Abstrakty

1. Funkcje skrótu – własności, bezpieczeństwo, zastosowania (na przykładzie SHA-256)

Wśród różnorodnych technik kryptograficznych funkcje skrótu stanowią istotny element systemów zabezpieczających dane. Są one niezbędnym narzędziem w procesach uwierzytelniania i integrowania danych, podpisach cyfrowych oraz przechowywaniu haseł w bazach danych. Ich uniwersalność sprawia, że są szeroko stosowane w informatyce. Celem referatu jest omówienie – od strony matematycznej – definicji i podstawowych własności funkcji skrótu, przybliżenie pojęć związanych z bezpieczeństwem tych funkcji, a wreszcie przedstawienie działania i zastosowań funkcji SHA-256. W części pierwszej zajmiemy się podstawami matematycznymi. Następnie, po zdefiniowaniu, czym jest kolizja, sklasyfikujemy ataki na funkcje skrótu; niektórym z tych ataków przyjrzymy się dokładniej. W dalszej części referatu przybliżymy algorytm SHA-256. Zaprezentujemy także program ilustrujący działanie tego algorytmu. Na koniec zajmiemy się pewnymi zastosowaniami SHA-256.

2. Przemytnik z Archipelagu.

Prelekcja oparta o artykuł „Smuggler on the archipelago of islands – a new optimization problem: algorithms and applications” autorstwa Tomasza Kopczewskiego, Eryka Kopczyńskiego i Doroty Celińskiej. W trakcie wykładu przyjrzymy się problemowi optymalizacji zarobku w handlu z barierami, ujmiemy go w kategoriach matematycznych, przeprowadzimy praktyczny eksperyment z aktywnym udziałem słuchaczy oraz zbadamy algorytm znajdujący rozwiązanie tego problemu.

3. Luki pomiędzy sumami dwóch kwadratów.

W referacie zajmuję się badaniem luk pomiędzy kolejnymi elementami zbioru

$$W := \{u^2 + v^2 : (u, v) \neq (0,0), u, v \in Z\}$$

Rozpocznę od przypomnienia najważniejszych twierdzeń i własności dotyczących sumy dwóch kwadratów liczb całkowitych. Następnie przyjrzymy się twierdzeniu, które podaje najlepiej znaną górną granicę maksymalnej luki pomiędzy kolejnymi elementami zbioru (W), uogólniając je do kolejnych elementów zbioru ($W_d := \{u^2 + dv^2 : (u, v) \neq (0,0), u, v \in Z\}$), gdzie ($d \in N^+$). Na koniec przedstawione zostanie twierdzenie mówiące o tym, że dowolna dodatnia liczba naturalna jest długością luki w zbiorze (W) nieskończenie często.

4. Metody równoległego całkowania w czasie dla równań nielokalnych.

Równania nielokalne odgrywają kluczową rolę w modelowaniu wielu zjawisk fizycznych i technicznych, jednak ich numeryczne rozwiązywanie bywa czasochłonne i obliczeniowo złożone. Metoda całkowania równoległego w czasie oferuje nowatorskie podejście, które pozwala na równoczesne przetwarzanie wielu kroków czasowych, znacząco przyspieszając obliczenia. Prezentacja przybliży zasady działania tej metody, jej zastosowania w kontekście równań nielokalnych oraz korzyści płynące z jej wykorzystania w systemach wieloprocesorowych. Zostaną również omówione wyzwania związane z implementacją i optymalizacją tej techniki oraz przykłady praktycznych zastosowań.

5. Jeśli mam wybierać dzięki AC to wolę nie wybierać wcale.

Aksjomat Determinacji (w skrócie AD) jest założeniem mówiącym o istnieniu strategii wygrywających w pewnych grach nieskończonych. Aksjomat ten stanowi swego rodzaju kontrę dla Aksjomatu Wyboru i może zostać przyjęty do systemu Zermelo-Fraenkla (ZF) zamiast wspomnianego Aksjomatu Wyboru (AC). W czasie referatu omówimy, czym są gry nieskończone, i przytoczymy przykład jednej z nich. Zaprezentowany zostanie Aksjomat Determinacji oraz przeanalizujemy konsekwencje, jakie wynikają z jego dodania do systemu ZF zamiast AC. Dodatkowo, na koniec pokażemy, że determinizacja gwarantuje nam pewien rodzaj wyboru.

6. Powody niestabilności grafów cyrkulantnych.

Podczas referatu omówię dotychczasowe podejścia do problemu stabilności dla grafów cyrkulantnych. Stabilność grafu to własność opisująca zachowanie grupy symetrii grafu po ztensorowaniu go z (K_2), czyli grafem składającym się z dwóch wierzchołków połączonych krawędzią. Dla grafu $(\Gamma = (V, E))$,gdzie (V) jest zbiorem wierzchołków, a (E) zbiorem krawędzi, wyżej wspomniany produkt tensorowy można opisać w następujący sposób: $[\Gamma \times K_2 = (V \times \{0,1\}, E_\times)$, gdzie $E_\times = \{((v,i),(w,j)) \mid (v,w) \in E \text{ oraz } i + j = 1\}.]$ Grafy cyrkulantne to grafy, których grupa symetrii zawiera cykliczną podgrupę działającą regularnie na zbiór wierzchołków. Równoważnie można o nich myśleć jako o grafach Cayley'a nad grupą cykliczną. Dotychczas w literaturze pojawiło się kilka hipotez dotyczących charakteryzacji wszystkich niestabilnych grafów cyrkulantnych. Obecnie znane są trzy różne rodziny niestabilnych grafów cyrkulantnych. Warto wspomnieć, że wszystkie znalezione niestabilne grafy cyrkulantne należą do jednej z tych trzech rodzin, jednak komputerowe obliczenia zostały przeprowadzone jedynie dla grafów posiadających nie więcej niż 50 wierzchołków. W dalszej części referatu dowiemy się, jak uogólnić wszystkie wcześniej znane kryteria w jednolity sposób. Postawiona w ten sposób hipoteza wskaże połączenie problemu stabilności dla grafów cyrkulantnych z problemem izomorfizmu między grafami Cayley'a.

7. Jak odróżnić zbiory borelowskie za pomocą gier, czyli o hierarchii Wadge'a.

Zbiory borelowskie stanowią fundamentalny element wielu działów matematyki, obejmując zbiory otwarte, domknięte, klasy (G_δ) i (F_σ), aż po niezwykle złożone zbiory o strukturze (Σ^0_ξ) i (Π^0_ξ). Ale jak bardzo skomplikowane są poszczególne klasy zbiorów? Co to znaczy, że jeden zbiór otwarty jest bardziej złożony od innego? Odpowiedzią jest Hierarchia Wadge'a. Ucząc się, jak wygrać grę Wadge'a, zyskujemy wgląd w strukturę poszczególnych klas zbiorów borelowskich.

8. Regresja procesami gaussowskimi i jej zastosowania w mechanice.

Analiza wypadków samochodowych to kluczowa dziedzina współczesnej medycyny sądowej, a wyniki takich dochodzeń często stanowią istotny dowód w postępowaniach prawnych. Powstaje pytanie: czy na podstawie skutków wypadku można dokładnie przewidzieć prędkość pojazdu przed zderzeniem? Jedną z metod umożliwiających takie prognozy jest regresja procesami gaussowskimi (GPR). Metoda ta pozwala nie tylko na precyzyjne oszacowanie prędkości, ale także na określenie stopnia niepewności tych prognoz, co ma krytyczne znaczenie w analizie i ocenie ryzyka wypadków drogowych.