J. Aust. Math. Soc. **85** (2008), 177–190
doi:10.1017/S1446788708000876

A POLYNOMIAL APPROACH TO COCYCLES OVER ELEMENTARY ABELIAN GROUPS

D. G. FARMER and K. J. HORADAM ✉

(Received 4 January 2008; accepted 12 May 2008)

Communicated by Martin W. Liebeck

Dedicated to Cheryl Praeger for her sixtieth birthday

Abstract

We derive bivariate polynomial formulae for cocycles and coboundaries in $Z^2(\mathbb{Z}_p^n, \mathbb{Z}_p^n)$, and a basis for the $(p^n - 1 - n)$-dimensional $\mathrm{GF}(p^n)$-space of coboundaries. When $p = 2$ we determine a basis for the $(2^n + \binom{n}{2} - 1)$-dimensional $\mathrm{GF}(2^n)$-space of cocycles and show that each cocycle has a unique decomposition as a direct sum of a coboundary and a multiplicative cocycle of restricted form.

2000 *Mathematics subject classification*: 11T06, 20J06.

Keywords and phrases: 2-cocycle, coboundary, multiplicative cocycle, basis, Pascal's triangle.

1. Introduction

We consider only two-dimensional cocycles between finite groups, with trivial action. These cocycles are functions arising naturally in surface topology, projective representation theory, combinatorial designs and quantum dynamics, amongst other areas. They are used to search for good high-distance error-correcting codes, low-correlation sequences and functions with strong nonlinearity properties for cryptographic applications. Two basic classes of cocycles, the coboundaries and the multiplicative cocycles, have proved very productive for these purposes. The coboundaries are used to find S-box functions with low differential uniformity, such as perfect nonlinear (PN) and almost perfect nonlinear (APN) functions, which are thus robust against differential cryptanalysis [4, 3]. The multiplicative cocycles over elementary abelian groups form a structured space within which to find generalized Hadamard matrices and codes [10, 12], relative difference sets [11] and finite semifields which coordinatize certain projective planes [9]. Cocycles fall into equivalence classes ('bundles') within which these desirable properties are invariant.

© 2008 Australian Mathematical Society 1446-7887/08 $A2.00 + 0.00

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

Very little is known about the form of individual cocycles or how to find all the cocycles (or even all the coboundaries) from a finite group G to a finite abelian group C. In the early 1990s, a group theoretic algorithm was developed that lists a minimal set of generators of the group of cocycles for *abelian* groups G. However, focus is usually on listing a set of representatives of the second cohomology group (the quotient group of the group of cocycles by the subgroup of coboundaries). Facilities for computation and manipulation of a set of cohomology class representatives exist in several computational algebra packages; for instance, MAGMA has a module (due to Flannery and O'Brien [7]) which uses the universal coefficient theorem to list them. Another algorithm uses a smaller homological model to compute such representatives much faster, but requires more precomputation.

The second cohomology group decomposes as an internal direct sum of two groups, so every cocycle is a sum of an 'inflation' cocycle, a 'transgression' cocycle and a coboundary, but the decomposition is not unique. Computation of a set of generators for the subgroup of coboundaries is usually left as an exercise in linear algebra, although for cocycles mapping to $\mathbb{Z}_2$ an algorithm is known. See [8, Chapter 6.3] for details.

This paper has two main purposes. The first is to present a formula for any cocycle from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$ as a bivariate polynomial over $\mathrm{GF}(p^n)$. This provides a new technique for working with these cocycles and a fourth algorithm for computation in this particular case. The second is to exploit an overlying vector space structure of the group of cocycles to extract a basis for the space of coboundaries. When $p = 2$—the most important case for applications—we then extract a basis for the space of cocycles.

The paper is organized as follows. In Section 2 we use Lagrange interpolation and the cocycle equation to derive polynomial formulae for coboundaries, cocycles and multiplicative cocycles from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$. In Section 3 we prove two results about coboundaries. The first (Theorem 3.1) is the basis theorem for coboundaries and we show that the bases exhibit self-similarity as n increments. The second (Theorem 3.4) captures this self-similarity in a recursive formula for the coboundary basis when $p = 2$, suitable for computation.

In the final Section 4, we concentrate on cocycles from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^m$, $n \geq m$. We show (Lemma 4.1) that every symmetrization cocycle is a coboundary (which, when $m = n$, must be defined by a unique Dembowski–Ostrom polynomial). We then derive the basis theorem for cocycles (Theorem 4.5) and, as a consequence, bases and dimensions for several other subspaces of interest. From this we prove that any cocycle over $\mathbb{Z}_2^n$ has a unique decomposition as a direct sum of a coboundary and a multiplicative noncoboundary cocycle of specific form (Corollary 4.7).

2. Cocycles and coboundaries

Let $\mathrm{GF}(q)$ be the finite field of order $q = p^n$, where p is prime and $n \in \mathbb{Z}^+$. Let G be a finite group, C be an additively written finite abelian group, and let $C^1(G, C) = \{\phi \mid G \to C,\ \phi(1) = 0\}$ be the group of all normalized functions from G to C.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

Each $\phi \in C^1(G, C)$ determines a *coboundary* $\partial\phi(x, y) = \phi(xy) - \phi(x) - \phi(y)$, which measures how much ϕ differs from a homomorphism from G to C. A coboundary is the simplest form of cocycle. A (two-dimensional normalized) *cocycle* (with trivial action) is a mapping $\psi : G \times G \to C$ satisfying

$$\psi(1, 1) = 0; \quad \psi(x, y) + \psi(xy, z) = \psi(x, yz) + \psi(y, z) \quad \forall x, y, z \in G. \tag{2.1}$$

The set $Z^2(G, C)$ of cocycles over G with values in C is an abelian group under pointwise addition. The subgroup of coboundaries is denoted $B^2(G, C)$, and the *coboundary mapping* $\partial : C^1(G, C) \to B^2(G, C)$ mapping ϕ to $\partial\phi$ is a group homomorphism with kernel $\ker(\partial) = \mathrm{Hom}(G, C)$.

In the reverse direction to ∂ is the *diagonal mapping*

$$D : Z^2(G, C) \to C^1(G, C), \quad D\psi(x) = \psi(x, x) \quad \forall x \in G. \tag{2.2}$$

It follows that $\partial \circ D : Z^2(G, C) \to B^2(G, C)$ and $(D \circ \partial)\phi(x) = \phi(x^2) - 2\phi(x)$. The mappings D and ∂ may be thought of as generalizing the mappings between bilinear and quadratic forms.

We are interested in two other subgroups of $Z^2(G, C)$: the subgroup $M^2(G, C)$ of multiplicative cocycles and the subgroup $S^2(G, C)$ of symmetric cocycles[1].

A cocycle is called *multiplicative* if it is a homomorphism on either coordinate (and hence on both coordinates, by (2.1)). If G is abelian, on defining $\psi^\top(x, y) = \psi(y, x)$ and $\psi^-(x, y) = \psi(x, y) - \psi(y, x)$ for all $x, y \in G$, we have that $\psi^\top$ and ψ^- are cocycles, the decomposition $\psi = \psi^\top + \psi^-$ is unique, and ψ^-, the commutator pairing, is multiplicative [2, Exercises IV.3.8 and V.6.5].

A cocycle ψ is called *symmetric* if $\psi(x, y) = \psi(y, x)$ for all $x, y \in G$. If G is abelian, the coboundaries are all symmetric, that is, $B^2(G, C) \leq S^2(G, C)$, the *symmetrization* ψ^+ of ψ, given by $\psi^+(x, y) = \psi(x, y) + \psi(y, x)$, is a symmetric cocycle, and then the *symmetrization mapping* $S^+ : Z^2(G, C) \to S^2(G, C)$, given by $S^+(\psi) = \psi^+$, is a group homomorphism. We set $S^2_+(G, C) = S^+(Z^2(G, C))$.

If G is abelian the isotype of the finite abelian group $Z^2(G, C)$ may be derived using cohomological techniques [8, Theorem 6.13, Corollary 6.16]. We record the elementary abelian case needed here.

PROPOSITION 2.1. *Let $G \cong \mathbb{Z}_p^n$ and $C \cong \mathbb{Z}_p^m$, $n \geq m \geq 1$ and set $N = p^n + \binom{n}{2} - 1$, with $\binom{n}{2} = 0$ if $n = 1$. Then $Z^2(\mathbb{Z}_p^n, \mathbb{Z}_p^m) \cong C^N \cong (\mathbb{Z}_p^m)^N$.*

2.1. A polynomial formula for cocycles over GF(q) This subsection is devoted to the representation of cocycles in $Z^2(\mathbb{Z}_p^n, \mathbb{Z}_p^n)$ as bivariate polynomials. We treat $\mathbb{Z}_p^n$ as the underlying additive group of the finite field GF(q), where $q = p^n$, so that $G = C = (\mathrm{GF}(q), +)$.

By the Lagrange interpolation formula [15, Theorem 1.71], if $m \geq 1$, then for m distinct points $a_0, \ldots, a_{m-1}$ of GF(q) and m arbitrary points $b_0, \ldots, b_{m-1}$ of

[1] In [8] the subgroup of symmetric cocycles is denoted $S^2_+(G, C)$ but the notation presented here, with $S^2_+(G, C)$ reserved for the subgroup of symmetrization cocycles, is more consistent.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

GF(q) there exists a unique polynomial $f \in \mathrm{GF}(q)[x]$ of degree less than m such that $f(a_i) = b_i$ for $i = 0, \ldots, m-1$. Any function $\pi : \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q)$ can therefore be represented by a unique polynomial $P \in \mathrm{GF}(q)[x, y]$ as follows. Let α be a primitive element of GF(q) and order GF(q) as $\mathrm{GF}(q) = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = \alpha, \ldots, \alpha_{q-1} = \alpha^{q-2}\}$. Under this ordering a $q \times q$ array A with entries from GF(q) determined by $\pi(\alpha_i, \alpha_j) = a_{ij}$ will have, for each row $A_i = [a_{i0}, \ldots, a_{i,q-1}]$, a unique polynomial $f_i(y) = \sum_{k=0}^{q-1} b_{ik} y^k \in \mathrm{GF}(q)[y]$ such that $f_i(\alpha_j) = a_{ij}$. For fixed k, the coefficients of y^k from each row are $\{b_{ik} \mid i = 0, \ldots, q-1\}$, and for each k there is a unique polynomial $g_k(x) = \sum_{l=0}^{q-1} \lambda_{lk} x^l$ such that $g_k(\alpha_i) = b_{ik}$. Since $f_i(y) = \sum_{k=0}^{q-1} g_k(\alpha_i) y^k$, there exists a unique polynomial $P \in \mathrm{GF}(q)[x, y]$ such that

$$\pi(x, y) = P(x, y) = \sum_{k=0}^{q-1} \sum_{l=0}^{q-1} \lambda_{lk} x^l y^k.$$

If $\psi : \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q)$ also satisfies $\psi(x, 0) = \psi(0, y) = 0$ for all $x, y \in \mathrm{GF}(q)$ (a necessary condition for the cocycle equation (2.1) to hold for $G = C = (\mathrm{GF}(q), +)$) then it has a unique representation in GF$(q)[x, y]$,

$$\psi(x, y) = \sum_{i=1}^{q-1} \sum_{j=1}^{q-1} \lambda_{ij} x^i y^j. \tag{2.3}$$

For a coboundary, the coefficients in (2.3) are very restricted. Again by Lagrange interpolation every $\phi \in C^1(G, G)$ may be represented uniquely as a polynomial of degree at most $q-1$ in GF$(q)[x]$.

LEMMA 2.2. *Let $\psi : \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q)$ be given by (2.3). If $\phi : \mathrm{GF}(q) \to \mathrm{GF}(q)$ is given by $\phi(x) = \sum_{i=1}^{q-1} \phi_i x^i$, then $\psi = \partial\phi$ if and only if:*

(1) $\lambda_{ij} = 0$, *for* $j = q-i, \ldots, q-1$;

(2) $\lambda_{ij} = \binom{i+j}{i} \phi_{i+j}$, *otherwise.*

PROOF.

$$\begin{aligned}\partial\phi(x, y) &= \sum_{i=1}^{q-1} \phi_i \{(x+y)^i - x^i - y^i\} = \sum_{i=2}^{q-1} \sum_{j=1}^{i-1} \phi_i \binom{i}{j} x^{i-j} y^j \\ &= \sum_{i=1}^{q-2} \sum_{j=1}^{q-i-1} \phi_{i+j} \binom{i+j}{j} x^i y^j,\end{aligned}$$

and the result follows on equating coefficients. □

Clearly, if $\psi : \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q)$ is given by (2.3) then ψ is symmetric if and only if $\lambda_{ij} = \lambda_{ji}$, $1 \le i, j \le q-1$.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

Subsequently we will need the following theorem, attributed to Lucas [16] in [6], and its corollaries.

THEOREM 2.3 (Lucas' theorem). [6, Theorem 1] *Let p be a prime, and let*

$$m = m_0 + m_1 p + m_2 p^2 + \cdots + m_k p^k \quad (0 \le m_r < p),$$
$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k \quad (0 \le n_r < p).$$

Then

$$\binom{m}{n} = \binom{m_0}{n_0}\binom{m_1}{n_1}\binom{m_2}{n_2}\cdots\binom{m_k}{n_k} \bmod p. \tag{2.4}$$

COROLLARY 2.4. [6, Theorem 3] *A necessary and sufficient condition that all the binomial coefficients*

$$\binom{m}{n}, \quad 0 < n < m, \tag{2.5}$$

be divisible by p is that m be a power of p.

The p-ary *weight* $w_p(k)$ of the natural number k is the weight of the vector of coefficients of its p-ary expansion, so, for example, $w_p(p^i) = 1$ and, for $i \neq j$, $w_p(p^i + p^j) = 2$.

COROLLARY 2.5. *Let $m = 2, \ldots, p^n - 1$ and $n < m$. Then $w_p(m) = 1$ implies $\binom{m}{n}$ $= 0 \bmod p$.*

The next function class of interest is that consisting of the 'multiplicative' bivariate polynomials (2.3); that is, those which are homomorphic in each coordinate. Such functions are always cocycles. The following result may be well known but a proof is provided for completeness. The coboundary case is well known [1].

THEOREM 2.6. *Let $\psi : \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q)$ be given by (2.3). Then ψ is multiplicative if and only if*

$$\psi(x, y) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \lambda_{p^i p^j} x^{p^i} y^{p^j}.$$

PROOF. It is straightforward to show that if ψ has this form it is multiplicative. To show that the converse is true, let ψ be multiplicative in both coordinates, that is

$$\psi(x + z, y) = \psi(x, y) + \psi(z, y), \tag{2.6}$$
$$\psi(x, y + z) = \psi(x, y) + \psi(x, z). \tag{2.7}$$

Expanding the left-hand side of (2.6) gives, for each $\lambda_{ij} \neq 0$,

$$\sum_{i=1}^{q-1} \left[\binom{i}{1} x^{i-1} z + \binom{i}{2} x^{i-2} z^2 + \cdots + \binom{i}{i-1} x z^{i-1} \right] = 0, \quad \forall x, z \in \mathrm{GF}(q).$$

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

Therefore, we must have that, for each $i = 1, 2, \ldots, q-1$,

$$\binom{i}{r} \equiv 0 \bmod p \quad \forall r = 1, 2, \ldots, i-1.$$

From Corollary 2.4, $i = p^s$ for $s = 0, 1, \ldots, \lfloor \log_p(q-1) \rfloor = n-1$. By symmetry, (2.7) implies $j = p^l$ only, with $l = 0, 1, \ldots, n-1$. □

Our main result for this section is the following formula for any cocycle in $Z^2(\mathbb{Z}_p^n, \mathbb{Z}_p^n)$, in terms of simultaneous linear equations over GF(q) in the bivariate polynomial coefficients λ_{ij}. The proof is a straightforward exercise in tracking limits of summation.

This new approach to studying $Z^2(\mathbb{Z}_p^n, \mathbb{Z}_p^n)$ complements those in [8].

THEOREM 2.7. *Let $\psi : \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q)$ be given by (2.3). Then ψ satisfies (2.1) if and only if:*

(1) $\binom{i+l}{l}\lambda_{i+l,j} = 0$, *for $i = 1, \ldots, j-1$ and $l = q-j, \ldots, q-1-i$;*

(2) $\binom{j+l}{l}\lambda_{i,l+j} = 0$, *for $i = j+1, \ldots, q-1$ and $l = q-i, \ldots, q-1-j$;*

(3) $\binom{i+l}{l}\lambda_{i+l,j} = \binom{j+l}{l}\lambda_{i,l+j}$, *otherwise.*

PROOF. Now, $\psi(g, h) + \psi(g+h, k) - \psi(g, h+k) - \psi(h, k) = 0$ if and only if

$$\begin{aligned} 0 &= \sum_{j=1}^{q-1}\sum_{i=2}^{q-1}\sum_{l=1}^{i-1} \lambda_{ij}\binom{i}{l} g^{i-l}h^l k^j - \sum_{j=2}^{q-1}\sum_{i=1}^{q-1}\sum_{l=1}^{j-1} \lambda_{ij}\binom{j}{l} g^i h^{j-l} k^l \\ &= \sum_{j=1}^{q-1}\sum_{i=1}^{q-2}\sum_{l=1}^{q-i-1} \lambda_{i+l,j}\binom{i+l}{l} g^i h^l k^j - \sum_{j=1}^{q-2}\sum_{i=1}^{q-1}\sum_{l=1}^{q-j-1} \lambda_{i,j+l}\binom{j+l}{l} g^i h^l k^j. \end{aligned}$$

Splitting this into cases for $i < j$, $i = j$ and $i > j$ gives

$$\begin{aligned} 0 = {} & \sum_{j=2}^{q-2}\sum_{i=1}^{j-1}\sum_{l=1}^{q-1-j} \left(\lambda_{i+l,j}\binom{i+l}{l} - \lambda_{i,l+j}\binom{j+l}{l}\right) g^i h^l k^j \\ & + \sum_{j=1}^{q-3}\sum_{i=j+1}^{q-2}\sum_{l=1}^{q-1-i} \left(\lambda_{i+l,j}\binom{i+l}{l} g^i h^l k^j - \lambda_{i,l+j}\binom{j+l}{l}\right) g^i h^l k^j \\ & + \sum_{i=1}^{q-2}\sum_{l=1}^{q-1-i} \left(\lambda_{i+l,i}\binom{i+l}{l} - \lambda_{i,l+i}\binom{i+l}{l}\right) g^i h^l k^i \\ & + \sum_{j=2}^{q-1}\sum_{i=1}^{j-1}\sum_{l=q-j}^{q-1-i} \lambda_{i+l,j}\binom{i+l}{l} g^i h^l k^j - \sum_{j=1}^{q-2}\sum_{i=j+1}^{q-1}\sum_{l=q-i}^{q-1-j} \lambda_{i,l+j}\binom{j+l}{l} g^i h^l k^j. \end{aligned}$$

The sum on the right-hand side contains each term $g^i h^l k^j$ exactly once, so by linear independence it is equal to 0 if and only if the stated conditions hold. □

Solution of these simultaneous equations using Theorem 2.3 will give the general cocycle formula for each q. Some coefficients will necessarily be zero.

We illustrate Theorem 2.7 for the smallest examples $q = 2, 3, 4, 5, 7, 8$. The number of independent coefficients λ_{ij}, namely 1, 2, 4, 4, 6, 10, is the integer N of Proposition 2.1. (See also [8, Examples 6.3.1 and 6.3.2].)

EXAMPLE 1. Let $G = C = (\mathrm{GF}(q), +)$. Let $\psi \in Z^2(G, G)$ have form (2.3).

(1) If $q = 2$, $\psi(x, y) = \lambda_{11}\, xy$.

(2) If $q = 3$, $\psi(x, y) = \lambda_{11}\, xy + \lambda_{12}(xy^2 + x^2y)$.

(3) If $q = 4$, $\psi(x, y) = \lambda_{11}\, xy + \lambda_{12}\, xy^2 + \lambda_{21}\, x^2y + \lambda_{22}\, x^2y^2$.

(4) If $q = 5$, $\psi(x, y) = \lambda_{11}\, xy + \lambda_{12}(xy^2 + x^2y) + \lambda_{22}(4xy^3 + x^2y^2 + 4x^3y) + \lambda_{14}(xy^4 + 2x^2y^3 + 2x^3y^2 + x^4y)$.

(5) If $q = 7$, $\psi(x, y) = \lambda_{11}\, xy + \lambda_{12}(xy^2 + x^2y) + \lambda_{13}(xy^3 + 5x^2y^2 + x^3y) + \lambda_{14}(xy^4 + 2x^2y^3 + 2x^3y^2 + x^4y) + \lambda_{15}(xy^5 + 6x^2y^4 + x^3y^3 + 6x^4y^2 + x^5y) + \lambda_{16}(xy^6 + 3x^2y^5 + 5x^3y^4 + 5x^4y^3 + 3x^5y^2 + x^6y)$.

(6) If $q = 8$, $\psi(x, y) = \lambda_{11}\, xy + \lambda_{12}\, xy^2 + \lambda_{21}\, x^2y + \lambda_{22}\, x^2y^2 + \lambda_{14}\, xy^4 + \lambda_{41}\, x^4y + \lambda_{24}\, x^2y^4 + \lambda_{42}\, x^4y^2 + \lambda_{44}\, x^4y^4 + \lambda_{16}(xy^6 + x^2y^5 + x^3y^4 + x^4y^3 + x^5y^2 + x^6y)$.

3. Coboundaries over GF(p^n)

We will abbreviate by B the finite abelian group of coboundaries $B^2(\mathbb{Z}_p^n, \mathbb{Z}_p^n)$.

THEOREM 3.1 (Coboundary basis theorem). *For $n > 1$ and $k = 2, \ldots, p^n - 1$, define $c_k \in B$ by*

$$c_k(x, y) = \sum_{i=1}^{k-1} \binom{k}{i} x^i y^{k-i}.$$

Then $\{c_k \mid k = 2, \ldots, p^n - 1, w_p(k) \geq 2\}$ is a basis for B over GF(p^n), *and* $\dim(B) = p^n - 1 - n$.

PROOF. For $\phi(x)$ as in Lemma 2.2,

$$\partial\phi(x, y) = \sum_{i=1}^{p^n-2} \sum_{j=1}^{p^n-i-1} \phi_{i+j} \binom{i+j}{i} x^i y^j = \sum_{k=2}^{p^n-1} \sum_{i=1}^{k-1} \phi_k \binom{k}{i} x^i y^{k-i}$$
$$= \sum_{k=2}^{p^n-1} \phi_k\, c_k(x, y),$$

so $\{c_k \mid k = 2, \ldots, p^n - 1\}$ spans B. From Corollary 2.5, $w_p(k) = 1$ implies $c_k \equiv 0$ so there are $p^n - 1 - n$ elements c_k spanning B. These c_k are linearly independent since distinct c_k have no monomial summands in common. □

MAGMA computations using Theorem 3.1 show that the coboundary bases exhibit recursive patterns as n increments. In effect, this recursion occurs because the

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

coefficients $\binom{k}{i}$, $i = 1, \ldots, k-1$, of each basis element c_k are the nontrivial binomial coefficients in a row of Pascal's triangle. In [17], Wolfram describes the self-similar geometry of Pascal's triangle when the binomial coefficients are taken modulo r. In the case of prime r, it is observed to have a very regular self-similar pattern, but no reason is given. We can explain this regularity in terms of Lucas' theorem and the matrix Kronecker product. The matrix P_n in Theorem 3.2 has the successive rows of Pascal's triangle as its upper diagonals, with the convention $\binom{m}{0} = 1$. The core of P_n, that is, P_n stripped of its first row and column of 1's, has the coefficients of successive basis elements c_k as its upper and main diagonals.

THEOREM 3.2. *Define* $P_n = [a_{ij}]$, *where* $a_{ij} = \binom{i+j}{i} \bmod p$, $i, j = 0, 1, \ldots, p^n - 1$. *Then* $P_{n+1} = P_n \otimes P_1 = \otimes^{n+1} P_1$.

PROOF. Consider any entry a_{ij} of P_k where $i + j \geq p^k$. These entries will all have a factor p^k, and hence $a_{ij} = 0 \bmod p$ for $i + j \geq p^k$. Therefore,

$$P_k = \begin{bmatrix} \binom{0}{0} & \binom{1}{0} & \binom{2}{0} & \ldots & \binom{p^k-1}{0} \\ \binom{1}{1} & \binom{2}{1} & \binom{3}{1} & \ldots & 0 \\ \binom{2}{2} & \binom{3}{2} & \binom{4}{2} & \ldots & 0 \\ \vdots & & & \ldots & \vdots \\ \binom{p^k-1}{p^k-1} & 0 & 0 & \ldots & 0 \end{bmatrix}. \tag{3.1}$$

Now consider the (i, j)th entry of P_{k+1}, where $i = up^k + m$, $0 \leq u < p$, $0 \leq m < p^k$ and $j = vp^k + n$, $0 \leq v < p$, $0 \leq n < p^k$. Then

$$a_{ij} = \binom{(m+n) + (u+v)p^k}{up^k + m}.$$

From (3.1), if $(m+n) + (u+v)p^k \geq p^{k+1}$, then $a_{ij} = 0 \bmod p$. Two cases can occur if $(m+n) + (u+v)p^k < p^{k+1}$. If $m + n \geq p^k$ then a_{ij} will have a factor $(1 + u + v)p^k$, and hence $a_{ij} = 0 \bmod p$. If $m + n < p^k$, then by Theorem 2.3,

$$\begin{aligned} a_{ij} &= \binom{m + n + (u+v)p^k}{up^k + m} \\ &= \binom{m+n}{m}\binom{u+v}{u} \bmod p. \end{aligned}$$

Since $P_k = [a_{mn}]$ for $0 \leq m, n < p^k$, and $P_1 = [a_{uv}]$ for $0 \leq u, v < p$, we have that $P_{k+1} = P_k \otimes P_1$. □

Theorem 3.2 implies that the basis elements for $B^2(\mathbb{Z}_p^n, \mathbb{Z}_p^n)$ are bivariate polynomial functions of the basis elements for $B^2(\mathbb{Z}_p^{n-1}, \mathbb{Z}_p^{n-1})$.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

For $p = 2$ the recursion formula is very simple, and can be deduced by different methods. An intermediate inductive lemma is our key; proof is left to the reader. We sum over all the basis elements c_k, that is, we sum all terms with coefficients in the core of P_n.

LEMMA 3.3. *For $n > 1$, define*

$$A_n(x, y) = \sum_{k=2}^{2^n-1} c_k(x, y),\ A_n^{(c)}(x, y) = y^{2^n} \sum_{l=1}^{2^n-1} \binom{l+2^n}{l} x^l$$

and

$$A_n^{(r)}(x, y) = x^{2^n} \sum_{l=1}^{2^n-1} \binom{l+2^n}{2^n} y^l.$$

Then $A_{n+1} = A_n + y^{2^n} A_n + A_n^{(c)} + A_n^{(r)} + x^{2^n} A_n$.

THEOREM 3.4. *For $n > 1$ and $2^{n-1} < k < 2^n$, the coboundaries c_k over $\mathbb{Z}_2^n$ can be defined recursively:*

$$c_k(x, y) = \begin{cases} (x^{k-2^{n-1}} + c_{k-2^{n-1}})y^{2^{n-1}} + x^{2^{n-1}}(y^{k-2^{n-1}} + c_{k-2^{n-1}}), & w_2(k) \geq 3 \\ x^{2^r} y^{2^{n-1}} + x^{2^{n-1}} y^{2^r}, \quad k = 2^{n-1} + 2^r,\ r = 0, \ldots, n-2. \end{cases}$$

PROOF. By Lemma 3.3,

$$\sum_{k=2^{n-1}}^{2^n-1} c_k(x, y) = y^{2^{n-1}} A_{n-1} + A_{n-1}^{(c)} + A_{n-1}^{(r)} + x^{2^{n-1}} A_{n-1}.$$

Hence

$$c_k(x, y) = y^{2^{n-1}} c_{k-2^{n-1}} + x^{k-2^{n-1}} y^{2^{n-1}} + x^{2^{n-1}} y^{k-2^{n-1}} + x^{2^{n-1}} c_{k-2^{n-1}}.$$

If $w_2(k) = 2$ then $w_2(k - 2^{n-1}) = 1$ and $c_{k-2^{n-1}} \equiv 0$. □

4. A polynomial basis for cocycles over $\mathbb{Z}_2^n$

From now on, we consider cocycles in $Z^2(\mathbb{Z}_2^n, \mathbb{Z}_2^m)$, $n \geq m \geq 1$, where we can say more about the subgroup of symmetrization cocycles S_+^2. Not only is every symmetrization multiplicative, it is also a coboundary.

LEMMA 4.1. *Let $G \cong \mathbb{Z}_2^n$ and $C \cong \mathbb{Z}_2^m$, $n \geq m \geq 1$.*

(i) $\ker(S^+) = S^2(G, C)$ *so* $S_+^2(G, C) \leq M^2(G, C) \cap S^2(G, C)$.

(ii) $S^+ = \partial \circ D$ *so* $S_+^2(G, C) = (\partial \circ D)(Z^2(G, C)) \leq M^2(G, C) \cap B^2(G, C)$.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

PROOF. (i) This follows by definition since $\psi^- = \psi^+$ and ψ^- is multiplicative.

(ii) If $\psi \in Z^2(G, C)$, then

$$\begin{aligned}\partial(D\psi)(x, y) &= \psi(x+y, x+y) + \psi(x, x) + \psi(y, y)\\ &= (\psi(x, y) + \psi(x, y+x+y) + \psi(y, y+x)) + \psi(x, x) + \psi(y, y)\end{aligned}$$

by (2.1), which is equal to

$$\psi(x, y) + (\psi(y+y, x) + \psi(y, y) + \psi(y, x)) + \psi(y, y)$$

again by (2.1), which is equal to $S^+(\psi)(x, y)$. □

Hereafter, assume $G = C = (\mathrm{GF}(2^n), +) \cong \mathbb{Z}_2^n$. We will abbreviate by Z, B, M, S and S_+ the finite abelian groups of cocycles, coboundaries, multiplicative, symmetric and symmetrization cocycles respectively. In this case, by Proposition 2.1, Z is a $\mathrm{GF}(2^n)$-vector space of dimension $N = 2^n + \binom{n}{2} - 1$.

The function $\phi : G \to G$ is said to be *linearized* or *quadratic* if every monomial summand has degree of binary weight ≤ 1 or ≤ 2, respectively. A polynomial for which every monomial summand has degree of weight 2 is called a *Dembowski–Ostrom* (DO) polynomial in [5]. That is, a polynomial ϕ in $\mathrm{GF}(2^n)[x]$ is DO if, when reduced modulo $x^{2^n} - x$, it is of the form

$$\phi(x) = \sum_{j=1}^{n-1} \sum_{i=0}^{j-1} \lambda_{ij}\, x^{2^i+2^j}, \quad \lambda_{ij} \in \mathrm{GF}(2^n). \tag{4.1}$$

When $G = C$, Lemma 4.1 can be improved to show $M \cap B = S_+$. We need the following result, proof of which is an easy adaption of that of [5, Theorem 3.2] to the case $p = 2$. Proposition 4.2 has been rediscovered by other authors, for example [13].

PROPOSITION 4.2 (see [5]). *Let $G \cong \mathbb{Z}_2^n$, let $f \in C^1(G, G)$ have linearized summand ℓ and set $\phi = f - \ell$. Then $\partial\phi = \partial f \in M \cap B$ if and only if ϕ is DO, if and only if f is quadratic. That is, $M \cap B = \{\partial f \mid f = \phi + \ell, \phi$ DO, ℓ linearized$\}$.*

Every DO polynomial is the image under the diagonal mapping of at least one cocycle. For the DO polynomial ϕ in (4.1), define

$$\varphi(x, y) = \sum_{j=1}^{n-1} \sum_{i=0}^{j-1} \lambda_{ij}\, x^{2^i} y^{2^j}, \tag{4.2}$$

which is multiplicative by Theorem 2.6. Then $D\varphi = \phi$ and so $\partial\phi = \varphi^+$.

COROLLARY 4.3. *Let $G \cong \mathbb{Z}_2^n$, let ϕ be a DO polynomial (4.1) and let φ be the corresponding cocycle (4.2). Then:*

(i) $\partial\phi = \varphi^+ = \partial \circ D(\varphi)$;

(ii) $M \cap B = S_+ = (\partial \circ D)(Z)$.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

We distinguish between the basis coboundaries c_k with $w_2(k) = 2$ and those with $w_2(k) \geq 3$, since it is plain from (4.2) and Corollary 4.3 that the c_k with $w_2(k) = 2$ form a basis for S_+.

COROLLARY 4.4. *For $n > 1$, define*

$$b_{ij}(x, y) = c_{2^i+2^j}(x, y) = x^{2^i} y^{2^j} + x^{2^j} y^{2^i}, \quad x, y \in \mathrm{GF}(2^n), 0 \leq i < j \leq n-1.$$

Then $S_+ = \mathrm{span}\{b_{ij},\ 0 \leq i < j \leq n-1\}$ *and* $B = S_+ \oplus C$, *where* C is the span of $\{c_k, k = 2, \ldots, 2^n - 1, w_2(k) \geq 3\}$.

In Theorem 3.1 we proved the $\mathrm{GF}(2^n)$-subspace B of coboundaries has dimension $2^n - n - 1$. By Proposition 2.1, Z has $\mathrm{GF}(2^n)$-dimension $N = 2^n + \binom{n}{2} - 1$, so we need only to identify a further $n + \binom{n}{2}$ basis cocycles which are not coboundaries. We make the surprising and valuable observation that these may all be chosen to be multiplicative. This observation is not apparent from the theory described above. The multiplicative cocycles have already been identified in Theorem 2.6. If $i < j$, then

$$\begin{aligned}\lambda_{ij} x^{2^i} y^{2^j} + \lambda_{ji} x^{2^j} y^{2^i} &= (\lambda_{ji} + \lambda_{ij}) x^{2^j} y^{2^i} + \lambda_{ij}(x^{2^i} y^{2^j} + x^{2^j} y^{2^i}) \\ &= (\lambda_{ji} + \lambda_{ij}) x^{2^i} y^{2^j} + \lambda_{ji}(x^{2^i} y^{2^j} + x^{2^j} y^{2^i})\end{aligned}$$

and in either form the second summand is a multiple of the symmetrization coboundary $b_{ij}(x, y)$. We have two possible representations of $\lambda_{ij} x^{2^i} y^{2^j} + \lambda_{ji} x^{2^j} y^{2^i}$ here, and without loss of generality we choose the former.

Hence $\dim(M) = n^2 = n + 2\binom{n}{2}$ and in M there are n linearly independent multiplicative symmetric cocycles we denote by

$$d_i(x, y) = x^{2^i} y^{2^i}, \quad 0 \leq i \leq n-1,$$

and $\binom{n}{2}$ linearly independent multiplicative asymmetric cocycles we denote by

$$a_{ji}(x, y) = x^{2^j} y^{2^i}, \quad 0 \leq i < j \leq n-1$$

as well as the $\binom{n}{2}$ linearly independent symmetrization coboundaries $b_{ij}(x, y)$, $0 \leq i < j \leq n-1$ already found as a basis for S_+.

THEOREM 4.5 (Basis theorem). *A $\mathrm{GF}(2^n)$-basis for $Z^2(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$, $n > 1$, consists of the following $N = 2^n + \binom{n}{2} - 1$ polynomials:*

(1) *n multiplicative symmetric noncoboundary cocycles d_i, $i = 0, \ldots, n-1$;*
(2) *$\binom{n}{2}$ multiplicative asymmetric noncoboundary cocycles a_{ji}, $0 \leq i < j \leq n-1$;*
(3) *$\binom{n}{2}$ multiplicative symmetrization coboundaries b_{ij}, $0 \leq i < j \leq n-1$;*
(4) *$2^n - \binom{n}{2} - n - 1$ nonmultiplicative symmetric coboundaries c_k, $2 \leq k \leq 2^n - 1$, $w_2(k) \geq 3$.*

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

COROLLARY 4.6. *Define* $A = \mathrm{span}\{a_{ji}, 0 \le i < j \le n-1\}$ *and* $D = \mathrm{span}\{d_i, i = 0, \ldots, n-1\}$. *Then* $\dim(A) = \binom{n}{2}$, $\dim(B) = 2^n - n - 1$, $\dim(C) = 2^n - \binom{n}{2} - n - 1$, $\dim(D) = n$, $\dim(M) = n^2$, $\dim(S) = 2^n - 1$, $\dim(S_+) = \binom{n}{2}$ *and* $\dim(Z) = 2^n + \binom{n}{2} - 1$. *Furthermore:*

(1) $Z = A \oplus D \oplus S_+ \oplus C = M \oplus C = A \oplus S$;
(2) $S = D \oplus S_+ \oplus C$;
(3) $M = A \oplus D \oplus S_+$;
(4) $B = S_+ \oplus C$.

Theorems 3.4, 4.5 and Corollary 4.6 provide us with a new and effective approach to working with cocycles over $\mathbb{Z}_2^n$. Known algorithms for finding a generating set of cocycles require costly precomputation of representative cocycles in each cohomology class, and for a generating set of coboundaries to be found using linear algebra, on a case-by-case basis. There are iterative techniques for finding the cohomology class representatives as n increments, but no simple recursive formula for coboundaries, such as we have given in Theorem 3.4.

We illustrate the transformation from the basis found by another algorithm to this basis with a small example.

EXAMPLE 2. If $n = 2$, $Z \cong (\mathbb{Z}_2^2)^4$. Using [8, Algorithm 1, 6.3.1], each cocycle ψ is uniquely defined by the four values $\psi(1, 1) = \alpha$, $\psi(\omega, \omega) = \beta$, $\psi(1, \omega) = \gamma$ and $\psi(1, \omega) + \psi(\omega, 1) = \kappa$, where ω is a primitive element of GF(4). These values can be used to identify four basis cocycles. By Theorem 4.5, there are four basis polynomials $d_0(x, y) = xy$, $d_1(x, y) = x^2y^2$, $a_{10}(x, y) = x^2y$ and $b_{01}(x, y) = xy^2 + x^2y$. Suppose that $\psi = \lambda_1 d_0 + \lambda_2 d_1 + \lambda_3 a_{10} + \lambda_4 b_{01}$. Then the transform matrix is given by

$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix} = \begin{bmatrix} \omega & 1 & \omega^2 & 0 \\ \omega^2 & 1 & \omega & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & \omega & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \kappa \\ \gamma \end{bmatrix}.$$

As a consequence of the basis theorem, every cocycle from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ has a unique decomposition as a direct sum of a coboundary and a multiplicative cocycle of restricted type, a fact which we do not believe has been previously observed.

COROLLARY 4.7. *Since* $Z = (A \oplus D) \oplus B$, *every cocycle* $\psi \in Z$ *has a unique decomposition as a direct sum of the form* $\psi = \mu \oplus \partial\phi$ *where* $\mu \in A \oplus D$ *is multiplicative and* $\partial\phi$ *is a coboundary.*

The known but previously unusable unique decomposition $\psi = \psi^\top + \psi^-$, where ψ^- is the commutator pairing, is now revealed as the decomposition $Z = (A \oplus D \oplus C) \oplus S_+$, since $\psi^- = \psi^+ = S^+(\psi)$.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

We expect that the basis theorem and Corollary 4.7 will prove very useful in the search for orthogonal and other cocycles with low differential uniformity in $Z^2(\mathbb{Z}_2^n, \mathbb{Z}_2^m)$, $m \leq n$, for applications in coding and cryptography. For instance, it is conjectured in [14] that all orthogonal cocycles in $Z^2(\mathbb{Z}_2^n, \mathbb{Z}_2^m)$, $n \geq m \geq 2$ are multiplicative, based on computed results for $n \leq 4$. The decomposition above may be the clue to discovering if this is true for all n when $p = 2$. (It cannot be true for odd p [5].)

Acknowledgements

This work forms part of the PhD thesis of the first author, taken under the supervision of the second author.

References

[1] Lynn M. Batten, Robert S. Coulter and Marie Henderson, 'Extending abelian groups to rings', *J. Aust. Math. Soc.* **82** (2007), 297–313.

[2] Kenneth S. Brown, *Cohomology of Groups*, Geometry and Topology Monographs, 87 (Springer, New York, 1982).

[3] Lilya Budaghyan, Claude Carlet and Alexander Pott, 'New classes of almost bent and almost perfect nonlinear polynomials', *IEEE Trans. Inform. Theory* **52** (2006), 1141–1152.

[4] Anne Canteaut, 'Cryptographic functions and design criteria for block ciphers', in: *INDOCRYPT 2001*, Lecture Notes in Computer Science, 2247 (eds. C. Pandu Rangan and C. Ding) (Springer, Berlin, 2001), pp. 1–16.

[5] Robert S. Coulter and Rex W. Matthews, 'Planar functions and planes of Lenz–Barlotti Class II', *Des. Codes Cryptogr.* **10** (1997), 167–184.

[6] N. J. Fine, 'Binomial coefficients modulo a prime', *Amer. Math. Monthly* **54** (1947), 589–592.

[7] D. L. Flannery and E. A. O'Brien, 'Computing 2-cocycles for central extensions and relative difference sets', *Comm. Algebra* **28** (2000), 1939–1955.

[8] K. J. Horadam, *Hadamard Matrices and Their Applications* (Princeton University Press, Princeton, NJ, 2006).

[9] K. J. Horadam and D. G. Farmer, 'Bundles, presemifields and nonlinear functions', *Des. Codes Cryptogr.* **48** (2008), 79–94.

[10] Kathy J. Horadam and Parampalli Udaya, 'Cocyclic Hadamard codes', *IEEE Trans. Inform. Theory* **46** (2000), 1545–1550.

[11] ———, 'A new construction of central relative $(p^a, p^a, p^a, 1)$-difference sets', *Des. Codes Cryptogr.* **27** (2002), 281–295.

[12] ———, 'A new class of ternary cocyclic Hadamard codes', *Appl. Algebra Engrg. Comm. Comput.* **14** (2003), 65–73.

[13] Gohar M. Kyureghyan, 'Crooked maps in $\mathbb{F}_{2^n}$', *Finite Field Appl.* **13** (2007), 713–726.

[14] Alain LeBel, 'Shift actions on 2-cocycles', PhD Thesis, RMIT University, Melbourne, Australia, 2005.

[15] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, 2nd edn (Cambridge University Press, Cambridge, 1997).

[16] Édouard Lucas, *Théorie des Nombres, Tome premier* (Gauthier-Villars, Paris, 1891), pp. 417–420 (Reprinted by Albert Blanchard, 1961).

[17] Stephen Wolfram, 'Geometry of binomial coefficients', *Amer. Math. Monthly* **91** (1984), 566–571.

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press

D. G. FARMER, RMIT University, Melbourne, VIC 3001, Australia
e-mail: David.Farmer@ems.rmit.edu.au

K. J. HORADAM, RMIT University, Melbourne, VIC 3001, Australia
e-mail: Kathy.Horadam@rmit.edu.au

https://doi.org/10.1017/S1446788708000876 Published online by Cambridge University Press