Solvability of polynomial equations over finite fields.

Neeraj Kayal

Institute for Advanced Study / DIMACS

October 4th, 2006

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

The problem

- Solvability : Given a finite field $\mathbb{F}_q$ and a set of polynomials

$$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$$

of total degree at most d, determine whether there exists a point $\bar{\mathbf{a}} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that

$$f_1(\bar{\mathbf{a}}) = \ldots = f_m(\bar{\mathbf{a}}) = 0?$$

Our results

- For any fixed n, Solvability can be decided **deterministically** in polynomial time ($\mathrm{poly}(d \cdot m \cdot \log q)$-time).

- Moreover, the parallel time complexity of the algorithm is $\mathrm{poly}(\log d \cdot \log m \cdot \log q)$.

Our results

- For any fixed n, Solvability can be decided **deterministically** in polynomial time ($\mathrm{poly}(d \cdot m \cdot \log q)$-time).

- Moreover, the parallel time complexity of the algorithm is $\mathrm{poly}(\log d \cdot \log m \cdot \log q)$.

Handling inequations.

- **A modified problem:** Given a finite field $\mathbb{F}_q$ and a set of polynomials

  $$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$$

  of total degree at most d, determine whether exists a point $\bar{\mathbf{a}} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that

  $$f_1(\bar{\mathbf{a}}) = \ldots = f_m(\bar{\mathbf{a}}) = 0 \text{ and } g(\bar{\mathbf{a}}) \neq 0.$$

- **Trick (Rabinovich):** Introduce a new variable t and determine if there is a solution to

  $$f_1(\bar{\mathbf{a}}) = \ldots = f_m(\bar{\mathbf{a}}) = 0 \text{ and } t \cdot g(\bar{\mathbf{a}}) = 1.$$

Handling inequations.

- **A modified problem:** Given a finite field $\mathbb{F}_q$ and a set of polynomials

  $$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$$

  of total degree at most d, determine whether exists a point $\bar{\mathbf{a}} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that

  $$f_1(\bar{\mathbf{a}}) = \ldots = f_m(\bar{\mathbf{a}}) = 0 \text{ and } g(\bar{\mathbf{a}}) \neq 0.$$

- **Trick (Rabinovich):** Introduce a new variable t and determine if there is a solution to

  $$f_1(\bar{\mathbf{a}}) = \ldots = f_m(\bar{\mathbf{a}}) = 0 \text{ and } t \cdot g(\bar{\mathbf{a}}) = 1.$$

Motivation

- After primality testing, Solvability was the only "natural decision problem" known to be in ZPP but not known to be in P .

A Note.

- **Note:** We seek the existence of a solution in the given finite field $\mathbb{F}_q$ itself and not its algebraic closure $\overline{\mathbb{F}}_q$.

- For existence of solutions in the algebraic closure of $\mathbb{F}_q$, Hilbert Nullstellensatz implies a deterministic algorithm with the above complexity bounds.

A Note.

- **Note:** We seek the existence of a solution in the given finite field $\mathbb{F}_q$ itself and not its algebraic closure $\overline{\mathbb{F}}_q$.

- For existence of solutions in the algebraic closure of $\mathbb{F}_q$, Hilbert Nullstellensatz implies a deterministic algorithm with the above complexity bounds.

Solvability over algebraically closed fields.

- **Hilbert's Nulstellensatz** - Polynomials $f_1(\bar{\mathbf{x}}), \ldots, f_m(\bar{\mathbf{x}}) \in \mathbb{F}[\bar{\mathbf{x}}]$ have a common solution in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ if and only if there exist polynomials $g_1, \ldots, g_m \in \mathbb{F}[\bar{\mathbf{x}}]$ such that

$$g_1(\bar{\mathbf{x}}) \cdot f_1(\bar{\mathbf{x}}) + \ldots + g_m(\bar{\mathbf{x}}) \cdot f_m(\bar{\mathbf{x}}) = 1$$

.

- This implies that if the number of variables n is fixed then the existence of a common solution can be determined in NC .

Solvability over algebraically closed fields.

- **Hilbert's Nulstellensatz** - Polynomials $f_1(\bar{\mathbf{x}}), \ldots, f_m(\bar{\mathbf{x}}) \in \mathbb{F}[\bar{\mathbf{x}}]$ have a common solution in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ if and only if there exist polynomials $g_1, \ldots, g_m \in \mathbb{F}[\bar{\mathbf{x}}]$ such that

$$g_1(\bar{\mathbf{x}}) \cdot f_1(\bar{\mathbf{x}}) + \ldots + g_m(\bar{\mathbf{x}}) \cdot f_m(\bar{\mathbf{x}}) = 1$$

.

- This implies that if the number of variables n is fixed then the existence of a common solution can be determined in NC .

Solvability over $\mathbb{Q}$.

- **Fermat's Last Theorem.** - For any $n \geq 3$, the following system has no solution over the field $\mathbb{Q}$ of rational numbers.

$$x^n + y^n = 1 \ , \ xy \neq 0$$

- Over $\mathbb{Q}$, Solvability of a **bivariate** system is **not** even known to be decidable.

Solvability over $\mathbb{Q}$.

- **Fermat's Last Theorem.** - For any $n \geq 3$, the following system has no solution over the field $\mathbb{Q}$ of rational numbers.

$$x^n + y^n = 1 \ , \ xy \neq 0$$

- Over $\mathbb{Q}$, Solvability of a **bivariate** system is **not** even known to be decidable.

Solvability over $\mathbb{Z}$.

- Solvability over $\mathbb{Z}$ (integers) is decidable for **quadratic bivariate** polynomials.

- Adleman and Manders (1978) show that solubility of a **bivariate quadratic** polynomial over natural numbers ($\mathbb{N}$) is NP-hard.

Solvability over $\mathbb{Z}$.

- Solvability over $\mathbb{Z}$ (integers) is decidable for **quadratic bivariate** polynomials.

- Adleman and Manders (1978) show that solubility of a **bivariate quadratic** polynomial over natural numbers ($\mathbb{N}$) is NP-hard.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

Solvability over finite fields

- **Problem:** Given a finite field $\mathbb{F}_q$ and a set of polynomial equations with $\mathbb{F}_q$-coefficients, determine whether the system has a common zero.

- (Easy) Solvability over finite fields is NP-complete. Remains NP-complete even when the field size q is 2 and the degree of each polynomial is bounded by 2.

Previous work

- **Previous Result:** Huang and Wong (1996)
  There is a randomized algorithm that decides the solvability of a system of n-variate equations with time complexity $\text{poly}(d^{c_n} \cdot m \cdot \log q)$ and parallel-time complexity $\text{poly}(c_n \cdot \log d \cdot \log m \cdot \log q)$.
  Here, $c_n = 2^{O(n)}$ is a constant that depends on n alone.

Previous work

- **Our Result:**
  There is a ~~randomized~~ deterministic algorithm that decides the solvability of a system of n-variate equations with time complexity $\mathrm{poly}(d^{c_n} \cdot m \cdot \log q)$ and parallel-time complexity $\mathrm{poly}(c_n \cdot \log d \cdot \log m \cdot \log q)$.
  Here, $c_n = 2^{O(n)}$ is a constant that depends on n alone.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

Univariate Equations.

- **Fermat's Little Theorem:** Over a finite field $\mathbb{F}_q$,

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

- This implies that a polynomial $f(x)$ has a $\mathbb{F}_q$-root if and only if

$$\gcd(f(x), x^q - x) \neq 1.$$

Univariate Equations.

- **Fermat's Little Theorem:** Over a finite field $\mathbb{F}_q$,

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

- This implies that a polynomial $f(x)$ has a $\mathbb{F}_q$-root if and only if

$$\gcd(f(x), x^q - x) \neq 1.$$

Univariate Equations - parallelization.

- More generally, univariate polynomials $f_1(x), \ldots, f_m(x) \in \mathbb{F}_q[x]$ have a common root if and only if

$$\gcd(f_1(x), \ldots, f_m(x), x^q - x) \neq 1.$$

- **Parallelization**:
  1. Divide the input polynomials into two equal sets and compute gcd of each set recursively in parallel.
  2. For computing gcd of two polynomials, use efficient algorithms for linear algebra.

Univariate Equations - parallelization.

- More generally, univariate polynomials $f_1(x), \ldots, f_m(x) \in \mathbb{F}_q[x]$ have a common root if and only if

$$\gcd(f_1(x), \ldots, f_m(x), x^q - x) \neq 1.$$

- **Parallelization**:
  1. Divide the input polynomials into two equal sets and compute gcd of each set recursively in parallel.
  2. For computing gcd of two polynomials, use efficient algorithms for linear algebra.

Univariate Equations - parallelization.

- More generally, univariate polynomials $f_1(x), \ldots, f_m(x) \in \mathbb{F}_q[x]$ have a common root if and only if

$$\gcd(f_1(x), \ldots, f_m(x), x^q - x) \neq 1.$$

- **Parallelization**:
  1. Divide the input polynomials into two equal sets and compute gcd of each set recursively in parallel.
  2. For computing gcd of two polynomials, use efficient algorithms for linear algebra.

Univariate Equations - parallelization.

- More generally, univariate polynomials $f_1(x), \ldots, f_m(x) \in \mathbb{F}_q[x]$ have a common root if and only if

$$\gcd(f_1(x), \ldots, f_m(x), x^q - x) \neq 1.$$

- **Parallelization**:
  1. Divide the input polynomials into two equal sets and compute gcd of each set recursively in parallel.
  2. For computing gcd of two polynomials, use efficient algorithms for linear algebra.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

Algorithm: Input and Output

- **Input.** A finite field $\mathbb{F}_q$ and polynomials

$$f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$$

.

- **Question.** Is there a solution to the system

$$f_1(x,y) = f_2(x,y) = \cdots = f_m(x,y) = 0?$$

Algorithm: Input and Output

- **Input.** A finite field $\mathbb{F}_q$ and polynomials

$$f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$$

.

- **Question.** Is there a solution to the system

$$f_1(x,y) = f_2(x,y) = \cdots = f_m(x,y) = 0?$$

Weil Theorem: intuition

- **Question:** Given a bivariate polynomial $f(x, y)\mathbb{F}_q[x, y]$, how many $\mathbb{F}_q$-roots does it have?
- (Easy exercise): For a randomly chosen monic polynomial $g(x) \in \mathbb{F}_q[x]$ of degree d, the expected number of $\mathbb{F}_q$-roots is 1.
- **Conjecture:** Any bivariate polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ has about q solutions.

Weil Theorem: intuition

- **Question:** Given a bivariate polynomial $f(x, y)\mathbb{F}_q[x, y]$, how many $\mathbb{F}_q$-roots does it have?
- (Easy exercise): For a randomly chosen monic polynomial $g(x) \in \mathbb{F}_q[x]$ of degree d, the expected number of $\mathbb{F}_q$-roots is 1.
- **Conjecture:** Any bivariate polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ has about q solutions.

Weil Theorem: intuition

- **Question:** Given a bivariate polynomial $f(x, y)\mathbb{F}_q[x, y]$, how many $\mathbb{F}_q$-roots does it have?
- (Easy exercise): For a randomly chosen monic polynomial $g(x) \in \mathbb{F}_q[x]$ of degree d, the expected number of $\mathbb{F}_q$-roots is 1.
- **Conjecture:** Any bivariate polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ has about q solutions.

Some counterexamples.

- Consider $f(x,y) = (x+y)(x-y) \in \mathbb{F}_q[x,y]$. It has about $2q$ roots.
- Suppose $\sqrt{-1} \notin \mathbb{F}_q$. Consider

$$f(x,y) = x^2 + y^2 \in \mathbb{F}_q[x,y].$$

- Note that

$$f(x,y) = (x + \sqrt{-1}y)(x - \sqrt{-1}y)$$

so that $f(x,y)$ has exactly one $\mathbb{F}_q$-solution, the point $(0,0)$.

Some counterexamples.

- Consider $f(x,y) = (x+y)(x-y) \in \mathbb{F}_q[x,y]$. It has about $2q$ roots.
- Suppose $\sqrt{-1} \notin \mathbb{F}_q$. Consider

$$f(x,y) = x^2 + y^2 \in \mathbb{F}_q[x,y].$$

- Note that

$$f(x,y) = (x+\sqrt{-1}y)(x-\sqrt{-1}y)$$

so that $f(x,y)$ has exactly one $\mathbb{F}_q$-solution, the point $(0,0)$.

Some counterexamples.

- Consider $f(x,y) = (x+y)(x-y) \in \mathbb{F}_q[x,y]$. It has about $2q$ roots.
- Suppose $\sqrt{-1} \notin \mathbb{F}_q$. Consider

$$f(x,y) = x^2 + y^2 \in \mathbb{F}_q[x,y].$$

- Note that

$$f(x,y) = (x + \sqrt{-1}y)(x - \sqrt{-1}y)$$

so that $f(x,y)$ has exactly one $\mathbb{F}_q$-solution, the point $(0,0)$.

Absolute Irreducibility.

- Notice that in both these counterexamples $f(x, y)$ admitted a factorization - either over $\mathbb{F}_q$ itself or over its algebraic closure.
- **Definition:** $f(x, y) \in \mathbb{F}_q[x, y]$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{F}_q$.
- **Example:** $f(x, y) = y^2 - (x^3 + 1) \in \mathbb{F}_5[x, y]$ is absolutely irreducible.
- **Example:** $f(x, y) = y^2 + x^2 \in \mathbb{F}_3[x, y]$ is irreducible but not absolutely irreducible since $f(x, y) = (y + \sqrt{-1}x)(y - \sqrt{-1}x)$ over $\mathbb{F}_3(\sqrt{-1})$

Absolute Irreducibility.

- Notice that in both these counterexamples $f(x, y)$ admitted a factorization - either over $\mathbb{F}_q$ itself or over its algebraic closure.
- **Definition:** $f(x, y) \in \mathbb{F}_q[x, y]$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{F}_q$.
- **Example:** $f(x, y) = y^2 - (x^3 + 1) \in \mathbb{F}_5[x, y]$ is absolutely irreducible.
- **Example:** $f(x, y) = y^2 + x^2 \in \mathbb{F}_3[x, y]$ is irreducible but not absolutely irreducible since $f(x, y) = (y + \sqrt{-1}x)(y - \sqrt{-1}x)$ over $\mathbb{F}_3(\sqrt{-1})$

Absolute Irreducibility.

- Notice that in both these counterexamples $f(x, y)$ admitted a factorization - either over $\mathbb{F}_q$ itself or over its algebraic closure.
- **Definition:** $f(x, y) \in \mathbb{F}_q[x, y]$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{F}_q$.
- **Example:** $f(x, y) = y^2 - (x^3 + 1) \in \mathbb{F}_5[x, y]$ is absolutely irreducible.
- **Example:** $f(x, y) = y^2 + x^2 \in \mathbb{F}_3[x, y]$ is irreducible but not absolutely irreducible since $f(x, y) = (y + \sqrt{-1}x)(y - \sqrt{-1}x)$ over $\mathbb{F}_3(\sqrt{-1})$

Absolute Irreducibility.

- Notice that in both these counterexamples $f(x, y)$ admitted a factorization - either over $\mathbb{F}_q$ itself or over its algebraic closure.
- **Definition:** $f(x, y) \in \mathbb{F}_q[x, y]$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{F}_q$.
- **Example:** $f(x, y) = y^2 - (x^3 + 1) \in \mathbb{F}_5[x, y]$ is absolutely irreducible.
- **Example:** $f(x, y) = y^2 + x^2 \in \mathbb{F}_3[x, y]$ is irreducible but not absolutely irreducible since $f(x, y) = (y + \sqrt{-1}x)(y - \sqrt{-1}x)$ over $\mathbb{F}_3(\sqrt{-1})$

The Main Ingredient: Weil Theorem

- **Theorem** [Weil et al]. If $f(x, y) \in \mathbb{F}_q[x, y]$ is an absolutely irreducible bivariate polynomial, then the equation $f(x, y) = 0$ has $q \pm O(d^2\sqrt{q})$ solutions.

- There is also a converse to this.

The Main Ingredient: Weil Theorem

- **Theorem** [Weil et al]. If $f(x, y) \in \mathbb{F}_q[x, y]$ is an absolutely irreducible bivariate polynomial, then the equation $f(x, y) = 0$ has $q \pm O(d^2\sqrt{q})$ solutions.

- There is also a converse to this.

The converse to Weil's theorem.

- Assume that $f(x, y)$ is $\mathbb{F}_q$-irreducible.
- **Fact** - If $f(x, y) \in \mathbb{F}_q[x, y]$ is $\mathbb{F}_q$-irreducible but **not** absolutely irreducible then any $\mathbb{F}_q$-point on the curve $f(x, y) = 0$ **is a repeated point** (point with multiplicity more than one) of the curve $f(x, y) = 0$.

- **Fact** - A point (a, b) on the curve $f(x, y) = 0$ is a repeated point on this curve if and only if it is a common solution to the equations

$$f(x, y) = 0 \ , \ (\frac{\partial f}{\partial x})(x, y) = 0$$

The converse to Weil's theorem.

- Assume that $f(x, y)$ is $\mathbb{F}_q$-irreducible.
- **Fact** - If $f(x, y) \in \mathbb{F}_q[x, y]$ is $\mathbb{F}_q$-irreducible but **not** absolutely irreducible then any $\mathbb{F}_q$-point on the curve $f(x, y) = 0$ **is a repeated point** (point with multiplicity more than one) of the curve $f(x, y) = 0$.

- **Fact** - A point (a, b) on the curve $f(x, y) = 0$ is a repeated point on this curve if and only if it is a common solution to the equations

$$f(x, y) = 0 \ , \ (\frac{\partial f}{\partial x})(x, y) = 0$$

The converse to Weil's theorem.

- Assume that $f(x, y)$ is $\mathbb{F}_q$-irreducible.
- **Fact** - If $f(x, y) \in \mathbb{F}_q[x, y]$ is $\mathbb{F}_q$-irreducible but **not** absolutely irreducible then any $\mathbb{F}_q$-point on the curve $f(x, y) = 0$ **is a repeated point** (point with multiplicity more than one) of the curve $f(x, y) = 0$.

- **Fact** - A point (a, b) on the curve $f(x, y) = 0$ is a repeated point on this curve if and only if it is a common solution to the equations

$$f(x, y) = 0 \ , \ (\frac{\partial f}{\partial x})(x, y) = 0$$

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

Algorithm Outline (One equation).

- **Input.** A finite field $\mathbb{F}_q$ and a polynomial $f(x, y)$ of degree d.
- If q is **small** ($\leq d^4$) use brute force.
- **Preprocessing** - Make $f(x, y)$ monic with respect to x and $f(x, 0)$ square-free.
- If $f(x, y)$ has an absolutely irreducible factor then output SOLUTION EXISTS,
- else if $f(x, y)$ and $\frac{\partial f}{\partial x}$ have a common root in $\mathbb{F}_q \times \mathbb{F}_q$ then output SOLUTION EXISTS,
- else output NO SOLUTION.

Algorithm Outline (One equation).

- **Input.** A finite field $\mathbb{F}_q$ and a polynomial $f(x, y)$ of degree d.
- If q is **small** ($\leq d^4$) use brute force.
- **Preprocessing** - Make $f(x, y)$ monic with respect to x and $f(x, 0)$ square-free.
- If $f(x, y)$ has an absolutely irreducible factor then output SOLUTION EXISTS,
- else if $f(x, y)$ and $\frac{\partial f}{\partial x}$ have a common root in $\mathbb{F}_q \times \mathbb{F}_q$ then output SOLUTION EXISTS,
- else output NO SOLUTION.

Algorithm Outline (One equation).

- **Input.** A finite field $\mathbb{F}_q$ and a polynomial $f(x, y)$ of degree d.
- If q is **small** ($\leq d^4$) use brute force.
- **Preprocessing** - Make $f(x, y)$ monic with respect to x and $f(x, 0)$ square-free.
- If $f(x, y)$ has an absolutely irreducible factor then output SOLUTION EXISTS,
- else if $f(x, y)$ and $\frac{\partial f}{\partial x}$ have a common root in $\mathbb{F}_q \times \mathbb{F}_q$ then output SOLUTION EXISTS,
- else output NO SOLUTION.

Algorithm Outline (One equation).

- **Input.** A finite field $\mathbb{F}_q$ and a polynomial $f(x, y)$ of degree d.
- If q is **small** ($\leq d^4$) use brute force.
- **Preprocessing** - Make $f(x, y)$ monic with respect to x and $f(x, 0)$ square-free.
- If $f(x, y)$ has an absolutely irreducible factor then output SOLUTION EXISTS,
- else if $f(x, y)$ and $\frac{\partial f}{\partial x}$ have a common root in $\mathbb{F}_q \times \mathbb{F}_q$ then output SOLUTION EXISTS,
- else output NO SOLUTION.

Algorithm Outline (One equation).

- **Input.** A finite field $\mathbb{F}_q$ and a polynomial $f(x, y)$ of degree d.
- If q is **small** ($\leq d^4$) use brute force.
- **Preprocessing** - Make $f(x, y)$ monic with respect to x and $f(x, 0)$ square-free.
- If $f(x, y)$ has an absolutely irreducible factor then output SOLUTION EXISTS,
- else if $f(x, y)$ and $\frac{\partial f}{\partial x}$ have a common root in $\mathbb{F}_q \times \mathbb{F}_q$ then output SOLUTION EXISTS,
- else output NO SOLUTION.

Algorithm Outline (One equation).

- **Input.** A finite field $\mathbb{F}_q$ and a polynomial $f(x, y)$ of degree d.
- If q is **small** ($\leq d^4$) use brute force.
- **Preprocessing** - Make $f(x, y)$ monic with respect to x and $f(x, 0)$ square-free.
- If $f(x, y)$ has an absolutely irreducible factor then output SOLUTION EXISTS,
- else if $f(x, y)$ and $\frac{\partial f}{\partial x}$ have a common root in $\mathbb{F}_q \times \mathbb{F}_q$ then output SOLUTION EXISTS,
- else output NO SOLUTION.

Algorithm Outline (General case).

- **Input.** Polynomials $f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$.
- If $m = 1$ use algorithm above.
- Compute $h(x,y) \stackrel{\text{def}}{=} \gcd(f_1(x,y), f_2(x,y))$
- Recursively determine if there is a solution to the system $h(x,y) = f_3(x,y) = \cdots = f_m(x,y) = 0$. If yes output **SOLUTION EXISTS**.
- Determine if there is an $\mathbb{F}_q$-solution to the system

$$\frac{f_1}{h} = \frac{f_2}{h} = f_3 = \cdots = f_m = 0$$

Note. Now $\frac{f_1}{h}$ and $\frac{f_2}{h}$ are coprime.

Algorithm Outline (General case).

- **Input.** Polynomials $f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$.
- If $m = 1$ use algorithm above.
- Compute $h(x,y) \stackrel{\text{def}}{=} \gcd(f_1(x,y), f_2(x,y))$
- Recursively determine if there is a solution to the system $h(x,y) = f_3(x,y) = \cdots = f_m(x,y) = 0$. If yes output **SOLUTION EXISTS**.
- Determine if there is an $\mathbb{F}_q$-solution to the system

$$\frac{f_1}{h} = \frac{f_2}{h} = f_3 = \cdots = f_m = 0$$

Note. Now $\frac{f_1}{h}$ and $\frac{f_2}{h}$ are coprime.

Algorithm Outline (General case).

- **Input.** Polynomials $f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$.
- If $m = 1$ use algorithm above.
- Compute $h(x,y) \stackrel{\text{def}}{=} \gcd(f_1(x,y), f_2(x,y))$
- Recursively determine if there is a solution to the system $h(x,y) = f_3(x,y) = \cdots = f_m(x,y) = 0$. If yes output **SOLUTION EXISTS**.
- Determine if there is an $\mathbb{F}_q$-solution to the system

$$\frac{f_1}{h} = \frac{f_2}{h} = f_3 = \cdots = f_m = 0$$

Note. Now $\frac{f_1}{h}$ and $\frac{f_2}{h}$ are coprime.

Algorithm Outline (General case).

- **Input.** Polynomials $f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$.
- If $m = 1$ use algorithm above.
- Compute $h(x,y) \stackrel{\text{def}}{=} \gcd(f_1(x,y), f_2(x,y))$
- Recursively determine if there is a solution to the system $h(x,y) = f_3(x,y) = \cdots = f_m(x,y) = 0$. If yes output **SOLUTION EXISTS**.
- Determine if there is an $\mathbb{F}_q$-solution to the system

$$\frac{f_1}{h} = \frac{f_2}{h} = f_3 = \cdots = f_m = 0$$

Note. Now $\frac{f_1}{h}$ and $\frac{f_2}{h}$ are coprime.

Algorithm Outline (General case).

- **Input.** Polynomials $f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$.
- If $m = 1$ use algorithm above.
- Compute $h(x,y) \stackrel{\text{def}}{=} \gcd(f_1(x,y), f_2(x,y))$
- Recursively determine if there is a solution to the system $h(x,y) = f_3(x,y) = \cdots = f_m(x,y) = 0$. If yes output **SOLUTION EXISTS**.
- Determine if there is an $\mathbb{F}_q$-solution to the system

$$\frac{f_1}{h} = \frac{f_2}{h} = f_3 = \cdots = f_m = 0$$

Note. Now $\frac{f_1}{h}$ and $\frac{f_2}{h}$ are coprime.

Some questions.

- **First subproblem.** Determine whether $f(x, y)$ has any absolutely irreducible factor?
- **Second subproblem.** Given polynomials

$$f_1(x, y), f_2(x, y), \cdots, f_m(x, y)$$

with $f_1(x, y)$ and $f_2(x, y)$ coprime, determine if the system has a solution in $\mathbb{F}_q \times \mathbb{F}_q$.

Some questions.

- **First subproblem.** Determine whether $f(x, y)$ has any absolutely irreducible factor?
- **Second subproblem.** Given polynomials

$$f_1(x, y), f_2(x, y), \cdots, f_m(x, y)$$

with $f_1(x, y)$ and $f_2(x, y)$ coprime, determine if the system has a solution in $\mathbb{F}_q \times \mathbb{F}_q$.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

Resultants

- **Fact** - Suppose that (a, b) is a common zero of $f_1(x, y)$ and $f_2(x, y)$. Then a is a root of $\rho(x) \stackrel{\text{def}}{=} \text{Resultant}_y(f_1(x, y), f_2(x, y))$

If we could factor polynomials.

- Suppose that all the $\mathbb{F}_q$-roots of $\rho(x)$ are $a_1, a_2, \cdots, a_t$
- For each i do:
- If $\gcd(f_1(a_i, y), f_2(a_i, y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

If we could factor polynomials.

- Suppose that all the $\mathbb{F}_q$-roots of $\rho(x)$ are $a_1, a_2, \cdots, a_t$
- For each i do:
- If $\gcd(f_1(a_i, y), f_2(a_i, y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

If we could factor polynomials.

- Suppose that all the $\mathbb{F}_q$-roots of $\rho(x)$ are $a_1, a_2, \cdots, a_t$
- For each i do:
- If $\gcd(f_1(a_i, y), f_2(a_i, y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

If we could factor polynomials.

- Suppose that all the $\mathbb{F}_q$-roots of $\rho(x)$ are $a_1, a_2, \cdots, a_t$
- For each i do:
- If $\gcd(f_1(a_i, y), f_2(a_i, y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

To do this deterministically:

- Compute $\hat{\rho}(x) \stackrel{\text{def}}{=} gcd(\rho(x), x^q - x)$
- Let R be the ring $\mathbb{F}_q[z]/\langle\hat{\rho}(z)\rangle$
- **Main Idea.** Work over R, pretending that z is a $\mathbb{F}_q$-root of $\rho(x)$.
- Over R: If $\gcd(f_1(z,y), f_2(z,y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

To do this deterministically:

- Compute $\hat{\rho}(x) \stackrel{\text{def}}{=} gcd(\rho(x), x^q - x)$
- Let R be the ring $\mathbb{F}_q[z]/\langle\hat{\rho}(z)\rangle$
- **Main Idea.** Work over R, pretending that z is a $\mathbb{F}_q$-root of $\rho(x)$.
- Over R: If $\gcd(f_1(z,y), f_2(z,y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

To do this deterministically:

- Compute $\hat{\rho}(x) \stackrel{\text{def}}{=} gcd(\rho(x), x^q - x)$
- Let R be the ring $\mathbb{F}_q[z]/\langle\hat{\rho}(z)\rangle$
- **Main Idea.** Work over R, pretending that z is a $\mathbb{F}_q$-root of $\rho(x)$.
- Over R: If $\gcd(f_1(z,y), f_2(z,y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

To do this deterministically:

- Compute $\hat{\rho}(x) \stackrel{\text{def}}{=} gcd(\rho(x), x^q - x)$
- Let R be the ring $\mathbb{F}_q[z]/\langle\hat{\rho}(z)\rangle$
- **Main Idea.** Work over R, pretending that z is a $\mathbb{F}_q$-root of $\rho(x)$.
- Over R: If $\gcd(f_1(z,y), f_2(z,y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

To do this deterministically:

- Compute $\hat{\rho}(x) \stackrel{\text{def}}{=} gcd(\rho(x), x^q - x)$
- Let R be the ring $\mathbb{F}_q[z]/\langle\hat{\rho}(z)\rangle$
- **Main Idea.** Work over R, pretending that z is a $\mathbb{F}_q$-root of $\rho(x)$.
- Over R: If $\gcd(f_1(z,y), f_2(z,y), y^q - y) \neq 1$ output **SOLUTION EXISTS**.
- Else output **NO SOLUTION**.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

If we could factor (univariate) polynomials.

- **First subproblem.** Determine whether $f(x, y)$ has any absolutely irreducible factor?
- If we can factor **univariate** polynomials deterministically then we can also factor a **bivariate** polynomial $f(x, y)$ into its $\mathbb{F}_q$-irreducible factors by a procedure known as Hensel Lifting.
- For an $\mathbb{F}_q$-irreducible factor $f_i(x, y)$ of $f(x, y)$ there is a deterministic polynomial-time algorithm for testing its absolute irreducibility (Kaltofen, 85).

If we could factor (univariate) polynomials.

- **First subproblem.** Determine whether $f(x, y)$ has any absolutely irreducible factor?
- If we can factor **univariate** polynomials deterministically then we can also factor a **bivariate** polynomial $f(x, y)$ into its $\mathbb{F}_q$-irreducible factors by a procedure known as Hensel Lifting.
- For an $\mathbb{F}_q$-irreducible factor $f_i(x, y)$ of $f(x, y)$ there is a deterministic polynomial-time algorithm for testing its absolute irreducibility (Kaltofen, 85).

If we could factor (univariate) polynomials.

- **First subproblem.** Determine whether $f(x, y)$ has any absolutely irreducible factor?
- If we can factor **univariate** polynomials deterministically then we can also factor a **bivariate** polynomial $f(x, y)$ into its $\mathbb{F}_q$-irreducible factors by a procedure known as Hensel Lifting.
- For an $\mathbb{F}_q$-irreducible factor $f_i(x, y)$ of $f(x, y)$ there is a deterministic polynomial-time algorithm for testing its absolute irreducibility (Kaltofen, 85).

Factoring $f(x, y)$ - Hensel Lifting.

- A reduction algorithm: There is a deterministic algorithm (Hensel Lifting) that given a root of $f(x, 0)$, **lifts** this root to compute a factor of $f(x, y)$.

- Hensel Lifting requires a root of $f(x, 0)$ to work but we do not have a root.
- **Idea:** Manufacture an **artificial** root of $f(x, 0)$ and work with that!

Factoring $f(x, y)$ - Hensel Lifting.

- A reduction algorithm: There is a deterministic algorithm (Hensel Lifting) that given a root of $f(x, 0)$, **lifts** this root to compute a factor of $f(x, y)$.

- Hensel Lifting requires a root of $f(x, 0)$ to work but we do not have a root.
- **Idea:** Manufacture an **artificial** root of $f(x, 0)$ and work with that!

Factoring $f(x, y)$ - Hensel Lifting.

- A reduction algorithm: There is a deterministic algorithm (Hensel Lifting) that given a root of $f(x, 0)$, **lifts** this root to compute a factor of $f(x, y)$.

- Hensel Lifting requires a root of $f(x, 0)$ to work but we do not have a root.
- **Idea:** Manufacture an **artificial** root of $f(x, 0)$ and work with that!

Factoring $f(x, y)$ - Main Idea.

- Let $\rho(z) = f(z, 0)$. Let $R \stackrel{\text{def}}{=} \mathbb{F}_q[z]/\langle \rho(z) \rangle$.
- **Main Idea.** Do Hensel Lifting over the ring R, pretending that $(x - z)$ is an **irreducible** factor of $f(x, 0)$ and **if all goes well** obtain a **artificial factor** $\tilde{f}$ of f.
- **Main Idea (Part II).** If something goes wrong, **use** that to factor the ring R and thereby the polynomial $f(x, y)$.

Factoring $f(x, y)$ - Main Idea.

- Let $\rho(z) = f(z, 0)$. Let $R \stackrel{\text{def}}{=} \mathbb{F}_q[z]/\langle \rho(z) \rangle$.
- **Main Idea.** Do Hensel Lifting over the ring R, pretending that $(x - z)$ is an **irreducible** factor of $f(x, 0)$ and **if all goes well** obtain a **artificial factor** $\tilde{f}$ of f.
- **Main Idea (Part II).** If something goes wrong, **use** that to factor the ring R and thereby the polynomial $f(x, y)$.

Factoring $f(x, y)$ - Main Idea.

- Let $\rho(z) = f(z, 0)$. Let $R \stackrel{\text{def}}{=} \mathbb{F}_q[z]/\langle \rho(z) \rangle$.
- **Main Idea.** Do Hensel Lifting over the ring R, pretending that $(x - z)$ is an **irreducible** factor of $f(x, 0)$ and **if all goes well** obtain a **artificial factor** $\tilde{f}$ of f.
- **Main Idea (Part II).** If something goes wrong, **use** that to factor the ring R and thereby the polynomial $f(x, y)$.

Factoring $f(x, y)$ - Main Idea.

- **The Structure of R.** R is a **direct sum** of component field, each field corresponding to one particular irreducible polynomial of $f(x, 0)$.
- If $\rho(z) = \prod_i \rho_i(z)$ then $R = \bigoplus_i \mathbb{F}_q[z]/\langle \rho_i(z) \rangle$
- Suppose $f(x, y) = f_1(x, y) f_2(x, y)$. Then each component $\mathbb{F}_q[z]/\langle \rho_i(z) \rangle$ of R corresponds to either the factor $f_1(x, y)$ or to the factor $f_2(x, y)$ depending on whether $\rho_i(z)$ divides $f_1(z, 0)$ or $f_2(z, 0)$.

Factoring $f(x, y)$ - Main Idea.

- **The Structure of R.** R is a **direct sum** of component field, each field corresponding to one particular irreducible polynomial of $f(x, 0)$.
- If $\rho(z) = \prod_i \rho_i(z)$ then $R = \bigoplus_i \mathbb{F}_q[z]/\langle \rho_i(z) \rangle$
- Suppose $f(x, y) = f_1(x, y) f_2(x, y)$. Then each component $\mathbb{F}_q[z]/\langle \rho_i(z) \rangle$ of R corresponds to either the factor $f_1(x, y)$ or to the factor $f_2(x, y)$ depending on whether $\rho_i(z)$ divides $f_1(z, 0)$ or $f_2(z, 0)$.

Factoring $f(x, y)$ - Main Idea.

- **The Structure of R.** R is a **direct sum** of component field, each field corresponding to one particular irreducible polynomial of $f(x, 0)$.
- If $\rho(z) = \prod_i \rho_i(z)$ then $R = \bigoplus_i \mathbb{F}_q[z]/\langle \rho_i(z) \rangle$
- Suppose $f(x, y) = f_1(x, y) f_2(x, y)$. Then each component $\mathbb{F}_q[z]/\langle \rho_i(z) \rangle$ of R corresponds to either the factor $f_1(x, y)$ or to the factor $f_2(x, y)$ depending on whether $\rho_i(z)$ divides $f_1(z, 0)$ or $f_2(z, 0)$.

Distinct degree factorization

- **Distinct degree factorization** . Gao, Kaltofen, Lauder (2004)
- Assume $f(x,y) = f_1(x,y)f_2(x,y)$ and $\deg(f_1) = 2$, $\deg(f_2) = 3$.
- **Question.** What will be the degree of the artificial factor $\tilde{f}(x,y)$? Will it be 2 or 3?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Distinct degree factorization

- **Distinct degree factorization** . Gao, Kaltofen, Lauder (2004)
- Assume $f(x,y) = f_1(x,y)f_2(x,y)$ and $\deg(f_1) = 2$, $\deg(f_2) = 3$.
- **Question.** What will be the degree of the artificial factor $\tilde{f}(x,y)$? Will it be 2 or 3?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Distinct degree factorization

- **Distinct degree factorization** . Gao, Kaltofen, Lauder (2004)
- Assume $f(x,y) = f_1(x,y)f_2(x,y)$ and $\deg(f_1) = 2$, $\deg(f_2) = 3$.
- **Question.** What will be the degree of the artificial factor $\tilde{f}(x,y)$? Will it be 2 or 3?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Distinct degree factorization

- **Distinct degree factorization** . Gao, Kaltofen, Lauder (2004)
- Assume $f(x,y) = f_1(x,y)f_2(x,y)$ and $\deg(f_1) = 2\,,\ \deg(f_2) = 3$.
- **Question.** What will be the degree of the artificial factor $\tilde{f}(x,y)$? Will it be 2 or 3?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Factorization

- Now assume $f(x,y) = f_1(x,y)f_2(x,y)$ and both factors have the same degree 4. But f_1 splits completely over $\mathbb{F}_q$ itself whereas f_2 splits completely only over $\mathbb{F}_{q^2}$.
- **Lemma.** If $\alpha \in \bar{\mathbb{F}}_q$ is an **actual root** of $f_1(x,0)$ but not of $f_2(x,0)$ then Hensel Lifting over $\mathbb{F}_q(\alpha)$ using α will yield an absolutely irreducible factor of $f_1(x,y)$.
- **Question.** What will be the degree of the artificial-factor $\tilde{f}(x,y)$ - 4 or 2?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Factorization

- Now assume $f(x,y) = f_1(x,y)f_2(x,y)$ and both factors have the same degree 4. But f_1 splits completely over $\mathbb{F}_q$ itself whereas f_2 splits completely only over $\mathbb{F}_{q^2}$.
- **Lemma.** If $\alpha \in \bar{\mathbb{F}}_q$ is an **actual root** of $f_1(x,0)$ but not of $f_2(x,0)$ then Hensel Lifting over $\mathbb{F}_q(\alpha)$ using α will yield an absolutely irreducible factor of $f_1(x,y)$.
- **Question.** What will be the degree of the artificial-factor $\tilde{f}(x,y)$ - 4 or 2?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Factorization

- Now assume $f(x,y) = f_1(x,y)f_2(x,y)$ and both factors have the same degree 4. But f_1 splits completely over $\mathbb{F}_q$ itself whereas f_2 splits completely only over $\mathbb{F}_{q^2}$.
- **Lemma.** If $\alpha \in \bar{\mathbb{F}}_q$ is an **actual root** of $f_1(x,0)$ but not of $f_2(x,0)$ then Hensel Lifting over $\mathbb{F}_q(\alpha)$ using α will yield an absolutely irreducible factor of $f_1(x,y)$.
- **Question.** What will be the degree of the artificial-factor $\tilde{f}(x,y)$ - 4 or 2?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Factorization

- Now assume $f(x,y) = f_1(x,y)f_2(x,y)$ and both factors have the same degree 4. But f_1 splits completely over $\mathbb{F}_q$ itself whereas f_2 splits completely only over $\mathbb{F}_{q^2}$.
- **Lemma.** If $\alpha \in \bar{\mathbb{F}}_q$ is an **actual root** of $f_1(x,0)$ but not of $f_2(x,0)$ then Hensel Lifting over $\mathbb{F}_q(\alpha)$ using α will yield an absolutely irreducible factor of $f_1(x,y)$.
- **Question.** What will be the degree of the artificial-factor $\tilde{f}(x,y)$ - 4 or 2?
- **Ans.** Neither. Hensel lifting will fail and we can factor $f(x,y)$!

Summary for this section.

- There is a **deterministic** polynomial-time algorithm for the following problem -
- **Bivariate Solvability :** Given a finite field $\mathbb{F}_q$ and a set of polynomials

$$f_1(x, y), f_2(x, y), \cdots, f_m(x, y) \in \mathbb{F}_q[x, y]$$

determine whether exists a point $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$ such that

$$f_1(a, b) = f_2(a, b) = \cdots = f_m(a, b) = 0$$

Summary for this section.

- There is a **deterministic** polynomial-time algorithm for the following problem -
- **Bivariate Solvability :** Given a finite field $\mathbb{F}_q$ and a set of polynomials

$$f_1(x,y), f_2(x,y), \cdots, f_m(x,y) \in \mathbb{F}_q[x,y]$$

determine whether exists a point $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ such that

$$f_1(a,b) = f_2(a,b) = \cdots = f_m(a,b) = 0$$

Parallelization.

- Divide the given set of polynomials $\{f_1, \ldots, f_m\}$ into two sets $\{f_1, \ldots, f_{m/2}\}$ and $\{f_{m/2+1}, \ldots, f_m\}$ and recursively in parallel "compute the common solutions" of each of these sets.
- "Combine the common solutions" to obtain the common solutions for the given system of equations.
- Use fast parallel algorithms for linear algebra.
- This gives a $\text{poly}(\log d \cdot \log m \cdot \log q)$-time parallel algorithm for bivariate solvability.

Parallelization.

- Divide the given set of polynomials $\{f_1, \ldots, f_m\}$ into two sets $\{f_1, \ldots, f_{m/2}\}$ and $\{f_{m/2+1}, \ldots, f_m\}$ and recursively in parallel "compute the common solutions" of each of these sets.
- "Combine the common solutions" to obtain the common solutions for the given system of equations.
- Use fast parallel algorithms for linear algebra.
- This gives a $\text{poly}(\log d \cdot \log m \cdot \log q)$-time parallel algorithm for bivariate solvability.

Parallelization.

- Divide the given set of polynomials $\{f_1, \ldots, f_m\}$ into two sets $\{f_1, \ldots, f_{m/2}\}$ and $\{f_{m/2+1}, \ldots, f_m\}$ and recursively in parallel "compute the common solutions" of each of these sets.
- "Combine the common solutions" to obtain the common solutions for the given system of equations.
- Use fast parallel algorithms for linear algebra.
- This gives a $\mathrm{poly}(\log d \cdot \log m \cdot \log q)$-time parallel algorithm for bivariate solvability.

Parallelization.

- Divide the given set of polynomials $\{f_1, \ldots, f_m\}$ into two sets $\{f_1, \ldots, f_{m/2}\}$ and $\{f_{m/2+1}, \ldots, f_m\}$ and recursively in parallel "compute the common solutions" of each of these sets.
- "Combine the common solutions" to obtain the common solutions for the given system of equations.
- Use fast parallel algorithms for linear algebra.
- This gives a $\text{poly}(\log d \cdot \log m \cdot \log q)$-time parallel algorithm for bivariate solvability.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

The algorithm for general n.

- There is a deterministic reduction of Solvability to the problem of determining if one ℓ-variate polynomial ($\ell \leq n$) over $\mathbb{F}_q$ has a solution or not.

- We will now briefly mention some ideas in this reduction.

The algorithm for general n.

- There is a deterministic reduction of Solvability to the problem of determining if one ℓ-variate polynomial ($\ell \leq n$) over $\mathbb{F}_q$ has a solution or not.

- We will now briefly mention some ideas in this reduction.

Basic Algebraic Geometry - I.

- Let $\mathtt{X} \subset \overline{\mathbb{F}}_q^n$ be the set of all common zeroes of the system of polynomial equations

$$f_1(\bar{\mathbf{x}}) = \ldots = f_m(\bar{\mathbf{x}}) = 0.$$

- We next define a ring $R_{\mathtt{X}}$ which will capture the algebraic set $\mathtt{X}$. The structure of $R_{\mathtt{X}}$ shall correspond to the structure of $\mathtt{X}$.
- The ring $R_{\mathtt{X}}$ is defined as

$$R_{\mathtt{X}} \stackrel{\text{def}}{=} \mathbb{F}_q[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle.$$

Basic Algebraic Geometry - I.

- Let $\mathtt{X} \subset \overline{\mathbb{F}}_q^n$ be the set of all common zeroes of the system of polynomial equations

$$f_1(\bar{\mathbf{x}}) = \ldots = f_m(\bar{\mathbf{x}}) = 0.$$

- We next define a ring $R_{\mathtt{X}}$ which will capture the algebraic set $\mathtt{X}$. The structure of $R_{\mathtt{X}}$ shall correspond to the structure of $\mathtt{X}$.
- The ring $R_{\mathtt{X}}$ is defined as

$$R_{\mathtt{X}} \stackrel{\text{def}}{=} \mathbb{F}_q[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle.$$

Basic Algebraic Geometry - I.

- Let $\mathtt{X} \subset \overline{\mathbb{F}}_q^n$ be the set of all common zeroes of the system of polynomial equations

$$f_1(\bar{\mathbf{x}}) = \ldots = f_m(\bar{\mathbf{x}}) = 0.$$

- We next define a ring $R_{\mathtt{X}}$ which will capture the algebraic set $\mathtt{X}$. The structure of $R_{\mathtt{X}}$ shall correspond to the structure of $\mathtt{X}$.
- The ring $R_{\mathtt{X}}$ is defined as

$$R_{\mathtt{X}} \stackrel{\text{def}}{=} \mathbb{F}_q[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle.$$

Basic Algebraic Geometry - II.

- Homomorphisms from $R_{\mathtt{X}}$ to $\mathbb{F}_q$ correspond to $\mathbb{F}_q$-rational points in $\mathtt{X}$.
- A point $\bar{\mathbf{a}} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ is an $\mathbb{F}_q$-rational point in $\mathtt{X}$ if and only if the map

$$\phi : R_{\mathtt{X}} \mapsto \mathbb{F}_q, \ \phi : x_i \mapsto a_i \ \forall 1 \leq i \leq n$$

is a homomorphism.

Basic Algebraic Geometry - II.

- Homomorphisms from $R_{\mathtt{X}}$ to $\mathbb{F}_q$ correspond to $\mathbb{F}_q$-rational points in $\mathtt{X}$.
- A point $\bar{\mathbf{a}} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ is an $\mathbb{F}_q$-rational point in $\mathtt{X}$ if and only if the map

$$\phi : R_{\mathtt{X}} \mapsto \mathbb{F}_q, \ \phi : x_i \mapsto a_i \ \forall 1 \leq i \leq n$$

is a homomorphism.

Basic Algebraic Geometry - III.

- Let $R_{\mathtt{X}}^{fr}$ be the ring of fractions of $R_{\mathtt{X}}$.
- **Theorem:** For $\mathtt{X}$ satisfying some mild conditions, $R_{\mathtt{X}}^{fr}$ is isomorphic to a ring of the form

$$R_{\mathtt{Y}}^{fr} = \mathbb{F}_q(y_1, \ldots, y_\ell)/\langle g(y_1, \ldots, y_l)\rangle.$$

- The reduction from m equations to 1 equation then consists of computing such an equivalent ring $R_{\mathtt{Y}}^{fr}$.

Basic Algebraic Geometry - III.

- Let $R_{\mathtt{X}}^{fr}$ be the ring of fractions of $R_{\mathtt{X}}$.
- **Theorem:** For $\mathtt{X}$ satisfying some mild conditions, $R_{\mathtt{X}}^{fr}$ is isomorphic to a ring of the form

$$R_{\mathtt{Y}}^{fr} = \mathbb{F}_q(y_1, \ldots, y_\ell)/\langle g(y_1, \ldots, y_l)\rangle.$$

- The reduction from m equations to 1 equation then consists of computing such an equivalent ring $R_{\mathtt{Y}}^{fr}$.

Basic Algebraic Geometry - III.

- Let $R_{\mathtt{X}}^{fr}$ be the ring of fractions of $R_{\mathtt{X}}$.
- **Theorem:** For $\mathtt{X}$ satisfying some mild conditions, $R_{\mathtt{X}}^{fr}$ is isomorphic to a ring of the form

$$R_{\mathtt{Y}}^{fr} = \mathbb{F}_q(y_1, \ldots, y_\ell)/\langle g(y_1, \ldots, y_l)\rangle.$$

- The reduction from m equations to 1 equation then consists of computing such an equivalent ring $R_{\mathtt{Y}}^{fr}$.

Summary.

- Combining a deterministic version of this reduction algorithm with a suitable generalization of Weil's theorem, we get:
- **Theorem:** There is a deterministic algorithm for the Solvability problem whose running time is bounded by a polynomial in $(d^{c_n} \cdot m \log q)$, where $c_n = 2^{O(n)}$ is a constant that depends on n alone.

Summary.

- Combining a deterministic version of this reduction algorithm with a suitable generalization of Weil's theorem, we get:
- **Theorem:** There is a deterministic algorithm for the Solvability problem whose running time is bounded by a polynomial in $(d^{c_n} \cdot m \log q)$, where $c_n = 2^{O(n)}$ is a constant that depends on n alone.

Outline

Motivation
- Problem Statement
- Solvability over finite fields
- System of univariate equations.

System of Bivariate Equations
- Bivariate Solvability
- Algorithm Overview
- Second Subproblem
- First Subproblem

Generalization.
- Outline of steps in generalization.
- A conjecture.

Polynomial Factorization

- Suppose $f(x, y) \in \mathbb{F}_q[x, y]$ where $f(x, y) = f_1(x, y)f_2(x, y)$ and the two factors $f_1(x, y)$ and $f_2(x, y)$ are **not isomorphic**.
- **Conjecture.** There is a deterministic polynomial-time algorithm that given $f(x, y)$, recovers the factors $f_1(x, y)$ and $f_2(x, y)$.
- If this conjecture is true, then polynomial factorization itself can be done in deterministic polynomial time!

Polynomial Factorization

- Suppose $f(x, y) \in \mathbb{F}_q[x, y]$ where $f(x, y) = f_1(x, y)f_2(x, y)$ and the two factors $f_1(x, y)$ and $f_2(x, y)$ are **not isomorphic**.
- **Conjecture.** There is a deterministic polynomial-time algorithm that given $f(x, y)$, recovers the factors $f_1(x, y)$ and $f_2(x, y)$.
- If this conjecture is true, then polynomial factorization itself can be done in deterministic polynomial time!

Polynomial Factorization

- Suppose $f(x, y) \in \mathbb{F}_q[x, y]$ where $f(x, y) = f_1(x, y)f_2(x, y)$ and the two factors $f_1(x, y)$ and $f_2(x, y)$ are **not isomorphic**.
- **Conjecture.** There is a deterministic polynomial-time algorithm that given $f(x, y)$, recovers the factors $f_1(x, y)$ and $f_2(x, y)$.
- If this conjecture is true, then polynomial factorization itself can be done in deterministic polynomial time!

Thank You!

Questions?