Robust Coin Flipping

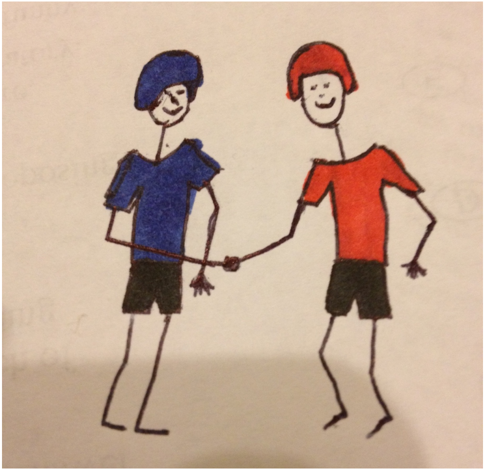
Gene Kopp and John Wiltshire-Gordon

University of Michigan

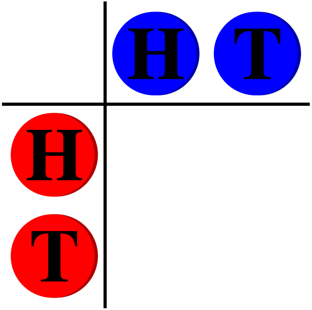
gkopp@umich.edu
jwiltshiregordon@umich.edu

April 15, 2012

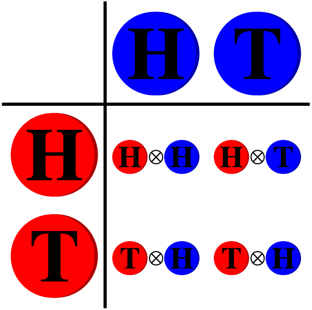
Sport Match



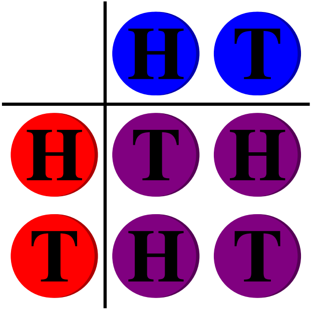
Sport Match



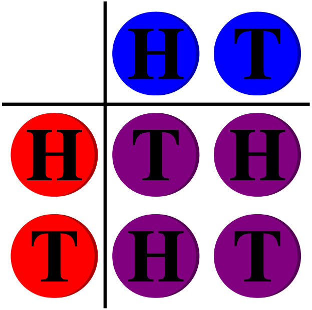
Sport Match



Sport Match

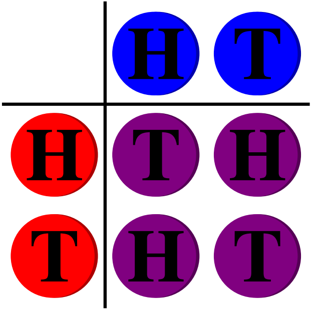


Sport Match



Probability of **H**?

Sport Match

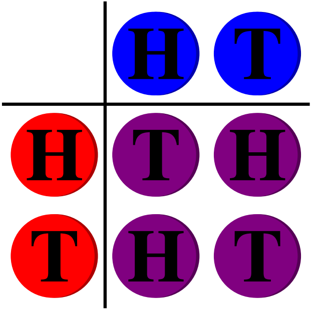


Probability of 

?

$\frac{1}{2}$ $\frac{1}{2}$

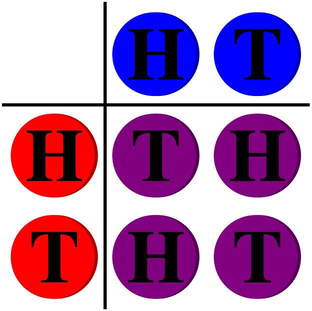
Sport Match



Probability of H?

$\frac{1}{2} \cdot 0.73 + \frac{1}{2} \cdot 0.27$

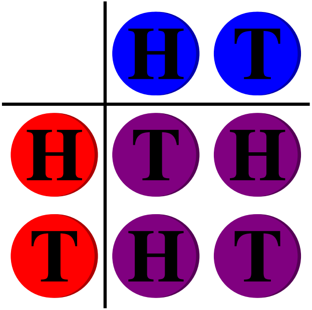
Sport Match



Probability of H?

$$\frac{1}{2} \cdot 0.73 + \frac{1}{2} \cdot 0.27 = \frac{1}{2}$$

Sport Match

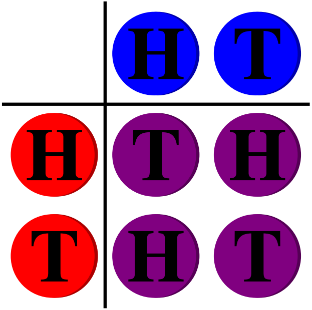


Probability of H?

$$\frac{1}{2} \cdot 0.73 + \frac{1}{2} \cdot 0.27 = \frac{1}{2}$$

0.64 0.36

Sport Match

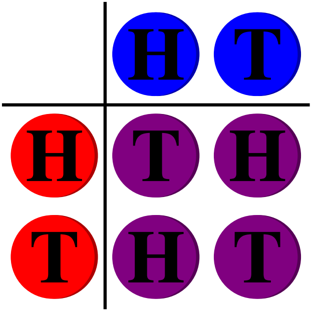


Probability of H?

$$\frac{1}{2}\cdot 0.73+\frac{1}{2}\cdot 0.27=\frac{1}{2}$$

$$0.64\cdot\frac{1}{2}+0.36\cdot\frac{1}{2}$$

Sport Match



Probability of H?

$\frac{1}{2} \cdot 0.73 + \frac{1}{2} \cdot 0.27 = \frac{1}{2}$

$0.64 \cdot \frac{1}{2} + 0.36 \cdot \frac{1}{2} = \frac{1}{2}$

Sport Match

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0.73 \\ 0.27 \end{pmatrix} = \frac{1}{2}$$

Sport Match

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0.73 \\ 0.27 \end{pmatrix} = \frac{1}{2}$$

$$\begin{pmatrix} 0.64 & 0.26 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \frac{1}{2}$$

The Hero of the Sport Match

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0.73 \\ 0.27 \end{pmatrix} = \frac{1}{2}$$

$$\begin{pmatrix} 0.64 & 0.26 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \frac{1}{2}$$

The Hero of the Sport Match

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The Hero of the Sport Match

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This bilinear operator encodes the operation "XOR"

The Hero of the Sport Match

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This bilinear operator encodes the operation "XOR"
Once you discover A the problem is easy.

Philosophy: Three Easy Steps

1. Begin with a natural cryptological problem

Philosophy: Three Easy Steps

1. Begin with a natural cryptological problem
2. Recast problem in terms of multilinear algebra:

Philosophy: Three Easy Steps

1. Begin with a natural cryptological problem
2. Recast problem in terms of multilinear algebra:

"Does there exist a multilinear operator with these properties? If so, can I construct one?"

Philosophy: Three Easy Steps

1. Begin with a natural cryptological problem
2. Recast problem in terms of multilinear algebra:
"Does there exist a multilinear operator with these properties? If so, can I construct one?"
3. Draw on a rich array of techniques in algebraic geometry to to find or disprove the key multilinear operator

The Robust Coin Flipping Problem

The problem we solved is *fun*

The Robust Coin Flipping Problem

The problem we solved is *fun*
But...

The Robust Coin Flipping Problem

The problem we solved is *fun*
But...
We hope to convince you that
the techniques are *serious* and *practical*.

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

q of them are faulty;

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

q of them are faulty;

r of them are reliable.

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

q of them are faulty;

r of them are reliable.

And the two types are indistinguishable!

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

q of them are faulty;

r of them are reliable.

And the two types are indistinguishable!

She wishes to generate a coin flip such that

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

  q of them are faulty;

  r of them are reliable.

And the two types are indistinguishable!

She wishes to generate a coin flip such that

  the probability of heads is α

The Robust Coin Flipping Problem

Alice has $p = q + r$ programmable random sources:

  q of them are faulty;

  r of them are reliable.

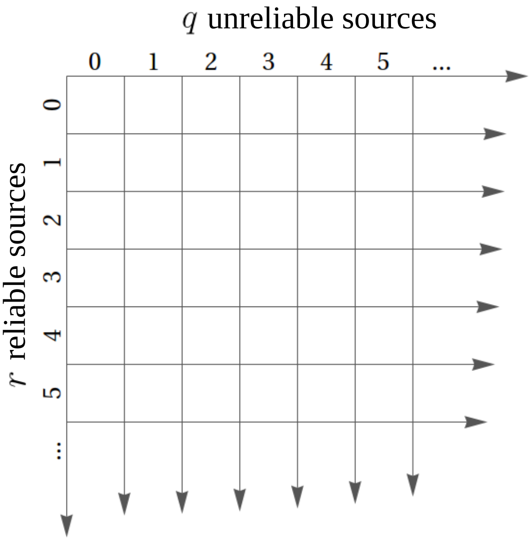
And the two types are indistinguishable!

She wishes to generate a coin flip such that

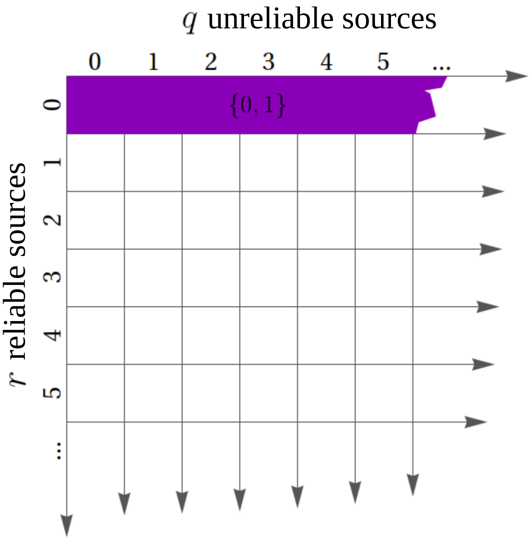
  the probability of heads is α

  the probability of tails is $1 - \alpha$.

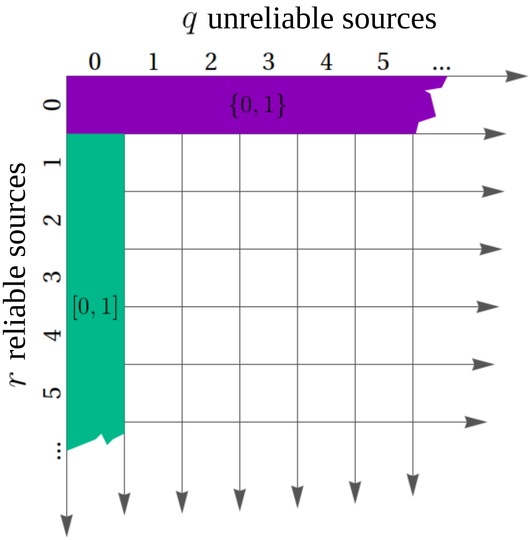
Results



Results

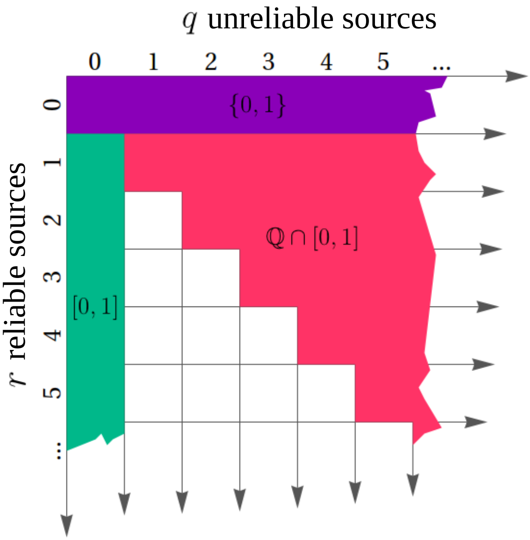


Results



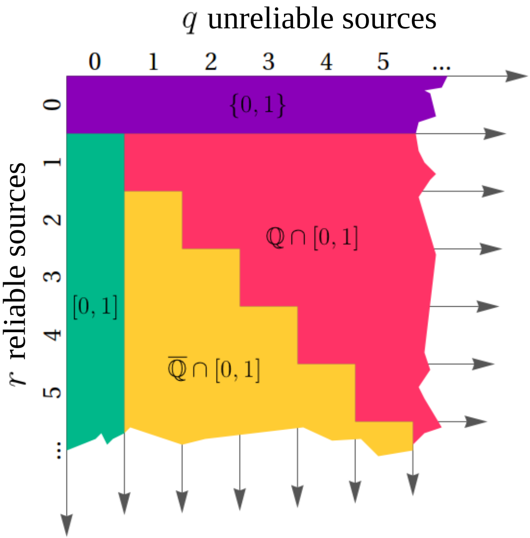
q unreliable sources
0 1 2 3 4 5 ...
r reliable sources
0 1 2 3 4 5 ...
$\{0, 1\}$
$[0, 1]$

Results



q unreliable sources
0 1 2 3 4 5 ...
r reliable sources
0 1 2 3 4 5 ...
$\{0,1\}$
$\mathbb{Q} \cap [0,1]$
$[0,1]$

Results



q unreliable sources
0
1
2
3
4
5
...
r reliable sources
0
1
2
3
4
5
...
$\{0, 1\}$
$[0, 1]$
$\mathbb{Q} \cap [0, 1]$
$\overline{\mathbb{Q}} \cap [0, 1]$

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.
- Alice programs source i to pick x_i from $\mathbb{Z}/b\mathbb{Z}$ with the uniform distribution.

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.
- Alice programs source i to pick x_i from $\mathbb{Z}/b\mathbb{Z}$ with the uniform distribution.
- Heads if $\sum_{i=1}^{p} x_i \in \{0, ..., a-1\}$; tails otherwise.

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.
- Alice programs source i to pick x_i from $\mathbb{Z}/b\mathbb{Z}$ with the uniform distribution.
- Heads if $\sum_{i=1}^{p} x_i \in \{0, ..., a-1\}$; tails otherwise.

Works if even one source is reliable (i.e. if $r \geq 1$)

When $p = 2$, Every α is Rational

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0.73 \\ 0.27 \end{pmatrix} = \frac{1}{2}$$

$$\begin{pmatrix} 0.64 & 0.26 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \frac{1}{2}$$

When $p = 2$, Every α is Rational

Lemma

Any bilinear form A has at most one associated α.

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0.73 \\ 0.27 \end{pmatrix} = \frac{1}{2}$$

$$\begin{pmatrix} 0.64 & 0.26 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \frac{1}{2}$$

When $p = 2$, Every α is Rational

Lemma

Any bilinear form A has at most one associated α.

Corollary

When $p = 2$, $\alpha \in \mathbb{Q}$.

When $p = 2$, Every α is Rational

Lemma

Any bilinear form A has at most one associated α.

Corollary

When $p = 2$, $\alpha \in \mathbb{Q}$.

- Since A is a zero-one matrix, it is fixed by any field automorphism of $\mathbb{C}/\mathbb{Q}$

When $p = 2$, Every α is Rational

Lemma

Any bilinear form A has at most one associated α.

Corollary

When $p = 2$, $\alpha \in \mathbb{Q}$.

- Since A is a zero-one matrix, it is fixed by any field automorphism of $\mathbb{C}/\mathbb{Q}$
- But any nontrivial Galois conjugate of α would violate the lemma!

Restatement using Multilinear Algebra

For $p = 3$, $q = 1$, we want to find a $\{0, 1\}$-hypermatrix A and probability vectors $\beta^{(i)}$ such that, for all probability vectors $x^{(i)}$,

$$\alpha = A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) = A(\beta^{(1)}, x^{(2)}, \beta^{(3)}) = A(\beta^{(1)}, \beta^{(2)}, x^{(3)}).$$

An Example Solution

An Example Solution

$$A = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array} \right)$$

An Example Solution

$$A = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right)$$

$$\beta^{(1)} = \left(\begin{array}{c|c} \frac{1}{2}(-1+\sqrt{5}) & \frac{1}{2}(3-\sqrt{5}) \end{array}\right)$$

$$\beta^{(2)} = \begin{pmatrix} \frac{1}{2}(3-\sqrt{5}) \\ \frac{1}{2}(-1+\sqrt{5}) \end{pmatrix}$$

$$\beta^{(3)} = \begin{pmatrix} \frac{1}{10}(5-\sqrt{5}) & \frac{1}{10}(5-\sqrt{5}) & \frac{1}{5}\sqrt{5} \end{pmatrix}$$

An Example Solution

$$
\begin{aligned}
A &= \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right) \\
\beta^{(1)} &= \left(\begin{array}{c|c} \frac{1}{2}(-1+\sqrt{5}) & \frac{1}{2}(3-\sqrt{5}) \end{array}\right) \\
\beta^{(2)} &= \begin{pmatrix} \frac{1}{2}(3-\sqrt{5}) \\ \frac{1}{2}(-1+\sqrt{5}) \end{pmatrix} \\
\beta^{(3)} &= \begin{pmatrix} \frac{1}{10}(5-\sqrt{5}) & \frac{1}{10}(5-\sqrt{5}) & \frac{1}{5}\sqrt{5} \end{pmatrix} \\
\alpha &= \frac{\sqrt{5}-1}{2}
\end{aligned}
$$

Any α is an Algebraic Number?

Any α is an Algebraic Number?

$$\alpha = A(x^{(1)}, \beta^{(2)}, \beta^{(3)})$$

Any α is an Algebraic Number?

$$\begin{aligned} \alpha &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\ \alpha J(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \end{aligned}$$

Any α is an Algebraic Number?

$$\begin{aligned}
\alpha &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\
\alpha J(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\
(\alpha J - A)(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= 0
\end{aligned}$$

Any α is an Algebraic Number?

$$\begin{aligned} \alpha &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\ \alpha J(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\ (\alpha J - A)(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= 0 \end{aligned}$$

So $\alpha J - A$ satisfies the degeneracy conditions:

$$\begin{aligned} (\alpha J - A)(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= 0 \\ (\alpha J - A)(\beta^{(1)}, x^{(2)}, \beta^{(3)}) &= 0 \\ (\alpha J - A)(\beta^{(1)}, \beta^{(2)}, x^{(3)}) &= 0 \end{aligned}$$

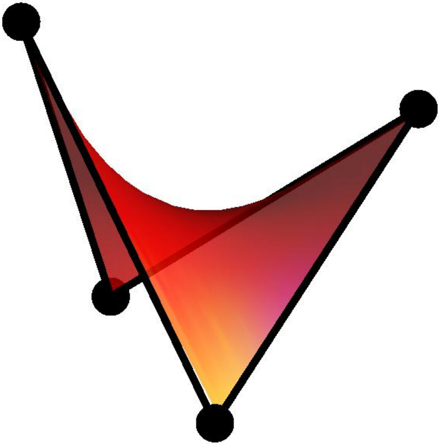
Any α is an Algebraic Number?

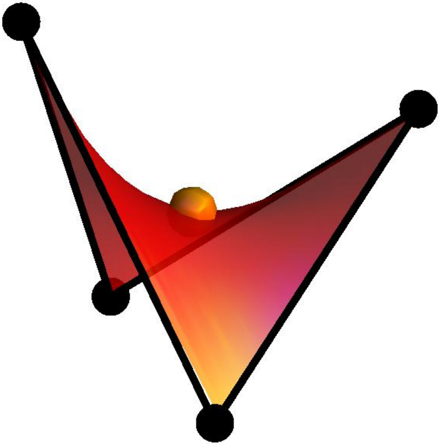
$$\begin{aligned} \alpha &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\ \alpha J(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) \\ (\alpha J - A)(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= 0 \end{aligned}$$

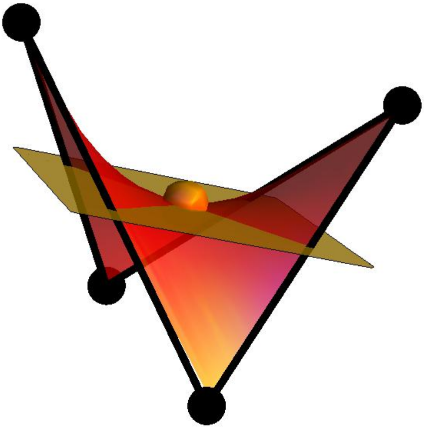
So $\alpha J - A$ satisfies the degeneracy conditions:

$$\begin{aligned} (\alpha J - A)(x^{(1)}, \beta^{(2)}, \beta^{(3)}) &= 0 \\ (\alpha J - A)(\beta^{(1)}, x^{(2)}, \beta^{(3)}) &= 0 \\ (\alpha J - A)(\beta^{(1)}, \beta^{(2)}, x^{(3)}) &= 0 \end{aligned}$$

$$\iff \mathrm{Det}(\alpha J - A) = 0$$







Any α is an Algebraic Number

- The hyperplane defined by $(\alpha J - A)(x) = 0$ is tangent to the Segre variety at the point $\beta^{(1)} \otimes \cdots \otimes \beta^{(p)}$.

Any α is an Algebraic Number

- The hyperplane defined by $(\alpha J - A)(x) = 0$ is tangent to the Segre variety at the point $\beta^{(1)} \otimes \cdots \otimes \beta^{(p)}$.
- Projective duality gives the set of tangent hyperplanes the structure of a variety, too.

Any α is an Algebraic Number

- The hyperplane defined by $(\alpha J - A)(x) = 0$ is tangent to the Segre variety at the point $\beta^{(1)} \otimes \cdots \otimes \beta^{(p)}$.
- Projective duality gives the set of tangent hyperplanes the structure of a variety, too.
- Under favorable conditions, this variety is cut out by a single polynomial Det. So $\mathrm{Det}(\alpha J - A) = 0$.

Any α is an Algebraic Number

- The hyperplane defined by $(\alpha J - A)(x) = 0$ is tangent to the Segre variety at the point $\beta^{(1)} \otimes \cdots \otimes \beta^{(p)}$.
- Projective duality gives the set of tangent hyperplanes the structure of a variety, too.
- Under favorable conditions, this variety is cut out by a single polynomial Det. So $\mathrm{Det}(\alpha J - A) = 0$.
- There's a problem when $\mathrm{Det}(tJ - A) \equiv 0 \ldots$

Any α is an Algebraic Number

- The hyperplane defined by $(\alpha J - A)(x) = 0$ is tangent to the Segre variety at the point $\beta^{(1)} \otimes \cdots \otimes \beta^{(p)}$.
- Projective duality gives the set of tangent hyperplanes the structure of a variety, too.
- Under favorable conditions, this variety is cut out by a single polynomial Det. So $\mathrm{Det}(\alpha J - A) = 0$.
- There's a problem when $\mathrm{Det}(tJ - A) \equiv 0 \ldots$ We repeat the argument is a suitable singular stratum.

Constructing any Algebraic α

- Case $p = 3$, $q = 1$ is the core of the proof of the constructive direction for algebraic α.

Constructing any Algebraic α

- Case $p = 3$, $q = 1$ is the core of the proof of the constructive direction for algebraic α.

Proof in two steps:

Constructing any Algebraic α

- Case $p = 3$, $q = 1$ is the core of the proof of the constructive direction for algebraic α.

Proof in two steps:

- Use algebraic geometry to produce a point on the variety

Constructing any Algebraic α

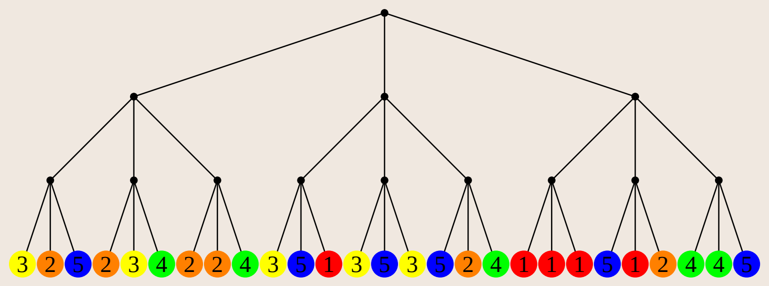
- Case $p = 3$, $q = 1$ is the core of the proof of the constructive direction for algebraic α.

Proof in two steps:

- Use algebraic geometry to produce a point on the variety
- Use Diophantine approximation and analysis to wiggle the solution into the positive cone

Constructing any Algebraic α

- Deduce general case from $p = 3$, $q = 1$ case using the Bureaucracy Lemma.



Recap

- The algebraic geometry of multilinear operators is a powerful tool...

Recap

- The algebraic geometry of multilinear operators is a powerful tool...
- which can be applied to cryptologic problems in a serious way.

Recap

- The algebraic geometry of multilinear operators is a powerful tool...
- which can be applied to cryptologic problems in a serious way.
- Thank you!