Discrete Mathematics 89 (1991) 185–194
North-Holland

On the parameters of codes for the Lee and modular distance

Patrick Solé

School of Computer and Information Science, Syracuse University, 313 Link Hall, Syracuse, NY 13244–1240, USA
Current address: CNRS, I3S, 250 r.A. Einstein, 06560 Valbonne, France

Received 25 November 1987
Revised 6 September 1988

Abstract

Solé, P., On the parameters of codes for the Lee and modular distance, Discrete Mathematics 89 (1991) 185–194.

We introduce the concept of a *weakly metric* association scheme, a generalization of metric schemes. We undertake a combinatorial study of the parameters of codes in these schemes, along the lines of [9]. Applications are codes over Z_q for the Lee distance and arithmetic codes for the modular distance.

Our main result is an inequality which generalizes both the Delsarte upper bound on covering radius, and the MacWilliams lower bound on the external distance, yielding a strong necessary existence condition on completely regular codes.

The external distance (in the Lee metric) of some self-dual codes of moderate length over Z_5 is computed.

1. Introduction

The external distance s' of a code C for the Hamming metric, introduced by Delsarte [9], is a useful upper bound on the covering radius of a code [7]. It can be computed from the distance distribution. If C is linear, s' is the number of nonzero weights of the orthogonal dual. Recently, Helleseth [10] noted that this bound failed in the case of arithmetic codes for the modular distances, and proposed another bound.

In this work we introduce a new parameter, still called external distance, and denoted by μ, which is well suited to metrics less regular than the Hamming metric, like the Lee metric or the modular distance, and can be computed either from the Lee composition distribution [12], or from enumeration of cyclotomic cosets. We recover Helleseth's bound and give a tighter bound, which applies equally well to the Lee metric. As a by-product, we obtain results on the regularity of codes. An appendix collects some numerical applications to self-dual codes over Z_5.

2. Weakly metric schemes

2.1. *Definitions*

A *commutative association scheme* with t classes consists of a finite set X along with a partition $R=(R_0, R_1, \ldots, R_t)$ on $X\times X$, satisfying the following axioms:

A_1: $R_0=\{(x,x)\mid x\in X\}$,

A_2: $R_i^{-1}=\{(y,x)\mid (x,y)\in R_i\}=R_{i'}$, for some i',

A_3: The cardinality of $\{z\mid (x,z)\in R_i \text{ and } (z,y)\in R_j\}$ is a function p_{ij}^k which depends on k, but not on $(x,y)\in R_k$,

A_4: $p_{ij}^k=p_{ji}^k$.

We call a *quasi-distance* on X any mapping from X^2 to the nonnegative reals satisfying the triangle inequality. If furthermore, this mapping is symmetric, it is called a *distance*, or *metric*. If we replace A_2 by the stronger condition A_2': $R_i^{-1}=R_i$ the scheme is said to be of the Bose–Mesner type. We call *weakly metric* [19] an association scheme equipped with a quasi-distance d constant on the classes of the scheme. This means that there exists a monovariate function, still denoted by d, from $[0,\ldots,t]$ to the nonnegative reals such that:

$$aR_kb \;\Rightarrow\; d(a,b)=d(k). \tag{1}$$

In Tarnanen's terminology [16], d is said to be R-invariant. However, we will not use the concept of quasi-metric scheme, which is central in [16]. When d is graphic, i.e., is the shortest path distance of some graph on X, [9] and $d(k)=k$, we recover exactly the definition of a metric scheme [8]. In the following subsections we construct examples of both practical and theoretical interest.

2.2. *An all-purpose construction*

Let X be a finite set endowed with a metric d. We suppose that a subgroup of the group G of isometries of d acts transitively on X, and we consider the action of G on the cartesian product $X\times X$. Let $(R_0, R_1, \ldots, R_t)$ be the orbits with $R_0=\{(x,x)\mid x\in X\}$. We assume that every R_i is symmetric.

Proposition 1. *(X, R) is a weakly metric scheme, of Bose–Mesner type.*

Proof. The pair (X, R) satisfies axioms A_1, A_2, A_3 by Lemma 1.2 of [1]. Axiom A_4 is entailed by Lemma 1.5 of [1]. Since G is a subgroup of the isometry group, d is constant on the R_i. □

2.3. *The Hamming association scheme*

Let GF(q) denote the finite field with q elements. The Hamming scheme $H(n,q)$ [8, 12] is defined by:

$$xR_ky \;\Leftrightarrow\; d_H(x,y)=k \tag{2}$$

where d_H stands for the Hamming distance [12]. The Hamming scheme is metric, hence weakly metric for the Hamming distance. This can be recovered from Proposition 1 by letting $X = \mathrm{GF}(q)^n$ and $G = S_q \int S_n$ where $\int$ denotes the wreath product [1].

2.4. The Lee association scheme

We consider the scheme on Z_q with $s = [q/2]$ classes (called ordinary q-gon in [1]):

$$xR'_k y \iff x - y = \pm k.$$

For any vector z in Z_q^n we define its Lee composition, denoted $lc(z)$: $lc(z) = (c_0, c_1, \ldots, c_s)$ where the c_i are given by:

$$c_i = |\{j \in [0, n] \mid z_j = \pm i\}|.$$

We now define a scheme with $N = \binom{n+s}{s} - 1$ classes on Z_q^n by: $xR_{\boldsymbol{k}}y \iff lc(x-y) = \boldsymbol{k}$ where $\boldsymbol{k}$ is any composition vector.

This scheme is called the *extension* of order n of the q-gon and is denoted by $L(n, q)$ (and extensively studied) in [16]. It was first introduced for q an odd prime in [8]. The Lee metric is constant on the classes of the scheme, since we can define the Lee distance by:

$$xR_{\boldsymbol{k}}y \implies d(x, y) = k_1 + 2k_2 + \cdots + sk_s.$$

Starting from this definition, we could recover everything by Proposition 1 [15]. Note that the Lee distance is the shortest-path distance on the cartesian product of n copies of the q-gon.

The Lee scheme is *weakly metric* for the Lee distance, but in most cases not metric [14] and [22, an encyclopedic reference].

2.5. Arithmetic codes for the modular distance

(This example is new.) We let $X = Z_M$, the integers modulo M, we let d be the modular distance in the sense of [6] with radix r, and G be the semi-direct product of T_M by $G_{r,M}$. The group T_M is the group of translations of Z_M, and $G_{r,M}$ the group of permutations of Z_M generated by multiplications by r, and -1. We assume that r is prime to M so that $G_{r,M}$ is an isometry group for d (see [6] for a proof in the case of $M = r^m - 1$). d is graphic from the discussion in [17, p. 123]. Roughly speaking, the orbits of $G_{r,M}$ on Z_M are the cyclotomic classes merged with their opposite. If $X_0 = \{0\}, X_1, X_2, \ldots, X_t$ denote these orbits, then the relation:

$$xR_k y \iff x - y \in X_k$$

defines a scheme on Z_M that we call the Clark–Liang scheme $CL(M, r)$. For instance, $M = 17$, $r = 2$, the nontrivial orbits on Z_M are

$$X_1 = \{1, 2, 4, 8, -1, -2, -4, -8\} \tag{3}$$

of modular weight 1, and

$$X_2 = \{3, 6, 12, 7, -3, -6, -12, -7\} \tag{4}$$

of modular weight 2.

We obtain a two-class association scheme in the Bose–Mesner sense, or equivalently, a strongly regular graph [8, 12]. (Here the cyclotomic classes coincide with their opposites.) Its parameters in the notation of [5] are $(17, 8, 2, 4)$.

In the previous case the scheme was metric for the modular distance. This is not always the case. A counterexample is $CL(31, 2)$ with the orbits on Z_{31}: $\{0\}$, $C_3 \cup C_7$, $C_5 \cup C_{11}$, $C_1 \cup C_{15}$ of weights $0, 2, 2, 1$ where C_i stands for the ith cyclotomic class. This latter scheme is *weakly metric,* but not metric for the modular distance, since two classes of the scheme share the same modular weight.

3. Packings and coverings

We call any non-empty subset of X, a *code.* A code Y is said to be an E-packing if the spheres for d of radius E centered on the points of Y, are disjoint. The largest E such that Y is an E-packing is called the *packing radius,* or *error correcting capacity* of Y, and denoted by e.

The distance of a point x to the code Y is defined as:

$$d(x, Y) = \min_{y \in Y} d(x, y).$$

A code Y is said to be an r-covering if the spheres of radius r centered on the points of Y cover X. The smallest r such that Y is an r-covering is called the *covering radius* of Y and denoted by ρ.

Clearly, $\rho \geqslant e$. Codes such that $\rho = e$ are called *perfect.* Perfect codes in weakly metric schemes are investigated in [19].

The principal aim of this paper is to derive an upper bound on ρ (Theorem 3), involving e and a parameter to be defined in the next section.

4. MacWilliams transform in a scheme

Let Y denote a code. Its *inner distribution* [8, p. 25], is defined by:

$$a_i = \frac{1}{|Y|} |R_i \cap Y^2|; \quad i = 0, 1, \ldots, t. \tag{5}$$

In $H(n, q)$, $(a_i)_i$ is the distance distribution, and in $L(n, q)$ the Lee composition distribution. Its dual inner distribution is defined by:

$$a'_k = \sum_{i=0}^{t} q_k(i) a_i \tag{6}$$

where the $q_k(i)$ are numbers depending on the scheme (X, R) and called *second eigenvalues*. There is an inversion formula:

$$a_i = \frac{1}{|X|} \sum_{i=0}^{t} p_k(i) a_i' \tag{7}$$

where the $p_k(i)$ are numbers depending on (X, R) and called *first eigenvalues.*

Suppose now that X is an abelian group, with characters $\{x \to \Phi_y(x) \mid y \in X\}$, and Y a subgroup of X. We define the dual subgroup Y' [8, pp. 23–88] by:

$$Y' = \{y \in X \mid \forall x \in Y \Phi_y(x) = 1\}. \tag{8}$$

In this case the a_k' are, up to a constant factor, the inner distribution of Y'. For an unrestricted code Y, the number of indices $k \geqslant 1$ such that a_k' is nonzero is called the *dual degree* of Y and is denoted by s'.

5. The outer distribution of a code

The *outer distribution matrix* of a code is defined ([8, p. 25]) by the relation:

$$B_{x,i} = |\{y \in Y \mid xR_i y\}|. \tag{12}$$

In $H(n, q)$ the row B_x of B is the weight distribution of the translate of the code Y by x. For future use, we quote the following lemma.

Lemma 1. $\operatorname{rank}(B) = s' + 1$.

Proof. See [8, Theorem 3.1 and Corollary 3.2, p. 26], or [9] for the case of $H(n, q)$. □

6. Bounds on the parameters

We call the *dispersion function* and denote by $\Pi(e)$, [14], the number of i such that: $0 \leqslant d(i) \leqslant e$. This parameter reduces to $e + 1$ in metric schemes. For the connection with the Lloyd theorem in the Lee metric, see [14, 18–19].

Theorem 1. $s' \geqslant \Pi(e) - 1$.

Proof. Let y denote an arbitrary point of Y, fixed once and for all, and such that $xR_i y$ with $d(i) \leqslant e$.

By the definition of $\Pi(e)$ there are $\Pi(e)$ such x with pair-wise distinct i, yielding that many rows beginning with i zeros, and a nonzero $(i + 1)$th entry. This yields a regular $\Pi(e) \times \Pi(e)$ upper triangular submatrix of B, hence $\Pi(e)$

linearly independent rows ($i = 0$ is counted in this process). By elementary linear algebra, we have that $\Pi(e) \leqslant \text{rank}(B)$. Using Lemma 1, the result follows. □

In the case of $H(n, q)$ this yields the MacWilliams inequality [8, 12]:

$$s' \geqslant e.$$

The proof in [8–9], makes use of the P-polynomial structure. Though more general, our proof is simpler.

We give the natural generalization of the Delsarte bound in $H(n, q)$ [9]. Theorem 3 is a tighter bound, but its proof combines the arguments of Theorems 1 and 2, so that we give all three proofs, with a decreasing amount of details. The proof in [9, 12] makes use of a recursion on the weight distribution of translates. Again, despite its greater generality, our proof is simpler. Of course, we do not obtain a recursion on the columns of B.

First, we recall a simple fact [20] on graphic distances.

Lemma 2. *A distance d is graphic iff for every pair of points (x, y) at distance k apart, there is a point z with $d(x, y) = k - 1$, and $d(y, z) = 1$.*

Theorem 2. *In a weakly metric scheme with d graphic $\rho \leqslant s'$.*

Proof. Same reasoning as in the proof of Theorem 1 with the x_i such that $d(x_i, Y) = i$, $i = 0, \ldots, \rho$. The point x_ρ exists by definition of ρ. The point $x_{\rho-1}$ exists by application of Lemma 2. By induction all x_i exist. □

Example 1. Consider an AN code [10] for the modular distance [6] with radix r (r prime to M) and modulus M such that $M = AD$.

$$AN = \{Ai \mid 1 \leqslant i \leqslant D\}. \tag{21}$$

Then the additive dual of AN in the sense of Section 3 is DN and s' is the number of nontrivial orbits of $G_{r,A}$ on DN. This is also the number of nontrivial orbits of $G_{r,A}$ on Z_A, say n_A, since, for any integers a and $b \leqslant A$ we have that

$$a \equiv b(\pm r^i)[A] \quad \Leftrightarrow \quad Da \equiv Db(\pm r^i)[M]. \tag{22}$$

We obtain immediately the known [10] result:

$$\rho(AN) \leqslant n_A. \tag{23}$$

As shown in [10] this bound is attained on examples and the number of modular weights of DN can be $<\rho(AN)$, so that the analogous statement of Delsarte bound in $H(n, q)$ is wrong in general. It is obviously true when the modular scheme is metric, but this seems to occur rarely. This means that the relations $xR'_k y \;\Leftrightarrow\; d(x, y) = k$ do not always yield an association scheme, as in the first example of Subsection 2.5. Since d is graphic, this scheme would be metric, s' would count nonzero weights, and Delsarte bound on covering radius would always hold.

We introduce a parameter called *external distance*, denoted by μ, and defined as:

$$\mu = s' - \Pi(e) + e + 1.$$

This parameter is the usual external distance in metric schemes, since there $\Pi(e) = e + 1$. We are now in a position to prove the main result of this paper, which implies both Theorems 1 and 2.

Theorem 3. *In a weakly metric scheme with d graphic, $\rho \leqslant \mu$.*

Proof. Take the same i as in Theorem 1, plus $\rho - e$ points x_i such that $d(x_i, C) = i \in [e+1, \rho]$. Using lemma 1 we obtain:

$$\Pi(e) + (\rho - e) \leqslant s' + 1. \quad \square$$

Example 2. For the double error-correcting code Q_{12} of the appendix we obtain $\rho \leqslant 11$ instead of $\rho \leqslant 12$ with Corollary 2.

Example 3. In $CL(2^{18} - 1, 2)$ we consider the AN code with $A = (2^{18} - 1)/19$ (Mandelbaum–Barrow code). It has minimum distance $d = 6$, hence packing radius $e = 2$. It is easily seen by counting in base 2 that the first cyclotomic cosets C_{2k+1}, $0 \leqslant k \leqslant 2^8$ are disjoint [12, p. 262] and disjoint from their opposites. By taking $2k + 1$ for some j we get $2 \cdot 9 = 18$ cosets of modular weight 2, implying that $\Pi(2) \geqslant 20$, which by Corollary 3 yields $\rho \leqslant s' - 17$, a dramatic improvement on Theorem 2.

7. The regularity of codes

We shall assume henceforth that d is graphic. We call b the number of distinct rows in B for x not in Y.

Proposition 2. $b \geqslant s'$.

Proof. There are $b + 1$ distinct rows in B, whose rank is $s' + 1$. $\square$

A set Y is said to be *λ-regular* if the row $B(x)$ depends only on $d(x, Y)$ for $d(x, Y) \leqslant \lambda$ and *completely regular* iff ρ-regular, i.e., $\rho = b$. These definitions are a straightforward generalization of those in [8–9].

Corollary 1. *If Y is completely regular then $\rho = s'$.*

Proof. Obvious from Theorem 2 and Proposition 2. $\square$

Proposition 3. *If Y is a completely regular set then*:

$$\Pi(e) - 1 = e.$$

Proof. Y is completely regular, hence $\rho = s'$, by Corollary 1. Since $s' + e \geqslant \Pi(e) - 1 + \rho$ we have $e \geqslant \Pi(e) - 1$. The result follows, for $e \leqslant \Pi(e) - 1$ holds by definition of Π. □

We point out that there exists perfect sets in *weakly metric* schemes that are not completely regular. This contrasts strongly with metric schemes, where every perfect code is completely regular. For instance, we take $X = L(n, q)$ with $n = 2$, $q = 13$, and Y the negacyclic self dual perfect code [2] with generator polynomial $g(x) = x + 5$ and 'negacycle representatives' $(0, 0)$, $(1, 5)$, $(3, 2)$, $(6, 4)$.

We have $\rho = e = 2$ and $s' = 3 \neq 2$. Therefore Y is not completely regular.

Theorem 4. *For $q \geqslant 5$ and $e \geqslant 2$ there are no completely regular codes in $L(n, q)$.*

Proof. Clearly $\Pi(e + 1) - \Pi(e) \geqslant 1$. Since $q \geqslant 5$, $1 \neq 2$ in Z_q and $\Pi(2) = 4$, then an easy induction proof shows that $\Pi(e) \geqslant e + 2$ for $e \geqslant 2$. □

Theorem 5. *For $n \geqslant 3$ and $e \geqslant 2$, there are no completely regular codes in $CL(2^n - 1, 2)$.*

Proof. As in Theorem 4, it suffices to show that $\Pi(2) \geqslant 4$. More precisely, we show that $\Pi(2) = 2\lfloor n/2 \rfloor$. Note that $\Pi(1) = 2$. We just have to count $\Pi(2) - \Pi(1)$, which is the number of CNAF (cyclic non-adjacent form [6, 19]) of weight 2, not equivalent by cyclic shift, nor complementation.

There are $2(\lfloor n/2 \rfloor - 1)$ of them, the 2 coming from the factor ±1, and $n/2$ from the fact that the CNAF in $CL(2^n - 1, 2)$ is of length $\lfloor n/2 \rfloor$. □

It can be shown [21], that there are completely regular codes in the Lee metric $(\rho = 1)$ and modular distance $(\rho = 1, 2, 3)$. A very simple example with ρ arbitrary is given in the next section.

8. Appendix on self-dual codes over Z_5

An interesting feature of the external distance in $L(n, q)$ is that it can be computed from the Lee composition distribution. Using information and notation of [11], we have compiled the following table, where the last column was established by using the preceding results and decompositions of the codes. It is easily seen that C_2^m is completely regular of covering radius m. Computations of Lee enumerators were done in MACSYMA. See Table 1.

Table 1

Length	Name	e	Weight En.	Covering Bound	s'	ρ
2	C_2	0	α	1	1	1
4	C_2^2	0	α^2	2	2	2
6	C_2^3	0	α^3	3	3	3
6	F_6	1	β'	3	4	≤ 4
8	C_2^4	0	α^4	3	4	4
8	C_2F_6	0	$\alpha\beta'$	3	8	≤ 5
8	F_8	1	δ	3	7	≤ 7
10	C_2^5	0	α^5	4	5	≤ 5
10	C_2F_6	0	$\alpha^2\beta'$	4	11	≤ 6
10	C_2F_8	0	$\alpha\delta$	4	11	≤ 8
10	F_{10}	1	$\alpha^5 - 20\alpha^2\beta$	4	10	≤ 10
12	C_2^6	0	α^6	4	6	6
12	$C_2^3F_6$	0	$\alpha^3\beta'$	4	14	≤ 7
12	$C_2^3F_8$	0	$\alpha^2\delta$	4	14	≤ 11
12	F_6^2	1	β'^2	4	13	≤ 8
12	Q_{12}	2	ref[11]	4	12	≤ 11

The entry 'covering bound' is the lower bound on ρ computed through the well-known sphere-covering argument. Generating functions for the volume of the Lee spheres were found in [2], and computed in MACSYMA. See [24] for details.

9. Conclusion

In this paper, and in [19], we have introduced the concept of weakly metric scheme, a generalization of Delsarte's metric schemes. If this concept is not completely new (cf. [16] and Section 2.1), a combinatorial study of codes in this setting, along the lines of [9], certainly is.

We generalize to weakly metric schemes the MacWilliams inequality on the dual degree, and the Delsarte inequality on the covering radius. This solves a research problem raised in [10].

In particular, a new parameter, called the dispersion function, measures the 'nonmetricity' of a scheme. Connections with Neumaier's classification of graphs by regularity [23] are pointed out in [24]. See also [25] for a coding theoretic use of [23]. An algebraic characterization of association schemes with a given $\Pi(e)$, generalizing Theorem 5.6 of [8], would be of great interest.

From a constructive point of view, the Lee scheme seems less promising than the Clark–Liang scheme (compare the hypotheses of Theorems 4 and 5). In [21] we construct distance regular graphs of diameter 3 from completely regular arithmetic codes.

Acknowledgements

We thank the referees for their helpful comments, which have improved greatly the readability and correctness of this paper, and Ms. Elaine Weinman for careful T_EXing.

References

[1] E. Bannai and T. Ito, Algebraic Combinatorics Association Schemes 1 (Benjamin/Cummings, Menlo Park, CA, 1984).

[2] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York, 1968).

[3] N. Biggs, Perfect codes in graphs. J. Combin. Theory 15, 289–296.

[4] N. Biggs, Finite Groups of Automorphisms (Cambridge Univ. Press, Cambridge).

[5] P.J. Cameron and J.H. Van Lint, Graph Theory, Codes and Designs, Lond. Math. Soc. Lect. Notes (Cambridge Univ. Press, Cambridge, 1980).

[6] W.E. Clark and J.J. Liang, On modular weight and cyclic non-adjacent forms for arithmetic codes, IEEE Trans. Inform. Theory 20 (1974) 767–770.

[7] G. Cohen, M.R. Karpovsky, H.F. Mattson Jr and J.R. Schatz, Covering radius: survey and recent results, IEEE Trans. Inform. Theory 31 (1985) 328–343.

[8] P. Delsarte, Thesis, Catholic University of Louvain, Belgium, 1973, Phillips Res. Rep. Supp. 10 (1973).

[9] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. and Control 23 (1973) 407–438.

[10] T. Helleseth, On the covering radius of linear cyclic codes and arithmetic codes, Discrete App. Math. 11 (1985) 157–173.

[11] J.S. Leon, V. Pless and N.J.A. Sloane, Self dual codes over GF(5), J. Combin. Theory Ser. A (1982) 178–194.

[12] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes (North-Holland, Amsterdam, 1977).

[13] W.W. Peterson and E.J. Weldon, Error Correcting Codes (MIT Press, Cambridge, MA, 1972).

[14] P. Solé, The Lee association scheme, Proceedings of the Congrés of Cachan (Springer, Lect. Not. In Comp. Sc. 311) INRIA Research Report No. 591 (December 1986).

[15] P. Solé, Covering radius in weakly metric schemes, INRIA Research Report No. 592, December 1986.

[16] H. Tarnanen, Bounds on constant weight and Lee codes by the methods of association schemes, Thesis, Turku, Finland, 1982.

[17] J.H. Van Lint, Introduction to Coding Theory (Springer, Berlin, 1982).

[18] L.A. Bassalygo, A necessary condition for the existence of perfect codes in Lee metric, Math. Zam. 15 (2) (1974) 313–320.

[20] D.C. Kay and G. Chartrand, A characterization of certain ptolemaic graphs, Canad. J. Math. 17 (1965).

[21] P. Solé, Completely regular codes in weakly metric schemes, in preparation.

[22] J. Astola, The theory of Lee codes, Lappeenranta University, Finland, Research Report, 1982.

[23] A. Neumaier, Classification of graphs by regularity, J. Combin. Theory Ser. B 30 (1981).

[24] P. Solé, Rayon de recouvrement et schémas d'association, Ph.D. Thesis, E.N.S.T., Paris, France, 1987.

[25] A. Monpetit, Codes dans les graphes réguliers, Ph.D. Thesis, Sherbrooke, Canada, 1987.