Saddle Point Techniques in Asymptotic Coding Theory

Daniele Gardy[1]
Patrick Sole[2]

Technical Report No. CS-91-29

April, 1991

[1]LRI, CNRS-URA 410, Batiment 490, Universite de Paris XI, 91405 Orsay, France
[2]CNRS-URA 1376, Laboratoire I.3.S., Batiment 4, 250 rue Albert Einstein, Sophia - Antipolis, 06560 Valbonne, France

Saddle Point Techniques in Asymptotic Coding Theory

Danièle Gardy [1]
LRI, CNRS-URA 410,
Bâtiment 490,
Université de Paris XI,
91405 Orsay,
France
&
Patrick Solé [2]
CNRS-URA 1376,
Laboratoire I.3.S.,
Bâtiment 4,
250 rue Albert Einstein,
Sophia - Antipolis,
06560 Valbonne,
France.

[1]This work was partially supported by the PRC Mathématique-Informatique and by ESPRIT-II Basic Research Action No. 3075 (project ALCOM), and partially performed while this author was visiting Brown University, Providence, R.I., U.S.A.
[2]This work was partially supported by the PRC C^3 of CNRS and MRT.

Abstract

Asymptotic estimates on coefficients of generating functions are derived by contour integration. In particular, we obtain Lee analogues of the entropy function both for small and large alphabets. An estimate on the central moments of the Binomial Law allows us to derive an asymptotic upper bound on the covering radius of binary codes of given dual distance.

1 Introduction.

From a graph theoretic point of view, codes for the Hamming metric are sets of vertices in the n-dimensional hypercube. Due to the cartesian product structure of this graph (or of the n-dimensional torus, which is the graph adapted to the Lee metric) many statistics of interest (surface of spheres, for instance) are additive; this leads to generating functions which are n^{th} powers of the generating function for the one-dimensional case.

This type of generating function has been extensively studied in statistics [4, 7], and in analysis of algorithms [6, 8]. The techniques used involve complex analysis [3, 5], and in particular the method of steepest descent to estimate contour integrals.

The paper is organized as follows. In Section 2 we recall the analytic results that we need. In Section 3 we rederive the classical estimate for the volume of Hamming spheres via the entropy function. In Section 4, we give a simpler proof of an estimate of Astola [1] for the volume of the Lee spheres for small alphabets. In Section 5, we discover a new estimate for Lee spheres over large alphabets. Note that the function L is not essentially more complicated than the binary entropy function. In Section 6, we tackle a different kind of problem: the asymptotic analysis of power moment bounds for the covering radius versus dual distance problem.

2 The Saddle Point Method

In this section our aim is to estimate the coefficient of order r of a generating function $\Phi(z)$, a quantity that we shall denote henceforth by $[z^r]\Phi(z)$. More precisely, we are concerned by generating functions of the kind $\Phi(z) = f(z)^n g(z)$, where $f(z)$ and $g(z)$ do not depend on n, and where $r \sim \lambda n$ for large n, with $0 < \lambda < 1$.

In order to use complex variable techniques we need to introduce the Cauchy formula [3, p.72].

Lemma 1 *Let D denote a simply connected domain containing the origin and where Φ is analytic. Let Γ denote a simply closed contour contained in D. Then*

$$[z^r]\Phi(z) = \frac{1}{2\pi i}\int_\Gamma \Phi(z)\frac{dz}{z^{r+1}}.$$

Rewriting the integrand in Cauchy's formula in the form $e^{h(z)}$ with $h(z) = \log\Phi(z) - (r+1)\log(z)$, we are left to estimate a contour integral $I_{r,n}$, say, of the type

$$I_{r,n} = \frac{1}{2\pi i}\int_\Gamma e^{h(z)}dz.$$

The basic idea of the saddle point method is to use a second order Taylor approximation of $h(z)$ about a point ρ where $h'(\rho) = 0$. This point is called a *saddle point* because in its neighborhood the surface $z \mapsto h(z)$ resembles a saddle. The part of Γ nearby the saddle point is the most important contribution in $I_{r,n}$ and we obtain

$$I_{r,n} \approx \frac{e^{h(\rho)}}{\sqrt{2\pi h''(\rho)}}.$$

This holds under suitable conditions on ρ, e.g. $h''(\rho) > 0$. To get a condition bearing on r only, we define two operators acting on f

$$\Delta f(z) = z\frac{f'(z)}{f(z)},$$

and

$$\delta f(z) = \frac{(\Delta f)'(z)}{z}.$$

It can be shown (see for example [6, p.65]) that when f is a power series or a polynomial with positive coefficients, then $\delta f(\rho) > 0$. We shall say that f is *degenerate* if $f(0) = 0$ or if there exists an analytic function h and an integer m such that $f(z) = h(z^m)$. We summarize the discussion in the following statement, which is essentially due to [4].

Theorem 1 *If f is non degenerate, if the modulus of any singularity of g is larger than the saddle point ρ defined by $\Delta f(\rho) = (r+1)/n$, and if $\delta f(\rho) > 0$, then for large n and $r \sim \lambda n$*

$$[z^r]\{f(z)^n g(z)\} = \frac{f(\rho)^n g(\rho)}{\rho^{r+1}\sqrt{2\pi n \delta f(\rho)}}(1 + o(1)).$$

In general, this theorem is difficult to apply, because ρ is a function of n and $f(\rho)^n$ is difficult to estimate. So, we shall use the following corollary.

Corollary 1 *Under the hypotheses of Theorem 1, and with $\Phi(z) = f(z)^n g(z)$,*

$$\frac{1}{n}\log([z^r]\Phi(z)) = \log(f(\rho)) - \lambda(1 + o(1))\log(\rho) + \frac{\log(g(\rho)/\sqrt{2\pi f(\rho)})}{n} + o(1).$$

In general the third term is negligible compared with the first two.

3 Hamming Spheres

As is well-known, the generating function for the volume of the Hamming spheres is $\Phi_n(z) = \frac{(1+z)^n}{1-z}$. Here $f(z) = 1 + z$ and $g(z) = \frac{1}{1-z}$. The function f is entire, with positive coefficients, and non-degenerate, and g has a simple pole in 1. The following result can be derived by more elementary but also more tedious means.

Theorem 2 *Let $H(x) = -x\log(x) - (1-x)\log(1-x)$ be defined on $(0,1)$. If $\lambda < 0.5$, then for $r \sim \lambda n$ and large n*

$$\frac{1}{n}\log_2([z^r]\Phi_n(z)) = H(\lambda) + o(1).$$

Proof: The saddle point equation can be written as

$$\frac{n}{1+z} + \frac{1}{1-z} = \frac{r+1}{z},$$

which can be reduced to the quadratic equation in z:

$$(n - r - 2)z^2 - (n + 1)z + r + 1 = 0.$$

The left-hand side is asymptotically

$$(1-\lambda)z^2 - z + \lambda = (1-\lambda)(z-1)(z-\frac{\lambda}{1-\lambda}).$$

The second root is < 1 iff $\lambda < \frac{1}{2}$. The result follows by Corollary 1. $\square$

We leave as an exercise to the reader to derive an analogous result for q-ary codes (Cf. [11] Lemma 5.1.6 p.55).

4 Lee Spheres for Small Alphabets

Let $s = \lfloor \frac{q}{2} \rfloor$. Then, from [2], we know that the generating function for the volume of the Lee spheres over $\mathbf{F}_q^n$ is $\Phi_{n,q}(z) = f(z)^n g(z)$, with $f(z) = 1 + 2\sum_{i=1}^{s} z^i$ and $g(z) = \frac{1}{1-z}$. The function f has positive coefficients and is not degenerate. The following result was proved by Astola [1] using multinomial coefficients and Lagrange multipliers.

Let

$$L(\tau, q) = \lim_{n \mapsto +\infty} (1 - \frac{1}{n} \log_q([z^{ns\tau}]\Phi_{n,q}(z))).$$

Then Astola's result can be stated as follows

Theorem 3 *Let $q = 2s+1$. Then $L(\tau, q) = 1 + \log_q(\alpha\beta^{\tau s})$, where $\alpha \geq 0$ and $\beta \geq 0$ are defined by the two equations*

$$\alpha(1 + \sum_{i=1}^{s} \beta^i) = 1$$

and

$$\alpha \sum_{i=1}^{s} i\beta^i = \frac{\tau s}{2},$$

and where $0 \leq \tau \leq \frac{q+1}{2}$. Moreover $L(\tau, q) = 0$ if $\tau \geq \frac{q+1}{2}$.

Our method gives the following result valid without restrictions on q.

Theorem 4 *If $\lambda < \frac{s(s+1)}{2s+1}$, then*

$$\frac{1}{n} \log_q([z^r]\Phi_{n,q}(z)) = \log_q(f(\rho)) - \lambda \log_q(\rho) + o(1),$$

where ρ is the unique real positive solution of

$$2\sum_{i=1}^{s} (i - \lambda) z^i = \lambda, \tag{1}$$

and where $f(\rho) = \frac{s\rho + (s+1)}{\rho(\lambda - s) + (s+1) - \lambda}$.

Proof: Let $\sigma(z) = \sum_{i=1}^{s} z^i$. Then, we see that $f(z) = 1 + 2\sigma(z)$. Tedious but straightforward calculations show that $\sigma(z)$ satisfies to the first order ODE

$$z(z-1)\sigma'(z) + (-sz + s + 1)\sigma(z) = sz.$$

The saddle point equation can be written as

$$z\sigma'(z) - \lambda\sigma(z) = \frac{\lambda}{2}.$$

Getting rid of $\sigma'(z)$ between these two equations yields an expression for $\sigma(z)$, hence the above-mentioned expression for $f(\rho)$.
The condition on λ comes from $\Delta f(1) > \lambda$, and ensures that the saddle point ρ is smaller than 1, the pole of g. $\square$

The dictionary between Astola's notations [1] and ours is the following: His β is our ρ, his α is $\frac{1}{f(\rho)}$, his τ is λ/s.

5 Lee Spheres for Large Alphabets

This is the limiting case of the preceding section, when s gets large, and $f(z)$ goes to $\frac{1+z}{1-z}$. The following result appears to be new or at least unpublished.

Theorem 5 *Let $V_{n,r}$ denotes the volume of the Lee sphere of radius r in $\mathbf{Z}_q^n$. When $q \geq 2r+1$ this quantity does not depend on q, and for large n and $\frac{r}{n}$ going to λ, we get*

$$\frac{1}{n}\log(V_{n,r}) = L(\lambda) + o(1),$$

where

$$L(x) = x\log(x) + \log(x + \sqrt{x^2+1}) - x\log(\sqrt{x^2+1} - 1).$$

Proof: The saddle point equation can be written as

$$(r+2)z^2 + (2n+1)z - (r+1) = 0.$$

The only positive root is $\rho = \frac{\sqrt{(2n+1)^2+4(r+1)(r+2)}-(2n+1)}{2(r+2)}$. When n is large and r/n goes to λ we have

$$\rho \sim \frac{\sqrt{1+\lambda^2}-1}{\lambda}.$$

It is easily checked that this quantity is always < 1. Hence the pole of g is not a problem. $\square$

Using this result we obtain the analogues of the Hamming and Gilbert-Varshamov bound.

Corollary 2 *Let $R(\delta)$ denote the largest achievable rate of a family of codes of minimum Lee distance δn for large n, and such that $q \geq 2\delta n + 1$. Then, for $0 \leq \delta \leq L^{-1}(1) \approx 0.37$ we have*

$$1 - L(\delta) \leq R(\delta) \leq 1 - L(\frac{\delta}{2}).$$

These bounds are tabulated in the following table and drawn in Figure 1.

Open Problem 1 *Are there families of codes which are better than the lower-bound?*

Open Problem 2 *Study $V_{n,r}$ when $n = o(r)$, and both n and r are large.*

x	$1 - L(x)$	$1 - L(\frac{x}{2})$
0.05	0.76	0.87
0.10	0.60	0.77
0.15	0.46	0.68
0.20	0.34	0.60
0.25	0.23	0.53
0.30	0.13	0.46
0.35	0.04	0.40
0.40	< 0	0.33
0.45	< 0	0.28
0.50	< 0	0.23
0.55	< 0	0.18
0.60	< 0	0.13
0.65	< 0	0.08
0.70	< 0	0.04

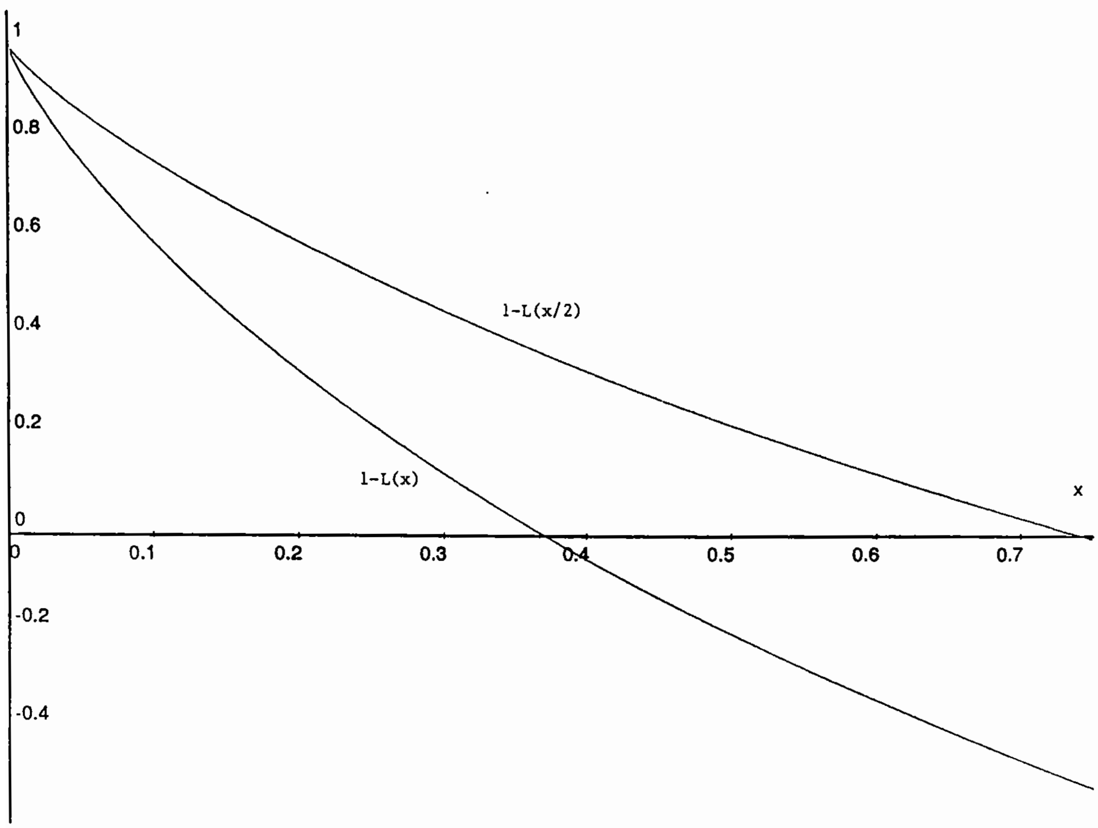

Figure 1: Bounds for $R(\delta)$

6 Covering Radius and Dual Distance

A current research problem in coding theory is to find upper bounds on the covering radius as a function of the dual distance. A connection with zeroes of Krawtchouk polynomials was discovered in [10]. A simpler power-sum approach was initiated in [9]. Here we derive an asymptotic version of the following Theorem of [9]:

Theorem 6 *Let C be a code of dual distance at least $2s+1$. Then its covering radius ρ is bounded from above by*

$$\rho \leq \frac{n}{2} - (2^{\frac{s}{s+1}} - 1)\mu_s(n)^{\frac{1}{2s}},$$

where $\mu_s(n) = [\frac{t^s}{(2s)!}]\cosh^n(\frac{\sqrt{t}}{2})$.

To meet this goal we need the following Lemma.

Lemma 2 *Assume that the ratio $2s/n$ goes to a constant $\lambda \in [0,1]$ for both n and s large. Then $\frac{1}{n}\mu_s(n)^{\frac{1}{2s}}$ goes to $\frac{\lambda}{2e}\frac{\cosh(x_0)^{\frac{1}{\lambda}}}{x_0}$ where x_0 is the positive solution of $x\tanh(x) = 2\lambda$.*

Proof: Here $g(z) = 1$ has no singularity; and $f(z) = \cosh(\frac{\sqrt{z}}{2})$ is entire with positive coefficients. It is not degenerate. Letting $x = \frac{\sqrt{z}}{2}$, the saddle point equation can be written as

$$x\tanh(x) = 2\lambda.$$

Let x_0 be the unique real positive solution of this equation. Corollary 1 applied to the saddle point $z_0 = \sqrt{x_0}/2$ gives

$$(\frac{\mu_s(n)}{(2s)!})^{\frac{1}{2s}} \sim \frac{\cosh^{\frac{1}{\lambda}}(x_0)}{2x_0}.$$

Stirling's approximation yields easily

$$(2s)!^{\frac{1}{2s}} \sim \frac{2s}{e}.$$

□

Theorem 7 *Let C be a code of length n, and dual distance $2s+1$. Assume n large, ρ/n having r as a limit, and $s \sim \lambda n$. Then, we have*

$$r \leq \frac{1}{2} - \frac{\lambda}{2e}\frac{\cosh(x_0)^{\frac{1}{\lambda}}}{x_0}$$

where x_0 is the unique positive solution of $x\tanh(x) = 2\lambda$.

Proof: Dividing up the bound of Theorem 6 by n, and using Lemma 2 yields the desired result. □

It seems that this asymptotic bound is slighty less precise than the bound obtained in [10]. For instance, for λ small we obtain $r \leq 0.5 - 0.35\sqrt{\lambda}(1+o(1))$ versus $r \leq 0.5 - 0.7\sqrt{\lambda}(1+o(1))$. For $\lambda = 0.5$ we get $r \leq 0.25$ versus $r \leq 0.07$.

Open Problem 3 *Develop analogous results for q-ary codes.*

7 Conclusion

We hope to have demonstrated in this article the wide range of applicability of the saddle point approximation in asymptotic problems of Information Theory and Combinatorial Coding Theory. Many other problems remain open. In particular many families of Lee codes have distance growing faster than n, and the asymptotic problems of Sections 4 and 5 are well worth studying for $n = o(r)$.

References

[1] J. Astola, "On the Asymptotic Behaviour of Lee codes," Discr. Appl. Math, Vol. 8, pp. 13-23 (1984).

[2] E.R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press (1984).

[3] H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann (1961).

[4] H.E. Daniels, "Saddlepoint Approximation in Statistics," Ann. Math. Stat., Vol. 25, pp. 631-650 (1954).

[5] P. Henrici, *Applied and Computational Analysis*, Wiley (1977).

[6] D. Gardy, *Bases de données, allocations aléatoires: quelques analyses de performances*, Thèse d'Etat, Orsay University (1989).

[7] I.J. Good, "Saddle point methods for the multinomial distribution," Ann. Math. Stat., Vol. 28, pp. 861-881 (1957).

[8] D.H. Greene, D.E. Knuth, *Mathematics for the analysis of algorithms*, Birkhäuser Verlag (1982).

[9] P. Solé, K. G. Mehrothra, "A Generalization of the Norse Bound to Codes of Higher Strength," IEEE Trans. Information Theory, IT-37, pp. 190-192 (1991).

[10] A. Tietäväinen, "An Upper Bound on the Covering Radius as a Function of the Dual Distance," IEEE Trans. Information Theory, IT-36, pp. 1472-1474 (1990).

[11] J. H. van Lint, *Introduction to Coding Theory*, Springer, Graduate Texts in Math. 86 (1982).