An Improved Sphere-Packing Bound for Finite-Length Codes over Symmetric Memoryless Channels

Gil Wiechman Igal Sason
Department of Electrical Engineering
Technion, Haifa 32000, Israel
{igillw@tx,sason@ee}.technion.ac.il

***Abstract*— We present an improved sphere-packing (ISP) bound for finite-length error-correcting codes whose transmission takes place over symmetric memoryless channels, and the codes are decoded by an arbitrary list decoder. Some applications of the ISP bound are also exemplified. Its tightness under maximum-likelihood (ML) decoding is studied by comparing the ISP bound to previously reported upper and lower bounds on the ML decoding error probability, and also to computer simulations of iteratively decoded turbo-like codes.**

I. Introduction

The 1967 sphere-packing (SP67) bound, derived by Shannon, Gallager and Berlekamp [8], provides a lower bound on the decoding error probability of block codes as a function of their block length and code rate, and applies to arbitrary discrete memoryless channels (DMCs). Like the random-coding bound (RCB) of Gallager [3], the SP67 bound decays to zero exponentially with the block length for all rates below the channel capacity. Further, the error exponent of the SP67 bound is known to be tight at the portion of the rate region between the critical rate ($R_{\rm c}$) and the channel capacity; for all the rates in this range, the error exponents of the SP67 bound and RCB coincide (see [8, Part 1]).

In spite of the exponential decay of the SP67 bound in terms of the block length at all rates below the channel capacity, this bound appears to be loose for codes of small to moderate block lengths. The weakness of this bound is due to the original focus in [8] on asymptotic analysis. In [11], Valembois and Fossorier revisit the SP67 bound in order to improve its tightness for finite-length block codes (especially, for codes of short to moderate block lengths), and also extend its validity to memoryless continuous-output channels (e.g., the binary-input AWGN channel). The remarkable improvement of their bound over the classical SP67 bound is exemplified in [11]. Moreover, the extension of the bound in [11] to memoryless continuous-output channels provides an alternative to the 1959 sphere-packing (SP59) bound of Shannon [7] which solely applies to the AWGN channel [7].

In this work, we present an improved sphere-packing bound (referred to as the 'ISP bound') which tightens the bounds in [8] and [11], especially for codes of short to moderate block lengths. This new bound is valid for all symmetric memoryless channels. The structure of this paper is as follows: Section II briefly reviews the SP67 bound [8, Part 1] and its improved version in [11]. In Section III, we present the ISP bound which improves the bound in [11] for symmetric memoryless channels. Section IV provides numerical results which serve to compare the ISP bound to previously reported upper and lower bounds on the error probability. Additionally, sphere-packing bounds are applied in Section IV to study the tradeoff between the performance and the required block length of error-correcting codes. We conclude our discussion in Section V. Due to space limitations, proofs are omitted. We refer the interested reader to the full paper version [12], which provides full proofs, as well as numerous remarks, discussions, and numerical results.

II. The 1967 Sphere-Packing Bound and Improvements

In the following, we present the SP67 bound and its improvement in [11]. Classical sphere-packing bounds are reviewed in [6, Chapter 5]. This section serves as a preliminary step towards the presentation of an improved sphere-packing bound in the next section.

A. The 1967 Sphere-Packing Bound

Consider a block code $\mathcal{C}$ which consists of M codewords each of length N. Assume that $\mathcal{C}$ is transmitted over a DMC and decoded by a *list decoder*; for each received sequence, the decoder outputs a list of at most L integers from the set $\{1, 2, \ldots, M\}$ which correspond to the indices of the codewords. A list decoding error occurs if the index of the transmitted codeword does not appear in the list. The SP67 bound [8] forms a lower bound on the decoding error probability of an arbitrary block code with M codewords of length N. This bound applies to an arbitrary list decoder where the size of the list is limited to L. The particular case where $L = 1$ clearly provides a lower bound on the error probability under maximum-likelihood (ML) decoding. The SP67 bound is given in the following theorem:

Theorem 2.1: **[The 1967 Sphere-Packing Bound for Discrete Memoryless Channels]** [8, Theorem 2]. Let $\mathcal{C}$ be an arbitrary block code whose transmission takes place over a DMC. Assume that the DMC is specified by the set of transition probabilities $P(j|k)$ where $k \in \{0, \ldots, K-1\}$ and $j \in \{0, \ldots, J-1\}$ designate the channel input and output alphabets, respectively. Assume that the code $\mathcal{C}$ forms a set of M codewords of length N (i.e., each codeword is a sequence of N letters from the input alphabet), and consider an arbitrary

list decoder where the size of the list is limited to L. Then, the *average decoding error probability* of the code $\mathcal{C}$ satisfies

$$P_{\mathrm{e}}(N,M,L) \geq \exp\left\{-N\left[E_{\mathrm{sp}}\left(R\text{–}O_1\Big(\frac{\ln N}{N}\Big)\right)+O_2\Big(\frac{1}{\sqrt{N}}\Big)\right]\right\}$$

where $R \triangleq \frac{\ln\left(\frac{M}{L}\right)}{N}$ is the rate of the code, and the error exponent $E_{\mathrm{sp}}(R)$ is given by

$$E_{\mathrm{sp}}(R) \triangleq \sup_{\rho\geq 0}\big(E_0(\rho)-\rho R\big) \tag{1}$$

$$E_0(\rho) \triangleq \max_{\mathbf{q}}\left\{-\ln\left(\sum_{j=0}^{J-1}\Big[\sum_{k=0}^{K-1} q_k P(j|k)^{\frac{1}{1+\rho}}\Big]^{1+\rho}\right)\right\} \tag{2}$$

where the maximum on the RHS of (2) is taken over all probability vectors $\mathbf{q}=(q_0,\ldots,q_{K-1})$, i.e., the maximization is over all the vectors $\mathbf{q}$ whose K components are non-negative and their sum is 1. The terms

$$\begin{aligned} O_1\Big(\frac{\ln N}{N}\Big) &= \frac{\ln 8}{N}+\frac{K\ln N}{N} \\ O_2\Big(\frac{1}{\sqrt{N}}\Big) &= \sqrt{\frac{8}{N}}\,\ln\Big(\frac{e}{\sqrt{P_{\min}}}\Big)+\frac{\ln 8}{N} \end{aligned} \tag{3}$$

scale like $\frac{\ln N}{N}$ and $\frac{1}{\sqrt{N}}$, respectively (hence, they both vanish as we let N tend to infinity), and $P_{\min}$ denotes the smallest non-zero transition probability of the DMC.

The derivation of the SP67 bound in [8, Part 1] is divided into three main steps. In the first step, a lower bound on the error probability of a pair of probability distributions is derived. Next, the derivation considers fixed composition block codes composed of M codewords, each of length N. The transmission is assumed to take place over a DMC and the code is decoded using a list decoder with list size L. By appropriate assignments of probability distributions and decoding regions, the lower bound on the pairwise error probability is applied to relate the conditional error probability given that a specific codeword is transmitted and the size of the decoding region of this codeword. To this end, an arbitrary memoryless probability measure f_N for vectors of length N over the channel output alphabet is introduced. The size of a decoding region is defined to be the probability of this region under f_N. Since f_N is a probability measure and the list size of the decoder is limited to L, the size of the smallest decision region is upper bounded by $\frac{L}{M}$. The conditional error probability of the codeword with the smallest decoding region is then upper bounded by the maximal conditional error probability over all the codewords to produce a lower bound on the maximal error probability of the code. This bound depends on the choice of the probability measure f_N and the composition of the codewords. The *tightest universal* lower bound on the maximal error probability of fixed composition codes is achieved by finding the probability measure which *maximizes* the lower bound for the composition which *minimizes* this bound. The solution to this min-max problem is provided in [8, Eqs. (4.18)–(4.20)] and serves for the derivation of a lower bound on the maximal error probability of fixed composition block codes whose transmission takes place over DMCs. The third step of the derivation considers arbitrary block codes transmitted over a DMC and decoded by a list decoder with list size L. The number of possible compositions for vectors of length N over an alphabet of size $K \in \mathbb{N}$ is upper bounded by N^K. Hence, a block code consisting of M codewords of length N over an alphabet of size K contains a fixed composition subcode with at least $\frac{M}{N^K}$ codewords. The maximal error probability of the above code is therefore lower bounded by the maximal error probability of a fixed composition block code containing $\frac{M}{N^K}$ codewords of length N. Furthermore, by expurgating half of the codewords with the highest conditional error probability, it is shown in [8] that the *average* error probability of a block code is lower bounded by one half of the *maximal* error probability of some block code with the same length containing one half of the number of codewords. Combining the two statements above, the average error probability of an arbitrary block code containing M codewords of length N over an alphabet of size K is lower bounded by half of the maximal error probability of some fixed composition block code of the same length and over the same alphabet, which contains $\frac{M}{2\,N^K}$ codewords. The lower bound on the latter probability presented in the second step of the derivation is thus used to produce the SP67 bound in Theorem 2.1.

B. Recent Improvements on the 1967 Sphere-Packing Bound

In [11], Valembois and Fossorier revisit the derivation of the SP67 bound, focusing on finite-length block codes. They present four modifications to the classical derivation in [8] which improve the pre-exponent of the SP67 bound. The new bound derived in [11] (referred to here as the 'VF bound') is also valid for memoryless channels with discrete input and continuous output (as opposed to the SP67 bound which is only valid for DMCs). Under the assumptions and notation used in Theorem 2.1, the VF bound [11] is as follows:

Theorem 2.2: **[Improvement on the 1967 Sphere-Packing Bound for Discrete Memoryless Channels]** [11, Theorem 7]. The average decoding error probability satisfies $P_{\mathrm{e}}(N,M,L) \geq \exp\big(-NE_{\mathrm{VF}}(R,N)\big)$ where

$$\begin{aligned} E_{\mathrm{VF}}(R,N) \triangleq \inf_{x>\frac{\sqrt{2}}{2}}\Bigg\{ & E_0(\rho_x)-\rho_x\left(R-O_1\Big(\frac{\ln N}{N},x\Big)\right) \\ & +O_2\Big(\frac{1}{\sqrt{N}},x,\rho_x\Big)\Bigg\} \end{aligned}$$

and

$$\begin{aligned} O_1\Big(\frac{\ln N}{N},x\Big) &\triangleq \frac{\ln 8}{N}+\frac{\ln\binom{N+K-1}{K-1}}{N}-\frac{\ln\left(2-\frac{1}{x^2}\right)}{N} \\ O_2\Big(\frac{1}{\sqrt{N}},x,\rho\Big) &\triangleq x\sqrt{\frac{8}{N}\sum_{k=0}^{K-1} q_{k,\rho}\,\nu_k^{(2)}(\rho)}+\frac{\ln 8}{N} \end{aligned} \tag{4}$$

where ρ_x and the function $\nu_k^{(2)}$ are defined in [11, Theorem 7]. For a more detailed review of the improvements suggested in [11], the reader is referred to [6, Section 5.4].

III. An Improved Sphere-Packing Bound for Symmetric Memoryless Channels

In this section, we present an improved lower bound on the decoding error probability which utilizes the sphere-packing bounding technique. This new bound is valid for *symmetric* memoryless channels with a finite input alphabet, and is referred to as an improved sphere-packing (ISP) bound. Note that the symmetry of the channel is crucial for the derivation of the ISP bound, which stays in contrast to the SP67 and VF bounds where channel symmetry is not required. The symmetry conditions used for the derivation of the ISP bound require the definition of unitary mappings below:

Definition 3.1: A bijective mapping $g : \mathcal{J} \to \mathcal{J}$ where $\mathcal{J} \subseteq \mathbb{R}^d$ is said to be *unitary* if for any integrable generalized function $f : \mathcal{J} \to \mathbb{R}$

$$\int_{\mathcal{J}} f(x)\,\mathrm{d}x = \int_{\mathcal{J}} f(g(x))\,\mathrm{d}x \tag{5}$$

where by a generalized function we mean a function which may contain a countable number of shifted Dirac delta functions. If the projection of $\mathcal{J}$ over some of the d dimensions is countable, the integration over these dimensions is turned into a sum.

We are now ready to define K-ary input symmetric channels:

Definition 3.2: **[Symmetric Memoryless Channels]** A memoryless channel with input alphabet $\mathcal{K} = \{0, 1, \ldots, K-1\}$, output alphabet $\mathcal{J} \subseteq \mathbb{R}^d$ (where $K, d \in \mathbb{N}$) and transition probability (or density if $\mathcal{J}$ is non-countable) function $P(\cdot|\cdot)$ is said to be *symmetric* if there exists a set of bijective and unitary mappings $\{g_k\}_{k=0}^{K-1}$ where $g_k : \mathcal{J} \to \mathcal{J}$ for all $k \in \mathcal{K}$ such that

$$\forall \mathbf{y} \in \mathcal{J},\, k \in \mathcal{K} \quad P(\mathbf{y}|0) = P\big(g_k(\mathbf{y})|k\big) \tag{6}$$

and

$$\forall k_1, k_2 \in \mathcal{K} \quad g_{k_1}^{-1} \circ g_{k_2} = g_{(k_2-k_1) \bmod K}\,. \tag{7}$$

Remark 3.1: From (6), the mapping g_0 is the identity mapping. Assigning $k_1 = k$ and $k_2 = 0$ in (7) gives

$$\forall k \in \mathcal{K} \quad g_k^{-1} = g_{(-k) \bmod K} = g_{K-k}\,.$$

The class of symmetric memoryless channels, as given in Definition 3.2, is quite large. In particular, it can be shown (see [12, Corollary 3.1]) to contain the class of memoryless binary-input output-symmetric (MBIOS) channels. Coherently detected M-ary PSK modulated signaling transmitted over a fully interleaved fading channel followed by an additive white Gaussian noise forms another example of a symmetric memoryless channel. In this case, $\mathcal{J} = \mathbb{R}^2$ and the mapping g_k for $k = 0, \ldots, M-1$ forms a clockwise rotation by $\frac{2\pi k}{M}$ (i.e., $g_k(\mathbf{y}) = \exp\big(\frac{2j\pi k}{M}\big)\,\mathbf{y}$).

The derivation of the SP67 bound relies on an intermediate step where a lower bound on the maximal error probability of fixed composition block codes is derived. The maximal error probability of an arbitrary block code is then lower bounded by considering its largest fixed composition subcode. Since the number of possible compositions grows only polynomially with the block length (when the code alphabet is finite), the loss in the rate of the code scales like $\frac{\ln N}{N}$ (where N is the block length) and therefore vanishes in the asymptotic case where the block length tends to infinity. For finite-length codes, however, this rate shift causes a considerable loss in the tightness of the SP67 bound. The same intermediate step is also used in the tightened version of the SP67 bound, as provided in [11]. The reason for considering fixed composition codes lies in the choice of the optimal probability measure f_N used to derive the bound. As noted in Section II, the derivation of the lower bound on the maximal error probability of fixed composition codes hinges on considering the codeword with the smallest decision region. The size of a decision region, as defined in [8], depends on both the composition of the considered codeword and the choice of the probability measure f_N. For general block codes, the consideration of the codeword with the smallest decoding region creates an interdependency between the optimal probability measure and the composition of the considered codeword. This dependency makes the optimization of f_N, as to get the tightest possible lower bound, untractable. For fixed composition codes the composition does not depend on the considered codeword, facilitating the optimization of f_N. For *symmetric* memoryless channels, we show in [12] that the lower bound on the conditional error probability does not depend on the composition of the considered codeword. Therefore, the optimization of the probability measure f_N is tractable even for general block codes. This modification in the derivation of the bound removes the logarithmic term of the rate shift in the exponent of the SP67 and VF lower bounds (see (3) and (4)), providing a considerable tightening of the bound for finite-length block codes.

Another point which restricts the tightness of the SP67 and VF bounds for finite-length block codes is the need for expurgating half of the codewords in order to convert a lower bound on the maximal error probability to a lower bound on the average error probability. This expurgation causes a loss in rate of $\frac{\ln 2}{N}$ nats per code symbol and adds a factor of $\frac{1}{2}$ to the pre-exponent of the bounds. The consideration of the maximal error probability in the second step of the derivation (see [8]) is due to the consideration of a single codeword, which in turn stems from the fact that the initial step of the derivation considered only a single pair of probability distributions. In [12], we consider a scenario where there are M distinct pairs of probability distributions and the pair used for transmission is chosen uniformly at random and is known to the decoder. In this setup, one can derive lower bounds on the error probability given that the first or second message was sent, averaged over the M probability pairs. This facilitates a modification of the second step of the derivation to consider the average probability of error and the average decoding region size, instead of focusing on a specific codeword, removing the need for expurgation of half of the codewords. It is noted that the symmetry of the memoryless communication channel is required in order to consider M probability distribution pairs

in the first part of the derivation.

Applying the modifications above and the improvements suggested in [11], we derive in [12] a new sphere-packing lower bound on the decoding error probability of block codes transmitted over symmetric memoryless channels, as given in the following theorem:

Theorem 3.1: **[An Improved Sphere-Packing (ISP) Bound for Symmetric Memoryless Channels]** Let $\mathcal{C}$ be an arbitrary block code consisting of M codewords, each of length N. Assume that $\mathcal{C}$ is transmitted over a memoryless symmetric channel which is specified by the transition probabilities (or densities) $P(j|k)$ where $k \in \mathcal{K} = \{0, \ldots, K-1\}$ and $j \in \mathcal{J} \subseteq \mathbb{R}^d$ designate the channel input and output alphabets, respectively. Assume an arbitrary list decoder where the size of the list is limited to L. Then, the *average decoding error probability* satisfies

$$P_{\mathrm{e}}(N, M, L) \geq \exp\bigl(-N E_{\mathrm{ISP}}(R, N)\bigr)$$

where

$$E_{\mathrm{ISP}}(R, N) \triangleq \inf_{x > \frac{\sqrt{2}}{2}} \biggl\{ E_0(\rho_x) - \rho_x \Bigl(R - O_1\Bigl(\frac{1}{N}, x\Bigr)\Bigr) + O_2\Bigl(\frac{1}{\sqrt{N}}, x, \rho_x\Bigr) \biggr\} \tag{8}$$

the function E_0 is introduced in (2), $R \triangleq \frac{1}{N} \ln\Bigl(\frac{M}{L}\Bigr)$, and

$$O_1\Bigl(\frac{1}{N}, x\Bigr) \triangleq -\frac{1}{N} \ln\left(\frac{1}{2} - \frac{1}{4x^2}\right) \tag{9}$$

$$O_2\Bigl(\frac{1}{\sqrt{N}}, x, \rho\Bigr) \triangleq s(\rho) x \sqrt{\frac{8}{N} \mu_0''\bigl(s(\rho), f_{s(\rho)}\bigr)} - \frac{1}{N} \ln\left(\frac{1}{2} - \frac{1}{4x^2}\right). \tag{10}$$

Here, $s(\rho) \triangleq \frac{\rho}{1+\rho}$, and the non-negative parameter $\rho = \rho_x$ on the RHS of (8) is determined by solving the equation

$$\begin{aligned} & R - O_1\Bigl(\frac{1}{N}, x\Bigr) \\ &= -\mu_0\bigl(s(\rho), f_{s(\rho)}\bigr) - \bigl(1 - s(\rho)\bigr) \mu_0'\bigl(s(\rho), f_{s(\rho)}\bigr) \\ &\quad + \bigl(1 - s(\rho)\bigr) x \sqrt{\frac{2\mu_0''\bigl(s(\rho), f_{s(\rho)}\bigr)}{N}}, \end{aligned} \tag{11}$$

where the functions $\mu_0(s, f)$ and f_s are in [8, Eqs. (4.8)] and [8, Eq. (4.20)], respectively, and the differentiation of μ_0 is performed w.r.t. s while keeping f_s fixed.

IV. Numerical Results for Sphere-Packing Bounds

This section presents some numerical results which serve to exemplify the improved tightness of the ISP bound derived in Section III. We consider performance bounds for coherent detection of M-ary PSK block coded modulation where the signals are transmitted over the additive white Gaussian noise (AWGN) channel. The ISP bound, presented here (see [12]), is compared to the VF bound [11] and the SP59 bound [7] (where the latter bound refers to any set of equal energy signals transmitted over the AWGN channel), as well as some upper bounds on the decoding error probability. The bounds are also compared to computer simulations of the performance of modern error-correcting codes when practical decoding algorithms are used.

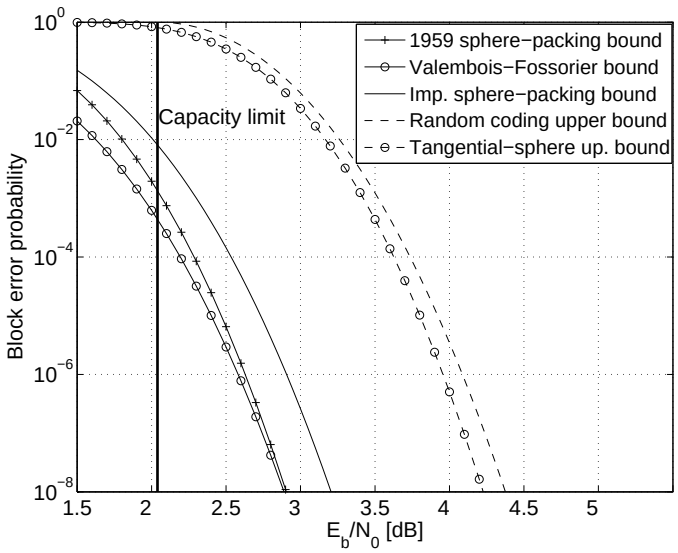

Fig. 1. A comparison between upper and lower bounds on the ML decoding error probability for block codes of length $N = 500$ bits and code rate of $0.8 \frac{\text{bits}}{\text{channel use}}$. This figure refers to BPSK modulated signals whose transmission takes place over an AWGN channel. The compared bounds are the SP59 bound of Shannon [7], the Valembios-Fossorier (VF) bound [11], the improved sphere-packing (ISP) bound presented in Section III, the random-coding upper bound (RCB) of Gallager [3], and the tangential-sphere upper bound (TSB) [4], [5] when applied to fully random block codes with the above block length and rate.

A. Performance Bounds for M-ary PSK Block Coded Modulation over the AWGN Channel

The ISP bound is applied here to consider M-ary PSK modulated signals which are transmitted over the AWGN channel and coherently detected. As noted in Section III, this channel model satisfies the symmetry conditions in Definition 3.2.

Figure 1 compares the SP59 bound [7], the VF bound [11], and the ISP bound derived in Section III. The comparison refers to block codes of length 500 bits and rate $0.8 \frac{\text{bits}}{\text{channel use}}$ which are BPSK modulated and transmitted over an AWGN channel. The plot also depicts the RCB of Gallager [3], the tangential-sphere upper bound (TSB) of Poltyrev ([4], [5]) when applied to fully random block codes with the above block length and rate, and the capacity limit bound (CLB).[1] It is observed from this figure that even for relatively short block lengths, the ISP bound outperforms the SP59 bound for block error probabilities below 10^{-1}. For a block error probability of 10^{-5}, the ISP bound provides gains of about 0.26 and 0.33 dB over the SP59 and VF bounds, respectively. For these code

[1] Although the CLB refers to the asymptotic case where the block length tends to infinity, it is plotted in [11] and here as a reference, in order to examine whether the improvement in the tightness of the ISP bound occurs at rates above or below the channel capacity.

parameters, the TSB provides a tighter upper bound on the block error probability of random codes, as compared to the RCB of Gallager; e.g., the gain of the TSB over the Gallager bound is about 0.2 dB for a block error probability of 10^{-5}. Note that the Gallager bound is tighter than the TSB for fully random block codes of large enough block lengths, as the latter bound does not reproduce the random-coding error exponent for the AWGN channel [5]. However, Figure 1 exemplifies the advantage of the TSB over the Gallager bound, when applied to random block codes of relatively short block lengths; this advantage is especially pronounced for low code rates where the gap between the error exponents of these two bounds is marginal (see [6, p. 67]), but it is also reflected from Figure 1 for BPSK modulation with a code rate of $0.8 \frac{\text{bits}}{\text{channel use}}$. The gap between the TSB and the ISP bound, as upper and lower bounds respectively, is less than 1.2 dB for all block error probabilities lower than 10^{-1}. Also, the ISP bound is more informative than the CLB for block error probabilities below $8 \cdot 10^{-3}$ while the SP59 and VF bounds require block error probabilities below $1.5 \cdot 10^{-3}$ and $5 \cdot 10^{-4}$, respectively, to outperform the capacity limit.

B. Minimal Block Length as a Function of Performance

In a wide range of applications, the system designer needs to design a communication system which fulfills several requirements on the available bandwidth, acceptable delay for transmitting and processing the data while maintaining a certain fidelity criterion in reconstructing the data (e.g., the block error probability needs to be below a certain threshold). In this setting, one wishes to design a code which satisfies the delay constraint (i.e., the block length is limited) while adhering to the required performance over the given channel. By fixing the communication channel model, code rate (which is related to the bandwidth expansion caused by the error-correcting code) and the block error probability, sphere-packing bounds are transformed into lower bounds on the minimal block length required to achieve the desired block error probability at a certain gap to capacity using an arbitrary block code and decoding algorithm. Similarly, by fixing these parameters, the RCB of Gallager [3] and the TSB [5] (when applied to random block codes) are transformed into upper bounds on the block length required for ML decoded random codes to achieve a desired block error probability on a given communication channel.

In this section, we consider some practically decodable codes taken from some recent papers ([1], [2], [9], [10]). We examine the gap between channel capacity and the $\frac{E_\mathrm{b}}{N_0}$ for which they achieve a required block error probability as a function of the block length of these codes. The performance of these specific codes under their practical decoding algorithms is compared to the lower and upper bounds on the block length required to achieve a given block error probability and code rate on a given channel using an optimal block code and decoding algorithm. Comparing the performance of specific codes and decoding algorithms to the information-theoretic limitations provided by the sphere-packing bounds, enables one to deduce how far in terms of delay is a practical system from the fundamental limitations of information theory.

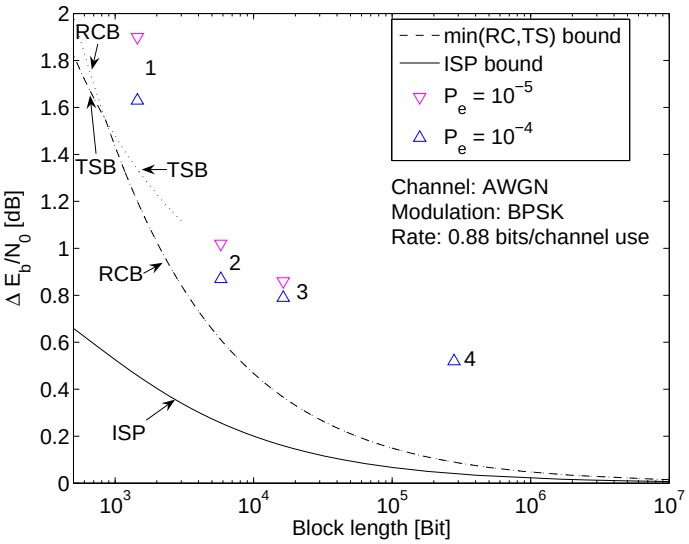

Fig. 2. This figure refers to the tradeoff between the block length and the gap to capacity of error-correcting codes which are BPSK modulated and transmitted over an AWGN channel. The horizontal axis refers to the block length of the codes, and the vertical axis refers to the gap, measured in decibels, between the channel capacity and the energy per bit to spectral noise density ($\frac{E_\mathrm{b}}{N_0}$) which is required to obtain a block error probability P_e (set either to 10^{-4} or 10^{-5}). The considered rate of all the codes is 0.88 bit per channel use. The minimal gap to capacity which is required for achieving a block error probability of 10^{-5} is depicted via bounds: the upper bound is calculated using the random-coding bound (RCB) of Gallager [3] and the tangential-sphere bound (TSB) of Poltyrev [5] applied to fully random and binary block codes, and the lower bound on this minimal block length is calculated via the improved sphere-packing (ISP) bound presented in Section III. In addition to bounds, this tradeoff between the block length (delay) and gap to capacity, is shown for some efficiently decodable error-correcting codes; the codes labelled by 1, 2, 3 and 4 are taken from [1], [2], [9] and [10], respectively.

Figure 2 considers some LDPC codes of rate 0.88 bits per channel use which are BPSK modulated and transmitted over the AWGN channel. The gap to capacity in dB for which these codes achieve block error probabilities of 10^{-4} and 10^{-5} under iterative decoding is plotted as a function of block length. The figure uses upper and lower bounds on the achievable gap to capacity in terms of the block length: for this (relatively high) code rate and the considered range of block lengths, the ISP bound is uniformly tighter than the SP59 bound (so only the ISP bound is depicted in this figure, and the SP59 bound is omitted). The upper bounds on the required block lengths for achieving a target block error probability in terms of the achievable gap to capacity are obtained via the RCB and the TSB when it is applied to the ensemble of fully random block codes. The upper and lower bounds refer to a block error probability of 10^{-5}. The tradeoff between the gap to capacity (in terms of $\frac{E_\mathrm{b}}{N_0}$) versus the block length is depicted in Figure 2 for some efficient error-correcting codes, in order to compare their practical performance and delay to the information-theoretic bounds.

For the examined block error probabilities (of 10^{-4} and 10^{-5}), the depicted codes require a gap to capacity of between 0.63 and 1.9 dB. For this range of $\frac{E_b}{N_0}$, the lower bound on the block lengths which is derived from the ISP bound is looser than the one given by the SP59 bound. However, both bounds are not very informative in this range. For cases where the gap to capacity is below 0.5 dB, the difference between the lower bound on the block length of optimal codes which stems from the ISP bound and the upper bound on the block length of random codes is less than one order of magnitude. Code number 1 is an LDPC of length 1448 bits whose construction of is based on balanced incomplete block designs [1]. This code achieves a block error probability of 10^{-5} at a gap to capacity of 1.9 dB while the RCB shows that the block length which is required to achieve this performance using random codes is upper bounded by 600 bits. The code labeled 2 is a prototype-based LDPC code of length 5176 bits which is taken from [2]. Code number 3 is a quasi-cyclic LDPC code of length 16362 bits taken from [9]. These code achieve under iterative decoding a block error probability of 10^{-5} at gaps to capacity of 1.02 and 0.86 dB, respectively. In terms of block length, the gap between the performance of these codes under iterative decoding and the upper bound on the block length of random codes which achieve a block error probability of 10^{-5} under the same channel conditions is less than one order of magnitude. The code labeled 4 is a finite-geometry LDPC code of length 279552 bits which is taken from [10]. For this code we only have the gap to capacity required to achieve a block error probability of 10^{-4}, however, it is clear that the difference in block length from the RCB becomes quite large as the gap to capacity is reduced.

V. Summary

This paper presents an improved sphere-packing (ISP) bound for finite-length block codes whose transmission takes place over *symmetric* memoryless channels. The improved tightness of the bound is especially pronounced for codes of short to moderate block lengths, and some of its applications are exemplified in this paper. The derivation of the ISP bound was motivated by the outstanding performance of finite-length turbo-like codes. It was also stimulated by the recent improvements on the sphere-packing bound of [8] for finite-length codes, as suggested by Valembois and Fossorier [11].

We apply the ISP bound to various memoryless symmetric channels. The tightness of the ISP bound is exemplified by comparing it with upper and lower bounds on the ML decoding error probability and also with reported computer simulations of turbo-like codes under iterative decoding.

In a wide range of applications, one wishes to design a block code which satisfies a known delay constraint (i.e., the block length is limited) while adhering to a required performance over a given channel model. By fixing the communication channel model, code rate and the block error probability, sphere-packing bounds are transformed into lower bounds on the minimal block length required to achieve the target block error probability at a certain gap to capacity when an arbitrary block code and decoding algorithm are used. Comparing the performance of specific codes and decoding algorithms to the information-theoretic limitations provided by the sphere-packing bounds, enables one to deduce how far in terms of delay is a practical system from the fundamental limitations of information theory. Further details on the comparison between practically decodable codes and the sphere-packing bounds are found in Section IV-B.

The ISP bound is especially attractive for block codes of short to moderate block lengths, and its advantage is especially pronounced for high rate codes. Its improvement over the SP67 bound and the bound in [11, Theorem 7] also becomes more significant as the input alphabet of the considered modulation is increased.

Acknowledgment

This work was supported by the Israel Science Foundation (ISF grant no. 1070/07). The authors are grateful to Prof. Amos Lapidoth for raising the question which stimulated the discussion in Section IV-B.

References

[1] B. Ammar, Y. Kou, J. Xu and S. Lin, "Construction of low-density parity-check codes based on balanced incomplete block designs," *IEEE Trans. on Information Theory*, vol. 50, no. 6, pp. 1257-1268, June 2004.

[2] D. Divsalar and C. Jones, "Protograph LDPC codes with node degrees at least 3," *Proceedings of the 2006 IEEE Global Communications Conference (GlobeCom)*, San Francisco, CA, USA, November 2006.

[3] R. G. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Trans. on Information Theory*, vol. 11, pp. 3–18, January 1965.

[4] H. Herzberg and G. Poltyrev, "The error probability of M-ary PSK block coded modulation schemes," *IEEE Trans. on Communications*, vol. 44, no. 4, pp. 427–433, April 1996.

[5] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. on Information Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.

[6] I. Sason and S. Shamai, "Performance Analysis of Linear Codes under Maximum-Likelihood Decoding: A Tutorial," *Foundations and Trends in Communications and Information Theory*, vol. 3, no. 1–2, pp. 1–222, Now Publishers, Delft, the Netherlands, July 2006. [Online]. Available: `http://www.ee.technion.ac.il/people/sason/monograph_postprint.pdf`.

[7] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell System Technical Journal*, vol. 38, pp. 611–656, May 1959.

[8] C. Shannon, R. Gallager and E. Berlekamp, "Lower bounds to error probability for decoding on discrete memoryless channels," *Information and Control*, vol. 10, Part 1: pp. 65–103, and Part 2: pp. 522–552, February/May 1967.

[9] Y. Tai, L. Lan, L. Zeng, S. Lin and K. Abdel-Ghaffar, "Algebraic construction of quasi-cyclic LDPC codes for the AWGN and erasure channels," *IEEE Trans. on Communications*, vol. 54, no. 10, pp. 1756–1765, October 2006.

[10] H. Tang, J. Xu, S. Lin and K. Abdel-Ghaffar, "Codes on finite geometries," *IEEE Trans. on Information Theory*, vol. 51, no. 2, pp. 572–596, February 2005.

[11] A. Valembois and M. Fossorier, "Sphere-packing bounds revisited for moderate block length," *IEEE Trans. on Information Theory*, vol. 50, no. 12, pp. 2998–3014, Decemeber 2004.

[12] G. Wiechman and I. Sason, "An improved sphere-packing bound for finite-length error-correcting codes," submitted to *IEEE Transactions on Information Theory*, March 2007. [Online]. Available: `http://www.arxiv.org/abs/cs.IT/0608042`. The latest version of this paper is available at `http://www.ee.technion.ac.il/people/sason/ISP.pdf`.