Constructive Spherical Codes near the Shannon Bound

Patrick Solé, Jean-Claude Belfiore

Constructive Spherical Codes near the Shannon Bound

Patrick Solé and Jean-Claude Belfiore

Telecom ParisTech, CNRS LTCI
Communications and Electronics Dept.
46 rue Barrault, 75634 Paris CEDEX 13, France
sole@enst.fr,belfiore@enst.fr

Abstract. Shannon gave a lower bound in 1959 on the binary rate of spherical codes of given minimum Euclidean distance ρ. Using nonconstructive codes over a finite alphabet, we give a lower bound that is weaker but very close for small values of ρ. The construction is based on the Yaglom map combined with some finite sphere packings obtained from nonconstructive codes for the Euclidean metric. Concatenating geometric codes meeting the TVZ bound with a Lee metric BCH code over $GF(p)$, we obtain spherical codes that are polynomial time constructible. Their parameters outperform those obtained by Lachaud and Stern in 1994. At very high rate they are above 98 per cent of the Shannon bound.

Keywords: spherical codes, codes for the Euclidean metric, saddle point method

1 Introduction

A **spherical code** is a finite set of points of the unit sphere in a Euclidean space of finite dimension. For motivation and background see [5, 2]. Let X denote a spherical code of $\mathbb{R}^n$. Denote by ρ its Euclidean squared minimum distance. Define its binary rate as

$$R(\rho) := \limsup \frac{\log_2(|X|)}{n}.$$

Chabauty in 1953 and Shannon in 1959 [7], gave a lower bound

$$R(\rho) \geq R_S(\rho) := 1 - (1/2)\log_2(\rho(4-\rho)).$$

Lachaud and Stern, in 1994 gave a lower bound on the rate $R_*(\rho)$ of *polynomial time constructible* spherical codes as

$$R_*(\rho) \geq 0.5 R_S(\rho).$$

In the present, work we shall give a lower bound based on nonconstructive lattice packings

$$R(\rho) \geq R_L(\rho) := -(1/2)\log_2(\rho).$$

It can be shown by direct substitution that

$$R_S(\rho) \geq R_L(\rho)$$

for all $0 \leq \rho \leq 4$.

However, for small ρ, the two curves are very close to each other:

$$R(\rho) - R_L(\rho) = O(\rho^2).$$

We give a family of spherical codes based on non constructive codes for the Euclidean metric whose asymptotic performance is just as good.

$$R(\rho) \geq R_L(\rho),$$

This shows that using finite alphabet codes for constructing finite packings is as efficient as using truncation of dense infinite sphere packings.

However, the main result of this work is a lower bound based on an explicit family of polynomial time constructible codes for the Euclidean metric that outperforms the Lachaud Stern bound almost by a factor of 2

$$R_*(\rho) \geq 0.98 R_S(\rho).$$

for some very small values of ρ in the range $0 < \rho \leq 1$. These codes, furthermore admit efficient encoding and decoding algorithms.

The article is organized as follows. In the next section we explore the Yaglom map and use it on truncations of infinite lattices. In Section III we study the performance of long codes for the Euclidean metric over a fixed alphabet. The analysis technique is based on the saddle point method. In Section IV we give the explicit construction of long such codes and prove it is better not only than the relevant Gilbert bound but also after Yaglom map than 98 per cent of the Shannon bound.

2 The Yaglom map

Following Yaglom [2, Chap. 9, Thm. 6], we inject $\mathbb{R}^n$ into $\mathbb{R}^{n+1}$ by the map

$$Y: \; x \mapsto (x, \sqrt{R^2 - x \cdot x}).$$

Note that this map sends the ball $B(n, R)$ of radius R that is

$$B(n, R) := \{x \in \mathbb{R}^n | \, x \cdot x \leq R^2\}$$

in $\mathbb{R}^n$ into the sphere $S(n, R)$ of radius R in $\mathbb{R}^{n+1}$

$$S(n, R) := \{x \in \mathbb{R}^{n+1} | \, x \cdot x = R^2\}$$

and that distance between points can only increase. The following result is then immediate.

Proposition 1 *If P is a packing of spheres of diameter d in $B(n,R)$ then $Y(P)$ is a spherical code in $S(n,R)$ of minimum square distance d^2.*

Using lattice packings we can prove our first bound.

Theorem 1 *There are families of spherical codes built from lattice packings by the Yaglom map such that*

$$R(\rho) \geq R_L(\rho) := -(1/2)\log_2(\rho).$$

Proof. By the Yaglom bound [2, Chap. 9, Thm. 6] we know there are spherical codes satisfying

$$R \geq \delta + 1 + R_L(\rho),$$

where δ is the asymptotic exponent of the best density of lattice packings in $\mathbb{R}^n$, or $\frac{\log_2(\Delta)}{n}$ in the notation of [2, Chap. 1]. Now by the Minkowski bound [2, Chap. 1, (46)], we know that $\delta \geq -1$. The result follows.

Using lattice packings built from codes over fields by the so-called Construction A [2, p.182] we obtain our second bound.

Theorem 2 *There are families of spherical codes built from Construction A lattice packings such that*

$$R(\rho) \geq R_L(\rho).$$

Proof. By [11] we know there are lattice packings built from codes over prime fields by Construction A having asymptotic density

$$\delta \geq -1.$$

The result follows, as the preceding one, upon applying the Yaglom bound.

This result will be obtained also for finite sphere packings made of codes for the Euclidean metric (Theorem (6)). Using **constructive** lattice packings constructed by AG techniques we can prove our last bound.

Theorem 3 *There are families of spherical codes built from lattice packings by the Yaglom map such that*

$$R(\rho) \geq R_L(\rho) - 0.39.$$

Proof. By the Yaglom bound [2, Chap. 9, Thm. 6] we know there are spherical codes satisfying

$$R \geq \delta + 1 + R_L(\rho),$$

where $\delta \geq -1.39$ is the asymptotic exponent of the best density of lattice packings constructed in [8]. The result follows.

3 Codes for the Euclidean metric

We consider codes of length n over the integers modulo an integer q. If $q = 2s+1$ is odd we represent $\mathbb{Z}_q$ on the real line by the constellation

$$\{-s, \cdots, -1, 0, 1, \cdots, s.\}$$

If $q = 2s + 2$ is even we represent $\mathbb{Z}_q$ on the real line by the constellation

$$\{-s - 1/2, \cdots, -3/2, -1/2, 1/2, \cdots, s - 1/2, s + 1/2\},$$

which is a shift of the natural representation

$$\{-s, \cdots, -1, 0, 1, \cdots, s, s + 1\}$$

by $-1/2$. We denote by ϕ the induced map from $\mathbb{Z}_q^n$ into $\mathbb{R}^n$. If q is odd then $\phi(x) \cdot \phi(x) \leq ns^2$, while if q is even $\phi(x) \cdot \phi(x) \leq n(s + 1/2)^2$, We consider the Euclidean distance $d_E(,)$ on $\mathbb{Z}_q^n$ defined by $d_E(x, y) = (\phi(x) - \phi(y))^2$. This distance could have been defined as induced by the standard Euclidean weight $w_E()$ on $\mathbb{Z}_q$ that is $w_E(x) = \min(x^2, (q - x)^2$.

Proposition 2 *If C is a code of length n and minimum Euclidean distance d over $\mathbb{Z}_q$ then $\phi(C)$ is a packing of spheres of diameter $\sqrt{d}$ of $B(n, s\sqrt{n})$ if q is odd and of $B(n, (s + 1/2)\sqrt{n})$ if q is even.*

Combining with Proposition 1 we obtain

Proposition 3 *If C is a code of length n and minimum Euclidean distance d over $\mathbb{Z}_q$ then $Y(\phi(C))$ is a spherical code of squared Euclidean distance d of $S(n, s\sqrt{n})$ if q is odd and of $S(n, (s + 1/2)\sqrt{n})$ if q is even.*

Let $V(n, q, r)$ denote the size of the ball of radius r for the Euclidean metric in $\mathbb{Z}_q^n$. The following result is the analogue of the standard Gilbert bound in that setting.

Proposition 4 *There are codes in $\mathbb{Z}_q^n$ of Euclidean distance d and of cardinality*

$$|C| \geq \frac{q^n}{V(n, q, d - 1)}.$$

The technically difficult part is to estimate the asymptotic exponent of $V(n, q, r)$ for n large and $r = \lfloor \lambda n \rfloor$. To that end, we introduce the following generating series $f(z) = 1 + 2s(z)$ with

$$s(z) = \sum_{i=1}^{s} z^{i^2}$$

for odd q and

$$s(z) = \sum_{i=1}^{s-1} z^{i^2} + z^{s^2}$$

for even q.

Theorem 4 *The asymptotic exponent of $V(n,q,r)$ for n large and $r = \lfloor \lambda n \rfloor$ is*

$$\lim(\frac{\log_2(V(n,q,r))}{n}) = \log_2(f(\mu)) - \lambda \log_2(\mu)$$

where μ is the unique real positive solution of $zf'(z) = \lambda f(z)$.

Proof. The generating function for the numbers $V(n,q,r)$ is of the form $f(z)^n g(z)$ with $g(z) = 1/(1-z)$. The result follows by application of [4, Corollary 2].

Theorem 5 *With the preceding notation, there are spherical codes of the unit sphere $S(n+1,1)$ with relative squared Euclidean distance $\rho \leq 1$ of binary rate*

$$R \geq \log_2(q) - \log_2(f(\mu)) + a\rho \log_2(\mu)$$

where μ is the unique real positive solution of $zf'(z) = a\rho f(z)$, with $a = s^2$ for q odd and $a = (s+1/2)^2$ for q even.

Proof. We combine the Gilbert bound of Proposition 4 with the estimate of Theorem 4 to construct long Euclidean metric codes with prescribed parameters and the Yaglom map of Proposition 3 to derive spherical codes from them. Note that we let $\lambda = a\rho$ to rescale $S(n+1,\sqrt{na})$ to $S(n+1,1)$.

This approach can be generalized to the case of a large varying alphabet.

Theorem 6 *There are spherical codes, constructed from codes over $\mathbb{Z}_q$, with q odd and variable and asymptotic rate*

$$R(\rho) \geq R_L(\rho) - c,$$

with $c \approx 0.77 \times 10^{-8}$.

Proof. We use the same saddle point analysis as [10] on the generating function

$$1 + 2\sum_{i=1}^{\infty} z^{i^2}.$$

Note that s does not occur in the latter expression since $q \geq 2r+1$.

4 Constructive bound

By the TVZ bound [6, Th. 13.5.4] we know there are families of geometric codes over $GF(Q)$ for Q a square with rate $\mathcal{R}$ and relative distance Δ satisfying

$$\mathcal{R} + \Delta \geq 1 - \frac{1}{\sqrt{Q}-1}.$$

We concatenate this geometric code with a code over $\mathbb{Z}_q$ of parameters $[n,k]$ and minimum Euclidean distance d_E. We must assume therefore that $Q = q^k$. If q is not a prime, we label $\mathbb{Z}_q$ by the elements of $GF(q)$ in an arbitrary fashion. In order to apply the TVZ bound we must assume Q to be square.

Proposition 5 *With the above notation, the Yaglom map of the concatenated code has parameters (R, ρ) above the straight line*

$$\frac{Rn}{\log_2(q)k} + \frac{\rho n s^2}{d_E} \geq 1 - \frac{1}{\sqrt{q^k} - 1}$$

Proof. We assume some familiarity with concatenation [6, §5.5]. The $q-$ary rate of the concatenated code is $\frac{k}{n}\mathcal{R}$. The binary rate of the spherical code is therefore $R = \log_2(q)\frac{k}{n}\mathcal{R}$. The relative distance of the inner Euclidean metric code is $\frac{d_E}{n}$. The relative distance of the concatenated code is $\Delta\frac{d_E}{n}$. After normalization to reduce to the unit sphere Proposition (2) yields

$$\rho \geq \Delta\frac{d_E}{ns^2}.$$

Substituting into the TVZ bound we are done.

Let us take, as inner codes, the Roth-Siegel BCH codes [9]. The Lee minimum distance is an immediate lower bound on the Euclidean minimum distance of such a code.

Theorem 7 *For each prime $p \geq 7$ and every integer $1 \leq t \leq (p+1)/2$, such that p is congruent to $t+1 \mod 2$, there is a family of spherical codes with binary rate R and minimum squared Euclidean distance ρ over $\mathbb{Z}_p$ satisfying*

$$\frac{R(p-1)}{(p-t-1)\log_2(p)} + \frac{\rho(p-1)^3}{8t} \geq 1 - \frac{1}{p^{(p-t-1)/2} - 1}.$$

Proof. For these codes $n = p-1$, $d_L \geq 2t$ and $k \geq n - t$, by [9].

We need the following elementary result whose proof is omitted.

Proposition 6 *The equation of the tangent in ρ of the curve $(\rho, \lambda R_L(\rho))$ is of the form*

$$\frac{X}{A} + \frac{Y}{B} = 1,$$

with

$$A = \rho(1 - \ln(\rho))$$
$$B = \frac{\lambda}{2\ln(2)}(1 - \ln(\rho))$$

We are now in a position to state and prove the main result of this note.

Theorem 8 *Take* $p = 54324557194526233431402996499932247126422684050879721482365330417236755446526748745089584552036020441984626385846298664106668659730094751$ *and* $t/n = 0 : 00155359$ *in Theorem (7). For all values of $\rho \leq e^{-}640 : 48$ and $\lambda = 0.98$ the bound of Theorem (7) is strictly above the tangent to the curve $(\rho, \lambda R_L(\rho))$ at ρ.*

Proof. Denote by $f = 1 - \frac{1}{p^{(p-t-1)/2}-1}$ a number very close to 1. Put $\tau = t/n$. We find values of p and ρ that the intersections of the tangent with the axes are less than

$$B \leq \frac{(p-t-1)\log_2(p)}{p-1}$$
$$A \leq \frac{8\tau f}{(p-1)^2}$$

Approximating $p-1$ by p and f by 1 we get by replacing A, B by their expressions from Proposition 6,

$$\lambda(1-\ln(\rho)) \leq 2(1-\tau)\ln(p)$$
$$\rho(1-\ln(\rho)) \leq \frac{8\tau}{p^2}$$

Write

$$x = \ln(\rho)$$
$$y = \ln(p)$$

After this change of variables, and getting rid of τ, between

$$(1-x)\exp(x+2y)/8 \leq \tau \leq 1 - \lambda(1-x)/2y$$

we obtain the equation

$$\exp(x+2y)(1-x) + 4\lambda(1-x)/y \leq 8,$$

which can be solved numerically and graphically as shown in Figure 1. Once the values of x and y have been constrained in that way the assertions of the Theorem are checked by direct (machine) computation.

Recall that the envelope of a family of curves is a curve all the points of which are tangent at some point to one of the curves in the family. We can obtain the envelope of the family of straight lines promised by TVZ when p varies as follows

Theorem 9 *Some points produced by Theorem 7 lie on the curve*

$$\frac{R\ln(2)}{(1-\tau)y} + \frac{1}{1-x} = 1$$

where

$$x = \ln(\rho)$$
$$y = \ln(p)$$
$$x + 2y = c$$
$$8\tau = (1-x)\exp(c)$$

and c is a constant depending on the range of τ.

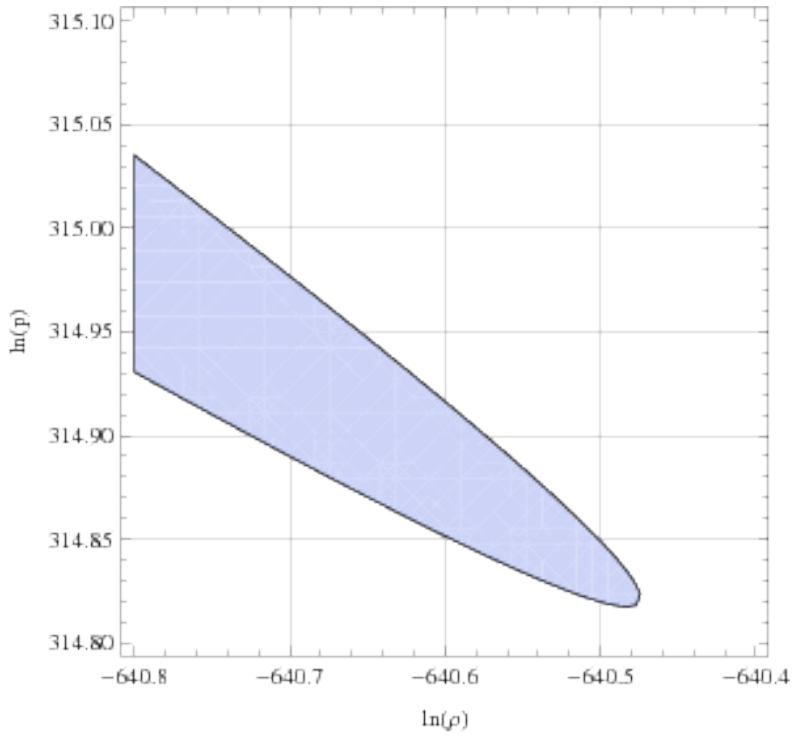

Fig. 1. Attainable Region for $\ln \rho$ and $\ln p$; here, $\lambda = 0.98$

Proof. Keep the notation of the preceding proof. An approximate equation for the straight line of Theorem 7 is

$$\frac{R}{(1-\tau)\ln_2(p} + \frac{p^2}{8\tau} = 1$$

We choose arbitrarily

$$x + 2y = c$$

for some constant c and

$$8\tau = (1-x)\exp(c).$$

The result follows afer some algebra.

Experimentally, the curve obtained in Figure 2 shows that our constructive codes outperform $\lambda\times$ the Shannon bound. Note that we took, here, a value of $\lambda = 0.976$ to show more clearly the performance of such codes, even if these codes have been designed for $\lambda = 0.98$.

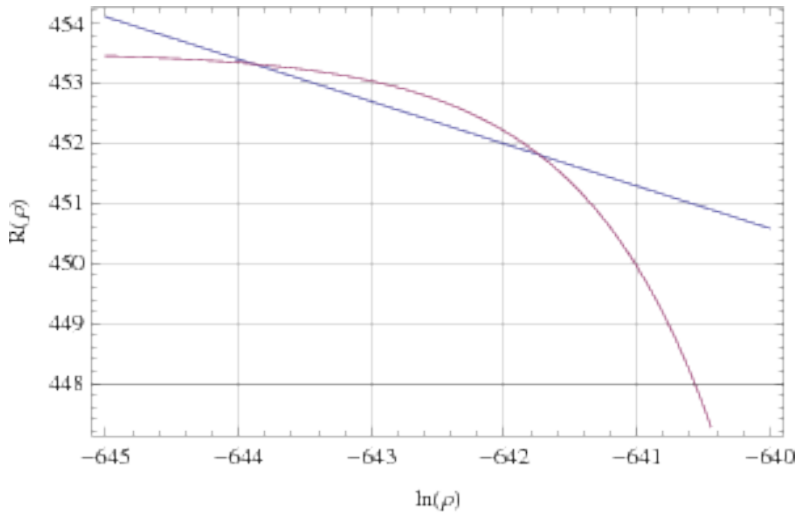

Fig. 2. Rate as a function of $\ln \rho$ for both our constructive codes and $\lambda\times$ the Shannon bound for $\lambda = 0.976$

5 Complexity issues

While the size of the large prime in Theorem 8 might seem outlandish, we believe that our constructions of spherical codes might have some practical interest for more realistic inner codes. We observe that the complexity of the Yaglom map is $O(N)$ and that the concatenated codes being linear, encoding of the spherical codes is linear in time and space. This contrasts with most standard constructions of spherical codes, especially those based on constant weight codes [5]. As for decoding, the decoding of concatenated code is possible knowing decoding algorithms for the inner and outer codes [3]. As explained in [6, §13.5.2] polynomial time decoding algorithms are known for certain codes obtained from the Garcia Stichtenoth towers of function fields. An algebraic decoding algorithm up to the Lee error correcting capacity is provided for the BCH codes we use in [9].

6 Conclusion

In this work we have constructed spherical codes by using finite packings of spheres within a ball and mapping them on the surface of the sphere in the next dimension by using the Yaglom map. The construction of finite packing was done by using codes for the Euclidean metric. We hope this will stimulate research in this area. For instance can the minimum Lee distance bounds of [9] for BCH codes be improved for the Euclidean metric? Are there perfect codes for the Euclidean metric? This might provide stronger inner codes for the concatenation construction and might lead to an improvement of the Shannon lower bound.

Acknowledgement The authors thank Christine Bachoc and Philippe Gaborit for helpful discussions.

References

1. E. R. Berlekamp, *Algebraic coding theory*. McGraw-Hill Book Co., New York-Toronto, Ont.-London 1968
2. J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices and groups*, Springer Verlag, GMW 290, (2003).
3. I.I. Dumer, Concatenated codes and their multilevel generalizations in *Handbook of coding theory*, Vol. II, V. Pless and W.C Huffman, eds, 1911–1988, North-Holland, Amsterdam, 1998.
4. D. Gardy, P. Solé, Saddle point techniques in asymptotic coding theory, in Algebraic coding (Paris, 1991), 75–81, Lecture Notes in Comput. Sci., 573, Springer, Berlin, 1992.
5. T. Ericson,V. Zinoviev, *Codes on Euclidean spheres*, North-Holland, Amsterdam, 2001
6. W.C. Huffman, V. Pless,*Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.
7. G. Lachaud, J. Stern, Polynomial-time construction of codes. II. Spherical codes and the kissing number of spheres. *IEEE Trans. Inform. Theory* 40 (1994), no. 4, 1140–1146.
8. M.Y. Rosenbloom, M.A.Tsfasman, Multiplicative lattices in global fields. Invent. Math. 101 (1990), no. 3, 687–696.
9. R. M. Roth, P.H. Siegel, Lee-metric BCH codes and their application to constrained and partial-response channels. IEEE Trans. Inform. Theory 40 (1994), no. 4, 1083–1096.
10. J.A. Rush, N.J.A. Sloane, An improvement to Minkowski-Hlawka bound for packing superballs, Mathematika, 34 (1987) 8–18.
11. J. A. Rush, A lower bound on packing density. Invent. Math. 98 (1989), no. 3, 499–509.