Journal of Algebraic Combinatorics 4 (1995), 317–327

A Family of Antipodal Distance-Regular Graphs Related to the Classical Preparata Codes

D. DE CAEN
Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6

R. MATHON
Department of Computer Science, University of Toronto, Toronto, Ontario M5S 1A1

G.E. MOORHOUSE
Department of Mathematics, University of Wyoming, Laramie, WY 82071

Received August 6, 1993; Revised November 4, 1994

Abstract. A new family of distance-regular graphs is constructed. They are antipodal 2^{2t-1}-fold covers of the complete graph on 2^{2t} vertices. The automorphism groups are determined, and the extended Preparata codes are reconstructed using walks on these graphs.

There are connections to other interesting structures: the graphs are equivalent to certain generalized Hadamard matrices; and their underlying 3-class association scheme is formally dual to the scheme of a system of linked symmetric designs obtained from Kerdock sets of skew matrices in characteristic two.

1. Introduction

We refer to Brouwer, Cohen and Neumaier [3] for the definition and theory of distance-regular graphs. Such a graph Γ, of diameter d, is said to be *antipodal* if all vertices at distance d from any given vertex are at distance d from each other; cf. [3], Section 4.2. When d equals three, Γ is an r-fold cover of a complete graph K_n, where n is the number of antipodal classes (called *fibres*) and r is the size of each fibre. See Godsil and Hensel [6] for an extensive study of this class of graphs. In particular, they show ([6] Lemma 3.1) that an antipodal distance-regular graph of diameter three can be specified by the triple of parameters (n, r, c_2), where n and r are as above and c_2 is the number of common neighbours to any pair of vertices at distance two. Such a graph is called an (n, r, c_2)-cover. Our main result is the construction of $(2^{2t}, 2^{2t-1}, 2)$-covers for every positive integer t. In the following statement ϕ denotes Euler's phi function.

Theorem 1.1 *There exist at least* $\frac{1}{2}\phi(2t-1)$ *pairwise nonisomorphic* $(2^{2t}, 2^{2t-1}, 2)$-*covers.*

The description of these graphs follows. Put $q = 2^{2t-1}$ and $s = 2^e$ where $\gcd(e, 2t-1) = 1$. The graph $\Gamma(q, s)$ has vertex-set $GF(q) \times GF(2) \times GF(q)$, and adjacency relation determined by

$$(a, i, \alpha) \sim (b, j, \beta) \Leftrightarrow \alpha + \beta = a^s b + ab^s + (i + j)(a^{s+1} + b^{s+1}),$$

where '$\sim$' means 'is adjacent or equal to'. We will show after Lemma 2.2 that $\Gamma(q, s)$ is distance-regular. It is clear from the definition that $\Gamma(q, s)$ is a q-fold cover of K_{2q}, having

as its fibres the point-sets

$$V_{a,i} = \{(a, i, \alpha): \alpha \in GF(q)\}, a \in GF(q), i \in GF(2).$$

Note that $\Gamma(2, 2)$ is the familiar 3-cube; the other graphs are new. We will determine the automorphism groups of these graphs in Section 2. The result is the following.

Theorem 1.2 *For any $t \geq 3$ and any e coprime to $2t - 1$, the full automorphism group of $\Gamma(2^{2t-1}, 2^e)$ has order $2^{2t}(2^{2t-1} - 1)(2t - 1)$. It is generated by the following vertex permutations, where $q = 2^{2t-1}$ and $s = 2^e$:*

(i) $(a, i, \alpha) \mapsto (a, i, \alpha + u)$, $u \in GF(q)$;
(ii) $(a, i, \alpha) \mapsto (\lambda a^\tau, i, \lambda^{s+1}\alpha^\tau)$, $\lambda \in GF(q)\backslash\{0\}$, $\tau \in Aut(GF(q))$;
(iii) $(a, i, \alpha) \mapsto (a, i + 1, \alpha)$.

This group has just two orbits on vertices, one of which is $V_{0,0} \cup V_{0,1}$.

We remark that $\Gamma(8, 2)$ is indeed an exceptional graph: Marston Conder (private communication) has shown that Aut $\Gamma(8, 2)$ is a vertex-transitive group isomorphic to 2×2^3. SL(3, 2) (where the latter extension 2^3. SL(3, 2) is non-split), and that the Sylow 2-subgroup acts regularly on $\Gamma(8, 2)$.

It will be shown in Section 3 that $\Gamma(q, 2^e)$ and $\Gamma(q, 2^f)$ are isomorphic if and only if $e + f \equiv 0 \bmod(2t - 1)$; this will complete the proof of Theorem 1.1. The argument will exploit an interesting connection to the Preparata codes: the latter may be constructed using certain walks in the graphs $\Gamma(q, s)$, so that Kantor's work [9] on the automorphism groups of the codes applies.

Observe that the group of automorphisms of type (i) in Theorem 1.2 fixes every fibre and acts regularly on each fibre. It follows from a quotienting construction of [6], Corollary 6.3, that there exist $(2^{2t}, 2^{2t-i}, 2^i)$-covers for $1 \leq i \leq 2t$. Such covers were already known in the range $t \leq i \leq 2t$, cf. [6], p. 220; the other parameter sets are new.

2. Automorphisms of the covers

Let Tr:$GF(q) \to GF(2)$ denote the trace map, where as before $q = 2^{2t-1}$. Note that $\mathrm{Tr}(1) = 1$ since $2t - 1$ is odd. Also, if $s = 2^e$ is any integer with e coprime to $2t - 1$, then $\mathrm{Tr}(x) = \sum_{i=0}^{2t-2} x^{s^i}$.

Lemma 2.1 *Given $a \in GF(q)$, the equation $x^s + x + a = 0$ has 0 or 2 solutions $x \in GF(q)$, according as $Tr(a) = 1$ or 0.*

Proof: If x is a solution, then $\mathrm{Tr}(a) = \mathrm{Tr}(x^s + x) = 0$. On the other hand, suppose that $\mathrm{Tr}(a) = 0$. Set $\theta = x + \sum_{i=0}^{t-1} a^{s^{2i}}$. Then $\theta^s = x^s + \sum_{i=0}^{t-1} a^{s^{2i+1}}$ and therefore $\theta^s + \theta = x^s + x + a + \mathrm{Tr}(a) = x^s + x + a$. Since the fixed field of the automorphism $\theta \mapsto \theta^s$ is $GF(2)$, this gives two solutions θ to the equation $\theta^s + \theta = 0$, and hence exactly two solutions x to the equation $x^s + x + a = 0$. □

Remark In what follows we will frequently make use of the fact that the maps $x \mapsto x^{s-1}$ and $x \mapsto x^{s+1}$ are bijections of the field $GF(q)$. This follows from the computation

$\gcd(s^2-1, q-1) = \gcd(2^{2e}-1, 2^{2t-1}-1) = 2^{\gcd(2e,2t-1)}-1 = 2^{\gcd(e,2t-1)}-1 = 2^1-1 = 1$.

Lemma 2.2 *Let $A = (a, i, \alpha)$ and $B = (b, j, \beta)$ be two non-adjacent vertices of $\Gamma = \Gamma(q, s)$ in distinct fibres. Then A and B have exactly two common neighbours in Γ. Moreover,*

(i) *If $i = j$, these two common neighbours lie in the fibres $V_{c,k}$ and $V_{a+b+c,k}$, where $k = i + Tr((\alpha+\beta)/(a+b)^{s+1})$, and c is one solution of*

$$\left(\frac{c}{a+b}\right)^s + \frac{c}{a+b} + \frac{(i+k)(a^{s+1}+b^{s+1})+\alpha+\beta}{(a+b)^{s+1}} = 0.$$

(ii) *If $i \neq j$, these two common neighbours lie in the fibres $V_{c,k+i}$ where $k = 0, 1$, and c satisfies*

$$(c+a+b)^{s+1} = ka^{s+1} + (k+1)b^{s+1} + \alpha + \beta + (a+b)^{s+1}.$$

Proof: If the vertex $C = (c, k, \gamma)$ is adjacent to both A and B, then

$$\alpha + \gamma = a^s c + ac^s + (i+k)(a^{s+1} + c^{s+1}), \tag{1}$$

and

$$\beta + \gamma = b^s c + bc^s + (j+k)(b^{s+1} + c^{s+1}). \tag{2}$$

Consider first the case $i = j$. Adding (1) and (2) and rearranging terms gives the equation for c given in (i) above. By Lemma 2.1, in order for solutions to exist, we require that

$$\begin{aligned} 0 &= \mathrm{Tr}\left[\frac{(i+k)(a^{s+1}+b^{s+1})+\alpha+\beta}{(a+b)^{s+1}}\right] \\ &= \mathrm{Tr}\left[(i+k)\left(1+\frac{a}{a+b}+\left(\frac{a}{a+b}\right)^s\right)+\frac{\alpha+\beta}{(a+b)^{s+1}}\right] \\ &= i+k+\mathrm{Tr}\left[\frac{\alpha+\beta}{(a+b)^{s+1}}\right], \end{aligned}$$

which gives the required formula for k. By Lemma 2.1, the resulting equation for c has exactly two solutions. One may solve uniquely for γ using either (1) or (2), so that there exist exactly two vertices C satisfying $A \sim C \sim B$. Since $A \not\sim B$, such vertices C do not coincide with either A or B. Therefore A and B have exactly two common neighbours, and these lie in the fibres described in (i).

Now consider the case $i \neq j$. Again adding (1) and (2) and rearranging gives

$$(c+a+b)^{s+1} = (i+k)a^{s+1} + (j+k)b^{s+1} + \alpha + \beta + (a+b)^{s+1}.$$

Replacing k by $i+k$ gives the equation for c given in conclusion (ii). Since $x \mapsto x^{s+1}$ is bijective, each value of $k \in \{0, 1\}$ gives a unique solution for c. The result follows as before. □

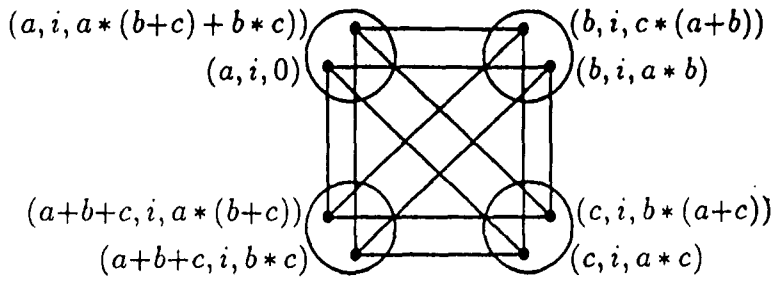

Figure 1.

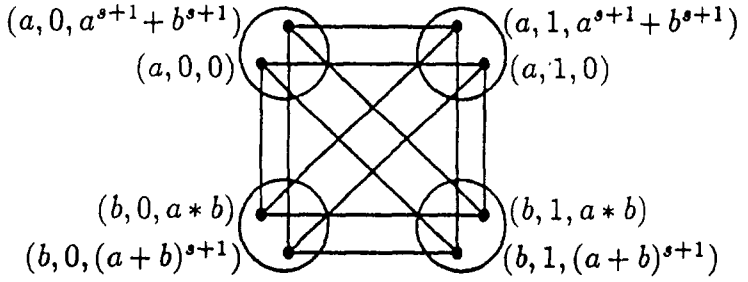

Figure 2.

By Lemma 3.1 of [6], we immediately obtain that $\Gamma(q, s)$ is a $(2q, q, 2)$-cover, for any $s = 2^e$ with $\gcd(e, 2t-1) = 1$. This yields $\phi(2t-1)$ distinct graphs; but it is easy to check that the map $(a, i, \alpha) \mapsto (a, i, \alpha^s)$ is an isomorphism from $\Gamma(q, q/s)$ to $\Gamma(q, s)$. We will show after Theorem 3.3 that we have in fact $\frac{1}{2}\phi(2t-1)$ nonisomorphic graphs.

We call a set of four fibres of $\Gamma = \Gamma(q, s)$ a *quad* if their union contains an isometrically embedded copy of the 3-cube. Clearly this can only happen if opposite vertices of the cube are in the same fibre. Figures 1 and 2 illustrate two types of quads that occur in Γ. There we use the abbreviation $a*b := a^s b + ab^s$. Note that in these figures a, b and c are distinct elements of $GF(q)$.

Lemma 2.3 *The quads are the sets of the form*

(i) $\{V_{a,i}, V_{b,i}, V_{c,i}, V_{a+b+c,i}\}$ *where* $a, b, c \in GF(q)$ *are distinct, and* $i \in GF(2)$, *and*
(ii) $\{V_{a,0}, V_{a,1}, V_{b,0}, V_{b,1}\}$ *where* $a, b \in GF(q)$ *are distinct.*

Proof: Figures 1 and 2 show that sets of the form (i) and (ii) are quads. We proceed to prove the converse.

Let us say that the fibre $V_{a,i}$ is of type i. If a quad consists of four fibres $V_{a,i}$, $V_{b,i}$, $V_{c,i}$, $V_{d,i}$ of the same type, then it is clear from Lemma 2.2(i) that $a+b+c+d = 0$, and so conclusion (i) holds.

Otherwise, it is clear from Lemma 2.2 that we have two fibres of each type, say $V_{a,0}$, $V_{b,1}$, $V_{c,0}$, $V_{d,1}$. Again by Lemma 2.2(i) we have $a+b+c+d = 0$. But by Lemma 2.2(ii), we

have $(c+a+b)^{s+1}+(d+a+b)^{s+1}=a^{s+1}+b^{s+1}$, i.e.

$$\begin{aligned}0 &= a^{s+1}+b^{s+1}+c^{s+1}+(a+b+c)^{s+1}\\ &= a^sb+ab^s+a^sc+ac^s+b^sc+bc^s\\ &= (a+b)(a+c)[(a+b)^{s-1}+(a+c)^{s-1}].\end{aligned}$$

But $a \neq c$ and $x \mapsto x^{s-1}$ is bijective, so either $a=b$ and $c=d$, or $b=c$ and $a=d$, so that conclusion (ii) holds. □

The collection of fibres forms a system of imprimitivity for the action of $G = \mathrm{Aut}(\Gamma)$ on the vertices, because the fibres are equivalence classes for the antipodal relation. Let N be the elementary abelian subgroup of G consisting of all automorphisms of the form $(a,i,\alpha) \mapsto (a,i,\alpha+u)$, $u \in GF(q)$. Clearly N fixes each fibre, and acts regularly on the vertices in each fibre. By [6, Lemma 7.3], N is the full kernel of the action of G on the set of fibres, which proves the following.

Lemma 2.4 *The action of G on the set of fibres is given by $\bar{G} = G/N$.*

Corollary 2.5 *Suppose $q > 2$. Then the permutation group $\bar{G}$ is imprimitive. Two systems of imprimitivity are given by*

(i) $\{\{V_{a,0}: a \in GF(q)\}, \{V_{a,1}: a \in GF(q)\}\}$, *and*
(ii) $\{\{V_{a,0}, V_{a,1}\}: a \in GF(q)\}$.

Proof: If $S_i := \{V_{a,i}: a \in GF(q)\}$, $i \in \{0,1\}$, then by Lemma 2.3, any three fibres in S_i are contained in a quad in S_i; moreover S_0 and S_1 are the only q-sets of fibres with this property. It follows that (i) is a system of imprimitivity for $\bar{G}$. Similarly, the system (ii) can be recognized via Lemma 2.3, by the property that any pair $\{V_{a,0}, V_{a,1}\}$, together with an arbitrary third fibre, is contained in a unique quad. □

Once again we use the abbreviation $a * b := a^sb + ab^s = (a+b)^{s+1} + a^{s+1} + b^{s+1}$, which is an alternating $GF(2)$-bilinear form on $GF(q)$.

Lemma 2.6 *If $q > 2$, then the automorphisms of Γ are the transformations of the form $(a,i,\alpha) \mapsto (a^\rho + c, i+k, \alpha^\pi + c * a^\rho + \gamma)$ where $c, \gamma \in GF(q)$, $k \in GF(2)$, and $\rho, \pi: GF(q) \to GF(q)$ are additive (i.e. $GF(2)$-linear) bijections such that $(x^{s+1})^\pi = (x^\rho + c)^{s+1} + c^{s+1}$ for all $x \in GF(q)$.*

Proof: It is straightforward to check that all transformations of the latter form are isomorphisms of Γ, and we leave this as an exercise.

Conversely, let $\theta \in G$. We may suppose that θ maps type-0 fibres to type-0 fibres; otherwise, by Corollary 2.5(i), θ maps type-0 fibres to type-1 fibres, and we may replace θ by $\theta \circ \phi$, where $\phi: (a,i,\alpha) \mapsto (a, i+1, \alpha)$. Let $V_{c,0} = V_{0,0}^\theta$. Then θ induces a permutation on the type-0 fibres given by $V_{a,0}^\theta = V_{a^\rho+c,0}$ where $\rho: GF(q) \to GF(q)$ is some permutation fixing 0. Also, there exists a bijection $\pi: GF(q) \to GF(q)$ satisfying $(0,0,\alpha)^\theta = (c,0,\alpha^\pi)$. Since translations $(a,i,\alpha) \mapsto (a,i,\alpha+u)$ are automorphisms, there is no loss of generality in assuming $0^\pi = 0$. It is now easy to see that the pair

of permutations (ρ, π) completely determines θ. Indeed, note that $(a, 0, \alpha) \sim (0, 0, \alpha)$, and therefore $(a, 0, \alpha)^\theta = (a^\rho + c, 0, \alpha^\pi + c * a^\rho)$, since this is the unique vertex in $V_{a^\rho+c,0}$ adjacent/equal to $(0, 0, \alpha)^\theta = (c, 0, \alpha^\pi)$. Furthermore, by Corollary 2.5(ii), we have $V^\theta_{a,1} = V_{a^\rho+c,1}$, and since $(a, 0, \alpha) \sim (a, 1, \alpha)$, we have

$$(a, i, \alpha)^\theta = (a^\rho + c, i, \alpha^\pi + c * a^\rho)$$

for every vertex (a, i, α). Now $(a, 0, \alpha) \sim (b, 1, \alpha + (a + b)^{s+1})$, so applying θ gives $(a^\rho + c, 0, \alpha^\pi + c * a^\rho) \sim (b^\rho + c, 1, [\alpha + (a + b)^{s+1}]^\pi + c * b^\rho)$, i.e.

$$\begin{aligned}[\alpha + (a + b)^{s+1}]^\pi &= \alpha^\pi + c * (a^\rho + b^\rho) + (a^\rho + b^\rho)^{s+1} \\ &= \alpha^\pi + (a^\rho + b^\rho + c)^{s+1} + c^{s+1} \end{aligned} \tag{3}$$

for all $a, b, \beta \in GF(q)$. The special case $b = 0$ gives $(\alpha + a^{s+1})^\pi = \alpha^\pi + (a^\rho + c)^{s+1} + c^{s+1}$ since $0^\rho = 0$. Specializing further to the case $\alpha = b = 0$ gives

$$(a^{s+1})^\pi = (a^\rho + c)^{s+1} + c^{s+1} \tag{4}$$

since $0^\pi = 0$. Combining this with the previous relation, we obtain $(\alpha + a^{s+1})^\pi = \alpha^\pi + (a^{s+1})^\pi$. However, every element of $GF(q)$ is expressible in the form a^{s+1}, so the latter identity implies that $\pi: GF(q) \to GF(q)$ is additive. Returning to (3), this implies that $((a + b)^{s+1})^\pi = (a^\rho + b^\rho + c)^{s+1} + c^{s+1}$. Applying (4) to the left side of the latter identity yields $((a + b)^\rho + c)^{s+1} + c^{s+1} = (a^\rho + b^\rho + c)^{s+1} + c^{s+1}$. Since $x \mapsto x^{s+1}$ is bijective, this implies that $(a + b)^\rho = a^\rho + b^\rho$ for all $a, b \in GF(q)$. □

At this point it is convenient to recall the Baker-van Lint-Wilson generalization [1] (see also [4], p. 185) of the Preparata code. The *extended Preparata code* $\bar{\mathcal{P}}(q, s)$ is the set of all pairs (X, Y) such that $X, Y \subseteq GF(q)$ satisfy the conditions

(i) $|X|$ and $|Y|$ are both even;
(ii) $\sum_{x\in X} x = \sum_{y\in Y} y$; and
(iii) $\sum_{x\in X} x^{s+1} + (\sum_{x\in X} x)^{s+1} = \sum_{y\in Y} y^{s+1}$.

Note that we may identify X and Y with their characteristic vectors, so that $\bar{\mathcal{P}}(q, s)$ is a binary code of length $2q$.

Proof of Theorem 1.2: Let θ be any automorphism of Γ, with the associated permutations $\pi, \rho: GF(q) \to GF(q)$ in the notation of Lemma 2.6. We will prove that θ induces an automorphism $\tilde{\theta}$ of $\bar{\mathcal{P}}(q, s)$, so that we may appeal to Kantor [9]. For $S \subseteq GF(q)$, define $S^\rho := \{x^\rho : x \in S\}$ and $S + d := \{x + d : x \in S\}$. Suppose that $(X, Y) \in \bar{\mathcal{P}}(q, s)$; we will show that $(X, Y)^{\tilde{\theta}} := (X^\rho, Y^\rho + c)$, where c is as in the statement of Lemma 2.6, also belongs to $\bar{\mathcal{P}}(q, s)$. The conditions (i) and (ii) defining the codes are very easy to verify, since $|X^\rho| = |X|$ and $|Y^\rho + c| = |Y|$ are both even and also

$$\sum_{x\in X} x^\rho = \left(\sum_{x\in X} x\right)^\rho = \left(\sum_{y\in Y} y\right)^\rho = \sum_{y\in Y} y^\rho = \sum_{y\in Y} (y^\rho + c),$$

the last equation holding since $|Y|$ is even. To verify the third Preparata condition, we use the identity $(x^{s+1})^\pi = (x^\rho + c)^{s+1} + c^{s+1} = (x^\rho)^{s+1} + c * x^\rho$ to compute that

$$\begin{aligned}
&\sum_{x\in X}(x^\rho)^{s+1} + \left(\sum_{x\in X} x^\rho\right)^{s+1} \\
&\quad = \sum_{x\in X}[(x^{s+1})^\pi + c * x^\rho] + \left(\left(\sum_{x\in X} x\right)^\rho\right)^{s+1} \\
&\quad = \left(\sum_{x\in X} x^{s+1}\right)^\pi + c * \left(\sum_{x\in X} x\right)^\rho + \left(\left(\sum_{x\in X} x\right)^{s+1}\right)^\pi + c * \left(\sum_{x\in X} x\right)^\rho \\
&\quad = \left[\sum_{x\in X} x^{s+1} + \left(\sum_{x\in X} x\right)^{s+1}\right]^\pi = \left(\sum_{y\in Y} y^{s+1}\right)^\pi \\
&\quad = \sum_{y\in Y}(y^{s+1})^\pi = \sum_{y\in Y}[(y^\rho + c)^{s+1} + c^{s+1}] = \sum_{y\in Y}(y^\rho + c)^{s+1}.
\end{aligned}$$

Thus $\tilde{\theta}$ is an automorphism of $\bar{\mathcal{P}}(q, s)$. When $q \geq 32$, Theorem 3 of [9] implies that $c = 0$ and that $x^\rho = \lambda x^\tau$, $x^\pi = \lambda^{s+1} x^\tau$ for some $\lambda \in GF(q)\backslash\{0\}$ and $\tau \in \mathrm{Aut}\, GF(q)$. □

3. Construction of the extended Preparata codes from the graphs

In this section, we construct a code C using walks on the graph $\Gamma = \Gamma(q, s)$. Recall that a *walk* is a sequence of adjacent vertices, with possibly repeated vertices. Although it is possible to describe this code C in terms of Γ using our previous coordinatization by $GF(q) \times GF(2) \times GF(q)$, we instead use new notation in order to make clear that C is an isomorphism invariant of Γ. Using our previous coordinatization we will show that C is equivalent to the extended Preparata code $\bar{\mathcal{P}}(q, s)$.

Let us start by distinguishing one vertex O as the origin of Γ. For $q \geq 2^5$, we choose O to be any vertex in the smaller orbit of $\mathrm{Aut}(\Gamma)$. In view of the action of $\mathrm{Aut}(\Gamma)$ we may suppose that $O = (0, 0, 0)$. For $q = 8$, Γ is vertex transitive, so O can be chosen arbitrarily, but again, we will suppose that $O = (0, 0, 0)$. Let V_O be the fibre containing O, and let V'_O be its matched fibre, as in Corollary 2.5(ii). These are the fibres previously coordinatized as $V_{0,0}$ and $V_{0,1}$.

Next, we define a relation on the vertices of each fibre. For A and B in the same fibre, we write $A \approx B$ if there exist vertices $C_0 \in V_O$ and $C_1 \in V'_O$ such that $A \sim C_0 \sim C_1 \sim B$. The proof of the following is left as an exercise.

Lemma 3.1 *We have $(a, i, \alpha) \approx (a, i, \beta)$ if and only if $\alpha + \beta = a^{s+1}$. Therefore the relation $\approx$ is symmetric. On the fibres V_O and V'_O, the relation $\approx$ means '='. On the fibres $V_{a,i}$ with $a \neq 0$, the relation $\approx$ is irreflexive and induces a pairing of the vertices.*

We will say that the vertex (a, i, α), and the fibre $V_{a,i}$, are of type i. Note that the partition of fibres (or vertices) into two types is isomorphism-invariant by Corollary 2.5,

and by Theorem 1.2(iii), it matters not which type we call type 0. Next, consider the matching between fibres of opposite type, given by Corollary 2.5(ii). We colour these pairs of matched fibres using q arbitrary but distinct colours, COL $= \{C_a : a \in GF(q)\}$, where C_a is the colour of the matched pair $\{V_{a,0}, V_{a,1}\}$. We are going to label the edges of mixed type (i.e. edges between type 0 and 1 vertices) using this same set of colours. Let A and B be adjacent vertices of type 0 and 1 respectively. By Lemma 2.2, there exist unique vertices C and D of type 0 and 1 respectively, such that $C \in V_O$ and we have a 4-cycle $A \sim B \sim C \sim D \sim A$. Then we assign the colour C_d to the edge (A, B), where C_d is the colour of the fibre containing D. The next result follows easily from Lemma 2.2(i); the details are left as an exercise.

Lemma 3.2 *Each edge between $V_{a,0}$ and $V_{b,1}$ is coloured C_{a+b}. Each vertex of Γ shares exactly q coloured (mixed-type) edges, one of each colour. The unique edge of colour C_x from (a, i, α) leads to $(a + x, i + 1, \alpha + x^{s+1})$.*

Given a subset $\mathcal{X} \subseteq$ COL (or the corresponding subset $X \subset GF(q)$, $X = \{x \in GF(q) : C_x \in \mathcal{X}\}$) such that $|\mathcal{X}|$ is even, a *walk* of colour $\mathcal{X}$ from a vertex A, is a walk of length $|\mathcal{X}|$ on Γ, starting at A and using one edge of colour C_x for each element $C_x \in \mathcal{X}$. Note that for $|\mathcal{X}| \geq 2$, there is more than one walk of colour $\mathcal{X}$ starting at any given vertex A. However, by Lemma 3.2, any walk of colour $\mathcal{X}$ starting at (a, i, α) will always end up at $W_{\mathcal{X}}(a, i, \alpha) := (a + \sum_{x \in X} x, i, \alpha + \sum_{x \in X} x^{s+1})$, independent of the order of colours chosen from $\mathcal{X}$. The condition that $|\mathcal{X}|$ is even, ensures that the walk ends up at a vertex of the same type as it starts.

Now define $\mathcal{C}$ to be the set of all pairs $(\mathcal{X}, \mathcal{Y})$ such that $\mathcal{X}, \mathcal{Y} \subseteq$ COL, with $|\mathcal{X}|$ and $|\mathcal{Y}|$ both even, such that $W_{\mathcal{X}}(O) \approx W_{\mathcal{Y}}(O)$. In particular, note that the walks of colours $\mathcal{X}$ and $\mathcal{Y}$ starting at O, are required to both end up at the *same* fibre of type 0. Identifying $\mathcal{X} \subseteq$ COL with $X \subseteq GF(q)$, and $\mathcal{Y} \subseteq$ COL with $Y \subseteq GF(q)$ similarly, we have the following.

Theorem 3.3 $\mathcal{C} = \tilde{\mathcal{P}}(q, s)$.

Proof: Since $W_{\mathcal{X}}(O) = (\sum_{x \in X} x, 0, \sum_{x \in X} x^{s+1})$ and $W_{\mathcal{Y}}(O) = (\sum_{y \in Y} y, 0, \sum_{y \in Y} y^{s+1})$, the result follows from Lemma 3.1 and the definition of the generalized Preparata codes. □

We may now easily complete the proof of Theorem 1.1. Our construction of $\mathcal{C}$ from $\Gamma(q, s)$ is isomorphism invariant. Thus if $\Gamma(q, 2^e) \simeq \Gamma(q, 2^f)$ then $\tilde{\mathcal{P}}(q, 2^e) \simeq \tilde{\mathcal{P}}(q, 2^f)$; and Theorem 2 of [9] implies that $e + f \equiv 0 \bmod (2t - 1)$. Hence we have $\frac{1}{2}\phi(2t - 1)$ nonisomorphic graphs, as desired.

4. Generalized Hadamard matrices

Since the graphs $\Gamma(q, s)$ are regular covers in the sense of Godsil and Hensel ([6], Section 7), they are associated to certain generalized Hadamard matrices. Recall that a GHM(n, G) is an $n \times n$ matrix H, with entries from an additively written group G, such that the rows of H are formally orthogonal, i.e. for any pair i, j of distinct row indices the differences $h_{ik} - h_{jk}$ $(k = 1, 2, \ldots, n)$ represent each element of G the same number of times, namely

$\frac{n}{r}$ where $r = |G|$. If H is formally skew, i.e. $h_{ij} = -h_{ji}$ for $i \neq j$ and $h_{ii} = 0$ for all i, then one can construct an $(n, r, \frac{n}{r})$-cover from H, as follows. Replace each diagonal entry by an $r \times r$ block of zeroes; and for $i \neq j$ replace $h_{ij} = g$ by the $r \times r$ permutation matrix corresponding to g in the regular representation of G. This yields the adjacency matrix of a distance-regular cover of K_n; see [6], Sections 7–9, for more details.

Theorem 4.1 *For each $t \geq 1$ there exists a formally skew $GHM(2^{2t}, EA(2^{2t-1}))$.*

Proof: Here $EA(2^{2t-1})$ denotes the elementary abelian 2-group of rank $2t-1$, i.e. the additive group of $GF(2^{2t-1})$. Fix e coprime to $2t-1$, and set $s = 2^e$. Now define a matrix H of order 2^{2t}, with indices represented as pairs $ai \in GF(2^{2t-1}) \times GF(2)$, as follows:

$$h_{ai,bj} := a^s b + ab^s + (i+j)(a^{s+1} + b^{s+1})$$

It is not hard to show that H has all the desired properties; indeed, from the equivalence proven in [6], Theorem 7.4, this follows from our earlier work. □

We remark that Jungnickel [8] has constructed GHM$(2^{2t}, EA(2^{2t-1}))$, but his examples are not formally skew.

5. Maximum cocliques

A simple counting argument shows that in any $(2^{2t}, 2^{2t-1}, 2)$-cover $a_1 = 0$, i.e. the graph is triangle-free. Gardiner [5] has studied such graphs; in particular he showed that the only feasible parameter sets for triangle-free $(n, r, 2)$-covers must have $n = 4k^2$ and $r = 2k^2$ for some integer k. Thus our Theorem 1.1 settles the existence question when k is a power of two.

Let $\alpha = \alpha(\Gamma)$ denote the size of a largest coclique (independent set) in the graph Γ. A deep theorem of Ajtai, Komlós and Szemerédi (see e.g. [2], Ch. XII.3) implies that there is an absolute positive constant c such that, for every r-regular triangle-free Γ on v vertices, $\alpha(\Gamma) > cvr^{-1} \ln r$. It is an open question whether this estimate is asymptotically best possible. If Γ is a $(2^{2t}, 2^{2t-1}, 2)$-cover, we thus have that $\alpha(\Gamma) > dt2^{2t}$ for some absolute $d > 0$. It appears difficult to verify this estimate for our graphs $\Gamma(q, s)$ in a constructive manner. We note the following upper bound.

Theorem 5.1 *For any $(2^{2t}, 2^{2t-1}, 2)$-cover, $\alpha \leq 2^{3t-1}$.*

Proof: One can easily compute (cf. [6]) that the smallest eigenvalue is $\tau = -2^t - 1$. Hoffman's upper bound (cf. [3], Prop. 1.3.2(i)) is

$$\alpha \leq v \cdot \frac{-\tau}{d - \tau} \quad \text{(where } d = \text{valency)}$$
$$= 2^{4t-1} \cdot \frac{(2^t + 1)}{(2^{2t} - 1) + (2^t + 1)} = 2^{3t-1}.$$ □

Note that when $t = 1$, i.e. the 3-cube, this upper bound is tight. For any (16, 8, 2)-cover we get $\alpha \leq 32$. A computer check showed that in fact $\Gamma(8, 2)$ has $\alpha = 29$. The structure

of cocliques of size 29 is interesting: there are exactly 128 of them, and the point-coclique incidence matrix is a square partially balanced incomplete block design.

6. Formal duality with respect to systems of linked square designs

An (n, r, c_2)-cover has four eigenvalues; in the notation of [6] they are $n-1, -1, \theta$ and τ, with $\theta > 0 > \tau$. The eigenmatrix of the underlying 3-class association scheme $\mathcal{B}$ is

$$P = \begin{bmatrix} 1 & (n-1) & (n-1)(r-1) & (r-1) \\ 1 & -1 & -(r-1) & (r-1) \\ 1 & \theta & -\theta & -1 \\ 1 & \tau & -\tau & -1 \end{bmatrix}$$

and the dual eigenmatrix (satisfying $PQ = nrI$) is

$$Q = \begin{bmatrix} 1 & n-1 & \dfrac{\tau n(r-1)}{a} & \dfrac{\theta n(r-1)}{a} \\ 1 & -1 & \dfrac{n(r-1)}{a} & \dfrac{n(r-1)}{a} \\ 1 & -1 & \dfrac{n}{a} & \dfrac{n}{a} \\ 1 & n-1 & \dfrac{\tau n}{a} & \dfrac{\theta n}{a} \end{bmatrix}$$

where a is the square root of $(n-2-rc_2)^2 + 4(n-1)$.

It may happen that some other 3-class association scheme $\mathcal{B}^*$ has eigenmatrix equal to Q and dual eigenmatrix equal to P; when this happens $\mathcal{B}$ and $\mathcal{B}^*$ are said to be *formally dual* to each other. See [3], p. 49, for a brief introduction to this notion. One should stress that $\mathcal{B}$ and $\mathcal{B}^*$ need not be structurally related; formal duality is on the face of it just a question of parameters.

Now in the case of $(2^{2t}, 2^{2t-1}, 2)$-covers, there *is* a formally dual object, namely a system of 2^{2t-1} linked square (v, k, λ)-designs with $v = 2^{2t}, k = 2^{2t-1} - 2^{t-1}$ and $\lambda = 2^{2t-2} - 2^{t-1}$. See [10] and [4], p. 148, for information on linked square designs. One may readily check (cf. the eigenmatrices on p. 133 of [10]) that the underlying 3-class scheme of linked designs with the above parameters is indeed formally dual to the scheme of a $(2^{2t}, 2^{2t-1}, 2)$-cover. Furthermore, the known construction of linked designs uses Kerdock sets of skew matrices in even characteristic. Thus, intriguingly, there is a parallel between the present formal duality (between covers and linked designs) and the formal duality, via the MacWilliams transform, between Kerdock codes and Preparata codes; cf. [4], especially p. 144 and p. 187. In important recent work, Hammons et al. [7] have constructed new Preparata-like codes that are dual over $\mathbf{Z}_4$ to the classical Kerdock codes. This prompted the use of the word "classical" in the title of the present paper.

Acknowledgment

The first two authors' research is supported financially by grants from the Natural Sciences and Engineering Research Council of Canada. We thank the referees for some helpful comments, and Andries Brouwer for suggesting a simplified proof of Corollary 2.5.

References

1. R.D. Baker, J.H. van Lint, and R.M. Wilson, "On the Preparata and Goethals codes," *IEEE Trans. Info. Th.* **29** (1983), 342–345.
2. B. Bollobás, *Random Graphs*, Academic Press, 1985.
3. A.E. Brouwer, A.M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, 1989.
4. P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, 1991.
5. A. Gardiner, "Antipodal Graphs of Diameter Three," *Linear Algebra and its Applications* **46** (1982), 215–219.
6. C.D. Godsil and A.D. Hensel, "Distance regular covers of the complete graph," *Journal of Combin. Th. Ser. B* **56** (1992), 205–238.
7. A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, "The Z_4-linearity of Kerdock, Preparata, Goethals and Related Codes," *IEEE Trans. Inform. Theory* **40** (1994), 301–319.
8. D. Jungnickel, "On difference matrices, resolvable transversal designs and generalized Hadamard matrices," *Math. Z.* **167** (1969), 49–60.
9. W.M. Kantor, "On the inequivalence of generalized Preparata codes," *IEEE Trans. Info. Th.* **29** (1983), 345–348.
10. R. Mathon, "The systems of linked 2-(16,6,2) designs," *Ars Combinatoria* **11** (1981), 131–148.