do the traceback process and decode k information bits. As a result, the traceback depth of the punctured trellis is the same as that of the corresponding ordinary trellis.

A rate-k/n code has 2^k branches leaving or entering each state, and requires 2^n different branch metrics to be computed. A punctured code of the same rate is treated as k steps of a binary-branching trellis to perform the basic computation. Thus we must perform $m2^k$ ACS operations for the regular form of the trellis, and $2km$ operations in the punctured form. Thus treating the code in its punctured form results in considerable complexity savings in metric accumulation and branch comparison operations for higher rate codes.

VI. Discussion

We have designed rate-$2/3$ and rate-$3/4$ PTCM with QAM and rate-$2/3$ PTCM with PSK. We found the optimal position for puncturing, generators for the rate-$1/2$ trellis, branch metrics, and coset partitioning in QAM and PSK. As a result, we obtained very good rate-$2/3$ PTCM codes. We have also designed another kind of PTCM which is using the existing best punctured convolutional code and can be used in the easy construction of a $180°$ rotationally invariant PTCM.

In general, whenever the metric can be decomposed into orthogonal components, a punctured code can be constructed which apart from negligible boundary effects has no performance loss with respect to the equivalent original TCM scheme.

We provided a $90°$ RI-PTCM for QAM signaling. $90°$ invariance requires nonlinear codes when the cosets are two-dimensional. This may be accomplished by using ordinary punctured coding and then swapping state labels, or rearranging the branch labels which decreases the minimum distance. On the other hand, we can easily design a $180°$ RI-PTCM, where the original rate-$1/2$ code must be $180°$-invariant and all punctured versions of the code will be invariant. Thus we may continue to use the the same decoder structure for all members of the family.

References

[1] J. K. Wolf and E. Zehavi, "P^2 codes: Pragmatic trellis codes utilizing punctured convolutional codes," *IEEE Commun. Mag.*, vol. 33, no. 2, pp. 94–99, Feb. 1995.

[2] F. Chan and D. Haccoun, "High-rate punctured convolutional codes for trellis-coded modulation," in *Proc. IEEE Int. Symp. on Information Theory* (San Antonio, TX 1993), p. 414.

[3] E. Biglieri, D. Divsalar, P. J. McLane, and M. K. Simon, *Introduction to Trellis-Coded Modulation with Applications*. New York: Macmillan, 1991.

[4] J. B. Anderson and S. Mohan, *Source and Channel Coding–An Algorithmic Approach*. Norwell, MA: Kluwer, 1991.

[5] A. R. Calderbank, Lecture notes on Trellis Coded Modulation.

[6] A. Viterbi, J. K. Wolf, E. Zehavi, and R. Padovani, "A pragmatic approach to trellis coded modulation," *IEEE Commun. Mag.*, vol. 27, no. 7, pp. 11–19, July 1989.

[7] G. D. Forney Jr., "Coset codes Part I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123–1151, Sept. 1988.

[8] L. F. Wei, "Trellis-coded modulation with multidimensional constellations," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 483–501, July 1987.

[9] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 55–67, Jan. 1982.

[10] J. B. Cain, G. C. Clark, and J. M. Geist, "Punctured convolutional codes of rate $(n-1)/n$ and simplified maximum likelihood decoding," *IEEE Trans. Inform. Theory*, vol IT-25, pp. 97–100, Jan. 1979.

The Ternary Golay Code, the Integers mod 9, and the Coxeter–Todd Lattice

A. R. Calderbank, *Member, IEEE*, and N. J. A. Sloane, *Fellow, IEEE*

***Abstract*— The 12-dimensional Coxeter–Todd lattice can be obtained by lifting the ternary Golay code to a code over the integers mod 9 and applying Construction A.**

Several recent papers have pointed out connections between codes over $\mathbb{Z}_4$ and lattices [1], [3]. It is the aim of this correspondence to show that the Coxeter–Todd lattice K_{12} ([4], [5, ch. 4, sec. 9]) can be obtained in a similar way from a code over $\mathbb{Z}_9$.

Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ denote the ring of integers mod m. Let C be a cyclic code of length n over $\mathbb{Z}_p$, where p is a prime such that $(n,p)=1$, with generator polynomial $g(x)$. If α is a primitive element of $\mathbb{Z}_p$, let S denote the set of s such that α^s is a root of $g(x)$. It is pointed out in [2] that C is self-orthogonal if and only if $S \cup (-S)$ contains representatives from every residue class mod n. Furthermore, for $a = 2, 3, \cdots$, exactly the same condition is also necessary and sufficient for the Hensel lift (cf. [6]) of C to a cyclic code over $\mathbb{Z}_{p^a}$ to be self-orthogonal mod p^a. Self-orthogonality of the lifted code is a purely combinatorial property of the roots of the original code.

Consider now the $[11, 5, 6]$ self-orthogonal ternary Golay code, with generator polynomial

$$g(x) = x^6 - x^5 - x^4 - x^3 + x^2 + 1$$

([7, p. 482]). This lifts to

$$G(x) = x^6 + 2x^5 - 4x^4 + 2x^3 + x^2 - 3x + 1$$

a divisor of $x^{11} - 1 \bmod 9$, which by the previous remark generates a self-orthogonal code over $\mathbb{Z}_9$. Appending a 0 to these words and adjoining the all-1's vector as an additional generator, we obtain a self-dual code $\mathcal{G}$ of length 12 over $\mathbb{Z}_9$.

By applying Construction A (cf. [5, chs. 5, 7]), that is, taking all vectors in $\mathbb{Z}^{12}$ that are congruent to any codeword of $\mathcal{G}$ mod 9, and rescaling by dividing by $\sqrt{3}$, we obtain the Coxeter–Todd lattice: a 12-dimensional lattice of determinant 729, minimal squared length 4, and 756 minimal vectors. We omit the straightforward proof that this is isomorphic to the standard construction from a code (the "hexacode") of length 6 over GF(4) ([4], [5, p. 128], [8]).

References

[1] A. Bonnecaze, A. R. Calderbank, and P. Solé, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, vol. 41, pp. 366–377 and 1536, 1995.

[2] A. R. Calderbank, W.-C. W. Li, and B. Poonen, "A 2-adic approach to the analysis of cyclic codes," preprint.

[3] A. R. Calderbank and N. J. A. Sloane, "Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices," *J. Algebraic Combin.*, submitted.

[4] J. H. Conway and N. J. A. Sloane, "The Coxeter–Todd lattice, the Mitchell group and related sphere packings," *Math. Proc. Comb. Phil. Soc.*, vol. 93, pp. 421–440, 1983.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed. New York: Springer-Verlag, 1993.

Manuscript received October 10, 1995.

The authors are with the Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974 USA.

Publisher Item Identifier S 0018-9448(96)01480-0.

[6] F. Q. Gouvêa, *P-adic Numbers*. New York: Springer-Verlag, 1993, esp. sec. 3.4.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: The Netherlands, North-Holland, 1977.
[8] N. J. A. Sloane, "Self-dual codes and lattices," in *Relations Between Combinatorics and Other Parts of Mathematics* (Proc. Symp. Pure Math., vol. 34). Providence, RI: Amer. Math. Soc., 1979, pp. 273–308.

Complex Hadamard Matrices Related to Bent Sequences

Shinya Matsufuji and Naoki Suehiro

***Abstract*— This correspondence gives construction of complex Hadamard matrices of order p^n, where p is prime and n is even. The complex Hadamard matrices include bi-phase Hadamard matrices whose elements take $\{-1,+1\}$, and four-phase Hadamard matrices whose elements take $\{\pm 1,\pm j\}$ with $j=\sqrt{-1}$.**

***Index Terms*—Hadamard matrix , unitary matrix, bent function, bent sequence, spread-spectrum communication**

I. Introduction

Hadamard matrices are often used for some applications, such as error-correcting codes, spread sequences, and so on [1], [2].

Let H be a complex matrix of order N, whose elements take the unit magnitude. Then the matrix H is called as a complex Hadamard matrix if

$$HH^* = NE \tag{1}$$

where H^* denotes the complex-conjugate transpose of H, and E is the unit matrix of order N.

In this correspondence we give complex Hadamard matrices of order $N=p^n$ related to bent sequences, so that the magnitude of the sum of elements for each row is 0 except one row whose all the elements are 1, where p is prime, n is positive integer.

II. Complex Hadamard Matrices Related to Bent Sequences

Let α be a primitive element of $\mathrm{GF}(p^n)$ with an even n, z an element of

$$\mathrm{GF}(p^n)=\{0,\alpha^i\}(0\le i\le p^n-2).$$

Let $\mathrm{tr}(\cdot)$ be a trace function from $\mathrm{GF}(p^n)$ onto $\mathrm{GF}(p)$ defined by

$$\mathrm{tr}(z)=z+z^p+z^{p^2}+\cdots+z^{p^{n-1}}. \tag{2}$$

Then we consider the following functions:

$$f_{\vec{a}}(z)=g_{\vec{a}}(L(z))+\mathrm{tr}(\sigma z) \tag{3}$$

$$g_{\vec{a}}(\vec{x})=h(\vec{x})+\vec{a}\vec{x}^T,\quad \vec{a}\in V_p^{n/2} \tag{4}$$

$$\vec{x}=L(z)=(\mathrm{tr}(\beta_1 z),\mathrm{tr}(\beta_2 z),\cdots,\mathrm{tr}(\beta_{n/2}z))\in V_p^{n/2} \tag{5}$$

$$\sigma\in \mathrm{GF}(p^n)\backslash\mathrm{GF}(p^{n/2}) \tag{6}$$

Manuscript received December 16, 1994; revised September 28, 1995. The material in this correspondence was presented at the IEEE International Simposium on Information Theory, Trondheim, Norway, June 1994.

S. Matsufuji is with the Department of Information Science, Saga University, Saga 840, Japan.

N. Suehiro is with the Institute of Applied Physics, University of Tsukuba, 1-1-1 Tennoudai, Tsukuba, Ibaraki 305, Japan.

Publisher Item Identifier S 0018-9448(96)01348-X.

where $\{\beta_1,\cdots,\beta_{n/2}\}$ is a basis of $\mathrm{GF}(p^{n/2})$, and $h(\vec{x})$ is a nonlinear function mapping $n/2$-tuples over $\mathrm{GF}(p)$, i.e., $V_p^{n/2}$, into real numbers. If $g_{\vec{a}}(\vec{x})$ or $h(\vec{x})$ is a real-valued bent function, $f_{\vec{a}}(z)$ is a function generating bent sequences of period p^n-1 with optimal periodic-correlation properties [3], [4].

Theorem 1: A matrix of order $N=p^n$ given by

$$H=\begin{pmatrix} 1,1,\cdots,1 \\ \omega^{\mathrm{tr}(z)} \\ \omega^{\mathrm{tr}(\alpha^{(p^{n/2}+1)}z)} \\ \omega^{\mathrm{tr}(\alpha^{(p^{n/2}+1)2}z)} \\ \vdots \\ \omega^{\mathrm{tr}(\alpha^{(p^{n/2}+1)(p^{n/2}-2)}z)} \\ \omega^{f_{\vec{a}}(z)} \\ \omega^{f_{\vec{a}}(\alpha^{(p^{n/2}+1)}z)} \\ \omega^{f_{\vec{a}}(\alpha^{(p^{n/2}+1)2}z)} \\ \vdots \\ \omega^{f_{\vec{a}}(\alpha^{(p^{n/2}+1)(p^{n/2}-2)}z)} \end{pmatrix} z\in \mathrm{GF}(p^n),\ \vec{a}\in V_p^{n/2} \tag{7}$$

is a complex Hadamard matrix, so that the magnitude of the sum of elements for each row in H is 0 except one row so that all the elements are 1.

Theorem 1 can be derived in consideration of periodic correlation of bent sequences [3]–[5]. That is, it follows from the fact that the auto- and crosscorrelation functions between the M-sequence of period p^n-1 expressed by $\mathrm{tr}(z)$ and bent sequences of period p^n-1 take the value -1 for particular shifts which are a multiple of $p^{n/2}+1$.

We note that the number of complex Hadamard matrices is infinite, because the function $h(\vec{x})$ of (4) can be made infinite. We also note that if $p=2$, the complex Hadamard matrices include bi-phase Hadamard matrices whose elements take $\{-1,+1\}$, and four-phase Hadamard matrices whose elements take $\{\pm 1,\pm j\}$ with $j=\sqrt{-1}$.

III. Conclusion

We have given complex Hadamard matrices of order p^n with a prime p and an even n, which is similar to the M-sequence-type Hadamard matrix. The complex Hadamard matrix using a bent function $h(\vec{x})$ may well be adapted for spread spectrum (SS) communication, because rows in the complex Hadamard matrix, which consist of different sequences, possess low periodic correlation values. We desire to find the factorization of complex Hadamard matrices which can give a fast algorithm for a correlation detactor in SS communication.

References

[1] S. S. Agaian, *Hadamard Matrices and their Applications* (Lecture Notes in Mathematics 1168). Berlin, Germany: Springer-Verlag, 1985.
[2] N. Suehiro, "Fast algorithms for M-sequence type and E-sequence type Hadamard matrices," in *Proc. Int. Symp. on Spread Spectrum Technology and Applications* (Yokohama, Japan, Nov. 29–December 2, 1992), pp. 55–58.
[3] P. V. Kumar, "On bent sequences and generalized bent functions," Ph.D. dissertation, Elec. Eng. Dept., Univ. Southern Calif., Aug. 1983.
[4] S. Matsufuji and K. Imamura, "Real-valued bent function and its application to the design of balanced quadriphase sequences with optimal correlation properties," *Springer Verlag, Lecture Notes in Computer Science*, vol. 508, pp. 113–121, Aug. 1991.
[5] ——, "Balanced quadriphase sequences with optimal correlation properties constructed by real-valued bent functions," *IEEE Trans. Inform. Theory*, vol. 39, pp. 305–310, Jan. 1993.