Unconditional Proof of Tightness of Johnson Bound

Venkatesan Guruswami* Igor Shparlinski†

1 Introduction

This paper continues the investigation of the relation between the *relative distance* and the *list decoding radius* of a binary **linear** code. This line of research has been pursued recently in [2, 1]. The motivation comes in part because the Johnson bound is a classical bound in coding theory and therefore it is important to understand if it can be improved for linear codes, and also because the Johnson bound, though a purely combinatorial result, also fueled a lot of the recent work on efficient list decoding algorithms (by highlighting how many errors one could hope to list decode with polynomial-sized lists) — see [1] for a detailed discussion.

As usual, we denote by $\mathbb{F}_q$ a finite field of q elements, and recall that an $[n, k]$ binary linear code is a k-dimensional subspace of $\mathbb{F}_2^n$; elements in the subspace are referred to as codewords, n is called the block length and k its dimension. Its relative distance is the largest value of δ for which every pair of codewords differ in at least δn coordinates, and the list decoding radius is the largest value of e for which every Hamming ball of radius en has at most a polynomial in n number of codewords.[1]

The list decoding radius as a function of the relative distance is denoted by the function L^{poly} in [2, 1] and the Johnson bound (for binary codes) can be rephrased as the statement $L^{\mathrm{poly}}(\delta) \geq J(\delta) \stackrel{\mathrm{def}}{=} \frac{1}{2} \cdot \left(1 - \sqrt{1-2\delta}\right)$. Guruswami [1], building upon earlier work of [2], showed that this relation is tight and that $L^{\mathrm{poly}}(\delta) = J(\delta)$ assuming a widely believed number theoretic conjecture. If one includes also non-linear codes in the discussion, then it is well-known that $L^{\mathrm{poly}}(\delta) = J(\delta)$, see [3].

In this work, we prove a slightly weaker bound on $L^{\mathrm{poly}}(\delta)$ *without making any number-theoretic assumption.* Our result shows that $L^{\mathrm{poly}}(\delta) \leq J(\delta) + \gamma_0$ for a very small absolute constant γ_0. The larger the value of a prime with a certain property that one can find, the better the bound on γ_0. In particular, if infinitely many primes with the property we need exist (a fact which is unproven), then we have $L^{\mathrm{poly}}(\delta) = J(\delta)$. We note that proving an upper bound, say $U(\delta)$, on $L^{\mathrm{poly}}(\delta)$ amounts to constructing a binary linear code family with relative distance δ that has a super-polynomial (in block length) number of codewords in a Hamming ball of (relative) radius $U(\delta)$. The requirement of linearity makes the task of constructing such codes quite tricky.

We stress that our unconditional result does not follow from the approach taken in [1] as the block length of the code constructed there was tied to the size of certain kinds of prime numbers, and thus one *cannot* deduce a result similar to ours that holds for an infinite family of codes without a guarantee of the infinititude of such primes. In contrast, we construct a family of codes whose block lengths are related to powers of a fixed prime p (and thus are able to get infinitely many codes using a single prime), and the larger the p the better the upper bound on $L^{\mathrm{poly}}(\delta)$ that we get. Since primes of the form we need that are bigger than 10^{50} exist, we get a near-tight upper bound on $L^{\mathrm{poly}}(\delta)$.

2 Main Results

Let us define a prime p to be 2-*good* if 2 is a *primitive root modulo* p (i.e., $2^{p-1} \equiv 1 \pmod p$ but $2^a \not\equiv 1 \pmod p$ for any $a < p-1$), and p is not a *Wieferich prime* (i.e., $2^{p-1} \not\equiv 1 \pmod{p^2}$). It is well known that this requirement is equivalent to saying that 2 is a primitive root modulo p^s for *every* $s \geq 1$. With any 2-good prime at our disposal, we can prove:

THEOREM 2.1. *Let p be a 2-good prime. Then, for every δ, $0 < \delta < 1/2$ and $\varepsilon > 0$, there exists infinitely many N for which there exists a binary linear code of block length N and relative distance at least δ that has at least $N^{\Omega(\varepsilon \log\log\log N)}$ codewords in a Hamming ball of radius* $\frac{N}{2}\frac{p-1}{p}\left(1 - \sqrt{1-2\delta-\varepsilon}\right) + \frac{N}{p}$.

Letting $\varepsilon \to 0$ and using the fact that there exist 2-good primes which are larger than 10^{50} (e.g., $10^{50} + 709$ is one such prime[2]), we have our main result:

*Department of Computer Science, University of Washington, Seattle, WA 98195, USA; venkat@cs.washington.edu. Work done while a Miller Research Fellow at UC Berkeley.

†Deptartment of Computing, Macquarie University, North Ryde, NSW 2109, Australia; igor@aomp.mq.edu.au.

[1] Of course for the latter definition to make sense we need a family of codes, and we will always implicitly be interested in infinite families of codes of increasing block lengths.

[2] We stopped at a very modest size of 10^{50} for the size of 2-good primes; we can easily push it much higher.

THEOREM 2.2. *For every δ, $0 < \delta < 1/2$, we have* $L^{\text{poly}}(\delta) \le J(\delta) + 10^{-50}$.

3 Technical Tools

Our starting point is the following lemma which is Lemma 7 in [1] and which essentially shows that one can any desired constant number of codewords in a Hamming ball of radius close to the Johnson bound.

LEMMA 3.1. *For every $\varepsilon > 0$, the following holds. For all large enough integers k and every δ, $0 < \delta < 1/2$, there exist an integer $b = 2^{O(2^k)}$, and a binary linear code $C^{\text{bin}}_{k,\delta}$ that has the following properties:*

(i) It has dimension kb, block length $n \le 2^{O(k\sqrt{b})}$, and relative distance δ.

(ii) There exists a Hamming ball of radius $\frac{n}{2}(1 - \sqrt{1-2\delta-\varepsilon})$ which contains at least 2^k codewords of $C^{\text{bin}}_{k,\delta}$.

The main algebraic fact used in our proof is:

LEMMA 3.2. *Let p be a 2-good prime and let $s \ge 1$ be any integer. Let α be a primitive p^s'th root of unity over $\mathbb{F}_2$ in the field $\mathbb{F}_q$ with $q = 2^{(p-1)p^{s-1}}$ (such a root must exist since p^s divides $2^{(p-1)p^{s-1}} - 1$ by Euler's theorem). Then the $(p-1)p^{s-1}$ elements $S = \{\alpha^i : 0 \le i < (p-1)p^{s-1}\}$ are linearly independent over $\mathbb{F}_2$.*[3]

4 Proof of Theorem 2.1

The basic approach is to use an outer Reed-Solomon code over a finite field $\mathbb{F} = \mathbb{F}_{2^l}$ where $l = (p-1)p^{s-1}$ for a 2-good prime p and integer $s \ge 1$, and concatenate it with a tailor-made inner code C_{in}, whose construction we outline below. The inner code will have the following property. Let α be a primitive p^s'th root of unity in $\mathbb{F}_{2^l}$. Then $S' = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^s-1}\}$ is the multiplicative subgroup of $\mathbb{F}^*$ consisting of the r'th powers where $r = \frac{2^{(p-1)p^{s-1}}-1}{p^s}$. Now, if the inner code had the property that all elements in S were mapped into some small Hamming ball $\mathbf{B}$ centered around $\mathbf{v}$ (of radius close to the Johnson bound), then all codewords of the concatenated code that correspond to evaluations of polynomials that are perfect r'th powers get mapped into a small Hamming ball (around $\mathbf{w} = \mathbf{v} \circ \cdots \circ \mathbf{v}$, the 2^l-fold concatenation of $\mathbf{v}$). If parameters could be picked so that there are a super-polynomial number of such r'th powers, we will have the desired construction.

Let C be the code guaranteed by Lemma 3.1, with a suitable choice of k in relation to the size of S'. But now this inner code is only guaranteed to map *some* 2^k messages into a small Hamming ball, and these 2^k messages need not have anything to do with the elements of S under consideration. However, here comes the crucial idea, which was also used in [1] earlier. These 2^k messages (viewed as vectors over $\mathbb{F}_2$ of suitable length) must contain a linearly independent subset T of size k. Now, if the elements of $S' \subseteq \mathbb{F}_{2^l}$ are linearly independent over $\mathbb{F}_2$, then there must exist a invertible $\mathbb{F}_2$-linear map F which maps elements of S' into those of T (in so me arbitrary ordering of the elements of S', T). We can let the inner code C_{in} to be $C \circ F$ (in other words, the encoding under C_{in} first encodes the message by the invertible map F, and then encodes the resulting string using C). Note that since F, C are linear codes, so is C_{in}. Now C'_{in} will map all elements of S' into a small Hamming ball, since C does so for elements of T.

However, the elements in S' cannot be assumed to be linearly independent, but if p is 2-good, then we know by Lemma 3.2 that it has a large subset $S = \{\alpha^i : 0 \le i < (p-1)p^{s-1}\}$ that is linearly independent. For the r'th power of a random polynomial, we can expect its evaluation at $\gamma \in \mathbb{F}_{2^l}$ to land in S for a fraction $(p-1)/p$ of the field elements γ. For all these positions, the inner encoding will further map the evaluation into the ball $\mathbf{B}$. The overall (normalized) distance from $\mathbf{w}$ will be roughly the Johnson radius plus $1/p$ (corresponding to the evaluations which may not land in S). After a suitable choice of parameters, we will thus be able to get a super-polynomial number of codewords of the concatenated code all of which lie in a Hamming ball of radius roughly $1/p$ more than the Johnson bound.

We note that [1] used Lemma 3.2 for the case $s = 1$ and assumed infinitely many such primes p existed. In this case, the slack of $1/p$ in the above argument disappears as one can pick larger and larger primes and get as close to the Johnson bound as one desires. The contribution here is in realizing that one can get an infinite family of codes using just a fixed (large) prime p, but the upper bound has a slack of $1/p$.

Acknowledgment. We thank Paul Zimmermann for his help with computation, for example, for finding the prime we use in the proof of Theorem 2.1.

References

[1] V. Guruswami. Limits to list decodability of linear codes. *Proc. of 34th STOC*, 2002, pp. 802–811.

[2] V. Guruswami, J. Håstad, M. Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. *IEEE Trans. on Inform. Theory*, **48** (2002), pp. 1021–1034.

[3] O. Goldreich, R. Rubinfeld, and M. Sudan. Learning polynomials with queries: The highly noisy case. *Proc. of 36th FOCS*, 1995, pp. 294–303.

[3] The fact that elements of S are linearly independent over $\mathbb{F}_2$ is independent of the specific representation of $\mathbb{F}_{2^l}$ over $\mathbb{F}_2$, since this fact only depends on the additive properties of S.