Combining the results in Lemmas 1.1, 1.2, and Theorems 4.3, 5.7, and 6.4, we have the following.

Theorem 6.5: There exists an optimal $(v, 4, 1)$-OOC for all positive integers $v \equiv 6 \pmod{12}$ or $v \equiv 24 \pmod{48}$. There exists also an optimal $(12v, 4, 1)$-OOC exists for any positive integer v whose prime factors are all congruent to 1 modulo 4.

ACKNOWLEDGMENT

The authors wish to thank the referees and Prof. L. Zhu for their helpful comments. They are especially grateful to one of the referees for providing a short proof of Lemma 6.1.

REFERENCES

[1] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[2] S. Bitan and T. Etzion, "Constructions for optimal constant weight cyclically permutable codes and difference families," *IEEE Trans. Inform. Theory*, vol. 41, pp. 77–87, Jan. 1995.
[3] R. C. Bose, "On the construction of balanced incomplete block designs," *Ann. Eugenics*, vol. 9, pp. 353–399, 1939.
[4] A. E. Brouwer, A. Schrijver, and H. Hanani, "Group divisible designs with block-size 4," *Discr. Math.*, vol. 20, pp. 1–19, 1977.
[5] M. Buratti, "Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$," *Discr. Math.*, vol. 138, pp. 169–175, 1995.
[6] ——, "Recursive constructions for difference matrices and relative difference families," *J. Combin. Des.*, vol. 6, pp. 165–182, 1998.
[7] ——, "Some regular Steiner 2-designs with block size 4," *Ars Combin.*, vol. 55, pp. 133–137, 2000.
[8] C. J. Colbourn, "Difference triangle sets," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL: CRC, 1996, pp. 312–317.
[9] M. J. Colbourn and C. J. Colbourn, "Recursive constructions for cyclic block designs," *J. Statist. Plann. Inference*, vol. 10, pp. 97–103, 1984.
[10] C. J. Colbourn and W. de Launey, "Difference matrices," in *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL: CRC, 1996, pp. 287–297.
[11] C. J. Colbourn and J. H. Dinitz, *CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC, 1996.
[12] C. J. Colbourn, J. H. Dinitz, and D. R. Stinson, "Applications of combinatorial designs to communications, cryptography, and networking," *London Math. Soc. Lecture Note Ser.*, vol. 267, pp. 37–100, 1999.
[13] K. Chen, G. Ge, and L. Zhu, "Starters and related codes," *J. Statist. Plann. Inference*, vol. 86, pp. 379–395, 2000.
[14] K. Chen and L. Zhu, "Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$," *J. Combin. Des.*, vol. 7, pp. 21–30, 1999.
[15] ——, "Existence of $(q, 6, 1)$ difference families with q a prime power," *Des. Codes. Cryptogr.*, vol. 15, pp. 167–173, 1998.
[16] F. P. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inform. Theory*, vol. 35, pp. 595–604, May 1989. Correction: *IEEE Trans. Inform. Theory*, vol. 38, p. 1492, July 1992.
[17] J. H. Dinitz and D. R. Stinson, "Room squares and related designs," in *Contemporary Design Theory: A Collection of Surveys*. New York: Wiley, 1992, pp. 137–204.
[18] R. Fuji-Hara and Y. Miao, "Optical orthogonal codes: Their bounds and new optimal constructions," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2396–2406, Nov. 2000.
[19] M. Hall, Jr., *Combinatorial Theory*, 2nd ed, New York: Wiley, 1986.
[20] M. Jimbo and S. Kuriki, "On a composition of cyclic 2-designs," *Discr. Math.*, vol. 46, pp. 249–255, 1983.
[21] J. A. John, *Cyclic Designs*. New York: Chapman and Hall, 1987.
[22] S. M. Johnson, "A new upper bound for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, Apr. 1962.
[23] D. Jungnickel, "On difference matrices, resolvable transversal designs and generalized Hadamard matrices," *Math. Z.*, vol. 167, pp. 49–60, 1979.
[24] S. V. Maric and V. K. N. Lau, "Multirate fiber-optic CDMA: System design and performance analysis," *J. Lightwave Technol.*, vol. 16, pp. 9–17, 1998.
[25] S. V. Maric, O. Moreno, and C. Corrada, "Multimedia transmission in fiber-optic LAN's using optical CDMA," *J. Lightwave Technol.*, vol. 14, pp. 2149–2153, 1996.
[26] A. Pott, "A survey on relative difference sets," in *Groups, Difference Sets and the Monster*, Berlin-New York: de Gruyter, 1996, pp. 195–232.
[27] J. A. Salehi and C. A. Brackett, "Code-division multiple access techniques in optical fiber networks: Part 1 and part 2," *IEEE Trans. Commun.*, vol. 37, pp. 824–842, 1989.
[28] Y. X. Yang and X. D. Lin, *Code and Cryptography (in Chinese)*. Beijing, China: Renmin Youdian, 1992.
[29] J. Yin, "Some combinatorial constructions for optical orthogonal codes," *Discr. Math.*, vol. 185, pp. 201–219, 1998.

A Table of Upper Bounds for Binary Codes

Erik Agrell, *Member, IEEE*, Alexander Vardy, *Fellow, IEEE*, and Kenneth Zeger, *Fellow, IEEE*

***Abstract*—Let $A(n, d)$ denote the maximum possible number of codewords in an (n, d) binary code. We establish four new bounds on $A(n, d)$, namely, $A(21, 4) \leqslant 43\,689$, $A(22, 4) \leqslant 87\,378$, $A(22, 6) \leqslant 6941$, and $A(23, 4) \leqslant 173\,491$. Furthermore, using recent upper bounds on the size of constant-weight binary codes, we reapply known methods to generate a table of bounds on $A(n, d)$ for all $n \leqslant 28$. This table extends the range of parameters compared with previously known tables.**

***Index Terms*—Binary codes, constant-weight codes, Delsarte inequalities, linear programming, upper bounds.**

I. INTRODUCTION

An (n, d) *binary code* is a set of binary vectors (or *codewords*) of length n such that the Hamming distance between any two of them is at least d. An (n, d, w) *constant-weight* binary code is an (n, d) binary code in which all codewords have the same number w of ones. The *size* of a code is its cardinality. The maximum possible sizes of binary codes and constant-weight binary codes are denoted $A(n, d)$ and $A(n, d, w)$, respectively. Known methods to bound $A(n, d)$ often assume that bounds on $A(n, d, w)$ are known. Motivated by the recently published [1] tables of upper bounds on $A(n, d, w)$, we compute bounds on $A(n, d)$ for all lengths $n \leqslant 28$. This generates Table I, which is the main result of this correspondence. The table gives upper bounds for longer codes than existing tables; it also includes several updates to bounds in these tables.

The latest published table of upper bounds on $A(n, d)$ is [5, p. 248], for the range $n \leqslant 24$ and $d \leqslant 10$. A wider range of parameters is included in [4, Table II]. Updates to the combination of the upper bounds in [4] and [5] are given in boldface in Table I. Specifically, we establish

Manuscript received February 28, 2001; revised July 6, 2001. This work was supported in part by the National Science Foundation, the David and Lucile Packard Foundation, Stiftelsen ISS'90, and Svensk Informations- och Mikrografiorganisation. This work was carried out in part while E. Agrell was visiting the University of California, San Diego.

E. Agrell is with the Department of Signals and Systems, Chalmers University of Technology, 41296 Göteborg, Sweden (e-mail: agrell@s2.chalmers.se).

A. Vardy and K. Zeger are with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093-0407 USA (e-mail: vardy@montblanc.ucsd.edu; zeger@ucsd.edu).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)08950-7.

TABLE I
A TABLE OF BOUNDS ON $A(n,\, d)$. BOLDFACE DENOTES UPDATES TO [4] AND [5]

n	$d=4$	$d=6$	$d=8$	$d=10$	$d=12$	$d=14$
6	4^{1}	2^{1}				
7	8^{1}	2^{1}				
8	16^{1}	2^{1}	2^{1}			
9	20^{4}	4^{1}	2^{1}			
10	40^{1}	6^{1}	2^{1}	2^{1}		
11	72^{S}	12^{1}	2^{1}	2^{1}		
12	144^{S}	24^{1}	4^{1}	2^{1}	2^{1}	
13	256^{3}	32^{S}	4^{1}	2^{1}	2^{1}	
14	512^{3}	64^{3}	8^{1}	2^{1}	2^{1}	2^{1}
15	1024^{2}	128^{3}	16^{1}	4^{1}	2^{1}	2^{1}
16	2048^{2}	256^{2}	32^{1}	4^{1}	2^{1}	2^{1}
17	$2720-3276^{3}$	$256-340^{\mathrm{S}}$	$36-37^{\mathrm{S}}$	6^{1}	2^{1}	2^{1}
18	$5312-6552^{1}$	$512-680^{1}$	$64-72^{\mathrm{S}}$	10^{1}	4^{1}	2^{1}
19	$10496-13104^{1}$	$1024-1288^{4}$	$128-144^{4}$	20^{1}	4^{1}	2^{1}
20	$20480-26208^{1}$	$2048-2372^{4}$	$256-279^{3}$	40^{1}	6^{1}	2^{1}
21	$36864-\mathbf{43689}^{4}$	$2560-4096^{\mathrm{S}}$	512^{S}	$42-48^{\mathrm{S}}$	8^{1}	4^{1}
22	$73728-\mathbf{87378}^{1}$	$4096-\mathbf{6941}^{4}$	1024^{3}	$50-88^{\mathrm{S}}$	12^{1}	4^{1}
23	$147456-\mathbf{173491}^{3}$	$8192-13774^{4}$	2048^{3}	$76-150^{4}$	24^{1}	4^{1}
24	$294912-\mathbf{344308}^{2}$	$16384-24106^{4}$	4096^{2}	$128-280^{3}$	48^{1}	6^{1}
25	$524288-\mathbf{599185}^{4}$	$16384-\mathbf{48148}^{3}$	$4096-\mathbf{6425}^{4}$	$176-\mathbf{549}^{4}$	$52-\mathbf{56}^{\mathrm{S}}$	8^{1}
26	$1048576-\mathbf{1198370}^{1}$	$32768-\mathbf{86132}^{4}$	$4096-\mathbf{10336}^{4}$	$270-\mathbf{1029}^{4}$	$64-\mathbf{98}^{\mathrm{S}}$	14^{1}
27	$2097152-\mathbf{2396740}^{1}$	$65536-\mathbf{162400}^{4}$	$8192-\mathbf{17804}^{3}$	$512-\mathbf{1764}^{3}$	$128-\mathbf{169}^{4}$	28^{1}
28	$4194304-\mathbf{4793480}^{1}$	$131072-\mathbf{291269}^{4}$	$16384-\mathbf{32205}^{4}$	$1024-\mathbf{3200}^{3}$	$178-\mathbf{288}^{3}$	56^{1}

four new bounds on $A(n,\, d)$ for $n \leqslant 24$, namely, $A(21,\, 4) \leqslant 43\,689$, $A(22,\, 4) \leqslant 87\,378$, $A(22,\, 6) \leqslant 6941$, and $A(23,\, 4) \leqslant 173\,491$. Superscripts in Table I indicate the method used to obtain each upper bound, where integers refer to theorem numbers in this correspondence while S refers to bounds for specific parameters (discussed in the last paragraph of the next section). The best known lower bounds are included for completeness; these are taken from [9].

Online versions of the tables of bounds on $A(n,\, d)$ and $A(n,\, d,\, w)$ are available at [2]. We welcome reports of any updates, which will be recorded at [2] upon verification.

II. A TABLE OF BOUNDS ON $A(n,\, d)$

We start with a brief review of known upper bounds on $A(n,\, d)$ that are referenced in Table I. The following bounds are due to Plotkin [12].

Theorem 1:

$$\begin{aligned} A(n,\, d) &\leqslant 2A(n-1,\, d) \\ A(n,\, d) &\leqslant 2\left\lfloor \frac{d}{2d-n} \right\rfloor, && \text{if } n < 2d \\ A(n,\, d) &\leqslant 2n, && \text{if } n = 2d. \end{aligned}$$

Johnson [10, p. 532] showed that the sphere-packing bound can be improved as follows.

Theorem 2: For every positive integer δ

$$A(n,\, 2\delta) \leqslant 2^{n-1} \left(\binom{n-1}{0} + \cdots + \binom{n-1}{\delta-1} + \frac{\binom{n-1}{\delta} - \binom{2\delta-1}{\delta-1} A(n-1,\, 2\delta,\, 2\delta-1)}{\left\lfloor \binom{n-1}{\delta} \right\rfloor} \right)^{-1}.$$

The best known bounds on $A(n,\, d,\, w)$ are tabulated in [1], [2]. One useful result of Theorem 2 is $A(24,\, 4) \leqslant 344\,308$. This was known to Johnson [8, Table I] in 1971, but has been overlooked in later tables [4], [5].

The *distance distribution* of a binary code $\mathcal{C}$ is defined as the sequence

$$A_i = |\{(\boldsymbol{c}_1,\, \boldsymbol{c}_2) \in \mathcal{C} \times \mathcal{C}\colon d(\boldsymbol{c}_1,\, \boldsymbol{c}_2) = i\}| / |\mathcal{C}|$$

for $i = 0,\, 1,\, \ldots,\, n$, where $d(\cdot,\, \cdot)$ is the Hamming distance. It is known that

$$A(n,\, d) = A(n+1,\, d+1)$$

if d is odd. Furthermore, for any $(n,\, d)$ binary code with even d, there exists another $(n,\, d)$ binary code with the same number of codewords, in which all codewords have even weight. Hence, the search for $A(n,\, d)$ can be limited to those codes for which d is even and $A_i = 0$ for all odd i. The linear programming bound was introduced by Delsarte [6], who showed that the distance distribution of any code satisfies

$$\sum_{i=0}^{n} A_i P_k(i) \geqslant 0$$

for $k = 0,\, 1,\, \ldots,\, n$, where $P_k(x)$ is the *Krawtchouk polynomial* of degree k, given by

$$P_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}.$$

As discussed above, it would suffice to consider only even values of d, while assuming that $A_i = 0$ except for A_0 and A_d, $A_{d+2},\, \ldots,\, A_{2\lfloor n/2 \rfloor}$. This leads to the following theorem.

Theorem 3: For every positive even integer d

$$A(n,\, d) \leqslant 1 + \left\lfloor \max(A_d + A_{d+2} + \cdots + A_{2\lfloor n/2 \rfloor}) \right\rfloor$$

subject to the constraints

$$0 \leqslant A_i \leqslant A(n,\, d,\, i), \qquad i = d,\, d+2,\, \ldots,\, 2\lfloor n/2 \rfloor$$

$$\sum_{j=d/2}^{\lfloor n/2 \rfloor} A_{2j} P_k(2j) \geqslant -\binom{n}{k}, \qquad k = 1,\, 2,\, \ldots,\, \lfloor n/2 \rfloor. \tag{1}$$

In some cases, the right-hand side of (1) can be slightly increased, as in the following theorem [3, Theorems 5, 8].

Theorem 4: The distance distribution of an (n, d) binary code of odd size M satisfies

$$\sum_{j=d/2}^{\lfloor n/2 \rfloor} A_{2j} P_k(2j) \geqslant \frac{1-M}{M} \binom{n}{k}, \qquad k = 1, 2, \ldots, \lfloor n/2 \rfloor$$

while if $M \equiv 2 (\bmod 4)$, then for at least one $l \in \{0, \ldots, n\}$

$$\sum_{j=d/2}^{\lfloor n/2 \rfloor} A_{2j} P_k(2j) \geqslant \frac{(2-M)\binom{n}{k} + 2P_k(l)}{M}, \qquad k = 1, \ldots, \lfloor n/2 \rfloor.$$

Finally, some bounds hold only for specific values of n and d. The following bounds, which do not follow from Theorems 1–4, are included in Table I. $A(13, 6) \leqslant 32$ was proved by linear programming in [10, pp. 538–540], using constraints specifically derived for these parameters. In a similar manner, van Pul [13, pp. 32–39] proved $A(18, 8) \leqslant 72$, $A(21, 10) \leqslant 48$, and $A(22, 10) \leqslant 88$, while Honkala [7, pp. 25–27] obtained $A(25, 12) \leqslant 56$ and $A(26, 12) \leqslant 98$. The bounds $A(17, 6) \leqslant 340$, $A(21, 6) \leqslant 4096$, $A(17, 8) \leqslant 37$, and $A(21, 8) \leqslant 512$ have been derived in [3], apparently by linear programming, although the specific inequalities used in the optimization are not disclosed in [3]. The bounds $A(11, 4) \leqslant 72$ and $A(12, 4) \leqslant 144$ have been established in [11] with the help of a computer-assisted search method (thereby proving a long-standing conjecture).

References

[1] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2373–2395, Nov. 2000.

[2] E. Agrell, A. Vardy, and K. Zeger. Tables of binary block codes. [Online]. Available: www.s2.chalmers.se/~agrell

[3] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, "Bounds for binary codes of length less than 25," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 81–93, Jan. 1978.

[4] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY: Springer, 1999.

[6] Ph. Delsarte, "Bounds for unrestricted codes, by linear programming," *Philips Res. Repts.*, vol. 27, pp. 272–289, June 1972.

[7] I. Honkala, "Bounds for binary constant weight and covering codes," Licentiate thesis, Dept. Math., Univ. Turku, Turku, Finland, Mar. 1987.

[8] S. M. Johnson, "On upper bounds for unrestricted binary error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 466–478, July 1971.

[9] S. Litsyn, "An updated table of the best binary codes known," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. 1, pp. 463–498.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[11] P. R. J. Östergård, T. Baicheva, and E. Kolev, "Optimal binary one-error-correcting codes of length 10 have 72 codewords," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1229–1231, May 1999.

[12] M. Plotkin, "Binary codes with specified minimum distance," *IRE Trans. Inform. Theory*, vol. IT-6, pp. 445–450, Sept. 1960.

[13] C. L. M. van Pul, "On bounds on codes," Master's thesis, Dept. Math. Comput. Sci., Eindhoven Univ. Technol., Eindhoven, The Netherlands, Aug. 1982.

Construction of Fast Recovery Codes Using A New Optimal Importance Sampling Method

Michael Yung Chung Wei and Lei Wei, *Senior Member, IEEE*

***Abstract*—In this correspondence, we introduce the problem of constructing good fast recovery convolutional codes. When the constraint lengths of the candidate codes are long (say more than 12), it is too computationally complex to perform the code search task. Fortunately, we can transform the code construction problem to a problem related to a transient Markov system. We then develop an optimal importance sampling (IS) method to fulfill the tasks. In this correspondence, we also prove several propositions for optimal IS. For instance, we show analytically that the optimal IS method is unique. We prove that the optimal IS method must converge to the standard Monte Carlo (MC) simulation method when the sample path length approaches infinity. This finding shows that it is not the size of the state space of the Markov system, but the sample path length, that limits the efficiency of the IS method. Based on insights from the optimal IS method, a suboptimal IS method is then proposed to search for long fast recovery codes. The suboptimal method can achieve a substantial speedup gain. After that, several numerical results are presented to study the efficiency of the IS methods and to justify the code search procedures. Finally, we give the code search results and the application of these codes.**

***Index Terms*—Convolutional codes, fast simulation, importance sampling (IS), M-algorithm (MA), Markov systems, sequential decoding.**

I. Introduction

Over the last 30 years, the famous Viterbi algorithm (VA) has been widely applied in digital communications [1], [2]. The complexity of the VA (in terms of the number of states) grows exponentially with the constraint length of the code. For codes with large constraint lengths, sequential algorithms such as the Fano algorithm [3], [4] and Stack algorithm [5] are often used, since they can achieve a better balance between the error performance and the decoding complexity at a high bit energy-to-noise ratio (E_b/N_o).

Many other reduced complexity VAs have been proposed and studied [6], but most of these are only successful for near-optimal detection on intersymbol interference (ISI) channels or multiuser interference channels. The M-algorithm (MA) has been well studied by Anderson *et al.* [6], [7]. When the MA is applied to decode convolutional codes, its error performance is often much worse than that of the M-state VA using good M-state convolutional codes, especially when the E_b/N_o is small. This poor performance is due to error propagation caused by the correct path lost event. The performance of the MA can be improved either by using error control codes with fast recovery capability (for example, systematic feed forward (SFF) codes [8]) or by modifying the transmission structure to overcome error propagation (for example, short block packet transmission [9] and [10]).

Manuscript received January 13, 2000; revised July 2, 2001. This work was supported in part by ARC under Grant A00103310. The material in this correspondencewas presented in part at the IEEE International Conference on Communications, New Orleans, LA, June 18–22, 2000.

M. Y. C. Wei is with Taiwan Defense Minstrial Office, Taipei, ROC (e-mail: l.wei@elec.uow.edu.au).

L. Wei was with the School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Wollongong, NSW2522, Australia. He is now with the School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816 USA (e-mail: lei@ee.ucf.edu).

Communicated by T. E. Fuja, Associate Editor At-Large.

Publisher Item Identifier S 0018-9448(01)08951-9.