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

Orthogonality of the Krawtchouk polynomials $\{K_i : 0 \le i \le n\}$

Given q and n, the Krawtchouk polynomials

$$K_i(x) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{x}{j} \binom{n-x}{i-j} \quad (0 \le i \le n)$$

are orthogonal with respect to the inner product

$$\langle f, g \rangle := \frac{1}{q^n} \sum_{x=0}^{n} \binom{n}{x} (q-1)^x f(x) g(x).$$

This is clear from Parseval together with the fact that $K_i(\mathrm{wt}(\cdot))$ is the discrete Fourier transform of 1_{S_i} (and that the Hamming spheres $S_i = \{c : \mathrm{wt}(c) = i\}$ are disjoint). We can also prove it, and evaluate $\langle K_i, K_i \rangle$, generatingfunctionologically: Start from our formula

$$\sum_{i=0}^{n} K_i(x) X^{n-i} Y^i = (X + (q-1)Y)^{n-x} (X - Y)^x,$$

and write $\langle K_i, K_j \rangle$ as the $Y^i Z^j$ coefficient of[1]

$$\frac{1}{q^n} \sum_{x=0}^{n} \binom{n}{x} (q-1)^x \big[(1 + (q-1)Y)^{n-x} (1-Y)^x\big] \big[(1 + (q-1)Z)^{n-x} (1-Z)^x\big].$$

Reorganizing the summand into

$$\binom{n}{x} (q-1)^x \big[(1 + (q-1)Y)(1 + (q-1)Z)\big]^{n-x} \big[(1-Y)(1-Z)\big]^x,$$

we recognize a binomial expansion:

$$\frac{1}{q^n} \big[(1 + (q-1)Y)(1 + (q-1)Z) + (q-1)(1-Y)(1-Z)\big]^n = \frac{1}{q^n} \big[q(1 + (q-1)YZ)\big]^n$$

which clearly involves only powers of YZ, and simplifies further to $\big(1 + (q-1)YZ\big)^n$. Applying the binoimal theorem once more to extract the $(YZ)^i$ coefficient, we also find

$$\langle K_i, K_i \rangle = \binom{n}{i} (q-1)^i.$$

[1] We dehomogenize by setting $X = 1$.