Fourier Analysis of MAC Polarization

Rajai Nasser, Emre Telatar
Ecole Polytechnique Fédérale de Lausanne,
Lausanne, Switzerland
Email: {rajai.nasser, emre.telatar}@epfl.ch

Abstract

A problem of the polar code construction for multiple access channels (MACs) is that they do not always achieve the whole capacity region. Although polar codes achieve the sum-capacity of symmetric MACs, polarization may induce a loss in the capacity region which prevents polar codes from achieving the whole capacity region. This paper provides a single letter necessary and sufficient condition which characterizes all the MACs that do not lose any part of their capacity region by polarization.

I. Introduction

Polar coding is a low complexity coding technique invented by Arıkan which achieves the capacity of symmetric binary input channels [1]. The probability of error of polar codes was shown to be roughly $o(2^{-N^{\frac{1}{2}-\epsilon}})$ where N is the block length [2]. The polar coding construction of Arıkan transforms a set of identical and independent channels to a set of "almost perfect" or "almost useless channels". This phenomenon is called *polarization*.

Polarizing transformations can also be constructed for non-binary input channels. Şaşoğlu et al. [3] generalized Arıkan's results to channels where the input alphabet size is prime. Park and Barg [4] showed that if the size of the input alphabet is of the form 2^r with $r > 1$, then using the algebraic structure $\mathbb{Z}_{2^r}$ in the polarizing transformation leads to a multilevel polarization phenomenon: while we don't always have polarization to "almost perfect" or "almost useless" channels, we always have polarization to channels which are easy to use for communication. Multilevel polarization can be used to construct capacity achieving polar codes.

Sahebi and Pradhan [5] showed that multilevel polarization also happens if any Abelian group operation on the input alphabet is used. This allows the construction of polar codes for arbitrary discrete memoryless channels (DMC) since any alphabet can be endowed with an Abelian group structure. Polar codes for arbitrary DMCs were also constructed by Şaşoğlu [6] by using a special quasigroup operation that ensures two-level polarization. The authors showed in [7] that all quasigroup operations are polarizing (in the general multilevel sense) and can be used to construct capacity-achieving polar codes for arbitrary DMCs [8].

In the context of multiple access channels (MAC), Şaşoğlu et al. showed that if W is a 2-user MAC where the two users have $\mathbb{F}_q$ as input alphabet, then using the addition modulo q for the two users lead to a polarization phenomenon [9]. Abbe and Telatar used Matroid theory to show that for binary input MACs with $m \geq 2$ users, using the XOR operation for each user is MAC-polarizing [10]. A problem of the MAC polar code construction in [9] and [10] is that they do not always achieve the whole capacity region. Although polar codes achieve the sum-capacity of symmetric MACs, polarization may induce a loss in the capacity region which prevents polar codes from achieving the whole capacity region.

A characterization of all the polarizing transformations that are based on binary operations — in both the single-user and the multiple access settings — can be found in [11] and [12]. Abelian group operations are a special case of the characterization in [12]. Therefore, using Abelian group operations for all users is MAC-polarizing.

This paper provides a necessary and sufficient condition which characterizes all the MACs that do not lose any part of their capacity region by polarization. The characterization that we provide works in the general setting where we have an arbitrary number of users and each user uses an arbitrary Abelian group operation on his input alphabet.

II. PRELIMINARIES

Throughout this paper, $G_1, \ldots, G_m$ are finite Abelian groups. We will use the addition symbol $+$ to denote the group operations of $G_1, \ldots, G_m$.

A. Polarization

Notation 1. *Let $W : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}$ be an m-user MAC. Throughout this section, we write $(X_1, \ldots, X_m) \xrightarrow{W} Z$ to denote the following:*

- *$X_1, \ldots, X_m$ are independent random variables uniformly distributed in $G_1, \ldots, G_m$ respectively.*
- *Z is the output of the MAC W when $X_1, \ldots, X_m$ are the inputs.*

Notation 2. *Fix $S \subset \{1, \ldots, m\}$ and let $S = \{i_1, \ldots, i_{|S|}\}$. Define G_S as*

$$G_S := \prod_{i \in S} G_i = G_{i_1} \times \ldots \times G_{i_{|S|}}.$$

For every $(x_1, \ldots, x_m) \in G_1 \times \ldots \times G_m$, we write x_S to denote $(x_{i_1}, \ldots, x_{i_{|S|}})$.

Notation 3. *Let $W : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}$ and $(X_1, \ldots, X_m) \xrightarrow{W} Z$. For every $S \subset \{1, \ldots, m\}$, we write $I_S(W)$ to denote $I(X_S; ZX_{S^c})$. If $S = \{i\}$, we denote $I_{\{i\}}(W)$ by $I_i(W)$.*
$I(W) := I_{\{1,\ldots,m\}}(W) = I(X_1, \ldots, X_m; Z)$ is called the symmetric sum-capacity *of W.*

Definition 1. *The* symmetric capacity region *of an m-user MAC $W : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}$ is given by:*

$$\mathcal{J}(W) = \Big\{(R_1, \ldots, R_m) \in \mathbb{R}^m : \ \forall S \subset \{1, \ldots, m\}, \ \sum_{i \in S} R_i \leq I_S(W)\Big\}.$$

Notation 4. $\{-,+\}^* := \bigcup_{n \geq 0} \{-,+\}^n$, *where* $\{-,+\}^0 = \{\emptyset\}$.

Definition 2. *Let $W : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}$. We define the m-user MACs $W^- : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}^2$ and $W^+ : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}^2 \times G_1 \times \ldots \times G_m$ as follows:*

$$W^-(z_1, z_2 | u_{11}, \ldots, u_{1m}) = \sum_{\substack{u_{21} \in G_1 \\ \vdots \\ u_{2m} \in G_m}} \frac{1}{|G_1| \cdots |G_m|} W(z_1 | u_{11} + u_{21}, \ldots, u_{1m} + u_{2m}) \times W(z_2 | u_{21}, \ldots, u_{2m}),$$

and

$$W^+(z_1, z_2, u_{11}, \ldots, u_{1m} | u_{21}, \ldots, u_{2m}) = \frac{1}{|G_1| \cdots |G_m|} W(z_1 | u_{11} + u_{21}, \ldots, u_{1m} + u_{2m}) \times W(z_2 | u_{21}, \ldots, u_{2m}).$$

For every $s \in \{-,+\}^*$, we define the MAC W^s as follows:

$$W^s := \begin{cases} W & \text{if } s = \emptyset, \\ (\ldots((W^{s_1})^{s_2})\ldots)^{s_n} & \text{if } s = (s_1, \ldots, s_n). \end{cases}$$

Remark 1. *Let U_1^m and $U_1'^m$ be two independent random variables uniformly distributed in $G_1 \times \ldots \times G_m$. Let $X_1^m = U_1^m + U_1'^m$ and $X_1'^m = U_1'^m$. Let $(X_1, \ldots, X_m) \xrightarrow{W} Z$ and $(X_1', \ldots, X_m') \xrightarrow{W} Z'$. We have:*

- *$I(W^-) = I(U_1^m; ZZ')$ and $I(W^+) = I(U_1'^m; ZZ'U_1^m)$.*
- *$I(W) = I(X_1^m; Z)$ and $I(W^+) = I(X_1'^m; Z')$.*

Hence,

$$\begin{aligned}2I(W) &= I(X_1^m;Z)+I(X_1'^m;Z') = I(X_1^mX_1'^m;ZZ') = I(U_1^mU_1'^m;ZZ')\\ &= I(U_1^m;ZZ')+I(U_1'^m;ZZ'U_1^m) = I(W^-)+I(W^+).\end{aligned}$$

Therefore, the symmetric sum-capacity is preserved by polarization. On the other hand, I_S might not be preserved if $S \subsetneq \{1,\dots,m\}$.

For example, consider the two-user MAC case. Let $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$. Let (U_1,V_1) and (U_2,V_2) be two independent random pairs uniformly distributed in $G_1\times G_2$. Let $X_1 = U_1+U_2$, $X_2 = U_2$, $Y_1 = V_1+V_2$ and $Y_2 = V_2$. Let $(X_1,Y_1) \xrightarrow{W} Z_1$ and $(X_2,Y_2) \xrightarrow{W} Z_2$. We have:

- $I_1(W^-) = I(U_1;Z_1Z_2V_1)$ *and* $I_1(W^+) = I(U_2;Z_1Z_2U_1V_1V_2)$.
- $I_2(W^-) = I(V_1;Z_1Z_2U_1)$ *and* $I_2(W^+) = I(V_2;Z_1Z_2U_1V_1U_2)$.

On the other hand, we have

- $I_1(W) = I(X_1;Z_1Y_1) = I(X_2;Z_2Y_2)$.
- $I_2(W) = I(Y_1;Z_1X_1) = I(Y_2;Z_2X_2)$.

Therefore,

$$\begin{aligned}2I_1(W) &= I(X_1;Z_1Y_1)+I(X_2;Z_2Y_2) = I(X_1X_2;Z_1Z_2Y_1Y_2) = I(U_1U_2;Z_1Z_2V_1V_2)\\ &= I(U_1;Z_1Z_2V_1V_2)+I(U_2;Z_1Z_2V_1V_2U_1) \geq I(U_1;Z_1Z_2V_1)+I(U_2;Z_1Z_2V_1V_2U_1)\\ &= I_1(W^-)+I_1(W^+),\end{aligned} \tag{1}$$

$$\begin{aligned}2I_2(W) &= I(Y_1;Z_1X_1)+I(Y_2;Z_2X_2) = I(Y_1Y_2;Z_1Z_2X_1X_2) = I(V_1V_2;Z_1Z_2U_1U_2)\\ &= I(V_1;Z_1Z_2U_1U_2)+I(V_2;Z_1Z_2U_1U_2V_1) \geq I(V_1;Z_1Z_2U_1)+I(V_2;Z_1Z_2U_1U_2V_1)\\ &= I_2(W^-)+I_2(W^+).\end{aligned}$$

By induction on $n \geq 0$, we can show that:

$$\frac{1}{2^n}\sum_{s\in\{-,+\}^n} I_1(W^s) \leq I_1(W), \tag{2}$$

$$\frac{1}{2^n}\sum_{s\in\{-,+\}^n} I_2(W^s) \leq I_2(W), \tag{3}$$

$$\frac{1}{2^n}\sum_{s\in\{-,+\}^n} I(W^s) = I(W). \tag{4}$$

While (4) *shows that polarization preserves the symmetric sum-capacity,* (2) *and* (3) *show that polarization may result into a loss in the capacity region.*

Similarly, for the m-user case, we have

$$\frac{1}{2^n}\sum_{s\in\{-,+\}^n} I_S(W^s) \leq I_S(W),\ \forall S \subsetneq \{1,\dots,m\}.$$

Definition 3. *Let $S \subset \{1,\dots,m\}$. We say that polarization* $*$-preserves *I_S for W if for all $n \geq 0$ we have:*

$$\frac{1}{2^n}\sum_{s\in\{-,+\}^n} I_S(W^s) = I_S(W).$$

If polarization $*$-preserves I_S for every $S \subset \{1,\dots,m\}$, we say that polarization $*$-preserves *the symmetric capacity region for W.*

Remark 2. *If polarization $*$-preserves the symmetric capacity for W, then the whole symmetric capacity region can be achieved by polar codes.*

Section III provides a characterization of two-user MACs whose I_1 are $*$-preserved by polarization. Section IV generalizes the results of section III and provides a characterization of m-user MACs whose I_S are $*$-preserved by polarization, where $S \subsetneq \{1, \ldots, m\}$. This yields a complete characterization of the MACs with $*$-preservable symmetric capacity regions.

B. Discrete Fourier Transform on finite Abelian Groups

A tool that we are going to need for the analysis of the polarization process is the discrete Fourier transform (DFT) on finite Abelian groups. The DFT on finite Abelian groups can be defined based on the usual multidimensional DFT.

Definition 4. *(Multidimensional DFT) The m-dimensional discrete Fourier transform of a mapping $f : \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m} \to \mathbb{C}$ is the mapping $\hat{f} : \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m} \to \mathbb{C}$ defined as:*

$$\hat{f}(\hat{x}_1, \ldots, \hat{x}_m) = \sum_{x_1 \in \mathbb{Z}_{N_1}, \ldots, x_m \in \mathbb{Z}_{N_m}} f(x_1, \ldots, x_m) e^{-j\frac{2\pi \hat{x}_1 x_1}{N_1} \ldots - j\frac{2\pi \hat{x}_m x_m}{N_m}}.$$

Notation 5. *For every $x = (x_1, \ldots, x_m) \in \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$ and every $\hat{x} = (\hat{x}_1, \ldots, \hat{x}_m) \in \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$ define $\langle \hat{x}, x \rangle \in \mathbb{R}$ as:*

$$\langle \hat{x}, x \rangle := \frac{\hat{x}_1 x_1}{N_1} + \ldots + \frac{\hat{x}_m x_m}{N_m} \in \mathbb{R}.$$

Using this notation, the DFT can have a compact formula:

$$\hat{f}(\hat{x}) = \sum_{x \, \in \, \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}} f(x) e^{-j2\pi \langle \hat{x}, x \rangle}.$$

It is known that every finite Abelian group is isomorphic to the direct product of cyclic groups, i.e., if $(G, +)$ is a finite Abelian group then there exist m integers $N_1, \ldots, N_m > 0$ such that G is isomorphic to $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$. This allows us to define a DFT on G using the multidimensional DFT on $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$:

Definition 5. *Let $(G, +)$ be a finite Abelian group which is isomorphic to $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$. Fix an isomorphism between G and $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$. The discrete Fourier transform of a mapping $f : G \to \mathbb{C}$ is the mapping $\hat{f} : G \to \mathbb{C}$ defined as:*

$$\hat{f}(\hat{x}) = \sum_{x \in G} f(x) e^{-j2\pi \langle \hat{x}, x \rangle},$$

where $\langle \hat{x}, x \rangle$ is computed by identifying $\hat{x}$ and x with their respective images in $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$ by the fixed isomorphism.

In the following two propositions, we recall well known properties of DFT.

Proposition 1. *The inverse DFT is given by the following formula:*

$$f(x) = \frac{1}{|G|} \sum_{\hat{x} \in G} \hat{f}(\hat{x}) e^{j2\pi \langle \hat{x}, x \rangle},$$

where $\langle \hat{x}, x \rangle$ is computed by identifying $\hat{x}$ and x with their respective images in $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$ by the fixed isomorphism.

Remark 3. *The DFT on G as defined in this paper depends on the fixed isomorphism between G and $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_m}$. If the DFT is computed using a fixed isomorphism, the inverse DFT must be computed using the same isomorphism in order to have consistent computations.*

It is possible to define the DFT on finite Abelian groups without the need to fix any isomorphism, but this requires the character theory of finite Abelian groups.

Definition 6. *The convolution of two mappings $f : G \to \mathbb{C}$ and $g : G \to \mathbb{C}$ is the mapping $f * g : G \to \mathbb{C}$ defined as:*

$$(f * g)(x) = \sum_{x' \in G} f(x')g(x - x').$$

We will sometimes write $f(x) * g(x)$ to denote $(f * g)(x)$.

Proposition 2. *Let $f : G \to \mathbb{C}$ and $g : G \to \mathbb{C}$ be two mappings, we have:*

- $\widehat{(f * g)}(\hat{x}) = \hat{f}(\hat{x})\hat{g}(\hat{x})$.
- $\widehat{(f \cdot g)}(\hat{x}) = \frac{1}{|G|}(\hat{f} * \hat{g})(\hat{x})$.
- *If $f_a : G \to \mathbb{C}$ is defined as $f_a(x) = f(x - a)$, then $\hat{f}_a(\hat{x}) = \hat{f}(\hat{x})e^{j2\pi\langle \hat{x}, a\rangle}$.*
- *If $\tilde{f} : G \to \mathbb{C}$ is defined as $\tilde{f}(x) = f(-x)$, then $\hat{\tilde{f}}(\hat{x}) = \hat{f}(\hat{x})^*$.*

III. Two-user MACs with $*$-preserved I_1

In this section, we only consider two-user MACs $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$, where G_1 and G_2 are finite Abelian groups.

A. Preserved and $*^-$ Preserved

Definition 7. *Let $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$. We say that I_1 is* preserved *for W if and only if $I_1(W^-) + I_1(W^+) = 2I_1(W)$. We say that I_1 is $*^-$* preserved *for W if and only if I_1 is preserved for $W^{[n]^-}$ for every $n \geq 0$, where $[n]^- \in \{-,+\}^n$ is the sequence containing n minus signs (e.g., $[0]^- = \emptyset$, $[2]^- = (-,-)$).*

Lemma 1. *Polarization $*$-preserves I_1 for W if and only if I_1 is preserved for W^s for every $s \in \{-,+\}^*$. Similarly, polarization preserves I_1 for W if and only if I_1 is $*^-$ preserved for W^s for every $s \in \{-,+\}^*$.*

Proof: Polarization $*$-preserves I_1 for W if and only if

$$\begin{aligned}
\forall n \geq 0,\ I_1(W) = \frac{1}{2^n}\sum_{s\in\{-,+\}^n} I_1(W^s) \quad &\Leftrightarrow \quad \forall n \geq 0,\ \frac{1}{2^n}\sum_{s\in\{-,+\}^n} I_1(W^s) = \frac{1}{2^{n+1}}\sum_{s'\in\{-,+\}^{n+1}} I_1(W^{s'}) \\
&\Leftrightarrow \quad \forall n \geq 0,\ \sum_{s\in\{-,+\}^n} 2I_1(W^s) = \sum_{s\in\{-,+\}^n} (I_1(W^{(s,-)}) + I_1(W^{(s,+)})) \\
&\Leftrightarrow \quad \forall n \geq 0,\ \sum_{s\in\{-,+\}^n} \big(2I_1(W^s) - I_1(W^{(s,-)}) - I_1(W^{(s,+)})\big) = 0.
\end{aligned}$$

But since $2I_1(W^s) - I_1(W^{(s,-)}) - I_1(W^{(s,+)}) \geq 0$, we conclude that polarization $*$-preserves I_1 for W if and only if $\forall n \geq 0, \forall s \in \{-,+\}^n,\ I_1(W^{(s,-)}) + I_1(W^{(s,+)}) = 2I_1(W^s)$. In other words, polarization $*$-preserves I_1 for W if and only if I_1 is preserved for W^s for every $s \in \{-,+\}^*$. Moreover, we have

$$\begin{aligned}
\forall s \in \{-,+\}^*,\ I_1 \text{ is preserved for } W^s \quad &\Leftrightarrow \forall s \in \{-,+\}^*, \forall n \geq 0,\ I_1 \text{ is preserved for } W^{(s,[n]^-)} \\
&\Leftrightarrow \forall s \in \{-,+\}^*, I_1 \text{ is } *^- \text{ preserved for } W^s.
\end{aligned}$$

■

B. Necessary condition

According to (1), I_1 is preserved for W if and only if $I(U_1;V_2|Z_1Z_2V_1)=0$, which means that for every $z_1,z_2\in\mathcal{Z}$ and every $v_1,v_2\in G_2$, if $\mathbb{P}_{V_2,Z_1,Z_2,V_1}(v_2,z_1,z_2,v_1)>0$ then $\mathbb{P}_{U_1|V_2,Z_1,Z_2,V_1}(u_1|v_2,z_1,z_2,v_1)$ does not depend on v_2.

In order to study this condition, we should keep track of the values of $z_1,z_2\in\mathcal{Z}$ and $v_1,v_2\in G_2$ for which $\mathbb{P}_{V_2,Z_1,Z_2,V_1}(v_2,z_1,z_2,v_1)>0$. But $\mathbb{P}_{V_2,Z_1,Z_2,V_1}(v_2,z_1,z_2,v_1)=\mathbb{P}_{Y_1,Z_1}(v_1+v_2,z_1)\mathbb{P}_{Y_2,Z_2}(v_2,z_2)$, so it is sufficient to keep track of the pairs $(y,z)\in G_2\times\mathcal{Z}$ satisfying $\mathbb{P}_{Y,Z}(y,z)>0$:

Definition 8. *Let $W:G_1\times G_2\longrightarrow\mathcal{Z}$ and let $(X,Y)\xrightarrow{W}Z$. Define the following:*

- *For every $z\in\mathcal{Z}$, let $\mathrm{Y}^z(W)=\{y\in G_2:\ \mathbb{P}_{Y,Z}(y,z)>0\}$.*
- $\mathrm{YZ}(W)=\{(y,z):\ z\in\mathcal{Z},y\in\mathrm{Y}^z(W)\}$.
- *For every $(y,z)\in\mathrm{YZ}(W)$, define $p_{y,z,W}:G_1\to[0,1]$ as $p_{y,z,W}(x)=\mathbb{P}_{X|Y,Z}(x|y,z)$.*

In the rest of this section, we consider a fixed two-user MAC $W:G_1\times G_2\longrightarrow\mathcal{Z}$. For the sake of simplicity, we write $p_{y,z}(x)$ to denote $p_{y,z,W}(x)$.

The following lemma gives a characterization of two user MACs with preserved I_1 in terms of the Fourier transform of the distributions $p_{y,z}$.

Lemma 2. *I_1 is preserved for W if and only if for every $y_1,y_2,y_1',y_2'\in G_2$ and every $z_1,z_2\in\mathcal{Z}$ satisfying*

- $y_1-y_2=y_1'-y_2'$,
- $y_1,y_1'\in\mathrm{Y}^{z_1}(W)$ *and* $y_2,y_2'\in\mathrm{Y}^{z_2}(W)$,

we have

$$\hat{p}_{y_1,z_1}(\hat{x})\cdot\hat{p}_{y_2,z_2}(\hat{x})^*=\hat{p}_{y_1',z_1}(\hat{x})\cdot\hat{p}_{y_2',z_2}(\hat{x})^*,\ \ \forall\hat{x}\in G_1.$$

Proof: Let $U_1,U_2,V_1,V_2,X_1,X_2,Y_1,Y_2,Z_1,Z_2$ be as in Remark 1. We know that I_1 is preserved for W if and only if $I(U_1;V_2|Z_1Z_2V_1)=0$, which is equivalent to say that U_1 is independent of V_2 conditionally on (Z_1,Z_2,V_1).

In other words, for any fixed $(z_1,z_2,v_1)\in\mathcal{Z}\times\mathcal{Z}\times G_2$ satisfying $\mathbb{P}_{Z_1,Z_2,V_1}(z_1,z_2,v_1)>0$, if $v_2,v_2'\in G_2$ satisfy $\mathbb{P}_{V_2|Z_1,Z_2,V_1}(v_2|z_1,z_2,v_1)>0$ and $\mathbb{P}_{V_2|Z_1,Z_2,V_1}(v_2'|z_1,z_2,v_1)>0$, then we have

$$\forall u_1\in G_1,\ \mathbb{P}_{U_1|V_2,Z_1,Z_2,V_1}(u_1|v_2,z_1,z_2,v_1)=\mathbb{P}_{U_1|V_2,Z_1,Z_2,V_1}(u_1|v_2',z_1,z_2,v_1),$$

This condition is equivalent to say that for every $z_1,z_2\in\mathcal{Z}$ and every $v_1,v_2,v_2'\in G_2$ satisfying $\mathbb{P}_{Z_1,Z_2,Y_1,Y_2}(z_1,z_2,v_1+v_2,v_2)>0$ and $\mathbb{P}_{Z_1,Z_2,Y_1,Y_2}(z_1,z_2,v_1+v_2',v_2')>0$ we have

$$\forall u_1\in G_1,\mathbb{P}_{X_1-X_2|Z_1,Z_2,Y_1,Y_2}(u_1|z_1,z_2,v_1+v_2,v_2)=\mathbb{P}_{X_1-X_2|Z_1,Z_2,Y_1,Y_2}(u_1|z_1,z_2,v_1+v_2',v_2').$$

By denoting v_1+v_2,v_2,v_1+v_2' and v_2' as y_1,y_2,y_1' and y_2' respectively (so that $y_1-y_2=y_1'-y_2'=v_1$), we can deduce that I_1 is preserved for W if and only if for every $y_1,y_2,y_1',y_2'\in G_2$ and every $z_1,z_2\in\mathcal{Z}$ satisfying $y_1-y_2=y_1'-y_2'$, $\mathbb{P}_{Z_1,Z_2,Y_1,Y_2}(z_1,z_2,y_1,y_2)>0$ and $\mathbb{P}_{Z_1,Z_2,Y_1,Y_2}(z_1,z_2,y_1',y_2')>0$ (i.e., $y_1,y_1'\in\mathrm{Y}^{z_1}(W)$ and $y_2,y_2'\in\mathrm{Y}^{z_2}(W)$), we have

$$\forall u_1\in G_1,\mathbb{P}_{X_1-X_2|Z_1,Z_2,Y_1,Y_2}(u_1|z_1,z_2,y_1,y_2)=\mathbb{P}_{X_1-X_2|Z_1,Z_2,Y_1,Y_2}(u_1|z_1,z_2,y_1',y_2').$$

On the other hand, we have:

$$\begin{aligned}\mathbb{P}_{X_1-X_2|Z_1,Z_2,Y_1,Y_2}(u_1|z_1,z_2,y_1,y_2)&=\sum_{u_2\in G_1}\mathbb{P}_{X_1|Z_1,Y_1}(u_1+u_2|z_1,y_1)\mathbb{P}_{X_2|Z_2,Y_2}(u_2|z_2,y_2)\\&=\sum_{u_2\in G_1}p_{y_1,z_1}(u_1+u_2)p_{y_2,z_2}(u_2)=(p_{y_1,z_1}*\tilde{p}_{y_2,z_2})(u_1),\end{aligned}$$

where $\tilde{p}_{y_2,z_2}(x)=p_{y_2,z_2}(-x)$. Similarly $\mathbb{P}_{X_1-X_2|Z_1,Z_2,Y_1,Y_2}(u_1|z_1,z_2,y_1',y_2')=(p_{y_1',z_1}*\tilde{p}_{y_2',z_2})(u_1)$. Therefore, for every $u_1\in G_1$, we have

$$(p_{y_1,z_1}*\tilde{p}_{y_2,z_2})(u_1)=(p_{y_1',z_1}*\tilde{p}_{y_2',z_2})(u_1),$$

which is equivalent to $\hat{p}_{y_1,z_1}(\hat{u}_1)\cdot\hat{p}_{y_2,z_2}(\hat{u}_1)^* = \hat{p}_{y_1',z_1}(\hat{u}_1)\cdot\hat{p}_{y_2',z_2}(\hat{u}_1)^*$ for every $\hat{u}_1 \in G_1$. ■

Lemma 3. *Suppose that I_1 is $*^-$ preserved for W. Fix $n > 0$ and let $(U_i, V_i)_{0\le i<2^n}$ be a sequence of random pairs which are independent and uniformly distributed in $G_1 \times G_2$. Let*

$$F = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Define $X_0^{2^n-1} = F^{\otimes n}\cdot U_0^{2^n-1}$ and $Y_0^{2^n-1} = F^{\otimes n}\cdot V_0^{2^n-1}$, and for each $0 \le i < 2^n$ let $(X_i, Y_i) \xrightarrow{W} Z_i$. We have the following:

- *The MAC $(U_0, V_0) \longrightarrow Z_0^{2^n-1}$ is equivalent to $W^{[n]^-}$.*
- *$I(U_0; V_1^{2^n-1}|Z_0^{2^n-1}V_0) = 0$.*

Proof: We will show the lemma by induction on $n > 0$. For $n = 1$, the claim follows from Remark 1 and from the fact that I_1 is preserved for W if and only if $I(U_0; V_1|Z_0Z_1V_0) = 0$ (see (1)).

Now let $n > 1$ and suppose that the claim is true for $n-1$. Let $N = 2^{n-1}$. We have $X_0^{2^n-1} = F^{\otimes n}\cdot U_0^{2^n-1}$ and $Y_0^{2^n-1} = F^{\otimes n}\cdot V_0^{2^n-1}$, i.e., $X_0^{2N-1} = F^{\otimes n}\cdot U_0^{2N-1}$ and $Y_0^{2N-1} = F^{\otimes n}\cdot V_0^{2N-1}$. Therefore, we have:

- $X_0^{N-1} = F^{\otimes(n-1)}\cdot(U_0^{N-1} + U_N^{2N-1})$ and $X_N^{2N-1} = F^{\otimes(n-1)}\cdot U_N^{2N-1}$.
- $Y_0^{N-1} = F^{\otimes(n-1)}\cdot(V_0^{N-1} + V_N^{2N-1})$ and $Y_N^{2N-1} = F^{\otimes(n-1)}\cdot V_N^{2N-1}$.

This means that $(U_0^{N-1}+U_N^{2N-1}, V_0^{N-1}+V_N^{2N-1}, Z_0^{N-1})$ and $(U_N^{2N-1}, V_N^{2N-1}, Z_N^{2N-1})$ satisfy the conditions of the induction hypothesis. Therefore,

- $I(U_0 + U_N; V_1^{N-1} + V_{N+1}^{2N-1}|Z_0^{N-1}, V_0 + V_N) = 0$.
- $I(U_N; V_{N+1}^{2N-1}|Z_N^{2N-1}, V_N) = 0$.

Moreover, since $(U_0^{N-1} + U_N^{2N-1}, V_0^{N-1} + V_N^{2N-1}, Z_0^{N-1})$ is independent of $(U_N^{2N-1}, V_N^{2N-1}, Z_N^{2N-1})$, we can combine the above two equations to get:

$$I(U_0 + U_N, U_N; V_1^{N-1} + V_{N+1}^{2N-1}, V_{N+1}^{2N-1}|Z_0^{2N-1}, V_0 + V_N, V_N) = 0,$$

which can be rewritten as

$$I(U_0U_N; V_1^{N-1}V_{N+1}^{2N-1}|Z_0^{2N-1}V_0V_N) = 0. \tag{5}$$

On the other hand, it also follow from the induction hypothesis that:

- The MAC $(U_0 + U_N, V_0 + V_N) \longrightarrow Z_0^{N-1}$ is equivalent to $W^{[n-1]^-}$.
- The MAC $(U_N, V_N) \longrightarrow Z_N^{2N-1}$ is equivalent to $W^{[n-1]^-}$.

This implies that the MAC $(U_0, V_0) \longrightarrow Z_0^{2N-1}$ is equivalent to $W^{[n]^-}$. Now since I_1 is $*^-$ preserved for W, I_1 must be preserved for $W^{[n-1]^-}$. Therefore,

$$I(U_0; V_N|Z_0^{2N-1}V_0) = I(U_0; V_N|Z_0^{N-1}Z_N^{2N-1}V_0) \overset{(a)}{=} 0, \tag{6}$$

where (a) follows from (1). We conclude that:

$$\begin{aligned} I(U_0; V_1^{2N-1}|Z_0^{2N-1}V_0) &= I(U_0; V_N|Z_0^{2N-1}V_0) + I(U_0; V_1^{N-1}V_{N+1}^{2N-1}|Z_0^{2N-1}V_0V_N) \\ &\le I(U_0; V_N|Z_0^{2N-1}V_0) + I(U_0U_N; V_1^{N-1}V_{N+1}^{2N-1}|Z_0^{2N-1}V_0V_N) \overset{(b)}{=} 0, \end{aligned}$$

where (b) follows from (5) and (6). ■

Lemma 4. *For every $n > 0$, if $X_0^{2^n-1} = F^{\otimes n}U_0^{2^n-1}$, then $U_0 = \sum_{i=0}^{2^n-1}(-1)^{|i|_b}X_i$, where $|i|_b$ is the number of ones in the binary expansion of i.*

Proof: We will show the lemma by induction on $n > 0$. For $n = 1$, the fact that $X_0^1 = F^{\otimes 1}\cdot U_0^1 = F\cdot U_0^1$ implies that $X_0 = U_0 + U_1$ and $X_1 = U_1$. Therefore $U_0 = X_0 - X_1 = \sum_{i=0}^{1}(-1)^{|i|_b}X_i$.

Now let $n > 1$ and suppose that the claim is true for $n-1$. Let $N = 2^{n-1}$. The fact that $X_0^{2N-1} = F^{\otimes n} \cdot U_0^{2N-1}$ implies that:

- $X_0^{N-1} = F^{\otimes(n-1)} \cdot (U_0^{N-1} + U_N^{2N-1})$.
- $X_N^{2N-1} = F^{\otimes(n-1)} \cdot U_N^{2N-1}$.

We can apply the induction hypothesis to get:

- $U_0 + U_N = \sum_{i=0}^{N-1} (-1)^{|i|_b} X_i$.
- $U_N = \sum_{i=0}^{N-1} (-1)^{|i|_b} X_{i+N}$.

Therefore,

$$\begin{aligned} U_0 &= \sum_{i=0}^{N-1} (-1)^{|i|_b} X_i - \sum_{i=0}^{N-1} (-1)^{|i|_b} X_{i+N} = \sum_{i=0}^{N-1} (-1)^{|i|_b} X_i + \sum_{i=0}^{N-1} (-1)^{1+|i|_b} X_{i+N} \\ &= \sum_{i=0}^{N-1} (-1)^{|i|_b} X_i + \sum_{i=N}^{2N-1} (-1)^{1+|i-N|_b} X_i \overset{(a)}{=} \sum_{i=0}^{N-1} (-1)^{|i|_b} X_i + \sum_{i=N}^{2N-1} (-1)^{|i|_b} X_i \\ &= \sum_{i=0}^{2N-1} (-1)^{|i|_b} X_i, \end{aligned}$$

where (a) follows from the fact that for $2^n = N \leq i < 2N = 2^{n+1}$, we have $|i-N|_b = |i-2^n|_b = |i|_b - 1$. ■

Lemma 5. *If I_1 is $*^-$ preserved for W, then for every $n > 0$, every $y_1, \ldots, y_{2^n}, y'_1, \ldots, y'_{2^n} \in G_2$ and every $z_1, \ldots, z_{2^n} \in \mathcal{Z}$ satisfying*

- $\sum_{i=1}^{2^n} y_i = \sum_{i=1}^{2^n} y'_i$,
- $y_1 \in \mathrm{Y}^{z_1}(W), \ldots, y_{2^n} \in \mathrm{Y}^{z_{2^n}}(W)$, *and*
- $y'_1 \in \mathrm{Y}^{z_1}(W), \ldots y'_{2^n} \in \mathrm{Y}^{z_{2^n}}(W)$,

we have

$$\prod_{i=1}^{2^n} \hat{p}_{y_i,z_i}(\hat{x}) = \prod_{i=1}^{2^n} \hat{p}_{y'_i,z_i}(\hat{x}), \quad \forall \hat{x} \in G_1.$$

Proof: Fix $\hat{x} \in G_1$. If $\hat{p}_{y,z}(\hat{x}) = 0$ for every $(y,z) \in \mathrm{YZ}(W)$, then we clearly have

$$\prod_{i=1}^{2^n} \hat{p}_{y_i,z_i}(\hat{x}) = \prod_{i=1}^{2^n} \hat{p}_{y'_i,z_i}(\hat{x}).$$

Therefore, we can assume without loss of generality that there exists $(y,z) \in \mathrm{YZ}(W)$ which satisfies $\hat{p}_{y,z}(\hat{x}) \neq 0$.

Let $U_0^{2^{n+1}-1}$, $V_0^{2^{n+1}-1}$, $X_0^{2^{n+1}-1}$, $Y_0^{2^{n+1}-1}$ and $Z_0^{2^{n+1}-1}$ be as in Lemma 3 and let $N = 2^{n+1}$ so that we have

$$I(U_0; V_1^{N-1} | Z_0^{N-1} V_0) = 0. \tag{7}$$

Since $X_0^{N-1} = F^{\otimes(n+1)} \cdot U_0^{N-1}$ and $Y_0^{N-1} = F^{\otimes(n+1)} \cdot V_0^{N-1}$, Lemma 4 implies that

$$U_0 = \sum_{i=0}^{N-1} (-1)^{|i|_b} X_i \text{ and } V_0 = \sum_{i=0}^{N-1} (-1)^{|i|_b} Y_i. \tag{8}$$

Notice that $\left|\left\{0 \le i < N = 2^{n+1} : \ |i|_b \equiv 0 \bmod 2\right\}\right| = \left|\left\{0 \le i < N = 2^{n+1} : \ |i|_b \equiv 1 \bmod 2\right\}\right| = 2^n$. Let $k_1, \ldots, k_{2^n}$ be the elements of $\left\{0 \le i < N : \ |i|_b \equiv 0 \bmod 2\right\}$ and let $l_1, \ldots, l_{2^n}$ be the elements of $\left\{0 \le i < N : \ |i|_b \equiv 1 \bmod 2\right\}$.

Define $(\tilde{y}_i, \tilde{y}'_i, \tilde{z}_i)_{0 \le i < N}$ as follows:

- For every $1 \le i \le 2^n$, let $\tilde{y}_{k_i} = y_i$, $\tilde{y}'_{k_i} = y'_i$ and $\tilde{z}_{k_i} = z_i$.
- For every $1 \le i \le 2^n$, let $\tilde{y}_{l_i} = \tilde{y}'_{l_i} = y$ and $\tilde{z}_{l_i} = z$.

Now let $\tilde{v}_0^{N-1} = (F^{\otimes(n+1)})^{-1} \cdot \tilde{y}_0^{N-1}$ and $\tilde{v}_0'^{N-1} = (F^{\otimes(n+1)})^{-1} \cdot \tilde{y}_0'^{N-1}$. We have

$$\begin{aligned}\tilde{v}_0 &\overset{(a)}{=} \sum_{i=0}^{N-1} (-1)^{|i|_b} \tilde{y}_i = \sum_{i=1}^{2^n} (\tilde{y}_{k_i} - \tilde{y}_{l_i}) = \sum_{i=1}^{2^n} y_i - 2^n y \\ &\overset{(b)}{=} \sum_{i=1}^{2^n} y'_i - 2^n y = \sum_{i=1}^{2^n} (\tilde{y}'_{k_i} - \tilde{y}'_{l_i}) = \sum_{i=0}^{N-1} (-1)^{|i|_b} \tilde{y}'_i \overset{(c)}{=} \tilde{v}'_0,\end{aligned}$$

where (a) and (c) follow from Lemma 4. (b) follows from the fact that $\sum_{i=1}^{2^n} y_i = \sum_{i=1}^{2^n} y'_i$. Therefore,

$$(\tilde{v}_0, \tilde{z}_0^{N-1}) = (\tilde{v}'_0, \tilde{z}_0^{N-1}). \tag{9}$$

On the other hand, since $\tilde{y}_i \in \mathrm{Y}^{\tilde{z}_i}(W)$ for every $0 \le i < N$, we have

$$\begin{aligned}\mathbb{P}_{V_0, V_1^{N-1}, Z_0^{N-1}}(\tilde{v}_0, \tilde{v}_1^{N-1}, \tilde{z}_0^{N-1}) &= \mathbb{P}_{V_0^{N-1}, Z_0^{N-1}}(\tilde{v}_0^{N-1}, \tilde{z}_0^{N-1}) \\ &= \mathbb{P}_{Y_0^{N-1}, Z_0^{N-1}}(\tilde{y}_0^{N-1}, \tilde{z}_0^{N-1}) > 0.\end{aligned} \tag{10}$$

Similarly, since $\tilde{y}'_i \in \mathrm{Y}^{\tilde{z}_i}(W)$ for every $0 \le i < N$, we have

$$\begin{aligned}\mathbb{P}_{V_0, V_1^{N-1}, Z_0^{N-1}}(\tilde{v}'_0, \tilde{v}_1'^{N-1}, \tilde{z}_0^{N-1}) &= \mathbb{P}_{V_0^{N-1}, Z_0^{N-1}}\left(\tilde{v}_0'^{N-1}, \tilde{z}_0^{N-1}\right) \\ &= \mathbb{P}_{Y_0^{N-1}, Z_0^{N-1}}(\tilde{y}_0'^{N-1}, \tilde{z}_0^{N-1}) > 0.\end{aligned} \tag{11}$$

(7) implies that conditioned on (V_0, Z_0^{N-1}), U_0 is independent of V_1^{N-1}. (9), (10) and (11) now imply that for every $u_0 \in G_1$, we have:

$$\begin{aligned}&\mathbb{P}_{U_0|V_1^{N-1}, V_0, Z_0^{N-1}}(u_0|\tilde{v}_1^{N-1}, \tilde{v}_0, \tilde{z}_0^{N-1}) = \mathbb{P}_{U_0|V_1^{N-1}, V_0, Z_0^{N-1}}(u_0|\tilde{v}_1'^{N-1}, \tilde{v}'_0, \tilde{z}_0^{N-1}) \\ &\quad\Leftrightarrow\ \mathbb{P}_{U_0|V_0^{N-1}, Z_0^{N-1}}(u_0|\tilde{v}_0^{N-1}, \tilde{z}_0^{N-1}) = \mathbb{P}_{U_0|V_0^{N-1}, Z_0^{N-1}}(u_0|\tilde{v}_0'^{N-1}, \tilde{z}_0^{N-1}) \\ &\quad\Leftrightarrow\ \mathbb{P}_{U_0|Y_0^{N-1}, Z_0^{N-1}}(u_0|\tilde{y}_0^{N-1}, \tilde{z}_0^{N-1}) = \mathbb{P}_{U_0|Y_0^{N-1}, Z_0^{N-1}}(u_0|\tilde{y}_0'^{N-1}, \tilde{z}_0^{N-1}) \\ &\quad\overset{(a)}{\Leftrightarrow} \sum_{\substack{\tilde{x}_0^{N-1} \in G_1^N: \\ \sum_{i=0}^{N-1} (-1)^{|i|_b} \tilde{x}_i = u_0}} \prod_{i=0}^{N-1} \mathbb{P}_{X_i|Y_i, Z_1}(\tilde{x}_i|\tilde{y}_i, \tilde{z}_i) = \sum_{\substack{\tilde{x}_0^{N-1} \in G_1^N: \\ \sum_{i=0}^{N-1} (-1)^{|i|_b} \tilde{x}_i = u_0}} \prod_{i=0}^{N-1} \mathbb{P}_{X_i|Y_i, Z_1}(\tilde{x}_i|\tilde{y}'_i, \tilde{z}_i) \\ &\quad\overset{(b)}{\Leftrightarrow} \sum_{\substack{x_1^N \in G_1^N: \\ \sum_{i=1}^{2^n} x_i - \sum_{i=2^n+1}^{N} x_i = u_0}} \prod_{i=1}^{2^n} p_{y_i, z_i}(x_i) \prod_{i=2^n+1}^{N} p_{y,z}(x_i) \\ &\qquad = \sum_{\substack{x_1^N \in G_1^N: \\ \sum_{i=1}^{2^n} x_i - \sum_{i=2^n+1}^{N} x_i = u_0}} \prod_{i=1}^{2^n} p_{y'_i, z_i}(x_i) \prod_{i=2^n+1}^{N} p_{y,z}(x_i),\end{aligned} \tag{12}$$

where (a) follows from (8) and (b) follows from the following change of variables:

$$x_i = \begin{cases} \tilde{x}_{k_i} & \text{if } 1 \le i \le 2^n, \\ \tilde{x}_{l_{i-2^n}} & \text{if } 2^n \le i \le 2^{n+1} = N. \end{cases}$$

Now notice that the left hand side of (12) is the convolution of $(p_{y_i,z_i})_{1\le i\le 2^n}$ and 2^n copies of $\tilde{p}_{y,z}$ (where $\tilde{p}_{y,z}(x)=p_{y,z}(-x)$). Likewise, the right hand side of (12) is the convolution of $(p_{y'_i,z_i})_{1\le i\le 2^n}$ and 2^n copies of $\tilde{p}_{y,z}$. By applying the DFT on (12), we get:

$$\prod_{i=1}^{2^n}\hat{p}_{y_i,z_i}(\hat{u}_1)\prod_{i=2^n+1}^{N}\hat{p}_{y,z}(\hat{u}_1)^*=\prod_{i=1}^{2^n}\hat{p}_{y'_i,z_i}(\hat{u}_1)\prod_{i=2^n+1}^{N}\hat{p}_{y,z}(\hat{u}_1)^*,\ \ \forall\hat{u}_1\in G_1.$$

In particular,

$$\prod_{i=1}^{2^n}\hat{p}_{y_i,z_i}(\hat{x})\prod_{i=2^n+1}^{N}\hat{p}_{y,z}(\hat{x})^*=\prod_{i=1}^{2^n}\hat{p}_{y'_i,z_i}(\hat{x})\prod_{i=2^n+1}^{N}\hat{p}_{y,z}(\hat{x})^*.$$

Now since $\hat{p}_{y,z}(\hat{x})\neq 0$, we conclude that

$$\prod_{i=1}^{2^n}\hat{p}_{y_i,z_i}(\hat{x})=\prod_{i=1}^{2^n}\hat{p}_{y'_i,z_i}(\hat{x})$$

■

Definition 9. *For every $z\in\mathcal{Z}$ define:*

$$\hat{\mathrm{X}}^z(W):=\big\{\hat{x}\in G_1:\exists y\in\mathrm{Y}^z(W),\hat{p}_{y,z}(\hat{x})\neq 0\big\}.$$

Let

$$\hat{\mathrm{X}}\mathrm{Z}(W):=\big\{(\hat{x},z):\ z\in\mathcal{Z},\ \hat{x}\in\hat{\mathrm{X}}^z(W)\big\},$$
$$\hat{\mathrm{X}}(W):=\textstyle\bigcup_{z\in\mathcal{Z}}\hat{\mathrm{X}}^z(W).$$

Lemma 6. *If I_1 is $*^-$ preserved for W then for every $\hat{x}\in\hat{\mathrm{X}}^z(W)$, we have:*

- *$\hat{p}_{y,z}(\hat{x})\neq 0$ for all $y\in\mathrm{Y}^z(W)$.*
- *$\dfrac{\hat{p}_{y,z}(\hat{x})}{\hat{p}_{y',z}(\hat{x})}\in\mathbb{T}$ for every $y,y'\in\mathrm{Y}^z(W)$, where $\mathbb{T}=\{\omega\in\mathbb{C}:\ |\omega|=1\}$.*

Proof: If $\hat{x}\in\hat{\mathrm{X}}^z(W)$, there exists $y'\in\mathrm{Y}^z(W)$ satisfying $\hat{p}_{y',z}(\hat{x})\neq 0$. Fix $y\in\mathrm{Y}^z(W)$ and let $a>0$ be the order of $y-y'$ (i.e., $a(y-y')=0_{G_2}$, where 0_{G_2} is the neutral element of G_2). Let $n>0$ be such that $a<2^n$ and define the two sequences $(y_i)_{1\le i\le 2^n}$ and $(y'_i)_{1\le i\le 2^n}$ as follows:

- If $i\le a$, $y_i=y$ and $y'_i=y'$.
- If $i>a$, $y_i=y'_i=y'$.

Since $a(y-y')=0_{G_2}$, we have $ay=ay'$ and so $\displaystyle\sum_{i=1}^{2^n}y_i=ay+(2^n-a)y'=ay'+(2^n-a)y'=\sum_{i=1}^{2^n}y'_i$.
By applying Lemma 5, we get

$$\begin{aligned}\big(\hat{p}_{y,z}(\hat{x})\big)^a\big(\hat{p}_{y',z}(\hat{x})\big)^{2^n-a}&=\prod_{i=1}^{2^n}\hat{p}_{y_i,z}(\hat{x})=\prod_{i=1}^{2^n}\hat{p}_{y'_i,z}(\hat{x})\\&=\big(\hat{p}_{y',z}(\hat{x})\big)^{2^n}\neq 0.\end{aligned}$$

Therefore, $\hat{p}_{y,z}(\hat{x})\neq 0$. Moreover,

$$\Big(\frac{\hat{p}_{y,z}(\hat{x})}{\hat{p}_{y',z}(\hat{x})}\Big)^a=1,$$

which means that $\dfrac{\hat{p}_{y,z}(\hat{x})}{\hat{p}_{y',z}(\hat{x})}$ is a root of unity, i.e., $\dfrac{\hat{p}_{y,z}(\hat{x})}{\hat{p}_{y',z}(\hat{x})}\in\mathbb{T}$. ■

Definition 10. *Define the following:*

- *For every* $(\hat{x},z)\in\hat{\mathrm{X}}\mathrm{Z}(W)$, *let* $\mathrm{Y}^{\hat{x},z}(W):=\big\{y\in\mathrm{Y}^{z}(W):\ \hat{p}_{y,z}(\hat{x})\neq 0\big\}$.
- *For every* $(\hat{x},z)\in\hat{\mathrm{X}}\mathrm{Z}(W)$, *let* $\Delta\mathrm{Y}^{\hat{x},z}(W):=\big\{y_1-y_2:\ y_1,y_2\in\mathrm{Y}^{\hat{x},z}(W)\big\}$.
- *For every* $z\in\mathcal{Z}$, *let* $\mathrm{D}^{z}(W):=\big\{(\hat{x},y):\ \hat{x}\in\hat{\mathrm{X}}^{z}(W),\ y\in\Delta\mathrm{Y}^{\hat{x},z}(W)\big\}$.
- $\mathrm{D}(W):=\bigcup_{z\in\mathcal{Z}}\mathrm{D}^{z}(W)$.

Lemma 7. *If* I_1 *is* $*^{-}$ *preserved for* W, *there exists a unique mapping* $\hat{f}_W:\mathrm{D}(W)\to\mathbb{T}$ *such that for every* $(\hat{x},z)\in\hat{\mathrm{X}}\mathrm{Z}(W)$ *and every* $y_1,y_2\in\mathrm{Y}^{z}(W)$, *we have*

$$\hat{p}_{y_1,z}(\hat{x})=\hat{f}_W(\hat{x},y_1-y_2)\cdot\hat{p}_{y_2,z}(\hat{x}).$$

Proof: Let $(\hat{x},y)\in\mathrm{D}(W)$. Let z be such that $(\hat{x},y)\in\mathrm{D}^{z}(W)$, and let $y_1,y_2\in\mathrm{Y}^{\hat{x},z}(W)$ be such that $y_1-y_2=y$. Suppose there exist $z'\in\mathcal{Z}$ and $y_1',y_2'\in\mathrm{Y}^{z'}(W)$ which satisfy $\hat{x}\in\hat{\mathrm{X}}^{z'}(W)$ and $y_1'-y_2'=y=y_1-y_2$. Lemma 6 implies that $p_{y_1',z'}(\hat{x})\neq 0$ and $p_{y_2',z'}(\hat{x})\neq 0$. Lemma 5 shows that

$$p_{y_1,z}(\hat{x})\cdot p_{y_2',z'}(\hat{x})=p_{y_2,z}(\hat{x})\cdot p_{y_1',z'}(\hat{x}).$$

Therefore, $\dfrac{p_{y_1,z}(\hat{x})}{p_{y_2,z}(\hat{x})}=\dfrac{p_{y_1',z'}(\hat{x})}{p_{y_2',z'}(\hat{x})}\overset{(a)}{\in}\mathbb{T}$, where (a) follows from Lemma 6. This shows that the value of $\dfrac{p_{y_1,z}(\hat{x})}{p_{y_2,z}(\hat{x})}\in\mathbb{T}$ depends only on $(\hat{x},y)$ and does not depend on the choice of z,y_1,y_2. We conclude that there exists a unique $\hat{f}_W(\hat{x},y)\in\mathbb{T}$ such that for every $z\in\mathcal{Z}$ and every $y_1,y_2\in\mathrm{Y}^{z}(W)$ satisfying $\hat{x}\in\hat{\mathrm{X}}^{z}(W)$ and $y_1-y_2=y$, we have

$$\hat{p}_{y_1,z}(\hat{x})=\hat{f}_W(\hat{x},y)\cdot\hat{p}_{y_2,z}(\hat{x}).$$

■

Lemma 8. *For every MAC* W, *we have:*

$$\mathrm{Y}^{(z_1,z_2)}(W^{-})=\big\{y_1-y_2:\ y_1\in\mathrm{Y}^{z_1}(W),y_2\in\mathrm{Y}^{z_2}(W)\big\}.$$

Proof: Let $U_1,U_2,V_1,V_2,X_1,X_2,Y_1,Y_2,Z_1,Z_2$ be as in Remark 1. For every $v_1\in G_2$ and every $z_1,z_2\in\mathcal{Z}$, we have:

$$\mathbb{P}_{V_1,Z_1,Z_2}(v_1,z_1,z_2)=\sum_{\substack{y_1,y_2\in G_2:\\ v_1=y_1-y_2}}\mathbb{P}_{Y_1,Y_2,Z_1,Z_2}(y_1,y_2,z_1,z_2)=\sum_{\substack{y_1,y_2\in G_2:\\ v_1=y_1-y_2}}\mathbb{P}_{Y_1,Z_1}(y_1,z_1)\mathbb{P}_{Y_2,Z_2}(y_2,z_2).$$

Therefore, $v_1\in\mathrm{Y}^{(z_1,z_2)}(W^{-})$ if and only if there exist $y_1,y_2\in G_2$ such that $y_1\in\mathrm{Y}^{z_1}(W)$, $y_2\in\mathrm{Y}^{z_2}(W)$ and $v_1=y_1-y_2$. Hence,

$$\mathrm{Y}^{(z_1,z_2)}(W^{-})=\big\{y_1-y_2:\ y_1\in\mathrm{Y}^{z_1}(W),y_2\in\mathrm{Y}^{z_2}(W)\big\}.$$

■

Lemma 9. *For every* $z_1,z_2\in\mathcal{Z}$, *every* $v_1\in\mathrm{Y}^{(z_1,z_2)}(W^{-})$ *and every* $\hat{u}_1\in G_1$, *we have:*

$$\hat{p}_{v_1,z_1,z_2,W^{-}}(\hat{u}_1)=\sum_{\substack{v_2\in\mathrm{Y}^{z_2}(W):\\ v_1+v_2\in\mathrm{Y}^{z_1}(W)}}\frac{\mathbb{P}_{Y_1|Z_1}(v_1+v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1|z_1,z_2)}\hat{p}_{v_1+v_2,z_1}(\hat{u}_1)\cdot\hat{p}_{v_2,z_2}(\hat{u}_1)^{*}.\tag{13}$$

Proof: Let $U_1, U_2, V_1, V_2, X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be as in Remark 1. Fix $z_1, z_2 \in \mathcal{Z}$ and $v_1 \in \mathrm{Y}^{(z_1,z_2)}(W^-)$, and let $\beta = \mathbb{P}_{V_1|Z_1,Z_2}(v_1|z_1,z_2) > 0$. For every $u_1 \in G_1$, we have:

$$\begin{aligned}
p_{v_1,z_1,z_2,W^-}(u_1) &= \mathbb{P}_{U_1|V_1,Z_1,Z_2}(u_1|v_1,z_1,z_2) = \frac{1}{\beta}\mathbb{P}_{U_1,V_1|Z_1,Z_2}(u_1,v_1|z_1,z_2) \\
&= \frac{1}{\beta}\sum_{\substack{u_2\in G_1\\ v_2\in G_2}} \mathbb{P}_{U_1,U_2,V_1,V_2|Z_1,Z_2}(u_1,u_2,v_1,v_2|z_1,z_2) \\
&= \frac{1}{\beta}\sum_{\substack{u_2\in G_1\\ v_2\in G_2}} \mathbb{P}_{X_1,X_2,Y_1,Y_2|Z_1,Z_2}(u_1+u_2,u_2,v_1+v_2,v_2|z_1,z_2) \\
&= \frac{1}{\beta}\sum_{\substack{u_2\in G_1\\ v_2\in G_2}} \mathbb{P}_{X_1,Y_1|Z_1}(u_1+u_2,v_1+v_2|z_1)\mathbb{P}_{X_2,Y_2|Z_2}(u_2,v_2|z_2) \\
&= \frac{1}{\beta}\sum_{\substack{v_2\in \mathrm{Y}^{z_2}(W):\\ v_1+v_2\in \mathrm{Y}^{z_1}(W)}}\ \sum_{u_2\in G_1} \mathbb{P}_{X_1,Y_1|Z_1}(u_1+u_2,v_1+v_2|z_1)\mathbb{P}_{X_2,Y_2|Z_2}(u_2,v_2|z_2) \\
&= \frac{1}{\beta}\sum_{\substack{v_2\in \mathrm{Y}^{z_2}(W):\\ v_1+v_2\in \mathrm{Y}^{z_1}(W)}} \mathbb{P}_{Y_1|Z_1}(v_1+v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)\sum_{u_2\in G_1} p_{v_1+v_2,z_1}(u_1+u_2)p_{v_2,z_2}(u_2) \\
&= \frac{1}{\beta}\sum_{\substack{v_2\in \mathrm{Y}^{z_2}(W):\\ v_1+v_2\in \mathrm{Y}^{z_1}(W)}} \mathbb{P}_{Y_1|Z_1}(v_1+v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)(p_{v_1+v_2,z_1} * \tilde{p}_{v_2,z_2})(u_1),
\end{aligned}$$

where $\tilde{p}_{v_2,z_2}(x) = p_{v_2,x_2}(-x)$ for every $x \in G_1$. Therefore, for every $\hat{u}_1 \in G_1$, we have:

$$\hat{p}_{v_1,z_1,z_2,W^-}(\hat{u}_1) = \sum_{\substack{v_2\in \mathrm{Y}^{z_2}(W):\\ v_1+v_2\in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1+v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1|z_1,z_2)}\hat{p}_{v_1+v_2,z_1}(\hat{u}_1)\cdot\hat{p}_{v_2,z_2}(\hat{u}_1)^*.$$

■

Lemma 10. $\mathrm{D}(W^-) \subset \{(\hat{x}, y_1+y_2) :\ (\hat{x},y_1),(\hat{x},y_2) \in \mathrm{D}(W)\}$.

Proof: Let $U_1, U_2, V_1, V_2, X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be as in Remark 1. Let $(\hat{u}_1, v_1) \in \mathrm{D}(W^-)$. There exists $z^- = (z_1,z_2) \in \mathcal{Z}^-$ such that $(\hat{u}_1,v_1) \in \mathrm{D}^{z^-}(W^-)$. This implies the existence of $v_1', v_1'' \in \mathrm{Y}^{z^-}(W^-)$ such that $v_1 = v_1' - v_1''$, $\hat{p}_{v_1',z^-,W^-}(\hat{u}_1) \neq 0$ and $\hat{p}_{v_1'',z^-,W^-}(\hat{u}_1) \neq 0$. From (13), we have:

$$\hat{p}_{v_1',z^-,W^-}(\hat{u}_1) = \sum_{\substack{v_2'\in \mathrm{Y}^{z_2}(W):\\ v_1'+v_2'\in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1'+v_2'|z_1)\mathbb{P}_{Y_2|Z_2}(v_2'|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1'|z_1,z_2)}\hat{p}_{v_1'+v_2',z_1}(\hat{u}_1)\cdot\hat{p}_{v_2',z_2}(\hat{u}_1)^*. \tag{14}$$

Since $\hat{p}_{v_1',z^-,W^-}(\hat{u}_1) \neq 0$, the terms in the above sum cannot all be zero. Therefore, there exists $v_2' \in \mathrm{Y}^{z_2}(W)$ such that $v_1'+v_2' \in \mathrm{Y}^{z_1}(W)$, $\hat{p}_{v_1'+v_2',z_1}(\hat{u}_1) \neq 0$ and $\hat{p}_{v_2',z_2}(\hat{u}_1) \neq 0$. Similarly, since $\hat{p}_{v_1'',z^-,W^-}(\hat{u}_1) \neq 0$, there exists $v_2'' \in \mathrm{Y}^{z_2}(W)$ such that $v_1''+v_2'' \in \mathrm{Y}^{z_1}(W)$, $\hat{p}_{v_1''+v_2'',z_1}(\hat{u}_1) \neq 0$ and $\hat{p}_{v_2'',z_2}(\hat{u}_1) \neq 0$. We can now see that $(\hat{u}_1, v_1+v_2'-v_2'') = \big(\hat{u}_1, v_1'+v_2'-(v_1''+v_2'')\big) \in \mathrm{D}(W)$ and $(\hat{u}_1, v_2''-v_2') \in XDY(W)$. By noticing that $v_1 = (v_1+v_2'-v_2'')+(v_2''-v_2')$, we conclude that:

$$\mathrm{D}(W^-) \subset \big\{(\hat{x}, y_1+y_2) :\ (\hat{x},y_1),(\hat{x},y_2) \in \mathrm{D}(W)\big\}.$$

■

Proposition 3. *If I_1 is $*^-$ preserved for W, we have:*

1) $\mathrm{D}(W^-) = \{(\hat{x}, y_1 + y_2) : \ (\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)\}$.
2) *For every* $\hat{x}, y_1, y_2$ *satisfying* $(\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)$*, we have*

$$\hat{f}_{W^-}(\hat{x}, y_1 + y_2) = \hat{f}_W(\hat{x}, y_1) \cdot \hat{f}_W(\hat{x}, y_2).$$

Proof: Let $U_1, U_2, V_1, V_2, X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be as in Remark 1. We have:

1) Let $\hat{x}, y_1, y_2$ be such that $(\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)$. There exist $z_1, z_2 \in \mathcal{Z}$, $y_1', y_1'' \in \mathrm{Y}^{z_1}(W)$ and $y_2', y_2'' \in \mathrm{Y}^{z_2}(W)$ such that $y_1 = y_1' - y_1''$, $y_2 = y_2' - y_2''$, $\hat{p}_{y_1',z_1}(\hat{x}) \neq 0$, $\hat{p}_{y_1'',z_1}(\hat{x}) \neq 0$, $\hat{p}_{y_2',z_2}(\hat{x}) \neq 0$ and $\hat{p}_{y_2'',z_2}(\hat{x}) \neq 0$. Now from Lemma 8 we get $y_1' - y_2'' \in \mathrm{Y}^{(z_1,z_2)}(W^-)$ and $y_1'' - y_2' \in \mathrm{Y}^{(z_1,z_2)}(W^-)$. For every $v_2 \in \mathrm{Y}^{z_2}(W)$ satisfying $y_1' - y_2'' + v_2 \in \mathrm{Y}^{z_1}(W)$, we have:

$$\begin{aligned} \hat{p}_{y_1'-y_2''+v_2,z_1}(\hat{x}) \cdot \hat{p}_{v_2,z_2}(\hat{x})^* &= \hat{p}_{y_1',z_1}(\hat{x}) \hat{f}_W(\hat{x}, v_2 - y_2'') \cdot \hat{p}_{y_2'',z_2}(\hat{x})^* \hat{f}_W(\hat{x}, v_2 - y_2'')^* \\ &\overset{(a)}{=} \hat{p}_{y_1',z_1}(\hat{x}) \hat{p}_{y_2'',z_2}(\hat{x})^*, \end{aligned} \tag{15}$$

where (a) follows from the fact that $\hat{f}_W(\hat{x}, v_2 - y_2'') \in \mathbb{T}$, which means that

$$\hat{f}_W(\hat{x}, v_2 - y_2'') \hat{f}_W(\hat{x}, v_2 - y_2'')^* = |\hat{f}_W(\hat{x}, v_2 - y_2'')|^2 = 1.$$

Let $z^- = (z_1, z_2) \in \mathcal{Z}^-$. By using (13), we get:

$$\begin{aligned} &\hat{p}_{y_1'-y_2'',z^-,W^-}(\hat{x}) \\ &\quad= \sum_{\substack{v_2 \in \mathrm{Y}^{z_2}(W): \\ y_1'-y_2''+v_2 \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(y_1' - y_2'' + v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(y_1' - y_2''|z_1, z_2)} \hat{p}_{y_1'-y_2''+v_2,z_1}(\hat{x}) \cdot \hat{p}_{v_2,z_2}(\hat{x})^* \\ &\quad\overset{(a)}{=} \sum_{\substack{v_2 \in \mathrm{Y}^{z_2}(W): \\ y_1'-y_2''+v_2 \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(y_1' - y_2'' + v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(y_1' - y_2''|z_1, z_2)} \hat{p}_{y_1',z_1}(\hat{x}) \hat{p}_{y_2'',z_2}(\hat{x})^* \\ &\quad= \hat{p}_{y_1',z_1}(\hat{x}) \hat{p}_{y_2'',z_2}(\hat{x})^* \sum_{\substack{v_2 \in \mathrm{Y}^{z_2}(W): \\ y_1'-y_2''+v_2 \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(y_1' - y_2'' + v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(y_1' - y_2''|z_1, z_2)} \\ &\quad= \hat{p}_{y_1',z_1}(\hat{x}) \hat{p}_{y_2'',z_2}(\hat{x})^* \neq 0, \end{aligned}$$

where (a) follows from (15). Similarly, we can show that $\hat{p}_{y_1''-y_2',z_1,z_2,W^-}(\hat{x}) = \hat{p}_{y_1'',z_1}(\hat{x}) \hat{p}_{y_2',z_2}(\hat{x})^* \neq 0$. This means that $y_1' - y_2'' \in \mathrm{Y}^{\hat{x},z^-}(W^-)$ and $y_1'' - y_2' \in \mathrm{Y}^{\hat{x},z^-}(W^-)$. Therefore,

$$(\hat{x}, y_1 + y_2) = (\hat{x}, y_1' - y_1'' + y_2' - y_2'') = \big(\hat{x}, (y_1' - y_2'') - (y_1'' - y_2')\big) \in \mathrm{D}(W^-).$$

Hence, $\big\{(\hat{x}, y_1 + y_2) : \ (\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)\big\} \subset \mathrm{D}(W^-)$. We conclude that

$$\mathrm{D}(W^-) = \big\{(\hat{x}, y_1 + y_2) : \ (\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)\big\}$$

since the other inclusion follows from Lemma 10.

2) Let $\hat{x}, y_1, y_2$ be such that $(\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)$. Define $y_1', y_1'', y_2', y_2'', z_1, z_2$ as in 1). We have shown that $\hat{p}_{y_1'-y_2'',z^-,W^-}(\hat{x}) = \hat{p}_{y_1',z_1}(\hat{x}) \hat{p}_{y_2'',z_2}(\hat{x})^*$ and $\hat{p}_{y_1''-y_2',z_1,z_2,W^-}(\hat{x}) = \hat{p}_{y_1'',z_1}(\hat{x}) \hat{p}_{y_2',z_2}(\hat{x})^*$. Therefore,

$$\hat{f}_{W^-}(\hat{x}, y_1 + y_2) = \frac{\hat{p}_{y_1',z_1}(\hat{x}) \hat{p}_{y_2'',z_2}(\hat{x})^*}{\hat{p}_{y_1'',z_1}(\hat{x}) \hat{p}_{y_2',z_2}(\hat{x})^*} = \frac{\hat{f}_W(\hat{x}, y_1)}{\hat{f}_W(\hat{x}, y_2)^*} \overset{(a)}{=} \hat{f}_W(\hat{x}, y_1) \cdot \hat{f}_W(\hat{x}, y_2),$$

where (a) follows from the fact that $\hat{f}_W(\hat{x}, y_2) \cdot \hat{f}_W(\hat{x}, y_2)^* = |\hat{f}_W(\hat{x}, y_2)|^2 = 1$.

■

Corollary 1. *If polarization* $*$*-preserves* I_1 *for* W*, then* $\mathrm{D}(W) \subset \mathrm{D}(W^-)$ *and* $\hat{f}_{W^-}(\hat{x}, y) = \hat{f}_W(\hat{x}, y)$ *for every* $(\hat{x}, y) \in \mathrm{D}(W)$*, i.e.,* $\hat{f}_{W^-}$ *is an extension of* $\hat{f}_W$*.*

Proof: For every $(\hat{x}, y) \in \mathrm{D}(W)$, there exists $z \in \mathcal{Z}$ and $y_1, y_2 \in \mathrm{Y}^z(W)$ such that $y = y_1 - y_2$, $\hat{p}_{y_1,z}(\hat{x}) \neq 0$ and $\hat{p}_{y_2,z}(\hat{x}) \neq 0$. Therefore, we have $(\hat{x}, 0) \in \mathrm{D}(W)$ and $\hat{f}_W(\hat{x}, 0) = \dfrac{\hat{p}_{y_1,z}(\hat{x})}{\hat{p}_{y_1,z}(\hat{x})} = 1$.

Since $(\hat{x}, y) \in \mathrm{D}(W)$ and $(\hat{x}, 0) \in \mathrm{D}(W)$, Proposition 3 implies that $(\hat{x}, y) \in \mathrm{D}(W^-)$ and $\hat{f}_{W^-}(\hat{x}, y) = \hat{f}_W(\hat{x}, y) \cdot \hat{f}_W(\hat{x}, 0) = \hat{f}_W(\hat{x}, y)$. ■

Lemma 11. *For every $y_1, y_2 \in G_2$ and every $z_1, z_2 \in \mathcal{Z}$, we have:*

- *If $y_1 \notin \mathrm{Y}^{z_1}(W)$ or $y_2 \notin \mathrm{Y}^{z_2}(W)$, then $(y_2, z_1, z_2, u_1, y_1 - y_2) \notin \mathrm{YZ}(W^+)$ for every $u_1 \in G_1$.*
- *If $(y_1, z_1) \in \mathrm{YZ}(W)$ and $(y_2, z_2) \in \mathrm{YZ}(W)$, there exists $u_1 \in G_1$ such that $(y_2, z_1, z_2, u_1, y_1 - y_2) \in \mathrm{YZ}(W^+)$.*

Proof: Let $U_1, U_2, V_1, V_2, X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be as in Remark 1. For every $u_1 \in G_1$, every $y_1, y_2 \in G_2$ and every $z_1, z_2 \in \mathcal{Z}$, we have:

$$\begin{aligned}
\mathbb{P}_{V_2,Z_1,Z_2,U_1,V_1}(y_2, z_1, z_2, u_1, y_1 - y_2) &= \sum_{u_2 \in G_1} \mathbb{P}_{U_2,V_2,Z_1,Z_2,U_1,V_1}(u_2, y_2, z_1, z_2, u_1, y_1 - y_2) \\
&= \sum_{u_2 \in G_1} \mathbb{P}_{X_1,X_2,Y_1,Y_2,Z_1,Z_2}(u_1 + u_2, u_2, y_1, y_2, z_1, z_2) \\
&= \sum_{u_2 \in G_1} \mathbb{P}_{X_1,Y_1,Z_1}(u_1 + u_2, y_1, z_1) \cdot \mathbb{P}_{X_2,Y_2,Z_2}(u_2, y_2, z_2).
\end{aligned}$$

Therefore, we have:

- If $(y_1, z_1) \notin \mathrm{YZ}(W)$ or $(y_2, z_2) \notin \mathrm{YZ}(W)$, then for all $u_1, u_2 \in G_1$, we have $\mathbb{P}_{X_1,Y_1,Z_1}(u_1 + u_2, y_1, z_1) \leq \mathbb{P}_{Y_1,Z_1}(y_1, z_1) = 0$ or $\mathbb{P}_{X_2,Y_2,Z_2}(u_2, y_2, z_2) \leq \mathbb{P}_{Y_2,Z_2}(y_2, z_2) = 0$, which means that $\mathbb{P}_{V_2,Z_1,Z_2,U_1,V_1}(y_2, z_1, z_2, u_1, y_1 - y_2) = 0$. Hence $(y_2, z_1, z_2, u_1, y_1 - y_2) \notin \mathrm{YZ}(W^+)$ for every $u_1 \in G_1$.
- If $(y_1, z_1) \in \mathrm{YZ}(W)$ and $(y_2, z_2) \in \mathrm{YZ}(W)$, then $\mathbb{P}_{Y_1,Z_1}(y_1, z_1) > 0$ and $\mathbb{P}_{Y_2,Z_2}(y_2, z_2) > 0$. This means that there exist $x_1, x_2 \in G_1$ such that $\mathbb{P}_{X_1,Y_1,Z_1}(x_1, y_1, z_1) > 0$ and $\mathbb{P}_{X_2,Y_2,Z_2}(x_2, y_2, z_2) > 0$. Let $u_1 = x_1 - x_2$ and $u_2 = x_2$. We have $\mathbb{P}_{X_1,Y_1,Z_1}(u_1 + u_2, y_1, z_1) \cdot \mathbb{P}_{X_2,Y_2,Z_2}(u_2, y_2, z_2) > 0$, which implies that $\mathbb{P}_{V_2,Z_1,Z_2,U_1,V_1}(y_2, z_1, z_2, u_1, y_1 - y_2) > 0$ hence $(y_2, z_1, z_2, u_1, y_1 - y_2) \in \mathrm{YZ}(W^+)$.

■

Lemma 12. *Let $U_1, U_2, V_1, V_2, X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be as in Remark 1. For every $(v_2, z_1, z_2, u_1, v_1) \in \mathrm{YZ}(W^+)$, we have:*

$$\hat{p}_{v_2,z_1,z_2,u_1,v_1,W^+}(\hat{u}_2) = \sum_{\hat{u}_2' \in G_1} \frac{\hat{p}_{v_1+v_2,z_1}(\hat{u}_2') \cdot \hat{p}_{v_2,z_2}(\hat{u}_2 - \hat{u}_2')}{|G_1| \alpha(u_1, z_1, z_2, v_1, v_2)} e^{j2\pi\langle \hat{u}_2', u_1 \rangle}, \tag{16}$$

where $\alpha(u_1, z_1, z_2, v_1, v_2) = \mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(u_1|z_1, z_2, v_1, v_2)$.

Proof: For every $(v_2, z_1, z_2, u_1, v_1) \in \mathrm{YZ}(W^+)$ and every $u_2 \in G_2$, we have:

$$\begin{aligned}
p_{v_2,z_1,z_2,u_1,v_1,W^+}(u_2) &= \mathbb{P}_{U_2|V_2,Z_1,Z_2,U_1,V_1}(u_2|v_2, z_1, z_2, u_1, v_1) \\
&= \frac{\mathbb{P}_{U_1,U_2|Z_1,Z_2,V_1,V_2}(u_1, u_2|z_1, z_2, v_1, v_2)}{\mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(z_1, z_2, v_1, v_2)} \\
&= \frac{\mathbb{P}_{X_1,X_2|Z_1,Z_2,Y_1,Y_2}(u_1 + u_2, u_2|z_1, z_2, v_1 + v_2, v_2)}{\alpha(u_1, z_1, z_2, v_1, v_2)} \\
&= \frac{\mathbb{P}_{X_1|Z_1,Y_1}(u_1 + u_2|z_1, v_1 + v_2) \mathbb{P}_{X_2|Z_2,Y_2}(u_2|z_2, v_2)}{\alpha(u_1, z_1, z_2, v_1, v_2)} \\
&= \frac{p_{v_1+v_2,z_1}(u_1 + u_2) p_{v_2,z_2}(u_2)}{\alpha(u_1, z_1, z_2, v_1, v_2)}.
\end{aligned}$$

Therefore,

$$\begin{aligned}\hat{p}_{v_2,z_1,z_2,u_1,v_1,W^+}(\hat{u}_2) &= \frac{\frac{1}{|G_1|}\left(\hat{p}_{v_1+v_2,z_1}(\hat{u}_2)e^{j2\pi\langle\hat{u}_2,u_1\rangle}\right) * \hat{p}_{v_2,z_2}(\hat{u}_2)}{\alpha(u_1,z_1,z_2,v_1,v_2)} \\ &= \frac{\sum_{\hat{u}_2'\in G_1}\hat{p}_{v_1+v_2,z_1}(\hat{u}_2')e^{j2\pi\langle\hat{u}_2',u_1\rangle}\hat{p}_{v_2,z_2}(\hat{u}_2-\hat{u}_2')}{|G_1|\alpha(u_1,z_1,z_2,v_1,v_2)} \\ &= \sum_{\hat{u}_2'\in G_1}\frac{\hat{p}_{v_1+v_2,z_1}(\hat{u}_2')\cdot\hat{p}_{v_2,z_2}(\hat{u}_2-\hat{u}_2')}{|G_1|\alpha(u_1,z_1,z_2,v_1,v_2)}e^{j2\pi\langle\hat{u}_2',u_1\rangle}.\end{aligned}$$

■

Lemma 13. *Let* $(y_1,z_1),(y_2,z_2)\in \mathrm{YZ}(W)$ *and* $\hat{x}\in G_1$. *If there exists* $u_1\in G_1$ *such that*

$$\sum_{\hat{u}\in G_1}\hat{p}_{y_1,z_1}(\hat{u})\cdot\hat{p}_{y_2,z_2}(\hat{x}-\hat{u})e^{j2\pi\langle\hat{u},u_1\rangle}\neq 0. \tag{17}$$

then we have:

- $(y_2,z^+)\in\mathrm{YZ}(W^+)$, *where* $z^+=(z_1,z_2,u_1,y_1-y_2)$.
- $\hat{p}_{y_2,z^+,W^+}(\hat{x})\neq 0$.

Proof: Let $U_1,U_2,V_1,V_2,X_1,X_2,Y_1,Y_2,Z_1,Z_2$ be as in Remark 1. Let $v_1=y_1+y_2$ and $v_2=y_2$. Notice that the expression in (17) is the DFT of the mapping $K:G_1\to\mathbb{C}$ defined as

$$K(x)=p_{y_1,z_1}(u_1+x)\cdot p_{y_2,z_2}(x).$$

(17) shows that $\hat{K}$ is not zero everywhere which implies that K is not zero everywhere. Therefore, there exists $x\in G_1$ such that $K(x)\neq 0$. We have:

$$\begin{aligned}\mathbb{P}_{V_2,Z_1,Z_2,U_1,V_1}(v_2,z_1,z_2,u_1,v_1) &\geq \mathbb{P}_{U_1,U_2,V_1,V_2,Z_1,Z_2}(u_1,x,y_1-y_2,y_2,z_1,z_2) \\ &= \mathbb{P}_{X_1,X_2,Y_1,Y_2,Z_1,Z_2}(u_1+x,x,y_1,y_2,z_1,z_2) \\ &= \mathbb{P}_{X_1,Y_1,Z_1}(u_1+x,y_1,z_1)\mathbb{P}_{X_2,Y_2,Z_2}(x,y_2,z_2) \\ &= \mathbb{P}_{Y_1,Z_1}(y_1,z_1)p_{y_1,z_1}(u_1+x)\cdot\mathbb{P}_{Y_2,Z_2}(y_2,z_2)p_{y_2,z_2}(x) \\ &= \mathbb{P}_{Y_1,Z_1}(y_1,z_1)\cdot\mathbb{P}_{Y_2,Z_2}(y_2,z_2)\cdot K(x) \overset{(a)}{>} 0,\end{aligned}$$

where (a) follows from the fact that $y_1\in\mathrm{Y}^{z_1}(W)$, $y_2\in\mathrm{Y}^{z_2}(W)$ and $K(x)>0$. We conclude that $(v_2,z_1,z_2,u_1,v_1)\in\mathrm{YZ}(W^+)$ and so we can apply (16) to (v_2,z_1,z_2,u_1,v_1):

$$\hat{p}_{v_2,z_1,z_2,u_1,v_1,W^+}(\hat{x}) \overset{(a)}{=} \sum_{\hat{u}\in G_1}\frac{\hat{p}_{y_1,z_1}(\hat{u})\cdot\hat{p}_{y_2,z_2}(\hat{x}-\hat{u})}{|G_1|\alpha(u_1,z_1,z_2,v_1,v_2)}e^{j2\pi\langle\hat{u},u_1\rangle} \overset{(b)}{\neq} 0,$$

where (a) follows from (16) and (b) follows from (17). Therefore, $\hat{p}_{y_2,z^+,W^+}(\hat{x})\neq 0$, where $z^+=(z_1,z_2,u_1,y_1-y_2)$. ■

Proposition 4. *Suppose that polarization* $*$*-preserves* I_1 *for* W. *We have:*

1) $\left\{(\hat{x}_1+\hat{x}_2,y):\ (\hat{x}_1,y),(\hat{x}_2,y)\in\mathrm{D}(W)\right\}\subset\mathrm{D}(W^+)$.
2) *For every* $\hat{x}_1,\hat{x}_2,y$ *satisfying* $(\hat{x}_1,y),(\hat{x}_2,y)\in\mathrm{D}(W)$, *we have* $\hat{f}_{W^+}(\hat{x}_1+\hat{x}_2,y)=\hat{f}_W(\hat{x}_1,y)\cdot\hat{f}_W(\hat{x}_2,y)$.

Proof: Let $U_1,U_2,V_1,V_2,X_1,X_2,Y_1,Y_2,Z_1,Z_2$ be as in Remark 1.

1) Suppose that $\hat{x}_1,\hat{x}_2,y$ satisfy $(\hat{x}_1,y),(\hat{x}_2,y)\in\mathrm{D}(W)$ and let $\hat{x}=\hat{x}_1+\hat{x}_2$. There exist $z_1,z_2\in\mathcal{Z}$, $y_1,y_1'\in\mathrm{Y}^{z_1}(W)$ and $y_2,y_2'\in\mathrm{Y}^{z_2}(W)$ such that:
   - $y=y_1-y_1'$, $\hat{p}_{y_1,z_1}(\hat{x}_1)\neq 0$ and $\hat{p}_{y_1',z_1}(\hat{x}_1)\neq 0$.

- $y = y_2 - y_2'$, $\hat{p}_{y_2,z_2}(\hat{x}_2) \neq 0$ and $\hat{p}_{y_2',z_2}(\hat{x}_2) \neq 0$.

Let $v_1 = y_1 - y_2 = y_1' - y_2'$, $v_2 = y_2$ and $v_2' = y_2'$. Define the mapping $\hat{L} : G_1 \to \mathbb{C}$ as

$$\hat{L}(\hat{u}) = \hat{p}_{y_1,z_1}(\hat{u}) \cdot \hat{p}_{y_2,z_2}(\hat{x} - \hat{u}).$$

We have: $\hat{L}(\hat{x}_1) = \hat{p}_{y_1,z_1}(\hat{x}_1) \cdot \hat{p}_{y_2,z_2}(\hat{x}_2) \neq 0$. Therefore, the mapping $\hat{L}$ is not zero everywhere, which implies that its inverse DFT is not zero everywhere. Hence there exists $u_1 \in G_1$ such that:

$$\sum_{\hat{u} \in G_1} \hat{p}_{y_1,z_1}(\hat{u}) \cdot \hat{p}_{y_2,z_2}(\hat{x} - \hat{u}) e^{j2\pi\langle \hat{u}, u_1 \rangle} \neq 0.$$

It follows from Lemma 13 that $(v_2, z^+) \in \mathrm{YZ}(W^+)$ and $\hat{p}_{v_2,z^+,W^+}(\hat{x}) \neq 0$, where $z^+ = (z_1, z_2, u_1, v_1)$. If we can also show that $(v_2', z^+) \in \mathrm{YZ}(W^+)$ and $\hat{p}_{v_2',z^+,W^+}(\hat{x}) \neq 0$ we will be able to conclude that $(\hat{x}, y) \in \mathrm{D}(W^+)$ since $y = v_2 - v_2'$. We have the following:

- $\mathbb{P}_{U_1,Z_1,Z_2,V_1}(u_1, z_1, z_2, v_1) \geq \mathbb{P}_{V_2,Z_1,Z_2,U_1,V_1}(v_2, z_1, z_2, u_1, v_1) > 0$ since $(v_2, z^+) \in \mathrm{YZ}(W^+)$. Hence,
$$\mathbb{P}_{U_1|Z_1,Z_2,V_1}(u_1|z_1, z_2, v_1) > 0.$$
- $\mathbb{P}_{V_2,Z_1,Z_2,V_1}(v_2', z_1, z_2, v_1) = \mathbb{P}_{Y_1,Z_1,Y_2,Z_2}(y_1', z_1, y_2', z_2) > 0$ since $y_1' \in \mathrm{Y}^{z_1}(W)$ and $y_2' \in \mathrm{Y}^{z_2}(W)$. Thus,
$$\mathbb{P}_{V_2|Z_1,Z_2,V_1}(v_2'|z_1, z_2, v_1) > 0.$$

But I_1 is preserved for W, so we must have $I(U_1; V_2|Z_1Z_2V_1) = 0$. Therefore,

$$\mathbb{P}_{U_1,V_2|Z_1,Z_2,V_1}(u_1, v_2'|z_1, z_2, v_1) = \mathbb{P}_{U_1|Z_1,Z_2,V_1}(u_1|z_1, z_2, v_1) \cdot \mathbb{P}_{V_2|Z_1,Z_2,V_1}(v_2'|z_1, z_2, v_1) > 0. \tag{18}$$

We conclude that $\mathbb{P}_{U_2,Z_1,Z_2,U_1,V_1}(v_2', z_1, z_2, u_1, v_1) > 0$ and so $(v_2', z^+) \in \mathrm{YZ}(W^+)$. Now since we have showed that $\hat{p}_{v_2,z^+,W^+}(\hat{x}) \neq 0$ and since I_1 is $*^-$ preserved for W^+ (by Lemma 1), it follows from Lemma 6 that we also have $\hat{p}_{v_2',z^+,W^+}(\hat{x}) \neq 0$. We conclude that $(\hat{x}_1 + \hat{x}_2, y) \in \mathrm{D}(W^+)$ for every $\hat{x}_1, \hat{x}_2, y$ satisfying $(\hat{x}_1, y), (\hat{x}_2, y) \in \mathrm{D}(W)$. Therefore,

$$\big\{(\hat{x}_1 + \hat{x}_2, y) : \ (\hat{x}_1, y), (\hat{x}_2, y) \in \mathrm{D}(W)\big\} \subset \mathrm{D}(W^+).$$

2) Suppose that $\hat{x}_1, \hat{x}_2, y$ satisfy $(\hat{x}_1, y), (\hat{x}_2, y) \in \mathrm{D}(W)$ and let $\hat{x} = \hat{x}_1 + \hat{x}_2$. Let $y_1, y_2, y_1', y_2', v_1, v_2, v_2', z_1, z_2, z^+$ be defined as in 1) so that $v_2, v_2' \in \mathrm{Y}^{z+}(W^+)$, $y = v_2 - v_2'$, $\hat{p}_{v_2,z^+,W^+}(\hat{x}) \neq 0$ and $\hat{p}_{v_2',z^+,W^+}(\hat{x}) \neq 0$. Since $(\hat{x}, y) = (\hat{x}, v_1 - v_2) \in \mathrm{D}(W^+)$, we have:

$$\begin{aligned} \hat{p}_{v_2,z_1,z_2,u_1,v_1,W^+}(\hat{x}) &= \hat{p}_{v_2,z^+,W^+}(\hat{x}) = \hat{f}_{W^+}(\hat{x}, y) \cdot \hat{p}_{v_2',z^+,W^+}(\hat{x}) \\ &= \hat{f}_{W^+}(\hat{x}, y) \cdot \hat{p}_{v_2',z_1,z_2,u_1,v_1,W^+}(\hat{x}). \end{aligned} \tag{19}$$

Define $F : G_1 \to \mathbb{C}$ and $F' : G_1 \to \mathbb{C}$ as follows:

$$F(u_1') = \sum_{\hat{u} \in G_1} \hat{p}_{y_1,z_1}(\hat{u}) \cdot \hat{p}_{y_2,z_2}(\hat{x} - \hat{u}) e^{j2\pi\langle \hat{u}, u_1' \rangle}.$$

$$F'(u_1') = \sum_{\hat{u} \in G_1} \hat{p}_{y_1',z_1}(\hat{u}) \cdot \hat{p}_{y_2',z_2}(\hat{x} - \hat{u}) e^{j2\pi\langle \hat{u}, u_1' \rangle}.$$

For every $u_1' \in G_1$, we have the following:

- If $F(u_1') \neq 0$ then $(v_2, z_1, z_2, u_1', v_1) \in \mathrm{YZ}(W^+)$ and $\hat{p}_{v_2,z_1,z_2,u_1',v_1}(\hat{x}) \neq 0$ by Lemma 13. By replacing u_1 by u_1' in (18), we can get $(v_2', z_1, z_2, u_1', v_1) \in \mathrm{YZ}(W^+)$, which means that $\hat{p}_{v_2',z_1,z_2,u_1',v_1}(\hat{x}) \neq 0$ (see Lemma 6). We have:

$$\begin{aligned}
F(u_1') &= \sum_{\hat{u}\in G_1} \hat{p}_{y_1,z_1}(\hat{u}) \cdot \hat{p}_{y_2,z_2}(\hat{x}-\hat{u}) e^{j2\pi\langle \hat{u}, u_1'\rangle} \\
&\overset{(a)}{=} |G_1| \cdot \alpha(u_1', z_1, z_2, v_1, v_2) \hat{p}_{v_2,z_1,z_2,u_1',v_1}(\hat{x}) \\
&\overset{(b)}{=} \frac{\alpha(u_1', z_1, z_2, v_1, v_2)}{\alpha(u_1', z_1, z_2, v_1, v_2')} |G_1| \alpha(u_1', z_1, z_2, v_1, v_2') \hat{p}_{v_2',z_1,z_2,u_1',v_1}(\hat{x}) \hat{f}_{W^+}(\hat{x}, y) \\
&\overset{(c)}{=} \frac{\alpha(u_1', z_1, z_2, v_1, v_2)}{\alpha(u_1', z_1, z_2, v_1, v_2')} \sum_{\hat{u}\in G_1} \hat{p}_{y_1',z_1}(\hat{u}) \cdot \hat{p}_{y_2',z_2}(\hat{x}-\hat{u}) e^{j2\pi\langle \hat{u}, u_1'\rangle} \hat{f}_{W^+}(\hat{x}, y) \\
&= \frac{\mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(u_1', z_1, z_2, v_1, v_2)}{\mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(u_1', z_1, z_2, v_1, v_2')} \hat{f}_{W^+}(\hat{x}, y) F'(u_1') \\
&\overset{(d)}{=} \hat{f}_{W^+}(\hat{x}, y) F'(u_1'),
\end{aligned}$$

  where (a) and (c) follow from (16), (b) follows from (19) and (d) follows from the fact that $I(U_1; V_2 | Z_1 Z_2 V_1) = 0$.
- If $F(u_1') = 0$ then we must have $F'(u_1') = 0$ (because $F'(u_1') \neq 0$ would yield $F(u_1') \neq 0$, a contradiction). Therefore, we have $F(u_1') = 0 = \hat{f}_{W^+}(\hat{x}, y) F'(u_1')$.

We conclude that for every $u_1' \in G_1$, we have

$$F(u_1') = \hat{f}_{W^+}(\hat{x}, y) F'(u_1') = \sum_{\hat{u}\in G_1} \hat{f}_{W^+}(\hat{x}, y) \cdot \hat{p}_{y_1',z_1}(\hat{u}) \cdot \hat{p}_{y_2',z_2}(\hat{x}-\hat{u}) e^{j2\pi\langle \hat{u}, u_1'\rangle}. \tag{20}$$

Now define $g : G_1 \times G_2 \to \mathbb{C}$ as follows:

$$g(\hat{x}', y') = \begin{cases} \hat{f}_W(\hat{x}', y') & \text{if } (\hat{x}', y') \in \mathrm{D}(W), \\ 0 & \text{otherwise.} \end{cases} \tag{21}$$

For every $\hat{x}' \in G_1$, we have:

- If $\hat{p}_{y_1,z_1}(\hat{x}') \neq 0$ then $\hat{p}_{y_1',z_1}(\hat{x}') \neq 0$ (by Lemma 6) and $\hat{p}_{y_1,z_1}(\hat{x}') = \hat{f}_W(\hat{x}', y_1 - y_1') \hat{p}_{y_1',z_1}(\hat{x}') = g(\hat{x}', y) \hat{p}_{y_1',z_1}(\hat{x}')$.
- If $\hat{p}_{y_1,z_1}(\hat{x}') = 0$ then $\hat{p}_{y_1',z_1}(\hat{x}') = 0$ (by Lemma 6) and so $\hat{p}_{y_1,z_1}(\hat{x}') = 0 = g(\hat{x}', y) \hat{p}_{y_1',z_1}(\hat{x}')$.

Therefore, for every $\hat{x}' \in G_1$ we have $\hat{p}_{y_1,z_1}(\hat{x}') = g(\hat{x}', y) \hat{p}_{y_1',z_1}(\hat{x}')$. Similarly, $\hat{p}_{y_2,z_2}(\hat{x}') = g(\hat{x}', y) \hat{p}_{y_2',z_2}(\hat{x}')$ for all $\hat{x}' \in G_1$. Hence,

$$\begin{aligned}
F(u_1') &= \sum_{\hat{u}\in G_1} \hat{p}_{y_1,z_1}(\hat{u}) \cdot \hat{p}_{y_2,z_2}(\hat{x}-\hat{u}) e^{j2\pi\langle \hat{u}, u_1'\rangle} \\
&= \sum_{\hat{u}\in G_1} g(\hat{u}, y) \hat{p}_{y_1',z_1}(\hat{u}) \cdot g(\hat{x}-\hat{u}, y) \hat{p}_{y_2',z_2}(\hat{x}-\hat{u}) e^{j2\pi\langle \hat{u}, u_1'\rangle}.
\end{aligned} \tag{22}$$

We conclude that for every $u_1' \in G_1$, we have:

$$\sum_{\hat{u}\in G_1} \Big[\hat{f}_{W^+}(\hat{x}, y) - g(\hat{u}, y) g(\hat{x}-\hat{u}, y)\Big] \hat{p}_{y_1',z_1}(\hat{u}) \cdot \hat{p}_{y_2',z_2}(\hat{x}-\hat{u}) e^{j2\pi\langle \hat{u}, u_1'\rangle} \overset{(a)}{=} F(u_1') - F(u_1') = 0, \tag{23}$$

where (a) follows from (20) and (22). Notice that the sum in (23) is the inverse DFT of the function $\hat{K} : G_1 \to \mathbb{C}$ defined as:

$$\hat{K}(\hat{u}) = \Big[\hat{f}_{W^+}(\hat{x}, y) - g(\hat{u}, y) g(\hat{x}-\hat{u}, y)\Big] \hat{p}_{y_1',z_1}(\hat{u}) \cdot \hat{p}_{y_2',z_2}(\hat{x}-\hat{u}).$$

Now (23) implies that the inverse DFT of $\hat{K}$ is zero everywhere. Therefore, $\hat{K}$ is also zero everywhere. In particular,

$$\hat{K}(\hat{x_1}) = \Big[\hat{f}_{W^+}(\hat{x}, y) - g(\hat{x}_1, y)g(\hat{x}_2, y)\Big]\hat{p}_{y_1',z_1}(\hat{x}_1) \cdot \hat{p}_{y_2',z_2}(\hat{x}_2) = 0.$$

But $\hat{p}_{y_1',z_1}(\hat{x}_1) \neq 0$ and $\hat{p}_{y_2',z_2}(\hat{x}_2) \neq 0$, so we must have $\hat{f}_{W^+}(\hat{x}, y) - g(\hat{x}_1, y)g(\hat{x}_2, y) = 0$. Therefore,

$$\hat{f}_{W^+}(\hat{x}, y) = g(\hat{x}_1, y)g(\hat{x}_2, y) = \hat{f}_W(\hat{x}_1, y) \cdot \hat{f}_W(\hat{x}_2, y).$$

■

Corollary 2. *If polarization $*$-preserves I_1 for W, then $\mathrm{D}(W) \subset \mathrm{D}(W^+)$ and $\hat{f}_{W^+}(\hat{x}, y) = \hat{f}_W(\hat{x}, y)$ for every $(\hat{x}, y) \in \mathrm{D}(W)$, i.e., $\hat{f}_{W^+}$ is an extension of $\hat{f}_W$.*

Proof: For every $(\hat{x}, y) \in \mathrm{D}(W)$, there exists $z \in \mathcal{Z}$ and $y_1, y_2 \in \mathrm{Y}^z(W)$ such that $y = y_1 - y_2$, $\hat{p}_{y_1,z}(\hat{x}) \neq 0$ and $\hat{p}_{y_2,z}(\hat{x}) \neq 0$. We have:

$$\hat{p}_{y_1,z}(0) = \sum_{x \in G_1} p_{y_1,z}(x)e^{-j2\pi\langle 0,x\rangle} = \sum_{x \in G_1} p_{y_1,z}(x) = 1 \neq 0.$$

Similarly, $\hat{p}_{y_2,z}(0) = 1 \neq 0$. Therefore, we have $(0, y) \in \mathrm{D}(W)$ and $\hat{f}_W(0, y) = \dfrac{\hat{p}_{y_1,z}(0)}{\hat{p}_{y_2,z}(0)} = 1$.

Since $(\hat{x}, y) \in \mathrm{D}(W)$ and $(0, y) \in \mathrm{D}(W)$, Proposition 4 implies that $(\hat{x}, y) \in \mathrm{D}(W^+)$ and $\hat{f}_{W^+}(\hat{x}, y) = \hat{f}_W(\hat{x}, y)\hat{f}_W(0, y) = \hat{f}_W(\hat{x}, y)$. ■

Proposition 3 implies that $\mathrm{D}(W^{[n]^-})$ extends $\mathrm{D}(W)$ to the point where all the G_2-sections of $\mathrm{D}(W^{[n]^-})$ for fixed $\hat{x}$ become subgroups of G_2. $\mathrm{D}(W^{[n]^-})$ cannot grow after this point. Similarly, Proposition 4 implies that $\mathrm{D}(W^{[n]^+})$ keeps growing until a point where all its G_1-section for fixed y become subgroups of G_1. This motivates us to introduce the following two definitions:

Definition 11. *Let $D \subset G_1 \times G_2$. Define the following sets:*

- $H_1(D) = \{x : \exists y,\ (x, y) \in D\}$.
- *For every $x \in H_1(D)$, let $H_2^x(D) = \{y : (x, y) \in D\}$.*
- $H_2(D) = \{y : \exists x,\ (x, y) \in D\}$.
- *For every $y \in H_2(D)$, let $H_1^y(D) = \{x : (x, y) \in D\}$.*

We say that D is a pseudo quadratic domain *if:*

- *$H_1^y(D)$ is a subgroup of G_1 for every $y \in H_2(D)$.*
- *$H_2^x(D)$ is a subgroup of G_2 for every $x \in H_1(D)$.*

Definition 12. *Let $D \subset G_1 \times G_2$ and let $F : D \to \mathbb{T}$ be a mapping from D to $\mathbb{T}$. We say that F is* pseudo quadratic *if:*

- *D is a pseudo quadratic domain.*
- *For every $y \in H_2(D)$, the mapping $x \to F(x, y)$ is a group homomorphism from $\big(H_1^y(D), +\big)$ to $(\mathbb{T}, \cdot)$.*
- *For every $x \in H_1(D)$, the mapping $y \to F(x, y)$ is a group homomorphism from $\big(H_2^x(D), +\big)$ to $(\mathbb{T}, \cdot)$.*

Proposition 5. *If polarization $*$-preserves I_1 for W, then $\hat{f}_W$ can be extended to a pseudo quadratic function.*

Proof: Define the sequence $(W_n)_{n \geq 0}$ of MACs recursively as follows:

- $W_0 = W$.
- $W_n = W_{n-1}^-$ if $n > 0$ is odd.
- $W_n = W_{n-1}^+$ if $n > 0$ is even.

For example, we have $W_1 = W^-$, $W_2 = W^{(-,+)}$, $W_3 = W^{(-,+,-)}$, $W_4 = W^{(-,+,-,+)}$ ...

It follows from Corollaries 1 and 2 that:

- The sequence of sets $\big(\mathrm{D}(W_n)\big)_{n\geq 0}$ is increasing.
- $\hat{f}_{W_n}$ is an extension of $\hat{f}_W$ for every $n > 0$.

Since $\big(\mathrm{D}(W_n)\big)_{n\geq 0}$ is increasing and since $G_1 \times G_2$ is finite, there exists $n_0 > 0$ such that for every $n \geq n_0$ we have $\mathrm{D}(W_n) = \mathrm{D}(W_{n_0})$ for all $n \geq n_0$. We may assume without loss of generality that n_0 is even. Define the following sets:

- $\hat{H}_1 = \{\hat{x} :\ \exists y,\ (\hat{x}, y) \in \mathrm{D}(W_n)\}$.
- For every $\hat{x} \in \hat{H}_1$, let $H_2^{\hat{x}} = \{y :\ (\hat{x}, y) \in \mathrm{D}(W_n)\}$.
- $H_2 = \{y :\ \exists \hat{x},\ (\hat{x}, y) \in \mathrm{D}(W_n)\}$.
- For every $y \in H_2$, let $\hat{H}_1^y = \{\hat{x} :\ (\hat{x}, y) \in \mathrm{D}(W_n)\}$.

We have the following:

- For every fixed $y \in H_2$, let $\hat{x}_1, \hat{x}_2 \in \hat{H}_1^y$ so $(\hat{x}_1, y), (\hat{x}_2, y) \in \mathrm{D}(W_{n_0}) \subset \mathrm{D}(W_{n_0+1})$. Therefore, it follows from Proposition 4 that $(\hat{x}_1 + \hat{x}_2, y) \in \mathrm{D}(W^+_{n_0+1}) = \mathrm{D}(W_{n_0+2}) = \mathrm{D}(W_{n_0})$ which implies that $\hat{x}_1 + \hat{x}_2 \in \hat{H}_1^y$. Hence $\hat{H}_1^y$ is a subgroup of G_1. Moreover, Proposition 4 implies that

$$\begin{aligned}\hat{f}_{W_{n_0}}(\hat{x}_1 + \hat{x}_2, y) &= \hat{f}_{W_{n_0+2}}(\hat{x}_1 + \hat{x}_2, y) = \hat{f}_{W^+_{n_0+1}}(\hat{x}_1 + \hat{x}_2, y)\\ &= \hat{f}_{W_{n_0+1}}(\hat{x}_1, y) \cdot \hat{f}_{W_{n_0+1}}(\hat{x}_2, y) = \hat{f}_{W_{n_0}}(\hat{x}_1, y) \cdot \hat{f}_{W_{n_0}}(\hat{x}_2, y).\end{aligned}$$

  Therefore the mapping $\hat{x} \to \hat{f}_{W_{n_0}}(\hat{x}, y)$ is a group homomorphism from $\hat{H}_1^y$ to $\mathbb{C}$.
- For every fixed $\hat{x} \in \hat{H}_1$, let $y_1, y_2 \in H_2^{\hat{x}}$ so $(\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W_{n_0})$. Therefore, it follows from Proposition 3 that $(\hat{x}, y_1 + y_2) \in \mathrm{D}(W^-_{n_0}) = \mathrm{D}(W_{n_0+1}) = \mathrm{D}(W_{n_0})$ which implies that $y_1 + y_2 \in H_2^{\hat{x}}$. Hence $H_2^{\hat{x}}$ is a subgroup of G_2. Moreover, Proposition 3 implies that

$$\begin{aligned}\hat{f}_{W_{n_0}}(\hat{x}, y_1 + y_2) &= \hat{f}_{W_{n_0+1}}(\hat{x}, y_1 + y_2) = \hat{f}_{W^-_{n_0}}(\hat{x}, y_1 + y_2)\\ &= \hat{f}_{W_{n_0}}(\hat{x}, y_1) \cdot \hat{f}_{W_{n_0}}(\hat{x}, y_2).\end{aligned}$$

  Therefore the mapping $y \to \hat{f}_{W_{n_0}}(\hat{x}, y)$ is a group homomorphism from $H_2^{\hat{x}}$ to $\mathbb{C}$.

We conclude that $\hat{f}_{W_{n_0}}$ is pseudo quadratic. ■

The necessary conditions found in Lemma 6 and Proposition 5 motivate us to introduce the following definition:

Definition 13. *We say that $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$ is* polarization compatible *with respect to the first user if there exists a pseudo quadratic function $F : D \to \mathbb{T}$ such that:*

- $\mathrm{D}(W) \subset D \subset G_1 \times G_2$.
- *For every $(\hat{x}, z) \in \hat{\mathrm{X}}\mathrm{Z}(W)$, we have $\hat{p}_{y,z}(\hat{x}) \neq 0$ for every $y \in \mathrm{Y}^z(W)$.*
- *For every $(\hat{x}, z) \in \hat{\mathrm{X}}\mathrm{Z}(W)$ and every $y_1, y_2 \in \mathrm{Y}^z(W)$, we have $\hat{p}_{y_1,z}(\hat{x}) = F(\hat{x}, y_1 - y_2) \cdot \hat{p}_{y_2,z}(\hat{x})$.*

For the sake of simplicity and brevity, we will write "polarization compatible" to denote "polarization compatible with respect to the first user". Lemma 6 and Proposition 5 show that if polarization $*$-preserves I_1 for W then W must be polarization compatible.

C. Sufficient condition

In this subsection, we show that polarization compatibility is a sufficient condition for the $*$-preservability of I_1.

Lemma 14. *If $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$ is polarization compatible then I_1 is preserved for W.*

Proof: Let $F : D \to \mathbb{T}$ be the pseudo quadratic function of Definition 13. Suppose that $y_1, y_2, y_1', y_2' \in G_2$ and $z_1, z_2 \in \mathcal{Z}$ satisfy:

- $y_1 - y_2 = y_1' - y_2'$.
- $y_1, y_1' \in \mathrm{Y}^{z_1}(W)$ and $y_2, y_2' \in \mathrm{Y}^{z_2}(W)$.

For every $\hat{x} \in G_1$, we have:

- If $\hat{p}_{y_1,z_1}(\hat{x}) = 0$ then $\hat{p}_{y_1',z_1}(\hat{x}) = 0$ by Definition 13 and so
$$\hat{p}_{y_1,z_1}(\hat{x})\hat{p}_{y_2,z_2}(\hat{x})^* = \hat{p}_{y_1',z_1}(\hat{x})\hat{p}_{y_2',z_2}(\hat{x})^* = 0.$$
- If $\hat{p}_{y_2,z_2}(\hat{x}) = 0$ then $\hat{p}_{y_2',z_2}(\hat{x}) = 0$ by Definition 13 and so
$$\hat{p}_{y_1,z_1}(\hat{x})\hat{p}_{y_2,z_2}(\hat{x})^* = \hat{p}_{y_1',z_1}(\hat{x})\hat{p}_{y_2',z_2}(\hat{x})^* = 0.$$
- If $\hat{p}_{y_1,z_1}(\hat{x}) \neq 0$ and $\hat{p}_{y_2,z_2}(\hat{x}) \neq 0$ then $(\hat{x}, z_1) \in \hat{\mathrm{XZ}}(W)$ and $(\hat{x}, z_2) \in \hat{\mathrm{XZ}}(W)$. By noticing that $y_1 - y_1' = y_2 - y_2'$, we get
$$\hat{p}_{y_1,z_1}(\hat{x})\hat{p}_{y_2,z_2}(\hat{x})^* = \hat{p}_{y_1',z_1}(\hat{x})F(\hat{x}, y_1 - y_1')\hat{p}_{y_2',z_2}(\hat{x})^*F(\hat{x}, y_2 - y_2')^* \overset{(a)}{=} \hat{p}_{y_1',z_1}(\hat{x})\hat{p}_{y_2',z_2}(\hat{x})^*,$$
where (a) follows from the fact that $F(\hat{x}, y_1 - y_1')F(\hat{x}, y_2 - y_2')^* = |F(\hat{x}, y_1 - y_1')|^2 = 1$.

Therefore, we have $\hat{p}_{y_1,z_1}(\hat{x})\hat{p}_{y_2,z_2}(\hat{x})^* = \hat{p}_{y_1',z_1}(\hat{x})\hat{p}_{y_2',z_2}(\hat{x})^*$ for all $\hat{x} \in G_1$. Lemma 2 now implies that I_1 is preserved for W. ■

Lemma 15. *If $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$ is polarization compatible then W^- is also polarization compatible.*

Proof: Let $U_1, U_2, V_1, V_2, X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be as in Remark 1. Let $F : D \to \mathbb{T}$ be the pseudo quadratic function of Definition 13. By Lemma 10 we have:

$$\mathrm{D}(W^-) \subset \big\{(\hat{x}, y_1 + y_2) : \ (\hat{x}, y_1), (\hat{x}, y_2) \in \mathrm{D}(W)\big\} \overset{(a)}{\subset} \big\{(\hat{x}, y_1 + y_2) : \ (\hat{x}, y_1), (\hat{x}, y_2) \in D\big\} \overset{(b)}{=} D,$$

where (a) follows from the fact that $\mathrm{D}(W) \subset D$ and (b) follows from the fact that D is a pseudo quadratic domain.

Let $(\hat{u}_1, z^-) \in \hat{\mathrm{XZ}}(W^-)$, where $z^- = (z_1, z_2) \in \mathcal{Z}^-$. There exists $v_1 \in \mathrm{Y}^{z^-}(W^-)$ such that $\hat{p}_{v_1,z^-,W^-}(\hat{u}_1) \neq 0$. From (13), we have:

$$\hat{p}_{v_1,z^-,W^-}(\hat{u}_1) = \sum_{\substack{v_2 \in \mathrm{Y}^{z_2}(W):\\ v_1+v_2 \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1 + v_2|z_1)\mathbb{P}_{Y_2|Z_2}(v_2|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1|z_1, z_2)} \hat{p}_{v_1+v_2,z_1}(\hat{u}_1) \cdot \hat{p}_{v_2,z_2}(\hat{u}_1)^*.$$

Since $\hat{p}_{v_1,z^-,W^-}(\hat{u}_1) \neq 0$, the terms in the above sum cannot all be zero. Therefore, there exists $v_2 \in \mathrm{Y}^{z_1}(W)$ such that $v_1 + v_2 \in \mathrm{Y}^{z_2}(W)$, $\hat{p}_{v_1+v_2,z_1}(\hat{u}_1) \neq 0$ and $\hat{p}_{v_2,z_2}(\hat{u}_1) \neq 0$. Let $y_1 = v_1 + v_2$ and $y_2 = v_2$.

For every $v_1' \in \mathrm{Y}^{z^-}(W^-)$, we have:

$$\begin{aligned}
&\hat{p}_{v_1',z^-,W^-}(\hat{u}_1) \\
&= \sum_{\substack{v_2' \in \mathrm{Y}^{z_2}(W):\\ v_1'+v_2' \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1' + v_2'|z_1)\mathbb{P}_{Y_2|Z_2}(v_2'|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1'|z_1, z_2)} \hat{p}_{v_1'+v_2',z_1}(\hat{u}_1) \cdot \hat{p}_{v_2',z_2}(\hat{u}_1)^* \\
&\overset{(a)}{=} \sum_{\substack{v_2' \in \mathrm{Y}^{z_2}(W):\\ v_1'+v_2' \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1' + v_2'|z_1)\mathbb{P}_{Y_2|Z_2}(v_2'|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1'|z_1, z_2)} \hat{p}_{y_1,z_1}(\hat{u}_1) \cdot F(\hat{u}_1, v_1' + v_2' - y_1) \cdot \frac{\hat{p}_{y_2,z_2}(\hat{u}_1)^*}{F(\hat{u}_1, v_2' - y_2)} \\
&\overset{(b)}{=} \hat{p}_{y_1,z_1}(\hat{u}_1) \cdot \hat{p}_{y_2,z_2}(\hat{u}_1)^* \sum_{\substack{v_2' \in \mathrm{Y}^{z_2}(W):\\ v_1'+v_2' \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1' + v_2'|z_1)\mathbb{P}_{Y_2|Z_2}(v_2'|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1'|z_1, z_2)} F(\hat{u}_1, v_1' + v_2' - y_1 - v_2' + y_2) \\
&= \hat{p}_{y_1,z_1}(\hat{u}_1) \cdot \hat{p}_{y_2,z_2}(\hat{u}_1)^* \cdot F(\hat{u}_1, v_1' - y_1 + y_2) \sum_{\substack{v_2' \in \mathrm{Y}^{z_2}(W):\\ v_1'+v_2' \in \mathrm{Y}^{z_1}(W)}} \frac{\mathbb{P}_{Y_1|Z_1}(v_1' + v_2'|z_1)\mathbb{P}_{Y_2|Z_2}(v_2'|z_2)}{\mathbb{P}_{V_1|Z_1,Z_2}(v_1'|z_1, z_2)} \\
&= \hat{p}_{y_1,z_1}(\hat{u}_1) \cdot \hat{p}_{y_2,z_2}(\hat{u}_1)^* \cdot F(\hat{u}_1, v_1' - y_1 + y_2) = \hat{p}_{y_1,z_1}(\hat{u}_1) \cdot \hat{p}_{y_2,z_2}(\hat{u}_1)^* \cdot F(\hat{u}_1, v_1' - v_1) \neq 0,
\end{aligned}$$

where (a) follows from the fact that $F(\hat{u}_1, v_2'-v_2) \in \mathbb{T}$ which implies that $F(\hat{u}_1, v_2'-v_2)^* = \dfrac{1}{F(\hat{u}_1, v_2'-v_2)}$. (b) follows from the fact that the mapping $y \to F(\hat{u}_1, y)$ is a group homomorphism from $H_2^{\hat{u}_1}(D)$ to $\mathbb{T}$. Therefore, for every $v_1' \in \mathrm{Y}^{z^-}(W^-)$ we have $\hat{p}_{v_1',z^-,W^-}(\hat{u}_1) \neq 0$. Moreover, for every $v_1', v_1'' \in \mathrm{Y}^{z^-}(W^-)$, we have:

$$\begin{aligned}\frac{\hat{p}_{v_1',z^-,W^-}(\hat{u}_1)}{\hat{p}_{v_1'',z^-,W^-}(\hat{u}_1)} &= \frac{\hat{p}_{y_1,z_1}(\hat{u}_1)\cdot\hat{p}_{y_2,z_2}(\hat{u}_1)^*\cdot F(\hat{u}_1, v_1'-v_1)}{\hat{p}_{y_1,z_1}(\hat{u}_1)\cdot\hat{p}_{y_2,z_2}(\hat{u}_1)^*\cdot F(\hat{u}_1, v_1''-v_1)}\\ &= F(\hat{u}_1, v_1'-v_1-v_1''+v_1) = F(\hat{u}_1, v_1'-v_1'').\end{aligned}$$

Hence, $\hat{p}_{v_1',z^-,W^-}(\hat{u}_1) = F(\hat{u}_1, v_1'-v_1'')\cdot\hat{p}_{v_1'',z^-,W^-}(\hat{u}_1)$.

We conclude that W^- is polarization compatible. ■

Lemma 16. *If $W : G_1 \times G_2 \longrightarrow \mathcal{Z}$ is polarization compatible then W^+ is also polarization compatible.*

Proof: Let $F : D \to \mathbb{T}$ be the pseudo quadratic function of Definition 13.

Let $(\hat{u}_2, v_2) \in \mathrm{D}(W^+)$. There exist $z^+ = (z_1, z_2, u_1, v_1) \in \mathcal{Z}^+$ and $v_2', v_2'' \in \mathrm{Y}^{z^+}(W^+)$ such that $v_2 = v_2' - v_2''$, $\hat{p}_{v_2',z^+}(\hat{u}_2) \neq 0$ and $\hat{p}_{v_2'',z^+}(\hat{u}_2) \neq 0$. From (16) we have

$$\hat{p}_{v_2',z_1,z_2,u_1,v_1,W^+}(\hat{u}_2) = \sum_{\hat{u}_2' \in G_1} \frac{\hat{p}_{v_1+v_2',z_1}(\hat{u}_2')\cdot\hat{p}_{v_2',z_2}(\hat{u}_2-\hat{u}_2')}{|G_1|\alpha(u_1,z_1,z_2,v_1,v_2')} e^{j2\pi\langle\hat{u}_2',u_1\rangle},$$

Since $\hat{p}_{v_2',z_1,z_2,u_1,v_1,W^+}(\hat{u}_2) \neq 0$, there must exist $\hat{u}_2' \in G_1$ such that $\hat{p}_{v_1+v_2',z_1}(\hat{u}_2') \neq 0$ and $\hat{p}_{v_2',z_2}(\hat{u}_2-\hat{u}_2') \neq 0$. Therefore, $(\hat{u}_2', z_1), (\hat{u}_2-\hat{u}_2', z_2) \in \hat{\mathrm{XZ}}(W^+)$. On the other hand, $v_2'' \in \mathrm{Y}^{z^+}(W^+)$ implies that $v_1 + v_2'' \in \mathrm{Y}^{z_1}(W)$ and $v_2'' \in \mathrm{Y}^{z_2}(W)$ (see Lemma 11). It follows from the polarization compatibility of W that $\hat{p}_{v_1+v_2'',z_1}(\hat{u}_2') \neq 0$ and $\hat{p}_{v_2'',z_2}(\hat{u}_2-\hat{u}_2') \neq 0$ (see Definition 13). Therefore

$$(\hat{u}_2', v_2) = \big(\hat{u}_2', v_1 + v_2' - (v_1 + v_2'')\big) \in \mathrm{D}(W) \subset D$$

and

$$(\hat{u}_2 - \hat{u}_2', v_2) = \big(\hat{u}_2 - \hat{u}_2', v_2' - v_2''\big) \in \mathrm{D}(W) \subset D$$

Now since D is a pseudo quadratic domain, we have $(\hat{u}_2, v_2) = \big(\hat{u}_2' + (\hat{u}_2 - \hat{u}_2'), v_2\big) \in D$. We conclude that $\mathrm{D}(W^+) \subset D$.

Now let $(\hat{u}_2, z^+) \in \hat{\mathrm{XZ}}(W^+)$, where $z^+ = (z_1, z_2, u_1, v_1) \in \mathcal{Z}^+$. There exists $v_2 \in \mathrm{Y}^{z^+}(W)$ such that $\hat{p}_{v_2,z^+}(\hat{u}_2) \neq 0$. For every $v_2' \in \mathrm{Y}^{z^+}(W)$, we have

$$\begin{aligned}\hat{p}_{v_2',z^+,W^+}(\hat{u}_2) = \hat{p}_{v_2',z_1,z_2,u_1,v_1,W^+}(\hat{u}_2) &= \sum_{\hat{u}_2' \in G_1} \frac{\hat{p}_{v_1+v_2',z_1}(\hat{u}_2')\cdot\hat{p}_{v_2',z_2}(\hat{u}_2-\hat{u}_2')}{|G_1|\alpha(u_1,z_1,z_2,v_1,v_2')} e^{j2\pi\langle\hat{u}_2',u_1\rangle}\\ &= \sum_{\hat{u}_2' \in G_1} \frac{\hat{p}_{v_1+v_2,z_1}(\hat{u}_2')F(\hat{u}_2', v_2'-v_2)\cdot\hat{p}_{v_2,z_2}(\hat{u}_2-\hat{u}_2')F(\hat{u}_2-\hat{u}_2', v_2'-v_2)}{|G_1|\cdot\mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(u_1|z_1,z_2,v_1,v_2')} e^{j2\pi\langle\hat{u}_2',u_1\rangle}\\ &\overset{(a)}{=} \sum_{\hat{u}_2' \in G_1} \frac{\hat{p}_{v_1+v_2,z_1}(\hat{u}_2')\cdot\hat{p}_{v_2,z_2}(\hat{u}_2-\hat{u}_2')}{|G_1|\cdot\mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(u_1|z_1,z_2,v_1,v_2)} F(\hat{u}_2'+\hat{u}_2-\hat{u}_2', v_2'-v_2)\cdot e^{j2\pi\langle\hat{u}_2',u_1\rangle}\\ &= F(\hat{u}_2, v_2'-v_2)\sum_{\hat{u}_2' \in G_1} \frac{\hat{p}_{v_1+v_2,z_1}(\hat{u}_2')\cdot\hat{p}_{v_2,z_2}(\hat{u}_2-\hat{u}_2')}{|G_1|\cdot\mathbb{P}_{U_1|Z_1,Z_2,V_1,V_2}(u_1|z_1,z_2,v_1,v_2)} e^{j2\pi\langle\hat{u}_2',u_1\rangle}\\ &= F(\hat{u}_2, v_2'-v_2)\hat{p}_{v_2,z_1,z_2,u_1,v_1,W^+}(\hat{u}_2) = F(\hat{u}_2, v_2'-v_2)\hat{p}_{v_2,z^+,W^+}(\hat{u}_2) \neq 0,\end{aligned}$$

where (a) follows from the fact that F is pseudo quadratic and the fact that U_1 is independent of V_2 conditioned on (Z_1, Z_2, V_1) (the polarization compatibility of W implies that I_1 is preserved for W by

Lemma 14). Therefore, for every $v_2' \in \mathrm{Y}^{z^+}(W^+)$, we have $\hat{p}_{v_2',z^+,W^+}(\hat{u}_2) \neq 0$. Moreover, for every $v_2', v_2'' \in \mathrm{Y}^{z^+}(W^+)$, we have

$$\begin{aligned}\frac{\hat{p}_{v_2',z^+,W^+}(\hat{u}_2)}{\hat{p}_{v_2'',z^+,W^+}(\hat{u}_2)} &= \frac{F(\hat{u}_2, v_2' - v_2) \cdot \hat{p}_{v_2,z^+,W^+}(\hat{u}_2)}{F(\hat{u}_2, v_2'' - v_2) \cdot \hat{p}_{v_2,z^+,W^+}(\hat{u}_2)} \\ &= F(\hat{u}_2, v_2' - v_2 - v_2'' + v_2) = F(\hat{u}_2, v_2' - v_2'').\end{aligned}$$

Hence, $\hat{p}_{v_2',z^+,W^+}(\hat{u}_2) = F(\hat{u}_2, v_2' - v_2'') \cdot \hat{p}_{v_2'',z^+,W^+}(\hat{u}_2)$.

We conclude that W^+ is polarization compatible. ∎

Proposition 6. *If W is polarization compatible then polarization $*$-preserves I_1 for W.*

Proof: Suppose that W is polarization compatible. Using Lemmas 15 and 16, we can show by induction that W^s is polarization compatible for every $s \in \{-,+\}^*$. Lemma 14 now implies that I_1 is preserved for W^s for every $s \in \{-,+\}^*$. By applying Lemma 1, we deduce that polarization $*$-preserves I_1 for W. ∎

Theorem 1. *polarization $*$-preserves I_1 for W if and only if W is polarization compatible.*

Proof: The theorem follows from Lemma 6 and Propositions 5 and 6. ∎

D. Application: $G_1 = G_2 = \mathbb{F}_q$

The characterization found in Theorem 1 (i.e., polarization compatibility) takes a simple form in the special case where $G_1 = G_2 = \mathbb{F}_q$ for a prime q:

Proposition 7. *Let $W : \mathbb{F}_q \times \mathbb{F}_q \longrightarrow \mathcal{Z}$ and $(X, Y) \xrightarrow{W} Z$. Polarization $*$-preserves I_1 for W if and only if there exists $a \in \mathbb{F}_q$ such that $I(X + aY; Y|Z) = 0$.*

Proof: If polarization $*$-preserves I_1 for W then W is polarization compatible. Let $F : D \to \mathbb{T}$ be the pseudo quadratic function of Definition 13. We have the following:

- If there exists $(\hat{x}, y) \in D$ such that $\hat{x} \neq 0$ and $y \neq 0$ then $D = \mathbb{F}_q \times \mathbb{F}_q$ since D is a pseudo quadratic domain.
- If for all $(\hat{x}, y) \in D$ we have either $\hat{x} = 0$ or $y = 0$, then $F(\hat{x}, y) = 1$ for every $(\hat{x}, y) \in D$. Hence the mapping $F' : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{T}$ defined as $F'(\hat{x}, y) = 1$ is an extension of F which preserves the pseudo quadratic property.

Therefore, we can assume without loss of generality that $D = \mathbb{F}_q \times \mathbb{F}_q$, which means that F is quadratic. Let $a \in \mathbb{F}_q$ be such that $F(1, 1) = e^{-j2\pi\frac{a}{q}}$.

Fix $z \in \mathcal{Z}$ and $y_1, y_2 \in \mathrm{Y}^z(W)$. For every $\hat{x} \in \mathbb{F}_q$ we have $\hat{p}_{y_1,z}(\hat{x}) = \hat{p}_{y_2,z}(\hat{x}) \cdot e^{-j2\pi a\frac{(y_1-y_2)\hat{x}}{q}}$, which implies that for every $x \in \mathbb{F}_q$, we have $p_{y_1,z}(x) = p_{y_2,z}(x + a(y_1 - y_2))$, i.e.,

$$\mathbb{P}_{X|Y,Z}(x|y_1, z) = \mathbb{P}_{X|Y,Z}(x + a(y_1 - y_2)|y_2, z) \tag{24}$$

Therefore, for every $x \in G_1$ we have

$$\begin{aligned}\mathbb{P}_{X+aY|Y,Z}(x|y_1, z) &= \mathbb{P}_{X|Y,Z}(x - ay_1|y_1, z) \overset{(b)}{=} \mathbb{P}_{X|Y,Z}(x - ay_1 + a(y_1 - y_2)|y_2, z) \\ &= \mathbb{P}_{X|Y,Z}(x - ay_2|y_2, z) = \mathbb{P}_{X+aY|Y,Z}(x|y_2, z),\end{aligned}$$

where (b) follows from (24). We conclude that $X + aY$ is independent of Y conditioned on Z, i.e., $I(X + aY; Y|Z) = 0$. ∎

Remark 4. *It may look promising to try to generalize Proposition 7 to the case where $G_1 = \mathbb{F}_q^k$ and $G_2 = \mathbb{F}_q^l$ by considering the condition $I(X + AY; Y|Z) = 0$ for some matrix $A \in \mathbb{F}_q^{k\times l}$. It turns out that this condition is sufficient for $*$-preservability of I_1 but it is not necessary.*

IV. Generalization to multiple user MACs

Definition 14. *Let $W : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}$. For every $S \subset \{1, \ldots, m\}$, we define the two-user MAC $W_S : G_S \times G_{S^c} \longrightarrow \mathcal{Z}$ as $W_S(y|x_S, x_{S^c}) = W(y|x_1, \ldots, x_m)$.*

Remark 5. *It is easy to see that for every $s \in \{-,+\}^*$ and every $S \subset \{1, \ldots, m\}$, we have $(W^s)_S = (W_S)^s$. Therefore, Polarization $*$-preserves I_S for W if and only if Polarization $*$-preserves I_1 for W_S.*

Theorem 2. *Let $W : G_1 \times \ldots \times G_m \longrightarrow \mathcal{Z}$. Polarization $*$-preserves I_S for W if and only if W_S is polarization compatible.*

Proof: Direct corollary of Theorem 1 and Remark 5. ■

V. Discussion and Conclusion

The necessary and sufficient condition that we provided is a single letter characterization: the mapping $\hat{f}_W$ can be directly computed using the transition probabilities of W. Moreover, since the number of pseudo quadratic functions is finite, checking whether $\hat{f}_W$ is extendable to a pseudo quadratic function can be accomplished in a finite number of computations.

References

[1] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 3051 –3073, 2009.

[2] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 28 2009.

[3] E. Şaşoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," in *Information Theory Workshop, 2009. ITW 2009. IEEE*, 2009, pp. 144 –148.

[4] W. Park and A. Barg, "Polar codes for q-ary channels,," *Information Theory, IEEE Transactions on*, vol. 59, no. 2, pp. 955–969, 2013.

[5] A. Sahebi and S. Pradhan, "Multilevel polarization of polar codes over arbitrary discrete memoryless channels," in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, 2011, pp. 1718–1725.

[6] E. Şaşoğlu, "Polar codes for discrete alphabets," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, 2012, pp. 2137–2141.

[7] R. Nasser and E. Telatar, "Polarization theorems for arbitrary DMCs," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, 2013, pp. 1297–1301.

[8] ——, "Polar codes for arbitrary DMCs and arbitrary MACs," *CoRR*, vol. abs/1311.3123, 2013. [Online]. Available: http://arxiv.org/abs/1311.3123

[9] E. Şaşoğlu, E. Telatar, and E. Yeh, "Polar codes for the two-user multiple-access channel," *CoRR*, vol. abs/1006.4255, 2010. [Online]. Available: http://arxiv.org/abs/1006.4255

[10] E. Abbe and E. Telatar, "Polar codes for the -user multiple access channel," *Information Theory, IEEE Transactions on*, vol. 58, no. 8, pp. 5437 –5448, aug. 2012.

[11] R. Nasser, "Ergodic theory meets polarization. I: An ergodic theory for binary operations," *CoRR*, vol. abs/1406.2943, 2014. [Online]. Available: http://arxiv.org/abs/1406.2943

[12] ——, "Ergodic theory meets polarization. II: A foundation of polarization theory," *CoRR*, vol. abs/1406.2949, 2014. [Online]. Available: http://arxiv.org/abs/1406.2949