Analýza odolnosti Stellar konsenzus protokolu voči Byzantínskym chybám

Samuel Sládek

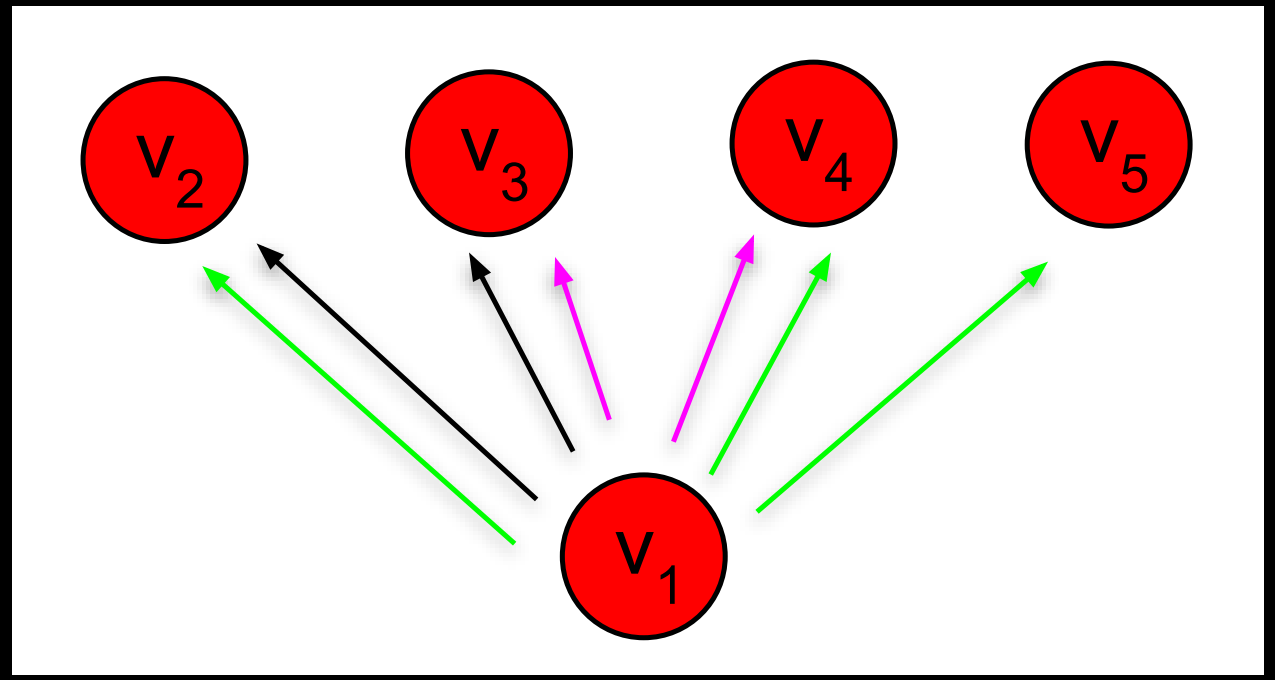
RNDr. Tomáš Kulich, PhD.

STELLAR KONSENZUS PROTOKOL

- Decentralizovaná kontrola
- Nízka latencia
- Otvorené členstvo
- Flexibilná dôvera
- Odolnosť voči zlyhaniam

KVÓROVÉ REZY

$$\mathbf{Q}(v_1) = \{\{v_2, v_3\}, \{v_3, v_4\}, \{v_2, v_4, v_5\}\}$$

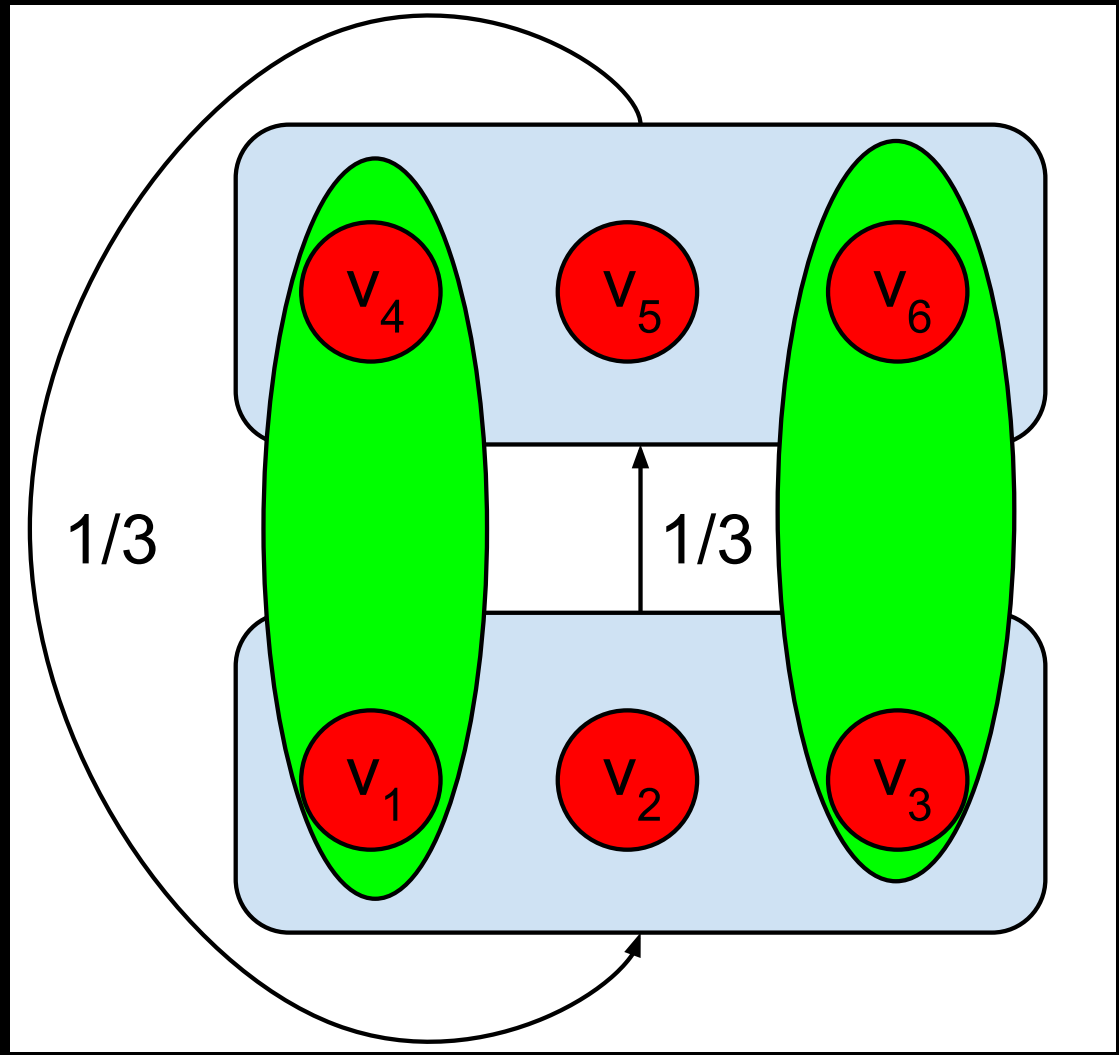


ODOLNOSŤ SIETE

- Koeficient životaschopnosti
- Bezpečnostný koeficient
- Koeficient odolnosti

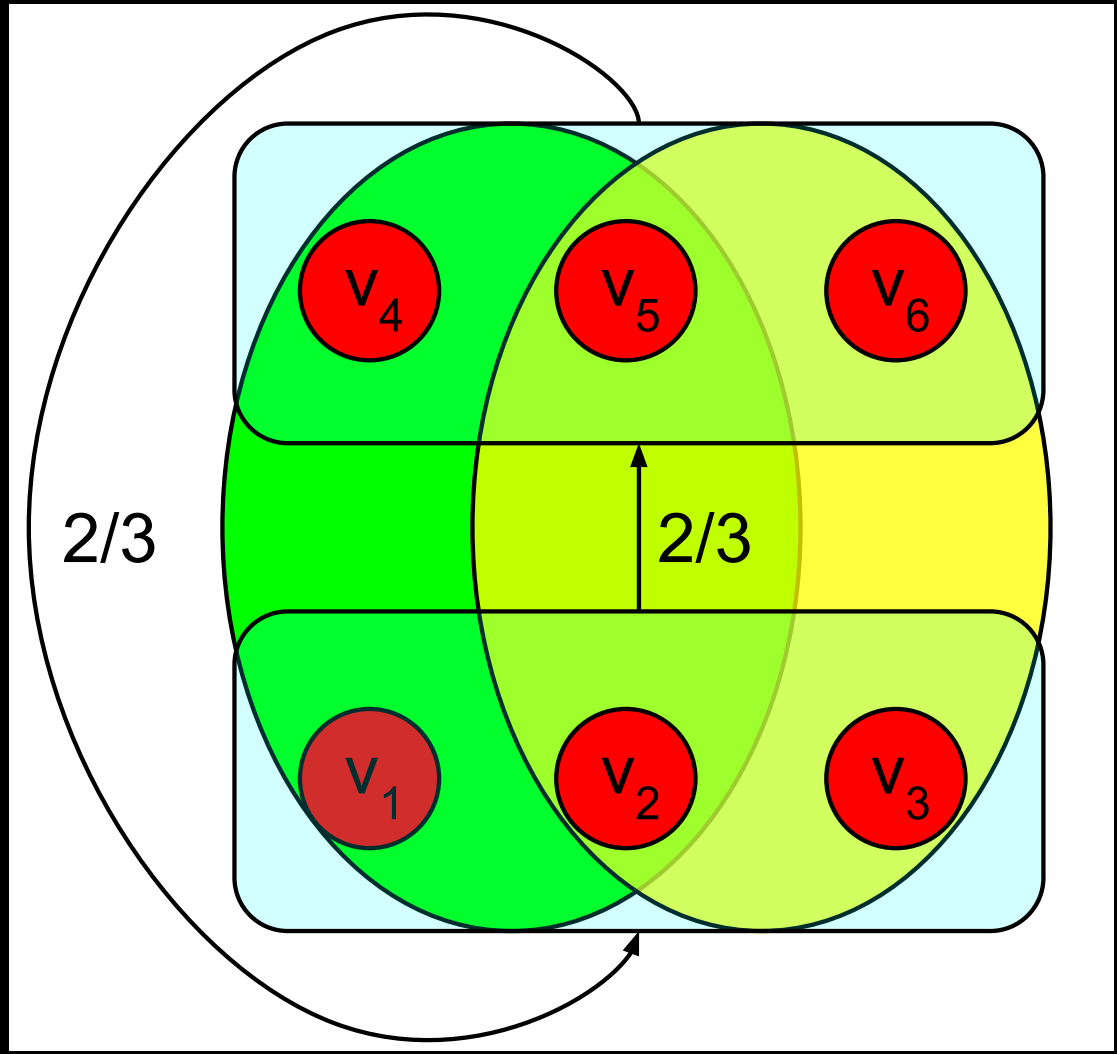
ODOLNOSŤ SIETE

- Určiť koeficienty je NP-ťažké
- Skúmame len NQK-siete

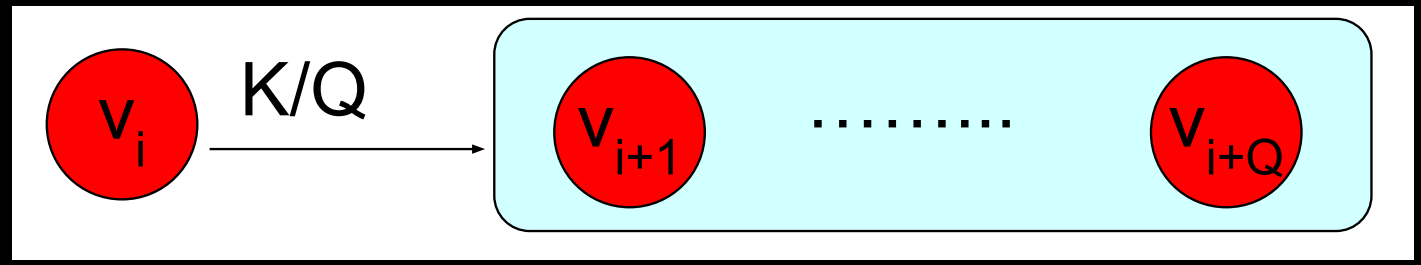


ODOLNOSŤ SIETE

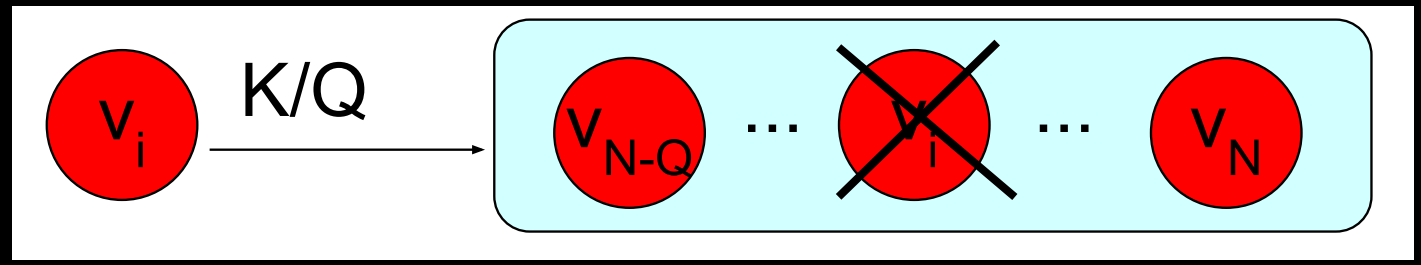
- Určiť koeficienty je NP-ťažké
- Skúmame len NQK-siete



REŤAZOVÉ SIETE

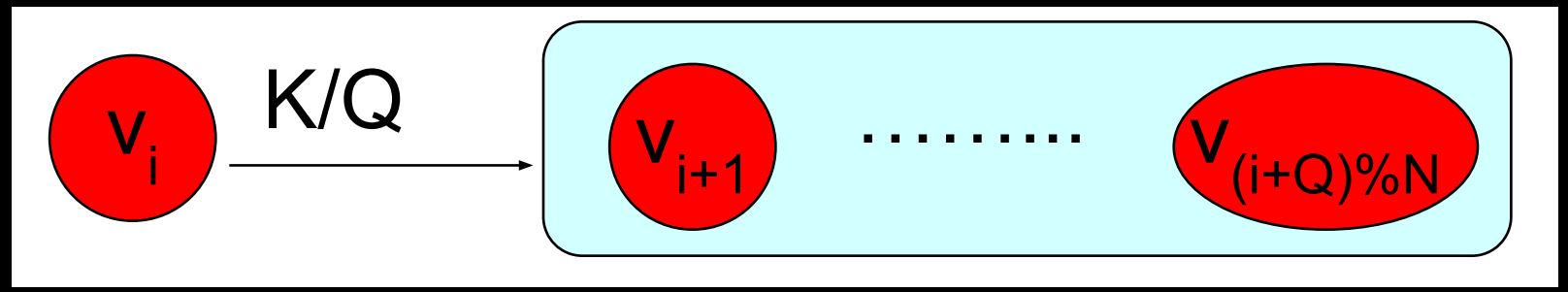


OPTIMÁLNE JE VOLIŤ K = $\frac{2}{3}$Q



DOSAHUJE ODOLNOSŤ $\frac{1}{3}$Q ZLYHANÍ

CYKLICKÉ SIETE



OPTIMÁLNE JE VOLIŤ K = $\frac{Q+N+1}{2N+Q}$Q

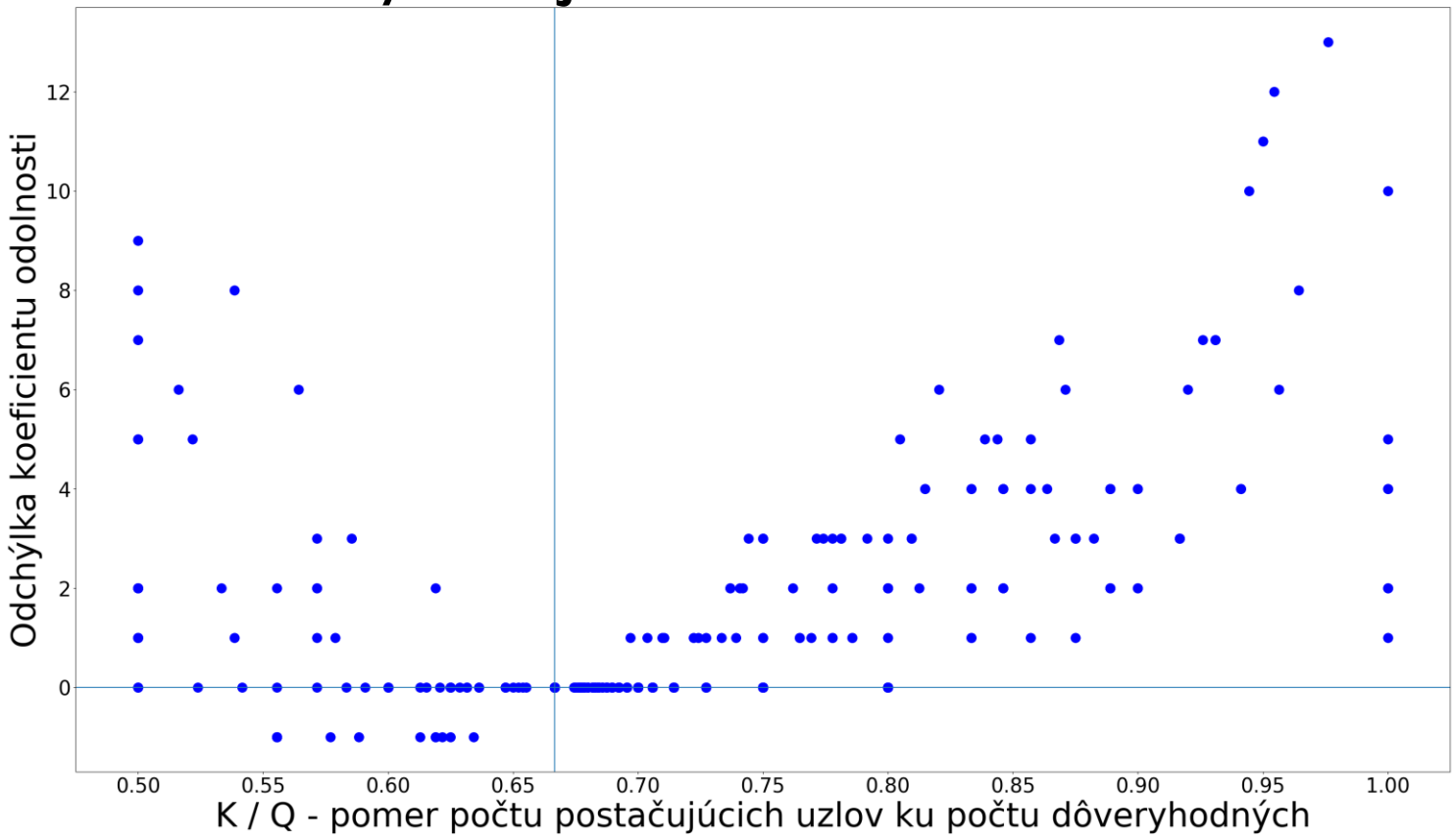
DOKÁŽEME ZÍSKAŤ ODOLNOSŤ BLÍZKU $\frac{1}{2}$Q CHYBÁM

NÁHODNÉ SIETE

Siete v ktorých je do 17 uzlov

NÁHODNÉ SIETE

Siete v ktorých je do 50 uzlov



ZHRNUTIE

- Ukázali sme, že vyrátať jednotlivé koeficienty je **NP-ťažké**
- Rozanalyzovali sme odolnosť **reťazových** a **cyklických** sietí
- Zistili sme vhodné nastavenie parametrov pre **náhodné** siete

Ďakujem za pozornosť