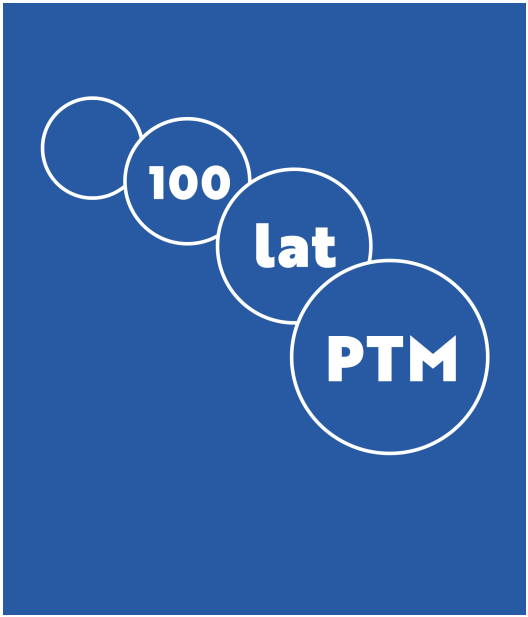

kombinatoryka i kryptografia

patroni sesji: Marian Rejewski,
Jerzy Różycki, Henryk Zygalski

Jubileuszowy Zjazd Matematyków Polskich
w stulecie
Polskiego Towarzystwa Matematycznego
Kraków 3 -7 września 2019

Spis treści

Większościowe kolorowanie grafów

Bartłomiej Bosek
bosek@tcs.uj.edu.pl
Uniwersytet Jagielloński

Jedną z odmian kolorowania grafu jest przypisanie kolorów do wierzchołków takie, że dla każdego wierzchołka v, co najwyżej połowa sąsiadów v ma ten sam kolor co v. Takie kolorowanie nazywamy kolorowaniem większościowym grafu. Celem jest większościowe pokolorowanie grafu za pomocą jak najmniejszej liczby kolorów. Podczas prezentacji zostaną omówione różne warianty tego problemu, wyniki historyczne, najnowsze rezultaty jak i intrygujące wciąż hipotezy. Między innymi zostaną zaprezentowane efekty wspólnej współpracy z Marcinem Anholcerem, Jarosławem Grytczukiem, oraz Gabrielem Jakóbczakiem.

Bibliografia

[1] László Lovász, *On decomposition of graphs* Studia Scientiarum Mathematicarum Hungarica. A Quarterly of the Hungarian Academy of Sciences, 1, 237–238, 1966.

[2] Paul D. Seymour, *On the two-colouring of hypergraphs*, The Quarterly Journal of Mathematics. Oxford. Second Series, 25, 303–312, 1974 https://doi.org/10.1093/qmath/25.1.303.

[3] Dominic van der Zypen, *Majority coloring for directed graphs* MathOverflow, 2016, https://mathoverflow.net/questions/233014/majority-coloring-for-directed-graphs.

[4] Stephan Kreutzer, Sang-il Oum, Paul D. Seymour, Dominic van der Zypen, and David R. Wood, *Majority colourings of digraphs*, Electronic Journal of Combinatorics, 24(2):Paper 2.25, 9, 2017.
http://www.combinatorics.org/v24i2p25.

[5] Marcin Anholcer, Bartłomiej Bosek, Jarosław Grytczuk, *Majority Choosability of Digraphs* Electronic Journal of Combinatorics, 24 (3), Paper 3.57, 2017,
http://www.combinatorics.org/v24i3p57.

[6] António Girão, Teeradej Kittipassorn, Kamil Popielarz, *Generalized majority colourings of digraphs*, Combinatorics, Probability and Computing, 26(6), 850–855, 2017.
https://doi.org/10.1017/S096354831700044X.

[7] Fiachra Knox and Robert Šámal, *Linear bound for majority colourings of digraphs*, Electronic Journal of Combinatorics, 25(3):Paper 3.29, 4, 2018,
http://www.combinatorics.org/v25i3p29.

[8] Bartłomiej Bosek, Jarosław Grytczuk, Gabriel Jakóbczak, *Majority Coloring Game*, Discrete Applied Mathematics, 255, 15 – 20, 2019.
https://doi.org/10.1016/j.dam.2018.07.020.

● Powrót do indeksu abstraktów sekcji

Realization of digraphs in Abelian groups

Sylwia Cichacz
cichacz@agh.edu.pl
Akademia Górniczo-Hutnicza

Co-author:
Zsolt Tuza
mailto:tuza@dcs.uni-pannon.hu
University of Pannonia, Veszprém, Hungary

Suppose that there exists a mapping ψ from the arc set $E(\overrightarrow{G})$ of $\overrightarrow{G}$ to a finite Abelian group Γ such that if we define a mapping φ from the vertex set $V(\overrightarrow{G})$ of G to Γ by

$$\varphi_\psi(x) = \sum_{y \in N^+(x)} \psi(yx) - \sum_{y \in N^-(x)} \psi(xy), \quad (x \in V(G)),$$

then φ_ψ is injective. In this situation, we say that $\overrightarrow{G}$ is *realizable* in Γ.

Let $\overrightarrow{G}$ be a directed graph of order n with no component of order less than 3. So far the problem of realization of digraphs was considered only in case of elementary Abelian groups [1,2]. In this talk we will show that $\overrightarrow{G}$ is realizable in any finite Abelian group Γ such that $|\Gamma| \geqslant 4n$. Moreover if n is sufficiently large for fixed $\varepsilon > 0$ ($n \geqslant n_0(\varepsilon)$) then $\overrightarrow{G}$ is realizable in any Γ such that $|\Gamma| > (1+\varepsilon)n$.

References

[1] Y. Egawa, *Graph labelings in elementary abelian 2-groups*, Tokyo Journal of Mathematics **20**: 365–379

(1997).
[2] Y. Fukuchi, *Graph labelings in elementary abelian groups*, Discrete Mathematics **189**: 117–122 (1998).
● Powrót do indeksu abstraktów sekcji

Lack of Unique Factorization as a Tool in Block Cipher Cryptanalysis

Nicolas T. Courtois
n.courtois@ucl.ac.uk
University College London, Wielka Brytania

Classical attacks on block ciphers are about super simple linear invariants and the space of possible attacks is small. Non-linear polynomial invariants offer a substantially richer space to explore. If so, why is that cryptographers have found so few attacks on block ciphers? Our method it to search for invariant attacks explicitly through the study of roots of the so-called Fundamental Equation (FE). We show that certain properties of the ring of Boolean polynomials such as lack of unique factorization allow for a certain type of product construction attacks to succeed. We show how to construct a complex non-trivial attack where a polynomial of degree 7 is an invariant for any number of rounds for a complex block cipher.

References

[1] Nicolas T. Courtois, Aidan Patrick, *Lack of Unique Factorization as a Tool in Block Cipher Cryptanalysis*, Preprint, https://arxiv.org/abs/1905.04684 12 May 2019.

[2] Nicolas Courtois and Willi Meier: *Algebraic Attacks on Stream Ciphers with Linear Feedback*, Eurocrypt 2003, Warsaw, Poland, LNCS 2656, pp. 345–359, Springer

[3] Nicolas Courtois, *Feistel Schemes and Bi-Linear Cryp-*

tanalysis, Crypto 2004, LNCS 3152, pp. 23–40, Springer, 2004.

● Powrót do indeksu abstraktów sekcji

Metoda wielomianowa dla problemów kolorowania grafów

Przemysław Gordinowicz
pgordin@p.lodz.pl
Politechnika Łódzka

W naturalny sposób z grafem $G = (V, E)$ (formalnie z jego ustaloną orientacją, choć jej wpływ ogranicza się do określenia znaku) można stowarzyszyć *wielomian grafowy* nad zadanym ciałem liczbowym $P(G) = \prod_{uv \in E}(x_u - x_v)$, którego zmienne odpowiadają wierzchołkom grafu, a stopień jest równy $|E|$. Pojęcia grafu i jego wielomianu były w historii utożsamiane. Stąd pochodzi np. pojęcie czynnika (ang. factor) jako uogólnienie skojarzenia doskonałego.

Istotną cechą wielomianu grafowego jest fakt, że niezerujące podstawienie wyznacza kolorowanie grafu. Użytecznym narzędziem jest kombinatoryczne twierdzenie o zerach (Alon, 1999) implikujące istnienie kolorowań z list o długościach o 1 większych od odpowiadających wykładników w dowolnym, nieznikającym jednomianie. Ostatnio Zhu (2019+) zaprezentował inspirujący wynik — uogólnienie twierdzenia Thomassena o 5-wybieralności grafów planarnych w języku wielomianów grafowych.

Podczas referatu zostaną zaprezentowane pewne rozważane warianty twierdzenia Thomassena, w szczególności podany przez Hutchinson (2012) dla grafów zewnętrznie planarnych, a rozszerzony przez Postle i Thomasa (2015, 2016). Przedyskutowane zostanie zastosowanie metody wielomianowej do tych problemów. Przedstawiony będzie także do-

wód 3-wybieralności grafów kolejkowych, uzyskany metodą wielomianową w bardzo podobny sposób to wielomianowego uogólnienia twierdzenia Hutchinson.

Referat opiera się o wyniki uzyskane wspólnie z P. Twardowskim i Z. Wiśniewską (PŁ).

● Powrót do indeksu abstraktów sekcji

Indeks rozróżniający grafów spójnych w zależności od maksymalnego stopnia grafu

Aleksandra Gorzkowska
agorzkow@agh.edu.pl
Akademia Górniczo-Hutnicza w Krakowie

Mówimy, że kolorowanie c *przełamuje* automorfizm φ grafu G, jeśli istnieje co najmniej jedna krawędź grafu G, której kolor jest inny niż kolor jej obrazu w automorfizmie φ. *Indeksem rozróżniającym* $D'(G)$ grafu G nazywamy najmniejszą liczbę d taką, że istnieje kolorowanie krawędziowe grafu G za pomocą d kolorów przełamujące wszystkie nietrywialne automorfizmy tego grafu. Pojęcie to zostało wprowadzone przez Kalinowskiego i Pilśniak. Udowodnili oni, że jeśli graf G rzędu co najmniej trzy jest spójny i skończony, to $D'(G) \leqslant \Delta(G)$, z wyjątkiem grafów C_3, C_4 oraz C_5. Kolejne wyniki, w których podano ograniczenie górne indeksu rozróżniającego w zależności od stopnia maksymalnego grafu doprowadziły do sformułowania przez Woźniaka hipotezy, że jeśli graf G jest spójny o stopniu minimalnym δ, to $D'(G) \leqslant \lceil \sqrt[\delta]{\Delta(G)} \rceil + 1$. Podczas referatu przestawione zostaną rezultaty dotyczące tej hipotezy, głównie w przypadku grafów 3-spójnych.

Bibliografia

[1] R. Kalinowski i M. Pilśniak, *Distinguishing graphs by edge-colourings*, European J. Combin. **45**: 124–131 (2015).
[2] M. Pilśniak, *Improving upper bounds for the distinguishing index* Ars Math. Contemp. **13**: 259–274 (2017).

Powrót do indeksu abstraktów sekcji

Liczby Turána i ich uogólnienia

Andrzej Grzesik
Andrzej.Grzesik@uj.edu.pl
Uniwersytet Jagielloński

Klasycznym zagadnieniem teorii grafów ekstremalnych jest znalezienie maksymalnej możliwej liczby krawędzi w grafach, które nie zawierają ustalonego podgrafu. Ponad 110 lat temu Mantel rozwiązał ten problem dla trójkąta, w 1941 roku Turán dla grafów pełnych, a w 1946 roku Erdős i Stone roztrzygnęli go asymptotycznie dla dowolnego grafu, który nie jest dwudzielny. Brakujący przypadek pozostaje problemem otwartym i często nawet rząd wielkości maksymalnej liczby krawędzi w takich grafach nie jest znany.

Jedną z istotnych hipotez w tym temacie jest hipoteza Erdősa z 1967 roku, która mówi, że każdy graf na n wierzchołkach bez dwudzielnego r-zdegenerowanego podgrafu F ma co najwyżej $Cn^{2-\frac{1}{r}}$ krawędzi, gdzie C jest pewną stałą zależną tylko od F. Na wykładzie zostaną przedstawione wyniki uzyskane ze współpracownikami (Oliver Janzer oraz Zoltán Lóránt Nagy), które udowadniają hipotezę Erdősa dla szerokiej klasy grafów, uogólniając wiele wcześniejszych rezultatów.

Omawiane zagadnienie można uogólnić na problem maksymalizacji nie liczby krawędzi, ale liczby kopii pewnego ustalonego grafu. W tym temacie wiadomo jeszcze mniej i brakuje optymalnych wyników nawet dla małych lub bardzo specyficznych grafów. Na wykładzie zostaną przedstawione wyniki uzyskane wspólnie z Bartłomiejem Kielakiem doty-

cząсe cykli nieparzystej długości.

● Powrót do indeksu abstraktów sekcji

Podpisy pierścieniowe

Lucjan Hanzlik
lucjan.hanzlik@stanford.edu
Stanford University, Kanada

Podpisy pierścieniowe (z ang. ring signatures) [1] pozwalają na wykonanie elektronicznego podpisu w imieniu grupy (tzw. pierścienia) stworzonej w momencie jego generacji. W odróżnieniu od standardowych podpisów tożsamość podpisującego pozostaje ukryta. Zostały one zaproponowane jako anonimowy sposób na wyciek autentycznych (tj. podpisanych) tajemnic jednak, z racji swoich korzyści znalazły zastosowanie w kryptowalutach.

Naturalnym celem jest zaprojektowanie schematu, dla którego długość podpisu jest krótka w wielkości pierścienia. W niniejszej pracy zaprezentujemy pierwszy schemat dla którego:

- długość podpisu jest logarytmiczna w wielkości pierścienia,
- bezpieczeństwo jest oparte o standardowy problem obliczeniowy, a dowód bezpieczeństwa nie wymaga wyroczni losowych i parametrów wygenerowanych przez zaufaną stronę.

Pomimo wielu lat badań w tej dziedzinie, ten problem był ciągle otwarty. Rozszerzamy nasze wyniki na przypadek, w którym podpisy wykonane z użyciem tego samego klucza prywatnego mogą zostać połączone (z ang. linkable ring signatures).

Bibliografia

[1] Ronald L. Rivest, Adi Shamir, and Yael Tauman, *How to leak a secret*, Springer, Heidelberg, 2001.

• Powrót do indeksu abstraktów sekcji

Ekstremalne losowe hipergrafy dla problemu efektywnej dwukolorowalności

Jakub Kozik
Jakub.Kozik@uj.edu.pl
Uniwersytet Jagielloński

Jaka jest minimalna liczba krawędzi, która pozwala na zbudowanie k-grafu (czyli k-jednolitego hipergrafu) który nie byłby dwukolorowalny? Liczba ta, oznaczona przez $m(k)$, została wprowadzona przez Erdősa i Hajnala w roku 1961. Od tego czasu wiele wysiłków poświęcono na wyznaczenie asymptotycznego zachowania funkcji m. Ostatnia poprawa dolnego ograniczenia nastąpiła w roku 2000. Radhakrishnan i Srinivasan udowodnili w [3] ograniczenie dolne na $m(k)$ rzędu $(k/\log(k))^{1/2} \cdot 2^k$. Co ciekawe, najlepsze znane górne ograniczenie $m(k) = O(k^2 \cdot 2^k)$, udowodnione przez Erdősa w roku 1964, nie zostało od tego czasu poprawione. Wynika ono z faktu, że losowy k-graf na k^2 wierzchołkach z dużym prawdopodobieństwem przestaje być dwukolorowalny mniej więcej przy tej liczbie krawędzi. W celu lepszego zrozumienia tego zjawiska, w naszych badaniach skupiamy się na ewolucji przestrzeni poprawnych kolorowań, gdy kolejne losowe krawędzie są dodawane do hipergrafu budowanego nad zbiorem wierzchołków rozmiaru k^2. Jednym z otrzymanych w ten sposób wyników jest konstrukcja i analiza algorytmu, który z dużym prawdopodobieństwem poprawnie koloruje losowe instancje, w których liczba krawędzi jest rzędu $k\log(k) \cdot 2^k$. Wynik ten poprawia ograniczenie rzędu $k \cdot 2^k$ wynikające z pracy [2]. Nasze badania są w dużym stopniu inspirowane

rozważaniami prowadzonymi w kontekście problemów spełnialności więzów dla losowych instancji, w których przyjmuje się, że rozmiar krawędzi k jest stały, a jedynie liczba wierzchołków zmierza do nieskończoności (patrz np. [1]).

Bibliografia

[1] D. Achlioptas and A. Coja-Oghlan, *Algorithmic barriers from phase transitions*, in Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science, FOCS â 08, Washington, DC, USA, 2008.

[2] D. Achlioptas, J.H. Kim, M. Krivelevich and P. Tetali, *Two-colorings random hypergraphs*, Random Structures and Algorithms,20:2, 2002.

[3] J. Radhakrishnan and A. Srinivasan, *Improved bounds and algorithms for hypergraph 2-coloring*, Random Structures and Algorithms, 16, 2000.

● Powrót do indeksu abstraktów sekcji

O pewnych naturalnych strukturach na matroidach i powiązanych problemach algebraicznych

Michał Lasoń
michalason@gmail.com
Polska Akademia Nauk

Gdy obiekt algebraiczny zadany jest kombinatorycznie, naturalne jest przypuszczenie, że jego własności również można opisać kombinatorycznie. Próba uzyskania takiego opisu często prowadzi do zaskakująco trudnych problemów kombinatorycznych. Dobrym przykładem jest hipoteza White'a. Stanowi ona, że ideał toryczny matroidu generowany jest przez dwumiany kwadratowe odpowiadające symetrycznej własności wymiany baz.

Powyższy problem redukuje się do jednego z podstawowych pytań kombinatorycznych dla pewnej naturalnej struktury na matroidzie - struktury uogólniającej dobrze znany graf baz matroidu. Opowiemy o paru wynikach i paru intrygujących problemach otwartych.

Bibliografia

[1] M. Lasoń, M. Michałek, On the toric ideal of a matroid, *Adv. Math.* **259**: 1–12 (2014).

[2] M. Lasoń, On the toric ideals of matroids of a fixed rank, arXiv: 1601.08199.

● Powrót do indeksu abstraktów sekcji

Bezpieczeństwo i wiarygodność sieci neuronowych

Paweł Morawiecki
pawel.morawiecki@gmail.com
Polska Akademia Nauk

W ostatnich kilku latach sztuczne sieci neuronowe pozwalają rozwiązywac coraz trudniejsze problemy z zakresu grafiki czy robotyki. Jednakze bezpieczenstwo i wiarygodność tych algorytmów jest dalekie od ideału. Zwodnicze przykłady (ang. adversarial examples) to dane wejściowe, które zostały tak przygotowane by oszukac klasyfikator (np. sieć neuronową). Dla ludzkiej percepcji takie przykłady nie wydają sie podejrzane, dlatego tez mogą być niebezpieczne. W referacie zostanie przedstawiona metoda generowania takich danych oraz podstawowe metody obrony. Dodatkowo zostanie zaprezentowanych kilka kierunków badan, które wydają się interesujące.

● Powrót do indeksu abstraktów sekcji

O unikaniu repetycji

Barbara Nayar
B.Nayar@mini.pw.edu.pl
Politechnika Warszawska

Przedstawię kilka wyników dotyczących unikania repetycji i innych wzorców w ciągach, unikania repetycji z przeskokami, unikania repetycji na prostych w kolorowaniu płaszczyzny. Zagadnienia te inspirowane są klasycznym wynikiem Thuego o istnieniu dowolnie długiego ciągu bez repetycji nad trzyelementowym alfabetem.

Prezentowane wyniki zostały uzyskane z M. Dębskim, J. Grytczukiem, U. Pastwą, J. Sokół, M. Tuczyńskim, P. Wenusem, K. Węskiem.

Bibliografia

[1] M. Dębski, J. Grytczuk, B. Nayar, U. Pastwa, J. Sokół, M. Tuczyński, P. Wenus, K. Węsek, *Avoiding multiple repetitions in Euclidean spaces*, preprint (2018)

[2] M. Dębski, U. Pastwa, K. Węsek, *Grasshopper Avoidance of Patterns*, Electron. J. Combin. **23** (2016)

● Powrót do indeksu abstraktów sekcji

Ćwierć całkowite pakowanie cyklu

Marcin Pilipczuk
malcin@mimuw.edu.pl
Uniwersytet Warszawski

Powszechnie znanie twierdzenie Erdősa i Pósy głosi, że jeśli w grafie nieskierowanym nie istnieje rodzina k rozłącznych wierzchołkowo cykli, to istnieje w nim zbiór rozcyklający (zbiór wierzchołków przecinający każdy cykl w grafie) wielkości $\mathcal{O}(k \log k)$. Analogiczne stwierdzenie dla grafów skierowanych przez laty było znane jako hipoteza Youngera, aż zostało w 1996 roku udowodnione przez Reeda, Robertsona, Seymoura i Thomasa. W ich dowodzie zależność między wielkością zbioru rozcyklającego i liczbą rozłącznych wierzchołkowo cykli nie jest elementarna.

W pracy razem z Tomášem Masaříkiem, Ireną Muzi, Pawłem Rzążewskim oraz Manuelem Sorge pokazujemy, że otrzymamy zależność wielomianową, jeśli porównamy najmniejszą możliwą wielkość zbioru rozcyklającego z największą możliwą licznością *ćwierć całkowitą* rodziną cykli w grafie. Dowodzimy, że jeśli w skierowanym grafie G nie istnieje rodzina k cykli takich, że każdy wierzchołek G leży na co najwyżej czterech cyklach w rodzinie, to w G można znaleźć zbiór rozcyklający wielkości $\mathcal{O}(k^4)$. Używając opracowanych technik, dowodzimy bardziej ogólnego wyniku dotyczącego ćwierć całkowitego pakowania podgrafów o dużej (skierowanej) szerokości drzewiastej: dla każdych dwóch liczb całkowitych dodatnich a oraz b, jeśli skierowany graf G ma (skierowaną) szerokość drzewiastą $\Omega(a^8 b^8 \log^2(ab))$, to znaj-

dziemy w G rodzinę podgrafów wielkości a, której każdy element ma (skierowaną) szerokość drzewiastą co najmniej b, a każdy wierzchołek G leży w co najwyżej czterech podgrafach z rodziny.

Bibliografia

[1] T. Masařík, I. Muzi, M. Pilipczuk, P. Rzążewski, M. Sorge, *Packing directed circuits quarter-integrally*, arXiv:1907.02494.
`https://arxiv.org/abs/1907.02494`

[2] B. Reed, N. Robertson, P. Seymour, R. Thomas, *Packing directed circuits*, Combinatorica (1996) 16: 535.
`https://doi.org/10.1007/BF01271272`

● Powrót do indeksu abstraktów sekcji

Hipoteza 1–2–3 jest niemal niemal prawdziwa dla grafów regularnych

Jakub Przybyło
jakubprz@agh.edu.pl
Akademia Górniczo-Hutnicza

Znana *hipoteza 1–2–3* sugeruje, iż krawędziom dowolnego grafu bez składowej K_2 można nadać wagi ze zbioru $\{1, 2, 3\}$ tak, by sąsiednie wierzchołki otrzymały różne tzw. ważone stopnie. Problem ten pozostaje nierozwiązany, podczas gdy wiadomo, że jest to możliwe przy użyciu wag ze zbioru $\{1, 2, 3, 4, 5\}$. Hipoteza ta jest ponadto udowodniona dla grafów 3-kolorowalnych. Niewiele więcej wiadomo w przypadku grafów regularnych. Zaprezentuję dowód, iż dla tej rodziny grafów wystarczy wykorzystać jedynie wagi 1, 2, 3, 4; oraz omówię pewne przypadki, w których teza hipotezy 1–2–3 jest w istocie spełniona.

● Powrót do indeksu abstraktów sekcji

Powers of Hamiltonian cycles in randomly augmented graphs

Andrzej Ruciński
rucinski@amu.edu.pl
Uniwersytet im. Adama Mickiewicza w Poznaniu

I will present recent results on the existence of powers of Hamiltonian cycles in graphs with large minimum degree to which some additional edges have been added in a random manner. For all integers $k, \ell, r \geqslant 1$ with $\ell \geqslant (r+1)r$ and any $\alpha > \frac{k}{k+1}$ we show that adding $O(n^{2-2/\ell})$ random edges to an n-vertex graph G with minimum degree at least αn yields, with probability close to one, the existence of the $(k\ell + r)$-th power of a Hamiltonian cycle. In particular, for $r = 1$ and $\ell = 2$ this implies that adding only $O(n)$ random edges to such a graph G already ensures the $(2k+1)$-st power of a Hamiltonian cycle (proved independently by Nenadov and Trujic). In this instance and for several other choices of k, ℓ, and r we can show that our result is asymptotically optimal.

This is joint work with S. Antoniuk (Poznań), A. Dudek (Kalamazoo), Chr. Reiher and M. Schacht (both from Hamburg).

• Powrót do indeksu abstraktów sekcji

Glosowanie przez Internet — ZA i PRZECIW

Marian Srebrny
marians@ipipan.waw.pl
Polska akademia Nauk

Współautorzy:
Artur Jakubski
ajakubski@icis.pcz.pl
Politechnika Częstochowska

Josef Pieprzyk
josef.pieprzyk@qut.edu.au
Queensland University of Technology, Australia

Te wyniki motywowane są przez słynne niedawne wpadki Facebooka. W odpowiedzi ze strony społeczności kryptograficznej artykuł ten skupia się na zaufaniu, bezpieczeństwie sieciowym i prywatności w systemach równoległych i rozproszonych. Kwestie te mają kluczowe znaczenie w dzisiejszych czasach, ponieważ zadania są przydzielane, a informacje są wymieniane między urządzeniami systemu, które mogą należeć do różnych użytkowników. Podkreślamy najnowsze postępy w zakresie zaufania, bezpieczeństwa i prywatności dla powstających systemów równoległych i rozproszonych.

Przedstawiamy nowy projekt protokołu głosowania przez Internetâ weryfikowalnego od początku do końcaâ (ang. End-To-End Verifiable), przeznaczonego dla niewielkiej grupy wyborców. Szczególny nacisk w naszym protokole głosowania dotyczy gwarancji, że każdy głosujący może skutecznie zweryfikować, czy jego głos jest odpowiednio zarejestrowany i

policzony. Procedura pozwala uniknąć sabotażu, manipulacji lub fałszowania, z powodu możliwego fałszywego sprzętu lub oprogramowania. Drugą ważną właściwością protokołu jest to, że żaden głosujący nie może udowodnić, na kogo głosował. Eliminuje to, a przynajmniej zasadniczo ogranicza możliwość wymuszania, kupowania lub sprzedawania głosów. Z technicznego punktu widzenia protokół opiera się na kryptograficznym współdzieleniu sekretów, obliczeniach wielostronnych, modularnej arytmetyce z Chińskim Twierdzeniem o Resztach oraz rozproszonej księdze rejestru typu łańcuch bloków (ang. blockchain) bez żadnej strony obdarzonej zaufaniem.

Ponadto, przeprowadzimy dyskusję szeregu uwag krytycznych pojawiających się na świecie, które zasadniczo kwestionują wiarygodność elektronicznych procedur głosowania.

● Powrót do indeksu abstraktów sekcji

Maximal k-edge-colorings of graphs

Magdalena Tyniec-Motyka
tyniecm@agh.edu.pl
Akademia Górniczo Hutnicza

Maximal k-edge-coloring of a graph G of order n is a proper edge-coloring of a graph G with k colors such that no edge of G can be attached to G without violating the conditions of proper edge-coloring. We define the spectrum of maximal edge-coloring $MEC_k(n)$ as the set of all m such that there exists a maximal k-edge-coloring of some graph G, where $|V(G)| = n$ and $|E(G)| = m$.

In the talk the lower bound for the spectrum will be presented. Results concerning maximal edge-colorings of a graph of order n using $\chi'(n)$ colors will be mentioned. We show that the largest nontrivial number of colors used in maximal edge-coloring of a graph of order n is $2n - 4$. We also present constructions of such colorings for two, three and four colors and the largest nontrivial number of colors.

● Powrót do indeksu abstraktów sekcji

Skierowane wersje hipotez 1-2-3 i 1-2

Mariusz Woźniak
mwozniak@agh.edu.pl
Akademia Górniczo Hutnicza

Niech $G = (V, E)$ będzie grafem, k liczbą naturalną. Funkcję $f : E \to \{1, 2, \ldots, k\}$ nazywamy k-kolorowaniem grafu G. Kolorowanie f może byc interpretowane jako zastąpienie krawędzi $e \in E$ przez multikrawędź o krotności $f(e)$. Stopień wierzchołka $x \in V$ w tak otrzymanym multigrafie jest równy sumie kolorów wokół x. Hipoteza 1-2-3 (postawiona w [5]) mówi, że dla grafów bez krawędzi izolowanych istnieje takie 3-kolorowanie f, że odpowiedni multigraf jest *lokalnie nieregularny* tj. dla każdej krawędzi $xy \in E$ mamy $\sigma(x) \neq \sigma(y)$ gdzie $\sigma(x) = \sum_{e \ni x} f(e)$. Hipoteza 1-2 dotyczy sytuacji kiedy kolorujemy także wierzchołki grafu.

W trakcie referatu zobaczymy kilka wersji tych problemów w przypadku grafów skierowanych, a w szczególności wyniki zawarte w pracach wzmiankowanych w literaturze.

Bibliografia

[1] E. Barme, J. Bensmail, J. Przybyło, M. Woźniak, *On a directed variation of the* 1-2-3 *and* 1-2 *Conjectures*, Discrete Appl. Math. 217 (2017) 123–131.

[2] O. Baudon, J. Bensmail, É. Sopena, *An oriented version of the* 1-2-3 *Conjecture*, Discuss. Math. Graph Theory 35(1) (2015) 141–156.

[3] M. Borowiecki, J. Grytczuk, M. Pilśniak, *Coloring chip configurations on graphs and digraphs*, Inform. Process.

Lett. 112 (2012) 1–4.
[4] M. Horňák, J. Przybyło, M. Woźniak, *A note on a directed version of the 1-2-3 Conjecture*, Discrete Applied Math. **236** (2018), 472 – 476.
[5] M. Karoński, T. Łuczak, A. Thomason, *Edge weights and vertex colours*, J. Combin. Theory **B 91** (2004) 151–157.
● Powrót do indeksu abstraktów sekcji

Konstrukcje rzadkich maksymalnych niehamiltonowskich hipergrafów

Andrzej Żak
zakandrz@agh.edu.pl
Akademia Górniczo-Hutnicza

Wsółautor:
Andrzej Ruciński
rucinski@amu.edu.pl
Uniwersytet im. Adama Mickiewicza w Poznaniu

Dla $1 \leqslant \ell < k$, *ℓ-ciasnym k-cyklem* nazywamy k-jednolity hipergraf w którym, dla pewnego cyklicznego uporządkowania wierzchołków, każda krawędź składa się z k kolejnych wierzchołków, oraz każde dwie kolejne krawędzie mają ℓ wspólnych wierzchołków. k-jednolity hipergraf H jest *ℓ-hamiltonowski nasycony* jeżeli H nie zawiera ℓ-ciasnego k-cyklu Hamiltona, ale po dodaniu jakiejkolwiek nowej krawędzi taki cykl już zawiera. Niech $\mathrm{sat}(n, k, \ell)$ będzie najmniejszą liczbą krawędzi w ℓ-hamiltonowskim nasyconym k-jednolitym hipergrafie na n wierzchołkach. W przypadku grafów, Clark i Entringer pokazali w 1983 [1], że $\mathrm{sat}(n, 2, 1) = \lceil \frac{3n}{2} \rceil$. Wspólnie z Rucińskim pokazaliśmy w 2013 [2], że dla $k \geqslant 3$ i $\ell = 1$, oraz dla wszystkich $0.8k \leqslant \ell \leqslant k-1$, $\mathrm{sat}(n, k, \ell) = \Theta(n^\ell)$. Tym razem udowodnimy, że $\mathrm{sat}(n, 2\ell, \ell) = \Theta\left(n^\ell\right)$.

Bibliografia

[1] L. Clark and R. Entringer, Smallest maximally non-Hamiltonian graphs, *Period. Math. Hungar.*, **14**: 57–68

(1983).
[2] A. Ruciński and A. Żak, Hamilton saturated hypergraphs of essentially minimum size, *Electr. J. Combin.*, **20**: P25 (2013).

● Powrót do indeksu abstraktów sekcji