Lecture Notes for Math 696
Coding Theory
Iterative Decoding

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
wwww-rohan.sdsu.edu/ ~ mosulliv

April 10, 2002

Let $A = \{1, 2, \ldots, n\}$ and $\mathbb{F} = \{0, 1\}$. For each $i \in A$,

- Let p_i be a distribution on $\mathbb{F}$
- Define for $a \in \mathbb{F}$,
$$\mu_i(a) = \sum_{v \in \mathbb{F}^B} \chi(a, v) \prod_{j \in B} p_j(v_j)$$
where $B = A \setminus \{j\}$. For example
$$\mu_1(a) = \sum_{v \in \mathbb{F}^{n-1}} \chi(a, v) \prod_{j=2}^{n} p_j(v_j)$$
- Define a new distribution q_i on $\mathbb{F}$ by
$$q_i'(a) = p_i(a)\mu_i(a)$$
$$q_i(a) = \frac{q_i'(a)}{q_i'(0) + q_i'(1)}$$

This is the algorithm we want to implement. It iterates by applying the algorithm to its own output.

The computation in item 3 is a simple product of n terms followed by a sum and a division. No problem. Item 2 involves a sum of 2^{n-1} terms, each a product. It turns out there is a simpler way to compute it. Let's also check that μ is a probability distribution.

Proposition 0.1. *For $i = 1, \ldots, n$, let p_i be distributions on $\mathbb{F}$ and let*
$$\mu(a) = \sum_{\substack{v \in \mathbb{F}^n \\ \mathrm{wt}(v) = a \mod 2}} \prod_{i=1}^{n} p_j(v_j)$$
Then $\mu(0) + \mu(1) = 1$, and $\mu(0) - \mu(1) = \prod_{i=1}^{n}(p_i(0) - p_i(1))$.

PROOF:

$$\begin{aligned}\mu(0)+\mu(1) &= \sum_{\substack{v\in\mathbb{F}^n \\ \mathrm{wt}(v)=0 \mod 2}} \prod_{j\in B} p_j(v_j) + \sum_{\substack{v\in\mathbb{F}^n \\ \mathrm{wt}(v)=1 \mod 2}} \prod_{j\in B} p_j(v_j) \\ &= \sum_{v\in\mathbb{F}^n}\prod_{j\in B} p_j(v_j) \\ &= \prod_{j=1^n}(p_j(0)+p_j(1)) \\ &= 1\end{aligned}$$

On the other hand,

$$\begin{aligned}\mu(0)+\mu(1) &= \sum_{\substack{v\in\mathbb{F}^n \\ \mathrm{wt}(v)=0 \mod 2}} \prod_{j\in B} p_j(v_j) - \sum_{\substack{v\in\mathbb{F}^n \\ \mathrm{wt}(v)=1 \mod 2}} \prod_{j\in B} p_j(v_j) \\ &= \prod_{j=1^n}(p_j(0)-p_j(1)\end{aligned}$$

□

The theorem applies to μ_i, since

$$\mu_i(a) = \sum_{\substack{v\in\mathbb{F}^B \\ \mathrm{wt}(v)=a \mod 2}} \prod_{j\in B} p_j(v_j)$$

In fact we see that $\mu_i(0)-\mu_i(1) = (\mu(0)-\mu(1))/(p_i(0)-p_i(1))$.

This gives us a way to compute μ_i. First let's define for any distribution q on $\mathbb{F}$, $\delta q = q(0)-q(1)$. Notice that

$$\delta q = q(0) - (1-q(0)) = 2q(0)-1$$

So

$$q(0) = (\delta q + 1)/2$$

Here is our new algorithm. I've changed it a bit to be closer to a possible implementation.

- Let $q_i = p_i(0)$ be the probability of 0 in the ith bit.
- Let $\delta p_i = 2q_i - 1$.
- Let $\delta\mu = \mu(0)-\mu(1) = \prod_{i=1}^n \delta p_i$.
- Then $\mu_i(0) = (\delta\mu/\delta p_i + 1)/2$.
- Let $B = A\setminus\{i\}$. Define a new distribution q_i on $\mathbb{F}$ by

$$\begin{aligned}q_i'(0) &= q_i\mu_i(0) \\ q_i'(1) &= (1-q_i)(1-\mu_i(0)) \\ q_i &= \frac{q_i'(0)}{q_i'(0)+q_i'(1)}\end{aligned}$$