Chalmers Publication Library

Copyright Notice

©2001 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This document was downloaded from Chalmers Publication Library (http://publications.lib.chalmers.se/), where it is available in accordance with the IEEE PSPB Operations Manual, amended 19 Nov. 2010, Sec. 8.1.9 (http://www.ieee.org/documents/opsmanual.pdf)

(Article begins on next page)

A Table of Upper Bounds for Binary Codes

Erik Agrell, Alexander Vardy, and Kenneth Zeger

Abstract— **Let $A(n,d)$ denote the maximum possible number of codewords in an (n,d) binary code. We establish 4 new bounds on $A(n,d)$, namely $A(21,4) \leqslant 43689$, $A(22,4) \leqslant 87378$, $A(22,6) \leqslant 6941$, and $A(23,4) \leqslant 173491$. 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.**

Keywords— **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 four new bounds on $A(n,d)$ for $n \leqslant 24$, namely $A(21,4) \leqslant 43689$, $A(22,4) \leqslant 87378$, $A(22,6) \leqslant 6941$, and $A(23,4) \leqslant 173491$. 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.

Manuscript submitted February 28, 2001 to the IEEE Transactions on Information Theory. Research 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 Erik Agrell was visiting the University of California, San Diego.

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

Alexander Vardy and Kenneth Zeger are with the Department of Electrical and Computer Engineering, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0407, USA (e-mail: vardy@montblanc.ucsd.edu and zeger@ucsd.edu).

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 $A(24,4) \leqslant 344308$. 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 $\mathscr{C}$ is defined as the sequence $A_i = |\{(\boldsymbol{c}_1, \boldsymbol{c}_2) \in \mathscr{C} \times \mathscr{C} : d(\boldsymbol{c}_1, \boldsymbol{c}_2) = i\}|/|\mathscr{C}|$ 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.

Erratum: In Theorem 2, the denominator "\lfloor {n-1 \choose \delta} \rfloor" should be "\lfloor (n-1)/\delta \rfloor"

TABLE I
A table of bounds on $A(n,d)$. Boldface denotes updates to [4, 5].

n	d = 4	6	8	10	12	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

Theorem 3. *For every positive even integer d,*

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

subject to the constraints

$$0 \leqslant A_i \leqslant A(n,d,i), \qquad i = d, d+2, \ldots, 2\lfloor n/2 \rfloor$$
$$\sum_{j=d/2}^{\lfloor n/2 \rfloor} A_{2j} P_k(2j) \geqslant -\binom{n}{k}, \qquad k = 1, 2, \ldots, \lfloor n/2 \rfloor. \quad (2)$$

In some cases, the right-hand side of (2) 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 $M \equiv 2 \pmod 4$, then for at least one $l \in \{0, \ldots, n\}$

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

Finally, some bounds hold only for specific values of n and d. The following bounds, that 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," available online at `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. 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*. New York, NY: Springer, 3rd ed., 1999.

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

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

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

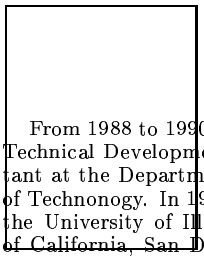
[9] S. Litsyn, "An updated table of the best binary codes known," in *Handbook of Coding Theory* (V. S. Pless and W. C. Huffman, eds.), vol. 1, pp. 463–498, Amsterdam: Elsevier, 1998.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: 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. 6, pp. 445–450, Sept. 1960.

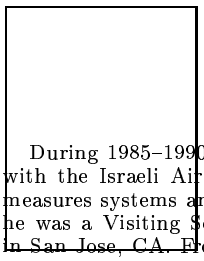
[13] C. L. M. van Pul, "On bounds on codes," *Master's thesis*, Dept. of Mathematics and Computing Science, Eindhoven Univ. of Technology, Eindhoven, The Netherlands, Aug. 1982.



Erik Agrell was born in Göteborg, Sweden in 1965. He received the M.S. degree in electrical engineering in 1989 and the Ph.D. degree in information theory in 1997, both from Chalmers University of Technology, Sweden.

From 1988 to 1990 he was employed as a Systems Analyst at Volvo Technical Development, and from 1990 to 1997 as a Research Assistant at the Department of Information Theory, Chalmers University of Technonogy. In 1997–1999, he was a Postdoctoral Researcher with the University of Illinois at Urbana-Champaign and the University of California, San Diego. In 1999, he joined Chalmers Lindholmen University College, Sweden, as an Associate Professor. He is now an Associate Professor in the Department of Signals and Systems, Chalmers University of Technology, Sweden. His research interests include block codes and lattices, vector quantization, and algorithms.

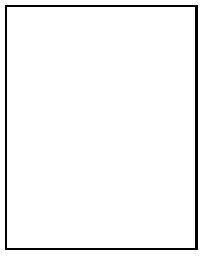
He is Publications Editor for IEEE Transactions on Information Theory.



Alexander Vardy (S'88, M'91, SM'94, F'98) was born in Moscow, USSR, in 1963. He received his B.Sc. (summa cum laude) from the Technion—Israel Institute of Technology, in 1985, and Ph.D. from the Tel-Aviv University, Israel, in 1991.

During 1985–1990 he was a Research and Development Engineer with the Israeli Air Force, where he worked on electronic counter measures systems and algorithms. During the years 1992 and 1993 he was a Visiting Scientist at the IBM Almaden Research Center, in San Jose, CA. From 1993 to 1998, he was with the University of Illinois at Urbana-Champaign, first as an Assistant Professor then as an Associate Professor. During 1998-1999 he was on sabbatical leave with Centre Nationale de la Recherche Scientifique, France. He is presently a Professor in the Department of Electrical Engineering and in the Depratment of Computer Science at the University of California, San Diego. His research interests include error-correcting codes, decoding algorithms, signal constellations and sphere packings, coding for storage devices, and computational complexity.

Dr. Vardy received the Levi Eshkol, Rothschild, and Fulbright Fellowships in 1990, 1992, and 1992, respectively. He was awarded the NSF Research Initiation and CAREER awards in 1994 and 1995. In 1996, he received the Xerox Award for faculty research, and was appointed Fellow in the Center for Advanced Study at the University of Illinois. In the same year, he became a Fellow of the David and Lucile Packard Foundation, Palo Alto, CA. He was Guest Editor for the special issue on "Codes and Complexity" of the IEEE Transactions on Information Theory, published in November 1996. He served one the Editorial Board of the IEEE Transactions on Information Theory as Associate Editor for Coding Theory during 1995-1998, and as Editor-in-Chief during 1998-2001. He is a member of the Board of Governors of the IEEE Information Theory Society.



Kenneth Zeger (S'85-M'90-SM'95-F'00) was born in Boston in 1963. He received both the S.B. and S.M. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology in 1984, and both the M.A. degree in mathematics and the Ph.D. in electrical engineering at the University of California, Santa Barbara, in 1989 and 1990, respectively. He was an Assistant Professor of Electrical Engineering at the University of Hawaii from 1990 to 1992. He was in the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory at the University of Illinois at Urbana-Champaign, as an Assistant Professor from 1992 to 1995, and as an Associate Professor from 1995 to 1996. He has been in the Department of Electrical and Computer Engineering at the University of California at San Diego, as an Associate Professor from 1996 to 1998, and as a Professor from 1998 to present. He received an NSF Presidential Young Investigator Award in 1991. He served as Associate Editor At-Large for the *IEEE Transactions on Information Theory* during 1995-1998, is serving as a member of the Board of Governors of the IEEE Information Theory Society during 1998-2000, and is an IEEE Fellow.