Advances in Pure Mathematics, 2014, 4, 368-372
Published Online August 2014 in SciRes. http://www.scirp.org/journal/apm
http://dx.doi.org/10.4236/apm.2014.48047

Scientific Research

Boolean Automorphisms of a Hypercube Coincide with the Linear Isometries

Eberto R. Morgado[1], Marco V. José[2]

[1]Facultad de Matemática, Física y Computación, Universidad Central "Marta Abreu" de Las Villas, Santa Clara, Cuba
[2]Theoretical Biology Group, Instituto de Investigaciones Biomédicas, Universidad Nacional Autónoma de México, México D.F., México
Email: morgado@uclv.edu.cu, marcojose@biomedicas.unam.mx

Received 10 June 2014; revised 10 July 2014; accepted 23 July 2014

Abstract

Boolean homomorphisms of a hypercube, which correspond to the morphisms in the category of finite Boolean algebras, coincide with the linear isometries of the category of finite binary metric vector spaces.

Keywords

Boolean Automorphisms, Boolean Algebra, Hypercube, Linear Isometries

1. Introduction

An automorphism is an isomorphism from a mathematical object to itself. It is, in some sense, symmetry of the object, and a way of mapping the object to itself while preserving all of its structure. The set of all automorphisms of an object forms a group, called the automorphism group. It is, loosely speaking, the symmetry group of the object.

As is well known, a Boolean lattice is a partially ordered set with some special properties of its partial order relation, and it can also be envisaged as an algebraic system with two algebraic binary operations. This algebraic system is the so-called Boolean algebra, associated to the Boolean lattice. The Boolean algebra can also be provided with a ring structure, the so-called Boolean ring, associated to the Boolean lattice. It can even be regarded as a binary vector space, that is, a vector space over the binary field $\mathbb{Z}_2 = \{0,1\}$ of two elements [1]. These four categories are functorial related by isofunctors that carry over the morphisms of one category over morphisms of the other [2]. The Boolean lattice is also a metric space with the so-called Hamming distance, where the morphisms are the so-called isometries.

How to cite this paper: Morgado, E.R. and José, M.V. (2014) Boolean Automorphisms of a Hypercube Coincide with the Linear Isometries. *Advances in Pure Mathematics*, **4**, 368-372. http://dx.doi.org/10.4236/apm.2014.48047

The aim of the present work is to show that the Boolean homomorphisms, that is, the morphisms in the category of the finite Boolean algebras, are the same to the linear isometries in the category of finite binary vector spaces when the Hamming distance is used.

2. Some Previous Definitions and Concepts

2.1. Definition

Given a Boolean algebra $(B,\vee,\wedge)$ a function $f:B\to B$ such that $f(x\vee y)=f(x)\vee f(y)$, $f(x\wedge y)=f(x)\wedge f(y)$ for all *x*, *y* of *B*, and $f(0)=0$, $f(1)=1$, where 0 and 1 denote the neutral elements of $\vee,\wedge$, respectively, is called a Boolean endomorphism. If *f* is bijective, it is called a Boolean automorphism.

It is immediate that, for the Boolean addition +, defined as $x+y=(x\vee y)\wedge(x'\vee y')$, which provides to *B* a structure of Abelian group, *f* is a group endomorphism, or a group authomorphism if it is bijective.

It is well known that the triple $(B,+,\bullet)$ where $\bullet$ denotes the obviously defined external operation of the binary field $\mathbb{Z}_2=\{0,1\}$ over *B*, is a $\mathbb{Z}_2$-vector space.

It is not difficult to prove that every group endomorphism of the Abelian group $(B,+)$ is also a linear endomorphism of the vector space $(B,+,\bullet)$.

The triplet $(B,+,\wedge)$ is a unitary commutative ring, such that every element x is idempotent, that is, $x\wedge x=x$.

It is easy to notice that every Boolean endomorphism is also a unitary ring endomorphism, and conversely, every unitary ring endomorphism is a Boolean endomorphism.

It is also well known that, the binary relation $\le$, defined as $x\le y\Leftrightarrow x\wedge y=x$, is a partial order relation with minimum and maximum 0 and 1, respectively.

The ordered pair $(B,\le)$ defines a lattice, such that for every binary subset $\{x,y\}$ the elements $x\vee y$ and $x\wedge y$ are, respectively, the least upper bound (supremum) and the greatest lower bound (infimum) of the set $\{x,y\}$.

A function $f:B\to B$ is a Boolean endomorphism if, and only if, it is isotonic with respect to the partial order relation $\le$, that is, if $x\le y\Rightarrow f(x)\le f(y)$ for all *x*, *y* of *B*.

If the vector space $(B,+,\bullet)$ has a finite basis of *n* elements, we will say that the Boolean algebra $(B,\vee,\wedge)$ is finite-dimensional, being the number *n* its dimension.

It can be proved that every *n*-dimensional Boolean algebra is isomorphic to the Boolean algebra $((\mathbb{Z}_2)^n,\vee,\wedge)$, where the operations are bitwise induced by the logic operations of disjunction and conjunction, according to the following **Table 1**.

The elements 0 and 1 represent, respectively, falsity or veracity of a proposition. The Boolean algebra $((\mathbb{Z}_2)^n,\vee,\wedge)$ is generally called the *n*-dimensional hypercube. It is due to the fact that in the case $n=3$, the triplets of zeros and ones are the algebraic representations of the vertexes of a cube, inserted, as a subset, in the 3-dimensional $\mathbb{R}$-vector space $\mathbb{R}$, being $\mathbb{R}$ the field of real numbers.

2.2. The Inner Product in the Hypercube $((\mathbb{Z}_2)^n,\vee,\wedge)$

2.2.1. Definition

For two *n*-tuples $u=(x_1,x_2,\cdots,x_n)$ and $v=(y_1,y_2,\cdots,y_n)$ of $(\mathbb{Z}_2)^n$ we call scalar product or inner product of *u* with *v* the number $\langle u,v\rangle=x_1y_2+x_2y_2+\cdots x_ny_n$, where the addition and the multiplication are the ordinary operations in the ring $\mathbb{Z}$ of integers.

This inner product is the restriction to the set $(\mathbb{Z}_2)^n$ of the ordinary inner product of the Euclidean *n*-dimensional $\mathbb{R}$-vector space $\mathbb{R}^n$.

Table 1. Logic operations in Boolean algebra.

$\vee$	0	1	$\wedge$	0	1
0	0	1	0	0	0
1	1	1	1	0	1

If the column matrices $\boldsymbol{X}=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ and $\boldsymbol{Y}=\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$ are the matrix representation of the *n*-tuples *u* and *v*, respectively, the inner product $\langle u,v\rangle$ can be expressed as the matrix product ${}^{t}\boldsymbol{XY}$, where ${}^{t}\boldsymbol{X}$ denotes the transpose matrix of ***X***, that is, the row matrix $(x_1,x_2,\cdots,x_n)$.

2.2.2. Definition

For a vector $u=(x_1,x_2,\cdots,x_n)$ we call the norm, absolute value, or weight of *u*, the inner product $\langle u,u\rangle = x_1x_1+x_2x_2+\cdots+x_nx_n$ of *u* with itself, denoted as $|u|$. Obviously, the norm $|u|$ is equal to the number of times the number 1 is a component of *u*.

It is not difficult to notice that the inner product $\langle u,v\rangle$ of the vector *u* and *v*, is equal to the norm of the vector product $u\wedge v$ in the Boolean ring $\left((\mathbb{Z}_2)^n,+,\wedge\right)$.

A vector *u* of norm $|u|=1$ is called unitary vector. The only unitary vectors are $e_1=(1,0,\cdots,0), e_2=(0,1,\cdots,),\cdots,e_i=(0,0,\cdots,1,\cdots,0),\cdots,e_n=(0,0,\cdots,n)$ and they conform the so-called canonical basis $(e_1,e_2,\cdots,e_n)$ of the binary vector space $\left((\mathbb{Z}_2)^n,+,\bullet\right)$.

3. The Concept of Orthogonality

Definition

We say that two vectors *u* and *v* are orthogonal or perpendicular if the inner product $\langle u,v\rangle$ is equal to 0.

4. The Hamming Distance in the Hypercube

Definition

For two vectors *u* and *v*, we define the Hamming distance between them, as the norm $|u+v|$ of their Boolean addition. Obviously, it is equal to the number of places where the components of both vectors are different.

5. Linear Isometries of the Hypercube

Definition

A function $f:(\mathbb{Z}_2)^n\to(\mathbb{Z}_2)^n$ is called an isometry if it preserves the distance between points, that is, if $|u+v|=|f(u)+f(v)|$ for all u,v of the set.

If the isometry *f* is also a linear transformation, then, the matrix ***A*** of *f*, with respect to the canonical basis $(e_1,e_2,\cdots,e_n)$ is an orthogonal matrix, that is, such that ${}^{t}\boldsymbol{AA}=\boldsymbol{I}_n$, the identity $n\times n$ matrix.

It is clear that a linear isometry also preserves the absolute value of any vector and the inner product of any two vectors.

The hypercube $\left((\mathbb{Z}_2)^n,+,\bullet\right)$ can also be envisaged as a graph, where the vertexes or nodes are the *n*-tuplesand the edges are the binary subsets $\{u,v\}$ such that the distance $|u+v|$ is equal to 1. Two vectors *u* and *v* of an edge $\{u,v\}$, that is, such that $|u+v|=1$, are called adjacent points of the hypercube.

It can be proved that the Hamming distance between two points *u* and *v* is equal to the minimal length of a path between them, that is, the minimal number of edges for going from one to the other.

6. Main Results

6.1. Lemma

In the hypercube $(\mathbb{Z}_2)^n, n\geq 2,$ the only set of *n* non-null vectors, which are pairwise orthogonal, is the set $\{e_1,e_2,\cdots,e_n\}$ of the unitary canonical vectors.

Proof: (Induction over *n*)

For *n* = 2 the assertion is trivially true.

Let us suppose that it is true for every $t < n$, , being $n > 2$.

Let $\{a_1, a_2, \cdots, a_n\}$ be a set of non-null and pairwise orthogonal vectors in the hypercube $(\mathbb{Z}_2)^n$. To prove that they are all unitary vectors let us suppose that one of them, say a_1 is not unitary, that is of norm $|a_1| = k > 1$. Then, the vectors $a_2, \cdots, a_n$ belong to the $(n-k)$-dimensional vector subspace, which is the supplementary orthogonal vector subspace of the line $\{0, a_1\}$. As the vectors $a_2, \cdots, a_n$ are linearly independent, then $n-1 = n-k$, then $k = 1$ in contradiction with the assumption $k > 1$. Hence, all the vectors of the set are unitary, as we wanted to show.

Now, we are in conditions to carry out the proof of the following.

6.2. Theorem

A function *f* is a Boolean automorphism if, and only if, it is a linear isometry.

Proof: If *f* is a Boolean automorphism it means that $f(u \vee v) = f(u) \vee f(v)$, $f(u \wedge v) = f(u) \wedge f(v)$ for all *u*, *v* of $(\mathbb{Z}_2)^n$, and $f(0) = 0,\ f(1) = 1$.

Then, $f(u+v) = f(u) + f(v)$ for the Boolean addition + such that, $x + y = (x \vee y) \wedge (x' \vee y')$. Hence, *f* is a linear transformation of the vector space.

For canonical vectors e_i, e_j we have that $\langle e_i e_j \rangle = 0$ if $i \neq j$, and $\langle e_i e_j \rangle = e_i$ if $i = j$, which means that they are unitary and pairwise orthogonal. From this, we have that $f(e_i) \wedge f(e_j) = f(e_i \wedge e_j) = 0$ if $i \neq j$ and $f(e_i) \wedge f(e_j) = f(e_i)$ if $i = j$. Then, the vectors $f(e_1), f(e_2), \cdots, f(e_n)$ are pairwise orthogonal and, from the lemma, they are unitary vectors. Hence, the linear function *f* is a permutation of the canonical basis $(e_1, e_2, \cdots, e_n)$. Then, the matrix $\boldsymbol{A}$ of *f*, with respect to this basis, is orthogonal, that is, such that ${}^{\mathrm{t}}\boldsymbol{A}\boldsymbol{A} = \boldsymbol{I}_{\mathrm{n}}$. Then, *f* is a linear isometry of the space, as we wanted to prove.

Conversely, if *f* is a Boolean isometry, $f(e_i) \wedge f(e_j) = f(e_i \wedge e_j)$ for all *i* and *j*, then for

$u = (x_1, x_2, \cdots, x_n)$ and $v = (y_1, y_2, \cdots, y_n)$, $f(u) = \sum_{i=1}^{n} x_i f(e_i)$, $f(v) = \sum_{j=1}^{n} y_j f(e_j)$.

Then, $f(u) \wedge f(v) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j f(e_i) \wedge f(e_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j f(e_i \wedge e_j) = f\left(\sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j (e_i \wedge e_j)\right) = f(u \wedge v)$.

On the other hand, it is known that $u \vee v = u + v + (u \wedge v)$ for all *u* and *v*. Then,

$$f(u \vee v) = f(u) + f(v) + f(u) \wedge f(v) = f(u) \vee f(v).$$

Then, we have proved that $f(u \vee v) = f(u) \vee f(v)$, $f(u \wedge v) = f(u) \wedge f(v)$ for all *u*, *v* elements of the space.

As *f* is linear we have $f(0) = 0$ and as for every *u*, $u \vee u' = 1$, we obtain that $f(1) = f(u) \vee f(u) = 1$.

Then, we have proved that *f* is a Boolean homomorphism.

7. Concluding Remarks

In this work we have demonstrated that Boolean automorphisms of a hypercube are the same to the linear isometries of finite binary metric spaces taking as a metric the Hamming distance. This fundamental result becomes of much interest when characterizing the symmetry groups of polytopes [3]. The use of the theory of categories imparts novel insights for understanding and generalizing the symmetries of any object. This result is of interest in many areas of research. For example, the representation of the Universal Genetic Code as a 6-dimensional hypercube [4] [5] has permitted to study its evolution by a series of successive symmetry breakings [6].

Acknowledgements

MVJ was financially supported by PAPIIT-IN107112, UNAM, México.

References

[1] Dubreil, P. and Jacotin, M.L. (1961) Lecciones de Algebra Moderna. Editorial Dunod, Francia.

[2] Mitchell, B. (1965) Theory of Categories. Academic Press, New York.

[3] Coxeter, H.S.M. (1973) Regular Polytopes. 3rd Edition. Dover Publication Inc., New York.

[4] José, M.V., Morgado, E.R. and Govezensky, T. (2007) An Extended RNA Code and Its Relationship to the Standard Genetic Code: An Algebraic and Geometrical Approach. *Bulletin of Mathematical Biology*, **69**, 215-243. http://dx.doi.org/10.1007/s11538-006-9119-3

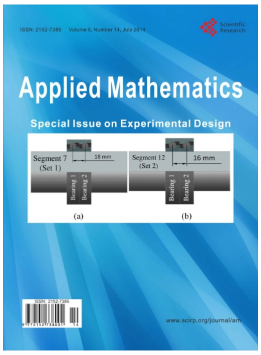
[5] José, M.V., Morgado, E.R., Sánchez, R. and Govesenky, T. (2012) The 24 Possible Algebraic Representations of the Standard Genetic Code in Six or in Three Dimensions. *Advanced Studies in Biology*, **4**, 119-152.

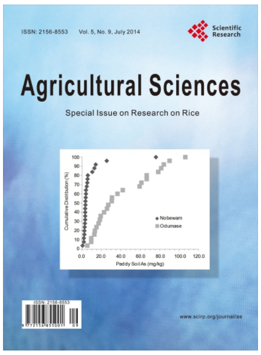
[6] José, M.V., Govesenky, T., García, J.A. and Bobadilla, J.R. (2009) On the Evolution of the Standard Genetic Code: Vestiges of Critical Scale Invariance from the RNA World to Current Prokaryote Genomes. *PLoS ONE*, **4**, e4340. http://dx.doi.org/10.1371/journal.pone.0004340

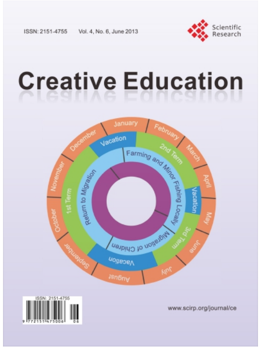
Advances in Bioscience and Biotechnology

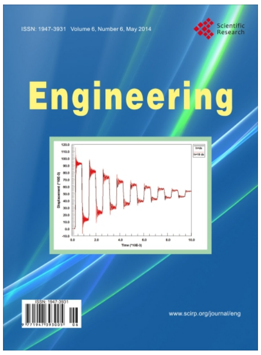
American Journal of Analytical Chemistry

American Journal of Plant Sciences
Special Issue on Photosynthesis

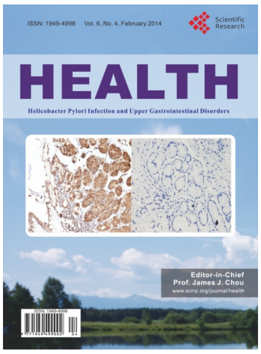

Applied Mathematics
Special Issue on Experimental Design


Agricultural Sciences
Special Issue on Research on Rice


Creative Education

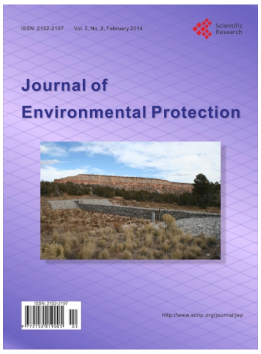

Engineering

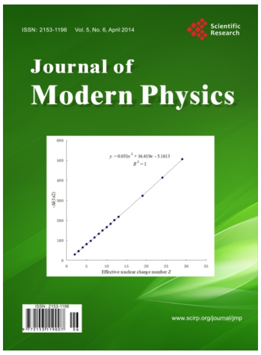
Food and Nutrition Sciences


HEALTH
Helicobacter Pylori Infection and Upper Gastrointestinal Disorders
Editor-in-Chief
Prof. James J. Chou

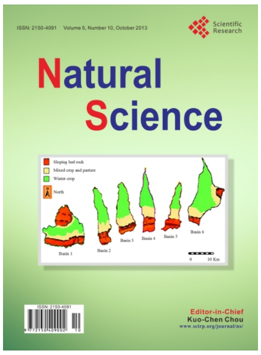
Journal of Computer and Communications

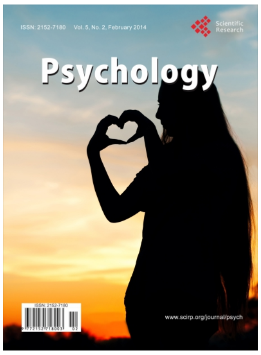
Journal of Cancer Therapy
Special Issue on Bone Tumor Research


Journal of Environmental Protection


Journal of Modern Physics

Modern Economy


Natural Science
Editor-in-Chief
Kuo-Chen Chou


Psychology