NMMB331 - HW4

Jan Oupický

1

1. $\sim_{EA}$ is reflexive since we can take $A = id = B$ (identities) and $C = 0$ (null map).
2. If A, B are affine permutations and C is an affine map s.t. $G(x) = A \circ F \circ B(x) + C(x) \iff F \sim_{EA} G$ then we can write $A^{-1} \circ G \circ B^{-1}(x) + A^{-1} \circ C \circ B^{-1}(x) = F(x) \iff G \sim_{EA} F$. Since A, B are affine permutations then their inverses are also affine permutations and also $A^{-1} \circ C \circ B^{-1}$ is affine since C is affine and A^{-1}, B^{-1} are affine permutations. This proves symmetry.
3. Assume $F \sim_{EA} G$, $G \sim_{EA} H$ and we want to show $F \sim_{EA} H$. By definition we have $G(x) = A_1 \circ F \circ B_1(x) + C_1(x)$ and $H(x) = A_2 \circ G \circ B_2(x) + C_2(x)$. $A_2(x) = M(x) + y$ for some M linear permutation and y vector.

$$H(x) = A_2 \circ G \circ B_2(x) + C_2(x) = A_2(A_1 \circ F \circ B_1(B_2(x)) + C_1(B_2(x))) + C_2(x) =$$
$$M(A_1 \circ F \circ B_1(B_2(x)) + C_1(B_2(x))) + y + C_2(x) =$$
$$M(A_1 \circ F \circ B_1(B_2(x))) + M(C_1(B_2(x))) + y + C_2(x) =$$
$$(M \circ A_1) \circ F \circ (B_1 \circ B_2)(x) + (M \circ C_1 \circ B_2(x) + y + C_2(x))$$

$M \circ A_1$ is an affine permutation since M is linear permutation and A_1 is affine permutation. $B_1 \circ B_2$ is affine permutation since both are affine permutations. $M \circ C_1 \circ B_2$ is affine map since M, B_2 are affine permutations and C_1 affine map, $C_2(x) + y$ is an affine map. Sum of affine maps is affine map. This proves transitivity.

□

2

A point $(x, F(x))$ on Γ_F corresponds with a point $(F(x), x)$ on $\Gamma_{F^{-1}}$ since $F^{-1}(F(x)) = x$. Therefore our affine permutation should just switch those two "coordinates".

Using the notation mentioned we can set $A, D = 0$ (zero matrix) and B, C to be identity matrices of dimension n. The affine parts u, v are also zero vectors. This map is clearly an affine permutation and as said before it maps $\Gamma_{F^{-1}} = \mathcal{A}(\Gamma_F)$. □

3

Since $G \sim_{CCZ} F$ we know that for a $x \in \mathbb{F}_2^n$ there exists $y \in \mathbb{F}_2^n$ s.t.:

$$\begin{pmatrix} y \\ G(y) \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} \begin{pmatrix} x \\ F(x) \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix}$$
$$\iff$$
$$y = Ax + u$$
$$G(y) = Cx + (D \circ F)(x) + v$$

Since $\mathcal{A}$ is an affine permutation it must be that the map $M : x \mapsto Ax + u$ is invertible i.e. $x = A^{-1}(y + u) = A^{-1}(y) + A^{-1}(u)$ where A^{-1} is the matrix inverse of A. Therefore the inverse map $M^{-1} : y \mapsto A^{-1}y + A^{-1}u$ is also an affine permutation. Now we will just apply it to our equality above.

$$G(y) = Cx + (D \circ F)(x) + v \iff (G \circ M)(x) = Cx + (D \circ F)(x) + v$$
$$\text{Apply inverse } M^{-1}:$$
$$G(x) = (C \circ M^{-1})(x) + (D \circ F \circ M^{-1})(x) + M^{-1}v$$
$$G(x) = (D \circ F \circ M^{-1})(x) + ((C \circ M^{-1})(x) + M^{-1}v)$$

We know that M^{-1} is an affine permutation . C is a linear map and therefore the composition of M^{-1} and C is also an linear map and together with the constant vector $M^{-1}v$ they form an affine map.

Now we just need to show that D is an affine permutation to fullfil the EA requirements. Since $\mathcal{A} = \mathcal{L} + (u, v)$ and $\mathcal{A}$ is an affine permutation and $\mathcal{L}$ is linear, it must be that $\mathcal{L}$ is a linear permuation. Since $\mathcal{L}$ can be represented as a matrix and is a permutation that means that every subset of it columns must be linearly independent. Choose the subset of columns containing D. They must be linearly independent and this implies that columns of D must be linearly independent since $B = 0$. This means that D is a linear permutation. $\square$

4

Since $F \sim_{CCZ} G$ where $u, v = 0$ we can write that for some $x \in \mathbb{F}_2^n : y = F_1(x)$ and $G(y) = F_2(x)$. We want to show that there exists 1 to 1 correpondence between $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ and some $(a', b') \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ s.t. $\hat{G}(a, b) = \hat{F}(a', b')$.

$$\hat{G}(a, b) = \sum_{y \in \mathbb{F}_2^n} (-1)^{\langle a, G(y) \rangle + \langle b, y \rangle} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle a, F_2(x) \rangle + \langle b, F_1(x) \rangle}$$
$$\text{Lets focus on the exponent now:}$$
$$\langle a, F_2(x) \rangle + \langle b, F_1(x) \rangle = \langle a, Cx + D(F(x)) \rangle + \langle b, Ax + B(F(x)) \rangle =$$
$$\langle a, Cx \rangle + \langle a, D(F(x)) \rangle + \langle b, Ax \rangle + \langle b, B(F(x)) \rangle =$$
$$A, B, C, D \text{ are all linear so we will use their adjoint maps:}$$
$$= \langle C^* a, x \rangle + \langle D^* a, F(x) \rangle + \langle A^* b, x \rangle + \langle B^* b, F(x) \rangle =$$
$$\langle C^* a + A^* b, x \rangle + \langle D^* a + B^* b, F(x) \rangle \implies$$
$$\hat{G}(a, b) = \hat{F}(a', b') \text{ where } a' = C^* a + A^* b, b' = D^* a + B^* b$$
$$\text{In matrix notation:}$$
$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} A^* & C^* \\ B^* & D^* \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} \iff (a', b') = \mathcal{L}^*(b, a)$$

Since we know that $\mathcal{L}^*$ is a permutation then we have the 1 to 1 correspondence between (a, b) and (a', b'). $\square$