has no root in any subfield of $\mathbb{F}_{q^{2e}}$ containing $\mathbb{F}_{q^2}$, it suffices to show that it has no root in the largest proper subfield $\mathbb{F}_{q^{2m}}$, $m = e/p$. Suppose β is a root of $f(x)$ in $\mathbb{F}_{q^{2m}}$. Set $\alpha_k := G_0(\beta)$, $\alpha_{k-1} := G_1(\beta)$, and so on. We get $\alpha_0 := G_k(\beta) \neq 0$, thus, obtain a solution to (11) with $\alpha_0 \neq 0$ contained in $\mathbb{F}_{q^{2m}}$. In particular, there is an integer $\ell \le k$ such that $\ell + 1 = pm$ (since $pm \le k+1$). The polynomial $x^q + x + \alpha_\ell$ has a root in $\mathbb{F}_{q^{2m}}$. This contradicts Proposition 6. □

Recall that $K = \mathrm{GF}\,(q^2)$, K_m is $\mathrm{GF}\,(q^{2p^m})$, and $\lg(l)$ is defined as the unique integer such that $2^{\lg(l)} \le l \le 2^{\lg(l)+1} - 1$.

Proposition 8: If $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ is a sequence of elements of Φ that satisfies

$$\begin{aligned} &\alpha_0^q + \alpha_0 = 0, && \alpha_0 \neq 0, \\ &\alpha_i^q + \alpha_i = \alpha_{i-1}, && \text{for } i = 1, 2, 3, \ldots \end{aligned}$$

then $\alpha_0 \in \mathbb{F}_q$, $\alpha_1 \in K \setminus \mathbb{F}_q$, and $\alpha_i \in K_{\lg(i)} \setminus K_{\lg(i)-1}$ for $i > 1$.

Proof: It is obvious that $\alpha_0^q = \alpha_0 \Rightarrow \alpha_0 \in \mathbb{F}_q$. Repeated applications of Proposition 7 show that $\alpha_i \in K_{\lg(i)} \setminus K_{\lg(i)-1}$ for each $i = 1, 2, \ldots$. □

References

[1] V. D. Goppa, "Codes on algebraic curves," *Sov. Math.–Dokl.*, vol. 24, pp. 170–172, 1981.

[2] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound," *Math. Nachrichtentech.*, vol. 109, pp. 21–28, 1982.

[3] G. L. Katsman, M. Tsfasman, and S. G. Vlăduţ, "Modular curves and codes with a polynomial construction," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 353–355, Mar. 1984.

[4] B. López *et al.*, "Codes on Drinfeld modular curves," in *Coding Theory, Cryptography and Related Areas*, J. Buchmann *et al.*, Eds. Heidelberg, Germany: Springer, 1998, pp. 175–183.

[5] A. Garcia and H. Stichtenoth, "A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vlăduţ bound," *Invent. Math*, vol. 121, pp. 211–222, 1995.

[6] ——, "On the asymptotic behavior of some towers of function fields over finite fields," *J. Number Theory*, vol. 61, no. 2, pp. 248–273, Dec. 1996.

[7] I. Aleshnikov, V. Deolalikar, P. V. Kumar, and H. Stichtenoth, "Toward a basis for the space of regular functions in a tower of function fields meeting the Drinfeld–Vlăduţ bound," in *Proc. 5th Int. Conf. Finite Fields and Applications*. Augsburg, Germany, Aug. 1999.

[8] K. Shum, I. Aleshnikov, P. V. Kumar, and H. Stichtenoth, "A low-complexity algorithm for the construction of algebraic geometric codes better than the Gilbert–Varshamov bound," I*EEE Trans. Inform. Theory*, to be published.

[9] K. Shum, "A low-complexity construction of algebraic geometric codes better than the Gilbert–Varshamov bound," Ph.D. dissertation, Univ. So. Calif., Los Angeles, 2000.

[10] C. Voss and T. Høholdt, "An explicit construction of a sequence of codes attaining the Tsfasman–Vlăduţ–Zink bound: The first steps," *IEEE Trans. Inform. Theory*, vol. 43, pp. 128–135, Jan. 1997.

[11] G. Haché, "Construction effective des codes géométriques," Ph.D. dissertation, Univ. Pierre and Marie Curie Paris VI, Paris, France, 1996.

[12] R. Pellikaan, H. Stichtenoth, and F. Torres, "Weiestrass semigroups in an asymptotically good tower of function fields," *Finite Fields their Applic.*, vol. 4, pp. 381–392, 1998.

[13] N. Elkies, "Explicit modular towers," in *Proc. 35th Annu. Allerton Conf. Communication, Control and Computing*, Urbana, IL, 1997.

[14] D. Leonard, "Finding the defining functions for one-point AG codes," paper, preprint.

[15] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Heidelberg, Germany: Universitext. Springer-Verlag, 1993.

[16] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed. Camabridge, U.K.: Cambridge Univ. Press, 1997.

Nonexistence of Completely Transitive Codes with Error-Correcting Capability $e > 3$

Joaquim Borges, Josep Rifà, *Member, IEEE*, and Victor Zinoviev

***Abstract*—The class of completely transitive codes was introduced by Solé as a proper subclass of binary linear completely regular codes. There exist completely transitive codes with error-correcting capabilities $e = 1, 2,$ and 3. In a previous correspondence, Borges and Rifà proved the nonexistence of completely transitive codes with more than two codewords and error-correcting capability $e > 4$. In this correspondence, we prove the nonexistence for the remaining case, namely, $e = 4$. Therefore, the question of the existence of such codes, depending on their error-correcting capability, is completely solved.**

***Index Terms*—Completely regular codes, completely transitive codes, permutation groups.**

I. Introduction

Let F^n be the n-dimensional vector space over $\mathrm{GF}\,(2)$. The *Hamming weight* $\mathrm{wt}\,(v)$ of a vector $v \in F^n$ is the number of its nonzero coordinates. The *Hamming distance* between two vectors $v, u \in F^n$ is $d(v, u) = \mathrm{wt}\,(v + u)$.

A *binary linear code* $\mathcal{C}$ of *length* n is a linear subspace of F^n. The elements of $\mathcal{C}$ are called *codewords*. We will denote by d the *minimum distance* between any two distinct codewords. We call $\mathcal{C}$ an e-*error-correcting* code if $e \le \frac{d-1}{2}$. Given any vector $v \in F^n$, its *distance to the code* $\mathcal{C}$ is $d(v, \mathcal{C}) = \min_{x \in \mathcal{C}}\{d(v, x)\}$ and the *covering radius* of the code $\mathcal{C}$ is $\rho = \max_{v \in F^n}\{d(v, \mathcal{C})\}$. Given two sets $X, Y \subset F^n$, we also define the sum $X + Y$ as the set of all vectors that can be expressed as the sum of a vector in X and a vector in Y. We write $X + x$ instead of $X + \{x\}$.

A binary linear code $\mathcal{C}$ of length n is called *completely regular* if $\forall v \in F^n$ and $\forall p = 0, \ldots, n$, the number of codewords at distance p apart from v depends only on p and $d(v, \mathcal{C})$.

An *automorphism* of $\mathcal{C}$ is a coordinate permutation fixing $\mathcal{C}$. The set of all automorphisms of $\mathcal{C}$ is the *full automorphism group* of $\mathcal{C}$ and is denoted by $\mathrm{Aut}\,(\mathcal{C})$. $\mathrm{Aut}\,(\mathcal{C})$ acts in the following way on the quotient set $F^n/\mathcal{C}$:

$$\forall \alpha \in \mathrm{Aut}(\mathcal{C}) \;\; \alpha(\mathcal{C} + x) = \mathcal{C} + \alpha(x)$$

for all $x \in F^n$.

We call $\mathcal{C}$ a *completely transitive* code if $\mathrm{Aut}\,(\mathcal{C})$ acting on $F^n/\mathcal{C}$ has exactly $\rho + 1$ orbits. Since two cosets in the same orbit have identical weight distribution, we have that a completely transitive code is always completely regular. For a more detailed proof see [14].

Let $\mathcal{C}$ be a binary linear e-error-correcting code. It has been conjectured for a long time that if $\mathcal{C}$ is a completely regular code and $\mid \mathcal{C} \mid > 2$, then $e \le 3$. In fact, this conjecture has been also stated for nonbinary

Manuscript received October 24, 2000; revised November 15, 2000. This work was supported in part under Spanish Grant TICZ000-0739-C04-01, and in part by Russian Fond of Fundamental Research (Project 99-01-00828).

J. Borges and J. Rifà are with the Departament d'Informàtica, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail:quim@ccd.uab.es; jrifa@ccd.uab.es).

V. Zinoviev is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia (zinov@iitp.ru).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)02852-8.

and nonlinear codes. Moreover, in [11] it is conjectured that the only completely regular code $\mathcal{C}$ with $| \mathcal{C} |> 2$ and $d \geq 8$ is the well-known extended binary Golay code.

For $e = 1, 2$, or 3, there exist completely transitive codes (see [2], [5], [14]). As we have mentioned earlier, for $e > 3$ it has been conjectured that there is no completely regular code containing more than two codewords, and hence there is no completely transitive code, with the exception of the trivial or the repetition codes. This has been proven for the case $e = \rho$ (*perfect* codes) independently by Zinoviev and Leontiev [17] and by Tietäväinen [15] in 1973, and also for the case $e + 1 = \rho$ (*quasi-perfect uniformly packed* codes) by Van Tilborg in 1976 (see [6] and also [13]). For $\rho > e + 1$ there is no proof of the conjecture.

In [2], we proved that there are no completely transitive codes with error-correcting capability $e \geq 5$ and more than two codewords. Hence, the case $e = 4$ remained unsolved after [2]. In this correspondence, we solve this last case by showing the nonexistence of completely transitive codes with $e \geq 4$ and more than two codewords.

II. Multiple Transitivity and Homogeneity

Let G be a finite permutation group acting on an n-set X. We say that G has *degree* n. G is called *t-transitive* $(0 < t \leq n)$ if for any pair of ordered t-tuples of distinct elements of X $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ there exists $\alpha \in G$ such that $\alpha(x_i) = y_i (1 \leq i \leq n)$. G is called *t-homogeneous* $(0 < t \leq n)$ if for any pair of unordered t-sets of distinct elements of $X \{x_1, \ldots, x_t\}$ and $\{y_1, \ldots, y_t\}$ there exists $\alpha \in G$ such that $\alpha(\{x_1, \ldots, x_t\}) = \{y_1, \ldots, y_t\}$.

Of course, if G is t-transitive, it is also $(t-1)$-transitive and t-homogeneous. We also remark that if G is t-homogeneous it is $(n - t)$-homogeneous.

The following result on transitivity and homogeneity was stated by Livingstone and Wagner (1965, [10]),

Theorem 1: If G is t-homogeneous, where $2 \leq t \leq n/2$, then G is $(t - 1)$-transitive, and for $t \geq 5$, even t-transitive.

Proof: See [10] or [1, Theorem 2.19, p. 251]. □

We will use the following classification theorem.

Theorem 2: Let G be a finite t-transitive group of degree n.

i) If $t > 5$, then G is the symmetric or the alternating group of degree n.

ii) If $t = 5$ and G is not the symmetric or the alternating group, then G is one of the Mathieu groups M_{12} or M_{24} (of degree 12 or 24, respectively).

iii) If $t = 4$, then G is one of the above, or G is one of the Mathieu groups M_{11} or M_{23} (of degree 11 or 23, respectively).

Proof: The reader may see [3], [4, p. 591], or [7, pp. 623–625]. □

Finally, we will also use a result due to Kantor (1972, [9]).

Theorem 3: Let G be a finite 4-homogeneous group of degree $n \geq 8$ which is not 4-transitive. Then G is similar to $PSL(2, 8)$, $P\Gamma L(2, 8)$ or $P\Gamma L(2, 32)$, in their usual permutation representations.

Proof: See [9]. □

III. The Nonexistence of Completely Transitive Codes

The following result may be found in [14, Proposition 7.3].

Proposition 4: If an e-error-correcting code $\mathcal{C}$ is a completely transitive code, then $\mathrm{Aut}\,(\mathcal{C})$ is e-homogeneous on the coordinate positions.

In order to prove our main theorem, we need some lemmas.

Lemma 5: Let $\mathcal{C} \subset F^n$ be a binary code with minimum distance $d \geq 3$. If $\mathrm{Aut}\,(\mathcal{C})$ is the symmetric group $\mathcal{S}_n$ or the alternating group $\mathcal{A}_n$, then $|\mathcal{C}| \leq 2$.

Proof: Suppose that $\mathcal{C}$ has a codeword $x = (x_1, \ldots, x_n)$ which is neither the all-zero vector nor the all-one vector. Then, let i, j, and k be distinct indexes such that $x_j \neq x_k (i, j, k \in \{1, \ldots, n\})$. The permutation cycle $\pi = (i, j, k)$ is in the alternating and symmetric group, so $d(x, \pi(x)) = 2$ and this contradicts the assumption $d \geq 3$. □

Lemma 6: There is no binary linear completely regular code $\mathcal{C}$ of length $n = 33$ and minimum distance $d \in \{9, 10\}$.

Proof: Suppose that $\mathcal{C}$ is such a code. Then the minimum weight codewords form a $4 - (33, 9, \lambda)$-design, if $d = 9$; or a $5 - (33, 10, \mu)$-design, if $d = 10$ (see [16]).

In the first case, the number of blocks should be

$$\lambda \frac{\binom{33}{4}}{\binom{9}{4}} = \lambda \frac{31 \cdot 11 \cdot 4 \cdot 5}{3 \cdot 7}$$

which clearly implies $\lambda \geq 21$. Given four coordinate positions, there are λ codewords of weight 9 covering these four coordinates. Since the minimum distance between two codewords is 9, it follows that the supports of two minimum-weight codewords covering the same 4-set of coordinates do not intersect in any other position. Hence we obtain

$$\lambda \leq \frac{33 - 4}{9 - 4} = \frac{29}{5}$$

which implies $\lambda \leq 5$, a contradiction.

For the second case $(d = 10)$ one can obtain exactly the same contradiction with this argument. □

The following property on binary linear codes is known as the Griesmer bound.

Lemma 7: Let $\mathcal{C}$ be a binary linear code of length n, dimension k, and minimum distance d. Then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$$

Proof: See [8]. □

Now, we prove our main result which is a generalization of [2, Theorem 5].

Theorem 8: If $\mathcal{C} \subset F^n$ is an e-error-correcting completely transitive code, then $e \leq 3$ or $|\mathcal{C}| \leq 2$.

Proof: Assume that $\mathcal{C}$ is an e-error-correcting completely transitive code, with $e \geq 4$. $\mathrm{Aut}\,(\mathcal{C})$ must be e-homogeneous by Proposition 4. If $|\mathcal{C}| > 2$, then $\mathcal{C}$ has dimension $k > 1$, minimum distance $d < n$, and error-correcting capability $e < n/2$. Thus, if $e \geq 5$, $\mathrm{Aut}\,(\mathcal{C})$ must also be e-transitive by Theorem 1, whereas $e = 4$ implies that $\mathrm{Aut}\,(\mathcal{C})$ is 4-transitive or it is similar to $PSL(2, 8)$, $P\Gamma L(2, 8)$, or $P\Gamma L(2, 32)$ by Theorem 3. Now, by Theorems 2 and 3, we have that $\mathrm{Aut}\,(\mathcal{C})$ must be one of the following:

i) $\mathcal{S}_n$, $\mathcal{A}_n$; or

ii) M_n, for $n \in \{11, 12, 23, 24\}$; or

iii) $PSL(2, 8)$, $P\Gamma L(2, 8)$, $P\Gamma L(2, 32)$.

For case i), we would have $|\mathcal{C}| \leq 2$ by Lemma 5.

For case ii), if $n = 11$ or $n = 12$, then $d \geq 2e + 1 \geq 9$ is clearly impossible because the Griesmer bound (Lemma 7) gives $n \geq 14$ for $k \geq 2$. If $n = 23$, then the minimum-weight codewords form an $e - (n, d, \lambda)$-design (recall that $\mathcal{C}$ is also a completely regular code, see [16]) with $e \geq 4$ and $n \geq d + 2$, therefore, the number of blocks should be $b \geq n(n-1)/2$ (this bound is given in [12]). Hence, we have at least $23 \cdot 22/2 = 253$ minimum-weight codewords and $\mathcal{C}$ has dimension $k \geq$

8. Moreover, if $d = 9$, then the subspace spanned by the minimum-weight codewords will have twice this number of codewords (because adding two codewords of weight 9 cannot give another codeword of weight 9); thus, if $d = 9$, we have $k \geq 9$. Now, using the Griesmer bound (Lemma 7) for $k \geq 8$, $d \geq 10$ or $k \geq 9$, $d \geq 9$, we obtain $n \geq 24$. Hence, case $n = 23$ is impossible. Finally, if $n = 24$, we have that the number of minimum-weight codewords is at least $n(n-1)/2 = 276$ and $\mathcal{C}$ has dimension $k \geq 9$. As before, if $d = 9$, then $k \geq 10$. Now the Griesmer bound for $k \geq 9, d \geq 10$ or $k \geq 10, d \geq 9$ gives $n \geq 25$. Therefore, case $n = 24$ is also impossible.

For case iii), recall that the projective special linear group $PSL(2, 8)$ and the projective semilinear group $P\Gamma L(2, 8)$ are 4-homogeneous acting on $n = 9$ points. Since $n > d \geq 9$, $\mathrm{Aut}\,(\mathcal{C})$ cannot be anyone of these groups. Finally, the projective semilinear group $P\Gamma L(2, 32)$ acts 4-homogeneously (not 4-transitively) on 33 points. Thus, if $\mathrm{Aut}\,(\mathcal{C}) = P\Gamma L(2, 32)$, then $\mathcal{C}$ is a 4-error-correcting completely transitive (and completely regular) code of length $n = 33$ and $d \in \{9, 10\}$, but this code does not exist, as we have seen in Lemma 6.

References

[1] T. Beth, D. Junickel, and H. Lenz, *Design Theory*. Manheim, Germany: Wiessenschaftverlag, 1985. English edition: Cambridge, U.K.: Cambridge Univ. Press, 1986.

[2] J. Borges and J. Rifà, "On the nonexistence of completely transitive codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 279–280, Jan. 2000.

[3] P. J. Cameron, "Finite permutation groups and finite simple groups," *Bull. London Math. Soc.*, vol. 13, pp. 1–22, 1981.

[4] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC, 1996.

[5] M. Giudici, "Completely transitive codes in Hamming graphs," Master thesis, Univ. Western Australia, 1998.

[6] J. M. Goethals and H. C. A. Van Tilborg, "Uniformly packed codes," *Philips Res.*, vol. 30, pp. 9–36, 1975.

[7] R. L. Graham, M. Grötschel, and L. Lovász, *Handbook of Combinatorics*. Amsterdam, The Netherlands: Elsevier Science B. V., 1995.

[8] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res. Devel.*, vol. 4, pp. 532–542, 1960.

[9] W. M. Kantor, "k-homogeneous groups," *Math. Z.*, vol. 124, pp. 261–265, 1972.

[10] D. Livingston and A. Wagner, "Transitivity of finite permutation groups on unordered sets," *Math. Z.*, vol. 90, pp. 393–403, 1965.

[11] A. Neumaier, "Completely regular codes," *Discr. Math.*, vol. 106/107, pp. 335–360, 1992.

[12] D. K. Ray-Chaudhuri and R. M. Wilson, "On t-designs," *Osaka J. Math.*, vol. 12, pp. 737–744, 1975.

[13] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev, "Uniformly packed codes," *Probl. Inform. Transm.*, vol. 7, pp. 38–50, 1971.

[14] P. Solé, "Completely regular codes and completely transitive codes," *Discr. Math.*, vol. 81, pp. 193–201, 1990.

[15] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.

[16] H. C. A. Van Tilborg, "Uniformly packed codes," Ph.D. dissertation, Eindhoven Univ. Technol., Eindhoven, The Netherlands, 1976.

[17] V. Zinoviev and V. Leontiev, "The nonexistence of perfect codes over Galois fields," *Probl. Contr. Inform. Theory*, vol. 2, pp. 16–24, 1973.

Intersection Matrices for Partitions by Binary Perfect Codes

Sergey V. Avgustinovich, Antoine C. Lobstein, and Faina I. Solov'eva

***Abstract*—We investigate the following problem: given two partitions of the Hamming space, their *intersection matrix* provides the cardinalities of the pairwise intersections of the subsets of these partitions. If we consider partitions by extended perfect codes, how many intersection matrices can we construct?**

***Index Terms*—Concatenated codes, extended perfect codes, intersection matrices, partitions, strongly orthogonal Latin squares.**

I. Introduction

Let $\mathcal{F}_q^n$ be the vector space of length n over the field $\mathcal{F}_q$, q a prime power. The (Hamming) *distance*, $d(\boldsymbol{x}, \boldsymbol{y})$, between two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ of $\mathcal{F}_q^n$ is the number of positions where they differ; the (Hamming) *weight* of a vector is its distance to the all-zero vector. A q-ary *code* of length n is simply a subset of $\mathcal{F}_q^n$, whose elements are called *codewords*. Assuming that $|C| \geq 2$, the *minimum distance* of C is the smallest distance between two distinct codewords of C.

Here we shall mainly deal with *binary extended perfect codes*. These are codes with the following parameters: alphabet $\mathcal{F}_2 := \mathcal{F} := \{0, 1\}$, length $n = 2^t$ ($t \geq 2$ integer), size 2^{n-1-t}, and minimum distance 4.

It is known that n extended perfect codes $C_1, C_2, \ldots, C_n$ can partition the set $\mathcal{E}^n \subset \mathcal{F}^n$ of even-weight vectors, and n extended perfect codes $C_{n+1}, C_{n+2}, \ldots, C_{2n}$ can partition the set $\mathcal{O}^n := \mathcal{F}^n \backslash \mathcal{E}^n$, the set of odd-weight vectors. Two constructions of nontrivial partitions of $\mathcal{F}^{n-1}$ into nonextended perfect codes can be found in [1]. The problem of the construction of partitions of $\mathcal{F}^n$ is also considered in [2].

If we are given a second partition $D_1, D_2, \ldots, D_n$ of $\mathcal{E}^n$ and $D_{n+1}, D_{n+2}, \ldots, D_{2n}$ of $\mathcal{O}^n$, we are interested in the following problem: we define the *intersection matrix* of these two partitions, $\mathbf{IM}(C, D)$, by

$$\mathbf{IM}(C, D) = [|C_i \cap D_j|]_{i=1,\ldots,2n,\, j=1,\ldots,2n}.$$

Note that each row and each column of $\mathbf{IM}(C, D)$ sums up to 2^{n-1-t}.

Two matrices are called *equivalent* if one can be obtained from the other by permutations of rows and columns. Now, how many *different* and how many *nonequivalent* intersection matrices of two partitions can we construct? In order to obtain bounds on these numbers, we first consider different partitions of $\mathcal{F}^n$, which we use for building two partitions of $\mathcal{F}^{2n}$, of which we study the possible intersection matrices. We then establish that the number of different, or nonequivalent, intersection matrices is at least 2^{cn^2} and at most $2^{c'n^3}$, where n is large and c, c' are positive constants.

In the next sections, we shall use the following notation and need the following definitions.

Manuscript received December 13, 1999; revised September 12, 2000. The work of S. V. Avgustinovich was supported in part under Grants RFBR 00-01-00916 and INTAS 97-1001. The work of F. I. Solov'eva was supported in part under Grant RFBR 00-01-00822.

S. V. Avgustinovich and F. I. Solov'eva are with the Sobolev Institute of Mathematics, Novosibirsk 63 00 90, Russia (e-mail: avgust@math.nsc.ru; sol@math.nsc.ru).

A. C. Lobstein is with Centre National de la Recherche Scientifique, URA 820, 75634 Paris, France (e-mail: lobstein@infres.enst.fr).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)02854-1.