Perfect codes II

Let us first recall the so-called *Hamming bound (or: sphere packing bound)* for codes and the definition of perfect codes.

Proposition (Hamming bound)**.** *Assume that $C \subseteq Q^n$, $|Q| = q$, and C is a t-error correcting code. Then*

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Definition. Codes attaining equality in the Hamming-bound are called *perfect* codes. So, for perfect codes we have

$$|C| = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

Note that the parameters $(n, M, d)_q$ determine whether the code is perfect or not. For example, a binary $(23, 2^{12}, 7)$ code and a ternary $(11, 3^6, 5)_3$ code are perfect. In the former case a ball of radius 3 contains $1 + 23 + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11}$, in the latter $1 + 11 \cdot 2 + \binom{11}{2} \cdot 4 = 1 + 22 + 220 = 243 = 3^5$ words.

Let us first focus on the binary case ($q = 2$) and $t = 1$. We saw that the parameters of a binary perfect code are $n = 2^m - 1$, $|C| = 2^{n-m}$ (and $d = 3$) and constructed the Hamming-codes $\mathrm{Ham}(m)$, which are perfect, 1-error correcting linear codes. We also saw that among linear codes, these codes are unique.

It is then natural to ask whether these codes are unique or there are, for example, non-linear codes with the same parameters. Of course, we can replace the Hamming code by a coset, but we also wish to exclude this possibility. So, we will suppose that $0 \in C$. The following construction is due to Vassil'ev.

Let $C = \mathrm{Ham}(m)$, $m \geq 3$, $n = 2^m - 1$, $V = V(n, 2)$. Let $N = 2n + 1 (= 2^{m+1} - 1$. We will construct a non-linear perfect code C^* of length N. If C^* is linear, then every projection to one coordinate has to be linear. Vassil'ev's construction is the following:

$$C^* = \{(v, c + v, p(v) + f(c)) : c \in C,\ v \in V\},$$

where $p : v \mapsto p(v)$ is the parity check bit (that is $p(v) = v_1 + \ldots v_n)$), $f : c \in C \mapsto f(c) \in \mathrm{GF}(2)$ is a function with $f(0) = 0$, $f(c) = 1$, if $c \neq 0$. Intuitively, f is a very much non-linear function, because a non-constant linear function takes the value 0 and 1 the same number of times. Actually, we can take any non-linear f with $f(0) = 0$.

We are going to show that C^* is a code with the same parameters as $\mathrm{Ham}(m)$, so it is perfect.

First observe that c and v can be chosen independently, so we get $|C^*| = |C||V|$. Hence $|C^*| = 2^{n-m} \cdot 2^n = 2^{N-(m+1)}$, which is $|\mathrm{Ham}(m+1)|$. So, we only have to prove that C^* has minimum distance 3.

We will consider two distinct codewords $(v, c+v, p(v)+f(c))$ and $(v', c'+v', p(v')+f(c'))$ and distinguish several cases.

1) If $d(v, v') \geq 3$, then the above two codewords are at distance at least 3.

2) If $d(v, v') = 0$ (that is, $v = v'$), then $c \neq c'$, and since $d(c, c') \geq 3$, so $d(v+c, v'+c') \geq 3$, and the above two codewords are at distance at least 3.

3) If $d(v, v') = 2$, then $v+c \neq v'+c'$, because either $c = c'$ or the distance of c and c' is at least 3. Hence $d(v+c, v'+c') \geq 1$, and the above two codewords are at distance at least 3.

4) If $d(v, v') = 1$ and $c = c'$, then $d(v+c, v'+c') = 1$, but also $p(v) \neq p(v')$, so all the three parts of the above two codewords are at distance 1. If $d(v, v') = 1$ and $c \neq c'$, then $d(v+c, v'+c') \geq 2$, because c and c' are at distance at least 3. This menas that also in this case the above two codewords are at distance at least 3.

The nonlinearity of the code follows from the fact that the projection onto the last coordinate is not linear, since f is non-linear.

The situation is the same for q-ary codes. We generalized the Hamming codes over a q-ary alphabet, and $\mathrm{Ham}_q(m)$ has length $n = (q^m - 1)/(q-1)$. In this case Lindström and Schönheim proved the existence of non-linear 1-error correcting perfect codes with a generalization of Vassil'ev's construction.

Let us continue with the existence/non-existence of some special perfect codes. First, we show that for $q = p^h$, the parameters of a 1-error correcting perfect code are those of a $\mathrm{Ham}_q(m)$.

Proposition. *If there is a 1-error correcting perfect code of length n, then $1 + n(q-1) | q^n$. Let $q = p^h$, p prime. Then $1 + n(q-1) = q^a$.*

The first condition is trivial. For the second, $1 + n(q-1)$ has to be a power of p. Write $1 + n(q-1) = q^a \cdot p^s$ for some $0 \leq s \leq h-1$. Then, by expressing n we get

$$n = \frac{q^a p^s - 1}{q-1} = \frac{q^a p^s - p^s + p^s - 1}{q-1} = p^s \frac{q^a - 1}{q-1} + \frac{p^s - 1}{q-1}.$$

Since n is an integer we get $s = 0$.

The situation is the same for t-error correcting perfect codes. We will not prove this more general result.

Proposition. *If there is a t-error correcting perfect code of length n, then $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i | q^n$. Let $q = p^h$, p prime. Then $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i = q^a$.*

In case of binary codes, we saw that the repetition code is perfect. Besides this example, codes with $|C| \leq 1$ are also called trivial.

Proposition. *If a binary perfect code corrects 3 errors, then it is either trivial or $n = 23$.*

The ball of radius 3 contains $1 + n + \binom{n}{2} + \binom{n}{3}$ words. This has to be 2^a for some a, so we get

$$(n+1)(n^2 - n + 6) = 3 \cdot 2^{a+1}.$$

Considering the second factor modulo $(n+1)$, we see that it is 8. So, there are two possibilities: either $(n+1)$ is divisible by 16, or $(n+1)$ divides 24. In the former case, the second factor should divide 24. One can check that it is only possible for $n = 1, 2, 3$. In the latter case $n = 0, 1, 2, 3, 7, 11$ or $n = 23$. For $n = 0, 1, 2$, there is no 3-error correcting code, for $n = 3$, it is the trivial code with $|C| = 1$. In case of $n = 7$, we must have the repetition code. For $n = 11$, the second factor is 116, which is divisible by 29, so this is not possible. So in all cases (except $n = 23$) the code is trivial.

We will see later the binary Golay-codes, which are of length 23, and they are perfect 3-error correcting codes.

Proposition. *There is no non-trivial binary perfect 2-error-correcting code.*

In this case the ball of radius 2 contains $1 + n + \binom{n}{2}$ words, which must be a power of 2. So we get the diophantine equation $(2n+1)^2 = 2^{a+3} - 7$. Luckily, this equation was studied in algebraic number theory, and the solution are $2n+1 = 1, 3, 5, 11$ and 181.We will exclude the case $n = 90$ and the remaining cases either do not correspond to codes or give a trivial perfect code (e.g. $n = 5$ gives the repetition code).

The best result in this direction is the following.

Theorem (Tietäväinen,van Lint)**.** *Assume that the alphabet Q has p^h elements, p prime, and C is a t-error correcting code for some $t > 1$. Then C is either trivial or $n = 23, |Q| = 2$ or $n = 11, |Q| = 3$ (and the corresponding codes are the binary or ternary Golay codes).*

Another approach to study binary perfect codes is to connect them with block designs.

Definition. Let P be a ground set, and B be a set of certain subsets of P. The elements of P are called *points*, those of B are called *blocks*. The structure (P, B) is a $t-(v, k, \lambda)$-*design* if

- $|P| = v$,
- for every $b \in B$ we have $|b| = k$,
- for every t distinct points $p_1, \dots p_t$ there are precisely λ blocks containing the.

If multiple blocks are allowed then the structure is called a $t-(v, k, \lambda)$-*system*.

Let us first see some examples. There are many examples for $t = 2$. For example, if we consider the k-dimensional subspaces of an n-dimensional projective space, then we get a $2-(\begin{bmatrix} n+1 \\ 1 \end{bmatrix}, \begin{bmatrix} k+1 \\ 1 \end{bmatrix}, \begin{bmatrix} n-1 \\ k-1 \end{bmatrix})$ design. A more concrete example is $n = 2, k = 1$, when the parameters are $2-(q^2+q+1, q+1, 1)$. Similarly, affine spaces also give designs with $t = 2$.

There are necessary divisibility conditions for the existence of $t-(v,k,\lambda)$-designs.

Proposition. *Let (P, B) be a $t-(v,k,\lambda)$-design. Then*

$$\lambda_i = \lambda \cdot \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$$

must be an integer for $i = 0, 1, \ldots, t$.

For the proof, observe that λ_i is just the number of blocks through a set of i distinct points. Indeed, there are $v-i$ other points. If we choose $t-i$ of them, then we obtain a set of t points. Through this set of t points, by definition, there are λ blocks. With this naive counting we count every block as many times, as we can choose the $t-i$ points inside one block. This explains the denominator.

For $i = 0$, the number of blocks $b = |B|$ is obtained, for $i = 1$ we get the number r of blocks containing a given point. For $i = t$, we get back $\lambda_t = \lambda$ and putting $i = t-1$ gives that $k-t+1$ has to divide $\lambda(v-t+1)$.

For $t \geq 3$ it is far from being easy to construct t-designs. For $t = 3$, there are quite some examples, but for larger t only trivial and sporadic ones (the so-called Witt-designs that we will see later) were known until the seventies. The first examples with $t = 6$ came around that time (Magliveras, Leavitt, Mezzaroba), then Teirlinck in the eighties showed that t can be arbitrary large. Recently, Keevash showed that the above divisibility conditions are sufficient if k, λ are fixed and v is (very) large.

The relation of block designs and perfect codes is given in the next proposition.

Proposition. *Let $C \subseteq \{0,1\}^n$ be a perfect, binary e-error correcting code, $0 \in C$, $d = 2e+1$. Let $P = \{1, 2, \ldots n\}$, the set of coordinates. Define B as the set $\{\mathrm{supp}(c) : c \in C, w(c) = 2e+1\}$. (Recall that the support of a codeword is the set of non-zero coordinates.) Then (P, B) is a block design with parameters $(e+1)-(n, 2e+1, 1)$.*

Consider $e+1$ distinct coordinates. This is the support of a word x with weight $e+1$. As C is perfect, there is a unique codeword $0 \neq c \in C$ so that $d(x,c) \leq e$. Because of the triangle inequality, $w(c) \leq 2e+1$, so $w(c) = 2e+1$. Observe that the support of c (which is a block of our design) contains the support of x. The uniqueness of c shows $\lambda = 1$.

The divisibility conditions for t-designs give the following for the existence of binary perfect codes.

Proposition. *For an e-error correcting, binary perfect code of length n, the numbers*

$$\frac{\binom{n-i}{e+1-i}}{\binom{2e+1-i}{e+1-i}}, \quad i = 0, 1, \ldots e+1$$

are all integers. In particular, by putting $i = e$, we get $e+1 | n+1$.

We can say somewhat more. If A_i denotes the number of codewords of weight i, then $A_{2e+1} = |B| = \binom{n}{e+1} / \binom{2e+1}{e+1}$. This can be extended to q-ary codes, when we obtain $A_{2e+1} = \binom{n}{e+1}(q-1)^{e+1} / \binom{2e+1}{e+1}$. This comes from counting the pairs (x, c), where $w(x) = e+1$, and c is the unique codeword at distance (at most) e from x. We can say even more, namely that a perfect code determines the entire sequence A_i (if we assume that $0 \in C$, which means that $A_0 = 1$). We only prove this for 1-error correcting codes.

Proposition. *Let $0 \in C$ be a 1-error-correcting, binary perfect code. Then*

$$\binom{n}{i} = A_{i-1}(n-i+1) + A_i + A_{i+1}(i+1).$$

Together with $A_0 = 1, A_1 = 0, A_2 = 0$ this recurrence indeed determines the sequence A_i.

The recurrence relation is clear: the left-hand side counts the words of weight i, the right-hand side counts the words of weight i that are at distance 1 from a codeword of weight $i-1$, codewords of weight i, and words that are at distance 1 from a codeword of weight $i+1$.

We can remark that for q-ary 1-error correcting perfect codes the recurrence relation is only slightly more complicated, it is

$$\binom{n}{i}(q-1)^i = A_{i-1}(n-i+1)(q-1) + A_i(1+i(q-2)) + A_{i+1}(i+1).$$

As we said before, this is also true for e-error correcting perfect codes, but the recurrence rekation is more complicated. We will see the illustration of the general recurrence when studying the binary Golay-codes.