Saddle Point Techniques in Asymptotic Coding Theory

Danièle GARDY [*]
L.R.I., CNRS-URA 410,
Bât. 490, Université Paris XI,
91405 Orsay, France
&
Patrick SOLÉ [†]
Laboratoire I.3.S., CNRS-URA 1376,
Bât. 4, 250 rue Albert Einstein,
Sophia-Antipolis, 06560 Valbonne, France.

Abstract

We use asymptotic estimates on coefficients of generating functions to derive anew the asymptotic behaviour of the volume of Hamming spheres and Lee spheres for small alphabets. We then derive the asymptotic volume of Lee spheres for large alphabets, and an asymptotic relation between the covering radius and the dual distance of binary codes.

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 to get an asymptotic approximation of their coefficients involve complex analysis [3, 5], and in particular the method of steepest descent to estimate contour integrals.

The paper is organized as follows. We recall the analytic results that we need in Section 2. We rederive the classical estimate for the volume of Hamming spheres via the entropy function in Section 3, and give in Section 4 a simpler proof of an estimate of Astola [1] for the volume of the Lee spheres, for small alphabets of odd cardinality. We also derive a similar result when this cardinality is even. We present in Section 5 a new estimate for Lee spheres over large alphabets, which is expressed using a function not essentially more complicated than the binary entropy function. Finally we derive in Section 6 an asymptotic relation between the covering radius of a binary code and its dual distance.

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 interested in generating functions of the kind $\Phi(z) = f(z)^n g(z)$, and in their coefficients $[z^r]\{f(z)^n g(z)\}$ for large n and $r \sim \lambda n$.

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

[*] This work was partially performed while this author was visiting Brown University, Providence, R.I., U.S.A. The author also acknowledges the support of the PRC Mathématique-Informatique (CNRS) and of ESPRIT-II Basic Research Action No. 3075 (project ALCOM).

[†] This work was partially supported by the PRC C^3 (CNRS and MRT).

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 a function f

$$\Delta f(z) = zf'(z)/f(z) \qquad \text{and} \qquad \delta f(z) = (\Delta f)'(z)/z.$$

It can be shown that, when f is a power series with positive coefficients, then $\delta f(\rho) > 0$ (see for example [6, p.65]). 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] but is best given in the version of [7, p.868]:

Theorem 1 *Let f be a power series with real positive coefficients and non degenerate; assume that the equation $\Delta f(z) = (r+1)/n$ has a real positive solution ρ. If f is analytic in an open set including the disk of radius ρ and center the origin, then for large n and r, and with r/n restricted to an interval $[A, B]$ $(A > 0)$*

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

This result is easily extended to take into account a factor $g(z)$, as long as g does not introduce singularities closer to the origin than the saddle point:

Theorem 2 *Let f and g be non degenerate power series with positive coefficients. Assume that the equation $\Delta f(z) + \Delta g(z)/n = (r+1)/n$ has a real positive solution ρ. If f and g are analytic in an open disk including the circle of radius ρ and center the origin, then for large n and r with r/n restricted to an interval $[A, B]$ $(A > 0)$*

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

Proof: The proof of Theorem 2 is similar to that of Theorem 1 and to a method of Hayman [9][13, Ch.5]. For this reason we only give a sketch of the proof.

To approximate the integral $\int e^{h(z)}dz$, with $h(z) = n\log f(z) + \log g(z) - (r+1)\log z$, we first compute the saddle point ρ (or an approximate value), which is defined by $h'(z) = 0$. We then choose as integration path the circle of center 0 and radius ρ, and divide the integral in two parts. The first part comprises the values of $z = \rho e^{i\theta}$ which are close to ρ: $|\theta| < \alpha$, for some suitable small α. For these values, the function $h(\rho e^{i\theta})$ has a second order Taylor expansion with an error term $O(\theta^3)$; we plug this expansion into the integral, which we then extend to a gaussian integral of known value.

We next have to show that the part of the integral far from the saddle point ($\alpha \le |\theta| \le \pi$) is negligeable. But this follows from the fact that the function $|g(z)|$ is maximal on the real axis, that the function $|f(z)|$ is maximal on the real axis and nowhere else on the circle $\{z = \rho e^{i\theta}\}$, and that $|f(z)^n g(z)|$ decreases exponentially when n increases. □

In general, Theorems 1 and 2 are difficult to apply, because ρ is a function of n and r, and $f(\rho)^n$ is difficult to estimate. So, we shall use the following corollary.

Corollary 1 *Under the hypotheses of Theorem 2, with $r/n = \lambda$ and with $\Phi(z) = f(z)^n g(z)$,*

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

We can also extend Corollary 1 to use a simpler saddle point:

Corollary 2 *Corollary 1 is still valid if we use the simpler saddle point defined by $\Delta f(z) = r/n$.*

Proof: The points ρ, defined by $\Delta f(z) + \Delta g(z)/n = (r+1)/n$, and ρ_0, defined by $\Delta f(z) = r/n$, are such that $\rho_0 = \rho(1 + O(1/n))$. Hence $\log f(\rho_0) - \lambda\log(\rho_0) = \log f(\rho) - \lambda\log(\rho) + o(1)$. □

3 Hamming Spheres

Recall that the Hamming weight $W(\mathrm{x})$ of $\mathrm{x} = (x_1, \ldots, x_n) \in \mathbf{F}_q^n$ is $W(\mathrm{x}) = Card\{i \in [1, \ldots, n] | x_i \neq 0\}$. The Hamming sphere of radius r centered at $(0, \ldots, 0)$ is $\mathbf{B}_r = \{\mathrm{x} \in \mathbf{F}_q^n | W(\mathrm{x}) \leq r\}$; its volume is $|\mathbf{B}_r|$. The generating function for the volume of the Hamming spheres is $\Phi_n(z) = \sum_{r=0}^{n} |\mathbf{B}_r| z^r = (1+z)^n/(1-z)$. Let $f(z) = 1 + z$ and $g(z) = 1/(1-z)$; then $\Phi_n(z) = f(z)^n g(z)$. The function f is entire, with positive coefficients, and non-degenerate, and the function g has positive coefficients and a simple pole in 1. The following result can be derived by more elementary but also more tedious means.

Theorem 3 *Let $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ 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: To check that the function $\Phi_n(z)$ satisfies the assumptions of Theorem 2, we have to compare the singularity of g, which is 1, to the saddle point defined by the equation

$$\frac{z}{1+z} + \frac{z}{n(1-z)} = \frac{r+1}{n}.$$

This has for solution $\rho = \lambda/(1-\lambda)$, which is < 1 iff $\lambda < 1/2$. The result follows by Corollary 2. □

We leave as an exercise to the reader to derive an analogous result for q-ary codes (Cf. [12] Lemma 5.1.6 p.55).

4 Lee Spheres for Small Alphabets

Let $s = \lfloor q/2 \rfloor$ and $\mathbf{Z}_q = \{-s, -(s-1), \ldots, 0, \ldots, (s-1), s\}$. We recall that the Lee weight of $x \in \mathbf{Z}_q$ is

$$\begin{aligned} W_L(x) &= x \quad \text{if } x \geq 0; \\ &= -x \quad \text{if } x < 0. \end{aligned}$$

The Lee weight of $\mathrm{x} = (x_1, \ldots, x_n) \in \mathbf{Z}_q^n$ is $W_L(\mathrm{x}) = \sum_{i=1}^{n} W_L(x_i)$. The Lee sphere of radius r is $\mathbf{B}_r^L = \{\mathrm{x} \in \mathbf{F}_q^n | W_L(\mathrm{x}) \leq r\}$; its volume is $|\mathbf{B}_r^L|$. Then we know from [2, p.298] that the generating function $\Phi_{n,q}(z) = \sum_{r \geq 0} |\mathbf{B}_r^L| z^r$ can be evaluated as

$$\Phi_{n,q}(z) = \frac{f(z)^n}{1-z}$$

with

$$\begin{aligned} f(z) &= \quad 1 + 2\textstyle\sum_{i=1}^{s} z^i \qquad (q = 2s+1); \\ f(z) &= 1 + 2\textstyle\sum_{i=1}^{s-1} z^i + z^s \quad (q = 2s). \end{aligned}$$

Let

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

The following result was proved by Astola [1] using multinomial coefficients and Lagrange multipliers.

Theorem 4 *Let $q = 2s + 1$. Then $L(\tau, q) = 1 + \log_q(\alpha\rho^{\tau s})$, where $\alpha \geq 0$ and $\rho \geq 0$ are defined by the two equations*

$$\alpha(1 + 2\sum_{i=1}^{s} \rho^i) = 1 \qquad \text{and} \qquad \alpha\sum_{i=1}^{s} i\rho^i = \frac{\tau s}{2},$$

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

Our method allows us to get a new derivation of Astola's result (Theorem 5) when q is odd and to prove a similar result (Theorem 6) when q is even. The term ρ in Theorems 4 and 5 is the same (it is defined by the same equation), and we have the relation $\alpha = 1/f(\rho)$.

Theorem 5 *Let $q = 2s + 1$. If $\tau < (q+1)/(2q)$, then*

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

where ρ is the unique real positive solution of

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

and where $f(\rho) = (s\rho + s + 1)/(s(\rho\tau - \rho - \tau) + s + 1)$.

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 the first order ODE

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

The saddle point ρ satisfies the equation

$$2z\sigma'(z) = s\tau(1 + 2\sigma(z)).$$

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 τ comes from $\Delta f(1) > s\tau$, and ensures that the saddle point $\rho = (\Delta f)^{-1}(s\tau)$ is smaller than 1, the pole of g. □

Theorem 6 *Let $q = 2s$. If $\tau < 1/2$, then*

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

where ρ is the unique real positive solution of

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

and where $f(\rho) = (s\rho + s + 1 - \rho^s)/(s(\rho\tau - \rho - \tau) + s + 1)$.

Proof: Here $f(z) = 1 + 2\sigma(z) - z^s$, with $\sigma(z) = \sum_{i=1}^{s} z^i$ as above. The saddle point satisfies the equation

$$2z\sigma'(z) - sz^s = s\tau(1 + 2\sigma(z) - z^s).$$

As before, we get rid of $\sigma'(z)$ and get an expression for $\sigma(z)$, which gives readily the expression for $f(\rho)$. The bound on τ comes again from $\Delta f(1) > s\tau$. □

5 Lee Spheres for Large Alphabets

We note that, for $q \geq 2r + 1$:

$$[z^r]\{\Phi_{n,q}(z)\} = [z^r]\{\frac{(1 + 2\sum_{i\geq 1} z^i)^n}{1 - z}\} = [z^r]\{\frac{(1+z)^n}{(1-z)^{n+1}}\}.$$

The following result appears to be new or at least unpublished.

Theorem 7 *Let $V_{n,r}$ denotes the volume of the Lee sphere of radius r in $\mathbb{Z}_q^n$. When $q \geq 2r+1$ this quantity does not depend on q, and for large n and r/n going to λ ($\lambda > 0$), we get*

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

where

$$L_q(x) = x\log_q(x) + \log_q(x + \sqrt{x^2+1}) - x\log_q(\sqrt{x^2+1} - 1).$$

Proof: We have $V_{n,r} = [x^n]\{(1+z)^n/(1-z)^{n+1}\}$. The saddle point equation can be written as

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

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

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

It is easily checked that this quantity is always < 1. Hence the pole of g is not a problem and Corollary 1 gives the result. □

Using this result we obtain the analogues of the Hamming bound [2, p.299] and the Gilbert-Varshamov bound [2, p.321]:

Corollary 3 *Let $R(\lambda)$ denote the largest achievable rate of a family of codes of minimum Lee distance λn for large n, and such that $q \geq 2\lambda n + 1$. Then, for $0 \leq \lambda < q/e$ we have*

$$1 - L_q(\lambda) \leq R(\lambda) \leq 1 - L_q(\frac{\lambda}{2}).$$

Proof: We have the result for $\lambda \leq 2L_q^{-1}(1)$. But $L_q(x) = \log_q(2ex) + O(1/x^2)$ for large x; hence the solution of the equation $L_q(x) = 1$ for large q is $x = q/(2e)(1 + o(1))$.

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

Open Problem 2 *Study $V_{n,r}$ when n and r are both large but no longer proportional.*

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 [11]. A simpler power-sum approach was initiated in [10]. Here we derive an asymptotic version of Theorem 6 of [10], which we recall below:

Theorem 8 *Let C be a code of dual distance at least $2s+1$. Then its covering radius ρ is bounded from above by*

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

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

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 n and s large. Then $(1/n)\,\mu_s(n)^{1/2s}$ goes to $\lambda\cosh(x_0)^{1/\lambda}/(2ex_0)$ where x_0 is the positive solution of $x\tanh(x) = 2\lambda$.*

Proof: Here $f(z) = \cosh(\sqrt{z}/2)$ is entire with positive coefficients and non degenerate, so we apply Theorem 1. Letting $x = \sqrt{z}/2$, the saddle point equation can be written as

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

λ	Our bound	Tietäväinen's bound
.5	.249	0
.4	.276	0.010
.3	.306	0.042
.2	.342	0.100
.1	.388	0.200
.01	.465	0.400
.005	.475	0.429

Figure 1: Bounds for the covering radius ($\rho_0 = \lim \rho/n$)

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

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

Stirling's approximation yields easily

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

□

Theorem 9 *Let C be a code of length n, covering radius ρ, and dual distance at least $2s+1$. Assume n large, ρ/n having ρ_0 as a limit, and $s \sim \lambda n$. Then, we have*

$$\rho_0 \leq \frac{1}{2} - \frac{\lambda}{2e} \frac{\cosh(x_0)^{1/\lambda}}{x_0}$$

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

Proof: Dividing up the bound of Theorem 8 by n, and using Lemma 2 yields the desired result. □

Numerical computations show that this asymptotic bound is less precise than the bound $\rho_0 \leq 0.5 - \sqrt{\lambda(1-\lambda)}$ obtained in [11], although the bounds are in closer agreement for small λ. We give some results in Figure 1.

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 questions 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 that case. Theorems 1 and 2 are no longer valid as stated when n and r are both large but their ratio does not have a constant, non null, limit; any extension of the asymptotic results of this paper to such cases thus requires a similar extension of Theorems 1 and 2. We hope to present this in a forthcoming paper.

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, Université Paris-Sud, Orsay (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] W.K. Hayman, "A generalisation of Stirling's formula," Journal für die reine und angewandte Mathematik, Vol. 196, pp. 67-95 (1956).

[10] 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).

[11] 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).

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

[13] H.S. Wilf, *Generatingfunctionology*, Academic Press (1990).