Some nonexistence theorems for perfect error-correcting codes

by

H. Reuvers
1. Definitions

Let $S$ be a set of $q$ symbols and $V := S^n$. For $x \in V$, $y \in V$ define the Hamming distance $d(x,y)$ to be the number of coordinates in which $x$ and $y$ differ. Let

$$S_e(x) := \{z \in V \mid d(z,x) \leq e\}.$$ 

A perfect $e$-error-correcting code is a subset $C \subset V$ such that the $S_e(x)$ ($x \in C$) form a partition of $V$.

2. Conditions

Necessary conditions for the existence of perfect codes are:

a) the sphere packing condition:

$$\{1 + n(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{e}(q-1)^e\}^e q^n$$

b) the polynomial condition (see [3], [4]):

$$P_e(x) = \sum_{i=0}^{e} (-1)^i \binom{n}{e-i} (n-x)^i (q-1)^{e-i}$$

has $e$ different integer zeros $x_1 < x_2 < \ldots < x_e$ among $1,2,3,\ldots,n$.

3. Previous results

A. Tietäväinen and J.H. van Lint proved that there are no perfect codes with $e > 1$, $q = p^m$, $p$ prime, except for trivial codes and the two Golay codes (see [1], [2]).

4. Main theorem

Theorem 1. If $e \geq 2$, then the number of perfect $e$-error-correcting codes is finite whenever we have the number $q$ of symbols fixed.

Proof. Cfr. theorem 8 of [5]. There is a deep result of C.L. Siegel from the theory of numbers, quoted by Slotnick, which from the context clearly must be interpreted as follows:

"Let $f(x)$ be any polynomial which takes integer values whenever $x \in Z$. Then, unless $f(x)$ is a constant times a power of a linear polynomial, the largest prime factor $q_n$ of $f(n)$ satisfies: $\forall_{\text{NdN}} \exists_{\text{MdN}} [n > M \implies q_n > N]$".

Now assume that there exists a perfect $e$-code of word length $n$ on $q$ symbols, and $e \geq 2$. 
Let
\[ f(x) := 1 + \binom{x}{1}(q-1) + \binom{x}{2}(q-1)^2 + \ldots + \binom{x}{e}(q-1)^e. \]

Then \( f(x) \in \mathbb{Z} \) whenever \( x \in \mathbb{Z} \) and supposing \( f(x) = a(b + cx)^e \) we derive a contradiction as follows:

\[
\begin{align*}
    f(0) &= 1 = ab^e, \text{ so } f(x) = (1 + rx)^e \text{ with } r = \frac{c}{b} \\
    f(1) &= 1 + (q-1) = q = (1 + r)^e \\
    f(2) &= 1 + 2(q-1) + (q-1)^2 = q^2 = (1 + 2r)^e.
\end{align*}
\]

So \((1 + r)^{2e} = (1 + r^2 + 2r) = (1 + 2r)^e\), so \( r = 0 \) and \( q = 1 \). Hence, taking \( N > q \), there is a \( M \in \mathbb{N} \) such that for \( n > M \) the largest prime factor \( q_n \) of \( f(n) \) satisfies:

\[ q_n \mid f(n) = 1 + n(q-1) + \ldots + \binom{n}{e}(q-1)^e \text{ and } q_n > N. \]

Then \( f(n) \mid q^n \) (from the sphere packing condition) contradicts \( q_n > N > q \), so \( n < M \).

5. The case \( e = 3 \).

In the following we use a substitution \( \theta \) first applied by van Lint in [1], such that \( \theta(x) = 0 \) implies that \( x \) is near to the arithmetical mean of the zeros of \( P_e(x) \). The method can also be applied on \( e = 5 \), \( e = 7 \) and so on.

Theorem 2. The only nontrivial perfect 3-error-correcting code is the binary Golay code of length 23.

Proof. Let \( \theta := qx - n(q-1) \) and \( q > 2 \). By \( \theta \) the Lloyd polynomial \( P_3(x) \) is transformed into \( F_3(\theta) \), where

\[
3! F_3(\theta) = (n-1)(n-2)(n-3) - 3(n-2)(n-3)(n-\theta) + \\
+ 3(n-3)(n-\theta)(n-\theta-q) - (n-\theta)(n-\theta-q)(n-\theta-2q).
\]

Now we compare \( F(1) \) and \( F(3-q) \):

\[
\begin{align*}
    3!F(1) &= 2(q-1)(q-2)(1-n) < 0 \\
    3!F(3-q) &= (q-1)(q-2)(n-3) > 0.
\end{align*}
\]
Now assume that there exists a perfect 3-error-correcting code over a \( q \)-symbol-alphabet with \( q > 2 \) and \( n > 7 \). Then, for the zeros of \( P_3(x) \) we have:

\[
x_1 + x_2 + x_3 = e(n - e)\left(\frac{q-1}{q}\right) + e\left(\frac{e+1}{2}\right) = 3(n - 3)\left(\frac{q-1}{q}\right) + 6 \in \mathbb{Z},
\]

so \( q \mid 3(n - 3) \).

Then if \( 3 \nmid q \) we have \( n = e + qv \) for some \( v \in \mathbb{N} \), if \( q = 3p \) we have \( n = 3 + pv \).

Since \( F(1) < 0 \), \( F(3 - 2q) > 0 \), there is a \( \theta = qx - n(q - 1) \) with \( x \in \mathbb{Z} \) such that \( 3 - q < \theta < 1 \).

Then if \( 3 \nmid q \) this contradicts \( \theta \equiv n \equiv 3 \pmod{q} \), and if \( q = 3p \), since \( \theta \equiv n \equiv 3 \pmod{p} \) we must have \( \theta = 3 - p \) or \( \theta = 3 - 2p \).

But

\[
F(3 - p) = -10p^3 + p^2(27 - 9n) + p(9 - 3n) + 48 + 2n < 0
\]

and

\[
F(3 - 2p) = -8p^3 + (18 - 6n)p + 2n + 48 < 0
\]

since \( n > 7 \).

Furthermore if \( q = 2 \) or generally a prime power all perfect 3-codes are known (see [1], [2]).

6. A closer look on \( q \)

A. Theorem 3. If a perfect \( e \)-error-correcting code on \( q = p_1^{s_1} \cdots p_k^{s_k} \) symbols does exist, where for \( i \in \{1, 2, \ldots, k\} \),

\[
p_i > e!(1 + \log e), \quad \text{then } e \leq k.
\]

Argument. Assume there is such a code, then, since for the zeros \( x_1, x_2, \ldots, x_e \) of \( P_e(x) \)

\[
\prod_{i=1}^{e} x_i = e(n - e)\left(\frac{q-1}{q}\right) + e\left(\frac{e+1}{2}\right)
\]

and

\[
\prod_{i=1}^{e} (x_i - 1) = (n - 1) \cdots (n - e)\left(\frac{q-1}{q}\right)^{e},
\]

we find \( p_i \mid n - e \) \((i = 1, \ldots, k)\).

Now it is not difficult to see that (modulo \( \frac{n - e}{q - e - 1} \))
from the lower bound on $p_i$ we have $\sum_{j \neq i} x_j \neq 0 \pmod{p_i}$, so at most one of $x_i, \ldots, x_k$ is divisible by $p_i$. Furthermore any zero is divisible by one of $p_i, \ldots, p_k$ because $x_i > e!$ (and

$$\prod_{i=1}^e x_i = e!p_1 \cdots p_k e$$

which can be seen as follows:

Since $p_i \mid n - e$ we have $n > q^e$ and (cfr [4], page 115)

$$x_i > \frac{(n-e+1)(q-1)+e}{q-1+e} > \frac{(q^e-e+1)(q-1)}{q+e} > \frac{4e-e+1}{2} > e!$$

where the last two inequalities follow easily from the bounds on $p_i$. Hence, since any $p_i$ occurs in at most one zero, and any zero contains at least one $p_i$, the number $e$ of zeros is at least as large as the number of primes $k$ in $q$.

B. I shall sharpen the preceding in the case $e = 4$. I shall use the inequality $x_4 < 2x_1$ which can be deduced from Tietävänens method (see [2]).

**Theorem 4.** If a four-error-correcting perfect code on $q$ symbols does exist then either $q$ is divisible by at least four distinct primes or $\gcd(q,30) > 1$.

**Proof.** By calculating the coefficients of $P_4(x)$ we see that

1)

$$x_1 + x_2 + x_3 + x_4 = 4\left(\frac{q-1}{q}\right)(n-4) + 10$$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4(n-4)^2 + 20(n+4) + 30 - \frac{4(n-4)}{q} ((2q-1)(n-3) + 4)$$

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 = 4(n-4)^2 + 30(n-4)^2 + 90(n-4) + 100$$

$$- \frac{(n-4)}{q} \left\{(n-4)^2(12q^2 - 12q + 4) + (n-4)(24q^2 + 42q - 36) + (12q^2 + 54q + 24)\right\}.$$
2) Now if $q$ has exactly $s$ factors $p \geq 5$, from (1) we see that $p^s | n - 4$, so since
\[ (x_i - 1) = (n - 1)(n - 2)(n - 3)(n - 4) \left( \frac{q - 1}{4} \right)^4 p^4 \]
and again from (1)
\[ x_1 + x_2 + x_3 + x_4 \equiv 10 \pmod{p^s} \]
\[ x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 30 \pmod{p^s} \]
\[ x_1^3 + x_2^3 + x_3^3 + x_4^3 \equiv 100 \pmod{p^s} . \]

3) Now if $q = p_1 \cdots p_e$ we have $x_1 x_2 x_3 x_4 = 24 p_1^{s_1} p_2^{s_2} \cdots p_e^{s_e}$. If $x_1 \leq 24$ then since $x_4 < 2x_1$ (cfr.[2])
\[ x_1 + x_2 + x_3 + x_4 < 24 + 46 + 47 + 48, \text{ contradicting } \exists x_1 \equiv 10 \pmod{q^3} \text{ if } q \geq 6 \text{ and } \gcd(q,30) = 1. \text{ So } x_1 > 24. \]
So if $q$ is divisible by no more than 3 primes there is a $x_i$ and a $x_j$ such that $x_i$ and $x_j$ are divisible by the same prime $p$. Then the either two $x$ and $y$ satisfy:
\[ x + y \equiv 10 \pmod{p} \]
\[ x^2 + y^2 \equiv 30 \pmod{p} \]
\[ x^3 + y^3 \equiv 100 \pmod{p} . \]

But then $(x + y)^2 \equiv 100 \equiv x^2 + y^2 + 2xy \equiv 30 + 2xy$. So $xy \equiv 35$ and
\[ (x + y)^3 \equiv 1000 \equiv x^3 + y^3 + 3xy(x + y) \equiv x^3 + y^3 + 3 \cdot 35.10. \text{ So } x^3 + y^3 \equiv -50 \equiv 100 \pmod{p} \text{ and } p | 150 = 2 \cdot 3 \cdot 5^2. \]

Now it is not difficult to extend this theorem to the following: If a four-error-correcting perfect code on $q = p_1^{s_1} p_2^{s_2}$ symbols does exist then $q = 6$ or $q = 12$ or $q = 24$.

7. The case $e = 2$

The case $e = 2$ is particularly difficult. We have the following general approach:

Assume that a perfect double-error-correcting code of word length $n$ over a $q$-symbol alphabet does exist.

Let $q := p_1^{s_1} \cdots p_e^{s_e}$ be the prime factorization of $q$. The following observations are useful:
i) Let \( 1 + n(q - 1) + \binom{n}{2}(q - 1)^2 = p_1^{k+\alpha_1} \cdots p_e^{k+\alpha_e} \) where \( k \) is defined by \( a_i \geq 0, a_1 \cdots a_e = 0. \) Then

\[
(q - 1)((q - 1)n + q + 1)(n - 2) = 2(p_1^{k+\alpha_1} \cdots p_e^{k+\alpha_e} - q^2).
\]

ii) \( P_2(x) = x^2 - \frac{2(q - 1)}{q} (n - 2) + 3x + 2p_1^{k+\alpha_1 - 2s} \cdots p_e^{k+\alpha_e - 2s} \)

so this yields the sum and the product of the zeros of \( P_2(x) \).

iii) Now we can easily check that

\[
q(x_1 - x_2)^2 - 2(x_1 + x_2) = q - 6
\]

So if \( p_i \neq 2 \) we find \( x_1 + x_2 \equiv 3 \pmod{p_i^s} \). Furthermore we see that \( \gcd(x_1, x_2) = 1 \) if \( \gcd(q, 6) = 1 \), and if \( \gcd(q, 3) = 1 \) and \( 4 | q \).

iv) Since \( x_1 + x_2 = \frac{2(q - 1)(n - 2) + 3 \in \mathbb{Z} \) we find \( x_1 + x_2 \equiv 3 \pmod{x_1, x_2} \). Furthermore, since \( q^n - p_1^{k+\alpha} \cdots p_e^{k+\alpha} = \sum_{m=3}^{n} \binom{n}{m}(q - 1)^m \) we have \( \sum_{m=3}^{n} \binom{n}{m}(q - 1)^m \) have \( p_1^{k+\alpha_1} \cdots p_e^{k+\alpha_e} \equiv 1 \pmod{(q - 1)} \) and \( x_1 x_2 \equiv 2 \pmod{(q - 1)} \). So for every prime factor \( t \) of \( q - 1 \) we have \( x_1 \equiv 1 \pmod{t} \) and \( x_2 \equiv 2 \pmod{t} \) or vice versa.

v) According to the method in [2] and [4], page 115 we find

\[
\frac{(n-1)(q-1)+2}{q+1} < x_1 < x_2 < 2x_1 \quad \text{(and of course } x_2 < n) \]

These observations lead easily to the following results:

Claim. There is no perfect double-error-correcting code with any word length \( n > 5 \) over a \( q \)-symbol alphabet if:

a) \( q = 2p^k \) and \( p \equiv 1 \pmod{8} \)

b) \( q = 2p^{2s} \) and \( p \equiv 5 \pmod{8} \)

c) \( q = 2^k \) and \( k \geq 2 \) and \( p \equiv 1 \pmod{4} \)

d) \( q = 2^k \) and there is no \( s \in \mathbb{N} \) such that \( 2^s = 3 \pmod{p} \) \( (p = 7, 31, ...) \)

e) \( q = p_1^{s_1} p_2^{s_2} \) and \( \gcd(6, p_1 p_2) = 1 \) and \( p_1 \equiv 1 \pmod{p_2} \) \( (q = 5^{s_1} 11^{s_2}, ...) \).

I shall give one example:

Theorem 5. A perfect code with parameters \( (n > 5), e = 2, q = 2p^k \) does not exist if \( p \equiv 1 \pmod{8} \) nor if \( \ell = 2s \) and \( p \equiv 5 \pmod{8} \).
Proof. In this case we have from ii) \(x_1 x_2 = 2^a p^b\). Since from iii) \(x_1 + x_2 \equiv 3 \pmod{p}\) we find \(x_1 = 2^a, x_2 = 2^b p^b\). Since \(q \geq 6, P_2(4) > 0\) so \(x_1 > 4\) and \(a \geq 3\). Now from i) we have:

\[(q - 1)((q - 1)n + q + 1)(n - 2) \equiv 0 \pmod{8}.

Hence either \(n\) is even and \(n \equiv 2 \pmod{8}\), or \(n\) is odd and \((q - 1)n + q + 1 \equiv 0 \pmod{8}\). In the latter case we have:

- if \(n \equiv 1 \pmod{8}\), \(2q \equiv 4p^b \equiv 0\), contradiction
- if \(n \equiv 3 \pmod{8}\), \(4q - 2 \equiv 0\), contradiction
- if \(n \equiv 5 \pmod{8}\), \(6q - 4 \equiv 0\), possible!
- if \(n \equiv 7 \pmod{8}\), \(8q - 6 \equiv 0\), contradiction.

Now we distinguish between \(n \equiv 2 \pmod{8}\) and \(n \equiv 5 \pmod{8}\) and remark that \(p^2 \equiv 1 \pmod{8}\), so \(p^{2k} \equiv 1 \pmod{8}\) and \(p^{2k+1} \equiv p \pmod{8}\) for \(k \in \mathbb{N}\).

a) \(n \equiv 2 \pmod{8}\). From ii) we then have \(x_1 + x_2 \equiv 3 \pmod{8}\), so \(x_1 = 2^a, x_2 = p^b\) and \(p^b \equiv 3 \pmod{8}\), \(p \equiv 3 \pmod{8}\).

b) \(n \equiv 5 \pmod{8}\). From ii) we then have, substituting \(n = 5 + 8t\)

\[(2p^b - 1)(3 + 8t) + 3p^b = p^b(x_1 + x_2)\).

Then modulo 8 we see:

- if \(p^b \equiv 1 \pmod{8}\) is \(x_1 + x_2 \equiv 6\) if \(p^b \equiv 3 \pmod{8}\) is \(x_1 + x_2 \equiv 0\)
- if \(p^b \equiv 5 \pmod{8}\) is \(x_1 + x_2 \equiv 2\) if \(p^b \equiv 7 \pmod{8}\) is \(x_1 + x_2 \equiv 4\).

If \(p^b \equiv 1 \pmod{8}\) or \(p^b \equiv 5 \pmod{8}\) we then have \(\{x_1, x_2\} = \{2^{a-1}, 2^b p\}\) and in iii) we find:

\[4p^{2b+1} - 2p^b \equiv p - 3 \pmod{8}\]

This is a contradiction if \(p^b \equiv 1 \pmod{8}\) and \(p \equiv 1\) or \(5 \pmod{8}\).

In fact it is rather easy to deal with fixed \(q\). I did for \(q \leq 30\). I shall give again one example. In the following all unannounced symbols stand for unspecified naturals.

Theorem 6. There exists no double-error-correcting perfect code on fifteen symbols.
Proof. In this case from ii) we have $x_1 x_2 = 2.3^1 5^2$ where $\beta_1 = \alpha_1 + \alpha_2 = 0$. Furthermore since $x_1 < x_2 < 2x_1$ we have $\beta_1 > 0$.

Now from iii) $x_1 + x_2 \equiv 3 \pmod{5}$, so $x_1$ and $x_2$ have no factor 5 in common and again from iii) $x_1 + x_2 \equiv 0 \pmod{3}$, so since $\beta_1 > 0$ both $x_1$ and $x_2$ are divisible by 3. Furthermore (with $3.5 = p_1 p_2$) we see from (iv) that if $\alpha_i \neq 0$ then $p_1^{\alpha_i} \equiv 1 \pmod{7}$, so $\alpha_i = 6s$.

Therefore, writing $k$ instead of $k-2$, we have four possibilities (with $\beta \gamma \geq 1$):

a) $\{x_1, x_2\} = \{x, y\}$ and $x = 2.3^5 5^{k+6s}$, $y = 3^\gamma$, $\beta + \gamma = k$  
b) $\{x_1, x_2\} = \{x, y\}$ and $x = 3^{5^k} 5^{6s}$, $y = 2.3^{\gamma}$, $\beta + \gamma = k$  
c) $\{x_1, x_2\} = \{x, y\}$ and $x = 2.3^{5^{k}}$, $y = 3^\gamma$, $\beta + \gamma = k + 6s$  
d) $\{x_1, x_2\} = \{x, y\}$ and $x = 3^{5^k}$, $y = 2.3^{\gamma}$, $\beta + \gamma = k + 6s$.

From v) the cases a) and b) are impossible since then $x > 2y$. Now we distinguish between c) and d) and use iii): $15(x_1 - x_2)^2 - 2(x_1 + x_2)^2 = 9$.

c) $15(3^{5^k} - 3^{\gamma})^2 - 2(3^{5^k} + 3^{\gamma}) = 9$ and $\beta + \gamma = k + 6s \geq 6$, $\beta \gamma \geq 1$.

Hence $-2(3^{5^k} + 3^{\gamma}) \equiv 9 \pmod{27}$, so since $\beta + \gamma \geq 6$ we have $\beta = 2$ and $\gamma \geq 4$. Hence $15(3^{5^k} - 3^{\gamma-2}) = 2(2^{5^k} + 3^{\gamma-2}) = 1$, so $-4.5^k \equiv 1 \pmod{9}$ and $k + 1 = 6t$.

Furthermore, modulo 5 we have $-2.3^\gamma \equiv 4 \pmod{5}$ and since $\gamma = k + 6s - \beta = = k + 6s - 2 = 6t + 6s - 3$ we find $3^{6t+6s-2} \equiv 4 \pmod{5}$ so $6t + 6s - 2 = = 2 + 4u$, $6t + 6s = 4v = 12w$. Now from iv) $x_1 + x_2 \equiv 3 \pmod{7}$, so

$$18.5^{6t-1} + 3^{4(4w-1)} \equiv 3 \pmod{7} \equiv 4.5^{6t-1} + (-1)^{4w-1},$$

so $5^{6t-1} \equiv 1 \pmod{7}$ and $6t - 1 = 6z$, which is a contradiction.

d) $15(3^{5^k} - 2.3^\gamma)^2 - 2(3^{5^k} + 2.3^\gamma) = 9 \pmod{27}$ gives $-2(3^{5^k} + 2.3^{\gamma}) \equiv 9 \pmod{27}$. Hence as above $\beta = 2$, $\gamma = k + 6s - 2$ and again since $\gamma \geq 4$ we see like in c) that $-2.3^k \equiv 1 \pmod{9}$, so $k = 6t + 4$. Then modulo 5 we have $-2.3^{6t+6s+2} \equiv 2.3^{6t+6s+3} \equiv 4 \pmod{5}$, so $6t + 6s + 3 = 3 + 4u$ and $6t + 6s = 12w$. Finally from iv) $x_1 + x_2 \equiv 3 \pmod{7}$ gives $9.5^{6t+4} + 2.9.3^{12w} \equiv \equiv 2.5^{6t+4} + 4$. Then $5^{6t+4} \equiv 3 \pmod{7}$, so $6t + 4 = 6v + 5$, which is a contradiction.

So we conclude that $q = 15$ is impossible.
8. References


