

A random Bockstein operator

Matthew Zabka

Communicated by V. Lyubashenko

ABSTRACT. As more of topology’s tools become popular in analyzing high-dimensional data sets, the goal of understanding the underlying probabilistic properties of these tools becomes even more important. While much attention has been given to understanding the probabilistic properties of methods that use homological groups in topological data analysis, the probabilistic properties of methods that employ cohomology operations remain unstudied. In this paper, we investigate the Bockstein operator with randomness in a strictly algebraic setting.

1. Introduction

Using the tools of algebraic topology to better understand a data set is a relatively new idea with many applications. For example, Carlsson’s survey [1] reviews the generalization of cluster analysis to persistent homology, a technique that provides more information on the shape of a data set than traditional cluster analysis. Other authors, such as Kahle in [3], have investigated the topology of a random simplicial complex.

Both of these approaches have only considered Betti numbers, i.e., the ranks of cohomology groups. A natural question that arises is whether one can gather any additional information from a data set by looking at operations on the topological structure generated by that data set. That is, how can we expand the idea of randomness to cohomology operations? The Bockstein homomorphism is a well-known example of a cohomology

2010 MSC: 08, 55.

Key words and phrases: random cohomology operations, topological data analysis, Bockstein operation.

operator, and in this paper, we shall attempt to investigate this cohomology operator with randomness.

Cohomology operators are a topological invariants that can reveal additional structure not seen in cohomological groups. For example, the cohomology groups of for $S^1 \vee S^2$ and $\mathbb{R}P^2$ are the same, but they are not homotopy equivalent spaces. To see this, one can compute the Bockstein homomorphism of both $S^1 \vee S^2$, which is trivial, and of $\mathbb{R}P^2$, which is non-trivial.

In general, the Bockstein homomorphism is a connecting homomorphism of cohomology groups defined on a chain complex. Ideally, we should consider the case of a chain complex of a randomly generated topological space. Unfortunately, this problem is very difficult. The length of the chain complex, each Abelian group in the complex, and each boundary map would all add complexity to this model. We shall therefore examine in this paper a simpler algebraic version of the above problem whose only degrees of freedom are determined by a single boundary map.

Let V and W be free-modules with coefficients in \mathbb{Z}/p^2 . We have then have the following short exact sequences

$$0 \rightarrow pV \hookrightarrow V \rightarrow \bar{V} \rightarrow 0 \quad \text{and} \quad 0 \rightarrow pW \hookrightarrow W \rightarrow \bar{W} \rightarrow 0,$$

where \bar{V} and \bar{W} are the reductions of V and $W \pmod{p}$. Given a map $\phi : V \rightarrow W$, which is the boundary map we describe in the paragraph above, define ψ from \bar{V} to \bar{W} to be the map induced by ϕ . The Bockstein homomorphism induced by ϕ is then a map from $\ker \psi$ to $\text{coker } \psi$. We give construction of the Bockstein homomorphism for this case in more detail in Section 4.

Since Bockstein homomorphisms are elements of $\text{hom}(\ker \psi, \text{coker } \psi)$, it makes sense only to compare Bocksteins induced by functions from V to W that are equal modulo p . If V has dimension n and W has dimension m , then a choice of random function from V to W is the same as choosing a random m by n matrix. To this end, let ϕ be a random matrix whose entries are chosen i.i.d. randomly from the discrete uniform distribution on $\{0, 1, 2, \dots, p^2 - 1\}$. Let $\bar{\phi}$ be the reduction of ϕ modulo p . Let ψ be an m by n matrix with entries in $\{0, 1, 2, \dots, p - 1\}$. Let β_ϕ be the Bockstein homomorphism induced by ϕ . Let β be in $\text{hom}(\ker \psi, \text{coker } \psi)$. We shall show that

$$\mathbb{P}(\beta_\phi = \beta | \bar{\phi} = \psi) = \frac{1}{p^{k(m-n+k)}}.$$

In other words, we shall show that, conditioned on $\bar{\phi} = \psi$, the Bockstein homomorphisms are distributed uniformly.

2. Linear algebra over \mathbb{Z}/p^2

Many of our calculations will be done over \mathbb{Z}/p^2 -modules. This section reviews the theory of \mathbb{Z}/p^2 -modules over \mathbb{Z}/p^2 . Some of the techniques used in this section work for modules over rings other than \mathbb{Z}/p^2 , but we shall not explore these ideas here.

Let R be a ring. Given an R -module M , we say that a subset E of M is a basis for M whenever E generates M and E is linearly independent. This definition is equivalent to the condition that every x in M can be written as a unique linear combination of elements of E with scalars in R . A module that has a basis is called a free module.

Let p be prime, and let V and W be free \mathbb{Z}/p^2 -modules. Define

$$\bar{V} := V \bigotimes_{\mathbb{Z}/p^2} \mathbb{Z}/p \quad \text{and} \quad \bar{W} := W \bigotimes_{\mathbb{Z}/p^2} \mathbb{Z}/p.$$

So $\bar{V} = V/pV$ and $\bar{W} = W/pW$ are the reductions of V and $W \pmod{p}$. Note that these are \mathbb{Z}/p vector spaces. For an element $x \in V$, we use \bar{x} to denote its reduction modulo p . For an element y in \bar{V} , we use \tilde{y} to denote a choice of representative in V of y , so that $\bar{\tilde{y}} = y$. Given a \mathbb{Z}/p^2 -linear map $\phi : V \rightarrow W$, let $\bar{\phi}$ denote the induced function from \bar{V} to \bar{W} .

Lemma 2.1. Let V be a free \mathbb{Z}/p^2 -module. Let $p : V \rightarrow V$ be multiplication by p . Then the kernel of p is equal to the image of p .

Proof. Let $\{e_i\}$ be a basis for V . Let x be in $\ker p$. Since $\{e_i\}$ is a basis, there are α_i in \mathbb{Z}/p^2 such that $x = \sum_i \alpha_i e_i$. Since x is in $\ker p$ we have $px = \sum_i p\alpha_i \cdot e_i = 0$. By the independence of the e_i , we have $p\alpha_i = 0$ for each i . Thus $\alpha_i = p\beta_i$ for some $\beta_i \in \mathbb{Z}/p^2$. Then $p(\sum_i \beta_i e_i) = \sum_i \alpha_i e_i = x$. So that x is in the image of p .

Next, assume that y is in the image of p . Then there exists a $z \in V$ with $pz = y$. So $py = p^2z = 0$. So y is in the kernel of p . \square

We know that pV and \bar{V} are isomorphic as \mathbb{Z}/p -vector spaces, because they both have the same dimension. The following lemma gives an explicit isomorphism between these two spaces.

Lemma 2.2. The map $f : pV \rightarrow \bar{V}$ defined by $px \mapsto \bar{x}$ is a \mathbb{Z}/p -linear isomorphism.

Proof. We show that both f and its inverse mapping g , which maps \bar{x} in \bar{V} to px in pV , are well-defined. To show that f is well-defined, assume

that $px = py$ for some x and y in V . Then $px - py = p(x - y) = 0$. So $x - y = pz$ for some $z \in V$ by Lemma 2.1. Note that

$$\bar{x} - \bar{y} = \overline{x - y} = p\bar{z} = \bar{0},$$

so that f is well-defined.

For the inverse mapping g , suppose $\bar{x} = \bar{y}$. Then $\overline{x - y} = \bar{0}$. So by Lemma 2.1, $x - y = pz$ for some $z \in V$. We have

$$px - py = p(x - y) = p^2z = 0.$$

So g is well-defined. By inspection we see that both f and g are \mathbb{Z}/p -linear functions, and so the proof is complete. \square

The main proposition of this section shows that any lift of a basis of \bar{V} is a basis of V . Such bases will be useful for constructing linear maps out of V . That is, if one defines a map on any basis of V , then this map extends linearly to all of V .

Proposition 2.3. Let $\{e_i\}$ be a basis for \bar{V} . For each e_i , let \tilde{e}_i in V be any lift of e_i . Then $\{\tilde{e}_i\}$ is a basis for V .

Proof. We first show that the set $\{\tilde{e}_i\}$ is linearly independent. Suppose $\alpha_i \in \mathbb{Z}/p^2$ with

$$\sum_i \alpha_i \tilde{e}_i = 0. \tag{1}$$

Projecting to \bar{V} we obtain $\sum_i \bar{\alpha}_i e_i = \bar{0}$. Since $\{e_i\}$ is a basis for \bar{V} , we must have that $\bar{\alpha}_i = \bar{0}$ for every i . So each $\alpha_i = p\beta_i$ for some β_i in \mathbb{Z}/p^2 . Thus, (1) gives that $\sum_i \beta_i \cdot p\tilde{e}_i = 0$ in pV . Under the isomorphism given in Lemma 2.2, we have $\sum_i \beta_i \bar{e}_i = \bar{0}$ in \bar{V} . Since the set $\{e_i\}$ is linearly independent, each $\bar{\beta}_i = \bar{0}$, so each $\beta_i = p\gamma_i$ for some γ_i in \mathbb{Z}/p^2 . This gives that each $\alpha_i = p\beta_i = p^2\gamma_i = 0$. So the set $\{\tilde{e}_i\}$ is linearly independent.

We next show that $\{\tilde{e}_i\}$ spans V . Let $x \in V$. Since the set $\{e_i\}$ is a basis for \bar{V} , there are $\alpha_i \in \mathbb{Z}/p^2$ such that $\sum_i \bar{\alpha}_i e_i = \bar{x}$. So for some $y \in V$,

$$x = py + \sum_i \alpha_i \tilde{e}_i. \tag{2}$$

Under the isomorphism given in Lemma 2.2, the element py in pV is mapped to \bar{y} in \bar{V} . Since the e_i form a basis for \bar{V} , there exist β_i in

\mathbb{Z}/p^2 such that $\sum_i \bar{\beta}_i e_i = \bar{y}$. Thus $pz + \sum_i \beta_i \tilde{e}_i = y$ for some $z \in V$. Substituting this into (2) gives

$$x = p \left(pz + \sum_i \beta_i \tilde{e}_i \right) + \sum_i \alpha_i \tilde{e}_i.$$

Simplifying gives $x = \sum_i (\alpha_i - p\beta_i) \tilde{e}_i$, so that x is in the span of $\{\tilde{e}_i\}$, as desired. \square

For the map ψ with domain \bar{V} and target \bar{W} , recall that $\text{coker } \psi$ is defined as the quotient $\bar{W}/\psi(\bar{V})$. Our next lemma shows that we may regard the Bockstein homomorphism as a map $\beta : \ker \psi \rightarrow \text{coker } \psi$. The techniques used in the proof are similar to the techniques used in Lemma 2.2.

Lemma 2.4. The map f from $pW/\phi(pV)$ to $\text{coker } \psi$ defined by

$$f : pw + \phi(pV) \rightarrow \bar{w} + \psi(\bar{V})$$

is an isomorphism.

Proof. We must show that f and its inverse mapping g are well-defined.

To show that f is well-defined, suppose $pw + \phi(pV) = pw' + \phi(pV)$ in $pW/\phi(pV)$. We must show that $\bar{w} - \bar{w}'$ is in $\psi(\bar{V})$. We have that $p(w - w') \in \phi(pV)$. Thus $p(w - w') = p\phi(v)$ for some $v \in V$. By Lemma 2.1, we have $w - w' - \phi(v) = py$. Thus $\bar{w} - \bar{w}' = \overline{\phi(v)} = \psi(\bar{v})$. So $\bar{w} - \bar{w}'$ is in $\psi(\bar{V})$, and this shows that f is well-defined.

We next want to show that the inverse mapping g is well-defined. Suppose that $\bar{w} + \psi(\bar{V}) = \bar{w}' + \psi(\bar{V})$. We must show that $pw + \phi(pV) = pw' + \phi(pV)$. Since $\bar{w} - \bar{w}' + \overline{\phi(\bar{V})} = \bar{0} + \overline{\phi(\bar{V})}$, there exists a $\bar{v} \in \bar{V}$ with $\bar{w} - \bar{w}' = \overline{\phi(\bar{v})}$. Thus $w - w' - \phi(v) = px$ for some x , which, by Lemma 2.1 gives $p[w - w' - p\phi(v)] = 0$. So $pw + \phi(pV) = pw' + \phi(pV)$. By inspection, f and g are both linear, and the proof is complete. \square

3. Spaces of linear maps

We should like to further investigate the connection between a map $\psi : \bar{V} \rightarrow \bar{W}$ and the Bockstein homomorphisms induced by a map $\phi : V \rightarrow W$ such that $\bar{\phi} = \psi$. For this section, we shall treat ψ as a fixed \mathbb{Z}/p -linear map from \bar{V} to \bar{W} .

Definition 3.1. Let V and W be \mathbb{Z}/p^2 -modules. Let \overline{V} and \overline{W} be the reductions of V and W modulo p . Let ψ be a fixed \mathbb{Z}/p -linear map from \overline{V} to \overline{W} . Define L_ψ to be the collection of all maps from V to W whose reduction modulo p is ψ .

It will also be useful in this section to choose a basis for \overline{V} , which, by Proposition 2.3 will lift to a basis for V .

Definition 3.2. Let V , \overline{V} , and ψ be as in Definition 3.1. Let $\{e_i\} \cup \{f_j\}$ be a basis for \overline{V} such that $\{e_i\}$ is a basis for the subspace $\ker \psi$ of \overline{V} . For each i , let \tilde{e}_i in V be a lift of e_i . For each j let \tilde{f}_j in V be a lift of f_j .

By Proposition 2.3, $\{\tilde{e}_i\} \cup \{\tilde{f}_j\}$ is a basis for V . If the map $\psi : \overline{V} \rightarrow \overline{W}$ is not the zero map, then we know that L_ψ is not a vector space, for in this case, 0 is not in L_ψ . This fact, along with the next lemma, gives that L_ψ is a vector space if and only if ψ is the zero map.

Lemma 3.3. The space L_0 with pointwise addition and \mathbb{Z}/p scalar multiplication defined by

$$\overline{\alpha} \cdot \phi := \alpha \cdot \phi,$$

where α is in \mathbb{Z}/p^2 and ϕ is in L_0 , is a \mathbb{Z}/p -vector space. In particular, if V has dimension n and W has dimension m , then L_0 is a \mathbb{Z}/p -vector space of dimension $m \cdot n$.

Proof. We shall only show that this scalar multiplication is well-defined, as the other parts of the proof are straightforward. Let α_1 and α_2 be in \mathbb{Z}/p^2 with $\overline{\alpha_1} = \overline{\alpha_2}$. Let ϕ be in L_0 and let $v \in V$. Then $\alpha_1 - \alpha_2 = p\beta$ for some β in \mathbb{Z}/p^2 and $\phi(v) = pw$ for some w in W , because $\overline{\phi} = 0$. So we have

$$\begin{aligned} \overline{\alpha_1} \cdot \phi(v) - \overline{\alpha_2} \cdot \phi(v) &= \alpha_1 \phi(v) - \alpha_2 \phi(v) \\ &= (\alpha_1 - \alpha_2) \phi(v) \\ &= (p\beta)(pw) \\ &= p^2 \beta w \\ &= 0, \end{aligned}$$

which shows that this scalar multiplication in \mathbb{Z}/p^2 is well-defined. \square

Let ϕ_0 be any element of L_ψ . Then $\phi_0 + L_0 = L_\psi$, so we may regard L_ψ as a coset of L_0 . It will be useful however to choose a particular $\phi_0 \in L_\psi$ whenever we wish to regard L_ψ as a coset of L_0 . For this, we need only define ϕ_0 on the basis $\{\tilde{e}_i\} \cup \{\tilde{f}_j\}$ given in Definition 3.2.

Remark 3.4. When we regard L_ψ as a coset of L_0 , we shall choose ϕ_0 such that, for all i , $\phi_0(\tilde{e}_i) = 0$, and for all j , $\phi_0(\tilde{f}_j)$ is any value whose reduction modulo p is $\psi(f_j)$.

We are now ready to count the number of elements in L_ψ .

Lemma 3.5. For any $\psi : \bar{V} \rightarrow \bar{W}$, the set L_ψ has p^{mn} elements.

Proof. Lemma 3.3 tells us that L_0 is a \mathbb{Z}/p -vector space, but by definition, L_0 also is a \mathbb{Z}/p^2 -submodule of $\text{Hom}(V, W)$. When we regard L_ψ as $\phi_0 + L_\psi$, where ϕ_0 is as defined in Remark 3.4, this addition occurs in a \mathbb{Z}/p^2 -submodule. So, while L_ψ is not a translate of L_0 as a \mathbb{Z}/p -vector space, we still know that L_ψ has the same number of elements as L_0 . This information, along with Lemma 3.3, completes the proof. \square

4. The Bockstein homomorphism

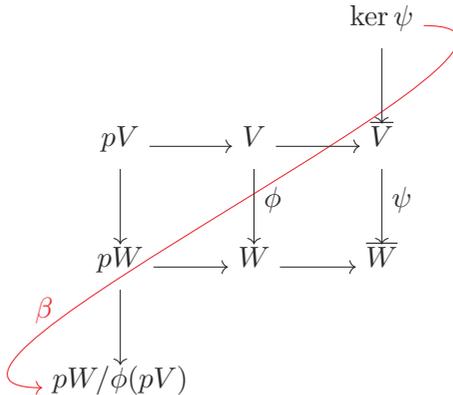
What follows is a short review of the Bockstein homomorphism in the context that is relevant for our study of cohomology operations with randomness. Several references cover the Bockstein homomorphism and cohomology operations in more generality. See, for example, [4].

As in Section 2, let V and W be \mathbb{Z}/p^2 free-modules with coefficients in \mathbb{Z}/p^2 . We have the following short exact sequences:

$$0 \rightarrow pV \hookrightarrow V \rightarrow \bar{V} \rightarrow 0 \quad \text{and} \quad 0 \rightarrow pW \hookrightarrow W \rightarrow \bar{W} \rightarrow 0,$$

where \bar{V} and \bar{W} are the reductions of V and $W \pmod p$.

Consider a \mathbb{Z}/p^2 -linear map ϕ from V to W . Let ψ be the map from \bar{V} to \bar{W} induced by ϕ . Then the Snake Lemma [5] defines a map β with domain $\ker \psi$ and target $pW/\phi(pV)$. The following diagram illustrates the Snake Lemma.



More precisely, for $\bar{v} \in \ker \psi$, choose any representative $v \in V$ of \bar{v} . Since the squares in the above diagram commute, we have $\overline{\phi(v)} = \psi(\bar{v}) = \bar{0}$. So $\phi(v) = pw$ for some $w \in W$. Define the Bockstein homomorphism β from $\ker \psi$ to $pW/\phi(pV)$ by

$$\beta(\bar{v}) := pw + \phi(pV).$$

The following diagram shows the process described above.

$$\begin{array}{ccc} & v & \longrightarrow \bar{v} \\ & \downarrow \phi & \\ pw & \longrightarrow & pw = \phi(v) \\ \downarrow & & \\ pw + \phi(pV) & & \end{array}$$

By construction, the target of β is $pW/\phi(pV)$. However, by Lemma 2.4, we know that $pW/\phi(pV)$ is isomorphic to $\text{coker } \psi$. So henceforth we shall regard β as a map into $\text{coker } \psi$.

Remark 4.1. We note here that if one regards an arbitrary chain complex, the map β is often called a connecting homomorphism. When the chain complex is generated by a topological space, the map β is called the Bockstein homomorphism. If we regard ϕ as the map between V and W in the following chain complex

$$\dots \longrightarrow 0 \longrightarrow V \xrightarrow{\phi} W \longrightarrow 0 \longrightarrow \dots,$$

and consider the reduced chain complex

$$\dots \longrightarrow 0 \longrightarrow \bar{V} \xrightarrow{\psi} \bar{W} \longrightarrow 0 \longrightarrow \dots,$$

then the only possible non-trivial homology groups of this chain complex are $\ker \psi$ and $\text{coker } \psi$. Although we are in a strictly algebraic setting, we shall continue to refer to the map β as the Bockstein homomorphism between $\ker \psi$ and $\text{coker } \psi$.

Remark 4.2. The Bockstein homomorphism is often constructed in the case where V and W are \mathbb{Z} -modules. In this case, first reduce V and W to \mathbb{Z}/p^2 modules, and then apply the above construction.

In this section we have described how to every $\phi \in L_\psi$, there is a unique Bockstein homomorphism $\beta_\phi : \ker \psi \rightarrow \text{coker } \psi$. This fact defines the following map.

Definition 4.3. Define Γ to be the map from L_ψ to $\text{Hom}(\ker \psi, \text{coker } \psi)$ that sends ϕ in L_ψ to the unique Bockstein homomorphism β_ϕ , which is in $\text{Hom}(\ker \psi, \text{coker } \psi)$, that is given by ϕ .

Composing Γ with addition by ϕ_0 gives a well defined set map B with domain L_0 and target $\text{Hom}(\ker \psi, \text{coker } \psi)$. This is shown in the following diagram.

$$L_0 \xrightarrow{+\phi_0} L_\psi \xrightarrow{\Gamma} \text{Hom}(\ker \psi, \text{coker } \psi)$$

We should like to examine the properties of this map. The map from L_0 to L_ψ given by adding ϕ_0 is a bijection. The next lemma shows that the map Γ is onto, which shows that B is also onto. In particular, every \mathbb{Z}/p linear map from the kernel of ψ to the cokernel of ψ is the Bockstein homomorphism of some $\phi : V \rightarrow W$ that induces ψ .

Lemma 4.4. The map Γ from L_ψ to $\text{Hom}(\ker \psi, \text{coker } \psi)$ is onto.

Proof. Let $\beta \in \text{Hom}(\ker \psi, \text{coker } \psi)$. Let $\{e_i\} \cup \{f_j\}$ and $\{\tilde{e}_i\} \cup \{\tilde{f}_j\}$ be bases of \overline{V} and V as defined in Definition 3.2. We shall define ϕ on the basis for V and then extend linearly to define ϕ on all of V . We must show that the Bockstein homomorphism β_ϕ of ϕ is equal to β .

For each i , we know that e_i is in the domain of β . So $\beta(e_i) = \overline{w_i} + \psi(\overline{V})$ for some w_i in W . Define $\phi(\tilde{e}_i) = pw_i$. Define $\phi(\tilde{f}_j)$ to be any value in W whose reduction modulo p is $\psi(f_j)$. Then $\overline{\phi(e_i)} = \overline{pw_i} = 0 = \psi(e_i)$ and $\overline{\phi(\tilde{f}_j)} = \psi(f_j)$. This shows that $\overline{\phi} = \psi$. In particular ϕ is in L_ψ .

By construction, $\beta_\phi(e_i) = \overline{w_i} + \psi(\overline{V}) = \beta(e_i)$. Since β_ϕ is equal to β on the basis of $\ker \psi$, they are equal as \mathbb{Z}/p -linear functions. □

Lemma 4.5. The map B is a \mathbb{Z}/p -linear map.

Proof. Let ϕ and ϕ' be in L_0 . We must show that $\Gamma(\phi + \phi' + \phi_0) = \Gamma(\phi + \phi_0) + \Gamma(\phi' + \phi_0)$, for $\phi_0 \in L_\psi$ as described in Remark 3.4. For a basis $\{e_i\}$ of $\ker \psi$, it suffices to show that

$$\Gamma(\phi + \phi' + \phi_0)(e_i) = \Gamma(\phi + \phi_0)(e_i) + \Gamma(\phi' + \phi_0)(e_i)$$

Let \tilde{e}_i be any lift of e_i . Then $\phi_0(\tilde{e}_i) = 0$ by construction. Also,

$$\overline{(\phi + \phi')(\tilde{e}_i)} = \overline{\phi(\tilde{e}_i)} + \overline{\phi'(\tilde{e}_i)} = 0, \quad (3)$$

and

$$\overline{\phi(\tilde{e}_i)} = \overline{\phi'(\tilde{e}_i)} = 0, \quad (4)$$

because ϕ and ϕ' are in L_0 . Thus there are w_i and w'_i in W with $\phi(\tilde{e}_i) = pw$ and $\phi'(\tilde{e}_i) = pw'$. Thus by (4) we know that

$$\begin{aligned} \Gamma(\phi + \phi_0)(e_i) + \Gamma(\phi' + \phi_0)(e_i) &= (\overline{w_i} + \psi(\overline{V})) + (\overline{w'_i} + \psi(\overline{V})) \\ &= \overline{w_i} + \overline{w'_i} + \psi(\overline{V}). \end{aligned}$$

Equations (3) and (4) together give that

$$\Gamma(\phi + \phi' + \phi_0)(e_i) = \overline{w_i} + \overline{w'_i} + \psi(\overline{V}).$$

So $\Gamma(\phi + \phi' + \phi_0)(e_i) = \Gamma(\phi + \phi_0)(e_i) + \Gamma(\phi' + \phi_0)(e_i)$, as desired. \square

5. Counting

Let V and W be \mathbb{Z}/p^2 -modules of dimensions n and m respectively. In Section 3 we defined L_ψ as the collection of all maps from V to W whose reduction modulo p is ψ . We then found that L_ψ has $p^{m \cdot n}$ elements. We should next like to answer the following question: Given a Bockstein homomorphism β , which is in $\text{hom}(\ker \psi, \text{coker } \psi)$, how many ϕ in L_ψ have β as their Bockstein homomorphisms? To answer this question, we shall first look at the size of $\Gamma^{-1}(\beta)$.

Lemma 5.1. Let $k := \dim(\ker \psi)$. Then the space $\Gamma^{-1}(\beta)$ has exactly $p^{(m+k)(n-k)}$ elements.

Proof. Since translation by the ϕ_0 given in Remark 3.4 is a bijection, we know that $B^{-1}(\beta)$ has the same size as $\Gamma^{-1}(\beta)$. Since B is a linear map, we also know that $B^{-1}(0)$ has the same size as $B^{-1}(\beta)$. Thus $\Gamma^{-1}(\beta)$ has the same size as $B^{-1}(0)$, so we shall find the size of $B^{-1}(0)$.

Since V and W have dimension n and m respectively, we know by Proposition 2.3 that \overline{V} and \overline{W} also have dimensions n and m respectively. Recall that $\text{coker } \psi$ is defined as $\overline{W}/\psi(\overline{V})$. Let $k := \dim(\ker(\psi))$. Since ψ is a \mathbb{Z}/p -linear map, by the Rank-Nullity Theorem, we have that $n = k + \dim(\psi(\overline{V}))$. So $\dim(\psi(\overline{V})) = n - k$. Thus $\dim(\text{coker}(\psi)) = m - (n - k)$. From this, we have that the number of elements in $B^{-1}(0)$ is

$$p^{mn-k(m-n+k)} = p^{(m+k)(n-k)}. \quad \square$$

We now come to our main result. Recall that a choice of random function from V to W is the same as choosing a random m by n matrix.

Theorem 5.2. Let ϕ be a random m by n matrix whose entries are chosen i.i.d. from the discrete uniform distribution on $\{0, 1, 2, \dots, p^2 - 1\}$. Let $\bar{\phi}$ be the reduction of ϕ modulo p . Let ψ be a matrix with entries in $\{0, 1, 2, \dots, p - 1\}$. Let β_ϕ be the Bockstein homomorphism defined by ϕ as in Definition 4.3. Note that β_ϕ is a random variable. Let β be in $\text{hom}(\ker \psi, \text{coker } \psi)$. Then

$$\mathbb{P}(\beta_\phi = \beta | \bar{\phi} = \psi) = \frac{1}{p^{k(m-n+k)}}.$$

Proof. We know from Remark 3.5 that L_ψ has p^{mn} elements. By Lemma 4.4, we know that Γ is onto, and by Lemma 5.1, we know that the size of $\text{hom}(\ker \psi, \text{coker } \psi)$ is $p^{mn-k(m-n+k)}$. \square

References

- [1] G. Carlsson, *Topology and data*, Bulletin of the American Mathematical Society, N.2, 2009, pp.255-308.
- [2] M. Kahle, *Topology of random clique complexes*, Discrete Mathematics, N.6, 2009, pp.1658-1671.
- [3] M. Kahle, *Random geometric complexes*, Discrete & Computational Geometry, N.3, 2011, pp.553-573.
- [4] Mosher, Robert E. and Tangora, Martin C., *Cohomology Operations and Applications in Homotopy Theory*, Dover, 2008.
- [5] Atiyah, Michael F. and Macdonald, Ian G., *Introduction to Commutative Algebra*, Addison-Wesley Reading, 1969.

CONTACT INFORMATION

Matthew Zabka

Dept of Mathematics and Computer Science,
SM 178, Southwest Minnesota State University,
1501 State Street, Marshall, MN 56258, USA
E-Mail(s): matthew.zabka@smsu.edu

Received by the editors: 25.05.2016
and in final form 24.06.2017.