaternary sequences  $\{c_t\}$  given (in the notation of the present paper) by

$$c_t = (-1)^t \{T(\lambda \xi^t) + \delta\},$$

$0 \leq t \leq 2^{m+1} - 3$ ,  $\lambda \in R$ ,  $\delta \in \mathbb{Z}_4$ , and their 2-adic expansions  $c_t = a_t + 2b_t$ , where  $a_t, b_t \in \{0, 1\}$ . The principal result of [N89/91] shows that the set of  $\{b_t\}$  is a nonlinear binary cyclic code which is equivalent to the binary Kerdock code punctured in two coordinates. However, [N89/91] makes no mention of the fundamental isometry of (15), nor of Preparata codes and the sense in which they are duals of Kerdock codes.

## References

- [BHK92] S. Boztaş, A. R. Hammons, Jr., and P. V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1101–1113, 1992.
- [LM88] R. A. Liebler and R. A. Mena, "Certain distance-regular digraphs and related rings of characteristic 4," *J. Combin. Theory, Series A*, vol. 47, pp. 111–123, 1988.
- [Mc74] B. R. MacDonald, *Finite Rings with Identity*. New York: Marcel Dekker, 1974.
- [N89/91] A. A. Nechaev, "The Kerdock code in a cyclic form," *Discrete Mat.*, vol. 1, pp. 123–139, 1989. English translation in *Discrete Math. Appl.*, vol. 1, pp. 365–384, 1991.
- [Sh79] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 480–483, 1979.
- [S89] P. Solé, "A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties," *Lecture Notes in Computer Science*, vol. 388, 1989, pp. 193–201.
- [Y90] M. Yamada, "Distance-regular digraphs of girth 4 over an extension ring of  $\mathbb{Z}/4\mathbb{Z}$ ," *Graphs and Combinatorics*, vol. 6, pp. 381–394, 1990.

A. R. Hammons, Jr.  
Hughes Network Systems  
Germantown, MD 20876 USA

P. V. Kumar  
Communication Science Institute  
EE-Systems

University of Southern California  
Los Angeles, CA 90089 USA

A. R. Calderbank and N. J. A. Sloane  
Mathematical Sciences Research Center  
AT&T Bell Laboratories  
Murray Hill, NJ 07974 USA

P. Solé  
CNRS-13S  
Sophia Antipolis  
06560 Valbonne, France