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

"Linear programming" (LP) bounds II

Fix q and n, and let $\{K_i\}_{i=0}^n$ be the system of Krawtchouk orthogonal polynomials with these parameters. We saw that if $P = \sum_{j=0}^n a_j K_j$ is a linear combination of with nonnegative coefficients a_j, such that $a_0 > 0$ and $P(x) \le 0$ for all $x \ge d$, then any code in A^n (with $|A| = q$) that has minimum distance at least d contains at most $P(0)/a_0$ words. We next use the Darboux-Christoffel formula to construct such P that gives the best asymptotic upper bound known as $n \to \infty$ for many choices of q and $\delta = d/n$.

Recall that the Darboux-Christoffel formula is

$$\sum_{j=0}^{i} \frac{1}{h_j} K_j(x) K_j(y) = \frac{1}{h_i} \frac{l_i}{l_{i+1}} \frac{K_i(y)K_{i+1}(x) - K_{i+1}(y)K_i(x)}{x - y},$$

where l_j is the leading coefficient of K_j and $h_j = \langle K_j, K_j \rangle$; we've seen already that $h_j = \binom{n}{j}(q-1)^j$, and that $l_j = (-q)^j/j!$ (which in turn implies $l_i/l_{i+1} = -(i+1)/q$). We shall take

$$P(x) = -\frac{(K_i(y)K_{i+1}(x) - K_{i+1}(y)K_i(x))^2}{x - y},$$

so that $P(x) \le 0$ for $x \ge y$ (note the minus sign before the fraction). We choose y as follows: for each $j > 0$ let ρ_j be the smallest root of K_j, so by the interlacing property $\rho_1 > \rho_2 > \rho_3 > \cdots$, and we saw that $\rho_1 = (1 - \frac{1}{q})n$. Then we shall take y such that $\rho_{i+1} < y < \rho_i$, with the specific choice to be made next page. We shall show that for such y our P is a nonnegative combination of the K_j, and evaluate a_0 to compare it with $P(0)$.

By Darboux-Christoffel

$$P(x) = \frac{i+1}{q}(K_i(y)K_{i+1}(x) - K_{i+1}(y)K_i(x)) \sum_{j=0}^{i} \frac{h_i}{h_j} K_j(y)K_j(x).$$

By our choice of y and the interlacing property, $K_{i+1}(y) < 0$ and $K_j(y) > 0$ for each $j \le i$. Therefore P is a product of two nonnegative linear combinations of P_j. We shall show that this makes P such a combination as well (considered as a function $\{0, 1, 2, \ldots, n\} \to \mathbf{R}$, not necessarily as a polynomial, which wouldn't make sense once $2i + 1 > n$). Equivalently we claim that

$$\sum_{x=0}^{n} \binom{n}{x} (q-1)^x K_j(x) K_{j'}(x) K_{j''}(x) \ge 0$$

for all j, j', j''. (This also implies by induction that the product of *any* number of K_j is a nonnegative linear combination of Krawtchouk polynomials.) Such an inequality can be stated for any system of orthogonal polynomials, but it need not hold in general. In our case, though, we can obtain this result from any of the three approaches we have indicated to developing the theory of the K_i. Using the generating function, we're led to the $Y^j (Y')^{j'} (Y'')^{j''}$ coefficient of

$$\Big((1 + (q-1)Y)(1 + (q-1)Y')(1 + (q-1)Y'') + (q-1)(1-Y)(1-Y')(1-Y'')\Big)^n,$$

which is the n-th power of $q + q(q-1)(YY' + YY'' + Y'Y'') + q(q-1)(q-2)YY'Y''$ and thus clearly has nonnegative coefficients. If we define K_i using the discrete Fourier transform of 1_{S_i} then we can observe that the convolution of nonnegative functions is nonnegative. Finally if we obtain K_j from

the j-th representation of $\mathrm{Aut}(A^n) = (S_q^n) \rtimes S_n$ then we can use the decomposition of the tensor products of the j-th and j'-th representations, in which each irreducible representation occurs with nonnegative multiplicity.

So P satisfies our criteria. Its value at $x = 0$ is

$$P(0) = \frac{1}{y}(K_i(y)K_{i+1}(0) - K_{i+1}(y)K_i(0))^2,$$

and we know already that $K_j(0) = (q-1)^j \binom{n}{j}$ (which "happens" to equal h_j) for each j. The constant coefficient a_0 is

$$\frac{i+1}{q}\left\langle K_i(y)K_{i+1}(\cdot) - K_{i+1}(y)K_i(\cdot),\ \sum_{j=0}^{i}\frac{h_i}{h_j}K_j(y)K_j(\cdot)\right\rangle,$$

which by orthogonality simplifies to $-\frac{i+1}{q}h_iK_i(y)K_{i+1}(y)$ (note that this is positive because $K_{i+1}(y) < 0 < K_i(y)$).

The resulting bound $P(0)/a_0$ is $1/y$ times a degree-2 rational function of $r := -K_{i+1}(y)/K_i(y)$, namely

$$f(r) := \frac{q}{(i+1)h_i}\frac{(K_i(0)r + K_{i+1}(0))^2}{r}.$$

As y varies between ρ_{i+1} and ρ_i, this ratio r varies from 0 to $+\infty$. At these two extremes $f(r) \to \infty$. We choose r, and thus y, to minimize $f(r)$, finding $r = K_{i+1}(0)/K_i(0)$ and $f(r) = 4K_i(0)K_{i+1}(0)$. Thus our upper bound is

$$\frac{P(0)}{a_0} = \frac{4qK_i(0)K_{i+1}(0)}{(i+1)yh_i} < \frac{4qK_i(0)K_{i+1}(0)}{(i+1)\rho_{i+1}h_i} = \frac{4qK_i(0)}{(i+1)\rho_{i+1}}K_{i+1}(0),$$

valid for any code of minimal distance at least ρ_{i+1}. If we let $i, n \to \infty$ with $i/n \to \iota$ then

$$\frac{1}{n}\log\frac{P(0)}{a_0} \to H_q(\iota),$$

where H_q is the q-entropy function we introduced earlier in the course,

$$H_q(\epsilon) = -\epsilon\log\epsilon - (1-\epsilon)\log(1-\epsilon) + \epsilon\log(q-1).$$

It remains to estimate how ρ_i depends asymptotically on i/n. We extract $K_i(x)$ from the generating function as a contour integral and apply a stationary-phase estimate, finding that there are two critical points depending on x, which are real for x near 0 and n, and complex conjugates for x near the root $(1-q^{-1})n$ of K_1. In the latter regime, P_i oscillates, and ρ_i is approximately at the smallest x in that regime, when the critical points collide on the real axis. We want that i as a function of x, because that is what we need to estimate our upper bound $P(0)/a_0$ on a code of minimum distance at least x.

The computation proceeds as follows. Because $P_i(x)$ is the z^i coefficient of $(1+(q-1)z)^{n-x}(1-z)^x$, it is the average of $z^{-i}(1+(q-1)z)^{n-x}(1-z)^x$ over any circle centered at the origin. The critical points of this function of z are the zeros of its logarithmic derivative

$$\frac{(q-1)(n-x)}{1+(q-1)z} - \frac{x}{1-z} - \frac{i}{z} = \frac{(n-i)(q-1)z^2 + ((x+i-n)q + n - 2i)z + i}{z(z-1)(1+(q-1)z)}.$$

The numerator is a quadratic in z whose discriminant is

$$q^2i^2 + 2((q-2)x - (q-1)n)qi + (qx - (q-1)n)^2.$$

As expected this is a homogeneous quadratic polynomial in x, n, i. Taking $x = \delta n$ and $i = \iota n$, we find that the critical value of ι is

$$\iota_0(\delta) = \frac{q-1}{q} - \frac{q-2}{q}\delta - \frac{2}{q}\sqrt{(q-1)(\delta - \delta^2)}.$$

This is an decreasing function of δ in the relevant range $0 \le \delta \le (q-1)/q$, with $\iota_0(0) = (q-1)/q$ and $\iota_0((q-1)/q) = 0$. [This symmetry is not coincidental: $\iota_0(\delta)$ is the smaller solution of a quadratic that's symmetrical in ι and δ,

$$q^2(\iota+\delta)^2 - 4q\iota\delta - 2q(q-1)(\iota+\delta) + (q-1)^2 = 0.]$$

The final form of our asymptotic LP bound is then

$$\log M \le nH_q(\iota_0(\delta)) + o(n),$$

whose main term decreases as expected from $n \log q$ for $\delta = 0$ to zero for $\delta = (q-1)/q$, and improves on $1 - H_q(\delta/2)$ (the asymptotic form of the sphere-packing bound) for all $\delta > 0$.