Do we need Number Theory? II

Václav Snášel

What is a number?

MCDXIX

||||||||||||||||||||||

664554

0xABCD

01717

010101010111011100001

i^i

$$1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\cdots$$

СОВРЕМЕННАЯ МАТЕМАТИКА
ДЛЯ СТУДЕНТОВ

А. А. КИРИЛЛОВ

ЧТО ТАКОЕ ЧИСЛО?

МОСКВА
ИЗДАТЕЛЬСКАЯ ФИРМА
«ФИЗИКО-МАТЕМАТИЧЕС
ВО «НАУКА»
1993

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[А] Атья М. Лекции по К-теории.— М.: Мир, 1967.

[Б] Березин Ф. А. Метод вторичного квантования.— М.: Наука, 1965.—2-е изд.— М.: Наука, 1986.

[БР] Браттели О., Робинсон Д. В. Операторные алгебры и квантовая статистическая механика.— М.: Мир, 1985.

[В] Вейль А. Основы теории чисел.— М.: Мир, 1972.

[ВВ] Владимиров В. С., Волович И. В. Введение в суперанализ // Теорет. и мат. физика.— 1984.— Т. 59, № 1.— С. 3—27; Т. 60, № 2.— С. 169—198.

[ГГПШ] Гельфанд И. М., Граев М. И., Пятецкий-Шапиро И. И. Теория представлений и автоморфные функции.— М.: Наука, 1966.— (Обобщенные функции.— Вып. 6.)

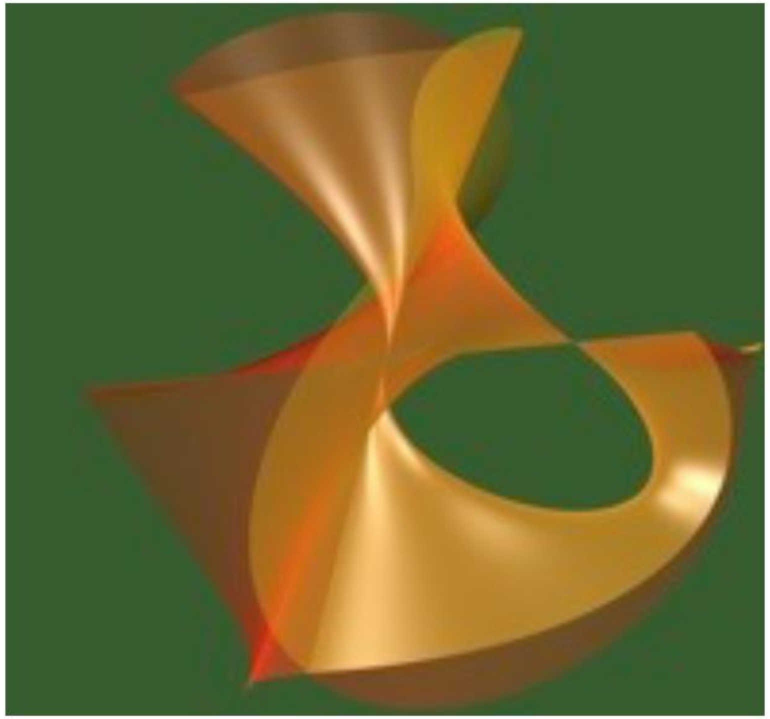
[ГК] Гельфанд И. М., Кириллов А. А. Структура тела, связанного с полупростой расщепимой алгеброй Ли // Функцион. анализ и его прил.— 1969.— Т. 3, № 1.— С. 7—26.

[ГМ] Гельфанд С. И., Манин Ю. И. Методы гомологической алгебры. 1: Введение в теорию когомологий и производные категории.— М.: Наука, 1988.

References

- Z. I. Borevich, I. R. Shafarevich, Number theory, Academic Press, 1986
- John Vince, Quaternions for Computer Graphics, Springer 2011
- John C. Baez, The Octonions, Bulletin of the American Mathematical Society 2002, 39 (2): 145–205
- C.C. Chang and H.J. Keisler, Model Theory, North-Holland, 1990
- Mathématiques & Arts, Catalogue 2013, Exposants ESMA
- А.Т.Фоменко, Математика и Миф Сквозь Призму Геометрии, http://dfgm.math.msu.su/files/fomenko/myth-sec6.php

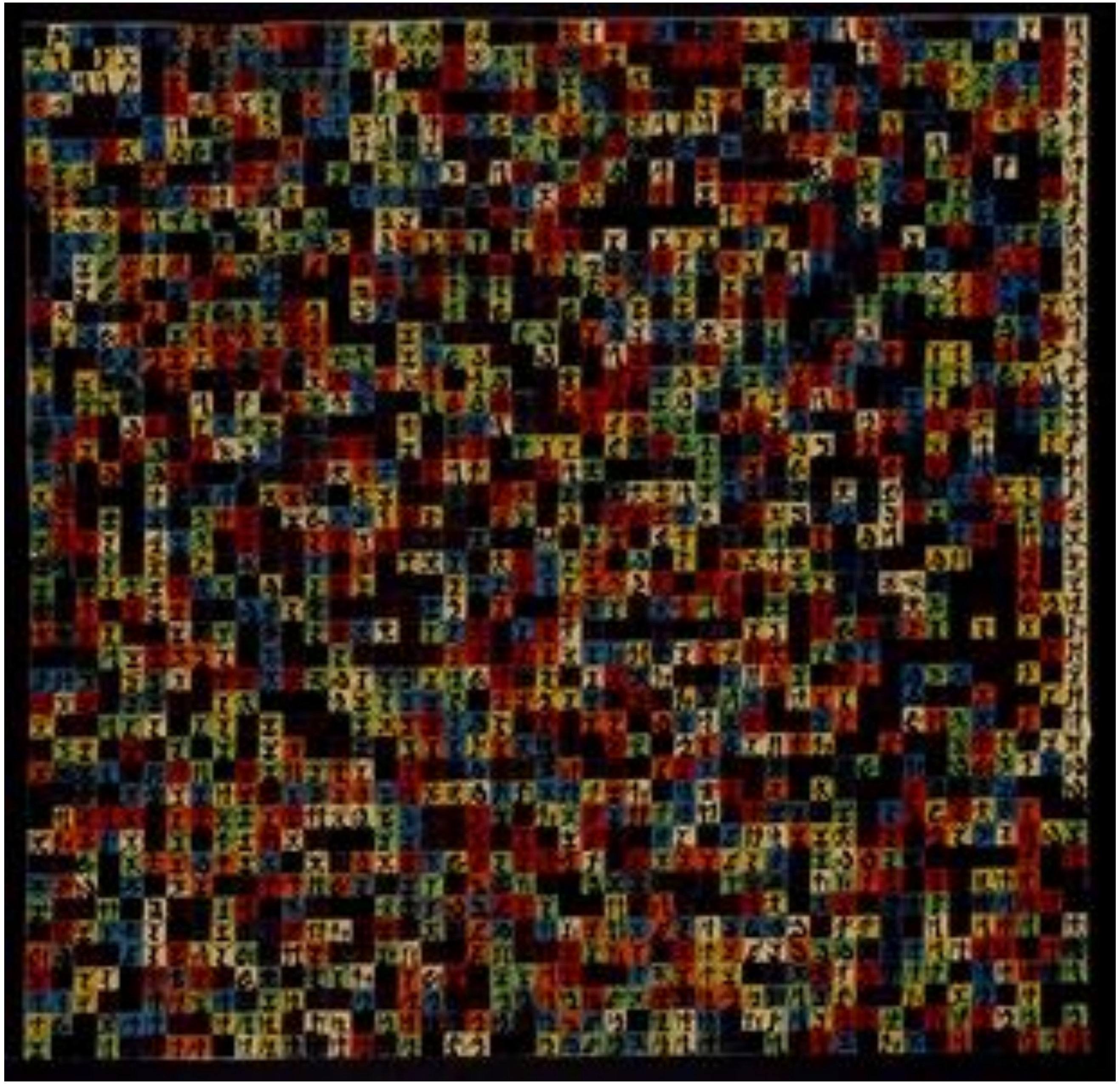
Images



Mouvement, élégance et harmonie

Pirouette, 2008

$$x^3\ y\ z + x^2\ z^3 - y^3 * z - y^3 + x^2\ y\ z^2 = 0$$



Number construction

Algebraic number

An algebraic number field is a finite extension of $\mathbb{Q}$; an algebraic number is an element of an algebraic number field.

Ring of integers. Let K be an algebraic number field. Because K is of finite degree over $\mathbb{Q}$, every element α of K is a root of monic polynomial

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_1 \qquad a_i \in \mathbb{Q}$$

If α is root of polynomial with integer coefficient, then α is called an algebraic integer of K.

Algebraic number

Consider more generally an integral domain A. An element a $\in A$ is said to be a unit if it has an inverse in A; we write A^* for the multiplicative group of units in A.

An element p of an integral domain A is said to be **irreducible** if it

is neither zero nor a unit, and can’t be written as a product of two nonunits.

An element p of A is said to **prime** if it is neither zero nor a unit, and if

$p|ab \ \Rightarrow p|a \ or \ p|b.$

Algebraic number

Example:

In $\mathbb{Z}\left[\sqrt{-5}\right]$ we have

$$6 = 2.3 = \left(1 + \sqrt{-5}\right).(1 - \sqrt{-5})$$

To see that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible, and no two are associates, we use norm map

$$N\colon \mathbb{Z}\left[\sqrt{-5}\right] \longrightarrow \mathbb{Q}, \qquad a + b\sqrt{-5} \longrightarrow a^2 + 5b^2$$

Algebraic number

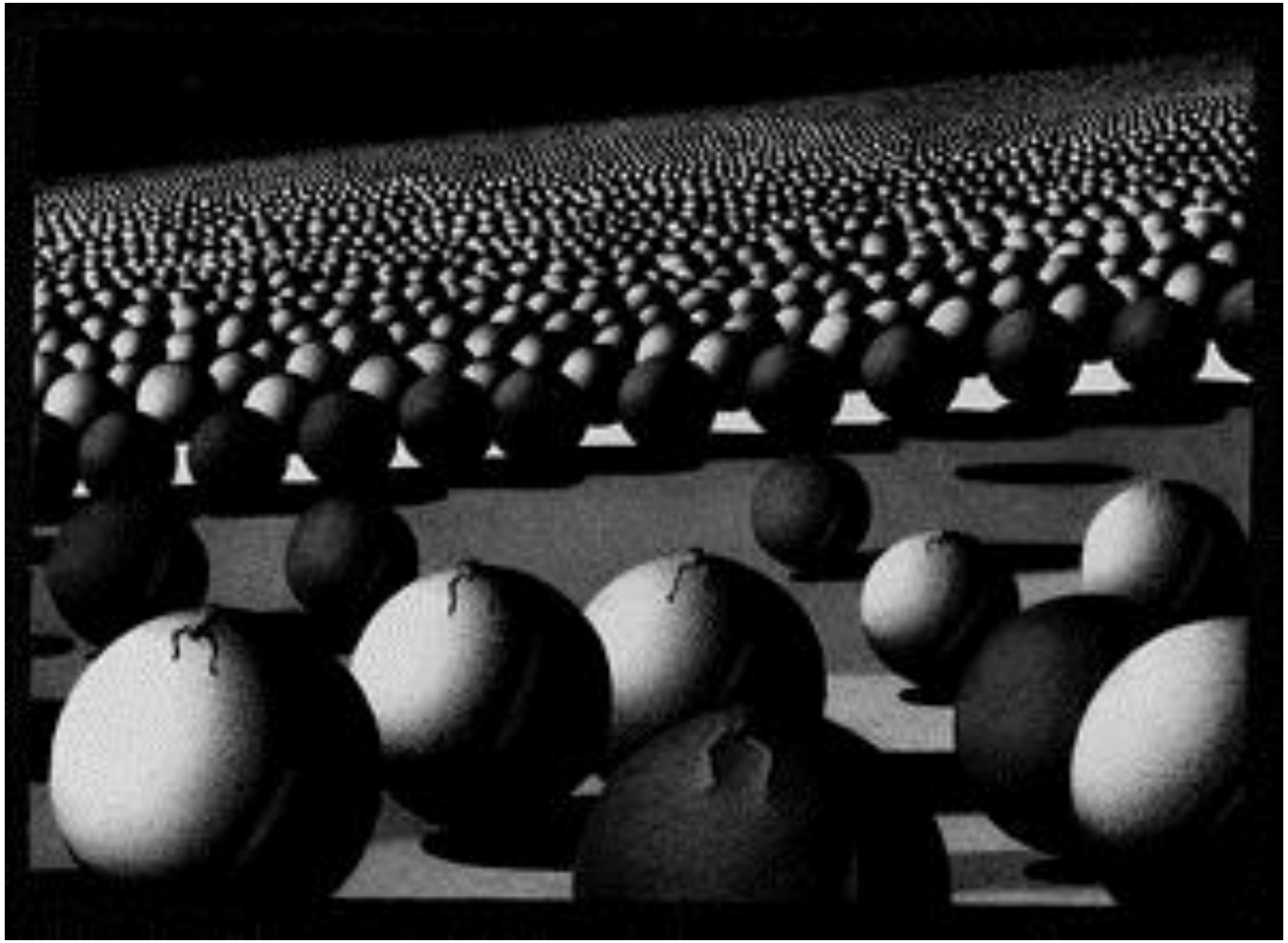
Why does unique factorization fail in $\mathbb{Z}\left[\sqrt{-5}\right]$? The problem is that irreducible elements in $\mathbb{Z}\left[\sqrt{-5}\right]$ need not be prime.

$$N\left(1+\sqrt{-5}\right)=6=2.3$$

$1+\sqrt{-5}$ divides 2.3 but it divides neither 2 nor 3. In fact, in an integral domain in which factorizations exist (e.g. a Noetherian ring), factorization is unique if all irreducible elements are prime.

(Noetherian ring is a ring in which every non-empty set of ideals has a maximal element)

Complex number



Quaternion - Brief History

- Invented in 1843 by Irish mathematician Sir William Rowan Hamilton
- Founded when attempting to extend complex numbers to the 3rd dimension
- Discovered on October 16 in the form of the equation:

$$i^2 = j^2 = k^2 = ijk = -1$$

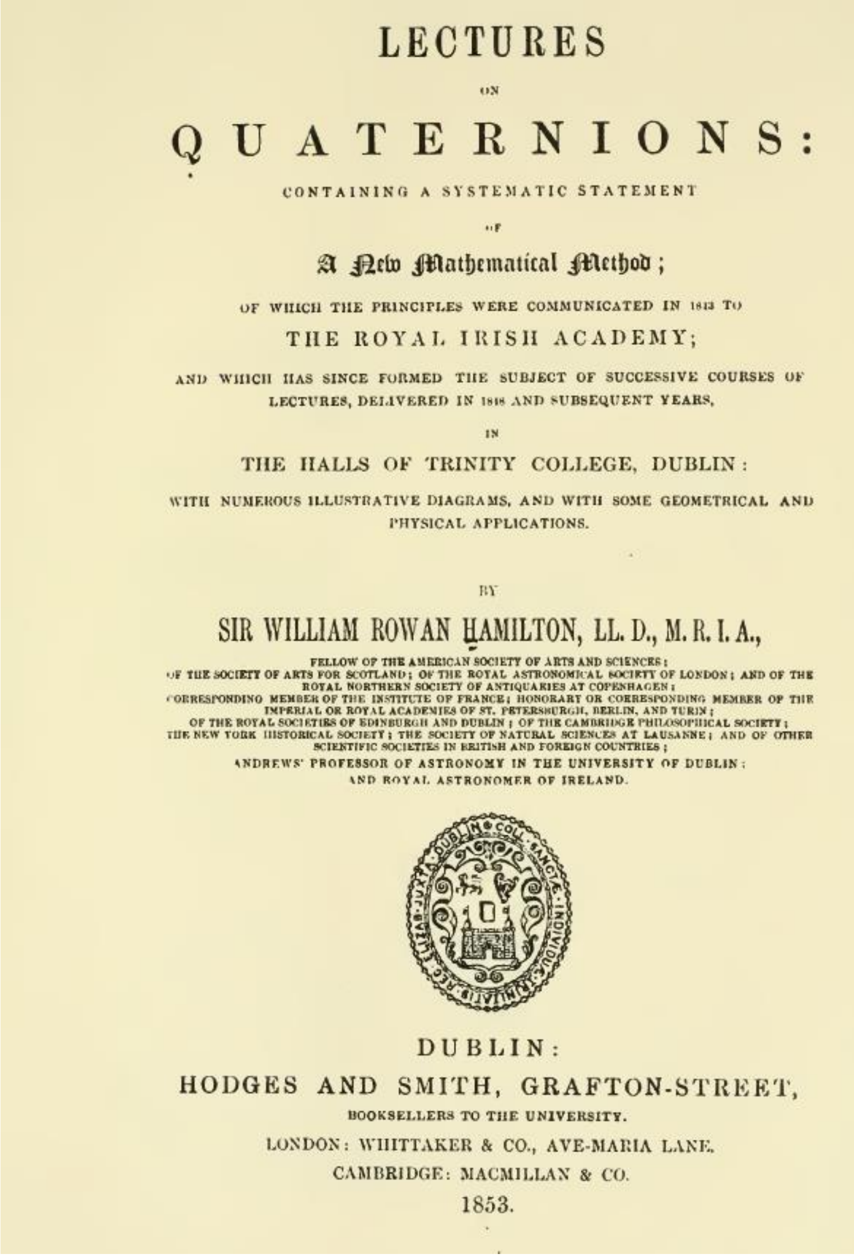
Quaternion - Brief History

Most mathematicians have heard the story of how Hamilton invented the quaternions.

In 1835, at the age of 30, he had discovered how to treat complex numbers as pairs of real numbers. Fascinated by the relation between ℂ and 2-dimensional geometry,

he tried for many years to invent a bigger algebra that would play a similar role in

3-dimensional geometry. In modern language, it seems he was looking for a 3-dimensional normed division algebra.



LECTURES

ON

QUATERNIONS:

CONTAINING A SYSTEMATIC STATEMENT

OF

A New Mathematical Method;

OF WHICH THE PRINCIPLES WERE COMMUNICATED IN 1843 TO

THE ROYAL IRISH ACADEMY;

AND WHICH HAS SINCE FORMED THE SUBJECT OF SUCCESSIVE COURSES OF LECTURES, DELIVERED IN 1848 AND SUBSEQUENT YEARS,

IN

THE HALLS OF TRINITY COLLEGE, DUBLIN:

WITH NUMEROUS ILLUSTRATIVE DIAGRAMS, AND WITH SOME GEOMETRICAL AND PHYSICAL APPLICATIONS.

BY

SIR WILLIAM ROWAN HAMILTON, LL. D., M. R. I. A.,

FELLOW OF THE AMERICAN SOCIETY OF ARTS AND SCIENCES; OF THE SOCIETY OF ARTS FOR SCOTLAND; OF THE ROYAL ASTRONOMICAL SOCIETY OF LONDON; AND OF THE ROYAL NORTHERN SOCIETY OF ANTIQUARIES AT COPENHAGEN; CORRESPONDING MEMBER OF THE INSTITUTE OF FRANCE; HONORARY OR CORRESPONDING MEMBER OF THE IMPERIAL OR ROYAL ACADEMIES OF ST. PETERSBURGH, BERLIN, AND TURIN; OF THE ROYAL SOCIETIES OF EDINBURGH AND DUBLIN; OF THE CAMBRIDGE PHILOSOPHICAL SOCIETY; THE NEW YORK HISTORICAL SOCIETY; THE SOCIETY OF NATURAL SCIENCES AT LAUSANNE; AND OF OTHER SCIENTIFIC SOCIETIES IN BRITISH AND FOREIGN COUNTRIES;

ANDREWS' PROFESSOR OF ASTRONOMY IN THE UNIVERSITY OF DUBLIN:

AND ROYAL ASTRONOMER OF IRELAND.

DUBLIN:

HODGES AND SMITH, GRAFTON-STREET,

BOOKSELLERS TO THE UNIVERSITY.

LONDON: WHITTAKER & CO., AVE-MARIA LANE.

CAMBRIDGE: MACMILLAN & CO.

1853.

Quaternion

- Definition

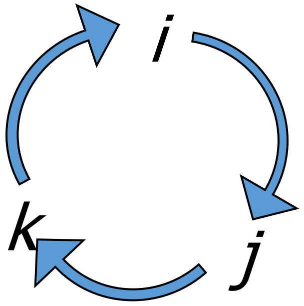
$$q = q_0 + q_1 i + q_2 j + q_3 k = q_0 + \vec{q}$$

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$



Applications of Quaternions

- Used to represent rotations and orientations of objects in three-dimensional space in:
  - Computer graphics
  - Image procession
  - Control theory
  - Signal processing
  - Attitude controls
  - Physics
  - Orbital mechanics
  - Quantum Computing

Advantages of Quaternions

- Avoids *Gimbal Lock*
- Faster multiplication algorithms to combine successive rotations than using rotation matrices
- Easier to normalize than rotation matrices
- Interpolation
- Representation color in image RGB

Gimbal lock is the loss of one degree of freedom in a three-dimensional, three-gimbal mechanism that occurs when the axes of two of the three gimbals are driven into a parallel configuration, "locking" the system into rotation in a degenerate two-dimensional space.

Quaternions

Multiplication as Rotation and Scaling	
MULTIPLICATION AS ROTATION	**MULTIPLICATION AS SCALING**
• 1 Represents the identity	• Choose a direction—not coordinate free
• Unit vectors represent rotations	•Similar to complex multiplication
• $c > 0$ represents scaling	• Similar to real multiplication
RULES	**REASONS**
• Associative	•Rotation is associative
•Distributes through addition	• Rotation is a linear transformation
• Identity and inverses	• Rotations can be undone
• Not Commutative	• Rotation in 3-D not commutative
• Preserves length ($\|pq\| = \|p\| \|q\|$)	• Rotation is an isometry

Singular value decomposition

For an $m \times n$ matrix **A (Document term)** of rank r there exists a factorization (Singular Value Decomposition = **SVD**) as follows:

$$A = U\Sigma V^T$$

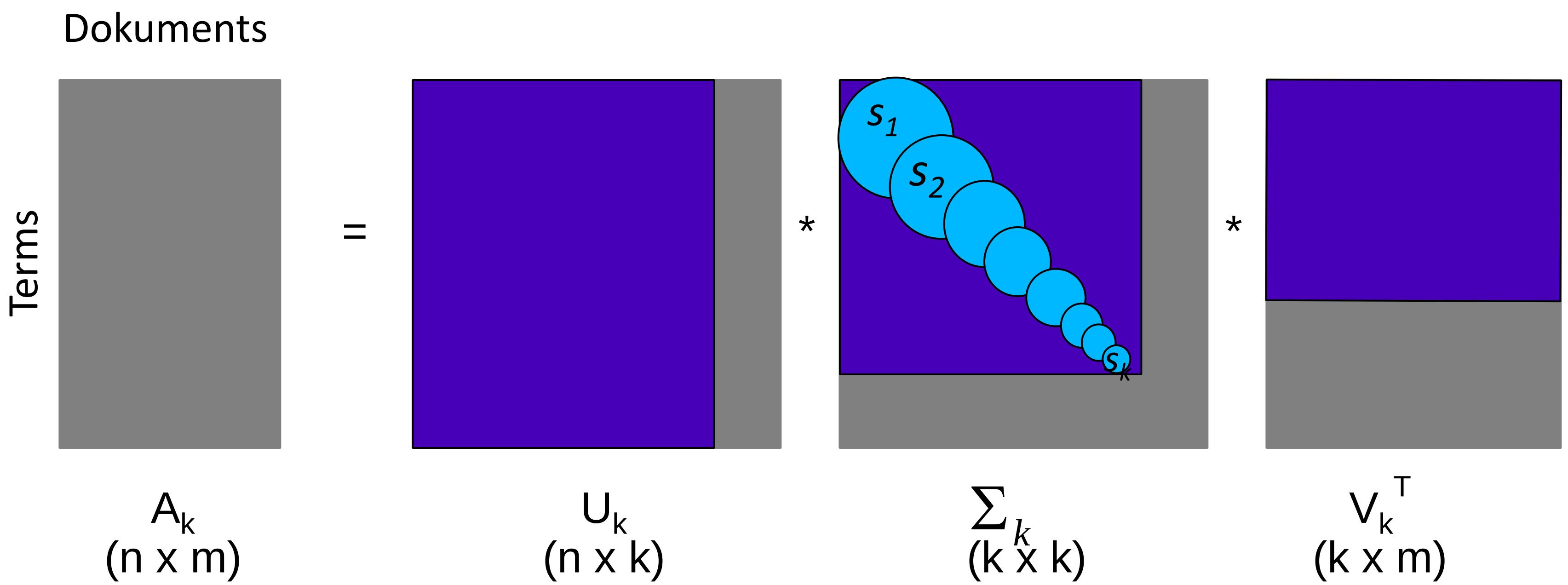
$m \times m$ | $m \times n$ | V is $n \times n$

The columns of ***U*** are orthogonal eigenvectors of $\boldsymbol{AA^T}$.

The columns of ***V*** are orthogonal eigenvectors of $\boldsymbol{A^TA}$.
Eigenvalues $\lambda_1 \ldots \lambda_r$ of $\boldsymbol{AA^T}$ are the eigenvalues of $\boldsymbol{A^TA}$.

$$\sigma_i = \sqrt{\lambda_i} \qquad \Sigma = diag(\sigma_1 \ldots \sigma_r)$$

Singular value decomposition



Latent semantic indexing 1/1

- LSI – k-reduced singular decomposition of the term-by-document matrix
- Latent semantics – hidden connections between both terms and documents determined on documents' content

- Document matrix $D_k = \mathbf{\Sigma_k} \mathbf{V_k}^{\mathbf{T}}$ (or $D_k' = \mathbf{V_k}^{\mathbf{T}}$)
- Term matrix $T_k = \mathbf{U_k} \mathbf{\Sigma_k}$ (or $T_k' = \mathbf{U_k}$)
- Query in reduced dimension $q_k = \mathbf{U_k}^T q$ (or $q_k' = \mathbf{\Sigma_k}^{-1} \mathbf{U_k}^T q$)

Latent semantic indexing 1/2

In another words. Documents are represented as linear combination of meta terms.

$d_1 = \Sigma\, w_{1i} m_i$

$d_2 = \Sigma\, w_{2i} m_i$

....

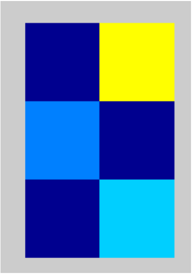
$d_n = \Sigma\, w_{ni} m_i$

Retrieval in LSI

- Similarity between two documents or a document and a query is usually calculated as normalized scalar product of their vectors of meta term.

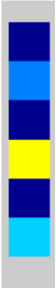
$$sim(d_k, d_l) = \frac{\sum_{i=1}^{m} w_{ki} w_{li}}{\sqrt{\sum_{i=1}^{m} w_{ki}^2} \sqrt{\sum_{i=1}^{m} w_{li}^2}}$$

Picture matrix



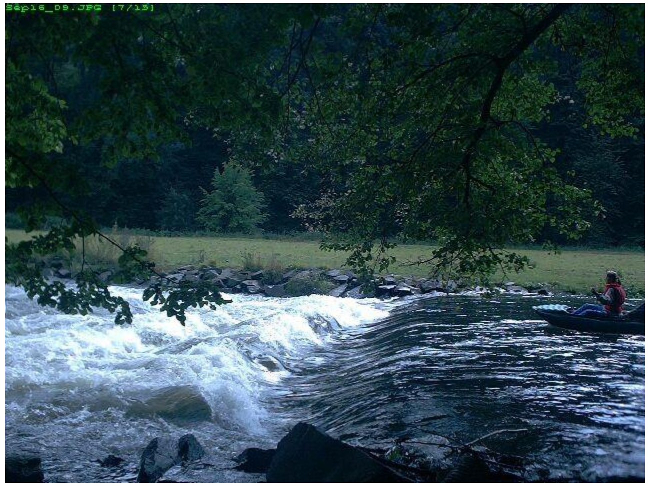
pic

$$A=\begin{pmatrix} . & 0 & . & \cdots & . \\ . & 15 & . & \cdots & . \\ . & 0 & . & \cdots & . \\ . & 40 & . & \cdots & . \\ . & 0 & . & \cdots & . \\ . & 20 & . & \cdots & . \end{pmatrix}$$



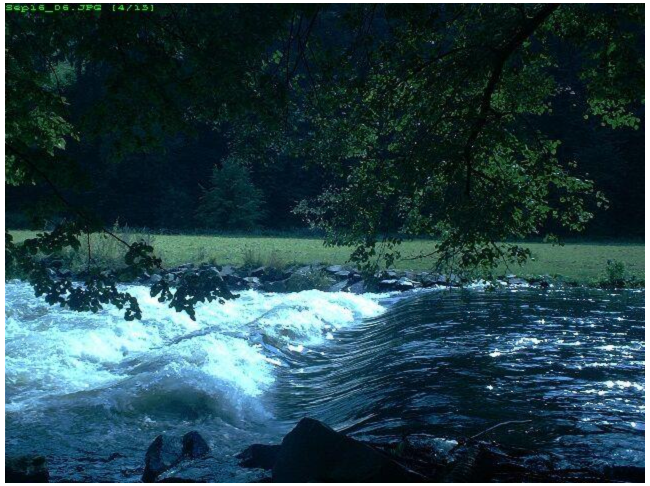
$$pic=\begin{pmatrix} 0 & 40 \\ 15 & 0 \\ 0 & 20 \end{pmatrix}$$

Retrieval in LSI



Query

Fig02
0.9740



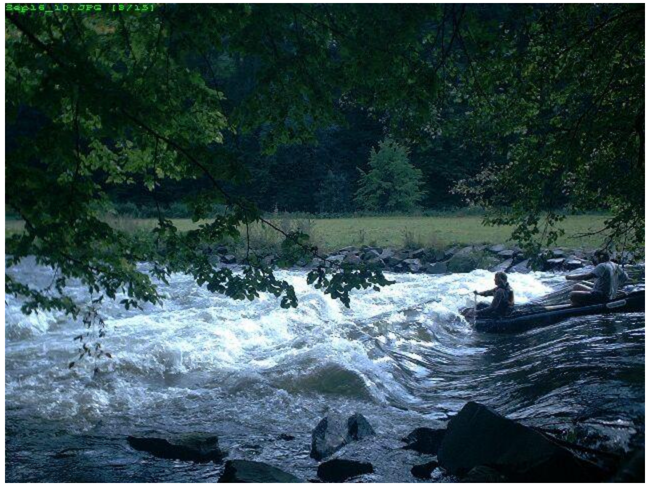


Fig06
0.3011

Retrieval in LSI

Query

Fig14
0.3640

Fig11
0.3482

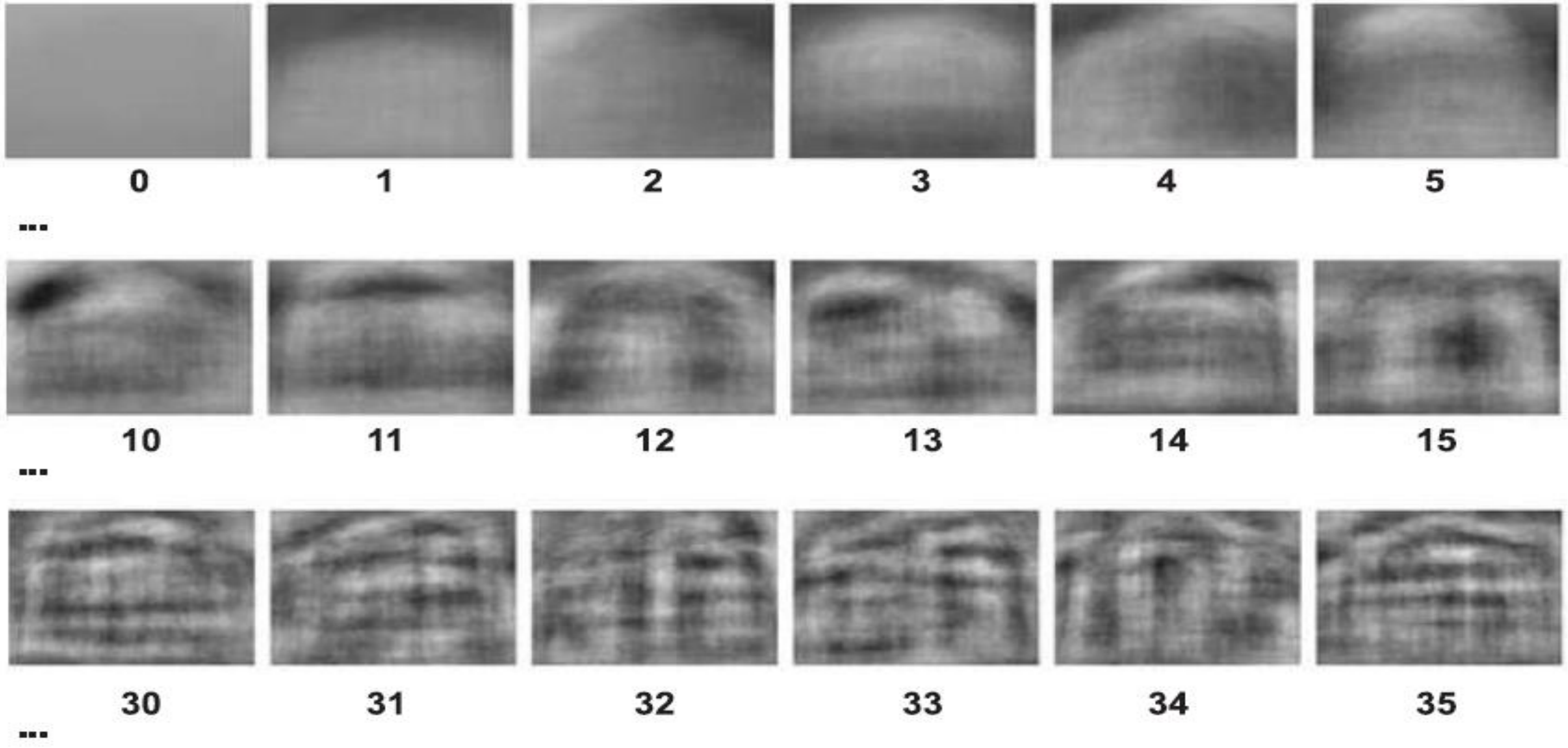
Latent semantic indexing

What is eigen-image?

Eigen-image is linear combination of pixels.

Building collection

Eigen-images



DCT

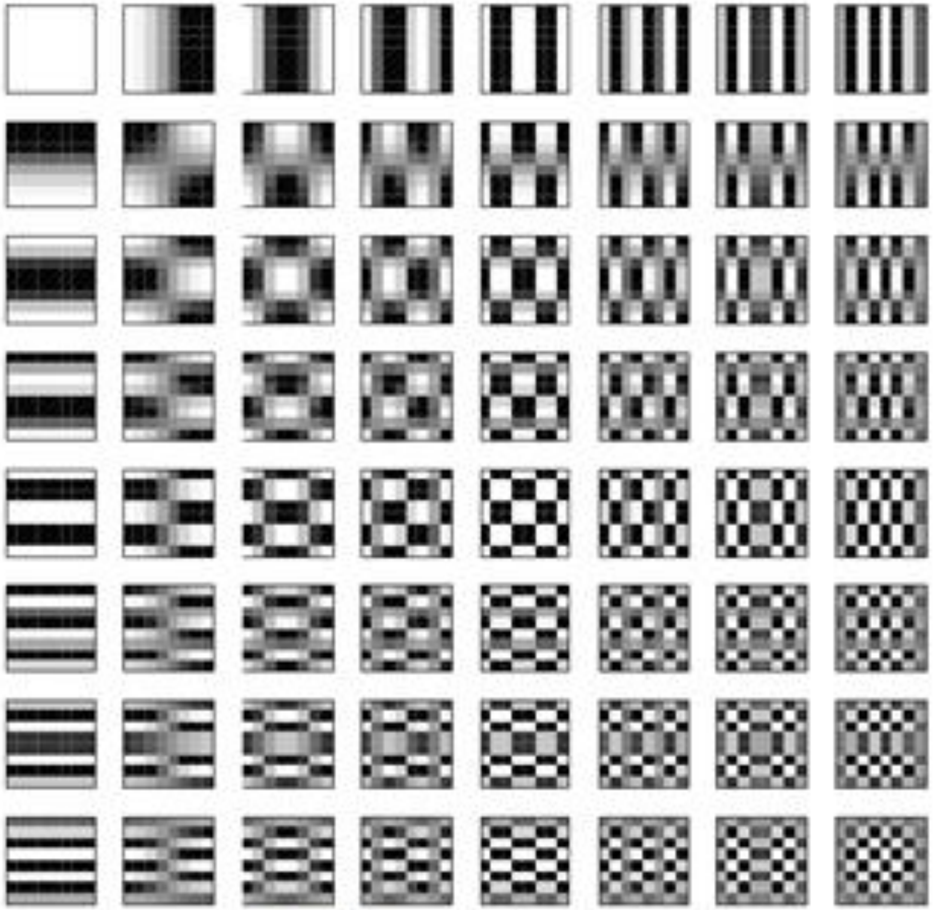
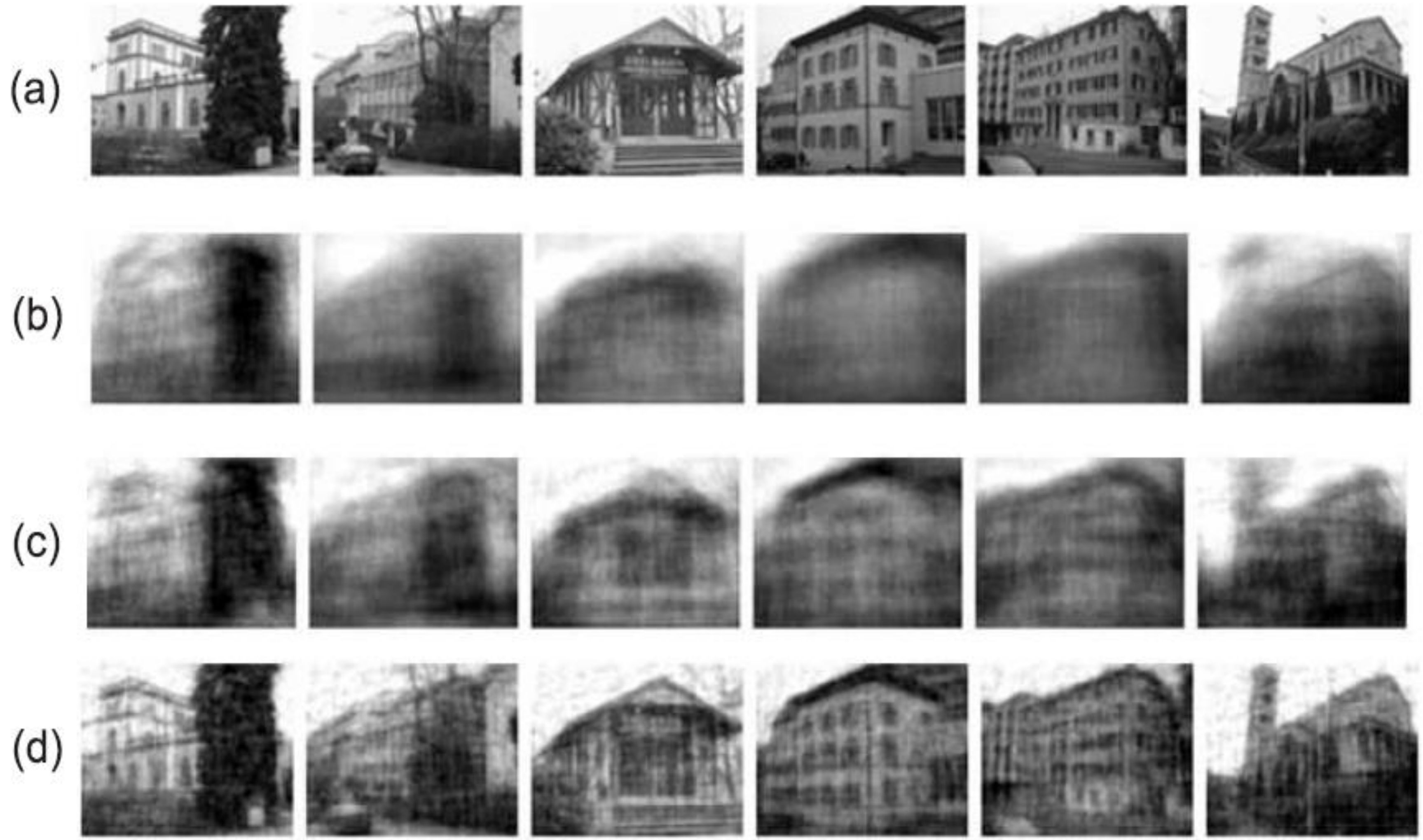


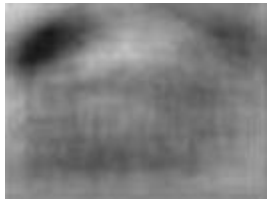
Figure 3.28 8 × 8 DCT basis patterns



(b) k = 15, (c) k = 50, (d) k = 250

Eigen-images

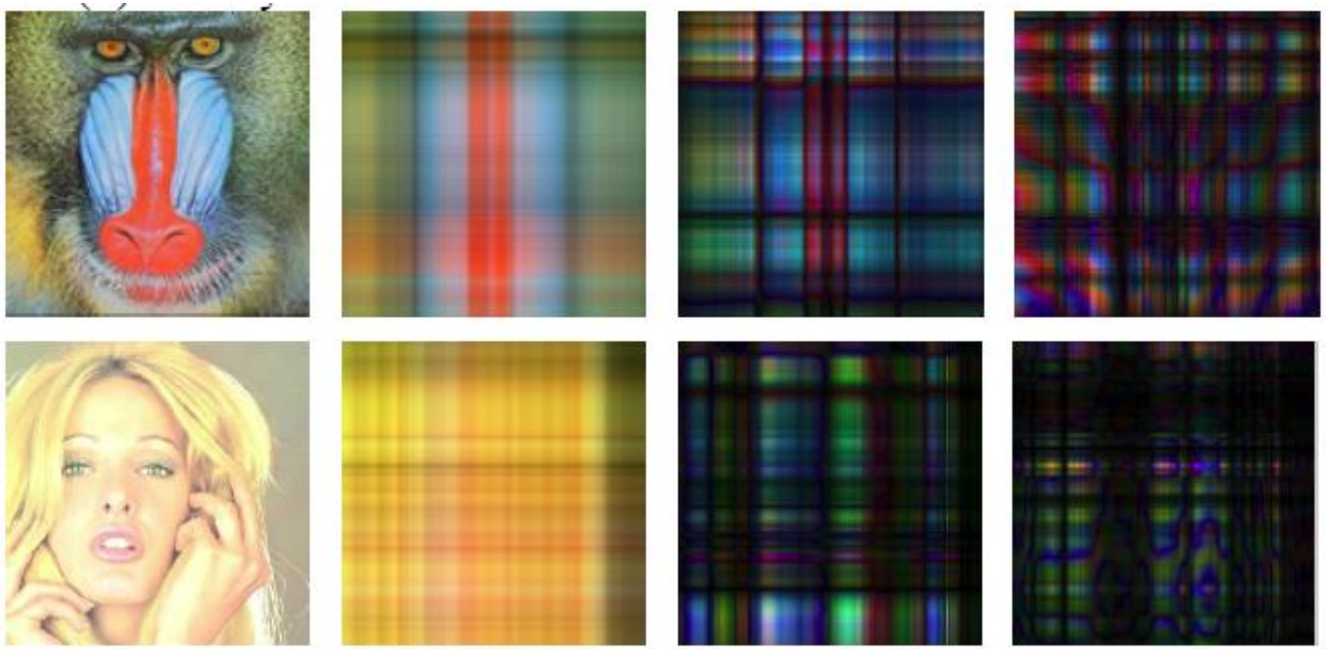
 = s_1  $+s_2$  $+s_3$ 

$+s_4$  $+s_5$  $+s_6$  $+s_7$ 

...

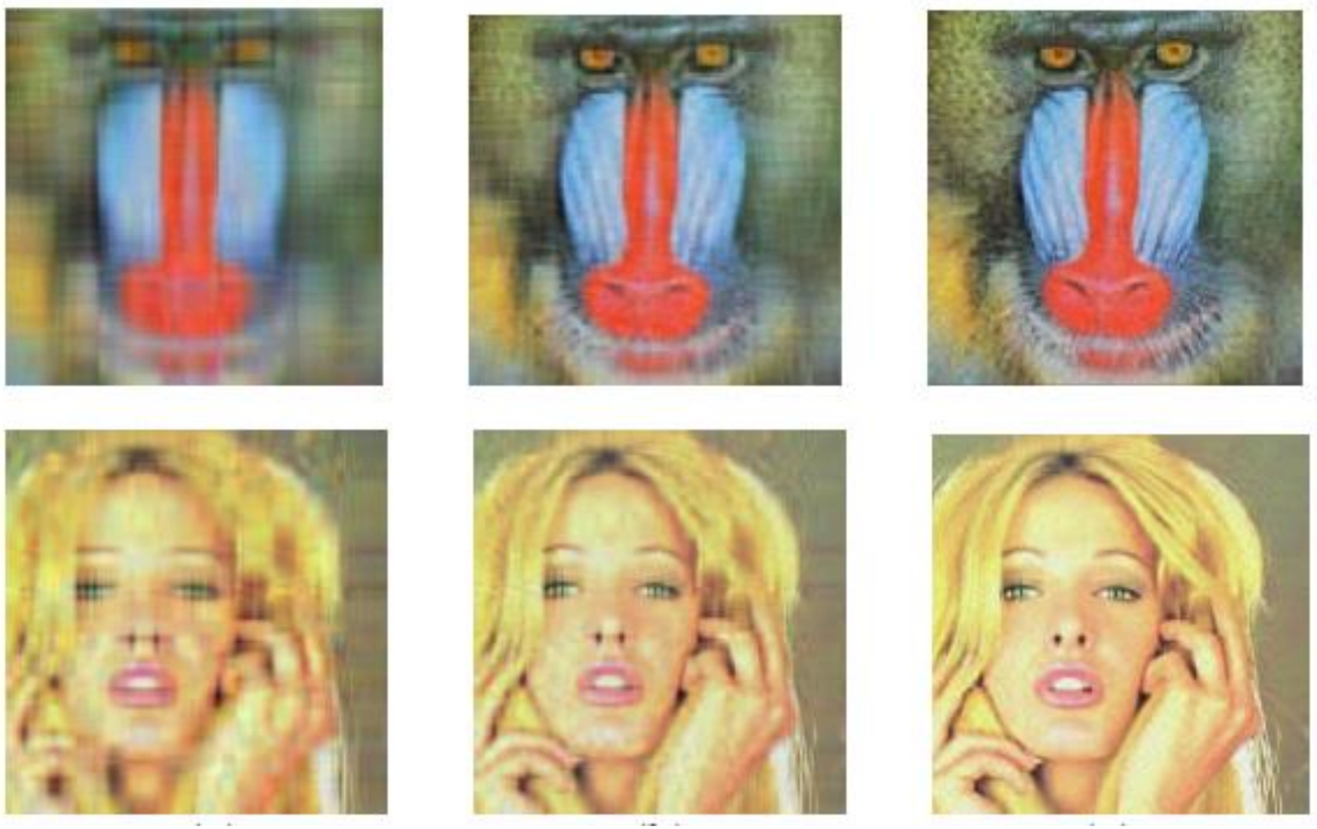
Quaternion SVD

Selected eigen-images $X + Ri + Gj + Bk$



SC Pei, JH Chang, JJ Ding, Quaternion matrix singular value decomposition and its applications for color image processing, Image Processing, ICIP, 2003.

Quaternion SVD



SC Pei, JH Chang, JJ Ding, Quaternion matrix singular value decomposition and its applications for color image processing, Image Processing, ICIP, 2003.

OCTONIONS

There are exactly four normed division algebras: the real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, quaternions $\mathbb{H}$, and octonions $\mathbb{O}$.

The real numbers are the dependable breadwinner of the family, the complete ordered field we all rely on.

The complex numbers are a slightly ashier but still respectable younger brother: not ordered, but algebraically complete.

The quaternions, being noncommutative, are the eccentric cousin who is shunned at important family gatherings.

The octonions are the crazy old uncle nobody lets out of the attic: they are nonassociative.

OCTONIONS

Theorem 1. $\mathbb{R}, \mathbb{C}, \mathbb{H}$ *and* $\mathbb{O}$ *are the only normed division algebras.*

Theorem 2. $\mathbb{R}, \mathbb{C}, \mathbb{H}$ *and* $\mathbb{O}$ *are the only alternative division algebras.*

The first theorem goes back to an 1898 paper by Hurwitz. It was subsequently generalized in many directions, for example, to algebras over other fields.

A version of the second theorem appears in an 1930 paper by Zorn. Note that we did *not* state that R*;*C*;*H and O are the only division algebras.

This is not true. For example, we have already described a way to get 4-dimensional division algebras that do not have multiplicative inverses. However, we do have this fact:

Theorem 3. *All division algebras have dimension* 1*;* 2*;* 4*; or* 8*.*

This was independently proved by Kervaire and Bott in 1958.

Number construction

Hyperreal number

Recall: The Axiomatic Definition of $\mathbb{R}$

Definition: We define the structure $(\mathbb{R},+,\cdot,<)$ by the following axioms:

1) $(\mathbb{R},+,\cdot)$ is a field, i.e. $+$ and $\cdot$ satisfy the usual properties, e.g. $x\cdot(y + z) = x\cdot y + x\cdot z$.

2) $(\mathbb{R},<)$ is a linear order, i.e. for any x and y, either

$x < y$ or $x = y$ or $x > y$, and the relation $<$ is transitive, i.e. for all x,y, and z; $x < y < z \Rightarrow x < z$.

3) $<$ is congruent with respect to $+$ and $\cdot$, i.e. for all x,y, and z; $x < y \Rightarrow x + z < y + z$. Also, $x < y$ and $z > 0 \Rightarrow xz < yz$.

4) Every nonempty subset of $\mathbb{R}$ that is bounded above, has a least upper bound.

Question: Are these axioms consistent?

I.e.: Is there any mathematical structure that satisfies all of Axioms 1-4?

Theorem: Yes. In fact, there is a unique structure $(\mathbb{R},+,\cdot,<)$ (up to isomorphism) satisfying all of Axioms 1-4.

Note: This means that any other structure $(\mathbb{R}',+',\cdot',<')$ satisfying the axioms is just a renaming of $(\mathbb{R},+,\cdot,<)$, i.e. there is a bijection $f:\mathbb{R}\to\mathbb{R}'$, that respects the arithmetic operations and the order.

Question: How is $\mathbb{R}$ constructed?

- **Step 1:** We recursively define the natural numbers together with their addition and multiplication.
- **Step 2:** We define the non-negative rational numbers $\mathbf{Q}^+$ as the set of equivalence classes of pairs of positive natural numbers (x,y) under the equivalence:
$$(x_1,y_1) \equiv (x_2,y_2) \text{ iff } (x_1y_2 = x_2y_1)$$
- **Reason:** A pair (x,y) just denotes x/y.
- Also, we define addition and multiplication of these.
- **Step 3:** We define the set of all rational numbers as the union $\mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$, where $\mathbb{Q}^-$ is just an identical copy of $\mathbb{Q}^+$, together with addition and multiplication.

Construction of $\mathbb{R}$, Step 4.

- **Definition:** A **Cauchy sequence** (x_n) is a sequence satisfying $\lim_n \sup_k |x_{n+k} - x_n| = 0$
- **Example:** Any sequence of rationals (x_n) of the form $x_n = 0.d_1 d_2 d_3 \ldots d_n$ is Cauchy. In particular, the sequence 0.9,0.99,0.999,… is Cauchy.
- **Step 4:** $\mathbb{R}$ is the set of equivalence classes of Cauchy sequences (x_n) of rationals under the equivalence: $(x_n) \equiv (y_n)$ iff $\lim_n (x_n - y_n) = 0$
- **Note:** We simply identify each Cauchy sequence with its limit.

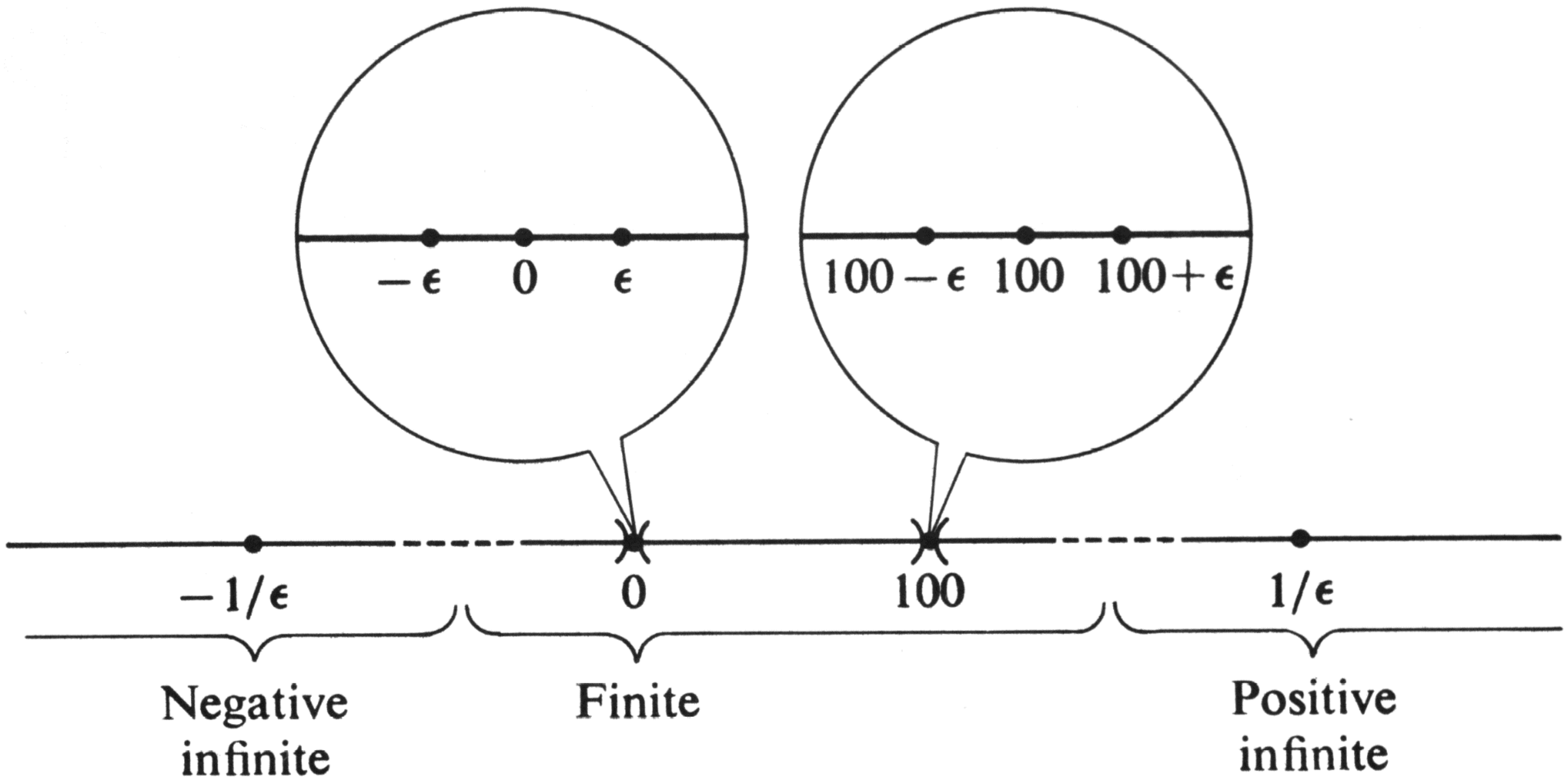
Recall

- **Definition:** A number N is infinite iff $N > n$ for all natural numbers n.
- **Fact:** There are no infinite numbers in $\mathbb{R}$.
- Thus, to introduce infinite numbers, we must abandon one of Axioms 1-4.
- We decide to abandon Axiom 4 (the Completeness Axiom), and introduce the following axiom:
- **Axiom 4*:** There is an infinite number N.
- **Question:** Are Axioms 1,2,3,4* consistent?

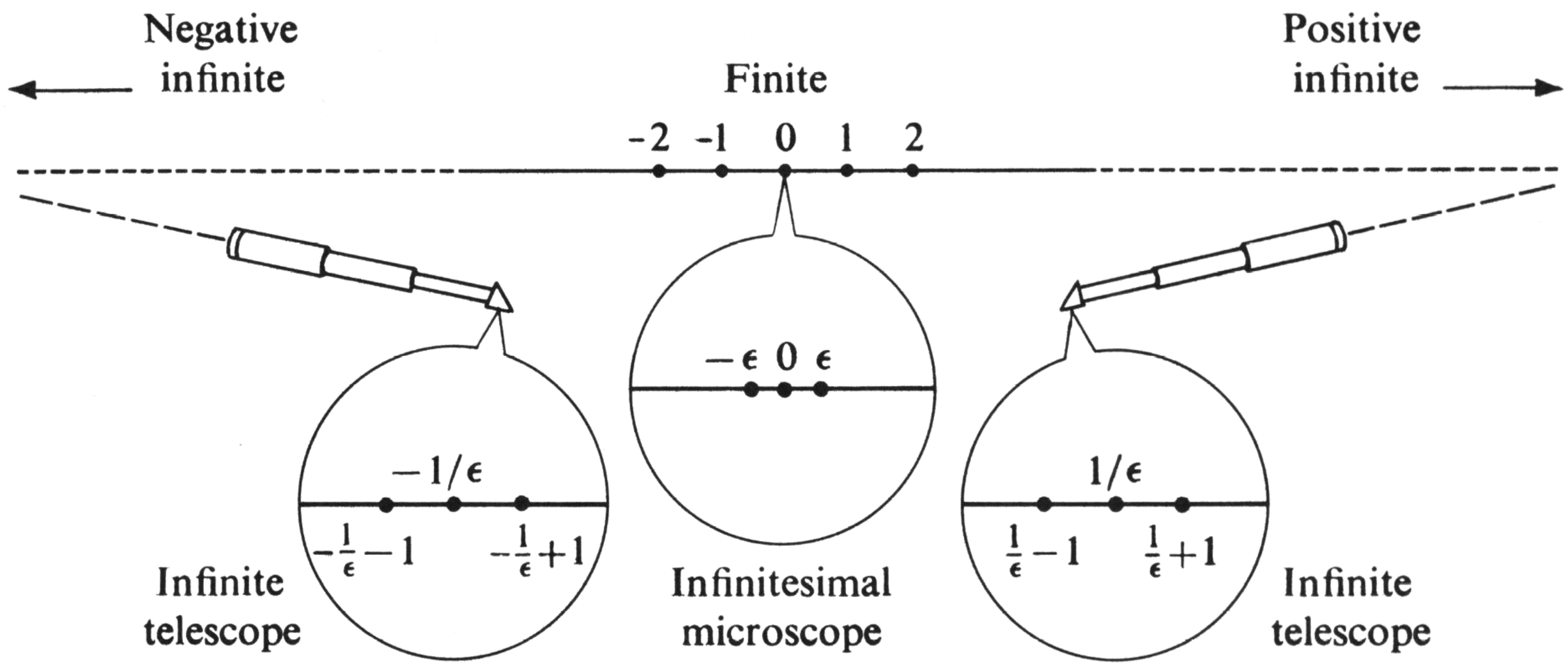
Answer: Yes.

- **Theorem:** There are many possible structures $(\mathbb{R}^*,+^*,\cdot^*,<^*)$, satisfying Axioms 1,2,3,4^*.
- In each of these structures there is an infinite number N, i.e. $N > n$, for all natural numbers n.
- In fact, there are infinitely many such infinite numbers, e.g. $N+r$, with $r\in \mathbb{R}$, and rN, with $r > 0$.
- Also, there must also be a positive infinitesimal number $\varepsilon = 1/N$, i.e. $0 < \varepsilon < 1/n$, for all natural numbers n.
- In fact, there are infinitely many of those.

Infinites and Infinitesimals Picture 1



Infinites and Infinitesimals Picture 2



Construction of the Hyperreals $\mathbb{R}^*$

- We start with the set of infinite sequences (x_n) of real numbers.
- Define addition and multiplication componentwise,
- i.e. $(x_n) + (y_n) = (x_n + y_n)$, and $(x_n)\cdot(y_n) = (x_n\cdot y_n)$.
- **Problem:** The product of the two sequences $(0,1,0,1,0,1,\dots)\cdot(1,0,1,0,1,0,\dots) = (0,0,0,0,0,0,\dots)$
- Since $(0,0,0,0,0,0,\dots)$ is the zero element, one of the sequences $(0,1,0,1,0,1,\dots),(1,0,1,0,1,0,\dots)$ is declared zero.
- **Question:** How?

The Need of Free Ultrafilters

- **Definition:** A **filter** over the set of natural numbers **N** is a set F of subsets of **N**, such that:
- 1) $\emptyset \notin F$
- 2) $(A \in F$ and $A \subseteq B) \Rightarrow B \in F$
- 3) $(A \in F$ and $B \in F) \Rightarrow (A \cap B) \in F$
- An **ultrafilter** F is a filter satisfying the extra condition:
- 4) $(A \cup B) = \mathbf{N} \Rightarrow (A \in F$ or $B \in F)$
- **Example:** For any number $n \in \mathbf{N}$, the set of subsets defined by $F = \{A|\ n \in A\}$ is an ultrafilter over **N**.
- A **free ultrafilter** is an ultrafilter containing no finite sets.
- **Fact:** There are infinitely many free ultrafilters.

Construction of $\mathbb{R}^*$ (cont.)

- Given a free ultrafilter F, we define the following relation on the set of infinite sequences of real numbers:
- $(x_n) \equiv (y_n)$ iff $\{n: x_n = y_n\} \in F$.
- **Fact:** $\equiv$ is an equivalence relation, that respects the operations $+$ and $\cdot$ defined on the sequences.
- $(\mathbb{R}^*,+,\cdot)$ is the set of equivalence classes of sequences together with the operations defined componentwise.
- Also, defining $(x_n) < (y_n)$ iff $\{n: x_n < y_n\} \in F$, we get the ordered field of hyperreals $(\mathbb{R}^*,+,\cdot,<)$

Behavior of $\mathbb{R}^*$

- **Theorem:** The structure $(\mathbb{R}^*,+,\cdot,<)$ is an ordered field that behaves like R in a very strong sense, as illustrated by:
- **The Extension Principle:** $\mathbb{R}^*$ extends $\mathbb{R}$; $+$, $\cdot$, and in $\mathbb{R}^*$ extend those of $\mathbb{R}$. Moreover, each real function f on $\mathbb{R}$ extends to a function f^* on $\mathbb{R}^*$. We call f^* the natural extension of f.
- **The Transfer Principle:** Each valid first order statement about $\mathbb{R}$ is still valid about $\mathbb{R}^*$, where each function is replaced by its natural extension.

The Standard Part Principle

- **Definitions:**
- A number x in $\mathbb{R}^*$ is called finite iff $|x| < r$ for some positive real number r in $\mathbb{R}$.
- A number x in $\mathbb{R}^*$ is called infinitesimal iff $|x| < r$ for every positive real number r in $\mathbb{R}$.
- Two numbers x and y are called infinitely close to each other ($x \approx y$) iff $x - y$ is infinitesimal.
- **The Standard Part Principle:** Every finite hyperreal x is infinitely close to a unique real number r. r is called the standard part of x ($\text{st}(x)$).

Nonstandard Analysis

- Using hyperreals we define:

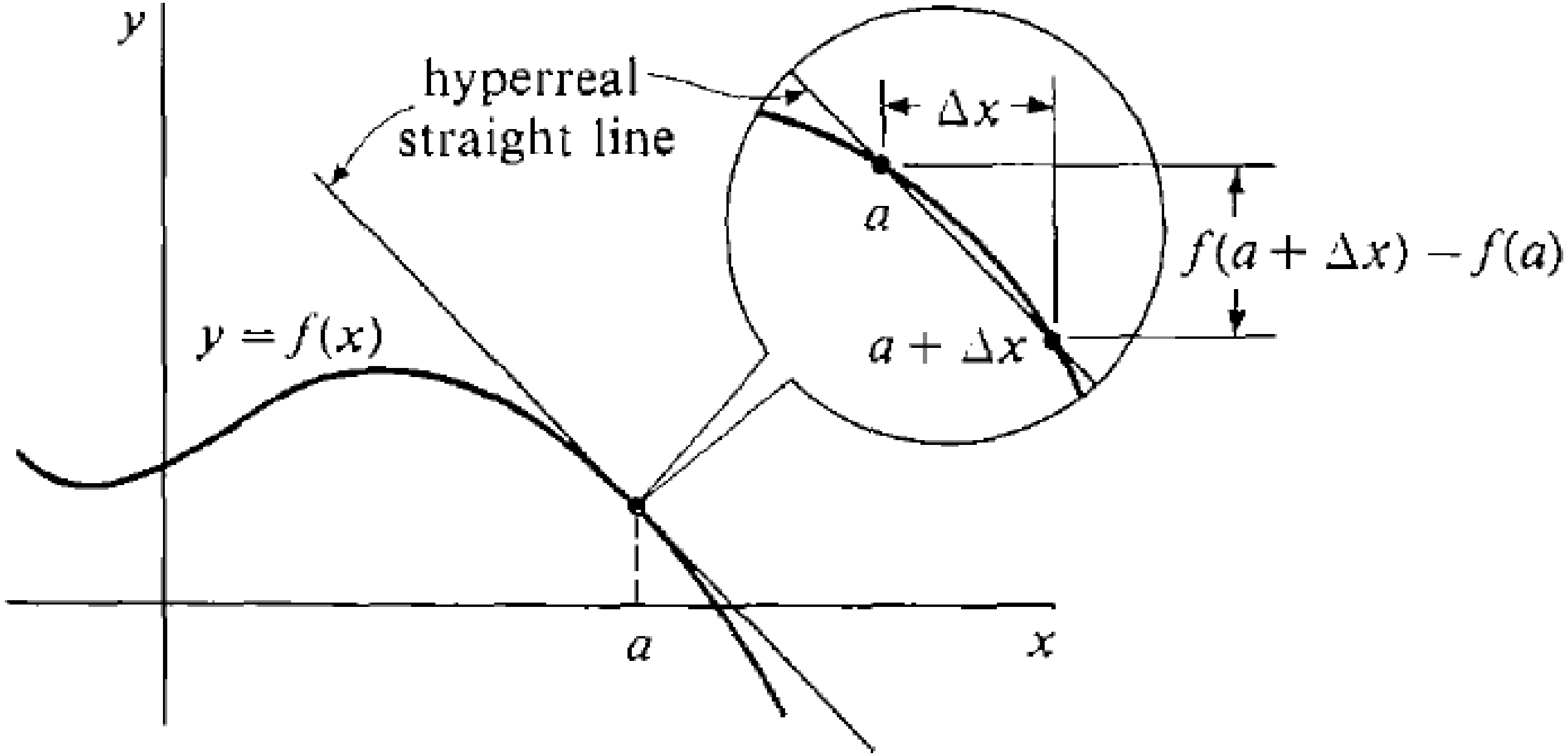
$$f'(x) = st\left(\frac{f(x+\Delta x) - f(x)}{\Delta x} \right)$$

for every (any) nonzero infinitesimal Δx, and:

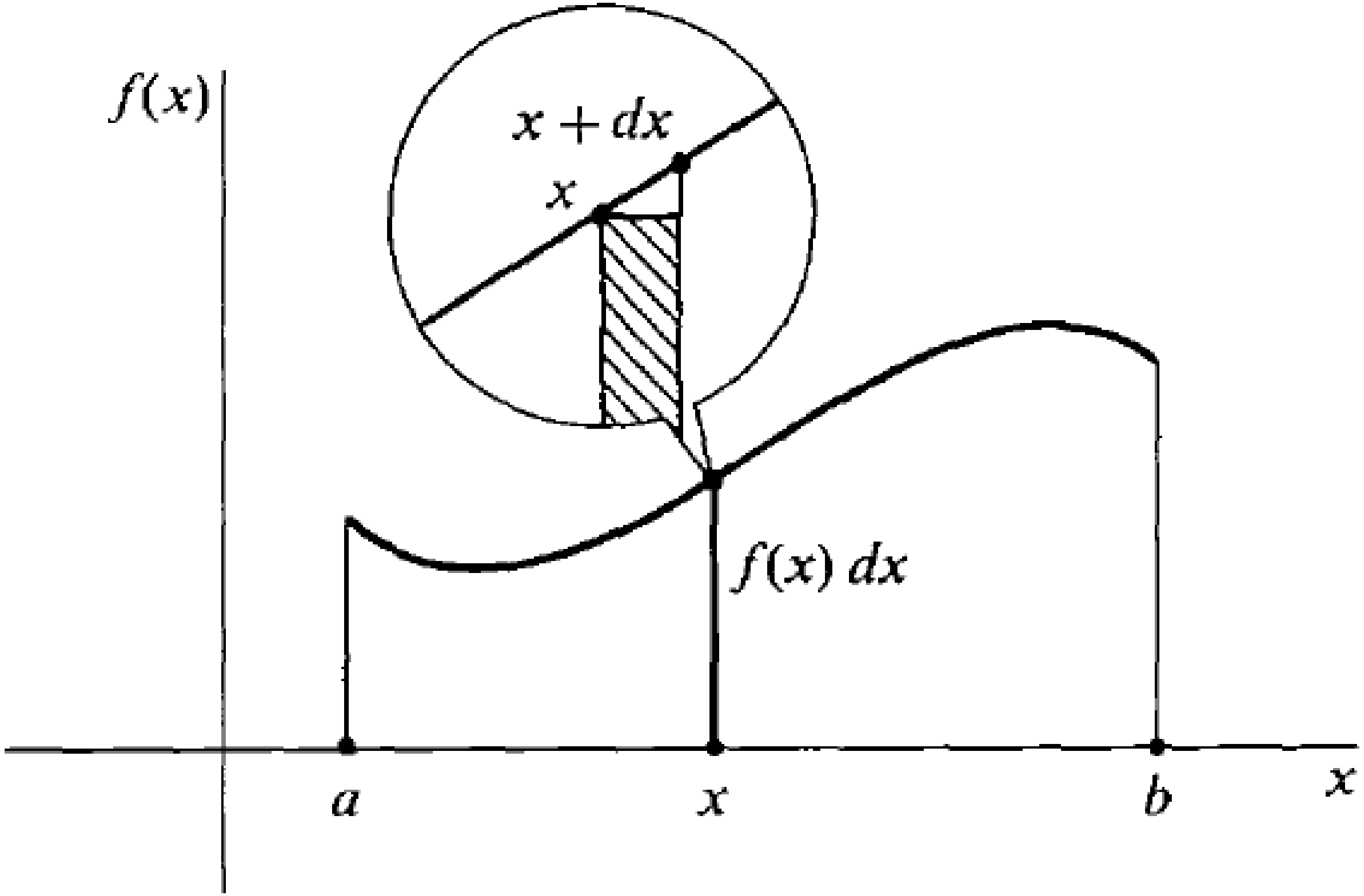
$$\int_a^b f(x)dx = st\left(\sum_{k=1}^{N} f(a+k\Delta x)\Delta x \right), \ \Delta x = \frac{b-a}{N}$$

for every (any) nonzero positive infinite integer N.

Picture of the Derivative



Picture of the Definite Integral



Number construction – cont.

Surreal number

Surreal number

Donald E. Knuth, Nadreálná čísla

Pokroky matematiky, fyziky a astronomie, Vol. 23 (1978), No. 2, 66--76

The Construction of $\mathbb{R}$ from $\mathbb{Q}$.

- Recall that the set of reals $\mathbb{R}$ can be constructed from the set of rationals $\mathbb{Q}$ using Cauchy sequences.
- A real number is defined as an equivalence class of Cauchy sequences under the equivalence:

$$(x_n) \equiv (y_n) \text{ iff } \lim_n (x_n - y_n) = 0$$

- A modification on this idea lead to the set $\mathbb{Q}^*$ of hyperreal numbers.
- Another alternative of constructing $\mathbb{Q}$ is to use Dedekind cuts.

Dedekind Cuts

- **Definition:** A Dedekind Cut of $\mathbb{Q}$ is a pair (X,Y) of nonempty sets of $\mathbb{Q}$, such that:
- 1) X and Y partition $\mathbb{Q}$, i.e. $X \cup Y = \mathbb{Q}$ and $X \cap Y = \varnothing$
- 2) X < Y, i.e. for all $x \in X$, $y \in Y$, $x < y$
- 3) X has no greatest element
- **Example:** For any real $r \in \mathbb{R}$, we get the Dedekind cut: $X = \{x \in \mathbb{Q} : x < r\}$; $Y = \{y \in \mathbb{Q} : r \geq y\}$.
- Also, each Dedekind cut uniquely determines a real number.
- We define $\mathbb{R}$ to be the set of Dedekind cuts.

Defining the Surreal Numbers

- Inspired by Dedekind cuts, we get the following: definition:
- 1) A **surreal number** x is a pair (X_L, X_R), where:
  - a) X_L and X_R are themselves sets of surreals
  - b) $X_L < X_R$, i.e. for all $x_L \in X_L$, $x_R \in X_R$, $x_L < x_R$
- 2) For two surreals $x = (X_L, X_R)$, $y = (Y_L, Y_R)$,
  $y < x$ iff not $x \leq y$
- 3) Also, $x \leq y$
  - a) $x < Y_R$, i.e. for all $y_R \in Y_R$, $x < y_R$
  - b) $X_L < y$, i.e. for all $x_L \in X_L$, $x_L < y$
- **Note:** This definition is "very" recursive.

What could a recursive definition do?

- Though our definition of surreals is recursive, we get the following examples:
- The first surreal we can construct is $0 = (\{\},\{\})$
- **Note:** The empty set {} is a set of surreals, whatever they are.
- Also, for all $x_L, x_R \in \{\}$, $x_L < x_R$. (*)
- This is true, since the statement (*) is logically equivalent to: $(\forall x_L, x_R)(x_L, x_R \in \{\} \Rightarrow x_L < x_R)$.
- We say that such statements are vacuously true.
- Also, $\{\} < 0 < \{\}$. Thus, $(\{\},\{\}) \leq (\{\},\{\})$, i.e. $0 \leq 0$.

More Surreals

- With the hyperreal $0 = (\{\},\{\})$ we also get:
- $1 = (\{0\},\{\})$. **Note:** $\{0\} < \{\}$.
- $-1 = (\{\},\{0\})$: **Note:** $\{\} < \{0\}$.
- These names are justified by the following:
- **Fact:** $-1 < 0 < 1$
- **Proof:** Since $0 \le 0$, $(\{0\},\{\}) \le (\{\},\{\}) = 0$ is not true. Thus, $(\{\},\{\}) < (\{0\},\{\})$, i.e. $0 < 1$.
- Also, $(\{\},\{\}) \le (\{\},\{0\})$ is not true. Thus, $(\{\},\{0\}) < (\{\},\{\})$, i.e. $0 < 1$.
- However, $(\{0\},\{0\})$ is NOT a surreal number, since it is not true that $0 < 0$.

A Simpler Notation:

- If $x = (\{x_{L1}, x_{L2},\ldots\},\{x_{R1}, x_{R2},\ldots\})$, we can simply denote it by: $x = \{x_{L1}, x_{L2},\ldots|x_{R1}, x_{R2},\ldots\}$, as if x is just a set with left and right elements. Thus:
- $0 = \{|\}$
- $1 = \{0|\}$
- $-1 = \{|0\}$
- **Note:** The notation $x = \{x_{L1}, x_{L2},\ldots|x_{R1}, x_{R2},\ldots\}$ does not necessarily mean that the two sets

  $$\{x_{L1}, x_{L2},\ldots\} \text{ and } \{x_{R1}, x_{R2},\ldots\}$$

  are finite or countable.

More Surreals:

- $0 = \{|\}$
- $1 = \{0|\}$
- $2 = \{1|\}$
- $3 = \{2|\}$, actually $3 = (\{(\{(\{(\{\},\{\})\},\{\})\},\{\})\},\{\})$.
- ... (These look like the ordinals)
- $\omega = \{0,1,2,3,\ldots|\}$
- **Fact:** $0 < 1 < 2 < 3 < \ldots < \omega$
- In general: $\{x_{L1}, x_{L2},\ldots|x_{R1}, x_{R2},\ldots\}$ defines a surreal x, such that: $x_{L1}, x_{L2},\ldots< x < x_{R1}, x_{R2},\ldots$

Negative Surreals:

- $0 = \{|\}$, $-1 = \{|0\}$, $-2 = \{|-1\}$, $-3 = \{|-2\}$
- ... (These are the negative ordinals)
- Also, $-\omega = \{|\ldots,-3,-2,-1,0\}$
- **In general:** For a surreal $x = \{x_{L1},x_{L2},\ldots|x_{R1},x_{R2},\ldots\}$, we define: $-x = \{-x_{R1},-x_{R2},\ldots|-x_{L1},-x_{L2},\ldots\}$.
- $-x$ is called the negation of x.
- **Note:** This definition is again recursive!
- Our notations are justified, e.g. $-2 = -\{1|\} = \{|-1\}$.
- Also, $-0 = -\{|\} = \{|\} = 0$.

Equality of Surreals

- **Example:** Let $x = \{-1|1\}$.
- One can show that $x \leq 0$ and $0 \leq x$.
- If $\leq$ is a linear order, we need to identify x with 0.
- **Definition:** For two surreals x and y, we write $x = y$ iff both $x \leq y$ and $y \leq x$. (*)
- **Note:** Actually, (*) above defines an equivalence relation, and the surreals are defined to be its equivalence classes.
- **Examples:** $\{-2,-1|0,1\} = \{-1|1\} = \{|\} = 0$,
- $\{1,2,4,8,16,\ldots|\} = \{0,1,2,3,\ldots|\} = \omega$

Addition of Surreals:

- If $x = \{x_{L1},\ldots|x_{R1},\ldots\}$ and $y = \{y_{L1},\ldots|y_{R1},\ldots\}$ are surreals, define: $x{+}y = \{x_{L1}{+}y,\ldots,x{+}y_{L1},\ldots|x_{R1}{+}y,\ldots,x{+}y_{R1},\ldots\}$
- **Motivation:** A surreal $x = \{x_{L1},\ldots|x_{R1},\ldots\}$ can be considered as a special kind of a game played between two players L and R.
- If L is next, he chooses one of the left options $x_{L1},\ldots$.
- If R is next, she chooses one of the right options $x_{R1},\ldots$.
- Thus, $x{+}y$ is both x and y played in parallel. Each player chooses to move in any one of them, leaving the other unchanged.
- The above definition is again recursive!

Examples of Sums:

- For surreals $x = \{x_{L1},\ldots|x_{R1},\ldots\}$, $y = \{y_{L1},\ldots|y_{R1},\ldots\}$, $x+y = \{x_{L1}+y,\ldots,x+y_{L1},\ldots|x_{R1}+y,\ldots,x+y_{R1},\ldots\}$
- **Examples:**
- $1 + 1 = \{0|\} + \{0|\} = \{0+1,1+0|\} = \{1|\} = 2$
- $2 + 1 = \{1|\} + \{0|\} = \{1+1,2+0|\} = \{2|\} = 3$, etc..
- $1 + (-1) = \{0|\} + \{|0\} = \{0+(-1)|1+0\} = \{-1|1\} = 0$.
- $\omega + 1 = \{1,2,3,\ldots,\omega|\} = \{\omega|\}$
- $\omega + 2 = \{1,2,3,\ldots,\omega+1|\} = \{\omega+1|\}$, etc..
- $-\omega + (-1) = \{|-\omega,\ldots,-3,-2,-1,0|\} = \{|-\omega\}$, etc..

Exercises:

- Show that for all surreals x, y, z:
- $x + y = x + y$
- $(x + y) + z = x + (y + z)$
- $x + 0 = x$
- $x + (-x) = 0$
- Thus, the class of surreals with addition behaves like a group.
- **Note:** the class of surreals is a proper class (too big to be a set). Thus, it's not a group.

More Examples of Sums:

- For surreals $x = \{x_{L1},\ldots|x_{R1},\ldots\}$, $y = \{y_{L1},\ldots|y_{R1},\ldots\}$, $x+y = \{x_{L1}+y,\ldots,x+y_{L1},\ldots|x_{R1}+y,\ldots,x+y_{R1},\ldots\}$
- **Examples:**
- $\{0|1\} + \{0|1\} = 1$, thus we call $\{0|1\} = ½$
- $\{0|½\} + \{0|½\} = ½$, thus we call $\{0|½\} = ¼$
- In general, we can get the set **D** of all dyadic fractions: $(2k+1)/2^{n+1} = \{k/2^n|(k+1)/2^n\}$
- **Question:** Where are the rest of the reals?
- **Answer:** $\pi = \{d\in\mathbf{D}: d < \pi \mid d\in\mathbf{D}: d > \pi\}$

Multiplication of Surreals:

- If $x = \{x_{L1},\ldots|x_{R1},\ldots\}$, $y = \{y_{L1},\ldots|y_{R1},\ldots\}$, are surreals, define xy to be the surreal:
- $xy=\{x_{L1}y + xy_{L1} - x_{L1}y_{L1},\ldots, x_{R1}y + xy_{R1} - x_{R1}\,y_{R1},\ldots|$
  $x_{L1}y + xy_{R1} - x_{L1}y_{R1},\ldots, x_{R1}y + xy_{L1} - x_{R1}y_{L1},\ldots\}$
- The definition is again recursive!
- **Theorem:** Multiplication has all the required properties. E.g., for all surreals x,y,z,
- $xy = xy$, $(xy)z = x(yz)$, $x1 = x$, and
- For all $x \neq 0$, there is x^{-1}, such that $x(x^{-1}) = 1$.
- Also, $x(y + z) = xy + xz$, and $x0 = 0$.

The Largest Ordered Field

- **Theorem:** The class of surreals behaves like an ordered field. Moreover, it includes a copy of every ordered field.
- In particular, it includes all hyperreals.
- E.g. $\omega^{-1} = \{0|\ldots,¼,½,1\}$ is an infinitesimal.
- The class of surreals includes the class of all ordinals, and consequently all cardinals.
- It also includes other stuff like $-\omega$, $\omega_1/2$, etc..
- **Remember:** The class of surreals is too large to be a set.

Conclusion