## The AfHom and boolean functions

Anna Jenčová

June 14, 2024

AfH is the subcategory of Af generated from first order objects by taking tensor products and duals. Any first order object X has the form  $X = (V_X, \{\tilde{a}_X\}^{\sim})$  where  $\tilde{a}_X \in V_X^*$ . We have

$$S_X = V_X, \qquad L_X = \{\tilde{a}_X\}^{\perp}.$$

Let us pick any  $a_X \in \{\tilde{a}_X\}^{\sim}$  and let us denote

$$L_{X,0} := \mathbb{R}a_X, \quad L_{X,1} := \{\tilde{a}_X\}^{\perp}, \quad L_{X^*,0} := \mathbb{R}\tilde{a}_X, \quad L_{X^*,1} := \{a_X\}^{\perp}.$$

We have the decompositions

$$V_X = L_{X,0} \oplus L_{X,1}, \qquad V_X^* = L_{X^*,0} \oplus L_{X^*,1}$$
 (1)

and

$$L_{X,0}^{\perp} = L_{X^*,1}, \quad L_{X,1}^{\perp} = L_{X^*,0}.$$
 (2)

Let Y be an object of AfH. Ten Y is constructed from a set of distinct first order object  $X_1, \ldots, X_n$ . In this case, we will write  $Y \sim [X_1, \ldots, X_n]$ . Since FinVect is compact,  $(V \otimes W)^* = V^* \otimes W^*$ , so that the vector space of Y has the form

$$V_Y = V_{i_1} \otimes \cdots \otimes V_{i_n},$$

where  $V_i$  is either  $V_{X_i}$  or  $V_{X_i}^*$ , according to whether  $X_i$  was subjected to taking duals an even or odd number of times. The indices such that the first case is true will be called the outputs and the subset of outputs in [n] will be denoted by O, or  $O_Y$ , when we need to specify the object. The set  $I = I_Y := [n] \setminus O_Y$  is the set of inputs. The following statement shows the reason for this terminology. The proof of Proposition 1 will be given later below.

**Proposition 1.** Let  $Y \sim [X_1, \ldots, X_n]$ . Let us denote

$$X_I := \bigotimes_{i \in I} X_i, \qquad X_O := \bigotimes_{i \in O} X_i.$$

Then there is a permutation  $\sigma \in S_n$  such that

$$X_I^* \otimes X_O \xrightarrow{\sigma} Y \xrightarrow{\sigma^{-1}} [X_I, X_O].$$

We introduce the following notations:

$$V_i := V_{X_i}, \quad L_{i,u} := L_{X_i,u}, \quad \tilde{L}_{i,u} = L_{X_i^*,u}, \ u \in \{0,1\}, \qquad i \in O$$

and

$$V_i := V_{X_i}^*, \quad L_{i,u} := L_{X_i^*,u}, \quad \tilde{L}_{i,u} = L_{X_i,u}, \ u \in \{0,1\}, \qquad i \in I.$$

Further,

$$a_i := a_{X_i}, \quad \tilde{a}_i := \tilde{a}_{X_i}, \quad i \in O, \qquad a_i := \tilde{a}_{X_i}, \quad \tilde{a}_i := a_{X_i}, \quad i \in I.$$

We will also denote for  $s \in \{0,1\}^n$ ,

$$L_s := L_{i_1, s_{i_1}} \otimes \cdots \otimes L_{i_n, s_{i_n}}, \qquad \tilde{L}_s := \tilde{L}_{i_1, s_{i_1}} \otimes \cdots \otimes \tilde{L}_{i_n, s_{i_n}}.$$

Notice that the subspaces  $L_s$ ,  $s \in \{0,1\}^n$  form an independent decomposition of the space  $V_Y$ , so that they generate a distributive sublattice in the latice of subspaces of  $V_Y$ . Similarly,  $\tilde{L}_s$ ,  $s \in \{0,1\}^n$  form an independent decomposition of  $V_Y^*$ .

We next describe the affine subspace  $A_Y$ . We will need the following easy lemmas.

Lemma 1. We have

$$a_Y := a_{i_1} \otimes \cdots \otimes a_{i_n} \in A_Y, \quad \tilde{a}_Y := \tilde{a}_{i_1} \otimes \cdots \otimes \tilde{a}_{i_n} \in \tilde{A}_Y.$$

*Proof.* Easy.

**Lemma 2.** For any  $s \in \{0,1\}^n$ , we have

$$L_s^{\perp} = \bigoplus_{\substack{t \in \{0,1\}^n \\ t \neq s}} \tilde{L}_t.$$

*Proof.* Using (1) and (2), we get

$$(L_{i_1,s_{i_1}} \otimes \cdots \otimes L_{i_n,s_{i_n}})^{\perp} = \bigvee_{j} \left( V_{i_1}^* \otimes \cdots \otimes V_{i_{j-1}}^* \otimes \tilde{L}_{i_j,1-s_{i_j}} \otimes V_{i_{j+1}}^* \otimes \cdots \otimes V_{i_n}^* \right)$$

$$= \bigvee_{t \in \{0,1\}^n \atop t \neq s} \tilde{L}_{i_1,t_{i_1}} \otimes \cdots \otimes \tilde{L}_{i_n,t_{i_n}} \right)$$

$$= \bigoplus_{t \in \{0,1\}^n \atop t \neq s} \left( \tilde{L}_{i_1,t_{i_1}} \otimes \cdots \otimes \tilde{L}_{i_n,t_{i_n}} \right).$$

We next show how the objects are related to some boolean functions, in fact, these functions are related to types of objects in AfH, rather than objects themselves.

**Theorem 1.** For any object in AfH, there is a function  $f = f_Y : \{0,1\}^n \to \{0,1\}$  and a permutation  $i_1, \ldots, i_n$  of elements in [n], such that

$$S_Y = \bigoplus_{s \in \{0,1\}^n} f(s) L_{i_1,s_{i_1}} \otimes \cdots \otimes L_{i_n,s_{i_n}}.$$

*Proof.* We will proceed by induction on n. For n = 1, the assertion is easily seen to be true, since in this case, Y is itself first order and

$$S_Y = V_Y = L_{1,0} \oplus L_{1,1} = f(0)L_{1,0} \oplus f(1)L_{1,1},$$

here  $f: \{0,1\} \to \{0,1\}$  is the constant 1. Assume now that the assertion is true for all m < n. By construction, Y is either the tensor product of two other objects in AfH or Y is the dual of such a product. Let us assume the first case. Then there is a parmutation  $i_1, \ldots, i_n$  of [n] and 0 < m < n such that  $Y = Y_1 \otimes Y_2$ , with

$$Y_1 \sim [X_{i_1}, \dots, X_{i_m}], \qquad Y_2 \sim [X_{i_{m+1}}, \dots, X_{i_n}].$$

By the assumption, there are functions  $f_1: \{0,1\}^m \to \{0,1\}$  and  $f_2: \{0,1\}^{n-m} \to \{0,1\}$ , and permutations  $k_1, \ldots, k_m$  of  $[m], l_1, \ldots, l_{n-m}$  of [n-m] such that

$$S_Y = S_{Y_1} \otimes S_{Y_2} = \bigoplus_{\substack{s \in \{0,1\}^m \\ t \in \{0,1\}^{n-m}}} f_1(s) f_2(t) L_{i_{k_1}, s_{k_1}} \otimes \cdots \otimes L_{i_{k_m}, s_{k_m}} \otimes L_{i_{m+l_1}, t_{l_1}} \otimes \cdots \otimes L_{i_{m+l_{n-m}}, t_{l_{n-m}}}$$

Since  $\{0,1\}^n \simeq \{0,1\}^m \times \{0,1\}^{n-m}$ , we get the assertion, with  $f(s,t) = f_1(s)f_2(t)$  and the permutation  $i_{k_1}, \ldots, i_{k_m}, i_{m+l_1}, \ldots, i_{m+l_{n-m}}$  of [n].

To finish the proof, it is now enough to observe that if the assertion holds for Y then it also holds for  $Y^*$ . So assume that Y has the required form. Let  $a_Y$  and  $\tilde{a}_Y$  be as in Lemma 1, then  $\tilde{a}_Y \in \tilde{A}_Y$ , so that  $L_Y = S_Y \cap \{\tilde{a}_Y\}^{\perp}$ . As before, we use the notation

$$L_s := L_{i_1, s_{i_1}} \otimes \cdots \otimes L_{i_n, s_{i_n}}, \qquad \tilde{L}_s := \tilde{L}_{i_1, s_{i_1}} \otimes \cdots \otimes \tilde{L}_{i_n, s_{i_n}}.$$

respecting the permutation  $i_1, \ldots, i_n$  of Y, so that

$$S_Y = \bigoplus_{s \in \{0,1\}^n} f(s) L_s.$$

It is easily seen that for any  $s \in \{0,1\}^n$ ,  $L_s \subseteq \{\tilde{a}_Y\}^{\perp}$  if and only if  $s_i = 1$  for at least some  $i \in [n]$ , that is,  $s \neq 00...0$ . Hence

$$L_Y = \bigoplus_{\substack{s \in \{0,1\}^n \\ s \neq 0}} f(s) L_s.$$

We then have using Lemma 2 and the fact that  $\tilde{L}_t$ ,  $t \in \{0,1\}^n$  form an independent decomposition of  $V_V^*$ ,

$$S_{Y^*} = L_Y^{\perp} = \left(\bigoplus_{\substack{s \in \{0,1\}^n \\ s \neq 0}} f(s)L_s\right)^{\perp} = \bigwedge_{\substack{s \in \{0,1\}^n \\ s \neq 0, f(s) = 1}} L_s^{\perp} = \bigwedge_{\substack{s \in \{0,1\}^n \\ s \neq 0, f(s) = 1}} \left(\bigoplus_{\substack{t \in \{0,1\}^n \\ t \neq s}} \tilde{L}_t\right)$$

$$= \bigoplus_{\substack{t \in \{0,1\}^n \\ s \neq 0, f(s) = 1}} \left(\bigwedge_{\substack{s \in \{0,1\}^n \\ s \neq 0, f(s) = 1}} (1 - \chi_s(t))\tilde{L}_t\right) = \bigoplus_{\substack{t \in \{0,1\}^n \\ s \neq 0, f(s) = 1}} f^*(t)\tilde{L}_t.$$

Here  $\chi_s: \{0,1\}^n \to \{0,1\}$  is the characteristic function of s and  $f^*: \{0,1\}^n \to \{0,1\}$  is given as

$$f^*(t) := \bigwedge_{\substack{s \in \{0,1\}^n \\ s \neq 0, f(s) = 1}} (1 - \chi_s(t)) = \begin{cases} 1 & \text{if } t = 0 \\ 1 - f(t) & \text{if } t \neq 0. \end{cases}$$

Note also that the change  $L_s$  to  $\tilde{L}_s$  corresponds precisely to swapping the sets of inputs and outputs, which is what happens after taking the dual. This finishes the proof.

The above theorem shows that any element  $Y \sim [X_1, \ldots, X_n]$  is up to a permutation determined by a unique boolean function  $f = f_Y : \{0,1\}^n \to \{0,1\}$ , uniqueness follows from the fact that  $L_s, s \in \{0,1\}^n$  form an independent decomposition of  $V_Y$ . It is rather obvious that not all boolean functions give rise to an object of AfH, for example, for  $Y \sim [X]$  we only have Y = X and  $Y = X^*$ , which corresponds to constant 1 and the negation, respectively. In general, one can see from the above proof that we necessarily have

$$f \in \mathcal{F}_n = \{g : \{0,1\}^n \to \{0,1\}, \ g(0) = 1\}.$$

Pick any  $f \in \mathcal{F}_n$  and any permutation  $i_1, \ldots, i_n$ . Keeping the above notations, in particular the input-output decomposition  $[n] = I \cup O$ , let

$$S_f := \bigoplus_{s \in \{0,1\}^n} f(s)L_s, \qquad A_f := S_f \cap \{\tilde{a}\}^{\sim}.$$

Then  $A_f$  is a proper affinne subspace in  $V := \bigotimes_j V_{i_j}$ , this follows from the fact that f(0) = 1, so that S contains the subspace  $\mathbb{R}a$ . Then  $Y_f := (\bigotimes_j V_{i_j}, A_f)$  defines an object in Af such that  $a \in A_f$  and  $\tilde{a} \in \tilde{A}_f$ . Such objects might not belong to AfH in general. With the pointwise ordering,  $\mathcal{F}_n$  is a distributive lattice, with the smallest element  $\chi_0$  and largest element 1. It is easy to see that for  $f, g \in \mathcal{F}_n$  and some corresponding objects  $Y_f, Y_g$ , we have  $f \leq g$  if and only if there is some permutation  $\sigma \in S_n$  such that  $Y_f \stackrel{\sigma}{\to} Y_g$ . In particular, since  $\chi_0 \leq f \leq 1$  for all  $f \in \mathcal{F}_n$ , there is some permutation  $\sigma$  such that

$$Y_{\min} \xrightarrow{\sigma} Y_f \xrightarrow{\sigma^{-1}} Y_{\max},$$

where

$$Y_{\min} := (V_1 \otimes \cdots \otimes V_n, \{a_1 \otimes \cdots \otimes a_n\}), \qquad Y_{\max} := (V_1 \otimes \cdots \otimes V_n, \{\tilde{a}_1 \otimes \cdots \otimes \tilde{a}_n\}^{\sim}).$$

If  $Y_g$  is an object such that

$$Y_{\min} \xrightarrow{\rho} Y_g \xrightarrow{\rho^{-1}} Y_{\max},$$

for a permutation  $\rho$ , then we may define an object corresponding to  $f \wedge g$  as the pullback of the two arrows  $f \xrightarrow{\sigma^{-1}} Y_{\text{max}}$  and  $g \xrightarrow{\rho^{-1}} Y_{\text{max}}$ , similarly,  $Y_{f \vee g}$  can be found as a pushout.

## 1 Boolean functions

We will work with certain boolean functions, which are defined as functions from binary strings to  $\{0,1\}$ . We now list some basic notations used below.

For  $s \in \{0,1\}$ , we denote  $\bar{s} := 1-s$ . For binary strings of fixed length n, that is, elements of  $\{0,1\}^n$ , we will denote by  $0_n$  or just 0 the string 00...0 and by  $e^i$  the string such that  $e^i_j = \delta_{i,j}$ . For  $m, n \in \mathbb{N}$ , the concatenation of strings  $s \in \{0,1\}^m$  and  $t \in \{0,1\}^n$  will be denoted by st, that is,

$$st = s_1 \dots s_m t_1 \dots t_n \in \{0, 1\}^{m+n}$$
.

For any permutation  $\sigma \in S_n$ , we will denote by the same symbol the obvious action on  $\{0,1\}^n$ , that is

$$\sigma(s_1 \dots s_n) = s_{\sigma^{-1}(1)} \dots s_{\sigma^{-1}(n)}.$$

We start by looking at the set

$$\mathcal{F}_n := \{ f : \{0,1\}^n \to \{0,1\}, \ f(0) = 1 \}.$$

With the poitwise ordering,  $\mathcal{F}_n$  is a (finite) distributive lattice, with top element the constant 1 function and the bottom element  $p_n := \chi_0$ . We may also define the complementation in  $\mathcal{F}_n$  as

$$f^* := 1 - f + p_n.$$

It can be easily checked that with these structures  $\mathcal{F}_n$  is a boolean algebra.

We now introduce some more operations in  $\mathcal{F}_n$ . For  $f \in \mathcal{F}_n$  and any permutation  $\sigma \in S_n$ , we see that  $f \circ \sigma \in \mathcal{F}_n$ . For  $f \in \mathcal{F}_m$  and  $g \in \mathcal{F}_n$ , we define the function  $f \otimes g \in \mathcal{F}_{m+n}$  as

$$(f \otimes g)(st) = f(s)g(t).$$

As it is, this tensor product is not symmetric, but there is a permutation  $\sigma \in S_{m+n}$  such that  $(g \otimes f) = (f \otimes g) \circ \sigma$  for any  $f \in \mathcal{F}_m$  and  $g \in \mathcal{F}_n$ .

**Lemma 3.** For  $f \in \mathcal{F}_m$ ,  $g \in \mathcal{F}_n$ , we have

$$f \otimes g \le (f^* \otimes g^*)^*$$
.

Equality holds if and only if f and g are both maximal or both minimal elements in  $\mathcal{F}_m$  resp.  $\mathcal{F}_n$ .

Proof. The inequality is easily checked, since  $(f \otimes g)(st)$  can be 1 only if f(s) = g(t) = 1. If both s and t are the zero strings, then  $st = 0_{m+n}$  and both sides are equal to 1. Otherwise, the condition f(s) = g(t) = 1 implies that  $(f^* \otimes g^*)(st) = 0$ , which implies that the right hand side must be 1. If f and g are both constant 1, then  $(1 \otimes 1)^* = 1^* = p_{n+m} = 1^* \otimes 1^*$ , the other case follows by duality. Finally, asume the equality holds and that  $f \neq 1$ , so that there is some s such that f(s) = 0. But then  $s \neq 0$  and for any t,

$$0 = f(s)g(t) = 1 - f^*(s)g^*(t) + p_{m+n}(st) = 1 - g^*(t),$$

which implies that g(t) = 0 for all  $t \neq 0$ , that is,  $g = p_n$ . By the same argument,  $f = p_m$  if  $g \neq 1$ .

We now show an important example.

Example 1. Let  $S \subseteq [n]$  be any subset. We will denote

$$p_S(s) := \prod_{i \in S} \bar{s}_i.$$

It is clear that  $p_S \in \mathcal{F}_n$ ,  $p_{\emptyset} = 1$ ,  $p_{[n]} = \chi_0 = p_n$ . The following properties are also easy to see for  $S, T \subseteq [n]$ :

- (i) if  $S \subseteq T$ , then  $p_T \leq p_S$ ,
- (ii)  $p_S \wedge p_T = p_S p_T = p_{S \cup T}$ ,
- (iii)  $p_S \vee p_T = p_S + p_T p_{S \cup T}$ .
- (iv) let  $S \subseteq [m]$  and  $T \subseteq [n]$ , then

$$p_S \otimes p_T = p_{S \cup (m+T)}$$
.

We will use the above functions to introduce a convenient parametrization to  $\mathcal{F}_n$ . For this, we first include  $\mathcal{F}_n$  into a larger set

$$\mathcal{F}_n \subseteq \{f: \{0,1\}^n \to \mathbb{R}\} =: \mathcal{V},$$

which is a  $2^n$ -dimensional real vector space. It becomes a Hilbert space with respect to the inner product

$$\langle f, g \rangle = \sum_{s \in \{0,1\}^n} f(s)g(s).$$

**Lemma 4.** The set  $\{p_S, S \subseteq [n]\}$  is a basis of  $\mathcal{V}$ . Any  $f \in \mathcal{V}$  can be written as

$$f = \sum_{S \subseteq [n]} \hat{f}_S p_S,$$

where the coefficients are obtained as

$$\hat{f}_S = \sum_{\substack{x \in \{0,1\}^n \\ x_i = 1 \ \forall i \in S^c}} (-1)^{\sum_{i \in S} x_i} f(x)$$

*Proof.* For  $T \subseteq [n]$ , let us define the function  $p_T^{\perp}$  as

$$p_T^{\perp}(x) := (-1)^{\sum_{i \in T} x_i} \prod_{i \in T^c} x_i.$$

We prove that for  $S, T \subseteq [n]$ ,

$$\langle p_S, p_T^{\perp} \rangle = \delta_{S,T},$$

which shows that  $\{p_S, S \subseteq [n]\}$  is a basis and  $\{p_T^{\perp}, T \subseteq [n]\}$  is the dual basis. We compute

$$\langle p_S, p_T^{\perp} \rangle = \sum_x p_S(x) p_T^{\perp}(x) = \sum_x (-1)^{\sum_{i \in T} x_i} \prod_{i \in S} \bar{x}_i \prod_{j \in T^c} x_j.$$

This expression can be nonzero only if  $S \cap T^c = \emptyset$ , that is,  $S \subseteq T$ . In this case, the last sum is equal to

$$\sum_{\substack{x \in \{0,1\}^n \\ x_i = 0, \forall i \in S \\ x : -1, \forall i \in T^c}} (-1)^{\sum_{j \in T \setminus S} x_j} = \begin{cases} 0 & \text{if } S \subsetneq T \\ 1 & \text{if } S = T \end{cases}$$

It is now clear that the coefficients

$$\hat{f}_S = \langle f, p_S^{\perp} \rangle$$

have the given form.

It may be useful to visualise the lattice  $\mathcal{L}_n = \{S \subseteq [n]\}$  as a hypercube, and the coefficients of f as labels for its vertices. The fact that the function f has values in  $\{0,1\}$  means that for a string  $x \in \{0,1\}^n$  such that  $x_j = 1$  if and only if  $j \in T$ , we must have

$$f(x) = \sum_{\substack{S \subseteq [n] \\ S \cap T = \emptyset}} \hat{f}_S \in \{0, 1\},$$

that is, the sum of labels  $\hat{f}_S$  over any face containing the vertex  $\emptyset$  must be 0 or 1. In particular,  $\hat{f}_{\emptyset} = f(11...1) \in \{0,1\}$ , which restricts the values of  $\hat{f}_{\{i\}} \in \{0,1,-1\}$ , etc. The fact that  $f \in \mathcal{F}_n$  means that in addition,

$$f(0) = \sum_{S \subseteq [n]} \hat{f}_S = 1.$$

## 1.1 Types

We are now interested in the subset  $\mathcal{F}_n^H$  in  $\mathcal{F}_n$  of elements that can be obtained from the constant function 1 on  $\{0,1\}$  by taking complements, tensor products and precomposing with permutations. This gives the following description.

**Definition 1.** The set  $\mathcal{F}_n^H$  is the smallest subset in  $\mathcal{F}_n$  such that:

- 1. it is invariant under permutations: if  $f \in \mathcal{F}_n^H$ , then  $f \circ \sigma \in \mathcal{F}_n^H$  for any permutation  $\sigma$ ,
- 2. it is invariant under complementation: if  $f \in \mathcal{F}_n^H$  then  $f^* \in \mathcal{F}_n^H$ ,
- 3. if  $f \in \mathcal{F}_n^H$  and  $g \in \mathcal{F}_m^H$ , then  $f \otimes g \in \mathcal{F}_{n+m}^H$ ,
- 4.  $\mathcal{F}_1^H = \{1, \chi_0\} = \mathcal{F}_1$ .

Given a function  $f \in \mathcal{F}_n^H$ , we see from the above definition that it has the form

$$f(x_1 \dots x_n) = ((1(x_1 \dots x_k)1^*(x_{k+1} \dots x_l))^* \dots)^* 1(x_{m+1} \dots x_n) \circ \sigma$$

where  $\sigma$  is some permutation. let  $O \subseteq [n]$  be the set of indices such that

Example 2. We have  $p_S \in \mathcal{F}_n^H$  for any  $S \subseteq [n]$ . Indeed, we have  $p_S = f_1 \otimes \cdots \otimes f_n$ , where  $f_i = \chi_0 = 1^*$  if  $i \in S$  and  $f_i = 1$  otherwise. The complement is  $f^* = 1 - p_S + p_n$ , the corresponding objects are  $[X_{[n]\setminus S}, X_S]$ . Note that in this case, S is the set of inputs of  $p_S$  and the set of outputs of  $p_S^*$ .

For  $Y \sim [X_1, \ldots, X_n]$ , let  $f \in \mathcal{F}_n^H$  be the corresponding function and let  $O \subseteq [n]$  be the corresponding set of outputs. By the construction of the functions in Theorem 1, we can see that the set O can be obtained from f, as the set of indices such that the corresponding element was under complementation an even number of times.

**Proposition 2.** Let  $f \in \mathcal{F}_n^H$  and let  $O \subseteq [n]$  be the set of outputs,  $I = [n] \setminus O$  the set of inputs. Then

$$p_I \le f \le p_O^*$$
.

*Proof.* This is obviously true for n = 1. In this case,  $\mathcal{F}_1^H = \mathcal{F}_1 = \{1, \chi_0 = p_{\{1\}}\}$  and  $1^* = p_{\{1\}}$ . If f = 1, then  $O = \{1\}$ , so that

$$p_I = p_{\emptyset} = 1 = p_{\{1\}}^*,$$

the other case is obtained by taking complements. Assume that the assertion holds for m < n. Let  $f \in \mathcal{F}_n^H$  and assume that  $f = g \otimes h$  for some  $g \in \mathcal{F}_m^H$ ,  $h \in \mathcal{F}_{n-m}^H$ . Let  $O_1 \subseteq [n_1]$  be the set of outputs for g and  $O_2 \subseteq [n-m]$  for h. By the assumption,

$$p_{I_1} \otimes p_{I_2} \leq g \otimes h \leq p_{O_1}^* \otimes p_{O_2}^* \leq (p_{O_1} \otimes p_{O_2})^*.$$

Here the last inequality is from a more general inequality  $f^* \otimes g^* \leq (f \otimes g)^*$  which holds for any  $f \in \mathcal{F}_m$ ,  $g \in \mathcal{F}_{n-m}$ . Indeed, for any s,t not both equal to 0, we have  $f^*(s)g^*(t) = 1$  if and only if f(t) = g(s) = 0, in which case  $(f(s)g(t))^* = 1$ . It is now enough to notice that the outputs of f are precisely  $i \in O_1$  and m + j,  $j \in O_2$ . Assume that the inequality holds for  $f \in \mathcal{F}_n^H$ , we will show that it is preserved by permutations and complements. Indeed, let  $\sigma$  be any permutation of the indices, then clearly

$$p_I \circ \sigma \le f \circ \sigma \le p_O^* \circ \sigma.$$

It is enough to note that the outputs of  $f \circ \sigma$  are  $\sigma^{-1}(O)$ , similarly for the inputs, and  $p_{\sigma^{-1}(S)} = p_S \circ \sigma$  for any  $S \subseteq [n]$ . Finally, we have by duality

$$p_O \le f^* \le p_I^*,$$

and taking complements exchanges inputs and outputs.

The next result shows that there is a direct way to obtain this set from f.

**Proposition 3.** Let  $f \in \mathcal{F}_n^H$  and let  $O \subseteq [n]$  be the corresponding set of outputs. Then  $i \in O$  if and only if  $f(e^i) = 1$  (here  $e_j^i = \delta_{i,j}$ ,  $j = 1, \ldots, n$ ).

Proof.