Random Self-Reducibility of Learning Problems over Burnside Groups

William Skeith

CCNY and Graduate Center
CAISS

Joint work with Nelly Fazio, Kevin Iga, Antonio Nicolosi and Ludovic Perret
1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
1 Motivation & Background
   - Why Group-Theoretic Cryptography?
     - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
Motivation

- Interesting mathematical problem on its own . . .
- Tackling crypto challenges of post-quantum era [Sh’94]
  - Shor’s algorithm: Efficient *quantum* procedure to compute the order of any element in a cyclic group
  - Hardness of order-finding at the heart of most popular public-key cryptosystems (RSA, DH, ECDH)
  - If quantum computing becomes practical, we’ll need alternative crypto platforms
- Quantum computing aside, *diversifying assumptions* still seems prudent
Interesting mathematical problem on its own . . .

Tackling crypto challenges of post-quantum era [Sh’94]
  - Shor’s algorithm: Efficient *quantum* procedure to compute the order of any element in a cyclic group
  - Hardness of order-finding at the heart of most popular public-key cryptosystems (RSA, DH, ECDH)
  - If quantum computing becomes practical, we’ll need alternative crypto platforms

Quantum computing aside, diversifying assumptions still seems prudent
Motivation

- Interesting mathematical problem on its own . . .
- Tackling crypto challenges of post-quantum era [Sh’94]
  - Shor’s algorithm: Efficient *quantum* procedure to compute the order of any element in a cyclic group
  - Hardness of order-finding at the heart of most popular public-key cryptosystems (RSA, DH, ECDH)
  - If quantum computing becomes practical, we’ll need alternative crypto platforms
- Quantum computing aside, *diversifying assumptions* still seems prudent
Motivation

- Interesting mathematical problem on its own . . .
- Tackling crypto challenges of post-quantum era [Sh’94]
  - Shor’s algorithm: Efficient *quantum* procedure to compute the order of any element in a cyclic group
  - Hardness of order-finding at the heart of most popular public-key cryptosystems (RSA, DH, ECDH)
- If quantum computing becomes practical, we’ll need alternative crypto platforms
- Quantum computing aside, diversifying assumptions still seems prudent
Motivation

Interesting mathematical problem on its own . . .

Tackling crypto challenges of post-quantum era [Sh’94]

- Shor’s algorithm: Efficient *quantum* procedure to compute the order of any element in a cyclic group
- Hardness of order-finding at the heart of most popular public-key cryptosystems (RSA, DH, ECDH)

∴ If quantum computing becomes practical, we’ll need alternative crypto platforms

- Quantum computing aside, diversifying assumptions still seems prudent
Interesting mathematical problem on its own . . .

Tackling crypto challenges of post-quantum era [Sh’94]
  - Shor’s algorithm: Efficient *quantum* procedure to compute the order of any element in a cyclic group
  - Hardness of order-finding at the heart of most popular public-key cryptosystems (RSA, DH, ECDH)
  . . . If quantum computing becomes practical, we’ll need alternative crypto platforms

Quantum computing aside, *diversifying assumptions* still seems prudent
Challenging computational problems abound in group theory, however...

- Many hard problems are based on infinite groups
- This makes probabilistic modeling difficult
- Average-case hardness for many problems seems to be not well-understood
Challenging computational problems abound in group theory, however...

- Many hard problems are based on infinite groups
- This makes probabilistic modeling difficult
- **Average-case hardness for many problems seems to be not well-understood**
In this work we demonstrate a random self-reducibility property for a new group-theoretic problem put forth in the work of Baumslag et al. [BFNSS11].

In particular, we show a worst-case to average-case reduction for the $B_n$-LHN problem (more on that later...).
In this work we demonstrate a random self-reducibility property for a new group-theoretic problem put forth in the work of Baumslag et al. [BFNSS11].

In particular, we show a worst-case to average-case reduction for the $B_n$-LHN problem (more on that later...).
Main Results

- In this work we demonstrate a random self-reducibility property for a new group-theoretic problem put forth in the work of Baumslag et al. [BFNSS11].
- In particular, we show a **worst-case to average-case** reduction for the $B_n$-LHN problem (more on that later...).
1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
Random self-reducibility makes a statement about the average case complexity of a problem. In particular, it says that

Random self-reducibility

Solving a random instance is not any easier than solving an arbitrary instance.
Random self-reducibility makes a statement about the average case complexity of a problem. In particular, it says that

**Random self-reducibility**

Solving a *random* instance is not any easier than solving an *arbitrary* instance.
Random self-reducibility has been a hallmark of every successful cryptographic assumption to-date.

This is not so surprising:

- Any cryptosystem implementation must include an algorithm which samples hard instances of a computational problem.
- RSR ensures that hard instances are not difficult to find: a random instance will suffice.
Random self-reducibility has been a hallmark of every successful cryptographic assumption to-date.

This is not so surprising:

- Any cryptosystem implementation must include an algorithm which samples hard instances of a computational problem.
- RSR ensures that hard instances are not difficult to find: a random instance will suffice.
Random self-reducibility has been a hallmark of every successful cryptographic assumption to-date.

This is not so surprising:

- Any cryptosystem implementation must include an algorithm which samples **hard instances** of a computational problem.
- RSR ensures that hard instances are not difficult to find: a random instance will suffice.
Random self-reducibility has been a hallmark of every successful cryptographic assumption to-date.

This is not so surprising:

- Any cryptosystem implementation must include an algorithm which 
  samples **hard instances** of a computational problem.
- RSR ensures that hard instances are not difficult to find: a random 
  instance will suffice.
The $B_n$-LHN Problem

$B_n$-LHN

- The problem is a generalization of LWE, moving from vector spaces and inner products to the setting of groups and homomorphisms.
- As shown in [BFNSS11], this assumption suffices for some basic cryptographic tasks, e.g., symmetric encryption.
- We’ll start with a quick review of LWE.
The $B_n$-LHN Problem

$B_n$-LHN

- The problem is a generalization of LWE, moving from vector spaces and inner products to the setting of groups and homomorphisms.
- As shown in [BFNSS11], this assumption suffices for some basic cryptographic tasks, e.g., symmetric encryption.
- We’ll start with a quick review of LWE.
The $B_n$-LHN Problem

$B_n$-LHN

- The problem is a generalization of LWE, moving from vector spaces and inner products to the setting of groups and homomorphisms.
- As shown in [BFNSS11], this assumption suffices for some basic cryptographic tasks, e.g., symmetric encryption.
- We'll start with a quick review of LWE.
The $B_n$-LHN Problem

$B_n$-LHN

- The problem is a generalization of LWE, moving from vector spaces and inner products to the setting of groups and homomorphisms.
- As shown in [BFNSS11], this assumption suffices for some basic cryptographic tasks, e.g., symmetric encryption.
- We’ll start with a quick review of LWE.
Outline

1 Motivation & Background
   • Why Group-Theoretic Cryptography?
   • Random self-reducibility

2 Learning Problems Over Burnside Groups
   • Background: LWE
   • LHN Problem
   • Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   • Step 1: An Observation
   • Step 2: Completeness for Surjections
   • Step 3: Irrelevance of the Restriction
Let $s \in \mathbb{F}_p^n$. The picture is as follows:

$$\mathbb{F}_p^n \ni a \approx s \cdot a \ni b = s \cdot a + e$$

**LWE, Informally**

Roughly, the Learning With Errors problem is to recover $s$ by sampling preimage-image pairs in the presence of some small "noise".
Let $s \in \mathbb{F}_p^n$. The picture is as follows:

$$\begin{align*}
\mathbb{F}_p^n & \ni s \\
\mathbb{F}_p & \ni a \\
\mathbb{F}_p & \ni b = s \cdot a + e
\end{align*}$$

LWE, Informally

Roughly, the Learning With Errors problem is to recover $s$ by sampling preimage-image pairs in the presence of some small “noise”
Let $s \in \mathbb{F}_p^n$. The picture is as follows:

$$\begin{align*}
\mathbb{F}_p^n & \ni s \\
\mathbb{F}_p & \ni a \\
\mathbb{F}_p & \ni b
\end{align*}$$

with

$$b \approx s \cdot a = s \cdot a + e$$

**LWE, Informally**

Roughly, the Learning With Errors problem is to recover $s$ by sampling preimage-image pairs in the presence of some small “noise”
More precisely, let

- \( s \in \mathbb{F}_p^n \)
- \( \Psi \) be a discrete gaussian distribution over \( \mathbb{F}_p \) centered at 0
- Define a distribution \( A_{s, \Psi} \) on \( \mathbb{F}_p^n \times \mathbb{F}_p \) whose samples are pairs \((a, b)\) where \( a \sim \mathbb{F}_p^n \), \( b = s \cdot a + e \), \( e \sim \Psi \)

**Definition (LWE Search)**

The Learning With Errors problem is to recover \( s \) by sampling the distribution \( A_{s, \Psi} \).

**Definition (LWE Decision)**

Distinguish the distribution \( A_{s, \Psi} \) from the uniform distribution \( U(\mathbb{F}_p^n \times \mathbb{F}_p) \).
More precisely, let

- \( s \in \mathbb{F}_p^n \)
- \( \psi \) be a discrete gaussian distribution over \( \mathbb{F}_p \) centered at 0
- Define a distribution \( A_{s,\psi} \) on \( \mathbb{F}_p^n \times \mathbb{F}_p \) whose samples are pairs \((a, b)\) where \( a \sim \mathbb{F}_p^n \), \( b = s \cdot a + e \), \( e \sim \psi \)

**Definition (LWE Search)**

The **Learning With Errors** problem is to recover \( s \) by sampling the distribution \( A_{s,\psi} \).

**Definition (LWE Decision)**

Distinguish the distribution \( A_{s,\psi} \) from the uniform distribution \( U(\mathbb{F}_p^n \times \mathbb{F}_p) \).
More precisely, let

- \( s \in \mathbb{F}_p^n \)
- \( \Psi \) be a discrete gaussian distribution over \( \mathbb{F}_p \) centered at 0

Define a distribution \( A_{s, \Psi} \) on \( \mathbb{F}_p^n \times \mathbb{F}_p \) whose samples are pairs \((a, b)\) where \( a \leftarrow \mathbb{F}_p^n \), \( b = s \cdot a + e \), \( e \leftarrow \Psi \)

**Definition (LWE Search)**

The **Learning With Errors** problem is to recover \( s \) by sampling the distribution \( A_{s, \Psi} \).

**Definition (LWE Decision)**

Distinguish the distribution \( A_{s, \Psi} \) from the uniform distribution \( U(\mathbb{F}_p^n \times \mathbb{F}_p) \).
More precisely, let

- $s \in \mathbb{F}_p^n$
- $\Psi$ be a discrete gaussian distribution over $\mathbb{F}_p$ centered at 0
- Define a distribution $A_{s,\Psi}$ on $\mathbb{F}_p^n \times \mathbb{F}_p$ whose samples are pairs $(a, b)$ where $a \leftarrow \mathbb{F}_p^n$, $b = s \cdot a + e$, $e \leftarrow \Psi$

### Definition (LWE Search)

The Learning With Errors problem is to recover $s$ by sampling the distribution $A_{s,\Psi}$.

### Definition (LWE Decision)

Distinguish the distribution $A_{s,\Psi}$ from the uniform distribution $\mathcal{U}(\mathbb{F}_p^n \times \mathbb{F}_p)$. 

More precisely, let

- \( s \in \mathbb{F}_p^n \)
- \( \Psi \) be a discrete gaussian distribution over \( \mathbb{F}_p \) centered at 0
- Define a distribution \( A_{s, \Psi} \) on \( \mathbb{F}_p^n \times \mathbb{F}_p \) whose samples are pairs \((a, b)\) where \( a \leftarrow \mathbb{F}_p^n, b = s \cdot a + e, e \leftarrow \Psi \)

**Definition (LWE Search)**

The **Learning With Errors** problem is to recover \( s \) by sampling the distribution \( A_{s, \Psi} \).

**Definition (LWE Decision)**

Distinguish the distribution \( A_{s, \Psi} \) from the uniform distribution \( U(\mathbb{F}_p^n \times \mathbb{F}_p) \).
More precisely, let

- \( s \in \mathbb{F}_p^n \)
- \( \Psi \) be a discrete gaussian distribution over \( \mathbb{F}_p \) centered at 0

Define a distribution \( A_{s,\Psi} \) on \( \mathbb{F}_p^n \times \mathbb{F}_p \) whose samples are pairs

\((a, b)\) where \( a \overset{\$}{\leftarrow} \mathbb{F}_p^n, b = s \cdot a + e, e \overset{\$}{\leftarrow} \Psi\)

**Definition (LWE Search)**

The Learning With Errors problem is to recover \( s \) by sampling the distribution \( A_{s,\Psi} \).

**Definition (LWE Decision)**

Distinguish the distribution \( A_{s,\Psi} \) from the uniform distribution \( U(\mathbb{F}_p^n \times \mathbb{F}_p) \).
Outline

1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
Observation

LWE’s formulation was mainly algebraic:

- Expressed in terms of homomorphisms
- Complexity reductions (worst case to average case, search to decision) also algebraic

This motivates the following

Question

Can similar learning problems yield viable intractability assumptions based on group theory?
Learning Homomorphisms With Errors

Observation
LWE’s formulation was mainly algebraic:
- Expressed in terms of homomorphisms
- Complexity reductions (worst case to average case, search to decision) also algebraic

This motivates the following

Question
Can similar learning problems yield viable intractability assumptions based on group theory?
Observation

LWE’s formulation was mainly algebraic:
- Expressed in terms of homomorphisms
- Complexity reductions (worst case to average case, search to decision) also algebraic

This motivates the following

Question

Can similar learning problems yield viable intractability assumptions based on group theory?
Learning Homomorphisms With Errors

Observation

LWE’s formulation was mainly algebraic:
- Expressed in terms of homomorphisms
- Complexity reductions (worst case to average case, search to decision) also algebraic

This motivates the following

Question

Can similar learning problems yield viable intractability assumptions based on group theory?
Observation
LWE’s formulation was mainly algebraic:
- Expressed in terms of homomorphisms
- Complexity reductions (worst case to average case, search to decision) also algebraic

This motivates the following

Question
Can similar learning problems yield viable intractability assumptions based on group theory?
LWE Over Groups \[\text{[BFNSS11]}\]

Vector Spaces

\[
\mathbb{F}_p^n \ni a \quad \Rightarrow \quad \mathbb{F}_p \ni s \cdot a + e
\]

Groups

\[
G_n \ni a \quad \Rightarrow \quad P_n \ni \varphi(a) e
\]
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n$, $\Psi_n$, distributions on $G_n$, $P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \leftarrow \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \leftarrow \Gamma_n$
- $e \leftarrow \Psi_n$
- $b = \varphi(a)e$
Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n$, $\Psi_n$, distributions on $G_n$, $P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \xleftarrow{\$} \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \xleftarrow{\$} \Gamma_n$;
- $e \xleftarrow{\$} \Psi_n$;
- $b = \varphi(a)e$
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n$, $\Psi_n$, distributions on $G_n$, $P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \xleftarrow{\$} \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \xleftarrow{\$} \Gamma_n$
- $e \xleftarrow{\$} \Psi_n$
- $b = \varphi(a)e$
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups.
- Set $\Gamma_n, \Psi_n$, distributions on $G_n, P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \xleftarrow{\$} \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \xleftarrow{\$} \Gamma_n$;
- $b \xleftarrow{\$} \Psi_n$;
- $b = \varphi(a)e$.
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n, \Psi_n$, distributions on $G_n, P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \leftarrow \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \leftarrow \Gamma_n$;
- $e \leftarrow \Psi_n$;
- $b = \varphi(a)e$
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n$, $\Psi_n$, distributions on $G_n$, $P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \leftarrow \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \leftarrow \Gamma_n$;
- $e \leftarrow \Psi_n$;
- $b = \varphi(a)e$
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n, \Psi_n$, distributions on $G_n, P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi,\psi_n}$

For $\varphi \leftarrow \Phi_n$, define the analogous distribution $A_{\varphi,\psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \leftarrow \Gamma_n$;
- $e \leftarrow \Psi_n$;
- $b = \varphi(a)e$
Learning Homomorphisms from Images with Errors

Setup

- Let $G_n$ and $P_n$ be groups
- Set $\Gamma_n$, $\Psi_n$, distributions on $G_n$, $P_n$, resp.
- Let $\Phi_n$ be a distribution on the set of all homomorphisms, $\text{hom}(G_n, P_n)$

The Distribution $A_{\varphi, \psi_n}$

For $\varphi \leftarrow \Phi_n$, define the analogous distribution $A_{\varphi, \psi_n}$ on $G_n \times P_n$ whose samples are $(a, b)$ where

- $a \leftarrow \Gamma_n$;
- $e \leftarrow \Psi_n$;
- $b = \varphi(a)e$
Learning Homomorphisms from Images with Errors

Search Problem
Given $A_{\varphi, \psi_n}$, recover $\varphi$.

Decision Problem
Given samples from an unknown distribution $R \in \{A_{\varphi, \psi_n}, U(G_n \times P_n)\}$, determine $R$.

Hardness Assumption (Decision Version)
$$A_{\varphi, \psi_n} \approx_{\text{PPT}} U(G_n \times P_n)$$
Learning Homomorphisms from Images with Errors

**Search Problem**

Given $A_{\varphi, \psi_n}$, recover $\varphi$.

**Decision Problem**

Given samples from an unknown distribution $R \in \{A_{\varphi, \psi_n}, \mathcal{U}(G_n \times P_n)\}$, determine $R$.

**Hardness Assumption (Decision Version)**

$A_{\varphi, \psi_n} \approx_{\text{PPT}} \mathcal{U}(G_n \times P_n)$
Learning Homomorphisms from Images with Errors

<table>
<thead>
<tr>
<th>Search Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given $A_{\varphi,\psi_n}$, recover $\varphi$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Decision Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given samples from an unknown distribution $R \in {A_{\varphi,\psi_n}, U(G_n \times P_n)}$, determine $R$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardness Assumption (Decision Version)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_{\varphi,\psi_n} \approx_{\text{PPT}} U(G_n \times P_n)$</td>
</tr>
</tbody>
</table>
1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
Question

For which groups (if any) does the abstract problem make sense?

- The authors of [BFNS11] suggested the use of free Burnside groups.
- We’ll review some of the intuition for this choice, as well as some of the key facts about these groups below.
Question

For which groups (if any) does the abstract problem make sense?

- The authors of [BFNS11] suggested the use of free Burnside groups.
- We’ll review some of the intuition for this choice, as well as some of the key facts about these groups below.
Question
For which groups (if any) does the abstract problem make sense?

- The authors of [BFNS11] suggested the use of free Burnside groups.
- We’ll review some of the intuition for this choice, as well as some of the key facts about these groups below.
The free Burnside groups can be thought of as living in a certain variety of groups.

**Variety of Groups (Informal)**

Roughly speaking, a **variety** is the class of all groups whose elements satisfy a certain set of equations.

**Example**

Abelian groups can be seen as the variety corresponding to the equation

\[ XY = YX. \]

The Burnside groups live in the variety defined by the equation

\[ X^m = 1. \]
The free Burnside groups can be thought of as living in a certain variety of groups.

**Variety of Groups (Informal)**

Roughly speaking, a *variety* is the class of all groups whose elements satisfy a certain set of equations.

**Example**

Abelian groups can be seen as the variety corresponding to the equation

\[ XY = YX. \]

The Burnside groups live in the variety defined by the equation \( X^m = 1 \).
The free Burnside groups can be thought of as living in a certain variety of groups.

**Variety of Groups (Informal)**
Roughly speaking, a *variety* is the class of all groups whose elements satisfy a certain set of equations.

**Example**
Abelian groups can be seen as the variety corresponding to the equation

\[ XY = YX. \]

The Burnside groups live in the variety defined by the equation \( X^m = 1 \).
The free Burnside groups can be thought of as living in a certain variety of groups.

**Variety of Groups (Informal)**

Roughly speaking, a **variety** is the class of all groups whose elements satisfy a certain set of equations.

**Example**

Abelian groups can be seen as the variety corresponding to the equation

\[ XY = YX. \]

The Burnside groups live in the variety defined by the equation \( X^m = 1 \).
Via the usual “abstract nonsense”, it is easy to see that varieties of groups contain free objects—just take a free group and factor out the normal subgroup resulting from all the “equations”...
Via the usual “abstract nonsense”, it is easy to see that varieties of groups contain free objects—just take a free group and factor out the normal subgroup resulting from all the “equations”...
Question

Which varieties of groups contain finite free objects???

If the equations are say,

\[
[X, Y] = 1 \\
X^p = 1
\]

then the free objects are exactly \( \mathbb{Z}_p \), which are the objects of study in LWE (if \( p \) is prime).

Question

What happens if the \([X, Y] = 1\) equation is removed? In general, the answer is not so simple...

\(^a\)Note: \([X, Y] = X^{-1} Y^{-1} XY\).
Varieties of Groups

Question

Which varieties of groups contain finite free objects???

If the equations are say,

\[
[X, Y] = 1 \\
X^p = 1
\]

then the free objects are exactly \(\mathbb{Z}_p^n\), which are the objects of study in LWE (if \(p\) is prime).

Question

What happens if the \([X, Y] = 1\) equation is removed? In general, the answer is not so simple...

\(^a\)Note: \([X, Y] = X^{-1} Y^{-1} XY\).
Question
Which varieties of groups contain finite free objects???

If the equations are say,

\[ [X, Y] = 1 \]
\[ X^p = 1 \]

then the free objects are exactly \( \mathbb{Z}_p^n \), which are the objects of study in LWE (if \( p \) is prime).

Question
What happens if the \([X, Y] = 1\) equation is removed?\(^a\) In general, the answer is not so simple...

\(^a\)Note: \([X, Y] = X^{-1}Y^{-1}XY\).
Notation

For the variety of groups defined by the equation $X^m = 1$, denote the free group on $n$ generators in this variety by $B(n, m)$.

Determining the finiteness of $B(n, m)$ is known as the Bounded Burnside Problem.
Notation

For the variety of groups defined by the equation $X^m = 1$, denote the free group on $n$ generators in this variety by $B(n, m)$.

Determining the finiteness of $B(n, m)$ is known as the **Bounded Burnside Problem**.
For $n > 1$ and for sufficiently large $m$, it is known that $|B(n, m)| = \infty$, yet for small $m$, our understanding is far from complete:

\begin{align*}
B(n, 2) & \quad \text{Finite (also abelian)} \\
B(n, 3) & \quad \text{Finite} \\
B(n, 4) & \quad \text{Finite} \\
B(n, 5) & \quad \text{Unknown} \\
B(n, 6) & \quad \text{Finite} \\
B(n, 7) & \quad \text{Unknown} \\
\vdots & \quad \vdots
\end{align*}
The authors of [BFNSS11] chose to use $B(n, 3)$ to instantiate the abstract LHN problem.

- It’s finite
- It’s the smallest non-abelian case
- The structure of $B(3, n)$ is fairly well understood

From here out, we’ll denote $B(3, n)$ by $B_n$ for brevity.
The authors of [BFNSS11] chose to use $B(n, 3)$ to instantiate the abstract LHN problem.

- It’s finite
  - It’s the smallest non-abelian case
  - The structure of $B(3, n)$ is fairly well understood
- From here out, we’ll denote $B(3, n)$ by $B_n$ for brevity.
The authors of [BFNSS11] chose to use $B(n, 3)$ to instantiate the abstract LHN problem.

- It’s finite
- It’s the smallest non-abelian case
- The structure of $B(3, n)$ is fairly well understood

From here out, we’ll denote $B(3, n)$ by $B_n$ for brevity.
The authors of [BFNSS11] chose to use $B(n, 3)$ to instantiate the abstract LHN problem.

- It’s finite
- It’s the smallest non-abelian case
- The structure of $B(3, n)$ is fairly well understood

From here out, we’ll denote $B(3, n)$ by $B_n$ for brevity.
The authors of [BFNSS11] chose to use $B(n, 3)$ to instantiate the abstract LHN problem.

- It’s finite
- It’s the smallest non-abelian case
- The structure of $B(3, n)$ is fairly well understood

From here out, we’ll denote $B(3, n)$ by $B_n$ for brevity.
The $B_n$-LHN Problem

This is simply the LHN problem, instantiated with free Burnside groups.

- The homomorphisms are sampled uniformly from $\text{hom}(B_n, B_r)$.
- We’ll ignore the error distribution for the moment, since those details are not important to the reduction.
The $B_n$-LHN Problem

This is simply the LHN problem, instantiated with free Burnside groups.

- The homomorphisms are sampled uniformly from $\text{hom}(B_n, B_r)$.
- We’ll ignore the error distribution for the moment, since those details are not important to the reduction.
The $B_n$-LHN Problem

This is simply the LHN problem, instantiated with free Burnside groups.

- The homomorphisms are sampled uniformly from $\text{hom}(B_n, B_r)$.
- We’ll ignore the error distribution for the moment, since those details are not important to the reduction.
1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
We can break the argument into 3 easy steps:

1. Start with a simple observation for a partial randomization.
2. Show this randomization is complete for a restricted version of the problem.
3. Show that the restricted version is statistically equivalent to the original problem.

Hence the reduction applies to the original problem as well. Any efficient algorithm that solves the modified problem would solve the original; no efficient procedure can do anything substantially different on one versus the other.
We can break the argument into 3 easy steps:

1. Start with a simple observation for a partial randomization.
2. Show this randomization is complete for a restricted version of the problem.
3. Show that the restricted version is statistically equivalent to the original problem.

Hence the reduction applies to the original problem as well. Any efficient algorithm that solves the modified problem would solve the original, no efficient procedure can do anything substantially different on one versus the other.
We can break the argument into 3 easy steps:

1. Start with a simple observation for a partial randomization.
2. Show this randomization is complete for a restricted version of the problem.
3. Show that the restricted version is statistically equivalent to the original problem.

Hence the reduction applies to the original problem as well. Any efficient algorithm that solves the modified problem would solve the original; no efficient procedure can do anything substantially different on one versus the other.
We can break the argument into 3 easy steps:

1. Start with a simple observation for a partial randomization.
2. Show this randomization is complete for a restricted version of the problem.
3. Show that the restricted version is statistically equivalent to the original problem.

- Hence the reduction applies to the original problem as well.
- Any efficient algorithm that solves the modified problem would solve the original—no efficient procedure can do anything substantially different on one versus the other.
We can break the argument into 3 easy steps:

1. Start with a simple observation for a partial randomization.
2. Show this randomization is complete for a restricted version of the problem.
3. Show that the restricted version is statistically equivalent to the original problem.

- Hence the reduction applies to the original problem as well
- Any efficient algorithm that solves the modified problem would solve the original—no efficient procedure can do anything substantially different on one versus the other.
We can break the argument into 3 easy steps:

1. Start with a simple observation for a partial randomization.
2. Show this randomization is complete for a restricted version of the problem.
3. Show that the restricted version is statistically equivalent to the original problem.

- Hence the reduction applies to the original problem as well
- Any efficient algorithm that solves the modified problem would solve the original- no efficient procedure can do anything substantially different on one versus the other.
1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
An Observation

**Lemma**

Let $(a, b = \varphi(a) \cdot e) \in G_n \times P_n$ be an instance of LHN sampled according to $A_{\psi_n}^\Psi$, and $\alpha$ be a permutation of $G_n$. It holds that $(a', b) = (\alpha(a), b) \in G_n \times P_n$ is sampled according to $A_{\varphi \circ \alpha^{-1}}^\Psi$. 

**Proof.**

Observe that

\[(a' = \alpha(a), b) = (\alpha(a), \varphi(a) \cdot e) = (\alpha(a), \varphi \circ \alpha^{-1}(\alpha(a)) \cdot e) = (a', \varphi \circ \alpha^{-1}(a') \cdot e).\]
Lemma

Let \((a, b = \varphi(a) \cdot e) \in G_n \times P_n\) be an instance of LHN sampled according to \(A_{\psi_n}\), and \(\alpha\) be a permutation of \(G_n\). It holds that \((a', b) = (\alpha(a), b) \in G_n \times P_n\) is sampled according to \(A_{\psi_n}^{\varphi \circ \alpha^{-1}}\).

Proof.

Observe that

\[
(a' = \alpha(a), b) = (\alpha(a), \varphi(a) \cdot e) = (\alpha(a), \varphi \circ \alpha^{-1}(\alpha(a)) \cdot e) = (a', \varphi \circ \alpha^{-1}(a') \cdot e).
\]
So, we can take instances from any $A_{\psi^n}$ and transform them to instances from $A_{\psi^n \circ \alpha}$ for some bijection $\alpha$, giving at least a partial randomization.

Next, we show that this randomization is complete for a subset of homomorphisms...
An Observation

So, we can take instances from any $A_{\Psi^n}$ and transform them to instances from $A_{\varphi^n \circ \alpha}$ for some bijection $\alpha$, giving at least a partial randomization.

Next, we show that this randomization is complete for a subset of homomorphisms...
Outline

1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
Completeness of the Randomization

Observation
Right-composition by an automorphism will not change the image of $\varphi$.

- Okay, so the technique from the lemma will not suffice to randomize all instances, but what about surjective homomorphisms???
- The following would be ideal:

Lemma
The action of $\text{Aut}(B_n)$ on $\text{Epi}(B_n, B_r)$ is transitive.

- This is true, but requires some work...
- Wait- what’s this about “work”, you say? I know... but still, $\frac{2}{3}$ easy steps isn’t so bad : )
Observation

Right-composition by an automorphism will not change the image of $\varphi$.

Okay, so the technique from the lemma will not suffice to randomize all instances, but what about surjective homomorphisms???

The following would be ideal:

Lemma

The action of $\text{Aut}(B_n)$ on $\text{Epi}(B_n, B_r)$ is transitive.

This is true, but requires some work...

Wait- what’s this about “work”, you say? I know... but still, $\frac{2}{3}$ easy steps isn’t so bad : )
Completeness of the Randomization

**Observation**
Right-composition by an automorphism will not change the image of $\varphi$.

- Okay, so the technique from the lemma will not suffice to randomize all instances, but what about **surjective homomorphisms??**
- The following would be ideal:

**Lemma**
The action of $\text{Aut}(B_n)$ on $\text{Epi}(B_n, B_r)$ is transitive.

- This is true, but requires some work...
- Wait- what’s this about “work”, you say? I know... but still, $\frac{2}{3}$ easy steps isn’t so bad : )
Completeness of the Randomization

**Observation**
Right-composition by an automorphism will not change the image of $\varphi$.

- Okay, so the technique from the lemma will not suffice to randomize all instances, but what about **surjective homomorphisms**???
- The following would be ideal:

**Lemma**
The action of $\text{Aut}(B_n)$ on $\text{Epi}(B_n, B_r)$ is transitive.

- This is true, but requires some work...
- Wait- what’s this about “work”, you say? I know... but still, $\frac{2}{3}$ easy steps isn’t so bad : )
Observation
Right-composition by an automorphism will not change the image of $\varphi$.

- Okay, so the technique from the lemma will not suffice to randomize all instances, but what about surjective homomorphisms???
- The following would be ideal:

Lemma
The action of $\text{Aut}(B_n)$ on $\text{Epi}(B_n, B_r)$ is transitive.

- This is true, but requires some work...
  - Wait- what’s this about “work”, you say? I know... but still, $\frac{2}{3}$ easy steps isn’t so bad : )
Completeness of the Randomization

**Observation**
Right-composition by an automorphism will not change the image of $\phi$.

- Okay, so the technique from the lemma will not suffice to randomize all instances, but what about **surjective homomorphisms**???
- The following would be ideal:

**Lemma**

*The action of $\text{Aut}(B_n)$ on $\text{Epi}(B_n, B_r)$ is transitive.*

- This is true, but requires some work...
- Wait- what’s this about “work”, you say? I know... but still, $\frac{2}{3}$ easy steps isn’t so bad : )
Consider the following commutative diagram, where $\rho$ is the projection on to the commutator factor, taking $B_n \longrightarrow B_n/[B_n, B_n] \cong (\mathbb{F}_3^n, +)$:

The main technical lemma used to prove transitivity is the following:

**Lemma**

Surjections from $B_n \longrightarrow B_r$ are precisely the maps whose abelianization is also surjective.
Proving Transitivity

Consider the following commutative diagram, where $\rho$ is the projection on to the commutator factor, taking $B_n \rightarrow B_n/[B_n, B_n] \cong (\mathbb{F}_3^n, +)$:

\[
\begin{array}{ccc}
B_n & \xrightarrow{\rho} & \mathbb{F}_3^n \\
\downarrow{\varphi} & & \downarrow{\overline{\varphi}} \\
B_r & \xrightarrow{\rho} & \mathbb{F}_3^r
\end{array}
\]

The main technical lemma used to prove transitivity is the following:

**Lemma**

*Surjections from $B_n \rightarrow B_r$ are precisely the maps whose abelianization is also surjective.*
Consider the following commutative diagram, where $\rho$ is the projection onto the commutator factor, taking $B_n \twoheadrightarrow B_n/[B_n, B_n] \cong (\mathbb{F}_3^n, +)$:

\[
\begin{array}{ccc}
B_n & \xrightarrow{\rho} & \mathbb{F}_3^n \\
\downarrow{\varphi} & & \downarrow{\overline{\varphi}} \\
B_r & \xrightarrow{\rho} & \mathbb{F}_3^r
\end{array}
\]

The main technical lemma used to prove transitivity is the following:

**Lemma**

*Surjections from $B_n \twoheadrightarrow B_r$ are precisely the maps whose abelianization is also surjective.*
The proof is somewhat involved, and makes use of some specific details of the structure of free Burnside groups.

However, some of the details can be abstracted away by a few invocations of the Five Lemma.
Consider the following commutative diagram, where the rows are exact.

\[ \begin{array}{cccccc}
A & \rightarrow & B & \rightarrow & C & \rightarrow & D & \rightarrow & E \\
\downarrow e & & \downarrow f & & \downarrow g & & \downarrow h & & \downarrow i \\
A' & \rightarrow & B' & \rightarrow & C' & \rightarrow & D' & \rightarrow & E'
\end{array} \]

**Lemma (Five Lemma)**

The five lemma states that if \( e \) is surjective and \( i \) is injective, then if \( f \) and \( h \) are isomorphisms, so is \( g \). Furthermore, if \( i \) is injective and \( f \) and \( h \) are surjective, then \( g \) is also surjective.\(^a\)

\(^a\)Dually, if \( e \) is surjective and \( f, h \) injective, then \( g \) is also injective.
The Five Lemma

Consider the following commutative diagram, where the rows are exact.

\[
\begin{array}{cccccc}
A & \rightarrow & B & \rightarrow & C & \rightarrow & D & \rightarrow & E \\
\downarrow e & & \downarrow f & & \downarrow g & & \downarrow h & & \downarrow i \\
A' & \rightarrow & B' & \rightarrow & C' & \rightarrow & D' & \rightarrow & E'
\end{array}
\]

**Lemma (Five Lemma)**

The five lemma states that if \( e \) is surjective and \( i \) is injective, then if \( f \) and \( h \) are isomorphisms, so is \( g \). Furthermore, if \( i \) is injective and \( f \) and \( h \) are surjective, then \( g \) is also surjective.\(^a\)

\(^a\)Dually, if \( e \) is surjective and \( f, h \) injective, then \( g \) is also injective.
Proving the Lemma

We’ll apply the lemma to the following diagram:

\[
\begin{array}{cccccc}
0 & \rightarrow & [B_n, B_n] & \xrightarrow{i} & B_n & \xrightarrow{\rho} & \mathbb{F}_3^n & \rightarrow & 0 \\
\downarrow{\hat{\varphi}} & & \downarrow{\varphi} & & \downarrow{\overline{\varphi}} & & & & \\
0 & \rightarrow & [B_r, B_r] & \xrightarrow{i} & B_r & \xrightarrow{\rho} & \mathbb{F}_3^r & \rightarrow & 0
\end{array}
\]

(1)

- By the Five Lemma, proving \( \hat{\varphi} \) is onto would suffice to prove our lemma, since then \( \varphi \) would be onto as well.
- Intuitively, dealing with the restriction to \([B_n, B_n]\) should be easier than the original map \( \varphi \).\(^1\)

\(^1\)We actually invoke the five lemma yet again to show that \( \hat{\varphi} \) is surjective...
We’ll apply the lemma to the following diagram:

\[
\begin{array}{cccccc}
0 & \rightarrow & [B_n, B_n] & \xrightarrow{i} & B_n & \xrightarrow{\rho} & \mathbb{F}_3^n & \rightarrow & 0 \\
\downarrow{\hat{\varphi}} & & \downarrow{\varphi} & & \downarrow{\overline{\varphi}} & & & \\
0 & \rightarrow & [B_r, B_r] & \xrightarrow{i} & B_r & \xrightarrow{\rho} & \mathbb{F}_3^r & \rightarrow & 0
\end{array}
\] (1)

- By the Five Lemma, proving \( \hat{\varphi} \) is onto would suffice to prove our lemma, since then \( \varphi \) would be onto as well.

- Intuitively, dealing with the restriction to \([B_n, B_n]\) should be easier than the original map \( \varphi \).\(^1\)

\(^1\)We actually invoke the five lemma yet again to show that \( \hat{\varphi} \) is surjective...
We’ll apply the lemma to the following diagram:

\[
\begin{array}{ccccccccc}
0 & \rightarrow & [B_n, B_n] & \overset{i}{\rightarrow} & B_n & \overset{\rho}{\rightarrow} & \mathbb{F}_3^n & \rightarrow & 0 \\
\downarrow{\hat{\varphi}} & & \downarrow{\varphi} & & \downarrow{\overline{\varphi}} & & & & \\
0 & \rightarrow & [B_r, B_r] & \overset{i}{\rightarrow} & B_r & \overset{\rho}{\rightarrow} & \mathbb{F}_3^r & \rightarrow & 0
\end{array}
\] (1)

- By the Five Lemma, proving \( \hat{\varphi} \) is onto would suffice to prove our lemma, since then \( \varphi \) would be onto as well.
- Intuitively, dealing with the restriction to \([B_n, B_n]\) should be easier than the original map \( \varphi \).\(^1\)

\(^1\)We actually invoke the five lemma yet again to show that \( \hat{\varphi} \) is surjective...
Now Back to Transitivity...

We proceed in a straightforward manner:

**Goal**

Given an arbitrary epimorphism $\varphi$ and a target epimorphism $\varphi^*$ we want to find an automorphism $\alpha$ such that

$$\varphi^* = \varphi \circ \alpha.$$
We proceed in a straightforward manner:

**Goal**

Given an arbitrary epimorphism $\varphi$ and a target epimorphism $\varphi^*$ we want to find an automorphism $\alpha$ such that

$$\varphi^* = \varphi \circ \alpha.$$
Proving Transitivity

We’d like to find an automorphism $\alpha$ so that the following diagram commutes:

\[
\begin{array}{ccc}
0 & \rightarrow & K \\
\downarrow \rho & & \downarrow \rho \\
F_3^n & \rightarrow & B_n \\
\downarrow \varphi & & \downarrow \varphi \\
F_3 & \rightarrow & 0 \\
\end{array}
\]

\[
\begin{array}{ccc}
B_n & \xrightarrow{\varphi^*} & B_r \\
\downarrow \rho & & \downarrow \rho \\
F_3^n & \rightarrow & F_3' \\
\downarrow \varphi' & & \downarrow \varphi' \\
K & \xrightarrow{\alpha} & 0 \\
\end{array}
\]

(2)
The idea is simple—after all, $B_n$ is free!

This allows us to define $\alpha$ to explicitly send basis elements where they need to go to make the composition work.
From the fact that $B_n$ is free, we know that such an $\alpha$ exists. With the help of the previous lemma, we can show there is always a way to choose $\alpha$ to be bijective.
From the fact that $B_n$ is free, we know that such an $\alpha$ exists. With the help of the previous lemma, we can show there is always a way to choose $\alpha$ to be bijective.
All that remains to show RSR for our restricted problem is to show the following

**Lemma**

Let $G$ be a finite group, and $S$ a set on which $G$ acts transitively. Let $s \in S$ be an arbitrary element, and consider the distribution $A_s$ on $S$ whose samples are $g \cdot s$ where $g \leftarrow U(G)$. Then $A_s = U(S)$.

**Proof.**

A simple counting argument (say, using the orbit-stabilizer theorem) suffices to show that each element $t \in S$ has the same number of preimages under the map from $G \rightarrow S$ defined by $g \mapsto g \cdot s$. 
All that remains to show RSR for our restricted problem is to show the following

**Lemma**

Let $G$ be a finite group, and $S$ a set on which $G$ acts transitively. Let $s \in S$ be an arbitrary element, and consider the distribution $A_s$ on $S$ whose samples are $g \cdot s$ where $g \sim U(G)$. Then $A_s = U(S)$.

**Proof.**

A simple counting argument (say, using the orbit-stabilizer theorem) suffices to show that each element $t \in S$ has the same number of preimages under the map from $G \rightarrow S$ defined by $g \mapsto g \cdot s$. 
All that remains to show RSR for our restricted problem is to show the following

**Lemma**

Let $G$ be a finite group, and $S$ a set on which $G$ acts transitively. Let $s \in S$ be an arbitrary element, and consider the distribution $A_s$ on $S$ whose samples are $g \cdot s$ where $g \overset{\$}{\leftarrow} U(G)$. Then $A_s = U(S)$.

**Proof.**

A simple counting argument (say, using the orbit-stabilizer theorem) suffices to show that each element $t \in S$ has the same number of preimages under the map from $G \rightarrow S$ defined by $g \mapsto g \cdot s$. 
Outline

1 Motivation & Background
   - Why Group-Theoretic Cryptography?
   - Random self-reducibility

2 Learning Problems Over Burnside Groups
   - Background: LWE
   - LHN Problem
   - Burnside Groups and $B_n$-LHN

3 The Reduction, in 3 Easy Steps
   - Step 1: An Observation
   - Step 2: Completeness for Surjections
   - Step 3: Irrelevance of the Restriction
Most homomorphisms $\varphi : B_n \rightarrow B_r$ are surjective.

In fact, if there is just a superlogarithmic gap between $r$ and $n$ then non-surjective maps comprise only a negligible fraction of the set of all homomorphisms.

Even a crude estimate gives a $3^{r-n}$ fraction of all homomorphisms being non-surjective.
Most homomorphisms $\varphi : B_n \rightarrow B_r$ are surjective.

In fact, if there is just a superlogarithmic gap between $r$ and $n$ then non-surjective maps comprise only a negligible fraction of the set of all homomorphisms.

Even a crude estimate gives a $3^{r-n}$ fraction of all homomorphisms being non-surjective.
Most homomorphisms $\varphi : B_n \rightarrow B_r$ are surjective.

In fact, if there is just a superlogarithmic gap between $r$ and $n$ then non-surjective maps comprise only a negligible fraction of the set of all homomorphisms.

Even a crude estimate gives a $3^{r-n}$ fraction of all homomorphisms being non-surjective.
As a result, the altered distribution of instances (coming from sampling uniform surjective maps) is statistically close to the uniform distribution $U(\text{hom}(B_n, B_r))$. In general,

**Observation**

For any $X_n \subset S_n$,

$$\Delta(U(X_n), U(S_n)) = \frac{|S_n \setminus X_n|}{|S_n|}$$

Hence, whenever $\nu(n) = \frac{|S_n \setminus X_n|}{|S_n|}$ is negligible in $n$ (as in our case), then the ensemble of distributions $U(X_n)$ is statistically close to $U(S_n)$. 
As a result, the altered distribution of instances (coming from sampling uniform surjective maps) is statistically close to the uniform distribution $U(\text{hom}(B_n, B_r))$. In general,

\[
\Delta(U(X_n), U(S_n)) = \left| \frac{S_n \setminus X_n}{|S_n|} \right|
\]

Hence, whenever $\nu(n) = \frac{|S_n \setminus X_n|}{|S_n|}$ is negligible in $n$ (as in our case), then the ensemble of distributions $U(X_n)$ is statistically close to $U(S_n)$.
The modified problem is no different than the original from a computational perspective

- Any efficient algorithm breaking the modified scheme could be used to break the original scheme (and vice versa).
- This proves the random self reducibility of the $B_n$-LHN problem.
Irrelevance of the Restriction

- The modified problem is no different than the original from a computational perspective.
- Any efficient algorithm breaking the modified scheme could be used to break the original scheme (and vice versa).
- This proves the random self reducibility of the $B_n$-LHN problem.
Irrelevance of the Restriction

- The modified problem is no different than the original from a computational perspective.
- Any efficient algorithm breaking the modified scheme could be used to break the original scheme (and vice versa).
- This proves the random self reducibility of the $B_n$-LHN problem.
Upper bounds on complexity of $B_n$-LHN?

More complexity reductions: Search to decision?
Work in Progress / Open Questions

- Upper bounds on complexity of $B_n$-LHN?
- More complexity reductions: Search to decision?