Annales Mathematicae Silesianae **33** (2019), 284–297
DOI: 10.2478/amsil-2019-0006

INVERSE AMBIGUOUS FUNCTIONS AND AUTOMORPHISMS ON FINITE GROUPS

Imke Toborg

Abstract. If G is a finite group, then a bijective function $f : G \to G$ is inverse ambiguous if and only if $f(x)^{-1} = f^{-1}(x)$ for all $x \in G$. We give a precise description when a finite group admits an inverse ambiguous function and when a finite group admits an inverse ambiguous automorphism.

1. Introduction

Suppose $(G, \cdot)$ is a finite group and $f : G \to G$ is a bijective function and let $x \in G$. Then $f(x)^{-1}$ denotes the inverse of the image of x under f while $f^{-1}(x)$ denotes the pre-image of x under f. In general $f(x)^{-1}$ and $f^{-1}(x)$ are different elements.

Inspired from students being confused by this similar notation, several authors investigated functions $f\colon K \to K$ such that $f^{-1}(x) = f(x)^{-1}$ for all $x \in K$ where K is equal to $(0,\infty) \subseteq \mathbb{R}, \mathbb{R}$, or $\mathbb{C}$ (see for example [2] and [3]). Furthermore in [4] functions $f\colon \mathbb{R} \to \mathbb{R}$ satisfying the functional equation $f(f(x)) = -x$ for all $x \in \mathbb{R}$ have been investigated. Recently, David J. Schmitz introduced in [7] the notion of an inverse ambiguous function of a group G. This is a bijective function $f\colon G \to G$ that is a solution of the functional equation $f^{-1}(x) = f(x)^{-1}$ for all $x \in G$. He analysed the question whether a group admits an inverse ambiguous function and answered it for several

Received: 22.11.2018. Accepted: 12.05.2019. Published online: 13.06.2019.
(2010) Mathematics Subject Classification: 20D99, 20K30, 39B52.
Key words and phrases: inverse function, functional equation, finite groups, abelian groups.

abelian groups. Moreover he gave a criteria for the existence of an inverse ambiguous function of a finite group in terms of the number of elements of order at least 3. This criteria was used by him together with Katherine Gallagher in [8] to answer the question whether a symmetric or alternating group or $\mathrm{GL}(2,q)$ for an arbitrary prime power q admits an inverse ambiguous function. In their introduction they refer to an article by Marcel Herzog [5] from which some of their conclusions may also be derived.

In this paper we study finite groups in general. We use the work of Herzog in Section 2 to show that the existence of an inverse ambiguous function of a finite group $(G,\cdot)$ depends on the order of G as well as the structure or number of Sylow 2-subgroups of G. We are also interested in inverse ambiguous automorphisms. These are inverse ambiguous functions that are also homomorphisms. Non-abelian groups do not admit inverse ambiguous automorphisms. In Section 3 we give a precise characterisation of finite abelian p-groups admitting an inverse ambiguous automorphism for odd primes. Finally in Section 4 we investigate finite abelian 2-groups and characterise those that admit an inverse ambiguous automorphism. This theorem together with the results of Section 3 lead to a characterisation of finite groups admitting inverse ambiguous automorphism.

All groups are written multiplicatively and we use standard group-theoretic notation (see for example [6]). In particular 1 denotes the neutral element of a group G as well as its trivial subgroup generated by the neutral element.

2. Inverse ambiguous functions

Definition 2.1. Let G be a group and $f\colon G \to G$ be a bijective function. Then f is an *inverse ambiguous function* if and only if

$$f(x)^{-1} = f^{-1}(x) \text{ for all } x \in G.$$

If further f is an automorphism, then f is an *inverse ambiguous automorphism.*

Lemma 2.2. *Let G be a finite group such that $|G|$ is a multiple of 4. Then the following statements are equivalent.*

(a) *There is an inverse ambiguous function $f\colon G \to G$.*

(b) *We have $|\{x \in G \mid o(x) \geqslant 3\}| \equiv 0$ mod 4.*

(c) *We have $|\{x \in G \mid o(x) = 2\}| \equiv (-1)$ mod 4.*

(d) *A Sylow 2-subgroup of G is neither cyclic, a quaternion group, a non-abelian dihedral group nor semi-dihedral.*

(e) *A Sylow* 2*-subgroup of* G *is not a dihedral group of order* 8 *and contains a normal subgroup which is elementary abelian of order* 4*.*

(f) *The group* G *has an elementary abelian subgroup of order* 4 *that either is a Sylow* 2*-subgroup of* G *or not a Sylow* 2*-subgroup of its centraliser.*

Proof. By Theorem 4.1 of [7] we see that (a) and (b) are equivalent.

From $G = \{1\}\dot\cup\{x \in G \mid o(x) \geqslant 3\}\dot\cup\{x \in G \mid o(x) = 2\}$ and from $|G| \equiv 0 \bmod 4$ we moreover obtain that (b) and (c) are equivalent.

Furthermore the equivalence of (c) and (d) follows from Theorem 3 of [5].

Lemma 1.4 of [1] shows that (d) implies (e).

We now assume that (e) is true and let S be a Sylow 2-subgroup of G. Then S contains an elementary abelian normal subgroup A which has order 4. We suppose for a contradiction that $S \neq A$ and $C_S(A) = A$. From $S = N_S(A)$ we get that $N_S(A)/C_S(A)$ is isomorphic to a non-trivial 2-subgroup of $\mathrm{Aut}(A)$ by 3.1.9 of [6]. Since $\mathrm{Aut}(A)$ has order 6 by 2.1.8 (b) of [6], we conclude that $S/A = N_S(A)/C_S(A)$ has order 2 and so $|S| = 8$. From $C_S(A) \neq S$ we see that S is non-abelian. There are exactly two non-abelian groups of order 8, the quaternion group of order 8 which contains a unique element of order 2 and the dihedral group of order 8 (see for example 3.2.2 of [9]). This is a contradiction. So we have $S = N_S(A) = C_S(A)$ or $A \neq C_S(A)$. This implies that $A = S$ or that $A \lneqq C_S(A)$. In the second case A is not a Sylow 2-subgroup of $C_G(A)$. Thus (f) is true in both cases.

We finally assume (f). Then there is an elementary abelian subgroup A of order 4 of G that is either a Sylow 2-subgroup of G or not a Sylow 2-subgroup of its centraliser. In the first case (d) is true. So let S be a Sylow 2-subgroup of G such that $C_S(A)$ is a Sylow 2-subgroup of $C_G(A)$. Suppose that $A \neq S$. Then we have $A \leqslant C_S(A) \leqslant S$ and hence S is neither cyclic nor a quaternion group, as it contains at least two elements of order 2 by 5.3.7 of [6]. We suppose for a contradiction that S is dihedral or semi-dihedral. In both cases $Z(S)$ is cyclic and S contains a cyclic normal subgroup $\langle c\rangle$ of index 2 (see for example the remark below 5.3.2 of [6]). Hence there is some $a \in A\backslash Z(S)$ and furthermore 5.3.2 of [6] yields that $c^a = c^{-1}$ or $c^a = c^{-1+2^n}$ where $o(c) = 2^{n+1}$. This implies that $|C_{\langle c\rangle}(a)| = 2$. From $a \in C_S(a)\backslash\langle c\rangle$ we deduce that $\langle c\rangle \lneqq \langle c\rangle C_S(a) \leqslant S$. This implies that $S = \langle c\rangle C_S(a)$. Now 1.1.6 of [6] shows that

$$|C_S(a)| = \frac{|S||C_S(a) \cap \langle c\rangle|}{|\langle c\rangle|} = |S : \langle c\rangle| \cdot |C_{\langle c\rangle}(a)| = 4.$$

This implies the contradiction $A = C_S(a)$. We conclude that (d) holds. □

Theorem 2.3. *Let* G *be a finite group. Then* G *admits an inverse ambiguous function if and only if one of the following holds:*

(a) $|G| \equiv 1$ *mod* 4,
(b) $4 \nmid |G|$ *and there is some* $z \in G$ *of order* 2 *such that* $|G : C_G(z)| \equiv 1$ *mod* 4,
(c) $4 \mid |G|$ *and* G *has one of the properties in Lemma* 2.2.

Proof. We first notice from Theorem 4.1 of [7] that G admits an inverse ambiguous function $f\colon G \to G$ if and only if $|\{x \in G \mid o(x) \geqslant 3\}| \equiv 0 \bmod 4$.

Let G have odd order. Then we have $\{x \in G \mid o(x) \geqslant 3\} = G\backslash\{1\}$ and so we see with regard to (a) that the theorem holds in this case.

If $|G|$ is a multiple of 4, then Lemma 2.2 shows that the assertion is true.

It remains the case $|G| \equiv 2 \bmod 4$. Then $|G|$ is even and so there is an element z in G of order 2. Then $\langle z\rangle$ is a Sylow 2-subgroup of G and so Sylow's theorem (see for example 3.2.3 (b) of [6]) implies that $z^G := \{g^{-1}zg \mid g \in G\}$ is the set of all elements of order 2 of G. From 3.1.5 of [6] we moreover see that $|z^G| = |G : C_G(z)|$.

It follows that $\{x \in G \mid o(x) \geqslant 3\} \dot\cup z^G = G\backslash\{1\}$ and hence

$$|\{x \in G \mid o(x) \geqslant 3\}| + |G : C_G(z)| \equiv 2 - 1 \bmod 4.$$

Summarising we obtain in this last case that G admits an inverse ambiguous function if and only if $|G : C_G(z)| \equiv 1 \bmod 4$. □

3. Inverse ambiguous automorphisms

Lemma 3.1. *Let G be a finite group and $f\colon G \to G$ be an automorphism of G. Then f is inverse ambiguous if and only if the composition $f \circ f$ inverts every $x \in G$.*

Proof. Let x be an element of G. Then we have

$$f(x)^{-1} = f^{-1}(x) \Leftrightarrow f(f(x^{-1})) = x \Leftrightarrow (f \circ f)(x^{-1}) = x.$$

This implies the assertion. □

Theorem 3.2. *Let G be a finite group admitting an inverse ambiguous automorphism f. Then G is abelian. Furthermore, f has order 4 or G is an elementary abelian 2-group.*

Proof. From Lemma 3.1 we see that $f \circ f$ inverts G. Thus G is abelian (see for example Exercise 4 of 1.3 in [6]).

Furthermore we see that $f^4 = (f \circ f) \circ (f \circ f)$ is the identity on G. So the order of f divides 4. If f does not have order 4, then $f \circ f$ is the identity on G. In this case we conclude that $x^{-1} = (f \circ f)(x) = x$ for all $x \in G$. In particular every element of $G\backslash\{1\}$ has order 2 and so G is an elementary abelian 2-group. □

Lemma 3.3. *Let G be a finite group admitting an inverse ambiguous automorphism and let $x \in G$. Then $\langle x\rangle \cap \langle f(x)\rangle$ and $\langle x, f(x)\rangle$ are f-invariant. In particular both groups admit an inverse ambiguous automorphism.*

Proof. We apply Lemma 3.1. It yields $f(\langle f(x)\rangle) = \langle (f \circ f)(x)\rangle = \langle x^{-1}\rangle = \langle x\rangle$. So we get that $f(\langle x\rangle \cap \langle f(x)\rangle) = \langle f(x)\rangle \cap \langle x\rangle$. As G is abelian by Theorem 3.2, we further see $\langle x, f(x)\rangle = \langle x\rangle\langle f(x)\rangle = \langle f(x)\rangle\langle x\rangle$ and hence $f(\langle x, f(x)\rangle) = f(\langle x\rangle\langle f(x)\rangle) = \langle f(x)\rangle\langle x\rangle = \langle x, f(x)\rangle$. □

Lemma 3.4. *Let G be a finite group admitting an inverse ambiguous automorphism f and let $A \leqslant G$ be f-invariant. Then $\bar{f}\colon G/A \to G/A$ defined via $\bar{f}(Ag) := Af(g)$ is an inverse ambiguous automorphism of G/A.*

Proof. By Lemma 3.2 the group G is abelian and so A is a normal subgroup of G. Since f is an automorphism of the finite group G, elementary arguments show that $\bar{f}$ is an automorphism of G/A. Finally we see from Lemma 3.1 that for all $g \in G$ we have $(\bar{f} \circ \bar{f})(Ag) = Af(f(g)) = Ag^{-1} = (Ag)^{-1}$. Thus $\bar{f}$ is inverse ambiguous by Lemma 3.1. □

Lemma 3.5. *Let G and H be finite groups and let $f_1\colon G \to G$ and $f_2\colon H \to H$ be inverse ambiguous automorphisms. Then $f\colon G \times H \to G \times H$ defined via $f(x, y) := (f_1(x), f_2(y))$ for all $x \in G$ and all $y \in H$ is an inverse ambiguous automorphism.*

Proof. We first remark that f is an automorphism from $G \times H$. Furthermore for all $x \in G$ and $y \in H$ Lemma 3.1 yields that $f^2(x, y) = (f_1^2(x), f_2^2(y)) = (x^{-1}, y^{-1})$. Thus f is inverse ambiguous by Lemma 3.1. □

Lemma 3.6. *Let G be a non-trivial cyclic p-group for some prime p. Then G admits an inverse ambiguous automorphism if and only if $p \equiv 1 \bmod 4$ or $|G| = 2$.*

Proof. Let n be such that $|G| = p^n$. From 2.2.5 of [6] we obtain that $\mathrm{Aut}(G)$ is a direct product of a group of order p^{n-1} and a cyclic group of order $p - 1$.

Suppose first that $p \equiv 3 \bmod 4$. Then G does not admit an automorphism of order 4. Thus Theorem 3.2 implies that G does not have an inverse ambiguous automorphism in this case.

If $p \equiv 1 \bmod 4$, then G admits exactly one automorphism of order 4, say f. It further admits a unique automorphism of order 2, namely $f \circ f$. In particular $f \circ f$ inverts the elements of G and so the assertion follows from Lemma 3.1.

It remains the case $p = 2$. If $|G| = 2$, then the identity is inverse ambiguous. If $|G| \geqslant 2^2$, then there does not exist an inverse ambiguous function on G by Lemma 2.2 ($(a) \Leftrightarrow (d)$). □

Theorem 3.7. *Let G be a non-trivial abelian p-group for some prime p such that $p \equiv 1 \bmod 4$. Then G admits an inverse ambiguous automorphism.*

Proof. Let first G be cyclic. Then Lemma 3.6 provides the statement.

Let now G be non-cyclic. Since G is abelian, we see that G is a direct product of cyclic groups. Thus Lemma 3.5 and the cyclic case imply the assertion. □

Lemma 3.8. *Let $G = \langle a \rangle \times \langle b \rangle$ be an abelian group. If $o(a) = o(b)$, then $f \colon G \to G$ is defined via $f(a^i b^j) := a^{-j} b^i$ is an inverse ambiguous automorphism.*

Proof. Let $f \colon G \to G$ be the function defined via $f(a) = b$ and $f(b) = a^{-1}$. Then f is an isomorphism of G and we have $f^2(a) = a^{-1}$, $f^2(b) = b^{-1}$. Thus Lemma 3.1 implies that f is an ambiguous isomorphism. □

Lemma 3.9. *Let p be a prime such that $p \equiv 3 \bmod 4$ and let G be an abelian p-group of rank 2. If G admits an inverse ambiguous automorphism f, then there is an element $a \in G$ such that $G = \langle a \rangle \times \langle f(a) \rangle$.*

In particular, G admits an inverse ambiguous automorphism if and only if G is isomorphic to a direct product of two cyclic groups of the same order.

Proof. Let G admit the inverse ambiguous automorphism f and let $a \in G$ be of maximal order. Then we have $|G| \leqslant o(a)^2$, as G is generated by two elements. Furthermore we have $o(f(a)) = o(a)$, since f is an automorphism. Lemma 3.3 and Lemma 3.6 imply that $\langle a \rangle \cap \langle f(a) \rangle = 1$.

Altogether we have $\langle a \rangle \times \langle f(a) \rangle \leqslant G$ and

$$|\langle a \rangle \times \langle f(a) \rangle| = o(a) \cdot o(f(a)) = o(a)^2 \geqslant |G|.$$

This implies that $G = \langle a \rangle \times \langle f(a) \rangle$.

On the other hand if $G = \langle a \rangle \times \langle b \rangle$ with $o(a) = |\langle a \rangle| = |\langle b \rangle| = o(b)$, then Lemma 3.8 provides an inverse ambiguous automorphism of G. □

Lemma 3.10. *Let G be an abelian p-group for some prime p. Suppose further that G admits an inverse ambiguous automorphism f. If $a \in G$ is an* *element of maximal order and such that* $\langle a\rangle \cap \langle f(a)\rangle = 1$, *then* $\langle a, f(a)\rangle$ *has rank* 2 *and a complement in* G.

In particular if $p \equiv 3$ *mod* 4, *then there is a subgroup* $1 \neq A$ *of* G *of rank* 2 *such that* $f(A) = A$ *and such that* A *has a complement in* G.

Proof. Let $a \in G$ be of maximal order and such that $\langle a\rangle \cap \langle f(a)\rangle = 1$. Then $A := \langle a, f(a)\rangle$ has rank 2 and $o(f(a)) = o(a)$ is maximal as well. We further deduce that $\langle a\rangle$ has a complement in G, say B, by 2.1.2 of [6]. Hence 1.1.6 of [6] yields

$$\frac{|\langle a\rangle| \cdot |B|}{|\langle a\rangle \times B|} = |\langle a\rangle \cap B| = 1$$

and the Dedekind identity (see for example 1.1.11 of [6]) gives $A = \langle a\rangle(A \cap B)$. We conclude that $|A| = |\langle a\rangle \times \langle f(a)\rangle| = o(a)^2$ by 1.1.6 of [6]. Now, the same lemma shows that

$$|A \cap B| = \frac{|A| \cdot |B|}{|AB|} = \frac{o(a)^2 \cdot |B|}{|G|} = o(a) \cdot \frac{|\langle a\rangle| \cdot |B|}{|\langle a\rangle \times B|} = o(a).$$

From $(A \cap B) \cap \langle a\rangle = A \cap (B \cap \langle a\rangle) = A \cap 1 = 1$ and 1.2.6 of [6] it follows that $A \cap B \cong A \cap B/1 = (A \cap B)/((A \cap B) \cap \langle a\rangle) \cong ((A \cap B)\langle a\rangle/\langle a\rangle) = A/\langle a\rangle \cong (\langle f(a)\rangle \times \langle a\rangle)/\langle a\rangle \cong \langle f(a)\rangle/(\langle a\rangle \cap \langle f(a)\rangle) = \langle f(a)\rangle/1 \cong \langle f(a)\rangle$ is cyclic of maximal order.

Again we apply 2.1.2 of [6] to find a complement C of $A \cap B$ in B. But now C is a complement of A in G, as $AC = \langle a\rangle(A \cap B)C = \langle a\rangle B = G$ and $A \cap C \leqslant A \cap (B \cap C) = (A \cap B) \cap C = 1$. Altogether the first statement is true.

Let now $p \equiv 3$ mod 4 and $a \in G$ have maximal order. Then the cyclic group $\langle a\rangle \cap \langle f(a)\rangle$ admits an inverse ambiguous automorphism by Lemma 3.3. Hence Lemma 3.6 and our assumption that $p \equiv 3$ mod 4 imply that $\langle a\rangle \cap \langle f(a)\rangle = 1$. Thus $1 \neq A = \langle a, f(a)\rangle$ has rank 2 and a complement in G by the previous investigation. As $f(A) = A$ by Lemma 3.3, we obtain the assertion. □

Theorem 3.11. *Let* G *be a non-trivial abelian* p*-group for some prime* p *such that* $p \equiv 3$ *mod 4. Then* G *admits an inverse ambiguous automorphism if and only if* $G = A_1 \times ... \times A_n$ *for some positive integer* n *and such that for all* $i \in \{1, ..., n\}$ *the group* A_i *is the direct product of two cyclic groups of the same order.*

Proof. Let first n be a positive integer and $G = A_1 \times ... \times A_n$ be such that for all $i \in \{1, ..., n\}$ the group A_i is the direct product of two cyclic groups of the same order. Then Lemma 3.9 shows that A_i admits an inverse ambiguous automorphism. From Lemma 3.5 we deduce that G admits an inverse ambiguous automorphism.

Suppose now that G admits an inverse ambiguous automorphism. We prove the structure assertion of G via induction on the rank r of G.

If $r = 1$, then G is cyclic and Lemma 3.6 yields a contradiction. For $r = 2$ we obtain the assertion from Lemma 3.9.

Let $r \geqslant 3$. Then Lemma 3.10 provides an f-invariant subgroup $A \neq 1$ of G of rank at most 2 and such that A has a complement, say B, in G.

By Lemma 3.4 the mapping f induces an inverse ambiguous automorphism $\bar{f}$ on G/A via $\bar{f}(Ax) = Af(x)$ for all $x \in G$, since A is f-invariant. In particular $B \cong G/A$ admits an inverse ambiguous automorphism. Induction yields that $B = A_1 \times ... \times A_n$ for some positive integer n and such that for all $i \in \{1, ..., n\}$ the group A_i is the direct product of two cyclic groups of the same order.

We set $A_{n+1} := A$. As A has rank at most 2, Lemma 3.6 implies that A_{n+1} has rank 2. Since A is f-invariant, Lemma 3.9 shows that $A_{n+1} = A$ is the direct product of two cyclic groups of the same order.

Altogether we have $G = B \times A = A_1 \times ... \times A_{n+1}$ and for all $i \in \{1, ..., n+1\}$ the group A_i is the direct product of two cyclic groups of the same order. □

4. Inverse ambiguous automorphisms on 2-groups

We now turn our attention to the remaining prime 2. The next lemma shows that the structure of 2-groups of rank 2 admitting an inverse ambiguous automorphism is more complicated to describe.

Lemma 4.1. *Let $G = \langle a \rangle \times \langle b \rangle$ be an abelian 2-group. If $o(a) = \frac{1}{2} o(b)$, then $f\colon G \to G$ defined via $f(a^i b^j) := a^{j-i} b^{j-2i}$ is an inverse ambiguous automorphism.*

Proof. Notice that $o(ab^2) = o(a)$, $o(b) = o(ab)$ and $G = \langle a \rangle \times \langle b \rangle = \langle ab^2 \rangle \times \langle ab \rangle$. So the function $f\colon G \to G$ defined via $f(a) = a^{-1}b^{-2}$ and $f(b) = ab$ is an isomorphism. From $f^2(a) = a^{-1}$, $f^2(b) = b^{-1}$ and Lemma 3.1 we see that f is an ambiguous isomorphism. □

Lemma 4.2. *Let p be a prime and G be a non-trivial abelian p-group. If G admits an inverse ambiguous automorphism f such that $f(x) = x$ for all elements x of order p, then G is an elementary abelian 2-group.*

Proof. As $G \neq 1$, there is some element $x \in G$ of order p. The assumption implies that $\langle x \rangle$ is f-invariant. Thus Lemma 3.1 shows that $x^{-1} = f(f(x)) = f(x) = x$. We deduce that $2 = o(x) = p$.

Suppose for a contradiction that G has some element y of order 4. Then we have $f(y)^2 = f(y^2) = y^2 \in \langle y \rangle \cap \langle f(y) \rangle$. This implies together with Lemma 3.3 and Lemma 3.6 that the cyclic group $\langle y \rangle \cap \langle f(y) \rangle$ has order 2. With 1.1.6 of [6] we calculate that $A := \langle y, f(y) \rangle$ has order

$$|\langle y \rangle \cdot \langle f(y) \rangle| = \frac{o(y) \cdot o(f(y))}{|\langle y \rangle \cap \langle f(y) \rangle|} = \frac{4 \cdot 4}{2} = 8.$$

Since A is not cyclic 2.1.2 of [6] provides some element $b \in A$ of order 2 such that $A = \langle y \rangle \times \langle b \rangle$. Furthermore $f(y) \in A \backslash \langle y \rangle$ and hence there is some integer i such that $f(y) = y^i \cdot b$. We conclude from Lemma 3.1:

$$y^{-1} = f(f(y)) = f(y)^i \cdot f(b) = (y^i \cdot b)^i \cdot b = y^{i^2} \cdot b^{i+1}.$$

This implies that $b^{i+1} = 1$ and $i^2 \equiv -1 \bmod 4$; a contradiction. We conclude that $x^2 = 1$ for all $x \in G$ and so G is an elementary abelian 2-group. □

Lemma 4.3. *Let G be an abelian 2-group of rank 2. If G admits an inverse ambiguous automorphism f, then G is elementary abelian and f is the identity, or there is an element $a \in G$ such that $G = \langle a, f(a) \rangle$ and $|G| \in \{o(a)^2, \frac{1}{2}o(a)^2\}$.*

In particular, G admits an inverse ambiguous automorphism if and only if we have $G = \langle a \rangle \times \langle b \rangle$ with $o(b) \in \{o(a), \frac{1}{2}o(a)\}$.

Proof. Let f be an inverse ambiguous automorphism of G. Similarly to the proof of Lemma 3.9, we investigate an element $a \in G$ of maximal order. Then, since G is generated by two elements and f is an automorphism, we have $|G| \leqslant o(a)^2$ and $o(f(a)) = o(a)$. Hence Lemma 3.3 and Lemma 3.6 yield $|\langle a \rangle \cap \langle f(a) \rangle| \leqslant 2$.

Thus $\langle a, f(a) \rangle \leqslant G$ and

$$|\langle a, f(a) \rangle| = \frac{o(a)o(f(a))}{|\langle a \rangle \cap \langle f(a) \rangle|} \geqslant \frac{1}{2}o(a)^2$$

by 1.1.6 of [6].

If $G = \langle a, f(a) \rangle$, then the first statement holds. Hence we may suppose that $G \neq \langle a, f(a) \rangle$. This is only possible in the case of $|\langle a \rangle \cap \langle f(a) \rangle| = 2$ and $|G| = o(a)^2$. Since a has maximal order 2.1.2 of [6] implies that $\langle a \rangle$ has a complement in G. Hence, there is some element $b \in G$ such that $G = \langle a \rangle \times \langle b \rangle$ and our assumption implies that $o(b) = |G : \langle a \rangle| = o(a)$.

Again, if $G = \langle b\rangle \times \langle f(b)\rangle$, then the first statement holds, as $G = \langle b, f(b)\rangle$ and $|G| = o(a)^2 = o(b)^2$. Hence we may suppose that $G \neq \langle b, f(b)\rangle$. Then, as above, we have $|\langle b\rangle \cap \langle f(b)\rangle| = 2$. In particular f fixes the element of order 2 in $\langle b\rangle$ and f fixes the element of order 2 in $\langle a\rangle$. These elements of order 2 are different, as $G = \langle a\rangle \times \langle b\rangle$. It follows from 2.1.9 of [6], that G has exactly three elements of order 2. Hence we conclude that f fixes every element of order 2. Then Lemma 4.2 implies that G is elementary abelian and f is the identity.

Altogether we have shown that $G = \langle a, f(a)\rangle$, or $G = \langle b, f(b)\rangle$, or that G is elementary abelian. This is the first statement.

In all cases $G = \langle a\rangle \times \langle c\rangle$ with $o(c) \in \{o(a), \frac{1}{2}o(a)\rangle$ for some $c \in \{f(a), b\}$.

Let conversely $G = \langle a\rangle \times \langle b\rangle$ with $o(b) \in \{o(a), \frac{1}{2}o(a)\}$. Then G admits an inverse ambiguous automorphism by Lemma 3.8 or Lemma 4.1. □

The next lemma generalises Lemma 3.10.

Lemma 4.4. *Let G be a non-trivial abelian 2-group admitting an inverse ambiguous automorphism f. Then G contains an element a of maximal order such that $\langle a, f(a)\rangle$ has a complement in G.*

Proof. Suppose for a contradiction that the lemma is false. Then let G be a counterexample of minimal order.

(I) *For every $g \in G$ of maximal order the group $\langle f(g)\rangle \cap \langle g\rangle$ has order 2.*

Proof. Let $g \in G$ have maximal order. Then Lemma 3.10 and our assumption that G is a counterexample imply that $\langle f(g)\rangle \cap \langle g\rangle \neq 1$. Since $\langle f(g)\rangle \cap \langle g\rangle$ is a cyclic and f-invariant 2-group by Lemma 3.3, we obtain the assertion from Lemma 3.6.

(II) *G is not elementary abelian.*

Proof. Suppose for a contradiction that G is elementary abelian and let $g \in G\backslash 1$. Then $o(g) = 2$ and g has maximal order. Thus $\langle g\rangle$ has a complement in G by 2.1.2 of [6]. From $1 \neq \langle g\rangle \cap \langle f(g)\rangle \leqslant \langle g\rangle = \{1, g\}$ it follows that $f(g) = g$ and so $\langle g, f(g)\rangle = \langle g\rangle$ has a complement in G.

(III) *If $a \in G$ has maximal order, then exactly one element of order 2 in $\langle a, f(a)\rangle$ is fixed by f. This fixed element of order 2 is an element of $\langle a\rangle \cap \langle f(a)\rangle$.*

Proof. From Lemma 3.3 we see that $\langle a, f(a)\rangle$ and $\langle a\rangle \cap \langle f(a)\rangle$ admit inverse ambiguous automorphisms. In addition $\langle a\rangle \cap \langle f(a)\rangle$ has two elements by (I). Therefore the element of order 2 in $\langle a\rangle \cap \langle f(a)\rangle$ is fixed.

On the other hand $o(a) \geqslant 4$ by (II). Hence Lemma 3.6 implies that $\langle a, f(a)\rangle$ is not cyclic. Consequently $\langle a, f(a)\rangle$ has rank 2. From Lemma 4.2 it moreover follows that $\langle a, f(a)\rangle$ contains an element of order 2 that is not fixed by f. We deduce that at least two elements of order 2 are permuted by f. Since $\langle a, f(a)\rangle$ has exactly three elements of order 2 (see 2.1.9 of [6]), we see that exactly one element of order 2 in $\langle a, f(a)\rangle$ is fixed by f.

(IV) *G has rank at least* 3.

Proof. If G was cyclic, then G had order 2 by Lemma 3.6 contradicting (II).

Suppose for a contradiction that G has rank 2. Then G contains exactly three elements of order 2 by 2.1.9 of [6]. Further there are $a, b \in G$ such that $G = \langle a\rangle \times \langle b\rangle$. We choose notation such that $o(a) \geqslant o(b)$ and set $A := \langle a, f(a)\rangle = \langle a\rangle\langle f(a)\rangle$.

Then a is an element of maximal order in G. From this and 1.1.6 of [6] we deduce that $|G| = o(a)o(b) \leqslant o(a)^2$. In addition

$$|G| \geqslant \frac{|\langle a\rangle| \cdot |\langle f(a)|}{|\langle a\rangle \cap \langle f(a)\rangle|} = \frac{1}{2}o(a)^2$$

by (I). In particular $A = G$ or $|G : A| = 2$. In the first case we obtain a contradiction, since 1 is a complement of G in G. We conclude that

$$\begin{aligned} 2 = |G : A| = \frac{|G|}{|A|} = \frac{|\langle a\rangle \times \langle b\rangle|}{|\langle a\rangle\langle f(a)\rangle|} \\ = \frac{o(a) \cdot o(b) \cdot |\langle a\rangle \cap \langle f(a)\rangle|}{o(a) \cdot o(f(a))} = \frac{2 \cdot o(b)}{o(f(a))} = 2 \cdot \frac{o(b)}{o(f(a))} \end{aligned}$$

by 1.1.6 of [6]. Hence $o(b) = o(a)$ is maximal and so (III) yields that the element of order 2 in $\langle a\rangle \cap \langle f(a)\rangle$ and the element of order 2 in $\langle b\rangle \cap \langle f(b)\rangle$ are fixed. From $G = \langle a\rangle \times \langle b\rangle$ and 2.1.9 of [6] we see that at least two of the three involutions in G are fixed by f. Consequently every element of order 2 in G is fixed by f. But now (II) contradicts Lemma 4.2.

(V) *G contains at least two elements of order* 2 *that are fixed by f.*

Proof. Suppose for a contradiction that G has exactly one element of order 2 fixed by f. Then we apply 9.1.1 (b) of [6] on $V := \{g \in G \mid g^2 = 1\}$. Since G is abelian, V is an elementary abelian subgroup of G that is f-invariant. In particular we see that $f(g) = f(g)^{-1}$ for all $g \in V$. It follows that $[g, f, f] = [g^{-1}f(g), f] = gf(g)^{-1}f(g^{-1})f(f(g)) = gf(g)f(g)^{-1}g^{-1} = 1$. In addition our assumption implies that $C_V(f) := \{g \in V \mid f(g) = g\}$ has order 2. Thus 9.1.1 of [6] is applicable and Part (b) implies that $|\{g \in G \mid g^2 = 1\}| \leqslant 2^2 = 4$. This and 1.29 of [6] force G to have rank at most 2. This contradicts (IV).

Let now $b \in G$ have maximal order and set $B = \langle b, f(b)\rangle$. Then (III) and (V) provide some $c \in G\backslash B$ such that $c^2 = 1$ and $f(c) = c$. Let $- : G \to G/\langle c\rangle$

be the natural homomorphism. Then Lemma 3.4 shows that $\bar{G}$ admits the inverse ambiguous automorphism $\bar{f}$ defined via $\bar{f}(\bar{x}) = \overline{f(x)}$.

Since G is a minimal counterexample and $|\bar{G}| < |G|$ we find some $\bar{a} \in \bar{G}$ of maximal order such that $\langle \bar{a}, \bar{f}(\bar{a})\rangle$ has a complement $\bar{C}$ in $\bar{G}$. Let $C \leqslant G$ be the full pre-image of $\bar{C}$ and choose $a \in G$ as a pre-image of $\bar{a}$.

(VI) $o(b) = o(a) = o(\bar{a})$.

Proof. From $c \notin B$ and 1.2.6 of [6] we obtain that $\bar{B} = B\langle c\rangle/\langle c\rangle \cong B/(B \cap \langle c\rangle) \cong B$. In particular we get $o(\bar{b}) = o(b)$. From $o(b) \geqslant o(a) \geqslant o(\bar{a}) \geqslant o(\bar{b}) = o(b)$ we finally see that $o(b) = o(a) = o(\bar{a})$.

(VII) $c \notin \langle f(a), a\rangle$

Proof. Suppose for a contradiction that $c \in \langle f(a), a\rangle$. Then (VI) and (III) imply that $c \in \langle a\rangle \cap \langle f(a)\rangle \leqslant \langle a\rangle$. But this implies the contradiction that $o(\bar{a}) = \frac{1}{2}o(a)$.

We will finally show that C is a complement of $\langle a, f(a)\rangle =: A$ in G.

For this we first observe that $\bar{A} = \overline{\langle a, f(a)\rangle} = \langle \bar{a}, \overline{f(a)}\rangle = \langle \bar{a}, \bar{f}(\bar{a})\rangle$. It follows that $\bar{G} = \bar{A} \cdot \bar{C}$. As C is the full pre-image of $\bar{C}$ in G, we get $G = AC$. Moreover $\bar{A} \cap \bar{C} = 1$ implies that $A \cap C \leqslant \langle c\rangle$ and so $A \cap C \leqslant A \cap \langle c\rangle = 1$ by (VII). □

Theorem 4.5. *Let G be a non-trivial abelian 2-group. Then G admits an inverse ambiguous automorphism if and only if $G = A_1 \times ... \times A_n$ for some positive integer n, where for all $i \in \{1, ..., n\}$ the group A_i is elementary abelian, or of the form in Lemma 4.3.*

Proof. Suppose first that $G = A_1 \times ... \times A_n$ for some positive integer n and for all $i \in \{1, ..., n\}$ the group A_i is elementary abelian, or of the form in Lemma 4.3. If A_i is an elementary abelian 2-group, then the identity is inverse ambiguous. Otherwise Lemma 4.3 shows that A_i admits an inverse ambiguous automorphism. From Lemma 3.5 we deduce that $G := A_1 \times ... \times A_n$ admits an inverse ambiguous automorphism.

Conversely, suppose that G admits an inverse ambiguous automorphism. We prove the structure assertion of G via induction on the rank r of G.

If $r = 1$, then G is cyclic. In this case Lemma 3.6 implies that G is elementary abelian of order 2 and hence the assertion is true.

If $r = 2$, then the second part of Lemma 4.3 implies the assertion.

Suppose that $r \geqslant 3$. Then Lemma 4.4 provides an f-invariant subgroup $A \neq 1$ of G of rank at most 2 and such that A has a complement, say B, in G.

By Lemma 3.4 the mapping f induces an inverse ambiguous automorphism $\bar{f}$ on G/A via $\bar{f}(Ax) = Af(x)$ for all $x \in G$, since A is f-invariant. In particular $B \cong G/A$ admits an inverse ambiguous automorphism. Induction yields that

$B = A_1 \times ... \times A_n$ for some positive integer n and such that for all $i \in \{1, ..., n\}$ the group A_i is elementary abelian, or of the form in Lemma 4.3.

We set $A_{n+1} := A$. If A is cyclic, then Lemma 3.6 implies that $A = A_{n+1}$ has order 2 and is hence elementary abelian. If A has rank 2, then we see from Lemma 4.3 that $A = A_{n+1}$ has the desired structure, as A is f-invariant.

In both cases we have $G = B \times A = A_1 \times \ldots \times A_{n+1}$ and for all $i \in \{1, \ldots, n+1\}$ the group A_i is elementary abelian, or of the form in Lemma 4.3. □

THEOREM 4.6. *Let G be a finite group, then G admits an inverse ambiguous automorphism if and only if $G = A_1 \times \ldots \times A_n$ for some positive integer n and for every $i \in \{1, \ldots, n\}$ one of the following holds:*

(a) *A_i is an abelian p-group for some prime $p \equiv 1 \mod 4$,*
(b) *A_i is a direct product of two cyclic groups of the same order,*
(c) *there is a positive integer r such that A_i is a direct product of two cyclic groups of order 2^r and 2^{r+1},*
(d) *A_i is an elementary abelian 2-group.*

PROOF. For every $U \leqslant G$ we denote by $\pi(U)$ the set of all primes dividing $|U|$.

Let first G admit an inverse ambiguous automorphism f. Then Lemma 3.2 forces G to be abelian. So 2.1.6 of [6] yields that $G = \bigtimes_{p\in\pi(G)} G_p$, where for all $p \in \pi(G)$ we have $G_p := \{x \in G \mid o(x) \text{ is a power of } p\}$. Furthermore 2.1.5 of [6] implies that $f(G_p) = G_p$ for all $p \in \pi(G)$. In particular for every $p \in \pi(G)$ the group G_p admits an inverse ambiguous function.

We choose $p \in \pi(G)$. If $p \equiv 1$ mod 4, then G_p has the structure described in (a). If $p \equiv 3$ mod 4, then Theorem 3.11 yields that $G_p = A(p)_1 \times ... \times A(p)_{n_p}$ for some positive integer n_p, where for all $i \in \{1, ..., n_p\}$ the group $A(p)_i$ is the direct product of two cyclic groups of the same order. In the last case, if $p = 2$, then Theorem 4.5 gives that $G_2 = A(2)_1 \times ... \times A(2)_{n_2}$ for some positive integer n_2, where for all $i \in \{1, ..., n_2\}$ the group $A(2)_i$ is elementary abelian, or of the form in Lemma 4.3. In particular $A(2)_i$ has one of the structures described in (b), (c), or (d).

Altogether we have

$$\begin{aligned} G = \bigtimes_{p\in\pi(G)} G_p &= G_2 \times \bigtimes_{\substack{p\in\pi(G)\\ p\equiv 1 \bmod 4}} G_p \times \bigtimes_{\substack{p\in\pi(G)\\ p\equiv 3 \bmod 4}} G_p \\ &= (A(2)_1 \times ... \times A(2)_{n_2}) \times \bigtimes_{\substack{p\in\pi(G)\\ p\equiv 1 \bmod 4}} G_p \times \bigtimes_{\substack{p\in\pi(G)\\ p\equiv 3 \bmod 4}} (A(p)_1 \times ... \times A(p)_{n_p}). \end{aligned}$$

Hence, G has the desired structure.

Let, conversely, n be a positive integer such that $G = A_1 \times ... \times A_n$ is an abelian group and for every $i \in \{1, ..., n\}$ the group A_i has one of the structures described in (a), (b), (c) or (d).

Let $i \in \{1, ..., n\}$. If A_i is as in (a), then Theorem 3.7 shows that A_i admits an inverse ambiguous automorphism. If A_i satisfies (b) or (c), then Lemma 3.8 or Lemma 4.1, respectively, provide an inverse ambiguous automorphism on A_i. Finally if A_i is an elementary abelian 2-group, then the identity is inverse ambiguous on A_i.

Consequently for each $i \in \{1, ..., n\}$ the group A_i admits an inverse ambiguous automorphism. Thus Lemma 3.5 implies that G admits an inverse ambiguous automorphism, too. □

References

[1] Y. Berkovich, *Groups of Prime Power Order*, Vol. 1, De Gruyter Expositions in Mathematics, 46, Walter de Gruyter GmbH & Co. KG, Berlin, 2008.

[2] R. Cheng, A. Dasgupta, B.R. Ebanks, L.F. Kinch, L.M. Larson and R.B. McFadden, *When does $f^{-1} = 1/f$?*, Amer. Math. Monthly **105** (1998), no. 8, 704–717.

[3] R. Euler and J. Foran, *On functions whose inverse is their reciprocal*, Math. Mag. **54** (1981), no. 4, 185–189.

[4] M. Griffiths, *$f(f(x)) = x$, windmills, and beyond*, Math. Mag. **83** (2010), no. 1, 15–23.

[5] M. Herzog, *Counting group elements of order p modulo p^2*, Proc. Amer. Math. Soc. **66** (1977), no. 2, 247–250.

[6] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups. An Introduction*, Springer-Verlag, New York, 2004.

[7] D.J. Schmitz, *Inverse ambiguous functions on fields*, Aequationes Math. **91** (2017), no. 2, 373–389.

[8] D. Schmitz and K. Gallagher, *Inverse ambiguous functions on some finite non-abelian groups*, Aequationes Math. **92** (2018), no. 5, 963–973.

[9] R. Schnabel, *Elemente der Gruppentheorie*, Mathematik für die Lehrerausbildung, B.G. Teubner, Stuttgart, 1984.

Institut für Mathematik
Martin-Luther-Universität Halle-Wittenberg
06099 Halle (Saale)
Germany
e-mail: imke.toborg@mathematik.uni-halle.de