Constant-Weight Code Bounds from Spherical Code Bounds

Erik Agrell
Department of Electrical Engineering
Chalmers Lindholmen University College
P.O. Box 8873, 40272 Göteborg, Sweden
agrell@chl.chalmers.se

Alexander Vardy
Department of Electrical Engineering
University of California at San Diego
La Jolla, CA 92093–0407, U.S.A.
vardy@montblanc.ucsd.edu

Kenneth Zeger
Department of Electrical Engineering
University of California at San Diego
La Jolla, CA 92093–0407, U.S.A.
zeger@ucsd.edu

Abstract — **We present new upper bounds on the size of constant-weight binary codes, derived from bounds for spherical codes. In particular, we improve upon the 1962 Johnson bound and the linear programming bound for constant-weight codes.**

I. Introduction

An (n, d, w) constant-weight code is a binary nonlinear code with length n and minimum Hamming distance d, where all codewords have the same number of ones, w. The maximum size of such a code is denoted $A(n, d, w)$. The value of $A(n, d, w)$ is in general not known, but a number of lower and upper bounds have been established. See [2–4] for summaries of the best bounds known today.

The new bounds presented here are based on concepts from Euclidean geometry, in particular, spherical codes. An (n, s) *spherical code* is a set of points on the n-dimensional unit sphere such that the inner product of any two points is at most s. Its maximum size is denoted by $A_S(n, s)$.

II. Improved Johnson Bound

Through an elementary mapping from binary space to Euclidean space, we obtain the following upper bound. It is equivalent to the well-known Johnson bound from 1962 [2] for $b > \delta/(n+1)$ and improves on it for $0 \le b \le \delta/(n+1)$.

Theorem 1. *Let $b = \delta - w(n-w)/n$. Then*

$$\begin{aligned} A(n, 2\delta, w) &\le \lfloor \delta/b \rfloor, && \text{if } b \ge \delta/n \\ A(n, 2\delta, w) &\le n, && \text{if } 0 < b \le \delta/n \\ A(n, 2\delta, w) &\le 2n-2, && \text{if } b = 0 \end{aligned}$$

Proof: Consider any constant-weight code $\mathscr{C}$ with parameters $(n, 2\delta, w)$ and map it into Euclidean space by replacing the binary components 0 and 1 with, respectively, 1 and -1. After translation and scaling, this yields an $(n-1, s)$ spherical code, where $s = 1 - \delta n/(w(n-w))$. Since its size is upper-bounded by $A_S(n-1, s)$, so is the size of $\mathscr{C}$. Applying known values of $A_S(n-1, s)$ for $s \le 0$ [1] completes the proof. ∎

Some values of $A(n, d, w)$ for which Theorem 1, in conjunction with known lower bounds [3], yields previously unknown exact values are $A(20, 10, 9) = 20$, $A(21, 10, 8) = 21$, $A(24, 10, 7) = 24$, $A(24, 12, 11) = 24$, $A(26, 12, 9) = 26$, and, somewhat surprisingly, $A(28, 14, 12) = A(28, 14, 13) = 28$.

III. Improved Linear Programming Bound

The *distance distribution* of any binary code $\mathscr{C}$ is defined as $A_i = \frac{1}{|\mathscr{C}|}\sum_{\mathbf{c}\in\mathscr{C}} |\{\mathbf{c}' \in \mathscr{C} \mid d(\mathbf{c}, \mathbf{c}') = i\}|$ for $i = 0, \ldots, n$, where $d(\cdot,\cdot)$ denotes the Hamming distance. The *linear programming* bound for a constant-weight code with $w \le n/2$ is $A(n, 2\delta, w) \le 1 + \max \sum_{i=\delta}^{w} A_{2i}$, where the maximum is taken over all $\{A_i\}$ that satisfy certain well-known constraints [2].

We propose an additional constraint in the maximization, which sharpens the bound. In the following theorem, $T'(w_1, n_1, w_2, n_2, d)$ and $T(w_1, n_1, w_2, n_2, d)$ denote the maximum size of an $(n_1 + n_2, d, w_1 + w_2)$ constant-weight code in which the number of ones in the first n_1 positions of all codewords is, respectively, at most w_1 and exactly w_1.

Theorem 2. *For all $i, j \in \{\delta, \delta+1, \ldots, w\}$ with $i \ne j$,*

$$\begin{aligned} P_{ji}A_{2i} + (P_i - P_{ij})\,A_{2j} &\le P_iP_{ji}, && \text{if } P_{ij}/P_i + P_{ji}/P_j > 1 \\ (P_j - P_{ji})\,A_{2i} + P_{ij}A_{2j} &\le P_jP_{ij}, && \text{if } P_{ij}/P_i + P_{ji}/P_j > 1 \\ P_jA_{2i} + P_iA_{2j} &\le P_iP_j, && \text{if } P_{ij}/P_i + P_{ji}/P_j \le 1 \end{aligned}$$

where P_i, P_j, P_{ij}, and P_{ji} are any numbers that satisfy

$$\begin{aligned} &P_i \ge T(i, w, i, n-w, 2\delta) \\ &P_j \ge T(j, w, j, n-w, 2\delta) \\ &P_{ij} \ge \min\{P_i, T'(w-\delta, j, \delta-w+i, n-w-j, \\ &\quad 2\delta-2w+2i)\}, && \text{if } i+j \le n-\delta \\ &P_{ji} \ge \min\{P_j, T'(w-\delta, i, \delta-w+j, n-w-i, \\ &\quad 2\delta-2w+2j)\}, && \text{if } i+j \le n-\delta \\ &P_{ji} = P_{ij} = 0, && \text{if } i+j > n-\delta. \end{aligned}$$

The entities T and T' can be upper-bounded using bounds for spherical codes and so-called *zonal spherical codes*. Details and proofs are given in [1], which also contains several other new bounds, a survey of known bounds on $A(n, d, w)$, and updated tables of $A(n, d, w)$ for $n \le 28$.

New upper bounds obtained through Theorem 2 include $A(20, 8, 9) \le 195$, $A(21, 8, 9) \le 320$, $A(22, 8, 10) \le 641$, $A(24, 8, 11) \le 2188$, and $A(23, 10, 9) \le 81$.

References

[1] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, submitted December 15, 1999, available online at `www.chl.chalmers.se/~agrell`.

[2] 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.

[3] 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.

[4] R.L. Graham and N.J.A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. 26, pp. 37–43, Jan. 1980.

[1] This work was supported in part by the National Science Foundation and by the David and Lucile Packard Foundation.