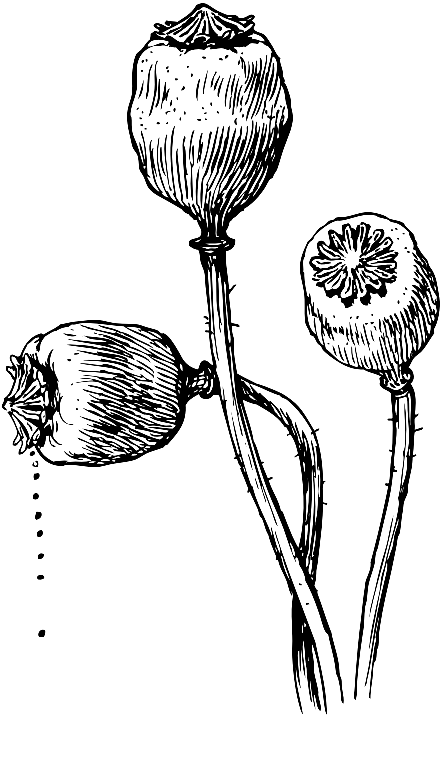
Spring School of the Department of Algebra

Rapotín, April 6–9, 2017

BOOK OF ABSTRACTS



Cover image by openclipart.

Contents

The “H-coefficients” technique in a nutshell

Miloslav Homer

The H-coefficients technique by Patarin is an abstract way of upper bounding a deterministic distinguisher advantage. A high-level overview of reasoning behind this technique will be presented in this talk.

Let D be a deterministic distinguisher, let $\mathsf{Real}, \mathsf{Random}$ be oracles (chosen from sets $\Omega_{\mathsf{Real}}, \Omega_{\mathsf{Random}}$). Denote D^R that D has access to oracle R, denote $D^R = 1$ the event of D claiming that oracle R is Real. We also say that D finished experiment with oracle R deciding R is Real.

Definition 1. Define *advantage* of D as

$$\mathrm{Adv}(D) = \Pr\left[D^{\mathsf{Real}} = 1\right] - \Pr\left[D^{\mathsf{Random}} = 1\right].$$

Definition 2. Define *view* as set of queries for R that D made during the experiment. Let the number of queries be q. Define the view ν as

$$\nu = \{\, (P_i, C_i) \mid i \leq q \,\}.$$

Denote V the set of all views obtainable by distinguisher D. Denote X the probability distribution on views induced by Real oracles and Y for Random oracles (functions $\Omega_{\mathsf{Real}} \to V$ and $\Omega_{\mathsf{Random}} \to V$ respectively). Denote $\Pr[X = \nu]$ probability that D produced view ν. Denote (the so-called *statistical distance*)

$$\Delta(X, Y) = \frac{1}{2} \sum_{\nu \in V} \left|\Pr[X = \nu] - \Pr[Y = \nu]\right|.$$

Proposition 3. *For fixed distinguisher D:*

$$\Delta(X, Y) \geq \mathrm{Adv}(D).$$

Lemma 4.

$$\Delta(X, Y) = 1 - \mathbb{E}_{\nu \sim Y}\left[\min\left(1, \frac{\Pr[X = \nu]}{\Pr[Y = \nu]}\right)\right].$$

Proposition 5. *Let $V_1 \cup V_2 = V$ and V_1, V_2 be disjoint. Let ϵ_i be such that:*

$$\forall \nu \in V_i \colon \frac{\Pr[X = \nu]}{\Pr[Y = \nu]} \geq 1 - \epsilon_i.$$

Then

$$\Delta(X, Y) \leq \Pr[Y \in V_1]\, \epsilon_1 + \Pr[Y \in V_2]\, \epsilon_2.$$

Moreover, if ϵ_1 is small and ϵ_2 is large while $\Pr[Y \in V_1]$ is large and $\Pr[Y \in V_2]$ is small, then:

$$\mathrm{Adv}(D) \leq \epsilon_1 + \Pr[Y \in V_2].$$

Definition 6. We call view ν compatible with oracle R if for any $(P, C) \in \nu$ it holds that $R(P) = C$. Given view ν denote $\mathrm{comp}_\Omega(\nu)$ set of oracles of Ω that are compatible with view ν.

Given ν a possible transcript of D (either $\Pr[X = \nu] > 0$ or $\Pr[Y = \nu] > 0$) it holds that:

$$\Pr[X = \nu] = \frac{\left|\mathrm{comp}_{\Omega_{\mathsf{Real}}}(\nu)\right|}{|\Omega_{\mathsf{Real}}|} \quad \text{and} \quad \Pr[Y = \nu] = \frac{\left|\mathrm{comp}_{\Omega_{\mathsf{Random}}}(\nu)\right|}{|\Omega_{\mathsf{Random}}|}.$$

Consequently:

(1) The order in which queries appear in a view ν does not affect the probability of ν occuring, only the set of queries does.

(2) If two different deterministic distinguishers can obtain ν with nonzero probability they would obtain ν with *equal* probability (even if the order of queries differs).

Cobham's Theorem

Barbora Hudcová

1. Introduction

This talk will be an introduction to the topic of automatic sequences. More specifically, I will introduce finite automata with output as well as some basic operations on words. The main goal of this talk will be to show the correspondence between k-automatic sequences and fixed points of k-uniform morphisms.

2. Alphabets and Words

Definition 1 (Alphabet)**.** Let Σ be a finite, nonempty set called an *alphabet.* The elements of Σ are referred to as *letters.* By Σ_k we understand the alphabet $\{0, 1, \ldots, k-1\}$.

Definition 2 (Words)**.** A *finite word* over an alphabet Σ is any finite sequence of letters from Σ. The *empty word* will be denoted by ϵ. By Σ^* we understand the set of all finite words over Σ.

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$. An *infinite word* is a map from $\mathbb{N}$ to Σ. If $\mathbf{w}$ is an infinite word, we often write $\mathbf{w} = w_0 w_1 w_2 \ldots$ where each $w_i \in \Sigma$.

Definition 3 (Morphism)**.** Let Σ be an alphabet. A map $h\colon \Sigma^* \longrightarrow \Sigma^*$ is called a *morphism* if h satisfies $h(xy) = h(x)h(y)$ $\forall x, y \in \Sigma^*$.

If there exists a constant k such that $|h(a)| = k$ $\forall a \in \Sigma$, we say h is *k-uniform.* A 1-uniform morphism is called a *coding.*

Let $h\colon \Sigma^* \longrightarrow \Sigma^*$ be a morphism. A finite or infinite word satisfying $h(w) = w$ is said to be a *fixed point* of h.

If there exists $a \in \Sigma$ such that $h(a) = ax$ for some $x \in \Sigma^*$ such that $h(x) \neq \epsilon$, we say h is *prolongable on a.* In this case, the sequence of words $a, h(a), h^2(a), \ldots$ converges, in the limit, to the infinite word

$$\overrightarrow{h^{\omega}}(a) \coloneqq axh(x)h^2(x)h^3(x)\ldots$$

which is a fixed point of h.

3. Numeration System Notation

Definition 4 (Base-k expansion)**.** Let $n \in \{0, 1, 2, \ldots\}$, $k \geq 2$ an integer. By $(n)_k$ we understand the unique base-k expansion of n. More formally: $(n)_k = a_t a_{t-1} \ldots a_1 a_0$ such that $n = \sum_{i=0}^{t} a_i k^i$.

Let $k \geq 2$ be an integer, $w \in \Sigma_k = \{0, 1, \ldots, k-1\}$; $w = a_t a_{t-1} \ldots a_1 a_0$. Then we define $[w]_k \coloneqq \sum_{i=0}^{t} a_i k^i$.

4. Finite Automata with Output

Definition 5 (Finite automaton with output)**.** A *deterministic finite automaton with output*, or DFAO is a 6-tuple $M = (\mathcal{Q}, \Sigma, \delta, q_0, \Delta, \tau)$ where

- $\mathcal{Q}$ is a finite set of states
- Σ is the finite input alphabet
- $\delta\colon \mathcal{Q} \times \Sigma \to \mathcal{Q}$ is the transition function
- $q_0 \in \mathcal{Q}$ is the initial state and
- Δ is the finite output alphabet
- $\tau\colon \mathcal{Q} \to \Delta$ is the output function.

Moreover, when the input alphabet $\Sigma = \Sigma_k$ for an integer $k \geq 2$, we call a DFAO a k-DFAO.

Definition 6 (k-automatic sequence)**.** We say the sequence $(a_n)_{n\geq 0}$ over a finite alphabet Δ is *k-automatic* if there exists a k-DFAO $M = (\mathcal{Q}, \Sigma_k, \delta, q_0, \Delta, \tau)$ such that $a_n = \tau(\delta(q_0, w))$ for all $n \geq 0$ and all w with $[w]_k = n$.

5. Cobham's Theorem

Theorem 7 (Cobham's Theorem)**.** *Let $k \geq 2$. Then a sequence $\mathbf{u} = (u_n)_{n\geq 0}$ is k-automatic if and only if it is the image, under a coding, of a fixed point of a k-uniform morphism.*

6. Sequences

Definition 8 (Thue-Morse sequence)**.** *Thue-Morse sequence* $\mathbf{t} = (t_n)_{n\geq 0}$ is defined as:

- $t_n = 0$ if the number of 1's in $(n)_2$ is even
- $t_n = 1$ if the number of 1's in $(n)_2$ is odd

Definition 9 (Thue-Morse morphism)**.** The *Thue-Morse morphism* is a morphism

$$\mu\colon \Sigma_2^* \longrightarrow \Sigma_2^*$$

where $\mu(0) = 01$ and $\mu(1) = 10$.

Definition 10 (Rudin-Shapiro sequence)**.** *Rudin-Shapiro sequence* $\mathbf{r} = (r_n)_{n\geq 0}$ is defined by the following:

- $r_n = 1$ if the number of (possibly overlapping) occurences of the block 11 in $(n)_2$ is even
- $r_n = -1$ otherwise.

Very transitive groups and geometries

Pavel Surý

This presentation introduces a family of groups, which act multiply transitively on a finite set. By definition, a group action is k-transitive if for every two k-tuples of distinct points there exists a group element that maps the first tuple to the second one. Particularly, we show that there are infinite classes of 3-transitive groups and suggest a way to construct the only four non-trivial finite permutation groups with a degree of transitivity higher than 3.

1. Introduction

Definition 1. Let G act on X.

- A subset $\mathrm{Orb}(x) = \{\, g(x) \in X \mid g \in G \,\}$ is called *orbit of point x*.
- A subgroup $\mathrm{Stab}(x) = \{\, g \in G \mid g(x) = x \,\}$ is called *stabilizer of point x*.

Theorem 2 (orbit-stabilizer property)**.** *Let G act on X. For all $x \in X$ we have $|\mathrm{Orb}(x)| = |G : \mathrm{Stab}(x)|$ (or $|\mathrm{Orb}(x)|\,|\mathrm{Stab}(x)| = |G|$ if G is finite).*

Definition 3. Let G act on X. The actions is

- *transitive*, if for all $x, y \in X$ there is $g \in G$ such that $g(x) = y$.
- *k-transitive*, if for all $x_1 \neq \cdots \neq x_k, y_1 \neq \cdots \neq y_k \in X$ there is $g \in G$ such that $g(x_j) = y_j$ for all $1 \leq j \leq k$.

Theorem 4. *Let G act k-transitively on X and $|X| = n$. Then $n(n-1)\dots(n-k+1)$ divides $|G|$.*

Example.

- S_n is n-transitive on $\{1, \dots, n\}$.
- A_n is $(n-2)$-transitive on $\{1, \dots, n\}$.
- D_n is 1-transitive on $\{1, \dots, n\}$.

Lemma 5. *Let G act on X. The action is k-transitive, iff:*

(1) G acts transitively on X.

(2) Every point stabilizer $\mathrm{Stab}(x)$ acts $(k-1)$-transitively on $X \setminus \{x\}$.

The condition (2) can be equivalently replaced with

(2') Some point stabilizer $\mathrm{Stab}(y)$ acts $(k-1)$-transitively on $X \setminus \{y\}$.

2. Affine and projective groups

Example. Let $X = (V, E)$ be a graph. If $\mathrm{Aut}(X)$ is 2-transitive, then $X = K_n$ or $X = \bar{K_n}$.

Example. $GL_n(\mathbb{F}_q)$ acts transitively on $\mathbb{F}_q \setminus \{0\}$. The action is 2-transitive only in cases

(1) $q = 3$ a $n = 1$,

(2) $q = 2$ a $n > 1$.

Example. $AGL_n(\mathbb{F}_q)$ acts 2-transitively on $\mathbb{F}_q$. The action is 3-transitive only in cases from previous example.

Example. $PGL_n(\mathbb{F}_q)$ acts 2-transitively on projective space and acts 3-transitively, iff $n = 2$.

Steiner system	Parameters	Blocks	Automorphism group
W_{11}	(4,5,11)	66	M_{11}
W_{12}	(5,6,12)	132	M_{12}
W_{23}	(4,7,23)	253	M_{23}
W_{24}	(5,8,24)	759	M_{24}

TABLE 1. Mathieu groups

3. STEINER SYSTEMS

Definition 6. A structure $S(\Omega, \mathcal{B})$, where Ω is a finite set and $\mathcal{B}$ is a system of subsets (blocks), is called a *Steiner system* if

(1) all blocks have the same size k,

(2) for some $t \in \mathbb{N}$, every subset of size t lies in exactly on block.

Such Steiner system has parameters $S(t, k, v)$, where $v = |\Omega|$.

Example. Affine space over $\mathbb{F}_q$ is a $S(2, q, q^d)$ Steiner system for $q > 2$. Its automorphism group is $A\Gamma L_d(\mathbb{F}_q)$, which equals $AGL_d(\mathbb{F}_q)$ for q prime.

Example. Projective space over $\mathbb{F}_q$ is a $S(2, q+1, (q^d-1)/(q-1))$ Steiner system. Its automorphism group is $P\Gamma L_{d+1}(\mathbb{F}_q)$, which equals $PGL_{d+1}(\mathbb{F}_q)$ for q prime.

We show that number of blocks is determined by parameters (they do not depend on particular Steiner system).

Theorem 7. *Let $S(\Omega, \mathcal{B})$ be a $S(t, k, v)$ Steiner system.*

(1) There are $r = \binom{v-1}{t-1} / \binom{k-1}{t-1}$ block containing a particular point.

(2) There are $b = \frac{vr}{k}$ blocks.

It's possible to show that there exist unique Steiner systems of parameters denoted in Table 1. Groups M_{11}, M_{12}, M_{23} and M_{24} are constructed as their automorphism groups.

Theorem 8. *Let G act faithfully k-transitively on X with $k \geq 4$, where X is finite. Then either $G \cong S_n$ (for $n \geq 4$), $G \cong A_n$ ($n \geq 6$) or $G \cong M_n$ ($n \in \{11, 12, 23, 24\}$).*

Almost Perfect Nonlienear Permutations

Dáša Krasnayová

Existence of Almost Perfect Nonlinear (APN) permutations in fields with even dimension has been an interesting problem for many years now. In this talk I would like to present some results from my master thesis and the research that followed.

Definition 1 (Boolean function)**.** A *boolean function* is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ for some non-negative integer n. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where $n \geq m \geq 1$, n, m non-negative integers, is called a *vectorial boolean function.*

Definition 2 (APN function)**.** A function $F\colon \mathbb{F}_{2^n} = \mathbb{F} \to \mathbb{F}$ is called *Almost Perfect Nonlinear (APN)* if equation $F(x)+F(x+a) = b$ has two or zero solutions $x \in \mathbb{F}$ for every $a, b \in \mathbb{F}$, $a \neq 0$. Equivalently, F is APN if and only if $|D_aF| = |\{D_aF(x)\colon x \in \mathbb{F}\}| = |\mathbb{F}|/2$ for every $a \in \mathbb{F}^*$, where $D_aF(x) = F(x) + F(x + a) + F(a) + F(0)$ is a *derivative* of F.

The first and the only example of an APN function in even dimension so far was presented by Dillon et al., in 2009. The function is known as the *Kim function* or κ *function* and is defined as

$$\kappa(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $x^6 + x^4 + x^3 + x + 1$.

Main technique used to solve equations in my master thesis is simplifying them using so-called *Trace*-0*/Trace*-1 *decomposition.* We define

$$\mathcal{T}_1 = \Big\{g \in \mathbb{F}_{q^2} : \mathsf{Tr}_m^n(g) = g^q + g = 1\Big\} \cup \{1\}$$

a set of all Trace-1 elements and 1. Moreover, we can notice that elements of the sub-field $\mathbb{F}_q$ are exactly all Trace-0 elements of $\mathbb{F}_{q^2}$, i.e. $\mathbb{F}_q = \{X \in \mathbb{F}_{q^2} : \mathsf{Tr}_m^n(X) = 0\}$.

Every element of $\mathbb{F}_{q^2}$ can then be written using elements of $\mathcal{T}_1$ and $\mathbb{F}_q$ in two ways presented in following propositions.

Proposition 3. *Every $X \in \mathbb{F}_{q^2}^*$ can be uniquely written as $X = xg$, where $x \in \mathbb{F}_q^*$ and $g \in \mathcal{T}_1$.*

Proposition 4. *For every $g \in \mathcal{T}_1 \setminus \{1\}$, any $X \in \mathbb{F}_{q^2}$ can be uniquely written as $X = xg + y$, where $x, y \in \mathbb{F}_q$.*

These propositions were proven in a paper by Faruk Göloğlu in 2015.

1. Our research

We studied a family of the functions which can be written in a form

$$F(x) = x^3 + bx^{3q} + cx^{2q+1} + dx^{q+2},$$

where $q = 2^m$ and $b, c, d \in \mathbb{F}_q$. Functions from this family are a special case of functions introduced in a talk at BIRS Workshop by Petr Lisoněk in 2014. The Kim function is CCZ-equivalent to a member of this family.

In my master thesis we found equivalent conditions on b, c, d for F to be APN. The most complicated condition is:

$$\mathsf{Tr}_1^m\left(\frac{\Delta(T\Delta + c + d)(T^2\Delta^2 + bd + c)}{(T\Delta^2 + bc + d)^2}\right) = 1,$$

for every T such that $\mathsf{Tr}_1^m(T) = 1$, $\Delta T + 1 + b \neq 0$, $T\Delta^2 + bc + d \neq 0$ and $\Delta^2 T^2 + bd + c \neq 0$.

We were able to simplify this condition to

$$\mathsf{Tr}_1^m\left(\frac{(T\Delta + c + d)(bd + c + c^2 + d^2)(bd + c + b^2 + 1)}{\Delta(T\Delta^2 + bc + d)}\right) = 0$$

for every T such that $\mathsf{Tr}_1^m(T) = 1$, $\Delta T + 1 + b \neq 0$, $T\Delta^2 + bc + d \neq 0$ and $\Delta^2 T^2 + bd + c \neq 0$.

We managed to prove that this is not possible in larger fields unless one of the expressions $(bd + c + c^2 + d^2)$ and $(bd + c + b^2 + 1)$ is equal zero. If this happens, F is CCZ-equivalent to a function which is not CCZ-equivalent to a permutation.

2. Conclusion

There are no new APN functions equivalent to a permutation in the chosen family of functions.

Building Carmichael numbers with large number of prime factors

Ivana Trummová

This lecture will be based on a paper written by Dominique Guillaume and François Morain, who extend the method of Günther Löh and Wolfgang Niebuhr for the generation of Carmichael numbers with a large number of prime factors to other classes of pseudoprimes. I will present the algorithm used for building Carmichael numbers and several improvements and remarks.

1. Carmichael numbers

Definition 1. A Carmichael number C is a composite integer for which the identity

$$a^{C-1} \equiv 1 \pmod{C}$$

holds for all values of a prime to C.

Theorem 2 (Korselt's criterion)**.** *A Carmichael number C is an odd squarefree composite number, $C = p_1 * \cdots * p_r$, with $r \geq 3$ such that*

$$C - 1 \equiv 0 \pmod{(p_i - 1)} \quad \textit{for} \quad 1 \leq i \leq r.$$

Alternatively:

$$\lambda(C) \mid C - 1$$

where λ denotes Carmichael function:

Definition 3. Carmichael function of a positive integer n, denoted $\lambda(n)$, is defined as the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for every integer a that is prime to n.

Using these facts, we will look for Carmichael numbers with a large number of prime factors.

2. The Algorithm

We want to search for Carmichael numbers C with a fixed value of $\Lambda = \lambda(C)$. Let

$$S(\Lambda) = \{\, p, p \quad prime, p \nmid \Lambda, p - 1 \mid \Lambda \,\}$$

$\Longrightarrow$ a squarefree product N of elements of $S(\Lambda)$ satisfies

$$\lambda(N) \mid \Lambda$$

as well as the property

$$p_j \not\equiv 1 \pmod{p_i}$$

for $1 \leq i < j \leq r$.

Suppose one wants to find Carmichael numbers with r factors built up with the primes of $S := S(\Lambda)$.

- It is enough to look for r distinct elements $p_1, \ldots, p_r$ such that
$$C = p_1 * \cdots * p_r \equiv 1 \pmod{\Lambda}$$
- If this is the case, we have $C \equiv 1 \pmod{\lambda(C)}$ since $\lambda(N) \mid \Lambda$.

Circular units of abelian fields with four ramified primes

Vladimír Sedláček

1. Introduction

Circular units appear in many situations in algebraic number theory, because in some sense they are a good approximation of the full group of units of a given abelian field, which is very hard to describe explicitly. They are also closely related to the class group of the respective field, which was already known to E. Kummer. For abelian number fields which are not cyclotomic, there are even several possible definitions with different properties.

The problem is that a $\mathbb{Z}$-basis of the group of circular numbers is known only in a few very special cases, for example when the abelian field is cyclotomic, has at most two ramified primes, or has three ramified primes and satisfies some other conditions. The aim of this talk is to explore the case of an abelian field with four ramified primes under another assumptions, and to present a recent result of the author of this talk.

2. Preliminaries

Definition 1. An *abelian field* is a finite Galois extension of $\mathbb{Q}$ with an abelian Galois group. The *genus field* (in the narrow sense) of an abelian field is its maximal abelian extension (i.e., finite Galois extension with an abelian Galois group) unramified at all (finite) primes.

Theorem 2 (Kronecker-Weber)**.** *Every abelian field is a subfield of some cyclotomic field.*

Definition 3. Let k be an abelian field. The least number $f \in \mathbb{N}$ such that $k \subseteq \mathbb{Q}(\zeta_f)$ is called the conductor of k.

Definition 4. Let G be any group. The (integral) *group ring* $\mathbb{Z}[G]$ is the free $\mathbb{Z}$-module with basis G, which is made into a ring by using the group law on G and extending linearly.

3. The case of four ramified primes

Let k be a fixed real abelian field ramified at exactly four primes p_1, p_2, p_3, p_4 with genus field K, with $G := \mathrm{Gal}(K/\mathbb{Q})$ and $H := \mathrm{Gal}(K/k)$. Also let K_i be the maximal subfield of K ramified only at p_i and let $T_i = \mathrm{Gal}(K/K_j K_l K_h)$ be the inertia subgroup of G for the prime p_i (so that $G \cong T_1 \times T_2 \times T_3 \times T_4$). We will assume that H is cyclic and all the T_i's are cyclic, generated by σ_i. Finally, let $m := |H|, a_i := [K_i \cap k : Q], r_i := [K : kK_i], n_i := \frac{m}{r_i}$, as can be seen in the following diagram.

$$\begin{tikzcd}
& K \arrow[d, dash, "r_i"'] & \\
& kK_i \arrow[dl, dash, "n_i"'] \arrow[dr, dash] & \\
k \arrow[dr, dash] & & K_i \arrow[dl, dash] \\
& k \cap K_i \arrow[d, dash, "a_i"'] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Definition 5. The non-torsion part D^+ of the group of circular numbers of k (using Lettl's modification of Sinnott's definition) is a $\mathbb{Z}[G]$-module with one generator for each nonempty subset of the set of ramified primes of k. More specifically,

$$D^+ = \langle \eta, \eta_{123}, \eta_{124}, \eta_{134}, \eta_{234}, \eta_{12}, \eta_{13}, \eta_{14}, \eta_{23}, \eta_{24}, \eta_{34}, \eta_1, \eta_2, \eta_3, \eta_4 \rangle_{\mathbb{Z}[G]},$$

where

$$\begin{aligned}
\eta &= \mathrm{N}_{\mathbb{Q}(\zeta_f)/k}(1 - \zeta_f) \\
\eta_{ijl} &= \mathrm{N}_{\mathbb{Q}(\zeta_{f_{ijl}})/(K_iK_jK_l \cap k)}(1 - \zeta_{f_{ijl}}) \\
\eta_{ij} &= \mathrm{N}_{\mathbb{Q}(\zeta_{f_{ij}})/(K_iK_j \cap k)}(1 - \zeta_{f_{ij}}) \\
\eta_i &= \mathrm{N}_{\mathbb{Q}(\zeta_{f_i})/(K_i \cap k)}(1 - \zeta_{f_i})
\end{aligned}$$

and f, f_{ijl}, f_{ij}, f_i are the conductors of $K, K_iK_jK_l, K_iK_j, K_i$, respectively.

The non-torsion part C^+ of the group of circular units of k is $D^+ \cap E(k)$, where $E(k)$ are all units of k.

Lemma 6. *The $\mathbb{Z}$-rank of D^+ is $[k : \mathbb{Q}] + 3$.*

Lemma 7. *We have*

$$\begin{aligned}
Gal(k/\mathbb{Q}) \cong \{ \big(\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\big)\big|_k ;\ & 0 \le x_1 < a_1n_1, 0 \le x_2 < a_2\frac{n_2}{\gcd(r_3, r_4)}, \\
& 0 \le x_3 < a_3\frac{n_3}{r_4}\gcd(r_3, r_4), 0 \le x_4 < a_4\},
\end{aligned}$$

where each automorphism of k determines the quadruple (x_1, x_2, x_3, x_4) uniquely.

Let

$$R_i = \sum_{u=0}^{a_i - 1} \sigma_i^u, \quad N_i = \sum_{u=0}^{n_i - 1} \sigma_i^{ua_i} \in \mathbb{Z}[G].$$

Then R_iN_i is a norm operator from k to a maximal subfield ramified at three primes. We will use this a lot, since a basis of the non-torsion part of the group of circular numbers of an real abelian field with three ramified primes has (under some conditions) already been constructed.

In the talk, we will see how to construct a $\mathbb{Z}$-basis of D^+ (in quite a geometric way) in a special subcase.

Goldwasser-Killian primality test

Jiří Pavlů

Goldwasser-Killian test is one of the first primality proving algorithm, that at the same time:

- can be used for arbitrary natural number,
- runs in polynomial time,
- can actually *prove* a number is a prime,
- its correctness does not depend on any unproven conjecture.

In this lecture Goldwasser-Killian test will be presented, along with some basic introduction to algebraic concepts behind it – mainly elliptic curves. We will see how it works and why it works. Some modifications and their advantages will also be mentioned.

1. Elliptic curve group law

Definition 1. Let $\mathbb{F}$ be a field, $\operatorname{char}(\mathbb{F}) \neq 2, 3$. We will define an *elliptic curve over* $\mathbb{F}$ ((A, B)) as an ordered pair (A, B) such that $A, B \in \mathbb{F}$ and $4A^3 + 27B^2 \neq 0$.

Definition 2. Let $\mathbb{F}$ be a field and (A, B) an elliptic curve over $\mathbb{F}$. We will define its *set of points* ($E_{A,B}(\mathbb{F})$) as a set of ordered pairs (x, y) such that $x, y \in \mathbb{F}$ and $y^2 = x^3 + Ax + B$ along with a special point I.

Definition 3. Let $E_{A,B}(\mathbb{F})$ be a set of points of an elliptic curve. For $P = (x_p, y_p)$, $Q = (x_q, y_q) \in E_{A,B}(\mathbb{F})$ we define addition in a following way:

- $P + I = P$ for every $P \in E_{A,B}(\mathbb{F})$
- if $x_p = x_q$ and $y_p = -y_q$, then $P + Q = I$
- otherwise we define $P + Q$ as a point (x_{res}, y_{res}), where $x_{res} = s^2 - x_p - x_q$, $y_{res} = s(x_p - x_{res}) - y_p$, where s is defined as:
  - $s = \frac{3x_p + A}{y_p}$ if $P = Q$
  - $s = \frac{x_p - x_q}{y_p - y_q}$ if $P \neq Q$.

Note. The formulas can be used even if we take an elliptic curve over a ring (and not a field), they just sometimes fail.

2. Important theorems

Theorem 4. *Let (A, B) be an elliptic curve over $\mathbb{F}$. Let $|E_{A,B}(\mathbb{F})| = 2q$, for some odd prime number q. Then $E_{A,B}(\mathbb{F})$ is isomrphic to group $\mathbb{Z}_{2q}$.*

Proof. Divisors of $2q$ are only numbers: $1, 2, q, 2q$. So because of its cardinality and the divisibility of its order it must be isomorphic to $\mathbb{Z}_{2q} \simeq \mathbb{Z}_q \oplus \mathbb{Z}_2$. □

Theorem 5 (Hasse). *Let (A, B) be an elliptic curve over $\mathbb{F}_p$, and $E_{A,B}(\mathbb{F}_p)$ its set of points. Then $\big||E_{A,B}(\mathbb{F}_p)| - p - 1\big| \leq 2\sqrt{p}$.*

Theorem 6 (Lenstra)**.** *Let $p > 5$ be a prime, $S \subseteq \left[p+1-\lfloor\sqrt{p}\rfloor, p+1+\lfloor\sqrt{p}\rfloor\right]$. If (A,B) an ellipic curve over $\mathbb{F}_p$ is chosen uniformly randomly, then the probability*

$$P\left[\left|E_{A,B}(p)\right| \in S\right] > \frac{c}{\log(p)} * \frac{|S|-2}{2\lfloor\sqrt{p}\rfloor+1}.$$

Theorem 7. *Let $n \in N$, $\mathrm{GCD}(6,n) = 1$. Let (A,B) be an elliptic curve over $\mathbb{Z}_n$, $P \neq I \in E_{A,B}(\mathbb{Z}_n)$. Then if $qP = I$ for some prime number $q > n^{1/2} + 2n^{1/4} + 1$, then n is a prime.*

The automorphism tower of a group

Michal Hrbek

Let G be a group. We denote by the $\mathrm{Aut}(G)$ the group of all automorphisms of G. Then there is a natural group homomorphism

$$\pi_G \colon G \to \mathrm{Aut}(G),$$

assigning to an element $g \in G$ the inner automorphism $i_g \colon h \mapsto g^{-1}hg$. Note that this forces $\pi_G(g) = \mathrm{Id}_G$ for any g from the center of the group G. In particular, π_G is a trivial homomorphism whenever G is abelian.

On the other hand, if the center of G is trivial (i.e., G is *centerless*), then the map π_G is an embedding, and $\mathrm{Aut}(G)$ is also centerless.

The *automorphism tower* of G is defined by transfinite iteration. Explicitly, we define by induction on ordinals α a sequence of groups G_α and group homomorphisms $\pi_\alpha \colon G_\alpha \to G_{\alpha+1}$:

$$G_0 = G,$$

$$\pi_{G_\alpha} =: \pi_\alpha : G_\alpha \to G_{\alpha+1} := \mathrm{Aut}(G_\alpha),$$

$$G_\lambda = \varinjlim_{\alpha<\lambda} G_\alpha, \quad \text{when } \lambda \text{ is a limit ordinal.}$$

(Note: In case of G being centerless, all the maps π_α are embeddings, and the direct limit in a limit step λ is just a union $\bigcup_{\alpha<\lambda} G_\alpha$.)

(Another note: The non-centerless case can be a bit non-intuitive. E.g., consider $G = D_8$. Then $\mathrm{Aut}(D_8) = D_8$, and thus $G_n \simeq D_8$ for all $n < \omega$. The image π_n is always a quotient of D_8 over its center – a Klein subgroup of D_8. By the limit construction, $G_\omega \simeq \mathbb{Z}_2$, and $G_{\omega+1}$ is the trivial group. Hence, the automorphism tower of D_8 terminates at step $\omega + 1$, but not at ω.)

Problem. *Does the automorphism tower terminate for any group G? That is, is there for any G an ordinal β such that $G_\alpha = G_\beta$ for all $\alpha > \beta$?*

Theorem 1 (Wielandt, 1939)**.** *If G is finite and centerless, then the automorphism tower of G terminates after finitely many steps.*

Theorem 2 (Thomas, 1985)**.** *If G is infinite and centerless, then the automorphism tower of G terminates after at most $(2^{|G|})^+$ steps.*

Theorem 3 (Hamkins, 1998)**.** *The automorphism tower of any group terminates.*

I will try to explain the (rather short and very elegant!) proofs of Theorems 2 and 3.

Manim – the tool of 3blue1brown

Miroslav Olšák

1. Introduction

There are 3 basic classes (types of objects):

- Mobject = An object in the scene. It can be for instance square, TeX symbol or a group of such things.
- Scene = The main object containing all the mobject which are supposed to be drawn on the screen. The video itself is coded in a method of a successor of Scene.
- Animation = An auxiliary object providing a fluent movement of an Mobject or its fluent deformation into another. In our examples it is substituted by Transform, its successor.

2. Example code

Add the number of vertices and change color

```
class RegPolygons(Scene):
    def construct(self):
        for i in range(3, 100):
            polygon = RegularPolygon(i)
            polygon.set_color(rgb_to_color([i/99.0, (100-i)/99.0, 0]))
            self.add(polygon)
            self.update_frame()
            self.add_frames(self.get_frame())
            self.remove(polygon)
```

First circle, then square

```
class CircleSquare1(Scene):
    def construct(self):
        circle = Circle()
        square = Square()
        self.add(circle)
        self.dither()
        self.remove(circle)
        self.add(square)
        self.dither()
```

Transformation: Triangle+square → vice versa. There are two versions, the former transforms the objects while the latter switches them.

```
class CircleSquare2(Scene):
    def construct(self):
        begin = VGroup(Circle(), Square())
        end = VGroup(Square(), Circle())
        begin[0].shift([-2,0,0])
        begin[1].shift([2,0,0])
        end[0].shift([-2,0,0])
        end[1].shift([2,0,0])
        self.play(Transform(begin, end))

class CircleSquare3(Scene):
    def construct(self):
        begin = VGroup(Circle(), Square())
        end = VGroup(Circle(), Square())
        begin[0].shift([-2,0,0])
        begin[1].shift([2,0,0])
        end[0].shift([2,0,0])
        end[1].shift([-2,0,0])
        self.play(Transform(begin, end))
```

Colored TEXt

```
class ColorBinom(Scene):
    def construct(self):
        binom = TexMobject('\\binom nk')
        self.add(binom)
        binom[1].set_color(YELLOW)
        binom[2].set_color(BLUE)
        self.dither()
```

3. Links

- The manim library code: https://github.com/3b1b/manim
- 3blue1brown videos: https://www.3blue1brown.com/