A bound of the size of codes

Eleonora Guerrini, Emanuele Bellini, Sala Massimiliano

A bound on the size of codes

Emanuele Bellini (eemanuele.bellini@gmail.com)
Department of Mathematics, University of Trento, Italy.

Eleonora Guerrini (guerrini@lirmm.fr)
LIRMM, Université de Montpellier 2, France.

Massimiliano Sala (maxsalacodes@gmail.com)
Department of Mathematics, University of Trento, Italy.

Abstract

We present one upper bound on the size of non-linear codes and its restriction to systematic codes and linear codes. This bound is independent of other known theoretical bounds, e.g. the Griesmer bound, the Johnson bound or the Plotkin bound, and it is an improvement of a bound by Litsyn and Laihonen. Our experiments show that in some cases (the majority of cases for some q) our bounds provide the best value, compared to all other theoretical bounds.

Keywords: Hamming distance, linear code, systematic code, non-linear code, upper bound.

1 Introduction

The problem of bounding the size of a code depends heavily on the code family that we are considering. In this paper we are interested in three types of codes: linear codes, systematic codes and non-linear codes. Referring to the subsequent section for rigorous definitions, with **linear codes** we mean linear subspaces of $(\mathbb{F}_q)^n$, while with **non-linear codes** we mean (following consolidated tradition) codes that are not necessarily linear. In this sense, a linear code is always a non-linear code, while a non-linear code may be a linear code, although it is unlikely. Systematic codes form a less-studied family of codes, whose definition is given in the next section. Modulo code equivalence all (non-zero) linear codes are systematic and all systematic codes are non-linear. In some sense, systematic codes stand in the middle between linear codes and non-linear codes. The size of a systematic code is directly comparable with that of a linear code, since it is a power of the size of $\mathbb{F}_q$.

In this paper we are interested only in **theoretical bounds**, that is, bounds on the size of a code that can be obtained by a closed-formula expression, although other algorithmic bounds exist (e.g. the Linear Programming bound [Del73]). The algebraic structure of linear codes would suggest the knowledge of a high number of bounds strictly for linear codes, and only a few bounds for the other case. Rather surprisingly, the academic literature reports only one bound for linear codes, the Griesmer bound ([Gri60]), no bounds for systematic codes and many bounds for non-linear codes. Among those, we recall: the Johnson bound ([Joh62],[Joh71],[HP03]), the Elias-Bassalygo bound ([Bas65],[HP03]), the Levenshtein bound ([Lev98]), the Hamming (Sphere Packing) bound and the Singleton bound ([PBH98]), and the Plotkin bound ([Plo60], [HP03]).
Since the Griesmer bound is specialized for linear codes, we would expect it to beat the other bounds, but even this does not happen, except in some cases. So we have an unexpected situation where the bounds holding for the more general case are numerous and beat bounds holding for the specialized case.

In this paper we present one (closed-formula) bound (Bound $\mathcal{A}$) for non-linear codes, which is an improvement of a bound by Litsyn and Laihonen in [LL98]. The crux of our improvement is a preliminary result presented in Section 3, while in Section 4 we are able to prove Bound $\mathcal{A}$. Then we restrict Bound $\mathcal{A}$ to the systematic/linear case and compare it with all the beforementioned bounds by computing their values for a large set of parameters (corresponding to about one week of computations with our computers). Our findings are in favour of Bound $\mathcal{A}$ and are reported in Section 5. For large values of q, our bound provides the best value in the majority of cases.
The only bound that we never beat is Plotkin's, but its range is very small (the distance has to be at least $d > n(1 - 1/q)$) and the cases falling in this range are a tiny portion with large q's.

For standard definitions and known bounds, the reader is directed to the original articles or to any recent good book, e.g. [HP03] or [PBH98].

2 Preliminaries

We first recall a few definitions.
Let $\mathbb{F}_q$ be the finite field with q elements, where q is any power of any prime. Let $n \geq k \geq 1$ be integers. Let $C \subseteq \mathbb{F}_q^n, C \neq \emptyset$. We say that C is an (n, q) **code**. Any $c \in C$ is a **word**. Note that here and afterwards a "code" denotes what is called a "non-linear code" in the introduction.
Let $\phi : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$ be an injective function and let $C = \mathrm{Im}(\phi)$. We say that C is an (n, k, q) **systematic code** if $\phi(v)_i = v_i$ for any $v \in (\mathbb{F}_q)^k$ and any $1 \leq i \leq k$. If C is a vector subspace of $(\mathbb{F}_q)^n$, then C is a **linear** code. Clearly any non-zero linear code is equivalent to a systematic code.
From now on $\mathbb{F}$ will denote $\mathbb{F}_q$ and q is understood.
We denote with $\mathrm{d}(c, c')$ the **(Hamming) distance** of two words $c, c' \in C$,

which is the number of different components between c and c'. We denote with d a number such that $1 \leq d \leq n$ to indicate the **distance of a code**, which is $d = \min_{c,c' \in C, c \neq c'} \{ \mathrm{d}(c, c') \}$. Note that a code with only one word has, by convention, distance equal to infinity. The whole $\mathbb{F}^n$ has distance 1, and $d = n$ in a systematic code is possible only if $k = 1$.
From now on, n, k are understood.

Definition 2.1. *Let l, $m \in \mathbb{N}$ such that $l \leq m$. In $\mathbb{F}^m$, we denote by $B_x(l, m)$ the set of vectors with distance from the word x less than or equal to l, and we call it the **ball** centered in x of radius l.*
For conciseness, $B(l, m)$ denotes the ball centered in the zero vector.

Obviously, $B(l, m)$ is the set of vectors of weight less than or equal to l and

$$|B(l, m)| \; = \; \sum_{j=0}^{l} \binom{m}{j} (q-1)^j.$$

We also note that any two balls having the same radius over the same field contain the same number of vectors.

Definition 2.2. *The number $A_q(n, d)$ denotes the maximum number of words in a code over $\mathbb{F}_q$ of length n and distance d.*

3 A first result for a special code family

The maximum number of words in an (n, d) code can be smaller than $A_q(n, d)$ if we have extra constraints on the weight of words. The following result is an example and it will be instrumental of the proof of Bound $\mathcal{A}$.

Theorem 3.1. *Let C be a (n, d)-code over $\mathbb{F}^n$. Let $\epsilon \geq 1$ be such that for any $c \in C$ we have $\mathrm{w}(c) \geq d + \epsilon$. Then*

$$|C| \leq A_q(n, d) - \frac{|B(\epsilon, n)|}{|B(d-1, n)|}$$

Proof. C belongs to the set of all codes with distance d and contained in $\mathbb{F}^n \setminus B_0(d + \epsilon - 1, n)$. Let D be any code of the largest size in this set, then

$$|C| \leq |D| \tag{1}$$

Clearly, any word c of D has weight $\mathrm{w}(c) \geq d + \epsilon$. Consider also $\bar{D}$, the largest code over $\mathbb{F}^n$ of distance d such that $D \subseteq \bar{D}$. By definition, the only words of $\bar{D}$ of weight greater than $d + \epsilon - 1$ are those of D, while all other words of $\bar{D}$ are confined to the ball $B_0(d + \epsilon - 1, n)$. Thus

$$|C| \leq |D| \leq |\bar{D}| \leq A_q(n, d) \tag{2}$$

and

$$\bar{D} \setminus D \subseteq B_0(d+\epsilon-1, n)$$

Let $\rho = d-1$ and $r = d+\epsilon-1$, so that $r-\rho = \epsilon$, and let $N = \bar{D} \cap B_0(r, n)$. We have:

$$D = \bar{D} \setminus N, \qquad |D| = |\bar{D}| - |N| \tag{3}$$

We are searching for a lower bound on $|N|$, in order to have an upper bound on $|D|$. We start with proving

$$B_0(r-\rho, n) \subseteq \bigcup_{x \in N} B_x(\rho, n) \tag{4}$$

Consider $y \in B_0(r-\rho, n)$. If for all $x \in N$ we have that $y \notin B_x(\rho, n)$, then y is a vector whose distance from N is at least $\rho+1$. Since $y \in B_0(r-\rho, n)$, also its distance from $\bar{D} \setminus N$ is at least $\rho+1$. Therefore, the distance of y from the whole $\bar{D}$ is at least $\rho+1 = d$ and so we can obtain a new code $\bar{D} \cup \{y\}$ containing D and with distance d, contradicting the fact that $|\bar{D}|$ is the largest size for such a code in $\mathbb{F}^n$. So, (4) must hold.

A direct consequence of (4) is

$$|N| \cdot |B_x(\rho, n)| \geq |B_0(r-\rho, n)|,$$

which gives

$$|N| \geq \frac{|B_0(r-\rho, n)|}{|B_x(\rho, n)|} = \frac{|B_0(\epsilon, n)|}{|B_x(d-1, n)|} \tag{5}$$

Using (1), (2), (3) and (5), we obtain the desired bound:

$$\begin{aligned} |C| \leq |D| &= |\bar{D}| - |\bar{D} \cap B_0(d+\epsilon-1, n)| \\ &\leq A_q(n, d) - \frac{|B_0(\epsilon, n)|}{|B_x(d-1, n)|} \end{aligned}$$

□

4 An improvement of the Litsyn-Laihonen bound

In 1998 Litsyn and Laihonen prove a bound for non-linear codes: Theorem 1 of [LL98], which we write with our notation as follows.

Theorem 4.1 (Litsyn-Laihonen bound)**.** *Let $t \in \mathbb{N}$ be such that $t \leq n-d$. Let $1 \leq d \leq n$, $d-2r \leq n-t$, $0 \leq r \leq t$ and $0 \leq r \leq \frac{1}{2}d$. Then*

$$A_q(n, d) \leq \frac{q^t}{|B(r, t)|} A_q(n-t, d-2r)$$

We are ready to show a strengthening of their result: Bound $\mathcal{A}$.

Theorem 4.2 (Bound $\mathcal{A}$)**.** *Let $t \in \mathbb{N}$ be such that $t \leq n-d$. Let $1 \leq d \leq n$, $d-2r \leq n-t$, $0 \leq r \leq t$ and $0 \leq r \leq \frac{1}{2}d$. Then*

$$A_q(n,d) \leq \frac{q^t}{|B(r,t)|}\left(A_q(n-t,d-2r) - \frac{|B(r,n-t)|}{|B(d-2r-1,n-t)|}+1\right)$$

Proof. We follow initially the outline of the proof of [LL98][Theorem 1] and then we apply Theorem 3.1.
We consider an (n,d) code C such that $|C| = A_q(n,d)$. By definition of $A_q(n,d)$, C must exist. We claim that we can suppose $0 \in C$. Indeed, if $0 \notin C$, let c_0 be a word of C. Then the set $C_0 = \{c - c_0 \mid c \in C\}$ is a (n,d)-code containing the zero vector and with $|C_0| = |C|$.
We number all words in C in any order: $C = \{c_i \mid 1 \leq\ i \leq A_q(n,d)\}$.
We indicate the i-th word with $c_i = (c_{i,1}, \ldots, c_{i,n})$. We puncture C as follows:

(i) we choose any t columns $1 \leq j_1, \ldots, j_t \leq n$; since two codes are equivalent w.r.t. column permutations we suppose $j_1 = 1, \ldots, j_t = t$.
Let us split each word $c_i \in C$ in two parts

$$\tilde{c_i} = (c_{i,1}, \ldots, c_{i,t}) \quad \bar{c_i} = (c_{i,t+1}, \ldots, c_{i,n}), \qquad \text{so} \quad c_i = (\tilde{c_i}, \bar{c_i}).$$

(ii) We choose a $z \in \mathbb{F}^t$.

(iii) We collect in I all i's s.t. $d(z, \tilde{c_i}) \leq r$;

(iv) We delete the first t components of $\{c_i \mid i \in I\}$.

Then the punctured $(\bar{n}, \bar{d})$ code $\bar{C}_z$ obtained by (i),(ii),(iii) and (iv) is:

$$\bar{C}_z = \{\bar{c_i} \mid i \in I\} = \{\bar{c_i} \mid d(z, \tilde{c_i}) \leq r, 1 \leq i \leq A_q(n,d)\}$$

We claim that we can choose z in such a way that $\bar{C}_z$ satisfies:

$$\bar{n} = n - t \tag{6}$$
$$\bar{d} \geq d - 2r \tag{7}$$
$$|\bar{C}_z| \geq \frac{|C|}{q^t}|B(r,t)| \tag{8}$$
$$\mathrm{w}(\bar{c_i}) \geq d - r \text{ for all } \bar{c_i} \neq 0 \tag{9}$$

(6) is obvious. As regards (7), note that $\mathrm{d}(c_i, c_j) = \mathrm{d}(\tilde{c_i}, \tilde{c_j}) + \mathrm{d}(\bar{c_i}, \bar{c_j}) \geq d$ and also that $\tilde{c_i}, \tilde{c_j} \in B_z(r,t)$ implies $\mathrm{d}(\tilde{c_i}, \tilde{c_j}) \leq 2r$. Therefore for any $i \neq j$

$$2r + \mathrm{d}(\bar{c_i}, \bar{c_j}) \geq \mathrm{d}(\tilde{c_i}, \tilde{c_j}) + \mathrm{d}(\bar{c_i}, \bar{c_j}) \geq d\,.$$

The proof of (8) is more involved and we need to consider the average number M of the i's such that $\tilde{c_i}$ happens to be in a sphere of radius r (in $\mathbb{F}^t$). The

average is taken over all vectors x's in $\mathbb{F}^t$, so that

$$M = \frac{1}{|\mathbb{F}^t|} \sum_{x \in \mathbb{F}^t} |\{i \mid 1 \leq i \leq A_q(n,d), \tilde{c_i} \in B_x(r,t)\}| \,.$$

Let us define a function:

$$\psi : \mathbb{F}^t \times \mathbb{F}^t \longrightarrow \{0,1\}, \qquad \psi(x,y) = \begin{cases} 1, \ \mathrm{d}(x,y) \leq r \\ 0, \text{ otherwise} \end{cases} .$$

Then we can write M and $|B_y(r,t)|$ (for any $y \in \mathbb{F}^t$) as

$$M = \frac{1}{q^t} \sum_{x \in \mathbb{F}^t} \sum_{i=1}^{A_q(n,d)} \psi(x, \tilde{c_i}) \qquad |B_y(r,t)| = \sum_{x \in \mathbb{F}^t} \psi(x,y) \,.$$

By swapping variables we get

$$M = \frac{1}{q^t} \sum_{x \in \mathbb{F}^t} \sum_{i=1}^{A_q(n,d)} \psi(x, \tilde{c_i}) = \frac{1}{q^t} \sum_{i=1}^{A_q(n,d)} \sum_{x \in \mathbb{F}^t} \psi(x, \tilde{c_i}) = \frac{A_q(n,d)}{q^t} |B_{\tilde{c_i}}(r,t)| \,.$$

This means that there exists $\bar{x} \in \mathbb{F}^t$ such that

$$|\{i \mid 1 \leq i \leq A_q(n,d), \tilde{c_i} \in B_{\bar{x}}(r,t)\}| \geq M \geq \frac{A_q(n,d)}{q^t} |B(r,t)| \,.$$

In other words, there are at least $\frac{|C|}{q^t}|B(r,t)|$ c_i's such that their $\tilde{c_i}$'s are contained in $B_x(r,t)$. Distinct c_i's may well give rise to the same $\tilde{c_i}$'s, but they always correspond to distinct $\bar{c_i}$'s (see the proof of (7)), so there are at least $\frac{|C|}{q^t}|B_x(r,t)|$ (distinct) $\bar{c_i}$'s such that their corresponding $\tilde{c_i}$'s fall in $B_{\bar{x}}(r,t)$. By choosing $z = \bar{x}$ we then have at least $\frac{|C|}{q^t}|B_x(r,t)|$ (distinct) codewords of $\bar{C}_z$.

(9) holds since $0 \in C$. Infact:

$$\mathrm{w}(c) = \mathrm{d}(0,c) \geq d, \quad \forall c \in C \text{ such that } c \neq 0.$$

As a consequence, any nonzero word $c_i = (\tilde{c_i}, \bar{c_i})$ of weight at most r in c has weight at least $d - r$ in the other $n - t$ components.

Now, if we call D a $(\bar{n}, M, d-2r)$-code containing the zero word and such that $\forall d \in D$ then $\mathrm{w}(d) \leq r$. Then we can apply Theorem 3.1 to $D \setminus \{0\}$ and $\epsilon = r$, and obtain the following chain of inequalities:

$$\frac{|C|}{q^t}|B(r,t)| \leq |\bar{C}| \leq |D| \leq A_q(\bar{n}, d-2r) - \frac{|B(r,\bar{n})|}{|B(d-2r-1,\bar{n})|} + 1$$

and since $|C| = A_q(n,d)$ we have the bound:

$$A_q(n,d) \leq \frac{q^t}{|B(r,t)|}(A_q(\bar{n}, d-2r) - \frac{|B(r,\bar{n})|}{|B(d-2r-1,\bar{n})|} + 1).$$

□

4.1 Systematic case

When we restrict ourselves into the systematic/linear case, then the value $A_q(n,d)$ can only be a power of q, and if the dimension of the code C is k, then $A_q(n,d) = q^k$. Thus we have the following corollary:

Corollary 4.3 (Bound $\mathcal{B}$)**.** *Let $k, d, r \in \mathbb{N}, d \geq 2, k \geq 1$. Let n be such that there exists an (n,k,q) systematic code C with distance at least d.*
If $0 \leq r \leq \min\{\lfloor \frac{d-1}{2} \rfloor, k\}$, then

$$|B(r,k)| \leq A_q(n-k, d-2r) - \frac{|B(r,n-k)|}{|B(d-2r-1,n-k)|} + 1.$$

In the systematic/linear case the Litsyn-Laihonen bound becomes:

$$|B(r,k)| \leq A_q(n-k, d-2r).$$

Easy computations can be done in the case $d = 3$, since in this case r can be at most 1, so that:

- $|B(1,k)| = (q-1)k + 1$
- $A_q(n-k.d-2r) = A_q(n-k,1) = q^{n-k}$
- $|B(1,n-k)| = (q-1)(n-k) + 1$
- $|B(d-2r-1,n-k)| = |B(0,n-k)| = 1$

Our bound then reduces to:

$$0 \leq q^{n-k} - (q-1)n - 1$$

which is stronger then the Litsyn-Laihonen bound, which in the case $d = 3$ reduces to:

$$0 \leq q^{n-k} - (q-1)k - 1.$$

5 Experimental comparisons with other upper bounds, remarks and conclusion

We have analyzed the case of linear codes, implementing Bound $\mathcal{B}$. The algorithm to compute the bound takes as inputs n, d, and returns the largest k (checks are done until $k = n - d + 1$) such that the inequality of the bound

holds. If the inequality always holds in this range, $n-d+1$ is returned. Then we compared our upper bound on k with other bounds, restricting those which hold in the general non-linear case to the systematic case. In particular they give a bound on $A_q(n,d)$ instead of a bound on k. As a consequence, for example, if the Johnson bound returns the value $A_q(n,d)$ for a certain pair (n,d), then we compare our bound with the value $\lfloor \log_q(A_q(n,d)) \rfloor$, which is the largest power s of q such that $q^s \leq A_q(n,d)$.
The inequality in Theorem 4.3 involves the value $A_q(n-k, d-2r)$, which is the maximum number of words that we can have in a *non-linear* code of length $n-k$ and distance $d-2r$. To implement Bound $\mathcal{B}$ it is necessary to compute $A_q(n-k, d-2r)$; when this value is unknown (we use known values only in the binary case for $n = 3, \ldots, 28, d = 3, \ldots, 16$), we return instead an upper bound on it, choosing the best between the Hamming (Sphere Packing), Singleton, Johnson, and Elias bound (the Plotkin bound is used when possible). Even though it is a very strong bound, we do not use the Levenshtein bound because it is very slow as n grows. This means that if better values of $A_q(n-k, d-2r)$ can be found, then Bound $\mathcal{B}$ could return even tighter results.

Table 1 and 2 show a comparison between all bounds' performances, except for Plotkin's, due to its restricted range. For each bound and for each $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29$ we have computed, in the range $n = 3, \ldots, 100$ and $d = 3, \ldots, n-1$, the percentage of cases the bound is the "best" known bound between Bound $\mathcal{B}$, the Griesmer, Johnson, Levenshtein, Elias, Hamming and Singleton bound. Both wins and draws are counted in the percentage, since more than one bound may reach the best known bound, and in this case we increased the percentage of each best bound. For each q the most performing bound is in bold. Up to $q = 7$ the Levenshtein bound is the most performing. From $9 \leq q \leq 29$ we have that Bound $\mathcal{B}$ is the most performing bound, and in particular, in the case $q = 29$, it is the best known bound almost 91% of the times.

Table 3, instead, shows some cases (one per each $q = 7, \ldots, 29$) where Bound $\mathcal{B}$ beats all other known bounds. This happens from $q = 7$, for the range of n considered. The letters B, J, H, G, E, S and L stands respectively for Bound $\mathcal{B}$, Johnson, Hamming (Sphere Packing), Griesmer, Elias, Singleton, and Levenshtein bound. It can be seen that there are some cases where Bound $\mathcal{B}$ is tight, as for the parameters $(9, 17, 7)$, for which there exist a code with distance 10.

Tables 4, and 5 give emphasis to the number of times Bound $\mathcal{B}$ improves the best known bound (thus the cases where it beats all other bounds). In the considered range Bound $\mathcal{B}$ starts to beat all other bounds from $q = 7$.
The third row of Tables 4 and 5 shows how many times (percentage over the number of draws and wins) the value $\delta = \frac{|B(r,n-k)|}{|B(d-2r-1,n-k)|}$ is different from zero.

Informally, we can view δ as the probability to randomly pick up a word of weight less than r from a ball of radius $d - 2r - 1$. We can notice that this percentage is very high, which means that a weaker version of Bound $\mathcal{B}$, which is similar to the Litsyn-Laihonen bound for systematic codes, could be used, by simply searching the largest k satisfying:

$$|B(r,k)| \leq A_q(n-k, d-2r) + 1$$

It is curious to notice that in all the wins we have $\delta = 0$, and that $\delta = 0$ also 38094 times over the 46967 ties and wins. This means that the weaker version of Bound $\mathcal{B}$ is sufficient to obtain most of the wins and ties in the investigated cases.
We note that in general, if r is greater than d, we expect δ big, decreasing very quickly as r increases, holding d fixed; this happens since $|B(x,k)|$ decreases following a gaussian distribution (roughly approximating $|B(x,k)|$ with a factorial), and so any time we subtract $2r$ the decrease is doubled.
The fourth row of Tables 4 and 5 shows the ratio between the number of times the Plotkin bound has been used to bound $A_q(n-k, d-2r)$ and the number of draws and wins. Third and fourth row show values which are close for q small and gets further as q grows. This happens because almost all the times that the weaker version (with $\delta = 0$) of Bound $\mathcal{B}$ ties with the best known bound, a strong bound on $A_q(n-k, d-2r)$ must be used, and the strongest bound is Plotkin's, which though has a smaller range of applicability as q grows.
We report in the fifth row of Tables 4 and 5 the fact that the maximum ratio d/n reached in the wins of Bound $\mathcal{B}$ grows up to the value 0.64 and then seems to get stabilized toward 0.5. This means that Bound $\mathcal{B}$ is a very strong bound for distances which are no more than $\frac{2}{3}$ of the length n for small values of q, and no more than half of the length n for bigger values of q.

Comparisons have been made using inner MAGMA ([MAG]) implementations of known upper bounds, except for the Johnson bound. For this bound we noted that the inner MAGMA implementation could be improved and so we used our own MAGMA implementation for this bound.

Acknowledgements

The first two authors would like to thank the third author (their supervisor). Partial results appear in [Gue09]. The authors would like to thank: Ludo Tolhuizen (Philips Group Innovation, Research), the MAGMA group and in particular John Cannon.

References

[Bas65] L.A. Bassalygo, *New upper bounds for error correcting codes*, Problemy Peredachi Informatsii **1** (1965), no. 4, 41–44.

[Del73] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. (1973), no. 10, vi+97.

[Gri60] J.H. Griesmer, *A bound for error-correcting codes*, IBM Journal of Research and Development **4** (1960), no. 5, 532–542.

[Gue09] Eleonora Guerrini, *Systematic codes and polynomial ideals*, Ph.D. thesis, University of Trento, 2009.

[HP03] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[Joh62] S. Johnson, *A new upper bound for error-correcting codes*, Information Theory, IRE Transactions on **8** (1962), no. 3, 203–207.

[Joh71] ———, *On upper bounds for unrestricted binary-error-correcting codes*, Information Theory, IEEE Transactions on **17** (1971), no. 4, 466–478.

[Lev98] V.I. Levenshtein, *Universal bounds for codes and designs*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. 1, Elsevier, 1998, pp. 499–648.

[LL98] T. Laihonen and S. Litsyn, *On upper bounds for minimum distance and covering radius of non-binary codes*, Designs, Codes and Cryptography **14** (1998), no. 1, 71–80.

[MAG] *MAGMA: Computational Algebra System for Algebra, Number Theory and Geometry*, The University of Sydney Computational Algebra Group., http://magma.maths.usyd.edu.au/magma.

[PBH98] V. Pless, R.A. Brualdi, and W.C. Huffman, *Handbook of coding theory*, Elsevier Science Inc., 1998.

[Plo60] M. Plotkin, *Binary codes with specified minimum distance*, Information Theory, IRE Transactions on **6** (1960), no. 4, 445–450.

The following tables show the results computed in the range $n = 3, \ldots, 100$, $d = 3, \ldots, n-1$.

q	2	3	4	5	7	8	9	11
Bound $\mathcal{B}$	38.02	31.20	31.20	31.94	40.73	48.64	**55.27**	**66.44**
Johnson	40.65	31.18	33.50	35.13	35.70	35.51	35.09	33.26
Hamming	18.12	15.65	16.37	16.35	16.03	15.88	15.57	14.69
Griesmer	56.32	39.83	32.32	29.14	30.91	36.97	43.28	55.15
Levenshtein	**72.65**	**69.68**	**66.27**	**64.02**	**60.80**	**58.24**	54.47	46.26
Elias	6.859	32.28	38.27	40.02	40.82	40.14	37.24	31.37
Singleton	0.000	0.021	0.084	0.189	0.610	0.926	1.241	3.619

Table 1
When each bound is the best for $2 \leq q \leq 11$.

q	13	16	17	19	23	25	27	29
Bound $\mathcal{B}$	**76.43**	**81.61**	**82.75**	**85.42**	**88.11**	**88.72**	**89.40**	**90.77**
Johnson	30.80	26.61	24.87	21.88	17.08	15.51	14.37	13.34
Hamming	13.59	11.91	11.26	10.12	8.269	7.553	7.048	6.606
Griesmer	63.39	71.91	72.27	71.94	69.79	69.43	68.65	67.87
Levenshtein	39.93	32.86	30.65	27.50	22.62	20.70	19.44	18.37
Elias	27.06	21.84	20.01	17.59	12.48	10.84	9.657	8.689
Singleton	4.439	4.629	6.985	6.712	10.08	12.01	14.12	18.01

Table 2
When each bound is the best for $13 \leq q \leq 29$.

q	n	d	B	J	H	G	E	S	L
7	45	21	**22**	23	24	23	23	25	23
8	51	24	**25**	27	28	26	26	28	26
9	17	7	**10**	11	11	11	11	11	11
11	90	55	**30**	41	42	32	35	36	31
13	32	9	**23**	24	24	24	24	24	25
16	52	14	**38**	39	40	39	39	39	41
17	38	9	**29**	30	30	30	30	30	31
19	42	9	**33**	34	34	34	34	34	36
23	91	17	**74**	75	75	75	75	75	78
25	31	5	**26**	27	27	27	27	27	28
27	88	24	**64**	66	67	65	66	65	69
29	100	29	**71**	74	74	72	74	72	76

Table 3
Some cases where Bound $\mathcal{B}$ beats all the other bounds in the range $7 \leq q \leq 29$.

q	2	3	4	5	7	8	9	11
Draws(D) (%)	38.02	31.20	31.20	31.94	40.54	47.59	53.44	64.80
Wins(W) (%)	0	0	0	0	0.1894	1.052	1.830	3.955
$\delta = 0$ (% over D+W)	44.67	71.14	61.77	59.82	68.75	74.22	79.71	85.43
Use of Plotkin (% over D+W)	41.50	69.52	56.84	51.98	57.02	61.16	65.09	68.57
Maximum d/n in wins	-	-	-	-	0.47	0.48	0.52	0.63
Plotkin Range d/n	0.50	0.67	0.75	0.80	0.87	0.88	0.89	0.91

Table 4
Statistics for Bound $\mathcal{B}$ for $2 \leq q \leq 11$.

q	13	16	17	19	23	25	27	29
Draws(D) (%)	73.11	77.41	78.48	77.84	73.43	71.18	69.60	69.60
Wins(W) (%)	3.514	4.208	5.113	7.574	14.69	17.55	19.80	21.19
$\delta = 0$ (% over D+W)	87.96	88.45	88.49	88.28	85.00	83.02	80.89	78.62
Use of Plotkin (% over D+W)	65.54	67.00	66.09	61.80	55.16	51.98	48.98	46.54
Maximum d/n in wins	0.634	0.640	0.486	0.487	0.489	0.490	0.491	0.492
Plotkin Range d/n	0.92	0.94	0.94	0.95	0.96	0.96	0.96	0.97

Table 5
Statistics for Bound $\mathcal{B}$ for $13 \leq q \leq 29$.