Estimates for denominators of Pade approximants and applications to Diophantine equations (13rit174)

Michael Bennett (University of British Columbia),
Greg Martin (University of British Columbia),
Kevin O'Bryant (City University of New York)

April 28–May 5, 2013

1 Overview of the Field

The hypergeometric method of Thue and Siegel is a technique in Diophantine approximation that has proved to be widely applicable in number theory, ranging from classical results in Diophantine analysis (Thue and Thue–Mahler equations, unit equations) to much more analytic problems (gaps between k-free numbers). Despite being quite an old subject, the basic machinery underlying the approach (typically non-Archimedean valuations of off-diagonal Padé approximants) is not particularly well understood asymptotically.

2 Recent Developments, Open Problems, and Plan of Attack

The main objective of our BIRS Research in Teams week was to complete a long-standing program of Bennett to understand the non-archimedean asymptotics of Padé approximants to the binomial function. In particular, we want to handle the denominators of the rational numbers that can arise in the coefficients of these Padé approximants. To address these denominators, Chudnovsky [2, 3] introduced certain "characteristic numbers" Chr_n^m. These characteristic numbers can be written as an expression involving combinatorial information about elements a in the group $\mathbf{Z}/n\mathbf{Z}$, namely the distance between nearest elements (and, more generally, closely neighboring elements) among the first m multiples of a modulo n. The exact expression, however, assembles these distances in a weighted sense, namely as a certain sum of reciprocals that requires nontrivial analytic techniques to bound.

Chudnovsky did obtain an upper bound for these characteristic numbers, showing that $\mathrm{Chr}_n^m \ll m \log n$, which allowed him to employ fixed values of m in his arguments. In 2001, Bennett [1] conjectured the improved upper bound $\mathrm{Chr}_n^m \ll m \log \frac{n}{m}$; were this upper bound to be established, one could employ much larger values of m (having the same order of magnitude as n) and consequently open the door to substantial improvements in this subject.

We proposed to study the characteristic numbers Chr_n^m in detail. When n is prime, one can write

$$\mathrm{Chr}_n^m = \frac{1}{n-1} \sum_{a=1}^{n-1} \sum_{\alpha=1}^{m-1} -\frac{\Gamma'}{\Gamma}\left(\frac{d_{a,\alpha}}{n}\right) - (m-1)\left(\gamma + \frac{n \log n}{n-1}\right).$$

Here the quantities $d_{a,\alpha}$ measure how (un)evenly distributed are the first m multiples of a (mod n). By bringing in the theory of equidistribution of sequences modulo 1 (using tools such as the Erdős–Turan inequality), we had begun to make strides towards improving Chudnovsky's bound when $\frac{n}{m}$ is not too large.

This technique works well on all but the first few terms in the sum over α; we planned to apply combinatorial techniques (related to the continued fraction representation of $\frac{a}{n}$ and to the three-gaps theorem) to improve our bound for the terms with α small.

Our goal was to obtain explicit upper bounds upon these quantities that are relatively close to representing the "truth". In terms of applications, these bounds should enable us to dramatically improve virtually all the results in the literature appealing to these techniques (some dozen papers or more), including effectively producing a new proof of Gelfond's lower bounds for linear forms in two logarithms (see for example [8] for recent work along these lines) with better constants than anything to date.

3 Scientific Progress Made

The version of Padé approximation that we are improving uses polynomials $P_0(z), P_1(z), \ldots, P_{m-1}(z)$ with

$$P_0(z) + P_1(z)(1-z)^{1/n} + P_2(z)(1-z)^{2/n} + \ldots + P_{m-1}(z)(1-z)^{(m-1)/n} = z^\rho R(z) \qquad (1)$$

with ρ as large as the degrees of the P_i allow and R analytic around $z = 0$. By contour integration, one can [9, 3, 1] find formulas for the P_i and sharply control the size of R.

For number-theoretic applications, we need to multiply equation (1) by an integer that will clear the denominators of all of the coefficients of the P_i; call the smallest such multiplier Δ. Using a value for Δ that is unnecessarily large makes the remainder $\Delta z^\rho R(z)$ on the right-hand side unnecessarily large, and this is a significant source of loss in applications. Our work in BIRS in April–May was designed to remove this loss.

The coefficients of the P_i have factors that are ratios of Gamma functions evaluated at points with denominator n; the coefficients can be rewritten to have a denominator that is the product of the integers in a particular two-dimensional arithmetic progression. One way to bound Δ is simply to bound the sizes of each number in the two-dimensional arithmetic progressions and multiply them appropriately.

Chudnovsky [3] incorporated the observation that only primes in certain congruence classes can be divisors of Δ. By using asymptotic estimates on the number of primes in a congruence class, he was able to give a superior bound on Δ, provided that m is fixed (his work allows n and the degrees of the P_i to go to ∞). Our improvement over previous work lies partially in better effective estimates for primes in congruence classes, and mostly in better control over which power of each prime can divide some denominator.

Improved estimates for primes in residue classes are of independent interest. We are able to sharpen known results by appealing to a combination of recent arguments of Ford, Luca, and Moree [6] and of Dusart [4], improved zero-free regions for Dirichlet L-functions due to Kadiri [7], and massive computation of zeros of L-functions due to Platt [10]. The upshot of all this is that we are now able to obtain upper and lower bounds of the correct asymptotic orders for our non-archimedian estimates, something that was lacking in the earlier work of Bennett [1].

To precisely control the power of each prime that divides any denominator, it is sufficient [1] to control the quantity

$$V(n,m) = \frac{1}{n-1} \frac{1}{H(m-1)} \sum_{a=1}^{n-1} \sum_{\alpha=1}^{m-1} \frac{1}{d_{a,\alpha}}. \qquad (2)$$

Here n is a prime, $H(k) = \sum_{i=1}^{k} i^{-1}$ is the harmonic number, and $d_{a,\alpha}$ is the length of the shortest interval of integers that intersects $\alpha + 1$ of the congruence classes $\{0, a, 2d, \ldots, (m-1)a\} \pmod{n}$. At the end of our time at BIRS, our bound had the shape

$$V(n,m) \leq \frac{m}{n} + C \frac{\log\log n}{\log n},$$

at least when n is prime. Our first success at BIRS was to find the correct generalization of equation (2) to serve us when n is not prime.

The expression $V(n,m)$ is a weighted average, over all a and α, of the crucial quantities $d_{a,\alpha}$, whose values are extremely combinatorial in nature. We have had success in bounding $V(n,m)$ by breaking the summation in its definition into various regions according to whether α is small and whether $\frac{a}{n}$ is badly approximable by rational numbers of smaller height. As our bounds for each region improve (as happened multiple times during our week at BIRS), we needed to rebalance the regions in order to find the weak links. Further complicating the situation is that this balancing of the regions must depend on m, which in our applications is no longer fixed.

The results we have sketched here appear extremely technical. They do, however, enable us to make progress on a number of relatively classical Diophantine problems. By way of example, we can significantly sharpen work of Evertse [5], extending earlier results of Siegel on binomial Thue inequalities of the shape

$$|ax^n - by^n| \le c,$$

demonstrating that such inequalities possess at most a single large solution. Here, of fundamental importance for applications is that the definition of "large" is measured by an inequality of the shape

$$\max\{|ax^n|, |by^n|\} \ge c^{\kappa_n}.$$

Asymptotically, all previous work has had the property that $\lim_{n\to\infty} \kappa_n/n = 2$; we are able to relax this restriction to $\lim_{n\to\infty} \kappa_n/n = 1$.

4 Future Directions

The significant mysteries remaining are tied up with the behavior of the quantities $d_{a,\alpha}$ introduced by Bennett. The sizes of these combinatorial quantities are difficult to pin down, yet are of crucial importance to the expresion $V(n,m)$, most of all when α is small or when $\frac{a}{n}$ has a good rational approximation with small denominator. We have made good progress understanding the $d_{a,\alpha}$, particularly with new ideas targeted to these important ranges. However, we would still like to know the asymptotic size of $V(n,m)$, for all moduli n (whether prime or not) and for all ranges of m (whether large or not). To accomplish this goal, we would still need to study the $d_{a,\alpha}$ even further. The calculations when n is not prime are complicated enough that some technical issues regarding error terms remain hard to overcome (when m is very small); in some of those calculations, the constants are hard to make explicit as well.

It is important, for applications to Diophantine equations, that our final bounds be completely explicit; consequently, all of the tools that we employ in service to those final bounds must also be rendered into explicit forms. One of the major such tools is the asymptotically correct estimates for the number of primes in congruence classes. While at BIRS, we convinced ourselves of the existence of all the machinery necessary to carry out such estimates; explicit work of this nature, however, always requires thorough and patient implementation. Fortunately, tidy explicit estimates for the number of primes in congruence classes will be an invaluable tool for researchers all across analytic number theory. Therefore, one of our important upcoming tasks is to complete these state-of-the-art estimates and make them available for application to our own work and that of others.

Finally, once our results on $V(n,m)$ and hence the characteristic numbers Chr_n^m are optimized, we would like to make a comprehensive attempt to catalog the applications that will follow. There are over a dozen places in the literature where this method of Thue and Siegel is used; we want to look at all of these applications and determine when our tighter bounds on Chr_n^m yield significant improvements. These possibilities are quite exciting, and the best-case scenario is that some of these improvements would be in the form of groundbreaking and unprecedented theorems in Diophantine approximation.

References

[1] M.A. Bennett, Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$, *J. Reine Angew. Math.* **535** (2001), 1–49.

[2] G.V. Chudnovsky, Un système explicite d'approximants de Padé pour les fonctions hypergéométriques généralisées, avec applications à l'arithmétique, *C. R. Acad. Sci. Paris Sér. A–B* **288** (1979), no. 22, A1001–A1004.

[3] G.V. Chudnovsky, On the method of Thue-Siegel, *Ann. Math. II Ser.* **117** (1983), 325–382.

[4] P. Dusart, Estimates of $\theta(x; k, l)$ for large values of x, *Math. Comp.* **71** (2002), no. 239, 1137–1168.

[5] J.–H. Evertse, On the equation $ax^n - by^n = c$, *Compositio Math.* **47** (1982), 289–315.

[6] K. Ford, F. Luca, and P. Moree, Values of the Euler ϕ-function not divisible by a given odd prime, and the distribution of Euler–Kronecker constants for cyclotomic fields, *Math. Comp.* (to appear).

[7] H. Kadiri, Explicit zero-free regions for Dedekind zeta functions, *Int. J. Number Theory* **8** (2012), no. 1, 125–147.

[8] M. Laurent, M. Mignotte, and Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55** (1995), 285–321.

[9] K. Mahler, Ein Beweis des Thue–Siegelschen Satzes über die Approximation algebraischer Zahlen für binomische Gleichungen, *Math. Ann.* **105** (1931), 267–276.

[10] D.J. Platt, Computing degree 1 L-function rigorously, Ph.D. thesis, University of Bristol, 2011.