Autumn School of the Department of Algebra

Nedamov, November 9–12, 2017

BOOK OF ABSTRACTS

Cover image by openclipart.

Contents

Low-Communication Parallel Quantum Multi-target preimage search

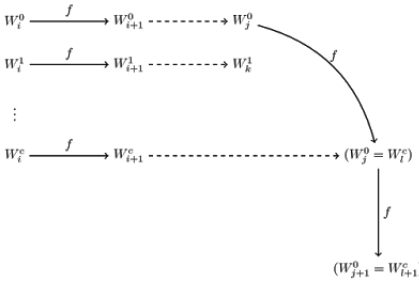
Adolf Středa

The most important pre-quantum threat to AES-128 is the Oorschot-Wiener's parallel rho method. While the quantum algorithms (more specifically Grover's algorithm) offer us a significant asymptotic speed-up, this speed-up alone may not be significant enough as they loose much of their potential on lengthy serial phases. To tackle this problem Banegas and Bernstein introduced an algorithm which tries to combine the strengths of Grover's algorithm quantum speed-up and Oorschot-Wiener's algorithm parallelization.

1. Parallel rho

Parallel rho utilises similar idea as a traditional Pollard's rho method. The intuitive idea is that we want to search for collisions of $F\colon \{0,1\}^n \to \{0,1\}^n$ in parallel thus we will have many different starting points. As the communication between machines to check for collisions would have generated a significant overhead and saving all the results would require too much space, we will have to utilize so-called distinguished points. This notion has to satisfy two properties – it has to be easily verified and also tweakable probability of their occurrence.

Definition 1. Fix $d \in \{0,\ldots,1\}$. Then $x \in \{0,1\}^n$ is called **distinguished point** if the first d bits are zero.

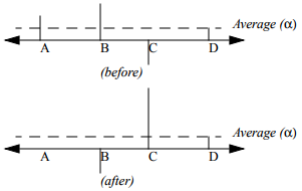


With such notion it is enough to save the starting point $x_{0,i}$, the path length d and the distinguished point $x_{d,i}$. We can do this without loss of functionality as the collision of two paths means that any subsequent points on these paths will also collide. There remain two problems to be tackled – we need to set maximum path length to avoid cycles without distinguished paths and tweak the parameters to make "Robin Hood" trails, which collide with another path's starting point, rare. This algorithm runs in $O(N/pt)$ (p processors, t ciphertexts, N ciphertext set size).

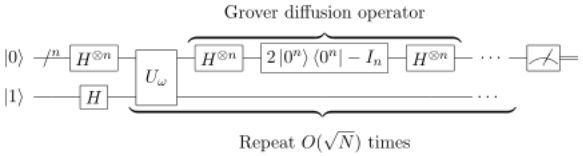
2. Grover's algorithm

This is originally an algorithm for finding an object in a database without any ordering. The basic idea is that we have a function S that returns 1 if the input is the item we are looking for and 0 otherwise.

Definition 2. The inversion about average operation on our state vector is an operator that takes the amplitude of the i'th state, and increases or decreases it so that it is as much above or below the average as it was below or above the average before the operation.



At first every item in the database is assigned the same amplitude (a complex number). Now we have to repeat two phases approximately $O(\sqrt{N})$ times – in the first phase we use function S to perform controlled rotation (shift the phase by π of items in the pre-image of 1 under S), then we apply diffusion operator which performs an inversion about average. After several iterations we will measure, with a high probability, a value corresponding to the item in the pre-image of 1 under S. This algorithm runs in $O(\sqrt{N/t})$ (t ciphertexts, N ciphertext set size).



3. Hybrid algorithm

In order to utilise quantum computer properties we have to modify a parallel rho, e.g. we will need the algorithm to be **reversible** (i.e., every step of computation can be reversed). To make basic logic gates reversible we will need a Toffoli gate.

Definition 3. A Toffoli gate is a gate that maps $(x, y, z) \mapsto (x, y, z + xy)$, $x, y, z \in \{0, 1\}$, where $+$ means XOR.

It is straightforward to prove that any logical gate can be simulated by Toffoli gate, e.g. we can fix third input bit of Toffoli gate to one (such fixed bits are called **ancilla bits**) produces reversible NAND gate which is universal logical gate.

We will now utilize said algorithms to e.g. find a pre-images of fixed $(y_1, y_2, \ldots, y_t)$ under function $H\colon k \mapsto AES_k(0)$.

- Input vector $(x_1, x_2, \ldots, x_t)$
- Compute, in parallel, the chain ends for $x_1, x_2, \ldots, x_t$ (parallel-rho)
- Compute chain ends for $y_1, y_2, \ldots, y_t$ (parallel-rho)
- Sort chain ends for $y_1, y_2, \ldots, y_t$ and $x_1, x_2, \ldots, x_t$ (odd-even mergesort)
- If there is a collision between chain end for x_i and y_j recompute the chain for x_i and check every chain element whether it is pre-image of y_j (Grover's algorithm)
- Output 0 if pre-image was found, otherwise 1

These steps should produce an algorithm running in $O(\sqrt{N/pt^{1/2}})$ (p processors, t ciphertexts, N ciphertext set size).

Avoiding additive cubes

Barbora Hudcová

In this talk we will explore the so-called avoidability problems from the area of combinatorics on words. The aim is to construct infinite words over finite alphabets which avoid a given pattern. We will look at various patterns that have been considered in the past and discuss how such "non-repetitive" words avoiding these patterns can be expressed.

1. Basic notions from combinatorics on words

Let Σ be a non-empty finite set. We will call Σ an *alphabet*. Each $a \in \Sigma$ is called a *letter*. A *(finite) word* over Σ is any sequence of the form

$$u = u_0 u_1 \cdots u_n, \qquad \text{such that } u_i \in \Sigma \text{ for all } i.$$

Σ^* denotes the set of all words over Σ. $\epsilon \in \Sigma^*$ denotes the empty word. The *length* of $u \in \Sigma^*$ is the number of elements in u. For $u = u_0 \cdots u_n$ we write $|u| = n + 1$.

Let $u = u_0 u_1 \cdots u_n$, $v = v_0 \cdots v_m$ be two words over Σ. By uv we understand the concatenation of the words u, v. That is

$$uv = u_0 u_1 \cdots u_n v_0 v_1 \cdots v_m.$$

We say v is a *factor* of u, we write $v \in u$, if there exist $x, y \in \Sigma^*$ such that $u = xvy$. If $x = \epsilon$ we call v the *prefix* of u.

An *infinite word* over Σ is any infinite sequence of the form

$$\mathbf{w} = w_0 w_1 w_2 \cdots \quad \text{such that } w_i \in \Sigma \text{ for all } i.$$

We say $u \in \Sigma^*$ is a factor of $\mathbf{w}$ if there exist $x \in \Sigma^*$ and $\mathbf{y}$ infinite word over Σ such that $\mathbf{w} = xu\mathbf{y}$.

Let $\Sigma = \{a_1, a_2, \dots a_n\}$, $w \in \Sigma^*$. Then $|w|_{a_i}$ denotes the number of occurrences of a_i in w. We define the following map

$$\psi \colon \Sigma^* \to \mathbb{N}^n$$
$$\psi(w) = (|w|_{a_1}, |w|_{a_2}, \cdots, |w|_{a_n})^\intercal.$$

We call ψ the *Parikh map* and $\psi(w)$ the *Parikh vector of* w.

2. Pattern definitions

Let Σ be an alphabet and $k \in \mathbb{N}$, $k \geq 2$. We will define the following patterns.

Powers. We say $u \in \Sigma^*$ is a *k-power* if $u = \underbrace{xx \dots x}_{k \text{ times}}$, where $x \in \Sigma^* \setminus \epsilon$.

Abelian Powers. We say $u \in \Sigma^*$ is an abelian k-power, if $u = x_1 x_2 \dots x_k$ where $x_i \in \Sigma^*$ for all i and for each $i, j \in \{1, 2, \dots, k\}$ we have that $\psi(x_i) = \psi(x_j)$.

Additive powers. Let $\Sigma \subset \mathbb{N}$ be an alphabet, $w \in \Sigma^*$. Then $S(w) = w_0 + w_1 + \cdots + w_n$ is called the *sum* of w. We say w is an additive k-power if $w = x_1 x_2 \cdots x_k$ where each $x_i \in \Sigma^*$, $|x_1| = |x_2| = \cdots = |x_k|$ and $S(x_1) = S(x_2) = \cdots = S(x_k)$.

3. Iterated Morphisms

A map $\varphi\colon \Sigma^* \to \Sigma^*$ is a *morphism* if φ satisfies $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in \Sigma^*$. If there exists $a \in \Sigma$ such that $\varphi(a) = ax$, where $x \in \Sigma^* \setminus \epsilon$, we say φ is *prolongable* on a.

Proposition 1. *If $\varphi\colon \Sigma^* \to \Sigma^*$ is prologable on a, that is $\varphi(a) = ax$ for some $x \in \Sigma^* \setminus \epsilon$, we have $\varphi^n(a) = ax\varphi(x)\varphi^2(x)\dots\varphi^{n-1}(x)$ for each $n \in \mathbb{N}$.*

Therefore, we can define the limit $\overrightarrow{\varphi^\omega}(a) \coloneqq \lim_{n\to\infty} \varphi^n(a) = ax\,\varphi(x)\,\varphi^2(x)\,\varphi^3(x)\cdots$. This method of iterating morphisms is very often used when constructing infinite words avoiding some pattern.

4. Additive cube free words

In 2014, a group of authors constructed the first infinite word over $\{0, 1, 3, 4\}$ which avoids additive cubes. In my thesis I present a similar word with the same property which I found by a brute force search. This word is defined below.

Let $\Sigma = \{0, 1, 3, 7\}$ and $\varphi\colon \Sigma^* \to \Sigma^*$ ba a morphism defined as follows:

$$\begin{aligned}\varphi(0) &= 03\\ \varphi(1) &= 73\\ \varphi(3) &= 1\\ \varphi(7) &= 01.\end{aligned}$$

We put $\mathbf{w} \coloneqq \overrightarrow{\varphi^\omega}(0) = 0317301103737303\cdots$.

Theorem 2. $\mathbf{w}$ *avoids additive cubes.*

Profinite semigroups and their importance in the theory of regular languages

Jana Bartoňová

In the talk we will show several different points of view to profinite semigroups, we'll explain their equivalence and the connection to the theory of regular languages. The talk was prepared by use of the paper *Profinite semigroups and applications* (lecture notes taken by Alfredo Costa, 2005) by Jorge Almeida who developed the theory of profinite semigroups notably.

1. Profinite semigroup

Definition 1. A *directed set* $(I, \leq)$ is a set I together with a quasiorder (i.e. a reflexive and transitive binary relation) $\leq$ on I such that every pair of elements of I has a common upper bound.

Definition 2. A *topological semigroup* is a semigroup S with a topology τ on S such that the semigroup operation $\cdot\colon S \times S \to S$ is a continuous function in the topological space (S, τ).

Definition 3. Let A be a finite set. A *category of A-generated topological semigroups* consists of:

- *objects* – functions $\varphi\colon A \to S$ to topological semigroups S such that the image $\varphi(A)$ generates a dense subsemigroup in S,
- *morphisms* $f\colon \varphi \to \psi$ (where $\varphi\colon A \to S$ and $\psi\colon A \to T$ are objects) – given by continuous homomorphisms $f'\colon S \to T$ such that the equality $f' \circ \varphi = \psi$ holds.

Hereafter all finite topological semigroups will be endowed with a discrete topology.

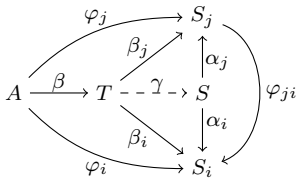
Definition 4. Let $(I, \leq)$ be a directed set. A *projective/ inverse system* of finite A-generated topological semigroups consists of:

- a set of finite A-generated topological semigroups $\{\varphi_i\colon A \to S_i \mid i \in I\}$,
- a set of *connecting morphisms* – a set of continuous homomorpisms $\{\varphi_{ji}\colon S_j \to S_i \mid i, j \in I,\ i \leq j\}$ such that
  - for all $i \in I$ the homomorphism φ_{ii} is the identity on S_i,
  - for all $i, j, k \in I,\ i \leq j \leq k$ the equality $\varphi_{ji} \circ \varphi_{kj} = \varphi_{ki}$ holds.

A *projective/ inverse limit* of this projective system is an A-generated topological semigroup $\alpha\colon A \to S$ together with a set of continuous homomorpisms $\{\alpha_i\colon S \to S_i \mid i \in I\}$ such that

- for all $i, j \in I,\ i \leq j$ the equality $\varphi_{ji} \circ \alpha_j = \alpha_i$ holds,
- for every A-generated topological semigroup $\beta\colon A \to T$ together with a set of continuous homomorpisms $\{\beta_i\colon T \to S_i \mid i \in I\}$ such that for all $i, j \in I,\ i \leq j$ the equality $\varphi_{ji} \circ \beta_j = \beta_i$ holds there exists a continuous homomorphism $\gamma\colon T \to S$ such that for all $i \in I$ the equality $\alpha_i \circ \gamma = \beta_i$ holds.

A *profinite semigroup* is a *projective limit* of a *projective system* of finite A-generated topological semigroups, for some finite set A.



2. Free pro-V semigroup

Definition 5. A *pseudovariety* of finite semigroups is a non-empty class of finite semigroups closed under subsemigroups, homomorphic images and *finite* direct products.

Definition 6. Let A be a finite set and V be a pseudovariety of finite semigroups. A *free pro*-V *semigroup*, denoted by $\overline{\Omega}_A\mathrm{V}$, is a projective limit of a projective system of all A-generated topological semigroups from V.

Proposition 7 (Universal property of a free pro-V semigroup)**.** *Let $\alpha\colon A \to \overline{\Omega}_A\mathrm{V}$ be a free pro*-V *semigroup and let $\varphi\colon A \to S$ be a function to a semigroup $S \in \mathrm{V}$. Then there exists a unique continuous homomorphism $\widehat{\varphi}\colon \overline{\Omega}_A\mathrm{V} \to S$ such that $\widehat{\varphi} \circ \alpha = \varphi$.*

3. Free pro-V semigroup as a completion of a certain metric space

For a finite set A and a pseudovariety of finite semigroups V we denote by $\Omega_A\mathrm{V}$ the variety of semigroups generated by V.

Definition 8. For $u, v \in \Omega_A\mathrm{V}$ we define

$$d(u,v) = \begin{cases} 2^{-r(u,v)} & \text{if } u \neq v \\ 0 & \text{if } u = v \end{cases}$$

where $r(u,v)$ denotes the least cardinality of a semigroup $S \in \mathrm{V}$ such that there exists a homomorphism $\varphi\colon \Omega_A\mathrm{V} \to S$ satisfying $\varphi(u) \neq \varphi(v)$.

Proposition 9. *$(\Omega_A\mathrm{V}, d)$ is a metric semigroup and its completion considered as a topological semigroup is isomorphic to $\overline{\Omega}_A\mathrm{V}$.*

4. Implicit operations

Definition 10. A *n-ary implicit operation* on a pseudovariety V is a mapping w which assigns to every semigroup $S \in \mathrm{V}$ a n-ary operation $w_S\colon S^n \to S$ such that for every pair of semigroups $S, T \in \mathrm{V}$ and for every homomorphism $f\colon S \to T$ the equality

$$f \circ w_S = w_T \circ f^n$$

holds where $f^n\colon S^n \to T^n$ is a homomorphism defined by $f^n(s_1, \ldots, s_n) = \big(f(s_1), \ldots, f(s_n)\big)$.

For every $w \in \overline{\Omega}_A\mathrm{V}$ and every semigroup $S \in \mathrm{V}$ we define a function $\overline{w}_S\colon S^A \to S$ by

$$\overline{w}_S(\varphi) = \widehat{\varphi}(w)$$

where $\widehat{\varphi}\colon \overline{\Omega}_A\mathrm{V} \to S$ is the unique continuous homomorphic extension of $\varphi\colon A \to S$.

Proposition 11. *Let A be a fixed set of cardinality n. The mapping which assigns to every element of $\overline{\Omega}_A\mathrm{V}$ a class of functions $(\overline{w}_S)_{S\in\mathrm{V}}$ is a bijection between $\overline{\Omega}_A\mathrm{V}$ and a set of all n-ary operations on* V.

Euclidean proofs of Dirichlet's Theorem about primes in arithmetic progressions

Martin Čech

1. Introduction

About 300 BC, Euclid used a simple but beautiful argument to prove that there are infinitely many prime numbers. More than 2000 years later, Dirichlet showed that there are infinitely many primes in every arithmetic progression $an + b$ with coprime a and b. His proof was much more complicated, it used analytic arguments and the machinery of L-functions. However, in some particular cases (e.g. the arithmetic progression $4k + 3$), it is possible to modify Euclid's simple argument to prove Dirichlet's theorem for this arithmetic progression.

The topic of the talk will be to investigate to what extent is it possible to generalize Euclid's simple proof and give an easy condition to determine whether *Euclidean proof* in our sense exists for a given progression.

2. Euclidean proofs

One of the main issues is to define what we actually mean by a Euclidean proof. Let us start with the definition of prime divisors of polynomials.

Definition 1. Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. We say that a prime number p is a divisor of f if $p|f(k)$ for some integer k. The set of all prime divisors of f is denoted by $P(f)$.

Divisors of polynomials have several interesting properties. The following can be proved using an argument similar to Euclid's:

Theorem 2. *If $f \in \mathbb{Z}[x]$, then $P(f)$ is infinite.*

The next theorem is more surprising and will have an important corollary for us.

Theorem 3 (Nagell)**.** *Let $f, g \in \mathbb{Z}$. Then $P(f) \cap P(g)$ is infinite.*

After several examples, we will see that the following definition is convenient.

Definition 4. Let a, b be coprime integers. We say that there exists a Euclidean proof of Dirichlet's Theorem for the progression $an + b$ if there exists a polynomial f such that with finitely many exceptions, all $p \in P(f)$ are $\equiv 1, b \pmod{a}$.

Two remarks need to be made about the definition of Euclidean proof.

First, why do we allow the prime divisors to be $\equiv 1 \pmod{a}$? We will see that it is not possible to get rid of this condition, i.e., every polynomial has infinitely many prime divisors which are $\equiv 1 \pmod{n}$ for any n. This will be the important corollary of Nagell's theorem.

Second, it is not obvious at first glance that the existence of a Euclidean proof in our definition actually ensures the existence of infinitely many primes in the given arithmetic progression. However, it can be proved using a Euclidean argument together with the Chinese remainder theorem.

3. Galois theory and cyclotomic fields

One of our main tools will be Galois theory. This section is devoted to the main definitions and facts we are going to use.

Definition 5. Let $L/\mathbb{Q}$ be an extension of fields. Then $\mathrm{Gal}(L/\mathbb{Q})$ denotes the group of all automorphisms of L (i.e., bijective homomorphisms $L \to L$) which pointwise fix the subfield $\mathbb{Q}$.

Galois groups have several important properties:

- the only elements of L fixed by all elements of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ are the rational numbers.
- If we pick an intermediate field $\mathbb{Q} \subset K \subset L$ and take those elements of $\mathrm{Gal}(L/\mathbb{Q})$ which fix the intermediate field K, we receive a subgroup of the Galois group. This group is called the *fixing* group of K.
- Vice versa to the previous case, if we are given a subgroup H of the Galois group, we can take all elements fixed H. These elements will form an intermediate field called the *fixed field* of H.

For $k \in \mathbb{N}$, let ζ_k denote the primitive k^{th} root of unity, i.e., $\zeta_k = e^{\frac{2\pi i}{k}}$.

Definition 6. Let $k \in \mathbb{N}$. Then $\mathbb{Q}(\zeta_k)$ is called the k^{th} cyclotomic field.

The Galois group of cyclotomic fields can be described as follows: since ζ_k is a generator of that field, each of its Galois automorphism σ is uniquely determined by $\sigma(\zeta_k)$. Because ζ_k is a primitive k^{th} root of unity, $\sigma(\zeta_k)$ has to be one as well. The primitive k^{th} roots of unity are exactly numbers of the form $e^{\frac{2\pi i \ell}{k}}$ with $\ell \in \mathbb{Z}/(k\mathbb{Z})^\times$ (where the last group denotes all invertible elements modulo k).

Therefore if by σ_ℓ we denote the automorphism satisfying $\sigma_\ell(\zeta_k) = \zeta_k^\ell$, we see that this gives us an isomorphism $\mathrm{Gal}\left(\mathbb{Q}(\zeta_k)/\mathbb{Q}\right) \simeq \mathbb{Z}/(k\mathbb{Z})^\times$.

We will see that the condition for a Euclidean proof to exist for the progression $an+b$ is that $\{1, b\}$ be a subgroup of $\mathbb{Z}/(a\mathbb{Z})^\times$, i.e., that $b^2 \equiv 1 \pmod{a}$.

Pappos's theorem – several proofs and variations

Ivana Trummová

Introduction to a part of algebraic geometry, which is neither crucial nor very necessary, but good-looking and minimalistic. The only objects involved in the statement of Pappos's theorem are points and lines, and the only relation needed in the formulation of the theorem is incidence.

Key notions:

1. The Hexagon theorem of Pappos

Theorem 1 (The Hexagon theorem of Pappos)**.** *Let A, B, C be three points on a straight line and let X, Y, Z be three points on another line. If the lines $\overline{AY}$, $\overline{BZ}$, $\overline{CX}$ intersect the lines $\overline{BX}$, $\overline{CY}$, $\overline{AZ}$, respectively, then the three points of intersection are collinear.*

Theorem 2 (A Euclidean version of Pappos's theorem)**.** *Consider two straight lines a and b in Euclidean geometry. Let A, B, C be three points on a and let X, Y, Z be three points on b. Then the following holds: If $\overline{AY}\|\overline{BX}$ and $\overline{BZ}\|\overline{CY}$ then automatically $\overline{AZ}\|\overline{CX}$.*

Theorem 3 (Another Euclidean version of Pappos's theorem)**.** *Start with a triangle A, B, C. Draw a point P on the line $\overline{AB}$. From there draw a parallel to $\overline{AC}$ and form the intersection with $\overline{BC}$. From this intersection draw a parallel to $\overline{AB}$ and form the intersection with $\overline{AC}$ and continue this procedure as indicated in the picture. After six steps you will reach point P again.*

2. Variations and generalizations

Theorem 4 (Variation 2: Cayley-Bacharach-Chasles theorem)**.** *Let A and B be two curves of degree three intersecting in nine proper points. If six of these points are on a conic, the remaining three points are collinear.*

Theorem 5 (Variation 1: Pascal's Hexagon theorem)**.** *Let A, B, C, X, Y, Z be six points on a conic. If the lines $\overline{AY}$, $\overline{BZ}$, $\overline{CX}$ intersect the lines $\overline{BX}$, $\overline{CY}$, $\overline{AZ}$ respectively, then the three points of intersection are collinear.*

Theorem 6 (Variation 3: Miquel's theorem)**.** *Consider four points A, B, C, D on a circle. Draw four more circles C_1, C_2, C_3, C_4 that pass through the pairs of points (A, B), (B, C), (C, D), and (D, A), respectively. Now consider the other intersections of C_i and C_{i+1} for $i = 1, \ldots, 4$ (indices modulo 4). These four intersections are again cocircular.*

Groebner basis and solutions of a system of polynomial equations

Lukáš Kubej

A Groebner basis is a special basis of a polynomial ideal, that allows many important properties of the ideal to be deduced easily. This lecture will cover basic properties of Groebner basis, way of finding them and their use in finding solutions of a system of polynomial equations.

1. Groebner basis

Definition 1. Let $I \subset k[x_1, \dots, x_n]$ be nonzero ideal. Let's denote $LT(I)$ the set of all leading terms from I. Finite subset $\{g_1, \dots, g_s\}$ of ideal I is called *Groebner basis*, if

$$\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle.$$

Lemma 2. *Fix a monomial order $>$ on $\mathbb{N}_0^n$ and let $f_1, \dots, f_n \in k[x_1, \dots, x_n]$. Then every $f \in k[x_1, \dots, x_n]$ can be writen as*

$$f = a_1 f_1 + \cdots + a_n f_n + r,$$

where $r, a_i \in k[x_1, \dots, x_n]$ and either $r = 0$ or r is a linear combination of monomials, none of which is divisible by any of $LT(f_1), \dots, LT(f_n)$. We will call r a remainder of f on division by $f_1, \dots, f_n$.

Lemma 3. *Let $G = \{g_1, \dots, g_s\}$ be a Groebner basis of an ideal $I \subset k[x_1, \dots, x_n]$ and $f \in k[x_1, \dots, x_n]$. Then there exists a* unique *$r \in k[x_1, \dots, x_n]$ with the following properties:*

- *No term of r is divisible by any of $LT(g_1), \dots, LT(g_s)$.*
- *There exists $g \in I$ such that $f = g + r$.*

Lemma 4. *Let $f \in k[x_1, \dots, x_n]$ and $G = \{g_1, \dots, g_s\}$ be a Groebner basis of an ideal $I \subset k[x_1, \dots, x_n]$. Then $f \in I$ if and only if the reminder of f on division by G is zero.*

2. Elimination theorem

Theorem 5 (Elimination theorem)**.** *Let $I \subset k[x_1, \dots, x_n]$ be an ideal and let G be a Groebner basis of I with respect to lexicografical order where $x_1 > \cdots > x_n$. Then for every $0 \leq l \leq n$ is the set*

$$G_l = G \cap k[x_{l+1}, \dots, x_n]$$

Groebner basis of the ideal $I_l \cap k[x_{l+1}, \dots, x_n]$.

Cards, Permutations and Quadratic Reciprocity

Jakub Löwit

Given a prime p, it is often interesting to examine the function $\mathbb{Z}_p \to \mathbb{Z}_p$, which maps $x \mapsto x^2$. Especially, one would like to find its image, the set of all *quadratic residues modulo p*. This isn't easy at all, but many general properties of the quadratic residues can be found. In 19th century, Euler conjectured the *Law of Quadratic reciprocity*, which was proved by Gauss fifteen years later. Gauss himself called this result *aureum theorema*, the golden theorem, and he has published 8 different proofs. During the next two centuries, many other unrelated proofs vere found. The goal of this lecture is to show one of them, which is due to *Zolotarev*, and which is especially beautiful and magical.

During the lecture, we shall revisit few basic facts and notions about *permutations*, the *groups* $\mathbb{Z}_p$ *and* $\mathbb{Z}_p*$ and the *quadratic residues*. Our reward will be an elegant algabraic proof of the Quadratic Reciprocity Law.

1. Permutations and their signs

Our proof of Quadratic Reciprocity rests upon the notion of a sign of a permutation, so it is only fair to restate some easy observations about them.

Lemma 1 (Equivalent definitions of signs)**.** *The* sign *of a permutation $\sigma \in S_n$ equals to the parity of*

(1) the number of transpositions in any decomposition of σ

(2) the number of cycles of even length in σ

(3) the number of inversions of σ

Lemma 2. *The* sign *is multiplicative, and it is the only epimorphism $S_n \to \mathbb{Z}_2$.*

2. Groups $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$

Concerning theese object, we only state two well-known facts in very specific form.

Lemma 3 (Chinese Remainder Theorem)**.** *For any coprime $a, b \in \mathbb{N}$, we have $\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b$.*

Lemma 4 (Existence of Primitive Roots)**.** *For every prime p, the group $\mathbb{Z}_p^*$ is cyclic.*

3. Quadratic residues

First, let us revise some notation and basic facts about quadratic residues.

Definition 5 (Legendre symbol)**.** Let p b a prime, $a \in \mathbb{Z}$. Then we define the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if } a \text{ is quadratic resdue modulo } p, \\ -1, & \text{otherwise.} \end{cases}$$

Lemma 6 (Euler's criterion)**.** *For prime $p \geq 3$ and $a \in \mathbb{Z}_p$ we have $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.*

From this, we see the multiplicativity of the Legendre symbol. The following lemma is a consequence of the Euler's criterion.

Lemma 7 (Gauss's lemma)**.** *Let $p \geq 3$ be a prime, $a \in \mathbb{Z}$. We denote by m the number of elements $i \in \mathbb{Z}_p^*$, for which $ia \in \{\frac{p+1}{2}, \ldots, p-1\}$. Then $\left(\frac{a}{p}\right) = (-1)^m$.*

Now, we turn from well-known facts to the approach of Zolotarev.

Lemma 8 (Zolotarev's lemma)**.** *For prime $p \geq 3$ and a coprime with p holds the equality $\left(\frac{a}{p}\right) = \left[\frac{a}{p}\right]$, where the right-hand side stands for the sign of the permutation on $\mathbb{Z}_p$ induced by multiplication with a.*

Theorem 9 (The Law of Quadratic Reciprocity)**.** *For distinct primes p, $q \geq 3$ the following equality holds*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} .$$

So, the theorem shows a connection between "p being a quadratic residue modulo q" and "q being a quadratic residue modulo p". And this connection is not complicated at all – it only depends of the values of p and q modulo 4. So, knowing p, q and whether p is quadratic residue modulo q or not, we can instantly compute whether q is quadratic residue modulo p. The Quadratic reciprocity is a great tool in elementary numer theory. I will not include the proof itself into this abstract, but anyone interested can use the references.

4. References

I would like to thank to Matthew Baker for his wonderful article *The Zolotarev's Magical proof of the Law of the Quadratic Reciprocity*, which was being followed throughout the lecture.

Four squares and universal quadratic forms

Ondrej Bínovský

We shall investigate the problem of representation of positive integers by integral quadratic forms. Our attention is focused especially on the sums of squares. We prove the famous result of Lagrange concerning the representation by four squares. In addition we describe a method for determining the number of representation of integers as a sum of two or four squares. Finally, we mention the 15 and 290 theorems of Conway and Bhargava and the technique of escalation.

Definition 1. A quadratic form $Q(\mathbf{x}) = Q(x_1, \ldots, x_n)$ over the integers is called positive definite if $Q(\mathbf{x}) > 0$ whenever $\mathbf{x} \neq \mathbf{0}$.

Definition 2. A quadratic form $Q(\mathbf{x})$ is said to represent an integer m if there exists $\mathbf{x}$ such that $Q(\mathbf{x}) = m$. $Q(\mathbf{x})$ is called universal if it represents every positive integer.

Theorem 3. *Let p be an odd prime number. Then*

$$\begin{aligned} p = x^2 + y^2 &\quad\Leftrightarrow\quad p \equiv 1 \pmod 4, \\ p = x^2 + 2y^2 &\quad\Leftrightarrow\quad p \equiv 1, 3 \pmod 8, \\ p = x^2 + 3y^2 &\quad\Leftrightarrow\quad p = 3 \text{ or } p \equiv 1 \pmod 3. \end{aligned}$$

In order to prove Theorem 3 we shall require the following two lemmas.

Lemma 4. *For every $x, y, z, w, n \in \mathbb{Z}$ we have*

$$\left(x^2 + ny^2\right)\left(z^2 + nw^2\right) = (xz \mp nyw)^2 + n\,(xw \pm yz)^2$$

Lemma 5. *Suppose that $N = a^2 + nb^2$ with a, b relatively prime. Let $q = x^2 + ny^2$ be a prime divisor of N. Then there exist relatively prime integers c, d such that $\frac{N}{q} = c^2 + nd^2$.*

Next we prove

Theorem 6 (Lagrange)**.** *Every positive integer is the sum of four squares.*

We need the following identity which expresses the fact that the norm of quaternions is multiplicative.

Lemma 7. *The following identity holds*

$$\begin{aligned} &(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &\quad = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &\quad + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad + (x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2)^2 \\ &\quad + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 \end{aligned}$$

We can determine the number of representation of a positive integer as the sum of two or four squares. In fact we have

Theorem 8. *The number of integral solutions (x, y), $x > 0$, $y \geq 0$ to the equation $x^2 + y^2 = n$ is $\sum_{d|n} \chi(d)$, where $\chi(n)$ is the nontrivial Dirichlet character modulo 4. In other words the number of solutions is the excess of positive divisors of n of the form $4k + 1$ over those of the form $4k + 3$.*

It is easily seen that the total number of representations as a sum of two squares of a positive integer n is $4\sum_{d|n}\chi(d)$. We observe that

$$\left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^2 = \left(1+2\sum_{n=1}^{\infty} q^{n^2}\right)^2 = 1+4\sum_{n=1}^{\infty}\left(\sum_{d|n}\chi(d)\right)q^n$$
$$= 1+4\sum_{d=1}^{\infty}\chi(d)\sum_{k=1}^{\infty} q^{kd} = 1+4\left(\frac{q}{1-q}-\frac{q^3}{1-q^3}+\cdots\right)$$

After squaring the identity and transforming the right hand side (which is nontrivial but elementary) we obtain a formula for the number of representations of a positive integer as a sum of four squares.

Corollary. *The number of representations of a positive integer n as a sum of four squares is $8\sum_{d|n} d$ or $24\sum_{d|n,d\ \mathrm{odd}} d$, according to whether n is odd or even.*

Theorem 9 (15)**.** *A quadratic form with integer matrix is universal if it takes the values $1, 2, \ldots, 15$.*

Theorem 10 (290)**.** *A positive definite quadratic form is universal if it takes the values $1, 2, \ldots, 290$.*

Universal quadratic forms over number fields

Kristýna Zemková

This talk is focused on universal quadratic forms with coefficients in the ring of integers of a number field. After a necessary introduction, some known results will be presented; mostly for quadratic number fields. Finally, a construction of a universal quadratic form in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ will be shown; the last part is a joint work with Martin Čech, Dominik Lachman, and Josef Svoboda.

1. Introduction

By a *number field* K we understand any algebraic extension of $\mathbb{Q}$ of finite degree; therefore, every element of K is a root of a polynomial with coefficients in $\mathbb{Q}$. The *ring of integers* $\mathcal{O}_K$ of a number field K consists of all algebraic integers from K, i.e. the elements of $\mathcal{O}_K$ are exactly the elements of K which are roots of monic polynomials with coefficients in $\mathbb{Z}$.

Definition 1. An element $\alpha \in K$ is said to be *totally positive*, denoted $\alpha \succ 0$, if $\sigma(\alpha) > 0$ for all embeddings $\sigma\colon K \hookrightarrow \mathbb{R}$. The set of totally positive elements of $\mathcal{O}_K$ is denoted by $\mathcal{O}_K^+$.

A *quadratic form over* K is a homogeneous polynomial of degree 2 with coefficients in $\mathcal{O}_K$. A quadratic form is called *classical* if all off-diagonal coefficients are divisible by 2 (then all the entries of the corresponding matrix are elements of $\mathcal{O}_K$), and *diagonal* if all off-diagonal coefficients are 0 (and hence the corresponding matrix is diagonal). A quadratic form $Q(\mathbf{x}) = \sum \alpha_{ij} x_i x_j$ is *totally positive definite* if $\sigma(Q)(\mathbf{x}) = \sum \sigma(\alpha_{ij}) x_i x_j$ is positive definite for all embeddings $\sigma\colon K \hookrightarrow \mathbb{R}$.

Definition 2. A quadratic form $Q(\mathbf{x})$ is *universal* if it represents all the elements of $\mathcal{O}_K^+$, i.e. if for every $\gamma \in \mathcal{O}_K^+$ there exist $c_i \in \mathcal{O}_K$, $i = 1, \dots, n$, such that $\gamma = Q(c_1, \dots, c_n)$.

2. Known results

Theorem 3 (Siegel, 1945)**.** *Let K be a totally real number field different from $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$. Then $\sum_{i=1}^{n} x_i^2$ is not universal for any n.*

Theorem 4 (Kim, 2000)**.** *Let $K = \mathbb{Q}(\sqrt{n^2-1})$, n^2-1 square-free, and let ϵ be the totally positive fundamental unit. Then the octonary diagonal form*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + \epsilon x_5^2 + \epsilon x_6^2 + \epsilon x_7^2 + \epsilon x_8^2$$

is universal over $\mathcal{O}_K$.

Theorem 5 (Blomer-Kala, 2015)**.** *Given any positive integer M, there exist infinitely many real quadratic fields that do not admit (classical) universal quadratic forms in M variables.*

Theorem 6 (Blomer-Kala, 2017)**.** *Let $K = \mathbb{Q}(\sqrt{D})$ and denote by $m_{diag}(D)$ the smallest integer m such that there exists a universal quadratic form*

$$Q(x_1, \dots, x_m) = a_1 x_1^2 + \cdots + a_m x_m^2, \qquad a_i \in \mathcal{O}_K^+.$$

Then

$$m_{diag}(D) \leq 8M_D,$$

where M_D is a constant given as a sum of the coefficients of the associated continued fraction.

Moreover, there is

$$M_D \leq c\sqrt{D}(\log D)^2$$

for an absolute constant $c > 0$.

3. Universal quadratic forms over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Definition 7. An element $\alpha \in \mathcal{O}_K$ is called *indecomposable* if it cannot be written as $\alpha = \beta + \gamma$ with $\beta, \gamma \in \mathcal{O}_K^+$. Equivalently, $\alpha \in \mathcal{O}_K$ is indecomposable if there does not exist any $\delta \in \mathcal{O}_K^+$ such that $\delta \prec \alpha$.

Proposition 8. *Any classical totally positive definite universal quadratic form over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has at least 4 variables.*

References

[BK1] V. Blomer, V. Kala, *Number fields without universal n-ary quadratic forms*, Math. Proc. Cambridge Philos. Soc. 159 (2015), 239-252

[BK2] V. Blomer, V. Kala, *Arity of universal quadratic forms over real quadratic fields*, preprint

[Ka] V. Kala, *Universal quadratic forms and elements of small norm in real quadratic fields*, Bull. Aust. Math. Soc. 94 (2016), no. 1, 7–14.

[Ki] B. M. Kim, *Universal octonary diagonal forms over some real quadratic fields*, Commentarii Math. Helv. 75 (2000), 410-414

[Sie] C. L. Siegel, *Sums of m-th powers of algebraic integers*, Ann. Math. 46 (1945), 313-339

Applications of Cryptography in Blockchain technology

Igor Eržiak

The invention of blockchain has led to creation of bitcoin and other cryptocurrencies. This was possible thanks to a couple of interesting cryptographic primitives namely *hash functions* and *digital signatures*.

In this lecture I would like to introduce the basic building blocks of the blockchain technology. Emphasis will be given on how cryptographic primitives can be used to build digital assets with similar (or better) properties as physical assets.

Definition 1. Cryptographic hash function is a function $\mathrm{h}\colon \{0,1\}^* \longrightarrow \{0,1\}^n$ with following properties:

- given a hash $x \in \{0,1\}^n$ it is hard to find a message $m \in \{0,1\}^*$ such that $x = \mathrm{h}(m)$
- given a message $m_1 \in \{0,1\}^*$ it is hard to find a different message $m_2 \in \{0,1\}^*$ such that $\mathrm{h}(m_1) = \mathrm{h}(m_2)$
- it is hard to find messages $m_1, m_2 \in \{0,1\}^*$ such that $\mathrm{h}(m_1) = \mathrm{h}(m_2)$

Definition 2. Digital signature scheme is a triple (G, S, V) where:

(1) G is a key generation algorithm that, given a security parameter, outputs a keypair (private key, public key)

(2) S is a signing algorithm that, given a message and a private key, outputs a signature.

(3) V is a verification algorithm that, given a message, signature and a public key, outputs *true* if the signature is valid and *false* otherwise.

Moreover it has to satisfy that:

- Verification is valid if and only if the message was signed using the private key corresponding to the given public key
- It is hard to impersonate someone, i.e. create a valid signature in the name of someone else without the knowledge of his/her private key

Definition 3. Blockchain is a continuously growing list of records – blocks. Each block contains:

- data (specific to the blockchain application)
- time-stamp
- hash pointer to the previous block

Annihilators of the minus class group of an imaginary cyclic field

Pavel Francírek

Annihilators can be very useful when solving diophantine equations. This was demonstrated by Preda Mihăilescu who proved Catalan's conjecture in 2002. Annihilators can also help us to obtain some information about the ideal class group. In this talk we shall provide some tools from algebraic number theory that are needed to understand the essence of annihilating the ideal class group. Most of the presented results are classical, except the last theorem which is an original result of the author.

1. The ideal class group

Definition 1. A subfield F of the complex numbers is called a *number field* if the degree $[F : \mathbb{Q}]$ is finite.

Definition 2. Let $A \subseteq \mathbb{C}$ be the ring of all algebraic integers. Let F be a number field. The *ring of algebraic integers of* F, denoted by $\mathcal{O}_F$, is the intersection $A \cap F$.

The ring $\mathcal{O}_F$ is not a UFD generally, but it has a property that is almost as good:

Proposition 3. *Every ideal* $\mathfrak{a}$ *of* $\mathcal{O}_F$ *different from* (0) *and* (1) *admits a factorization*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_i$ *of* $\mathcal{O}_F$ *which is unique up to the order of factors.*

Definition 4. A nonzero finitely generated $\mathcal{O}_F$-submodule of F is called a *fractional ideal* of $\mathcal{O}_F$. A fractional ideal with one generator is a *principal fractional ideal* of F.

Note. From now on, (fractional) ideals of $\mathcal{O}_F$ will be referred as ideals of F and principal (fractional) ideals of $\mathcal{O}_F$ will be referred as principal ideals of F.

Let us denote I_F and P_F the set of all ideals of F and the set of all principal ideals of F, respectively. Two ideals of F can be multiplied in the usual way and this operation makes I_F into an abelian group with P_F being its subgroup. The group $\mathcal{C}\ell(F) = I_F/P_F$ is called the *ideal class group* of F. This group is finite and its size $h = |\mathcal{C}\ell(F)|$ is called the *class number* of F.

2. Annihilators of the ideal class group

Definition 5. A number field K is *abelian* if $K/\mathbb{Q}$ is a Galois extension whose Galois group $\mathrm{Gal}\,(K/\mathbb{Q})$ is abelian. When the Galois group is also cyclic, the field K is also called *cyclic*.

Proposition 6. *Let* K *be an abelian field of degree* $n = [K : \mathbb{Q}]$. *Let* p *be an arbitrary prime number. Then there exist (unique) positive integers* $e_K(p)$ *and* $g_K(p)$ *such that*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_K(p)}\mathfrak{p}_2^{e_K(p)} \cdots \mathfrak{p}_{g_K(p)}^{e_K(p)},$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{g_K(p)}$ *are distinct prime ideals of* K. *Moreover,* $e_K(p)g_K(p)$ *divides* n.

Definition 7. We say that a prime number p *ramifies* in K if $e_K(p) > 1$, otherwise p is *unramified* in K.

For any positive integer n let $\zeta_n = e^{2\pi i/n}$. The n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ will be denoted by $\mathbb{Q}_n$.

Theorem 8 (Kronecker-Weber)**.** *If $K/\mathbb{Q}$ is a finite abelian extension, then $K \subseteq \mathbb{Q}_n$ for some n.*

The smallest n with this property is called the *conductor* of K.

Theorem 9. *Let K be an abelian field, K^+ its maximal real subfield, and let h and h^+ be the respective class numbers. Then h^+ divides h.*

The quotient $h^- = \frac{h}{h^+}$ is called the *relative class number* of K.

The Galois group $\mathrm{Gal}\,(K/\mathbb{Q})$ acts on ideals of K, so the ideal class group $\mathcal{C}\ell(K)$ is actually a module over the group ring $\mathbb{Z}[\mathrm{Gal}\,(K/\mathbb{Q})]$. Elements of $\mathbb{Z}[\mathrm{Gal}\,(K/\mathbb{Q})]$ that annihilate $\mathcal{C}\ell(K)$, are called *annihilators* of the class group. In other words, an annihilator of the class group is an element γ such that $\mathfrak{a}^\gamma$ is principal for every ideal $\mathfrak{a}$ of K.

For each $n \in \mathbb{N}$ we define *Stickelberger element* as

$$\theta_n = \sum_{\substack{a \pmod n \\ (a,n)=1}} \left\langle \frac{a}{n} \right\rangle \sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q})],$$

where $\langle x \rangle$ denotes the fractional part of the real number x and $\sigma_a \in \mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q})$ is given by $\sigma_a(\zeta_n) = \zeta_n^a$. Let K be an abelian field of conductor f. We define $\theta'_f = \mathrm{res}_{\mathbb{Q}_f/K}\theta_f$, where

$$\mathrm{res}_{\mathbb{Q}_f/K} \colon \mathbb{Q}[\mathrm{Gal}\,(\mathbb{Q}_f/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}\,(K/\mathbb{Q})]$$

is the ring homomorphism induced by the usual restriction $\mathrm{res}_{\mathbb{Q}_f/K} \colon \mathrm{Gal}\,(\mathbb{Q}_f/\mathbb{Q}) \to \mathrm{Gal}\,(K/\mathbb{Q})$.

Theorem 10 (Stickelberger)**.** *Let $\mathfrak{a}$ be a fractional ideal of K, let $\beta \in \mathbb{Z}[G]$, and suppose that $\beta \cdot \theta'_f \in \mathbb{Z}[G]$. Then $\mathfrak{a}^{\beta\cdot\theta'_f}$ is principal.*

3. Imaginary cyclic fields

We fix an odd prime ℓ. Let L be an imaginary cyclic field satisfying $\ell \mid [L : \mathbb{Q}]$. We can take L as the compositum of a real cyclic field K of ℓ-power degree and an imaginary cyclic field F, $\ell \nmid r = [F : \mathbb{Q}]$. We have $[K : \mathbb{Q}] = \ell^k$ for some $k \in \mathbb{N}$. Let us denote f and m the conductors of F and K, respectively. We further assume

- ℓ does not ramify in L (so $\ell \nmid fm$),
- $\gcd(m, f) = 1$ (so fm is the conductor of L).

Let $p_1, \ldots, p_t$ be the primes ramified in $K/\mathbb{Q}$. We set $I = \{1, \ldots, t\}$. Let us denote $\mathrm{Gal}\,(L/\mathbb{Q})$ by G. The ℓ-Sylow subgroup $\mathcal{C}\ell(L)_\ell$ of the ideal class group of L forms a $\mathbb{Z}_\ell[G]$-module. The elements

$$e^+ = \frac{1+\tau}{2} \qquad \text{and} \qquad e^- = \frac{1-\tau}{2},$$

where τ is the complex conjugation, form a full set of orthogonal idempotents. This gives us the following decomposition

$$\mathcal{C}\ell(L)_\ell = e^-\mathcal{C}\ell(L)_\ell \oplus e^+\mathcal{C}\ell(L)_\ell.$$

The minus part $e^-\mathcal{C}\ell(L)_\ell$ will be denoted by $\mathcal{C}\ell(L)_\ell^-$.

For each $n \in \mathbb{N}$ we define $\theta'_n = \mathrm{cor}_{L/\mathbb{Q}_n\cap L}\mathrm{res}_{\mathbb{Q}_n/\mathbb{Q}_n\cap L}\theta_n$, where the linear map

$$\mathrm{cor}_{L/\mathbb{Q}_n\cap L}\colon \mathbb{Q}[\mathrm{Gal}\,(\mathbb{Q}_n \cap L/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}\,(L/\mathbb{Q})]$$

is defined for $\sigma \in \mathrm{Gal}\,(\mathbb{Q}_n \cap L/\mathbb{Q})$ by

$$\mathrm{cor}_{L/\mathbb{Q}_n\cap L}(\sigma) = \sum_{\tau|_{\mathbb{Q}_n\cap L}=\sigma} \tau,$$

where the sum is taken over all automorphisms $\tau \in \mathrm{Gal}\,(L/\mathbb{Q})$ whose restriction to $\mathbb{Q}_n \cap L$ is σ. Let S' be the submodule of $\mathbb{Q}_\ell[G]$ generated by θ'_n for all $n \in \mathbb{N}$. We set $S = \mathbb{Z}_\ell[G] \cap S'$.

Theorem 11 (Sinnott)**.** *Ideal S annihilates $\mathcal{C}\ell(L)_\ell^-$.*

Let $\mathcal{I} = e^-S = \{e^-s; s \in S\}$.

Theorem 12 (Sinnott)**.** *The ideal $\mathcal{I}$ has a finite index in $\mathbb{Z}_\ell[G]^- = e^-\mathbb{Z}_\ell[G]$. This index is equal to*

$$h_\ell^- = \ell^{\mathrm{ord}_\ell(h^-)},$$

where h^- is the relative class number of L.

The group $\mathcal{C}\ell(L)_\ell^-$ is also annihilated by $e^+\mathbb{Z}_\ell[G]$, so

$$\mathcal{I} \oplus e^+\mathbb{Z}_\ell[G] \subseteq \mathrm{Ann}_{\mathbb{Z}_\ell[G]}\big(\mathcal{C}\ell(L)_\ell^-\big).$$

Question: Are there any other annihilators of $\mathcal{C}\ell(L)_\ell^-$?

We managed to construct (explicitly) an ideal $\mathcal{J}$, $\mathcal{I} \subseteq \mathcal{J} \subseteq \mathbb{Z}_\ell[G]^-$ and we proved that $\mathcal{J}$ annihilates $\mathcal{C}\ell(L)_\ell^-$. Morevover, we were able to compute the relative index $[\mathcal{J} : \mathcal{I}]$:

Theorem 13. *For each $j \in \{1, \dots, k\}$ and $s \in \mathbb{N}$ we define*

$$a_s^{(j)} = \begin{cases} |\{i \in I; e_K(p_i) > \ell^{k-j}\}|, & \text{for } s = 1 \\ \max\big\{|\{i \in I; e_K(p_i) > \ell^{k-j}, s \mid g_F(p_i)g_K(p_i)\}| - 1, 0\big\}, & \text{else.} \end{cases}$$

The ideal $\mathcal{J}$ annihilates $\mathcal{C}\ell(L)_\ell^-$ and the relative index $[\mathcal{J} : \mathcal{I}]$ is given by the formula

$$[\mathcal{J} : \mathcal{I}] = \ell^a,$$

where

$$a = \sum_{\substack{u|r \\ \frac{r}{u} \text{ is odd}}} \left(\varphi(u) \sum_{j=1}^{k} a_u^{(j)} + \varphi(u) \sum_{\substack{n|\ell^{k-1} \\ n\neq 1}} \left(\frac{n}{\ell}(\ell-1) \sum_{j=1}^{k} a_{un}^{(j)} \right) \right).$$

For example, if there are at least two primes p_1, p_2 that ramify in K, and $g_F(p_1) = g_F(p_2) = r$ then $\mathcal{J}$ is larger than $\mathcal{I}$ (there are new annihilators).

Putting Theorem 12 and Theorem 13 together we obtain the following corollary:

Corollary. *The relative class number of L is divisible by ℓ^a.*

Inscribing polygons into Jordan curves

Tomáš Ye

In 1911, German mathematician Otto Toepltitz conjectured that on every closed, simple curve in the Euclidean two dimensional space there can be found four points which are the vertices of a square. To this day, proving the general case or finding a counterexample to it is an open problem. However, if we slightly weaken the conclusion, particularly, if we only demand the four points to form a rectangle, then there exists a beautiful solution that combines geometrical and topological reasoning in a very nontrivial manner.

1. Stating of the inscribed rectangle problem

Definition 1. Let a, b be real numbers, $a < b$. A map $\gamma\colon [a,b] \to \mathbb{R}^2$ is called a *Jordan curve* if

(1) γ is continuous on $[a,b]$
(2) $\gamma(a) = \gamma(b)$
(3) γ is one-to-one on $[a,b)$

Theorem 2 (Vaughan 1977)**.** *Let γ be a Jordan curve. Then in the image of γ, there exist four distinct points which are the vertices of a rectangle.*

Remark 3. The main topic of the talk will be to introduce some topological concepts and then use them to convince the audience that the theorem stated above indeed holds true.

Remark 4. It is only assumed that γ is continuous. However, there exist continuous curves that are differentiable nowhere. Therefore, we cannot a priori assume anything about it's differentiability. One might think, that he does not need to limit himself only to the general case. It seems that if one can prove the theorem for a dense enough family of well-behaved curves, the ugly curves can be expressed as limits of sequences of nicer curves with rectangles inscribed in them. Though it is true, that the limit of a sequence of rectangles is a rectangle, it so far seems impossible to make sure, that the limiting rectangles do not collapse into a single point or a line segment, even in the case of smoother curves. Hence, the limiting arguments fails to reach the desired conclusion here. This makes the problem unsolvable using only the tools of differential geometry. Since the only assumption we have is continuity, it feels natural to look for help in the field of topology, because here continuous maps are the main objects of concern.

2. Topological ingredients

Remark 5. I do not want to bore the audience with proving abstract lemmas about homeomorphisms. Therefore I shall only present the necessary topological facts needed for proving Theorem 2 and omit their proofs.

Definition 6. Let X and Y be topological space. A map $f\colon X \to Y$ is called a *homeomorphism* if

(1) f is one-to-one and onto
(2) f is continuous (in the topological sense i.e. it preserves open sets)
(3) f^{-1} is continuous

Fact 1. Let X and Y be topological spaces and let map $f\colon X \to Y$ to be continuous, one-to-one and onto. If X is compact and Y is a Hassdorf space then f is a homeomorphism.

Remark 7. We will be only working with nice compact and Haussdorf manifolds, therefore to prove a space is homeomorphic to its image through some map f, we only need to show that f is one-to-one and continuous.

Fact 2 (Gluing lemma)**.** Let X and Y be topological spaces and let A and B be closed subsets of X such that $X = A \cup B$. If $f\colon A \to Y$ and $g\colon B \to Y$ are continuous and $f(x) = g(x)\ \forall x \in A \cap B$, then the map $h\colon X \to Y$ defined by

$$h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B \end{cases}$$

is a continuous map from X to Y.

Definition 8. A topological space is called a *manifold* if every point has a neighborhood homeomorphic to R^k for some fixed integer k.

Pseudo-definition 9 (Manifold orientation)**.** I am aware that here I am on somewhat unstable grounds. *Orientation* of a manifold is a property that is defined precisely using algebraic topology which is a field I am not that familiar with, yet. Intuitively, if a manifold is smooth, having an orientation means to have a continuous choice of the unit normal vector all over the manifold. If a manifold is closed, being orientable means that there is a clear distinction between the interior and the exterior of the manifold.

Remark 10. For the purpose of proving Vaughan's theorem, I will be using these two intuitive (but nontrivial) facts about orientation.

(1) Orientability is preserved by homeomorphisms
(2) The Mobius strip is not orientable and every manifold containing a part homeomorphic to the Mobius strip is not orientable.

3. Sketch of the proof

Let us reparametrize γ on the interval $[0, 1]$. Consider the set

$$M = \{[x, y]\colon 0 \le x \le 1,\ 0 \le y \le x\}\,.$$

Then M is the set of all unordered pairs $\{x, y\}$ and all singletons $\{x\}$ from $[0, 1]$ (Right angled triangle in the first quadrant). Now consider the equivalence $\sim$ defined on the unit interval like this: $[x, 0] \sim [1, x]$. We are basically gluing the legs of the right triangle M in a special way. One can show, that the $M/\sim$ is homeomorphic to the Mobius band. Now consider the map

$$\begin{aligned} f\colon M/\sim\ &\to \mathbb{R}^2 \times \mathbb{R} \\ [\ [x, y]\ ]_\sim &\mapsto \left[\ \frac{\gamma(x) + \gamma(y)}{2}\ ,\ \|\gamma(x) - \gamma(y)\|\ \right]. \end{aligned}$$

Because γ is Jordan, f is well defined and continuous. Then f maps the Mobius band $M/\sim$ onto some kind of a manifold in $\mathbb{R}^3$. The image of f is some surface in $\mathbb{R}^3$ and its border (the image of the line containing the point $[x, x]$) is glued to the curve γ.

It can be shown that if f is one to one, than we can construct a homeomorphism from the real projective plane (which is not orientable) to a closed compact manifold in $\mathbb{R}^3$ which orientable is. This will be a contradiction. So f must glue together two distinct pairs of points. Hence, we found two distinct pairs of points, such that they share a midpoint and all have the same distance from that midpoint. Then these four points must be the vertices of a rectangle.

RSA in post-quantum world

Jiří Pavlů

RSA is today one of the most well-known and widely used public key cryptography algorithms. However, with the possibility of scalable quantum computers becoming a reality, there is a widespread belief that it will be totally destroyed (via Shor's algorithm) since breaking it reduces to factoring.

But is it really true? We actually only know that it would break RSA and other currently used algorithms *as they are used on the internet today*. So the question needn't actually be: What other scheme will we use? But instead we can just ask – are we able to tune the RSA scheme in such a way that it won't be vulnerable to quantum attacks? And would it still be usable?

So in the presentation following things will be discussed:

- Disadvantages of Shor's algorithm.
- Other factoring algorithms.
- Computational complexity of different parts of RSA scheme and the cost of breaking it.
- The possibility of still making RSA viable thanks to fine-tuning its parameters.
- The limits of such RSA scheme.

We will thus see, that maybe RSA isn't quite dead yet. And that with very careful analysis we can make even "broken" schemes still useful and safe.

Cracking linear congruential generators

Pavel Surý

Linear congruential generators are among the oldest and simpliest ways to generate pseudo-random numbers. We will show that this approach is unsuitable for cryptography, because a sequence of generated numbers provides enough information to reveal the secret (modulus and coefficient).

Moreover, we will show that there exists a reasonably small system of hyperplanes that contains all the sequences of n generated values (represented as points in $\mathbb{R}^n$), which might come up as an issue even in Monte Carlo applications (consecutive values are not fully random, but have a fairly simple structure).

1. Definitions

Let $m \in \mathbb{N}$ (*modulus*), $k \in \mathbb{N}$ (*coefficient*), $r_0 \in \mathbb{N}, r_0 < m$ (*initial seed*). We define $r_i \in \mathbb{N}$ recursively by:

$$r_i = kr_{i-1} \mod m.$$

The sequence (r_i) will be called *output of the linear congruential generator*. We denote $u_i = r_i/m \in [0,1)$ (*normalised i-th value*). Now, fix $n \in \mathbb{N}$ (*dimension*) and denote $\pi_i = (u_i, \ldots, u_{i+n-1}) \in [0,1)^n$ (*i-th point in n-dimensional unit hypercube*).

2. Values fall into hyperplanes (Marsaglia G., 1968)

Theorem 1. *Let $c_0, \ldots, c_{n-1}$ be integers with the property*

$$c_0 + c_1 k + c_2 k^2 + \cdots + c_{n-1} k^{n-1} \equiv 0 \mod m. \tag{1}$$

Then, for all i, there exists $z \in \mathbb{Z}$ such that π_i lies in the hyperplane

$$c_0 x_0 + c_1 x_1 + \cdots + c_{n-1} x_{n-1} = z. \tag{2}$$

Observation 2. *There are at most $|c_0| + \cdots + |c_{n-1}|$ hyperplanes intersecting the unit cube.*

Theorem 3. *There is a choice of $c_0, \ldots, c_{n-1}$ (some of them non-zero) such that $|c_0| + \cdots + |c_{n-1}| \leq (n!m)^{1/n}$.*

3. Cracking a linear congruential generator

Assume we have a LCG. We consider a modulus and a coefficient as our secret, and generate four consecutive values r_0, r_1, r_2, r_3.

Observation 4. *Modulus divides $q = |(r_2 - r_1)^2 - (r_3 - r_2)(r_1 - r_0)|$.*

This way, we may approximate the modulus. We can factorise q (or $GCD(q_1, \ldots, q_i)$ if we have more than four values) and check the congruential relation with Euclid's algorithm for each suspected $\tilde{m}$.

When will computers master the math?

Miroslav Olšák

We will discuss the artificial intelligence (neural networks), formal theorem provers and possible future connections and challenges. We outline the basic ideas behind Alpha Go, the computer that has beaten humans in the game of Go, convolutional neural networks and reinforcement learning. We continue with the formal math language and ideas how these two disciplines can be combined.

1. Neural networks

Neural net is a differentiable function with multiple inputs, usually multiple outputs and many inner coefficients.

Convolutional neural net is a special type of neural net used for image recognition. The idea of convolutional layer in neural net is to use the same function in every part of the picture (pictures should be invariant translation).

Supervised training of a neural net is the process of setting the inner coefficient so that it gives on average the most appropriate answers to prepared inputs.

Reinforcement learning is a process of setting the coefficients with the purpose of maximizing the returns in an environment (say a computer game) controlled by the neural net.

2. Formal math

HOL (higher order language) is a typed language covering a basic yet general lambda calculus. There are 4 basic types of symbols – variables, constants, abstraction symbol and application symbol.

Application is just a simple function application – it receive a function $f\colon A \to B$ and an element $x \in A$ and returns the $f(x)$.

Lambda abstraction, on the other hand, makes functions. It receives the bounded variable and the body of the function and returns the appropriate function. For example, the function $\lambda_x(2x)$ is the function that doubles its input. So for example $(\lambda_x(2x))(3) = 6$.

The connection-based proving goes in the following way. We start with the negation of the statemtnt we want to prove. In every step we have a disjunction, say $\phi \vee \ldots$. Using an axiom $\psi_1 \vee \psi_2 \vee \ldots \vee \psi_k \vee \neg\phi$, we can replace ϕ by $\psi_1 \vee \psi_2 \vee \ldots \vee \psi_k$ (if $k = 0$ we just erase the ϕ) Our goal is to eliminate all the clauses in the disjunction.

Schedule

Thursday 9th.

8:30 *Breakfast*

9:46 *Arrival*

11:00 **Adolf Středa**:
Low-Communication Parallel Quantum Multi-target preimage search

11:45 **Barbora Hudcová**: Avoiding additive cubes

12:45 *Lunch*

14:00 **Jana Bartoňová**:
Profinite semigroups and their importance in the theory of regular languages

14:45 **Martin Čech**:
Euclidean proofs of Dirichlet's Theorem about primes in arithmetic progressions

15:30 *Coffee break*

15:50 **Ivana Trummová**: Variations of Pappos's theorem

16:35 **Lukáš Kubej**:
Groebner basis and solutions of a system of polynomial equations

17:20 *Break*

17:30 **Jakub Löwit**: Cards, Permutations and Quadratic Reciprocity

19:00 *Dinner*

Friday 10th.

8:30 *Breakfast*

9:30 **Ondrej Bínovský**: Four squares and universal quadratic forms

10:15 **Kristýna Zemková**: Universal quadratic forms over number fields

11:00 *Coffee break*

11:15 **Igor Eržiak**: Applications of Cryptography in Blockchain technology

12:00 **Pavel Francírek**:
Annihilators of the minus class group of an imaginary cyclic field

13:00 *Lunch*

19:00 *Dinner*

Saturday 11th.

8:30 *Breakfast*

9:30 **Tomáš Ye**: Inscribing polygons into Jordan curves

10:15 **Jiří Pavlů**: RSA in post-quantum world

11:00 *Coffee break*

11:15 **Pavel Surý**: Cracking linear congruential generators

12:00 **Miroslav Olšák**: When will computers master the math?

13:00 *Lunch*

19:00 *Dinner*