Decision problems on probabilistic programs over finite fields and all their extensions

Charlie Jacomme supervised by Hubert Comon & Steve Kremer

November 19,2019

LSV, INRIA Nancy

This is NOT an introduction to security

Probabilistic programs

Probabilistic programs over finite fields
Loosely speaking, a program:

- receives input values inside a finite fields,
- performs random sampling,
- performs operations, branchings, . . . , (no loops)
- returns some values inside the finite field.

Probabilistic programs

Probabilistic programs over finite fields
Loosely speaking, a program:

- receives input values inside a finite fields,
- performs random sampling,
- performs operations, branchings, . . . , (no loops)
- returns some values inside the finite field.

$\hookrightarrow$ Verifications for such programs ?

Verification of Probabilistic programs

Decisions problems

Decisions problems

- EQUIV: Are two programs equivalent ?

Verification of Probabilistic programs

Decisions problems

- EQUIV: Are two programs equivalent ?
- INDEP: Are two programs independent ?

Verification of Probabilistic programs

Decisions problems

- EQUIV: Are two programs equivalent ?
- INDEP: Are two programs independent ?
- MAJ: Can we bound the probability of an event inside a program ?

Verification of Probabilistic programs

Decisions problems

- EQUIV: Are two programs equivalent ?
- INDEP: Are two programs independent ?
- MAJ: Can we bound the probability of an event inside a program ?

Decidable ?

Verification of Probabilistic programs

Decisions problems

- EQUIV: Are two programs equivalent ?
- INDEP: Are two programs independent ?
- MAJ: Can we bound the probability of an event inside a program ?

Decidable ?

Given a finite field, everything is finite and can be computed.

Decisions problems

- EQUIV: Are two programs equivalent ?
- INDEP: Are two programs independent ?
- MAJ: Can we bound the probability of an event inside a program ?

Decidable ?

Given a finite field, everything is finite and can be computed.

$\hookrightarrow$ What about the complexity ?

Uniform Decisions problems

Uniform Verification of Probabilistic Programs

Uniform Decisions problems

Given probabilistic programs over $\mathbb{F}_2$ (booleans), using $\oplus$ and $\wedge$, are they equivalent for all length of bitstrings ?

Uniform Verification of Probabilistic Programs

Uniform Decisions problems

Given probabilistic programs over $\mathbb{F}_2$ (booleans), using $\oplus$ and $\wedge$, are they equivalent for all length of bitstrings ?

$\mathsf{EQUIV}_{2^\infty}$
input: two programs over $\mathbb{F}_2$ question: for any $k \geq 1$, are the programs equivalent over $\mathbb{F}_{2^k}$?

Uniform Decisions problems

Given probabilistic programs over $\mathbb{F}_2$ (booleans), using $\oplus$ and $\wedge$, are they equivalent for all length of bitstrings ?

$\mathrm{EQUIV}_{2^\infty}$
input: two programs over $\mathbb{F}_2$ question: for any $k \geq 1$, are the programs equivalent over $\mathbb{F}_{2^k}$?

$\hookrightarrow$ the length of the bitstrings could be a security parameter

Uniform Decisions problems

Given probabilistic programs over $\mathbb{F}_2$ (booleans), using $\oplus$ and $\wedge$, are they equivalent for all length of bitstrings ?

EQUIV_{2^∞}
input: two programs over $\mathbb{F}_2$ question: for any $k \geq 1$, are the programs equivalent over $\mathbb{F}_{2^k}$?

$\hookrightarrow$ the length of the bitstrings could be a security parameter

Decidable ?

Uniform Decisions problems

Given probabilistic programs over $\mathbb{F}_2$ (booleans), using $\oplus$ and $\wedge$, are they equivalent for all length of bitstrings ?

EQUIV_{2^∞}
input: two programs over $\mathbb{F}_2$ question: for any $k \geq 1$, are the programs equivalent over $\mathbb{F}_{2^k}$?

$\hookrightarrow$ the length of the bitstrings could be a security parameter

Decidable ?

There is an infinite number of cases to check, not so trivial anymore...

Probabilistic Programs over finite fields

Our contributions

$$\mathsf{INDEP}_q \Leftrightarrow \mathsf{EQUIV}_q$$

Probabilistic Programs over finite fields

Our contributions

$$\mathsf{INDEP}_q \Leftrightarrow \mathsf{EQUIV}_q$$
$$\mathsf{NI{-}EQUIV}_q \Leftrightarrow \mathsf{EQUIV}_q$$

Probabilistic Programs over finite fields

Our contributions

$$\mathsf{INDEP}_q \Leftrightarrow \mathsf{EQUIV}_q$$
$$\mathsf{NI{-}EQUIV}_q \Leftrightarrow \mathsf{EQUIV}_q$$

Probabilistic Programs over finite fields

Our contributions

$$\mathsf{INDEP}_q \Leftrightarrow \mathsf{EQUIV}_q$$
$$\mathsf{NI{-}EQUIV}_q \Leftrightarrow \mathsf{EQUIV}_q$$

	EQUIV_x	$\mathsf{NI} - \mathsf{MAJ}_x$	MAJ_x
$x = q$	$\mathsf{coNP}^{\mathsf{C_{=}P}}$-complete	PP-complete	$\mathsf{coNP}^{\mathsf{PP}}$-complete
$x = q^\infty$	EXP $\mathsf{coNP}^{\mathsf{C_{=}P}}$-hard	$\leq_{\mathsf{EXP}}$ POSITIVITY	?

Menus

Complexity Menu[1]

Formal definitions

⋆ ⋆ ⋆

Definition of $C_=P$

EQUIV_q is $\text{coNP}^{C_=P}$-complete

⋆ ⋆ ⋆

Decidability of EQUIV_{q^∞}

(without inputs/conditionals)

[1] Familiarity with coNP complexity, completeness and oracles TM appreciated.

Menus

Complexity Menu[1]

Formal definitions

⋆⋆⋆

Definition of $\mathsf{C_{=}P}$

EQUIV_q is $\mathsf{coNP}^{\mathsf{C_{=}P}}$-complete

⋆⋆⋆

Decidability of $\mathsf{EQUIV}_{q^\infty}$ (without inputs/conditionals)

Decidability Menu

Formal definitions

⋆⋆⋆

Removing the inputs

Decidability of $\mathsf{EQUIV}_{q^\infty}$ (without inputs/conditionals)

Removing the conditionals

[1] Familiarity with coNP complexity, completeness and oracles TM appreciated.

Formal definitions

Quick reminders

Classically, p denotes a prime number, $q = p^k$ a prime power.

Quick reminders

Classically, p denotes a prime number, $q = p^k$ a prime power.
There is a unique finite field for each size.

Quick reminders

Classically, p denotes a prime number, $q = p^k$ a prime power.
There is a unique finite field for each size.

Prime finite field

$$\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z} \text{ (integers modulo p)}$$

Quick reminders

Classically, p denotes a prime number, $q = p^k$ a prime power.

There is a unique finite field for each size.

Prime finite field

$$\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z} \text{ (integers modulo p)}$$

Finite fields

With α indeterminate and $P \in \mathbb{F}_p[\alpha]$ an irreducible polynomial of degree k:

$$\mathbb{F}_q \simeq \mathbb{F}_p[\alpha]/P(\alpha)$$

Programs

We consider in this talk:

$$
\begin{array}{rcll}
e & ::= & S & \text{a polynomial over } \mathbb{F}_q[I \uplus R] \\
 & | & \text{if } S = 0 \text{ then } e_1 \text{ else } e_2 & \text{conditionals} \\
 & & & \\
P & := & (e_1, \ldots, e_n) & \text{program}
\end{array}
$$

Programs

Variables corresponding to inputs.

We consider in this talk:

e	$::=$	S	a polynomial over $\mathbb{F}_q[I \uplus R]$
	$\mid$	if $S = 0$ then e_1 else e_2	conditionals
P	$:=$	$(e_1, \ldots, e_n)$	program

Programs

Variables corresponding to inputs.

We consider in this talk:

e	$::=$	S	a polynomial over $\mathbb{F}_q[I \uplus R]$
	$\mid$	if $S = 0$ then e_1 else e_2	conditionals
P	$:=$	$(e_1, \ldots, e_n)$	program

Variables corresponding to random samplings.

Programs examples

Examples

With $I = \{x, y\}$ and $R = \{u, v, w\}$:

- $(x + u, y, xy)$
- $(uv + vw + wu + xy)$

Programs examples

Input : x,y

Sample uniformly u

Return $(x + u, y, xy)$

Examples

With $I = \{x, y\}$ and $R = \{u, v, w\}$:

- $(x + u, y, xy)$
- $(uv + vw + wu + xy)$

Programs examples

Input : x,y
Sample uniformly u
Return $(x + u, y, xy)$

Examples

With $I = \{x, y\}$ and $R = \{u, v, w\}$:

- $(x + u, y, xy)$
- $(uv + vw + wu + xy)$

Input : x,y
Sample uniformly u,v,w
Return $(uv + vw + wu + xy)$

Semantics

We denote $\mathcal{P}_q(I, R)$ the set of programs with input variables I and random variables R, and $|P|$ the arity of P.

Semantics

We denote $\mathcal{P}_q(I, R)$ the set of programs with input variables I and random variables R, and $|P|$ the arity of P.

Probabilistic semantics
For $P \in \mathcal{P}_q(I, R)$, $\bar{i} \in \mathbb{F}_{q^k}^{\sharp I}$,

$$\begin{aligned} [\![P]\!]_{\bar{i}}^{q^k} : \mathbb{F}_{q^k}^{|P|} &\to \mathbb{R} \\ c &\mapsto \mathbb{P}\{P(\bar{i}, \bar{r}) = c \mid \bar{r} \xleftarrow{\$} \mathbb{F}_{q^k}^{\sharp R}\} \end{aligned}$$

Semantics

We denote $\mathcal{P}_q(I, R)$ the set of programs with input variables I and random variables R, and $|P|$ th

Evaluation of P given the specified values for the variables.

Probabilistic semantics

For $P \in \mathcal{P}_q(I, R)$, $\bar{i} \in \mathbb{F}_{q^k}^{\sharp I}$,

$$
\begin{aligned}
[\![P]\!]_{\bar{i}}^{q^k} : \mathbb{F}_{q^k}^{|P|} &\to \mathbb{R} \\
c &\mapsto \mathbb{P}\{P(\bar{i}, \bar{r}) = c \mid \bar{r} \xleftarrow{\$} \mathbb{F}_{q^k}^{\sharp R}\}
\end{aligned}
$$

Semantics

We denote $\mathcal{P}_q(I, R)$ the set of programs with input variables I and random variables R, and $|P|$ th

Evaluation of P given the specified values for the variables.

Probabilistic semantics

For $P \in \mathcal{P}_q(I, R)$, $\bar{i} \in \mathbb{F}_{q^k}^{\sharp I}$,

$$\begin{aligned} [\![P]\!]_{\bar{i}}^{q^k} : \mathbb{F}_{q^k}^{|P|} &\to \mathbb{R} \\ c &\mapsto \mathbb{P}\{P(\bar{i}, \bar{r}) = c \mid \bar{r} \overset{\$}{\leftarrow} \mathbb{F}_{q^k}^{\sharp R}\} \end{aligned}$$

Distribution induced when sampling the random variables uniformly.

Some examples

Over the booleans
With $I = \{i\}$ and $R = \{r\}$,

$$\begin{aligned} [\![r]\!]^2 : 0 &\mapsto \tfrac{1}{2} \\ 1 &\mapsto \tfrac{1}{2} \end{aligned}$$

Some examples

Over the booleans
With $I = \{i\}$ and $R = \{r\}$,

$$\begin{aligned} [\![r]\!]^2 : 0 &\mapsto \tfrac{1}{2} \\ 1 &\mapsto \tfrac{1}{2} \end{aligned}$$

$$\begin{aligned} [\![ir]\!]^2_1 : 0 &\mapsto \tfrac{1}{2} \\ 1 &\mapsto \tfrac{1}{2} \end{aligned}$$

$$\begin{aligned} [\![ir]\!]^2_0 : 0 &\mapsto 1 \\ 1 &\mapsto 0 \end{aligned}$$

Decision problem

Equivalence

$$P \approx_{q^k} Q$$
$$\Leftrightarrow$$
$$\forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k}$$

Decision problem

Equivalence

$$P \approx_{q^k} Q$$
$$\Leftrightarrow$$
$$\forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k}$$

Uniform Equivalence

$$P \approx_{q^\infty} Q$$
$$\Leftrightarrow$$
$$\forall k \geq 1.\ P \approx_{q^k} Q$$

The complexity of equivalence

A small reminder

SAT
input: ϕ a CNF boolean formula
question: Is ϕ true for some valuation ?

A small reminder

SAT
input: ϕ a CNF boolean formula
question: Is ϕ true for some valuation ?

L **is in** NP **if**

- there exists a non deterministic TM, such that

$$x \in L \Leftrightarrow M(x) \text{ has at least one accepting path}$$

A small reminder

SAT
input: ϕ a CNF boolean formula
question: Is ϕ true for some valuation ?

L **is in** NP **if**

- there exists a non deterministic TM, such that

$$x \in L \Leftrightarrow M(x) \text{ has at least one accepting path}$$

- there exists a probabilistic TM, such that

$$x \in L \Leftrightarrow M(x) \text{ accepts with non zero probability}$$

The exact counting complexity class

halfSAT
input: ϕ a CNF boolean formula
question: Is ϕ true for for exactly half of its valuations ?

The exact counting complexity class

halfSAT
input: ϕ a CNF boolean formula
question: Is ϕ true for for exactly half of its valuations ?

***L* is in $C_=P$ if**

- there exists a non deterministic TM, such that

$$x \in L \Leftrightarrow \text{ half of the paths of } M(x) \text{ are acceptings ones}$$

The exact counting complexity class

halfSAT
input: ϕ a CNF boolean formula
question: Is ϕ true for for exactly half of its valuations ?

L **is in** $C_{=}P$ **if**

- there exists a non deterministic TM, such that
$$x \in L \Leftrightarrow \text{ half of the paths of } M(x) \text{ are acceptings ones}$$
- there exists a probabilistic TM, such that
$$x \in L \Leftrightarrow M(x) \text{ accepts with probability } \frac{1}{2}$$

Some exotic complexity class

A−halfSAT
input: $\phi(X, Y)$ a CNF boolean formula
question: For any valuation of Y,
is ϕ true for for exactly half of the valuations of X ?

Some exotic complexity class

A−halfSAT
input: $\phi(X, Y)$ a CNF boolean formula
question: For any valuation of Y,
is ϕ true for for exactly half of the valuations of X ?

L **is in** $\mathsf{coNP}^{\mathsf{C_=P}}$ **if**

Some exotic complexity class

A−halfSAT
input: $\phi(X, Y)$ a CNF boolean formula
question: For any valuation of Y, is ϕ true for for exactly half of the valuations of X ?

L is in $\mathsf{coNP}^{\mathsf{C_=P}}$ **if**

- There exists a non deterministic TM with an oracle deciding problems in $\mathsf{C_=P}$, such that

$$x \in L \Leftrightarrow \text{all the paths of } M(x) \text{ are acceptings ones}$$

Hardness

Can we solve A$-$halfSAT using equivalence ?

Hardness

Can we solve A$-$halfSAT using equivalence ?

A simple reduction
Given ϕ,

$$\phi(X, Y) \in \text{A}-\text{halfSAT} \Leftrightarrow \tilde{\phi} \approx_2 r$$

Hardness

$$\tilde{\phi} := \begin{cases} \text{conversion from } \wedge, \vee \text{ to } +, \times \\ \text{X : random variables} \\ \text{Y : input variables} \end{cases}$$

Can we solve A−halfSAT using equivalence ?

A simple reduction
Given ϕ,

$$\phi(X, Y) \in \text{A}-\text{halfSAT} \Leftrightarrow \tilde{\phi} \approx_2 r$$

Hardness

$$\tilde{\phi} := \begin{cases} \text{conversion from } \wedge, \vee \text{ to } +, \times \\ \text{X : random variables} \\ \text{Y : input variables} \end{cases}$$

Can we solve A−halfSAT using equivalence ?

A simple reduction
Given ϕ,

$$\phi(X, Y) \in \text{A−halfSAT} \Leftrightarrow \tilde{\phi} \approx_2 r$$

$\hookrightarrow$ EQUIV_2 is $\text{coNP}^{\text{C}_=\text{P}}$-hard

Membership

$$
\begin{aligned}
&M(P, Q, c, \bar{i}) := \\
&\quad x \xleftarrow{\$} \{0,1\} \\
&\quad \bar{r} = (r_1, \ldots, r_m) \xleftarrow{\$} \mathbb{F}_q^m \\
&\quad \text{if } x = 0 \text{ then} \\
&\quad\quad \text{if } P(\bar{i}, \bar{r}) = c \text{ then ACCEPT else REJECT} \\
&\quad \text{else} \\
&\quad\quad \text{if } Q(\bar{i}, \bar{r}) = c \text{ then ACCEPT else REJECT}
\end{aligned}
$$

Membership

$$M(P, Q, c, \bar{i}) :=$$

$$x \xleftarrow{\$} \{0, 1\}$$

$$\bar{r} = (r_1, \ldots, r_m) \xleftarrow{\$} \mathbb{F}_q^m$$

if $x = 0$ then

  if $P(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

else

  if $Q(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{[\![P]\!]_{\bar{i}}^{q}(c) + [\![Q]\!]_{\bar{i}}^{q}(c)}{2}$$

Membership

$M(P, Q, c, \bar{i}) :=$

$x \xleftarrow{\$} \{0, 1\}$

$\bar{r} = (r_1, \ldots, r_m) \xleftarrow{\$} \mathbb{F}_q^m$

if $x = 0$ then

if $P(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

else

if $Q(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

Deterministic evaluation

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{[\![P]\!]_{\bar{i}}^{q}(c) + [\![Q]\!]_{\bar{i}}^{q}(c)}{2}$$

Probablity that P equals c on input $\bar{i}$

Membership

$$M(P, Q, c, \bar{i}) :=$$

$x \xleftarrow{\$} \{0, 1\}$

$\bar{r} = (r_1, \ldots, r_m) \xleftarrow{\$} \mathbb{F}_q^m$

if $x = 0$ then

  if $P(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

else

  if $Q(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{[\![P]\!]^q_{\bar{i}}(c) + [\![Q]\!]^q_{\bar{i}}(c)}{2}$$

Membership

$M(P, Q, c, \bar{i}) :=$

$x \xleftarrow{\$} \{0, 1\}$

$\bar{r} = (r_1, \dots, r_m) \xleftarrow{\$} \mathbb{F}_q^m$

if $x = 0$ then

  if $P(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

else

  if $Q(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{[\![P]\!]_{\bar{i}}^{q}(c) + [\![Q]\!]_{\bar{i}}^{q}(c)}{2}$$

Membership

$$M(P, Q, c, \bar{i}) :=$$

$$x \xleftarrow{\$} \{0, 1\}$$

$$\bar{r} = (r_1, \ldots, r_m) \xleftarrow{\$} \mathbb{F}_q^m$$

if $x = 0$ then

    if $P(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

else

    if $Q(\bar{i}, \bar{r}) \neq c$ then ACCEPT else REJECT

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{[\![P]\!]_{\bar{i}}^{q}(c) + ?}{2}$$

Membership

$$M(P, Q, c, \bar{i}) :=$$

$x \xleftarrow{\$} \{0, 1\}$

$\bar{r} = (r_1, \ldots, r_m) \xleftarrow{\$} \mathbb{F}_q^m$

if $x = 0$ then

  if $P(\bar{i}, \bar{r}) = c$ then ACCEPT else REJECT

else

  if $Q(\bar{i}, \bar{r}) \neq c$ then ACCEPT else REJECT

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{[\![P]\!]_{\bar{i}}^{q}(c) + (1 - [\![Q]\!]_{\bar{i}}^{q}(c))}{2}$$

Membership

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{1}{2} + \frac{[\![P]\!]^q_{\bar{i}}(c) - [\![Q]\!]^q_{\bar{i}}(c)}{2}$$

Membership

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{1}{2} + \frac{[\![P]\!]^q_{\bar{i}}(c) - [\![Q]\!]^q_{\bar{i}}(c)}{2}$$

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{1}{2} \Leftrightarrow [\![P]\!]^q_{\bar{i}}(c) = [\![Q]\!]^q_{\bar{i}}(c)$$

Membership

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{1}{2} + \frac{[\![P]\!]^q_{\bar{i}}(c) - [\![Q]\!]^q_{\bar{i}}(c)}{2}$$

$$\mathbb{P}_{accept}(P, Q, c, \bar{i}) = \frac{1}{2} \Leftrightarrow [\![P]\!]^q_{\bar{i}}(c) = [\![Q]\!]^q_{\bar{i}}(c)$$

$\hookrightarrow$ Given $P, Q, c, \bar{i}$, deciding if $[\![P]\!]^q_{\bar{i}}(c) = [\![Q]\!]^q_{\bar{i}}(c)$ is in $\mathsf{C_{=}P}$.

Membership

$$P \approx_q Q \Leftrightarrow \forall \bar{i} \in \mathbb{F}_q^m, \forall c \in \mathbb{F}_q^{|P|}, [\![P]\!]_{\bar{i}}^q(c) = [\![Q]\!]_{\bar{i}}^q(c)$$

$\hookrightarrow$ EQUIV$_q$ is coNP$^{\mathsf{C_=P}}$-complete

Deciding uniform equivalence

The issue of inputs

We do not need inputs !
Let $P, Q \in \mathcal{P}_q(I, R)$, we have:

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

The issue of inputs

Fresh random variables

We do not need inputs !
Let $P, Q \in \mathcal{P}_q(I, R)$, we have:

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

The issue of inputs

Fresh random variables

We do not need inputs !
Let $P, Q \in \mathcal{P}_q(I, R)$, we have:

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$\sigma : I \to R_I$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$P \approx_{q^k} Q$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$$\begin{aligned} &P \approx_{q^k} Q \\ &\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k} \end{aligned}$$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$$\begin{aligned} & P \approx_{q^k} Q \\ & \quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k} \\ & \quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n}.\ [\![P]\!]_{\bar{i}}^{q^k}(\overline{c}) = [\![Q]\!]_{\bar{i}}^{q^k}(\overline{c}) \end{aligned}$$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$$\begin{aligned}
&P \approx_{q^k} Q \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k} \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n}.\ [\![P]\!]_{\bar{i}}^{q^k}(\overline{c}) = [\![Q]\!]_{\bar{i}}^{q^k}(\overline{c}) \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n} [\![(P\sigma, R_I)]\!]_{\bar{i}}^{q^k}(c, \bar{i}) = [\![(Q\sigma, R_I)]\!]_{\bar{i}}^{q^k}(c, \bar{i})
\end{aligned}$$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$$\begin{aligned}
&P \approx_{q^k} Q \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k} \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n}.\ [\![P]\!]_{\bar{i}}^{q^k}(\overline{c}) = [\![Q]\!]_{\bar{i}}^{q^k}(\overline{c}) \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n} [\![(P\sigma, R_I)]\!]_{\bar{i}}^{q^k}(c, \bar{i}) = [\![(Q\sigma, R_I)]\!]_{\bar{i}}^{q^k}(c, \bar{i}) \\
&\quad \Leftrightarrow \forall c' \in \mathbb{F}_{q^k}^{n+\sharp I} [\![(P\sigma, R_I)]\!]^{q^k}(c') = [\![(Q\sigma, R_I)]\!]^{q^k}(c')
\end{aligned}$$

The issue of inputs - Let's prove it

We do not need inputs !

$$P \approx_{q^k} Q \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)$$

$$\begin{aligned}
&P \approx_{q^k} Q \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\ [\![P]\!]_{\bar{i}}^{q^k} = [\![Q]\!]_{\bar{i}}^{q^k} \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n}.\ [\![P]\!]_{\bar{i}}^{q^k}(\overline{c}) = [\![Q]\!]_{\bar{i}}^{q^k}(\overline{c}) \\
&\quad \Leftrightarrow \forall \bar{i} \in \mathbb{F}_{q^k}^{\sharp I}.\forall \overline{c} \in \mathbb{F}_{q^k}^{n} [\![(P\sigma, R_I)]\!]_{\bar{i}}^{q^k}(c, \bar{i}) = [\![(Q\sigma, R_I)]\!]_{\bar{i}}^{q^k}(c, \bar{i}) \\
&\quad \Leftrightarrow \forall c' \in \mathbb{F}_{q^k}^{n+\sharp I} [\![(P\sigma, R_I)]\!]^{q^k}(c') = [\![(Q\sigma, R_I)]\!]^{q^k}(c') \\
&\quad \Leftrightarrow (P\sigma, R_I) \approx_{q^k} (Q\sigma, R_I)
\end{aligned}$$

Uniform equivalence - restricted case

Straight line programs
Programs without conditionals $P, Q \in \mathcal{P}_{\boldsymbol{q}}(\emptyset, R)$

Uniform equivalence - restricted case

Straight line programs
Programs without conditionals $P, Q \in \mathcal{P}_q(\emptyset, R)$

$$P, Q \in (\mathbb{F}_q[R])^n$$

Uniform equivalence - restricted case

Straight line programs
Programs without conditionals $P, Q \in \mathcal{P}_q(\emptyset, R)$

$$P, Q \in (\mathbb{F}_q[R])^n$$

The mathematical question

$$P \approx_{q^\infty} Q$$
$$\Leftrightarrow$$
$$\forall \overline{c} \in \mathbb{F}_{q^k}^n.\ \forall k.\ \sharp\{\overline{r} \in \mathbb{F}_{q^k}^{\sharp R} | P(\overline{r}) = \overline{c}\} = \sharp\{\overline{r} \in \mathbb{F}_{q^k}^{\sharp R} | Q(\overline{r}) = \overline{c}\}$$

Mathemagic !

The local zeta function

For any $P \in \mathbb{F}_q[R]^n$,

$$Z(P) = exp\left(\sum_{k \geq 1} \frac{N_k(P) T^k}{k}\right)$$

Mathemagic !

An indeterminate

The local zeta function
For any $P \in \mathbb{F}_q[R]^n$,

$$Z(P) = exp\left(\sum_{k\geq 1} \frac{N_k(P)T^k}{k}\right)$$

An indeterminate

The local zeta function

For any $P \in \mathbb{F}_q[R]^n$,

$$Z(P) = exp\left(\sum_{k\geq 1} \frac{N_k(P)T^k}{k}\right)$$

$$N_k(P) = \sharp\{\bar{r} \in \mathbb{F}_{q^k}^{\sharp R} | P(\bar{r}) = \mathbf{0}\}$$

Mathemagic !

The local zeta function

For any $P \in \mathbb{F}_q[R]^n$,

$$Z(P) = exp\left(\sum_{k\geq 1} \frac{N_k(P)T^k}{k}\right)$$

Why is it interesting ?

$$Z(P) = Z(Q) \Leftrightarrow \forall k.\ \sharp\{\bar{r} \in \mathbb{F}_{q^k}^{\sharp R} | P(\bar{r}) = \mathbf{0}\} = \sharp\{\bar{r} \in \mathbb{F}_{q^k}^{\sharp R} | Q(\bar{r}) = \mathbf{0}\}$$

Mathemagic !

The local zeta function

For any $P \in \mathbb{F}_q[R]^n$,

$$Z(P) = exp\left(\sum_{k\geq 1} \frac{N_k(P)T^k}{k}\right)$$

Why is it interesting ?

$$Z(P) = Z(Q) \Leftrightarrow \forall k.\ \sharp\{\bar{r} \in \mathbb{F}_{q^k}^{\sharp R} | P(\bar{r}) = \mathbf{0}\} = \sharp\{\bar{r} \in \mathbb{F}_{q^k}^{\sharp R} | Q(\bar{r}) = \mathbf{0}\}$$

Black Magic

By Well's conjecture (proven by Dwork), $Z(P)$ is a rational function, and can thus be computed !

In a Nuttshell

Uniform equivalence for straight line programs
For P, Q straight line programs,

In a Nuttshell

Uniform equivalence for straight line programs
For P, Q straight line programs,

- using the local zeta function, we can decide if P and Q are equal to zero with the same probability on all extensions of a finite field;

In a Nuttshell

Uniform equivalence for straight line programs
For P, Q straight line programs,

- using the local zeta function, we can decide if P and Q are equal to zero with the same probability on all extensions of a finite field;
- with a bit of encoding, we can extend this to all values, and check the equality of the distributions.

In a Nuttshell

Uniform equivalence for straight line programs
For P, Q straight line programs,

- using the local zeta function, we can decide if P and Q are equal to zero with the same probability on all extensions of a finite field;
- with a bit of encoding, we can extend this to all values, and check the equality of the distributions.

$\hookrightarrow$ We can decide if $P \approx_{q^\infty} Q$!

What about conditionals ?

A first classical encoding

$$\text{if } B \neq 0 \text{ then } P \text{ else } Q \approx_{q^k} Q + B^{q^k - 1}(P - Q)$$

What about conditionals ?

$$B^{q^k-1} = \begin{cases} 0 \text{ if } B = 0 \\ 1 \text{ if } B \neq 0 \end{cases}$$

A first classical encoding

$$\text{if } B \neq 0 \text{ then } P \text{ else } Q \approx_{q^k} Q + B^{q^k-1}(P - Q)$$

What about conditionals ?

A first classical encoding

$$\text{if } B \neq 0 \text{ then } P \text{ else } Q \approx_{q^k} Q + B^{q^k-1}(P - Q)$$

It depends on k...

What about conditionals

The solution

- B has an inverse if and only if $B \neq 0$,
- $\exists t, Bt - 1 = 0$ if and only if $B \neq 0$,
- for any variable t and polynomial B:

$$(B(Bt-1) = 0 \wedge t(Bt-1) = 0) \Leftrightarrow t = B^{q^k-2}$$

What about conditionals

The solution

- B has an inverse if and only if $B \neq 0$,
- $\exists t, Bt - 1 = 0$ if and only if $B \neq 0$,
- for any variable t and polynomial B:

$$(B(Bt-1) = 0 \wedge t(Bt-1) = 0) \Leftrightarrow t = B^{q^k-2}$$

$$\sharp\{\bar{r} \in \mathbb{F}_{q^k}^m, t \in \mathbb{F}_{q^k} \mid (Q + tB(P-Q), B(Bt-1), t(Bt-1)) = \mathbf{0}\}$$

What about conditionals

The solution

- B has an inverse if and only if $B \neq 0$,
- $\exists t, Bt - 1 = 0$ if and only if $B \neq 0$,
- for any variable t and polynomial B:

$$(B(Bt-1) = 0 \wedge t(Bt-1) = 0) \Leftrightarrow t = B^{q^k - 2}$$

$$\begin{aligned}&\sharp\{\overline{r} \in \mathbb{F}_{q^k}^m, t \in \mathbb{F}_{q^k} \mid (Q + tB(P - Q), B(Bt-1), t(Bt-1)) = \mathbf{0}\} \\ &\quad = \sharp\{\overline{r} \in \mathbb{F}_{q^k}^m \mid Q + B^{q^k-1}(P - Q) = \mathbf{0}\}\end{aligned}$$

What about conditionals

The solution

- B has an inverse if and only if $B \neq 0$,
- $\exists t, Bt - 1 = 0$ if and only if $B \neq 0$,
- for any variable t and polynomial B:

$$(B(Bt-1) = 0 \wedge t(Bt-1) = 0) \Leftrightarrow t = B^{q^k - 2}$$

$$\begin{aligned}&\sharp\{\bar{r} \in \mathbb{F}_{q^k}^m, t \in \mathbb{F}_{q^k} \mid (Q + tB(P-Q), B(Bt-1), t(Bt-1)) = \mathbf{0}\} \\ &\quad = \sharp\{\bar{r} \in \mathbb{F}_{q^k}^m \mid Q + B^{q^k-1}(P-Q) = \mathbf{0}\}\end{aligned}$$

$\hookrightarrow$ We can use this inside N_k

Conclusions

Uniform independence and equivalence

Decidable !

Conclusions

Uniform independence and equivalence

Decidable !

Independence and equivalence

$\mathsf{coNP}^{\mathsf{C_=P}}$-complete...

Conclusions

Uniform independence and equivalence

Decidable !

Independence and equivalence

$\mathsf{coNP}^{\mathsf{C_{=}P}}$-complete...

Bounding the probability of an event
$\mathsf{coNP}^{\mathsf{PP}}$-complete in the finite case, reduces to the POSITIVITY problem in the uniform case.

Conclusions

Uniform independence and equivalence

Decidable !

Independence and equivalence

$\text{coNP}^{\text{C}_=\text{P}}$-complete...

Bounding the probability of an event

coNP^{PP}-complete in the finite case, reduces to the POSITIVITY problem in the uniform case.

Given a sequence defined by a recurrence equations, are all the term of the sequence positive ?

Conclusions

Uniform independence and equivalence

Decidable !

Independence and equivalence

$\mathsf{coNP}^{\mathsf{C_=P}}$-complete...

Bounding the probability of an event

$\mathsf{coNP}^{\mathsf{PP}}$-complete in the finite case, reduces to the POSITIVITY problem in the uniform case.

Which Programs ?

- Support of the observe primitive,
- sample variables inside a s polynomials,
- conditionals.

Given a sequence defined by a recurrence equations, are all the term of the sequence positive ?

Some open questions

The big question
Is the uniform problem strictly harder than the non uniform one ?

Some open questions

The big question
Is the uniform problem strictly harder than the non uniform one ?

Other open questions

- Can we support loops ?
- Is POSITIVITY decidable ?
- Can we extend to other probabilistic properties ?