Total perfect codes in Cayley graphs

Sanming Zhou

Department of Mathematics and Statistics
The University of Melbourne

December 2, 2011
VAC29, La Trobe University

perfect codes

Definition

Let V be an alphabet of size q, and let $1 \leq t \leq n$ be integers.

Denote by V^n the set of words of length n over V.

perfect codes

Definition

Let V be an alphabet of size q, and let $1 \leq t \leq n$ be integers.

Denote by V^n the set of words of length n over V.

A perfect t-code of length n is a subset $C \subset V^n$ such that every codeword in V^n is at Hamming-distance at most t from a unique codeword in C.

perfect codes

Definition

Let V be an alphabet of size q, and let $1 \leq t \leq n$ be integers.

Denote by V^n the set of words of length n over V.

A perfect t-code of length n is a subset $C \subset V^n$ such that every codeword in V^n is at Hamming-distance at most t from a unique codeword in C.

A perfect 1-code is usually called a perfect code.

perfect codes

Definition

Let V be an alphabet of size q, and let $1 \leq t \leq n$ be integers.

Denote by V^n the set of words of length n over V.

A perfect t-code of length n is a subset $C \subset V^n$ such that every codeword in V^n is at Hamming-distance at most t from a unique codeword in C.

A perfect 1-code is usually called a perfect code.

If a perfect t-code exists, then a certain polynomial of degree t has t distinct zeros among $1, 2, \ldots, n$.

This was proved by Lloyd when q is a prime power and Lenstra (1972) for all q.

perfect codes

Definition

A binary code of length $n = 2^r - 1$, $r \geq 2$, with an $r \times (2^r - 1)$ parity checking matrix H is called a binary Hamming code if the columns of H are all nonzero vectors of $\mathbb{F}_2^r$.

That is, the codewords of a binary Hamming code are precisely vectors $\mathbf{v} \in \mathbb{F}_2^n$ such that $H\mathbf{v} = \mathbf{0}$.

perfect codes

Definition

A binary code of length $n = 2^r - 1$, $r \geq 2$, with an $r \times (2^r - 1)$ parity checking matrix H is called a binary Hamming code if the columns of H are all nonzero vectors of $\mathbb{F}_2^r$.

That is, the codewords of a binary Hamming code are precisely vectors $\mathbf{v} \in \mathbb{F}_2^n$ such that $H\mathbf{v} = \mathbf{0}$.

Hamming codes are linear, i.e. subspaces of linear spaces.

perfect codes

Definition

A binary code of length $n = 2^r - 1$, $r \geq 2$, with an $r \times (2^r - 1)$ parity checking matrix H is called a binary Hamming code if the columns of H are all nonzero vectors of $\mathbb{F}_2^r$.

That is, the codewords of a binary Hamming code are precisely vectors $\mathbf{v} \in \mathbb{F}_2^n$ such that $H\mathbf{v} = \mathbf{0}$.

Hamming codes are linear, i.e. subspaces of linear spaces.

Theorem

(Tietäväinen 1973, Leontiev & Zinoviev 1973)
When q is a prime power, the only linear perfect t-codes are

(a) *the binary Hamming codes ($t = 1$),*

(b) *the trivial perfect codes ($n = t$, or $n = 2t + 1$ and $q = 2$), and*

(c) *the two Golay codes ($(n, q, t) = (11, 3, 2)$ or $(23, 2, 3)$).*

perfect codes in graphs

Definition

(N. Biggs 1973)
Let G be a graph. A subset C of $V(G)$ is a perfect t-code in G if for any $v \in V(G)$ there exists exactly one vertex in C whose distance to v is at most t.

That is, the subsets

$$N_t(u) := \{v \in V(G) : d(u, v) \leq t\},\ u \in C,$$

form a partition of $V(G)$.

A perfect 1-code is called a perfect code.

A perfect t-code in G must be an independent set of G.

perfect codes in graphs

Definition

(N. Biggs 1973)
Let G be a graph. A subset C of $V(G)$ is a perfect t-code in G if for any $v \in V(G)$ there exists exactly one vertex in C whose distance to v is at most t.

That is, the subsets

$$N_t(u) := \{v \in V(G) : d(u, v) \leq t\},\ u \in C,$$

form a partition of $V(G)$.

A perfect 1-code is called a perfect code.

A perfect t-code in G must be an independent set of G.

Question

When does a graph admit a perfect t-code or perfect code?

perfect codes in distance-transitive graphs

Theorem

(N. Biggs 1973)
Let G be a distance-transitive graph of diameter k.

If G has a perfect t-code, then $1 + v_1(\lambda) + \cdots + v_t(\lambda)$ divides $1 + v_1(\lambda) + \cdots + v_k(\lambda)$ in $\mathbb{Q}(\lambda)$,

where $v_1(\lambda), \ldots, v_k(\lambda)$ are certain polynomials defined in terms of the intersection matrix of G.

This generalises LLoyd's necessary condition.

perfect codes in distance-transitive graphs

Theorem
(N. Biggs 1973)
Let G be a distance-transitive graph of diameter k.

If G has a perfect t-code, then $1 + v_1(\lambda) + \cdots + v_t(\lambda)$ divides $1 + v_1(\lambda) + \cdots + v_k(\lambda)$ in $\mathbb{Q}(\lambda)$,

where $v_1(\lambda), \ldots, v_k(\lambda)$ are certain polynomials defined in terms of the intersection matrix of G.

This generalises LLoyd's necessary condition.

Theorem
(Biggs 1973)
A d-regular graph of order n admits a perfect code only when

(a) *$d + 1$ divides n, and*

(b) *-1 is an eigenvalue of the adjacency matrix of the graph.*

perfect codes in graphs

Existence of perfect t-codes has been studied for

- hypercubes (Hamming codes)

perfect codes in graphs

Existence of perfect t-codes has been studied for

- hypercubes (Hamming codes)
- cube-connected cycles (Livingston & Stout 1990)

perfect codes in graphs

Existence of perfect t-codes has been studied for

- hypercubes (Hamming codes)
- cube-connected cycles (Livingston & Stout 1990)
- meshes and tori (Livingston & Stout 1990)

perfect codes in graphs

Existence of perfect t-codes has been studied for

- hypercubes (Hamming codes)
- cube-connected cycles (Livingston & Stout 1990)
- meshes and tori (Livingston & Stout 1990)
- de Bruijn graphs (Livingston & Stout 1990)

perfect codes in graphs

Existence of perfect t-codes has been studied for

- hypercubes (Hamming codes)
- cube-connected cycles (Livingston & Stout 1990)
- meshes and tori (Livingston & Stout 1990)
- de Bruijn graphs (Livingston & Stout 1990)
- antipodal distance-transitive graphs (antipodal: $d(u, v) = d(u, w) = k$ (diameter) $\Rightarrow v = w$ or $d(v, w) = k$)

perfect codes in graphs

Existence of perfect t-codes has been studied for

- hypercubes (Hamming codes)
- cube-connected cycles (Livingston & Stout 1990)
- meshes and tori (Livingston & Stout 1990)
- de Bruijn graphs (Livingston & Stout 1990)
- antipodal distance-transitive graphs (antipodal: $d(u,v) = d(u,w) = k$ (diameter) $\Rightarrow v = w$ or $d(v,w) = k$)
- odd graphs (Hammond & Smith 1975)
- ...

terminology used by graph theorists

- efficient dominating set = perfect 1-code (Bange, Barkauskas and Slater 1987)
- perfect t-dominating set = perfect t-code

perfect codes in odd graphs

Definition

The odd graph $O(k)$ is defined to have vertices the k-subsets of $[2k+1]$ such that two vertices are adjacent iff they are disjoint.

perfect codes in odd graphs

Definition

The odd graph $O(k)$ is defined to have vertices the k-subsets of $[2k+1]$ such that two vertices are adjacent iff they are disjoint.

It is known that $O(3)$ and $O(5)$ have perfect codes.

perfect codes in odd graphs

Definition

The odd graph $O(k)$ is defined to have vertices the k-subsets of $[2k+1]$ such that two vertices are adjacent iff they are disjoint.

It is known that $O(3)$ and $O(5)$ have perfect codes.

No perfect code is known in other odd graphs.

perfect codes in odd graphs

Definition

The odd graph $O(k)$ is defined to have vertices the k-subsets of $[2k+1]$ such that two vertices are adjacent iff they are disjoint.

It is known that $O(3)$ and $O(5)$ have perfect codes.

No perfect code is known in other odd graphs.

It is believed that no more exist.

perfect codes in odd graphs

Definition

The odd graph $O(k)$ is defined to have vertices the k-subsets of $[2k+1]$ such that two vertices are adjacent iff they are disjoint.

It is known that $O(3)$ and $O(5)$ have perfect codes.

No perfect code is known in other odd graphs.

It is believed that no more exist.

Theorem

(Hammond & Smith 1975)
A set of k-subsets of $[2k+1]$ is a perfect code in $O(k)$ if and only if it is a 1-$(2k+1, k, k-1)$ design.

perfect codes in a family of distance-regular graphs

Perfect 1-codes in an infinite class of distance-regular graphs were constructed by Cameron, Thas and Payne (1976) using generalized hexagons.

perfect codes in a family of distance-regular graphs

Perfect 1-codes in an infinite class of distance-regular graphs were constructed by Cameron, Thas and Payne (1976) using generalized hexagons.

A generalized hexagon of order (s, t) is a point-line geometry whose incidence graph has girth 12 and diameter 6, and such that each line (point) is incident with exactly $s + 1$ points ($t + 1$ lines).

perfect codes in direct products of cycles

Definition

The direct product $G \times H$ is defined to have vertex set $V(G) \times V(H)$ such that $(u_1, v_1) \sim (u_2, v_2)$ if and only if $u_1 \sim u_2$ in G and $v_1 \sim v_2$ in H.

perfect codes in direct products of cycles

Definition

The direct product $G \times H$ is defined to have vertex set $V(G) \times V(H)$ such that $(u_1, v_1) \sim (u_2, v_2)$ if and only if $u_1 \sim u_2$ in G and $v_1 \sim v_2$ in H.

Theorem

(Žerovnik 2008)
The direct product $\times_{i=1}^{n} C_{\ell_i}$, $\ell_i \geq 2t+2$, *contains a perfect* t*-code if and only if every* ℓ_i *is a multiple of* $t^n + (t+1)^n$.

Partial results were obtained earlier by Klavžar, Špacapan and Žerovnik (Adv. Appl. Math. 2006).

perfect codes in product graphs

Perfect codes have been studied for

- direct product (Klavžar, Špacapan and Žerovnik 06)
- Cartesian product (M. Mollard 11)
- lexicographic product (D. T. Taylor 09)

E-chains in Cayley graphs

Definition

Let X be a group and $S \subseteq X - \{1\}$ be such that $S^{-1} = S$.

The Cayley graph $\mathrm{Cay}(X, S)$ is defined to have vertex set X in which $x \sim y$ iff $x^{-1}y \in S$.

Definition

(Dejter & Serra 2003)
A family of graphs

$$\{G_1, G_2, \ldots, G_i, G_{i+1}, \ldots\}$$

is called an E-chain if each G_i is an induced subgraph of G_{i+1} and each G_i has an perfect code.

E-chains in Cayley graphs

Definition

Let X be a group and $S \subseteq X - \{1\}$ be such that $S^{-1} = S$.

The Cayley graph $\mathrm{Cay}(X, S)$ is defined to have vertex set X in which $x \sim y$ iff $x^{-1}y \in S$.

Definition

(Dejter & Serra 2003)
A family of graphs

$$\{G_1, G_2, \ldots, G_i, G_{i+1}, \ldots\}$$

is called an E-chain if each G_i is an induced subgraph of G_{i+1} and each G_i has an perfect code.

Example

$\{Q_{2^r-1} : r \geq 2\}$ is an E-chain.

E-chains in Cayley graphs

Dejter and Serra (2003) gave a methodology for constructing E-chains of Cayley graphs.

They used this method to construct E-chains of Cayley graphs on symmetric groups, including the family of star graphs (Arumugam and Kala 1996).

perfect codes in Cayley graphs

Theorem

(J. Lee 2001)

Let C be a normal subset of a finite group X (i.e. $xC = Cx$ for all $x \in X$). Then the following are equivalent:

(a) *C is a perfect code in a connected Cayley graph $\mathrm{Cay}(X, S)$;*

(b) *there exists a covering $\mathrm{Cay}(X, S) \to K_{|S|+1}$ such that $p^{-1}(v) = C$ for some vertex v of $K_{|S|+1}$;*

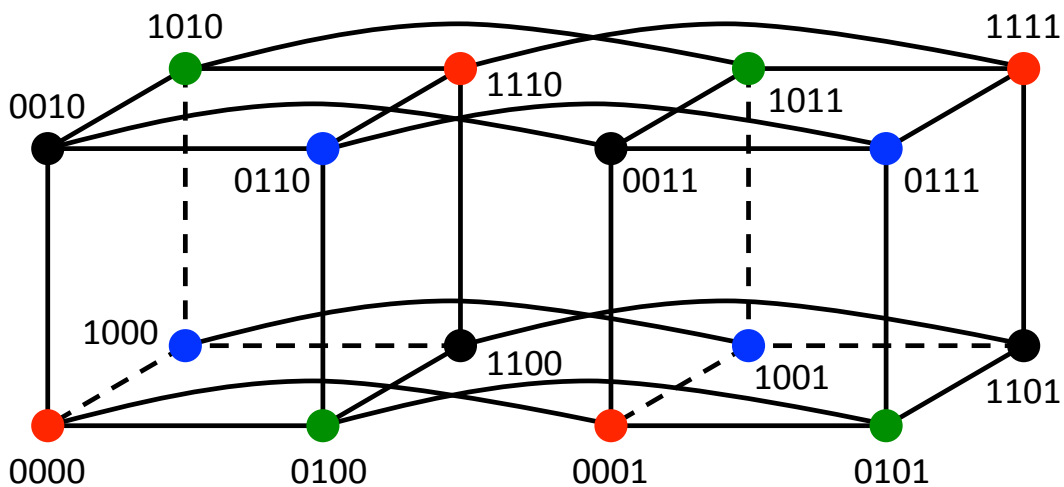
(c) *$|C|(|S| + 1) = |X|$ and $C \cap [C(S_0^2 - \{1\})] = \emptyset$, where $S_0 = S \cup \{1\}$.*

total perfect codes

Definition

A subset C of $V(G)$ is called a total perfect t-code in G if for every $u \in V(G)$ there is exactly one $v \in C$ such that $d(u, v) \leq t$.

A total perfect 1-code is called a total perfect code (Klostermeyer & Goldwasser 2006).



Total perfect codes in Q_4.

total perfect codes

Characterisations of the grid graphs that have total perfect codes were given by Klostermeyer and Goldwasser (2006).

total perfect codes

Characterisations of the grid graphs that have total perfect codes were given by Klostermeyer and Goldwasser (2006).

The direct product of any number of simple graphs has a total perfect code iff each factor has a total perfect code (Abay-Asmerom et al 2008).

total perfect codes

Characterisations of the grid graphs that have total perfect codes were given by Klostermeyer and Goldwasser (2006).

The direct product of any number of simple graphs has a total perfect code iff each factor has a total perfect code (Abay-Asmerom et al 2008).

The Cartesian product $C_m \Box C_n$ has a total perfect code iff both m and n are multiples of 4 (Dejter 2008).

total perfect codes in Cayley graphs

Definition

A graph H is called a pseudocover of a graph G if there exists a surjective mapping $p : V(H) \to V(G)$ such that $H[p^{-1}(v)]$ is a matching for all $v \in V(G)$ and deleting all such matching from H results in a cover of G with p the covering projection.

total perfect codes in Cayley graphs

Definition

A graph H is called a pseudocover of a graph G if there exists a surjective mapping $p : V(H) \to V(G)$ such that $H[p^{-1}(v)]$ is a matching for all $v \in V(G)$ and deleting all such matching from H results in a cover of G with p the covering projection.

Theorem

(Z 2011) Let C be a normal subset of a group X. Then the following are equivalent:

(a) *$C \subseteq X$ is a total perfect code of $\mathrm{Cay}(X, S)$;*

(b) *There exists a pseudocovering $p : \mathrm{Cay}(X, S) \to K_{|S|}$ such that Cs is a vertex-fibre of p for at least one element $s \in S$;*

(c) *C satisfies*

$$|C||S| = |X|, \;\; C \cap [C(S^2 - \{1\})] = \emptyset.$$

total perfect codes in Cayley graphs

Corollary

Let C be a normal subgroup of X. The following are equivalent:

(a) *C is a total perfect code of $\mathrm{Cay}(X, S)$;*

(b) *$\mathrm{Cay}(X, S)$ is a C-pseudocovering graph of $K_{|S|}$;*

(c) *C satisfies*

$$|X : C| = |S|, \quad C \cap S^2 = \{1\}.$$

total perfect codes in Cayley graphs

Corollary

Let C be a normal subgroup of X. The following are equivalent:

(a) *C is a total perfect code of $\mathrm{Cay}(X, S)$;*

(b) *$\mathrm{Cay}(X, S)$ is a C-pseudocovering graph of $K_{|S|}$;*

(c) *C satisfies*

$$|X : C| = |S|, \quad C \cap S^2 = \{1\}.$$

Definition

A pseudocovering $p : H \to G$ is called an A-pseudocovering if A is a subgroup of $\mathrm{Aut}(H)$ and there exists an isomorphism $h : G \to H_{\mathcal{P}_A}$ such that the quotient map $H \to H_{\mathcal{P}_A}$ is the composition of p and h, where $H_{\mathcal{P}_A}$ is the quotient graph of H with respect to the partition $\mathcal{P}_A$ of $V(H)$ into A-orbits.

Corollary

Let X be an abelian group. Then $C \subset X$ is a total perfect code in $\mathrm{Cay}(X, S)$ iff

$$|C||S| = |X| \text{ and } (C - C) \cap (S + S) = \{0\}.$$

In particular, a subgroup $C \leq X$ is a total perfect code iff $|C||S| = |X|$ and $C \cap (S + S) = \{0\}$.

an example

Example

The circulant $\mathrm{Cay}(\mathbb{Z}_n, S)$ has a total perfect code which is a subgroup of $\mathbb{Z}_n$ if and only if $|S| = m$ is a divisor of n and for any $s, s' \in S$, $s + s'$ is not a multiple of m unless $s + s' \equiv 0 \bmod n$.

In this case $C = \{[km] : k \in \mathbb{Z}\}$ is such a total perfect code.

If $n \geq 3$ is odd, then no $\mathrm{Cay}(\mathbb{Z}_n, S)$ has a total perfect code which is a subgroup of $\mathbb{Z}_n$.

$\mathrm{Cay}(\mathbb{Z}_{18}, \{[1], [9], [17]\})$ admits $C = \{[0], [3], [6], [9], [12], [15]\}$ as a total perfect code because $|S|$ divides 18 and the only common element of C and $S + S = \{[0], [2], [8], [10], [16]\}$ is $[0]$.

a family of Cayley graphs having total perfect codes

Theorem

(Z 2011) Suppose G is a connected graph such that $\mathrm{Aut}(G)$ contains a vertex-transitive abelian subgroup. Then G has total perfect codes iff its degree d is of the form $d = 2^n$ for some $n \geq 1$.

We give an explicit construction of total perfect codes in G when $d = 2^n$.

a family of Cayley graphs having total perfect codes

Theorem

(Z 2011) Suppose G is a connected graph such that $\mathrm{Aut}(G)$ contains a vertex-transitive abelian subgroup. Then G has total perfect codes iff its degree d is of the form $d = 2^n$ for some $n \geq 1$.

We give an explicit construction of total perfect codes in G when $d = 2^n$.

Corollary

(van Wee 1988) Q_d has a total perfect code iff $d = 2^n$ for some $n \geq 1$. Moreover, if $d = 2^n$, then for every $n \times d$ matrix M over $\mathrm{GF}(2)$ with rank n and pairwise distinct columns, the null space of M is a total perfect code.

a family of Cayley graphs having total perfect codes

Theorem

(Z 2011) Suppose G is a connected graph such that $\mathrm{Aut}(G)$ contains a vertex-transitive abelian subgroup. Then G has total perfect codes iff its degree d is of the form $d = 2^n$ for some $n \geq 1$.

We give an explicit construction of total perfect codes in G when $d = 2^n$.

Corollary

(van Wee 1988) Q_d has a total perfect code iff $d = 2^n$ for some $n \geq 1$. Moreover, if $d = 2^n$, then for every $n \times d$ matrix M over $\mathrm{GF}(2)$ with rank n and pairwise distinct columns, the null space of M is a total perfect code.

Conjecture

(I. Gorodezky 2007) If $d = 2^n$, $n \geq 3$, then every minimum dominating set of Q_d is a total perfect code in Q_d.

work in progress

- Existence and construction of total perfect codes in specific families of Cayley graphs

work in progress

- Existence and construction of total perfect codes in specific families of Cayley graphs
- Cartesian product of graphs

work in progress

- Existence and construction of total perfect codes in specific families of Cayley graphs
- Cartesian product of graphs
- Cartesian product of complete graphs (of non-uniform sizes)

work in progress

- Existence and construction of total perfect codes in specific families of Cayley graphs
- Cartesian product of graphs
- Cartesian product of complete graphs (of non-uniform sizes)
- Cartesian product of cycles

work in progress

- Existence and construction of total perfect codes in specific families of Cayley graphs
- Cartesian product of graphs
- Cartesian product of complete graphs (of non-uniform sizes)
- Cartesian product of cycles
- Direct product of cycles

two useful survey papers

J. H. van Lint, A survey of perfect codes, *Rocky Mountain J. Math.* 5 (1975), 199–224.

O. Heden, A survey of perfect codes, *Advances Math. Commun.* 2 (2008), 223–247.