Das Haus vom Nikolaus

N. Imeta (mail@spam.blorx) 30. Februar 2010

1 Grundlagen

Definition 1.1 (Das Haus vom Nikolaus)**.** Das *Haus vom Nikolaus* ist der Graph (V, E), der wie folgt gegeben ist:

$$V := \{1, \dots, 5\}$$
$$E := \big\{\{1,2\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\big\}$$

Man kann das Haus vom Nikolaus wie in Abbildung 1 veranschaulichen (weitere Informationen zu Ti*k*Z und PGF finden sich in der Dokumentation [15]).

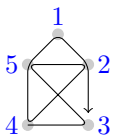

Abbildung 1: Das Haus vom Nikolaus

2 Eigenschaften des Hauses vom Nikolaus

Satz 2.1 (Das Haus vom Nikolaus)**.** *Das Haus vom Nikolaus ist unvollständig.*

Beweis. Wir verwenden die Notation aus Definition 1.1. Da die Kante $\{1,3\}$ nicht im Haus vom Nikolaus enthalten ist, ist das Haus vom Nikolaus kein vollständiger Graph. □

3 Beispiele

Beispiel 3.1.

- Hier ein Beispiel
- . . . und noch eins

Aufgabe 3.2. Vergessen Sie nicht, ein paar Aufgaben einzustreuen, an denen die Teilnehmer nochmal ihre Kenntnisse überprüfen können.

Seminar „Mathematical Literacy: Cryptocurrencies“, SS 2019, Universität Regensburg

Literatur

[1] A.M. Antonopoulos. *Mastering Bitcoin. Programming the Open Blockchain*, second edition, O'Reilly, 2017.

[2] A.M. Antonopoulos, G. Wood. *Mastering Ethereum. Building Smart Contracts and Dapps*, O'Reilly, 2018.

[3] A. Beutelspacher. *Das ist o.B.d.A. trivial!*, neunte Auflage, Vieweg+Teubner, 2009.

[4] I. Bentov, A. Gabizon, A. Mizrahi. Cryptocurrencies without proof of work, *FC 2016: Financial Cryptography and Data Security*, pp. 142–157, Lecture Notes in Computer Science, 9604, 2016.
arXiv:1406.5694 [cs.CR]

[5] A. Charapko, A. Ailijiang, M. Demirbas. Bridging Paxos and blockchain consensus, *2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*, 2018.

[6] B. David, P. Gaži, A. Kiayias, A. Russell. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake Blockchain, *EUROCRYPT 2018: Advances in Cryptology*, pp. 66–98, Lecture Notes in Computer Science, 10821, Springer, 2018.

[7] C. Decker, R. Wattenhofer. Bitcoin transaction malleability and MtGox, *ESORICS 2014*, pp. 313–326, Lecture Notes in Computer Science, 8713, 2014.

[8] J. Hoffstein, J. Pipher, J.H. Silverman. *An Introduction to Mathematical Cryptography*, second edition, Undergraduate Texts in Mathematics, Springer, 2014.

[9] A. Kiayias, A. Russell, B. David, R. Oliynykov. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol, *CRYPTO 2017: Advances in Cryptology*, pp. 357–388, Lecture Notes in Computer Science, 10401, Springer, 2017.

[10] L. Lamport. The part-time parliament, *ACM Transactions on Computer Systems*, 16(2), 133–169, 1998.

[11] L. Lamport. Paxos made simple, *ACM Sigact News*, 34(2), 18–25, 2001.

[12] J. Katz, Y. Lindell. *Introduction to Modern Cryptography*, Chapman & Hall, 2015.

[13] F. Mittelbach, M. Goossens, J. Braams, D. Carlisle, C. Rowley. *The LaTeX Companion*, zweite Auflage, Addison-Wesley, 2004.

[14] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
https://bitcoin.org/bitcoin.pdf

[15] T. Tantau. *The* Ti*k*Z *and* PGF *Packages*,
http://www.ctan.org/tex-archive/graphics/pgf/base/doc/generic/pgf/pgfmanual.pdf

[16] R. Wattenhofer. *Distributed Ledger Technology. The Science of Blockchain*, second revised edition, Inverted Forest Publishing, 2017.

[17] G. Wood. Ethereum: A secure decentralised generalised transaction ledger, yellow paper, 2014–
https://ethereum.github.io/yellowpaper/paper.pdf