stichting
mathematisch
centrum

MC

DEPARTMENT OF PURE MATHEMATICS ZW 72/76 APRIL

M.R. BEST

# THE WAX BOUND FOR BINARY CODES

2e boerhaavestraat 49 amsterdam

*Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.*

*The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.*

---

AMS(MOS) subject classification scheme (1970): 94A10, 05B40

---

# The Wax bound for binary codes

by

M.R. Best

ABSTRACT

It is shown that the results in N. WAX, Upper bounds for error detecting and correcting codes, I.R.E. Transactions on Information Theory 5 (1959) 168-174 are erroneous. In particular, the best upper bounds known for A(9,3), A(10,3) and A(11,3) are 40, 80 and 160 respectively.

KEY WORDS & PHRASES: *upper bounds for binary codes, sphere packing*

## 1. INTRODUCTION

In 1959 N. WAX [6] computed a number of upper bounds for binary codes by a method derived from sphere packing in Euclidean spaces as developed by R.A. RANKIN [4] [1]. Most of the bounds obtained were rather weak, but there were three special cases in which his "soft sphere model" seemingly yielded astonishingly good results. These were:

$$A(8,3) \leq 20,$$
$$A(9,3) \leq 39 \text{ (and hence } A(10,3) \leq 78),$$
$$A(11,3) \leq 154.$$

Here A(n,d) denotes the maximal cardinality of a code with wordlength n and minimal Hamming distance at least d.

The first bound was obtained recently by an extension of the linear programming bound (cf. [1]), but the other three bounds could not be obtained by any other method until nowadays.

Several investigators expressed their doubt about Wax's results, but as far as we know nobody carefully checked the technical calculations. In this note we do not either (although e.g. the functions defined in (7) and (8) in [6] certainly do not satisfy the basic conditions for density functions), but we establish a lower bound for the best upper bound that can be achieved with the soft sphere model, whatever clever weight function may be used. Since this lower bound is inconsistent with the data found by Wax, we may conclude that Wax's results are - at least in the interesting cases mentoned above - erroneous.

We are now left with the following bounds for A(8,3), A(9,3), A(10,3) and A(11,3):

---

[1] For more recent results on this theory, cf. C.A. ROGERS [5].

$$A(8,3) = 20$$
$$38 \leq A(9,3) \leq 40$$
$$72 \leq A(10,3) \leq 80$$
$$144 \leq A(11,3) \leq 160$$

(For the lower bounds cf. M.J.E. GOLAY [2] and D. JULIN [3].)

## 2. THE SOFT SPHERE MODEL

Consider an [n,d]-code (i.e. a binary code with wordlength n and minimal Hamming distance at least d) as a subset of the vertices of the hypercube $[0,1]^n$ in Euclidean n-space $\mathbb{R}^n$. The different codepoints have Hamming distance at least d, so their Euclidean distance is at least $\sqrt{d}$. Therefore the spheres with centers in the codepoints and radii $R = \frac{1}{2}\sqrt{d}$ are disjoint. If V denotes the volume of the intersection of each sphere with the hypercube $[0,1]^n$ (by symmetry these volumina are all equal), than the number of codepoints evidently cannot exceed 1/V. Hence $A(n,d) \leq \lfloor 1/V \rfloor$.

This method, using the "hard sphere model", yields very modest results, e.g. $A(9,3) \leq 566$ (and not 56.7 as in [6]) or $A(10,4) \leq 401$.

In order to sharpen the bounds, the hard spheres are replaced by larger ones with variable mass density. As basic conditions it is required that

(i) the density in a point of the sphere is a non-negative function $\rho$ of the distance to the center of the sphere only, and that

(ii) in any configuration of (partly overlapping) spheres with centers at least 2R apart, the total density in each point does not exceed unity.

If M is the mass of the intersection of each sphere with the hypercube[1], we now obtain:

---

1) In case $d \leq 4$ one may define M by $2^{-n}$ times the mass of the whole sphere instead, since the configuration may be continued with period 2 in all directions in $\mathbb{R}^n$. But even this extended model is included in our results, since we estimate M by that number.

$$A(n,d) \leq \lfloor 1/M \rfloor .$$

The main problem is to determine a suitable density which satisfies the basic conditions (i) and (ii), and optimizes the mass M. R.A. RANKIN studied this problem in [4]. In order to simplify computations, he required in addition:

(iii) the spheres have radius $R\sqrt{2}$, i.e. $\rho(r) = 0$ if $r \geq R\sqrt{2}$.

The model described, with the conditions (i), (ii) and (iii), is called the "soft sphere model". We shall denote the least upper bound for A(n,d) that can be achieved with this model by $A_w(n,d)$. Our aim is to give a lower bound for $A_w(n,d)$.

## 3. A LOWER BOUND FOR $A_w(n,d)$

First we derive an upper bound for $\rho$. We define for each positive integer m:

$$y_m = \sqrt{2(m-1)/m}$$

(note: $y_1 = 0$, $y_2 = 1$), and the function $\sigma: [0,\infty] \to [0,1]$ by

$$\begin{aligned} \sigma(r) &= \frac{1}{m} \quad \text{if} \quad Ry_m \leq r < Ry_{m+1} \quad (m=1,2,\ldots,n), \\ &= \frac{1}{n+1} \quad \text{if} \quad Ry_{n+1} \leq r < R\sqrt{2}, \\ &= 0 \quad \text{if} \quad r \geq R\sqrt{2}. \end{aligned}$$

Then we have:

LEMMA 1. $\rho \leq \sigma$.

PROOF. We have to prove that $\rho(r) \leq 1/m$ if $r \geq Ry_m$ for $m = 1,2,\ldots,n+1$. Let $m \in \{1,2,\ldots,n+1\}$. Suppose m spheres with density function $\rho$ are arranged such that their centers form the vertices of an $(m-1)$-dimensional hypertetrahedron in $\mathbb{R}^n$ with edges of length 2R. Then the distance from the center of gravity of the hypertetrahedron to each of the vertices equals

$$R\sqrt{2(m-1)/m} = Ry_m.$$

(Proof by induction.)

The total density in the center of gravity equals $m\rho(Ry_m)$. Hence $\rho(Ry_m) \le 1/m$ and a fortiori $\rho(r) \le 1/m$ if $r \ge Ry_m$. □

This estimate for $\rho$ immediately gives rise to an upper bound for the mass M:

LEMMA 2. $M \le \left(\frac{\pi e R^2}{n}\right)^{\frac{1}{2}n} \frac{1}{\sqrt{\pi n}} \left( \sum_{m=1}^{n} \frac{1}{m(m+1)} \left(\frac{m}{m+1}\right)^{\frac{1}{2}n} + \frac{1}{n+1} \right).$

PROOF. We denote the volume of the intersection of the n-dimensional hypersphere with radius r and center 0 in $\mathbb{R}^n$ and the n-dimensional hypercube $[0,1]^n$ by B(r). The volume of the n-dimensional unit sphere will be denoted by $J_n$. It is well known that

$$J_n = \frac{\pi^{\frac{1}{2}n}}{(\frac{1}{2}n)!} \le \frac{\pi^{\frac{1}{2}n} e^{\frac{1}{2}n}}{(\frac{1}{2}n)^{\frac{1}{2}n}\sqrt{\pi n}} = \left(\frac{2\pi e}{n}\right)^{\frac{1}{2}n} \frac{1}{\sqrt{\pi n}}.$$

Hence

$$M = \int_0^{R\sqrt{2}} \rho(r)\, dB(r) \le \int_0^{R\sqrt{2}} \sigma(r)\, dB(r) =$$

$$= -\int_0^{R\sqrt{2}} B(r)\, d\sigma(r) \le -\int_0^{R\sqrt{2}} 2^{-n} J_n r^n\, d\sigma(r) =$$

$$= 2^{-n} J_n \left( \sum_{m=2}^{n+1} \left(\frac{1}{m-1} - \frac{1}{m}\right) (Ry_m)^n + \frac{1}{n+1} (R\sqrt{2})^n \right) \le$$

$$\le \left(\frac{R}{2}\right)^n \left(\frac{2\pi e}{n}\right)^{\frac{1}{2}n} \frac{1}{\sqrt{\pi n}} \left( \sum_{m=2}^{n+1} \frac{1}{(m-1)m} \left(\frac{2(m-1)}{m}\right)^{\frac{1}{2}n} + \frac{2^{\frac{1}{2}n}}{n+1} \right) =$$

$$= \left(\frac{\pi e R^2}{n}\right)^{\frac{1}{2}n} \frac{1}{\sqrt{\pi n}} \left( \sum_{m=1}^{n} \frac{1}{m(m+1)} \left(\frac{m}{m+1}\right)^{\frac{1}{2}n} + \frac{1}{n+1} \right) . \quad \square$$

This leads to the lower bound for $A_w(n,d)$:

THEOREM. $$A_w(n,d) \geq \left\lfloor \left(\frac{4n}{\pi e d}\right)^{\frac{1}{2}n} \sqrt{\pi n} \left( \sum_{m=1}^{n} \frac{1}{m(m+1)} \left(\frac{m}{m+1}\right)^{\frac{1}{2}n} + \frac{1}{n+1} \right)^{-1} \right\rfloor .$$

PROOF. $R = \frac{1}{2}\sqrt{d}$ and $A_w(n,d) = \lfloor 1/M \rfloor$ for some density function $\rho$. $\square$

EXAMPLES.

| | |
|---|---|
| $A_w(8,3) \geq 45$ | $A_w(9,4) \geq 27$ |
| $A_w(9,3) \geq 101$ | $A_w(10,4) \geq 56$ |
| $A_w(10,3) \geq 238$ | $A_w(11,4) \geq 119$ |
| $A_w(11,3) \geq 579$ | $A_w(12,4) \geq 259$ |

REFERENCES


[1] BEST, M.R., A.E. BROUWER, F.J. MACWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes*, to be published.

[2] GOLAY, M.J.E., *Binary coding*, I.E.E.E. Transactions on Information Theory 4 (1954) 23-28.

[3] JULIN, D., *Two improved block codes*, I.E.E.E. Transactions on Information Theory 11 (1965) 459.

[4] RANKIN, R.A., *On the closest packing of spheres in* n *dimensions*, Annals of Math. 48 (1947) 1062-1081.

[5] ROGERS, C.A., *Packing and covering*, Cambridge 1964.

[6] WAX, N., *Upper bounds for error detecting and correcting codes*, I.R.E. Transactions on Information Theory 5 (1959) 168-174.