Annales Univ. Sci. Budapest., Sect. Comp. 47 (2018) 285–292

ELEMENTS OF THE HYPEROCTAHEDRAL GROUP OF GIVEN NORM AND DEVIATION

János Gonda (Budapest, Hungary)

Communicated by Imre Kátai

(Received February 26, 2018; accepted May 8, 2018)

Abstract. The n-dimensional hyperoctahedral group, denoted by T_n, is the group of the distance-preserving transforms of the n-dimensional cube. In this group, a norm and a deviation of an element can be defined as the maximum and minimum of the distances of each vertex and its transformed one. In previous papers the author proved results on the computation of these values and characterized the image of the norm and deviation functions. In the present paper we deal with the following problem: which ordered pair (p, q) belongs to a transform u so that the norm and the deviation of u is equal to p and q, respectively.

1. Introduction

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 $f_2(x_0, \dots, x_{n-1}) = f_1\left(x_{\pi(0)}^{\alpha_0}, \dots, x_{\pi(n-1)}^{\alpha_{n-1}}\right)$ where π is a permutation of the indices of the variables, $\alpha_i \in \{0, 1\}$ and $x^\alpha = \alpha \oplus x = \begin{cases} x & \text{, if } \alpha = 0 \\ \overline{x} & \text{, if } \alpha = 1 \end{cases}$. This fact explains why the hyperoctahedral group is so important when we investigate Boolean functions. And if it is so, then it is understandable that it is important to know

Key words and phrases: Hyperoctahedral group, metrics, norm, deviation, Boolean space.
2010 Mathematics Subject Classification: 11A25, 06E30, 94C10, 15A18.
https://doi.org/10.71352/ac.47.285

what is the maximal and the minimal impact of an element of the group on the Boolean functions. In other articles, in [2] and [3] we examined the maximal and the minimal effects of the transforms, and stated that these effects depend only on the transform given, and that every possible value can be achieved as the norm and as the deviation by a transform choosen in an appropriate way. 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 $d\left(\underline{x},\underline{y}\right)=\sum_{i=0}^{n-1}\left(x_i\oplus y_i\right)$ [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 modulo 2 sum. B_n is a representation of the abstract notion of the n-dimensional cubes. Indeed, the cardinality of B_n is equal to 2^n and this is the number of the vertices of an n-dimensional cube, too. 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 of the number of the edges we have to pass for reaching one of the two vertices from the other vertex, then it is easy to see that this value is really a distance. Now there is a one-to-one mapping preserving the distances between the vertices of the n-dimensional cube and the corresponding vectors of the n-dimensional Boolean space – more precisely there are $2^n n!$ correspondences having the before-mentioned properties. Indeed, let's fix an arbitrary vertex of the n-dimensional cube, denoted by v_0. We can correspond to this vertex any of the 2^n Boolean vectors. These are 2^n possibilities. After fixing one of these vectors, v_0 and this vector have n neighbouring vertices and neighbouring vectors of the same number, respectively. There are altogether $n!$ one-to-one mappings between the two sets each of them consisting of n elements. This choice and the previous one give altogether $2^n n!$ different one-to-one correspondences between $n+1$ elements of the corresponding sets. So far we have given the image of an arbitrarily choosen vertex of the cube and the images of the vertices neighbouring to the previously mentioned vertex. Let's denote this mapping by φ and by A the set of these $n+1$ vertices. Then it can be proved that there is exactly one such extension ψ of φ that $d\left(\psi\left(v'\right),\varphi\left(v\right)\right)=\widetilde{d}\left(v',v\right)$ for all of the pairs of the vertices v' of the cube and $v\in A$ (see for instance in [1]). From the previously mentioned facts follows that we can study the effects of the n-dimensional hyperoctahedral 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 $T_n=\left\{(\pi,\underline{\alpha})\,|\pi\in S_n \text{ and } \underline{\alpha}\in\{0,1\}^n\right\}$, where S_n is the symmetrical group of degree n acting on the set of nonnegative integers less

than n. If $\underline{x} = (x_0, \dots x_{n-1}) \in B_n$, $u = (\pi, \underline{\alpha}) \in T_n$ and $\underline{\alpha} = (\alpha_0, \dots, \alpha_{n-1})$, then $\underline{x}^u = \left(x_{\pi(0)}^{\alpha_0}, \dots, x_{\pi(n-1)}^{\alpha_{n-1}}\right)$ so that $x^\alpha = \alpha \oplus x$. The elements of T_n and only these elements among all of the transforms of B_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 ([7], [8], [9], [10]). In [2] and [3] we dealt with an inner characterization of the metrics, the norm and the deviation of the hyperoctahedral group. In the following section we shortly summarize the results of those articles.

2. Basic definitions and prior results

Definition 2.1. 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 metrics on T_n (see for instance in [10]).

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

$$\overline{d}(uw, vw) = \overline{d}(u, v) \tag{2.1}$$

and

$$\overline{d}(wu, wv) = \overline{d}(u, v). \tag{2.2}$$

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

$$\pi = \prod_{t=0}^{s-1} c_t \tag{2.3}$$

be the disjoint cycle decomposition of the permutation π. Further, let $c_k = (c_{k_0}, \dots, c_{k_{m_k-1}})$ be the k-th member of the product in (2.3), 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 $\underline{\alpha} = (\alpha_0, \dots, \alpha_{n-1}) \in \{0,1\}^n$, furthermore let $t_k = \left(m_k + \sum_{i=0}^{m_k-1} \alpha_{c_{k_i}}\right) \bmod 2$ and $\tau(w) = \sum_{k=0}^{s-1} t_k$.

The following theorem can be seen in [2].

Theorem 2.1. *Let u and v be two arbitrary elements from T_n. Then* $\overline{d}(u,v) = n - \tau\left(uv^{-1}\right)$.

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

Definition 2.2. 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 the 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 2.2. *Let* $\varphi : u \mapsto \|u\|$. *Then* $\mathrm{Im}(\varphi) = \mathbf{N}_n = \{k \in \mathbf{N} \,|k < n\}$.

In Theorem 2.2 (see in [2]) $\mathbf{N}$ denotes the set of the non-negative integers.

In the previous part of this 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 [3].

Definition 2.3. 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 [3].

Theorem 2.3. *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*

$$\langle\langle u \rangle\rangle = \sum_{k=0}^{s-1} t_k^{'}, \tag{2.4}$$

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

We would like to highlight the idea of the proof.

For the sake of simplicity let us suppose that π in $u = (\pi, \underline{\alpha}) \in T_n$ 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 $n > i \geq k, i \in \mathbf{N}$, $\alpha_i = 0$. 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 $x_i = x_{\pi(i)}^{\alpha_i} = x_{(i+1) \mod k}^{\alpha_i}$ for every $k > i \in \mathbf{N}$. Then

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

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

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

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 are 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 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.

The range of the values of the function $u \mapsto \langle\langle u \rangle\rangle$, where $u \in T_n$, is as follows [3].

Theorem 2.4. *The set of the values of the function $u \mapsto \langle\langle u \rangle\rangle$, defined on T_n, is equal to $A = \{k \in \mathbf{N} \,|\, k \leq n\}$.*

3. Simultaneous characterization of norm and deviation

Let n be a non-negative integer and let $\mathbf{N}_n$ denote the non-negative integers less than n, that is, let $\mathbf{N}_n = \{k \in \mathbf{N} \mid k < n\}$. In [2] and [3] it was proved and in the previous section it was outlined that for every $p \in \mathbf{N}_{n+1}$ and $q \in \mathbf{N}_{n+1}$ there exist such $u \in T_n$ and $v \in T_n$, such elements in the n-dimensional hyperoctahedral group that the norm of u is equal to p and the deviation of v is equal to q. Clearly, the question arises whether there is any element in the group whose norm and deviation are equal to a pair of given values within the allowed range, or what conditions have to be fulfilled for a particular pair. The next statement will show us that the two elements of the pair cannot be independent from each other.

Theorem 3.1. *Let $n \in \mathbf{N}$, $n \geq p \in \mathbf{N}$ and $p \geq q \in \mathbf{N}$. Then for the pair of (p, q) there exists such $u \in T_n$ that $\|u\| = p$ and $\langle\langle u \rangle\rangle = q$ if and only if $p \equiv q \pmod 2$.*

Proof. 1. *Necessity*: let $u = [\pi, \underline{\alpha}]$ be an arbitrary distance-preserving mapping, let $\pi = \prod_{k=0}^{s-1} c_k$ be the decomposition of π into pairwise disjunct cycles, let $c_k = (c_{k_0}, \ldots, c_{k_{m_{k-1}}})$ and $\underline{\alpha} = (\alpha_0, \ldots, \alpha_{n-1}) \in \{0,1\}^n$. Then $p = n - \sum_{k=0}^{s-1} p_k$, $q = \sum_{k=0}^{s-1} p'_k$, where $p_k = (m_k + \sum_{i=0}^{m_{k-1}} \alpha_{c_{k_i}}) \mod 2$ and $p'_k = \sum_{i=0}^{m_{k-1}} \alpha_{c_{k_i}} \mod 2$. Let $t_{e,e}$ be the number of the cycles where both the length of the cycle, m_k and the magnitude of the cycle, p'_k are even, let $t_{e,o}$ be the number of the cycles of even length and odd magnitude, $t_{o,e}$ the number of the cycles of odd length and even magnitude, and finally, let $t_{o,o}$ be the number of the cycles of odd length and odd magnitude. Now $t_{e,o} + t_{o,o} = q$, $t_{e,o} + t_{o,e} = n - p$. But $t_{o,e} + t_{o,o} \equiv n \pmod 2$, so $t_{o,e} + t_{o,o} \equiv t_{o,e} + t_{o,o} + 2t_{e,o} = (t_{e,o} + t_{o,e}) + (t_{o,o} + t_{o,e}) \pmod 2$, thus $n \equiv q + (n - p) = n + (q - p) \pmod 2$, so $p \equiv q \pmod 2$.

2. *Sufficiency*: let $p \equiv q \pmod 2$ and $m = \min(q, n - p)$. As $n \geq p \geq q \in \mathbf{N}$, so $m \leq \min(q, n - q) \leq \frac{n}{2}$. Let us choose such mapping, that $t_{e,o} = m$. There are two cases.

a) $m = q$. Now $t_{e,o} = q$ and $q = t_{e,o} + t_{o,o} = q + t_{o,o}$. From that equation follows that $t_{o,o} = 0$. Then $n - p = t_{e,o} + t_{o,e} = q + t_{o,e}$ and we get that $t_{o,e} = n - p - q$. If each of the $t_{e,o} = q$ pairwise disjoint even-length cycles is a transposition, that is a cycle of length of 2, while the length of the $t_{o,e} = n - p - q$ cycles of odd length, pairwise different and disjoint to every transposition mentioned previously is equal to 1, then the product of all the elements of those cycles affect $2q + n - p - q = n - p + q \geq 0$ elements altogether. If we take into consideration that $t_{o,o} = 0$ then the further $t_{e,e}$ cycles of even length contain $n - (n - p + q) = p - q$ elements. As p and q have the same

parity, $p-q$ is even, and then each of these cycles can be a transposition of two distinct elements. With the previous data let

$$\pi = \prod_{k=1}^{q} (2k-1, 2k) \prod_{k=q+1}^{q+\frac{(p-q)}{2}} (2k-1, 2k)$$

and

$$\underline{\alpha} = (\underbrace{1, 0, \ldots 1, 0}_{2q}, \underbrace{0, \ldots, 0}_{p-q}, \underbrace{0, \ldots, 0}_{n-p-q}).$$

With this π and $\underline{\alpha}$ we get that $t_{e,e} = \frac{p-q}{2}$, $t_{e,o} = q$, $t_{o,e} = n-p-q$ and $t_{o,o} = 0$.

b) $m = n - p$. Similarly counting as in the previous point, from $q = t_{e,o} + t_{o,o} = n - p + t_{o,o}$ we get that $t_{o,o} = q - n + p$, and the equation of $n - p = t_{e,o} + t_{o,e} = n - p + t_{o,e}$ is equivalent to $t_{o,e} = 0$. Let each of the $t_{e,o}$ cycles of even length be again a transposition and the length of each of the $t_{o,o} = q-n+p$ cycles of odd length be equal to 1. Then the number of the indices not involved in the previous cycles is equal to $n - (2(n-p) + q - n + p) = p - q$, like in case a), and we can again arrange these elements into pairwise disjoint cycles of length of 2. Now with the permutation

$$\pi = \prod_{k-1}^{n-p} (2k-1, 2k) \prod_{k=n-p+1}^{n-p+\frac{p-q}{2}} (2k-1, 2k)$$

and with the vector

$$\underline{\alpha} = (\underbrace{1, 0, \ldots, 1, 0}_{2(n-p)}, \underbrace{0, \ldots, 0}_{p-q}, \underbrace{1, \ldots, 1}_{q-n+p})$$

we get that $t_{e,e} = \frac{p-q}{2}$, $t_{e,o} = n - p$, $t_{o,e} = 0$ and $t_{o,o} = q - n + p$. ■

References

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

[2] **Gonda, J.,** Metrics on the hyperoctahedral group (in Hungarian), in: *Informatika a felsöoktatásban 2008*, `http://www.agr.unideb.hu/if2008/kiadvany/papers/F11.pdf`

[3] **Gonda, J.,** Metric on the hyper-octahedral group: the minimal deviation, *Acta Univ. Sapientiae, Mathematica*, **4(2)** (2012), 109–116.
[4] **Hall, M.jr.,** *The Theory of Groups*, MacMillan Co., New York, 1959.
[5] **Huppert, B.,** *Endliche Gruppen 1.*, Springer, Berlin, 1967.
[6] **Kaluzhnin, L.A., P.M. Beleckij and V.Z. Feinberg,** *Kranzprodukte*, Teubner-Texte Vol. 101., B. G. Teubner, Leipzig, 1987.
[7] **Kaluzhnin, L.A., M. Kh. Klin and V.I. Sushchanskii,** Exponantiation of permutation groups I. (in Russian), *Izv. Vyssch. Uchebn. Zaved. Mat.*, **8** (1979), 26–33.
[8] **Krasner, M. and L.A. Kaluzhnin,** Produit complet des groupes de permutations et problème d'extension de groupes I., *Acta Sci. Math. Szeged*, **13** (1950), 208–230.
[9] **Krasner, M. and L.A. Kaluzhnin,** Produit complet des groupes de permutations et problème d'extension de groupes II., *Acta Sci. Math. Szeged*, **14** (1951), 39–66, 69–82.
[10] **Pontryagin, L.S.,** *Continuous Groups*, in Russian, Nauka, Moscow, 1984.

J. Gonda
Department of Computer Algebra
Faculty of Informatics
Eötvös Loránd University
H-1117 Budapest
Pázmány Péter sétány 1/C
Hungary
andog@inf.elte.hu