Notes on the Vasil'ev Construction

Frank R. Kschischang

September 25, 2016

As usual, let $\mathbb{F}_2$ denote the field of two elements and for any positive integer n, let $\mathbb{F}_2^n$ denote the vector space of n-tuples over $\mathbb{F}_2$.

For any integer $m > 2$, let H_m be the binary $(2^m - 1, 2^m - m - 1)$ Hamming code, and let U_m be the whole vector space $\mathbb{F}_2^{2^m-1}$, i.e., U_m is the binary $(2^m - 1, 2^m - 1)$ code.

For any binary vector $x \in \mathbb{F}_2^n$, let $\pi(x) = x_1 + \cdots + x_n$ denote the parity of x. Note that π is linear, i.e., $\pi(x + y) = \pi(x) + \pi(y)$. Finally, let $\lambda : H_m \to \mathbb{F}_2$ be any function (possibly nonlinear) satisfying $\lambda(0) = 0$.

Now form the code

$$\mathcal{C}_{m+1} = \{(u, u + v, \pi(u) + \lambda(v)) : u \in U_m, v \in H_m\}.$$

Clearly $\mathcal{C}_{m+1}$ has length $2(2^m - 1) + 1 = 2^{m+1} - 1$ and, since each different choice of (u, v) gives a different codeword,

$$|\mathcal{C}_{m+1}| = 2^{2^m-1} \cdot 2^{2^m-m-1} = 2^{2^{m+1}-(m+1)-1} = |H_{m+1}|.$$

Thus $\mathcal{C}_{m+1}$ has the same length and number of codewords as H_{m+1}. Let us now show that $\mathcal{C}_{m+1}$ also has minimum distance 3.

Let

$$\begin{aligned} c_1 &= (u_1, u_1 + v_1, \pi(u_1) + \lambda(v_1)) \\ c_2 &= (u_2, u_2 + v_2, \pi(u_2) + \lambda(v_2)) \end{aligned}$$

be two arbitrary codewords of $\mathcal{C}_{m+1}$. These two words are separated by Hamming distance $d(c_1, c_2)$ given by

$$d(c_1, c_2) = \mathrm{wt}(u_1 + u_2) + \mathrm{wt}(u_1 + v_1 + u_2 + v_2) + \mathrm{wt}(\pi(u_1 + u_2) + \lambda(v_1) + \lambda(v_2)),$$

where $\mathrm{wt}(\cdot)$ denotes Hamming weight, and we have used the fact that $\pi(u_1) + \pi(u_2) = \pi(u_1 + u_2)$.

We consider several cases.

Case 0: $u_1 = u_2$, $v_1 = v_2$.

This is the trivial case where $c_1 = c_2$ and $d(c_1, c_2) = 0$.

Case 1: $u_1 \neq u_2$, $v_1 = v_2$.

In this case,
$$d(c_1, c_2) = 2\,\mathrm{wt}(u_1 + u_2) + \mathrm{wt}(\pi(u_1 + u_2)).$$
If $\mathrm{wt}(u_1 + u_2) = 1$, then $\mathrm{wt}(\pi(u_1 + u_2)) = 1$, so $d(c_1, c_2) = 3$. If $\mathrm{wt}(u_1 + u_2) \geq 2$, then $d(c_1, c_2) \geq 4$.

Case 2: $u_1 = u_2$, $v_1 \neq v_2$.

In this case,
$$d(c_1, c_2) = \mathrm{wt}(v_1 + v_2) + \mathrm{wt}(\lambda(v_1) + \lambda(v_2)) \geq 3$$
since v_1 and v_2 are Hamming codewords, and $\mathrm{wt}(v_1 + v_2) = d(v_1, v_2) \geq 3$.

Case 3: $u_1 \neq u_2$, $v_1 \neq v_2$.

Note that in this case, since v_1 and v_2 are Hamming codewords, $\mathrm{wt}(v_1 + v_2) = d(v_1, v_2) \geq 3$. Adding a word of weight one (or two) to $v_1 + v_2$ can change its weight by at most one (or two). Thus, if $\mathrm{wt}(u_1 + u_2) = 1$, then $\mathrm{wt}(u_1 + u_2 + v_1 + v_2) \geq 2$, and so $d(c_1, c_2) \geq 3$. If $\mathrm{wt}(u_1 + u_2) = 2$, then $\mathrm{wt}(u_1 + u_2 + v_1 + v_2) \geq 1$, and so $d(c_1, c_2) \geq 3$. Finally if $\mathrm{wt}(u_1 + u_2) \geq 3$, then $d(c_1, c_2) \geq 3$.

In all cases when $c_1 \neq c_2$, we have $d(c_1, c_2) \geq 3$. In fact, in Case 1 we can easily construct c_1 and c_2 with $d(c_1, c_2) = 3$. It follows from this (or from the Hamming bound) that $\mathcal{C}_{m+1}$ has minimum Hamming distance exactly 3.

As an example, consider the special case when $\lambda(x) = 0$. In this case $\mathcal{C}_{m+1}$ is linear with generator matrix
$$G_{m+1} = \left[\begin{array}{c|c|c} \multirow{3}{*}{I} & \multirow{3}{*}{I} & 1 \\ & & \vdots \\ & & 1 \\ \hline \multirow{3}{*}{0} & \multirow{3}{*}{G_m} & 0 \\ & & \vdots \\ & & 0 \end{array}\right],$$
where G_m is a generator matrix for the Hamming code H_m.

References

[1] Ju. L. Vasil'ev, "On nongroup close-packed codes," *Probl. Cybernet.* vol. 8, pp. 337-339, 1962.