



HAL
open science

Quelques problèmes combinatoires sur l'hypercube et les graphes de Hamming

Michel Mollard

► **To cite this version:**

Michel Mollard. Quelques problèmes combinatoires sur l'hypercube et les graphes de Hamming. Modélisation et simulation. Université Joseph-Fourier - Grenoble I, 1989. tel-00333335

HAL Id: tel-00333335

<https://theses.hal.science/tel-00333335>

Submitted on 23 Oct 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THESE

Présentée à

I'Université Joseph Fourier - Grenoble I

Pour obtenir le grade de
DOCTEUR ES SCIENCES

Michel Mollard

Quelques problèmes combinatoires
sur l'hypercube
et les graphes de Hamming.

Thèse soutenue le 9 Mai 1989 devant la comission d'examen:

C. BENZAKEN	Président
I. HAVEL	
J.M. LABORDE	
H.M. MULDER	Examineurs
C. PAYAN	
D. SOTTEAU	

Que Jean Marie Laborde soit remercié pour la générosité avec laquelle il a prodigué son temps à la direction de mes recherches.

Je remercie Dominique Sotteau, Ivan Havel et Henry Martyn Mulder qui ont bien voulu rapporter sur cette thèse et ont donc relus avec soin les épreuves.

Je remercie également Claude Benzaken d'avoir accepté d'en présider le jury et Charles Payan non seulement pour y participer mais aussi pour son aide constante et son amitié complice.

Merci de tout cœur, amis du LSDD, pour avoir supporté un savoyard, qui plus est chauvin, durant toutes ces années.

Note au lecteur

Les travaux correspondants à cette thèse ont donné lieu à un certain nombre d'articles parus, acceptés ou soumis dans des revues de Mathématiques discrètes ou d'Informatique. (À l'exception d'une annexe et d'un rapport de recherche contenant des résultats non publiés).

Ces articles constituent l'essentiel de cette thèse et sont regroupés en 4 chapitres. On trouvera à la tête de chaque chapitre une introduction qui pour chacun des problèmes étudiés fait le point sur la littérature classique; plaçant ainsi les résultats obtenus dans leur contexte sans revenir sur leur démonstration.

Table des Matières

Introduction

Chapitre 1: Les caractérisations de l'hypercube, des graphes associés et des graphes de Hamming

Introduction.

Two Characterizations of generalized hypercube.

Cycle-regular Graphs.

A Family of non regular distance monotone graphs.

Annexe.

Chapitre 2: Codes correcteurs d'erreurs parfaits non linéaires

Introduction.

A Generalised Parity function and its use in the construction of perfect codes.

Une nouvelle famille de 3-codes parfaits sur $GF(q)$.

Une généralisation de la fonction parité. Application à la construction de codes parfaits.

Chapitre 3: Problèmes divers sur l'hypercube

Introduction.

On shortest Cocycle Covers of Graphs.\$

Le nombre d'absorption du n-cube.

Un nouvel encadrement du Nombre de Cycles Hamiltoniens du n-cube.

Chapitre 4: Problèmes de valuations de types gracieux

Introduction.

On two conjectures about set-graceful graphs.£

Graceful Problems.¢

Elegant valuations and colorations.£

\$ en collaboration avec François Jaeger et Abdelkader Khelladi

£ en collaboration avec Charles Payan

¢ en collaboration avec Charles Payan et Sun Shi Xin

Introduction

Que ce soit dû à un regain actuel d'utilisation pratique (réseaux, architectures parallèles, codage), à son utilisation pour modéliser des problèmes ou simplement à l'intérêt de sa structure, l'hypercube, et plus généralement les graphes de Hamming (produits cartésiens de graphes complets) sont un objet d'étude particulièrement intéressant en combinatoire. Au fil des années l'essentiel de mon travail de recherche a concerné ces graphes et le sujet de cette thèse en est le reflet.

L'objet du premier chapitre est l'étude de leur place parmi les graphes. On donne pour ceci 2 caractérisations des graphes de Hamming et une nouvelle caractérisation de l'hypercube qui constitue un corollaire de résultats classiques. On introduit une nouvelle famille de graphes dont certains éléments maximaux sont les sous graphes induits par les couches centrales de l'hypercube. La notion de graphe distance monotone a été également utilisée pour caractériser les hypercubes; nous montrons qu'il existe de tels graphes non réguliers.

Dans les 2 chapitres suivants on s'intéresse à la recherche d'ensemble de sommets de l'hypercube ayant certaines propriétés. Ainsi le sujet du chapitre 2 est d'une part la construction de codes correcteurs d'erreurs parfaits binaires (autrement dit des absorbants parfaits de l'hypercube) et plus généralement sur $GF(q)$ et d'autre part l'introduction d'un nouveau type de produit de ces codes. D'autres types de propriétés de sommets sont étudiés dans le chapitre 3, notamment pour résoudre un problème de couverture de K_n par des cocycles.

L'objet du chapitre 4 est l'étude de plusieurs versions possibles de problèmes de recherche de valuations des sommets d'un graphe

induisant des valuations des arêtes ayant des propriétés du type de celles recherchées dans les valuations gracieuses; ce qui semble plus éloigné de l'hypercube. En fait certaines de ces valuations étant par des parties (valuations "set graceful") ou par des distances de Hamming (valuations "Hamming graceful") nous sommes toujours dans le même univers. Pour terminer on s'intéresse à l'existence de colorations optimales des arêtes de K_n telles qu' il existe une chaîne P_n multicoloriée.

Chapitre 1

Les caractérisations de l'hypercube,
des graphes associés et des
graphes de Hamming.

1 Les premières caractérisations de l'hypercube apparentées aux (0,2)-graphes

L'hypercube de dimension n , Q_n , quelquefois noté C_n (mais la première notation semble s'imposer), est le graphe dont l'ensemble des sommets est l'ensemble des mots binaires de longueur n et où deux sommets x et y sont adjacents ssi les mots correspondant diffèrent en une seule composante.

Désignons par $G \square G'$ le produit cartésien des graphes G et G' c'est à dire le graphe dont l'ensemble des sommets est $V(G) \times V(G')$ et où deux sommets (x,x') et (y,y') sont adjacents si et seulement si

$$x = y \text{ et } \{x',y'\} \in E'(G) \text{ ou}$$

$$x' = y' \text{ et } \{x,y\} \in E(G).$$

Il est clair que Q_n ($n \geq 1$) est isomorphe au graphe $K_2 \square K_2 \dots \square K_2$ (n fois).

La distance de Hamming entre deux mots binaires qui est le nombre de composantes dont ils diffèrent coïncide avec la distance au sens de la théorie des graphes $d(x,y)$ entre les deux sommets associés i.e. le nombre d'arêtes d'une plus courte chaîne les reliant. Nous noterons $\text{diam}(G)$ le diamètre d'un graphe G c'est à dire le maximum de $d(x,y)$ où x et y parcourent $V(G)$.

On peut attribuer à Alvarez [1] la première caractérisation de l'hypercube. En effet cet auteur a donné une caractérisation des graphes de couverture des treillis distributifs qui peut se prolonger en une caractérisation de l'hypercube.

Rappelons qu'un treillis (ensemble ordonné tel que deux éléments quelconques x,y possèdent une borne inférieure $x \wedge y$ et une borne supérieure $x \vee y$) est dit distributif s'il satisfait aux 2 règles de distributivité:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

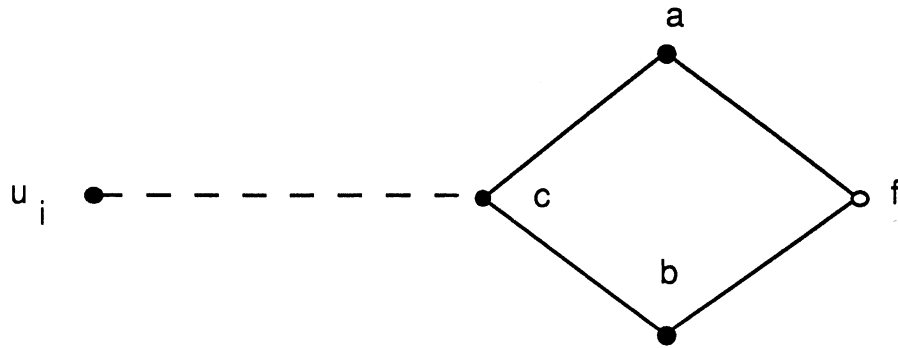
On dit que x couvre y dans un ensemble ordonné P si $x > y$ et si $x > z > y$ n'a lieu pour aucun z de P .

Le graphe de couverture d'un ensemble ordonné est le graphe non orienté correspondant à son diagramme de Hasse, c'est donc le graphe défini sur les éléments de l'ensemble où x et y sont adjacents si et ssi x couvre y ou y couvre x .

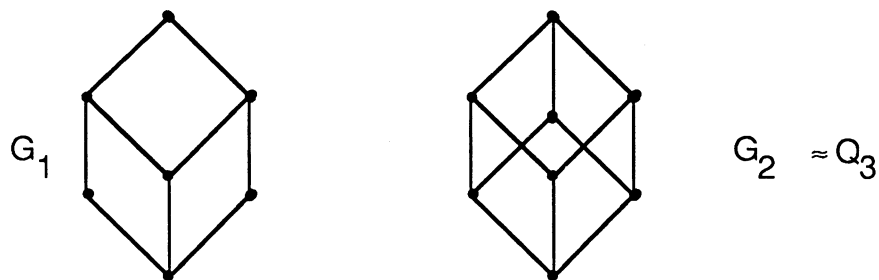
Théorème 1. (Alvarez[1])

Un graphe connexe $G = (V, E)$ est le graphe de couverture d'un treillis distributif si et seulement si G satisfait aux conditions suivantes:

- (1) G est biparti
- (2) Il existe 2 sommets u_1 et u_2 tels que $d(u_1, u_2) = \text{diam}(G)$ et tels que, pour $i=1$ et 2 et pour tous sommets a, b, c tels que $d(u_i, a) = d(u_i, b) = d(u_i, c) + 1$ (où $\{a, c\}$ et $\{b, c\}$ sont des arêtes de G), il existe un unique f adjacent à a et b tel que $d(u_i, f) = d(u_i, c) + 2$.



- (3) Si H_1 est un sous graphe de G isomorphe à G_1 alors il existe H_2 sous graphe de G isomorphe à G_2 tel que H_1 est un sous graphe de H_2 .

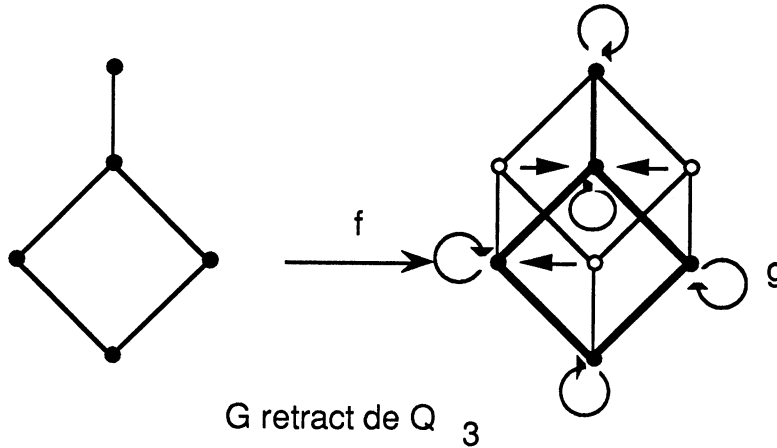


- (4) G ne contient pas de sous graphe isomorphe à $K_{2,3}$.

Définition.

Etant donnés deux graphes $G = (V(G), E(G))$ et $H = (V(H), E(H))$, un homomorphisme de G dans H est une application de $V(G)$ dans $V(H)$ telle

que, si u et v sont adjacents dans G leurs images le sont aussi dans H . Nous dirons que G est un "retract" de H ssi il existe 2 homomorphismes f de G dans H et g de H dans G tels que, pour tout sommet a de G , on ait $g(f(a)) = a$.



Les graphes de couverture d'un treillis distributif sont des sous graphes d'un hypercube (Duffus, Rival [5]) ; plus précisément ces auteurs ont démontré le résultat suivant.

Théorème 2.(Duffus, Rival [5])

Un graphe connexe $G = (V, E)$ est le graphe de couverture d'un treillis distributif de longueur n si et seulement si G est un retract d'un hypercube de dimension n et $\text{diam}(G) = n$.

Parmi ces retracts, on peut alors caractériser les hypercubes par une propriété supplémentaire et donc prolonger le résultat d'Alvarez en une caractérisation de l'hypercube. On obtient ainsi trivialement:

Théorème 3.

Un graphe connexe $G = (V, E)$ est un hypercube si et seulement si G satisfait aux conditions (1),(2),(3) et (4) du théorème 1 et vérifie

$$(5) |V| = 2^{\text{diam}(G)}.$$

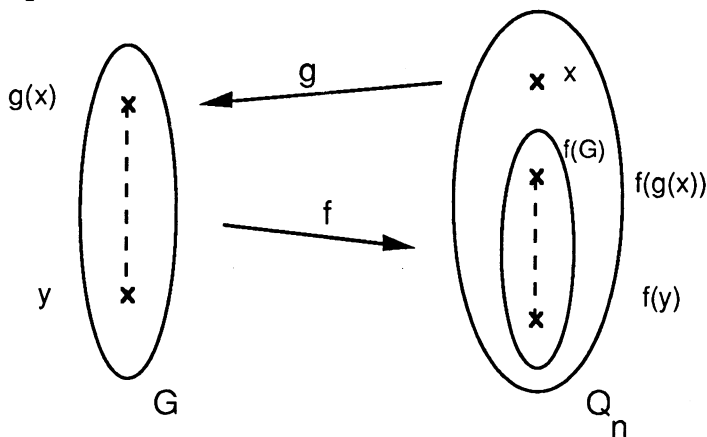
ou

Théorème 4.

Un graphe connexe $G = (V, E)$ est un hypercube si et seulement si G satisfait aux conditions (1),(2),(3) et (4) du théorème 1 et vérifie
 (5) $\forall x \in V(G) \exists y \in V(G)$ tel que $d(x, y) = \text{diam}(G)$.

En effet, soit G un retract de Q_n de diamètre n vérifiant (5). Prouvons que G est isomorphe à Q_n . Pour cela considérons les 2 homomorphismes f de G dans Q_n et g de Q_n dans G . Il est clair que l'image de G par f est un sous graphe de Q_n . Soit x un sommet de Q_n , montrons que $x \in f(G)$. Pour cela soit y un sommet de G tel que $d_G(g(x), y) = n$. Considérons une chaîne de longueur minimale $d_{Q_n}(x, f(y))$ entre x et $f(y)$. Cette chaîne est transformée par g en une chaîne de longueur au plus $d_{Q_n}(x, f(y))$ entre $g(x)$ et $g(f(y)) = y$. Puisque $d_G(g(x), y) = n$ on a alors $d_{Q_n}(x, f(y)) \geq n$ et donc cette distance est n .

De la même manière $d_G(g(x), y) = d_G(g(f(g(x))), g(f(y))) \leq d_{Q_n}(f(g(x)), f(y))$ et donc $d_{Q_n}(f(g(x)), f(y)) = n$. Or $d_{Q_n}(x, f(y)) = n$ et le sommet $f(y)$ de Q_n n'admet qu'un sommet à distance n ; donc on a $x = f(g(x))$ et de là $x \in f(G)$.



S. Foldes a donné la première caractérisation en tant que telle de l'hypercube:

Théorème 5. (S. Foldes [7])

Un graphe connexe $G = (V, E)$ est un hypercube si et seulement si G satisfait aux conditions suivantes:

- (1) G est biparti
- (2) pour toute paire x, y de sommets de G le nombre de plus courtes chaînes entre x et y est $d(x, y) !$.

Baptisons géodésiques les plus courtes chaînes entre deux sommets quelconques x et y et intervalle $I(x, y)$ l'ensemble des sommets appartenant aux géodésiques entre x et y (Mulder [14]). Par abus de langage on appellera également intervalle le sous graphe induit par $I(x, y)$.

Appelons graphe intervalle-régulier (Mulder [13]) un graphe connexe tel que pour toute paire de sommets u, v , le nombre de voisins de u dans $I(u, v)$ est exactement $d(u, v)$.

Comme S. Foldes puis H.M. Mulder l'ont remarqué le théorème 5 admet aussi la formulation suivante.

Théorème 6. (Foldes[7, Mulder[13]])

Un graphe connexe $G = (V, E)$ est un hypercube si et seulement si c'est un graphe intervalle-régulier biparti.

Pour toute paire de sommets u, v d'un graphe G et tout entier $k \leq d(u, v)$ soit $I_k(u, v) = \{w \in I(u, v) \mid d(u, w) = k\}$ et soit $w(u, v) = \max_{0 \leq k \leq d(u, v)} |I_k(u, v)|$.

D. Mac Fall est l'auteur du théorème suivant qui est lui aussi proche de la caractérisation de S. Foldes.

Théorème 7. (Mac Fall [12])

Un graphe connexe $G = (V, E)$ est un hypercube si et seulement si G satisfait aux conditions suivantes:

- (1) G est biparti

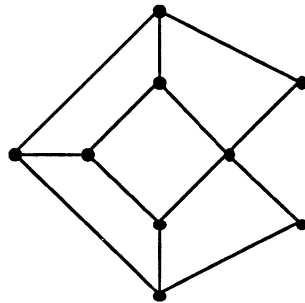
(2) pour toute paire x,y de sommets de G
 $w(x,y) = \binom{d(x,y)}{[d(x,y)/2]}$.

La caractérisation suivante est due à J.M. Laborde :

Théorème 8. (J.M. Laborde [10])

Un graphe connexe $G=(V,E)$ est un hypercube si et seulement si G satisfait aux conditions suivantes:

- (1) 2 sommets à distance 2 sont reliés par exactement 2 chemins de longueur 2
- (2) G ne contient pas de triangle
- (3) G ne contient pas de sous graphe isomorphe à



- (4) Il existe un entier n tel que $|V(G)| = 2^n$ et $|E(G)| = n2^{n-1}$.

Définition(H.M. Mulder [14]).

Un graphe simple connexe est un (0,2)-graphe si et seulement si deux sommets distincts ont exactement 2 voisins communs ou aucun.

Une propriété fondamentale de l'hypercube est d'être un (0,2)-graphe. Cette propriété sous-jacente dans le théorème 8 n'est pas sans relation non plus avec les conditions (2) des théorèmes 1,5 et 7.

Indépendamment J.M. Laborde, S.P. Rao Hebbare et H.M. Mulder l'ont utilisée pour obtenir la caractérisation suivante, aboutissement de ce type de

résultat .

Théorème 9. (J.M. Laborde, S.P. Rao Hebbare [11], H.M. Mulder [14])

Soit G un $(0,2)$ -graphe. Alors G est régulier et $|V(G)| \leq 2^n$, où n est le degré de G . De plus G est un hypercube si et seulement si $|V(G)| = 2^n$.

On peut en déduire [annexe 1] le résultat suivant :

Théorème 10.

Un graphe connexe $G = (V, E)$ est un hypercube si et seulement si, pour tout intervalle $I(u, v)$ et tout sommet x , il existe un sommet unique y dans $I(u, v)$ à distance maximale de x soit:

$$\forall u, \forall v, \forall x, \exists! y \in I(u, v) / \forall z \in I(u, v) \text{ tel que } z \neq y, d(x, z) < d(x, y) .$$

2 D'autres caractérisations de l'hypercube et les généralisations aux graphes de Hamming.

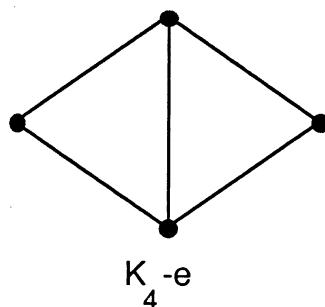
Les graphes de Hamming, produits cartésiens de graphes complets sont une généralisation naturelle de l'hypercube.

Définition.

Soient a_1, a_2, \dots, a_n des entiers positifs. Le graphe de Hamming H_{a_1, a_2, \dots, a_n} est le graphe dont les sommets sont les éléments du produit cartésien d'ensembles de a_i éléments et où deux sommets sont adjacents si et seulement si les vecteurs correspondants diffèrent en exactement une composante.

Une première caractérisation des graphes de Hamming a été obtenue par H.M. Mulder comme généralisation de la caractérisation de l'hypercube en temps que graphe intervalle régulier biparti (Théorème 6).

Les graphes de Hamming ne sont pas, en général, bipartis; cependant ils ne possèdent pas K_4-e comme sous graphe.



Théorème 11. (Mulder [13])

Un graphe connexe $G = (V, E)$ est un graphe de Hamming si et seulement si G n'admet pas $K_4 - e$ comme sous graphe, est intervalle régulier et vérifie:
 $\forall u, \forall v, \forall w, I(u, v) \cap I(v, w) = \{v\} \Rightarrow d(u, w) \geq \max\{d(u, v), d(v, w)\}.$

D'autres caractérisations de l'hypercube ont été étendues aux graphes de Hamming.

Définition.

Un graphe médian est un graphe tel que, pour tout triplet x,y,z de sommets, l'intersection des trois intervalles $I(x,y)$, $I(y,z)$ et $I(x,z)$ est réduite à un sommet.

Théorème 12 (Mulder [15]).

Un graphe connexe $G=(V,E)$ est un hypercube si et seulement si G est un graphe médian régulier.

Le même auteur a également caractérisé les hypercubes comme étant les graphes médians G tels que, pour tout sommet, il existe un sommet unique à distance égale au diamètre de G . Or H.J. Bandelt a prouvé [2] que les graphes médians sont exactement les retracts des hypercubes; cela permet indirectement de prouver le théorème 4 comme un corollaire de cette caractérisation.

H.M. Mulder [16] a introduit la notion de graphe quasi-médian pour obtenir un analogue au théorème 12 pour les graphes de Hamming.

Un ensemble de sommets W de cardinal au moins 2 est dit convexe si $I(u,v) \subset W$ pour tous u,v dans W . Un sous graphe induit par un ensemble de sommets convexe sera dit sous graphe convexe. On peut caractériser les hypercubes par l'ensemble $C(Q_n)$ de leurs sous graphes convexes propres non isomorphes.

Théorème 13. (Vanden Cruyce [17])

Pour tout graphe G tel que $C(G)=\{Q_1, Q_2, \dots, Q_{n-1}\}$ avec $n \geq 3$ on a $|V(G)| \geq 2^n$. De plus si $|V(G)| = 2^n$ alors G est isomorphe à Q_n .

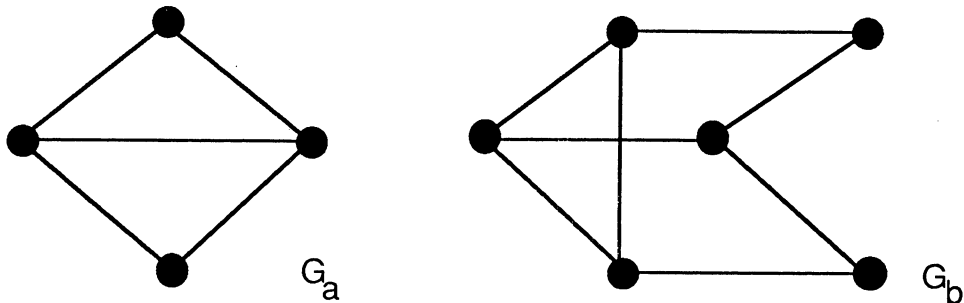
Ce résultat a été étendu aux graphes de Hamming:

Théorème 14. (Egawa [6])

Soient n_1, n_2, \dots, n_r des entiers ($r \geq 2$) tels que $n_i > 1$ pour tout i et soit G un graphe tel que l'ensemble de ses sous graphes convexes propres non isomorphes $C(G)$ est égal à $C(H_{n_1, n_2, \dots, n_r})$. Si il existe i avec $n_i > 2$ ou si $r > 2$ alors $|V(G)| \geq n_1 n_2 \dots n_r$. De plus si $|V(G)| = n_1 n_2 \dots n_r$ alors G est isomorphe à H_{n_1, n_2, \dots, n_r} .

La caractérisation de Q_n comme $(0,2)$ -graphe d'ordre maximum relativement au degré est certainement le plus beau des 10 premiers résultats. Il était donc particulièrement intéressant de l'étendre aux graphes de Hamming.

Il est clair qu'un graphe de Hamming n'est pas, en général un $(0,2)$ -graphe. Cependant les sommets à distance 2 possèdent exactement deux voisins communs. En effet le graphe étant sommet transitif posons $u = (0, 0, \dots, 0)$ et $v = (a_1, a_2, 0, \dots, 0)$ avec $a_1, a_2 \neq 0$. Il existe alors deux uniques voisins communs de u et v , $(a_1, 0, \dots, 0)$ et $(0, a_2, 0, \dots, 0)$. Cette condition n'est pas suffisante pour assurer la régularité. Cependant, si on rajoute le fait que G ne possède pas G_a ou G_b (voire figure ci-dessous) comme sous graphe, G est alors régulier et de plus le nombre $N_i(x)$ de cliques maximale à i éléments K_i contenant un sommet donné x est indépendant de x .



On obtient alors:

Théorème 15.

Soit G un graphe simple connexe ne contenant pas G_a et G_b comme sous graphe et tel que deux sommets quelconques à distance 2 possèdent exactement deux voisins communs on a

$$|V(G)| \leq \prod_{i=2}^p i^{N_i} \text{ et } \text{diam } G \leq \sum_{i=2}^p N_i$$

de plus

$$|V(G)| = \prod_{i=2}^p i^{N_i} \text{ si et seulement si } G \text{ est un graphe de Hamming.}$$

3 Graphes distance monotones.

Un graphe est dit intervalle monotone si tous ses intervalles sont convexes. La notion de graphe distance monotone introduite par G. Burosh, I. Havel et J.M. Laborde [3] a permis à ces auteurs de donner une nouvelle caractérisation de l'hypercube.

Définition.

Un graphe connexe est dit distance monotone si, pour tout intervalle $I(u,v)$ et tout sommet w hors de l'intervalle, il existe un sommet w' dans $I(u,v)$ tel que $d(w,w') > d(u,v)$.

Il est clair qu'un intervalle $I(u,v)$ est tel que, pour tous w, w' dans l'intervalle, $d(w,w') \leq d(u,v)$. Dans un graphe distance monotone cette propriété est donc caractéristique des sommets de l'intervalle.

Théorème 16. (Burosh, Havel et Laborde[3])

Soit G un graphe intervalle monotone et distance monotone de degré minimum $\delta \geq 3$ alors G est un hypercube.

Pour étendre ce type de résultat aux graphes de Hamming introduisons plusieurs notions:

Définitions.

Le quasi intervalle $I'(u,v)$ défini par 2 sommets u et v d'un graphe G est l'ensemble des sommets w tel qu'il n'existe pas de sommet distinct de w appartenant à la fois à une géodésique entre u et w et à une entre v et w . Comme pour les intervalles, par abus de langage, on appellera également quasi intervalle le sous graphe induit par un quasi intervalle.

Il est clair que $I(u,v) \subset I'(u,v)$; d'autre part dans un graphe de Hamming les intervalles sont des hypercubes et les quasi intervalles sont

des graphes de Hamming (comme dans un hypercube les intervalles sont des hypercubes).

Nous dirons qu'un graphe est quasi intervalle monotone si tous ses quasi intervalles $I(u,v)$ vérifient:

$$\forall x,y \in I(u,v), I(x,y) \subset I(u,v).$$

De même un graphe sera dit quasi distance monotone si tous ses quasi intervalles $I(u,v)$ vérifient:

$$w \in v(G) - I(u,v) \Rightarrow \exists w' \in I(u,v) \text{ tel que } d(w,w') > d(u,v).$$

Il est clair que les graphes de Hamming sont à la fois quasi intervalle monotones et quasi distance monotones.

Théorème 17.

Soit G un graphe connexe quasi intervalle monotone et quasi distance monotone contenant $K_{1,3}$ comme sous graphe, alors G est un graphe de Hamming.

Le fait de contenir $K_{1,3}$ comme sous graphe est une condition un peu plus forte que celle d'être de degré minimum au moins 3, utilisée dans le théorème 16.

En fait la démonstration de cette caractérisation revient à la considérer comme une conséquence du théorème 15.

Une question intéressante concernant les graphes distance monotones est celle de leur régularité. Nous avons vu que les $(0,2)$ -graphes sont réguliers. En est il de même pour les graphes distances monotones?

Conjecture. [3], [8]

Tout graphe distance monotone de degré minimum au moins 3 est régulier.

Nous prouvons que cette conjecture est fautive en exhibant une famille de contre exemples:

Proposition.

Pour $p \geq 4$ et $q \in \{ \frac{p(p+1)}{2}, \dots, 2^p - 1 \}$ il existe un graphe distance monotone avec des sommets de degré 2^p et des sommets de degré q .

Tous ces contre-exemples sont des graphes distance monotones de diamètre 4. En fait il existe une représentation matricielle de ces graphes (Havel, Laborde[8]). On peut alors formuler le problème de la recherche d'un graphe distance monotone non régulier de degré 4 comme celui de la recherche d'une matrice m par n binaire avec $m \neq n$, $M = (m_{ij})$, vérifiant:

(1) M possède au moins 4 lignes et 4 colonnes

(2) pour tout triplet d'indices distincts de lignes i, j, k il existe 4 colonnes a, b, c, d telles que:

$$m_{ia} = m_{ja} \neq m_{ka}$$

$$m_{ib} \neq m_{jb} = m_{kb}$$

$$m_{ic} \neq m_{jc} \neq m_{kc}$$

$$m_{id} = m_{jd} = m_{kd}$$

(3) pour tout triplet d'indices distincts de colonnes a, b, c il existe 4 lignes i, j, k, l telles que:

$$m_{ia} = m_{ib} \neq m_{ic}$$

$$m_{ja} \neq m_{jb} = m_{jc}$$

$$m_{ka} \neq m_{kb} \neq m_{kc}$$

$$m_{la} = m_{lb} = m_{lc}$$

Nous donnons la construction de telles matrices, comme par exemple la suivante:

0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1
0	0	1	1	1	1	0	0
0	1	0	1	1	0	1	0
0	1	1	0	0	1	1	0
0	1	1	0	1	0	0	1

Exemple:

Pour $i=1, j=2$ et $k=3$, $a=2, b=5, c=3$ et $d=1$ est solution

Pour $a=6, b=7$ et $c=8$, $i=6, j=4, k=5$ et $l=1$ est solution.

4 Graphes cycles-réguliers.

Pour définir cette notion il est nécessaire de fixer avec précision un certain nombre de termes.

Une chaîne de longueur l sera pour nous une suite de sommets u_0, u_1, \dots, u_l telle que 2 sommets consécutifs sont adjacents et les sommets sont tous distincts sauf peut être u_0 et u_l .

Un cycle élémentaire de G de longueur m est un sous graphe partiel de G sur m sommets distincts $\{v_1, v_2, \dots, v_m\}$, connexe et régulier de degré 2.

Nous dirons qu'une chaîne u_0, u_1, \dots, u_l appartient à un cycle élémentaire sur $\{v_1, v_2, \dots, v_m\}$ si $\{u_0, u_1, \dots, u_l\} \subset \{v_1, v_2, \dots, v_m\}$ et si la chaîne est un sous graphe partiel du cycle.

Les (0,2)-graphes définis par H.M. Mulder [14] sont des graphes tels que toute chaîne de longueur 2 appartient à exactement un cycle de longueur 4. Ces graphes sont réguliers. On peut s'intéresser à trouver une notion plus générale conservant la régularité et étudier les familles de graphes ainsi obtenues.

Définitions.

Soient l et λ deux entiers, $l \geq 2$ et $\lambda \geq 1$, et G un graphe connexe simple de maille au moins l .

Nous dirons que G est un graphe $[l, \lambda]$ -cycles-régulier s'il existe un ensemble non vide C de cycles élémentaires tel que toute chaîne de G de longueur l appartient à exactement λ cycles de C .

Dans le cas particulier où C est l'ensemble des cycles élémentaires d'une certaine longueur $m \geq 2l$, nous dirons que G est un graphe $[l, \lambda, m]$ -cycles-régulier.

Les $(0,2)$ -graphes sont des graphes $[2,1,4]$ -cycles réguliers. Comme les $(0,2)$ -graphes, les graphes $[l, \lambda]$ -cycles-réguliers ont des propriétés de régularité.

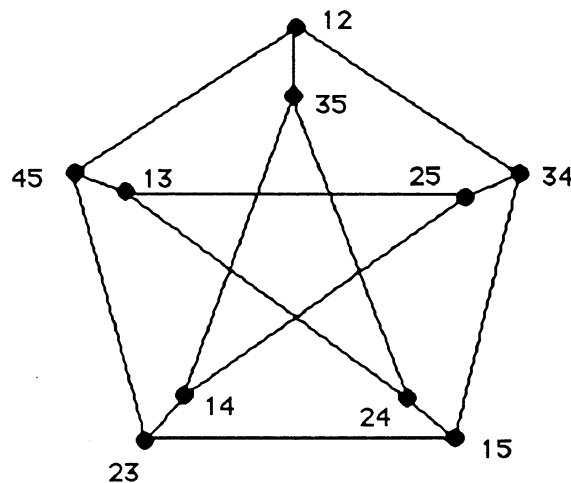
Théorème 18.

Si G est un graphe $[l, \lambda]$ -cycle-régulier de degré minimum $\delta > 2$, alors G est régulier ou est biparti et est tel que dans chacun des deux stables les sommets sont de même degré.

Si le degré minimum de G est 2 alors G est une subdivision d'un autre graphe cycle régulier G' dont le degré minimum est au moins 3.

Parmi les exemples de graphes $[3,1,6]$ -cycles-réguliers notons deux familles particulièrement intéressantes:

Pour tout entier $n \geq 2$ le graphe O_n , "odd graph" d'ordre n (Kowalewski [9]), est le graphe dont les sommets sont les parties à $n-1$ éléments de $N = \{1, 2, \dots, 2n-1\}$ et où 2 sommets sont adjacents si les parties correspondantes sont disjointes. O_3 est par exemple le graphe de Petersen.

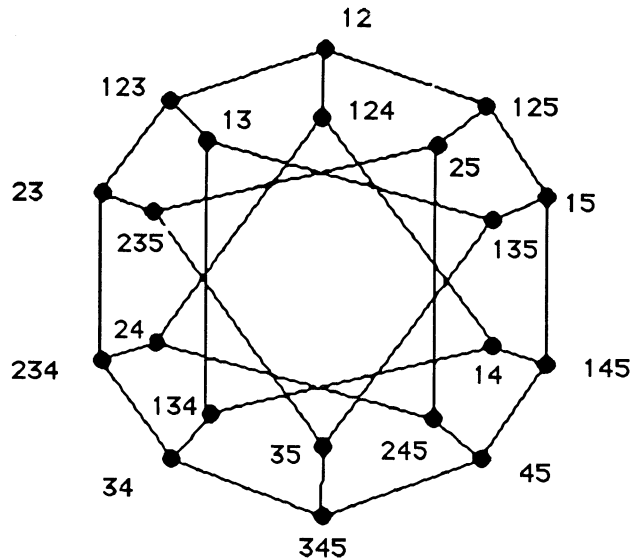


Pour tout $n > 2$, O_n est un graphe $[3,1,6]$ -cycle régulier de degré n et d'ordre $\binom{2n-1}{n-1}$.

Le second exemple est fourni par le sous graphe induit par 2 couches consécutives quelconques Γ_{p-1} et Γ_p d'un hypercube Q_n (une telle décomposition en couches de $V(Q_n)$ est obtenue en choisissant un sommet x et en posant pour $i=0,1,\dots,n$ $\Gamma_i = \{ y \in V(Q_n) / d(x,y)=i \}$).

Ce graphe est $[3,1,6]$ -cycle régulier et biparti, les sommets de Γ_{p-1} étant de degré $n-p+1$, ceux de Γ_p de degré p .

Un cas particulier intéressant est celui de H_p sous graphe induit par les couches centrales Γ_{p-1} et Γ_p d'un hypercube Q_{2p-1} . Ces graphes sont réguliers de degré p . Pour $p = 3$, par exemple, on obtient le graphe de Desargues H_3 .



De même que les hypercubes étaient d'ordre maximum pour un degré donné parmi les $(0,2)$ -graphes nous montrons que les graphes H_p sont maximaux parmi les graphes $[3,1,6]$ -cycles-réguliers.

Théorème 19.

Soit G un graphe $[3,1,6]$ -cycles-régulier de degré maximum n alors $|V(G)| \leq \binom{2n}{n}$ avec égalité si et seulement si G est H_n .

REFERENCES

- [1] L.R. Alvarez, Undirected graphs as graphs of modular lattices, *Canad.J.Math.*17(1965) 923-932.
- [2] H.J. Bandelt, Retracts of Hypercubes, *J. of Graph Theory* 8 (1984) 501-510.
- [3] G. Burosh, I. Havel, J.M. Laborde, DM-graphs and a new characterization of hypercubes, to appear in *Discrete Mathematics*.
- [4] P.V. Ceccherini, A q-analogous of the characterization of hypercubes as graphs , *J. of Geometry* 22 (1984) 57-74.
- [5] D. Duffus, I. Rival, Graphs orientable as distributive lattices, *Proc. Amer. Soc.* 88 (1983) 197-200.
- [6] Y. Egawa, Characterization of the cartesian product of complete graphs by convex subgraphs, *Discrete Mathematics* 58 (1986) 307-309.
- [7] S. Foldes, A Characterization of Hypercubes, *Discrete Mathematics*17 (1977) 155-159.
- [8] I. Havel,J.M. Laborde, On Distance Monotone Graphs, *Colloquia Mathematica Societatis Janos Bolyai* 52 (1987) 557-561.
- [9] A. Kowalewski, Topologische Deutung von Buntordnungsproblemen, *Sitzungsber. Akad. Wiss. Wien (Abdt IIa)* 126 (1917) 963-1007.
- [10] J.M. Laborde, Caractérisation locale du graphe du n-cube, in C. Benzaken(ed): *Actes du colloque algèbre appliquée et combinatoire*, Grenoble (1978) 198-200.
- [11] J.M. Laborde, S.P. Rao Hebbare, Another characterization of hypercubes, *Discrete Mathematics* 39 (1982) 161-166.
- [12] D. McFall, Characterizing Hypercubes, *Ann. Discrete Mathematics* 9 (1980) 237-241.
- [13] H.M. Mulder, Interval-regular graphs, *Discrete Mathematics* 41 (1982) 253-269.

- [14] H.M. Mulder, $(0,\lambda)$ graphs and n-cubes, *Discrete Mathematics* 28 (1979) 179-188.
- [15] H.M. Mulder, n-Cubes and Median Graphs, *J. of Graph Theory* 4 (1980) 107-110.
- [16] H.M. Mulder, The Interval Function of a Graph, *Mathematical Centre Tracts* 132, Amsterdam 1980.
- [17] P. Vanden Cruyce, A Characterization of the n-Cube by Convex Subgraphs, *Discrete Mathematics* 41 (1982) 109-110.

Two Characterizations of generalized hypercube

Michel Mollard
LSD(IMAG) BP 68
38041 Grenoble CEDEX , France

Summary We give two new characterizations of the Hamming graph, which is a natural generalization of the hypercube. The first one is the analogous of the characterization of the hypercube as $(O,2)$ -graph of maximal order; the second introduces the notion of quasi-interval.

0. A short introduction and some definitions.

Various characterizations of the hypercube Q_n have been recently given . For a survey on this subject one may consult [1] . The hypercube can be generalized in two different ways.

The first one, more geometric, is to consider graphs of the lattice of the subspaces of a graphic space of finite dimension and of finite order q . A characterization of these graphs is given by P.V.Ceccherini [2] in terms of the number of geodesics analogous to the characterization of the hypercube by S.Foldes [3].

The second kind of generalization arises naturally in studying words over composite alphabets:

Definition.

Let a_1, \dots, a_n be positive integers. The Hamming graph $H_{a_1 \dots a_n}$ is the graph with vertex-set $\prod_{i=1}^n \{0, 1, \dots, a_i - 1\}$, in which two vertices are joined by an edge if and only if the corresponding vectors differ in exactly one coordinate.

The Hamming distance of two vectors is the number of coordinates in which they differ. This value is precisely the distance (in the usual graph sense) between the associated vertices of the Hamming graph.

Then Q_n is the Hamming graph $H_{a_1 \dots a_n}$ with $a_1 = a_2 = \dots = a_n = 2$ and $H_{a_1 \dots a_n}$ is $H_{a_1} \square H_{a_2} \square \dots \square H_{a_n} = K_{a_1} \square K_{a_2} \square \dots \square K_{a_n}$ where \square denote the Cartesian product of graphs.

H.M.Mulder [4] has given a characterization of Hamming graphs as interval-regular graphs with some additional properties ; this is the analogous of his characterization of hypercubes as bipartite interval-regular graphs [4] .

An other extension to Hamming graph of a characterization of hypercubes is the characterization of Hamming graphs by convex subgraphs [8] .

In this paper Theorem 1 gives a characterization of Hamming graphs analogous to the characterization of hypercubes as $(0,2)$ graphs of maximal order [5] , [6] .

Theorem 2 contains an other characterization of Hamming graphs related to the recent study [7] of distance monotone graphs which gives a new characterization of the hypercube.

Though Hamming graphs are vertex-transitive, we specify the vertex 0 corresponding to the zero vector $\underline{0}$ and call the weight of a vector its distance to 0, i .e. the number of its non-zero coordinates and the "support" of the vertex the subset of $\{1, \dots, n\}$ corresponding to these coordinates.

We denote by $d(u,v)$ the length of a minimal path between u and v and by $\text{Diam}(G) = \max_{u,v} d(u,v)$ the diameter of G .

1.The first characterization.

Let $\Gamma(x)$ be the set of vertices of G adjacent to x and $N_i(x)$ be the number of maximal i -cliques K_i of G which contain x .

Theorem 1

Let G be a simple connected graph such that :

- (i) G does not contain G_a or G_b as induced subgraphs (figure 1).

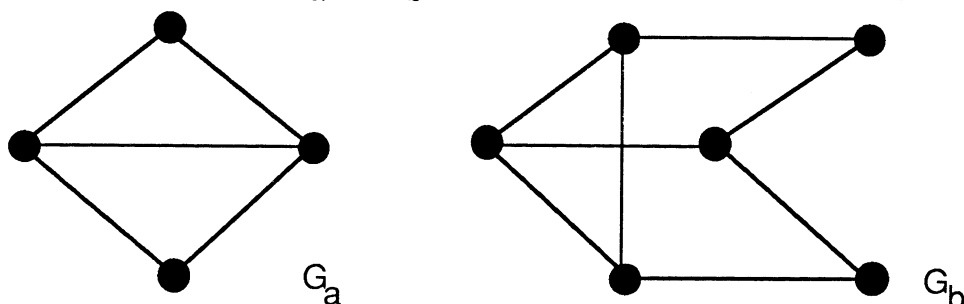


Figure 1

(ii) Two non-adjacent vertices in G have exactly 2 common neighbours or none at all.

Then, for all i , the number $N_i(x)$ is independent of the vertex x of G .

Furthermore if p is the maximum integer such that N_p is non zero, then

$$(1) |V(G)| \leq \prod_{i=2}^p i N_i \quad \text{and} \quad \text{diam}(G) \leq \sum_{i=2}^p N_i,$$

$$(2) G \text{ is a Hamming graph if and only if } |V(G)| = \prod_{i=2}^p i N_i.$$

All this section is a demonstration of Theorem 1

Proposition 1.1.

If u and v are two adjacent vertices then for all integer i $N_i(u) = N_i(v)$.

Proof

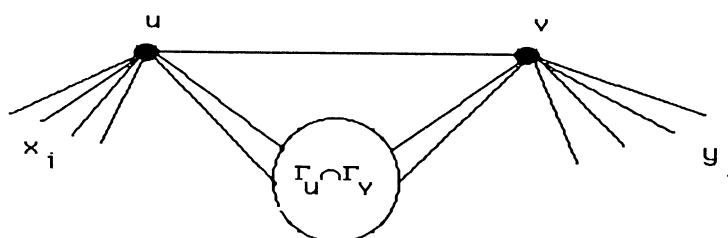


Figure 2

Let x_i ($i \in I$) be the vertices of G adjacent to u , distinct from v and not adjacent to v ; and let y_j ($j \in J$) be the vertices of G adjacent to v , distinct from u and not adjacent to u (figure 2).

For all x_i there is, by property (ii), a unique vertex adjacent to both x_i and v , and by (i) it is an y_j for some j . The mapping $f(i) = j$ is a one-to-one correspondence between I and J because if $f(i) = f(k)$ then x_i, x_k and v are common neighbours of the non-adjacent vertices u and $y_{f(i)}$ (figure 3).

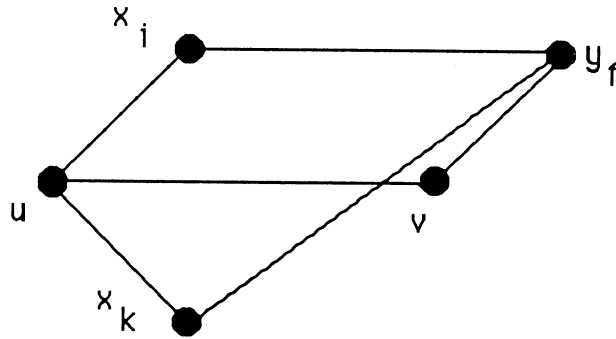


Figure 3

We can extend f to a one-to-one correspondence h between vertices of $\Gamma(u)$ and $\Gamma(v)$, taking $h(x) = x$ for x adjacent to u and v , $h(u) = v$, $h(v) = u$, and $h(x_i) = y_{f(i)}$ for $i \in I$. We have to prove now that h preserve the membership to maximal cliques of the same order ; in other words that x and u belongs to an i -clique if and only if $h(x)$ and v belong to an i -clique.

If x and v are adjacent, then $h(x) = x$ and x, u, v are in the same maximal clique. Indeed x, u and v are mutually adjacent and if $z \in \Gamma(u) \cap \Gamma(x)$, then $z \in \Gamma(v)$, otherwise G should contain G_a as induced subgraph (figure 4).

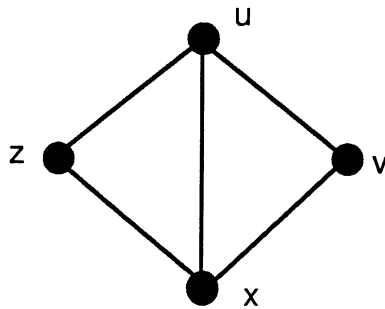


Figure 4

If x and v are not adjacent, then let $w \in \Gamma(u) \cap \Gamma(x)$. Now $h(x)$ and $h(w)$ are adjacent, otherwise :

- if $w \notin \Gamma(v)$, then G must contain G_b as induced subgraph (figure 5);

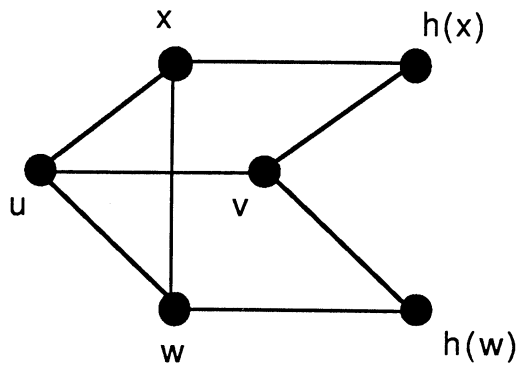


Figure 5

- if $w \in \Gamma(v)$, then G must contain G_a as induced subgraph (figure 6) and this case ends the proof. \square

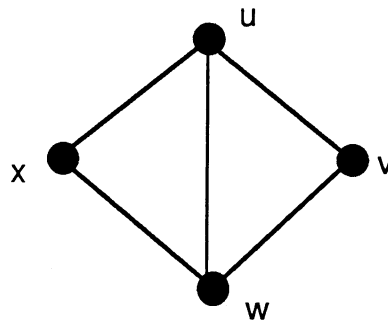


Figure 6

By connexity Proposition 1.1 implies that $N_i(x)$ is independent of the vertex x of G .

Let 0 be a fixed vertex of G such that there is some w in G with $d(0,w) = \text{Diam}(G)$, and denote by $A_{\alpha_2 \dots \alpha_p}$ ($0 \leq \alpha_i \leq N_i$) the set of vertices x of G such that there is a geodesic (shortest path) between 0 and x with α_i ($2 \leq i \leq p$) edges belonging to a maximal i -clique. Let C_j ($j = 0, \dots, \text{Diam}(G)$) be the set of vertices x of G such that $d(0,x) = j$. Trivially C_j is the union (not necessarily disjoint) of the $A_{\alpha_2 \dots \alpha_p}$ with $\sum_{i=2}^p \alpha_i = j$.

Proposition 1.2.

Let x be a vertex of C_j in $A_{\alpha_2 \dots \alpha_p}$. Then, for all i , there are at least α_i non-adjacent vertices z in $\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ such that $\{x,z\}$ belongs to a maximal i -clique.

Proof

If $j=0$ or 1 , the property is trivially true. Assume it for $j \geq 1$ and let x be a vertex of G in $A_{\alpha_2 \dots \alpha_p}$ with $\sum_{i=2}^p \alpha_i = j+1$. Let y be adjacent to x and on a geodesic between v and x with α_i edges belonging to a maximal i -clique for all i ($2 \leq i \leq p$). The edge $\{x,y\}$ belongs to a maximal clique and therefore there is an integer k ($2 \leq k \leq p$) with y in $\Gamma(x) \cap A_{\alpha'_2 \dots \alpha'_k \dots \alpha'_p}$, $\alpha'_k = \alpha_k - 1$ and $\alpha'_i = \alpha_i$, for $i \neq k$. By induction hypothesis, there are at least α'_i non-adjacent vertices $y_1 \dots y_{\alpha'_i}$ in $\Gamma(y) \cap A_{\alpha''_2 \dots \alpha''_i \dots \alpha''_p}$ with $\alpha''_i = \alpha'_i - 1$ and $\alpha''_j = \alpha'_j$ for $j \neq i$.

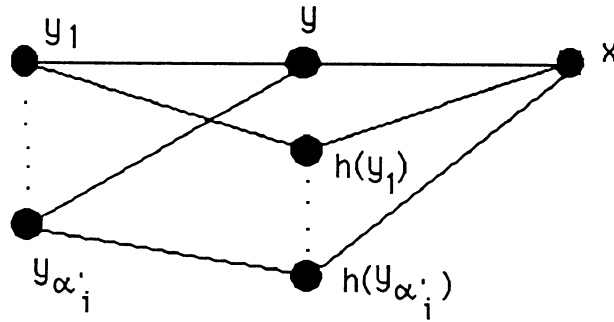


Figure 7

As in the proof of Proposition 1.1, if h is the mapping between $\Gamma(y)$ and $\Gamma(x)$ (figure 7), and if for all j , h_j is the mapping between $\Gamma(y)$ and $\Gamma(y_j)$, then h_j preserves the membership to maximal k -cliques. Now $h_j(y) = y_j$ and $h_j(x) = h(y_j)$, the edge $\{x,y\}$ belongs to a maximal k -clique whence $\{h(y_j), y_j\}$ also, and $h(y_j)$ belongs to $A_{\alpha''_2 \dots \alpha''_{k+1} \dots \alpha''_p}$. The vertices $h(y_1), \dots, h(y_{\alpha'_i})$ are not adjacent because $y_1, \dots, y_{\alpha'_i}$ are not and there is no G_b as induced subgraph in G . The vertex y is not adjacent to some $h(y_j)$ because there is no G_a and y_j cannot be adjacent to x .

The vertices $h(y_1), \dots, h(y_{\alpha'_i})$ are α_i not adjacent vertices in $\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ if $k \neq i$. And $y, h(y_1), \dots, h(y_{\alpha'_i})$ are such if $k = i$. Thus Proposition 1.2 is proved. \square

Proposition 1.3.

$$|A_{\alpha_2 \dots \alpha_p}| \leq \prod_{i=2}^p \binom{N_i}{\alpha_i} (i-1)^{\alpha_i}.$$

proof

This is true for $\sum_{i=2}^p \alpha_i = 0$ or 1 . Assume it for $j \geq 1$ and choose some integer i such

that $\alpha_i \neq 0$.

A vertex x in $A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ belongs to exactly N_i maximal i -clique, Thus by proposition 1.2 there are at most $(N_i - (\alpha_{i-1})) (i-1)$ vertices z in $\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ such that $\{x, z\}$ belongs to a maximal i -clique. The number of edges between some vertex in $A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ and some vertex in $A_{\alpha_2 \dots \alpha_i \dots \alpha_p}$ and belonging to a maximal i -clique is therefore at most $|A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}| (N_i - (\alpha_{i-1})) (i-1)$ and, by Proposition 1.2 at least $\alpha_i |A_{\alpha_2 \dots \alpha_i \dots \alpha_p}|$, which proves the proposition 1.3. \square

Note that $|V(G)| \leq \sum_{\alpha_2 \dots \alpha_p} |A_{\alpha_2 \dots \alpha_p}| \leq \sum_{\alpha_2 \dots \alpha_p} \left(\prod_{i=2}^p \binom{N_i}{\alpha_i} (i-1) \alpha_i \right)$ and this last sum is $\prod_{i=2}^p i N_i$.

If G is a Hamming graph, G satisfies (i) and (ii) and is $H = (K_2)^{N_2} \square (K_3)^{N_3} \square \dots \square (K_p)^{N_p}$ and therefore $|V(G)| = \prod_{i=2}^p i N_i$ and $\text{diam}(G) = \sum_{i=2}^p N_i$.

Assume now that G is a simple connected graph satisfying (i) and (ii) of order $|V(G)| = \prod_{i=2}^p i N_i$. Then for all $\alpha_2 \dots \alpha_p$ we have $|A_{\alpha_2 \dots \alpha_p}| = \prod_{i=2}^p \binom{N_i}{\alpha_i} (i-1) \alpha_i$ and all these sets are disjoint. Furthermore the number of edges between $A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ and $A_{\alpha_2 \dots \alpha_i \dots \alpha_p}$ belonging to a maximal i -clique is exactly $\alpha_i |A_{\alpha_2 \dots \alpha_i \dots \alpha_p}| = (N_i - (\alpha_{i-1})) (i-1) (|A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}|)$. Therefore every vertex of $A_{\alpha_2 \dots \alpha_i \dots \alpha_p}$ has exactly α_i neighbours in $A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ and exactly $(N_i - \alpha_i)(i-1)$ neighbours in $A_{\alpha_2 \dots \alpha_{i+1} \dots \alpha_p}$ and the corresponding edges belongs to maximal i -cliques.

We have an isomorphism between the levels C_0, C_1 of G and of $H = (K_2)^{N_2} \square (K_3)^{N_3} \square \dots \square (K_p)^{N_p}$. Assume we have such an isomorphism θ between the q -bottom levels C_0, \dots, C_q of G and of H , we are going to show how we can extend θ to an isomorphism between the $q+1$ bottom levels of G and of H .

Proposition 1.4

Let x and y two non-adjacent vertices of C_q . They have a common neighbour in C_{q-1} if and only if they have one in C_{q+1} .

proof

If x and y have a common neighbour z in C_{q-1} , then they have an other common neighbour. It cannot be in C_{q-1} or in C_q because of the isomorphism between the q -bottom levels of G and of H . Therefore it is in C_{q+1} .

Reciprocally for a fixed x in C_q (exactly in $A_{\alpha_2 \dots \alpha_i \dots \alpha_p}$ with $\sum_{i=2}^p \alpha_i = q$) the number of sets $\{y,z\}$ with y in C_q non-adjacent to x and z common neighbour of x and y in C_{q-1} is exactly $\sum_{i=2}^p \alpha_i \left(\sum_{k=2}^p (k-1)(N_k - \alpha_k) \right)$. Similarly the number of sets $\{y,t\}$ with y in C_q non-adjacent to x and t and a common neighbour of x and y in C_{q+1} is exactly $\sum_{i=2}^p \left((i-1)(N_i - \alpha_i) \sum_{k=2}^p \alpha_k \right)$. These two numbers are equals ; then by the first part of the proof, if for a fixed y a $\{y,z\}$ exists then exactly one $\{y,t\}$ also exists. Therefore by the second part the number of $\{y,t\}$ is exactly the number of $\{y,z\}$. \square

Proposition 1.5

If x and y are two adjacent vertices of C_{q+1} , they have a common neighbour in C_q .

proof

Let x be a vertex of C_{q+1} (exactly in $A_{\alpha_2 \dots \alpha_i \dots \alpha_p}$ with $\sum_{i=2}^p \alpha_i = q+1$). The number of vertices adjacent to x in C_{q+1} is $\sum_{i=2}^p \alpha_i (i-2)$ and this is exactly the number necessary to complete the $\sum_{i=2}^p \alpha_i$ maximal cliques encountering C_q and containing x . \square

Now let x be a vertex of C_{q+1} then x is adjacent to $q+1$ vertices x_0, \dots, x_q in C_q . For all distinct r, t in $\{0, \dots, q\}$ the vertices x_r and x_t have a common neighbour in C_{q-1} and are not adjacent. Therefore the supports of vectors $\theta(x_k)$ are all of cardinality q and the cardinality of their intersections two by two is $q-1$. Hence these supports satisfy $|\bigcup_k S(\theta(x_k))| = q+1$. But $\theta(x_r)$ and $\theta(x_t)$ are equal on $S(\theta(x_r)) \cap S(\theta(x_t))$. Then there exists a vector $w(x)$ of weight $q+1$ of support $|\bigcup_k S(\theta(x_k))|$, of which the subvectors of weight q are the $\theta(x_k)$ $k \in \{0, \dots, q\}$. We can extend θ to C_{q+1} setting for all x in C_{q+1} $\theta(x) = w(x)$.

We prove now that θ is an isomorphism. First notice that θ is a one to one correspondence because by construction we have only to consider the case x and y in C_{q+1} with $\theta(x) = \theta(y)$. Then the neighbours of x in C_q are the neighbours of y and two such neighbours cannot have two common neighbours in C_{q+1} .

Let x and y be two vertices of the bottom $q+1$ levels of G . By construction of θ , if x or y are not in C_{q+1} , then $\theta(x)$ and $\theta(y)$ are adjacent if and only if x, y are. Assume that x and y are in C_{q+1} .

If $d(\theta(x), \theta(y)) = 1$ then without loss of generality assume that

$$\theta(x) = (a_1, \dots, a_q, a_{q+1}, 0, \dots, 0),$$

$$\theta(y) = (a_1, \dots, a_q, b_{q+1}, 0, \dots, 0) \text{ with } a_i \neq 0, b_{q+1} \neq 0 \text{ and } b_{q+1} \neq a_{q+1},$$

and let z, t, u, v be vertices of G such that

$$\theta(z) = (a_1, \dots, a_q, 0, \dots, 0),$$

$$\theta(t) = (a_1, \dots, a_{q-1}, 0, \dots, 0),$$

$$\theta(u) = (a_1, \dots, a_{q-1}, 0, a_{q+1}, \dots, 0),$$

$$\theta(v) = (a_1, \dots, a_{q-1}, 0, b_{q+1}, \dots, 0).$$

Then u and v are not adjacent and x, y cannot be adjacent without generating G_b as induced subgraph (figure 8).

If $d(\theta(x), \theta(y)) > 2$, then x and y cannot be adjacent by Proposition 1.5.

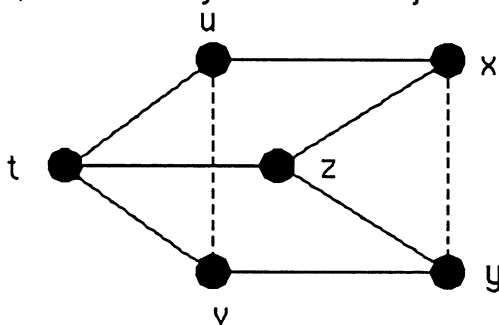


Figure 8

Similarly, if $d(\theta(x), \theta(y)) = 2$, then without loss of generality assume that

$$\theta(x) = (a_1, \dots, a_q, a_{q+1}, 0, \dots, 0),$$

$$\theta(y) = (a_1, \dots, a_q, 0, a_{q+2}, \dots, 0) \text{ with } a_i \neq 0,$$

and let z, t, u, v be vertices of G such that

$$\theta(z) = (a_1, \dots, a_q, 0, \dots, 0),$$

$$\theta(t) = (a_1, \dots, a_{q-1}, 0, \dots, 0),$$

$$\theta(u) = (a_1, \dots, a_{q-1}, 0, a_{q+1}, 0, \dots, 0),$$

$$\theta(v) = (a_1, \dots, a_{q-1}, 0, 0, a_{q+2}, 0, \dots, 0).$$

Then vertices u and v are adjacent and x, y cannot be adjacent without generating G_b as induced subgraph.

2. QIM and QDM-Graphs.

We first recall some definitions introduced in [5] or [7].

For two vertices u, v of a simple graph G the interval $I(u, v)$ is the set of vertices w lying on a shortest (u, v) path.

A subset W of $V(G)$ is convex if $I(u, v) \subset W$ for any u and v in W .

A graph G is interval monotone if all intervals in G are convex.

An interval $I(u, v)$ is closed if $w \in V(G) - I(u, v) \Rightarrow \exists w' \in I(u, v)$ such that $d(w, w') > d(u, v)$.

A graph G is distance monotone (DM) if each interval in G is closed.

In [7] there is a study of DM-graphs and the following characterization of the hypercube.

Let G be an interval monotone DM-graph of minimal degree at least 3 then G is Q_n for some $n \geq 3$.

To generalize this characterization to Hamming graphs we need an extension of the notion of interval.

Definition.

Let u, v be two vertices of a simple connected graph G . The quasi-interval $I'(u, v)$ is the set of vertices w such that there is no vertex of G distinct of w belonging to both a geodesic between u, w and a geodesic between w, v (we say a vertex w belongs to a geodesic if and only if there are two edges of the geodesic incident to w); i.e.

$$I'(u, v) = \{ w, I(u, w) \cap I(w, v) = \{w\} \}.$$

This notion was been introduced by L.Nebesky [9] in the study of a family of trees.

Notice that $I(u, v) \subset I'(u, v)$ and if G is an hypercube then $I(u, v) = I'(u, v)$.
Substituting $I'(u, v)$ to $I(u, v)$ in the above definitions we obtain the following notions:

A subset W of $V(G)$ is quasi-convex if $I(u,v) \subset W$ for every u,v in W .

A graph G is quasi-interval monotone (QIM) if all quasi-intervals in G are quasi-convex.

A quasi-interval $I(u,v)$ is closed if $w \in V(G) - I(u,v) \Rightarrow \exists w' \in I(u,v)$ such that $d(w,w') > d(u,v)$.

A graph G is quasi-distance monotone (QDM) if each quasi-interval in G is closed.

Proposition 2.1.

A quasi-interval monotone graph does not contain G_a and G_b as induced subgraphs .

proof

Assume u,v,x,z induce G_a in a quasi-interval monotone graph G , as depicted in figure 9.

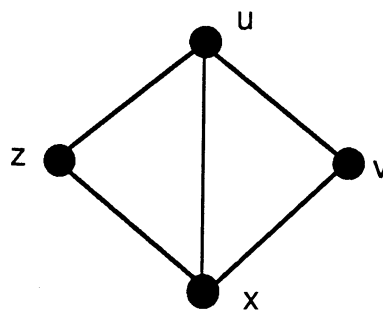


Figure 9

We have $x \in I(u,z)$, $u \in I(u,z)$ and therefore $I(u,x) \subset I(u,z)$, but $v \in I(u,x)$ and $v \notin I(u,z)$ i.e. a contradiction.

Assume u,v,x,y,z,t induce G_b in G , as depicted in figure 10.

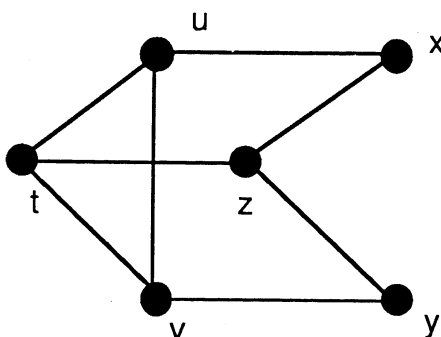


Figure 10

Then $d_G(u,y) = 2$. Now x,y are not adjacent, whence $u \in I'(x,y)$. Similarly $v \in I'(x,y)$. Then $I'(u,v) \subset I'(x,y)$, but $t \in I'(u,v)$ and $t \notin I'(x,y)$ i.e. a contradiction. \square

Proposition 2.2.

If G is a connected quasi-interval monotone and quasi-distance monotone graph containing a 3-star $(K_{1,3})$ as induced subgraph, then every vertex in G is the center of such a 3-star.

proof

Let u be the center of a 3-star u,w_1,w_2,w_3 and v be a neighbour of u . Assume there is no 3-star centered on u containing v . Then v must be adjacent to at least one w_i . It cannot be adjacent to two w_i 's, say w_1 and w_2 , because u,w_1,w_2,v would induce G_a (impossible by Proposition 2.1). But if u is not adjacent to w_2 and w_3 , then u,v,w_2,w_3 induce a 3-star therefore there is always a 3-star centered on u and containing v .

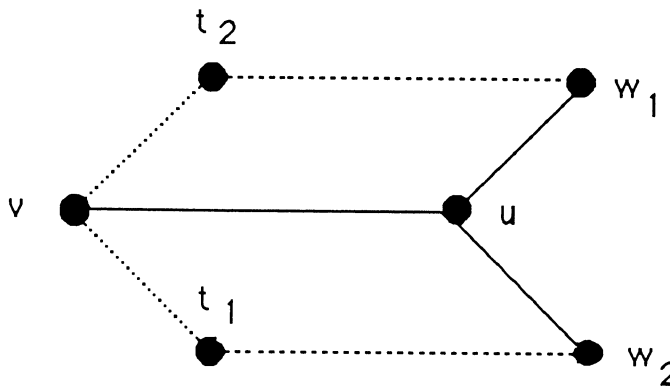


Figure 11

Let u,v,w_1,w_2 be such a 3-star (figure 11). Then w_1 is not in $I'(v,w_2)$ because w_1 is not adjacent to v or w_2 . Now G is QDM therefore there is some t_1 in $I(v,w_2)$ with $d(t_1,w_1) > 2$. Then t_1 is adjacent to both v and w_2 . Similarly there is some t_2 in $I(v,w_1)$ with $d(t_2,w_2) > 2$ and t_2 adjacent to both v and w_1 . Furthermore t_1 and t_2 are distinct and non-adjacent, and u is not adjacent to t_1 and t_2 ; therefore v is the center of an induced 3-star u,t_2,t_1 . By connexity we have proposition 2.2. \square

Notice that the condition "G contain a 3-star as induced subgraph" corresponds

to "G is of minimal degree 3" in the characterization of hypercubes as IM and DM-graphs.

Proposition 2.3.

Let G be a connected QDM and QIM-graph containing a 3-star as induced subgraph. If u is a vertex of G and v, w are two non-adjacent neighbours of u , then there is a vertex x adjacent to u and non-adjacent to v and w .

proof

By Proposition 2.2 there is a 3-star u, w_1, w_2, w_3 centered on u . A w_i cannot be adjacent to both v and w (otherwise w_i, u, v, w induce G_a) (figure 12).

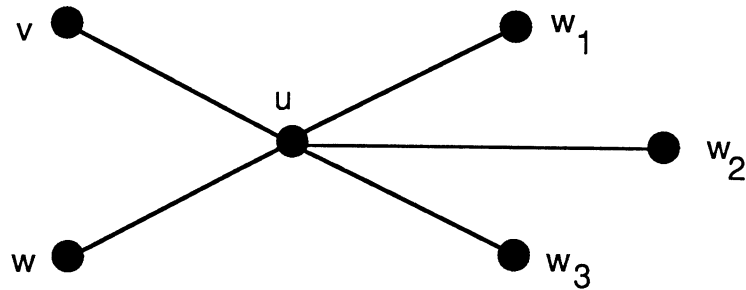


Figure 12

Notice that v (or w) cannot be adjacent to two w_i 's, w_1 and w_2 say (otherwise w_i, u, v, w induce G_a).

If v, w are two such w_i , then there is nothing to prove.

If v (respectively w) is a w_i (w_1 for example), then w cannot be adjacent to both w_2 and w_3 .

If v, w, w_1, w_2, w_3 are all distinct, then at least one w_i is not adjacent to both v and w . \square

Proposition 2.4.

If G is a connected QDM and a QIM-graph containing a 3-star as induced subgraph, then two non-adjacent vertices in G have exactly two common neighbours or none at all.

proof

Let u, v be two non-adjacent vertices in G and z a common neighbour. Let w be adjacent to z and not adjacent to u and v (w exists by Proposition 2.3).

We have $w \notin I'(u, v)$ and thus $\exists t \in I(u, v)$ such that $d(t, w) > 2$. Therefore u, v have at least two common neighbours. Let x be a third common neighbour (figure 13); then x, z, t are not adjacent.

But $x \in I'(u, v)$ and u, v are in $I'(z, t)$, therefore $x \in I'(z, t)$. This is not possible because $x \rightarrow u \rightarrow z$ and $x \rightarrow u \rightarrow t$ are two non disjoint geodesics. \square

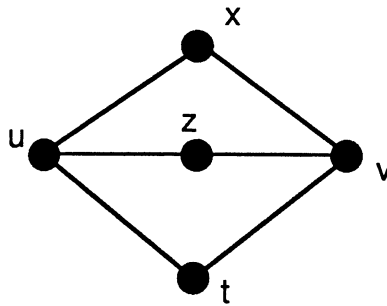


Figure 13

Theorem 2

Let G be a simple connected graph such that :

- (i) G is a QDM-graph,
- (ii) G is a QIM-graph,
- (iii) G contains a 3-star as induced subgraph.

Then G is a Hamming graph.

By Proposition 2.1 and 2.4, the hypotheses of Theorem 1 are satisfied. Then the number of maximal i -cliques in G containing x , viz. $N_i(x)$, is independent of the vertex x . We are going to prove that $|V(G)| = \prod_{i=1}^p N_i$ so that by Theorem 1 G will be the Hamming graph $(K_2)^{N_2} \square (K_3)^{N_3} \square \dots \square (K_p)^{N_p}$.

Proposition 2.5.

If x, y are two adjacent vertices of G in the same level C_i then there is some z in C_{i-1} adjacent to both x and y and therefore there is no vertex in C_{i+1} adjacent to both x and y .

proof

The proof is by induction on i . The property is true for $i = 1$. Assume it for the level C_{i-1} . Let t in C_{i-1} be adjacent to x . Assume that t is not adjacent to y . There is by Proposition 2.3 an other vertex u adjacent to both y and t .

Assume that u is in C_i (figure 14); then u cannot be adjacent to x (t and y should be adjacent).

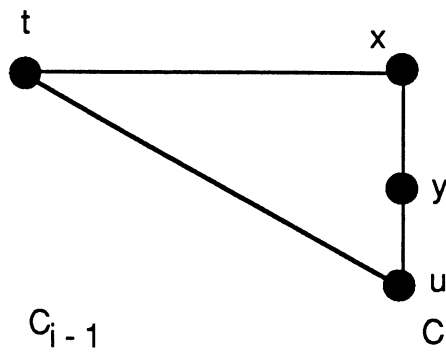


Figure 14

Assume that $y \in I'(0, x)$. We have $t \in I'(0, x)$ and therefore $I'(y, t) \subset I'(0, x)$. But we have $u \in I'(y, t)$ and $u \notin I'(0, x)$ (t belongs to $u \rightarrow t \rightarrow x$ and to $u \rightarrow t \rightarrow \dots \rightarrow 0$, being geodesics between u, x and $u, 0$).

Therefore $y \notin I'(0, x)$ and there is some z in $I(x, 0)$ with $d(y, z) > i$. But we have $d(y, 0) = i$ and x is on a path of length at most i between z and y , for every $z \neq 0$ in $I(x, 0)$.

Thus u is in C_{i-1} . By induction hypothesis there is some w common neighbour w of t and u in C_{i-2} . Let z be the other common neighbour of x and w . Then z is adjacent to y else w, t, u, x, y, z would induce G_b , and Proposition 2.5 is proved. \square

Proposition 2.6.

If x and y are two vertices of G in the same level C_i with a common neighbour z in C_{i+1} , then they have one in C_{i-1} .

proof

By Proposition 2.5, x and y are not adjacent. Therefore by 2.4 there is an other common neighbour t . If t is in C_{i+1} or in C_i ; then we have $x \in l'(0,t)$; $y \in l'(0,t)$ and $z \in l'(x,y)$, whence z is in $l'(0,t)$.

But this not possible because $z \rightarrow y \rightarrow t$ and $z \rightarrow y \rightarrow \dots \rightarrow 0$ are two non disjoint geodesics. Therefore t is in C_{i-1} . \square

Proposition 2.7.

All $A_{\alpha_2 \dots \alpha_p}$ are pairwise disjoint (with notations of the part one).

proof

The proof is by induction on $j = \sum_{i=2}^p \alpha_i$. If $j = 0$ or 1 this is trivial. Let z be in C_{i+1} and let $0 \rightarrow \dots \rightarrow x \rightarrow z$, $0 \rightarrow \dots \rightarrow y \rightarrow z$ be two geodesics.

If $x=y$, then the edge $\{x,z\}$ belonging to a unique maximal clique the induction hypothesis implies that the two geodesics use for all i α_i edges in a maximal i -clique.

If $x \neq y$ then x and y are not adjacent and by Proposition 2.5 and by 2.6 there is some t in C_{i-1} adjacent to x and y . Let h and h' be the one-to-one correspondences between vertices of $\Gamma(t)$, $\Gamma(y)$ and $\Gamma(y)$, $\Gamma(z)$, respectively. We know (see the proof of Proposition 1.1) that h and h' preserve the membership to maximal cliques of the same order. Therefore, if $\{x,t\}$ (respectively $\{y,t\}$) belongs to a maximal j -clique (respectively k -clique), then $\{y,z\}$ (respectively $\{x,z\}$) also.

By induction hypothesis t belongs to a unique $A_{\alpha_2 \dots \alpha_p}$ and y,x also. Now y belongs to $A_{\alpha'_2 \dots \alpha'_p}$ with $\alpha'_k = \alpha_k + 1$, $\alpha'_i = \alpha_i$ ($i \neq k$) and x belongs to $A_{\alpha''_2 \dots \alpha''_p}$ with $\alpha''_j = \alpha_{j+1}$, $\alpha''_i = \alpha_i$ ($i \neq j$). Therefore the edges of both $0 \rightarrow \dots \rightarrow x \rightarrow z$ and $0 \rightarrow \dots \rightarrow y \rightarrow z$ belong to α'''_i maximal i -cliques with $\alpha'''_k = \alpha_k + 1$, $\alpha'''_j = \alpha_{j+1}$, $\alpha'''_i = \alpha_i$ if $i \neq k$, $i \neq j$ (if $k \neq j$); and $\alpha'''_k = \alpha_k + 2$, $\alpha'''_i = \alpha_i$ if $i \neq k$ if $k=j$. \square

Proposition 2.8.

Let x be a vertex of C_j in $A_{\alpha_2 \dots \alpha_p}$. Then there are exactly

a) α_i vertices in $\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ for all i ,

- b) $\sum_{i=2}^p (i-2) \alpha_i$ vertices in $\Gamma(x) \cap C_j$,
 c) $(i-1) (N_i - \alpha_i)$ vertices in $\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i+1} \dots \alpha_p}$ for all i .

proof

The Proposition 2.8 a. is true for $j=0,1$. Let y in C_{j-1} be adjacent to x and let h be the one-to-one correspondence between $\Gamma(x)$ and $\Gamma(y)$. If $\{x,y\}$ belongs to a maximal k -clique with $k \neq i$ h is an isomorphism between $\Gamma(x) \cap C_{j-1}$ and $\Gamma(y) \cap C_{j-2}$ (by 2.6). Now h preserves the membership to maximal i -cliques and by induction hypothesis $|\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}| = |\Gamma(y) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_{k-1} \dots \alpha_p}| = \alpha_i$. If $k=i$, then we can make the same calculation obtaining $|\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}| = |\Gamma(y) \cap A_{\alpha_2 \dots \alpha_{i-2} \dots \alpha_p}| + 1 = \alpha_i$. Therefore we have 2.8 a. By Proposition 2.5 the number of vertices in $\Gamma(x) \cap C_j$ is exactly $\sum_{i=2}^p |\Gamma(x) \cap A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}| (i-2)$ and we have 2.8 b and thus 2.8 c. \square

By the above proposition the number of edges between vertices in $A_{\alpha_2 \dots \alpha_p}$ and vertices in $A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}$ is exactly :

$$|A_{\alpha_2 \dots \alpha_i \dots \alpha_p}| \alpha_i \text{ (by 2.8 a) and}$$

$$|A_{\alpha_2 \dots \alpha_{i-1} \dots \alpha_p}| (N_i - (\alpha_i - 1)) (i-1) \text{ (by 2.8 c).}$$

Therefore $|A_{\alpha_2 \dots \alpha_p}| = \prod_{i=2}^p \binom{N_i}{\alpha_i} (i-1) \alpha_i$ and by 2.7 $|V(G)| = \prod_{i=2}^p i N_i$, and then Theorem 2 is proved.

REFERENCES

1. **J.M.Laborde**, Charakterisierungen des Hyperwürfels , **Rostock. Math. Kolloq.** 21(1982) 63-68
2. **P.V.Ceccherini**, A q-analogous of the characterization of hypercubes as graphs , **J. Geometry** 22(1984) 57-74
3. **S.Foldes**, A characterization of Hypercubes , **Discrete Math.** 17(1977) 155-159
4. **M.Mulder**, Interval-regular graphs , **Discrete Math.** 41(1982) 253-269
5. **M.Mulder**, $(0,\lambda)$ graphs and n-cubes , **Discrete Math.** 28(1979) 179-188
6. **J.M. Laborde** , **S.P. Rao Hebbare** , Another characterization of hypercubes , **Discrete Math.** 39(1982) 161-166
7. **G.Burosh** , **I.Havel** , **J.M. Laborde**, DM-Graphs and a new characterization of Hypercubes, **Discrete Math** to appear
8. **Y. Egawa** , Characterization of the cartesian product of complete graphs by convex subgraphs, **Discrete Math.** 58 (1986) 307-309 .
9. **L.Nebesky** , Algebraic properties of Husimi trees, **Casopis Pest. Math.** 107 (1982) 116-123 .

CYCLE-REGULAR GRAPHS

Michel Mollard
LSD(IMAG) BP 53X
38041 Grenoble CEDEX, France

Summary:

H.M.Mulder introduced $(0, \lambda)$ -graphs and proved that maximum $(0, \lambda)$ -graphs are Hypercubes. One way of generalization of this concept is to consider cycle-regular graphs. We prove that these graphs have also some regularity properties and that maximum $[3, 1, 6]$ -cycle regular graphs are also related to hypercubes.

0. Introduction.

In this paper a path of length l of a graph G is a sequence of vertices u_0, u_1, \dots, u_l such that any two consecutive vertices are adjacent in G and the vertices are distinct except possibly u_0 and u_l .

An elementary cycle of length m of G is a connected subgraph of G on m distinct vertices $\{u_1, \dots, u_m\}$ regular of degree 2.

We say that a path u_0, u_1, \dots, u_l belongs to an elementary cycle on $\{v_1, \dots, v_m\}$ if and only if $\{u_0, u_1, \dots, u_l\} \subset \{v_1, \dots, v_m\}$ and the path is an induced subgraph of the cycle.

$(0, \lambda)$ -graphs (connected graph in which any two vertices have λ common neighbours or none at all) have been introduced by H.M.Mulder [1]. These graphs are regular.

Definition

Let l and λ be two integers with $l \geq 2$, $\lambda \geq 1$ and $G = (V, E)$ be a finite connected graph with neither loops nor multiple edges of girth at least l .

G is a $[l, \lambda]$ -cycle regular graph if there is a non-empty subset C of elementary cycles in G such that every path in G of length l belongs to exactly λ cycles in C .

In the important case where C is the set of elementary cycles of a given length m ($m \geq 2l$) we say that G is a $[l, \lambda, m]$ -cycle regular graph.

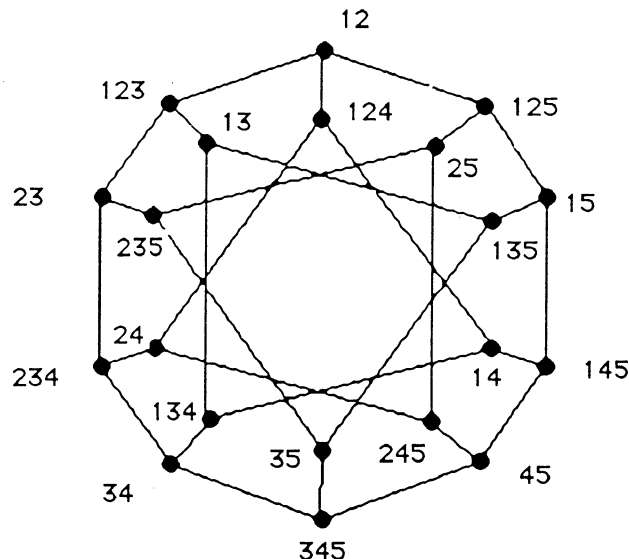


figure 1: An example of $[3, 1, 6]$ -cycle regular graph.

The $[2, 1, 4]$ -cycle regular graphs are exactly the $(0, 2)$ -graphs of H.M.Mulder. These graphs are regular and maximum ones are hypercubes [1], [2].

We first study the regularity of $[l, \lambda]$ -cycle regular graphs of minimal degree $\delta \geq 3$. In the second section we study the case $\delta = 2$ and in the third part we give two families of $[3, 1, 6]$ -cycle regular graphs and prove that maximum ones are also related to the hypercube.

1. General case.

Let $d(u)$ be the degree of a vertex u in G .

Lemma 1

Let u_1, u_2, \dots, u_l be a path of length $l-1$ in a $[l, \lambda]$ -cycle regular graph. Then $d(u_1) = d(u_l)$.

Proof. The girth of G is at least l . Therefore every vertex adjacent to u_1 and distinct from u_2 is not on the path u_1, u_2, \dots, u_l , but it may be u_l . If $l > 2$, delete an eventual edge (u_1, u_l) between u_1 and u_l . Let x_i ($i=0, 1, \dots, l$) and y_j ($j=0, 1, \dots, J$) be the vertices adjacent to respectively u_1 and u_l (we assume that $x_0 = u_2, y_0 = u_{l-1}$) (figure 2). We have to prove that $l=J$. For all non-zero i and j and all k , we have $x_i \neq u_k$ and $y_j \neq u_k$.

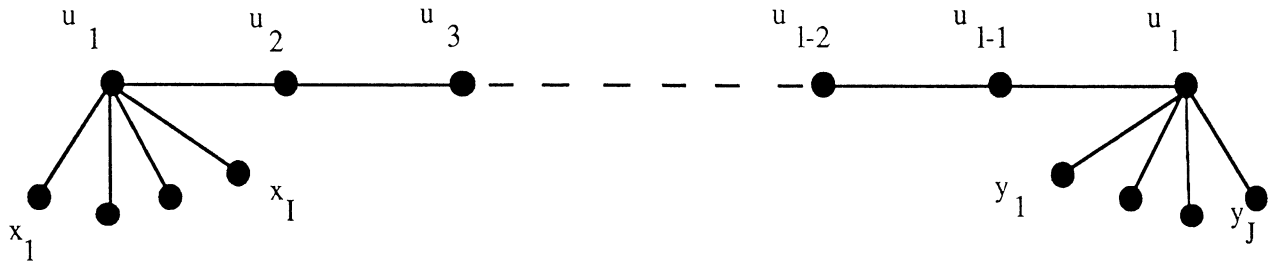


figure 2

For a non-zero $i < l$, let δ_i be the number of cycles in C which contain the path $x_i, u_1, u_2, \dots, u_l$. We have by definition of a $[l, \lambda]$ -cycle regular graph $\delta_i = \lambda$.

The number of cycles in C which contain the path u_1, u_2, \dots, u_l is exactly $\sum_{i=1, \dots, l} \delta_i$ because each of these cycles contains one and only one path $x_i, u_1, u_2, \dots, u_l$.

We can make the same computation for u_l and the paths $u_1, u_2, \dots, u_l, y_j$ so we have $\lambda l = \lambda J$ and therefore $d(u_1) = d(u_l)$.

□

Lemma 2

Every vertex v of a $[l, \lambda]$ -cycle regular graph is on at least one cycle in C .

Proof. Let C be a cycle of C (C is not empty). If v is not on this cycle there is a minimal path between v and C . Then C and this path are disjoint and we can choose on their union a path of length l with an end-point in v and this path belongs to λ cycles in C . \square

Definition

A bipartite graph is said to be semiregular if the vertices in the same bipartition are of the same valency.

Theorem 3

If G is a $[l, \lambda]$ -cycle regular graph of minimal degree $\delta \geq 3$ then G is regular or semiregular.

Proof. Let u and v be two vertices joined by a path of length 2 say u, x, v (figure 3). Since $\delta(G) \geq 3$, there is an other vertex w adjacent to x . Then w is on a cycle of C therefore there is on this cycle at least a path w, \dots, t of length $l-3$ which does not use the vertices x, u and v (G is of girth at least l). Then $u, x, (w, \dots, t)$ and $v, x, (w, \dots, t)$ are two paths of length $l-1$ so $d(u) = d(v) = d(t)$.

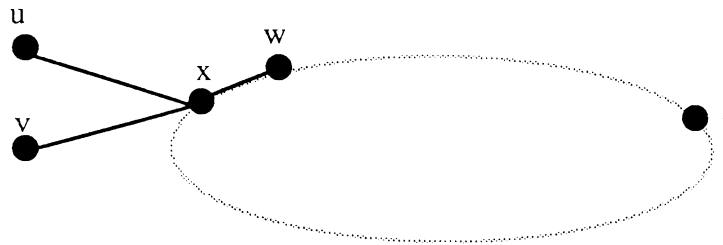


figure 3

By connectivity the vertices joined by paths of even length have the same degree. Therefore G is regular or without cycles of odd length and in this case it is a semiregular graph. This ends the proof of theorem 3.

Remark 4

We can extend the definition of $[l, \lambda]$ -cycle regular graph to multigraphs and lemma 1 (thus theorem 3) can be proved with the same demonstration counting the number of incident edges rather than adjacent vertices.

Remark 5

Notice that the condition $l \geq 2$ is necessary to give us some regularity properties. For example graphs of which the blocks are 3-cliques or the following graph with $\delta(G) \geq 4$ (figure 4) have the property that every edge belongs to exactly one 3-cycle, but they are not regular or semiregular.

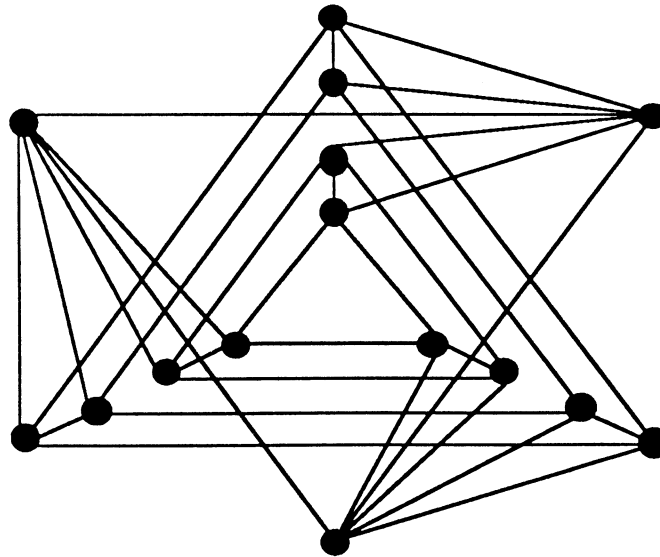


figure 4

In theorem 3 we assume $\delta(G) \geq 3$ and by lemma 2 we have $\delta(G) \geq 2$; we are now going to study the remaining case.

2.The case $\delta(G)=2$.

At every path P of length p with an end-vertex x we can associate the degree sequence of vertices on this path $D_x(P)$.

Proposition 6

Let P and P' be two paths of the same length $p < l$ with a common end-vertex x of degree at least 3. Then $D_x(P)$ and $D_x(P')$ are identical .

Proof. Let $P = x, \dots, z$ and $P' = x, \dots, t$. Let x_0 be an other vertex adjacent to x . Then x_0 is not on P or P' and x_0 is on a cycle of C (lemma 2). If we choose a path of length $l-p-1$ w, \dots, x_1, x_0 on this cycle with $x_1 \neq x$ we obtain two paths of length $l-1$, $(w, \dots, x_1, x_0) P$ between z and w and $(w, \dots, x_0, x_1) P'$ between t and w . Therefore by lemma 1 $d(w) = d(z) = d(t)$. We can clearly make the same reasoning with the subpaths of P and P' of a given length $p' < p$ and thus obtain $D_x(P) = D_x(P')$.

□

Proposition 7

Let G be a $[l, \lambda]$ -cycle regular graph of minimal degree $\delta = 2$. Then two vertices of degree more than 2 cannot be adjacent.

Proof. By proposition 6 (with $p=1$) and by connectivity it follows that if two vertices of degree more than 2 are adjacent then $\delta(G) > 2$.

If G is not a cycle, there are paths between vertices of degree more than 2 with all intermediate vertices of degree 2; we call such path a contractible path. We use this term because we are going to contract such a path in a single edge i.e. delete the inner

vertices of the path and add an edge between its extremities. The length of a contractible path is at most $l-1$ by lemma 1. If two such paths P and P' have a common end, then $l(P) = l(P')$ by proposition 6, therefore by connectivity all contractible paths have the same length.

Proposition 8

Let G be a $[l, \lambda]$ -cycle regular graph of minimal degree $\delta = 2$, let p be the common length of contractible paths in G and let G' be the connected graph obtained by contraction of contractible paths to single edges. Assume $p \neq l-1$ or $\lambda \neq 1$. Then G' is of minimal degree $\delta(G') \geq 3$ and G' is a $[\lceil l/p \rceil, \lambda]$ -cycle regular graph (where $\lceil x \rceil$ denote the upper integer part).

Proof. Notice first that p divides $l-1$ because there is in G some path of length $l-1$, of which the extremities are vertices of degree > 2 so are union of contractible paths.

Every vertex of G with degree > 2 is end of at least 3 contractible paths therefore $\delta(G') > 2$.

Assume that two contractible paths have the same two ends. We have $2p \geq l$ (because G is of girth at least l) but p divides $l-1$ thus $p = l-1$. Therefore, if $p \neq l-1$, then G' is without multiple edges.

If $p = l-1$ and if G' has multiples edges then we have $\lambda = 1$. Therefore we exclude this case because we have choose to consider only simple graphs.

Notice that every path in G with two vertices of degree at least 3 as extremities is the union of contractible paths. The vertices of G' are vertices of G with degree > 2 , therefore G' is connected. If there is a cycle in G' of length c it is a contraction of a cycle of length $p \cdot c$ in G . Therefore G' is of girth at least $\lceil l/p \rceil$.

Let P be a path in G' with length $\lceil l/p \rceil$ and extremities x, y . Then $\lceil l/p \rceil = (l-1/p) + 1$ because p divides $l-1$.

P is the contraction of a unique path in G of length $l-1 + p$. Every l -length subpath of this path belongs to the same λ cycles in C ; and the contraction of these λ cycles form exactly λ cycles of G' which are the only one (as contraction of cycles in C) containing the path P ; therefore G' is a $[\lceil l/p \rceil, \lambda]$ -cycle regular graph where cycles in C' are the contractions of cycles of C .

□

The $(p-1)$ -subdivision of a graph G' is obtained by inserting $p-1$ new vertices of degree 2 on every edges of G' .

Theorem 9

If G is a $[l, \lambda]$ -cycle regular graph of minimal degree $\delta = 2$, then there is an integer p with $2 \leq p \leq l-1$ such that G is a $(p-1)$ -subdivision of a $[\lceil l/p \rceil, \lambda]$ -cycle regular graph with minimal degree $\delta \geq 3$.

Notice that if $p = l-1$ the contracted graph G' can have multiple edges and in this case $\lambda = 1$; furthermore G' is obtained from a simple $[2, 1]$ -cycle regular graph G'' substituting some edges by a pair of edges. But not all these constructions are possible.

Reciprocally if G is a $[l, \lambda]$ -cycle regular graph (with $(l, \lambda) \neq (2, 1)$) and k is an integer, then the k -subdivision G' of G is a $[(l-1)(k+1)+1, \lambda]$ -cycle regular graph where

cycles in C' are the k -subdivisions of cycles in C . We have this property because every $(l-1)(k+1)+1$ path of G' is a subpath of the k -subdivision of a unique l path of G and therefore is contained in exactly λ k -subdivisions of cycles in C .

□

3. [3,1,6]-cycle regular graphs.

[2,1,4]-cycle regular graphs are (0,2) graphs of H.M.Mulder. Thus the maximum ones are hypercubes Q_n . We are going to prove that maximum [3,1,6]-cycle regular graphs are also related to Q_n .

Let x be a vertex of a graph G and let $\Gamma_{p(x)}$, $p \geq 0$ be the set of vertices y with $d(x,y) = p$. For a vertex-transitive graph like Q_n for every vertices x,y there is an automorphism of G mapping $\Gamma_{i(x)}$ on $\Gamma_{i(y)}$ for all i . In this case or in the general case if there is no ambiguity we call $\Gamma_{p(x)}$ the level Γ_p of G . Notice that for the case of hypercubes Q_n the level Γ_p can be seen as the p -subsets of a set of n vertices (vertices associated to X and Y are adjacent if and only if $X \Delta Y = 1$).

Proposition 10

Let G be the subgraph of the hypercube induced by two consecutive levels Γ_{p-1} and Γ_p ($p > 1$ and $p < n$), G is a [3,1,6]-cycle regular graphs of order $\binom{n}{p} + \binom{n}{p-1}$ and is semiregular of degrees $n-p+1$ and p .

Proof. It is clear that G is bipartite and connected. Let x,y,z,t be a 3-path and X,Y,Z,T be the corresponding sets. Assume x to be in Γ_{p-1} ; we have :

$$\exists! a \text{ with } Y = X \cup \{a\} \text{ and } a \notin X$$

$$\exists! b \text{ with } Y = Z \cup \{b\} \text{ and } b \notin Z, b \neq a$$

$$\exists! c \text{ with } T = Z \cup \{c\} \text{ and } c \notin X, b \neq c, a \neq c$$

Therefore if x and t are joined by a 3-path; X,T are such that

$$|X \cap T| = p-2$$

$$X \cup T = (X \cap T) \cup \{a,b,c\} \text{ with } a,c \notin X \text{ and } b \notin T.$$

$\{a,c\}$ and b are characterized by X and T . Thus there are exactly two 3-paths fixed by the choice of "a" in $\{a,c\}$. These two paths are disjoint then every 3-path belongs to an unique 6-cycle.

□

Remark 11

If Γ_{p-1} and Γ_p are central levels of Q_{2p-1} , then G is regular of degree p and order $2 \binom{2p-1}{p-1} = \binom{2p}{p}$. We denote this graph by H_p .

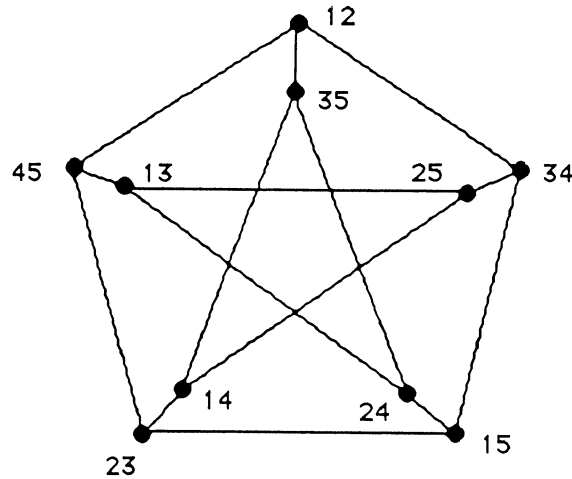
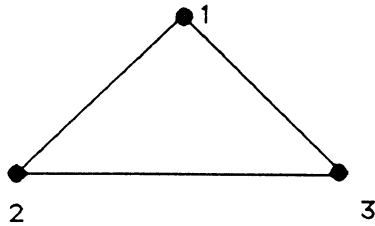
For example with $p=3$ we obtain the Desargues graph H_3 (figure 1).

An other important family of $[3,1,6]$ -cycle regular graphs consist of the Odd graphs introduced in [4].

Definition

For an integer $n \geq 2$, the Odd graph O_n has the $(n-1)$ -subsets of $N=\{1,2,\dots,2n-1\}$ as vertices and two vertices are joined by an edge if their corresponding subsets are disjoint.

The smallest Odd Graphs are K_3 and the Petersen graph.



Proposition 12

For every $n > 2$, the odd graph O_n is a $[3,1,6]$ -cycle regular graph of degree n and order $\binom{2n-1}{n-1}$.

Let x,y,z,t be a 3-path. Then the corresponding sets X,Y,Z,T are such that

- $\exists! a$ with $a \notin X \cup Y$
- $\exists! b$ with $b \in Y \cup Z$, $b \neq a$
- $\exists! c$ with $c \in Z \cup T$, $c \neq b$.

But we have $c \neq a$ (because $a \in Z$) and $X \cap T = \{b\}$ and $\overline{X \cup T} = \{a,c\}$. Therefore as in the proof of the above proposition there are exactly two disjoint 3-paths fixed by the choice of "a" in $\{a,c\}$.

Lemma 13

Let G be a $[3,1,6]$ -cycle regular graph and for an arbitrary level decomposition $\Gamma_0, \Gamma_1, \dots, \Gamma_r$ of G let u in Γ_i . Then $d^-(u) = |\Gamma_i(u) \cap \Gamma_{i-1}| \geq \lceil i/2 \rceil$.

Proof. This is true for $i=0,1$ and 2 . Assume the property for all vertices in Γ_i and let u in Γ_{i+2} and v in Γ_i be on a 2-path u,y_0,v .

Let x_1, \dots, x_p be the neighbours of v in Γ_{i-1} ($p \geq \lceil i/2 \rceil$) and y_1, \dots, y_q be the neighbours of u (distinct from y_0) in Γ_{i+1} (figure 6).

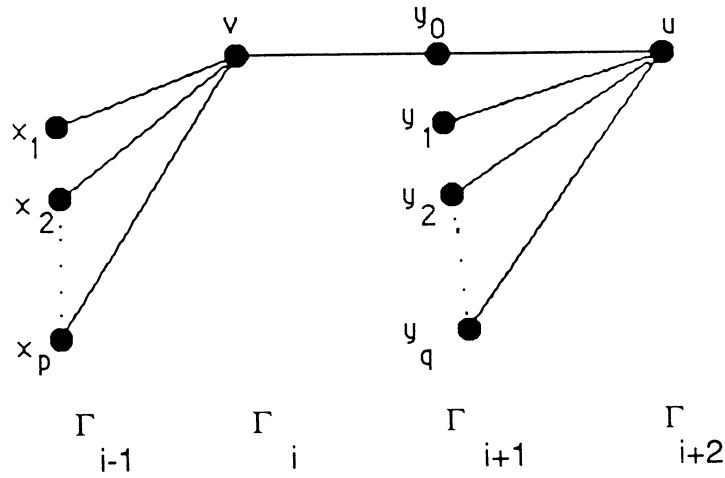


figure 6

Let $N_{i,j}$ ($i=1,\dots,p; j=1,\dots,q$) be the number of 6-cycles using the path x_i, v, y_0, u, y_j . By the fact that G is a $[3,1,6]$ -cycle regular graph using the two 3-paths x_i, v, y_0, u and v, y_0, u, y_j we obtain :

$$\forall i \sum_j N_{i,j} = 1 \text{ and } \forall j \sum_i N_{i,j} \leq 1.$$

Therefore $\sum_i \sum_j N_{i,j}$ is equal to p and is at most q ; but $d^-(u) = q+1$ and $d^-(v) = p$ then by induction the lemma follow.

□

Corollary14

Let G be a $[3,1,6]$ -cycle regular graph of maximum degree n and $\Gamma_0, \Gamma_1, \dots, \Gamma_p$ a level decomposition from a vertex of degree n then, for $k = 0, \dots, n-2$,

$$|\Gamma_{2k+1}| \leq (n/k+1) \binom{n-1}{k}^2, \text{ and } |\Gamma_{2k+2}| \leq (n(n-k-1)/(k+1)^2) \binom{n-1}{k}^2$$

Proof. This is true for $k = 0$. We have also $|\Gamma_1| = n$ and $|\Gamma_2| \leq n(n-1)$. Assume by induction hypothesis that $|\Gamma_{2k}| \leq (n(n-k)/k^2) \binom{n-1}{k-1}^2$. Let n' be the degree of vertices in odd levels.

By counting the edges between Γ_{2k} and Γ_{2k+1} , we get from lemma 13 that this number is at least $|\Gamma_{2k+1}| \lfloor 2k+1/2 \rfloor$ and at most $|\Gamma_{2k}| (n - \lceil 2k/2 \rceil)$. Thus we have

$$|\Gamma_{2k+1}| \leq |\Gamma_{2k}| (n-k)/(k+1) \leq (n(n-k)^2/k^2(k+1)) \binom{n-1}{k-1}^2 = (n/(k+1)) \binom{n-1}{k}^2.$$

Similarly counting the edges between Γ_{2k+1} and Γ_{2k+2} gives

$$|\Gamma_{2k+2}| \leq |\Gamma_{2k+1}| (n'-k-1)/(k+1) \leq (n(n-k-1)/(k+1)^2) \binom{n-1}{k}^2.$$

By the lemma 13, G is of diameter at most $2n-1$. Using the corollary we obtain:

$$|V(G)| \leq |\Gamma_0| + |\Gamma_{2n-1}| + \sum_{i=0, \dots, n-2} \binom{n-1}{i}^2 (n/i+1 + n(n-i-1)/(i+1)^2).$$

But $|\Gamma_{2n-1}| \leq 1$ and $|\Gamma_0| = 1$, whence

$$|V(G)| \leq 2 + \sum_{i=0, \dots, n-2} \binom{n-1}{i}^2 (n^2/(i+1)^2)$$

$$|V(G)| \leq 2 + \sum_{i=0, \dots, n-2} \binom{n}{i+1}^2 = \sum_{i=0, \dots, n} \binom{n}{i}^2 = \binom{2n}{n}.$$

Therefore every $[3,1,6]$ -cycle regular graph of maximum degree n is of order at most $\binom{2n}{n}$. We are going to prove now that maximum $[3,1,6]$ -cycle regular graphs are the subgraphs H_n induced by central levels Γ_{n-1} and Γ_n of odd dimension hypercubes Q_{2n-1} .

Assume that G is a $[3,1,6]$ -cycle regular graph of maximum degree n and of order $\binom{2n}{n}$. Then we have for $k = 0, \dots, n-1$

$$|\Gamma_{2k+1}| = (n/k+1) \binom{n-1}{k}^2 \quad \text{and} \quad |\Gamma_{2k+2}| = (n(n-k-1)/(k+1)^2) \binom{n-1}{k}^2.$$

Therefore G is regular and it is clear that using these equalities in the proof of the above corollary we obtain for all u in Γ_i ($i=0, \dots, 2n-1$)

$$d^-(u) = |\Gamma_{(u)} \cap \Gamma_{i-1}| = \lceil i/2 \rceil \quad \text{and} \quad d^+(u) = |\Gamma_{(u)} \cap \Gamma_{i+1}| = n - \lceil i/2 \rceil,$$

where $\Gamma_{(u)}$ is the set of neighbours of u

Lemma 15

Every 6-cycle of G encounters exactly 2 or 4 levels.

Proof. First count the number A_i of 6-cycles encountering the four levels $\Gamma_i, \Gamma_{i-1}, \Gamma_{i-2}, \Gamma_{i-3}$. This gives

$$A_i = 1/2 \cdot |\Gamma_{i-1}| d_{i-1}^+ d_{i-1}^- d_{i-2}^-.$$

Every 6-cycle of G encountering only the three levels $\Gamma_i, \Gamma_{i-1}, \Gamma_{i-2}$ contains a 3-path x,y,z,t with x in Γ_{i-2} , y and t in Γ_{i-1} , z in Γ_i . And the number of these paths is exactly $A_i = |\Gamma_{i-1}| d_{i-1}^+ d_{i-1}^- (d_{i-1}^- - 1) = 2 A_i$.

But The A_i 6-cycles contains exactly 2 A_i distinct such paths therefore there is no path belonging to a 6-cycle of G encountering 3 levels and thus no such cycles.

□

Lemma 16

Let A_1, A_2, \dots, A_p be p sets ($p \geq 2$) of the same cardinality $a \geq 2$ such that

$$\forall i \forall j \quad |A_i \cap A_j| = a-1.$$

Then we have

$$(1) \left| \bigcap_{i=1,\dots,p} A_i \right| = a-1 \text{ or}$$

$$(2) \left| \bigcup_{i=1,\dots,p} A_i \right| = a+1 .$$

Proof. Notice first that (1) and (2) are incompatible for $p > 2$. If $p = 2$, then we have (1) and (2) .

Assume the property (a fixed) for $p-1$ ($p \geq 3$).

If A_1, A_2, \dots, A_p are such that $\forall i \forall j \ |A_i \cap A_j| = a-1$, then A_1, A_2, \dots, A_{p-1} are also such and therefore by induction hypothesis we have

$$(3) \left| \bigcap_{i=1,\dots,p-1} A_i \right| = a-1 \text{ or}$$

$$(4) \left| \bigcup_{i=1,\dots,p-1} A_i \right| = a+1 .$$

Assume that we have the equality (3) with $\bigcap_{i=1,\dots,p-1} A_i \subset A_p$. Then clearly $\bigcap_{i=1,\dots,p} A_i = \bigcap_{i=1,\dots,p-1} A_i$ and we have (1).

Assume now that we have (3) with x in $\bigcap_{i=1,\dots,p-1} A_i$ and not in A_p . Then x is unique and $\forall i = 1, \dots, p-1$ we have $A_i = (A_i \cap A_p) \cup \{x\}$ is include in $A_p \cup \{x\}$. Thus $\bigcup_{i=1,\dots,p-1} A_i$ is include in $A_p \cup \{x\}$, and we have (4), this implies $p-1=2$ and $|A_1 \cup A_2 \cup A_3| = |A_3 \cup \{x\}| = a+1$.

Assume now that we have the equality (4). If $A_p \subset \bigcup_{i=1,\dots,p-1} A_i$, then we have (2). Else let x be in A_p but not in $\bigcup_{i=1,\dots,p-1} A_i$. For $i=1, \dots, p-1$ we have $A_p = (A_i \cap A_p) \cup \{x\}$, but $\bigcap_{i=1,\dots,p-1} A_i \cap A_p$ is included in $\bigcap_{i=1,\dots,p-1} A_i$ and we have (3). This implies $p=3$ and $(A_1 \cap A_2 \cap A_3) \cup \{x\} = A_3$, and (1) follows.

□

Let G be a $[3,1,6]$ -cycle regular graph of maximum degree n and of order $\binom{2n}{n}$. Choose an arbitrary level decomposition $\Gamma_0, \Gamma_1, \dots, \Gamma_{2n-1}$ of G . We prove now by induction on i , with $i \leq 2n-1$, that the subgraph induced by $\Gamma_0, \Gamma_1, \dots, \Gamma_i$ is isomorphic to the subgraph induced by the first levels $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_i$ of H_n .

We first prove the property for $i=3$. Let x in Γ_0 , let x_1, x_2, \dots, x_n be in Γ_1 and let $x_{1n+1}, x_{1n+2}, \dots, x_{12n-1}$ be the neighbours of x_1 in Γ_2 (figure 7). For $i=2, \dots, n$ and $j=n+1, \dots, 2n-1$, let x_{ij} be the unique vertex in $\Gamma(x_i) \cap \Gamma_2$ belonging to the 6-cycle which closes the path x_{1j}, x_1, x, x_i .

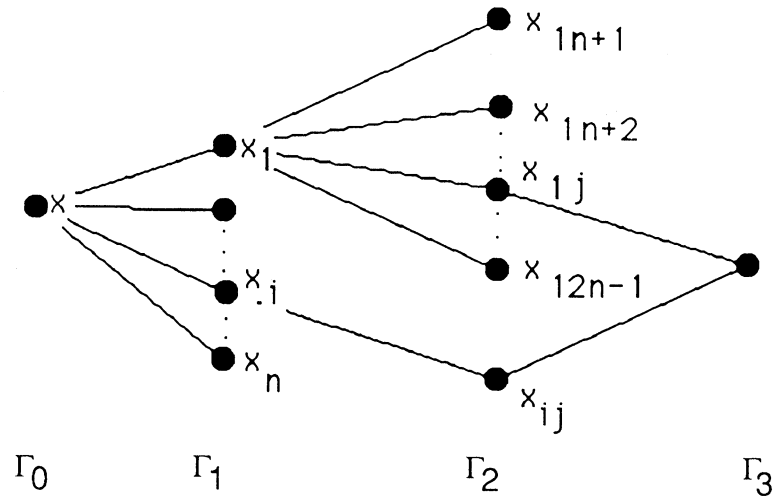


figure 7

An interesting property of this labeling is that x_{ij} belongs to the closure of the path x_{kj}, x_k, x, x_i for every k . Indeed if $x_{1j}, x_1, x, x_i, x_{ij}, t, x_{1j}$ and $x_{1j}, x_1, x, x_k, x_{kj}, z, x_{1j}$ are the closures of x_{1j}, x_1, x, x_i and x_{1j}, x_1, x, x_k (figure 8) then the 3-path z, x_{1j}, t, x_{ij} belongs to a cycle encountering two levels $z, x_{1j}, t, x_{ij}, u, x_{kj}, z$ (x_{1j} and x_{kj} are the unique neighbours of z in Γ_2 because $d^-(z)=2$) therefore x_{kj}, x_k, x, x_i is closed by $x_{kj}, x_k, x, x_i, x_{ij}, u, x_{kj}$.

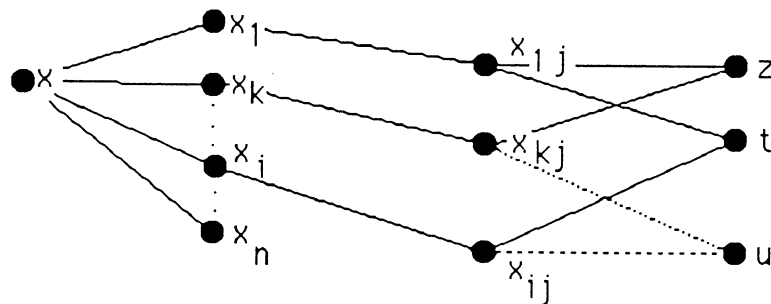


figure 8

If we label the vertex of Γ_3 belonging to the closure of x_{ij}, x_i, x, x_k by $x_{\{ik\}j}$ (and then of x_{kj}, x_k, x, x_i) the mapping

x	\leftrightarrow	$A = \{n+1, \dots, 2n-1\}$
x_i	\leftrightarrow	$\{i, n+1, \dots, 2n-1\}$
x_{ij}	\leftrightarrow	$\{i, n+1, \dots, j-1, j+1, \dots, 2n-1\}$
$x_{\{ik\}j}$	\leftrightarrow	$\{i, k, n+1, \dots, j-1, j+1, \dots, 2n-1\}$

gives an isomorphism between the subgraphs induced by $\Gamma_0, \Gamma_1, \dots, \Gamma_3$ and $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_3$.

Assume now by induction hypothesis that the subgraphs induced by $\Gamma_0, \Gamma_1, \dots, \Gamma_i$ and $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_i$ are isomorphic (with $i \geq 3$) by θ .

Let v be in Γ_{i+1} , let x_1, x_2 be two neighbours of v in Γ_i and let X_1, X_2 be the associated sets in Γ'_i (figure 9). We first prove that $|X_1 \Delta X_2| = 2$.

Let y in Γ_{i-1} adjacent to x_2 . Then y, x_2, v, x_1 are on a unique 6-cycle y, x_2, v, x_1, t, u, y with t in Γ_{i-1} and u in Γ_{i-2} by lemma 2. Let w a neighbour of u in Γ_{i-3} . If W, Y, X_2, V, X_1, T, U are the associated sets in H_n then $W \Delta U, U \Delta T, T \Delta X_1, X_2 \Delta Y, U \Delta Y$ are distinct singletons if $|X_1 \Delta X_2| = 4$. In this case the set $Z = X_2 \Delta (U \Delta W)$ is in Γ'_{i-1} and $|Z \Delta X_1| = 5$. But the path x_1, v, x_2, z belongs to a 6-cycle $x_1, v, x_2, z, z_1, z_2, x_1$ with z_1 in Γ_{i-2} and z_2 in Γ_{i-1} . And the existence in $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_i$ of a path z, z_1, z_2, x_1 is incompatible with $|Z \Delta X_1| = 5$.

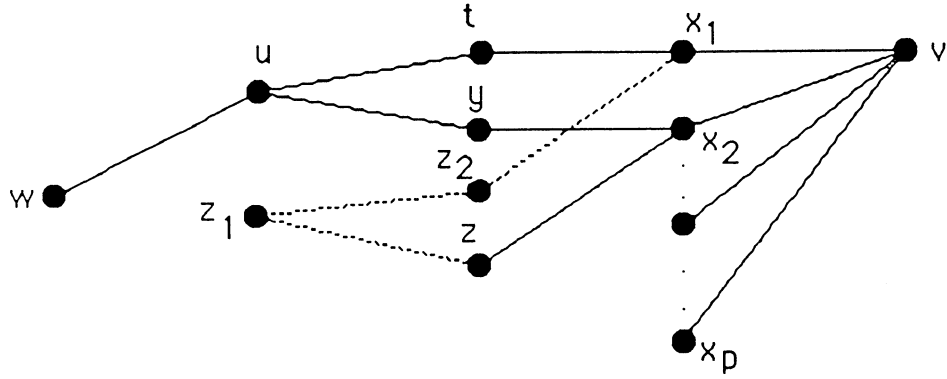


figure 9

Therefore $|X_1 \Delta X_2| \neq 4, |X_1 \Delta X_2| = 2$ and $T \Delta X_1 = X_2 \Delta Y$. Then the set $Z = X_1 \Delta (U \Delta Y) = X_2 \Delta (U \Delta T)$ is in Γ'_{i+1} and is a common neighbour of X_1 and X_2 . Thus x_1, x_2, \dots, x_p , with $p = \lceil (i+1)/2 \rceil$, which are the neighbours of v in Γ_i , are such that $\forall j \forall k$

- (1) the associated sets of Γ'_i satisfies $|X_j \cap X_k| = |X_1| - 1$
- (2) x_j and x_k have no common neighbour in Γ_{i-1} .

Assume without loss of generality that A , the origin of the level decomposition $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_{2n-1}$ of H_n , is of cardinality $n-1$. If i is even (respectively odd) then $|X_i| = n-1$ (resp. n) and we want to prove that $\bigcup_{i=1, \dots, p} X_i$ (resp. $\bigcap_{i=1, \dots, p} X_i$) is in Γ'_{i+1} .

Assume i to be even. By the above lemma we have $|\bigcap_{i=1, \dots, p} X_i| = n-2$ or $|\bigcup_{i=1, \dots, p} X_i| = n$. Assume $|\bigcap_{i=1, \dots, p} X_i| = n-2$. Then, for all $j = 2, \dots, p$, we have $|X_1 \cup X_j| = n$ and we know that $X_1 \cup X_j \notin \Gamma'_{i-1}$ (otherwise x_1 and x_j would have a common neighbour in Γ_{i-1}). Thus $X_1 \cup X_j \in \Gamma'_{i+1}$ and $\bigcap_{i=1, \dots, p} X_i = X_1 \cap X_2$ satisfies $|(\bigcap_{i=1, \dots, p} X_i) \Delta A| = i-1$. Therefore, for all j , the unique element of $X_j - X_1$ is not in A but is also the unique element of $X_j - \bigcap_{i=1, \dots, p} X_i$ and is not included in $\bigcap_{i=1, \dots, p} X_i$. Thus an element of $A - \bigcap_{i=1, \dots, p} X_i$ (which exists by cardinality argument) is an element k in A with $k \notin X_j$ for all j . Choose such a k ; For all j we have $X_j \cup \{k\} \in \Gamma'_{i-1}$ and $\bigcap_{i=1, \dots, p} X_i \cup \{k\} \in \Gamma'_{i-2}$ (figure 10).

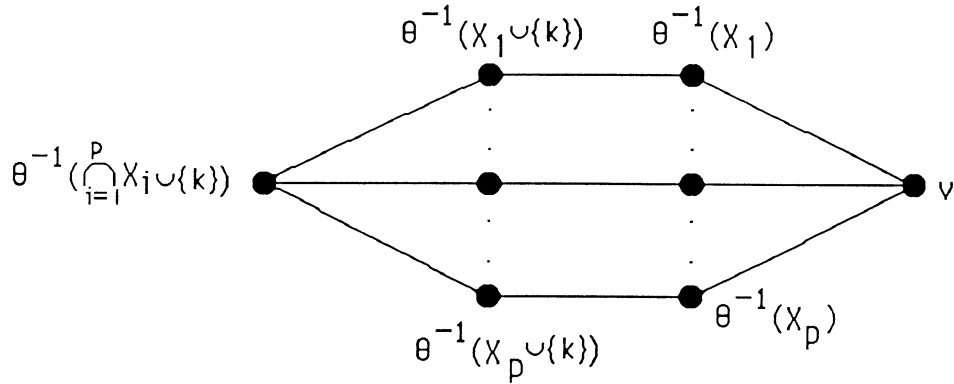


figure 10

Then we have p disjoint 3-paths in G between v and the vertex of Γ_{i-2} mapped to $\bigcap_{i=1, \dots, p} X_i \cup \{k\}$. But $p \geq 3$, with $i \geq 4$, and this not possible. Therefore $|\bigcap_{i=1, \dots, p} X_i| \neq n-2$ and $\bigcup_{i=1, \dots, p} X_i$ is of cardinality n , exactly is in Γ'_{i+1} . Mapping v to $\bigcup_{i=1, \dots, p} X_i$, for all v in Γ_{i+1} , we obtain the required isomorphism between the subgraphs induced by $\Gamma_0, \Gamma_1, \dots, \Gamma_{i+1}$ and $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_{i+1}$.

Assume now i to be odd. If $i=3$ then $X_1 \cap X_2$ is in Γ_{i+1} . If $i>3$, then $p \geq 3$. Assume that $|\bigcup_{i=1, \dots, p} X_i| = n+1$. For all $j \neq 2$, the set $X_1 \cap X_j$ is of cardinal $n-1$ and cannot be in Γ_{i-1} whence is in Γ_{i+1} . Then $X_1 - X_j$ is in A but on the other hand $\bigcup_{i=1, \dots, p} X_i = X_1 \cup X_j$. Therefore $\bigcup_{i=1, \dots, p} X_i - X_j$ is an element of A and by cardinality there is some k in $\bigcup_{i=1, \dots, p} X_i$, hence in $\bigcap_{i=1, \dots, p} X_i$, with $k \notin A$. For all j , let X'_j be the set of elements of X_j distinct from k . All the X'_j are in Γ_{i-1} and $\bigcup_{i=1, \dots, p} X'_i$ is in Γ'_{i-2} (figure 11).

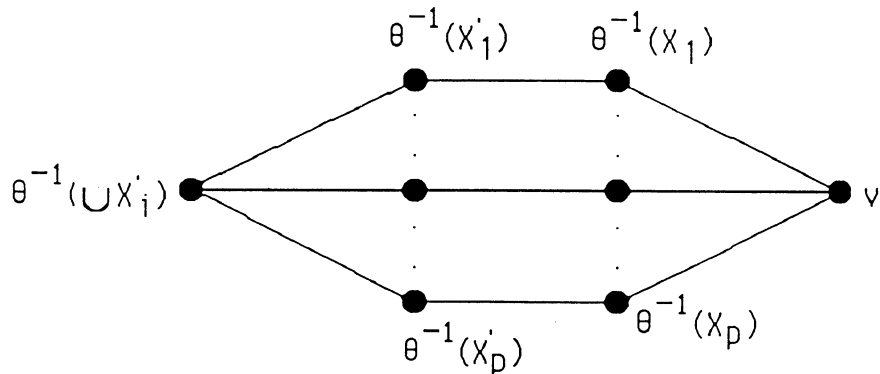


figure 11

There are at least 3 disjoint 3-paths between v and the vertex of Γ_{i-2} mapped to $\bigcup_{i=1, \dots, p} X'_i$ and this is impossible in a $[3,1,6]$ -cycle regular graph. Thus $\bigcap_{i=1, \dots, p} X_i$ is $X_1 \cap X_2$, therefore is in Γ_{i+1} and mapping v to $\bigcap_{i=1, \dots, p} X_i$ gives also an isomorphism

between the subgraphs induced by $\Gamma_0, \Gamma_1, \dots, \Gamma_{i+1}$ and $\Gamma'_0, \Gamma'_1, \dots, \Gamma'_{i+1}$. This ends the proof of the following theorem.

Theorem 17

Let G be $[3,1,6]$ -cycle regular graph of maximum degree n . Then $|V(G)| \leq \binom{2n}{n}$, and $|V(G)| = \binom{2n}{n}$ if and only if G is the subgraph H_n of Q_{2n-1} induced by the central levels Γ_{n-1} and Γ_n .

REFERENCES

1. H. M. Mulder . $(0, \lambda)$ -graphs and n -cubes , Discrete Math. 28(1979) 179-188
2. J.M. Laborde , S.P. Rao Hebbare . An other characterization of hypercubes , Discrete Math. 39(1982) 161-166
3. H.M. Mulder . The Interval Function of a Graph , Math Centre Tracts 132, Mathematisch Centrum, Amsterdam, 1980
4. A. Kowalewski . Topologische Deutung von Buntordnungsproblemen, Sitzungsber. Akad. Wiss. Wien (Abt IIa) 126 (1917) 963-1007

A family of non regular distance monotone graphs

Michel Mollard
LSD(IMAG) BP 68
38041 GRENOBLE CEDEX ,France

Summary We give the construction of a family of non regular distance monotone graphs, graphs previously conjectured to be regular.

0. Introduction and basic notions.

The (O,2)-graphs and the distance monotone graphs (DM-graphs) have been introduced in [1] and [2] , [4] and [5] , respectively, in two characterizations of hypercubes. H.M.Mulder [2] and independently J.M.Laborde-Rao Hebbare [3] proved that (O,2)-graphs are regular. In [5] and [6] the authors introduced the following conjecture.

Conjecture : Every DM-graph G with $d(G) \geq 3$ is regular.

We exhibit a family of counterexamples to this conjecture.

We first recall some definitions introduced in [2] and [5].

For any two vertices u,v in a simple graph G the interval $I(u,v)$ is the set of vertices lying on a shortest u,v -path. Let $d(u,v)$ be the distance between u and v .

A graph G is distance-monotone (DM-graph for short) if each interval $I(u,v)$ verifies $w \in V(G) - I(u,v) \Rightarrow \exists w' \in I(u,v)$ such that $d(w,w') > d(u,v)$.

DM-graphs of diameter 3 can be obtained from $K_{n,n}$ by deletion of a perfect matching [5]. In [6] a matrix representation of DM-graphs of diameter 4 is introduced.

Consider a (0,1)-matrix $M = (m_{i,j})$ fulfilling the following conditions

(1) M has at least 4 rows and 4 columns.

(2) For any 3 different row indices i,j,k there are 4 column indices a,b,c,d such that

$$m_{ia} = m_{ja} \neq m_{ka}$$

$$m_{ib} \neq m_{jb} = m_{kb}$$

$$m_{ic} = m_{kc} \neq m_{jc}$$

$$m_{id} = m_{jd} = m_{kd}$$

(2*) For any 3 different column indices a,b,c there are 4 row indices i,j,k,l such that

$$m_{ia} = m_{ib} \neq m_{ic}$$

$$m_{ja} \neq m_{jb} = m_{jc}$$

$$m_{ka} = m_{kc} \neq m_{kb}$$

$$m_{la} = m_{lb} = m_{lc}$$

To every such a m by n matrix M we associate a graph G of order $2(m+n)$ in the following way:

$$V(G) = \{u_1, u_2, \dots, u_m\} \cup \{u_1', u_2', \dots, u_m'\} \cup \{v_1, v_2, \dots, v_n\} \cup \{v_1', v_2', \dots, v_n'\}$$

$$m_{ij} = 1 \quad \Rightarrow \quad \{u_i, v_j\} \in E(G) \text{ and } \{u_i', v_j\} \in E(G)$$

$$m_{ij} = 0 \quad \Rightarrow \quad \{u_i, v_j\} \in E(G) \text{ and } \{u_i', v_j'\} \in E(G)$$

It is easy to verify that G is a DM-graph of diameter 4, and furthermore all DM-graphs of diameter 4 can be obtained in this way [6].

We are going to construct an $m \times n$ matrix ($m \neq n$) fulfilling the conditions (1),(2) and (2*). In the associated DM-graph vertices u_i, u_i' corresponding to row indices are of degree n and vertices v_i, v_i' corresponding to column indices are of degree m, therefore, the associated DM-graph is not regular.

Let $e_1, e_2, \dots, e_p, e_{p+1}, \dots, e_q$ be some mutually different vectors of $V(p,2)$ the vector space of dimension p over $GF(2)$, such that e_1, e_2, \dots, e_p is a basis of $V(p,2)$. We can associate to these q vectors a $q \times 2^p$ matrix $M = (m_{ij})$ in the following way:

To every vector u_j ($j=1, \dots, 2^p$) in $V(p,2)$ we associate the j^{th} column of M by $m_{i,j} = e_i \cdot u_j = e_{i1}u_{j1} + e_{i2}u_{j2} + \dots + e_{ip}u_{jp}$ where $e_i = (e_{i1}, e_{i2}, \dots, e_{ip})$ and $u_j = (u_{j1}, u_{j2}, \dots, u_{jp})$

in the basis e_1, e_2, \dots, e_p .

Proposition 1. Such a matrix with $q \geq p \geq 2$ and $q \geq 4$ verifies the property (2).

Proof. Consider 3 rows i, j, k , the vectors e_i, e_j, e_k and the two linear mappings from $V(p,2)$ into $V(3,2), V(2,2)$ respectively.

$$f(x) = (e_i \cdot x, e_j \cdot x, e_k \cdot x) \text{ and } g(x) = (e_i \cdot x, e_j \cdot x).$$

If the 3 vectors e_i, e_j, e_k are linearly independent then $f(x)$ ranges over all the vectors of $V(3,2)$ and therefore there are 4 vectors, thus 4 columns with the required submatrix.

If the 3 vectors are linearly dependent then either $e_k = e_i + e_j$ or one of the 3 vectors is 0.

In the first case there are 4 vectors of $V(p,2)$ the images of which by $g(x)$ are the 4 vectors of $V(2,2)$, then f applied on these vectors gives $(0,0,0), (0,1,1), (1,0,1)$ and $(1,1,0)$. The 4 columns associated to these 4 vectors of $V(p,2)$ are those required by the property (2).

In the second case assume $e_k = 0$. There are 4 vectors of $V(p,2)$ the images of which by $g(x)$ are the 4 vectors of $V(2,2)$, the images by f of this 4 vectors are thus $(0,0,0), (0,1,0), (1,0,0)$ and $(1,1,0)$.

□

Example. Let $p=3, q=7$ and $e_4=e_1+e_2, e_5=e_1+e_3, e_6=e_2+e_3, e_7=e_1+e_2+e_3$. We obtain the following 7x8 matrix:

$$(1) \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Proposition 2. The matrix (I) verifies the properties (2) and (2*). The associated DM-graph is therefore of order 30 with 14 vertices of degree 8 and 16 of degree 7.

Proposition 3. For $p \geq 4$ consider the matrix (II) with 2^p columns and $p(p+1)/2$ rows defined as above by the p basis vectors e_1, e_2, \dots, e_p and the $p(p-1)/2$ sums of two basis vectors (we don't need an other row like in (I)).

The matrix (II) verifies the properties (2) and (2*). The associated DM-graph is of order $2^{p+1} + p(p+1)$ with 2^{p+1} vertices of degree $p(p+1)/2$ and $p(p+1)$ of degree 2^p .

The proof is common to the two last propositions:

By proposition 1 we have the property (2). Choose 3 columns i, j, k and consider the values of the first p rows corresponding to the basis vectors. These are nothing else than that the vectors u_i, u_j, u_k expressed in the basis e_1, e_2, \dots, e_p .

First case : we have a row index $\alpha, \alpha \leq p$, with $m_{\alpha i} = m_{\alpha j} = m_{\alpha k}$.

Then there is an other row β (still in the first p rows) such that for example $m_{\beta i} = m_{\beta j} \neq m_{\beta k}$ (because u_i, u_j, u_k are distinct).

Therefore there is a third one γ with $m_{\gamma i} \neq m_{\gamma j} = m_{\gamma k}$ or $m_{\gamma i} \neq m_{\gamma j} \neq m_{\gamma k}$; in both cases the row associated to $e_\beta + e_\gamma$ is the fourth required.

Second case : there is no row index $\alpha, \alpha \leq p$ with $m_{\alpha i} = m_{\alpha j} = m_{\alpha k}$.

If $p=3$ (therefore we study the matrix (I)) we may have :

$$m_{1i} = m_{1j} \neq m_{1k}$$

$$m_{2i} \neq m_{2j} = m_{2k}$$

$$m_{3i} = m_{3k} \neq m_{3j}$$

In this case the 7th row is associated to $e_1 + e_2 + e_3$ and we have $m_{7i} = m_{7j} = m_{7k}$.

If we are not in this case, or if $p > 3$, we have two indices (in the first p ones), say α and β , with

$$\begin{aligned}
m_{\alpha i} &= m_{\alpha j} \neq m_{\alpha k} \\
m_{\beta i} &= m_{\beta j} \neq m_{\beta k} \\
&\text{(possibly permuting } i, j, k \text{)}.
\end{aligned}$$

The vectors u_i and u_j are different, therefore there exist an index $\gamma \leq p$ with

$$m_{\gamma i} \neq m_{\gamma j} \neq m_{\gamma k}$$

or

$$m_{\gamma i} \neq m_{\gamma j} = m_{\gamma k}$$

and we have the property (2*) with the row indices α, γ, δ and ε , with $e_\delta = e_\alpha + e_\beta$ and $e_\varepsilon = e_\beta + e_\gamma$.

Now for $p \geq 4$ let us choose q in $\{p(p+1)/2, \dots, 2^p\}$. If we consider the basis vectors, the sums two by two of those vectors, and $q - p(p+1)/2$ distinct vectors of $V(p, 2)$ different from the previous ones, then the associated q by 2^p matrix verifies property (2) by proposition 1 and (2*) because we only add some rows to the matrix (II).

Therefore we have the following property:

Proposition 4. For $p \geq 4$ and q in $\{p(p+1)/2, \dots, 2^p\}$ there exists a DM-graph with some vertices of degree 2^p and others of degree q .

REFERENCES

1. **J.M. Laborde**. Une caractérisation locale du graphe du n-cube, journées de Combinatoire, C. Benzaken éditeur, Grenoble 1978, 198-200.
2. **H.M. Mulder**. $(0,\lambda)$ graphs and n-cubes , Discrete Math. 28(1979) 179-188.
3. **Rao Hebbare , J.M. Laborde**. Another characterization of hypercubes , Discrete Math. 39(1982) 161-166.
4. **G. Burosh , J.M. Laborde**. Some Intersection Theorems for Structure. To appear in Journal Européen de Combinatoire volume 9 (1988).
5. **G.Burosh , I.Havel , J.M. Laborde** . DM-Graphs and a new characterization of Hypercubes. Discrete Math. (1988) to appear.
6. **I. Havel , J.M. Laborde** . On distance monotone graphs . Colloquia Mathematica Societatis Bolyai 52(1987) 557-561.

Annexe

Proposition:

Let $G=(V,E)$ be a connected graph such that for any two vertices u,v the interval $I(u,v)$ is such that

$$\forall x \in V \quad \exists y \in I(u,v) \text{ such that } \forall z \neq y \text{ in } I(u,v) \quad d(x,z) < d(x,y)$$

then G is a hypercube Q_n for some n .

Proof:

* G is bipartite

Consider an odd cycle of minimal length $x_1, x_2, \dots, x_{l+1}, x_{l+2}, \dots, x_{2l+1}, x_1$

then $I(x_{l+1}, x_{l+2}) = \{x_{l+1}, x_{l+2}\}$ but $d(x_1, x_{l+1}) = d(x_1, x_{l+2}) = l$

* G is a $(0,2)$ graph

Let x,y any two vertices and z a common neighbour then there is an other common neighbour t , else $I(x,y) = \{x,y,z\}$ and $d(z,x) = d(y,z) = 1$

Assume that x,y have a third common neighbour u then $\forall v \in I(x,y)$ we have $d(z,v) \leq 2$; but $d(t,z)=d(u,z)=2$ and t,u belongs to $I(x,y)$.

* in a level decomposition $\Gamma_0, \Gamma_1, \dots, \Gamma_p$, every 4-cycle meets 3

levels

Let $\Gamma_0 = \{x\}$ and u,v,w,t,u a cycle such that $u,w \in \Gamma_i$ and $t,v \in \Gamma_{i+1}$ (G is bipartite thus it is the only case to study) then $I(u,w) = \{u,v,w,t\}$ but $d(x,u)=d(x,w)=i$ and $d(x,v)=d(x,t)=i+1$.

* in a level decomposition $\Gamma_0 = \{x\}, \Gamma_1, \dots, \Gamma_p$ let n be the valency of x

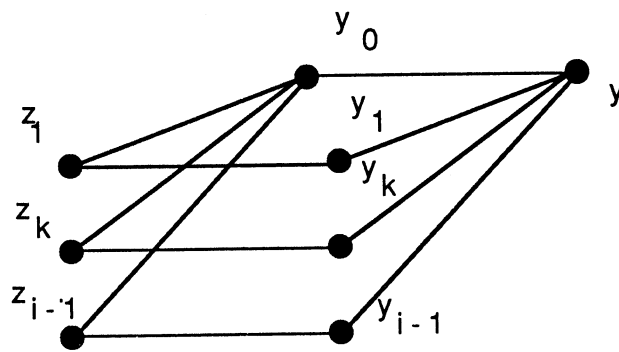
then $|\Gamma_i| = \binom{n}{i}$ and every vertex y in Γ_i has exactly i neighbours in

Γ_{i-1} .

This is clear for $i=0$ and 1 assume the property for $j < i$. Let y in Γ_i and y_0 a

neighbour of y in Γ_{i-1} . By induction hypothesis y_0 has exactly $i-1$ neighbours in Γ_{i-2} say z_1, z_2, \dots, z_{i-1} . For $k = 1$ to $i-1$ the 2-path y, y_0, z_k is closed by a vertex y_k , neighbour of y in Γ_{i-1} . The y_k are all distinct and it is clear that y has no other neighbours in Γ_{i-1} than y_0, y_1, \dots, y_{i-1} because a 4-cycle meet four levels therefore a path y_0, y, t with t in Γ_{i-1} is closed by a vertex in Γ_{i-2} thus a y_k for some k .

There is exactly $i |\Gamma_i|$ edges between Γ_i and Γ_{i-1} ; but on the other hand this number is exactly $|\Gamma_{i-1}| (n-i+1) = \binom{n}{i-1} (n-i+1)$ thus $|\Gamma_i| = \binom{n}{i}$.



* Therefore G is a 0,2 graph of valency n and order 2^n thus is a hypercube.

Chapitre 2

Codes correcteurs d'erreurs parfaits
non linéaires.

Les codes correcteurs d'erreurs sont utilisés pour véhiculer de l'information dans une transmission sujette à des erreurs.

De façon générale un code correcteurs d'erreur de longueur n sur $GF(q)$, corps à q éléments (où q est donc une puissance d'un nombre premier), est un sous ensemble de V_n l'espace vectoriel de dimension n sur $GF(q)$. On considérera souvent un élément du code comme un mot de longueur n sur un alphabet à q éléments et un code binaire de longueur n comme un ensemble de sommets de l'hypercube Q_n .

Un paramètre important des codes correcteurs d'erreurs est la distance minimale entre deux mots quelconques du code. La distance entre deux mots d'un code étant le nombre de composantes distinctes entre les deux vecteurs ou de manière équivalente dans le cas binaire la distance entre sommets de Q_n au sens de la théorie des graphes.

Un code de distance minimale d permet la correction de $\lfloor \frac{d-1}{2} \rfloor$ erreurs.

Soit en effet à transmettre de l'information sous forme de mots binaires de longueur m , on codera ces mots par 2^m éléments d'un code de longueur n , où n est plus grand que m , code choisi pour respecter une certaine distance minimale entre ces éléments.

Le deuxième paramètre d'un code est bien sûr son nombre de mots. Ces deux paramètres sont liés:

Pour tout élément x de V_n , nommons boule de rayon e centrée sur x l'ensemble

$$S(x,e) = \{ y \in V_n / d(x,y) \leq e \}.$$

Dans un code C de distance minimale $2e+1$ les boules de rayon e centrées sur les mots du code sont disjointes. Le cardinal d'une telle boule

$$\text{est } |S| = \sum_{i=0}^e (q-1)^i \binom{n}{i} \text{ et on aura } |C| \leq \frac{q^n}{|S|} .$$

Les codes de distance minimale $2e+1$ tels que les boules de rayon e centrées sur les mots constituent une partition de V_n sont dits parfaits et sont d'un grand intérêt théorique.

Théorème (Tietäväinen [12] et Van Lint [3], [4]).

Il existe un code parfait non trivial de longueur n et de distance minimale d sur $GF(q)$ si et seulement si:

- * $d=3$ $n = \frac{q^m-1}{q-1}$ et q et m quelconques
- * $d=5$ $n=11$ et $q=3$
- * $d=7$ $n=23$ et $q=2$.

En fait dans les deux derniers cas ces codes sont uniques (aux automorphismes près de V_n) et nous ne nous intéresserons qu'aux codes parfaits correcteurs d'une erreur (cas $d=3$).

Remarquons que la condition nécessaire $n = \frac{q^m-1}{q-1}$ pour un certain m provient directement du fait que les boules de rayon 1 sont de cardinal $n(q-1)+1$ et que ce cardinal doit diviser q^n .

On connaît depuis longtemps (pour $q=2$ (Hamming [1]), pour q quelconque (Shapiro, Slotnick [10])) une famille de codes parfaits, les codes de Hamming.

Bien que ce ne soit pas le procédé classique, on peut les définir récursivement dans le cas binaire par:

$$\left\{ \begin{array}{l} H_{p+1} = \{(x, c+x, P(x)) \mid x \in V_{2^p-1}, c \in H_p\} \\ H_1 = \{(0)\} \end{array} \right.$$

où $P(x)$ désigne la fonction parité

$$P((x_1, x_2, \dots, x_n)) = \sum_{i=1}^n x_i \pmod{2}.$$

Ces codes sont dits linéaires car ils constituent un sous espace vectoriel de V_n :

$$0 \in H_p \text{ et si } x, y \in H_p \text{ alors } x+y \in H_p$$

Vasiliev [13] a donné la première construction de codes parfaits binaires non linéaires, construction généralisé à $GF(q)$ par Shönheim [11].

C'est beaucoup plus récemment qu'une nouvelle famille de codes parfaits binaires a été découverte (Laborde[2], Phelps[7]).

Nous nous proposons dans un premier temps de généraliser ces constructions au cas de q quelconque.

Toutes ces familles de codes parfaits non linéaires sont basées sur une construction récursive consistant à passer d'un code parfait de longueur $\frac{q^m-1}{q-1}$ à un code parfait de longueur $\frac{q^{m+1}-1}{q-1}$ comme nous l'avons vu pour les codes de Hamming, en introduisant une 'distorsion' au passage. Pour ce faire on peut remarquer que l'on utilise les translations (Vasiliev[13]) et les permutations de coordonnées (Laborde[2], Phelps[7]), automorphismes de Q_n .

On peut considérer ces constructions comme des produits, produit d'un code parfait de longueur $\frac{q^m-1}{q-1}$ par le code parfait trivial de longueur 1 constitué par le mot (0), fournissant un code parfait de longueur $\frac{q^{m+1}-1}{q-1}$. Il paraît alors intéressant de rechercher à étendre ces notions de produits au produit de 2 codes parfaits non triviaux ; ceci pour obtenir de nouveaux codes parfaits. Un résultat de ce type est dû à K.T. Phelps [8] qui a généralisé son précédent résultat (Phelps [7]) à la construction d'un code parfait binaire de longueur $nm+n+m$ à partir de deux codes parfaits de longueur n et m .

Nous nous sommes intéressé pour notre part à l'autre type de construction en donnant un produit qui permet de généraliser le résultat de Vasiliev.

Ce résultat est étendu au produit de p codes parfaits binaires puis au produit de codes parfaits sur $GF(q)$ où on obtient alors un produit fournissant un code parfait de longueur $(q-1)nm+n+m$ à partir de deux codes parfaits de longueurs n et m .

Ces résultats sont basés sur l'utilisation de fonctions parité généralisées qui, dans le cas binaire, correspondent à une paire d'applications P_1 de V_{nm} dans V_n et P_2 de V_{nm} dans V_m qui si on représente les éléments de V_{nm} sous la forme d'un tableau de coordonnées de n lignes et m colonnes sont les applications correspondant aux sommes respectivement des lignes et des colonnes.

K.T. Phelps [9] a depuis donné un autre type de produit généralisant la construction de Vasiliev pour des codes parfaits sur des alphabets quelconques (q symboles où q n'est pas forcément puissance d'un premier). Précisons cependant que l'on ne connaît pas de tels codes.

Pour terminer mentionnons le lien entre les codes parfaits binaires et la recherche d'absorbants de cardinal minimum de l'hypercube (voir chapitre3), problème précédemment étudié (Mollard[6]) et qui depuis l'a été par A. Lobstein[5].

REFERENCES

- [1] R.W. Hamming, Error detecting and error correcting codes, Bell Syst. Tech. J. 29 (1950) 147-160.
- [2] J.M. Laborde, Une nouvelle famille de codes binaires, parfaits, non linéaires, C.R.Acad. Sc. Paris 297 (1983) 67-70.
- [3] J.H. van Lint, On the non existence of certain perfect codes, in A.O.L. Atkin and B.J. Birch eds., Computers in Number theory, Academic Press, New york (1971) 227-282.
- [4] J.H. van Lint, Non existence theorems for perfect error-correcting codes, in Computers in Algebra and Number theory Vol 4, SIAM-AMS proceedings (1971).
- [5] A. Lobstein, Contributions au codage combinatoire, Thèse de Docteur-ingénieur, ENST Paris (1985).
- [6] M. Mollard, Les Invariants du n cube, Thèse de 3^{ème} Cycle, USTMG Grenoble (1981).
- [7] K.T. Phelps, A Combinatorial Construction of Perfect Codes, SIAM J. Alg. Disc. Meth. 4 (1983) 398-403.
- [8] K.T. Phelps, A General Product Construction For Error Correcting Codes, SIAM J. Alg. Disc. Meth. 5 (1984) 224-228.
- [9] K.T. Phelps, A Product Construction For Perfect Codes Over Arbitrary Alphabets, IEEE Trans. Info.Theory 30 (1984) 769-771.
- [10] H.S. Shapiro, D.L. Slotnick, On the mathematical theory of error correcting codes, IBM J.Res.Develop. 3 (1959) 25-37.
- [11] J. Schönheim, On linear and Nonlinear Single-Error-Correcting q -ary Perfect Codes, Information and Control 12 (1968) 23-26.
- [12] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, SIAM J.Appl. Math. 24 (1973) 88-96.

- [13] J.L. Vasiliev, On nongroup close-packed codes, *Probl. Kibernet.* 8 (1962) 337-339.

A GENERALIZED PARITY FUNCTION AND ITS USE IN THE CONSTRUCTION OF PERFECT CODES*

M. MOLLARD†

Abstract. We define a new generalized parity function, and use it to obtain a product construction of single-error-correcting codes (binary or not).

Key words. combinatorics, error-correcting codes

1. Introduction. Let V_n be the vector space of dimension n over the finite field $GF(q)$. A code of length n is a subset C of V_n . If C is a subspace of V_n the code is called linear. A single-error-correcting code (or distance 3 code) is a code C having the property

$$\forall x \in C, \forall y \in C, \quad d(x, y) \geq 3, \quad \text{or } x = y,$$

where $d(x, y)$ is the Hamming distance between x and y . This is the only kind of code considered here. The Hamming bound states that

$$(1) \quad |C| \leq \frac{q^n}{n(q-1) + 1}.$$

C is called perfect if (1) is an equality. Perfect codes of length n exist if and only if for some m

$$n = \frac{q^m - 1}{q - 1}.$$

The earliest examples of perfect codes are linear ones (Hamming [1] for $q = 2$, Shapiro and Slotnick [2] for the general case). Nonlinear perfect codes have been constructed by Vasiliev [3] ($q = 2$) and Schönheim [4]. Other nonlinear codes are also known.

In this paper we present a product construction for combining codes, based on the use of a "generalized parity function". Starting with binary single-error-correcting codes of lengths n, m this construction gives us a single-error-correcting code of length $nm + n + m$. But our purpose here is to construct perfect codes, so we will only apply it to such codes.

Phelps [5] has also introduced a product construction which generalizes his "combinatorial construction of perfect codes" [6]. However, when compared to Vasiliev's construction, Phelps' appears as being of a very different nature: we think that, more than likely, it cannot produce the Vasiliev codes, while their generalization is precisely our aim.

2. Product construction in the binary case. Let n_1, n_2 be integers.

DEFINITION. The generalized parity function $(P_1(x), P_2(x))$ from $V_{n_1 n_2}$ to $V_{n_1 + n_2}$ is defined by

$$P_1(x) = \left(\sum_{j=1}^{n_2} x_{ij} \right), \quad i \in \{1, \dots, n_1\},$$

$$P_2(x) = \left(\sum_{i=1}^{n_1} x_{ij} \right), \quad j \in \{1, \dots, n_2\},$$

* Received by the editors December 15, 1983 and in revised form November 26, 1984.

† Laboratoire LSD (IMAG), 38402, St. Martin d'Hères Cédex, France.

where the components of x , an element of $V_{n_1 n_2}$, are $(x_{11}, \dots, x_{1n_2}, x_{21}, \dots, x_{n_1 n_2})$, i.e. the coordinate positions of x are arranged in lexicographic order over $\{1 < \dots < n_1\} \times \{1 < \dots < n_2\}$.

Let C and C' be perfect codes of lengths n_1, n_2 , and let f be a vector function from C to V_{n_2} . Now define F as

$$F = \{(x, c + P_1(x), c' + P_2(x) + f(c))\},$$

where $x \in V_{n_1 n_2}$, $c \in C$, and $c' \in C'$.

THEOREM 1. F is a single-error-correcting perfect code of length $n = n_1 n_2 + n_1 + n_2$.

Remark. Two important particular cases are:

- 1) f is a constant value function,
- 2) $n_2 = 1$, then $P_1(x) = x$, $P_2(x) = P(x)$ the classical parity function; this is Vasiliev's construction.

Proof of Theorem 1. First notice that for some a and b

$$n_1 = 2^a - 1, \quad n_2 = 2^b - 1,$$

and so

$$n = n_1 n_2 + n_1 + n_2 = 2^{a+b} - 1.$$

The number of vectors in F is

$$|F| = 2^{n_1 n_2} \frac{2^{n_1}}{n_1 + 1} \frac{2^{n_2}}{n_2 + 1} = \frac{2^n}{n + 1}.$$

Therefore, if F is single-error-correcting, it must be perfect. Let a and \bar{a} be two different vectors of F . We have to show that $d(a, \bar{a}) \geq 3$. For some $x, \bar{x}, c, \bar{c}, c', \bar{c}'$ we can write

$$a = (x, c + P_1(x), c' + P_2(x) + f(c)),$$

$$\bar{a} = (\bar{x}, \bar{c} + P_1(\bar{x}), \bar{c}' + P_2(\bar{x}) + f(\bar{c})).$$

- a) If $x = \bar{x}$, then $P_1(x) = P_1(\bar{x})$, $P_2(x) = P_2(\bar{x})$ and $d(a, \bar{a}) = d(c, \bar{c}) + d(c', \bar{c}') \geq 3$.
- b) If $d(x, \bar{x}) = 1$, then $d(P_1(x), P_1(\bar{x})) = d(P_2(x), P_2(\bar{x})) = 1$. If $c \neq \bar{c}$, then $d(c + P_1(x), \bar{c} + P_1(\bar{x})) \geq 2$ and $d(a, \bar{a}) \geq 3$. If $c = \bar{c}$, then $d(\bar{c}' + P_2(\bar{x}) + f(\bar{c}), c' + P_2(x) + f(c)) \geq 1$ and again $d(a, \bar{a}) \geq 3$.
- c) If $d(x, \bar{x}) = 2$, then $d(P_1(x), P_1(\bar{x}))$ and $d(P_2(x), P_2(\bar{x}))$ are 0 or 2 but both cannot be zero at the same time. Therefore, the equalities
 - 1) $c + P_1(x) = \bar{c} + P_1(\bar{x})$,
 - 2) $c' + P_2(x) + f(c) = \bar{c}' + P_2(\bar{x}) + f(\bar{c})$,
 are not compatible and $d(a, \bar{a}) \geq 3$.
- d) The trivial case $d(x, \bar{x}) \geq 3$ ends the proof.

Let C_1, C_2, \dots, C_p be perfect codes of lengths n_1, n_2, \dots, n_p and let

$$m = \prod_{i=1}^p (n_i + 1) - \sum_{i=1}^p n_i - 1.$$

We can define a family of functions R_k ($k \in \{1, 2, \dots, p\}$) from V_m to V_{n_k} , playing the part of a parity function, and use it to build perfect codes of length $\prod_{i=1}^p (n_i + 1) - 1$. The interested reader can find this generalization of the above construction in [8].

3. General construction. Finally, we are going to state a generalization to perfect codes over finite fields, and so generalize Schönheim's construction. A different generalization, over arbitrary alphabets, recently has been developed by Phelps [7].

Let q be a power of a prime and let a_i ($i = 1, 2, \dots, q-1$) be the nonzero elements of $GF(q)$ in a fixed order. For two integers n_1, n_2 arrange the coordinate positions of x , a word of $V_{(q-1)n_1n_2}$ in the lexicographic order over

$$\{1, \dots, q-1\} \times \{1, \dots, n_1\} \times \{1, \dots, n_2\}.$$

$P_1(x)$ will be the function from $V_{(q-1)n_1n_2}$ to V_{n_1} defined by

$$P_1(x) = (y_1, \dots, y_j, \dots, y_{n_1}),$$

where

$$y_j = \sum_{i=1}^{q-1} \sum_{k=1}^{n_2} x_{ijk}.$$

$P_2(x)$ will be from $V_{(q-1)n_1n_2}$ to V_{n_2} defined by

$$P_2(x) = (y_1, \dots, y_k, \dots, y_{n_2}),$$

where

$$y_k = \sum_{i=1}^{q-1} a_i \sum_{j=1}^{n_1} x_{ijk}.$$

THEOREM 2. Let C and C' be two perfect codes of lengths n_1, n_2 and let f be a function from C to V_{n_2} . F is a perfect code over $V_{(q-1)n_1n_2+n_1+n_2}$ where

$$F = \{(x, c + P_1(x), c' + P_2(x) + f(c)), \quad x \in V_{(q-1)n_1n_2}, \quad c \in C, \quad c' \in C'\}.$$

A proof of this theorem can be found in [8]. We only remark here that for $n_2 = 1$ we obtain the Schönheim nonlinear perfect codes.

REFERENCES

- [1] R. W. HAMMING, *Error detecting and error correcting codes*, Bell Syst. Tech. J., 29 (1950), pp. 147-160.
- [2] H. S. SHAPIRO and D. L. SLOTNICK, *On the mathematical theory of error correcting codes*, IBM J. Res. Develop., 3 (1959), pp. 25-37.
- [3] L. VASILIEV JR., *On nongroup close-packed codes*, 8 (1962), pp. 337-339.
- [4] J. SCHÖNHEIM, *On linear and nonlinear single-error-correcting q-nary perfect codes*, INFORM. and Control, 12 (1968), pp. 23-26.
- [5] K. T. PHELPS, *A general product construction for error correcting codes*, this Journal, 5 (1984), pp. 224-228.
- [6] ———, *A combinatorial construction of perfect codes*, this Journal, 4 (1983), pp. 398-403.
- [7] ———, *A product construction for perfect codes over arbitrary alphabets*, IEEE Trans. Inform. Theory, to appear.
- [8] M. MOLLARD, *Une généralisation de la fonction parité, application à la construction de codes parfaits*, R.R. no 395, Laboratoire de Mathématiques Appliquées de Grenoble, Grenoble, France.

COMMUNICATION

**UNE NOUVELLE FAMILLE DE 3-CODES
PARFAITS SUR $GF(q)$**

M. MOLLARD

*Université Scientifique et Médicale de Grenoble, Laboratoire IMAG, BP No. 68, 38402 St Martin
d'Hères Cedex, France*

Communicated by J.C. Bermond

Received 31 October 1983

A recent new construction of binary single error perfect codes is generalized over $GF(q)$.
These codes are in general non equivalent to linear codes.

1. Introduction

Les travaux concernant les 3-codes parfaits sur $GF(q)$ remontent à 1959. C'est à cette époque que Shapiro et Slotnick [1] ont généralisé les codes de Hamming.

Schönheim [2] a prouvé l'existence de 3-codes parfaits non linéaires en généralisant la construction de Vasiliev. Plus récemment Phelps [3] et J.M. Laborde [4] ont construit une nouvelle famille de 3-codes parfaits binaires. Nous nous proposons de généraliser cette construction à $GF(q)$, q puissance d'un nombre premier.

2. Notations et définitions

Soit q une puissance d'un nombre premier et soit $GF(q)$ le corps de Galois à q éléments.

Soit V_n l'espace vectoriel de dimension n sur $GF(q)$. Un code sur $GF(q)$ est un sous ensemble de V_n .

V_n est muni de la distance de Hamming: 2 éléments de V_n , x et y , sont à la distance d s'ils diffèrent en d composantes.

Un 3-code C est un code tel que 2 éléments distincts de C sont au moins à distance 3.

Nous désignerons par B_n la boule unité de V_n , ensemble des vecteurs à distance

au plus 1 du vecteur nul.

$$|B_n| = n(q-1) + 1.$$

La fonction parité $P(v)$ est définie de V_n sur $\text{GF}(q)$ par

$$P(v) = \sum_{i=1}^n x_i \quad \text{où } v = (x_1, \dots, x_n).$$

La fonction parité généralisée est définie de $(V_n)^{q-1}$ sur $\text{GF}(q)$ par

$$P(\{v_1, \dots, v_{q-1}\}) = \sum_{i=1}^{q-1} i \cdot P(v_i).$$

Théorème (Shapiro et Slotnick). *Il existe un 3-code parfait sur V_n si et seulement si il existe un entier m tel que $n = (q^m - 1)/(q - 1)$ (un 3-code parfait C est un code tel que $|C| \cdot |B_n| = |V_n|$).*

3. Construction

Soit n de la forme $(q^m - 1)/(q - 1)$. Soient $C_0, \dots, C_{n(q-1)}$ et $D_0, \dots, D_{n(q-1)}$ deux partitions de V_n en 3-codes parfaits (non forcément linéaires). Posons

$$F = \{(v_1, \dots, v_{q-1}, P(\{v_1, \dots, v_{q-1}\}), v_q)\}$$

où $v_i \in V_n$ pour $i = 1, \dots, q$ et $\exists j$ tel que $v_q \in D_j$ et $\sum_{i=1}^{q-1} v_i \in C_j$.

Théorème. *F est un 3-code parfait de V_{qn+1} .*

Démonstration

$$|F| = (q^n)^{q-1} \cdot \frac{q^n}{1+n(q-1)} = \frac{q^{nq}}{1+n(q-1)}.$$

Or $q(1+n(q-1)) = 1+(nq+1)(q-1) = |B_{qn+1}|$. D'où

$$F = |V_{qn+1}| / |B_{qn+1}|.$$

Donc si F est un 3-code, c'est un 3-code parfait de V_{qn+1} . Soient x et y deux éléments de F montrons que $d(x, y) \geq 3$.

$$\begin{aligned} x &= (v_1, \dots, v_{q-1}, P(\{v_1, \dots, v_{q-1}\}), v_q) && \text{avec } v_q \in C_j, \\ y &= (w_1, \dots, w_{q-1}, P(\{w_1, \dots, w_{q-1}\}), w_q) && \text{avec } w_q \in C_k. \end{aligned}$$

Nous allons étudier les différentes valeurs possibles de

$$d((v_1, \dots, v_{q-1}), (w_1, \dots, w_{q-1})).$$

Il est clair que si cette distance est supérieure à 2 nous aurons $d(x, y) \geq 3$.

$$1er \text{ cas: } d((v_1, \dots, v_{q-1}), (w_1, \dots, w_{q-1})) = 0.$$

On a alors $v_i = w_i$ pour $i = 1, \dots, q-1$. $P(\{v_1, \dots, v_{q-1}\}) = P(\{w_1, \dots, w_{q-1}\})$ donc $d(x, y) = d(v_q, w_q)$. Or $\sum_{i=1}^{q-1} v_i = \sum_{i=1}^{q-1} w_i$, donc $j = k$ et v_q et w_q sont dans le même code. D'où $x = y$ ou $d(x, y) \geq 3$.

$$2^{\text{ème cas}}: d((v_1, \dots, v_{q-1}), (w_1, \dots, w_{q-1})) = 1.$$

Soit $k \in \{1, \dots, q-1\}$ tel que $v_k \neq w_k$. k est donc unique et $d(v_k, w_k) = 1$. v_k et w_k diffèrent donc en une seule composante $v_{kl} \neq w_{kl}$.

$$P(\{v_1, \dots, v_{q-1}\}) - P(\{w_1, \dots, w_{q-1}\}) = k(P(v_k) - P(w_k)) = k(v_{kl} - w_{kl}) \neq 0.$$

D'autre part $d(\sum_{i=1}^{q-1} v_i, \sum_{i=1}^{q-1} w_i) = 1$, donc v_q et w_q ne sont pas dans le même code. D'où $d(v_q, w_q) \geq 1$ et $d(x, y) \geq 3$.

$$3^{\text{ème cas}}: d((v_1, \dots, v_{q-1}), (w_1, \dots, w_{q-1})) = 2.$$

(a) $\exists j$ tel que $d(v_j, w_j) = 2$. On a alors

$$d\left(\sum_{i=1}^{q-1} v_i, \sum_{i=1}^{q-1} w_i\right) = d(v_j, w_j) = 2,$$

donc v_q et w_q ne sont pas dans le même code donc sont différents et $d(x, y) \geq 3$.

(b) $\exists j$ et k tels que $d(v_j, w_j) = d(v_k, w_k) = 1$. Si $v_j - w_j \neq w_k - v_k$ on a

$$d\left(\sum_{i=1}^{q-1} v_i, \sum_{i=1}^{q-1} w_i\right) = 1 \text{ ou } 2,$$

donc v_q et w_q ne sont pas dans le même code donc sont différents et $d(x, y) \geq 3$.

On peut donc supposer $v_j - w_j = w_k - v_k$, donc $P(v_j) - P(w_j) = P(w_k) - P(v_k)$. On a alors $\sum_{i=1}^{q-1} v_i = \sum_{i=1}^{q-1} w_i$ et $d(x, y) < 3$ si et seulement si

$$\begin{aligned} P(\{v_1, \dots, v_{q-1}\}) &= P(\{w_1, \dots, w_{q-1}\}), \\ P(\{v_1, \dots, v_{q-1}\}) - P(\{w_1, \dots, w_{q-1}\}) &= j(P(v_j) - P(w_j)) + k(P(v_k) - P(w_k)) \\ &= (j - k)(P(v_j) - P(w_j)). \end{aligned}$$

Or $j \neq k$ et puisque $d(v_j, w_j) = 1$, $P(v_j) \neq P(w_j)$. Donc $(j - k)(P(v_j) - P(w_j)) \neq 0$ et $d(x, y) \geq 3$. F est donc un 3-code de V_{qn+1} .

Remarque. Désignons par b_i , $i = 0, 1, \dots, n(q-1)$ les éléments de la boule unité B_n . Soit σ une permutation sur $\{0, 1, \dots, n(q-1)\}$. Soient C et C' deux codes parfaits sur V_n . Alors comme cas particulier du théorème précédent, E est un 3-code parfait où:

$$E = \{(v_1, \dots, v_{q-2}, c + b_j - \sum_{i=1}^{q-2} v_i, P(\{v_1, \dots, v_{q-1}\}), c' + b_{\sigma j})\}$$

$$\text{où } v_i \in V_n, j \in \{0, \dots, n(q-1)\}, \quad c \in C, \quad c' \in C'.$$

On peut montrer que les codes obtenus ne sont pas équivalents à des codes linéaires.

Références

- [1] H.S. Shapiro et D.L. Slotnick, On the mathematical theory of error correcting codes, *IBM J. Res. Develop.* 3 (1959) 25–37.
- [2] J. Schönheim, On linear single error correcting q -nary perfect codes, *Information and Control* 12 (1968) 23–26.
- [3] K.T. Phelps, A combinatorial construction of perfect codes, School of Mathematics, Georgia Institute of Technology, Atlanta (1982).
- [4] J.M. Laborde, Une nouvelle famille de codes binaires parfaits non linéaires, C.R.A.S., Scéance du 2 mai 1983.

UNE GENERALISATION DE LA FONCTION PARITE
APPLICATION A LA CONSTRUCTION DE CODES PARFAITS

M.MOLLARD

Laboratoire IMAG

BP 68

38402 St Martin d'Hères Cedex

France

Résumé

Nous introduisons une généralisation de la fonction parité . Grace à cette définition nous donnons une construction qui permet de combiner plusieurs codes pour obtenir une nouvelle famille de codes parfaits (binaires ou non) .

Abstract

We give the definition of a new generalized parity function , and use it to obtain a product construction of single error-correcting perfect codes (binary or not) .

Mots clefs

Combinatoire , codes correcteurs d'erreurs

1 INTRODUCTION

Soit q une puissance d'un nombre premier ($q \geq 2$) et soit $GF(q)$ le corps de Galois à q éléments .

Désignons par V_n l'espace vectoriel de dimension n sur $GF(q)$. Un cas particulier important est celui où $q = 2$, nous identifierons alors V_n au n -cube Q_n .

V_n est muni de la distance de Hamming : 2 éléments x et y de V_n sont à la distance d si ils diffèrent en exactement d composantes . Cette distance est notée $d(x,y)$.

Un code à distance 3 de V_n est un ensemble C d'éléments de V_n tel que :

$$\forall x \in C, \forall y \in C \quad d(x,y) \geq 3$$

Nous n'étudierons par la suite que des codes à distance 3 que nous appellerons simplement "codes" .

Il est facile de montrer que :

$$(1) \quad |C| \leq \frac{q^n}{n(q-1) + 1}$$

C est dit code parfait si l'inégalité (1) est une égalité .

On peut montrer qu'il existe un code parfait sur V_n si et seulement si il existe un entier m tel que :

$$n = \frac{q^m - 1}{q - 1}$$

(Hamming [1] pour $q = 2$ puis Shapiro et Slotnick [2] pour le cas général) .

Les exemples alors construits étaient tous des codes linéaires . Vasiliev [3] pour $q = 2$ puis Schönheim [4] ont donné des exemples de codes parfaits non équivalents à des codes linéaires .

Ces 2 constructions utilisent la technique suivante : à partir d'un code parfait de V_n construire une famille de codes parfaits de V_{nq+1} ceci en utilisant la fonction parité et sa généralisation à $(V_n)^{q-1}$.

Nous nous proposons d'étendre cette technique en construisant une famille de codes parfaits de V_n à partir de deux codes parfaits de longueur n_1 et n_2 (avec $n = (q-1)n_1n_2 + n_1 + n_2$); où même à partir de plus de deux codes .

Phelps [5] a donné un autre procédé de construction d'un code parfait binaire à partir de deux codes ; mais son procédé est totalement différent puisqu'il généralise sa construction combinatoire de codes parfaits., alors que notre procédé généralise les codes de Vasiliev ; deux familles de codes parfaits de nature différente .

Dans le 2^{em} chapitre nous définirons l'outil nécessaire à notre construction, la généralisation de la fonction parité .

Le 3^{em} chapitre est consacré à la construction pour $q = 2$; résultat étendu au cas général dans le dernier chapitre .

2 GENERALISATION DE LA NOTION DE FONCTION PARITE

Rappel

Q_n désignant l'espace vectoriel de dimension n sur $GF(2)$ la fonction parité est classiquement définie comme l'application à valeurs dans $GF(2)$ qui à un élément $x = (x_1 \dots x_n)$ de Q_n

$$\text{associe } P(x) = \sum_{i=1}^n x_i \quad .$$

Remarque

L'ensemble des mots de Q_{2n+1} de la forme $(x, x, P(x))$ où x parcourt Q_n forme un code à distance 3 de Q_{2n+1} .

Définition 1

Soient n_1 et n_2 deux entiers positifs tels que $n = n_1 \cdot n_2$. Nous définirons P_1 et P_2 de la manière suivante :

P_1 est une application à valeurs dans Q_{n_1} qui à un élément $x = (x_1 \dots x_n)$ de Q_n associe $P_1(x) = (y_1 \dots y_{n_1})$ où pour $i=1, \dots, n_1$

$$y_i = \sum_{j=1}^{n_2} x_{n_2(i-1)+j}$$

P_2 est une application à valeurs dans Q_{n_2} qui à un élément $x = (x_1 \dots x_n)$ de Q_n associe $P_2(x) = (y_1 \dots y_{n_2})$ où pour $j=1, \dots, n_2$

$$y_j = \sum_{i=1}^{n_1} x_{n_2(i-1)+j}$$

Remarque

Ceci revient à indexer les coordonnées des éléments x de Q_n (dans la base canonique) suivant l'ordre lexicographique sur $\{1, \dots, n_1\} \times \{1, \dots, n_2\}$ en posant :

$$x = (x_{11} \dots x_{1n_2} x_{21} \dots x_{2n_2} \dots x_{n_1 n_2}) .$$

On a alors

$$P_1(x) = \left(\sum_{j=1}^{n_2} x_{ij} \right)_{i \in \{1 \dots n_1\}}$$

$$P_2(x) = \left(\sum_{i=1}^{n_1} x_{ij} \right)_{j \in \{1 \dots n_2\}}$$

Une deuxième interprétation revient à disposer les coordonnées de x sur un tableau $n_1 \times n_2$. P_1 représente alors la somme ligne par ligne, P_2 la somme colonne par colonne.

Proposition 1

L'ensemble des mots de $Q_{(n_1+1)(n_2+1)-1}$ de la forme $(x, P_1(x), P_2(x))$ est un code à distance 3.

En effet $(n_1+1)(n_2+1)-1 = n_1n_2 + n_1 + n_2$ et si x et \bar{x} sont deux éléments de $Q_{n_1n_2}$:

- * si $d(x, \bar{x}) = 0$ $P_1(x) = P_1(\bar{x})$ et $P_2(x) = P_2(\bar{x})$
- * si $d(x, \bar{x}) = 1$ $P_1(x) \neq P_1(\bar{x})$ et $P_2(x) \neq P_2(\bar{x})$
- * si $d(x, \bar{x}) = 2$ $P_1(x) \neq P_1(\bar{x})$ ou $P_2(x) \neq P_2(\bar{x})$ (il est en effet trivial de vérifier que les deux égalités sont incompatibles en se plaçant dans la dernière interprétation de P_1 et P_2).

Dans tous les cas $d((x, P_1(x), P_2(x)), (\bar{x}, P_1(\bar{x}), P_2(\bar{x}))) \geq 3$ ou est nulle.

Remarque

La fonction parité habituelle correspond à $P_1(x)$ pour $n_1 = 1$ et $n_2 = n$.

Nous allons généraliser cette définition :

Définition 2

Soient $n_1 \dots n_p$ des entiers tels que $n = \prod_{i=1}^p n_i$ ($p \geq 2$)

Posons $I = \{1, \dots, p\}$.

Indiquons les coordonnées d'un élément x de Q_n suivant l'ordre lexicographique de $\{1, \dots, n_1\} \times \{1, \dots, n_2\} \times \dots \times \{1, \dots, n_p\}$

Nous écrirons $x = (x_{i_1 i_2 \dots i_p} \quad i_1 i_2 \dots i_p)$.

Pour chaque k dans I nous définirons une fonction parité P_k de Q_n dans Q_{n_k} par : $P_k(x) = (y_1 \dots y_j \dots y_{n_k})$ où

$$y_j = \sum_{i_1 \dots i_{k-1} i_{k+1} \dots i_p} x_{i_1 \dots i_{k-1} j i_{k+1} \dots i_p}$$

Pour $I' \subset I$ et $k \in I'$ nous noterons également P_k la fonction parité de $Q_{\prod_{i \in I'} n_i}$ dans Q_{n_k} construite par le même procédé en indiquant les coordonnées de $Q_{\prod_{i \in I'} n_i}$ suivant l'ordre induit par l'ordre lexicographique de

$$\{1, \dots, n_1\} \times \{1, \dots, n_2\} \times \dots \times \{1, \dots, n_p\}$$

Proposition 2

Posons $m = \prod_{i \in I} (n_i + 1) - 1$

Désignons par $I = \{I_1 \dots I_{2^p - p - 1}\}$ l'ensemble des parties de I de cardinal au moins 2 ($I = I_1$ par convention) .

Soit F l'ensemble des mots de Q_m de la forme

$$(x_{I_1} \dots x_{I_{2^p - p - 1}} \quad \sum_{I_j \in I / 1 \in I_j} P_1(x_{I_j}) \dots \sum_{I_j \in I / p \in I_j} P_p(x_{I_j}))$$

Où pour tout j dans $\{1, \dots, 2^p - p - 1\}$ x_{I_j} parcourt $Q_{\prod_{k \in I_j} n_k}$

F est un code à distance 3 de Q_m

les mots de F sont bien dans Q_m puisque :

$$m = \prod_{i \in I} (n_i + 1) - 1 = \sum_{I' \subset I} \prod_{i \in I'} n_i = \sum_{I' \in I} \prod_{i \in I'} n_i + \sum_{i \in I} n_i$$

Montrons que deux mots a et \bar{a} de F sont à distance 3

a correspondant au choix $(x_{I_1} \dots x_{I_{2^{p-1}}})$

\bar{a} correspondant au choix $(\bar{x}_{I_1} \dots \bar{x}_{I_{2^{p-1}}})$

Pour $k = 1, \dots, 2^{p-1}$ posons $d_k = d(x_{I_k}, \bar{x}_{I_k})$

*Soit tous les d_k sont nuls et on aura $a = \bar{a}$

*Soit il existe un seul d_k non nul et de plus $d_k = 1$

alors pour tout élément l de I_k , $P_l(x_{I_k}) \neq P_l(\bar{x}_{I_k})$ et donc

$$\sum_{I_j \in I / l \in I_j} P_l(x_{I_j}) \neq \sum_{I_j \in I / l \in I_j} P_l(\bar{x}_{I_j})$$

I_k étant de cardinal au moins 2 on aura $d(a, \bar{a}) \geq 3$

*Soit il existe un seul d_k non nul et de plus $d_k = 2$

Il existe alors nécessairement l dans I_k tel que

$$P_l(x_{I_k}) \neq P_l(\bar{x}_{I_k})$$

car les égalités $\forall l \in I_k, P_l(x_{I_k}) = P_l(\bar{x}_{I_k})$ sont incompatibles

On aura par conséquent

$$\sum_{I_j \in I / l \in I_j} P_l(x_{I_j}) \neq \sum_{I_j \in I / l \in I_j} P_l(\bar{x}_{I_j})$$

*Soit il existe d_k et $d_{k'}$ non nuls avec $d_k = d_{k'} = 1$

Soit l tel que $l \in I_k$ et $l \notin I_{k'}$, (si $I_k \subset I_{k'}$, on intervertit les rôles de k et k').

On aura $P_1(x_{I_k}) \neq P_1(\bar{x}_{I_k})$ et donc :

$$\sum_{I_j \in I / 1 \in I_j} P_1(x_{I_j}) \neq \sum_{I_j \in I / 1 \in I_j} P_1(\bar{x}_{I_j})$$

*Soit $2^{\sum_{k=1}^{p-1} d_k} \geq 3$ et trivialement $d(a, \bar{a}) \geq 3$

3 APPLICATION AUX CODES PARFAITS BINAIRES

Vasiliev [3] a fourni une construction permettant à partir d'un code parfait C de Q_n de construire une famille de codes parfaits de Q_{2n+1} . L'intérêt de cette construction est de pouvoir construire des codes parfaits non équivalents à des codes linéaires.

Donnons cette construction pour mémoire :

Soit f une application de C dans $GF(2)$.

L'ensemble des mots de la forme $(x, c+x, P(x)+f(c))$ où x parcourt Q_n et c parcourt C est un code parfait de Q_{2n+1} .

Nous allons utiliser les définitions étendues de la fonction parité pour donner des constructions permettant d'obtenir de nouveaux codes parfaits à partir de plusieurs déjà connus.

Théorème 1

Soient C et C' deux codes parfaits de respectivement Q_{n_1} et Q_{n_2} (n_1 et n_2 entiers positifs). Soit f une application quelconque de C dans Q_{n_2} .

Posons $n = (n_1+1)(n_2+1)-1$.

L'ensemble F des mots de la forme

$$(x, c + P_1(x), c' + P_2(x) + f(c))$$

où x parcourt Q_{n_1, n_2} , c et c' parcourent respectivement C et C' est un code parfait de Q_n .

Notons l'important cas particulier f fonction constante ou nulle.

Remarque

Nous avons déjà montré que les mots de la forme $(x, P_1(x), P_2(x))$ forment un code à distance 3 .

Démonstration

Remarquons au préalable que n_1 et n_2 sont nécessairement de la forme $n_1 = 2^a - 1$ $n_2 = 2^b - 1$ pour deux entiers a et b (condition nécessaire à l'existence de codes parfaits) et que n possède bien la forme requise puisque :

$$n = n_1 n_2 + n_1 + n_2 = (n_1 + 1)(n_2 + 1) - 1 = 2^{a+b} - 1$$

Un mot de F est déterminé de manière unique par la donnée de x , c et c' . Donc :

$$|F| = 2^{n_1 n_2} \cdot \frac{2^{n_1}}{n_1 + 1} \cdot \frac{2^{n_2}}{n_2 + 1} = \frac{2^n}{n + 1}$$

Si F est un code à distance 3 c'est donc un code parfait .

Montrons que deux mots a et \bar{a} de F sont au moins à distance 3 .

$$\text{Posons } a = (x, c + P_1(x), c' + P_2(x) + f(c))$$

$$\bar{a} = (\bar{x}, \bar{c} + P_1(\bar{x}), \bar{c}' + P_2(\bar{x}) + f(\bar{c}))$$

Il est clair que si $d(x, \bar{x}) \geq 3$ on aura $d(a, \bar{a}) \geq 3$.

* $x = \bar{x}$. On a alors $P_1(x) = P_1(\bar{x})$ $P_2(x) = P_2(\bar{x})$

$a + \bar{a}$ s'écrit alors $(0, c + \bar{c}, c' + \bar{c}' + f(c) + f(\bar{c}))$ vecteur soit nul soit de poids au moins 3 .

* $d(x, \bar{x}) = 1$. On a alors $d(P_1(x), P_1(\bar{x})) = d(P_2(x), P_2(\bar{x})) = 1$

-Si $c = \bar{c}$ alors ou $c' = \bar{c}'$ et $d(a, \bar{a}) = 3$ ou $c' \neq \bar{c}'$ et $d(a, \bar{a}) \geq 4$

-Si $c \neq \bar{c}$ alors $d(c + P_1(x), c + P_1(\bar{x})) \geq 2$ donc $d(a, \bar{a}) \geq 3$.

* $d(x, \bar{x}) = 2$. $d(P_1(x), P_1(\bar{x}))$ et $d(P_2(x), P_2(\bar{x}))$ sont alors

soit nuls soit égaux à 2 . (le cas $P_1(x)=P_1(\bar{x})$ et $P_2(x)=P_2(\bar{x})$ étant exclu). Dans tous les cas :

- Si $c = \bar{c}$ alors ou $c' = \bar{c}'$ et $d(a, \bar{a}) \geq 4$
ou $c' \neq \bar{c}'$ et $d(a, \bar{a}) \geq 3$
- Si $c \neq \bar{c}$ alors $d(a, \bar{a}) \geq 3$

Remarque

La construction $(x, c+x, P(x))$ et la construction de Vasiliev sont des cas particuliers du théorème 1 où on prend un singleton comme code sur Q_1 .

Théorème 2

Soient C_1, C_2, \dots, C_p des codes parfaits de longueur respectivement n_1, n_2, \dots, n_p .

Pour $i=1, \dots, p-1$ soit f_i une application de $\prod_{j=1}^i C_j$ dans $Q_{n_{i+1}}$

Posons à nouveau $I = \{1, \dots, p\}$ et $I = \{I_1 \dots I_{2^{p-p-1}}\}$ ensemble des parties de I de cardinal au moins 2 (avec $I = I_1$ par convention) .

Posons $m = \prod_{i \in I} (n_i + 1) - 1$

Soit F l'ensemble des mots de Q_m de la forme

$$(x_{I_1}, \dots, x_{I_{2^{p-p-1}}}, c_1 + \sum_{I_j \in I / 1 \in I_j} P_1(x_{I_j}), \dots, c_i + \sum_{I_j \in I / i \in I_j} P_i(x_{I_j}) + f_{i-1}(c_1, c_2, \dots, c_{i-1}) \dots c_p + \sum_{I_j \in I / p \in I_j} P_p(x_{I_j}) + f_{p-1}(c_1, \dots, c_{p-1}))$$

où pour tout j dans $\{1, \dots, 2^{p-p-1}\}$ x_{I_j} parcourt $Q_{\prod_{i \in I_j} n_i}$ et

pour tout i dans $\{1, \dots, p\}$ c_i parcourt C_i .

F est un code parfait .

Il convient là aussi de mentionner l'important cas particulier où les f_i sont nulles .

Démonstration

Remarquons que m est bien un entier pour lequel il existe des codes parfaits sur Q_m ; ceci car :

$$\forall i \exists a_i \in \mathbb{N} \text{ tel que } n_i = 2^{a_i-1} \sum a_i$$

$$\text{et } m = \prod_{i \in I} (n_i + 1) - 1 = 2^{\sum_{i \in I} a_i} - 1$$

D'autre part les éléments de F sont bien des mots de longueur m puisque $m = \prod_{i \in I} (n_i + 1) - 1 = \sum_{I' \subset I} \prod_{i \in I'} n_i$

Un mot de F est déterminé de manière unique par la donnée des x_{I_j} ($j=1, \dots, 2^{p-1}$) et par celle des c_i ($i=1, \dots, p$) . Donc

$$|F| = 2^{m - \sum_{i=1}^p n_i} \cdot \prod_{i=1}^p \frac{2^{n_i}}{n_i + 1} = \frac{2^m}{\prod_{i=1}^p (n_i + 1)} = \frac{2^m}{m+1}$$

Si F est un code à distance 3 c'est donc un code parfait .

Soient a et \bar{a} deux mots de F déterminés respectivement par la donnée des x_{I_j} ($j=1, \dots, 2^{p-1}$) et des c_i ($i=1, \dots, p$)

et par celle des \bar{x}_{I_j} ($j=1, \dots, 2^{p-1}$) et des \bar{c}_i ($i=1, \dots, p$) .

Montrons que a et \bar{a} sont soit égaux soit au moins à distance 3 .

Pour $i = 1, \dots, p$ posons

$$d_i = d(c_i + \sum_{j/i \in I_j} p_i(x_{I_j}), f_{i-1}(c_1, \dots, c_{i-1}), \bar{c}_i + \sum_{j/i \in I_j} p_i(\bar{x}_{I_j}) + f_{i-1}(\bar{c}_1, \dots, \bar{c}_{i-1}))$$

et soit $d = d(x_{I_1} \dots x_{I_{2^{p-1}}}, \bar{x}_{I_1} \dots \bar{x}_{I_{2^{p-1}}})$. Nous avons donc

$$d(a, \bar{a}) = d + d_1 + \dots + d_p .$$

* $d \geq 3$ on aura alors trivialement $d(a, \bar{a}) \geq 3$

* $d = 0$. Soit $k = \min \{i \in \{1, \dots, p\} / c_i \neq \bar{c}_i\}$

k existe sinon on aurait $a = \bar{a}$.

Nous avons $\forall j \forall i P_i(x_{I_j}) = P_i(\bar{x}_{I_j})$ donc $d_k = d(c_k, \bar{c}_k) \geq 3$

* $d = 1$. Soit $k = \min \{i \in \{1, \dots, p\} / c_i \neq \bar{c}_i \text{ ou } \sum_{j/i \in I_j} P_i(x_{I_j}) \neq \sum_{j/i \in I_j} P_i(\bar{x}_{I_j})\}$

k existe nécessairement puisqu'il existe j_0 unique tel que

$$d(x_{I_{j_0}}, \bar{x}_{I_{j_0}}) = 1 .$$

-) Si $c_k \neq \bar{c}_k$ alors $d_k \geq 3$ ou $d_k \geq 2$ car

$$d\left(\sum_{j/k \in I_j} P_k(x_{I_j}), \sum_{j/k \in I_j} P_k(\bar{x}_{I_j})\right) \leq 1$$

-) Si $c_k = \bar{c}_k$ on a donc $k \in I_{j_0}$; I_{j_0} étant de cardinal

au moins 2 k' existe nécessairement où :

$$k' = \min \{i \in \{k+1, \dots, p\} / c_i \neq \bar{c}_i \text{ ou } \sum_{j/i \in I_j} P_i(x_{I_j}) \neq \sum_{j/i \in I_j} P_i(\bar{x}_{I_j})\}$$

Suivant les cas on aura $d_{k'} \geq 3$, $d_{k'} \geq 2$ ou $d_{k'} = 1$.

* $d = 2$. Soit $k = \min \{i \in \{1, \dots, p\} / c_i \neq \bar{c}_i \text{ ou } \sum_{j/i \in I_j} P_i(x_{I_j}) \neq \sum_{j/i \in I_j} P_i(\bar{x}_{I_j})\}$

k existe nécessairement puisqu'on ne peut avoir

$$\forall i \in \{1, \dots, p\} \quad \sum_{j/i \in I_j} P_i(x_{I_j}) = \sum_{j/i \in I_j} P_i(\bar{x}_{I_j})$$

d'après ce que nous avons vu au chapitre précédent (démonstration de la proposition 2) .

Remarquons que $d\left(\sum_{j/i \in I_j} P_i(x_{I_j}), \sum_{j/i \in I_j} P_i(\bar{x}_{I_j})\right) \leq 2$

donc ou $c_k \neq \bar{c}_k$ et $d_k \geq 1$, ou $c_k = \bar{c}_k$ et $d_k \geq 1$

F est donc un code à distance 3 .

4 GENERALISATION A GF(q)

Soit q une puissance d'un nombre premier, soit $GF(q)$ le corps de Galois à q éléments et soit V_n l'espace vectoriel de dimension n sur $GF(q)$.

Shapiro et Slotnick [2] ont été les premiers à s'intéresser aux codes parfaits sur $GF(q)$ en généralisant la construction de Hamming.

Schönheim a introduit [4] la fonction parité $P_{\{v_i\}}$ d'un ensemble $\{v_i \mid i=1, \dots, q-1\}$ de vecteurs de V_n . Sa définition est la suivante :

Pour $i=1, \dots, q-1$ posons $v_i = (x_{i1} \dots x_{in})$.

Soient a_i ($i=1, \dots, q-1$) les éléments non nuls de $GF(q)$ ordonnés de manière quelconque.

La fonction parité généralisée $P_{\{v_i\}}$ est :

$$P_{\{v_i\}} = \sum_{i=1}^{q-1} a_i \sum_{j=1}^n x_{ij}$$

L'intérêt d'une telle fonction parité est de pouvoir à partir d'un code parfait de V_n construire une famille de codes parfaits de V_{qn+1} ; ce qui permet de prouver l'existence de codes parfaits non équivalents à des codes linéaires sur V_n (avec $n = \frac{q^m - 1}{q - 1}$ et $m > 2$).

La construction de Schönheim consiste à montrer que si C est un code parfait de longueur n alors C_n est un code parfait de longueur $qn+1$ où :

$$C_n = \left\{ (v_1 \dots v_{q-1}, c + \sum_{i=1}^{q-1} v_i, P_{\{v_i\}} + f(c)) \right\}$$

où pour $i = 1, \dots, q-1$ v_i parcourt V_n , où c parcourt C et où f est une application quelconque de C dans $GF(q)$.

Remarquons qu'une telle construction est possible car l'ensemble des mots de V_{qn+1} de la forme $(v_1 \dots v_{q-1}, \sum_{i=1}^{q-1} v_i, P_{\{v_i\}})$ est aussi un code à distance 3. Ceci est bien entendu à rapprocher de la première proposition du chapitre 2.

Soient C et C' deux codes parfaits sur respectivement n_1 et n_2 espaces vectoriels sur $GF(q)$.

Nous avons nécessairement l'existence d'entiers α et β tels que

$$n_1 = \frac{q^\alpha - 1}{q - 1} \quad \text{et} \quad n_2 = \frac{q^\beta - 1}{q - 1}$$

Nous allons à partir de C et C' construire un code parfait de longueur :

$$(q-1) n_1 n_2 + n_1 + n_2 = \frac{q^{\alpha+\beta} - 1}{q - 1}$$

Soit x un mot de $V_{(q-1)n_1 n_2}$, indiquons ses coordonnées suivant l'ordre lexicographique sur $\{1, \dots, n_1\} \times \{1, \dots, n_2\} \times \{1, \dots, q-1\}$

Nous définirons $P_1(x)$ comme le mot de V_{n_1} ($y_1 \dots y_{n_1}$) où
 pour $i = 1, \dots, n_1$ $y_i = \sum_{j=1}^{n_2} \sum_{k=1}^{q-1} x_{ijk}$.

Nous définirons $P_2(x)$ comme le mot de V_{n_2} ($y_1 \dots y_{n_2}$) où
 pour $j = 1, \dots, n_2$ $y_j = \sum_{k=1}^{q-1} a_k \sum_{i=1}^{n_1} x_{ijk}$.

Cette dissymétrie entre P_1 et P_2 est nécessaire, elle était déjà présente dans le cas particulier de la construction de Schönheim (cas $n_2 = 1$).

Théorème

Soit f une application de C dans V_{n_2} . désignons par F le code de $V_{(q-1)n_1n_2+n_1+n_2}$ dont les mots sont de la forme :

$$(x, c + P_1(x), c' + P_2(x) + f(c))$$

où x parcourt $V_{(q-1)n_1n_2}$ où c parcourt C (code parfait de V_{n_1}) et où c' parcourt C' (code parfait de V_{n_2}).

F est un code parfait de $V_{(q-1)n_1n_2+n_1+n_2}$.

Démonstration

$$|F| = q^{(q-1)n_1n_2} \cdot \frac{q^{n_1}}{(q-1)n_1+1} \cdot \frac{q^{n_2}}{(q-1)n_2+1} = \frac{q^{(q-1)n_1n_2+n_1+n_2}}{(q-1)((q-1)n_1n_2+n_1+n_2)+1}$$

Donc si F est un code à distance 3 il est parfait.

Soient a et \bar{a} deux mots de F montrons que si ils sont différents ils sont au moins à distance 3.

$$a = (x, c + P_1(x), c' + P_2(x) + f(c)) \quad \bar{a} = (\bar{x}, \bar{c} + P_1(\bar{x}), \bar{c}' + P_2(\bar{x}) + f(\bar{c}))$$

Posons $d_1 = d(c + P_1(x), \bar{c} + P_1(\bar{x}))$ et $d_2 = d(c' + P_2(x) + f(c), \bar{c}' + P_2(\bar{x}) + f(\bar{c}))$

* $d(x, \bar{x}) = 0$. On a donc $P_1(x) = P_1(\bar{x})$. Soit $c = \bar{c}$ et dans ce cas $d_2 = d(c', \bar{c}') \geq 3$; soit $c \neq \bar{c}$ et $d_1 \geq 3$.

* $d(x, \bar{x}) = 1$. On a alors $d(P_1(x), P_1(\bar{x})) = d(P_2(x), P_2(\bar{x})) = 1$. Soit $c \neq \bar{c}$ et $d_1 \geq 2$; soit $c = \bar{c}$ et $d_1 = 1$, on a alors $d_2 = d(c' + P_2(x), \bar{c}' + P_2(x))$ donc $d_2 \geq 1$.

* $d(x, \bar{x}) = 2$. x et \bar{x} diffèrent donc en deux coordonnées

x_{ijk} et $x_{i'j'k'}$. On ne peut avoir $d(a, \bar{a}) < 3$ que si

$d_1 = d_2 = 0$. Comme $d(P_1(x), P_1(\bar{x})) \leq 2$ ceci n'est possible que si $c = \bar{c}$ et puisque $d(P_2(x), P_2(\bar{x})) \leq 2$ que si $c' = \bar{c}'$.

On doit donc avoir dans ce cas $P_1(x) = P_1(\bar{x})$ et $P_2(x) = P_2(\bar{x})$

Pour avoir $P_1(x) = P_1(\bar{x})$ il faut nécessairement $i' = i$.

$$\text{donc } (x_{ijk} - \bar{x}_{ijk}) + (x_{ij'k'} - \bar{x}_{ij'k'}) = 0 \quad (1)$$

De même pour avoir $P_2(x) = P_2(\bar{x})$ il faut nécessairement $j'=j$

$$\text{donc } a_k(x_{ijk} - \bar{x}_{ijk}) + a_{k'}(x_{ijk'} - \bar{x}_{ijk'}) = 0 \quad (2)$$

(1) et (2) sont incompatibles puisqu'on en déduirait

$$(a_k - a_{k'}) \cdot (x_{ijk} - \bar{x}_{ijk}) = 0 \text{ avec } k \neq k' \text{ et } x_{ijk} \neq \bar{x}_{ijk}$$

ce qui est impossible dans le Corps $GF(q)$.

Donc $P_1(x) = P_1(\bar{x})$ et $P_2(x) = P_2(\bar{x})$ ne peuvent avoir lieu simultanément et $d(a, \bar{a}) \geq 3$

* $d(x, \bar{x}) \geq 3$ on a alors trivialement $d(a, \bar{a}) \geq 3$

\bar{F} est donc un code à distance 3 ,donc un code parfait .

REFERENCES

- [1] HAMMING R.W.(1950) Error detecting and error correcting codes .Bell Syst.Tech.J. ,29
- [2] SHAPIRO H.S. et SLOTNICK D.L. On The Mathematical Theory of Error Correcting Codes IBM j.Res.Develop. 3,25-37(1959)
- [3] VASILIEV JR.L.(1963) On non group close-packed codes . Probl.Cybernet. 8,337-339
- [4] SCHONHEIM J.(1968) On Linear Single Error Correcting q-nary Perfect Codes . Information and Control 12,23-26
- [5] PHELPS K.T. (1982) A General Product Construction for Error correcting Codes ,Georgia Institute of Technology Atlanta

Chapitre 3

Problèmes divers sur l'hypercube

On peut se poser (et éventuellement résoudre !) de très beaux problèmes combinatoires sur l'hypercube. Parmi ces problèmes nous nous sommes intéressés particulièrement à la recherche d'ensembles de sommets possédant certaines propriétés .

Parmi ces types de problèmes citons la recherche :

* D'ensembles de sommets C de cardinal maximum qui respectent une distance mutuelle minimale d (codes correcteurs d'erreurs, voir chapitre2)

$$\forall x, y \in C \text{ distincts}, d(x, y) \geq d.$$

* D'ensembles de sommets A de cardinal minimum qui constituent un absorbant

$$\forall x \in V(Q_n) \exists y \in A / d(x, y) \leq 1.$$

* D'ensembles de sommets S de cardinal minimum qui constituent un stable maximal

$$\forall x, y \in S \text{ distincts}, d(x, y) > 1$$

$$\forall x \notin S \exists y \in S / d(x, y) = 1.$$

* D'ensembles de sommets T de cardinal maximum qui constituent un absorbant minimal

$$\forall x \in V(Q_n) \exists y \in T / d(x, y) \leq 1$$

$$\forall x \in T \exists y \in V(Q_n) / d(x, y) \leq 1 \text{ et } \forall z \in T \text{ distinct de } x, d(y, z) > 1.$$

Les 3 derniers problèmes sont étudiés dans ma thèse de 3^{ème} Cycle[4] ; le deuxième l'a été depuis par A. Lobstein [3] . Un nouveau problème de ce type est introduit et résolu ici en étudiant le problème de la détermination d'une couverture de longueur minimale des arêtes de K_n par des cocycles .

Ce problème peut se formaliser comme celui de déterminer un ensemble C de sommets d'un cardinal donné n de l'hypercube Q_k tel que

$$l(C) = \sum_{x,y \in C} d(x,y) \text{ soit minimum (notons ce minimum } l_n = \min_{|C|=n} l(C) \text{).}$$

Il est clair que l_n ne dépend pas de k si k est suffisamment grand.

Nous montrons que pour tout $k \geq n-1$ et $n \neq 4,8$ on a $l_n = (n-1)^2$. $l(C)$ étant minimum si et seulement si C est une étoile, sauf dans les cas $n=5,6,7$ où trois graphes sont possibles ("On Shortest Cocycle cover of Graphs" figure 1). Pour $n=4$ et 8 on a $l_n = (n-1)^2 - 1$ et $l(C)$ est minimum pour Q_2 et Q_3 .

Remarquons d'ailleurs que pour les hypercubes

$$\sum_{x,y \in Q_p} d(x,y) = p \cdot 2^{2p-2} = \frac{|V||E|}{2}.$$

Un autre type de problèmes sur l'hypercube consiste en la recherche de cycles ayant certaines propriétés sur l'hypercube et parmi ceux-ci de cycles hamiltoniens.

Il est facile de construire par induction sur n des cycles hamiltoniens de Q_n . Le cycle le plus simplement construit ainsi est connu sous le nom de Code de Gray ou code binaire réfléchi. En fait l'origine de ces codes est bien plus ancienne puisque avant leur utilisation en télécommunication par F. Gray[2], ces codes ont été utilisés par Emile Baudot dans son télégraphe à la fin du 19^{ème} siècle.

Dans le télégraphe de Baudot les 32 lettres et signes à transmettre sont répartis sur la périphérie d'un disque divisé en 32 secteurs sur lesquels sont présentes 5 pistes concentriques en cuivres utilisées comme contacts. Les pistes sont tour à tour conductrices et non conductrices sur les 32 secteurs; le caractère conducteur de la $j^{\text{ème}}$ piste du $i^{\text{ème}}$ secteur correspond à la présence d'un 1 dans la $j^{\text{ème}}$ coordonnée du $i^{\text{ème}}$ mot du

code de Gray sur Q_5 . L'intérêt de ce dispositif réside dans le fait qu'à la frontière de 2 secteurs un seul contact change d'état.

Le code de Gray intervient également dans la résolution de certains jeux (Gardner [1]); la solution du problème de la tour de Hanoi peut être vue, par exemple, comme un tel cycle.

Pour notre part nous avons travaillé sur un problème un peu plus éloigné de cette excursion technologique, la recherche du nombre de cycles Hamiltoniens de Q_n . Ce problème a déjà suscité plusieurs travaux et nous améliorons les majorants et minorants connus.

REFERENCES

- [1] M. Gardner, The curious properties of the Gray code, *Scientific American* (2) 227 (Aout1972) 106-109.
- [2] F. Gray, U.S. Patent 2632058 (17 Mars 1953).
- [3] A. Lobstein, Contributions au codage combinatoire, Thèse de Docteur-ingénieur, ENST Paris (1985).
- [4] M. Mollard, Les Invariants du n cube, Thèse de 3^{ème} Cycle, USTMG Grenoble (1981).

On Shortest Cocycle Covers of Graphs

FRANÇOIS JAEGER

LSD(IMAG), BP 68, 38402 St. Martin d'Hères Cedex, France

ABDELKADER KHELLADI

U.S.T.H.B., Institut de Mathématiques, BP 139 Bab Ezzouar, Algérie

AND

MICHEL MOLLARD

LSD(IMAG), BP 68, 38402 St. Martin d'Hères Cedex, France

A cocycle (resp. cycle) cover of a graph G is a family C of cocycles (resp. cycles) of G such that each edge of G belongs to at least one member of C . The length of C is the sum of the cardinalities of its members. While it is known (see [5, 6]) that every bridgeless graph $G = (V, E)$ has a cycle cover of length not greater than $\frac{5}{3}|E|$, it is shown that there exists no $\alpha < 2$ such that every loopless graph $G = (V, E)$ has a cocycle cover with length not greater than $\alpha|E|$. To do this, cocycle covers of minimal length are determined for the complete graphs, thus solving a problem stated at the end of [6]. © 1985 Academic Press, Inc.

1. INTRODUCTION

The graphs we consider are finite, undirected, and have at least one edge. For definitions not given here, the reader should refer to [1, or 2].

Let $G = (V, E)$ be a graph and $S \subseteq V$ be a set of vertices. The *cocycle of G defined by S* , which we denote by $\omega_G(S)$, is the set of edges of G with exactly one end in S . A *cocycle of G* is any set of edges of the form $\omega_G(S)$ for some $S \subseteq V$. A *vertex-cocycle of G* is any set of edges of the form $\omega_G(\{v\})$ for some $v \in V$.

A *cycle (resp. cocycle) cover* of the graph G is a family C of cycles (resp. cocycles) of G such that each edge of G belongs to at least one member of C . The *length* of C is the sum of the cardinalities of its members and is denoted by $l(C)$. Note that the graph G admits a cycle (resp. cocycle) cover if and only if it has no bridges (resp. loops).

Recently several authors have studied the length of cycle covers of

graphs (see [3–6]). In particular it is shown independently in [5, 6] that every bridgeless graph $G = (V, E)$ has a cycle cover of length not greater than $\frac{5}{3}|E|$. In fact a wide extension of this result to regular matroids is proved in [6]. This leads us to consider similar problems for the cocycle matroids of graphs, that is, to study the length of cocycle covers of loopless graphs.

Clearly every loopless graph $G = (V, E)$ has a cocycle cover C with $l(C) < 2|E|$ (use all vertex-cocycles but one). A first basic question is the following: does there exist $\alpha < 2$ such that every loopless graph $G = (V, E)$ has a cocycle cover C with $l(C) \leq \alpha |E|$? We shall prove that the answer is negative. To do this, we shall determine the minimum length of a cocycle cover of the complete graph K_n on n vertices for every n , thus solving the problem stated at the end of [6]. It turns out that, for all $n \geq 2$, $n \neq 4$, $n \neq 8$, one can obtain a cocycle cover of minimum length of K_n by taking all vertex-cocycles except one. Our proof is based on a reformulation of the problem in the following terms: what is the minimum of the sum of mutual distances of n points in a k -dimensional cube ($k \geq n - 1$)?

2. GEOMETRIC FORMULATION OF THE PROBLEM

2.1. We recall that the k -cube ($k \geq 1$) is the simple graph Q_k whose vertex-set is $[GF(2)]^k$ and where $x = (x_1, \dots, x_k)$ and $y = (y_1, \dots, y_k)$ are adjacent iff $x + y$ has exactly one non-zero component. If x and y are vertices of Q_k , the number of non-zero components of $x + y$ is the distance between x and y in Q_k and is denoted by $d(x, y)$ (thus $d(x, y)$ is the usual Hamming distance of x and y).

2.2. Let $n \geq 2$. We denote by V_n and E_n the vertex-set and edge-set of K_n , respectively. For distinct vertices u, v of K_n , the edge with ends u and v is denoted by $\{u, v\}$.

Let $\mathcal{S} = (S_1, \dots, S_k)$ be a k -tuple ($k \geq 1$) of subsets of V_n . We associate to \mathcal{S} a mapping from V_n to $[GF(2)]^k$ which we denote by s and which we define as follows. For every v in V_n , $s(v) = (s_1(v), \dots, s_k(v))$, where $s_i(v) = 1$ if $v \in S_i$ and $s_i(v) = 0$ otherwise ($i = 1, \dots, k$). Clearly the correspondence $\mathcal{S} \rightarrow s$ is a bijection from the set of k -tuples of subsets of V_n to the set of mappings from V_n to $[GF(2)]^k$.

Now we shall need the following properties.

(i) $C = (\omega_{K_n}(S_i), i = 1, \dots, k)$ is a cocycle cover of K_n if and only if the mapping s associated to (S_1, \dots, S_k) is injective.

Indeed, for distinct vertices u, v of K_n and $i \in \{1, \dots, k\}$, the edge $\{u, v\}$

belongs to $\omega_{K_n}(S_i)$ iff $s_i(u) \neq s_i(v)$. Hence $\{u, v\}$ belongs to some member of C iff $s(u) \neq s(v)$, and (i) follows immediately.

$$(ii) \quad \sum_{i=1}^k |\omega_{K_n}(S_i)| = \sum_{\{u,v\} \in E_n} d(s(u), s(v)).$$

Indeed it is easy to see that both sides of this equation represent the number of pairs $(\{u, v\}, i) (\{u, v\} \in E_n, i \in \{1, \dots, k\})$ such that $\{u, v\} \in \omega_{K_n}(S_i)$, or equivalently $s_i(u) \neq s_i(v)$.

The following property can now easily be deduced from (i) and (ii).

(iii) *The minimum length of a cocycle cover of K_n consisting of exactly k cocycles is equal to the minimum of the quantity $\sum_{\{u,v\} \in E_n} d(s(u), s(v))$ taken over all injective mappings s from V_n to $[GF(2)]^k$.*

Remarks. —It follows from (i) that there exists a cocycle cover of K_n using exactly k cocycles iff $n \leq 2^k$.

—Let us distinguish a vertex v_0 of V_n . Every cocycle of K_n can be written uniquely in the form $\omega_{K_n}(S)$, where $S \subseteq V_n - \{v_0\}$. Hence every k -tuple of cocycles of K_n can be written uniquely in the form $(\omega_{K_n}(S_i), i = 1, \dots, k)$, where $S_i \subseteq V_n - \{v_0\}$ for $i = 1, \dots, k$. Then, by (i), the cocycle covers of K_n consisting of exactly k cocycles are in bijective correspondence with the injective mappings s from V_n to $[GF(2)]^k$ such that $s(v_0) = (0, 0, \dots, 0)$.

2.3. For every set A of vertices of Q_k , we denote by $D(A)$ the sum $\sum d(x, y)$, where each unordered pair of distinct vertices x, y of A appears once. We denote the minimum length of a cocycle cover of K_n by $l(K_n)$.

PROPOSITION 1. *For every $n \geq 2, k \geq n - 1$:*

$$\min D(A) = l(K_n)$$

$$A \subseteq [GF(2)]^k$$

$$|A| = n.$$

Proof. First we note that a cocycle cover of K_n consisting of j cocycles with $j < k$ can be converted into a cocycle cover consisting of k cocycles, and with the same length, by simply adding $k - j$ empty cocycles. It then follows from 2.2(iii) that the minimum length of a cocycle cover of K_n consisting of at most k cocycles is equal to $\min D(A)$,

$$A \subseteq [GF(2)]^k$$

$$|A| = n.$$

Then we observe that a cocycle cover of K_n with minimum length has at most $n - 1$ non-empty elements. This is because every non-empty cocycle of

K_n has cardinality at least $n-1$, and there exists a cocycle cover consisting of $n-1$ cocycles of cardinality $n-1$ (all vertex-cocycles except one). Hence $l(K_n)$ is equal to the minimum length of a cocycle cover consisting of at most $n-1$ cocycles, and this clearly remains true if $n-1$ is replaced by some larger number. This completes the proof.

3. THE MAIN RESULT

3.1. Let $n \geq 2$, $k \geq n-1$. A set A of n vertices of Q_k will be called *extremal* if $D(A) = l(K_n)$ (see Proposition 1). The *n-star* is the simple graph on n vertices which has one vertex of degree $n-1$, the other vertices being of degree 1.

THEOREM 1. For every $n \geq 2$, $l(K_n) = (n-1)^2 - \varepsilon(n)$, where $\varepsilon(n) = 1$ if $n = 4$ or $n = 8$, $\varepsilon(n) = 0$ otherwise. Moreover, for every $k \geq n-1$, a set A of n vertices of Q_k is extremal if and only if the subgraph of Q_k induced by A is isomorphic to one of the following graphs:

—The *n*-star, for all $n \geq 2$, $n \neq 4$, $n \neq 8$.

—For $n = 4 + i$, $i = 0, \dots, 4$, the graph G_n obtained from the 3-dimensional cube Q_3 by deleting $4 - i$ vertices belonging to a square (where, for $i = 2$, we delete two adjacent vertices). The graphs G_4, \dots, G_8 are depicted on Fig. 1.

3.2. We recall some basic properties of the k -dimensional cube Q_k needed for the proof. First, Q_k is a bipartite graph, and we assume from

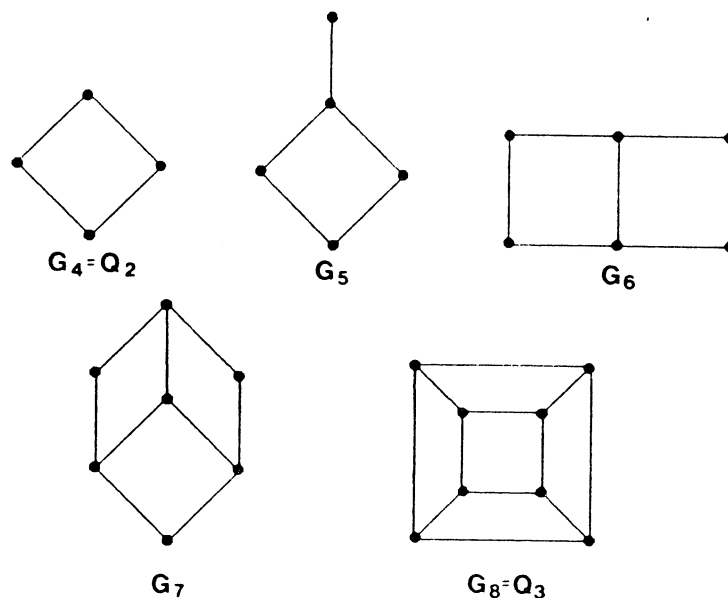


FIGURE 1

now on that we have defined a good coloring of its vertices with two colors we denote by 0 and 1. A second useful property is stated below.

LEMMA. If x and y are two vertices of Q_k with $d(x, y) = q$ ($1 \leq q \leq k$), then there exist exactly q vertices z such that $d(z, x) = 1$ and $d(z, y) = q - 1$.

3.3. An induced subgraph G of Q_k is called *distance-preserving* if the usual distance-function defined by G on its vertex-set coincides with the restriction of the Hamming distance d to this set. It follows immediately from the biparticity of Q_k that all induced subgraphs of Q_k of diameter at most 3 are distance-preserving. In particular, the n -stars ($n \geq 2$) and the graphs G_n ($n = 4, \dots, 8$) occurring in the statement of the theorem are distance-preserving. It is then easy to compute $D(A)$ when the subgraph of Q_k induced by A is isomorphic to one of these graphs. We obtain $(n - 1)^2$ for the n -star ($n \geq 2$), and 8, 16, 25, 36, 48 for G_4, G_5, G_6, G_7, G_8 , respectively. We conclude that:

(i) *If A is a subset of n vertices of Q_k which induces a subgraph isomorphic to an n -star ($n \geq 2, n \neq 4, n \neq 8$) or to G_n ($n = 4, \dots, 8$), then $D(A) = (n - 1)^2 - \varepsilon(n)$.*

3.4. We now consider a subset A of n vertices of Q_k ($n \geq 2, k \geq n - 1$) such that

$$D(A) \leq (n - 1)^2 - \varepsilon(n). \tag{I_1}$$

We shall show that

(ii) *The subgraph G of Q_k induced by A is isomorphic to an n -star (when $n \neq 4, n \neq 8$) or to G_n (when $n \in \{4, \dots, 8\}$).*

This, together with 3.3(i), will complete the proof of the theorem. We denote by m the number of edges of G and by Δ its maximum degree.

3.4.1. (ii) is true when $\Delta \leq 1$. Clearly, $D(A) \geq m + 2(n(n - 1)/2 - m) = n(n - 1) - m$. Then by (I₁), $n(n - 1) - m \leq (n - 1)^2$, and hence $m \geq n - 1$. Since $n \geq 2, m \geq 1$ and we must have $\Delta = 1$. Then $2n - 2 \leq 2m \leq n$. It follows that $n = 2, m = 1$ and G is the 2-star.

3.4.2. (ii) is true when $\Delta = 2$. Let A_i be the set of vertices of A of color i , and let $|A_i| = a_i$ ($i = 0, 1$). The distance between two vertices is even iff they have the same color. It easily follows that

$$D(A) \geq m + 3(a_0 a_1 - m) + 2 \left(\frac{a_0(a_0 - 1)}{2} + \frac{a_1(a_1 - 1)}{2} \right),$$

or equivalently, $D(A) \geq 3a_0 a_1 + a_0(a_0 - 1) + a_1(a_1 - 1) - 2m$. By (I₁),

$D(A) \leq (a_0 + a_1 - 1)^2$. It follows that $a_0^2 + a_1^2 + 2a_0a_1 - 2(a_0 + a_1) + 1 \geq 3a_0a_1 + a_0^2 + a_1^2 - a_0 - a_1 - 2m$. This reduces to $2m \geq a_0a_1 + a_0 + a_1 - 1$.

We may assume without loss of generality that $a_0 \leq a_1$. Since $\Delta = 2$, we have $m \leq 2a_0$. Using these three inequalities we may write

$$4a_0 \geq 2m \geq a_0a_1 + a_0 + a_1 - 1 \geq a_0^2 + 2a_0 - 1. \quad (\text{I}_2)$$

Hence $a_0^2 - 2a_0 - 1 \leq 0$. It follows that $a_0 \leq 2$.

If $a_0 = 2$, (I_2) gives $8 \geq 2m \geq 3a_1 + 1$. Since $a_1 \geq a_0 = 2$, we must have $a_1 = 2$, and hence $n = 4$, $m = 4$. Then G is isomorphic to the square G_4 .

If $a_0 < 2$, since $\Delta = 2$, we must have $a_0 = 1$. Then (I_2) gives $4 \geq 2m \geq 2a_1$. Hence $a_1 \leq 2$, and we must have equality since $\Delta = 2$. It follows that $n = 3$, $m = 2$, and G is the 3-star.

3.4.3. (ii) is true when $n \leq 4$. If $\Delta \leq 2$, the result is proved in 3.4.1, 3.4.2. Otherwise $3 \leq \Delta \leq n - 1$ implies that $n = 4$, $\Delta = 3$, and G is the 4-star. But then $D(A) = 9$, and this is a contradiction with (I_1) , so that this case cannot occur.

3.4.4. In the sequel we assume that $n \geq 5$, $\Delta \geq 3$, and we choose a vertex x of degree Δ in G . We denote by B the set of vertices of A equal or adjacent to x , by C the set $A - B$, and by $D(B, C)$ the sum $\sum_{y \in B, z \in C} d(y, z)$. Clearly the subgraph of Q_k induced by B is a $(\Delta + 1)$ -star, so that $D(B) = \Delta^2$. Moreover $D(A) = D(B) + D(C) + D(B, C)$, and hence,

$$D(A) = \Delta^2 + D(C) + D(B, C). \quad (\text{I}_3)$$

3.4.5. Consider a vertex z of C . By the definition of C , $d(z, x) \geq 2$.

3.4.5.1. If $d(z, x) = 2$, denote by B_z the set of vertices of B adjacent to z . Then x and z have the same color, and hence the vertices of $B - \{x\}$ are at odd distance from z . It follows that the vertices of $(B - \{x\}) - B_z$ are at distance 3 from z . Hence,

$$\sum_{y \in B} d(z, y) = d(z, x) + |B_z| + 3|(B - \{x\}) - B_z| = 3\Delta + 2 - 2|B_z|.$$

By the lemma, $|B_z| \leq 2$, so that $\sum_{y \in B} d(z, y) \geq 3\Delta - 2$.

3.4.5.2. If $d(z, x) = 3$, denote by B'_z the set of vertices of B at distance 2 from z . Then x and z have different colors, and hence the vertices of $B - \{x\}$ are at even distance from z . It follows that the vertices of $(B - \{x\}) - B'_z$ are at distance 4 from z . Hence,

$$\sum_{y \in B} d(z, y) = d(z, x) + 2|B'_z| + 4|(B - \{x\}) - B'_z| = 4\Delta + 3 - 2|B'_z|.$$

By the lemma, $|B'_z| \leq 3$, so that $\sum_{y \in B} d(z, y) \geq 4\Delta - 3$.

3.4.5.3. If $d(z, x) \geq 4$, every vertex of $B - \{x\}$ is at distance at least 3 from z . Hence

$$\sum_{y \in B} d(z, y) \geq d(z, x) + 3 |B - \{x\}| \geq 3\Delta + 4.$$

3.4.5.4. The case $\Delta = 3$ will be of special interest. We note that if $d(z, x) = 2$ and $|B_z| = 2$, $\sum_{y \in B} d(z, y) = 7$ (see Sect. 3.4.5.1). In any other case, $\sum_{y \in B} d(z, y) \geq 9$.

3.4.6. (ii) is true when $n \leq 6$. For $n = 5$, we must have $\Delta \leq 4$. If $\Delta = 4$, G is the 5-star and we are done. Otherwise $\Delta = 3$. Then $|C| = 1$, so that $D(C) = 0$. By (I_3) , $D(A) = 9 + D(B, C)$. By (I_1) , $D(A) \leq 16$. It follows that $D(B, C) \leq 7$. By 3.4.5.4, this is true if and only if the unique vertex of C is adjacent to exactly two vertices of B . Then G is isomorphic to G_5 .

For $n = 6$, we must have $\Delta \leq 5$. If $\Delta = 5$, G is the 6-star and we are done. If $\Delta = 4$, then $|C| = 1$, so that $D(C) = 0$. By (I_3) , $D(A) = 16 + D(B, C)$. By (I_1) , $D(A) \leq 25$. It follows that $D(B, C) \leq 9$. By 3.4.5.1, 3.4.5.2, and 3.4.5.3, $D(B, C) \geq 10$ and this case is impossible. Finally if $\Delta = 3$, then $|C| = 2$. By (I_3) , $D(A) = 9 + D(C) + D(B, C)$. By (I_1) , $D(A) \leq 25$. It follows that $D(C) + D(B, C) \leq 16$. Since $D(C) \geq 1$, we must have $D(B, C) \leq 15$.

By 3.4.5.4, this is true if and only if each of the two vertices of C is adjacent to exactly two vertices of B . By the lemma, the two vertices of C cannot be adjacent to the same pair of vertices of B . We conclude that G is isomorphic to G_6 .

3.4.7. (ii) is true for every n . We prove this by induction on n . If $C = \emptyset$, G is an n -star and the result is proved (the 4-star and 8-star are excluded because of (I_1)). Hence we may assume that $|C| \geq 1$. By 3.4.1 and 3.4.2, we also may assume that $\Delta \geq 3$. The initialization of the induction is given by 3.4.6. The induction hypothesis implies that $D(C) \geq (|C| - 1)^2 - \varepsilon(|C|)$ when $|C| \geq 2$. This remains true when $|C| = 1$ (we shall define $\varepsilon(1)$ as equal to zero). Hence we may write

$$D(C) \geq (n - \Delta - 2)^2 - \varepsilon(n - \Delta - 1) \geq (n - \Delta - 2)^2 - 1. \tag{I_4}$$

Since $\Delta \geq 3$, it follows from 3.4.5.1, 3.4.5.2, and 3.4.5.3 that for every vertex z in C , $\sum_{y \in B} d(z, y) \geq 3\Delta - 2$. Hence

$$D(B, C) \geq (n - \Delta - 1)(3\Delta - 2) \tag{I_5}$$

Then (I_3) together with (I_4) and (I_5) gives $D(A) \geq \Delta^2 + (n - \Delta - 2)^2 - 1 + (n - \Delta - 1)(3\Delta - 2)$, that is, $D(A) \geq \Delta^2 + (n - \Delta - 1)((n - \Delta - 3) + (3\Delta - 2))$.

It follows that $(n-1)^2 - D(A) \leq (n-1)^2 - \Delta^2 - (n-\Delta-1)(n+2\Delta-5)$, that is, $(n-1)^2 - D(A) \leq (n-\Delta-1)[(n-1+\Delta) - (n+2\Delta-5)] = (n-\Delta-1)(4-\Delta)$.

The left-hand side is non-negative by (I_1) . We have assumed that $C \neq \emptyset$, so that $n-\Delta-1 > 0$. It follows that $\Delta \leq 4$.

If $\Delta = 4$, clearly all the above inequalities must hold with equality. In particular, (I_5) holds with equality. This is true if and only if for every vertex z in C , $\sum_{y \in B} d(z, y) = 3\Delta - 2$. By 3.4.5, every vertex of C is adjacent to exactly two vertices of $B - \{x\}$. By the lemma, two vertices of C cannot be adjacent to the same pair of vertices of $B - \{x\}$. Since there are 6 distinct pairs of vertices of $B - \{x\}$, $|C| \leq 6$. Moreover, since (I_4) holds with equality, $\varepsilon(|C|) = 1$. It follows from 3.4.6 that $|C| = 4$ and the subgraph of Q_k induced by C is a square. Now a vertex of $B - \{x\}$ cannot be adjacent to two vertices of C (this would create a triangle or contradict the lemma). Hence the number of edges connecting B and C is at most 4, a contradiction. This case cannot occur.

If $\Delta = 3$, we refine the above calculations. (I_4) gives

$$D(C) \geq (n-5)^2 - \varepsilon(n-4). \quad (I'_4)$$

We denote by C_2 the set of vertices of C adjacent to exactly two vertices of B . Since no two vertices of C_2 are adjacent to the same pair of vertices of B , $|C_2| \leq 3$. It then follows from 3.4.5.4 that

$$D(B, C) \geq 7|C_2| + 9(n-4 - |C_2|)$$

and we may write

$$D(B, C) \geq 9n - 36 - 2|C_2| \geq 9n - 42. \quad (I'_5)$$

Then (I_3) together with (I'_4) and (I'_5) gives

$$\begin{aligned} D(A) &\geq 9 + 9n - 42 + (n-5)^2 - \varepsilon(n-4) \\ &= n^2 - n - 8 - \varepsilon(n-4). \end{aligned}$$

It follows that $(n-1)^2 - D(A) \leq (n^2 - 2n + 1) - [n^2 - n - 8 - \varepsilon(n-4)]$, that is, $(n-1)^2 - D(A) \leq 9 + \varepsilon(n-4) - n \leq 10 - n$.

The left-hand side is non-negative by (I_1) . Hence $n \leq 10$. The case $n = 10$ is excluded because $\varepsilon(6) = 0$.

For $n = 9$, since $\varepsilon(5) = 0$, all inequalities must hold with equality. The equality in (I'_5) implies that $|C_2| = 3$. Since $|C| = 5$ and (I'_4) holds with equality, it follows from 3.4.6 that the subgraph of Q_k induced by C is isomorphic to G_5 or to the 5-star. In both cases some vertex of C must be of degree greater than 3 in G , a contradiction.

For $n = 8$, (I'_4) becomes $D(C) \geq 9 - \varepsilon(4) = 8$ and (I'_5) gives $D(B, C) \geq 36 - 2|C_2|$. Using (I_3) we obtain $D(A) \geq 9 + 8 + 36 - 2|C_2| = 53 - 2|C_2|$. On the other hand, (I_1) gives $D(A) \leq 48$. Hence $2|C_2| \geq 53 - 48 = 5$, so that $|C_2| = 3$. Now $D(B, C) \geq 30$. Since $9 + D(C) + D(B, C) = D(A) \leq 48$, we must have $D(C) \leq 9$.

Moreover distinct vertices of C_2 are adjacent to distinct pairs of vertices of $B - \{x\}$, so that the edges with one end in C_2 and the other in $B - \{x\}$, form a cycle of length 6. Then no two vertices of C_2 are adjacent (otherwise we would obtain a triangle). Hence $D(C_2) \geq 6$. Then $D(C) \leq 9$ implies that the vertex of $C - C_2$ is adjacent to all vertices of C_2 . It follows that G is isomorphic to the 3-dimensional cube G_8 .

By 3.4.6, the only remaining case is $n = 7$. Then (I'_4) becomes $D(C) \geq 4 - \varepsilon(3) = 4$ and (I'_5) gives $D(B, C) \geq 27 - 2|C_2|$. Using (I_3) , we obtain $D(A) \geq 9 + 4 + 27 - 2|C_2| = 40 - 2|C_2|$. On the other hand, (I_1) gives $D(A) \leq 36$. Hence $2|C_2| \geq 40 - 36$, so that $|C_2| \geq 2$. If $|C_2| = 3$, every vertex of C is adjacent to two vertices of $B - \{x\}$, and no two vertices of C are adjacent to the same pair of vertices of $B - \{x\}$. Then G is clearly isomorphic to G_7 . Otherwise, $|C_2| = 2$. Then $D(B, C) \geq 23$. Since $36 \geq D(A) = 9 + D(C) + D(B, C)$, we must have $D(C) \leq 4$, so that $D(C) = 4$. By (ii) (applied to C) the subgraph of Q_k induced by C is a 3-star. Since $\Delta = 3$, the vertex of degree two of this 3-star is the vertex of $C - C_2$. Then again G is easily seen to be isomorphic to G_7 . This completes the proof of Theorem 1.

4. CONSEQUENCES

4.1. Using the correspondence described in Section 2.2, it is easy to reformulate Theorem 1 in terms of cocycle covers. For the sake of simplicity, we denote the vertex-set of K_n by $\{1, \dots, n\}$. Two cocycle covers $C = (\omega_{K_n}(S_i), i = 1, \dots, k)$ and $C' = (\omega_{K_n}(S'_i), i = 1, \dots, k)$ will be said to be isomorphic when there exists a bijection σ of $\{1, \dots, n\}$ such that $\forall i \in \{1, \dots, k\}, \omega_{K_n}(S_i) = \omega_{K_n}(\sigma(S'_i))$. Then we obtain

THEOREM 2. *For every $n \geq 2$, $l(K_n) = (n - 1)^2 - \varepsilon(n)$, where $\varepsilon(n) = 1$ if $n = 4$ or $n = 8$, $\varepsilon(n) = 0$ otherwise. Moreover a cocycle cover of K_n (consisting of non-empty cocycles) has length $l(K_n)$ if and only if it is isomorphic to one of the following cocycle covers:*

- $(\omega_{K_n}(\{1\}), i = 1, \dots, n - 1)$ for all $n \geq 2, n \neq 4, n \neq 8$
- $(\omega_{K_n}(\{1, 2\}), \omega_{K_n}(\{1, 3\}))$ for $n = 4$
- $(\omega_{K_n}(S_i), i = 1, 2, 3)$ for $n = 5, 6, 7, 8$, where $S_1 = \{1, 2, 3, 4\}$, $S_2 = \{1, 2, 7, 8\} \cap \{1, \dots, n\}$, $S_3 = \{1, 4, 5, 8\} \cap \{1, \dots, n\}$.

The proof is left to the reader.

4.2. PROPOSITION 2. *Let $G = (V, E)$ be a (loopless) n -colorable graph. Then the minimum length of a cocycle cover of G is at most.*

- $\frac{4}{3} |E|$ for $n = 4$
- $\frac{12}{7} |E|$ for $n = 8$
- $(2 - 2/n) |E|$ for every $n \geq 2$, $n \neq 4$, $n \neq 8$.

Moreover equality holds when G is the complete graph K_n .

Proof. The fact that equality holds when G is the complete graph K_n follows from Theorem 2.

Consider a coloring of G with n colors ($n \geq 2$), and denote by V_i ($i = 1, \dots, n$) the set of vertices which have received the i th color. We assume, without loss of generality that $|\omega_G(V_i)| \leq |\omega_G(V_n)|$ for all $i = 1, \dots, n$.

Clearly $C = (\omega_G(V_i), i = 1, \dots, n-1)$ is a cocycle cover of G , and $\sum_{i=1}^n |\omega_G(V_i)| = 2 |E|$. It follows that C has length $2 |E| - |\omega_G(V_n)|$, and that $|\omega_G(V_n)| \geq 2 |E|/n$. Hence the length of C is at most $(2 - 2/n) |E|$. This settles the general case.

For $n = 4$, we observe that every edge of G appears in exactly two of the three cocycles $\omega_G(V_1 \cup V_2)$, $\omega_G(V_1 \cup V_3)$, $\omega_G(V_1 \cup V_4)$. By deleting the largest one, we obtain a cocycle cover of G of length at most $\frac{4}{3} |E|$.

For $n = 8$, let Q be the set of 4-element subsets of $\{1, \dots, 8\}$. Let T be the set of 3-element subsets $\{q_1, q_2, q_3\}$ of Q with the following property: for every pair $\{i, j\}$ of distinct elements of $\{1, \dots, 8\}$, there exists $k \in \{1, 2, 3\}$ such that q_k contains exactly one of the elements i, j . Then for every $t = \{q_1, q_2, q_3\} \in T$, $(\omega_G(\cup_{i \in q_j} V_i), j = 1, 2, 3)$ is a cocycle cover of G , which we denote by C_t .

For $q \in Q$, let $k(q)$ be the number of elements of T which contain q . It is easy to see that $k(q)$ is independent of q . We denote the common value of all numbers $k(q)$ ($q \in Q$) by k . Then $\sum_{t \in T} l(C_t) = k \sum_{q \in Q} |\omega_G(\cup_{i \in q} V_i)|$.

Moreover for every pair i, j of distinct elements of $\{1, \dots, 8\}$, there exist exactly 40 elements q of Q such that q contains exactly one of the elements i, j . Equivalently, for every edge e of G there exists exactly 40 elements q of Q such that $e \in \omega_G(\cup_{i \in q} V_i)$. Hence $\sum_{q \in Q} |\omega_G(\cup_{i \in q} V_i)| = 40 |E|$. It follows that the average length of a cocycle cover of the form C_t ($t \in T$) is $40 k |E| / |T|$.

Now by counting in two ways the number of pairs (q, t) such that $q \in Q$, $t \in T$, and $q \in t$, we obtain $k |Q| = 3 |T|$. Since $|Q| = C_8^4 = 70$, we have that $k / |T| = \frac{3}{70}$; hence the average length of a cocycle cover of the form C_t ($t \in T$) is $\frac{3}{70} \times 40 |E| = \frac{12}{7} |E|$. We conclude that some cocycle cover of G has length at most $\frac{12}{7} |E|$. This completes the proof.

An immediate consequence of this result is the following:

4.3. PROPOSITION 3. *For every $\alpha < 2$, there exists a loopless graph $G = (V, E)$, each cocycle cover of which has length greater than $\alpha |E|$.*

REFERENCES

1. C. BERGE, "Graphes et Hypergraphes," Dunod, Paris, 1974.
2. J. A. BONDY AND U. S. R. MURTY, "Graph Theory with Applications," MacMillan & Co., London, 1976.
3. A. ITAI AND M. RODEH, Covering a graph by circuits, in "Automata, Languages, and Programming," Lecture Notes in Computer Science No. 62, Springer, Berlin, 1978.
4. A. ATAI, R. J. LIPTON, C. H. PAPADIMITRIOU, AND M. RODEH, Covering graphs by simple circuits, *SIAM J. Comput.* **10**, No. 4 (1981), 746–754.
5. J. C. BERMOND, B. JACKSON, AND F. JAEGER, Shortest coverings of graphs with cycles, *J. Combin. Theory Ser. B* **35**, No. 3 (1983), 297–308.
6. M. TARSI, Nowhere zero flow and short circuit covering in regular matroids, preprint.

LE NOMBRE D'ABSORPTION DU n -CUBE

M. MOLLARD

IMAG, BP 53 X, 38041 Grenoble, Cedex, France

Définition. Le n -cube est le graphe défini de la manière suivante:

- l'ensemble des sommets est $\{0, 1\}^n$;
- 2 sommets x et y sont reliés par une arête si et seulement si les deux n -uplets diffèrent d'exactly une composante.

C'est donc un graphe régulier de degré n et d'ordre 2^n .

Remarque. On a $\forall n, \forall p \in \{0, 1, \dots, n\}, C_n = C_p + C_{n-p}$ (somme cartésienne de graphe).

Le poids d'un sommet est sa distance à l'origine $(0, 0, \dots, 0)$.

Le n -cube est donc biparti puisqu'on peut partitionner l'ensemble des sommets en V_p (ensemble des sommets de poids pair) et V_i (ensemble des sommets de poids impair) 2 sommets reliés ne pouvant être de même parité.

On voit facilement que le nombre de stabilité du n -cube est $\alpha(C_n) = 2^{n-1}$ et que les stables maximum sont les clefs de parité V_i et V_p .

Désignons par $\beta(C_n)$ le cardinal minimum d'un absorbant A de C_n . Trivialement $\beta(C_n) \geq 2^n / (n + 1)$ puisque chaque sommet de A absorbe au plus $n + 1$ nouveaux sommets. Nous dirons que C_n admet un absorbant parfait A si chaque sommet de C_n est absorbé par exactement un sommet de A ou ce qui revient au même si

$$|A| = \frac{2^n}{n + 1}. \quad (1)$$

Remarquons que (1) implique $n = 2^p - 1$ pour un certain entier p . On peut donc se poser la question de l'existence d'absorbants parfaits pour $n = 2^p - 1$, pour cela il est nécessaire d'étudier un peu les codes correcteurs d'erreurs.

Définition. Un 3-code est un ensemble \mathcal{C} de sommets du n -cube tel que

$$\forall x \quad \forall y \in \mathcal{C} \quad x \neq y, \quad d(x, y) \geq 3.$$

Ce qui revient à dire que les boules de rayon 1 centrées sur les sommets de \mathcal{C} doivent être disjointes.

On désigne par $A(n, 3)$ le cardinal maximum d'un 3 code.

$$A(n, 3) \leq \frac{2^n}{n+1}, \quad (2)$$

ceci car le nombre total de sommets contenus dans les $|\mathcal{C}|$ boules disjointes est $|\mathcal{C}|(1+n)$.

Un 3-code est dit parfait si et seulement si on a égalité dans (2).

Pour $n = 2^p - 1$ de tels codes existent (construction de Hamming).

Proposition. \mathcal{C} est un 3-code parfait si et seulement si \mathcal{C} est un absorbant parfait.

Proposition

$$\beta(C_n) \leq \beta(C_{n+1}) \leq 2\beta(C_n). \quad (3)$$

Ce qui permet de prouver le résultat suivant:

$$\beta(C_n) = k_n \frac{2^n}{n+1} \quad \text{avec } k_n \in [1, 2].$$

Vizing a conjecturé [1] que pour toute paire de graphe G et H

$$\beta(G + H) \geq \beta(G)\beta(H).$$

Une conséquence de (3) est que pour tout couple (p, q) ,

$$\beta(C_p + C_q) \geq \beta(C_p)\beta(C_q).$$

D'autre part les valeurs de β sont reliées à celles de $A(n, 3)$ par les inégalités suivantes:

$$2A(n, 3) + (n-1)\beta(C_n) \geq 2^n,$$

$$nA(n, 3) + \beta(C_n) \leq 2^n.$$

Des résultats similaires existent pour $\alpha'(C_n)$ cardinal minimum d'un stable maximal du n -cube.

On peut également s'intéresser à $\beta'(C_n)$ cardinal maximum d'un absorbant minimal du n -cube.

Théorème. $\beta'(C_n) = 2^{n-1}$ et si \mathcal{C} est un absorbant minimal de cardinalité 2^{n-1} alors \mathcal{C} est d'un des deux types-suivants:

- (1) \mathcal{C} est l'une des 2 clefs de parité V_i et V_p ;
- (2) \mathcal{C} est isomorphe à un des sous cube de dimension $n-1$.

Remarquons que $\beta'(C_n) = 2^{n-1}$ peut se montrer directement en utilisant le fait que pour un graphe biparti $\beta' = \alpha$ [2].

Lemme 1. *Toutes les boules centrées sur un sommet de \mathcal{C} sont des types (Fig. 1):*

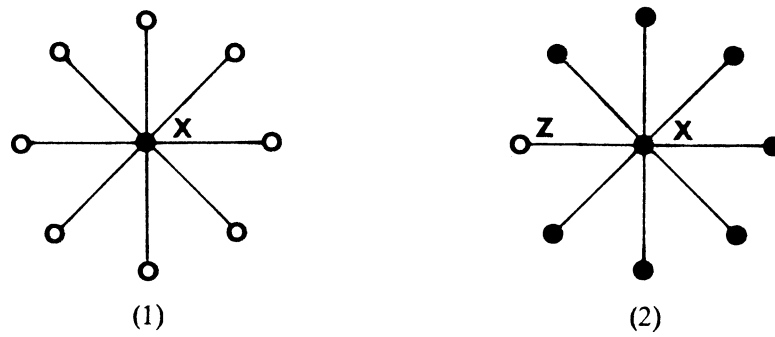


Fig. 1. (1) $x \in \mathcal{C}, \forall y \mid d(x, y) = 1, y \notin \mathcal{C}$; (2) $x \in \mathcal{C}, \exists! z \mid d(x, z) = 1$ et $z \notin \mathcal{C}$.

On obtient ce lemme en comptabilisant les boules-de tous les types possibles.

Lemme 2. *Toutes les boules centrées sur un sommet de \mathcal{C} sont soit toutes du type (1) soit toutes du type (2).*

Soient x et y tels que x soit le centre d'une boule de type (1), y d'une boule de type (2) et tels que $d(x, y)$ soit minimale.

Il est clair que $d(x, y) < 4$ (Fig. 2). z doit être absorbé par un sommet t de \mathcal{C} ce qui contredit la minimalité de $d(x, y)$, et trivialement $d(x, y) \geq 2$.

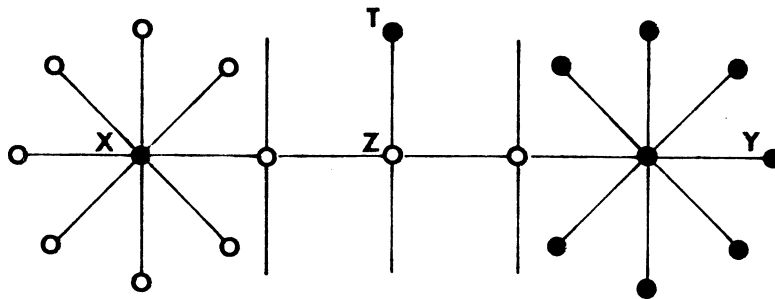


Fig. 2. $d(x, y) < 4$.

y et z sont à distance 2 donc (propriété du n -cube) il existe 2 chemins de longueur 2 entre y et z . Soit v le nouveau sommet, v ne peut-être le centre ni d'une boule de type (1) ni d'une boule de type (2) (Fig. 3).

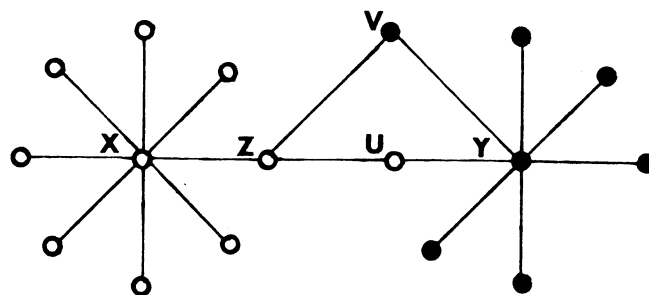


Fig. 3. $d(x, y) \neq 3$.

x et y sont à distance 2 donc reliés par 2 chemins de longueur 2 passant par u et v . Puisque x est du type (1), $u \notin \mathcal{C}$, $v \notin \mathcal{C}$, ce qui est impossible car y est du type (2) (Fig. 4).

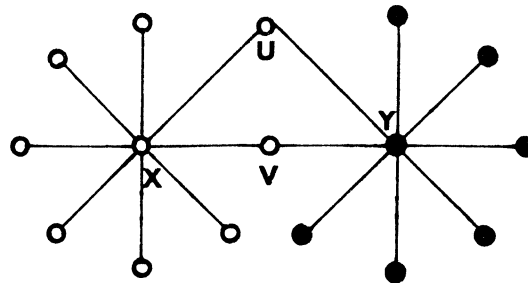


Fig. 4. $d(x, y) \neq 2$.

References

- [1] V.G. Vizing, *Vytchislitelnye systemy* 9 (1963) 30–43.
- [2] E.J. Cockayne, O. Favaron, C. Payan and A.G. Thomason, Contribution to the theory of domination independence and irredundance in graphs, *Discrete Math.* 33 (1981) 249–258.
- [3] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).

Un Nouvel Encadrement du Nombre de Cycles Hamiltoniens du n -Cube

M. MOLLARD

We give new upper and lower bounds for the number of Hamiltonian cycles $h(n)$ in the graph of the n -cube Q_n .

1. INTRODUCTION

Le n -cube Q_n est le graphe dont les 2^n sommets sont les n -uplets de $\{0, 1\}^n$ et où deux sommets sont reliés par une arête si ils diffèrent en exactement une coordonnée.

Un cycle hamiltonien de Q_n est une séquence circulaire v_1, \dots, v_{2^n} de tous les 2^n sommets de Q_n où:

- (i) v_i et v_{i+1} sont adjacents par $i = 1, 2, \dots, 2^n - 1$,
- (ii) v_{2^n} et v_1 sont adjacents.

Le problème de déterminer $h(n)$ le nombre de cycles hamiltoniens du n -cube a été étudié par un certain nombre d'auteurs. Il est clair que $h(2) = 1$ et $h(3) = 6$. Il a été calculé [1] que $h(4) = 1344$. Pour $n \geq 5$, on connaît uniquement des majorants et des minorants.

Dixon et Goodman ont prouvé [2]

$$h(n) \geq \frac{2^n}{n-1} h^2(n-1), \tag{1}$$

$$h(n) \leq \left(\frac{n(n-1)}{2} \right)^{2^{n-1}-1}. \tag{2}$$

Résultats améliorés par Douglas [3]

$$h(n) \geq \frac{n2^{n-1}}{n-1} h^2(n-1), \tag{3}$$

$$h(n) \leq \left(\frac{n(n-1)}{2} \right)^{2^{n-1} - 2^{[n-1 - \log_2 n]}} \tag{4}$$

(où $[x]$ désigne la partie entière).

Nous nous proposons d'améliorer à nouveau ces résultats.

2. MINORANT DE $h(n)$

Remarquons qu'en choisissant un sommet origine v_1 sur Q_n on peut représenter un cycle hamiltonien v_1, \dots, v_{2^n} par sa 'suite de nombres de transition': a_1, \dots, a_{2^n} où v_i et v_{i+1} diffèrent en leur $a_i^{\text{ème}}$ coordonnée.

Dans cette séquence de nombres de transition, chaque entier de $\{1, \dots, n\}$ présente un nombre pair, et non nul, d'occurrences. Douglas [3] a prouvé le lemme suivant:

LEMME. *Pour tout cycle hamiltonien H de Q_n , il existe au plus 2 entiers de $\{1, \dots, n\}$ ayant exactement 2 occurrences dans la séquence de nombres de transition de H .*

Il est en effet facile de montrer que si il existait au moins 3 entiers ayant cette propriété, H serait de longueur au plus $6 \cdot 2^{n-3}$ nombre strictement inférieur à 2^n .

Rappelons également le résultat classique (Abbott [4]). Le nombre de cycles hamiltoniens utilisant une arête donnée de Q_n est $2h(n)/n$.

THÉORÈME 1.

$$h(n) \geq \frac{n(2^n - 4)}{n - 1} h^2(n - 1), \quad n \geq 3.$$

Reprenons les idées de Douglas [3] utilisées pour démontrer la minoration (3).

Décomposons le n -cube en deux faces de dimension $n - 1$ G et \bar{G} . Une telle face correspond à un sous-graphe engendré par les sommets dont on fixe une coordonnée.

Soit H un cycle hamiltonien quelconque de G ; choisissons une arête $\{x, y\}$ de ce cycle. Soit $\{\bar{x}, \bar{y}\}$ l'arête correspondante de \bar{G} , et H' un cycle hamiltonien de \bar{G} utilisant l'arête $\{\bar{x}, \bar{y}\}$ (Figure 1).

L'ensemble d'arêtes obtenu à partir de $H \cup H'$ en supprimant $\{x, y\}$ et $\{\bar{x}, \bar{y}\}$ et en rajoutant $\{x, \bar{x}\}$ et $\{y, \bar{y}\}$ est un cycle hamiltonien de Q_n .

Pour une décomposition en $(n - 1)$ cubes donnée, à chaque paire de cycle H, H' on pourra associer un cycle distinct de Q_n . On construit ainsi

$$h(n - 1) \cdot 2^{n-1} \cdot \frac{2h(n - 1)}{n - 1} \text{ cycles hamiltoniens de } Q_n.$$

Il y a n décompositions possibles en $(n - 1)$ cubes. Il y a donc $n(n - 1)^{-1} h^2(n - 1) 2^n$ constructions possibles (un même cycle pouvant être construit plusieurs fois).

Mais les cycles que nous venons de construire ont la propriété d'utiliser exactement 2 fois le nombre de transition correspondant à l'arête $\{x, \bar{x}\}$. D'après le lemme, un cycle hamiltonien de Q_n sera donc obtenu au plus 2 fois par notre construction d'où (3).

Essayons de majorer le nombre de cycles obtenus exactement 2 fois. Supposons que K soit un cycle de Q_n obtenu 2 fois par notre construction. Soient p et q les nombres de transition ayant 2 occurrences dans K . Décomposons K suivant la direction p en deux $(n - 1)$ cubes. Pour que q apparaisse exactement 2 fois dans le cycle K , il faut qu'il ait 2 occurrences dans les cycles H et H' et que q corresponde au nombre de transition associé aux arêtes $\{x, y\}$ et $\{\bar{x}, \bar{y}\}$. Or d'après le lemme il y a donc au plus $h(n - 1)$ choix pour H , 4 pour $\{x, y\}$, et $2h(n - 1)/(n - 1)$ pour H' . Comme n choix sont possibles pour p et que chaque cycle est obtenu 2 fois; le nombre de cycles obtenus 2 fois est au plus:

$$h(n - 1) \cdot 4 \cdot \frac{2h(n - 1)}{n - 1} \cdot \frac{n}{2}.$$

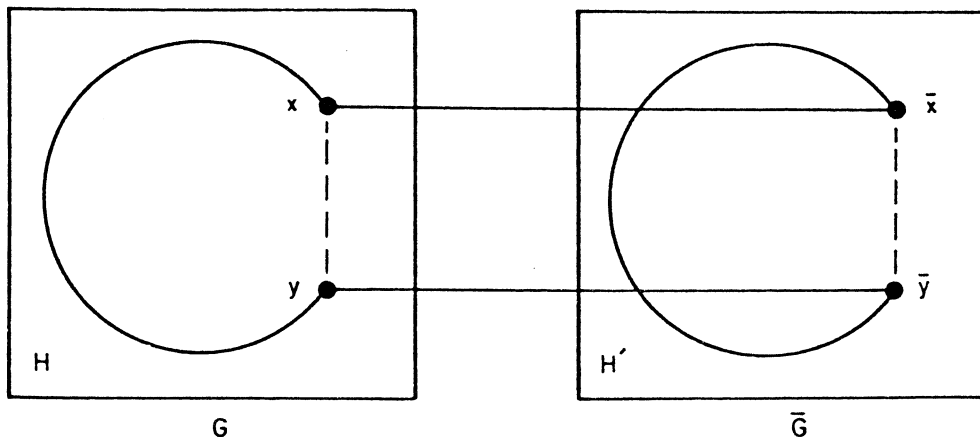


FIGURE 1.

On a donc:

$$h(n) \geq \frac{n(2^n - 4)}{n - 1} h^2(n - 1), \quad n \geq 3.$$

Ce qui constitue pour $n > 3$ un meilleur minorant que le résultat (3) de Douglas.

3. MAJORANT DE $h(n)$

Un sommet x de Q_n étant choisi, une décomposition en couches de Q_n est alors A_0, A_1, \dots, A_n , où A_i est l'ensemble des sommets à distance i de x . Posons $n_i = |A_i|$, on a alors $n_i = \binom{n}{i}$ et un sommet de A_i est relié à i sommets de A_{i-1} . La majoration (2) provient de la remarque: un cycle hamiltonien définit de manière injective une paire d'arêtes adjacentes pour chaque sommet de $A_2 \cup A_4 \cup \dots \cup A_{2\lfloor n/2 \rfloor}$. Or cet ensemble est de cardinal $2^{n-1} - 1$ d'où

$$h(n) \leq \left(\frac{n(n-1)}{2} \right)^{2^{n-1}-1}$$

ou de manière équivalente:

$$h(n) \leq \prod_{i=1}^{\lfloor n/2 \rfloor} \left(\frac{n(n-1)}{2} \right)^{\binom{n}{2i}} \quad (5)$$

PROPOSITION 1. *Le nombre d'arêtes d'un cycle hamiltonien entre A_i et A_{i+1} est $2^{\binom{n-1}{i}}$*

La preuve se fait par récurrence. Il y a bien 2 arêtes entre A_0 et A_1 , et comme $2\binom{n}{i+1}$ est la somme du nombre d'arêtes entre A_i et A_{i+1} et du nombre d'arêtes entre A_{i+1} et A_{i+2} , en utilisant l'hypothèse de récurrence le nombre d'arêtes entre A_{i+1} et A_{i+2} est bien $2\binom{n}{i+1} - 2\binom{n-1}{i} = 2\binom{n-1}{i+1}$.

Pour un cycle hamiltonien fixé, posons $A_i = Q_i \cup R_i \cup S_i$ où $x \in Q_i$ (respectivement R_i et S_i) si x est relié dans le cycle à 2 (respectivement 1 et 0) sommets de A_{i-1} . Posons $q_i = |Q_i|$, $r_i = |R_i|$ et $s_i = |S_i|$.

PROPOSITION 2. *Pour tout i nous avons les relations:*

$$2q_i + r_i = 2\binom{n-1}{i}, \quad (6)$$

$$2s_i + r_i = 2\binom{n-1}{i}, \quad (7)$$

$$q_i + r_i + s_i = \binom{n}{i}. \quad (8)$$

Les relations (6) and (7) sont obtenues en dénombrant les arêtes entre respectivement A_i , A_{i-1} et A_i , A_{i+1} .

Nous avons rappelé qu'on peut associer à chaque cycle hamiltonien, de manière injective, une paire d'arêtes adjacentes pour chaque sommet de $A_2 \cup A_4 \cup \dots \cup A_{2\lfloor n/2 \rfloor}$. Les paires d'arêtes associés aux sommets de chaque couche A_p définissent des nombres q_p, r_p, s_p vérifiant la proposition 2.

Respectivement la donnée des entiers q_p, r_p, s_p définie au plus $N(q_p, r_p, s_p)$ paires d'arêtes, où

$$N(q_p, r_p, s_p) = \binom{\binom{n}{p}}{q_p} \binom{\binom{n}{p} - q_p}{r_p} (p(n-p))^{r_p} \left(\frac{p(p-1)}{2} \right)^{q_p} \\ \times \left(\frac{(n-p)(n-p-1)}{2} \right)^{s_p}$$

si q_p, r_p, s_p sont tous positifs et $N(q_p, r_p, s_p) = 0$ sinon. La majoration de Dixon et Goodman revient à utiliser la seule relation $q_p + r_p + s_p = \binom{n}{p}$ donc à écrire:

$$h(n) \leq \prod_{i=1}^{\lfloor n/2 \rfloor} \alpha_{2i}$$

où

$$\alpha_{2i} = \alpha_p = \sum_{q_p=0}^{\binom{n}{p}} \sum_{r_p=0}^{\binom{n}{p}-q_p} N(q_p, r_p, \binom{n}{p} - q_p - r_p).$$

α_p est donc le développement de $(P(n-p) + \frac{1}{2}P(p-1) + \frac{1}{2}(n-p)(n-p-1))^{\binom{n}{p}}$ c'est à dire de $(\frac{1}{2}n(n-1))^{\binom{n}{p}}$, et on retrouve bien (5) soit le résultat de Dixon et Goodman.

Mais les relations (6) and (7) de la proposition 2 montrent que les valeurs de q_p et de r_p sont liées. On peut donc obtenir:

THÉORÈME 2.

$$h(n) \leq \prod_{i=1}^{\lfloor n/2 \rfloor} \beta_{2i}$$

où

$$\beta_{2i} = \beta_p = \sum_{q_p=0}^{\binom{n}{p}} N(q_p, 2(\binom{n-1}{p-1} - q_p), \binom{n}{p} - 2(\binom{n-1}{p-1}) + q_p),$$

ce qui constitue bien entendu une meilleure majoration de $h(n)$ (car trivialement $\beta_p < \alpha_p$). Numériquement on obtient ainsi $h(5) \leq 7.23 \cdot 10^{13}$ et $h(6) \leq 8.47 \cdot 10^{34}$ à comparer à $h(5) \leq 10^{15}$ et $h(6) \leq 2.88 \cdot 10^{36}$ de Dixon et Goodman.

D'autre part, Douglas a introduit le raffinement (4) qui consiste à remarquer que pour caractériser un cycle hamiltonien, il suffit de connaître les paires d'arêtes adjacentes aux sommets de $A_0 \cup A_2 \cup \dots \cup A_{2\lfloor n/2 \rfloor}$ privé d'un code binaire à distance 4 de parité constante (ensemble de sommets C tel que $\forall x \in C, \forall y \in C, d(x, y) \geq 4$). On pourrait également appliquer cette méthode à notre construction.

Pour terminer, remarquons qu'on peut faire la même construction sur $A_1 \cup A_3 \cup \dots \cup A_{2\lfloor n/2 \rfloor - 1}$. Si n est pair on obtient alors une deuxième majoration en général de valeur différente:

$$h(n) \leq \prod_{i=1}^{\lfloor n/2 \rfloor} \beta_{2i-1},$$

où la définition de $\beta_{2i-1} = \beta_p$ reste inchangée.

REFERENCES

1. E. Dixon and S. Goodman, An algorithm for finding all the Hamiltonian circuits and two factors in an arbitrary directed or undirected graph, DAMACS Technical Report, 3-73, University of Virginia, Charlottesville, VA, 1973.
2. E. Dixon and S. Goodman, On the number of Hamiltonian circuits in the n -cube, *Proc. Am. Math. Soc.* **50** (1975), 500-504.
3. R. J. Douglas, Bounds on the number of Hamiltonian circuits in the n -cube, *Discrete Math.* **17** (1977), 143-146.
4. H. L. Abbott, Hamiltonian circuits and paths on the n -cube, *Canad. Math. Bull.* **9**, (1966) 557-562.
5. M. Gardner, The curious properties of the Gray code, *Scientific American* (2), **227** (Aout 1972) 106-109.
6. D. Singmaster, Enumerating unlabelled Hamiltonian circuits, *Numerische Methoden bei graphentheoretischen und kombinatorischen Problemen, Internat. Series of Numerical Math* **29** (1975).

Received 10 January 1988

M. MOLLARD

Laboratoire LSD (I.M.A.G.), B.P. 68, 38402 Saint Martin d'Hères, France

Chapitre 4

Problèmes de valuations de type gracieux

Considérons une valuation g des sommets d'un graphe simple connexe $G=(V,E)$ par des entiers distincts de $\{0,1,\dots, |E|\}$. Une telle valuation des sommets induit une valuation des arêtes définie par $h(\{x,y\}) = |g(x)-g(y)|$. G est dit gracieux s'il existe une valuation g de ses sommets telle que h soit une bijection de E dans $\{1,\dots,|E|\}$.

Depuis leur introduction en théorie des graphes (Rosa [10]) les graphes gracieux ont suscité de nombreuses recherches (pour un survey voir les articles de Bermond[4], Bloom [5]) particulièrement pour résoudre la conjecture suivante de Kotzig pour certaines familles d'arbres.

Conjecture: (Kotzig)

Tous les arbres sont gracieux.

Deux versions "additives" de ce type de valuations ont été proposées:

Définition:

Un graphe $G=(V,E)$ est dit harmonieux (Graham et Sloane [8]) s'il est possible de valuer les sommets de G par des entiers distincts de $\{0,1,\dots,|E|-1\}$ de telle manière que la valuation induite sur les arêtes par

$$h(\{x,y\}) = g(x) + g(y) \quad \text{mod } |E|$$

soit une bijection de E dans $\{0,1,\dots,|E|-1\}$.

Les graphes élégants sont plus proches des graphes gracieux par leur définition :

Définition:

Un graphe $G=(V,E)$ est dit élégant (Chang,Hsu,Rogers [7]) si il est possible de valuer les sommets de G par des entiers distincts de $\{0,1,\dots,|E|\}$ de telle manière que la valuation induite sur les arêtes par

$$h(\{x,y\}) = g(x) + g(y) \pmod{|E|+1}$$

soit une bijection de E dans $\{1, \dots, |E|\}$.

Le tableau suivant indique le caractère gracieux G , harmonieux H ou élégant E de quelques graphes ayant peu d'arêtes par rapport au nombre de sommets.

	Gracieux	Harmonieux	Elégant
Chaînes	G	H	$E(n \neq 4)$
Arbres	$G ?$	$H ?$	
Cycles C_{4m}	G	non H	E
C_{4m+1}	non G	H	non E
C_{4m+2}	non G	non H	E
C_{4m+3}	G	H	E

Nous prouvons dans un premier temps que les cycles sur n sommets ($n \equiv 2 \pmod{4}$) sont élégants, les cas $n \equiv 0 \pmod{4}$ et $n \equiv 3 \pmod{4}$ ayant été déjà résolus (Chang, Hsu, Rogers [7]).

Nous donnons ensuite une interprétation géométrique des valuations élégantes de P_n qui permet de trouver une valuation plus simple de P_{4m} que celle précédemment donnée par I. Cahit[6].

On s'intéressera également à la valuation des sommets de G par des parties d'un ensemble S de telle façon que les différences symétriques sur les arêtes correspondent pour les graphes set-gracieux à toutes les parties non vides de S , ou pour les graphes Hamming-gracieux soient de tous les cardinaux possibles (donc de 1 à $|S| = |E|$).

B.D. Acharya avait conjecturé [1],[2],[3] que les cycles C_{2p-1} et les graphes complets pour lesquels il existe m avec $n = \frac{1+\sqrt{2m+3-7}}{2}$ étaient set-gracieux.

Nous prouvons qu'effectivement les C_{2p-1} sont set-gracieux., mais que seuls K_2 , K_3 et K_6 le sont parmi les graphes complets.

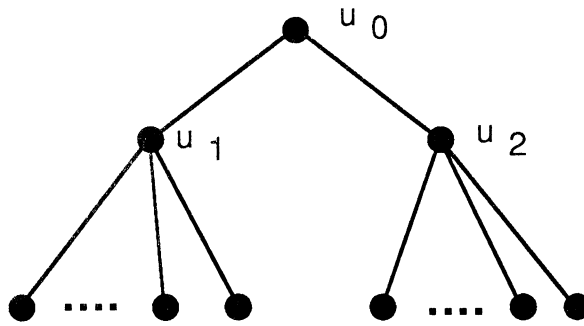
Les arbres et les cycles C_n ($n \equiv 0 \pmod{4}$ ou $n \equiv 3 \pmod{4}$) sont eux Hamming-gracieux.

A. Hartman[9] a proposé de rechercher l'ensemble $M(K_n)$ des graphes qui peuvent apparaître comme sous graphes partiels multicoloriés d'une coloration optimale des arêtes de K_n .

Ce problème est lié aux précédents. En effet, dans la coloration optimale classique de K_{2p+1} on value les sommets par $0,1,\dots,2p$ et on colore une arête $\{a,b\}$ avec la couleur $a+b \pmod{2p+1}$. Un graphe harmonieux avec $2p+1$ arêtes est donc un sous graphe partiel de K_{2p+1} multicolorié pour cette coloration.

De même, une coloration optimale de K_{2^n} peut s'obtenir en valant les sommets par les parties d'un ensemble à n éléments et en colorant chaque arête par la partie obtenue comme différence symétrique des parties valant ses extrémités. Un graphe set-gracieux avec 2^n-1 arêtes est alors un sous graphe partiel de K_{2^n} multicolorié pour cette coloration.

A. Hartman[9] a conjecturé que les chaînes P_n ($n \neq 4,6$) sont dans $M(K_n)$ de même que les arbres sauf ceux, sur un nombre pair n de sommets, constitués d'un sommet u_0 de degré 2 dont les deux voisins u_1 et u_2 sont



de degré total $n-1$ (en effet dans K_n l'arête liant u_1 et u_2 doit être d'une couleur différente des $n-1$ autres).

Nous prouvons la conjecture sur les chaînes en étudiant successivement les cas n impair, $n \equiv 2 \pmod{6}$, $n \equiv 4 \pmod{6}$, $n \equiv 0 \pmod{12}$ et $n \equiv 6 \pmod{12}$.

REFERENCES

- [1] B.D. Acharya, Set valuations of graphs and their applications, MRI Lecture Note in Applied Mathematics n°2, MRI, Allahabad (1983).
- [2] B.D. Acharya, Set valuations of graphs and their applications, MRI Technical Report of DST research problem, MRI, Allahabad (1986).
- [3] B.D. Acharya, Session de problèmes de la troisième Conférence "Théorie des Graphes et Combinatoire, Marseille (1986).
- [4] J.C. Bermond, Graceful graphs, radio antennae and French windmills, dans Problèmes de Théorie des Graphes et de Combinatoire, Edition du CNRS, Paris (1978) 35-38.
- [5] G.S. Bloom, A chronology of the Ringel-Kotzig conjecture and the continuing quest to call all trees graceful, Annals N.Y. Acad. Sci. 326 (1979) 32-51.
- [6] I. Cahit, Elegant valuation of the paths, Ars Combinatoria 16(1983) 223-227.
- [7] C.J. Chang, D.F. Hsu, D.G. Rogers, Additive variations on graceful theme, Congressus Numeratum 32 (1981) 181-197.
- [8] R.L. Graham, N.J.A. Sloane, On additive bases and harmonious graphs, SIAM Alg. Disc. Meth. vol1 n°4(1980) 382-404.
- [9] A. Hartman, Partial triple systems and edge colourings, Discrete Mathematics 62 (1986) 183-196.
- [10] A. Rosa, On certain valuations of the vertices of a graph, dans Theory of graphs, Dunod Paris (1967) 349-355.

On two conjectures about set-graceful graphs

M.Mollard
C.Payan

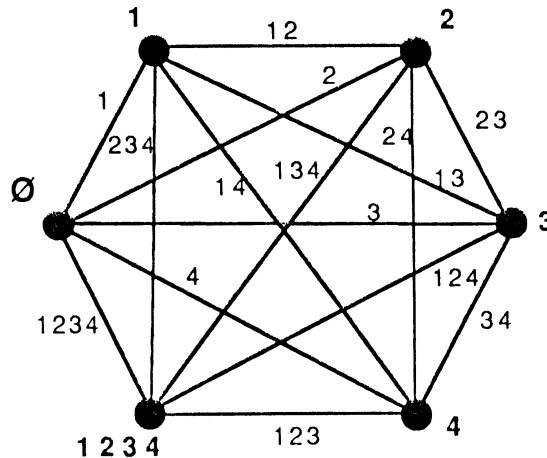
LSD (IMAG) BP 68
38402 St Martin d'Hères
France

0. Introduction.

B.D.Acharya [1] has introduced the notion of set-graceful graphs, a set analogue of the well known graceful numbering of graphs.

Following this author a set-indexer of a graph $G=(V,E)$ is an injective set assignment $f : V \rightarrow 2^X$ (where 2^X is the power-set of X) such that the induced set assignment on edges $f^\Delta : E \rightarrow 2^X$ defined by $f^\Delta (\{u,v\}) = f(u) \Delta f(v) \forall \{u,v\} \in E(G)$ is also injective (where Δ is the symmetric difference).

A graph is set-graceful if there exists a non empty set X and a set indexer $f : V \rightarrow 2^X$ such that $f^\Delta (E) = 2^X - \{\emptyset\}$.



A set-graceful labelling of K_6 .

B.D Acharya gives the following conjectures [1], [2]:

Conjecture1.

For every integer $m \geq 2$ the cycle of length $2^m - 1$ is set-graceful.

This conjecture was also proposed in an equivalent formulation during the problem session at the third International Conference "Théorie des Graphes et Combinatoire" in Marseille (June 86) .

A necessary condition for a graph to be set-graceful is clearly $|E(G)| = 2^{m-1}$. For a complete graph K_n this gives $n = \frac{1+\sqrt{t}}{2}$ with $t=2^{m+3}-7$

Conjecture2.

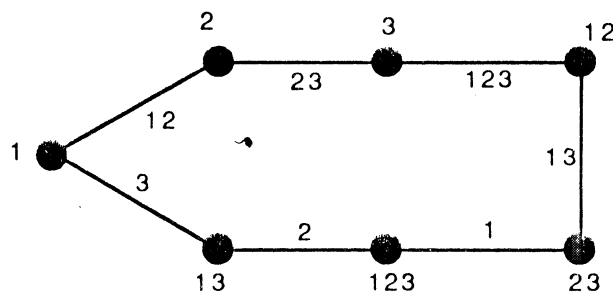
For every integer m such that $t=2^{m+3}-7$ is a perfect square the complete graph of order $n = \frac{1+\sqrt{t}}{2}$ is set-graceful.

In this note we prove the first conjecture and disprove the second.

1.Proof of Conjecture1.

Let p be a prime and consider the polynomials with coefficients in $GF(p)$. Basic results on finite fields or random number generators tell us that for every integer m and every prime p there is at least one primitive polynomial of degree m over $GF(p)$ (see for example [3] or [4]). Such a polynomial $P(x)$ is irreducible and $\{ x^i \text{ mod } P(x) , i = 1, \dots, p^m-1 \}$ is the set of all non-zero polynomials over $GF(p)$ of degree at most $m-1$. Let $X = \{1, \dots, m\}$. If we take such a polynomial with $p=2$ and label the successive vertices of C_{2^m-1} (following an arbitrary orientation) by $x, x^2, \dots, x^{2^m-1} \text{ (mod } P(x))$ we know that we have all non zero polynomials of degree at most $m-1$ over $GF(2)$ and thus every non-empty subset of X (associating to the polynomial $a_1+a_2x+\dots+a_mx^{m-1}$ the set $\{i \in X / a_i \neq 0\}$).

Now if we take two consecutive vertices labeled Y and Z associated to $x^i \text{ (mod } P(x))$ and $x^{i+1} \text{ (mod } P(x))$, the set $Y \Delta Z$ is associated to the polynomial $x^i + x^{i+1} \text{ (mod } P(x))$. Assuming that $x^i + x^{i+1} \equiv x^j + x^{j+1} \text{ (mod } P(x))$ with $j \geq i$, we have $x^i(x+1)(1+x^{j-i}) \equiv 0 \text{ (mod } P(x))$. But $P(x)$ is irreducible and hence divides neither $x+1$ nor x^i . Therefore $1+x^{j-i} \equiv 0 \text{ (mod } P(x))$, but $j-i < 2^m-1$ thus $j = i$.



A set-graceful labelling of C_7 induced by the primitive polynomial x^3+x+1 .

In fact if we consider the polynomials $x^i + x^{i+u_1} + x^{i+u_2} + \dots + x^{i+u_k}$ with $u_1 < u_2 < \dots < u_k < m$ we have also the same property because equality of two values implies $x^i (1 + x^{u_1} + x^{u_2} + \dots + x^{u_k}) (1 + x^{j-i}) \equiv 0 \pmod{P(x)}$ therefore $1 + x^{j-i} \equiv 0 \pmod{P(x)}$ and then $j=i$.

Given an arbitrary orientation to C_{2^m-1} let h be the mapping from $GF(2)^m$ to $GF(2)^m$ (viewed as vector space of polynomials of degree $\leq m-1$ and coefficients in $GF(2)$) which maps the polynomial associated to a vertex to the polynomial associated to its successor, and with $h(0) = 0$. It is easy to prove that by the above construction using all primitive polynomials we obtain all labellings such that h is linear. An interesting open question would be the existence of a labelling such that h is non linear.

2. Disproof of Conjecture 2.

The first values of m such that $2^{m+3} - 7$ is a perfect square are 1, 2, 4, 12 which gives $n=2, 3, 6$ and 91. K_2, K_3 and K_6 are set-graceful but K_{91} is not. In fact K_2, K_3 and K_6 are the only set-graceful complete graphs. T. Nagell [5] has prove that there is no integer m greater than 12 such that $2^{m+3} - 7$ is a perfect square. Therefore we can only consider the case $m=12$; but our disproof is elementary and is independent of the value of m then we prefer look at the general case without using the above result.

Assume then $|E(K_n)| = 2^{m-1}$ with $m \geq 2$ and that K_n is set-graceful. In a set of cardinality m there are 2^{m-1} subsets of each parity. Consider a partition of $V(K_n)$ in A and B with $\forall x \in A$ (resp. B) $f(x)$ is odd (resp. even). By symmetric difference between a vertex of A and one of B we obtain all the odd subsets of X thus

$$(1) \quad |A| \cdot |B| = 2^{m-1}$$

Therefore $|A|$ and $|B|$ are powers of 2. By Symmetric difference between the vertices of A and between the vertices of B we obtain all the even non empty subsets of X , thus

$$(2) \quad \frac{|A| (|A| - 1)}{2} + \frac{|B| (|B| - 1)}{2} = 2^{m-1} - 1$$

Therefore one of the terms is odd, say $\frac{|A| + |A|-1}{2}$. Then $|A| = 2$ and therefore $|B| = n-2$ and

$$(3) \quad 2^{m-1} = |A| \cdot |B| = 2(n-2)$$

$$(4) \quad 2^{m-1} = \frac{|A|(|A|-1)}{2} + \frac{|B|(|B|-1)}{2} + 1 = 2 + \frac{(n-2)(n-3)}{2}$$

(3) and (4) have no other solution than $n=3$ or 6 .

In fact if we consider the polynomials $x^i + x^{i+u_1} + x^{i+u_2} + \dots + x^{i+u_k}$ with $u_1 < u_2 < \dots < u_k < m$ we have also the same property because equality of two values implies $x^i (1 + x^{u_1} + x^{u_2} + \dots + x^{u_k}) (1 + x^{j-i}) \equiv 0 \pmod{P(x)}$ therefore $1 + x^{j-i} \equiv 0 \pmod{P(x)}$ and then $j=i$.

Given an arbitrary orientation to C_{2^m-1} let h be the mapping from $GF(2)^m$ to $GF(2)^m$ (viewed as vector space of polynomials of degree $\leq m-1$ and coefficients in $GF(2)$) which maps the polynomial associated to a vertex to the polynomial associated to its successor, and with $h(0) = 0$. It is easy to prove that by the above construction using all primitive polynomials we obtain all labellings such that h is linear. An interesting open question would be the existence of a labelling such that h is non linear.

2. Disproof of Conjecture 2.

The first values of m such that $2^{m+3} - 7$ is a perfect square are 1, 2, 4, 12 which gives $n=2, 3, 6$ and 91. K_2, K_3 and K_6 are set-graceful but K_{91} is not. In fact K_2, K_3 and K_6 are the only set-graceful complete graphs. T. Nagell [5] has prove that there is no integer m greater than 12 such that $2^{m+3} - 7$ is a perfect square. Therefore we can only consider the case $m=12$; but our disproof is elementary and is independent of the value of m then we prefer look at the general case without using the above result.

Assume then $|E(K_n)| = 2^{m-1}$ with $m \geq 2$ and that K_n is set-graceful. In a set of cardinality m there are 2^{m-1} subsets of each parity. Consider a partition of $V(K_n)$ in A and B with $\forall x \in A$ (resp. B) $f(x)$ is odd (resp. even). By symmetric difference between a vertex of A and one of B we obtain all the odd subsets of X thus

$$(1) \quad |A| \cdot |B| = 2^{m-1}$$

Therefore $|A|$ and $|B|$ are powers of 2. By Symmetric difference between the vertices of A and between the vertices of B we obtain all the even non empty subsets of X , thus

$$(2) \quad \frac{|A| (|A| - 1)}{2} + \frac{|B| (|B| - 1)}{2} = 2^{m-1} - 1$$

Therefore one of the terms is odd, say $\frac{|A| + |A|-1}{2}$. Then $|A| = 2$ and therefore $|B| = n-2$ and

$$(3) \quad 2^{m-1} = |A| \cdot |B| = 2(n-2)$$

$$(4) \quad 2^{m-1} = \frac{|A|(|A|-1)}{2} + \frac{|B|(|B|-1)}{2} + 1 = 2 + \frac{(n-2)(n-3)}{2}$$

(3) and (4) have no other solution than $n=3$ or 6 .

REFERENCES

- [1] B.D.Acharya. Set valuations of graphs and their applications, MRI Lecture Note in Applied Mathematics, n° 2 (MRI, Allahabad, 1983)
- [2] B.D.Acharya. Set valuations of graphs and their applications, Technical Report of DST research project (MRI, Allahabad, 1986)
- [3] N.J.A.Sloane F.J.MacWilliams . The theory of error-correcting codes North-Holland 1978
- [4] R.A.Dean . Elements of abstract Algebra John Wiley & Sons 1966
- [5] T.Nagell . Nordisk Mat. Tidskr. (30), 1948, p. 62-64

Graceful Problems.

Michel Mollard €
Charles Payan €
Sun Shi Xin \$

€ LSD (IMAG) BP 68
38402 St Martin d'Hères France
\$ Institut d'ingénieurs Radio
BP 83 Cengdu, République Populaire de Chine

Abstract. A graph $G=(V,E)$ is said to be graceful if it is possible to value its vertices by an injective mapping g in $\{0,1,\dots,|E|\}$ such that the induced valuation h on the edges defined by $h(x,y)=|g(x)-g(y)|$ take all the possible values: $\{1,\dots,|E|\}$. Many similar problems have been introduced (elegant, harmonious, set graceful...-graphs).

We present here some results on this kind of problems and introduce the following common formulation :

Consider an injective valuation of the vertices of a graph by the elements of some set and an induced valuation of the edges defined by some function f of the values of their ends. The graph is said to be f -graceful if the valuation of its edges can take all the possible values.

1. Introduction.

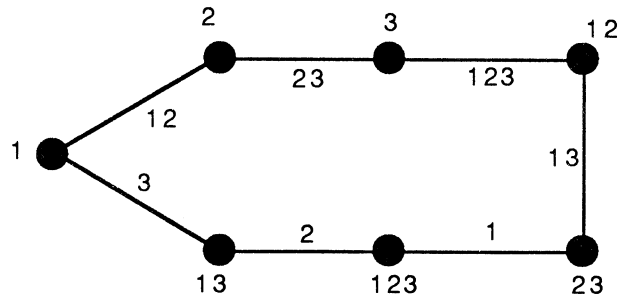
Let S,T be two finite sets. Let f be a mapping from $S \times S$ to T . A simple graph $G=(V,E)$ is said to be **f -graceful** if there exists an injective mapping g from V to S such that the induced valuation h , $h(x,y)=f(g(x),g(y))$, is a one-to-one mapping from E onto T .

When S is the set $\{0,1,\dots,|E|\}$, $T= S-\{0\}$ and f the absolute value of the difference we have the classical notion of **graceful** graphs which have raised up numerous studies motivated by the well known conjecture "*trees are graceful*" [6].

2. Set-graceful graphs.

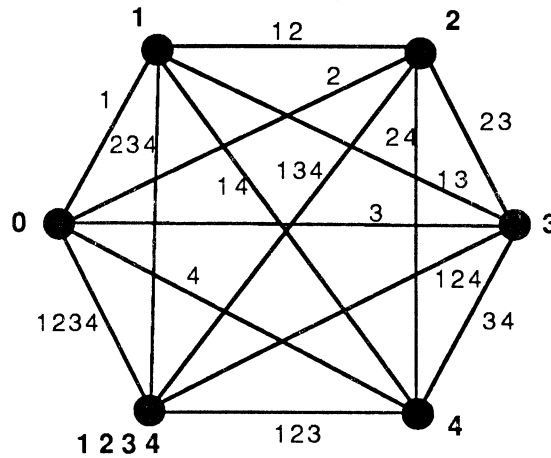
If S is the set of subsets of some set, $T= S-\{\emptyset\}$ and f is the symmetric difference we obtain the notion of (symmetric difference)-graceful graphs known as **set-graceful** graphs [1].

A trivial condition for G to be set-graceful is $|E(G)| = |S-\{\emptyset\}|$ and therefore $|E(G)| = 2^p - 1$ for some p .



A set-graceful labelling of C_7 .

The necessary condition for a cycle C_m to be set-graceful is therefore $m = 2^p - 1$ for some p .



A set-graceful labelling of K_6 .

The possible values of n for K_n to be set-graceful are

$$(1) \quad n = \frac{1 + \sqrt{t}}{2} \text{ with } t = 2^{m+3} - 7.$$

The first possible values are 2,3,6,91. In fact we have:

Proposition 1.

A cycle C_m is set-graceful if and only if $m = 2^p - 1$ for some p .

Proposition 2.

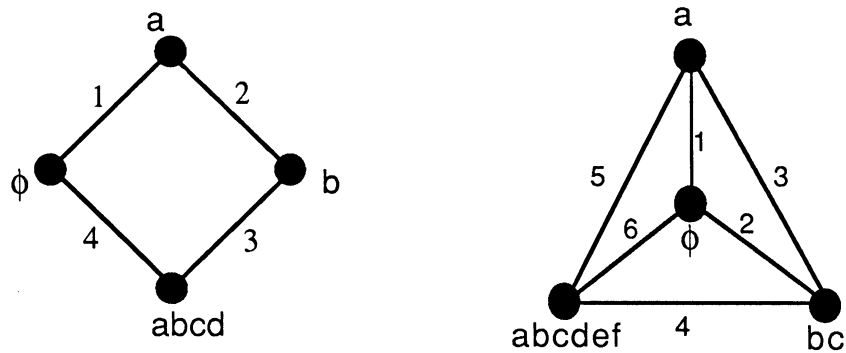
K_2, K_3, K_6 are the only set-graceful complete graphs.

The proofs of these two propositions can be found in [7]. The first result had been conjectured by B.D.Acharya [2] who had also conjectured that all complete graphs satisfying (1) are set-graceful. As shown in [7], K_{91} is the first counter-example.

3. Hamming-graceful graphs.

The Hamming distance of two subsets of a given set E is the cardinality of their symmetric difference.

With $S = \mathcal{P}(E)$, $T = \{1, 2, \dots, |S|\}$ and the Hamming distance for f we can define the notion of **Hamming-graceful** graphs.



Two Hamming-graceful graphs .

Proposition 3

Trees are Hamming-graceful.

The easy proof is left to the reader.

Proposition 4

Cycles C_n are Hamming-graceful if and only if $n \equiv 0$ or $3 \pmod{4}$.

Proof

Assume C_n to be Hamming-graceful labeled. By bipartiteness of the Hypercube every cycle on it is even therefore $1+2+\dots+n \equiv 0 \pmod{2}$ and thus $n \equiv 0$ or $3 \pmod{4}$.

Conversely, assume $n \equiv 0$ or $3 \pmod{4}$. We will prove by induction on n the existence of a required valuation such that the value of the edge x_i, x_{i+1} is $i+1$ (where integers are taken modulo n). This is true for C_3 and C_4 . Assume we have such a Hamming-graceful valuation g of C_n . There is an edge of C_n the valuation of which is 1. Without loss of generality assume its ends x_n, x_1 to be labeled ϕ and $\{1\}$, and let $E = \{1, 2, \dots, n, n+1, n+2, n+3, n+4\}$. Then the valuation g' of C_{n+4} defined by

$$\begin{aligned} g'(x_i) &= g(x_i), \quad i=1, \dots, n \\ g'(x_{n+1}) &= E - \{n+1, n+2, n+3\} \\ g'(x_{n+2}) &= \{n+1\} \\ g'(x_{n+3}) &= E - \{1, n+1\} \\ g'(x_{n+4}) &= \{1, n+1\} \end{aligned}$$

is an Hamming-graceful valuation of C_{n+4} with the above property. \square

A necessary condition for K_n to be Hamming-graceful is $n = k^2$ or k^2+2 for some k (G.Burosch, I.Havel, J.M.Laborde [9]). The sufficiency of this condition is an open problem. K_2, K_4, K_6 are known to be Hamming-graceful, the status of K_1 is unknown; we give below a Hamming-graceful valuation of the first really difficult case K_9 i.e. 9 vertices of the hypercube Q_{36} the mutual distances of which realize the 36 possible values.

$$\begin{aligned} a_1 &= 000000000 \ 000000000 \ 000000000 \ 000000000 \\ a_2 &= 110000000 \ 000000000 \ 000000000 \ 000000000 \\ a_3 &= 111111010 \ 000000000 \ 000000000 \ 000000000 \\ a_4 &= 110111011 \ 111111000 \ 000000000 \ 000000000 \\ a_5 &= 111101100 \ 000111111 \ 111111110 \ 000000000 \\ a_6 &= 111000001 \ 111111111 \ 111111111 \ 111100000 \\ a_7 &= 111100101 \ 111111111 \ 111111111 \ 111111110 \\ a_8 &= 111111111 \ 111111111 \ 111111111 \ 111111110 \\ a_9 &= 111111111 \ 111111111 \ 111111111 \ 111111111 \end{aligned}$$

A solution on K_9

	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
a_1	2	7	13	20	26	32	35	36
a_2		5	11	18	24	30	33	34
a_3			8	17	27	31	28	29
a_4				19	21	25	22	23
a_5					12	14	15	16
a_6						6	9	10
a_7							3	4
a_8								1

Remark.

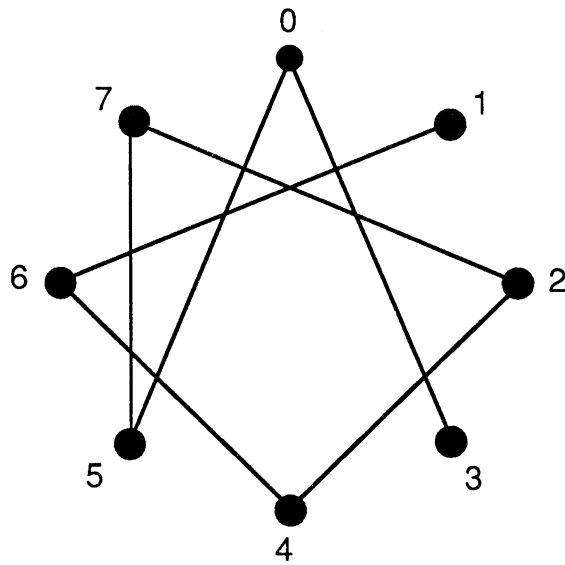
Instead of considering the "Hamming-distance", i.e. the distance on the Hypercube, we can consider the distance on any graph H .

For example if H is a path we obtain the usual notion of graceful-graph.

4 Harmonious and elegant graphs.

When $S = T = \{0, 1, \dots, m\}$ and f is the sum modulo $m+1$ we get the **harmonious** graphs introduced by R.L.Graham and N.J.A. Sloane [4].

A variant of this notion is the one of **elegant** graphs introduced by G.J.Chang, D.F.Hsu and D.G.Rogers [5] : for harmonious graph we want $T = \{0, 1, \dots, m\}$ as values on the edges, whereas for elegant graphs we want only $T = \{1, \dots, m\}$.



An elegant valuation of P_8 .

Proposition 5.

Paths on n vertices ($n \neq 4$) are elegant.

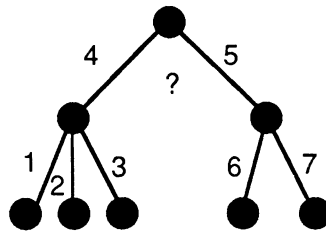
This result had been conjectured by G.J.Chang, D.F.Hsu and D.G.Rogers [5]; a proof can be found in [8].

5 An associated coloring problem.

Consider K_{2n+1} with vertices labeled by $\{0, 1, \dots, 2n\}$. If we color the edge a, b with the color $a+b \pmod{2n+1}$ we obtain an optimal edge-coloration of K_{2n+1} . Then an harmonious graph with $2n+1$ edges is a multicolored subgraph of K_{2n+1} .

Now if we label the vertices of K_{2^n} by the subsets of a set of n elements and the edges by the symmetric differences, we obtain an optimal edge coloration of K_{2^n} . Then a set-graceful graph with $2^n - 1$ edges is a multicolored subgraph of K_{2^n} .

An interesting open question is the characterization of the family $M(K_n)$ of graphs which can occur as multicolored subgraphs of K_n .



A tree not in $M(K_8)$.

A. Hartman proposed the two following conjectures [3] :

Conjecture 1

Path P_n belongs to $M(K_n)$ for $n \neq 4, 6$.

Conjecture 2

Trees belong to $M(K_n)$ except those with an odd number of edges obtained by adding pendant vertices to the extremities of a path of length 2.

We present a constructive proof of the first conjecture in [8].

REFERENCES

- [1] B.D. Acharya. Set valuations of graphs and their applications, MRI Lecture Note in applied Mathematics, n° 2 (MRI, Allahabad, 1983).
- [2] B.D. Acharya. Set valuations of graphs and their applications, Technical Report of DST research project (MRI, Allahabad, 1986).
- [3] A. Hartman. Partial triple systems and edge colourings, Discrete Mathematics 62 (1986) 183-196.
- [4] R.L. Graham and N.J.A. Sloane, On additive bases and harmonious graphs, SIAM J Alg. Disc. Meth., Vol 1 n°4 Dec 1980 382-404.
- [5] C.J. Chang, D.F. Hsu and D.G. Rogers, Additive variations on graceful theme, Congressus Numeratum, Vol 32 (1981) 181-197.
- [6] J.C. Bermond, Graceful graph, radio antennae and French windmills, Graph Theory and Combinatorics, Pitman (1979) 18-37.
- [7] M. Mollard, C. Payan, On two conjectures about set-graceful graphs, European Journal of Combinatorics Vol 10 2 (1989) 185-188 .
- [8] M. Mollard, C. Payan, Elegant valuations and colorations, submitted.
- [9] G. Burosch, I. Havel, J.M. Laborde, On distinct distance systems, Théorie des graphes et combinatoire, 3ème Colloque international, Marseille-Luminy. juin 1986.
- [10] Sun Shi Xin, Note sur l'immersion gracieuse de K_N dans Q_n , RR 637 IMAG, janvier 1987.

Elegant valuations and colorations

A proof of two conjectures of Hartman and Chang, Hsu, Rogers.

Michel Mollard
Charles Payan

LSD (IMAG) BP 53X
38041 Grenoble CEDEX
France

Abstract. A graph $G = (V, E)$ is said to be elegant if it is possible to value its vertices by an injective mapping g in $\{0, 1, \dots, |E|\}$ such that the induced valuation h on the edges defined for edge x, y by $h(x, y) = g(x) + g(y) \pmod{|E| + 1}$ takes all the values in $\{1, \dots, |E|\}$. In the first part of this paper we prove the existence of a coloring of K_n with a multicolored path on n vertices as subgraph, which had been conjectured by Hartman [2],.

In the second part we prove that the cycle on n vertices is elegant if and only if $n \not\equiv 1 \pmod{4}$ and we give a new construction of an elegant valuation of the path P_n ($n \neq 4$).

1. Introduction.

Two additive versions of the well known notion of **graceful graphs** ([3], [4], [5], [6]) have been proposed.

A connected graph with m edges is called **harmonious** if it is possible to label its vertices with distinct numbers (modulo m) in such a way that the values on the edges obtained by sums modulo m of their ends valuations are also distinct (R.L.Graham and N.J.A.Sloane [7]).

A connected graph with m edges is called **elegant** if it is possible to label its vertices with distinct numbers (modulo $m+1$) in such a way that the values on the edges obtained by sums modulo $m+1$ of their ends valuations are distinct and non zero (G.J.Chang, D.F.Hsu and D.G.Rogers [1]).

Consider K_{2n+1} with vertices labeled by $\{0, 1, \dots, 2n\}$. If we color the edge a, b with the color $a+b \pmod{2n+1}$ we obtain an optimal edge-coloration of K_{2n+1} . Then an harmonious graph with $2n+1$ edges is a multicolored subgraph of K_{2n+1} .

The aim of this paper is to answer two questions about paths and cycles : are they elegant? Does there exist an optimal edge-coloration of K_n with a multicolored path on n vertices?

2. A coloring problem.

Hartman [2] set the problem of characterizing the family $M(K_n)$ of graphs which can occur as multicolored subgraphs of K_n in a minimal edge coloring of this clique and conjectured the following result:

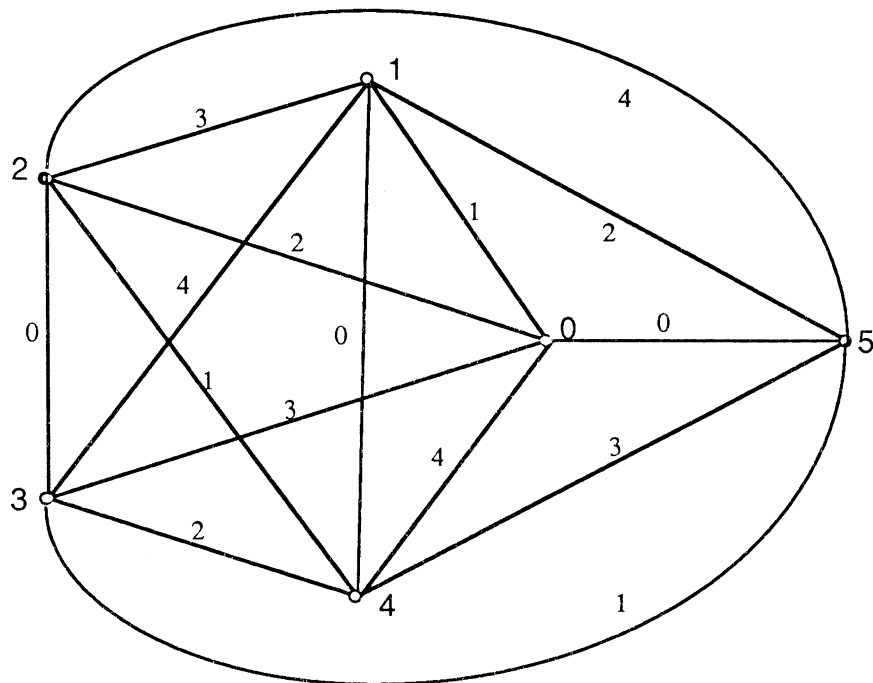
Theorem 1

Path P_n belongs to $M(K_n)$ for $n \neq 4, 6$.

Proof

In the classic way of coloring the edges of K_{2p+1} with $2p+1$ colors we label vertices by $\{0, 1, \dots, 2p\}$ and then color edges by the sum mod $2p+1$ of their ends. If we place the vertices to form a regular polygon $0, 1, \dots, 2p$, a color class in this coloration is a set of parallel edges. The boundary is a multicolored cycle and deleting one edge we obtain a multicolored path on $2p+1$ vertices.

In every optimal edge-coloration of K_{2p+1} exactly one color is missing at each vertex and all these missing colors are different. Thus we obtain a coloring of K_{2p+2} with $2p+1$ colors by coloring the edges incident to the new vertex with these missing colors.

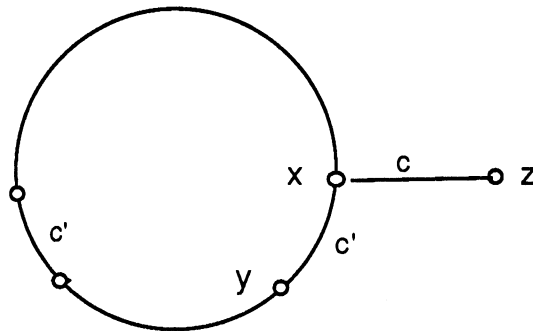


Assume we are able to color K_{2p+1} in such a way that :

-in the boundary every color appears exactly once except one color c which doesn't appear and one color c' which appears twice.

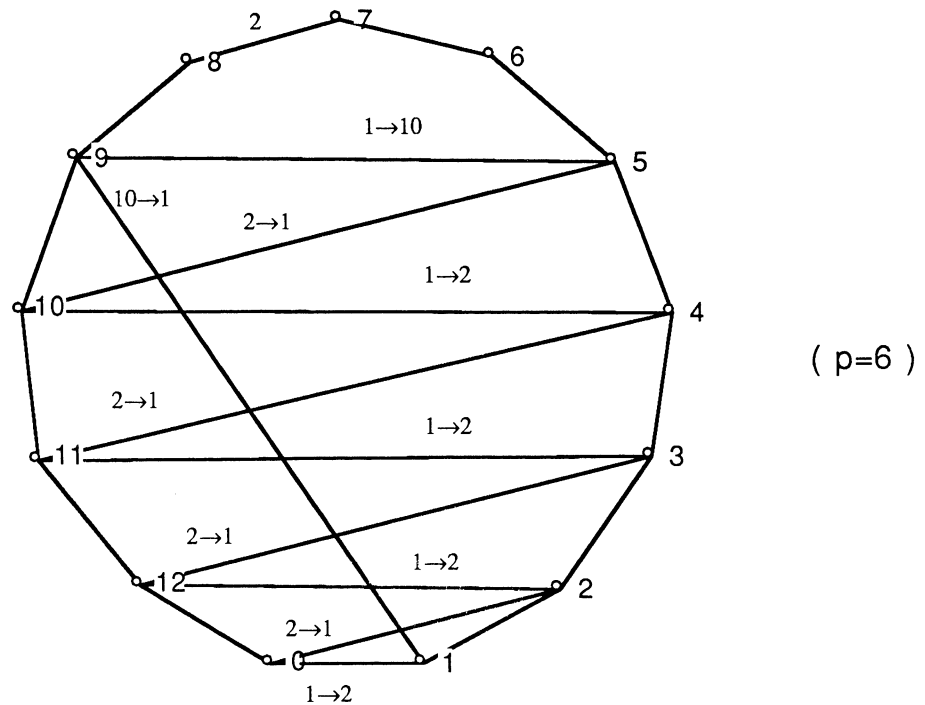
-the vertex x where c is missing is incident to an edge $\{x,y\}$ of the boundary colored with c' .

Extend this coloration to K_{2p+2} . Let z be the new vertex then $\{z,x\}$ is colored with c , and by deleting the edge $\{x,y\}$ from the boundary and adding the edge $\{x,z\}$ we obtain a multicolored path (y,\dots,x,z) .



We are now going to exhibit such a coloring of K_{2p+1} by some changes on the classical coloring defined above.

Case $p=0 \pmod{3}$.



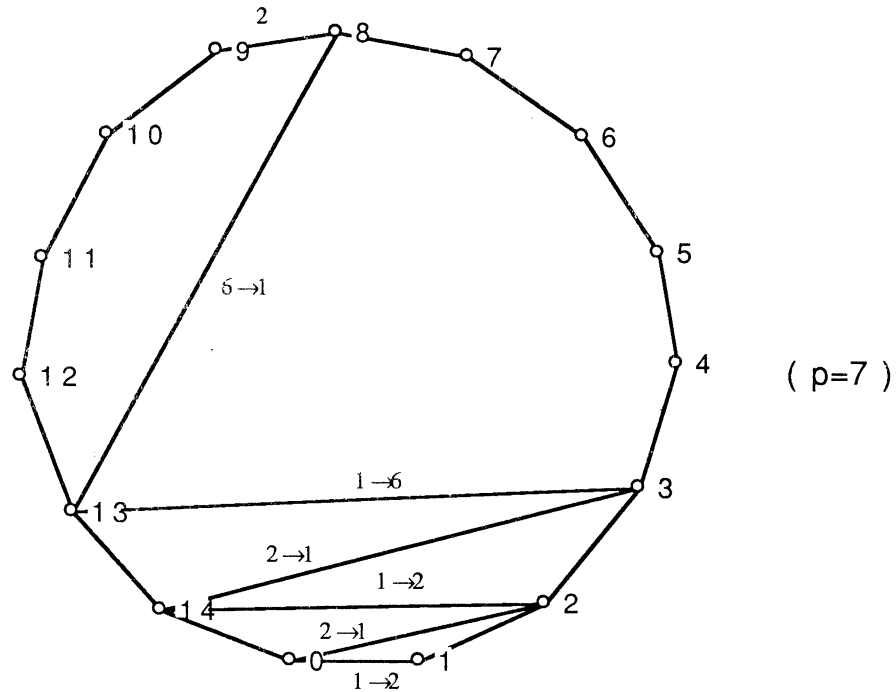
The cycle defined by the vertices $1, 0, 2, 2p, 3, 2p-1, \dots, 2p/3 + 1, 4p/3 + 1, 1$ has its edges colored $1, 2, 1, 2, \dots, 2, 1, 4p/3 + 2$. If we change

this coloration in $2, 1, 2, 1, \dots, 1, 4p/3 + 2, 1$ we have the required coloring of K_{2p+1} with $c=1, c'=2, x=p+1$ and $y= p+2$.

In the new coloring

the color missing at vertex	1	is now	$4p/3 + 2$	instead of	2,
the color missing	"	$2p/3 + 1$	"	2	" $4p/3 + 2$.

Case $p=1 \pmod 3$.



$1, 0, 2, 2p, 3, 2p-1, \dots, (p+2)/3, (5p+4)/3, p+1$ is a path colored $1, 2, 1, 2, \dots, 2, 1, (2p+4)/3$ and the color 1 is missing at $p+1$. If we change this coloration in $2, 1, 2, 1, \dots, 1, (2p+4)/3, 1$ now the color 1 is missing in 1 then we have the required coloring of K_{2p+1} with $c=1, c'=2, x=1$ and $y= 0$.

In the new coloring

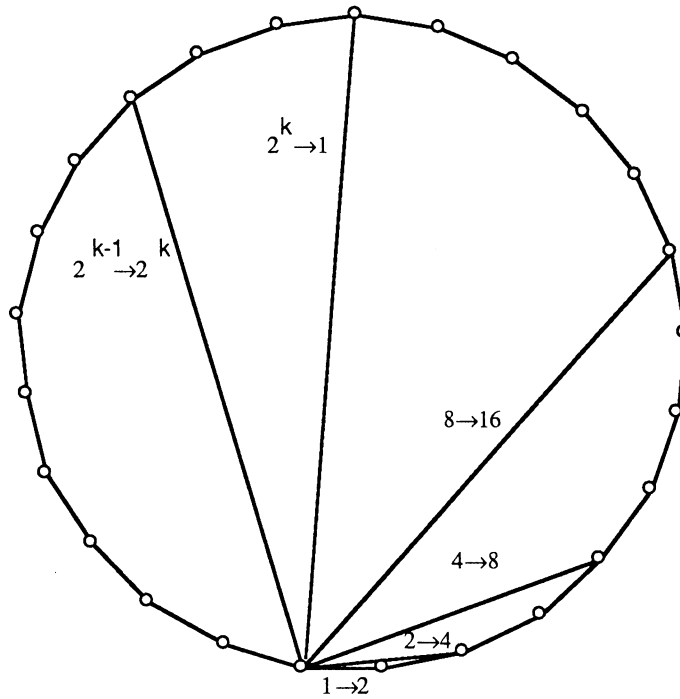
the color missing at vertex	1	is now	1	instead of	2,
the color missing	"	$p + 1$	"	$(2p+4)/3$	" 1,
the color missing	"	$(p+2)/3$	"	2	" $(2p+4)/3$

Case $p=2 \pmod 3$.

Consider the sequence of vertices $1, 2, 4, \dots, 2^k, \dots$ (taken mod $2p+1$). All

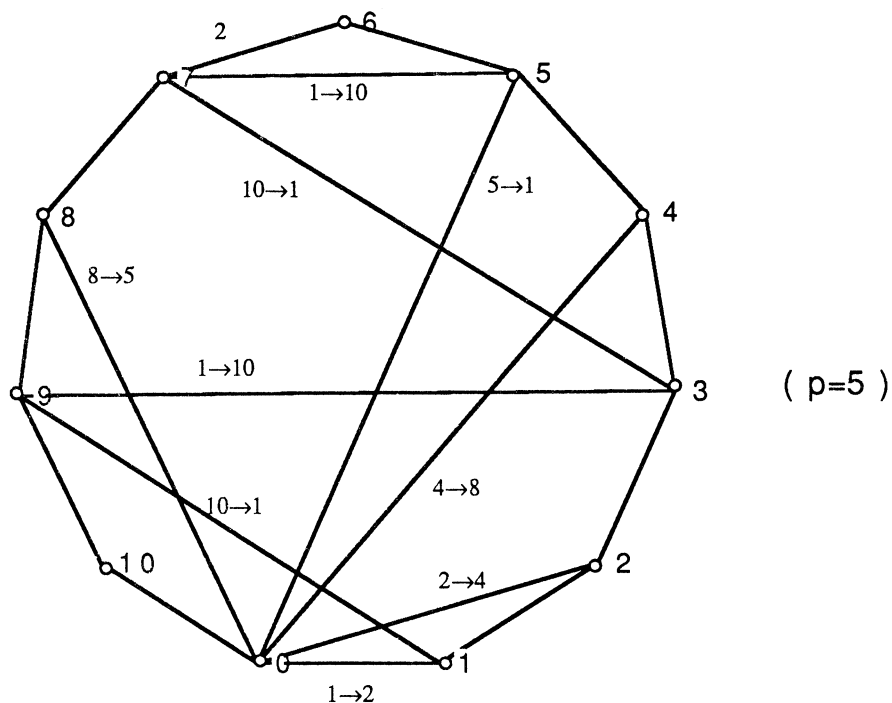
these vertices are different until 1 is met again (because $2p+1$ is odd).

Assume first that $2p$ doesn't belong to the sequence $1, 2, 4, \dots, 2^k, \dots, p+1, 1$. Then all the edges between the vertex 0 and $1, 2, 4, \dots, 2^k, \dots, p+1$ except the first one are not in the boundary. In the classical coloring for each k the edge $\{0, 2^k\}$ is colored with 2^k and the color 2^{k+1} is missing at vertex 2^k . Color this edge with 2^{k+1} . At vertex 0 we did nothing else than a rotation on the colors used for all these adjacent edges. Thus we still have a coloration. This is a required coloration with $c=1$, $c'=2$, $x=1$ and $y=0$.



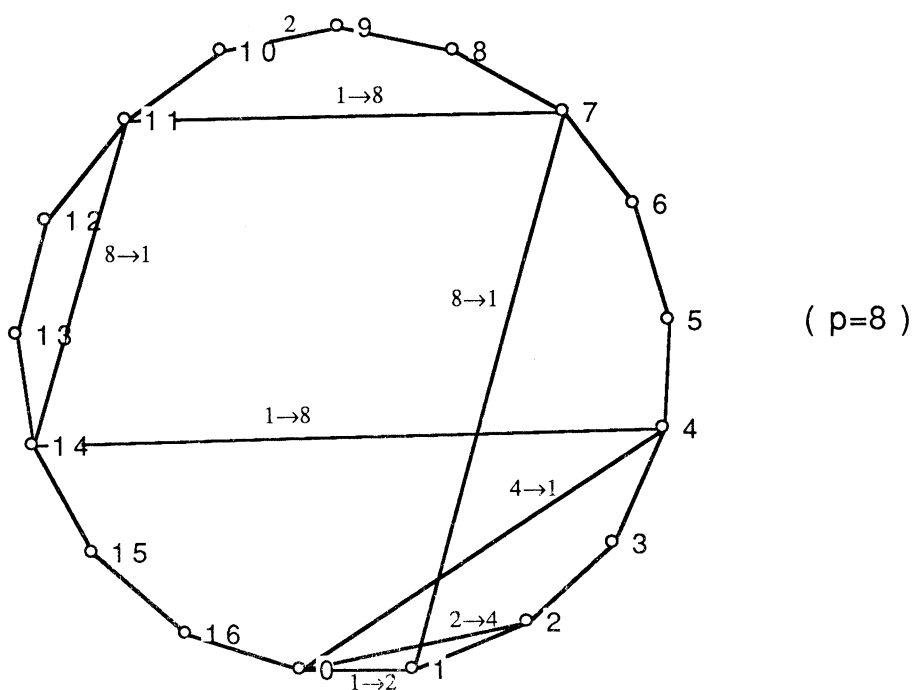
If we are not in the above case, we have a sequence of different vertices $1, 2, 4, \dots, 2^k, \dots, p, 2p$. In this case we cannot use the same change because the edge $\{0, 2p\}$ is in the boundary.

First case p is odd.



There is a path $p, p+2, p-2, p+4, p-4, \dots, 3, 2p-1, 1$ the edges of which are colored $1, 2p, 1, 2p, \dots, 1, 2p$. Consider now the sequence of edges $\{0,1\}, \{0,2\}, \{0,4\}, \dots, \{0,2^k\}, \dots, \{0,p\}, \{p,p+2\}, \{p+2,p-2\}, \{p-2,p+4\}, \dots, \{3,2p-1\}, \{2p-1,1\}$ colored $1, 2, 4, \dots, 2^k, \dots, p, 1, 2p, 1, 2p, \dots, 1, 2p$. We change these colors in $2, 4, 8, \dots, 2^{k+1}, \dots, 1, 2p, 1, 2p, \dots, 1, 2p, 1$. Then we obtain the required coloring with $c=1, c'=2, x=p+1$ and $y=p+2$.

Second case p is even.



Then $p \equiv 2 \pmod{6}$ and $p/2 \equiv 1 \pmod{3}$. There is a path $P = u_0, u_1, \dots, u_i, \dots, u_{(2p-4)/3}$ with

$$\begin{aligned} \text{for } i \equiv 0 \pmod{4}, & \quad u_i = p/2 - 3i/4 \\ \text{for } i \equiv 1 \pmod{4}, & \quad u_i = 3p/2 + 2 + 3(i-1)/4 \\ \text{for } i \equiv 2 \pmod{4}, & \quad u_i = 3p/2 - 1 - 3(i-2)/4 \\ \text{for } i \equiv 3 \pmod{4}, & \quad u_i = p/2 + 3 + 3(i-3)/4 \end{aligned}$$

So $P = p/2, 3p/2+2, 3p/2-1, p/2+3, p/2-3, 3p/2+5, 3p/2-4, p/2+6, p/2-6, \dots, 4, 2p-2, p+3, p-1, 1$.

The edges of P are colored $1, p, 1, p, \dots, 1, p$. Consider now the sequence of edges

$\{0,1\}, \{0,2\}, \{0,4\}, \dots, \{0,p/2\}, \{p/2, 3p/2+2\}, \{3p/2+2, 3p/2-1\}, \dots, \{p-1, 1\}$ colored $1, 2, 4, \dots, 2^k, \dots, p/2, 1, p, 1, p, \dots, 1, p$. We change these colors in $2, 4, \dots, 2^k, \dots, p/2, 1, p, 1, p, \dots, 1, p, 1$. Then we obtain the required coloring with $c=1, c'=2, x=p+1$ and $y=p+2$.

3. Elegant graphs.

Very few graphs are known to be elegant: cycles C_{4k} and C_{4k+3} , paths P_n ($n \neq 4$), fan f_n ...

Theorem 2.

Cycles on n vertices ($n \not\equiv 1 \pmod{4}$) are elegant.

Notice first that in an elegant valuation of the cycle C_n the sum of valuations of the edges, $1+2+\dots+n$, is equal to the sum of valuations of the vertices (modulo $n+1$). This remark gives the necessary condition $n \not\equiv 1 \pmod{4}$.

The two cases $n \equiv 0 \pmod{4}$ and $n \equiv 3 \pmod{4}$ have been previously solved by G.J.Chang, D.F.Hsu and D.G.Rogers [1] :

(1) if $n = 4p$ consider the valuation

$$\begin{aligned} & 1, 2, \dots, 2p-1, 2p, \\ & 2p+2, 2p+1, 2p+4, 2p+3, \dots, 4p, 4p-1 \end{aligned}$$

Notice that the induced valuation on the edges gives successively the odd and the even numbers.

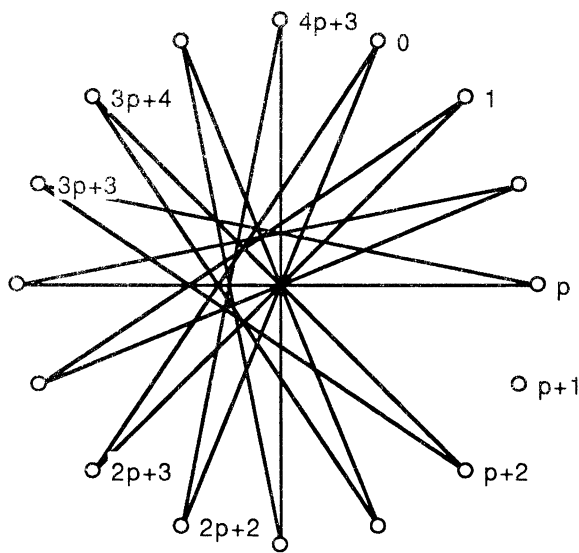
(2) if $n = 4p+3$ then we take the valuation

$0, 2p+3, 1, 2p+4, \dots, 3p+2, p, 3p+3,$
 $p+2, 3p+4, p+3, 3p+5, \dots, 2p+1, 4p+3, 2p+2$

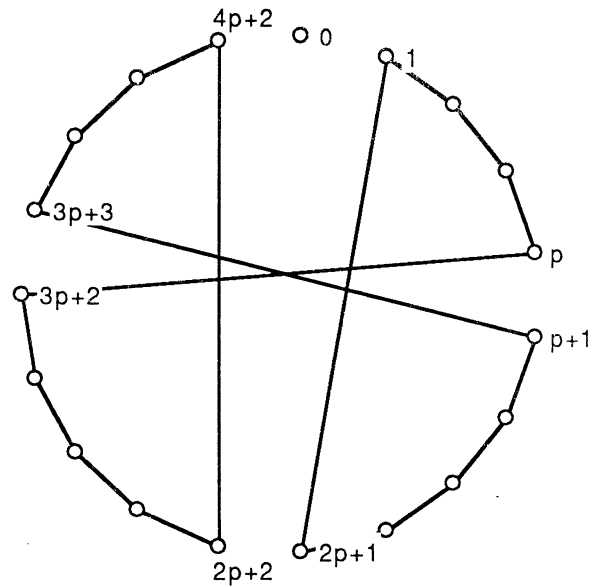
(3) if $n=4p+2$ an elegant valuation of C_{4p+2} is given by:

$1, 2, \dots, p-1, p,$
 $3p+2, 3p+1, \dots, 2p+3, 2p+2,$
 $4p+2, 4p+1, \dots, 3p+4, 3p+3,$
 $p+1, p+2, \dots, 2p, 2p+1$

It is easy to verify that the induced values on the edges are $\{1, \dots, 4p+2\}$.
 In the two later cases the geometric representation is more interpretable:



case $4p+3$



case $4p+2$

G.J.Chang, D.F.Hsu and D.G.Rogers have conjectured that paths on n vertices ($n \neq 4$) are elegant.

The case $n \neq 0 \pmod{4}$ have been proved by G.J.Chang, D.F.Hsu and D.G.Rogers [1]. The valuations are obtained by the perfect shuffle of two arithmetic progressions of step 1:

If $n=4p+1$:

$3p+1, p+1, 3p+2, p+2, \dots, p-1, 3p, p$

If $n=4p+2$:

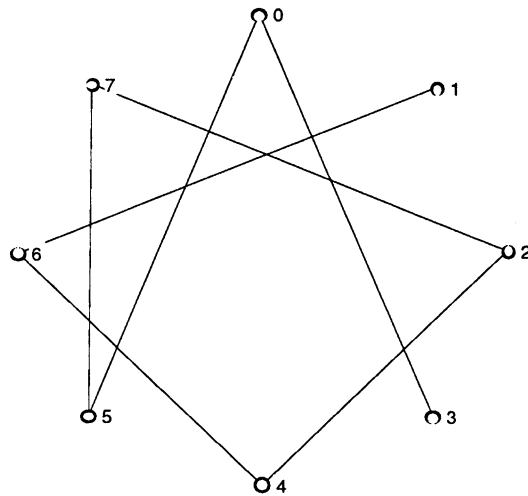
$p+1, 3p+2, p+2, 3p+3, \dots, 3p+1, p$

If $n=4p+3$:

$p+1, 3p+3, p+2, 3p+4, \dots, 3p+1, p, 3p+2$

The remaining case $n=4p$ has been solved by I. Cahit [8]. It needs a more complicated valuation. We will now give an other elegant valuation of P_{4p} , the construction of which is simpler and more geometric than the one given by I.Cahit.

First notice that P_4 is not elegant and an elegant valuation of P_8 is given in the following figure.



An elegant valuation of P_8 .

Assume now $n=4p$ ($n \geq 3$).

If **p is odd**, consider the following valuation of the vertices of P_{4p} :

1,

$2p+1, 2p+3, \dots, 3p-2, 3p,$

$3p+3, 3p+5, \dots, 4p-2, 0,$

$2p, 4p-1, 2p-2, 4p-3, \dots, 3p+4, p+3, 3p+2, p+1,$

$3p+1, p, 3p-1, p-2, \dots, 5, 2p+4, 3, 2p+2,$

$2, 4, \dots, p-3, p-1,$

$p+2, p+4, \dots, 2p-3, 2p-1.$

It is easy to check that these values are in $\{0, \dots, 4p-1\}$ and are all distinct; the values on the edges are also all distinct in $\{1, \dots, 4p-1\}$ and therefore we have an elegant valuation of P_{4p} with p odd.

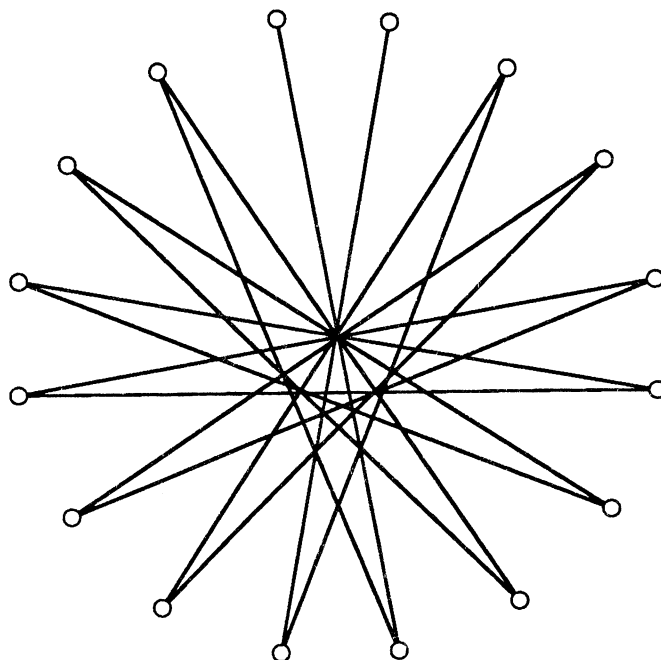
If p is even, consider the following valuation of the vertices of P_{4p} :

1,
 $2p+1, 2p+3, \dots, 3p-3, 3p-1,$
 $3p+2, 3p+4, \dots, 4p-2, 0,$
 $2p, 4p-1, 2p-2, 4p-3, \dots, p+4, 3p+3, p+2, 3p+1$
 $p+1, 3p, p-1, 3p-2, p-3, \dots, 5, 2p+4, 3, 2p+2,$
 $2, 4, \dots, p-2, p,$
 $p+3, p+5, \dots, 2p-3, 2p-1.$

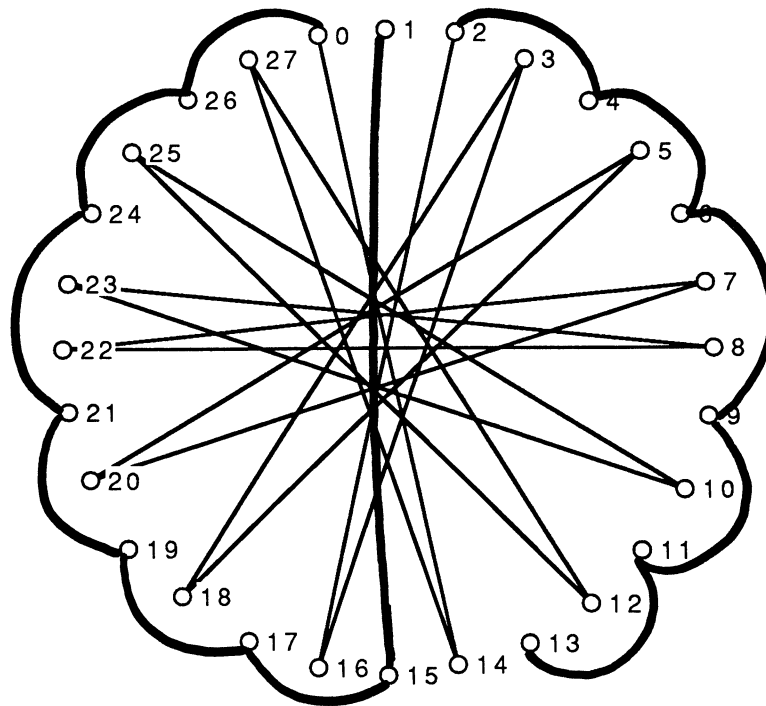
The induced values on the edges shows that we also have an elegant valuation of P_{4p} .

In the two cases the given valuation is obtained by a common geometrical construction. On a regular polygon with vertices labelled $0, 1, \dots, n-1$, edges are parallel if and only if the sum of the valuations of their ends are equal.

Consider the following path on $2p+1$ vertices.



Insert now the $2p-1$ remaining vertices joined by two disjoint paths as follows.



We obtain now a path on the $4p$ vertices such that edges are neither mutually 'parallel' nor parallel to the 'direction' 0 (i.e. $1, n-1$).

REFERENCES

- [1] C.J. Chang, D.F. Hsu and D.G. Rogers, Additive variations on graceful theme, *Congressus Numerantium*, Vol 32 (1981) 181-197.
- [2] A. Hartman, Partial triple systems and edge colourings, *Discrete Mathematics* 62 (1986) 183-196.
- [3] J.C.Bermond, Graceful graphs, radio antennae, and French windmills, in *Graph Theory and Combinatorics*, R. Wilson, ed., Pitman, London (1979) 18-37.
- [4] G.S.Bloom, A chronology of the Ringel-Kotzig conjecture and the continuing quest to call trees graceful, in *Topics in Graph Theory*, Annals of the New York Academy of Sciences, 328, F.Harary, ed., New York Academy of Sciences, New York (1979) 32-51.
- [5] S.W.Golomb, How to number a graph, in *Graph Theory and Computing*, R.C.Reed, ed., Academic press, New York (1972) 23-37.
- [6] A. Rosa, On certain valuations of the vertices of a graph, in *Theory of graphs*, P. Rosenstiehl, ed. Dunod, Paris (1967) 349-355.
- [7] R.L. Graham and N.J.A. Sloane, On additive bases and harmonious graphs, *SIAM J Alg. Disc. Meth.*, Vol 1 n°4 (1980) 382-404.
- [8] I.Cahit, Elegant valuation of the paths, *ARS COMBINATORIA*, vol 16 (1983) 223-227.

AUTORISATION DE SOUTENANCE

DOCTORAT D'ETAT

Vu les dispositions de l'Article 5 de l'Arrêté du 16 avril 1974,

Vu les rapports de M. J. M. Labrosse.....

M. J. Havel.....

M. H. M. Mulder.....

D. Solteau

M. Michel..... Mollard..... est autorisé à
présenter une thèse en vue de l'obtention du grade de DOCTEUR D'ETAT
ES SCIENCES.

Fait à Grenoble, le 27-6-89

Le Président de l'U.J.F.



Le Président,

A. NEMOZ

RESUME

Que ce soit dû à un regain actuel d'utilisation pratique (réseaux, architectures parallèles, codage), à son utilisation pour modéliser des problèmes ou simplement à l'intérêt de sa structure, l'hypercube, et plus généralement les graphes de Hamming (produits cartésiens de graphes complets) sont un objet d'étude particulièrement intéressant en combinatoire. Au fil des années l'essentiel de mon travail de recherche a concerné ces graphes et le sujet de cette thèse en est le reflet.

L'objet du premier chapitre est l'étude des caractérisations de ces graphes et d'autres graphes associés.

Dans les deux chapitres suivants on s'intéresse à la recherche d'ensemble de sommets de l'hypercube ayant certaines propriétés. Dans le chapitre 2 il s'agit de la construction de codes correcteurs d'erreurs parfaits, alors que dans le chapitre 3 on étudie des propriétés habituelles en théorie des graphes: absorbants, cycles hamiltoniens, etc..

Dans un dernier chapitre on introduit une formulation générale aux divers notions généralisant la notion de graphes gracieux. Dans ce cadre on résout plusieurs conjectures.

MOTS_CLES

hypercube, graphes de Hamming, cycles hamiltoniens, codes correcteurs d'erreurs, codes de Gray, valuations gracieuses.