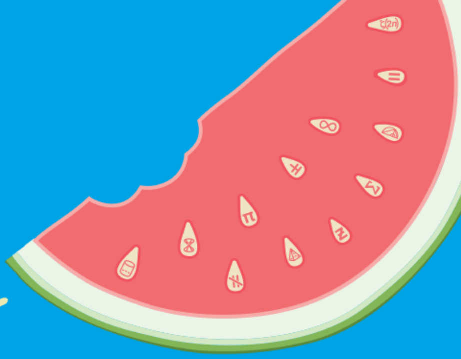
AMSI VACATIONRESEARCH SCHOLARSHIPS 2021–22

Get a taste for Research this Summer



Cocyclic Generalised Hadamard Matrices

Peter Gill

Supervised by Dr Santiago Barrera Acevedo

Monash University

AMSI AUSTRALIAN MATHEMATICAL SCIENCES INSTITUTE

1 Abstract

The five-fold constellation (or simply the constellation) is a mutual equivalence among five combinatorial objects with an underlying fixed group; depending on the type of group extension, a different kind of equivalence is exhibited. One of the objects in the constellation are the coupled cocyclic generalised Hadamard. In this work, we study coupled cocyclic generalised Hadamard matrices, and their place within the constellation via group extensions. We observe that for the binary case (standard binary Hadamard matrices), Hadamard full propelinear codes can be appended to the constellation.

2 Introduction

A square $n \times n$ matrix over $\{\pm 1\}$ is *Hadamard* if $HH^T = nI_n$, where I_n is the $n \times n$ identity matrix. The order n of a Hadamard matrix must be either 1, 2 or $4k$ for some integer k. The converse of this statement is known as the Hadamard conjecture, which proposes that for any positive integer k there is a Hadamard matrix of order $4k$. Currently, the Hadamard conjecture and is unresolved.

The most prolific way currently known of constructing Hadamard matrices is via cocycles (see Definition 4.3), as many classical constructions (such as Sylvester, Williamson, Ito, Paley) happen to be cocyclic as well [3]. Cocyclic Hadamard matrices could provide a uniform approach to solving the Hadamard conjecture. Perhaps another direction of attack is through generalising Hadamard matrices and studying their properties, especially those that are preserved when reducing generalised Hadamard matrices back to Hadamard matrices.

To this end, we have the constellation (see Theorem 5.1) which is a mutual equivalence of five combinatorial objects, one of them being the coupled cocyclic generalised Hadamard matrices. Moreover, the objects in the constellation can be constructed using group extensions. Depending on the type of group extension (normal, splitting, abelian kernel, central, abelian, binary), a different equivalence is seen among the objects. Horadam [3] presented this constellation first, though there were many partial results beforehand.

The outline of the report is as follows. Section 2 of this report sets our notation and preliminaries. Section 3 details the necessary group extension theory to display the constellation, more details can be found in the Appendix. Section 4 introduces the five objects in the constellation: coupled cocyclic generalised Hadamard matrices, orthogonal factor pairs, relative difference sets, divisible designs, and base sequences. Section 5 exhibits the constellation as seen in [3]. Section 6 defines Hadamard full propelinear codes and outlines their equivalence with the five objects in the constellation, though only under the central binary group extension case.

Most material and ideas in this report come from [3], we simply provide exposition.

2.1 Statement of Authorship

- Peter Gill read the literature, filled in details of some proofs, and wrote this report.
- Santiago Barrera Acevedo supervised the project, read the literature, helped with details in proofs, proofread and provided feedback on this report.

2.2 Notation and Preliminaries

We assume standard knowledge of group theory.

If $f : A \to B$ is a map, and $A' \subseteq A$ then $f[A'] \coloneqq \{f(a') \mid a' \in A'\}$. If a set A has an equivalence relation, then $[a]$ denotes the equivalence class containing $a \in A$.

Now let G be a group. We denote the identity element of a group G as 1 when G is multiplicatively writte, and 0 when G is additively written. The symmetric group of bijective maps on $\{1, \cdots, n\}$ under composition is denoted S_n. The identity map on a set A is denoted Id_A. If α is a map whose domain is G, then $g^\alpha \coloneqq \alpha(g)$. If $f : A \to G$ is a map, then f^{-1} denotes the map $f^{-1} : A \to G$ defined by $f^{-1}(a) = (f(a))^{-1}$, unless otherwise specified. The *opposite automorphism group* $\mathrm{Aut}(G)^{\mathrm{op}}$ is the group of automorphisms of G under the operation $\alpha_1\alpha_2 \coloneqq \alpha_1 \circ \alpha_2$. If $g \in G$, then $\overline{g} \in \mathrm{Aut}(G)^{\mathrm{op}}$ denotes the inner automorphism mapping $x \mapsto gxg^{-1}$ for all $x \in G$. If U is a subgroup of G (written $U \leq G$), then a set T containing exactly one element from each (left) coset of U is a *transversal of U in G*. Additionally, if T contains the identity of G, then T is a *normalised* transversal.

Throughout the rest of this report, U and G are finite groups of order u and n respectively.

3 Group Extensions and Factor Pairs

Underlying the constellation is the idea of group extensions. The objects and the kind of equivalence in the constellation depends on the type of group extension.

Here we introduce the necessary group extension and cohomology theory for the constellation, most of which comes from Galati [2], although we have adapted the exposition to focus on the bijective mapping between classes of group extensions and classes of factor pairs. For details on some of these results, see the Appendix.

Definition 3.1. *A* group extension of U by G *is a short exact sequence*

$$U \overset{i}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G,$$

that is, i is an injective homomorphism, π is a surjective homomorphism, and $\ker \pi = i[U]$.

We denote the set of group extensions of U by G with $\mathrm{GExt}(G, U)$, and define a natural equivalence relation on $\mathrm{GExt}(G, U)$.

Definition 3.2. *Let $e_1 : U \overset{i_1}{\rightarrowtail} E_1 \overset{\pi_1}{\twoheadrightarrow} G$ and $e_2 : U \overset{i_2}{\rightarrowtail} E_2 \overset{\pi_2}{\twoheadrightarrow} G$ be group extensions of U by G. We say e_1 is* equivalent to e_2 via γ *if there is an isomorphism $\gamma : E_1 \to E_2$ such that the diagram*

$$\begin{tikzcd}
& E_1 \arrow[dd, "\gamma"] \arrow[dr, two heads, "\pi_1"] & \\
U \arrow[ur, tail, "i_1"] \arrow[dr, tail, "i_2"'] & & G \\
& E_2 \arrow[ur, two heads, "\pi_2"'] &
\end{tikzcd}$$

commutes - that is, $i_2 = \gamma \circ i_1$ and $\pi_1 = \pi_2 \circ \gamma$. We say $e_1 \sim_\gamma e_2$ when e_1 is equivalent to e_2 via γ.

There are many types of group extensions, each giving a different equivalence in the constellation, and we exhibit a few here. Fix some group extension $e : U \overset{i}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$ of U by G. If there are no extra conditions on e, we say e is a *normal* group extension. The extension e is *split* if there is some subgroup $H \leq E$ such that $E = HU \coloneqq \{hu : h \in H, u \in U\}$ and $H \cap U = \{1\}$. We say e is an *abelian kernel* extension if U is abelian. We say e is a *central* extension if U is a central subgroup of E, meaning $ue = eu$ for all $u \in U$ and $e \in E$. Note U must be abelian in this case. We say e is an *abelian* extension if E is abelian, implying U and G must also be abelian. Finally, if $U \cong \mathbb{Z}_2$ is central in E, we say e is a *binary* extension. This last case is of interest as it reduces the theory down to $\mathbb{Z}_2$; in particular, generalised Hadamard matrices become, simply, Hadamard matrices in the constellation.

One way of constructing group extensions is via factor pairs.

Definition 3.3. *A* factor pair (ψ, ϵ) of U by G *is a pair of maps $\psi : G \times G \to U$ and $\epsilon : G \to \mathrm{Aut}(U)^{\mathrm{op}}$ such that for all $x, y, z \in U$,*

$$\epsilon(x) \circ \epsilon(y) = \overline{\psi(x, y)} \circ \epsilon(xy), \tag{3.1}$$

$$\psi(x, y)\psi(xy, z) = \psi(y, z)^{\epsilon(x)}\psi(x, yz). \tag{3.2}$$

We call ψ the factor set*, and ϵ the* coupling*. If $\psi(x, 1) = \psi(1, x) = 1$, then the factor pair (ψ, ϵ) is* normalised.

We denote the set of all factor pairs of U by G with $F^2(G, U)$.

As promised, group extensions indeed can arise from factor pairs.

Definition 3.4. *Let $(\psi, \epsilon) \in F^2(G, U)$. Then $E_{(\psi,\epsilon)}$ is the group with underlying set $U \times G$ and operation*

$$(a, x)(b, y) = (ab^{\epsilon(x)}\psi(x, y), xy)$$

for all $a, b \in U$ and $x, y \in G$. Moreover,

$$U \overset{\iota}{\rightarrowtail} E_{(\psi,\epsilon)} \overset{\kappa}{\twoheadrightarrow} G$$

is a (canonical) group extension of U by G, where ι and κ are the canonical injection $a \overset{\iota}{\mapsto} (a, 1)$ and projection $(a, x) \overset{\kappa}{\mapsto} x$ homomorphisms respectively.

As with group extensions, there is a natural equivalence relation on $F^2(G, U)$.

Definition 3.5. *Let $(\psi_1,\epsilon_1),(\psi_2,\epsilon_2)\in F^2(G,U)$. We say (ψ_1,ϵ_1)* is equivalent to *(ψ_2,ϵ_2)* via *ϕ if there is some map $\phi : G\to U$ with $\phi(1)=1$ such that for all $x,y\in G$,*

$$\epsilon_2(x)=\overline{\phi(x)}\circ\epsilon_1(x),$$
$$\psi_2(x,y)=\phi(x)\phi(y)^{\epsilon_1(x)}\psi_1(x,y)\phi^{-1}(xy).$$

Recall that in this section the main result underlying the constellation is a bijection

$$\xi : \mathrm{GExt}(G,U)/\sim\;\longrightarrow F^2(G,U)/\sim .$$

This bijection is driven by transversals in group extensions.

Theorem 3.1. ([2] Proposition 3.2) *Let $e : U\overset{i}{\rightarrowtail} E\overset{\pi}{\twoheadrightarrow} G$ be a group extension of U by G, and $T=\{t_x\in E : x\in G,\pi(t_x)=x\}$ be a normalised transversal of $i[U]$ in E. Then (ψ_T,ϵ_T) defined by*

$$\epsilon_T(x)=i^{-1}\circ\overline{t_x}\circ i,$$
$$\psi_T(x,y)=i^{-1}(t_xt_yt_{xy}^{-1})$$

for all $x,y\in G$ is a factor pair of U by G, where i^{-1} is the inverse map of i. Define ξ by mapping $[e]\mapsto[\psi_T,\epsilon_T]$ (with some abuse of notation, denoting the equivalence class containing (ψ_T,ϵ_T) by $[\psi_T,\epsilon_T]$). Then ξ is a bijection.

Indeed, ξ is well-defined by the following two lemmas.

Lemma 3.1. ([2] Proposition 3.2) *If $T=\{t_x\in E : x\in G,\pi(t_x)=x\}$ and $T^*=\{t_x^*\in E : x\in G,\pi(t_x^*)=x\}$ are normalised transversals of $i[U]$ in E, then $(\psi_{T*},\epsilon_{T*})\sim_\phi(\psi_T,\epsilon_T)$ with ϕ defined by $\phi(x)=i^{-1}(t_x^*t_x^{-1})$ for all $x\in G$.*

Lemma 3.2. *Let $e_1 : U\overset{i_1}{\rightarrowtail} E_1\overset{\pi_1}{\twoheadrightarrow} G$ and $e_2 : U\overset{i_2}{\rightarrowtail} E_2\overset{\pi_2}{\twoheadrightarrow} G$ be group extensions of U by G with $e_1\sim_\gamma e_2$, and let $T=\{t_x\in E_1 : x\in G,\pi_1(t_x)=x\}$ be a transversal of $i_1[U]$ in E_1. Then $S\coloneqq\gamma[T]$ is a transversal of $i_2[U]$ in E_2, and $(\psi_T,\epsilon_T)=(\psi_S,\epsilon_S)$ (in particular, $(\psi_T,\epsilon_T)\sim(\psi_S,\epsilon_S)$).*

We have that ξ is injective by the following lemma.

Lemma 3.3. ([2] Proposition 3.3) *Let $e_1 : U\overset{i_1}{\rightarrowtail} E_1\overset{\pi_1}{\twoheadrightarrow} G$ and $e_2 : U\overset{i_2}{\rightarrowtail} E_2\overset{\pi_2}{\twoheadrightarrow} G$ be group extensions of U by G, and let $T=\{t_x\in E_1 : x\in G,\pi_1(t_x)=x\}$ and $S=\{s_x\in E_2 : x\in G,\pi_2(s_x)=x\}$ be transversals of $i_1[U]$ in E_1 and of $i_2[U]$ in E_2 respectively, with $(\psi_S,\epsilon_S)\sim_\phi(\psi_T,\epsilon_T)$. Then $e_1\sim_\gamma e_2$, where γ is defined by*

$$\gamma(i_1(a)t_x)=i_2(a\phi^{-1}(x))s_x$$

for all $a\in U$ and $x\in G$.

The surjectivity of ξ follows from the next lemma.

Lemma 3.4. ([2] Proposition 3.4) *Let $(\psi,\epsilon)\in F^2(G,U)$. Then $T=\{(1,x)\in E_{(\psi,\epsilon)} : x\in G\}$ is a normalised transversal of $\iota[U]=U\times\{1\}$ in $E_{(\psi,\epsilon)}$ with $(\psi_T,\epsilon_T)=(\psi,\epsilon)$.*

In fact, every factor pair can be constructed from a transversal in any extension group E.

Lemma 3.5. ([2] Proposition 3.2) *Given any factor pair $(\psi, \epsilon) \in [\psi_T, \epsilon_T]$ where $T = \{t_x \in E : x \in G, \pi(t_x) = x\}$ is a transversal of $i[U]$ in E, there is some transversal S of $i[U]$ in E such that $(\psi, \epsilon) = (\psi_S, \epsilon_S)$.*

As a consequence of the bijectivity of ξ, every group extension is equivalent to some group extension built from a factor pair as in Definition 3.4. So factor pairs are, at least up to equivalence, a comprehensive way of constructing group extensions.

Corollary 3.1. ([2] Corollary 3.1) *Let $e : U \overset{i}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$ be a group extension and $T = \{t_x \in E_1 : x \in G, \pi(t_x) = x\}$ a normalised transversal of $i[U]$ in E. Then e is equivalent to the canonical extension $e' : U \overset{\iota}{\rightarrowtail} E_{(\psi_T, \epsilon_T)} \overset{\kappa}{\twoheadrightarrow} G$ via γ defined by*

$$i(a)t_x \mapsto (a, x)$$

for all $a \in U$ and $x \in G$. Furthermore, if $(\psi, \epsilon) \sim_\phi (\psi_T, \epsilon_T)$, then e is equivalent to the canonical extension $e' : U \overset{\iota}{\rightarrowtail} E_{(\psi, \epsilon)} \overset{\kappa}{\twoheadrightarrow} G$ via δ defined by

$$i(a)t_x \mapsto (a\phi^{-1}(x), x)$$

for all $a \in U$ and $x \in G$.

Now fix some group extension $e : U \overset{i}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$. In the case where e is a split group extension, we have that $\xi([e])$ is of the form $[1, \varrho]$, where the coupling $\varrho : G \to \mathrm{Aut}(U)^{\mathrm{op}}$ is a homomorphism and the factor set $1 : G \times G \to U$ is the trivial map that sends everything in $G \times G$ to the identity in U. We usually reserve the symbol ϱ to indicate that a coupling of a factor pair is a homomorphism.

Corollary 3.2. ([2] Proposition 3.5) *Let $(\psi, \epsilon), (1, \varrho) \in F^2(G, U)$. Then $E_{(\psi,\epsilon)} \cong E_{(1,\varrho)}$ if and only if $(\psi, \epsilon) \sim_\varrho (1, \varrho)$. Also, $E_{(1,\varrho)} = U \rtimes_\varrho G$.*

4 Objects of the Constellation

We introduce the five objects of the constellation as seen in Horadam's exhibition of the constellation [3]. A common theme throughout is that the most general equivalence in the constellation is not enough to capture the most general kinds of the objects - that is, there are some instances of these objects that cannot be reached by the constellation. So studying these objects without the constellation can still be fruitful.

4.1 Cocyclic Generalised Hadamard Matrices

Recall that a Hadamard matrix is an $n \times n$ matrix over $\{\pm 1\}$ such that $HH^T = nI_n$. A Hadamard matrix $H = [h_{ij}]_{1 \leq i,j \leq n}$ of order n has the *row pairwise balanced* property, which is that for any distinct rows with indices $1 \leq i, j \leq n$, the sequence $\{h_{ik}h_{jk}^{-1}\}_{1 \leq k \leq n}$ contains every element of $\{\pm 1\}$ exactly $n/2$ times. In fact, one can quickly show the row pairwise balanced property characterises Hadamard matrices over all square matrices with entries in $\{\pm 1\}$. This property serves as the inspiration for our definition of a generalised Hadamard matrix.

Definition 4.1. ([3] Definition 4.9) *An $n \times n$ matrix $H = [h_{ij}]_{1 \leq i,j \leq n}$ with entries in a finite group U of order u is a* generalised Hadamard matrix *if, for any two distinct rows $1 \leq i, j \leq n$, the sequence $\{h_{ik}h_{jk}^{-1}\}_{1 \leq k \leq n}$ contains each element of U exactly n/u times. In this case, we say H is a* $\mathrm{GH}(u, n/u)$ *over U.*

Note when U is the group $\{\pm 1\}$ under multiplication that this definition reduces back to a Hadamard matrix (since the row pairwise property characterises Hadamard matrices).
There is a natural equivalence relation on the set of all $n \times n$ generalised Hadamard matrices over U.

Definition 4.2. ([3] Definition 4.12) *Two $n \times n$ matrices A and B with entries in U are* Hadamard equivalent *if B is obtained from A through a finite sequence of the following operations:*

1. *permuting the rows or columns,*
2. *right-multiplying a column by an element in U,*
3. *left-multiplying a row by an element in U,*
4. *applying a fixed automorphism of U to every entry.*

We write $A \sim B$ when A is equivalent to B.

Importantly, the generalised Hadamard matrix property is preserved by this equivalence relation - that is, if $A \sim B$ then A is a $\mathrm{GH}(u, n/u)$ if and only if B is a $\mathrm{GH}(u, n/u)$. Observe that we can always find a *normalised* (meaning the initial row and column are full of 1s) representative in a class of Hadamard equivalent matrices by using operations 2 and 3 accordingly, though normalised representatives may not be unique (simply by permuting appropriate rows and/or columns).

Many classical constructions of Hadamard matrices (so, in the case $U = \{\pm 1\}$) are also cocyclic [3]. Thus cocycles are an important object of study for Hadamard matrices and could perhaps be a strong strategy to tackle the Hadamard conjecture.

Definition 4.3. *Let U be abelian. A* 2-cocycle *ψ, or simply a* cocycle, *is a map $\psi : G \times G \to U$ satisfying*

$$\psi(x, y)\psi(xy, z) = \psi(y, z)^{\epsilon(x)}\psi(x, yz)$$

for all $x, y, z \in G$, where $\epsilon : G \to \mathrm{Aut}(U)^{\mathrm{op}}$ is some fixed homomorphism. If $\psi(x, 1) = \psi(1, x) = 1$, then the cocycle is normalised.

The set of cocycles $\psi : G \times G \to U$ with a fixed homomorphism $\epsilon : G \to \mathrm{Aut}(U)^{\mathrm{op}}$ is denoted $Z_\epsilon^2(G, U)$.
It is quite natural to build a matrix from a cocycle.

Definition 4.4. ([3] Definition 6.3) *An $n \times n$ matrix M with entries in U is G-*cocyclic *if there is a cocycle $\psi : G \times G \to U$ and an ordering $g_1, \cdots, g_n$ of G with $g_1 = 1$ such that M is Hadamard equivalent to*

$$M_\psi := [\psi(g_i, g_j)]_{1 \leq i,j \leq n}.$$

One may notice that a factor pair (Definition 3.3) is almost a generalisation of a cocycle, the only caveats being that $\epsilon : G \to \mathrm{Aut}(U)^{\mathrm{op}}$ must be a homomorphism and U must be abelian for ψ to be a cocycle, however ϵ can simply be a map in the definition of a factor pair. We hence define a coupled cocyclic matrix, which is built from a factor pair in a similar way that cocyclic matrices are built from cocycles, to almost obtain a generalisation of cocyclic matrices.

Definition 4.5. ([3] Definition 7.18) *An $n \times n$ matrix M with entries in U is* coupled G-cocyclic over U *if there is a factor pair $(\psi, \epsilon) \in F^2(G, U)$ and an ordering $g_1, \cdots, g_n$ of G with $g_1 = 1$ such that M is Hadamard equivalent to*

$$M_{(\psi,\epsilon)} := \left[\psi^{-1}(g_i, g_j)^{\epsilon(g_i)^{-1}}\right]_{1\leq i,j\leq n}.$$

The reason behind the negative signs in the definition of $M_{(\psi,\epsilon)}$ above is so that Theorem 10.1 in [2] reads quickly - namely, $M_{(\psi,\epsilon)}$ is a generalised Hadamard matrix if and only if (ψ, ϵ) is orthogonal (see Definition 4.7).

We remark the coupled G-cocyclic matrix $M_{(\psi,\epsilon)}$ is G-cocyclic when U is abelian and $\epsilon = 1$ is trivial, as then the inversion map $x \mapsto x^{-1}$ is an automorphism on U, and so it follows that $M_{(\psi,1)} \sim M_{\psi}$.
In fact, coupled cocyclic matrices are the most general kind of generalised Hadamard matrices possibly studied in the constellation, because they correspond with normal group extensions - the most general kind of group extension.

There is another family of matrices over U that are special cases of coupled cocyclic matrices, but this time constructed from maps $\phi : G \to U$ with $\phi(1) = 1$. They correspond with the splitting group extension case in the constellation.

Definition 4.6. ([3] Definition 7.20) *An $n \times n$ matrix M with entries in U is a* coupled G-developed matrix over U *if there is a map $\phi : G \to U$ with $\phi(1) = 1$, a homomorphism $\varrho : G \to \mathrm{Aut}(U)^{\mathrm{op}}$, and an ordering $g_1, \cdots, g_n$ of G with $g_1 = 1$ such that*

$$M = \left[\phi(g_i g_j)^{\varrho(x_i^{-1})}\right]_{1\leq i,j\leq n}.$$

If ϱ is trivial, then we simply say M is G-developed.

Note that coupled G-developed matrices are coupled G-cocyclic (see [3] Lemma 7.24).
Unfortunately, there do exist generalised Hadamard matrices that are not coupled cocyclic (for instance, see [3] lemma 7.46), hence one may still benefit from studying a different aspect of Hadamard matrices without the constellation.

4.2 Orthogonal Factor Pairs

Orthogonality is the property of factor pairs characterising the existence of the other objects in the constellation. Galati [2] introduced the most general definition of orthogonal factor pairs to characterise factor pairs with relative difference sets and generalised Hadamard matrices.

Definition 4.7. ([2] Definition 4.1) *Let $(\psi, \epsilon) \in F^2(G, U)$ and $D \subseteq G$ with $|D| = k$. We say (ψ, ϵ) is (n, u, k, λ)-*orthogonal with respect to D *if for any $x \in G \setminus \{1\}$ the sequence $\{\psi(x, y)\}_{y \in D \cap x^{-1}D}$ lists each element of U exactly λ times.*

*If, in addition, N is abelian and ϵ maps everything to $\mathrm{Id}_U \in \mathrm{Aut}(U)^{\mathrm{op}}$, then we say ψ is (n, u, k, λ)-*orthogonal with respect to D*, omitting reference to ϵ.*

If $k = n$, necessarily $D = G$ and $\lambda = n/u$, and we then say (ψ, ϵ) is orthogonal, *omitting reference to the parameters (n, u, k, λ), since all parameters rely on the group orders n and u.*

Of course, if the above two cases hold (so N is abelian, ϵ is trivial, and $k = n$), we say ψ is orthogonal, omitting reference to everything but ψ.

Note ϵ does not affect whether a factor pair (ψ, ϵ) is orthogonal or not, however we keep it coupled with ψ when discussing orthogonality of factor pairs. This proves helpful, for example, when constructing a coupled cocyclic generalised Hadamard matrix from an orthogonal factor pair in the constellation.
The most general equivalence in the constellation (the one corresponding with a normal group extension), requires $k = n$. So, sadly, the constellation does not comprehensively cover all orthogonal factor pairs.

4.3 Relative Difference Sets

Relative difference sets are primarily objects from design theory.

Definition 4.8. ([3] Definition 4.18) *Let H be a group of order nu, and U a normal subgroup of H of order u. A* relative difference set R in H relative to U *is a k-element subset $R \subseteq H$ such that the sequence $\{r_1 r_2^{-1}\}_{(r_1, r_2) \in R'}$ lists each element in $H \setminus U$ exactly λ times, and no element in U, where $R' = \{(r_1, r_2) \in R \times R \mid r_1 \neq r_2\}$. In this case, we say R is a (n, u, k, λ)-*RDS *in H relative to U. If R contains the identity of H, then R is* normalised.

The most general equivalence in the constellation asks for $k = n$ and $\lambda = n/u$, and the relative difference sets that arise are termed *semiregular*. Semiregular relative difference sets have parameters of the form $(n, u, n, n/u)$ and are the maximal kind of relative difference sets possibly studied in the constellation.

4.4 Divisible Designs

Divisible designs are another object primarily from design theory. We use the definitions given by Horadam [3].

Definition 4.9. *A* divisible (n, u, k, λ)-design (P, B) *is a pair of nu* points P *and b* blocks B *which are subsets of P, along with a partition of P into n* point classes *each of size u. Let $p_1, p_2 \in P$. If p_1 and p_2 are in the same point class, then there are no blocks containing both p_1 and p_2. If p_1 and p_2 are in distinct point classes, then there are exactly λ blocks containing both p_1 and p_2. If $|B| = nu = |P|$ then (P, B) is a* square *divisible (n, u, k, λ)-design.*

Note some authors allow some fixed non-zero integer number of blocks containing distinct points in the same point class, but we are not interested in that case. Some also refer to the point classes as groups, however we avoid this terminology to avoid confusion with the algebraic concept of a group.

At first glance, perhaps it is unclear how to relate the information of a group extension to a divisible design. To this end, the notion of automorphisms of a divisible designs is needed.

Definition 4.10. *Let $\mathcal{D} = (P, B)$ be a divisible (n, u, k, λ)-design. We say a bijection α on $P \cup B$ (note $P \cap B = \emptyset$ by definition of a divisible design) is an* automorphism *of $\mathcal{D}$ if α preserves the divisible design structure of $\mathcal{D}$. This means, for any $p, p' \in P$ and $b \in B$, that $\alpha(p) \in P$, and $\alpha(b) \in B$, and $p \in b$ if and only if $\alpha(p) \in \alpha(b)$, and finally p and p' are in the same point class if and only if $\alpha(p)$ and $\alpha(p')$ are in the same point class.*

The set of all automorphisms of $\mathcal{D}$ under composition forms a group $\mathrm{Aut}(\mathcal{D})$ called the *full automorphism group* of $\mathcal{D}$.

Now we can introduce the idea of *regularity* of divisible designs.

Definition 4.11. *A square divisible (n, u, k, λ)-design is* regular with respect to a group U *if there is an automorphism group $U \leq \mathrm{Aut}(\mathcal{D})$ of the design that acts regularly on the points P, meaning that for any $p_1, p_2 \in P$, there is exactly one $\alpha \in U$ such that $\alpha(p_1) = p_2$.*

Definition 4.12. *A square divisible (n, u, k, λ)-design is* class regular with respect to a group U *if there is an automorphism group $U \leq \mathrm{Aut}(\mathcal{D})$ of the design that acts regularly on each point class, meaning that for any point class Q and any $p_1, p_2 \in Q$, there is exactly one $\alpha \in U$ such that $\alpha(p_1) = p_2$.*

With class regular and regular divisible designs, there is enough algebraic scaffolding to connect divisible designs to group extensions for the constellation. However, as the constellation requires $k = n$ and $\lambda = n/u$, like with relative difference sets, the divisible designs that arise are termed *semiregular*, and must have parameters of the form $(n, u, n, n/u)$.

4.5 Base Sequences and Perfect Nonlinear Functions

Base sequences and perfect nonlinear functions have their roots in signal processing and cryptography, as they have ideal auto-correlation properties. We use the definitions given by Horadam [3].

Definition 4.13. ([3] Definition 7.39) *Consider a list $(1, 1), \cdots, (\nu_s, \eta_s)$ of representatives for the equivalence classes in $F^2(G, U)$. Let $(\psi, \epsilon) \in F^2(G, U)$. There is thus a unique representative (ν_i, η_i) such that $(\psi, \epsilon) \sim_\phi (\nu_i, \eta_i)$ for some $\phi : G \to U$ with $\phi(1) = 1$. If (ψ, ϵ) is orthogonal, we say ϕ (or equivalently, the list of values $(\phi(x))_{x \in G}$) is a* base sequence with respect to *(ν_i, η_i).*

In the splitting group extension case of the constellation, base sequences reduce to *perfect nonlinear functions* (see [3] Theorem 7.40).

Definition 4.14. ([3] Definition 7.34) *Let u divide n, let $\phi : G \to U$ be a map with $\phi(1) = 1$, and let $\varrho : G \to \mathrm{Aut}(U)^{\mathrm{op}}$ be a homomorphism. Set*

$$M := \left[\phi(g_i g_j)^{\varrho(x_i^{-1})}\right]_{1\le i,j\le n}$$

(which is a coupled G-developed matrix). Then ϕ is perfect nonlinear relative to ϱ *if M is a* $\mathrm{GH}(u, n/u)$ *over U. If ϱ is trivial, we simply say ϕ is* perfect nonlinear*.*

These definitions make base sequences and perfect non-linear functions trivially equivalent to orthogonal factor pairs and coupled G-developed generalised Hadamard matrices respectively. However, it is their applications that make them desirable objects of study.

5 The Constellation

We present the constellation under the most general group extension - a normal group extension. Horadam gathered these objects altogether first [3], however partial results towards this equivalence were known beforehand.

Theorem 5.1. ([3] Theorem 7.29 and 7.40) *Consider a group extension $e : U \overset{i}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$ of U by G and let $\xi([e]) = [\varphi, \tau]$ be the associated equivalence class of factor pairs. Then the following statements are equivalent:*

1. *There is a coupled G-cocyclic* $\mathrm{GH}(u, n/u)$ *over U.*

2. *There is an orthogonal factor pair in $[\varphi, \tau]$.*

3. *There is a normal $(n, u, n, n/u)$-*RDS *in E relative to $i[U]$.*

4. *There is a $(n, u, n, n/u)$-divisible design with regular group E and class regular with respect to $i[U]$.*

5. *There is a base sequence ϕ with respect to $(\psi, \epsilon) \in [\varphi, \tau]$.*

An important remark here is that the equivalence is constructive, due to the constructiveness of the partial results Horadam collected. One of which is Theorem 5.1 in [2], which reveals an equivalence between orthogonal factor pairs and (normal) relative difference sets.

Lemma 5.1. ([2] Theorem 5.1) *Using the same terminology as in theorem 5.1 above, and letting $D \subseteq E$ be a size k subset, the following statements are equivalent:*

1. *There is a (n, u, k, λ)-*RDS *R in E relative to $i[U]$ with $\pi[R] = D$.*

2. *There is $(\psi, \epsilon) \in [\varphi, \tau]$ that is (n, u, k, λ)-orthogonal with respect to D.*

3. *There is $(\psi, \epsilon) \in [\varphi, \tau]$ such that $R_{(\psi,\epsilon)} := \{(1, x) : x \in D\}$ is an (n, u, k, λ)-*RDS *in $G_{(\psi,\epsilon)}$ relative to $U \times \{1\}$ with $\pi[R_{(\psi,\epsilon)}] = D$.*

Moreover, when the above statements are true, (ψ, ϵ) can be written in the form (ψ_T, ϵ_T) where T is a transversal of $i[U]$ in G containing R', where R' satisfies $R' = Rb$, and $R' \cap i[U] \in \{\emptyset, \{1\}\}$, and $\pi[R'] = D$.

The proof of 5.1 in [2] gives full details on the construction. For instance, constructing 1. from 3. is done by taking a transversal T such that $(\psi, \epsilon) = (\psi_T, \epsilon_T)$ (which exists by Lemma 3.5), then defining $R \coloneqq \gamma^{-1}[R_{(\psi,\epsilon)}]$ where $\gamma^{-1} : E_{(\psi,\epsilon)} \to E$ maps $(a, x) \mapsto i(a)t_x$ (see Corollary 3.1).

Observe that Lemma 5.1 characterises kinds of orthogonal factor pairs and of relative difference sets that are more general than those found in Theorem 5.1. This generality is lost when we extend to the full equivalence between each of the five objects in the constellation. In particular, for this case, the culprit is the equivalence with the coupled G-cocyclic generalised Hadamard matrices, by which Horadam used Theorem 10.1 in [2].

Lemma 5.2. ([2] Theorem 10.1) *Let u divide n (recall $u = |U|$ and $n = |G|$ are the respective orders of the groups U and G). Let $(\psi, \epsilon) \in F^2(G, U)$. Then (ψ, ϵ) is orthogonal if and only if the coupled G-cocyclic matrix*

$$M_{(\psi,\epsilon)} \coloneqq \left[\psi^{-1}(g_i, g_j)^{\epsilon(g_i)^{-1}}\right]_{1 \leq i,j \leq n}$$

is a $\mathrm{GH}(u, n/u)$ over U.

For completeness, here is a constructive equivalence between relative difference sets and divisible designs.

Lemma 5.3. ([3] Theorem 4.20) *Let E be a group of order nu with normal subgroup U of order u. Let $R \subseteq E$ be a size k subset of E. Then R is a (n, u, k, λ)-RDS in E relative to N if and only if $(E, \{Re : e \in E\})$ is a (n, u, k, λ)-divisible design with point class partition $\{Ne : e \in E\}$, regular group E acting on points by $e(h) \coloneqq he$ and on blocks by $e(Rh) \coloneqq R(he)$ for all $h, e \in E$, and class regular with respect to U.*

And of course, the characterisation of base sequences in the constellation follows from their definition.

To see the constellation under other types of group extensions, see [3, section 7.4].

6 Hadamard Full Propelinear Codes

We discuss a different object now that is equivalent to the objects in the constellation, albeit under a binary extension. Hadamard full propelinear codes were introduced in [4] and their equivalence with Hadamard groups is proven in [5]. We use the definitions from the latter paper [5].

For this section, we let $\mathbb{Z}_2 = \{0, 1\}$ be the cyclic group of order 2 under addition mod 2, and consider Hadamard matrices to be over $\mathbb{Z}_2$ rather than $\{\pm 1\}$ (the isomorphism $\beta : \{\pm 1\} \to \mathbb{Z}_2$ mapping $1 \mapsto 0$ and $-1 \mapsto 1$ translates between these two representations of Hadamard matrices). A *binary code C of length m* is a non-empty subset of $\mathbb{Z}_2^m$, and the elements of C are called codewords. We let $\mathbf{0} = (0, \cdots, 0) \in \mathbb{Z}_2^m$ denote the m-tuple of all 0s, and similarly $\mathbf{1} \in \mathbb{Z}_2^m$ the m-tuple of all 1s.

We define what it means for a code to have *propelinear* structure.

Definition 6.1. ([5] Definition 1.2) *A binary code C of length m containing* $\mathbf{0}$ *has a* propelinear structure *if for each codeword $x \in C$, there is a permutation $\pi_x \in S_m$ such that for all $y \in C$:*

1. $z \in C$,

2. $\pi_x \circ \pi_y = \pi_z$,

where $z := x + \pi_x(y)$ *and* π_x *maps* y *via* $(y_1, \cdots, y_m) \mapsto \left(y_{\pi_x^{-1}(1)}, \cdots, y_{\pi_x^{-1}(m)}\right)$. *In this case, we also say* C *is a propelinear code.*

Note the natural group operation $*$ on C arising from this definition, namely $x * y := x + \pi_x(y)$ for all $x, y \in C$. Furthermore, we quickly see $\pi_{\mathbf{0}}$ must be the identity permutation in S_m (let $y = \mathbf{0}$ in condition 2) and $\pi_{\mathbf{1}}^{-1} = \pi_{\mathbf{1}}$ (let $x = y = \mathbf{1}$ in condition 2).

Let H be a Hadamard matrix. A *Hadamard code* is a binary code where each codeword is either a row of H or a complement (meaning interchanging 1 with 0) of a row of H.
As one may expect, a *Hadamard propelinear code* is a binary code that is both Hadamard and propelinear. It remains to define the term *full*.

Definition 6.2. ([5] Definition 2.1) *A Hadamard* full *propelinear code is a Hadamard propelinear code* C *such that for all codewords* $a \in C \setminus \{\mathbf{0}, \mathbf{1}\}$ *the permutation* π_a *(from the definition of propelinear) does not fix any coordinate, and* $\pi_{\mathbf{1}}$ *is the identity permutation (as well as* $\pi_{\mathbf{0}}$*). In this case, we say* C *is a HFP-code.*

Definition 6.3. *Let* D *be a relative* $(4m, 2, 4m, 2m)$*-difference set in a group* K *of order* $8m$ *relative to a normal subgroup* $U \cong \mathbb{Z}_2$ *of* K*. Then* K *is a* Hadamard group *of order* $8m$*.*

Propositions 2.4 and 2.5 from [5] establish a constructive equivalence between Hadamard full propelinear codes and Hadamard groups. Moreover, Hadamard groups are equivalent to cocyclic Hadamard matrices in the central binary case (see [1]), and therefore we may include these extra objects in the constellation, but only in the central binary group extension case.

7 Discussion and Conclusion

We have presented the constellation as conjured by Horadam in [3, section 7.4]. A slight augmentation to the constellation is given by Hadamard full propelinear codes and Hadamard groups, in the sense that these objects only exist in the central binary extension case. This begs the question of whether there is a generalisation of Hadamard full propelinear codes, or of Hadamard groups, that is equivalent to the objects in the constellation under more general extensions. Searching for such an object or extending the constellation some other way are potential directions for further study.

The constellation identifies combinatorial objects together, allowing the freedom to regard these objects in a different light when facing applications and problems like the Hadamard conjecture. Group extensions glue the constellation together, but the reliance on them may also be a great limitation - as discussed, there are instances of the constellation objects that cannot be reached by the constellation. Nevertheless, the constellation is an interesting object itself in combinatorics, and hopefully permits new discoveries in the field.

References

[1] Flannery, D. L., 1997, 'Cocyclic Hadamard Matrices and Hadamard Groups Are Equivalent', *Journal of Algebra*, Vol. 192, No. 2, pp. 749-779.

[2] Galati, J. C., 2004, 'A group extensions approach to relative difference sets', *Journal of combinatorial designs*, Vol. 12, No. 4, pp. 279–298.

[3] Horadam, K. J., 2007, *Hadamard matrices and their applications*, 1st edn., Princeton University Press.

[4] Rifà Coma, J. & Suárez Canedo, E., 2014. 'About a class of Hadamard propelinear codes', *Electronic notes in discrete mathematics*, Vol. 46, pp. 289–296.

[5] Rifà Coma, J. & Suárez Canedo, E., 2017, 'Hadamard full propelinear codes of type Q; rank and kernel', *Designs, codes, and cryptography*, Vol. 86, No. 9, pp. 1905–1921.

8 Appendix

Here, our goal is to provide enough details to show that the map ξ defined in Theorem 3.1 is a bijection between classes of group extensions of U by G and classes of factor pairs of U by G.

We present some simple auxiliary results on factor pairs.

Lemma 8.1. ([3] Lemma 7.3) *Let $(\psi, \epsilon) \in F^2(G, U)$. Then, for all $x, y \in G$,*

1. $\epsilon(1) = \mathrm{Id}_U$,
2. $\psi^{-1}(x^{-1}, y)^{\epsilon(x)} = \psi(x, x^{-1}y)\psi^{-1}(x, x^{-1})$,
3. $\psi(x, x^{-1}) = \psi(x^{-1}, x)^{\epsilon(x)}$,
4. $\epsilon(x)^{-1} = \epsilon(x^{-1})\overline{\psi^{-1}(x, x^{-1})} = \overline{\psi^{-1}(x^{-1}, x)}\epsilon(x^{-1})$,
5. $(1, x)(1, y)^{-1} = \big(\psi^{-1}(xy^{-1}, y)xy^{-1}\big)$ *in* $E_{(\psi,\epsilon)}$,
6. $E_{(\psi,\epsilon)}$ *is abelian* $\iff$ U *and* G *are abelian,* $\epsilon \equiv 1$ *and* ψ *is symmetric.*

Proof. 1. Plug in $x = y = 1$ into (3.1) and use the fact that the factor pair is normalised:

$$\begin{aligned}\epsilon(1)\epsilon(1) &= \overline{\psi(1,1)}\epsilon(1)\\ \epsilon(1) &= \overline{1}\\ \epsilon(1) &= \mathrm{Id}_N\,.\end{aligned}$$

2. Note $\big(\psi(x, y)^{\epsilon(z)}\big)^{-1} = \big(\psi(x, y)^{-1}\big)^{\epsilon(z)}$ because the automorphism $\epsilon(z)$ preserves inverses. In particular we can write $\psi^{-1}(x^{-1}, y)^{\epsilon(x)}$ without worrying about ambiguity. Now set $y = x^{-1}$ in (3.2) and us the fact that the factor pair is normalised:

$$\psi(x, x^{-1}) = \psi(x, x^{-1})\psi(1, z) = \psi(x^{-1}, z)^{\epsilon(x)}\psi(x, x^{-1}z) \tag{8.1}$$

which gives the claim.

3. Set $z = x$ in (8.1) and use the fact that the factor pair is normalised.

4. Plugging $y = x^{-1}$ into (3.1), it follows from 1. that

$$\epsilon(x)\epsilon(x^{-1}) = \overline{\psi(x, x^{-1})}\epsilon(1) = \overline{\psi(x, x^{-1})}.$$

Since that $\overline{a^{-1}} = \bar{a}^{-1}$ in $\mathrm{Aut}(N)$ (which follows from the fact that $a^{-1}axa^{-1}a = aa^{-1}xaa^{-1} = x$ for all x), we have

$$\epsilon(x)\epsilon(x^{-1})\overline{\psi^{-1}(x, x^{-1})} = \mathrm{Id}_U,$$

which implies $\epsilon(x)^{-1} = \epsilon(x^{-1})\overline{\psi^{-1}(x, x^{-1})}$ (since $\mathrm{Aut}(U)$ is a group). Similarly, plugging $x = y^{-1}$ into (3.1), it follows from 1. that

$$\epsilon(y^{-1})\epsilon(y) = \overline{\psi(y^{-1}, y)}\epsilon(1) = \overline{\psi(y^{-1}, y)}.$$

With a similar argument as above, this implies $\epsilon(y)^{-1} = \overline{\psi^{-1}(y^{-1}, y)}\epsilon(y^{-1})$.

5. We compute

$$\begin{aligned}(1,x)(1,y)^{-1} &= (1,x)\left(\psi^{-1}(y^{-1},y)(1^{-1})^{\epsilon(y^{-1})}, y^{-1}\right)\\ &= (1,x)\left(\psi^{-1}(y^{-1},y), y^{-1}\right)\\ &= \left(1\left(\psi^{-1}(y^{-1},y)\right)^{\epsilon(x)}\psi(x,y^{-1}), xy^{-1}\right).\end{aligned}$$

It remains to show

$$\left(\psi^{-1}(y^{-1},y)\right)^{\epsilon(x)}\psi(x,y^{-1}) = \psi^{-1}(xy^{-1},y)$$

in N. As $\epsilon(x)$ is a homomorphism, (3.2) and the fact that (ψ,ϵ) is normalised give,

$$\begin{aligned}\left(\psi^{-1}(y^{-1},y)\right)^{\epsilon(x)}\psi(x,y^{-1})\psi(xy^{-1},y) &= \left(\psi^{-1}(y^{-1},y)\right)^{\epsilon(x)}\psi(y^{-1},y)^{\epsilon(x)}\psi(x,y^{-1}y)\\ &= \left(\psi^{-1}(y^{-1},y)\psi(y^{-1},y)\right)^{\epsilon(x)}\psi(x,1)\\ &= 1^{\epsilon(x)}1\\ &= 1.\end{aligned}$$

Thus the claim follows.

6. Suppose $E_{(\psi,\epsilon)}$ is abelian. Thus for all $x,y\in G$,

$$(\psi(x,y),xy) = (1,x)(1,y) = (1,y)(1,x) = (\psi(y,x),yx)$$

which forces $\psi(x,y)=\psi(y,x)$ and $xy=yx$, that is, ψ is symmetric and G is abelian. Furthermore, for all $x\in G$ and $b\in U$,

$$(b^{\epsilon(x)},x) = (1b^{\epsilon(x)}\psi(x,1),x) = (1,x)(b,1) = (b,1)(1,x) = (b1^{\epsilon(1)}\psi(1,x),x) = (b,x)$$

which implies $b^{\epsilon(x)}=b$, and thus $\epsilon(x)=1$ for all $x\in G$.
Similarly, for all $a,b\in U$,

$$(ab,1) = (ab^{\epsilon(1)}\psi(1,1),1) = (a,1)(b,1) = (b,1)(a,1) = (ba^{\epsilon(1)}\psi(1,1),1) = (ba,1)$$

meaning U is abelian. Conversely, if all these necessary conditions are met, then $E_{(\psi,\epsilon)}$ is clearly abelian by comparing

$$\begin{aligned}(a,x)(b,y) &= (ab^{\epsilon(x)}\psi(x,y),xy),\\ (b,y)(a,x) &= (ba^{\epsilon(y)}\psi(y,x),yx).\end{aligned}$$

□

We prove that $E_{(\psi,\epsilon)}$ in Definition 3.4 is indeed a group.

Proof. Let $a,b\in U$ and $x,y\in G$ be arbitrary.
Identity: Clearly

$$(1,1)(b,y) = \left(1b^{\epsilon(1)}\psi(1,y),1y\right) = \left(b^{\epsilon(1)},y\right)$$

thus for $(1,1)$ to be the identity, we need $b^{\epsilon(1)} = b$, which is true by Lemma 8.1-1. Similarly, since $\epsilon(x)$ is an automorphism and thus preserves the identity,

$$(a,x)(1,1) = \left(a1^{\epsilon(x)}\psi(x,1), x1\right) = (a,x)\,.$$

Associativity: We have

$$\begin{aligned}((a,x)(b,y))\,(c,z) &= \left(ab^{\epsilon(x)}\psi(x,y), xy\right)(c,z)\\ &= \left(ab^{\epsilon(x)}\psi(x,y)c^{\epsilon(xy)}\psi(xy,z), xyz\right)\end{aligned}$$

and

$$\begin{aligned}(a,x)\,((b,y)(c,z)) &= (a,x)\left(bc^{\epsilon(y)}\psi(y,z), yz\right)\\ &= \left(a\left(bc^{\epsilon(y)}\psi(y,z)\right)^{\epsilon(x)}\psi(x,yz), xyz\right)\\ &= \left(ab^{\epsilon(x)}c^{\epsilon(x)\epsilon(y)}\psi(y,z)^{\epsilon(x)}\psi(x,yz), xyz\right).\end{aligned}$$

So $E_{(\psi,\epsilon)}$ is associative if and only if

$$\psi(x,y)c^{\epsilon(xy)}\psi(xy,z) = c^{\epsilon(x)\epsilon(y)}\psi(y,z)^{\epsilon(x)}\psi(x,yz)$$

which by (3.2) is equivalent to

$$\begin{aligned}\psi(x,y)c^{\epsilon(xy)}\psi(xy,z) &= c^{\epsilon(x)\epsilon(y)}\psi(x,y)\psi(xy,z)\\ \psi(x,y)c^{\epsilon(xy)} &= c^{\epsilon(x)\epsilon(y)}\psi(x,y).\end{aligned}$$

Using (3.1),

$$\begin{aligned}c^{\epsilon(x)\epsilon(y)}\psi(x,y) &= c^{\overline{\psi(x,y)}\epsilon(xy)}\psi(x,y)\\ &= \psi(x,y)c^{\epsilon(xy)}\psi(x,y)^{-1}\psi(x,y)\\ &= \psi(x,y)c^{\epsilon(xy)}\end{aligned}$$

as required.

Inverses: If $(a,x) \in E_{(\psi,\epsilon)}$, then since $\epsilon(x)$ preserves inverses (it is an automorphism), and by (3.1), Lemma 8.1-1 and 8.1-3, we have

$$\begin{aligned}(a,x)\left(\psi^{-1}(x^{-1},x)(a^{-1})^{\epsilon(x^{-1})}, x^{-1}\right) &= \left(a\left(\psi^{-1}(x^{-1},x)(a^{-1})^{\epsilon(x^{-1})}\right)^{\epsilon(x)}\psi(x,x^{-1}), xx^{-1}\right)\\ &= \left(a\left(\psi^{-1}(x^{-1},x)\right)^{\epsilon(x)}(a^{-1})^{\epsilon(x)\epsilon(x^{-1})}\psi(x,x^{-1}), 1\right)\\ &= \left(a\left(\psi(x^{-1},x)^{\epsilon(x)}\right)^{-1}(a^{-1})^{\overline{\psi(x,x^{-1})}\epsilon(xx^{-1})}\psi(x,x^{-1}), 1\right)\\ &= \left(a\psi(x,x^{-1})^{-1}\psi(x,x^{-1})(a^{-1})^{\epsilon(1)}\psi(x,x^{-1})^{-1}\psi(x,x^{-1}), 1\right)\\ &= (1,1)\end{aligned}$$

as required. Likewise, as $\epsilon(x^{-1})$ is an automorphism,

$$\begin{aligned}\left(\psi^{-1}(x^{-1},x)(a^{-1})^{\epsilon(x^{-1})},x^{-1}\right)(a,x) &= \left(\psi^{-1}(x^{-1},x)(a^{-1})^{\epsilon(x^{-1})}a^{\epsilon(x^{-1})}\psi(x^{-1},x),x^{-1}x\right)\\ &= \left(\psi^{-1}(x^{-1},x)(a^{-1}a)^{\epsilon(x^{-1})}\psi(x^{-1},x),1\right)\\ &= (1,1)\end{aligned}$$

as required. Hence $E_{(\psi,\epsilon)}$ is a group. □

We check that the relation defined in Definition 3.5 is indeed an equivalence relation on $F^2(G,U)$.

Proof. **Reflexivity**: Consider the trivial map $1: G \to U$ with $g \mapsto 1$ (for all $g \in G$). Then $\epsilon(x) = \overline{1(x)}\epsilon(x)$ and $\psi(x,y) = 1(x)1(y)^{\epsilon(x)}\psi(x,y)1(xy)^{-1}$ since $\epsilon(x)$ is an automorphism.
Symmetry: Suppose $(\psi_2,\epsilon_2) \backsim_{\phi} (\psi_1,\epsilon_1)$, meaning

$$\epsilon_2(x) = \overline{\phi(x)}\epsilon_1(x), \tag{8.2}$$

$$\psi_2(x,y) = \phi(x)\phi(y)^{\epsilon_1(x)}\psi_1(x,y)\phi(xy)^{-1}. \tag{8.3}$$

Since the inverse mapping of $\bar{a}$ is $\overline{a^{-1}}$ in $\mathrm{Aut}(U)$, from (8.2) we immediately see

$$\epsilon_1(x) = \overline{\phi^{-1}(x)}\epsilon_2(x). \tag{8.4}$$

Also, from (8.3) and (8.4) and as the automorphism $\epsilon_1(x)$ preserves inverses,

$$\begin{aligned}\psi_1(x,y) &= \left(\phi(y)^{\epsilon_1(x)}\right)^{-1}\phi(x)^{-1}\psi_2(x,y)\phi(xy)\\ &= \phi^{-1}(y)^{\overline{\phi^{-1}(x)}\epsilon_2(x)}\phi^{-1}(x)\psi_2(x,y)\phi(xy)\\ &= \phi^{-1}(x)\phi^{-1}(y)^{\epsilon_2(x)}\phi(x)\phi^{-1}(x)\psi_2(x,y)\phi(xy)\\ &= \phi^{-1}(x)\phi^{-1}(y)^{\epsilon_2(x)}\psi_2(x,y)\phi(xy)\end{aligned}$$

which means $(\psi_1,\epsilon_1) \backsim_{\phi^{-1}} (\psi_2,\epsilon_2)$.
Transitivity: Suppose $(\psi_3,\epsilon_3) \backsim_{\phi_{32}} (\psi_2,\epsilon_2)$ and $(\psi_2,\epsilon_2) \backsim_{\phi_{21}} (\psi_1,\epsilon_1)$, hence

$$\epsilon_2(x) = \overline{\phi_{21}(x)}\epsilon_1(x), \tag{8.5}$$

$$\epsilon_3(x) = \overline{\phi_{32}(x)}\epsilon_2(x), \tag{8.6}$$

$$\psi_2(x,y) = \phi_{21}(x)\phi_{21}(y)^{\epsilon_1(x)}\psi_1(x,y)\phi_{21}^{-1}(xy), \tag{8.7}$$

$$\psi_3(x,y) = \phi_{32}(x)\phi_{32}(y)^{\epsilon_2(x)}\psi_2(x,y)\phi_{32}^{-1}(xy). \tag{8.8}$$

We claim $(\psi_3,\epsilon_3) \backsim_{\phi_{32}\phi_{21}} (\psi_1,\epsilon_1)$. Because $\overline{\phi_{32}(x)} \circ \overline{\phi_{21}(x)} = \overline{\phi_{32}(x)\phi_{21}(x)} = \overline{\phi_{32}\phi_{21}(x)}$ (by definition), subbing (8.5) into (8.6) we get

$$\epsilon_3(x) = \overline{\phi_{32}\phi_{21}(x)}\epsilon_1(x).$$

Also, by subbing (8.7) into (8.8),

$$\psi_3(x,y) = \phi_{32}(x)\phi_{32}(y)^{\epsilon_2(x)}\phi_{21}(x)\phi_{21}(y)^{\epsilon_1(x)}\psi_1(x,y)\phi_{21}^{-1}(xy)\phi_{32}^{-1}(xy).$$

Since $\phi_{21}^{-1}(xy)\phi_{32}^{-1}(xy) = (\phi_{32}\phi_{21})^{-1}(xy)$ by definition, it remains to show

$$\phi_{32}(x)\phi_{32}(y)^{\epsilon_2(x)}\phi_{21}(x)\phi_{21}(y)^{\epsilon_1(x)} = (\phi_{32}\phi_{21})(x)(\phi_{32}\phi_{21})(y)^{\epsilon_1(x)}$$

which is equivalent to

$$\phi_{32}(y)^{\epsilon_2(x)}\phi_{21}(x) = \phi_{21}(x)\phi_{32}(y)^{\epsilon_1(x)}.$$

Using (8.5), we have

$$\begin{aligned}\phi_{32}(y)^{\epsilon_2(x)}\phi_{21}(x) &= \phi_{32}(y)^{\overline{\phi_{21}(x)}\epsilon_1(x)}\phi_{21}(x)\\ &= \phi_{21}(x)\phi_{32}(y)^{\epsilon_1(x)}\phi_{21}(x)^{-1}\phi_{21}(x)\\ &= \phi_{32}(x)\phi_{32}(y)^{\epsilon_1(x)}\end{aligned}$$

as required. □

We prove Theorem 3.1, but omit the proof of the bijectivity of ξ as it follows from the other lemmas in the section.

Proof. First, we must show ϵ_T and ψ_T are well-defined, and that $\epsilon_T(x)$ is an automorphism on U for any $x \in G$. The key to seeing that ϵ_T is well-defined is to observe that the inner automorphism $\overline{t_x}$ of E is an automorphism on the subgroup $i[U]$ of E (this is a basic fact about inner automorphisms), and also that $i^{-1} : i[U] \to U$ exists as i is injective (and here i^{-1} denotes the inverse map of i). Now, for any $x \in G$, $\epsilon_T(x)$ is a homomorphism since it is a composition of homomorphisms. The inverse function is $(\epsilon_T(x))^{-1} := i^{-1} \circ \overline{t_x}^{-1} \circ i$; indeed

$$\epsilon_T(x)\left(\epsilon_T(x)\right)^{-1} = i^{-1} \circ \overline{t_x} \circ i \circ i^{-1} \circ \overline{t_x}^{-1} \circ i = \mathrm{Id}_U,$$

and similarly $(\epsilon_T(x))^{-1}\epsilon(x) = \mathrm{Id}_U$ as required. Hence $\epsilon_T(x)$ is bijective, which shows $\epsilon_T(x)$ is an isomorphism. For ψ_T to be well-defined, we need $t_x t_y t_{xy}^{-1} \in i[U]$ for all $x, y \in G$. Indeed, since $i[U] = \ker \pi$ by the exactness of e, it is enough to show $\pi(t_x t_y t_{xy}^{-1}) = 1$. Since π is a homomorphism,

$$\pi(t_x t_y t_{xy}^{-1}) = \pi(t_x)\pi(t_y)\pi(t_{xy}^{-1}) = xy(xy)^{-1} = 1$$

as required. Now we show (ψ_T, ϵ_T) is a factor pair. For (3.1), let $a \in U$ and $x, y \in G$, and see that because i^{-1} is a homomorphism,

$$\begin{aligned}a^{\overline{\psi_T(x,y)}\epsilon_T(xy)} &= \psi_T(x,y)a^{i^{-1}\circ\overline{t_{xy}}\circ i}\psi_T(x,y)^{-1}\\ &= \psi_T(x,y)i^{-1}\left(t_{xy}i(a)t_{xy}^{-1}\right)\psi_T(x,y)^{-1}\\ &= i^{-1}\left(t_x t_y t_{xy}^{-1}\right)i^{-1}\left(t_{xy}i(a)t_{xy}^{-1}\right)i^{-1}\left(t_x t_y t_{xy}^{-1}\right)^{-1}\\ &= i^{-1}\left(t_x t_y i(a) t_{xy}^{-1}\right)i^{-1}\left(t_{xy}t_y^{-1}t_x^{-1}\right)\\ &= i^{-1}\left(t_x t_y i(a) t_y^{-1} t_x^{-1}\right)\\ &= a^{i^{-1}\circ\overline{t_x}\circ\overline{t_y}\circ i}\\ &= a^{i^{-1}\circ\overline{t_x}\circ i\circ i^{-1}\circ\overline{t_y}\circ i}\\ &= a^{\epsilon_T(x)\epsilon_T(y)}\end{aligned}$$

as required.

For (3.2), let $x, y, z \in G$, then we have

$$\begin{aligned}\psi_T(y,z)^{\epsilon_T(x)}\psi_T(x,yz) &= i^{-1}\left(t_y t_z t_{yz}^{-1}\right)^{i^{-1}\circ\overline{t_x}\circ i} i^{-1}\left(t_x t_{yz} t_{xyz}^{-1}\right)\\ &= i^{-1}\left(t_x t_y t_z t_{yz}^{-1} t_x^{-1}\right) i^{-1}\left(t_x t_{yz} t_{xyz}^{-1}\right)\\ &= i^{-1}\left(t_x t_y t_z t_{xyz}^{-1}\right)\\ &= i^{-1}\left(t_x t_y t_{xy}^{-1}\right) i^{-1}\left(t_{xy} t_z t_{xyz}^{-1}\right)\\ &= \psi_T(x,y)\psi_T(xy,z)\end{aligned}$$

as required.

For (7.3), clearly $\psi_T(1,x) = i^{-1}\left(t_1 t_x t_{1x}^{-1}\right) = i^{-1}(t_1) = 1$ is equivalent to $t_1 = i(1) = 1$ since i is injective. Similarly, $\psi_T(x,1) = i^{-1}\left(t_x t_1 t_{x1}^{-1}\right) = 1$ is equivalent to $t_x t_1 t_x^{-1} = i(1) = 1$, which is equivalent to $t_1 = 1$. Of course $t_1 = 1$ is true since T is normalised. □

We prove lemma 3.1.

Proof. First note that ϕ is well-defined, because $\pi(t_x^* t_x^{-1}) = \pi(t_x^*)\pi(t_x^{-1}) = xx^{-1} = 1$ as π is a homomorphism, and that e is exact. We also require $\phi(1) = 1$, which is equivalent to $i(\phi(1)) = t_1^* t_1^{-1} = 1$ as i is injective. This is immediate since T and T^* are normalised.

For (7.8), since i^{-1} is a homomorphism, we have that for any $a \in U$,

$$\begin{aligned}a^{\overline{\phi(x)}\epsilon_T(x)} &= i^{-1}\left(t_x^* t_x^{-1}\right) a^{i^{-1}\circ\overline{t_x}\circ i}\left(i^{-1}\left(t_x^* t_x^{-1}\right)\right)^{-1}\\ &= i^{-1}\left(t_x^* t_x^{-1}\right) i^{-1}\left(t_x i(a) t_x^{-1}\right) i^{-1}\left(t_x t_x^{*\,-1}\right)\\ &= i^{-1}\left(t_x^* i(a) t_x^{*\,-1}\right)\\ &= a^{i^{-1}\circ\overline{t_x^*}\circ i}\\ &= a^{\epsilon_{T^*}(x)}\end{aligned}$$

as required. Similarly, observe that for any $x, y \in G$,

$$\begin{aligned}\phi(x)\phi(y)^{\epsilon_T(x)}\psi_T(x,y)\phi^{-1}(xy) &= i^{-1}\left(t_x^* t_x^{-1}\right)\left(i^{-1}\left(t_y^* t_y^{-1}\right)\right)^{i^{-1}\circ\overline{t_x}\circ i} i^{-1}\left(t_x t_y t_{xy}^{-1}\right)\left(i^{-1}\left(t_{xy}^* t_{xy}^{-1}\right)\right)^{-1}\\ &= i^{-1}\left(t_x^* t_x^{-1}\right) i^{-1}\left(t_x t_y^* t_y^{-1} t_x^{-1}\right) i^{-1}\left(t_x t_y t_{xy}^{-1}\right) i^{-1}\left(t_{xy} t_{xy}^{*-1}\right)\\ &= i^{-1}\left(t_x^* t_y^* t_{xy}^{*-1}\right)\\ &= \psi_{T^*}(x,y)\end{aligned}$$

as required. □

We prove lemma 3.2.

Proof. To show $S = \gamma[T]$ is a transversal of U in E_2, consider $t_x \in T$ and the coset $t_x U$. Then $\gamma(t_x)U = s_x U$ is a coset of U in E_2 with representative $s_x = \gamma(t_x)$. If $s_y = \gamma(t_y)$ is another representative, then $\gamma(t_y)\gamma(t_x)^{-1} \in U$, giving $\gamma(t_y t_x^{-1}) \in U$. The exactness of e_2 and that $\pi_1 = \pi_2 \circ \gamma$ imply $\pi_1(t_y t_x^{-1}) = \pi_2(\gamma(t_y t_x^{-1})) = 1$. But then $t_y t_x^{-1} \in U$ by exactness of e_1, and as T is a transversal, it follows that $x = y$. Therefore S is a transversal of U in E_2.

For any $x \in G$ and $a \in U$, note $\epsilon_S(x) = i_2^{-1} \circ \overline{s_x} \circ i_2 = i_2^{-1} \circ \overline{\gamma(t_x)} \circ i_2$, so as $i_2 = \gamma \circ i_1$,

$$
\begin{aligned}
a^{\epsilon_S(x)} &= i_2^{-1}\left(\gamma(t_x) i_2(a) \gamma(t_x)^{-1}\right) \\
&= i_1^{-1}\left(\gamma^{-1}\left(\gamma(t_x)\gamma(i_1(a))\gamma(t_x)^{-1}\right)\right) \\
&= i_1^{-1}\left(\gamma^{-1}\left(\gamma(t_x i_1(a)) t_x^{-1}\right)\right) \\
&= i_1^{-1}\left(t_x i_1(a) t_x^{-1}\right) \\
&= a^{\epsilon_T(x)}
\end{aligned}
$$

meaning $\epsilon_S(x) = \epsilon_T(x)$, and

$$
\begin{aligned}
\psi_S(x,y) &= i_2^{-1}\left(s_x s_y s_{xy}^{-1}\right) \\
&= i_2^{-1}\left(\gamma(t_x)\gamma(t_y)\gamma(t_{xy})^{-1}\right) \\
&= i_2^{-1}\left(\gamma\left(t_x t_y t_{xy}^{-1}\right)\right) \\
&= i_1^{-1}\left(t_x t_y t_{xy}^{-1}\right) \\
&= \psi_T(x,y)
\end{aligned}
$$

as required. □

We present another lemma.

Lemma 8.2. *If $(\psi,\epsilon) \sim_\phi (\psi',\epsilon')$ are factor pairs of U by G, then $\theta : E_{(\psi,\epsilon)} \to E_{(\psi',\epsilon')}$ defined by $(a,x) \mapsto (a\phi(x),x)$ is an isomorphism. Moreover, the canonical extensions $e : U \overset{\iota}{\rightarrowtail} E_{(\psi,\epsilon)} \overset{\kappa}{\twoheadrightarrow} G$ and $e' : U \overset{\iota}{\rightarrowtail} E_{(\psi',\epsilon')} \overset{\kappa}{\twoheadrightarrow} G$ are equivalent via θ.*

Proof. Suppose $(\psi,\epsilon) \sim_\phi (\psi',\epsilon')$. The map $(a,x) \overset{\theta^{-1}}{\mapsto} (a\phi(x)^{-1},x)$ is obviously the inverse map to θ. Hence θ is a bijection. To see that θ is a homomorphism, for any $a,b \in U$ and $x,y \in G$, we note

$$
\theta(a,x)\theta(b,y) = (a\phi(x),x)(b\phi(y),y) = \left(a\phi(x)\left(b\phi(y)\right)^{\epsilon'(x)}\psi'(x,y), xy\right)
$$

and

$$
\theta\left((a,x)(b,y)\right) = \theta\left(ab^{\epsilon(x)}\psi(x,y), xy\right) = \left(ab^{\epsilon(x)}\psi(x,y)\phi(xy), xy\right).
$$

Thus it remains to check

$$
b^{\epsilon(x)}\psi(x,y)\phi(xy) = \phi(x)\left(b\phi(y)\right)^{\epsilon'(x)}\psi'(x,y).
$$

Indeed, because $(\psi,\epsilon) \sim_\phi (\psi',\epsilon')$,

$$
\begin{aligned}
b^{\epsilon(x)}\psi(x,y)\phi(xy) &= b^{\overline{\phi(x)}\epsilon'(x)}\phi(x)\phi(y)^{\epsilon'(x)}\psi'(x,y)\phi(xy)^{-1}\phi(xy) \\
&= \phi(x)b^{\epsilon'(x)}\phi(x)^{-1}\phi(x)\phi(y)^{\epsilon'(x)}\psi'(x,y) \\
&= \phi(x)\left(b\phi(y)\right)^{\epsilon'(x)}\psi'(x,y)
\end{aligned}
$$

as required.

Now to show $e \sim_\theta e'$, we verify that the relevant diagram commutes. Indeed, for $\iota = \theta\iota$,

$$\theta(\iota(a)) = \theta(a, 1) = \left(a\phi(1)^{-1}, 1\right) = (a, 1) = \iota(a)$$

and for $\kappa = \kappa\theta$,

$$\kappa(\theta(a, x)) = \kappa(a\phi(x)^{-1}, x) = x = \kappa(a, x)$$

as required. □

To prove Lemma 3.3, we actually prove Corollary 3.1 first as the isomorphism there is easier to work with. There is no worry of a circular argument here though, as the corollary aspect of the result captures the fact that every group extension is equivalent to some canonical group extension built from a factor pair; the actual isomorphism inducing this equivalence is not easily found.

Proof. First, we show the mapping $\gamma : E \to E_{(\psi_T, \epsilon_T)}$ with $i(a)t_x \mapsto (a, x)$ is well-defined (that is, every element $f \in E$ is written in the form $f = i(a)t_x$ for some unique $a \in U$ and $x \in G$). Let $f \in E$ and set $H \coloneqq i[U]$. As T is a transversal, let t_x be the unique element in T that is in Hf (note the right coset). Then $ft_x^{-1} \in H$, and so there is $a \in N$ such that $ft_x^{-1} = i(a)$, which gives us $f = i(a)t_x$. Moreover, this a is unique because i is injective as needed.

Now we show γ is an isomorphism. It is a bijection since $(a, x) \mapsto i(a)t_x$ is clearly the inverse mapping. It is a homomorphism since for any $a, b \in U$ and $x, y \in G$,

$$\begin{aligned}
\gamma(i(a)t_x)\gamma(i(b)t_y) &= (a, x)(b, y) \\
&= \left(ab^{\epsilon_T(x)}\psi_T(x, y), xy\right) \\
&= \gamma\left[i\left(ab^{\epsilon_T(x)}\psi_T(x, y)\right)t_{xy}\right] \\
&= \gamma\left[i(a)i(b^{i^{-1}\circ\overline{t_x}\circ i})i\left(i^{-1}(t_x t_y t_{xy}^{-1})\right)t_{xy}\right] \\
&= \gamma\left[i(a)t_x i(b)t_x^{-1}t_x t_y t_{xy}^{-1}t_{xy}\right] \\
&= \gamma\left[i(a)t_x i(b)t_y\right]
\end{aligned}$$

as required.

Now we show γ makes the appropriate diagram commute. For $\gamma \circ i = \iota$, we have for any $u \in U$.

$$\gamma(i(u)) = \gamma(i(u)t_1) = (u, 1) = \iota(u).$$

For $\kappa \circ \gamma = \pi$, we have for any $i(a)t_x \in E$,

$$\kappa(\gamma(i(a)t_x)) = \kappa(a, x) = x = \pi(i(a))\pi(t_x) = \pi(i(a)t_x).$$

This is enough to make the diagram commute (since $\pi i = \kappa\gamma i = \kappa\iota$).

Consider the canonical extensions $e_T : U \overset{\iota}{\rightarrowtail} E_{(\psi_T, \epsilon_T)} \overset{\kappa}{\twoheadrightarrow} G$ and $e' : U \overset{\iota}{\rightarrowtail} E_{(\psi, \epsilon)} \overset{\kappa}{\twoheadrightarrow} G$ (note ι and κ are functions

$U \to U \times G$ and $U \times G \to G$ respectively, hence we can use the same labels for both extensions e_T and e_S). We demonstrate that if $(\psi, \epsilon) \in F^2(G, U)$ with $(\psi, \epsilon) \sim_\phi (\psi_T, \epsilon_T)$, then $\delta : E \to E_{(\psi,\epsilon)}$ defined by

$$i(a)t_x \mapsto (a\phi^{-1}(x), x)$$

is an isomorphism, and that $e \sim_\delta e'$. From the above work, $\gamma : E \to E_{(\psi_T,\epsilon_T)}$ defined by

$$i(a)t_x \mapsto (a, x)$$

is an isomorphism, and $e \sim_\gamma e_T$. Furthermore, from Lemma 8.2, $\theta^{-1} : E_{(\psi_T,\epsilon_T)} \to E_{(\psi,\epsilon)}$ defined by

$$(a, x) \mapsto (a\phi^{-1}(x), x)$$

is an isomorphism, and $e_T \sim_{\theta^{-1}} e'$. Note δ is the composition $\delta = \theta^{-1} \circ \gamma$, hence δ is indeed an isomorphism, and $e \sim_\delta e'$. □

Now we can prove 3.3.

Proof. Consider the canonical extensions $e_T : U \overset{\iota}{\rightarrowtail} E_{(\psi_T,\epsilon_T)} \overset{\kappa}{\twoheadrightarrow} G$ and $e_S : U \overset{\iota}{\rightarrowtail} E_{(\psi_S,\epsilon_S)} \overset{\kappa}{\twoheadrightarrow} G$. By Corollary 3.1, e_1 is equivalent to e_T via the isomorphism $\gamma_T : E_1 \to E_{(\psi_T,\epsilon_T)}$ defined by

$$i_1(a)t_x \mapsto (a, x).$$

Also, similarly, e_S is equivalent to e_2 via the isomorphism $\gamma_S^{-1} : E_{(\psi_S,\epsilon_S)} \to E_2$ defined by

$$(a, x) \mapsto i_2(a)s_x.$$

Finally, by Lemma 8.2, if $(\psi, \epsilon) \in F^2(G, U)$ is some factor pair with $(\psi, \epsilon) \sim_\phi (\psi_T, \epsilon_T)$, then e_T is equivalent to e_S via the isomorphism $\theta^{-1} : E_{(\psi_T,\epsilon_T)} \to E_{(\psi,\epsilon)}$ defined by

$$(a, x) \mapsto (a\phi(x)^{-1}, x),$$

and the special case $(\psi, \epsilon) = (\psi_S, \epsilon_S)$ allows us to put all the above together to get that e_1 is equivalent to e_2 via the composition $\gamma_S^{-1} \circ \theta^{-1} \circ \gamma_T$. □

Finally, we prove Lemma 3.4 to complete the proof that ξ is bijective.

Proof. We first check that T is a transversal of $\overline{U} := U \times \{1\}$ in $E_{(\psi,\epsilon)}$. If $(1, x) \in T$, then obviously $(1, x)\bar{U}$ is a coset of $\bar{U}$ in $E_{(\psi,\epsilon)}$. If $(1, x)\bar{U} = (1, y)\bar{U}$, then $(1, x)(1, y)^{-1} \in \bar{U}$ and so $(1, x)(1, y)^{-1} = (a, 1)$ for some $a \in U$. By Lemma 8.1-5,

$$(a, 1) = (1, x)(1, y)^{-1} = \big(\psi^{-1}(xy^{-1}, y), xy^{-1}\big)$$

so $x = y$ by comparing the second component, meaning $(1, x) = (1, y)$.

Now we verify $(\psi_T, \epsilon_T) = (\psi, \epsilon)$. Here, $\iota : U \to E_{(\psi,\epsilon)}$ is the natural injection $a \mapsto (a, 1)$. For any $x \in G$ and $a \in U$ (here ι^{-1} denotes the inverse map $(a, 1) \mapsto a$),

$$\begin{aligned}
a^{\epsilon_T(x)} &= a^{\iota^{-1}\circ\overline{(1,x)}\circ\iota} \\
&= \iota^{-1}\left[(1,x)(a,1)(1,x)^{-1}\right] \\
&= \iota^{-1}\left[\left(1a^{\epsilon(x)}\psi(x,1), x1\right)\left(\psi(x^{-1},x)^{-1}1^{\epsilon(x^{-1})}, x^{-1}\right)\right] \\
&= \iota^{-1}\left[(a^{\epsilon(x)}, x)(\psi(x^{-1},x)^{-1}, x^{-1})\right] \\
&= \iota^{-1}\left[\left(a^{\epsilon(x)}\left(\psi(x^{-1},x)^{-1}\right)^{\epsilon(x)}\psi(x,x^{-1}), 1\right)\right] \\
&= a^{\epsilon(x)}\left(\psi(x^{-1},x)^{-1}\right)^{\epsilon(x)}\psi(x,x^{-1})
\end{aligned}$$

It remains to show

$$\left(\psi(x^{-1},x)^{-1}\right)^{\epsilon(x)}\psi(x,x^{-1}) = 1 \tag{8.9}$$

Well, using Lemma 8.1-3,

$$\begin{aligned}
\left(\psi(x^{-1},x)^{-1}\right)^{\epsilon(x)}\psi(x,x^{-1}) &= \left(\psi(x^{-1},x)^{\epsilon(x)}\right)^{-1}\psi(x,x^{-1}) \\
&= \psi(x,x^{-1})^{-1}\psi(x,x^{-1}) \\
&= 1
\end{aligned}$$

as required. We also have

$$\begin{aligned}
\psi_T(x,y) &= \iota^{-1}\left[(1,x)(1,y)(1,xy)^{-1}\right] \\
&= \iota^{-1}\left[\left(1^{\epsilon(x)}\psi(x,y), xy\right)\left(\psi\left((xy)^{-1}, xy\right)^{-1}1^{\epsilon((xy)^{-1})}, (xy)^{-1}\right)\right] \\
&= \iota^{-1}\left[\left(\psi(x,y)\left(\psi\left((xy)^{-1}, xy\right)^{-1}\right)^{\epsilon(xy)}\psi(xy,(xy)^{-1}), 1\right)\right] \\
&= \psi(x,y)\left(\psi\left((xy)^{-1}, xy\right)^{-1}\right)^{\epsilon(xy)}\psi(xy,(xy)^{-1})
\end{aligned}$$

and observe that if we set $x := xy$ for (8.9) (and (8.9) is indeed true by our above work), we obtain $\psi_T(x,y) = \psi(x,y)$ as required. □