Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-024-01463-1

The classifications of o-monomials and of 2-to-1 binomials are equivalent

Lukas Kölsch[1] · Gohar Kyureghyan[2]

Received: 28 February 2024 / Revised: 5 June 2024 / Accepted: 12 July 2024

Abstract

We observe that on the binary finite fields the classification of 2-to-1 binomials is equivalent to the classification of o-monomials, which is a well-studied and elusive problem in finite geometry. This connection implies a complete classification of 2-to-1 binomials $b = x^d + ux^e$ for a large set of values of (d, e). Further, we show that a number of the known infinite families of 2-to-1 maps can be traced back to o-polynomials or to difference maps of APN maps. We also provide some connections between 2-to-1 maps and hyperovals in non-desarguesian planes.

Keywords 2-to-1 binomial · o-monomial · Hyperoval

Mathematics Subject Classification 11T06 · 51E21

1 Introduction

We call $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ a 2-to-1 map if every $y \in \mathbb{F}_{2^n}$ has either no or exactly two preimages, that is $|f^{-1}(y)| \in \{0, 2\}$. These maps appear naturally in many areas of research that relate to binary finite fields, like APN functions, bent functions [2] and hyperovals in finite geometry. Applications to the construction of special codes are for instance considered in [14, 17]. Compared to permutations, 2-to-1 maps have been less studied so far. A first systematic study has been started recently in [18] and was continued in [15, 19, 22]. Some of these papers describe infinite families of 2-to-1 maps. The presented there proofs are often quite technical, relying for instance on the study of related resultants that are partly calculated with computer help. In this paper, we show that many of these constructions arise naturally from previously known combinatorial objects. This connection implies then on the one side simple proofs along with natural explanations for the 2-to-1 property, and on the other side

Dedicated in memory of Kai-Uwe Schmidt.

✉ Gohar Kyureghyan
gohar.kyureghyan@uni-rostock.de

[1] University of South Florida, Tampa, USA

[2] University of Rostock, Rostock, Germany

Published online: 30 July 2024

it suggests a generic method for producing 2-to-1 maps, which may be designed to satisfy some additional properties if required.

In Sect. 2, we give some background of hyperovals in the desarguesian plane which we use in later sections. In Sect. 3, we show that all 2-to-1 binomials on $\mathbb{F}_{2^n}$ are constructed from certain hyperovals in the desarguesian plane and vice versa (Theorem 3.2). Using the classification of o-monomials of low degree, we obtain a complete classification of 2-to-1 binomials $b = x^d + ux^e$ for a large set of exponents (d, e) (Theorem 3.5). In Sect. 4, we use hyperovals and (in one case) APN maps to give short clear proofs of the 2-to-1 property for many infinite families of maps considered in [15, 19]. Our techniques also allow to extend these families of 2-to-1 maps in a straightforward manner and to prove a stronger version of a conjecture [19, Conjecture 12] on a specific family of 2-to-1 maps (Proposition 4.3). More importantly, our proof steps suggest a generic method for producing 2-to-1 maps with specific properties. In Sect. 5, we observe that hyperovals in non-desarguesian planes can also be used to construct 2-to-1 maps, similar to the desarguesian case.

2 Background on hyperovals in $PG(2, 2^n)$

A hyperoval in the desarguesian projective plane $PG(2, 2^n)$ is a set of $2^n + 2$ points such that no three of them are collinear. The following well-known result shows that the hyperovals in $PG(2, 2^n)$ correspond to a special class of permutations on $\mathbb{F}_{2^n}$ (see e.g. [12]).

Theorem 2.1 *Let $n \geq 2$. A hyperoval in $PG(2, 2^n)$ can be written in the form*

$$\mathcal{H}(f) = \{(1, t, f(t)) \colon t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, 0), (0, 0, 1)\},$$

where f is a permutation of $\mathbb{F}_{2^n}$ with $f(0) = 0$, $f(1) = 1$ and such that for every $a \in \mathbb{F}_{2^n}$ the map $g_a(x) = (f(x + a) + f(a))x^{2^n-2}$ is also a permutation. Conversely, for every such a permutation f the set $\mathcal{H}(f)$ is a hyperoval.

We call polynomials f that satisfy the conditions in Theorem 2.1 (and thus define hyperovals) *o-polynomials*.

The following connection between o-polynomials and 2-to-1 maps is easy to verify, see e.g. [16].

Theorem 2.2 *A polynomial $f \in \mathbb{F}_{2^n}[x]$ with $f(0) = 0$ and $f(1) = 1$ is an o-polynomial if and only if the map $f(x) + ax$ is 2-to-1 on $\mathbb{F}_{2^n}$ for every $a \in \mathbb{F}_{2^n}^*$.*

Recall that any map of the finite field $\mathbb{F}_{2^n}$ is uniquely described by a polynomial over $\mathbb{F}_{2^n}$ of degree not exceeding $2^n - 1$, since $x^{2^n} = x$ for any $x \in \mathbb{F}_{2^n}$. Therefore, by abuse of notation, we consider the exponents of polynomials as elements in $\mathbb{Z}_{2^n-1}$. For a unit d in $\mathbb{Z}_{2^n-1}$, we denote by $1/d$ its inverse.

Next we list the known o-polynomials of $\mathbb{F}_{2^n}$:

- Translation hyperovals: $f(x) = x^{2^i}$ where $\gcd(i, n) = 1$,
- Segre hyperoval: $f(x) = x^6$ if n is odd,
- Glynn I hyperoval: $f(x) = x^{3\cdot 2^{\frac{n+1}{2}}+4}$ if n is odd,
- Glynn II hyperoval: $f(x) = x^{2^{(n+1)/2}+2^{(3n+1)/4}}$ if $n \equiv 1 \pmod 4$ and $f(x) = x^{2^{(n+1)/2}+2^{(n+1)/4}}$ if $n \equiv 3 \pmod 4$,
- Cherowitzo hyperoval: $f(x) = x^{2^{(n+1)/2}+2^{(n+1)/2+2}+2^{(3n+1)/4}+4}$ if n is odd,

- Payne hyperoval: $f(x) = x^{5/6} + x^{3/6} + x^{1/6}$ if n is odd.

The list is completed by the more complicated Subiaco [5] and Adelaide [4] o-polynomials.

Given a polynomial $f \in \mathbb{F}_{2^n}[x]$, let $\bar{f}(x)$ denote a polynomial describing the map satisfying $\bar{f}(0) = 0$ and $\bar{f} : y \mapsto yf(1/y)$ for $y \in \mathbb{F}_{2^n}^*$. Observe that $xf(x^{2^n-2}) \pmod{x^{2^n} + x}$ is the unique such polynomial of degree less than 2^n.

There are several transformations that preserve the property of being an o-polynomial.

Theorem 2.3 *Let f be an o-polynomial on $\mathbb{F}_{2^n}$. The following are then also o-polynomials on $\mathbb{F}_{2^n}$:*

- *f^{-1} (the compositional inverse),*
- *$\bar{f}$, defined by $\bar{f}(0) = 0$ and $\bar{f} : y \mapsto yf(1/y)$ for $y \in \mathbb{F}_{2^n}^*$,*
- *$f(x^{2^j})^{2^{n-j}}$ for any $1 \le j \le n-1$,*
- *$f(x+1) + f(1)$.*

A polynomial $g \in \mathbb{F}_{2^n}[x]$ is called *o-equivalent* to the o-polynomial $f \in \mathbb{F}_{2^n}[x]$ if it can be obtained from f via a transformation appearing in Theorem 2.3. For o-monomials Theorem 2.3 reduces to:

Corollary 2.4 *Let $f(x) = x^d$ be an o-monomial on $\mathbb{F}_{2^n}$. Then*

$$x^{1/d}, x^{1-d}, x^{\frac{1}{1-d}}, x^{\frac{d}{d-1}}, x^{\frac{d-1}{d}}$$

are the o-monomials that are o-equivalent to f.

3 Every 2-to-1 binomial is induced by an o-monomial

By Theorem 2.2, every o-monomial induces 2-to-1 binomials. In [15], the authors observe experimentally that all 2-to-1 maps in odd dimension up to $n = 7$ can be explained like this. For n even, the authors mention the obvious 2-to-1 map $x \mapsto x^{2^n-2} + x$ as a counterexample that all 2-to-1 maps are constructed via o-monomials. This is however not correct: Indeed the map $x \mapsto x^{2^n-2} + x$ is induced by the o-monomial x^{2^n-2} which is o-equivalent to x^2 by Corollary 2.4, since $1 - 2 \equiv 2^n - 2 \pmod{2^n - 1}$.

We show in this section, that *all* 2-to-1 binomials on finite binary fields are induced by o-monomials. We would like to note that this statement can with some effort be deduced from Lemma 1 in [16] and the surrounding discussions.

Lemma 3.1 *Let $d < e$, $u \in \mathbb{F}_{2^n}^*$ and $b(x) = x^d + ux^e$ be a 2-to-1 binomial on $\mathbb{F}_{2^n}$. Then* $\gcd(e-d, 2^n-1) = 1$.

Proof We have $b(x) = x^d(1+ux^{e-d})$. Now assume $\gcd(e-d, 2^n-1) > 1$. Then $x \mapsto x^{e-d}$ is not a permutation, so $1 + ux^{e-d} = 0$ has either 0 or $\gcd(e-d, 2^n-1)$ many non-zero solutions. Then $b(x) = 0$ has either precisely 1 or more than 2 solutions, violating the 2-to-1 property. □

Theorem 3.2 *Let $d < e$. If $b(x) = x^d + ux^e$ is a 2-to-1 binomial on $\mathbb{F}_{2^n}$ for some $u \in \mathbb{F}_{2^n}^*$, then* $\gcd(e-d, 2^n-1) = \gcd(e, 2^n-1) = \gcd(d, 2^n-1) = 1$. *For such exponents e, d, the following four statements are equivalent:*

1. *There is one $u \in \mathbb{F}_{2^n}^*$ such that the binomial $b(x) = x^d + ux^e$ is 2-to-1 on $\mathbb{F}_{2^n}$.*

2. *For every $u \in \mathbb{F}_{2^n}^*$ the binomial $b(x) = x^d + ux^e$ is 2-to-1 on $\mathbb{F}_{2^n}$.*
3. *$x^{d/e}$ is an o-monomial on $\mathbb{F}_{2^n}$.*
4. *The map $h : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, defined by*

$$h(1) = 0 \text{ and } h(\alpha) = \frac{\alpha^d + 1}{\alpha^e + 1} \text{ for } \alpha \neq 1,$$

is a permutation of $\mathbb{F}_{2^n}$.

Proof We have $b(x) = x^d(1 + ux^{e-d})$ with $\gcd(e - d, 2^n - 1) = 1$ using Lemma 3.1. Note that 0 always has 2 preimages under b since $b(0) = 0$ and $1 + ux^{e-d} = 0$ has precisely one non-zero solution. We may thus restrict ourselves to considering $x \neq 0$ and $ux^{e-d} \neq 1$. Then consider the equation $b(x) = b(\alpha x)$ with $x, \alpha \in \mathbb{F}_{2^m}^*$. Clearly, b is 2-to-1 if and only if for each fixed x this equation has precisely 2 solutions, one of which is $\alpha = 1$. We have $x^d(1 + ux^{e-d}) = \alpha^d x^d(1 + u\alpha^{e-d}x^{e-d})$, which is equivalent to

$$(\alpha^e + 1)ux^{e-d} = \alpha^d + 1. \tag{1}$$

For each $x \neq 0$, $ux^{e-d} \neq 1$ we must have exactly one $\alpha \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ that satisfies this equation. Thus there is a one-to-one correspondence between $S_u = \{x : x \in \mathbb{F}_{2^n}, x \neq 0, ux^{e-d} \neq 1\}$ and $T = \{\alpha : \alpha \in \mathbb{F}_{2^n}, \alpha \neq 0, 1\}$: For each fixed $x \in S_u$, Eq. (1) has one solution $\alpha \in T$ and vice versa.

We now show $\gcd(d, 2^n - 1) = \gcd(e, 2^n - 1) = 1$. Assume $\gcd(d, 2^n - 1) > 1$. Then there are $\alpha \in T$ such that $\alpha^d = 1$. For this α, the right hand side of Eq. (1) vanishes, so the equation can only have a solution if $\alpha^e = 1$. But then $\alpha^{e-d} = 1$, contradicting $\gcd(e - d, 2^n - 1) = 1$. We conclude $\gcd(d, 2^n - 1) = 1$. Repeating the same arguments for e instead of d also yields $\gcd(e, 2^n - 1) = 1$.

In particular, $\alpha^e \neq 1$ for $\alpha \in T$, so dividing Eq. (1) by $\alpha^e + 1$ yields

$$ux^{e-d} = \frac{\alpha^d + 1}{\alpha^e + 1}.$$

If x ranges over all elements in S_u, then the left hand side ranges exactly over all elements $\mathbb{F}_{2^n} \setminus \{0, 1\}$, independently of the choice of u. Thus, the number of solutions $x \in S_u$ of Eq. (1) for a fixed $\alpha \in T$ only depends on d and e; it is in particular independent of $u \in \mathbb{F}_{2^n}^*$, so $b_{u'}(x) = x^d + u'x^e$ is also 2-to-1 for any $u' \in \mathbb{F}_{2^n}^*$. We conclude with Theorem 2.2 that $b(x) = x^d + ux^e$ is 2-to-1 for a fixed $u \in \mathbb{F}_{2^n}^*$ if and only if $b(x) = x^{d/e} + ux$ is 2-to-1 for all $u \in \mathbb{F}_{2^n}^*$, i.e. $x^{d/e}$ is an o-monomial on $\mathbb{F}_{2^n}$. □

Observe that the map h in 4. of Theorem 3.2 is the composition of permutations $g_1(x+1)$, defined in Theorem 2.1, and $x \mapsto x^e$. Hence the equivalence of statements 3. and 4. in Theorem 3.2 is not new.

By Theorem 3.2, every 2-to-1 binomial can be traced back to an o-monomial. Hence a complete classification of 2-to-1 binomials is equivalent to a classification of o-monomials which is a known hard open problem. All presently known o-monomials are described in Sect. 2. The o-monomials on $\mathbb{F}_{2^n}$ with $n \leq 30$ have been classified by computer search [10]; no examples outside of the infinite families were found.

The next result was conjectured by Segre and Bartocci in [21] and confirmed in [11] by Hernando and McGuire. A short elegant proof of it is presented by Zieve in [24].

Theorem 3.3 [11] *If x^d is an o-monomial on $\mathbb{F}_{2^n}$ for infinitely many n then $d = 6$ or $d = 2^k$ for a positive integer k.*

Recall that a polynomial is called an exceptional permutation polynomial, if it defines a permutation on $\mathbb{F}_{2^n}$ for infinitely many n, [23]. Theorems 2.1 and 3.3 imply that the polynomial

$$h(x) = g_1(x+1) = \frac{x^d + 1}{x + 1}$$

is an exceptional permutation polynomial if and only if $d = 6$ or $d = 2^k$. Using the fact that any permutation polynomial on $\mathbb{F}_{2^n}$ of degree at most $2^{n/4}$ is exceptional, Theorem 3.3 yields the complete classification of o-monomials of degree at most $2^{n/4}+1$. This was generalized for arbitrary o-polynomials of degree less $2^{n/4-1}$ by Florian Caullery and Kai-Uwe Schmidt [3].

Theorem 3.4 [3, Theorem 1.2.] *If f is an o-polynomial on $\mathbb{F}_{2^n}$ of degree less than $2^{n/4-1}$ then f is o-equivalent to x^6 or x^{2^k} for a positive integer k.*

Theorem 3.2 and the above discussions yield a complete classification of 2-to-1 binomials $b(x) = x^d + ux^e$ for a large set of exponents (d, e). Recall that the condition $\gcd(d, 2^n - 1) = \gcd(e, 2^n - 1) = 1$ is necessary for $b(x)$ to be 2-to-1 on $\mathbb{F}_{2^n}$.

Theorem 3.5 *Let $d < e$, $u \in \mathbb{F}_{2^n}^*$ and $b(x) = x^d + ux^e$ with $\gcd(d, 2^n - 1) = \gcd(e, 2^n - 1) = 1$. Set*

$$S = \left\{ \frac{d}{e}, \frac{e}{d}, 1 - \frac{d}{e}, 1 - \frac{e}{d}, \frac{e}{e-d}, \frac{d}{d-e} \right\} \subseteq \mathbb{Z}_{2^n-1},$$

where we take the elements in S to be between 1 and $2^n - 2$. Suppose, that at least one element in S does not exceed $2^{n/4} + 1$. Then the binomial $b(x)$ is 2-to-1 on $\mathbb{F}_{2^n}$ if and only if $6 \in S$ or $2^k \in S$ for some positive integer k.

Proof This follows from Theorems 3.2, 3.3 and the fact that any permutation of degree $\leq 2^{n/4}$ is exceptional. Note that the set S contains exactly the exponents of o-monomials that are o-equivalent to $x^{d/e}$ on $\mathbb{F}_{2^n}$. □

4 Explaining some known infinite families of 2-to-1 maps

In this section we show that many of the infinite families of 2-to-1 maps presented in [15, 19] can be traced back to a binomial and thus to an o-monomial via Theorem 3.2. In fact, six of the ten families of 2-to-1 quadrinomials presented in [15] are such cases. Along with a simple explanation of the 2-to-1 property, the connection to hyperovals suggests a straightforward way for extending these families. The next theorem generalizes the families presented in [15, 19], where only $a = 1$ was considered. More precisely, we extend the statements and clarify greatly the proofs of [15, Theorems V.1.1,2,5; Theorems V.4, V.5] and [19, Theorems 5 and 6(1)].

Theorem 4.1 *The following polynomials define 2-to-1 maps on $\mathbb{F}_{2^{2m+1}}$ for any $a \in \mathbb{F}_{2^{2m+1}}^*$:*

- $F_1(x) = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + ax,$
- $F_2(x) = x^{2^{m+1}+2} + ax^{2^{m+1}+1} + (a+1)x^{2^{m+1}} + x^2 + ax,$
- $F_3(x) = x^{2^n-2} + x^{2^n-2^{m+1}} + x^{2^n-2^{m+1}-2} + ax,$
- $F_4(x) = x^6 + x^4 + ax^3 + (a+1)x^2 + ax,$
- $F_5(x) = ax^6 + x^5 + x^3 + x,$

- $F_6(x) = x^{2^{m+1}+2^m} + x^{2^{m+1}} + x^{2^m} + ax^3 + ax^2 + ax$,
- $F_7(x) = x^{16} + ax^{12} + x^8 + a^2x^6 + x^4 + a^4x^3$, *if m is even or equivalently if $3 \nmid 2^m + 1$.*

Proof F_1: Note that $x^{2^{m+1}}$ is an o-monomial belonging to a translation hyperoval. Since

$$\frac{2^{m+1}}{2^{m+1}-1} \equiv 2^{m+1}(2^{m+1}+1) \equiv 2^{m+1}+2 \pmod{2^{2m+1}-1},$$

by Corollary 2.4, $x^{2^{m+1}+2}$ is an o-monomial, too. Then, by Theorem 2.3, also $(x+1)^{2^{m+1}+2} + 1 = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2$ is an o-polynomial, proving the statement.

F_2: Take again the o-monomial $x^{2^{m+1}}$. This monomial is o-equivalent to $x^{\frac{2^{m+1}+2}{2^{m+1}+1}}$, and thus the map $x \mapsto x^{\frac{2^{m+1}+2}{2^{m+1}+1}} + ax$ is 2-to-1 for any non-zero a. The map $x \mapsto x^{2^{m+1}+1}$ is a permutation, since $\gcd(2^{m+1}+1, 2^{2m+1}-1) = 1$. The composition of these two maps is $x \mapsto x^{2^{m+1}+2} + ax^{2^{m+1}+1}$, which is then 2-to-1 for any non-zero a. Finally, the substitution $x \mapsto x+1$ yields that $x \mapsto x^{2^{m+1}+2} + (a+1)x^{2^{m+1}} + ax^{2^{m+1}+1} + x^2 + ax$ is 2-to-1 for any non-zero a.

F_3: We start with the o-monomial $x \mapsto x^{2^{m+1}+2}$ which is o-equivalent to the translation o-monomial $x \mapsto x^{2^{m+1}}$ as described in the proof for F_1. Then $x \mapsto (x+1)^{2^{m+1}+2} + 1 = x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 = \overline{F_3}(x)$ is an o-polynomial by Theorem 2.3.

F_4: We start with the o-monomial $x \mapsto x^2$, implying the 2-to-1 maps $x \mapsto x^2 + ax$ for every non-zero a. Substituting $x \mapsto x^3$, we get the 2-to-1 maps $x \mapsto x^6 + ax^3$ and then the substitution $x \mapsto x+1$ leads to the result.

F_5: We take the Payne o-polynomial $P(x) = x^{5/6} + x^{3/6} + x^{1/6}$, so $x \mapsto x^{5/6} + x^{3/6} + x^{1/6} + ax$ is 2-to-1 for any non-zero a. Then $P(x^6) = ax^6 + x^5 + x^3 + x$ is 2-to-1, since $x \mapsto x^6$ permutes $\mathbb{F}_{2^{2m+1}}$.

F_6: Start with the 2-to-1 maps $x \mapsto x^{2^m} + ax, a \neq 0$ belonging to a translation hyperoval. The substitution $x \mapsto x^3$ yields $x \mapsto x^{2^{m+1}+2^m} + ax^3$ and then the substitution $x \mapsto x+1$ gives the result.

F_7: Observe that $F_7(x) = (x^4 + x^2 + x) \circ (x^4 + ax^3)$. Note that the zeros of the polynomial $x^4 + x^2 + x$ are in $\mathbb{F}_8$, since this polynomial describes the absolute trace map on $\mathbb{F}_8$. Since $3 \nmid 2m + 1$, the map $x \mapsto x^4 + x^2 + x$ is bijective on $\mathbb{F}_{2^{2m+1}}$. It then suffices to show that $x \mapsto x^4 + ax^3$ is 2-to-1 for any non-zero a. For this, consider the o-monomial x^4. By Corollary 2.4, $x^{4/3}$ is also an o-monomial, and thus $x \mapsto x^{4/3} + ax$ is 2-to-1 for any non-zero a. Substituting $x \mapsto x^3$ yields that $x \mapsto x^4 + ax^3$ is 2-to-1 and the result follows. □

Our proof of Theorem 4.1 shows that all 2-to-1 maps in its statement are secondary constructions, more precisely, compositions of permutations with 2-to-1 maps induced by o-polynomials via Theorem 2.2. Of course the list of Theorem 4.1 can be continued. For instance, in the proof of F_3, we also prove that $x \mapsto x^{2^{m+1}+2} + x^{2^{m+1}} + x^2 + ax$ is 2-to-1 on $\mathbb{F}_{2^{2m+1}}$ for any non-zero a. Another such example is the one given in Proposition 4.3. Observe that the substitution $x \mapsto x+1$ appears several times in the proofs of Theorem 4.1. The reason for this is that if the exponents of a sparse 2-to-1 polynomial have small binary weights, then the substitution $x \mapsto x+1$ produces again a sparse polynomial.

The connections we described so far can be applied to confirm a conjecture posed in [19, Conjecture 12].

Conjecture 4.2 *The map $F = x + x^3 + x^{2^{m+1}} + x^{2^{m+1}+2}$ is 2-to-1 over $\mathbb{F}_{2^{2m+1}}$.*

We prove the conjecture in a more general form by showing that it is induced by the Glynn I o-monomial.

Proposition 4.3 *For every $a \in \mathbb{F}_{2^{2m+1}}^*$, the map $F_a(x) = ax + (a+1)x^2 + ax^3 + x^{2^{m+1}} + x^{2^{m+1}+2}$ is 2-to-1 on $\mathbb{F}_{2^{2m+1}}$.*

Proof Let $G(x) = x^{3\cdot 2^{m+1}+4}$ be the o-monomial belonging to the Glynn I hyperoval. By Corollary 2.4, we have that $x^{\frac{3\cdot 2^{m+1}+4}{3\cdot(2^{m+1}+1)}}$ is an o-monomial that is o-equivalent to G. Note that $3\cdot 2^{m+1}+4 \equiv (2^{m+1}+2)(2^{m+1}+1) \pmod{2^{2m+1}-1}$, so

$$\frac{3\cdot 2^{m+1}+4}{3\cdot(2^{m+1}+1)} \equiv \frac{(2^{m+1}+2)(2^{m+1}+1)}{3\cdot(2^{m+1}+1)} \equiv \frac{2^{m+1}+2}{3} \pmod{2^{2m+1}-1}.$$

We conclude that $x^{\frac{2^{m+1}+2}{3}}$ is an o-monomial, and thus $x \mapsto x^{\frac{2^{m+1}+2}{3}} + ax$ is 2-to-1 for every $a \in \mathbb{F}_{2^{2m+1}}^*$. The substitution $x \mapsto x^3$ yields that $x \mapsto x^{2^{m+1}+2} + ax^3$ is 2-to-1 too, and a further substitution $x \mapsto x+1$ yields the result. □

Next we note, that another infinite family given in [19, Theorem 7(1)] is readily explained by an APN map. Recall that a map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if the difference map $D_{f,a}(x) = f(x+a) + f(x)$ is 2-to-1 for every non-zero a.

Proposition 4.4 [19, Theorem 7(1)] *The map given by $f(x) = x^{2^m+2} + x^{2^m+1} + x^{2^m} + x^3 + x^2 + x$ is 2-to-1 on $\mathbb{F}_{2^{2m+1}}$.*

Proof Up to the constant term, this is the difference map $D_{W,1}(x)$ for the APN Welch monomial $W(x) = x^{2^m+3}$ [8]. □

Again, the family only uses $D_{W,1}$, by considering $D_{W,a}$ for an arbitrary non-zero a, we can easily extend this result the result to construct the 2-to-1 maps $f(x) = ax^{2^m+2} + a^2x^{2^m+1} + a^3x^{2^m} + a^{2^m}x^3 + a^{2^m+1}x^2 + a^{2^m+2}x$ on $\mathbb{F}_{2^{2m+1}}$.

We conclude this section by observing that our proof ideas can also be used for secondary constructions of 2-to-1 maps with special properties like large/small degree, large/small multivariate degree or number of non-zero terms in its polynomial representation. Indeed, any o-polynomial $o(x)$ induces 2-to-1 polynomials $b(x) = o(x) + ax$ for any non-zero a. Compositions of $b(x)$ with permutations yield a large number of 2-to-1 maps. In order for the final 2-to-1 map to have some special properties, the permutations used in the compositions need to be chosen appropriately. For example, by composing with permutation monomials it could be possible to control the degree as well as the multivariate degree. Composing with an affine polynomial helps to control the number of terms.

5 2-to-1 maps from hyperovals in non-desarguesian planes

A hyperoval is a set of 2^n+2 points in a projective plane of order 2^n such that no three points are collinear. Using the definition, it is elementary to show that each line in the projective plane meets the hyperoval in exactly 0 or 2 points (i.e. all lines are either exterior or secants). In the previous sections, we explored the connection between 2-to-1 maps and hyperovals in the desarguesian plane $PG(2, 2^n)$. However, the 2-to-1 property is intrinsic to the geometric object and can thus also be recovered from hyperovals in non-desarguesian planes. The situation is a bit more delicate in the general case. Since the collineation group of non-desarguesian planes is different from the one of the desarguesian plane, we can in general no longer assume that a similar statement to Theorem 2.1 holds. Next we discuss the case of semifield planes (i.e. translation planes constructed from semifields; or, equivalently, translations planes whose dual is also a translation plane).

Let us first recall some definitions. A (finite) *semifield* is a finite set with two binary operations, addition and multiplication, that satisfies all axioms of a division ring, except for multiplicative associativity. The additive group of a semifield is always an elementary abelian p-group. A finite semifield S of size $q = p^n$ defines a projective plane of order p^n, just like the finite field does: We define the points of $\Pi(S)$ as $\{(1, a, b)\colon a, b \in S\} \cup \{(0, 1, a)\colon a \in S\} \cup \{(0, 0, 1)\}$. The q^2 points $\{(1, a, b)\colon a, b \in S\}$ are called the *affine points* of $\Pi(S)$. If $*$ is the multiplication of the semifield, then the lines are defined by $l_{a,b} = \{(1, a, a*x+b)\colon x \in S\} \cup \{(0, 1, a)\}$ for any $a, b \in S$, $l_a = \{(1, a, y)\colon y \in S\} \cup \{(0, 0, 1)\}$, $l_\infty = \{(0, 1, y)\colon y \in S\} \cup \{(0, 0, 1)\}$. Recall that a *translation hyperoval* in a projective plane of order 2^n is a hyperoval $\mathcal{H}$ such that

- the line at infinity l_∞ is secant to $\mathcal{H}$, and
- there is a subgroup of order 2^n in the translation group acting regularly on the 2^n affine points of $\mathcal{H}$.

Theorem 5.1 [9, Proposition 2.3.] *Let* Π *be a semifield plane of order* 2^n*. A translation hyperoval in* Π *is equivalent to a set of one of the following forms:*

(a) $\mathcal{H}(f) = \{(1, t, f(t))\colon t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, 0), (0, 0, 1)\}$, *where* f *is a bijective, additive map,*

(b) $\mathcal{H}(f) = \{(1, g(t), t)\colon t \in \mathbb{F}_{2^n}\} \cup \{(0, 1, \alpha), (0, 1, 0)\}$, *where* g *is a* 2*-to-*1 *additive map and* $\alpha \in \mathbb{F}_{2^n}^*$.

Since the hyperoval intersects the lines $l_{a,b} = \{(1, x, y)\colon y = a * x + b\}$ in 2 or 0 points, we immediately get that translation hyperovals of type a) yield $2^n - 1$ many 2-to-1 maps $h_a(x) = f(x) + a * x$ for any $a \in \mathbb{F}_{2^n}^*$ where f is the polynomial defining the hyperoval of type a). This of course generalizes the desarguesian case, see Theorems 2.1 and 2.2. With a bit more effort ([9, Eq. (6)]) a polynomial g defining a hyperoval of type b) yields also $2^n - 2$ many 2-to-1 maps via $h_a(x) = a * g(x) + x$ for any $a \notin \{0, \alpha\}$. Note that the maps h_a are additive, since f and g are.

Examples of sporadic hyperovals of both types in the binary Knuth semifield planes are found in [9, Tables 1 and 2]. An infinite family of hyperovals in Knuth semifield planes is given in [9, Theorem 2.5]. Using these hyperovals and the above discussion, we can hence obtain 2-to-1 maps. Note that it is not particularly hard to come up with a direct proof of the 2-to-1 property of these maps, but the result serves as an example how 2-to-1 maps can naturally be constructed using tools from finite geometry.

Corollary 5.2 *Let* $g(y) = y^2 + y$ *and define an operation* $*\colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *via* $x * y = xy + (y \operatorname{Tr}(x) + x \operatorname{Tr}(y))^2$, *where* Tr *denotes the absolute trace map. Then* $f(y) = a*g(y)+x$ *is* 2*-to-*1 *for any* $a \notin \{0, 1\}$.

Proof By [9, Theorem 2.5] the polynomial $g(y) = y^2 + y$ defines a hyperoval in the Knuth binary semifields of type (b) with $\alpha = 1$. The result follows from the preceding discussions. □

Again, we can apply a collineation of the projective plane to transform the o-polynomial $g(y) = y^2 + y$ into another (equivalent) translation o-polynomial of type (b) (for instance, $g'(y) = y^{2^{n-1}} + y^{2^{n-2}}$, as observed in [9]), yielding further 2-to-1 maps.

We want to note that translation hyperovals have also been constructed in translation planes that are not semifield planes, e.g. André planes [6] and Hall planes [13]. It has however also been observed that not all semifield planes contain a translation hyperoval [1]. For a complete classification of all hyperovals in all nondesarguesian planes of order 16 found by computer, see [20]. We leave as an open question if any hyperoval implies a construction for 2-to-1 maps.

Acknowledgements We thank Michael Zieve for informing us about the refinement of Theorem 3.4 in a recent paper [7], which in particularly implies that the statement holds for o-polynomials of degree not exceeding $2^{n/4}$.

Author Contributions Both authors were involved in any stage of preparing the manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest Gohar Kyureghyan is a member of the editorial board of DCC.

References

1. Allen K., Sheekey J.: On translation hyperovals in semifield planes. arXiv preprint arXiv:2309.01451 (2023).
2. Carlet C., Mesnager S.: On Dillon's class H of bent functions, Niho bent functions and o-polynomials. J. Comb. Theory Ser. A **118**(8), 2392–2410 (2011).
3. Caullery F., Schmidt K.-U.: On the classification of hyperovals. Adv. Math. **283**, 195–203 (2015).
4. Cherowitzo W., O'Keefe C., Penttila T.: A unified construction of finite geometries associated with q-clans in characteristic 2. Adv. Geom **3**, 1–21 (2003).
5. Cherowitzo W., Penttila T., Pinneri I., Royle G.F.: Flocks and ovals. Geom. Dedic. **60**, 17–37 (1996).
6. Denniston R.H.F.: Some non-desarguesian translation ovals. Ars Comb. **7**, 221–222 (1979).
7. Ding Z., Zieve M.E.: Determination of hyperovals by lines through a few points. arXiv preprint arXiv:2309.10866 (2023).
8. Dobbertin H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. IEEE Trans. Inf. Theory **45**(4), 1271–1275 (1999).
9. Durante N., Trombetti R., Zhou Y.: Hyperovals in Knuth's binary semifield planes. Eur. J. Comb. **62**, 77–91 (2017).
10. Glynn D.G.: A condition for the existence of ovals in PG(2, q), q even. Geom. Dedic. **32**(2), 247–252 (1989).
11. Hernando F., McGuire G.: Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes. Des. Codes Cryptogr. **65**, 275–289 (2012).
12. Hirschfeld J.: Ovals in desarguesian planes of even order. Annali di Matematica Pura ed Applicata **102**, 79–89 (1975).
13. Korchmáros G.: Inherited arcs in finite affine planes. J. Comb. Theory Ser. A **42**(1), 140–143 (1986).
14. Li K., Li C., Helleseth T., Qu L.: Binary linear codes with few weights from two-to-one functions. IEEE Trans. Inf. Theory **67**(7), 4263–4275 (2021).

15. Li K., Mesnager S., Longjiang Q.: Further study of 2-to-1 mappings over $\mathbb{F}_{2^n}$. IEEE Trans. Inf. Theory **67**(6), 3486–3496 (2021).
16. Maschietti A.: Difference sets and hyperovals. Des. Codes Cryptogr. **14**, 89–98 (1998).
17. Mesnager S., Qian L., Cao X., Yuan M.: Several families of binary minimal linear codes from two-to-one functions. IEEE Trans. Inf. Theory **69**(5), 3285–3301 (2023).
18. Mesnager S., Longjiang Q.: On two-to-one mappings over finite fields. IEEE Trans. Inf. Theory **65**(12), 7884–7895 (2019).
19. Mesnager S., Yuan M., Zheng D.: More about the corpus of involutions from two-to-one mappings and related cryptographic S-boxes. IEEE Trans. Inf. Theory **69**(2), 1315–1327 (2022).
20. Penttila T., Royle G.F., Simpson M.K.: Hyperovals in the known projective planes of order 16. J. Comb. Des. **4**(1), 59–65 (1996).
21. Segre B., Bartocci U.: Ovali ed altre curve nei piani di galois di caratteristica due. Acta Arith. **18**, 423–449 (1971).
22. Yuan M., Zheng D., Wang Y.P.: Two-to-one mappings and involutions without fixed points over $\mathbb{F}_{2^n}$. Finite Fields Their Appl. **76**, 101913 (2021).
23. Zieve M.: Exceptional polynomials. In: Handbook of finite fields, pp. 229–233. (2013).
24. Zieve M.: Planar functions and perfect nonlinear monomials over finite fields. Des. Codes Cryptogr. **75**, 71–80 (2015).