NON-DETECTABLE PATTERNS HIDDEN WITHIN SEQUENCES OF BITS

DAVID ALLEN, JONATHAN HARDWICK, JOSÉ J. LA LUZ,
AND GUARIONEX SALIVIA

Abstract. In this paper we construct families of bit sequences using combinatorial methods. Each sequence is derived by converting a collection of numbers encoding certain combinatorial numerics from objects exhibiting symmetry in various dimensions. Using the algorithms first described in [1] we show that the NIST testing suite described in publication 800-22 does not detect these symmetries hidden within these sequences.

1. Introduction

In previous work [1] the authors took a random graph R_G and grew it using the cone (Definition 3.5) to construct families of higher dimensional objects called simplicial complexes. Each of these complexes comes equipped with a vector that encodes the number of i simplicies. One of the main thrusts of [1] was to show that the bit sequence derived from the *f-vector* of these higher dimensional objects was deemed "random" by the NIST testing suite [9]. In the current paper, we show that the NIST test suite fails to see patterns in bit sequences derived from combinatorial objects that are symmetrical in a certain sense (Definition 4.16).

Given a simplicial complex $\mathcal{K}$ it is possible to determine a related combinatorial object called a *simple convex polyhedron* whose faces are roughly built out of cones over the geometric realization of certain posets. In the case that $\mathcal{K}$ is nice, say a simplicial sphere, then the dual P is a *simple convex polytope*. Polyhedra have f-vectors and they encode the number of faces in a given dimension, but we are primarily concerned with those P that are dual to those "nice" $\mathcal{K}$. Exactly how this duality works is explained in §4. It is worth noting that determining these vectors and classifying the combinatorial type of P are difficult problems [7].

Simple convex polytopes are interesting and show up in various fields of mathematics. They are well behaved in certain ways and there are

Key words and phrases. Cryptography, Pseudo-random number generator.

other vectors associated to them called the h-vector and they exhibit a symmetry described by the Dehn-Sommerville relations. For such polytopes, these vectors also satisfy a collection of inequalities that are described by the well-known g-theorem [2, 3].

In this paper we focus on a particularly nice and well-understood family of simple convex polytopes; the standard n-simplex Δ^n, for some positive integer $n \geq 1$. The face structure is understood and the corresponding vectors mentioned above can be determined as well as their dual simplicial complexes (and their respective f-vectors). This group of polytopes is sufficient in demonstrating the claims of the paper. Namely, the bits derived from complexes built out of the duals of Δ^n are determined to be random by the NIST test suite.

More is true, indeed; if we let $\mathcal{K}$ be the dual of Δ^n, then we construct a family of simplicial complexes $C^j(\mathcal{K})$ and show that they are not dual to a simple convex polytope by applying the g-theorem.

2. Main Results

The contributions of this paper are:

(1) Construct a family of simplicial complexes that exhibit a symmetry not detected by the NIST test suite.
(2) Show that the family of simplicial complexes are not dual to simple polyhedra.

Before stating the main results we list the most pertinent definitions. Let $\mathcal{K}$ be an n-dimensional simplicial complex on the set $\{1, \ldots, n-1\}$, then the *cone* on $\mathcal{K}$ is as follows: $C(\mathcal{K}) = \{x \cup \{n\} | x \in \mathcal{K}\} \cup \mathcal{K}$. Let j be a positive integer, then when the cone is iterated j-times, we refer to it as the j^{th}-cone on $\mathcal{K}$ and write it as $C^j(\mathcal{K})$. The dimension of the complex increases as j increases.

To keep track of the number of i simplicies in $\mathcal{K}$ or $C^j(\mathcal{K})$ there is the *f-vector* and it is the vector with the number of i simplicies in the i^{th} component. We represent the i^{th} component of $\overrightarrow{f}(\mathcal{K})$ by $f_i(\mathcal{K})$. The vector is very often written $(f_0, ..., f_{n-1})$ where the last component counts the number of maximal dimensional simplicies in $\mathcal{K}$ (as written this vector encodes the number of i-simplicies in an $(n-1)$-dimensional simplicial complex). A simplicial complex $\mathcal{K}$ is *symmetrical* if $f_i(\mathcal{K}) = f_{n-i-1}(\mathcal{K})$ for $0 \leq i \leq n-1$. When the components of this vector are converted into bit sequences, the NIST test suite classifies these as random. The results of the testing can be found in the following github

public repository `https://github.com/gnexeng/coning-analysis.git`. This is a fork of the repository used in [1].

When $\mathcal{K}$ is a *simplicial sphere* (meaning its geometric realization is homeomorphic to a sphere), then there is a simple polytope P that is dual to $\mathcal{K}$ and vice-versa. We briefly recall the construction; the interested reader can refer to §4 where a more detailed description is given. The vertices of $\mathcal{K}$ correspond to the codimension one faces of P, the edges correspond to the codimension two faces of P so on and so forth. Given this, the polytope P will satisfy the criteria of the g-theorem which describes certain symmetry conditions and inequalities of a vector related to P called the h-vector as described by [3] and it is related to the vector whose components counts the number of faces of P [3]. Unfortunately, this too, is called the f-vector, but when $\mathcal{K}$ is dual to P then there is the following relation that relates the two noting that $(h_0, h_1, \ldots, h_n)$ is the h-vector of the dual: $h_0t^n + \cdots + h_{n-1}t + h_n = (t-1)^n + f_0(t-1)^{n-1} + \cdots + f_{n-1}$.

In [2] the g-theorem is stated in terms of certain "g_i" that satisfy a variety of inequalities and they too are related to the components f_i in the f-vector of P. If a general P does not satisfy the conditions of the g-theorem then it is not simple. If $\mathcal{K}$ is a random graph R_G, then there are equations that follow from the g-theorem that one can use to show that the simplicial complexes $C^j(R_G)$ are not simplcial spheres (meaning, the dual P is not simple) for j sufficiently large.

The main results are:

Proposition 2.1. For a graph G such that $f_1(G) \neq 0$, let $C^j(G) = \mathcal{K}^{j+1}$. For j sufficiently large, the complexes $\mathcal{K}^{j+1}$ are not dual to a polytope that satisfies the g-theorem.

Proposition 4.15 applies to the case $G = R_G$, a random graph. In fact, Theorem 4.15 provides us with exactly the number of cones that have to be applied before passing through the class of simple polytopes.

Theorem 2.2. *Let $n > 1$ and suppose P^n is a polytope such that $\overrightarrow{h}(P^n) = (1, \ldots, 1)$, then the $n-1$ dimensional dual simplicial complex K_P is symmetrical.*

From a testing perspective the main results are as follows:

(1) The components of the f-vectors dual to P in Theorem 4.17 can be found in Pascal's Triangle. The NIST test suite views the converted bit sequences as random. (see section §5 and §7

(2) There is a family of complexes given by the j^{th}-cone on those complexes constructed from Pascal's Triangle that generate bit sequences that NIST classifies as random.

The paper is set-up as follows. In §3 we provide a brief overview of simplicial complexes and the algorithms used to generate $C^j(\mathcal{K})$. We also discuss the notion of the f-vector and, for the convenience of the reader, list a few calculations made in [1]. In §4 polyhedra and their duals are discussed along with their f and h-vectors. The relation between the f and h-vectors is given as well as specific low dimensional examples. For completeness, the g-Theorem is listed and a reference is provided for additional details. The main theorems needed in the sequel are proved in this section too. §5 contains a careful analysis of bit conversions. Here, we discuss truncation methods that are used to ensure that the bit stream fits into the NIST suite. §6 lists the algorithm to convert f-vectors to h-vectors and vice versa and §7 contains a summary of the results. §8 is an Appendix and it contains additional commentary regarding the original code [1], the improvement that was made and how to replicate the new and improved results.

3. Simplicial Complexes and Iterated Cones

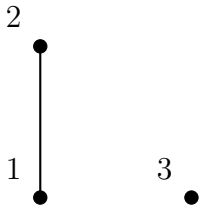
For the convenience of the reader we list background material from [1] along with a few other additions.

Definition 3.1. Let X be a non-empty set. A simplicial complex $\mathcal{K}$ on X is a non-empty subset of the power set of X such that if $x \in \mathcal{K}$ and $y \subset x$ then $y \in \mathcal{K}$.

In general $X = \{1, 2, \ldots, m\} = [m]$ where $m \in \mathbb{N}$. The sets in $\mathcal{K}$ are called simplices and the dimension of a simplex x, denoted $dim(x)$ is defined to be $|x| - 1$. The dimension of a simplicial complex is $max\{dim(x)|x \in \mathcal{K}\}$. If a simplicial complex $\mathcal{K}$ is $n-1$ dimensional we simply write $\mathcal{K}^{n-1}$. From the definition it follows that any simple graph can be regarded as a simplicial complex of dimension at most one. If such a graph has at least one edge, then it is a one dimensional.

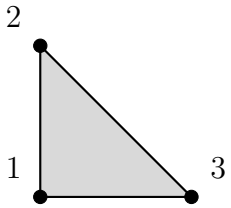
Remark 3.2. Notice that since $\mathcal{K}$ is a non-empty set and since $\emptyset \subseteq x$ for all subsets of X, then by definition $\emptyset \in \mathcal{K}$.

Example 3.3. The set $\mathcal{K} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}\}$ is a one-dimensional simplicial complex on the set $\{1, 2, 3\}$.



Notation 3.4. For a fixed $m \in \mathbb{N}$ let $\widehat{\Delta}^m = P([m])$ where $P([m])$ is the power set on $[m]$.

For instance, $\widehat{\Delta}^2$ is a *2-simplex*. Pictorially, it is

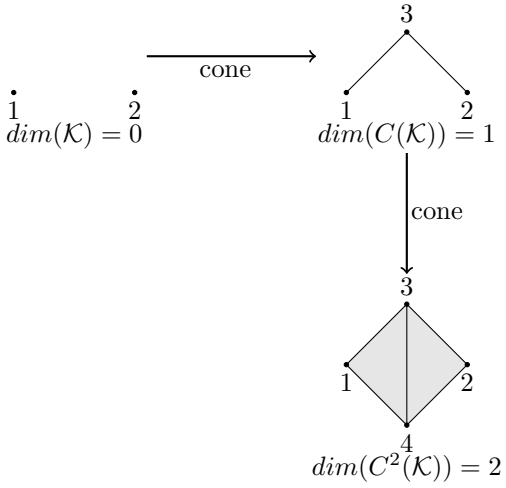


The following can be found in [3]

Definition 3.5. Let $\mathcal{K}$ be a simplicial complex on the set $\{1, \ldots, n-1\}$. We define and denote the cone over $\mathcal{K}$ as follows:

$$C(\mathcal{K}) = \{x \cup \{n\} | x \in \mathcal{K}\} \cup \mathcal{K}$$

Notice that if $\mathcal{K}$ is an n-dimensional complex then $C(\mathcal{K})$ is an $(n+1)$-dimensional complex. Since $C(\mathcal{K})$ is a simplicial complex it is possible to apply the cone again.



We write the j^{th} *cone on* $\mathcal{K}$ as $C^j(\mathcal{K})$. We have the following from [1] regarding a graph G.

Lemma 3.6. The dimension of $C^j(G)$ is $j+1$.

In general, counting the number of i-simplicies for a given simplicial complex is computationally difficult [7]. There is a vector that encodes all of these numerics. We list the following critical definition:

Definition 3.7. The f-vector of an $(n-1)$-dimensional simplicial complex $\mathcal{K}$, denoted by $\overrightarrow{f}(\mathcal{K})$, is the vector with the number of i simplicies in the i^{th} component. We represent the i^{th} component of $\overrightarrow{f}(\mathcal{K})$ by $f_i(\mathcal{K})$.

For a given fixed $\mathcal{K}$, the following notation is usually used to denote this vector $\overrightarrow{f}(\mathcal{K}) = (f_0, f_1, \ldots, f_{n-1})$. Often it is simply written as $(f_0, f_1, \ldots, f_{n-1})$. For the purposes of making calculations, recall, $f_{-1}(\mathcal{K}) = 1$ [3]. We have the following calculations from [1]; the proofs can be found there.

Example 3.8. For Example 3.3 we have $\overrightarrow{f}(\mathcal{K}) = (3, 1)$.

Lemma 3.9. For a graph G, $f_0(C^j(G)) = f_0(G) + j$ and $f_1(C^j(G)) = f_1(C^{j-1}(G)) + f_0(C^{j-1}(G))$

As an immediate Corollary of Lemma 3.9 we re-write $f_1(C^n(R_G))$ by unravelling the recursion.

Corollary 3.10. For a graph G the number of edges of $C^j(G)$ can be re-written as $f_1(C^j(G)) = f_1(G) + \sum_{k=0}^{j-1} f_0(C^k(G))$

If R_G is a random graph, we re-iterate that the f-vector of $C^j(R_G)$ will be the basis, after conversion (see §Bit Conversions for more details), of a sequence of bits that is to be analyzed by the suite [9]. In previous work [1], the authors discussed $C^j(R_G)$ and conducted a series of tests using [9] verifying that the construction generated families of random bits coming from a random graph. The implication is that our initial construction preserves this property as new simplicial complexes are "grown" from the random graph R_G.

When reference to a random graph is made, it refers to those graphs described in [5] and we use the notation R_G to label such. These graphs have f-vectors: (f_0, f_1) and we assume that $f_1(R_G) \neq 0$. For the convenience of the reader we list the algorithm implemented in [1] to generate such graphs and to determine the f-vector when the cone is applied successively.

Random Graph Algorithm

Input: n, p
Initialize $M_{ij} = 0 \ \ \forall i, j$
M_{ij} is the $(ij)^{th}$ entry in the matrix M
for $i, j = 1, \ldots, n$ **do**
Generate random number r
end for
if $r < p$ and $i < j$ **then**
$M_{ij} = 1$
else
$M_{ij} = 0$
end if
Construct R_G from the matrix M

In [1] the following algorithm was used to determine the f-vector of $C^j(R_G)$:

Computing the f-vector of the j^{th}-cone on R_G

Input: Random graph R_G
Compute $\overrightarrow{f}(R_G)$
for $j = 1, \ldots, n$ **do**
Compute $\overrightarrow{f}(C^j(R_G)$
end for

Observe: The random graph R_G is generated using the algorithm above and it is fixed, then we compute $\overrightarrow{f}(R_G)$ to initiate the algorithm mentioned above. Suppose $\overrightarrow{f}(C^{n-1}(R_G)) = (x_0, x_1, \ldots, x_n)$, then $\overrightarrow{f}(C^n(R_G)) = (y_0, y_1, \ldots, y_{n+1})$ where for $1 \leq i \leq n+1$

$$\begin{aligned} y_0 &= x_0 + 1 \\ y_i &= x_{i-1} + x_i \\ y_{n+1} &= x_n \end{aligned}$$

4. Dual Polyhedra and Symmetry

We begin by following the treatment in [2]. Additional details concerning polytopes and polyhedra can be found there. For a fixed integer $q > 0$ we work in the Euclidean space $\mathbb{R}^q$ and all scalars will be assumed to be real. Let $x_1, \ldots, x_n$ be points in $\mathbb{R}^q$, then an *affine combination* is the linear combination

$$\sum_{i=1}^{n} c_i x_i$$

where $c_1 + \cdots + c_n = 1$. A collection of points is said to be *affinely independent* if $c_1x_1 + \cdots + c_nx_n = 0$ then the $c_i = 0$. We say a subset C of $\mathbb{R}^q$ is a *convex set* if the following conditions hold for all $x_1, x_2 \in C$ and scalars c_1 and c_2 satisfying:

(1) $c_1x_1 + c_2x_2 \in C$ such that $c_1, c_2 \geq 0$.
(2) $c_1 + c_2 = 1$

Affine combinations are linear combinations where the scalars satisfy the conditions above. More specifically, let $x_1, \ldots, x_n$ be points in $\mathbb{R}^q$, then a convex combination is a linear combination $c_1x_1 + \cdots + c_nx_n$ such that:

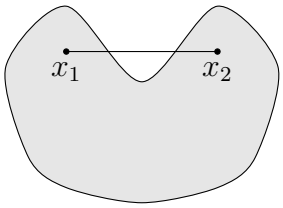
(1) $c_1 + \cdots + c_n = 1$.
(2) $c_i \geq 0$

We have the following

Theorem 4.1. *A subset C of $\mathbb{R}^d$ is convex if and only if any convex combination of points from C is again in C.*

Proof. [2] Pg 11. □

Given a subset C as above, the intersection of all convex sets in $\mathbb{R}^q$ containing it is a convex set denoted by *conv* C. This set is often referred to as the convex hull of C. When the set is clear we will simply say the convex hull.



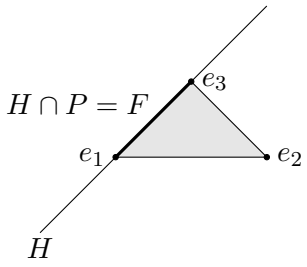
We have the following definition from [2] pg. 44.

Definition 4.2. A polytope P is the convex hull of a non-empty finite set.

Suppose $P = conv(\{x_1, \ldots, x_n\})$ for points $x_i \in \mathbb{R}^q$, then the dimension of P, $dim(P)$ is k if the following conditions hold for a finite number of points $x_1, \ldots, x_k$ from the set $\{x_1, \ldots, x_n\}$. First, there is a finite number of points $x_1, \ldots, x_{k+1}$ from the set $\{x_1, \ldots, x_n\}$ that are affinely independent. Second, there is no such $k+2$ affinely independent points that can be chosen from $\{x_1, \ldots, x_n\}$.

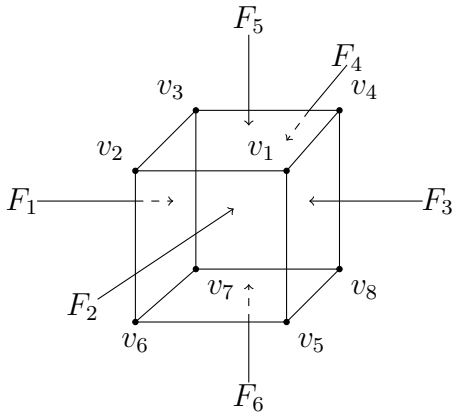
A vertex of P is a zero dimensional face. The set of all vertices of P will be denoted by $V(P)$ and $|V(P)|$ will be the cardinality of this set. Proper faces F of P are polytopes such that $V(F) = F \bigcap Ver(P)$ [2] pg. 45 Theorem 7.3. Since they are polytopes they have a dimension given by the above.

P can also be regarded as the intersection of finitely many halfspaces in a certain Euclidean space [2, 3] and such sets are often referred to as *polyhedral sets*. When the context is clear we will simply refer to P as a polytope. Given a polytope and a finite collection of halfspaces defining it, a supporting hyperplane is a hyperplane $\mathcal{H}$ such that $P \bigcap \mathcal{H} \neq \emptyset$ such that the polytope is contained in one of the halfspaces determined by the hyperplane [3]. In this context a *face* of P is $\mathcal{H} \bigcap P = F$.



Other faces of P include: P, vertices and edges, to name a few. For a given P its boundary $\partial P = \bigcup_{F \subseteq P} F$.

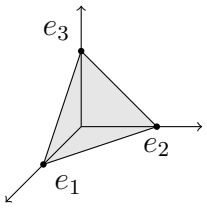
Given P, a facet is a face of dimension $n - 1$ and they are often called *codimension one faces*. A k-dimensional polytope is called *simple* if each zero face can be written as the intersection of exactly k codimension one faces. To clarify these points consider the following example, let P be the cube:



The codimension one faces are $F_1, \ldots, F_6$ (these are the faces of the cube). Each edge is the intersection of exactly two faces and these are

the codimension two faces. Each vertex is the intersection of exactly three faces (codimension one faces) and so these are the codimension three faces. One could equally consider the dimensions of the faces rather than the codimension. In such a case, the faces $F_1, \ldots, F_6$ would be the two dimensional faces, the edges the one-dimensional faces and the vertices the zero-dimensional faces of the cube.

Example 4.3. Following [3], let $P = \Delta^n$. Then this polytope is $conv(\{x_1, \ldots, x_{n+1}\})$ where $x_i \in \mathbb{R}^n$. This is called the *n-dimensional simplex* and the points are not on a common affine hyperplane. This is not to be confused with the simplicial complex $\widehat{\Delta}^n$ whose simplicies are the sets in the power set of $\{1, \ldots, n\}$. Given Δ^n, then for $i \leq n$, Δ^i is a face of P of dimension at most n. If the points x_i are the unit vectors e_i, then Δ^n is called the *standard n-simplex* [3] pg. 8. For example, in $\mathbb{R}^3$, the standard 2-simplex is the convex hull of the unit vectors e_1, e_2 and e_3. A picture can be found below:

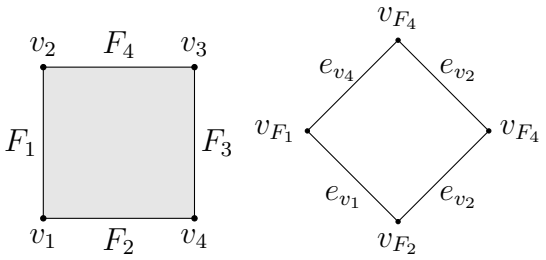


We now follow the treatment in [4]-specifically pages 425 and 430. The main idea is that given a polytope one may construct a simplicial complex dual to it and vice-versa. Assume P is an n-dimensional simple polytope (defined as above) and let $\Im = \{F_0, \ldots, F_m\}$ be the set of facets. Let $\mathcal{K}_P$ denote the dual simplicial complex with vertex set $\{F_0, \ldots, F_m\}$ with the requirement: $\sigma = \{F_0, \ldots, F_j\}$ span a $j+1$ simplex in $\mathcal{K}_P$ if and only if $F_0 \cap \cdots \cap F_j \neq \emptyset$ in P. We observe that a zero face in P (a vertex) is a codimension n face; hence, it is the intersection of exactly n facets. By the definition of the dual, such an intersection spans an $n-1$ simplex. Therefore, the dual complex $\mathcal{K}_P$ is $(n-1)$-dimensional. Furthermore, it is a simplicial sphere, roughly meaning, it is essentially a combinatorial representation of the sphere S^{n-1}.

Notation 4.4. We fix the notation regarding the dual. Given a simplicial complex $\mathcal{K}$ we will write the dual as P (or $P_{\mathcal{K}}$ if we need to stress certain properties of this combinatorial object). When convenient we may just say "the dual". If P is given then the dual, $\mathcal{K}_P$ will be written as $\mathcal{K}$ when there is no room for confusion. For reasons of convenience certain authors use the notation $\mathcal{K}^*$ to denote the dual, especially when

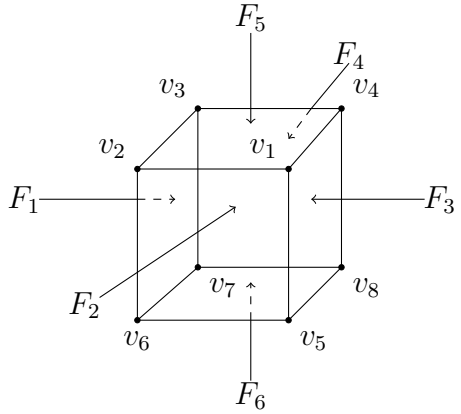
considering $\mathcal{K}^{**}$ ([6]), but we will stick with the conventions mentioned above. Given $\mathcal{K}$ the notation $P_{\mathcal{K}}$ is used in the paper [4].

Example 4.5. For the square we have



We now give a slightly more complicated example

Example 4.6. Recall, the cube



If F is a codimcension one face of the cube (a face of the cube) we let v_F denote the dual vertex in $\mathcal{K}_{P^3}$. Recall, the codimension one faces of the cube dualize to vertices, so each face of the cube dualizes to a vertex v_{F_i}. Each codimension two face in the cube is the intersection of two faces (e.g., $F_1 \bigcap F_6 = E$ where E is an edge in P) dualizes to an edge. In this very specific example $F_1 \bigcap F_6$ dualizes to the edge $\{v_{F_1}, v_{F_6}\}$. Finally, a vertex in the cube is a codimension three face since it is the intersection of three facets. Here, the vertex v_1 in the cube is the intersection: $F_2 \bigcap F_3 \bigcap F_5$ so it dualizes to $\{v_{F_2}, v_{F_3}, v_{F_5}\}$ The table below lists the simplicies in the dual two-dimensional simplicial complex $\mathcal{K}_{P^3}$.

0-simplices	1-simplices	2-simplices
v_{F_1}	$\{v_{F_1}, v_{F_6}\}$	$\{v_{F_2}, v_{F_3}, v_{F_5}\}$
v_{F_2}	$\{v_{F_2}, v_{F_6}\}$	$\{v_{F_1}, v_{F_2}, v_{F_5}\}$
v_{F_3}	$\{v_{F_3}, v_{F_6}\}$	$\{v_{F_1}, v_{F_4}, v_{F_5}\}$
v_{F_4}	$\{v_{F_4}, v_{F_6}\}$	$\{v_{F_3}, v_{F_4}, v_{F_5}\}$
v_{F_5}	$\{v_{F_1}, v_{F_2}\}$	$\{v_{F_2}, v_{F_3}, v_{F_6}\}$
v_{F_6}	$\{v_{F_2}, v_{F_3}\}$	$\{v_{F_1}, v_{F_2}, v_{F_6}\}$
v_{F_7}	$\{v_{F_3}, v_{F_4}\}$	$\{v_{F_1}, v_{F_4}, v_{F_6}\}$
v_{F_8}	$\{v_{F_1}, v_{F_4}\}$	$\{v_{F_3}, v_{F_4}, v_{F_6}\}$
	$\{v_{F_1}, v_{F_5}\}$	
	$\{v_{F_2}, v_{F_5}\}$	
	$\{v_{F_3}, v_{F_5}\}$	
	$\{v_{F_4}, v_{F_5}\}$	

In the case that a simplicial complex is a simplicial sphere, then the construction can made to generate a simple polytope. Since the zero simplicies in $\mathcal{K}$ are dual to codimension one faces in the dual polytope, the face structure of the polytope is given by working through higher dimensional simplicies of K and carefully fitting together the faces of the polytope using the definition of the simplicial complex along with the process to dualize.

If K is a general simplicial complex then it is possible to construct a simple polyhedral complex [4] pg. 428 and this involves the notion of a cone on a geometric realization of various posets.

Later we will consider $\mathcal{K} = C^j(R_G)$ (for some positive integer j) and then analyze certain inequalities derived from the g-theorem. To do so requires the analysis of the *h-vector*(denoted $\overrightarrow{h}$) of the dual and how it is related to the $\overrightarrow{f}$ of the simplicial complex we construct. Following [4] pg. 430 we have:

Definition 4.7. Let $(f_0, \ldots, f_{n-1})$ be the f-vector of an $(n-1)$-dimensional simplicial complex $\mathcal{K}$. Then the h-vector of the dual, $(h_0, h_1, \ldots, h_n)$, is defined by the following equation:

$$h_0 t^n + \cdots + h_{n-1} t + h_n = (t-1)^n + f_0(t-1)^{n-1} + \cdots + f_{n-1}$$

Observe that the number of components in the h-vector is the dimension of $\mathcal{K}$ plus one. In the case that K (simplicial sphere) is dual to P as above, then by [4], $f_i(K)$ is the number of codimension $i+1$ faces of P (or $n-i-1$ faces). From [3] pg. 12 there are the following two compact equations that relate specific components of the $\overrightarrow{h}$ and

$\overrightarrow{f}$. For $k = 0, ..., n$ we have:

$$h_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{n-i}{n-k} f_{i-1}$$

and

$$f_{n-1-k} = \sum_{q=k}^{n} \binom{q}{k} h_{n-q}$$

Example 4.8. Let $\mathcal{K}$ have the following f-vector $(4, 4)$. Referring to Example 4.5 it is a square. The claim is that the dual P has corresponding h-vector: $(1, 2, 1)$. Specifically, $h_0 = 1 = h_2$ and $h_1 = 2$. We have the polynomial $h_0t^2 + h_1t + h_2 = (t-1)^2 + f_0(t-1) + f_1$. Expanding and equating coefficients produces $h_0 = 1$, $h_1 = f_0 - 2$ and $h_2 = f_1 - f_0 + 1$ and we obtain the vector above.

For certain types of simplicial complexes the h-vector of the dual exhibits a symmetry exhibited by Dehn-Sommerville relations. From [3]

Theorem 4.9. *The h-vector of any simple n-polytope is symmetric $h_{n-i} = h_i$ for $i = 0, 1, \ldots, n$*

Example 4.10. For a positive integer $n > 1$ let $P = \Delta^n$ then $h_i(P) = 1$ for $i = 0, \ldots, n$. This follows from [3] along with a simple verification using Theorem 4.9. For each $i < n - 1$, the h-vectors of the proper faces Δ^i and Δ^{i+1} have components all consisting of ones and the h-vector of Δ^{i+1} has one more component then the h-vector of Δ^i. More specifically, consider Δ^2; it has h-vector $(1, 1, 1)$. Now Δ^1 is a face and has h-vector $(1, 1)$. We state the following interesting fact from [4] and observe that for the examples listed here, the following equation holds.

$$h_0 + \cdots + h_n = |V(P)|$$

Recall, R_G is a random graph generated using the methods described in [1] and the simplicial complex $\mathcal{K} = C^j(R_G)$ is the j^{th}-cone on R_G. A fundamental question we seek to answer is the following; given $\mathcal{K} = C^j(R_G)$ and $\overrightarrow{f}(\mathcal{K})$ what type of symmetry does this f-vector exhibit? Another interesting formulation of this question is to determine if the dual polytope is simple or not. Fortunately, the celebrated *g-theorem* provides an answer for a fairly general class of polyhedra. Using [2]

we note that the f-vector of P has components f_i and they equal the number of i-faces of P. So using this convention, if P is simple and n-dimensional, then the f-vector is $(f_0, ..., f_{n-1})$ where f_0 is the number of vertices of P and f_{n-1} is the number of facets of P.

The following material can be found in [2] pgs. 130-131 and we list it here for the convenience of the reader. Let $g_i(f) := \sum_{j=0}^{d}(-1)^{i+j}\binom{j}{i}f_j$ for $i = 0, .., d$. Let $m := \lfloor \frac{d-1}{2} \rfloor$ and $n := \lfloor \frac{d}{2} \rfloor$. The following is referred to as McMullen's Conditions [2], but other authors refer to it as the g-theorem [3]. For additional information regarding condition (3) the interested reader can refer to [2] pg. 130 (specifically, (2)-(4)).

Theorem 4.11. *A d-tuple $(f_0, ..., f_{d-1})$ of positive integers is the f-vector of a simple d-polytope if and only if the following conditions hold:*

(1) $g_i(f) = g_{d-i}(f)$ *for* $i = 0, .., m$.

(2) $g_i(f) \leq g_{i+1}(f)$ *for* $i = 0, .., n-1$.

(3) $g_{i+1}(f) - g_i(f) \leq (g_i(f) - g_{i-1}(f))^{\langle i \rangle}$ *for* $i = 1, ..., n-1$.

Theorem 4.11 encodes information regarding upper and lower bounds on the number of faces of simple polytopes. From [2] pg. 132 one equation that can be derived is the following:

$$f_0 = \sum_{i=0}^{d}\binom{i}{0}g_i(f)$$

This can be written as $f_0 = (d-1)f_{d-1} - (d+1)(d-2)$ and to clarify that this equation refers to the polytope P we will write

$$f_0(P) = (d-1)f_{d-1}(P) - (d+1)(d-2)$$

Remark 4.12. It is important to note that the generated random graph is fixed. Therefore, the terms $f_0(R_G)$ and $f_1(R_G)$ are fixed, but the parameter j can grow and this is the number of times the cone operation is performed.

To apply the g-theorem it is critical that we understand the dimension of the simplicial complex that results from applying the cone. We recall that $C^j(R_G)$ is a $(j+1)$-dimensional simplicial complex when $f_1(R_G) \neq 0$.

Lemma 4.13. Let $\mathcal{K}$ be an $(n-1)$-dimensional simplicial complex with given $\overrightarrow{f}(\mathcal{K}) = (f_0, \ldots, f_{n-1})$. For a positive integer $j > 0$ the following holds: $f_{n+j-1}(C^j(\mathcal{K})) = f_{n-1}(\mathcal{K})$

Proof. Let $\sigma_{max} = \{v_1, \ldots, v_n\}$ be a top dimensional simplex in $\mathcal{K}$ noting that $dim(\mathcal{K}) = |\sigma_{max}| - 1$. We observe that $C(\mathcal{K})$ has the effect of

adding one vertex to each simplex, but in particular for a $\sigma'_{max} \in C(\mathcal{K})$ we have $\sigma'_{max} = \sigma_{max} \cup \{c_1\}$ where c_1 refers to the new vertex added to the simplex, the cone point, and σ_{max} is a simplex counted in $f_{n-1}(\mathcal{K})$. Clearly, $|\sigma'_{max}| = |\sigma_{max}| + 1 = n + 1$ and there are f_{n-1} such simplicies. Furthermore, it is obvious that the dimension of $C(\mathcal{K})$ is n. Similarly, for $j > 1$ we have $dim(C^j(\mathcal{K})) = dim(\mathcal{K}) + j = n + j - 1$. Each top dimensional simplex in the iterated cone $C^j(\mathcal{K})$ are those that are the top dimensional simplicies in $\mathcal{K}$ with j vertices added coming from adjoining j "cone" points. These maximal dimensional simplicies have $n + j$ vertices and so the top component of $\overrightarrow{f}(C^j(\mathcal{K}))$ is f_{n+j-1} and such simplicies are enumerated by $f_{n-1}(\mathcal{K})$. □

Remark 4.14. Of particular interest is the case $\mathcal{K} = R_G$ such that $f_1(R_G) \neq 0$. The equation above, then takes the form:$f_{j+1}(C^j(R_G)) = f_1(R_G)$ noting that f_{j+1} is the component of the f-vector enumerating the simplicies of maximal cardinality.

Proposition 4.15. For a graph G such that $f_1(G) \neq 0$, let $C^j(G) = \mathcal{K}^{j+1}$. For j sufficiently large, the complexes $\mathcal{K}^{j+1}$ are not dual to a polytope that satisfies the g-theorem.

Proof. Given a fixed graph G let $f_0(G) = s$ and $f_1(G) = t$. We argue by contradiction. Suppose for all j we have $\mathcal{K}^{j+1}$ is dual to a $(j+2)$-dimensional polytope P that satisfies the g-theorem. Then the following equation must hold where $d = dim(P)$:

$$f_0(P) = (d-1)f_{d-1}(P) - (d+1)(d-2)$$

Since f_{j+1} is the number of codimension one faces of P we obtain, using the dual complex, $f_{j+1}(P) = s + j$. Plugging all of this into the equation above gives:

$$\frac{t-s}{s-2} = j$$

To obtain the result observe that the left hand side of the equation is fixed and j can be arbitrarily large.

□

Proposition 4.15 also implies that one can pass through the class of simple n polytopes. As a practical matter this is crucial in ensuring that the f-vectors do not exhibit a symmetry as described by the statements that follow, in particular Definition 4.16. One goal is to maintain the computational complexity of the resulting f-vector [7].

Let $P = \Delta^n$ and $\mathcal{K}_P = \mathcal{K}$ be its dual. It is shown that when $\overrightarrow{h}(P) = (1, 1, \ldots, 1)$, then $\overrightarrow{f}(\mathcal{K})$ satisfies a Dehn-Sommerville type relationship.

Let us recall Pascal's Triangle:

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

We note that the triangle starts from row zero and the entry $\binom{n}{k}$ refers to row n column k. The n^{th} row in the triangle is

$$\left\{ \binom{n}{r} \;\middle|\; 0 \leq r \leq n \right\}$$

There is a zeroth row and it contains $\binom{0}{0}$ and for each row there are columns starting at zero. For example, row two contains: $\binom{2}{0}$, $\binom{2}{1}$ and $\binom{2}{2}$. Using this notational convention, there are three columns whereby $\binom{2}{0}$ is in column zero for this row. There are diagonals too and they begin with the zeroth diagonal consisting of $\binom{y}{0}$ for positive integers $y \geq 0$.

For the convenience of the reader we recall the following. For $k = 0, \ldots, n$ we have:

$$h_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{n-i}{n-k} f_{i-1}$$

$$f_{n-1-k} = \sum_{q=k}^{n} \binom{q}{k} h_{n-q}$$

Definition 4.16. An $n-1$ dimensional simplicial complex $\mathcal{K}$ is called symmetrical if $f_j(\mathcal{K}) = f_{n-j-1}(\mathcal{K})$ for $0 \leq j \leq n-1$.

Theorem 4.17. *Let $n > 1$ and suppose P is an n-dimensional simple convex polytope such that $\overrightarrow{h}(P) = (1, \ldots, 1)$, then the $n-1$ dimensional dual simplicial complex $\mathcal{K}$ is symmetrical.*

Proof. We assume n is fixed. Since $h_i = 1$ for each i, then for $0 \leq k \leq n$ the components of the f-vector of $\mathcal{K}$ can be written as:

$$f_{n-1-k} = \sum_{q=k}^{n} \binom{q}{k}$$

We first deal with the extreme cases for k. If $k = n$, then it is clear that $f_{-1} = 1$. For $k = 0$, then

$$f_{n-1} = \sum_{q=0}^{n} \binom{q}{0} = n + 1$$

By similar calculations we obtain for $k = n - 1$:

$$f_0 = \binom{n-1}{n-1} + \binom{n}{n-1}$$

Hence, $f_0 = f_{n-1} = n + 1$. In what follows we will use certain summations in Pascal's triangle. Generally, consider a set $\{0, \ldots, t\}$ of consecutive positive integers. Fix $s \in \{0, \ldots, t\}$ such that $s \leq t$ then using the f-vector calculation above we have the summation:

$$f_{t-1-s} = \binom{s}{s} + \binom{s+1}{s} + \binom{s+2}{s} + \cdots + \binom{t}{s}$$

This is summation along a diagonal in Pascal's Triangle, therefore

$$f_{t-1-s} = \binom{t+1}{s+1}$$

Consider f_{n-1-k} and the two substitutions for k (observe that $t = n$ and $s = k$ in the formulation above):

(1) When $k = j$, then $f_{n-1-j} = \binom{n+1}{j+1}$.
(2) When $k = n - j - 1$, then $f_{n-1-j} = \binom{n+1}{n-j}$.

To complete the proof one must show that $\binom{n+1}{j+1} = \binom{n+1}{n-j}$, but this follows immediately from the properties of n choose k.

□

We note that the $\overrightarrow{h}$ has a component h_n but the entries of the dual $(n-1)$ dimensional complex are located in the $n+1$ row in Pascal's Triangle. The following statement follows immediately from Theorem 4.17 and the tests found in sections §7 and §8.

Remark 4.18. There are families of bit sequences that are derived from symmetrical simplicial complexes and their successive cones that are determined to be random using the NIST test suite described in publication 800-22 [9]. The key takeaway is that one starts with a combinatorial object with a clear pattern (symmetry) and dualizing it produces a simplicial complex that is highly symmetrical, yet the converted bit sequence shows up as random using the NIST test suite. More is true, using the cone it is possible to construct arbitrarily many bit sequences (derived from this symmetrical object) that the test suite deems random.

5. Bit Conversions

The experimental implementation uses arbitrary-sized integers to represent vector elements, and a vector is then implemented as a sequence of these integers. Since the NIST test suite [9] expects its input to be a binary file, we must convert a sequence of integers into the corresponding binary bit-stream. To do this we iterate over the vector elements, creating a binary representation of each integer, and concatenating this binary representation onto the output file.

Care must be taken when doing this to use a bit-wise approach instead of a byte-wise approach. In a byte-wise approach the binary representation of each integer will begin on a byte boundary, and since most integers will not completely fill their most-significant byte we will have up to 7 extraneous leading zero bits. In practice, this means that the binary representations of each integer should be bit-shifted before concatenation, to avoid these leading zero bits.

To illustrate the importance of this point, our initial implementation in [1] has a minor bug in the bit-shifting code that is only triggered for certain byte values, and when triggered drops a 0-bit from the output stream. Despite the relative rarity of this bug being triggered, the NIST test suite did detect its non-random contributions to the output file, as can be seen in Tables 1, 3, 13, and 15 in [1], which show a noticeable

"clustering" effect towards p-values of 0. In the current implementation used in this paper this bug has been fixed.

6. Algorithms

All our algorithms implemented are polynomial time and numeric in nature, since we only calculate a vector and its dual.

Algorithm for cone operation on f-vector of a simplicial complex

Input: $\overrightarrow{f}(R_G)$ **as** $x_1, \ldots, x_n$
Compute $C^k(R_G)$ **as** $y_1, \ldots, y_{n+1}$
for $i = 1, \ldots, n+1$ **do**
  if $i = 1$ **then**
    $y_1 = x_1 + 1$
  else if $i = n+1$ **then**
    $y_{n+1} = x_n$
  else
    $y_i = x_i + x_{i+1}$
  end if
end for

Algorithm determining the f-vector of a k-cone

Input : Random graph R_G
Compute $\overrightarrow{f}(R_G$
for $k = 1, \ldots, n$ **do**
  Compute $\overrightarrow{f}(C^k(R_G)$
end for

Algorithm to return the dual h-vector of this f-vector, if f-vector comes from a simplicial complex.

Input: $\overrightarrow{f}(R_G)$
Compute $\overrightarrow{h}(P)$
for $k = 0, \ldots, n$ **do**
  for $i = 0, \ldots, k$ **do**
    if $i = 0$ **then**

$h_k = \binom{n}{n-k}$
else
$h_k = (-1)^{k-i} \binom{n-i}{n-k} f_{i-1}$
end if
end for
end for

Return the dual f-vector of this h-vector, if h-vector comes from a polytope.

Input: $\overrightarrow{h}(P)$
Compute $\overrightarrow{f}(R_G)$
for $k = 0, \ldots, n$ **do**
for $i = 0, \ldots, k$ **do**
if $i = 0$ **then**
$h_k = \binom{n}{n-k}$
else
$h_k = (-1)^{k-i} \binom{n-i}{n-k} f_{i-1}$
end if
end for
end for

7. Results

We explored the effect of symmetry in h-vectors on the resulting dual f-vectors. To this end, we ran three sets of experiments as follows:

(1) Create an h-vector with obvious symmetry (e.g., all 1's)
(2) Compute the dual f-vector of the h-vector
(3) Cone the resulting f-vector zero or more times
(4) Run the resulting bit pattern through the NIST test suite

A non-random pattern should be consistently detected by the NIST test suite and shown with every data set having a p-value of close to 1.0 or close to 0.0, which will appear as a "clustering" of points towards the top or bottom of the graph. The sparklines represent the trend of all NIST tests, which if close to 0.0 or 1.0 would look like a flatline.

For the first experiment we fix the h-vector length at 3751, with a pattern of all 1's, and vary the number of coning operations from 0 to 99 times. (see Figure 2) For the second experiment we vary the h-vector length from 3750 to 3849, with a pattern of all 1's, and we do not apply the coning operation. 6 For the third experiment we fix the h-vector length at 3750, vary non-end elements in the pattern from 1 to 100, and do no apply the coning operation. 10

The time required to do this using a naive implementation on a modern consumer CPU (Intel Core i5-4590) is 2.3 seconds. This is therefore a gross upper bound.

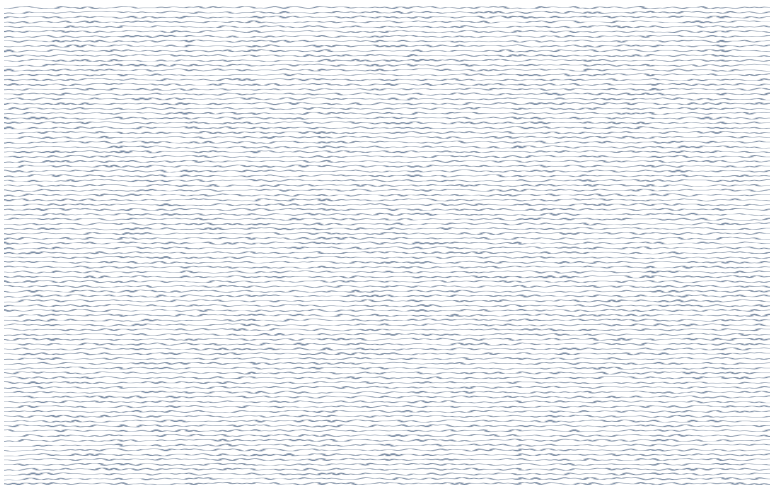


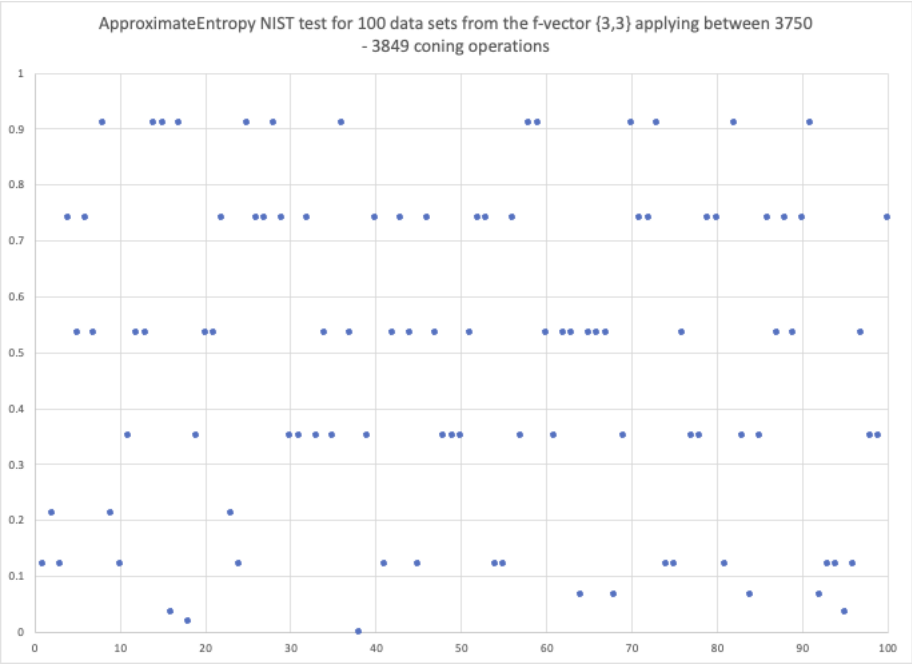
Figure 1. 100 trendlines for NIST tests p-values after applying between 0 and 99 coning operations on a vector of length 3751, with a pattern of all 1's

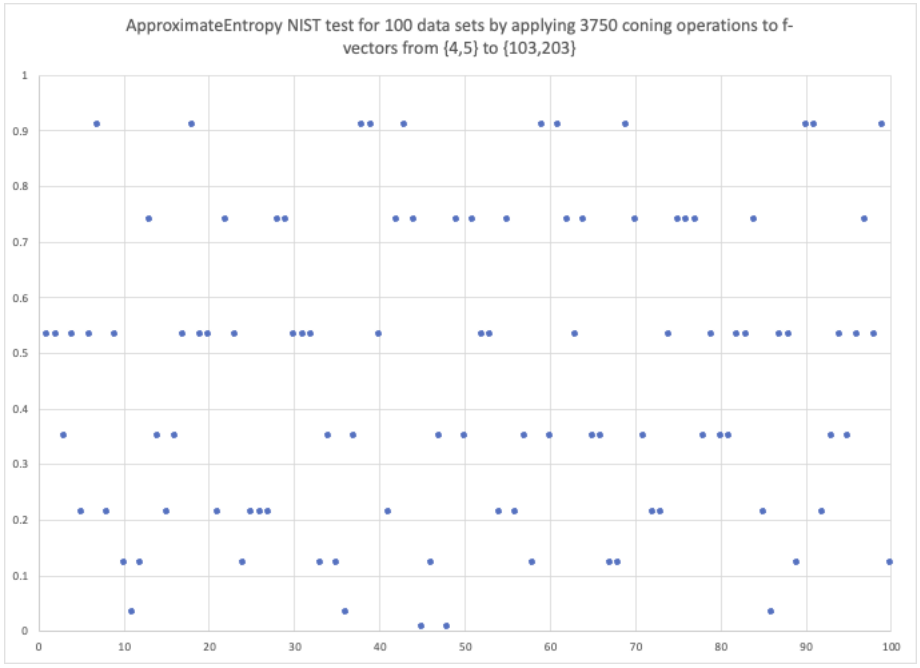
FIGURE 2. 100 trendlines for NIST tests p-values on vectors of lengths between 3750 and 3849 with a pattern of all 1's

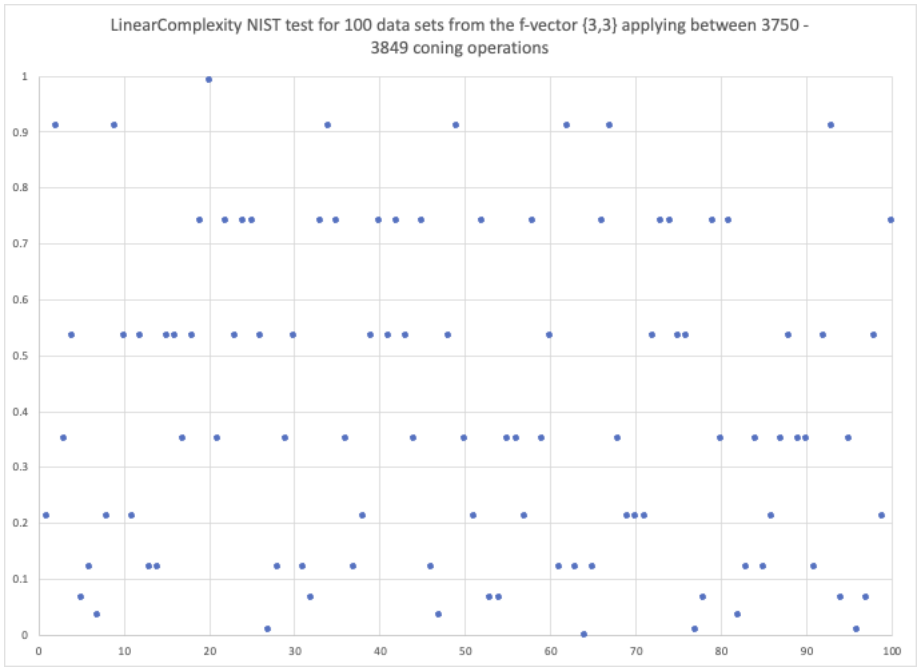
FIGURE 3. 100 trendlines for NIST tests p-values on vectors of length 3750 with non-end elements from 1 to 100.

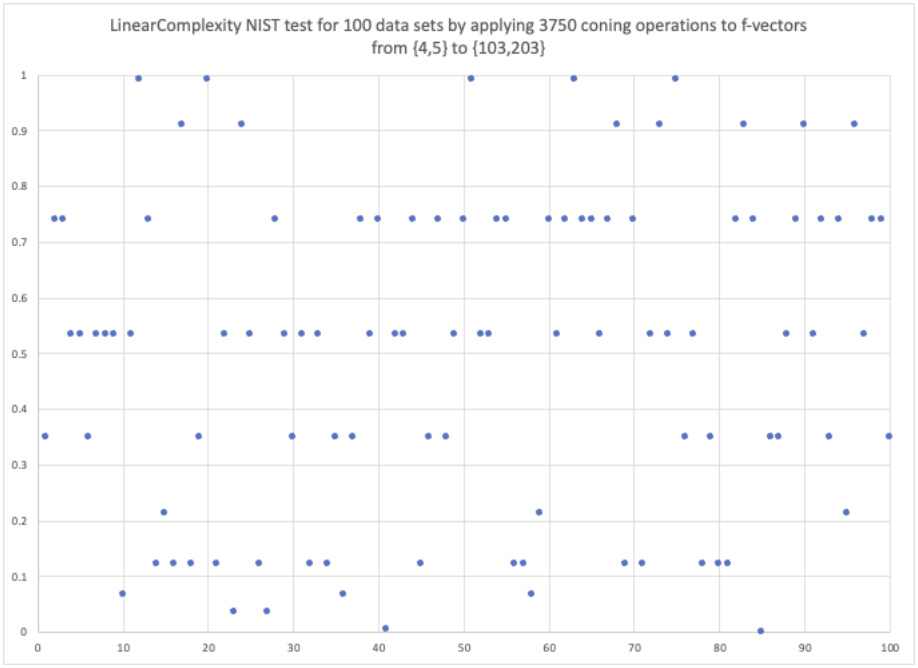
8. Appendix

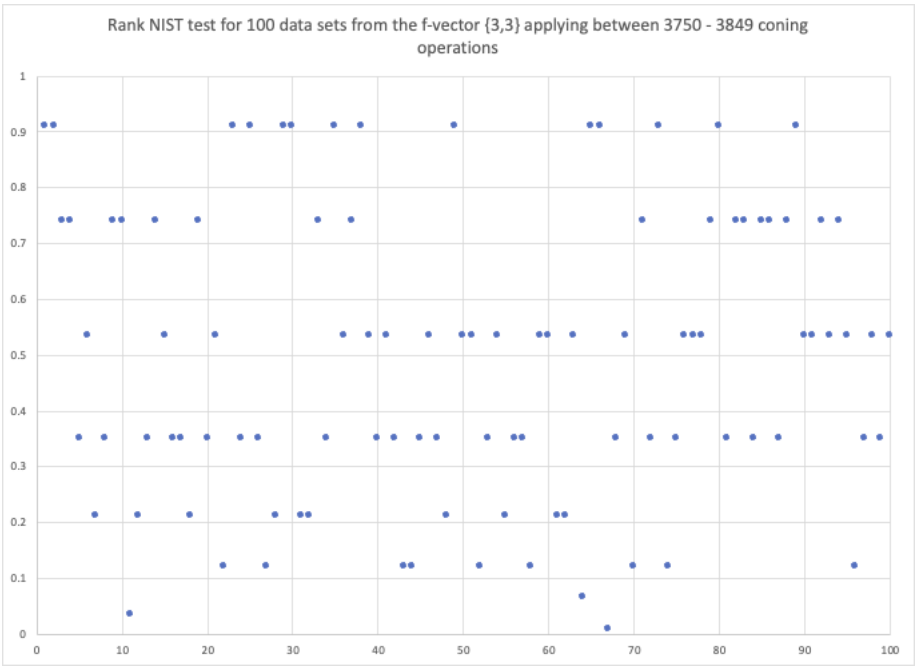
Since our first publication [1] we updated our code. Version 2.0 of the code fixes several bugs, including one where 0's were not being properly appended to the bit-stream. As a result it causes fewer false positives from the NIST test suite. We have posted the new results in the following github repository `https://github.com/gnexeng/coning-analysis`. The following is a sample of the results.

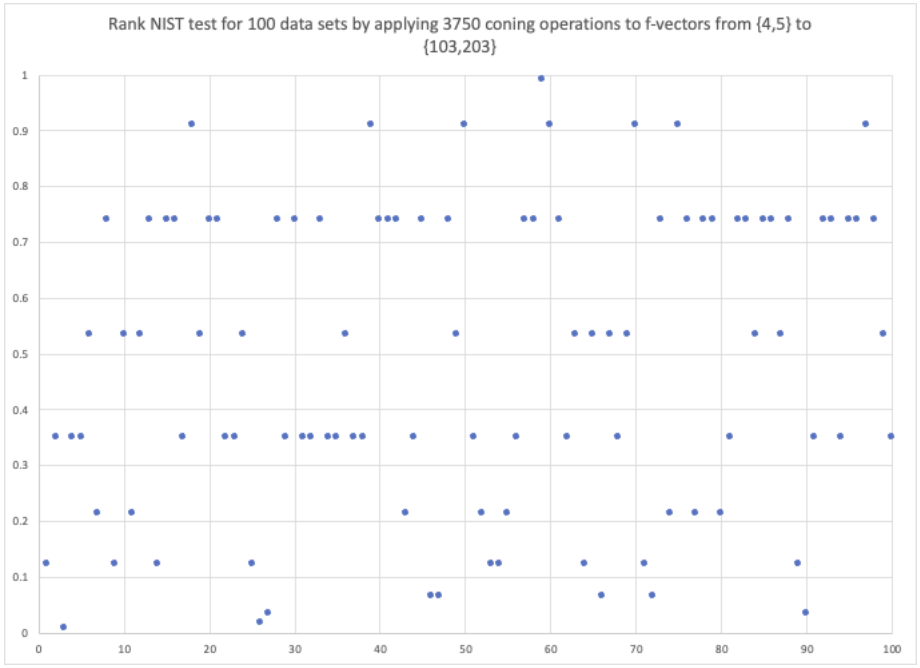



ApproximateEntropy NIST test for 100 data sets by applying 3750 coning operations to f-vectors from {4,5} to {103,203}
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60
70
80
90
100


LinearComplexity NIST test for 100 data sets from the f-vector {3,3} applying between 3750 - 3849 coning operations
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60
70
80
90
100


LinearComplexity NIST test for 100 data sets by applying 3750 coning operations to f-vectors from {4,5} to {103,203}
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60
70
80
90
100


Rank NIST test for 100 data sets from the f-vector {3,3} applying between 3750 - 3849 coning operations
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60
70
80
90
100


Rank NIST test for 100 data sets by applying 3750 coning operations to f-vectors from {4,5} to {103,203}
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60
70
80
90
100

References

[ALDH] Allen, D., L Luz, J., Salivia., G., Hardwick, J., *A Simplicial Pseudo-Number Random Generator*, Submitted.

[B] Bronstead., A., *An Introduction to Convex Polytopes*, Springer-Verlag (1983).

[BP1] Buchstaber V.M., Panov T.E., *Torus Actions and their Applications in Topology and Combinatorics,* University Lecture Seriers, AMS (2002).

[DJ] Davis M., Januszkiewicz T., *Convex polytopes, Coxter Orbifolds and Torus Actions,* Duke Math. Journal 62 no. 2, pp. 417-451 (1991).

[ER] P. Erdos., A. Renyi., *On the Evolution of Random Graphs,* Mathematical Institute of the Hungarian Academy of Sciences (1960).

[G] Gunbaum., B., *Convex Polytopes*, Springer-Verlag (1967).

[KP] V. Kaibel., M. Pfetsch., *Some Algorithmic Problems in Polytope Theory,* Algebra, Geometry and Software Systems pgs 23-47, Springer (2003).

[TW] W. Trappe., L. Washington., *Introduction to Cryptography with Coding Theory,* Pearson 2nd Ed. (2006).

[NIST] A. Runkhin., J. Soto., J. Nechvatal., M. Smid., E., Baker, S. Leigh., M. Levenson., M. Vangel., D. Banks., A., Heckert, J. Dray., S. Vo., *A Statistical Test Suite for Random Pseudorandom Number Generators for Cryptographic Applications,* NIST Special Publication 800-22, Revision 1a (Revision 2010) .

[NLKB] S. Nobari., X. Lu., P. Karras., S. Bressan., *Fast Random Graph Generation,* Proceedings of the 14th International Conference on Extending Database Technology (pp. 331-342). Uppsala, Sweden: ACM. doi:10.1145/1951365.1951406 (2011)

[NSC] National Science and Technology Council., Chairs: Holdren, J., Shannon, G., Co-chairs: Kurose., J. Marzullo, K., *Federal Cybersecuirty Research and Development Strategic Plan,* (February 2016) .

Department of Mathematics BMCC, CUNY, New York, New York 10007

Email address: dtallen@bmcc.cuny.edu

Department of Computer Science, Minnesota state University, Mankato, South Rd and Ellis Ave, Mankato, MN 56001

Email address: jonathan.hardwick@gmail.com

Departmento de Matemáticas, Universidad de Puerto Rico, Industrial Minillas 170 Car 174, Bayamón, PR, 00959-1919

Email address: jose.laluz1@upr.edu

Department of Mathematics, Computer Science and Statistics, Gustavus Adolphus College, 800 West College Avenue Saint Peter, MN 56082

Email address: gsalivia@gustavus.edu