1596 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997

|  |  |
| --- | --- |
| andThis leads to minor improvements in (4)–(6) in the coefficient of the term arising from the case .For and the small set of Kasami sequences of length we have approximately equal maximum even correlation. The Kasami set has considerably fewer sequences, however, the best known upper bound (see [7]) for their maximum aperiodic correlation has as the coefficient of where we have .References1. A.Barg, “On small families of sequences with low periodic correlation," in Lecture Notes in Computer Science, vol. 781. Berlin, Germany: Springer-Veilag, 1994, pp. 154-158.
2. S. Boztas, R. Hammons, and P. V. Kumar, "4-phase sequences with near optimum correlation properties," IEEE Trans. Inform. Theory, vol. 38, pp. 1101-1113, May 1992.
3. T. Helleseth and P. V. Kumar, "Sequences with low correlation,” in Handbook of Coding Theory, R. Brualdi, C. Huffman, and V. Pless, Eds., preprint.
4. T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag, “Improved estimates for the minimum distance of weighted degree trace codes,” in Proc. 1995 IEEE Int. Symp. on Information Theory (Whistler, B.C., Canada, Sept. 17-22, 1995).
5. S. M. Krone and D. V. Sarwate, "Quadriphase sequences for spread- spectrum multiple-access communication,” IEEE Trans. Inform. Theory. vol. 30, pp. 520-529, May 1984.
6. P. V. Kumar, T. Helleseth, and A. R. Calderbank, “An upper bound for Weil exponential sums over Galois rings and applications," IEEE Trans. Inform. Theory, vol. 41, pp. 456—468, Mar. 1995.
7. J. Lahtonen, “On the odd and the aperiodic correlation properties of the Kasami sequences,” IEEE Trans. Inform. Theory, vol. 41, pp. 1506-1508, Sept. 1995.
8. S. Litsyn and A. Tietavainen, "Character sum constructions of constrained error-correcting codes," Appl. Algebra in Eng., C'ommun. and Comp., vol. 5, pp. 45-51, 1994.
9. A.A. Nechaev, "Kerdock code in a cyclic form," Discr. Math. Appl.. vol. 1, pp. 365-384, 1991.
10. D. V. Sarwate, "An upper bound on the aperiodic autocorrelation function for a maximal-length sequence," IEEE Trans. Inform. Theory. vol. IT-30, pp. 685-687, July 1984.
11. A.G. Shanbhag, P. V. Kumar, and T. Helleseth, “An upper bound for the aperiodic correlation of weighted-degree CDMA sequences,” in Proc. 1995 IEEE Int. Symp. on Information Theory (Whistler, B.C., Canada, Sept. 17-22, 1995).
12. , "Improved binary codes and sequence families from -linear codes," IEEE Trans. Inform. Theory, vol. 42, pp. 1582-1587. Sept. 1996.
13. H. Tarnanen, "An elementary proof to the weight distribution formula of the first order shortened Reed-Muller coset code,” preprint.
14. P. Udaya and M. U. Siddiqi, "Optimal biphase sequences with large linear complexity derived from sequences over ," IEEE Trans. Inform. Theory, vol. 42, pp. 206-217, Jan. 1996.
15. I.M. Vinogradov, Elements of Number Theory. New York: Dover, 1954.
 | **New** **Construction** **for** **Families** **of** **Binary** **Sequences** **with** **Optimal** **Correlation** **Properties**Jong-Seon No, Kyeongcheol Yang, *Member,* *IEEE*, Habong Chung, *Member, IEEE*, and Hong-Yeop Song, *Member,* *IEEE****Abstract—*In** **this** **correspondence,** **we** **present** **a** **construction,** **in** **a** **closed** **form,** **for** **an** **optimal** **family** **of** **binary** **sequences** **of** **period** **with** **respect** **to** **Welch’s** **bound,** **whenever** **there** **exists** **a** **balanced** **binary** **sequence** **of** **period** **with** **ideal** **autocorrelation** **property** **using** **the** **trace** **function.** **This** **construction** **enables** **us** **to** **reinterpret** **a** **small** **set** **of** **Kasami** **and** **No** **sequences** **as** **a** **family** **constructed** **from**  **-sequences.** **New** **optimal** **families** **of** **binary** **sequences** **are** **constructed** **from** **the** **Legendre** **sequences** **of** **Mersenne** **prime** **period,** **Hall’s** **sextic** **residue** **sequences,** **and** **miscellaneous** **sequences** **of** **unknown** **type.** **In** **addition,** **we** **enumerate** **the** **number** **of** **distinct** **families** **of** **binary** **sequences,** **which** **are** **constructed** **from** **a** **given** **binary** **sequence** **by** **this** **method.*****Index*** ***Terms—*Kasami** **sequences,** **Legendre** **sequences,** **No** **sequences,** **optimal** **correlation** **property,** **signature** **sequences.**I. INTRODUCTIONCode-division multiple access (CDMA) systems use pseudonoise binary sequences as signature sequences, and several spread-spectrum communication systems also use them as spreading codes for low probability of intercept [18], [20]. Desirable characteristics of a family of binary sequences for such applications include long-period, low out-of-phase autocorrelation values, low crosscorrelation values, low nontrivial partial-period correlation values, large linear span, balance of symbols, large family size, and ease of implementation.A binary (0 or 1) sequence of period is called *balanced* if the number of 1’s is one more than the number of 0’s [8]. It is said to have the *ideal autocorrelation property* if its periodic autocorrelation function is given bywhere is defined asand computed modulo . Note that is the number of agreements minus the number of disagreements between and as runs from 0 to [7], [8], [21]. It is well known that the ideal autocorrelation property implies the balance property.Let and be two binary sequences of period . Two sequences and are said to be *cyclically equivalent*Manuscript received April 26, 1996; revised February 12, 1997. This work was supported in part by the Korean Ministry of Information and Communications. The material in this correspondence was presented in part at the 1996 IEEE International Symposium of Information Theory and Its Applications (ISITA’96), Victoria, BC, Canada, September 17–20, 1996 J.-S. No is with the Department of Electronic Engineering, Konkuk Uni- versity, Seoul 143-701, Korea. K. Yang is with the Department of Electronic Communication Engineering, Hanyang University, Seoul 133-791, Korea. H. Chung is with the Department of Electronic Engineering, Hong-Ik University, Seoul 121-791, Korea. H.-Y. Song is with the Department of Electronic Engineering, Yonsei University, Seoul 120-749, Korea.Publisher Item Identiﬁer S 0018-9448(97)05017-7. |

0018–9448/97$10.00 © 1997 IEEE

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997 1597

|  |  |
| --- | --- |
| if there exists an integer such that for all . Otherwise, they are said to be cyclically distinct. For an integer r, the sequence is called the decimation by of the sequence if for any integer . It is easily checked that the period of is given by divided by . It is also well known that if a sequence of period has the ideal autocorrelation property, so does its decimation by , where is an integer relatively prime to . Two sequences and are said to be equivalent if there are some integers and such that for all . They are said to be inequivalent, otherwise. Consider a set of binary sequences, each with period , denoted byThe periodic crosscorrelation at shift between two sequences and from this collection is defined asThe maximum out-of-phase periodic autocorrelation magnitude for this signal set is defined asand the maximum crosscorrelation magnitude between sequences in this set is given byThe criterion for signal design is to minimizeIn signal design, the Welch bound and the Sidelnikov bound are used to test the optimality of sequence sets. Some of well-known optimal families of binary sequences include Gold sequences [6], Kasami sequences [18], [20], bent sequences [12], [20], and No sequences [15]. Gold sequences form an optimal set with respect to Sidelnikov’s bound [19] which states that for any set of or more binary sequences of period The small set of Kasami sequences is an optimal collection of binary sequences with respect to Welch’s bound [22], which implies thatwhen it is applied to a set of sequences of period for an even integer . Bent and No sequences also form an optimal set with respect to Welch’s bound, respectively, but they have larger linear spans than Gold sequences and Kasami sequences.In this correspondence, we show that if a binary sequence of period in a trace expression has the ideal autocorrelation property, it can be used to construct, in a closed form, a family of binary sequences of period with optimal correlation with respect to Welch’s bound. This construction method enables us to reinterpret the small set of Kasami sequences as well as the No sequences as a family constructed from the -sequences. New optimal families of binary sequences are constructed from the Legendre sequences of Mersenne prime period, Hall’s sextic residue sequences, and miscellaneous sequences of unknown type. In addition, we enumerate the number of distinct families of binary sequences, which are constructed from a given binary sequence by this method.This correspondence is organized as follows. In Section II, we present the main results to construct an optimal family of binary | sequences with respect to Welch’s bound. In Section III, the small set of Kasami sequences and the No sequences are reinterpreted as a family constructed from the -sequences. New optimal families of binary sequences are constructed from the Legendre sequences of Mersenne prime period in Section IV. Hall’s sextic residue sequences and miscellaneous sequences of unknown type are also considered in Section IV.II. CONSTRUCTION OF A FAMILY OF BINARY SEQUENCES WITH OPTIMAL CORRELATIONLet be a prime power and be the finite field with elements. Let for some positive integers and . Then the trace function from to the subfield is a mapping [10], [11] given byNo *et* *al.* [17] presented a closed-form expression of binary sequences of longer period with ideal autocorrelation property in a trace representation, if a given binary sequence with ideal autocorrelation property is described using the trace function. The idea of extension in [17] will be helpful for our further discussion, so it is quoted without proof in the following theorem.*Theorem 1 [17]:* Let and be positive integers such that . Let be a primitive element of and set where . Assume that for an index set , the sequence of period given byhas the ideal autocorrelation property. For any integer , relatively prime to , the sequenceof period defined byalso has the ideal autocorrelation property.Based on the idea of extension in Theorem 1, we will provide a method to construct an optimal family of binary sequences of period from a given binary sequence of period with ideal autocorrelation property. Throughout the correspondence, we use the following notations. Let and be positive integers such that . Let be a primitive element of and set . Note that is primitive in . From now on, we assume that the sequence of period given byhas the ideal autocorrelation property for an index set .*Theorem* *2:* Let , and let be the sequence given bywhere , is an integer relatively prime to , and the index set is in (1). Define the family of binary sequences of period as |

1598 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997

|  |  |
| --- | --- |
| Then the family is an optimal set of binary sequences of period with respect to Welch’s bound. Furthemore, takes only a value , or for any and except for the case where and (mod N).*Proof:* We will show that the possible values of are , or for any , and except for the case where and (mod N). Let . Since any integer , can be uniquely written asThen each sequence becomessince and . For short notation, we defineThen we haveSimilarly, we havewhere , is also uniquely written asThus we get the equation at the bottom of this page. Note that the inner sumyields whenWhenwe claim that the inner sum is . If either or , the exponent to in the inner sum is essentially a shift of the sequences . Since , it is obvious that the sequence is balanced and has the ideal autocorrelation property. This implies that the inner sum gives . On the other hand, if and , the inner sum is the autocorrelation of the sequence at a nonzero shift (mod N), so it is by the assumption. Thus the inner sum always yields if | Therefore, it is sufficient to find the size of the set of ’s such that the inner sum gives the value in order to compute . LetThen we haveBy defining and , we haveNote that and , so we getSimilarly, we have . ThusThe degree of the polynomial in is at most 2, which means . Hence we conclude thatfrom (2).*Theorem 3:* Let , and let be a primitive element of . Set and . Let be the sequence given byfor and the index set in (1), where , is an integer relatively prime to , and , is an integer relatively prime to . Define the family of binary sequences of period asThen the family is an optimal set of binary sequences of period with respect to Welch’s bound, and takes only a value , , or for any , and except for the case where and (mod K).*Proof:* By Theorem 1, the sequence in (1) can be extended to a sequence of period with ideal autocorrelation property given byLet . Since , any integer , , can be uniquely written as |

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997 1599

|  |  |
| --- | --- |
| Then each sequence becomessince and . For short notation, we defineThen we haveNote thatSince is the decimation by of , it also has the ideal autocorrelation property. Hence, similar arguments as in the proof of the Theorem 2 complete the proof.*Remark 4:* The family of sequences in Theorem 3 can be obtained by applying Theorem 1 to in (1) and then Theorem 2. As a first step, can be extended to a sequence of period with ideal autocorrelation property, defined bywhere , is an integer relatively prime to M. Writing each trace term in asfor some index set , the sequence can be expressed asApplying Theorem 2 to we have a familygiven byfor an integer , relatively prime to On the other hand, in Theorem 3 can be expressed asusing the relation in (3). Hence, is exactly the same as .A general form for in Theorem 3 can be given as follows:Here, , and , is a relatively prime to for each  | In signal design for CDMA, it is desirable to have a lot of distinct families of binary sequences with optimal correlation for a given period. Hence it is an interesting problem to ﬁnd the number of distinct families of binary sequences constructed from a given binary sequence by Theorem 2.Two families and of sequences of the same period are said to be equivalent if each sequence in is a cyclic shift of some sequence in , and vice versa. Otherwise, they are said to be distinct. Furthermore, they are said to be fully distinct if each sequence in is cyclically distinct from every sequence in .For an integer , define the cyclotomic eoset of an integer , byFor the sake of convenience, the cyclotomic eoset representative of is often defined as the least integer in It is easily checked that either or . I fence the set is partitioned into pairwise disjoint cyclotomic eosets, that is, where A is the set of all the cyclotomic coset representatives. Note that for any integer .For an integer and an index set , define asand define the set of cyclotomic cosets associated with I asLet be the number of r’s relatively prime to M such that , i.e.*Theorem 5:* Let be the number of fully distinct families of binary sequences of period given in Theorem 2. Then we havewhere is the Euler’s phi function and is given in (4).*Proof:* In order to evaluate , we need to count the number of choices for and . The number of choices for is , since and give the same family for any in the cyclotomic coset mod containing . If , then the family associated with is exactly the same as the family associated with . Thus the number of choices for is , given by (4). Therefore, .III. KASAMI SEQUENCES AND NO SEQUENCESLet m and n be positive integers such that . Let be a primitive element of and set where . Then is a primitive element of . Let be a binary m-sequence of period , given byNote that the m-sequence is a binary sequence with ideal autocorrelation property. Applying Theorem 2 to , we get an optimal family defined by |

1600 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997

|  |  |
| --- | --- |
| where is the sequence of period N given byfor . Observe that the family in (5) is exactly the family of No sequences [15], In particular, the family becomes the small set of Kasami sequences when [14], [20], Hence the small set of Kasami sequences and the No sequences can be reinterpreted as a family constructed from the m-sequences. Similarly, generalized No sequences in [13] and [14] are shown to be families constructed from an m-sequence by applying Theorem I successively and then Theorem 2.Consider the number of fully distinct families of binary sequences of period constructed from an m-sequence by Theorem 2. Since I = {1}, it is easy to check that . Hence we havewhich is a known result [15],IV. New Optimal Families of Binary SequencesA. New Optimal Families from Legendre SequencesLet p be an odd prime. The Legendre sequence of period p is defined.It is not difficult to show that has the ideal autocorrelation property if and only if p=3(mod 4) [3], [8], Recently, a trace representation of the Legendre sequences of period (called Mersenne prime) was derived as follows [16]:Proposition 6 [16]: Let be a prime for some integer and let u be a primitive element of , the set of integers mod M. Then there exists a primitive element a of such thatand the sequence of period M given byis exactly the Legendre sequence given in (6).Consider a decimation by of the sequence given in (7). Clearly, if is an even integer, then is the Legendre sequence given in (6). It is also easy to show that if is an odd integer, then , then is the sequence given bySince has the ideal autocorrelation property regardless of , we will also refer to it as a Legendre sequence hereafter. The following theorem is the consequence of Theorem 2 and Proposition 6. | Theorem 7: Let m be an integer such that is a prime, and let . Let u be a primitive element of , the set of integers mod M. Let a be a primitive element of and set where . For an integer , let be the sequence of period given byThen the family defined by is an optimal set of binary sequences of period with respect to Welch’s bound.Consider the number of fully distinct families of binary sequences of period constructed from the Legendre sequence of period by Theorem 7. Since we havefor a primitive element u in , it is easy to check that . Hence we getRemark 8: By Theorem 3 and Remark 4, the Legendre sequences of Mersenne prime period can be used to construct optimal families of period , where is any even multiple of m. □ Example 9: Let m = 7 and thus M = 127(= 27—1). It is easy to check that u = 3 is a primitive element of Z127. Let be a primitive element of . The sequence given byis the Legendre sequence of period 127Let . Let be a primitive element of such that. For , we definewhere , is an integer. Then the family defined byis an optimal set of I 28 binary sequences of period 16383 with respect to Welch’s bound. Note that there are 1512 fully distinct families of binary sequences of period 16383, constructed from the Legendre sequences of period 127.*B.* *New* *Families* *from* *Hall’s* *Sextic* *Residue* *Sequences*Binary sequences of period with ideal autocorrelation property associated with Hall’s difference set appears only when is 5, 7, and 17 [1], [9], They are known as the Hall’s sextic residue sequences. In the case that , the Hall’s sextic residue sequences are exactly the m-sequences of period 31.Let be one of 5, 7, or 17, and set . Let be a primitive element in , and let be a primitive element. From a computer search for a trace representation of the I lull’s sextic residue sequence of period M, it is found that it can be expressed as |

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997 1601

|  |  |
| --- | --- |
| Note that its decimation by any integer also has the ideal autocorrelation property. Hence, and all of its decimations are called the Hall’s sextie residue sequences. Applying Theorem 2 to , we have an optimal family with respect to Welch’s bound in the following.Theorem 10: Let , where is one of 5, 7, or 17, and let be a primitive element in with Let be a primitive element of and set where . For an) integer let be the sequence of period given byThen the family defined byis an optimal set of binary sequences of period with respect to Welch’s bound.Consider the number of fully distinct families of binary sequences of period N constructed from the Hall's sextie residue sequences of period M by Theorem 10. Sincein , it is easy to check that . Hence we haveRemark II: Using Theorem 3 or Remark 4, the Hall’s sextic residue sequences of period can be applied to construct optimal families of period , where - is any even multiple of m.**V.** New Optimal Families fromMiscellaneous Sequences of Unknown TypeTo classify and construct balanced binary sequences of period is a very interesting problem in both theory and practice [7], [8], Especially, the balanced binary sequences of period with ideal autocorrelation property find many applications in spread-spectrum communication systems. A complete search for those sequences was conducted for period 127 by Baumert and Fredrickson [2], 255 by Cheng [4], and 511 by Drier [5],It is well known that there are six inequivalent binary sequences of period 127 with ideal autocorrelation property: an m-sequence, a Legendre sequence, a Hall’s sextic residue sequence, and three others called the miscellaneous sequences of unknown type I, II, and III. Let be a primitive element of . Then the three miscellaneous sequences are known to have the following trace representation by a computer search:1. Unknown Type I
2. Unknown Type II
3. Unknown Type III

where runs from 0 to 126. | By Theorem 2, new optimal families can be constructed from the above sequences of unknown type. For example, consider a family from the sequence Let . Let be a primitive element of and set where . For any integer , let be the sequence of period given bywhere and . Then the family defined byis an optimal set of 128 binary sequences of period with respect to Welch’s bound. It is easily checked that = 18. Hence we have optimal families from a binary sequence of each miscellaneous type.At period 255, it is found that there are four inequivalent binary sequences with ideal autocorrelation property: an m-sequence, a GMW sequence, and two others of unknown type. New optimal families can be constructed from a binary sequence of each unknown type. Note that in this case.At period 511, there are five inequivalent binary sequences with ideal autocorrelation property: an m-sequence, a GMW sequence, and three others of unknown type. New optimal families can be constructed from a binary sequence of each unknown type. Note that in this ease.In the ease of period 1023, a computer search found that there is at least one binary sequence with ideal autocorrelation property, which is inequivalent to any of known binary sequences such as the m-sequences, the GMW sequences, and the extensions of the Legendre sequences. It is given bywhere n is a primitive element of . Hence, a new optimal family of 1024 binary sequences of period can be constructed from the sequence described above.As in the cases of Legendre sequences and Hall’s sextic residue sequences, miscellaneous sequences of unknown type of period can be used to construct optimal families of period , where is any even multiple of m, by applying Theorem 3 or Remark 4.References1. L. D. Baumert, Cyclic Difference Sets (Lecture Notes in Mathematics). Berlin. Germany: Springer-Verlag, 1971.
2. L. D. Baumert and II. Fredrickson, "The cyclotomic numbers of order 18 with applications to difference sets." Math. Comput., vol. 21. pp. 204-219. 1967.
3. D. M. Burton, Elementary Number Theory. Newton, MA: Allyn. 1980.
4. U. Cheng, "Exhaustive construction of (255,127,63) cyclic difference sets.” J. Comb in. Theory, vol. A-35, pp. 115-125, 1983.
5. R. Drier, "(511.255,127) cyclic difference sets." IDA Talk. July 1992.
6. R. Gold, "Optimal binary sequences for spread spectrum multiplexing,” IEEE Trans. Inform. Theory, vol. IT-13, pp. 619-621, Oct. 1967.
7. S. W. Golomb, "On the classification of balanced binary sequences of period ," IEEE Trans. Inform. Theory, vol. IT-26, pp. 730-732, Nov. 1980.
8. Shift-Register Sequences. San Francisco, CA: Holden-Day, 1967: Laguna Hills. CA: Aegean Park. 1982.
9. D. Jungnickel, "Difference sets." in Contemporary Design Theory. .1. II. Dinitz and D. R. Stinson, Eds. New York: Wiley, 1992, pp. 241-324.

[10] R. I.idl and II. Niederreiter, Finite Fields, vol. 20 of Encyclopedia of Mathematics and Its Applications. Reading, MA: Addison-Wesley, 1983. |

1602 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 43, NO. 5, SEPTEMBER 1997

|  |  |
| --- | --- |
| [11] F. J. Mac Williams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland, 1977.1. J. D. Olsen, R. A. Scholtz, and L. R. Welch, “Bent-function sequences," IEEE Trans. Inform. Theory, vol. IT-28, pp. 858-864, Nov. 1982.
2. J.-S. No, “A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span,” Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, May 1988.
3. , “Generalization of GMW sequences and No sequences,” IEEE

Trans. Inform. Theory, vol. 42, pp. 260-262, Jan. 1996.1. J.-S. No and P. V. Kumar, “A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span,” IEEE Trans. Inform. Theory, vol. 35, pp. 371-379, Mar. 1989.
2. J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, “Trace representation of Legendre sequences of Mersenne prime period,” IEEE Trans. Inform. Theory, vol. 42, pp. 2254—2255, Nov. 1996.

[ 171 J.-S. No, K. Yang, H. Chung, and H.-Y. Song, “Extension of binary sequences with ideal autocorrelation property,” in Proc 1996 IEEE Int. Symp. on Information Theory and Its Applications (ISITA '96) (Victoria, BC, Canada, Sept. 17-20, 1996), pp. 837-840.1181 D. V. Sarwate and M. B. Pursley, “Crosscorrelation properties of pseudorandom and related sequences,” Proc. IEEE, vol. 68, pp. 593-619, May 1980.1191 V. M. Sidelnikov, “On mutual correlation of sequences,” Sov. Math- Dokl, vol. 12, pp. 197-201, 1971.|20] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications, vol. 1. Rockville, MD: Computer Sci. Press, 1985.1. H. Y. Song and S. W. Golomb, “On the existence of cyclic Hadamard difference sets," IEEE Trans. Inform. Theory, vol. 40, pp. 1266-1268, July 1994.
2. L. R. Welch, “Lower bounds on the maximum cross-correlation of signals,” IEEE Trans. Inform. Theory, vol. IT-20, pp. 397-399, May 1974.

Is Code Equivalence Easy to Decide?Erez Petrank and Ron M. Roth, Member, IEEE**Abstract—** **We** study the computational difficulty of deciding whether two matrices generate equivalent linear codes, i.e., codes that consist of the same codewords up to a fixed permutation on the codeword coordinates. We call this problem Code Equivalence. Using techniques from the area of interactive proofs, we show on the one hand, that under the assumption that the polynomial-time hierarchy does not collapse, Code Equivalence is not NP-complete. On the other hand, we present a polynomial-time reduction from the Graph Isomorphism problem to Code Equivalence. Thus if one could find an efficient (i.e., polynomial-time) algorithm for Code Equivalence, then one could settle the long-standing problem of determining whether there is an efficient algorithm for solving Graph Isomorphism.**Index Terms —** Code Equivalence, Graph Isomorphism, interactive proofs, polynomial hierarchy.I. IntroductionLet F be a finite field and let and be generator matrices of two linear codes and over F. We say that and are code-equivalent, denoted , if the sets and are theManuscript received November 30, 1995; revised February 12, 1997.E. Petrank is with the DIMACS Center, P.O. Box 1179, Piscataway, NJ 08855 USA.R. M. Roth is with Hewlett-Packard Laboratories, Palo Alto, CA 94304 USA, on leave from the Computer Science Department, Technion-Israel Institute of Technology, Haifa 32000, Israel.Publisher Item Identifier S 0018-9448(97)05216-4. | same, up to a fixed permutation on the coordinates of the codewords of . In other words, if and only if both matrices have the same order , and there exist an permutation matrix P and a nonsingular matrix S over F such that . The problem of deciding whether two generator matrices are code-equivalent will be referred to as the Code Equivalence problem.The purpose of this correspondence is to study the computational difficulty of the Code Equivalence problem. As one application of a related problem, we mention the public-key cryptosystems due to McEliece [9] and Niederreiter [11]. Recall that an alternant code over GF (q) is defined by a parity-check matrix of the form , where the ’s are distinct elements in and the ’s are nonzero elements in [8, ch. 12]. Goppa codes are special cases of alternant codes where certain restrictions are imposed on the values ’s, and generalized Reed-Solomon codes are special cases of alternant codes where m = 1. The mentioned cryptosystems are based on the assumption that it is difficult to identify the values and out of an arbitrary generator matrix (or parity-check matrix) of an alternant code. Namely, it is difficult to obtain a code- equivalent matrix of the form . On the other hand, as shown in [12], it is easy to extract the values ay and y3 from any systematic generator matrix of a generalized Reed-Solomon code; hence, cryptosystems based on such a code are breakable. This was pointed out explicitly by Sidelnikov and Shestakov in [13]. For related work, see also the references cited in [10, p. 317].The significance of the Code Equivalence problem can also be exhibited through the results of Kasami, Lin, and Peterson [6], and Kolesnik and Mironchikov [7], who showed that Reed- Muller codes are equivalent to subcodes of extended Bose- Chaudhuri-Hocquenghem (BCH) codes. Thus it should be interesting to design an efficient algorithm that decides whether two codes are indeed equivalent, and thus infer from the properties that arise from one code representation to the other.On the positive side, we first show that the Code Equivalence problem is unlikely to be NP-complete. The proof of this assertion relies on techniques developed in the field of interactive proofs, which we summarize in Section II. In Section III, we invoke results of Goldwasser, Micali, and Rackoff [4], Goldreich, Micali, and Wigderson [3], Goldwasser and Sipser [5], and Boppana, Hastad, and Zachos [2], to show that if Code Equivalence is NP-complete, then the polynomial hierarchy collapses.Yet, we do state also a negative result, namely, that Code Equivalence is also unlikely to be too easy. We do this by relating Code Equivalence to the Graph Isomorphism problem. Let and be two undirected graphs with the same set of vertices V, and with sets of edges and , respectively. We say that Qi is isomorphic to Q2 if there exists a permutation (isomorphism) such that if and only if (we assume here that the graphs have no parallel edges; if they do, then and are multisets, in which case isomorphism requires equality of the multiplicities of and in and E2, respectively). The problem of deciding efficiently (i.e., in polynomial time) whether two graphs are isomorphic is a notoriously open question in Computer Science. The problem has been studied extensively in recent decades, but the state of the art is that there is no known efficient algorithm for determining whether two given graphs are isomorphic.In Section IV, we show a polynomial-time reduction from Graph Isomorphism to Code Equivalence. This implies that presenting an |

0018-9448/97$ 10.00 © 1997 IEEE