On perfect binary arithmetic codes which can correct two errors or more

Antoine C. Lobstein

Centre National de la Recherche Scientifique,
URA 251, Télécom Paris,
Département Informatique, 46 rue Barrault, 75634 Paris Cedex 13, France.

Abstract. We state here that, for modulus m odd and less than $2^{29} + 2^{27} - 1$, no (nontrivial) perfect binary arithmetic code, correcting two errors or more, exists (this is to be taken with respect to the Garcia-Rao modular distance). In particular, in the case $m = 2^n \pm 1$, which is most frequently studied, no such code exists for $m < 2^{33} - 1$.

I Introduction

A *modified binary form* of an integer x is

$$x = \sum_{i=0}^{n} x_i \cdot 2^i, \quad \text{where } |x_i| < 2 \text{ for all } i = 0, 1, \ldots, n. \tag{1}$$

Form (1) is called *minimal* if the number of its nonzero coefficients x_i is minimal. A minimal form is not unique. If the coefficients x_i in (1) satisfy $x_i \cdot x_{i+1} = 0$ for all $i = 0, 1, \ldots, n-1$, then form (1) is called a *nonadjacent form* (NAF). A NAF has the following properties: it exists for all integer x, it is unique, minimal, and easy to compute. The *arithmetic weight*, $W(x)$, of x is the number of nonzero coefficients in a minimal form of x.

Let m be a fixed integer ($m > 0$), and let Z_m be the ring of integers $0, 1, \ldots, m-1 \pmod m$. The *modular weight*, $w_m(x)$, of an element x in Z_m is $\min(W(x), W(m-x))$, and the *modular distance*, d_m, between elements in Z_m is the modular weight of their difference (see for instance [9] or [8, pp. 449–453] for all these introductory definitions and properties).

w_m does *not* always induce a metric. Recently, Ernvall [2] completely characterized the moduli m for which d_m is a metric (i.e. it satisfies the triangle inequality); in the binary case, d_m is a metric if and only if the NAF of m has one of the following forms:

1) $m = 2^n + 2^{n-2} \pm 2^i, i \leq n-4$;
2) $m = 2^n - 2^j \pm 2^i, n-5 \leq j \leq n-2, i \leq j-2$;
3) $m = 2^n \pm 2^j, j \leq n-2$;
4) $m = 2^n$.

Let C be a subset of Z_m.

If d_m is a metric and is such that $d_m(x, y) \geq 2e + 1$ for all x and y in C ($x \neq y$), then C is capable of correcting e arithmetic errors. C is a *perfect* e-error-correcting code if moreover for each element z in Z_m there is a codeword within

distance e from z. In other words, the spheres of radius e, centered at the words of a perfect code, both fill in Z_m and do not intersect (partition of Z_m).

Very little is known about perfect arithmetic codes; some classes of perfect single-error-correcting binary codes are known (see [8, pp. 456–457] and [1]), but so far nothing has been said about perfect two-or-more-error-correcting codes, even in the binary case.

This situation strongly contrasts with algebraic block codes, for which it is well-known that the only nontrivial perfect codes (with respect to the Hamming distance) are codes having the same parameters as the single-error-correcting Hamming codes (length $n = (q^m - 1)/(q - 1)$, cardinality $K = q^{n-m}$, minimum distance $d = 3$, where q is any prime power), and codes equivalent either to the 3-error-correcting binary Golay code ($n = 23$, $K = 2^{12}$, $d = 7$), or to the 2-error-correcting ternary Golay code ($n = 11$, $K = 3^6$, $d = 5$) (see [7, pp. 179–186]).

Notice that an e-error-correcting code, with length n and B words over an alphabet with q symbols, is perfect if and only if

$$B \cdot \left(1 + (q-1)\binom{n}{1} + \ldots + (q-1)^e \binom{n}{e}\right) = q^n, \tag{2}$$

which expresses that the number of codewords multiplied by the volume of a sphere of radius e is equal to the volume of the whole space (see [7, p. 20]).

However, in the binary case, Ernvall [3] got some knowledge about perfect more-than-one-error-correcting arithmetic codes by deriving the volume of a sphere. We shall use her results in Section II.

II Perfect Codes

An e-error-correcting arithmetic code with modulus m and B words is perfect if and only if $B = m/V(m, e)$, where $V(m, e)$ is the volume of a sphere of radius e (independent of its centre): $V(m, e) = |\{x \in Z_m / w_m(x) \leq e\}|$. This is simply the transposition of equality (2) in the arithmetic case. But here the volume of a sphere is much more difficult to derive. However Ernvall [3] managed to compute $V(m, e)$ $(e \geq 2)$.

Her results are as follows:

- If $m = 2^n \pm 1$ $V(m, e) = \sum_{t=0}^{e} \left(2^t \binom{n-t}{t} + 2^t \binom{n-t-1}{t-1}\right)$;
- If $m = 2^n + 2^{n-2} \pm 1$
  $V(m, e) = \sum_{t=0}^{e} \left(2^t \binom{n-t}{t} + 3.2^{t-1} \binom{n-t-1}{t-1} + 2^{t-1} \binom{n-t-2}{t-1}\right)$;
- If $m = 2^n - 2^{n-2} \pm 1$
  $V(m, e) = \sum_{t=0}^{e} \left(2^t \binom{n-t}{t} + 2^t \binom{n-t-2}{t-1} - 2^{t-1} \binom{n-t-2}{t-2}\right)$;
- If $m = 2^n - 2^{n-3} \pm 1$
  $V(m, e) = \sum_{t=0}^{e} \left(2^t \binom{n-t}{t} + 2^t \binom{n-t-2}{t-1} + 2^t \binom{n-t-3}{t-2} - 2^{t-1} \binom{n-t-3}{t-3}\right)$;

- If $m = 2^n - 2^j \pm 1$ with $n-5 \leq j \leq n-4$

$$V(m,e) = \sum_{t=0}^{e} \left(2^t \binom{n-t}{t} + 2^t \binom{n-t-2}{t-1} + 2^{t+1} \binom{n-t-3}{t-2} - 2^{t-1} \binom{j+2-t}{j-n+t+2} + 2^{t-1} \binom{j-t}{t-2}\right);$$ (with $\binom{n}{j} = 0$ for $n < j$ or $j < 0$).

The moduli m considered here are those for which d_m is a metric (see Introduction), *restricted to odd cases*, because these results were derived exclusively for *AN-codes* (an AN-code C is a subset of Z_m which is generated by a divisor A of m : $C = \{0, A, 2A, \ldots, (B-1)A\}$ with $B \cdot A = m$), and an AN-code which corrects at least two errors has necessarily odd modulus [3].

A *necessary* condition to have a perfect code correcting e errors is that $m/V(m,e)$ is an integer.

By computer we checked the above expressions up to $m = 2^{33} + 1$.

We found 4 moduli m for which $m/V(m,e)$ is an integer, all of them with e equal to 2:

- for $m = 1791$ $V(m,2) = 199$ and $m/V(m,2) = 9$;
- for $m = 4097$ $V(m,2) = 241$ and $m/V(m,2) = 17$;
- for $m = 2^{29}+2^{27}-1 = 671,088,639$ $V(m,2) = 1671$ and $m/V(m,2) = 401,609$;
- for $m = 2^{33} - 1 = 8,589,934,591$ $V(m,2) = 2047$ $(= 2^{11} - 1)$ and $m/V(m,2) = 4,196,353$.

If we are looking for perfect double-error-correcting AN-codes however, they must be of the form $\{0, V(m,2), 2V(m,2), \ldots, ((m/V(m,2))-1)V(m,2)\}$.

But $199 = 2^8 - 2^6 + 2^3 - 2^0$, which proves that $W(199) = 4$, so $d_m(0,199) \leq 4$; $241 = 2^8 - 2^4 + 2^0$, so $d_m(10,241) \leq 3$; $19 \cdot 1671 = 31,749 = 2^{15} - 2^{10} + 2^2 + 2^0$, so $d_m(0, 19 \cdot 1671) \leq 4$; and $d_m(0,2047) \leq 2$.

This proves that such codes do not exist.

But perfect codes, other than AN-codes, could exist, for these moduli.

What we prove in [5] and [6] is that, for $m = 1791$ and $m = 4097$, there is no perfect double-error-correcting code.

As a consequence, the first (odd) modulus m for which there could be a perfect code correcting at least two errors is $m = 2^{29} + 2^{27} - 1$ (and in the particular case $m = 2^n \pm 1$, which is of great theoretical and practical interest, such a code can exist only for $m \geq 2^{33} - 1$), whereas numerous perfect single-error-correcting codes exist for small values of m ($m = 22$, $m = 33$, $m = 39$, $m = 52$, $m = 65$, or $m = 304$ for instance, see [8],[1]).

III Conclusion

As a conclusion, three remarks which lead to open problems:

- this study, limited to rather small values of m, now requires other methods in order to prove either the existence or nonexistence of perfect binary

codes correcting two errors or more. For example, in the algebraic case, in order to determine all perfect codes (see Introduction), of great importance is Lloyd's theorem (see [7, p. 179]), giving, for a perfect code, necessary conditions on the zeros of the so-called Lloyd polynomial, constructed with Krawtchouk polynomials. The same approach (which has been used in [10], where there is an extension of Lloyd's theorem to metrics other than the Hamming distance, including the Lee metric and the Clark-Liang modular metric) might be of interest in our case;

- In Section II is given the volume of a sphere when d_m is a metric and m *is odd,* because AN-codes necessarily lead to odd m. If we are interested in perfect codes other than AN-codes however, we also have to consider even m (for which d_m is a metric), and to compute the volume of a sphere in this case, which could give perfect (non AN-) codes;
- Very recently Ernvall [4] derived the volume of the sphere in the nonbinary case, settling, for AN-codes, almost all cases for which she had proved [2] that d_m is a metric. Now, do perfect nonbinary codes exist?

References

1. J. Astola, *A note on perfect arithmetic codes*, IEEE Trans. on Inform. Theory **IT-32** (1986), 443–445.
2. S. Ernvall, *On the modular distance*, IEEE Trans. on Inform. Theory **IT-31** (1985), 521–522.
3. S. Ernvall, *The Hamming bound for binary arithmetic AN codes*, Ars Combinatoria **20-B** (1985), 207–227.
4. S. Ernvall, *The Hamming bound for nonbinary arithmetic AN codes*, Ars Combinatoria **25-B** (1988), 31–53.
5. A. Lobstein, *On the nonexistence of a perfect binary arithmetic code with modulus 1791*, ENST Report **88D013** (1988).
6. A. Lobstein, *On the nonexistence of a perfect binary arithmetic code with modulus 4097*, ENST Report **88D013** (1988).
7. F.J. MacWilliams and N.J.A. Sloane, "The theory of error-correcting codes", North-Holland, 1983.
8. W.W. Peterson and E.J. Weldon, Jr., "Error-correcting codes", Cambridge: MIT Press, 1972.
9. T.R.N. Rao and O.N. Garcia, *Cyclic and multiresidue codes for arithmetic operations*, IEEE Trans. on Inform. Theory **IT-17** (1971), 85–91.
10. P. Solé, *Covering radius and association schemes*, In French, Thèse de Docteur-Ingénieur, Ecole Nationale Supérieure des Télécommunications (1987). Paris, France.