FFTs in Graphics and Vision

Fast String Matching
and
Math Review

Fast Pattern Matching in Strings
Knuth et al., 1977
Outline

Fast Substring Matching

Math Review

- Complex Numbers
- Vector Spaces
- Linear Operators
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$. 
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Example:

$$S = \text{ACDBEFCD} \text{BE} \quad T = \text{CDB}$$
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Brute Force:

• For each position in $S$:
  ◦ Test if the next $|T|$ letters in $S$ match $T$

$S = \text{ACDBEFCDBE}$
$T = \text{CDB}$

$O(|S| \times |T|)$
Fast Substring Matching

Challenge:
Given strings \( S \) and \( T \), find all occurrences of \( T \) as a substring of \( S \).

Brute Force:

- For each position in \( S \):
  - Test if the next \( |T| \) letters in \( S \) match \( T \)

Can we do this more efficiently?
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Observation:

On a failed match, we don’t have to compare all $|T|$ letters in $T$:

$S=ACDBEFCDBE$  $T=CDB$  
Comparisons: 3
Fast Substring Matching

Challenge:
Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Observation:
What if the situation is more complex?

$S=$AAAAAAAAAAAB  $T=$AAAB
AAAAAAAAAAAB
AAAAAAAAAB

Comparisons: 4
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Knuth et al. (1977):

On a failed match, we don’t have to re-start the matching.

$S=$AAAAAAAB

$T=$AAAB

$O(|S| + |T|)$
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Knuth et al. (1977):

On a failed match, we don’t have to re-start the matching.

The key is to know where in $T$ we have to start comparing.
Fast Substring Matching

Challenge:

Given strings $S$ and $T$, find all occurrences of $T$ as a substring of $S$.

Knuth et al. (1977):

The size of the shift on a mismatch is determined by the repetitions in $T$, is independent of $S$, and can be computed in $O(|T|)$ time.

For more details, see:

*Fast Pattern Matching in Strings.*
Fast Substring Matching

Recall:

Our goal is to perform registration and symmetry detection on the circle.
Fast Substring Matching

Applications:

If we think of a string as a signal on a circle:

- We can test if signal $T$ is a rotation of $S$ by testing if $T$ is a substring of $SS$

```
S = ABACABAC

T = ACABACAB

SS = ABACABACACABACABACABACABACAB

T = ACABACAB
```
Fast Substring Matching

Applications:

If we think of a string as a signal on a circle:

- We can test if signal $T$ is a rotation of $S$ by testing if $T$ is a substring of $SS$
- We can test if $S$ has rotational symmetry by testing if $S$ is a substring of $SS$

$S=\text{ABACABAC}$

$SS=\text{ABACABACABACABAC}$
Fast Substring Matching

Applications:

If we think of a string as a signal on a circle:

- We can test if signal $T$ is a rotation of $S$ by testing if $T$ is a substring of $SS$
- We can test if $S$ has *rotational* symmetry by testing if $S$ is a substring of $SS$

$S = \text{ABACABAC}$

$SS = \text{ABACABACABACABAC}$

$S = \text{ABACABAC}$

$S = \text{ABACABAC}$
Fast Substring Matching

Applications:

If we think of a string as a signal on a circle:

- We can test if signal $T$ is a rotation of $S$ by testing if $T$ is a substring of $SS$
- We can test if $S$ has *rotational* symmetry by testing if $S$ is a substring of $SS$
- We can test if $S$ has *reflective* symmetry by testing if $S$ is a substring of $(SS)^t$

$S = \text{ABACABAC}$

$(SS)^t = \text{CABACABACABACABAC}$
Fast Substring Matching

✓ A fast (linear time) algorithm for performing pattern detection on discrete signals

✗ Can only tell us if there is a perfect match
  ○ For real-world data, we need a continuous measure of similarity

✗ Only works for signals on a circle (or a line)
  ○ Hard to generalize to signals on other domains
Outline

Fast Substring Matching

Math Review
  - Complex Numbers
  - Vector Spaces
  - Linear Operators
Complex Numbers

A complex number $c \in \mathbb{C}$ is any number that can be written as:

$$c = a + ib$$

with $a, b \in \mathbb{R}$ and $i$ a square root of $-1$:

$$i^2 = -1$$
Complex Numbers

Given two complex numbers

\[ c_1 = a_1 + ib_1 \quad \text{and} \quad c_2 = a_2 + ib_2 \]

- The sum of the numbers is:
  \[ c_1 + c_2 = (a_1 + a_2) + i(b_1 + b_2) \]

- The product of the numbers is:
  \[
  c_1 \cdot c_2 = (a_1 + ib_1) \cdot (a_2 + ib_2) \\
  = a_1 \cdot a_2 + ib_1 \cdot ib_2 + a_1 \cdot ib_2 + ib_1 \cdot a_2 \\
  = (a_1 \cdot a_2 - b_1 \cdot b_2) + i(a_1 \cdot b_2 + b_1 \cdot a_2)
  \]
Complex Numbers

Given a complex numbers:

\[ c = a + ib \]

- The negation of the number is:
  \[ -c = -a - ib \]

- The conjugate of the number is:
  \[ \bar{c} = a - ib \]

- The reciprocal of the number is:
  \[ \frac{1}{c} = \frac{1}{a + ib} \cdot \frac{\bar{c}}{\bar{c}} = \frac{a - ib}{a^2 + b^2} \]
Complex Numbers

Why do we care?
Complex Numbers

Why do we care?

Fundamental Theorem of Algebra

Given any polynomial:

\[ p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \]

there always exists a complex number \( c_0 \in \mathbb{C} \) s.t.:

\[ p(c_0) = 0 \]
Vector Spaces

A (real/complex) vector space $V$ is a set of elements $v \in V$, with:

- An addition operator “+”, and
- A scaling operator “·”

(Adding two vectors together gives a vector and scaling a vector by a number gives a vector.)
Vector Spaces (Formal Properties 1)

For all \( u, v, w \in V \):

- **Associative addition:**
  \[
  (u + v) + w = u + (v + w)
  \]

- **Commutative addition:**
  \[
  u + v = v + u
  \]

- **Additive identity:**
  There exists a unique vector \( 0 \in V \) such that:
  \[
  v + 0 = v
  \]

- **Additive inverse:**
  There exists a vector \( (-v) \in V \) such that:
  \[
  v + (-v) = 0
  \]
Vector Spaces (Formal Properties 2)

For all $u, v \in V$, and (real / complex) scalars $a, b$:

- Distributive over vector addition:
  \[ a \cdot (u + v) = (a \cdot u) + (a \cdot v) \]

- Distributive over scalar addition:
  \[ (a + b) \cdot u = (a \cdot u) + (b \cdot u) \]

- Compatible scalar multiplication:
  \[ a \cdot (b \cdot u) = (a \cdot b) \cdot u \]

- Scalar Identity:
  \[ 1 \cdot u = u \]
Vector Spaces: Examples

Real Vector Spaces:
- The real / complex numbers
- The space of \( n \)-dimensional arrays with real / complex entries
- The space of \( m \times n \) matrices with real / complex entries
- The space of real / complex valued functions on a circle / line / plane / sphere / etc.

Complex Vector Spaces:
- The complex numbers
- The space of \( n \)-dimensional arrays with complex entries
- The space of \( m \times n \) matrices with complex entries
- The space of complex valued functions on a circle / line / plane / sphere / etc.
Vector Space Basis

A basis of $V$ is a set \( \{v_1, \ldots, v_n\} \subseteq V \) such that:

1. Any vector $v \in V$ can be expressed as:
   \[
   v = a_1 \cdot v_1 + \cdots + a_n \cdot v_n
   \]
   where the $a_i$ are (real / complex) scalars.

2. No basis vector $v_i$ can be expressed as the linear sum of the other basis vectors.

The dimension of $V$ is the number basis vectors and does not depend on the particular choice of basis.
Vector Space Basis

Many different bases can be used to represent the same vector space.

Example:

Consider the set of points in 2D Euclidean space.
Vector Space Basis

Many different bases can be used to represent the same vector space.

Example:

Consider the set of points in 2D Euclidean space.

We can represent each vector in terms of its \((x, y)\)-coordinates.
Vector Space Basis

Many different bases can be used to represent the same vector space.

Example:
Consider the set of points in 2D Euclidean space.

Or we could use a different basis…
Linear Maps

Given vector spaces $V$ and $W$, the map $L: V \to W$, is linear if for all $v_1, v_2 \in V$ and all scalars $a, b$:

$$L(a \cdot v_1 + b \cdot v_2) = a \cdot L(v_1) + b \cdot L(v_2)$$

If it exists, the inverse of a linear map $L$ is the map $L^{-1}$ with the property that:

$$L^{-1}(L(v)) = v$$
Linear Maps

If $L: V \to W$, is a linear map:

The set of vectors:
$$K = \{v \in V | L(v) = 0\}$$
is a vector subspace called the kernel.

The set of vectors:
$$I = \{w \in W | \exists v \in V \text{ s.t. } w = L(v)\}$$
is a vector subspace called the image.
Matrices

Given a vector space $V$, with basis $\{v_1, \ldots, v_n\}$, any element $v \in V$ can be expressed as:

$$v = a_1 \cdot v_1 + \cdots + a_n \cdot v_n$$

(with $a_1, \ldots, a_n$ scalars).

A linear map $L: V \rightarrow V$ can be expressed by an $n \times n$ matrix $M$ s.t.:

$$L(v) = b_1 \cdot v_1 + \cdots + b_n \cdot v_n$$

with:

$$\begin{bmatrix}
    b_1 \\
    \vdots \\
    b_n
\end{bmatrix} = \begin{pmatrix}
    M_{11} & \cdots & M_{1n} \\
    \vdots & \ddots & \vdots \\
    M_{n1} & \cdots & M_{nn}
\end{pmatrix} \begin{bmatrix}
    a_1 \\
    \vdots \\
    a_n
\end{bmatrix}$$
Change of Basis

Given a vector space $V$, and given two bases $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$, the matrix $B$ is the change of basis matrix:

- For all $v \in V$, we can write out $v$ in terms of the basis $\{v_1, \ldots, v_n\}$ as $v = a_1 \cdot v_1 + \cdots + a_n \cdot v_n$.
- We can also write out $v$ in terms of the basis $\{w_1, \ldots, w_n\}$ as $v = b_1 \cdot w_1 + \cdots + b_n \cdot w_n$.
- The coefficients are related by:

$$
\begin{bmatrix}
b_1 \\
\vdots \\
b_n
\end{bmatrix} = \begin{pmatrix}
B_{11} & \cdots & B_{1n} \\
\vdots & \ddots & \vdots \\
B_{n1} & \cdots & B_{nn}
\end{pmatrix}
\begin{bmatrix}
a_1 \\
\vdots \\
a_n
\end{bmatrix}
$$
Change of Basis

Given:

- A vector space $V$,
- Two bases $\{v_1, \cdots, v_n\}$ and $\{w_1, \cdots, w_n\}$,
- A linear operator $L$ represented by the matrix $M$ in terms of the basis $\{v_1, \cdots, v_n\}$.

The matrix representation for $L$ in terms of the basis $\{w_1, \cdots, w_n\}$ is given by:

$$BM B^{-1}$$
Change of Basis

Why do we care?
Change of Basis

Why do we care?

Choosing the appropriate basis can make it much easier to understand a linear operator.
Change of Basis

Why do we care?

Example:

\[ \mathbf{B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \mathbf{B}^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \]

\[ \mathbf{M} = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} \]
Change of Basis

Why do we care?

Example:

\[
\mathbf{M} = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} \implies \mathbf{B} \mathbf{M} \mathbf{B}^{-1}
\]

\[
\mathbf{B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \mathbf{B}^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}
\]
Change of Basis

Why do we care?

Example:

\[
\begin{bmatrix}
2 & 0 \\
-1 & 1
\end{bmatrix} \Rightarrow \mathbf{BMB}^{-1} = \begin{bmatrix}
1 & 0 \\
1 & 1
\end{bmatrix} \begin{bmatrix}
-1 & 0 \\
1 & 1
\end{bmatrix} \begin{bmatrix}
1 & 0 \\
-1 & 1
\end{bmatrix}
\]
Change of Basis

Why do we care?

Example:

\[
M = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} \implies BMB^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}
\]

In this basis the linear operator becomes anisotropic scaling!
Determinants

The determinant is a function that associates a scalar value to every linear map $L: V \to V$.

The determinant of $L: V \to V$ is the (signed) volume of the image of (any) unit cube in $V$. 
Determinants

The determinant of a linear map $L: V \to V$ equals zero if and only if there exists $v \in V$, with $v \neq 0$, such that $L(v) = 0$. 
Eigenvalues and Eigenvectors

The scalar $\lambda$ is an \underline{eigenvalue} of a linear operator $L: V \rightarrow V$ if there exists $v \in V$ such that:

$$\lambda \cdot v = L(v).$$

In this case, $v$ is an \underline{eigenvector} of $L$. 
Eigenvalues and Eigenvectors

If \( L: V \to V \) has an eigenpair \((\lambda, v)\), then:

\[
0 = (L - \lambda \cdot \text{Id.})(v)
\]

\( \Rightarrow \) The operator \( L - \lambda \cdot \text{Id.} \) has zero determinant.
Characteristic Polynomials

If we treat $\lambda$ as a variable, then the determinant:

$$\chi_L(\lambda) = \det(L - \lambda \cdot \text{Id.})$$

is a polynomial of degree $n$ in $\lambda$.

This is the characteristic polynomial of $L$. 
Characteristic Polynomials

The roots of the characteristic polynomial of $L$:

$$\chi_L(\lambda) = \det(L - \lambda \cdot \text{Id.})$$

are precisely the eigenvalues of $L$.

**Corollary:**

If $L: V \to V$ is a linear map on a complex vector space, $L$ always have at least one eigenvalue.