J Algebr Comb (2012) 35:477–496
DOI 10.1007/s10801-011-0310-8

Equivalence classes of functions between finite groups

K.J. Horadam

Received: 8 January 2011 / Accepted: 22 August 2011 / Published online: 14 September 2011

Abstract Two types of equivalence relation are used to classify functions between finite groups into classes which preserve combinatorial and algebraic properties important for a wide range of applications. However, it is very difficult to tell when functions equivalent under the coarser ("graph") equivalence are inequivalent under the finer ("bundle") equivalence. Here we relate graphs to transversals and splitting relative difference sets (RDSs) and introduce an intermediate relation, canonical equivalence, to aid in distinguishing the classes. We identify very precisely the conditions under which a graph equivalence determines a bundle equivalence, using transversals and extensions. We derive a new and easily computed algebraic measure of nonlinearity for a function f, calculated from the image of its coboundary ∂f. This measure is preserved by bundle equivalence but not by the coarser equivalences. It takes its minimum value if f is a homomorphism, and takes its maximum value if the graph of f contains a splitting RDS.

Keywords Equivalent functions · Graph of function · Finite field polynomial · Linear equivalence · Relative difference set · Nonlinear function · APN function

1 Introduction

Many equivalence relations for functions between finite groups exist: their usefulness depends on the groups, the types of functions and the purpose of the classification. In particular, classification of functions between finite rings and fields, as functions between the underlying finite abelian groups, is needed for applications in finite geometry, coding and cryptography.

K.J. Horadam (✉)
RMIT University, Melbourne, VIC 3001, Australia
e-mail: kathy.horadam@rmit.edu.au

Typically, classification of a set of functions between finite groups into equivalence classes will have value when each class consists of functions sharing common properties or invariants. Two quite separate approaches to defining equivalence for functions over $(GF(p^n),+)$, which preserve important algebraic or combinatorial properties across a wide range of interesting functions, have been used.

The first of these approaches involves pre- and post-composition of a given function $f : G \to G$, $G = GF(p^n)$, with other functions having specified characteristics, to obtain an equivalent function. Probably the earliest instance of this is the *weak equivalence* between f and f' introduced by Cavior [6] as

$$f' = \tau \circ f \circ \sigma \tag{1}$$

for any elements τ, σ of the symmetric group $\mathrm{Sym}(G)$ of G. Mullen [13] restricts τ and σ to (possibly equal) subgroups of $\mathrm{Sym}(G)$, so defining a relative form of weak equivalence, and shows, for instance, that a function f' is a permutation polynomial if and only if it is weakly equivalent to the identity polynomial $f(x) = x$. *Linear equivalence* (e.g. see [1, p. 80]) between f and f' is defined by

$$f' = \tau \circ f \circ \sigma + \chi, \tag{2}$$

where τ, σ are *linear* permutations and χ is linear, so is a coarsening of weak equivalence relative to linear permutations, by addition of a linear function.

The second approach involves defining equivalence between functions in terms of an equivalence between their graphs. This approach was introduced by Carlet, Charpin and Zinoviev [5, Proposition 3]. More generally, for a function $f : G \to N$ between finite *abelian* groups G and N, Pott [15] has recommended we focus on properties of the graph[1] $\{(f(x), x),\ x \in G\}$ of f as a means of measuring combinatorial and spectral properties of f.

In [11], the author generalises these two types of equivalence to functions $f : G \to N$ between arbitrary finite groups G and N, and shows that it is sufficient to work with the group $C^1(G,N)$ of normalised functions[2] (i.e. with $f(1) = 1$).

Definition 1 Two functions $f, f' \in C^1(G,N)$ are *bundle equivalent* if there exist $r \in G$, $\theta \in \mathrm{Aut}(G)$, $\gamma \in \mathrm{Aut}(N)$ and $\chi \in \mathrm{Hom}(G, \zeta(N))$ such that

$$f' = \bigl(\gamma \circ (f \cdot r) \circ \theta\bigr)\chi, \tag{3}$$

where $f \cdot r(x) = f(r)^{-1} f(rx)$ and $\zeta(N)$ is the centre of N.

Two functions $f, f' \in C^1(G,N)$ are *graph equivalent* if there exist $e \in N \times G$ and $\alpha \in \mathrm{Aut}(N \times G)$ such that

$$\alpha\bigl(\bigl\{\bigl(f(x), x\bigr), x \in G\bigr\}\bigr) = e\bigl\{\bigl(f'(x), x\bigr),\ x \in G\bigr\}. \tag{4}$$

[1] Usually the graph of f is the set $\{(x, f(x)) : x \in G\} \subset G \times N$, but we swap coordinates consistently, without loss of generality, for convenience later when working with split extensions.

[2] Usually $C^1(G,N)$ denotes the group of 1-cocycles, and N must be abelian. The notation is adopted here to cover the case of non-abelian N as well.

For example, suppose $G = N = (GF(p^n), +)$. Every $f \in C^1(G, G)$ is the evaluation map of some polynomial $f(x) \in GF(p^n)[x]$ of degree less than p^n with $f(0) = 0$. The homomorphisms $\mathrm{Hom}(G, G)$ are the linearised polynomials, and $\mathrm{Aut}(G)$ consists of the linearised permutation polynomials. Weak equivalence (1) relative to $\mathrm{Aut}(G)$ is the case $r = 0$, $\chi \equiv \mathbf{0}$ of (3) and linear equivalence (2) is the case $r = 0$ of (3).

The equivalence defined by (3) is known implicitly to finite geometers because planar functions equivalent by (3) will determine isomorphic planes [7]. Planarity of $f(x)$ is preserved by the operations of linear transformation, addition of a linearised polynomial of G or pre- or post-composition with a linearised permutation polynomial. In particular, if $r \in G$, then the linear transformation $f(x + r) - f(r)$ is $(f \cdot r)(x)$.

When (3) is extended to include un-normalised functions, it coincides with *extended affine (EA) equivalence*, introduced in [3], and now one of the main classifying equivalences for cryptographic functions. A very large number of cryptographically strong *almost perfect nonlinear* (APN) functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ have been found in the past 5 years, and it is important to be able to tell if they are genuinely new.

The choice of equivalence relation best suited to classify cryptographic functions has attracted considerable attention in this period. This has been prompted by the observation that if f is invertible, then its compositional inverse $\mathrm{inv}(f)$ has the same cryptographic robustness as f with respect to several measures of nonlinearity, so the inverse of a function is often regarded as being equivalent to it. However, $\mathrm{inv}(f)$ is not always EA equivalent to f.

One other equivalence has been very influential in this context. *CCZ equivalence* (which is, in fact, graph equivalence (4) for this case) is a coarser equivalence than EA equivalence and includes permutations and their inverses in the same equivalence class. It was originally proposed by Carlet, Charpin and Zinoviev [5, Proposition 3] for $p = 2$ (as cited in [3]), though Breveglieri et al. [1] appear to have arrived independently at the same idea, much later. In [3], translation by $e \in G \times G$ is on the right, rather than on the left as in (4), but composition with the inner automorphism defined by e shows they give the same CCZ equivalence classes. In [1], the graph of f is called the *implicit embedding* and no translation is included. It is currently very difficult to decide, either theoretically or computationally, whether two APN functions are CCZ (graph) equivalent, and if so, whether they are EA (bundle)-inequivalent.

In previous work [11], the author shows that in the general case of functions $f : G \to N$ between arbitrary finite groups G and N, bundle and graph equivalence have a common source in the equivalence relation for splitting semiregular relative difference sets (RDSs). Furthermore, graph equivalent functions f and f' are related by a formula

$$f' = \big(\beta \circ (f \cdot r) \circ \sigma\big)(\xi \circ \sigma), \tag{5}$$

where σ is a permutation of restricted type and β and ξ are homomorphisms. This formula is an intriguing mix of weak equivalence (1) and bundle equivalence (3).

This paper has three aims. The first aim is to pin down very precisely the relationship between graphs, transversals and splitting RDSs in $N \times G$, relative to $N \times \{1\}$. This is presented in Sect. 3, and involves introduction of an intermediate equivalence relation, *canonical equivalence*, which is coarser than bundle equivalence but finer than graph equivalence. In Theorem 2, we show that if the graph of f contains a splitting RDS, then the graph generates $N \times G$ and the canonical equivalence class of f equals its bundle equivalence class.

The second aim is to identify exactly the conditions under which the formula in (5) is rewritable as the formula in (3). This work is undertaken in Sect. 4 and the identification appears in Corollary 4. Proof takes two steps (Theorem 3 and Theorem 4), using the relationship between graphs and transversals identified in Sect. 3. The technical effort here only arises because N is arbitrary and we work with commuting diagrams of split extensions of N by G. In the elementary abelian case $N = \mathbb{Z}_p^n$, each canonical equivalence class is a single bundle equivalence class. This has implications for the classification of APN functions.

The third aim is to investigate invariants of our equivalence classes. We note that a combinatorial measure of nonlinearity, differential uniformity, is preserved by all three equivalences. When G and N are abelian, a spectral measure, maximal nonlinearity, is also preserved by all three equivalences. A new algebraic measure, $N(f)$, which is invariant on bundles but not in general on canonical or graph bundles, is derived. It is defined as $N(f) = |\widehat{N}_f|$, where

$$\widehat{N}_f = \left\{aba^{-1} : a \in N, b \in \left\langle f(x)f(y)f(xy)^{-1}, x, y \in G\right\rangle\right\}. \tag{6}$$

If f is a group homomorphism, $N(f)$ takes its minimum value 1, and if the graph of f contains a splitting RDS, $N(f)$ takes its maximum value $|N|$. This work appears in Sect. 5.

The next section covers the necessary background and terminology. A brief summary and discussion of future research questions appears in Sect. 6.

Throughout, let G and N be finite groups, written multiplicatively unless otherwise specified. Denote the group of permutations of the elements of a group A by $\mathrm{Sym}(A)$. Denote the subgroup of normalised permutations (permutations which fix the identity element 1) by $\mathrm{Sym}_1(A)$, and its subgroup of automorphisms by $\mathrm{Aut}(A)$. Denote the identity automorphism by id and the inverse under composition of a set injection $\iota : A \rightarrowtail B$ by $\mathrm{inv}(\iota)$ (whether or not ι is a bijection onto B). We denote by $C^1(G, N) = \{f : G \to N, f(1) = 1\}$ the group of all normalised functions from G to N, under the operation of pointwise multiplication. The pointwise inverse of f is denoted f^{-1}. The set of homomorphisms $\mathrm{Hom}(G, N)$ is a subgroup of $C^1(G, N)$, and $\mathrm{Hom}(G, \zeta(N))$, where $\zeta(N)$ is the centre of N, is a normal subgroup. Note $N = \zeta(N)$ if and only if N is abelian. Denote the trivial homomorphism by $\mathbf{1}$.

2 Equivalence classes of normalised functions

This section summarises background material and notation. New material in it is the definition of the three conditions **WeakC1**(α), **C1**(α) and **C2**(α); and the proof of some additional equivalences for [11, Theorem 4] (see Theorem 1).

Any un-normalised f has a *normalisation* $f \cdot 1 \in C^1(G,N)$ given by $f \cdot 1(x) = f(1)^{-1}f(x)$. If f is normalised, then $f \cdot 1 = f$. For each $r \in G$, the *shift* $f \cdot r$ of f by r is

$$(f \cdot r)(x) = f(r)^{-1}f(rx), \quad x \in G. \tag{7}$$

For any $r, s \in G$, $(f \cdot r) \cdot s = f \cdot (rs)$. Consequently, a right group action, the *shift action* of G on $C^1(G,N)$, is defined by the mapping $(f,r) \mapsto f \cdot r$. Furthermore, $f \in \mathrm{Hom}(G,N)$ if and only if $f \cdot r = f$ for all $r \in G$.

The *graph of* f is the set $S_f = \{(f(x),x),\ x \in G\} \subset N \times G$. It is *normalised* if f is normalised.

Two functions $f, f' \in C^1(G,N)$ are *graph equivalent* (written $f \sim_{\mathbf{g}} f'$) if their graphs S_f and $S_{f'}$ are equivalent, that is, if there exist $\alpha \in \mathrm{Aut}(N \times G)$ and $e \in N \times G$ such that $\alpha(S_f) = eS_{f'}$. They are graph *isomorphic* (written $f \simeq_{\mathbf{g}} f'$) if $\alpha(S_f) = S_{f'}$, i.e. $e = (1,1)$. The set of all normalised functions in the graph equivalence class of f is denoted $\mathbf{g}(f)$. We call it the *graph bundle* of f:

$$\mathbf{g}(f) = \bigl\{f' \in C^1(G,N) : \exists\, e \in N \times G, \alpha \in \mathrm{Aut}(N \times G) : \alpha(S_f) = eS_{f'}\bigr\}. \tag{8}$$

Multiplying each function in $\mathbf{g}(f)$ by any constant from N gives the *affine graph bundle* $\widehat{\mathbf{g}}(f)$ of f.

Two functions $f, f' \in C^1(G,N)$ are *bundle equivalent* (written $f \sim_{\mathbf{b}} f'$) if there exist $r \in G$, $\theta \in \mathrm{Aut}(G)$, $\gamma \in \mathrm{Aut}(N)$ and $\chi \in \mathrm{Hom}(G, \zeta(N))$ such that

$$f' = \bigl(\gamma \circ (f \cdot r) \circ \theta\bigr)\chi. \tag{9}$$

They are bundle *isomorphic* (written $f \simeq_{\mathbf{b}} f'$) if $r = 1$ in (9). The set of all normalised functions equivalent to f is denoted $\mathbf{b}(f)$ and called the *bundle* of f:

$$\mathbf{b}(f) = \bigl\{\bigl(\gamma \circ (f \cdot r) \circ \theta\bigr)\chi : r \in G, \gamma \in \mathrm{Aut}(N), \theta \in \mathrm{Aut}(G), \chi \in \mathrm{Hom}\bigl(G, \zeta(N)\bigr)\bigr\}. \tag{10}$$

Multiplying each function in $\mathbf{b}(f)$ by any constant from N gives the *affine bundle* $\widehat{\mathbf{b}}(f)$ of f.

It is sufficient [11, see (8) and (10)] to restrict consideration to normalised functions and, without loss of generality, **we assume from now on that every function $f : G \to N$ is normalised**.

2.1 The equivalences in terms of group actions

In this subsection, we relate graph and bundle equivalence within a common framework of group actions.

If $\alpha \in \mathrm{Aut}(N \times G)$, it has a factorisation $\alpha = \iota \times \eta$, where its action on the first component $N \times \{1\}$ determines a monomorphism $\iota = (\iota_1, \iota_2) : N \rightarrowtail N \times G$ and its action on the second component $\{1\} \times G$ determines a monomorphism $\eta = (\eta_1, \eta_2) : G \rightarrowtail N \times G$ which commutes with (ι_1, ι_2), with

$$\alpha(a,x) = (\iota \times \eta)(a,x) = \bigl(\iota_1(a)\eta_1(x), \iota_2(a)\eta_2(x)\bigr). \tag{11}$$

Set $\alpha_1(a,x) = \iota_1(a)\eta_1(x) = \eta_1(x)\iota_1(a)$, $\alpha_2(a,x) = \iota_2(a)\eta_2(x) = \eta_2(x)\iota_2(a)$ in (11) to give a second factorisation $\alpha = (\alpha_1, \alpha_2)$ of α into homomorphisms $\alpha_1 : N \times G \to N$ and $\alpha_2 : N \times G \to G$, with

$$\alpha(a,x) = (\alpha_1, \alpha_2)(a,x) = \bigl(\alpha_1(a,x), \alpha_2(a,x)\bigr). \tag{12}$$

If $\alpha(S_{f'}) = eS_f$ then, since the graphs are normalised, there exists $r \in G$ such that $e = (f(r)^{-1}, r^{-1})$ and $eS_f = S_{f\cdot r}$, so $e = (1,1)$ if and only if $r = 1$. Replacing α by its inverse we have: $f' \in \mathbf{g}(f)$ if and only if there exist $r \in G$ and $\alpha \in \mathrm{Aut}(N \times G)$ such that $\alpha(S_{f\cdot r}) = S_{f'}$ if and only if there exist $r \in G$ and $\alpha = \iota \times \eta \in \mathrm{Aut}(N \times G)$ such that

$$\rho := \bigl(\iota_2 \circ (f \cdot r)\bigr)\eta_2 \in \mathrm{Sym}_1(G), \tag{13}$$

$$f' = \bigl(\iota_1 \circ (f \cdot r) \circ \mathrm{inv}(\rho)\bigr)\bigl(\eta_1 \circ \mathrm{inv}(\rho)\bigr), \tag{14}$$

both hold. **Note the formal similarity between (14) and (9).** If it happens that $\rho \in \mathrm{Aut}(G)$ and $\iota_1 \in \mathrm{Aut}(N)$ then (14) is an example of (9) and $f' \sim_{\mathbf{b}} f$. It is tempting to hope that these sufficient conditions are necessary, but this is not so. Although we will show the first condition ($\rho \in \mathrm{Aut}(G)$) is indeed necessary, a more subtle conversion, which takes some effort to establish, is required (see Corollary 4).

Defining

$$A_f := \bigl\{\iota \times \eta \in \mathrm{Aut}(N \times G) : \rho = (\iota_2 \circ f)\ \eta_2 \in \mathrm{Sym}_1(G)\bigr\}, \tag{15}$$

$$f^{\iota\times\eta} := \bigl(\iota_1 \circ f \circ \mathrm{inv}(\rho)\bigr)\bigl(\eta_1 \circ \mathrm{inv}(\rho)\bigr), \quad \text{for } \iota \times \eta \in A_f, \tag{16}$$

we have

$$\mathbf{g}(f) = \bigl\{(f \cdot r)^\alpha : r \in G, \alpha \in A_f\bigr\}. \tag{17}$$

Formula (17) has two components, the shift action and an action by automorphisms in A_f. Since $f \cdot r \in \mathbf{b}(f)$ by (10), and $(f \cdot r)^\alpha = (f^\alpha) \cdot \rho(r)$ by [11, Lemma 15], where ρ is the permutation defined in (13) from α, shift action is wholly confined to bundles. Hence when considering how graph bundles partition into bundles we may ignore any translation action on graphs. **From now on, we restrict to $e = (1,1)$ in (8) and $r = 1$ in (10) and focus on graph isomorphisms $f \simeq_{\mathbf{g}} f'$ and bundle isomorphisms $f \simeq_{\mathbf{b}} f'$.**

In [11], the author investigates the problem of identifying all the automorphisms α in A_f for which $f^\alpha \in \mathbf{b}(f)$, in terms of three subsets E_f, B_f^+ and[3] B^- of A_f:

$$E_f := \bigl\{\alpha \in A_f : f^\alpha \in \mathbf{b}(f)\bigr\}, \tag{18}$$

$$B_f^+ := \bigl\{\alpha = \iota \times \eta \in \mathrm{Aut}(N \times G) : (\iota_2 \circ f)\eta_2 \in \mathrm{Aut}(G)\bigr\}, \tag{19}$$

$$B^- := \bigl\{\alpha = \iota \times \eta \in \mathrm{Aut}(N \times G) : \iota_2 = \mathbf{1}, \eta_2 \in \mathrm{Aut}(G)\bigr\}. \tag{20}$$

[3] In [11, Definition 10], the condition $\eta_2 \in \mathrm{Aut}(G)$ for B^- is implied but not explicitly stated.

These sets vary according to the invariants and characteristics of the function f. Plainly, $B^- \subseteq B_f^+$, for any f. If $\alpha = \iota \times \eta \in B^-$ then $\iota_1 \in \mathrm{Aut}(N)$ since ι is a monomorphism. On setting $\gamma = \iota_1$, $\theta = \mathrm{inv}(\eta_2)$ and $\chi = \eta_1 \circ \mathrm{inv}(\eta_2)$ in (9), for any f we have $f^\alpha \in \mathbf{b}(f)$, so $\alpha \in E_f$. We have

$$B^- \subseteq B_f^+ \subseteq A_f, \tag{21}$$

$$B^- \subseteq E_f \subseteq A_f, \tag{22}$$

and, in general, these four sets are different. For example, when $G = N$ is abelian, the trivial homomorphism $\mathbf{1} : G \to N$ has $B^- \neq B_{\mathbf{1}}^+$ [11, Example 19]. When $G = N = \mathbb{Z}_p^n$, $B^- \subseteq B_f^+ \subseteq E_f \subseteq A_f$ for any f, by [11, Theorem 21]. In this case, if $p = 2$ and n is odd, consider the permutation $f(x) = x^3$ (with multiplication defined in $\mathrm{GF}(2^n)$). It is in the graph bundle $\mathbf{g}(\mathrm{inv}(f))$ of its inverse $\mathrm{inv}(f)$ but not in the bundle $\mathbf{b}(\mathrm{inv}(f))$ of its inverse, so $E_{\mathrm{inv}(f)} \neq A_{\mathrm{inv}(f)}$ and $B^+_{\mathrm{inv}(f)} \neq A_{\mathrm{inv}(f)}$. By [3, Example 1], $B^- \neq E_{\mathrm{inv}(f)}$ and when $n = 3$ direct checking of this example shows $B^+_{\mathrm{inv}(f)} \neq E_{\mathrm{inv}(f)}$.

Given f, it is easy to characterise the $\alpha \in A_f$ for which $\alpha \in B_f^+$. We use the *coboundary* function $\partial f : G \times G \to N$ defined as

$$\partial f(x, y) = f(x) f(y) f(xy)^{-1}, \quad x, y \in G, \tag{23}$$

which measures how much f differs from a homomorphism.

Lemma 1 [11, Lemma 22] *Let* $\alpha = \iota \times \eta \in A_f$. *Then* $\alpha \in B_f^+$ *if and only if* $\mathrm{im}(\partial f) \subseteq \ker(\iota_2)$.

3 The common framework: transversals, graphs and RDSs

3.1 Transversals and graphs

In this subsection, transversals are used to compare graph and bundle isomorphism.

An *extension* of N by G is a short exact sequence of groups $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$, that is, ι is a monomorphism and π an epimorphism with $\ker\pi = \mathrm{im}\iota$, so $\iota(N)$ is normal in E and $E/\iota(N) \cong G$. Necessarily, $|E| = |N||G|$. Each *section* $t : G \to E$ of π (that is, a mapping $x \mapsto t_x$ such that $\pi(t_x) = x,\ x \in G$) determines a *transversal* $T = \{t_x,\ x \in G\}$ with $\pi(t_x) = x$, in E, and vice versa. Every element of E has a unique factorisation as $\iota(a)t_x$ for some $a \in N$ and $x \in G$, so T is a set of coset representatives[4] of the normal subgroup $\iota(N)$. A transversal T is *normalised* if it intersects $\iota(N)$ in 1, or equivalently, if $t_1 = 1$.

[4] Sometimes, for brevity, any set of coset representatives of $\iota(N)$ is called a transversal of $\iota(N)$. In this case, π is understood to be a composition of the canonical quotient map $E \twoheadrightarrow E/\iota(N)$ with some isomorphism $E/\iota(N) \overset{\cong}{\rightarrowtail} G$. We assume that π is known, and work with $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$.

Here we consider only the case $E = N \times G$, that is, we have a split extension

$$N \overset{\iota}{\rightarrowtail} N \times G \overset{\pi}{\twoheadrightarrow} G. \tag{24}$$

For each normalised transversal of π in (24), there exist an $f \in C^1(G, N)$ and a pair of functions of the form $(\partial f, \overline{f})$, which is a *factor pair* for a split extension equivalent to (24). The function ∂f is as in (23) and $\overline{f} : G \to \mathrm{Aut}(N)$ is the G-action induced by f on N by inner automorphisms:

$$\overline{f}(x)(a) = a^{f(x)} = f(x)af(x)^{-1}, \quad a \in N, x \in G. \tag{25}$$

Thus if N is abelian, the action induced by f is trivial. For details see a textbook such as [16], or [10, Sect. 7.1].

The graph S_f of $f : G \to N$ carries various structures. For instance, because $N \times \{1\}$ is a subgroup of $N \times G$, S_f is a complete set of coset representatives of $N \times \{1\}$ in $N \times G$. More importantly for us, because $N \times G$ is a split extension of N by G, the graph S_f has the overlying structure of a transversal (usually in many different ways).

The *standard* split extension of N by G

$$N \overset{\iota}{\rightarrowtail} N \times G \overset{\kappa}{\twoheadrightarrow} G, \tag{26}$$

has $\iota(a) = (a, 1)$ and $\kappa(a, x) = x$. For each f the section $t : G \to N \times G$ with $t(x) = t_x = (f(x), x)$ defines the *canonical transversal* T_f in (26),

$$T_f = \bigl\{t_x = (f(x), x),\ x \in G\bigr\}, \tag{27}$$

with $\kappa(t_x) = x$. T_f is a set of coset representatives of $\iota(N) = N \times \{1\}$, has S_f as underlying set, and defines the factor pair $(\partial f, \overline{f})$.

Note that the factor pair $(\partial f, \overline{f})$ determines not the split extension (26), but instead the equivalent split extension $N \overset{\iota}{\rightarrowtail} E_f \overset{\kappa}{\twoheadrightarrow} G$, where the group E_f is the set $N \times G$ with multiplication defined by $(a, x)(b, y) = (ab^{f(x)}\partial f(x, y),\ xy)$.

However, transversals other than T_f can define the same factor pair $(\partial f, \overline{f})$, and S_f can also carry a different transversal structure with respect to some other split extension $N \overset{\iota}{\rightarrowtail} N \times G \overset{\pi}{\twoheadrightarrow} G$. These alternatives are important, as we see in the work following.

Two transversals T, T', respectively, in split extensions $N \overset{\iota}{\rightarrowtail} N \times G \overset{\pi}{\twoheadrightarrow} G$, $N \overset{\iota'}{\rightarrowtail} N \times G \overset{\pi'}{\twoheadrightarrow} G$, respectively, are *isomorphic* (written $T \simeq T'$) if there exists $\alpha \in \mathrm{Aut}(N \times G)$ satisfying both the conditions

(i) $\alpha(T) = T'$, that is, α is a set bijection between sets T and T', and
(ii) $\alpha(\iota(N)) = \iota'(N)$, that is, α is an isomorphism between subgroups $\iota(N)$ and $\iota'(N)$.

Thus, an isomorphism of canonical transversals T_f and $T_{f'}$ requires two conditions, while an isomorphism of their underlying graphs S_f and $S_{f'}$ requires only one. However, the conditions are directly comparable.

Definition 2 Let $f, f' \in C^1(G,N)$ and $\alpha \in \mathrm{Aut}(N \times G)$. Define three conditions on α with respect to f, f':

1. $\mathbf{WeakC1}(\alpha)$: $\alpha(S_f) = S_{f'}$;
2. $\mathbf{C1}(\alpha)$: $\alpha(T_f) = T_{f'}$;
3. $\mathbf{C2}(\alpha)$: $\alpha(N \times \{1\}) = N \times \{1\}$.

By definition, $f \simeq_{\mathbf{g}} f'$ if and only if there exists $\alpha \in \mathrm{Aut}(N \times G)$ such that $\mathbf{WeakC1}(\alpha)$ holds. Obviously, if $\alpha(T_f) = T_{f'}$ then $\alpha(S_f) = S_{f'}$. Thus for any such α,

$$\mathbf{C1}(\alpha) \Rightarrow \mathbf{WeakC1}(\alpha) .$$

Transversal isomorphism is important because bundle isomorphism $f \simeq_{\mathbf{b}} f'$ is known to correspond to isomorphism of **any** pair of transversals T, T' in split extensions $N \overset{\iota}{\rightarrowtail} N \times G \overset{\pi}{\twoheadrightarrow} G$, $N \overset{\iota'}{\rightarrowtail} N \times G \overset{\pi'}{\twoheadrightarrow} G$, respectively, which define the pairs $(\partial f, \overline{f})$, $(\partial f', \overline{f'})$, respectively. The following result describes this correspondence, including two equivalences additional to those given in [11], which we need in subsequent proofs.

Theorem 1 *Let $f, f' \in C^1(G,N)$ and let T, T' be normalised transversals in the split extensions $N \overset{\iota}{\rightarrowtail} N \times G \overset{\pi}{\twoheadrightarrow} G$, $N \overset{\iota'}{\rightarrowtail} N \times G \overset{\pi'}{\twoheadrightarrow} G$, such that T, T' determine $(\partial f, \overline{f})$, $(\partial f', \overline{f'})$, respectively. Set $T = \{t_x, x \in G\}$, where $\pi(t_x) = x$ and, with the same order of elements in G, set $T' = \{t'_x, x \in G\}$, where $\pi'(t'_x) = x$.*

The following are equivalent to the statement $f \simeq_{\mathbf{b}} f'$.

1. *There exist $\gamma \in \mathrm{Aut}(N), \theta \in \mathrm{Aut}(G)$ and $\chi \in \mathrm{Hom}(G, \zeta(N))$ such that*
$$f = (\gamma \circ f' \circ \theta)\chi;$$
2. *There exists $\alpha \in \mathrm{Aut}(N \times G)$ such that $\alpha(T) = T'$ and $\alpha(\iota(N)) = \iota'(N)$;*
3. *There exist $\alpha \in \mathrm{Aut}(N \times G)$, $\delta \in \mathrm{Aut}(N)$ and $\theta \in \mathrm{Aut}(G)$ such that $\alpha(t_x) = t'_{\theta(x)}$, $x \in G$, and the diagram below commutes (corresponding transversals are listed on the right of each extension):*

$$\begin{tikzcd} N \arrow[r, "\iota"] \arrow[d, "\delta"'] & N \times G \arrow[r, "\pi"] \arrow[d, "\alpha"'] & G \arrow[d, "\theta"'] & T \\ N \arrow[r, "\iota'"] & N \times G \arrow[r, "\pi'"] & G & T' \end{tikzcd} \tag{28}$$

4. *There exist $\delta \in \mathrm{Aut}(N)$ and $\theta \in \mathrm{Aut}(G)$ such that the function*
$$\alpha\big(\iota(a)t_x\big) = \iota'\big(\delta(a)\big)t'_{\theta(x)}, \quad a \in N, x \in G \tag{29}$$
is an automorphism of $N \times G$.

Proof By (9), Part 1 is equivalent to $f \simeq_{\mathbf{b}} f'$. The equivalence Part 1 $\Leftrightarrow$ Part 2 appears in [11, Definition 3, Theorem 4] with $s = 1$ and $\delta = \mathrm{inv}(\gamma)$.

Part 2 $\Leftrightarrow$ Part 3. If Part 2 holds, the diagram (28) commutes, with $\delta = \mathrm{inv}(\iota') \circ \alpha \circ \iota \in \mathrm{Aut}(N)$ and some $\theta \in \mathrm{Aut}(G)$ satisfying $\theta \circ \pi = \pi' \circ \alpha$. By assumption $\alpha(T) = T'$, so there exists $\sigma \in \mathrm{Sym}_1(G)$ such that $\alpha(t_x) = t'_{\sigma(x)}$, $x \in G$. Thus $\pi'(\alpha(t_x)) = \pi'(t'_{\sigma(x)}) = \sigma(x) = \theta(\pi(t_x)) = \theta(x)$ and $\sigma = \theta \in \mathrm{Aut}(G)$. That is, $\alpha(t_x) = t'_{\theta(x)}$. The converse is immediate since $\alpha \circ \iota = \iota' \circ \delta$.

Part 3 $\Leftrightarrow$ Part 4. In the upper extension of (28), each element of $N \times G$ can be uniquely represented as $\iota(a)t_x$. If Part 3 holds then by definition $\alpha(\iota(a)t_x) = \alpha(\iota(a))\alpha(t_x) = \iota'(\delta(a))t'_{\theta(x)}$. If Part 4 holds then $\alpha \circ \iota = \iota' \circ \delta$, $\alpha(t_x) = t'_{\theta(x)}$ and $\theta \circ \pi(\iota(a)t_x) = \theta(t_x) = \theta(x) = \pi'(\iota'(\delta(a))t'_{\theta(x)})$, so (28) commutes. □

When Theorem 1 is applied to canonical transversals $T_f = T$ and $T_{f'} = T'$, we obtain a simple characterisation of bundle isomorphism in terms of automorphism action.

Corollary 1 [11, Lemma 18]

$$\begin{aligned} f \simeq_{\mathbf{b}} f' &\Leftrightarrow \exists \alpha \in \mathrm{Aut}(N \times G) : \mathbf{C1}(\alpha) \textit{ and } \mathbf{C2}(\alpha) \textit{ both hold} \\ &\Leftrightarrow \exists \alpha \in B^- : f' = f^\alpha. \end{aligned}$$

For each f, let $F_f \subseteq \mathrm{Aut}(G \times N)$ be the stabiliser of its graph S_f. By definition

$$F_f = \{\alpha \in \mathrm{Aut}(G \times N) : \alpha(S_f) = S_f\} = \{\alpha \in A_f : f^\alpha = f\} \subseteq E_f. \tag{30}$$

If $\alpha \in E_f$ and $f' = f^\alpha$ then $f' \in \mathbf{b}(f)$. By Corollary 1, there exists $\beta \in B^-$ such that $f' = f^\beta$, so $(f^\alpha)^{\mathrm{inv}(\beta)} = f$. Since $\alpha = (\alpha \circ \mathrm{inv}(\beta)) \circ \beta = \beta \circ (\mathrm{inv}(\beta) \circ \alpha)$, it follows that

$$E_f = F_{f'} \circ B^- = B^- \circ F_f. \tag{31}$$

We introduce a new equivalence relation, *canonical* equivalence, defined by $\mathbf{C1}(\alpha)$.

Definition 3 Two functions $f, f' \in C^1(G, N)$ are *canonically equivalent* (written $f \sim_{\mathbf{c}} f'$) if there exist $\alpha \in \mathrm{Aut}(N \times G)$ and $e \in N \times G$ such that $\alpha(T_f) = eT_{f'}$. They are *canonically isomorphic* (written $f \simeq_{\mathbf{c}} f'$) if there exists $\alpha \in \mathrm{Aut}(N \times G)$ such that $\alpha(T_f) = T_{f'}$, i.e. $e = (1, 1)$. The set of all functions in the canonical equivalence class of f is denoted $\mathbf{c}(f)$. We call it the *canonical bundle* of f.

Equivalently, by Theorem 3 (proved in Sect. 4 below), we have:

$f \simeq_{\mathbf{c}} f' \Leftrightarrow \exists\, \alpha \in B^+_f : f' = f^\alpha \Leftrightarrow \exists\, \alpha \in \mathrm{Aut}(N \times G) :$ $\mathbf{C1}(\alpha)$ *holds.*

Set

$$C_f = \{\alpha \in A_f : f^\alpha \in \mathbf{c}(f)\}. \tag{32}$$

We can mimic the argument giving (31) (with C_f replacing E_f, $\mathbf{c}(f)$ replacing $\mathbf{b}(f)$ and Theorem 3 in Sect. 4 replacing Corollary 1) to show that, for any $f' = f^\alpha$, $\alpha \in C_f$

$$C_f = F_{f'} \circ B^+_f = B^+_f \circ F_f. \tag{33}$$

As $E_f = B^- \circ F_f \subseteq B_f^+ \circ F_f = C_f$ we have

$$E_f \subseteq C_f, \quad \text{so} \quad \alpha \notin C_f \Rightarrow \alpha \notin E_f. \tag{34}$$

Lemma 2 $\mathbf{c}(f) = \mathbf{b}(f) \Leftrightarrow C_f = E_f \Leftrightarrow B_f^+ = B^- \circ (B_f^+ \cap F_f)$.

Proof Straightforward from the definitions, (31) and (33). □

Since F_f is a group under composition, A_f, C_f and E_f are all disjoint unions of cosets of F_f. We derive the following simple condition for testing non-membership of C_f, and thus of E_f. Whether or not this is a practical condition in application depends on how difficult it is to determine F_f.

Corollary 2 *Let $\alpha \in A_f$. If $\alpha \bmod F_f \notin B_f^+$ then $\alpha \notin C_f$ and $\alpha \notin E_f$. Furthermore, $B_f^+ \cap F_f$ is a subgroup of F_f, so that $|C_f| = |B_f^+|[F_f : B_f^+ \cap F_f]$.*

3.2 RDSs, transversals and graphs

In this subsection we apply Galati's work in [9] to relate RDSs, transversals and graphs.

A *relative* (v, w, k, λ)*-difference set* ((v, w, k, λ)-RDS) (Elliot and Butson [8]) in a finite group E of order vw relative to a normal subgroup K of order w, is a k-element subset R of E such that the multiset of quotients $r_1 r_2^{-1}$ of distinct elements r_1, r_2 of R contains each element of $E \backslash K$ exactly λ times, and contains no elements of K. Necessarily, $k(k-1) = \lambda w(v-1)$. If $k = v$ and $v = w\lambda$, the RDS is called *semiregular*; otherwise it is *regular*. The RDS is *splitting* if E is isomorphic to a semidirect product of K by E/K, and *normalised* if $R \cap K = 1$.

Here we work with the simplest case, that of splitting RDSs relative to $N \times \{1\}$ in the direct product $E = N \times G$, where $|N| = w$ and $|G| = v$. If R is a normalised RDS relative to $N \times \{1\}$ and $|R| = k$, then distinct elements of R belong to distinct cosets of $N \times \{1\}$ and take distinct values on their second component, so R has the form $\{(a_x,\ x),\ x \in D\}$ for some k-subset D of G. Because κ in (26) is an epimorphism, D is an ordinary $(v, k, w\lambda)$ difference set in G, and, following Galati [9] we say R *lifts* D.

Thus, for **each** of the w^{v-k} functions f satisfying $f(x) = a_x,\ x \in D$, the RDS $R = \{(f(x), x),\ x \in D\}$ is a k-element subset of the graph S_f, and therefore of the canonical transversal T_f.

Lemma 3 *Let G have order v, N have order w, let $f \in C^1(G, N)$ and let D be a k-element subset of G. The following are equivalent*:

1. *$R = \{(f(x), x),\ x \in D\}$ is a normalised (v, w, k, λ)-RDS in $N \times G$ relative to $N \times \{1\}$, lifting D.*
2. *For each $x \neq 1 \in G$, the sequence $\{\partial f(x, y),\ y \in D \cap x^{-1} D\}$ lists each element of N exactly λ times.*

Proof (Compare with [9, p. 287], noting that Galati's equation (19) should not include the term $\varepsilon(x)$.) By (7) and (8) in [9], we have $(\partial f, \overline{f}) \sim_f (1,1)$, so $(1,1) \sim_{f^{-1}} (\partial f, \overline{f})$. By [9, Proposition 3.5, Corollary 5.1], Part 1 holds $\Leftrightarrow$ $R_{(\partial f, \overline{f})} = \{(1,x), x \in D\}$ is a (v,w,k,λ)-RDS in $E_{(\partial f, \overline{f})} \cong N \times G$, relative to $N \times \{1\}$, lifting D. By [9, Definition 4.1, Theorem 5.1], this holds if and only if Part 2 holds. □

Two such normalised (v,w,k,λ)-RDSs R and R' are equivalent (written $R \sim R'$) if there exists $\alpha \in \mathrm{Aut}(N \times G)$ and $e \in N \times G$ such that $\alpha(R) = eR'$ and $\mathbf{C2}(\alpha)$ holds, and isomorphic (written $R \simeq R'$) if $e = (1,1)$.

Corollary 3 *Suppose R and R' are (v,w,k,λ)-RDSs in $N \times G$ relative to $N \times \{1\}$, and let $R \subseteq T_f$ for some $f \in C^1(G,N)$. Then*

$$R \simeq R' \Leftrightarrow \exists \alpha \in B^-, f' \in \mathbf{b}(f) : \alpha(R) = R' \subseteq T_{f'}.$$

Proof If $R \simeq R'$, suppose $\alpha \in \mathrm{Aut}(N \times G)$ such that $\alpha(R) = R'$ and $\mathbf{C2}(\alpha)$ holds. Then $\alpha(T_f)$ is a normalised set of coset representatives of $N \times \{1\}$ containing $\alpha(R) = R'$, so has the form $T_{f'}$ for some f'. Therefore, $\alpha(T_f) = T_{f'}$, so $\mathbf{C1}(\alpha)$ holds and by Corollary 1, $f \simeq_{\mathbf{b}} f'$. By definition, $\alpha \in B^-$. Conversely, any such α has $\iota_2 = \mathbf{1}$ and thus $\alpha(N \times \{1\}) = N \times \{1\}$. □

If the graph S_f of f does contain an RDS relative to $N \times \{1\}$, it is straightforward to show that $B_f^+ = B^-$, and thus that $\mathbf{c}(f) = \mathbf{b}(f)$.

Theorem 2 *Suppose $f \in C^1(G,N)$ and S_f contains a normalised (v,w,k,λ)-RDS relative to $N \times \{1\}$. Then*

1. $\mathrm{im}(\partial f) = N$;
2. *S_f generates $N \times G$;*
3. *If $\alpha \in B_f^+$ then $\alpha \in B^-$, that is, $\mathbf{b}(f^\alpha) = \mathbf{b}(f) = \mathbf{c}(f)$.*

Proof Part 1 follows from Lemma 3. If S_f lifts D, for each $x \neq 1 \in G$ the sequence $\{(\partial f(x,y),1), y \in D \cap x^{-1}D\}$ lists each element of $N \times \{1\}$ exactly λ times, and $(\partial f(x,y),1) = (f(x),x)(f(y),y)(f(xy),xy)^{-1}$ is generated by S_f. Thus for each $a \in N$ and each $b \neq 1 \in G$, there exist λ values y such that $f(b)^{-1}a = \partial f(x,y)$ and $(a,b) = (f(b)\partial f(x,y), b)$ is generated by S_f, giving Part 2. By Part 1 and Lemma 1, $\ker(\iota_2) = N$, so $\iota_2 = \mathbf{1}$, giving the first part of Part 3. The second part follows by (31) and (33). □

4 When graph isomorphism determines bundle isomorphism

By Corollary 1, $f \simeq_{\mathbf{b}} f'$ if and only if there exists $\alpha \in \mathrm{Aut}(N \times G)$ such that $\mathbf{C1}(\alpha)$ and $\mathbf{C2}(\alpha)$ both hold, in which case $\mathbf{WeakC1}(\alpha)$ also holds.

For which α is the converse "$\mathbf{WeakC1}(\alpha) \Rightarrow \mathbf{C1}(\alpha)$ and $\mathbf{C2}(\alpha)$" true? In this section, we use transversals and group extensions to solve this question. Specifically, we identify the conditions on α under which the formula for f^α in terms of f defined in (14) (with $r = 1$) can be rewritten as the formula for f^α in terms of f defined in (9) (with $r = 1$).

We observe that if $\alpha(S_f) = S_{f'}$, then $\alpha(T_f) = S_{f'}$, and $\alpha(T_f)$ is a transversal in the split extension $N \overset{\alpha\circ\iota}{\rightarrowtail} N \times G \overset{\kappa\circ\mathrm{inv}(\alpha)}{\twoheadrightarrow} G$. Clearly, $\alpha(T_f) = S_{f'}$ does not always imply $\alpha(T_f) = T_{f'}$. The next result shows exactly when $\mathbf{WeakC1}(\alpha) \Rightarrow \mathbf{C1}(\alpha)$ for the canonical transversals T_f and $T_{f'}$.

Theorem 3 *Suppose* $f \simeq_{\mathbf{g}} f'$, $\alpha \in \mathrm{Aut}(N \times G)$ *and* $\alpha(T_f) = S_{f'}$, *so the transversal* $\alpha(T_f) = \{t^*_x,\ x \in G\}$ *of* $\alpha(\iota(N))$ *in* $N \overset{\alpha\circ\iota}{\rightarrowtail} N \times G \overset{\kappa\circ\mathrm{inv}(\alpha)}{\twoheadrightarrow} G$ *has the form*

$$t^*_x = \alpha(t_x) = \bigl(f'\bigl(\rho(x)\bigr), \rho(x)\bigr), \quad t_x \in T_f, \tag{35}$$

with $\rho \in \mathrm{Sym}_1(G)$ *as in* (13). *Then* $\alpha(T_f) = T_{f'}$ *if and only if* $\rho \in \mathrm{Aut}(G)$.

That is, if $\mathbf{WeakC1}(\alpha)$ *holds,* $\mathbf{C1}(\alpha)$ *holds if and only if* $\alpha \in B^+_f$.

Proof Set $t'_x = (f'(x), x) \in T_{f'}$ for $x \in G$ (i.e. with the same ordering of G as for T_f) and let $\tau \in \mathrm{Sym}_1(G)$. Thus $t'_{\tau(x)} = (f'(\tau(x)), \tau(x))$ and $t'_{\tau(x)} = t^*_{\sigma(x)}$, where $\sigma = \mathrm{inv}(\rho) \circ \tau \in \mathrm{Sym}_1(G)$.

Then $t'_\tau : x \mapsto t^*_{\sigma(x)}$ is a section of π' in an extension $N \overset{\iota'}{\rightarrowtail} E \overset{\pi'}{\twoheadrightarrow} G$ in which $\iota'(N) = \alpha \circ \iota(N)$ if and only if $\sigma \in \mathrm{Aut}(G)$ and $\pi' = \mathrm{inv}(\sigma) \circ \kappa \circ \mathrm{inv}(\alpha)$. So, without loss of generality, we may take $\iota' = \alpha \circ \iota$.

Similarly, $t'_\tau : x \mapsto t'_{\tau(x)}$ is a section of π' in an extension $N \overset{\iota'}{\rightarrowtail} E \overset{\pi'}{\twoheadrightarrow} G$ in which $\iota'(N) = \iota(N) = N \times \{1\}$ if and only if $\tau \in \mathrm{Aut}(G)$ and $\pi' = \mathrm{inv}(\tau) \circ \kappa$. We may take $\iota' = \iota$.

Therefore, if there exists a permutation τ for which t'_τ is simultaneously a section of $\mathrm{inv}(\sigma) \circ \kappa \circ \mathrm{inv}(\alpha)$ and $\mathrm{inv}(\tau) \circ \kappa$ then $\rho \in \mathrm{Aut}(G)$. Conversely, if $\rho \in \mathrm{Aut}(G)$ we may take $\rho = \tau$ and $\sigma = \mathrm{id}$, and then t'_ρ is simultaneously a section of $\kappa \circ \mathrm{inv}(\alpha)$ and of $\mathrm{inv}(\rho) \circ \kappa$. □

In Theorem 3, we are interested *only* in the way α maps T_f onto $T_{f'}$, and not in where it maps $\iota(N)$. Any $\alpha' \in \mathrm{Aut}(N \times G)$ which coincides with α on T_f will determine the same automorphism ρ in (35) as α, and be indistinguishable from α in Theorem 3. We next find all such α' for which $\mathbf{C2}(\alpha')$ holds.

The identity mapping on $\alpha(T_f)$ always extends in many ways to a *permutation* of $N \times G$ which is an isomorphism from $\alpha(\iota(N))$ to $\iota(N)$. First, any $\delta \in \mathrm{Aut}(N)$ determines an isomorphism $\delta' = \iota \circ \delta \circ \mathrm{inv}(\alpha \circ \iota) : \alpha(\iota(N)) \to \iota(N)$. Conversely, any isomorphism $\delta' : \alpha(\iota(N)) \to \iota(N)$ determines $\delta = \mathrm{inv}(\iota) \circ \delta' \circ (\alpha \circ \iota) \in \mathrm{Aut}(N)$. Second, δ extends to the permutation $\hat{\delta} \in \mathrm{Sym}_1(N \times G)$ defined by

$$\hat{\delta} \circ \alpha\bigl(\iota(a)t_x\bigr) = \iota\bigl(\delta(a)\bigr)\alpha(t_x), \quad a \in N, x \in G. \tag{36}$$

Consideration of the proof of Theorem 3 when $\rho \in \mathrm{Aut}(G)$ shows that the following diagram commutes for any $\delta \in \mathrm{Aut}(N)$. The corresponding transversals are listed on the right of each extension, with $T^\rho_{f'}$ the transversal defined by $t'_\rho : x \mapsto$

$(f'(\rho(x)), \rho(x)) = \alpha(t_x)$.

$$\begin{tikzcd}
N \arrow[r, "\iota"] \arrow[d, "\mathrm{id}"'] & N \times G \arrow[r, "\kappa"] \arrow[d, "\alpha"'] & G \arrow[d, "\mathrm{id}"'] & T_f \\
N \arrow[r, "\alpha \circ \iota"] \arrow[d, "\delta"'] & N \times G \arrow[r, "\kappa \circ \mathrm{inv}(\alpha)"] \arrow[d, "\hat{\delta}"] & G \arrow[d, "\mathrm{id}"'] & \alpha(T_f) \\
N \arrow[r, "\iota"] \arrow[d, "\mathrm{id}"'] & N \times G \arrow[r, "\mathrm{inv}(\rho) \circ \kappa"] \arrow[d, "\mathrm{id}"'] & G \arrow[d, "\rho"'] & T_{f'}^{\rho} \\
N \arrow[r, "\iota"] & N \times G \arrow[r, "\kappa"] & G & T_{f'}
\end{tikzcd} \tag{37}$$

Diagram (37) simplifies to

$$\begin{tikzcd}
N \arrow[r, "\iota"] \arrow[d, "\delta"'] & N \times G \arrow[r, "\kappa"] \arrow[d, "\hat{\delta} \circ \alpha"'] & G \arrow[d, "\rho"'] & T_f \\
N \arrow[r, "\iota"] & N \times G \arrow[r, "\kappa"] & G & T_{f'}
\end{tikzcd} \tag{38}$$

By Theorem 1, any $\alpha' \in \mathrm{Aut}(N \times G)$ which is identical to α on T_f, and for which $\mathbf{C2}(\alpha')$ holds, will have the form $\alpha' = \hat{\delta} \circ \alpha$ for some $\delta \in \mathrm{Aut}(N)$ with $\hat{\delta}$ an automorphism which stabilises S_{f^α} pointwise. We want to find all δ for which the permutation $\hat{\delta}$ in (36) stabilising S_{f^α} pointwise, is an automorphism.

Definition 4 Denote the pointwise stabiliser of S_f by

$$\widehat{F}_f = \bigl\{\alpha \in \mathrm{Aut}(G \times N) : \alpha\bigl(\bigl(f(x), x\bigr)\bigr) = \bigl(f(x), x\bigr), x \in G\bigr\} \subseteq B_f^+ \cap F_f. \tag{39}$$

For $\alpha \in \mathrm{Aut}(N \times G)$ and $\delta \in \mathrm{Aut}(N)$, define the condition

$$\mathbf{C3}(\alpha, \delta) : \hat{\delta} \in \widehat{F}_{f^\alpha}.$$

$\mathbf{C3}(\alpha, \delta)$ holds if and only if diagram (38) is an instance of diagram (28) for T_f and $T_{f'}$. The next theorem identifies those δ for which $\mathbf{C3}(\alpha, \delta)$ holds.

To state it, we need a little more notation. Let ι be as in (26) and $\alpha \in \mathrm{Aut}(N \times G)$. Set $J = \alpha(\iota(N)) \cap \iota(N)$, $M = \mathrm{inv}(\alpha \circ \iota)(J) \le N$ and $M' = \mathrm{inv}(\iota)(J) \le N$, and let $\breve{\alpha} : M \to M'$ be the isomorphism induced by α, i.e.

$$\breve{\alpha}(a) = \mathrm{inv}(\iota) \circ \alpha \circ \iota(a), \quad a \in M. \tag{40}$$

Theorem 4 *Suppose $f \simeq_{\mathbf{c}} f'$, $\alpha \in \mathrm{Aut}(N \times G)$, $f' = f^\alpha$ and $\mathbf{C1}(\alpha)$ holds. Let $\breve{\alpha}$ be as in* (40)*. For each $\delta \in \mathrm{Aut}(N)$, define $\chi_\delta := (\delta \circ f)^{-1}(f' \circ \rho)$. The following are equivalent*:

1. $\mathbf{C3}(\alpha,\delta)$ *holds*;
2. $\delta=\breve{\alpha}$ *on* $\mathrm{im}\partial f$ *and* $\chi_\delta\in\mathrm{Hom}(G,\zeta(N))$;
3. $\hat{\delta}\circ\alpha\in B^-$.

Proof Calculation using (23) shows $\mathrm{im}\partial f\subseteq M$ and $\breve{\alpha}(\partial f)=\partial(f'\circ\rho)$. Calculation using (36) shows $\hat{\delta}\circ\alpha((a,x))=(\delta(a)\chi_\delta(x),\ \rho(x))$.

Part 2 ⇔ Part 1. Direct computation shows that the two conditions imply $\hat{\delta}$ is an automorphism. Conversely, if $\hat{\delta}$ is an automorphism, $\partial(f'\circ\rho)=\partial(\delta\circ f)=\delta(\partial f)=\breve{\alpha}(\partial f)$, so $\delta=\breve{\alpha}$ on $\mathrm{im}\partial f$. Then $\partial((\delta\circ f)^{-1}(f'\circ\rho))=\mathbf{1}$, so $\chi_\delta=(\delta\circ f)^{-1}(f'\circ\rho)\in\mathrm{Hom}(G,N)$. Application of Theorem 1 to the middle diagram in (37) shows χ_δ must actually be in $\mathrm{Hom}(G,\zeta(N))$.

Part 3 ⇔ Part 1. If $\hat{\delta}\circ\alpha\in B^-$ it is an automorphism so $\mathbf{C3}(\alpha,\delta)$ holds. Conversely, if $\mathbf{C3}(\alpha,\delta)$ holds, $\hat{\delta}\circ\alpha$ is an automorphism. With $\hat{\delta}\circ\alpha=\iota'\times\eta'$ in (11) we derive $\iota'_1=\delta$, $\eta'_1=\chi_\delta$, $\iota'_2=\mathbf{1}$ and $\eta'_2=\rho\in\mathrm{Aut}(G)$. Thus $\hat{\delta}\circ\alpha\in B^-$. □

As a consequence, we can identify precisely when (14) may be rewritten as (9), that is, when $f^\alpha\in\mathbf{b}(f)$. First, we know from Theorem 3 that $\mathbf{C1}(\alpha)$ must hold. If $\mathbf{C2}(\alpha)$ also holds, $\alpha\in B^-$ and (14) is already in the required form (9) defining bundle isomorphism. Second, if $\mathbf{C2}(\alpha)$ doesn't hold, we know from Theorem 4 the conditions under which we may replace α by a suitable $\hat{\delta}\circ\alpha$ to obtain (9). In particular, if $\iota_1\in\mathrm{Aut}(N)$ we may set $\delta=\iota_1$.

Corollary 4 *Suppose* $f\simeq_{\mathbf{c}}f'$, $\alpha\in\mathrm{Aut}(N\times G)$, $f'=f^\alpha$ *and* $\mathbf{C1}(\alpha)$ *holds, so*

$$f'=f^\alpha=\bigl(\iota_1\circ f\circ\mathrm{inv}(\rho)\bigr)\bigl(\eta_1\circ\mathrm{inv}(\rho)\bigr)\in\mathbf{c}(f),\tag{41}$$

with $\rho\in\mathrm{Aut}(G)$ *defined by* α *as in* (35). *For* $\delta\in\mathrm{Aut}(N)$, *set* $\alpha'=\hat{\delta}\circ\alpha$. *Then* $\mathbf{C3}(\alpha,\delta)$ *holds if and only if*

$$f'=f^{\alpha'}=\bigl(\delta\circ f\circ\mathrm{inv}(\rho)\bigr)\bigl(\chi_\delta\circ\mathrm{inv}(\rho)\bigr)\in\mathbf{b}(f).\tag{42}$$

Proof By Theorem 4, $\mathbf{C3}(\alpha,\delta)$ holds if and only if $\alpha'(\iota(N))=\iota(N)$ and $\alpha'((f(x),x))=(\delta(f(x))\chi_\delta(x),\ \rho(x))=(f'(\rho(x)),\ \rho(x))$, $x\in G$, where $\chi_\delta\in\mathrm{Hom}(G,\zeta(N))$, if and only if (9) holds, with $\gamma=\delta$, $\theta=\mathrm{inv}(\rho)$ and $\chi=\chi_\delta\circ\mathrm{inv}(\rho)$. □

We can derive new techniques for identifying bundle-inequivalent functions inside canonical bundles, and thus inside graph bundles. Note, however, that if N is elementary abelian, each canonical bundle is a single bundle.

Corollary 5 *Suppose* $f\simeq_{\mathbf{c}}f'$, $\alpha\in B_f^+$ *and* $f'=f^\alpha$.

1. *If* N *is elementary abelian, then* $f\simeq_{\mathbf{b}}f'$, *that is,* $\mathbf{c}(f)=\mathbf{b}(f)$.
2. *If* N *is not elementary abelian, suppose there is no* $\delta\in\mathrm{Aut}(N)$ *such that* $\delta=\breve{\alpha}$ *on* $\mathrm{im}\partial f$ *and* $\chi_\delta\in\mathrm{Hom}(G,\zeta(N))$.

   Then $f\not\simeq_{\mathbf{b}}f'$, *that is,* $\mathbf{b}(f^\alpha)\neq\mathbf{b}(f)$.
3. *If* N *is not elementary abelian, suppose* S_f *generates* $N\times G$ *and* $\mathbf{C2}(\alpha)$ *does not hold. Then* $f\not\simeq_{\mathbf{b}}f'$, *that is,* $\mathbf{b}(f^\alpha)\neq\mathbf{b}(f)$.

Proof Part 1. If N is elementary abelian, the isomorphism $\breve{\alpha}$ between subgroups of N always extends to at least one automorphism δ of N (by basis arguments), and $\zeta(N) = N$. By Theorem 4, $\mathbf{C3}(\alpha, \delta)$ holds, and by Corollary 4, $f' \in \mathbf{b}(f)$. Part 2 follows conversely.

Part 3. Suppose $\mathbf{C3}(\alpha, \delta)$ holds for some $\delta \in \mathrm{Aut}(N)$. By assumption, any $(a, b) \in N \times G$ can be written $(a, b) = \prod_{i=1}^{j}(f(x_i), x_i)^{m_i}$ for some $x_i \in G$, so $\hat{\delta} \circ \alpha((a, b)) = \prod_{i=1}^{j}[\hat{\delta} \circ \alpha((f(x_i), x_i))]^{m_i} = \alpha((a, b))$ by (36). That is, $\hat{\delta} = \mathrm{id}$, so $\alpha((a, 1)) = (\delta(a), 1)$ and $\mathbf{C2}(\alpha)$ holds. □

The following example generalises the seminal case over $\mathbb{Z}_2^n$ and shows that the inverse of a permutation is in the same graph bundle as the permutation, but need not be in the same bundle (an instance is the Gold power function over $\mathbb{Z}_2^n$).

Example 1 Let $G = N$ and let $f \in \mathrm{Sym}_1(G)$. The component swap mapping $\beta(x, y) = (y, x)$ is an automorphism of $G \times G$. Then

1. $f \simeq_{\mathbf{g}} \mathrm{inv}(f)$ and $\mathrm{inv}(f) = f^{\beta}$;
2. $f \simeq_{\mathbf{b}} \mathrm{inv}(f)$ and $\mathbf{C1}(\beta)$ and $\mathbf{C2}(\beta)$ hold $\Leftrightarrow$ $f \in \mathrm{Aut}(G)$ and G is abelian.

Proof $S_{\mathrm{inv}(f)} = \{(\mathrm{inv}(f)(x), x), x \in G\} = \{(x, f(x)), x \in G\}$ and $\beta(T_f) = S_{\mathrm{inv}(f)}$, so Part 1 follows by definition. Note that $\beta(\iota(a)t_x) = \beta((af(x), x)) = (x, af(x))$.

Since $\beta(t_x) = (x, f(x)) = (\mathrm{inv}(f)(f(x)), f(x))$, $\rho = f$ in Theorem 3 and $\beta(T_f) = T_{\mathrm{inv}(f)} \Leftrightarrow f \in \mathrm{Aut}(G)$. Since $J = \{(1, 1)\}$, for each $\delta \in \mathrm{Aut}(G)$, $\chi_\delta = (\delta \circ f)^{-1}$ and $\delta \circ f \in \mathrm{Aut}(G)$. Therefore, $(\delta \circ f)^{-1} \in \mathrm{Hom}(G, \zeta(G))$ if and only if $\zeta(G) = G$. In this case, we may set $\delta = \mathrm{id}$. □

5 Nonlinearity, equivalence class invariants and RDSs

For groups G and N of orders v and w, respectively, several notions of nonlinearity for functions $f : G \to N$ coexist. These measure how different f is from any *linear* function, which in our general context is any element of $\mathrm{Hom}(G, \zeta(N))$. Example 13 of [11] shows that for linear functions,

$$f \in \mathrm{Hom}\big(G, \zeta(N)\big) \Rightarrow \mathbf{b}(f) = \mathrm{Hom}\big(G, \zeta(N)\big); \mathbf{c}(f) = \mathbf{g}(f) \subseteq \mathrm{Hom}(G, N).$$

For abelian groups Nyberg [14, p. 58] defines f to be *differentially m-uniform* when

$$m = \max_{x \neq 1 \in G, c \in N} \big|\big\{y \in G : f(xy)f(y)^{-1} = c\big\}\big|,$$

and her definition clearly extends to any finite groups. We write $m = \Delta(f)$. By inversion of each term $f(xy)f(y)^{-1}$ and premultiplication by the fixed value $f(x)$, $x \neq 1$, this is the same (see (23)) as

$$\Delta(f) = \max_{x \neq 1 \in G, c \in N} \big|\big\{y \in G : \partial f(x, y) = c\big\}\big|. \tag{43}$$

If w divides v and $\Delta(f) = v/w$ we say f is *perfect nonlinear* (PN). If $G = N = \mathbb{Z}_p^n$ and $\Delta(f) = 2$ we say f is *almost perfect nonlinear* (APN).

If S_f contains an RDS it determines a lower bound for $\Delta(f)$, as we show next. The bound is met by semiregular RDSs.

Lemma 4 *Suppose $R = \{(f(x), x), x \in D\} \subseteq S_f$ is a normalised (v, w, k, λ)-RDS in $N \times G$ relative to $N \times \{1\}$, lifting D. Then $\Delta(f) \geq \lambda$.*

Furthermore, $\Delta(f) = \lambda$ iff R is semiregular iff $D = G$.

Proof By Lemma 3, for each $x \neq 1 \in G$, the sequence $\{\partial f(x, y),\ y \in D \cap x^{-1}D\}$ lists each element of N exactly λ times.

If $D \neq G$ then $D \cap x^{-1}D \neq G$, so there exists $y^* \in G \setminus D \cap x^{-1}D$ and $|\{y \in G : \partial f(x, y) = \partial f(x, y^*)\}| \geq \lambda + 1$, so $\Delta(f) > \lambda$. Since $k < v$, R is not semiregular.

If $D = G$ then $D \cap x^{-1}D = G$, $\Delta(f) = \lambda$, $k = v$, $\lambda = v/w$ and $R = S_f$ is semiregular. □

Differential uniformity is preserved by graph isomorphism, and consequently by bundle and canonical isomorphism.

Lemma 5 *Suppose $f \in C^1(G, N)$ and $\alpha \in A_f$. Then $\Delta(f) = \Delta(f^\alpha)$.*

Proof Fix $x \neq 1 \in G$ and $c \in N$, and suppose $y_i,\ i = 1, \dots, \ell$ satisfy $\partial f(x, y_i) = c$ and $\alpha(c, 1) = (a, b)$. Then, from (35),

$$\alpha\bigl(\partial f(x, y_i), 1\bigr) = (a, b) = \bigl(\partial\bigl(f^\alpha \circ \rho\bigr)(x, y_i), \partial\rho(x, y_i)\bigr)$$

for y_i, $i = 1, \dots, \ell$, with $\rho \in \mathrm{Sym}_1(G)$. In particular, equating the first component tells us $\Delta(f) = \Delta(f^\alpha \circ \rho)$. Equating the second component tells us that $\rho(xy_i) = (b^{-1}\rho(x))\rho(y_i)$, so $x' = b^{-1}\rho(x) \neq 1$ and $f^\alpha(\rho(y_i)) f^\alpha(x'\rho(y_i))^{-1} = f^\alpha(\rho(y_i)) f^\alpha(\rho(xy_i))^{-1} = f^\alpha(\rho(x))^{-1}a$, so is constant for $i = 1, \dots, \ell$. Thus $\Delta(f^\alpha \circ \rho) = \Delta(f^\alpha)$. □

Pott [15] extends the definition of another measure of nonlinearity, maximum nonlinearity, from the vectorial Boolean case to the case of abelian groups G and N. This is a character-theoretic definition, given in terms of the values of the characters of $N \times G$ on the graph S_f. If $\widehat{N \times G}$ is the character group of $N \times G$, the *maximum nonlinearity* of f is

$$\mathcal{L}(f) = \max\bigl\{\bigl|\chi(S_f)\bigr| : \chi \neq \chi_0 \in \widehat{N \times G}\bigr\},$$

with $\mathcal{L}(f) \geq \sqrt{v}$. f is *maximally nonlinear* if it attains the minimum possible value for $\mathcal{L}(f)$ for functions from G to N. He suggests that S_f is the correct instrument for measuring the nonlinear behaviour of functions $f : G \to N$.

This property is also preserved by graph isomorphism, and consequently by bundle and canonical isomorphism.

Lemma 6 *Suppose N and G are abelian, $f \in C^1(G, N)$ and $\alpha \in A_f$. Then $\mathcal{L}(f) = \mathcal{L}(f^\alpha)$.*

Proof Note $\chi \in \widehat{N \times G} \Leftrightarrow \chi \circ \alpha \in \widehat{N \times G}$ and $\chi_0 = \chi_0 \circ \alpha$. Thus $\{|\chi(S_f)| : \chi \neq \chi_0 \in \widehat{N \times G}\} = \{|\chi(\alpha(S_f))| : \chi \neq \chi_0 \in \widehat{N \times G}\}$ and its maximum value is the same. □

When w divides v, functions with maximum nonlinearity coincide with PN functions since S_f, considered as the transversal T_f, is a splitting abelian semiregular RDS relative to $N \times \{1\}$. If $G = \mathbb{Z}_2^n$ and $N = \mathbb{Z}_2^t$, a PN function is also bent, that is, it is maximally distant (in a specific sense) from all linear functions. The analogue of this result holds for abelian PN functions $f : G \to N$, using the definition of a bent function due to Logachev et al. [12], in terms of the characters $\chi_c \in \widehat{N}$.

Theorem 5 *Let G and N be abelian groups of orders v and w, respectively, where $w|v$, and let $f \in C^1(G, N)$. Then the following are equivalent:*

1. *f is PN;*
2. [10, Theorem 9.13] *T_f is a splitting abelian $(v, w, v, v/w)$-RDS in $N \times G$ relative to $N \times \{1\}$;*
3. [4, Theorem 16] *For every $c \neq 1 \in N$ the component $f_c = \chi_c \circ f$ is bent, that is, its Fourier Transform $\widehat{f_c}$ has magnitude $\widehat{f_c}(x) = \sqrt{v}$ for every $x \in G$;*
4. [15, Theorem 8] *f is maximally nonlinear with maximal nonlinearity $\sqrt{v}$.*

In the elementary abelian case of most interest in applications, many other invariants of EA and CCZ classes have been discussed, see for example [2]. We close by introducing a new algebraic invariant of bundles, which will in general not be preserved by either canonical or graph isomorphism. Its existence becomes apparent from observing the frequent appearance and significance of the coboundary function ∂f in the work so far.

Definition 5 For $f \in C^1(G, N)$, define $\widehat{N}_f$ to be the normaliser (in N) of the image of ∂f, that is, the smallest normal subgroup of N generated by $\mathrm{im}(\partial f)$:

$$\widehat{N}_f = \left\{ aba^{-1} : a \in N,\ b \in \left\langle \partial f(x, y),\ x,\ y \in G \right\rangle \right\}. \tag{44}$$

Define $N(f)$ to be the order $|\widehat{N}_f|$ of $\widehat{N}_f$, so $1 \le N(f) \le w$ and $N(f)|w$.

The following properties of $\widehat{N}_f$ and $N(f)$ are easy to prove.

Lemma 7 *If $f \in C^1(G, N)$, $\alpha = \iota \times \eta \in B_f^+$ and f^α is given by (41), then*

1. $\widehat{N}_f \lhd \ker(\iota_2)$;
2. $N(f) = 1 \Leftrightarrow \widehat{N}_f = \{1\} \Leftrightarrow f \in \mathrm{Hom}(G, N)$;
3. $N(f) = w \Leftrightarrow \widehat{N}_f = N \Rightarrow B_f^+ = B^- \Rightarrow \mathbf{c}(f) = \mathbf{b}(f)$;
4. *If S_f contains an RDS then $N(f) = w$;*
5. $\partial f^\alpha(x, y) = \iota_1 \circ \partial f(\mathrm{inv}(\rho)(x), \mathrm{inv}(\rho)(y))$;
6. $\iota_1(\widehat{N}_f) \le \widehat{N}_{f^\alpha}$*, so if* $\iota_1 \in \mathrm{Aut}(N)$, $\widehat{N}_{f^\alpha} = \iota_1(\widehat{N}_f)$ *and* $N(f^\alpha) = N(f)$;
7. *If $f' \simeq_{\mathbf{b}} f$, then $\widehat{N}_{f'} \cong \widehat{N}_f$ and $N(f') = N(f)$;*
8. *If N is abelian, $\widehat{N}_f = \langle \partial f(x, y),\ x,\ y \in G \rangle$;*
9. *If $N \cong \mathbb{Z}_p^n$ is elementary abelian (written additively), $\widehat{N}_f$ is a p-ary linear $[n,\ \log_p(N(f))]$ code.*

Proof Lemma 1 gives Property 1 since $\ker(\iota_2)$ is a normal subgroup of N, and Property 2 is straightforward. For Property 3, $\widehat{N}_f = N \Rightarrow$ for each $\alpha \in B_f^+$, $\ker(\iota_2) = N \Rightarrow \iota_2 = \mathbf{1} \Rightarrow \alpha \in B^-$. For Property 4, $\widehat{N}_f = N$ by Theorem 2. Direct computation gives Property 5, since ι_1 commutes with η_1 (see (11)). Then

$$\iota_1\bigl(a\,\partial f(x,y)a^{-1}\bigr) = \iota_1(a)\partial f^\alpha\bigl(\rho(x),\rho(y)\bigr)\iota_1(a)^{-1},$$

and Property 6 follows. Property 7 follows by similar arguments. Properties 8 and 9 are obvious. □

Corollary 6 *$N(f)$ is an invariant of $\mathbf{b}(f)$, but not necessarily of $\mathbf{c}(f)$ or $\mathbf{g}(f)$. If $\alpha \in A_f$ and $N(f^\alpha) \neq N(f)$ then $\mathbf{b}(f^\alpha) \neq \mathbf{b}(f)$.*

Proof Lemma 7.6 gives the first result. If there is an $\alpha \in B_f^+$ with $\iota_1 \notin \mathrm{Aut}(N)$ then Lemma 7.4 implies a minimal generating set in $\mathrm{im}(\partial f^\alpha)$ for $\widehat{N}_{f^\alpha}$ may be smaller than a minimal generating set in $\mathrm{im}(\partial f)$ for $\widehat{N}_f$, and the rest follows. □

6 Conclusion and future work

We have shown that the problem of partitioning a graph equivalence class $\mathbf{g}(f)$ into bundles splits naturally into two sequential parts: first, to partition $\mathbf{g}(f)$ into canonical bundles $\mathbf{c}(f = f_1), \mathbf{c}(f_2), \ldots, \mathbf{c}(f_k)$; and second, to partition canonical bundles into bundles.

We have shown that any automorphism acting on f within $\mathbf{g}(f)$ can map to an element of $\mathbf{b}(f)$ only under two very strict conditions, the first of which ensures it maps to an element of $\mathbf{c}(f)$ and the second of which ensures that within $\mathbf{c}(f)$ it maps to an element of $\mathbf{b}(f)$. The first problem then translates to characterising the stabiliser group of automorphisms F_f and in particular, its subgroup $B_f^+ \cap F_f$ (Corollary 2).

Much of the contribution of this paper applies to the second problem. We know now that if $\mathbf{c}(f)$ contains more than one bundle then S_f cannot contain a splitting RDS (Theorem 2), whereas if S_f does contain a splitting RDS the differential uniformity of f is bounded below by the multiplicity λ of the RDS (Lemma 4). If S_f is a semiregular RDS this lower bound is tight and f is PN. The precise relationship between the differential uniformity $\Delta(f)$ of f in less optimal cases (such as the APN functions when $N = G = \mathbb{Z}_2^n$), and the algebraic invariant $N(f)$ introduced here, is still to be discovered. By (43) and (44), it is a close relationship, but $N(f)$ is able to discriminate between bundles within some canonical bundles while $\Delta(f)$ and $\mathcal{L}(f)$ cannot. For functions over $GF(p^n)$, some other bundle invariants, such as the algebraic degree of f, are also known to discriminate within graph bundles (CCZ classes), and their relationship to the more general invariant $N(f)$ is yet to be determined. From the other direction, the dimension of the ideal generated by S_f in the group algebra $GF(2)(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ is an invariant of the CCZ class of f [2], and its relationship to $N(f)$ has yet to be determined.

In conclusion, we have a rich research field for further mining.

References

1. Breveglieri, L., Cherubini, A., Macchetti, M.: On the generalized linear equivalence of functions over finite fields. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 79–91. Springer, Berlin (2004)
2. Browning, K.A., Dillon, J.F., Kibler, R.E., McQuistan, M.T.: APN polynomials and related codes. J. Comb. Inf. Syst. Sci. **34**, 135–159 (2009). Special Issue honoring the 75th birthday of Prof. D.K. Ray-Chaudhuri
3. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inf. Theory **52**, 1141–1152 (2006)
4. Carlet, C., Ding, C.: Highly nonlinear mappings. J. Complex. **20**, 205–244 (2004)
5. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998)
6. Cavior, S.R.: Equivalence classes of functions over a finite field. Acta Arith. **10**, 119–136 (1964)
7. Coulter, R.S., Matthews, R.W.: Planar functions and planes of Lenz–Barlotti Class II. Des. Codes Cryptogr. **10**, 167–184 (1997)
8. Elliott, J.E.H., Butson, A.T.: Relative difference sets. Ill. J. Math. **10**, 517–531 (1966)
9. Galati, J.C.: A group extensions approach to relative difference sets. J. Comb. Des. **12**, 279–298 (2004)
10. Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007)
11. Horadam, K.J.: Relative difference sets, graphs and inequivalence of functions between groups. J. Comb. Des. **18**, 260–273 (2010)
12. Logachev, O.A., Salnikov, A.A., Yashchenko, V.V.: Bent functions on a finite abelian group. Discrete Math. Appl. **7**, 547–564 (1997)
13. Mullen, G.L.: Weak equivalence of functions over a finite field. Acta Arith. **35**, 259–272 (1979)
14. Nyberg, K.: Differentially uniform mappings for cryptography. In: EUROCRYPT-93. LNCS, vol. 765, pp. 55–64. Springer, New York (1994)
15. Pott, A.: Nonlinear functions in abelian groups and relative difference sets. Discrete Appl. Math. **138**, 177–193 (2004)
16. Robinson, D.J.S.: A Course in the Theory of Groups, 2nd edn. Springer, New York (1996)