Abstract. The performance of numerical algorithms, both regarding stability and complexity, can be understood in a unified way in terms of condition numbers. This requires to identify the appropriate geometric settings and to characterize condition in geometric ways. A probabilistic analysis of numerical algorithms can be reduced to a corresponding analysis of condition numbers, which leads to fascinating problems of geometric probability and integral geometry.

This is the theme of my recent monograph *Condition*, written with Felipe Cucker, that appeared in 2013 in Springer’s Grundlehren series. The monograph is divided into three parts. Its first part deals with the solution of linear systems of equations, where many of the concepts can be explained in an elementary way. The second part is devoted to linear programming, i.e., the solution of systems of linear inequalities (there exist natural extensions to convex programming). The third part is devoted to the solution of systems of polynomial equations, focusing on Smale’s 17th problem, which asks to find a solution of a given system of $n$ complex homogeneous polynomial equations in $n + 1$ unknowns. This problem can be solved in average (and even smoothed) polynomial time. Recently, Pierre Lairez succeeded in providing a complete solution of Smale’s 17th problem ("A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time," to appear in *J. FoCM*).

The enclosed course material in the form of slides follows the three part structure of the monograph and attempts to illustrate the main unifying concepts and key ideas. The framework seems quite generally applicable. For instance, a numerical algorithm for computing eigenpairs of matrices, that is numerically stable and provably runs in average polynomial time, was recently developed along these lines (Armentano, Beltrán, Bürgisser, Cucker, and Shub, “A stable, polynomial-time algorithm for the eigenpair problem,” accepted for *J. EMS*).
Condition: The Geometry of Numerical Algorithms

Peter Bürgisser
Technical University of Berlin

Journées Nationales de Calcul Formel 2017

Luminy, January 16–20, 2017
For more details I refer to my new monograph (Springer 2013) with Felipe Cucker:
Outline

Overview

Part I: Linear Equalities
- Turing’s Condition Number
- Average Probabilistic Analysis of $\kappa(A)$
- Smoothed Probabilistic Analysis of $\kappa(A)$
- Random Triangular Matrices

Part II: Linear Inequalities
- Interior-point methods
- Condition numbers of linear programming
- Average Analysis of GCC condition number
- Smoothed Analysis of GCC condition number
- Condition numbers of convex optimization

Part III: Polynomial Equations
- Smale’s 17th Problem
- Approximate zeros, condition, and homotopy continuation
- Probabilistic analyses
- Solution to Smale’s 17th problem
- Proof ideas
Overview
Motivation

- In computer science, the most common theoretical approach to understanding the behaviour of algorithms is worst-case analysis.
Motivation

- In computer science, the most common theoretical approach to understanding the behaviour of algorithms is worst-case analysis.
- There are cases of algorithms that perform exceedingly well in practice and still have a provably bad worst-case behaviour. A famous example is Dantzig's simplex algorithm.
Motivation

- In computer science, the most common theoretical approach to understanding the behaviour of algorithms is worst-case analysis.
- There are cases of algorithms that perform exceedingly well in practice and still have a provably bad worst-case behaviour. A famous example is Dantzig’s simplex algorithm.
- To rectify this discrepancy, the concept of average-case analysis was introduced. This means bounding the expected performance of an algorithm on random inputs. For the simplex algorithm: average-case analyses by Borgwardt (1982) and Smale (1983).
Motivation

- In computer science, the most common theoretical approach to understanding the behaviour of algorithms is worst-case analysis.
- There are cases of algorithms that perform exceedingly well in practice and still have a provably bad worst-case behaviour. A famous example is Dantzig's simplex algorithm.
- To rectify this discrepancy, the concept of average-case analysis was introduced. This means bounding the expected performance of an algorithm on random inputs. For the simplex algorithm: average-case analyses by Borgwardt (1982) and Smale (1983).
- However, average analysis can rarely explain a good performance in practice. Its results strongly depend on the distribution of the inputs, which is unknown, and usually assumed to be Gaussian for rendering the mathematical analysis feasible.
Smoothed analysis

Smoothed analysis is a newer form of analysis of algorithms, that arguably blends the best of both worst-case and average-case. It was proposed by Spielman and Teng who performed a smoothed analysis of the running time of the simplex algorithm (Gödel Prize 2008, Fulkerson Prize 2009).
Smoothed analysis

Smoothed analysis is a newer form of analysis of algorithms, that arguably blends the best of both worst-case and average-case. It was proposed by Spielman and Teng who performed a smoothed analysis of the running time of the simplex algorithm (Gödel Prize 2008, Fulkerson Prize 2009).

Let \( T: \mathbb{R}^p \to \mathbb{R}_+ \cup \{\infty\} \) be a function (running time, condition number). Instead of showing

"It is unlikely that \( T(a) \) will be large."

"..."
Smoothed analysis

Smoothed analysis is a newer form of analysis of algorithms, that arguably blends the best of both worst-case and average-case. It was proposed by Spielman and Teng who performed a smoothed analysis of the running time of the simplex algorithm (Gödel Prize 2008, Fulkerson Prize 2009).

Let $T : \mathbb{R}^p \to \mathbb{R}_+ \cup \{\infty\}$ be a function (running time, condition number).

Instead of showing

"It is unlikely that $T(a)$ will be large."

one shows that

"For all $\bar{a}$ and all slight random perturbations $\bar{a} + \Delta a$, it is unlikely that $T(\bar{a} + \Delta a)$ will be large."
Smoothed analysis

Smoothed analysis is a newer form of analysis of algorithms, that arguably blends the best of both worst-case and average-case. It was proposed by Spielman and Teng who performed a smoothed analysis of the running time of the simplex algorithm (Gödel Prize 2008, Fulkerson Prize 2009).

Let $T: \mathbb{R}^p \to \mathbb{R}_+ \cup \{\infty\}$ be a function (running time, condition number). Instead of showing

"It is unlikely that $T(a)$ will be large."

one shows that

"For all $\bar{a}$ and all slight random perturbations $\bar{a} + \Delta a$, it is unlikely that $T(\bar{a} + \Delta a)$ will be large."

<table>
<thead>
<tr>
<th>Worst case analysis</th>
<th>Average case analysis</th>
<th>Smoothed analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sup_{a \in \mathbb{R}^p} T(a)$</td>
<td>$\mathbb{E}_{a \in \mathcal{D}} T(a)$</td>
<td>$\sup_{\bar{a} \in \mathbb{R}^p} \mathbb{E}_{a \in N(\bar{a}, \sigma^2)} T(a)$</td>
</tr>
</tbody>
</table>

$\mathcal{D}$ distribution on $\mathbb{R}^p$, $N(\bar{a}, \sigma^2)$ Gaussian distribution centered at $\bar{a}$. 
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
- Condition numbers quantify the errors when the input has been modified by a small perturbation.
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
- Condition numbers quantify the errors when the input has been modified by a small perturbation.
- The best known condition number is $\kappa(A) = \|A\|\|A^{-1}\|$ for matrix inversion and linear equation solving.
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
- Condition numbers quantify the errors when the input has been modified by a small perturbation.
- The best known condition number is \( \kappa(A) = \|A\| \|A^{-1}\| \) for matrix inversion and linear equation solving.
- The running time \( T(x, \varepsilon) \) of iterative numerical algorithms, measured as the number of arithmetic operations, can often be bounded in the form

\[
T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c,
\]
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
- Condition numbers quantify the errors when the input has been modified by a small perturbation.
- The best known condition number is \( \kappa(A) = \|A\| \|A^{-1}\| \) for matrix inversion and linear equation solving.
- The running time \( T(x, \varepsilon) \) of iterative numerical algorithms, measured as the number of arithmetic operations, can often be bounded in the form

\[
T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c,
\]

- input \( x \in \mathbb{R}^n \) of size \( x := n \)
Condition based analysis

- Smoothened analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
- Condition numbers quantify the errors when the input has been modified by a small perturbation.
- The best known condition number is $\kappa(A) = \|A\| \|A^{-1}\|$ for matrix inversion and linear equation solving.
- The running time $T(x, \varepsilon)$ of iterative numerical algorithms, measured as the number of arithmetic operations, can often be bounded in the form

$$T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c,$$

- input $x \in \mathbb{R}^n$ of size$(x) := n$
- $\mu(x)$ measure of conditioning of $x$
Condition based analysis

- Smoothed analysis can be applied to a wide variety of numerical algorithms.
- For doing so, understanding the concept of condition numbers is an important intermediate step.
- Condition numbers quantify the errors when the input has been modified by a small perturbation.
- The best known condition number is $\kappa(A) = \|A\| \|A^{-1}\|$ for matrix inversion and linear equation solving.
- The running time $T(x, \varepsilon)$ of iterative numerical algorithms, measured as the number of arithmetic operations, can often be bounded in the form

$$T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c,$$

- input $x \in \mathbb{R}^n$ of size$(x) := n$
- $\mu(x)$ measure of conditioning of $x$
- $\varepsilon$ required accuracy.
Stochastic analysis of condition numbers

- Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
  
  - Condition based analysis:
    \[ T(x, \varepsilon) \leq \text{size}(x) + \mu(x) + \log \varepsilon \]
  
  - Stochastic analysis of condition number \( \mu(x) \) for random inputs.
  
  This approach was elaborated for average-case complexity since the eighties by many researchers, the pioneers being:
  
  Demmel, Edelman, Renegar, Shub, Smale, Todd, Vavasis, Ye, and others.

  Part two of Smale’s scheme can be naturally refined by performing a smoothed analysis of the condition number \( \mu(x) \) involved.

  Smoothed analysis for condition numbers since 2004: Amelunxen, Bürgisser, Cucker, Dunagan, Hauser, Lotz, Sankar, Spielman, Tao, Teng, Vu, Wschebor and others.

  Recent new idea: weak average-case analysis (Amelunxen & Lotz, 2016). Take average after excluding a set of outliers of exponentially small probability.
Overview

Stochastic analysis of condition numbers

- Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
  - Condition based analysis: \( T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c \)
Stochastic analysis of condition numbers

- Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
  1. **Condition based analysis:** $T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c$
  2. **Stochastic analysis of condition number** $\mu(x)$ for random inputs $x$.
Stochastic analysis of condition numbers

- Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
  1. **Condition based analysis**: \( T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c \)
  2. **Stochastic analysis of condition number** \( \mu(x) \) for random inputs \( x \).

- This approach was elaborated for average-case complexity since the eighties by many researchers, the pioneers being: Demmel, Edelman, Renegar, Shub, Smale, Todd, Vavasis, Ye, and others.
Stochastic analysis of condition numbers

- Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
  1. **Condition based analysis**: $T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c$
  2. **Stochastic analysis of condition number** $\mu(x)$ for random inputs $x$.

- This approach was elaborated for average-case complexity since the eighties by many researchers, the pioneers being: Demmel, Edelman, Renegar, Shub, Smale, Todd, Vavasis, Ye, and others.

- Part two of Smale’s scheme can be naturally refined by performing a smoothed analysis of the condition number $\mu(x)$ involved.
Overview

Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
- Condition based analysis: \( T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c \)
- Stochastic analysis of condition number \( \mu(x) \) for random inputs \( x \).

This approach was elaborated for average-case complexity since the eighties by many researchers, the pioneers being: Demmel, Edelman, Renegar, Shub, Smale, Todd, Vavasis, Ye, and others.

Part two of Smale’s scheme can be naturally refined by performing a smoothed analysis of the condition number \( \mu(x) \) involved.

Smoothed analysis for condition numbers since 2004: Amelunxen, Bürgisser, Cucker, Dunagan, Hauser, Lotz, Sankar, Spielman, Tao, Teng, Vu, Wschebor and others.

Stochastic analysis of condition numbers
Stochastic analysis of condition numbers

- Two-part scheme for dealing with complexity upper bounds in numerical analysis (Smale 1997):
  1. Condition based analysis: \( T(x, \varepsilon) \leq (\text{size}(x) + \mu(x) + \log \varepsilon^{-1})^c \)
  2. Stochastic analysis of condition number \( \mu(x) \) for random inputs \( x \).

- This approach was elaborated for average-case complexity since the eighties by many researchers, the pioneers being: Demmel, Edelman, Renegar, Shub, Smale, Todd, Vavasis, Ye, and others.

- Part two of Smale's scheme can be naturally refined by performing a smoothed analysis of the condition number \( \mu(x) \) involved.

- Smoothed analysis for condition numbers since 2004: Amelunxen, Bürgisser, Cucker, Dunagan, Hauser, Lotz, Sankar, Spielman, Tao, Teng, Vu, Wschebor and others.

- Recent new idea: weak average-case analysis (Amelunxen & Lotz, 2016). Take average after excluding a set of outliers of exponentially small probability.
Part I: Linear Equalities
Turing’s condition number of a matrix

A. Turing, 1948

J. von Neumann and H. Goldstine, 1947
General definition of condition number

- Suppose we have a numerical computation problem

\[ f : \mathbb{R}^p \to \mathbb{R}^q, \ x \mapsto y = f(x). \]

We fix norms \( \| \| \) on \( \mathbb{R}^p, \mathbb{R}^q \).
General definition of condition number

- Suppose we have a numerical computation problem

\[ f : \mathbb{R}^p \rightarrow \mathbb{R}^q, \quad x \mapsto y = f(x). \]

We fix norms \( \| \| \) on \( \mathbb{R}^p, \mathbb{R}^q \).

- Suppose the input \( x \) has a small relative error \( \| \Delta x \| / \| x \| \). We want to bound the relative error \( \| \Delta y \| / \| y \| \) of the output.
General definition of condition number

- Suppose we have a numerical computation problem

\[ f : \mathbb{R}^p \to \mathbb{R}^q, \ x \mapsto y = f(x). \]

We fix norms \( \| \| \) on \( \mathbb{R}^p, \mathbb{R}^q \).

- Suppose the input \( x \) has a small relative error \( \| \Delta x \|/\| x \| \). We want to bound the relative error \( \| \Delta y \|/\| y \| \) of the output.

- This is done by the condition number \( \kappa(f, x) \) of \( x \):

\[
\| \Delta y \|/\| y \| \preceq \kappa(f, x) \| \Delta x \|/\| x \|.
\]
General definition of condition number

- Suppose we have a numerical computation problem

\[ f: \mathbb{R}^p \to \mathbb{R}^q, \ x \mapsto y = f(x). \]

We fix norms \( \| \| \) on \( \mathbb{R}^p, \mathbb{R}^q \).
- Suppose the input \( x \) has a small relative error \( \| \Delta x \| / \| x \| \). We want to bound the relative error \( \| \Delta y \| / \| y \| \) of the output.
- This is done by the condition number \( \kappa(f, x) \) of \( x \):

\[ \| \Delta y \| / \| y \| \lesssim \kappa(f, x) \| \Delta x \| / \| x \|. \]

- Formal definition for differentiable \( f \):

\[ \kappa(f, x) := \| Df(x) \| \frac{\| x \|}{\| f(x) \|} \]

where \( \| Df(x) \| \) denotes the operator norm of the Jacobian of \( f \) at \( x \).
Turing’s condition number

- Consider matrix inversion

\[ f : \text{GL}(m, \mathbb{R}) \to \mathbb{R}^{m \times m}, \ A \mapsto A^{-1}. \]

We measure errors with the spectral norm.
Consider matrix inversion

\[ f : \text{GL}(m, \mathbb{R}) \to \mathbb{R}^{m \times m}, A \mapsto A^{-1}. \]

We measure errors with the spectral norm.

- We show by a perturbation argument that the condition number of \( A \) with respect to \( f \) equals the classical condition number of \( A \):

\[ \kappa(A) := \kappa(f, A) = \|A\| \|A^{-1}\|. \]
Turing’s condition number

- Consider matrix inversion

\[ f : \text{GL}(m, \mathbb{R}) \to \mathbb{R}^{m \times m}, A \mapsto A^{-1}. \]

We measure errors with the spectral norm.

- We show by a perturbation argument that the condition number of \( A \) with respect to \( f \) equals the classical condition number of \( A \):

\[ \kappa(A) := \kappa(f, A) = \| A \| \| A^{-1} \|. \]

- Note that \( \kappa(\lambda A) = \kappa(A) \) for \( \lambda \in \mathbb{R} \).
Turing’s condition number

- Consider matrix inversion

\[ f : \text{GL}(m, \mathbb{R}) \to \mathbb{R}^{m \times m}, \ A \mapsto A^{-1}. \]

We measure errors with the spectral norm.

- We show by a perturbation argument that the condition number of \( A \) with respect to \( f \) equals the classical condition number of \( A \):

\[ \kappa(A) := \kappa(f, A) = \|A\| \|A^{-1}\|. \]

- Note that \( \kappa(\lambda A) = \kappa(A) \) for \( \lambda \in \mathbb{R} \).

- \( \kappa(A) \) was introduced by A. Turing in 1948.
Connection to eigenvalues

Let $\lambda_1 \geq \ldots \geq \lambda_n$ be the eigenvalues of $A^T A$. 
Connection to eigenvalues

- Let $\lambda_1 \geq \ldots \geq \lambda_n$ be the eigenvalues of $A^T A$.
- Then

$$\|A\|^2 = \sup_{\|x\|=1} \|Ax\|^2 = \sup_{\|x\|=1} x^T A^T A x.$$

Hence $\|A\|^2 = \lambda_1$ is the largest eigenvalue of $A^T A$. 
Connection to eigenvalues

- Let $\lambda_1 \geq \ldots \geq \lambda_n$ be the eigenvalues of $A^T A$.
- Then
  \[ \|A\|^2 = \sup_{\|x\|=1} \|Ax\|^2 = \sup_{\|x\|=1} x^T A^T A x. \]
  Hence $\|A\|^2 = \lambda_1$ is the largest eigenvalue of $A^T A$.
- Since $\lambda_n^{-1} \geq \ldots \geq \lambda_1^{-1}$ are the eigenvalues of $A^{-1}(A^{-1})^T$, we get
  \[ \|A^{-1}\|^2 = \|(A^{-1})^T\|^2 = \lambda_n^{-1}. \]
Connection to eigenvalues

- Let $\lambda_1 \geq \ldots \geq \lambda_n$ be the eigenvalues of $A^T A$.
- Then 
  \[ \|A\|^2 = \sup_{\|x\|=1} \|Ax\|^2 = \sup_{\|x\|=1} x^T A^T A x. \]

  Hence $\|A\|^2 = \lambda_1$ is the largest eigenvalue of $A^T A$.
- Since $\lambda_n^{-1} \geq \ldots \geq \lambda_1^{-1}$ are the eigenvalues of $A^{-1}(A^{-1})^T$, we get 
  \[ \|A^{-1}\|^2 = \|(A^{-1})^T\|^2 = \lambda_n^{-1}. \]
- We obtain 
  \[ \kappa(A) = \|A\| \|A^{-1}\| = \frac{\sqrt{\lambda_1}}{\sqrt{\lambda_n}} \geq 1. \]
Connection to eigenvalues

- Let $\lambda_1 \geq \ldots \geq \lambda_n$ be the eigenvalues of $A^T A$.
- Then
  \[ \|A\|^2 = \sup_{\|x\|=1} \|Ax\|^2 = \sup_{\|x\|=1} x^T A^T A x. \]

  Hence $\|A\|^2 = \lambda_1$ is the largest eigenvalue of $A^T A$.
- Since $\lambda_n^{-1} \geq \ldots \geq \lambda_1^{-1}$ are the eigenvalues of $A^{-1}(A^{-1})^T$, we get
  \[ \|A^{-1}\|^2 = \|(A^{-1})^T\|^2 = \lambda_n^{-1}. \]
- We obtain
  \[ \kappa(A) = \|A\| \|A^{-1}\| = \frac{\sqrt{\lambda_1}}{\sqrt{\lambda_n}} \geq 1. \]
- $\sqrt{\lambda_1}$ and $\sqrt{\lambda_n}$ are called largest and smallest singular value of $A$. 
Distance to ill-posedness

- We call the set of singular matrices $\Sigma \subseteq \mathbb{R}^{m \times m}$ the set of ill-posed instances for matrix inversion. Clearly, $A \in \Sigma \iff \det A = 0$. 
Distance to ill-posedness

- We call the set of singular matrices $\Sigma \subseteq \mathbb{R}^{m \times m}$ the set of ill-posed instances for matrix inversion. Clearly, $A \in \Sigma \iff \det A = 0$.

- The Eckart-Young Theorem from 1936 states that

$$\|A^{-1}\| = \frac{1}{\operatorname{dist}(A, \Sigma)},$$

where dist either refers to operator norm or to Frobenius norm (Euclidean norm on $\mathbb{R}^{n \times n}$) defined as

$$\|A\|_F := (\operatorname{tr}(AA^T))^{1/2} = \left(\sum_{i,j} a_{ij}^2\right)^{1/2}.$$
Distance to ill-posedness

- We call the set of singular matrices $\Sigma \subseteq \mathbb{R}^{m \times m}$ the set of ill-posed instances for matrix inversion. Clearly, $A \in \Sigma \iff \det A = 0$.

- The Eckart-Young Theorem from 1936 states that

$$\|A^{-1}\| = \frac{1}{\text{dist}(A, \Sigma)},$$

where dist either refers to operator norm or to Frobenius norm (Euclidean norm on $\mathbb{R}^{n \times n}$) defined as

$$\|A\|_F := (\text{tr}(AA^T))^{1/2} = \left( \sum_{i,j} a_{ij}^2 \right)^{1/2}.$$

- Hence

$$\kappa(A) = \|A\| \|A^{-1}\| = \frac{\|A\|}{\text{dist}(A, \Sigma)}.$$
Finite precision

- Digital computers operate with floating-point numbers, and every arithmetic operations produces a *round-off error*.
Finite precision

- Digital computers operate with floating-point numbers, and every arithmetic operations produces a round-off error.
- Let $\epsilon_{\text{mach}}$ denote the round-off unit (e.g., $10^{-12}$).
Finite precision

- Digital computers operate with floating-point numbers, and every arithmetic operations produces a round-off error.
- Let $\epsilon_{\text{mach}}$ denote the round-off unit (e.g., $10^{-12}$).
- Suppose we compute the approximation $\tilde{x}$ of $x \in \mathbb{R}$ with relative error $\delta$, i.e. $\tilde{x} = x(1 + \delta)$. 
Digital computers operate with floating-point numbers, and every arithmetic operations produces a round-off error.

Let $\epsilon_{\text{mach}}$ denote the round-off unit (e.g., $10^{-12}$).

Suppose we compute the approximation $\tilde{x}$ of $x \in \mathbb{R}$ with relative error $\delta$, i.e. $\tilde{x} = x(1 + \delta)$.

The best we can hope for is $\delta \leq \frac{1}{2} \epsilon_{\text{mach}}$. 
Finite precision

- Digital computers operate with floating-point numbers, and every arithmetic operations produces a round-off error.
- Let $\epsilon_{\text{mach}}$ denote the round-off unit (e.g., $10^{-12}$).
- Suppose we compute the approximation $\tilde{x}$ of $x \in \mathbb{R}$ with relative error $\delta$, i.e. $\tilde{x} = x(1 + \delta)$.
- The best we can hope for is $\delta \leq \frac{1}{2} \epsilon_{\text{mach}}$.
- One calls $\log_{10} \left( \frac{\delta}{\epsilon_{\text{mach}}} \right)$ the loss of precision in decimal digits.
Condition number bounds loss of precision

- Turing’s condition number is relevant for finite precision analysis of linear algebra.
Condition number bounds loss of precision

- Turing’s condition number is relevant for finite precision analysis of linear algebra.
- For instance, QR factorization is one of the main engines in numerical linear algebra.
Turing’s condition number is relevant for finite precision analysis of linear algebra. For instance, QR factorization is one of the main engines in numerical linear algebra. Let $A \in \mathbb{R}^{n \times n}$ be invertible and $b \in \mathbb{R}^n$. If the system $Ax = b$ is solved using the Householder QR factorization, the computed solution $\tilde{x}$ has a loss of precision bounded by

$$\log_{10} \left( \frac{\|\tilde{x} - x\|}{\epsilon_{\text{mach}}\|x\|} \right) \leq 2 \log_{10} n + \log_{10} \kappa(A) + c,$$

where $c$ denotes a universal constant $c$. 
Consider a full-rank rectangular matrix $A \in \mathbb{R}^{m \times n}$ with $m > n$, a vector $c \in \mathbb{R}^m$, and the least squares problem

$$\min_{v \in \mathbb{R}^n} \|Av - c\|.$$
Method of conjugate gradients

- Consider a full-rank rectangular matrix $A \in \mathbb{R}^{m \times n}$ with $m > n$, a vector $c \in \mathbb{R}^m$, and the least squares problem

$$\min_{v \in \mathbb{R}^n} \|Av - c\|.$$ 

- The solution $x^* \in \mathbb{R}^n$ is given by the solution of the system $Sx = b$ with

$$S := A^T A \in \mathbb{R}^{n \times n}, \quad b := A^T c.$$
Method of conjugate gradients

- Consider a full-rank rectangular matrix $A \in \mathbb{R}^{m \times n}$ with $m > n$, a vector $c \in \mathbb{R}^m$, and the least squares problem

  $$\min_{v \in \mathbb{R}^n} \|Av - c\|.$$ 

- The solution $x^* \in \mathbb{R}^n$ is given by the solution of the system $Sx = b$ with

  $$S := A^T A \in \mathbb{R}^{n \times n}, \quad b := A^T c.$$ 

- By construction, $S$ is symmetric and positive definite.
Method of conjugate gradients

- Consider a full-rank rectangular matrix $A \in \mathbb{R}^{m \times n}$ with $m > n$, a vector $c \in \mathbb{R}^m$, and the least squares problem

$$\min_{v \in \mathbb{R}^n} \| Av - c \|.$$ 

- The solution $x^* \in \mathbb{R}^n$ is given by the solution of the system $Sx = b$ with

$$S := A^T A \in \mathbb{R}^{n \times n}, \quad b := A^T c.$$ 

- By construction, $S$ is symmetric and positive definite.

- The method of conjugate gradients is a powerful iterative method of numerical linear algebra. Upon input $S, b$ and a start vector $x_0$ it produces a sequence of iterates $x_1, x_2, \ldots, x_n = x^*$. 

Method of conjugate gradients

- Consider a full-rank rectangular matrix $A \in \mathbb{R}^{m \times n}$ with $m > n$, a vector $c \in \mathbb{R}^m$, and the least squares problem

$$\min_{v \in \mathbb{R}^n} \|Av - c\|.$$ 

- The solution $x^* \in \mathbb{R}^n$ is given by the solution of the system $Sx = b$ with

$$S := A^T A \in \mathbb{R}^{n \times n}, \quad b := A^T c.$$ 

- By construction, $S$ is symmetric and positive definite.

- The method of conjugate gradients is a powerful iterative method of numerical linear algebra. Upon input $S, b$ and a start vector $x_0$ it produces a sequence of iterates $x_1, x_2, \ldots, x_n = x^*$.

- In order to achieve a relative error $\varepsilon$, it suffices to execute

$$\frac{1}{2} \sqrt{\kappa(S)} \ln \left( \frac{1}{\varepsilon} \right)$$

iterations (Hestenes and Stiefel, 1952).


Probabilistic Analysis of Turing’s Condition Number

Average-case Analysis

H. Goldstine and J. von Neumann

Numerical inverting matrices of high order, II, 1951
Wishart distribution

- Suppose $A \in \mathbb{R}^{n \times n}$ is a random matrix with independent standard Gaussian entries.
Wishart distribution

- Suppose $A \in \mathbb{R}^{n \times n}$ is a random matrix with independent standard Gaussian entries.
- What can we say about the random variable $\kappa(A)$?
Wishart distribution

- Suppose $A \in \mathbb{R}^{n \times n}$ is a random matrix with independent standard Gaussian entries.
- What can we say about the random variable $\kappa(A)$?
- The distribution of $A^T A$ is known as **Wishart distribution** which is of relevance in multivariate statistics.
Suppose $A \in \mathbb{R}^{n \times n}$ is a random matrix with independent standard Gaussian entries.

What can we say about the random variable $\kappa(A)$?

The distribution of $A^T A$ is known as Wishart distribution which is of relevance in multivariate statistics.

The joint probability density of the eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$ of $A^T A$ is known (Fisher, Hsu, Roy, 1939) and equals

$$
\rho(\lambda) = c_n \ e^{-\frac{1}{2} \sum \lambda_i} \prod_i \lambda_i^{-\frac{1}{2}} \prod_{i<j} (\lambda_i - \lambda_j),
$$

with some normalizing constant $c_n$. 

Wishart distribution
Suppose $A \in \mathbb{R}^{n \times n}$ is a random matrix with independent standard Gaussian entries.

What can we say about the random variable $\kappa(A)$?

The distribution of $A^T A$ is known as Wishart distribution which is of relevance in multivariate statistics.

The joint probability density of the eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$ of $A^T A$ is known (Fisher, Hsu, Roy, 1939) and equals

$$
\rho(\lambda) = c_n \ e^{-\frac{1}{2} \sum_i \lambda_i} \ \prod_i \lambda_i^{-\frac{1}{2}} \ \prod_{i<j} (\lambda_i - \lambda_j),
$$

with some normalizing constant $c_n$.

It plays an important role in physics (cf. Wigner, 1967).
(Limit) distribution of $\kappa(A)$

- From the joint distribution of the eigenvalues, it is possible to derive the distribution of $\kappa(A) = \sqrt{\lambda_1/\lambda_n}$. 
From the joint distribution of the eigenvalues, it is possible to derive the distribution of \( \kappa(A) = \sqrt{\lambda_1/\lambda_n} \).

Edelman (1988)

\[
\lim_{n \to \infty} \text{Prob}\{\kappa(A) \geq nx\} = 1 - e^{-2/x-2/x^2} = \frac{2}{x} + O\left(\frac{1}{x^2}\right).
\]
From the joint distribution of the eigenvalues, it is possible to derive the distribution of \( \kappa(A) = \sqrt{\lambda_1/\lambda_n} \).

**Edelman (1988)**

\[
\lim_{n \to \infty} \text{Prob}\{\kappa(A) \geq nx\} = 1 - e^{-2/x - 2/x^2} = \frac{2}{x} + O\left(\frac{1}{x^2}\right).
\]

This implies for the expectation

\[ \mathbb{E}_A(\log \kappa(A)) = \log n + c + o(1). \]
(Limit) distribution of $\kappa(A)$

- From the joint distribution of the eigenvalues, it is possible to derive the distribution of $\kappa(A) = \sqrt{\lambda_1/\lambda_n}$.

**Edelman (1988)**

$$\lim_{n \to \infty} \text{Prob}\{\kappa(A) \geq nx\} = 1 - e^{-2/x - 2/x^2} = \frac{2}{x} + O\left(\frac{1}{x^2}\right).$$

- This implies for the expectation
  $$\mathbb{E}_A(\log \kappa(A)) = \log n + c + o(1).$$

- Application: the QR factorization has an average loss of precision $3 \log_{10} n + O(1)$. Satisfactory result!
(Limit) distribution of $\kappa(A)$

- From the joint distribution of the eigenvalues, it is possible to derive the distribution of $\kappa(A) = \sqrt{\lambda_1/\lambda_n}$.

Edelman (1988)

$$\lim_{n \to \infty} \text{Prob}\{\kappa(A) \geq nx\} = 1 - e^{-2/x - 2/x^2} = \frac{2}{x} + O\left(\frac{1}{x^2}\right).$$

- This implies for the expectation

$$\mathbb{E}_A(\log \kappa(A)) = \log n + c + o(1).$$

- Application: the QR factorization has an average loss of precision $3 \log_{10} n + O(1)$. Satisfactory result!

- There is an intuitive geometric way of deriving such results, that also has the virtue of generalizing to a wide variety of situations.
Link to geometry: reduction to sphere

- Define Frobenius condition number \( \kappa_F(A) := \|A\|_F \|A^{-1}\| \geq \kappa(A) \).
Link to geometry: reduction to sphere

- Define Frobenius condition number $\kappa_F(A) := \|A\|_F \|A^{-1}\| \geq \kappa(A)$.
- The standard Gaussian distribution on $\mathbb{R}^{n \times n}$ induces the uniform distribution on the sphere $S := S^{n^2-1} := \{ A \in \mathbb{R}^{n \times n} \mid \|A\|_F = 1 \}$ via

$$\mathbb{R}^{n \times n} \setminus \{0\} \to S, \quad A \mapsto B = \frac{1}{\|A\|_F} A$$
Link to geometry: reduction to sphere

- Define **Frobenius condition number** \( \kappa_F(A) := \|A\|_F \|A^{-1}\| \geq \kappa(A) \).
- The standard Gaussian distribution on \( \mathbb{R}^{n \times n} \) induces the uniform distribution on the sphere \( S := S^{n^2-1} := \{ A \in \mathbb{R}^{n \times n} \mid \|A\|_F = 1 \} \) via
  \[
  \mathbb{R}^{n \times n} \setminus \{0\} \to S, \quad A \mapsto B = \frac{1}{\|A\|_F} A
  \]
- By the characterization by inverse distance to ill-posedness
  \[
  \kappa_F(A) = \kappa_F(B) = \|B\|_F \|B^{-1}\| = \frac{\|B\|_F}{\text{dist}(B, \Sigma)} = \frac{1}{\text{dist}(B, \Sigma)},
  \]
  where \( \Sigma := \{ A' \in \mathbb{R}^{n \times n} \mid \det A' = 0 \} \) and dist is measured by Frobenius norm.
Link to geometry: reduction to sphere

- Define **Frobenius condition number** $\kappa_F(A) := \|A\|_F \|A^{-1}\| \geq \kappa(A)$.
- The standard Gaussian distribution on $\mathbb{R}^{n \times n}$ induces the uniform distribution on the sphere $S := S^{n^2 - 1} := \{ A \in \mathbb{R}^{n \times n} \mid \|A\|_F = 1 \}$ via
  \[
  \mathbb{R}^{n \times n} \setminus \{0\} \rightarrow S, \quad A \mapsto B = \frac{1}{\|A\|_F} A
  \]
- By the characterization by inverse distance to ill-posedness
  \[
  \kappa_F(A) = \kappa_F(B) = \|B\|_F \|B^{-1}\| = \frac{\|B\|_F}{\text{dist}(B, \Sigma)} = \frac{1}{\text{dist}(B, \Sigma)},
  \]
  where $\Sigma := \{ A' \in \mathbb{R}^{n \times n} \mid \det A' = 0 \}$ and dist is measured by Frobenius norm.
- Hence
  \[
  \text{Prob}_A\{\kappa_F(A) \geq \varepsilon^{-1}\} = \text{Prob}_B\{\kappa_F(B) \geq \varepsilon^{-1}\} = \text{Prob}_B\{\text{dist}(B, \Sigma) \leq \varepsilon\}.
  \]
Volume of tubes

Let \( T(\Sigma_S, \varepsilon) \) denote the neighborhood (or tube) of \( \Sigma_S := \Sigma \cap S \) of radius \( \arcsin \varepsilon \) in the sphere \( S \).
Volume of tubes

Let $T(\Sigma_S, \varepsilon)$ denote the neighborhood (or tube) of $\Sigma_S := \Sigma \cap S$ of radius $\arcsin \varepsilon$ in the sphere $S$.

\[
\begin{align*}
\text{Prob}_B \{ \kappa_F(B) \geq \varepsilon^{-1} \} &= \text{Prob}_B \{ \text{dist}(B, \Sigma) \leq \varepsilon \} \\
&= \frac{\text{vol}(T(\Sigma_S, \varepsilon))}{\text{vol}(S)} = \frac{\text{vol}(\Sigma_S) \cdot 2\varepsilon}{\text{vol}(S)} + o(\varepsilon).
\end{align*}
\]
Volume of determinant hypersurface $\Sigma_S$ (1)

- $\Sigma$ is the zero set of the determinant, a homogeneous polynomial of degree $d = n$. 

Let $P$ be a plane (two-dimensional subspace) in $\mathbb{R}^n \times \mathbb{R}^n$. How about the intersection $P \setminus \Sigma$?

Either $P \setminus \Sigma = P$ (degenerate case) or $P \setminus \Sigma$ is a union of $k$ lines through the origin, for $k \leq d$.

Hence, almost surely, $P \setminus \Sigma$ is either empty or consists of $2d$ points, two of which are diametral.

Let $S_0$ be the intersection of $S$ with a hyperplane (hyperequator). Poincaré’s formula of integral geometry states $\text{vol}(\Sigma_S) \cdot \text{vol}(S_0) = E_{P \sim \mathbb{R}^n} \#(P \setminus \Sigma)^2$, where the expectation is over random planes $P$.

Therefore, $\frac{\text{vol}(\Sigma_S)}{\text{vol}(S_0)} = d \cdot \text{Prob}_{P \sim \mathbb{R}^n} \{P \setminus \Sigma \neq \emptyset\} \leq d$. 


Volume of determinant hypersurface $\Sigma_S$ (1)

- $\Sigma$ is the zero set of the determinant, a homogeneous polynomial of degree $d = n$.
- Let $P$ be a plane (two-dimensional subspace) in $\mathbb{R}^{n \times n}$. How about the intersection $P \cap \Sigma$?
Volume of determinant hypersurface $\Sigma_S$ (1)

- $\Sigma$ is the zero set of the determinant, a homogeneous polynomial of degree $d = n$.
- Let $P$ be a plane (two-dimensional subspace) in $\mathbb{R}^{n\times n}$. How about the intersection $P \cap \Sigma$?
- Either $P \cap \Sigma = P$ (degenerate case) or $P \cap \Sigma$ is a union of $k$ lines through the origin, for $k \leq d$. 

$I$
Volume of determinant hypersurface $\Sigma_S$ (1)

- $\Sigma$ is the zero set of the determinant, a homogeneous polynomial of degree $d = n$.
- Let $P$ be a plane (two-dimensional subspace) in $\mathbb{R}^{n \times n}$. How about the intersection $P \cap \Sigma$?
- Either $P \cap \Sigma = P$ (degenerate case) or $P \cap \Sigma$ is a union of $k$ lines through the origin, for $k \leq d$.
- Hence, almost surely, $P \cap \Sigma_S$ is either empty or consists of $2d$ points, two of which are diametral.
Volume of determinant hypersurface $\Sigma_S$ (1)

- $\Sigma$ is the zero set of the determinant, a homogeneous polynomial of degree $d = n$.
- Let $P$ be a plane (two-dimensional subspace) in $\mathbb{R}^{n \times n}$. How about the intersection $P \cap \Sigma$?
- Either $P \cap \Sigma = P$ (degenerate case) or $P \cap \Sigma$ is a union of $k$ lines through the origin, for $k \leq d$.
- Hence, almost surely, $P \cap \Sigma_S$ is either empty or consists of $2d$ points, two of which are diametral.
- Let $S'$ be the intersection of $S$ with a hyperplane (hyperequator). Poincaré's formula of integral geometry states

$$\frac{\text{vol}(\Sigma_S)}{\text{vol}(S')} = \mathbb{E}_P \left( \frac{\#(P \cap \Sigma_S)}{2} \right),$$

where the expectation is over random planes $P$.  


Volume of determinant hypersurface $\Sigma_S$ (1)

- $\Sigma$ is the zero set of the determinant, a homogeneous polynomial of degree $d = n$.
- Let $P$ be a plane (two-dimensional subspace) in $\mathbb{R}^{n \times n}$. How about the intersection $P \cap \Sigma$?
- Either $P \cap \Sigma = P$ (degenerate case) or $P \cap \Sigma$ is a union of $k$ lines through the origin, for $k \leq d$.
- Hence, almost surely, $P \cap \Sigma_S$ is either empty or consists of $2d$ points, two of which are diametral.
- Let $S'$ be the intersection of $S$ with a hyperplane (hyperequator).

Poincaré’s formula of integral geometry states
\[
\frac{\text{vol}(\Sigma_S)}{\text{vol}(S')} = \mathbb{E}_P\left(\frac{\#(P \cap \Sigma_S)}{2}\right),
\]
where the expectation is over random planes $P$.

- Therefore,
\[
\frac{\text{vol}(\Sigma_S)}{\text{vol}(S')} = d \cdot \text{Prob}\{P \cap \Sigma_S \neq \emptyset\} \leq d.
\]
Volume of determinant hypersurface $\Sigma_\mathcal{S}$ (2)

From

$$\frac{\text{vol}(\Sigma_\mathcal{S})}{\text{vol}(\mathcal{S})} = \frac{\text{vol}(\Sigma_\mathcal{S})}{\text{vol}(\mathcal{S}')} \cdot \frac{\text{vol}(\mathcal{S}')}{\text{vol}(\mathcal{S})} \leq d \sqrt{\frac{\dim \mathcal{S}}{2\pi}} \leq \frac{n^2}{\sqrt{2\pi}}.$$

we obtain the asymptotic tail bound

$$\text{Prob}_{\mathcal{B}}\{\kappa_F(B) \geq \varepsilon^{-1}\} = \frac{\text{vol}(\Sigma_\mathcal{S}) \cdot 2\varepsilon}{\text{vol}(\mathcal{S})} + o(\varepsilon) \leq \sqrt{\frac{2}{\pi}} n^2 \varepsilon + o(\varepsilon).$$
Volume of determinant hypersurface $\Sigma_S (2)$

- From

$$\frac{\text{vol}(\Sigma_S)}{\text{vol}(S)} = \frac{\text{vol}(\Sigma_S)}{\text{vol}(S')} \cdot \frac{\text{vol}(S')}{\text{vol}(S)} \leq d \sqrt{\frac{\dim S}{2\pi}} \leq \frac{n^2}{\sqrt{2\pi}}.$$  

we obtain the asymptotic tail bound

$$\text{Prob}_B \{ \kappa_F(B) \geq \epsilon^{-1} \} = \frac{\text{vol}(\Sigma_S)}{\text{vol}(S)} \cdot 2\epsilon + o(\epsilon) \leq \sqrt{\frac{2}{\pi}} n^2 \epsilon + o(\epsilon).$$

- This bound is larger by a factor $\approx n$ than Edelman’s bound

$$\text{Prob}_B \{ \kappa(B) \geq \epsilon^{-1} \} = 2n \epsilon + o(\epsilon).$$
Volume of determinant hypersurface $\Sigma_S$ \((2)\)

- From

$$\frac{\text{vol}(\Sigma_S)}{\text{vol}(\mathbb{S})} = \frac{\text{vol}(\Sigma_S)}{\text{vol}(\mathbb{S}')} \cdot \frac{\text{vol}(\mathbb{S}')}{\text{vol}(\mathbb{S})} \leq d \sqrt{\frac{\text{dim } \mathbb{S}}{2\pi}} \leq \frac{n^2}{\sqrt{2\pi}}.$$  

we obtain the asymptotic tail bound

$$\text{Prob}_B\{\kappa_F(B) \geq \varepsilon^{-1}\} = \frac{\text{vol}(\Sigma_S) \cdot 2\varepsilon}{\text{vol}(\mathbb{S})} + o(\varepsilon) \leq \sqrt{\frac{2}{\pi}} n^2 \varepsilon + o(\varepsilon).$$

- This bound is larger by a factor $\approx n$ than Edelman’s bound

$$\text{Prob}_B\{\kappa(B) \geq \varepsilon^{-1}\} = 2n \varepsilon + o(\varepsilon).$$

- By a more careful estimation of tube volumes one can derive nonasymptotic bounds.
Volume of determinant hypersurface $\Sigma_S$ (2)

From

$$\frac{\text{vol}(\Sigma_S)}{\text{vol}(S)} = \frac{\text{vol}(\Sigma_S)}{\text{vol}(S')} \cdot \frac{\text{vol}(S')}{\text{vol}(S)} \leq d \sqrt{\frac{\dim S}{2\pi}} \leq \frac{n^2}{\sqrt{2\pi}}.$$ 

we obtain the asymptotic tail bound

$$\text{Prob}_B \{ \kappa_F(B) \geq \varepsilon^{-1} \} = \frac{\text{vol}(\Sigma_S) \cdot 2\varepsilon}{\text{vol}(S)} + o(\varepsilon) \leq \sqrt{\frac{2}{\pi}} \cdot n^2 \varepsilon + o(\varepsilon).$$

This bound is larger by a factor $\approx n$ than Edelman’s bound

$$\text{Prob}_B \{ \kappa(B) \geq \varepsilon^{-1} \} = 2n \varepsilon + o(\varepsilon).$$

By a more careful estimation of tube volumes one can derive nonasymptotic bounds.

These ideas have been developed in detail by Demmel (1988).
Application to method of conjugate gradients

- The method of conjugate gradients, on input $S = A^T A$, takes

$$\frac{1}{2} \sqrt{\kappa(S)} \ln \left( \frac{1}{\varepsilon} \right) = \frac{1}{2} \kappa(A) \ln \left( \frac{1}{\varepsilon} \right).$$

iterations to achieve relative error $\varepsilon$. 

However, $\text{Prob} \{ \kappa(A) \} = O(n^t)$ implies $E(\kappa(A)) = 1$. This is inconsistent with the success of CGM in practice! Explanation?
Application to method of conjugate gradients

- The method of conjugate gradients, on input $S = A^T A$, takes
  $$\frac{1}{2} \sqrt{\kappa(S)} \ln \left( \frac{1}{\varepsilon} \right) = \frac{1}{2} \kappa(A) \ln \left( \frac{1}{\varepsilon} \right).$$
  iterations to achieve relative error $\varepsilon$.

- However,
  $$\text{Prob}\{\kappa(A) \geq t\} = O\left( \frac{n}{t} \right)$$
  implies
  $$\mathbb{E}(\kappa(A)) = \infty.$$  
  This is inconsistent with the success of CGM in practice!

**Explanation?**
Condition of rectangular matrices

- CGM is usually applied to $S = R^T R$, where $R \in \mathbb{R}^{m \times n}$ is rectangular with $m \geq n$. (E.g., overdetermined least square problem with $m$ linear constraints in $n$ variables.)
Condition of rectangular matrices

- CGM is usually applied to $S = R^T R$, where $R \in \mathbb{R}^{m \times n}$ is rectangular with $m \geq n$. (E.g., overdetermined least square problem with $m$ linear constraints in $n$ variables.)

- Let $q \in (0, 1)$. It is known (Geman (1980), Silverstein (1985)) that for standard Gaussian $R$ of size $m_n \times n$ and $m_n/n \to q$ for $n \to \infty$

$$\kappa(R) \xrightarrow{a.s.} \frac{1 + \sqrt{q}}{1 - \sqrt{q}}.$$
Condition of rectangular matrices

- CGM is usually applied to $S = R^T R$, where $R \in \mathbb{R}^{m \times n}$ is rectangular with $m \geq n$. (E.g., overdetermined least square problem with $m$ linear constraints in $n$ variables.)
- Let $q \in (0, 1)$. It is known (Geman (1980), Silverstein (1985)) that for standard Gaussian $R$ of size $m \times n$ and $m_n/n \to q$ for $n \to \infty$

$$\kappa(R) \overset{a.s.}{\to} \frac{1 + \sqrt{q}}{1 - \sqrt{q}}.$$

- Hence: The expected number of iterations of CGM is independent of $n$ and only depends on the ratio $q$. 

\[ \kappa(A) \]
Condition of rectangular matrices

- CGM is usually applied to $S = R^T R$, where $R \in \mathbb{R}^{m \times n}$ is rectangular with $m \geq n$. (E.g., overdetermined least square problem with $m$ linear constraints in $n$ variables.)

- Let $q \in (0, 1)$. It is known (Geman (1980), Silverstein (1985)) that for standard Gaussian $R$ of size $m_n \times n$ and $m_n/n \to q$ for $n \to \infty$

$$\kappa(R) \xrightarrow{a.s.} \frac{1 + \sqrt{q}}{1 - \sqrt{q}}.$$

- Hence: The expected number of iterations of CGM is independent of $n$ and only depends on the ratio $q$.

- E.g., for $4n \times n$ matrices $R$ and large $n$, $\kappa(A) \simeq 3$. 
Probabilistic Analysis of Turing’s Condition Number

Smoothed Analysis
Smoothed analysis of $\kappa(A)$

- Take now any $\overline{A} \in \mathbb{R}^{n \times n}$, $0 < \sigma \leq 1$ and consider the isotropic Gaussian density

$$
\rho(A) = \frac{1}{(\sigma \sqrt{2\pi})^{n^2}} \exp\left(-\frac{\|A - \overline{A}\|_F^2}{2\sigma^2}\right)
$$

with mean $\overline{A}$ and covariance matrix $\sigma^2 I$. Notation: $A \sim N(\overline{A}, \sigma^2 I)$. 
Smoothed analysis of $\kappa(A)$

- Take now any $\bar{A} \in \mathbb{R}^{n \times n}$, $0 < \sigma \leq 1$ and consider the isotropic Gaussian density

$$
\rho(A) = \frac{1}{(\sigma \sqrt{2\pi})^n} \exp \left( - \frac{\|A - \bar{A}\|_F^2}{2\sigma^2} \right)
$$

with mean $\bar{A}$ and covariance matrix $\sigma^2 I$. Notation: $A \sim N(\bar{A}, \sigma^2 I)$.

- This models a slight perturbation of $A$ due to noise, round-off, etc.
Smoothed analysis of $\kappa(A)$

- Take now any $\overline{A} \in \mathbb{R}^{n \times n}$, $0 < \sigma \leq 1$ and consider the isotropic Gaussian density

$$\rho(A) = \frac{1}{(\sigma \sqrt{2\pi})^n} \exp \left( - \frac{\|A - \overline{A}\|^2_F}{2\sigma^2} \right)$$

with mean $\overline{A}$ and covariance matrix $\sigma^2 I$. Notation: $A \sim N(\overline{A}, \sigma^2 I)$.

- This models a slight perturbation of $A$ due to noise, round-off, etc.

- The goal of a smoothed analysis of $\kappa(A)$ is to derive tail bounds on it that are independent of the center $\overline{A}$. 
Smoothed analysis of $\kappa(A)$

- Take now any $\overline{A} \in \mathbb{R}^{n \times n}$, $0 < \sigma \leq 1$ and consider the isotropic Gaussian density

$$
\rho(A) = \frac{1}{(\sigma \sqrt{2\pi})^n} \exp \left( - \frac{\|A - \overline{A}\|_F^2}{2\sigma^2} \right)
$$

with mean $\overline{A}$ and covariance matrix $\sigma^2 I$. Notation: $A \sim N(\overline{A}, \sigma^2 I)$.

- This models a slight perturbation of $A$ due to noise, round-off, etc.

- The goal of a smoothed analysis of $\kappa(A)$ is to derive tail bounds on it that are independent of the center $\overline{A}$.

- Due to scale invariance of $\kappa(A)$ we assume $\|\overline{A}\|_F = 1$. 
Smoothed analysis of $\kappa(A)$

- Take now any $\overline{A} \in \mathbb{R}^{n \times n}$, $0 < \sigma \leq 1$ and consider the isotropic Gaussian density

$$
\rho(A) = \frac{1}{(\sigma \sqrt{2\pi})^n} \exp \left( - \frac{\|A - \overline{A}\|_F^2}{2\sigma^2} \right)
$$

with mean $\overline{A}$ and covariance matrix $\sigma^2 I$. Notation: $A \sim N(\overline{A}, \sigma^2 I)$.

- This models a slight perturbation of $A$ due to noise, round-off, etc.

- The goal of a smoothed analysis of $\kappa(A)$ is to derive tail bounds on it that are independent of the center $\overline{A}$.

- Due to scale invariance of $\kappa(A)$ we assume $\|\overline{A}\|_F = 1$.

- Improving results by Sankar, Spielman, and Teng (2006), Wschebor showed:
Smoothed analysis of $\kappa(A)$

- Take now any $\overline{A} \in \mathbb{R}^{n \times n}$, $0 < \sigma \leq 1$ and consider the isotropic Gaussian density
  \[
  \rho(A) = \frac{1}{(\sigma \sqrt{2\pi})^{n^2}} \exp\left(-\frac{\|A - \overline{A}\|_F^2}{2\sigma^2}\right)
  \]
  with mean $\overline{A}$ and covariance matrix $\sigma^2 I$. Notation: $A \sim N(\overline{A}, \sigma^2 I)$.

- This models a slight perturbation of $A$ due to noise, round-off, etc.

- The goal of a smoothed analysis of $\kappa(A)$ is to derive tail bounds on it that are independent of the center $\overline{A}$.

- Due to scale invariance of $\kappa(A)$ we assume $\|\overline{A}\|_F = 1$.

- Improving results by Sankar, Spielman, and Teng (2006), Wschebor showed:

Wschebor (2004)

\[
\sup_{\|\overline{A}\|_F=1} \text{Prob} \{\kappa(A) \geq t\} = O\left(\frac{n}{\sigma t}\right).
\]
Smoothed analysis of $\kappa(A)$: rectangular case

- Wschebor’s tail bound implies

$$\sup_{\|\bar{A}\|=1} \mathbb{E}_{A \sim N(\bar{A}, \sigma^2 I)} \left( \log \kappa(A) \right) = \log \frac{n}{\sigma} + \mathcal{O}(1).$$
Smoothed analysis of $\kappa(A)$: rectangular case

- Wschebor’s tail bound implies

$$\sup_{\|A\|=1} \mathbb{E}_{A \sim N(A, \sigma^2 I)} \left( \log \kappa(A) \right) = \log \frac{n}{\sigma} + O(1).$$

- This gives a more compelling probabilistic interpretation of the success of several procedures in numerical linear algebra.
Smoothed analysis of $\kappa(A)$: rectangular case

- Wschebor’s tail bound implies

$$\sup_{\|A\|=1} \mathbb{E}_{A \sim N(A, \sigma^2 I)} \left( \log \kappa(A) \right) = \log \frac{n}{\sigma} + O(1).$$

- This gives a more compelling probabilistic interpretation of the success of several procedures in numerical linear algebra.

- For the rectangular case $R \in \mathbb{R}^{m \times n}$ we have:
Smoothed analysis of $\kappa(A)$: rectangular case

- Wschebor’s tail bound implies

$$\sup_{\|A\|_2=1} \mathbb{E}_{A \sim N(\overline{A}, \sigma^2 I)} \left( \log \kappa(A) \right) = \log \frac{n}{\sigma} + O(1).$$

- This gives a more compelling probabilistic interpretation of the success of several procedures in numerical linear algebra.

- For the rectangular case $R \in \mathbb{R}^{m \times n}$ we have:

**B, Cucker (2010)**

$$\sup_{\|R\|_F=1} \mathbb{E}_{R \sim N(\overline{R}, \sigma^2 I)} (\kappa(R)) \leq \frac{20.1}{1 - q}$$

for $q \in (0, 1)$, $m/n \leq q$, and sufficiently large $n$. 
Smoothed analysis of $\kappa(A)$: rectangular case

- Wschebor’s tail bound implies
  \[
  \sup_{\|A\|_1 = 1} \mathbb{E}_{A \sim N(\overline{A}, \sigma^2 I)} \left( \log \kappa(A) \right) = \log \frac{n}{\sigma} + O(1).
  \]

- This gives a more compelling probabilistic interpretation of the success of several procedures in numerical linear algebra.

- For the rectangular case $R \in \mathbb{R}^{m \times n}$ we have:

\[
\sup_{\|R\|_F = 1} \mathbb{E}_{R \sim N(\overline{R}, \sigma^2 I)} \left( \kappa(R) \right) \leq \frac{20.1}{1 - q}
\]

for $q \in (0, 1)$, $m/n \leq q$, and sufficiently large $n$.

- As in the average case, the bound is independent of $n$. Interestingly, it is also independent of $\sigma$ (for large $n$)!
Smoothed analysis of $\kappa(A)$: rectangular case

- Wschebor’s tail bound implies
  \[ \sup_{\|A\|=1} E_{A \sim N(\bar{A}, \sigma^2 I)} \left( \log \kappa(A) \right) = \log \frac{n}{\sigma} + O(1). \]

- This gives a more compelling probabilistic interpretation of the success of several procedures in numerical linear algebra.
- For the rectangular case $R \in \mathbb{R}^{m \times n}$ we have:

B, Cucker (2010)

\[ \sup_{\|R\|_F=1} E_{R \sim N(\bar{R}, \sigma^2 I)} (\kappa(R)) \leq \frac{20.1}{1 - q} \]

for $q \in (0, 1)$, $m/n \leq q$, and sufficiently large $n$.

- As in the average case, the bound is independent of $n$. Interestingly, it is also independent of $\sigma$ (for large $n$)!
- Has obvious consequence for the probabilistic analysis of CGM.
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
- As for the average-case analysis, it is possible to give smoothed analysis bounds in a geometrically intuitive way that apply to a wide variety of situations.
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
- As for the average-case analysis, it is possible to give smoothed analysis bounds in a geometrically intuitive way that apply to a wide variety of situations.
- Think of $\kappa$ as a function defined on the sphere $\mathbb{S} = S^{n^2-1}$.
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
- As for the average-case analysis, it is possible to give smoothed analysis bounds in a geometrically intuitive way that apply to a wide variety of situations.
- Think of $\kappa$ as a function defined on the sphere $\mathbb{S} = S^{n^2-1}$.
- Let $B(\overline{A}, \sigma)$ denote the spherical cap in $\mathbb{S}$ of angular radius $\arcsin \sigma$ with center $\overline{A} \in \mathbb{S}$, where $0 \leq \sigma \leq 1$. 
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
- As for the average-case analysis, it is possible to give smoothed analysis bounds in a geometrically intuitive way that apply to a wide variety of situations.
- Think of $\kappa$ as a function defined on the sphere $\mathbb{S} = S_{n^2-1}$.
- Let $B(\overline{A}, \sigma)$ denote the spherical cap in $\mathbb{S}$ of angular radius $\arcsin \sigma$ with center $\overline{A} \in \mathbb{S}$, where $0 \leq \sigma \leq 1$.
- We model now perturbations by $A$ chosen from a uniform distribution on $B(\overline{A}, \sigma)$: uniform smoothed analysis.
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
- As for the average-case analysis, it is possible to give smoothed analysis bounds in a geometrically intuitive way that apply to a wide variety of situations.
- Think of $\kappa$ as a function defined on the sphere $\mathbb{S} = S^{n^2-1}$.
- Let $B(\overline{A}, \sigma)$ denote the spherical cap in $\mathbb{S}$ of angular radius $\arcsin \sigma$ with center $\overline{A} \in \mathbb{S}$, where $0 \leq \sigma \leq 1$.
- We model now perturbations by $A$ chosen from a uniform distribution on $B(\overline{A}, \sigma)$: uniform smoothed analysis.
  - $\sigma = 0$ yields worst-case analysis
Geometric ideas for smoothed analysis (1)

- The mentioned smoothed analysis bounds were derived by direct, problem adapted methods from probability.
- As for the average-case analysis, it is possible to give smoothed analysis bounds in a geometrically intuitive way that apply to a wide variety of situations.
- Think of $\kappa$ as a function defined on the sphere $S = S^{n^2-1}$.
- Let $B(\overline{A}, \sigma)$ denote the spherical cap in $S$ of angular radius $\arcsin \sigma$ with center $\overline{A} \in S$, where $0 \leq \sigma \leq 1$.
- We model now perturbations by $A$ chosen from a uniform distribution on $B(\overline{A}, \sigma)$: uniform smoothed analysis.
  - $\sigma = 0$ yields worst-case analysis
  - $\sigma = 1$ yields average-case analysis
Geometric ideas for smoothed analysis (2)

Let $T(\Sigma_S, \varepsilon)$ denote the neighborhood (or tube) of $\Sigma_S$ of radius $\arcsin \varepsilon$. 
Geometric ideas for smoothed analysis (2)

Let $T(\Sigma_S, \varepsilon)$ denote the neighborhood (or tube) of $\Sigma_S$ of radius $\arcsin \varepsilon$.

\[
\text{Prob}_{A \in B(\bar{A}, \sigma)} \{ \kappa_F(A) \geq \varepsilon^{-1} \} = \text{Prob}_{A \in B(\bar{A}, \sigma)} \{ \text{dist}(A, \Sigma) \leq \varepsilon \}
\]
\[
= \text{Prob}_{A \in B(\bar{A}, \sigma)} \{ A \in T(\Sigma_S, \varepsilon) \} = \frac{\text{vol}(T(\Sigma_S, \varepsilon) \cap B(\bar{A}, \sigma))}{\text{vol}(B(\bar{A}, \sigma))}
\]

Uniform smoothed analysis means to provide relative bounds on the volume of tubes intersected with small spherical caps!
Heuristic estimation (1)

Write $B := B(\bar{A}, \sigma)$. Then

$$\frac{\text{vol}(T(S, \varepsilon) \cap B)}{\text{vol}(B)} \approx \frac{\text{vol}(S \cap B) \cdot 2\varepsilon}{\text{vol}(B)}.$$
Heuristic estimation (1)

Write $B := B(\overline{A}, \sigma)$. Then

$$\frac{\text{vol}(T(\Sigma_S, \varepsilon) \cap B)}{\text{vol}(B)} \approx \frac{\text{vol}(\Sigma_S \cap B) \cdot 2\varepsilon}{\text{vol}(B)}.$$ 

Poincaré’s formula yields as before, with $d = n$,

$$\frac{\text{vol}(\Sigma_S \cap B)}{\text{vol}(S')} = \mathbb{E}_P\left(\frac{\#(P \cap \Sigma_S \cap B)}{2}\right) \leq d \cdot \text{Prob}_P\{P \cap B \neq \emptyset\}. $$

where the expectation is over random planes $P$.
Heuristic estimation (1)

- Write $B := B(A, \sigma)$. Then
  \[
  \frac{\text{vol}(T(\Sigma, \varepsilon) \cap B)}{\text{vol}(B)} \approx \frac{\text{vol}(\Sigma \cap B) \cdot 2\varepsilon}{\text{vol}(B)}.
  \]

- Poincaré’s formula yields as before, with $d = n$,
  \[
  \frac{\text{vol}(\Sigma \cap B)}{\text{vol}(S')} = \mathbb{E}_P\left(\frac{\#(P \cap \Sigma \cap B)}{2}\right) \leq d \cdot \text{Prob}_P\{P \cap B \neq \emptyset\}.
  \]
  where the expectation is over random planes $P$.

- Therefore, writing $p := \text{dim} S$,
  \[
  \frac{\text{vol}(\Sigma \cap B)}{\text{vol}(B)} = \frac{\text{vol}(\Sigma \cap B)}{\text{vol}(S')} \cdot \frac{\text{vol}(S')}{\text{vol}(S)} \cdot \frac{\text{vol}(S)}{\text{vol}(B)} \leq d \cdot \text{Prob}_P\{P \cap B \neq \emptyset\} \cdot \sqrt{p} \cdot \frac{1}{\sigma^p}.
  \]
Heuristic estimation (2)

- \( P \cap S := S^1 \) is a circle. We may as well fix this circle and take a random cap \( B \) of radius \( \arcsin \sigma \).
Heuristic estimation (2)

- $P \cap S := S^1$ is a circle. We may as well fix this circle and take a random cap $B$ of radius $\arcsin \sigma$.
- The cap $B$ meets $S^1$ iff the center of $B$ is $\sigma$-close to $S^1$. Therefore,

$$\Pr_B\{S^1 \cap B \neq \emptyset\} = \frac{\text{vol}(T(S^1, \sigma))}{\text{vol}(S)}.$$
Heuristic estimation (2)

- $P \cap S := S^1$ is a circle. We may as well fix this circle and take a random cap $B$ of radius $\arcsin \sigma$.

- The cap $B$ meets $S^1$ iff the center of $B$ is $\sigma$-close to $S^1$. Therefore,

$$\Pr_B\{S^1 \cap B \neq \emptyset\} = \frac{\text{vol}(T(S^1, \sigma))}{\text{vol}(S)}.$$ 

- This is roughly $2\pi$ times the volume of a $(p - 1)$-dimensional ball of radius $\sigma$ in the cross section to $S^1$, divided by $\text{vol}(S)$. It is roughly $\sigma^{p-1}$. 
Heuristic estimation (2)

- $P \cap S := S^1$ is a circle. We may as well fix this circle and take a random cap $B$ of radius $\arcsin \sigma$.
- The cap $B$ meets $S^1$ iff the center of $B$ is $\sigma$-close to $S^1$. Therefore,

$$\Pr_B\{S^1 \cap B \neq \emptyset\} = \frac{\text{vol}(T(S^1, \sigma))}{\text{vol}(S)}.$$  

- This is roughly $2\pi$ times the volume of a $(p-1)$-dimensional ball of radius $\sigma$ in the cross section to $S^1$, divided by $\text{vol}(S)$. It is roughly $\sigma^{p-1}$.
- Hence

$$\frac{\text{vol}(S \cap B)}{\text{vol}(B)} \lesssim d \cdot \Pr_P\{P \cap B \neq \emptyset\} \cdot \sqrt{p} \cdot \frac{1}{\sigma^p}$$

$$\approx d \cdot \sigma^{p-1} \cdot \sqrt{p} \cdot \frac{1}{\sigma^p} = \frac{d\sqrt{p}}{\sigma}.$$
Heuristic estimation (3)

- Altogether

\[
\text{Prob}_{A \in B(\overline{A}, \sigma)} \{ \kappa_F(A) \geq \epsilon^{-1} \} = \frac{\text{vol}(T(\Sigma_\mathcal{S}, \epsilon) \cap B)}{\text{vol}(B)} \\
\approx \frac{\text{vol}(\Sigma_\mathcal{S} \cap B) \cdot 2\epsilon}{\text{vol}(B)} \preceq \frac{d \sqrt{p} \epsilon}{\sigma} = \mathcal{O}\left(\frac{n^2 \epsilon}{\sigma}\right).
\]
Heuristic estimation (3)

- Altogether

\[ \text{Prob}_{A \in B(A, \sigma)} \left\{ \kappa_F(A) \geq \varepsilon^{-1} \right\} = \frac{\text{vol}(T(\Sigma_B, \varepsilon) \cap B)}{\text{vol}(B)} \]

\[ \approx \frac{\text{vol}(\Sigma_B \cap B) \cdot 2\varepsilon}{\text{vol}(B)} \ll \frac{d \sqrt{p} \varepsilon}{\sigma} = O \left( \frac{n^2 \varepsilon}{\sigma} \right). \]

- Using some differential and integral geometry, this can be turned into a proof, yielding a bound of essentially this order of magnitude.
Heuristic estimation (3)

- Altogether

\[
\text{Prob}_{A \in B(A, \sigma)} \{ \kappa_F(A) \geq \varepsilon^{-1} \} = \frac{\text{vol}(T(\Sigma, \varepsilon) \cap B)}{\text{vol}(B)} \\
\approx \frac{\text{vol}(\Sigma \cap B) \cdot 2 \varepsilon}{\text{vol}(B)} \ll \frac{d \sqrt{p} \varepsilon}{\sigma} = O\left(\frac{n^2 \varepsilon}{\sigma}\right).
\]

- Using some differential and integral geometry, this can be turned into a proof, yielding a bound of essentially this order of magnitude.

- The bound is worse by a factor \( n \) compared to Wschebor’s result. But it has the advantage to be true in a much more general situation.
A general result for smoothed analysis

- Assume that \( \Sigma \subset \mathbb{R}^{p+1} \) is given as the zero set of a homogeneous polynomial of degree \( d \).
A general result for smoothed analysis

- Assume that \( \Sigma \subset \mathbb{R}^{p+1} \) is given as the zero set of a homogeneous polynomial of degree \( d \).
- For \( a \in \mathbb{R}^{p+1} \) define the conic condition number of \( a \) abstractly by

\[
C(a) = \frac{\|a\|}{\text{dist}(a, \Sigma)}.
\]
A general result for smoothed analysis

- Assume that $\Sigma \subset \mathbb{R}^{p+1}$ is given as the zero set of a homogeneous polynomial of degree $d$.
- For $a \in \mathbb{R}^{p+1}$ define the **conic condition number** of $a$ abstractly by

$$C(a) = \frac{\|a\|}{\text{dist}(a, \Sigma)}.$$
A general result for smoothed analysis

- Assume that $\Sigma \subset \mathbb{R}^{p+1}$ is given as the zero set of a homogeneous polynomial of degree $d$.
- For $a \in \mathbb{R}^{p+1}$ define the conic condition number of $a$ abstractly by
  \[ C(a) = \frac{\|a\|}{\text{dist}(a, \Sigma)}. \]


For all $\sigma \in (0, 1]$ and all $t \geq (2d + 1) \frac{p}{\sigma}$,

\[
\sup_{a \in S^p} \mathbb{P}_{a \in B(\overline{a}, \sigma)} \{ C(a) \geq t \} \leq 26 dp \frac{1}{\sigma t}.
\]

\[
\sup_{a \in S^p} \mathbb{E}_{a \in B(\overline{a}, \sigma)} (\ln C(a)) \leq 2 \ln \left( \frac{dp}{\sigma} \right) + 4.7.
\]
Application: Eigenvalue computation

- A similar result can be shown over the complex numbers, where the set \( \Sigma \) of ill-posed inputs is a complex algebraic hypersurface. (Considerably simpler proof.)
Application: Eigenvalue computation

- A similar result can be shown over the complex numbers, where the set $\Sigma$ of ill-posed inputs is a complex algebraic hypersurface. (Considerably simpler proof.)
- **Problem:** Compute the (complex) eigenvalues of a matrix $A \in \mathbb{C}^{n \times n}$
Application: Eigenvalue computation

- A similar result can be shown over the complex numbers, where the set $\Sigma$ of ill-posed inputs is a complex algebraic hypersurface. (Considerably simpler proof.)

- **Problem:** Compute the (complex) eigenvalues of a matrix $A \in \mathbb{C}^{n \times n}$

- **Set of ill-posed inputs:** Set $\Sigma$ of matrices $A$ having multiple eigenvalues. This is the zero set of the discriminant polynomial of the characteristic polynomial, which has degree $d = n^2 - n$. 
Application: Eigenvalue computation

- A similar result can be shown over the complex numbers, where the set $\Sigma$ of ill-posed inputs is a complex algebraic hypersurface. (Considerably simpler proof.)
- **Problem:** Compute the (complex) eigenvalues of a matrix $A \in \mathbb{C}^{n \times n}$
- **Set of ill-posed inputs:** Set $\Sigma$ of matrices $A$ having multiple eigenvalues. This is the zero set of the discriminant polynomial of the characteristic polynomial, which has degree $d = n^2 - n$.
- **Condition number (Wilkinson, 1965):** Satisfies $\kappa_{\text{eigen}}(A) \leq \frac{\sqrt{2} \|A\|_F}{\text{dist}(A,\Sigma)}$
Application: Eigenvalue computation

- A similar result can be shown over the complex numbers, where the set $\Sigma$ of ill-posed inputs is a complex algebraic hypersurface. (Considerably simpler proof.)
- **Problem:** Compute the (complex) eigenvalues of a matrix $A \in \mathbb{C}^{n \times n}$
- **Set of ill-posed inputs:** Set $\Sigma$ of matrices $A$ having multiple eigenvalues. This is the zero set of the discriminant polynomial of the characteristic polynomial, which has degree $d = n^2 - n$.
- **Condition number (Wilkinson, 1965):** Satisfies $\kappa_{\text{eigen}}(A) \leq \frac{\sqrt{2} \|A\|_F}{\text{dist}(A, \Sigma)}$
- **Corollary:** For all $\bar{A} \in \mathbb{R}^{n \times n}$ of Frobenius norm one and $0 < \sigma \leq 1$

\[
\mathbb{E}_{A \in B(\bar{A}, \sigma)}(\ln \kappa_{\text{eigen}}(A)) \leq 2 \ln \frac{n^4}{\sigma} + 5.
\]
Random Triangular Matrices:

The classical condition number is not always appropriate!
Random triangular matrices are ill-conditioned

- Practitioners observed since long that triangular systems of equations are generally solved to high accuracy in spite of being, in general, ill-conditioned.
Random triangular matrices are ill-conditioned

- Practitioners observed since long that triangular systems of equations are generally solved to high accuracy in spite of being, in general, ill-conditioned.
- Let $L = (l_{ij}) \in \mathbb{R}^{n \times n}$ be a random lower-triangular matrix with independent standard Gaussian random entries $l_{ij}$ for $i \geq j$. 

\[ E(\log |L|) = \Omega(n). \]

We give a simple proof of a related result later on.

If the loss of precision in the solution of triangular systems conforms to this bound, we would not be able to accurately find these solutions!
Random triangular matrices are ill-conditioned

- Practitioners observed since long that triangular systems of equations are generally solved to high accuracy in spite of being, in general, ill-conditioned.
- Let $L = (l_{ij}) \in \mathbb{R}^{n \times n}$ be a random lower-triangular matrix with independent standard Gaussian random entries $l_{ij}$ for $i \geq j$.

Viswanathan and Trefethen (1998)

$$\mathbb{E} (\ln \kappa (L)) \geq \Omega (n).$$
Random triangular matrices are ill-conditioned

- Practitioners observed since long that triangular systems of equations are generally solved to high accuracy in spite of being, in general, ill-conditioned.
- Let $L = (l_{ij}) \in \mathbb{R}^{n \times n}$ be a random lower-triangular matrix with independent standard Gaussian random entries $l_{ij}$ for $i \geq j$.

**Viswanathan and Trefethen (1998)**

$$\mathbb{E}(\ln \kappa(L)) \geq \Omega(n).$$

- We give a simple proof of a related result later on.
Random triangular matrices are ill-conditioned

- Practitioners observed since long that triangular systems of equations are generally solved to high accuracy in spite of being, in general, ill-conditioned.
- Let \( L = (l_{ij}) \in \mathbb{R}^{n \times n} \) be a random lower-triangular matrix with independent standard Gaussian random entries \( l_{ij} \) for \( i \geq j \).

Viswanathan and Trefethen (1998)

\[ \mathbb{E}(\ln \kappa(L)) \geq \Omega(n). \]

- We give a simple proof of a related result later on.
- Would the loss of precision in the solution of triangular systems conform to this bound, we would not be able to accurately find these solutions!

**Explanation?**
Componentwise relative errors

The classical condition number is the condition number of matrix inversion $A \mapsto A^{-1}$:

$$\kappa(A) = \lim_{\delta \to 0} \sup_{\text{RelError}(A) \leq \delta} \frac{\text{RelError}(A^{-1})}{\text{RelError}(A)}.$$  

Here, we use the normwise relative error

$$\text{RelError}(A) := \frac{\|\tilde{A} - A\|}{\|A\|},$$

with the spectral norm $\|\|$.
Instead of RelError we may use the possibly much larger componentwise relative error

\[ \text{CwRelError}(A) := \max_{i,j} \frac{\| \tilde{a}_{ij} - a_{ij} \|}{\| a_{ij} \|}. \]
Componentwise condition number

- Instead of RelError we may use the possibly much larger componentwise relative error

\[ Cw\text{RelError}(A) := \max_{i,j} \frac{\|\tilde{a}_{ij} - a_{ij}\|}{\|a_{ij}\|}. \]

- We define the componentwise condition number of matrix inversion correspondingly as

\[ Cw^\dagger(A) := \lim_{\delta \to 0} \sup_{\text{CwRelError}(A) \leq \delta} \frac{\text{CwRelError}(A^{-1})}{\text{CwRelError}(A)}. \]
Backward substitution is componentwise stable

- **Backward substitution** is the obvious algorithm for solving a triangular linear system $Lx = b$. 


Cheung & Cucker (2009)

$\mathbb{E}(\log C_w(\Delta L)) = O(\log n)$

for a random lower-triangular matrix $L \in \mathbb{R}^{n \times n}$ with independent standard Gaussian random entries.

This explains why linear triangular systems can be solved by backward substitution with high accuracy.
Backward substitution is componentwise stable

- **Backward substitution** is the obvious algorithm for solving a triangular linear system $Lx = b$.
- The loss of precision of backward substitution can be shown to be bounded by $O(\log Cw^\dagger(L) + \log n)$. 

- Recent result: Cheung & Cucker (2009)
  
  $E(\log Cw^\dagger(L)) = O(\log n)$ for a random lower-triangular matrix $L \in \mathbb{R}^{n \times n}$ with independent standard Gaussian random entries.

This explains why linear triangular systems can be solved by backward substitution with high accuracy.
Backward substitution is componentwise stable

- **Backward substitution** is the obvious algorithm for solving a triangular linear system $Lx = b$.
- The loss of precision of backward substitution can be shown to be bounded by $O(\log Cw^*(L) + \log n)$.
- Recent result:
Backward substitution is componentwise stable

- **Backward substitution** is the obvious algorithm for solving a triangular linear system $Lx = b$.
- The loss of precision of backward substitution can be shown to be bounded by $O(\log Cw^\dagger(L) + \log n)$.
- Recent result:
  
  **Cheung & Cucker (2009)**

  $$\mathbb{E}(\log Cw^\dagger(L)) = O(\log n)$$

  for a random lower-triangular matrix $L \in \mathbb{R}^{n \times n}$ with independent standard Gaussian random entries $\ell_{ij}$. 
Backward substitution is componentwise stable

- **Backward substitution** is the obvious algorithm for solving a triangular linear system $Lx = b$.
- The loss of precision of backward substitution can be shown to be bounded by $O(\log C_{w}^\dagger(L) + \log n)$.
- Recent result:

  **Cheung & Cucker (2009)**

  $\mathbb{E}(\log C_{w}^\dagger(L)) = O(\log n)$

  for a random lower-triangular matrix $L \in \mathbb{R}^{n \times n}$ with independent standard Gaussian random entries $\ell_{ij}$

- This explains why linear triangular systems can be solved by backward substitution with high accuracy.
Why random triang. matrices are ill-conditioned (1)

Let $L = (l_{ij})$ denote a random unit lower-triangular matrix with $l_{ii} = 1$ and with independent standard Gaussian random entries $l_{ij}$ for $i > j$. Then we have

$$
\mathbb{E}(\|L^{-1}\|_F^2) = 2^n - 1.
$$

In particular, $\mathbb{E}(\|L\|_F^2\|L^{-1}\|_F^2) \geq n(2^n - 1)$, hence $\mathbb{E}(\kappa(L)^2)$ grows exponentially in $n$. 
Why random triang. matrices are ill-conditioned (1)

Let \( L = (\ell_{ij}) \) denote a random unit lower-triangular matrix with \( \ell_{ii} = 1 \) and with independent standard Gaussian random entries \( \ell_{ij} \) for \( i > j \). Then we have

\[
\mathbb{E}(\|L^{-1}\|_F^2) = 2^n - 1.
\]

In particular, \( \mathbb{E}(\|L\|_F^2 \|L^{-1}\|_F^2) \geq n(2^n - 1) \), hence \( \mathbb{E}(\kappa(L)^2) \) grows exponentially in \( n \).

Proof.

- The first column \((s_1, \ldots, s_n)\) of \( L^{-1} \) is characterized by \( s_1 = 1 \) and the recursive relation

\[
s_i = -\sum_{j=1}^{i-1} \ell_{ij}s_j \quad \text{for } i = 2, \ldots, n.
\]
Why random triang. matrices are ill-conditioned (1)

Let $L = (\ell_{ij})$ denote a random unit lower-triangular matrix with $\ell_{ii} = 1$ and with independent standard Gaussian random entries $\ell_{ij}$ for $i > j$. Then we have

$$\mathbb{E}(\|L^{-1}\|_F^2) = 2^n - 1.$$  

In particular, $\mathbb{E}(\|L\|_F^2\|L^{-1}\|_F^2) \geq n(2^n - 1)$, hence $\mathbb{E}(\kappa(L)^2)$ grows exponentially in $n$.

Proof.

- The first column $(s_1, \ldots, s_n)$ of $L^{-1}$ is characterized by $s_1 = 1$ and the recursive relation

$$s_i = -\sum_{j=1}^{i-1} \ell_{ij}s_j \quad \text{for } i = 2, \ldots, n.$$  

- Hence $s_i$ is a function of the first $i$ rows of $L$ and thus independent of the entries of $L$ in the rows with index larger than $i$. 
Why random triang. matrices are ill-conditioned (2)

By squaring we obtain for $i \geq 2$

$$s_i^2 = \sum_{j \neq k, j, k < i} \ell_{ij} \ell_{ik} s_j s_k + \sum_{j < i} \ell_{ij}^2 s_j^2.$$
Why random triangular matrices are ill-conditioned (2)

- By squaring we obtain for $i \geq 2$

$$s_i^2 = \sum_{\substack{j \neq k \in [i-1] \setminus \{i\}}} \ell_{ij} \ell_{ik} s_j s_k + \sum_{j < i} \ell_{ij}^2 s_j^2.$$

- By the preceding observation, $s_j s_k$ is independent of $\ell_{ij} \ell_{ik}$ for $j, k < i$. If additionally $j \neq k$, we get

$$\mathbb{E}(\ell_{ij} \ell_{ik} s_j s_k) = \mathbb{E}(\ell_{ij} \ell_{ik}) \mathbb{E}(s_j s_k) = \mathbb{E}(\ell_{ij}) \mathbb{E}(\ell_{ik}) \mathbb{E}(s_j s_k) = 0$$

as $\ell_{ij}$ and $\ell_{ik}$ are independent and centered.
Why random triang. matrices are ill-conditioned (2)

- By squaring we obtain for \( i \geq 2 \)
  \[
  s_i^2 = \sum_{j \neq k, j, k < i} \ell_{ij} \ell_{ik} s_j s_k + \sum_{j < i} \ell_{ij}^2 s_j^2.
  \]

- By the preceding observation, \( s_j s_k \) is independent of \( \ell_{ij} \ell_{ik} \) for \( j, k < i \). If additionally \( j \neq k \), we get
  \[
  \mathbb{E}(\ell_{ij} \ell_{ik} s_j s_k) = \mathbb{E}(\ell_{ij} \ell_{ik}) \mathbb{E}(s_j s_k) = \mathbb{E}(\ell_{ij}) \mathbb{E}(\ell_{ik}) \mathbb{E}(s_j s_k) = 0
  \]
  as \( \ell_{ij} \) and \( \ell_{ik} \) are independent and centered.

- So the expectations of the mixed terms vanish and we obtain, using \( \mathbb{E}(\ell_{ij}^2) = 1 \), that
  \[
  \mathbb{E}(s_i^2) = \sum_{j=1}^{i-1} \mathbb{E}(s_j^2) \quad \text{for } i \geq 2.
  \]
Why random triang. matrices are ill-conditioned (2)

- By squaring we obtain for \( i \geq 2 \)
  \[
  s_i^2 = \sum_{j \neq k, j, k < i} \ell_{ij} \ell_{ik} s_j s_k + \sum_{j < i} \ell_{ij}^2 s_j^2.
  \]

- By the preceding observation, \( s_j s_k \) is independent of \( \ell_{ij} \ell_{ik} \) for \( j, k < i \). If additionally \( j \neq k \), we get
  \[
  \mathbb{E}(\ell_{ij} \ell_{ik} s_j s_k) = \mathbb{E}(\ell_{ij} \ell_{ik}) \mathbb{E}(s_j s_k) = \mathbb{E}(\ell_{ij}) \mathbb{E}(\ell_{ik}) \mathbb{E}(s_j s_k) = 0
  \]
as \( \ell_{ij} \) and \( \ell_{ik} \) are independent and centered.

- So the expectations of the mixed terms vanish and we obtain, using \( \mathbb{E}(\ell_{ij}^2) = 1 \), that
  \[
  \mathbb{E}(s_i^2) = \sum_{j=1}^{i-1} \mathbb{E}(s_j^2) \quad \text{for } i \geq 2.
  \]

- Solving this recursion with \( \mathbb{E}(s_1^2) = 1 \) yields
  \[
  \mathbb{E}(s_i^2) = 2^{i-2} \quad \text{for } i \geq 2.
  \]
Why random triang. matrices are ill-conditioned (3)

Therefore, the first column $v_1$ of $L^{-1}$ satisfies

$$
\mathbb{E}(\|v_1\|^2) = \mathbb{E}\left(\sum_{i=1}^{n} s_i^2\right) = 2^{n-1}.
$$
Therefore, the first column $v_1$ of $L^{-1}$ satisfies
\[ \mathbb{E}(\|v_1\|^2) = \mathbb{E}(\sum_{i=1}^{n} s_i^2) = 2^{n-1}. \]

By an analogous argument one shows that
\[ \mathbb{E}(\|v_k\|^2) = 2^{n-k} \]
for the $k$th column $v_k$ of $L^{-1}$. Altogether, we obtain
\[ \mathbb{E}(\|L^{-1}\|_F^2) = \mathbb{E}\left(\sum_{k=1}^{n} \|v_k\|^2\right) = \sum_{k=1}^{n} \mathbb{E}(\|v_k\|^2) = 2^n - 1. \]
Part II: Linear Inequalities
Interior-point methods for linear programming
Linear programming (1)

- **Standard primal form of linear programs:** given $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$; look for optimal $x \in \mathbb{R}^n$

$$\min c^T x \quad \text{subject to } Ax = b, \ x \geq 0 \quad (P)$$
Linear programming (1)

- **Standard primal form of linear programs**: given \( A \in \mathbb{R}^{m \times n}, b \in \mathbb{R}^m, c \in \mathbb{R}^n \); look for optimal \( x \in \mathbb{R}^n \)

\[
\min c^T x \quad \text{subject to} \quad Ax = b, \ x \geq 0
\]  
(P)

- **Standard dual form of linear programs**: Given \( A, b, c \), look for optimal \( y \in \mathbb{R}^m \).

\[
\max b^T y \quad \text{subject to} \quad A^T y \leq c
\]  
(D)
Linear programming (1)

- **Standard primal form of linear programs**: given $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$; look for optimal $x \in \mathbb{R}^n$

$$
\min c^T x \text{ subject to } Ax = b, \ x \geq 0 \quad (P)
$$

- **Standard dual form of linear programs**: Given $A$, $b$, $c$, look for optimal $y \in \mathbb{R}^m$.

$$
\max b^T y \text{ subject to } A^T y \leq c \quad (D)
$$

- It is known that $\max b^T y = \min c^T x$ if (P) and (D) are both feasible (duality).
Linear programming (1)

- **Standard primal form of linear programs**: given $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$; look for optimal $x \in \mathbb{R}^n$

  $$\min c^T x \quad \text{subject to} \quad Ax = b, \ x \geq 0 \quad (P)$$

- **Standard dual form of linear programs**: Given $A, b, c$, look for optimal $y \in \mathbb{R}^m$.

  $$\max b^T y \quad \text{subject to} \quad A^T y \leq c \quad (D)$$

- It is known that $\max b^T y = \min c^T x$ if (P) and (D) are both feasible (duality).

- We always assume $n \geq m$. 
Suppose that (P) and (D) are both feasible, the vector 
\( s := c - A^T y \) of slack variables satisfies 
\[ A^T y + s = c, \quad s \geq 0, \]

hence, using \( Ax = b, \)
\[ c^T x - b^T y = (s^T + y^T A)x - b^T y = s^T x + y^T (Ax - b) = s^T x \geq 0. \]
Suppose that (P) and (D) are both feasible, the vector $s := c - A^Ty$ of slack variables satisfies

$$A^Ty + s = c, \quad s \geq 0,$$

hence, using $Ax = b$,

$$c^Tx - b^Ty = (s^T + y^TA)x - b^Ty = s^Tx + y^T(Ax - b) = s^Tx \geq 0.$$

Optimality is equivalent to $s^Tx = 0$, which is equivalent to the complementary slackness condition

$$x_is_i = 0, \quad i = 1, 2, \ldots, n. \quad (1)$$
Idea of primal-dual interior point methods (1)

- Dantzig’s simplex method follows a path of vertices on the boundary of the polyhedron of solutions.
**Idea of primal-dual interior point methods (1)**

- **Dantzig’s simplex method** follows a path of vertices on the boundary of the polyhedron of solutions.
- By contrast, interior point methods follow a path in the interior of the polyhedron, hence the name. This path is a nonlinear curve that is approximately followed by a variant of **Newton’s method**.
Idea of primal-dual interior point methods (1)

- Dantzig’s simplex method follows a path of vertices on the boundary of the polyhedron of solutions.
- By contrast, interior point methods follow a path in the interior of the polyhedron, hence the name. This path is a nonlinear curve that is approximately followed by a variant of Newton’s method.
- More specifically, primal-dual interior point methods follow the central path in the strictly feasible set $\mathcal{F}^o \subseteq \mathbb{R}^{n+m+n}$ defined by

$$Ax = b, \ A^Ty + s = c, \ x > 0, \ s > 0.$$  

with the additional quadratic constraints for $\mu > 0$

$$x_1s_1 = \mu, \ldots, x_ns_n = \mu.$$
Idea of primal-dual interior point methods (1)

- **Dantzig’s simplex method** follows a path of vertices on the boundary of the polyhedron of solutions.

- By contrast, interior point methods follow a path in the interior of the polyhedron, hence the name. This path is a nonlinear curve that is approximately followed by a variant of **Newton’s method**.

- More specifically, primal-dual interior point methods follow the central path in the strictly feasible set $\mathcal{F}^\circ \subseteq \mathbb{R}^{n+m+n}$ defined by

\[
Ax = b, \quad A^T y + s = c, \quad x > 0, \quad s > 0.
\]

with the additional quadratic constraints for $\mu > 0$

\[
x_1 s_1 = \mu, \ldots, \ x_n s_n = \mu.
\]

- It can be shown that, if $\text{rank} A = m$, there is exactly one solution $\zeta_\mu$ of this system, for all $\mu > 0$. 
Idea of primal-dual interior point methods (2)

- Suppose we know $\zeta_{\mu_0}$ for some $\mu_0 > 0$. 
Idea of primal-dual interior point methods (2)

- Suppose we know $\mu_0$ for some $\mu_0 > 0$.
- We choose a centering parameter $\sigma \in (0, 1)$ and consider $\mu_k = \sigma^k \mu_0$ converging to 0.
Idea of primal-dual interior point methods (2)

- Suppose we know $\zeta_{\mu_0}$ for some $\mu_0 > 0$.
- We choose a centering parameter $\sigma \in (0, 1)$ and consider $\mu_k = \sigma^k \mu_0$ converging to 0.
- We successively compute approximations $z_k$ of $\zeta_k := \zeta_{\mu_k}$ for $k = 0, 1, 2, \ldots$ until a certain accuracy is reached.
Idea of primal-dual interior point methods (2)

- Suppose we know $\zeta_{\mu_0}$ for some $\mu_0 > 0$.
- We choose a centering parameter $\sigma \in (0, 1)$ and consider $\mu_k = \sigma^k \mu_0$ converging to 0.
- We successively compute approximations $z_k$ of $\zeta_k := \zeta_{\mu_k}$ for $k = 0, 1, 2, \ldots$ until a certain accuracy is reached.

The duality measure of $z = (x, y, s) \in \mathcal{F}^\circ$ is defined as

$$\mu(z) := \frac{1}{n} \sum_{i=1}^{n} x_i s_i.$$
Derivation of the algorithm (1)

- We get the approximations $z_k$ by Newton’s method, one of the most fundamental methods in computational mathematics.
Derivation of the algorithm (1)

- We get the approximations $z_k$ by Newton’s method, one of the most fundamental methods in computational mathematics.

- Consider the map $F: \mathbb{R}^{n+m+n} \to \mathbb{R}^{n+m+n}$,

$$z = (x, y, s) \mapsto F(z) = (A^T y + s - c, Ax - b, x_1 s_1, \ldots, x_n s_n)$$

satisfying $\{z_\mu\} = F^{-1}(0, 0, \mu e_n)$, where $e_n := (1, \ldots, 1) \in \mathbb{R}^n$. The Jacobian matrix of $F$ at $z$ equals

$$DF(z) = \begin{bmatrix}
0 & A^T & I \\
A & 0 & 0 \\
S & 0 & X
\end{bmatrix},$$

where here and in the following we set

$$S = \text{diag}(s_1, \ldots, s_n), \quad X = \text{diag}(x_1, \ldots, x_n).$$
Derivation of the algorithm (1)

- We get the approximations $z_k$ by Newton's method, one of the most fundamental methods in computational mathematics.
- Consider the map $F : \mathbb{R}^{n+m+n} \to \mathbb{R}^{n+m+n}$,

$$z = (x, y, s) \mapsto F(z) = (A^T y + s - c, Ax - b, x_1 s_1, \ldots, x_n s_n)$$

satisfying $\{\zeta_\mu\} = F^{-1}(0, 0, \mu e_n)$, where $e_n := (1, \ldots, 1) \in \mathbb{R}^n$. The Jacobian matrix of $F$ at $z$ equals

$$DF(z) = \begin{bmatrix}
0 & A^T & I \\
A & 0 & 0 \\
S & 0 & X
\end{bmatrix},$$

where here and in the following we set

$$S = \text{diag}(s_1, \ldots, s_n), \ X = \text{diag}(x_1, \ldots, x_n).$$

- Fact: $DF(z)$ is invertible if $\text{rank } A = m$ and $s_i x_i \neq 0$ for all $i$. 
Derivation of the algorithm (2)

- Set $\zeta_k = \zeta\mu_k$. Then $F(\zeta_k) = (0, 0, \mu_k e_n)$ for all $k \in \mathbb{N}$. A first order approximation gives

$$F(\zeta_{k+1}) \approx F(\zeta_k) + DF(\zeta_k)(\zeta_{k+1} - \zeta_k).$$

(2)
Derivation of the algorithm (2)

- Set $\zeta_k = \zeta_{\mu_k}$. Then $F(\zeta_k) = (0, 0, \mu_k e_n)$ for all $k \in \mathbb{N}$. A first order approximation gives

$$F(\zeta_{k+1}) \approx F(\zeta_k) + DF(\zeta_k)(\zeta_{k+1} - \zeta_k). \quad (2)$$

- Suppose now that $z_k = (x, y, s) \in F^\circ$ is an approximation of $\zeta_k$. Then $F(z_k) = (0, 0, x_1s_1, \ldots, x_ns_n) = (0, 0, X S e_n)$. We obtain from (2), replacing the unknowns $\zeta_k$ by $z_k$,

$$(0, 0, \mu_{k+1} e_n) = F(\zeta_{k+1}) \approx F(z_k) + DF(z_k)(\zeta_{k+1} - z_k).$$
Derivation of the algorithm (2)

- Set $\zeta_k = \zeta_{\mu_k}$. Then $F(\zeta_k) = (0, 0, \mu_k e_n)$ for all $k \in \mathbb{N}$. A first order approximation gives

$$F(\zeta_{k+1}) \approx F(\zeta_k) + DF(\zeta_k)(\zeta_{k+1} - \zeta_k). \tag{2}$$

- Suppose now that $z_k = (x, y, s) \in F^\circ$ is an approximation of $\zeta_k$. Then $F(z_k) = (0, 0, x_1 s_1, \ldots, x_n s_n) = (0, 0, X S e_n)$. We obtain from (2), replacing the unknowns $\zeta_k$ by $z_k$,

$$(0, 0, \mu_{k+1} e_n) = F(\zeta_{k+1}) \approx F(z_k) + DF(z_k)(\zeta_{k+1} - z_k).$$

- This leads to the following choice of the approximation of $\zeta_{k+1}$.

$$z_{k+1} := z_k + DF(z_k)^{-1}(0, 0, \mu_{k+1} e_n - X S e_n)$$
Derivation of the algorithm (2)

- Set $\zeta_k = \zeta_{\mu_k}$. Then $F(\zeta_k) = (0, 0, \mu_k e_n)$ for all $k \in \mathbb{N}$. A first order approximation gives

$$F(\zeta_{k+1}) \approx F(\zeta_k) + DF(\zeta_k)(\zeta_{k+1} - \zeta_k). \quad (2)$$

- Suppose now that $z_k = (x, y, s) \in F^\circ$ is an approximation of $\zeta_k$. Then $F(z_k) = (0, 0, x_1 s_1, \ldots, x_n s_n) = (0, 0, X S e_n)$. We obtain from (2), replacing the unknowns $\zeta_k$ by $z_k$,

$$(0, 0, \mu_{k+1} e_n) = F(\zeta_{k+1}) \approx F(z_k) + DF(z_k)(\zeta_{k+1} - z_k).$$

- This leads to the following choice of the approximation of $\zeta_{k+1}$.

$$z_{k+1} := z_k + DF(z_k)^{-1}(0, 0, \mu_{k+1} e_n - X S e_n)$$

- One easily checks for $z_{k+1} = z_k + (\Delta x, \Delta y, \Delta s)$

$$A^T(y + \Delta y) + (s + \Delta s) = c, \quad A(x + \Delta x) = b.$$
Primal-dual IPM

We choose \( \sigma := 1 - \frac{1}{4\sqrt{n}} \).

**Algorithm: Primal-Dual IPM**

**Input:** \( A \in \mathbb{R}^{m \times n}, \ b \in \mathbb{R}^m, \ c \in \mathbb{R}^n \) s.t. \( \text{rank } A = m \leq n \).

Choose starting point \( z_0 = (x^0, y^0, s^0) \in \mathcal{F}^\circ \) with duality measure \( \mu_0 \).

**for** \( k = 0, 1, 2, \ldots \)

Solve

\[
\begin{bmatrix}
0 & A^T & I \\
A & 0 & 0 \\
S^k & 0 & X^k
\end{bmatrix}
\begin{bmatrix}
\Delta x^k \\
\Delta y^k \\
\Delta s^k
\end{bmatrix}
= \begin{bmatrix}
0 \\
0 \\
\sigma^{k+1} \mu_0 e_n - X^k S^k e_n
\end{bmatrix},
\]

where \( X^k = \text{diag}(x^k_1, \ldots, x^k_n), \ S^k = \text{diag}(s^k_1, \ldots, s^k_n) \).

Set

\[(x^{k+1}, y^{k+1}, s^{k+1}) = (x^k, y^k, s^k) + (\Delta x^k, \Delta y^k, \Delta s^k).
\]

**until** some stopping criterion is matched.
For the following, see Wright (1997).

**Theorem.**

**Primal-Dual IPM** produces, on a strictly feasible starting point \( z_0 \) on the central path (or close to it), a sequence of iterates \( z_k \in \mathcal{F}^\circ \) such that \( \mu(z_k) = \sigma^k \mu(z_0) \). After

\[
k \geq 4\sqrt{n} \ln \frac{\mu_0}{\varepsilon}.
\]

iterations we have \( \mu(z^k) \leq \varepsilon \).
Condition: The Geometry of Numerical Algorithms

Part II: Linear Inequalities

Condition numbers of linear programming

Condition numbers of linear programming

Jim Renegar, 1995
Linear Programming Feasibility Problem (1)

- We focus on the homogeneous feasibility problem.
Linear Programming Feasibility Problem (1)

- We focus on the homogeneous feasibility problem.
- For $A \in \mathbb{R}^{m \times n}$, $n > m$, consider the system of linear inequalities

$$\exists x \in \mathbb{R}^n \ Ax = 0, \ x > 0.$$  \hfill (P)

and its dual problem

$$\exists y \in \mathbb{R}^m \ A^T y < 0$$  \hfill (D)
Linear Programming Feasibility Problem (1)

- We focus on the **homogeneous feasibility problem**.
- For \( A \in \mathbb{R}^{m \times n}, n > m \), consider the system of linear inequalities
  \[
  \exists x \in \mathbb{R}^n \ Ax = 0, \ x > 0. \quad (P)
  \]
  and its dual problem
  \[
  \exists y \in \mathbb{R}^m \ A^T y < 0 \quad (D)
  \]
- Let \( \mathcal{F}_P \) and \( \mathcal{F}_D \) denote the set of instances where \( P \) and \( D \) are solvable, respectively.
We focus on the homogeneous feasibility problem.

For $A \in \mathbb{R}^{m \times n}$, $n > m$, consider the system of linear inequalities
\[ \exists x \in \mathbb{R}^n \ Ax = 0, \ x > 0. \quad (P) \]
and its dual problem
\[ \exists y \in \mathbb{R}^m \ A^T y < 0 \quad (D) \]

Let $\mathcal{F}_P^\circ$ and $\mathcal{F}_D^\circ$ denote the set of instances where $P$ and $D$ are solvable, respectively.

We have a disjoint union
\[ \mathbb{R}^{n \times m} = \mathcal{F}_P^\circ \cup \mathcal{F}_D^\circ \cup \Sigma, \]
where the set of ill-posed instances $\Sigma$ is the common boundary of $\mathcal{F}_P^\circ$ and $\mathcal{F}_D^\circ$. 
The Homogeneous Linear Programming Feasibility problem (HLPF) is to decide for given $A$, whether $A \in \mathcal{F}_P^0$ or $A \in \mathcal{F}_D^0$. 

\[
\mathbb{R}^{n \times m} = \mathcal{F}_P^0 \cup \mathcal{F}_D^0 \cup \Sigma,
\]
Renegar’s condition number

- For the HLPF problem, J. Renegar defined the condition number of the instance $A \in \mathbb{R}^{m \times n}$ as

$$C_R(A) := \frac{\|A\|}{\text{dist}(A, \Sigma)}.$$
Renegar’s condition number

- For the HLPF problem, J. Renegar defined the condition number of the instance $A \in \mathbb{R}^{m \times n}$ as

$$C_R(A) := \frac{\|A\|}{\text{dist}(A, \Sigma)}.$$

- Note that $C_R(A) = \infty$ iff $A \in \Sigma$. 
For the HLPF problem, J. Renegar defined the condition number of the instance $A \in \mathbb{R}^{m \times n}$ as

$$C_R(A) := \frac{\|A\|}{\text{dist}(A, \Sigma)}.$$ 

Note that $C_R(A) = \infty$ iff $A \in \Sigma$.

HLPF can be solved by solving a related linear programming optimization problem up to a certain accuracy. More specifically,

$$\mu(z_k) = O\left(\frac{1}{n^2 C_R(A)}\right)$$

suffices for the decision $A \in \mathcal{F}_P^o$ or $A \in \mathcal{F}_D^o$ (Renegar, 1995).
Renegar’s condition number

- For the HLPF problem, J. Renegar defined the condition number of the instance $A \in \mathbb{R}^{m \times n}$ as
  \[ C_R(A) := \frac{\|A\|}{\text{dist}(A, \Sigma)}. \]

- Note that $C_R(A) = \infty$ iff $A \in \Sigma$.

- HLPF can be solved by solving a related linear programming optimization problem up to a certain accuracy. More specifically,
  \[ \mu(z_k) = O\left(\frac{1}{n^2C_R(A)}\right) \]
  suffices for the decision $A \in \mathcal{F}_P^\circ$ or $A \in \mathcal{F}_D^\circ$ (Renegar, 1995).

- By the previous analysis
Renegar’s condition number

- For the HLPF problem, J. Renegar defined the condition number of the instance $A \in \mathbb{R}^{m \times n}$ as
\[
C_R(A) := \frac{\|A\|}{\text{dist}(A, \Sigma)}.
\]

- Note that $C_R(A) = \infty$ iff $A \in \Sigma$.
- HLPF can be solved by solving a related linear programming optimization problem up to a certain accuracy. More specifically,
\[
\mu(z_k) = O\left(\frac{1}{n^2 C_R(A)}\right)
\]
suffices for the decision $A \in \mathcal{F}_P^\circ$ or $A \in \mathcal{F}_D^\circ$ (Renegar, 1995).

Primal-Dual IPM can be solved with a number of iterations bounded by
\[
O\left(\sqrt{n \log(nC_R(A))}\right).
\]
Khachian (1979): for an integer matrix $A$, HLPF can be solved in polynomial time (in the bit size of $A$).
Condition-based Complexity Analysis

- Khachian (1979): for an integer matrix $A$, HLPF can be solved in polynomial time (in the bit size of $A$).
- Notorious open problem: can HLPF be solved for real matrix $A$ with a number of arithmetic operations polynomial in $m, n$?
Khachian (1979): for an integer matrix $A$, HLPF can be solved in polynomial time (in the bit size of $A$).

Notorious open problem: can HLPF be solved for real matrix $A$ with a number of arithmetic operations polynomial in $m, n$?

Renegar’s analysis bounds the number of arithmetic operations by a polynomial in both the
  - dimension $n$ of the problem
  - logarithm of its condition number.
Condition-based Complexity Analysis

- Khachian (1979): for an \textbf{integer} matrix $A$, HLPF can be solved in polynomial time (in the bit size of $A$).
- Notorious open problem: can HLPF be solved for \textbf{real} matrix $A$ with a number of arithmetic operations polynomial in $m, n$?
- Renegar’s analysis bounds the number of arithmetic operations by a polynomial in both the
  - \textbf{dimension} $n$ of the problem
  - \textbf{logarithm} of its \textbf{condition number}.
- $\log C_R(A)$ is polynomially bounded in bitsize of $A$ for integer matrices $A \notin \Sigma$. 
Condition-based Complexity Analysis

- Khachian (1979): for an **integer** matrix $A$, HLPF can be solved in polynomial time (in the bit size of $A$).

- Notorious open problem: can HLPF be solved for **real** matrix $A$ with a number of arithmetic operations polynomial in $m, n$?

- Renegar’s analysis bounds the number of arithmetic operations by a polynomial in both the
  - dimension $n$ of the problem
  - logarithm of its condition number.

- $\log C_R(A)$ is polynomially bounded in bitsize of $A$ for integer matrices $A \notin \Sigma$.

- Consequence: HLPF can be solved in polynomial time for an integer matrix $A$, counting bit operations.
Characterization of ill-posedness

Let $A \in \mathbb{R}^{m \times n}$ be of full rank, $n > m$. Denote by $a_1, \ldots, a_n$ the columns of $A$ and $\Delta$ its convex hull.
Characterization of ill-posedness

- Let $A \in \mathbb{R}^{m \times n}$ be of full rank, $n > m$. Denote by $a_1, \ldots, a_n$ the columns of $A$ and $\Delta$ its convex hull.

- Primal feasibility

\[ \exists x \in \mathbb{R}^n \ Ax = 0, \ x > 0 \quad (P) \]

means that $x_1 a_1 + \cdots + x_n a_n = 0$ for some $x_i > 0$, that is, $0 \in \text{int} \Delta$. 

Characterization of ill-posedness

- Let $A \in \mathbb{R}^{m \times n}$ be of full rank, $n > m$. Denote by $a_1, \ldots, a_n$ the columns of $A$ and $\Delta$ its convex hull.

- Primal feasibility
  $$\exists x \in \mathbb{R}^n \; Ax = 0, \; x > 0$$  
  (P)
  means that $x_1 a_1 + \cdots + x_n a_n = 0$ for some $x_i > 0$, that is, $0 \in \text{int} \Delta$.

- Dual feasibility
  $$\exists y \in \mathbb{R}^m \; A^T y < 0$$  
  (D)
  means that $\langle a_i, y \rangle < 0$ for some $y$, that is, $\Delta$ lies in some open halfspace.
Characterization of ill-posedness

- Let $A \in \mathbb{R}^{m \times n}$ be of full rank, $n > m$. Denote by $a_1, \ldots, a_n$ the columns of $A$ and $\Delta$ its convex hull.
- Primal feasibility
  \[
  \exists x \in \mathbb{R}^n \ Ax = 0, x > 0 \quad (P)
  \]
  means that $x_1 a_1 + \cdots + x_n a_n = 0$ for some $x_i > 0$, that is, $0 \in \text{int} \Delta$.
- Dual feasibility
  \[
  \exists y \in \mathbb{R}^m \ A^T y < 0 \quad (D)
  \]
  means that $\langle a_i, y \rangle < 0$ for some $y$, that is, $\Delta$ lies in some open halfspace.
- Recall $\Sigma = \overline{F_P} \cap \overline{F_D}$.
Characterization of ill-posedness

- Let $A \in \mathbb{R}^{m \times n}$ be of full rank, $n > m$. Denote by $a_1, \ldots, a_n$ the columns of $A$ and $\Delta$ its convex hull.

- Primal feasibility
  \[
  \exists x \in \mathbb{R}^n \ Ax = 0, \ x > 0 \quad (P)
  \]
  means that $x_1 a_1 + \cdots + x_n a_n = 0$ for some $x_i > 0$, that is, $0 \in \text{int} \Delta$.

- Dual feasibility
  \[
  \exists y \in \mathbb{R}^m \ A^T y < 0 \quad (D)
  \]
  means that $\langle a_i, y \rangle < 0$ for some $y$, that is, $\Delta$ lies in some open halfspace.

- Recall $\Sigma = \overline{F_P^0} \cap \overline{F_D^0}$.

- Hence $A$ is ill-posed, $A \in \Sigma$, iff $\Delta$ is contained in a closed halfspace and $0 \in \Delta$. 
We are going to define a variant of Renegar’s condition number, that is better suited for probabilistic analysis.
We are going to define a variant of Renegar’s condition number, that is better suited for probabilistic analysis.

Suppose $A \in \mathcal{F}_S^\circ$ for $S \in \{P, D\}$. We define

$$\Delta(A) := \sup \left\{ \delta > 0 \left| \forall A' \in \mathbb{R}^{m \times n} \left( \max_{i \leq n} \frac{\|a'_i - a_i\|}{\|a_i\|} < \delta \Rightarrow A' \in \mathcal{F}_S^\circ \right) \right. \right\},$$

where $a'_i$ stands for the $i$th column of $A'$. 

**GCC condition number (1)**
We are going to define a variant of Renegar’s condition number, that is better suited for probabilistic analysis.

Suppose $A \in \mathcal{F}_S^\circ$ for $S \in \{P, D\}$. We define

$$\Delta(A) := \sup \left\{ \delta > 0 \mid \forall A' \in \mathbb{R}^{m \times n} \left( \max_{i \leq n} \frac{\|a'_i - a_i\|}{\|a_i\|} < \delta \Rightarrow A' \in \mathcal{F}_S^\circ \right) \right\},$$

where $a'_i$ stands for the $i$th column of $A'$.

The GCC-condition number of $A$ is defined as (Goffin (1980), Cheung, Cucker (2001)):

$$\mathcal{C}(A) := 1/\Delta(A).$$
We are going to define a variant of Renegar’s condition number, that is better suited for probabilistic analysis.

Suppose $A \in F^\circ_S$ for $S \in \{P, D\}$. We define

$$\Delta(A) := \sup \left\{ \delta > 0 \left| \forall A' \in \mathbb{R}^{m \times n} \left( \max_{i \leq n} \frac{\|a'_i - a_i\|}{\|a_i\|} < \delta \Rightarrow A' \in F^\circ_S \right) \right\},$$

where $a'_i$ stands for the $i$th column of $A'$.

The GCC-condition number of $A$ is defined as (Goffin (1980), Cheung, Cucker (2001)):

$$C(A) := \frac{1}{\Delta(A)}.$$

Note that we measure the relative size of the perturbation for each column $a_i$ with respect to the norm of $a_i$. 
GCC condition number (1)

- We are going to define a variant of Renegar’s condition number, that is better suited for probabilistic analysis.

- Suppose $A \in F_S^\circ$ for $S \in \{P, D\}$. We define

$$\Delta(A) := \sup \left\{ \delta > 0 \mid \forall A' \in \mathbb{R}^{m \times n} \left( \max_{i \leq n} \frac{\|a'_i - a_i\|}{\|a_i\|} < \delta \Rightarrow A' \in F_S^\circ \right) \right\},$$

where $a'_i$ stands for the $i$th column of $A'$.

- The GCC-condition number of $A$ is defined as (Goffin (1980), Cheung, Cucker (2001)):

$$\mathcal{C}(A) := 1/\Delta(A).$$

- Note that we measure the relative size of the perturbation for each column $a_i$ with respect to the norm of $a_i$.

- Also, $\Delta(A)$ is scale invariant. We may therefore assume, without loss of generality, that $\|a_i\| = 1$ for all $i$. 
GCC condition number (1)

- We are going to define a variant of Renegar’s condition number, that is better suited for probabilistic analysis.
- Suppose $A \in F^o_S$ for $S \in \{P, D\}$. We define

$$\Delta(A) := \sup \left\{ \delta > 0 \mid \forall A' \in \mathbb{R}^{m \times n} \left( \max_{i \leq n} \frac{\|a'_i - a_i\|}{\|a_i\|} < \delta \Rightarrow A' \in F^o_S \right) \right\},$$

where $a'_i$ stands for the $i$th column of $A'$.
- The GCC-condition number of $A$ is defined as (Goffin (1980), Cheung, Cucker (2001)):

$$\mathcal{C}(A) := 1/\Delta(A).$$

- Note that we measure the relative size of the perturbation for each column $a_i$ with respect to the norm of $a_i$.
- Also, $\Delta(A)$ is scale invariant. We may therefore assume, without loss of generality, that $\|a_i\| = 1$ for all $i$.
- Hence we can interpret $A$ with columns $a_1, \ldots, a_n$ as an element in the product $\mathbb{S}^n = \mathbb{S} \times \cdots \times \mathbb{S}$ of spheres $\mathbb{S} := \mathbb{S}^{m-1}$. 

---

Condition: The Geometry of Numerical Algorithms

Part II: Linear Inequalities

Condition numbers of linear programming
GCC condition number (2)

Let $d$ denote angular distance on $\mathbb{S}$. Define a metric on $\mathbb{S}^n$ by

$$d_{\mathbb{S}}(A, B) := \max_{1 \leq i \leq n} d(a_i, b_i).$$
Let $d$ denote angular distance on $S$. Define a metric on $S^n$ by

$$d_S(A, B) := \max_{1 \leq i \leq n} d(a_i, b_i).$$

It is straightforward to show

$$C(A) = \frac{1}{\sin d_S(A, \Sigma)}.$$
GCC condition number (2)

- Let \( d \) denote angular distance on \( \mathbb{S} \). Define a metric on \( \mathbb{S}^n \) by

\[
d_{\mathbb{S}}(A, B) := \max_{1 \leq i \leq n} d(a_i, b_i).
\]

- It is straightforward to show

\[
\mathcal{C}(A) = \frac{1}{\sin d_{\mathbb{S}}(A, \Sigma)}.
\]

- We note that HLPF can be solved by a primal-dual interior-point method with a number of iterations

\[
O\left(\sqrt{n} \log(n \mathcal{C}(A))\right).
\]
Minimal spherical caps

- Let $\rho(A)$ be the angular radius of a spherical cap of minimal radius containing $a_1, \ldots, a_n \in S$. 
Minimal spherical caps

- Let $\rho(A)$ be the angular radius of a spherical cap of minimal radius containing $a_1, \ldots, a_n \in \mathbb{S}$.
- Easy to see: $\rho(A) < \frac{\pi}{2}$ iff $A \in F_D^0$. Hence, $\rho(A) = \frac{\pi}{2}$ iff $A \in \Sigma$. 
Minimal spherical caps

- Let $\rho(A)$ be the angular radius of a spherical cap of minimal radius containing $a_1, \ldots, a_n \in \mathbb{S}$.
- Easy to see: $\rho(A) < \frac{\pi}{2}$ iff $A \in \mathcal{F}_D^o$. Hence, $\rho(A) = \frac{\pi}{2}$ iff $A \in \Sigma$.

- In particular, $d_\mathbb{S}(A, \Sigma) \leq \frac{\pi}{2}$ and

$$\mathcal{C}(A)^{-1} = \sin d_\mathbb{S}(A, \Sigma) = |\cos \rho(A)|.$$
Minimal spherical caps

- Let $\rho(A)$ be the angular radius of a spherical cap of minimal radius containing $a_1, \ldots, a_n \in S$.
- Easy to see: $\rho(A) < \frac{\pi}{2}$ iff $A \in F_D^\circ$. Hence, $\rho(A) = \frac{\pi}{2}$ iff $A \in \Sigma$.

**Cheung & Cucker (2001)**

$$d_S(A, \Sigma) = \begin{cases} \frac{\pi}{2} - \rho(A) & \text{if } A \in F_D^\circ \\ \rho(A) - \frac{\pi}{2} & \text{if } A \in S^n \setminus F_D^\circ \end{cases}.$$  

- In particular, $d_S(A, \Sigma) \leq \frac{\pi}{2}$ and

$$\mathcal{C}(A)^{-1} = \sin d_S(A, \Sigma) = |\cos \rho(A)|.$$
Average Analysis of GCC condition number
Suppose \( A \in \mathbb{R}^{n \times m} \) is standard Gaussian.
GCC condition number and coverage processes (1)

- Suppose $A \in \mathbb{R}^{n \times m}$ is standard Gaussian.
- After normalization, this means that each column $a_i$ is independently chosen from the uniform distribution on the sphere $S$. 
GCC condition number and coverage processes (1)

- Suppose $A \in \mathbb{R}^{n \times m}$ is standard Gaussian.
- After normalization, this means that each column $a_i$ is independently chosen from the uniform distribution on the sphere $S$.
- The probability distribution of $\mathcal{C}(A)$ is related to a classical question on covering a sphere by random spherical caps.
Suppose $A \in \mathbb{R}^{n \times m}$ is standard Gaussian.

After normalization, this means that each column $a_i$ is independently chosen from the uniform distribution on the sphere $S$.

The probability distribution of $\mathcal{C}(A)$ is related to a classical question on covering a sphere by random spherical caps.

Let $p(n, m, \alpha)$ denote the probability that randomly chosen spherical caps with centers $a_1, \ldots, a_n$ and angular radius $\alpha$ do not cover the sphere $S = S^{m-1}$. 

GCC condition number and coverage processes (1)

- Suppose $A \in \mathbb{R}^{n \times m}$ is standard Gaussian.
- After normalization, this means that each column $a_i$ is independently chosen from the uniform distribution on the sphere $S$.
- The probability distribution of $C(A)$ is related to a classical question on covering a sphere by random spherical caps.
- Let $p(n, m, \alpha)$ denote the probability that randomly chosen spherical caps with centers $a_1, \ldots, a_n$ and angular radius $\alpha$ do not cover the sphere $S = S^{m-1}$.
- We claim that

$$p(n, m, \alpha) = \text{Prob} \{ \rho(A) \leq \pi - \alpha \}.$$
GCC condition number and coverage processes (2)

- **Claim:** $p(n, m, \alpha) = \text{Prob} \{ \rho(A) \leq \pi - \alpha \}$. 
Claim: $p(n, m, \alpha) = \text{Prob} \{ \rho(A) \leq \pi - \alpha \}$.

Proof. The caps of radius $\alpha$ with center $a_1, \ldots, a_n$ do not cover $S$ iff there exists $y \in S$ having distance greater than $\alpha$ from all $a_i$. 
Claim: $p(n, m, \alpha) = \text{Prob} \{ \rho(A) \leq \pi - \alpha \}$.

Proof. The caps of radius $\alpha$ with center $a_1, \ldots, a_n$ do not cover $S$ iff there exists $y \in S$ having distance greater than $\alpha$ from all $a_i$.

This means that the cap of radius $\pi - \alpha$ centered at $-y$ contains all the $a_i$. Hence

$$p(n, m, \alpha) = \text{Prob} \{ \rho(A) \leq \pi - \alpha \}.$$
Average analysis of $C$

- The problem to determine the coverage probabilities $p(n, m, \alpha)$ is classical and completely solved only for $m - 1 = \dim S \leq 2$ (Gilbert (1965), Miles (1969)).
Average analysis of $C$

- The problem to determine the coverage probabilities $p(n, m, \alpha)$ is classical and completely solved only for $m - 1 = \dim \mathcal{S} \leq 2$ (Gilbert (1965), Miles (1969)).

- For $m > 3$ little was known except, Wendel (1962),

$$p(n, m, \pi/2) = \frac{1}{2^{n-1}} \sum_{k=0}^{m-1} \binom{n-1}{k}$$

and asymptotic formulas for $p(n, m, \alpha)$ for $\alpha \to 0$, Janson (1986).
Average analysis of $C$

- The problem to determine the coverage probabilities $p(n, m, \alpha)$ is classical and completely solved only for $m - 1 = \dim S \leq 2$ (Gilbert (1965), Miles (1969)).
- For $m > 3$ little was known except, Wendel (1962),
  
  $$p(n, m, \pi/2) = \frac{1}{2^{n-1}} \sum_{k=0}^{m-1} \binom{n-1}{k}$$

  and asymptotic formulas for $p(n, m, \alpha)$ for $\alpha \to 0$, Janson (1986).
- B, Cucker, Lotz (2010) discovered a closed formula for $p(n, m, \alpha)$ in the case $\alpha \geq \pi/2$
  and an upper bound for $p(n, m, \alpha)$ in the case $\alpha \leq \pi/2$. 

This implies $E(\ln C(A)) \lesssim 2 \ln m + 3$. 

Consequence: the expected number of iterations of interior point methods for HLPF is $O(p_n \log n)$.
The problem to determine the coverage probabilities $p(n, m, \alpha)$ is classical and completely solved only for $m - 1 = \dim \mathbb{S} \leq 2$ (Gilbert (1965), Miles (1969)).

For $m > 3$ little was known except, Wendel (1962),

$$p(n, m, \pi/2) = \frac{1}{2n-1} \sum_{k=0}^{m-1} \binom{n-1}{k}$$

and asymptotic formulas for $p(n, m, \alpha)$ for $\alpha \to 0$, Janson (1986).

B, Cucker, Lotz (2010) discovered a closed formula for $p(n, m, \alpha)$ in the case $\alpha \geq \pi/2$

and an upper bound for $p(n, m, \alpha)$ in the case $\alpha \leq \pi/2$.

This implies

$$\mathbb{E}(\ln C(A)) \leq 2 \ln m + 3.31.$$
Average analysis of $\mathcal{C}$

- The problem to determine the coverage probabilities $p(n, m, \alpha)$ is classical and completely solved only for $m - 1 = \dim \mathcal{S} \leq 2$ (Gilbert (1965), Miles (1969)).
- For $m > 3$ little was known except, Wendel (1962),

$$p(n, m, \pi/2) = \frac{1}{2^{n-1}} \sum_{k=0}^{m-1} \binom{n-1}{k}$$

and asymptotic formulas for $p(n, m, \alpha)$ for $\alpha \to 0$, Janson (1986).
- B, Cucker, Lotz (2010) discovered a closed formula for $p(n, m, \alpha)$ in the case $\alpha \geq \pi/2$
and an upper bound for $p(n, m, \alpha)$ in the case $\alpha \leq \pi/2$.
- This implies

$$\mathbb{E}(\ln \mathcal{C}(A)) \leq 2 \ln m + 3.31.$$
- Consequence: the expected number of iterations of interior point methods for HLPF is $\mathcal{O}(\sqrt{n} \log n)$. 
Closed formula for $p(n, m, \alpha)$

For $\alpha \geq \pi/2$, setting $\varepsilon := |\cos(\alpha)|$,

$$p(n, m+1, \alpha) = \sum_{k=1}^{m} \binom{n}{k + 1} C(m, k) \int_{\varepsilon}^{1} t^{m-k} (1-t^2)^{\frac{1}{2} km-1} \lambda_m(t)^{n-k-1} dt.$$ 

Here, $\lambda_m(t)$ denotes the relative volume of a spherical cap of radius $\arccos t \in [0, \pi/2]$ in $S^m$ and the constants $C(m, k)$ describe higher moments of the volume of certain random simplices.
Closed formula for \( p(n, m, \alpha) \)

- For \( \alpha \geq \pi/2 \), setting \( \varepsilon := |\cos(\alpha)| \),

\[
p(n, m+1, \alpha) = \sum_{k=1}^{m} \binom{n}{k+1} C(m, k) \int_{\varepsilon}^{1} t^{m-k} (1-t^2)^{\frac{1}{2} km-1} \lambda_m(t)^{n-k-1} \, dt.
\]

Here, \( \lambda_m(t) \) denotes the relative volume of a spherical cap of radius \( \arccos t \in [0, \pi/2] \) in \( S^m \) and the constants \( C(m, k) \) describe higher moments of the volume of certain random simplices.

- Let \( O_m \) denote the \( m \)-dimensional volume of the sphere \( S^m \).

\[
\frac{\text{vol}(\Sigma) \cdot \varepsilon}{\text{vol}(S)^n} + o(\varepsilon^2) = \\
= \text{Prob} \left\{ A \in F_D^0, \ C(A)^{-1} \leq \varepsilon \right\} = p(n, m, \pi/2) - p(n, m, \alpha) \\
= \binom{n}{m+1} (m+1) \frac{O_{m-1}}{O_m} \frac{1}{2^{n-2}} \varepsilon + o(\varepsilon^2).
\]
Smoothed Analysis of GCC condition number
Gaussian smoothed analysis

▶ Model for local perturbations: $\overline{A} \in \mathbb{R}^{m \times n}$, Gaussians $A \in \mathbb{R}^{m \times n}$. 
Gaussian smoothed analysis

- Model for local perturbations: $\tilde{A} \in \mathbb{R}^{m \times n}$, Gaussians $A \in \mathbb{R}^{m \times n}$. 
Gaussian smoothed analysis

- Model for local perturbations: $\overline{A} \in \mathbb{R}^{m \times n}$, Gaussians $A \in \mathbb{R}^{m \times n}$.

Dunagan, Spielman, Teng (2011)

$$\sup_{||A||=1} \mathbb{E}_{A \sim N(\overline{A}, \sigma^2 I)} \left( \ln \mathcal{C}_R(A) \right) = \mathcal{O} \left( \ln \frac{n}{\sigma} \right).$$
Gaussian smoothed analysis

- Model for local perturbations: \( \widetilde{A} \in \mathbb{R}^{m \times n} \), Gaussians \( A \in \mathbb{R}^{m \times n} \).

Dunagan, Spielman, Teng (2011)

\[
\sup_{\|\widetilde{A}\|=1} \mathbb{E}_{A \sim N(\widetilde{A}, \sigma^2 I)} \left( \ln C_R(A) \right) = \mathcal{O} \left( \ln \frac{n}{\sigma} \right).
\]

- This implies the bound \( \mathcal{O}(\sqrt{n \log \frac{n}{\sigma}}) \) on the smoothed expected number of iterations of the IPM considered for HLPF. Excellent result!
Uniform smoothed analysis of $C$

- Model for smoothed analysis on product of spheres: $\vec{a}_1, \ldots, \vec{a}_n \in S$, independently choose $a_i$ uniformly at random in spherical cap $B(\bar{a}_i, \sigma)$ of $S$ centered at $\bar{a}_i$ with angular radius $\text{arcsin} \sigma$. That is, choose $A \in B(\bar{A}, \sigma) := \prod_i B(\bar{a}_i, \sigma)$ uniformly.
Uniform smoothed analysis of $C$

- Model for smoothed analysis on product of spheres: $\bar{a}_1, \ldots, \bar{a}_n \in S$, independently choose $a_i$ uniformly at random in spherical cap $B(\bar{a}_i, \sigma)$ of $S$ centered at $\bar{a}_i$ with angular radius $\arcsin \sigma$. That is, choose $A \in B(\bar{A}, \sigma) := \prod_i B(\bar{a}_i, \sigma)$ uniformly.

- Amelunxen and B (2012): For $0 < \varepsilon \leq \sigma/(2m(m+1))$

$$\sup_{A \in S^n} \operatorname{Prob}_{A \in B(\bar{A}, \sigma)} \{ A \in F^0_D, C(A) \geq \varepsilon^{-1} \} \leq 6.5 nm^2 \frac{\varepsilon}{\sigma}.$$
Uniform smoothed analysis of $\mathcal{C}$

- Model for smoothed analysis on product of spheres: $\bar{a}_1, \ldots, \bar{a}_n \in S$, independently choose $a_i$ uniformly at random in spherical cap $B(\bar{a}_i, \sigma)$ of $S$ centered at $\bar{a}_i$ with angular radius $\arcsin \sigma$. That is, choose $A \in B(\bar{A}, \sigma) := \prod_i B(\bar{a}_i, \sigma)$ uniformly.

- Amelunxen and B (2012): For $0 < \varepsilon \leq \sigma/(2m(m+1))$

$$\sup_{\bar{A} \in \mathbb{S}^n} \text{Prob}_{A \in B(\bar{A}, \sigma)} \{ A \in \mathcal{F}_D^\circ, \mathcal{C}(A) \geq \varepsilon^{-1} \} \leq 6.5 \, n \, m^2 \frac{\varepsilon}{\sigma}. $$

- For the infeasible case ($A \not\in \mathcal{F}_P^\circ$) a slightly worse tail estimate is obtained. Moreover,

$$\sup_{\bar{A} \in \mathbb{S}^n} \mathbb{E}_{A \in B(\bar{A}, \sigma)} (\ln \mathcal{C}(A)) = \mathcal{O}(\ln \frac{n}{\sigma}).$$
Uniform smoothed analysis of $C$

- Model for smoothed analysis on product of spheres: $\bar{a}_1, \ldots, \bar{a}_n \in S$, independently choose $a_i$ uniformly at random in spherical cap $B(\bar{a}_i, \sigma)$ of $S$ centered at $\bar{a}_i$ with angular radius $\arcsin \sigma$. That is, choose $A \in B(\bar{A}, \sigma) := \prod_i B(\bar{a}_i, \sigma)$ uniformly.

- Amelunxen and B (2012): For $0 < \varepsilon \leq \sigma/(2m(m + 1))$
  \[
  \sup_{\bar{A} \in S^n} \text{Prob}_{A \in B(\bar{A}, \sigma)} \{ A \in F_D, \ C(A) \geq \varepsilon^{-1} \} \leq 6.5n^2 \frac{\varepsilon}{\sigma}.
  \]

- For the infeasible case ($A \not\in F_D$) a slightly worse tail estimate is obtained. Moreover,
  \[
  \sup_{\bar{A} \in S^n} \mathbb{E}_{A \in B(\bar{A}, \sigma)} \left( \ln C(A) \right) = \mathcal{O} \left( \ln \frac{n}{\sigma} \right).
  \]

- We even obtain robustness results.
Sketch of proof (1)

- By a **convex body** $K$ in the sphere $S$ we understand the intersection with $S$ of a closed regular convex cone $C$ in $\mathbb{R}^m$. 
Sketch of proof (1)

- By a **convex body** $K$ in the sphere $S$ we understand the intersection with $S$ of a closed regular convex cone $C$ in $\mathbb{R}^m$.
- We call $T_o(\partial K, \varepsilon) := T(\partial K, \varepsilon) \setminus K$ the **outer $\varepsilon$-neighborhood** of the boundary $\partial K$. Then

\[
\frac{\text{vol}(T_o(\partial K, \varepsilon) \cap B(\overline{a}, \sigma))}{\text{vol}B(\overline{a}, \sigma)} \leq 6.5 \frac{m}{\sigma} \varepsilon \quad \text{if } \varepsilon \leq \frac{\sigma}{2m},
\]

and the same upper bound holds for the relative volume of the inner $\varepsilon$-neighborhood of $\partial K$. 

Sketch of proof (1)

- By a **convex body** $K$ in the sphere $S$ we understand the intersection with $S$ of a closed regular convex cone $C$ in $\mathbb{R}^m$.
- We call $T_o(\partial K, \varepsilon) := T(\partial K, \varepsilon) \setminus K$ the **outer $\varepsilon$-neighborhood** of the boundary $\partial K$. Then
  \[
  \frac{\text{vol}(T_o(\partial K, \varepsilon) \cap B(\bar{a}, \sigma))}{\text{vol}B(\bar{a}, \sigma)} \leq 6.5 \frac{m}{\sigma} \frac{\varepsilon}{\sigma^2} \quad \text{if} \quad \varepsilon \leq \frac{\sigma}{2m}, \quad (*)
  \]
  and the same upper bound holds for the relative volume of the inner $\varepsilon$-neighborhood of $\partial K$.
- The proof idea is similar to the previously mentioned (volume of tubes, integral geometry, counting argument).
Sketch of proof (1)

- By a convex body $K$ in the sphere $S$ we understand the intersection with $S$ of a closed regular convex cone $C$ in $\mathbb{R}^m$.
- We call $T_o(\partial K, \varepsilon) := T(\partial K, \varepsilon) \setminus K$ the outer $\varepsilon$-neighborhood of the boundary $\partial K$. Then
  \[
  \frac{\text{vol}(T_o(\partial K, \varepsilon) \cap B(\bar{a}, \sigma))}{\text{vol}B(\bar{a}, \sigma)} \leq 6.5 \frac{m \varepsilon}{\sigma} \quad \text{if } \varepsilon \leq \frac{\sigma}{2m}, \quad (*)
  \]
  and the same upper bound holds for the relative volume of the inner $\varepsilon$-neighborhood of $\partial K$.
- The proof idea is similar to the previously mentioned (volume of tubes, integral geometry, counting argument).
- In particular, Poincaré’s formula implies
  \[
  \frac{\text{vol}(\partial K)}{\text{vol}(S')} \leq 1.
  \]
  Indeed, by convexity, the intersection of $\partial K$ with a hyperequator $S'$ of $S$ in general position consists of at most two points.
Sketch of proof (2)

**Crucial Lemma.** Let $A = (a_1, \ldots, a_n) \in \mathcal{F}_D^\circ$ and $\mathcal{C}(A) \geq m\varepsilon^{-1}$. Then there exists $i \in \{1, \ldots, n\}$ such that $a_i \in T_o(\partial K_i, \varepsilon)$, where $-K_i$ is the spherical convex hull of $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$. 

Note that $B(A, \varepsilon) = B(A_0, \varepsilon) \times B(a_n, \varepsilon)$ where $A_0 := (a_1, \ldots, a_{n-1})$. 

We bound the probability on the right-hand side for $i = n$ by an integral of probabilities conditioned on $A_0 := (a_1, \ldots, a_{n-1})$:

$$
\Pr\left\{ A_0 \in \mathcal{F}_D^\circ \right\} \Pr\left\{ a_n \in T_o(\partial K_n, \varepsilon) \mid A_0 \right\} = \frac{1}{\text{vol} B(A_0, \varepsilon)} \int_{A_0 \in \mathcal{F}_D^\circ} \Pr\left\{ a_n \in T_o(\partial K_n, \varepsilon) \mid A_0 \right\} \, dA_0.
$$
Sketch of proof (2)

- **Crucial Lemma.** Let $A = (a_1, \ldots, a_n) \in F_D^\circ$ and $\mathcal{C}(A) \geq m\varepsilon^{-1}$. Then there exists $i \in \{1, \ldots, n\}$ such that $a_i \in T_o(\partial K_i, \varepsilon)$, where $-K_i$ is the spherical convex hull of $a_1, \ldots, a_i-1, a_{i+1}, \ldots, a_n$.

- The Lemma yields with $t = m/\varepsilon$

$$\Pr\{A \in F_D^\circ, \mathcal{C}(A) \geq t\} \leq \sum_{i=1}^{n} \Pr\{A \in F_D^\circ, a_i \in T_o(\partial K_i, \varepsilon)\}.$$ 

Note that $B(\overline{A}, \sigma) = B(\overline{A'}, \sigma) \times B(\overline{a_n}, \sigma)$ where $\overline{A'} := (\overline{a_1}, \ldots, \overline{a_{n-1}})$. 


Sketch of proof (2)

**Crucial Lemma.** Let \( A = (a_1, \ldots, a_n) \in \mathcal{F}_D^o \) and \( \mathcal{C}(A) \geq m\varepsilon^{-1} \).

Then there exists \( i \in \{1, \ldots, n\} \) such that \( a_i \in \mathcal{T}_o(\partial K_i, \varepsilon) \), where \(-K_i\) is the spherical convex hull of \( a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\).

The Lemma yields with \( t = m/\varepsilon \)

\[
\text{Prob}\{ A \in \mathcal{F}_D^o, \mathcal{C}(A) \geq t \} \leq \sum_{i=1}^{n} \text{Prob}\{ A \in \mathcal{F}_D^o, a_i \in \mathcal{T}_o(\partial K_i, \varepsilon) \}.
\]

Note that \( B(\overline{A}, \sigma) = B(\overline{A}', \sigma) \times B(\overline{a}_n, \sigma) \) where \( \overline{A} := (\overline{a}_1, \ldots, \overline{a}_{n-1})\).

We bound the probability on the right-hand side for \( i = n \) by an integral of probabilities conditioned on \( A' := (a_1, \ldots, a_{n-1}) \):

\[
\text{Prob}\{ A' \in \mathcal{F}_D^o \text{ and } a_n \in \mathcal{T}_o(\partial K_n, \varepsilon) \} = \frac{1}{\text{vol} B(\overline{A}', \sigma)} \int_{A' \in \mathcal{F}_D^o \cap B(\overline{A}', \sigma)} \text{Prob}\{ a_n \in \mathcal{T}_o(\partial K_n, \varepsilon) \mid A' \} dA'.
\]
Sketch of proof (3)

Fix now $A' \in \mathcal{F}_{n-1,m}$ and consider the convex set $K_n$ in $\mathbb{S}$. The volume bound (*) yields

$$\text{Prob}\{a_n \in T_o(\partial K_n, \varepsilon) \mid A'\} = \frac{\text{vol}(T_o(\partial K_n, \varepsilon) \cap B(\bar{a}_n, \sigma))}{\text{vol}B(\bar{a}_n, \sigma)} \leq 6.5 \frac{m \varepsilon}{\sigma}.$$  

We conclude that

$$\text{Prob}\{A \in \mathcal{F}_D^o, a_n \in T_o(\partial K_n, \phi)\} \leq 6.5 \frac{m \varepsilon}{\sigma}.$$
Sketch of proof (3)

- Fix now $A' \in \mathcal{F}_{n-1,m}$ and consider the convex set $K_n$ in $\mathbb{S}$. The volume bound (*) yields

$$\text{Prob}\{a_n \in T_o(\partial K_n, \varepsilon) \mid A'\} = \frac{\text{vol}(T_o(\partial K_n, \varepsilon) \cap B(\bar{a}_n, \sigma))}{\text{vol}B(\bar{a}_n, \sigma)} \leq 6.5 \frac{m \varepsilon}{\sigma}.$$  

We conclude that

$$\text{Prob}\{A \in \mathcal{F}_D^\circ, a_n \in T_o(\partial K_n, \phi)\} \leq 6.5 \frac{m \varepsilon}{\sigma}.$$  

- The same upper bound holds for any $K_i$. Altogether, we obtain

$$\text{Prob}\{A \in \mathcal{F}_D^\circ \text{ and } \mathcal{C}(A) \geq t\} \leq 6.5 nm^2 \frac{1}{\sigma t},$$

\[ \square \]
Condition Numbers of Convex Optimization
Convex homogeneous feasibility problem

- Much of what has been said for linear optimization can be generalized to convex optimization.
Convex homogeneous feasibility problem

- Much of what has been said for linear optimization can be generalized to convex optimization.
- Fix a closed regular convex cone $C \subseteq \mathbb{R}^n$ with dual cone

$$\tilde{C} := \{y \in \mathbb{R}^n \mid \forall x \in C : \langle y, x \rangle \geq 0\}$$
Convex homogeneous feasibility problem

- Much of what has been said for linear optimization can be generalized to convex optimization.
- Fix a closed regular convex cone $C \subseteq \mathbb{R}^n$ with dual cone $\tilde{C} := \{y \in \mathbb{R}^n \mid \forall x \in C : \langle y, x \rangle \geq 0\}$

Homogeneous convex feasibility problem (HCFP)

Input $A \in \mathbb{R}^{m \times n}$ ($n > m$)

Decide the alternative

$$\exists x \in \mathbb{R}^n \setminus \{0\} : Ax = 0, x \in \tilde{C} \quad \text{ (P)}$$

$$\exists y \in \mathbb{R}^m \setminus \{0\} : A^Ty \in C \quad \text{ (D)}$$
Convex homogeneous feasibility problem

- Most important cases:

  **Linear Programming** : \( C = \mathbb{R}_+^n = \mathbb{R}_+ \times \ldots \times \mathbb{R}_+ \)

  **Semidefinite Programming** : \( C = \{ M \in \mathbb{R}^{\ell \times \ell} \mid M \text{ is pos. semidef.} \} \)
Convex homogeneous feasibility problem

- Most important cases:
  
  **Linear Programming** : \( C = \mathbb{R}_{+}^{n} = \mathbb{R}_{+} \times \ldots \times \mathbb{R}_{+} \)

  **Semidefinite Programming** : \( C = \{ M \in \mathbb{R}^{\ell \times \ell}, \ M \text{ is pos. semidef.} \} \)

- Define

  \[ F_{P} := \{ A \mid (P) \text{ is feasible} \}, \]

  \[ F_{D} := \{ A \mid (D) \text{ is feasible} \}, \]

  \[ \Sigma := F_{P} \cap F_{D}. \]
Convex homogeneous feasibility problem

- Most important cases:
  
  **Linear Programming** : \( C = \mathbb{R}^n_+ = \mathbb{R}_+ \times \ldots \times \mathbb{R}_+ \)
  
  **Semidefinite Programming** : \( C = \{ M \in \mathbb{R}^{\ell \times \ell} : M \text{ is pos. semidef.} \} \)

- Define
  
  \[ F_P := \{ A \mid (P) \text{ is feasible} \}, \]
  
  \[ F_D := \{ A \mid (D) \text{ is feasible} \}, \]
  
  \[ \Sigma := F_P \cap F_D. \]

- Renegar’s condition number is defined as:
  
  \[ CR(A) := \frac{\|A\|}{\text{dist}(A, \Sigma)}. \]
Convex homogeneous feasibility problem

- The probabilistic analyses for LP-condition numbers rely on the product structure of the cone $C = \mathbb{R}_+^n = \mathbb{R}_+ \times \ldots \times \mathbb{R}_+$. 
Convex homogeneous feasibility problem

- The probabilistic analyses for LP-condition numbers rely on the product structure of the cone $C = \mathbb{R}_+^n = \mathbb{R}_+ \times \ldots \times \mathbb{R}_+$.
- For general cones (like SDP), we look for a different, more coordinate-free approach.
Convex homogeneous feasibility problem

- The probabilistic analyses for LP-condition numbers rely on the product structure of the cone $C = \mathbb{R}_+^n = \mathbb{R}_+ \times \ldots \times \mathbb{R}_+$.
- For general cones (like SDP), we look for a different, more coordinate-free approach.
- Suppose $A \in \mathbb{R}^{m \times n}$ has rank $m$. Consider the $m$-dimensional linear subspace $W := \text{im} A^T$ of $\mathbb{R}^n$.

\[
\exists x \in \mathbb{R}^n \setminus \{0\} : \quad Ax = 0 \quad (P) \quad \exists y \in \mathbb{R}^m \setminus \{0\} : \quad A^T y \in C \quad (D)
\]

\[
\iff \quad \ker A \cap \tilde{C} \neq \{0\} \quad \iff \quad \text{im} A^T \cap C \neq \{0\}
\]

\[
= W^\perp \quad =: W
\]
Grassmann condition number (1)

Consider the inputs as an element of the Grassmann manifold

\[ W \in \mathcal{G}_{n,m} := \{ W \subseteq \mathbb{R}^n \mid \text{lin. subspace} \, , \, \dim W = m \}. \]

We have to decide the alternative

\[ W^\perp \cap \check{C} \neq \{0\} \quad \text{(P)} \quad \text{or} \quad W \cap C \neq \{0\} \quad \text{(D)} \]
Grassmann condition number (1)

- Consider the inputs as an element of the Grassmann manifold

\[ W \in \mathbb{G}_{n,m} := \{ W \subseteq \mathbb{R}^n \mid W \text{ lin. subspace, dim } W = m \}. \]

We have to decide the alternative

\[ W^\perp \cap \mathcal{C} \neq \{0\} \quad \text{(P)} \quad \text{or} \quad W \cap \mathcal{C} \neq \{0\} \quad \text{(D)} \]

- Define

\[ \mathcal{F}_P := \{ W \in \mathbb{G}_{n,m} \mid W^\perp \cap \mathcal{C} \neq \{0\} \} \quad \text{(primal feasible)} \]

\[ \mathcal{F}_D := \{ W \in \mathbb{G}_{n,m} \mid W \cap \mathcal{C} \neq \{0\} \} \quad \text{(dual feasible)} \]

\[ \Sigma_G := \mathcal{F}_P \cap \mathcal{F}_D \quad \text{(ill-posed)} \]
Grassmann condition number (1)

➤ Consider the inputs as an element of the Grassmann manifold

\[
\mathcal{W} \in \mathbb{G}_{n,m} := \{ \mathcal{W} \subseteq \mathbb{R}^n \mid \text{lin. subspace, dim } \mathcal{W} = m \}.
\]

We have to decide the alternative

\[
\mathcal{W}^\perp \cap \tilde{C} \neq \{0\} \quad \text{(P)} \quad \text{or} \quad \mathcal{W} \cap C \neq \{0\} \quad \text{(D)}
\]

➤ Define

\[
\mathcal{F}_P := \{ \mathcal{W} \in \mathbb{G}_{n,m} \mid \mathcal{W}^\perp \cap \tilde{C} \neq \{0\} \} \quad \text{(primal feasible)}
\]

\[
\mathcal{F}_D := \{ \mathcal{W} \in \mathbb{G}_{n,m} \mid \mathcal{W} \cap C \neq \{0\} \} \quad \text{(dual feasible)}
\]

\[
\Sigma_G := \mathcal{F}_P \cap \mathcal{F}_D \quad \text{(ill-posed)}
\]

➤ \( \mathbb{G}_{n,m} \) is a compact Riemannian manifold. We have thus well-defined notions of (geodesic) distance (“angle”) and volume.
Grassmann condition number (2)

- We define the **Grassmann condition number** for $W \in \mathbb{G}_{n,m}$ as

$$C_G(W) := \frac{1}{\sin d(W, \Sigma_G)},$$

where $d$ denotes the geodesic distance in $\mathbb{G}_{n,m}$. 
Grassmann condition number (2)

- We define the Grassmann condition number for $\mathcal{W} \in \mathbb{G}_{n,m}$ as

$$C_G(\mathcal{W}) := \frac{1}{\sin d(\mathcal{W}, \Sigma_G)},$$

where $d$ denotes the geodesic distance in $\mathbb{G}_{n,m}$.

- The following result (Amelunxen (2011), Belloni, Freund (2009)) separates Renegar's condition number into an “intrinsic” and “extrinsic” part.
Grassmann condition number (2)

- We define the Grassmann condition number for $W \in \mathbb{G}_{n,m}$ as
  $$C_G(W) := \frac{1}{\sin d(W, \Sigma_G)},$$
  where $d$ denotes the geodesic distance in $\mathbb{G}_{n,m}$.

- The following result (Amelunxen (2011), Belloni, Freund (2009)) separates Renegar’s condition number into an “intrinsic” and “extrinsic” part.

  For $A \in \mathbb{R}^{m \times n}$ of rank $m$ and $W := \text{im} A^T$ we have
  $$C_G(A) \leq C_R(A) \leq \kappa(A) \cdot C_G(A).$$
Average analysis of Grassmann condition number

- Fix any closed regular convex cone $C \subset \mathbb{R}^n$. 
Average analysis of Grassmann condition number

- Fix any closed regular convex cone $C \subset \mathbb{R}^n$.
- If $A \in \mathbb{R}^{m \times n}$ is standard Gaussian, then $W := \text{im}A^T$ is uniformly distributed in $\mathcal{G}_{n,m}$ (w.r.t. orthogonal invariant volume form).
Average analysis of Grassmann condition number

- Fix any closed regular convex cone $C \subset \mathbb{R}^n$.
- If $A \in \mathbb{R}^{m \times n}$ is standard Gaussian, then $W := \text{im} A^T$ is uniformly distributed in $G_{n,m}$ (w.r.t. orthogonal invariant volume form).
- With the volume of tube interpretation and some differential geometry, one can show:
Fix any closed regular convex cone $C \subset \mathbb{R}^n$.

If $A \in \mathbb{R}^{m \times n}$ is standard Gaussian, then $W := \text{im} A^T$ is uniformly distributed in $\mathcal{G}_{n,m}$ (w.r.t. orthogonal invariant volume form).

With the volume of tube interpretation and some differential geometry, one can show:

B, Amelunxen (2015)

$$\text{Prob} \left( \mathcal{C}_G(A) \geq \frac{1}{\varepsilon} \right) \leq 6 \cdot n \varepsilon \quad \text{if } \varepsilon < n^{-\frac{3}{2}}.$$

$$\mathbb{E}(\ln \mathcal{C}_G(A)) \leq 2.5 \cdot \ln(n) + 2.8.$$
Average analysis of Grassmann condition number

- Fix any closed regular convex cone $C \subset \mathbb{R}^n$.
- If $A \in \mathbb{R}^{m \times n}$ is standard Gaussian, then $W := \text{im}A^T$ is uniformly distributed in $\mathbb{G}_{n,m}$ (w.r.t. orthogonal invariant volume form).
- With the volume of tube interpretation and some differential geometry, one can show:

\[ \text{Prob} \left( \mathcal{G}(A) \geq \frac{1}{\varepsilon} \right) \leq 6 \cdot n \varepsilon \quad \text{if} \quad \varepsilon < n^{-\frac{3}{2}}. \]

\[ \mathbb{E}(\ln \mathcal{G}(A)) \leq 2.5 \cdot \ln(n) + 2.8. \]

- It is a challenge to extend this result to a uniform smoothed analysis.
Part III: Polynomial Equations

Complexity of Bezout’s Theorem

(Shub and Smale 1993–1996)
Smale’s 17th problem

The 17th of S. Smale’s problems for the 21st century asks:

*Can a zero of n complex polynomial equations in n unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?*
Let us explain this question in detail.
Let us explain this question in detail.

For a degree vector $d = (d_1, \ldots, d_n)$ we define

$$\mathcal{H}_d := \{ f = (f_1, \ldots, f_n) \mid f_i \in \mathbb{C}[X_0, \ldots, X_n] \text{ homogeneous of degree } d_i \}.$$
Let us explain this question in detail.

For a degree vector $d = (d_1, \ldots, d_n)$ we define

$$\mathcal{H}_d := \{ f = (f_1, \ldots, f_n) \mid f_i \in \mathbb{C}[X_0, \ldots, X_n] \text{ homogeneous of degree } d_i \}.$$ 

The input size is $N := \dim_{\mathbb{C}} \mathcal{H}_d$. 

Notations
Notations

- Let us explain this question in detail.
- For a degree vector $d = (d_1, \ldots, d_n)$ we define
  \[ \mathcal{H}_d := \{ f = (f_1, \ldots, f_n) \mid f_i \in \mathbb{C}[X_0, \ldots, X_n] \text{ homogeneous of degree } d_i \} \].
- The input size is $N := \dim_{\mathbb{C}} \mathcal{H}_d$.
- We look for zeros $\zeta$ of $f$ in complex projective space $\mathbb{P}^n$: $f(\zeta) = 0$. 
Bombieri-Weyl inner product

- For homogeneous polynomials of degree $d_i$,

$$f_i(x) = \sum_{|\alpha| = d_i} a_\alpha^i X^{\alpha}, \quad g_i(x) = \sum_{|\alpha| = d_i} b_\alpha^i X^{\alpha},$$

we define the Bombieri-Weyl hermitian inner product as

$$\langle f_i, g_i \rangle := \sum_{|\alpha| = d_i} a_\alpha^i \overline{b_\alpha^i} \binom{d_i}{\alpha}^{-1}.$$
Bombieri-Weyl inner product

- For homogeneous polynomials of degree $d_i$, 
  
  $$f_i(x) = \sum_{|\alpha| = d_i} a^{i}_{\alpha} X^{\alpha}, \quad g_i(x) = \sum_{|\alpha| = d_i} b^{i}_{\alpha} X^{\alpha},$$ 

  we define the **Bombieri-Weyl hermitian inner product** as 

  $$\langle f_i, g_i \rangle := \sum_{|\alpha| = d_i} a^{i}_{\alpha} \overline{b^{i}_{\alpha}} \left( \frac{d_i}{\alpha} \right)^{-1}.$$

- This inner product is invariant under the natural action of the unitary group $U(n + 1)$: up to scaling it is uniquely characterized by the invariance.
Bombieri-Weyl inner product

- For homogeneous polynomials of degree $d_i$, 
  \[ f_i(x) = \sum_{|\alpha| = d_i} a_\alpha^i X^\alpha, \quad g_i(x) = \sum_{|\alpha| = d_i} b_\alpha^i X^\alpha, \]
  we define the Bombieri-Weyl hermitian inner product as
  \[ \langle f_i, g_i \rangle := \sum_{|\alpha| = d_i} a_\alpha^i \overline{b_\alpha^i} \left( \binom{d_i}{\alpha} \right)^{-1}. \]

- This inner product is invariant under the natural action of the unitary group $U(n + 1)$: up to scaling it is uniquely characterized by the invariance.

- For $f, g \in \mathcal{H}_d$ we define $\langle f, g \rangle := \sum_{i=1}^n \langle f_i, g_i \rangle$ and $\| f \| := \langle f, f \rangle^{1/2}$. 
Bombieri-Weyl inner product

- For homogeneous polynomials of degree $d_i$,
  \[
  f_i(x) = \sum_{|\alpha|=d_i} a^i_\alpha x^\alpha, \quad g_i(x) = \sum_{|\alpha|=d_i} b^i_\alpha x^\alpha,
  \]
  we define the **Bombieri-Weyl hermitian inner product** as
  \[
  \langle f_i, g_i \rangle := \sum_{|\alpha|=d_i} a^i_\alpha \overline{b^i_\alpha} \binom{d_i}{\alpha}^{-1}.
  \]

- This inner product is invariant under the natural action of the unitary group $U(n+1)$: up to scaling it is uniquely characterized by the invariance.

- For $f, g \in \mathcal{H}_d$ we define $\langle f, g \rangle := \sum_{i=1}^n \langle f_i, g_i \rangle$ and $\|f\| := \langle f, f \rangle^{1/2}$.

- We have a **standard Gaussian** distribution on $\mathcal{H}_d$ with density
  \[
  \rho(f) = \frac{1}{\sqrt{2\pi}^{2N}} \exp \left( - \frac{1}{2} \|f\|^2 \right).
  \]
approximate zeros

For $f \in \mathcal{H}_d$ we define the Newton operator $N_f : \mathbb{P}^n \to \mathbb{P}^n$ by

$$N_f(z) := z - (Df(z)|_{T_z \mathbb{P}^n})^{-1} f(z).$$
Approximate zeros

- For \( f \in \mathcal{H}_d \) we define the **Newton operator** \( N_f : \mathbb{P}^n \to \mathbb{P}^n \) by

  \[
  N_f(z) := z - \left( Df(z) \big|_{T_z\mathbb{P}^n} \right)^{-1} f(z).
  \]

- Iterating \( N_f \) with starting point \( x_0 \) yields \( x_0, x_1, \ldots \in \mathbb{P}^n \), where

  \[
  x_{k+1} = N_f(x_k)
  \]
Approximate zeros

- For \( f \in \mathcal{H}_d \) we define the Newton operator \( N_f : \mathbb{P}^n \to \mathbb{P}^n \) by

\[
N_f(z) := z - \left( Df(z)\big|_{T_z\mathbb{P}^n} \right)^{-1} f(z).
\]

- Iterating \( N_f \) with starting point \( x_0 \) yields \( x_0, x_1, \ldots \in \mathbb{P}^n \), where

\[
x_{k+1} = N_f(x_k)
\]

- Definition (Smale 1986). \( x \in \mathbb{P}^n \) is called approximate zero of \( f \) with associated zero \( \zeta \) iff

\[
\forall i \in \mathbb{N} : \quad d(x_i, \zeta) \leq \frac{1}{2^{2^i-1}} d(x_0, \zeta).
\]
Approximate zeros

- For $f \in \mathcal{H}_d$ we define the Newton operator $N_f : \mathbb{P}^n \rightarrow \mathbb{P}^n$ by
  \[
  N_f(z) := z - (Df(z)|_{T_z\mathbb{P}^n})^{-1} f(z).
  \]

- Iterating $N_f$ with starting point $x_0$ yields $x_0, x_1, \ldots \in \mathbb{P}^n$, where
  \[
  x_{k+1} = N_f(x_k).
  \]

- **Definition (Smale 1986).** $x \in \mathbb{P}^n$ is called approximate zero of $f$ with associated zero $\zeta$ iff
  \[
  \forall i \in \mathbb{N} : \quad d(x_i, \zeta) \leq \frac{1}{2^{i-1}} d(x_0, \zeta).
  \]

- Here the distance $d$ refers to the geodesic distance (angle) on the Riemannian manifold $\mathbb{P}^n$ (Fubini-Study metric).
Condition number

- Let $f(\zeta) = 0$. How much does $\zeta$ change when we perturb $f$ a little?
Condition number

- Let \( f(\zeta) = 0 \). How much does \( \zeta \) change when we perturb \( f \) a little?
- Consider the solution variety \( V := \{(f, \zeta) \mid f(\zeta) = 0\} \subseteq \mathcal{H}_d \times \mathbb{P}^n \), which is a smooth Riemannian submanifold.
Condition: The Geometry of Numerical Algorithms
Part III: Polynomial Equations
Approximate zeros, condition, and homotopy continuation

Condition number

- Let \( f(\zeta) = 0 \). How much does \( \zeta \) change when we perturb \( f \) a little?
- Consider the solution variety \( V := \{(f, \zeta) \mid f(\zeta) = 0\} \subseteq \mathcal{H}_d \times \mathbb{P}^n \), which is a smooth Riemannian submanifold
- If \( \zeta \) is a simple solution of \( f \), there is a locally defined solution map

\[
G: \mathcal{H}_d \rightarrow \mathbb{P}^n
\]

such that \( f' \mapsto (f', G(f')) \) is the local inverse of the projection map \( V \rightarrow \mathcal{H}_d, (f', \zeta') \mapsto f' \) (implicit function theorem).
Condition number

- Let \( f(\zeta) = 0 \). How much does \( \zeta \) change when we perturb \( f \) a little?
- Consider the solution variety \( V := \{(f, \zeta) \mid f(\zeta) = 0\} \subseteq \mathcal{H}_d \times \mathbb{P}^n \), which is a smooth Riemannian submanifold.
- If \( \zeta \) is a simple solution of \( f \), there is a locally defined solution map
  \[
  G : \mathcal{H}_d \to \mathbb{P}^n
  \]
  such that \( f' \mapsto (f', G(f')) \) is the local inverse of the projection map \( V \to \mathcal{H}_d \), \((f', \zeta') \mapsto f' \) (implicit function theorem).
- Consider the derivative of the solution map
  \[
  DG(f) : \mathcal{H}_d \to T_{\zeta} \mathbb{P}^n.
  \]
Condition number

- Let $f(\zeta) = 0$. How much does $\zeta$ change when we perturb $f$ a little?
- Consider the solution variety $V := \{(f, \zeta) \mid f(\zeta) = 0\} \subseteq \mathcal{H}_d \times \mathbb{P}^n$, which is a smooth Riemannian submanifold.
- If $\zeta$ is a simple solution of $f$, there is a locally defined solution map $G: \mathcal{H}_d \rightarrow \mathbb{P}^n$ such that $f' \mapsto (f', G(f'))$ is the local inverse of the projection map $V \rightarrow \mathcal{H}_d, (f', \zeta') \mapsto f'$ (implicit function theorem).
- Consider the derivative of the solution map $DG(f): \mathcal{H}_d \rightarrow T_{\zeta}\mathbb{P}^n$.
- We define the condition number of $f$ at $(f, \zeta)$ by
  $$\mu(f, \zeta) := \|f\| \cdot \|DG(f)\|.$$
Radius of quadratic convergence

Put $D := \max_i d_i$.

Combining Smale’s Gamma Theorem (1986) with the developments in Shub and Smale (1993–1996), one obtains:

**Version of Smale’s Gamma Theorem**

If $d(x, \zeta) \leq \frac{0.3}{D^3/2 \mu(f, \zeta)}$, then $x$ is an approximate zero of $f$ associated with $\zeta$. 
Adaptive linear homotopy continuation (1)

- Given a start system \((g, \zeta) \in V\) and an input \(f \in \mathcal{H}_d\).
Adaptive linear homotopy continuation (1)

- Given a start system \((g, \zeta) \in V\) and an input \(f \in \mathcal{H}_d\).
- Consider the line segment \([g, f]\) connecting \(g\) and \(f\) that consists of the systems

\[ q_t := (1 - t)g + tf \quad \text{for} \ t \in [0, 1]. \]
Adaptive linear homotopy continuation (1)

- Given a start system \((g, \zeta) \in V\) and an input \(f \in \mathcal{H}_d\).
- Consider the line segment \([g, f]\) connecting \(g\) and \(f\) that consists of the systems
  \[q_t := (1 - t)g + tf \quad \text{for} \quad t \in [0, 1].\]
- If \([g, f]\) does not meet the discriminant variety (i.e., none of the \(q_t\) has a multiple zero), then there exists a unique lifting to \(V\),
  \[\gamma: [0, 1] \to V, t \mapsto (f_t, \zeta_t),\]
  such that \(f_0 = g\).
Adaptive linear homotopy continuation (2)

The idea is to follow the path numerically: partition \([0, 1]\) into \(t_0 = 0, \ldots, t_k = 1\). Writing \(q_i := q_{t_i}\), successively compute approximations \(z_i\) of \(\zeta_{t_i}\) by Newton's method starting with \(z_0 := \zeta\). More specifically, compute \(z_{i+1} = N_{q_{i+1}}(z_i)\). 

![Diagram](image-url)
The idea is to follow the path $\gamma$ numerically: partition $[0, 1]$ into $t_0 = 0, \ldots, t_k = 1$. Writing $q_i := q_{t_i}$, successively compute approximations $z_i$ of $\zeta_{t_i}$ by Newton’s method starting with $z_0 := \zeta$. More specifically, compute

$$z_{i+1} := N_{q_{i+1}}(z_i).$$
Complexity of adaptive linear homotopy continuation

- We compute $t_{i+1}$ adaptively from $t_i$ such that
  \[ d(q_{i+1}, q_i) = \frac{c}{D^{3/2} \mu^2(q_i, z_i)}. \]

This defines the Adaptive Linear Homotopy ALH algorithm.
We compute $t_{i+1}$ adaptively from $t_i$ such that

$$d(q_{i+1}, q_i) = \frac{c}{D^{3/2} \mu^2(q_i, z_i)}.$$ 

This defines the \textbf{Adaptive Linear Homotopy ALH} algorithm.

We denote by $K(f, g, \zeta)$ the number $k$ of Newton continuation steps that are needed to follow the homotopy.
Complexity of adaptive linear homotopy continuation

- We compute $t_{i+1}$ adaptively from $t_i$ such that

$$d(q_{i+1}, q_i) = \frac{c}{D^{3/2} \mu^2(q_i, z_i)}.$$ 

This defines the Adaptive Linear Homotopy ALH algorithm.

- We denote by $K(f, g, \zeta)$ the number $k$ of Newton continuation steps that are needed to follow the homotopy.


$z_i$ is an approximate zero of $\zeta_i$ for all $i$. Moreover,

$$K(f, g, \zeta) \leq 217 D^{3/2} \int_0^1 \mu_{\text{norm}}(\gamma(t))^2 \|\dot{\gamma}(t)\| \, dt.$$
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
- Since we don’t know how to construct a good start system \((g, \zeta_0)\), we choose it at random:
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
- Since we don’t know how to construct a good start system \((g, \zeta_0)\), we choose it at random:
  - choose \(g \in \mathcal{H}_d\) from standard Gaussian,
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
- Since we don’t know how to construct a good start system \((g, \zeta_0)\), we choose it at random:
  - choose \(g \in \mathcal{H}_d\) from standard Gaussian,
  - choose one of the Bezout number \(D := d_1 \cdots d_n\) many zeros \(\zeta\) of \(g\) uniformly at random.
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
- Since we don’t know how to construct a good start system \((g, \zeta_0)\), we choose it at random:
  - choose \(g \in \mathcal{H}_d\) from standard Gaussian,
  - choose one of the Bezout number \(D := d_1 \cdots d_n\) many zeros \(\zeta\) of \(g\) uniformly at random.
- Efficient sampling of \((g, \zeta)\) is possible (Beltrán & Pardo 2008).
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
- Since we don’t know how to construct a good start system \((g, \zeta_0)\), we choose it at random:
  - choose \(g \in H_d\) from standard Gaussian,
  - choose one of the Bezout number \(D := d_1 \cdots d_n\) many zeros \(\zeta\) of \(g\) uniformly at random.
- Efficient sampling of \((g, \zeta)\) is possible (Beltrán & Pardo 2008).
- Las Vegas Algorithm LV
  draw \((g, \zeta) \in V\) at random
  run ALH on input \((f, g, \zeta)\)
Randomized algorithm

- Shub and Smale had shown that almost all \((g, \zeta) \in V\) have a condition number polynomial bounded in \(N, D\).
- However, it is unknown how to efficiently construct such \((g, \zeta)\).
- Since we don’t know how to construct a good start system \((g, \zeta_0)\), we choose it at random:
  - choose \(g \in \mathcal{H}_d\) from standard Gaussian,
  - choose one of the Bezout number \(D := d_1 \cdots d_n\) many zeros \(\zeta\) of \(g\) uniformly at random.
- Efficient sampling of \((g, \zeta)\) is possible (Beltrán & Pardo 2008).
- Las Vegas Algorithm LV
  - draw \((g, \zeta) \in V\) at random
  - run ALH on input \((f, g, \zeta)\)
- LV has the expected “running time”

\[ K(f) := E_{g, \zeta} K(f, g, \zeta). \]
LV runs in average expected polynomial time.
Average expected polynomial time

- LV runs in **average expected polynomial time**:

Beltrán and Pardo (2009, 2011)

\[ \mathbb{E}_f K(f) = O(D^{3/2}Nn), \]

where the expectation is over a standard Gaussian \( f \in \mathcal{H}_d \).
Average expected polynomial time

- LV runs in average expected polynomial time:

\[ \mathbb{E}_f K(f) = O\left( D^{3/2} Nn \right), \]

where the expectation is over a standard Gaussian \( f \in \mathcal{H}_d \).

- When allowing randomized algorithms, this is a solution to Smale’s 17th problem.
Average expected polynomial time

- LV runs in average expected polynomial time:

\[
E_f K(f) = O(D^{3/2} N n),
\]

where the expectation is over a standard Gaussian \( f \in \mathcal{H}_d \).

- When allowing randomized algorithms, this is a solution to Smale’s 17th problem.
- Note that randomness enters here in two ways: as an algorithmic tool and as a way to measure the performance of algorithms.
Smoothed expected polynomial time

Smoothed analysis: let \( \bar{f} \in \mathcal{H}_d \) and suppose that \( f \) is isotropic Gaussian with mean \( \bar{f} \) and variance \( \sigma^2 \).

**Smoothed analysis (B, Cucker (2011))**

\[
\sup_{\|f\| \leq 1} \mathbb{E}_{f \sim N(\bar{f}, \sigma^2 I)} K(f) = \mathcal{O}\left(\frac{D^{3/2} N \eta}{\sigma}\right).
\]
A near solution to Smale’s 17th problem

B, Cucker (2011)

There is a deterministic algorithm for Smale’s 17th problem taking on standard Gaussian input $f \in \mathcal{H}_d$ an expected number of arithmetic operations $T(f)$ bounded by

$$E_f T(f) = N^{O(\log \log N)}.$$
A near solution to Smale’s 17th problem

B, Cucker (2011)

There is a deterministic algorithm for Smale’s 17th problem taking on standard Gaussian input $f \in \mathcal{H}_d$ an expected number of arithmetic operations $T(f)$ bounded by

$$\mathbb{E}_f T(f) = N^{O(\log \log N)}.$$

- If $D \leq n$, the algorithm runs ALH with the start system $(g, \zeta)$, where

  $$g_i = X_i^{d_i} - X_0^{d_i}, \quad \zeta = (1, \ldots, 1)$$

  (the zeros of $g_i$ consist of roots of unity).
A near solution to Smale’s 17th problem

B, Cucker (2011)

There is a deterministic algorithm for Smale’s 17th problem taking on standard Gaussian input $f \in \mathcal{H}_{d}$ an expected number of arithmetic operations $T(f)$ bounded by

$$\mathbb{E}_f T(f) = N^{O(\log \log N)}.$$ 

- If $D \leq n$, the algorithm runs ALH with the start system $(g, \zeta)$, where

  $$g_i = X_i^{d_i} - X_0^{d_i}, \quad \zeta = (1, \ldots, 1)$$

  (the zeros of $g_i$ consist of roots of unity).

- If $D \geq n$, the algorithm runs ALH with the start system $(g, \zeta)$, where

  $$g_i := X_0^{d_i-i} X_i, \quad \zeta = (1, 0, \ldots, 0);$$

Solution to Smale’s 17th problem

- Pierre Lairez had a clever idea: the average analysis assumes a randomness in the input $f \in \mathcal{H}_d$. 

Solution to Smale’s 17th problem

- Pierre Lairez had a clever idea: the average analysis assumes a randomness in the input $f \in \mathcal{H}_d$.
- Based on this randomness, one can construct a random start system $(g, \zeta)$ for ALH.
Pierre Lairez had a clever idea: the average analysis assumes a randomness in the input \( f \in \mathcal{H}_d \).

Based on this randomness, one can construct a random start system \((g, \zeta)\) for ALH.

This is a general principle. It leads to a deterministic algorithm!
Solution to Smale’s 17th problem

- Pierre Lairez had a clever idea: the average analysis assumes a randomness in the input $f \in \mathcal{H}_d$.
- Based on this randomness, one can construct a random start system $(g, \zeta)$ for ALH.
- This is a general principle. It leads to a deterministic algorithm!

Lairez (2016)

There is a deterministic algorithm for Smale’s 17th problem taking on standard Gaussian input $f \in \mathcal{H}_d$ an expected number of arithmetic operations $T(f)$ bounded by a polynomial in the input size $N$. 
Proof idea for smoothed analysis of ALH (1)

- A relevant idea is the systematic use of Gaussians, which before B & Cucker were not used in this context.
Proof idea for smoothed analysis of ALH (1)

- A relevant idea is the systematic use of Gaussians, which before B & Cucker were not used in this context.
- Consider the mean square condition number

\[ \mu_2(q)^2 := \frac{1}{D} \sum_{\zeta \in V(q)} \mu(q, \zeta)^2 \quad \text{for } g \in \mathcal{H}_d. \]
Proof idea for smoothed analysis of ALH (1)

- A relevant idea is the systematic use of Gaussians, which before B & Cucker were not used in this context.
- Consider the mean square condition number
  \[
  \mu_2(q)^2 := \frac{1}{\mathcal{D}} \sum_{\zeta \in \mathcal{V}(q)} \mu(q, \zeta)^2 \quad \text{for } g \in \mathcal{H}_d.
  \]
- The analysis of ALH gives
  \[
  \mathbb{E}_{\zeta \in \mathcal{V}(g)} K(f, g, \zeta) \leq c D^{3/2} \int_0^1 \mu_2(q_t)^2 \|\dot{\gamma}(t)\| \, dt
  \leq c D^{3/2} \int_0^1 \mu_2(q_t)^2 \frac{\|f\| \cdot \|g\|}{\|q_t\|^2} \, dt.
  \]
Proof idea for smoothed analysis of ALH (1)

- A relevant idea is the systematic use of Gaussians, which before B & Cucker were not used in this context.

- Consider the mean square condition number

\[
\mu_2(q)^2 \ := \ \frac{1}{D} \sum_{\zeta \in V(q)} \mu(q, \zeta)^2 \quad \text{for} \ g \in \mathcal{H}_d.
\]

- The analysis of ALH gives

\[
\mathbb{E}_{\zeta \in V(g)} K(f, g, \zeta) \leq c D^{3/2} \int_0^1 \mu_2(q_t)^2 \| \dot{\gamma}(t) \| \, dt
\]

\[
\leq c D^{3/2} \int_0^1 \mu_2(q_t)^2 \frac{\|f\| \cdot \|g\|}{\|q_t\|^2} \, dt.
\]

- \( \mathbb{E}(\|f\|^2) = 2N \) (chi-square). Replace \( \|f\| \) by \( \sqrt{N} \) (cheating a bit).
Proof idea for smoothed analysis of ALH (2)

\[ \mathbb{E}_{\zeta \in \mathcal{V}(g)} K(f, g, \zeta) \leq c D^{3/2} N \int_0^1 \frac{\mu_2(q_t)^2}{\|q_t\|^2} \, dt. \]
Proof idea for smoothed analysis of ALH (2)

\[ \mathbb{E}_{\zeta \in V(g)} K(f, g, \zeta) \leq c D^{3/2} N \int_0^1 \frac{\mu_2(q_t)^2}{\|q_t\|^2} \, dt. \]

By Fubini,

\[ \mathbb{E}_{f \sim N(\bar{f}, \sigma^2 I)} \mathbb{E}_{g \sim N(0, I)} \mathbb{E}_{\zeta \in V(g)} K(f, g, \zeta) \leq c D^{3/2} N \int_0^1 \mathbb{E} \left( \frac{\mu_2(q_t)^2}{\|q_t\|^2} \right) \, dt. \]
Proof ideas for smoothed analysis of ALH (2)

- \( \mathbb{E}_{\zeta \in V(g)} K(f, g, \zeta) \leq c D^{3/2} N \int_0^1 \frac{\mu_2(q_t)^2}{\|q_t\|^2} \, dt \).

- By Fubini,

\[ \mathbb{E}_{f \sim N(\bar{f}, \sigma^2 I)} \mathbb{E}_{g \sim N(0, I)} \mathbb{E}_{\zeta \in V(g)} K(f, g, \zeta) \leq c D^{3/2} N \int_0^1 \mathbb{E} \left( \frac{\mu_2(q_t)^2}{\|q_t\|^2} \right) \, dt. \]

- For fixed \( t \), \( q_t = (1 - t)g + tf \) is again Gaussian, \( q_t \sim N(\bar{q}_t, \sigma_t^2 I) \), with

\[ \bar{q}_t = tf, \quad \sigma_t^2 = (1 - t)^2 + \sigma^2 t^2. \]
Proof idea for smoothed analysis of ALH (3)

Main technical contribution of proof

\[ \mathbb{E}_{q \sim N(q, \sigma^2 I)} \left( \frac{\mu_2(q)}{\|q\|^2} \right) = O \left( \frac{n}{\sigma^2} \right). \]

Using this,

\[ \mathbb{E}_{f \sim N(\bar{f}, \sigma^2 I)} K(f) \leq c \, D^{3/2} N \int_0^1 \frac{n}{(1 - t)^2 + \sigma^2 t^2} dt = c \, D^{3/2} N \frac{n}{\sigma}. \]
Proof ideas

Proof idea for smoothed analysis of ALH (3)

**Main technical contribution of proof**

\[ \mathbb{E}_{q \sim N(q, \sigma^2 I)} \left( \frac{\mu_2(q)^2}{\|q\|^2} \right) = O \left( \frac{n}{\sigma^2} \right). \]

Using this,

\[ \mathbb{E}_{f \sim N(\bar{f}, \sigma^2 I)} K(f) \leq c D^{3/2} N \int_0^1 \frac{n}{(1-t)^2 + \sigma^2 t^2} \, dt = c D^{3/2} N \frac{n}{\sigma}. \]

A slightly better estimate, with a simpler proof, was obtained by Armentano, B, Béltran, Cucker, Shub (2016).
On proving the main technical contribution (1)

- Put $\mathcal{M} := \mathbb{C}^{n \times (n+1)}$ and consider the map (slightly cheating ...)

  $$\Psi : V \rightarrow \mathcal{M}, \quad (q, \zeta) \mapsto M := \text{diag}(\sqrt{d_1}, \ldots, \sqrt{d_n})^{-1} Df(\zeta).$$

Recall $\mu(q, \zeta)/\|q\| = \|M^\dagger\|$. 
On proving the main technical contribution (1)

- Put $\mathcal{M} := \mathbb{C}^{n \times (n+1)}$ and consider the map (slightly cheating ...)

$$\Psi: V \to \mathcal{M}, (q, \zeta) \mapsto M := \text{diag}(\sqrt{d_1}, \ldots, \sqrt{d_n})^{-1} Df(\zeta).$$

Recall $\mu(q, \zeta)/\|q\| = \|M^\dagger\|$.

- The noncentered Gaussian on $\mathcal{H}_d$ defines a distribution on $V$ (choose $q$ and then one of its $D$ zeros uniformly at random). Then

$$\mathbb{E}_{\mathcal{H}_d} \left( \frac{\mu_2(q)^2}{\|q\|^2} \right) = \mathbb{E}_V \left( \frac{\mu(q, \zeta)^2}{\|q\|^2} \right) = \mathbb{E}_\mathcal{M} \left( \|M^\dagger\|^2 \right)$$

where the last expectation is w.r.t. the distribution on $\mathcal{M}$ induced by $\Psi$. 
On proving the main technical contribution (2)

- For $\zeta \in \mathbb{P}^n$ let $R_\zeta$ be the set of those $q \in \mathcal{H}_d$ that vanish at $\zeta$ of order $> 1$. 
On proving the main technical contribution (2)

- For \( \zeta \in \mathbb{P}^n \) let \( R_\zeta \) be the set of those \( q \in \mathcal{H}_d \) that vanish at \( \zeta \) of order \( > 1 \).
- Further, let \( L_\zeta \) be the orthogonal complement in \( R_\zeta \) in the space of \( q \in \mathcal{H}_d \) vanishing at \( \zeta \).
On proving the main technical contribution (2)

- For $\zeta \in \mathbb{P}^n$ let $R_\zeta$ be the set of those $q \in \mathcal{H}_d$ that vanish at $\zeta$ of order $> 1$.
- Further, let $L_\zeta$ be the orthogonal complement in $R_\zeta$ in the space of $q \in \mathcal{H}_d$ vanishing at $\zeta$.
- We obtain an orthogonal decomposition

$$\mathcal{H}_d = C_\zeta \oplus L_\zeta \oplus R_\zeta, \quad \overline{q} = \overline{k}_\zeta + \overline{g}_\zeta + \overline{h}_\zeta.$$
On proving the main technical contribution (2)

- For $\zeta \in \mathbb{P}^n$ let $R_\zeta$ be the set of those $q \in \mathcal{H}_d$ that vanish at $\zeta$ of order $> 1$.
- Further, let $L_\zeta$ be the orthogonal complement in $R_\zeta$ in the space of $q \in \mathcal{H}_d$ vanishing at $\zeta$.
- We obtain an orthogonal decomposition
  \[ \mathcal{H}_d = C_\zeta \oplus L_\zeta \oplus R_\zeta, \quad \bar{q} = \overline{k}_\zeta + \overline{g}_\zeta + \overline{h}_\zeta. \]
- The density of $N(\bar{q}, \sigma^2 I)$ factors into Gaussians:
  \[ \rho_{\mathcal{H}_d}(k + g + h) = \rho_{C_\zeta}(k) \cdot \rho_{L_\zeta}(g) \cdot \rho_{R_\zeta}(h). \]
On proving the main technical contribution (2)

- For \( \zeta \in \mathbb{P}^n \) let \( R_\zeta \) be the set of those \( q \in H_d \) that vanish at \( \zeta \) of order \( > 1 \).
- Further, let \( L_\zeta \) be the orthogonal complement in \( R_\zeta \) in the space of \( q \in H_d \) vanishing at \( \zeta \).
- We obtain an orthogonal decomposition
  \[ H_d = C_\zeta \oplus L_\zeta \oplus R_\zeta, \quad \bar{q} = \bar{k}_\zeta + \bar{g}_\zeta + \bar{h}_\zeta. \]
- The density of \( N(\bar{q}, \sigma^2 I) \) factors into Gaussians:
  \[ \rho_{H_d}(k + g + h) = \rho_{C_\zeta}(k) \cdot \rho_{L_\zeta}(g) \cdot \rho_{R_\zeta}(h). \]
- \( L_\zeta \) is isometrically isomorphic to \( \mathcal{M}_\zeta := \{ M \in \mathcal{M}: M\zeta = 0 \} \)
  inducing a Gaussian \( N(\bar{M}_\zeta, \sigma^2 I) \) on the fiber \( \mathcal{M}_\zeta \).
On proving the main technical contribution (3)

- For $M \in \mathcal{M}$ of full rank with zero $\zeta$ one can show that

$$\rho_{\mathcal{M}}(M) = \rho_{\zeta}(0) \cdot \rho_{\mathcal{M}\zeta}(M)$$
On proving the main technical contribution (3)

- For $M \in \mathcal{M}$ of full rank with zero $\zeta$ one can show that
  \[ \rho_\mathcal{M}(M) = \rho_{C_\zeta}(0) \cdot \rho_\mathcal{M}_\zeta(M) \]

- With the coarea formula (transformation of integrals) one shows
  \[
  \mathbb{E}_\mathcal{M}(\|M^\dagger\|^2) = \int_{\mathcal{M}} \|M^\dagger\|^2 \rho_\mathcal{M}(M) dM \\
  = \mathbb{E}_{\zeta \in \mathbb{P}^n}(\mathbb{E}_{\tilde{p}_\mathcal{M}_\zeta}(\|M^\dagger\|^2))
  \]

Right expectation is over induced distribution of the zeros $\zeta$ of $M$, second expectation is w.r.t. the following conditional density on $\mathcal{M}_\zeta$:

\[ \tilde{p}_\mathcal{M}_\zeta(M) = c_\zeta \rho_\mathcal{M}_\zeta(M) \det(MM^*) \]
Proof ideas

On proving the main technical contribution (3)

- For $M \in \mathcal{M}$ of full rank with zero $\zeta$ one can show that

$$ \rho_\mathcal{M}(M) = \rho_{C_\zeta}(0) \cdot \rho_\mathcal{M}_\zeta(M) $$

- With the coarea formula (transformation of integrals) one shows

$$ \mathbb{E}_\mathcal{M}(\|M^\dagger\|^2) = \int_{\mathcal{M}} \|M^\dagger\|^2 \rho_\mathcal{M}(M) dM $$

$$ = \mathbb{E}_{\zeta \in \mathbb{P}^n}(\mathbb{E}_{\tilde{\rho}_\mathcal{M}_\zeta}(\|M^\dagger\|^2)) $$

Right expectation is over induced distribution of the zeros $\zeta$ of $M$, second expectation is w.r.t. the following conditional density on $\mathcal{M}_\zeta$:

$$ \tilde{\rho}_\mathcal{M}_\zeta(M) = c_\zeta \rho_\mathcal{M}_\zeta(M) \det(MM^*) $$

- As for the smoothed analysis of matrix condition numbers one can show

$$ \mathbb{E}_{\tilde{\rho}_\mathcal{M}_\zeta}(\|M^\dagger\|^2) = \mathcal{O}\left(\frac{n}{\sigma^2}\right) $$
On proving the main technical contribution (3)

- For $M \in \mathcal{M}$ of full rank with zero $\zeta$ one can show that
  \[
  \rho_{\mathcal{M}}(M) = \rho_{\mathcal{C}_0}(0) \cdot \rho_{\mathcal{M}_\zeta}(M)
  \]

- With the coarea formula (transformation of integrals) one shows
  \[
  \mathbb{E}_{\mathcal{M}}(\|M^\dagger\|^2) = \int_{\mathcal{M}} \|M^\dagger\|^2 \rho_{\mathcal{M}}(M) \, dM \\
  = \mathbb{E}_{\zeta \in \mathbb{P}_n} \left( \mathbb{E}_{\tilde{\rho}_{\mathcal{M}_\zeta}}(\|M^\dagger\|^2) \right)
  \]
  Right expectation is over induced distribution of the zeros $\zeta$ of $M$, second expectation is w.r.t. the following conditional density on $\mathcal{M}_\zeta$:
  \[
  \tilde{\rho}_{\mathcal{M}_\zeta}(M) = c_\zeta \rho_{\mathcal{M}_\zeta}(M) \det(MM^*)
  \]

- As for the smoothed analysis of matrix condition numbers one can show
  \[
  \mathbb{E}_{\tilde{\rho}_{\mathcal{M}_\zeta}}(\|M^\dagger\|^2) = \mathcal{O}\left(\frac{n}{\sigma^2}\right).
  \]

- Hence $\mathbb{E}_{\mathcal{M}}(\|M^\dagger\|^2) = \mathcal{O}\left(\frac{n}{\sigma^2}\right)$. □
Thank you for your attention!
References


Institute of Mathematics, Technische Universität Berlin

E-mail address: pbuerg@math.tu-berlin.de