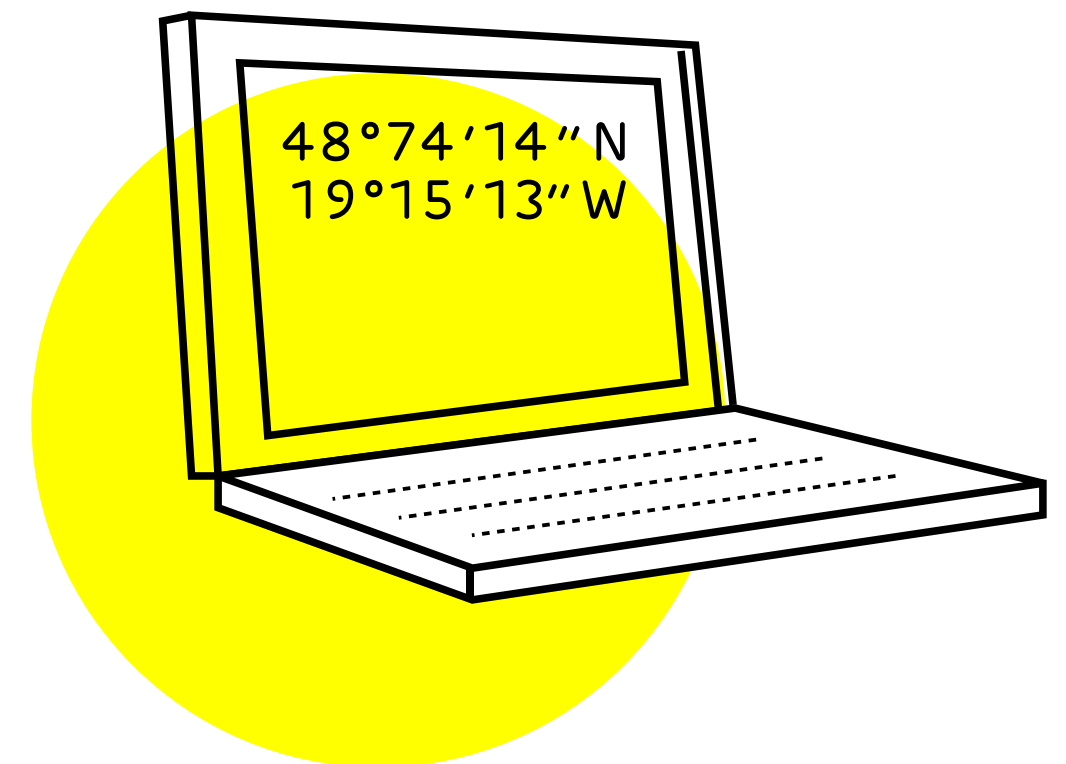
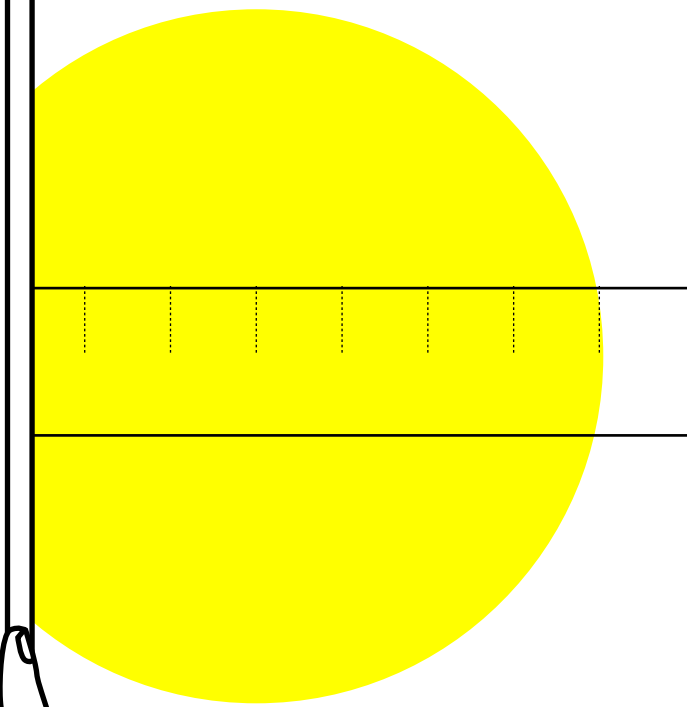


**GRAPHIC  
DESIGN  
PRINCIPLES**

**POSTER**





**01**

**02**

**03**

**04**

**05**

**Definition of graphic design**

**Graphic design principles**

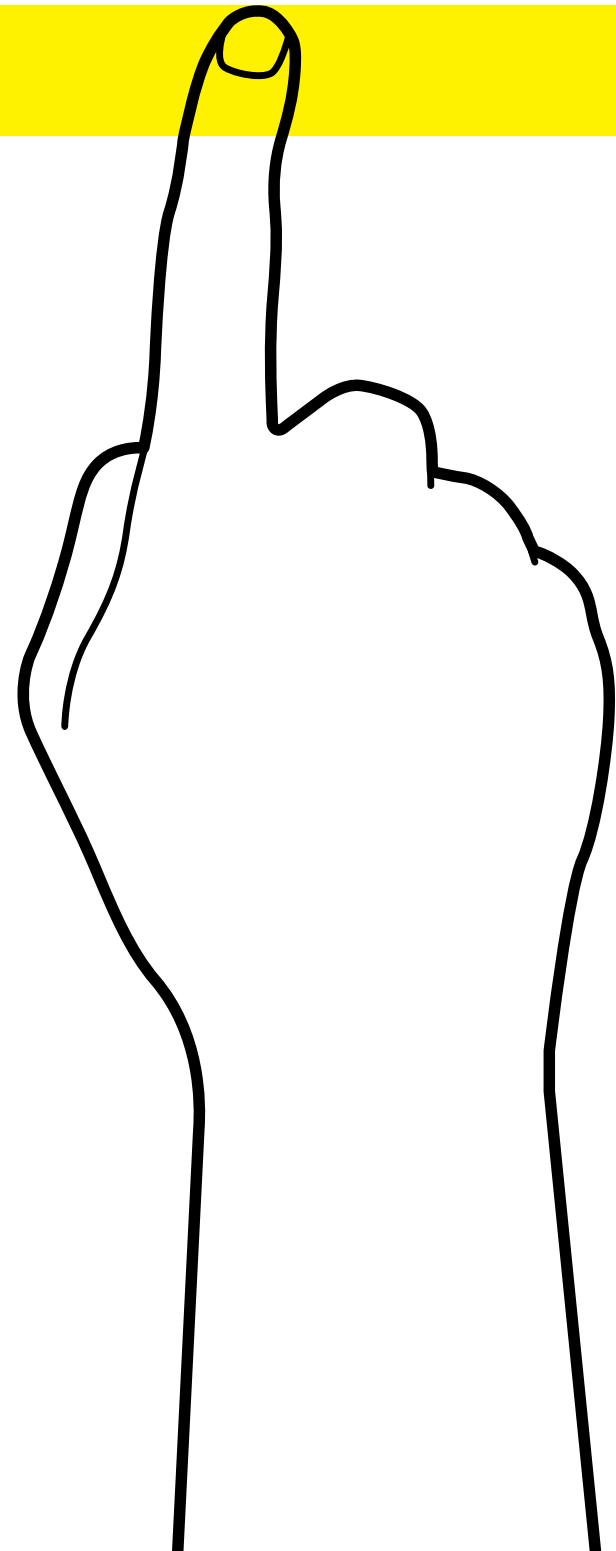
**Typography**

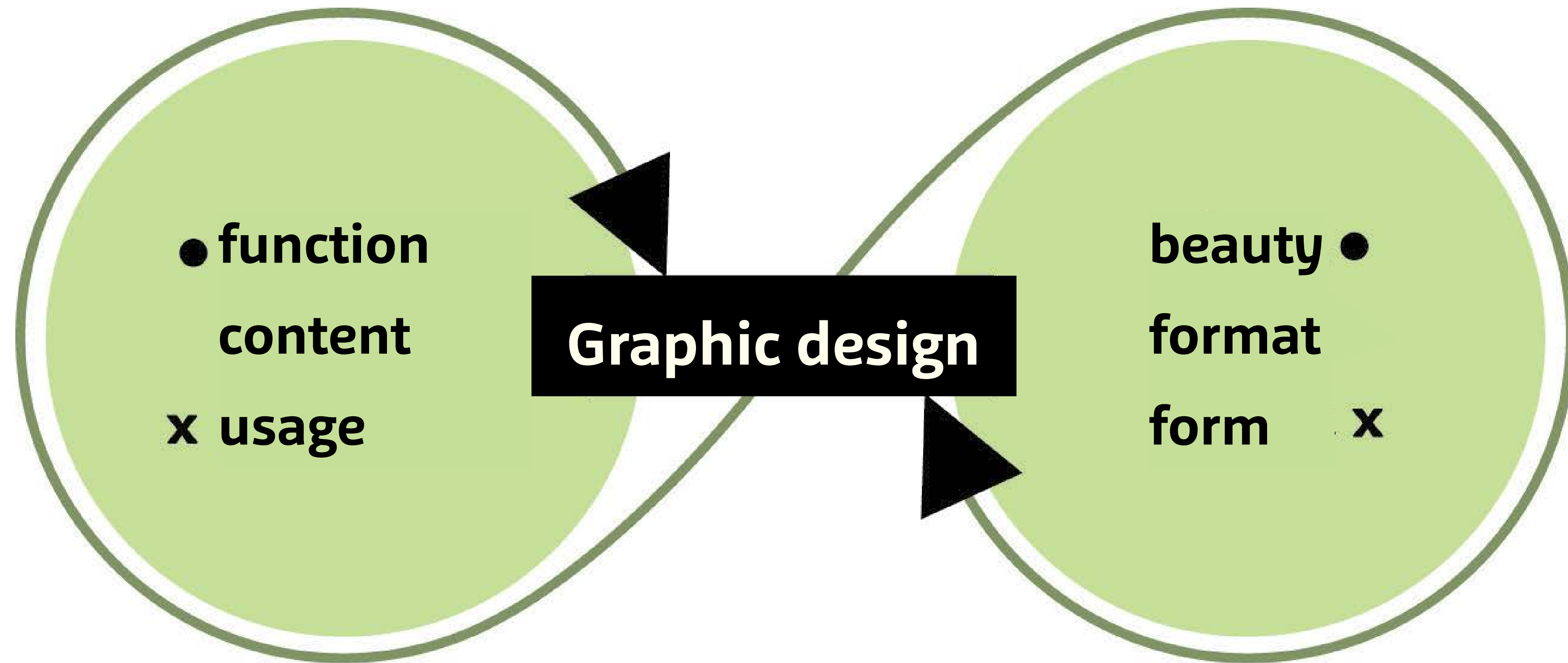
**Process of creating a poster**

**Case study**

# Graphic design

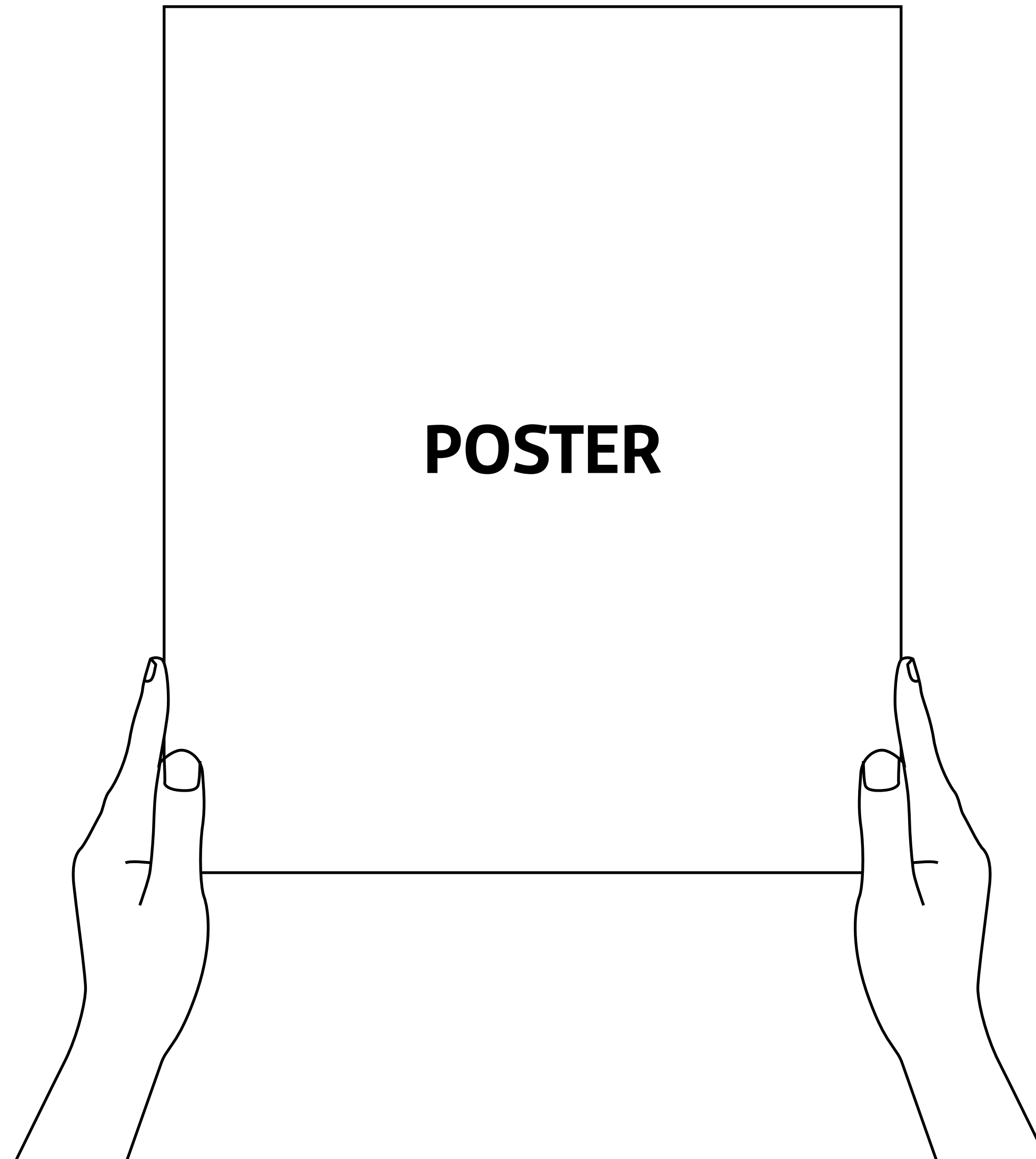
## DEFINITION





\*

**Poster**  
Definition

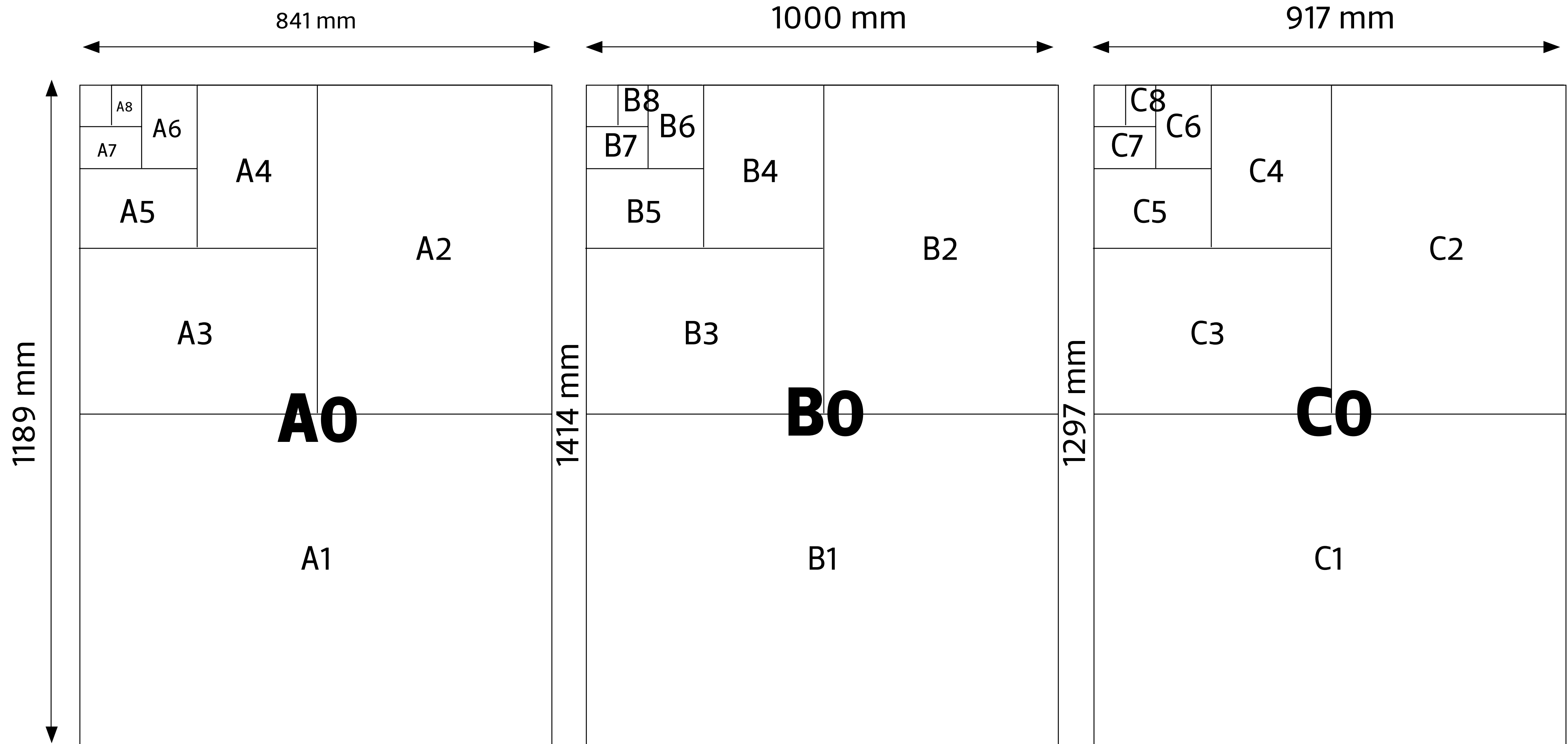


**Large printed format consisting of text, image, photography**

**On public places**

**To inform**

Format



**A0, A1**

**A1, A2**

**A2, A3**

**A4**

**A5**

**A6**

**B5, A5, B6, A6**

**C4, C5, C6**

**B4, A3**

**B8, A8**

**Science posters and technical drawings**

**Working boards (at meetings)**

**Diagrams, drawings and big boards**

**Magazines, letter, leaflets,...**

**Notebooks, calendars**

**Postcards**

**Books**

**Letter envelopes**

**Newspaper**

**Playing cards**

# Science posters

## Case studies

### Real-time Analysis of NetFlow Data for Generating Network Traffic Statistics using Apache Spark

Milan Čermák, Tomáš Jirsík, Martin Laštovička  
Institute of Computer Science, Masaryk University  
Botanická 68a, 602 00, Brno, Czech Republic  
E-mail: {cermak, jirsik, lastovicka}@ics.muni.cz

**Abstract** — We present a framework for the real-time generation of network traffic statistics on Apache Spark Streaming, a modern distributed stream processing system. Our previous results [1] showed that stream processing systems provide enough throughput to process a large volume of NetFlow data and hence they are suitable for network traffic monitoring. This demo describes the integration of Apache Spark Streaming into a current network monitoring architecture. We prove that it is possible to implement the same basic methods for NetFlow data analysis in the stream processing framework as in the traditional ones. Moreover, our stream processing implementation discovers new information which is not available when using traditional network monitoring approaches.

**Systems Performance Benchmark — Four Nodes (32 vCPUs)**

- Samza and Spark have a high-enough flow throughput and can be used for the analysis of data from multiple networks at the same time.
- Apache Spark system has been chosen as it offers an easy management and a high versatility in terms of the running environment and proprietary processing methods (e.g., sliding window).

**Framework Architecture**

The demonstration cluster consists of 7 virtual machines, one is dedicated to IPFIXcol, 5 to Spark and one to the Kibana and Web server. The following configuration is the same for all machines:

- 4 vCPUs Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz,
- 8GB 1600MHz DIMM DRAM EDO,
- 85GB SCSI Disk with 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI,
- 10 Gbit/s network connection, 1 Gbit/s virtual NICs.

IPFIXcol is a flexible IPFIX flow data collector designed to be easily extensible by plugins. In our demonstration, we use only part of its wide functionality – data acquisition from multiple network probes and their transformation into a JSON data stream.

**Statistics Volatility of Network Traffic Data**

- Stream processing provides more accurate statistics about network traffic.
- Statistics generated by the stream processing showed increased volatility in results compared to traditional flow data processing approaches.
- Allows to observe short, but strong bursts of the network traffic that were lost due to the aggregation used in traditional batch approaches.

**Real-time TOP K Statistics**

Provides a real-time computation of Top K statistics to enhance network situational overview.

**References**

[1] M. Čermák, D. Tovarňák, M. Laštovička, and P. Čeleda. *A Performance Benchmark for NetFlow Data Analysis on Distributed Stream Processing Systems*. In Proceedings of NOMS, 2016.

**Acknowledgements**

This research was supported by the Technology Agency of the Czech Republic under No. TA0401062 Technology for processing and analysis of network data in big data concept.

### Verification of Programs with Inputs

Henrich Lauko, Vladimír Štill, Petr Ročkal, Jan Mrázek and Jiří Barnat

**DIVINE**

**Symbolic States**

Consider a simple program with 32 bit input variable  $x$  and a branch on the value of this variable. In the current DIVINE, this program gives rise to  $2^{32}$  possible memory configurations. In symbolic version, possible values of variables  $x$  and  $b$  are represented symbolically using bitvector formulae, therefore, there are only two possible configurations at the end of the program.

**Proposed Approach**

To take advantage of symbolic representation of states, we transform the LLVM bitcode in such a way that it represents variables which contain values dependent on inputs symbolically. This transformation is performed by LART and is presented in detail later. Apart from that, the verification algorithm is modified to handle symbolic states with the help of an SMT solver.

Our approach aims for minimizing changes to the LLVM interpreter that is used to execute instructions in DIVINE. The reason is that the interpreter is complex and performance tuned and therefore it is not desirable to make it even more complex by adding symbolic data manipulation into it. Instead, symbolic data are to be handled by the program itself. To encode symbolic manipulations into the program we transform the LLVM bitcode produced by the compiler and create symbolic LLVM from it. This not only minimizes changes to the interpreter, but the transformation can also be used for different representation of symbolic data quite easily. The transformation is handled by LART – LLVM Abstraction & Refinement Tool. Furthermore, DIVINE's verification algorithm has to be modified. It has to check if symbolic states are valid (nonempty), that is if they can represent at least one concrete state. It also has to handle comparison of symbolic states. For both of these tasks, DIVINE has to extract SMT formulae from the program state and use SMT solver.

**Details of Program Transformation**

LLVM bitcode is generated from C++ source code. Dependence graph of LLVM instructions is created from the control flow of a program. Instructions dependent on the input are computed. Dependent instructions are substituted with symbolic calls, path condition manipulations are added. A program simulating original instructions in a symbolic manner.

LART takes the LLVM bitcode of the program and libraries produced by the compiler and transforms it into a bitcode which manipulates data symbolically. In this modified program, any variable which can depend on an input value is represented symbolically using bitvector formulae. Bitvector formulae describe integers of fixed bit width with overflow and bitwise operations, and therefore are well suited for exact representation of computer integers. All the manipulations with such variables have to be transformed to their symbolic versions which modify the formulae accordingly. Furthermore, any branch which depends on an input value has to put constraints on the possible values of symbolic variables (this constraint is given in the form of a path condition formula).

### EACirc

Using genetics to improve encryption

Martin Ukrop, Petr Švenda, Marek Šys, Václav Matyáš et alii

**Problem statement**

**Randomness testing**

The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?

**Iterative design**

The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions). It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

**EACirc workflow**

- Forming a population**: A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.
- Test vector generation**: Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.
- Fitness assessment**: Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0, 1].
- Survival of the fittest**: Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival. The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.
- Mutation & crossover**: To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population. The new population now enters the evolution cycle again, gradually improving its fitness.

**Comparison to existing tools**

**EACirc vs statistical testing**

The standard way to assess randomness is to use batteries of statistical tests such as NIST STS, Dieharder or TestU01. We run them along with EACirc and compare the results.

Interested in EACirc? See the papers referenced below or ask directly at the lab (CROCS @ F. M. U.).

To have a fine-grained comparison, we have analyzed 77 different functions (eStream, SHA-3 and CAESAR candidates). For 2-round Hermes and 1-round Fubuki we confidently surpass NIST STS.

**Further information**

[1] Švenda, Ukrop, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications. Vol. 456. SCISPT 2013. Springer Berlin Heidelberg, 2014.

[2] Kubček, Novotný, Švenda, Ukrop. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications. Vol. 8, iss. 1, 2016.

### CERIT Scientific Cloud

Looking for Synergies in Scientific Computing

David Ambó, Aed Kinnel, Ivana Klenková, Luděk Matyska  
Institute of Comp. Science, Masaryk University, Brno

**Mission**

CERIT Scientific Cloud centre, the successor of Supercomputing Centre Brno at Masaryk University, is a national centre providing flexible computational and storage capacities. Provision of these resources is complemented with extensive research activities, carried both in cooperation with the user communities and in the e-Infrastructure area itself.

**History**

Supercomputing Centre Brno (SCB) is a part of Institute of Comp. Science, Masaryk University. SCB was founded in 1994 as one of big supercomputing centres in the Czech Republic of that time. Similar cooperating centres were founded by other universities (Prague, Pilsen, Brno, Ostrava). SCB has been working with Faculty of Informatics, Masaryk University, for a long time. The cooperation is both personal and factual, formally expressed, e.g. in a common research intent "Highly parallel and distributed computation systems".

**Funding**

Transformation of SCB into CERIT-SC will be supported by a project of the 3rd axis of the RD&I Operational Program. The project will be realized from May 2011 to October 2013. Its overall budget is 5 M€.

CERIT-SC is included in the Roadmap for Large Research, Development and Innovation Infrastructures in the Czech Republic.

**Equipment and Purchase Schedule**

The project will purchase the following resources:

- SMP – Symmetric MultiProcessing clusters, with more than 64 cores and 128 GB memory per node (1000 cores total)
- HD – High Density clusters with higher number of nodes with 8-16 cores and 16-32 GB memory (2500 cores total)
- HSM Hierarchical Storage Management (3 PB)
- disk storage (600 TB)
- development tools and application software

**Cooperation with Users**

Deluge of experimental data is expected in near future. Many existing computational methods will break or stop scaling, new developments will be required. User communities will come up with interesting problems, CERIT-SC will provide the necessary IT expertise. We expect formation of joint teams consisting of experts from both sides, addressing specific research areas – both ad-hoc and long term work, involving students (undergraduate and Ph.D.). This work will result in common publications. Targeted projects are also expected.

**Formal agreement on future collaboration (LoI):**

- RD&I: AdMas, BIOCIV, CETEC, CzechGlobe, RECAMO
- cooperating institutions: IBA, MZK, Loschmidt Labs, RECTOX
- ESFRI projects (in negotiation): LINDAT-CLARIN, Euro-BioImaging

**Flexible Resources**

Provision of the resources will range from traditional batch queues, through interactive access up to the cloud paradigm. The resources will be provided free of charge. Prioritization of the users will be based on their scientific results; resulting resource allocation will be achieved by technical means, combining advanced resource scheduling, virtualization, and the cloud paradigm; no complex administrative process will be required. By careful balancing the scheduling strategies, successful users will get better share while new users, students etc. will not be prevented from using the resources. CERIT-SC computational resources are intended to serve unexpected and unplanned requirements of the users primarily. Data resources will serve to store and share data semipermanently and permanently. They will be tightly integrated with the computational resources. The target community are the end-users again.

**Equipment and Purchase Schedule (Timeline)**

cores, capacities in current price/capacity ratios

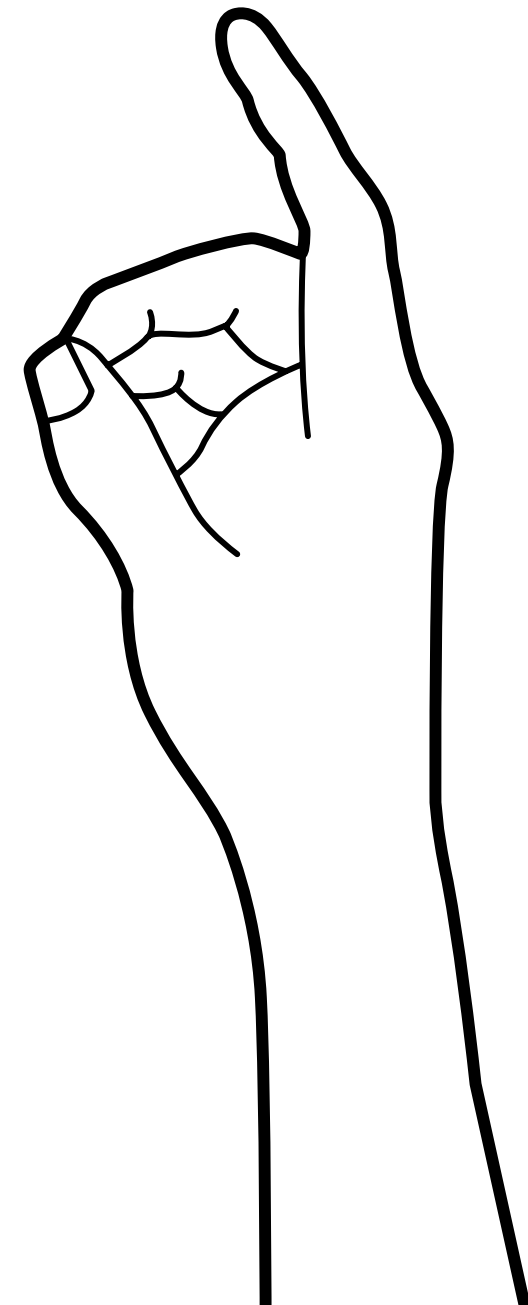
Scientific director Prof. RNDr. Luděk Matyska, CSc.  
Project manager Roman Čermák, M.Sc., MBA  
<http://www.cerit-sc.cz>

This poster presentation is partially supported by project "Podpora výzkumných aktivit" (Support of research activities) IČZ.1.07/2.3/00/08/0074\*

Investments in Education Development

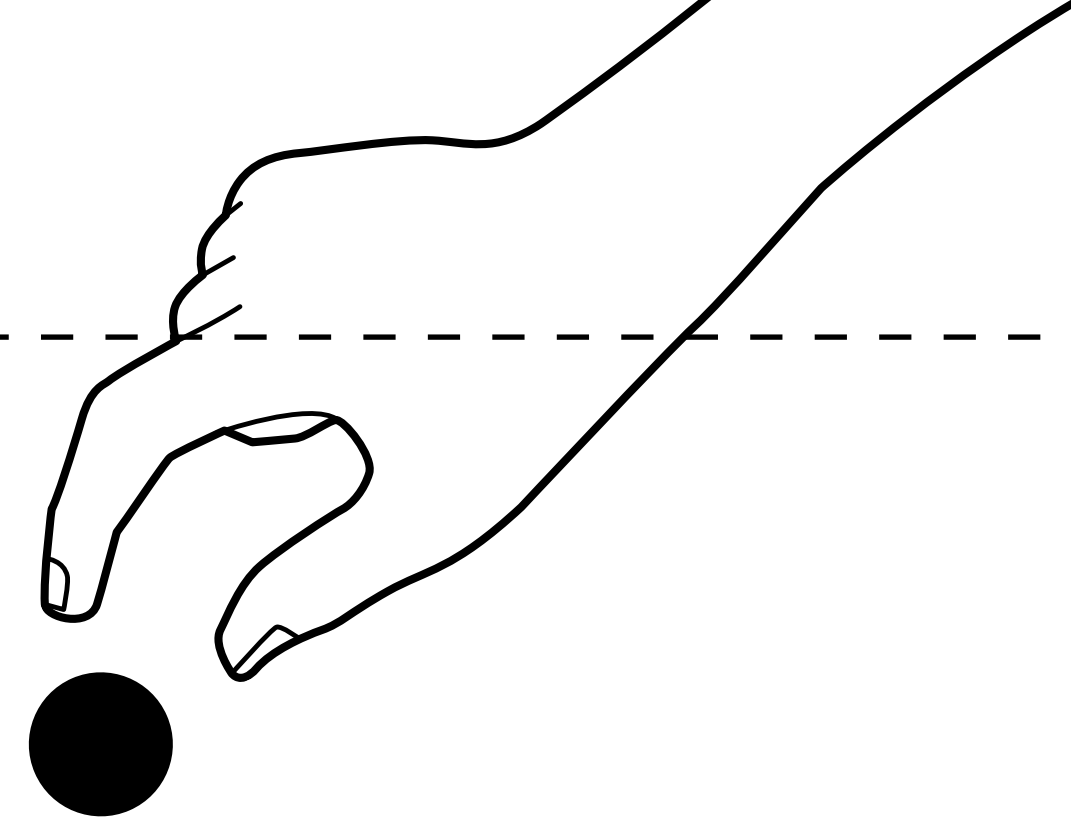


● **Composition**

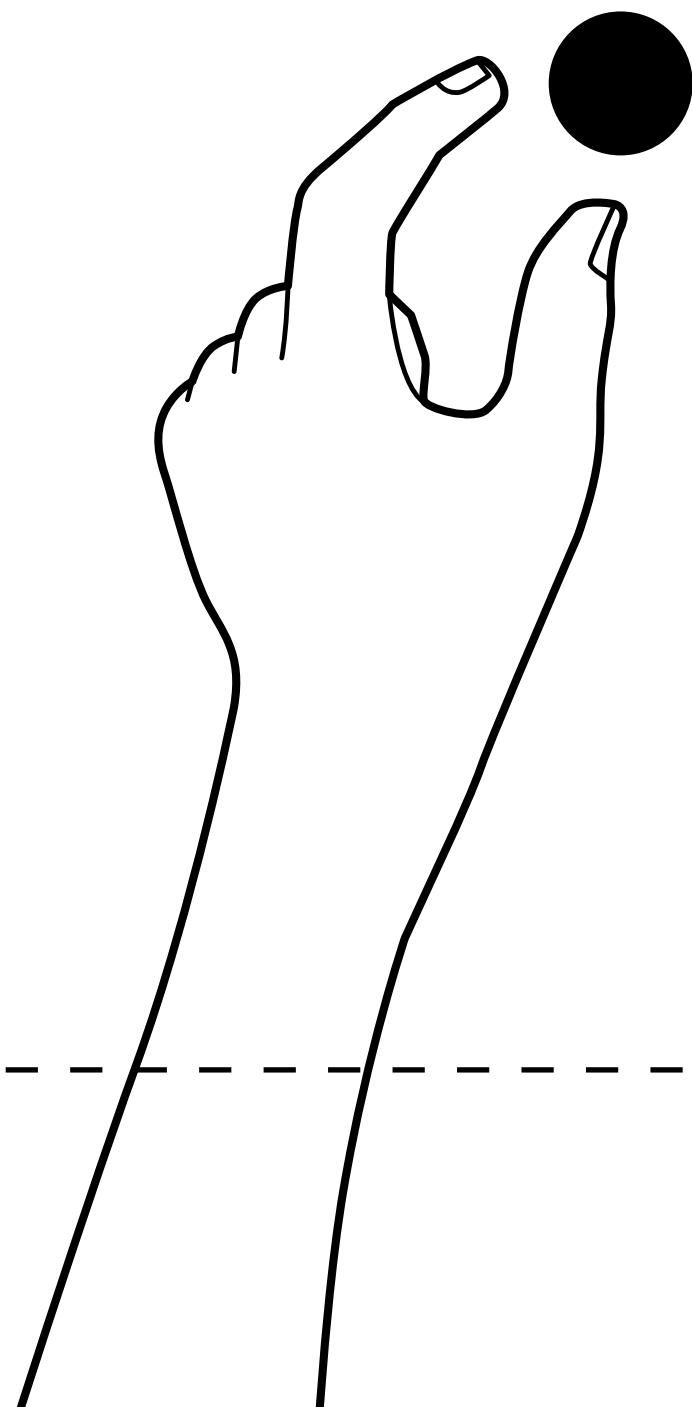


**Comoposition**

**text**

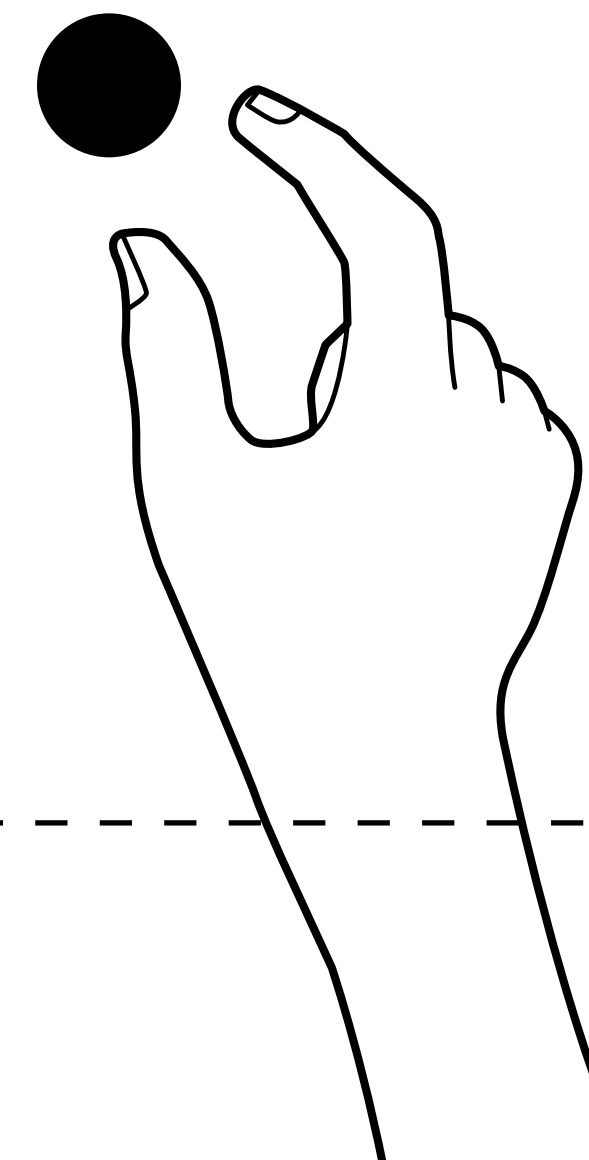


**picture**

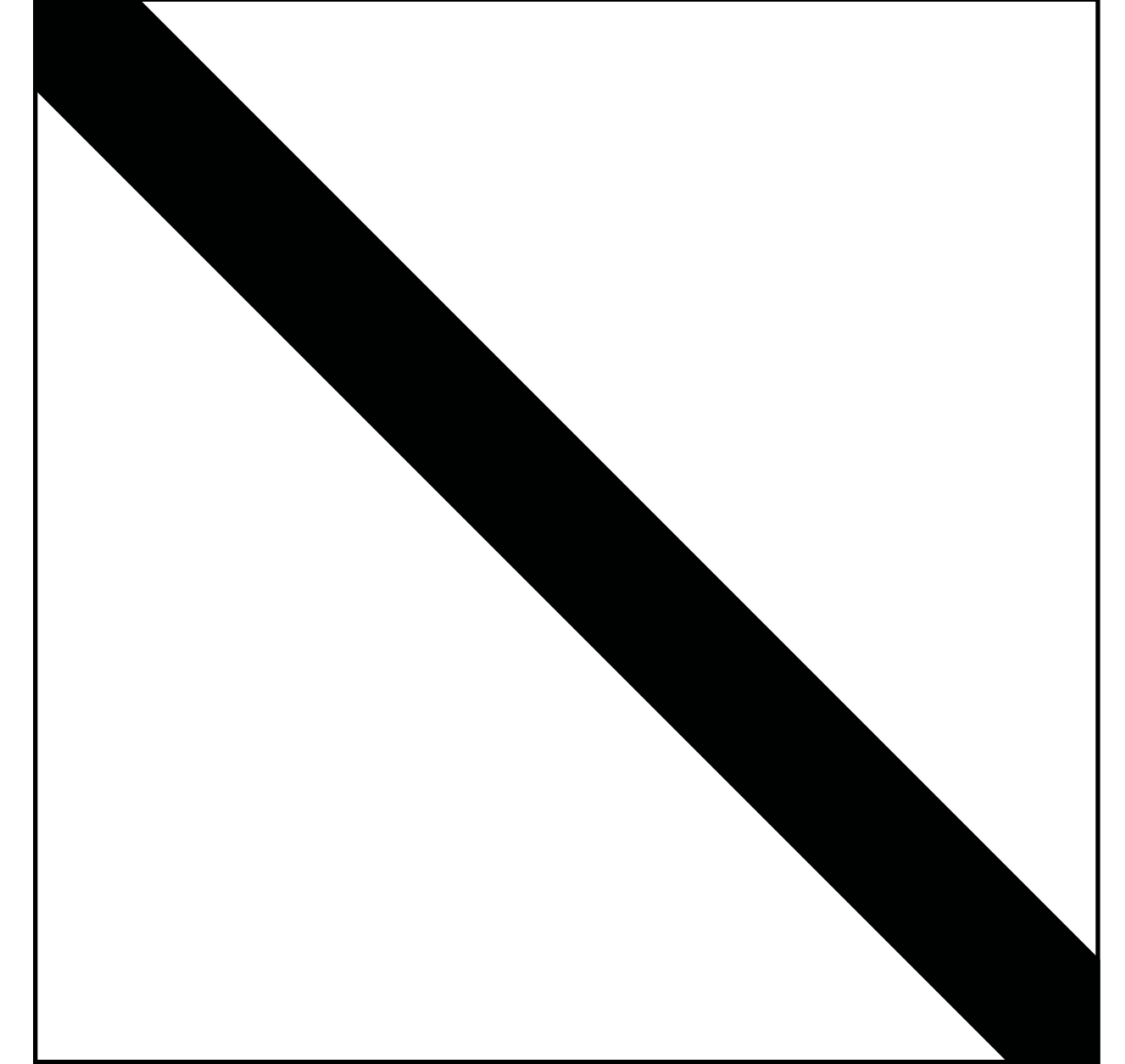
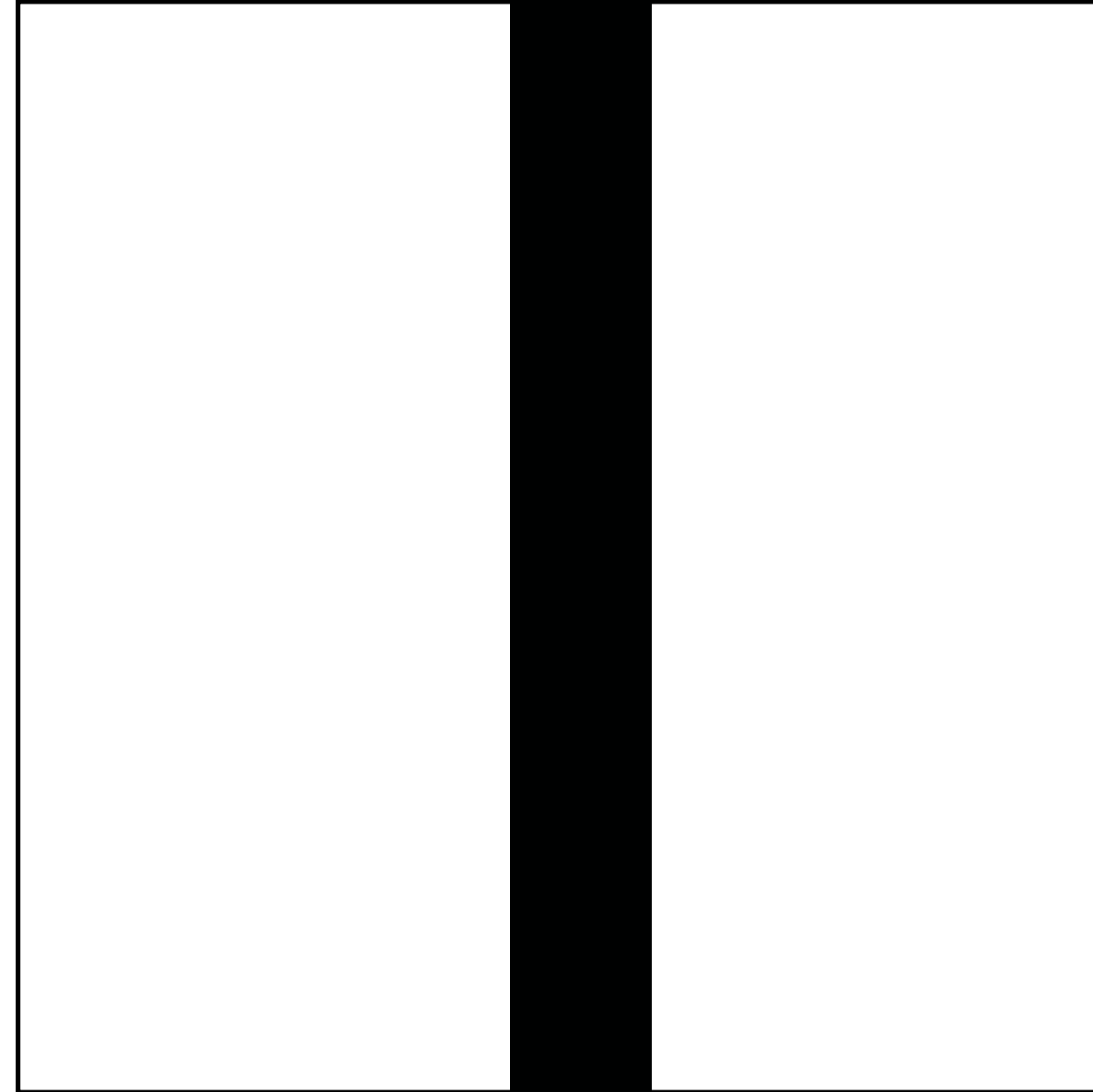
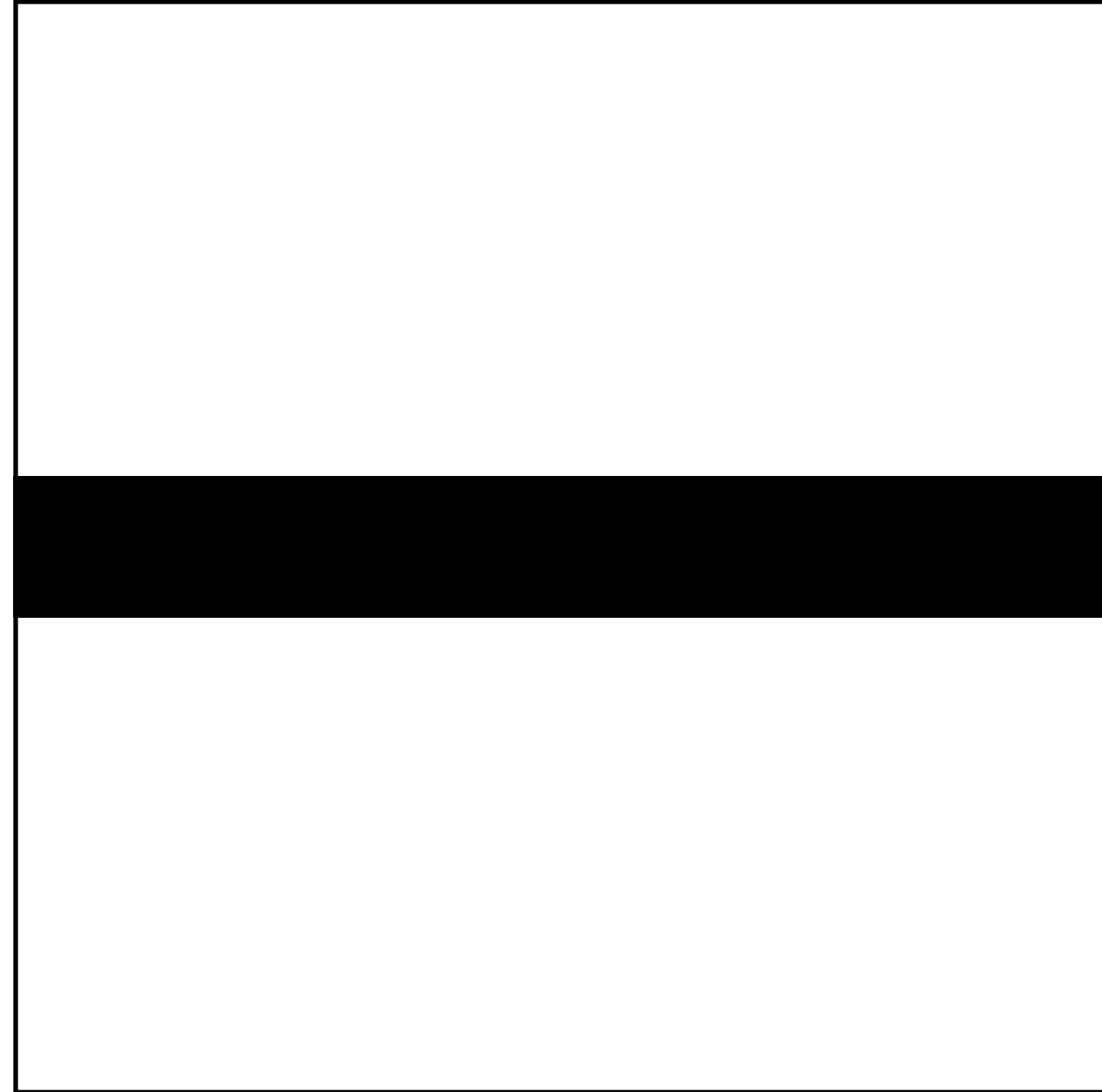


**Balance between various elements**

**infographics**

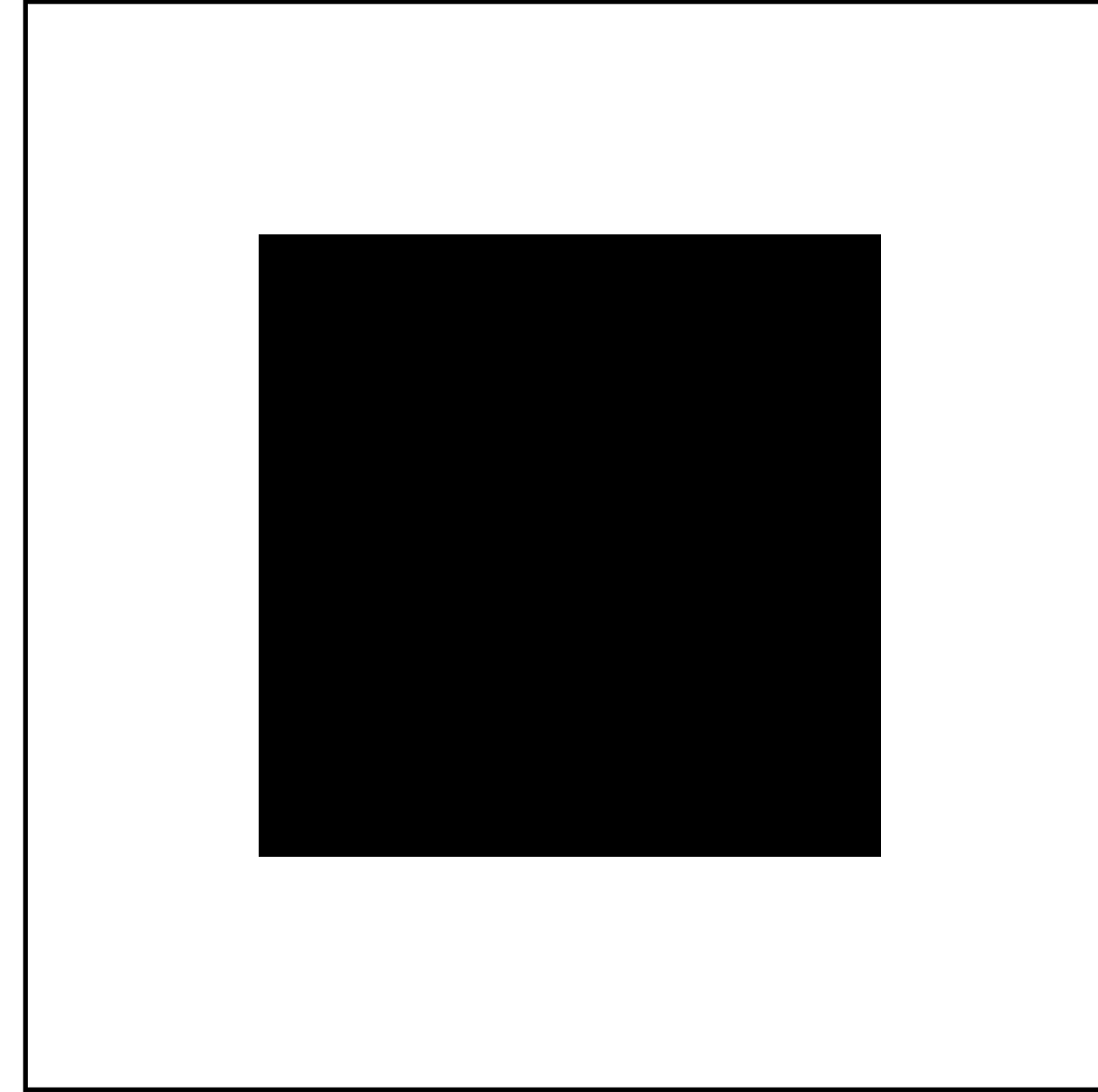
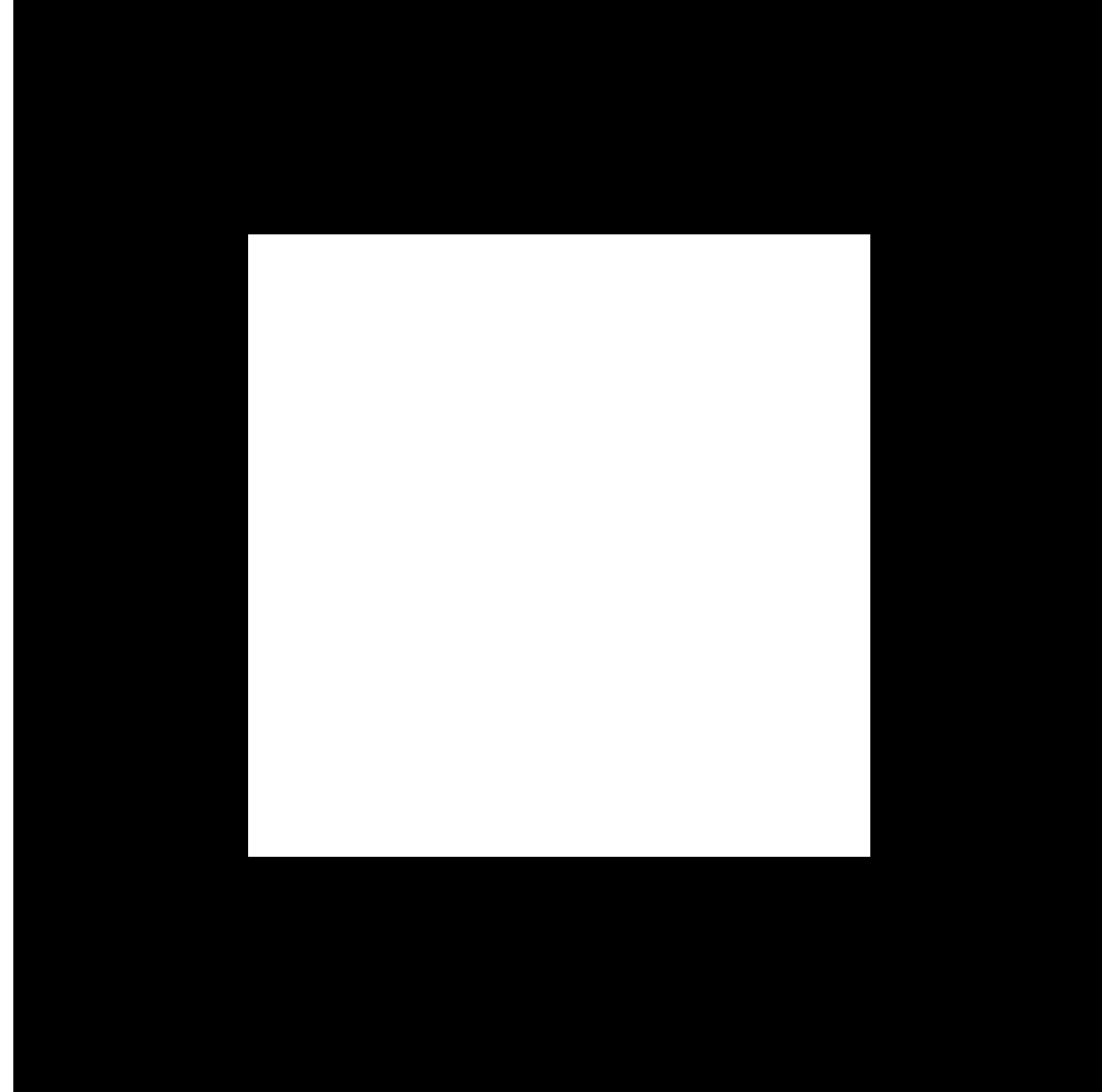


## Comoposition



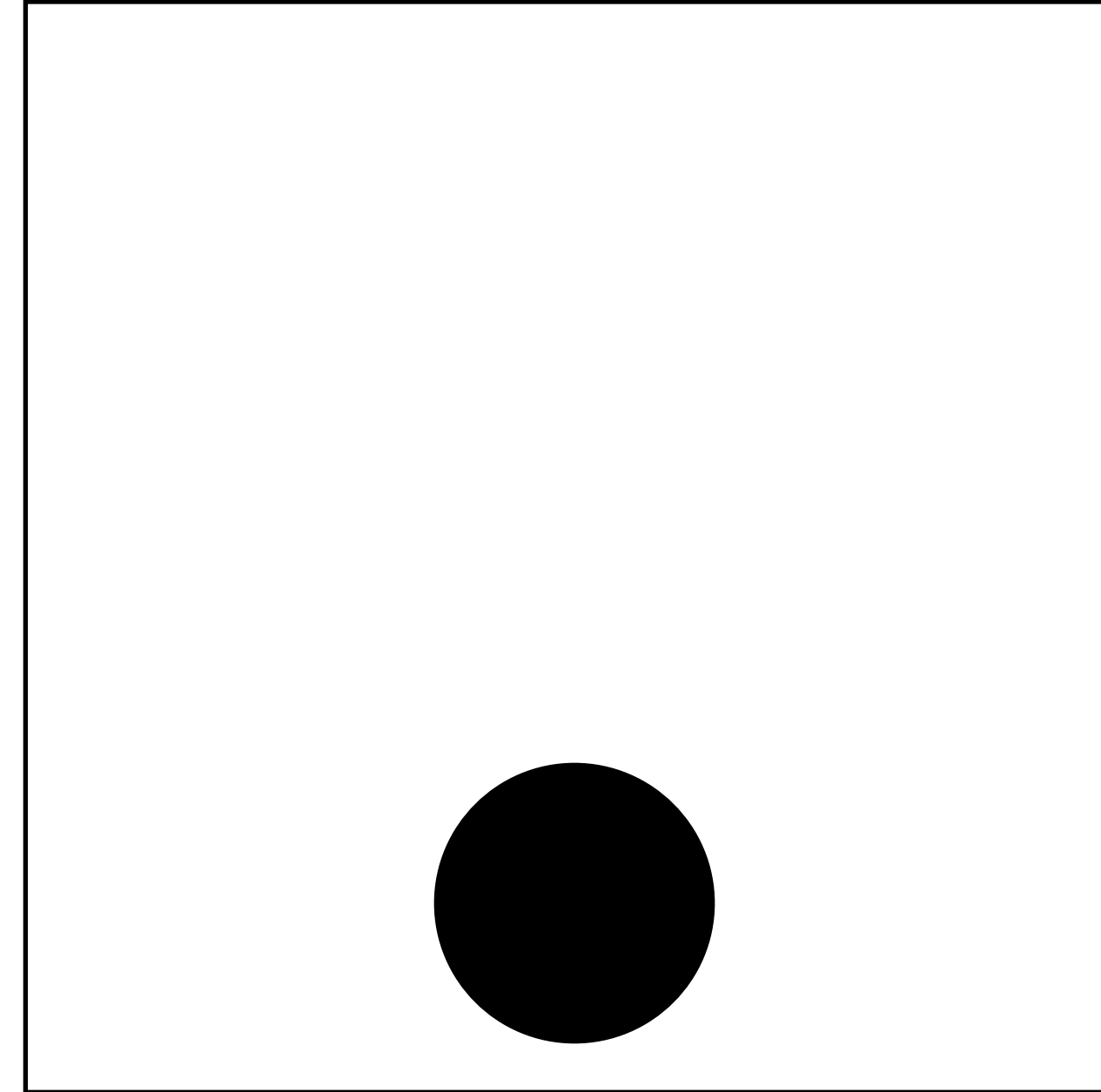
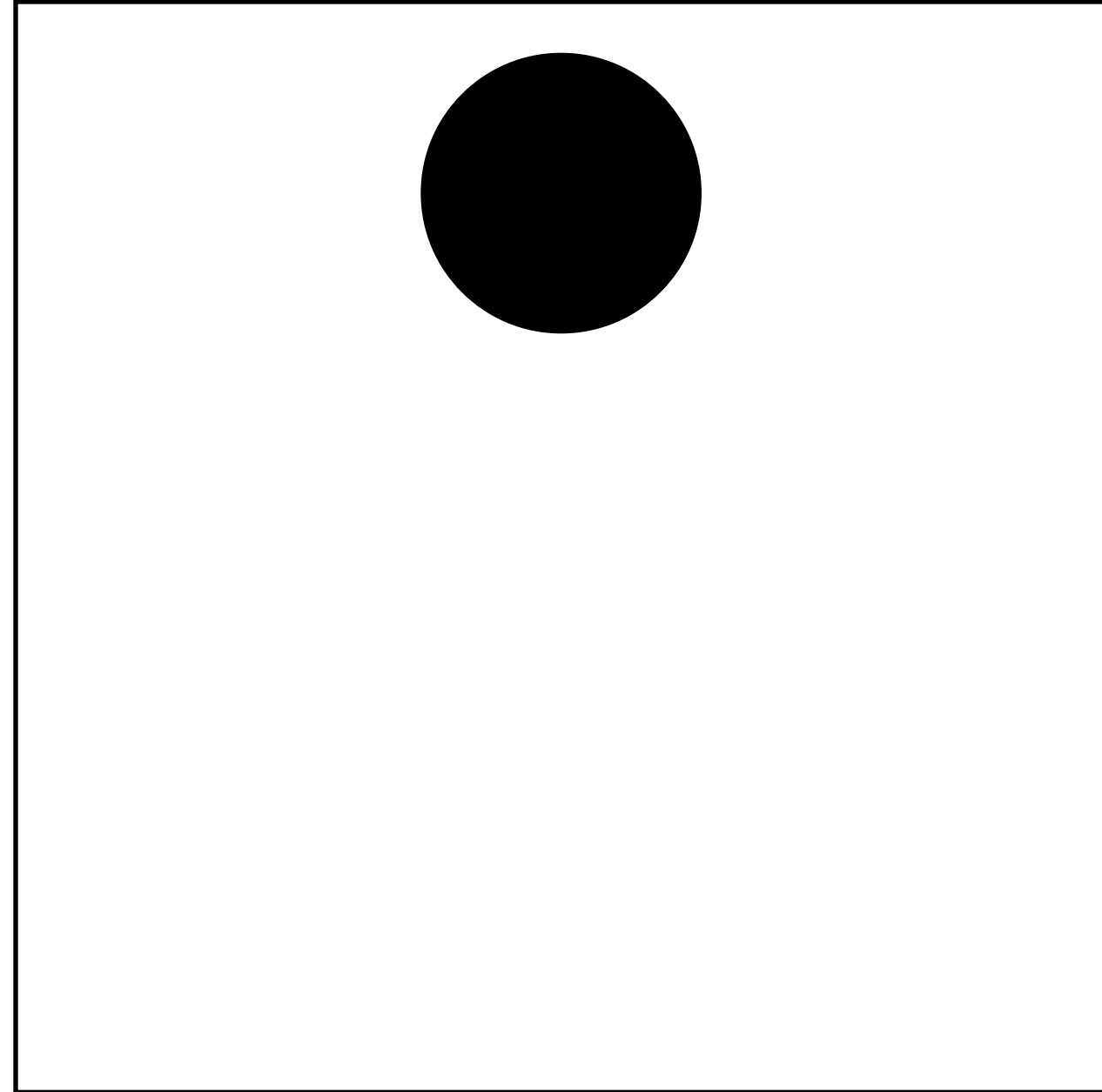
**Vertical objects appear heavier than horizontal objects.  
A diagonal orientation carries more visual weight than  
a horizontal or vertical one.**

## Comoposition



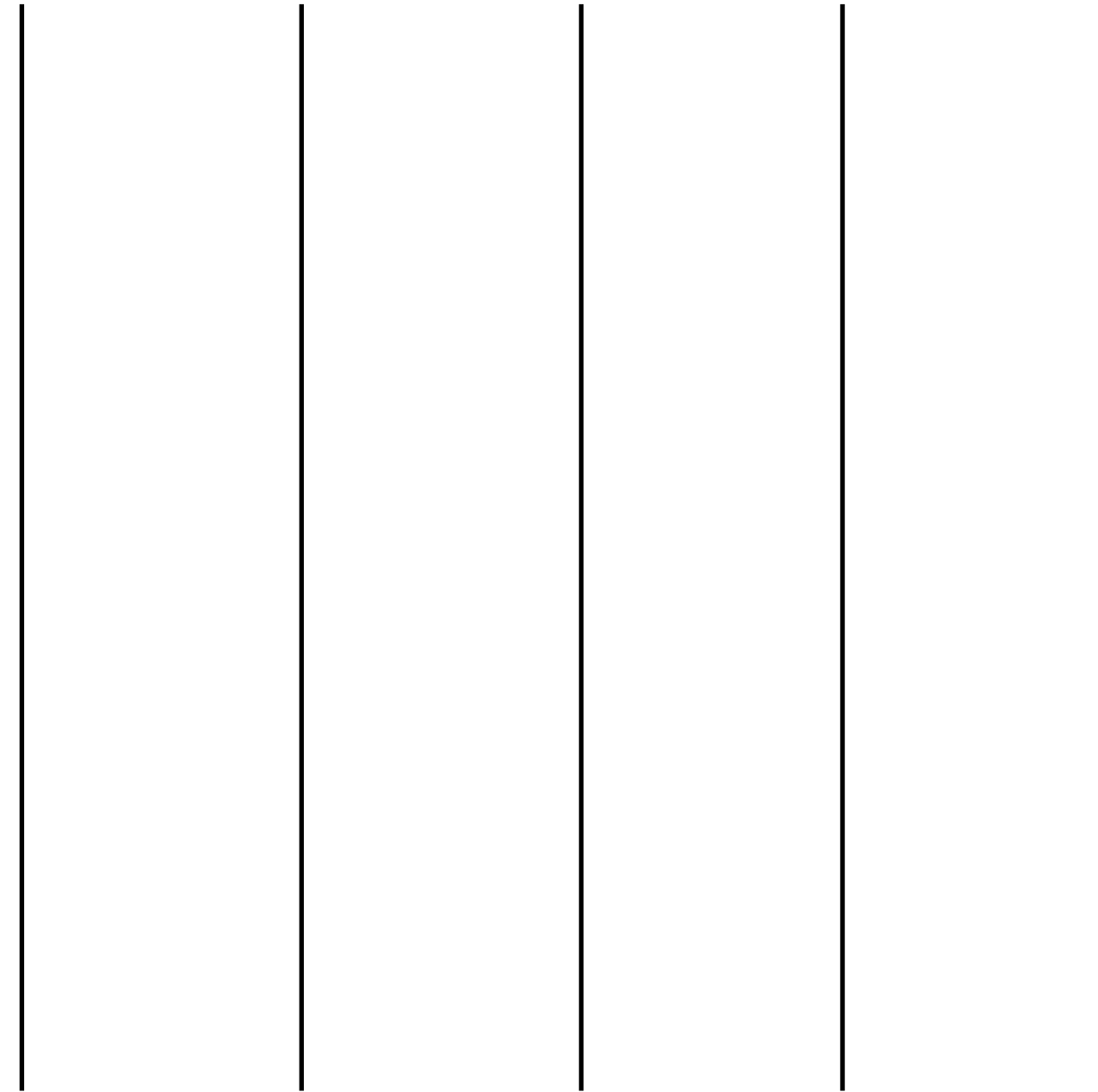
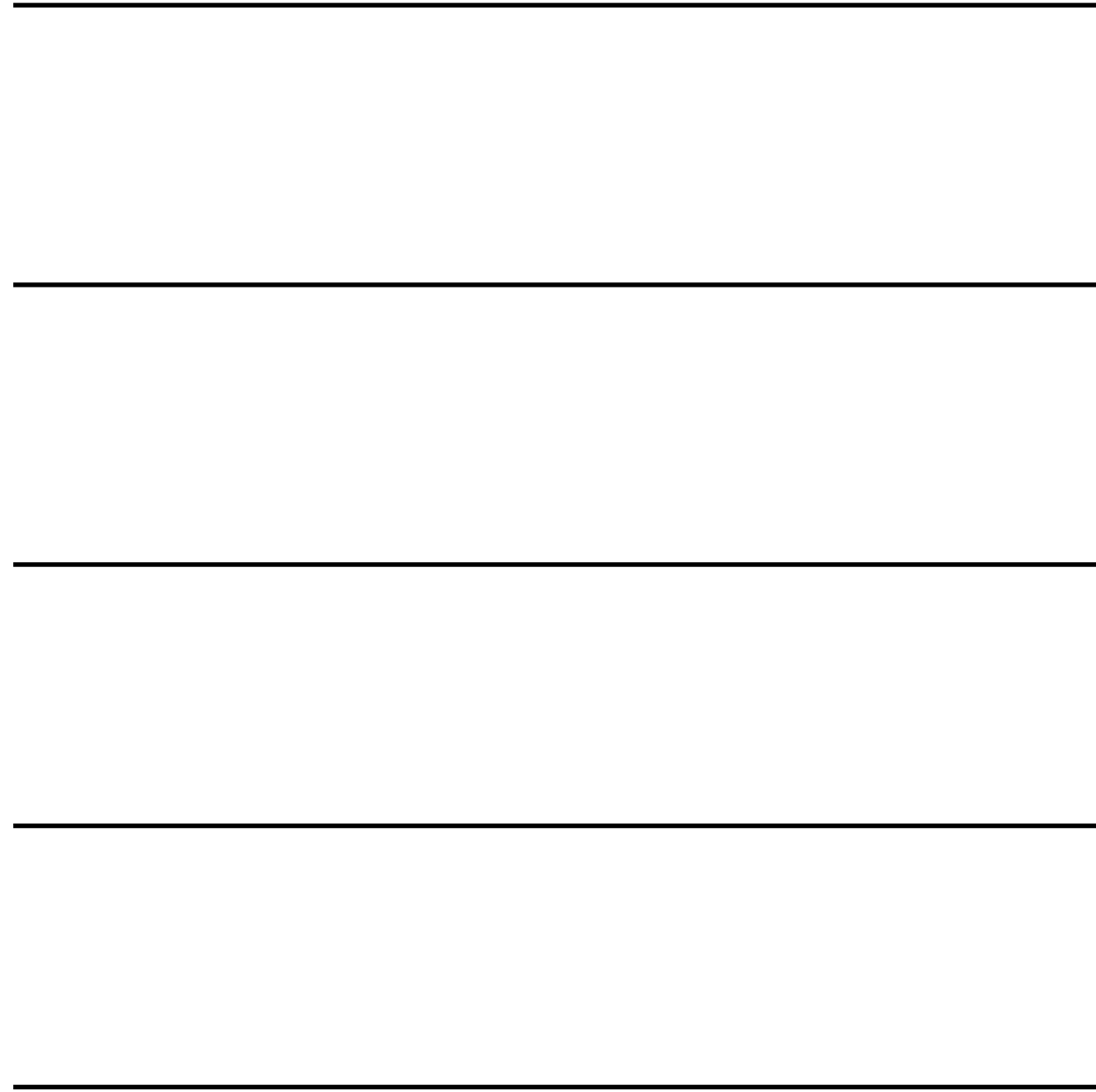
**White square on the black background appears bigger than the black square on white colour.**

## Comoposition



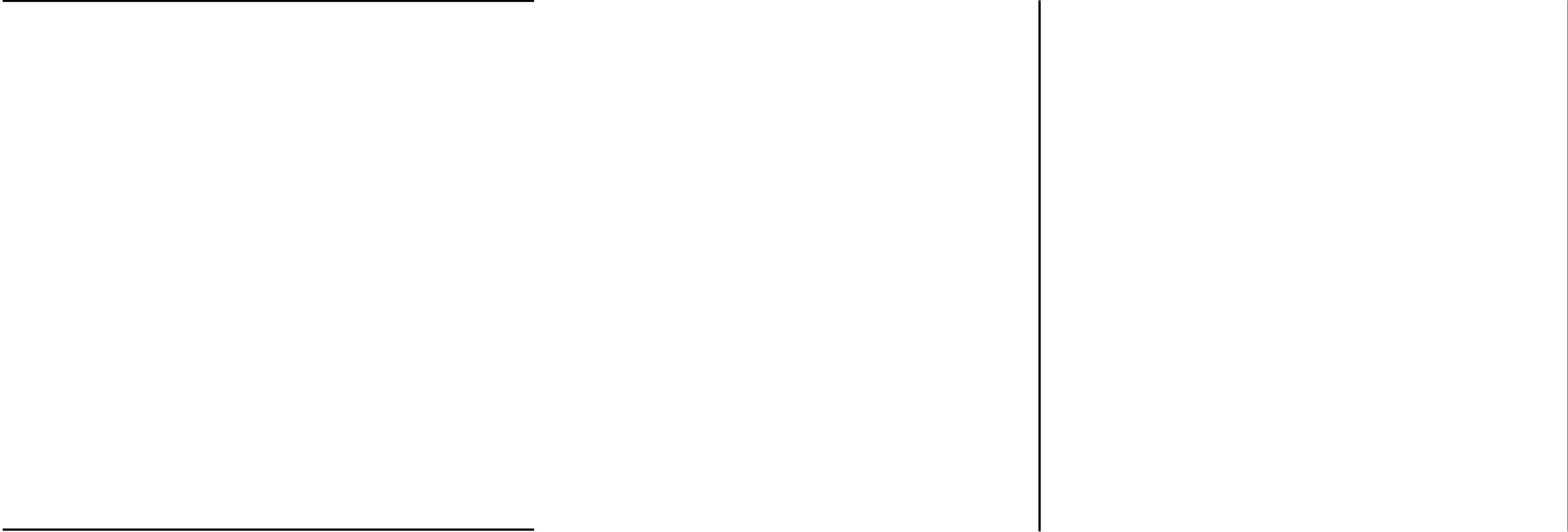
**The visual weight of an object increases in proportion to its distance from the center (or dominant area) of the composition.**

# Comoposition



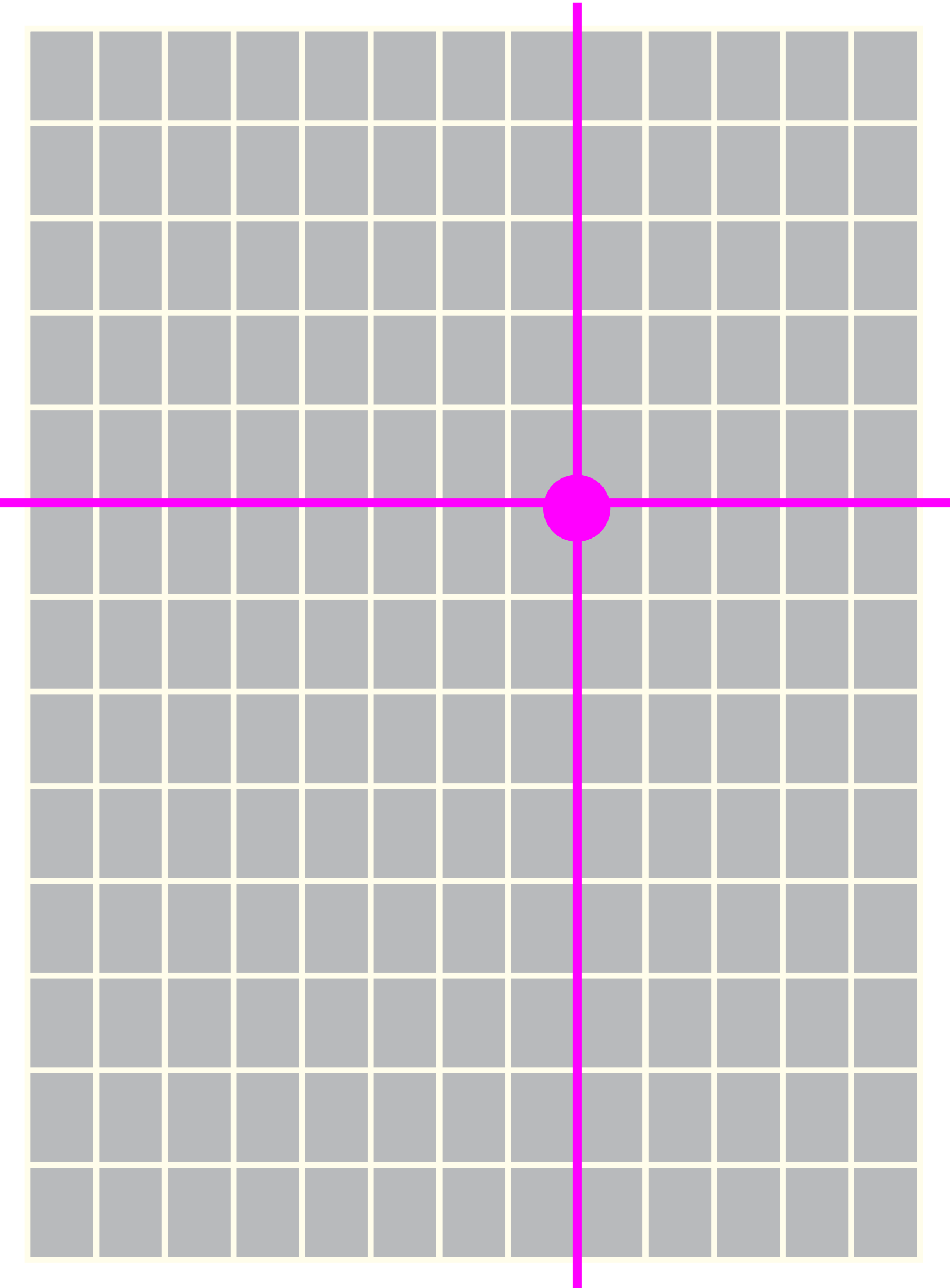
**Horizontal lines makes shape higher, vertical lines  
makes it wider.**

**Comoposition**



**Border horizontal lines makes shape wider,  
vertical lines makes it higher.**

Comoposition



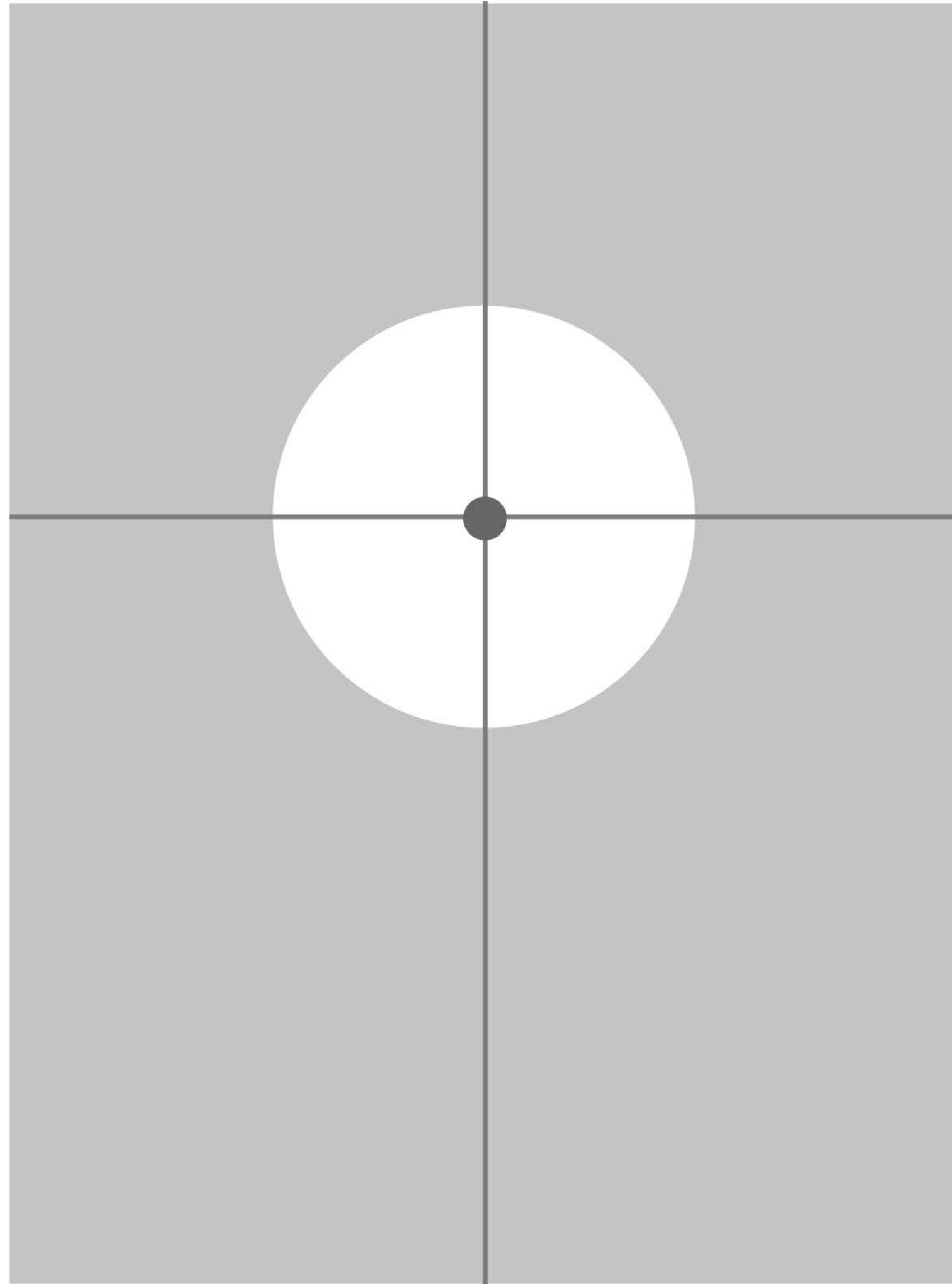
The Golden Section or Ratio is is a ratio or proportion defined by the number Phi (= 1.618033988749895... )



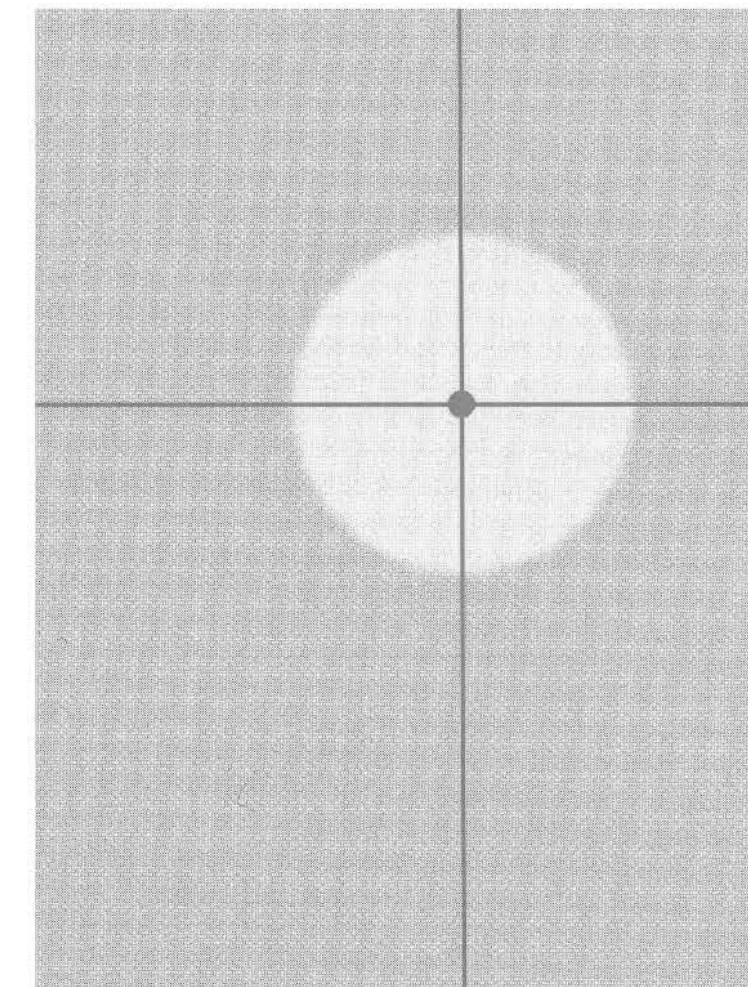
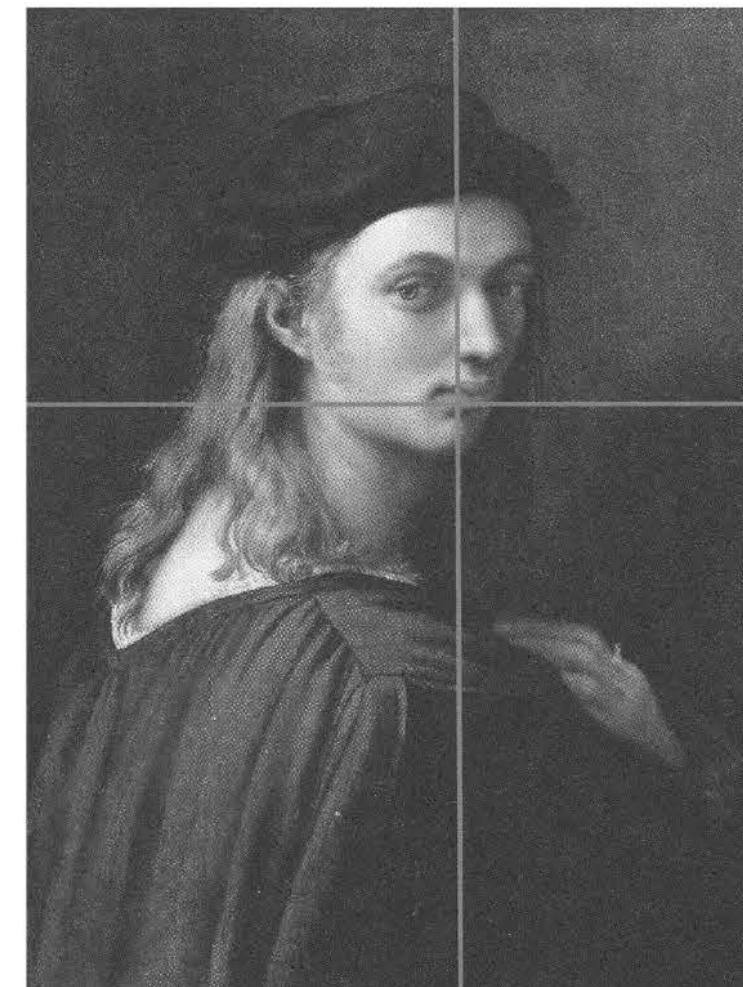
Jan Tschichold



# Comoposition

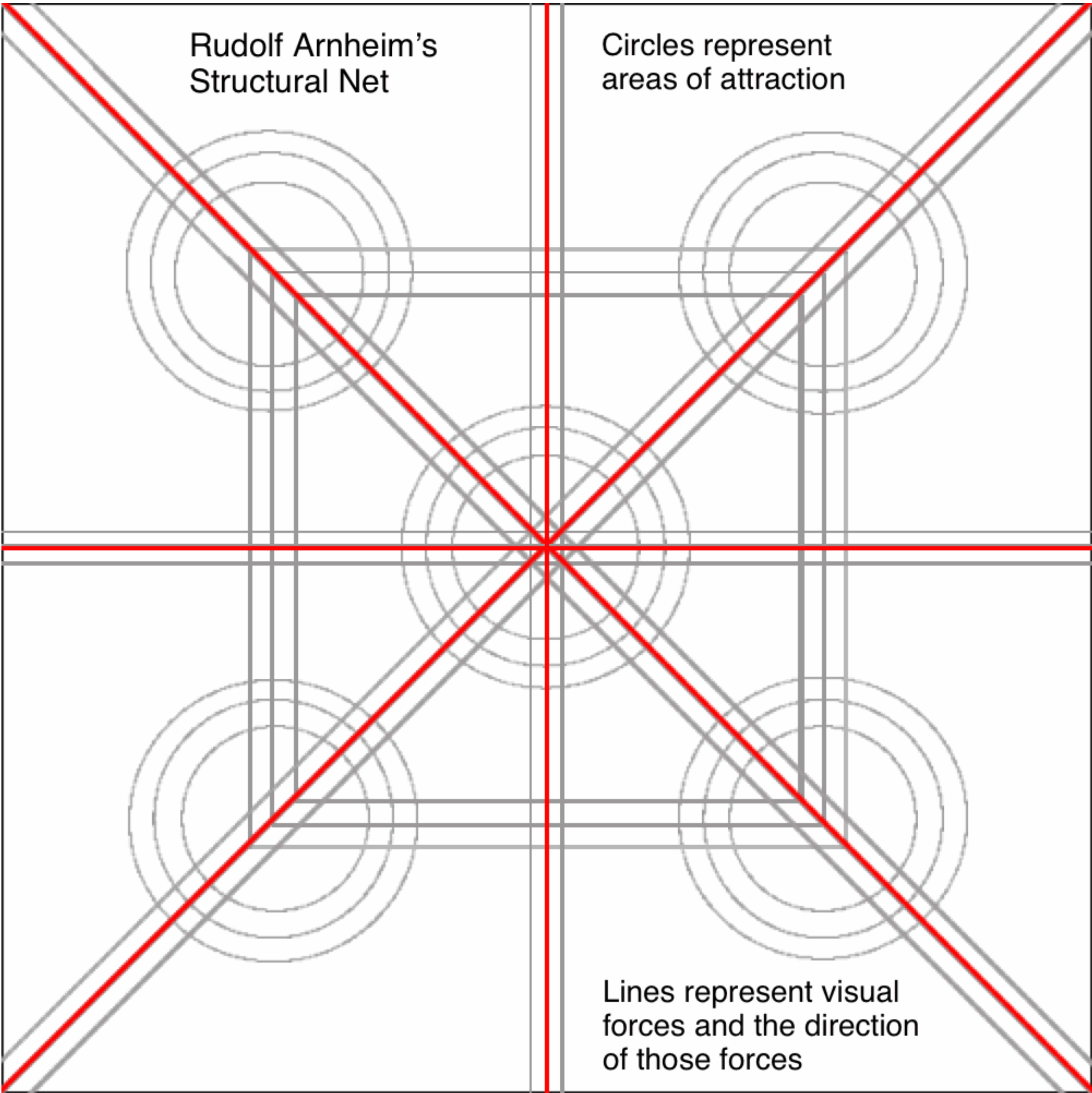


**Portrait of Bindo Altoviti (1514), Raphael  
– mouth and eyes are the key points  
places in optical centre**



**Comoposition**  
Optical centre

**Rudolf Arnheim's diagram**



# Case studies

## Centered layout

FACULTY OF INFORMATICS  
Masaryk University

## Verification of Programs with Inputs

Heňrich Lauko, Vladimír Štill, Petr Ročkai, Jan Mrázek and Jiří Barnat

### DIVINE

DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choices which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

### Symbolic States

Consider a simple program with 32 bit input variable  $x$  and a branch on the value of this variable. In the current DIVINE, this program gives rise to  $2^{32}$  possible memory configurations. In symbolic version, possible values of variables  $x$  and  $b$  are represented symbolically using bitvector formulae, therefore, there are only two possible configurations at the end of the program.

### Proposed Approach

To take advantage of symbolic representation of states, we transform the LLVM bitcode in such a way that it represents variables which can contain values dependent on inputs symbolically. This transformation is performed by LART and is presented in detail later. Apart from that, the verification algorithm is modified to handle symbolic states with the help of an SMT solver.

Our approach aims for minimizing changes to the LLVM interpreter that is used to execute instructions in DIVINE. The reason is that the interpreter is complex and performance tuned and therefore it is not desirable to make it even more complex by adding symbolic data manipulation into it. Instead, symbolic data are to be handled by the program itself. To encode symbolic manipulations into the program we transform the LLVM bitcode produced by the compiler and create symbolic LLVM from it. This not only minimizes changes to the interpreter, but the transformation can also be used for different representation of symbolic data quite easily. The transformation is handled by LART – LLVM Abstraction & Refinement Tool. Furthermore, DIVINE's verification algorithm has to be modified. It has to check if symbolic states are valid (nonempty), that is if they can represent at least one concrete state. It also has to handle comparison of symbolic states. For both of these tasks, DIVINE has to extract SMT formulae from the program state and use SMT solver.

### Details of Program Transformation

LLVM bitcode is generated from C++ source code. Dependence graph of LLVM instructions is created from the control flow of a program. Instructions dependent on the input are computed. Dependent instructions are substituted with symbolic calls, path condition manipulations are added. A program simulating original instructions in a symbolic manner.

LART takes the LLVM bitcode of the program and libraries produced by the compiler and transforms it into a bitcode which manipulates data symbolically. In this modified program, any variable which can depend on an input value is represented symbolically using bitvector formulae. Bitvector formulae describe integers of fixed bit width with overflow and bitwise operations, and therefore are well suited for exact representation of computer integers. All the manipulations with such variables have to be transformed to their symbolic versions which modify the formulae accordingly. Furthermore, any branch which depends on an input value has to put constraints on the possible values of symbolic variables (this constraint is given in the form of a path condition formula).

ParaDiSe  
Parallel & Distributed Systems Laboratory

MASARYK UNIVERSITY

## EACirc

Using genetics to improve encryption

Martin Ukrop, Petr Švenda, Marek Sýs, Václav Matyáš et alii

Fork me on GitHub  
github.com/crccs/eacirc

### Problem statement

#### Randomness testing

The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?

EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.

#### Iterative design

The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions). It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

### EACirc workflow

- Forming a population**  
A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.
- Test vector generation**  
Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.
- Fitness assessment**  
Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0, 1].
- Survival of the fittest**  
Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival. The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.
- Mutation & crossover**  
To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population. The new population now enters the evolution cycle again, gradually improving its fitness.

### Comparison to existing tools

#### EACirc vs statistical testing

The standard way to assess randomness is to use batteries of statistical tests such as NIST STS, Dieharder or TestU01. We run them along with EACirc and compare the results.

To have a fine-grained comparison, we have analyzed 77 different functions (eStream, SHA-3 and CAESAR candidates). For 2-round *Hermes* and 1-round *Fubuki* we confidently surpass NIST STS.

#### Further information

Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).

[1] Švenda, Ukrop, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications, Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.

[2] Kubiček, Novotný, Švenda, Ukrop. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications, Vol. 8, iss. 1, 2016.

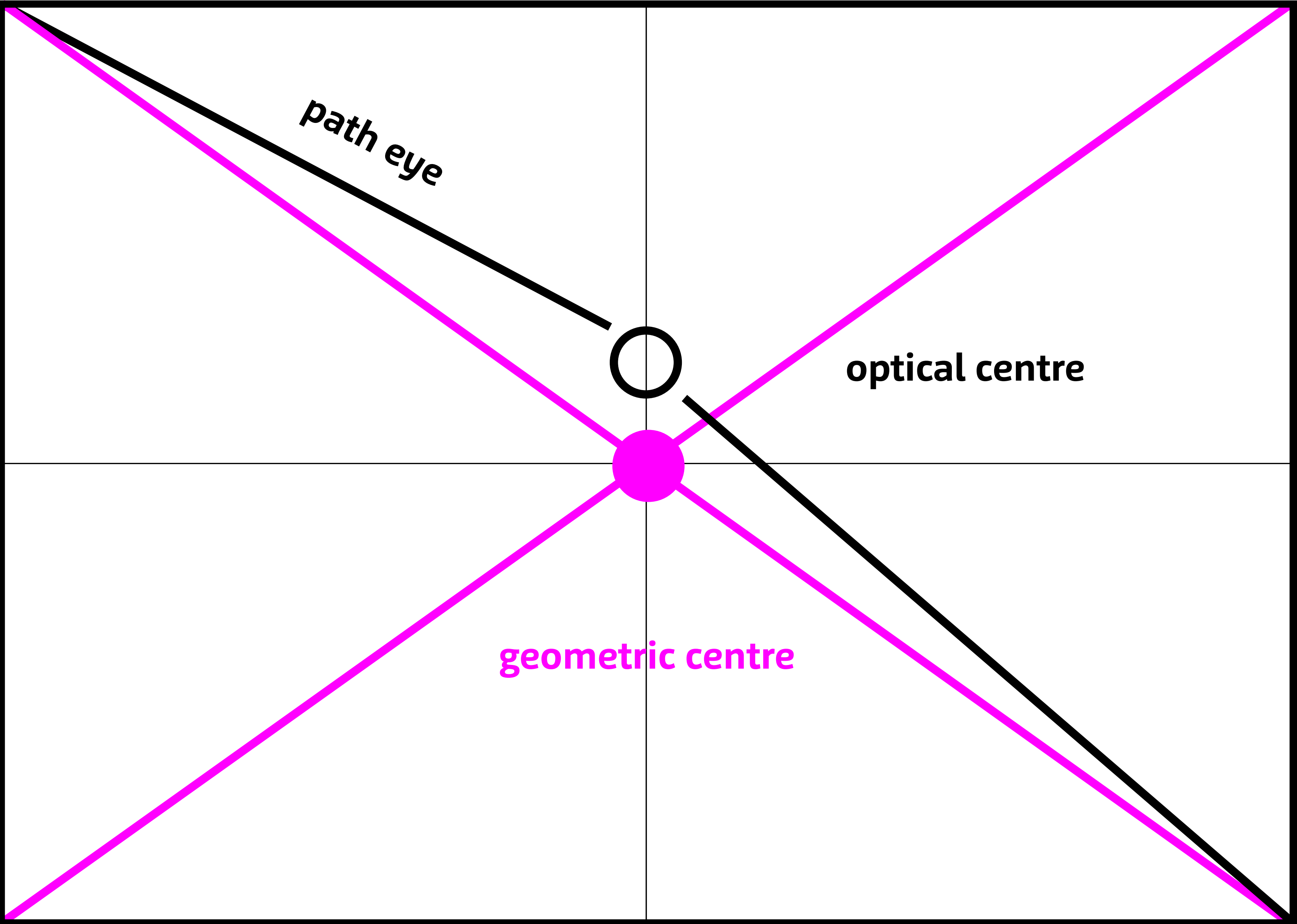
CRoCS  
Centre for Research on Cryptography and Security

This work was supported by the Czech Science Foundation project GAP202/11/0422.

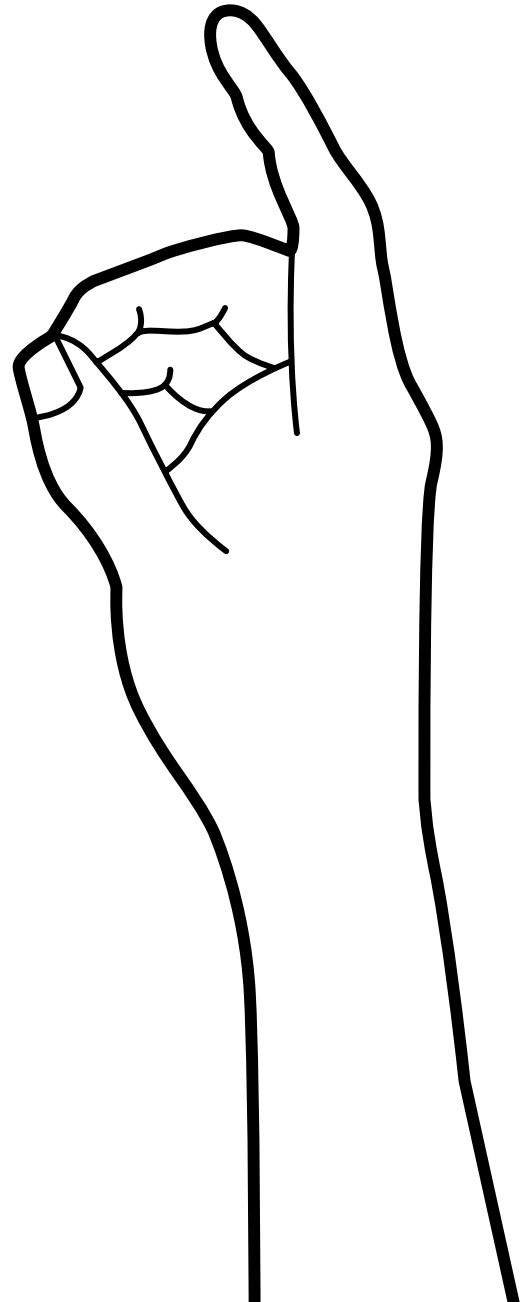
**Comoposition**

Optical centre

**The optical center is a point that attracts the viewer's eye unless other visual elements pull the eye elsewhere.**



● **Colour**

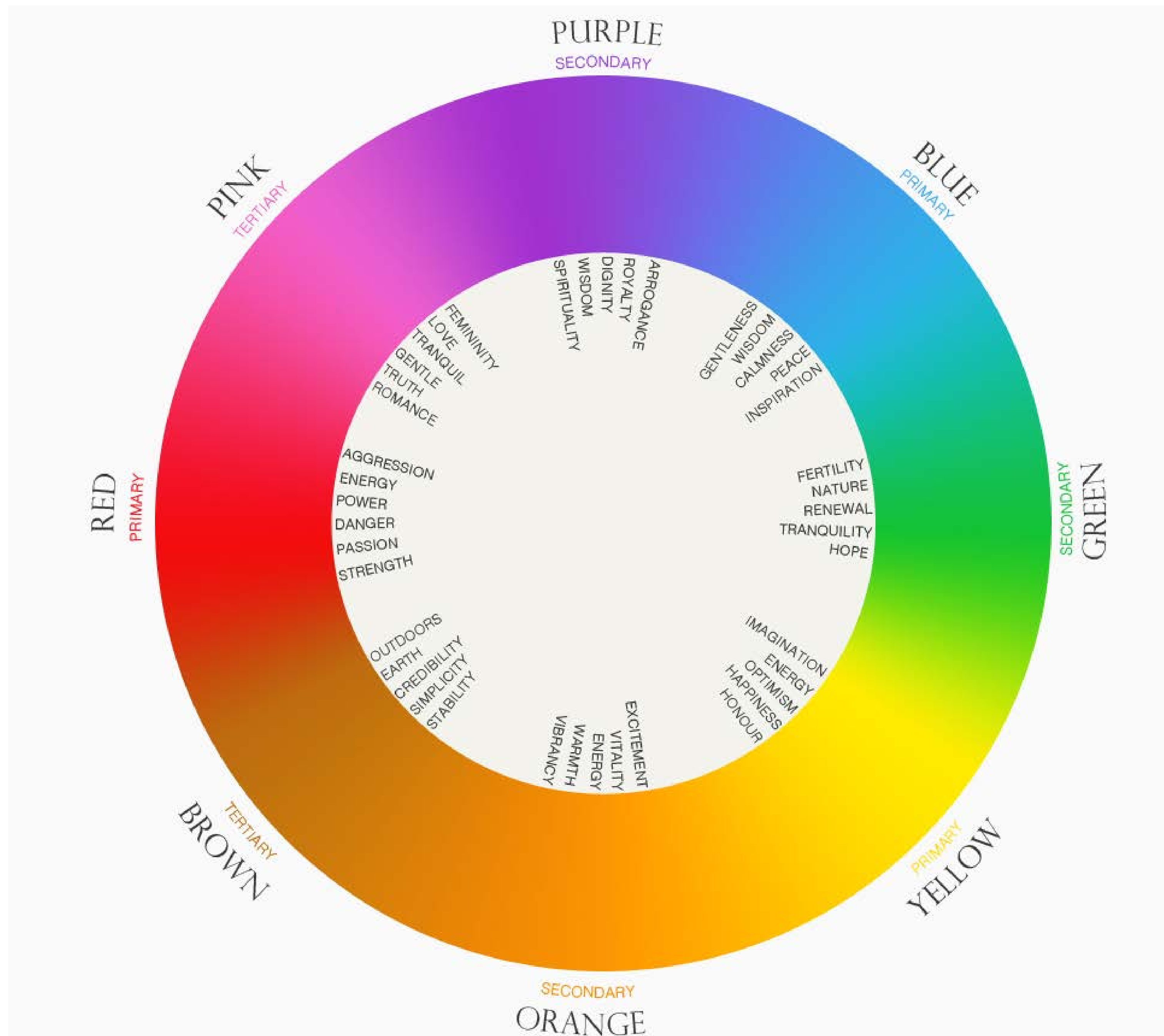


## Colour

Meaning of colour is always completely accepted subjectively. The perception depends on two imperfect human organs – eyes and brain, depends on light waves.

Colour has a powerful function in graphic design.

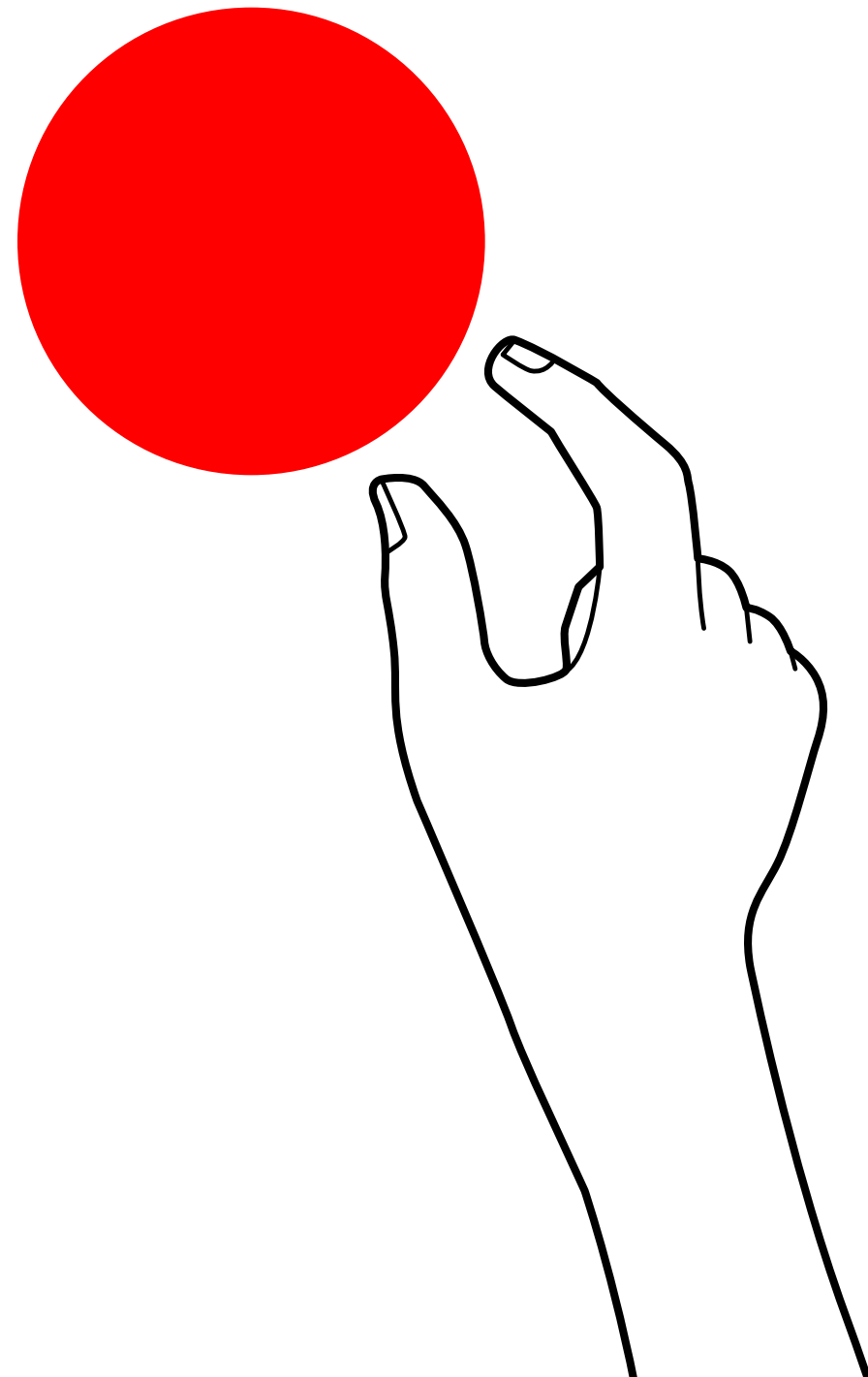
Colour defines hue, saturation and lightness.



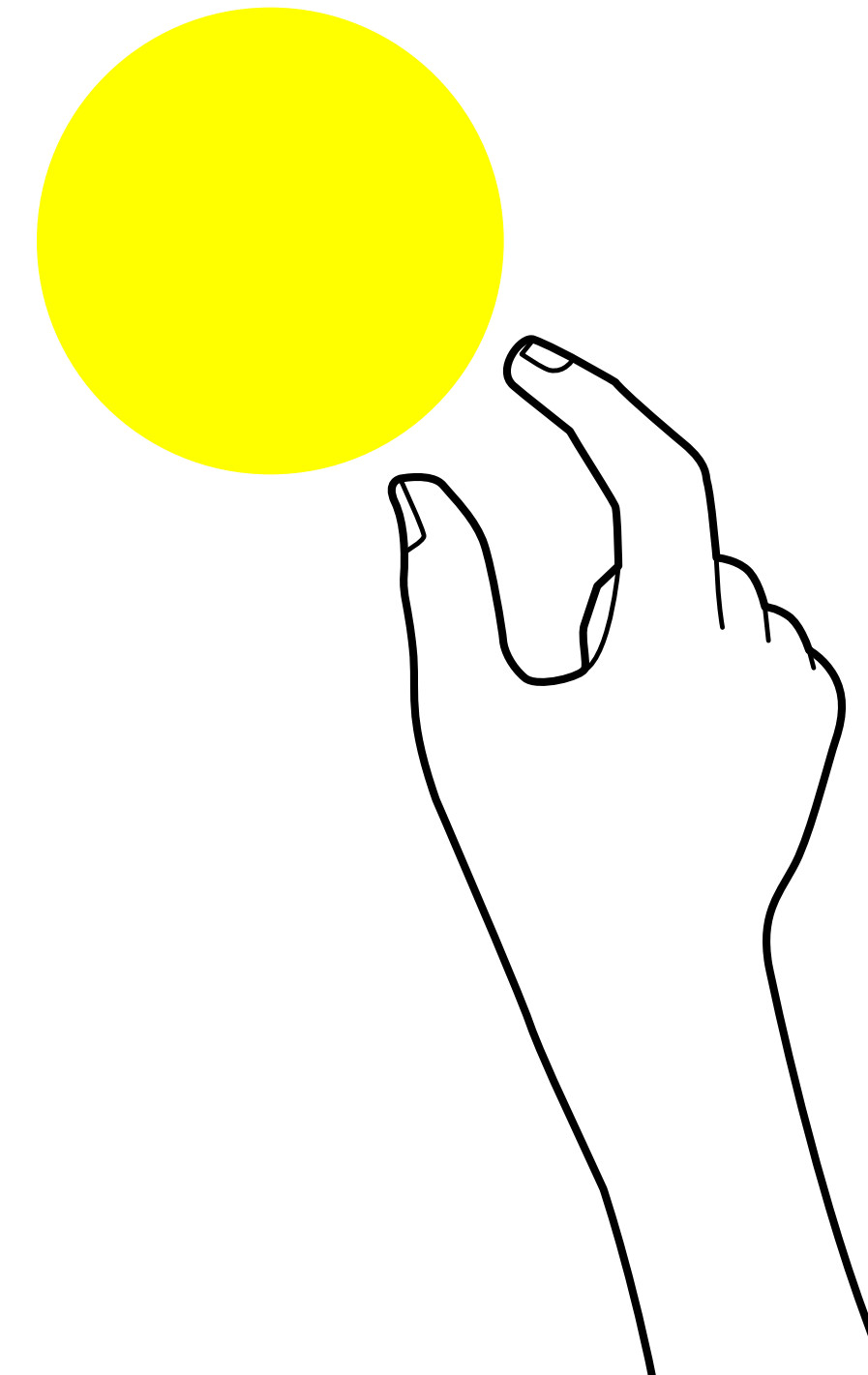
# Colour

**Warmer colours appear heavier than cooler colours**

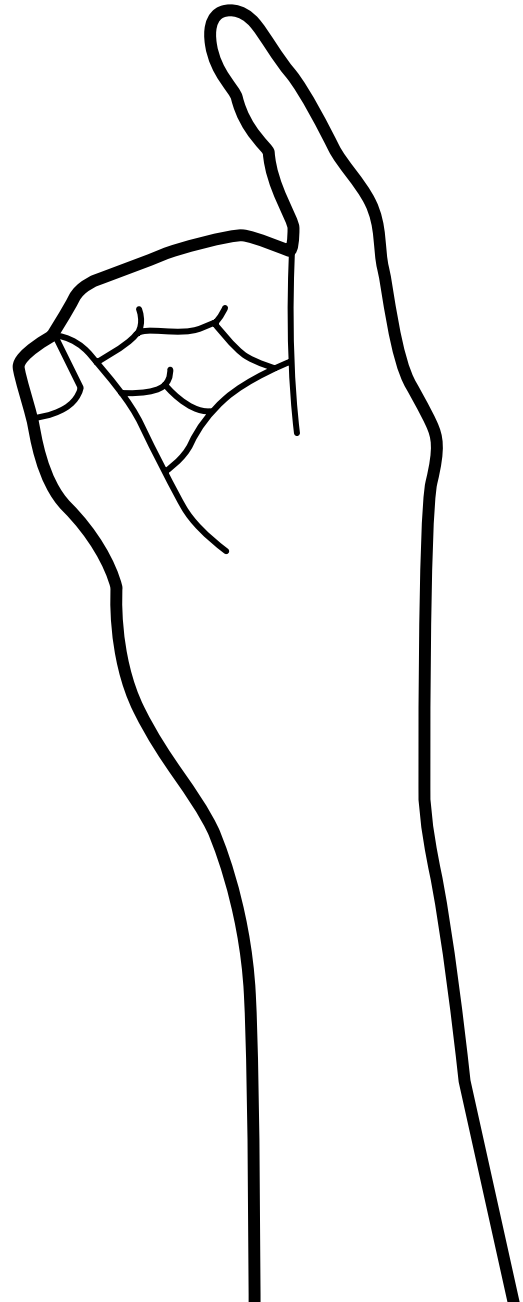
**Red colour – seems to be heaviest colour**



**Yellow colour – seems to be lightest**



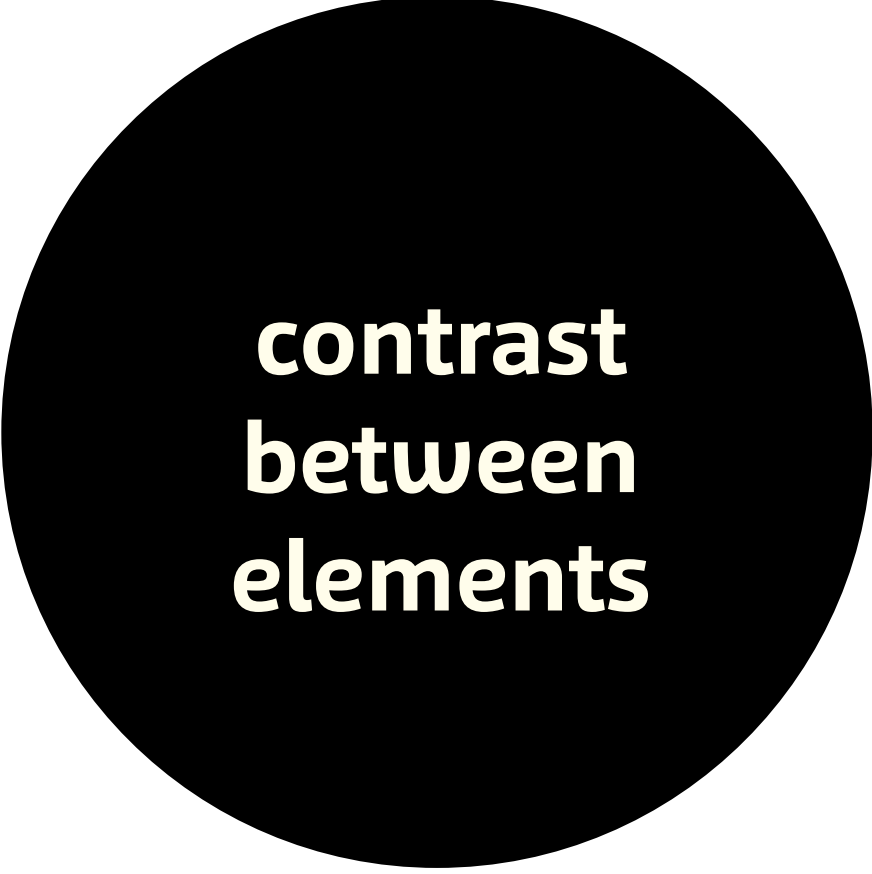
● **Contrast**



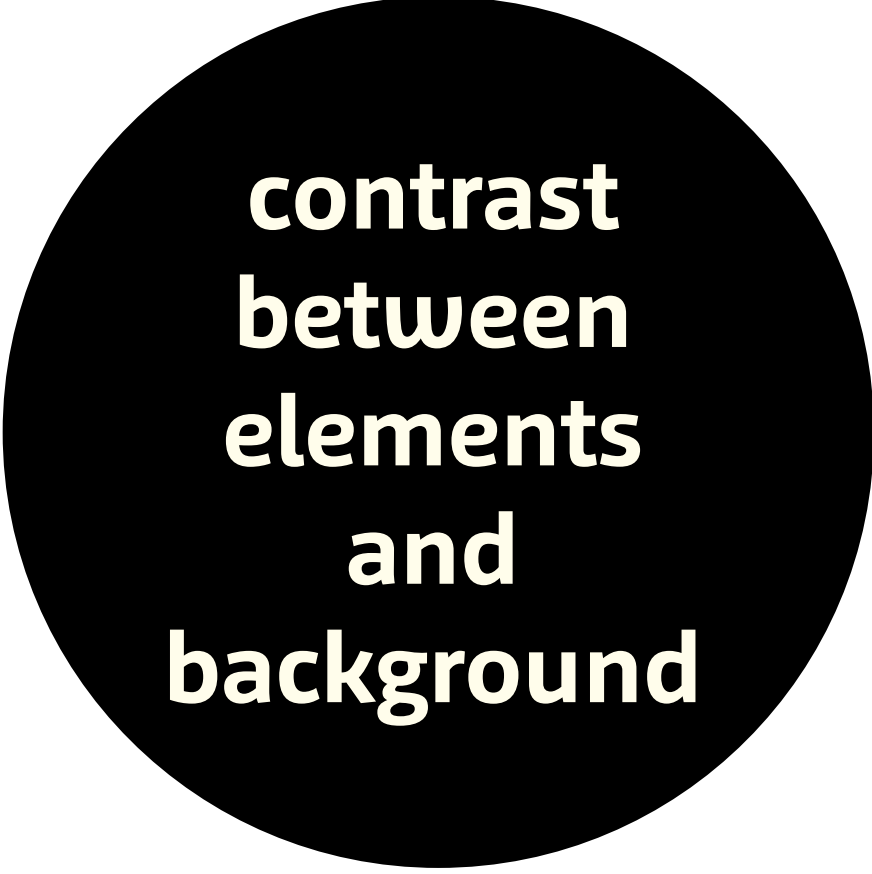




**colour contrast**



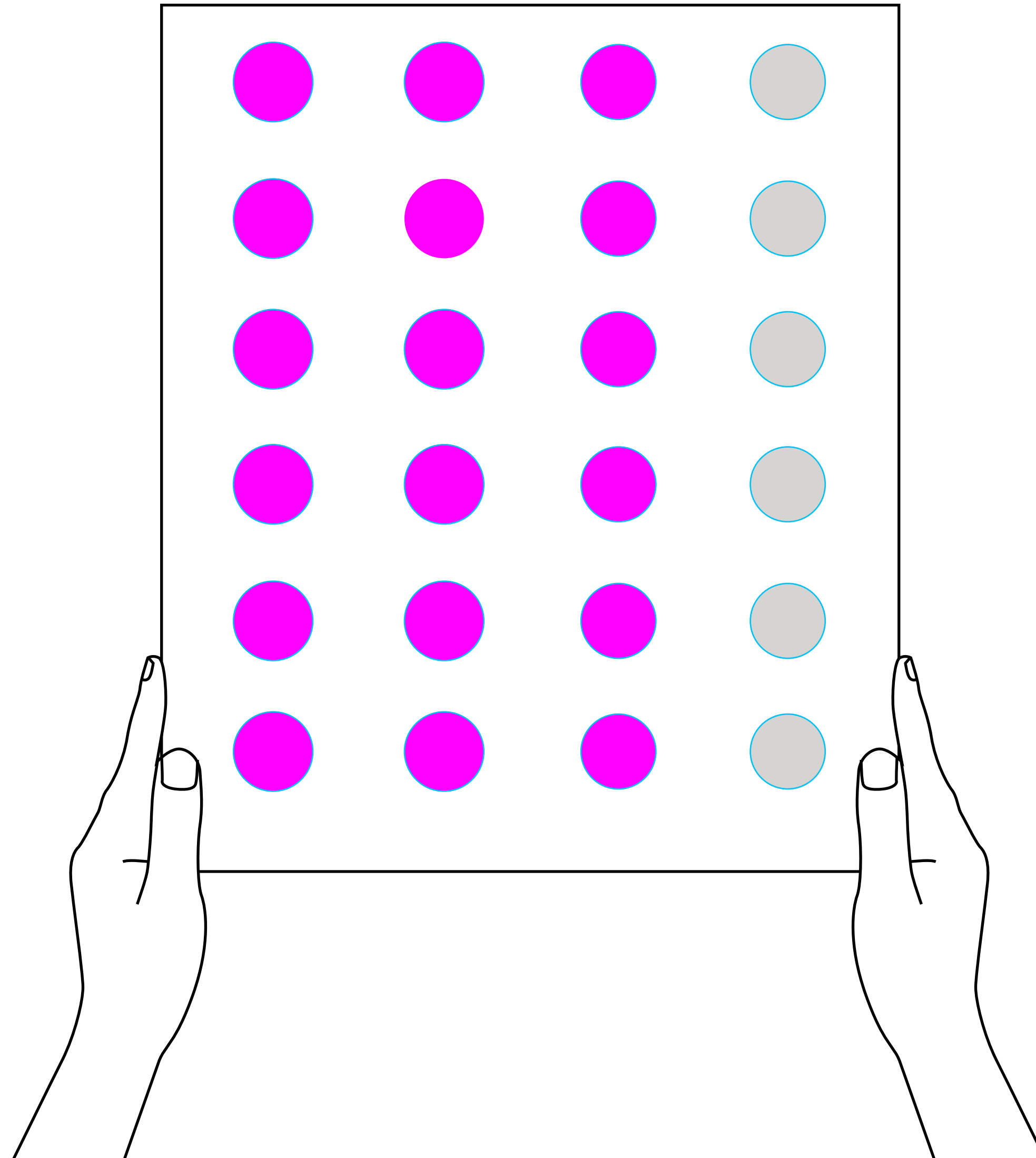
**contrast  
between  
elements**



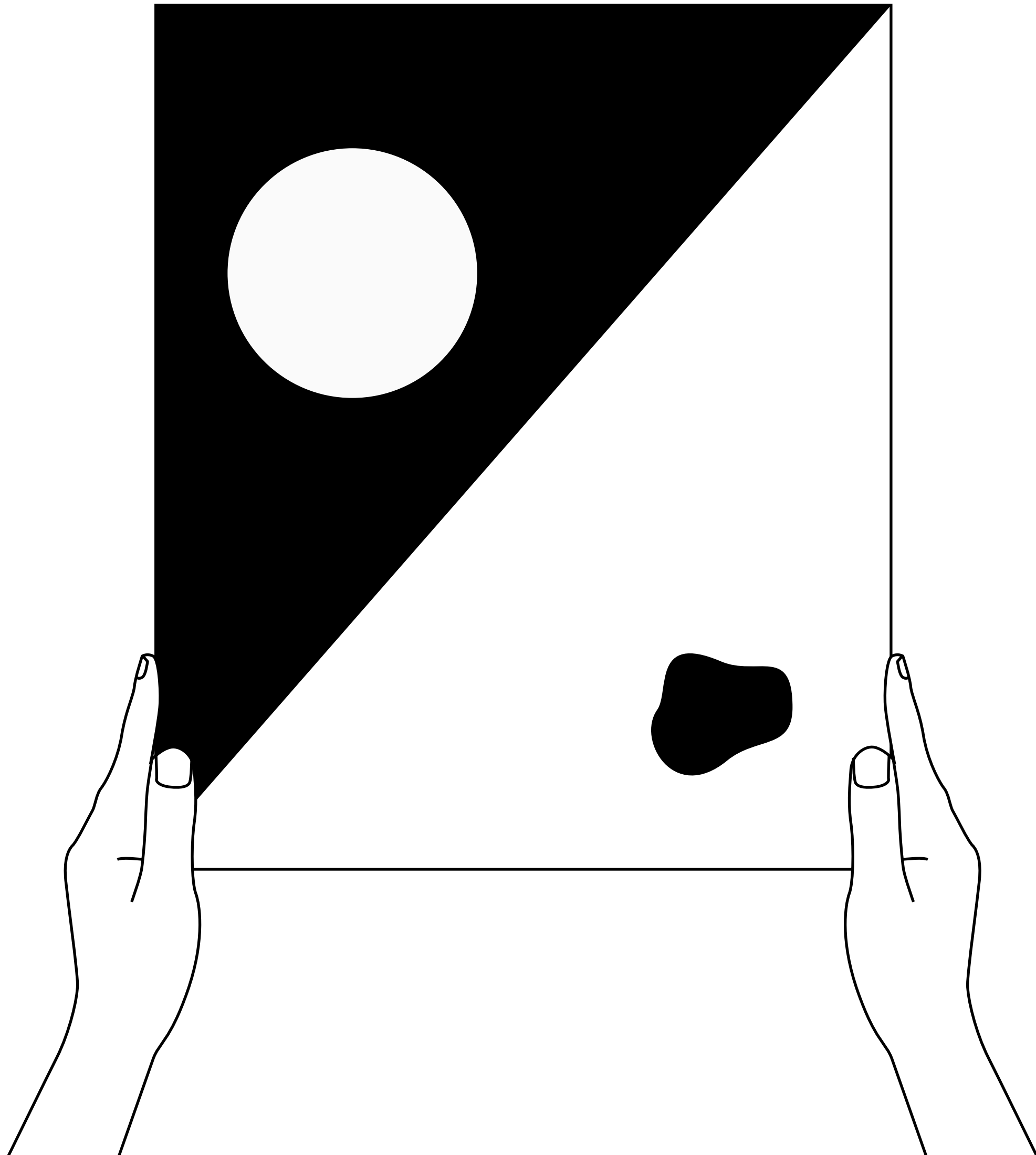
**contrast  
between  
elements  
and  
background**

**Contrast**  
Colour

**High-Intensity colours appear heavier than low-intensity ones**



**Contrast**  
Elements



**positive and neagtive space**

**geometric and biomorph shapes**

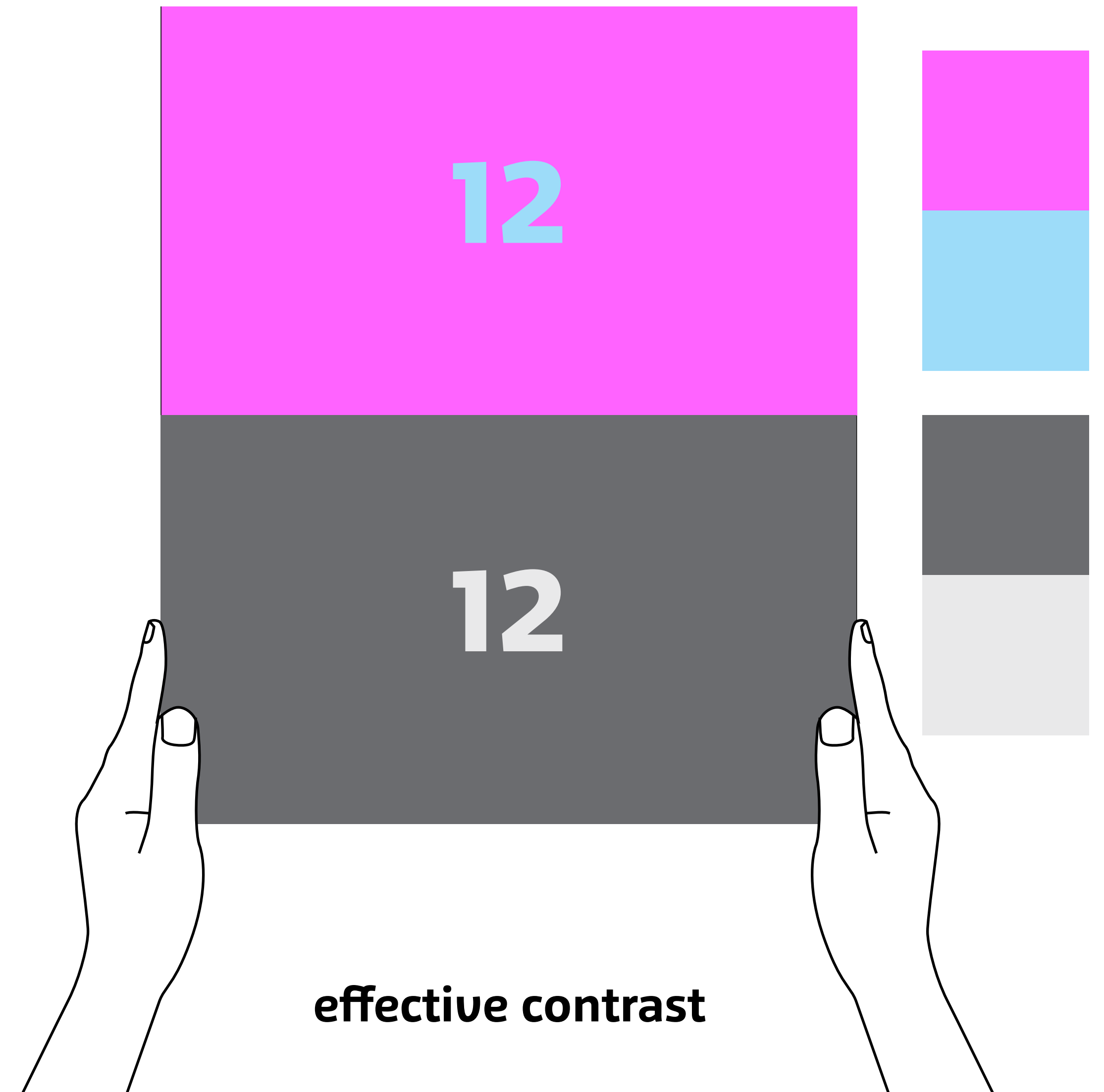
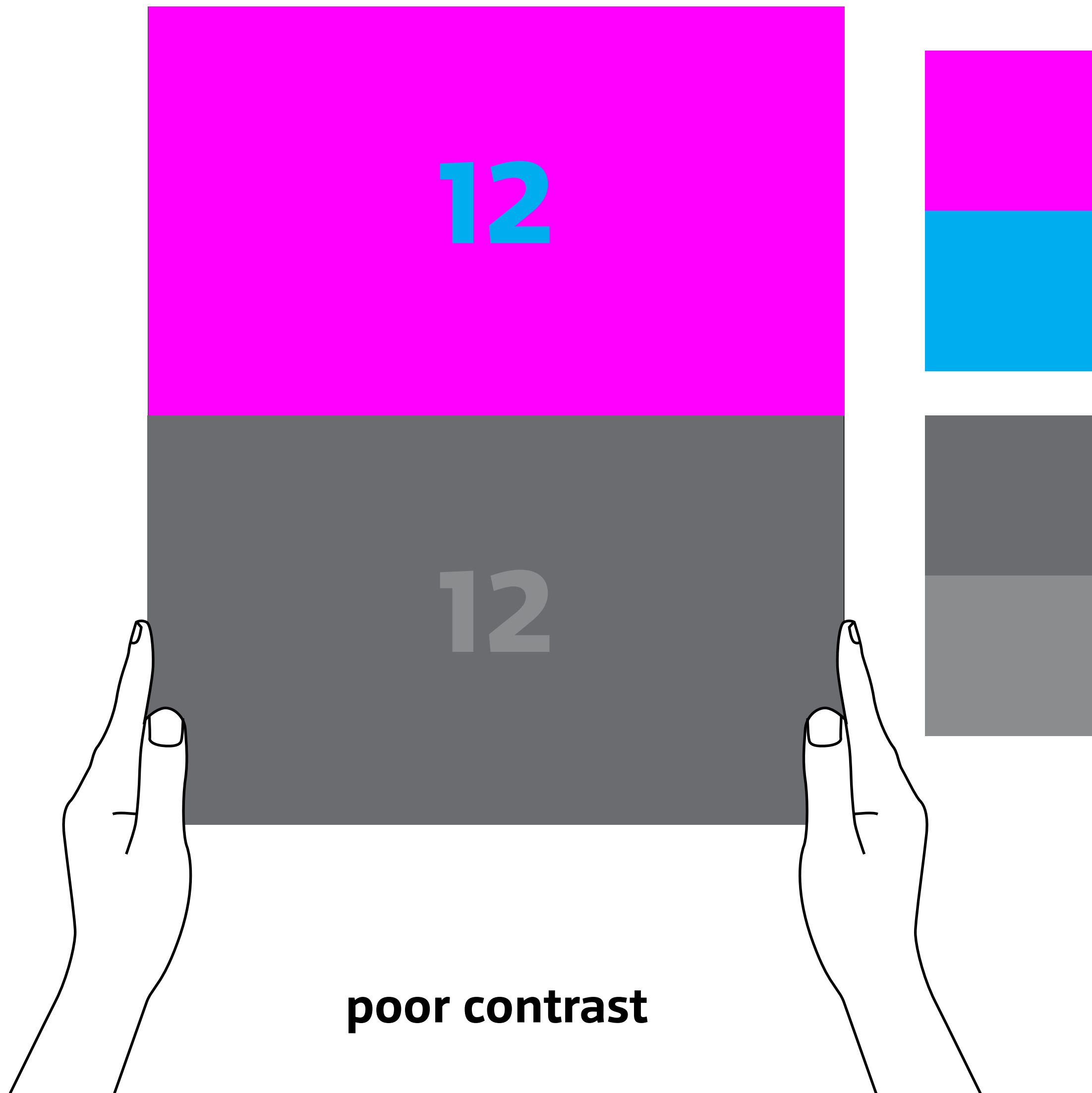
**softness and sharpness**

**stillness and movement**

**big and small**

**Contrast**  
Elements and background

**The higher the value-contrast, the heavier the weight of the object**



● **White space**





in Spain

# Housing

- government quarters
- rental guaranty
- on-the-economy

ON ANY permanent change of station, housing, or rather its availability, becomes the most important question asked by the service family. The common problems you meet in the United States are somewhat magnified on an overseas movement because of differences in language, law and custom. Actually, at least for Spain so our experiences have proved, these problems aren't very big at all if you're told beforehand what to expect.

First of all, at the time this booklet was published, automatic concurrent travel of dependents to Spain was authorized only for colonels and general officers. All other military personnel must apply to the appropriate overseas commander for concurrent travel. Specific instructions on how to do this can be obtained from your personnel officer. When the overseas commander grants approval for concurrent travel, he will tell you whether government quarters are or are not available. And, of course, this will determine many of your subsequent actions.

Government quarters consist of on-base and rental guaranty housing, some what similar to the so-called Wherry housing in the United States. On-base housing at the Air Force bases is very limited, ranging from 20-40 units and is restricted to key personnel.

The Rota Naval Base, where housing

in the local communities is extremely limited, there are 496 on-base units. There is no rental guaranty housing in the Rota area. Forty-six units are under construction at the Cartagena Naval Facility. There are none at the El Ferrol Naval Facility.

There are 20 units each at the aircraft control and warning sites at Villatobas (W-2) and Constantina (W-3). Twenty units are under construction at Rosas (W-4) and Benidorm (W-5). Housing is under design for some of the other sites.

#### RENTAL GUARANTY HOUSING

In the Madrid area (this includes the Joint U. S. Military Group, Spain; MAAG; NAVACTS, Spain; Headquarters Sixteenth Air Force; Headquarters, 65th Air Division; Torrejón Air Base and several smaller units there are 866 housing units, called Royal Oaks, located five miles north of Madrid and approximately 20 miles from Torrejón Air Base.

In Zaragoza, there are 222 units; in Sevilla (Morón and San Pablo air bases), there are 494 units about one mile from the city.

All units are spacious, although the bedrooms are somewhat smaller than American standards since emphasis has been placed on the living-dining areas.

A typical two-bedroom unit has a large terrace, living room, dining room, master bedroom, a smaller bedroom, bath, kitchen, utility room, storage room, and a maid's room and bath. The larger units are basically the same.

If you are notified that you are to occupy government quarters—either on-base or rental guaranty—you will be allowed to ship only 2,000 pounds of household goods, plus your hold baggage and hand luggage. All government quarters are adequately and comfortably furnished, including stove, refrigerator, automatic washer-dryer combination, vacuum cleaners, rugs and draperies. Also included are lamps, waste-paper baskets, porch furniture, ironing board, etc.

Personnel being assigned to Rota Naval Base should note that these units do not include washing machines or clothes driers.

Normally, you will need bring only dishes, silverware, pots and pans, linens (including pillows and blankets), and personal items. You will probably want to bring your small appliances—iron, mixer, toaster—actually, all items of this type work well in Spain and will save you as much work as they do in the United States. You should include in your 2,000 pound weight limit all special items for babies and small children since no items of this nature are furnished. This would include cribs, youth beds (if you use them), vaporizers, bottle sterilizers, etc. As a matter of fact, if you are traveling with a bottle-baby, we suggest you include in your hand baggage (that is, bring it with you) a bottle sterilizer—the type you can use on the top of a stove. By the way, plastic bottles are much more practical. Include extra nipples.

Consider your sports equipment, children's toys, etc., in the 2,000 pounds. Hold baggage, which will arrive much sooner than your furniture, should include those items you will immediately need. We found this meant the baby crib, some toys, a tool kit (hammer, saw, pliers, screwdrivers, etc.), dishes, pots and pans and other cooking paraphernalia, silverware, linens, blankets—enough to set up temporary house-keeping for about six to eight weeks.

In our hand baggage, other than clothing which is discussed elsewhere, we included extra tooth paste, razor blades, at least one toy per child, and other small personal items which you cannot conveniently buy while enroute.

#### ON ECONOMY HOUSING

Living on the economy, according to the many Americans who do so, provides a lively and interesting contrast to the American way of life. True, the differences are sometimes frustrating, but they are usually minor, and don't detract from the opportunity to learn the language and customs of Spain. Whether you eventually choose a house (of which there are very few) or an

White space, unprinted space without any element which surrounds other elements to make design more legible and lighter.

in Spain

# Housing

- government quarters
- rental guaranty
- on-the-economy

ON ANY permanent change of station, housing, or rather its availability, becomes the most important question asked by the service family. The common problems you meet in the United States are somewhat magnified on an overseas movement because of differences in language, law and custom. Actually, at least for Spain so our experiences have proved, these problems aren't very big at all if you're told beforehand what to expect.

First of all, at the time this booklet was published, automatic concurrent travel of dependents to Spain was authorized only for colonels and general officers. All other military personnel must apply to the appropriate overseas commander for concurrent travel. Specific instructions on how to do this can be obtained from your personnel officer. When the overseas commander grants approval for concurrent travel, he will tell you whether government quarters are or are not available. And, of course, this will determine many of your subsequent actions.

Government quarters consist of on-base and rental guaranty housing, some what similar to the so-called Wherry housing in the United States. On-base housing at the Air Force bases is very limited, ranging from 20-40 units and is restricted to key personnel.

The Rota Naval Base, where housing in the local communities is extremely limited, these are the on-base units. There is no rental guaranty housing in the Rota area. Forty-six units are under construction at the Cartagena Naval Facility. There are none at the El Ferrol Naval Facility.

There are 20 units each at the aircraft control and warning sites at Villatobas (W-2) and Constantina (W-3). Twenty units are under construction at Rosas (W-4) and Benidorm (W-5). Housing is under design for some of the other sites.

### RENTAL GUARANTY HOUSING

In the Madrid area (this includes the Joint U. S. Military Group, Spain; MAAG; NAVACTS, Spain; Headquarters Sixteenth Air Force; Headquarters, 65th Air Division; Torrejón Air Base and several smaller units there are 866 housing units, called Royal Oaks, located five miles north of Madrid and approximately 20 miles from Torrejón Air Base.

In Zaragoza, there are 222 units; in Sevilla (Morón and San Pablo air bases), there are 494 units about one mile from the city.

All units are spacious, although the bedrooms are somewhat smaller than American standards since emphasis has been placed on the living-dining areas.

A typical two-bedroom unit has a large terrace, living room, dining room, master bedroom, a smaller bedroom, bath, kitchen, utility room, storage room, and a maid's room and bath. The larger units are basically the same.

If you are notified that you are to occupy government quarters—either on-base or rental guaranty—you will be allowed to ship only 2,000 pounds of household goods, plus your hold baggage and hand luggage. All government quarters are adequately and comfortably furnished, including stove, refrigerator, automatic washer-dryer combination, vacuum cleaners, rugs and draperies. Also included are lamps, wastepaper baskets, porch furniture, ironing board, etc.

Personnel being assigned to Rota Naval Base should note that these units do not include washing machines or clothes driers.

Normally, you will need bring only dishes, silverware, pots and pans, linens (including pillows and blankets), and personal items. You will probably want to bring your small appliances—iron, mixer, toaster—actually, all items of this type work well in Spain and will save you as much work as they do in the United States. You should include in your 2,000 pound weight limit all special items for babies and small children since no items of this nature are furnished. This would include cribs, youth beds (if you use them), vaporizers, bottle sterilizers, etc. As a matter of fact, if you are traveling with a bottle-baby, we suggest you include in your hand baggage (that is, bring it with you) a bottle sterilizer—the type you can use on the top of a stove. By the way, plastic bottles are much more practical. Include extra nipples.

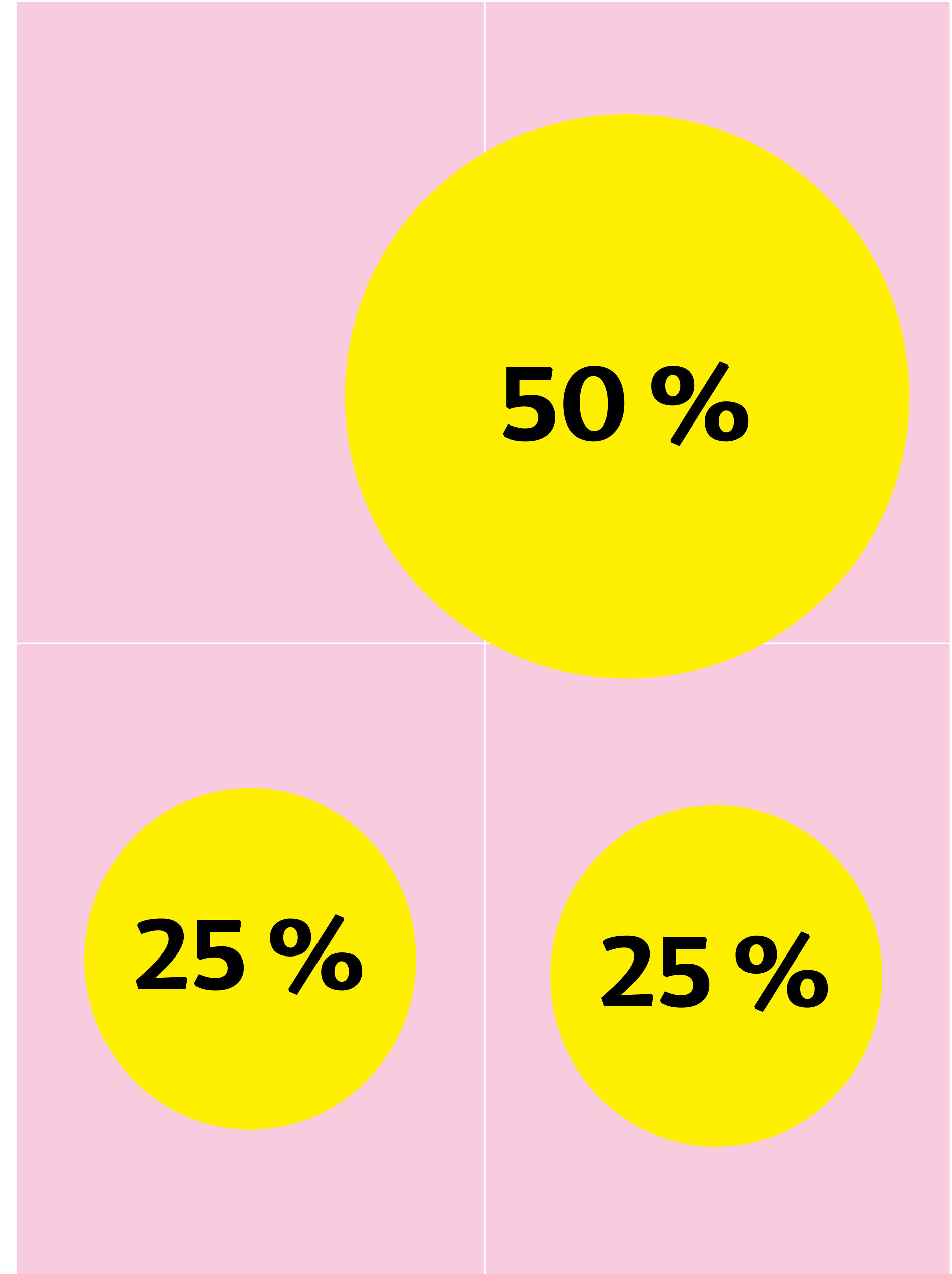
Consider your sports equipment, children's toys, etc., in the 2,000 pounds. Hold baggage, which will arrive much sooner than your furniture, should include those items you will immediately need. We found this meant the baby crib, some toys, a tool kit (hammer, saw, pliers, screwdrivers, etc.), dishes, pots and pans and other cooking paraphernalia, silverware, linens, blankets—enough to set up temporary house-keeping for about six to eight weeks.

In our hand baggage, other than clothing which is discussed elsewhere, we included extra tooth paste, razor blades, at least one toy per child, and other small personal items which you cannot conveniently buy while enroute.

### ON ECONOMY HOUSING

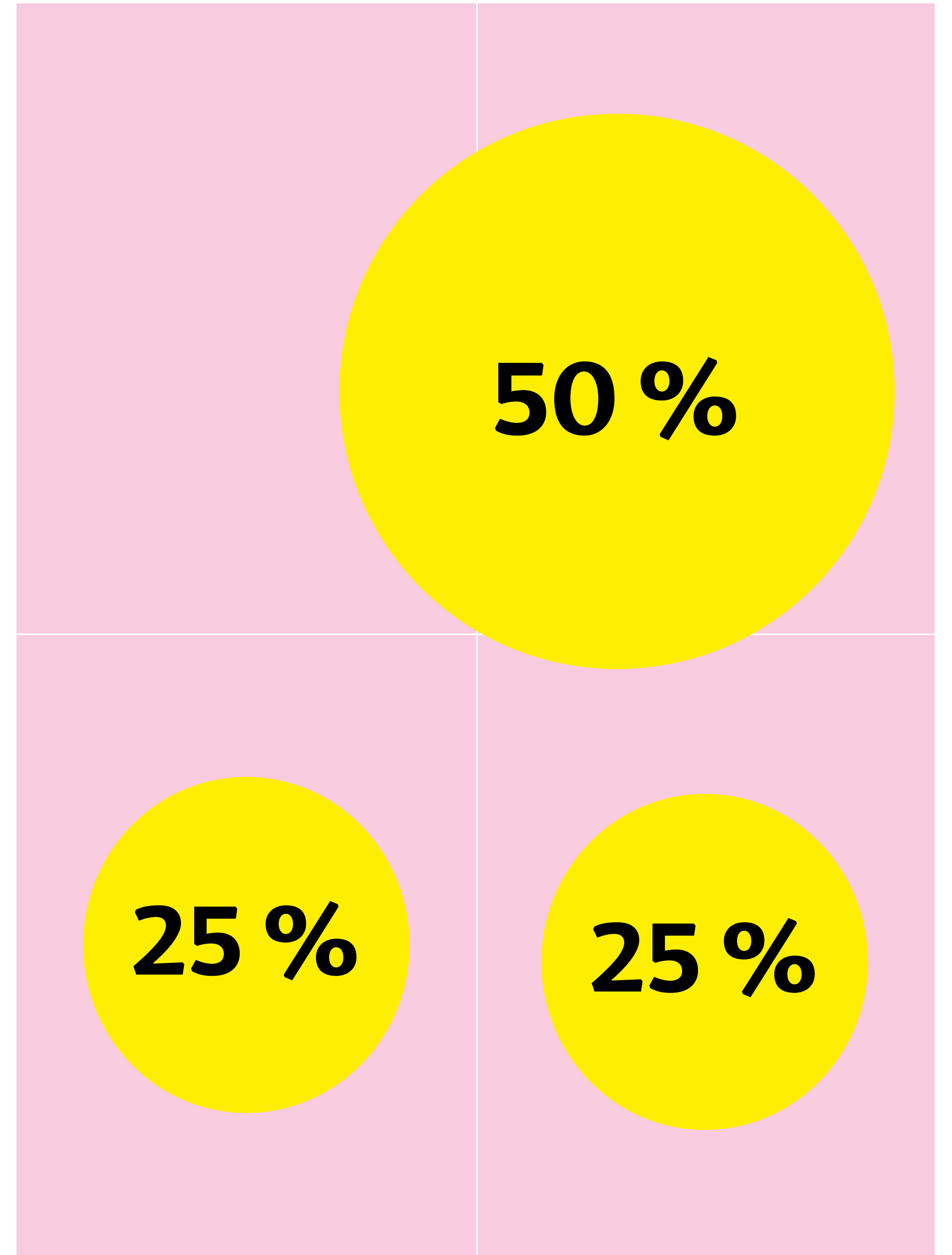
Living on the economy, according to the many Americans who do so, provides a lively and interesting contrast to the American way of life. True, the differences are sometimes frustrating, but they are usually minor, and don't detract from the opportunity to learn the language and customs of Spain. Whether you eventually choose a house (of which there are very few) or an

10



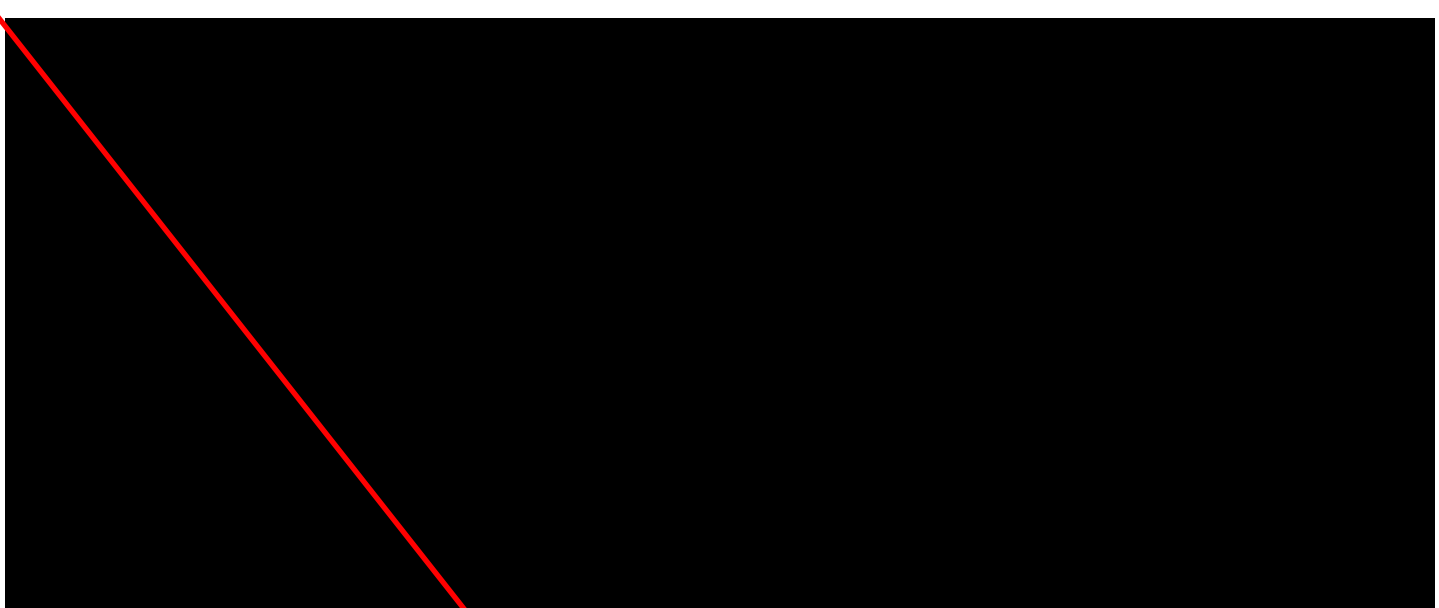
## White space

**Orientation in space according the white space.**



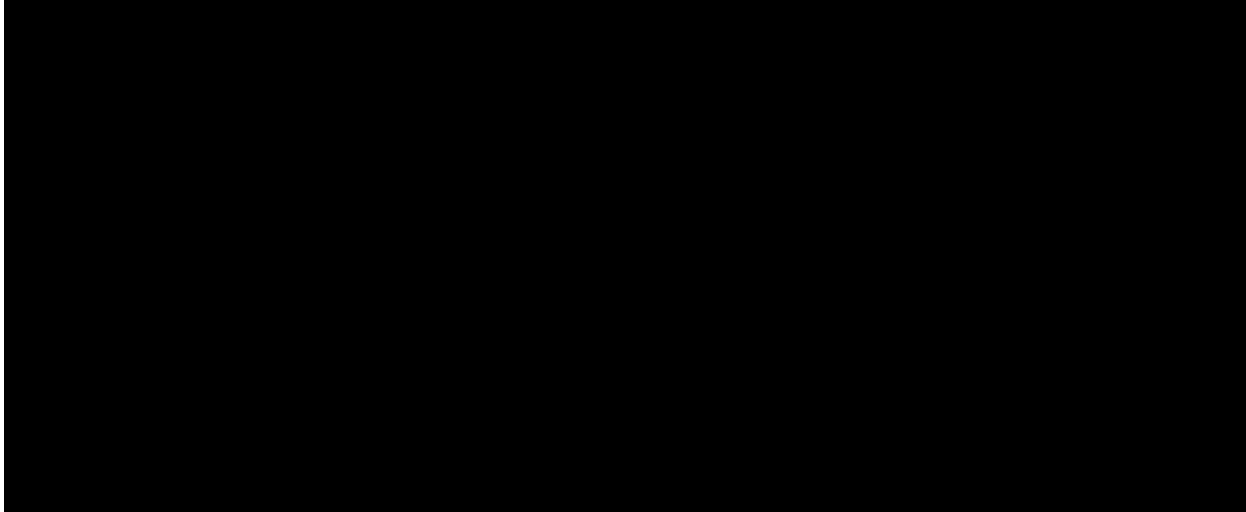


# White space



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec interdum mi purus, eu maximus mi efficitur eu. Vestibulum porttitor est in venenatis egestas. Morbi placerat maximus suscipit. Proin  
 Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec interdum mi purus, eu maximus mi efficitur eu. Vestibulum porttitor est in venenatis egestas. Morbi placerat maximus suscipit. Proin interdum diam massa. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum al-

iquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec interdum mi purus, eu maximus mi efficitur eu. Vestibulum porttitor est in venenatis egestas. Morbi placerat maximus suscipit. Proin  
 Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Proin interdum diam massa. Consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec interdum mi



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec interdum mi purus, eu maximus mi efficitur eu. Vestibulum porttitor est in venenatis egestas. Morbi placerat maximus suscipit. Proin  
 Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id

dolor tellus. Donec interdum mi purus, eu maximus mi efficitur eu. Vestibulum porttitor est in venenatis egestas. Morbi placerat maximus suscipit. Proin interdum diam massa. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam massa id, elementum vestibulum dolor. Curabitur id dolor tellus. Donec Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean neque quam, interdum non aliquet non, sagittis vel sapien. In risus purus, rutrum aliquam mas-

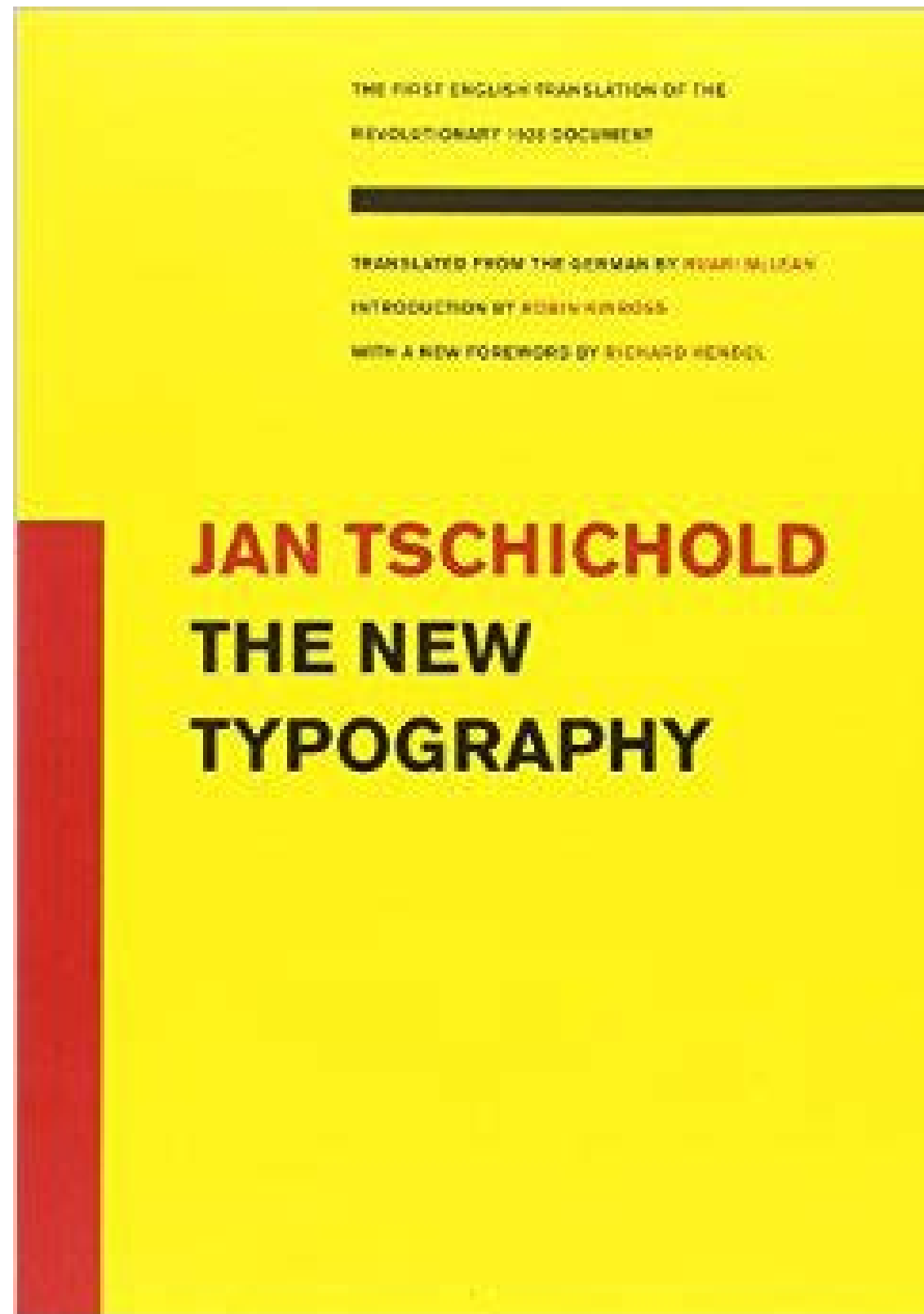
# White space between elements



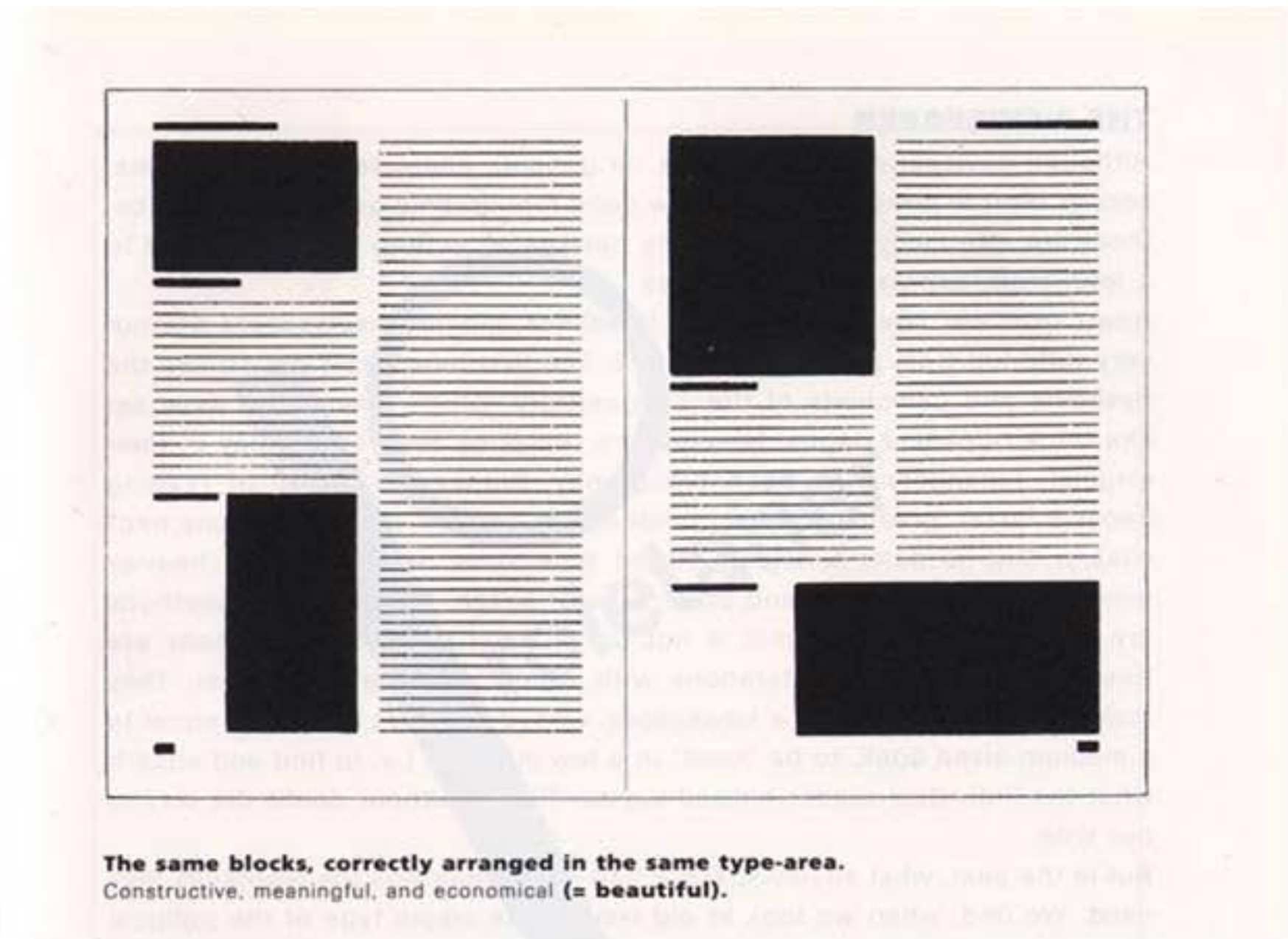


Case study  
White space

Jan Tschichold  
Die neue typographie



**How blocks used to be arranged in magazines.**  
Schematic, thoughtless centring of blocks. "Decorative," impractical, uneconomic (= ugly).



**The same blocks, correctly arranged in the same type-area.**  
Constructive, meaningful, and economical (= beautiful).

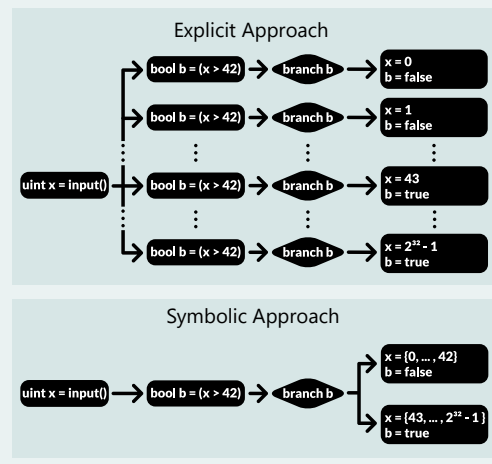
## DIVINE



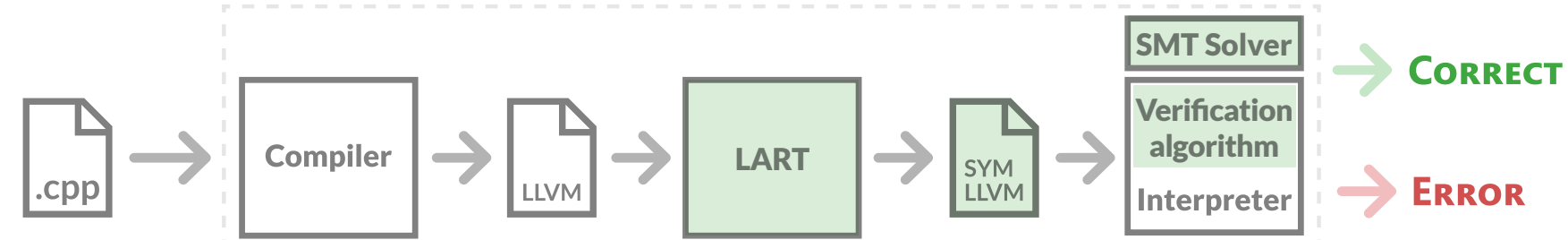
DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choice which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

## Symbolic States

Consider a simple program with 32 bit input variable  $x$  and a branch on the value of this variable. In the current DIVINE, this program gives rise to  $2^{32}$  possible memory configurations. In symbolic version, possible values of variables  $x$  and  $b$  are represented symbolically using bitvector formulae, therefore, there are only two possible configurations at the end of the program.



## Proposed Approach



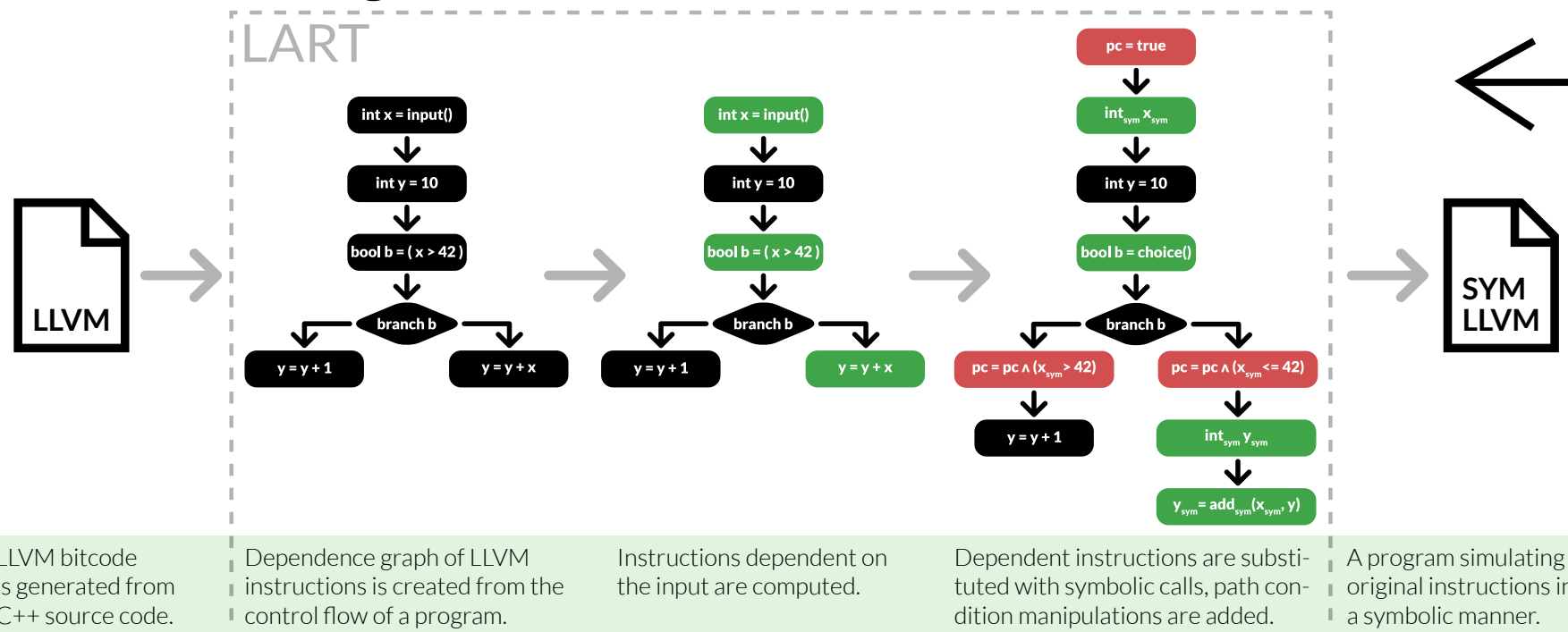
To take advantage of symbolic representation of states, we transform the LLVM bitcode in such a way that it represents variables which can contain values dependent on inputs symbolically. This transformation is performed by LART and is resented

in detail later. Apart from that, the verification algorithm is modified to handle symbolic states with the help of an SMT solver.

Our approach aims for minimizing changes to the LLVM interpreter that is used to execute instructions in DIVINE. The reason is that the interpreter is complex and performance tuned and therefore it is not desirable to make it even more complex by adding symbolic data manipulation into it. Instead, symbolic data are to be handled by the program itself. To encode symbolic manipulations into the program we transform the LLVM bitcode produced by the compiler and create symbolic LLVM from it. This not only minimizes changes to the interpreter, but

the transformation can also be used for different representation of symbolic data quite easily. The transformation is handled by LART – LLVM Abstraction & Refinement Tool. Furthermore, DIVINE's verification algorithm has to be modified. It has to check if symbolic states are valid (nonempty), that is if they can represent at least one concrete state. It also has to handle comparison of symbolic states. For both of these tasks, DIVINE has to extract SMT formulae from the program state and use SMT solver.

## Details of Program Transformation



LLVM bitcode is generated from C++ source code. Dependence graph of LLVM instructions is created from the control flow of a program. Instructions dependent on the input are computed. Dependent instructions are substituted with symbolic calls, path condition manipulations are added. A program simulating original instructions in a symbolic manner.

LART takes the LLVM bitcode of the program and libraries produced by the compiler and transforms it into a bitcode which manipulates data symbolically. In this modified program, any variable which can depend on an input value is represented symbolically using bitvector formulae. Bitvector formulae describe integers of fixed bit width with overflow and bitwise operations, and therefore

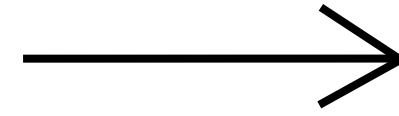
are well suited for exact representation of computer integers. All the manipulations with such variables have to be transformed to their symbolic versions which modify the formulae accordingly. Furthermore, any branch which depends on an input value has to put constraints on the possible values of symbolic variables (this constraint is given in the form of a path condition formula).

white space

# Case study

## White space

without white space



### Real-time Analysis of NetFlow Data for Generating Network Traffic Statistics using Apache Spark

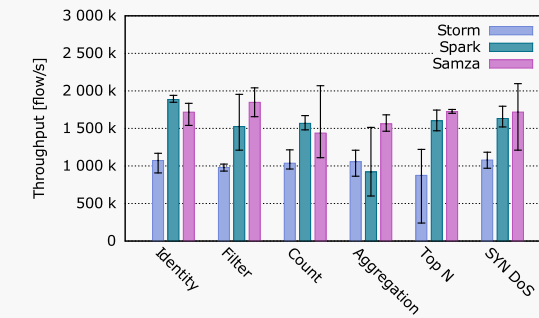
Milan Čermák, Tomáš Jirsík, Martin Laštovička

Institute of Computer Science, Masaryk University  
 Botanická 68a, 602 00, Brno, Czech Republic  
 E-mail: {cermak, jirsik, lastovicka}@ics.muni.cz



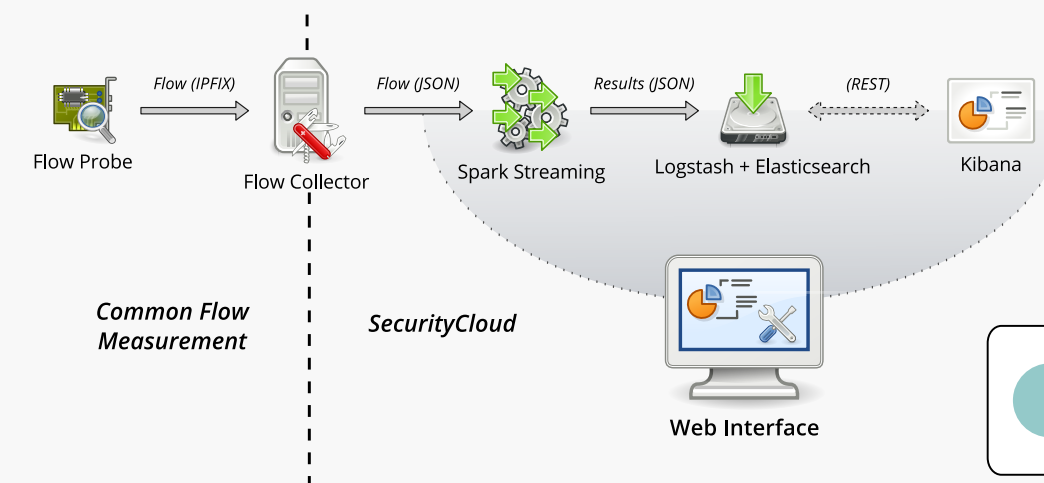
**Abstract** — We present a framework for the realtime generation of network traffic statistics on Apache Spark Streaming, a modern distributed stream processing system. Our previous results [1] showed that stream processing systems provide enough throughput to process a large volume of NetFlow data and hence they are suitable for network traffic monitoring. This demo describes the integration of Apache Spark Streaming into a current network monitoring architecture. We prove that it is possible to implement the same basic methods for NetFlow data analysis in the stream processing framework as in the traditional ones. Moreover, our stream processing implementation discovers new information which is not available when using traditional network monitoring approaches.

#### Systems Performance Benchmark — Four Nodes (32 vCPUs)



- Samza and Spark have a high-enough flow throughput and can be used for the analysis of data from multiple networks at the same time.
- Apache Spark system has been chosen as it offers an easy management and a high versatility in terms of the running environment and proprietary processing methods (e.g., sliding window).

#### Framework Architecture



The demonstration cluster consists of 7 virtual machines, one is dedicated to IPFIXcol, 5 to Spark and one to the Kibana and Web server. The following configuration is the same for all machines:

- 4 vCPUs Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz,
- 8GB 1600MMHz DIMM DRAM EDO,
- 85GB SCSI Disk with 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI,
- 10 Gbit/s network connection, 1 Gbit/s virtual NICs.

IPFIXcol is a flexible IPFIX flow data collector designed to be easily extensible by plugins. In our demonstration, we use only part of its wide functionality – data acquisition from multiple network probes and their transformation into a JSON data stream.

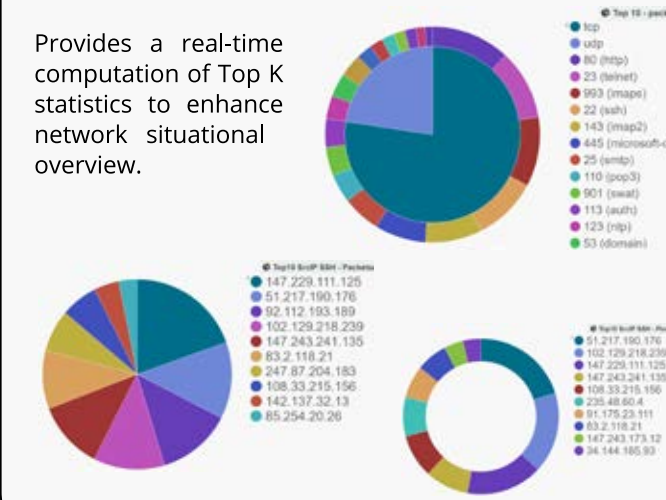
#### Statistics Volatility of Network Traffic Data

- Stream processing provides more accurate statistics about network traffic.
- Statistics generated by the stream processing showed increased volatility in results compared to traditional flow data processing approaches.
- Allows to observe short, but strong bursts of the network traffic that were lost due to the aggregation used in traditional batch approaches.



#### Real-time TOP K Statistics

Provides a real-time computation of Top K statistics to enhance network situational overview.

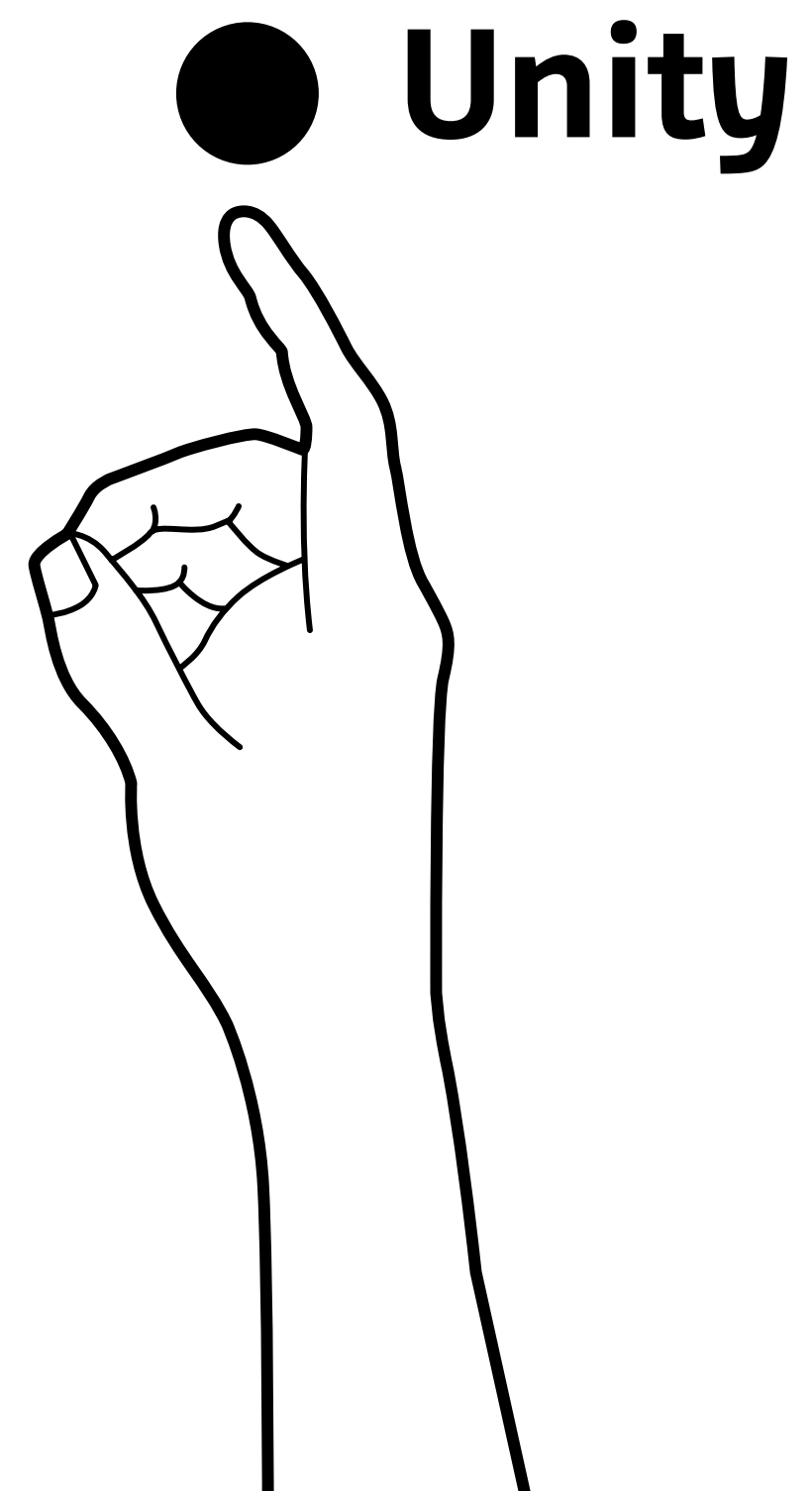


#### References

[1] M. Čermák, D. Tovarňák, M. Laštovička, and P. Čeleda. A Performance Benchmark for NetFlow Data Analysis on Distributed Stream Processing Systems. In Proceedings of NOMS, 2016.

#### Acknowledgements

This research was supported by the Technology Agency of the Czech Republic under No. TA04010062  
 Technology for processing and analysis of network data in big data concept.



All elements should  
collerate together

typography

graphic style  
of elements

grid

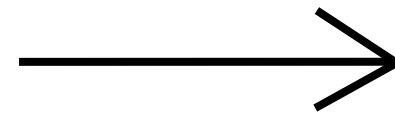
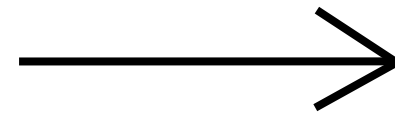


# Case study

## Graphic design style

san serif  
typography

left and right  
alignment



MASARYK UNIVERSITY

# EACirc

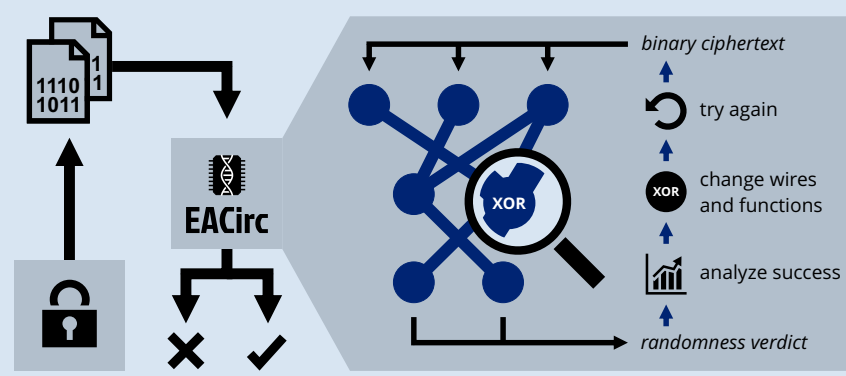
## Using genetics to improve encryption

Martin Ukrop, Petr Švenda, Marek Sýs, Václav Matyáš et alii

For me on GitHub  
github.com/crocs-muni/eacirc

### Problem statement

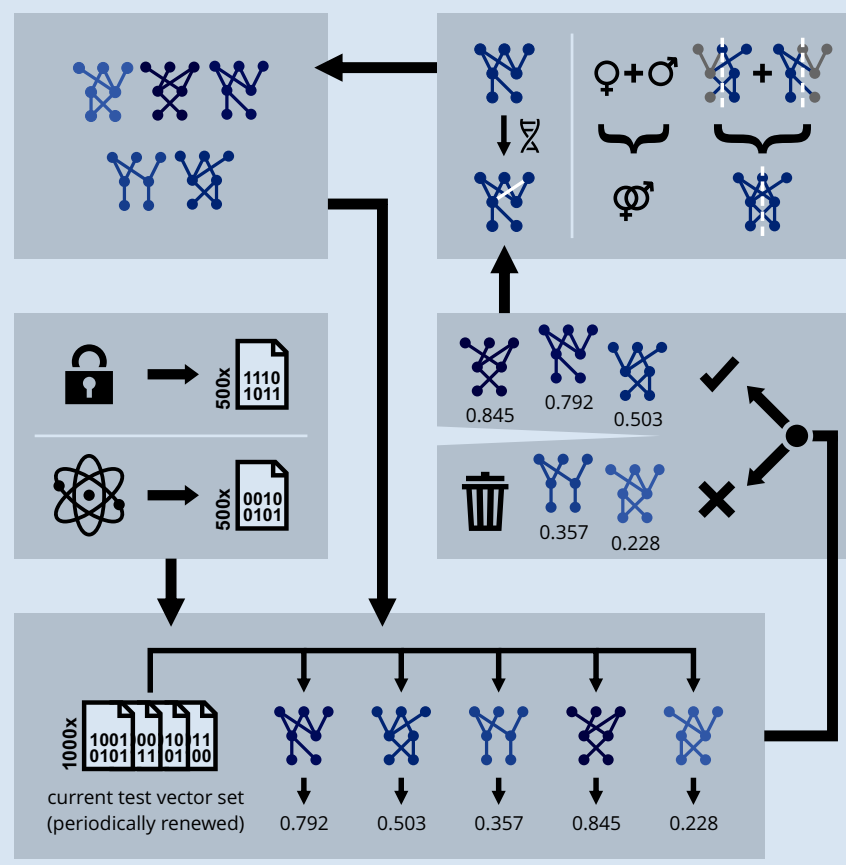
**Randomness testing**  
The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?  
EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.



**Iterative design**  
The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions).  
It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

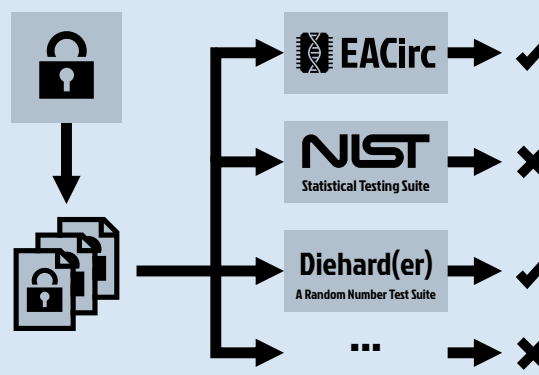
### EACirc workflow

- 1. Forming a population**  
A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.
- 2. Test vector generation**  
Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.
- 3. Fitness assessment**  
Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0,1].
- 4. Survival of the fittest**  
Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival.  
The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.
- 5. Mutation & crossover**  
To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population.



### Comparison to existing tools

**EACirc vs statistical testing**  
The standard way to assess randomness is to use batteries of statistical tests such as *NIST STS*, *Dieharder* or *TestU01*. We run them along with EACirc and compare the results.  
To have a fine-grained comparison, we have analyzed 77 different functions (*eStream*, *SHA-3* and *CAESAR* candidates). For 2-round *Hermes* and 1-round *Fubuki* we confidently surpass *NIST STS*.



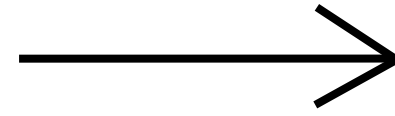
**Further information**  
Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).  
[1] Švenda, Ukrop, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications. Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.  
[2] Kubiček, Novotný, Švenda, Ukrop. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications. Vol. 8, iss. 1. 2016.

CRoCS Centre for Research on Cryptography and Security

This work was supported by the Czech Science Foundation project GAP202/11/0422.

# Style of typography

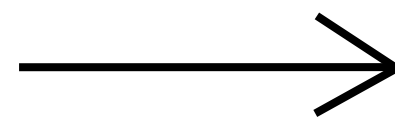
same styles of  
arrows



same colour  
of background  
shapes



same weights of  
strokes

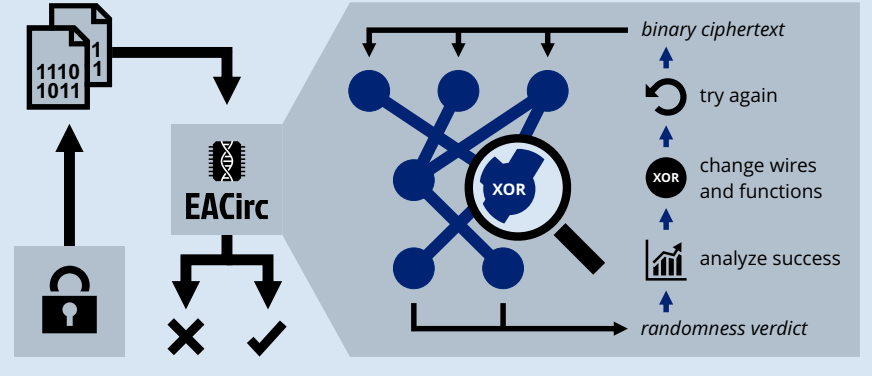


MASARYK UNIVERSITY **EACirc**  
Using genetics to improve encryption  
Martin Ukrop, Petr Švenda, Marek Sýs, Václav Matyáš et alii

Fort me on GitHub!  
github.com/crocs-muni/eacirc

### Problem statement

**Randomness testing**  
The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?  
EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.



**Iterative design**  
The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions). It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

### EACirc workflow

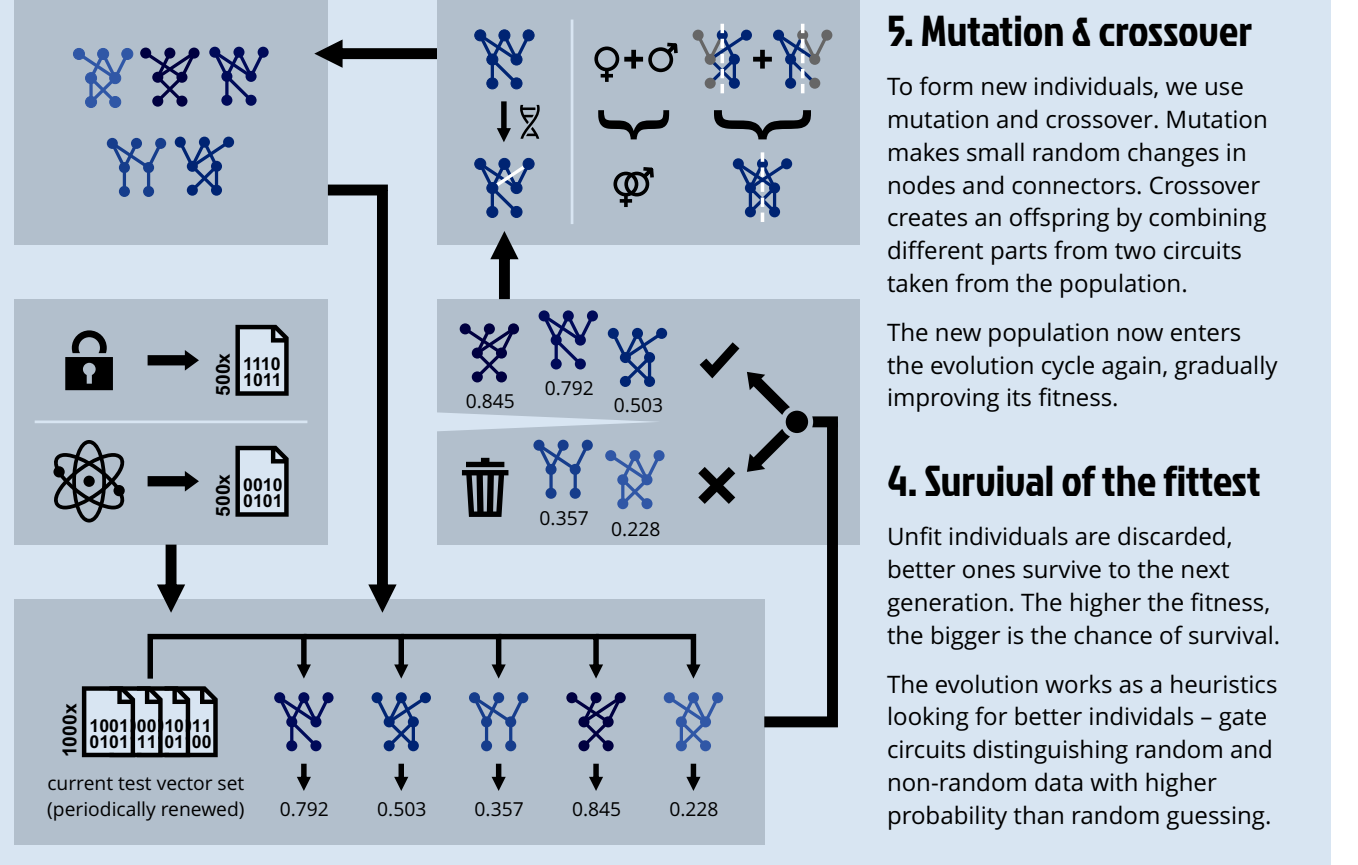
**1. Forming a population**  
A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.

**2. Test vector generation**  
Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.

**3. Fitness assessment**  
Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0,1].

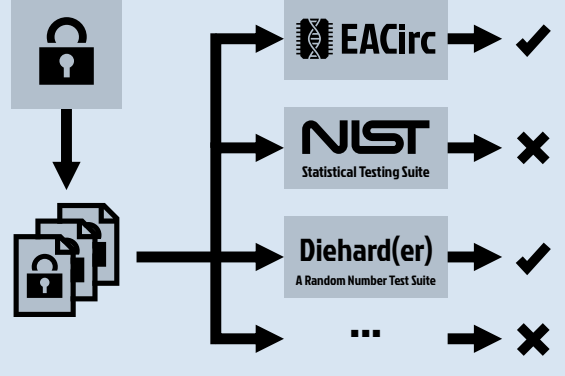
**4. Survival of the fittest**  
Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival. The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.

**5. Mutation & crossover**  
To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population.



### Comparison to existing tools

**EACirc vs statistical testing**  
The standard way to assess randomness is to use batteries of statistical tests such as *NIST STS*, *Dieharder* or *TestU01*. We run them along with EACirc and compare the results.  
To have a fine-grained comparison, we have analyzed 77 different functions (*eStream*, *SHA-3* and *CAESAR* candidates). For 2-round *Hermes* and 1-round *Fubuki* we confidently surpass *NIST STS*.

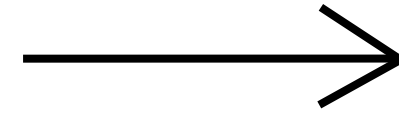



**Further information**  
Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).  
[1] Švenda, Ukrop, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications. Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.  
[2] Kubiček, Novotný, Švenda, Ukrop. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications. Vol. 8, iss. 1. 2016.

CRoCS Centre for Research on Cryptography and Security  
This work was supported by the Czech Science Foundation project GAP202/11/0422.

Same graphic style should be applied on each element


different styles  
of graphics





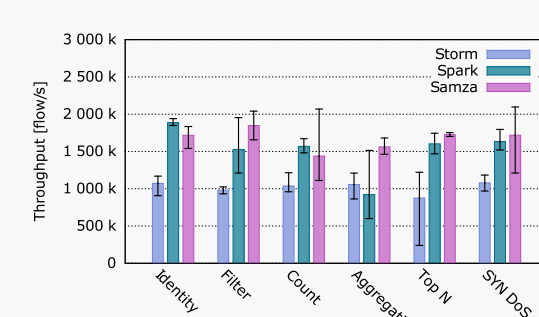
## Real-time Analysis of NetFlow Data for Generating Network Traffic Statistics using Apache Spark

Milan Čermák, Tomáš Jirsík, Martin Laštovička  
Institute of Computer Science, Masaryk University  
Botanická 68a, 602 00, Brno, Czech Republic  
E-mail: {cermak, jirsik, lastovicka}@ics.muni.cz



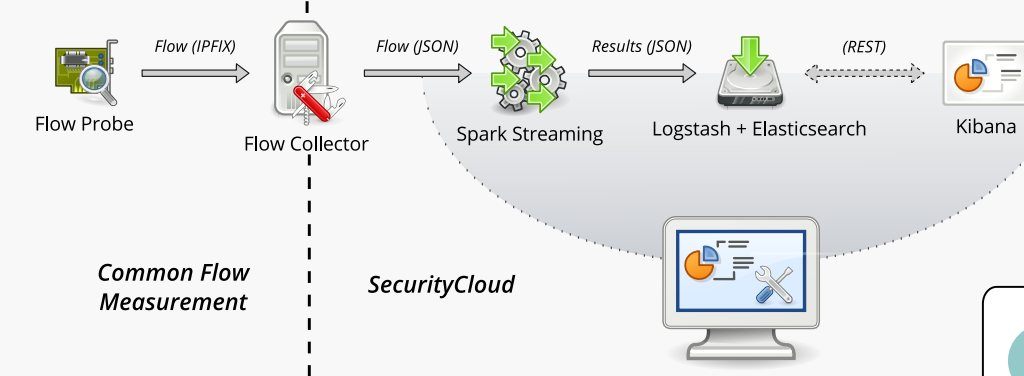
**Abstract** — We present a framework for the realtime generation of network traffic statistics on Apache Spark Streaming, a modern distributed stream processing system. Our previous results [1] showed that stream processing systems provide enough throughput to process a large volume of NetFlow data and hence they are suitable for network traffic monitoring. This demo describes the integration of Apache Spark Streaming into a current network monitoring architecture. We prove that it is possible to implement the same basic methods for NetFlow data analysis in the stream processing framework as in the traditional ones. Moreover, our stream processing implementation discovers new information which is not available when using traditional network monitoring approaches.

### Systems Performance Benchmark — Four Nodes (32 vCPUs)



- Samza and Spark have a high-enough flow throughput and can be used for the analysis of data from multiple networks at the same time.
- Apache Spark system has been chosen as it offers an easy management and a high versatility in terms of the running environment and proprietary processing methods (e.g., sliding window).

### Framework Architecture



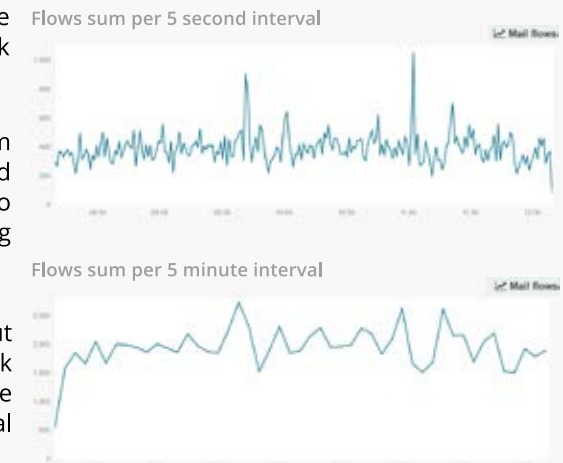
The demonstration cluster consists of 7 virtual machines, one is dedicated to IPFIXcol, 5 to Spark and one to the Kibana and Web server. The following configuration is the same for all machines:

- 4 vCPUs Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz,
- 8GB 1600MHz DIMM DRAM EDO,
- 85GB SCSI Disk with 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI,
- 10 Gbit/s network connection, 1 Gbit/s virtual NICs.

IPFIXcol is a flexible IPFIX flow data collector designed to be easily extensible by plugins. In our demonstration, we use only part of its wide functionality – data acquisition from multiple network probes and their transformation into a JSON data stream.

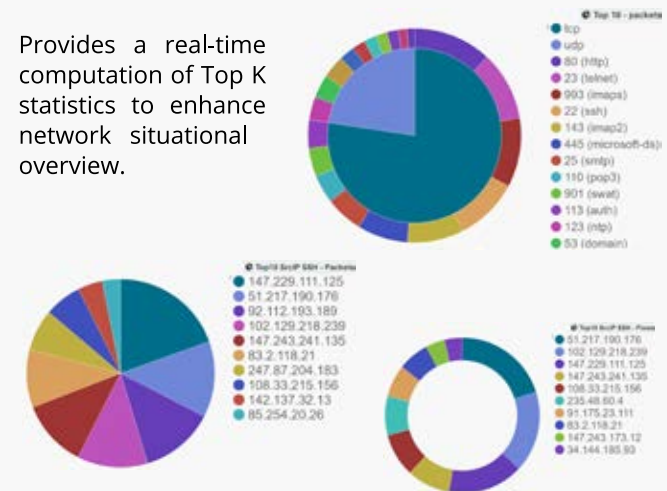
### Statistics Volatility of Network Traffic Data


- Stream processing provides more accurate statistics about network traffic.
- Statistics generated by the stream processing showed increased volatility in results compared to traditional flow data processing approaches.
- Allows to observe short, but strong bursts of the network traffic that were lost due to the aggregation used in traditional batch approaches.



### Real-time TOP K Statistics

Provides a real-time computation of Top K statistics to enhance network situational overview.





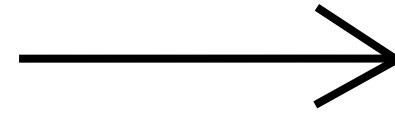
### References


[1] M. Čermák, D. Tovarňák, M. Laštovička, and P. Čeleda. *A Performance Benchmark for NetFlow Data Analysis on Distributed Stream Processing Systems*. In Proceedings of NOMS, 2016.


### Acknowledgements

**T A** This research was supported by the Technology Agency of the Czech Republic under No. TA04010062  
**Č R** Technology for processing and analysis of network data in big data concept.

Same graphic style should be applied on each element







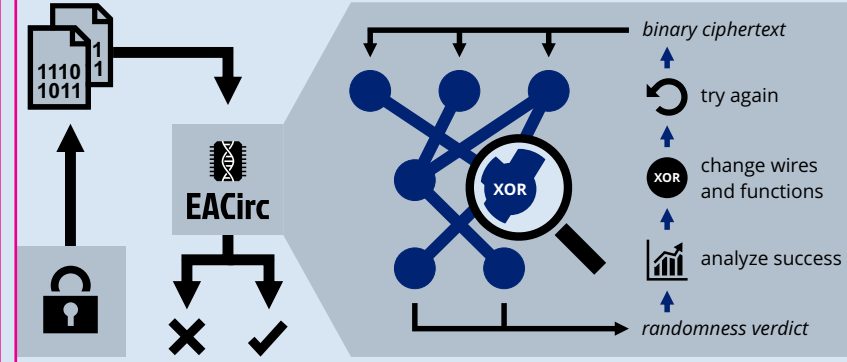
## Using genetics to improve encryption

Martin Ukrop, Petr Švenda, Marek Sýs, Václav Matyáš et alii

[Fork me on GitHub!](https://github.com/crocs-muni/eacirc)  
[github.com/crocs-muni/eacirc](https://github.com/crocs-muni/eacirc)

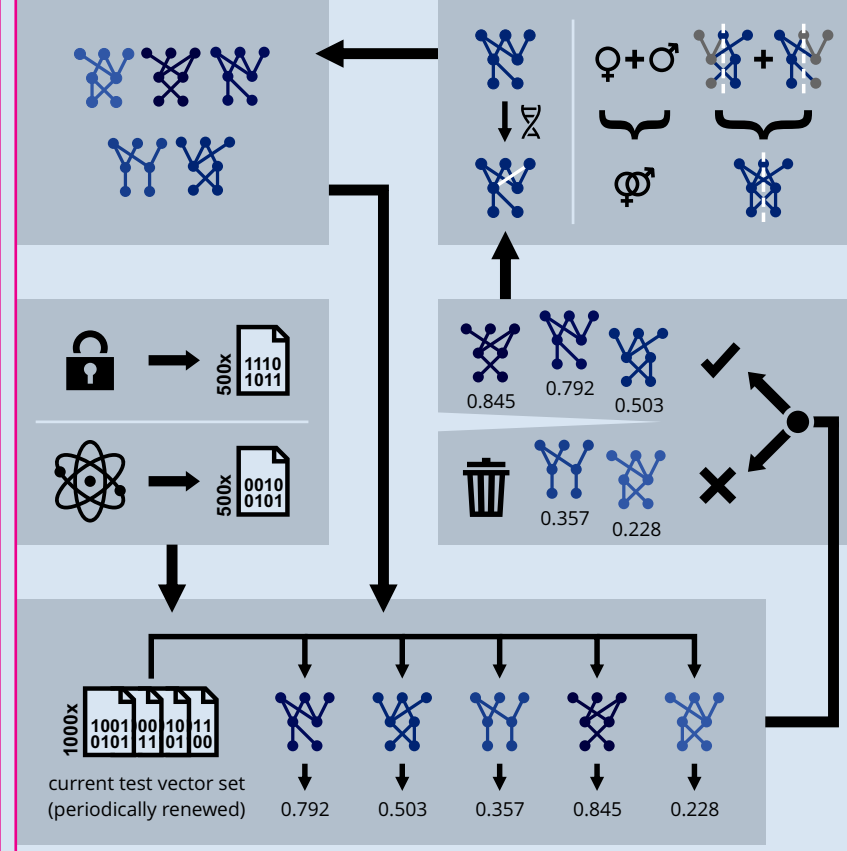

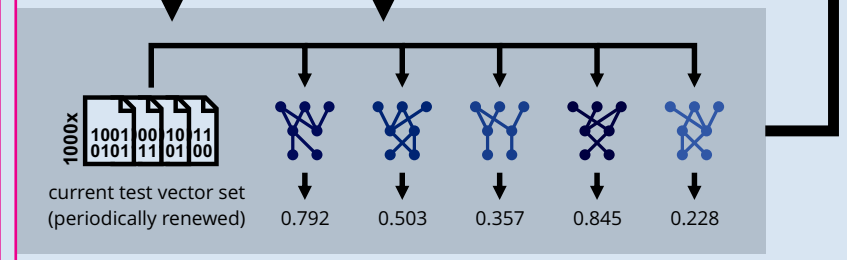
---

### Problem statement

<p><b>Randomness testing</b></p> <p>The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?</p> <p>EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.</p>		<p><b>Iterative design</b></p> <p>The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions). It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).</p>
---	---	--

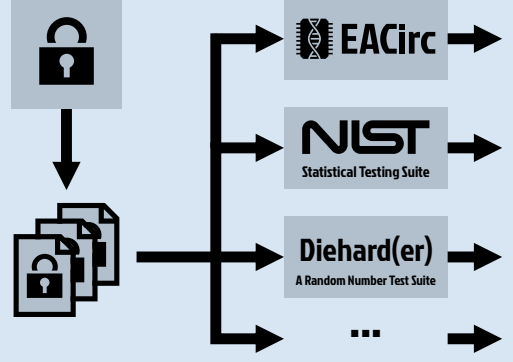
---


### EACirc workflow

<p><b>1. Forming a population</b></p> <p>A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.</p>		<p><b>5. Mutation &amp; crossover</b></p> <p>To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population.</p>
<p><b>2. Test vector generation</b></p> <p>Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.</p>		<p><b>4. Survival of the fittest</b></p> <p>Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival.</p> <p>The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.</p>
<p><b>3. Fitness assessment</b></p> <p>Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0,1].</p>		<p><b>5. Mutation &amp; crossover</b></p> <p>To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population.</p>

---


### Comparison to existing tools

<p><b>EACirc vs statistical testing</b></p> <p>The standard way to assess randomness is to use batteries of statistical tests such as <i>NIST STS</i>, <i>Dieharder</i> or <i>TestU01</i>. We run them along with EACirc and compare the results.</p> <p>To have a fine-grained comparison, we have analyzed 77 different functions (<i>eStream</i>, <i>SHA-3</i> and <i>CAESAR</i> candidates). For 2-round <i>Hermes</i> and 1-round <i>Fubuki</i> we confidently surpass <i>NIST STS</i>.</p>		<p><b>Further information</b></p> <p>Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).</p> <p>[1] Švenda, Ukrop, Matyáš. <i>Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits</i>. In: E-Business and Telecommunications. Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.</p> <p>[2] Kubiček, Novotný, Švenda, Ukrop. <i>New results on reduced-round Tiny Encryption Algorithm using genetic programming</i>. IEEE Infocommunications. Vol. 8, iss. 1. 2016.</p>
--	---	--

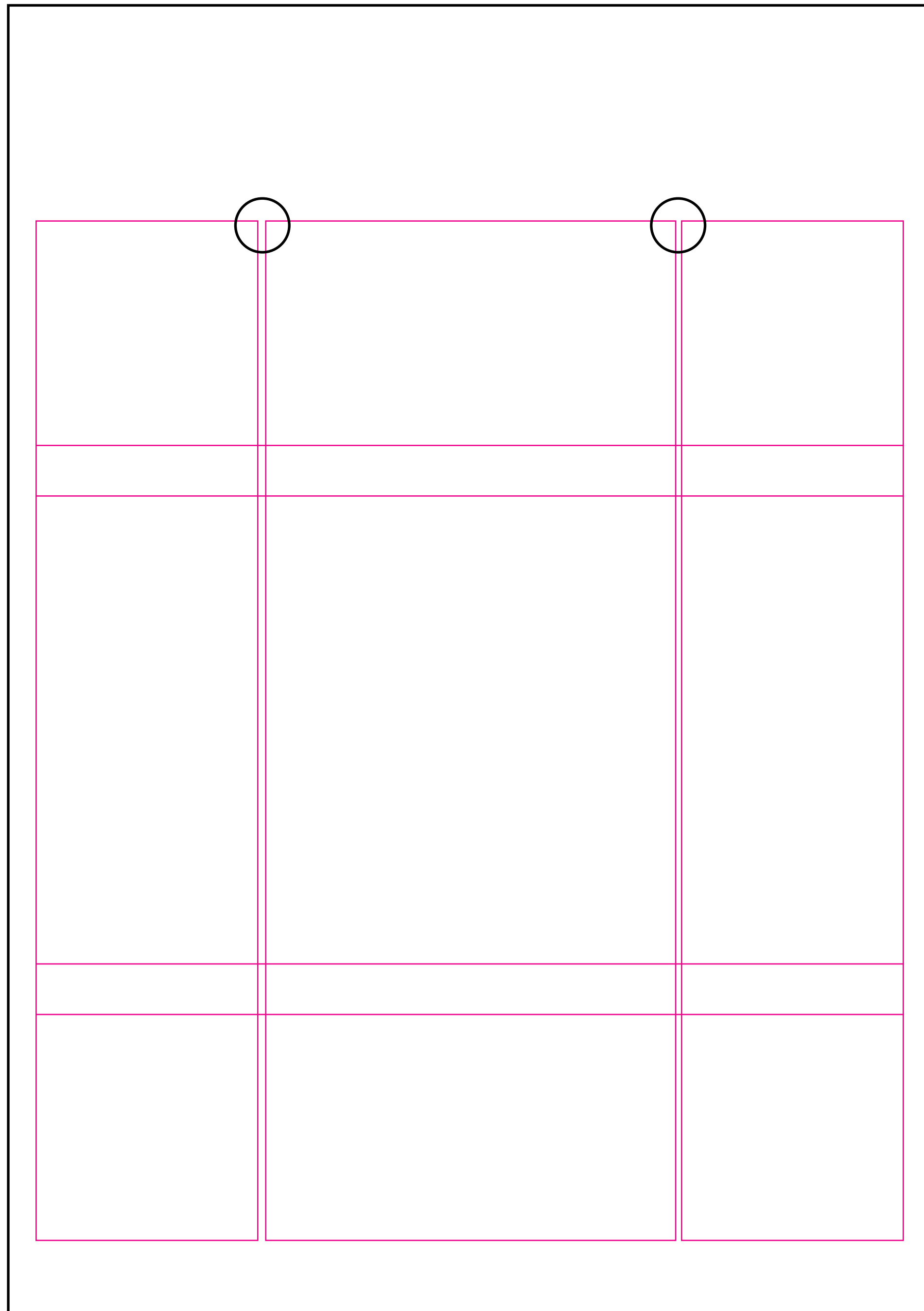
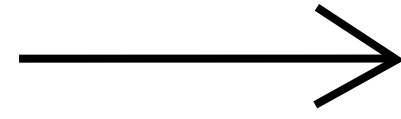
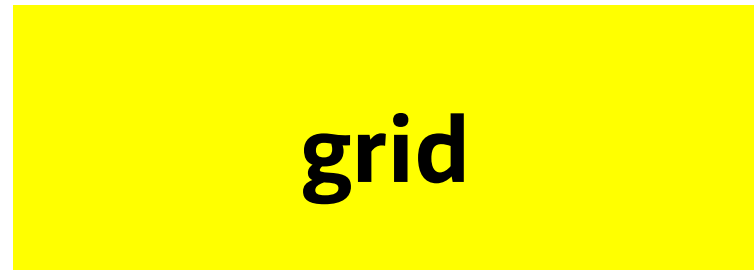


Centre for Research on  
Cryptography and Security

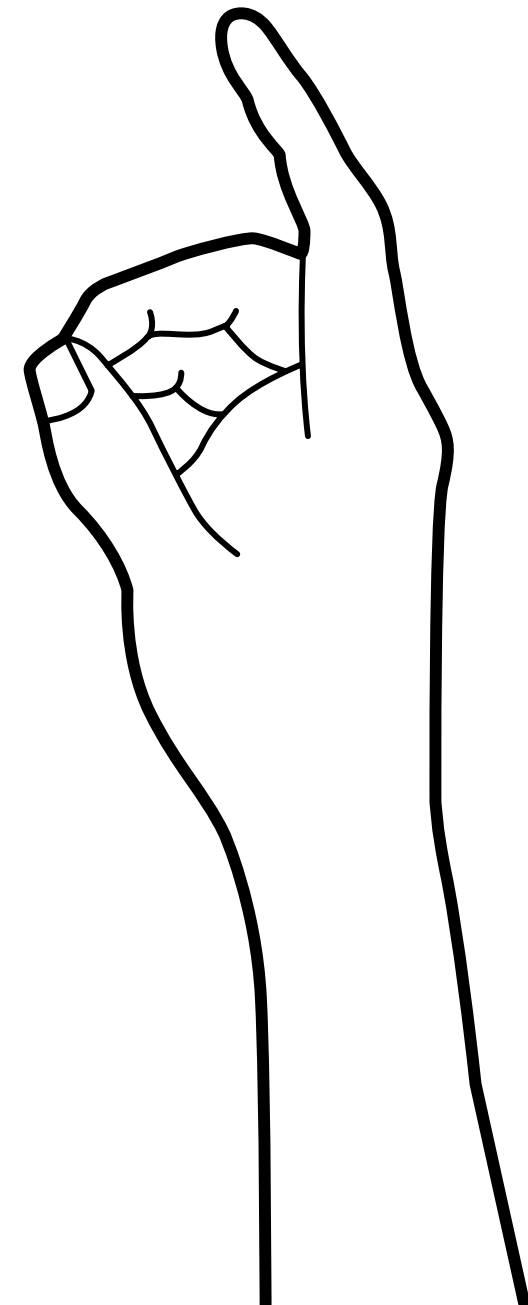
This work was supported by the Czech Science  
Foundation project GAP202/11/0422.



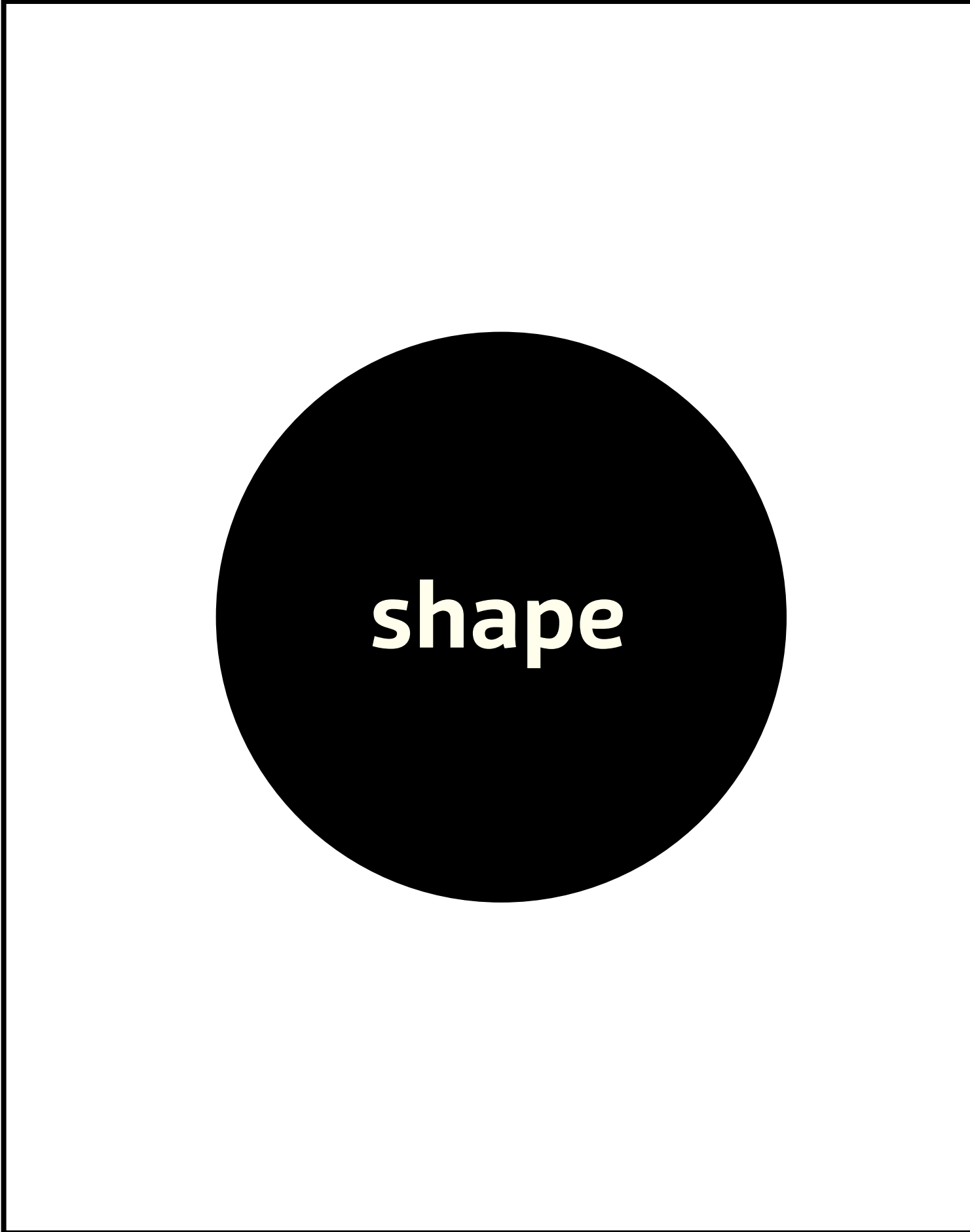
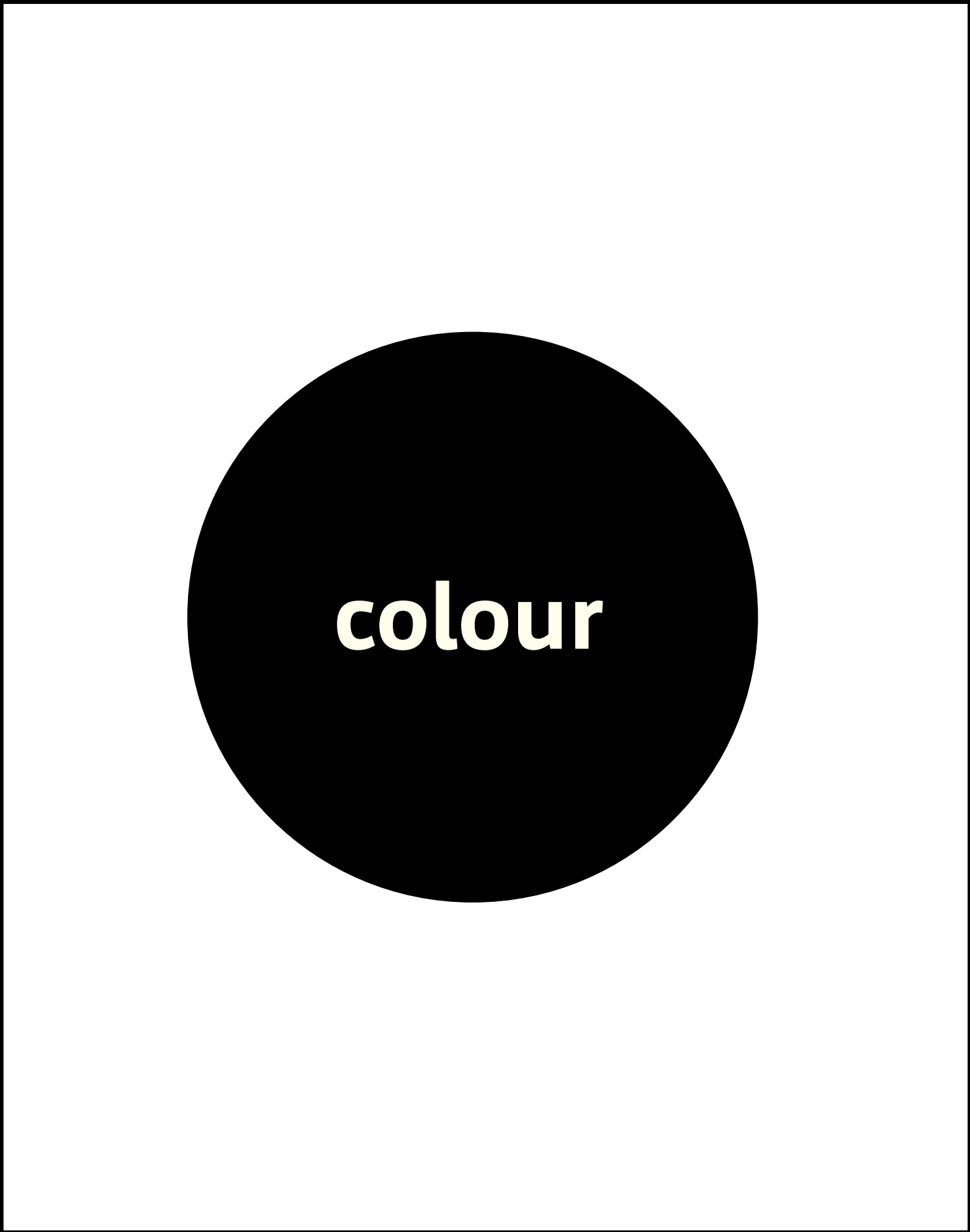
Case study  
Unity



# ● Connection & Disconnection



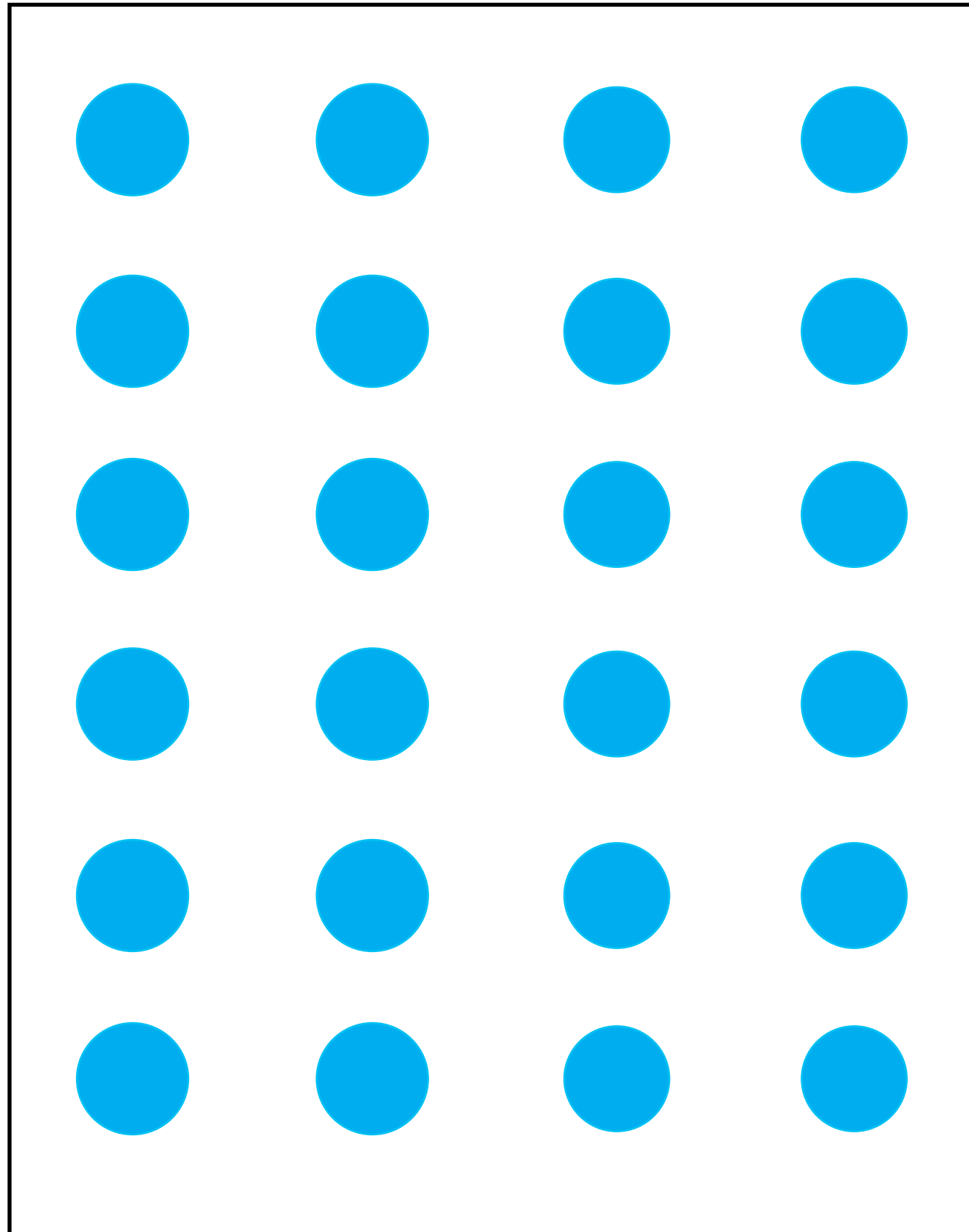
**Connection and Disconnection**



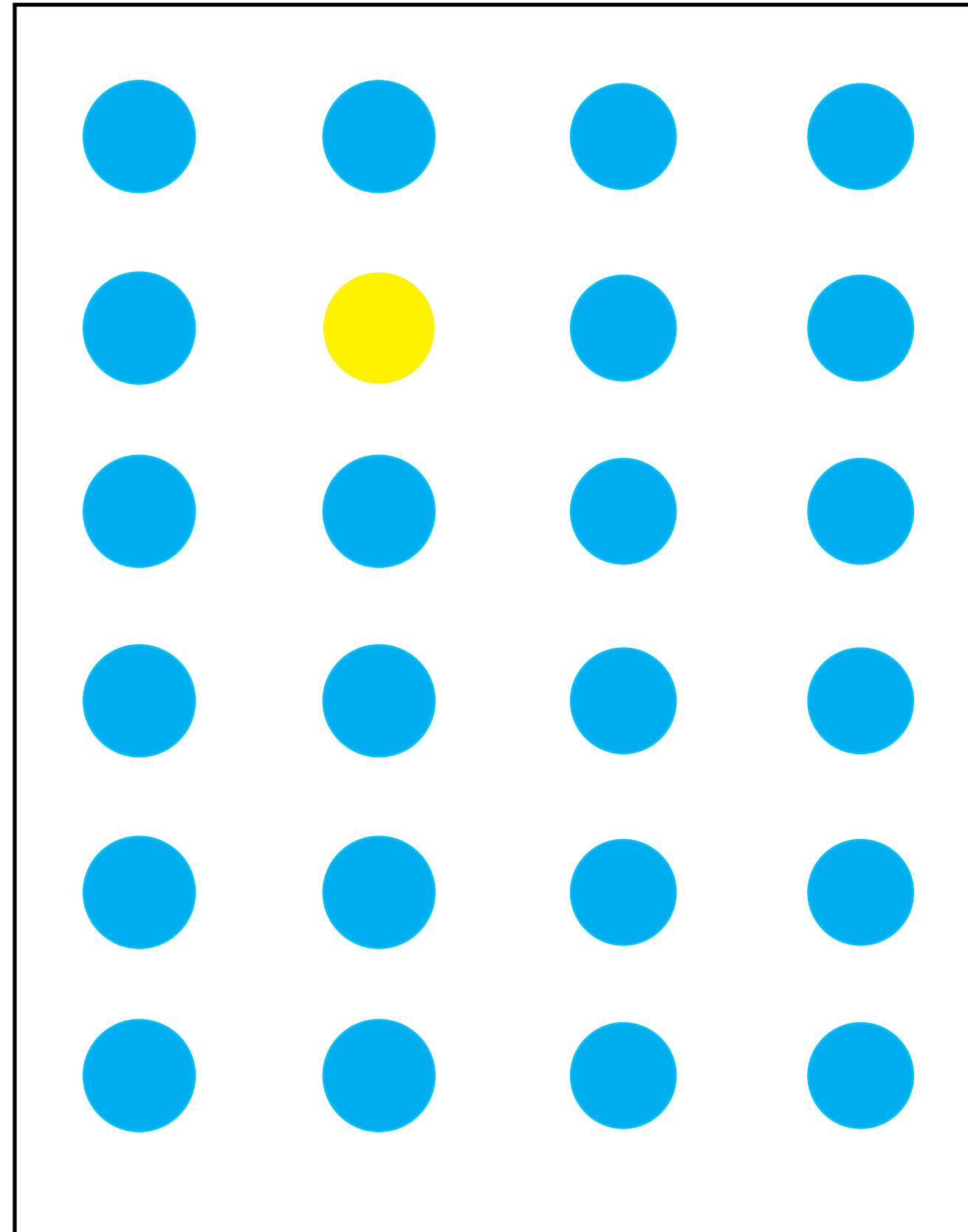
# Connection and Disconnection

Colour

**Elements with the same colours  
are perceived as one group**



**connection**



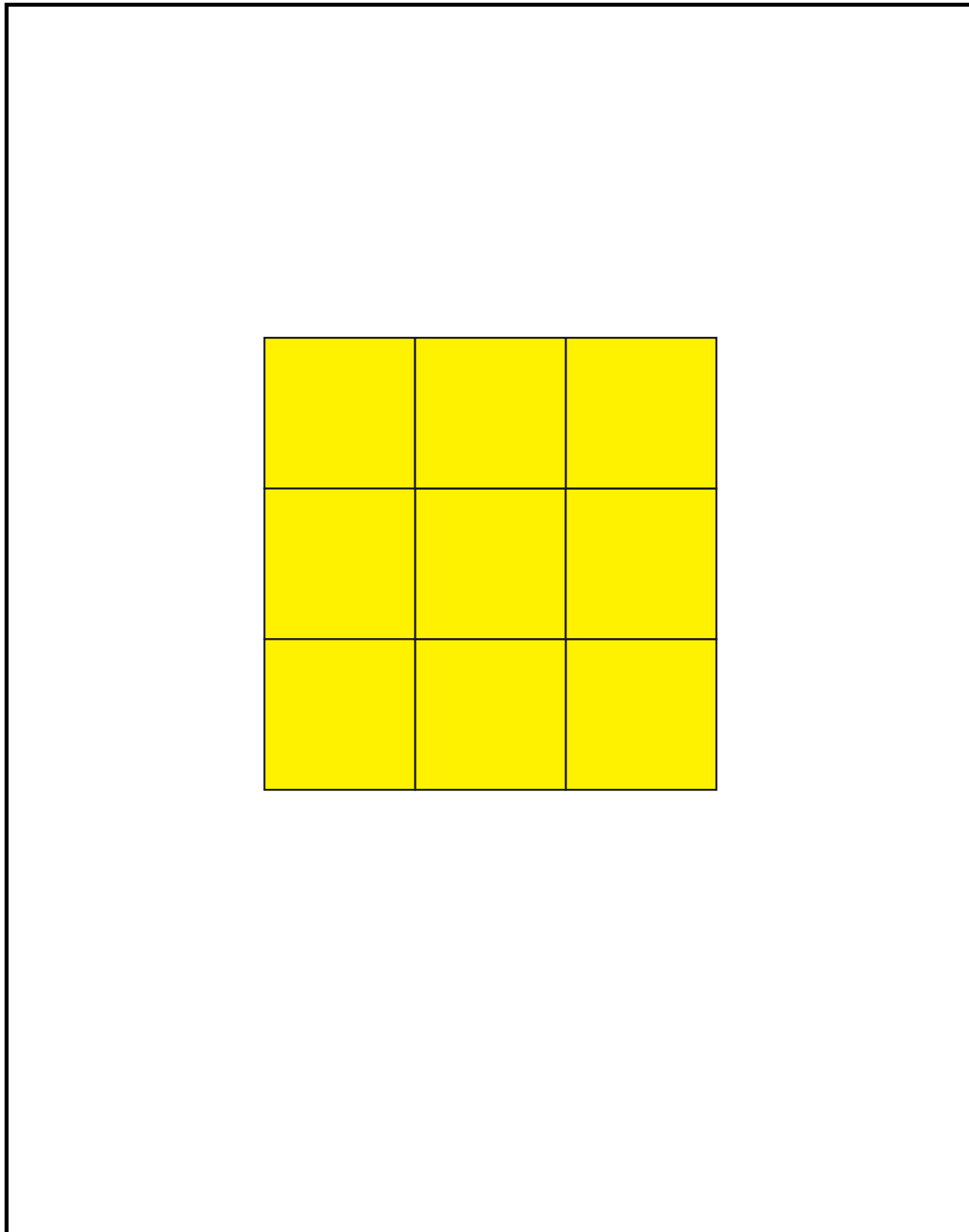
**disconnection**

\* GESTALT principles

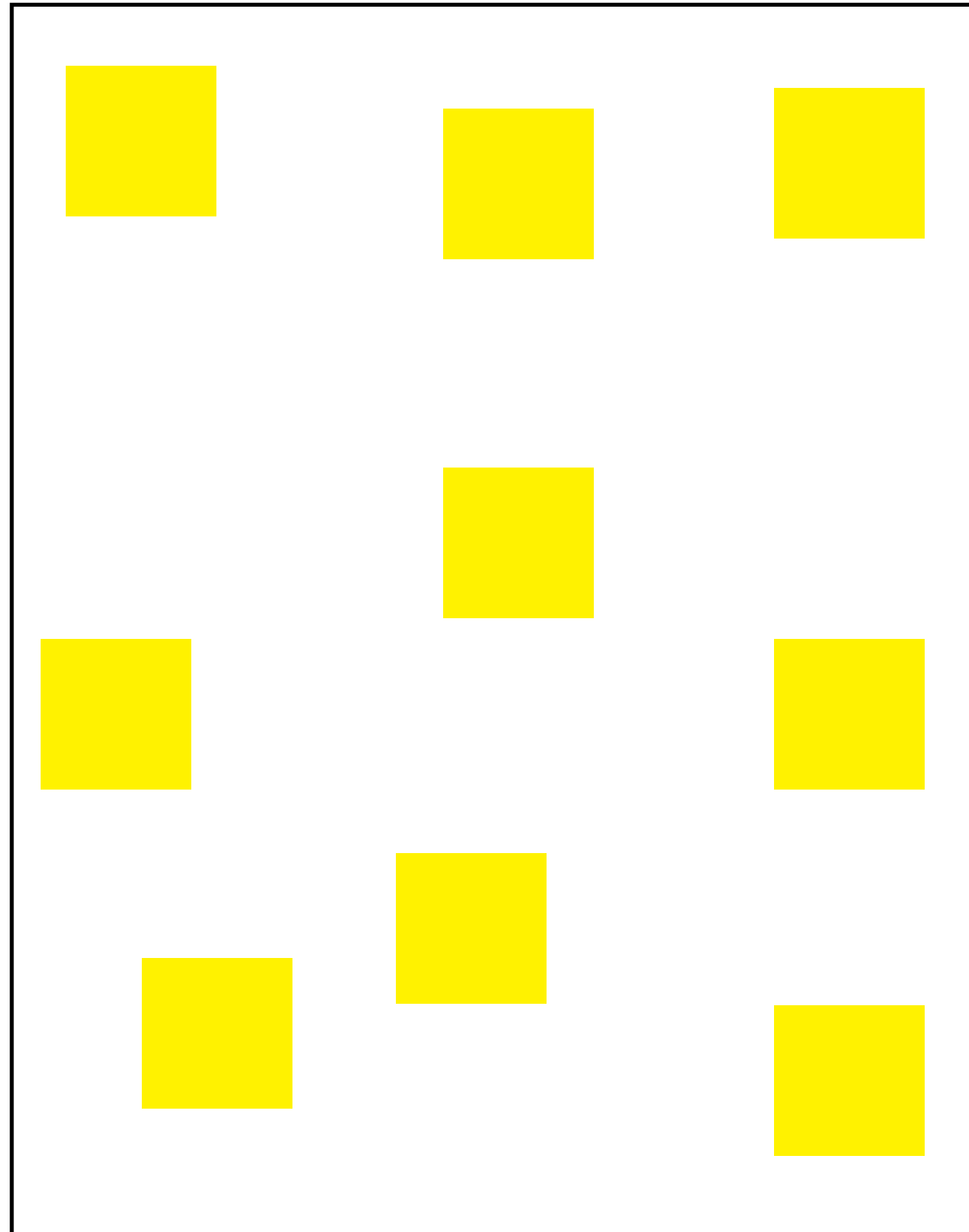


**Connection and Disconnection**  
Positioning

**Closer elements relate together**



**one group**

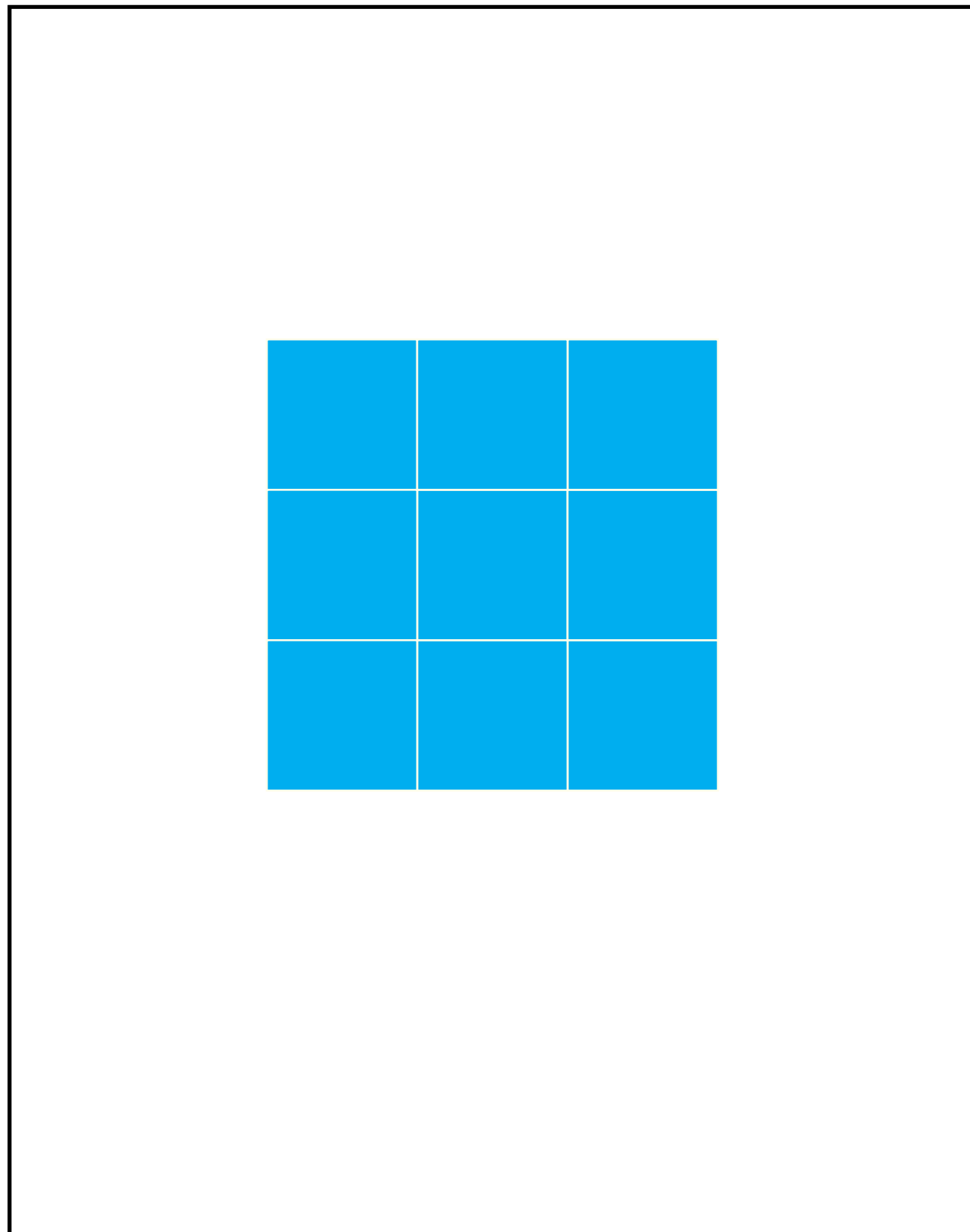


**separete shapes**

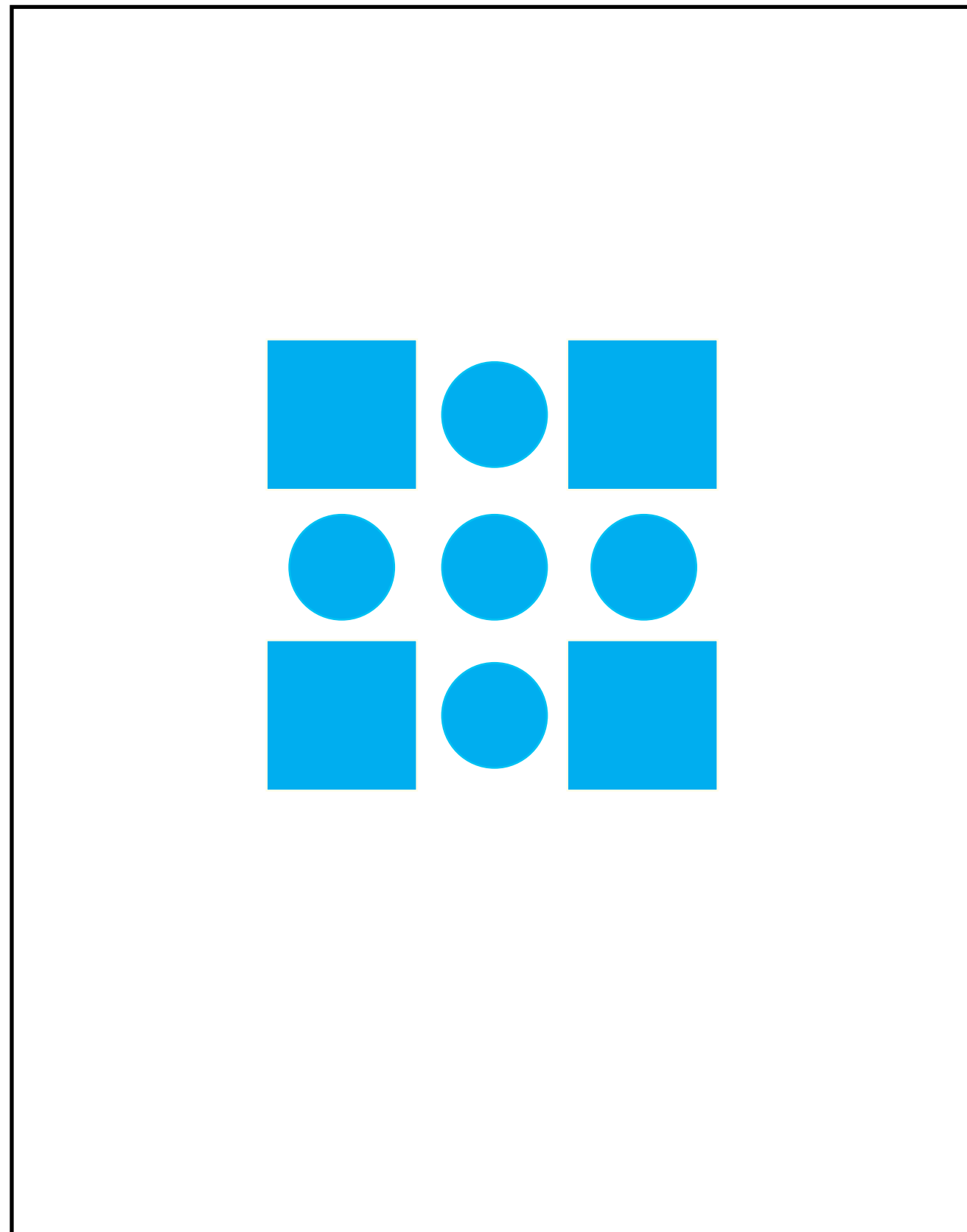
\* GESTALT principles

**Connection and Disconnection**  
Shape

**Same shapes are perceived  
as a group**



**one group**



**different shapes**

\* GESTALT principles

# Connection and Disconnection

## Case study

disconnection

disconnection



### CERIT Scientific Cloud

#### Looking for Synergies in Scientific Computing

David Antoš, Aleš Křenek, Ivana Křenková, Luděk Matyska  
Institute of Compt. Science, Masaryk University, Brno

#### Mission

CERIT Scientific Cloud centre, the successor of Supercomputing Centre Brno at Masaryk University, is a national centre providing flexible computational and storage capacities. Provision of these resources is complemented with extensive research activities, carried both in cooperation with the user communities and in the e-Infrastructure area itself.

#### History

Supercomputing Centre Brno (SCB) is a part of Institute of Compt. Science, Masaryk University. SCB was founded in 1994 as one of big supercomputing centres in the Czech Republic of that time. Similar cooperating centres were founded by other universities (Prague, Pilsen, Brno, Ostrava).

SCB has been working with Faculty of Informatics, Masaryk University, for a long time. The cooperation is both personal and factual, formally expressed, e.g., in a common research intent "Highly parallel and distributed computation systems".

#### Funding

Transformation of SCB into CERIT-SC will be supported by a project of the 3rd axis of the RD&I Operational Programme. The project will be realised from May 2011 to October 2013. Its overall budget is 5 MEur.

CERIT-SC is included in the **Roadmap for Large Research, Development and Innovation Infrastructures in the Czech Republic**.



Scientific director Prof. RNDr. Luděk Matyska, CSc.  
Project manager Roman Čermák, M.Sc., MBA  
<http://www.cerit-sc.cz>

#### Goals

CERIT-SC will provide **highly flexible computation environment** and primary **data storage capacities** for the national e-Infrastructure.

**Research and development** in CERIT-SC is focused on

- work with the users on tools and means for **efficient use** of the e-Infrastructure by applications
- cooperation with the users in development, deployment, and operation of
  - new and modified systems and programs running in flexible computation environment
  - systems for storing, archiving, and retrieval of data
  - tools and protocols for data storage facilities interconnection, ...

The research work will evolve in a **doctoral school** with student participation from both IT and application areas.

CERIT-SC will become an **important node of national e-Infrastructure**, including integration into the European Grid Infrastructure. This will be achieved by tight cooperation with CESNET on development and adoption of appropriate standards.

#### Cooperation with Users

**Deluge of experimental data** is expected in near future. Many existing computational methods will **break or stop scaling**, new **developments** will be required.

User communities will come up with **interesting problems**, CERIT-SC will provide the necessary **IT expertise**. We expect formation of **joint teams**

- consisting of experts from both sides,
  - addressing specific research areas – both ad-hoc and long term work,
  - involving students (undergraduate and Ph.D.).
- This work will result in **common publications**. Targeted projects are also expected.

Formal **agreement on future collaboration** (LoI):

- R&D: AdMaS, BIOCEV, CEITEC, CzechGlobe, RECAMO
- cooperating institutions: IBA, MZK, Loschmidt Labs, RECETOX
- ESFRI projects (in negotiation): LINDAT-CLARIN, Euro-Bioluming

#### Flexible Resources

Provision of the resources will range from traditional **batch queues**, through **interactive access** upto the **cloud** paradigm. The resources will be provided free of charge.

**Prioritization** of the users will be based on their **scientific results**; resulting resource allocation will be achieved by technical means, combining advanced resource scheduling, virtualization, and the cloud paradigm; no complex administrative process will be required.

By careful ballancing the scheduling strategies, successful users will get better share while new users, students etc. will not be prevented from using the resources.

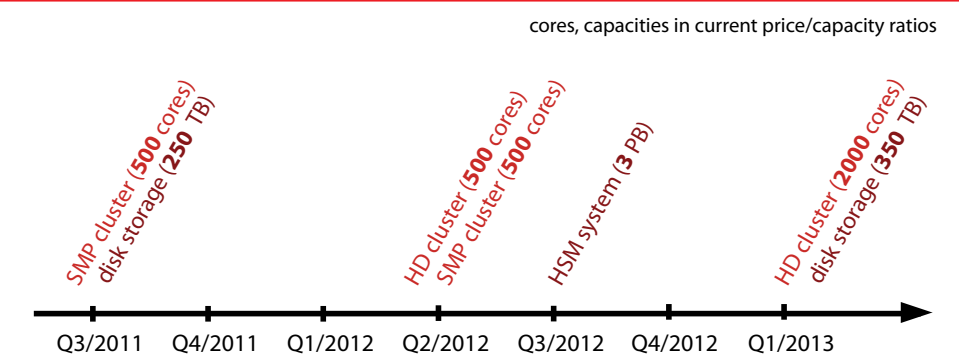
CERIT-SC computational resources are intended to serve **unexpected and unplanned requirements** of the users primarily.

Data resources will serve to **store and share data** semipermanently and permanently. They will be tightly integrated with the computational resources. The target community are the **end-users** again.

#### Equipment and Purchase Schedule

The project will purchase the following resources:

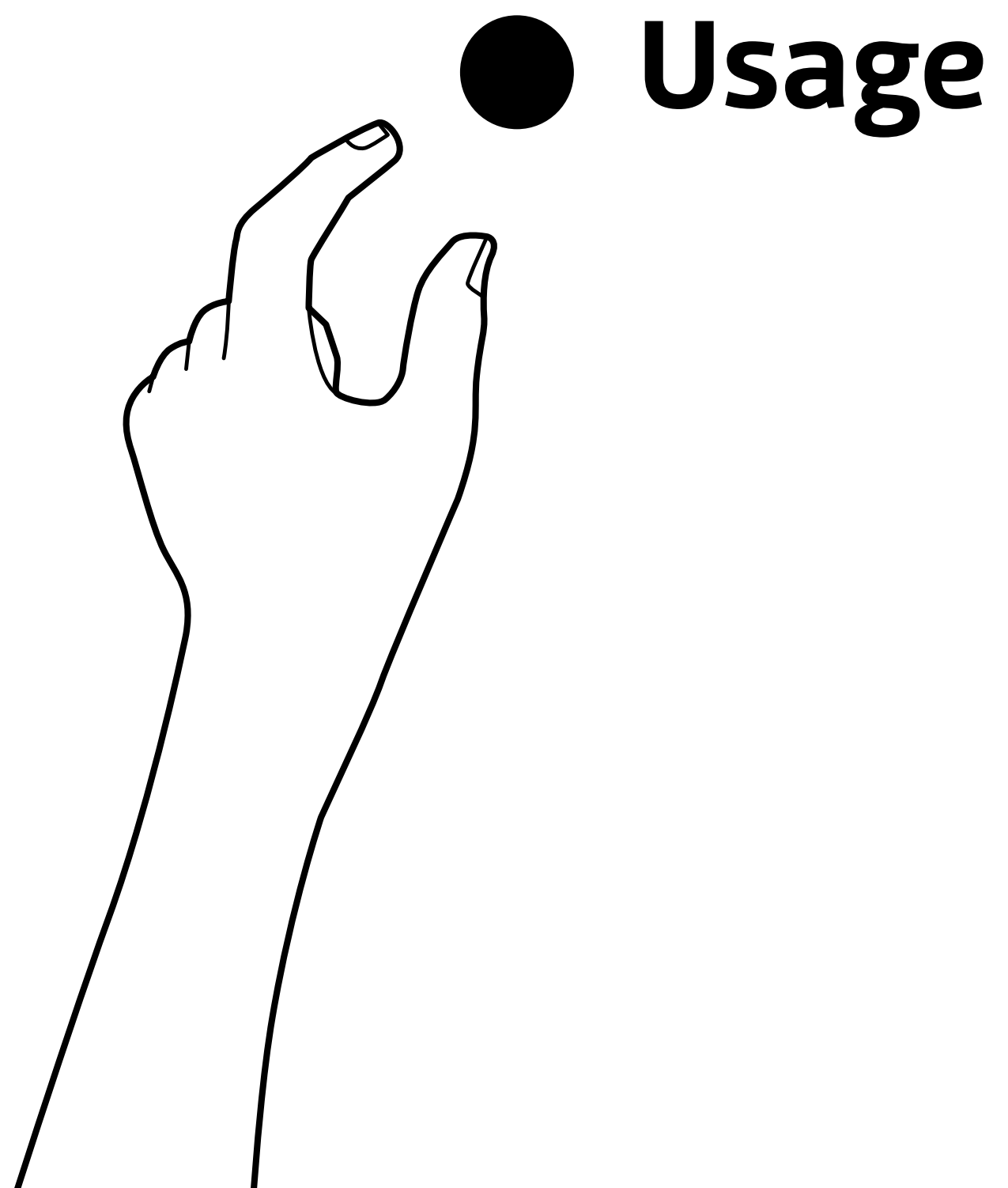
- SMP – Symmetric MultiProcessing clusters, with more than 64 cores and 128 GB memory per node (1000 cores total)
- HD – High Density clusters with higher number of nodes with 8-16 cores and 16-32 GB memory (2500 cores total)
- HSM Hierarchical Storage Management (3 PB)
- disk storage (600 TB)
- development tools and application software



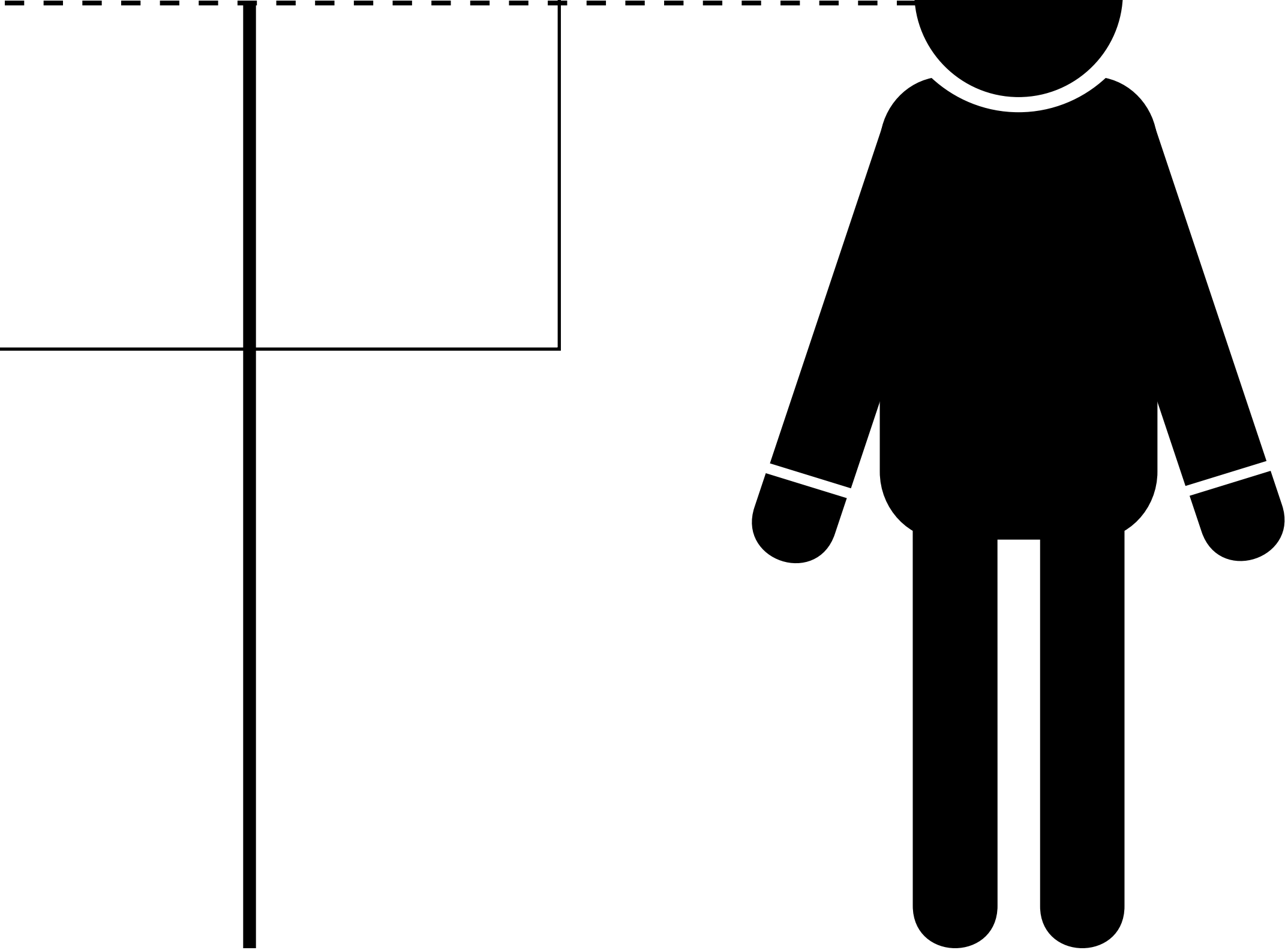
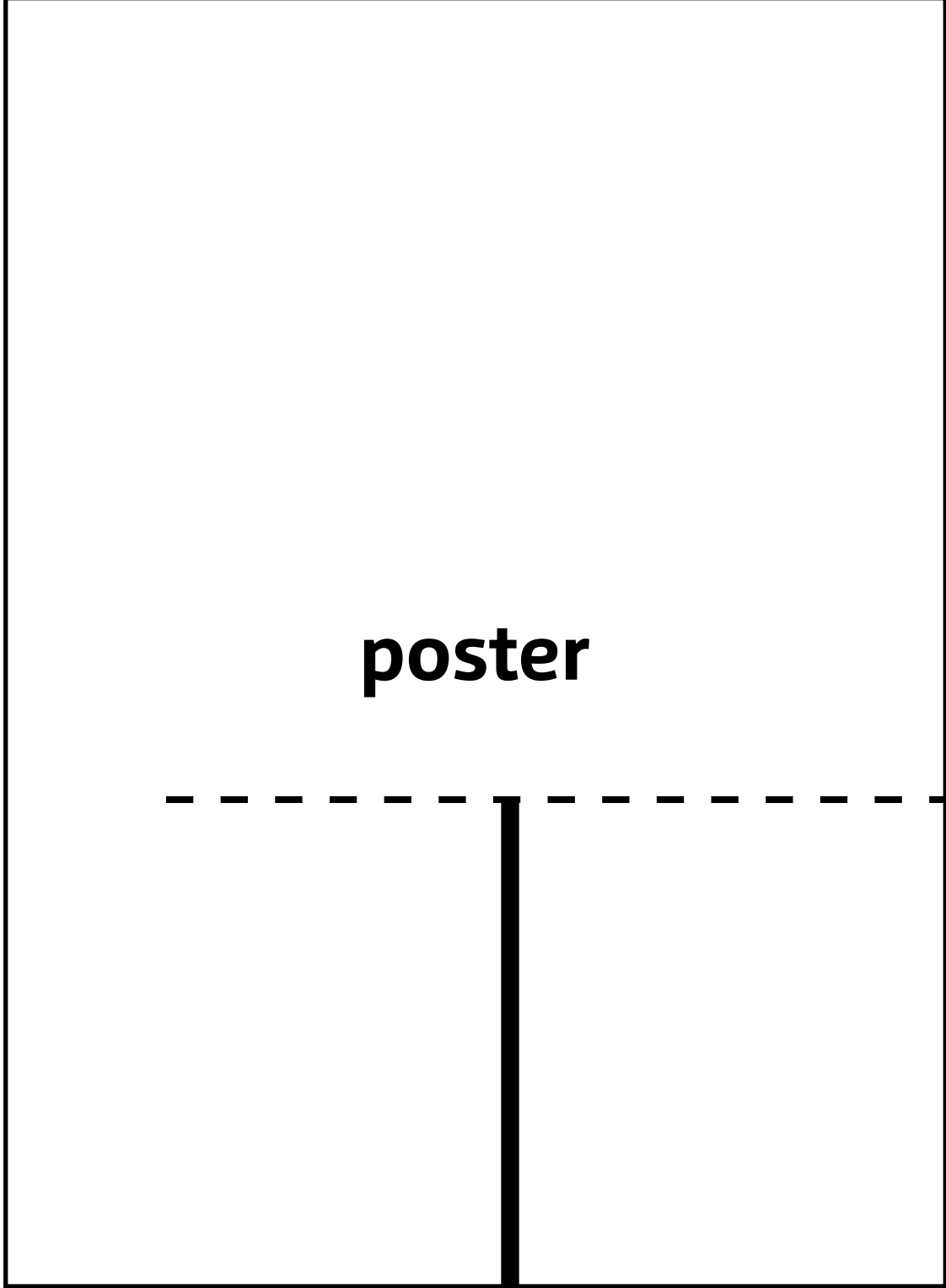
This poster presentation is partially supported by project "Vzdělávání akademických pracovníků v oblasti e-infrastruktur (CZ.1.07/2.3.00/09.0074)"



INVESTMENTS IN EDUCATION DEVELOPMENT

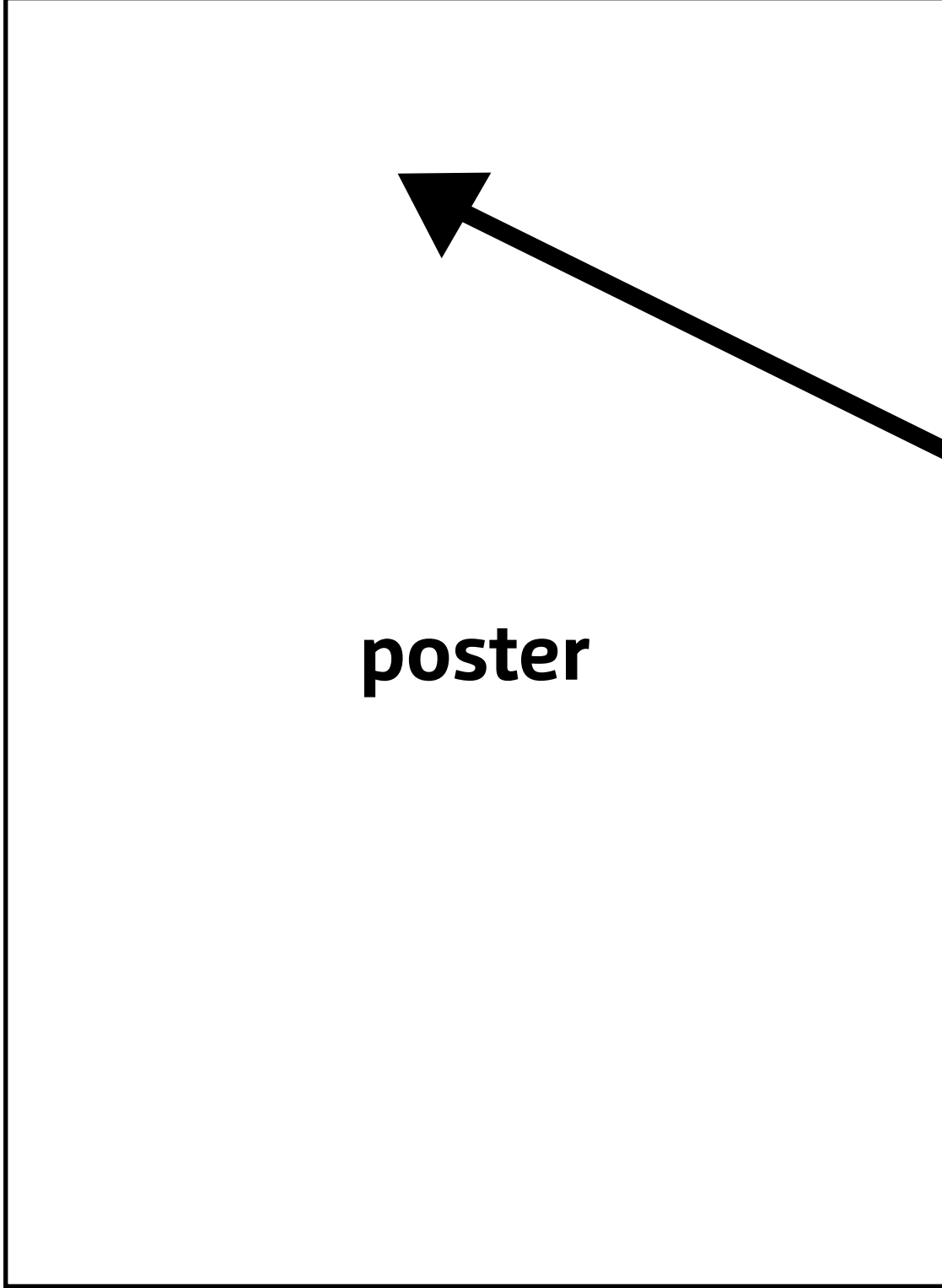


Usage

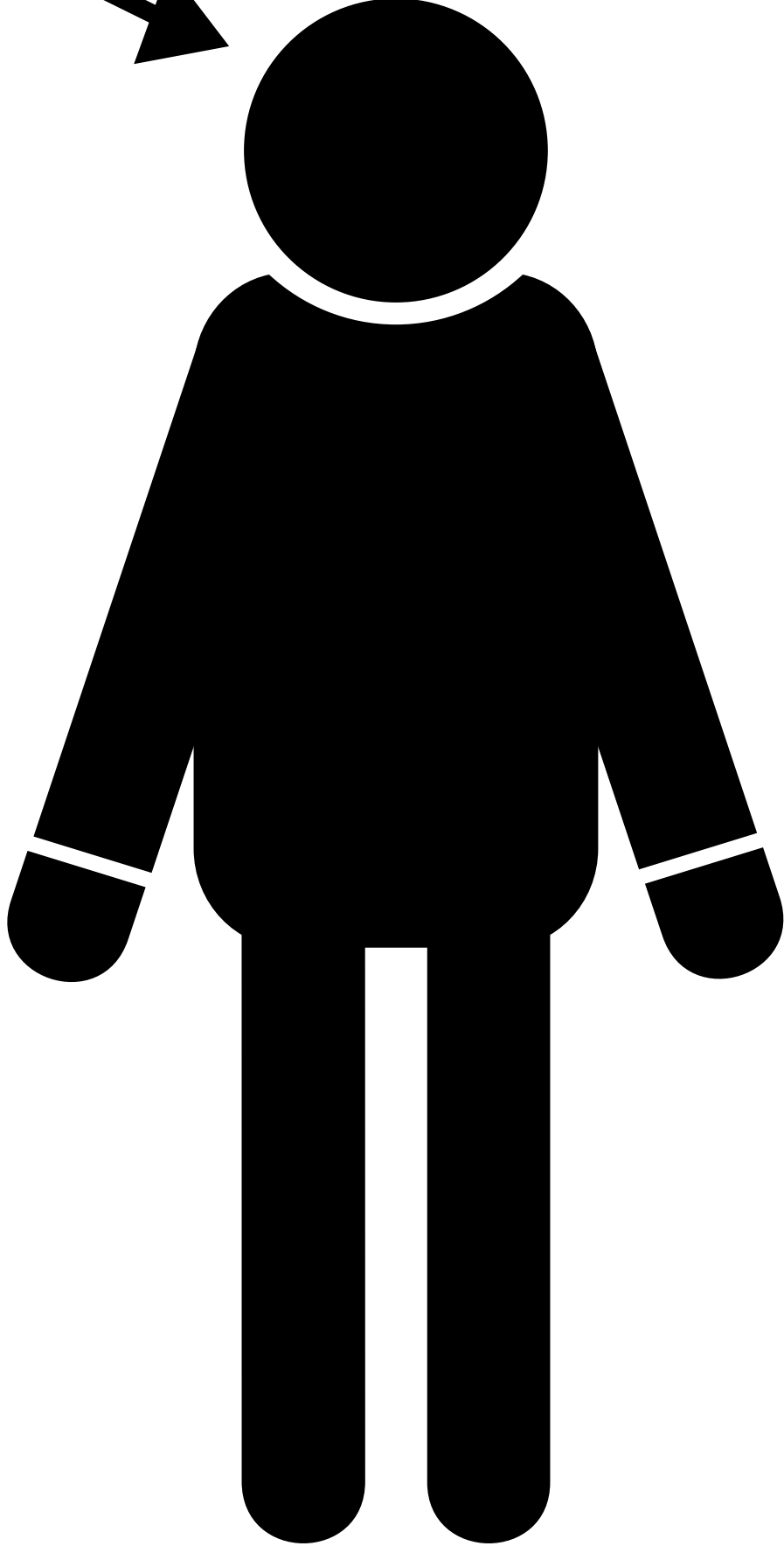
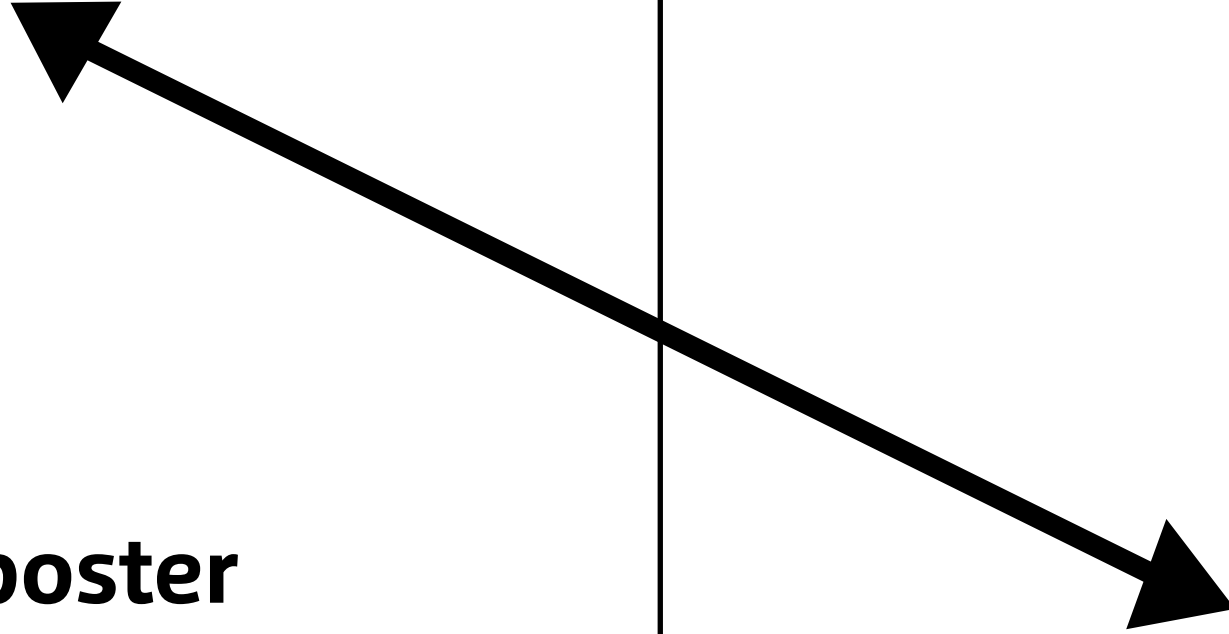


Position of the poster

Usage

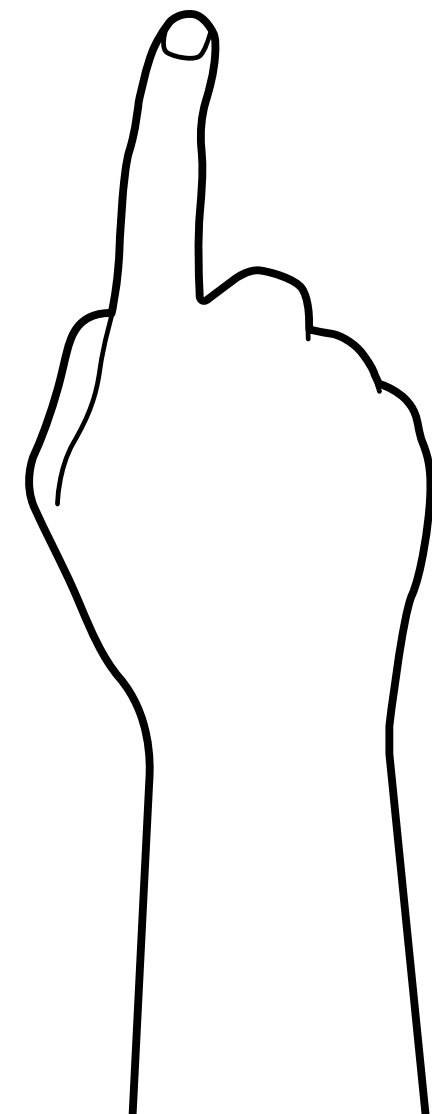


poster



Distance between medium

# Ways of reading



Ways of reading  
from left to right

## **Navigation**

Position of elements, contrast, style of shapes could navigate user how to read the poster.

## **Input element**

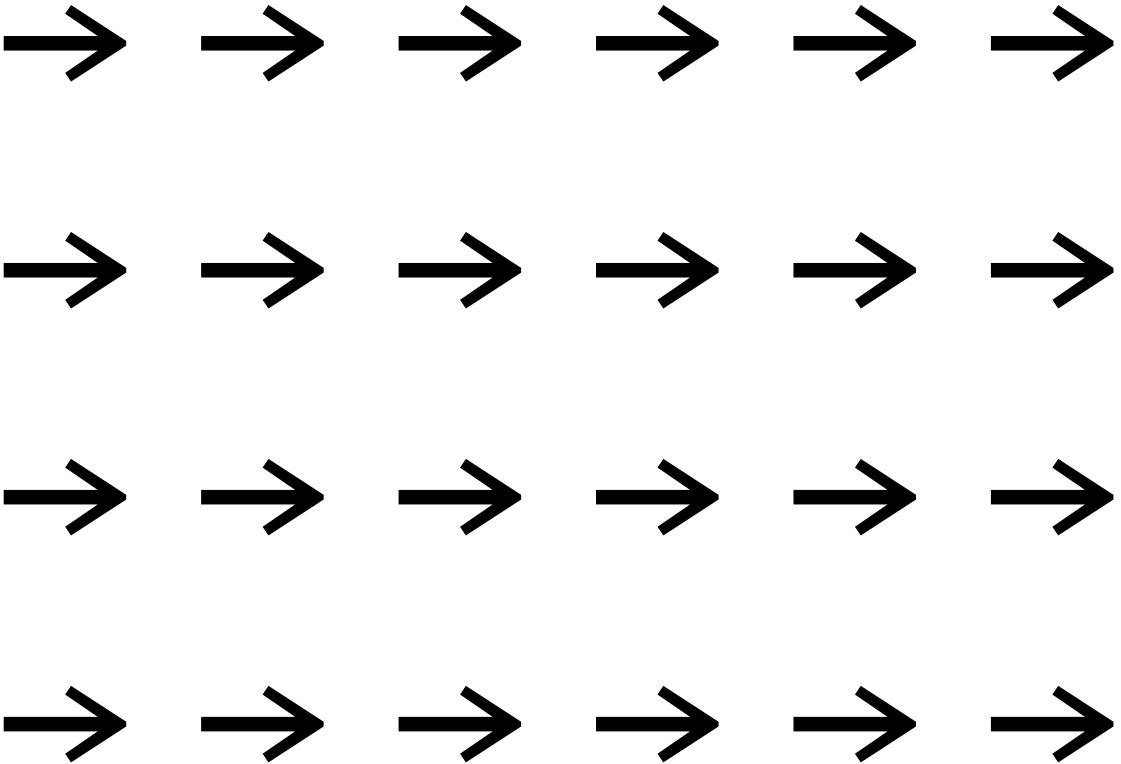
The element which should be read the first.

## **Colours and movents attracts attention**

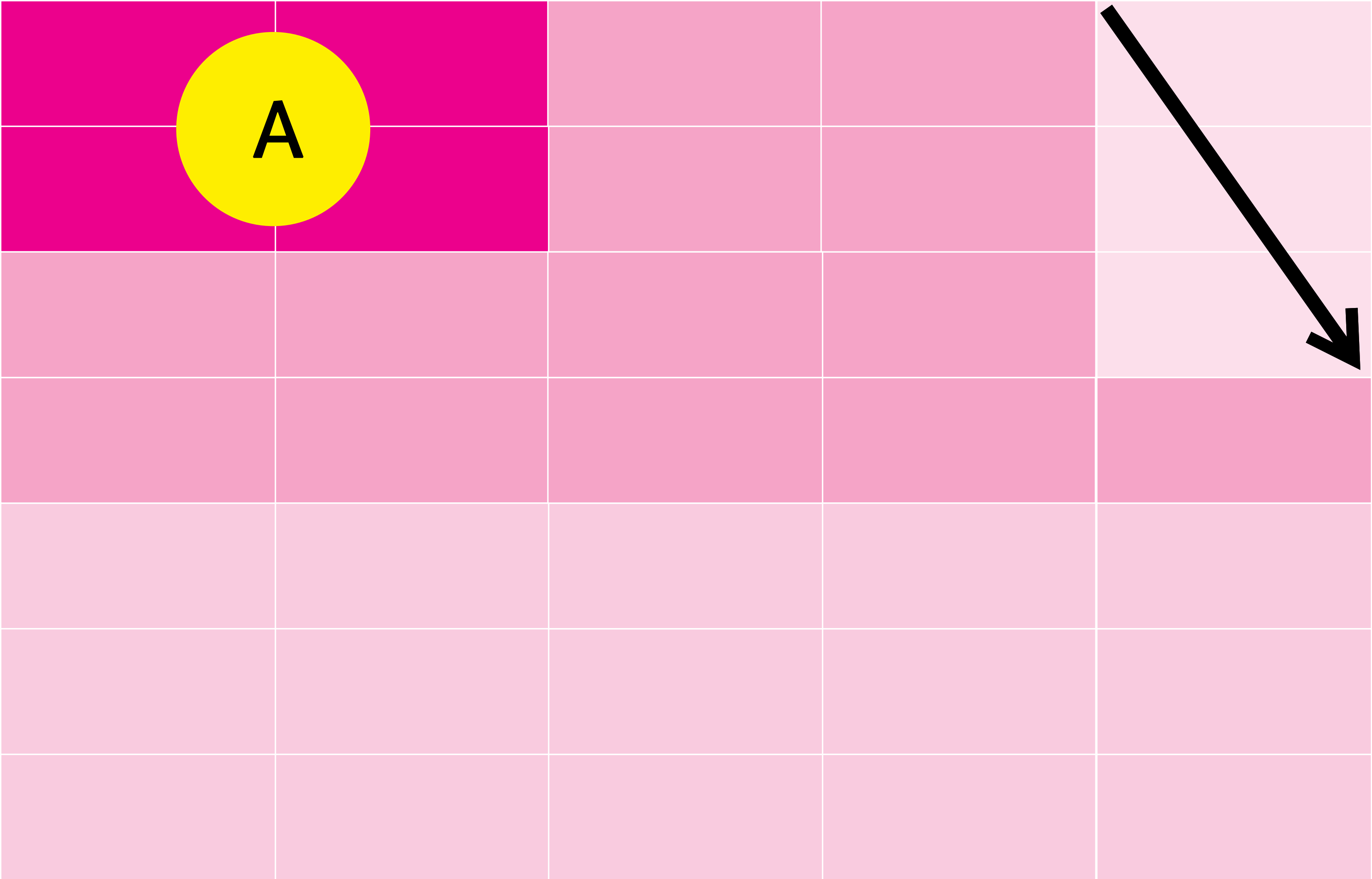


Ways of reading  
from left to right

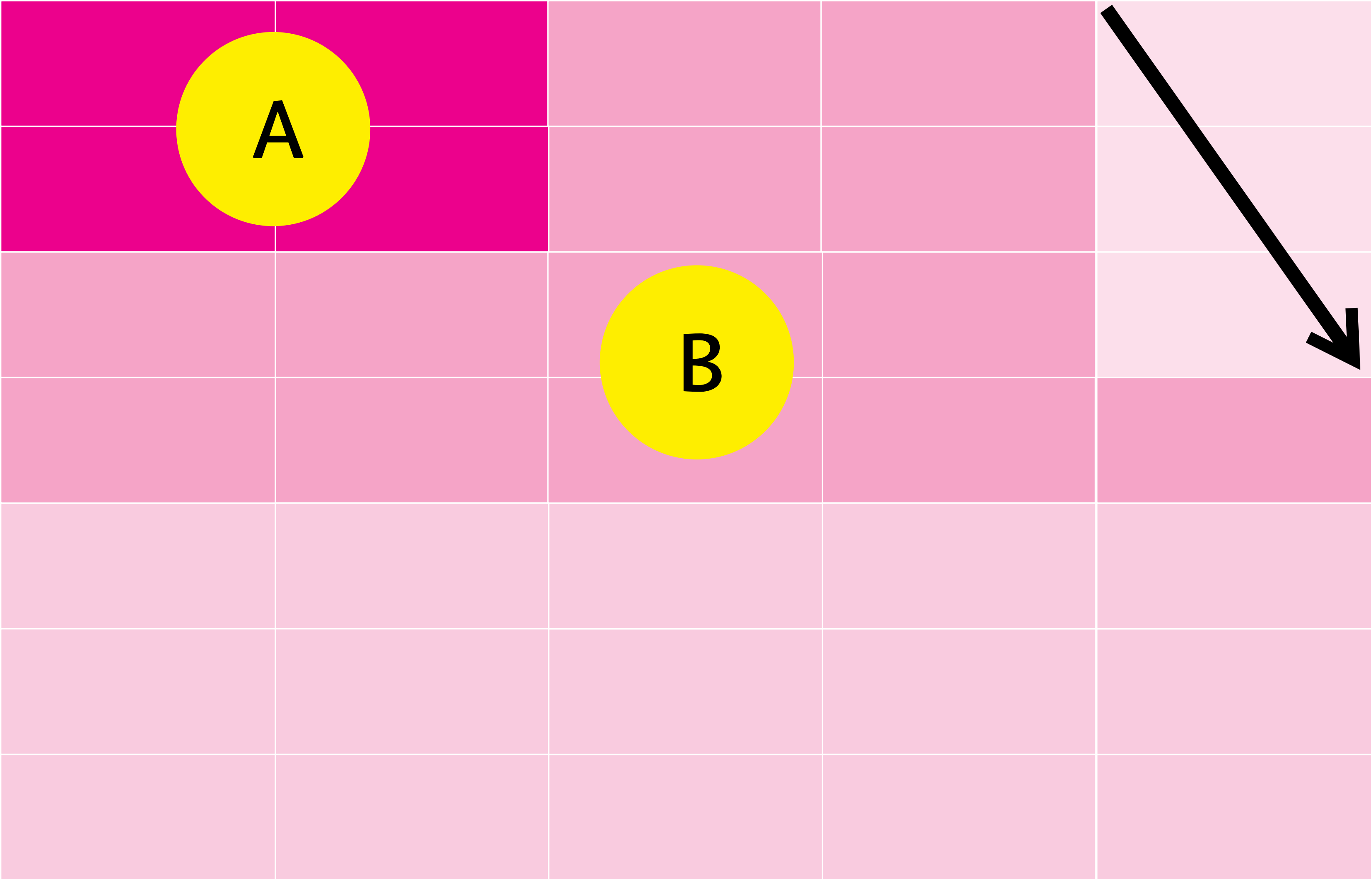
Latin – from left to right



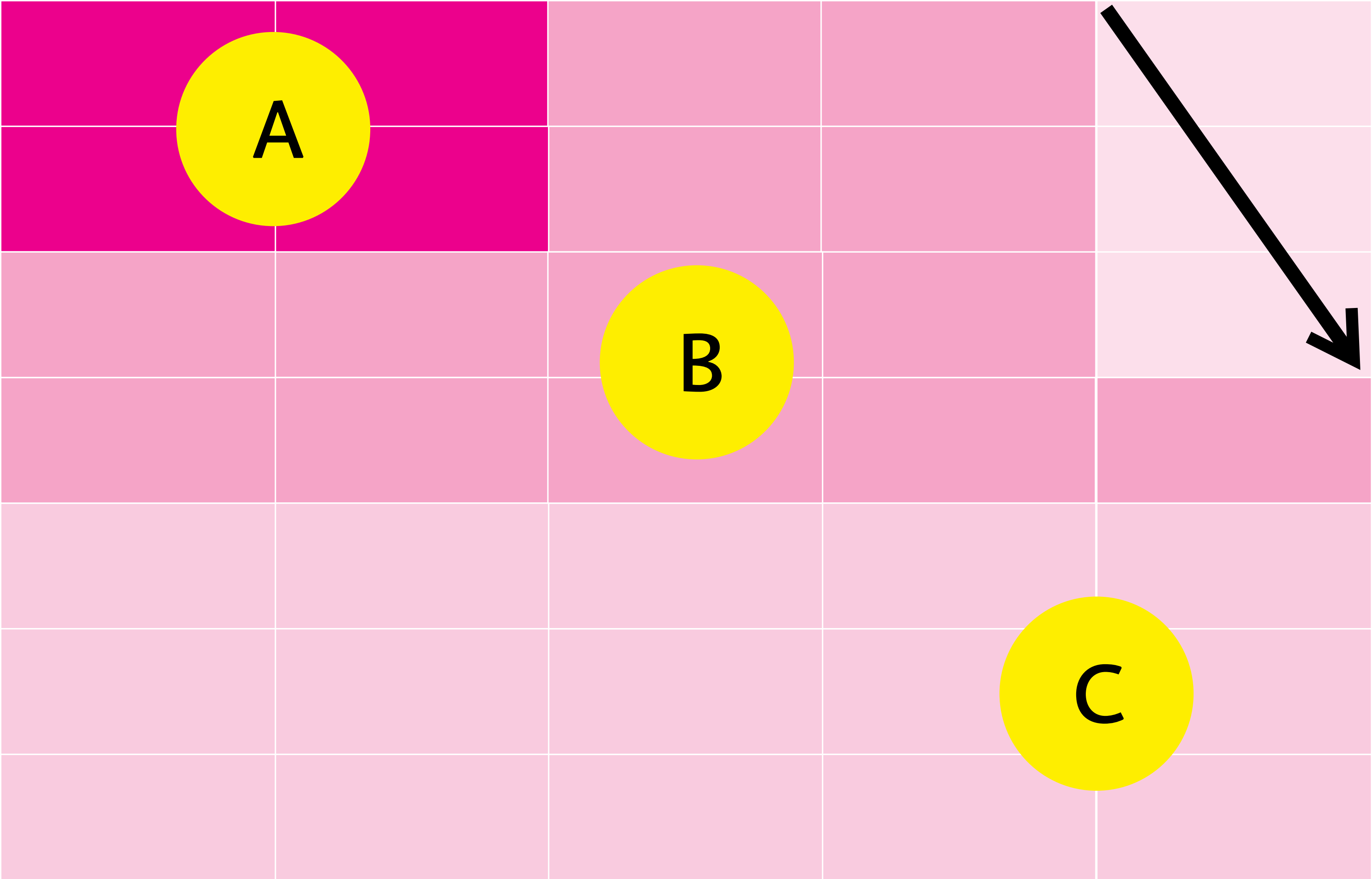
**Ways of reading**  
from left to right




**Ways of reading**  
from left to right

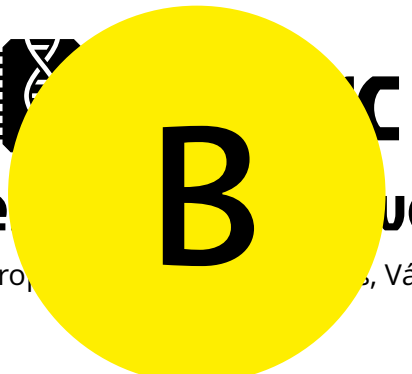


**Ways of reading**  
from left to right





MASARYK UNIVERSITY



# Using genetic programming for true encryption

Martin Ukropný, Václav Matyáš et alii

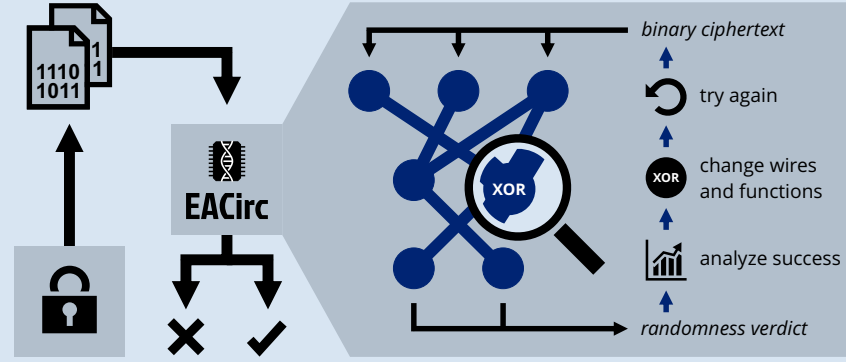
Find me on GitHub!  
github.com/crocs-muni/eacirc

## Problem statement

**Randomness testing**

The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?

EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.



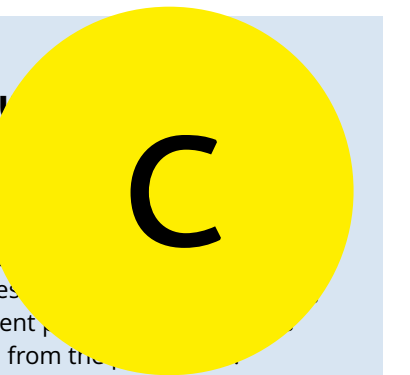
**Iterative design**

The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions). It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

## EACirc workflow

**1. Forming a population**

A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.

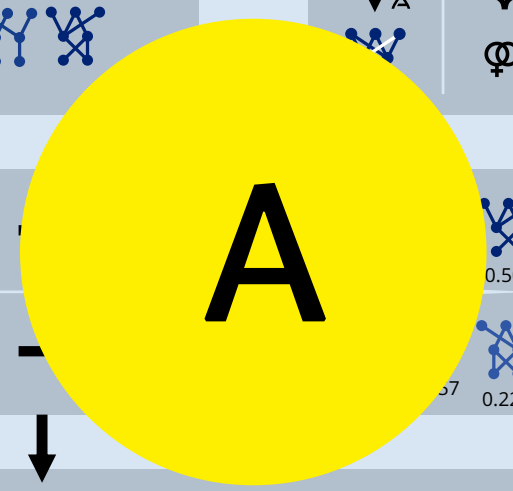


**5. Mutation**

To form a new population, mutations are applied to the current population. Mutations make changes to the gate circuits, creating different individuals. Mutations are taken from the current population.

**2. Test vector generation**

Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.

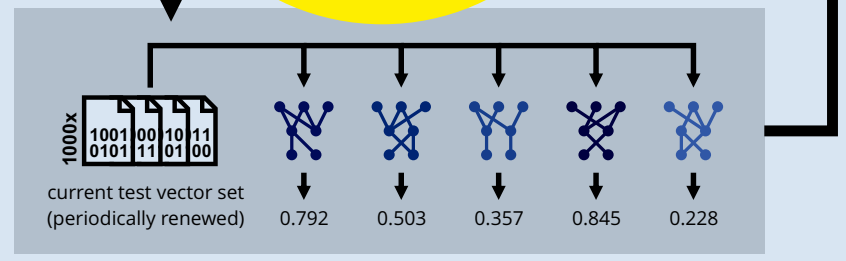


**4. Survival of the fittest**

Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival. The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.

**3. Fitness assessment**

Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0,1].

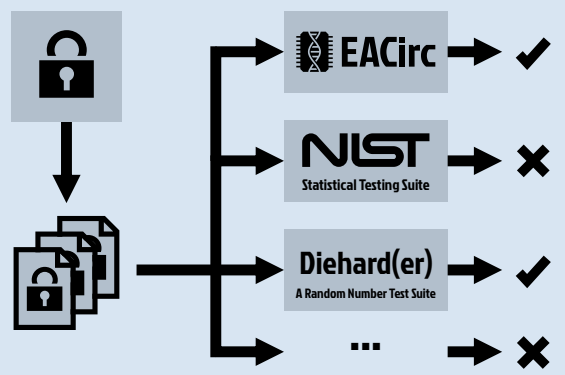


## Comparison to existing tools

**EACirc vs statistical testing**

The standard way to assess randomness is to use batteries of statistical tests such as *NIST STS*, *Dieharder* or *TestU01*. We run them along with EACirc and compare the results.

To have a fine-grained comparison, we have analyzed 77 different functions (*eStream*, *SHA-3* and *CAESAR* candidates). For 2-round *Hermes* and 1-round *Fubuki* we confidently surpass *NIST STS*.



**Further information**

Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).

[1] Švenda, Ukropný, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications. Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.

[2] Kubiček, Novotný, Švenda, Ukropný. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications. Vol. 8, iss. 1. 2016.

**CRoCS** Centre for Research on Cryptography and Security

This work was supported by the Czech Science Foundation project GAP202/11/0422.

1. pictures – infographics

2. title

3. text

# Ways of reading

## Case study

FACULTY OF INFORMATICS  
Masaryk University

# Verification of Programs with Inputs

Vladimír Štill, Petr Ročkal, Jan Mrázek and Jiří Barnat

B

### DIVINE

DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choice which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

### Symbolic States

Consider a simple program with 32 bit input variable  $x$  and a branch on the value of this variable. In the current DIVINE, this program gives rise to  $2^{32}$  possible memory configurations. In symbolic version, possible values of variables  $x$  and  $b$  are represented symbolically using bitvector formulae, therefore, there are only two possible configurations at the end of the program.

C

A

### Proposed Approach

To take advantage of symbolic representation of states, we transform the LLVM bitcode in such a way that it represents variables which can contain values dependent on inputs symbolically. This transformation is performed by LART and is presented in detail later. Apart from that, the verification algorithm is modified to handle symbolic states with the help of an SMT solver.

Our approach aims for minimizing changes to the LLVM interpreter that is used to execute instructions in DIVINE. The reason is that the interpreter is complex and performance tuned and therefore it is not desirable to make it even more complex by adding symbolic data manipulation into it. Instead, symbolic data are to be handled by the program itself. To encode symbolic manipulations into the program we transform the LLVM bitcode produced by the compiler and create symbolic LLVM from it. This not only minimizes changes to the interpreter, but the transformation can also be used for other purposes like symbolic data quite easily. The transformation is handled by the Symbolic and Refinement Tool. Furthermore, DIVINE's interpreter can be modified. It has to check if symbolic states are possible, that is if they can represent at least one concrete state. For both of these tasks, DIVINE uses SMT solver. For both of these tasks, DIVINE uses SMT solver.

### Details of Program Transformation

LLVM bitcode is generated from C++ source code.

Dependence graph of LLVM instructions is created from the control flow of a program.

Instructions dependent on the input are computed.

Dependent instructions are substituted with symbolic calls, path condition manipulations are added.

A program simulating original instructions in a symbolic manner.


LART takes the LLVM bitcode of the program and libraries produced by the compiler and transforms it into a bitcode which manipulates data symbolically. In this modified program, any variable which can depend on an input value is represented symbolically using bitvector formulae. Bitvector formulae describe integers of fixed bit width with overflow and bitwise operations, and therefore are well suited for exact representation of computer integers. All the manipulations with such variables have to be transformed to their symbolic versions which modify the formulae accordingly. Furthermore, any branch which depends on an input value has to put constraints on the possible values of symbolic variables (this constraint is given in the form of a path condition formula).

ParaDiSe  
Parallel & Distributed  
Systems Laboratory

1. pictures – infographics
2. title
3. text

# Ways of reading

## Case study


B

## Technologies in Scientific Computing

### Mission

CERIT Scientific Cloud centre, the successor of Supercomputing Centre Brno at Masaryk University, is a national centre providing flexible computational and storage capacities. Provision of these resources is complemented with extensive research activities, carried both in cooperation with the user communities and in the e-Infrastructure area itself.

### History


Supercomputing Centre Brno (SCB) is a part of Institute of Compt. Science, Masaryk University. SCB was founded in 1994 as one of big supercomputing centres in the Czech Republic of that time. Similar cooperating centres were founded by other universities (Prague, Pilsen, Brno, Ostrava).

SCB has been working with Faculty of Informatics, Masaryk University, for a long time. The cooperation is both personal and factual, formally expressed, e.g., in a common research intent "Highly parallel and distributed computation systems".

### Funding

Transformation of SCB into CERIT-SC will be supported by a project of the 3rd axis of the RD&I Operational Programme. The project will be realised from May 2011 to October 2013. Its overall budget is 5 MEur.

CERIT-SC is included in the **Roadmap for Large Research, Development and Innovation Infrastructures in the Czech Republic**.



A

Scientific director Prof. RNDr. Luděk Matyska, CSc.  
Project manager Roman Čermák, M.Sc., MBA

<http://www.cerit-sc.cz>

### Cooperation with Users

**Deluge of experimental data** is expected in near future. Many existing computational methods will **break or stop scaling**, new **developments** will be required.

User communities will come up with **interesting problems**, CERIT-SC will provide the necessary **IT expertise**. We expect formation of **joint teams**

- consisting of experts from both sides,
- addressing specific research areas – both ad-hoc and long-term
- involving students (undergraduate and Ph.D.).

This work will result in **common publications**. Targeted formal **agreement on future collaboration (LoI)**:

- R&DI: AdMaS, BIOCEV, CEITEC, CzechGlobe, RECAMO
- cooperating institutions: IBA, MZK, Loschmidt Labs., RE
- ESFRI projects (in negotiation): LINDAT-CLARIN, Euro-Biol

### Flexible Resources

Provision of the resources will range from traditional **batch queues**, through **interactive access** upto the **cloud** paradigm. The resources will be provided free of charge.

**Prioritization** of the users will be based on their **scientific results**; resulting resource allocation will be achieved by technical means, combining advanced resource scheduling, virtualization, and the cloud paradigm; no complex administrative process will be required.

By careful ballancing the scheduling strategies, successful users will get better share while new users, students etc. will not be prevented from using the resources.

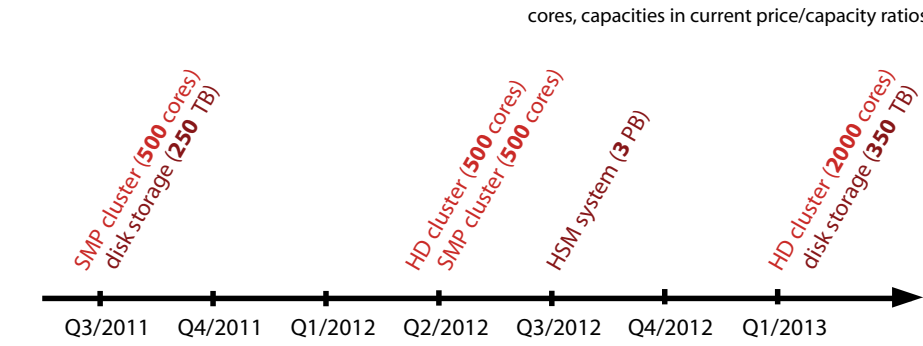
CERIT-SC computational resources are intended to serve **unexpected and unplanned requirements** of the users primarily.

Data resources will serve to **store and share data** semipermanently and permanently. They will be tightly integrated with the computational resources. The target community are the **end-users** again.


### Equipment and Purchase Schedule

The project will purchase the following resources:


- SMP – Symmetric MultiProcessing clusters, with more than 64 cores and 128 GB memory per node (1000 cores total)
- HD – High Density clusters with higher number of nodes with 8-16 cores and 16-32 GB memory (2500 cores total)
- HSM Hierarchical Storage Management (3 PB)
- disk storage (600 TB)
- development tools and application software



cores, capacities in current price/capacity ratios



This poster presentation is partially supported by project "Vzdělávání akademických pracovníků v oblasti e-infrastruktur" (CZ.1.07/2.3.00/09/0074)



INVESTMENTS IN EDUCATION DEVELOPMENT

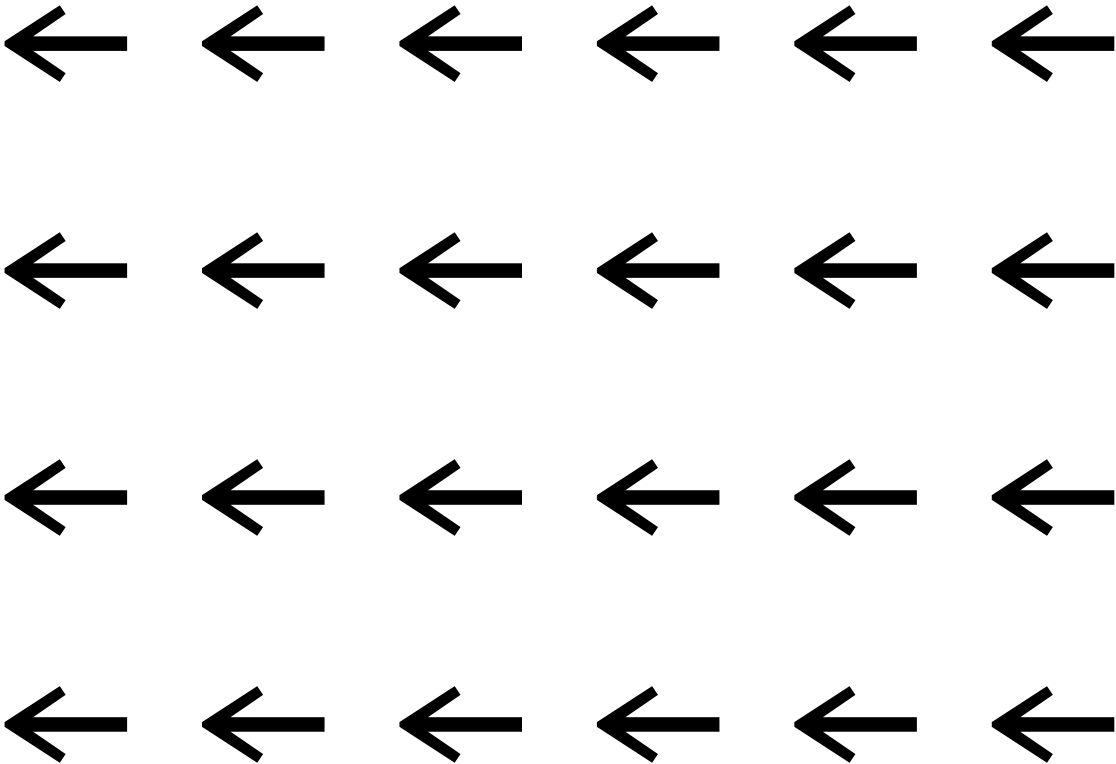
## Function of image

1. pictures – infographics

2. title

3. text

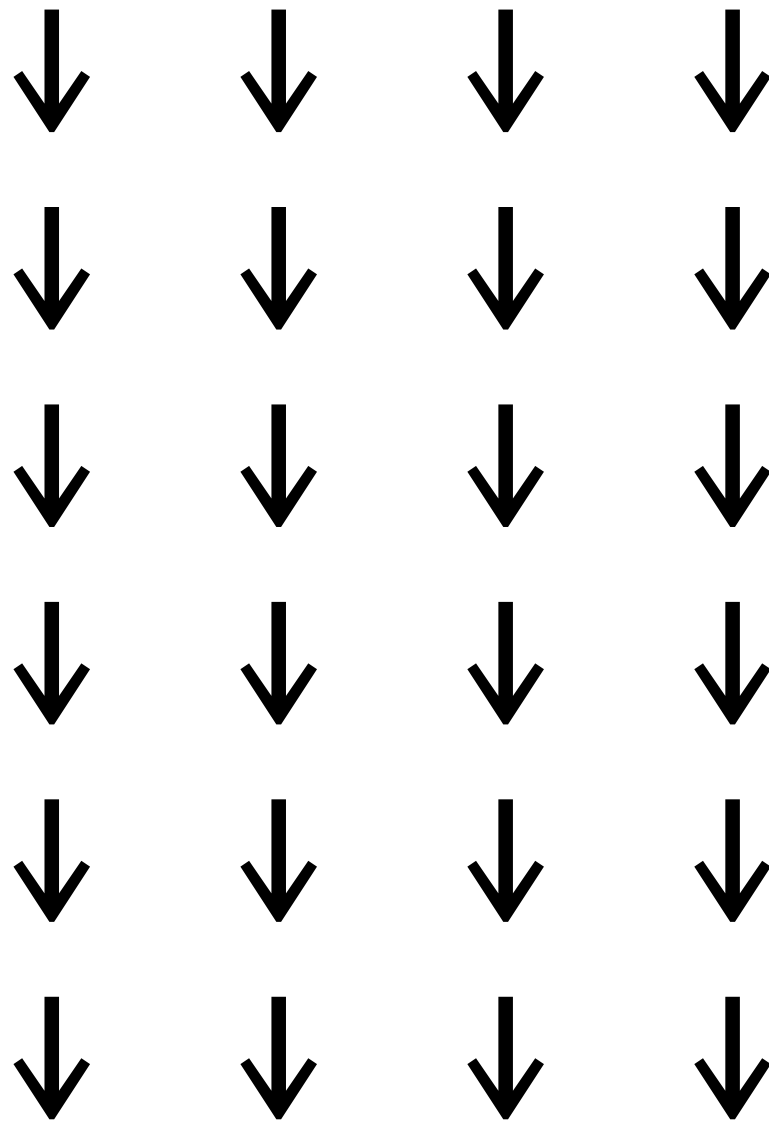
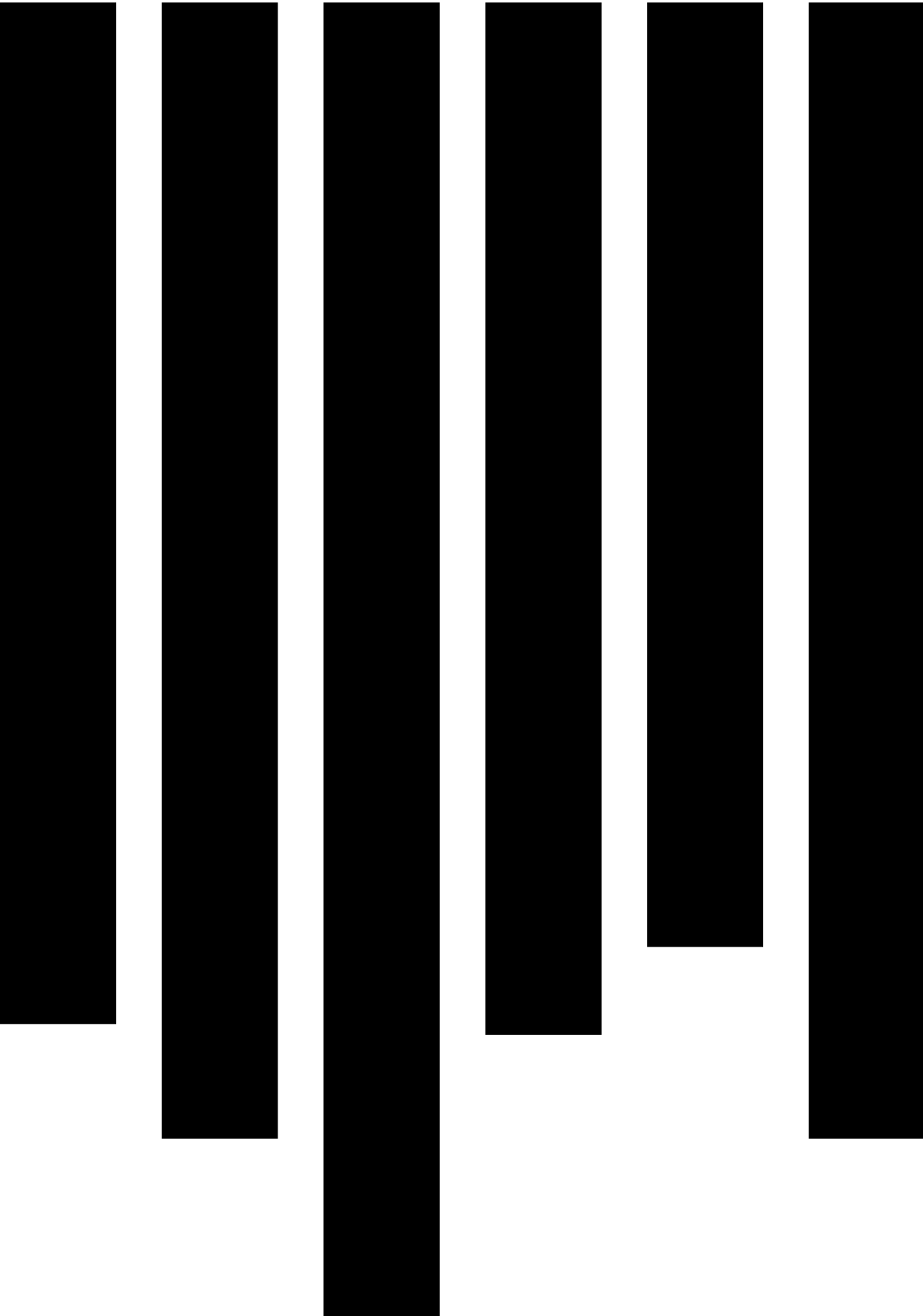
Arabic – from right to left





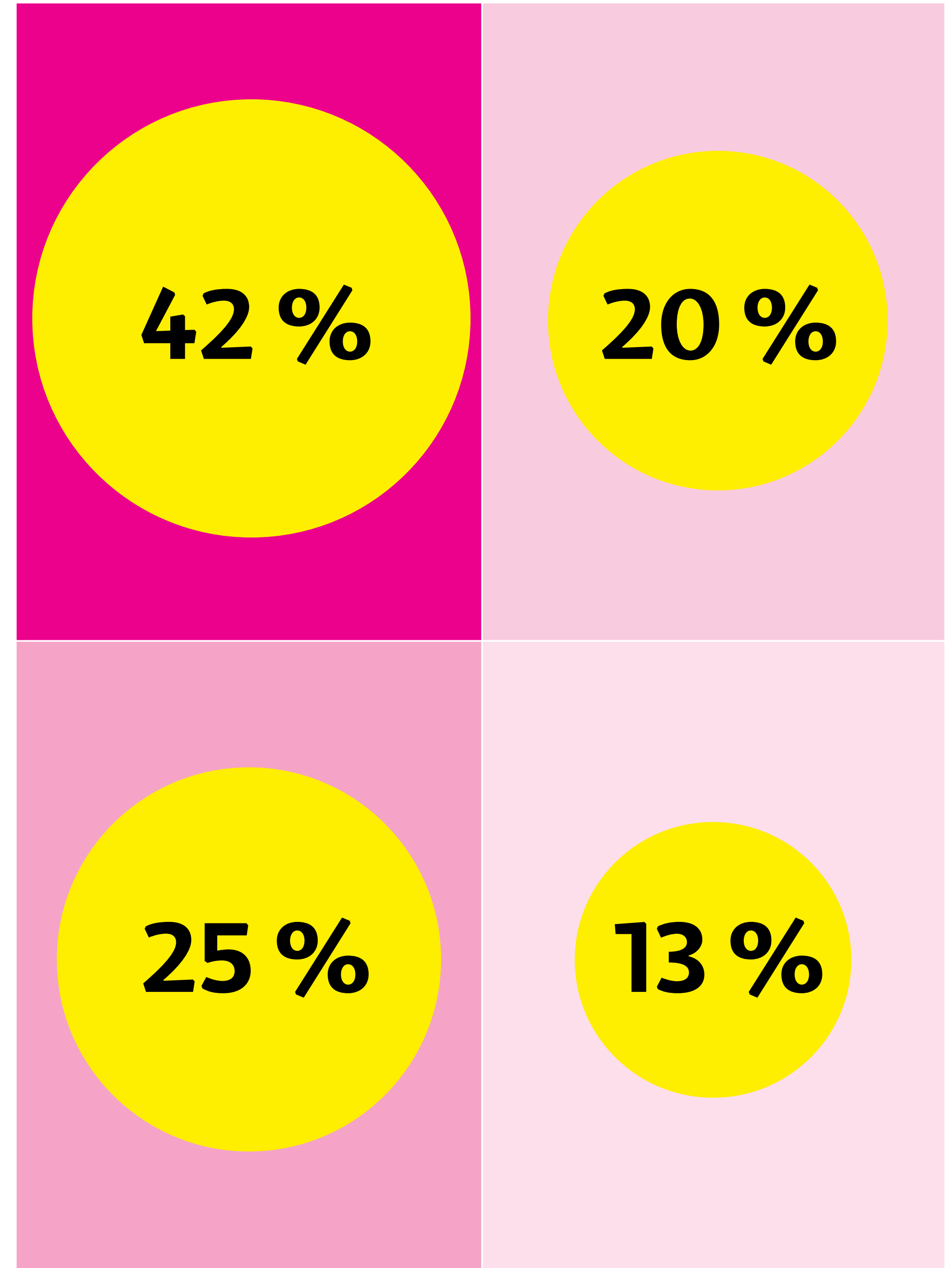
Ways of reading  
from top to bottom

# Chinese – ideograms from top to bottom



**Ways of reading**  
from left to right

**Percentual result of European  
reading.**



## **Location of elements**

The visual weight of an element attracts neighboring elements, imparting direction to them

## **Shape of element**

The shapes of an object creates an axis that imparts directional forces in two opposing directions along that axis

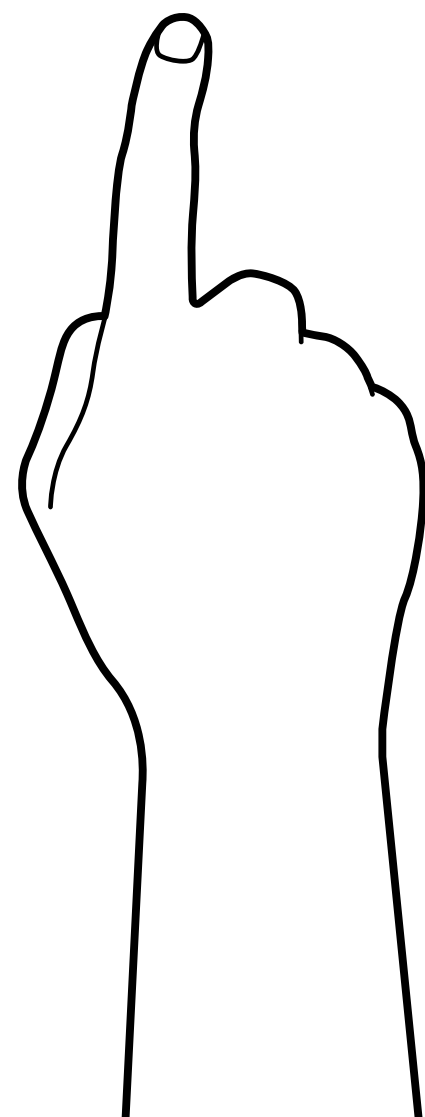
## **Subject matter of an element**

Objects in a design may naturally point in a direction. For example an arrow.

Objects opposing the intrinsic directional forces of an object can impart visual direction to other elements in the composition

# Visual elements and Hierarchy

---



“

Approximately one in 40 area residents — some of whom may be your friends, colleagues or even your romantic partner — are looking for no-strings-attached relationships with people who are not their spouses.

# INFIDELITY

## CAN BE A CATALYST FOR CHANGE. IT CAN START A CONVERSATION.

**CHEATERS, FROM PAGE 1:**

er, Noel Biderman, 39, a wealthy and controversial man. He's been called a pimp and a pornographer, and has been compared to a drug dealer who knowingly destroys people's lives and marriages. Biderman doesn't shy away from the controversy. He embraces it, not only for its marketing potential, but for the opportunities it presents to add his voice to public discussions about marriage and infidelity—as he puts it, to “recalibrate notions about why people stray and what it means.” Biderman, who describes himself as a happily married father of two, got the idea to create a dating service for married people after learning that 30 percent of people who visit dating sites intended for singles are attached. And, although technically not a dating site, Facebook is being cited in more and more divorce proceedings, according to a law firm in Britain, which contends that 1 in 5 divorce petitions filed in the past year named the social networking site as a factor. Biderman recognized that an

untapped and potentially lucrative market existed for married people seeking affairs, and set out to create a platform explicitly for them. “What’s wrong with giving people access to a community of like-minded people?” he says. Biderman approaches the topic of infidelity as both a savvy businessman and an amateur sociologist. He spent nearly a year and \$200,000 on research before launching the site, and delved into literature on monogamy and infidelity to learn about the biological, evolutionary and cultural roots of infidelity. “My biggest challenge when I did research,” he says, “was that I couldn’t find any evidence that women had affairs.” But Biderman knew that women did, in fact, stray — it takes two to tango, after all — and, as he puts it, “it is not in our DNA to be monogamous.” While he was confident men would use the site, Biderman focused on building a brand that would appeal to women. There is nothing accidental about the name Ashley Madison, or the fact that the website’s colors are pink and purple.

So who, exactly, uses Ashley Madison? The ratio of men to women is 2 to 1, with variations across age groups. The primary users are married men in sexless relationships and men who find their stride later in life and are looking to meet younger women. According to Biderman, there are also a number of young married women on the site, some of whom have been married less than a year. The meanings of marriage and infidelity have changed, Biderman explains. Younger people in particular are less willing to settle for relationships that leave them feeling unsatisfied. Biderman himself says he “would” use his own service, although he didn’t say whether he has. Ashley Madison typically sees an uptick in new members the day after Valentine’s Day. For a number of people who don’t get what they want from their partners on this high-pressure holiday — flowers, gifts or affection — it’s the last straw, Biderman says. They wake up the next day, take stock of their relationship

and decide to meet someone who might make them happier. “Nobody can be talked into having an affair,” Biderman says. “No one is going to watch my commercials and suddenly get the idea to cheat. Life takes them there, not my commercials.” This was the case with Morgan, an attractive 40-something married woman from Las Vegas who preferred not to use her real name for this story. Morgan set up a profile on Ashley Madison to meet other women shortly after she and her husband decided to be non-monogamous several years ago. In fact, it was Morgan’s husband of 12 years who told her about the site. “I wasn’t looking for anything serious,” Morgan tells me, “which is why it was such a good fit, because there’s an understanding that people are already in relationships. I liked that there was this upfront understanding. “It didn’t feel like a meal market, although it was,” she explains, adding that it felt inviting rather than sleazy. Morgan and her husband are still married, and she says their

relationship is stronger than ever. “We’ve realized that our friendship is very, very deep. We very much support whatever will make the other person happiest. And we truly mean that.” She scoffs at the idea that Biderman is breaking up relationships. “Ashley Madison doesn’t create a cheating environment,” she says. Biderman “is not ruining people’s marriages; it’s the people in the marriages who are ruining them.” Biderman, of course, agrees. Ashley Madison didn’t invent cheating, he says, adding that cheating doesn’t make someone a bad person; nor does it have to be the end of a marriage. “Infidelity can be a catalyst for change. It can start a conversation. It can save your marriage,” he says. As for Ashley Madison, business is booming and more growth is in sight. As Biderman puts it, “There is no stopping this train.” A version of this story appears in this week’s *Las Vegas Weekly*, a sister publication of the Sun. Lynn Comella is a women’s studies professor at UNLV.



## HIERARCHY:

visual elements composed in a logical sequence

crucial elements in contrast with elements with less importance

layering of elements according to their importance

position of elements leads the way how the image is to be read

## TYPOGRAPHIC HIERARCHY:

highlighting various information and its importance

working with different size of font

working with various weights of font

Hierarchy

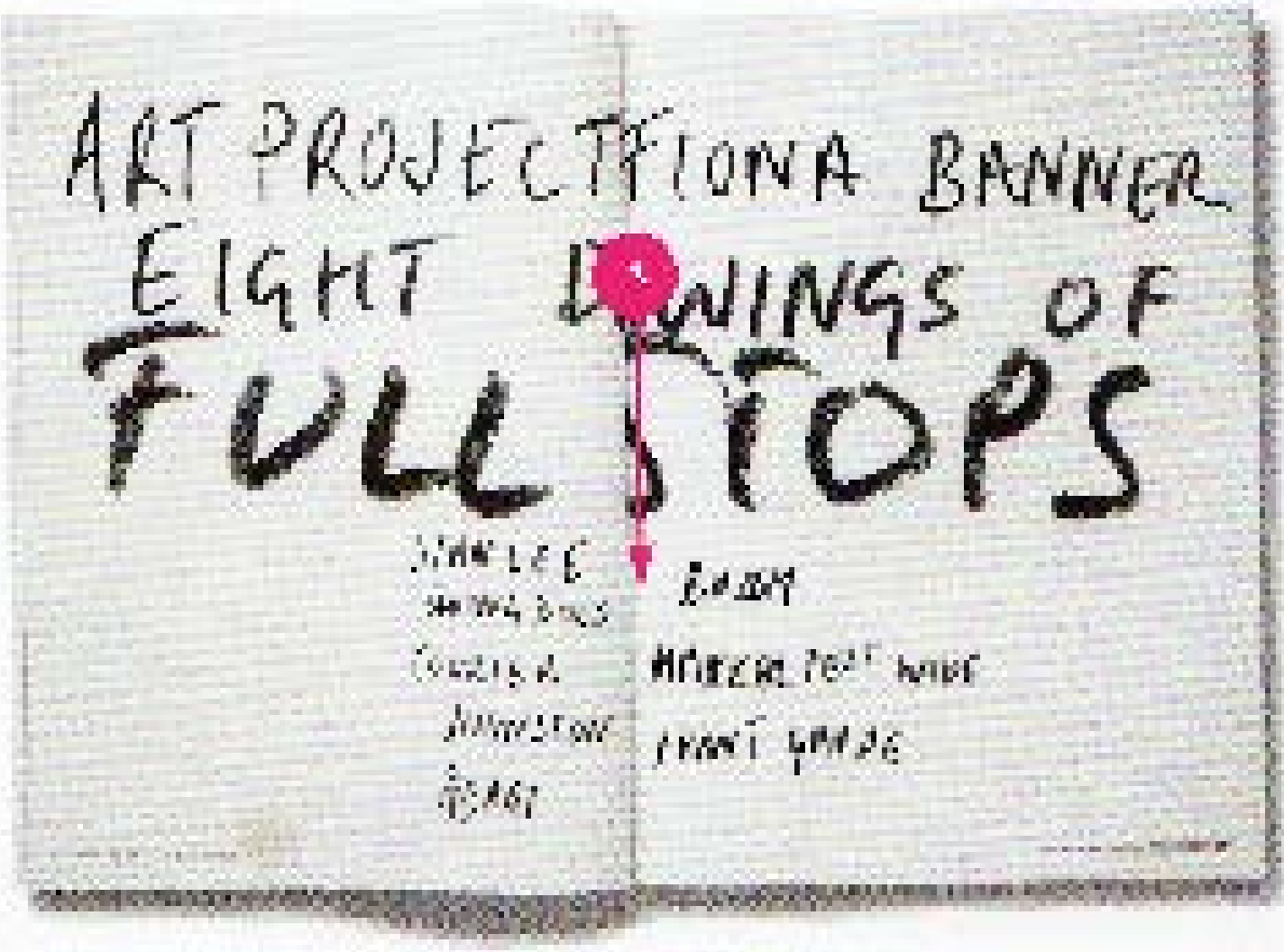
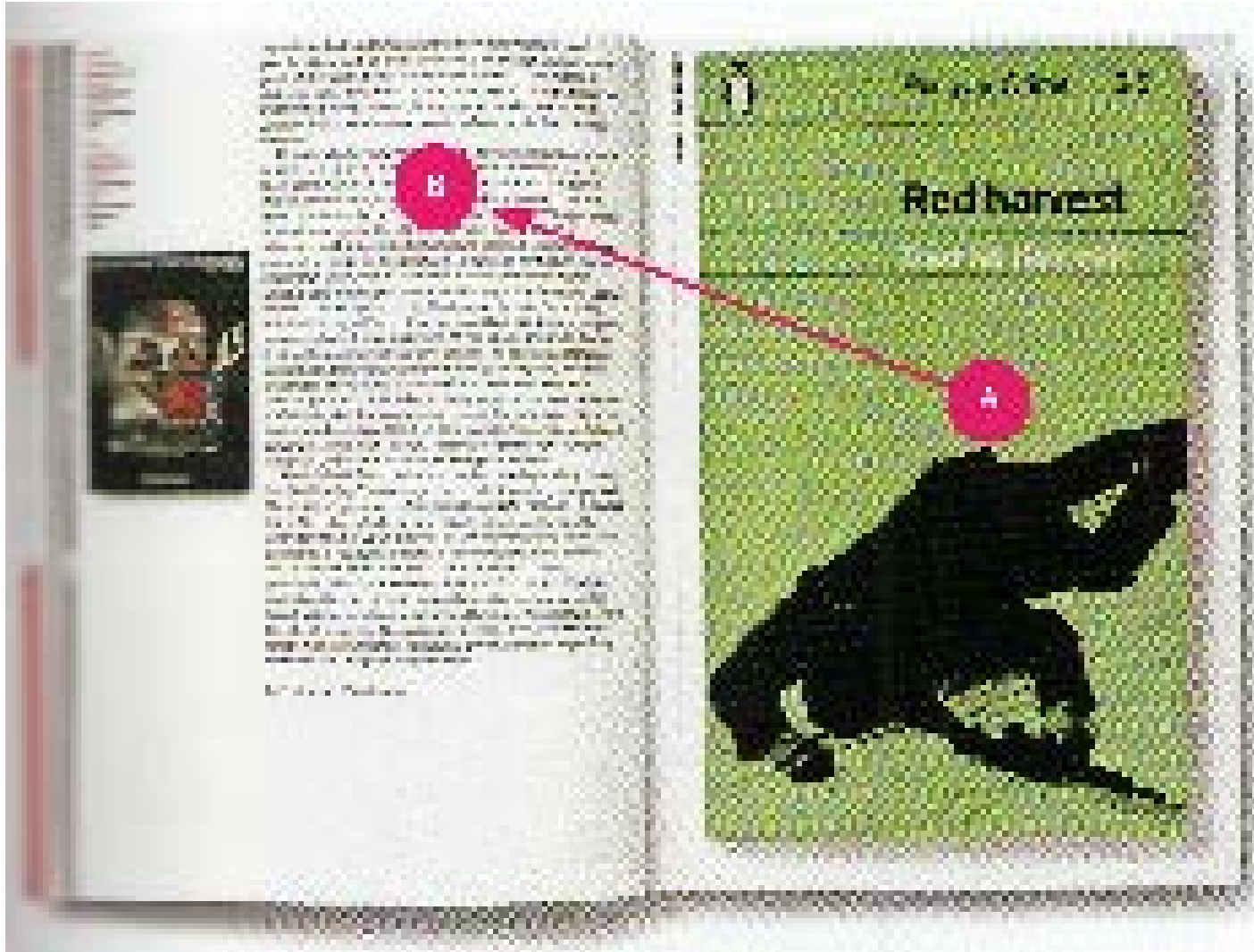




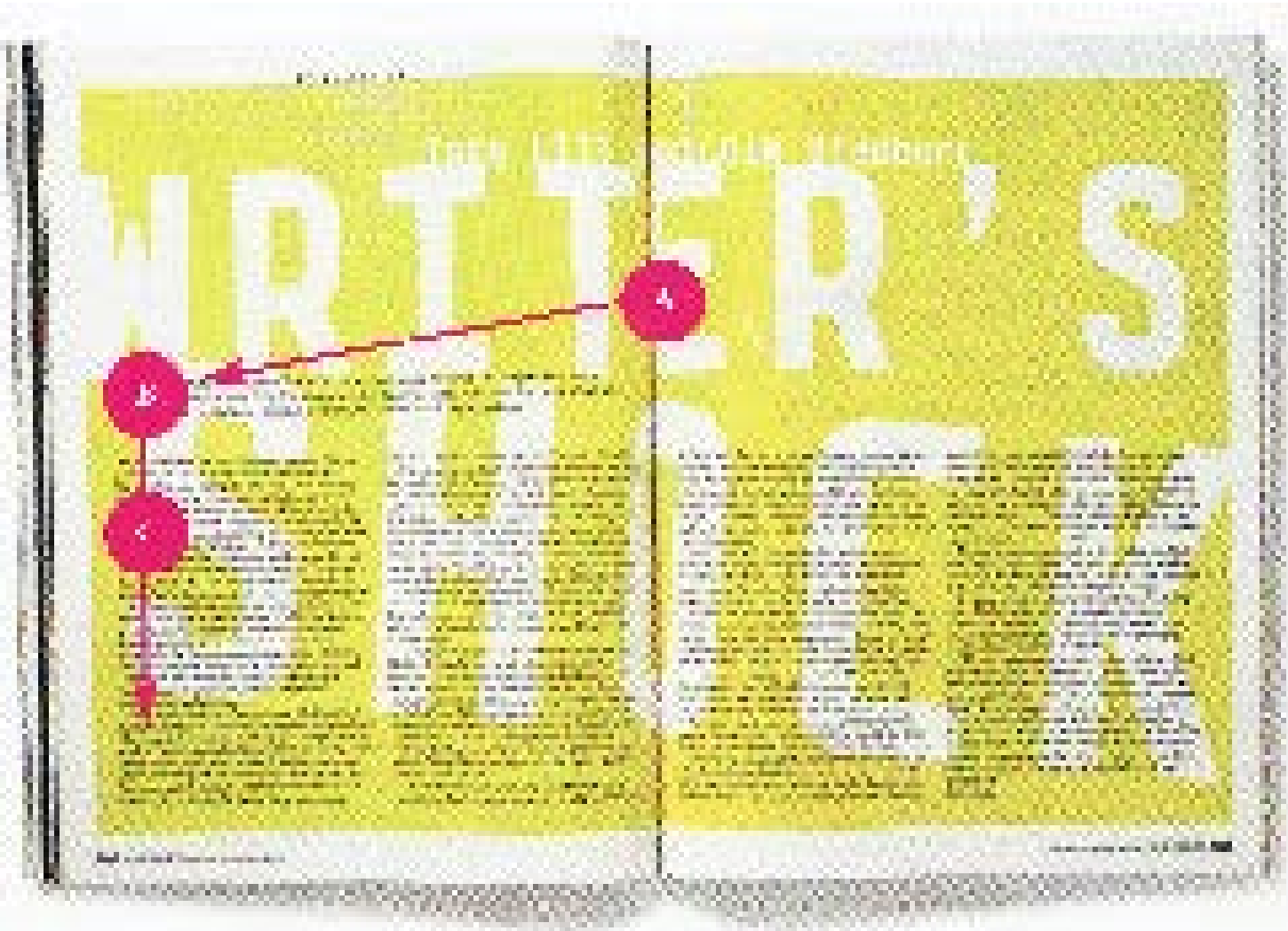
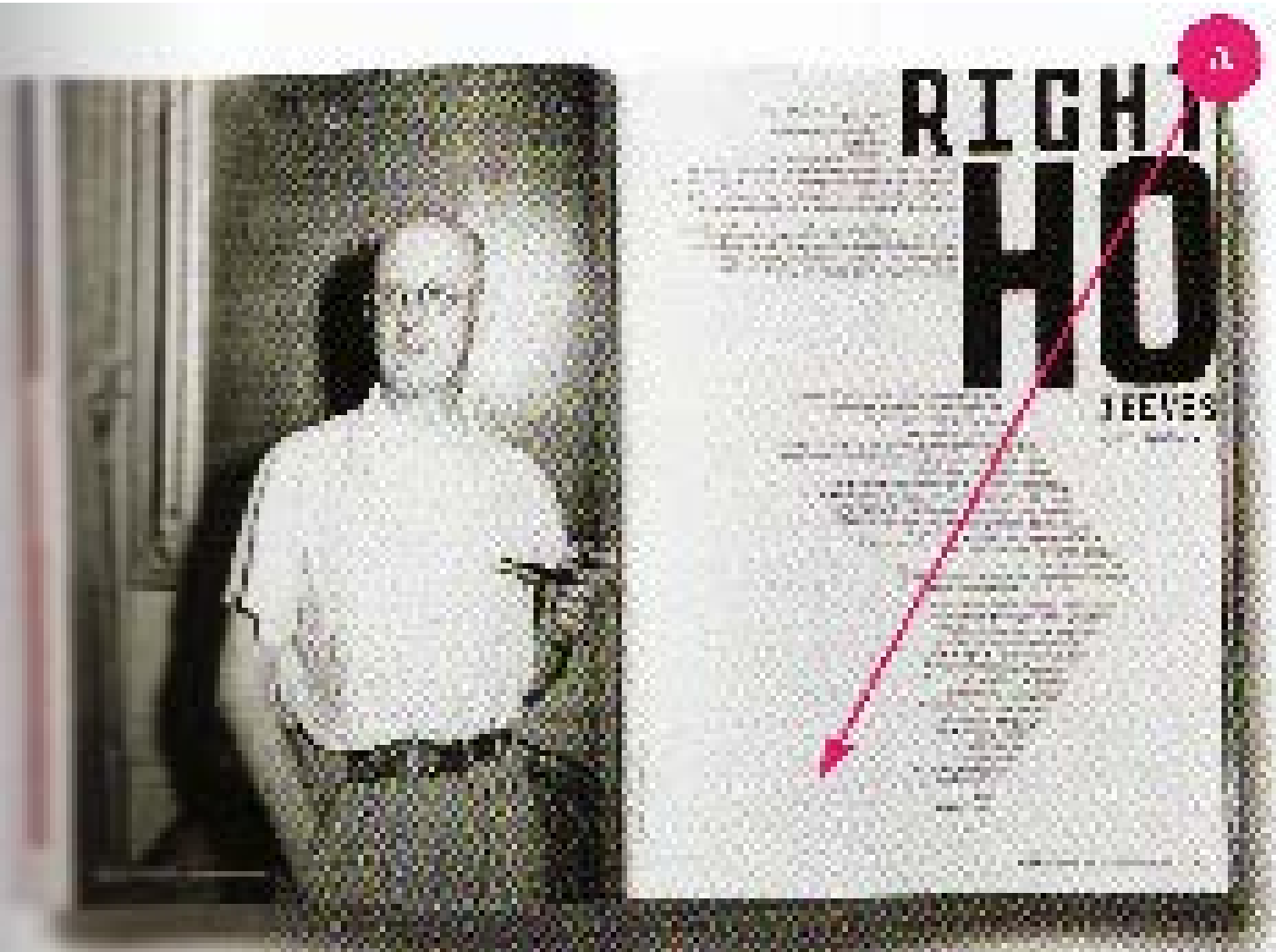
# Hierarchy



Hierarchy



Hierarchy

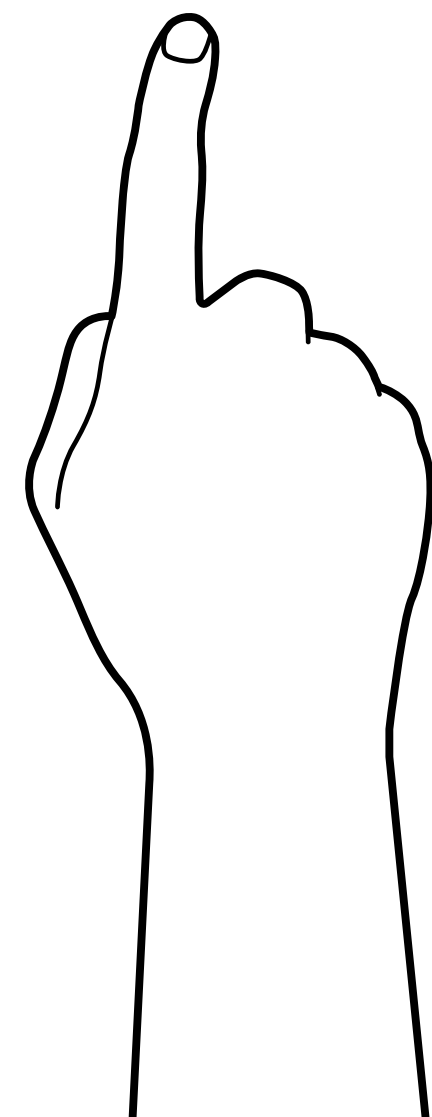


# Hierarchy



# Ogilvy's way of reading posters

---



# HOW WE LOOK AT A POSTER

## OGILVY:

illustration > upper element

title > above the illustration

text > above the title



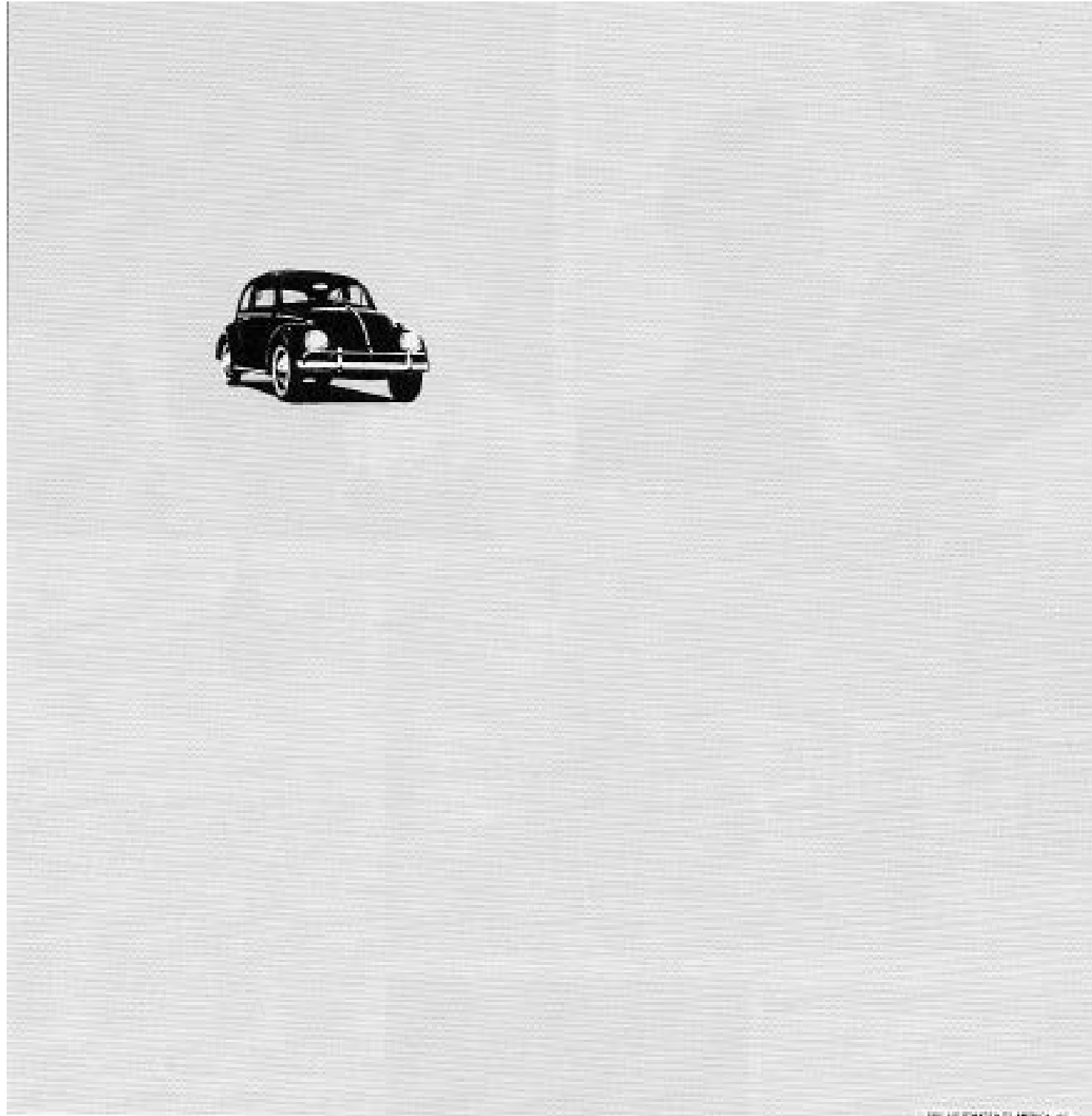
## Lemon.

The VW Beetle is not the car.  
The 1978 VW Beetle is the car.  
It's the only car that gives you the  
best of both worlds. It's the only  
car that's been around for over 50  
years. It's the only car that's  
still going strong.

It's the only car that's been  
around for over 50 years. It's  
the only car that's still going  
strong. It's the only car that's  
still going strong.

It's the only car that's been  
around for over 50 years. It's  
the only car that's still going  
strong. It's the only car that's  
still going strong.





## Think small.

Our little car isn't so much of a novelty any more.  
A couple of dozen college kids don't try to squeeze inside it.  
The guy at the gas station doesn't ask where the gas goes.  
Nobody even stares at our shape.  
In fact, some people who drive our little

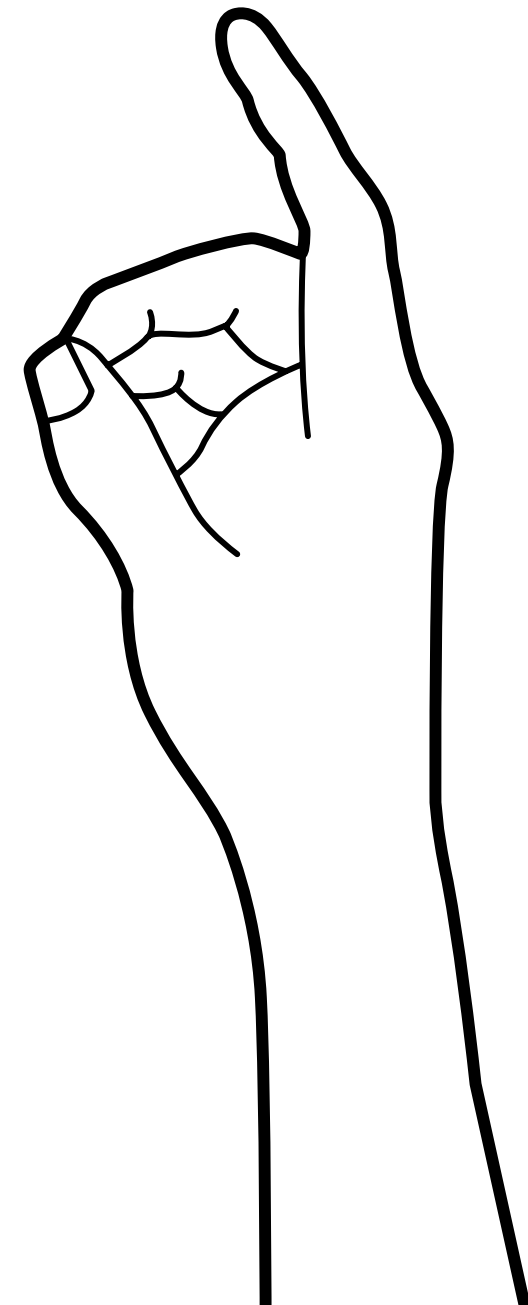
flivver don't even think 35 miles to the gallon is going any great guns.  
Or using five pints of oil instead of five quarts.  
Or never needing anti-freeze.  
Or racking up 40,000 miles on a set of tires.  
That's because once you get used to

some of our accessories, you don't even think about them any more.  
Except when you squeeze into a small parking spot. Or renew your small insurance. Or pay a small repair bill. Or trade in your old VW for a new one.  
Think it over.

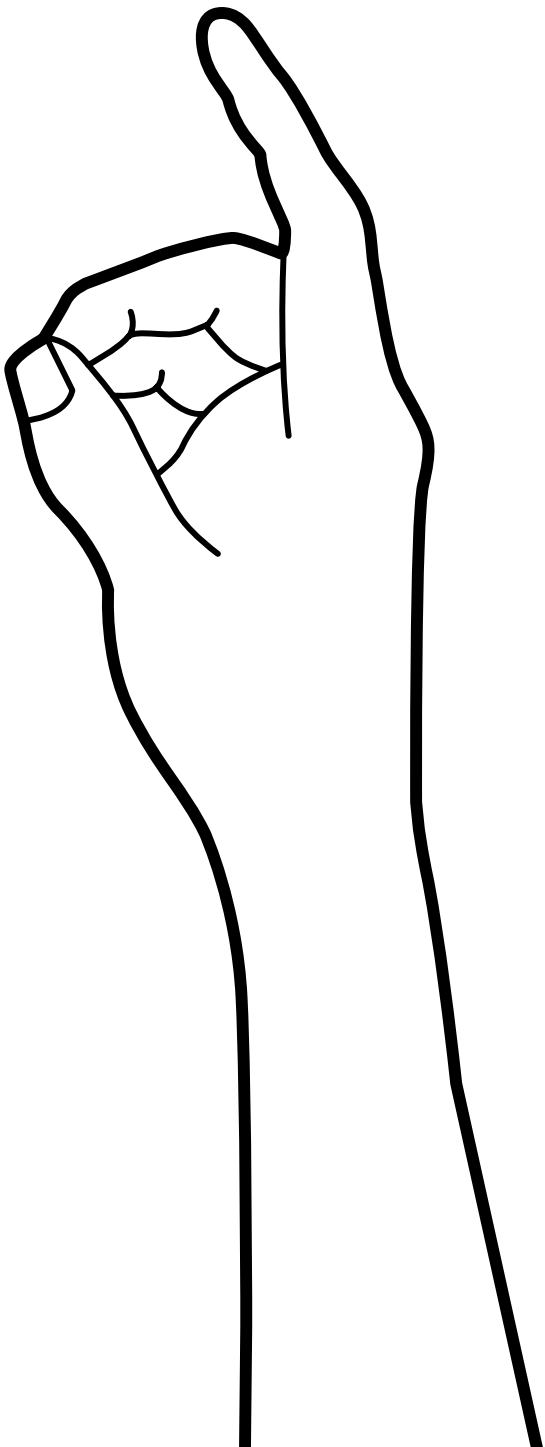




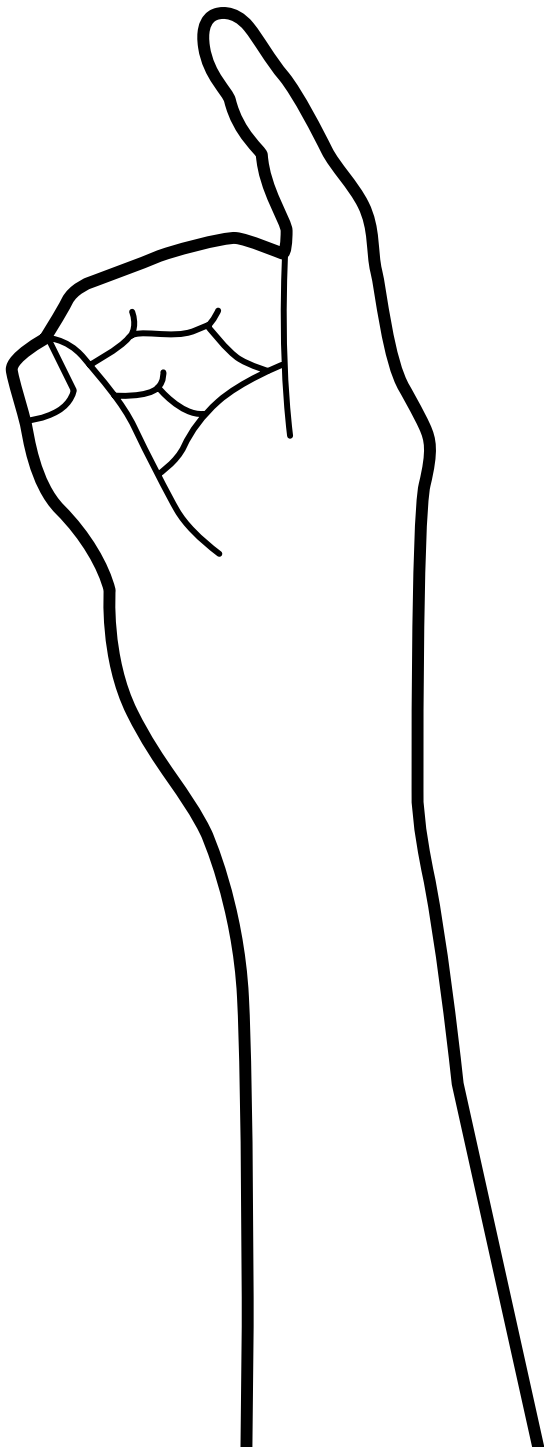
● **Typography**



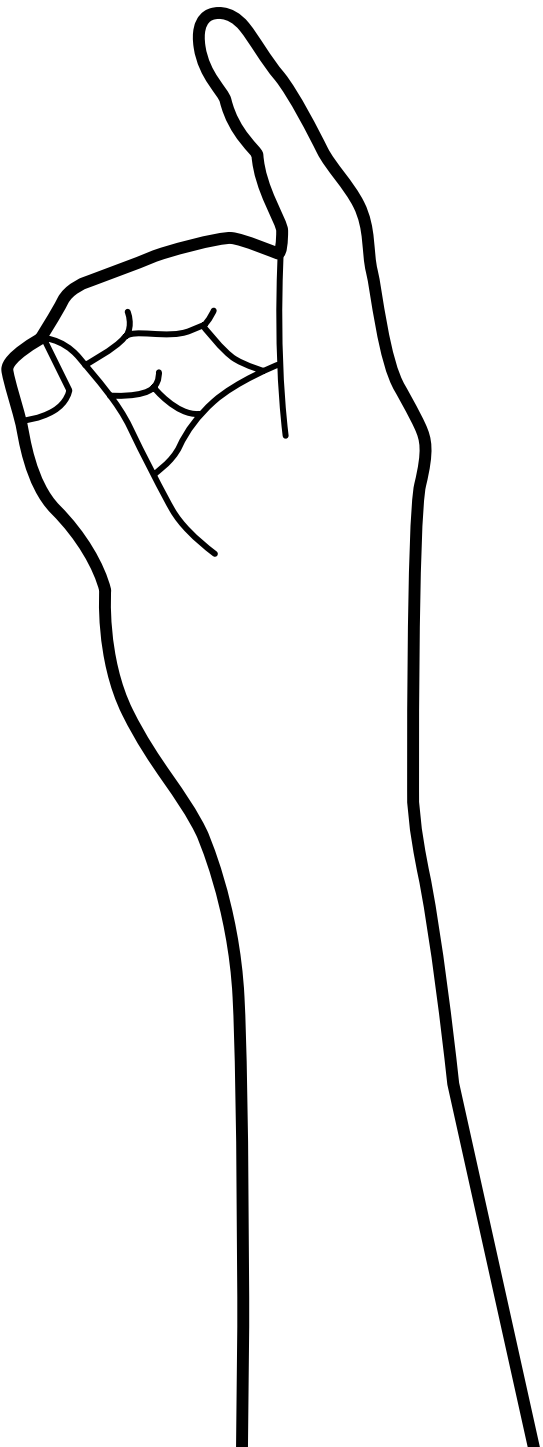
**Font style**



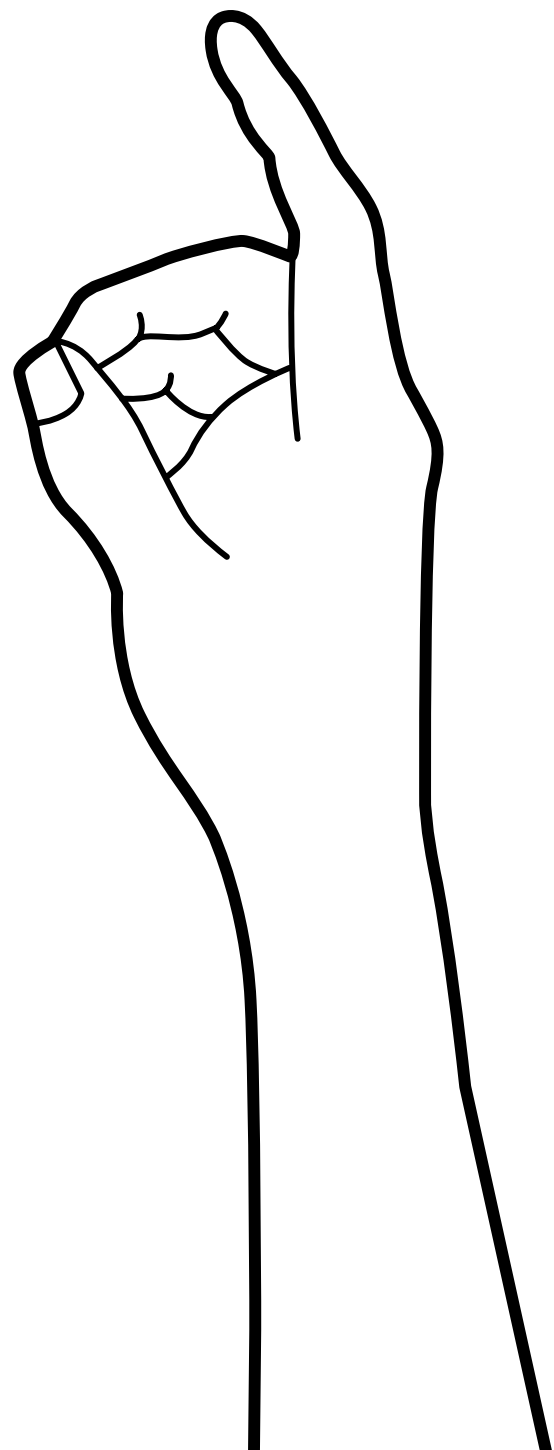
**Font family**



**Font weights**



### Setting of text boxes



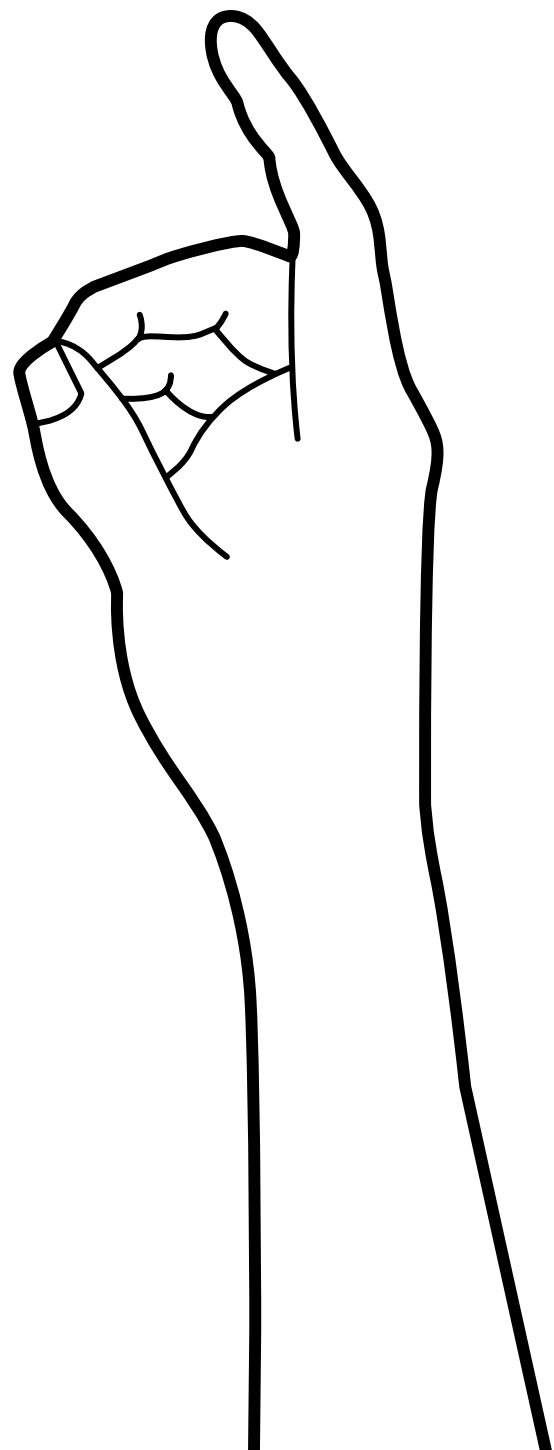
DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choice which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

left alignment

DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choice which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

left justify alignment

### Setting of text boxes



DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choice which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases). A big downside of the current version of DIVINE is that for programs with inputs, this input has to be simulated by nondeterministic choice which is very inefficient. Therefore we present an approach for symbolic representation of inputs in DIVINE.

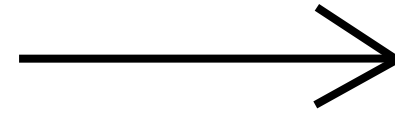
**alignment**

**width of a text box**

**font size**

**leading**

left alignment



Left alignment keeps same  
gaps between words

**MASARYK UNIVERSITY**

**EACirc**

**Using genetics to improve encryption**  
Martin Ukrop, Petr Švenda, Marek Sýs, Václav Matyáš et alii

Fort me on GitHub!  
github.com/crocs-muni/eacirc

### Problem statement

**Randomness testing**  
The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?  
EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.

**Iterative design**  
The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions).  
It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

### EACirc workflow

**1. Forming a population**  
A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.

**2. Test vector generation**  
Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.

**3. Fitness assessment**  
Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0,1].

**4. Survival of the fittest**  
Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival.  
The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.

**5. Mutation & crossover**  
To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population.

### Comparison to existing tools

**EACirc vs statistical testing**  
The standard way to assess randomness is to use batteries of statistical tests such as *NIST STS*, *Dieharder* or *TestU01*. We run them along with EACirc and compare the results.  
To have a fine-grained comparison, we have analyzed 77 different functions (*eStream*, *SHA-3* and *CAESAR* candidates). For 2-round *Hermes* and 1-round *Fubuki* we confidently surpass *NIST STS*.

**Further information**  
Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).  
[1] Švenda, Ukrop, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications. Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.  
[2] Kubiček, Novotný, Švenda, Ukrop. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications. Vol. 8, iss. 1. 2016.

**CRoCS** Centre for Research on Cryptography and Security

This work was supported by the Czech Science Foundation project GAP202/11/0422.

## Text and legibility

**Black text on a white  
background allows  
common speed  
reading.**

**Black text on a white  
background allows  
common speed of  
reading.**

**White text on black  
background  
reduces reading  
process of 15 %.**

**White text on black  
background is  
optically thicker.**



*Text in Italics reduces readability of 15 %.*

**LONGER UPPERCASE TEXT REDUCES  
REDABILITY OF 15 %**

**TEXT**

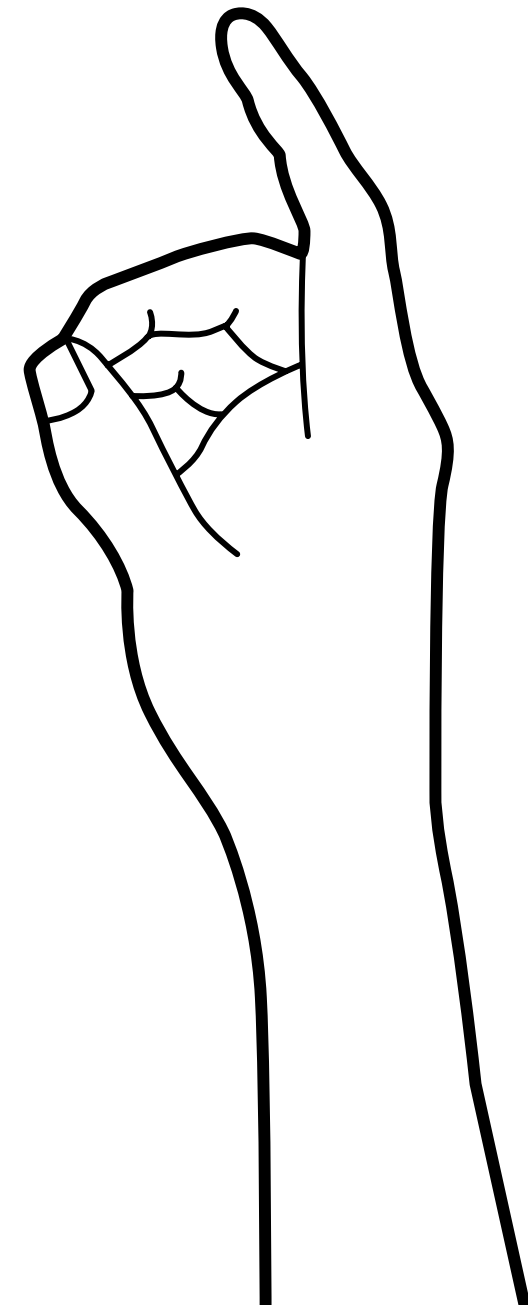
**Left alignment doesn't  
have any affect on speed  
of reading.**

**Left alignment doesn't  
have any affect on speed  
of reading.**

**TEXT**

**Left justify alignment  
doesn't have any affect  
on speed of reading. Left  
justify alignment doesn't  
have any affect on speed  
of reading.**

## ● **Typography and errors**



# A TYPOGRAPHIC RIVERS

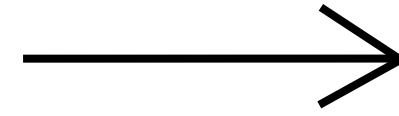
Dr. Jozef Ferenczy učil celé generácie študentov a nitrianske gymnázium malo aj jeho zásluhou veľmi dobré meno. Okrem Karola Pongrácza k jeho žiakom patrili okrem iných i maliari Maximilián Schurmann (1890 – 1960).

gaps in typesetting, which appear to run through a paragraph of text, due to a coincidental alignment of spaces

spaces caused by full text justification or monospaced fonts

no hyphenation

left justify  
alignment



### Systems Performance Benchmark — Four Nodes (32 vCPUs)

Category	Storm	Spark	Samza
Identity	~1000k	~1800k	~1600k
Filter	~1000k	~1500k	~1800k
Count	~1000k	~1500k	~1400k
Aggregation	~1000k	~900k	~1500k
Top N	~900k	~1500k	~1600k
SYN_Dos	~1000k	~1500k	~1600k

- Samza and Spark have a high-enough flow throughput and can be used for the analysis of data from multiple networks at the same time.
- Apache Spark system has been chosen as it offers an easy management and a high versatility in terms of the running environment and proprietary processing methods (e.g., sliding window).

The demonstration cluster consists of 7 virtual machines, one is dedicated to IPFIXcol, 5 to Spark and one to the Kibana and Web server. The following configuration is the same for all machines:

- (4 vCPUs) Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz,
- 8GB 1600MMHz DIMM DRAM EDO,
- 85GB SCSI Disk with 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI,
- 10 Gbit/s network connection, 1 Gbit/s virtual NICs.

IPFIXcol is a flexible IPFIX flow data collector designed to be easily extensible by plugins. In our demonstration, we use only part of its wide functionality – data acquisition from multiple network probes and their transformation into a JSON data stream.

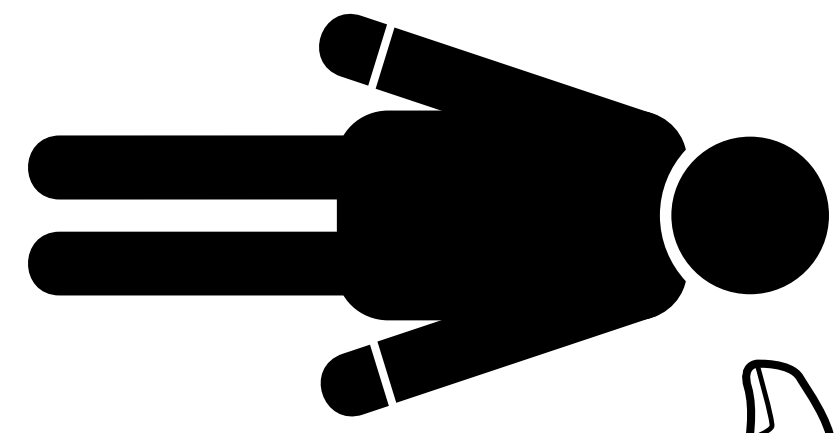
### Real-time TOP K Statistics

Provides a real-time computation of Top K statistics to enhance network situational overview.

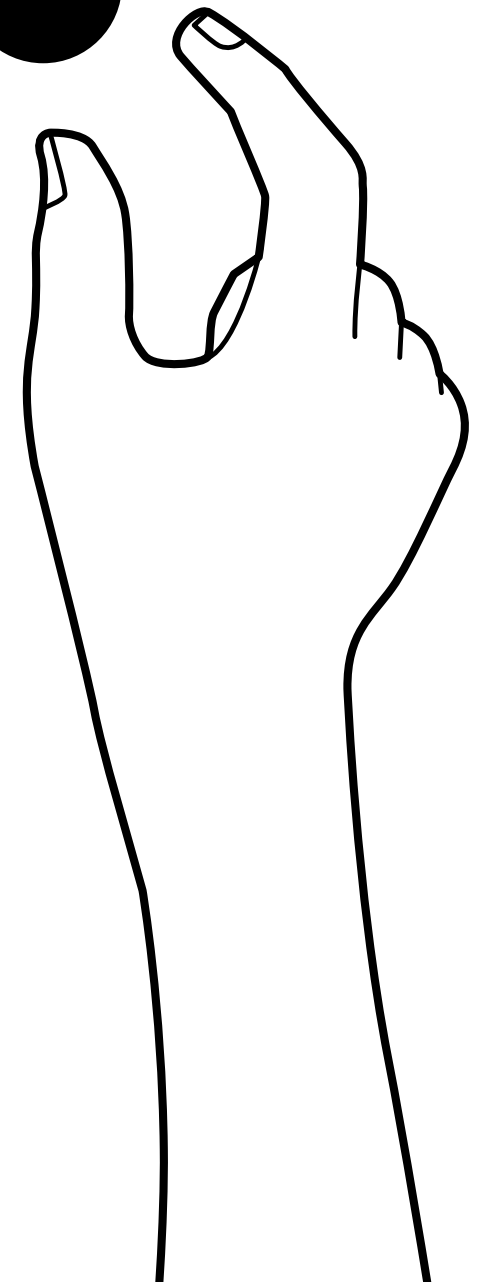
Left alignment keeps same  
gaps between words

typographic  
rivers

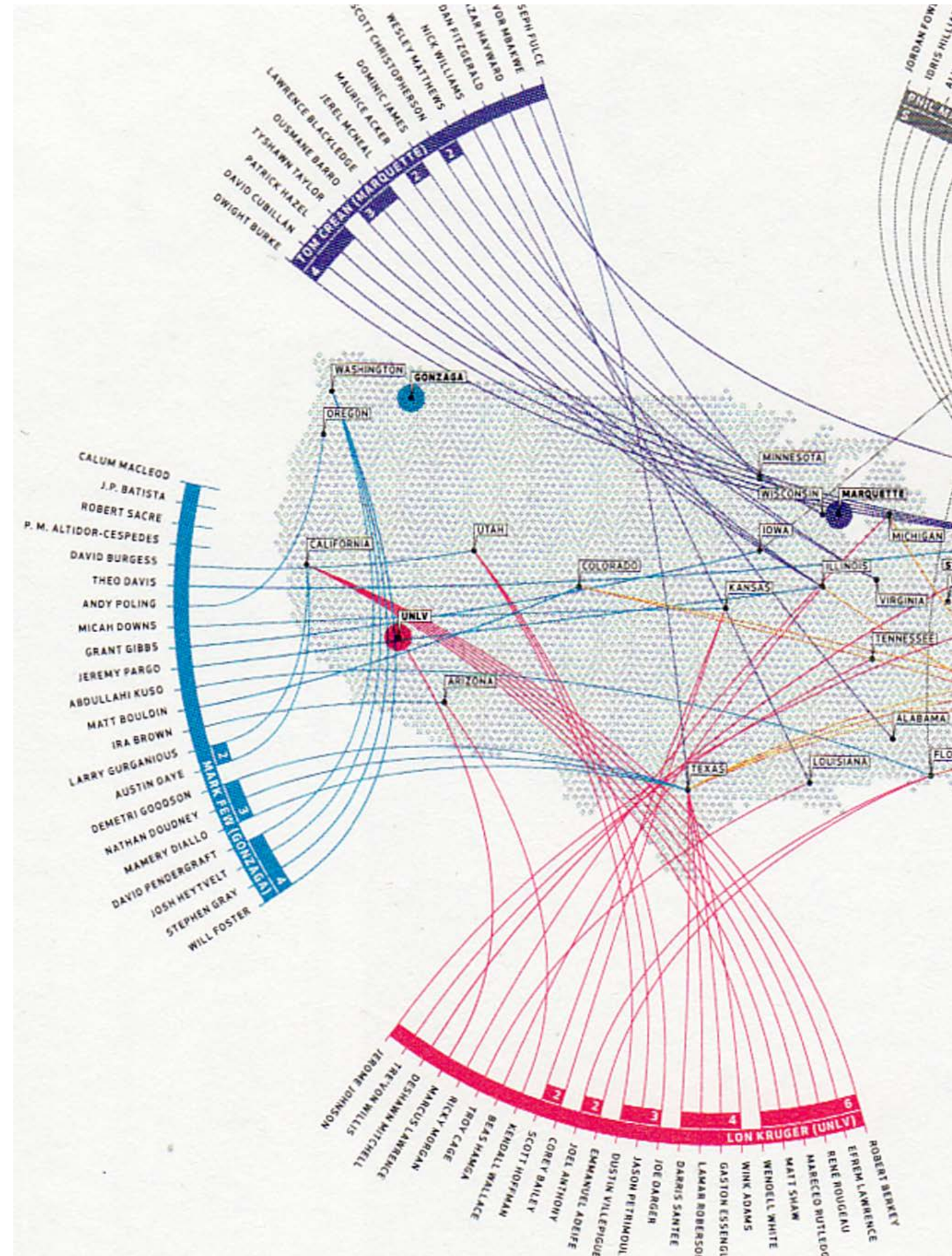
without  
hyphenation



**Infographics**

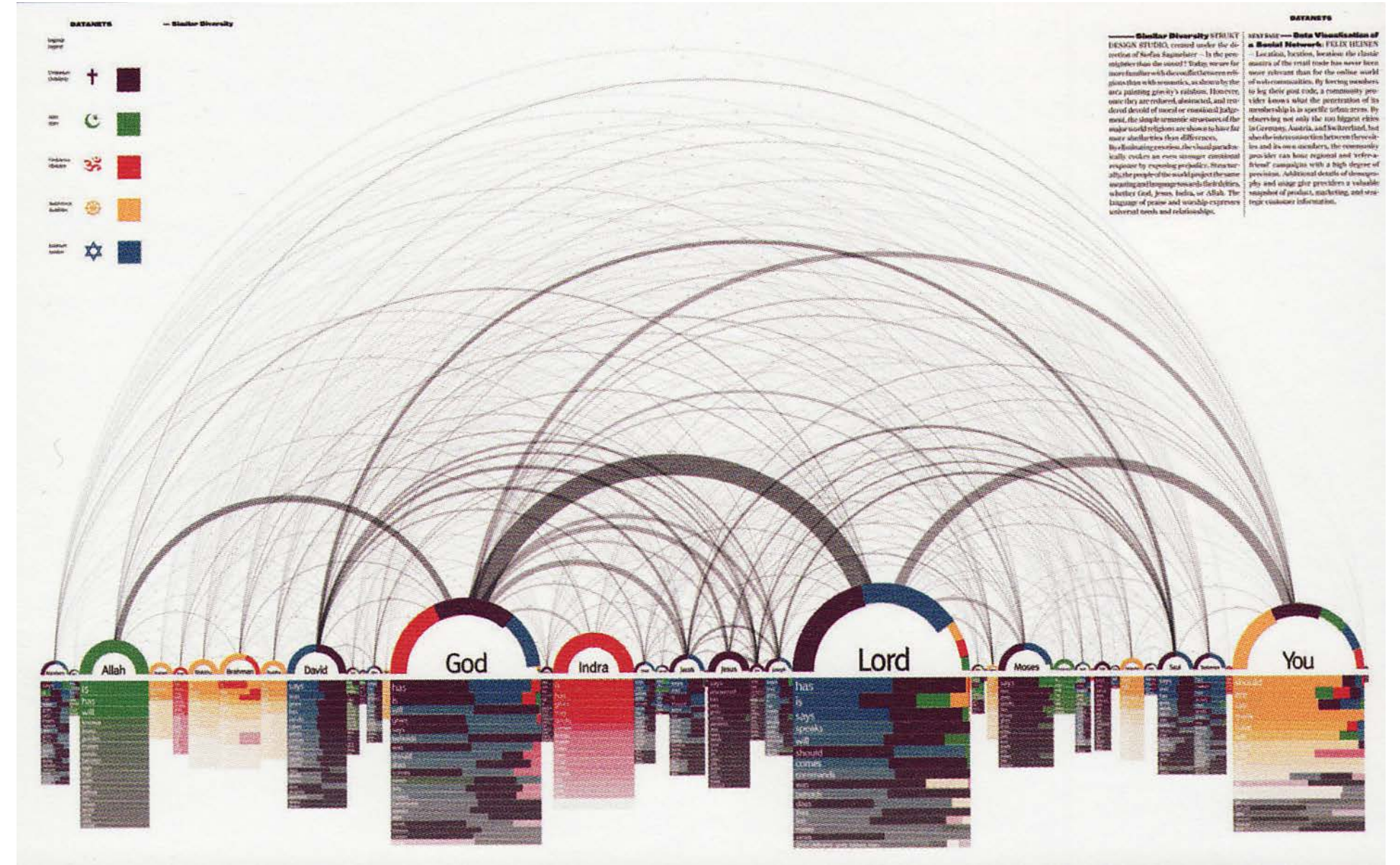
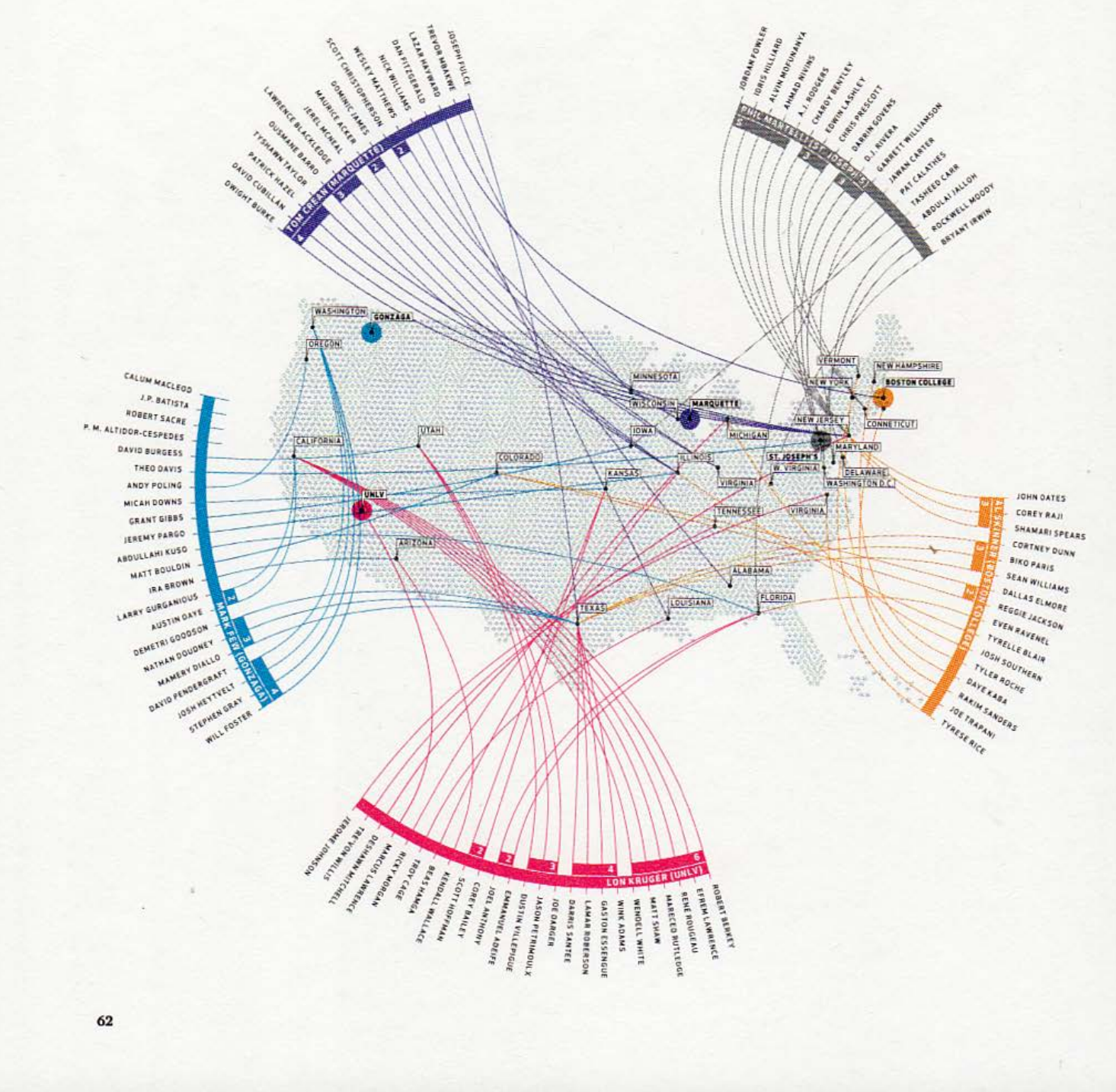


# Infographics



**DATANETS** — **Seen There** (CATALOGTREE) — 'It isn't what you know, it's who you know that counts in business.' Building a network of contacts is just as important in the sports world as it is in business, and as the importance of NBA coaches as 'kingmakers' has grown, so has too interest in their behaviour and strategy. This study for ESPN elegantly shows how the top five coaches criss-cross the United States to find the Shaq O'Neills and Michael Jordans of tomorrow. From this work, based on the map of North America, a prospective NBA star can quickly spot the best networking opportunities, as well as the likely hotspots of success and stardom.

**Cluster-Ball: Humans, Medicine, History** CHRIS HARRISON, data provided by Wikipedia — Language can be seen as a semiological net, exposed through the internet by a web of volunteer workers. And Wikipedia is becoming the default reference to knowledge and understanding. In this diagram, Chris Harrison not only shows the connection between the concepts pervading our humanity, but indicates the hierarchy in which they have been placed by Wikipedians. Genetics, extinction, technology, and even personal life are all displayed in the click-work tapestry surrounding the concept. The structured network of meaning and content subtly alludes to new ways of thinking about evolution, and about how the DNA of different species is represented. Rather than being portrayed as distinct branches on a tree, subsequent stages of evolution are captured inside and through species. In a similar way, we can look at language not as a tree, but as a network of references and dynamic relationships.





## GET TO KNOW YOUR STREET VENDORS

### WAYS TO A BETTER VENDOR WORLD

In New York, street vending has always attracted ambitious, hard-working men and women with limited economic options. Successive waves of immigrants - Jewish and Italian in a previous era, now Chinese, Bangladeshi, Afghan, and Senegalese - have used vending to gain a foothold in their new country. Its low startup costs, independence, and flexibility make vending a traditional first stop for small business entrepreneurs.

But vending isn't an easy way to get ahead. Throughout New York City's history, merchants resentful of "unfair" competition have joined forces with city officials concerned with congestion, modernization, and "quality of life" to bar vendors from streets and regulate them excessively. These complex and shifting laws force vendors back and forth across the border between the formal and informal economies, making it difficult for vendors to serve the public and make a decent and honest living.

Here are four basic ways the City can make vending laws work better for vendors, their customers, and everyone else.

### 1. LIFT THE CAPS

It's virtually impossible to get a vending license in New York City because of strict caps, or limits, placed on the number of vendors in the 1970s and '80s. The estimated wait for a general vending license is several decades. By setting the caps far below vendor supply and public demand, the City unintentionally creates a thriving and exploitative black market for permits and licenses. Legal vendors have to buy licenses from illegal middlemen at exorbitant prices. Other vendors are driven underground, where they're unlicensed and unregulated. To bring vendors into the legal mainstream, the City should raise the caps to realistic levels and crack down on the black market in licenses and permits.

### 2. INCREASE STREET ACCESS

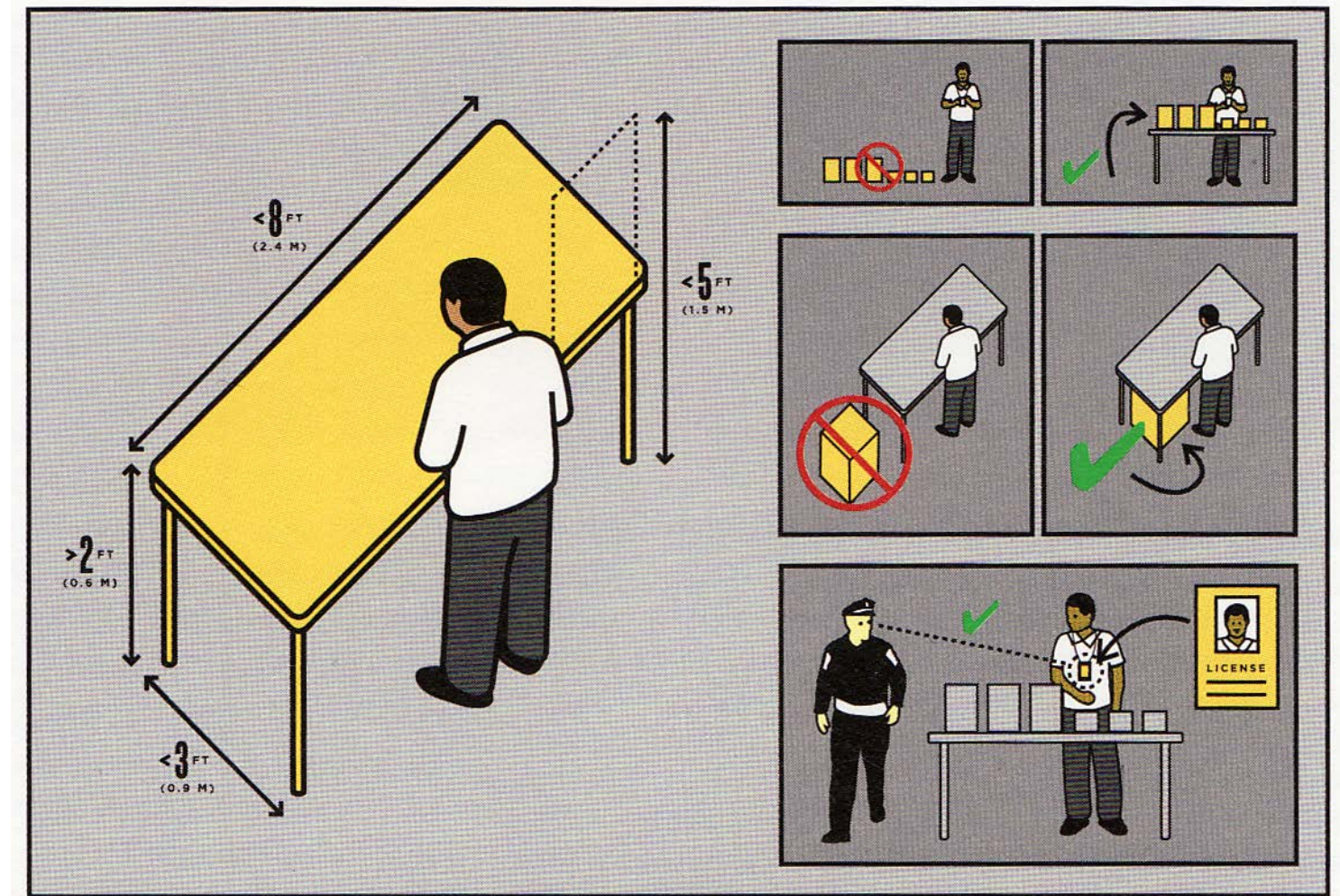
Vendors need foot traffic to survive, but waves of street restrictions have forced them farther away from the areas of the city that can support them. Pressure from merchant associations in the 1970s and Business Improvement Districts (BIDs) in later decades led to widespread restrictions, and Mayor Rudolph Giuliani made street restrictions a centerpiece of his "quality of life" campaign. Even on open streets, complex rules make it difficult to legally vend. The City should review street closings according to set criteria and rescind restrictions not founded in legitimate concerns about safety and street congestion. It should also simplify time-of-day restrictions to make them easier for vendors to understand and follow.

### 3. REDUCE THE FINES

In 2008, Mayor Michael Bloomberg quadrupled the maximum fines for street vendor violations from \$250 to \$1,000. A few tickets for parking a cart more than 18 inches from the curb or less than 20 feet from a storefront can wipe out months of earnings. Other businesses pay less for more serious violations while having a greater ability to pay. Vendors are entry-level small business owners who cannot absorb fines as a cost of business. The city should reduce fines to pre-2008 amounts - a level that deters violations but doesn't put vendors out of business.

### 4. REFORM ADMINISTRATION AND ENFORCEMENT

Vending regulation is a patchwork of policies from the last hundred years that both vendors and the police find hard to understand. The official rulebook is a series of photocopied and unformatted excerpts from the city code - rough going, even for native English speakers. As a consequence, vendors who want to follow the rules often get tickets for violations they don't understand, and police who want to enforce the rules often give tickets for violations that don't exist. To increase compliance, the City should simplify vendor regulation and create a new rulebook that clearly explains the rules in English and a few of the many languages vendors speak.



### FOOD VENDORS

**COMMON ITEMS SOLD:** Hot dogs, coffee, fruit, ice cream, donuts, bagels, burritos, health, toast, tamales, capers, cream, flavored nuts, pretzels.

**NUMBER OF VENDORS:** Only 5,000 street food vending permits are available. The average wait time to receive one is 5-10 years.

### GENERAL VENDORS

**COMMON ITEMS SOLD:** T-shirts, hand bags, watches, scarves, gloves, belts, neckties, perfumes, umbrellas, cell phone accessories.

**NUMBER OF VENDORS:** The City of New York has capped the number of general vending licenses at 882 (excluding veteran vendors). The waiting list for licenses has been closed since 1992.

### FIRST AMENDMENT VENDORS

**COMMON ITEMS SOLD:** Books, newspapers, CDs, DVDs, paintings, photographs, handbags, coats and jewelry, items with political messages.

**NUMBER OF VENDORS:** Since 1982, vendors who sell expressive materials are protected by the First Amendment and do not need a license. There are around 1,000 First Amendment vendors.

### VETERAN VENDORS

**COMMON ITEMS SOLD:** Anything from the general vendor category: gloves, neckties, cell phone accessories, scarves, 1-800s, hand bags, watches, belts, perfumes, umbrellas.

**NUMBER OF VENDORS:** Under New York state law, honorably discharged U.S. military veterans may receive a general vending license despite the 883-cap. There were 1,704 veteran vendors on record in 2005.

### UNLICENSED VENDORS

**COMMON ITEMS SOLD:** Anything from the previous categories: umbrellas, tamales, ice cream, hand bags, scarves, watches, perfumes, DVDs.

**NUMBER OF VENDORS:** There are perhaps 6,000 unlicensed vendors (vendors really know). Only half of vendors are licensed due to license caps.

## THE CITY DEFINES FOUR TYPES OF VENDORS

## THE CITY DEFINES FOUR TYPES OF VENDORS

## THE CITY DEFINES FOUR TYPES OF VENDORS

## THE CITY DEFINES FOUR TYPES OF VENDORS

## THE CITY DEFINES FOUR TYPES OF VENDORS

**HI, I'M MUNNU DEWAN**  
I sell hot dogs and pretzels in front of 2 Lafayette Street. I moved here from Bangladesh in 1991 and I have been a street vendor for 17 years. I love it but this is not easy. I haven't gotten a ticket in three years, but before that I got around 100 tickets. One time I got a ticket because my jacket covered my license. And then I have to pay a \$1,000 fine. Do you have \$1,000 in your pocket? You don't have it! I don't have it! This is a small business. I sell 20 hot dogs a day. This hand makes money and the other hand finishes it very fast. How do they think I can give so much?

**HI, I'M NOR DIOP**  
I'm here at 55th Street and I sell handbags. If it's very cold, I sell scarves and gloves. But that job is not easy. My family is in Africa. I send some back to them. If I have anything, I send \$100, \$150, but it's not enough for my family. My wife, my children, my mother is over there. Working outside is very hard. I wear jackets, gloves, and three pairs of pants. Sometimes I can only stay out here for 4 or 5 hours. I'm going to finish this for this month and see, if it's not good after this month, I'm going to stop and give the city my license back. Maybe I could drive a taxi or get a job in a restaurant. I have no other possibilities. I don't want to stay at home.

**HI, I'M XIAN LING DONG**  
I sell paintings in Times Square on 52nd and 7th Ave. I came here from Qingdao, China and I've lived in the U.S. for six years. I've been vending for five. I enjoy vending because it allows work when I want, which you can't do working at a restaurant. It is also good for my husband who for health reasons cannot work another job. The trouble with the job is the way the police bother me and the tickets they give. Sometimes they say my display is too high, sometimes they say I am too far from the curb. They say all kinds of things, but I know the law, and I know that everything I'm doing is exactly right. When I am not vending, I like traveling - San Francisco and Las Vegas are two of my favorite spots. (Translated from Mandarin)

**HI, I'M BERT STEIN**  
On the street they call me Mr. B or Mr. Bert. That's because I'm 73 and a disabled war veteran and they show some respect. I started vending when my printing business went bankrupt after 9/11. I sell neckties, perfumes, scarves in winter. A lot of people come to New York strictly because of the street vendors. They can get things here that they can't get other places. The police don't know the rules. The book is written in such a way that everybody scratches their heads and wonders what they're talking about. Sometimes the police will take your merchandise away, and they move it around - downtown, to Brooklyn, to Queens - and no one's keeping track. It took me three days of constant calling to track down my merchandise, and I was shown not guilty. But I took three days and I lost a lot of money.

**HI, I'M RAFAELA MENDOZA SANTANA**  
I couldn't find a job when I moved here from Mexico four years ago, so I make tamales, ames, corn tortillas, and churros. Like I did in Mexico, where I'm from, I start cooking at 2 a.m., and head out at 6 a.m. I'm selling in the cold, in the heat, everyday by the hospital at East 149th in the Bronx. The doctors and nurses get off the bus or pull over in the car to get one. I sell about 80 a day, sometimes 50, sometimes 70, enough to send some money to my mother in Mexico. I have a cooker, so the police watch me and make me move sometimes. But if I'm not here my clients start to call me! (Translated from Spanish)

**BUT WAIT! THERE'S ALSO**

Some photos were used to illustrate the story. All photos are the property of the author. All other photos are the property of the author.

## A electricidade em Portugal

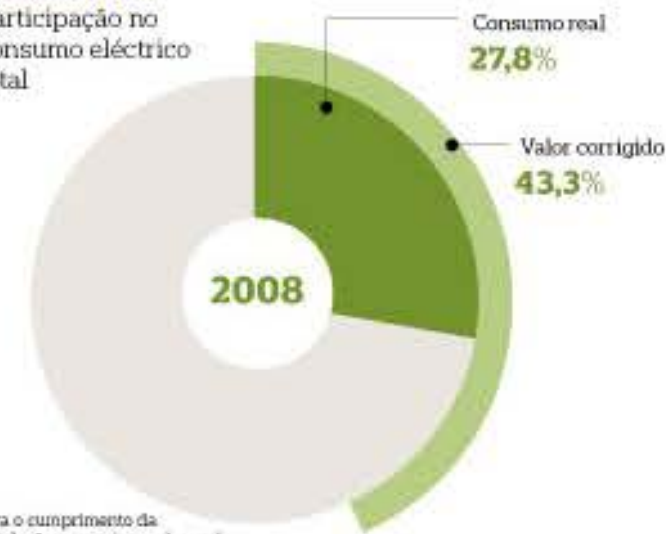
### De onde vem a nossa luz?

A eletricidade que chega às nossas casas vem de um complexo cabaz de fontes energéticas, que varia conforme o ano. Em 2008, houve muita importação e pouca produção hidroelétrica. Mas a energia do vento já começa a ter um peso significativo  
 Ricardo Garcia (texto) e Joaquim Guerreiro (infografia)

As renováveis estão a avançar, mas Portugal ainda depende muito das poluentes centrais térmicas para produzir a electricidade de que necessita. Em 2008, as termoelétricas asseguraram quase metade do consumo nacional. Se tudo ainda fosse como há duas décadas, no entanto, seria pior. Não havia ainda centrais a gás natural e o país dependia fortemente do carvão, que polui muito mais. Em anos secos, o país não tinha alternativa de fontes renováveis de electricidade, dado que a única opção realmente importante eram as barragens. Hoje, o cabaz de fontes energéticas para a produção eléctrica é muito mais variado. O vento, no ano passado, forneceu quase tanta energia quanto as barragens, reduzindo o peso das centrais térmicas. O que os dados aqui coligidos pelo PÚBLICO mostram é que, salvo as eólicas, as chamadas "novas" renováveis contribuem ainda apenas marginalmente para o bolo nacional - independentemente da relevância que o discurso político lhes dá. A produção eléctrica a partir de painéis solares fotovoltaicos, por exemplo, entra com uma fatia inferior a um por cento. A parcela mais oculta da nossa electricidade é aquela que é importada de outros países. As necessidades de importação variam ano a ano, conforme o clima e os preços dos combustíveis. No ano passado, a factura foi elevada: Portugal importou 18 por cento da electricidade que consumiu. A energia veio de vizinhos, como Espanha, que tem outro cabaz energético, onde estão incluídas oito centrais atómicas. Para muitos, esta realidade conduz a uma conclusão incómoda: queiram ou não, os portugueses consomem energia nuclear.

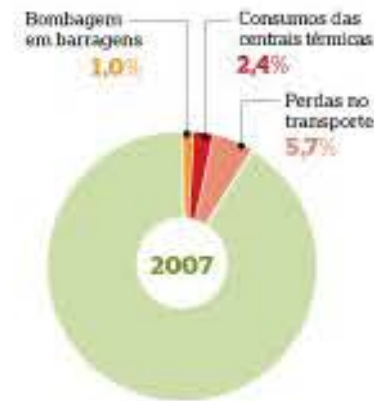
#### Electricidade renovável

Participação no consumo eléctrico total



Para o cumprimento da legislação europeia, o valor real é corrigido com base no índice de produtividade hidroelétrica de cada ano

#### O que não chega aos consumidores

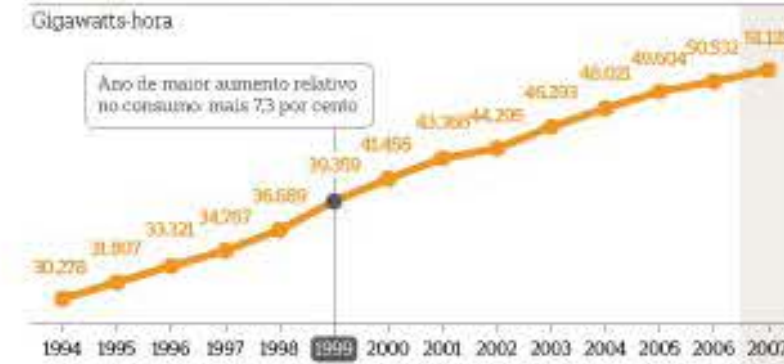


#### Perdas do total produzido

Diferença entre 1994 e 2007



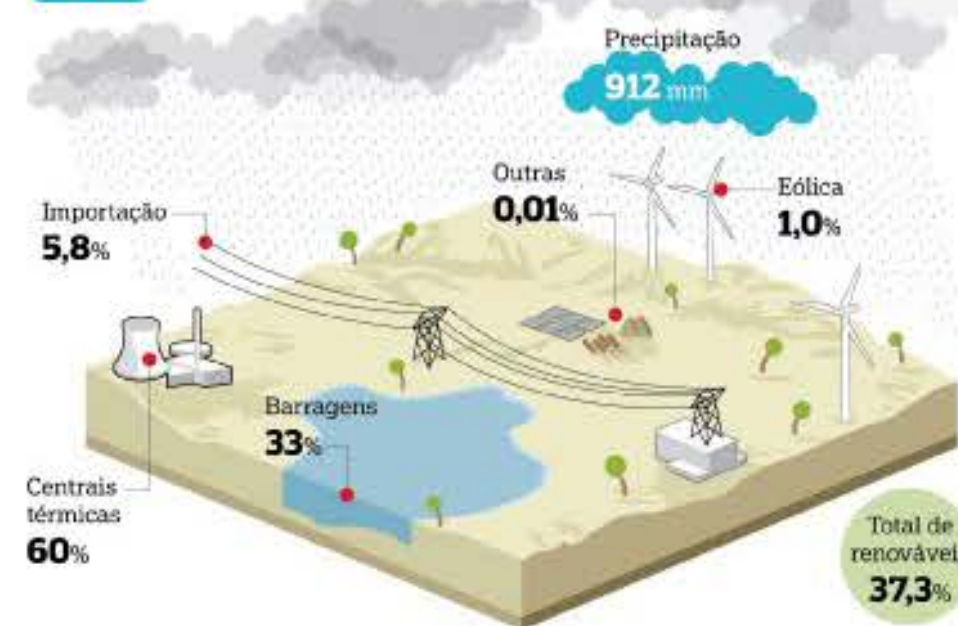
#### Evolução do consumo



#### O clima também pesa

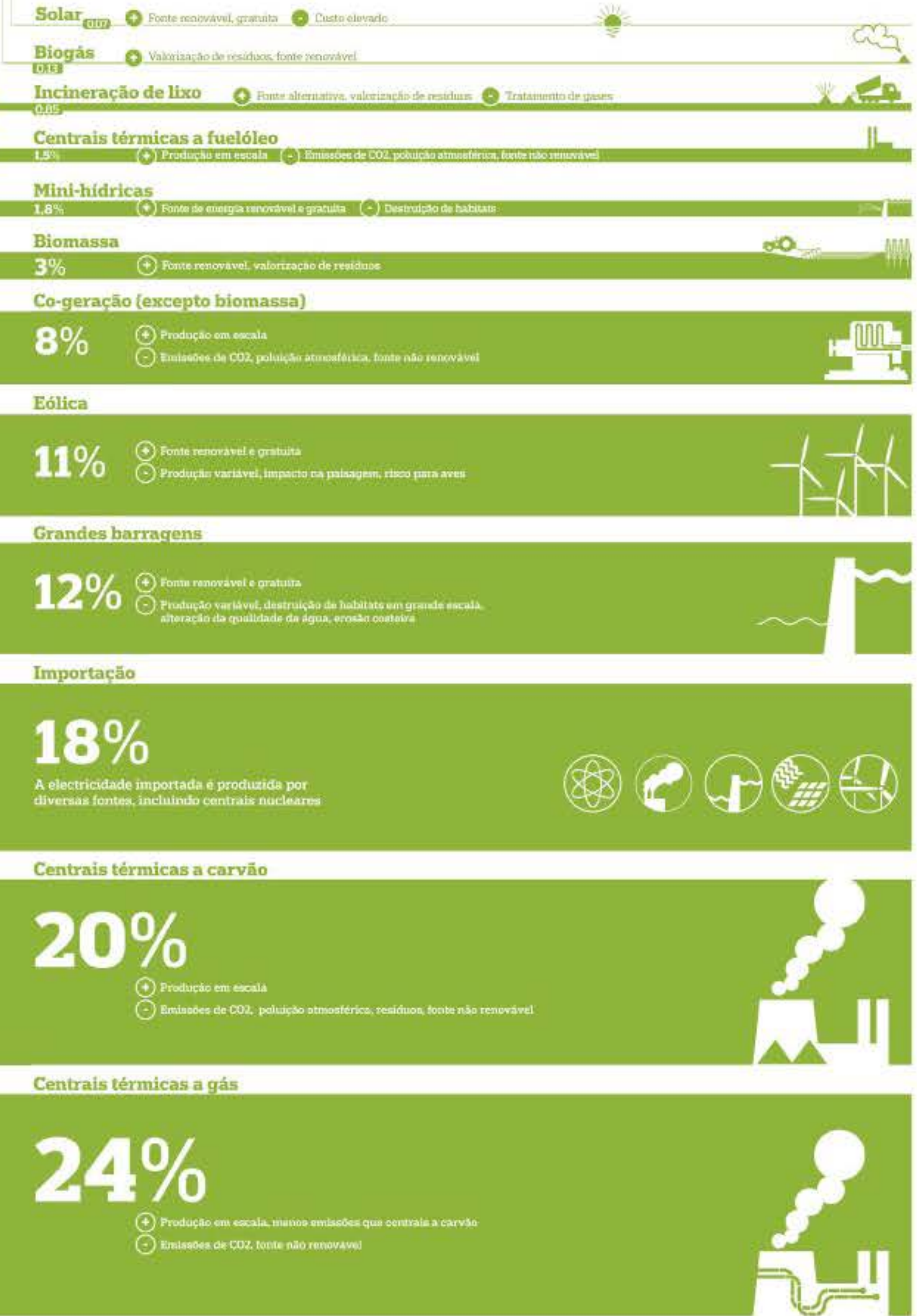
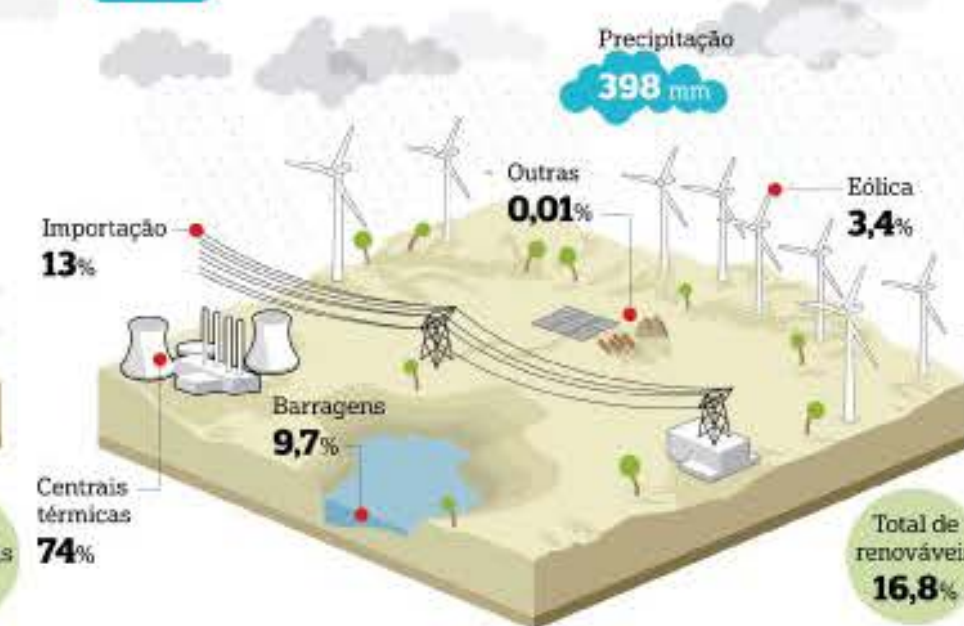
##### Ano com mais chuva

###### 2003



##### Ano com menos chuva

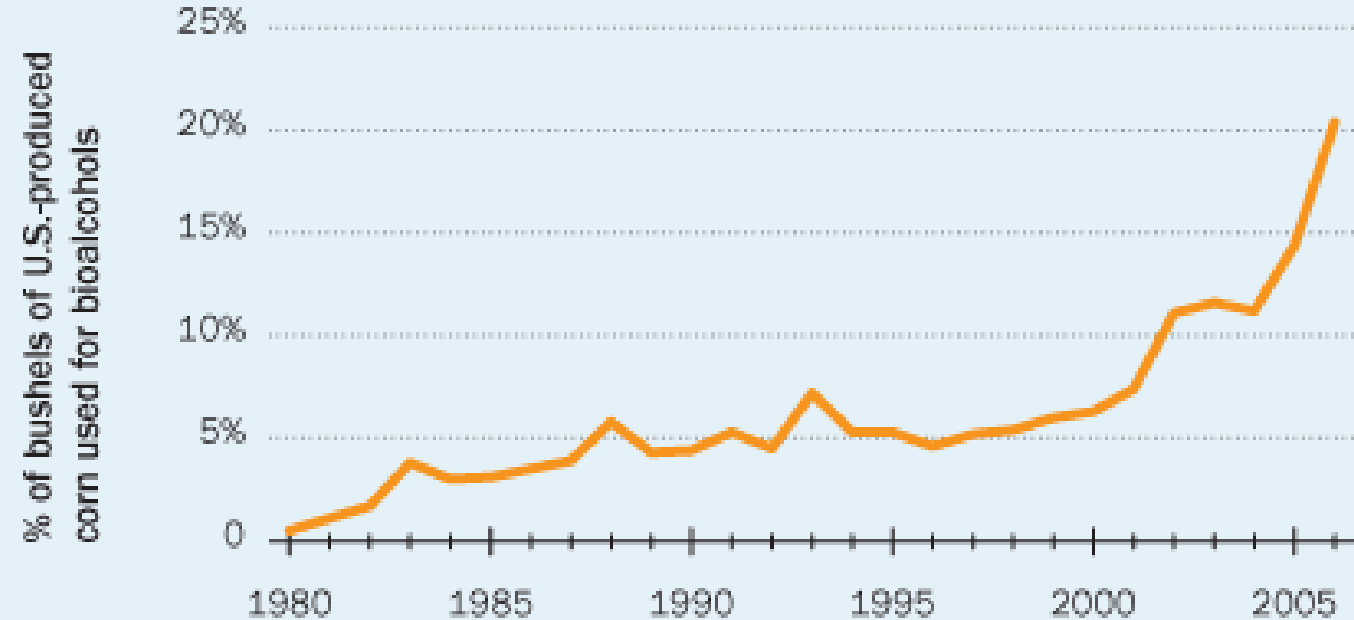
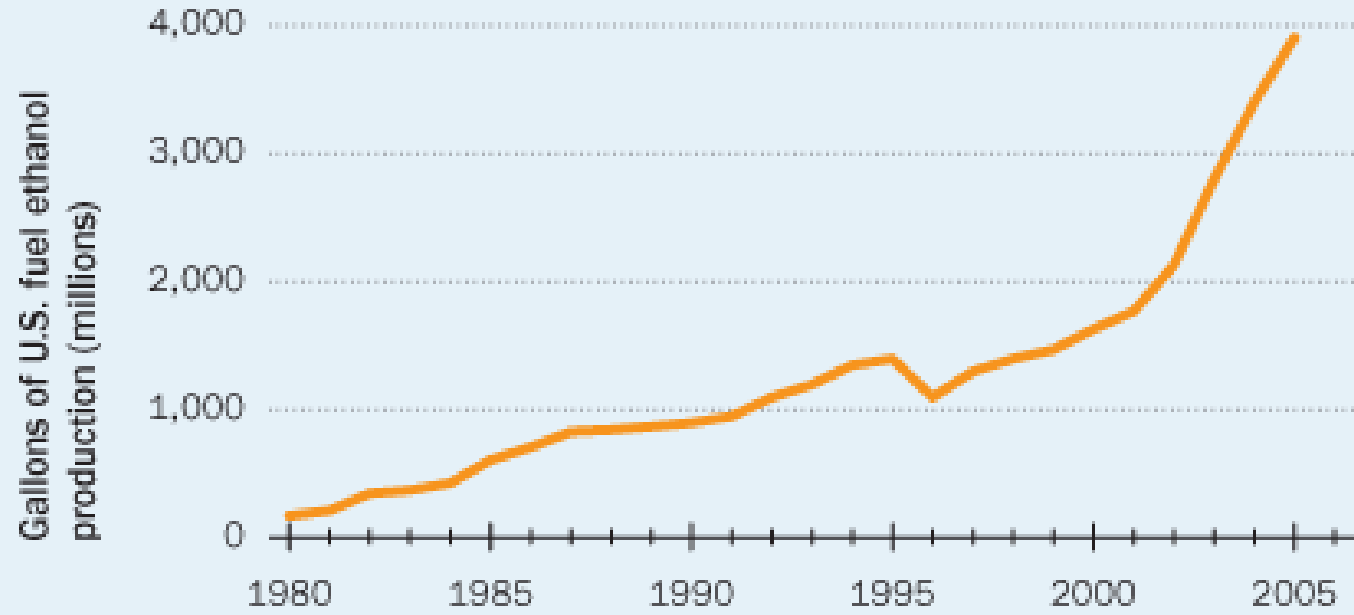
###### 2005



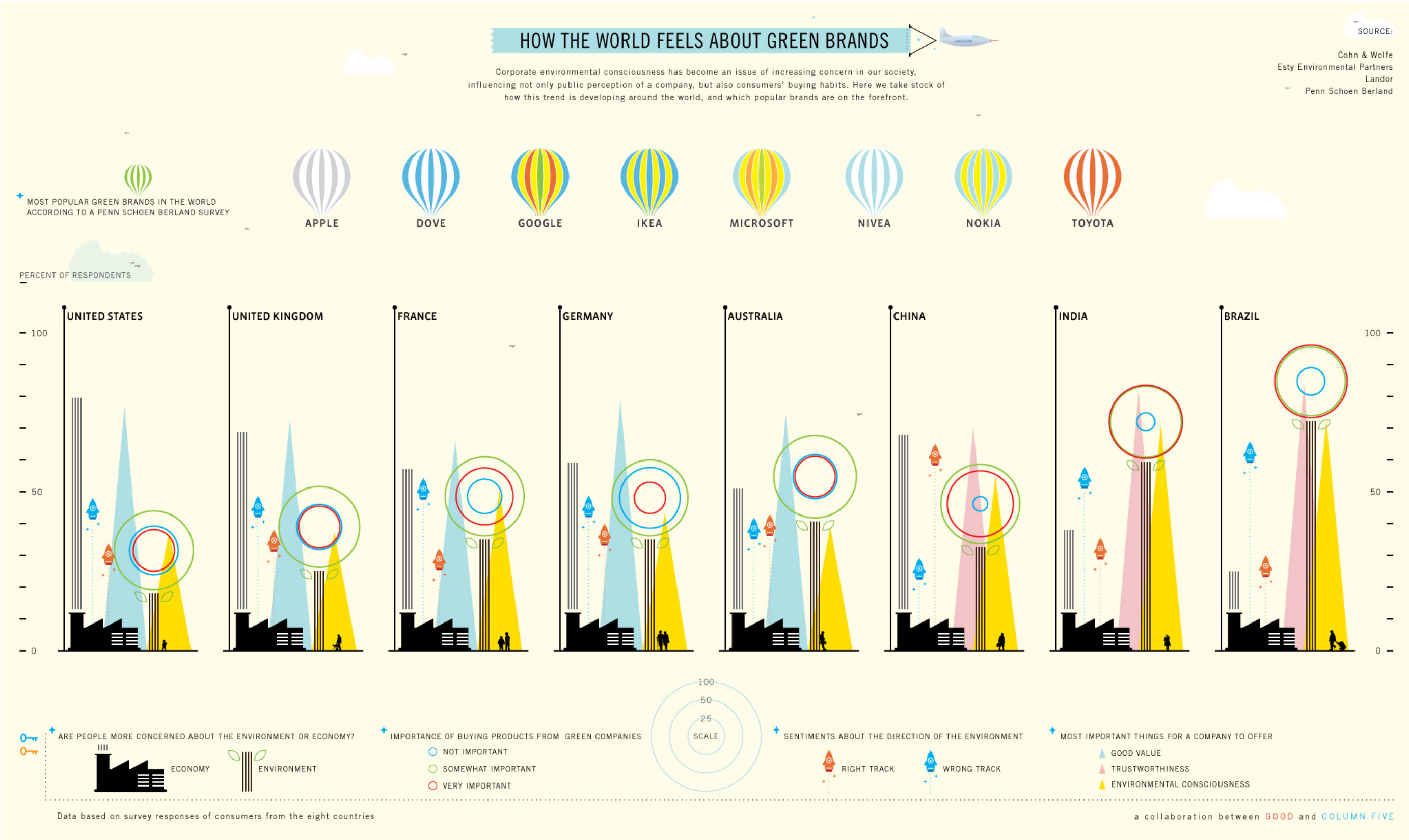
# Infographics

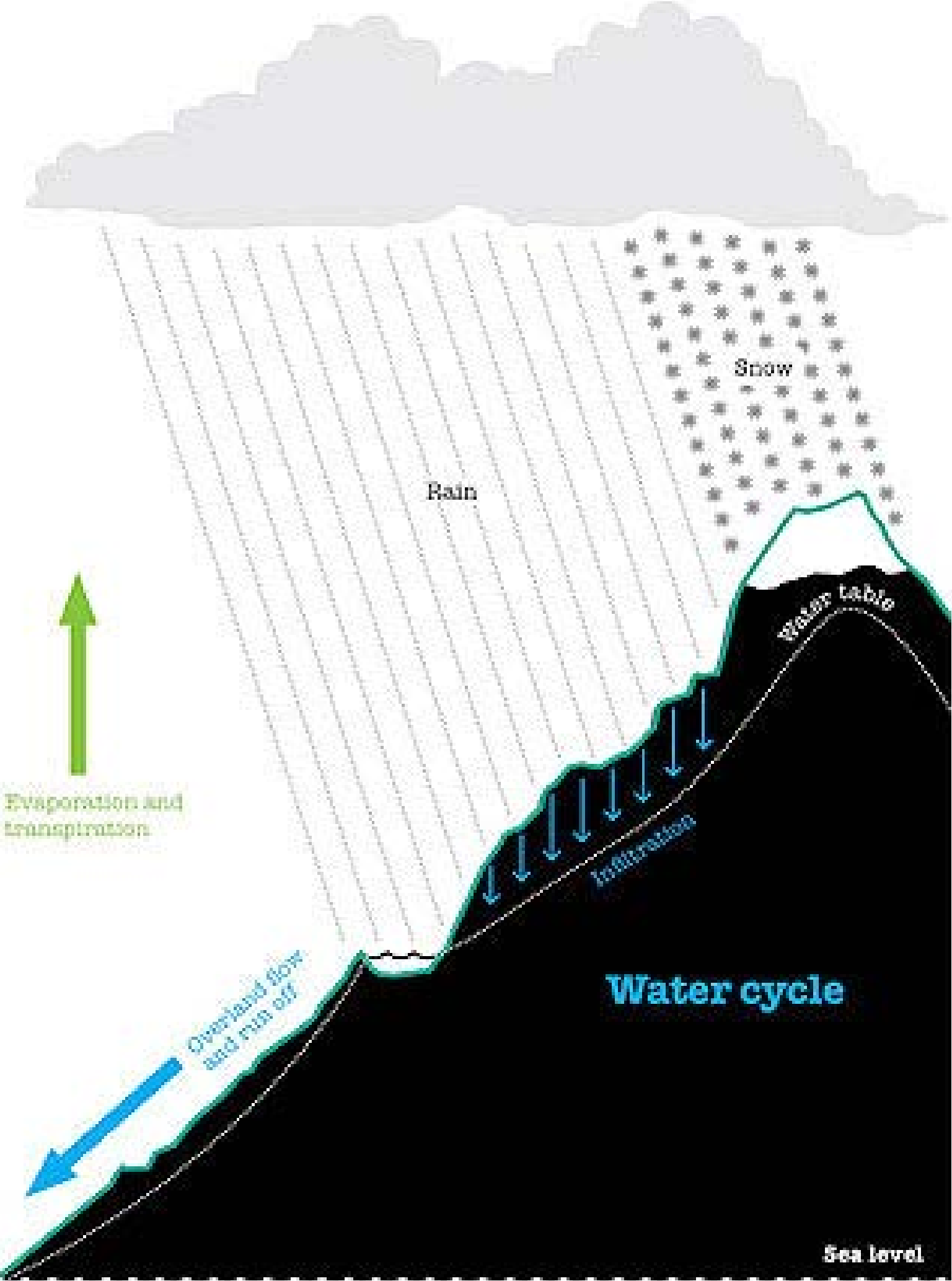
## More Corn Used for Biofuels

The more the U.S. turns to alternative fuel production, the greater the percentage of corn bushels used for fuel bioalcohols, such as ethanol.



SOURCE: USDA, Economic Research Service, Feed Grains Database; Renewable Fuels Association.





# Case study

## Graphic design style

MASARYK UNIVERSITY

**EACirc**

Using genetics to improve encryption

Martin Ukrop, Petr Švenda, Marek Sýs, Václav Matyáš et alii

fork me on github! [github.com/crocs-muni/eacirc](https://github.com/crocs-muni/eacirc)

### Problem statement

**Randomness testing**

The ciphertext produced by encryption should be completely indistinguishable from random data. But how to compare?

EACirc is a framework for designing a distinguisher – a simple program that decides whether generated ciphertext looks random enough.

**Iterative design**

The designed distinguisher is in the form of a gate circuit (layers of simple interconnected functions). It processes binary data and outputs a randomness verdict. It is improved iteratively, using ideas from evolutionary algorithms (see the next section for details).

### EACirc workflow

**1. Forming a population**

A set of currently considered partial solutions (gate circuits distinguishing cipher data from random data). The initial population is created randomly.

**2. Test vector generation**

Testing data for learning is sampled from both sources. That is, non-random data from the inspected cipher and random data from a truly random source.

**3. Fitness assessment**

Each circuit from the population is evaluated on all test vectors from the current set. Based on the outputs, it is assigned a fitness value from the interval [0,1].

**5. Mutation & crossover**

To form new individuals, we use mutation and crossover. Mutation makes small random changes in nodes and connectors. Crossover creates an offspring by combining different parts from two circuits taken from the population.

**4. Survival of the fittest**

Unfit individuals are discarded, better ones survive to the next generation. The higher the fitness, the bigger is the chance of survival.

The evolution works as a heuristics looking for better individuals – gate circuits distinguishing random and non-random data with higher probability than random guessing.

### Comparison to existing tools

**EACirc vs statistical testing**

The standard way to assess randomness is to use batteries of statistical tests such as *NIST STS*, *Dieharder* or *TestU01*. We run them along with EACirc and compare the results.

To have a fine-grained comparison, we have analyzed 77 different functions (*eStream*, *SHA-3* and *CAESAR* candidates). For 2-round *Hermes* and 1-round *Fubuki* we confidently surpass *NIST STS*.

**Further information**

Interested in EACirc? See the papers referenced below or ask directly at the lab (CRoCS @ FI MU).

[1] Švenda, Ukrop, Matyáš. *Determining cryptographic distinguishers for eStream and SHA-3 candidate functions with evolutionary circuits*. In: E-Business and Telecommunications. Vol. 456 (SECRYPT 2013). Springer Berlin Heidelberg, 2014.

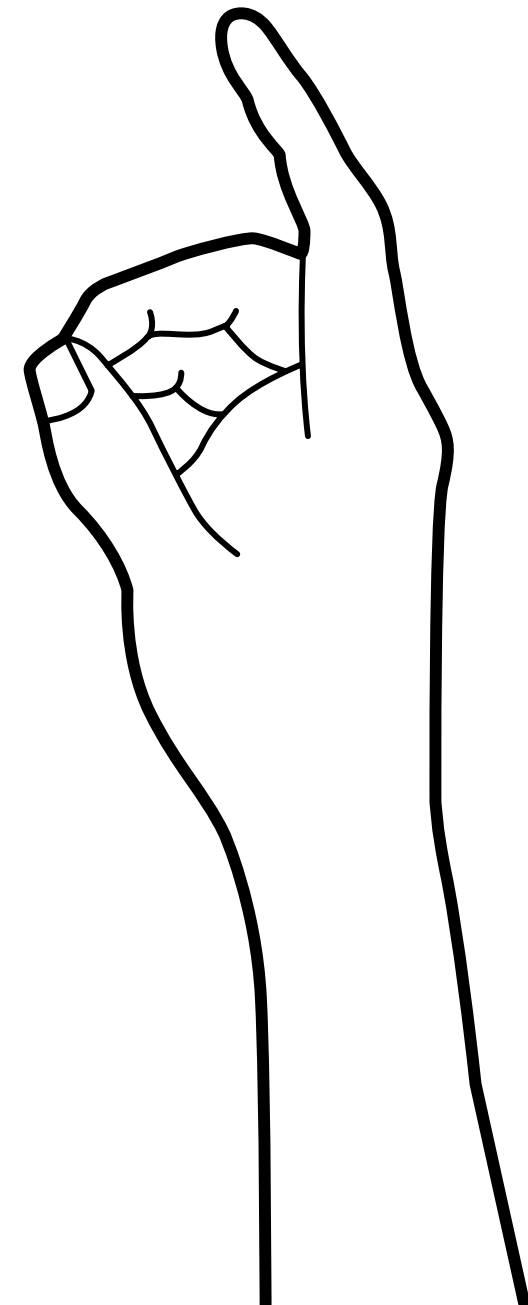
[2] Kubiček, Novotný, Švenda, Ukrop. *New results on reduced-round Tiny Encryption Algorithm using genetic programming*. IEEE Infocommunications. Vol. 8, iss. 1. 2016.

CRoCS Centre for Research on Cryptography and Security

This work was supported by the Czech Science Foundation project GAP202/11/0422.

Infographics enhance the design

● **Process of creating poster**

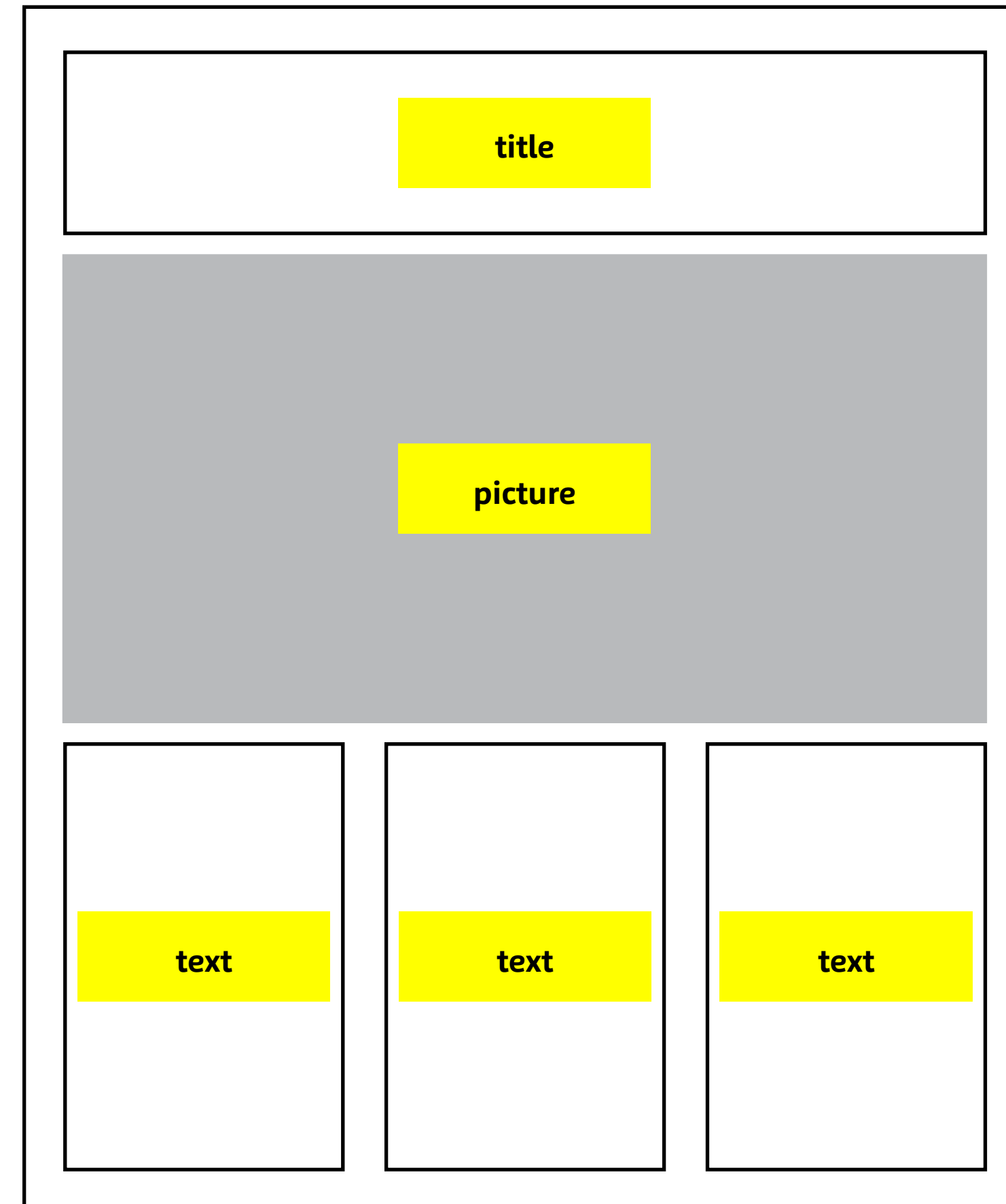
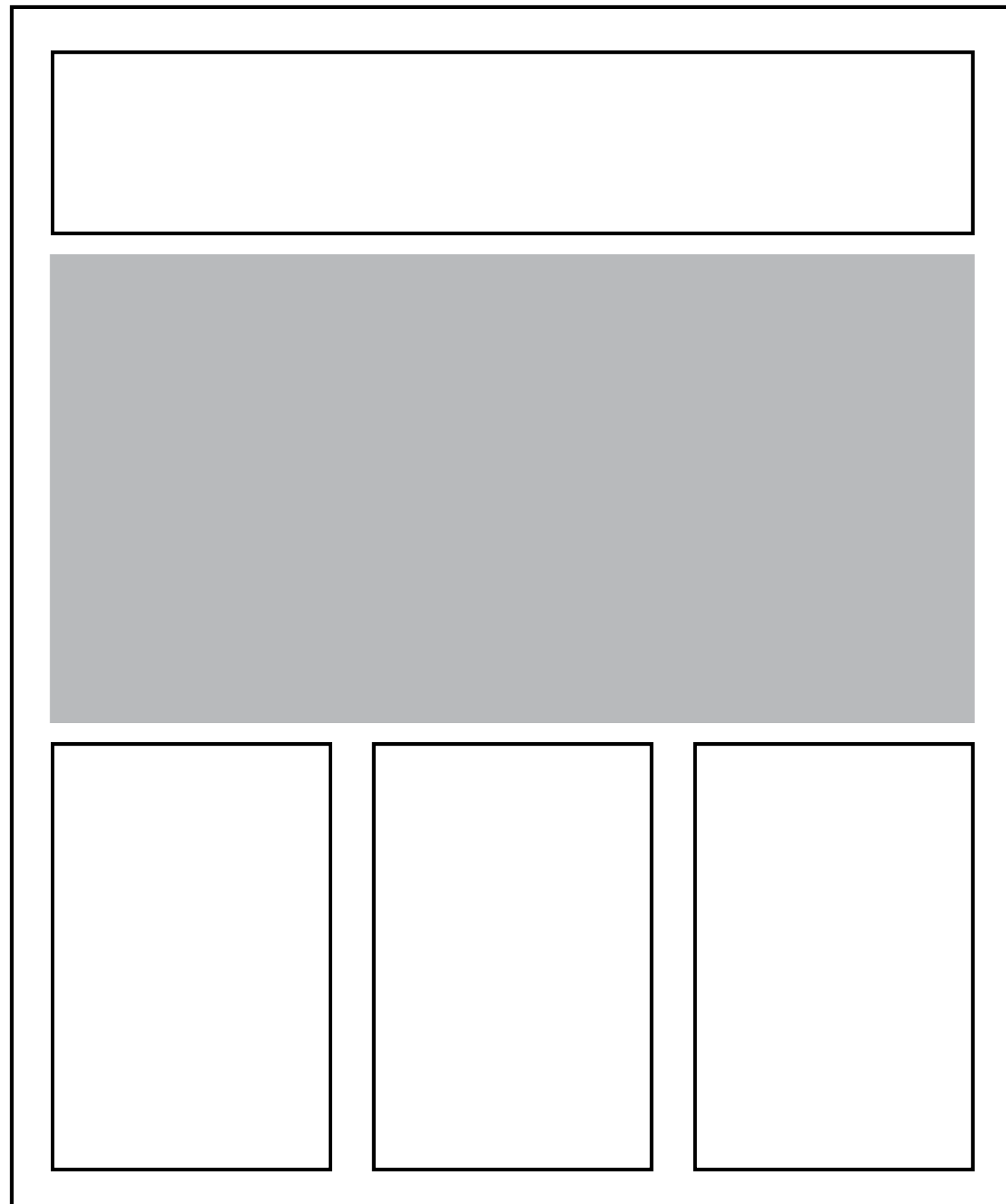


# Define a grid

Define a layout

Define a position of text and pictures

1



# Hierarchy of information

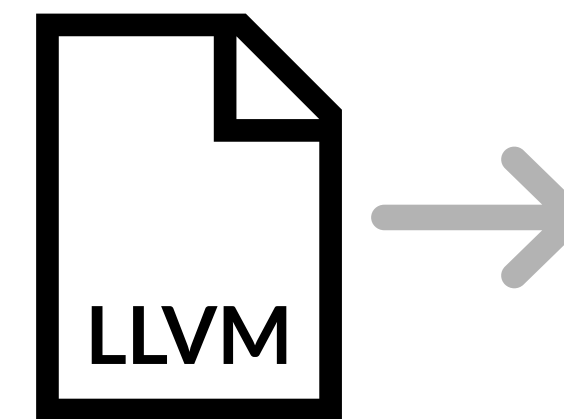
# 2

## Compose elements

Try to find balance between text and images

# DIVINE

**DIVINE** is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. **DIVINE** is rather efficient when dealing with programs without inputs (for example test cases).





## Typography

### 3

#### Choose typography

Find a way how to highlight the text – working with different styles (italic, bold,... )

## DIVINE

**DIVINE** is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. **DIVINE** is rather efficient when dealing with programs without inputs (for example test cases).

## DIVINE

DIVINE is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. DIVINE is rather efficient when dealing with programs without inputs (for example test cases).

## DIVINE

**DIVINE** is a tool for verification of parallel C++ programs. By using the LLVM compilation framework with the Clang compiler and the libc++ library it provides support for most of the standard C++ library and all the C++ language features. **DIVINE** is rather efficient when dealing with programs without inputs (for example test cases).

A electricidade em Portugal

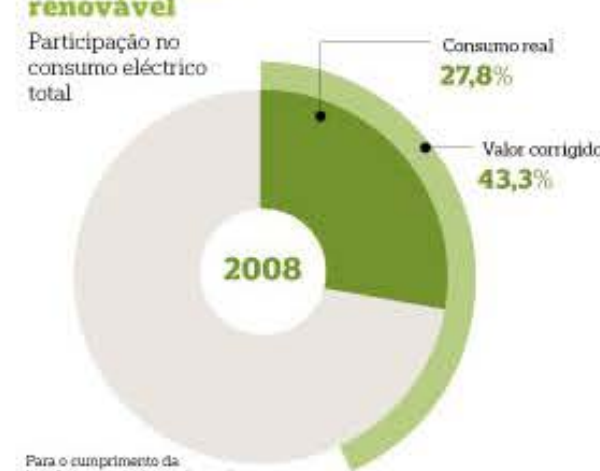
## De onde vem a nossa luz?

A electricidade que chega às nossas casas vem de um complexo cabaz de fontes energéticas, que varia conforme o ano. Em 2008, houve muita importação e pouca produção hidroelétrica. Mas a energia do vento já começa a ter um peso significativo

Ricardo Garcia (texto) e Joaquim Guerreiro (infografia)

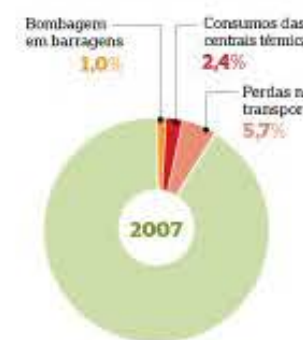
As renováveis estão a avançar, mas Portugal ainda depende muito das poluentes centrais térmicas para produzir a electricidade de que necessita. Em 2008, as termoelétricas asseguraram quase metade do consumo nacional. Se tudo ainda fosse como há duas décadas, no entanto, seria pior. Não havia ainda centrais a gás natural e o país dependia fortemente do carvão, que polui muito mais. Em anos secos, o país não tinha alternativa de fontes renováveis de electricidade, dado que a única opção realmente importante eram as barragens. Hoje, o cabaz de fontes energéticas para a produção eléctrica é muito mais variado. O vento, no ano passado, forneceu quase tanta energia quanto as barragens, reduzindo o peso das centrais térmicas. O que os dados aqui coligidos pelo PHLJO mostram é que, salvo as eólicas, as chamadas "novas" renováveis contribuem ainda apenas marginalmente para o bolo nacional independentemente da relevância que o discurso político lhes dá. A produção eléctrica a partir de painéis solares fotovoltaicos, por exemplo, entra com uma fatia inferior a um por cento. A parcela mais oculta da nossa electricidade é aquela que é importada de outros países. As necessidades de importação variam ano a ano, conforme o clima e os preços dos combustíveis. No ano passado, a factura foi elevada: Portugal importou 18 por cento da electricidade que consumiu. A energia veio de vizinhos, como Espanha, que tem outro cabaz energético, onde estão incluídas oito centrais atómicas. Para muitos, esta realidade conduz a uma conclusão incómoda: quando ou não, os portugueses consomem energia nuclear.

### Electricidade renovável



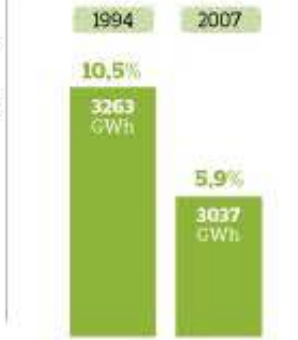
Para o cumprimento da legislação europeia, o valor real é corrigido com base no índice de produtividade hidroelétrica de cada ano

### O que não chega aos consumidores



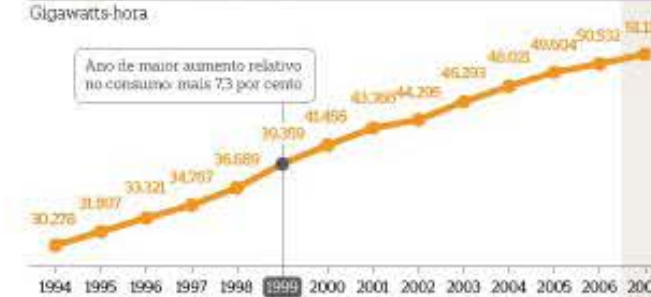
### Perdas do total produzido

Diferença entre 1994 e 2007



### Evolução do consumo

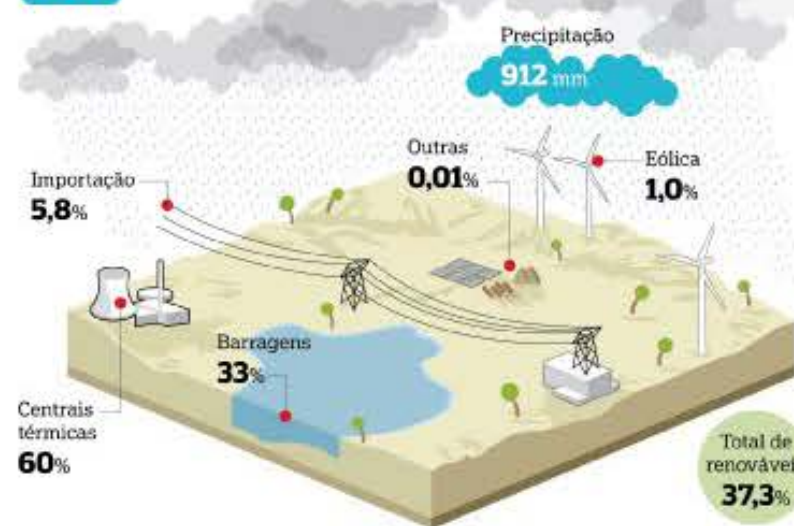
Gigawatts-hora



### O clima também pesa

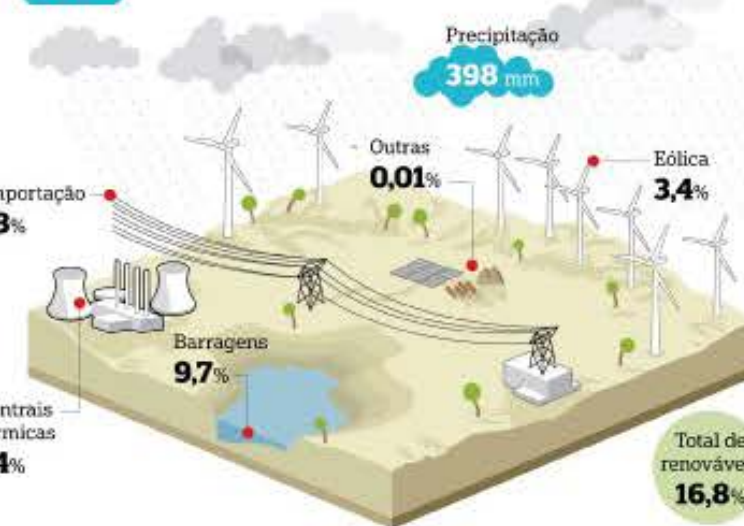
#### Ano com mais chuva

2003

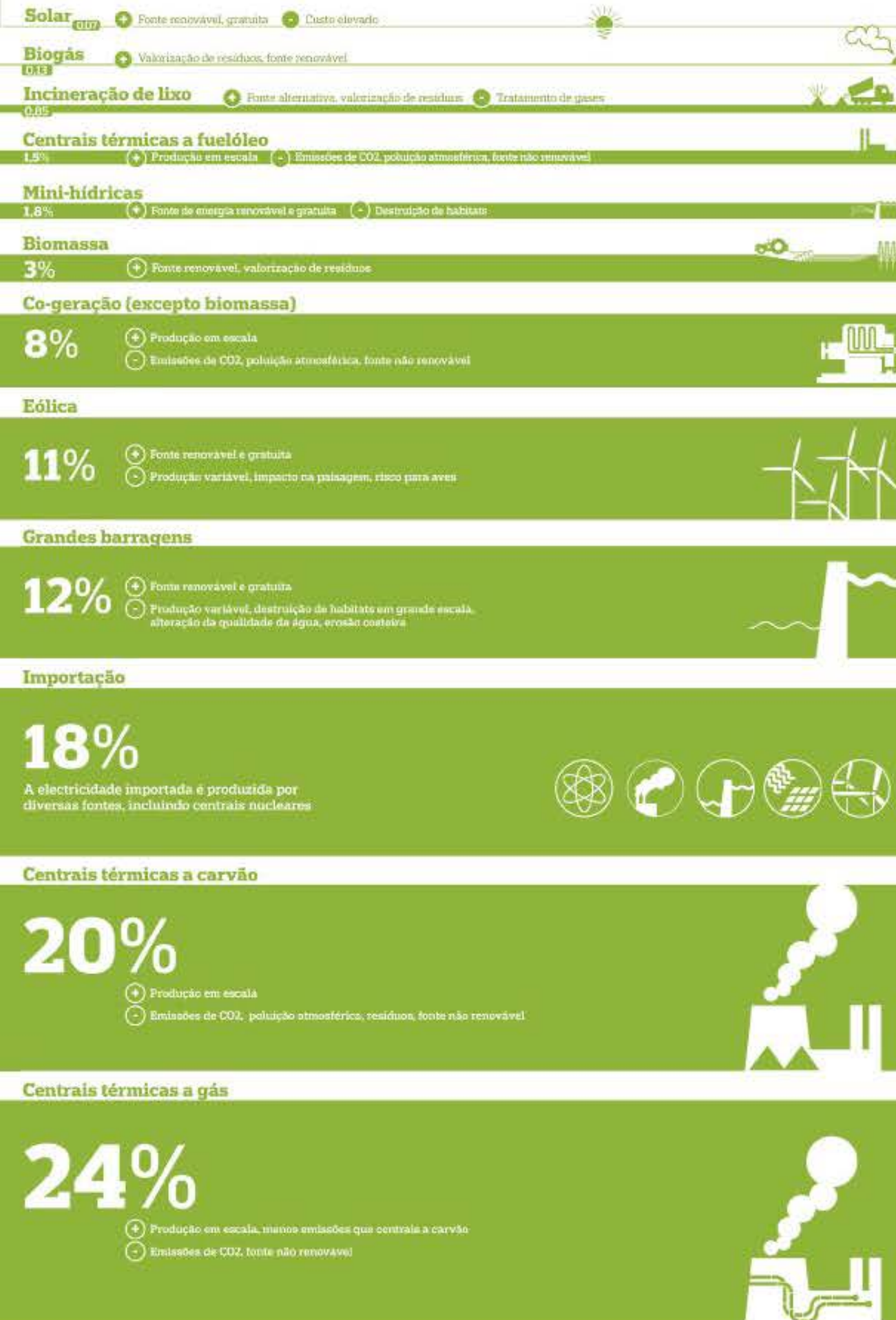


#### Ano com menos chuva

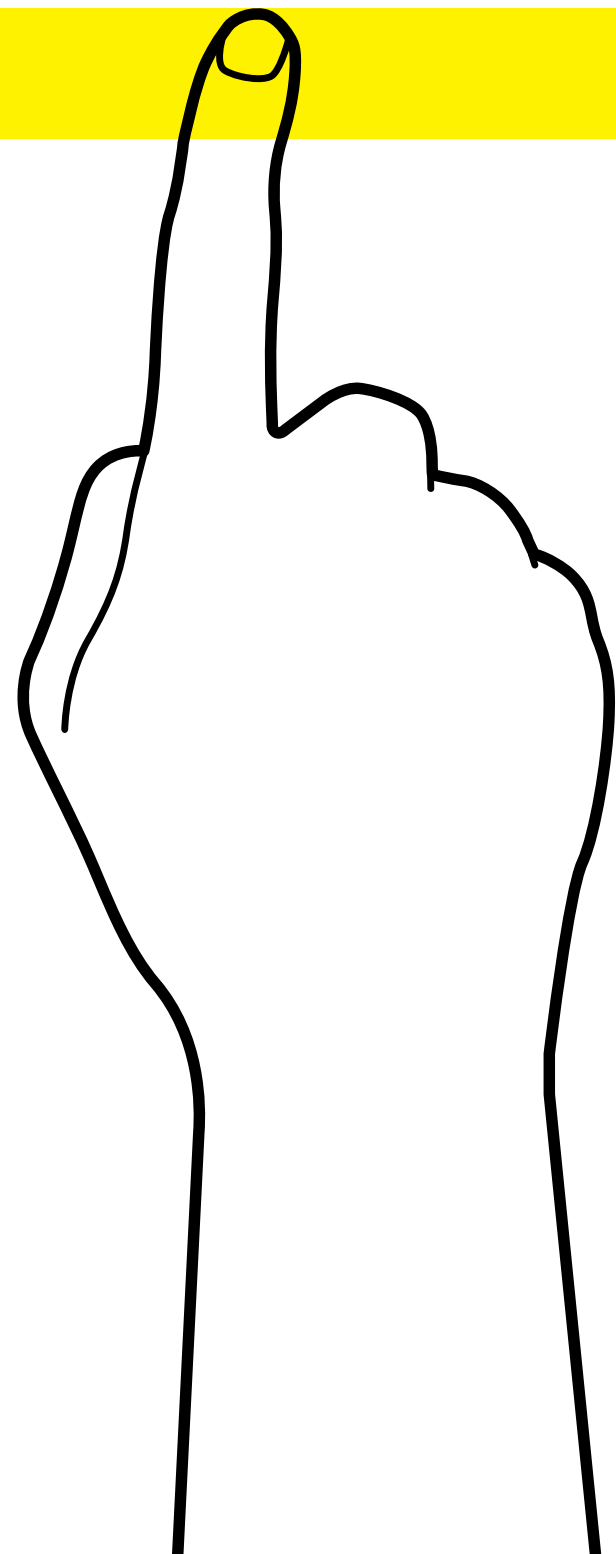
2005



FORNTE: Direcção-Geral de Energia e Geologia; REN; Instituto de Meteorologia; Instituto da Água



# How Visual Weight and Direction Impact Design



## **Balance**

Your composition needs to be in balance, whether symmetrical, asymmetrical, or radial. You'll achieve this balance by placing elements of combined equal visual weight on either side of the optical center

## **Dominance/Focal Points**

Focal points are elements that attract the eye. They're elements of greater visual weight. The dominant element of a design is the element with the greatest visual weight.

## **Flow**

Through focal points, hierarchy, and visual direction you can lead the eye from one part of your design to the next. You'll create a flow through your design.

## **Scale**

Is generally considered to be the relative size of different objects. Here we can consider it in the context of the relative visual weight of different objects.

## **Depth**

Elements with greater visual weight appear to move forward in a design while visually lighter elements recede into the background. We can use this understanding to create depth in a design.

## **Proportion**

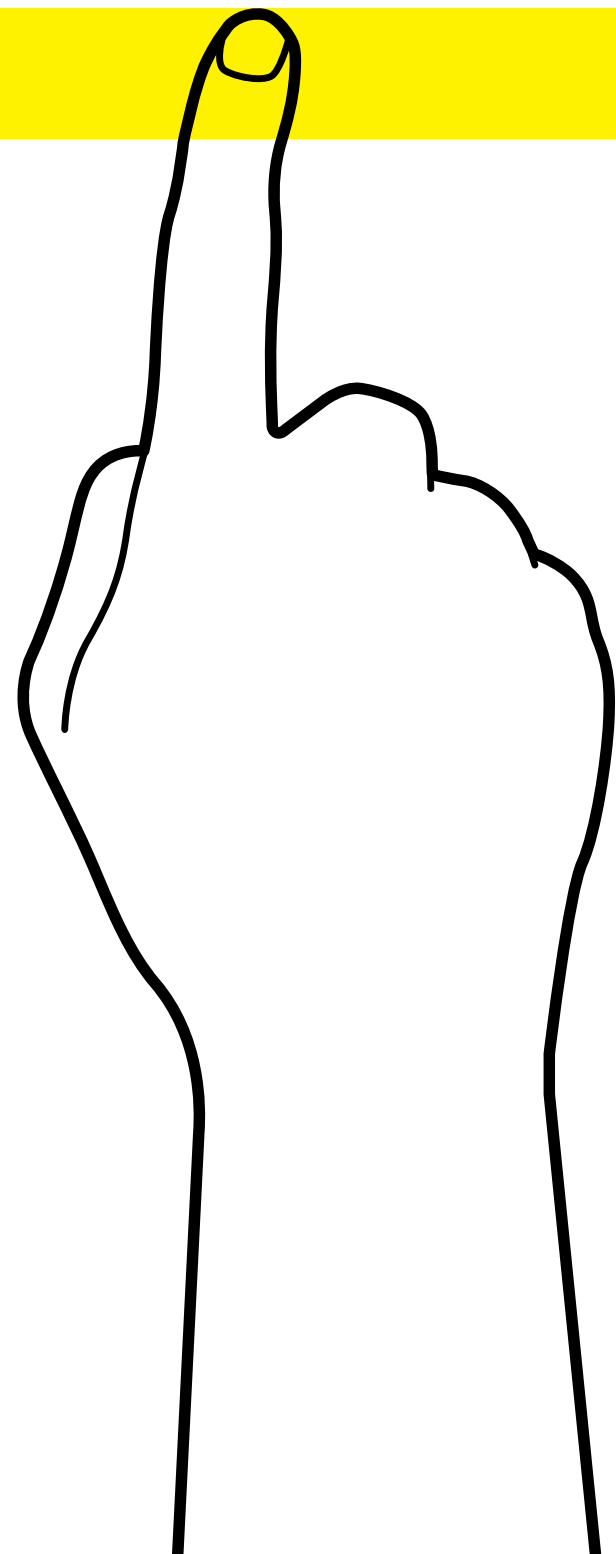
Is the relationship in scale between elements. Different proportions in a composition relate to different kinds of balance and can help establish visual weight and depth.

## **Hierarchy**

By creating a scale of focal points or elements of different visual weights you can create a hierarchy of design elements. The difference in visual weights is what makes certain elements stand out improving scanability.

# Case study

## POSTERS



# Case study

## Posters

### Ultrasound Painting of Vascular Tree

Åsmund Birkeland and Ivan Viola  
University of Bergen

#### Ultrasound Painting

- Segmentation of medical data can be slow and cumbersome and are rarely used by doctors
- Ultrasound Painting utilize the examiners natural interaction to extract hypo-echoic regions, such as blood-vessels, live during examination.
- The examiner starts with inserting an initial seed-point in a cross-section of a blood-vessel in the ultrasound image.
- The cross-section of the vessel is extracted and the vessel is tracked to the following time-frame.
- The outline of the cross-section is put into a 3D point cloud which is triangulated live, providing instant feed-back to the examiner.

#### Vessel Tracking

- Due to the high frame-rate of ultrasound, the vessel is assumed to overlap from frame to frame.
- A new seed-point is calculated at the center current cross-section and used as an educated guess of where the vessel will be in the next frame.
- To detect branching, we calculated additional seed-points in outer edge of the cross-section. Branching occurs at the end-points to the "skeleton" of a cross-section.
- A regular distribution of points on the outline is added into a 3D point-cloud and the center-seed point is added into a center-line tree.

#### Point Cloud Processing

- Local triangulation of recently added points reduce overhead and enable live triangulation.
- Voronoi triangulation based on point normal and the local neighborhood
- Point-normals are estimated using local neighborhood evaluation.

MEDVIZ FROM VISION TO DECISION UNIVERSITY OF BERGEN ILLUSTRASOUND

### VisBio

September 19, 2013  
VilVite Bergen Science Center  
Auditorium / Free Admission

#### Visualization & Biology: Challenges and Perspectives

#### Program Highlights

The rapid growth in volume, complexity, and diversity of biological data represents an increasing challenge for researchers in many areas. The aim of this workshop is to bring together experts from biology, bioinformatics, and visualization to develop a joint understanding of the key technologies, obstacles, and opportunities involved in generating insight from these large and highly complex data sets.

**08:45 Opening**

**09:00 Ines Heiland**  
University in Tromsø

**Metabolic modelling: From networks to dynamics and back**

**10:45 Jan Aerts**  
University of Leuven

**Visual analytics in omics: Why, what and how?**

**13:15 Jan G. Bjålie**  
University of Oslo

**Digital brain atlasing: 3-D "Google maps" of the brain**

**15:15 Ewan Birney**  
European Bioinformatics Institute  
**Horizon Lecture**

**Understanding basic biology using outbred genetics**

**16:45 Panel Discussion**

#### Additional Speakers

**Pina Kingman**  
University of Bergen

**Ivan Kolesar**  
University of Bergen

**Mathieu Le Muzic**  
Vienna University of Technology

**Július Parulek**  
University of Bergen

**Ivan Viola**  
Vienna University of Technology

<http://www.iu.uib.no/vis/events/VisBio13/>  
Contact: Stefan Bruckner (stefan.bruckner@uib.no)  
Department of Informatics - University of Bergen

UNIVERSITY OF BERGEN

### Physiollustration Research Project

Ivan Viola  
University of Bergen

#### 1 Illustrative Visualization

computer supported interactive and expressive visualization of complex data through abstractions from traditional illustrations

acquisition reconstruction segmentation visualization

interactive cut-aways stylized ghosting chromatic shadows selective visualization

#### 2 Structure versus Process

While structural visualization usually communicates spatially relevant information, such as shapes, distances, or neighborhood information, visualization of process is often abstracted into time-concentration curves.

None of them alone comprehensively communicate how things work!

chaperonin structure enzymatic concentration interactions

#### 3 New Multi-Scale Visualization Pipeline

The visualization metaphors investigated are inspired by textbook illustrations and handcrafted animated illustrations. The visualization technology will be developed and evaluated on multiple scale levels, from molecular machines, up to the organ level.

The primary focus of this research project is on development of:

- novel graphics data representations
- integration of physiological models
- visual representations
- occlusion handling
- visual guidance and storytelling
- zooming
- interaction

models geometry visual abstractions

#### 4 Staff to Hire

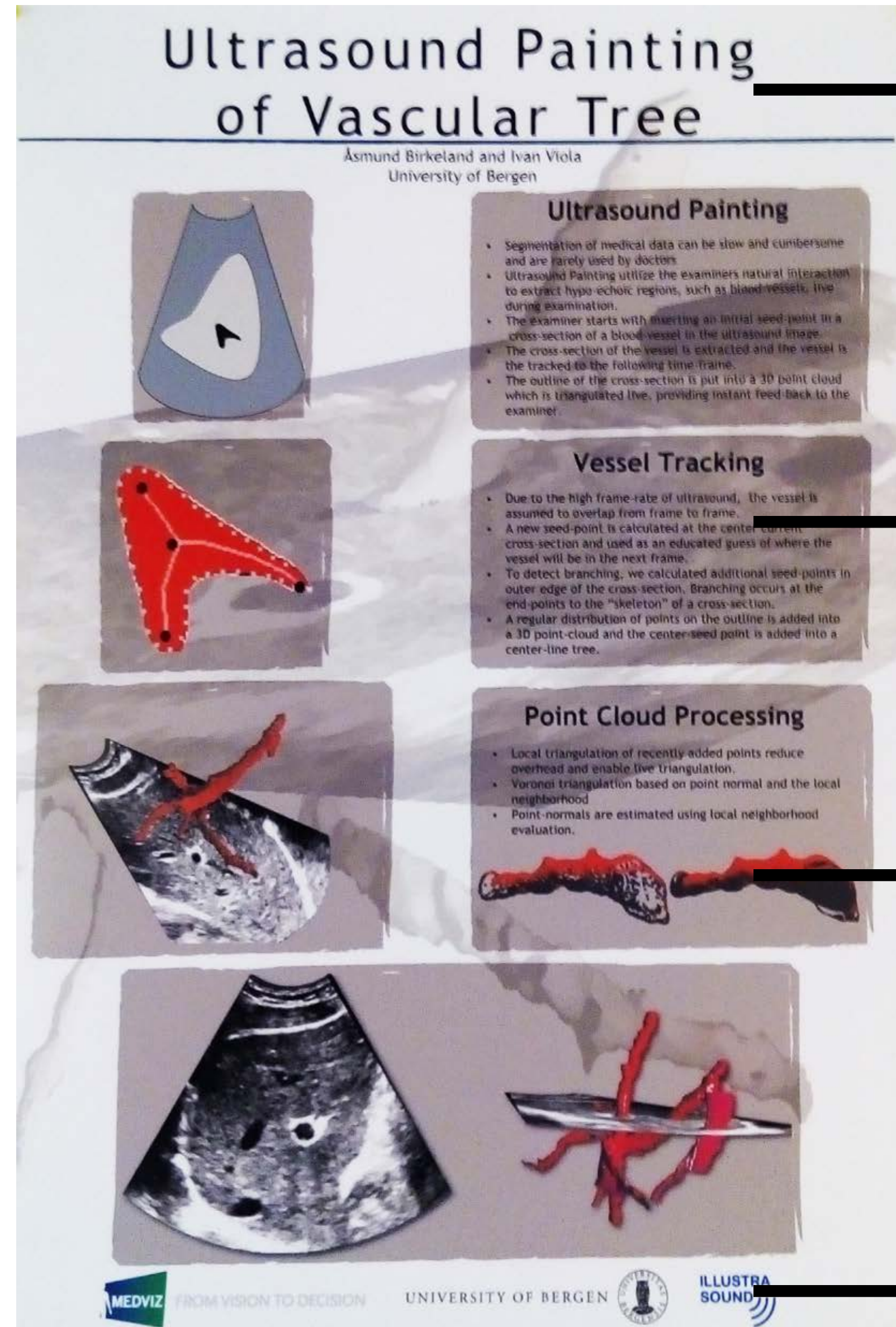
To develop illustrative visualization technology that communicates how physiological processes work, we want to build-up a unique interdisciplinary team consisting of:

- Visualization researcher
- computational biology researcher
- scientific illustrator or a 3D animator

#### 5 What is Next?

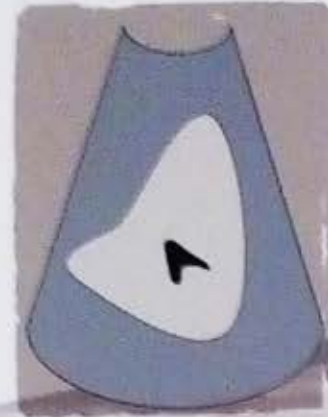
Join the team or stay tuned!

UNIVERSITY OF BERGEN



# Ultrasound Painting of Vascular Tree

Asmund Birkeland and Ivan Viola  
University of Bergen



## Ultrasound Painting

- Segmentation of medical data can be slow and cumbersome and are rarely used by doctors.
- Ultrasound Painting utilize the examiners natural interaction to extract hypo-echoic regions, such as blood vessels, live during examination.
- The examiner starts with inserting an initial seed-point in a cross-section of a blood-vessel in the ultrasound image.
- The cross-section of the vessel is extracted and the vessel is tracked to the following time-frame.
- The outline of the cross-section is put into a 3D point cloud which is triangulated live, providing instant feed-back to the examiner.



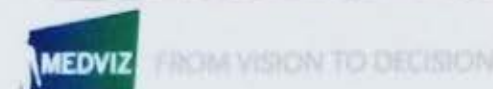
## Vessel Tracking

- Due to the high frame-rate of ultrasound, the vessel is assumed to overlap from frame to frame.
- A new seed-point is calculated at the center-current cross-section and used as an educated guess of where the vessel will be in the next frame.
- To detect branching, we calculated additional seed-points in outer edge of the cross-section. Branching occurs at the end-points to the "skeleton" of a cross-section.
- A regular distribution of points on the outline is added into a 3D point-cloud and the center-seed point is added into a center-line tree.



## Point Cloud Processing

- Local triangulation of recently-added points reduce overhead and enable live triangulation.
- Voronoi triangulation based on point normal and the local neighborhood.
- Point-normals are estimated using local neighborhood evaluation.



UNIVERSITY OF BERGEN



text - title

text

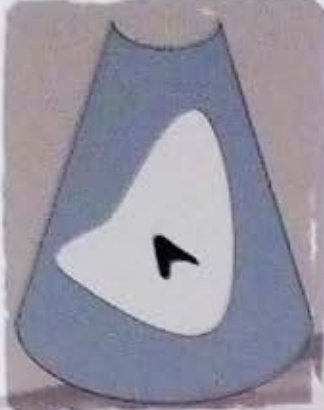
images

logos



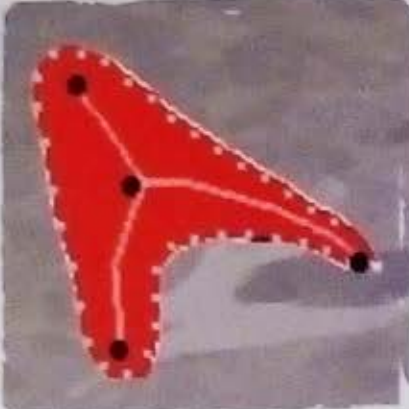
# Ultrasound Painting of Vascular Tree

Åsmund Birkeland and Ivan Viola  
University of Bergen




### Ultrasound Painting

- Segmentation of medical data can be slow and cumbersome and are rarely used by doctors.
- Ultrasound Painting utilize the examiners natural interaction to extract hypo-echoic regions, such as blood-vessels, live during examination.
- The examiner starts with inserting an initial seed-point in a cross-section of a blood-vessel in the ultrasound image.
- The cross-section of the vessel is extracted and the vessel is tracked to the following time-frame.
- The outline of the cross-section is put into a 3D point-cloud which is triangulated live, providing instant feedback to the examiner.





### Vessel Tracking

- Due to the high frame-rate of ultrasound, the vessel is assumed to overlap from frame to frame.
- A new seed-point is calculated at the center current cross-section and used as an educated guess of where the vessel will be in the next frame.
- To detect branching, we calculated additional seed-points in outer edge of the cross-section. Branching occurs at the end-points to the "skeleton" of a cross-section.
- A regular distribution of points on the outline is added into a 3D point-cloud and the center-**seed** point is added into a center-line tree.

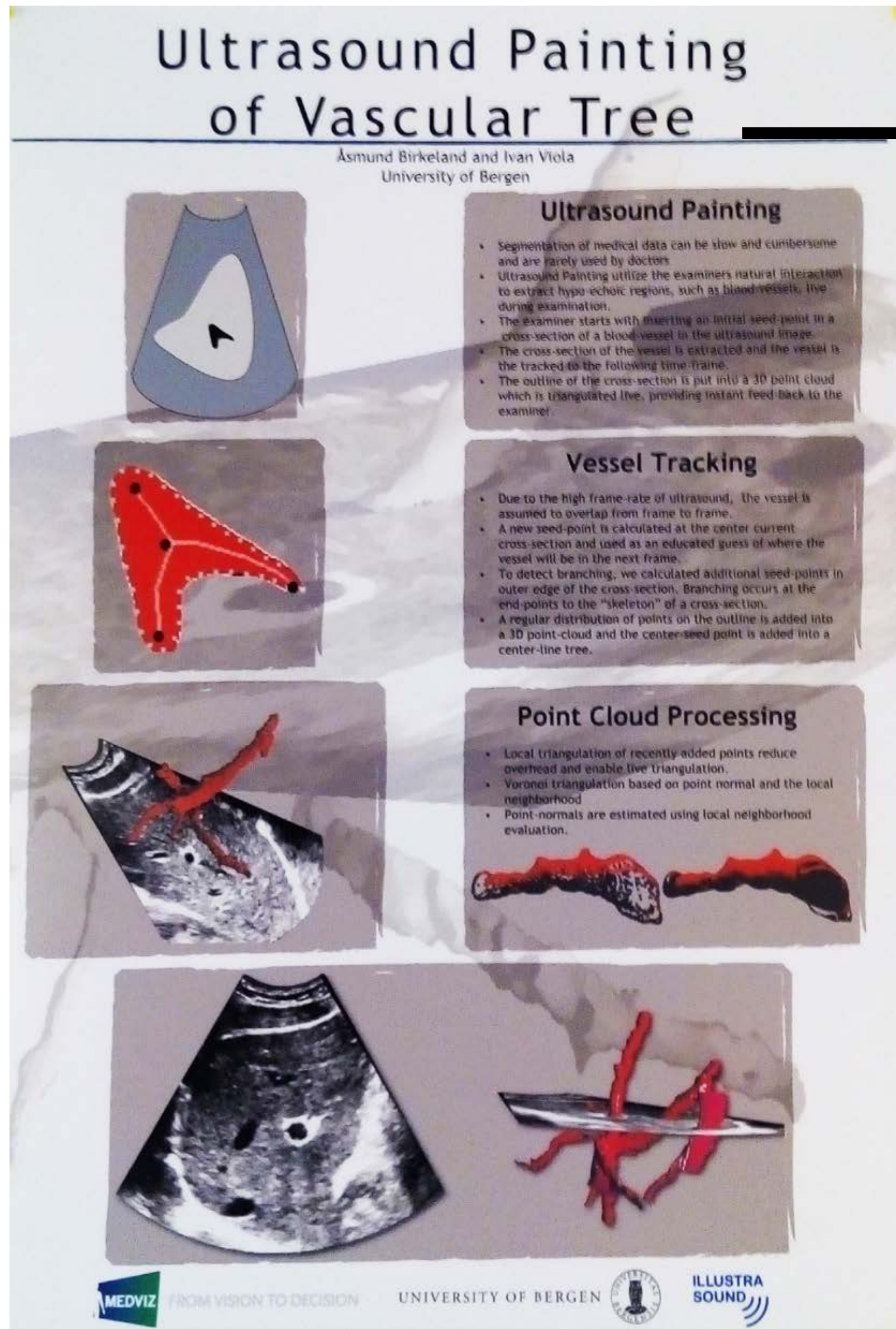


### Point Cloud Processing

- Local triangulation of recently added points reduce overhead and enable live triangulation.
- Voronoi triangulation based on point normal and the local neighborhood.
- Point-normals are estimated using local neighborhood evaluation.



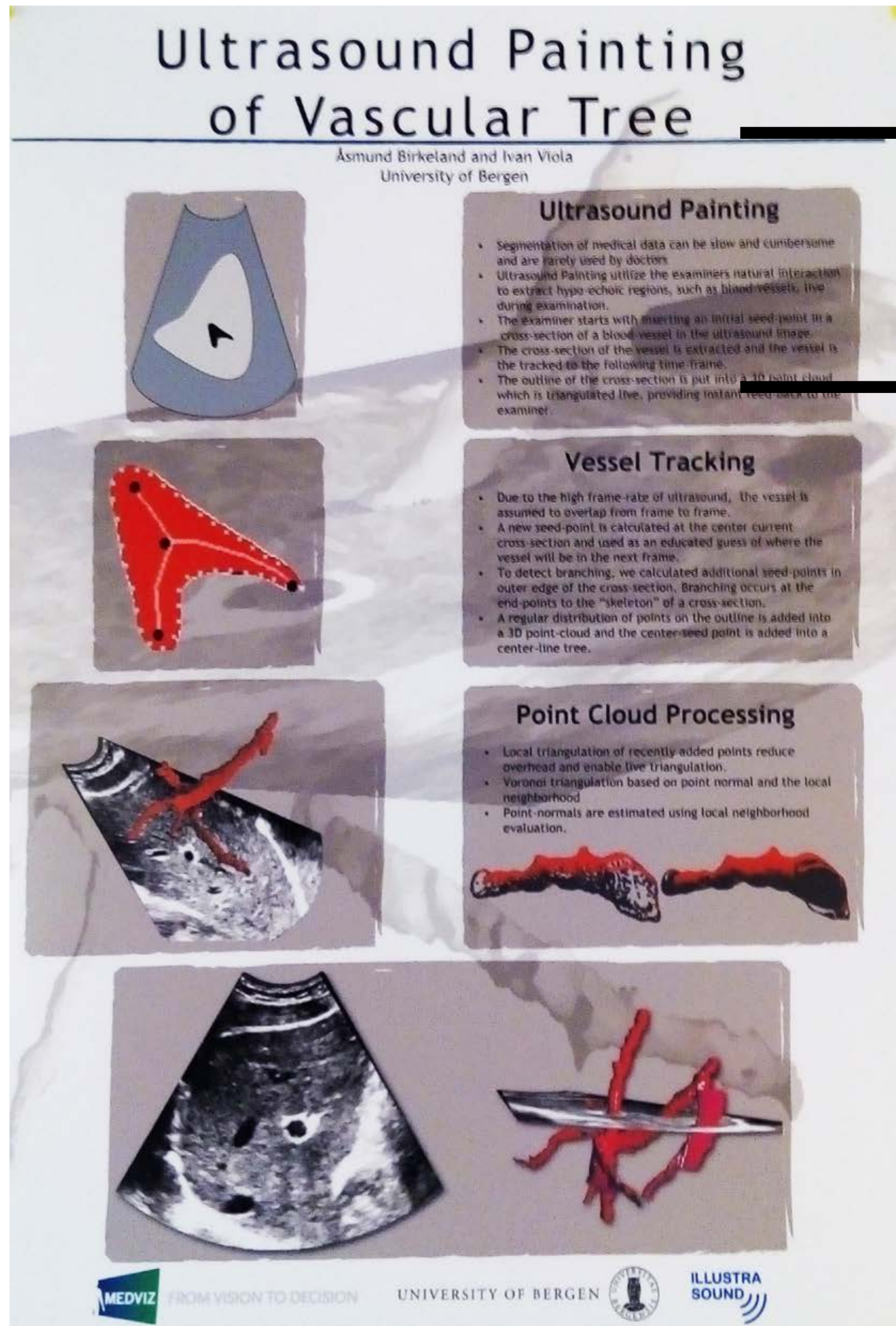
MEDVIZ FROM VISION TO DECISION UNIVERSITY OF BERGEN ILLUSTRA SOUND



more space between  
elements



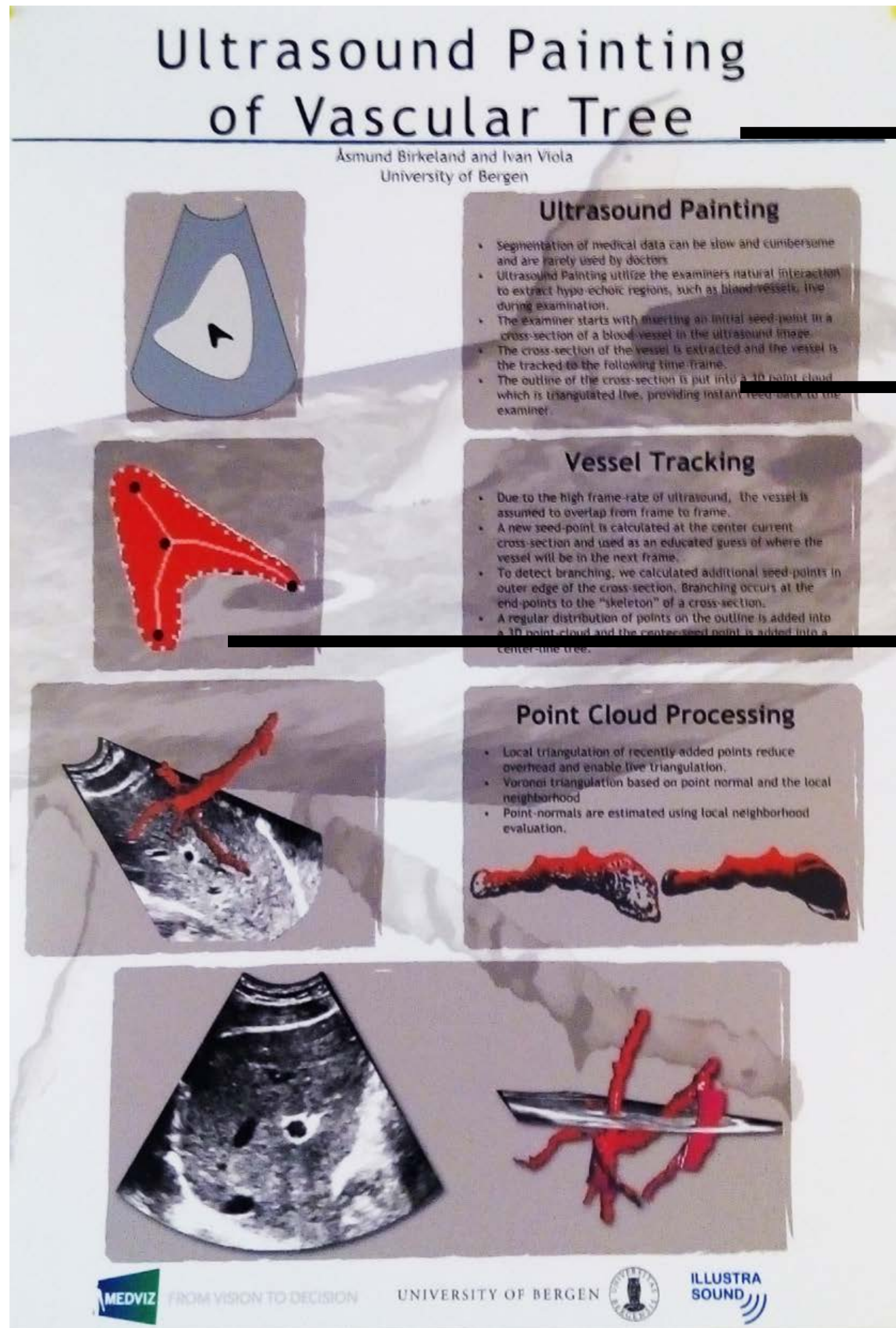
Suggestions



more space between  
elements



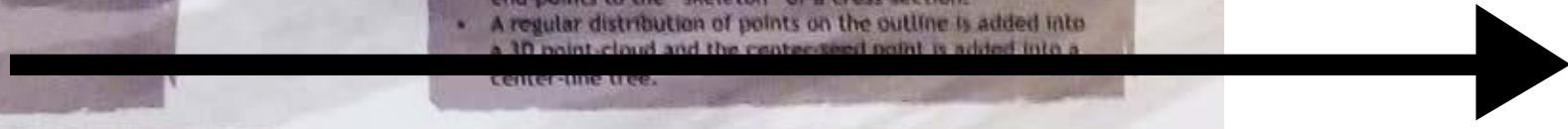
background photo  
makes text illegible



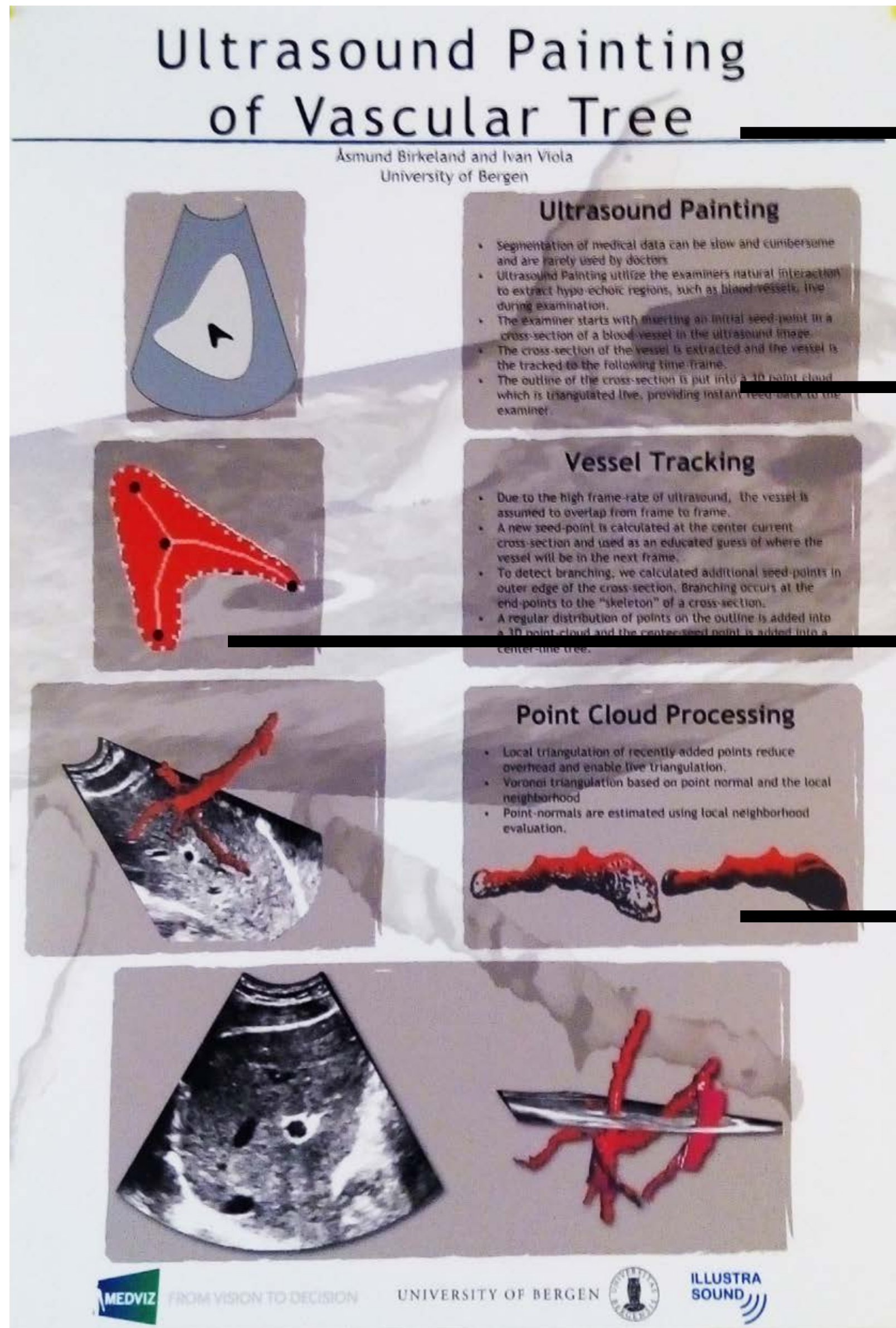
more space between  
elements



background photo  
makes text illegible



unite the size and positions of elements

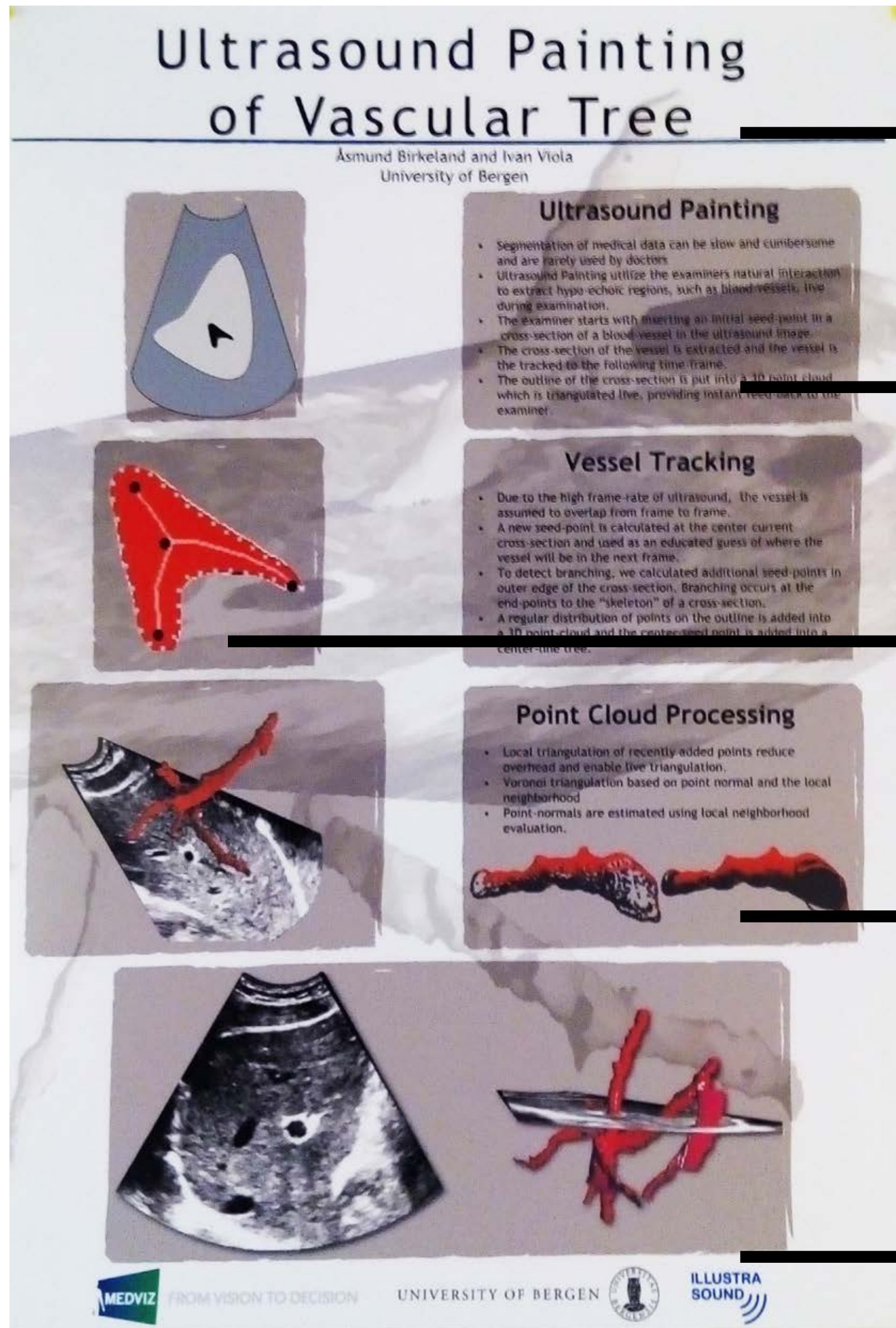


more space between elements

background photo makes text illegible

unite the size and positions of elements

too many overlapping elements - visualizations, photos, ...



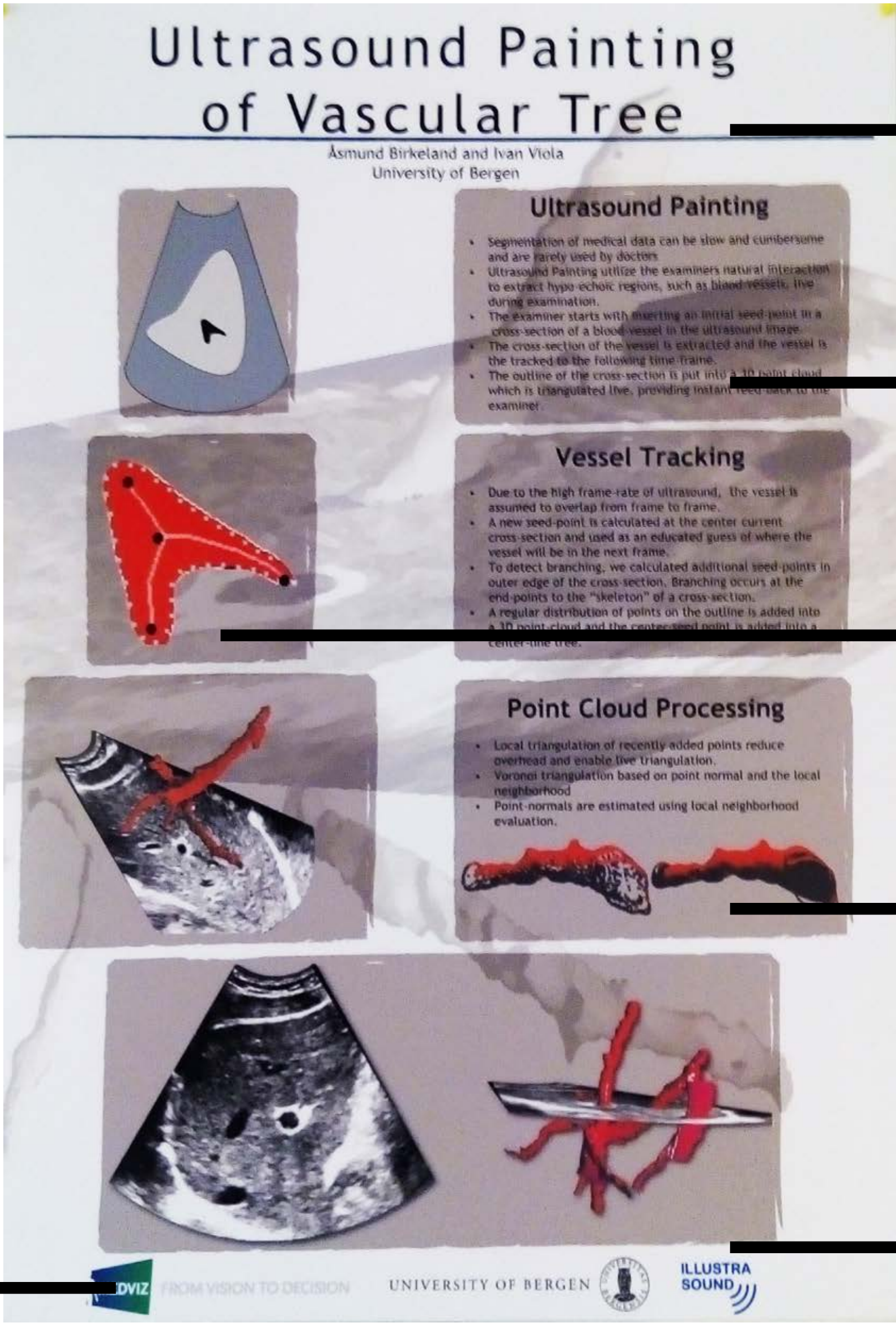
more space between elements

background photo makes text illegible

unite the size and positions of elements

too many overlapping elements - visualizations, photos, ...

more space between logos and graphic elements



more space between elements

background photo makes text illegible

unite the size and positions of elements

too many overlapping elements - visualizations, photos, ...

more space between logos and graphic elements

keep a safety zone around the logo



## Case study

### Posters

Nis escienime namende corepe  
nobis ullam, aut elenda coris  
exero volorpo ressund empore  
pa vendem. Bit ut aligendunt  
alique isti cusa nihic to tem sant  
quias ea dolorum eumquatem  
quae nulpa cuptata ipisciuntis  
dolorescid et abor alitinc  
imilleste pro volendam, ut  
voluptata qui consedit aut  
rectotatur, nis ut porum eos  
samusae consequodi dunt  
excerio consedit iderum ne  
sum volorib usapediscias.

**rivers**

Nisescienimenamendecorepenobisullam,autelenda  
coris exero volorpo ressund empore pa vendem.  
Bit ut aligendunt alique isti cusa nihic to tem sant  
quias ea dolorum eumquatem quae nulpa cuptata  
ipisciuntis dolorescid et abor alitinc imilleste pro  
volendam, ut voluptata qui consedit aut rectotatur,  
nis ut porum eos samusae consequodi dunt excerio  
consedit iderum ne sum volorib usapediscia

**wider text box**

**Typography**



## Case study

### Posters

Nis escienime namende corepe  
nobis ullam, aut elenda coris  
exero volorpo ressund empore  
pa vendem. Bit ut aligendunt  
alique isti cusa nihic to tem sant  
quias ea dolorum eumquatem  
quae nulpa cuptata ipisciuntis  
dolorescid et abor alitinc  
imilleste pro volendam, ut  
voluptata qui consedit aut  
rectotatur, nis ut porum eos  
samusae consequodi dunt  
excerio consedit iderum ne  
sum volorib usapediscias.

**rivers**

Nis escienime namende  
corepe nobis ullam, aut  
elenda coris exero volorpo  
ressund empore pa vendem.  
Bit ut aligendunt alique isti  
cusa nihic to tem sant quias  
ea dolorum eumquatem quae  
nulpa cuptata ipisciuntis  
dolorescid et abor alitinc  
imilleste pro volendam, ut  
voluptata qui consedit aut  
rectotatur, nis ut porum eos  
samusae consequodi dunt  
excerio consedit iderum ne

**left alignment**

**Settings of type  
and type box  
influences the layout**

## Case study

### Posters

Nis escienime namende corepe  
nobis ullam, aut elenda coris  
exero volorpo ressund empore  
pa vendem. Bit ut aligendunt  
alique isti cusa nihic to tem sant  
quias ea dolorum eumquatem  
quae nulpa cuptata ipisciuntis  
dolorescid et abor alitinc  
imilleste pro volendam, ut  
voluptata qui consedit aut  
rectotatur, nis ut porum eos  
samusae consequodi dunt  
excerio consedit iderum ne  
sum volorib usapediscias.

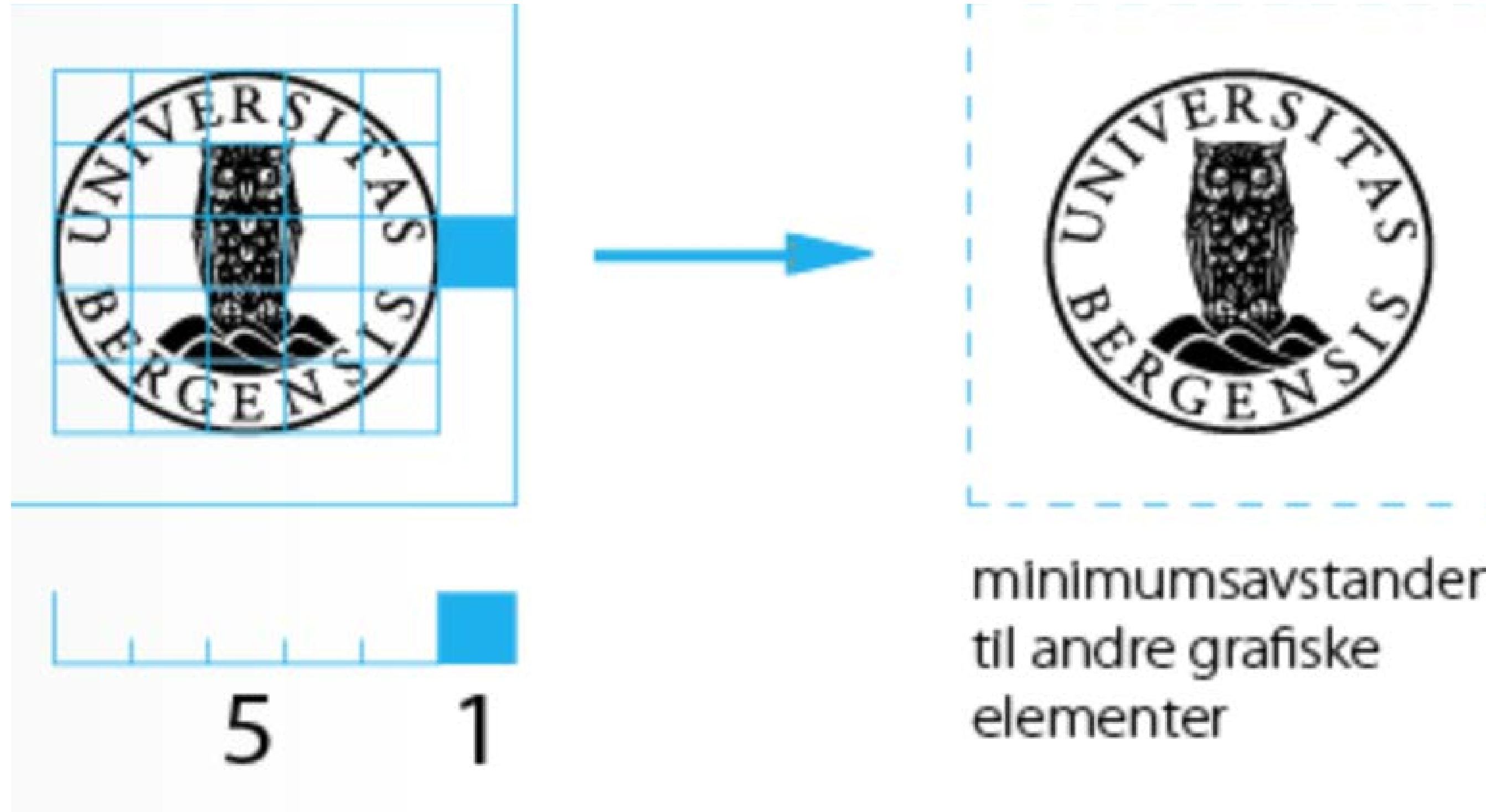
**rivers**

Nis escienime namende corepe nobis ul-  
lam, aut elenda coris exero volorpo res-  
sund empore pa vendem. Bit ut aligend-  
unt aliquie isti cusa nihic to tem sant quias  
ea dolorum eumquatem quae nulpa cup-  
tata ipisciuntis dolorescid et abor alitinc  
imilleste pro volendam, ut voluptata qui  
consedit aut rectotatur, nis ut porum eos  
samusae consequodi dunt excerio conse-  
.dit iderum ne sum volorib usapediscias

**smaller font size  
+ hyphenation**

**Settings of type  
and type box  
influences the layout**

Case study  
Posters



**Logo safety zone**

A minimalist line drawing of two hands holding a rectangular sign. The hands are positioned at the bottom corners of the sign, with the index fingers pointing upwards. The sign is a simple rectangle with a thin black border. Inside the rectangle, the text "THANK YOU :)" is written in a bold, black, sans-serif font, centered horizontally and vertically.

**THANK YOU :)**