Asymptotically faster quantum algorithms to solve multivariate quadratic equations

Daniel J. Bernstein, Bo-Yin Yang

https://eprint.iacr.org/2017/1206.pdf

Conjectured asymptotic random MQ

How quickly can we solve a system of
m quadratic equations in n variables over $\mathbf{F}_q$?

Conjectured asymptotic random MQ

How quickly can we solve a system of m quadratic equations in n variables over $\mathbf{F}_q$?

Focus on **random** systems: each coefficient in equations is chosen randomly. Solving this problem for $m \approx n$ conjecturally breaks, e.g., $\mathrm{HFE}^{\mathrm{v}-}$ signatures.

Conjectured asymptotic random MQ

How quickly can we solve a system of
m quadratic equations in n variables over $\mathbf{F}_q$?

Focus on **random** systems:
each coefficient in equations is chosen randomly.
Solving this problem for $m \approx n$
conjecturally breaks, e.g., $\mathrm{HFE}^{\mathrm{v}-}$ signatures.

Focus on **asymptotic** cost exponents:
scalability as $n \to \infty$ with $m/n \to \mu$.

Conjectured asymptotic random MQ

How quickly can we solve a system of
m quadratic equations in n variables over $\mathbf{F}_q$?

Focus on **random** systems:
each coefficient in equations is chosen randomly.
Solving this problem for $m \approx n$
conjecturally breaks, e.g., $\mathrm{HFE}^{\mathrm{v}-}$ signatures.

Focus on **asymptotic** cost exponents:
scalability as $n \to \infty$ with $m/n \to \mu$.

Focus on best **conjectured** speeds.

Previous exponents for $q = 2$ and $\mu = 1$

$2^{(e+o(1))n}$ operations as $n \to \infty$:

- $e = 1$ proven: Brute force.
- $e = 0.8765$ proven:
  2017 Lokshtanov–Paturi–Tamaki–Williams–Yu.

Previous exponents for $q = 2$ and $\mu = 1$

$2^{(e+o(1))n}$ operations as $n \to \infty$:

- $e = 1$ proven: Brute force.
- $e = 0.8765$ proven: 2017 Lokshtanov–Paturi–Tamaki–Williams–Yu.
- $e = 0.87280\ldots$: "XL". Algorithm from 1981 Lazard. Analysis and optimization from 2004 Yang–Chen–Courtois.

Previous exponents for $q = 2$ and $\mu = 1$

$2^{(e+o(1))n}$ operations as $n \to \infty$:

- $e = 1$ proven: Brute force.
- $e = 0.8765$ proven: 2017 Lokshtanov–Paturi–Tamaki–Williams–Yu.
- $e = 0.87280\ldots$: "XL". Algorithm from 1981 Lazard. Analysis and optimization from 2004 Yang–Chen–Courtois.
- $e = 0.79106\ldots$: "FXL". Algorithm from 2000 Courtois–Klimov–Patarin–Shamir. Analysis and optimization from 2004 Yang–Chen–Courtois.

Previous exponents for $q = 2$ and $\mu = 1$

$2^{(e+o(1))n}$ operations as $n \to \infty$:

- $e = 1$ proven: Brute force.
- $e = 0.8765$ proven: 2017 Lokshtanov–Paturi–Tamaki–Williams–Yu.
- $e = 0.87280\ldots$: "XL". Algorithm from 1981 Lazard. Analysis and optimization from 2004 Yang–Chen–Courtois.
- $e = 0.79106\ldots$: "FXL". Algorithm from 2000 Courtois–Klimov–Patarin–Shamir. Analysis and optimization from 2004 Yang–Chen–Courtois.
- $e = 0.5$ proven: Grover's quantum algorithm.

New exponents

$e = 0.46240\ldots$:
"GroverXL", 2017.12.15 Bernstein–Yang.
Independently "QuantumBooleanSolve", 2017.12.19 Faugère–Horan–Kahrobaei–Kaplan–Kashefi–Perret.

New exponents

$e = 0.46240\ldots$:
"GroverXL", 2017.12.15 Bernstein–Yang.
Independently "QuantumBooleanSolve", 2017.12.19 Faugère–Horan–Kahrobaei–Kaplan–Kashefi–Perret.

More results in 2017.12.15 (not 2017.12.19) paper:

- Area-time product on mesh: $0.47210\ldots$.
- Area under specified time limits.

New exponents

$e = 0.46240\ldots$:
"GroverXL", 2017.12.15 Bernstein–Yang.
Independently "QuantumBooleanSolve", 2017.12.19 Faugère–Horan–Kahrobaei–Kaplan–Kashefi–Perret.

More results in 2017.12.15 (not 2017.12.19) paper:

- Area-time product on mesh: $0.47210\ldots$.
- Area under specified time limits.
- $q > 2$: e.g., $0.72468\ldots$ (base 2) for $q = 3$.

New exponents

$e = 0.46240\ldots$:
"GroverXL", 2017.12.15 Bernstein–Yang.
Independently "QuantumBooleanSolve", 2017.12.19 Faugère–Horan–Kahrobaei–Kaplan–Kashefi–Perret.

More results in 2017.12.15 (not 2017.12.19) paper:

- Area-time product on mesh: $0.47210\ldots$.
- Area under specified time limits.
- $q > 2$: e.g., $0.72468\ldots$ (base 2) for $q = 3$.
- $\mu > 1$: e.g., $0.65688\ldots$ for $\mu = 2$, $q = 3$.

New exponents

$e = 0.46240\ldots$:
"GroverXL", 2017.12.15 Bernstein–Yang.
Independently "QuantumBooleanSolve", 2017.12.19
Faugère–Horan–Kahrobaei–Kaplan–Kashefi–Perret.

More results in 2017.12.15 (not 2017.12.19) paper:

- Area-time product on mesh: $0.47210\ldots$.
- Area under specified time limits.
- $q > 2$: e.g., $0.72468\ldots$ (base 2) for $q = 3$.
- $\mu > 1$: e.g., $0.65688\ldots$ for $\mu = 2$, $q = 3$.
- Sage script to automate all these analyses.

A small example of XL

Goal: Find $(x, y, z) \in \mathbf{F}_2^3$ with

$xy + x + yz + z = 0;$

$xz + x + y + 1 = 0;$

$xz + yz + y + z = 0.$

A small example of XL

Goal: Find $(x, y, z) \in \mathbf{F}_2^3$ with
$xy + x + yz + z = 0;$
$xz + x + y + 1 = 0;$
$xz + yz + y + z = 0.$

Degree-d XL multiplies each quadratic equation by each monomial of degree $\le d - 2$.

e.g.: Degree-3 XL multiplies each quadratic equation by each monomial of degree ≤ 1: i.e., by $x, y, z, 1$.

A small example of XL: products

$$\begin{aligned}
xyz + xy + xz + x &= 0 && (x \cdot \text{first equation})\\
0 &= 0 && (y \cdot \text{first equation})\\
xyz + xz + yz + z &= 0 && (z \cdot \text{first equation})\\
xy + x + yz + z &= 0 && (1 \cdot \text{first equation})\\
xy + xz &= 0 && (x \cdot \text{second equation})\\
xyz + xy &= 0 && (y \cdot \text{second equation})\\
yz + z &= 0 && (z \cdot \text{second equation})\\
xz + x + y + 1 &= 0 && (1 \cdot \text{second equation})\\
xyz + xy &= 0 && (x \cdot \text{third equation})\\
xyz + y &= 0 && (y \cdot \text{third equation})\\
xz + z &= 0 && (z \cdot \text{third equation})\\
xz + yz + y + z &= 0 && (1 \cdot \text{third equation})
\end{aligned}$$

A small example of XL: Macaulay matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} xyz \\ xy \\ xz \\ x \\ yz \\ y \\ z \\ 1 \end{bmatrix} = 0$$

A small example of XL: row-echelon form

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} xyz \\ xy \\ xz \\ x \\ yz \\ y \\ z \\ 1 \end{bmatrix} = 0$$

A small example of XL: row-echelon form

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} xyz \\ xy \\ xz \\ x \\ yz \\ y \\ z \\ 1 \end{bmatrix} = 0$$

Now have *linear* relations:
$x = 1$,
$y = 1$,
$z = 1$.

Does XL produce enough relations?

Write A for number of monomials of degree $\leq d$ in n variables with exponents $<q$.

Does XL produce enough relations?

Write A for number of monomials of degree $\leq d$ in n variables with exponents $<q$.

Then A is z^d coeff in $\varphi_q(z)^n/(1-z)$ where $\varphi_q(z) = (1-z^q)/(1-z)$.

Does XL produce enough relations?

Write A for number of monomials of degree $\leq d$ in n variables with exponents $<q$.

Then A is z^d coeff in $\varphi_q(z)^n/(1-z)$ where $\varphi_q(z) = (1-z^q)/(1-z)$.

Define B as z^d coeff in $\varphi_q(z)^n/(1-z)\varphi_q(z^2)^m$.

2004 Yang–Chen: Rank of XL matrix $\leq A - B$.

Does XL produce enough relations?

Write A for number of monomials of degree $\leq d$ in n variables with exponents $< q$.

Then A is z^d coeff in $\varphi_q(z)^n/(1-z)$ where $\varphi_q(z) = (1-z^q)/(1-z)$.

Define B as z^d coeff in $\varphi_q(z)^n/(1-z)\varphi_q(z^2)^m$.

2004 Yang–Chen: Rank of XL matrix $\leq A - B$.

Sharp switch between cases as d crosses a cutoff:

- Huge B; experimentally, XL (almost always) fails.
- Huge $-B$; experimentally, XL succeeds.

What is the asymptotic cutoff?

Say $m/n \to \mu \geq 1$ as $n \to \infty$.

What is the asymptotic cutoff?

Say $m/n \to \mu \geq 1$ as $n \to \infty$. Define $h \in \mathbf{R}[x, z]$ as

$$z\frac{1-z^{2q}}{1-z}\left(\frac{-x}{z}-\frac{qz^{q-1}}{1-z^q}+\frac{1}{1-z}-\frac{2\mu z}{1-z^2}+\frac{2\mu q z^{2q-1}}{1-z^{2q}}\right).$$

What is the asymptotic cutoff?

Say $m/n \to \mu \geq 1$ as $n \to \infty$. Define $h \in \mathbf{R}[x, z]$ as

$$z\frac{1-z^{2q}}{1-z}\left(\frac{-x}{z}-\frac{qz^{q-1}}{1-z^q}+\frac{1}{1-z}-\frac{2\mu z}{1-z^2}+\frac{2\mu qz^{2q-1}}{1-z^{2q}}\right).$$

Define $\Delta \in \mathbf{R}[x]$ as z-discriminant of h.

What is the asymptotic cutoff?

Say $m/n \to \mu \geq 1$ as $n \to \infty$. Define $h \in \mathbf{R}[x, z]$ as

$$z\frac{1-z^{2q}}{1-z}\left(\frac{-x}{z}-\frac{qz^{q-1}}{1-z^q}+\frac{1}{1-z}-\frac{2\mu z}{1-z^2}+\frac{2\mu qz^{2q-1}}{1-z^{2q}}\right).$$

Define $\Delta \in \mathbf{R}[x]$ as z-discriminant of h.
Define δ as unique positive real root of Δ.

What is the asymptotic cutoff?

Say $m/n \to \mu \geq 1$ as $n \to \infty$. Define $h \in \mathbf{R}[x, z]$ as

$$z\frac{1-z^{2q}}{1-z}\left(\frac{-x}{z}-\frac{qz^{q-1}}{1-z^q}+\frac{1}{1-z}-\frac{2\mu z}{1-z^2}+\frac{2\mu q z^{2q-1}}{1-z^{2q}}\right).$$

Define $\Delta \in \mathbf{R}[x]$ as z-discriminant of h.
Define δ as unique positive real root of Δ.
Then B transition is for $d/n \to \delta$ as $n \to \infty$.

What is the asymptotic cutoff?

Say $m/n \to \mu \geq 1$ as $n \to \infty$. Define $h \in \mathbf{R}[x, z]$ as

$$z\frac{1 - z^{2q}}{1 - z}\left(\frac{-x}{z} - \frac{qz^{q-1}}{1 - z^q} + \frac{1}{1 - z} - \frac{2\mu z}{1 - z^2} + \frac{2\mu q z^{2q-1}}{1 - z^{2q}}\right).$$

Define $\Delta \in \mathbf{R}[x]$ as z-discriminant of h.
Define δ as unique positive real root of Δ.
Then B transition is for $d/n \to \delta$ as $n \to \infty$.

$(\log_2 A)/n \to \log_2(\varphi_q(\rho)/\rho^\delta)$ for $d/n \to \delta$
where ρ is unique positive solution to
$-\delta + (1-\delta)\rho + (2-\delta)\rho^2 + \cdots + (q-1-\delta)\rho^{q-1} = 0$.

FXL and naive Grover search

FXL: Guess values for some variables.
Apply XL to the other variables.

FXL and naive Grover search

FXL: Guess values for some variables.
Apply XL to the other variables.

Conceptually straightforward quantum speedup:
Grover search for values of some variables
where XL finds a solution for the other variables.

FXL and naive Grover search

FXL: Guess values for some variables.
Apply XL to the other variables.

Conceptually straightforward quantum speedup:
Grover search for values of some variables
where XL finds a solution for the other variables.

Hopeless-for-big-enough-sizes analysis: 2016
Chen–Hülsing–Rijneveld–Samardjiska–Schwabe.

FXL and naive Grover search

FXL: Guess values for some variables.
Apply XL to the other variables.

Conceptually straightforward quantum speedup:
Grover search for values of some variables
where XL finds a solution for the other variables.

Hopeless-for-big-enough-sizes analysis: 2016
Chen–Hülsing–Rijneveld–Samardjiska–Schwabe.

Asymptotic exponent $0.46240\ldots$: 2017.12.15
Bernstein–Yang, independently 2017.12.19
Faugère–Horan–Kahrobaei–Kaplan–Kashefi–Perret.

Why the naive approach is unsatisfactory

Internally, XL uses sparse linear algebra.
See 2004 Yang–Chen, 2004 Yang–Chen–Courtois.
(Various implementations starting in 2006:
e.g., 2012 Cheng–Chou–Niederhagen–Yang.)

Why the naive approach is unsatisfactory

Internally, XL uses sparse linear algebra.
See 2004 Yang–Chen, 2004 Yang–Chen–Courtois.
(Various implementations starting in 2006:
e.g., 2012 Cheng–Chou–Niederhagen–Yang.)

Bottleneck inside sparse linear algebra:
repeatedly overwrite a vector v with Mv.

Why the naive approach is unsatisfactory

Internally, XL uses sparse linear algebra.
See 2004 Yang–Chen, 2004 Yang–Chen–Courtois.
(Various implementations starting in 2006:
e.g., 2012 Cheng–Chou–Niederhagen–Yang.)

Bottleneck inside sparse linear algebra:
repeatedly overwrite a vector v with Mv.

Cannot erase data inside quantum computation!
Can uncompute, but only if input is still available.

Why the naive approach is unsatisfactory

Internally, XL uses sparse linear algebra.
See 2004 Yang–Chen, 2004 Yang–Chen–Courtois.
(Various implementations starting in 2006:
e.g., 2012 Cheng–Chou–Niederhagen–Yang.)

Bottleneck inside sparse linear algebra:
repeatedly overwrite a vector v with Mv.

Cannot erase data inside quantum computation!
Can uncompute, but only if input is still available.

Naive Grover for XL ends up storing many
intermediate vectors. Can this compete with
parallel non-quantum machine of same size?

ReversibleXL and GroverXL

1989 Bennett thm for multitape Turing machines:
time-T space-S computation $\Rightarrow$ reversible
time-$T^{\log_2 3}$ space-$O(S \log T)$ computation.

ReversibleXL and GroverXL

1989 Bennett thm for multitape Turing machines:
time-T space-S computation $\Rightarrow$ reversible
time-$T^{\log_2 3}$ space-$O(S \log T)$ computation.

1989 Bennett–Tompa: $1 + \epsilon$ instead of $\log_2 3$.
1995 Knill: subexponential overhead in both S, T.

ReversibleXL and GroverXL

1989 Bennett thm for multitape Turing machines: time-T space-S computation $\Rightarrow$ reversible time-$T^{\log_2 3}$ space-$O(S \log T)$ computation.

1989 Bennett–Tompa: $1 + \epsilon$ instead of $\log_2 3$.
1995 Knill: subexponential overhead in both S, T.

2017 Bernstein–Yang: conversion idea is compatible with parallelism and local computation.
"ReversibleXL": apply this conversion to XL using parallel sparse linear algebra.
"GroverXL": Grover's method using ReversibleXL.

Backup slide: finding linear relations

1986 Wiedemann sparse-linear-algebra algorithm quickly finds solution to $Mx = y$ if solution exists.

Backup slide: finding linear relations

1986 Wiedemann sparse-linear-algebra algorithm quickly finds solution to $Mx = y$ if solution exists. Also finds uniform random r with $Mr = 0$: take uniform random s; solve $Mx = Ms$; $r = x - s$.

Backup slide: finding linear relations

1986 Wiedemann sparse-linear-algebra algorithm quickly finds solution to $Mx = y$ if solution exists. Also finds uniform random r with $Mr = 0$: take uniform random s; solve $Mx = Ms$; $r = x - s$.

Easy exercises: use Wiedemann to quickly

- check whether relations give $1 = 0$;
- check whether relations give linear equation;
- check whether relations give all monomials.

Backup slide: finding linear relations

1986 Wiedemann sparse-linear-algebra algorithm quickly finds solution to $Mx = y$ if solution exists. Also finds uniform random r with $Mr = 0$: take uniform random s; solve $Mx = Ms$; $r = x - s$.

Easy exercises: use Wiedemann to quickly

- check whether relations give $1 = 0$;
- check whether relations give linear equation;
- check whether relations give all monomials.

2013 Bardet–Faugère–Salvy–Spaenlehauer incorrectly claims that this requires computation of "row echelon form" (no known quick algorithms).