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

Lloyd's theorem: a necessary condition for perfect error correction

Recall that we promised to show that, while the identity $\binom{90}{2} + 90 + 1 = 4096 = 2^{12}$ (equivalent to Ramanujan's $181^2 + 7 = 2^{15}$) suggests that there might be a perfect 2-error-correcting code of length 90, in fact there is no binary $[90, 78, 5]$ code, nor even a $(90, 2^{78}, 5)$ code. We prove this next, and generalize to Lloyd's criterion that gives a strong necessary condition on the parameters of a perfect code. Along the way we encounter the Krawtchouk polynomials which we'll also use to improve on our asymptotic upper bounds on error-correcting codes.

We use the *group ring* (a.k.a. *group algebra*) of F^n. We already introduced the group ring $\mathbf{Z}[X]/(X^n-1)$ of a cyclic group $\mathbf{Z}/N\mathbf{Z}$. In general, for a commutative ring A and any finite group G we have an associative group ring $A[G]$, which is commutative *iff* G is (and we'll use only commutative groups here). As an A-module, it is just $A^{|G|}$; we think of an element of A^G as a formal A-linear combination $\sum_{g\in G} a_g g$ of elements of G, or a map $G \to A$, $g \mapsto a_g$. We define multiplication as the A-bilinear map $A[G] \times A[G] \to A[G]$ that takes (the characteristic functions of) group elements g, h to (the characteristic functions of) their product gh. The product of functions $g \mapsto a_g$, $h \mapsto b_h$ is their *convolution* $s \mapsto \sum_{gh=s} a_g b_h$. The identity element of $A[G]$ is (the characteristic function of) the identity of G.

This is relevant to us for the following reason. Let C be any subset of F^n, and $1_C \in A[F^n]$ its characteristic function, representing the formal sum $\sum_{c\in C} c$. Then C is perfect e-error-correcting code in F^n *iff* $1_C 1_{B_e} = 1$ in $A[G]$, where B_e is the closed ball $\{w \in F^n \mid \mathrm{wt}(w) \le e\}$, and plain "1" is the constant function 1 on F^n, representing the formal sum of all $w \in F^n$.

Now take $A = \mathbf{C}$, and suppose $\chi : F^n \to \mathbf{C}^*$ is any nontrivial character (a.k.a. nonzero element of the Pontrjagin dual of $(F^n, +)$). Then χ extends linearly to a ring homomorphism $\mathbf{C}[F^n] \to \mathbf{C}$ such that $\chi(1) = 0$. Therefore, either $\chi(1_C) = 0$ or $\chi(1_{B_e}) = 0$. That is, either $\sum_{c\in C} \chi(c) = 0$ or $\sum_{\mathrm{wt}(w)\le e} \chi(w) = 0$.

In our first application, we take $F = \mathbf{Z}/2\mathbf{Z}$. The characters $F^n \to \mathbf{C}^*$ are just the maps $\chi_v : w \mapsto (-1)^{\langle v,w\rangle}$ for $v \in \mathbf{Z}/2\mathbf{Z}$. By symmetry $\chi(1_{B_e})$ depends only on the weight of v, call it x. It is easier to find the character of a Hamming *sphere* $S_i = \{w \in F^n \mid \mathrm{wt}(w) = i\}$, and then sum over $0 \le i \le e$. We find that

$$\chi(1_{S_i}) = \sum_{j=0}^{i} (-1)^j \binom{x}{j}\binom{n-x}{i-j},$$

a polynomial of degree i in x called the i-th *Krawtchouk*[1] *polynomial*, which we denote by $K_i(x)$. Then $\chi(1_{B_e}) = \sum_{i=0}^{e} K_i(x)$; this too is a polynomial of degree i in x, which we shall call $L_e(x)$ (with "L" for "Lloyd"). So $\sum_{c\in C}(-1)^{\langle c,v\rangle} = 0$ for all nonzero v whose weight is not a root of L_i. Now for $n = 90$ and $e = 2$ we compute $L_2(x) = 2(x^2 - 91x + 2^{11})$, which is irreducible (discriminant 89 — in general $\mathrm{disc}(L_2/2) = n - 1$), so $L_2(x) \ne 0$ for all integers x. But then a perfect $(90, 2^{78}, 5)$ code C would have $\chi(1_C) = 0$ for *all* nontrivial χ, which is impossible because 1_C would then be a constant function (in general $\chi_v(a)$ is the value at v of the discrete Fourier transform $\hat{a}$ of the map $w \mapsto a_w$, and if $\hat{a}$ is supported on the identity then a is constant). This proves that there is no such code C, as claimed.

What happens for values of n for which we do know a perfect code? For $e = 2$, these are $n = 2$ (single-word) and $n = 5$ (repetition), and indeed in each case $n - 1$ is a square; we find that $L_2(x) = 2(x-1)(x-2)$ and $2(x-2)(x-4)$ respectively. Moreover we can now show that there are no further

[1] 1929; The Ukrainian name is also seen in other transliterations such as Kravchuk.

perfect 2-error-correcting binary codes.[2] If there were such a code of length n then $\#(B_2)$ would be a power of 2 and L_2 would have rational roots. But $\#(B_2)$ is the image of 1_{B_2} under the trivial character, which is $L_2(0)$. If L_2 has integer roots then both are powers of 2 (because L_2 has integer coefficients, leading coefficient 2, and power-of-2 constant term). But the roots are $(n+1 \pm \sqrt{n-1})/2$, and thus not equal but too close to be distinct powers of 2 once $n > 5$. Once we have Lloyd's criterion we'll be able to generalize this argument to prove the theorem of Tietäväinen and van Lint[3] that the known list of parameters of perfect codes *over alphabets of prime-power order* is complete.

First let's see what L_e does for $e = 3$, for which we know a nontrivial perfect code $\mathcal{G}_{23}$ as well as the trivial perfect codes: here $L_3(x)$ factors as

$$-\frac{4}{3}(m-1)(m-2)(m-3), \quad -\frac{4}{3}(m-2)(m-4)(m-6), \quad -\frac{4}{3}(m-8)(m-12)(m-16)$$

for $n = 3$, 7, 23 respectively. This is quite suggestive; not only does L_3 factor completely (so far we knew only that it had to vanish at one integer $x \in [1, n]$), but in each case, including the sporadic $\mathcal{G}_{23}$, we recognize the roots as the nonzero weights of the dual code! The same was true for the $n = 2$ and $n = 5$ cases of perfect codes of length $e = 2$.

What happens to this analysis for finite fields F with $q = \#F$ other than 2? Again $C \subseteq F^n$ is a perfect e-error-correcting code C *iff* $1_C 1_{B_e} = 1$ in $A[G]$, which again implies that for every nontrivial χ in the Pontrjagin dual of $(F^n, +)$ either $\chi(1_C)$ or $\chi(1_{B_e})$ vanishes. As usual we identify this Pontrjagin dual with F^n by fixing a nontrivial character $\psi : F \to \mathbf{C}^*$ and writing an arbitrary χ as $\chi_v : w \mapsto \psi(\langle v, w \rangle)$. Then we see as before that $\sum_{w \in B_e} \chi_v(w)$ depends only on $x = \mathrm{wt}(v)$, and write the sum as $L_e(x) = \sum_{i=0}^{e} K_i(x)$ where for general q the Krawtchouk polynomial is defined by

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

We argue as before that L_i must have at least one integer root, and shall show that in fact all e roots must be integers. For example, the ternary Golay code with $q = 2$, $n = 11$, and $e = 2$ yields $L_2(x) = (9/2)(x-6)(x-9)$, with roots at the nonzero weights 6 and 9 of $\mathcal{G}_{11}^{\perp}$.

We now prove Lloyd's theorem: if there is a perfect e-error-correcting code $C \subseteq F^n$ then the associated polynomial $L_e = \sum_{i=0}^{e} K_e$ has all e roots integral. Suppose not. Then there is a nonzero polynomial $P(x)$ of degree strictly below e such that $P(x) = 0$ on every integral root of L_e. We can write P as a nonzero linear combination $\sum_{i=0}^{e-1} p_i K_i$ of Krawtchouk polynomials of degree $i < e$. Then the function $P(\mathrm{wt}(\cdot))$ is the discrete Fourier transform of $\beta := \sum_{i=0}^{e-1} p_i 1_{S_i}$, so $\chi(1_C \beta) = 0$ for all nonzero χ, whence $1_C \beta$ is a constant function. But this is impossible because the C-translates of S_i $(0 \le i < e)$ are disjoint and do not cover F^n, Q.E.D.

[2] This also follows from the fact that $\#(B_2)$ is never a power of 2 for $n > 90$, i.e. that there is no $y > 181$ for which $y^2 + 7$ is a power of 2; but that's a harder theorem (Nagell 1948, 1961).

[3] 1973; I see on Google Books that Raymond Hill reports (in *A First Course in Coding Theory* (1986), page 102) that the result was obtained independently by Zinov'ev and Leont'ev in the same year. For lack of time we shall not complete the proof of the Tietäväinen-van Lint(-Leont'ev-Zinov'ev) theorem in Math 256.