Chapter Four
Gelfond's Solution of Hilbert's Seventh Problem

(Revised January 2, 2011)

Before we consider Gelfond's, and then Schneider's, complete solutions to Hilbert's seventh problem let's look back and see what common elements we can find in Fourier's demonstration of the irrationality of e, Hermite's demonstration of the transcendence of e, and Gelfond's demonstration of the transcendence of e^{π}. The first, and most obvious, common feature these proofs share is that they are all proofs by contradiction–the value under consideration is assumed to be rational or algebraic and a contradiction is deduced from that assumption. The second common feature concerns the nature of the contradiction obtained–in each case the deduction leads to a small positive integer, more specifically an integer between 0 and 1. (This was used in Gelfond's proof to show $A_n = 0$ for n sufficiently large yet, as seen in the exercises from the previous chapter, Gelfond's proof could be restructured so that the proof's final contradiction is the existence of an integer between 0 and 1.)

In Fourier's proof this integer was produced through a truncation of the power series representation for the number e. Hermite obtains this contrarian integer through simultaneous good rational approximations to $e, e^2, \ldots, e^n$. Gelfond was led to this integer through an examination of the coefficients of a so-called Newton interpolation series to the function $e^{\pi z}$ In each case, the conclusion of the proof relied on establishing two facts about the integer that had been produced: That the integer is nonzero and that its absolute value is less than 1.

Yet these proof's all share another common feature that is only obvious once it is pointed out–each of these proofs are opportunistic in that they rely on a previously known, and explicit, series representation for the number e or the function e^z or the function $e^{\pi z}$. We will see that while both Gelfond and Schneider based their solutions to Hilbert's α^{β} problem on assuming the contrary of what the wished to establish they did not use previously studied functions. Instead, they each produced a new function that would allow them to exploit the assumed arithmetic nature of the value under consideration to reach the ultimate contradiction. And, although Gelfond and Schneider used it differently, each of the functions they produced depended on an application of the pigeonhole principle, which is more elegantly known as Dirichlet's box principle.

We begin by stating what Gelfond established (which is the third, equivalent version of the α^{β} portion of Hilbert's seventh problem we discussed in Chapter 1).

Theorem (Gelfond, 1933). *Suppose that α and β are nonzero algebraic numbers. If*

$$\frac{\log \alpha}{\log \beta} \tag{1}$$

is irrational then it is transcendental.

Before we look at Gelfond's application of the pigeonhole principle to produce an advantageous function let's look at an outline of his proof, which we will see could appear to be a bit convoluted. (This sketch, and the complete proof below, are slightly simplified versions of Gelfond's original argument. These were given by Hille in an exposition of Gelfond's argument for an English-speaking audience.)

STEP 1. This is Gelfond's point of departure from the earlier opportunistic transcendence proofs. Gelfond used the pigeonhole principle to find integers $c_{k\ell}$, not all zero, so that the function:

$$F(z) = \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} \alpha^{kz} \beta^{\ell z} = \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} e^{\log(\alpha)kz} e^{\log(\beta)\ell z}$$

has the property that $|F^{(t)}(0)|$ is small for a modest range of derivatives.

STEP 2. Note that any t the tth derivative of $F(z)$ has a particularly simple form:

$$F^{(t)}(z) = \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} \big(k \log \alpha + \ell \log \beta\big)^t e^{\log(\alpha)kz} e^{\log(\beta)\ell z}.$$

So when $F^{(t)}(z)$ is evaluated at $z = 0$ we obtain an expression:

$$\begin{aligned} F^{(t)}(0) &= \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} (k \log \alpha + \ell \log \beta)^t \\ &= (\log \beta)^t \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} (k \frac{\log \alpha}{\log \beta} + \ell)^t \end{aligned}$$

Thus, using the assumption that $\dfrac{\log \alpha}{\log \beta}$ is algebraic Gelfond would know that for each t,

$$(\log \beta)^{-t} F^{(t)}(0) = \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} (k \frac{\log \alpha}{\log \beta} + \ell)^t$$

is an algebraic number.

Each of the values $|F^{(t)}(0)|$ in STEP 1, is indeed so small that *if it is nonzero*, then the nonzero algebraic norm of the algebraic integer derived from $(\log \beta)^{-t} F^{(t)}(0)$ has absolute value less than 1. Thus Gelfond has actually found the original integer coefficients $c_{k\ell}$, not all zero, so that the function:

$$F(z) = \sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell} e^{\log(\alpha)kz} e^{\log(\beta)\ell z}$$

has the property that $F^{(t)}(0) = 0$ for a modest range of derivatives.

STEP 3. Here is where Gelfond's proof becomes iterative–it only appears to be convoluted until you see its structure. Gelfond used analysis, essentially a clever application of the Maximum Modulus Principle and then the Cauchy Integral Formula, to show that $|F^{(t)}(n)|$ is small for a modest range of integers and for slightly fewer derivatives than in STEP 1.

STEP 4. Again by taking the algebraic norm of the algebraic integer associated with each of the values

$$(\log\beta)^{-t}F^{(t)}(n) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}(k\frac{\log\alpha}{\log\beta}+\ell)\alpha^{kn}\beta^{\ell n}$$

Gelfond concludes that each of the values $|F^{(t)}(n)|$ is not only small but is equal to 0.

The conclusion of STEP 4 implies that the original function has a higher order of vanishing at $z = 0$ than had been discovered in STEP 2. This discovery implies that a certain system of equations, with an equal number of equations and unknowns, has a nonzero solution. Since $F(z) \neq 0$, because all of the coefficients $c_{k\ell}$ are not zero and the functions $e^{(\log\alpha)z}$ and $e^{(\log\beta)z}$ are algebraically independent, this implies that a certain Vandermonde matrix vanishes, which implies that the ratio $\dfrac{\log\alpha}{\log\beta}$ is rational (contrary to the hypothesis of the theorem).

Finding the advantageous function.

Before we give the precise sort of result Gelfond used to find coefficients $c_{k\ell}$, which yields what we called an advantageous function, let's just look at the general principle behind finding those coefficients. Suppose you have a linear form with real coefficients $a_1, a_2, \ldots, a_k$:

$$L(\vec{X}) = a_1X_1 + a_2X_2 + \ldots + a_kX_k.$$

Imagine that your goal is to find a nonzero integer vector $\vec{X}$, with *small* coordinates, so that $|L(\vec{X})|$ is also *small.* This is possible where the two senses of the word *small* are inversely related.

To find the vector $\vec{X} = (X_1, \ldots, X_k)$ consider the mapping from $\mathbf{Z}^k$ to $\mathbf{R}$ given by $\vec{n} \mapsto L(\vec{n})$, so

$$(n_1, n_2, \ldots, n_k) \mapsto a_1n_1 + a_2n_2 + \ldots + a_kn_k.$$

Take N to be a positive integer, then this mapping maps the set of integer vectors

$$\mathbf{N}(N) = \{(n_1, n_2, \ldots, n_k) : 0 \leq n_i \leq N \text{ for each } i\}$$

into an interval of the real line. The above set contains $(N+1)^k$ vectors and if we divide the interval of the real line containing the image of $\mathbf{N}(N)$ into fewer than $(N+1)^k$ subintervals, then, by the pigeonhole principle, two of the images will have to lie in the same subinterval: That is there will exist two vectors $\vec{X}_1$ and $\vec{X}_2$ in $\mathbf{N}(N)$ so that $L(\vec{X}_1)$ and $L(\vec{X}_2)$ lie in the same subinterval. If everything is set up correctly we than know that $|L(\vec{X}_1 - \vec{X}_2)| = |L(\vec{X}_1) - L(\vec{X}_2)|$ is *small*; note that the absolute values of the coordinates of the vector $\vec{X}_1 - \vec{X}_2$ will be at most N, as each of these vectors is an element of $\mathbf{N}(N)$.

We formalize the above discussion as a lemma:

Lemma. *Let $a_1, a_2, \ldots, a_k$ be real numbers and let $A = \max\{|a_i| : 1 \le i \le k\}$. Take any two positive integers N and ℓ so that $(N+1)^k > \ell$. Then there exist rational integers $n_1, \ldots, n_k$ with*

$$0 < \max\{|n_1|, \ldots, |n_k|\} \le N \tag{2}$$

and

$$|a_1n_1 + a_2n_2 + \ldots + a_kn_k| \le \frac{kAN}{\ell}. \tag{3}$$

Proof. The lemma follows from the outline above. The only subtlety is to let $-T$ denote the sum of the negative numbers among the a_i and let S denote the sum of the positive numbers among the a_i. Then the mapping $\vec{n} \mapsto L(\vec{n})\big)$ maps the vectors $\mathbf{N}(N)$ into the real interval $[-kNT, kNS]$, which we subdivide into ℓ intervals of equal length.

Note: There is one trade off between which of the two inequalities (2) or (3) you wish to have in a simpler form, and another between which of them you wish to be smaller. For example, since the proof of the above lemma requires that $(N+1)^k > \ell$, by way of illustration take $\ell = N^k$. Then (3) offers the upper bound:

$$|a_1n_1 + a_2n_2 + \ldots + a_kn_k| \le \frac{kA}{N^{k-1}}.$$

So, as we might expect, the smaller we want the linear form to be the larger we might have to take the integers $n_1, n_2, \ldots, n_k$. Or, put differently, the larger we allow the integers $n_1, \ldots, n_k$ to be the smaller we can make the linear form.

The above simple argument concerning a single linear form with real coefficients can be extended to include the case where the coefficients are complex numbers (each form is viewed as two forms, one involving the real parts of the coefficients and the other the imaginary parts of the coefficients) and to simultaneously include several linear forms (the mapping will then be into $\mathbf{R}^m$, for the appropriate m). Instead of subdividing the image into intervals you subdivide it into $m-$dimensional cubes. The point is to have fewer cubes than image points so two points map into the same cube. This leads to the following result, which we state in a readily applicable form.

Theorem. *Let $a_{ij}, 1 \le i \le n$ and $1 \le j \le m$ be complex numbers, with $n > 2m$. Consider the linear forms*

$$L_j(\vec{X}) = a_{1j}X_1 + a_{2j}X_2 + \ldots + a_{nj}X_n, \text{ for } 1 \le j \le m.$$

Let X be any positive number. Then there exist n rational integers, $N_1, N_2, \ldots, N_n$, not all zero, so that for each j,

$$|a_{1j}N_1 + a_{2j}N_2 + \ldots + a_{nj}N_n| \leq X$$

with

$$\max_{1\leq i\leq n}\{|N_i|\} \leq [\frac{2^{3/2}nA}{X}]^{\frac{2m}{n-2m}},$$

where $\max\{a_{ij}|\} \leq A$.

Return to Gelfond's Proof.

Although Gelfond did not formalize the information about his function that his iterative application of basic analysis and algebra led to, it helps clarify his proof if we codify the result Gelfond obtained in the Steps 1 through 4 (as outlined above) into a single proposition.

Proposition. *Suppose α and β are nonzero algebraic numbers and that $\dfrac{\log\alpha}{\log\beta}$ is an irrational algebraic number. If K is a sufficiently large positive integer then there exist rational integers $c_{k\ell}, -K \leq k, \ell \leq K$ with* $\max\{|c_{k,\ell}|\} \leq 3^{K^2}$ *so that the function*

$$F(z) = P(\alpha^z, \beta^z) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}\alpha^{kz}\beta^{\ell z} \tag{4}$$

satisfies

$$F^{(t)}(0) = 0 \textit{ for } 0 \leq t \leq K^{5/2}. \tag{5}$$

Sketch of proof. As we qualitatively discussed in our brief look at Steps 1 and 2, above, Gelfond sought to find integers $c_{k\ell}$, not all zero, so that the function:

$$F(z) = P(\alpha^z, \beta^z) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}\alpha^{kz}\beta^{\ell z}$$

has the property that the algebraic numbers $|(\log\beta)^{-t})F^{(t)}(0)|$, for $0 \leq t < T$, have algebraic integer equivalents whose algebraic norms are less than 1 in absolute values. We will leave the parameters K and T unspecified until we see what is required of them for this proof to succeed.

In order to find the coefficients $c_{k\ell}$, the expression $(\log\beta)^{-t}F^{(t)}(0)$, for each t, $0 \leq t < T$, is replaced by a linear form. Specifically, we introduce the notation $\vec{C}$ for the vector of coefficients $(\ldots, c_{k\ell}, \ldots)$ and consider the linear forms

$$L_t(\vec{C}) = (\log\beta)^{-t}F^{(t)}(0) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}(k\frac{\log\alpha}{\log\beta} + \ell)^t. \tag{6}$$

This is a system of T linear forms with complex coefficients $(k\frac{\log\alpha}{\log\beta}+\ell)^t$ and $(2K+1)^2$ unknowns $c_{k\ell}$.

We may apply the earlier theorem to find the unknown integers $c_{k\ell}$ if we have

$$(2K+1)^2 > 2T. \tag{7}$$

Before we attempt to specify K or T, let's assume that the above inequality holds and see what we need to obtain an appropriate function. We know from the above theorem concerning several linear forms that for any $X>0$, we can find integers $c_{k\ell}$, not all zero so that

$$\big|L_t(\vec{C})\big| < X, \text{ for each } t,$$

where we have the estimate for $C=\max\{|c_{k\ell}|\}$ of,

$$C \le \left(\frac{2^{3/2}(2K+1)^2\big(K(\big|\frac{\log\alpha}{\log\beta}+1\big|)\big)^{T-1}}{X}\right)^{\frac{2T}{(2K+1)^2-2T}}. \tag{8}$$

This is a rather intimidating inequality, so do not stare at it too long, but simply note that, imagining T and K as having been already chosen, it does offer a relationship between C and X. This relationship is critical at the next step of the proof, where we take an algebraic norm.

If we let δ denote a denominator for the algebraic number $\dfrac{\log\alpha}{\log\beta}$ then $\delta^t L_t(\vec{C})$ is an algebraic integer whose norm is easily estimated, at least in terms of our as-yet undetermined entities $K, T, X,$ and C. Let $\eta_1 = \dfrac{\log\alpha}{\log\beta}, \eta_2, \ldots, \eta_d$ denote the conjugates of $\dfrac{\log\alpha}{\log\beta}$ and, temporarily, use notation stressing the dependence of $\delta^t L_t(\vec{C})$ on $\dfrac{\log\alpha}{\log\beta}$ by writing, $\delta^t L_t(\vec{C}) = P_t(\dfrac{\log\alpha}{\log\beta})$. We note that $P_t(x)$ is the integral polynomial

$$P_t(x) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}(k\delta x + \delta\ell)^t.$$

Therefore, *if* $P_t(\dfrac{\log\alpha}{\log\beta}) \ne 0$ the expression

$$N_t = P_t(\frac{\log\alpha}{\log\beta})\prod_{j=2,\cdots,d} P_t(\eta_j). \tag{9}$$

is a nonzero integer.

The first factor in (9) is already known to be relatively small (once we solve for the coefficients $c_{k\ell}$):

$$\big|P_t(\frac{\log\alpha}{\log\beta})\big| = \big|\delta^t L_t(\vec{C})\big| < \delta^t X.$$

Each of the other factors may be estimated in terms of the other unspecified parameters. To assist us in writing down this estimate we let $c_0 = \max\{|\delta|, |\eta_2|, \ldots, |\eta_d|\}$. Then,

$$\big|P_t(\eta_j)\big| \le (2K+1)^2|\delta|^t(K(|\eta_j|+1))^t C \le c_0^t K^{T+3} C \le K^{3/2T} C,$$

where each of these two inequalities holds if K is sufficiently large.

Therefore, for each $t,\ 0 \le t < T$,

$$\big|N_t\big| < X \times C^{d-1} \times K^{2T}.$$

If we ignore the appearances of K and T, which will be chosen momentarily, we see that in order to have $\big|N_t\big| < 1$, so we can conclude that each of the derivatives $F^{(t)}(0) = 0$, we need the product $X \times C^d$ to be small.

Step 3. To uncover a final bit of information about the relationship between C and the basic parameters of K and T that allows Gelfond's proof to go through, we look at his application of the Maximum Modulus Principle. Gelfond employed a theorem due to Jensen, whose proof relied on the Maximum Modulus Principle, but it is possible to simply appeal to that principle.

Let a be a complex number with $|a| = K^{2/3}$ for which $|F(a)| = \max_{|\zeta|=K^{2/3}}\{|F(\zeta)|\}$. The function $\frac{F(z)}{z^{T-1}}$ is entire, because the parameters will be chosen so the $|N_t| < 1$, so $F(z)$ will have a zero of order $T-1$ at $z = 0$. Therefore

$$\big|\frac{F(a)}{a^{T-1}}\big| \le \max_{|\zeta|=K}\{\big|\frac{F(\zeta)}{\zeta^{T-1}}\big|.$$

Since

$$F(z) = P(\alpha^z, \beta^z) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}\alpha^{kz}\beta^{\ell z}$$

we have the estimate

$$\max_{|\zeta|=K}\{\big|F(\zeta)\big|\} \le (2K+1)^2 C \max_{|\zeta|=K}\{\big|\alpha^{K\zeta}\beta^{K\zeta}\big|\} \le (2K+1)^2 C e^{\max\{|\log\alpha|, |\log\beta|\}K^2}.$$

It follows that

$$\big|F(a)\big| \le (2K+1)^2 C e^{\max\{|\log\alpha|,|\log\beta|\}K^2}\left(\frac{K^{2/3}}{K}\right)^{T-1} \le (2K+1)^2 C e^{\max\{|\log\alpha|,|\log\beta|\}K^2 - \frac{1}{3}(T-1)\log K},$$

which is a quantity we want to be small.

Thus it is a fairly delicate thing to balance all of these requirements on $K, T, X,$ and C. By looking at these conditions Gelfond/Hille gave the choices, in terms of the free parameter K, of:

$$T = [K^2\frac{\log\log K}{\log K}] \quad X = \exp\left(-cK^2\frac{\log K}{\log\log K}\right) \tag{10}$$

where the constant c can be seen to only depend on α, β and α^β. It follows from (8) that we can take as an estimate for the coefficients $C = 3^{K^2}$. (Note that with these choices, by allowing the coefficients to be fairly large, we are forcing the absolute values on the linear forms to be very small.)

With the above choices it is still a daunting matter to conclude that there are integers $c_{k,\ell}$, not all zero, with $\max\{|c_{k,\ell}|\} \le 3^{K^2}$ so that $F(z)$ satisfies

$$F^{(t)}(0) = 0 \text{ for } 0 \le t < T. \tag{11}$$

And moreover, by the above application of the Maximum Modulus Principle, we already know that for K sufficiently large

$$\max_{|\zeta|=K^{2/3}}\{|F(\zeta)|\} \le e^{-\frac{1}{6}K\log\log K}.$$

Completion of Step 3. We now apply the Cauchy Integral Formula to show that $|F^{(t)}(z)|$ is small for a modest range of integers t for all z in a fairly large disc. (In Step 4 we will then use an algebraic norm to find that $F(z)$ has a fairly large order of vanishing at a range of integers.)

Consider the integral representation of $F^{(t)}(z_0)$ where we will take $|z_0| \le (1/2)K^{2/3}$,

$$F^{(t)}(z_0) = \frac{t!}{2\pi i}\int_{|\zeta|=K^{2/3}} \frac{F(\zeta)d\zeta}{(\zeta - z_0)^{t+1}}.$$

It follows that for K sufficiently large

$$|F^{(t)}(z)| < e^{-\frac{1}{12}K^2\log\log K} \text{ for } |z| \le \frac{1}{2}K^{2/3},\ 0 \le t \le \frac{K^2}{\log K}.$$

Then for any integer n, $-[\frac{1}{2}K^{2/3}] \le n \le [\frac{1}{2}K^{2/3}]$ the algebraic values

$$(\log\beta)^{-t}F^{(t)}(n) = \sum_{k=-K}^{K}\sum_{\ell=-K}^{K} c_{k\ell}(k\frac{\log\alpha}{\log\beta} + \ell)\alpha^{kn}\beta^{\ell n}$$

satisfy

$$\left|(\log\beta)^{-t}F^{(t)}(n)\right| < e^{-\frac{1}{24}K^2\log\log K} \text{ for } 0 \le t \le \frac{K^2}{\log K},$$

provided K is sufficiently large.

Step 4. An application of the *algebraic norm idea* implies that each of the algebraic values above equals zero. Therefore $F(z)$ has a zero at each integer n, $-[\frac{1}{2}K^{2/3}] \le n \le [\frac{1}{2}K^{2/3}]$ to order at least $\dfrac{K^2}{\log K}$. Another application of the Maximum Modulus Principle followed by an application of the Cauchy Integral Formula completes the proof of the proposition. We leave these details to the dedicated reader (for details see Hille's paper [Hi]).

The conclusion of Gelfond's solution

The above proposition tells us that $F^{(t)}(0) = 0$ for $0 \leq t \leq K^{5/2}$. We translate this conclusion into a system of equations

$$\sum_{k=-K}^{K} \sum_{\ell=-K}^{K} c_{k\ell}(k\frac{\log\alpha}{\log\beta} + \ell)^t = 0, \ 0 \leq t \leq K^{5/2}$$

Since this system of equations has a non-zero solution, namely the $(2K+1)^2$ coefficients $c_{k\ell}$, we know that any $(2K+1)^2-$rowed determinant of the matrix associated with the above system of equations must vanish. In particular,

$$\det \left| \left(k\frac{\log\alpha}{\log\beta} + \ell \right) \right| = 0, \ \ -K \leq k, \ell \leq K, \ 0 \leq t \leq 4K(K+1) = (2K+1)^2 - 1.$$

The above determinant is a Vandermonde determinant, so it vanishes if and only if two of its columns are equal. This is the same as the condition that for two pairs of integers $(k,\ell) \neq (k',\ell')$, $k\dfrac{\log\alpha}{\log\beta} + \ell = k'\dfrac{\log\alpha}{\log\beta} + \ell'$, which implies that $\dfrac{\log\alpha}{\log\beta} = \dfrac{\ell - \ell'}{k' - k}$ is a rational number, contrary to Hilbert's, and Gelfond's hypothesis.

Preliminaries to Schneider's solution: Siegel's Lemma

Schneider's solution to Hilbert's seventh problem appeared within a few months of Gelfond's. (The story goes that Schneider learned of Gelfond's solution the day he submitted his own paper for publication.) Like Gelfond's proof, Schneider's depended on an application of the pigeonhole principle, elementary complex analysis, and the fundamental fact that the algebraic norm of a nonzero algebraic integer is a nonzero rational integer. However, Schneider did not apply the pigeonhole principle to solve a system of *inequalities*, and then show that these inequalities implied the vanishing of a function at certain points (with multiplicities). Rather, he directly solved a system of *equalities*, indeed a system of homogeneous linear equations. This allowed him to find an entire function with prescribed zeros, without having to iterate the use of an analytic estimate and of algebraic norms. (This idea has been attributed to Schneider's thesis advisor, C.L. Siegel (1929), and it can even be traced back to Axel Thue (1909).)

Before we explain Schneider's use of the pigeonhole principle we state a proposition which follows from that application. We will see that the deduction of this proposition is significantly more straightforward than the deduction of the analogous proposition in Gelfond's solution, even if its statement is not.

Proposition. *Suppose α and β are algebraic numbers with $\alpha \neq 0, 1$ and β irrational. Further assume that α^β is algebraic and let $d = [\mathbf{Q}(\alpha, \beta, \alpha^\beta) : \mathbf{Q}]$. Let m be a positive integer and put $D_1 = [\sqrt{2d}m^{3/2}]$ and $D_2 = [\sqrt{2d}m^{1/2}]$. Then if m is sufficiently large there exist rational integers $c_{k\ell}$, $0 \leq k \leq D_1 - 1, 0 \leq$*

$\ell \leq D_2 - 1$, *not all zero, such that the function*

$$F(z) = \sum_{k=0}^{D_1-1} \sum_{\ell=0}^{D_2-1} c_{k\ell} z^k \alpha^{\ell z} \tag{12}$$

satisfies

$$F(a + b\beta) = 0 \text{ for } 1 \leq a, b \leq m. \tag{13}$$

Moreover, there exists a constant $c_0 = c_0(\alpha, \beta)$ *so that the integers* $c_{k\ell}$ *satisfy*

$$0 < \max |c_{k\ell}| \leq c_0^{m^{2/3} \log m}. \tag{14}$$

Before we prove this proposition we note how it differs in two significant ways from Gelfond's proposition. First, the function vanishes at several points, and, second, there is no reference to the derivatives of the function. We will see that, because of this later observation, Schneider's method can be applied to some problems that are not immediately approachable by Gelfond's method.

The proof of this proposition depends on an elementary result to guarantee the existence of the unknown coefficients $c_{k\ell}$.

Suppose we wish to find a nonzero integral solution to the homogeneous system of M linear equations in N unknowns given by

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \cdots + \ a_{1N}X_N &= 0 \\ a_{21}X_1 + a_{22}X_2 + \cdots + \ a_{2N}X_N &= 0 \\ &\vdots \\ a_{M1}X_1 + a_{M2}X_2 + \cdots + a_{MN}X_N &= 0 \end{aligned}$$

where the coefficients a_{mn} are *integers*, not all equal to 0.

The matrix of coefficients (a_{mn}) may be viewed as a mapping from $\mathbf{R}^N$ to $\mathbf{R}^M$ so basic linear algebra tells us that if $N > M$ then there is a nonzero vector in the mapping's kernel, thus there is a *real* solution to the above system of equations. But the result we seek is that if $N > M$ there are *integral* solutions to this system of equations whose absolute values may be bounded from above. We will see that this bound will depend only on M, N, and the absolute values of the coefficients a_{mn}. It is perhaps surprising that the deduction of this result is no more difficult than the deduction of result Gelfond employed.

We start with the notation $A = \max\{|a_{mn}| : 1 \leq m \leq M,\ 1 \leq n \leq N\}$. We want to use the system of equations to map integral vectors in $\mathbf{Z}^N$ into $\mathbf{Z}^M$, so we consider the $M \times N$ matrix

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} & \dots & a_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ a_{M1} & a_{M2} & \dots & a_{MN} \end{pmatrix}.$$

Then we are searching for a nonzero vector

$$\vec{X} = \begin{pmatrix} X_1 \\ \vdots \\ X_N \end{pmatrix} \in \mathbf{Z}^N$$

satisfying $\mathbf{A}\vec{X} = \vec{0}$, or equivalently, $\vec{X}$ is a nonzero solution to the system of equations above.

Suppose we take a cube of vectors $\mathcal{D}$ in $\mathbf{Z}^N$ and using the matrix $\mathbf{A}$, map them all into a rectangular box of vectors $\mathcal{R}$ in $\mathbf{Z}^M$. If there are fewer integral vectors in the range set $\mathcal{R}$ than in the domain set $\mathcal{D}$, then there must exist two *distinct* integer vectors $\vec{x_1}$ and $\vec{x_2}$ in $\mathcal{D}$ that get mapped to the *same* vector in $\mathcal{R}$. That is, $\mathbf{A}\vec{x_1} = \mathbf{A}\vec{x_2}$. Thus we see that $\vec{X} = \vec{x_1} - \vec{x_2}$ is a *nonzero* integer solution to $\mathbf{A}\vec{X} = \vec{0}$. Moreover, since the vectors $\vec{x_1}$ and $\vec{x_2}$ are both from the domain cube $\mathcal{D}$, we can bound the size of the largest component of the solution vector $\vec{x_1} - \vec{x_2}$.

To carry this out we let $X \geq 1$ be an integer and define the N-dimensional domain cube $\mathcal{D}(X)$ by

$$\mathcal{D}(X) = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} \in \mathbf{Z}^N : 0 \leq x_n \leq X \text{ , for all } n = 1, 2, \ldots, N \right\}.$$

$\mathcal{D}(X)$ contains $(1+X)^N$ vectors.

The matrix $\mathbf{A}$ maps $\mathcal{D}(X)$ into an easily described subset of $\mathbf{Z}^M$. The description of this set is simplified if for any integer k we put $k^+ = \max\{0, k\}$ and $k^- = \max\{0, -k\}$. We can then define the appropriate set by

$$\mathbf{R}(X) = \left\{ \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_M \end{pmatrix} \in \mathbf{Z}^M : -X \sum_{n=1}^{N} a_{mn}^- \leq y_m \leq X \sum_{n=1}^{N} a_{mn}^+, \ 1 \leq m \leq M \right\}.$$

It is easy to verify that $\mathbf{A}(\mathcal{D}(X)) \subseteq \mathbf{R}(X)$. A calculation shows that the cardinality of $\mathbf{R}(X)$ is at most $(1 + XAN)^M$, where we recall that $A = \max\{|a_{mn}|\}$.

By the pigeonhole principle, if there are more integral vectors in $\mathcal{D}(X)$ than there are integral vectors in $\mathbf{R}(X)$ then $\mathbf{A}$ must map two vectors to the same vector. Explicitly, if

$$(1+X)^N > (1 + XAN)^M, \tag{15}$$

then $\mathbf{A}$ will map two distinct vectors $\vec{x_1}, \vec{x_2} \in \mathcal{D}(X)$ to the same vector in $\mathbf{R}(X)$. Thus we have that $\mathbf{A}(\vec{x_1} - \vec{x_2}) = \vec{0}$, where $\vec{x_1} - \vec{x_2}$ is a *nonzero* integer vector. Moreover, each coordinate of both $\vec{x_1}$ and $\vec{x_2}$ is an element of the set $\{0, 1, \ldots, X\}$, so the maximum absolute value of the difference of any two of their coordinates must be less than or equal to X.

We are naturally led to the following question: Given that condition (15) must hold for us to apply the pigeonhole principle we next seek the smallest possible X that satisfies that condition as this will lead to a good estimate for the size of the solutions to our original system of equations. It can be shown, and it is an exercise below to do so, that given positive integers A, M, and N, with $N > M$, the value

$$X = \left[(AN)^{\frac{M}{N-M}}\right], \tag{16}$$

suffices.

The above discussion establishes the following lemma that we apply in the next chapter to establish the above proposition we are attributing to Schneider.

Theorem (Siegel's Lemma). *Let* $\mathbf{A} = (a_{mn})$ *be a nonzero* $M \times N$ *matrix having integer entries and let* $A = \max\{|a_{mn}| : 1 \leq m \leq M,\ 1 \leq n \leq N\}$. *Assume* $A \geq 1$. *If* $N > M > 0$ *then there exists a nonzero vector*

$$\vec{X} = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_N \end{pmatrix} \in \mathbf{Z}^N,$$

with $\max\{|X_1|, \ldots, |X_N|\} \leq (AN)^{\frac{M}{N-M}}$, *satisfying*

$$\mathbf{A}\vec{X} = \vec{0}. \tag{17}$$

Exercises

1. Let $a_1, a_2, \ldots, a_n$ be complex numbers.

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \ldots & a_n^{n-1} \end{pmatrix}.$$

Show that the determinant of the above matrix, a so-called Vandermonde determinant, equals 0 if and only if $a_i = a_j$ for some $i \neq j$.

2. Can Gelfond's Proposition be deduced from a direct application of Siegel's Lemma (why or why not)?

3. Verify that with the choices of parameters (10) the inequality (8) allows us to assume that $C = 3^{K^2}$, provided K is sufficiently large.

4. Did Gelfond use his assumption that $\frac{\log \alpha}{\log \beta}$ is algebraic in Step 1 of his proof. If so, how?