Eigenvalues, eigenspaces and distances to subsets

C. Delorme[a], J.P. Tillich[b]

[a] *Université Paris-Sud, LRI URA40, Bat 490, 91405 Orsay Cedex, France*
[b] *Department of Mathematics, UBC, Vancouver V6T 1Z2, Canada*

Abstract

In this note we show how to improve and generalize some calculations of diameters and distances in sufficiently symmetrical graphs, by taking all the eigenvalues of the adjacency matrix of the graph into account. We present some applications of these results to the problem of finding tight upper bounds on the covering radius of error-correcting codes, when the weight distribution of the code (or the dual code) is known.

1. Generalities

We aim here at improving known bounds linking the diameter of a graph (or more generally distances between subsets of vertices of the graph) and eigenvalues of the graph. Our main result is when mild symmetry requirements are fulfilled (such as vertex transitivity) then using the whole spectrum of the graph, one can improve substantially the known bounds. This approach has applications to coding theory, when one wishes to obtain an upper bound on the covering radius of a code. Indeed in this case it is known that for a linear code one can associate a Cayley graph whose diameter is the covering radius of the code, and its spectrum can be computed from the weight distribution of the dual code. In this case when this distribution is known (and there are examples for which this is the case) one can obtain a rather sharp bound on the covering radius of the code.

First of all let us recall a few graph theoretical concepts that we are going to use. Let V be the vertex set of a graph G, and E its set of edges. The graphs we are going to consider are all undirected. This implies that their adjacency matrix A is symmetric (which is a square matrix indexed by the vertices of the graph and $a_{v,w} = 1$ if there is an edge between v and w, and 0 otherwise). The eigenvalues of the graph are defined as the eigenvalues of this matrix.

This matrix can be viewed as a linear operator on the vector space of functions $V \to \mathbb{R}$. We denote by $\{1_v\}_{v \in V}$ the canonical basis of this vector space, i.e. 1_v has only zero entries except for v where the corresponding entry is equal to 1. This space

is given the (usual) inner product $\langle f \mid g \rangle = \sum_V f(v)g(v)$. It is readily seen that $A.f(v) = \sum_{\{v,w\}\in E} f(w)$.

A is symmetric, so that the eigenvalues of A are real and each function f is a sum $\sum_\lambda f_\lambda$, f_λ being the orthogonal projection of f on the eigenspace associated to the eigenvalue λ. All these components f_λ are mutually orthogonal.

It is well known that the entry $a_{v,w}^{(l)}$ of the lth power of A represents the number of walks of length l going from v to w. Therefore the value at vertex t of the function $A^l(1_s)$ (in other words the inner product $\langle 1_t \mid A^l(1_s)\rangle$) is the number of paths of length l between s and t.

The key fact which explains how we will bring in linear algebra is the simple remark (see [3])

Fact 1. *If* $\langle 1_t \mid A^d(1_s)\rangle \neq 0$ *then the distance between* t *and* s *is at most* d.

It has been noticed by several authors [4,7,9–11,14,18] that one can improve on this approach by using instead of A^d a linear combination of the A^l's

Fact 2. *If some polynomial P of degree d satisfies* $\langle 1_t \mid P(A)(1_s)\rangle \neq 0$ *then the distance between* t *and* s *is at most* d.

The term $\langle 1_t \mid P(A)(1_s)\rangle \neq 0$ is shown to be different from 0 by simple considerations on the spectrum of the graph. Recall that this spectrum is defined as the spectrum of the adjacency matrix, and that if the graph is connected and not bipartite, the eigenvalue with largest modulus k is unique and has an eigenspace of dimension one, generated by a positive function f. This is Perron–Frobenius theorem (see [17]). Of course one may choose f of norm 1. If n is big enough, the component $k^n\langle f \mid 1_s\rangle f$ of $A^n(1_s)$ becomes so large that its inner products with 1_t cannot be cancelled by the inner products of the other components of $A^n(1_s)$ with 1_t. Hence such a number n is an upper bound on the diameter.

More generally, if one replaces A^n by some polynomial $P(A)$ such that

$$P(k)\langle f \mid 1_s\rangle\langle f \mid 1_t\rangle > |P(\lambda)|\sqrt{1 - \langle f \mid 1_s\rangle^2}\sqrt{1 - \langle f \mid 1_t\rangle^2}$$

then for any eigenvalue $\lambda \neq k$, the distance between s and t is at most the degree of P.

In particular, the diameter of G is less than the number of eigenvalues of G. This can be obtained from $P(X) = \prod_{\lambda \neq k}(X - \lambda)$. See [1, Corollary 2.7] for a direct proof.

A drawback of all these known results is that even if these bounds can be tight for certain graphs (see [11]) they are not in general, and there is definitely a gap between these upper bounds on the diameter (and this even with 'optimal' eigenvalues) and the Moore bound (for example all the results given in [4,3,11,14,18] miss the Moore bound by a multiplicative factor which is at least 2). Let us consider the following graph for instance.

Table 1

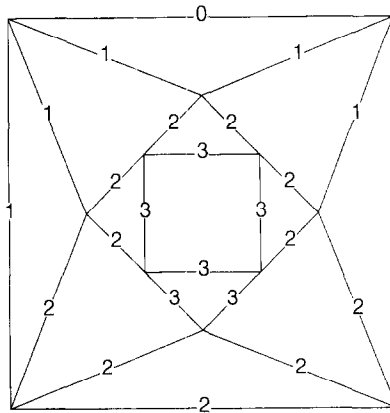| Degree	[4]		[10]	
1	$X - 1$	5/3	$X - 1$	5/3
2	$(X - 1)^2 - \frac{9}{2}$	41/9	$(X - 1)^2 - 5$	5
3	$(X - 1)^3 - (27/4)(X - 1)$	365/27	$(X - 1)^3 - 7(X - 1)$	15
4	$(X - 1)^4 - 9X^2 + 81/4$	3281/81	$(X - 4)(X - 2)X(X + 2)$	∞

Fig. 1. The line graph of the cube and the diameter of its line-graph.

Example 1. The line-graph of the line-graph of the cube Q_3 has spectrum 6^1, 4^3, 2^3, 0^5, -2^{12} where the bold exponents show the multiplicities of the eigenvalues. Since the graph is regular, the function f is constant and $\langle f \mid 1_s \rangle = \sqrt{(1/24)}$ for each vertex s. The length of the part of 1_s orthogonal to f is $\sqrt{(23/24)}$. The projection of f on each 1_t has length $\sqrt{(1/24)}$, and the projection of any vector of length 1 orthogonal to f on 1_t has length $\leqslant \sqrt{(23/24)}$.

The polynomials used to bound the diameter, according to [4] (adjusted Tchebychev polynomials) or [10] (optimized polynomials) are given in Table 1 with the ratio $P(k)/\max |P(\lambda)|$. These methods give $D \leqslant 4$. The diameter is in Fact 3. This can be checked on Fig. 1.

2. Using the multiplicities

We can refine the previous calculations when the graph displays some symmetries. Basically the idea is that if the graph is vertex transitive, one can easily calculate the lengths of the projection of a vector 1_s on all the eigenspaces E_λ of the operator A, and use them in order to study the inner product $\langle P(A)(1_s) \mid 1_t \rangle$.

This is done by calculating in two ways the trace of A^{2l}. Denote by m_λ the dimension of E_λ. Clearly

$$\text{Tr}(A^{2l}) = \sum_\lambda m_\lambda \lambda^{2l}.$$

On the other hand, this trace is readily seen to be the sum of the squared entries of A^l, since this sum is the trace of the matrix $(A^*)^l A^l$ (A^* denotes the transpose of A), which is A^{2l} for A is symmetric. Note that this sum of these squared entries is just the sum of the squared norms of the columns of A^l. Therefore

$$\text{Tr}(A^{2l}) = \sum_{s \in V} |A^l(1_s)|^2.$$

All these $|A^l(1_s)|^2$ are equal because the graph is vertex transitive (this follows easily from the combinatorial interpretation of the entries of the vector $A^l(1_s)$). Comparing these two different expressions of the trace we obtain

$$|A^l(1_s)|^2 = \frac{1}{N} \sum m_\lambda \lambda^{2l} \tag{1}$$

This innocent looking equality (1) is in fact surprisingly powerful. It is the key fact used in [8] for example (see Lemma 1 Ch. 3B) in order to find tight upper bounds on the rate of convergence of random walks over Cayley graphs towards the uniform distribution. This is proved in this setting by using Fourier analysis on groups, and more precisely the Plancherel theorem. The proof technique used above would have yielded a much simpler proof of this Lemma 1 in Ch. 3B.

A consequence of this equality is

Proposition 1. *If the graph is vertex transitive, the projection s_λ of 1_s on the eigenspace E_λ has length $\sqrt{m_\lambda/N}$ where m_λ is the multiplicity of λ and N the number of vertices in the graph.*

Proof. We have for every l

$$|A^l(1_s)|^2 = \sum |s_\lambda|^2 \lambda^{2l}$$

By comparing this with equality 1, we obtain that $|s_\lambda|^2 = \frac{m_\lambda}{N}$. □

Corollary 1. *Let G be a connected vertex-transitive graph of degree k. If $|P(k)| > \sum_{\Lambda \setminus k} |P(\lambda)| m_\lambda$ then the diameter of G is at most the degree of P.*

Proof. Consider $P(A)(1_s)$. The inequality ensures that the projection on 1_t of its component in E_k cannot be cancelled by the projections of the other components. More precisely assume that $\langle P(A)1_s \mid 1_t \rangle = 0$, since $\langle P(A)1_s \mid 1_t \rangle = \sum_\lambda P(\lambda)\langle s_\lambda \mid t_\lambda \rangle$ and $\langle s_k \mid t_k \rangle = \frac{1}{N}$ one has

$$P(k)\frac{1}{N} = - \sum_{\lambda \in \Lambda \setminus k} P(\lambda)\langle s_\lambda \mid t_\lambda \rangle$$

Then by the Cauchy-Schwartz inequality

$$P(k)\frac{1}{N} \leqslant \sum_{\lambda \in \Lambda \setminus k} |P(\lambda)| \|s_\lambda\| \|t_\lambda\|$$

$$\leqslant \sum_{\lambda \in \Lambda \setminus k} |P(\lambda)| \frac{m_\lambda}{N}$$

This is impossible, and we conclude the proof by using Fact 2. □

Example 2. With the graph of Example 1, we choose $P = (X - 4)(X - 1)(X + 2)$ and observe the inequality $P(6) > 3|P(4)| + 3|P(2)| + 5|P(0)| + 12|P(-2)|$. This gives $D \leqslant 3$, which is the actual value.

Remark. The replacement of the sum on the set of vertices by N times the term corresponding to a vertex holds also if the graph is walk-regular; i.e. for every n the number of walks of length n with both endpoints at s does not depend on s. In other words, any power A^k has its diagonal entries all equal to $\mathrm{Tr}(A^k)/N$. We will show later that this property is indeed a characterization of walk-regular graphs. This class of walk-regular graphs contains the class of vertex transitive graphs and the class of distance-regular graphs.

The class of matrices for which each power of a matrix of this set has diagonal entries which are all equal is stable by Kronecker products or polynomial transformations. Hence the class of walk-regular graphs is also stable under miscellaneous operations like cartesian products, cartesian sums, strong products and other so-called NEPS (a multilingual acronym), see [6]. Therefore it contains graphs that are neither vertex-transitive nor distance-regular; it is well-known that some distance-regular graph are not vertex-transitive (the trivalent bipartite graph of diameter 6 on 126 vertices described in [1] is an example). This implies that the cartesian sum of this graph and K_2 is neither vertex-transitive nor distance-regular.

3. Optimization and relationship with linear programming

We may improve on this method by giving various weights to the edges. If the weights are positive and preserve the vertex transitivity, i.e. for each pair of vertices u and v, there is an automorphism α which maps u to v and preserves the weights, $w(\alpha s \alpha t) = w(st)$ for every pair of adjacent vertices $\{s, t\}$, then our method is still valid. The matrix A is replaced by A_w where the (u, v)-entry is the weight of the edge uv if it exists, and 0 otherwise.

Corollary 1 holds even if the weighted graph is walk regular in the following sense: any walk has a weight which is the product of the weights of the edges it uses (e.g. $w(abac) = w^2(ab)w(ac)$ if the vertex a is adjacent to vertices b and c), and entry (u, v) of A^k is the sum of the weights of the walks of length k from u to v. We say that the

weighted graph is walk regular iff for every l the total weight of all closed walks of length l starting at some given vertex v does not depend on the chosen vertex v.

Proposition 2. *Let A be a symmetric matrix. If the diagonal entries for each power of A are all equal, then the projections of the 1_v's on each eigenspace E_λ have the same length and conversely.*

Proof. If the diagonal entries are equal for powers, they are also for polynomials. Among these we can look at

$$B_\mu = \frac{\prod_{A\setminus\mu}(A - \lambda Id)}{\prod_{A\setminus\mu}(\mu - \lambda)}.$$

This idempotent operator is just the projection on the eigenspace E_μ. Computing $\langle 1_v \,|\, B_\mu(1_v)\rangle$, which is the vth diagonal entry of B_μ, we see that this quantity is just the square of the length of the projection of 1_v on E_μ.

On the other hand, if these lengths depend only on λ, then the diagonal entry (v,v) of A^k is $\langle 1_v\,|\,A^k 1_v\rangle = \sum_A \lambda^k \langle p_\lambda\,|\,p_\lambda\rangle$, where p_λ is the projection of 1_v on E_λ, and does not depend on v. □

Therefore, Corollary 1 holds for walk regular weighted graphs too. The point is that a convenient choice of weights can decrease the number of eigenvalues, or increase the ratio $P(k)/\sum_{A\setminus k}|P(\lambda)|m_\lambda$, k being the largest eigenvalue of the adjacency matrix of the weighted graph.

Example 3. The cartesian sum of t complete graphs $K_{a_1}, K_{a_2}, \ldots, K_{a_t}$ has clearly diameter t. This can be obtained by our method too, by letting the weight $1/a$ on the edges that come from a K_a. Then there are only $t+1$ eigenvalues, namely $A, A+1, A+2, \ldots, A+t$, where $A = -\sum_{i=1}^t 1/a_i$. And therefore by using a polynomial of degree t whose zeros are $A, A+1, \ldots, A+t-1$ we obtain that the diameter of the graph is at most t. Without optimizing the weights of edges, there may be up to 2^t eigenvalues.

The issue of finding a polynomial of degree at most d which maximizes $P(k)/\sum_{A\setminus k}|P(\lambda)|m_\lambda$ is indeed a linear programming problem, with the constraints $\sum_{A\setminus k}\varepsilon_\lambda P(\lambda)m_\lambda \leqslant 1$, where ε_λ takes its values in $\{-1,1\}$ (i.e. $2^{\#(A\setminus k)}$ constraints), and the objective function $P(k)$. The constraints and the objective function are linear with respect to the $d+1$ coefficients of the polynomial P of degree $\leqslant d$.

First of all let us notice that

Proposition 3. *The ratio $P(k)/\sum_{A\setminus k}|P(\lambda)|m_\lambda$ is maximized over all polynomials of degree d by some polynomial $P(X) = \Pi_{i=1}^d(X - \lambda_i)$, where the λ_i's are d different eigenvalues chosen from $A \setminus k$.*

A proof of this proposition will be given in what follows. Therefore a straightforward algorithm to find this polynomial $P(X)$ could be

Step 1: Choose an initial polynomial $P(X) = \Pi_{i=1}^{d}(X - \lambda_i)$, where the λ_i's are d different eigenvalues chosen from $\Lambda \setminus k$.

Step 2: Compute $P(k)/\sum_{\Lambda \setminus k} |P(\lambda)|m_\lambda$.

Step 3: Replace one of these λ_i's by a new eigenvalue λ_j which increases the value obtained at step 2.

Step 4: Iterate step 3 till it becomes impossible to increase the ratio $P(k)/\sum_{\Lambda \setminus k} |P(\lambda)|m_\lambda$. The maximum of $P(k)/\sum_{\Lambda \setminus k} |P(\lambda)|m_\lambda$ is obtained by this polynomial P which we cannot modify anymore.

All what we have to do in order to prove that this polynomial yields the biggest ratio $P(k)/\sum_{\Lambda \setminus k} |P(\lambda)|m_\lambda$, is to prove the following lemma about the set of extreme points of the convex region $\mathscr{C}$ in $\mathbb{R}^{d+1}$ defined by the set of points $(a_0, a_1, \ldots, a_d)$ for which the polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ satisfies $\sum_{\Lambda \setminus k} |P(\lambda)|m_\lambda \leqslant 1$.

Lemma 1. *When d is less than the number of elements of $\Lambda \setminus k$ the extreme points of $\mathscr{C}$ correspond to polynomials of degree d whose roots are d distinct eigenvalues λ_i's. When d is equal to the cardinality of $\Lambda \setminus k$ the set $\mathscr{C}$ has no extreme points.*

Indeed we have to find the maximum of a linear function (in the coefficients of the polynomial) $P(k)$ in this polyhedron $\mathscr{C}$ of R^{d+1}. The maximum occurs therefore at one of the finite number of extreme points of $\mathscr{C}$ (see [5, Ch. 2, Section 1]). To find this maximum we can use the simplex algorithm. That is, start at some extreme point, compute the value of the objective function at this point. Find a neighbouring extreme point for which the value of the objective function is larger and iterate this process until an extreme point for which the value of the objective function cannot be increased by choosing another neighbouring extreme point is reached. It can be proved that this extreme point is the global maximum of the objective function on $\mathscr{C}$ (see [5, Chs. 2 and 3]).

The aforementioned algorithm is just the simplex algorithm. It remains to prove our claim about the extreme points of $\mathscr{C}$. An extreme point of a convex region $\mathscr{C}$ is a point p for which the equality $p = (x + y)/2$, where x and y are two points in $\mathscr{C}$, can be achieved only if $p = x = y$.

Proof of Lemma 1. In order to avoid cumbersome statements, we will identify from now on a polynomial with its image in R^{d+1} given by its $(d + 1)$-tuple of coefficients. Let us first prove that every extreme point $P(x)$ of $\mathscr{C}$ is necessarily a polynomial which has d distinct roots among Λ. We proceed by contradiction. Let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be the roots of P belonging to Λ (there may be none), and assume that $s < d$. Call this set of roots Λ'. Let $Q(x) = \Pi_{i=1}^{s}(x - \lambda_i)R(x)$ where $R(x)$ is an unspecified polynomial of degree $d - s$. We will show that there exists such a polynomial $R(x)$ and a real $\varepsilon > 0$ such that when ε is small enough and for all λ not belonging to the set of the λ_i's,

the sign of $P(\lambda) \pm \varepsilon Q(\lambda)$ is equal to the sign of $P(\lambda)$. For such an ε we have

$$\sum_{\Lambda \setminus k} |P(\lambda) \pm \varepsilon Q(\lambda)| m_\lambda = \sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} |P(\lambda) \pm \varepsilon Q(\lambda)| m_\lambda$$

$$= \sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} \operatorname{sign}(P(\lambda))(P(\lambda) \pm \varepsilon Q(\lambda)) m_\lambda$$

$$= \sum_{\lambda \in (\Lambda \setminus k)} |P(\lambda)| m_\lambda \pm \varepsilon \sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} \operatorname{sign}(P(\lambda)) Q(\lambda) m_\lambda.$$

$R(x)$ can be chosen such as to make the sum $\sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} \operatorname{sign}(P(\lambda)) Q(\lambda) m_\lambda$ equal 0 (and this without being equal to 0 itself). With this choice of $R(x)$ it appears that $P(x) + \varepsilon Q(x)$ and $P(x) - \varepsilon Q(x)$ both belong to $\mathscr{C}$. Therefore such a polynomial $P(x)$ is not an extreme point of $\mathscr{C}$.

Let us prove now that every polynomial $P(x) = \alpha \Pi_{i=1}^{d}(x - \lambda_i)$ for distinct λ_i's in $\Lambda \setminus k$ and for a suitable α (i.e. such that $\sum_{\Lambda \setminus k} |P(\lambda)| m_\lambda = 1$) is an extreme point of $\mathscr{C}$; and this unless the set $\Lambda' = \{\lambda_1, \lambda_2, \dots, \lambda_d\}$ is equal to $\Lambda \setminus k$. In this case it is straightforward to check that there are no extreme points in $\mathscr{C}$, because the infinite line generated by $\Pi_{\Lambda \setminus k}(x - \lambda)$ belongs to $\mathscr{C}$ and adding to every point of $\mathscr{C}$ a point of this line yields another point of $\mathscr{C}$. If $P(x)$ is not an extreme point there exists a polynomial $Q(x)$ of degree at most d such that for every $\varepsilon \in [-1, 1]$:

$$\sum_{\Lambda \setminus k} |P(\lambda) + \varepsilon Q(\lambda)| m_\lambda \leqslant 1.$$

When the absolute value of ε is small enough the sign of $P(\lambda) + \varepsilon Q(\lambda)$ is given by the sign of $P(\lambda)$, and this for every λ which does not belong to Λ'. Therefore for such values of ε

$$\sum_{i=1}^{d} |\varepsilon Q(\lambda_i) m_{\lambda_i}| \leqslant 1 - \sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} \operatorname{sign}(P(\lambda))(P(\lambda) + \varepsilon Q(\lambda)) m_\lambda$$

$$\sum_{i=1}^{d} |\varepsilon Q(\lambda_i) m_{\lambda_i}| \leqslant -\varepsilon \sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} \operatorname{sign}(P(\lambda)) Q(\lambda) m_\lambda.$$

This implies that $\sum_{\lambda \in (\Lambda \setminus k) \setminus \Lambda'} \operatorname{sign}(P(\lambda)) Q(\lambda) m_\lambda = 0$, and therefore $\sum_{i=1}^{d} |\varepsilon Q(\lambda_i) m_{\lambda_i}| = 0$ and thus $Q(x)$ is proportional to $\Pi_{i=1}^{d}(x - \lambda_i)$. This can only happen if $Q(x) = 0$, and this means that $P(x)$ is an extreme point. $\square$

4. Subsets with no short distance

The technique we used to find upper bounds on the diameter of a graph can be used in a similar setting where we want to find upper bounds on the number of vertices of a k-regular vertex transitive graph, which are all at distance d from each other.

Proposition 4. *If we have n vertices of such a graph with mutual distances $> d$, and P a polynomial of degree d with $P(k) > 0$, the following inequality holds:*

$$(n-1)P(k) + \sum_{\Lambda \setminus k} \varepsilon_\lambda P(\lambda) m_\lambda \leqslant 0,$$

where $\varepsilon_\lambda = n - 1$ if $P(\lambda) < 0$, and $\varepsilon_\lambda = -1$ if $P(\lambda) > 0$ (the value of ε_λ has no influence on the sum if $P(\lambda) = 0$).

Proof. Let $\mathscr{C} = \{w^{(1)}, w^{(2)}, \dots, w^{(n)}\}$ be this set of vertices, and $S_i = S \setminus w^{(i)}$. We have

$$\langle P(1_{w^{(1)}}) \mid 1_{\mathscr{C}_1} \rangle = 0,$$
$$\langle P(1_{w^{(2)}}) \mid 1_{\mathscr{C}_2} \rangle = 0,$$

$$\dots$$

$$\langle P(1_{w^{(n)}}) \mid 1_{\mathscr{C}_n} \rangle \dots 0.$$

Therefore $\sum_{i=1}^{n} \langle P(1^{w_i}) \mid 1_{\mathscr{C}_i} \rangle = 0$. Decompose now each vector $1_{w^{(i)}}$ as the sum of its projections $w_\lambda^{(i)}$ onto the eigenspaces E_λ. This implies

$$\sum_\lambda P(\lambda) \sum_{i \neq j} \langle w_\lambda^{(i)} \mid w_\lambda^{(j)} \rangle = 0. \tag{2}$$

For the eigenspace of dimension 1 corresponding to k we have $\sum_{i \neq j} \langle w_k^{(i)} \mid w_k^{(j)} \rangle = n(n-1)/N$. Note that if we have n unit vectors v_i, then the squared length of $\sum_{1 \leqslant i \leqslant n} v_i$ lies between 0 and n^2, and therefore $-n \leqslant \sum_{i \neq j} \langle v_i \mid v_j \rangle \leqslant n(n-1)$. From this and Proposition 1 we deduce that

$$-\frac{nm_\lambda}{N} \leqslant \sum_{i \neq j} \langle w_\lambda^{(i)} \mid w_\lambda^{(j)} \rangle \leqslant \frac{n(n-1)m_\lambda}{N}.$$

By using this information in Eq. 2 we obtain our inequality. □

This proposition enables us to give upper bounds on the stability number of the nth power of a graph. In particular, if μ is the lowest eigenvalue, the polynomial $X - \mu$ gives the Lovász bound for the usual stability number α, namely $\alpha \leqslant -\mu N/(k - \mu)$ [13]. This proposition can be improved a little bit when the dimension of the eigenspace E_λ is 1, and n is odd. In this case

$$\frac{(1-n)m_\lambda}{N} \leqslant \sum_{i \neq j} \langle w_\lambda^{(i)} \mid w_\lambda^{(j)} \rangle \leqslant \frac{n(n-1)m_\lambda}{N}.$$

Example 4. Let G be the circulant graph with 12 vertices labelled with the congruence classes modulo 12, each vertex x being adjacent to $x + 2$, $x - 2$, $x + 3$, $x - 3$.

Edges $\{x, x + 2\}$ are given weight 1, and edges $\{x, x + 3\}$ are given weight $\frac{1}{2}$. The spectrum is 3^1, 1^5, 0^2, $(-2)^4$, the polynomial $X + 2$ gives $4 \cdot 5 + (-1) \cdot 3 \cdot 5 + (-1) \cdot 2 \cdot 2 > 0$,
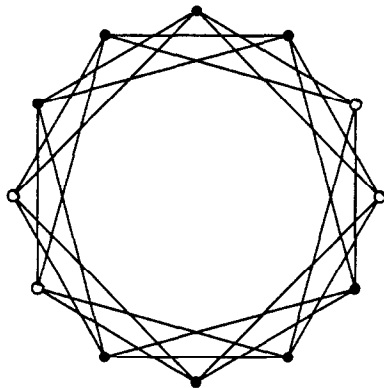
Fig. 2. A circulant graph and a maximum stable set.

hence the maximum stable set in G has at most 4 vertices. This is the actual value, as can be checked from Fig. 2.

Example 5. Let G be the bipartite double cover of the Petersen graph. It can be regarded as the set of the 20 subsets on 2 or 3 elements of a set on 5 elements, say $\{a,b,c,d,e\}$, with adjacency representing strict inclusion.

This graph G has spectrum 3^1, 2^4, 1^5, $(-1)^5$, $(-2)^4$, $(-3)^1$. The sets of vertices with mutual distance 3 can be shown to have at most 5 vertices, owing to the polynomial $P = (X + 2)(X + 1)$, that yields $(n - 1)P(3) - 4P(2) - 5P(1) - P(-3) = 0$ for $n = 5$.

This complies with the Lovász bound for the stability number of the square of G, where the weights 3 and 1 are attributed to the edges in G and the edges in G^2 out of G, respectively, in order to optimize the ratio between the smallest eigenvalue, and the difference of extreme eigenvalues. The smallest eigenvalue is -5 and the largest 15, whence the bound $20(5/20) = 5$ for the stability number of G^2.

But then we have $n(n - 1)P(3) - 4nP(2) - 5nP(1) - (n - 1)P(-3) > 0$, thus there are at most 4 vertices at distance $\geqslant 3$. Such a subset of vertices exists, e.g. *abc*, *ade*, *cd*, *be*.

5. Some examples with line-graphs of bipartite graphs

It is well known that the spectrum $\Lambda(\text{LG})$ of the line-graph LG of a k-regular graph G on N vertices is easily obtained from the spectrum $\Lambda(G)$ of the graph itself. The cases $k \leqslant 2$ are not interesting. For $k \geqslant 3$ we have for each $\lambda \neq -d$ in $\Lambda(G)$, the eigenvalue $\lambda + d - 2$ with the same multiplicity in $\Lambda(\text{LG})$, and -2 is an eigenvalue of LG with multiplicity $E - N + m_G(-d)$ where $m_G(\lambda)$ is the multiplicity of the eigenvalue λ in the spectrum of G, or 0 if λ is not an eigenvalue of G and E is the number of edges in G (see [5]).

To prove this we consider the edge–vertex incidence matrix $B = (b_{ij})$ of G with N columns and E rows, where $b_{ij} = 1$ if edge i is incident to vertex j. Then $BB^{\mathrm{T}} = 2I_E + A(\mathrm{LG})$ and $B^{\mathrm{T}}B = kI_N + A(G)$ have the same spectrum but for the multiplicity of 0. $A(G)$ and $A(\mathrm{LG})$ denote, respectively, the adjacency matrices of G and LG.

Now we adapt this proof to simple connected biregular bipartite (k_1, k_2) graphs. This notation means that there is a partition of the vertices of the graph into blocks, such that all the vertices in the first block of size N_1 have k_1 neighbours which are all in the second block, whereas the vertices of the second block of size N_2 have all their k_2 neighbours in the first block. This implies that $E = N_1 k_1 = N_2 k_2$. This partition splits the edge–vertex incidence matrix B into two blocks $B = [\, B_1 \;\; B_2 \,]$. We will actually consider a weighted version $B_w = [\, \sqrt{s_1}B_1 \;\; \sqrt{s_2}B_2 \,]$ of B.

The case of non-connected graphs is a straightforward extension of this one.

The equality $BB^{\mathrm{T}} = 2I_e + M(\mathrm{LG})$ becomes $B_w B_w^{\mathrm{T}} = (s_1 + s_2)I_e + M_w(\mathrm{LG})$, where $M_w(\mathrm{LG})$ is the adjacency matrix of the line-graph, with weights s_1 or s_2 on the edge pq of the line-graph according to the stable component that contains the common vertex of edges p and q of G.

Proposition 5. *Let G be a simple connected biregular bipartite graph with degrees d_1 and d_2, and let M_w be the adjacency matrix of its weighted line-graph.*

If $0 < \lambda < \sqrt{d_1 d_2}$ is an eigenvalue of G with multiplicity m, then the roots of $(Z + s_1 + s_2)^2 - (s_1 d_1 + s_2 d_2)(Z + s_1 + s_2) + s_1 s_2 (d_1 d_2 - \lambda^2)$ are eigenvalues of M_w with multiplicity m.

If 0 is eigenvalue of G with multiplicity m, then $s_1(d_1 - 1)$ and $s_2(d_2 - 1)$ are eigenvalues of M_w with multiplicities $(m + v_1 - v_2)/2$ and $(m + v_2 - v_1)/2$ (one of these eigenvalues is missing if U has rank $\min\{v_1, v_2\}$).

The eigenvalue $\sqrt{d_1 d_2}$ (which is simple since it is the maximal eigenvalue of the connected graph G) yields the simple eigenvalue $s_1(d_1 - 1) + s_2(d_2 - 1)$ and the eigenvalue $-s_1 - s_2$ with multiplicity $1 + e - v_1 - v_2$.

This a mere generalization of Theorem 2.16 in [5] where the case of the unweighted line-graph is described.

Proof. The adjacency matrix of G is in a natural way split into blocks of sizes v_1 and v_2 as follows:

$$M = \begin{bmatrix} 0 & U \\ U^{\mathrm{T}} & 0 \end{bmatrix}$$

We have

$$B_w^{\mathrm{T}}B_w = \begin{bmatrix} s_1 d_1 I_{v_1} & \sqrt{s_1 s_2}\,U \\ \sqrt{s_1 s_2}\,U^{\mathrm{T}} & s_2 d_2 I_{v_2} \end{bmatrix},$$

and hence $(B_w^{\mathrm{T}}B_w)^2 - (s_1 d_1 + s_2 d_2)B_w^{\mathrm{T}}B_w = s_1 s_2(M^2 - d_1 d_2 I_{v_1 + v_2})$.

We then see that if

$$\begin{bmatrix} s_1 d_1 I_{V_1} & U \\ U^T & s_2 d_2 I_{V_2} \end{bmatrix}$$

has eigenvalue α with eigenvector

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

then it has also eigenvalue $s_1 d_1 + s_2 d_2 - \alpha$ with eigenvector

$$\begin{bmatrix} (\alpha - s_1 d_1)x_1 \\ (s_2 d_2 - \alpha)x_2 \end{bmatrix}. \qquad \square$$

Example 6. The complete bipartite graph K_{d_2, d_1} has spectrum $\sqrt{d_2 d_1}^1$, $0^{d_2 + d_1 - 2}$, $-\sqrt{d_2 d_1}^1$.

Its line-graph has spectrum $(d_2 + d_1 - 2)^1$, $(d_2 - 2)^{d_1 - 1}$, $(d_1 - 2)^{d_2 - 1}$, $(-2)^{d_2 d_1 - d_2 - d_1 + 1}$; this spectrum could also be computed from the remark that this line-graph is also the cartesian sum of K_{d_2} and K_{d_1}.

In the same way, we could compute the spectrum of the weighted line-graph, namely $(s_1(d_1 - 1) + s_2(d_2 - 1))^1$, $(s_1(d_1 - 1) - s_2)^{d_2 - 1}$, $(-s_1 + s_2(d_2 - 1))^{d_1 - 1}$, $(-s_1 - s_2)^{d_2 d_1 - d_2 - d_1 + 1}$.

Example 7. The subdivision of K_4 has 6 vertices of degree 2 and 4 vertices of degree 3. The spectrum is $\sqrt{6}^1$, $\sqrt{2}^3$, 0^2, $(-\sqrt{2})^3$, $(-\sqrt{6})^1$.

The spectrum of the line-graph is 3^1, 2^3, 0^2, $(-1)^3$, $(-2)^3$, the weighted spectrum is

$$(2s_1 + s_2)^1, \quad (-s_1 + 2s_2)^2, \quad (-s_1 - s_2)^3, \quad \left(\frac{s_1^2 + \sqrt{9s_1^4 - 4s_1^2 s_2^2 + 4s_2^4}}{2} \right)^3,$$

$$\left(\frac{s_1^2 - \sqrt{9s_1^4 - 4s_1^2 s_2^2 + 4s_2^4}}{2} \right)^3.$$

This line-graph has diameter $\leqslant 3$, as one sees with the polynomial $P = (X - 2)(X + 1)$ $(X + 2)$ that gives $P(3) + 2P(0) > 0$ and at most 3 vertices can have mutual distance 3, as one can see with the polynomial $P = (X + 2)(X + 1)$ that gives $3P(3) - 3P(2) - 2P(0) > 0$.

These are the actual values, see Fig. 3.

Example 8. The rhombic dodecahedron has 8 vertices of degree 3 and 6 vertices of degree 4. It is also the 4-cube with 2 opposite vertices removed, or the incidence graph of faces and vertices of the 3-cube. The spectrum is $\sqrt{12}^1$, 2^3, 0^6, $(-2)^3$, $-\sqrt{12}^1$.

The spectrum of its line-graph is

$$5^1, \quad \left(\frac{3 + \sqrt{17}}{2} \right)^3, \quad 2^2, \quad 1^4, \quad \left(\frac{3 - \sqrt{17}}{2} \right)^3, \quad (-2)^{11}.$$
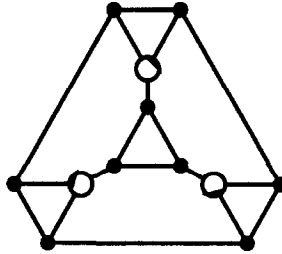
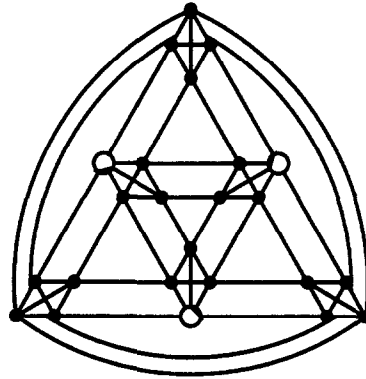Fig. 3. The line-graph of the subdivision of K_4.

Fig. 4. The line-graph of the rhombic dodecahedron.

The diameter is at most 4 (use the polynomial $P = (X + 2)(X - 1)(X^2 - 3X - 2)$ and the inequality $P(5) + 2P(2) > 0$), and there are at most 3 vertices with mutual distance $\geqslant 3$ (use $P = (X + 2)(X - 1)$ and $3(P(5) + 3P((3 - \sqrt{17})/2)) > 2P(2) + 3P((3 + \sqrt{17})/2))$. These are the true values, see Fig. 4.

6. Distance to a set of vertices

Stronger results on distances between the set of vertices of a graph can be obtained. when the graph is distance-regular. In this case good bounds can be given on the distance between a vertex v and a set of vertices C (defined as the length of a shortest path connecting v to a vertex of C).

For that purpose we need some facts from [1]. A distance regular graph is a graph such that for every couple of vertices (u, v) at distance j the following holds (see 1. Ch. 20):

(1) the number of vertices at distance $j - 1$ from v adjacent to u is always c_j a number which depends only on j;

(2) the number of vertices at distance $j + 1$ from v adjacent to u is always b_j;

(3) the number of vertices at distance j from v adjacent to u is always a_j some number depending only on j.

It is straightforward to check that for every eigenvalue λ of a distance-regular graph, the inner product $\langle s_\lambda \,|\, t_\lambda \rangle$ depends only on λ and the distance n of s and t. It can be computed by

$$f(\lambda, n) = \frac{m_\lambda}{N} \frac{R_n(\lambda)}{R_n(k)}$$

where R_n is the polynomial given by $R_{-1} = 0$, $R_0 = 1$, $R_{D+1} = 0$ and $XR_n = a_n R_n + c_{n+1}R_{n+1} + b_{n-1}R_{n-1}$ for $0 \leqslant n \leqslant D$ where D is the diameter of the graph.

Thus, if the graph is distance-regular, one can compute the lengths of the projections C_λ on the eigenspaces from the distance distribution inside $\mathscr{C}$.

$$|C_\lambda|^2 = \sum_n f(\lambda, n) T_n$$

where T_n is the number of couples inside C with distance n.

Now let 1_C be the characteristic function of C, in other words $\sum_{v \in C} 1_v$. Then the distance between C and s is also the smallest integer $m \geqslant 0$ such that $\langle 1_C \,|\, A^m(1_s) \rangle \neq 0$; and if Q is a polynomial of degree d such that $\langle 1_C \,|\, Q(A)1_s \rangle > 0$ then the distance between C and s is at most d. If this inner product is equal to zero, then this means that (the sum being on all eigenvalues λ of the regular graph we consider)

$$\sum_\lambda \langle C_\lambda \,|\, Q(\lambda)v_\lambda \rangle = 0. \tag{3}$$

Let us notice that a distance-regular is always regular — say that in our case the degree is k. Here $\langle C_k \,|\, s_k \rangle = |C|/N$, so the sum of inner products in expression (3) cannot be equal to 0 if

$$\langle C_k \,|\, Q(k)s_k \rangle = \frac{Q(k)|C|}{N} > \sum_{\lambda \in \Lambda \backslash k} \langle C_\lambda \,|\, Q(\lambda)s_\lambda \rangle.$$

Using the Cauchy–Schwartz inequality $\langle C_\lambda \,|\, s_\lambda \rangle \leqslant |C_\lambda| |s_\lambda|$ and Proposition 1 (a distance-regular graph is necessarily vertex transitive) we see that if

$$\frac{Q(k)|C|}{N} > \sum_{\lambda \in \Lambda \backslash k} |Q(\lambda)| \, |C_\lambda| \sqrt{\frac{m_\lambda}{N}}$$

we necessarily have $\langle 1_C \,|\, Q(A)1_s \rangle > 0$. From this we deduce

Proposition 6. *Let G be a connected distance-regular graph of degree k, and C a subset of vertices of G. If there is a polynomial Q of degree d such that*

$$\frac{Q(k)|C|}{N} > \sum_{\lambda \in \Lambda \backslash k} |Q(\lambda)| \, |C_\lambda| \sqrt{\frac{m_\lambda}{N}}$$

then the distance between C and any vertex of G is at most d.

We will see in the next section how this proposition can be improved when G is a Cayley graph, and C a subgroup of G.

Example 9. Petersen graph has spectrum $3^1, 1^5, (-2)^4$. We can compute $\langle s_\lambda \mid t_i \rangle$ as a function of λ and the distance n of s and t.

$\lambda \backslash n$	0	1	2
3	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{1}{10}$
1	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{-1}{6}$
-2	$\frac{2}{5}$	$\frac{-4}{15}$	$\frac{1}{15}$

Let us consider a subset C consisting of 4 vertices with mutual distances 2 and let us compute the lengths of the components of 1_C

$$|C_3|^2 = 4\frac{1}{10} + 12\frac{1}{10} = \frac{16}{10},$$

$$|C_1|^2 = 4\frac{1}{2} + 12\frac{-1}{6} = 0,$$

$$|C_{-2}|^2 = 4\frac{2}{5} + 12\frac{1}{15} = \frac{12}{5}.$$

Using Proposition 6 and the polynomial $Q = X + 1$ we obtain

$$Q(3)\frac{1}{10} > |Q(1)||C_1|\sqrt{\frac{5}{10}} + |Q(-2)||C_{-2}|\sqrt{\frac{4}{10}}.$$

Hence each vertex of the graph is at most distance 1 from C.

7. Application to codes

There are several applications of these results to coding theory. For example Sections 2 and 6 can be used in order to obtain an upper bound on the covering radius of a code, when the weight distribution of the codewords is known. Section 4 is relevant to the problem of obtaining upper bounds on the cardinality of a code with a given maximum distance. We bring in our graph-theoretic results by observing that a code of length n on F_q (the finite field of q elements) — in other words a subset of F_q^n can be viewed as a subset of vertices of the Hamming graph $H(n,q)$ which is the cartesian sum of n complete graphs with q vertices each. An equivalent definition of $H(n,q)$ is to say that the set of vertices of this graph is F_q^n, and two vertices $(x_1, y_1, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ are adjacent iff they differ by exactly one coordinate. In this case the usual Hamming distance between two codewords (i.e. the number of places where they differ) is exactly the distance between the two corresponding vertices in $H(n,q)$.

An interesting feature of these graphs $H(n,q)$ is that they are distance-regular, and that their spectrum is well known (see [2])

Proposition 7. $H(n,q)$ *is a distance-regular graph and the associated polynomial* $R_0(x), R_1(x), \ldots, R_n(x)$ *(see Section 6) are given by*

$$R_k(x) = P_k^{q,n}\left(\frac{q-1}{q}n - \frac{x}{q}\right),$$

where $P_k^{q,n}$ *is the Krawtchouk polynomial of degree* k*, associated to* q *and* n *(see* [15, *Ch. 5]). These polynomials are defined by*

$$(1 + (q-1)z)^{n-x}(1-z)^x = \sum_{k=0}^{\infty} P_k^{q,n}(x)z^k.$$

The eigenvalues of this graph are $\lambda_i = (q-1)n - qi$*,* $0 \leqslant i \leqslant n$*, with multiplicities* $m_i = \binom{n}{i}(q-1)^i$*. The eigenspace associated to the eigenvalue* $\lambda_i = (q-1)n - qi$ *is obtained from a primitive* q*th root of unity* ξ *as the vector space spanned by the vectors*

$$e_u = \begin{pmatrix} \xi^{\langle u \mid v_1 \rangle} \\ \xi^{\langle u \mid v_2 \rangle} \\ \ldots \\ \xi^{\langle u \mid v_{q^n} \rangle} \end{pmatrix},$$

u *running over the set of vectors of weight* i*, where* $v_1, v_2, \ldots, v_{q^n}$ *are the vectors representing the vertices of the Hamming graph* $H(n,q)$*, and* $\langle \mid \rangle$ *the usual inner product of two vectors of length* n *over* F_q.

7.1. An upper bound on the cardinality of a code of minimum distance 3

By viewing a code as a subset of vertices of $H(n,q)$, it becomes obvious that a binary code of length n of minimum distance d, is a set of vertices of the n-cube which are at distance at least d apart. A subset of vertices of this graph whose mutual distances are at least 3 can be seen to have a cardinality smaller than or equal to $2^n/(n+1)$ for n odd, by using Proposition 4 with the polynomial $(x+1)^2$, and smaller than or equal to $2^n/(n+2)$ for n even. This is essentially equivalent to the sphere-packing bound (see [15, Theorem 12, Ch. 17, Section 3]).

7.2. MacWilliams identities

Before we see how to use the results of Section 6 in order to get upper bounds on the covering radius of a graph, it might be insightful to observe that the lengths of the projections C_λ have a simple combinatorial interpretation when C is a subset of vertices of the Hamming graph $H(n,q)$, and represents therefore a q-ary code of length n.

Indeed we can use Proposition 7 and calculate from that

$$
|C_{(q-1)n-qi}|^2 = \frac{1}{q^n} \sum_{u/wt(u)=i} \left| \sum_{v \in C} \xi^{\langle u \mid v \rangle} \right|^2
$$

$$
= \frac{1}{q^n} \sum_{u/wt(u)=i} \sum_{v \in C} \xi^{\langle u \mid v \rangle} \sum_{w \in C} \xi^{\langle u \mid -w \rangle}
$$

$$
= \frac{1}{q^n} \sum_{u/wt(u)=i} \sum_{v,w \in C} \xi^{\langle u \mid v-w \rangle} \tag{4}
$$

($wt(u)$ denotes here the weight of vector u). It is readily seen that the last sum is equal to $(|C|^2/q^n)B_i'$, B_i' denoting here the transform of the distance distribution of C corresponding to the weight i (see [15, Ch. 5, Section 5]). When the code C is linear this number has an interesting combinatorial interpretation, for it is straightforward to check that $\sum_{v \in C} \xi^{\langle u \mid v \rangle} = 0$ when $\langle u \mid v \rangle \neq 0$ for some v in C, and $\sum_{v \in C} \xi^{\langle u \mid v \rangle} = |C|$ if $\langle u \mid v \rangle = 0$ for all $v \in C$. Therefore $|C_{(q-1)n-qi}|^2$ is equal to $|C|^2/q^n$ times the number of codewords of weight i in the dual of C. So that when C is linear, B_i' is just the number of codewords of weight i in dual the $C^\perp$ of C.

By using the results of Section 6 we can calculate in another way the lengths of these projections C_λ, by doing this we obtain the MacWilliams identities in coding theory (see [15, Ch. 5]). From Proposition 7 (T_j denotes the number of couples of codewords which are at distance j)

$$
|C_{(q-1)n-qi}|^2 = \sum_{j=0}^{n} \binom{n}{i} \frac{(q-1)^i}{q^n} \frac{P_j(i)}{P_j(0)} T_j.
$$

We recall two well-known facts about Krawtchouk polynomials

$$
\frac{P_j(i)}{P_j(0)} = \frac{P_i(j)}{P_i(0)} \quad \text{and} \quad P_i(0) = \binom{n}{i}(q-1)^i.
$$

Hence

$$
|C_{(q-1)n-qi}|^2 = \frac{1}{q^n} \sum_{j=0}^{n} P_i(j) T_j. \tag{5}
$$

Comparing expressions (4) and (5) we get

$$
B_i' = \frac{1}{|C|^2} \sum_{j=0}^{n} P_i(j) T_j.
$$

This is the generalized MacWilliams identity (see [15, Theorem 5]). Let us denote by B_i the number of codewords of weight i in C, when C is a linear code, $T_j = |C|B_j$, and therefore we obtain the usual MacWilliams identity for linear codes

$$
B_i' = \frac{1}{|C|} \sum_{j=0}^{n} P_i(j) B_j.
$$

7.3. The covering radius of a code

7.3.1. The covering radius of a linear code

Two different approaches may be used to obtain an upper bound on the covering radius of a code. The obvious approach is to use Proposition 6. However when the code C is linear it is better to use Corollary 1. This is done by associating to a linear code a Cayley graph — the so-called coset graph of the code. Let us recall here — for more details see Chapter 11 in [2] for example — that given a linear code C over F_q (the field of order q) of length n, i.e. a vector subspace of F_q^n, one can construct the coset graph $\Gamma(C)$ of this code as follows:

- the set of vertices is F_q^n/C,
- two vertices x and y are joined by an edge if and only if the coset $x - y$ contains a vector of F_q^n with exactly one non-zero coordinate.

This graph is sometimes called the syndrome graph associated to the linear code C for it can be described from a parity-check matrix of the code as follows.. Let us recall that, given a $r \times n$ parity-check matrix H of rank r which defines the code C as the set of vectors $x \in F_q^n$ satisfying $Hx = 0$, the syndrome of a vector $x \in F_q^n$ is Hx. It can be checked that the coset graph is isomorphic to the graph with vertex set the set of syndromes, and there is an edge between two different syndromes y and y' iff there is a vector e of weight 1 such that $y - y' = He$. Viewing these vectors y and y' as column vectors, they differ in this case by a vector proportional to a column of H.

It can be easily checked that this graph displays the following interesting features (for a proof see [2, Ch. 11]):

Proposition 8. 1. *The coset graph is a $(q-1)n$-regular Cayley graph.*

2. *The distance between the all-0 vector in F_q^r and a syndrome y is the least number of columns of H which generate y.*

3. *Its diameter is equal to the covering radius of C.*

4. *Its spectrum Λ can be described by using the dual code $C^\perp$ of C, more precisely*

$$\Lambda = \{n(q-1) - qw(x)/x \in C^\perp\}$$

where $w(x)$ denotes the Hamming weight of the codeword x, i.e., the number of its non-zero coordinates, and the dual code of C is the set of vectors x such that $\langle x \mid y \rangle = 0$ for every y in C, the inner product being performed in F_q.

Thus all what we need to obtain an upper bound on the covering radius is to know the weight-distribution of its dual code. Putting Proposition 8 and Corollary 1 together we get

Proposition 9. *Let C be a linear code of length n. If there is a polynomial Q of degree d such that*

$$Q(0) > \sum_{i=1}^{n} |Q(i)|B_i'$$

where B_i' is the number of words of weight i in the dual of C, then the covering radius of C is at most d.

(We apply Corollary 8 to the coset graph of the code — and we have a polynomial P of degree d which meets the condition given in the corollary, iff the polynomial $Q(x) = P((q-1)n - qx))$ of degree d satisfies the aforementioned inequality).

Remark. This proposition is actually an improved version of Proposition 6 when used for codes, and can be derived from the arguments given in Section 6 by modifying one of the characteristic vectors a little bit. Assume that vertex s is at some distance d from C in the graph $H(n,q)$. When C is a linear code, $C + s$ is at the same distance d from C. Therefore $\langle 1_C \mid P(A)1_s \rangle = 0$ iff $\langle 1_C \mid P(A)1_{C+s} \rangle = 0$. Call C_λ^s the projection on the eigenspace corresponding to λ of the vector 1_{C-s}. If we replace the quantities s_λ by C_λ^s in the discussion given in Section 6, then whenever there is a polynomial P of degree d such that

$$\frac{P((q-1)n)|C|^2}{N} > \sum_{i=1}^{n} |P((q-1)n - qi)||C_{(q-1)n-qi}|^2$$

or if we let $Q(x) = P((q-1)n - qx)$,

$$\frac{Q(0)|C|^2}{N} > \sum_{i=1}^{n} |Q(i)||C_{(q-1)n-qi}|^2,$$

the covering radius of the code is less than or equal to the the degree of P. We can use the interpretation of $|C_\lambda|^2$ given in the previous subsection, and notice that this gives us another proof of Proposition 9. Actually this trick can be used in a more general setting, and works for example when the graph is a Cayley graph, and the subset $\mathscr{C}$ a subgroup of the set of vertices.

7.3.2. Covering radius and dual distance

Now what if less is known about the weight distribution of the dual $C^\perp$? Interesting results about the covering radius may be obtained, if we can at least estimate the minimum distance of the dual code. The best of these upper bounds on the covering radius depending on the minimum distance can be found in [12] and can be easily derived by a graph-theoretic approach when the code is linear by using Proposition 8 and the main theorem given in [4], although it was obtained by other means in [12]. Let us mention that these results can be obtained by our approach too.

Indeed if we had a polynomial Q such that

$$Q(0) > |C^\perp| \max_{x \in [d',n]} |Q(x)|$$

d' denoting here the smallest $i > 0$ such that $B_i' \neq 0$ (i.e. what is called the minimum distance of the dual code of C), and $|C^\perp|$ the number of codewords in the dual of C.

e.g $\sum_{i=0}^{n} B'_i$) then

$$|Q(0)| > \sum_{i=1}^{n} |Q(i)| B'_i.$$

This implies that the covering radius of C would be less than or equal to the degree of this polynomial Q, by using Proposition 9. It is well known (see [4] for example) that a polynomial $Q(x)$ of a given degree d such that $Q(0)/\max_{x \in [d',n]} |Q(x)|$ is maximum is proportional to $T_d((n+d'-2x)/(n-d'))/T_d((n+d')/(n-d'))$, where $T_d(x)$ is the Tchebychev polynomial of the first kind of degree d, i.e. $\cosh(d \cosh^{-1}(x))$. The corresponding ratio is $1/T_d(n+d'/n-d')$. In other words if

$$\frac{1}{T_d \left(\frac{n+d'}{n-d'} \right)} > |C^{\perp}| \tag{6}$$

then the covering radius is less than or equal to d. When the dual code $C^{\perp}$ has minimum distance d', then it has asymptotically at most $2^{n(1+o(1))H_2(1/2-\sqrt{d/n(1-d/n)})}$ codewords, $H_2(x)$ being $-x \log_2 x - (1-x)log_2(1-x)$ (this is the McEliece–Rodemich–Rumsey–Welch upper bound see [15, Ch. 17, Section 7]). Denote by δ' the ratio d'/n and by ρ the fraction R/n, where R is the covering radius of the code. Then inequality 6 certainly holds for a Tchebychev polynomial of degree greater (asymptotically) than

$$n \frac{H_2 \left(\frac{1}{2} - \sqrt{\delta'(1-\delta')} \right)}{\log_2 e \cosh^{-1} \left(\frac{1+\delta'}{1-\delta'} \right)},$$

this implies that

$$\rho < (1+o(1)) \frac{H_2 \left(\frac{1}{2} - \sqrt{\delta'(1-\delta')} \right)}{\log_2 e \cosh^{-1} \left(\frac{1+\delta'}{1-\delta'} \right)}$$

which is the bound given in [12].

7.3.3. The Delsarte bound

Not so many upper bounds on the covering radius are known, and Propositions 6 and 9 give here a new bound which is always at least as good as the Delsarte bound (which says that the covering radius is at most the number l of non-zero distinct weights $w_1, w_2, \ldots, w_l$ of the dual code). We just have to choose $Q(X)$ in Proposition 6 to be $\Pi_i(X - w_i)$. Proposition 6 sometimes gives results which are substantially better than the Delsarte bound, as shown by the following examples.

7.4. Examples

Example 10. It is well known that the Delsarte bound is not always tight (see [16] for example). In [16] an alternative approach is used to find the covering radius of

Table 2

$n \backslash \lambda$	7	5	3	1	-1	-3	-5	-7
0	1	1	1	1	1	1	1	1
1	7	5	3	1	-1	-3	-5	-7
2	21	9	1	-3	-3	1	9	21
3	35	5	-5	-3	3	5	-5	-35
4	35	-5	-5	3	3	-5	-5	35
5	21	-9	1	3	-3	-1	9	-21
6	7	-5	3	-1	-1	3	-5	7
7	1	-1	1	-1	1	-1	1	-1
m_λ	1	7	21	35	35	21	7	1

codes for which the bound of Delsarte fails to meet the actual value. In that article H.F Mattson considers for instance a code of parity-check matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

The corresponding code C has length 10, dimension 4 and minimum distance 4. It can be checked that its dual D has the following weight distribution:

Weight	0	3	4	5	6	7	10
Number of words	1	10	15	12	15	10	1

The Delsarte bound shows that the covering radius of C is less than or equal to 6, the number of distinct nonzero weights of codewords of D. Nevertheless, it can be proved that the covering radius is 4 [16]. Let us show that this result can be obtained from our approach too. From Proposition 9, and by choosing $Q(X) = (X - 3)(X - 4)$ $(X - 6)(X - 10)$ it can be shown that the covering radius of C is at most 4 (since $Q(0) > 12Q(5) + 10Q(7)$). The covering radius is 4 because the syndrome $(1, 1, 1, 1, 1, 1)$ (considered as a column vector) is neither the sum of two columns of H, nor the sum of an odd number of columns of H (by an obvious parity argument). Therefore, it is the sum of at least 4 columns of H, and we conclude by using Proposition 8.

Example 11. The ambiant graph is the 7-cube K_2^7.

The eigenvalues, their multiplicities and the value of $R_n(\lambda)$ appear in Table 2.

The cyclic linear binary code of length 7 generated by 1001011 has 8 vectors, with distance 0 occurring 8 times and distance 4 occurring 56 times. Thus the lengths of the components C_λ of this code are given by Table 3.

Table 3

λ	7	5	3	1	−1	−3	−5	−7
8×	1	7	21	35	35	21	7	1
56×	1	−1	−3	3	3	−3	−1	1
$N\|C_\lambda\|^2$	64	0	0	448	448	0	0	64

Table 4

λ	7	5	3	1	−1	−3	−5	−7
$\|\langle s_\lambda \mid C_\lambda\rangle\|$	$\frac{1}{2}$	0	0	$\leqslant \frac{7\sqrt{5}}{2}$	$\leqslant \frac{7\sqrt{5}}{2}$	0	0	$\frac{1}{2}$

Table 5

λ	5	3	1	−1	−3	−5
$\|C_\lambda\|^2$	10	0	4	0	18	0
$\|z_\lambda\|^2$	1	5	10	10	5	1
$\|C_\lambda z_\lambda\|$	1	0	$\leqslant 2$	0	$\leqslant 3$	0

From this we can estimate $|\langle s_\lambda \mid C_\lambda\rangle|$ (see Table 4).

Hence $2\langle 1_C \mid (A^3 + A^2)(1_x)\rangle \geqslant 392 - 14\sqrt{5} - 294 > 0$, and the maximum distance is at most 3 (this is the actual value).

Example 12. The ambiant graph is the 5-cube. The nonlinear code formed by all words of length 1 or 4 has weight distribution proportional to 1,0,4,4,0,1. Thus the squares of the lengths of the vectors C_λ and z_λ and their inner products are proportional to the values in the following Table 5.

Thus if $Q(5) > 2|Q(1)| + 3|Q(-3)|$ the covering radius is at most the degree of Q. For $Q = (X - 1)(X + 3)$ the relation obviously holds. For $Q = X + 3$, we have only $Q(5) = 2Q(1)$. Thus the vertices z such that the vectors z_1 and C_1 have opposite directions are at most at distance 1 from C. In fact the covering radius is easily seen to be 1 from the definition of the code.

Example 13. For the linear code C with length 15 and weight distribution [15] given in Table 6 we obtain the squares of the lengths of the vectors C_λ; those which are not equal to 0 are proportional to values given in Table 7.

This also gives the weight distribution of its dual D (see Table 8).

From the number of eigenvalues giving a nonnull component C_λ or D_λ, we see that the covering radius of D is at most 5 and the one of C is at most 7.

Table 6

Weight	0	4	6	8	10	12
Number of words	1	15	100	75	60	5

Table 7

λ	± 15	± 5	± 3	± 1
Squared length	1	18	30	15

Table 8

Weight	0	5	6	7	8	9	10	15
Number of words	1	18	30	15	15	30	18	1

To improve the first bound by our method, we have to find a polynomial Q_D of degree 4 or less such that

$$Q_D(15) > \sqrt{15 \times 1365}|Q_D(7)| + \sqrt{100 \times 5005}|Q_D(3)| + \sqrt{75 \times 6435}|Q_D(-1)|$$
$$+ \sqrt{60 \times 3003}|Q_D(-5)| + \sqrt{5 \times 455}|Q_D(-9)|.$$

This is impossible, this polynomial Q being optimal as can be checked by using the algorithm given in Section 3.

The calculation can be made simpler in the case of a binary code C where all the weights are even. Indeed, if z is at even distance from all points of the code C, we have $\langle 1_C | A^n(1_C) \rangle = 0$ for all odd exponents n, and if z is at odd distance from all points of C, then $\langle 1_C | A^n(1_C) \rangle = 0$ for all even exponents n. This shows that $\langle C_\lambda | z_\lambda \rangle$ and $\langle C_{-\lambda} | z_{-\lambda} \rangle$ are equal in the first case and opposite in the second case for each eigenvalue λ.

With z at odd distance from C the odd polynomial $Q_C = X((X^2 - 13)^2 - 80)$ gives the sum of the equal quantities $\langle C_{15} | Q_C(A)(z_{15}) \rangle$ and $\langle C_{-15} | Q_C(A)(z_{-15}) \rangle$ larger than the remaining part of $\langle 1_C | Q_C(A)(1_z) \rangle$, since $Q_C(15) > |Q_C(5)|\sqrt{18 \times 3003} + |Q_C(3)|\sqrt{30 \times 5005} + |Q_C(1)|\sqrt{15 \times 6435}$. This shows that the covering radius is at most 6.

We can improve on these results by using Proposition 9. The spectrum of the coset graph of C is $\pm 15^1$, $\pm 5^{18}$, $\pm 3^{30}$, $\pm 1^{15}$. The polynomial $P = (X - 3)(X - 1)(X + 5)$ $(X + 15)$ takes only positive values on the other eigenvalues, and we have $P(15) = 100\,800 > 52\,800 = 18P(5) + 15P(-1) + 30P(-3)$. Hence the diameter of the coset graph of C is at most 4 as well as the covering radius of C.

In the same way the spectrum of the coset graph of D shows that it contains at most 2 vertices at distance > 4, owing to the polynomial $P = (X - 3)(X + 1)(X + 5)(X + 9)$ for which $P(15) = 15P(7) > 0$.

References

[1] N. Biggs, Algebraic graph theory, Cambridge Tracts in Mathematics, vol. 67 (Cambridge University Press, London, 1974).

[2] A.E. Brouwer, A.M. Cohen and A. Neumaier, Distance-regular graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete, No 18 (Springer, Berlin, 1989).

[3] F.R.K. Chung, Diameters and eigenvalues, J. Amer. Math. Soc. 2(2) (1989) 187–196.

[4] F.R.K. Chung, V. Faber and T.A. Manteuffel, An upper bound on the diameter of a graph from eigenvalues associated with its Laplacian, SIAM J. Discrete Math. 7 (1994) 443–457.

[5] B.D. Craven, Mathematical programming and control theory, Chapman and Hall Mathematics Series (Chapman & Hall, 1978).

[6] D. Čvetković, M. Doob and H. Sachs, Spectra of graphs (Academic Press, New York, 1980).

[7] C. Delorme and P. Solé, Diameter, covering index, covering radius and eigenvalues, European J. Combin. 12 (1991) 95–108.

[8] P. Diaconis, Group Representations in Probability and Statistics, Institute of Mathematical Statistics, Lecture Notes-Monograph Series, vol. 11 (1988).

[9] V. Faber, An estimate of the diameter of a graph from the singular values and eigenvalues of its adjacency matrix, preprint, 1990.

[10] M.A. Fiol, E. Garriga and J.L.A. Yebra, On a class of polynomials and its relation with the spectra and diameter of graphs, J. Combin. Theory Ser. B 67 (1996) 48–61.

[11] N. Kahale, Isoperimetric Inequalities and eigenvalues, Technical Report DIMACS 93-83, 1993.

[12] S.N. Litsyn and A. Tietäväinen, Covering radius, dual distance and codimension, European J. Combin. 17 (1996) 265–270.

[13] L. Lovász, On the Shannon capacity of a graph, IEEE Trans. Inform. Theory, IT 25 (1979) 1–7.

[14] A. Lubotsky, R. Phillips and P. Sarnak, Ramanujan graphs, Combinatorica 8 1988 261–277.

[15] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes (North-Holland, Amsterdam, 1981).

[16] H.F. Mattson, An upper bound on covering radius, Ann. of Discrete Math. 17 (1982) 453–458.

[17] H. Minc, Nonnegative Matrices (Wiley Interscience, New York, 1988).

[18] P. Sarnak, Some Applications of Modular Forms (Cambridge University Press, London, 1990).

[19] P. Solé and P. Stokes, Covering radius, codimension and dual distance width, IEEE Trans. Inform. Theory 39 (1993) 1195–1203.

[20] J.H. van Lint, Introduction to coding theory, Graduate texts in Mathematics, No. 86 (Springer, Berlin, 2nd ed., 1992).