Acta Univ. Sapientiae, Mathematica, **4**, 2 (2012) 109–116

Metric on the hyper-octahedral group: the minimal deviation

János Gonda
Eötvös Loránd University
Department of Computer Algebra
Budapest, Hungary
email: andog@inf.elte.hu

Abstract. The n-dimensional hyper-octahedral group is the group of the distance-preserving transformations of the n-dimensional cube. This group, denoted by T_n, is the semi-direct product of S_2^n and S_n, where for any positive integer k, S_k is the symmetric group of degree k. On this group a metric can be defined in the following way. Let us consider the set of the distances between the images under the two transformations of every vertex of the hypercube. Then the distance between the two transformations is the maximum of this set. If we consider the vertices of the cube as the points of the n-dimensional Boolean space, that is, if we represent the vertices of the n-dimensional cube by the elements of the set of $\{0,1\}^n$, then a particular element of T_n can be given in the form of $(\pi, \underline{\alpha})$, where $\underline{\alpha} \in \{0,1\}^n$, and π is a permutation of the set of $\{k \in \mathbf{N} \,|\, k < n\}$ ($\mathbf{N}$ denotes the set of the non-negative integers, and the elements of $\{0,1\}^n$ are indexed from 0). By this representation the metric defined on T_n can be determined by an inner manner, that is, the distance of two transformations is determined by $\underline{\alpha}$ and the decomposition of π into disjoint cycles (see for instance in [2]).

This metric involves a norm on the group, the norm of a transformation being its distance from the identity of the group. This norm is a maximum, being the maximum of the set of distances between a vertex and its transformed image, for every vertex of the hypercube. However, sometimes the minimum of these distances can be interesting. In this paper we deal with this value.

2010 Mathematics Subject Classification: 11A25, 06E30, 94C10, 15A18
Key words and phrases: hyperoctahedral group, metric, norm, deviance, Boolean space

1 Introduction

Let B_n denote the set of the n-dimensional Boolean vectors. B_n is a metric space with the Hamming-distance, that is, with $d(\underline{x},\underline{y}) = \sum_{i=0}^{n-1}(x_i \oplus y_i)$ [1] where $\underline{x} \in B_n$, $\underline{y} \in B_n$, x_i and y_i are the i-th coordinates of $\underline{x}$ and $\underline{y}$, respectively, and $\oplus$ denotes the $\mathtt{modulo}\ 2$ sum. B_n is a representation of the abstract notion of the n-dimensional cube. The cardinality of B_n is equal to 2^n, this being the number of the vertices of an n-dimensional cube. Two vertices of the n-dimensional cube are neighbouring if and only if they are connected by an edge of the cube. We can define a similar relation, the relation of neighbourhood, between the elements of the n-dimensional Boolean vectors as follows. Let two Boolean vectors be neighbouring if and only if they differ from each other in exactly one component, that is, if and only if the Hamming-distance of the two Boolean vectors is 1. A vertex of an n-dimensional cube has n neighbouring vertices, and this is the number of the Boolean vectors having a Hamming-distance of 1 from a fixed Boolean vector. If we define the distance of two vertices of an n-dimensional cube as the minimum number of edges we have to pass from one to the other, then it is easy to see that this rule defines a distance function. There are $2^n n!$ distance-preserving bijections between the the vertices of the n-dimensional cube and the vectors of the n-dimensional Boolean space. Indeed, let us fix an arbitrary vertex of the n-dimensional cube, denoted by ν_0. We have 2^n different choices for a corresponding Boolean vector. Every Boolean vector has n neighbouring vectors in the same way as every vertex of the cube has n neighbouring vertices. There are altogether $n!$ one to one mappings between these two sets of n elements, so we have a total of $2^n n!$ different bijections between $n+1$ elements of the corresponding sets. Till now we have given the image of an arbitrarily chosen vertex, together with its neighbours. Let us denote this mapping by φ and let A be the set of these $n+1$ vertices. Then it can be proved that there is exactly one extension ψ of φ such that $d(\psi(\nu'), \varphi(\nu)) = \widetilde{d}(\nu', \nu)$ for all pairs of vertices ν' of the cube and $\nu \in A$ (see for instance [1]).

From the previously mentioned facts follows that we can study the effects of the n-dimensional hyper-octahedral group on B_n. Let T_n denote the group of the congruences of the n-dimensional cube acting on B_n. In this case $T_n = \{(\pi, \underline{\alpha}) \,|\, \pi \in S_n \text{ and } \underline{\alpha} \in \{0,1\}^n\}$, where S_n is the symmetric group of degree n acting on the set of the non-negative integers less than n. If $\underline{x} = (x_0, \ldots x_{n-1}) \in B_n$, $u = (\pi, \underline{\alpha}) \in T_n$ and $\underline{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$, then $\underline{x}^u = \left(x_{\pi(0)}^{\alpha_0}, \ldots, x_{\pi(n-1)}^{\alpha_{n-1}}\right)$ so that $x^\alpha = \alpha \oplus x$. Among all transformations on B_n, only the elements of T_n

preserve the distances between the elements of B_n, so this group is the isometric group of B_n. T_n is the wreath product of S_2 and S_n, that is, $T_n = S_2 \wr S_n$, where S_n is the symmetric group of degree n [5], [6], [7], [8].

In [2] we have dealt with an inner characterization of the metric and the norm of the hyper-octahedral group. In the following we shortly summarize the results of that article, and then, in the next section, we deal with the minimal value of the effect of a transformation of the hyper-octahedral group.

Definition 1 *Let* $n \in \mathbf{N}$, $u \in T_n$, $v \in T_n$. *Then* $\overline{d}(u,v) = \max\limits_{\underline{x} \in B_n} \{d(\underline{x}^u, \underline{x}^v)\}$.

$\overline{d}$ defines a metric on T_n (see for instance in [9]).

$\overline{d}$ is left and right invariant on T_n, that is, for any $u \in T_n$, $v \in T_n$ and $w \in T_n$,

$$\overline{d}(uw, vw) = \overline{d}(u,v) \tag{1}$$

and

$$\overline{d}(wu, wv) = \overline{d}(u,v). \tag{2}$$

$\overline{d}$ can be determined in an inner manner. Let $w = (\pi, \underline{\alpha}) \in T_n$ be an arbitrary element, let

$$\pi = \prod_{t=0}^{s-1} c_t \tag{3}$$

be the disjoint cycle decomposition of the permutation π. Further, let $c_k = \left(c_{k_0}, \ldots, c_{k_{m_k-1}}\right)$ be the k-th member of the product in (3), where $0 \le k < s$, m_k is the length of the k-th cycle of the previous product for $0 \le k < s$, and $\underline{\alpha} = (\alpha_0, \ldots, \alpha_{n-1}) \in \{0,1\}^n$, furthermore let $t_k = \left(m_k + \sum_{i=0}^{m_k-1} \alpha_{c_{k_i}}\right) \bmod 2$ and $\tau(w) = \sum_{k=0}^{s-1} t_k$.

Theorem 1 *Let* u *and* v *be two arbitrary elements from* T_n. *Then* $\overline{d}(u,v) = n - \tau\left(uv^{-1}\right)$.

Using the metric studied above, one can define the norm of the elements of T_n [2].

Definition 2 *Let* T_n *be the isometric group of the* n*-dimensional Boolean space. Then* $\|u\| = \overline{d}(e,u)$ *is the norm of* $u \in T_n$.

From this definition immediately follows that

1. $\|u\| = 0$ if and only if $u = e$;

2. $\|u\| = \left\|u^{-1}\right\|$ for every $u \in T_n$;
3. $\overline{d}(u,v) = \left\|uv^{-1}\right\|$ for every $(u,v) \in T_n^2$.

Theorem 2 *Let* $\varphi : u \mapsto \|u\|$. *Then* $\mathrm{Im}(\varphi) = \mathbf{N}_n = \{k \in \mathbf{N} \,|\, k < n\}$.

In Theorem 2 $\mathbf{N}$ denotes the set of the non-negative integers.

2 New results

In the previous section we characterized an element of the hyper-octahedral group by its maximal effect regarded as the distance between a vector of the Boolean space and its transformed image. But sometimes the expectation is the opposite, that is, we wish that the effect of the transformation be as little as possible. This expectation leads to the following notion.

Definition 3 *Let* T_n *be the isometric group of the* n*-dimensional Boolean space and let* $u \in T_n$. *Then* $\langle\langle u \rangle\rangle = \min\limits_{\underline{x} \in B_n} \{d(\underline{x}, \underline{x}^u)\}$.

$\langle\langle u \rangle\rangle$ shows the minimal effect of $u \in T_n$. By the definition it seems, that $\langle\langle u \rangle\rangle$ depends not only on u, but on the elements of the Boolean space. However, the next statement proves that $\langle\langle u \rangle\rangle$ can be given in a form depending only on u.

Theorem 3 *Let* $u = (\pi, \underline{\alpha}) \in T_n$, *where* $\pi \in S_n$ *and* $\underline{\alpha} \in \{0,1\}^n$. *If* $\pi = \prod_{t=0}^{s-1} c_t$ *is the disjoint cycle decomposition of the permutation* π, *for* $0 \le k < s$ $c_k = \left(c_{k_0}, \ldots, c_{k_{m_k-1}}\right)$ *is the* k*-th member of the previous product, then*

$$\langle\langle u \rangle\rangle = \sum_{k=0}^{s-1} t_k', \tag{4}$$

where t_k' *denotes the remainder of* $\sum_{i=0}^{m_k-1} \alpha_{c_{k_i}}$ *by* modulo 2.

Before the precise verification of the theorem we would like to highlight the idea of the proof.

For the sake of the simplicity let us suppose that π in $u = (\pi, \alpha) \in T_n$ is a cycle, for instance the cycle of the first k elements of the indices, that is, $\pi = (0, 1, \ldots, k-1)$, where $n > k \in \mathbf{N}$, and for $n > i \ge k, i \in \mathbf{N}$, $\alpha_i = 0$. In this case for an arbitrary element $\underline{x}$ of B_n,

$$\begin{pmatrix} \underline{x} \\ \underline{x}^u \end{pmatrix} = \begin{pmatrix} x_0 & x_1 & \ldots & x_{k-2} & x_{k-1} & x_k & \ldots & x_{n-1} \\ x_1^{\alpha_0} & x_2^{\alpha_1} & & x_{k-1}^{\alpha_{k-2}} & x_0^{\alpha_{k-1}} & x_k & \ldots & x_{n-1} \end{pmatrix}.$$

Now the number of the positions where the original and the transformed vectors differ from each other can be calculated as follows. If $n > i \geq k, i \in \mathbf{N}$, then $x_i = x_{\pi(i)}^{\alpha_i} = (\underline{x}^u)_i$, so in that part of the vector there is no position where the two vectors differ, the number of the different positions of that domain is equal to 0. Now let us consider the first part of the vectors, that is, the first k positions. We try to get as few different positions as possible. The best result is, if $x_i = x_{\pi(i)}^{\alpha_i} = x_{(i+1) \bmod k}^{\alpha_i}$ for every $k > i \in \mathbf{N}$. Then

$$\begin{array}{ccccccc}
x_0 & & & & & = & x_1^{\alpha_0} \\
x_0 & = & x_1^{\alpha_0} & = & \left(x_2^{\alpha_1}\right)^{\alpha_0} & = & x_2^{\alpha_1 \oplus \alpha_0} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
x_0 & = & x_{k-2}^{\alpha_{k-3} \oplus \cdots \oplus \alpha_0} & = & \left(x_{k-1}^{\alpha_{k-2}}\right)^{\alpha_{k-3} \oplus \cdots \oplus \alpha_0} & = & x_{k-1}^{\alpha_{k-2} \oplus \alpha_{k-3} \oplus \cdots \oplus \alpha_0}
\end{array}$$

and finally

$$x_0 = x_{k-1}^{\alpha_{k-2} \oplus \alpha_{k-3} \oplus \cdots \oplus \alpha_0} = \left(x_0^{\alpha_{k-1}}\right)^{\alpha_{k-2} \oplus \cdots \oplus \alpha_0} = x_0^{\alpha_{k-1} \oplus \alpha_{k-2} \oplus \cdots \oplus \alpha_0}$$

($\oplus$ denotes the modulo 2 sum).

All but the last conditions can be easily satisfied. As $a^b = a \oplus b$, so

$$\begin{aligned}
x_0 &= x_0^{\alpha_{k-1} \oplus \alpha_{k-2} \oplus \cdots \oplus \alpha_0} \\
&= x_0 \oplus \alpha_{k-1} \oplus \alpha_{k-2} \oplus \cdots \oplus \alpha_0.
\end{aligned}$$

This last equality is true if and only if $\alpha_{k-1} \oplus \alpha_{k-2} \oplus \cdots \oplus \alpha_0 = 0$, that is, if and only if $\alpha_{k-1} + \alpha_{k-2} + \cdots + \alpha_0$ is an even number. In this case the two vectors are identical, there is no differences, the distance of the two vectors is equal to 0. In the other case, that is, if the sum of the exponents is an odd number, then there is exactly one position where the two vectors differ, so, the distance of the two vectors, and then $\langle\langle u \rangle\rangle$ is equal to 1. That means that the minimal number of the differences, in another words, the minimal deviation caused by this transform is either 0 or 1, depending on the parity of the sum of the exponents.

Now we prove exactly the statement.

Proof. Let $x_{c_{k_1}} = x_{c_{k_0}}^{\alpha_{c_{k_0}}} = x_{c_{k_0}} \oplus \alpha_{c_{k_0}}$. Then

$$\begin{aligned}
(x^u)_{c_{k_0}} &= x_{\pi(c_{k_0})}^{\alpha_{c_{k_0}}} = x_{\pi(c_{k_0})} \oplus \alpha_{c_{k_0}} = x_{c_{k_1}} \oplus \alpha_{c_{k_0}} \\
&= \left(x_{c_{k_0}} \oplus \alpha_{c_{k_0}}\right) \oplus \alpha_{c_{k_0}} = x_{c_{k_0}}. \qquad (5)
\end{aligned}$$

For every $1 \leq i < m_k$ we have that

$$\begin{aligned} x_{c_{k_i}} &= x_{c_{k_{i-1}}}^{\alpha_{c_{k_{i-1}}}} = x_{c_{k_{i-1}}} \oplus \alpha_{c_{k_{i-1}}} \\ &= x_{c_{k_0}} \oplus \left(\bigoplus_{j=0}^{i-1} \alpha_{c_{k_j}} \right). \end{aligned} \tag{6}$$

Then we get that

$$x_{c_{k_{m_k-1}}} = x_{c_{k_0}} \oplus \left(\bigoplus_{j=0}^{m_k-2} \alpha_{c_{k_j}} \right). \tag{7}$$

The equality $(x^u)_{c_{k_{m_k-1}}} = x_{c_{k_{m_k-1}}}$ holds if and only if $x_{\pi\left(c_{k_{m_k-1}}\right)}^{\alpha_{c_{k_{m_k-1}}}} = x_{c_{k_{m_k-1}}}$, or, in another way, if and only if

$$x_{c_{k_0}} \oplus \alpha_{c_{k_{m_k-1}}} = x_{c_{k_{m_k-1}}} = x_{c_{k_0}} \oplus \left(\bigoplus_{j=0}^{m_k-2} \alpha_{c_{k_j}} \right). \tag{8}$$

From the equation above we get that

$$\bigoplus_{j=0}^{m_k-1} \alpha_{c_{k_j}} = 0. \tag{9}$$

If this condition is fulfilled then all of the components of $\underline{x}$ and $\underline{x}^u$ belonging to the k-th cycle of the decomposition of π are the same. In the opposite case they differ exactly in one position, and then

$$\bigoplus_{j=0}^{m_k-1} \alpha_{c_{k_j}} = 1. \tag{10}$$

These results mean that if we construct a vector $\underline{x}_0$ taking into consideration the above-mentioned conditions, then the number of the different coordinates of the vectors $\underline{x}_0$ and $\underline{x}_0^u$ is exactly $\sum_{k=0}^{s-1} \left(\oplus_{j=0}^{m_k-1} \alpha_{c_{k_j}} \right)$, and this is the minimal value of the Hamming-distances between the elements of the Boolean space and their transformed images under u, according to the statement of the theorem. □

The range of the values of the function $u \mapsto \langle\langle u \rangle\rangle$, where $u \in T_n$, is as follows.

Theorem 4 *The set of the values of the function* $u \mapsto \langle\langle u \rangle\rangle$, *defined on* T_n, *is equal to* $A = \{k \in \mathbf{N} \,|\, k \leq n\}$.

Proof. It is obvious that the set of the values of the function is a subset of the set of $A = \{k \in \mathbf{N} \,|\, k \leq n\}$. We have to show that for every element of that set there is at least one element in T_n so, that $\langle\langle u \rangle\rangle$ is equal to the given integer. Let us consider the following transformation:

$$u = \left(\varepsilon, \left(\underbrace{1, \ldots, 1}_{k}, \underbrace{0, \ldots, 0}_{n-k} \right) \right), \tag{11}$$

where ε is the identity of S_n. Then for any $\underline{x} = (x_0, \ldots, x_{n-1}) \in B_n$ we have that

$$\begin{aligned} \underline{x}^u &= (x_0, \ldots, x_{n-1})^u \\ &= (\overline{x}_0, \ldots, \overline{x}_{k-1}, x_k, \ldots, x_{n-1}) \,. \end{aligned} \tag{12}$$

As $d\left((x_0, \ldots, x_{k-1}, x_k, \ldots, x_{n-1}), (\overline{x}_0, \ldots, \overline{x}_{k-1}, x_k, \ldots, x_{n-1})\right) = k$, that is, $d(\underline{x}, \underline{x}^u) = k$ for every $\underline{x} \in B_n$, so $\langle\langle u \rangle\rangle = \min\limits_{\underline{x} \in B_n} \{d(\underline{x}, \underline{x}^u)\} = k$. □

3 Conclusion

Considering two Boolean functions of the same variables, they are not essentially different if they differ only in the ordering of the variables and in assigning the 0 and 1 to the variables that is in the case when $f_2(x_0, \ldots, x_{n-1}) = f_1\left(x_{\pi(0)}^{\alpha_0}, \ldots, x_{\pi(n-1)}^{\alpha_{n-1}}\right)$, where π is a permutation of the indices of the variables, $\alpha_i \in \{0, 1\}$ and $x^\alpha = \alpha \oplus x = \begin{cases} x & \text{, if } \alpha = 0 \\ \overline{x} & \text{, if } \alpha = 1 \end{cases}$. For instance, let us suppose that we want to describe the statement

"Now it is either raining or the sky is blue, and yesterday MU won again" by the help of mathematical formalism. Then we can denote the first part of the sentence by A (A = "it is raining"), the second part of the sentence by B (B = "the sky is blue") and the third part of it by C (C = "Yesterday MU won again"). By these notations our statement is $F = (A \vee B) \wedge C$, if $\vee$ denotes the disjunction and $\wedge$ denotes the conjunction. But the meaning of $B \wedge (\neg A \vee C)$ is the same as the meaning of the previous form, if now B denotes the sentence "yesterday MU won again", C denotes "the sky is blue" and A stands for "Now it is not raining". As this simple example shows, the two forms of $(A \vee B) \wedge B$ and $B \wedge (\neg A \vee C)$ do not differ essentially, they differ only in the assignment of the variables to the original statements.

This fact explains, why the hyper-octahedral group is so important when we investigate the Boolean functions. And if it is so, then it is understandable that it is important to know, what is the maximal and the minimal impact of an element of the group on the Boolean functions. In another article [2] we examined the maximal effect, and now the minimal effect of the transformations, and stated, that this effect depends only on the transformation given, and that every possible value can be achieved by a transformation chosen in an appropriate way.

References

[1] P. J. Cameron, J. H. van Lint, Designs, Graphs, Codes and their Links, *London Mathematical Society Student Texts 22*, Cambridge University Press, Cambridge, 1991.

[2] J. Gonda, Metrics on the hyper-octahedral group, In: *Informatika a felsőoktatásban 2008*, (http://www.agr.unideb.hu/if2008/kiadvany/papers/F11.pdf, in Hungarian).

[3] M. Hall jr., The theory of groups, MacMillan Co., New York, 1959.

[4] B. Huppert, Endliche Gruppen 1. Springer, Berlin, 1967.

[5] L. A. Kaluzhnin, P. M. Beleckij, V. Z. Feinberg, Kranzprodukte, *Teubner-Texte Vol. 101*, B. G. Tebner, Leipzig, 1987.

[6] L. A. Kaluzhnin, M. Kh. Klin, V. I. Sushchanskii, Exponentiation of permutation groups I. *Izv. Vyssch. Uchebn. Zaved. Mat.* **8** (1979) 26–33 (in Russian).

[7] M. Krasner M. L. Kaloujnine, Produit complet des groupes de permutations et problème d'extension de groupes I. *Acta Sci. Math. Szeged* **13** (1950) 208–230.

[8] M. Krasner M. L. Kaloujnine, Produit complet des groupes de permutations et problème d'extension de groupes II. *Acta Sci. Math. Szeged* **14** (1951) 39–66, 69–82.

[9] L. S. Pontrjagin, Nepreryvnye gruppy, Nauka, Moscow, 1984.

Received: July 14, 2011