On the nonexistence of perfect 5, 6 and 7-error-correcting codes over GF(q)

Citation for published version (APA):

Document status and date:
Published: 01/01/1970

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the author's version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
https://www.tue.nl/index.php?id=71870

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.

Download date: 13. Feb. 2019
On the nonexistence of perfect 5-, 6- and 7-Hamming-error-correcting codes over GF(q)

by

J.H. van Lint

T.H.-Report 70-WSK-06

May 1970
Introduction. This report is intended as a supplement to the paper "Nonexistence theorems for perfect codes" published in the proceedings of the A.M.S. Symposium on Computers in Algebra and Number Theory 1970. We shall give the details of the proofs of nonexistence for the codes mentioned in the title. Numbers used indicate formulae and theorems of the paper mentioned above (which consists of the sections 1 to 4).

5. An extension of theorems 2 and 3

Let us assume that $e$ is a prime, $p = e$ and $q = p^a > e$ and that a perfect code exists with these parameters. By (3.5) we have $n \equiv e \pmod{p^{a-1}}$. Let $p^c \| (n-e)$. Then the first term in the sum in (3.7) is divisible by $p^{c-1}$ exactly. Hence $c > a+1 \geq 3$. The terms with $0 < j < e$ are divisible by $p^{c+1+a_j}$ and the last term by $p^{ae}$ exactly. Since the sum must be divisible by $q^e+1$ we find that $c-1 = ae$ and hence $n-e \equiv 0 \pmod{pq}$. Just as in the proof of theorem 1 this implies that $x_1 \leq e!$ and then (3.4) yields $e! \geq e^2$ which is a contradiction. We have proved

THEOREM 3': If $e$ is a prime, $q = p^a$ and if a nontrivial perfect $e$-error-correcting code over GF$(q)$ exists then $p < e$ or $q = e$.

We now study the case $q = p = e.$ First remark that for any 3-tuple $e,q,n$ the following formulae are consequences of (3.7):

\[
(5.1) \quad \frac{1}{e!} \cdot (n-2)(n-3) \cdots (n-e)[(qe-1)(n-1)+qe] \equiv 0 \pmod{q^2},
\]

\[
(5.2) \quad \frac{1}{e!} \cdot (n-3)(n-4) \cdots (n-e)[(n-1)(n-2)-qn(n-2)e+\frac{1}{2}q^2n(n-1)e(e-1)] \equiv 0 \pmod{q^3}.
\]

Now if $q = p = e$ exactly one of the factors $(q-1)$ is divisible by $q$. Then (5.2) implies that $n \equiv 3,4,\ldots,e \pmod{q^3}$ or $n \equiv q^2 + 1 \pmod{q^4}$ or $n \equiv q^3 + 2 \pmod{q^4}$. Since $n > e$ we find

\[
(5.3) \quad \text{If a nontrivial perfect } e \text{-error-correcting code exists over GF}(q) \text{ where } q = e \text{ (prime) then } n = q^2 + 1 \text{ or } n = q^3 + 2 \text{ or } n > q^4.
\]
6. Nonexistence of perfect 5-error-correcting codes

By theorem 1 we need only study $q = p^a$ where $p \leq 5$. If $p = 5$ then theorem 3' shows we need only consider $q = 5$. If $p = 2$ or 3 then theorem 2 shows that only $q \leq 4$ is possible.

(a) If $q = 5$ then the first term on the right-hand side of (3.2) is either not divisible by 5 or divisible by 25 as was shown above. Since the second term is 15 there is a zero of $P_5$ which is not divisible by 25 and therefore $x_1 \leq 120$. Together with (3.4) this implies $n < 273$ and by (5.3) we then have $n = 26$ or $n = 127$. The values $e = q = 5$ and $n = 26$ or 127 do not satisfy (1.1).

(b) If $q = 4$ then by (3.5) $n \equiv 1 \pmod{4}$. If we substitute this in (5.1) we find $n \equiv 5 \pmod{8}$. Then by (3.2) $P_e$ has an odd zero and therefore $x_1 \leq 15$. Then (3.4) yields $n \leq 42$. In [8] these possibilities were excluded.

(c) If $q = 3$ then by (3.5) $n \equiv 2 \pmod{3}$. If we substitute this in (5.2) we find $n \equiv 5$ or 11 $\pmod{27}$. Then by (3.2) the sum of the zeros of $P_e$ is not divisible by 9 and hence $x_1 \leq 120$ and once again by (3.4) we have $n \leq 421$. This leaves a range covered by [8]. There were no solutions to (1.1).

(d) If $q = 2$ we refer to [12] Theorem 7, Corollary 2 and [8].

Since all possibilities have been considered we have proved:

THEOREM 6: There are no nontrivial perfect 5-error-correcting codes over $GF(q)$.

7. Nonexistence of perfect 6-error-correcting codes

In a search for 6-error-correcting codes over $GF(q)$ we must consider only $q < 6$, $q = 2^a > 6$ and $q = 3^a > 6$ by theorems 1 and 2.

(a) If $q = 2^a > 6$ then by theorem 3 we have $n \leq 95$. From (3.5) we find $n \equiv 2 \pmod{4}$ and then (5.2) yields $n \equiv 2$ or $6 \pmod{27}$ and therefore $n = 6$, i.e. only the trivial one word code is possible.

(b) If $q = 3^a > 6$ then we use the method of theorem 3. The bound $M_3(6)$ is too large since in the proof it was shown that there is a zero of $P_3$ with at most one factor 3. Hence $x_1 \leq 240$ and hence by (3.4) $n \leq 424$. 
By (3.5) we know \( n \) is divisible by 3 and from (5.2) it then follows that \( n \equiv 3 \) or 6 (mod 37), i.e. \( n = 6 \) (trivial code).

(c) If \( q = 5 \) then from (3.5) we find \( n \equiv 1 \) (mod 5) and then from (5.1) it follows that \( n \equiv 6 \) (mod 25). By (3.2) there is a zero of \( P_6 \) which is not divisible by 5 and therefore \( x_1 \leq 144 \) and hence \( n \leq 363 \). The values \( e = 6, q = 5, n \leq 363 \) were excluded in [8].

(d) If \( q = 4 \) then by (3.5) \( n \) is even. From (5.1) it follows that \( n \equiv 4 \) (mod 2^6) or \( n \equiv 2 \) or 6 (mod 2^5). For each of these cases we find from (3.2) that not all the zeros of \( P_6 \) are divisible by 8 and therefore \( x_1 \leq 180 \) and hence \( n \leq 543 \). The values \( e = 6, q = 4, n \leq 543 \) were excluded in [8].

(e) If \( q = 3 \) the reasoning used up to now will lead to values of \( n \) not covered by the computer search in [8]. So we proceed a little more carefully. From (5.2) we find that \( n \equiv 3 \) or 6 (mod 81). If \( n \equiv 6 \) (mod 81) then from (3.2) we find in the usual way that \( x_1 \leq 240 \) and therefore \( n \leq 962 \) which is still in the range excluded by [8]. If on the other hand \( n \equiv 3 \) (mod 81) then we consider the first 4 terms in the sum of (3.7). The sum of these terms is divisible by \( 3^4 \) which implies \( n \equiv 165 \) (mod 243). If we then compute the powers of 3 which divide the last three terms of the sum in (3.7) they turn out to be \( 3^9, 3^{10} \) and \( 3^3 \) respectively. Hence also the sum of the first 4 terms in (3.7) is divisible by \( 3^9 \) which then implies \( n \equiv 1623 \) (mod 37). From (3.2) we now find that \( x_1 \leq 720 \) and therefore by (3.4) \( n \leq 2882 \). Apparently \( n = 1623 \) is the only possibility in this case. Substitution in (3.7) shows that this value of \( n \) is also excluded.

(f) If finally \( q = 2 \) then (3.2) yields \( x_1 + x_2 + \ldots + x_6 = 3(n+1) \) and \( n \equiv -1 \) (mod 8) would make the first term in (3.7) odd which is impossible. So at least one zero is not divisible by 8, i.e. \( x_1 \leq 180 \) and therefore \( n \leq 1260 \). These values were excluded in [11].

Now (a) to (f) show that we have

**Theorem 7:** There are no nontrivial perfect 6-error-correcting codes over \( GF(q) \).
8. Nonexistence of perfect 7-error-correcting codes

It is clear that we cannot go on in this way indefinitely. So as a last attempt to come up with a new perfect code we treat the case of 7 errors. By theorems 2 and 3' there are only 5 cases to be studied, namely \( q = 2, 3, 4, 5 \) or 7.

(a) If \( q = 7 \) and \( n \not\equiv 0 \pmod{7} \) then by (3.2) there is a zero not divisible by 7 and hence \( x_1 \leq 6! = 720 \) and \( n \leq 264 \). By (5.3) this implies that \( n = 50 \) and by [8] there is no perfect code with \( e = q = 7, n = 50 \). If \( n \equiv 0 \pmod{7} \) then from (3.7) we find \( n \equiv 7 \pmod{7^7} \) and by (3.2) and (3.4) we then have in the usual way: \( x_1 \leq 7! \) and \( n \leq 10924 \). Therefore \( n = 7 \), i.e. the code is trivial.

(b) If \( q = 5 \) then by (3.5) we have \( n \equiv 2 \pmod{5} \). From (3.7) it follows that \( n \equiv 2 \) or 7 \( \pmod{25} \) and then we see from (3.2) that there is a zero not divisible by 5 and hence \( x_1 \leq 1008 \). From (3.4) it follows that \( n \leq 2776 \). Since this is not covered by [8] we must find a sharper congruence condition on \( n \) from (3.7). First assume \( n \equiv 2 \pmod{25} \). Then in (3.7) all the terms with \( j \geq 3 \) are divisible by 5\(^6\) and so is the right-hand side. Considering the sum of the first 3 terms then shows that \( n \equiv 3577 \pmod{5^6} \) disposing of the possibility \( n \equiv 2 \pmod{25} \). Next we consider \( n \equiv 7 \pmod{25} \). In that case just as in the proof of theorem 1 we see that the first term and last term of the sum in (3.7) are divisible by the same power of 5, i.e. \( n \equiv 7 \pmod{5^7} \) and therefore the code is trivial.

(c) If \( q = 4 \) then by (3.5) \( n \equiv 3 \pmod{4} \). Substitution in (3.7) yields \( n \equiv 3 \pmod{2^6} \) or \( n \equiv 7 \pmod{2^{14}} \). In the second case there is an odd zero of \( P_7 \) and hence \( x_1 \leq 315 \) and \( n \leq 1053 \), i.e. \( n = 7 \) and the code is trivial. In the first case \( 2^6 \| n-3 \) and then by (3.2) \( 2^4 \| (x_1 + x_2 + \ldots + x_7) \). Therefore there is a zero which is not divisible by 32 and hence \( x_1 \leq 2^4 \cdot 315 = 5040 \). We now find \( n \leq 16803 \). Since again this is outside of the range of [8] we are once more forced to do a more detailed analysis. All terms in (3.7) with \( j > 3 \) are divisible by \( 2^{14} \). So the sum of the first four terms must also be divisible by \( 2^{14} \). This implies \( n \equiv 13251 \pmod{2^{14}} \) and therefore \( n \) must be 13251. We substitute this in (3.7). The result is not a power of 2 (in fact not divisible by \( 2^{15} \)).
(d) If \( q = 3 \) then from (3.5) we have \( n \equiv 1 \pmod{3} \). Then considering the first two terms of the sum in (3.7) we find \( n \equiv 4 \) or \( 7 \pmod{3^5} \). By (3.2) there is a zero of \( P_7 \) which is not divisible by 3. Therefore \( x_1 \leq 560 \) and \( n \leq 2522 \). By now we are not surprised that a sharper look at (3.7) is necessary. By taking the first five terms of the sum in (3.7) the possibility \( n \equiv 4 \pmod{3^5} \) is excluded and we find \( n \equiv 7 \pmod{3^{12}} \) i.e. \( n = 7 \) and the code is trivial.

(e) If \( q = 2 \), the hardest case to study, we do not use our methods but refer to the attack described in [12]. By [12] Theorem 7 one of the numbers \( m := n+1 \) or \( m^6 - 21m^5 + 217m^4 - 1155m^3 + 3934m^2 - 6384m + 8448 \) is a divisor of \( 2^8 \cdot 315 \). On the other hand it was found in [11] that \( n \) is at least 270. These requirements are contradictory and the last possibility is disposed of.

Once again the result is negative:

**THEOREM 8:** There are no nontrivial perfect 7-error-correcting codes over \( \text{GF}(q) \).

At the moment it seems more interesting to find a new idea which would make calculations of the type discussed in this report superfluous or to generalize Lloyd's theorem to the case of nonfield alphabets. For practical purposes the computer search in [8] has already excluded all possibilities where the alphabet is a field.