Math 2^8: The Theory of Error-Correcting Codes

The asymptotic impossibility of nearly-extremal codes

Recall that we've fixed power series $F = F_0^t = 1+O(q)$ and $\Delta = q+O(q^2)$ and an integer $a \in [0,t)$, and for every positive integer m defined W_m to be the unique power series of the form $W_m = F_0^a P(F,\Delta) = 1 + O(q^{m+1})$ with P_m some homogeneous polynomial of degree m. We found that the q^{m+1} coefficient N_{m+1} of W_m is $(tm+a)/(tm+t)$ times the q^{-1} coefficient of $F_0^{-a}F'/\Delta^{m+1} = aF_0'F_0^{t-1-a}/\Delta^{m+1}$, where $F' = dF/dq$. We deduced that if F_0 has nonnegative coefficients, and $1/\Delta$ has positive q^k coefficient for all $k \geq -1$, then $N_{m+1} > 0$. In our setting these power series also satisfy the conditions we gave for N_{m+1} to have an asymptotic expansion of the form

$$N_{m+1} \sim \frac{1}{\sqrt{m}}\Delta(q_0)^{-m}\left(\alpha_0 + \frac{\alpha_1}{m} + \frac{\alpha_2}{m^2} + \cdots\right),$$

where q_0 is the positive number at which Δ is minimal (e.g. $q_0 = 1/5$ for the F, Δ that arise for Type II codes), and $\alpha_0 > 0$. We next give a formula for N_{m+2} that shows that under the same hypotheses $N_{m+2}/N_{m+1} = O(1) - c_0 m$ for some $c_0 > 0$, namely the constant coefficient of $1/\Delta$ (which is minus the q^2 coefficient of Δ). In particular $N_{m+2} < 0$ for m sufficiently large, so W_m cannot be a weight enumerator or theta function.

We start as before by setting $z = \Delta/F = q + O(q^2)$ and expanding $1/(F_0^a F^m)$ in powers of z as $\sum_{k=0}^{\infty} b_k z^k$ to find that

$$\frac{1 - W_m}{F_0^a F^m} = \sum_{k=m+1}^{\infty} b_k z^k.$$

We noted already that $N_{m+1} = -b_{m+1}$. To find N_{m+2} we must determine b_{m+2}. We again write it as a residue at $z = 0$, this time of $(1/(F_0^a F^m))\,\frac{dz}{z^{m+3}}$ (with an extra factor of z in the denominator), and use invariance of the residue and integration by parts to find that $-b_{m+2}$ is $(tm+a)/(tm+2t)$ coefficient of $F_0^{t-a}F'(q)/\Delta^{m+2}$. Using again the example of $\mathcal{G}_{24}$, we compute

$$\frac{F_0^{t-a}F'(q)}{\Delta^{m+1}} = \frac{(42+6q)F_0^5}{\Delta^3} = 42q^{-3} + 3450q^{-2} + 121578q^{-1} + 2416506 + 30193194q + \cdots$$

and so $-b_3 = \frac{3}{9}121578 = 40526$, which is confirmed by direct computation. In particular, $-b_{m+2}$ is asymptotic to a constant positive multiple of $-b_{m+1}$ (the multiplier being the value of F/Δ at q_0).

But N_{m+2} is not simply $-b_{m+2}$, because $-b_{m+1}$ contributes too, multiplied by the q^{m+2} coefficient of $F_0^a F^m z^{m+1}$. (In our example that's

$$Fz^2 = \Delta^2/F = \frac{(1 - 4q + O(q^2))^2}{1 + 42a + O(q^2)} = 1 - 50q + O(q^2),$$

and $40526 - 50 \cdot 759$ does come to 2576, the number of weight-12 codewords ("[umbral] dodecads") of $\mathcal{G}_{24}$.) In general, the q^{m+2} coefficient of $F_0^a F^m z^{m+1}$ is the q coefficient of

$$q^{-(m+1)}F_0^a F^m z^{m+1} = \frac{F_0^a\Delta}{q}(\Delta/q)^m,$$

which is a constant plus m times the q^2 coefficient of Δ, which as we already observed is $-c_0 < 0$. So we've proven that $N_{m+2} = (-c_0 m + O(1))N_{m+1} < 0$ for large m.

Now suppose we fix some $j > 0$ and relax the extremality condition by allowing power series of the form $W = F_0^a P(F,\Delta) = 1 + O(q^{m+1-j})$, i.e. adding to W_m an arbitrary linear combination of the j monomials $F^h\Delta^{m-h}$ with $0 \leq h < j$. I claim that even then one of the coefficients $N_{m+1-j}, N_{m+2-j}, \ldots, N_{m+1}, N_{m+2}$ is bound to be negative for m large enough. We do this by finding the linear relation $\sum_{i=0}^{j+1}\gamma_i N_{m+2-i} = 0$ that any such power series must satisfy, and showing that for large enough m the coefficients γ_i are all positive by calculating $\gamma_i = (c_0 m)^i/i! + O(m^{i-1})$. This in turn follows from our estimates for N_{m+1} and N_{m+2} together with the observation that in each monomial $F^h\Delta^{m-h}$ the q^{m+2-i} coefficient is $(-c_0 m)^{h+2-i}/(h+2-i)! + O(m^{h+1-i})$ for each $i = 0, 1, \ldots, h+2$ (and the fact that for each row of Pascal's triangle other than the zeroth row the alternating sum vanishes). This completes the proof of the Mallows-Odlyzko-Sloane theorem of 1975.